INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

April 2025

The total zero-day vulnerabilities count for April month: 1103

Command Injection	SQL Injection	SSRF	Path Traversal	Cross-Site Scripting	HTML Injection	XXE
29	247	29	17	778	1	2

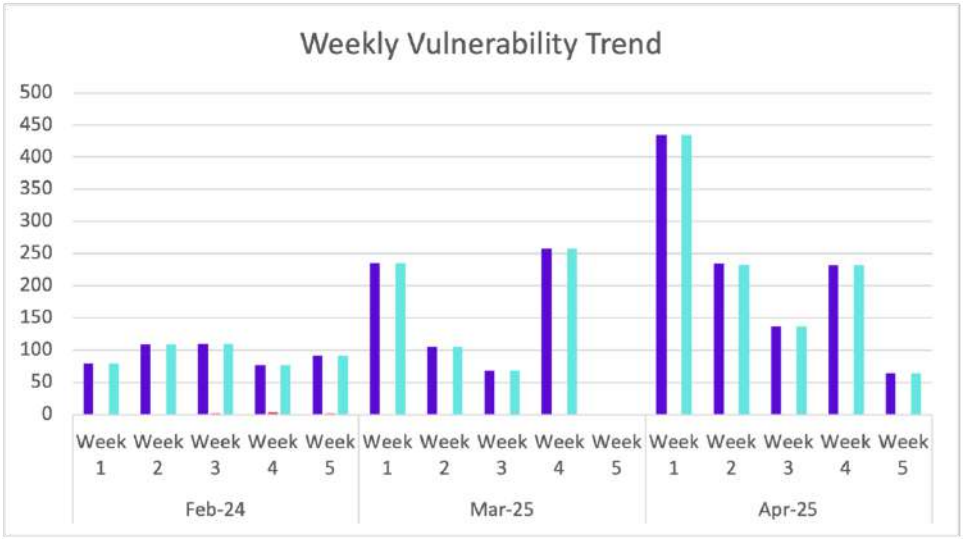
Zero-day vulnerabilities protected through core rules	1103
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities found by Indusface WAS	1103

- To enable custom rules, please contact support@indusface.com
- Learn more about zero-day vulnerabilities, detection, and prevention, here

Vulnerability Trend:

The weekly trend displays the total number of vulnerabilities discovered and the type of protection provided for the last quarter.

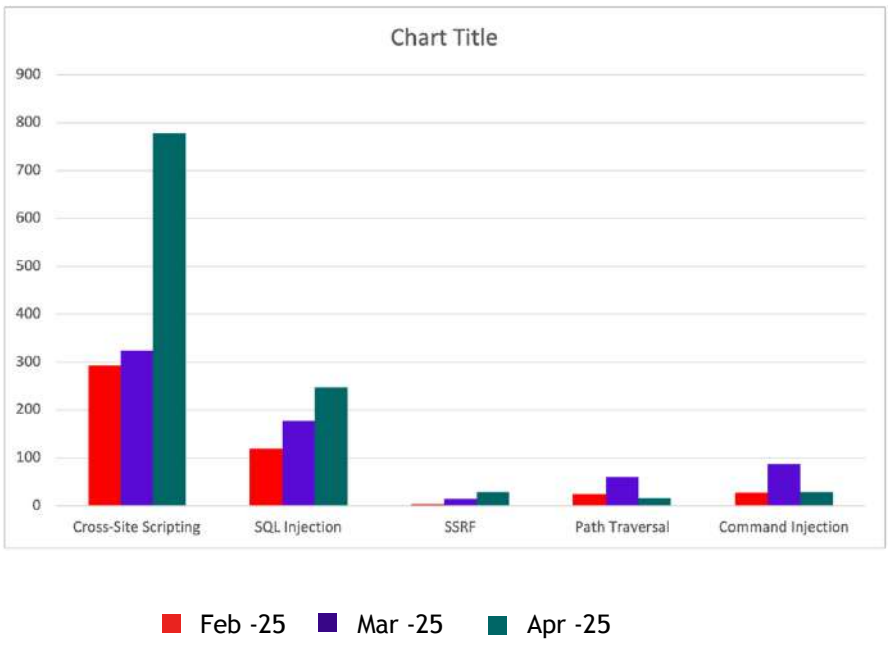
Weekly Vulnerability Trend



of the zero-day vulnerabilities were protected by the core rules in the last month

of the zero-day vulnerabilities were reported by Indusface Scanner in the last month

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-11235	Reference counting in php_request_shutdown causes Use-After-Free	In PHP versions 8.3.* before 8.3.19 and 8.4.* before 8.4.5, a code sequence involving __set handler or ??= operator and exceptions can lead to a use-after-free vulnerability. If the third party can control the memory layout leading to this, for example by supplying specially crafted inputs to the script, it could lead to remote code execution.	Patched by core rule	Y
CVE-2024-9773	Improper Neutralization of Special Elements used in a Command ('Command Injection') in GitLab	An issue was discovered in GitLab EE affecting all versions starting from 14.9 before 17.8.6, all versions starting from 17.9 before 17.8.3, all versions starting from 17.10 before 17.10.1. An input validation issue in the Harbor registry integration could have allowed a maintainer to add malicious code to the CLI commands shown in the UI.	Patched by core rule	Y
CVE-2025-2257	Total Upkeep – WordPress Backup Plugin plus Restore & Migrate by BoldGrid <= 1.16.10 - Authenticated (Admin+) Command Injection	The Total Upkeep – WordPress Backup Plugin plus Restore & Migrate by BoldGrid plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.16.10 via the compression_level setting. This is due to the plugin using the compression_level setting in proc_open() without any validation. This makes it possible for authenticated attackers, with administrator-level access and above, to execute code on the server.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-26996	WordPress Sign-up Sheets plugin <= 2.3.0.1 - Shortcode Injection vulnerability	Improper Control of Generation of Code ('Code Injection') vulnerability in Fetch Designs Sign-up Sheets allows Code Injection. This issue affects Sign-up Sheets: from n/a through 2.3.0.1.	Patched by core rule	Y
CVE-2025-2916	Aishida Call Center System amr2mp3 command injection	A vulnerability, which was classified as critical, has been found in Aishida Call Center System up to 20250314. This issue affects some unknown processing of the file /doscall/weixin/open/amr2mp3. The manipulation of the argument File leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-3002	Digital China DCME-520 mon_merge_stat_hist.php os command injection	A vulnerability, which was classified as critical, has been found in Digital China DCME-520 up to 20250320. This issue affects some unknown processing of the file /usr/local/WWW/function/audit/newstatistics/mon_merge_stat_hist.php. The manipulation of the argument type_name leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-30370	jupyterlab-git has a command injection vulnerability in "Open Git Repository in Terminal"	jupyterlab-git is a JupyterLab extension for version control using Git. On many platforms, a third party can create a Git repository under a name that includes a shell command substitution string in the syntax $(<command>). These directory names are allowed in macOS and a majority of Linux distributions. If a user starts jupyter-lab in a parent directory of this inappropriately-named Git repository, opens it, and clicks "Git > Open Git Repository in Terminal" from the menu bar, then the injected command <command> is run in the user's shell without the user's permission. This issue is occurring because when that menu entry is clicked, jupyterlab-git opens the terminal and runs cd <git-repo-path> through the shell to set the current directory. Doing so runs any command substitution strings present in the directory name, which leads to the command injection issue described here. A previous patch provided an incomplete fix. This vulnerability is fixed in 0.51.1.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-31499	Jellyfin Vulnerable to Argument Injection in FFmpeg	Jellyfin is an open source self hosted media server. Versions before 10.10.7 are vulnerable to argument injection in FFmpeg. This can be leveraged to possibly achieve remote code execution by anyone with credentials to a low-privileged user. This vulnerability was previously reported in CVE-2023-49096 and patched in version 10.8.13, but the patch can be bypassed. The original fix sanitizes some parameters to make injection impossible, but certain unsanitized parameters can still be used for argument injection. The same unauthenticated endpoints are vulnerable: /Videos/<itemId>/stream and /Videos/<itemId>/stream.<container>, likely alongside similar endpoints in AudioController. This argument injection can be exploited to achieve arbitrary file write, leading to possible remote code execution through the plugin system. While the unauthenticated endpoints are vulnerable, a valid itemId is required for exploitation and any authenticated attacker could easily retrieve a valid itemId to make the exploit work. This vulnerability is patched in version 10.10.7.	Patched by core rule	Y
CVE-2025-3163	InternLM LMDeploy conf.py open code injection	A vulnerability was found in InternLM LMDeploy up to 0.7.1. It has been declared as critical. Affected by this vulnerability is the function Open of the file lmdeploy/docs/en/conf.py. The manipulation leads to code injection. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3164	Tencent Music Entertainment SuperSonic H2 Database Connection testConnect code injection	A vulnerability was found in Tencent Music Entertainment SuperSonic up to 0.9.8. It has been rated as critical. Affected by this issue is some unknown functionality of the file /api/semantic/database/testConnect of the component H2 Database Connection Handler. The manipulation leads to code injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-32200	WordPress Advanced WordPress Backgrounds Plugin <= 1.12.4 - Content Injection vulnerability	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Nikita Advanced WordPress Backgrounds allows Code Injection. This issue affects Advanced WordPress Backgrounds: from n/a through 1.12.4.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-32432	Craft CMS Allows Remote Code Execution	Craft is a flexible, user-friendly CMS for creating custom digital experiences on the web and beyond. Starting from version 3.0.0-RC1 to before 3.9.15, 4.0.0-RC1 to before 4.14.15, and 5.0.0-RC1 to before 5.6.17, Craft is vulnerable to remote code execution. This is a high-impact, low-complexity attack vector. This issue has been patched in versions 3.9.15, 4.14.15, and 5.6.17, and is an additional fix for CVE-2023-41892.	Patched by core rule	Y
CVE-2025-32434	PyTorch: `torch.load` with `weights_only=True` leads to remote code execution	PyTorch is a Python package that provides tensor computation with strong GPU acceleration and deep neural networks built on a tape-based autograd system. In version 2.5.1 and prior, a Remote Command Execution (RCE) vulnerability exists in PyTorch when loading a model using torch.load with weights_only=True. This issue has been patched in version 2.6.0.	Patched by core rule	Y
CVE-2025-3249	TOTOLINK A6000R mtkwifi.lua apcli_cancel_wps command injection	A vulnerability classified as critical was found in TOTOLINK A6000R 1.0.1-B20201211.2000. Affected by this vulnerability is the function apcli_cancel_wps of the file /usr/lib/lua/luci/controller/mtkwifi.lua. The manipulation leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-32778	Web-Check allows command Injection via Unvalidated URL in Screenshot API	Web-Check is an all-in-one OSINT tool for analyzing any website. A command injection vulnerability exists in the screenshot API of the Web Check project (Lissy93/web-check). The issue stems from user-controlled input (url) being passed unsanitized into a shell command using exec(), allowing attackers to execute arbitrary system commands on the underlying host. This could be exploited by sending crafted url parameters to extract files or even establish remote access. The vulnerability has been patched by replacing exec() with execFile(), which avoids using a shell and properly isolates arguments.	Patched by core rule	Y
CVE-2025-32955	Harden-Runner Evasion of 'disable-sudo' policy	Harden-Runner is a CI/CD security agent that works like an EDR for GitHub Actions runners. Versions from 0.12.0 to before 2.12.0 are vulnerable to `disable-sudo` bypass. Harden-Runner includes a policy option `disable-sudo` to prevent the GitHub Actions runner user from using sudo. This is implemented by removing the runner user	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		from the sudoers file. However, this control can be bypassed as the runner user, being part of the docker group, can interact with the Docker daemon to launch privileged containers or access the host filesystem. This allows the attacker to regain root access or restore the sudoers file, effectively bypassing the restriction. This issue has been patched in version 2.12.0.		
CVE-2025-3509	Pre-Receive Hook Remote Code Execution vulnerability was identified in GitHub Enterprise Server that allowing Privilege Escalation	A Remote Code Execution (RCE) vulnerability was identified in GitHub Enterprise Server that allowed attackers to execute arbitrary code by exploiting the pre-receive hook functionality, potentially leading to privilege escalation and system compromise. The vulnerability involves using dynamically allocated ports that become temporarily available, such as during a hot patch upgrade. This means the vulnerability is only exploitable during specific operational conditions, which limits the attack window. Exploitation required either site administrator permissions to enable and configure pre-receive hooks or a user with permissions to modify repositories containing pre-receive hooks where this functionality was already enabled. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.17 and was fixed in versions 3.16.2, 3.15.6, 3.14.11, 3.13.14. This vulnerability was reported via the GitHub Bug Bounty program.	Patched by core rule	Y
CVE-2025-3539	H3C Magic BE18000 HTTP POST Request getBasicInfo FCGI_CheckStringIfContainsSemicolon command injection	A vulnerability classified as critical has been found in H3C Magic NX15, Magic NX30 Pro, Magic NX400, Magic R3010 and Magic BE18000 up to V100R014. Affected is the function FCGI_CheckStringIfContainsSemicolon of the file /api/wizard/getBasicInfo of the component HTTP POST Request Handler. The manipulation leads to command injection. The attack can only be done within the local network. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-3540	H3C Magic NX15/Magic NX30 Pro/Magic NX400/Magic R3010 HTTP POST Request getCapability FCGI_WizardProtoProcess command injection	A vulnerability classified as critical was found in H3C Magic NX15, Magic NX30 Pro, Magic NX400 and Magic R3010 up to V100R014. Affected by this vulnerability is the function FCGI_WizardProtoProcess of the file /api/wizard/getCapability of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the component HTTP POST Request Handler. The manipulation leads to command injection. The attack can only be initiated within the local network. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component.		
CVE-2025-3541	H3C Magic NX15/Magic NX30 Pro/Magic NX400/Magic R3010 HTTP POST Request getSpecs FCGI_WizardProtoProcess command injection	A vulnerability, which was classified as critical, has been found in H3C Magic NX15, Magic NX30 Pro, Magic NX400 and Magic R3010 up to V100R014. Affected by this issue is the function FCGI_WizardProtoProcess of the file /api/wizard/getSpecs of the component HTTP POST Request Handler. The manipulation leads to command injection. The attack needs to be done within the local network. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-3542	H3C Magic NX15/Magic NX400/Magic R3010 HTTP POST Request getsyncpppoecfg FCGI_WizardProtoProcess command injection	A vulnerability, which was classified as critical, was found in H3C Magic NX15, Magic NX400 and Magic R3010 up to V100R014. This affects the function FCGI_WizardProtoProcess of the file /api/wizard/getsyncpppoecfg of the component HTTP POST Request Handler. The manipulation leads to command injection. The attack needs to be initiated within the local network. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-3543	H3C Magic NX15/Magic NX30 Pro/Magic NX400/Magic R3010 HTTP POST Request setsyncpppoecfg FCGI_WizardProtoProcess command injection	A vulnerability has been found in H3C Magic NX15, Magic NX30 Pro, Magic NX400 and Magic R3010 up to V100R014 and classified as critical. This vulnerability affects the function FCGI_WizardProtoProcess of the file /api/wizard/setsyncpppoecfg of the component HTTP POST Request Handler. The manipulation leads to command injection. Access to the local network is required for this attack. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-3544	H3C Magic BE18000 HTTP POST Request getCapabilityWeb FCGI_CheckStringIfContainsSemicolon command injection	A vulnerability was found in H3C Magic NX15, Magic NX30 Pro, Magic NX400, Magic R3010 and Magic BE18000 up to V100R014 and classified as critical. This issue affects the function FCGI_CheckStringIfContainsSemicolon of the file /api/wizard/getCapabilityWe	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		b of the component HTTP POST Request Handler. The manipulation leads to command injection. Access to the local network is required for this attack to succeed. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component.		
CVE-2025-3545	H3C Magic BE18000 HTTP POST Request setLanguage FCGI_CheckStringIfContainsSemicolon command injection	A vulnerability was found in H3C Magic NX15, Magic NX30 Pro, Magic NX400, Magic R3010 and Magic BE18000 up to V100R014. It has been classified as critical. Affected is the function FCGI_CheckStringIfContainsSemicolon of the file /api/wizard/setLanguage of the component HTTP POST Request Handler. The manipulation leads to command injection. The attack needs to be approached within the local network. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-3546	H3C Magic BE18000 HTTP POST Request getLanguage FCGI_CheckStringIfContainsSemicolon command injection	A vulnerability was found in H3C Magic NX15, Magic NX30 Pro, Magic NX400, Magic R3010 and Magic BE18000 up to V100R014. It has been declared as critical. Affected by this vulnerability is the function FCGI_CheckStringIfContainsSemicolon of the file /api/wizard/getLanguage of the component HTTP POST Request Handler. The manipulation leads to command injection. The attack can only be done within the local network. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-3729	SourceCodester Web-based Pharmacy Product Management System Database Backup backup.php os command injection	A vulnerability, which was classified as critical, has been found in SourceCodester Web-based Pharmacy Product Management System 1.0. This issue affects some unknown processing of the file backup.php of the component Database Backup Handler. The manipulation of the argument txtdbname leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3816	westboy CicadasCMS Scheduled Task save os command injection	A vulnerability classified as critical was found in westboy CicadasCMS 2.0. This vulnerability affects unknown code of the file /system/schedule/save of the component Scheduled Task Handler. The manipulation leads to os command injection. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3842	panhainan DS-Java FileUpload.java uploadUserPic.action code injection	A vulnerability was found in panhainan DS-Java 1.0 and classified as critical. This issue affects the function uploadUserPic.action of the file src/com/phn/action/FileUpload.java. The manipulation of the argument fileUpload leads to code injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-43858	YoutubeDLSharp allows command injection on windows system due to non sanitized arguments	YoutubeDLSharp is a wrapper for the command-line video downloaders youtube-dl and yt-dlp. In versions starting from 1.0.0-beta4 and prior to 1.1.2, an unsafe conversion of arguments allows the injection of a malicious commands when starting `yt-dlp` from a commands prompt running on Windows OS with the `UseWindowsEncodingWorkaround` value defined to true (default behavior). If a user is using built-in methods from the YoutubeDL.cs file, the value is true by default and a user cannot disable it from these methods. This issue has been patched in version 1.1.2.	Patched by core rule	Y

Path Traversal Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-54362	WordPress GetShop ecommerce plugin <= 1.3 - Path Traversal vulnerability	Path Traversal vulnerability in NotFound GetShop ecommerce allows Path Traversal. This issue affects GetShop ecommerce: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-2961	opensolon org.noear.solon.core.handle.RenderManager aa render_mav path traversal	A vulnerability classified as problematic was found in opensolon up to 3.1.0. This vulnerability affects the function render_mav of the file /aa of the component org.noear.solon.core.handle.RenderManager. The manipulation of the argument template with the input ../org/example/HelloApp.class leads to path traversal: '../filedir'. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-30095	N/A	VyOS 1.3 through 1.5 (fixed in 1.4.2) or any Debian-based system using dropbear in combination with live-build has the same Dropbear private host keys across different installations. Thus, an attacker can conduct active man-in-the-middle attacks against SSH connections if Dropbear is enabled as the SSH daemon. I n VyOS, this is not the default configuration for the system SSH daemon, but is for the console service. To mitigate this, one can run "rm -f /etc/dropbear/*key*" and/or "rm -f /etc/dropbear-initramfs/*key*" and then dropbearkey -t rsa -s 4096 -f /etc/dropbear_rsa_host_key and reload the service or reboot the system before using Dropbear as the SSH daemon (this clears out all keys mistakenly built into the release image) or update to the latest version of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		VyOS 1.4 or 1.5. Note that this vulnerability is not unique to VyOS and may appear in any Debian-based Linux distribution that uses Dropbear in combination with live-build, which has a safeguard against this behavior in OpenSSH but no equivalent one for Dropbear.		
CVE-2025-3043	GuoMinJim PersonManage login preHandle path traversal	A vulnerability, which was classified as critical, has been found in GuoMinJim PersonManage 1.0. This issue affects the function preHandle of the file /login/. The manipulation of the argument Request leads to path traversal. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available.	Patched by core rule	Y
CVE-2025-30834	WordPress Bit Assist plugin <= 1.5.4 - Path Traversal vulnerability	Path Traversal vulnerability in Bit Apps Bit Assist allows Path Traversal. This issue affects Bit Assist: from n/a through 1.5.4.	Patched by core rule	Y
CVE-2025-30966	WordPress WPJobBoard plugin < 5.11.1 - Path Traversal vulnerability	Path Traversal vulnerability in NotFound WPJobBoard allows Path Traversal. This issue affects WPJobBoard: from n/a through n/a.	Patched by core rule	Y
CVE-2025-31131	Path Traversal allowing arbitrary read of files in Yeswiki	YesWiki is a wiki system written in PHP. The squelette parameter is vulnerable to path traversal attacks, enabling read access to arbitrary files on the server. This vulnerability is fixed in 4.5.2.	Patched by core rule	Y
CVE-2025-32017	Umbraco has a Management API Vulnerability to Path Traversal With Authenticated Users	Umbraco is a free and open source .NET content management system. Authenticated users to the Umbraco backoffice are able to craft management API request that exploit a path traversal vulnerability to upload files into a incorrect location. The issue affects Umbraco 14+ and is patched in 14.3.4	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and 15.3.1.		
CVE-2025-3214	JFinal CMS readTemplate engine.getTemplate path traversal	A vulnerability has been found in JFinal CMS up to 5.2.4 and classified as problematic. Affected by this vulnerability is the function engine.getTemplate of the file /readTemplate. The manipulation of the argument template leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. The vendor explains that this is not a bug but a feature.	Patched by core rule	Y
CVE-2025-32205	WordPress piotnetforms plugin <=1.0.30 - Path Traversal vulnerability	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in piotnetdotcom Piotnet Forms. This issue affects Piotnet Forms: from n/a through 1.0.30.	Patched by core rule	Y
CVE-2025-32779	labsai/eddi Vulnerable to Path Traversal (Zip Slip) in ZIP Import Function	E.D.D.I (Enhanced Dialog Driven Interface) is a middleware to connect and manage LLM API bots. In versions before 5.5.0, an attacker with access to the `/backup/import` API endpoint can write arbitrary files to locations outside the intended extraction directory due to a Zip Slip vulnerability. Although the application runs as a non-root user (`185`), limiting direct impact on system-level files, this vulnerability can still be exploited to overwrite application files (e.g., JAR libraries) owned by the application user. This overwrite can potentially lead to Remote Code Execution (RCE) within the application's context. This issue has been patched in version 5.5.0.	Patched by core rule	Y
CVE-2025-32943	PeerTube HLS Video Files Path Traversal	The vulnerability allows any authenticated user to leak the contents of arbitrary ".m3u8" files from the PeerTube server	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		due to a path traversal in the HLS endpoint.		
CVE-2025-3317	fumiao opencms dataPage.jsp path traversal	A vulnerability classified as problematic has been found in fumiao opencms up to a0fafa5cff58719e9b27c2a2eec204cc165ce14f. Affected is an unknown function of the file opencms-dev/src/main/webapp/view/admin/document/dataPage.jsp. The manipulation of the argument path leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available.	Patched by core rule	Y
CVE-2025-3381	zhangyanbo2007 youkefu File Upload WebIMController.java path traversal	A vulnerability, which was classified as critical, was found in zhangyanbo2007 youkefu 4.2.0. This affects an unknown part of the file WebIMController.java of the component File Upload. The manipulation of the argument ID leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3686	misstt123 oasys show image path traversal	A vulnerability classified as problematic was found in misstt123 oasys 1.0. Affected by this vulnerability is the function image of the file /show. The manipulation leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.	Patched by core rule	Y
CVE-2025-39598	WordPress Administrator Z <= 2025.03.28 - Directory Traversal Vulnerability	Path Traversal vulnerability in Quý Lê 91 Administrator Z allows Path Traversal. This issue affects Administrator Z:	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		from n/a through 2025.03.28.		
CVE-2025-46546	N/A	In Sherpa Orchestrator 141851, multiple time-based blind SQL injections can be performed by an authenticated user. This affects api/gui/asset/list, /api/gui/files/export/csv/, /api/gui/files/list, /api/gui/process/export/csv, /api/gui/process/export/xlsx, /api/gui/process/listAll, /api/gui/processVersion/export/csv/, /api/gui/processVersion/export/xlsx/, /api/gui/processVersion/list/, /api/gui/robot/list/, /api/gui/task/export/csv/, /api/gui/task/export/xlsx/, and /api/gui/task/list/.	Patched by core rule	Y

Server-side Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-1781	N/A	There is a XXE in W3CSS Validator versions before cssval-20250226 that allows an attacker to use specially-crafted XML objects to coerce server-side request forgery (SSRF). This could be exploited to read arbitrary local files if an attacker has access to exception messages.	Patched by core rule	Y
CVE-2025-22672	WordPress Video & Photo Gallery for Ultimate Member plugin <= 1.1.2 - Server Side Request Forgery (SSRF) vulnerability	Server-Side Request Forgery (SSRF) vulnerability in SuitePlugins Video & Photo Gallery for Ultimate Member allows Server Side Request Forgery.This issue affects Video & Photo Gallery for Ultimate Member: from n/a through 1.1.2.	Patched by core rule	Y
CVE-2025-26990	WordPress Royal Elementor Addons plugin <= 1.7.1006 - Server Side Request Forgery (SSRF) vulnerability	Server-Side Request Forgery (SSRF) vulnerability in WP Royal Royal Elementor Addons allows Server Side Request Forgery. This issue affects Royal Elementor Addons: from n/a through 1.7.1006.	Patched by core rule	Y
CVE-2025-2835	zhangyd-c OneBlog RestApiController.java autoLink server-side request forgery	A vulnerability was found in zhangyd-c OneBlog up to 2.3.9. It has been declared as problematic. Affected by this vulnerability is the function autoLink of the file com/zyd/blog/controller/RestApiController.java. The manipulation leads to server-side request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-2997	zhangyanbo2007 youkefu url server-side request forgery	A vulnerability was found in zhangyanbo2007 youkefu 4.2.0. It has been classified as critical. Affected is an unknown function of the file /res/url. The manipulation of the argument url leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-30914	WordPress Metform Elementor Contact Form Builder plugin <= 3.9.2 - Server Side Request Forgery (SSRF) vulnerability	Server-Side Request Forgery (SSRF) vulnerability in XpeedStudio Metform allows Server Side Request Forgery. This issue affects Metform: from n/a through	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		3.9.2.		
CVE-2025-30964	WordPress Photography theme <= 7.5.2 - Server Side Request Forgery (SSRF) vulnerability	Server-Side Request Forgery (SSRF) vulnerability in EPC Photography. This issue affects Photography: from n/a through 7.5.2.	Patched by core rule	Y
CVE-2025-31009	WordPress IndieBlocks <= 0.13.1 - Server Side Request Forgery (SSRF) Vulnerability	Server-Side Request Forgery (SSRF) vulnerability in Jan Boddez IndieBlocks allows Server Side Request Forgery. This issue affects IndieBlocks: from n/a through 0.13.1.	Patched by core rule	Y
CVE-2025-31076	WordPress WP Compress for MainWP plugin <= 6.30.03 - Server Side Request Forgery (SSRF) vulnerability	Server-Side Request Forgery (SSRF) vulnerability in WP Compress WP Compress for MainWP allows Server Side Request Forgery. This issue affects WP Compress for MainWP: from n/a through 6.30.03.	Patched by core rule	Y
CVE-2025-31116	Mobile Security Framework (MobSF) has a SSRF Vulnerability fix bypass on assetlinks_check with DNS Rebinding	Mobile Security Framework (MobSF) is a pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis. The mitigation for CVE-2024-29190 in valid_host() uses socket.gethostbyname(), which is vulnerable to SSRF abuse using DNS rebinding technique. This vulnerability is fixed in 4.3.2.	Patched by core rule	Y
CVE-2025-31490	AutoGPT allows SSRF due to DNS Rebinding in requests wrapper	AutoGPT is a platform that allows users to create, deploy, and manage continuous artificial intelligence agents that automate complex workflows. Prior to 0.6.1, AutoGPT allows SSRF due to DNS Rebinding in requests wrapper. AutoGPT is built with a wrapper around Python's requests library, hardening the application against SSRF. The code for this wrapper can be found in autogpt_platform/backend/backend/util/request.py. The requested hostname of a URL which is being requested is validated, ensuring that it does not resolve to any local ipv4 or ipv6 addresses. However, this check is not sufficient, as a DNS server may initially respond with a non-blocked address, with a TTL of 0. This means that the initial resolution would appear as a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		non-blocked address. In this case, validate_url() will return the url as successful. After validate_url() has successfully returned the url, the url is then passed to the real request() function. When the real request() function is called with the validated url, request() will once again resolve the address of the hostname, because the record will not have been cached (due to TTL 0). This resolution may be in the "invalid range". This type of attack is called a "DNS Rebinding Attack". This vulnerability is fixed in 0.6.1.		
CVE-2025-31497	TEIGarage XML External Entity (XXE) Injection in Document Conversion Service	TEIGarage is a webservice and RESTful service to transform, convert and validate various formats, focussing on the TEI format. The Document Conversion Service contains a critical XML External Entity (XXE) Injection vulnerability in its document conversion functionality. The service processes XML files during the conversion process but fails to disable external entity processing, allowing an attacker to read arbitrary files from the server's filesystem. This vulnerability could allow attackers to read sensitive files from the server's filesystem, potentially exposing configuration files, credentials, or other confidential information. Additionally, depending on the server configuration, this could potentially be used to perform server-side request forgery (SSRF) attacks by making the server connect to internal services. This issue is patched in version 1.2.4. A workaround for this vulnerability includes disabling external entity processing in the XML parser by setting the appropriate security features (e.g., XMLConstants.FEATURE_SECURE_PROCESSING).	Patched by core rule	Y
CVE-2025-31527	WordPress WP Link Preview plugin <= 1.4.1 - Server Side Request Forgery (SSRF) vulnerability	Server-Side Request Forgery (SSRF) vulnerability in Kishan WP Link Preview allows Server Side Request Forgery. This issue affects WP Link Preview: from n/a through	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		1.4.1.		
CVE-2025-31796	WordPress ElementsCSS Addons for Elementor plugin <= 1.0.8.7 - Server Side Request Forgery (SSRF) vulnerability	Server-Side Request Forgery (SSRF) vulnerability in TheInnovs Team ElementsCSS Addons for Elementor allows Server Side Request Forgery. This issue affects ElementsCSS Addons for Elementor: from n/a through 1.0.8.7.	Patched by core rule	Y
CVE-2025-31824	WordPress WP Optin Wheel Plugin <= 1.4.7 - Server Side Request Forgery (SSRF) vulnerability	Server-Side Request Forgery (SSRF) vulnerability in Wombat Plugins WP Optin Wheel allows Server Side Request Forgery. This issue affects WP Optin Wheel: from n/a through 1.4.7.	Patched by core rule	Y
CVE-2025-32013	Server-Side Request Forgery via LNURL Authentication Callback in LNbits Lightning Network Payment System	LNbits is a Lightning wallet and accounts system. A Server-Side Request Forgery (SSRF) vulnerability has been discovered in LNbits' LNURL authentication handling functionality. When processing LNURL authentication requests, the application accepts a callback URL parameter and makes an HTTP request to that URL using the httpx library with redirect following enabled. The application doesn't properly validate the callback URL, allowing attackers to specify internal network addresses and access internal resources.	Patched by core rule	Y
CVE-2025-32487	WordPress Waymark <= 1.5.2 - Server Side Request Forgery (SSRF) Vulnerability	Server-Side Request Forgery (SSRF) vulnerability in Joe Waymark allows Server Side Request Forgery. This issue affects Waymark: from n/a through 1.5.2.	Patched by core rule	Y
CVE-2025-3254	xujiangfei admintwo add server-side request forgery	A vulnerability was found in xujiangfei admintwo 1.0. It has been classified as critical. Affected is an unknown function of the file /resource/add. The manipulation of the argument description leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-32675	WordPress SEO Help plugin <= 6.6.0 - Server Side Request Forgery (SSRF) vulnerability	Server-Side Request Forgery (SSRF) vulnerability in QuantumCloud SEO Help allows Server Side Request Forgery. This issue affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		SEO Help: from n/a through 6.6.0.		
CVE-2025-32691	WordPress PowerPress Podcasting <= 11.12.4 - Server Side Request Forgery (SSRF) Vulnerability	Server-Side Request Forgery (SSRF) vulnerability in Angelo Mandato PowerPress Podcasting allows Server Side Request Forgery. This issue affects PowerPress Podcasting: from n/a through 11.12.4.	Patched by core rule	Y
CVE-2025-3411	mymagicpower AIAS AsrController.java server-side request forgery	A vulnerability, which was classified as critical, has been found in mymagicpower AIAS 20250308. This issue affects some unknown processing of the file 3_api_platform/api-platform/src/main/java/top/aias/platform/controller/AsrController.java. The manipulation of the argument url leads to server-side request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-3412	mymagicpower AIAS InferController.java server-side request forgery	A vulnerability, which was classified as critical, was found in mymagicpower AIAS 20250308. Affected is an unknown function of the file 2_training_platform/train-platform/src/main/java/top/aias/training/controller/InferController.java. The manipulation of the argument url leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-3691	mirweiye Seven Bears Library CMS Add Link server-side request forgery	A vulnerability was found in mirweiye Seven Bears Library CMS 2023. It has been classified as problematic. Affected is an unknown function of the component Add Link Handler. The manipulation leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-3787	PbootCMS Image server-side request forgery	A vulnerability was found in PbootCMS 3.2.5. It has been classified as problematic. Affected is an unknown function of the component Image Handler. The manipulation leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-46443	WordPress Animate <= 0.5 - Server Side Request Forgery (SSRF) Vulnerability	Server-Side Request Forgery (SSRF) vulnerability in Adam Pery Animate allows Server Side Request Forgery. This issue affects Animate: from n/a through 0.5.	Patched by core rule	Y
CVE-2025-46473	WordPress Social Counter <= 2.0.5 - PHP Object Injection Vulnerability	Deserialization of Untrusted Data vulnerability in djjmz Social Counter allows Object Injection. This issue affects Social Counter: from n/a through 2.0.5.	Patched by core rule	Y
CVE-2025-46503	WordPress Simple Google Photos Grid <= 1.5 - Server Side Request Forgery (SSRF) Vulnerability	Server-Side Request Forgery (SSRF) vulnerability in josheli Simple Google Photos Grid allows Server Side Request Forgery. This issue affects Simple Google Photos Grid: from n/a through 1.5.	Patched by core rule	Y
CVE-2025-46511	WordPress BeerXML Shortcode <= 0.71 - Server Side Request Forgery (SSRF) Vulnerability	Server-Side Request Forgery (SSRF) vulnerability in Derek Springer BeerXML Shortcode allows Server Side Request Forgery. This issue affects BeerXML Shortcode: from n/a through 0.71.	Patched by core rule	Y
CVE-2025-46531	WordPress WP AVCL Automation Helper (formerly WPFlyLeads) <= 3.4 - Server Side Request Forgery (SSRF) Vulnerability	Server-Side Request Forgery (SSRF) vulnerability in Ankur Vishwakarma WP AVCL Automation Helper (formerly WPFlyLeads) allows Server Side Request Forgery. This issue affects WP AVCL Automation Helper (formerly WPFlyLeads): from n/a through 3.4.	Patched by core rule	Y

