INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

May 2025

The total zero-day vulnerabilities count for May month: 463

Command Injection	SQL Injection	SSRF	Path Traversal	Cross-Site Scripting	Malicious File Upload
28	198	7	30	174	26

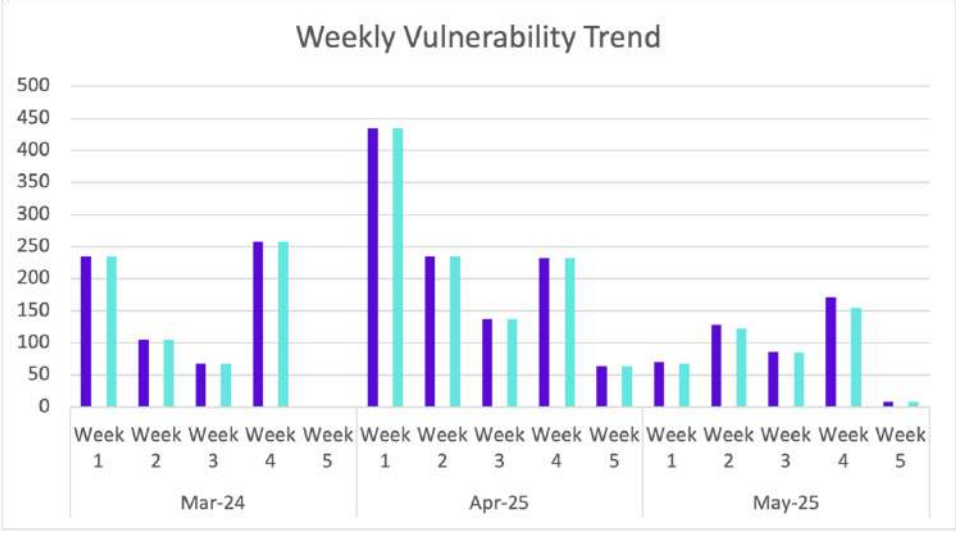
Zero-day vulnerabilities protected through core rules	463
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities found by Indusface WAS	437

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

Vulnerability Trend:

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

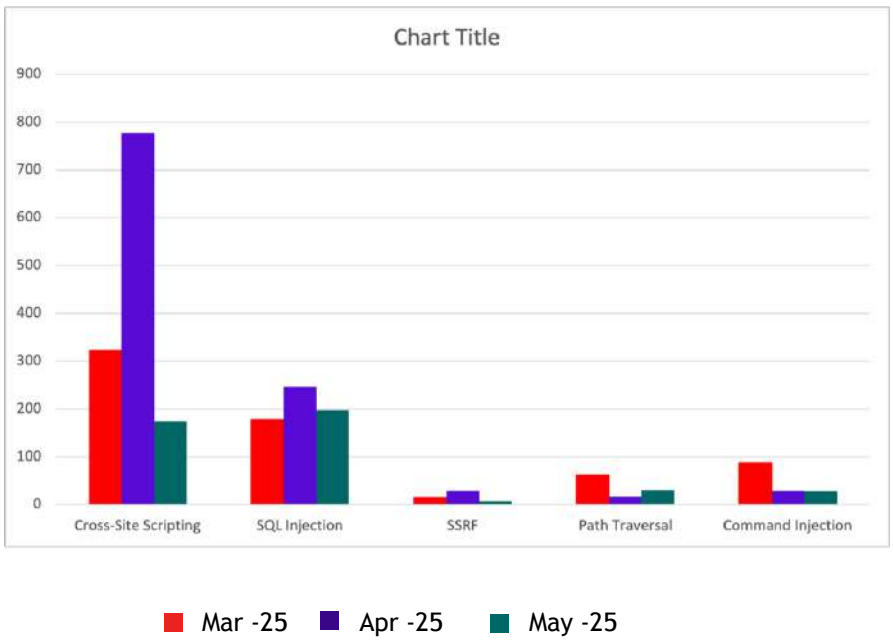
Weekly Vulnerability Trend



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

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

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-13808	Xpro Elementor Addons - Pro <= 1.4.9 - Authenticated (Contributor+) Remote Code Execution	The Xpro Elementor Addons - Pro plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.4.9 via the custom PHP widget. This is due to their only being client side controls when determining who can access the widget. This makes it possible for authenticated attackers, with Contributor-level access and above, to execute code on the server.	Patched by core rule	Y
CVE-2025-3983	AMTT Hotel Broadband Operation System nlog_down.php command injection	A vulnerability has been found in AMTT Hotel Broadband Operation System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /manager/system/nlog_down.php. The manipulation of the argument ProtocolType leads to command 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. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-4121	Netgear JWNR2000v2 cmd_wireless command injection	A vulnerability was found in Netgear JWNR2000v2 1.0.0.11. It has been declared as critical. Affected by this vulnerability is the function cmd_wireless. The manipulation of the argument host leads to command injection. The attack can be launched remotely. The vendor was contacted early about this	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		disclosure but did not respond in any way.		
CVE-2025-4122	Netgear JWNR2000v2 sub_435E04 command injection	A vulnerability was found in Netgear JWNR2000v2 1.0.0.11. It has been rated as critical. Affected by this issue is the function sub_435E04. The manipulation of the argument host leads to command injection. The attack may be launched remotely. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-4135	Netgear WG302v2 ui_get_input_value command injection	A vulnerability was found in Netgear WG302v2 up to 5.2.9 and classified as critical. Affected by this issue is the function ui_get_input_value. The manipulation of the argument host leads to command injection. The attack may be launched remotely. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-4340	D-Link DIR-890L/DIR-806A1 soap.cgi sub_175C8 command injection	A vulnerability classified as critical has been found in D-Link DIR-890L and DIR-806A1 up to 100CNb11/108B03. Affected is the function sub_175C8 of the file /htdocs/soap.cgi. The manipulation leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-4341	D-Link DIR-880L Request Header ssdpcgi sub_16570 command injection	A vulnerability classified as critical was found in D-Link DIR-880L up to 104WWb01. Affected by this vulnerability is the function sub_16570 of the file /htdocs/ssdpcgi of the component Request Header Handler. The manipulation of the argument HTTP_ST/REMOTE_ADDR/REMOTE_PORT/SERVER_ID 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-2025-4349	D-Link DIR-600L formSysCmd command injection	A vulnerability classified as critical has been found in D-Link DIR-600L up to 2.07B01. This affects the function formSysCmd. The manipulation of the argument host leads to command injection. It is possible to initiate the attack remotely. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-4350	D-Link DIR-600L	A vulnerability classified as	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	wake_on_lan command injection	critical was found in D-Link DIR-600L up to 2.07B01. This vulnerability affects the function wake_on_lan. The manipulation of the argument host leads to command injection. The attack can be initiated remotely. This vulnerability only affects products that are no longer supported by the maintainer.	rule	
CVE-2025-4357	Tenda RX3 telnet command injection	A vulnerability was found in Tenda RX3 16.03.13.11_multi. It has been rated as critical. This issue affects some unknown processing of the file /goform/telnet. The manipulation 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-2025-47481	WordPress GS Testimonial Slider plugin <= 3.2.9 - Content Injection vulnerability	Improper Control of Generation of Code ('Code Injection') vulnerability in GS Plugins GS Testimonial Slider allows Code Injection. This issue affects GS Testimonial Slider: from n/a through 3.2.9.	Patched by core rule	Y
CVE-2025-47691	WordPress Ultimate Member plugin <= 2.10.3 - Arbitrary Function Call vulnerability	Improper Control of Generation of Code ('Code Injection') vulnerability in Ultimate Member Ultimate Member allows Code Injection. This issue affects Ultimate Member: from n/a through 2.10.3.	Patched by core rule	Y
CVE-2025-4443	D-Link DIR-605L sub_454F2C command injection	A vulnerability was found in D-Link DIR-605L 2.13B01. It has been rated as critical. This issue affects the function sub_454F2C. The manipulation of the argument sysCmd leads to command injection. The attack may be initiated remotely. The vendor was contacted early about this disclosure. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2024-11861	Command injection in EnerSys AMPA 22.09 and prior versions	EnerSys AMPA 22.09 and prior versions are vulnerable to command injection leading to privileged remote shell access.	Patched by core rule	Y
CVE-2024-12442	Command injection in EnerSys AMPA versions 24.04 through 24.16, inclusive	EnerSys AMPA versions 24.04 through 24.16, inclusive, are vulnerable to command injection leading to privileged remote shell access.	Patched by core rule	Y
CVE-2025-4445	D-Link DIR-605L wake_on_lan command injection	A vulnerability classified as critical has been found in D-Link DIR-605L 2.13B01. Affected is the function wake_on_lan. The manipulation of the argument mac leads to command injection. It is possible to launch the attack remotely. The vendor was contacted early about this disclosure. This vulnerability only affects products that are no longer supported by	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the maintainer.		
CVE-2025-4453	D-Link DIR-619L formSysCmd command injection	A vulnerability was found in D-Link DIR-619L 2.04B04. It has been classified as critical. This affects the function formSysCmd. The manipulation of the argument sysCmd leads to command injection. It is possible to initiate the attack remotely. The vendor was contacted early about this disclosure. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-4454	D-Link DIR-619L wake_on_lan command injection	A vulnerability was found in D-Link DIR-619L 2.04B04. It has been declared as critical. This vulnerability affects the function wake_on_lan. The manipulation of the argument mac leads to command injection. The attack can be initiated remotely. The vendor was contacted early about this disclosure. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-4729	TOTOLINK A3002R/A3002RU HTTP POST Request formMapDelDevice command injection	A vulnerability was found in TOTOLINK A3002R and A3002RU 3.0.0-B20230809.1615. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /boafrm/formMapDelDevice of the component HTTP POST Request Handler. The manipulation of the argument macstr leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-47562	WordPress MapSVG <= 8.5.34 - Content Injection Vulnerability	Improper Control of Generation of Code ('Code Injection') vulnerability in RomanCode MapSVG allows Code Injection. This issue affects MapSVG: from n/a through 8.5.34.	Patched by core rule	Y
CVE-2025-48119	WordPress RS WP Book Showcase plugin <= 6.7.41 - Arbitrary Shortcode Execution vulnerability	Improper Control of Generation of Code ('Code Injection') vulnerability in RS WP THEMES RS WP Book Showcase allows Code Injection. This issue affects RS WP Book Showcase: from n/a through 6.7.41.	Patched by core rule	Y
CVE-2025-48120	WordPress MapSVG Lite plugin <= 8.6.4 - Arbitrary Shortcode Execution vulnerability	Improper Control of Generation of Code ('Code Injection') vulnerability in RomanCode MapSVG Lite allows Code Injection. This issue affects MapSVG Lite: from n/a through 8.6.4.	Patched by core rule	Y
CVE-2025-4849	TOTOLINK N300RH cstecgi.cgi CloudACMunualUpdateUserdata command injection	A vulnerability was found in TOTOLINK N300RH 6.1c.1390_B20191101. It has been rated as critical. Affected by this issue is the function CloudACMunualUpdateUserdata of the file /cgi-bin/cstecgi.cgi. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument url leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-4850	TOTOLINK N300RH cstecgi.cgi setUnloadUserData command injection	A vulnerability classified as critical has been found in TOTOLINK N300RH 6.1c.1390_B20191101. This affects the function setUnloadUserData of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument plugin_name 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-2025-4851	TOTOLINK N300RH cstecgi.cgi setUploadUserData command injection	A vulnerability classified as critical was found in TOTOLINK N300RH 6.1c.1390_B20191101. This vulnerability affects the function setUploadUserData of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument FileName 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-2025-4999	Linksys FGW3000-AH/FGW3000-HK HTTP POST Request sysconf.cgi sub_4153FC command injection	A vulnerability was found in Linksys FGW3000-AH and FGW3000-HK up to 1.0.17.000000 and classified as critical. Affected by this issue is the function sub_4153FC of the file /cgi-bin/sysconf.cgi of the component HTTP POST Request Handler. The manipulation of the argument supplicant_rnd_id_en leads to 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-2025-5000	Linksys FGW3000-AH/FGW3000-HK HTTP POST Request sysconf.cgi control_panel_sw command injection	A vulnerability was found in Linksys FGW3000-AH and FGW3000-HK up to 1.0.17.000000. It has been classified as critical. This affects the function control_panel_sw of the file /cgi-bin/sysconf.cgi of the component HTTP POST Request Handler. The manipulation of the argument filename leads to 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-2025-5126	FLIR AX8 settingsregional.php setDataTime command injection	A vulnerability classified as critical was found in FLIR AX8 up to 1.46.16. This vulnerability affects the function setDataTime of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		\usr\www\application\models\settingsregional.php. The manipulation of the argument year/month/day/hour/minute leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		

