INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

July 2025

The total zero-day vulnerabilities count for July month: 595

Command Injection	SQL Injection	SSRF	Path Traversal	XSS	Malicious File Upload	Remote Code Execution
41	315	13	33	125	48	20

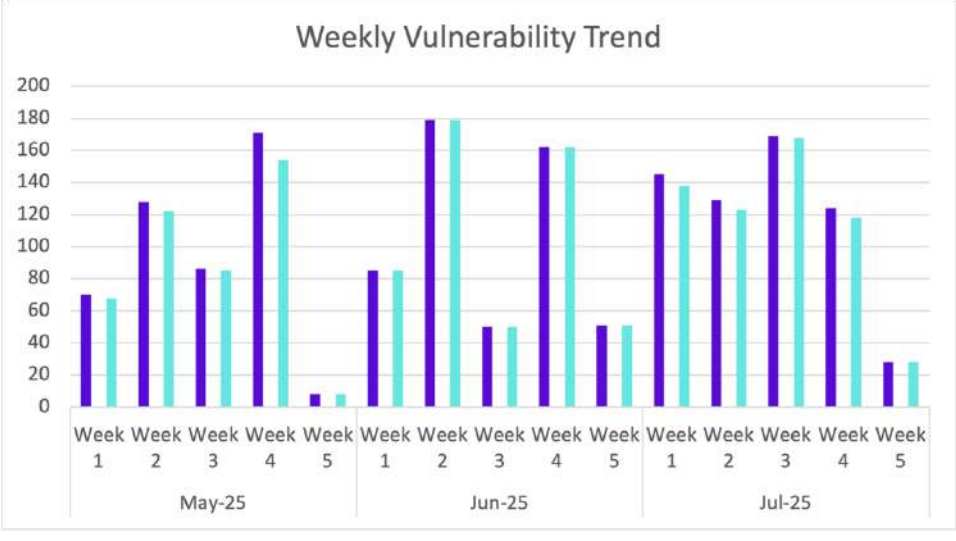
Zero-day vulnerabilities protected through core rules	595
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities found by Indusface WAS	575

- 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.

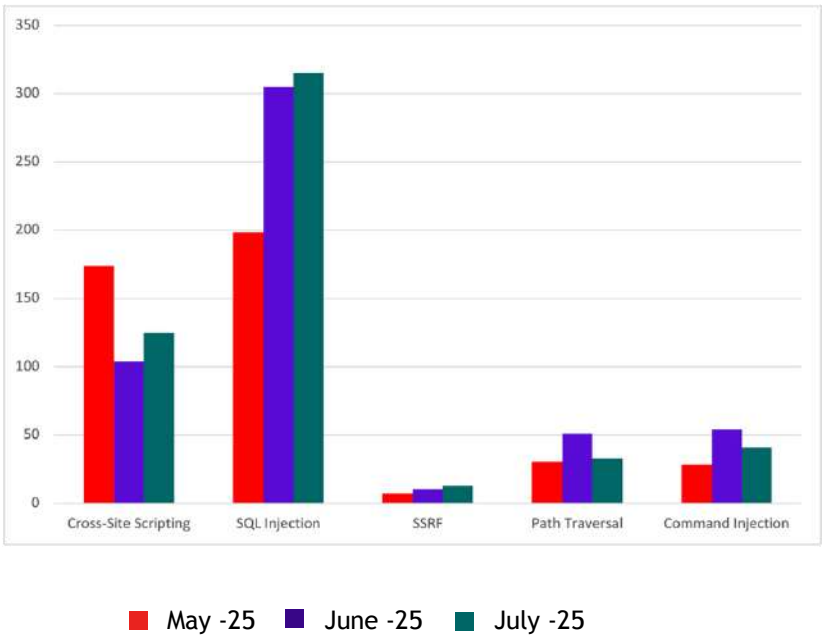
Weekly Vulnerability Trend



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-2025-52573	Command Injection in MCP Server ios-simulator-mcp	iOS Simulator MCP Server (ios-simulator-mcp) is a Model Context Protocol (MCP) server for interacting with iOS simulators. Versions prior to 1.3.3 are written in a way that is vulnerable to command injection vulnerability attacks as part of some of its MCP Server tool definition and implementation. The MCP Server exposes the tool `ui_tap` which relies on Node.js child process API `exec` which is an unsafe and vulnerable API if concatenated with untrusted user input. LLM exposed user input for `duration`, `udid`, and `x` and `y` args can be replaced with shell meta-characters like `;` or `&&` or others to change the behavior from running the expected command `idb` to another command. When LLMs are tricked through prompt injection (and other techniques and attack vectors) to call the tool with input that uses special shell characters such as `; rm -rf /tmp;#` and other payload variations, the full command-line text will be interepted by the shell and result in other commands except of `ps` executing on the host running the MCP Server. Version 1.3.3 contains a patch for the issue.	Patched by core rule	Y
CVE-2025-53097	Roo Code extension vulnerable to Potential Information Leakage via JSON Schema	Roo Code is an AI-powered autonomous coding agent. Prior to version 3.20.3, there was an issue where the Roo	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Code agent's `search_files` tool did not respect the setting to disable reads outside of the VS Code workspace. This means that an attacker who was able to inject a prompt into the agent could potentially read a sensitive file and then write the information to a JSON schema. Users have the option to disable schema fetching in VS Code, but the feature is enabled by default. For users with this feature enabled, writing to the schema would trigger a network request without the user having a chance to deny. This issue is of moderate severity, since it requires the attacker to already be able to submit prompts to the agent. Version 3.20.3 fixed the issue where `search_files` did not respect the setting to limit it to the workspace. This reduces the scope of the damage if an attacker is able to take control of the agent through prompt injection or another vector.		
CVE-2025-53098	Roo Code Vulnerable to Potential Remote Code Execution via Model Context Protocol	Roo Code is an AI-powered autonomous coding agent. The project-specific MCP configuration for the Roo Code agent is stored in the `.roo/mcp.json` file within the VS Code workspace. Because the MCP configuration format allows for execution of arbitrary commands, prior to version 3.20.3, it would have been possible for an attacker with access to craft a prompt to ask the agent to write a malicious command to the MCP configuration file. If the user had opted-in to auto-approving file writes within the project, this would have led to arbitrary command execution. This issue is of moderate severity, since it requires the attacker to already be able to submit prompts to the agent (for instance through a prompt injection attack), for the user to have MCP enabled (on by default), and for the user to have enabled auto-approved file writes (off by default). Version 3.20.3 fixes the issue by adding an additional layer of opt-in configuration for auto-approving writing to Roo's configuration files, including all files within the `.roo/` folder.	Patched by core rule	Y
CVE-2025-53100	RestDB's Codehooks.io MCP Server Vulnerable to Command Injection	RestDB's Codehooks.io MCP Server is an MCP server on the Codehooks.io platform. Prior to version 0.2.2, the MCP server is written in a way that is vulnerable to command injection attacks as part of some of its MCP Server tools definition and implementation. This could result in a user initiated remote command injection	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack on a running MCP Server. This issue has been patched in version 0.2.2.		
CVE-2025-53104	gluestack-ui Command Injection Vulnerability via discussion-to-slack GitHub Action Workflow	gluestack-ui is a library of copy-pasteable components & patterns crafted with Tailwind CSS (NativeWind). Prior to commit e6b4271, a command injection vulnerability was discovered in the discussion-to-slack.yml GitHub Actions workflow. Untrusted discussion fields (title, body, etc.) were directly interpolated into shell commands in a run: block. An attacker could craft a malicious GitHub Discussion title or body (e.g., $(curl ...)) to execute arbitrary shell commands on the Actions runner. This issue has been fixed in commit e6b4271 where the discussion-to-slack.yml workflow was removed. Users should remove the discussion-to-slack.yml workflow if using a fork or derivative of this repository.	Patched by core rule	Y
CVE-2025-53107	@cyanheads/git-mcp-server vulnerable to command injection in several tools	@cyanheads/git-mcp-server is an MCP server designed to interact with Git repositories. Prior to version 2.1.5, there is a command injection vulnerability caused by the unsanitized use of input parameters within a call to child_process.exec, enabling an attacker to inject arbitrary system commands. Successful exploitation can lead to remote code execution under the server process's privileges. The server constructs and executes shell commands using unvalidated user input directly within command-line strings. This introduces the possibility of shell metacharacter injection (|, >, &&, etc.). An MCP Client can be instructed to execute additional actions for example via indirect prompt injection when asked to read git logs. This issue has been patched in version 2.1.5.	Patched by core rule	Y
CVE-2025-47228		In the Production Environment extension in Netmake ScriptCase through 9.12.006 (23), shell injection in the SSH connection settings allows authenticated attackers to execute system commands via crafted HTTP requests.	Patched by core rule	Y
CVE-2025-7081	Belkin F9K1122 webs formSetWanStatic os command injection	A vulnerability has been found in Belkin F9K1122 1.00.33 and classified as critical. Affected by this vulnerability is the function formSetWanStatic of the file /goform/formSetWanStatic of the component webs. The manipulation of the argument m_wan_ipaddr/m_wan_netmask/m_wan_gateway/m_wan_staticdns1/m_wan_stat	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		icdns2 is directly passed by the attacker/so we can control the m_wan_ipaddr/m_wan_netmask/m_wan_gateway/m_wan_staticdns1/m_wan_staticdns2 leads to os command injection. 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.		
CVE-2025-7082	Belkin F9K1122 webs formBSSetSitesurvey os command injection	A vulnerability was found in Belkin F9K1122 1.00.33 and classified as critical. Affected by this issue is the function formBSSetSitesurvey of the file /goform/formBSSetSitesurvey of the component webs. The manipulation of the argument wan_ipaddr/wan_netmask/wan_gateway/wl_ssid is directly passed by the attacker/so we can control the wan_ipaddr/wan_netmask/wan_gateway/wl_ssid leads to os command 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-2025-7083	Belkin F9K1122 webs mp os command injection	A vulnerability was found in Belkin F9K1122 1.00.33. It has been classified as critical. This affects the function mp of the file /goform/mp of the component webs. The manipulation of the argument command leads to os command 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-2025-53355	mcp-server-kubernetes vulnerable to command injection in several tools	MCP Server Kubernetes is an MCP Server that can connect to a Kubernetes cluster and manage it. A command injection vulnerability exists in the mcp-server-kubernetes MCP Server. The vulnerability is caused by the unsanitized use of input parameters within a call to child_process.execSync, enabling an attacker to inject arbitrary system commands. Successful exploitation can lead to remote code execution under the server process's privileges. This vulnerability is fixed in 2.5.0.	Patched by core rule	Y
CVE-2025-53372	node-code-sandbox-mcp has a Sandbox Escape via Command Injection	node-code-sandbox-mcp is a Node.js–based Model Context Protocol server that spins up disposable Docker containers to execute arbitrary JavaScript. Prior to 1.3.0, a command injection	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability exists in the node-code-sandbox-mcp MCP Server. The vulnerability is caused by the unsanitized use of input parameters within a call to child_process.execSync, enabling an attacker to inject arbitrary system commands. Successful exploitation can lead to remote code execution under the server process's privileges on the host machine, bypassing the sandbox protection of running code inside docker. This vulnerability is fixed in 1.3.0.		
CVE-2025-7154	TOTOLINK N200RE cstecgi.cgi sub_41A0F8 os command injection	A vulnerability, which was classified as critical, has been found in TOTOLINK N200RE 9.3.5u.6095_B20200916/9.3.5u.6139_B20201216. Affected by this issue is the function sub_41A0F8 of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument Hostname leads to os command 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-2025-27613	Gitk can create and truncate files in the user's home directory	Gitk is a Tcl/Tk based Git history browser. Starting with 1.7.0, when a user clones an untrusted repository and runs gitk without additional command arguments, files for which the user has write permission can be created and truncated. The option Support per-file encoding must have been enabled before in Gitk's Preferences. This option is disabled by default. The same happens when Show origin of this line is used in the main window (regardless of whether Support per-file encoding is enabled or not). This vulnerability is fixed in 2.43.7, 2.44.4, 2.45.4, 2.46.4, 2.47.3, 2.48.2, 2.49.1, and 2.50.1.	Patched by core rule	Y
CVE-2025-27614	Gitk allows arbitrary command execution	Gitk is a Tcl/Tk based Git history browser. Starting with 2.41.0, a Git repository can be crafted in such a way that with some social engineering a user who has cloned the repository can be tricked into running any script (e.g., Bourne shell, Perl, Python, ...) supplied by the attacker by invoking gitk filename, where filename has a particular structure. The script is run with the privileges of the user. This vulnerability is fixed in 2.43.7, 2.44.4, 2.45.4, 2.46.4, 2.47.3, 2.48.2, 2.49.1, and 2.50.	Patched by core rule	Y
CVE-2025-46334	Git GUI malicious command injection on Windows	Git GUI allows you to use the Git source control management tools via a GUI. A malicious repository can ship versions of sh.exe or	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		typical textconv filter programs such as astextplain. Due to the unfortunate design of Tcl on Windows, the search path when looking for an executable always includes the current directory. The mentioned programs are invoked when the user selects Git Bash or Browse Files from the menu. This vulnerability is fixed in 2.43.7, 2.44.4, 2.45.4, 2.46.4, 2.47.3, 2.48.2, 2.49.1, and 2.50.1.		
CVE-2025-46835	Git GUI can create and overwrite files for which the user has write permission	Git GUI allows you to use the Git source control management tools via a GUI. When a user clones an untrusted repository and is tricked into editing a file located in a maliciously named directory in the repository, then Git GUI can create and overwrite files for which the user has write permission. This vulnerability is fixed in 2.43.7, 2.44.4, 2.45.4, 2.46.4, 2.47.3, 2.48.2, 2.49.1, and 2.50.1.	Patched by core rule	Y
CVE-2025-53542	Kubernetes Headlamp Allows Arbitrary Command Injection in macOS Process headlamp@codeSign	Headlamp is an extensible Kubernetes web UI. A command injection vulnerability was discovered in the codeSign.js script used in the macOS packaging workflow of the Kubernetes Headlamp project. This issue arises due to the improper use of Node.js's execSync() function with unsanitized input derived from environment variables, which can be influenced by an attacker. The variables ${teamID}, ${entitlementsPath}, and ${config.app} are dynamically derived from the environment or application config and passed directly to the shell command without proper escaping or argument separation. This exposes the system to command injection if any of the values contain malicious input. This vulnerability is fixed in 0.31.1.	Patched by core rule	Y
CVE-2025-53637	Meshtastic allows Command Injection in GitHub Action	Meshtastic is an open source mesh networking solution. The main_matrix.yml GitHub Action is triggered by the pull_request_target event, which has extensive permissions, and can be initiated by an attacker who forked the repository and created a pull request. In the shell code execution part, user-controlled input is interpolated unsafely into the code. If this were to be exploited, attackers could inject unauthorized code into the repository. This vulnerability is fixed in 2.6.6.	Patched by core rule	Y
CVE-2025-7407	Netgear D6400 diag.cgi os command injection	A vulnerability, which was classified as critical, was found in Netgear D6400	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		1.0.0.114. This affects an unknown part of the file diag.cgi. The manipulation of the argument host_name leads to os command 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 and confirmed the existence of the vulnerability. They reacted very quickly, professional and kind. This vulnerability only affects products that are no longer supported by the maintainer.		
CVE-2025-7414	Tenda O3V2 httpd setPingInfo fromNetToolGet os command injection	A vulnerability classified as critical was found in Tenda O3V2 1.0.0.12(3880). This vulnerability affects the function fromNetToolGet of the file /goform/setPingInfo of the component httpd. The manipulation of the argument domain leads to os command 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-2025-7415	Tenda O3V2 httpd getTraceroute fromTraceroutGet command injection	A vulnerability, which was classified as critical, has been found in Tenda O3V2 1.0.0.12(3880). This issue affects the function fromTraceroutGet of the file /goform/getTraceroute of the component httpd. The manipulation of the argument dest leads to 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-2025-52994		gif_outputAsJpeg in phpThumb through 1.7.23 allows phpthumb.gif.php OS Command Injection via a crafted parameter value. This is fixed in 1.7.23-202506081709.	Patched by core rule	Y
CVE-2025-53623	Job Iteration API is vulnerable to OS Command Injection attack through its CsvEnumerator class	The Job Iteration API is an an extension for ActiveJob that make jobs interruptible and resumable Versions prior to 1.11.0 have an arbitrary code execution vulnerability in the `CsvEnumerator` class. This vulnerability can be exploited by an attacker to execute arbitrary commands on the system where the application is running, potentially leading to unauthorized access, data leakage, or complete system compromise. The issue is fixed in versions `1.11.0` and above. Users can mitigate the risk by avoiding the use of untrusted input in the `CsvEnumerator` class and ensuring that any file paths are properly sanitized and validated before being passed to the class methods. Users should avoid using the `count_of_rows_in_file` method with untrusted CSV	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		filenames.		
CVE-2025-53818	github-kanban-mcp-server Command Injection vulnerability	GitHub Kanban MCP Server is a Model Context Protocol (MCP) server for managing GitHub issues in Kanban board format and streamlining LLM task management. Versions 0.3.0 and 0.4.0 of the MCP Server are written in a way that is vulnerable to command injection vulnerability attacks as part of some of its MCP Server tool definition and implementation. The MCP Server exposes the tool `add_comment` which relies on Node.js child process API `exec` to execute the GitHub (`gh`) command, is an unsafe and vulnerable API if concatenated with untrusted user input. As of time of publication, no known patches are available.	Patched by core rule	Y
CVE-2025-7578	Teledyne FLIR FB-Series O/FLIR FH-Series ID runcmd.sh sendCommand command injection	A vulnerability was found in Teledyne FLIR FB-Series O and FLIR FH-Series ID 1.3.2.16. It has been declared as critical. This vulnerability affects the function sendCommand of the file runcmd.sh. The manipulation of the argument cmd leads to command injection. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The researcher highlights, that "[a]lthough this functionality is currently disabled due to server CGI configuration errors, it is essentially a 'time bomb' waiting to be activated". The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-7613	TOTOLINK T6 HTTP POST Request cstecgi.cgi CloudSrvVersionCheck command injection	A vulnerability was found in TOTOLINK T6 4.1.5cu.748. It has been rated as critical. This issue affects the function CloudSrvVersionCheck of the file /cgi-bin/cstecgi.cgi of the component HTTP POST Request Handler. The manipulation of the argument ip leads to 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-2025-7614	TOTOLINK T6 HTTP POST Request cstecgi.cgi delDevice command injection	A vulnerability classified as critical has been found in TOTOLINK T6 4.1.5cu.748. Affected is the function delDevice of the file /cgi-bin/cstecgi.cgi of the component HTTP POST Request Handler. The manipulation of the argument ipAddr leads to command 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-2025-7615	TOTOLINK T6 HTTP POST	A vulnerability classified as	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Request cstecgi.cgi clearPairCfg command injection	critical was found in TOTOLINK T6 4.1.5cu.748. Affected by this vulnerability is the function clearPairCfg of the file /cgi-bin/cstecgi.cgi of the component HTTP POST Request Handler. The manipulation of the argument ip leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	rule	
CVE-2025-49833	GHSL-2025-045: GPT-SoVITS Command Injection vulnerability	GPT-SoVITS-WebUI is a voice conversion and text-to-speech webUI. In versions 20250228v3 and prior, there is a command injection vulnerability in the webui.py open_slice function. slice_opt_root and slice-inp-path takes user input, which is passed to the open_slice function, which concatenates the user input into a command and runs it on the server, leading to arbitrary command execution. At time of publication, no known patched versions are available.	Patched by core rule	Y
CVE-2025-49834	GHSL-2025-046: GPT-SoVITS Command Injection vulnerability	GPT-SoVITS-WebUI is a voice conversion and text-to-speech webUI. In versions 20250228v3 and prior, there is a command injection vulnerability in webui.py open_denoise function. denoise_inp_dir and denoise_opt_dir take user input, which is passed to the open_denoise function, which concatenates the user input into a command and runs it on the server, leading to arbitrary command execution. At time of publication, no known patched versions are available.	Patched by core rule	Y
CVE-2025-49835	GHSL-2025-047: GPT-SoVITS Command Injection vulnerability	GPT-SoVITS-WebUI is a voice conversion and text-to-speech webUI. In versions 20250228v3 and prior, there is a command injection vulnerability in webui.py open_asr function. asr_inp_dir (and a number of other variables) takes user input, which is passed to the open_asr function, which concatenates the user input into a command and runs it on the server, leading to arbitrary command execution. At time of publication, no known patched versions are available.	Patched by core rule	Y
CVE-2025-49836	GHSL-2025-048: GPT-SoVITS Command Injection vulnerability	GPT-SoVITS-WebUI is a voice conversion and text-to-speech webUI. In versions 20250228v3 and prior, there is a command injection vulnerability in webui.py change_label function. path_list takes user input, which is passed to the change_label function, which concatenates the user input into a command and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		runs it on the server, leading to arbitrary command execution. At time of publication, no known patched versions are available.		
CVE-2025-7788	Xuxueli xxl-job SampleXxlJob.java commandJobHandler os command injection	A vulnerability has been found in Xuxueli xxl-job up to 3.1.1 and classified as critical. Affected by this vulnerability is the function commandJobHandler of the file src\main\java\com\xxl\job\executor\service\jobhandler\SampleXxlJob.java. The manipulation leads to os 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-2025-7836	D-Link DIR-816L Environment Variable cgibin lxmldbc_system command injection	A vulnerability has been found in D-Link DIR-816L up to 2.06B01 and classified as critical. Affected by this vulnerability is the function lxmldbc_system of the file /htdocs/cgibin of the component Environment Variable Handler. The manipulation leads to command injection. The attack can be launched 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-2025-53832	@translated/lara-mcp vulnerable to command injection in import_tmx tool	Lara Translate MCP Server is a Model Context Protocol (MCP) Server for Lara Translate API. Versions 0.0.11 and below contain a command injection vulnerability which exists in the @translated/lara-mcp MCP Server. The vulnerability is caused by the unsanitized use of input parameters within a call to child_process.exec, enabling an attacker to inject arbitrary system commands. Successful exploitation can lead to remote code execution under the server process's privileges. The server constructs and executes shell commands using unvalidated user input directly within command-line strings. This introduces the possibility of shell metacharacter injection (|, >, &&, etc.). This vulnerability is fixed in version 0.0.12.	Patched by core rule	Y
CVE-2025-7932	D-Link DIR-817L ssdpcgi lxmldbc_system command injection	A vulnerability classified as critical has been found in D-Link DIR-817L up to 1.04B01. This affects the function lxmldbc_system of the file ssdpcgi. The manipulation leads to command 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-2025-54072	yt-dlp allows `--exec`	yt-dlp is a feature-rich	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	command injection when using placeholder on Windows	command-line audio/video downloader. In versions 2025.06.25 and below, when the --exec option is used on Windows with the default placeholder (or {}), insufficient sanitization is applied to the expanded filepath, allowing for remote code execution. This is a bypass of the mitigation for CVE-2024-22423 where the default placeholder and {} were not covered by the new escaping rules. Windows users who are unable to upgrade should avoid using --exec altogether. Instead, the --write-info-json or --dump-json options could be used, with an external script or command line consuming the JSON output. This is fixed in version 2025.07.21.	rule	
CVE-2025-54141	ViewVC's standalone server exposes arbitrary server filesystem content	ViewVC is a browser interface for CVS and Subversion version control repositories. In versions 1.1.0 through 1.1.31 and 1.2.0 through 1.2.3, the standalone.py script provided in the ViewVC distribution can expose the contents of the host server's filesystem though a directory traversal-style attack. This is fixed in versions 1.1.31 and 1.2.4.	Patched by core rule	Y
CVE-2025-7952	TOTOLINK T6 MQTT Packet wireless.so ckeckKeepAlive command injection	A vulnerability classified as critical was found in TOTOLINK T6 4.1.5cu.748. This vulnerability affects the function ckeckKeepAlive of the file wireless.so of the component MQTT Packet Handler. The manipulation leads to command 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-2025-7404	Calibre Web 0.6.24 & Autocaliweb 0.7.0 - Blind C	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Calibre Web, Autocaliweb allows Blind OS Command Injection.This issue affects Calibre Web: 0.6.24 (Nicolette); Autocaliweb: from 0.7.0 before 0.7.1.	Patched by core rule	Y