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2017-20197	propanetank Roommate-Bill-Tracking login.php sql injection	A vulnerability was found in propanetank Roommate-Bill-Tracking up to 288437f658fc9ee7d4b92a9da12557024d8bc55c. It has been declared as critical. This vulnerability affects unknown code of the file /includes/login.php. The manipulation of the argument Username leads to sql injection. The attack can be initiated remotely. The name of the patch is b32bb1b940f82d38fb9310cd66ebe349e20a1d0a. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y
CVE-2025-1520	PostHog ClickHouse Table Functions SQL Injection Remote Code Execution Vulnerability	PostHog ClickHouse Table Functions SQL Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of PostHog. Authentication is required to exploit this vulnerability. The specific flaw exists within the implementation of the SQL parser. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to execute code in the context of the database account. Was ZDI-CAN-25350.	Patched by core rule	Y
CVE-2025-22523	WordPress Schedule Plugin <= 1.0.0 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in NotFound Schedule allows Blind SQL Injection. This issue affects Schedule: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-22652	WordPress Payment Forms for Paystack plugin <= 4.0.1 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in kendysond Payment Forms for Paystack allows SQL Injection.This issue affects Payment Forms for Paystack: from n/a through 4.0.1.	Patched by core rule	Y
CVE-2025-22655	WordPress CWD - Stealth Links plugin <= 1.3 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Injection') vulnerability in Caio Web Dev CWD – Stealth Links allows SQL Injection. This issue affects CWD – Stealth Links: from n/a through 1.3.		
CVE-2025-22783	WordPress SEO Plugin by Squirrly SEO plugin <= 12.4.03 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in SEO Squirrly SEO Plugin by Squirrly SEO allows SQL Injection.This issue affects SEO Plugin by Squirrly SEO: from n/a through 12.4.03.	Patched by core rule	Y
CVE-2025-25228	Extension - virtuemart.net - SQL injection in VirtueMart component 1.0.0 - 4.4.7 for Joomla	A SQL injection in VirtueMart component 1.0.0 - 4.4.7 for Joomla allows authenticated attackers (administrator) to execute arbitrary SQL commands in the product management area in backend.	Patched by core rule	Y
CVE-2025-26898	WordPress Traveler theme <= 3.1.8 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Shinetheme Traveler.This issue affects Traveler: from n/a through 3.1.8.	Patched by core rule	Y
CVE-2025-26908	WordPress Kargo Entegratör plugin <= 1.1.14 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Gurmehub Kargo Entegratör allows SQL Injection. This issue affects Kargo Entegratör: from n/a through 1.1.14.	Patched by core rule	Y
CVE-2025-26941	WordPress Church Admin plugin <= 5.0.18 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Andy Moyle Church Admin allows SQL Injection.This issue affects Church Admin: from n/a through 5.0.18.	Patched by core rule	Y
CVE-2025-27302	WordPress CHATLIVE plugin <= 2.0.1 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Claudio Adrian Marrero CHATLIVE allows SQL Injection. This issue affects CHATLIVE: from n/a through 2.0.1.	Patched by core rule	Y
CVE-2025-2831	mingyuefusu 明月复苏 tushuguanlixitong 图书管理系统 bookList getBookList sql injection	A vulnerability has been found in mingyuefusu 明月复苏 tushuguanlixitong 图书管理系统 up to d4836f6b49cd0ac79a4021b15ce99ff7229d4694 and classified as critical. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability affects the function getBookList of the file /admin/bookList?page=1&limit=10. The manipulation of the argument condition leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-2846	SourceCodester Online Eyewear Shop Registration Users.php registration sql injection	A vulnerability classified as critical was found in SourceCodester Online Eyewear Shop 1.0. This vulnerability affects the function registration of the file /oews/classes/Users.php?f=registration of the component Registration. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-2854	code-projects Payroll Management System update_employee.php sql injection	A vulnerability classified as critical was found in code-projects Payroll Management System 1.0. Affected by this vulnerability is an unknown functionality of the file update_employee.php. The manipulation of the argument emp_type leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-28873	WordPress Shuffle plugin <= 0.5 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in NotFound Shuffle allows Blind SQL Injection. This issue affects Shuffle: from n/a through 0.5.	Patched by core rule	Y
CVE-2025-28898	WordPress WP Multistore Locator plugin <= 2.5.2 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in NotFound WP Multistore Locator allows SQL Injection. This issue affects WP Multistore Locator: from n/a through 2.5.2.	Patched by core rule	Y
CVE-2025-28939	WordPress WP Google Calendar Manager plugin <= 2.1 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in NotFound WP Google	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Calendar Manager allows Blind SQL Injection. This issue affects WP Google Calendar Manager: from n/a through 2.1.		
CVE-2025-28942	WordPress Trust Payments Gateway for WooCommerce plugin <= 1.1.4 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Trust Payments Trust Payments Gateway for WooCommerce allows SQL Injection. This issue affects Trust Payments Gateway for WooCommerce: from n/a through 1.1.4.	Patched by core rule	Y
CVE-2025-2927	ESAFENET CDG getFileTypeList.jsp sql injection	A vulnerability was found in ESAFENET CDG 5.6.3.154.205. It has been classified as critical. Affected is an unknown function of the file /parameter/getFileTypeList.jsp. The manipulation of the argument typename leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2984	code-projects Payroll Management System delete.php sql injection	A vulnerability was found in code-projects Payroll Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /delete.php. The manipulation of the argument emp_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-2985	code-projects Payroll Management System update_account.php sql injection	A vulnerability was found in code-projects Payroll Management System 1.0. It has been classified as critical. This affects an unknown part of the file update_account.php. The manipulation of the argument deduction leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-3003	ESAFENET CDG UserAjax sql injection	A vulnerability, which was classified as critical, was found in ESAFENET CDG 3.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Affected is an unknown function of the file /CDGServer3/UserAjax. The manipulation of the argument Username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-3006	PHPGurukul e-Diary Management System edit-category.php sql injection	A vulnerability was found in PHPGurukul e-Diary Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /edit-category.php?id=8. The manipulation of the argument Category leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3009	Jinher Network OA NetDiskProperty.aspx sql injection	A vulnerability classified as critical was found in Jinher Network OA C6. Affected by this vulnerability is an unknown functionality of the file /C6/JHSoft.Web.NetDisk/NetDiskProperty.aspx. The manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3018	SourceCodester Online Eyewear Shop Users.php sql injection	A vulnerability, which was classified as critical, was found in SourceCodester Online Eyewear Shop 1.0. Affected is an unknown function of the file /classes/Users.php?f=delete. The manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-30217	Frappe has possibility of SQL injection due to improper validations	Frappe is a full-stack web application framework. Prior to versions 14.93.2 and 15.55.0, a SQL Injection vulnerability has been identified in Frappe Framework which could allow a malicious actor to access sensitive information. Versions 14.93.2 and 15.55.0 contain a patch for the issue.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		No known workarounds are available.		
CVE-2025-30364	WeGIA vulnerable to SQL Injection (Blind Time-Based) in remuneracao.php parameter id_funcionario	WeGIA is a Web manager for charitable institutions. A SQL Injection vulnerability was identified in versions prior to 3.2.8 in the endpoint /WeGIA/html/funcionario/remuneracao.php, in the id_funcionario parameter. This vulnerability allows the execution of arbitrary SQL commands, which can compromise the confidentiality, integrity, and availability of stored data. Version 3.2.8 fixes the issue.	Patched by core rule	Y
CVE-2025-30365	SQL Injection in query_geracao_auto.php	WeGIA is a Web manager for charitable institutions. A SQL Injection vulnerability was identified in versions prior to 3.2.8 in the endpoint /WeGIA/html/socio/sistema/controller/query_geracao_auto.php, specifically in the query parameter. This vulnerability allows the execution of arbitrary SQL commands, compromising the confidentiality, integrity, and availability of the database. Version 3.2.8 fixes the issue.	Patched by core rule	Y
CVE-2025-30367	WeGIA SQL Injection Vulnerability in nextPage Parameter on control.php Endpoint	WeGIA is a Web manager for charitable institutions. A SQL Injection vulnerability was identified in versions prior to 3.2.6 in the nextPage parameter of the /WeGIA/controle/control.php endpoint. This vulnerability allows attacker to manipulate SQL queries and access sensitive database information, such as table names and sensitive data. Version 3.2.6 contains a fix for the issue.	Patched by core rule	Y
CVE-2025-30372	Emlog Pro contains an SQL injection vulnerability.	Emlog is an open source website building system. Emlog Pro versions pro-2.5.7 and pro-2.5.8 contain an SQL injection vulnerability. `search_controller.php` does not use addslashes after urldecode, allowing the preceeding addslashes to be bypassed by URL double encoding. This could result in potential leakage of sensitive information from the user database. Version pro-2.5.9 fixes the issue.	Patched by core rule	Y
CVE-2025-3038	code-projects Payroll Management System	A vulnerability was found in code-projects Payroll	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	view_account.php sql injection	Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /view_account.php. The manipulation of the argument salary_rate leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3039	code-projects Payroll Management System add_employee.php sql injection	A vulnerability was found in code-projects Payroll Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /add_employee.php. The manipulation of the argument lname/fname leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-3045	oretnom23/SourceCodester Apartment Visitor Management System remove-apartment.php sql injection	A vulnerability, which was classified as critical, was found in oretnom23/SourceCodester Apartment Visitor Management System 1.0. Affected is an unknown function of the file /remove-apartment.php. The manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-30473	Apache Airflow Common SQL Provider: Remote Code Execution via Sql Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Airflow Common SQL Provider. When using the partition clause in SQLTableCheckOperator as parameter (which was a recommended pattern), Authenticated UI User could inject arbitrary SQL command when triggering DAG exposing partition_clause to the user. This allowed the DAG Triggering user to escalate privileges to execute those arbitrary commands which they normally would not	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		have. This issue affects Apache Airflow Common SQL Provider: before 1.24.1. Users are recommended to upgrade to version 1.24.1, which fixes the issue.		
CVE-2025-30524	WordPress Product Catalog plugin <= 1.0.4 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in origincode Product Catalog allows SQL Injection. This issue affects Product Catalog: from n/a through 1.0.4.	Patched by core rule	Y
CVE-2025-30589	WordPress Flickr set slideshows plugin <= 0.9 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in NotFound Flickr set slideshows allows SQL Injection. This issue affects Flickr set slideshows: from n/a through 0.9.	Patched by core rule	Y
CVE-2025-30622	WordPress PostMash <= 1.0.3 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in torsteino PostMash allows SQL Injection. This issue affects PostMash: from n/a through 1.0.3.	Patched by core rule	Y
CVE-2025-30765	WordPress FlexStock <= 3.13.1 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPPOOL FlexStock allows Blind SQL Injection. This issue affects FlexStock: from n/a through 3.13.1.	Patched by core rule	Y
CVE-2025-30774	WordPress Quiz Maker plugin <= 6.6.8.7 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ays Pro Quiz Maker allows SQL Injection. This issue affects Quiz Maker: from n/a through 6.6.8.7.	Patched by core rule	Y
CVE-2025-30775	WordPress WPGuppy plugin <= 1.1.3 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AmentoTech Private Limited WPGuppy allows SQL Injection. This issue affects WPGuppy: from n/a through 1.1.3.	Patched by core rule	Y
CVE-2025-30784	WordPress WP Subscription Forms <= 1.2.3 - SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Vulnerability	Injection') vulnerability in WP Shuffle WP Subscription Forms allows SQL Injection. This issue affects WP Subscription Forms: from n/a through 1.2.3.		
CVE-2025-30791	WordPress Cart tracking for WooCommerce plugin <= 1.0.16 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in wpdever Cart tracking for WooCommerce allows SQL Injection. This issue affects Cart tracking for WooCommerce: from n/a through 1.0.16.	Patched by core rule	Y
CVE-2025-30806	WordPress Vimeotheque plugin <= 2.3.4.2 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Constantin Boiangiu Vimeotheque allows SQL Injection. This issue affects Vimeotheque: from n/a through 2.3.4.2.	Patched by core rule	Y
CVE-2025-30807	WordPress Next-Cart Store to WooCommerce Migration plugin <= 3.9.4 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Martin Nguyen Next-Cart Store to WooCommerce Migration allows SQL Injection. This issue affects Next-Cart Store to WooCommerce Migration: from n/a through 3.9.4.	Patched by core rule	Y
CVE-2025-30810	WordPress Lead Form Data Collection to CRM plugin <= 3.0.1 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in smackcoders Lead Form Data Collection to CRM allows Blind SQL Injection. This issue affects Lead Form Data Collection to CRM: from n/a through 3.0.1.	Patched by core rule	Y
CVE-2025-30819	WordPress Simple Giveaways plugin <= 2.48.1 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Igor Benic Simple Giveaways allows SQL Injection. This issue affects Simple Giveaways: from n/a through 2.48.1.	Patched by core rule	Y
CVE-2025-30843	WordPress bizcalendar-web plugin <= 1.1.0.34 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in setriosoft bizcalendar-web allows SQL Injection. This issue affects bizcalendar-web: from n/a through 1.1.0.34.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-30876	WordPress Ads by WPQuads plugin <= 2.0.87.1 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ads by WPQuads Ads by WPQuads allows SQL Injection. This issue affects Ads by WPQuads: from n/a through 2.0.87.1.	Patched by core rule	Y
CVE-2025-30879	WordPress MC Woocommerce Wishlist plugin <= 1.8.9 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in moreconvert MC Woocommerce Wishlist allows SQL Injection. This issue affects MC Woocommerce Wishlist: from n/a through 1.8.9.	Patched by core rule	Y
CVE-2025-30886	WordPress JS Help Desk plugin <= 2.9.2 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in JoomSky JS Help Desk allows SQL Injection. This issue affects JS Help Desk: from n/a through 2.9.2.	Patched by core rule	Y
CVE-2025-30921	WordPress Newsletters plugin <= 4.9.9.7 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Tribulant Software Newsletters allows SQL Injection. This issue affects Newsletters: from n/a through 4.9.9.7.	Patched by core rule	Y
CVE-2025-30971	WordPress XV Random Quotes plugin <= 1.40 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Xavi Ivars XV Random Quotes allows SQL Injection. This issue affects XV Random Quotes: from n/a through 1.40.	Patched by core rule	Y
CVE-2025-31024	WordPress RJ Quickcharts plugin <= 0.6.1 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in randyjensen RJ Quickcharts allows SQL Injection. This issue affects RJ Quickcharts: from n/a through 0.6.1.	Patched by core rule	Y
CVE-2025-31089	WordPress Order Splitter for WooCommerce <= 5.3.0 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Fahad Mahmood Order Splitter for WooCommerce allows SQL Injection. This issue affects Order Splitter for WooCommerce: from n/a through 5.3.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-31099	WordPress Slider by BestWebSoft <= 1.1.0 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in bestwebsoft Slider by BestWebSoft allows SQL Injection. This issue affects Slider by BestWebSoft: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-3118	SourceCodester Online Tutor Portal view_course.php sql injection	A vulnerability was found in SourceCodester Online Tutor Portal 1.0. It has been classified as critical. This affects an unknown part of the file /tutor/courses/view_course.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3119	SourceCodester Online Tutor Portal manage_course.php sql injection	A vulnerability was found in SourceCodester Online Tutor Portal 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /tutor/courses/manage_course.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3120	SourceCodester Apartment Visitors Management System add-apartment.php sql injection	A vulnerability was found in SourceCodester Apartment Visitors Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /add-apartment.php. The manipulation of the argument apartmentno leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-3134	code-projects Payroll Management System add_overtime.php sql injection	A vulnerability classified as critical has been found in code-projects Payroll Management System 1.0. This affects an unknown part of the file /add_overtime.php. The manipulation of the argument rate leads to sql injection. It is possible to initiate the attack remotely. The exploit has been	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		disclosed to the public and may be used.		
CVE-2025-3137	PHPGurukul Online Security Guards Hiring System changeimage.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Online Security Guards Hiring System 1.0. Affected is an unknown function of the file /admin/changeimage.php. The manipulation of the argument editid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3138	PHPGurukul Online Security Guards Hiring System edit-guard-detail.php sql injection	A vulnerability has been found in PHPGurukul Online Security Guards Hiring System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/edit-guard-detail.php. The manipulation of the argument editid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3140	SourceCodester Online Medicine Ordering System view_category.php sql injection	A vulnerability was found in SourceCodester Online Medicine Ordering System 1.0. It has been classified as critical. This affects an unknown part of the file /view_category.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-31403	WordPress Booking Calendar and Notification plugin <= 4.0.3 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in shiptrack Booking Calendar and Notification allows Blind SQL Injection.This issue affects Booking Calendar and Notification: from n/a through 4.0.3.	Patched by core rule	Y
CVE-2025-3141	SourceCodester Online Medicine Ordering System manage_category.php sql injection	A vulnerability was found in SourceCodester Online Medicine Ordering System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /manage_category.php. The manipulation of the argument ID leads to sql injection. The attack can be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3142	SourceCodester Apartment Visitor Management System add-apartment.php sql injection	A vulnerability was found in SourceCodester Apartment Visitor Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /add-apartment.php. The manipulation of the argument buildingno leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Multiple parameters might be affected.	Patched by core rule	Y
CVE-2025-3143	SourceCodester Apartment Visitor Management System visitor-entry.php sql injection	A vulnerability classified as critical has been found in SourceCodester Apartment Visitor Management System 1.0. Affected is an unknown function of the file /visitor-entry.php. The manipulation of the argument visname/address leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Multiple parameters might be affected.	Patched by core rule	Y
CVE-2025-3146	PHPGurukul Bus Pass Management System view-pass-detail.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Bus Pass Management System 1.0. This affects an unknown part of the file /view-pass-detail.php. The manipulation of the argument viewid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-31466	WordPress Duplicate Page and Post <= 1.0 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Falcon Solutions Duplicate Page and Post allows Blind SQL Injection. This issue affects Duplicate Page and Post: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-3147	PHPGurukul Boat Booking System add-subadmin.php sql injection	A vulnerability has been found in PHPGurukul Boat Booking System 1.0 and classified as critical. This vulnerability affects unknown code of the file /add-subadmin.php. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument sadminusername leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3151	SourceCodester Gym Management System signup.php sql injection	A vulnerability was found in SourceCodester Gym Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /signup.php. The manipulation of the argument user_name leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-31526	WordPress Behance Portfolio Manager plugin <= 1.7.4 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in eleopard Behance Portfolio Manager allows SQL Injection. This issue affects Behance Portfolio Manager: from n/a through 1.7.4.	Patched by core rule	Y
CVE-2025-31531	WordPress History Log by click5 plugin <= 1.0.13 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in click5 History Log by click5 allows SQL Injection. This issue affects History Log by click5: from n/a through 1.0.13.	Patched by core rule	Y
CVE-2025-31534	WordPress Shopper plugin <= 3.2.5 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in shopperdotcom Shopper allows SQL Injection. This issue affects Shopper: from n/a through 3.2.5.	Patched by core rule	Y
CVE-2025-31542	WordPress My auctions allegro plugin <= 3.6.20 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in wphocus My auctions allegro allows Blind SQL Injection. This issue affects My auctions allegro: from n/a through 3.6.20.	Patched by core rule	Y
CVE-2025-31547	WordPress Uptime Robot Plugin for WordPress plugin <= 2.3 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Aphotrax Uptime Robot Plugin for WordPress allows SQL Injection. This issue affects Uptime Robot Plugin	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		for WordPress: from n/a through 2.3.		
CVE-2025-31551	WordPress Salesmate Add-On for Gravity Forms plugin <= 2.0.3 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Salesmate.io Salesmate Add-On for Gravity Forms allows SQL Injection. This issue affects Salesmate Add-On for Gravity Forms: from n/a through 2.0.3.	Patched by core rule	Y
CVE-2025-31552	WordPress RSVPMarker plugin <= 11.4.8 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in davidfcarr RSVPMarker allows SQL Injection. This issue affects RSVPMarker : from n/a through 11.4.8.	Patched by core rule	Y
CVE-2025-31553	WordPress Advanced WooCommerce Product Sales Reporting plugin <= 3.1 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPFactory Advanced WooCommerce Product Sales Reporting allows SQL Injection. This issue affects Advanced WooCommerce Product Sales Reporting: from n/a through 3.1.	Patched by core rule	Y
CVE-2025-31561	WordPress Ultimate Push Notifications plugin <= 1.1.8 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in M. Tuhin Ultimate Push Notifications allows SQL Injection. This issue affects Ultimate Push Notifications: from n/a through 1.1.8.	Patched by core rule	Y
CVE-2025-31564	ChatGPT Ai Auto Tool Content Writing Assistant (Gemini Writer, ChatGPT) All in One plugin <= 2.1.7 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in aitool Ai Auto Tool Content Writing Assistant (Gemini Writer, ChatGPT) All in One allows Blind SQL Injection. This issue affects Ai Auto Tool Content Writing Assistant (Gemini Writer, ChatGPT) All in One: from n/a through 2.1.7.	Patched by core rule	Y
CVE-2025-31565	WordPress WPSmartContracts plugin <= 2.0.10 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPSmartContracts WPSmartContracts allows Blind SQL Injection. This issue affects WPSmartContracts: from n/a through 2.0.10.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-31579	WordPress WP AutoKeyword plugin <= 1.0 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in EXEIdeas International WP AutoKeyword allows SQL Injection. This issue affects WP AutoKeyword: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-31599	WordPress Bulk Product Sync plugin <= 8.6 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in N-Media Bulk Product Sync allows SQL Injection. This issue affects Bulk Product Sync: from n/a through 8.6.	Patched by core rule	Y
CVE-2025-31619	WordPress Actionwear products sync plugin <= 2.3.3 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in marcoingraiti Actionwear products sync allows SQL Injection. This issue affects Actionwear products sync: from n/a through 2.3.3.	Patched by core rule	Y
CVE-2025-3168	PHPGurukul Time Table Generator System edit-class.php sql injection	A vulnerability was found in PHPGurukul Time Table Generator System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/edit-class.php. The manipulation of the argument editid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3170	Project Worlds Online Lawyer Management System admin_user.php sql injection	A vulnerability classified as critical has been found in Project Worlds Online Lawyer Management System 1.0. This affects an unknown part of the file /admin_user.php. The manipulation of the argument block_id/unblock_id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3171	Project Worlds Online Lawyer Management System approve_lawyer.php sql injection	A vulnerability classified as critical was found in Project Worlds Online Lawyer Management System 1.0. This vulnerability affects unknown code of the file /approve_lawyer.php. The manipulation of the argument unblock_id leads	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3172	Project Worlds Online Lawyer Management System lawyer_booking.php sql injection	A vulnerability, which was classified as critical, has been found in Project Worlds Online Lawyer Management System 1.0. This issue affects some unknown processing of the file /lawyer_booking.php. The manipulation of the argument unblock_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3173	Project Worlds Online Lawyer Management System save_booking.php sql injection	A vulnerability, which was classified as critical, was found in Project Worlds Online Lawyer Management System 1.0. Affected is an unknown function of the file /save_booking.php. The manipulation of the argument lawyer_id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3174	Project Worlds Online Lawyer Management System searchLawyer.php sql injection	A vulnerability has been found in Project Worlds Online Lawyer Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /searchLawyer.php. The manipulation of the argument experience leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3175	Project Worlds Online Lawyer Management System save_user_edit_profile.php sql injection	A vulnerability was found in Project Worlds Online Lawyer Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /save_user_edit_profile.php. The manipulation of the argument first_Name leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3176	Project Worlds Online	A vulnerability was found in	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Lawyer Management System single_lawyer.php sql injection	Project Worlds Online Lawyer Management System 1.0. It has been classified as critical. This affects an unknown part of the file /single_lawyer.php. The manipulation of the argument u_id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	rule	
CVE-2025-3178	projectworlds Online Doctor Appointment Booking System deleteappointment.php sql injection	A vulnerability was found in projectworlds Online Doctor Appointment Booking System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /doctor/deleteappointment.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3179	projectworlds Online Doctor Appointment Booking System deletepatient.php sql injection	A vulnerability classified as critical has been found in projectworlds Online Doctor Appointment Booking System 1.0. Affected is an unknown function of the file /doctor/deletepatient.php. The manipulation of the argument ic leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3180	projectworlds Online Doctor Appointment Booking System deleteschedule.php sql injection	A vulnerability classified as critical was found in projectworlds Online Doctor Appointment Booking System 1.0. Affected by this vulnerability is an unknown functionality of the file /doctor/deleteschedule.php. The manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3181	projectworlds Online Doctor Appointment Booking System appointment.php sql injection	A vulnerability, which was classified as critical, has been found in projectworlds Online Doctor Appointment Booking System 1.0. Affected by this issue is some unknown functionality of the file /patient/appointment.php?scheduleDate=1&appid=1.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The manipulation of the argument scheduleDate leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3182	projectworlds Online Doctor Appointment Booking System getschedule.php sql injection	A vulnerability, which was classified as critical, was found in projectworlds Online Doctor Appointment Booking System 1.0. This affects an unknown part of the file /patient/getschedule.php. The manipulation of the argument q leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3183	projectworlds Online Doctor Appointment Booking System patientupdateprofile.php sql injection	A vulnerability has been found in projectworlds Online Doctor Appointment Booking System 1.0 and classified as critical. This vulnerability affects unknown code of the file /patient/patientupdateprofile.php. The manipulation of the argument patientFirstName leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-3184	projectworlds Online Doctor Appointment Booking System profile.php sql injection	A vulnerability was found in projectworlds Online Doctor Appointment Booking System 1.0 and classified as critical. This issue affects some unknown processing of the file /patient/profile.php?patientId=1. The manipulation of the argument patientFirstName leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-3185	projectworlds Online Doctor Appointment Booking System patientupdateprofile.php sql injection	A vulnerability was found in projectworlds Online Doctor Appointment Booking System 1.0. It has been classified as critical. Affected is an unknown function of the file /patient/patientupdateprofile.php. The manipulation of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the argument patientFirstName leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.		
CVE-2025-3186	projectworlds Online Doctor Appointment Booking System invoice.php sql injection	A vulnerability was found in projectworlds Online Doctor Appointment Booking System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /patient/invoice.php. The manipulation of the argument appid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3187	PHPGurukul e-Diary Management System login.php sql injection	A vulnerability was found in PHPGurukul e-Diary Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /login.php. The manipulation of the argument logindetail leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3188	PHPGurukul e-Diary Management System add-notes.php sql injection	A vulnerability classified as critical has been found in PHPGurukul e-Diary Management System 1.0. This affects an unknown part of the file /add-notes.php. The manipulation of the argument Category leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-31910	WordPress BookingPress Plugin <= 1.1.28 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in reputeinfosystems BookingPress allows SQL Injection. This issue affects BookingPress: from n/a through 1.1.28.	Patched by core rule	Y
CVE-2025-31911	WordPress Social Share And Social Locker plugin <= 1.4.2 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in NotFound Social Share And Social Locker allows Blind	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		SQL Injection. This issue affects Social Share And Social Locker: from n/a through 1.4.2.		
CVE-2025-3195	itsourcecode Online Blood Bank Management System bbms.php sql injection	A vulnerability, which was classified as critical, has been found in itsourcecode Online Blood Bank Management System 1.0. This issue affects some unknown processing of the file /bbms.php. The manipulation of the argument Search leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-32020	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') in crud-query-parser	The crud-query-parser library parses query parameters from HTTP requests and converts them to database queries. Improper neutralization of the order/sort parameter in the TypeORM adapter, which allows SQL injection. You are impacted by this vulnerability if you are using the TypeORM adapter, ordering is enabled and you have not set-up a property filter. This vulnerability is fixed in 0.1.0.	Patched by core rule	Y
CVE-2025-3204	CodeAstro Car Rental System returncar.php sql injection	A vulnerability, which was classified as critical, has been found in CodeAstro Car Rental System 1.0. Affected by this issue is some unknown functionality of the file /returncar.php. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3205	CodeAstro Student Grading System studentsubject.php sql injection	A vulnerability, which was classified as critical, was found in CodeAstro Student Grading System 1.0. This affects an unknown part of the file studentsubject.php. The manipulation of the argument studentId leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3206	code-projects Hospital Management System doctor-specilization.php sql injection	A vulnerability has been found in code-projects Hospital Management System 1.0 and classified as critical. This vulnerability	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects unknown code of the file /admin/doctor-specilization.php. The manipulation of the argument doctorspecilization leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3207	code-projects Patient Record Management System birthing_form.php sql injection	A vulnerability was found in code-projects Patient Record Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /birthing_form.php. The manipulation of the argument birth_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3208	code-projects Patient Record Management System xray_print.php sql injection	A vulnerability was found in code-projects Patient Record Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /xray_print.php. The manipulation of the argument itr_no leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3209	code-projects Patient Record Management System add_patient.php sql injection	A vulnerability was found in code-projects Patient Record Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /add_patient.php. The manipulation of the argument itr_no leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3210	code-projects Patient Record Management System birthing_pending.php sql injection	A vulnerability was found in code-projects Patient Record Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /birthing_pending.php. The manipulation of the argument birth_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3211	code-projects Patient	A vulnerability classified as	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Record Management System birthing_print.php sql injection	critical has been found in code-projects Patient Record Management System 1.0. This affects an unknown part of the file /birthing_print.php. The manipulation of the argument itr_no leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	rule	
CVE-2025-32119	WordPress CardGate Payments for WooCommerce plugin <= 3.2.1 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CardGate CardGate Payments for WooCommerce allows Blind SQL Injection. This issue affects CardGate Payments for WooCommerce: from n/a through 3.2.1.	Patched by core rule	Y
CVE-2025-32120	WordPress Easy Query – WP Query Builder <= 2.0.4 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Erick Danzer Easy Query – WP Query Builder allows Blind SQL Injection. This issue affects Easy Query – WP Query Builder: from n/a through 2.0.4.	Patched by core rule	Y
CVE-2025-32121	WordPress Video & Photo Gallery for Ultimate Member plugin <= 1.1.3 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in SuitePlugins Video & Photo Gallery for Ultimate Member allows SQL Injection. This issue affects Video & Photo Gallery for Ultimate Member: from n/a through 1.1.3.	Patched by core rule	Y
CVE-2025-32122	WordPress uListing plugin <= 2.1.9 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Stylemix uListing allows Blind SQL Injection. This issue affects uListing: from n/a through 2.1.9.	Patched by core rule	Y
CVE-2025-32124	WordPress Behance Portfolio Manager plugin <=1.7.4 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in eleopard Behance Portfolio Manager allows Blind SQL Injection. This issue affects Behance Portfolio Manager: from n/a through 1.7.4.	Patched by core rule	Y
CVE-2025-32125	WordPress Silvasoft boekhouden Plugin <=	Improper Neutralization of Special Elements used in an	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	3.0.1 - SQL Injection vulnerability	SQL Command ('SQL Injection') vulnerability in silvasoft Silvasoft boekhouden allows SQL Injection. This issue affects Silvasoft boekhouden: from n/a through 3.0.1.		
CVE-2025-32126	WordPress Pay with Contact Form 7 Plugin <= 1.0.4 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in cmsMinds Pay with Contact Form 7 allows SQL Injection. This issue affects Pay with Contact Form 7: from n/a through 1.0.4.	Patched by core rule	Y
CVE-2025-32127	WordPress onOffice for WP-Websites plugin <= 5.7 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in onOffice GmbH onOffice for WP-Websites allows SQL Injection. This issue affects onOffice for WP-Websites: from n/a through 5.7.	Patched by core rule	Y
CVE-2025-32128	WordPress Nearby Locations Plugin <= 1.1.1 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in aaronfrey Nearby Locations allows SQL Injection. This issue affects Nearby Locations: from n/a through 1.1.1.	Patched by core rule	Y
CVE-2025-3213	PHPGurukul e-Diary Management System view-note.php sql injection	A vulnerability classified as critical was found in PHPGurukul e-Diary Management System 1.0. This vulnerability affects unknown code of the file /view-note.php?noteid=11. The manipulation of the argument remark leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-32148	WordPress Daisycon prijsvergelijkers plugin <= 4.8.4 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Daisycon Daisycon prijsvergelijkers allows SQL Injection. This issue affects Daisycon prijsvergelijkers: from n/a through 4.8.4.	Patched by core rule	Y
CVE-2025-32149	WordPress teachPress plugin <= 9.0.11 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in winkm89 teachPress allows SQL Injection. This issue affects teachPress: from n/a through 9.0.11.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-3215	PHPGurukul Restaurant Table Booking System add-subadmin.php sql injection	A vulnerability was found in PHPGurukul Restaurant Table Booking System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/add-subadmin.php. The manipulation of the argument fullname leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-3216	PHPGurukul e-Diary Management System password-recovery.php sql injection	A vulnerability was found in PHPGurukul e-Diary Management System 1.0. It has been classified as critical. This affects an unknown part of the file /password-recovery.php. The manipulation of the argument username/contactno leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3217	PHPGurukul e-Diary Management System registration.php sql injection	A vulnerability was found in PHPGurukul e-Diary Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /registration.php. The manipulation of the argument emailid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3220	PHPGurukul e-Diary Management System dashboard.php sql injection	A vulnerability was found in PHPGurukul e-Diary Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /dashboard.php. The manipulation of the argument Category leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-32203	WordPress Falling things Plugin <= 1.08 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in manu225 Falling things allows SQL Injection. This issue affects Falling things: from n/a through 1.08.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-32204	WordPress Split Test For Elementor Plugin <= 1.8.2 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in rocketelements Split Test For Elementor allows SQL Injection. This issue affects Split Test For Elementor: from n/a through 1.8.2.	Patched by core rule	Y
CVE-2025-3229	PHPGurukul Restaurant Table Booking System edit-subadmin.php sql injection	A vulnerability was found in PHPGurukul Restaurant Table Booking System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /edit-subadmin.php. The manipulation of the argument fullname leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-3231	PHPGurukul Zoo Management System aboutus.php sql injection	A vulnerability was found in PHPGurukul Zoo Management System 2.1. It has been rated as critical. This issue affects some unknown processing of the file /aboutus.php. The manipulation of the argument pagetitle leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3235	PHPGurukul Old Age Home Management System profile.php sql injection	A vulnerability was found in PHPGurukul Old Age Home Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/profile.php. The manipulation of the argument adminname leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3238	PHPGurukul Online Fire Reporting System search-request.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Online Fire Reporting System 1.2. Affected is an unknown function of the file /search-request.php. The manipulation of the argument searchdata leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-32389	NamelessMC Vulnerable to SQL Injections in /user/messaging and /panel/users/reports Pages	NamelessMC is a free, easy to use & powerful website software for Minecraft servers. Prior to version 2.1.4, NamelessMC is vulnerable to SQL injection by providing an unexpected square bracket GET parameter syntax. Square bracket GET parameter syntax refers to the structure `?param[0]=a&param[1]=b&param[2]=c` utilized by PHP, which is parsed by PHP as `$_GET['param']` being of type array. This issue has been patched in version 2.1.4.	Patched by core rule	Y
CVE-2025-3239	PHPGurukul Online Fire Reporting System edit-guard-detail.php sql injection	A vulnerability classified as critical was found in PHPGurukul Online Fire Reporting System 1.2. Affected by this vulnerability is an unknown functionality of the file /admin/edit-guard-detail.php. The manipulation of the argument editid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3240	PHPGurukul Online Fire Reporting System search.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Online Fire Reporting System 1.2. Affected by this issue is some unknown functionality of the file /admin/search.php. The manipulation of the argument searchdata leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3242	PHPGurukul e-Diary Management System search-result.php sql injection	A vulnerability has been found in PHPGurukul e-Diary Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /search-result.php. The manipulation of the argument searchdata leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3243	code-projects Patient Record Management System dental_form.php	A vulnerability was found in code-projects Patient Record Management System 1.0	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	sql injection	and classified as critical. This issue affects some unknown processing of the file /dental_form.php. The manipulation of the argument itr_no leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3245	itsourcecode Library Management System Forgot.java search sql injection	A vulnerability was found in itsourcecode Library Management System 1.0. It has been rated as critical. Affected by this issue is the function Search of the file library_management/src/Library_Management/Forgot.java. The manipulation of the argument txtuname leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-32550	WordPress Click & Pledge Connect Plugin Plugin <= 2.24080000-WP6.6.1 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ClickandPledge Click & Pledge Connect Plugin allows SQL Injection. This issue affects Click & Pledge Connect Plugin: from 2.24080000 through WP6.6.1.	Patched by core rule	Y
CVE-2025-32558	WordPress Duplicate Title Checker Plugin <= 1.2 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ketanajani Duplicate Title Checker allows Blind SQL Injection. This issue affects Duplicate Title Checker: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-32565	WordPress Neon Product Designer Plugin <= 2.1.1 - Unauthenticated SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in vertim Neon Product Designer allows SQL Injection. This issue affects Neon Product Designer: from n/a through 2.1.1.	Patched by core rule	Y
CVE-2025-32567	WordPress Easy Post Duplicator Plugin <= 1.0.1 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in dev02ali Easy Post Duplicator allows SQL Injection. This issue affects Easy Post Duplicator: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-32573	WordPress KiotViet Sync Plugin <= 1.8.3 - SQL	Improper Neutralization of Special Elements used in an	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Injection vulnerability	SQL Command ('SQL Injection') vulnerability in Kiotviet KiotViet Sync allows SQL Injection. This issue affects KiotViet Sync: from n/a through 1.8.3.		
CVE-2025-3258	PHPGurukul Old Age Home Management System search.php sql injection	A vulnerability classified as critical was found in PHPGurukul Old Age Home Management System 1.0. This vulnerability affects unknown code of the file /search.php. The manipulation of the argument searchdata leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-32603	WordPress WP Online Users Stats plugin <= 1.0.0 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in HK WP Online Users Stats allows Blind SQL Injection. This issue affects WP Online Users Stats: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-32618	WordPress Wishlist plugin <= 1.0.43 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in PickPlugins Wishlist allows SQL Injection. This issue affects Wishlist: from n/a through 1.0.43.	Patched by core rule	Y
CVE-2025-32626	WordPress JS Job Manager plugin <= 2.0.2 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in JoomSky JS Job Manager allows SQL Injection. This issue affects JS Job Manager: from n/a through 2.0.2.	Patched by core rule	Y
CVE-2025-32636	WordPress Local Magic Plugin <= 2.6.0 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in matthewrubin Local Magic allows SQL Injection. This issue affects Local Magic: from n/a through 2.6.0.	Patched by core rule	Y
CVE-2025-3265	PHPGurukul e-Diary Management System add-category.php sql injection	A vulnerability classified as critical was found in PHPGurukul e-Diary Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /add-category.php. The manipulation of the argument Category leads to sql injection. The attack can	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-32650	WordPress Accessibility Suite by Ability, Inc plugin <= 4.18 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ability, Inc Accessibility Suite by Online ADA allows SQL Injection. This issue affects Accessibility Suite by Online ADA: from n/a through 4.18.	Patched by core rule	Y
CVE-2025-32665	WordPress Office Locator plugin <= 1.3.0 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WebbyTemplate Office Locator allows SQL Injection. This issue affects Office Locator: from n/a through 1.3.0.	Patched by core rule	Y
CVE-2025-3267	qinguoyi TinyWebServer http_conn.cpp sql injection	A vulnerability, which was classified as critical, was found in qinguoyi TinyWebServer up to 1.0. This affects an unknown part of the file /http/http_conn.cpp. The manipulation of the argument name/password leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-32676	WordPress Verowa Connect plugin <= 3.0.5 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Picture-Planet GmbH Verowa Connect allows Blind SQL Injection. This issue affects Verowa Connect: from n/a through 3.0.5.	Patched by core rule	Y
CVE-2025-32677	WordPress WP Social Stream Designer plugin <= 1.3 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in solwininfotech WP Social Stream Designer allows Blind SQL Injection. This issue affects WP Social Stream Designer: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-32681	WordPress Error Log Viewer By WP Guru plugin <= 1.0.5 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WP Guru Error Log Viewer allows Blind SQL Injection. This issue affects Error Log Viewer: from n/a through 1.0.5.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-32685	WordPress WP Inquiries <= 0.2.1 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Aristo Rinjuang WP Inquiries allows SQL Injection. This issue affects WP Inquiries: from n/a through 0.2.1.	Patched by core rule	Y
CVE-2025-32687	WordPress Review Stars Count For WooCommerce <= 2.0 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Magnigenie Review Stars Count For WooCommerce allows SQL Injection. This issue affects Review Stars Count For WooCommerce: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-32956	ManageWiki has SQL injection vulnerability in NamespaceMigrationJob	ManageWiki is a MediaWiki extension allowing users to manage wikis. Versions before commit f504ed8, are vulnerable to SQL injection when renaming a namespace in Special:ManageWiki/namespaces when using a page prefix (namespace name, which is the current namespace you are renaming) with an injection payload. This issue has been patched in commit f504ed8. A workaround for this vulnerability involves setting `$wgManageWiki['namespaces'] = false;`.	Patched by core rule	Y
CVE-2025-3296	SourceCodester Online Eyewear Shop Users.php sql injection	A vulnerability, which was classified as critical, has been found in SourceCodester Online Eyewear Shop 1.0. This issue affects some unknown processing of the file /classes/Users.php?f=delete_customer. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-32968	org.xwiki.platform:xwiki-platform-oldcore allows SQL injection in short form select requests through the script query API	XWiki is a generic wiki platform. In versions starting from 1.6-milestone-1 to before 15.10.16, 16.4.6, and 16.10.1, it is possible for a user with SCRIPT right to escape from the HQL execution context and perform a blind SQL injection to execute arbitrary SQL statements on the database backend. Depending on the used	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		database backend, the attacker may be able to not only obtain confidential information such as password hashes from the database, but also execute UPDATE/INSERT/DELETE queries. This issue has been patched in versions 16.10.1, 16.4.6 and 15.10.16. There is no known workaround, other than upgrading XWiki. The protection added to this REST API is the same as the one used to validate complete select queries, making it more consistent. However, while the script API always had this protection for complete queries, it's important to note that it's a very strict protection and some valid, but complex, queries might suddenly require the author to have programming right.		
CVE-2025-32969	org.xwiki.platform:xwiki-platform-rest-server allows SQL injection in query endpoint of REST API	XWiki is a generic wiki platform. In versions starting from 1.8 and prior to 15.10.16, 16.4.6, and 16.10.1, it is possible for a remote unauthenticated user to escape from the HQL execution context and perform a blind SQL injection to execute arbitrary SQL statements on the database backend, including when "Prevent unregistered users from viewing pages, regardless of the page rights" and "Prevent unregistered users from editing pages, regardless of the page rights" options are enabled. Depending on the used database backend, the attacker may be able to not only obtain confidential information such as password hashes from the database, but also execute UPDATE/INSERT/DELETE queries. This issue has been patched in versions 16.10.1, 16.4.6 and 15.10.16. There is no known workaround, other than upgrading XWiki.	Patched by core rule	Y
CVE-2025-3299	PHPGurukul Men Salon Management System appointment.php sql injection	A vulnerability was found in PHPGurukul Men Salon Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /appointment.php. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument Name leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3303	code-projects Patient Record Management System birthing_record.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Patient Record Management System 1.0. Affected by this issue is some unknown functionality of the file /birthing_record.php. The manipulation of the argument itr_no leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3304	code-projects Patient Record Management System dental_not.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Patient Record Management System 1.0. This affects an unknown part of the file /dental_not.php. The manipulation of the argument itr_no leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3306	code-projects Blood Bank Management System don.php sql injection	A vulnerability was found in code-projects Blood Bank Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /don.php. The manipulation of the argument fullname leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-3307	code-projects Blood Bank Management System reset.php sql injection	A vulnerability was found in code-projects Blood Bank Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /reset.php. The manipulation of the argument useremail leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3308	code-projects Blood Bank Management System	A vulnerability was found in code-projects Blood Bank	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	viewrequest.php sql injection	Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /viewrequest.php. The manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3309	code-projects Blood Bank Management System campsdetails.php sql injection	A vulnerability was found in code-projects Blood Bank Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/campsdetails.php. The manipulation of the argument hospital leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3310	code-projects Blood Bank Management System delete.php sql injection	A vulnerability classified as critical has been found in code-projects Blood Bank Management System 1.0. This affects an unknown part of the file /admin/delete.php. The manipulation of the argument Search leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3311	PHPGurukul Men Salon Management System about-us.php sql injection	A vulnerability classified as critical was found in PHPGurukul Men Salon Management System 1.0. This vulnerability affects unknown code of the file /admin/about-us.php. The manipulation of the argument pagetitle leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3312	PHPGurukul Men Salon Management System add-customer-services.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Men Salon Management System 1.0. This issue affects some unknown processing of the file /admin/add-customer-services.php. The manipulation of the argument sids[] leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the public and may be used.		
CVE-2025-3313	PHPGurukul Men Salon Management System add-customer.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Men Salon Management System 1.0. Affected is an unknown function of the file /admin/add-customer.php. The manipulation of the argument Name leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3314	SourceCodester Apartment Visitor Management System forgotpw.php sql injection	A vulnerability has been found in SourceCodester Apartment Visitor Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /forgotpw.php. The manipulation of the argument secode leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3315	SourceCodester Apartment Visitor Management System view-report.php sql injection	A vulnerability was found in SourceCodester Apartment Visitor Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /view-report.php. The manipulation of the argument fromdate/todate leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3316	PHPGurukul Men Salon Management System search-invoices.php sql injection	A vulnerability was found in PHPGurukul Men Salon Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/search-invoices.php. The manipulation of the argument searchdata leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3318	Kenj_Frog 肯尼基蛙 company-financial-management 公司财务管理系统 ShangpinleixingController	A vulnerability classified as critical was found in Kenj_Frog 肯尼基蛙 company-financial-management 公司财务管理	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	.java page sql injection	系统 1.0. Affected by this vulnerability is the function page of the file src/main/java/com/controller/ShangpinleixingController.java. The manipulation of the argument sort leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available.		
CVE-2025-3323	godcheese/code-projects Nimrod ViewMenuCategoryRestController.java sql injection	A vulnerability classified as critical was found in godcheese/code-projects Nimrod 0.8. Affected by this vulnerability is an unknown functionality of the file ViewMenuCategoryRestController.java. The manipulation of the argument Name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3330	codeprojects Online Restaurant Management System reservation_save.php sql injection	A vulnerability classified as critical was found in codeprojects Online Restaurant Management System 1.0. This vulnerability affects unknown code of the file /reservation_save.php. The manipulation of the argument first leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-3331	codeprojects Online Restaurant Management System payment_save.php sql injection	A vulnerability, which was classified as critical, has been found in codeprojects Online Restaurant Management System 1.0. This issue affects some unknown processing of the file /payment_save.php. The manipulation of the argument mode leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3332	codeprojects Online Restaurant Management System menu_save.php sql injection	A vulnerability, which was classified as critical, was found in codeprojects Online Restaurant Management	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		System 1.0. Affected is an unknown function of the file /admin/menu_save.php. The manipulation of the argument menu leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3333	codeprojects Online Restaurant Management System menu_update.php sql injection	A vulnerability has been found in codeprojects Online Restaurant Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/menu_update.php. The manipulation of the argument menu leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3334	codeprojects Online Restaurant Management System category_save.php sql injection	A vulnerability was found in codeprojects Online Restaurant Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/category_save.php. The manipulation of the argument Category leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3335	codeprojects Online Restaurant Management System category_update.php sql injection	A vulnerability was found in codeprojects Online Restaurant Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/category_update.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3336	codeprojects Online Restaurant Management System member_save.php sql injection	A vulnerability was found in codeprojects Online Restaurant Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/member_save.php. The manipulation of the argument last leads to sql injection. The attack can be initiated remotely. The		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit has been disclosed to the public and may be used. Other parameters might be affected as well.		
CVE-2025-3337	codeprojects Online Restaurant Management System member_update.php sql injection	A vulnerability was found in codeprojects Online Restaurant Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/member_update.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3338	codeprojects Online Restaurant Management System user_save.php sql injection	A vulnerability classified as critical has been found in codeprojects Online Restaurant Management System 1.0. Affected is an unknown function of the file /admin/user_save.php. The manipulation of the argument Name leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-3339	codeprojects Online Restaurant Management System user_update.php sql injection	A vulnerability classified as critical was found in codeprojects Online Restaurant Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/user_update.php. The manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3340	codeprojects Online Restaurant Management System combo_update.php sql injection	A vulnerability, which was classified as critical, has been found in codeprojects Online Restaurant Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/combo_update.php. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3341	codeprojects Online Restaurant Management	A vulnerability, which was classified as critical, was	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System reservation_view.php sql injection	found in codeprojects Online Restaurant Management System 1.0. This affects an unknown part of the file /admin/reservation_view.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3342	codeprojects Online Restaurant Management System payment_save.php sql injection	A vulnerability has been found in codeprojects Online Restaurant Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/payment_save.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3343	codeprojects Online Restaurant Management System reservation_update.php sql injection	A vulnerability was found in codeprojects Online Restaurant Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/reservation_update.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3344	codeprojects Online Restaurant Management System assign_save.php sql injection	A vulnerability was found in codeprojects Online Restaurant Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/assign_save.php. The manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3345	codeprojects Online Restaurant Management System combo.php sql injection	A vulnerability was found in codeprojects Online Restaurant Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/combo.php. The manipulation of the argument del leads to sql	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3347	code-projects Patient Record Management System dental_pending.php sql injection	A vulnerability classified as critical has been found in code-projects Patient Record Management System 1.0. This affects an unknown part of the file /dental_pending.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3348	code-projects Patient Record Management System edit_dpatient.php sql injection	A vulnerability classified as critical was found in code-projects Patient Record Management System 1.0. This vulnerability affects unknown code of the file /edit_dpatient.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3350	PHPGurukul Old Age Home Management System view-enquiry.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Old Age Home Management System 1.0. Affected is an unknown function of the file /admin/view-enquiry.php. The manipulation of the argument viewid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3351	PHPGurukul Old Age Home Management System login.php sql injection	A vulnerability has been found in PHPGurukul Old Age Home Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/login.php. The manipulation of the argument Username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3352	PHPGurukul Old Age Home Management System edit-scdetails.php sql injection	A vulnerability was found in PHPGurukul Old Age Home Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the file /admin/edit-scdetails.php. The manipulation of the argument contnum leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3353	PHPGurukul Men Salon Management System add-services.php sql injection	A vulnerability was found in PHPGurukul Men Salon Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/add-services.php. The manipulation of the argument cost leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3369	xxyopen Novel-Plus list sql injection	A vulnerability was found in xxyopen Novel-Plus 5.1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /novel/friendLink/list. The manipulation of the argument sort leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3370	PHPGurukul Men Salon Management System admin-profile.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Men Salon Management System 1.0. This affects an unknown part of the file /admin/admin-profile.php. The manipulation of the argument contactnumber leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-3382	joey-zhou xiaozhi-esp32-server-java update sql injection	A vulnerability has been found in joey-zhou xiaozhi-esp32-server-java up to a14fe8115842ee42ab5c7a51706b8a85db5200b7 and classified as critical. This vulnerability affects the function update of the file /api/user/update. The manipulation of the argument state leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available.		
CVE-2025-3383	SourceCodester Web-based Pharmacy Product Management System search_sales.php sql injection	A vulnerability was found in SourceCodester Web-based Pharmacy Product Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /search/search_sales.php. The manipulation of the argument Name leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3384	1000 Projects Human Resource Management System employee.php sql injection	A vulnerability was found in 1000 Projects Human Resource Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /controller/employee.php. The manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3399	ESAFENET CDG updateNotice.jsp sql injection	A vulnerability, which was classified as critical, has been found in ESAFENET CDG 5.6.3.154.205_20250114. Affected by this issue is some unknown functionality of the file /pubinfo/updateNotice.jsp. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-3400	ESAFENET CDG UnChkMailApplication.jsp sql injection	A vulnerability, which was classified as critical, was found in ESAFENET CDG 5.6.3.154.205_20250114. This affects an unknown part of the file /client/UnChkMailApplication.jsp. The manipulation of the argument typename leads to sql injection. It is		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-3401	ESAFENET CDG getLimitIPList.jsp sql injection	A vulnerability has been found in ESAFENET CDG 5.6.3.154.205_20250114 and classified as critical. This vulnerability affects unknown code of the file /parameter/getLimitIPList.jsp. The manipulation of the argument noticeId leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-3402	Seeyon Zhiyuan Interconnect FE Collaborative Office Platform check.js%70 sql injection	A vulnerability was found in Seeyon Zhiyuan Interconnect FE Collaborative Office Platform 5.5.2 and classified as critical. This issue affects some unknown processing of the file /sysform/042/check.js%70. The manipulation of the argument Name leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-3534	PowerCreator CMS OpenPublicCourse.aspx sql injection	A vulnerability, which was classified as critical, was found in PowerCreator CMS 1.0. Affected is an unknown function of the file /OpenPublicCourse.aspx. The manipulation of the argument cid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-3589	SourceCodester Music Class Enrollment System manage_class.php sql injection	A vulnerability, which was classified as critical, was found in SourceCodester Music Class Enrollment System 1.0. Affected is an unknown function of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/manage_class.php. The manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3676	xxyopen Novel-Plus books sql injection	A vulnerability classified as critical has been found in xxyopen Novel-Plus 3.5.0. This affects an unknown part of the file /api/front/search/books. The manipulation of the argument sort leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-3684	Xianqi Kindergarten Management System Child Management stu_list.php sql injection	A vulnerability was found in Xianqi Kindergarten Management System 2.0 Bulid 20190808. It has been rated as critical. This issue affects some unknown processing of the file stu_list.php of the component Child Management. The manipulation of the argument sex leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-3685	code-projects Patient Record Management System edit_fpatient.php sql injection	A vulnerability classified as critical has been found in code-projects Patient Record Management System 1.0. Affected is an unknown function of the file /edit_fpatient.php. The manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3689	PHPGurukul Men Salon Management System edit-customer-detailed.php sql injection	A vulnerability has been found in PHPGurukul Men Salon Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/edit-customer-detailed.php. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument editid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3690	PHPGurukul Men Salon Management System edit-services.php sql injection	A vulnerability was found in PHPGurukul Men Salon Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/edit-services.php. The manipulation of the argument cost leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3694	SourceCodester Web-based Pharmacy Product Management System Login sql injection	A vulnerability classified as critical has been found in SourceCodester Web-based Pharmacy Product Management System 1.0. This affects an unknown part of the component Login Handler. The manipulation of the argument login_email leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3696	SourceCodester Web-based Pharmacy Product Management System search_stock. php sql injection	A vulnerability classified as critical was found in SourceCodester Web-based Pharmacy Product Management System 1.0. This vulnerability affects unknown code of the file /search/search_stock. php. The manipulation of the argument Name leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3697	SourceCodester Web-based Pharmacy Product Management System edit-product.php sql injection	A vulnerability, which was classified as critical, has been found in SourceCodester Web-based Pharmacy Product Management System 1.0. This issue affects some unknown processing of the file /edit-product.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3767	SQL Injection in Centreon BAM boolean KPI listing	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Centreon BAM (Boolean KPi Listing modules) allows SQL Injection. This page is only accessible to authenticated users with high privileges. This issue affects Centreon BAM: from 24.10 before 24.10.1, from 24.04 before 24.04.5, from 23.10 before 23.10.10, from 23.04 before 23.04.10.		
CVE-2025-3792	SeaCMS admin_link.php sql injection	A vulnerability, which was classified as critical, has been found in SeaCMS up to 13.3. This issue affects some unknown processing of the file /admin_link.php?action=delall. The manipulation of the argument e_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3796	PHPGurukul Men Salon Management System contact-us.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Men Salon Management System 1.0. This affects an unknown part of the file /admin/contact-us.php. The manipulation of the argument pagetitle/pagedes/email/mobnumber/timing leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3797	SeaCMS admin_topic.php sql injection	A vulnerability classified as critical was found in SeaCMS up to 13.3. This vulnerability affects unknown code of the file /admin_topic.php?action=delall. The manipulation of the argument e_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3799	WCMS AnonymousController.php sql injection	A vulnerability, which was classified as critical, was found in WCMS 11. Affected is an unknown function of the file app/controllers/AnonymousController.php. The manipulation of the argument email/username leads to sql injection. It is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.		
CVE-2025-3800	WCMS AnonymousController.php sql injection	A vulnerability has been found in WCMS 11 and classified as critical. Affected by this vulnerability is an unknown functionality of the file app/controllers/AnonymousController.php. The manipulation of the argument mobile_phone leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-3817	SourceCodester Online Eyewear Shop Master.php sql injection	A vulnerability, which was classified as critical, has been found in SourceCodester Online Eyewear Shop 1.0. This issue affects some unknown processing of the file /oews/classes/Master.php?f=delete_stock. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3819	PHPGurukul Men Salon Management System search-appointment.php sql injection	A vulnerability has been found in PHPGurukul Men Salon Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/search-appointment.php. The manipulation of the argument searchdata leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3827	PHPGurukul Men Salon Management System forgot-password.php sql injection	A vulnerability has been found in PHPGurukul Men Salon Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/forgot-password.php. The manipulation of the argument email leads to sql injection. The attack can be initiated remotely. The		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit has been disclosed to the public and may be used.		
CVE-2025-3828	PHPGurukul Men Salon Management System view-appointment.php sql injection	A vulnerability was found in PHPGurukul Men Salon Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/view-appointment.php?viewid=11. The manipulation of the argument remark leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-3829	PHPGurukul Men Salon Management System sales-reports-detail.php sql injection	A vulnerability was found in PHPGurukul Men Salon Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/sales-reports-detail.php. The manipulation of the argument fromdate/todate leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3856	xxyopen Novel-Plus searchByPage sql injection	A vulnerability was found in xxyopen Novel-Plus 5.1.0. It has been classified as critical. This affects the function searchByPage of the file /book/searchByPage. The manipulation of the argument sort leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-3872	Privilege escalation by altering payload in contact form	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Centreon centreon-web (User configuration form modules) allows SQL Injection. A user with high privileges is able to become administrator by intercepting the contact form request and altering its payload.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This issue affects Centreon: from 22.10.0 before 22.10.28, from 23.04.0 before 23.04.25, from 23.10.0 before 23.10.20, from 24.04.0 before 24.04.10, from 24.10.0 before 24.10.4.		
CVE-2025-39377	WordPress Appsero Helper plugin <= 1.3.4 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in weDevs Appsero Helper allows SQL Injection. This issue affects Appsero Helper: from n/a through 1.3.4.	Patched by core rule	Y
CVE-2025-39471	WordPress Modal Survey plugin <= 2.0.2.0.1 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Pantherius Modal Survey.This issue affects Modal Survey: from n/a through 2.0.2.0.1.	Patched by core rule	Y
CVE-2025-39518	WordPress BMA Lite <= 1.4.2 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in RedefiningTheWeb BMA Lite allows SQL Injection. This issue affects BMA Lite: from n/a through 1.4.2.	Patched by core rule	Y
CVE-2025-39566	WordPress Hostel <= 1.1.5.6 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Bob Hostel allows Blind SQL Injection. This issue affects Hostel: from n/a through 1.1.5.6.	Patched by core rule	Y
CVE-2025-39569	WordPress Taskbuilder <= 4.0.1 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in taskbuilder Taskbuilder allows Blind SQL Injection. This issue affects Taskbuilder: from n/a through 4.0.1.	Patched by core rule	Y
CVE-2025-39586	WordPress ProfileGrid <= 5.9.4.8 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Metagauss ProfileGrid allows SQL Injection. This issue affects ProfileGrid : from n/a through 5.9.4.8.	Patched by core rule	Y
CVE-2025-39587	WordPress Cost Calculator Builder <= 3.2.65 - SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Vulnerability	Injection') vulnerability in Stylemix Cost Calculator Builder allows SQL Injection. This issue affects Cost Calculator Builder: from n/a through 3.2.65.		
CVE-2025-39595	WordPress Quentn WP <= 1.2.8 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Quentn.com GmbH Quentn WP allows SQL Injection. This issue affects Quentn WP: from n/a through 1.2.8.	Patched by core rule	Y
CVE-2025-46242	WordPress Watu Quiz <= 3.4.3 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Bob Watu Quiz allows SQL Injection. This issue affects Watu Quiz: from n/a through 3.4.3.	Patched by core rule	Y
CVE-2025-46248	WordPress Frontend Dashboard <= 2.2.5 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in M A Vinoth Kumar Frontend Dashboard allows SQL Injection. This issue affects Frontend Dashboard: from n/a through 2.2.5.	Patched by core rule	Y
CVE-2025-46252	WordPress Message Filter for Contact Form 7 plugin <= 1.6.3.2 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in kofimokome Message Filter for Contact Form 7 allows SQL Injection. This issue affects Message Filter for Contact Form 7: from n/a through 1.6.3.2.	Patched by core rule	Y