Path Traversal Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-4036	201206030 Novel Chapter AuthorController.java updateBookChapter access control	A vulnerability was found in 201206030 Novel 3.5.0 and classified as critical. This issue affects the function updateBookChapter of the file src/main/java/io/github/xxyopen/novel/controller/author/AuthorController.java of the component Chapter Handler. The manipulation leads to improper access controls. 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-2025-4078	Wangshen SecGate 3600 g=log_export_file path traversal	A vulnerability, which was classified as problematic, has been found in Wangshen SecGate 3600 2400. This issue affects some unknown processing of the file ?g=log_export_file. The manipulation of the argument file_name leads to path traversal. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-4175	AlanBinu007 Spring-Boot-Advanced-Projects Upload Profile API Endpoint UserProfileController.jav uploadUserProfileImage path traversal	A vulnerability, which was classified as critical, was found in AlanBinu007 Spring-Boot-Advanced-Projects up to 3.1.3. This affects the function uploadUserProfileImage of the file /Spring-Boot-Advanced-Projects-main/Project-4.SpringBoot-AWS-S3/backend/src/main/java/com/urunov/profile/UserProfileController.jav of the component Upload Profile API Endpoint. The manipulation of the argument File leads to path traversal. 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		respond in any way.		
CVE-2025-4178	xiaowei1118 java_server File Upload API FoodController.java path traversal	A vulnerability was found in xiaowei1118 java_server up to 11a5bac8f4ba1c17e4bc1b27cad6d24868500e3a on Windows and classified as critical. This issue affects some unknown processing of the file /src/main/java/com/changyu/foryou/controller/FoodController.java of the component File Upload API. The manipulation leads to path traversal. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available.	Patched by core rule	Y
CVE-2025-4185	Wangshen SecGate 3600 g=obj_area_export_save path traversal	A vulnerability, which was classified as critical, has been found in Wangshen SecGate 3600 2024. This issue affects some unknown processing of the file ?g=obj_area_export_save. The manipulation of the argument file_name leads to path traversal. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-4186	Wangshen SecGate 3600 g=route_ispinfo_export_save path traversal	A vulnerability, which was classified as critical, was found in Wangshen SecGate 3600 2024. Affected is an unknown function of the file /?g=route_ispinfo_export_save. The manipulation of the argument file_name 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-2025-4329	74CMS index path traversal	A vulnerability was found in 74CMS up to 3.33.0. It has been rated as problematic. Affected by this issue is the function index of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/index.php/index/download/index. The manipulation of the argument url leads to path traversal. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-4511	vector4wang spring-boot-quick quick-img2txt Img2TxtController.java ResponseEntity path traversal	A vulnerability was found in vector4wang spring-boot-quick up to 20250422. It has been rated as critical. This issue affects the function ResponseEntity of the file /spring-boot-quick-master/quick-img2txt/src/main/java/com/quick/controller/Img2TxtController.java of the component quick-img2txt. The manipulation leads to path traversal. 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-2025-4545	CTCMS Content Management System File Tpl.php del path traversal	A vulnerability was found in CTCMS Content Management System 2.1.2. It has been classified as critical. Affected is the function del of the file ctcms\apps\controllers\admin\Tpl.php of the component File Handler. 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-2025-3659	Improper authentication handling for Digi PortServer TS; Digi One SP, SP IA, IA; Digi One IAP	Improper authentication handling was identified in a set of HTTP POST requests affecting the following product families: * Digi PortServer TS - prior to and including 82000747_AA, build date 06/17/2022 * Digi One SP/Digi One SP IA/Digi One IA - prior to and including 82000774_Z, build date 10/19/2020 * Digi One IAP – prior to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and including 82000770 Z, build date 10/19/2020 A specially crafted POST request to the device's web interface may allow an unauthenticated attacker to modify configuration settings.		
CVE-2025-47445	WordPress Eventin <= 4.0.26 - Arbitrary File Download Vulnerability	Relative Path Traversal vulnerability in Themewinter Eventin allows Path Traversal.This issue affects Eventin: from n/a through 4.0.26.	Patched by core rule	Y
CVE-2025-4755	D-Link DI-7003GV2 netconfig.asp sub_497DE4 improper authentication	A vulnerability was found in D-Link DI-7003GV2 24.04.18D1 R(68125). It has been classified as critical. This affects the function sub_497DE4 of the file /H5/netconfig.asp. The manipulation leads to improper authentication. 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-2025-4868	merikbest ecommerce-spring-reactjs File Upload Endpoint admin path traversal	A vulnerability was found in merikbest ecommerce-spring-reactjs up to 464e610bb11cc2619cf6ce8212ccc2d1fd4277fd. It has been rated as critical. Affected by this issue is some unknown functionality of the file /api/v1/admin/ of the component File Upload Endpoint. 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. 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-2025-4893	jammy928 CoinExchange_CryptoExchange_Java File Upload Endpoint UploadFileUtil.java uploadLocalImage path traversal	A vulnerability classified as critical has been found in jammy928 CoinExchange_CryptoExchange_Java up to 8adf508b996020d3efbeeb2473d7235bd01436fa. This affects the function	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		uploadLocalImage of the file /CoinExchange_CryptoExchange_Java-master/00_framework/core/src/main/java/com/bizzan/bitrade/util/UploadFileUtil.java of the component File Upload Endpoint. 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 does not use versioning. This is why information about affected and unaffected releases are unavailable.		
CVE-2025-4898	SourceCodester Student Result Management System Logo File update_system.php unlink path traversal	A vulnerability was found in SourceCodester Student Result Management System 1.0. It has been declared as critical. This vulnerability affects the function unlink of the file update_system.php of the component Logo File Handler. The manipulation of the argument old_logo 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-2025-3223	WorkstationST EGD Configuration Server Path Traversal Vulnerability	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in GE Vernova WorkstationST on Windows (EGD Configuration Server modules) allows Path Traversal.This issue affects WorkstationST: WorkstationST V07.10.10C and earlier.	Patched by core rule	Y
CVE-2025-46441	WordPress Section Widget plugin <= 3.3.1 - Path Traversal vulnerability	Path Traversal: '.../...//' vulnerability in ctltwp Section Widget allows Path Traversal.This issue affects Section Widget: from n/a through 3.3.1.	Patched by core rule	Y
CVE-2025-4912	SourceCodester Student Result Management System Image File update_student.php path traversal	A vulnerability has been found in SourceCodester Student Result Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/core/update_stud	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		ent.php of the component Image File Handler. The manipulation of the argument old_photo leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-31053	WordPress KBx Pro Ultimate <= 7.9.8 - Arbitrary File Deletion Vulnerability	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in quantumcloud KBx Pro Ultimate allows Path Traversal. This issue affects KBx Pro Ultimate: from n/a through 7.9.8.	Patched by core rule	Y
CVE-2025-46486	WordPress Nomupay Payment Processing Gateway <= 7.1.7 - Arbitrary File Download Vulnerability	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in totalprocessing Nomupay Payment Processing Gateway allows Path Traversal. This issue affects Nomupay Payment Processing Gateway: from n/a through 7.1.7.	Patched by core rule	Y
CVE-2025-46527	WordPress Web3Press – Decentralize Publishing with Writing NFT plugin <= 3.2.0 - Arbitrary File Read vulnerability	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in LikeCoin Web3Press allows Path Traversal. This issue affects Web3Press: from n/a through 3.2.0.	Patched by core rule	Y
CVE-2025-47492	WordPress Drag and Drop File Upload for Elementor Forms <= 1.4.3 - Arbitrary File Deletion Vulnerability	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in add-ons.org Drag and Drop File Upload for Elementor Forms allows Path Traversal. This issue affects Drag and Drop File Upload for Elementor Forms: from n/a through 1.4.3.	Patched by core rule	Y
CVE-2025-47512	WordPress Tainacan plugin <= 0.21.14 - Arbitrary File Deletion vulnerability	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in tainacan Tainacan allows Path Traversal. This issue affects Tainacan: from n/a through 0.21.14.	Patched by core rule	Y
CVE-2025-47513	WordPress Infocob CRM Forms plugin <= 2.4.0 - Arbitrary File Download vulnerability	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in James Laforge Infocob CRM Forms allows Path Traversal. This issue	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects Infocob CRM Forms: from n/a through 2.4.0.		
CVE-2025-5157	H3C SecCenter SMP-E1114P02 fileContent path traversal	A vulnerability was found in H3C SecCenter SMP-E1114P02 up to 20250513. It has been classified as critical. This affects the function fileContent of the file /cfgFile/fileContent. The manipulation of the argument filePath leads to path traversal. It is possible to initiate the attack remotely. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-5158	H3C SecCenter SMP-E1114P02 downloadSoftware path traversal	A vulnerability was found in H3C SecCenter SMP-E1114P02 up to 20250513. It has been declared as problematic. This vulnerability affects the function downloadSoftware of the file /cfgFile/downloadSoftware. 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. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-5159	H3C SecCenter SMP-E1114P02 download path traversal	A vulnerability was found in H3C SecCenter SMP-E1114P02 up to 20250513. It has been rated as problematic. This issue affects the function Download of the file /cfgFile/1/download. The manipulation of the argument Name leads to path traversal. 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-2025-39366	WordPress wProject theme < 5.8.0 - Subscriber+ Privilege Escalation vulnerability	Incorrect Privilege Assignment vulnerability in Rocket Apps wProject.This issue affects wProject: from n/a before 5.8.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-4537	yangzongzhuan RuoYi-Vue Password login.vue sensitive information in a cookie	A vulnerability was found in yangzongzhuan RuoYi-Vue up to 3.8.9 and classified as problematic. Affected by this issue is some unknown functionality of the file ruoyi-ui/jsencrypt.js and ruoyi-ui/login.vue of the component Password Handler. The manipulation leads to cleartext storage of sensitive information in a cookie. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-48134	WordPress WP Tabs <= 2.2.11 - PHP Object Injection Vulnerability	Deserialization of Untrusted Data vulnerability in ShapedPlugin LLC WP Tabs allows Object Injection. This issue affects WP Tabs: from n/a through 2.2.11.	Patched by core rule	Y

Server-side Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-47464	WordPress Solace Extra <= 1.3.1 - Server Side Request Forgery (SSRF) Vulnerability	Server-Side Request Forgery (SSRF) vulnerability in solacewp Solace Extra allows Server Side Request Forgery. This issue affects Solace Extra: from n/a through 1.3.1.	Patched by core rule	Y
CVE-2025-47483	WordPress Easy Replace Image <= 3.5.0 - Server Side Request Forgery (SSRF) Vulnerability	Server-Side Request Forgery (SSRF) vulnerability in Iulia Cazan Easy Replace Image allows Server Side Request Forgery. This issue affects Easy Replace Image: from n/a through 3.5.0.	Patched by core rule	Y
CVE-2025-47484	WordPress Display Remote Posts Block <= 1.1.0 - Server Side Request Forgery (SSRF) Vulnerability	Server-Side Request Forgery (SSRF) vulnerability in Oliver Campion Display Remote Posts Block allows Server Side Request Forgery. This issue affects Display Remote Posts Block: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-47548	WordPress Wbcom Designs - Activity Link Preview For BuddyPress <= 1.4.4 - Server Side Request Forgery (SSRF) Vulnerability	Server-Side Request Forgery (SSRF) vulnerability in Varun Dubey Wbcom Designs - Activity Link Preview For BuddyPress allows Server Side Request Forgery. This issue affects Wbcom Designs - Activity Link Preview For BuddyPress: from n/a through 1.4.4.	Patched by core rule	Y
CVE-2025-47635	WordPress WebinarPress <= 1.33.27 - Server Side Request Forgery (SSRF) Vulnerability	Server-Side Request Forgery (SSRF) vulnerability in WPWebinarSystem WebinarPress allows Server Side Request Forgery. This issue affects WebinarPress: from n/a through 1.33.27.	Patched by core rule	Y
CVE-2025-47664	WordPress WP Pipes <= 1.4.2 - Server Side Request Forgery (SSRF) Vulnerability	Server-Side Request Forgery (SSRF) vulnerability in ThimPress WP Pipes allows Server Side Request Forgery. This issue affects WP Pipes: from n/a through 1.4.2.	Patched by core rule	Y
CVE-2025-48739		A Server-Side Request Forgery (SSRF) vulnerability in StrangeBee TheHive 5.2.0 before 5.2.16, 5.3.0 before 5.3.11, 5.4.0 before 5.4.10, and 5.5.0 before 5.5.1 allows remote authenticated attackers with admin permissions (allowing them to access specific API endpoints) to manipulate URLs to direct requests to unexpected hosts or ports. This allows the attacker to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		use a TheHive server as a proxy to reach internal or otherwise restricted resources. This could be exploited to access other servers on the internal network.		