Path Traversal Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-34045	WeiPHP Path Traversal Arbitrary File Read	A path traversal vulnerability exists in WeiPHP 5.0, an open source WeChat public account platform development framework by Shenzhen Yuanmengyun Technology Co., Ltd. The flaw occurs in the picUrl parameter of the /public/index.php/material/Material/_download_image endpoint, where insufficient input validation allows unauthenticated remote attackers to perform directory traversal via crafted POST requests. This enables arbitrary file read on the server, potentially exposing sensitive information such as configuration files and source code.	Patched by core rule	Y
CVE-2025-34047	Leadsec VPN Path Traversal Arbitrary File Read	A path traversal vulnerability exists in the Leadsec SSL VPN (formerly Lenovo NetGuard), allowing unauthenticated attackers to read arbitrary files on the underlying system via the ostype parameter in the /vpn/user/download/client endpoint. This flaw arises from insufficient input sanitation, enabling traversal sequences to escape the intended directory and access sensitive files.	Patched by core rule	Y
CVE-2025-34048	D-Link DSL-2730U/2750U/2750E Path Traversal Arbitrary File Read	A path traversal vulnerability exists in the web management interface of D-Link DSL-2730U, DSL-2750U, and DSL-2750E ADSL routers with firmware versions IN_1.02, SEA_1.04, and SEA_1.07. The vulnerability is due to insufficient input validation on the getpage parameter within the /cgi-bin/webproc CGI script. This flaw allows an unauthenticated remote attacker to perform path traversal attacks by supplying crafted requests,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		enabling arbitrary file read on the affected device.		
CVE-2025-6731	yzcheng90 X-SpringBoot APK File apk uploadApk path traversal	A vulnerability was found in yzcheng90 X-SpringBoot up to 5.0 and classified as critical. Affected by this issue is the function uploadApk of the file /sys/oss/upload/apk of the component APK File Handler. The manipulation of the argument File leads to path traversal. 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-2025-6772	eosphoros-ai db-gpt import import_flow path traversal	A vulnerability was found in eosphoros-ai db-gpt up to 0.7.2. It has been classified as critical. Affected is the function import_flow of the file /api/v2/serve/awel/flow/import. The manipulation of the argument File leads to path traversal. 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-2025-6773	HKUDS LightRAG File Upload document_routes.py upload_to_input_dir path traversal	A vulnerability was found in HKUDS LightRAG up to 1.3.8. It has been declared as critical. Affected by this vulnerability is the function upload_to_input_dir of the file lightrag/api/routers/document_routes.py of the component File Upload. The manipulation of the argument file.filename leads to path traversal. It is possible to launch the attack on the local host. The identifier of the patch is 60777d535b719631680bcf5d0969bdef79ca4eaf. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y
CVE-2025-6774	gooaclok819 sublinkX template.go AddTemp path traversal	A vulnerability was found in gooaclok819 sublinkX up to 1.8. It has been rated as critical. Affected by this issue is the function AddTemp of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		api/template.go. The manipulation of the argument filename leads to path traversal. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.9 is able to address this issue. The patch is identified as 778d26aef723daa58df98c8060c43f5bf5d1b10b. It is recommended to upgrade the affected component.		
CVE-2025-6776	xiaoyunjie openvpn-cms-flask File Upload controller.py upload path traversal	A vulnerability classified as critical was found in xiaoyunjie openvpn-cms-flask up to 1.2.7. This vulnerability affects the function Upload of the file app/plugins/oss/app/controller.py of the component File Upload. The manipulation of the argument image leads to path traversal. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.2.8 is able to address this issue. The name of the patch is e23559b98c8ea2957f09978c29f4e512ba789eb6. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-6853	chatchat-space Langchain-Chatchat Backend upload_temp_docs path traversal	A vulnerability classified as critical has been found in chatchat-space Langchain-Chatchat up to 0.3.1. This affects the function upload_temp_docs of the file /knowledge_base/upload_temp_docs of the component Backend. The manipulation of the argument flag 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-2025-6854	chatchat-space Langchain-Chatchat files path traversal	A vulnerability classified as problematic was found in chatchat-space Langchain-Chatchat up to 0.3.1. This vulnerability affects unknown code of the file /v1/files?purpose=assistants. The manipulation leads to path traversal. The attack can 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-2025-6855	chatchat-space Langchain-Chatchat file path traversal	A vulnerability, which was classified as critical, has been found in chatchat-space Langchain-Chatchat up to 0.3.1. This issue affects some unknown processing of the file /v1/file. The manipulation of the argument flag leads to path traversal. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6866	code-projects Simple Forum forum_downloadfile.php path traversal	A vulnerability has been found in code-projects Simple Forum 1.0 and classified as critical. This vulnerability affects unknown code of the file /forum_downloadfile.php. The manipulation of the argument filename leads to path traversal. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6925	Dromara RuoYi-Vue-Plus Mail MailController.java path traversal	A vulnerability has been found in Dromara RuoYi-Vue-Plus 5.4.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /src/main/java/org/dromara/demo/controller/MailController.java of the component Mail Handler. The manipulation of the argument filePath leads to path traversal. 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-2025-53109	Model Context Protocol Servers Vulnerable to Path Validation Bypass via Prefix Matching and Symlink Handling	Model Context Protocol Servers is a collection of reference implementations for the model context protocol (MCP). Versions of Filesystem prior to 0.6.4 or 2025.7.01 could allow access to unintended files via symlinks within allowed directories. Users are advised to upgrade to 0.6.4 or 2025.7.01 resolve.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-53110	Model Context Protocol Servers Vulnerable to Path Validation Bypass via Colliding Path Prefix	Model Context Protocol Servers is a collection of reference implementations for the model context protocol (MCP). Versions of Filesystem prior to 0.6.4 or 2025.7.01 could allow access to unintended files in cases where the prefix matches an allowed directory. Users are advised to upgrade to 0.6.4 or 2025.7.01 resolve.	Patched by core rule	Y
CVE-2025-53358	kotaemon Vulnerable to Path Traversal via Link Upload	kotaemon is an open-source RAG-based tool for document comprehension. From versions 0.10.6 and prior, in libs/ktem/ktem/index/file/ui.py, the index_fn method accepts both URLs and local file paths without validation. The pipeline streams these paths directly and stores them, enabling attackers to traverse directories (e.g. ../../../../../.env) and exfiltrate sensitive files. This issue has been patched via commit 37cdc28, in version 0.10.7 which has not been made public at time of publication.	Patched by core rule	Y
CVE-2025-3046	Path Traversal via Symbolic Links in run-llama/llama_index	A vulnerability in the `ObsidianReader` class of the run-llama/llama_index repository, versions 0.12.23 to 0.12.28, allows for arbitrary file read through symbolic links. The `ObsidianReader` fails to resolve symlinks to their real paths and does not validate whether the resolved paths lie within the intended directory. This flaw enables attackers to place symlinks pointing to files outside the vault directory, which are then processed as valid Markdown files, potentially exposing sensitive information.	Patched by core rule	Y
CVE-2025-53375	Dokploy allows attackers to read any file that the Traefik process user can access	Dokploy is a self-hostable Platform as a Service (PaaS) that simplifies the deployment and management of applications and databases. An authenticated attacker can	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		read any file that the Traefik process user can access (e.g., /etc/passwd, application source, environment variable files containing credentials and secrets). This may lead to full compromise of other services or lateral movement. This vulnerability is fixed in 0.23.7.		
CVE-2025-6210	Hardlink-Based Path Traversal in run-llama/llama_index	A vulnerability in the ObsidianReader class of the run-llama/llama_index repository, specifically in version 0.12.27, allows for hardlink-based path traversal. This flaw permits attackers to bypass path restrictions and access sensitive system files, such as /etc/passwd, by exploiting hardlinks. The vulnerability arises from inadequate handling of hardlinks in the load_data() method, where the security checks fail to differentiate between real files and hardlinks. This issue is resolved in version 0.5.2.	Patched by core rule	Y
CVE-2025-7108	risesoft-y9 Digital-Infrastructure Y9FileController.java deleteFile path traversal	A vulnerability classified as critical was found in risesoft-y9 Digital-Infrastructure up to 9.6.7. Affected by this vulnerability is the function deleteFile of the file /Digital-Infrastructure-9.6.7/y9-digitalbase-webapp/y9-module-filemanager/risenet-y9boot-webapp-filemanager/src/main/java/net/risesoft/y9public/controller/Y9FileController.java. The manipulation of the argument fullPath leads to path traversal. 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-2025-7450	letseeqiji gorobbs API user.go ResetUserAvatar path traversal	A vulnerability was found in letseeqiji gorobbs up to 1.0.8. It has been classified as critical. This affects the function ResetUserAvatar of the file controller/api/v1/user.go of the component API. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument filename leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-7452	kone-net go-chat Endpoint file_controller.go GetFile path traversal	A vulnerability was found in kone-net go-chat up to f9e58d0afa9bbdb31faf25e7739da330692c4c63. It has been declared as critical. This vulnerability affects the function GetFile of the file go-chat/api/v1/file_controller.go of the component Endpoint. The manipulation of the argument fileName leads to path traversal. The attack can be initiated 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-2025-7488	JoeyBling SpringBoot_MyBatisPlus download path traversal	A vulnerability has been found in JoeyBling SpringBoot_MyBatisPlus up to a6a825513bd688f717dbae3a196bc9c9622fea26 and classified as critical. This vulnerability affects the function Download of the file /file/download. The manipulation of the argument Name leads to path traversal. 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-2025-7566	jshERP SystemConfigController.java exportExcelByParam path traversal	A vulnerability has been found in jshERP up to 3.5 and classified as critical. This vulnerability affects the function exportExcelByParam of the file /src/main/java/com/jsh/erp/controller/SystemConfigController.java. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument Title leads to path traversal. 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.		
CVE-2025-7575	Zavy86 WikiDocs submit.php image_delete_ajax path traversal	A vulnerability has been found in Zavy86 WikiDocs up to 1.0.77 and classified as critical. Affected by this vulnerability is the function image_drop_upload_ajax/image_delete_ajax of the file submit.php. The manipulation leads to path traversal. The attack can be launched remotely. Upgrading to version 1.0.78 is able to address this issue. The identifier of the patch is 98ea9ee4a2052c4327f89d2f7688cc1b5749450d. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-7625	YiJiuSmile kkFileViewOfficeEdit download path traversal	A vulnerability, which was classified as critical, was found in YiJiuSmile kkFileViewOfficeEdit up to 5fbc57c48e8fe6c1b91e0e7995e2d59615f37abd. Affected is the function Download of the file /download. The manipulation of the argument url leads to path traversal. It is possible to launch the attack 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-2025-7626	YiJiuSmile kkFileViewOfficeEdit onlinePreview path traversal	A vulnerability has been found in YiJiuSmile kkFileViewOfficeEdit up to 5fbc57c48e8fe6c1b91e0e7995e2d59615f37abd and classified as critical. Affected by this vulnerability is the function onlinePreview of the file /onlinePreview. The manipulation of the argument url leads to path traversal. The attack can be launched remotely. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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-2025-7628	YiJiuSmile kkFileViewOfficeEdit deleteFile path traversal	A vulnerability was found in YiJiuSmile kkFileViewOfficeEdit up to 5fbc57c48e8fe6c1b91e0e7995e2d59615f37abd. It has been classified as critical. This affects the function deleteFile of the file /deleteFile. The manipulation of the argument fileName leads to path traversal. It is possible to initiate the attack 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-2025-49830	Conjur OSS and Secrets Manager, Self-Hosted (formerly Conjur Enterprise) vulnerable to path traversal and file disclosure	Conjur provides secrets management and application identity for infrastructure. An authenticated attacker who is able to load policy can use the policy yaml parser to reference files on the Secrets Manager, Self-Hosted server. These references may be used as reconnaissance to better understand the folder structure of the Secrets Manager/Conjur server or to have the yaml parser include files on the server in the yaml that is processed as the policy loads. This issue affects Secrets Manager, Self-Hosted (formerly Conjur Enterprise) prior to versions 13.5.1 and 13.6.1 and Conjur OSS prior to version 1.22.1. Conjur OSS version 1.22.1 and Secrets Manager, Self-Hosted versions 13.5.1 and 13.6.1 fix the issue.	Patched by core rule	Y
CVE-2025-53905	Vim has path traversial issue with tar.vim and special crafted tar files	Vim is an open source, command line text editor. Prior to version 9.1.1552, a path traversal issue in Vim's tar.vim plugin can allow overwriting of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		arbitrary files when opening specially crafted tar archives. Impact is low because this exploit requires direct user interaction. However, successfully exploitation can lead to overwriting sensitive files or placing executable code in privileged locations, depending on the permissions of the process editing the archive. The victim must edit such a file using Vim which will reveal the filename and the file content, a careful user may suspect some strange things going on. Successful exploitation could results in the ability to execute arbitrary commands on the underlying operating system. Version 9.1.1552 contains a patch for the vulnerability.		
CVE-2025-53906	Vim has path traversal issue with zip.vim and special crafted zip archives	Vim is an open source, command line text editor. Prior to version 9.1.1551, a path traversal issue in Vim's zip.vim plugin can allow overwriting of arbitrary files when opening specially crafted zip archives. Impact is low because this exploit requires direct user interaction. However, successfully exploitation can lead to overwriting sensitive files or placing executable code in privileged locations, depending on the permissions of the process editing the archive. The victim must edit such a file using Vim which will reveal the filename and the file content, a careful user may suspect some strange things going on. Successful exploitation could results in the ability to execute arbitrary commands on the underlying operating system. Version 9.1.1551 contains a patch for the vulnerability.	Patched by core rule	Y
CVE-2015-10136	GI-Media Library < 3.0 - Directory Traversal	The GI-Media Library plugin for WordPress is vulnerable to Directory Traversal in versions before 3.0 via the 'fileid' parameter. This allows	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information.		
CVE-2025-8132	yanyutao0402 ChanCMS utils.js delfile path traversal	A vulnerability was found in yanyutao0402 ChanCMS up to 3.1.2. It has been rated as critical. Affected by this issue is the function delfile of the file app/extend/utils.js. The manipulation leads to path traversal. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.1.3 is able to address this issue. The name of the patch is c8a282bf02a62b59ec60b4699e91c51aff2ee9cd. It is recommended to upgrade the affected component.	Patched by core rule	Y

Server-side Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-52477	Octo-STS Vulnerable to Unauthenticated SSRF with HTTP Response Reflection in OIDC Flow	Octo-STS is a GitHub App that acts like a Security Token Service (STS) for the GitHub API. Octo-STS versions before v0.5.3 are vulnerable to unauthenticated SSRF by abusing fields in OpenID Connect tokens. Malicious tokens were shown to trigger internal network requests which could reflect error logs with sensitive information. Upgrade to v0.5.3 to resolve this issue. This version includes patch sets to sanitize input and redact logging.	Patched by core rule	Y
CVE-2025-53018	Lychee has Server-Side Request Forgery (SSRF) in Photo::fromUrl API via unvalidated remote image URLs	Lychee is a free, open-source photo-management tool. Prior to version 6.6.13, a critical Server-Side Request Forgery (SSRF) vulnerability exists in the `/api/v2/Photo::fromUrl` endpoint. This flaw lets an attacker instruct the application's backend to make HTTP requests to any URL they choose. Consequently, internal network resources—such as localhost services or cloud-provider metadata endpoints—become reachable. The endpoint takes a URL from the user and calls it server-side via fopen() without any safeguards. There is no IP address validation, nor are there any allow-list, timeout, or size restrictions. Because of this, attackers can point the application at internal targets. Using this flaw, an attacker can perform internal port scans or retrieve sensitive cloud metadata. Version 6.6.13 contains a patch for the issue.	Patched by core rule	Y
CVE-2025-6762	diyhi bbs HTTP Header login getUrl server-side request forgery	A vulnerability classified as critical has been found in diyhi bbs up to 6.8. This affects the function getUrl of the file /admin/login of the component HTTP Header Handler. The manipulation of the argument Host leads to server-side request forgery. It is possible to initiate the attack 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.		
CVE-2025-53371	DiscordNotifications allows DOS, SSRF, and possible RCE through requests to user-controlled URLs	DiscordNotifications is an extension for MediaWiki that sends notifications of actions in your Wiki to a Discord channel. DiscordNotifications allows sending requests via curl and file_get_contents to arbitrary URLs set via $wgDiscordIncomingWebhookUrl and $wgDiscordAdditionalIncomingWebhookUrls. This allows for DOS by causing the server to read large files. SSRF is also possible if there are internal unprotected APIs that can be accessed using HTTP POST requests, which could also possibly lead to RCE. This vulnerability is fixed in commit 1f20d850cbcce5b15951c7c6127b87b927a5415e.	Patched by core rule	Y
CVE-2025-53641	Postiz allows header mutation in middleware facilitates resulting in SSRF	Postiz is an AI social media scheduling tool. From 1.45.1 to 1.62.3, the Postiz frontend application allows an attacker to inject arbitrary HTTP headers into the middleware pipeline. This flaw enables a server-side request forgery (SSRF) condition, which can be exploited to initiate unauthorized outbound requests from the server hosting the Postiz application. This vulnerability is fixed in 1.62.3.	Patched by core rule	Y
CVE-2025-1220	Null byte termination in hostnames	In PHP versions:8.1.* before 8.1.33, 8.2.* before 8.2.29, 8.3.* before 8.3.23, 8.4.* before 8.4.10 some functions like fsockopen() lack validation that the hostname supplied does not contain null characters. This may lead to other functions like parse_url() treat the hostname in different way, thus opening way to security problems if the user code implements access checks before access using such functions.	Patched by core rule	Y
CVE-2025-7523	Jinher OA DelTemp.aspx xml external entity reference	A vulnerability was found in Jinher OA 1.0 and classified as problematic. Affected by this issue is some unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		functionality of the file /c6/Jhsoft.Web.message/ToolBar/DelTemp.aspx. The manipulation leads to xml external entity reference. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-7759	thinkgem JeeSite UEditor Image Grabber ActionEnter.java server-side request forgery	A vulnerability, which was classified as critical, was found in thinkgem JeeSite up to 5.12.0. This affects an unknown part of the file modules/core/src/main/java/com/jeesite/common/ueditor/ActionEnter.java of the component UEditor Image Grabber. The manipulation of the argument Source leads to server-side request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is 1c5e49b0818037452148e0f8ff69ed04cb8fefdc. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y
CVE-2025-7787	Xuxueli xxl-job SampleXxlJob.java httpJobHandler server-side request forgery	A vulnerability, which was classified as critical, was found in Xuxueli xxl-job up to 3.1.1. Affected is the function httpJobHandler of the file src\main\java\com\xxl\job\executor\service\jobhandler\SampleXxlJob.java. 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-2025-7823	Jinher OA ProjectScheduleDelete.aspx xml external entity reference	A vulnerability was found in Jinher OA 1.2. It has been declared as problematic. This vulnerability affects unknown code of the file ProjectScheduleDelete.aspx. The manipulation leads to xml external entity reference. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-7824	Jinher OA XmlHttp.aspx xml external entity reference	A vulnerability was found in Jinher OA 1.1. It has been rated as problematic. This issue affects some unknown processing of the file XmlHttp.aspx. The manipulation leads to xml	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		external entity reference. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-54122	Manager-io/Manager allows unauthenticated full read server-side request forgery in "proxy" endpoint	Manager-io/Manager is accounting software. A critical unauthenticated full read Server-Side Request Forgery (SSRF) vulnerability has been identified in the proxy handler component of both manager Desktop and Server edition versions up to and including 25.7.18.2519. This vulnerability allows an unauthenticated attacker to bypass network isolation and access restrictions, potentially enabling access to internal services, cloud metadata endpoints, and exfiltration of sensitive data from isolated network segments. This vulnerability is fixed in version 25.7.21.2525.	Patched by core rule	Y
CVE-2025-8133	yanyutao0402 ChanCMS gather.js getArticle server-side request forgery	A vulnerability classified as critical has been found in yanyutao0402 ChanCMS up to 3.1.2. This affects the function getArticle of the file app/modules/api/service/gather.js. The manipulation of the argument targetUrl leads to server-side request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.1.3 is able to address this issue. The identifier of the patch is 3ef58a50e8b3c427b03c8cf3c9e19a79aa809be6. It is recommended to upgrade the affected component.	Patched by core rule	Y