XML External Entity Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-32138	WordPress Easy Google Maps plugin <= 1.11.17 - XML External Entity vulnerability	Improper Restriction of XML External Entity Reference vulnerability in supsystic Easy Google Maps allows XML Injection. This issue affects Easy Google Maps: from n/a through 1.11.17.	Patched by core rule	Y
CVE-2025-3241	zhangyanbo2007 youkefu XML Document CallCenterRouterController.java xml external entity reference	A vulnerability, which was classified as problematic, was found in zhangyanbo2007 youkefu up to 4.2.0. This affects an unknown part of the file src/main/java/com/ukefu/webim/web/handler/admin/callcenter/CallCenterRouterController.java of the component XML Document Handler. The manipulation of the argument routercontent leads to xml external entity reference. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y

HTML Injection Vulnerability

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-30166	Pimcore's Admin Classic Bundle allows HTML Injection	Pimcore's Admin Classic Bundle provides a Backend UI for Pimcore. An HTML injection issue allows users with access to the email sending functionality to inject arbitrary HTML code into emails sent via the admin interface, potentially leading to session cookie theft and the alteration of page content. The vulnerability was discovered in the /admin/email/send-test-email endpoint using the POST method. The vulnerable parameter is content, which permits the injection of arbitrary HTML code during the email sending process. While JavaScript code injection is blocked through filtering, HTML code injection remains possible. This vulnerability is fixed in 1.7.6.	Patched by Custom Rule	Y