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-3955	codeprojects Patient Record Management System edit_rpatient.php.php sql injection	A vulnerability, which was classified as critical, was found in codeprojects Patient Record Management System 1.0. This affects an unknown part of the file /edit_rpatient.php.php. The manipulation of the argument id/lastname 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-2025-3956	201206030 novel-cloud BookInfoMapper.xml RestResp sql injection	A vulnerability has been found in 201206030 novel-cloud 1.4.0 and classified as critical. This vulnerability affects the function RestResp of the file novel-cloud-master/novel-book/novel-book-service/src/main/resources/mapper/BookInfoMapper.xml. The manipulation leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-3957	opplus springboot-admin SysLogDao.xml sql injection	A vulnerability was found in opplus springboot-admin 1.0 and classified as critical. This issue affects some unknown processing of the file \src\main\resources\mapper\sys\SysLogDao.xml. The manipulation of the argument order 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-2025-3968	codeprojects News Publishing Site Dashboard api.php sql injection	A vulnerability was found in codeprojects News Publishing Site Dashboard 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /api.php. The manipulation of the argument cat_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-2025-3971	PHPGurukul COVID19 Testing Management System add-	A vulnerability classified as critical was found in PHPGurukul COVID19	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	phlebotomist.php sql injection	Testing Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /add-phlebotomist.php. The manipulation of the argument empid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3972	PHPGurukul COVID19 Testing Management System bwdates-report-result.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul COVID19 Testing Management System 1.0. Affected by this issue is some unknown functionality of the file /bwdates-report-result.php. The manipulation of the argument todate 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-2025-3973	PHPGurukul COVID19 Testing Management System check_availability.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul COVID19 Testing Management System 1.0. This affects an unknown part of the file /check_availability.php. The manipulation of the argument mobnumber leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-3974	PHPGurukul COVID19 Testing Management System edit-phlebotomist.php sql injection	A vulnerability has been found in PHPGurukul COVID19 Testing Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /edit-phlebotomist.php?pid=11. The manipulation of the argument mobilenumber leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-3976	PHPGurukul COVID19 Testing Management	A vulnerability was found in PHPGurukul COVID19	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System new-user-testing.php sql injection	Testing Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /new-user-testing.php. The manipulation of the argument mobilenumber leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.		
CVE-2025-4004	PHPGurukul COVID19 Testing Management System password-recovery.php sql injection	A vulnerability was found in PHPGurukul COVID19 Testing Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /password-recovery.php. The manipulation of the argument contactno leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-4005	PHPGurukul COVID19 Testing Management System patient-report.php sql injection	A vulnerability was found in PHPGurukul COVID19 Testing Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /patient-report.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-2025-4013	PHPGurukul Art Gallery Management System aboutus.php sql injection	A vulnerability was found in PHPGurukul Art Gallery Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/aboutus.php. The manipulation of the argument pagetitle 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-2025-4014	PHPGurukul Art Gallery Management System manage-art-medium.php sql injection	A vulnerability was found in PHPGurukul Art Gallery Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/manage-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		art-medium.php. The manipulation of the argument artmed leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-4020	PHPGurukul Old Age Home Management System contact.php sql injection	A vulnerability was found in PHPGurukul Old Age Home Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /contact.php. The manipulation of the argument fname 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-2025-4021	code-projects Patient Record Management System edit_spatient.php sql injection	A vulnerability was found in code-projects Patient Record Management System 1.0. It has been classified as critical. This affects an unknown part of the file /edit_spatient.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-2025-4026	PHPGurukul Nipah Virus Testing Management System profile.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Nipah Virus Testing Management System 1.0. This issue affects some unknown processing of the file /profile.php. The manipulation of the argument adminname 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-2025-4027	PHPGurukul Old Age Home Management System rules.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/rules.php. The manipulation of the argument pagetitle 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-2025-4028	PHPGurukul COVID19 Testing Management System profile.php sql injection	A vulnerability has been found in PHPGurukul COVID19 Testing Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /profile.php. The manipulation of the argument mobilenumber 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-2025-4030	PHPGurukul COVID19 Testing Management System search-report-result.php sql injection	A vulnerability was found in PHPGurukul COVID19 Testing Management System 1.0. It has been classified as critical. This affects an unknown part of the file /search-report-result.php. The manipulation of the argument serachdata 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-2025-4031	PHPGurukul Pre-School Enrollment System aboutus.php sql injection	A vulnerability was found in PHPGurukul Pre-School Enrollment System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/aboutus.php. The manipulation of the argument pagetitle leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-4033	PHPGurukul Nipah Virus Testing Management System patient-search-report.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Nipah Virus Testing Management System 1.0. Affected is an unknown function of the file /patient-search-report.php. The manipulation of the argument searchdata leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-4039	PHPGurukul Rail Pass Management System search-pass.php sql injection	A vulnerability was found in PHPGurukul Rail Pass Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/search-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		pass.php. The manipulation of the argument searchdata leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-4060	PHPGurukul Notice Board System category.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Notice Board System 1.0. This issue affects some unknown processing of the file /category.php. The manipulation of the argument catname 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-2025-4070	PHPGurukul Rail Pass Management System changeimage.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Rail Pass Management System 1.0. This affects an unknown part of the file /admin/changeimage.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-2025-4071	PHPGurukul COVID19 Testing Management System test-details.php sql injection	A vulnerability has been found in PHPGurukul COVID19 Testing Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /test-details.php. The manipulation of the argument Status 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-2025-4072	PHPGurukul Online Nurse Hiring System edit-nurse.php sql injection	A vulnerability was found in PHPGurukul Online Nurse Hiring System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/edit-nurse.php. The manipulation leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Multiple parameters might be affected.	Patched by core rule	Y
CVE-2025-4073	PHPGurukul Student Record System change-password.php sql	A vulnerability was found in PHPGurukul Student Record System 3.20. It has been	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	classified as critical. Affected is an unknown function of the file /change-password.php. The manipulation of the argument currentpassword 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-2025-4074	PHPGurukul Curfew e-Pass Management System pass-bwdates-report.php sql injection	A vulnerability was found in PHPGurukul Curfew e-Pass Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/pass-bwdates-report.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-2025-4080	PHPGurukul Online Nurse Hiring System view-request.php sql injection	A vulnerability has been found in PHPGurukul Online Nurse Hiring System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/view-request.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-2025-4108	PHPGurukul Student Record System add-subject.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Student Record System 3.20. Affected is an unknown function of the file /add-subject.php. The manipulation of the argument sub1 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-2025-4109	PHPGurukul Pre-School Enrollment System edit-subadmin.php sql injection	A vulnerability has been found in PHPGurukul Pre-School Enrollment System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/edit-subadmin.php. The manipulation of the argument mobilenumber leads to sql injection. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.		
CVE-2025-4110	PHPGurukul Pre-School Enrollment System edit-teacher.php sql injection	A vulnerability was found in PHPGurukul Pre-School Enrollment System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/edit-teacher.php. The manipulation of the argument mobilenumber 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-2025-4111	PHPGurukul Pre-School Enrollment System visitor-details.php sql injection	A vulnerability was found in PHPGurukul Pre-School Enrollment System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/visitor-details.php. The manipulation of the argument Status 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-2025-4112	PHPGurukul Student Record System add-course.php sql injection	A vulnerability was found in PHPGurukul Student Record System 3.20. It has been declared as critical. This vulnerability affects unknown code of the file /add-course.php. The manipulation of the argument course-short 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-2025-4113	PHPGurukul Curfew e-Pass Management System edit-pass-detail.php sql injection	A vulnerability was found in PHPGurukul Curfew e-Pass Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/edit-pass-detail.php. The manipulation of the argument editid 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-4151	PHPGurukul Curfew e-Pass Management System pass-bwdates-reports-details.php sql injection	A vulnerability was found in PHPGurukul Curfew e-Pass Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/pass-bwdates-reports-details.php. The manipulation of the argument fromdate leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-4152	PHPGurukul Online Birth Certificate System bwdates-reports-details.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Online Birth Certificate System 1.0. Affected is an unknown function of the file /admin/bwdates-reports-details.php. The manipulation of the argument fromdate 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-2025-4153	PHPGurukul Park Ticketing Management System profile.php sql injection	A vulnerability classified as critical was found in PHPGurukul Park Ticketing Management System 2.0. Affected by this vulnerability is an unknown functionality of the file /profile.php. The manipulation of the argument adminname 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-2025-4154	PHPGurukul Pre-School Enrollment System enrollment-details.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Pre-School Enrollment System 1.0. Affected by this issue is some unknown functionality of the file /admin/enrollment-details.php. The manipulation of the argument Status 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-2025-4155	PHPGurukul Boat Booking System edit-boat.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Boat	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Booking System 1.0. This affects an unknown part of the file /admin/edit-boat.php. The manipulation of the argument bid 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-2025-4156	PHPGurukul Boat Booking System change-image.php sql injection	A vulnerability has been found in PHPGurukul Boat Booking System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/change-image.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-2025-4157	PHPGurukul Boat Booking System booking-details.php sql injection	A vulnerability was found in PHPGurukul Boat Booking System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/booking-details.php. The manipulation of the argument Status 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-2025-4163	PHPGurukul Land Record System aboutus.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Land Record System 1.0. This issue affects some unknown processing of the file /admin/aboutus.php. The manipulation of the argument pagetitle leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-4164	PHPGurukul Employee Record Management System changepassword.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Employee Record Management System 1.3. Affected is an unknown function of the file changepassword.php. The manipulation of the argument currentpassword leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and may be used.		
CVE-2025-4173	SourceCodester Online Eyewear Shop Master.php delete_cart sql injection	A vulnerability classified as critical was found in SourceCodester Online Eyewear Shop 1.0. Affected by this vulnerability is the function delete_cart of the file /oews/classes/Master.php?f=delete_cart. 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-2025-4174	PHPGurukul COVID19 Testing Management System login.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul COVID19 Testing Management System 1.0. Affected by this issue is some unknown 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.	Patched by core rule	Y
CVE-2025-4176	PHPGurukul Blood Bank & Donor Management System request-received-bydonar.php sql injection	A vulnerability has been found in PHPGurukul Blood Bank & Donor Management System 2.4 and classified as critical. This vulnerability affects unknown code of the file /admin/request-received-bydonar.php. The manipulation of the argument searchdata leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-4191	PHPGurukul Employee Record Management System editmyeducation.php sql injection	A vulnerability has been found in PHPGurukul Employee Record Management System 1.3 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /editmyeducation.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-2025-4196	SourceCodester Patient Record Management System birthing.php sql injection	A vulnerability was found in SourceCodester Patient Record Management 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 /birthing.php. The manipulation of the argument comp_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-4197	code-projects Patient Record Management System edit_xpatient.php sql injection	A vulnerability classified as critical has been found in code-projects Patient Record Management System 1.0. Affected is an unknown function of the file /edit_xpatient.php. The manipulation of the argument lastname 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-2025-4213	PHPGurukul Online Birth Certificate System search.php sql injection	A vulnerability has been found in PHPGurukul Online Birth Certificate System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/search.php. The manipulation of the argument searchdata leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-4226	PHPGurukul Cyber Cafe Management System add-computer.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Cyber Cafe Management System 1.0. This affects an unknown part of the file /add-computer.php. The manipulation of the argument compname 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-2025-4241	PHPGurukul Teacher Subject Allocation Management System search.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Teacher Subject Allocation Management System 1.0. Affected is an unknown function of the file /admin/search.php. The manipulation of the argument searchdata leads to sql injection. It is possible to launch the attack remotely. The exploit has		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		been disclosed to the public and may be used.		
CVE-2025-4242	PHPGurukul Online Birth Certificate System between-dates-report.php sql injection	A vulnerability classified as critical was found in PHPGurukul Online Birth Certificate System 2.0. Affected by this vulnerability is an unknown functionality of the file /admin/between-dates-report.php. The manipulation of the argument fromdate 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-2025-4243	code-projects Online Bus Reservation System print.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Online Bus Reservation System 1.0. Affected by this issue is some unknown functionality of the file /print.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-2025-4244	code-projects Online Bus Reservation System seatlocation.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Online Bus Reservation System 1.0. This affects an unknown part of the file /seatlocation.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-2025-4249	PHPGurukul e-Diary Management System manage-categories.php sql injection	A vulnerability was found in PHPGurukul e-Diary Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /manage-categories.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-2025-4250	code-projects Nero Social Networking Site index.php sql injection	A vulnerability was found in code-projects Nero Social Networking Site 1.0. It has been classified as critical. This affects an unknown part of the file /index.php. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument fname/lname/login/password2/cpassword/address/cnumber/email/gender/propic/month 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-2025-4262	PHPGurukul Online DJ Booking Management System user-search.php sql injection	A vulnerability was found in PHPGurukul Online DJ Booking Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/user-search.php. The manipulation of the argument searchdata leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-4263	PHPGurukul Online DJ Booking Management System booking-search.php sql injection	A vulnerability was found in PHPGurukul Online DJ Booking Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/booking-search.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-2025-4264	PHPGurukul Emergency Ambulance Hiring Portal edit-ambulance.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Emergency Ambulance Hiring Portal 1.0. Affected is an unknown function of the file /admin/edit-ambulance.php. The manipulation of the argument dconnum 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-2025-4265	PHPGurukul Emergency Ambulance Hiring Portal contact-us.php sql injection	A vulnerability classified as critical was found in PHPGurukul Emergency Ambulance Hiring Portal 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/contact-us.php. The manipulation of the argument mobnum leads to sql injection. The attack can be launched	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. Other parameters might be affected as well.		
CVE-2025-4266	PHPGurukul Notice Board System bwdates-reports-details.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Notice Board System 1.0. Affected by this issue is some unknown functionality of the file /bwdates-reports-details.php?vid=2. The manipulation of the argument fromdate/tomdate 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-2025-4267	SourceCodester/oretnom23 Stock Management System Purchase Order Details Page view_po sql injection	A vulnerability, which was classified as critical, was found in SourceCodester/oretnom23 Stock Management System 1.0. This affects an unknown part of the file /admin/?page=purchase_order/view_po of the component Purchase Order Details Page. 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-2025-4283	SourceCodester/oretnom23 Stock Management System Login.php sql injection	A vulnerability was found in SourceCodester/oretnom23 Stock Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /classes/Login.php?f=login. 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-2025-4297	PHPGurukul Men Salon Management System change-password.php sql injection	A vulnerability was found in PHPGurukul Men Salon Management System 2.0. It has been classified as critical. This affects an unknown part of the file /admin/change-password.php. The manipulation 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. Multiple parameters might be affected.		
CVE-2025-4303	PHPGurukul Human Metapneumovirus Testing Management System add-phlebotomist.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Human Metapneumovirus Testing Management System 1.0. Affected by this issue is some unknown functionality of the file /add-phlebotomist.php. The manipulation of the argument empid 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-2025-4304	PHPGurukul Cyber Cafe Management System adminprofile.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Cyber Cafe Management System 1.0. This affects an unknown part of the file /adminprofile.php. The manipulation of the argument mobilenumber leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-4306	PHPGurukul Nipah Virus Testing Management System edit-phlebotomist.php sql injection	A vulnerability was found in PHPGurukul Nipah Virus Testing Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /edit-phlebotomist.php. The manipulation of the argument mobilenumber leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-4307	PHPGurukul Art Gallery Management System add-art-medium.php sql injection	A vulnerability was found in PHPGurukul Art Gallery Management System 1.1. It has been classified as critical. Affected is an unknown function of the file /admin/add-art-medium.php. The manipulation of the argument artmed 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-2025-4308	PHPGurukul Art Gallery Management System add-art-type.php sql injection	A vulnerability was found in PHPGurukul Art Gallery Management System 1.1. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/add-art-type.php. The manipulation of the argument arttype 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-2025-4309	PHPGurukul Art Gallery Management System add-art-type.php sql injection	A vulnerability was found in PHPGurukul Art Gallery Management System 1.1. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/add-art-type.php. The manipulation of the argument arttype 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-2025-4331	SourceCodester Online Student Clearance System login.php sql injection	A vulnerability classified as critical was found in SourceCodester Online Student Clearance System 1.0. This vulnerability affects unknown code of the file /Admin/login.php. The manipulation of the argument username/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-2025-4332	PHPGurukul Company Visitor Management System visitor-detail.php sql injection	A vulnerability was found in PHPGurukul Company Visitor Management System 2.0 and classified as critical. Affected by this issue is some unknown functionality of the file /visitor-detail.php. The manipulation of the argument editid 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-2025-4352	Golden Link Secondary System tcEntrFlowSelect.htm sql injection	A vulnerability, which was classified as critical, has been found in Golden Link Secondary System up to 20250424. This issue affects some unknown processing of the file /reprotframework/tcEntrFlowSelect.htm. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument custTradeId leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-4353	Golden Link Secondary System queryTsDictionaryType.htm sql injection	A vulnerability, which was classified as critical, was found in Golden Link Secondary System up to 20250424. Affected is an unknown function of the file /paraframework/queryTsDictionaryType.htm. The manipulation of the argument dictCn1 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-2025-4358	PHPGurukul Company Visitor Management System admin-profile.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Company Visitor Management System 2.0. Affected is an unknown function of the file /admin-profile.php. The manipulation of the argument adminname 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-2025-4361	PHPGurukul Company Visitor Management System department.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Company Visitor Management System 2.0. This affects an unknown part of the file /department.php. The manipulation of the argument departmentname 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-2025-47460	WordPress TrackShip for WooCommerce <= 1.9.1 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in TrackShip TrackShip for WooCommerce allows SQL Injection. This issue affects TrackShip for WooCommerce: from n/a through 1.9.1.	Patched by core rule	Y
CVE-2025-47490	WordPress Ultimate WP Mail <= 1.3.4 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Rustaurius Ultimate WP Mail allows SQL Injection. This issue affects Ultimate WP	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Mail: from n/a through 1.3.4.		
CVE-2025-47537	WordPress PDF Invoices for WooCommerce + Drag and Drop Template Builder <= 5.3.8 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in add-ons.org PDF Invoices for WooCommerce + Drag and Drop Template Builder allows SQL Injection. This issue affects PDF Invoices for WooCommerce + Drag and Drop Template Builder: from n/a through 5.3.8.	Patched by core rule	Y
CVE-2025-47538	WordPress Cart tracking for WooCommerce <= 1.0.17 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in wpdever Cart tracking for WooCommerce allows SQL Injection. This issue affects Cart tracking for WooCommerce: from n/a through 1.0.17.	Patched by core rule	Y
CVE-2025-47544	WordPress Dynamic Pricing With Discount Rules for WooCommerce <= 4.5.8 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in acowebs Dynamic Pricing With Discount Rules for WooCommerce allows Blind SQL Injection. This issue affects Dynamic Pricing With Discount Rules for WooCommerce: from n/a through 4.5.8.	Patched by core rule	Y
CVE-2025-47587	WordPress YaySMTP <= 2.6.4 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in YayCommerce YaySMTP allows Blind SQL Injection. This issue affects YaySMTP: from n/a through 2.6.4.	Patched by core rule	Y
CVE-2025-47643	WordPress ELEX Product Feed for WooCommerce <= 3.1.2 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ELEXtensions ELEX Product Feed for WooCommerce allows SQL Injection. This issue affects ELEX Product Feed for WooCommerce: from n/a through 3.1.2.	Patched by core rule	Y
CVE-2025-47657	WordPress Productive Commerce <= 1.1.22 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Productive Minds Productive Commerce allows SQL Injection. This issue affects Productive Commerce: from n/a through 1.1.22.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-4458	code-projects Patient Record Management System edit_upatient.php sql injection	A vulnerability was found in code-projects Patient Record Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /edit_upatient.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-2025-4459	code-projects Patient Record Management System fecalysis_form.php sql injection	A vulnerability was found in code-projects Patient Record Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file fecalysis_form.php. The manipulation of the argument itr_no leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-4467	SourceCodester Online Student Clearance System edit-admin.php sql injection	A vulnerability was found in SourceCodester Online Student Clearance System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/edit-admin.php. The manipulation of the argument txtfullname/txtemail/cmddesignation 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-2025-4505	PHPGurukul Apartment Visitors Management System category.php sql injection	A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /category.php. The manipulation of the argument categoryname 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-2025-4508	PHPGurukul e-Diary Management System my-profile.php sql injection	A vulnerability classified as critical was found in PHPGurukul e-Diary Management System 1.0. This vulnerability affects unknown code of the file /my-profile.php. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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-2025-4509	PHPGurukul e-Diary Management System manage-notes.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul e-Diary Management System 1.0. This issue affects some unknown processing of the file /manage-notes.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-2025-4541	LmxCMS POST Request ZtAction.class.php manageZt sql injection	A vulnerability classified as critical has been found in LmxCMS 1.41. Affected is the function manageZt of the file c\admin\ZtAction.class.php of the component POST Request Handler. The manipulation of the argument sortid 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-2025-4543	LyLme Spage ajax_link.php sql injection	A vulnerability, which was classified as critical, was found in LyLme Spage 2.1. This affects an unknown part of the file lylme_spage/blob/master/admin/ajax_link.php. The manipulation of the argument sort leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-4550	PHPGurukul Apartment Visitors Management System pass-details.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Apartment Visitors Management System 1.0. This issue affects some unknown processing of the file /admin/pass-details.php. The manipulation of the argument pid 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-2025-4553	PHPGurukul Apartment Visitors Management System bwdates-reports-details.php sql injection	A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/bwdates-reports-details.php. The manipulation of the argument fromdate/todate leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-4554	PHPGurukul Apartment Visitors Management System bwdates-passreports-details.php sql injection	A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/bwdates-passreports-details.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-2025-47682	WordPress SMS Alert Order Notifications – WooCommerce <= 3.8.2 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Cozy Vision Technologies Pvt. Ltd. SMS Alert Order Notifications – WooCommerce allows SQL Injection.This issue affects SMS Alert Order Notifications – WooCommerce: from n/a through 3.8.2.	Patched by core rule	Y