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-53091	WeGIA has Unauthenticated Time-Based Blind SQL Injection in almox Parameter	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Time-Based Blind SQL Injection vulnerability was discovered in version 3.3.3 the almox parameter of the `/controle/getProdutosPorAlmox.php` endpoint. This issue allows any unauthenticated attacker to inject arbitrary SQL queries, potentially leading to unauthorized data access or further exploitation depending on database configuration. Version 3.4.0 fixes the issue.	Patched by core rule	Y
CVE-2025-6738	huija bicycleSharingServer UserServiceImpl.java userDao.selectUserByUserNameLike sql injection	A vulnerability, which was classified as critical, has been found in huija bicycleSharingServer up to 7b8a3ba48ad618604abd4797d2e7cf3b5ac7625a. Affected by this issue is the function userDao.selectUserByUserNameLike of the file UserServiceImpl.java. The manipulation of the argument Username leads to sql injection. The attack may be launched 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-2025-6749	huija bicycleSharingServer AdminController.java searchAdminMessageShow sql injection	A vulnerability classified as critical was found in huija bicycleSharingServer up to 7b8a3ba48ad618604abd4797d2e7cf3b5ac7625a. Affected by this vulnerability is the function searchAdminMessageShow of the file AdminController.java. The manipulation of the argument Title leads to sql injection. 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unavailable.		
CVE-2025-6753	huija bicycleSharingServer AdminController.java selectAdminByNameLike sql injection	A vulnerability was found in huija bicycleSharingServer 1.0 and classified as critical. This issue affects the function selectAdminByNameLike of the file AdminController.java. The manipulation 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-2025-6766	sfturing hosp_order OfficeServiceImpl.java getOfficeName sql injection	A vulnerability was found in sfturing hosp_order up to 627f426331da8086ce8fff2017d65b1ddef384f8. It has been declared as critical. This vulnerability affects the function getOfficeName of the file OfficeServiceImpl.java. The manipulation of the argument officesName leads to sql injection. The attack can be initiated 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-2025-6767	sfturing hosp_order DoctorServiceImpl.java findDoctorByCondition sql injection	A vulnerability was found in sfturing hosp_order up to 627f426331da8086ce8fff2017d65b1ddef384f8. It has been rated as critical. This issue affects the function findDoctorByCondition of the file DoctorServiceImpl.java. The manipulation of the argument hospitalName leads to sql injection. 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-2025-6768	sfturing hosp_order HospitalServiceImpl.java findAllHosByCondition sql injection	A vulnerability classified as critical has been found in sfturing hosp_order up to 627f426331da8086ce8fff2017d65b1ddef384f8. Affected is the function findAllHosByCondition of the file HospitalServiceImpl.java.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The manipulation of the argument hospitalName leads to sql injection. It is possible to launch the attack 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-2025-6775	xiaoyunjie openvpn-cms-flask User Creation Endpoint openvpn.py create_user command injection	A vulnerability classified as critical has been found in xiaoyunjie openvpn-cms-flask up to 1.2.7. This affects the function create_user of the file /app/api/v1/openvpn.py of the component User Creation Endpoint. The manipulation of the argument Username leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.2.8 is able to address this issue. The patch is named e23559b98c8ea2957f09978c29f4e512ba789eb6. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-6777	code-projects Food Distributor Site process_login.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Food Distributor Site 1.0. This issue affects some unknown processing of the file /admin/process_login.php. The manipulation of the argument username/password 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-2025-6819	code-projects Inventory Management System removeBrand.php sql injection	A vulnerability has been found in code-projects Inventory Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /php_action/removeBrand.php. The manipulation of the argument brandId 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-2025-6820	code-projects Inventory	A vulnerability was found in	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Management System createProduct.php sql injection	code-projects Inventory Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /php_action/createProduct.php. The manipulation of the argument productName leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	rule	
CVE-2025-6821	code-projects Inventory Management System createOrder.php sql injection	A vulnerability was found in code-projects Inventory Management System 1.0. It has been classified as critical. This affects an unknown part of the file /php_action/createOrder.php. The manipulation 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-2025-6822	code-projects Inventory Management System removeProduct.php sql injection	A vulnerability was found in code-projects Inventory Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /php_action/removeProduct.php. The manipulation of the argument productId 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-2025-6823	code-projects Inventory Management System editProduct.php sql injection	A vulnerability was found in code-projects Inventory Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /php_action/editProduct.php. The manipulation of the argument editProductName 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-2025-6826	code-projects Payroll Management System ajax.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Payroll Management System 1.0. Affected by this issue is some unknown functionality of the file /Payroll_Management_System/ajax.php?action=save_de	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		partment. 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.		
CVE-2025-6827	code-projects Inventory Management System editOrder.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Inventory Management System 1.0. This affects an unknown part of the file /php_action/editOrder.php. The manipulation 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-2025-6828	code-projects Inventory Management System orders.php sql injection	A vulnerability has been found in code-projects Inventory Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /orders.php. The manipulation of the argument i 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-2025-6829	aaluoxiang oa_system External Address Book outAddress sql injection	A vulnerability was found in aaluoxiang oa_system up to c3a08168c144f27256a90838492c713f55f1b207 and classified as critical. This issue affects the function outAddress of the component External Address Book Handler. The manipulation leads to sql injection. The attack may be initiated remotely. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.	Patched by core rule	Y
CVE-2025-6834	code-projects Inventory Management System editPayment.php sql injection	A vulnerability was found in code-projects Inventory Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /php_action/editPayment.php. The manipulation of the argument orderId 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-2025-6835	code-projects Library System student-issue-book.php sql injection	A vulnerability was found in code-projects Library System 1.0. It has been rated as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		critical. This issue affects some unknown processing of the file /student-issue-book.php. The manipulation of the argument reg leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6836	code-projects Library System profile.php sql injection	A vulnerability classified as critical has been found in code-projects Library System 1.0. Affected is an unknown function of the file /profile.php. The manipulation of the argument phone 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-2025-6840	code-projects Product Inventory System Login index.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Product Inventory System 1.0. This affects an unknown part of the file /index.php of the component Login. The manipulation of the argument Username 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-2025-6841	code-projects Product Inventory System edit_product.php sql injection	A vulnerability has been found in code-projects Product Inventory System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/edit_product.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-2025-6842	code-projects Product Inventory System edit_user.php sql injection	A vulnerability was found in code-projects Product Inventory System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/edit_user.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-2025-6844	code-projects Simple	A vulnerability was found in	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Forum signin.php sql injection	code-projects Simple Forum 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /signin.php. The manipulation of the argument User leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	rule	
CVE-2025-6845	code-projects Simple Forum register1.php sql injection	A vulnerability was found in code-projects Simple Forum 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /register1.php. The manipulation of the argument User 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-2025-6846	code-projects Simple Forum forum_viewfile.php sql injection	A vulnerability classified as critical has been found in code-projects Simple Forum 1.0. This affects an unknown part of the file /forum_viewfile.php. The manipulation of the argument Name 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-2025-6847	code-projects Simple Forum forum_edit.php sql injection	A vulnerability classified as critical was found in code-projects Simple Forum 1.0. This vulnerability affects unknown code of the file /forum_edit.php. The manipulation of the argument iii 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-2025-6850	code-projects Simple Forum forum1.php sql injection	A vulnerability has been found in code-projects Simple Forum 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /forum1.php. The manipulation of the argument File 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-2025-6859	SourceCodester Best Salon Management	A vulnerability was found in SourceCodester Best Salon	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System pro_sale.php sql injection	Management System 1.0. It has been classified as critical. This affects an unknown part of the file /panel/pro_sale.php. The manipulation of the argument fromdate/todate 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-2025-6860	SourceCodester Best Salon Management System staff_commision.php sql injection	A vulnerability was found in SourceCodester Best Salon Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /panel/staff_commision.php. The manipulation of the argument fromdate/todate 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-2025-6861	SourceCodester Best Salon Management System add_plan.php sql injection	A vulnerability was found in SourceCodester Best Salon Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /panel/add_plan.php. The manipulation of the argument plan_name/description/duration_days/price 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-2025-6862	SourceCodester Best Salon Management System edit_plan.php sql injection	A vulnerability classified as critical has been found in SourceCodester Best Salon Management System 1.0. Affected is an unknown function of the file /panel/edit_plan.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-2025-6863	PHPGurukul Local Services Search Engine Management System edit-category-detail.php sql injection	A vulnerability classified as critical was found in PHPGurukul Local Services Search Engine Management System 2.1. Affected by this vulnerability is an unknown functionality of the file /admin/edit-category-detail.php. The manipulation of the argument editid leads	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6867	SourceCodester Simple Company Website manage.php sql injection	A vulnerability was found in SourceCodester Simple Company Website 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/services/manage.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-2025-6868	SourceCodester Simple Company Website manage.php sql injection	A vulnerability was found in SourceCodester Simple Company Website 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/clients/manage.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-2025-6869	SourceCodester Simple Company Website manage.php sql injection	A vulnerability was found in SourceCodester Simple Company Website 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/testimonials/manage.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-2025-6871	SourceCodester Simple Company Website Login.php sql injection	A vulnerability classified as critical has been found in SourceCodester Simple Company Website 1.0. This affects an unknown part of the file /classes/Login.php. The manipulation of the argument Username 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-2025-6874	SourceCodester Best Salon Management System add_subscribe.php sql injection	A vulnerability, which was classified as critical, was found in SourceCodester Best Salon Management 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
		/panel/add_subscribe.php. The manipulation of the argument user_id/plan_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-2025-6875	SourceCodester Best Salon Management System edit-subscription.php sql injection	A vulnerability has been found in SourceCodester Best Salon Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /panel/edit-subscription.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-2025-6876	SourceCodester Best Salon Management System add-category.php sql injection	A vulnerability was found in SourceCodester Best Salon Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /panel/add-category.php. The 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.	Patched by core rule	Y
CVE-2025-6877	SourceCodester Best Salon Management System edit-category.php sql injection	A vulnerability was found in SourceCodester Best Salon Management System 1.0. It has been classified as critical. This affects an unknown part of the file /panel/edit-category.php. The manipulation of the argument editid 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-2025-52895	Frappe possibility of SQL injection due to improper validations	Frappe is a full-stack web application framework. Prior to versions 14.94.3 and 15.58.0, SQL injection could be achieved via a specially crafted request, which could allow malicious person to gain access to sensitive information. This issue has been patched in versions 14.94.3 and 15.58.0. There are no workarounds for this issue other than upgrading.	Patched by core rule	Y
CVE-2025-6878	SourceCodester Best	A vulnerability was found in	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Salon Management System search-appointment.php sql injection	SourceCodester Best Salon Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /panel/search-appointment.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.	rule	
CVE-2025-6879	SourceCodester Best Salon Management System add-tax.php sql injection	A vulnerability was found in SourceCodester Best Salon Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /panel/add-tax.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-2025-6880	SourceCodester Best Salon Management System edit-tax.php sql injection	A vulnerability classified as critical has been found in SourceCodester Best Salon Management System 1.0. Affected is an unknown function of the file /panel/edit-tax.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-2025-6883	code-projects Staff Audit System update_index.php sql injection	A vulnerability classified as critical was found in code-projects Staff Audit System 1.0. This vulnerability affects unknown code of the file /update_index.php. The manipulation of the argument updateid 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-2025-6884	code-projects Staff Audit System search_index.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Staff Audit System 1.0. This issue affects some unknown processing of the file /search_index.php. The manipulation of the argument Search 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-2025-6885	PHPGurukul Teachers Record Management System edit-teacher-detail.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Teachers Record Management System 2.1. Affected is an unknown function of the file /admin/edit-teacher-detail.php. The manipulation of the argument tid 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-2025-6888	PHPGurukul Teachers Record Management System changeimage.php sql injection	A vulnerability was found in PHPGurukul Teachers Record Management System 2.1. It has been classified as critical. This affects an unknown part of the file /admin/changeimage.php. The manipulation of the argument tid 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-2025-6889	code-projects Movie Ticketing System logIn.php sql injection	A vulnerability was found in code-projects Movie Ticketing System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /logIn.php. The manipulation of the argument postName 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-2025-6890	code-projects Movie Ticketing System ticketConfirmation.php sql injection	A vulnerability was found in code-projects Movie Ticketing System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /ticketConfirmation.php. The manipulation of the argument Date 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-2025-6891	code-projects Inventory Management System createUser.php sql injection	A vulnerability classified as critical has been found in code-projects Inventory Management System 1.0. Affected is an unknown function of the file /php_action/createUser.php	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		. 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.		
CVE-2025-6896	D-Link DI-7300G+ wget_test.asp os command injection	A vulnerability classified as critical has been found in D-Link DI-7300G+ 19.12.25A1. Affected is an unknown function of the file wget_test.asp. The manipulation of the argument url leads to os command 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-2025-6897	D-Link DI-7300G+ httpd_debug.asp os command injection	A vulnerability classified as critical was found in D-Link DI-7300G+ 19.12.25A1. Affected by this vulnerability is an unknown functionality of the file httpd_debug.asp. The manipulation of the argument Time leads to os command injection. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6898	D-Link DI-7300G+ in proxy_client.asp os command injection	A vulnerability, which was classified as critical, has been found in D-Link DI-7300G+ 19.12.25A1. Affected by this issue is some unknown functionality of the file in proxy_client.asp. The manipulation of the argument proxy_srv/proxy_lanport/proxy_lanip/proxy_srvport leads to os command 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-2025-6899	D-Link DI-7300G+/DI-8200G msp_info.htm os command injection	A vulnerability, which was classified as critical, was found in D-Link DI-7300G+ and DI-8200G 17.12.20A1/19.12.25A1. This affects an unknown part of the file msp_info.htm. The manipulation of the argument flag/cmd/iface leads to os command 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-2025-6901	code-projects Inventory Management System	A vulnerability was found in code-projects Inventory	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	removeUser.php sql injection	Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /php_action/removeUser.php. The manipulation of the argument userid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6902	code-projects Inventory Management System editUser.php sql injection	A vulnerability was found in code-projects Inventory Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /php_action/editUser.php. The manipulation of the argument edituserName 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-2025-6903	code-projects Car Rental System approve.php sql injection	A vulnerability was found in code-projects Car Rental System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/approve.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-2025-6904	code-projects Car Rental System add_cars.php sql injection	A vulnerability was found in code-projects Car Rental System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/add_cars.php. The manipulation of the argument car_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-2025-6905	code-projects Car Rental System signup.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Car Rental System 1.0. This issue affects some unknown processing of the file /signup.php. The manipulation of the argument fname 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-2025-6906	code-projects Car Rental	A vulnerability classified as	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System login.php sql injection	critical has been found in code-projects Car Rental System 1.0. This affects an unknown part of the file /login.php. The manipulation of the argument uname 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-2025-6907	code-projects Car Rental System book_car.php sql injection	A vulnerability classified as critical was found in code-projects Car Rental System 1.0. This vulnerability affects unknown code of the file /book_car.php. The manipulation of the argument fname 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-2025-6908	PHPGurukul Old Age Home Management System edit-services.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/edit-services.php. The manipulation of the argument sertitle 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-2025-6909	PHPGurukul Old Age Home Management System add-scdetails.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/add-scdetails.php. The manipulation of the argument emeradd 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-2025-6910	PHPGurukul Student Record System session.php sql injection	A vulnerability was found in PHPGurukul Student Record System 3.2. It has been classified as critical. This affects an unknown part of the file /session.php. The manipulation of the argument session 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-2025-6911	PHPGurukul Student	A vulnerability was found in	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Record System manage-subjects.php sql injection	PHPGurukul Student Record System 3.2. It has been declared as critical. This vulnerability affects unknown code of the file /manage-subjects.php. The manipulation of the argument del leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	rule	
CVE-2025-6912	PHPGurukul Student Record System manage-students.php sql injection	A vulnerability was found in PHPGurukul Student Record System 3.2. It has been rated as critical. This issue affects some unknown processing of the file /manage-students.php. The manipulation of the argument del 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-2025-6913	PHPGurukul Student Record System admin-profile.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Student Record System 3.2. Affected is an unknown function of the file /admin-profile.php. The manipulation of the argument aemailid 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-2025-6914	PHPGurukul Student Record System edit-student.php sql injection	A vulnerability classified as critical was found in PHPGurukul Student Record System 3.2. Affected by this vulnerability is an unknown functionality of the file /edit-student.php. The manipulation of the argument fmarks2 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-2025-6915	PHPGurukul Student Record System register.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Student Record System 3.2. Affected by this issue is some unknown functionality of the file /register.php. The manipulation of the argument session 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-2025-6917	code-projects Online	A vulnerability has been	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Hotel Booking registration.php sql injection	found in code-projects Online Hotel Booking 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/registration.php. The manipulation of the argument uname leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	rule	
CVE-2025-6929	PHPGurukul Zoo Management System view-normal-ticket.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 /admin/view-normal-ticket.php. The manipulation of the argument viewid 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-2025-6930	PHPGurukul Zoo Management System manage-foreigners-ticket.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Zoo Management System 2.1. Affected is an unknown function of the file /admin/manage-foreigners-ticket.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-2025-6935	Campcodes Sales and Inventory System payment_add.php sql injection	A vulnerability was found in Campcodes Sales and Inventory System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /pages/payment_add.php. The manipulation of the argument cid 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-2025-6936	code-projects Simple Pizza Ordering System addpro.php sql injection	A vulnerability was found in code-projects Simple Pizza Ordering System 1.0. It has been classified as critical. This affects an unknown part of the file /addpro.php. The manipulation of the argument ID 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-2025-6937	code-projects Simple Pizza Ordering System large.php sql injection	A vulnerability was found in code-projects Simple Pizza Ordering System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /large.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-2025-6938	code-projects Simple Pizza Ordering System editcus.php sql injection	A vulnerability was found in code-projects Simple Pizza Ordering System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /editcus.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-2025-6954	Campcodes Employee Management System applyleave.php sql injection	A vulnerability has been found in Campcodes Employee Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /applyleave.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-2025-6955	Campcodes Employee Management System aprocess.php sql injection	A vulnerability was found in Campcodes Employee Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /process/aprocess.php. The manipulation of the argument mailuid 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-2025-6956	Campcodes Employee Management System changepassemp.php sql injection	A vulnerability was found in Campcodes Employee Management System 1.0. It has been classified as critical. This affects an unknown part of the file /changepassemp.php. The manipulation of the argument ID leads to sql	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6957	Campcodes Employee Management System eprocess.php sql injection	A vulnerability was found in Campcodes Employee Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /process/eprocess.php. The manipulation of the argument mailuid 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-2025-6958	Campcodes Employee Management System edit.php sql injection	A vulnerability was found in Campcodes Employee Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /edit.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-2025-6959	Campcodes Employee Management System eloginwel.php sql injection	A vulnerability classified as critical has been found in Campcodes Employee Management System 1.0. Affected is an unknown function of the file /eloginwel.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-2025-6960	Campcodes Employee Management System empproject.php sql injection	A vulnerability classified as critical was found in Campcodes Employee Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /empproject.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-2025-6961	Campcodes Employee Management System mark.php sql injection	A vulnerability, which was classified as critical, has been found in Campcodes Employee Management System 1.0. Affected by this issue is some unknown functionality of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/mark.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.		
CVE-2025-6962	Campcodes Employee Management System myprofileup.php sql injection	A vulnerability, which was classified as critical, was found in Campcodes Employee Management System 1.0. This affects an unknown part of the file /myprofileup.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-2025-6963	Campcodes Employee Management System myprofile.php sql injection	A vulnerability has been found in Campcodes Employee Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /myprofile.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-2025-7119	Campcodes Complaint Management System index.php sql injection	A vulnerability has been found in Campcodes Complaint Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /users/index.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-2025-7120	Campcodes Complaint Management System check_availability.php sql injection	A vulnerability was found in Campcodes Complaint Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /users/check_availability.php. The manipulation of the argument email 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-2025-7121	Campcodes Complaint Management System complaint-details.php sql	A vulnerability was found in Campcodes Complaint Management System 1.0. It	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	has been classified as critical. This affects an unknown part of the file /users/complaint-details.php. The manipulation of the argument cid 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-2025-7122	Campcodes Complaint Management System index.php sql injection	A vulnerability was found in Campcodes Complaint Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/index.php. The manipulation of the argument Username 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-2025-7123	Campcodes Complaint Management System complaint-details.php sql injection	A vulnerability was found in Campcodes Complaint Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/complaint-details.php. The manipulation of the argument cid/uid 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-2025-7125	itsourcecode Employee Management System editempeducation.php sql injection	A vulnerability classified as critical was found in itsourcecode Employee Management System up to 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/editempeducation.php. The manipulation of the argument coursepg 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-2025-7126	itsourcecode Employee Management System adminprofile.php sql injection	A vulnerability, which was classified as critical, has been found in itsourcecode Employee Management System up to 1.0. Affected by this issue is some unknown functionality of the file /admin/adminprofile.php. The manipulation of the argument AdminName leads to sql injection. The attack		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-7127	itsourcecode Employee Management System changepassword.php sql injection	A vulnerability, which was classified as critical, was found in itsourcecode Employee Management System up to 1.0. This affects an unknown part of the file /admin/changepassword.php. The manipulation of the argument currentpassword 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-2025-7128	Campcodes Payroll Management System ajax.php sql injection	A vulnerability has been found in Campcodes Payroll Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /ajax.php?action=calculate_payroll. 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-2025-7129	Campcodes Payroll Management System ajax.php sql injection	A vulnerability was found in Campcodes Payroll Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /ajax.php?action=delete_employee_attendance_single. 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-2025-7130	Campcodes Payroll Management System ajax.php sql injection	A vulnerability was found in Campcodes Payroll Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /ajax.php?action=delete_payroll. 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-2025-7131	Campcodes Payroll Management System ajax.php sql injection	A vulnerability was found in Campcodes Payroll Management System 1.0. It has been declared as critical. Affected by this vulnerability	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		is an unknown functionality of the file /ajax.php?action=save_employee_attendance. The manipulation of the argument employee_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-7132	Campcodes Payroll Management System ajax.php sql injection	A vulnerability was found in Campcodes Payroll Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /ajax.php?action=save_payroll. 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-2025-7134	Campcodes Online Recruitment Management System ajax.php sql injection	A vulnerability classified as critical was found in Campcodes Online Recruitment Management System 1.0. This vulnerability affects unknown code of the file /admin/ajax.php?action=delete_application. 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-2025-7135	Campcodes Online Recruitment Management System ajax.php sql injection	A vulnerability, which was classified as critical, has been found in Campcodes Online Recruitment Management System 1.0. This issue affects some unknown processing of the file /admin/ajax.php?action=save_vacancy. 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-2025-7136	Campcodes Online Recruitment Management System view_vacancy.php sql injection	A vulnerability, which was classified as critical, was found in Campcodes Online Recruitment Management System 1.0. Affected is an unknown function of the file /admin/view_vacancy.php. The manipulation of the argument ID leads to sql		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-7137	SourceCodester Best Salon Management System schedule-staff.php sql injection	A vulnerability was found in SourceCodester Best Salon Management System 1.0. It has been classified as critical. This affects an unknown part of the file /panel/schedule-staff.php. The manipulation of the argument staff_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-2025-7138	SourceCodester Best Salon Management System admin-profile.php sql injection	A vulnerability was found in SourceCodester Best Salon Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /panel/admin-profile.php. The manipulation of the argument adminname 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-2025-7147	CodeAstro Patient Record Management System login.php sql injection	A vulnerability has been found in CodeAstro Patient Record Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /login.php. The manipulation of the argument uname 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-2025-7149	Campcodes Advanced Online Voting System candidates_delete.php sql injection	A vulnerability was found in Campcodes Advanced Online Voting System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/candidates_delete.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-2025-7150	Campcodes Advanced Online Voting System voters_delete.php sql injection	A vulnerability was found in Campcodes Advanced Online Voting System 1.0. It has been declared as critical. This vulnerability affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown code of the file /admin/voters_delete.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.		
CVE-2025-48385	Git alllows arbitrary file writes via bundle-uri parameter injection	Git is a fast, scalable, distributed revision control system with an unusually rich command set that provides both high-level operations and full access to internals. When cloning a repository Git knows to optionally fetch a bundle advertised by the remote server, which allows the server-side to offload parts of the clone to a CDN. The Git client does not perform sufficient validation of the advertised bundles, which allows the remote side to perform protocol injection. This protocol injection can cause the client to write the fetched bundle to a location controlled by the adversary. The fetched content is fully controlled by the server, which can in the worst case lead to arbitrary code execution. The use of bundle URIs is not enabled by default and can be controlled by the bundle.heuristic config option. Some cases of the vulnerability require that the adversary is in control of where a repository will be cloned to. This either requires social engineering or a recursive clone with submodules. These cases can thus be avoided by disabling recursive clones. This vulnerability is fixed in v2.43.7, v2.44.4, v2.45.4, v2.46.4, v2.47.3, v2.48.2, v2.49.1, and v2.50.1.	Patched by core rule	Y
CVE-2025-7155	PHPGurukul Online Notes Sharing System Cookie Dashboard sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Online Notes Sharing System 1.0. This affects an unknown part of the file /Dashboard of the component Cookie Handler. The manipulation of the argument sessionid leads to sql injection. It is possible to initiate 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 original researcher disclosure suspects an XPath Injection vulnerability; however, the provided attack payload appears to be characteristic of an SQL Injection attack.		
CVE-2025-7157	code-projects Online Note Sharing login.php sql injection	A vulnerability was found in code-projects Online Note Sharing 1.0. It has been classified as critical. Affected is an unknown function of the file /login.php. The manipulation of the argument username/password 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-2025-7158	PHPGurukul Zoo Management System manage-normal-ticket.php sql injection	A vulnerability was found in PHPGurukul Zoo Management System 2.1. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/manage-normal-ticket.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-2025-7159	PHPGurukul Zoo Management System manage-animals.php sql injection	A vulnerability was found in PHPGurukul Zoo Management System 2.1. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/manage-animals.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-2025-7160	PHPGurukul Zoo Management System index.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Zoo Management System 2.1. This affects an unknown part of the file /admin/index.php. The manipulation of the argument Username 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-2025-7161	PHPGurukul Zoo Management System add-normal-ticket.php	A vulnerability classified as critical was found in PHPGurukul Zoo	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	sql injection	Management System 2.1. This vulnerability affects unknown code of the file /admin/add-normal-ticket.php. The manipulation of the argument cprice leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-7162	PHPGurukul Zoo Management System add-foreigners-ticket.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Zoo Management System 2.1. This issue affects some unknown processing of the file /admin/add-foreigners-ticket.php. The manipulation of the argument cprice 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-2025-7163	PHPGurukul Zoo Management System add-animals.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Zoo Management System 2.1. Affected is an unknown function of the file /admin/add-animals.php. The manipulation of the argument cnum 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-2025-7164	PHPGurukul/Campcodes Cyber Cafe Management System index.php sql injection	A vulnerability has been found in PHPGurukul/Campcodes Cyber Cafe Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /index.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-2025-7165	PHPGurukul/Campcodes Cyber Cafe Management System forgot-password.php sql injection	A vulnerability was found in PHPGurukul/Campcodes Cyber Cafe Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /forgot-password.php. The manipulation of the argument email leads to sql injection. The attack may be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-7166	code-projects Responsive Blog Site single.php sql injection	A vulnerability was found in code-projects Responsive Blog Site 1.0. It has been classified as critical. This affects an unknown part of the file /single.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-2025-7167	code-projects Responsive Blog Site category.php sql injection	A vulnerability was found in code-projects Responsive Blog Site 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /category.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-2025-7168	code-projects Crime Reporting System userlogin.php sql injection	A vulnerability was found in code-projects Crime Reporting System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /userlogin.php. The manipulation of the argument email 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-2025-7169	code-projects Crime Reporting System complainer_page.php sql injection	A vulnerability classified as critical has been found in code-projects Crime Reporting System 1.0. Affected is an unknown function of the file /complainer_page.php. The manipulation of the argument location 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-2025-7170	code-projects Crime Reporting System registration.php sql injection	A vulnerability classified as critical was found in code-projects Crime Reporting System 1.0. Affected by this vulnerability is an unknown functionality of the file /registration.php. The manipulation of the argument Name 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-2025-7171	code-projects Crime Reporting System policelogin.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Crime Reporting System 1.0. Affected by this issue is some unknown functionality of the file /policelogin.php. The manipulation of the argument email 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-2025-7172	code-projects Crime Reporting System headlogin.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Crime Reporting System 1.0. This affects an unknown part of the file /headlogin.php. The manipulation of the argument 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-2025-7173	code-projects Library System add-student.php sql injection	A vulnerability has been found in code-projects Library System 1.0 and classified as critical. This vulnerability affects unknown code of the file /add-student.php. The manipulation of the argument Username 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-2025-7174	code-projects Library System teacher-issue-book.php sql injection	A vulnerability was found in code-projects Library System 1.0 and classified as critical. This issue affects some unknown processing of the file /teacher-issue-book.php. The manipulation of the argument idn 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-2025-7176	PHPGurukul Hospital Management System view-medhistory.php sql injection	A vulnerability was found in PHPGurukul Hospital Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file view-medhistory.php. The manipulation of the argument viewid 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-2025-7177	PHPGurukul Car Washing Management System editcar-washpoint.php sql injection	A vulnerability was found in PHPGurukul Car Washing Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/editcar-washpoint.php. The manipulation of the argument wpid 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-2025-7178	code-projects Food Distributor Site login.php sql injection	A vulnerability classified as critical has been found in code-projects Food Distributor Site 1.0. This affects an unknown part of the file /admin/login.php. The manipulation of the argument Username 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-2025-7179	code-projects Library System add-teacher.php sql injection	A vulnerability classified as critical was found in code-projects Library System 1.0. This vulnerability affects unknown code of the file /add-teacher.php. The manipulation of the argument Username 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-2025-7180	code-projects Staff Audit System login.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Staff Audit System 1.0. This issue affects some unknown processing of the file /login.php. The manipulation of the argument User 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-2025-7183	Campcodes Sales and Inventory System customer_account.php sql injection	A vulnerability was found in Campcodes Sales and Inventory System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /pages/customer_account.php. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument Customer leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-7184	code-projects Library System books.php sql injection	A vulnerability was found in code-projects Library System 1.0. It has been classified as critical. This affects an unknown part of the file /user/teacher/books.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-2025-7185	code-projects Library System approve.php sql injection	A vulnerability was found in code-projects Library System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /approve.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-2025-7186	code-projects Chat System fetch_chat.php sql injection	A vulnerability was found in code-projects Chat System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /user/fetch_chat.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-2025-7187	code-projects Chat System fetch_member.php sql injection	A vulnerability classified as critical has been found in code-projects Chat System 1.0. Affected is an unknown function of the file /user/fetch_member.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-2025-7188	code-projects Chat System addmember.php sql injection	A vulnerability classified as critical was found in code-projects Chat System 1.0. Affected by this vulnerability is an unknown functionality of the file /user/addmember.php. The manipulation of the argument ID leads to sql		