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-39311	Publify Vulnerable To Cross-Site Scripting (XSS) Via Redirects Requiring User Interaction	Publify is a self hosted Web publishing platform on Rails. Prior to version 10.0.1 of Publify, corresponding to versions prior to 10.0.2 of the `publify_core` rubygem, publisher on a `publify` application is able to perform a cross-site scripting (XSS) attack on an administrator using the redirect functionality. The exploitation of this XSS vulnerability requires the administrator to click a malicious link. An attack could attempt to hide their payload by using HTML, or other encodings, as to not make it obvious to an administrator that this is a malicious link. A publisher may attempt to use this vulnerability to escalate their privileges and become an administrator. Version 10.0.1 of Publify and version 10.0.2 of the `publify_core` rubygem fix the issue.	Patched by core rule	Y
CVE-2024-51624	WordPress Já-Já Pagamentos for WooCommerce plugin <= 1.3.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jajapagamentos Já-Já Pagamentos for WooCommerce allows Reflected XSS. This issue affects Já-Já Pagamentos for WooCommerce: from n/a through 1.3.0.	Patched by core rule	Y
CVE-2024-52281	Stored Cross-site Scripting vulnerability in Rancher UI	A: Improper Neutralization of Input During Web Page Generation vulnerability in SUSE rancher allows a malicious actor to perform a Stored XSS attack through the cluster description field. This issue affects rancher: from 2.9.0 before 2.9.4.	Patched by core rule	Y
CVE-2024-55093	N/A	phpIPAM through 1.7.3 has a reflected Cross-Site Scripting (XSS) vulnerability in the install scripts.	Patched by core rule	Y
CVE-2024-58128	N/A	In MISP before 2.4.193, menu_custom_right_link parameters can be set via the UI (i.e., without using the CLI) and thus attackers with admin privileges can conduct XSS attacks via a global menu link.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-58129	N/A	In MISP before 2.4.193, menu_custom_right_link_html parameters can be set via the UI (i.e., without using the CLI) and thus attackers with admin privileges can conduct XSS attacks against every page.	Patched by core rule	Y
CVE-2025-0811	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in GitLab	An issue has been discovered in GitLab CE/EE affecting all versions from 17.7 before 17.8.6, 17.9 before 17.9.3, and 17.10 before 17.10.1. Improper rendering of certain file types leads to cross-site scripting.	Patched by core rule	Y
CVE-2025-1267	Groundhogg <= 3.7.4.1 - Authenticated (Administrator+) Stored Cross-Site Scripting via label Parameter	The Groundhogg plugin for Wordpress is vulnerable to Stored Cross-Site Scripting via the ‘label' parameter in versions up to, and including, 3.7.4.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	Patched by core rule	Y
CVE-2025-22263	WordPress Global Gallery plugin <= 8.8.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Global Gallery allows Reflected XSS. This issue affects Global Gallery: from n/a through 8.8.0.	Patched by core rule	Y
CVE-2025-22268	WordPress Uncanny Toolkit for LearnDash plugin <= 3.7.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Uncanny Owl Uncanny Toolkit for LearnDash allows Stored XSS. This issue affects Uncanny Toolkit for LearnDash: from n/a through 3.7.0.1.	Patched by core rule	Y
CVE-2025-22269	WordPress Real Testimonials plugin <= 3.1.6 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ShapedPlugin LLC Real Testimonials allows Stored XSS. This issue affects Real Testimonials: from n/a through 3.1.6.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-22278	WordPress Whitish Lite theme <= 2.1.13 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in yudleethemes Whitish Lite allows Stored XSS.This issue affects Whitish Lite: from n/a through 2.1.13.	Patched by core rule	Y
CVE-2025-22281	WordPress Simplish theme <= 2.6.4 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in joshix Simplish allows Stored XSS.This issue affects Simplish: from n/a through 2.6.4.	Patched by core rule	Y
CVE-2025-22282	WordPress ez Form Calculator - WordPress plugin plugin <= 2.14.1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in EPC ez Form Calculator - WordPress plugin allows Reflected XSS.This issue affects ez Form Calculator - WordPress plugin: from n/a through 2.14.1.2.	Patched by core rule	Y
CVE-2025-22283	WordPress GetSocial Plugin <= 2.0.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Riyaz GetSocial allows Reflected XSS. This issue affects GetSocial: from n/a through 2.0.1.	Patched by core rule	Y
CVE-2025-22340	WordPress Data Dash plugin <= 1.2.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Think201 Data Dash allows Stored XSS. This issue affects Data Dash: from n/a through 1.2.3.	Patched by core rule	Y
CVE-2025-22356	WordPress Stencies plugin <= 0.58 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Stencies Stencies allows Reflected XSS. This issue affects Stencies: from n/a through 0.58.	Patched by core rule	Y
CVE-2025-22360	WordPress WP Azure offload plugin <= 2.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WP Azure offload allows Reflected XSS. This issue affects WP Azure offload: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-2255	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in GitLab	An issue has been discovered in Gitlab EE/CE for AppSec affecting all versions from 13.5.0 before	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		17.8.6, 17.9 before 17.9.3, and 17.10 before 17.10.1. Certain error messages could allow Cross-Site Scripting attacks (XSS). for AppSec.		
CVE-2025-22565	WordPress vooPlayer v4 Plugin <= 4.0.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bill Zimmerman vooPlayer v4 allows Reflected XSS. This issue affects vooPlayer v4: from n/a through 4.0.4.	Patched by core rule	Y
CVE-2025-22566	WordPress ULTIMATE VIDEO GALLERY Plugin <= 1.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound ULTIMATE VIDEO GALLERY allows Reflected XSS. This issue affects ULTIMATE VIDEO GALLERY: from n/a through 1.4.	Patched by core rule	Y
CVE-2025-22575	WordPress SUPER RESPONSIVE SLIDER Plugin <= 1.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in extendyourweb SUPER RESPONSIVE SLIDER allows Reflected XSS. This issue affects SUPER RESPONSIVE SLIDER: from n/a through 1.4.	Patched by core rule	Y
CVE-2025-22628	WordPress Filled In Plugin <= 1.9.2 - CSRF to Stored XSS vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Foliovision Filled In allows Stored XSS.This issue affects Filled In: from n/a through 1.9.2.	Patched by core rule	Y
CVE-2025-22636	WordPress VR-Frases plugin <= 3.0.1 - Reflected XSS to SQL Injection vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vicente Ruiz Gálvez VR-Frases allows Reflected XSS. This issue affects VR-Frases: from n/a through 3.0.1.	Patched by core rule	Y
CVE-2025-22638	WordPress Product Table For WooCommerce Plugin <= 1.2.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Acowebs Product Table For WooCommerce allows Stored XSS.This issue affects Product Table For WooCommerce: from n/a through 1.2.3.	Patched by core rule	Y
CVE-2025-22640	WordPress Paytm Payment Donation Plugin <= 2.3.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Paytm Paytm Payment	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Donation allows Stored XSS.This issue affects Paytm Payment Donation: from n/a through 2.3.3.		
CVE-2025-22644	WordPress Vayu Blocks – Gutenberg Blocks plugin <= 1.2.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeHunk Vayu Blocks – Gutenberg Blocks for WordPress & WooCommerce allows Stored XSS.This issue affects Vayu Blocks – Gutenberg Blocks for WordPress & WooCommerce: from n/a through 1.2.1.	Patched by core rule	Y
CVE-2025-22646	WordPress aThemes Addons for Elementor plugin <= 1.0.8 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in aThemes aThemes Addons for Elementor allows Stored XSS.This issue affects aThemes Addons for Elementor: from n/a through 1.0.8.	Patched by core rule	Y
CVE-2025-22648	WordPress Blog, Posts and Category Filter for Elementor plugin <= 2.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Plugin Devs Blog, Posts and Category Filter for Elementor allows Stored XSS.This issue affects Blog, Posts and Category Filter for Elementor: from n/a through 2.0.1.	Patched by core rule	Y
CVE-2025-22649	WordPress WP Project Manager plugin <= 2.6.22 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in weDevs WP Project Manager wedevs-project-manager allows Stored XSS.This issue affects WP Project Manager: from n/a through 2.6.22.	Patched by core rule	Y
CVE-2025-22651	WordPress Stylish Google Sheet Reader plugin <= 4.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wppluginboxdev Stylish Google Sheet Reader allows Reflected XSS. This issue affects Stylish Google Sheet Reader: from n/a through 4.0.	Patched by core rule	Y
CVE-2025-22659	WordPress Orbit Fox by ThemeIsle plugin <= 2.10.44 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeisle Orbit Fox by ThemeIsle allows Stored XSS.This issue affects Orbit	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Fox by ThemeIsle: from n/a through 2.10.44.		
CVE-2025-22660	WordPress Include Mastodon Feed plugin <= 1.9.9 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wolfgang Include Mastodon Feed allows DOM-Based XSS.This issue affects Include Mastodon Feed: from n/a through 1.9.9.	Patched by core rule	Y
CVE-2025-22692	WordPress Sponsered Link plugin <= 4.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rachanaS Sponsered Link allows Reflected XSS. This issue affects Sponsered Link: from n/a through 4.0.	Patched by core rule	Y
CVE-2025-22767	WordPress GlobalPayments WooCommerce Plugin <= 1.13.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in globalpayments GlobalPayments WooCommerce allows Reflected XSS. This issue affects GlobalPayments WooCommerce: from n/a through 1.13.0.	Patched by core rule	Y
CVE-2025-22771	WordPress The Great Firewords of China plugin <= 1.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Studio Hyperset The Great Firewords of China allows Stored XSS. This issue affects The Great Firewords of China: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-22774	WordPress CRUDLab Scroll to Top Plugin <= 1.0.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CRUDLab CRUDLab Scroll to Top allows Reflected XSS. This issue affects CRUDLab Scroll to Top: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-22796	WordPress WP-Asambleas Plugin <= 2.85.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in platcom WP-Asambleas allows Reflected XSS. This issue affects WP-Asambleas: from n/a through 2.85.0.	Patched by core rule	Y
CVE-2025-22816	WordPress Power Mag theme <= 1.1.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodeTrendy Power Mag allows DOM-Based XSS.This issue affects Power Mag: from n/a through 1.1.5.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-23443	WordPress Author Showcase plugin <= 1.4.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Claire Ryan Author Showcase allows Reflected XSS. This issue affects Author Showcase: from n/a through 1.4.3.	Patched by core rule	Y
CVE-2025-23448	WordPress visualslider Sldier plugin <= 1.1.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in dastan800 visualslider Sldier allows Reflected XSS. This issue affects visualslider Sldier: from n/a through 1.1.1.	Patched by core rule	Y
CVE-2025-23459	WordPress NS Simple Intro Loader plugin <= 2.2.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound NS Simple Intro Loader allows Reflected XSS. This issue affects NS Simple Intro Loader: from n/a through 2.2.3.	Patched by core rule	Y
CVE-2025-23460	WordPress RWS Enquiry And Lead Follow-up plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound RWS Enquiry And Lead Follow-up allows Reflected XSS. This issue affects RWS Enquiry And Lead Follow-up: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23466	WordPress Site Editor Google Map plugin <= 1.0.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpsiteeditor Site Editor Google Map allows Reflected XSS. This issue affects Site Editor Google Map: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-23542	WordPress RDP Linkedin Login plugin <= 1.7.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Robert D Payne RDP Linkedin Login allows Reflected XSS. This issue affects RDP Linkedin Login: from n/a through 1.7.0.	Patched by core rule	Y
CVE-2025-23543	WordPress FOMO Pay Chinese Payment Solution plugin <= 2.0.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound FOMO Pay Chinese Payment Solution allows Reflected XSS. This issue affects FOMO Pay	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Chinese Payment Solution: from n/a through 2.0.4.		
CVE-2025-23546	WordPress RDP inGroups+ plugin <= 1.0.6 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound RDP inGroups+ allows Reflected XSS. This issue affects RDP inGroups+: from n/a through 1.0.6.	Patched by core rule	Y
CVE-2025-23612	WordPress Pixobe Cartography plugin <= 1.0.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Pixobe Cartography allows Reflected XSS. This issue affects Pixobe Cartography: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-23632	WordPress CG Button plugin <= 1.0.5.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rhizome Networks CG Button allows Reflected XSS. This issue affects CG Button: from n/a through 1.0.5.6.	Patched by core rule	Y
CVE-2025-23633	WordPress WP Database Audit plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WP Database Audit allows Reflected XSS. This issue affects WP Database Audit: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23638	WordPress Frontend Post Submission plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Frontend Post Submission allows Reflected XSS. This issue affects Frontend Post Submission: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23666	WordPress Management-screen-droptiles plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Management-screen-droptiles allows Reflected XSS. This issue affects Management-screen-droptiles: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23680	WordPress Narnoo Operator plugin <= 2.0.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Narnoo Operator allows Reflected XSS. This issue affects Narnoo Operator: from n/a through 2.0.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-23704	WordPress Your Lightbox plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Reuven Karasik Your Lightbox allows Reflected XSS. This issue affects Your Lightbox: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23714	WordPress AppReview plugin <= 0.2.9 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound AppReview allows Reflected XSS. This issue affects AppReview: from n/a through 0.2.9.	Patched by core rule	Y
CVE-2025-23728	WordPress AuMenu plugin <= 1.1.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound AuMenu allows Reflected XSS. This issue affects AuMenu: from n/a through 1.1.5.	Patched by core rule	Y
CVE-2025-23735	WordPress Infugrator plugin <= 1.0.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Cosmin Schiopu Infugrator allows Reflected XSS. This issue affects Infugrator: from n/a through 1.0.3.	Patched by core rule	Y
CVE-2025-23782	WordPress TotalContest Lite Plugin <= 2.8.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in TotalSuite TotalContest Lite allows Reflected XSS. This issue affects TotalContest Lite: from n/a through 2.8.1.	Patched by core rule	Y
CVE-2025-23855	WordPress SpiderDisplay plugin <= 1.9.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fyljp SpiderDisplay allows Reflected XSS. This issue affects SpiderDisplay: from n/a through 1.9.1.	Patched by core rule	Y
CVE-2025-23858	WordPress Custom Users Order Plugin <= 4.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hiren Patel Custom Users Order allows Reflected XSS. This issue affects Custom Users Order: from n/a through 4.2.	Patched by core rule	Y
CVE-2025-23964	WordPress Google Plus Plugin <= 1.0.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Google Plus	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		allows Reflected XSS. This issue affects Google Plus: from n/a through 1.0.2.		
CVE-2025-23995	WordPress Tantyyellow theme <= 1.0.0.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ta2g Tantyyellow allows Reflected XSS.This issue affects Tantyyellow: from n/a through 1.0.0.5.	Patched by core rule	Y
CVE-2025-24539	WordPress DeBounce Email Validator plugin <= 5.6.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in debounce DeBounce Email Validator allows Reflected XSS. This issue affects DeBounce Email Validator: from n/a through 5.6.5.	Patched by core rule	Y
CVE-2025-24548	WordPress Autoglot – Automatic WordPress Translation plugin <=2.4.7 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Autoglot Autoglot – Automatic WordPress Translation allows Reflected XSS. This issue affects Autoglot – Automatic WordPress Translation: from n/a through 2.4.7.	Patched by core rule	Y
CVE-2025-24550	WordPress Job Manager plugin <= 2.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in JobScore Job Manager allows Stored XSS. This issue affects Job Manager: from n/a through 2.2.	Patched by core rule	Y
CVE-2025-24553	WordPress Shipping with Venipak for WooCommerce plugin <= 1.22.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Akadrama Shipping with Venipak for WooCommerce allows Reflected XSS. This issue affects Shipping with Venipak for WooCommerce: from n/a through 1.22.3.	Patched by core rule	Y
CVE-2025-24586	WordPress Shipment Tracker for Woocommerce plugin <= 1.4.23 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bitsstech Shipment Tracker for Woocommerce allows Reflected XSS. This issue affects Shipment Tracker for Woocommerce: from n/a through 1.4.23.	Patched by core rule	Y
CVE-2025-24619	WordPress WP Log Action Plugin <= 0.51 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webheadcoder WP Log	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Action allows Reflected XSS. This issue affects WP Log Action: from n/a through 0.51.		
CVE-2025-24621	WordPress Arconix Shortcodes plugin <= 2.1.15 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tychesoftwares Arconix Shortcodes allows Reflected XSS. This issue affects Arconix Shortcodes: from n/a through 2.1.15.	Patched by core rule	Y
CVE-2025-24624	WordPress HT Event – WordPress Event Manager Plugin for Elementor Plugin <= 1.4.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HasTech HT Event allows Reflected XSS. This issue affects HT Event: from n/a through 1.4.6.	Patched by core rule	Y
CVE-2025-24637	WordPress Beacon Lead Magnets and Lead Capture Plugin <= 1.5.7 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Syed Balkhi Beacon Lead Magnets and Lead Capture allows Reflected XSS. This issue affects Beacon Lead Magnets and Lead Capture: from n/a through 1.5.7.	Patched by core rule	Y
CVE-2025-24640	WordPress Empty Tags Remover Plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dan-Lucian Stefancu Empty Tags Remover allows Reflected XSS. This issue affects Empty Tags Remover: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-24645	WordPress Eazy Under Construction Plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rob Scott Eazy Under Construction allows Reflected XSS. This issue affects Eazy Under Construction: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-24655	WordPress Wishlist Plugin <= 1.0.39 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PickPlugins Wishlist allows Reflected XSS. This issue affects Wishlist: from n/a through 1.0.39.	Patched by core rule	Y
CVE-2025-24670	WordPress Term Taxonomy Converter Plugin <= 1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dhanendran Rajagopal Term Taxonomy Converter allows	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Reflected XSS. This issue affects Term Taxonomy Converter: from n/a through 1.2.		
CVE-2025-24745	WordPress Classified Listing plugin <= 4.0.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RadiusTheme Classified Listing allows Reflected XSS. This issue affects Classified Listing: from n/a through 4.0.1.	Patched by core rule	Y
CVE-2025-24752	WordPress Essential Addons for Elementor plugin <= 6.0.14 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPDeveloper Essential Addons for Elementor allows Reflected XSS. This issue affects Essential Addons for Elementor: from n/a through 6.0.14.	Patched by core rule	Y
CVE-2025-25197	Silverstripe Elemental enables XSS attacks in elemental "Content blocks in use" reports	Silverstripe Elemental extends a page type to swap the content area for a list of manageable elements to compose a page out of rather than a single text field. An elemental block can include an XSS payload, which can be executed when viewing the "Content blocks in use" report. The vulnerability is specific to that report and is a result of failure to cast input prior to including it in the grid field. This vulnerability is fixed in 5.3.12.	Patched by core rule	Y
CVE-2025-25427	XSS in TP-Link TL-WR841N Upnp page	A Stored cross-site scripting (XSS) vulnerability in upnp page of the web Interface in TP-Link WR841N <=4.19 allows remote attackers to inject arbitrary JavaScript code via the port mapping description. This leads to an execution of the JavaScript payload when the upnp page is loaded.	Patched by core rule	Y
CVE-2025-26536	WordPress Another Events Calendar Plugin <= 1.7.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Yendif Player Another Events Calendar allows Reflected XSS. This issue affects Another Events Calendar: from n/a through 1.7.0.	Patched by core rule	Y
CVE-2025-26537	WordPress GDPR Tools	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	plugin <= 1.0.2 - Cross Site Scripting (XSS) vulnerability	Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound GDPR Tools allows Stored XSS. This issue affects GDPR Tools: from n/a through 1.0.2.	rule	
CVE-2025-26541	WordPress Bitcoin / AltCoin Payment Gateway for WooCommerce plugin <= 1.7.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodeSolz Bitcoin / AltCoin Payment Gateway for WooCommerce allows Reflected XSS. This issue affects Bitcoin / AltCoin Payment Gateway for WooCommerce: from n/a through 1.7.6.	Patched by core rule	Y
CVE-2025-26542	WordPress Zalo Live Chat Plugin <= 1.1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Zalo Live Chat allows Reflected XSS. This issue affects Zalo Live Chat: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-26544	WordPressUTM tags + Landing page plugin <= 1.4 - CSRF to Stored XSS vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound UTM tags tracking for Contact Form 7 allows Reflected XSS. This issue affects UTM tags tracking for Contact Form 7: from n/a through 2.1.	Patched by core rule	Y
CVE-2025-26546	WordPress Cookies Pro plugin <= 1.0 - CSRF to Stored XSS vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Cookies Pro allows Reflected XSS. This issue affects Cookies Pro: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-26559	WordPress Secure Invites plugin <= 1.2.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Secure Invites allows Reflected XSS. This issue affects Secure Invites: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-26560	WordPress WP Contact Form III Plugin <= 1.6.2d - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WP Contact Form III allows Reflected XSS. This issue affects WP Contact Form III: from n/a through 1.6.2d.	Patched by core rule	Y
CVE-2025-26564	WordPress GNUCommerce Plugin <=	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	1.5.4 - Reflected Cross Site Scripting (XSS) vulnerability	Generation ('Cross-site Scripting') vulnerability in kagla GNUCommerce allows Reflected XSS. This issue affects GNUCommerce: from n/a through 1.5.4.		
CVE-2025-26565	WordPress GNUPress Plugin <= 0.2.9 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kagla GNUPress allows Reflected XSS. This issue affects GNUPress: from n/a through 0.2.9.	Patched by core rule	Y
CVE-2025-26566	WordPress In Stock Mailer for WooCommerce Plugin <= 2.1.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound In Stock Mailer for WooCommerce allows Reflected XSS. This issue affects In Stock Mailer for WooCommerce: from n/a through 2.1.1.	Patched by core rule	Y
CVE-2025-26573	WordPress Rizzi Guestbook plugin <= 4.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Rizzi Guestbook allows Reflected XSS. This issue affects Rizzi Guestbook: from n/a through 4.0.1.	Patched by core rule	Y
CVE-2025-26575	WordPress Display Post Meta plugin <= 1.5- Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kyle Maurer Display Post Meta allows Reflected XSS. This issue affects Display Post Meta: from n/a through 2.4.4.	Patched by core rule	Y
CVE-2025-26576	WordPress WP Simple Slideshow Plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in takumin WP Simple Slideshow allows Reflected XSS. This issue affects WP Simple Slideshow: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-26579	WordPress MicroPayments Paid Membership plugin <= 3.1.6 - Reflected Cross-Site Scripting vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in videowhisper MicroPayments allows Reflected XSS. This issue affects MicroPayments: from n/a through 3.1.6.	Patched by core rule	Y
CVE-2025-26581	WordPress Picture Gallery plugin <= 1.6.2 - CSRF to Stored XSS vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		videowhisper Picture Gallery allows Reflected XSS. This issue affects Picture Gallery: from n/a through 1.6.2.		
CVE-2025-26583	WordPress Video Share VOD plugin <= 2.7.2 - Reflected Cross-Site Scripting vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in videowhisper Video Share VOD allows Reflected XSS. This issue affects Video Share VOD: from n/a through 2.7.2.	Patched by core rule	Y
CVE-2025-26584	WordPress TBTestimonials Plugin <= 1.7.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound TBTestimonials allows Reflected XSS. This issue affects TBTestimonials: from n/a through 1.7.3.	Patched by core rule	Y
CVE-2025-26731	WordPress ARPrice plugin <= 4.1.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Repute Infosystems ARPrice allows Stored XSS.This issue affects ARPrice: from n/a through 4.1.3.	Patched by core rule	Y
CVE-2025-26732	WordPress StoreBiz plugin <= 1.0.32 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BurgerThemes StoreBiz allows DOM-Based XSS.This issue affects StoreBiz: from n/a through 1.0.32.	Patched by core rule	Y
CVE-2025-26734	WordPress Hester plugin <= 1.1.10 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in peregrinethemes Hester allows Stored XSS.This issue affects Hester: from n/a through 1.1.10.	Patched by core rule	Y
CVE-2025-26736	WordPress MorningTime Lite theme <= 1.3.2 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in viktoras MorningTime Lite allows Stored XSS.This issue affects MorningTime Lite: from n/a through 1.3.2.	Patched by core rule	Y
CVE-2025-26737	WordPress City Store theme <= 1.4.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in yudleethemes City Store allows DOM-Based XSS.This issue affects City Store: from n/a through 1.4.5.	Patched by core rule	Y
CVE-2025-26738	WordPress Quick Interest Slider plugin <= 3.1.3 -	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Cross Site Scripting (XSS) vulnerability	Generation ('Cross-site Scripting') vulnerability in Graham Quick Interest Slider allows DOM-Based XSS.This issue affects Quick Interest Slider: from n/a through 3.1.3.		
CVE-2025-26739	WordPress newseqo theme <= 2.1.1 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themefunction newseqo allows Stored XSS.This issue affects newseqo: from n/a through 2.1.1.	Patched by core rule	Y
CVE-2025-26740	WordPress SpaBiz plugin <= 1.0.18 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in burgersoftware SpaBiz allows DOM-Based XSS. This issue affects SpaBiz: from n/a through 1.0.18.	Patched by core rule	Y
CVE-2025-26743	WordPress Advance WP Query Search Filter plugin <= 1.0.10 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in TC.K Advance WP Query Search Filter allows Reflected XSS. This issue affects Advance WP Query Search Filter: from n/a through 1.0.10.	Patched by core rule	Y
CVE-2025-26744	WordPress JetBlog plugin <= 2.4.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound JetBlog allows DOM-Based XSS. This issue affects JetBlog: from n/a through 2.4.3.	Patched by core rule	Y
CVE-2025-26745	WordPress RS Elements Elementor Addon plugin <= 1.1.5 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RSTheme RS Elements Elementor Addon allows Stored XSS. This issue affects RS Elements Elementor Addon: from n/a through 1.1.5.	Patched by core rule	Y
CVE-2025-26746	WordPress Advanced Custom Fields: Link Picker Field plugin <= 1.2.8 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Advanced Custom Fields: Link Picker Field allows Reflected XSS. This issue affects Advanced Custom Fields: Link Picker Field: from n/a through 1.2.8.	Patched by core rule	Y
CVE-2025-26747	WordPress RainbowNews theme <= 1.0.7 - Cross	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Site Scripting (XSS) vulnerability	Generation ('Cross-site Scripting') vulnerability in 99colorthemes RainbowNews allows Stored XSS.This issue affects RainbowNews: from n/a through 1.0.7.		
CVE-2025-26749	WordPress Additional Custom Product Tabs for WooCommerce plugin <= 1.7.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Additional Custom Product Tabs for WooCommerce allows Stored XSS. This issue affects Additional Custom Product Tabs for WooCommerce: from n/a through 1.7.0.	Patched by core rule	Y
CVE-2025-26762	WordPress WooCommerce plugin <= 9.7.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Automattic WooCommerce allows Stored XSS.This issue affects WooCommerce: from n/a through 9.7.0.	Patched by core rule	Y
CVE-2025-26869	WordPress Build theme <= 1.0.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Build allows Stored XSS.This issue affects Build: from n/a through 1.0.3.	Patched by core rule	Y
CVE-2025-26870	WordPress JetEngine plugin <= 3.6.4.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound JetEngine allows DOM-Based XSS. This issue affects JetEngine: from n/a through 3.6.4.1.	Patched by core rule	Y
CVE-2025-26874	WordPress MemberSpace plugin <= 2.1.13 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MemberSpace allows Reflected XSS.This issue affects MemberSpace: from n/a through 2.1.13.	Patched by core rule	Y
CVE-2025-26880	WordPress SKT Skill Bar plugin <= 2.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sonalsinha21 SKT Skill Bar allows Stored XSS. This issue affects SKT Skill Bar: from n/a through 2.3.	Patched by core rule	Y
CVE-2025-26906	WordPress WP Delete User Accounts plugin <= 1.2.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ren Ventura WP Delete User Accounts allows DOM-Based XSS. This issue affects WP	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Delete User Accounts: from n/a through 1.2.3.		
CVE-2025-26919	WordPress Tainá plugin <= 0.2.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tainacan Tainá allows Stored XSS. This issue affects Tainá: from n/a through 0.2.2.	Patched by core rule	Y
CVE-2025-26922	WordPress AuraMart theme <= 2.0.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in techthemes AuraMart allows Stored XSS.This issue affects AuraMart: from n/a through 2.0.7.	Patched by core rule	Y
CVE-2025-26923	WordPress Event post plugin <= 5.9.8 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bastien Ho Event post allows Stored XSS.This issue affects Event post: from n/a through 5.9.8.	Patched by core rule	Y
CVE-2025-26929	WordPress Accounting for WooCommerce plugin <= 1.6.8 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NOUS Ouvert Utile et Simple Accounting for WooCommerce allows Stored XSS.This issue affects Accounting for WooCommerce: from n/a through 1.6.8.	Patched by core rule	Y
CVE-2025-26930	WordPress Home Services plugin <= 1.2.6 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in alleythemes Home Services allows DOM-Based XSS. This issue affects Home Services: from n/a through 1.2.6.	Patched by core rule	Y
CVE-2025-26934	WordPress Glossy Blog theme <= 1.0.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in graphthemes Glossy Blog allows Stored XSS. This issue affects Glossy Blog: from n/a through 1.0.3.	Patched by core rule	Y
CVE-2025-26950	WordPress Nepali Date Converter plugin <= 2.0.8 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AddonsPress Nepali Date Converter allows Stored XSS. This issue affects Nepali Date Converter: from n/a through 2.0.8.	Patched by core rule	Y
CVE-2025-26951	WordPress C9 Blocks plugin <= 1.7.7 - Cross	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Site Scripting (XSS) vulnerability	Generation ('Cross-site Scripting') vulnerability in covertnine C9 Blocks allows DOM-Based XSS. This issue affects C9 Blocks: from n/a through 1.7.7.		
CVE-2025-26954	WordPress ZooEffect plugin <= 1.11 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 1pluginjquery ZooEffect allows Reflected XSS. This issue affects ZooEffect: from n/a through 1.11.	Patched by core rule	Y
CVE-2025-26982	WordPress DSGVO Youtube plugin <= 1.5.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Eric-Oliver Mächler DSGVO Youtube allows DOM-Based XSS. This issue affects DSGVO Youtube: from n/a through 1.5.1.	Patched by core rule	Y
CVE-2025-26992	WordPress Landing Page Cat plugin <= 1.7.8 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fatcatapps Landing Page Cat allows Reflected XSS. This issue affects Landing Page Cat: from n/a through 1.7.8.	Patched by core rule	Y
CVE-2025-26998	WordPress SKT Blocks – Gutenberg based Page Builder plugin <= 1.8 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sonalsinha21 SKT Blocks – Gutenberg based Page Builder allows Stored XSS. This issue affects SKT Blocks – Gutenberg based Page Builder: from n/a through 1.8.	Patched by core rule	Y
CVE-2025-27014	WordPress Hostiko Theme < 30.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in designingmedia Hostiko allows Reflected XSS.This issue affects Hostiko: from n/a before 30.1.	Patched by core rule	Y
CVE-2025-27267	WordPress Random Quotes Plugin <= 1.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in srcoley Random Quotes allows Reflected XSS. This issue affects Random Quotes: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-27284	WordPress Flagged Content Plugin <= 1.0.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in divspark Flagged Content	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		allows Reflected XSS. This issue affects Flagged Content: from n/a through 1.0.2.		
CVE-2025-27285	WordPress Easy Form by AYS Plugin <= 2.6.9 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ays Pro Easy Form by AYS allows Reflected XSS. This issue affects Easy Form by AYS: from n/a through 2.6.9.	Patched by core rule	Y
CVE-2025-27288	WordPress File Icons Plugin <= 2.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BjornW File Icons allows Reflected XSS. This issue affects File Icons: from n/a through 2.1.	Patched by core rule	Y
CVE-2025-27289	WordPress Restrict Taxonomies Plugin <= 1.3.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Antoine Guillien Restrict Taxonomies allows Reflected XSS. This issue affects Restrict Taxonomies: from n/a through 1.3.3.	Patched by core rule	Y
CVE-2025-27291	WordPress Photo Gallery – Image Gallery Plugin <= 2.0.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in uxgallery WordPress Photo Gallery – Image Gallery allows Reflected XSS. This issue affects WordPress Photo Gallery – Image Gallery: from n/a through 2.0.4.	Patched by core rule	Y
CVE-2025-27292	WordPress WPYog Documents Plugin <= 1.3.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPyog WPYog Documents allows Reflected XSS. This issue affects WPYog Documents: from n/a through 1.3.3.	Patched by core rule	Y
CVE-2025-27293	WordPress Shipmozo Courier Tracking plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webparexapp Shipmozo Courier Tracking allows Reflected XSS. This issue affects Shipmozo Courier Tracking: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-27295	WordPress Live css plugin <= 1.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpion Live css allows Stored	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		XSS. This issue affects Live css: from n/a through 1.3.		
CVE-2025-27308	WordPress WP Video Posts plugin <= 3.5.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cmstactics WP Video Posts allows Reflected XSS. This issue affects WP Video Posts: from n/a through 3.5.1.	Patched by core rule	Y
CVE-2025-27309	WordPress flickr-slideshow-wrapper Plugin <= 5.4.6 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeannot Muller flickr-slideshow-wrapper allows Stored XSS. This issue affects flickr-slideshow-wrapper: from n/a through 5.4.6.	Patched by core rule	Y
CVE-2025-27313	WordPress Google Maps GPX Viewer Plugin <= 3.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bernd Altmeier Google Maps GPX Viewer allows Reflected XSS. This issue affects Google Maps GPX Viewer: from n/a through 3.6.	Patched by core rule	Y
CVE-2025-27314	WordPress Kush Micro News Plugin <= 1.6.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kush Sharma Kush Micro News allows Stored XSS. This issue affects Kush Micro News: from n/a through 1.6.7.	Patched by core rule	Y
CVE-2025-27319	WordPress User List plugin <= 1.5.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ivan82 User List allows Reflected XSS. This issue affects User List: from n/a through 1.5.1.	Patched by core rule	Y
CVE-2025-27322	WordPress QR Code for WooCommerce Plugin <= 1.2.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bappa Mal QR Code for WooCommerce allows Reflected XSS. This issue affects QR Code for WooCommerce: from n/a through 1.2.0.	Patched by core rule	Y
CVE-2025-27324	WordPress 17TRACK for WooCommerce Plugin <= 1.2.10 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 17track 17TRACK for WooCommerce allows Reflected XSS. This issue affects 17TRACK for	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		WooCommerce: from n/a through 1.2.10.		
CVE-2025-27333	WordPress Protected wp-login Plugin <= 2.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in alvego Protected wp-login allows Reflected XSS. This issue affects Protected wp-login: from n/a through 2.1.	Patched by core rule	Y
CVE-2025-27337	WordPress Fontsampler Plugin <= 0.4.14 - CSRF to Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kontur Fontsampler allows Reflected XSS. This issue affects Fontsampler: from n/a through 0.4.14.	Patched by core rule	Y
CVE-2025-27338	WordPress List Urls Plugin <= 0.2 - CSRF to Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in graphems List Urls allows Reflected XSS. This issue affects List Urls: from n/a through 0.2.	Patched by core rule	Y
CVE-2025-27343	WordPress WooCommerce HTML5 Video Plugin <= 1.7.10 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Webilop WooCommerce HTML5 Video allows Reflected XSS. This issue affects WooCommerce HTML5 Video: from n/a through 1.7.10.	Patched by core rule	Y
CVE-2025-27345	WordPress Booking Ultra Pro Plugin <= 1.1.19 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Deetronix Booking Ultra Pro allows Reflected XSS. This issue affects Booking Ultra Pro: from n/a through 1.1.19.	Patched by core rule	Y
CVE-2025-27346	WordPress Rebuild Permalinks Plugin <= 1.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gerrygooner Rebuild Permalinks allows Reflected XSS. This issue affects Rebuild Permalinks: from n/a through 1.6.	Patched by core rule	Y
CVE-2025-27350	WordPress Vice Versa plugin <= 2.2.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hugh Mungus Vice Versa allows Reflected XSS.This issue affects Vice Versa: from n/a through 2.2.3.	Patched by core rule	Y
CVE-2025-27354	WordPress Simple Email	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Subscriber plugin <= 2.3 - Reflected Cross Site Scripting (XSS) vulnerability	Input During Web Page Generation ('Cross-site Scripting') vulnerability in phil88530 Simple Email Subscriber allows Reflected XSS. This issue affects Simple Email Subscriber: from n/a through 2.3.	rule	
CVE-2025-27608	Self Cross-Site Scripting in Arduino IDE	Arduino IDE 2.x is an IDE based on the Theia IDE framework and built with Electron. A Self Cross-Site Scripting (XSS) vulnerability has been identified within the Arduino-IDE prior to version v2.3.5. The vulnerability occurs in the Additional Board Manager URLs field, which can be found in the Preferences -> Settings section of the Arduino IDE interface. In the vulnerable versions, any values entered in this field are directly displayed to the user through a notification tooltip object, without a proper output encoding routine, due to the underlying ElectronJS engine interpretation. This vulnerability exposes the input parameter to Self-XSS attacks, which may lead to security risks depending on where the malicious payload is injected. This vulnerability is fixed in 2.3.5.	Patched by core rule	Y
CVE-2025-28855	WordPress Teleport plugin <= 1.2.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Teleport allows Reflected XSS. This issue affects Teleport: from n/a through 1.2.4.	Patched by core rule	Y
CVE-2025-28858	WordPress Arrow Maps plugin <= 1.0.9 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Arrow Plugins Arrow Maps allows Reflected XSS. This issue affects Arrow Maps: from n/a through 1.0.9.	Patched by core rule	Y
CVE-2025-28865	WordPress WP Colorful Tag Cloud plugin <= 2.0.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in lionelroux WP Colorful Tag Cloud allows Reflected XSS. This issue affects WP Colorful Tag Cloud: from n/a through 2.0.1.	Patched by core rule	Y
CVE-2025-28869	WordPress NextGEN Gallery Voting plugin <=	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	2.7.6 - Reflected Cross Site Scripting (XSS) vulnerability	Generation ('Cross-site Scripting') vulnerability in NotFound NextGEN Gallery Voting allows Reflected XSS. This issue affects NextGEN Gallery Voting: from n/a through 2.7.6.		
CVE-2025-28877	WordPress Key4ce osTicket Bridge plugin <= 1.4.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Key4ce osTicket Bridge allows Reflected XSS. This issue affects Key4ce osTicket Bridge: from n/a through 1.4.0.	Patched by core rule	Y
CVE-2025-28880	WordPress Blue Captcha plugin <= 1.7.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Blue Captcha allows Reflected XSS. This issue affects Blue Captcha: from n/a through 1.7.4.	Patched by core rule	Y
CVE-2025-28882	WordPress Omnify plugin <= 2.0.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Omnify, Inc. Omnify allows Reflected XSS. This issue affects Omnify: from n/a through 2.0.3.	Patched by core rule	Y
CVE-2025-28885	WordPress Fiverr.com Official Search Box plugin <= 1.0.8 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Fiverr.com Official Search Box allows Stored XSS. This issue affects Fiverr.com Official Search Box: from n/a through 1.0.8.	Patched by core rule	Y