CVE-2025-4695	PHPGurukul Cyber Cafe Management System add-users.php sql injection	A vulnerability was found in PHPGurukul Cyber Cafe Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /add-users.php. The manipulation of the argument uadd 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-2025-4696	PHPGurukul Cyber Cafe Management System search.php sql injection	A vulnerability was found in PHPGurukul Cyber Cafe 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 /search.php. The manipulation of the argument searchdata leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-4697	PHPGurukul Directory Management System edit-directory.php sql injection	A vulnerability was found in PHPGurukul Directory Management System 2.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/edit-directory.php. The manipulation of the argument editid 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-2025-4698	PHPGurukul Directory Management System forget-password.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Directory Management System 2.0. This affects an unknown part of the file /admin/forget-password.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-2025-4699	PHPGurukul Apartment Visitors Management System visitors-form.php sql injection	A vulnerability classified as critical was found in PHPGurukul Apartment Visitors Management System 1.0. This vulnerability affects unknown code of the file /admin/visitors-form.php. The manipulation of the argument Category leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-4702	PHPGurukul Vehicle Parking Management System add-category.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/add-category.php. The manipulation of the argument catename 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-2025-4703	PHPGurukul Vehicle Parking Management System admin-profile.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/admin-profile.php. The manipulation of the argument contactnumber 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-2025-4704	PHPGurukul Vehicle Parking Management System edit-category.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 /admin/edit-category.php. The manipulation of the argument editid 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-2025-4705	PHPGurukul Vehicle Parking Management System view-incomingvehicle-detail.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 /admin/view-incomingvehicle-detail.php. The manipulation of the argument viewid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-4717	PHPGurukul Company Visitor Management System visitors-form.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Company Visitor Management System 2.0. Affected is an unknown function of the file /visitors-form.php. The manipulation of the argument fullname 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-2025-31637	WordPress SHOUT <= 3.5.3 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup SHOUT allows SQL Injection. This issue affects SHOUT: from	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		n/a through 3.5.3.		
CVE-2025-31640	WordPress Magic Responsive Slider and Carousel WordPress <= 1.4 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup Magic Responsive Slider and Carousel WordPress allows SQL Injection. This issue affects Magic Responsive Slider and Carousel WordPress: from n/a through 1.4.	Patched by core rule	Y
CVE-2025-31641	WordPress UberSlider <= 2.3 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup UberSlider allows SQL Injection. This issue affects UberSlider: from n/a through 2.3.	Patched by core rule	Y
CVE-2025-31926	WordPress Sticky Radio Player <= 3.4 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup Sticky Radio Player allows SQL Injection. This issue affects Sticky Radio Player: from n/a through 3.4.	Patched by core rule	Y
CVE-2025-31928	WordPress Multimedia Responsive Carousel with Image Video Audio Support <= 2.6.0 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup Multimedia Responsive Carousel with Image Video Audio Support allows SQL Injection. This issue affects Multimedia Responsive Carousel with Image Video Audio Support: from n/a through 2.6.0.	Patched by core rule	Y
CVE-2025-32245	WordPress Apollo <= 3.6.3 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup Apollo allows SQL Injection. This issue affects Apollo: from n/a through 3.6.3.	Patched by core rule	Y
CVE-2025-32287	WordPress Responsive HTML5 Audio Player PRO With Playlist <= 3.5.7 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup Responsive HTML5 Audio Player PRO With Playlist allows SQL Injection. This issue affects Responsive HTML5 Audio Player PRO With Playlist: from n/a through 3.5.7.	Patched by core rule	Y
CVE-2025-32290	WordPress Sticky HTML5 Music Player <= 3.1.6 -	Improper Neutralization of Special Elements used in an	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	SQL Injection Vulnerability	SQL Command ('SQL Injection') vulnerability in LambertGroup Sticky HTML5 Music Player allows SQL Injection. This issue affects Sticky HTML5 Music Player: from n/a through 3.1.6.		
CVE-2025-32301	WordPress CountDown Pro WP Plugin <= 2.7 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup CountDown Pro WP Plugin allows SQL Injection. This issue affects CountDown Pro WP Plugin: from n/a through 2.7.	Patched by core rule	Y
CVE-2025-32306	WordPress Radio Player Shoutcast & Icecast WordPress Plugin <= 4.4.6 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup Radio Player Shoutcast & Icecast WordPress Plugin allows Blind SQL Injection. This issue affects Radio Player Shoutcast & Icecast WordPress Plugin: from n/a through 4.4.6.	Patched by core rule	Y
CVE-2025-32307	WordPress Chameleon HTML5 Audio Player With/Without Playlist <= 3.5.6 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup Chameleon HTML5 Audio Player With/Without Playlist allows SQL Injection. This issue affects Chameleon HTML5 Audio Player With/Without Playlist: from n/a through 3.5.6.	Patched by core rule	Y
CVE-2025-32643	WordPress WPGYM Plugin <= 65.0 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in mojoomla WPGYM allows Blind SQL Injection. This issue affects WPGYM: from n/a through 65.0.	Patched by core rule	Y
CVE-2025-39481	WordPress Eventer - WordPress Event & Booking Manager Plugin plugin <= 3.9.6 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in imithemes Eventer allows Blind SQL Injection. This issue affects Eventer: from n/a through 3.9.6.	Patched by core rule	Y
CVE-2025-4736	PHPGurukul Daily Expense Tracker register.php sql injection	A vulnerability was found in PHPGurukul Daily Expense Tracker 1.1 and classified as critical. Affected by this issue is some unknown functionality of the file /register.php. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-4743	code-projects Employee Record System getData.php sql injection	A vulnerability classified as critical was found in code-projects Employee Record System 1.0. Affected by this vulnerability is an unknown functionality of the file /dashboard/getData.php. The manipulation of the argument keywords 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-2025-47567	WordPress Video Player & FullScreen Video Background plugin <= 2.4.1 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup Video Player & FullScreen Video Background allows Blind SQL Injection. This issue affects Video Player & FullScreen Video Background: from n/a through 2.4.1.	Patched by core rule	Y
CVE-2025-4757	PHPGurukul Beauty Parlour Management System forgot-password.php sql injection	A vulnerability was found in PHPGurukul Beauty Parlour Management System 1.1. It has been rated as critical. This issue affects some unknown processing of the file /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-2025-4758	PHPGurukul Beauty Parlour Management System contact.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Beauty Parlour Management System 1.1. Affected is an unknown function of the file /contact.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-2025-4761	PHPGurukul Complaint Management System admin-profile.php sql injection	A vulnerability has been found in PHPGurukul Complaint Management System 2.0 and classified as critical. This vulnerability affects unknown code of the file /admin/admin-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		profile.php. The manipulation of the argument mobilenumber leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-4765	PHPGurukul Zoo Management System contactus.php sql injection	A vulnerability was found in PHPGurukul Zoo Management System 2.1. It has been classified as critical. Affected is an unknown function of the file /admin/contactus.php. The manipulation of the argument mobnum 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-2025-4766	PHPGurukul Zoo Management System profile.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/profile.php. The manipulation of the argument contactnumber 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-2025-4770	PHPGurukul Park Ticketing Management System view-normal-ticket.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Park Ticketing Management System 2.0. This issue affects some unknown processing of the file /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-2025-4771	PHPGurukul Online Course Registration course.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Online Course Registration 3.1. Affected is an unknown function of the file /admin/course.php. The manipulation of the argument coursecode 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-2025-4772	PHPGurukul Online Course Registration department.php sql injection	A vulnerability has been found in PHPGurukul Online Course Registration 3.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/department.php. The manipulation of the argument department 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-2025-4773	PHPGurukul Online Course Registration level.php sql injection	A vulnerability was found in PHPGurukul Online Course Registration 3.1 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/level.php. The manipulation of the argument level 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-2025-4777	PHPGurukul Park Ticketing Management System view-foreigner-ticket.php sql injection	A vulnerability was found in PHPGurukul Park Ticketing Management System 2.0. It has been classified as critical. This affects an unknown part of the file /view-foreigner-ticket.php. The manipulation of the argument viewid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-4778	PHPGurukul Park Ticketing Management System normal-search.php sql injection	A vulnerability was found in PHPGurukul Park Ticketing Management System 2.0. It has been declared as critical. This vulnerability affects unknown code of the file /normal-search.php. The manipulation of the argument searchdata leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-4780	PHPGurukul Park Ticketing Management System foreigner-search.php sql injection	A vulnerability was found in PHPGurukul Park Ticketing Management System 2.0. It has been rated as critical. This issue affects some unknown processing of the file /foreigner-search.php. The manipulation of the argument searchdata leads to sql injection. The attack	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-4781	PHPGurukul Park Ticketing Management System forgot-password.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Park Ticketing Management System 2.0. Affected is an unknown function of the file /forgot-password.php. The manipulation of the argument email/contactno 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-2025-4782	SourceCodester/oretnom23 Stock Management System view_receiving sql injection	A vulnerability has been found in SourceCodester/oretnom23 Stock Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /sms/admin/?page=receiving/view_receiving&id=1. 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-2025-4785	PHPGurukul Daily Expense Tracker System user-profile.php sql injection	A vulnerability was found in PHPGurukul Daily Expense Tracker System 1.1. It has been rated as critical. Affected by this issue is some unknown functionality of the file /user-profile.php. The manipulation of the argument fullname/contactnumber 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-2025-4786	SourceCodester/oretnom23 Stock Management System view_return sql injection	A vulnerability was found in SourceCodester/oretnom23 Stock Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/?page=return/view_return. 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-2025-4787	SourceCodester/oretnom23 Stock Management System view_sale sql	A vulnerability classified as critical has been found in SourceCodester/oretnom23	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	Stock Management System 1.0. Affected is an unknown function of the file /admin/?page=sales/view_sale. 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-2025-4793	PHPGurukul Online Course Registration edit-student-profile.php sql injection	A vulnerability was found in PHPGurukul Online Course Registration 3.1. It has been classified as critical. Affected is an unknown function of the file /edit-student-profile.php. The manipulation of the argument cgpa 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-2025-4794	PHPGurukul Online Course Registration news.php sql injection	A vulnerability was found in PHPGurukul Online Course Registration 3.1. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /news.php. The manipulation of the argument newstitle 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-2025-4806	SourceCodester/oretnom23 Stock Management System view_bo sql injection	A vulnerability, which was classified as critical, has been found in SourceCodester/oretnom23 Stock Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/?page=back_order/view_bo. 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-2025-4808	PHPGurukul Park Ticketing Management System add-normal-ticket.php sql injection	A vulnerability was found in PHPGurukul Park Ticketing Management System 2.0 and classified as critical. This issue affects some unknown processing of the file /add-normal-ticket.php. The manipulation of the argument noadult leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the public and may be used. Other parameters might be affected as well.		
CVE-2025-4812	PHPGurukul Human Metapneumovirus Testing Management System profile.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Human Metapneumovirus Testing Management System 1.0. This issue affects some unknown processing of the file /profile.php. The manipulation of the argument mobilenumber 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-2025-4813	PHPGurukul Human Metapneumovirus Testing Management System edit-phlebotomist.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Human Metapneumovirus Testing Management System 1.0. Affected is an unknown function of the file /edit-phlebotomist.php. The manipulation of the argument mobilenumber 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-2025-48137	WordPress Interview <= 1.01 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in proxymis Interview allows SQL Injection. This issue affects Interview: from n/a through 1.01.	Patched by core rule	Y
CVE-2025-4861	PHPGurukul Beauty Parlour Management System admin-profile.php sql injection	A vulnerability classified as critical was found in PHPGurukul Beauty Parlour Management System 1.1. Affected by this vulnerability is an unknown functionality of the file /admin/admin-profile.php. The manipulation of the argument contactnumber 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-2025-4873	PHPGurukul News Portal Login index.php sql injection	A vulnerability has been found in PHPGurukul News Portal 4.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/index.php of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component Login. 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.		
CVE-2025-4874	PHPGurukul News Portal Project contactus.php sql injection	A vulnerability was found in PHPGurukul News Portal Project 4.1 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/contactus.php. The manipulation of the argument pagetitle 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-2025-4880	PHPGurukul News Portal aboutus.php sql injection	A vulnerability has been found in PHPGurukul News Portal 4.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/aboutus.php. The manipulation of the argument pagetitle 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-2025-32924	WordPress Revy plugin <= 2.1 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in roninwp Revy allows SQL Injection.This issue affects Revy: from n/a through 2.1.	Patched by core rule	Y
CVE-2025-39355	WordPress FAT Services Booking plugin <= 5.6 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in roninwp FAT Services Booking allows SQL Injection.This issue affects FAT Services Booking: from n/a through 5.6.	Patched by core rule	Y
CVE-2025-39357	WordPress Hospital Management System plugin <= 47.0(20-11-2023) - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in mojoomla Hospital Management System allows SQL Injection.This issue affects Hospital Management System: from n/a through 47.0(20-11-2023).	Patched by core rule	Y
CVE-2025-39370	WordPress iCafe Library plugin <= 1.8.3 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Cnilsson iCafe Library allows SQL Injection.This issue affects iCafe Library: from n/a through 1.8.3.		
CVE-2025-39386	WordPress Hospital Management System plugin <= 47.0(20-11-2023) - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in mojoomla Hospital Management System allows SQL Injection.This issue affects Hospital Management System: from n/a through 47.0(20-11-2023).	Patched by core rule	Y
CVE-2025-39389	WordPress AnalyticsWP <= 2.1.2 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Solid Plugins AnalyticsWP allows SQL Injection.This issue affects AnalyticsWP: from n/a through 2.1.2.	Patched by core rule	Y
CVE-2025-39395	WordPress WPAMS plugin <= 44.0 (17-08-2023) - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in mojoomla WPAMS allows SQL Injection.This issue affects WPAMS: from n/a through 44.0 (17-08-2023).	Patched by core rule	Y
CVE-2025-39403	WordPress WPAMS plugin <= 44.0 (17-08-2023) - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in mojoomla WPAMS allows SQL Injection.This issue affects WPAMS: from n/a through 44.0 (17-08-2023).	Patched by core rule	Y
CVE-2025-39445	WordPress Super Store Finder <= 7.2 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in highwarden Super Store Finder allows SQL Injection.This issue affects Super Store Finder: from n/a through 7.2.	Patched by core rule	Y
CVE-2025-43833	WordPress Absolute Links plugin <= 1.1.1 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Amir Helzer Absolute Links allows Blind SQL Injection.This issue affects Absolute Links: from n/a through 1.1.1.	Patched by core rule	Y
CVE-2025-48278	WordPress RSVPMarker <= 11.5.6 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in davidfcarr RSVPMarker allows SQL Injection. This issue affects RSVPMarker :	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		from n/a through 11.5.6.		
CVE-2025-48280	WordPress AutomatorWP <= 5.2.1.3 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ruben Garcia AutomatorWP allows Blind SQL Injection. This issue affects AutomatorWP: from n/a through 5.2.1.3.	Patched by core rule	Y
CVE-2025-4906	PHPGurukul Notice Board System login.php sql injection	A vulnerability was found in PHPGurukul Notice Board System 1.0. It has been classified as critical. Affected is an unknown function of the file /login.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-2025-4907	PHPGurukul Daily Expense Tracker System forgot-password.php sql injection	A vulnerability was found in PHPGurukul Daily Expense Tracker System 1.1. It has been rated 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 launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-4908	PHPGurukul Daily Expense Tracker System expense-datewise-reports-detailed.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Daily Expense Tracker System 1.1. This affects an unknown part of the file /expense-datewise-reports-detailed.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-2025-4910	PHPGurukul Zoo Management System edit-animal-details.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/edit-animal-details.php. The manipulation of the argument aname 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. Other parameters might be affected as well.		
CVE-2025-4911	PHPGurukul Zoo Management System view-foreigner-ticket.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/view-foreigner-ticket.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-2025-4913	PHPGurukul Auto Taxi Stand Management System index.php sql injection	A vulnerability was found in PHPGurukul Auto Taxi Stand Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/index.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.	Patched by core rule	Y
CVE-2025-4914	PHPGurukul Auto Taxi Stand Management System forgot-password.php sql injection	A vulnerability was found in PHPGurukul Auto Taxi Stand Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/forgot-password.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-2025-4915	PHPGurukul Auto Taxi Stand Management System auto-taxi-entry-detail.php sql injection	A vulnerability was found in PHPGurukul Auto Taxi Stand Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/auto-taxi-entry-detail.php. The manipulation of the argument price 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-2025-4916	PHPGurukul Auto Taxi Stand Management System admin-profile.php sql injection	A vulnerability was found in PHPGurukul Auto Taxi Stand Management System 1.0. It has been rated as critical. 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 /admin/admin-profile.php. The manipulation of the argument mobilenumber 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-2025-4917	PHPGurukul Auto Taxi Stand Management System new-autoortaxi-entry-form.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Auto Taxi Stand Management System 1.0. Affected is an unknown function of the file /admin/new-autoortaxi-entry-form.php. The manipulation of the argument drivername 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-2025-4925	PHPGurukul Daily Expense Tracker System expense-monthwise-reports-detailed.php sql injection	A vulnerability has been found in PHPGurukul Daily Expense Tracker System 1.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /expense-monthwise-reports-detailed.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-2025-4927	PHPGurukul Online Marriage Registration System between-dates-application-report.php sql injection	A vulnerability was found in PHPGurukul Online Marriage Registration System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/between-dates-application-report.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-2025-4934	PHPGurukul User Registration & Login and User Management System edit-profile.php sql injection	A vulnerability has been found in PHPGurukul User Registration & Login and User Management System 3.3 and classified 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 /edit-profile.php. The manipulation of the argument Contact leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-4937	SourceCodester Apartment Visitor Management System profile.php sql injection	A vulnerability was found in SourceCodester Apartment Visitor Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /profile.php. The manipulation of the argument mobilenumber 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-2025-4938	PHPGurukul Employee Record Management System registererms.php sql injection	A vulnerability was found in PHPGurukul Employee Record Management System 1.3. It has been rated as critical. Affected by this issue is some unknown functionality of the file /registererms.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-2025-4941	PHPGurukul Credit Card Application Management System index.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Credit Card Application 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-2025-31056	WordPress WhatsCart plugin <= 1.1.0 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Techspawn WhatsCart - Whatsapp Abandoned Cart Recovery, Order Notifications, Chat Box, OTP for WooCommerce allows SQL Injection. This issue affects WhatsCart -	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Whatsapp Abandoned Cart Recovery, Order Notifications, Chat Box, OTP for WooCommerce: from n/a through 1.1.0.		
CVE-2025-31397	WordPress Bus Ticket Booking with Seat Reservation for WooCommerce plugin <= 1.7 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in smartcms Bus Ticket Booking with Seat Reservation for WooCommerce allows SQL Injection. This issue affects Bus Ticket Booking with Seat Reservation for WooCommerce: from n/a through 1.7.	Patched by core rule	Y
CVE-2025-31914	WordPress Pixel WordPress Form BuilderPlugin & Autoresponder <= 1.0.2 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in kamleshyadav Pixel WordPress Form BuilderPlugin & Autoresponder allows Blind SQL Injection. This issue affects Pixel WordPress Form BuilderPlugin & Autoresponder: from n/a through 1.0.2.	Patched by core rule	Y
CVE-2025-39501	WordPress Goodlayers Hostel Plugin <= 3.1.2 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in GoodLayers Goodlayers Hostel allows Blind SQL Injection. This issue affects Goodlayers Hostel: from n/a through 3.1.2.	Patched by core rule	Y
CVE-2025-39504	WordPress Goodlayers Hotel plugin <= 3.1.4 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in GoodLayers Goodlayers Hotel allows Blind SQL Injection. This issue affects Goodlayers Hotel: from n/a through 3.1.4.	Patched by core rule	Y
CVE-2025-46455	WordPress WP HRM LITE <= 1.1 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in IndigoThemes WP HRM LITE allows SQL Injection. This issue affects WP HRM LITE: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-46460	WordPress Easy Guide <= 1.0.0 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Detheme Easy Guide allows SQL Injection. This issue affects Easy Guide: from n/a through 1.0.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-46463	WordPress Mailing Group Listserv <= 3.0.4 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Yamna Khawaja Mailing Group Listserv allows SQL Injection. This issue affects Mailing Group Listserv: from n/a through 3.0.4.	Patched by core rule	Y
CVE-2025-46539	WordPress Fable Extra <= 1.0.6 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPFable Fable Extra allows Blind SQL Injection. This issue affects Fable Extra: from n/a through 1.0.6.	Patched by core rule	Y
CVE-2025-47478	WordPress ProfileGrid <= 5.9.5.0 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Metagauss ProfileGrid allows SQL Injection. This issue affects ProfileGrid : from n/a through 5.9.5.0.	Patched by core rule	Y
CVE-2025-47575	WordPress School Management plugin <= 92.0.0 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in mojoomla School Management allows SQL Injection. This issue affects School Management: from n/a through 92.0.0.	Patched by core rule	Y
CVE-2025-47599	WordPress Facturante <= 1.11 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in facturante Facturante allows SQL Injection. This issue affects Facturante: from n/a through 1.11.	Patched by core rule	Y
CVE-2025-47640	WordPress Printcart Web to Print Product Designer for WooCommerce <= 2.3.8 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in printcart Printcart Web to Print Product Designer for WooCommerce allows SQL Injection. This issue affects Printcart Web to Print Product Designer for WooCommerce: from n/a through 2.3.8.	Patched by core rule	Y
CVE-2025-47671	WordPress Binary MLM Plan <= 3.0 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LETSCMS MLM Software Binary MLM Plan allows SQL Injection. This issue affects Binary MLM Plan: from n/a through 3.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-48283	WordPress Majestic Support <= 1.1.0 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Majestic Support Majestic Support allows SQL Injection. This issue affects Majestic Support: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-48735		A SQL Injection issue in the request body processing in BOS IPCs with firmware 21.45.8.2.2_220219 before 21.45.8.2.3_230220 allows remote attackers to obtain sensitive information from the database via crafted input in the request body.	Patched by core rule	Y
CVE-2025-5152	Chanjet CRM newActivityedit.php sql injection	A vulnerability classified as critical was found in Chanjet CRM up to 20250510. This vulnerability affects unknown code of the file /activity/newActivityedit.php?DontCheckLogin=1&id=null&ret=mod1. The manipulation of the argument gblOrgID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-5155	qianfox FoxCMS Article.php batchCope sql injection	A vulnerability has been found in qianfox FoxCMS 1.2.5 and classified as critical. Affected by this vulnerability is the function batchCope of the file app/admin/controller/Article.php. The manipulation of the argument ids 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