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-2025-7189	code-projects Chat System send_message.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Chat System 1.0. Affected by this issue is some unknown functionality of the file /user/send_message.php. The manipulation of the argument msg 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-2025-7191	code-projects Student Enrollment System login.php sql injection	A vulnerability has been found in code-projects Student Enrollment System 1.0 and classified as critical. This vulnerability affects unknown code of the file /login.php. The manipulation of the argument Username 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-2025-7192	D-Link DIR-645 ssdpcgi cgibin ssdpcgi_main command injection	A vulnerability was found in D-Link DIR-645 up to 1.05B01 and classified as critical. This issue affects the function ssdpcgi_main of the file /htdocs/cgibin of the component ssdpcgi. The manipulation leads to command injection. The attack may be initiated 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-2025-7193	itsourcecode Agri-Trading Online Shopping System suppliercontroller.php sql injection	A vulnerability was found in itsourcecode Agri-Trading Online Shopping System up to 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/suppliercontroller.php. The manipulation of the argument supplier 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-2025-7196	code-projects Jonnys Liquor browse.php sql injection	A vulnerability was found in code-projects Jonnys Liquor 1.0. It has been rated as critical. Affected by this issue	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		is some unknown functionality of the file /browse.php. The manipulation of the argument Search leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-7197	code-projects Jonnys Liquor delete-row.php sql injection	A vulnerability classified as critical has been found in code-projects Jonnys Liquor 1.0. This affects an unknown part of the file /admin/delete-row.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-2025-7198	code-projects Jonnys Liquor admin-area.php sql injection	A vulnerability classified as critical was found in code-projects Jonnys Liquor 1.0. This vulnerability affects unknown code of the file /admin/admin-area.php. The manipulation of the argument drink 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-2025-7199	code-projects Library System notapprove.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Library System 1.0. This issue affects some unknown processing of the file /notapprove.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-2025-7200	krishna9772 Pharmacy Management System quantity_upd.php sql injection	A vulnerability, which was classified as critical, was found in krishna9772 Pharmacy Management System up to a2efc8442931ec9308f3b4cf4778e5701153f4e5. Affected is an unknown function of the file quantity_upd.php. The manipulation of the argument med_name/med_cat/ex_date leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		is used by this product. Therefore, no version details of affected nor updated releases are available.		
CVE-2025-6514	OS command injection in mcp-remote when connecting to untrusted MCP servers	mcp-remote is exposed to OS command injection when connecting to untrusted MCP servers due to crafted input from the authorization_endpoint response URL	Patched by core rule	Y
CVE-2025-7211	code-projects LifeStyle Store cart_add.php sql injection	A vulnerability was found in code-projects LifeStyle Store 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /cart_add.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-2025-7212	itsourcecode Insurance Management System insertAgent.php sql injection	A vulnerability was found in itsourcecode Insurance Management System up to 1.0. It has been rated as critical. This issue affects some unknown processing of the file /insertAgent.php. The manipulation of the argument agent_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-2025-7217	Campcodes Payroll Management System ajax.php sql injection	A vulnerability has been found in Campcodes Payroll Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /ajax.php?action=save_position. 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-2025-7218	Campcodes Payroll Management System ajax.php sql injection	A vulnerability was found in Campcodes Payroll Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /ajax.php?action=delete_position. 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-2025-7219	Campcodes Payroll Management System	A vulnerability was found in Campcodes Payroll	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	ajax.php sql injection	Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /ajax.php?action=delete_allowances. 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-2025-7220	Campcodes Payroll Management System ajax.php sql injection	A vulnerability was found in Campcodes Payroll Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /ajax.php?action=save_deductions. 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-2025-53549	Matrix Rust SDK allows SQL injection in the EventCache implementation	The Matrix Rust SDK is a collection of libraries that make it easier to build Matrix clients in Rust. An SQL injection vulnerability in the EventCache::find_event_with_relations method of matrix-sdk 0.11 and 0.12 allows malicious room members to execute arbitrary SQL commands in Matrix clients that directly pass relation types provided by those room members into this method, when used with the default sqlite-based store backend. Exploitation is unlikely, as no known clients currently use the API in this manner. This vulnerability is fixed in 0.13.	Patched by core rule	Y
CVE-2025-7409	code-projects Mobile Shop LoginAsAdmin.php sql injection	A vulnerability was found in code-projects Mobile Shop 1.0 and classified as critical. This issue affects some unknown processing of the file /LoginAsAdmin.php. The manipulation of the argument email 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-2025-7410	code-projects LifeStyle Store cart_remove.php sql injection	A vulnerability was found in code-projects LifeStyle Store 1.0. It has been classified as critical. Affected is an unknown function of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/cart_remove.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-2025-7411	code-projects LifeStyle Store success.php sql injection	A vulnerability was found in code-projects LifeStyle Store 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /success.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-2025-7436	Campcodes Online Recruitment Management System ajax.php sql injection	A vulnerability was found in Campcodes Online Recruitment Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/ajax.php?action=delete_vacancy. 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-2025-7454	Campcodes Online Movie Theater Seat Reservation System manage_theater.php sql injection	A vulnerability classified as critical has been found in Campcodes Online Movie Theater Seat Reservation System 1.0. Affected is an unknown function of the file /admin/manage_theater.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-2025-7455	Campcodes Online Movie Theater Seat Reservation System manage_reserve.php sql injection	A vulnerability classified as critical was found in Campcodes Online Movie Theater Seat Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file /manage_reserve.php. The manipulation of the argument mid 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-2025-7456	Campcodes Online Movie	A vulnerability, which was	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Theater Seat Reservation System reserve.php sql injection	classified as critical, has been found in Campcodes Online Movie Theater Seat Reservation System 1.0. Affected by this issue is some unknown functionality of the file /reserve.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.	rule	
CVE-2025-7457	Campcodes Online Movie Theater Seat Reservation System manage_movie.php sql injection	A vulnerability, which was classified as critical, was found in Campcodes Online Movie Theater Seat Reservation System 1.0. This affects an unknown part of the file /admin/manage_movie.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-2025-7459	code-projects Mobile Shop EditMobile.php sql injection	A vulnerability classified as critical was found in code-projects Mobile Shop 1.0. This vulnerability affects unknown code of the file /EditMobile.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-2025-7461	code-projects Modern Bag action.php sql injection	A vulnerability was found in code-projects Modern Bag 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /action.php. The manipulation of the argument proId 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-2025-7466	1000projects ABC Courier Management add_dealerrequest.php sql injection	A vulnerability, which was classified as critical, has been found in 1000projects ABC Courier Management 1.0. Affected by this issue is some unknown functionality of the file /add_dealerrequest.php. The manipulation of the argument Name leads to sql injection. The attack may be launched 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-2025-7467	code-projects Modern Bag product-detail.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Modern Bag 1.0. This affects an unknown part of the file /product-detail.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-2025-7469	Campcodes Sales and Inventory System product_add.php sql injection	A vulnerability was found in Campcodes Sales and Inventory System 1.0 and classified as critical. This issue affects some unknown processing of the file /pages/product_add.php. The manipulation of the argument prod_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-2025-7471	code-projects Modern Bag login-back.php sql injection	A vulnerability was found in code-projects Modern Bag 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/login-back.php. The manipulation of the argument user-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-2025-7474	code-projects Job Diary search.php sql injection	A vulnerability was found in code-projects Job Diary 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /search.php. The manipulation of the argument Search 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-2025-7475	code-projects Simple Car Rental System pay.php sql injection	A vulnerability classified as critical has been found in code-projects Simple Car Rental System 1.0. This affects an unknown part of the file /pay.php. The manipulation of the argument mpesa leads to sql injection. It is possible to initiate the attack 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.		
CVE-2025-7476	code-projects Simple Car Rental System approve.php sql injection	A vulnerability classified as critical was found in code-projects Simple Car Rental System 1.0. This vulnerability affects unknown code of the file /admin/approve.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-2025-7478	code-projects Modern Bag category-list.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Modern Bag 1.0. Affected is an unknown function of the file /admin/category-list.php. The manipulation of the argument idCate 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-2025-7479	PHPGurukul Vehicle Parking Management System view--detail.php sql injection	A vulnerability has been found in PHPGurukul Vehicle Parking Management System 1.13 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /users/view--detail.php. The manipulation of the argument viewid 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-2025-7480	PHPGurukul Vehicle Parking Management System signup.php sql injection	A vulnerability was found in PHPGurukul Vehicle Parking Management System 1.13 and classified as critical. Affected by this issue is some unknown functionality of the file /users/signup.php. The manipulation of the argument email 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-2025-7481	PHPGurukul Vehicle Parking Management System profile.php sql injection	A vulnerability was found in PHPGurukul Vehicle Parking Management System 1.13. It has been classified as critical. This affects an unknown part of the file /users/profile.php. The manipulation of the argument firstname leads to sql injection. It is possible to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		initiate the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.		
CVE-2025-7482	PHPGurukul Vehicle Parking Management System print.php sql injection	A vulnerability was found in PHPGurukul Vehicle Parking Management System 1.13. It has been declared as critical. This vulnerability affects unknown code of the file /users/print.php. The manipulation of the argument vid 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-2025-7483	PHPGurukul Vehicle Parking Management System forgot-password.php sql injection	A vulnerability was found in PHPGurukul Vehicle Parking Management System 1.13. It has been rated as critical. This issue affects some unknown processing of the file /users/forgot-password.php. The manipulation of the argument email 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-2025-7484	PHPGurukul Vehicle Parking Management System view-outgoingvehicle-detail.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Vehicle Parking Management System 1.13. Affected is an unknown function of the file /admin/view-outgoingvehicle-detail.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-2025-7489	PHPGurukul Vehicle Parking Management System search-vehicle.php sql injection	A vulnerability was found in PHPGurukul Vehicle Parking Management System 1.13 and classified as critical. This issue affects some unknown processing of the file /admin/search-vehicle.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-2025-7490	PHPGurukul Vehicle Parking Management System reg-users.php sql	A vulnerability was found in PHPGurukul Vehicle Parking Management System 1.13. It	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	has been classified as critical. Affected is an unknown function of the file /admin/reg-users.php. The manipulation of the argument del 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-2025-7491	PHPGurukul Vehicle Parking Management System manage-outgoingvehicle.php sql injection	A vulnerability was found in PHPGurukul Vehicle Parking Management System 1.13. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/manage-outgoingvehicle.php. The manipulation of the argument del 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-2025-7492	PHPGurukul Vehicle Parking Management System manage-incomingvehicle.php sql injection	A vulnerability was found in PHPGurukul Vehicle Parking Management System 1.13. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/manage-incomingvehicle.php. The manipulation of the argument del 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-2025-7508	code-projects Modern Bag product-update.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Modern Bag 1.0. Affected by this issue is some unknown functionality of the file /admin/product-update.php. The manipulation of the argument idProduct 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-2025-1735	pgsql extension does not check for errors during escaping	In PHP versions:8.1.* before 8.1.33, 8.2.* before 8.2.29, 8.3.* before 8.3.23, 8.4.* pgsql and pdo_pgsql escaping functions do not check if the underlying quoting functions returned errors. This could cause crashes if Postgres server rejects the string as invalid.	Patched by core rule	Y
CVE-2025-7509	code-projects Modern Bag slide.php sql injection	A vulnerability, which was classified as critical, was found in code-projects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Modern Bag 1.0. This affects an unknown part of the file /admin/slide.php. The manipulation of the argument idSlide 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-2025-7510	code-projects Modern Bag productadd_back.php sql injection	A vulnerability has been found in code-projects Modern Bag 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/productadd_back.php. The manipulation of the argument namepro 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-2025-7511	code-projects Chat System update_account.php sql injection	A vulnerability was found in code-projects Chat System 1.0 and classified as critical. This issue affects some unknown processing of the file /user/update_account.php. The manipulation of the argument musername 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-2025-7512	code-projects Modern Bag contact-back.php sql injection	A vulnerability was found in code-projects Modern Bag 1.0. It has been classified as critical. Affected is an unknown function of the file /contact-back.php. The manipulation of the argument contact-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-2025-7513	code-projects Modern Bag slideupdate.php sql injection	A vulnerability was found in code-projects Modern Bag 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/slideupdate.php. The manipulation of the argument idSlide 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-2025-7514	code-projects Modern Bag contact-list.php sql	A vulnerability was found in code-projects Modern Bag	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/contact-list.php. The manipulation of the argument idStatus leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-7515	code-projects Online Appointment Booking System ulocateus.php sql injection	A vulnerability classified as critical has been found in code-projects Online Appointment Booking System 1.0. This affects an unknown part of the file /ulocateus.php. The manipulation of the argument doctorname 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-2025-7516	code-projects Online Appointment Booking System cancelbookingpatient.php sql injection	A vulnerability classified as critical was found in code-projects Online Appointment Booking System 1.0. This vulnerability affects unknown code of the file /cancelbookingpatient.php. The manipulation of the argument appointment 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-2025-7517	code-projects Online Appointment Booking System getDay.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Online Appointment Booking System 1.0. This issue affects some unknown processing of the file /getDay.php. The manipulation of the argument cidval 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-2025-7520	PHPGurukul Vehicle Parking Management System manage-category.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Vehicle Parking Management System 1.13. This issue affects some unknown processing of the file /admin/manage-category.php. The manipulation of the argument del leads to sql injection. The attack may be initiated remotely. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit has been disclosed to the public and may be used.		
CVE-2025-7521	PHPGurukul Vehicle Parking Management System index.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Vehicle Parking Management System 1.13. Affected is an unknown function of the file /admin/index.php. 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.	Patched by core rule	Y
CVE-2025-7522	PHPGurukul Vehicle Parking Management System bwdates-reports-details.php sql injection	A vulnerability has been found in PHPGurukul Vehicle Parking Management System 1.13 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/bwdates-reports-details.php. The manipulation of the argument fromdate/todate 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-2025-7524	TOTOLINK T6 HTTP POST Request cstecgi.cgi setDiagnosisCfg command injection	A vulnerability was found in TOTOLINK T6 4.1.5cu.748_B20211015. It has been classified as critical. This affects the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi of the component HTTP POST Request Handler. The manipulation of the argument ip leads to command 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-2025-7525	TOTOLINK T6 HTTP POST Request cstecgi.cgi setTracerouteCfg command injection	A vulnerability was found in TOTOLINK T6 4.1.5cu.748_B20211015. It has been declared as critical. This vulnerability affects the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi of the component HTTP POST Request Handler. The manipulation of the argument command leads to command 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-2025-7533	code-projects Job Diary	A vulnerability was found in	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	view-details.php sql injection	code-projects Job Diary 1.0 and classified as critical. This issue affects some unknown processing of the file /view-details.php. The manipulation of the argument job_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	rule	
CVE-2025-7534	PHPGurukul Student Result Management System GET Parameter notice-details.php sql injection	A vulnerability was found in PHPGurukul Student Result Management System 2.0. It has been classified as critical. Affected is an unknown function of the file /notice-details.php of the component GET Parameter Handler. The manipulation of the argument nid 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-2025-7535	Campcodes Sales and Inventory System reprint_cash.php sql injection	A vulnerability was found in Campcodes Sales and Inventory System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /pages/reprint_cash.php. The manipulation of the argument sid 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-2025-7536	Campcodes Sales and Inventory System receipt_credit.php sql injection	A vulnerability was found in Campcodes Sales and Inventory System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /pages/receipt_credit.php. The manipulation of the argument sid 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-2025-7537	Campcodes Sales and Inventory System product_update.php sql injection	A vulnerability classified as critical has been found in Campcodes Sales and Inventory System 1.0. This affects an unknown part of the file /pages/product_update.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack 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.		
CVE-2025-7539	code-projects Online Appointment Booking System getdoctordaybooking.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Online Appointment Booking System 1.0. This issue affects some unknown processing of the file /getdoctordaybooking.php. The manipulation of the argument cid 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-2025-7540	code-projects Online Appointment Booking System getclinic.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Online Appointment Booking System 1.0. Affected is an unknown function of the file /getclinic.php. The manipulation of the argument townid 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-2025-7541	code-projects Online Appointment Booking System get_town.php sql injection	A vulnerability has been found in code-projects Online Appointment Booking System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /get_town.php. The manipulation of the argument countryid 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-2025-7542	PHPGurukul User Registration & Login and User Management System user-profile.php sql injection	A vulnerability was found in PHPGurukul User Registration & Login and User Management System 3.3 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/user-profile.php. The manipulation of the argument uid 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-2025-7543	PHPGurukul User	A vulnerability was found in	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Registration & Login and User Management System manage-users.php sql injection	PHPGurukul User Registration & Login and User Management System 3.3. It has been classified as critical. This affects an unknown part of the file /admin/manage-users.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.	rule	
CVE-2025-53639	Metersphere has SQL Injection Vulnerability in Sorting Field	MeterSphere is an open source continuous testing platform. Prior to version 3.6.5-lts, the sortField parameter in certain API endpoints is not properly validated or sanitized. An attacker can supply crafted input to inject and execute arbitrary SQL statements through the sorting functionality. This could result in modification or deletion of database contents, with a potential full compromise of the application's database integrity and availability. Version 3.6.5-lts fixes the issue.	Patched by core rule	Y
CVE-2025-7555	code-projects Voting System voters_add.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Voting System 1.0. This issue affects some unknown processing of the file /admin/voters_add.php. The manipulation of the argument firstname/lastname 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-2025-7556	code-projects Voting System voters_edit.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Voting System 1.0. Affected is an unknown function of the file /admin/voters_edit.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-2025-7557	code-projects Voting System voters_row.php sql injection	A vulnerability has been found in code-projects Voting System 1.0 and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/voters_row.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-2025-7558	code-projects Voting System positions_add.php sql injection	A vulnerability was found in code-projects Voting System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/positions_add.php. The manipulation of the argument description 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-2025-7559	PHPGurukul Online Fire Reporting System bwdates-report-result.php sql injection	A vulnerability was found in PHPGurukul Online Fire Reporting System 1.2. It has been classified as critical. This affects an unknown part of the file /admin/bwdates-report-result.php. The manipulation of the argument fromdate/todate 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-2025-7560	PHPGurukul Online Fire Reporting System workin-progress-requests.php sql injection	A vulnerability was found in PHPGurukul Online Fire Reporting System 1.2. It has been declared as critical. This vulnerability affects unknown code of the file /admin/workin-progress-requests.php. The manipulation of the argument teamid 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-2025-7561	PHPGurukul Online Fire Reporting System team-ontheway-requests.php sql injection	A vulnerability was found in PHPGurukul Online Fire Reporting System 1.2. It has been rated as critical. This issue affects some unknown processing of the file /admin/team-ontheway-requests.php. The manipulation of the argument teamid 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-2025-7562	PHPGurukul Online Fire Reporting System new-requests.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 /admin/new-requests.php. The manipulation of the argument teamid 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-2025-7563	PHPGurukul Online Fire Reporting System completed-requests.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/completed-requests.php. The manipulation of the argument teamid 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-2025-7568	qianfox FoxCMS Video.php batchCope sql injection	A vulnerability was found in qianfox FoxCMS up to 1.2.5. It has been classified as critical. Affected is the function batchCope of the file app/admin/controller/Video.php. The manipulation of the argument ids 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-2025-7580	code-projects Voting System positions_row.php sql injection	A vulnerability classified as critical was found in code-projects Voting System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/positions_row.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-2025-7581	code-projects Voting System positions_edit.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Voting System 1.0. Affected	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		by this issue is some unknown functionality of the file /admin/positions_edit.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.		
CVE-2025-7582	PHPGurukul Online Fire Reporting System assigned-requests.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Online Fire Reporting System 1.2. This affects an unknown part of the file /admin/assigned-requests.php. The manipulation of the argument teamid 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-2025-7583	PHPGurukul Online Fire Reporting System all-requests.php sql injection	A vulnerability has been found in PHPGurukul Online Fire Reporting System 1.2 and classified as critical. This vulnerability affects unknown code of the file /admin/all-requests.php. The manipulation of the argument teamid 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-2025-7584	PHPGurukul Online Fire Reporting System add-team.php sql injection	A vulnerability was found in PHPGurukul Online Fire Reporting System 1.2 and classified as critical. This issue affects some unknown processing of the file /admin/add-team.php. The manipulation of the argument teammember 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-2025-7585	PHPGurukul Online Fire Reporting System manage-site.php sql injection	A vulnerability was found in PHPGurukul Online Fire Reporting System 1.2. It has been classified as critical. Affected is an unknown function of the file /admin/manage-site.php. The manipulation of the argument webtitle 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-2025-7587	code-projects Online Appointment Booking System cover.php sql injection	A vulnerability was found in code-projects Online Appointment Booking System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /cover.php. The manipulation of the argument uname/psw 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-2025-7588	PHPGurukul Dairy Farm Shop Management System edit-product.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Dairy Farm Shop Management System 1.3. This affects an unknown part of the file edit-product.php. The manipulation of the argument productname 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-2025-7589	PHPGurukul Dairy Farm Shop Management System edit-company.php sql injection	A vulnerability classified as critical was found in PHPGurukul Dairy Farm Shop Management System 1.3. This vulnerability affects unknown code of the file edit-company.php. The manipulation of the argument companyname 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-2025-7590	PHPGurukul Dairy Farm Shop Management System edit-category.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Dairy Farm Shop Management System 1.3. This issue affects some unknown processing of the file edit-category.php. The manipulation of the argument categorycode 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-2025-7591	PHPGurukul Dairy Farm Shop Management System view-invoice.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Dairy Farm Shop Management System 1.3. Affected is an unknown function of the file view-invoice.php. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument invid 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-2025-7592	PHPGurukul Dairy Farm Shop Management System invoices.php sql injection	A vulnerability has been found in PHPGurukul Dairy Farm Shop Management System 1.3 and classified as critical. Affected by this vulnerability is an unknown functionality of the file invoices.php. The manipulation of the argument del 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-2025-7593	code-projects Job Diary view-all.php sql injection	A vulnerability was found in code-projects Job Diary 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /view-all.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-2025-7594	code-projects Job Diary view-emp.php sql injection	A vulnerability was found in code-projects Job Diary 1.0. It has been classified as critical. This affects an unknown part of the file /view-emp.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-2025-7595	code-projects Job Diary view-cad.php sql injection	A vulnerability was found in code-projects Job Diary 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /view-cad.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-2025-7599	PHPGurukul Dairy Farm Shop Management System invoice.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Dairy Farm Shop Management System 1.3. Affected by this issue is some unknown functionality of the file /invoice.php. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument del leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-7600	PHPGurukul Online Library Management System student-history.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Online Library Management System 3.0. This affects an unknown part of the file /admin/student-history.php. The manipulation of the argument stdid 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-2025-7604	PHPGurukul Hospital Management System user-login.php sql injection	A vulnerability was found in PHPGurukul Hospital Management System 4.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /user-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-2025-7605	code-projects AVL Rooms profile.php sql injection	A vulnerability was found in code-projects AVL Rooms 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /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-2025-7606	code-projects AVL Rooms city.php sql injection	A vulnerability classified as critical has been found in code-projects AVL Rooms 1.0. This affects an unknown part of the file /city.php. The manipulation of the argument city 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-2025-7607	code-projects Simple Shopping Cart save_order.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Simple Shopping Cart 1.0. This issue affects some unknown processing of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file /Customers/save_order.php. The manipulation of the argument order_price leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-7608	code-projects Simple Shopping Cart userlogin.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Simple Shopping Cart 1.0. Affected is an unknown function of the file /userlogin.php. The manipulation of the argument user_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-2025-7609	code-projects Simple Shopping Cart register.php sql injection	A vulnerability has been found in code-projects Simple Shopping Cart 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /register.php. The manipulation of the argument ruser_email 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-2025-7610	code-projects Electricity Billing System change_password.php sql injection	A vulnerability was found in code-projects Electricity Billing System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /user/change_password.php. The manipulation of the argument new_password 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-2025-7611	code-projects Wedding Reservation global.php sql injection	A vulnerability was found in code-projects Wedding Reservation 1.0. It has been classified as critical. This affects an unknown part of the file /global.php. The manipulation of the argument lu 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-7612	code-projects Mobile Shop login.php sql injection	A vulnerability was found in code-projects Mobile Shop 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /login.php. The manipulation of the argument email 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-2025-53937	WeGIA has SQL Injection (Blind Time-Based) Vulnerability in `cargo` Parameter on `control.php` Endpoint	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A SQL Injection vulnerability was identified in the `/controle/control.php` endpoint, specifically in the `cargo` parameter, of WeGIA prior to version 3.4.5. This vulnerability allows attackers to execute arbitrary SQL commands, compromising the confidentiality, integrity, and availability of the database. Version 3.4.5 fixes the issue.	Patched by core rule	Y
CVE-2025-53946	WeGIA vulnerable to SQL Injection in endpoint profile_paciente.php parameter id_fichamedica	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A SQL Injection vulnerability was identified in versions prior to 3.4.5 in the `id_funcionario` parameter of the `/html/saude/profile_paciente.php` endpoint. This vulnerability allows attacker to manipulate SQL queries and access sensitive database information, such as table names and sensitive data. Version 3.4.5 fixes the issue.	Patched by core rule	Y
CVE-2025-54058	WeGIA SQL Injection (Blind Time-Based) Vulnerability in idatendido_familiares Parameter on dependente_editarEnderecо.php Endpoint	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A SQL Injection vulnerability was identified in versions prior to 3.4.6 in the `idatendido_familiares` parameter of the `/html/funcionario/dependente_editarEndereco.php` endpoint. This vulnerability allows attacker to manipulate SQL queries and access sensitive database information, such as table names and sensitive data. Version 3.4.6 fixes the issue.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-54060	WeGIA SQL Injection (Blind Time-Based) Vulnerability in idatendido_familiares Parameter on dependente_editarInfoPessoal.php Endpoint	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A SQL Injection vulnerability was identified in versions prior to 3.4.6 in the `idatendido_familiares` parameter of the `/html/funcionario/dependente_editarInfoPessoal.php` endpoint. This vulnerability allows attacker to manipulate SQL queries and access sensitive database information, such as table names and sensitive data. Version 3.4.6 fixes the issue.	Patched by core rule	Y
CVE-2025-54061	WeGIASQL Injection (Blind Time-Based) Vulnerability in idatendido_familiares Parameter on dependente_editarDoc.php Endpoint	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A SQL Injection vulnerability was identified in versions prior to 3.4.6 in the `idatendido_familiares` parameter of the `/html/funcionario/dependente_editarDoc.php` endpoint. This vulnerability allows attacker to manipulate SQL queries and access sensitive database information, such as table names and sensitive data. Version 3.4.6 fixes the issue.	Patched by core rule	Y
CVE-2025-54062	WeGIA SQL Injection (Blind Time-Based) Vulnerability in id_dependente Parameter on profile_dependente.php Endpoint	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A SQL Injection vulnerability was identified in versions prior to 3.4.6 in the `/html/funcionario/profile_dependente.php` endpoint, specifically in the `id_dependente` parameter. This vulnerability allows attackers to execute arbitrary SQL commands, compromising the confidentiality, integrity, and availability of the database. Version 3.4.6 fixes the issue.	Patched by core rule	Y
CVE-2025-7749	code-projects Online Appointment Booking System getmanagerregion.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Online Appointment Booking System 1.0. This issue affects some unknown processing of the file /admin/getmanagerregion.php. The manipulation of the argument city leads to sql injection. The attack may 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-2025-7750	code-projects Online Appointment Booking System adddoctorclinic.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Online Appointment Booking System 1.0. Affected is an unknown function of the file /admin/adddoctorclinic.php. The manipulation of the argument clinic 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-2025-7751	code-projects Online Appointment Booking System addclinic.php sql injection	A vulnerability has been found in code-projects Online Appointment Booking System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/addclinic.php. The manipulation of the argument cid 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-2025-7752	code-projects Online Appointment Booking System deletedoctor.php sql injection	A vulnerability was found in code-projects Online Appointment Booking System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/deletedoctor.php. The manipulation of the argument did 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-2025-7753	code-projects Online Appointment Booking System adddoctor.php sql injection	A vulnerability was found in code-projects Online Appointment Booking System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/adddoctor.php. The manipulation of the argument Username 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-2025-7754	code-projects Patient Record Management System xray_form.php sql injection	A vulnerability was found in code-projects Patient Record Management System 1.0. It has been declared as critical. This vulnerability affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown code of the file /xray_form.php. The manipulation of the argument itr_no leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-7757	PHPGurukul Land Record System edit-property.php sql injection	A vulnerability classified as critical was found in PHPGurukul Land Record System 1.0. Affected by this vulnerability is an unknown functionality of the file /edit-property.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-2025-7764	code-projects Online Appointment Booking System deletedoctorclinic.php sql injection	A vulnerability classified as critical has been found in code-projects Online Appointment Booking System 1.0. Affected is an unknown function of the file /admin/deletedoctorclinic.php. The manipulation of the argument clinic 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-2025-7765	code-projects Online Appointment Booking System addmanagerclinic.php sql injection	A vulnerability classified as critical was found in code-projects Online Appointment Booking System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/addmanagerclinic.php. The manipulation of the argument clinic 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-2025-49484	Extension - joomsky.com - SQL injection in JS jobs component version 1.1.5 - 1.4.1 for Joomla	A SQL injection vulnerability in the JS Jobs plugin versions 1.0.0-1.4.1 for Joomla allows low-privilege users to execute arbitrary SQL commands via the 'cvid' parameter in the employee application feature.	Patched by core rule	Y
CVE-2025-54073	mcp-package-docs vulnerable to command injection in several tools	mcp-package-docs is an MCP (Model Context Protocol) server that provides LLMs with efficient access to package documentation across multiple programming languages and language server protocol	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		(LSP) capabilities. A command injection vulnerability exists in the `mcp-package-docs` MCP Server prior to the fix in commit cb4ad49615275379fd6f2f1cf1ec4731eec56eb9. The vulnerability is caused by the unsanitized use of input parameters within a call to `child_process.exec`, enabling an attacker to inject arbitrary system commands. Successful exploitation can lead to remote code execution under the server process's privileges. The server constructs and executes shell commands using unvalidated user input directly within command-line strings. This introduces the possibility of shell metacharacter injection (`|`, `>`, `&&`, etc.). Commit cb4ad49615275379fd6f2f1cf1ec4731eec56eb9 in version 0.1.27 contains a fix for the issue, but upgrading to 0.1.28 is recommended.		
CVE-2025-7798	Beijing Shenzhou Shihan Technology Multimedia Integrated Business Display System companyManage sql injection	A vulnerability classified as critical has been found in Beijing Shenzhou Shihan Technology Multimedia Integrated Business Display System up to 8.2. This affects an unknown part of the file /admin/system/structure/getdirectorydata/web/baseinfo/companyManage. The manipulation of the argument Struccture_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-2025-7801	BossSoft CRM HNDCBas_customPrmSearchDtl.jsp sql injection	A vulnerability has been found in BossSoft CRM 6.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /crm/module/HNDCBas_customPrmSearchDtl.jsp. The manipulation of the argument cstid 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-2025-7814	code-projects Food Ordering Review System	A vulnerability classified as critical was found in code-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	signup_function.php sql injection	projects Food Ordering Review System 1.0. This vulnerability affects unknown code of the file /pages/signup_function.php. The manipulation of the argument fname 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.		
CVE-2025-7829	code-projects Church Donation System login.php sql injection	A vulnerability was found in code-projects Church Donation System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /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-2025-7830	code-projects Church Donation System reg.php sql injection	A vulnerability was found in code-projects Church Donation System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /reg.php. The manipulation of the argument mobile 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-2025-7831	code-projects Church Donation System Tithes.php sql injection	A vulnerability classified as critical has been found in code-projects Church Donation System 1.0. This affects an unknown part of the file /members/Tithes.php. The manipulation of the argument trcode 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-2025-7832	code-projects Church Donation System offering.php sql injection	A vulnerability classified as critical was found in code-projects Church Donation System 1.0. This vulnerability affects unknown code of the file /members/offering.php. The manipulation of the argument trcode leads to sql injection. The attack can be initiated remotely. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit has been disclosed to the public and may be used.		
CVE-2025-7833	code-projects Church Donation System giving.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Church Donation System 1.0. This issue affects some unknown processing of the file /members/giving.php. The manipulation of the argument Amount 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-2025-7838	Campcodes Online Movie Theater Seat Reservation System manage_seat.php sql injection	A vulnerability has been found in Campcodes Online Movie Theater Seat Reservation System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/manage_seat.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-2025-54314		Thor before 1.4.0 can construct an unsafe shell command from library input.	Patched by core rule	Y
CVE-2025-7859	code-projects Church Donation System update_password_admin .php sql injection	A vulnerability classified as critical was found in code-projects Church Donation System 1.0. This vulnerability affects unknown code of the file /members/update_password_admin.php. The manipulation of the argument new_password 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-2025-7860	code-projects Church Donation System login_admin.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Church Donation System 1.0. This issue affects some unknown processing of the file /members/login_admin.php. The manipulation of the argument Username 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-2025-7861	code-projects Church Donation System search.php sql injection	A vulnerability, which was classified as critical, was found in code-projects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Church Donation System 1.0. Affected is an unknown function of the file /members/search.php. 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.		
CVE-2025-7873	Metasoft 美特软件 MetaCRM mcc_login.jsp sql injection	A vulnerability was found in Metasoft 美特软件 MetaCRM up to 6.4.2. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file mcc_login.jsp. The manipulation of the argument workerid leads to sql injection. 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-2025-7888	TDuckCloud tduck-platform UserFormDataMapper.java UserFormDataMapper sql injection	A vulnerability was found in TDuckCloud tduck-platform 5.1 and classified as critical. This issue affects the function UserFormDataMapper of the file src/main/java/com/tduck/cloud/form/mapper/UserFormDataMapper.java. The manipulation of the argument formKey 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-2025-7904	itsourcecode Insurance Management System insertNominee.php sql injection	A vulnerability, which was classified as critical, was found in itsourcecode Insurance Management System 1.0. This affects an unknown part of the file /insertNominee.php. The manipulation of the argument nominee_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-2025-7905	itsourcecode Insurance Management System insertPayment.php sql	A vulnerability has been found in itsourcecode Insurance Management	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	System 1.0 and classified as critical. This vulnerability affects unknown code of the file /insertPayment.php. The manipulation of the argument recipt_no leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-52575	EspoCRM vulnerable to LDAP Injection through Improper Neutralization of Special Elements	EspoCRM is an Open Source CRM (Customer Relationship Management) software. EspoCRM versions 9.1.6 and earlier are vulnerable to blind LDAP Injection when LDAP authentication is enabled. A remote, unauthenticated attacker can manipulate LDAP queries by injecting crafted input containing wildcard characters (e.g., *). This may allow the attacker to bypass authentication controls, enumerate valid usernames, or retrieve sensitive directory information depending on the LDAP server configuration. This was fixed in version 9.1.7.	Patched by core rule	Y
CVE-2025-7915	Chanjet CRM Login Page mailinactive.php sql injection	A vulnerability was found in Chanjet CRM 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /mail/mailinactive.php of the component Login Page. The manipulation 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-2025-7927	PHPGurukul Online Banquet Booking System view-user-queries.php sql injection	A vulnerability has been found in PHPGurukul Online Banquet Booking System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/view-user-queries.php. The manipulation of the argument viewid 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-2025-7928	code-projects Church Donation System edit_user.php sql injection	A vulnerability was found in code-projects Church Donation System 1.0 and classified as critical. This issue affects some unknown processing of the file /members/edit_user.php. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument firstname 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.		
CVE-2025-7929	code-projects Church Donation System edit_Members.php sql injection	A vulnerability was found in code-projects Church Donation System 1.0. It has been classified as critical. Affected is an unknown function of the file /members/edit_Members.php. The manipulation of the argument 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-2025-7930	code-projects Church Donation System add_members.php sql injection	A vulnerability was found in code-projects Church Donation System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /members/add_members.php. The manipulation of the argument mobile 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-2025-7933	Campcodes Sales and Inventory System Setting settings_update.php sql injection	A vulnerability classified as critical was found in Campcodes Sales and Inventory System 1.0. This vulnerability affects unknown code of the file /pages/settings_update.php of the component Setting Handler. 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-2025-7934	fuyang_lipengjun platform ScheduleJobController.java queryPage sql injection	A vulnerability, which was classified as critical, has been found in fuyang_lipengjun platform up to ca9aceff6902feb7b0b6bf510842aea88430796a. This issue affects the function queryPage of the file platform-schedule/src/main/java/com/platform/controller/Schedu	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		leJobController.java. The manipulation of the argument beanName leads to sql injection. The 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-2025-7935	fuyang_lipengjun platform SysLogController.java SysLogController sql injection	A vulnerability, which was classified as critical, was found in fuyang_lipengjun platform up to ca9aceff6902feb7b0b6bf510842aea88430796a. Affected is the function SysLogController of the file platform-admin/src/main/java/com/platform/controller/SysLogController.java. The manipulation of the argument key leads to sql injection. 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-2025-7936	fuyang_lipengjun platform ScheduleJobLogController.java queryPage sql injection	A vulnerability has been found in fuyang_lipengjun platform up to ca9aceff6902feb7b0b6bf510842aea88430796a and classified as critical. Affected by this vulnerability is the function queryPage of the file com/platform/controller/ScheduleJobLogController.java. The manipulation of the argument beanName/methodName 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.	Patched by core rule	Y
CVE-2025-7950	code-projects Public Chat Room login.php sql injection	A vulnerability was found in code-projects Public Chat Room 1.0. It has been rated as critical. Affected by this issue is some unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		functionality of the file /login.php. The manipulation of the argument Username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-8018	code-projects Food Ordering Review System reservation_page.php sql injection	A vulnerability was found in code-projects Food Ordering Review System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /user/reservation_page.php. The manipulation of the argument reg_Id 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-2025-32429	XWiki Platform vulnerable to SQL injection through getdeleteddocuments.vm template sort parameter	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In versions 9.4-rc-1 through 16.10.5 and 17.0.0-rc-1 through 17.2.2, it's possible for anyone to inject SQL using the parameter sort of the getdeleteddocuments.vm. It's injected as is as an ORDER BY value. This is fixed in versions 16.10.6 and 17.3.0-rc-1.	Patched by core rule	Y
CVE-2025-54379	eKuiper API endpoints handling SQL queries with user-controlled table names.	LF Edge eKuiper is a lightweight IoT data analytics and stream processing engine running on resource-constraint edge devices. In versions before 2.2.1, there is a critical SQL Injection vulnerability in the getLast API functionality of the eKuiper project. This flaw allows unauthenticated remote attackers to execute arbitrary SQL statements on the underlying SQLite database by manipulating the table name input in an API request. Exploitation can lead to data theft, corruption, or deletion, and full database compromise. This is fixed in version 2.2.1.	Patched by core rule	Y
CVE-2025-8123	deerwms deer-wms-2 edit sql injection	A vulnerability was found in deerwms deer-wms-2 up to 3.3. It has been classified as critical. Affected is an unknown function of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/system/dept/edit. The manipulation of the argument ancestors 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-2025-8124	deerwms deer-wms-2 unallocatedList sql injection	A vulnerability was found in deerwms deer-wms-2 up to 3.3. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /system/role/authUser/unallocatedList. The manipulation of the argument params[dataScope] 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-2025-8125	deerwms deer-wms-2 allocatedList sql injection	A vulnerability was found in deerwms deer-wms-2 up to 3.3. It has been rated as critical. Affected by this issue is some unknown functionality of the file /system/role/authUser/allocatedList. The manipulation of the argument params[dataScope] 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-2025-8126	deerwms deer-wms-2 export sql injection	A vulnerability classified as critical has been found in deerwms deer-wms-2 up to 3.3. This affects an unknown part of the file /system/user/export. The manipulation of the argument params[dataScope] 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-2025-8127	deerwms deer-wms-2 list sql injection	A vulnerability classified as critical was found in deerwms deer-wms-2 up to 3.3. This vulnerability affects unknown code of the file /system/user/list. The manipulation of the argument params[dataScope] 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-2025-8134	PHPGurukul BP Monitoring Management	A vulnerability classified as critical was found in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System bwdates-report-result.php sql injection	PHPGurukul BP Monitoring Management System 1.0. This vulnerability affects unknown code of the file /bwdates-report-result.php. The manipulation of the argument fromdate/todate leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-8135	itsourcecode Insurance Management System updateAgent.php sql injection	A vulnerability, which was classified as critical, has been found in itsourcecode Insurance Management System 1.0. This issue affects some unknown processing of the file /updateAgent.php. The manipulation of the argument agent_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-2025-8156	PHPGurukul User Registration & Login and User Management lastsevendays-reg-users.php sql injection	A vulnerability was found in PHPGurukul User Registration & Login and User Management 3.3 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/lastsevendays-reg-users.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-2025-8157	PHPGurukul User Registration & Login and User Management lastthirtyays-reg-users.php sql injection	A vulnerability was found in PHPGurukul User Registration & Login and User Management 3.3. It has been classified as critical. This affects an unknown part of the file /admin/lastthirtyays-reg-users.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-2025-8158	PHPGurukul Login and User Management System yesterday-reg-users.php sql injection	A vulnerability was found in PHPGurukul Login and User Management System 3.3. It has been declared as critical. This vulnerability affects unknown code of the file /admin/yesterday-reg-users.php. The manipulation of the argument ID leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-8161	deerwms deer-wms-2 export sql injection	A vulnerability classified as critical was found in deerwms deer-wms-2 up to 3.3. Affected by this vulnerability is an unknown functionality of the file /system/role/export. The manipulation of the argument params[dataScope] 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-2025-8162	deerwms deer-wms-2 list sql injection	A vulnerability, which was classified as critical, has been found in deerwms deer-wms-2 up to 3.3. Affected by this issue is some unknown functionality of the file /system/dept/list. The manipulation of the argument params[dataScope] 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-2025-8163	deerwms deer-wms-2 list sql injection	A vulnerability, which was classified as critical, was found in deerwms deer-wms-2 up to 3.3. This affects an unknown part of the file /system/role/list. The manipulation of the argument params[dataScope] 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-2025-8164	code-projects Public Chat Room send_message.php sql injection	A vulnerability has been found in code-projects Public Chat Room 1.0 and classified as critical. This vulnerability affects unknown code of the file send_message.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-2025-8165	code-projects Food Review System approve_reservation.php sql injection	A vulnerability was found in code-projects Food Review System 1.0 and classified as critical. This issue affects some unknown processing of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/admin/approve_reservation .php. The manipulation of the argument occasion leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-8166	code-projects Church Donation System HTTP POST Request index.php sql injection	A vulnerability was found in code-projects Church Donation System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/index.php of the component HTTP POST Request Handler. 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.	Patched by core rule	Y
CVE-2025-8172	itsourcecode Employee Management System index.php sql injection	A vulnerability, which was classified as critical, was found in itsourcecode Employee Management System 1.0. Affected is an unknown function of the file /admin/index.php. 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.	Patched by core rule	Y
CVE-2025-8173	1000 Projects ABC Courier Management System Add_reciver.php sql injection	A vulnerability has been found in 1000 Projects ABC Courier Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /Add_reciver.php. The manipulation of the argument reciver_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