CVE-2025-28889	WordPress Custom Product Stickers for Woocommerce plugin <= 1.9.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Custom Product Stickers for Woocommerce allows Reflected XSS. This issue affects Custom Product Stickers for Woocommerce: from n/a through 1.9.0.	Patched by core rule	Y
CVE-2025-28890	WordPress Lightview Plus plugin <= 3.1.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Lightview Plus allows Reflected XSS. This issue affects Lightview Plus: from n/a through 3.1.3.	Patched by core rule	Y
CVE-2025-28899	WordPress WP Event Ticketing plugin <= 1.3.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WP Event	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Ticketing allows Reflected XSS. This issue affects WP Event Ticketing: from n/a through 1.3.4.		
CVE-2025-28903	WordPress Driving Directions plugin <= 1.4.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Driving Directions allows Reflected XSS. This issue affects Driving Directions: from n/a through 1.4.4.	Patched by core rule	Y
CVE-2025-28911	WordPress Gravity 2 PDF plugin <= 3.1.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gravity2pdf Gravity 2 PDF allows Reflected XSS. This issue affects Gravity 2 PDF: from n/a through 3.1.3.	Patched by core rule	Y
CVE-2025-28917	WordPress Custom Smilies plugin <= 2.9.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Custom Smilies allows Stored XSS. This issue affects Custom Smilies: from n/a through 2.9.2.	Patched by core rule	Y
CVE-2025-28921	WordPress SpatialMatch IDX plugin <= 3.0.9 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound SpatialMatch IDX allows Reflected XSS. This issue affects SpatialMatch IDX: from n/a through 3.0.9.	Patched by core rule	Y
CVE-2025-28924	WordPress ZenphotoPress plugin <= 1.8 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound ZenphotoPress allows Reflected XSS. This issue affects ZenphotoPress: from n/a through 1.8.	Patched by core rule	Y
CVE-2025-28928	WordPress Are you robot google recaptcha for Wordpress plugin <= 2.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sureshdsk Are you robot google recaptcha for wordpress allows Reflected XSS. This issue affects Are you robot google recaptcha for wordpress: from n/a through 2.2.	Patched by core rule	Y
CVE-2025-28934	WordPress Simple Post Series plugin <= 2.4.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Simple Post Series allows Reflected XSS. This issue affects Simple Post Series: from n/a through	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		2.4.4.		
CVE-2025-28935	WordPress Fancybox Plus plugin <= 1.0.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in puzich Fancybox Plus allows Reflected XSS. This issue affects Fancybox Plus: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-2963	ConcreteCMS Legacy Form Block addEditQuestion cross site scripting	A vulnerability, which was classified as problematic, has been found in ConcreteCMS up to 9.3.9. This issue affects the function addEditQuestion of the component Legacy Form Block Handler. The manipulation of the argument Question leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2964	ConcreteCMS FAQ Block save cross site scripting	A vulnerability, which was classified as problematic, was found in ConcreteCMS up to 9.3.9. Affected is the function Save of the component FAQ Block Handler. The manipulation of the argument Navigation/Title Text/Description Source leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2965	ConcreteCMS Accordion Block save cross site scripting	A vulnerability has been found in ConcreteCMS up to 9.3.9 and classified as problematic. Affected by this vulnerability is the function Save of the component Accordion Block Handler. The manipulation of the argument Title/Body Source leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2966	ConcreteCMS Content Block save cross site	A vulnerability was found in ConcreteCMS up to 9.3.9	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	scripting	and classified as problematic. Affected by this issue is the function Save of the component Content Block Handler. The manipulation of the argument Source leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-2968	ConcreteCMS Feature Block save cross site scripting	A vulnerability was found in ConcreteCMS up to 9.3.9. It has been declared as problematic. This vulnerability affects the function Save of the component Feature Block Handler. The manipulation of the argument Paragraph Source leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2969	ConcreteCMS Feature Link Block save cross site scripting	A vulnerability was found in ConcreteCMS up to 9.3.9. It has been rated as problematic. This issue affects the function Save of the component Feature Link Block Handler. The manipulation of the argument Title/Body Source/Button Text leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2970	ConcreteCMS Switch Language Block cross site scripting	A vulnerability classified as problematic has been found in ConcreteCMS up to 9.3.9. Affected is an unknown function of the component Switch Language Block Handler. The manipulation of the argument Label leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		not respond in any way.		
CVE-2025-2971	ConcreteCMS List Block cross site scripting	A vulnerability classified as problematic was found in ConcreteCMS up to 9.3.9. Affected by this vulnerability is an unknown functionality of the component List Block Handler. The manipulation of the argument Name/Description leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2972	ConcreteCMS Page Attribute Display Block cross site scripting	A vulnerability, which was classified as problematic, has been found in ConcreteCMS up to 9.3.9. Affected by this issue is some unknown functionality of the component Page Attribute Display Block Handler. The manipulation of the argument Title leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2975	GFI KerioConnect Signature EditHtmlSource cross site scripting	A vulnerability was found in GFI KerioConnect 10.0.6 and classified as problematic. This issue affects some unknown processing of the file Settings/Email/Signature/EditHtmlSource of the component Signature Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2976	GFI KerioConnect File Upload cross site scripting	A vulnerability was found in GFI KerioConnect 10.0.6. It has been classified as problematic. Affected is an unknown function of the component File Upload. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-2977	GFI KerioConnect PDF File cross site scripting	A vulnerability was found in GFI KerioConnect 10.0.6. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component PDF File Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-29772	OpenEMR allows Reflected XSS in CAMOS new.php	OpenEMR is a free and open source electronic health records and medical practice management application. The POST parameter hidden_subcategory is output to the page without being properly processed. This leads to a reflected cross-site scripting (XSS) vul;nerability in CAMOS new.php. This vulnerability is fixed in 7.0.3.	Patched by core rule	Y
CVE-2025-2979	WCMS Registration setregister cross site scripting	A vulnerability classified as problematic has been found in WCMS 11. This affects an unknown part of the file /index.php?anonymous/setregister of the component Registration. The manipulation of the argument Username leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-3004	Sayski ForestBlog search cross site scripting	A vulnerability has been found in Sayski ForestBlog up to 20250321 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /search. The manipulation of the argument keywords leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3005	Sayski ForestBlog Friend	A vulnerability was found in	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Link cross site scripting	Sayski ForestBlog up to 20250321 and classified as problematic. Affected by this issue is some unknown functionality of the component Friend Link Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	rule	
CVE-2025-30149	OpenEMR Reflected XSS in AJAX Script	OpenEMR is a free and open source electronic health records and medical practice management application. OpenEMR allows reflected cross-site scripting (XSS) in the AJAX Script interface\super\layout_listitems_ajax.php via the target parameter. This vulnerability is fixed in 7.0.3.	Patched by core rule	Y
CVE-2025-30161	OpenEMR Stored XSS in OpenEMR Bronchitis Form	OpenEMR is a free and open source electronic health records and medical practice management application. A stored XSS vulnerability in the Bronchitis form component of OpenEMR allows anyone who is able to edit a bronchitis form to steal credentials from administrators. This vulnerability is fixed in 7.0.3.	Patched by core rule	Y
CVE-2025-30203	Tuleap allows XSS via the content of RSS feeds in the RSS widgets	Tuleap is an Open Source Suite to improve management of software developments and collaboration. Tuleap allows cross-site scripting (XSS) via the content of RSS feeds in the RSS widgets. A project administrator or someone with control over an used RSS feed could use this vulnerability to force victims to execute uncontrolled code. This vulnerability is fixed in Tuleap Community Edition 16.5.99.1742562878 and Tuleap Enterprise Edition 16.5-5 and 16.4-8.	Patched by core rule	Y
CVE-2025-30210	Bruno XSS On Environment Name	Bruno is an open source IDE for exploring and testing APIs. Prior to 1.39.1, the custom tool-tip components which internally use react-tooltip were setting the content (in this case the Environment name) as raw HTML which then gets injected into DOM on hover. This, combined with loose Content Security Policy	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		restrictions, allowed any valid HTML text containing inline script to get executed on hovering over the respective Environment's name. This vulnerability's attack surface is limited strictly to scenarios where users import collections from untrusted or malicious sources. The exploit requires deliberate action from the user—specifically, downloading and opening an externally provided malicious Bruno or Postman collection export and the user hovers on the environment name. This vulnerability is fixed in 1.39.1.		
CVE-2025-30223	Beego allows Reflected/Stored XSS in Beego's RenderForm() Function Due to Unescaped User Input	Beego is an open-source web framework for the Go programming language. Prior to 2.3.6, a Cross-Site Scripting (XSS) vulnerability exists in Beego's RenderForm() function due to improper HTML escaping of user-controlled data. This vulnerability allows attackers to inject malicious JavaScript code that executes in victims' browsers, potentially leading to session hijacking, credential theft, or account takeover. The vulnerability affects any application using Beego's RenderForm() function with user-provided data. Since it is a high-level function generating an entire form markup, many developers would assume it automatically escapes attributes (the way most frameworks do). This vulnerability is fixed in 2.3.6.	Patched by core rule	Y
CVE-2025-3036	yzk2356911358 StudentServlet-JSP Student Management cross site scripting	A vulnerability, which was classified as problematic, was found in yzk2356911358 StudentServlet-JSP cc0cdce25fbe43b6c58b60a77a2c85f52d2102f5/d4d7a0643f1dae908a4831206f2714b21820f991. This affects an unknown part of the component Student Management Handler. The manipulation of the argument Name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available.		
CVE-2025-30362	WeGIA vulnerable to Stored XSS in documentos_funcionario.php parameter id	WeGIA is a Web manager for charitable institutions. A stored Cross-Site Scripting (XSS) vulnerability was identified in versions prior to 3.2.8. This vulnerability allows unauthorized scripts to be executed within the user's browser context. Stored XSS is particularly critical, as the malicious code is permanently stored on the server and executed whenever a compromised page is loaded, affecting all users accessing this page. Version 3.2.8 fixes the issue.	Patched by core rule	Y
CVE-2025-30363	WeGIA vulnerable to Stored XSS in documentos_funcionario.php parameter dados_addInfo	WeGIA is a Web manager for charitable institutions. A stored Cross-Site Scripting (XSS) vulnerability was identified in versions prior to 3.2.6. This vulnerability allows unauthorized scripts to be executed within the user's browser context. Stored XSS is particularly critical, as the malicious code is permanently stored on the server and executed whenever a compromised page is loaded, affecting all users accessing this page. Version 3.2.6 fixes the issue.	Patched by core rule	Y
CVE-2025-30366	WeGIA vulnerable to Stored XSS in personalizacao.php	WeGIA is a Web manager for charitable institutions. Versions prior to 3.2.8 are vulnerable to stored cross-site scripting. This vulnerability allows unauthorized scripts to be executed within the user's browser context. Stored XSS is particularly critical, as the malicious code is permanently stored on the server and executed whenever a compromised page is loaded, affecting all users accessing this page. Version 3.2.8 fixes the issue.	Patched by core rule	Y
CVE-2025-30544	WordPress OK Poster Group plugin <= 1.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound OK Poster Group allows Reflected XSS. This issue affects OK Poster	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Group: from n/a through 1.1.		
CVE-2025-30547	WordPress WP Cards plugin <= 1.5.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in David Tufts WP Cards allows Reflected XSS. This issue affects WP Cards: from n/a through 1.5.1.	Patched by core rule	Y
CVE-2025-30548	WordPress Advanced Post Search plugin <= 1.1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VarDump s.r.l. Advanced Post Search allows Reflected XSS. This issue affects Advanced Post Search: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-30554	WordPress Frizzly plugin <= 1.1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Frizzly allows Reflected XSS. This issue affects Frizzly: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-30559	WordPress Kento WordPress Stats plugin <= 1.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Kento WordPress Stats allows Stored XSS. This issue affects Kento WordPress Stats: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-30563	WordPress Tidekey plugin <= 1.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Tidekey allows Reflected XSS. This issue affects Tidekey: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-30579	WordPress Pesapal Gateway for Woocommerce plugin <= 2.1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jakeii Pesapal Gateway for Woocommerce allows Reflected XSS. This issue affects Pesapal Gateway for Woocommerce: from n/a through 2.1.0.	Patched by core rule	Y
CVE-2025-30607	WordPress Quick Localization plugin <= 0.1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Name.ly Quick Localization allows Reflected XSS. This issue affects Quick Localization: from n/a through 0.1.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-30611	WordPress Wptobe-signinup plugin <= 1.1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Wptobe-signinup allows Reflected XSS. This issue affects Wptobe-signinup: from n/a through 1.1.2.	Patched by core rule	Y
CVE-2025-30613	WordPress Nmedia MailChimp plugin <= 5.4 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in N-Media Nmedia MailChimp allows Stored XSS. This issue affects Nmedia MailChimp: from n/a through 5.4.	Patched by core rule	Y
CVE-2025-30614	WordPress Google Font Fix plugin <= 2.3.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Haozhe Xie Google Font Fix allows Reflected XSS. This issue affects Google Font Fix: from n/a through 2.3.1.	Patched by core rule	Y
CVE-2025-30616	WordPress Latest Custom Post Type Updates plugin <= 1.3.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Latest Custom Post Type Updates allows Reflected XSS. This issue affects Latest Custom Post Type Updates: from n/a through 1.3.0.	Patched by core rule	Y
CVE-2025-30763	WordPress EO4WP <= 1.0.8.4 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Olaf Lederer EO4WP allows Stored XSS. This issue affects EO4WP: from n/a through 1.0.8.4.	Patched by core rule	Y
CVE-2025-30766	WordPress Happy Addons for Elementor <= 3.16.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HappyMonster Happy Addons for Elementor allows DOM-Based XSS. This issue affects Happy Addons for Elementor: from n/a through 3.16.2.	Patched by core rule	Y
CVE-2025-30768	WordPress jAlbum Bridge <= 2.0.18 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mlaza jAlbum Bridge allows Stored XSS. This issue affects jAlbum Bridge: from n/a through 2.0.18.	Patched by core rule	Y
CVE-2025-30770	WordPress Charitable <= 1.8.4.7 - Cross Site	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Scripting (XSS) Vulnerability	Generation ('Cross-site Scripting') vulnerability in Syed Balkhi Charitable allows DOM-Based XSS. This issue affects Charitable: from n/a through 1.8.4.7.		
CVE-2025-30771	WordPress WP Cassify <= 2.3.5 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alain-Aymerick FRANCOIS WP Cassify allows DOM-Based XSS. This issue affects WP Cassify: from n/a through 2.3.5.	Patched by core rule	Y
CVE-2025-30776	WordPress Sitekit <= 1.8 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webvitaly Sitekit allows Stored XSS. This issue affects Sitekit: from n/a through 1.8.	Patched by core rule	Y
CVE-2025-30778	WordPress VForm plugin <= 3.1.9 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vikas Ratudi VForm allows Reflected XSS. This issue affects VForm: from n/a through 3.1.9.	Patched by core rule	Y
CVE-2025-30779	WordPress Doneren met Mollie <= 2.10.7 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nick Doneren met Mollie allows Stored XSS. This issue affects Doneren met Mollie: from n/a through 2.10.7.	Patched by core rule	Y
CVE-2025-30780	WordPress Audio Album <= 1.5.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cubecolour Audio Album allows Stored XSS. This issue affects Audio Album: from n/a through 1.5.0.	Patched by core rule	Y
CVE-2025-30786	WordPress Quotes llama <= 3.1.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in oooorgle Quotes llama allows DOM-Based XSS. This issue affects Quotes llama: from n/a through 3.1.0.	Patched by core rule	Y
CVE-2025-30789	WordPress Clearout Email Validator <= 3.2.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in clearoutio Clearout Email Validator allows Stored XSS. This issue affects Clearout Email Validator: from n/a through 3.2.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-30792	WordPress Comment Approved Notifier Extended plugin <= 5.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zumbo Comment Approved Notifier Extended allows Stored XSS. This issue affects Comment Approved Notifier Extended: from n/a through 5.2.	Patched by core rule	Y
CVE-2025-30794	WordPress Event Tickets plugin <= 5.20.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in The Events Calendar Event Tickets allows Reflected XSS. This issue affects Event Tickets: from n/a through 5.20.0.	Patched by core rule	Y
CVE-2025-30796	WordPress The Ultimate WordPress Toolkit – WP Extended plugin <= 3.0.14 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Extended The Ultimate WordPress Toolkit – WP Extended allows Reflected XSS. This issue affects The Ultimate WordPress Toolkit – WP Extended: from n/a through 3.0.14.	Patched by core rule	Y
CVE-2025-30798	WordPress Better WishList API plugin <= 1.1.4 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rickonline_nl Better WishList API allows Reflected XSS. This issue affects Better WishList API: from n/a through 1.1.4.	Patched by core rule	Y
CVE-2025-30799	WordPress WP Google Street View plugin <= 1.1.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pagup WP Google Street View allows Stored XSS. This issue affects WP Google Street View: from n/a through 1.1.5.	Patched by core rule	Y
CVE-2025-30800	WordPress Gum Elementor Addon plugin <= 1.3.10 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Atawai Gum Elementor Addon allows Stored XSS. This issue affects Gum Elementor Addon: from n/a through 1.3.10.	Patched by core rule	Y
CVE-2025-30808	WordPress About Author plugin <= 1.6.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in weblizar About Author allows Reflected XSS. This issue affects About Author:	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		from n/a through 1.6.2.		
CVE-2025-30812	WordPress SKT Addons for Elementor plugin <= 3.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sonalsinha21 SKT Addons for Elementor allows Stored XSS. This issue affects SKT Addons for Elementor: from n/a through 3.5.	Patched by core rule	Y
CVE-2025-30813	WordPress Listamester plugin <= 2.3.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in listamester Listamester allows Stored XSS. This issue affects Listamester: from n/a through 2.3.5.	Patched by core rule	Y
CVE-2025-30818	WordPress jAlbum Bridge plugin <= 2.0.17 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mlaza jAlbum Bridge allows DOM-Based XSS. This issue affects jAlbum Bridge: from n/a through 2.0.17.	Patched by core rule	Y
CVE-2025-30826	WordPress IP Locator plugin <= 4.1.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pierre Lannoy IP Locator allows DOM-Based XSS. This issue affects IP Locator: from n/a through 4.1.0.	Patched by core rule	Y
CVE-2025-30827	WordPress WP2LEADS plugin <= 3.4.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Saleswonder Team Tobias WP2LEADS allows Reflected XSS. This issue affects WP2LEADS: from n/a through 3.4.5.	Patched by core rule	Y
CVE-2025-30832	WordPress Themify Event Post Plugin <= 1.3.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themifyme Themify Event Post allows DOM-Based XSS. This issue affects Themify Event Post: from n/a through 1.3.2.	Patched by core rule	Y
CVE-2025-30836	WordPress LatePoint plugin <= 5.1.6 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LatePoint LatePoint allows Stored XSS. This issue affects LatePoint: from n/a through 5.1.6.	Patched by core rule	Y
CVE-2025-30837	WordPress WooCommerce	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Fattureincloud plugin <= 2.6.7 - Cross Site Scripting (XSS) vulnerability	Generation ('Cross-site Scripting') vulnerability in Cristiano Zanca WooCommerce Fattureincloud allows Reflected XSS. This issue affects WooCommerce Fattureincloud: from n/a through 2.6.7.		
CVE-2025-30838	WordPress Cozy Blocks plugin <= 2.1.6 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CozyThemes Cozy Blocks allows Stored XSS. This issue affects Cozy Blocks: from n/a through 2.1.6.	Patched by core rule	Y
CVE-2025-30840	WordPress xili-dictionary plugin <= 2.12.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michel - xiligroup dev xili-dictionary allows Reflected XSS. This issue affects xili-dictionary: from n/a through 2.12.5.	Patched by core rule	Y
CVE-2025-30844	WordPress Watu Quiz plugin <= 3.4.2 - Reflected Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bob Watu Quiz allows Reflected XSS. This issue affects Watu Quiz: from n/a through 3.4.2.	Patched by core rule	Y
CVE-2025-30847	WordPress Novelist plugin <= 1.2.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ashley Novelist allows Stored XSS. This issue affects Novelist: from n/a through 1.2.3.	Patched by core rule	Y
CVE-2025-30848	WordPress Hostel plugin <= 1.1.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bob Hostel allows Reflected XSS. This issue affects Hostel: from n/a through 1.1.5.	Patched by core rule	Y
CVE-2025-30850	WordPress Dr. Flex plugin <= 2.0.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sfaerber Dr. Flex allows Stored XSS. This issue affects Dr. Flex: from n/a through 2.0.0.	Patched by core rule	Y
CVE-2025-30852	WordPress Oracle Cards Lite plugin <= 1.2.1 - Reflected Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in emotionalonlinestorytelling Oracle Cards Lite allows	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Reflected XSS. This issue affects Oracle Cards Lite: from n/a through 1.2.1.		
CVE-2025-30858	WordPress Snow Storm plugin <= 1.4.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tribulant Software Snow Storm allows Reflected XSS. This issue affects Snow Storm: from n/a through 1.4.6.	Patched by core rule	Y
CVE-2025-30860	WordPress Off-Canvas Sidebars & Menus (Slidebars) plugin <= 0.5.8.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jory Hogeveen Off-Canvas Sidebars & Menus (Slidebars) allows DOM-Based XSS. This issue affects Off-Canvas Sidebars & Menus (Slidebars): from n/a through 0.5.8.2.	Patched by core rule	Y
CVE-2025-30867	WordPress SearchIQ plugin <= 4.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SearchIQ SearchIQ allows Stored XSS. This issue affects SearchIQ: from n/a through 4.7.	Patched by core rule	Y
CVE-2025-30869	WordPress Image Wall plugin <= 3.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Parakoos Image Wall allows Reflected XSS. This issue affects Image Wall: from n/a through 3.0.	Patched by core rule	Y
CVE-2025-30873	WordPress Greenshift plugin <= 11.0.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpsoul Greenshift allows Stored XSS. This issue affects Greenshift: from n/a through 11.0.2.	Patched by core rule	Y
CVE-2025-30893	WordPress LeadConnector plugin <= 3.0.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LeadConnector LeadConnector allows DOM-Based XSS. This issue affects LeadConnector: from n/a through 3.0.2.	Patched by core rule	Y
CVE-2025-30898	WordPress افزونه حمل و نقل ووکامرس)پست پیشتاز و سفارشی، پیک موتوری) plugin <= 4.2.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mahdi Yousefi [MahdiY] افزونه حمل و نقل ووکامرس)پست پیشتاز و سفارشی، پیک موتوری) allows Stored XSS. This issue	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		افزونه حمل و نقل affects ووکامرس)پست پیشتاز و سفارشی، پیک موتوری): from n/a through 4.2.3.		
CVE-2025-30899	WordPress User Registration plugin <= 4.0.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpeverest User Registration allows Stored XSS. This issue affects User Registration: from n/a through 4.0.3.	Patched by core rule	Y
CVE-2025-30900	WordPress Zoho Billing – Embed Payment Form plugin <= 4.0 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zoho Subscriptions Zoho Billing – Embed Payment Form allows Stored XSS. This issue affects Zoho Billing – Embed Payment Form: from n/a through 4.0.	Patched by core rule	Y
CVE-2025-30902	WordPress AEC Kiosque plugin <= 1.9.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ATL Software SRL AEC Kiosque allows Reflected XSS. This issue affects AEC Kiosque: from n/a through 1.9.3.	Patched by core rule	Y
CVE-2025-30903	WordPress SyntaxHighlighter Evolved plugin <= 3.7.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alex Mills SyntaxHighlighter Evolved allows DOM-Based XSS. This issue affects SyntaxHighlighter Evolved: from n/a through 3.7.1.	Patched by core rule	Y
CVE-2025-30904	WordPress Chartify plugin <= 3.1.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ays Pro Chartify allows Stored XSS. This issue affects Chartify: from n/a through 3.1.7.	Patched by core rule	Y
CVE-2025-30905	WordPress Secure Copy Content Protection and Content Locking plugin <= 4.4.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ays Pro Secure Copy Content Protection and Content Locking allows Stored XSS. This issue affects Secure Copy Content Protection and Content Locking: from n/a through 4.4.3.	Patched by core rule	Y
CVE-2025-30906	WordPress Plugin Oficial – Getnet para WooCommerce plugin <= 1.7.3 - Reflected Cross Site Scripting (XSS)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Coffee Code Tech Plugin	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	vulnerability	Oficial – Getnet para WooCommerce allows Reflected XSS. This issue affects Plugin Oficial – Getnet para WooCommerce: from n/a through 1.7.3.		
CVE-2025-30907	WordPress SecuPress Free plugin <= 2.2.5.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SecuPress SecuPress Free allows DOM-Based XSS. This issue affects SecuPress Free: from n/a through 2.2.5.3.	Patched by core rule	Y
CVE-2025-30913	WordPress Access Areas Plugin <= 1.5.19 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in podpirate Access Areas allows Reflected XSS. This issue affects Access Areas: from n/a through 1.5.19.	Patched by core rule	Y
CVE-2025-30917	WordPress SKU Generator for WooCommerce plugin <= 1.6.2 - Reflected Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Wham SKU Generator for WooCommerce allows Reflected XSS. This issue affects SKU Generator for WooCommerce: from n/a through 1.6.2.	Patched by core rule	Y
CVE-2025-30918	WordPress Structured Content plugin 1.6.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in codemacher Structured Content allows Stored XSS. This issue affects Structured Content: from n/a through 1.6.3.	Patched by core rule	Y
CVE-2025-30920	WordPress WP Posts Carousel plugin <= 1.3.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in teastudio.pl WP Posts Carousel allows Stored XSS. This issue affects WP Posts Carousel: from n/a through 1.3.7.	Patched by core rule	Y
CVE-2025-30922	WordPress Simplebooklet PDF Viewer and Embedder plugin <= 1.1.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in simplebooklet Simplebooklet PDF Viewer and Embedder allows Stored XSS. This issue affects Simplebooklet PDF Viewer and Embedder: from n/a through 1.1.1.	Patched by core rule	Y
CVE-2025-30924	WordPress Primer MyData for Woocommerce plugin <	Improper Neutralization of Input During Web Page Generation ('Cross-site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	4.2.4 - Reflected Cross Site Scripting (XSS) vulnerability	Scripting') vulnerability in primersoftware Primer MyData for Woocommerce allows Reflected XSS. This issue affects Primer MyData for Woocommerce: from n/a through n/a.		
CVE-2025-30925	WordPress The Pack Elementor addons plugin <= 2.1.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webangon The Pack Elementor addons allows Stored XSS. This issue affects The Pack Elementor addons: from n/a through 2.1.1.	Patched by core rule	Y
CVE-2025-30961	WordPress Trackserver plugin <= 5.0.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tinuzz Trackserver allows DOM-Based XSS.This issue affects Trackserver: from n/a through 5.0.3.	Patched by core rule	Y
CVE-2025-30962	WordPress FS Poster plugin <= 6.5.8 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound FS Poster allows Reflected XSS. This issue affects FS Poster: from n/a through 6.5.8.	Patched by core rule	Y
CVE-2025-30963	WordPress JetSmartFilters plugin <= 3.6.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetSmartFilters allows DOM-Based XSS.This issue affects JetSmartFilters: from n/a through 3.6.3.	Patched by core rule	Y
CVE-2025-30970	WordPress Easy Contact plugin <= 0.1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Easy Contact allows Reflected XSS. This issue affects Easy Contact: from n/a through 0.1.2.	Patched by core rule	Y
CVE-2025-3098	Video Url <= 1.0.0.3 - Reflected Cross-Site Scripting	The Video Url plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'id' parameter in all versions up to, and including, 1.0.0.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-30982	WordPress MyBookProgress by Stormhill Media plugin <= 1.0.8 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in zookatron MyBookProgress by Stormhill Media allows Stored XSS. This issue affects MyBookProgress by Stormhill Media: from n/a through 1.0.8.	Patched by core rule	Y
CVE-2025-30984	WordPress SEO Tools plugin <= 4.0.7 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound SEO Tools allows Reflected XSS. This issue affects SEO Tools: from n/a through 4.0.7.	Patched by core rule	Y
CVE-2025-30987	WordPress JetBlocks For Elementor plugin <= 1.3.16 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound JetBlocks For Elementor allows Stored XSS. This issue affects JetBlocks For Elementor: from n/a through 1.3.16.	Patched by core rule	Y
CVE-2025-31006	WordPress Activity Reactions For Buddypress plugin <= 1.0.22 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in arete-it Activity Reactions For Buddypress allows Reflected XSS. This issue affects Activity Reactions For Buddypress: from n/a through 1.0.22.	Patched by core rule	Y
CVE-2025-31008	WordPress YouTube Embed <= 5.3.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in YouTube Embed Plugin Support YouTube Embed allows Stored XSS. This issue affects YouTube Embed: from n/a through 5.3.1.	Patched by core rule	Y
CVE-2025-31011	WordPress SimplyRETS Real Estate IDX plugin <= 3.0.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ReichertBrothers SimplyRETS Real Estate IDX allows Reflected XSS. This issue affects SimplyRETS Real Estate IDX: from n/a through 3.0.3.	Patched by core rule	Y
CVE-2025-31017	WordPress Nav Menu Manager <= 3.2.5 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Robert Noakes Nav Menu Manager allows Stored XSS. This issue affects Nav Menu Manager: from n/a through	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		3.2.5.		
CVE-2025-31018	WordPress FireDrum Email Marketing plugin <= 1.64 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FireDrum FireDrum Email Marketing allows Reflected XSS. This issue affects FireDrum Email Marketing: from n/a through 1.64.	Patched by core rule	Y
CVE-2025-31020	WordPress Simple Spoiler <= 1.4 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Webliberty Simple Spoiler allows Stored XSS. This issue affects Simple Spoiler: from n/a through 1.4.	Patched by core rule	Y
CVE-2025-31021	WordPress Mobile Smart plugin <= v1.3.16 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in dolby_uk Mobile Smart allows Reflected XSS. This issue affects Mobile Smart: from n/a through v1.3.16.	Patched by core rule	Y
CVE-2025-31028	WordPress WP Hide Categories <= 1.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WP Hide Categories allows Reflected XSS. This issue affects WP Hide Categories: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-31031	WordPress Job Colors for WP Job Manager plugin <= 1.0.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Astoundify Job Colors for WP Job Manager allows Stored XSS.This issue affects Job Colors for WP Job Manager: from n/a through 1.0.4.	Patched by core rule	Y
CVE-2025-31035	WordPress WP Editor.md – The Perfect WordPress Markdown Editor <= 10.2.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Benjamin Chris WP Editor.md – The Perfect WordPress Markdown Editor allows Stored XSS. This issue affects WP Editor.md – The Perfect WordPress Markdown Editor: from n/a through 10.2.1.	Patched by core rule	Y
CVE-2025-31043	WordPress JetSearch plugin <= 3.5.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound JetSearch allows DOM-Based XSS. This issue	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects JetSearch: from n/a through 3.5.7.		
CVE-2025-31073	WordPress Unlimited <= 1.45 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Compete Themes Unlimited allows Stored XSS. This issue affects Unlimited: from n/a through 1.45.	Patched by core rule	Y
CVE-2025-31075	WordPress MicroPayments plugin <= 2.9.29 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in videowhisper MicroPayments allows Stored XSS. This issue affects MicroPayments: from n/a through 2.9.29.	Patched by core rule	Y
CVE-2025-31077	WordPress Ultimate Blocks plugin <= 3.2.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ultimate Blocks Ultimate Blocks allows DOM-Based XSS. This issue affects Ultimate Blocks: from n/a through 3.2.7.	Patched by core rule	Y
CVE-2025-31078	WordPress Small Package Quotes – Worldwide Express Edition plugin <= 5.2.18 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in enituretechnology Small Package Quotes – Worldwide Express Edition allows Reflected XSS. This issue affects Small Package Quotes – Worldwide Express Edition: from n/a through 5.2.18.	Patched by core rule	Y
CVE-2025-31080	WordPress HTML Forms plugin <= 1.5.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Link Software LLC HTML Forms allows Stored XSS. This issue affects HTML Forms: from n/a through 1.5.1.	Patched by core rule	Y
CVE-2025-31081	WordPress Enable Media Replace plugin <= 4.1.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ShortPixel Enable Media Replace allows Reflected XSS. This issue affects Enable Media Replace: from n/a through 4.1.5.	Patched by core rule	Y
CVE-2025-31083	WordPress Leaky Paywall <= 4.21.7 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ZEEN101 Leaky Paywall allows Stored XSS. This issue affects Leaky Paywall: from	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		n/a through 4.21.7.		
CVE-2025-31085	WordPress xili-language plugin <= 2.21.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michel - xiligroup dev xili-language allows Reflected XSS. This issue affects xili-language: from n/a through 2.21.2.	Patched by core rule	Y
CVE-2025-31086	WordPress Product Table by WBW plugin <= 2.1.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nick McReynolds Product Table by WBW allows Reflected XSS. This issue affects Product Table by WBW: from n/a through 2.1.4.	Patched by core rule	Y
CVE-2025-31088	WordPress Paid Member Subscriptions <= 2.14.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Cozmoslabs Paid Member Subscriptions allows Stored XSS. This issue affects Paid Member Subscriptions: from n/a through 2.14.3.	Patched by core rule	Y
CVE-2025-31090	WordPress Dropdown Multisite selector < 0.9.4 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in alordiel Dropdown Multisite selector allows Stored XSS. This issue affects Dropdown Multisite selector: from n/a through n/a.	Patched by core rule	Y
CVE-2025-31091	WordPress CM Header and Footer <= 1.2.4 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CreativeMindsSolutions CM Header and Footer allows Stored XSS. This issue affects CM Header and Footer: from n/a through 1.2.4.	Patched by core rule	Y
CVE-2025-31092	WordPress Click to Chat – WP Support All-in-One Floating Widget plugin <= 2.3.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ninja Team Click to Chat – WP Support All-in-One Floating Widget allows Stored XSS. This issue affects Click to Chat – WP Support All-in-One Floating Widget: from n/a through 2.3.4.	Patched by core rule	Y
CVE-2025-31093	WordPress RPS Include Content <= 1.2.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in redpixelstudios RPS Include	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Content allows DOM-Based XSS. This issue affects RPS Include Content: from n/a through 1.2.1.		
CVE-2025-31094	WordPress WP Posts Carousel <= 1.3.8 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in teastudio.pl WP Posts Carousel allows Stored XSS. This issue affects WP Posts Carousel: from n/a through 1.3.8.	Patched by core rule	Y
CVE-2025-31096	WordPress PostX <= 4.1.25 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPXPO PostX allows DOM-Based XSS. This issue affects PostX: from n/a through 4.1.25.	Patched by core rule	Y
CVE-2025-31101	WordPress VaultRE Contact Form 7 plugin <= 1.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vault Group Pty Ltd VaultRE Contact Form 7 allows Stored XSS.This issue affects VaultRE Contact Form 7: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-31102	WordPress Hostel plugin <= 1.1.5.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bob Hostel allows Reflected XSS. This issue affects Hostel: from n/a through 1.1.5.5.	Patched by core rule	Y
CVE-2025-31121	OpenEMR allows XSS in Patient Image feature	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 7.0.3.1, the Patient Image feature in OpenEMR is vulnerable to cross-site scripting attacks via the EXIF title in an image. This vulnerability is fixed in 7.0.3.1.	Patched by core rule	Y
CVE-2025-31128	gifplayer XSS vulnerability	gifplayer is a customizable jquery plugin to play and stop animated gifs. gifplayer contains a cross-site scripting (XSS) vulnerability. This vulnerability is fixed in 0.3.7.	Patched by core rule	Y
CVE-2025-31378	WordPress Oppso Unit Converter plugin <= 1.1.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in danbwb Oppso Unit Converter allows Reflected XSS. This issue affects Oppso Unit Converter: from n/a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		through 1.1.1.		
CVE-2025-31379	WordPress Insert HTML Here plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in programphases Insert HTML Here allows Reflected XSS. This issue affects Insert HTML Here: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-31384	WordPress Videos plugin <= 1.0.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Aviplugins Videos allows Reflected XSS.This issue affects Videos: from n/a through 1.0.5.	Patched by core rule	Y
CVE-2025-31389	WordPress Sequel plugin <= 1.0.11 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sequel.Io Sequel allows Reflected XSS.This issue affects Sequel: from n/a through 1.0.11.	Patched by core rule	Y
CVE-2025-31394	WordPress More Mime Type Filters plugin <= 0.3 - CSRF to Stored XSS vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kailey (trepmal) More Mime Type Filters allows Stored XSS. This issue affects More Mime Type Filters: from n/a through 0.3.	Patched by core rule	Y
CVE-2025-31407	WordPress Tiger theme <= 2.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hutsixdigital Tiger allows Stored XSS.This issue affects Tiger: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-31409	WordPress Bridge Core plugin < 3.3.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Bridge Core allows Stored XSS. This issue affects Bridge Core: from n/a through n/a.	Patched by core rule	Y
CVE-2025-31412	WordPress JetProductGallery plugin <= 2.1.22 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound JetProductGallery allows DOM-Based XSS. This issue affects JetProductGallery: from n/a through 2.1.22.	Patched by core rule	Y
CVE-2025-31414	WordPress Cost Calculator Builder plugin <= 3.2.65 - Cross Site Scripting (XSS)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	vulnerability	Stylemix Cost Calculator Builder allows Stored XSS. This issue affects Cost Calculator Builder: from n/a through 3.2.65.		
CVE-2025-31416	WordPress Awesome Event Booking plugin <= 2.8.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AwesomeTOGI Awesome Event Booking allows Reflected XSS.This issue affects Awesome Event Booking: from n/a through 2.8.4.	Patched by core rule	Y
CVE-2025-31418	WordPress Gravel theme <= 1.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in noonnoo Gravel allows Reflected XSS.This issue affects Gravel: from n/a through 1.6.	Patched by core rule	Y