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-3969	codeprojects News Publishing Site Dashboard Edit Category Page edit-category.php unrestricted upload	A vulnerability was found in codeprojects News Publishing Site Dashboard 1.0. It has been rated as critical. This issue affects some unknown processing of the file /edit-category.php of the component Edit Category Page. The manipulation of the argument category_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	N
CVE-2025-4258	zhangyanbo2007 youkefu MediaController.java upload unrestricted upload	A vulnerability, which was classified as critical, was found in zhangyanbo2007 youkefu up to 4.2.0. Affected is the function Upload of the file \youkefu-master\src\main\java\com\ukefu\webim\web\handler\resource\MediaController.java. The manipulation of the argument imgFile 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	N
CVE-2025-4259	newbee-mall UploadController.java upload unrestricted upload	A vulnerability has been found in newbee-mall 1.0 and classified as critical. Affected by this vulnerability is the function Upload of the file ltd/newbee/mall/controller/common/UploadController.java. The manipulation of the argument File leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.	Patched by core rule	N
CVE-2025-4305	kefaming mayi File.php upload unrestricted upload	A vulnerability has been found in kefaming mayi up to 1.3.9 and classified as critical. This vulnerability affects the function Upload of the file app/tools/controller/File.php. The manipulation of the argument File leads to unrestricted upload. The attack can be initiated	Patched by core rule	N