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-34046	Fanwei E-Office Unauthenticated File Upload	An unauthenticated file upload vulnerability exists in the Fanwei E-Office <= v9.4 web management interface. The vulnerability affects the /general/index/UploadFile.php endpoint, which improperly validates uploaded files when invoked with certain parameters (uploadType=eoffice_logo or uploadType=theme). An attacker can exploit this flaw by sending a crafted HTTP POST request to upload arbitrary files without requiring authentication. Successful exploitation could enable remote code execution on the affected server, leading to complete compromise of the web application and potentially the underlying system.	Patched by core rule	Y
CVE-2025-6837	code-projects Library System profile.php unrestricted upload	A vulnerability classified as critical was found in code-projects Library System 1.0. Affected by this vulnerability is an unknown functionality of the file /profile.php. The manipulation of the argument image leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6843	code-projects Simple Photo Gallery upload-photo.php unrestricted upload	A vulnerability was found in code-projects Simple Photo Gallery 1.0. It has been classified as critical. Affected is an unknown function of the file /upload-photo.php. The manipulation of the argument file_img leads to unrestricted upload. 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-2025-6848	code-projects Simple Forum forum1.php unrestricted upload	A vulnerability, which was classified as critical, has been found in code-projects Simple Forum 1.0. This issue affects some unknown processing of the file /forum1.php. The manipulation of the argument File leads to unrestricted upload. The attack may be initiated 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-2025-6870	SourceCodester Simple Company Website Content.php unrestricted upload	A vulnerability was found in SourceCodester Simple Company Website 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /classes/Content.php?f=service. The manipulation of the argument img leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6872	SourceCodester Simple Company Website SystemSettings.php unrestricted upload	A vulnerability classified as critical was found in SourceCodester Simple Company Website 1.0. This vulnerability affects unknown code of the file /classes/SystemSettings.php?f=update_settings. The manipulation of the argument img leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6873	SourceCodester Simple Company Website Users.php unrestricted upload	A vulnerability, which was classified as critical, has been found in SourceCodester Simple Company Website 1.0. This issue affects some unknown processing of the file /classes/Users.php?f=save. The manipulation of the argument img leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6900	code-projects Library System add-book.php unrestricted upload	A vulnerability has been found in code-projects Library System 1.0 and classified as critical. This vulnerability affects unknown code of the file /add-book.php. The manipulation of the argument image leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-23968	WordPress AiBud WP plugin <= 1.8.5 - Arbitrary File Upload vulnerability	Unrestricted Upload of File with Dangerous Type vulnerability in WPCenter AiBud WP allows Upload a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Web Shell to a Web Server.This issue affects AiBud WP: from n/a through 1.8.5.		
CVE-2025-5961	Migration, Backup, Staging – WPvivid Backup & Migration <= 0.9.116 - Authenticated (Administrator+) Arbitrary File Upload	The Migration, Backup, Staging – WPvivid Backup & Migration plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'wpvivid_upload_import_files' function in all versions up to, and including, 0.9.116. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. NOTE: Uploaded files are only accessible on WordPress instances running on the NGINX web server as the existing .htaccess within the target file upload folder prevents access on Apache servers.	Patched by core rule	Y
CVE-2025-7075	BlackVue Dashcam 590X HTTP Endpoint upload.cgi unrestricted upload	A vulnerability was found in BlackVue Dashcam 590X up to 20250624. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /upload.cgi of the component HTTP Endpoint. The manipulation leads to unrestricted upload. The attack needs to be done within the local network. 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-2025-7076	BlackVue Dashcam 590X Configuration upload.cgi access control	A vulnerability was found in BlackVue Dashcam 590X up to 20250624. It has been rated as critical. Affected by this issue is some unknown functionality of the file /upload.cgi of the component Configuration Handler. The manipulation leads to improper access controls. The attack needs to be initiated within the local network. 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-2025-7124	code-projects Online Note Sharing Profile Image userprofile.php unrestricted upload	A vulnerability classified as critical has been found in code-projects Online Note Sharing 1.0. Affected is an unknown function of the file /dashboard/userprofile.php of the component Profile Image Handler. The manipulation of the argument image leads to unrestricted upload. 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-2025-7151	Campcodes Advanced Online Voting System voters_add.php unrestricted upload	A vulnerability was found in Campcodes Advanced Online Voting System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/voters_add.php. The manipulation of the argument photo leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-7152	Campcodes Advanced Online Voting System candidates_add.php unrestricted upload	A vulnerability classified as critical has been found in Campcodes Advanced Online Voting System 1.0. Affected is an unknown function of the file /admin/candidates_add.php . The manipulation of the argument photo leads to unrestricted upload. 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-2025-0928	Arbitrary executable upload via authenticated endpoint	In Juju versions prior to 3.6.8 and 2.9.52, any authenticated controller user was allowed to upload arbitrary agent binaries to any model or to the controller itself, without verifying model membership or requiring explicit permissions. This enabled the distribution of poisoned binaries to new or upgraded machines, potentially resulting in remote code execution.	Patched by core rule	Y
CVE-2025-48384	Git allows arbitrary code execution through broken config quoting	Git is a fast, scalable, distributed revision control system with an unusually rich command set that provides both high-level operations and full access to internals. When reading a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		config value, Git strips any trailing carriage return and line feed (CRLF). When writing a config entry, values with a trailing CR are not quoted, causing the CR to be lost when the config is later read. When initializing a submodule, if the submodule path contains a trailing CR, the altered path is read resulting in the submodule being checked out to an incorrect location. If a symlink exists that points the altered path to the submodule hooks directory, and the submodule contains an executable post-checkout hook, the script may be unintentionally executed after checkout. This vulnerability is fixed in v2.43.7, v2.44.4, v2.45.4, v2.46.4, v2.47.3, v2.48.2, v2.49.1, and v2.50.1.		
CVE-2025-53512	Sensitive log retrieval in Juju	The /log endpoint on a Juju controller lacked sufficient authorization checks, allowing unauthorized users to access debug messages that could contain sensitive information.	Patched by core rule	Y
CVE-2025-7175	code-projects E-Commerce Site users_photo.php unrestricted upload	A vulnerability was found in code-projects E-Commerce Site 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/users_photo.php. The manipulation of the argument photo leads to unrestricted upload. 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-2025-7181	code-projects Staff Audit System test.php unrestricted upload	A vulnerability, which was classified as critical, was found in code-projects Staff Audit System 1.0. Affected is an unknown function of the file /test.php. The manipulation of the argument uploadedfile leads to unrestricted upload. 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-2025-7190	code-projects Library Management System student_edit_photo.php unrestricted upload	A vulnerability, which was classified as critical, was found in code-projects Library Management System 2.0. This affects an unknown part of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/admin/student_edit_photo.php. The manipulation of the argument photo leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-7210	code-projects/Fabian Ros Library Management System profile_update.php unrestricted upload	A vulnerability was found in code-projects/Fabian Ros Library Management System 2.0 and classified as critical. Affected by this issue is some unknown functionality of the file admin/profile_update.php. The manipulation of the argument photo leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-53632	Chall-Manager's scenario decoding process does not check for zip slips	Chall-Manager is a platform-agnostic system able to start Challenges on Demand of a player. When decoding a scenario (i.e. a zip archive), the path of the file to write is not checked, potentially leading to zip slips. Exploitation does not require authentication nor authorization, so anyone can exploit it. It should nonetheless not be exploitable as it is highly recommended to bury Chall-Manager deep within the infrastructure due to its large capabilities, so no users could reach the system. Patch has been implemented by commit 47d188f and shipped in v0.1.4.	Patched by core rule	Y
CVE-2025-7412	code-projects Library System profile.php unrestricted upload	A vulnerability was found in code-projects Library System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /user/student/profile.php. The manipulation of the argument image leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-7413	code-projects Library System profile.php unrestricted upload	A vulnerability classified as critical has been found in code-projects Library System 1.0. This affects an unknown part of the file /user/teacher/profile.php.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The manipulation of the argument image leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-30661	Junos OS: Low-privileged user can cause script to run as root, leading to privilege escalation	An Incorrect Permission Assignment for Critical Resource vulnerability in line card script processing of Juniper Networks Junos OS allows a local, low-privileged user to install scripts to be executed as root, leading to privilege escalation. A local user with access to the local file system can copy a script to the router in a way that will be executed as root, as the system boots. Execution of the script as root can lead to privilege escalation, potentially providing the adversary complete control of the system. This issue only affects specific line cards, such as the MPC10, MPC11, LC4800, LC9600, MX304-LMIC16, SRX4700, and EX9200-15C. This issue affects Junos OS: * from 23.2 before 23.2R2-S4, * from 23.4 before 23.4R2-S5, * from 24.2 before 24.2R2-S1, * from 24.4 before 24.4R1-S3, 24.4R2. This issue does not affect versions prior to 23.1R2.	Patched by core rule	Y
CVE-2020-36849	AIT CSV import/export <= 3.0.3 - Unauthenticated Arbitrary File Upload	The AIT CSV import/export plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the /wp-content/plugins/ait-csv-import-export/admin/upload-handler.php file in versions up to, and including, 3.0.3. This makes it possible for unauthorized attackers to upload arbitrary files on the affected sites server which may make remote code	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		execution possible.		
CVE-2025-7470	Campcodes Sales and Inventory System product_add.php unrestricted upload	A vulnerability was found in Campcodes Sales and Inventory System 1.0. It has been classified as critical. Affected is an unknown function of the file /pages/product_add.php. The manipulation of the argument image leads to unrestricted upload. 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-2025-7477	code-projects Simple Car Rental System add_cars.php unrestricted upload	A vulnerability, which was classified as critical, has been found in code-projects Simple Car Rental System 1.0. This issue affects some unknown processing of the file /admin/add_cars.php. The manipulation of the argument image leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-7487	JoeyBling SpringBoot_MyBatisPlus upload SysFileController unrestricted upload	A vulnerability, which was classified as critical, was found in JoeyBling SpringBoot_MyBatisPlus up to a6a825513bd688f717dbae3a196bc9c9622fea26. This affects the function SysFileController of the file /file/upload. The manipulation of the argument portraitFile leads to unrestricted upload. It is possible to initiate the attack 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-2025-7547	Campcodes Online Movie Theater Seat Reservation System admin_class.php save_movie unrestricted upload	A vulnerability, which was classified as critical, was found in Campcodes Online Movie Theater Seat Reservation System 1.0. This affects the function save_movie of the file /admin/admin_class.php. The manipulation of the argument cover leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		been disclosed to the public and may be used.		
CVE-2025-7627	YiJiuSmile kkFileViewOfficeEdit fileUpload unrestricted upload	A vulnerability was found in YiJiuSmile kkFileViewOfficeEdit up to 5fbc57c48e8fe6c1b91e0e7995e2d59615f37abd and classified as critical. Affected by this issue is the function fileUpload of the file /fileUpload. The manipulation of the argument File leads to unrestricted upload. The attack may be launched 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-2025-53891	TIME LINE has Improper File Validation in Upload Section	The timelineofficial/Time-Line- repository contains the source code for the TIME LINE website. A vulnerability was found in the TIME LINE website where uploaded files (instruction/message media) are not strictly validated for type and size. A user may upload renamed or oversized files that can disrupt performance or bypass restrictions. This could result in malicious file upload, denial of service, or client-side crashes. Version 1.0.5 contains a fix for the issue.	Patched by core rule	Y
CVE-2025-7755	code-projects Online Ordering System edit_product.php unrestricted upload	A vulnerability was found in code-projects Online Ordering System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/edit_product.php. The manipulation of the argument image leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2015-10135	WPshop 2 – E-Commerce < 1.3.9.6 - Arbitrary File Upload	The WPshop 2 – E-Commerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the ajaxUpload function in versions before 1.3.9.6. This makes it possible for unauthenticated attackers to upload arbitrary files on the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affected sites server which may make remote code execution possible.		
CVE-2025-7864	thinkgem JeeSite FileUploadController.java upload unrestricted upload	A vulnerability was found in thinkgem JeeSite up to 5.12.0. It has been classified as critical. This affects the function Upload of the file src/main/java/com/jeesite/modules/file/web/FileUploadController.java. The manipulation leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is 3585737d21fe490ff6948d913fcbd8d99c41fc08. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y
CVE-2025-7877	Metasoft 美特软件 MetaCRM sendfile.jsp unrestricted upload	A vulnerability, which was classified as critical, has been found in Metasoft 美特软件 MetaCRM up to 6.4.2. This issue affects some unknown processing of the file sendfile.jsp. The manipulation of the argument File leads to unrestricted upload. 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-2025-7878	Metasoft 美特软件 MetaCRM upload2.jsp unrestricted upload	A vulnerability, which was classified as critical, was found in Metasoft 美特软件 MetaCRM up to 6.4.2. Affected is an unknown function of the file /common/jsp/upload2.jsp. The manipulation of the argument File leads to unrestricted upload. 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-2025-7879	Metasoft 美特软件 MetaCRM mobileupload.jsp unrestricted upload	A vulnerability has been found in Metasoft 美特软件 MetaCRM up to 6.4.2 and classified as critical. Affected by this vulnerability is an unknown functionality of the file mobileupload.jsp. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument File leads to unrestricted upload. 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.		
CVE-2025-7880	Metasoft 美特软件 MetaCRM sendsms.jsp unrestricted upload	A vulnerability was found in Metasoft 美特软件 MetaCRM up to 6.4.2 and classified as critical. Affected by this issue is some unknown functionality of the file /business/common/sms/sendsms.jsp. The manipulation of the argument File leads to unrestricted upload. 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-2025-7906	yangzongzhuan RuoYi CommonController.java uploadFile unrestricted upload	A vulnerability was found in yangzongzhuan RuoYi up to 4.8.1 and classified as critical. This issue affects the function uploadFile of the file ruoyi-admin/src/main/java/com/ruoyi/web/controller/common/CommonController.java. The manipulation of the argument File leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-54071	RomM's authenticated arbitrary file write vulnerability can lead to Remote Code Execution	RomM (ROM Manager) allows users to scan, enrich, browse and play their game collections with a clean and responsive interface. In versions 4.0.0-beta.3 and below, an authenticated arbitrary file write vulnerability exists in the /api/saves endpoint. This can lead to Remote Code Execution on the system. The vulnerability permits arbitrary file write operations, allowing attackers to create or modify files at any filesystem location with user-supplied content. A user with viewer role or Scope.ASSETS_WRITE permission or above is required to pass authentication checks. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability is fixed in version 4.0.0-beta.4.		
CVE-2025-54082	nova-tiptap has an Unauthenticated Arbitrary File Upload Vulnerability	marshmallow-packages/nova-tiptap is a rich text editor for Laravel Nova based on tiptap. Prior to 5.7.0, a vulnerability was discovered in the marshmallow-packages/nova-tiptap Laravel Nova package that allows unauthenticated users to upload arbitrary files to any Laravel disk configured in the application. The vulnerability is due to missing authentication middleware (Nova and Nova.Auth) on the /nova-tiptap/api/file upload endpoint, the lack of validation on uploaded files (no MIME/type or extension restrictions), and the ability for an attacker to choose the disk parameter dynamically. This means an attacker can craft a custom form and send a POST request to /nova-tiptap/api/file, supplying a valid CSRF token, and upload executable or malicious files (e.g., .php, binaries) to public disks such as local, public, or s3. If a publicly accessible storage path is used (e.g. S3 with public access, or Laravel's public disk), the attacker may gain the ability to execute or distribute arbitrary files — amounting to a potential Remote Code Execution (RCE) vector in some environments. This vulnerability was fixed in 5.7.0.	Patched by core rule	Y
CVE-2025-7931	code-projects Church Donation System admin_pic.php unrestricted upload	A vulnerability was found in code-projects Church Donation System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /members/admin_pic.php. The manipulation of the argument image leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-7939	jerryshensjf JPACookieShop 蛋糕商城 JPA版	A vulnerability was found in jerryshensjf JPACookieShop 蛋糕商城JPA版 1.0. It has been classified as critical.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	GoodsController.java addGoods unrestricted upload	Affected is the function addGoods of the file GoodsController.java. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely.		
CVE-2025-54140	pyLoad has Path Traversal Vulnerability in json/upload Endpoint that allows Arbitrary File Write	pyLoad is a free and open-source Download Manager written in pure Python. In version 0.5.0b3.dev89, an authenticated path traversal vulnerability exists in the /json/upload endpoint of pyLoad. By manipulating the filename of an uploaded file, an attacker can traverse out of the intended upload directory, allowing them to write arbitrary files to any location on the system accessible to the pyLoad process. This may lead to: Remote Code Execution (RCE), local privilege escalation, system-wide compromise, persistence, and backdoors. This is fixed in version 0.5.0b3.dev90.	Patched by core rule	Y
CVE-2025-8128	zhousg letao product.js unrestricted upload	A vulnerability, which was classified as critical, has been found in zhousg letao up to 7d8df0386a6522847629094 9e0413de48f7fbe98. This issue affects some unknown processing of the file routes\bf\product.js. The manipulation of the argument pictrdtz leads to unrestricted upload. 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-2025-8171	code-projects Document Management System insert.php unrestricted upload	A vulnerability, which was classified as critical, has been found in code-projects Document Management System 1.0. This issue affects some unknown processing of the file /insert.php. The manipulation of the argument uploaded_file leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y