CVE-2025-31419	WordPress Churel plugin <= 1.0.8 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeix Churel allows DOM-Based XSS.This issue affects Churel: from n/a through 1.0.8.	Patched by core rule	Y
CVE-2025-31431	WordPress WP Bookmarks plugin <= 1.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WP Bookmarks allows Reflected XSS. This issue affects WP Bookmarks: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-31433	WordPress Magic Embeds <= 3.1.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Miguel Sirvent Magic Embeds allows Stored XSS. This issue affects Magic Embeds: from n/a through 3.1.2.	Patched by core rule	Y
CVE-2025-31434	WordPress FormLift for Infusionsoft Web Forms <= 7.5.19 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Adrian Tobey FormLift for Infusionsoft Web Forms allows Stored XSS. This issue affects FormLift for Infusionsoft Web Forms: from n/a through 7.5.19.	Patched by core rule	Y
CVE-2025-31436	WordPress Blubrry PowerPress Podcasting plugin MultiSite add-on plugin <= 0.1.1 - Reflected Cross Site Scripting (XSS)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Angelo Mandato Blubrry PowerPress Podcasting	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	vulnerability	plugin MultiSite add-on allows Reflected XSS. This issue affects Blubrry PowerPress Podcasting plugin MultiSite add-on: from n/a through 0.1.1.		
CVE-2025-31437	WordPress WP-OGP <= 1.0.5 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in David Miller WP-OGP allows Stored XSS. This issue affects WP-OGP: from n/a through 1.0.5.	Patched by core rule	Y
CVE-2025-31441	WordPress WordPress Galleria plugin <= 1.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in S WordPress Galleria allows Reflected XSS. This issue affects WordPress Galleria: from n/a through 1.4.	Patched by core rule	Y
CVE-2025-31442	WordPress Search engine keywords highlighter plugin <= 0.1.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Search engine keywords highlighter allows Reflected XSS. This issue affects Search engine keywords highlighter: from n/a through 0.1.3.	Patched by core rule	Y
CVE-2025-31445	WordPress Pages Order plugin <= 1.1.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Pages Order allows Reflected XSS. This issue affects Pages Order: from n/a through 1.1.3.	Patched by core rule	Y
CVE-2025-31446	WordPress WP Cleaner plugin <= 1.1.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jiangmiao WP Cleaner allows Reflected XSS. This issue affects WP Cleaner: from n/a through 1.1.5.	Patched by core rule	Y
CVE-2025-31450	WordPress Toggle Box <= 1.6 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in phantom.omaga Toggle Box allows Stored XSS. This issue affects Toggle Box: from n/a through 1.6.	Patched by core rule	Y
CVE-2025-31451	WordPress wBounce <= 1.8.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kevinweber wBounce allows Stored XSS. This issue affects wBounce: from n/a through 1.8.1.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-31452	WordPress WP Ultimate Search <= 2.0.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mindshare Labs, Inc. WP Ultimate Search allows Stored XSS. This issue affects WP Ultimate Search: from n/a through 2.0.3.	Patched by core rule	Y
CVE-2025-31453	WordPress YouTube SimpleGallery <= 2.0.6 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Stian Andreassen YouTube SimpleGallery allows Stored XSS. This issue affects YouTube SimpleGallery: from n/a through 2.0.6.	Patched by core rule	Y
CVE-2025-31454	WordPress Delete Post Revision plugin <= 1.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Delete Post Revision allows Reflected XSS. This issue affects Delete Post Revision: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-31455	WordPress Limit Max IPs Per User plugin <= 1.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Limit Max IPs Per User allows DOM-Based XSS. This issue affects Limit Max IPs Per User: from n/a through 1.5.	Patched by core rule	Y
CVE-2025-31461	WordPress NanoSupport plugin <= 0.6.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound NanoSupport allows Reflected XSS. This issue affects NanoSupport: from n/a through 0.6.0.	Patched by core rule	Y
CVE-2025-31462	WordPress CGM Event Calendar <= 0.8.5 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rzfarrell CGM Event Calendar allows Reflected XSS. This issue affects CGM Event Calendar: from n/a through 0.8.5.	Patched by core rule	Y
CVE-2025-31463	WordPress TGG WP Optimizer <= 1.22 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Preetinder Singh TGG WP Optimizer allows Stored XSS. This issue affects TGG WP Optimizer: from n/a through 1.22.	Patched by core rule	Y
CVE-2025-31464	WordPress Text Selection	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Color <= 1.6 - Cross Site Scripting (XSS) Vulnerability	Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nazmur Rahman Text Selection Color allows Stored XSS. This issue affects Text Selection Color: from n/a through 1.6.	rule	
CVE-2025-31465	WordPress Better Section Navigation Widget <= 1.6.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in cornershop Better Section Navigation Widget allows Stored XSS. This issue affects Better Section Navigation Widget: from n/a through 1.6.1.	Patched by core rule	Y
CVE-2025-31467	WordPress Flickr Photostream plugin <= 3.1.8 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Flickr Photostream allows Reflected XSS. This issue affects Flickr Photostream: from n/a through 3.1.8.	Patched by core rule	Y
CVE-2025-31468	WordPress WP_Identicon plugin <= 2.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WP_Identicon allows Reflected XSS. This issue affects WP_Identicon: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-31470	WordPress Page Takeover <= 1.1.6 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FancyThemes Page Takeover allows Stored XSS. This issue affects Page Takeover: from n/a through 1.1.6.	Patched by core rule	Y
CVE-2025-31471	WordPress Duplicate Page and Post <= 1.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Falcon Solutions Duplicate Page and Post allows Stored XSS. This issue affects Duplicate Page and Post: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-31472	WordPress Flatty <= 2.0.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michele Marri Flatty allows Stored XSS. This issue affects Flatty: from n/a through 2.0.0.	Patched by core rule	Y
CVE-2025-31473	WordPress WP Database Optimizer <= 1.2.1.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in matthewprice1178 WP	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Database Optimizer allows Stored XSS. This issue affects WP Database Optimizer: from n/a through 1.2.1.3.		
CVE-2025-31483	Stored XSS in Miniflux Media Proxy due to improper Content-Security-Policy configuration	Miniflux is a feed reader. Due to a weak Content Security Policy on the /proxy/* route, an attacker can bypass the CSP of the media proxy and execute cross-site scripting when opening external images in a new tab/window. To mitigate the vulnerability, the CSP for the media proxy has been changed from default-src 'self' to default-src 'none'; form-action 'none'; sandbox;. This vulnerability is fixed in 2.2.7.	Patched by core rule	Y
CVE-2025-3149	itning Student Homework Management System Edit Job Page fileupload cross site scripting	A vulnerability was found in itning Student Homework Management System up to 1.2.7. It has been classified as problematic. Affected is an unknown function of the file /shw_war/fileupload of the component Edit Job Page. The manipulation of the argument Course leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-3152	caipeichao ThinkOX Search search.html cross site scripting	A vulnerability classified as problematic has been found in caipeichao ThinkOX 1.0. This affects an unknown part of the file /ThinkOX-master/index.php?s=/Weibo/Index/search.html of the component Search. The manipulation of the argument keywords leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3153	Concrete CMS version 9 below 9.4.0RC2 and versions below 8.5.20 - CSRF and XSS in Concrete CMS Custom Address attributeC	Concrete CMS version 9 below 9.4.0RC2 and versions below 8.5.20 are vulnerable to CSRF and XSS in the Concrete CMS Address attribute because addresses are not properly sanitized in the output when a country is not specified. Attackers are limited to individuals whom a site administrator has	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		granted the ability to fill in an address attribute. It is possible for the attacker to glean limited information from the site but amount and type is restricted by mitigating controls and the level of access of the attacker. Limited data modification is possible. The dashboard page itself could be rendered unavailable. The fix only sanitizes new data uploaded post update to Concrete CMS 9.4.0RC2. Existing database entries added before the update will still be “live” if there were successful exploits added under previous versions; a database search is recommended. The Concrete CMS security team gave this vulnerability CVSS v.4.0 score of 5.1 with vector CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:L/VI:L/VA:L/SC:L/SI:L/SA:L Thanks Myq Larson for reporting.		
CVE-2025-31532	WordPress AtomChat plugin <= 1.1.6 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Team AtomChat AtomChat allows Stored XSS. This issue affects AtomChat: from n/a through 1.1.6.	Patched by core rule	Y
CVE-2025-31535	WordPress Simple Owl Carousel plugin <= 1.1.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PressTigers Simple Owl Carousel allows DOM-Based XSS. This issue affects Simple Owl Carousel: from n/a through 1.1.1.	Patched by core rule	Y
CVE-2025-31536	WordPress CF7 Spreadsheets plugin <= 2.3.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in moshensky CF7 Spreadsheets allows Reflected XSS. This issue affects CF7 Spreadsheets: from n/a through 2.3.2.	Patched by core rule	Y
CVE-2025-31537	WordPress Bulk NoIndex & NoFollow Toolkit plugin <= 2.16 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in madfishdigital Bulk NoIndex & NoFollow Toolkit allows Reflected XSS. This issue affects Bulk NoIndex & NoFollow Toolkit: from n/a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		through 2.16.		
CVE-2025-31538	WordPress Checklist plugin <= 1.1.9 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in checklistcom Checklist allows Stored XSS. This issue affects Checklist: from n/a through 1.1.9.	Patched by core rule	Y
CVE-2025-31543	WordPress Twice Commerce plugin <= 1.3.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Twice Commerce Twice Commerce allows DOM-Based XSS. This issue affects Twice Commerce: from n/a through 1.3.1.	Patched by core rule	Y
CVE-2025-31548	WordPress Ultimate Push Notifications plugin <= 1.1.8 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in M. Tuhin Ultimate Push Notifications allows Reflected XSS. This issue affects Ultimate Push Notifications: from n/a through 1.1.8.	Patched by core rule	Y
CVE-2025-31549	WordPress Fusion plugin <= 1.6.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Agency Dominion Inc. Fusion allows DOM-Based XSS. This issue affects Fusion: from n/a through 1.6.3.	Patched by core rule	Y
CVE-2025-31556	WordPress IMPress for IDX Broker plugin <= 3.2.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in IDX Broker IMPress for IDX Broker allows Stored XSS. This issue affects IMPress for IDX Broker: from n/a through 3.2.3.	Patched by core rule	Y
CVE-2025-31557	WordPress OSM – OpenStreetMap plugin <= 6.1.6 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MiKa OSM – OpenStreetMap allows DOM-Based XSS. This issue affects OSM – OpenStreetMap: from n/a through 6.1.6.	Patched by core rule	Y
CVE-2025-31559	WordPress Custom Database Applications by Caspio plugin <= 2.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Caspio Bridge Custom Database Applications by Caspio allows DOM-Based XSS. This issue affects Custom Database	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Applications by Caspio: from n/a through 2.1.		
CVE-2025-31562	WordPress Uptime Robot Plugin for WordPress plugin <= 2.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aphotrax Uptime Robot Plugin for WordPress allows DOM-Based XSS. This issue affects Uptime Robot Plugin for WordPress: from n/a through 2.3.	Patched by core rule	Y
CVE-2025-31563	WordPress AI Search Bar plugin <= 1.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vimal Kava AI Search Bar allows Stored XSS. This issue affects AI Search Bar: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-31567	WordPress Themesflat Addons For Elementor plugin <= 2.2.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themesflat Themesflat Addons For Elementor allows Stored XSS. This issue affects Themesflat Addons For Elementor: from n/a through 2.2.5.	Patched by core rule	Y
CVE-2025-31568	WordPress LeadLab by wiredminds plugin <= 1.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wiredmindshelp LeadLab by wiredminds allows Reflected XSS. This issue affects LeadLab by wiredminds: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-31571	WordPress The Logo Slider plugin <= 1.0.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Cynob IT Consultancy The Logo Slider allows Reflected XSS. This issue affects The Logo Slider: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-31573	WordPress PeproDev CF7 Database plugin <= 2.0.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pepro Dev. Group PeproDev CF7 Database allows Stored XSS. This issue affects PeproDev CF7 Database: from n/a through 2.0.0.	Patched by core rule	Y
CVE-2025-31574	WordPress Custom Content Scrollbar plugin <= 1.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SoftHopper Custom Content Scrollbar allows Stored XSS. This issue affects Custom	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Content Scrollbar: from n/a through 1.3.		
CVE-2025-31575	WordPress Flag Icons plugin <= 2.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Vasilis Triantafyllou Flag Icons allows Stored XSS. This issue affects Flag Icons: from n/a through 2.2.	Patched by core rule	Y
CVE-2025-31578	WordPress Fonts Manager | Custom Fonts plugin <= 1.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wisdomlogix Solutions Pvt. Ltd. Fonts Manager | Custom Fonts allows Reflected XSS. This issue affects Fonts Manager | Custom Fonts: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-31582	WordPress Contact Form vCard Generator plugin <= 2.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ashish Ajani Contact Form vCard Generator allows Stored XSS. This issue affects Contact Form vCard Generator: from n/a through 2.4.	Patched by core rule	Y
CVE-2025-31586	WordPress Gallery – Photo Albums Plugin plugin <= 1.3.170 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GhozyLab Gallery – Photo Albums Plugin allows Stored XSS. This issue affects Gallery – Photo Albums Plugin: from n/a through 1.3.170.	Patched by core rule	Y
CVE-2025-31587	WordPress Elfsight Testimonials Slider plugin <= 1.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in elfsight Elfsight Testimonials Slider allows Stored XSS. This issue affects Elfsight Testimonials Slider: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-31589	WordPress Ethiopian Calendar plugin <= 1.1.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kibru Demeke Ethiopian Calendar allows Stored XSS. This issue affects Ethiopian Calendar: from n/a through 1.1.1.	Patched by core rule	Y
CVE-2025-31590	WordPress WP Date and Time Shortcode plugin <= 2.6.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Denra.com WP Date and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Time Shortcode allows Stored XSS. This issue affects WP Date and Time Shortcode: from n/a through 2.6.7.		
CVE-2025-31591	WordPress Exit Popup Free plugin <= 1.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in promoz73 Exit Popup Free allows Stored XSS. This issue affects Exit Popup Free: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-31592	WordPress Send E-mail plugin <= 1.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Paolo Melchiorre Send E-mail allows Stored XSS. This issue affects Send E-mail: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-31593	WordPress OpenMenu plugin <= 3.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in OpenMenu OpenMenu allows Stored XSS. This issue affects OpenMenu: from n/a through 3.5.	Patched by core rule	Y
CVE-2025-31594	WordPress Auto scroll for reading plugin <= 1.1.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPglob Auto scroll for reading allows Reflected XSS. This issue affects Auto scroll for reading: from n/a through 1.1.4.	Patched by core rule	Y
CVE-2025-31595	WordPress Timeline Event History plugin <= 3.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpdiscover Timeline Event History allows Stored XSS. This issue affects Timeline Event History: from n/a through 3.2.	Patched by core rule	Y
CVE-2025-31597	WordPress Ultimate Live Cricket WordPress Lite plugin <= 1.4.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in crazycric Ultimate Live Cricket WordPress Lite allows Stored XSS. This issue affects Ultimate Live Cricket WordPress Lite: from n/a through 1.4.2.	Patched by core rule	Y
CVE-2025-31598	WordPress Quantity Dynamic Pricing & Bulk Discounts for WooCommerce plugin <= 4.0.0 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Quantity Dynamic Pricing & Bulk Discounts for	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		WooCommerce allows Stored XSS. This issue affects Quantity Dynamic Pricing & Bulk Discounts for WooCommerce: from n/a through 4.0.0.		
CVE-2025-31604	WordPress Cal.com plugin <= 1.0.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Cal.com Cal.com allows Stored XSS. This issue affects Cal.com: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-31605	WordPress Welcome Popup plugin <= 1.0.10 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WeblineIndia Welcome Popup allows Stored XSS. This issue affects Welcome Popup: from n/a through 1.0.10.	Patched by core rule	Y
CVE-2025-31607	WordPress Simple-Audioplayer plugin <= 1.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in flomei Simple-Audioplayer allows Stored XSS. This issue affects Simple-Audioplayer: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-31608	WordPress CookieHint WP plugin <= 1.0.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in reDim GmbH CookieHint WP allows Stored XSS. This issue affects CookieHint WP: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-31610	WordPress Notification Bar, Sticky Notification Bar, Sticky Welcome Bar for any theme plugin <= 1.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gingerplugins Notification Bar, Sticky Notification Bar, Sticky Welcome Bar for any theme allows Stored XSS. This issue affects Notification Bar, Sticky Notification Bar, Sticky Welcome Bar for any theme: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-31614	WordPress Terms Before Download plugin <= 1.0.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hiroprot Terms Before Download allows Stored XSS. This issue affects Terms Before Download: from n/a through 1.0.4.	Patched by core rule	Y
CVE-2025-31615	WordPress Simple Contact Forms plugin <= 1.6.4 - CSRF to Stored XSS vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		owenr88 Simple Contact Forms allows Stored XSS. This issue affects Simple Contact Forms: from n/a through 1.6.4.		
CVE-2025-31620	WordPress CoverManager plugin <= 0.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in carperfer CoverManager allows Stored XSS. This issue affects CoverManager: from n/a through 0.0.1.	Patched by core rule	Y
CVE-2025-31621	WordPress byBrick Accordion plugin <= 1.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in davidpaulsson byBrick Accordion allows Stored XSS. This issue affects byBrick Accordion: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-31622	WordPress Advanced Typekit plugin <= 1.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Utkarsh Kukreti Advanced Typekit allows Stored XSS. This issue affects Advanced Typekit: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-31624	WordPress Processing Projects plugin <= 1.0.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LABCAT Processing Projects allows DOM-Based XSS. This issue affects Processing Projects: from n/a through 1.0.2.	Patched by core rule	Y
CVE-2025-31625	WordPress Useinfluence plugin <= 1.0.8 - Cross Site Request Forgery (CSRF) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ramanparashar Useinfluence allows Stored XSS. This issue affects Useinfluence: from n/a through 1.0.8.	Patched by core rule	Y
CVE-2025-31626	WordPress Support Helpdesk Ticket System Lite plugin <= 4.5.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in M. Ali Saleem Support Helpdesk Ticket System Lite allows Reflected XSS. This issue affects Support Helpdesk Ticket System Lite: from n/a through 4.5.2.	Patched by core rule	Y
CVE-2025-31627	WordPress Media Library Assistant plugin <= 3.24 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in David Lingren Media Library Assistant allows Stored XSS.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This issue affects Media Library Assistant: from n/a through 3.24.		
CVE-2025-31629	WordPress Infusionsoft Web Form JavaScript plugin <= 1.1.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jacob Allred Infusionsoft Web Form JavaScript allows Stored XSS. This issue affects Infusionsoft Web Form JavaScript: from n/a through 1.1.1.	Patched by core rule	Y
CVE-2025-31730	WordPress Marketer Addons Plugin <= 1.0.1 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DigitalCourt Marketer Addons allows Stored XSS. This issue affects Marketer Addons: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-31731	WordPress Author Bio Shortcode Plugin <= 2.5.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Philip John Author Bio Shortcode allows Stored XSS. This issue affects Author Bio Shortcode: from n/a through 2.5.3.	Patched by core rule	Y
CVE-2025-31733	WordPress WP Sitemap Plugin <= 1.0.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Boot Div WP Sitemap allows Stored XSS. This issue affects WP Sitemap: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-31734	WordPress Simple Post Expiration plugin <= 1.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Syed Balkhi Simple Post Expiration allows DOM-Based XSS. This issue affects Simple Post Expiration: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-31735	WordPress Footnotes for WordPress plugin <= 2016.1230 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in C. Johnson Footnotes for WordPress allows Stored XSS. This issue affects Footnotes for WordPress: from n/a through 2016.1230.	Patched by core rule	Y
CVE-2025-31737	WordPress Client Showcase plugin <= 1.2.0 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in dxladner Client Showcase allows Stored XSS. This issue	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects Client Showcase: from n/a through 1.2.0.		
CVE-2025-31738	WordPress LeadQuizzes Plugin <= 1.1.0 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in yazamodeveloper LeadQuizzes allows Stored XSS. This issue affects LeadQuizzes: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-31740	WordPress News, Magazine and Blog Elements Plugin <= 1.3 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in aThemeArt News, Magazine and Blog Elements allows Stored XSS. This issue affects News, Magazine and Blog Elements: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-31741	WordPress Easy Magazine plugin <= 2.1.13 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Filtr8 Easy Magazine allows DOM-Based XSS. This issue affects Easy Magazine: from n/a through 2.1.13.	Patched by core rule	Y
CVE-2025-31742	WordPress Dima Take Action Plugin <= 1.0.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PixelDima Dima Take Action allows Stored XSS. This issue affects Dima Take Action: from n/a through 1.0.5.	Patched by core rule	Y
CVE-2025-31743	WordPress Lightweight and Responsive Youtube Embed Plugin <= 1.0.0 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpszaki Lightweight and Responsive Youtube Embed allows Stored XSS. This issue affects Lightweight and Responsive Youtube Embed: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-31744	WordPress Lightweight and Responsive Youtube Embed plugin <= 1.0.0 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpszaki Lightweight and Responsive Youtube Embed allows Stored XSS. This issue affects Lightweight and Responsive Youtube Embed: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-31745	WordPress Subscription Form for Feedblitz Plugin <= 1.0.9 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Arni Cinco Subscription Form for Feedblitz allows Stored XSS. This issue affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Subscription Form for Feedblitz: from n/a through 1.0.9.		
CVE-2025-31747	WordPress WP Chrono plugin <= 1.5.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in milan.latinovic WP Chrono allows DOM-Based XSS. This issue affects WP Chrono: from n/a through 1.5.4.	Patched by core rule	Y
CVE-2025-31748	WordPress Opal Portfolio Plugin <= 1.0.4 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpopal Opal Portfolio allows Stored XSS. This issue affects Opal Portfolio: from n/a through 1.0.4.	Patched by core rule	Y
CVE-2025-31749	WordPress HMH Footer Builder For Elementor plugin <= 1.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPelite HMH Footer Builder For Elementor allows Stored XSS. This issue affects HMH Footer Builder For Elementor: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-31750	WordPress Breaking News WP Plugin <= 1.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in doit Breaking News WP allows Stored XSS. This issue affects Breaking News WP: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-31754	WordPress DobsonDev Shortcodes plugin <= 2.1.12 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DobsonDev DobsonDev Shortcodes allows Stored XSS. This issue affects DobsonDev Shortcodes: from n/a through 2.1.12.	Patched by core rule	Y
CVE-2025-31759	WordPress Boo Recipes plugin <= 2.4.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BooSpot Boo Recipes allows Stored XSS. This issue affects Boo Recipes: from n/a through 2.4.1.	Patched by core rule	Y
CVE-2025-31760	WordPress SnapWidget Social Photo Feed Widget plugin <= 1.1.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in snapwidget SnapWidget Social Photo Feed Widget allows DOM-Based XSS. This issue affects SnapWidget Social Photo Feed Widget: from n/a through 1.1.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-31761	WordPress Hypotext plugin <= 1.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DEJAN Hypotext allows Stored XSS. This issue affects Hypotext: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-31762	WordPress Sheet2Site plugin <= 1.0.18 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in andreyazimov Sheet2Site allows Stored XSS. This issue affects Sheet2Site: from n/a through 1.0.18.	Patched by core rule	Y
CVE-2025-31764	WordPress Cache control by Cacholong plugin <= 5.4.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Preliot Cache control by Cacholong allows Stored XSS. This issue affects Cache control by Cacholong: from n/a through 5.4.1.	Patched by core rule	Y
CVE-2025-31766	WordPress PhotoShelter for Photographers Blog Feed plugin <= 1.5.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PhotoShelter PhotoShelter for Photographers Blog Feed Plugin allows Stored XSS. This issue affects PhotoShelter for Photographers Blog Feed Plugin: from n/a through 1.5.7.	Patched by core rule	Y
CVE-2025-31767	WordPress Post Custom Templates Lite plugin <= 1.14 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in OTWthemes Post Custom Templates Lite allows Stored XSS. This issue affects Post Custom Templates Lite: from n/a through 1.14.	Patched by core rule	Y
CVE-2025-31770	WordPress Content Manager Light plugin <= 3.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in OTWthemes Content Manager Light allows Stored XSS. This issue affects Content Manager Light: from n/a through 3.2.	Patched by core rule	Y
CVE-2025-31771	WordPress Team Members for Elementor Page Builder plugin <= 1.0.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sultan Nasir Uddin Team Members for Elementor Page Builder allows Stored XSS. This issue affects Team Members for Elementor	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Page Builder: from n/a through 1.0.4.		
CVE-2025-31772	WordPress WP Modal Popup with Cookie Integration plugin <= 2.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Astoundify WP Modal Popup with Cookie Integration allows Stored XSS. This issue affects WP Modal Popup with Cookie Integration: from n/a through 2.4.	Patched by core rule	Y
CVE-2025-31778	WordPress Donate Me Plugin <= 1.2.5 - Stored Cross-Site Scripting vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in raphaelheide Donate Me allows Reflected XSS. This issue affects Donate Me: from n/a through 1.2.5.	Patched by core rule	Y
CVE-2025-31783	WordPress Leartes TRY Exchange Rates Plugin <= 2.1 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Leartes.NET Leartes TRY Exchange Rates allows Stored XSS. This issue affects Leartes TRY Exchange Rates: from n/a through 2.1.	Patched by core rule	Y
CVE-2025-31790	WordPress Posten plugin <= 0.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Binsaifullah Posten allows DOM-Based XSS. This issue affects Posten: from n/a through 0.0.1.	Patched by core rule	Y
CVE-2025-31792	WordPress Piotnet Forms plugin <= 1.0.30 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in piotnetdotcom Piotnet Forms allows Stored XSS. This issue affects Piotnet Forms: from n/a through 1.0.30.	Patched by core rule	Y
CVE-2025-31793	WordPress Piotnet Forms plugin <= 1.0.30 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in piotnetdotcom Piotnet Forms allows Stored XSS. This issue affects Piotnet Forms: from n/a through 1.0.30.	Patched by core rule	Y
CVE-2025-31797	WordPress Sprout Clients plugin <= 3.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BoldGrid Sprout Clients allows Stored XSS. This issue affects Sprout Clients: from n/a through 3.2.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-31801	WordPress MX Time Zone Clocks plugin <= 5.1.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Maksym Marko MX Time Zone Clocks allows Reflected XSS. This issue affects MX Time Zone Clocks: from n/a through 5.1.1.	Patched by core rule	Y
CVE-2025-31803	WordPress Turisbook Booking System plugin <= 1.3.7 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Neteuro Turisbook Booking System allows Stored XSS. This issue affects Turisbook Booking System: from n/a through 1.3.7.	Patched by core rule	Y
CVE-2025-31804	WordPress Follow Us Badges plugin <= 3.1.11 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DraftPress Team Follow Us Badges allows Stored XSS. This issue affects Follow Us Badges: from n/a through 3.1.11.	Patched by core rule	Y
CVE-2025-31805	WordPress Gutena Kit plugin <= 2.0.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ExpressTech Systems Gutena Kit – Gutenberg Blocks and Templates allows Stored XSS. This issue affects Gutena Kit – Gutenberg Blocks and Templates: from n/a through 2.0.7.	Patched by core rule	Y
CVE-2025-31806	WordPress Webling Plugin <= 3.9.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in uSystems Webling allows Stored XSS. This issue affects Webling: from n/a through 3.9.0.	Patched by core rule	Y
CVE-2025-31811	WordPress Planyo online reservation system plugin <= 3.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in xtreeme Planyo online reservation system allows Stored XSS. This issue affects Planyo online reservation system: from n/a through 3.0.	Patched by core rule	Y
CVE-2025-31812	WordPress BuddyPress Members Only plugin <= 3.5.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tomas BuddyPress Members Only allows Stored XSS. This issue affects BuddyPress Members Only: from n/a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		through 3.5.3.		
CVE-2025-31813	WordPress WPSHARE247 Elementor Addons plugin <= 2.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Website366.com WPSHARE247 Elementor Addons allows Stored XSS. This issue affects WPSHARE247 Elementor Addons: from n/a through 2.1.	Patched by core rule	Y
CVE-2025-31815	WordPress Design Blocks plugin <= 1.2.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in devscred Design Blocks allows Stored XSS. This issue affects Design Blocks: from n/a through 1.2.2.	Patched by core rule	Y
CVE-2025-31817	WordPress BlockWheels plugin <= 1.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPWheels BlockWheels allows DOM-Based XSS. This issue affects BlockWheels: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-31818	WordPress ContentBot AI Writer plugin <= 1.2.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ContentBot.ai ContentBot AI Writer allows Stored XSS. This issue affects ContentBot AI Writer: from n/a through 1.2.4.	Patched by core rule	Y
CVE-2025-31819	WordPress Nova Blocks by Pixelgrade plugin <= 2.1.8 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pixelgrade Nova Blocks by Pixelgrade. This issue affects Nova Blocks by Pixelgrade: from n/a through 2.1.8.	Patched by core rule	Y
CVE-2025-31823	WordPress WPoperation Elementor Addons plugin 1.1.9 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpoperations WPoperation Elementor Addons allows Stored XSS. This issue affects WPoperation Elementor Addons: from n/a through 1.1.9.	Patched by core rule	Y
CVE-2025-31829	WordPress ShopCred plugin <= 1.2.8 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in devscred ShopCred allows DOM-Based XSS. This issue affects ShopCred: from n/a through 1.2.8.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-31835	WordPress WP Plugin Info Card plugin <= 5.2.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brice Capobianco WP Plugin Info Card allows DOM-Based XSS. This issue affects WP Plugin Info Card: from n/a through 5.2.5.	Patched by core rule	Y
CVE-2025-31837	WordPress WP Proposals plugin <= 2.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Codeus WP Proposals allows Stored XSS. This issue affects WP Proposals: from n/a through 2.3.	Patched by core rule	Y
CVE-2025-31838	WordPress Eventbee RSVP Widget plugin <= 1.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eventbee Eventbee RSVP Widget allows DOM-Based XSS. This issue affects Eventbee RSVP Widget: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-31844	WordPress Magical Blocks plugin <= 1.0.10 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Noor Alam Magical Blocks allows Stored XSS. This issue affects Magical Blocks: from n/a through 1.0.10.	Patched by core rule	Y
CVE-2025-31847	WordPress mFolio Lite plugin <= 1.2.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themelooks mFolio Lite allows DOM-Based XSS. This issue affects mFolio Lite: from n/a through 1.2.2.	Patched by core rule	Y
CVE-2025-31849	WordPress Nemesis All-in-One | Newspaper Builder Elementor Extention plugin <= 1.1.0 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fbtemplates Nemesis All-in-One allows Stored XSS. This issue affects Nemesis All-in-One: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-31850	WordPress PDF Generator Addon for Elementor Page Builder plugin <= 1.7.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RedefiningTheWeb PDF Generator Addon for Elementor Page Builder allows Stored XSS. This issue affects PDF Generator Addon for Elementor Page Builder: from n/a through 1.7.5.	Patched by core rule	Y
CVE-2025-31851	WordPress Beds24	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Online Booking plugin <= 2.0.26 - Cross Site Scripting (XSS) vulnerability	Input During Web Page Generation ('Cross-site Scripting') vulnerability in markkinchin Beds24 Online Booking allows Stored XSS. This issue affects Beds24 Online Booking: from n/a through 2.0.26.	rule	
CVE-2025-31853	WordPress Smartarget Popup Plugin <= 1.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Erez Hadas-Sonnenschein Smartarget Popup allows Stored XSS. This issue affects Smartarget Popup: from n/a through 1.4.	Patched by core rule	Y
CVE-2025-31855	WordPress SMM API plugin <= 6.0.27 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in softnwords SMM API allows Stored XSS. This issue affects SMM API: from n/a through 6.0.27.	Patched by core rule	Y
CVE-2025-31857	WordPress Directorist AddonsKit for Elementor plugin <= 1.1.6 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpWax Directorist AddonsKit for Elementor allows Stored XSS. This issue affects Directorist AddonsKit for Elementor: from n/a through 1.1.6.	Patched by core rule	Y
CVE-2025-31860	WordPress WP AdCenter plugin <= 2.5.9 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPeka WP AdCenter allows Stored XSS. This issue affects WP AdCenter: from n/a through 2.5.9.	Patched by core rule	Y
CVE-2025-31861	WordPress Perfect Font Awesome Integration Plugin <= 2.2 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPOrbit Support Perfect Font Awesome Integration allows Stored XSS. This issue affects Perfect Font Awesome Integration: from n/a through 2.2.	Patched by core rule	Y
CVE-2025-31864	WordPress Beam me up Scotty – Back to Top Button plugin <= 1.0.23 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Out the Box Beam me up Scotty – Back to Top Button allows Stored XSS. This issue affects Beam me up Scotty – Back to Top Button: from n/a through 1.0.23.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-31869	WordPress Black Widgets For Elementor plugin <= 1.3.9 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Modernaweb Studio Black Widgets For Elementor allows Stored XSS. This issue affects Black Widgets For Elementor: from n/a through 1.3.9.	Patched by core rule	Y
CVE-2025-31873	WordPress SheetDB Plugin <= 1.3.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sheetdb SheetDB allows Stored XSS. This issue affects SheetDB: from n/a through 1.3.3.	Patched by core rule	Y
CVE-2025-31874	WordPress WebberZone Snippetz plugin <= 2.1.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ajay WebberZone Snippetz allows Stored XSS. This issue affects WebberZone Snippetz: from n/a through 2.1.0.	Patched by core rule	Y
CVE-2025-31875	WordPress FancyPost plugin <= 6.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pluginic FancyPost allows DOM-Based XSS. This issue affects FancyPost: from n/a through 6.0.1.	Patched by core rule	Y
CVE-2025-31883	WordPress WebinarPress plugin <= 1.33.27 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPWebinarSystem WebinarPress allows Stored XSS. This issue affects WebinarPress: from n/a through 1.33.27.	Patched by core rule	Y
CVE-2025-31884	WordPress Norse Rune Oracle Plugin plugin <= 1.4.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP CMS Ninja Norse Rune Oracle Plugin allows Stored XSS. This issue affects Norse Rune Oracle Plugin: from n/a through 1.4.3.	Patched by core rule	Y
CVE-2025-31885	WordPress Hyperlink Group Block plugin <= 2.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Daniel Floeter Hyperlink Group Block allows DOM-Based XSS. This issue affects Hyperlink Group Block: from n/a through 2.0.1.	Patched by core rule	Y
CVE-2025-31889	WordPress Extensions for	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Elementor plugin <= 2.0.40 - Cross Site Scripting (XSS) vulnerability	Input During Web Page Generation ('Cross-site Scripting') vulnerability in petesheppard84 Extensions for Elementor. This issue affects Extensions for Elementor: from n/a through 2.0.40.	rule	
CVE-2025-31890	WordPress Simple Map No Api plugin <= 1.9 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mashi Simple Map No Api allows Stored XSS. This issue affects Simple Map No Api: from n/a through 1.9.	Patched by core rule	Y
CVE-2025-31891	WordPress Gosign – Posts Slider Block plugin <= 1.1.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Gosign Gosign – Posts Slider Block allows Stored XSS. This issue affects Gosign – Posts Slider Block: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-31892	WordPress WP Crowdfunding plugin <= 2.1.13 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeum WP Crowdfunding allows Stored XSS. This issue affects WP Crowdfunding: from n/a through 2.1.13.	Patched by core rule	Y
CVE-2025-31893	WordPress Botnet Attack Blocker plugin <= 2.0.0 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cheesefather Botnet Attack Blocker allows Stored XSS. This issue affects Botnet Attack Blocker: from n/a through 2.0.0.	Patched by core rule	Y
CVE-2025-31894	WordPress Ebook Downloader plugin <= 1.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Infoway LLC Ebook Downloader allows Stored XSS. This issue affects Ebook Downloader: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-31895	WordPress ABC Notation Plugin <= 6.1.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in paulrosen ABC Notation allows Stored XSS. This issue affects ABC Notation: from n/a through 6.1.3.	Patched by core rule	Y
CVE-2025-31897	WordPress Arrow Custom Feed for Twitter plugin <= 1.5.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Arrow Plugins Arrow Custom	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Feed for Twitter allows Stored XSS. This issue affects Arrow Custom Feed for Twitter: from n/a through 1.5.3.		
CVE-2025-31898	WordPress MediaView plugin <= 1.1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound MediaView allows Reflected XSS. This issue affects MediaView: from n/a through 1.1.2.	Patched by core rule	Y
CVE-2025-31899	WordPress Awesome Logos plugin <= 1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpshopee Awesome Logos allows Reflected XSS. This issue affects Awesome Logos: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-31900	WordPress Lexicata plugin <= 1.0.16 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in lexicata Lexicata allows Reflected XSS. This issue affects Lexicata: from n/a through 1.0.16.	Patched by core rule	Y
CVE-2025-31901	WordPress Digihood HTML Sitemap Plugin <= 3.1.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Digihood Digihood HTML Sitemap allows Reflected XSS. This issue affects Digihood HTML Sitemap: from n/a through 3.1.1.	Patched by core rule	Y
CVE-2025-31902	WordPress Social Share And Social Locker Plugin <= 1.4.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Social Share And Social Locker allows Reflected XSS. This issue affects Social Share And Social Locker: from n/a through 1.4.1.	Patched by core rule	Y
CVE-2025-31903	WordPress XV Random Quotes Plugin <= 1.37 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound XV Random Quotes allows Reflected XSS. This issue affects XV Random Quotes: from n/a through 1.37.	Patched by core rule	Y