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-2025-47549	WordPress BEAF <= 4.6.10 - Arbitrary File Upload Vulnerability	Unrestricted Upload of File with Dangerous Type vulnerability in Themefic BEAF allows Upload a Web Shell to a Web Server. This issue affects BEAF: from n/a through 4.6.10.	Patched by core rule	N
CVE-2025-47550	WordPress Instantio <= 3.3.16 - Arbitrary File Upload Vulnerability	Unrestricted Upload of File with Dangerous Type vulnerability in Themefic Instantio allows Upload a Web Shell to a Web Server. This issue affects Instantio: from n/a through 3.3.16.	Patched by core rule	N
CVE-2025-4468	SourceCodester Online Student Clearance System edit-photo.php unrestricted upload	A vulnerability was found in SourceCodester Online Student Clearance System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /edit-photo.php. The manipulation of the argument userImage 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	N
CVE-2025-4538	kkFileView fileUpload unrestricted upload	A vulnerability was found in kkFileView 4.4.0. It has been classified as critical. This affects an unknown part of the file /fileUpload. The manipulation of the argument File 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 vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	N
CVE-2025-26872	WordPress Eximius theme <= 2.2 - Arbitrary File Upload vulnerability	Unrestricted Upload of File with Dangerous Type vulnerability in dkszone Eximius allows Using Malicious Files.This issue affects Eximius: from n/a through 2.2.	Patched by core rule	N
CVE-2025-26892	WordPress Celestial Aura plugin <= 2.2 - Arbitrary File Upload vulnerability	Unrestricted Upload of File with Dangerous Type vulnerability in dkszone Celestial Aura allows Using Malicious Files.This issue affects Celestial Aura: from n/a through 2.2.	Patched by core rule	N
CVE-2025-39380	WordPress Hospital Management System plugin <= 47.0(20-11-2023) - Arbitrary File	Unrestricted Upload of File with Dangerous Type vulnerability in mojoomla Hospital Management	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Upload vulnerability	System allows Upload a Web Shell to a Web Server.This issue affects Hospital Management System: from n/a through 47.0(20-11-2023).		
CVE-2025-39401	WordPress WPAMS plugin <= 44.0 (17-08-2023) - Arbitrary File Upload vulnerability	Unrestricted Upload of File with Dangerous Type vulnerability in mojoomla WPAMS allows Upload a Web Shell to a Web Server.This issue affects WPAMS: from n/a through 44.0 (17-08-2023).	Patched by core rule	N
CVE-2025-39402	WordPress WPAMS plugin <= 44.0 (17-08-2023) - Arbitrary File Upload vulnerability	Unrestricted Upload of File with Dangerous Type vulnerability in mojoomla WPAMS allows Upload a Web Shell to a Web Server.This issue affects WPAMS: from n/a through 44.0 (17-08-2023).	Patched by core rule	N
CVE-2025-47577	WordPress TI WooCommerce Wishlist <= 2.9.2 - Arbitrary File Upload Vulnerability	Unrestricted Upload of File with Dangerous Type vulnerability in TemplateInvaders TI WooCommerce Wishlist allows Upload a Web Shell to a Web Server.This issue affects TI WooCommerce Wishlist: from n/a through 2.9.2.	Patched by core rule	N
CVE-2025-4926	PHPGurukul Car Rental Project post-avehical.php unrestricted upload	A vulnerability was found in PHPGurukul Car Rental Project 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/post-avehical.php. The manipulation of the argument img1/img2/img3/img4/img5 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	N
CVE-2025-31916	WordPress JP Students Result Management System Premium plugin 1.1.7 - Arbitrary File Upload vulnerability	Unrestricted Upload of File with Dangerous Type vulnerability in joy2012bd JP Students Result Management System Premium allows Upload a Web Shell to a Web Server. This issue affects JP Students Result Management System Premium: from 1.1.7 through n/a.	Patched by core rule	N
CVE-2025-46490	WordPress Crossword Compiler Puzzles <= 5.2 - Arbitrary File Upload Vulnerability	Unrestricted Upload of File with Dangerous Type vulnerability in wordwebsoftware Crossword Compiler Puzzles allows Upload a Web Shell to	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		a Web Server. This issue affects Crossword Compiler Puzzles: from n/a through 5.2.		
CVE-2025-47637	WordPress STAGGS <= 2.11.0 - Arbitrary File Upload Vulnerability	Unrestricted Upload of File with Dangerous Type vulnerability in STAGGS STAGGS allows Upload a Web Shell to a Web Server. This issue affects STAGGS: from n/a through 2.11.0.	Patched by core rule	N
CVE-2025-47641	WordPress Printcart Web to Print Product Designer for WooCommerce <= 2.3.8 - Arbitrary File Upload Vulnerability	Unrestricted Upload of File with Dangerous Type vulnerability in printcart Printcart Web to Print Product Designer for WooCommerce allows Upload a Web Shell to a Web Server. This issue affects Printcart Web to Print Product Designer for WooCommerce: from n/a through 2.3.8.	Patched by core rule	N
CVE-2025-47642	WordPress Ajar in5 Embed <= 3.1.5 - Arbitrary File Upload Vulnerability	Unrestricted Upload of File with Dangerous Type vulnerability in Ajar Productions Ajar in5 Embed allows Upload a Web Shell to a Web Server. This issue affects Ajar in5 Embed: from n/a through 3.1.5.	Patched by core rule	N
CVE-2025-47658	WordPress ELEX WordPress HelpDesk & Customer Ticketing System <= 3.2.7 - Arbitrary File Upload Vulnerability	Unrestricted Upload of File with Dangerous Type vulnerability in ELEXtensions ELEX WordPress HelpDesk & Customer Ticketing System allows Upload a Web Shell to a Web Server. This issue affects ELEX WordPress HelpDesk & Customer Ticketing System: from n/a through 3.2.7.	Patched by core rule	N
CVE-2025-47663	WordPress Hospital Management System plugin <= 47.0(20-11-2023) - Arbitrary File Upload vulnerability	Unrestricted Upload of File with Dangerous Type vulnerability in mojoomla Hospital Management System allows Upload a Web Shell to a Web Server. This issue affects Hospital Management System: from 47.0(20 through 11.	Patched by core rule	N
CVE-2025-47687	WordPress StoreKeeper for WooCommerce <= 14.4.4 - Arbitrary File Upload Vulnerability	Unrestricted Upload of File with Dangerous Type vulnerability in StoreKeeper B.V. StoreKeeper for WooCommerce allows Upload a Web Shell to a Web Server. This issue affects StoreKeeper for WooCommerce: from n/a through 14.4.4.	Patched by core rule	N
CVE-2025-5108	zongzhige ShopXO ZIP File Payment.php Upload unrestricted upload	A vulnerability was found in zongzhige ShopXO 6.5.0. It has been rated as critical.	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This issue affects the function Upload of the file app/admin/controller/Payment.php of the component ZIP File Handler. The manipulation of the argument params 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.		
CVE-2025-48741		A Broken Access Control vulnerability in StrangeBee TheHive 5.2.0 before 5.2.16, 5.3.0 before 5.3.11, and 5.4.0 before 5.4.10 allows remote, authenticated, and unprivileged users to retrieve alerts, cases, logs, observables, or tasks, regardless of the user's permissions, through a specific API endpoint.	Patched by core rule	N
CVE-2025-46652		In IZArc through 4.5, there is a Mark-of-the-Web Bypass Vulnerability. When a user performs an extraction from an archive file that bears Mark-of-the-Web, Mark-of-the-Web is not propagated to the extracted files.	Patched by core rule	N