Remote Code Execution Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-34044	WIFISKY 7-Layer Flow Control Router Remote Command Execution	A remote command injection vulnerability exists in the confirm.php interface of the WIFISKY 7-layer Flow Control Router via a specially-crafted HTTP GET request to the t parameter. Insufficient input validation allows unauthenticated attackers to execute arbitrary OS commands.	Y	N
CVE-2025-52903	File Browser Allows Execution of Shell Commands That Can Spawn Other Commands	File Browser provides a file managing interface within a specified directory and it can be used to upload, delete, preview, rename and edit files. In version 2.32.0, the Command Execution feature of File Browser only allows the execution of shell command which have been predefined on a user-specific allowlist. Many tools allow the execution of arbitrary different commands, rendering this limitation void. The concrete impact depends on the commands being granted to the attacker, but the large number of standard commands allowing the execution of subcommands makes it likely that every user having the `Execute commands` permissions can exploit this vulnerability. Everyone who can exploit it will have full code execution rights with the uid of the server process. Until this issue is fixed, the maintainers recommend to completely disable `Execute commands` for all accounts. Since the command execution is an inherently dangerous feature that is not used by all deployments, it should be possible to completely disable it in the application's configuration. As a defense-in-depth measure, organizations not requiring command execution should operate the Filebrowser from a distroless container image. A patch version has been pushed to disable the feature for all existent installations, and making it opt-in. A warning has been added to the documentation	Y	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and is printed on the console if the feature is enabled. Due to the project being in maintenance-only mode, the bug has not been fixed. The fix is tracked on pull request 5199.		
CVE-2025-52904	File Browser: Command Execution not Limited to Scope	File Browser provides a file managing interface within a specified directory and it can be used to upload, delete, preview, rename and edit files. In version 2.32.0 of the web application, all users have a scope assigned, and they only have access to the files within that scope. The Command Execution feature of Filebrowser allows the execution of shell commands which are not restricted to the scope, potentially giving an attacker read and write access to all files managed by the server. Until this issue is fixed, the maintainers recommend to completely disable `Execute commands` for all accounts. Since the command execution is an inherently dangerous feature that is not used by all deployments, it should be possible to completely disable it in the application's configuration. As a defense-in-depth measure, organizations not requiring command execution should operate the Filebrowser from a distroless container image. A patch version has been pushed to disable the feature for all existent installations, and making it opt-in. A warning has been added to the documentation and is printed on the console if the feature is enabled. Due to the project being in maintenance-only mode, the bug has not been fixed. Fix is tracked on pull request 5199.	Y	N
CVE-2025-53002	LLaMA-Factory Remote Code Execution (RCE) Vulnerability	LLaMA-Factory is a tuning library for large language models. A remote code execution vulnerability was discovered in LLaMA-Factory versions up to and including 0.9.3 during the LLaMA-Factory training process. This vulnerability arises because the `vhead_file` is loaded without proper safeguards, allowing	Y	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		malicious attackers to execute arbitrary malicious code on the host system simply by passing a malicious `Checkpoint path` parameter through the `WebUI` interface. The attack is stealthy, as the victim remains unaware of the exploitation. The root cause is that the `vhead_file` argument is loaded without the secure parameter `weights_only=True`. Version 0.9.4 contains a fix for the issue.		
CVE-2025-52995	File Browser vulnerable to command execution allowlist bypass	File Browser provides a file managing interface within a specified directory and it can be used to upload, delete, preview, rename and edit files. Prior to version 2.33.10, the implementation of the allowlist is erroneous, allowing a user to execute more shell commands than they are authorized for. The concrete impact of this vulnerability depends on the commands configured, and the binaries installed on the server or in the container image. Due to the missing separation of scopes on the OS-level, this could give an attacker access to all files managed the application, including the File Browser database. This issue has been patched in version 2.33.10.	Y	N
CVE-2025-34067	Hikvision HikCentral (formerly "Integrated Security Management Platform") Remote Command Execution via applyCT Fastjson	An unauthenticated remote command execution vulnerability exists in the applyCT component of the Hikvision Integrated Security Management Platform due to the use of a vulnerable version of the Fastjson library. The endpoint /bic/ssoService/v1/applyCT deserializes untrusted user input, allowing an attacker to trigger Fastjson's auto-type feature to load arbitrary Java classes. By referencing a malicious class via an LDAP URL, an attacker can achieve remote code execution on the underlying system.	Y	N
CVE-2025-34074	Lucee Admin Interface Authenticated Remote Code Execution via Scheduled Job File Write	An authenticated remote code execution vulnerability exists in Lucee's administrative interface due to insecure design in the	Y	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		scheduled task functionality. An administrator with access to /lucee/admin/web.cfm can configure a scheduled job to retrieve a remote .cfm file from an attacker-controlled server, which is written to the Lucee webroot and executed with the privileges of the Lucee service account. Because Lucee does not enforce integrity checks, path restrictions, or execution controls for scheduled task fetches, this feature can be abused to achieve arbitrary code execution. This issue is distinct from CVE-2024-55354.		
CVE-2025-34086	Bolt CMS Authenticated Remote Code Execution via Profile Injection and File Rename	Bolt CMS versions 3.7.0 and earlier contain a chain of vulnerabilities that together allow an authenticated user to achieve remote code execution. A user with valid credentials can inject arbitrary PHP code into the displayname field of the user profile, which is rendered unsanitized in backend templates. The attacker can then list and rename cached session files via the /async/browse/cache/.sessions and /async/folder/rename endpoints. By renaming a .session file to a path under the publicly accessible /files/ directory with a .php extension, the attacker can turn the injected code into an executable web shell. Finally, the attacker triggers the payload via a crafted HTTP GET request to the rogue file. NOTE: The vendor announced that Bolt 3 reached end-of-life after 31 December 2021.	Y	N
CVE-2025-34087	Pi-Hole AdminLTE Whitelist (now 'Web Allowlist') Remote Command Execution	An authenticated command injection vulnerability exists in Pi-hole versions up to 3.3. When adding a domain to the allowlist via the web interface, the domain parameter is not properly sanitized, allowing an attacker to append OS commands to the domain string. These commands are executed on the underlying operating system with the privileges of the Pi-hole	Y	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		service user. This behavior was present in the legacy AdminLTE interface and has since been patched in later versions.		
CVE-2025-34088	Pandora FMS Authenticated Remote Code Execution via Ping Module	An authenticated remote code execution vulnerability exists in Pandora FMS version 7.0NG and earlier. The net_tools.php functionality allows authenticated users to execute arbitrary OS commands via the select_ips parameter when performing network tools operations, such as pinging. This occurs because user input is not properly sanitized before being passed to system commands, enabling command injection.	Y	N
CVE-2025-53547	Helm Chart Dependency Updating With Malicious Chart.yaml Content And Symlink Can Lead To Code Execution	Helm is a package manager for Charts for Kubernetes. Prior to 3.18.4, a specially crafted Chart.yaml file along with a specially linked Chart.lock file can lead to local code execution when dependencies are updated. Fields in a Chart.yaml file, that are carried over to a Chart.lock file when dependencies are updated and this file is written, can be crafted in a way that can cause execution if that same content were in a file that is executed (e.g., a bash.rc file or shell script). If the Chart.lock file is symlinked to one of these files updating dependencies will write the lock file content to the symlinked file. This can lead to unwanted execution. Helm warns of the symlinked file but did not stop execution due to symlinking. This issue has been resolved in Helm v3.18.4.	Y	N
CVE-2025-34077	WordPress Pie Register Plugin ≤ 3.7.1.4 Authentication Bypass RCE	An authentication bypass vulnerability exists in the WordPress Pie Register plugin ≤ 3.7.1.4 that allows unauthenticated attackers to impersonate arbitrary users by submitting a crafted POST request to the login endpoint. By setting social_site=true and manipulating the	Y	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		user_id_social_site parameter, an attacker can generate a valid WordPress session cookie for any user ID, including administrators. Once authenticated, the attacker may exploit plugin upload functionality to install a malicious plugin containing arbitrary PHP code, resulting in remote code execution on the underlying server.		
CVE-2025-34083	WordPress AIT CSV Import/Export Plugin ≤ 3.0.3 Unauthenticated RCE	An unrestricted file upload vulnerability exists in the WordPress AIT CSV Import/Export plugin ≤ 3.0.3. The plugin exposes an upload handler at upload-handler.php that allows arbitrary file upload via a multipart/form-data POST request. This endpoint does not enforce authentication or content-type validation, enabling attackers to upload malicious PHP code directly to the server. Although the upload may produce an error related to CSV parsing, the malicious file is still saved under wp-content/uploads/ and remains executable. Notably, the plugin does not need to be active for exploitation to succeed.	Y	N
CVE-2025-53890	pyLoad vulnerable to remote code execution through js2py onCaptchaResult	pyload is an open-source Download Manager written in pure Python. An unsafe JavaScript evaluation vulnerability in pyLoad's CAPTCHA processing code allows unauthenticated remote attackers to execute arbitrary code in the client browser and potentially the backend server. Exploitation requires no user interaction or authentication and can result in session hijacking, credential theft, and full system remote code execution. Commit 909e5c97885237530d1264cfceb5555870eb9546, the patch for the issue, is included in version 0.5.0b3.dev89.	Y	N
CVE-2025-53927	MaxKB sandbox bypass	MaxKB is an open-source AI assistant for enterprise. Prior to version 2.0.0, the sandbox design rules can be bypassed because MaxKB only restricts the execution permissions of files in a	Y	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		specific directory. Therefore, an attacker can use the `shutil.copy2` method in Python to copy the command they want to execute to the executable directory. This bypasses directory restrictions and reverse shell. Version 2.0.0 fixes the issue.		
CVE-2025-53928	MaxKB has RCE in MCP call	MaxKB is an open-source AI assistant for enterprise. Prior to versions 1.10.9-lts and 2.0.0, a Remote Command Execution vulnerability exists in the MCP call. Versions 1.10.9-lts and 2.0.0 fix the issue.	Y	N
CVE-2025-54068	Livewire vulnerable to remote command execution during property update hydration	Livewire is a full-stack framework for Laravel. In Livewire v3 up to and including v3.6.3, a vulnerability allows unauthenticated attackers to achieve remote command execution in specific scenarios. The issue stems from how certain component property updates are hydrated. This vulnerability is unique to Livewire v3 and does not affect prior major versions. Exploitation requires a component to be mounted and configured in a particular way, but does not require authentication or user interaction. This issue has been patched in Livewire v3.6.4. All users are strongly encouraged to upgrade to this version or later as soon as possible. No known workarounds are available.	Y	N
CVE-2025-53770	Microsoft SharePoint Server Remote Code Execution Vulnerability	Deserialization of untrusted data in on-premises Microsoft SharePoint Server allows an unauthorized attacker to execute code over a network. Microsoft is aware that an exploit for CVE-2025-53770 exists in the wild. Microsoft is preparing and fully testing a comprehensive update to address this vulnerability. In the meantime, please make sure that the mitigation provided in this CVE documentation is in place so that you are protected from exploitation.	Y	N
CVE-2025-6213	Nginx Cache Purge Preload <= 2.1.1 -	The Nginx Cache Purge Preload plugin for	Y	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Authenticated (Administrator+) Remote Code Execution	WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 2.1.1 via the 'nppp_preload_cache_on_update' function. This is due to insufficient sanitization of the $_SERVER['HTTP_REFERERER'] parameter passed from the 'nppp_handle_fastcgi_cache_actions_admin_bar' function. This makes it possible for authenticated attackers, with Administrator-level access and above, to execute code on the server.		
CVE-2025-54377	Roo Code Lacks Line Break Validation in its Command Execution Tool	Roo Code is an AI-powered autonomous coding agent that lives in users' editors. In versions 3.23.18 and below, RooCode does not validate line breaks (\n) in its command input, allowing potential bypass of the allow-list mechanism. The project appears to lack parsing or validation logic to prevent multi-line command injection. When commands are evaluated for execution, only the first line or token may be considered, enabling attackers to smuggle additional commands in subsequent lines. This is fixed in version 3.23.19.	Y	N