CVE-2025-31905	WordPress Team Rosters Plugin <= 4.7 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Team Rosters allows Reflected XSS. This issue affects Team Rosters:	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		from n/a through 4.7.		
CVE-2025-31907	WordPress Team Builder plugin <= 1.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Labib Ahmed Team Builder allows Reflected XSS. This issue affects Team Builder: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-32027	Yii does not prevent XSS in scenarios where fallback error renderer is used	Yii is an open source PHP web framework. Prior to 1.1.31, yiisoft/yii is vulnerable to Reflected XSS in specific scenarios where the fallback error renderer is used. Upgrade yiisoft/yii to version 1.1.31 or higher.	Patched by core rule	Y
CVE-2025-32114	WordPress 5sterrenspecialist plugin <= 1.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 5sterrenspecialist 5sterrenspecialist allows Reflected XSS. This issue affects 5sterrenspecialist: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-32115	WordPress Popping Content Light plugin <= 2.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in OTWthemes Popping Content Light allows Reflected XSS. This issue affects Popping Content Light: from n/a through 2.4.	Patched by core rule	Y
CVE-2025-32116	WordPress QR Master plugin <= 1.0.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Studi7 QR Master allows Reflected XSS. This issue affects QR Master: from n/a through 1.0.5.	Patched by core rule	Y
CVE-2025-32117	WordPress Widgetize Pages Light plugin <= 3.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in OTWthemes Widgetize Pages Light allows Reflected XSS. This issue affects Widgetize Pages Light: from n/a through 3.0.	Patched by core rule	Y
CVE-2025-32129	WordPress Welcome Bar plugin <= 2.0.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Data443 Risk Migitation, Inc. Welcome Bar allows Stored XSS. This issue affects Welcome Bar: from n/a through 2.0.4.	Patched by core rule	Y
CVE-2025-32130	WordPress Posts Footer	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Manager plugin <= 2.2.0 - Cross Site Scripting (XSS) Vulnerability	Input During Web Page Generation ('Cross-site Scripting') vulnerability in Data443 Risk Migitation, Inc. Posts Footer Manager allows Stored XSS. This issue affects Posts Footer Manager: from n/a through 2.2.0.	rule	
CVE-2025-32131	WordPress Social Intents plugin <= 1.6.14 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in socialintents Social Intents allows Stored XSS. This issue affects Social Intents: from n/a through 1.6.14.	Patched by core rule	Y
CVE-2025-32132	WordPress FunnelCockpit Plugin <= 1.4.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FunnelCockpit FunnelCockpit allows Stored XSS. This issue affects FunnelCockpit: from n/a through 1.4.2.	Patched by core rule	Y
CVE-2025-32133	WordPress Secure Copy Content Protection and Content Locking plugin <= 4.5.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ays Pro Secure Copy Content Protection and Content Locking allows Stored XSS. This issue affects Secure Copy Content Protection and Content Locking: from n/a through 4.5.1.	Patched by core rule	Y
CVE-2025-32134	WordPress URL Shortify Plugin <= 1.10.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in KaizenCoders URL Shortify allows Stored XSS. This issue affects URL Shortify: from n/a through 1.10.4.	Patched by core rule	Y
CVE-2025-32135	WordPress Split Test For Elementor plugin <= 1.8.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rocketelements Split Test For Elementor allows Stored XSS. This issue affects Split Test For Elementor: from n/a through 1.8.3.	Patched by core rule	Y
CVE-2025-32136	WordPress ActiveCampaign Plugin <= 8.1.16 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in activecampaign ActiveCampaign allows Stored XSS. This issue affects ActiveCampaign: from n/a through 8.1.16.	Patched by core rule	Y
CVE-2025-32139	WordPress Lightbox & Modal Popup WordPress Plugin – FooBox plugin <=	Improper Neutralization of Input During Web Page Generation ('Cross-site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	2.7.33 - Cross Site Scripting (XSS) vulnerability	Scripting') vulnerability in bradvin FooBox Image Lightbox . This issue affects FooBox Image Lightbox : from n/a through 2.7.33.		
CVE-2025-32161	WordPress Arkhe Blocks <= 2.27.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ryo Arkhe Blocks allows Stored XSS. This issue affects Arkhe Blocks: from n/a through 2.27.1.	Patched by core rule	Y
CVE-2025-32162	WordPress Chamber Dashboard Business Directory plugin <= 3.3.11 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Morgan Kay Chamber Dashboard Business Directory allows DOM-Based XSS. This issue affects Chamber Dashboard Business Directory: from n/a through 3.3.11.	Patched by core rule	Y
CVE-2025-32163	WordPress Xpro Elementor Addons plugin <= 1.4.9 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Xpro Xpro Elementor Addons allows Stored XSS. This issue affects Xpro Elementor Addons: from n/a through 1.4.9.	Patched by core rule	Y
CVE-2025-32165	WordPress Doppler Forms plugin <= 2.4.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fromdoppler Doppler Forms allows Stored XSS. This issue affects Doppler Forms: from n/a through 2.4.5.	Patched by core rule	Y
CVE-2025-32166	WordPress Emma for WordPress plugin <= 1.3.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in John Housholder Emma for WordPress allows Stored XSS. This issue affects Emma for WordPress: from n/a through 1.3.3.	Patched by core rule	Y
CVE-2025-32167	WordPress SurveyJS plugin <= 1.12.20 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in devsoftbaltic SurveyJS allows Stored XSS. This issue affects SurveyJS: from n/a through 1.12.20.	Patched by core rule	Y
CVE-2025-32168	WordPress Gutenify plugin <= 1.4.9 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodeYatri Gutenify allows Stored XSS. This issue affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Gutenify: from n/a through 1.4.9.		
CVE-2025-32169	WordPress Showeblogin Social plugin <= 7.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Suresh Prasad Showeblogin Social allows DOM-Based XSS. This issue affects Showeblogin Social: from n/a through 7.0.	Patched by core rule	Y
CVE-2025-32170	WordPress Motors plugin <= 1.4.65 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Stylemix Motors allows Stored XSS. This issue affects Motors: from n/a through 1.4.65.	Patched by core rule	Y
CVE-2025-32171	WordPress Table Block by Tableberg – Best WordPress Table Plugin plugin <= 0.6.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Imtiaz Rayhan Table Block by Tableberg allows Stored XSS. This issue affects Table Block by Tableberg: from n/a through 0.6.0.	Patched by core rule	Y
CVE-2025-32172	WordPress YaMaps for WordPress plugin <= 0.6.31 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Yuri Baranov YaMaps for WordPress allows Stored XSS. This issue affects YaMaps for WordPress: from n/a through 0.6.31.	Patched by core rule	Y
CVE-2025-32173	WordPress B Blocks - The ultimate block collection plugin <= 2.0.0 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins B Blocks - The ultimate block collection allows Stored XSS. This issue affects B Blocks - The ultimate block collection: from n/a through 2.0.0.	Patched by core rule	Y
CVE-2025-32174	WordPress Tockify Events Calendar plugin <= 2.2.13 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tockify Tockify Events Calendar allows DOM-Based XSS. This issue affects Tockify Events Calendar: from n/a through 2.2.13.	Patched by core rule	Y
CVE-2025-32175	WordPress VK Filter Search plugin <= 2.14.1.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vektor,Inc. VK Filter Search allows Stored XSS. This issue affects VK Filter Search: from n/a through 2.14.1.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-32176	WordPress Gallery Blocks with Lightbox plugin <= 3.2.5 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GalleryCreator Gallery Blocks with Lightbox allows Stored XSS. This issue affects Gallery Blocks with Lightbox: from n/a through 3.2.5.	Patched by core rule	Y
CVE-2025-32177	WordPress Embed Chessboard plugin <= 3.07.00 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pgn4web Embed Chessboard allows Stored XSS. This issue affects Embed Chessboard: from n/a through 3.07.00.	Patched by core rule	Y
CVE-2025-32179	WordPress Maps for WP Plugin <= 1.2.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in icopydoc Maps for WP allows Stored XSS. This issue affects Maps for WP: from n/a through 1.2.4.	Patched by core rule	Y
CVE-2025-32181	WordPress Search, Filters & Merchandising for WooCommerce plugin <= 3.0.57 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fast Simon Search, Filters & Merchandising for WooCommerce allows Stored XSS. This issue affects Search, Filters & Merchandising for WooCommerce: from n/a through 3.0.57.	Patched by core rule	Y
CVE-2025-32182	WordPress Spider Elements – Addons for Elementor plugin <= 1.6.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Spider Themes Spider Elements – Addons for Elementor allows Stored XSS. This issue affects Spider Elements – Addons for Elementor: from n/a through 1.6.2.	Patched by core rule	Y
CVE-2025-32183	WordPress Video Playlist For YouTube plugin <= 6.6 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Galaxy Weblinks Video Playlist For YouTube allows Stored XSS. This issue affects Video Playlist For YouTube: from n/a through 6.6.	Patched by core rule	Y
CVE-2025-32184	WordPress Ultimate Store Kit Elementor Addons plugin <= 2.4.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bdthemes Ultimate Store Kit Elementor Addons allows Stored XSS. This issue affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Ultimate Store Kit Elementor Addons: from n/a through 2.4.0.		
CVE-2025-32185	WordPress Colibri Page Builder plugin <= 1.0.319 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Extend Themes Colibri Page Builder allows Stored XSS. This issue affects Colibri Page Builder: from n/a through 1.0.319.	Patched by core rule	Y
CVE-2025-32186	WordPress Turbo Addons for Elementor plugin <= 1.7.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Turbo Addons Turbo Addons for Elementor allows DOM-Based XSS. This issue affects Turbo Addons for Elementor: from n/a through 1.7.1.	Patched by core rule	Y
CVE-2025-32187	WordPress Administrator Z plugin <= 2025.03.04 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Quý Lê 91 Administrator Z allows DOM-Based XSS. This issue affects Administrator Z: from n/a through 2025.03.04.	Patched by core rule	Y
CVE-2025-32188	WordPress Advanced Woo Labels plugin <= 2.14 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ILLID Advanced Woo Labels allows Stored XSS. This issue affects Advanced Woo Labels: from n/a through 2.14.	Patched by core rule	Y
CVE-2025-32189	WordPress BWD Elementor Addons plugin <= 4.3.20 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Best WP Developer BWD Elementor Addons allows DOM-Based XSS. This issue affects BWD Elementor Addons: from n/a through 4.3.20.	Patched by core rule	Y
CVE-2025-3219	CodeCanyon Perfex CRM Project Discussions Module 2 cross site scripting	A vulnerability was found in CodeCanyon Perfex CRM 3.2.1. It has been classified as problematic. Affected is an unknown function of the file /perfex/clients/project/2 of the component Project Discussions Module. The manipulation of the argument description leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and may be used.		
CVE-2025-32190	WordPress Musician's Pack for Elementor plugin <= 1.8.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in smartwpress Musician's Pack for Elementor allows DOM-Based XSS. This issue affects Musician's Pack for Elementor: from n/a through 1.8.4.	Patched by core rule	Y
CVE-2025-32191	WordPress News Element Elementor Blog Magazine plugin <= 1.0.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webangon News Element Elementor Blog Magazine allows DOM-Based XSS. This issue affects News Element Elementor Blog Magazine: from n/a through 1.0.7.	Patched by core rule	Y
CVE-2025-32192	WordPress Ultra Addons Lite for Elementor plugin <= 1.1.8 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in UltraPress Ultra Addons Lite for Elementor allows Stored XSS. This issue affects Ultra Addons Lite for Elementor: from n/a through 1.1.8.	Patched by core rule	Y
CVE-2025-32193	WordPress Simple WP Events plugin <= 1.8.17 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPMinds Simple WP Events allows Stored XSS. This issue affects Simple WP Events: from n/a through 1.8.17.	Patched by core rule	Y
CVE-2025-32194	WordPress LA-Studio Element Kit for Elementor plugin <= 1.4.9 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LA-Studio LA-Studio Element Kit for Elementor allows Stored XSS. This issue affects LA-Studio Element Kit for Elementor: from n/a through 1.4.9.	Patched by core rule	Y
CVE-2025-32195	WordPress Ecwid Shopping Cart plugin <= 7.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ecwid by Lightspeed Ecommerce Shopping Cart Ecwid Shopping Cart allows Stored XSS. This issue affects Ecwid Shopping Cart: from n/a through 7.0.	Patched by core rule	Y
CVE-2025-32196	WordPress News Kit Elementor Addons plugin <= 1.3.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in blazethemes News Kit	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Elementor Addons allows Stored XSS. This issue affects News Kit Elementor Addons: from n/a through 1.3.1.		
CVE-2025-32197	WordPress Piotnet Addons For Elementor plugin <= 2.4.34 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in piotnetdotcom Piotnet Addons For Elementor allows Stored XSS. This issue affects Piotnet Addons For Elementor: from n/a through 2.4.34.	Patched by core rule	Y
CVE-2025-32198	WordPress Brizy plugin <= 2.6.14 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themefusecom Brizy. This issue affects Brizy: from n/a through 2.6.14.	Patched by core rule	Y
CVE-2025-32199	WordPress Contact Form Builder by vcita plugin <= 4.10.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eyale-vc Contact Form Builder by vcita. This issue affects Contact Form Builder by vcita: from n/a through 4.10.2.	Patched by core rule	Y
CVE-2025-32207	WordPress Ni WooCommerce Cost Of Goods plugin <= 3.2.8 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Anzar Ahmed Ni WooCommerce Cost Of Goods allows Stored XSS. This issue affects Ni WooCommerce Cost Of Goods: from n/a through 3.2.8.	Patched by core rule	Y
CVE-2025-32211	WordPress Broadstreet plugin <= 1.51.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Broadstreet Broadstreet allows Stored XSS. This issue affects Broadstreet: from n/a through 1.51.2.	Patched by core rule	Y
CVE-2025-32214	WordPress Hive Support plugin <= 1.2.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hive Support Hive Support allows Stored XSS. This issue affects Hive Support: from n/a through 1.2.2.	Patched by core rule	Y
CVE-2025-32215	WordPress Accessibility Suite plugin <= 4.18 - Arbitrary File Upload vulnerability	Unrestricted Upload of File with Dangerous Type vulnerability in Ability, Inc Accessibility Suite by Online ADA allows Stored XSS. This issue affects Accessibility Suite by Online ADA: from	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		n/a through 4.18.		
CVE-2025-32230	WordPress Tutor LMS plugin <= 3.4.0 - HTML Injection vulnerability	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Themeum Tutor LMS. This issue affects Tutor LMS: from n/a through 3.4.0.	Patched by core rule	Y
CVE-2025-32379	XSS at ctx.redirect() function in Koajs	Koa is expressive middleware for Node.js using ES2017 async functions. In koa < 2.16.1 and < 3.0.0-alpha.5, passing untrusted user input to ctx.redirect() even after sanitizing it, may execute javascript code on the user who use the app. This issue is patched in 2.16.1 and 3.0.0-alpha.5.	Patched by core rule	Y
CVE-2025-32388	SvelteKit allows XSS via tracked search_params	SvelteKit is a framework for rapidly developing robust, performant web applications using Svelte. Prior to 2.20.6 , unsanitized search param names cause XSS vulnerability. You are affected if you iterate over all entries of event.url.searchParams inside a server load function. Attackers can exploit it by crafting a malicious URL and getting a user to click a link with said URL. This vulnerability is fixed in 2.20.6.	Patched by core rule	Y
CVE-2025-32391	HedgeDoc allows XSS possibility through malicious SVG uploads	HedgeDoc is an open source, real-time, collaborative, markdown notes application. Prior to 1.10.3, a malicious SVG file uploaded to HedgeDoc results in the possibility of XSS when opened in a new tab instead of the editor itself. The XSS is possible by exploiting the JSONP capabilities of GitHub Gist embeddings. Only instances with the local filesystem upload backend or special configurations, where the uploads are served from the same domain as HedgeDoc, are vulnerable. This vulnerability is fixed in 1.10.3. When upgrading to HedgeDoc 1.10.3 is not possible, instance owners could add the following headers for all routes under /uploads as a first-countermeasure: Content-Disposition: attachment and Content-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Security-Policy: default-src 'none'. Additionally, the external URLs in the script-src attribute of the Content-Security-Policy header should be removed.		
CVE-2025-32413	N/A	Vulnerability-Lookup before 2.7.1 allows stored XSS via a user bio in website/web/views/user.py.	Patched by core rule	Y
CVE-2025-32426	Formie has a XSS vulnerability for email notification content for preview	Formie is a Craft CMS plugin for creating forms. Prior to version 2.1.44, it is possible to inject malicious code into the HTML content of an email notification, which is then rendered on the preview. There is no issue when rendering the email via normal means (a delivered email). This would require access to the form's email notification settings. This has been fixed in Formie 2.1.44.	Patched by core rule	Y
CVE-2025-32427	Formie has a XSS vulnerability for importing forms	Formie is a Craft CMS plugin for creating forms. Prior to 2.1.44, when importing a form from JSON, if the field label or handle contained malicious content, the output wasn't correctly escaped when viewing a preview of what was to be imported. As imports are undertaking primarily by users who have themselves exported the form from one environment to another, and would require direct manipulation of the JSON export, this is marked as moderate. This vulnerability will not occur unless someone deliberately tampers with the export. This vulnerability is fixed in 2.1.44.	Patched by core rule	Y
CVE-2025-3246	Markdown math block sanitization bypass allows privilege escalation and unauthorized workflow triggers	An improper neutralization of input vulnerability was identified in GitHub Enterprise Server that allowed cross-site scripting in GitHub Markdown that used `$$..$$` math blocks. Exploitation required access to the target GitHub Enterprise Server instance and privileged user interaction with the malicious elements. This vulnerability affected version 3.16.1 of GitHub Enterprise Server and was fixed in version 3.16.2. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability was reported via the GitHub Bug Bounty program.		
CVE-2025-32483	WordPress Request Call Back <= 1.4.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Scott Salisbury Request Call Back allows Stored XSS. This issue affects Request Call Back: from n/a through 1.4.1.	Patched by core rule	Y
CVE-2025-32488	WordPress Aria Font <= 1.4 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in آریا وردپرس Aria Font allows Stored XSS. This issue affects Aria Font: from n/a through 1.4.	Patched by core rule	Y
CVE-2025-32489	WordPress Wetterwarner <= 2.7.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tim Wetterwarner allows Stored XSS. This issue affects Wetterwarner: from n/a through 2.7.2.	Patched by core rule	Y
CVE-2025-32490	WordPress wp secure <= 1.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebsiteDefender wp secure allows Stored XSS. This issue affects wp secure: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-32492	WordPress Admin Menu Post List <= 2.0.7 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Eliot Akira Admin Menu Post List allows Stored XSS. This issue affects Admin Menu Post List: from n/a through 2.0.7.	Patched by core rule	Y
CVE-2025-32493	WordPress BP Social Connect <= 1.6.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VibeThemes BP Social Connect allows Stored XSS. This issue affects BP Social Connect: from n/a through 1.6.2.	Patched by core rule	Y
CVE-2025-32495	WordPress Waymark <= 1.5.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Joe Waymark allows Stored XSS. This issue affects Waymark: from n/a through 1.5.2.	Patched by core rule	Y
CVE-2025-32503	WordPress Link Shield	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	plugin <= 0.5.4 - CSRF to Stored Cross Site Scripting (XSS) vulnerability	Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jose Conti Link Shield allows Stored XSS. This issue affects Link Shield: from n/a through 0.5.4.	rule	
CVE-2025-32504	WordPress Silvasoft boekhouden plugin <= 3.0.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in silvasoft Silvasoft boekhouden allows Reflected XSS. This issue affects Silvasoft boekhouden: from n/a through 3.0.5.	Patched by core rule	Y
CVE-2025-32506	WordPress AT Internet SmartTag plugin <= 0.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BenDlz AT Internet SmartTag allows Reflected XSS. This issue affects AT Internet SmartTag: from n/a through 0.2.	Patched by core rule	Y
CVE-2025-32507	WordPress Event Espresso plugin <= 1.0.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aakif Kadiwala Event Espresso – Custom Email Template Shortcode allows Reflected XSS. This issue affects Event Espresso – Custom Email Template Shortcode: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-32508	WordPress Course Booking System plugin <= 6.0.7 - Reflected Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ComMotion Course Booking System allows Reflected XSS. This issue affects Course Booking System: from n/a through 6.0.7.	Patched by core rule	Y
CVE-2025-3251	xujiangfei admintwo updateSet cross site scripting	A vulnerability, which was classified as problematic, was found in xujiangfei admintwo 1.0. This affects an unknown part of the file /user/updateSet. The manipulation of the argument motto leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-32511	WordPress Make Email Customizer for WooCommerce plugin <= 1.0.5 - Reflected Cross	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Site Scripting (XSS) vulnerability	Excellent Dynamics Make Email Customizer for WooCommerce allows Reflected XSS. This issue affects Make Email Customizer for WooCommerce: from n/a through 1.0.5.		
CVE-2025-32512	WordPress Revamp CRM for WooCommerce plugin <= 1.1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in revampcrm Revamp CRM for WooCommerce allows Reflected XSS. This issue affects Revamp CRM for WooCommerce: from n/a through 1.1.2.	Patched by core rule	Y
CVE-2025-32513	WordPress Total processing card payments for WooCommerce plugin <= 7.1.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in totalprocessing Nomupay Payment Processing Gateway allows Reflected XSS. This issue affects Nomupay Payment Processing Gateway: from n/a through 7.1.6.	Patched by core rule	Y
CVE-2025-32514	WordPress WooCommerce Estimate and Quote plugin <= 1.0.2.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cscode WooCommerce Estimate and Quote allows Reflected XSS. This issue affects WooCommerce Estimate and Quote: from n/a through 1.0.2.5.	Patched by core rule	Y
CVE-2025-32515	WordPress Terminal Africa plugin <= 1.13.17 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in terminalafrica Terminal Africa allows Reflected XSS. This issue affects Terminal Africa: from n/a through 1.13.17.	Patched by core rule	Y
CVE-2025-32516	WordPress Related Videos for JW Player plugin <= 1.2.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ilGhera Related Videos for JW Player allows Reflected XSS. This issue affects Related Videos for JW Player: from n/a through 1.2.0.	Patched by core rule	Y
CVE-2025-32517	WordPress MultiMailer plugin <= 1.0.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SCAND MultiMailer allows Reflected XSS. This issue	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects MultiMailer: from n/a through 1.0.3.		
CVE-2025-3252	xujiangfei admintwo add cross site scripting	A vulnerability has been found in xujiangfei admintwo 1.0 and classified as problematic. This vulnerability affects unknown code of the file /resource/add. The manipulation of the argument Name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-32520	WordPress WordPress Health and Server Condition plugin <= 4.1.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in M. Ali Saleem WordPress Health and Server Condition – Integrated with Google Page Speed allows Reflected XSS. This issue affects WordPress Health and Server Condition – Integrated with Google Page Speed: from n/a through 4.1.1.	Patched by core rule	Y
CVE-2025-32521	WordPress Cool Flipbox plugin <= 1.8.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CoolHappy Cool Flipbox – Shortcode & Gutenberg Block allows Reflected XSS. This issue affects Cool Flipbox – Shortcode & Gutenberg Block: from n/a through 1.8.3.	Patched by core rule	Y
CVE-2025-32522	WordPress License Manager for WooCommerce plugin <= 3.0.9 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPExperts.io License Manager for WooCommerce allows Reflected XSS. This issue affects License Manager for WooCommerce: from n/a through 3.0.9.	Patched by core rule	Y
CVE-2025-32523	WordPress WooCommerce – Payphone Gateway plugin <= 3.2.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in payphone WooCommerce – Payphone Gateway allows Reflected XSS. This issue affects WooCommerce – Payphone Gateway: from n/a through 3.2.0.	Patched by core rule	Y
CVE-2025-32524	WordPress MyWorks WooCommerce Sync for QuickBooks Online plugin	Improper Neutralization of Input During Web Page Generation ('Cross-site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	<= 2.9.1 - Reflected Cross Site Scripting (XSS) vulnerability	Scripting') vulnerability in MyWorks MyWorks WooCommerce Sync for QuickBooks Online allows Reflected XSS. This issue affects MyWorks WooCommerce Sync for QuickBooks Online: from n/a through 2.9.1.		
CVE-2025-32525	WordPress Interactive Geo Maps plugin <= 1.6.24 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in interactivegeomaps Interactive Geo Maps allows Reflected XSS. This issue affects Interactive Geo Maps: from n/a through 1.6.24.	Patched by core rule	Y
CVE-2025-32526	WordPress Zephyr Project Manager plugin <= 3.3.101 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dylan James Zephyr Project Manager allows Reflected XSS. This issue affects Zephyr Project Manager: from n/a through 3.3.101.	Patched by core rule	Y
CVE-2025-32527	WordPress T&P Gallery Slider plugin <= 1.2 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pey22 T&P Gallery Slider allows Stored XSS. This issue affects T&P Gallery Slider: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-32528	WordPress iCal Feeds Plugin <= 1.5.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in maximevalette iCal Feeds allows Reflected XSS. This issue affects iCal Feeds: from n/a through 1.5.3.	Patched by core rule	Y
CVE-2025-32529	WordPress iONE360 configurator plugin <= 2.0.56 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in iONE360 iONE360 configurator allows Reflected XSS. This issue affects iONE360 configurator: from n/a through 2.0.56.	Patched by core rule	Y
CVE-2025-3253	xujiangfei admintwo insertTree cross site scripting	A vulnerability was found in xujiangfei admintwo 1.0 and classified as problematic. This issue affects some unknown processing of the file /ztree/insertTree. The manipulation of the argument Name leads to cross site scripting. The attack may be initiated	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-32530	WordPress Wallet System for WooCommerce plugin <= 2.6.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Swings Wallet System for WooCommerce allows Reflected XSS. This issue affects Wallet System for WooCommerce: from n/a through 2.6.5.	Patched by core rule	Y
CVE-2025-32531	WordPress Arconix FAQ plugin <= 1.9.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tychesoftwares Arconix FAQ allows Reflected XSS. This issue affects Arconix FAQ: from n/a through 1.9.5.	Patched by core rule	Y
CVE-2025-32532	WordPress UXsniff Plugin <= 1.2.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pei Yong Goh UXsniff allows Reflected XSS. This issue affects UXsniff: from n/a through 1.2.4.	Patched by core rule	Y
CVE-2025-32533	WordPress Deliver via Shipos for WooCommerce Plugin <= 2.1.7 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Matat Technologies Deliver via Shipos for WooCommerce allows Reflected XSS. This issue affects Deliver via Shipos for WooCommerce: from n/a through 2.1.7.	Patched by core rule	Y
CVE-2025-32534	WordPress Workbox Video from Vimeo & Youtube Plugin Plugin <= 3.2.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Workbox Workbox Video from Vimeo & Youtube allows Reflected XSS. This issue affects Workbox Video from Vimeo & Youtube: from n/a through 3.2.2.	Patched by core rule	Y
CVE-2025-32535	WordPress DN Shipping by Weight for WooCommerce Plugin <= 1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in digireturn DN Shipping by Weight for WooCommerce allows Reflected XSS. This issue affects DN Shipping by Weight for WooCommerce: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-32536	WordPress HTML5 Video Player with Playlist Plugin <= 2.50 - Reflected Cross Site Scripting (XSS)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	vulnerability	Sandeep Verma HTML5 Video Player with Playlist allows Reflected XSS. This issue affects HTML5 Video Player with Playlist: from n/a through 2.50.		
CVE-2025-32537	WordPress Lock Your Updates Plugin <= 1.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rachel Cherry Lock Your Updates allows Reflected XSS. This issue affects Lock Your Updates: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-32538	WordPress Easy Post Duplicator Plugin <= 1.0.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in dev02ali Easy Post Duplicator allows Reflected XSS. This issue affects Easy Post Duplicator: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-32539	WordPress WooCommerce – Store Exporter plugin <= 2.7.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Josh Kohlbach WooCommerce – Store Exporter allows Reflected XSS. This issue affects WooCommerce – Store Exporter: from n/a through 2.7.4.	Patched by core rule	Y
CVE-2025-32540	WordPress Feedify – Web Push Notifications plugin <= 2.4.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in feedify Feedify – Web Push Notifications allows Reflected XSS. This issue affects Feedify – Web Push Notifications: from n/a through 2.4.5.	Patched by core rule	Y
CVE-2025-32541	WordPress WooCommerce Sales MIS Report Plugin <= 4.0.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in infosoftplugin WooCommerce Sales MIS Report allows Reflected XSS. This issue affects WooCommerce Sales MIS Report: from n/a through 4.0.3.	Patched by core rule	Y
CVE-2025-32543	WordPress Canonical Attachments Plugin <= 1.7 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hivedigital Canonical Attachments allows Reflected XSS. This issue affects Canonical	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Attachments: from n/a through 1.7.		
CVE-2025-32548	WordPress Hamburger Icon Menu Lite Plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in borisolhor Hamburger Icon Menu Lite allows Reflected XSS. This issue affects Hamburger Icon Menu Lite: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-32551	WordPress Connector to CiviCRM with CiviMcRestFace plugin <= 1.0.8 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jaap Jansma Connector to CiviCRM with CiviMcRestFace allows Reflected XSS. This issue affects Connector to CiviCRM with CiviMcRestFace: from n/a through 1.0.8.	Patched by core rule	Y
CVE-2025-32552	WordPress MSRP (RRP) Pricing for WooCommerce Plugin <= 1.8.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory MSRP (RRP) Pricing for WooCommerce allows Reflected XSS. This issue affects MSRP (RRP) Pricing for WooCommerce: from n/a through 1.8.1.	Patched by core rule	Y
CVE-2025-32553	WordPress RestroPres Plugin <= 3.1.8.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Magnigenie RestroPress allows Reflected XSS. This issue affects RestroPress: from n/a through 3.1.8.4.	Patched by core rule	Y
CVE-2025-32554	WordPress Raptive Ads plugin <= 3.7.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Raptive Raptive Ads allows Reflected XSS. This issue affects Raptive Ads: from n/a through 3.7.3.	Patched by core rule	Y
CVE-2025-32557	WordPress WP Featured Screenshot Plugin <= 1.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rico Macchi WP Featured Screenshot allows Reflected XSS. This issue affects WP Featured Screenshot: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-32560	WordPress WP-Hijri Plugin <= 1.5.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mohammad I. Okfie WP-Hijri allows Reflected XSS. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		issue affects WP-Hijri: from n/a through 1.5.3.		
CVE-2025-32561	WordPress WP_DEBUG Toggle plugin <= 1.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in plugins.club WP_DEBUG Toggle allows Reflected XSS. This issue affects WP_DEBUG Toggle: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-32562	WordPress WP Easy Poll Plugin <= 2.2.9 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in aviplugins.com WP Easy Poll allows Reflected XSS. This issue affects WP Easy Poll: from n/a through 2.2.9.	Patched by core rule	Y
CVE-2025-32564	WordPress Stop Registration Spam Plugin <= 1.24 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tomroyal Stop Registration Spam allows Reflected XSS. This issue affects Stop Registration Spam: from n/a through 1.24.	Patched by core rule	Y
CVE-2025-32566	WordPress License For Envato Plugin <= 1.0.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ashraful Sarkar Naiem License For Envato allows Reflected XSS. This issue affects License For Envato: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-32570	WordPress ChillPay WooCommerce Plugin <= 2.5.3 - CSRF to Stored XSS vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ChillPay ChillPay WooCommerce allows Stored XSS. This issue affects ChillPay WooCommerce: from n/a through 2.5.3.	Patched by core rule	Y
CVE-2025-32578	WordPress Coming Soon Countdown Plugin <= 2.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mapro Collins Coming Soon Countdown allows Reflected XSS. This issue affects Coming Soon Countdown: from n/a through 2.2.	Patched by core rule	Y
CVE-2025-32580	WordPress DeBounce Email Validator plugin <= 5.7.1 - CSRF to Stored XSS vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in debounce DeBounce Email Validator allows Stored XSS. This issue affects DeBounce Email Validator: from n/a through 5.7.1.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-32581	WordPress WordPress Spam Blocker Plugin <= 2.0.4 - CSRF to Stored XSS vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ankit Singla WordPress Spam Blocker allows Stored XSS. This issue affects WordPress Spam Blocker: from n/a through 2.0.4.	Patched by core rule	Y
CVE-2025-32582	WordPress WP AutoKeyword Plugin <= 1.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in EXEIdeas International WP AutoKeyword allows Stored XSS. This issue affects WP AutoKeyword: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-32586	WordPress ABA PayWay Payment Gateway for WooCommerce Plugin <= 2.1.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ABA Bank ABA PayWay Payment Gateway for WooCommerce allows Reflected XSS. This issue affects ABA PayWay Payment Gateway for WooCommerce: from n/a through 2.1.3.	Patched by core rule	Y
CVE-2025-32588	WordPress Credova_Financial plugin <= 2.4.8 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Credova Financial Credova_Financial allows Reflected XSS. This issue affects Credova_Financial: from n/a through 2.4.8.	Patched by core rule	Y
CVE-2025-32590	WordPress Web2application Plugin <= 5.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tzin111 Web2application allows Reflected XSS. This issue affects Web2application: from n/a through 5.6.	Patched by core rule	Y
CVE-2025-32592	WordPress TableOn Plugin <= 1.0.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RealMag777 TableOn – WordPress Posts Table Filterable allows Stored XSS. This issue affects TableOn – WordPress Posts Table Filterable: from n/a through 1.0.3.	Patched by core rule	Y
CVE-2025-32598	WordPress WP Table Builder plugin <= 2.0.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Table Builder WP Table	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Builder allows Reflected XSS. This issue affects WP Table Builder: from n/a through 2.0.4.		
CVE-2025-32599	WordPress Task Scheduler Plugin <= 1.6.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in miunosoft Task Scheduler allows Reflected XSS. This issue affects Task Scheduler: from n/a through 1.6.3.	Patched by core rule	Y
CVE-2025-32600	WordPress Tournamatch Plugin <= 4.6.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tournamatch Tournamatch allows Reflected XSS. This issue affects Tournamatch: from n/a through 4.6.1.	Patched by core rule	Y
CVE-2025-32601	WordPress Twispay Credit Card Payments Plugin <= 2.1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in twispay Twispay Credit Card Payments allows Reflected XSS. This issue affects Twispay Credit Card Payments: from n/a through 2.1.2.	Patched by core rule	Y
CVE-2025-32602	WordPress WooMS Plugin <= 9.12 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in aiiddqd WooMS allows Reflected XSS. This issue affects WooMS: from n/a through 9.12.	Patched by core rule	Y
CVE-2025-32604	WordPress AWSA Shipping Plugin <= 1.3.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sajjad Aslani AWSA Shipping allows Reflected XSS. This issue affects AWSA Shipping: from n/a through 1.3.0.	Patched by core rule	Y
CVE-2025-32605	WordPress MemberPress Discord Addon Plugin <= 1.1.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in expresstechsoftware MemberPress Discord Addon allows Reflected XSS. This issue affects MemberPress Discord Addon: from n/a through 1.1.1.	Patched by core rule	Y
CVE-2025-32608	WordPress Movylo Marketing Automation Plugin <= 2.0.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Movylo Movylo Marketing Automation allows Reflected XSS. This issue affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Movylo Marketing Automation: from n/a through 2.0.7.		
CVE-2025-32609	WordPress Verowa Connect Plugin <= 3.0.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Picture-Planet GmbH Verowa Connect allows Reflected XSS. This issue affects Verowa Connect: from n/a through 3.0.4.	Patched by core rule	Y
CVE-2025-32611	WordPress WooCommerce TBC Credit Card Payment Gateway (Free) Plugin <= 2.0.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in We Are De WooCommerce TBC Credit Card Payment Gateway (Free) allows Reflected XSS. This issue affects WooCommerce TBC Credit Card Payment Gateway (Free): from n/a through 2.0.0.	Patched by core rule	Y
CVE-2025-32613	WordPress Debug Log Manager plugin <= 2.3.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bowo Debug Log Manager allows Stored XSS. This issue affects Debug Log Manager: from n/a through 2.3.4.	Patched by core rule	Y
CVE-2025-32615	WordPress Clinked Client Portal Plugin <= 1.10 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Clinked Clinked Client Portal allows Reflected XSS. This issue affects Clinked Client Portal: from n/a through 1.10.	Patched by core rule	Y
CVE-2025-32622	WordPress OTP-less one tap Sign in Plugin <= 2.0.58 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in OTP-less OTP-less one tap Sign in allows Reflected XSS. This issue affects OTP-less one tap Sign in: from n/a through 2.0.58.	Patched by core rule	Y
CVE-2025-32625	WordPress Mobile Blocks Plugin <= 1.0.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pootlepress Mobile Pages allows Reflected XSS. This issue affects Mobile Pages: from n/a through 1.0.2.	Patched by core rule	Y
CVE-2025-32628	WordPress Crowdfunding for WooCommerce Plugin <= 3.1.12 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Wham Crowdfunding for WooCommerce allows	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Reflected XSS. This issue affects Crowdfunding for WooCommerce: from n/a through 3.1.12.		
CVE-2025-32630	WordPress WP-BusinessDirectory Plugin <= 3.1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CMSJunkie - WordPress Business Directory Plugins WP-BusinessDirectory allows Reflected XSS. This issue affects WP-BusinessDirectory: from n/a through 3.1.2.	Patched by core rule	Y
CVE-2025-32632	WordPress Automatic Ban IP Plugin <= 1.0.7 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in KaizenCoders Automatic Ban IP allows Reflected XSS. This issue affects Automatic Ban IP: from n/a through 1.0.7.	Patched by core rule	Y
CVE-2025-32634	WordPress Run Contests, Raffles, and Giveaways Plugin <= 2.0.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mdedev Run Contests, Raffles, and Giveaways with ContestsWP allows Reflected XSS. This issue affects Run Contests, Raffles, and Giveaways with ContestsWP: from n/a through 2.0.6.	Patched by core rule	Y
CVE-2025-32637	WordPress WP Donate Plugin <= 2.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ketanajani WP Donate allows Stored XSS. This issue affects WP Donate: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-32638	WordPress ShopApper plugin <= 0.4.39 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in weptile ShopApper allows Stored XSS. This issue affects ShopApper: from n/a through 0.4.39.	Patched by core rule	Y
CVE-2025-32639	WordPress Affiliate Links plugin <= 3.1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wecantrack Affiliate Links Lite allows Reflected XSS. This issue affects Affiliate Links Lite: from n/a through 3.1.0.	Patched by core rule	Y
CVE-2025-32640	WordPress One Click Accessibility plugin <= 3.1.0 - Cross-Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Elementor One Click	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Accessibility allows Stored XSS. This issue affects One Click Accessibility: from n/a through 3.1.0.		
CVE-2025-32646	WordPress Question Answer Plugin <= 1.2.70 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PickPlugins Question Answer allows Reflected XSS. This issue affects Question Answer: from n/a through 1.2.70.	Patched by core rule	Y