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-3958	withstars Books-Management-System Book Edit Page book_edit_do.html cross site scripting	A vulnerability was found in withstars Books-Management-System 1.0. It has been classified as problematic. Affected is an unknown function of the file /book_edit_do.html of the component Book Edit Page. The manipulation of the argument 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. Other parameters might be affected as well. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-3961	withstars Books-Management-System do cross site scripting	A vulnerability classified as problematic has been found in withstars Books-Management-System 1.0. This affects an unknown part of the file /admin/article/add/do. The manipulation of the argument Title 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. Other parameters might be affected as well. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-3962	withstars Books-Management-System Comment add cross site scripting	A vulnerability classified as problematic was found in withstars Books-Management-System 1.0. This vulnerability affects unknown code of the file /api/comment/add of the component Comment Handler. The manipulation of the argument content leads to cross site scripting. The attack can 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-2025-3965	itwanger paicoding post cross site scripting	A vulnerability has been found in itwanger paicoding 1.0.3 and classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		problematic. Affected by this vulnerability is an unknown functionality of the file /article/app/post. The manipulation of the argument content leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-3970	baseweb JSite save cross site scripting	A vulnerability classified as problematic has been found in baseweb JSite up to 1.0. Affected is an unknown function of the file /sys/office/save. The manipulation of the argument Remarks 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-2025-46657		Karaz Karazal through 2025-04-14 allows reflected XSS via the lang parameter to the default URI.	Patched by core rule	Y
CVE-2025-39363	WordPress Custom Login and Registration <= 1.0.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AlphaEfficiencyTeam Custom Login and Registration allows Stored XSS.This issue affects Custom Login and Registration: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-39361	WordPress Royal Elementor Addons plugin <= 1.7.1017 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WProyal Royal Elementor Addons allows Stored XSS.This issue affects Royal Elementor Addons: from n/a through 1.7.1017.	Patched by core rule	Y
CVE-2025-47441	WordPress Progress Bar <= 2.2.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chris Reynolds Progress Bar allows Stored XSS. This issue affects Progress Bar: from n/a through 2.2.3.	Patched by core rule	Y
CVE-2025-47442	WordPress CC BMI Calculator <= 2.1.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CC CC BMI Calculator allows Stored XSS. This issue affects CC BMI Calculator: from n/a through 2.1.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-47443	WordPress Widget Countdown <= 2.7.4 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpdevart Widget Countdown allows Stored XSS. This issue affects Widget Countdown: from n/a through 2.7.4.	Patched by core rule	Y
CVE-2025-47449	WordPress Meow Gallery <= 5.2.7 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jordy Meow Meow Gallery allows Stored XSS. This issue affects Meow Gallery: from n/a through 5.2.7.	Patched by core rule	Y
CVE-2025-47475	WordPress JupiterX Core <= 4.8.11 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in artbees JupiterX Core allows Stored XSS. This issue affects JupiterX Core: from n/a through 4.8.11.	Patched by core rule	Y
CVE-2025-47476	WordPress Cost Calculator for Elementor <= 1.3.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in add-ons.org Cost Calculator for Elementor allows DOM-Based XSS. This issue affects Cost Calculator for Elementor: from n/a through 1.3.3.	Patched by core rule	Y
CVE-2025-47482	WordPress SKT Skill Bar <= 2.4 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sonalsinha21 SKT Skill Bar allows Stored XSS. This issue affects SKT Skill Bar: from n/a through 2.4.	Patched by core rule	Y
CVE-2025-47488	WordPress Bold Page Builder <= 5.3.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in boldthemes Bold Page Builder allows DOM-Based XSS. This issue affects Bold Page Builder: from n/a through 5.3.2.	Patched by core rule	Y
CVE-2025-47489	WordPress Beds24 Online Booking <= 2.0.29 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in markkinchin Beds24 Online Booking allows Stored XSS. This issue affects Beds24 Online Booking: from n/a through 2.0.29.	Patched by core rule	Y
CVE-2025-47493	WordPress Ultimate Blocks <= 3.2.9 - Cross	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Site Scripting (XSS) Vulnerability	Generation ('Cross-site Scripting') vulnerability in Ultimate Blocks Ultimate Blocks allows DOM-Based XSS. This issue affects Ultimate Blocks: from n/a through 3.2.9.		
CVE-2025-47495	WordPress Blockspare <= 3.2.9 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Blockspare Blockspare allows Stored XSS. This issue affects Blockspare: from n/a through 3.2.9.	Patched by core rule	Y
CVE-2025-47497	WordPress Logo Showcase <= 3.0.4 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themepoints Logo Showcase allows DOM-Based XSS. This issue affects Logo Showcase: from n/a through 3.0.4.	Patched by core rule	Y
CVE-2025-47499	WordPress Simple Blog Stats <= 20250416 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeff Starr Simple Blog Stats allows Stored XSS. This issue affects Simple Blog Stats: from n/a through 20250416.	Patched by core rule	Y
CVE-2025-47501	WordPress Content Control <= 2.6.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Code Atlantic Content Control allows DOM-Based XSS. This issue affects Content Control: from n/a through 2.6.1.	Patched by core rule	Y
CVE-2025-47502	WordPress Mollie Forms <= 2.7.12 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nick Mollie Forms allows Stored XSS. This issue affects Mollie Forms: from n/a through 2.7.12.	Patched by core rule	Y
CVE-2025-47503	WordPress NGG Smart Image Search <= 3.3.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpo-HR NGG Smart Image Search allows Stored XSS. This issue affects NGG Smart Image Search: from n/a through 3.3.3.	Patched by core rule	Y
CVE-2025-47504	WordPress Custom Checkout Fields for WooCommerce <= 1.8.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Custom Checkout Fields for WooCommerce allows Stored XSS. This issue	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects Custom Checkout Fields for WooCommerce: from n/a through 1.8.3.		
CVE-2025-47505	WordPress Product Time Countdown for WooCommerce <= 1.6.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ProWCPlugins Product Time Countdown for WooCommerce allows Stored XSS. This issue affects Product Time Countdown for WooCommerce: from n/a through 1.6.2.	Patched by core rule	Y
CVE-2025-47506	WordPress Contextual Related Posts <= 4.0.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ajay Contextual Related Posts allows DOM-Based XSS. This issue affects Contextual Related Posts: from n/a through 4.0.2.	Patched by core rule	Y
CVE-2025-47507	WordPress Better Search <= 4.1.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ajay Better Search allows DOM-Based XSS. This issue affects Better Search: from n/a through 4.1.0.	Patched by core rule	Y
CVE-2025-47509	WordPress Top 10 <= 4.1.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ajay Top 10 allows Stored XSS. This issue affects Top 10: from n/a through 4.1.0.	Patched by core rule	Y
CVE-2025-47515	WordPress WP DPE-GES <= 1.6 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Seb WP DPE-GES allows DOM-Based XSS. This issue affects WP DPE-GES: from n/a through 1.6.	Patched by core rule	Y
CVE-2025-47516	WordPress Time Clock <= 1.2.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Scott Paterson Time Clock allows Stored XSS. This issue affects Time Clock: from n/a through 1.2.3.	Patched by core rule	Y
CVE-2025-47518	WordPress Contact Form 7 – PayPal & Stripe Add-on <= 2.3.4 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Scott Paterson Contact Form 7 – PayPal & Stripe Add-on allows Stored XSS. This issue affects Contact Form 7 – PayPal & Stripe Add-on: from n/a through 2.3.4.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-47520	WordPress Charitable <= 1.8.5.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Syed Balkhi Charitable allows Stored XSS. This issue affects Charitable: from n/a through 1.8.5.1.	Patched by core rule	Y
CVE-2025-47521	WordPress Robo Gallery <= 5.0.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in robosoft Robo Gallery allows Stored XSS. This issue affects Robo Gallery: from n/a through 5.0.2.	Patched by core rule	Y
CVE-2025-47522	WordPress AWEOS WP Lock <= 1.4.8 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AWEOS GmbH AWEOS WP Lock allows Stored XSS. This issue affects AWEOS WP Lock: from n/a through 1.4.8.	Patched by core rule	Y
CVE-2025-47524	WordPress Quran multilanguage Text & Audio <= 2.3.23 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in karim42 Quran multilanguage Text & Audio allows Stored XSS. This issue affects Quran multilanguage Text & Audio: from n/a through 2.3.23.	Patched by core rule	Y
CVE-2025-47525	WordPress Bold Page Builder <= 5.3.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in boldthemes Bold Page Builder allows Stored XSS. This issue affects Bold Page Builder: from n/a through 5.3.0.	Patched by core rule	Y
CVE-2025-47547	WordPress SendPulse Email Marketing Newsletter <= 2.1.6 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SendPulse SendPulse Email Marketing Newsletter allows Stored XSS. This issue affects SendPulse Email Marketing Newsletter: from n/a through 2.1.6.	Patched by core rule	Y
CVE-2025-47589	WordPress Ebook Store <= 5.8007 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in motov.net Ebook Store allows DOM-Based XSS. This issue affects Ebook Store: from n/a through 5.8007.	Patched by core rule	Y
CVE-2025-47592	WordPress Legal Terms	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	and Conditions Popup for User Login and WooCommerce Checkout – TPUL <= 2.0.3 - Cross Site Scripting (XSS) Vulnerability	Input During Web Page Generation ('Cross-site Scripting') vulnerability in Lehel Mátyus Legal Terms and Conditions Popup for User Login and WooCommerce Checkout – TPUL allows Stored XSS. This issue affects Legal Terms and Conditions Popup for User Login and WooCommerce Checkout – TPUL: from n/a through 2.0.3.	rule	
CVE-2025-47593	WordPress Really Simple Under Construction Page <= 1.4.6 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jonas Hjalmarsson Really Simple Under Construction Page allows Stored XSS. This issue affects Really Simple Under Construction Page: from n/a through 1.4.6.	Patched by core rule	Y
CVE-2025-47595	WordPress Color Your Bar <= 2.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Darshan Saroya Color Your Bar allows Stored XSS. This issue affects Color Your Bar: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-47604	WordPress Inline Related Posts <= 3.8.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Data443 Risk Migitation, Inc. Inline Related Posts allows Stored XSS. This issue affects Inline Related Posts: from n/a through 3.8.0.	Patched by core rule	Y
CVE-2025-47605	WordPress WP jQuery DataTable <= 4.1.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AppJetty WP jQuery DataTable allows Stored XSS. This issue affects WP jQuery DataTable: from n/a through 4.1.0.	Patched by core rule	Y
CVE-2025-47607	WordPress Show All Comments <= 7.0.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AppJetty Show All Comments allows Stored XSS. This issue affects Show All Comments: from n/a through 7.0.1.	Patched by core rule	Y
CVE-2025-47615	WordPress Amazon Product in a Post <= 5.2.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in flowdee Amazon Product in a Post allows Stored XSS.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This issue affects Amazon Product in a Post: from n/a through 5.2.2.		
CVE-2025-47616	WordPress aBlocks <= 1.9.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tushar Imran aBlocks allows Stored XSS. This issue affects aBlocks: from n/a through 1.9.1.	Patched by core rule	Y
CVE-2025-47617	WordPress WP Front User Submit / Front Editor <= 4.9.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in aharonyan WP Front User Submit / Front Editor allows Stored XSS. This issue affects WP Front User Submit / Front Editor: from n/a through 4.9.3.	Patched by core rule	Y
CVE-2025-47621	WordPress Meks Flexible Shortcodes <= 1.3.6 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Meks Meks Flexible Shortcodes allows Stored XSS. This issue affects Meks Flexible Shortcodes: from n/a through 1.3.6.	Patched by core rule	Y
CVE-2025-47622	WordPress Email Notification on Login <= 1.6.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in apasionados Email Notification on Login allows Stored XSS. This issue affects Email Notification on Login: from n/a through 1.6.1.	Patched by core rule	Y
CVE-2025-47623	WordPress Easy PayPal Buy Now Button <= 2.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Scott Paterson Easy PayPal Buy Now Button allows Stored XSS. This issue affects Easy PayPal Buy Now Button: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-47625	WordPress DoFollow Case by Case <= 3.5.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in apasionados DoFollow Case by Case allows Stored XSS. This issue affects DoFollow Case by Case: from n/a through 3.5.1.	Patched by core rule	Y
CVE-2025-47626	WordPress Submission DOM tracking for Contact Form 7 <= 2.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in apasionados Submission DOM tracking for Contact	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Form 7 allows Stored XSS. This issue affects Submission DOM tracking for Contact Form 7: from n/a through 2.0.		
CVE-2025-47630	WordPress Ajax Load More <= 7.3.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Darren Cooney Ajax Load More allows Stored XSS. This issue affects Ajax Load More: from n/a through 7.3.1.	Patched by core rule	Y
CVE-2025-47632	WordPress Awesome Gallery <= 1.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Raihanul Islam Awesome Gallery allows Stored XSS. This issue affects Awesome Gallery: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-47638	WordPress WP Discord Invite <= 2.5.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sarvesh M Rao WP Discord Invite allows Stored XSS. This issue affects WP Discord Invite: from n/a through 2.5.3.	Patched by core rule	Y
CVE-2025-47656	WordPress Spiraclethemes Site Library <= 1.4.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in spiraclethemes Spiraclethemes Site Library allows Stored XSS. This issue affects Spiraclethemes Site Library: from n/a through 1.4.0.	Patched by core rule	Y
CVE-2025-47659	WordPress WPBakery Visual Composer WHMCS Elements <= 1.0.4.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in voidcoders WPBakery Visual Composer WHMCS Elements allows Stored XSS. This issue affects WPBakery Visual Composer WHMCS Elements: from n/a through 1.0.4.1.	Patched by core rule	Y
CVE-2025-47662	WordPress Woobox <= 1.6 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in woobox Woobox allows Stored XSS. This issue affects Woobox: from n/a through 1.6.	Patched by core rule	Y
CVE-2025-47665	WordPress N360 | Splash Screen <= 1.0.6 - Cross Site Scripting (XSS)	Improper Neutralization of Input During Web Page Generation ('Cross-site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Vulnerability	Scripting') vulnerability in bistromatic N360 | Splash Screen allows Stored XSS. This issue affects N360 | Splash Screen: from n/a through 1.0.6.		
CVE-2025-47668	WordPress CookieCode <= 2.4.4 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cookiecode CookieCode allows Stored XSS. This issue affects CookieCode: from n/a through 2.4.4.	Patched by core rule	Y
CVE-2025-47669	WordPress CBX Map for Google Map & OpenStreetMap <= 1.1.12 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sabuj Kundu CBX Map for Google Map & OpenStreetMap allows DOM-Based XSS. This issue affects CBX Map for Google Map & OpenStreetMap: from n/a through 1.1.12.	Patched by core rule	Y
CVE-2025-47675	WordPress Woobox <= 1.6 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in woobox Woobox allows DOM-Based XSS. This issue affects Woobox: from n/a through 1.6.	Patched by core rule	Y
CVE-2025-47676	WordPress User Login History <= 2.1.6 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Faiyaz Alam User Login History allows Stored XSS. This issue affects User Login History: from n/a through 2.1.6.	Patched by core rule	Y
CVE-2025-47677	WordPress Photo Gallery - GT3 Image Gallery & Gutenberg Block Gallery <= 2.7.7.25 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gt3themes Photo Gallery - GT3 Image Gallery & Gutenberg Block Gallery allows Stored XSS. This issue affects Photo Gallery - GT3 Image Gallery & Gutenberg Block Gallery: from n/a through 2.7.7.25.	Patched by core rule	Y
CVE-2025-47679	WordPress RS WP Book Showcase <= 6.7.40 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RS WP THEMES RS WP Book Showcase allows DOM-Based XSS. This issue affects RS WP Book Showcase: from n/a through 6.7.40.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-47686	WordPress DELUCKS SEO <= 2.5.9 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DELUCKS DELUCKS SEO allows Stored XSS. This issue affects DELUCKS SEO: from n/a through 2.5.9.	Patched by core rule	Y
CVE-2025-4434	Remote Images Grabber <= 0.6 - Reflected Cross-Site Scripting	The Remote Images Grabber plugin for WordPress is vulnerable to Reflected Cross-Site Scripting in all versions up to, and including, 0.6 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-2025-4469	SourceCodester Online Student Clearance System add-admin.php cross site scripting	A vulnerability classified as problematic has been found in SourceCodester Online Student Clearance System 1.0. Affected is an unknown function of the file /admin/add-admin.php. 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.	Patched by core rule	Y
CVE-2025-4470	SourceCodester Online Student Clearance System add-student.php cross site scripting	A vulnerability classified as problematic was found in SourceCodester Online Student Clearance System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/add-student.php. The manipulation of the argument Fullname 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
CVE-2025-4547	SourceCodester Web-based Pharmacy Product Management System Add User Page cross site scripting	A vulnerability was found in SourceCodester Web-based Pharmacy Product Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Add User Page. The manipulation leads to cross site scripting. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack may be launched remotely. The exploit has been disclosed to the public and may be used. Multiple parameters might be affected.		
CVE-2025-47578	WordPress BNS Twitter Follow Button plugin <= 0.3.8 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Edward Caissie BNS Twitter Follow Button allows DOM-Based XSS.This issue affects BNS Twitter Follow Button: from n/a through 0.3.8.	Patched by core rule	Y
CVE-2025-47777	5ire Client Vulnerable to Cross-Site Scripting (XSS) and Remote Code Execution (RCE)	5ire is a cross-platform desktop artificial intelligence assistant and model context protocol client. Versions prior to 0.11.1 are vulnerable to stored cross-site scripting in chatbot responses due to insufficient sanitization. This, in turn, can lead to Remote Code Execution (RCE) via unsafe Electron protocol handling and exposed Electron APIs. All users of 5ire client versions prior to patched releases, particularly those interacting with untrusted chatbots or pasting external content, are affected. Version 0.11.1 contains a patch for the issue.	Patched by core rule	Y
CVE-2025-39509	WordPress TNC FlipBook plugin <= 12.1.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeNcode TNC FlipBook allows Stored XSS. This issue affects TNC FlipBook: from n/a through 12.1.0.	Patched by core rule	Y
CVE-2025-46464	WordPress Ads Pro plugin <= 4.88 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in scripteo Ads Pro Plugin allows Stored XSS. This issue affects Ads Pro Plugin: from n/a through 4.88.	Patched by core rule	Y