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-52902	File Browser has Stored Cross-Site Scripting vulnerability	File Browser provides a file managing interface within a specified directory and it can be used to upload, delete, preview, rename and edit files. The Markdown preview function of File Browser prior to v2.33.7 is vulnerable to Stored Cross-Site-Scripting (XSS). Any JavaScript code that is part of a Markdown file uploaded by a user will be executed by the browser. Version 2.33.7 contains a fix for the issue.	Patched by core rule	Y
CVE-2025-53121	Stored XSS in multiple 33.0.8files in opennms/opennms	Multiple stored XSS were found on different nodes with unsanitized parameters in OpenMNS Horizon 33.0.8 and versions earlier than 33.1.6 on multiple platforms that allow an attacker to store on database and then inject HTML and/or Javascript on the page. The solution is to upgrade to Horizon 33.1.6, 33.1.7 or Meridian 2024.2.6, 2024.2.7 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet. OpenNMS thanks Fábio Tomé for reporting this issue.	Patched by core rule	Y
CVE-2025-53122	SQLi in OpenNMS Horizon and Meridian	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in OpenNMS Horizon and Meridian applications allows SQL Injection. Users should upgrade to Meridian 2024.2.6 or newer, or Horizon 33.16 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet.	Patched by core rule	Y
CVE-2025-6694	LabRedesCefetRJ WeGIA Adicionar Unidade adicionar_unidade.php cross site scripting	A vulnerability has been found in LabRedesCefetRJ WeGIA 3.4.0 and classified as problematic. This vulnerability affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown code of the file /html/matPat/adicionar_unidade.php of the component Adicionar Unidade. The manipulation of the argument Insira a nova unidade 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.		
CVE-2025-6695	LabRedesCefetRJ WeGIA Additional Categoria adicionar_categoria.php cross site scripting	A vulnerability was found in LabRedesCefetRJ WeGIA 3.4.0 and classified as problematic. This issue affects some unknown processing of the file /html/matPat/adicionar_categoria.php of the component Additional Categoria. The manipulation of the argument Insira a nova categoria 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-2025-6696	LabRedesCefetRJ WeGIA Cadastro de Atendio Cadastro_Atendido.php cross site scripting	A vulnerability was found in LabRedesCefetRJ WeGIA 3.4.0. It has been classified as problematic. Affected is an unknown function of the file /html/atendido/Cadastro_Atendido.php of the component Cadastro de Atendio. The manipulation of the argument Nome/Sobrenome 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 is a different issue than CVE-2025-22615. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-6697	LabRedesCefetRJ WeGIA Adicionar tipo adicionar_tipoEntrada.php cross site scripting	A vulnerability was found in LabRedesCefetRJ WeGIA 3.4.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /html/matPat/adicionar_tipoEntrada.php of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component Adicionar tipo. The manipulation of the argument Insira o novo tipo 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.		
CVE-2025-6698	LabRedesCefetRJ WeGIA Adicionar tipo adicionar_tipoSaida.php cross site scripting	A vulnerability was found in LabRedesCefetRJ WeGIA 3.4.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /html/matPat/adicionar_tipoSaida.php of the component Adicionar tipo. The manipulation of the argument Insira o novo tipo 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-2025-6699	LabRedesCefetRJ WeGIA Cadastro de Funcionário cadastro_funcionario.php cross site scripting	A vulnerability classified as problematic has been found in LabRedesCefetRJ WeGIA 3.4.0. This affects an unknown part of the file /html/funcionario/cadastro_funcionario.php of the component Cadastro de Funcionário. The manipulation of the argument Nome/Sobrenome 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 is a different issue than CVE-2025-23030. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-6700	Xuxueli xxl-sso login cross site scripting	A vulnerability classified as problematic was found in Xuxueli xxl-sso 1.1.0. This vulnerability affects unknown code of the file /xxl-sso-server/login. The manipulation of the argument errorMsg 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		not respond in any way.		
CVE-2025-53093	TabberNeue vulnerable to Stored XSS through wikitext	TabberNeue is a MediaWiki extension that allows the wiki to create tabs. Starting in version 3.0.0 and prior to version 3.1.1, any user can insert arbitrary HTMLinto the DOM by inserting a payload into any allowed attribute of the `<tabber>` tag. Version 3.1.1 contains a patch for the bug.	Patched by core rule	Y
CVE-2025-6778	code-projects Food Distributor Site save_settings.php cross site scripting	A vulnerability, which was classified as problematic, was found in code-projects Food Distributor Site 1.0. Affected is an unknown function of the file /admin/save_settings.php. The manipulation of the argument site_phone/site_email/address 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.	Patched by core rule	Y
CVE-2025-6849	code-projects Simple Forum forum_edit1.php cross site scripting	A vulnerability, which was classified as problematic, was found in code-projects Simple Forum 1.0. Affected is an unknown function of the file /forum_edit1.php. The manipulation of the argument text 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.	Patched by core rule	Y
CVE-2025-52896	Frappe authenticated XSS via data import	Frappe is a full-stack web application framework. Prior to versions 14.94.2 and 15.57.0, authenticated users could upload carefully crafted malicious files via Data Import, leading to cross-site scripting (XSS). This issue has been patched in versions 14.94.2 and 15.57.0. There are no workarounds for this issue other than upgrading.	Patched by core rule	Y
CVE-2025-52559	Zulip XSS in digest preview URL	Zulip is an open-source team chat application. From versions 2.0.0-rc1 to before 10.4 in Zulip Server, the /digest/ URL of a server shows a preview of what the email weekly digest would contain. This URL, though not the digest itself, contains a cross-site scripting (XSS)	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability in both topic names and channel names. This issue has been fixed in Zulip Server 10.4. A workaround for this issue involves denying access to /digest/.		
CVE-2025-52842	Laundry 2.3.0 - Account Takeover via Reflected XSS	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Laundry on Linux, MacOS allows Account Takeover. This issue affects Laundry: 2.3.0.	Patched by core rule	Y
CVE-2024-5647	Multiple Plugins <= (Various Versions) - Authenticated (Contributor+) Stored DOM-Based Cross-Site Scripting via Magnific Popups JavaScript Library	Multiple plugins for WordPress are vulnerable to Stored Cross-Site Scripting via the plugin's bundled Magnific Popups library (version 1.1.0) in various versions due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. NOTE: This vulnerability was fixed in the upstream library (Magnific Popups version 1.2.0) by disabling the loading of HTML within certain fields by default.	Patched by core rule	Y
CVE-2025-53368	Citizen is vulnerable to stored XSS attack in the legacy search bar	Citizen is a MediaWiki skin that makes extensions part of the cohesive experience. From versions 1.9.4 to before 3.4.0, page descriptions are inserted into raw HTML without proper sanitization by the Citizen skin when using the old search bar. Any user with page editing privileges can insert cross-site scripting (XSS) payloads into the DOM for other users who are searching for specific pages. This issue has been patched in version 3.4.0.	Patched by core rule	Y
CVE-2025-53369	Citizen Short Description stored XSS vulnerability through wikitext	Short Description is a MediaWiki extension that provides local short description support. In version 4.0.0, short descriptions are not properly sanitized before being inserted as HTML using mw.util.addSubtitle, allowing any user to insert	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		arbitrary HTML into the DOM by editing a page. This issue has been patched in version 4.0.1.		
CVE-2025-53370	Citizen stored XSS vulnerability through short descriptions	Citizen is a MediaWiki skin that makes extensions part of the cohesive experience. From versions 1.9.4 to before 3.4.0, short descriptions set via the ShortDescription extension are inserted as raw HTML by the Citizen skin, allowing any user to insert arbitrary HTML into the DOM by editing a page. This issue has been patched in version 3.4.0.	Patched by core rule	Y
CVE-2025-5944	Element Pack Addons for Elementor <= 8.0.0 - Authenticated (Contributor+) DOM-Based Stored Cross-Site Scripting via data-caption Attribute	The Element Pack Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'data-caption' attribute in all versions up to, and including, 8.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-7053	Cockpit save cross site scripting	A vulnerability was found in Cockpit up to 2.11.3. It has been rated as problematic. This issue affects some unknown processing of the file /system/users/save. The manipulation of the argument name/email leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 2.11.4 is able to address this issue. The patch is named bdcd5e3bc651c0839c7eea807f3eb6af856dbc76. It is recommended to upgrade the affected component. The vendor was contacted early about this disclosure and acted very professional. A patch and new release was made available very quickly.	Patched by core rule	Y
CVE-2025-7066	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in Jirafeau	Jirafeau normally prevents browser preview for text files due to the possibility that for example SVG and HTML documents could be exploited for cross site scripting. This was done by storing the MIME type of a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file and allowing only browser preview for MIME types beginning with image (except for image/svg+xml, see CVE-2022-30110 and CVE-2024-12326), video and audio. However, it was possible to bypass this check by sending a manipulated MIME type containing a comma and an other MIME type like text/html (for example image/png,text/html). Browsers see multiple MIME types and text/html would takes precedence, allowing a possible attacker to do a cross-site scripting attack. The check for MIME types was enhanced to prevent a browser preview when the stored MIME type contains a comma.		
CVE-2025-3467	XSS Vulnerability in langgenius/dify	An XSS vulnerability exists in langgenius/dify versions prior to 1.1.3, specifically affecting Firefox browsers. This vulnerability allows an attacker to obtain the administrator's token by sending a payload in the published chat. When the administrator views the conversation content through the monitoring/log function using Firefox, the XSS vulnerability is triggered, potentially exposing sensitive token information to the attacker.	Patched by core rule	Y
CVE-2025-4779	Stored Cross-site Scripting (XSS) in lunary-ai/lunary	lunary-ai/lunary versions prior to 1.9.24 are vulnerable to stored cross-site scripting (XSS). An unauthenticated attacker can inject malicious JavaScript into the `v1/runs/ingest` endpoint by adding an empty `citations` field, triggering a code path where `dangerouslySetInnerHTML` is used to render attacker-controlled text. This vulnerability allows the execution of arbitrary JavaScript in the context of the user's browser, potentially leading to session hijacking, data theft, or other malicious actions.	Patched by core rule	Y
CVE-2025-53376	Dokploy allows attackers to run arbitrary OS commands on the Dokploy host.	Dokploy is a self-hostable Platform as a Service (PaaS) that simplifies the deployment and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		management of applications and databases. An authenticated, low-privileged user can run arbitrary OS commands on the Dokploy host. The tRPC procedure docker.getContainersByAppNameMatch interpolates the attacker-supplied appName value into a Docker CLI call without sanitisation, enabling command injection under the Dokploy service account. This vulnerability is fixed in 0.23.7.		
CVE-2025-53377	WebGia allows Cross-Site Scripting (XSS) in cadastro_dependente_pessoa_nova.php via the id_funcionario parameter	WeGIA is a web manager for charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the cadastro_dependente_pessoa_nova.php endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the id_funcionario parameter. This vulnerability is fixed in 3.4.3.	Patched by core rule	Y
CVE-2025-53525	WebGia allows Cross-Site Scripting (XSS) in profile_familiar.php via the id_dependente parameter	WeGIA is a web manager for charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the profile_familiar.php endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the id_dependente parameter. This vulnerability is fixed in 3.4.3.	Patched by core rule	Y
CVE-2025-53526	WeGIA allows Stored XSS attacks in novo_memorando.php	WeGIA is a web manager for charitable institutions. An XSS Injection vulnerability was identified in novo_memorando.php. After the memo was submitted, the vulnerability was confirmed by accessing listar_memorandos_antigos.php. Upon loading this page, the injected script was executed in the browser. This vulnerability is fixed in 3.4.3.	Patched by core rule	Y
CVE-2025-53527	WeGIA allows Time-Based Blind SQL Injection in the relatorio_geracao.php endpoint	WeGIA is a web manager for charitable institutions. A Time-Based Blind SQL Injection vulnerability was discovered in the almox parameter of the /controle/relatorio_geracao.php endpoint. This issue allows attacker to inject	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		arbitrary SQL queries, potentially leading to unauthorized data access or further exploitation depending on database configuration. This vulnerability is fixed in 3.4.1.		
CVE-2025-53529	WeGIA allows SQL Injection in html/funcionario/profile_funcionario.php (id_funcionario parameter)	WeGIA is a web manager for charitable institutions. An SQL Injection vulnerability was identified in the /html/funcionario/profile_funcionario.php endpoint. The id_funcionario parameter is not properly sanitized or validated before being used in a SQL query, allowing an unauthenticated attacker to inject arbitrary SQL commands. The vulnerability is fixed in 3.4.3.	Patched by core rule	Y
CVE-2025-53543	Kestra allows Stored XSS before 0.22	Kestra is an event-driven orchestration platform. The error message in execution "Overview" tab is vulnerable to stored XSS due to improper handling of HTTP response received. This vulnerability is fixed in 0.22.0.	Patched by core rule	Y
CVE-2025-7109	Portabilis i-Educar Student Benefits Registration educar_aluno_beneficio_lst.php cross site scripting	A vulnerability, which was classified as problematic, has been found in Portabilis i-Educar 2.9.0. Affected by this issue is some unknown functionality of the file /intranet/educar_aluno_beneficio_lst.php of the component Student Benefits Registration. The manipulation of the argument Benefício 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-2025-7110	Portabilis i-Educar School Module educar_escola_lst.php cross site scripting	A vulnerability, which was classified as problematic, was found in Portabilis i-Educar 2.9.0. This affects an unknown part of the file /intranet/educar_escola_lst.php of the component School Module. The manipulation of the argument Escola 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-7111	Portabilis i-Educar Course Module educar_curso_det.php cross site scripting	A vulnerability has been found in Portabilis i-Educar 2.9.0 and classified as problematic. This vulnerability affects unknown code of the file /intranet/educar_curso_det.php?cod_curso=ID of the component Course Module. The manipulation of the argument Curso 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-2025-7112	Portabilis i-Educar Function Management Module educar_funcao_det.php cross site scripting	A vulnerability was found in Portabilis i-Educar 2.9.0 and classified as problematic. This issue affects some unknown processing of the file /intranet/educar_funcao_det.php?cod_funcao=COD&ref_cod_instituicao=COD of the component Function Management Module. The manipulation of the argument Função 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-2025-7113	Portabilis i-Educar Curricular Components Module edit cross site scripting	A vulnerability was found in Portabilis i-Educar 2.9.0. It has been classified as problematic. Affected is an unknown function of the file /module/ComponenteCurricular/edit?id=ID of the component Curricular Components Module. The manipulation of the argument Nome 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-2025-7139	SourceCodester Best Salon Management System Update Customer	A vulnerability was found in SourceCodester Best Salon Management System 1.0. It	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Details Page edit-customer-detailed.php cross site scripting	has been rated as problematic. This issue affects some unknown processing of the file /panel/edit-customer-detailed.php of the component Update Customer Details Page. The manipulation of the argument Name leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-7140	SourceCodester Best Salon Management System Update Staff Page edit-staff.php cross site scripting	A vulnerability classified as problematic has been found in SourceCodester Best Salon Management System 1.0. Affected is an unknown function of the file /panel/edit-staff.php of the component Update Staff Page. The manipulation of the argument Staff Name 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.	Patched by core rule	Y
CVE-2025-7141	SourceCodester Best Salon Management System Update Staff Page edit_plan.php cross site scripting	A vulnerability classified as problematic was found in SourceCodester Best Salon Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /panel/edit_plan.php of the component Update Staff Page. 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-2025-7142	SourceCodester Best Salon Management System search-appointment.php cross site scripting	A vulnerability, which was classified as problematic, has been found in SourceCodester Best Salon Management System 1.0. Affected by this issue is some unknown functionality of the file /panel/search-appointment.php. 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-2025-7143	SourceCodester Best Salon Management System Update Tax Page edit-tax.php cross site scripting	A vulnerability, which was classified as problematic, was found in SourceCodester Best Salon Management System 1.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This affects an unknown part of the file /panel/edit-tax.php of the component Update Tax Page. The manipulation of the argument Tax Name 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-2025-7144	SourceCodester Best Salon Management System Admin Profile Page admin-profile.php cross site scripting	A vulnerability has been found in SourceCodester Best Salon Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /panel/admin-profile.php of the component Admin Profile Page. The manipulation of the argument Admin 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-2025-7148	CodeAstro Simple Hospital Management System POST Parameter patient.html cross site scripting	A vulnerability was found in CodeAstro Simple Hospital Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /patient.html of the component POST Parameter 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. Multiple parameters might be affected.	Patched by core rule	Y
CVE-2025-7153	CodeAstro Simple Hospital Management System POST Parameter doctor.html cross site scripting	A vulnerability classified as problematic was found in CodeAstro Simple Hospital Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /doctor.html of the component POST Parameter Handler. The manipulation of the argument First Name/Last name/Address 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-2025-7182	itsourcecode Student Transcript Processing System edit.php cross site scripting	A vulnerability has been found in itsourcecode Student Transcript Processing System 1.0 and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		classified as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/modules/subject/edit.php. The manipulation of the argument pre leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6948	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 17.11 before 17.11.6, 18.0 before 18.0.4, and 18.1 before 18.1.2 that, under certain conditions, could have allowed a successful attacker to execute actions on behalf of users by injecting malicious content.	Patched by core rule	Y
CVE-2025-7408	SourceCodester Zoo Management System animal_form_template.php cross site scripting	A vulnerability has been found in SourceCodester Zoo Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/templates/animal_form_template.php. The manipulation of the argument msg 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-2025-7435	LiveHelperChat lhc-php-resque Extension List list cross site scripting	A vulnerability was found in LiveHelperChat lhc-php-resque Extension up to ee1270b35625f552425e32a6a3061cd54b5085c4. It has been classified as problematic. This affects an unknown part of the file /site_admin/lhcphpresque/list/ of the component List Handler. The manipulation of the argument queue name 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 takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The identifier of the patch is 542aa8449b5aa889b3a54f419e794afe19f56d5d/0ce7b4f1193c0ed6c6e31a960fafed	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		edf979eef2. It is recommended to apply a patch to fix this issue.		
CVE-2025-53820	WeGIA vulnerable to Cross-Site Scripting (XSS) Reflected via endpoint 'index.php' parameter 'erro'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the `index.php` endpoint of the WeGIA application prior to version 3.4.5. This vulnerability allows attackers to inject malicious scripts in the `erro` parameter. Version 3.4.5 contains a patch for the issue.	Patched by core rule	Y
CVE-2025-53822	WeGIA vulnerable to Reflected Cross-Site Scripting in endpoint 'relatorio_geracao.php' parameter 'tipo_relatorio'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the `relatorio_geracao.php` endpoint of the WeGIA application prior to version 3.4.5. This vulnerability allows attackers to inject malicious scripts in the `tipo_relatorio` parameter. Version 3.4.5 has a patch for the issue.	Patched by core rule	Y
CVE-2025-53823	WeGIA vulnerable to SQL Injection (Blind Time-Based) in `processa_deletar_socio.php` parameter `id_socio`	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. Versions prior to 3.4.5 have a SQL Injection vulnerability in the endpoint `/WeGIA/html/socio/sistema/processa_deletar_socio.php`, in the `id_socio` parameter. This vulnerability allows the execution of arbitrary SQL commands, which can compromise the confidentiality, integrity, and availability of stored data. Version 3.4.5 fixes the issue.	Patched by core rule	Y
CVE-2025-53824	WeGIA ReflectedCross-Site Scripting (XSS) vulnerability in endpoint 'cadastro_pet.php' parameter 'msg'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the editar_permissoes.php endpoint of the WeGIA application prior to version 3.4.4. This vulnerability allows attackers to inject malicious scripts in the msg_c parameter. Version		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		3.4.4 fixes the issue.		
CVE-2025-53834	Caido Toast Vulnerable to Reflected Cross-site Scripting	Caido is a web security auditing toolkit. A reflected cross-site scripting (XSS) vulnerability was discovered in Caido's toast UI component in versions prior to 0.49.0. Toast messages may reflect unsanitized user input in certain tools such as Match&Replace and Scope. This could allow an attacker to craft input that results in arbitrary script execution. Version 0.49.0 fixes the issue.	Patched by core rule	Y
CVE-2025-53835	XWiki Rendering is vulnerable to XSS attacks through insecure XHTML syntax	XWiki Rendering is a generic rendering system that converts textual input in a given syntax (wiki syntax, HTML, etc) into another syntax (XHTML, etc). Starting in version 5.4.5 and prior to version 14.10, the XHTML syntax depended on the `xdom+xml/current` syntax which allows the creation of raw blocks that permit the insertion of arbitrary HTML content including JavaScript. This allows XSS attacks for users who can edit a document like their user profile (enabled by default). This has been fixed in version 14.10 by removing the dependency on the `xdom+xml/current` syntax from the XHTML syntax. Note that the `xdom+xml` syntax is still vulnerable to this attack. As it's main purpose is testing and its use is quite difficult, this syntax shouldn't be installed or used on a regular wiki. There are no known workarounds apart from upgrading.	Patched by core rule	Y
CVE-2025-53836	XWiki Rendering is vulnerable to RCE attacks when processing nested macros	XWiki Rendering is a generic rendering system that converts textual input in a given syntax (wiki syntax, HTML, etc) into another syntax (XHTML, etc). Starting in version 4.2-milestone-1 and prior to versions 13.10.11, 14.4.7, and 14.10, the default macro content parser doesn't preserve the restricted attribute of the transformation context when executing nested macros. This allows executing macros that are normally forbidden in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		restricted mode, in particular script macros. The cache and chart macros that are bundled in XWiki use the vulnerable feature. This has been patched in XWiki 13.10.11, 14.4.7 and 14.10. To avoid the exploitation of this bug, comments can be disabled for untrusted users until an upgrade to a patched version has been performed. Note that users with edit rights will still be able to add comments via the object editor even if comments have been disabled.		
CVE-2025-53839	DRACOON Branding Service vulnerable to Cross-site Scripting	DRACOON is a file sharing service, and the DRACOON Branding Service allows customers to customize their DRACOON interface with their brand. Versions of the DRACOON Branding Service prior to 2.10.0 are vulnerable to cross-site scripting. Improper neutralization of input from administrative users could inject HTML code into the workflow for newly onboarded users. A fix was made available in version 2.10.0 and rolled out to the DRACOON service. DRACOON customers do not need to take action.	Patched by core rule	Y
CVE-2025-7567	ShopXO header.html cross site scripting	A vulnerability was found in ShopXO up to 6.5.0 and classified as problematic. This issue affects some unknown processing of the file header.html. The manipulation of the argument lang/system_type 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-2025-7569	Bigotry OneBase think_exception.tpl parse_args cross site scripting	A vulnerability was found in Bigotry OneBase up to 1.3.6. It has been declared as problematic. Affected by this vulnerability is the function parse_args of the file /tpl/think_exception.tpl. The manipulation of the argument args 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		but did not respond in any way.		
CVE-2025-7601	PHPGurukul Online Library Management System student-history.php cross site scripting	A vulnerability has been found in PHPGurukul Online Library Management System 3.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/student-history.php. The manipulation of the argument stdid 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-2025-53903	The Scratch Channel Has Potential Cross-Site Scripting (XSS) Vulnerability	The Scratch Channel is a news website that is under development as of time of this writing. The file `/api/users.js` doesn't properly sanitize text box inputs, leading to a potential vulnerability to cross-site scripting attacks. Commit 90b39eb56b27b2bac29001abb1a3cac0964b8ddb addresses this issue.	Patched by core rule	Y