CVE-2025-32649	WordPress GB Gallery Slideshow Plugin <= 1.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gb-plugins GB Gallery Slideshow allows Reflected XSS. This issue affects GB Gallery Slideshow: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-32651	WordPress SERPed.net Plugin <= 4.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in serpednet SERPed.net allows Reflected XSS. This issue affects SERPed.net: from n/a through 4.6.	Patched by core rule	Y
CVE-2025-32653	WordPress Cart66 Cloud Plugin <= 2.3.7 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Lee Blue Cart66 Cloud allows Reflected XSS. This issue affects Cart66 Cloud: from n/a through 2.3.7.	Patched by core rule	Y
CVE-2025-32666	WordPress Hive Support plugin <= 1.2.2- Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hive Support Hive Support allows Reflected XSS. This issue affects Hive Support: from n/a through 1.2.2.	Patched by core rule	Y
CVE-2025-32670	WordPress Spark GF Failed Submissions plugin <= 1.3.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mark Parnell Spark GF Failed Submissions allows Reflected XSS. This issue affects Spark GF Failed Submissions: from n/a through 1.3.5.	Patched by core rule	Y
CVE-2025-32674	WordPress Product Excel Import Export & Bulk Edit for WooCommerce plugin <= 4.7 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Product Excel Import Export & Bulk Edit for WooCommerce allows Reflected XSS. This issue	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects Product Excel Import Export & Bulk Edit for WooCommerce: from n/a through 4.7.		
CVE-2025-32680	WordPress Review Stream plugin <= 1.6.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Grade Us, Inc. Review Stream allows Stored XSS. This issue affects Review Stream: from n/a through 1.6.7.	Patched by core rule	Y
CVE-2025-32683	WordPress MapSVG Lite plugin <= 8.5.32 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RomanCode MapSVG Lite allows DOM-Based XSS. This issue affects MapSVG Lite: from n/a through 8.5.32.	Patched by core rule	Y
CVE-2025-32690	WordPress PowerPress Podcasting <= 11.12.4 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Angelo Mandato PowerPress Podcasting allows DOM-Based XSS. This issue affects PowerPress Podcasting: from n/a through 11.12.4.	Patched by core rule	Y
CVE-2025-32960	CUBA Generic REST API Vulnerable to Cross-Site Scripting (XSS) in the /files Endpoint	The CUBA REST API add-on performs operations on data and entities. Prior to version 7.2.7, the input parameter, which consists of a file path and name, can be manipulated to return the Content-Type header with text/html if the name part ends with .html. This could allow malicious JavaScript code to be executed in the browser. For a successful attack, a malicious file needs to be uploaded beforehand. This issue has been patched in version 7.2.7. A workaround is provided on the Jmix documentation website.	Patched by core rule	Y
CVE-2025-32961	CUBA JPA Web API Vulnerable to Cross-Site Scripting (XSS) in the /download Endpoint	The Cuba JPA web API enables loading and saving any entities defined in the application data model by sending simple HTTP requests. Prior to version 1.1.1, the input parameter, which consists of a file path and name, can be manipulated to return the Content-Type header with text/html if the name part ends with .html. This could allow malicious JavaScript code to be executed in the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		browser. For a successful attack, a malicious file needs to be uploaded beforehand. This issue has been patched in version 1.1.1. A workaround is provided on the Jmix documentation website.		
CVE-2025-3297	SourceCodester Online Eyewear Shop Master.php cross site scripting	A vulnerability, which was classified as problematic, was found in SourceCodester Online Eyewear Shop 1.0. Affected is an unknown function of the file /classes/Master.php?f=save_product. The manipulation of the argument brand leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-3326	iteaj iboot 物联网网关 File Upload upload cross site scripting	A vulnerability has been found in iteaj iboot 物联网网关 1.1.3 and classified as problematic. This vulnerability affects unknown code of the file /common/upload of the component File Upload. The manipulation of the argument File leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3327	iteaj iboot 物联网网关 File Upload batch cross site scripting	A vulnerability was found in iteaj iboot 物联网网关 1.1.3 and classified as problematic. This issue affects some unknown processing of the file /common/upload/batch of the component File Upload. The manipulation of the argument File leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3385	LinZhaoguan pb-cms Classification Management Page cross site scripting	A vulnerability was found in LinZhaoguan pb-cms 2.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Classification Management Page. The manipulation of the argument Classification	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3386	LinZhaoguan pb-cms Friendship Link admin#links cross site scripting	A vulnerability was found in LinZhaoguan pb-cms 2.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin#links of the component Friendship Link Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3387	renrenio renren-security JSON cross site scripting	A vulnerability classified as problematic has been found in renrenio renren-security up to 5.4.0. This affects an unknown part of the component JSON Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3388	hailey888 oa_system Frontend LoginsController.java loginCheck cross site scripting	A vulnerability classified as problematic was found in hailey888 oa_system up to 2025.01.01. This vulnerability affects the function loginCheck of the file cn/gson/oasys/controller/login/LoginsController.java of the component Frontend. The manipulation of the argument Username leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available.	Patched by core rule	Y
CVE-2025-3389	hailey888 oa_system Backend InformManageController.java testMess cross site scripting	A vulnerability, which was classified as problematic, has been found in hailey888 oa_system up to 2025.01.01. This issue affects the function testMess of the file cn/gson/oasys/controller/inform/InformManageController.java of the component Backend. The manipulation of the argument menu leads to cross site scripting. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.		
CVE-2025-3390	hailey888 oa_system Backend DaymanageController.java addandchangeday cross site scripting	A vulnerability, which was classified as problematic, was found in hailey888 oa_system up to 2025.01.01. Affected is the function addandchangeday of the file cn/gson/oass/controller/daymanager/DaymanageController.java of the component Backend. The manipulation of the argument scheduleList leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available.	Patched by core rule	Y
CVE-2025-3391	hailey888 oa_system Backend AddrController.java outAddress cross site scripting	A vulnerability has been found in hailey888 oa_system up to 2025.01.01 and classified as problematic. Affected by this vulnerability is the function outAddress of the file cn/gson/oass/controller/address/AddrController. java of the component Backend. The manipulation of the argument outtype leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available.	Patched by core rule	Y
CVE-2025-3392	hailey888 oa_system Backend MailController.java save cross site scripting	A vulnerability was found in hailey888 oa_system up to 2025.01.01 and classified as problematic. Affected by this issue is the function Save of the file cn/gson/oasys/controller/mail/MailController.java of the component Backend. The manipulation of the argument MailNumberId leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available.		
CVE-2025-3393	mrcen springboot-ucan-admin Personal Settings Interface index cross site scripting	A vulnerability was found in mrcen springboot-ucan-admin up to 5f35162032cbe9288a04e429ef35301545143509. It has been classified as problematic. This affects an unknown part of the file /ucan-admin/index of the component Personal Settings Interface. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.	Patched by core rule	Y
CVE-2025-3531	YouDianCMS index.html cross site scripting	A vulnerability classified as problematic has been found in YouDianCMS 9.5.21. This affects an unknown part of the file /App/Tpl/Admin/Default/Log/index.html. The manipulation of the argument UserName/LogType leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-3532	YouDianCMS index.html.Attackers cross site scripting	A vulnerability classified as problematic was found in YouDianCMS 9.5.21. This vulnerability affects unknown code of the file /App/Tpl/Member/Default/Order/index.html.Attackers. The manipulation of the argument OrderNumber leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-3533	YouDianCMS index.html.Attackers cross site scripting	A vulnerability, which was classified as problematic, has been found in YouDianCMS 9.5.21. This issue affects some unknown processing of the file /App/Tpl/Admin/Default/Channel/index.html.Attackers. The manipulation of the argument Parent leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-3568	Webkul Krayin CRM SVG File edit cross site scripting	A vulnerability has been found in Webkul Krayin CRM up to 2.1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/settings/users/edit/ of the component SVG File Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor prepares a fix for the next major release and explains that he does not think therefore that this should qualify for a CVE.	Patched by core rule	Y
CVE-2025-3570	JamesZBL/code-projects db-hospital-drug ContentController.java save cross site scripting	A vulnerability was found in JamesZBL/code-projects db-hospital-drug 1.0. It has been classified as problematic. This affects the function Save of the file ContentController.java. The manipulation of the argument content leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-3591	ZHENFENG13/code-projects My-Blog-layui edit cross site scripting	A vulnerability was found in ZHENFENG13/code-projects My-Blog-layui 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/v1/blog/edit. The manipulation leads to cross site scripting. The attack may be launched remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The exploit has been disclosed to the public and may be used. Multiple parameters might be affected. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-3592	ZHENFENG13/code-projects My-Blog-layui edit cross site scripting	A vulnerability was found in ZHENFENG13/code-projects My-Blog-layui 1.0. It has been classified as problematic. This affects an unknown part of the file /admin/v1/link/edit. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Multiple parameters might be affected. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-3612	Demtec Graphytics HTTP GET Parameter visualization cross site scripting	A vulnerability, which was classified as problematic, was found in Demtec Graphytics 5.0.7. This affects an unknown part of the file /visualization of the component HTTP GET Parameter Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-3613	Demtec Graphytics visualization cross site scripting	A vulnerability has been found in Demtec Graphytics 5.0.7 and classified as problematic. This vulnerability affects unknown code of the file /visualization. The manipulation of the argument description leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-3688	mirweiye Seven Bears Library CMS Background Management Page cross site scripting	A vulnerability, which was classified as problematic, was found in mirweiye Seven Bears Library CMS 2023. This affects an	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown part of the component Background Management Page. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3692	SourceCodester Online Eyewear Shop Master.php cross site scripting	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /oews/classes/Master.php?f=save_product. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3788	baseweb JSite save cross site scripting	A vulnerability was found in baseweb JSite 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /a/sys/user/save. The manipulation of the argument Name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3789	baseweb JSite save cross site scripting	A vulnerability was found in baseweb JSite 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /a/sys/area/save. The manipulation of the argument Name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3795	DaiCuo SEO Optimization Settings Section cross site scripting	A vulnerability was found in DaiCuo 1.3.13. It has been rated as problematic. Affected by this issue is some unknown functionality of the component SEO Optimization Settings Section. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3801	songquanpeng one-api System Setting cross site	A vulnerability was found in songquanpeng one-api up to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	scripting	0.6.10. It has been classified as problematic. This affects an unknown part of the component System Setting Handler. The manipulation of the argument Homepage Content leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3806	dazhouda lecms Edit Profile admin cross site scripting	A vulnerability, which was classified as problematic, has been found in dazhouda lecms up to 3.0.3. Affected by this issue is some unknown functionality of the file /admin of the component Edit Profile Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3821	SourceCodester Web-based Pharmacy Product Management System add-admin.php cross site scripting	A vulnerability was found in SourceCodester Web-based Pharmacy Product Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file add-admin.php. The manipulation of the argument txtpassword/txtfullname/txtemail leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3822	SourceCodester Web-based Pharmacy Product Management System changepassword.php cross site scripting	A vulnerability was found in SourceCodester Web-based Pharmacy Product Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file changepassword.php. The manipulation of the argument txtconfirm_password/txtnew_password/txtold_password leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3823	SourceCodester Web-based Pharmacy Product Management System add-stock.php cross site	A vulnerability classified as problematic has been found in SourceCodester Web-based Pharmacy Product	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	scripting	Management System 1.0. Affected is an unknown function of the file add-stock.php. The manipulation of the argument txttotalcost/txtproductID/txtprice/txtexpirydate leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3824	SourceCodester Web-based Pharmacy Product Management System add-product.php cross site scripting	A vulnerability classified as problematic was found in SourceCodester Web-based Pharmacy Product Management System 1.0. Affected by this vulnerability is an unknown functionality of the file add-product.php. The manipulation of the argument txtprice/txtproduct_name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3825	SourceCodester Web-based Pharmacy Product Management System add-category.php cross site scripting	A vulnerability, which was classified as problematic, has been found in SourceCodester Web-based Pharmacy Product Management System 1.0. Affected by this issue is some unknown functionality of the file add-category.php. The manipulation of the argument txtcategory_name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-3826	SourceCodester Web-based Pharmacy Product Management System add-supplier.php cross site scripting	A vulnerability, which was classified as problematic, was found in SourceCodester Web-based Pharmacy Product Management System 1.0. This affects an unknown part of the file add-supplier.php. The manipulation of the argument txtsupplier_name/txtaddress leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-39382	WordPress ACF: Google Font Selector plugin <= 3.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in danielpataki ACF: Google	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Font Selector allows Reflected XSS. This issue affects ACF: Google Font Selector: from n/a through 3.0.1.		
CVE-2025-39397	WordPress Anything Popup plugin <= 7.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gopiplus@hotmail.com Anything Popup allows Reflected XSS. This issue affects Anything Popup: from n/a through 7.3.	Patched by core rule	Y
CVE-2025-39400	WordPress User Registration plugin < 4.2.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpeverest User Registration allows Reflected XSS. This issue affects User Registration: from n/a through n/a.	Patched by core rule	Y
CVE-2025-39408	WordPress BruteGuard – Brute Force Login Protection plugin <= 0.1.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in EverPress BruteGuard – Brute Force Login Protection allows Reflected XSS. This issue affects BruteGuard – Brute Force Login Protection: from n/a through 0.1.4.	Patched by core rule	Y
CVE-2025-39420	WordPress WP Twitter Button plugin <= 1.4.1 - Cross Site Request Forgery (CSRF) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ruudkok WP Twitter Button allows Stored XSS. This issue affects WP Twitter Button: from n/a through 1.4.1.	Patched by core rule	Y
CVE-2025-39427	WordPress WP Post to PDF Enhanced plugin <= 1.1.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Beth Tucker Long WP Post to PDF Enhanced allows Stored XSS. This issue affects WP Post to PDF Enhanced: from n/a through 1.1.1.	Patched by core rule	Y
CVE-2025-39428	WordPress Gravity Forms CSS Themes with Fontawesome and Placeholders plugin <= 8.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Maros Pristas Gravity Forms CSS Themes with Fontawesome and Placeholders allows Stored XSS. This issue affects Gravity Forms CSS Themes with Fontawesome and Placeholders: from n/a through 8.5.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-39432	WordPress bbPress2 shortcode whitelist plugin <= 2.2.1 - CSRF to XSS vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in antonchanning bbPress2 shortcode whitelist allows Stored XSS. This issue affects bbPress2 shortcode whitelist: from n/a through 2.2.1.	Patched by core rule	Y
CVE-2025-39444	WordPress MaxButtons plugin <= 9.8.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in maxfoundry MaxButtons allows Stored XSS. This issue affects MaxButtons: from n/a through 9.8.3.	Patched by core rule	Y
CVE-2025-39464	WordPress AdminQuickbar plugin <= 1.9.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rtowebsites AdminQuickbar allows Reflected XSS. This issue affects AdminQuickbar: from n/a through 1.9.1.	Patched by core rule	Y
CVE-2025-39469	WordPress Modal Survey plugin <= 2.0.2.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pantherius Modal Survey allows Reflected XSS.This issue affects Modal Survey: from n/a through 2.0.2.0.1.	Patched by core rule	Y
CVE-2025-39514	WordPress Asgaros Forum <= 3.0.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Asgaros Asgaros Forum allows Stored XSS. This issue affects Asgaros Forum: from n/a through 3.0.0.	Patched by core rule	Y
CVE-2025-39515	WordPress Attendance Manager <= 0.6.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tnomi Attendance Manager allows Stored XSS. This issue affects Attendance Manager: from n/a through 0.6.2.	Patched by core rule	Y
CVE-2025-39516	WordPress Author WIP Progress Bar <= 1.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alan Petersen Author WIP Progress Bar allows DOM-Based XSS. This issue affects Author WIP Progress Bar: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-39519	WordPress Bulk Page Stub Creator plugin <= 1.1 - Reflected Cross Site	Improper Neutralization of Input During Web Page Generation ('Cross-site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Scripting (XSS) vulnerability	Scripting') vulnerability in rtpHarry Bulk Page Stub Creator allows Reflected XSS. This issue affects Bulk Page Stub Creator: from n/a through 1.1.		
CVE-2025-39520	WordPress Checkout Files Upload for WooCommerce <= 2.2.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Wham Checkout Files Upload for WooCommerce allows Stored XSS. This issue affects Checkout Files Upload for WooCommerce: from n/a through 2.2.0.	Patched by core rule	Y
CVE-2025-39521	WordPress Contact Form vCard Generator plugin <= 2.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ashish Ajani Contact Form vCard Generator allows Reflected XSS. This issue affects Contact Form vCard Generator: from n/a through 2.4.	Patched by core rule	Y
CVE-2025-39524	WordPress Html5 Audio Player <= 2.2.28 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in bPlugins Html5 Audio Player allows Stored XSS. This issue affects Html5 Audio Player: from n/a through 2.2.28.	Patched by core rule	Y
CVE-2025-39525	WordPress Logo Carousel Slider <= 2.1.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpWax Logo Carousel Slider allows Stored XSS. This issue affects Logo Carousel Slider: from n/a through 2.1.3.	Patched by core rule	Y
CVE-2025-39528	WordPress Rescue Shortcodes plugin <= 3.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rescue Themes Rescue Shortcodes allows Stored XSS. This issue affects Rescue Shortcodes: from n/a through 3.1.	Patched by core rule	Y
CVE-2025-39529	WordPress Scriptless Social Sharing <= 3.2.4 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Robin Cornett Scriptless Social Sharing allows Stored XSS. This issue affects Scriptless Social Sharing: from n/a through 3.2.4.	Patched by core rule	Y
CVE-2025-39540	WordPress WP Flipclock plugin <= 1.9 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Rhys Wynne WP Flipclock allows DOM-Based XSS. This issue affects WP Flipclock: from n/a through 1.9.		
CVE-2025-39543	WordPress Royal Elementor Addons plugin <= 1.3.977 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Royal Royal Elementor Addons allows Stored XSS. This issue affects Royal Elementor Addons: from n/a through 1.3.977.	Patched by core rule	Y
CVE-2025-39549	WordPress Most And Least Read Posts Widget <= 2.5.20 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in whiletrue Most And Least Read Posts Widget allows Stored XSS. This issue affects Most And Least Read Posts Widget: from n/a through 2.5.20.	Patched by core rule	Y
CVE-2025-39555	WordPress Church Admin plugin <= 5.0.23 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in andy_moyle Church Admin allows Stored XSS. This issue affects Church Admin: from n/a through 5.0.23.	Patched by core rule	Y
CVE-2025-39558	WordPress CRM Perks plugin <= 1.1.7 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CRM Perks CRM Perks allows Reflected XSS. This issue affects CRM Perks: from n/a through 1.1.7.	Patched by core rule	Y
CVE-2025-39562	WordPress Payment Form for PayPal Pro <= 1.1.72 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in codepeople Payment Form for PayPal Pro allows Stored XSS. This issue affects Payment Form for PayPal Pro: from n/a through 1.1.72.	Patched by core rule	Y
CVE-2025-39567	WordPress Web Directory Free plugin <= 1.7.8 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Shamalli Web Directory Free allows Reflected XSS. This issue affects Web Directory Free: from n/a through 1.7.8.	Patched by core rule	Y
CVE-2025-39572	WordPress Checkout for PayPal <= 1.0.38 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Noor Alam Checkout for PayPal allows Stored XSS.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This issue affects Checkout for PayPal: from n/a through 1.0.38.		
CVE-2025-39573	WordPress WP Posts Carousel <= 1.3.10 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in teastudio.pl WP Posts Carousel allows Stored XSS. This issue affects WP Posts Carousel: from n/a through 1.3.10.	Patched by core rule	Y
CVE-2025-39574	WordPress Uix Shortcodes <= 2.0.4 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in UIUX Lab Uix Shortcodes allows Stored XSS. This issue affects Uix Shortcodes: from n/a through 2.0.4.	Patched by core rule	Y
CVE-2025-39575	WordPress WPCasa <= 1.3.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPSight WPCasa allows Stored XSS. This issue affects WPCasa: from n/a through 1.3.2.	Patched by core rule	Y
CVE-2025-39576	WordPress WPAdverts <= 2.2.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Greg Winiarski WPAdverts allows Stored XSS. This issue affects WPAdverts: from n/a through 2.2.1.	Patched by core rule	Y
CVE-2025-39577	WordPress PropertyHive <= 2.1.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Property Hive PropertyHive allows Stored XSS. This issue affects PropertyHive: from n/a through 2.1.2.	Patched by core rule	Y
CVE-2025-39578	WordPress Responsive Blocks <= 2.0.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CyberChimps Responsive Blocks allows Stored XSS. This issue affects Responsive Blocks: from n/a through 2.0.2.	Patched by core rule	Y
CVE-2025-39579	WordPress Membership For WooCommerce <= 2.8.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Swings Membership For WooCommerce allows DOM-Based XSS. This issue affects Membership For WooCommerce: from n/a through 2.8.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-39581	WordPress Themify Shortcodes <= 2.1.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themifyme Themify Shortcodes allows Stored XSS. This issue affects Themify Shortcodes: from n/a through 2.1.3.	Patched by core rule	Y
CVE-2025-39582	WordPress WP Data Access <= 5.5.36 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Passionate Programmer Peter WP Data Access allows DOM-Based XSS. This issue affects WP Data Access: from n/a through 5.5.36.	Patched by core rule	Y
CVE-2025-39585	WordPress Travelfic Toolkit <= 1.2.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themefic Travelfic Toolkit allows Stored XSS. This issue affects Travelfic Toolkit: from n/a through 1.2.1.	Patched by core rule	Y
CVE-2025-39590	WordPress Essential Addons for Elementor <= 6.1.9 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPDeveloper Essential Addons for Elementor allows Stored XSS. This issue affects Essential Addons for Elementor: from n/a through 6.1.9.	Patched by core rule	Y
CVE-2025-39594	WordPress Arigato Autoresponder and Newsletter plugin <= 2.7.2.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bob Arigato Autoresponder and Newsletter allows Reflected XSS. This issue affects Arigato Autoresponder and Newsletter: from n/a through 2.7.2.4.	Patched by core rule	Y
CVE-2025-43861	ManageWiki Vulnerable to Self-XSS in review dialog via unsanitized field reflection	ManageWiki is a MediaWiki extension allowing users to manage wikis. Prior to commit 2f177dc, ManageWiki is vulnerable to reflected or stored XSS in the review dialog. A logged-in attacker must change a form field to include a malicious payload. If that same user then opens the "Review Changes" dialog, the payload will be rendered and executed in the context of their own session. This issue has been patched in commit 2f177dc.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-43954	N/A	QMarkdown (aka quasar-ui-qmarkdown) before 2.0.5 allows XSS via headers even when when no-html is set.	Patched by core rule	Y
CVE-2025-46225	WordPress Post in page for Elementor plugin <= 1.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michael Post in page for Elementor allows DOM-Based XSS. This issue affects Post in page for Elementor: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-46226	WordPress MPL-Publisher <= 2.18.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ferranfg MPL-Publisher allows Stored XSS. This issue affects MPL-Publisher: from n/a through 2.18.0.	Patched by core rule	Y
CVE-2025-46227	WordPress Custom Related Posts <= 1.7.4 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brecht Custom Related Posts allows Stored XSS. This issue affects Custom Related Posts: from n/a through 1.7.4.	Patched by core rule	Y
CVE-2025-46228	WordPress Event post <= 5.9.11 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bastien Ho Event post allows DOM-Based XSS. This issue affects Event post: from n/a through 5.9.11.	Patched by core rule	Y
CVE-2025-46229	WordPress Textmetrics <= 3.6.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Israpil Textmetrics allows Stored XSS. This issue affects Textmetrics: from n/a through 3.6.2.	Patched by core rule	Y
CVE-2025-46233	WordPress Sirv <= 7.5.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sirv CDN and Image Hosting Sirv allows Stored XSS. This issue affects Sirv: from n/a through 7.5.3.	Patched by core rule	Y
CVE-2025-46234	WordPress Control Listings plugin <= 1.0.4.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Habibur Rahman Razib Control Listings allows Reflected XSS. This issue affects Control Listings: from n/a through 1.0.4.1.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-46235	WordPress SKT Blocks – Gutenberg based Page Builder <= 2.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sonalsinha21 SKT Blocks – Gutenberg based Page Builder allows Stored XSS. This issue affects SKT Blocks – Gutenberg based Page Builder: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-46236	WordPress HTML Forms <= 1.5.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Link Software LLC HTML Forms allows Stored XSS. This issue affects HTML Forms: from n/a through 1.5.2.	Patched by core rule	Y
CVE-2025-46237	WordPress Link Library <= 7.8 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Yannick Lefebvre Link Library allows Stored XSS. This issue affects Link Library: from n/a through 7.8.	Patched by core rule	Y
CVE-2025-46238	WordPress List Last Changes <= 1.2.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rbaer List Last Changes allows Stored XSS. This issue affects List Last Changes: from n/a through 1.2.1.	Patched by core rule	Y
CVE-2025-46239	WordPress Theme Switcha <= 3.4 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeff Starr Theme Switcha allows Stored XSS. This issue affects Theme Switcha: from n/a through 3.4.	Patched by core rule	Y
CVE-2025-46240	WordPress Simple Download Counter <= 2.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeff Starr Simple Download Counter allows Stored XSS. This issue affects Simple Download Counter: from n/a through 2.2.	Patched by core rule	Y
CVE-2025-46250	WordPress VForm <= 3.1.14 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vikas Ratudi VForm allows Stored XSS. This issue affects VForm: from n/a through 3.1.14.	Patched by core rule	Y
CVE-2025-46253	WordPress GutenKit plugin <= 2.2.2 - Cross	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Site Scripting (XSS) vulnerability	Generation ('Cross-site Scripting') vulnerability in Ataur R GutenKit allows Stored XSS. This issue affects GutenKit: from n/a through 2.2.2.		
CVE-2025-46254	WordPress Visual Composer Website Builder plugin <= 45.10.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Visual Composer Visual Composer Website Builder allows Stored XSS. This issue affects Visual Composer Website Builder: from n/a through 45.10.0.	Patched by core rule	Y
CVE-2025-46260	WordPress Sky Addons for Elementor plugin <= 3.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wowDevs Sky Addons for Elementor allows Stored XSS. This issue affects Sky Addons for Elementor: from n/a through 3.0.1.	Patched by core rule	Y
CVE-2025-46261	WordPress Seriously Simple Podcasting plugin <= 3.9.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Craig Hewitt Seriously Simple Podcasting allows Stored XSS. This issue affects Seriously Simple Podcasting: from n/a through 3.9.0.	Patched by core rule	Y
CVE-2025-46438	WordPress GTDB Guitar Tuners <= 4.2.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in warmwhisky GTDB Guitar Tuners allows Stored XSS. This issue affects GTDB Guitar Tuners: from n/a through 4.2.2.	Patched by core rule	Y
CVE-2025-46445	WordPress External Markdown <= 0.0.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pReya External Markdown allows Stored XSS. This issue affects External Markdown: from n/a through 0.0.1.	Patched by core rule	Y
CVE-2025-46447	WordPress Fable Extra <= 1.0.6 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFable Fable Extra allows DOM-Based XSS. This issue affects Fable Extra: from n/a through 1.0.6.	Patched by core rule	Y
CVE-2025-46449	WordPress WoWHead Tooltips <= 2.0.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Novium WoWHead Tooltips	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		allows Stored XSS. This issue affects WoWHead Tooltips: from n/a through 2.0.1.		
CVE-2025-46451	WordPress Floating Social Bar <= 1.1.7 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Syed Balkhi Floating Social Bar allows Stored XSS. This issue affects Floating Social Bar: from n/a through 1.1.7.	Patched by core rule	Y
CVE-2025-46453	WordPress Zoho Creator Forms <= 1.0.5 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CreatorTeam Zoho Creator Forms allows Stored XSS. This issue affects Zoho Creator Forms: from n/a through 1.0.5.	Patched by core rule	Y
CVE-2025-46459	WordPress Confirm User Registration <= 2.1.5 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ralf Hortt Confirm User Registration allows Stored XSS. This issue affects Confirm User Registration: from n/a through 2.1.5.	Patched by core rule	Y
CVE-2025-46461	WordPress RRSSB <= 1.0.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Relentless Apps RRSSB allows DOM-Based XSS. This issue affects RRSSB: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-46467	WordPress RAphicon <= 2.1.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rahendra Putra K™ RAphicon allows DOM-Based XSS. This issue affects RAphicon: from n/a through 2.1.2.	Patched by core rule	Y
CVE-2025-46469	WordPress Send From <= 2.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Benjamin Buddle Send From allows Stored XSS. This issue affects Send From: from n/a through 2.2.	Patched by core rule	Y
CVE-2025-46471	WordPress WP Custom Post Popup <= 1.0.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gnanavelshenll WP Custom Post Popup allows DOM-Based XSS. This issue affects WP Custom Post Popup: from n/a through 1.0.1.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-46472	WordPress The Pack Elementor addons <= 2.1.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webangon The Pack Elementor addons allows Stored XSS. This issue affects The Pack Elementor addons: from n/a through 2.1.2.	Patched by core rule	Y
CVE-2025-46475	WordPress Able Player <= 1.2.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in terrillthompson Able Player allows DOM-Based XSS. This issue affects Able Player: from n/a through 1.2.1.	Patched by core rule	Y
CVE-2025-46476	WordPress Awesome Wp Image Gallery <= 1.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in nayon46 Awesome Wp Image Gallery allows Stored XSS. This issue affects Awesome Wp Image Gallery: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-46477	WordPress WP Customize Login Page <= 1.6.5 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Carlo La Pera WP Customize Login Page allows Stored XSS. This issue affects WP Customize Login Page: from n/a through 1.6.5.	Patched by core rule	Y
CVE-2025-46478	WordPress Dropdown Content <= 1.0.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in metaloha Dropdown Content allows Stored XSS. This issue affects Dropdown Content: from n/a through 1.0.2.	Patched by core rule	Y
CVE-2025-46479	WordPress BBCode Deluxe <= 2020.08.01.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DevynCJohnson BBCode Deluxe allows DOM-Based XSS. This issue affects BBCode Deluxe: from n/a through 2020.08.01.2.	Patched by core rule	Y
CVE-2025-46480	WordPress Nepali Post Date <= 5.1.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Padam Shankhadev Nepali Post Date allows Stored XSS. This issue affects Nepali Post Date: from n/a through 5.1.1.	Patched by core rule	Y
CVE-2025-46482	WordPress WP Quiz	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	plugin <= 2.0.10 - Cross Site Scripting (XSS) vulnerability	Input During Web Page Generation ('Cross-site Scripting') vulnerability in MyThemeShop WP Quiz allows Stored XSS.This issue affects WP Quiz: from n/a through 2.0.10.	rule	
CVE-2025-46483	WordPress Peadig's Google +1 Button <= 0.1.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alex Moss Peadig's Google +1 Button allows DOM-Based XSS. This issue affects Peadig's Google +1 Button: from n/a through 0.1.2.	Patched by core rule	Y
CVE-2025-46484	WordPress Image Hover Effects For WPBakery Page Builder <= 2.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in nasir179125 Image Hover Effects For WPBakery Page Builder allows DOM-Based XSS. This issue affects Image Hover Effects For WPBakery Page Builder: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-46491	WordPress Multi-Column Taxonomy List <= 1.5 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Matthew Muro Multi-Column Taxonomy List allows Stored XSS. This issue affects Multi-Column Taxonomy List: from n/a through 1.5.	Patched by core rule	Y
CVE-2025-46496	WordPress Mini twitter feed <= 3.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in oniswap Mini twitter feed allows Stored XSS. This issue affects Mini twitter feed: from n/a through 3.0.	Patched by core rule	Y
CVE-2025-46499	WordPress PayPal Express Checkout plugin <= 2.1.2 - Cross Site Request Forgery (CSRF) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hccoder PayPal Express Checkout allows Stored XSS. This issue affects PayPal Express Checkout: from n/a through 2.1.2.	Patched by core rule	Y
CVE-2025-46501	WordPress Mixcloud Embed <= 2.2.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in biancardi Mixcloud Embed allows Stored XSS. This issue affects Mixcloud Embed: from n/a through 2.2.0.	Patched by core rule	Y
CVE-2025-46502	WordPress LSD Custom taxonomy and category	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	meta plugin <= 1.3.2 - CSRF to XSS vulnerability	Generation ('Cross-site Scripting') vulnerability in Bas Matthee LSD Custom taxonomy and category meta allows Cross Site Request Forgery. This issue affects LSD Custom taxonomy and category meta: from n/a through 1.3.2.		
CVE-2025-46505	WordPress Peekaboo <= 1.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in farinspace Peekaboo allows Stored XSS. This issue affects Peekaboo: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-46509	WordPress 360 View <= 1.1.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Andrey Mikhalchuk 360 View allows Stored XSS. This issue affects 360 View: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-46517	WordPress Blog Manager WP <= 1.0.5 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpdiscover Blog Manager WP allows Stored XSS. This issue affects Blog Manager WP: from n/a through 1.0.5.	Patched by core rule	Y
CVE-2025-46521	WordPress WS Force Login Page <= 3.0.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Silver Muru WS Force Login Page allows Stored XSS. This issue affects WS Force Login Page: from n/a through 3.0.3.	Patched by core rule	Y
CVE-2025-46523	WordPress COVID-19 (Coronavirus) Update Your Customers <= 1.5.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in devignstudiosltd COVID-19 (Coronavirus) Update Your Customers allows Stored XSS. This issue affects COVID-19 (Coronavirus) Update Your Customers: from n/a through 1.5.1.	Patched by core rule	Y
CVE-2025-46525	WordPress WP Cookie Consent <= 1.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in msmitley WP Cookie Consent allows Stored XSS. This issue affects WP Cookie Consent: from n/a through 1.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-46529	WordPress Business Contact Widget <= 2.7.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in StressFree Sites Business Contact Widget allows Stored XSS. This issue affects Business Contact Widget: from n/a through 2.7.0.	Patched by core rule	Y
CVE-2025-46532	WordPress Tooltip <= 1.0.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Haris Zulfiqar Tooltip allows DOM-Based XSS. This issue affects Tooltip: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-46533	WordPress Landing pages and Domain aliases for WordPress <= 0.8 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpdrift.no Landing pages and Domain aliases for WordPress allows Stored XSS. This issue affects Landing pages and Domain aliases for WordPress: from n/a through 0.8.	Patched by core rule	Y
CVE-2025-46534	WordPress Image Style Hover <= 1.0.6 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DanielRiera Image Style Hover allows DOM-Based XSS. This issue affects Image Style Hover: from n/a through 1.0.6.	Patched by core rule	Y
CVE-2025-46536	WordPress Carousel-of-post-images <= 1.07 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RichardHarrison Carousel-of-post-images allows DOM-Based XSS. This issue affects Carousel-of-post-images: from n/a through 1.07.	Patched by core rule	Y
CVE-2025-46538	WordPress Inline Text Popup <= 1.0.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webplanetsoft Inline Text Popup allows DOM-Based XSS. This issue affects Inline Text Popup: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-46540	WordPress GNA Search Shortcode <= 0.9.5 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chris Mok GNA Search Shortcode allows Stored XSS. This issue affects GNA Search Shortcode: from n/a through 0.9.5.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-46541	WordPress WP-reCAPTCHA-bp <= 4.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in elrata_ WP-reCAPTCHA-bp allows Stored XSS. This issue affects WP-reCAPTCHA-bp: from n/a through 4.1.	Patched by core rule	Y
CVE-2025-46542	WordPress Xpert Tab <= 1.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeXpert Xpert Tab allows Stored XSS. This issue affects Xpert Tab: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-46545	N/A	In Sherpa Orchestrator 141851, the functionality for adding or updating licenses allows for stored XSS attacks by an administrator through the name parameter. The XSS payload can execute when the license expires.	Patched by core rule	Y

INDUSFACE™

Indusface is a leading application security SaaS company, securing over 5,000 customers across 95 countries with its award-winning platform. Funded by institutional investors, it has been a category leader in Gartner Peer Insights™ for the past three years.

The industry's only AI-powered, all-in-one AppSec platform helps businesses discover, detect, remediate, and protect web applications and APIs at internet scale, backed by a 100% uptime guarantee.

Indusface is the only cloud WAAP (WAF) vendor with 100% customer recommendation for 4 consecutive years

A Customers' Choice from 2022 to 2024 Gartner® Peer Insights™

CONTACT US - +91 265 6133021 | +1 866 537 8234