CVE-2025-53892	Intlify Vue I18n's escapeParameterHtml does not prevent DOM-based XSS via tag attributes like onerror	Vue I18n is the internationalization plugin for Vue.js. The escapeParameterHtml: true option in Vue I18n is designed to protect against HTML/script injection by escaping interpolated parameters. However, starting in version 9.0.0 and prior to versions 9.14.5, 10.0.8, and 11.1.0, this setting fails to prevent execution of certain tag-based payloads, such as <img src=x onerror=...>, if the interpolated value is inserted inside an HTML context using v-html. This may lead to a DOM-based XSS vulnerability, even when using escapeParameterHtml: true, if a translation string includes minor HTML and is rendered via v-html. Versions 9.14.5, 10.0.8, and 11.1.0 contain a fix for the issue.	Patched by core rule	Y
CVE-2025-53904	The Scratch Channel Has Potential Reflected Cross-Site Scripting (XSS) Vulnerability	The Scratch Channel is a news website that is under development as of time of this writing. The file `/api/admin.js` contains code that could make the website vulnerable to cross-site scripting. No known	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		patches exist as of time of publication.		
CVE-2025-53923	Emlog vulnerable to reflected Cross-site Scripting in admin panel	Emlog is an open source website building system. A cross-site scripting (XSS) vulnerability in emlog up to and including pro-2.5.17 allows remote attackers to inject arbitrary web script or HTML via the keyword parameter. Due to lack of sanitization it is possible to inject HTML/JS code into keyword parameter. If one persuades an user into clicking into prepared link it is possible to execute any JS code in admin's browser. As of time of publication, no known patched versions exist.	Patched by core rule	Y
CVE-2025-53924	Emlog vulnerable to stored Cross-site Scripting in links functionality	Emlog is an open source website building system. A cross-site scripting (XSS) vulnerability in emlog up to and including pro-2.5.17 allows authenticated remote attackers to inject arbitrary web script or HTML via the siteurl parameter. It is possible to inject malicious code into siteurl parameter resulting in Stored XSS. When someone clicks on the link the malicious code is executed. As of time of publication, no known patched versions exist.	Patched by core rule	Y
CVE-2025-53925	Emlog has Stored Cross-site Scripting vulnerability in file upload functionality	Emlog is an open source website building system. A cross-site scripting (XSS) vulnerability in emlog up to and including pro-2.5.17 allows authenticated remote attackers to inject arbitrary web script or HTML via the file upload functionality. As an authenticated user it is possible to upload an .svg file that contains JavaScript code that is later executed. As of time of publication, no known patched versions exist.	Patched by core rule	Y
CVE-2025-53926	Emlog has Stored Cross-site Scripting vulnerability due to error	Emlog is an open source website building system. A cross-site scripting (XSS) vulnerability in emlog up to and including pro-2.5.17 allows remote attackers to inject arbitrary web script or HTML via the comment and comname parameters. Reflected XSS requires the victim to send POST	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		requests, therefore the victim must be persuaded into clicking into sent URL. As of time of publication, no known patched versions exist.		
CVE-2025-53929	WeGIA vulnerable to Stored Cross-Site Scripting (XSS) via endpoint `adicionar_cor.php` parameter `cor`	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the `adicionar_cor.php` endpoint of the WeGIA application prior to version 3.4.5. This vulnerability allows attackers to inject malicious scripts into the `cor` parameter. The injected scripts are stored on the server and executed automatically whenever the affected page `cadastro_pet.php` is accessed by users, posing a significant security risk. Version 3.4.5 fixes the issue.	Patched by core rule	Y
CVE-2025-53930	WeGIA vulnerable to Stored Cross-Site Scripting (XSS) via endpoint 'adicionar_especie.php' parameter 'especie'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the `adicionar_especie.php` endpoint of the WeGIA application prior to version 3.4.5. This vulnerability allows attackers to inject malicious scripts into the `especie` parameter. The injected scripts are stored on the server and executed automatically whenever the affected page is accessed by users, posing a significant security risk. Version 3.4.5 fixes the issue.	Patched by core rule	Y
CVE-2025-53931	WeGIA vulnerable to Stored Cross-Site Scripting via endpoint `adicionar_raca.php` parameter `raca`	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the `adicionar_raca.php` endpoint of the WeGIA application prior to version 3.4.5. This vulnerability allows attackers to inject malicious scripts into the `raca` parameter. The injected scripts are stored on the server and executed automatically whenever the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affected page is accessed by users, posing a significant security risk. Version 3.4.5 fixes the issue.		
CVE-2025-53932	WeGIA vulnerable to Reflected Cross-Site Scripting via endpoint 'cadastro_adotante.php' parameter 'cpf'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the `cadastro_adotante.php` endpoint of the WeGIA application prior to version 3.4.5. This vulnerability allows attackers to inject malicious scripts in the `cpf` parameter. Version 3.4.5 fixes the issue.	Patched by core rule	Y
CVE-2025-53933	WeGIA vulnerable to Stored Cross-Site Scripting via endpoint 'adicionar_enfermidade.php' parameter 'nome'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the `adicionar_enfermidade.php` endpoint of the WeGIA application prior to version 3.4.5. This vulnerability allows attackers to inject malicious scripts into the `nome` parameter. The injected scripts are stored on the server and executed automatically whenever the affected page is accessed by users, posing a significant security risk. Version 3.4.5 fixes the issue.	Patched by core rule	Y
CVE-2025-53934	WeGIA vulnerable to Stored Cross-Site Scripting via endpoint 'control.php' parameter 'descricao_emergencia'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the `control.php` endpoint of the WeGIA application prior to version 3.4.5. This vulnerability allows attackers to inject malicious scripts into the `descricao_emergencia` parameter. The injected scripts are stored on the server and executed automatically whenever the affected page is accessed by users, posing a significant security risk. Version 3.4.5 fixes the issue.	Patched by core rule	Y
CVE-2025-53935	WeGIA vulnerable to Reflected Cross-Site Scripting via endpoint	WeGIA is an open source web manager with a focus on the Portuguese language	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	`personalizacao_selecao.php` parameter `id`	and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the `personalizacao_selecao.php` endpoint of the WeGIA application prior to version 3.4.5. This vulnerability allows attackers to inject malicious scripts in the `id` parameter. Version 3.4.5 fixes the issue.		
CVE-2025-53936	WeGIA vulnerable to Reflected Cross-Site Scripting via endpoint `personalizacao_selecao.php` parameter `nome_car`	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the `personalizacao_selecao.php` endpoint of the WeGIA application prior to version 3.4.5. This vulnerability allows attackers to inject malicious scripts in the `nome_car` parameter. Version 3.4.5 fixes the issue.	Patched by core rule	Y
CVE-2025-7728	Scada-LTS users.shtm cross site scripting	A vulnerability classified as problematic has been found in Scada-LTS up to 2.7.8.1. Affected is an unknown function of the file users.shtm. The manipulation of the argument Username 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 issue and confirmed that it will be fixed in the upcoming release 2.8.0.	Patched by core rule	Y
CVE-2025-7729	Scada-LTS usersProfiles.shtm cross site scripting	A vulnerability classified as problematic was found in Scada-LTS up to 2.7.8.1. Affected by this vulnerability is an unknown functionality of the file usersProfiles.shtm. The manipulation of the argument Username 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 issue and confirmed that it will be fixed in the upcoming release 2.8.0.	Patched by core rule	Y
CVE-2025-7748	ZCMS Create Article Page	A vulnerability classified as	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	cross site scripting	problematic was found in ZCMS 3.6.0. This vulnerability affects unknown code of the component Create Article Page. The manipulation of the argument Title leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	rule	
CVE-2025-54075	mdc vulnerable to XSS in markdown rendering bypassing HTML filter. (N°4)	MDC is a tool to take regular Markdown and write documents interacting deeply with a Vue component. Prior to version 0.17.2, a remote script-inclusion / stored cross-site scripting vulnerability in @nuxtjs/mdc lets a Markdown author inject a `<base href="https://attacker.tld">` element. The `<base>` tag rewrites how all subsequent relative URLs are resolved, so an attacker can make the page load scripts, styles, or images from an external, attacker-controlled origin and execute arbitrary JavaScript in the site's context. Version 0.17.2 contains a fix for the issue.	Patched by core rule	Y
CVE-2025-54076	WeGIA Reflected Cross-Site Scripting (XSS) vulnerability in endpoint 'pre_cadastro_atendido.php' parameter 'msg_e'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in versions prior to 3.4.6 in the `pre_cadastro_atendido.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the `msg_e` parameter. Version 3.4.6 fixes the issue.	Patched by core rule	Y
CVE-2025-54077	WeGIA Reflected Cross-Site Scripting (XSS) vulnerability in endpoint 'personalizacao.php' parameter 'err'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in versions prior to 3.4.6 in the `personalizacao.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the `err` parameter. Version 3.4.6 fixes the issue.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-54078	WeGIA Reflected Cross-Site Scripting (XSS) vulnerability in endpoint 'personalizacao_imagem.php' parameter 'err'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in versions prior to 3.4.6 in the `personalizacao_imagem.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the `err` parameter. Version 3.4.6 fixes the issue.	Patched by core rule	Y
CVE-2025-54079	WeGIA vulnerable to SQL Injection (Blind Time-Based) in endpoint 'Profile_Atendido.php' parameter 'idatendido'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A SQL Injection vulnerability was identified in versions prior to 3.4.6 in the endpoint `/html/atendido/Profile_Atendido.php`, in the `idatendido` parameter. This vulnerability allow an authorized attacker to execute arbitrary SQL queries, allowing access to sensitive information. Version 3.4.6 fixes the issue.	Patched by core rule	Y
CVE-2025-7767	PHPGurukul Art Gallery Management System edit-art-medium-detail.php cross site scripting	A vulnerability, which was classified as problematic, has been found in PHPGurukul Art Gallery Management System 1.1. Affected by this issue is some unknown functionality of the file /admin/edit-art-medium-detail.php. The manipulation of the argument artmed 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-2025-7786	Gnuboard g6 Post Reply qa cross site scripting	A vulnerability, which was classified as problematic, has been found in Gnuboard g6 up to 6.0.10. This issue affects some unknown processing of the file /bbs/scrap_popin_update/qa/ of the component Post Reply 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.	Patched by core rule	Y
CVE-2025-7791	PHPGurukul Online Security Guards Hiring System search.php cross site scripting	A vulnerability was found in PHPGurukul Online Security Guards Hiring System 1.0. It has been declared as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		problematic. This vulnerability affects unknown code of the file /admin/search.php. The manipulation of the argument searchdata leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-7802	PHPGurukul Complaint Management System complaint-search.php cross site scripting	A vulnerability was found in PHPGurukul Complaint Management System 2.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/complaint-search.php. The manipulation of the argument Search 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-2025-7815	PHPGurukul Apartment Visitors Management System HTTP POST Request manage-newvisitors.php cross site scripting	A vulnerability, which was classified as problematic, has been found in PHPGurukul Apartment Visitors Management System 1.0. This issue affects some unknown processing of the file /manage-newvisitors.php of the component HTTP POST Request Handler. The manipulation of the argument visname leads to cross site scripting. 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-2025-7816	PHPGurukul Apartment Visitors Management System HTTP POST Request visitor-detail.php cross site scripting	A vulnerability, which was classified as problematic, was found in PHPGurukul Apartment Visitors Management System 1.0. Affected is an unknown function of the file /visitor-detail.php of the component HTTP POST Request Handler. The manipulation of the argument visname 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.	Patched by core rule	Y
CVE-2025-7817	PHPGurukul Apartment Visitors Management	A vulnerability has been found in PHPGurukul	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System HTTP POST Request bwdates-reports.php cross site scripting	Apartment Visitors Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /bwdates-reports.php of the component HTTP POST Request Handler. The manipulation of the argument visname leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-7818	PHPGurukul Apartment Visitors Management System HTTP POST Request category.php cross site scripting	A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /category.php of the component HTTP POST Request Handler. The manipulation of the argument categoryname 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-2025-7819	PHPGurukul Apartment Visitors Management System HTTP POST Request create-pass.php cross site scripting	A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /create-pass.php of the component HTTP POST Request Handler. The manipulation of the argument visname leads to cross site scripting. It is possible to initiate the attack remotely.	Patched by core rule	Y
CVE-2025-7840	Campcodes Online Movie Theater Seat Reservation System Reserve Your Seat Page index.php cross site scripting	A vulnerability was found in Campcodes Online Movie Theater Seat Reservation System 1.0. It has been classified as problematic. This affects an unknown part of the file /index.php?page=reserve of the component Reserve Your Seat Page. The manipulation of the argument Firstname/Lastname 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-7856	PHPGurukul Apartment Visitors Management System HTTP POST Request pass-details.php cross site scripting	A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file pass-details.php of the component HTTP POST Request Handler. The manipulation of the argument visname 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-2025-7857	PHPGurukul Apartment Visitors Management System HTTP POST Request bwdates-passreports-details.php cross site scripting	A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file bwdates-passreports-details.php of the component HTTP POST Request Handler. The manipulation of the argument visname 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-2025-7858	PHPGurukul Apartment Visitors Management System HTTP POST Request admin-profile.php cross site scripting	A vulnerability classified as problematic has been found in PHPGurukul Apartment Visitors Management System 1.0. This affects an unknown part of the file /admin-profile.php of the component HTTP POST Request Handler. The manipulation of the argument adminname 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-2025-7865	thinkgem JeeSite XSS Filter EncodeUtils.java xssFilter cross site scripting	A vulnerability was found in thinkgem JeeSite up to 5.12.0. It has been declared as problematic. This vulnerability affects the function xssFilter of the file src/main/java/com/jeesite/common/codec/EncodeUtils.java of the component XSS Filter. The manipulation of the argument text leads to cross site scripting. The attack can be initiated remotely. The exploit has	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		been disclosed to the public and may be used. The patch is identified as 3585737d21fe490ff6948d913fcbd8d99c41fc08. It is recommended to apply a patch to fix this issue.		
CVE-2025-7866	Portabilis i-Educar Disabilities Module educar_deficiencia_lst.php cross site scripting	A vulnerability was found in Portabilis i-Educar 2.9.0. It has been rated as problematic. This issue affects some unknown processing of the file /intranet/educar_deficiencia_lst.php of the component Disabilities Module. The manipulation of the argument Deficiência ou Transtorno 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-2025-7867	Portabilis i-Educar Agenda Module agenda.php cross site scripting	A vulnerability classified as problematic has been found in Portabilis i-Educar 2.9.0. Affected is an unknown function of the file /intranet/agenda.php of the component Agenda Module. The manipulation of the argument novo_titulo 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-2025-7868	Portabilis i-Educar Calendar Module educar_calendario_dia_motivo_cad.php cross site scripting	A vulnerability classified as problematic was found in Portabilis i-Educar 2.9.0. Affected by this vulnerability is an unknown functionality of the file /intranet/educar_calendario_dia_motivo_cad.php of the component Calendar Module. The manipulation of the argument Motivo 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-2025-7869	Portabilis i-Educar Turma Module	A vulnerability, which was classified as problematic, has	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	educar_turma_tipo_det.php cross site scripting	been found in Portabilis i-Educar 2.9.0. Affected by this issue is some unknown functionality of the file intranet/educar_turma_tipo_det.php?cod_turma_tipo=ID of the component Turma Module. The manipulation of the argument nm_tipo 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-2025-7870	Portabilis i-Diario justificativas-de-falta Endpoint cross site scripting	A vulnerability, which was classified as problematic, was found in Portabilis i-Diario 1.5.0. This affects an unknown part of the component justificativas-de-falta Endpoint. The manipulation of the argument Anexo 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-2025-7871	Portabilis i-Diario conteudos cross site scripting	A vulnerability has been found in Portabilis i-Diario 1.5.0 and classified as problematic. This vulnerability affects unknown code of the file /conteudos. The manipulation of the argument filter[by_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-2025-7872	Portabilis i-Diario justificativas-de-falta cross site scripting	A vulnerability was found in Portabilis i-Diario 1.5.0 and classified as problematic. This issue affects some unknown processing of the file /justificativas-de-falta. The manipulation of the argument Justificativa 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		about this disclosure but did not respond in any way.		
CVE-2025-7885	Huashengdun WebSSH Login Page cross site scripting	A vulnerability, which was classified as problematic, has been found in Huashengdun WebSSH up to 1.6.2. Affected by this issue is some unknown functionality of the component Login Page. The manipulation of the argument hostname/port 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-2025-7887	Zavy86 WikiDocs template.inc.php cross site scripting	A vulnerability has been found in Zavy86 WikiDocs up to 1.0.78 and classified as problematic. This vulnerability affects unknown code of the file template.inc.php. The manipulation of the argument path 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-2025-7901	yangzongzhuan RuoYi Swagger UI index.html cross site scripting	A vulnerability was found in yangzongzhuan RuoYi up to 4.8.1. It has been rated as problematic. This issue affects some unknown processing of the file /swagger-ui/index.html of the component Swagger UI. The manipulation of the argument configUrl leads to cross site scripting. The attack may be initiated remotely.	Patched by core rule	Y
CVE-2025-7902	yangzongzhuan RuoYi SysNoticeController.java addSave cross site scripting	A vulnerability classified as problematic has been found in yangzongzhuan RuoYi up to 4.8.1. Affected is the function addSave of the file com/ruoyi/web/controller/system/SysNoticeController.java. The manipulation 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.	Patched by core rule	Y
CVE-2025-53528	Cadwyn is vulnerable to an XSS attack through its docs page	Cadwyn creates production-ready community-driven modern Stripe-like API versioning in FastAPI. In versions 5.4.3 and below, the version parameter of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		"/docs" endpoint is vulnerable to a Reflected XSS (Cross-Site Scripting) attack. This XSS would notably allow an attacker to execute JavaScript code on a user's session for any application based on Cadwyn via a one-click attack. The vulnerability has been fixed in version 5.4.4.		
CVE-2025-54128	HAX CMS NodeJs's Disabled Content Security Policy Enables Cross-Site Scripting	HAX CMS NodeJs allows users to manage their microsite universe with a NodeJs backend. In versions 11.0.7 and below, the NodeJS version of HAX CMS has a disabled Content Security Policy (CSP). This configuration is insecure for a production application because it does not protect against cross-site-scripting attacks. The contentSecurityPolicy value is explicitly disabled in the application's Helmet configuration in app.js. This is fixed in version 11.0.8.	Patched by core rule	Y
CVE-2025-7924	PHPGurukul Online Banquet Booking System admin-profile.php cross site scripting	A vulnerability classified as problematic was found in PHPGurukul Online Banquet Booking System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/admin-profile.php. The manipulation of the argument adminname 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-2025-7925	PHPGurukul Online Banquet Booking System login.php cross site scripting	A vulnerability, which was classified as problematic, has been found in PHPGurukul Online Banquet Booking System 1.0. Affected by this issue is some unknown functionality of the file /admin/login.php. The manipulation of the argument user_login/userpassword 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-2025-7926	PHPGurukul Online Banquet Booking System booking-search.php cross site scripting	A vulnerability, which was classified as problematic, was found in PHPGurukul Online Banquet Booking System 1.0. This affects an	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown part of the file /admin/booking-search.php. The manipulation of the argument searchdata 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-2025-7941	PHPGurukul Time Table Generator System profile.php cross site scripting	A vulnerability, which was classified as problematic, was found in PHPGurukul Time Table Generator System 1.0. Affected is an unknown function of the file /admin/profile.php. The manipulation of the argument adminname 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.	Patched by core rule	Y
CVE-2025-7942	PHPGurukul Taxi Stand Management System admin-profile.php cross site scripting	A vulnerability has been found in PHPGurukul Taxi Stand Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/admin-profile.php. The manipulation of the argument adminname 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-2025-7943	PHPGurukul Taxi Stand Management System search-autoortaxi.php cross site scripting	A vulnerability was found in PHPGurukul Taxi Stand Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/search-autoortaxi.php. The manipulation of the argument searchdata 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-2025-7944	PHPGurukul Taxi Stand Management System search.php cross site scripting	A vulnerability was found in PHPGurukul Taxi Stand Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /search.php. The manipulation of the argument searchdata leads to cross site scripting. It is possible to initiate the attack	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-2025-7946	PHPGurukul Apartment Visitors Management System HTTP POST Request search-visitor.php cross site scripting	A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /search-visitor.php of the component HTTP POST Request Handler. The manipulation of the argument searchdata 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-2025-7951	code-projects Public Chat Room send_message.php cross site scripting	A vulnerability classified as problematic has been found in code-projects Public Chat Room 1.0. This affects an unknown part of the file /send_message.php. The manipulation of the argument chat_msg/your_name 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-2025-32019	Harbor's repository description page allows for XSS	Harbor is an open source trusted cloud native registry project that stores, signs, and scans content. Versions 2.11.2 and below, as well as versions 2.12.0-rc1 and 2.13.0-rc1, contain a vulnerability where the markdown field in the info tab page can be exploited to inject XSS code. This is fixed in versions 2.11.3 and 2.12.3.	Patched by core rule	Y
CVE-2025-4439	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 15.10 before 18.0.5, 18.1 before 18.1.3, and 18.2 before 18.2.1 that could have allowed an authenticated user to perform cross-site scripting attacks when the instance is served through certain content delivery networks.	Patched by core rule	Y
CVE-2025-4700	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 15.10 before 18.0.5, 18.1 before 18.1.3, and 18.2 before 18.2.1 that, under	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		specific circumstances, could have potentially allowed a successful attacker to trigger unintended content rendering leading to XSS.		
CVE-2025-5084	Post Grid Master <= 3.4.13 - Reflected Cross-Site Scripting via argsArray['read_more_text']	The Post Grid Master plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'argsArray['read_more_text']' parameter in all versions up to, and including, 3.4.13 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
CVE-2025-8115	PHPGurukul Taxi Stand Management System new-autoortaxi-entry-form.php cross site scripting	A vulnerability has been found in PHPGurukul Taxi Stand Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/new-autoortaxi-entry-form.php. The manipulation of the argument registrationnumber/licensenumber 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-2025-8167	code-projects Church Donation System edit_members.php cross site scripting	A vulnerability was found in code-projects Church Donation System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/edit_members.php. The manipulation of the argument fname leads to cross site scripting. 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

Monthly Zero-Day Vulnerability Coverage Bulletin July 2025

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