CVE-2025-4744	code-projects Employee Record System edit_employee.php cross site scripting	A vulnerability, which was classified as problematic, has been found in code-projects Employee Record System 1.0. Affected by this issue is some unknown functionality of the file dashboard\edit_employee.php. The manipulation of the argument employeed_id/first_name/middle_name/last_name leads to cross site scripting. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-4745	code-projects Employee Record System current_employees.php cross site scripting	A vulnerability, which was classified as problematic, was found in code-projects Employee Record System 1.0. This affects an unknown part of the file current_employees.php. The manipulation of the argument employeed_id/first_name/middle_name/last_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-2025-47557	WordPress MapSVG plugin <= 8.5.31 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RomanCode MapSVG allows Stored XSS. This issue affects MapSVG: from n/a through 8.5.31.	Patched by core rule	Y
CVE-2025-48080	WordPress Uncanny Toolkit for LearnDash <= 3.7.0.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Uncanny Owl Uncanny Toolkit for LearnDash allows Stored XSS. This issue affects Uncanny Toolkit for LearnDash: from n/a through 3.7.0.2.	Patched by core rule	Y
CVE-2025-48112	WordPress Dot html,php,xml etc pages plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in karimmughal Dot html,php,xml etc pages allows Reflected XSS. This issue affects Dot html,php,xml etc pages: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-48113	WordPress Broadstreet <= 1.51.8 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Broadstreet Broadstreet allows Stored XSS. This issue affects Broadstreet: from n/a through 1.51.8.	Patched by core rule	Y
CVE-2025-48121	WordPress WP Notes Widget <= 1.0.6 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Steve Puddick WP Notes Widget allows DOM-Based XSS. This issue affects WP Notes Widget: from n/a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		through 1.0.6.		
CVE-2025-48131	WordPress UltraAddons Elementor Lite <= 2.0.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Saiful Islam UltraAddons Elementor Lite allows Stored XSS. This issue affects UltraAddons Elementor Lite: from n/a through 2.0.0.	Patched by core rule	Y
CVE-2025-48132	WordPress X Addons for Elementor <= 1.0.14 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pencilwp X Addons for Elementor allows Stored XSS. This issue affects X Addons for Elementor: from n/a through 1.0.14.	Patched by core rule	Y
CVE-2025-48135	WordPress Aptivada for WP <= 2.0.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in aptivadadev Aptivada for WP allows DOM-Based XSS. This issue affects Aptivada for WP: from n/a through 2.0.0.	Patched by core rule	Y
CVE-2025-4862	PHPGurukul Directory Management System searchdata.php cross site scripting	A vulnerability, which was classified as problematic, has been found in PHPGurukul Directory Management System 2.0. Affected by this issue is some unknown functionality of the file /searchdata.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-2025-22678	WordPress my white theme <= 2.0.8 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mythemes my white allows Reflected XSS.This issue affects my white: from n/a through 2.0.8.	Patched by core rule	Y
CVE-2025-22687	WordPress tuaug4 theme <= 1.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Asmedia Tuaug4 allows Reflected XSS.This issue affects Tuaug4: from n/a through 1.4.	Patched by core rule	Y
CVE-2025-22789	WordPress polka dots theme <= 1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		fyrewurks polka dots allows Reflected XSS.This issue affects polka dots: from n/a through 1.2.		
CVE-2025-22790	WordPress moseter theme <= 1.3.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in asmedia allows Reflected XSS.This issue affects moseter: from n/a through 1.3.1.	Patched by core rule	Y
CVE-2025-22791	WordPress offset writing theme <= 1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in twh offset writing allows Reflected XSS.This issue affects offset writing: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-22792	WordPress Js O3 Lite theme <= 1.5.8.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jinwen Js O3 Lite allows Reflected XSS.This issue affects Js O3 Lite: from n/a through 1.5.8.2.	Patched by core rule	Y
CVE-2025-23979	WordPress Flashy theme <= 1.2.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in duwasai Flashy allows Reflected XSS.This issue affects Flashy: from n/a through 1.2.1.	Patched by core rule	Y
CVE-2025-23981	WordPress CarZine theme <= 1.4.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Takimi Themes CarZine allows Reflected XSS.This issue affects CarZine: from n/a through 1.4.6.	Patched by core rule	Y
CVE-2025-23983	WordPress Tijaji theme <= 1.43 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tijaji allows Reflected XSS.This issue affects Tijaji: from n/a through 1.43.	Patched by core rule	Y
CVE-2025-23986	WordPress Tiki Time theme <= 1.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fyrewurks Tiki Time allows Reflected XSS.This issue affects Tiki Time: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-23988	WordPress ghostwriter theme <= 1.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Bruno Cavalcante Ghostwriter allows Reflected XSS.This issue affects Ghostwriter: from n/a through 1.4.		
CVE-2025-26997	WordPress Wireless Butler plugin <= 1.0.11 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in validas Wireless Butler allows Reflected XSS.This issue affects Wireless Butler: from n/a through 1.0.11.	Patched by core rule	Y
CVE-2025-31027	WordPress Tiger theme <= 2.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jocoxdesign Tiger tiger allows Reflected XSS.This issue affects Tiger: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-32920	WordPress TI WooCommerce Wishlist plugin <= 2.9.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in TemplateInvaders TI WooCommerce Wishlist allows Stored XSS.This issue affects TI WooCommerce Wishlist: from n/a through 2.9.2.	Patched by core rule	Y
CVE-2025-39365	WordPress wProject theme < 5.8.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rocket Apps wProject allows Reflected XSS.This issue affects wProject: from n/a before 5.8.0.	Patched by core rule	Y
CVE-2025-39369	WordPress Posts for Page plugin <= 2.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sihibbs Posts for Page allows DOM-Based XSS.This issue affects Posts for Page: from n/a through 2.1.	Patched by core rule	Y
CVE-2025-39372	WordPress WordPress Events Calendar Registration & Tickets plugin <= 2.6.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in elbisnero WordPress Events Calendar Registration & Tickets allows Reflected XSS.This issue affects WordPress Events Calendar Registration & Tickets: from n/a through 2.6.0.	Patched by core rule	Y
CVE-2025-39392	WordPress WPAMS plugin <= 44.0 (17-08-2023) - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mojoomla WPAMS allows Reflected XSS.This issue	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects WPAMS: from n/a through 44.0 (17-08-2023).		
CVE-2025-39393	WordPress Hospital Management System plugin <= 47.0 (20-11-2023) - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mojoomla Hospital Management System allows Reflected XSS.This issue affects Hospital Management System: from n/a through 47.0 (20-11-2023).	Patched by core rule	Y
CVE-2025-39407	WordPress Memberpress plugin <= 1.11.37 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Caseproof, LLC Memberpress allows Reflected XSS.This issue affects Memberpress: from n/a through 1.11.37.	Patched by core rule	Y
CVE-2025-39409	WordPress WordPress Video Robot - The Ultimate Video Importer plugin <= 1.20.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pressaholic WordPress Video Robot - The Ultimate Video Importer.This issue affects WordPress Video Robot - The Ultimate Video Importer: from n/a through 1.20.0.	Patched by core rule	Y
CVE-2025-39446	WordPress Booster Plus for WooCommerce plugin <= 7.2.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pluggabl LLC Booster Plus for WooCommerce allows Reflected XSS.This issue affects Booster Plus for WooCommerce: from n/a through 7.2.4.	Patched by core rule	Y
CVE-2025-39448	WordPress JetElements For Elementor plugin <= 2.7.4.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetElements For Elementor allows Stored XSS.This issue affects JetElements For Elementor: from n/a through 2.7.4.1.	Patched by core rule	Y
CVE-2025-39450	WordPress JetTabs plugin <= 2.2.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetTabs allows DOM-Based XSS.This issue affects JetTabs: from n/a through 2.2.7.	Patched by core rule	Y
CVE-2025-43832	WordPress Remote Images Grabber plugin <= 0.6 - Reflected Cross Site Scripting (XSS)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	vulnerability	andreyk Remote Images Grabber allows Reflected XSS.This issue affects Remote Images Grabber: from n/a through 0.6.		
CVE-2025-43834	WordPress cookieBAR plugin <= 1.7.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tox82 cookieBAR allows Stored XSS.This issue affects cookieBAR: from n/a through 1.7.0.	Patched by core rule	Y
CVE-2025-43836	WordPress Syndicate Out <= 0.9 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in confuzzledduck Syndicate Out allows Reflected XSS.This issue affects Syndicate Out: from n/a through 0.9.	Patched by core rule	Y
CVE-2025-43837	WordPress Total Donations <= 3.0.8 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in binti76 Total Donations allows Reflected XSS.This issue affects Total Donations: from n/a through 3.0.8.	Patched by core rule	Y
CVE-2025-43839	WordPress BP Messages Tool plugin <= 2.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in shanebp BP Messages Tool allows Reflected XSS.This issue affects BP Messages Tool: from n/a through 2.2.	Patched by core rule	Y
CVE-2025-43841	WordPress WP Vegas plugin <= 2.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jamesdbruner WP Vegas allows Stored XSS.This issue affects WP Vegas: from n/a through 2.2.	Patched by core rule	Y
CVE-2025-46262	WordPress Mad Mimi for WordPress plugin <= 1.5.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zack Katz Mad Mimi for WordPress allows Stored XSS.This issue affects Mad Mimi for WordPress: from n/a through 1.5.1.	Patched by core rule	Y
CVE-2025-46263	WordPress Author Box After Posts plugin <= 1.6 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Lloyd Saunders Author Box After Posts allows Stored XSS.This issue affects Author Box After Posts: from n/a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		through 1.6.		
CVE-2025-46543	WordPress Enhanced Paypal Shortcodes plugin <= 0.5a - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Charly Leetham Enhanced Paypal Shortcodes allows Stored XSS.This issue affects Enhanced Paypal Shortcodes: from n/a through 0.5a.	Patched by core rule	Y
CVE-2025-48232	WordPress Xpro Addons For Beaver Builder – Lite <= 1.5.5 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Xpro Xpro Addons For Beaver Builder – Lite allows Stored XSS. This issue affects Xpro Addons For Beaver Builder – Lite: from n/a through 1.5.5.	Patched by core rule	Y
CVE-2025-48234	WordPress Ultimate Blocks <= 3.3.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ultimate Blocks Ultimate Blocks allows DOM-Based XSS. This issue affects Ultimate Blocks: from n/a through 3.3.0.	Patched by core rule	Y
CVE-2025-48235	WordPress WP Image Mask <= 3.1.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bogdan Bendziukov WP Image Mask allows DOM-Based XSS. This issue affects WP Image Mask: from n/a through 3.1.2.	Patched by core rule	Y
CVE-2025-48236	WordPress bunny.net <= 2.3.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bunny.net bunny.net allows Stored XSS. This issue affects bunny.net: from n/a through 2.3.0.	Patched by core rule	Y
CVE-2025-48237	WordPress Wishlist for WooCommerce <= 3.2.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Wishlist for WooCommerce allows Stored XSS. This issue affects Wishlist for WooCommerce: from n/a through 3.2.2.	Patched by core rule	Y
CVE-2025-48239	WordPress Product Notes Tab & Private Admin Notes for WooCommerce <= 3.1.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Product Notes Tab & Private Admin Notes for WooCommerce allows	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Stored XSS. This issue affects Product Notes Tab & Private Admin Notes for WooCommerce: from n/a through 3.1.0.		
CVE-2025-48240	WordPress Cost of Goods for WooCommerce <= 3.7.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Cost of Goods for WooCommerce allows Stored XSS. This issue affects Cost of Goods for WooCommerce: from n/a through 3.7.0.	Patched by core rule	Y
CVE-2025-48244	WordPress Exclusive Addons Elementor <= 2.7.9 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tim Strifler Exclusive Addons Elementor allows Stored XSS. This issue affects Exclusive Addons Elementor: from n/a through 2.7.9.	Patched by core rule	Y
CVE-2025-48248	WordPress Sitewide Discount for WooCommerce: Apply Discount to All Products <= 2.2.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Sitewide Discount for WooCommerce: Apply Discount to All Products allows Stored XSS. This issue affects Sitewide Discount for WooCommerce: Apply Discount to All Products: from n/a through 2.2.1.	Patched by core rule	Y
CVE-2025-48249	WordPress EAN for WooCommerce <= 5.4.6 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory EAN for WooCommerce allows Stored XSS. This issue affects EAN for WooCommerce: from n/a through 5.4.6.	Patched by core rule	Y
CVE-2025-48250	WordPress Coupons & Add to Cart by URL Links for WooCommerce <= 1.7.7 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Coupons & Add to Cart by URL Links for WooCommerce allows Stored XSS. This issue affects Coupons & Add to Cart by URL Links for WooCommerce: from n/a through 1.7.7.	Patched by core rule	Y
CVE-2025-48251	WordPress Additional Custom Emails & Recipients for WooCommerce <= 3.5.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Additional Custom Emails &	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Recipients for WooCommerce allows Stored XSS. This issue affects Additional Custom Emails & Recipients for WooCommerce: from n/a through 3.5.1.		
CVE-2025-48252	WordPress Back Button Widget <= 1.6.8 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Back Button Widget allows Stored XSS. This issue affects Back Button Widget: from n/a through 1.6.8.	Patched by core rule	Y
CVE-2025-48253	WordPress Free Shipping Bar: Amount Left for Free Shipping for WooCommerce <= 2.4.6 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Free Shipping Bar: Amount Left for Free Shipping for WooCommerce allows Stored XSS. This issue affects Free Shipping Bar: Amount Left for Free Shipping for WooCommerce: from n/a through 2.4.6.	Patched by core rule	Y
CVE-2025-48254	WordPress Change Add to Cart Button Text for WooCommerce <= 2.2.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Change Add to Cart Button Text for WooCommerce allows Stored XSS. This issue affects Change Add to Cart Button Text for WooCommerce: from n/a through 2.2.2.	Patched by core rule	Y
CVE-2025-48256	WordPress Import Social Events <= 1.8.5 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Xylus Themes Import Social Events allows Stored XSS. This issue affects Import Social Events: from n/a through 1.8.5.	Patched by core rule	Y
CVE-2025-48258	WordPress Mega Menu Block <= 1.0.6 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jetmonsters Mega Menu Block allows Stored XSS. This issue affects Mega Menu Block: from n/a through 1.0.6.	Patched by core rule	Y
CVE-2025-48263	WordPress MultiVendorX <= 4.2.22 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MultiVendorX MultiVendorX allows Stored XSS. This issue affects MultiVendorX: from	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		n/a through 4.2.22.		
CVE-2025-48266	WordPress Active Products Tables for WooCommerce <= 1.0.6.8 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RealMag777 Active Products Tables for WooCommerce allows Stored XSS. This issue affects Active Products Tables for WooCommerce: from n/a through 1.0.6.8.	Patched by core rule	Y
CVE-2025-48269	WordPress WPAdverts <= 2.2.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Greg Winiarski WPAdverts allows DOM-Based XSS. This issue affects WPAdverts: from n/a through 2.2.3.	Patched by core rule	Y
CVE-2025-48270	WordPress SKT Blocks <= 2.2 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sonalsinha21 SKT Blocks allows DOM-Based XSS. This issue affects SKT Blocks: from n/a through 2.2.	Patched by core rule	Y
CVE-2025-48276	WordPress Visual Composer Website Builder <= 45.11.0 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Visual Composer Visual Composer Website Builder allows Stored XSS. This issue affects Visual Composer Website Builder: from n/a through 45.11.0.	Patched by core rule	Y
CVE-2025-48277	WordPress Cost Calculator Builder <= 3.2.74 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Stylemix Cost Calculator Builder allows Stored XSS. This issue affects Cost Calculator Builder: from n/a through 3.2.74.	Patched by core rule	Y
CVE-2025-48288	WordPress ElementInvader Addons for Elementor <= 1.3.5 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Element Invader ElementInvader Addons for Elementor allows Stored XSS. This issue affects ElementInvader Addons for Elementor: from n/a through 1.3.5.	Patched by core rule	Y
CVE-2025-48341	WordPress Form Maker by 10Web <= 1.15.33 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 10Web Form Maker by 10Web allows Stored XSS.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This issue affects Form Maker by 10Web: from n/a through 1.15.33.		
CVE-2025-4939	PHPGurukul Credit Card Application Management System new-ccapplication.php cross site scripting	A vulnerability classified as problematic was found in PHPGurukul Credit Card Application Management System 1.0. This vulnerability affects unknown code of the file /admin/new-ccapplication.php. The manipulation 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-2025-5007	Part-DB Profile Picture Feature AttachmentSubmitHandler.php handleUpload cross site scripting	A vulnerability was found in Part-DB up to 1.17.0. It has been declared as problematic. Affected by this vulnerability is the function handleUpload of the file src/Services/Attachments/AttachmentSubmitHandler.php of the component Profile Picture Feature. The manipulation of the argument attachment leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.17.1 is able to address this issue. The identifier of the patch is 2c4f44e808500db19c391159b30cb6142896d415. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-5010	moonlightL hexo-boot Blog Backend index.html cross site scripting	A vulnerability classified as problematic has been found in moonlightL hexo-boot 4.3.0. This affects an unknown part of the file /admin/home/index.html of the component Blog Backend. The manipulation of the argument Description 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-2025-31636	WordPress WP Post Modules for Elementor plugin <= 2.5.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SaurabhSharma WP Post Modules for Elementor allows Reflected XSS. This issue affects WP Post Modules for Elementor: from n/a through 2.5.0.	Patched by core rule	Y
CVE-2025-32285	WordPress Butcher	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	theme <= 2.40 - Reflected Cross Site Scripting (XSS) vulnerability	Input During Web Page Generation ('Cross-site Scripting') vulnerability in ApusTheme Butcher allows Reflected XSS. This issue affects Butcher: from n/a through 2.40.	rule	
CVE-2025-39502	WordPress Goodlayers Hostel Plugin <= 3.1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GoodLayers Goodlayers Hostel allows Reflected XSS. This issue affects Goodlayers Hostel: from n/a through 3.1.2.	Patched by core rule	Y
CVE-2025-39505	WordPress Goodlayers Hotel plugin <= 3.1.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GoodLayers Goodlayers Hotel allows Reflected XSS. This issue affects Goodlayers Hotel: from n/a through 3.1.4.	Patched by core rule	Y
CVE-2025-46437	WordPress Tayori Form plugin <= 1.2.9 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tayoricom Tayori Form allows Reflected XSS. This issue affects Tayori Form: from n/a through 1.2.9.	Patched by core rule	Y
CVE-2025-46440	WordPress kStats Reloaded plugin <= 0.7.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mark kStats Reloaded allows Reflected XSS. This issue affects kStats Reloaded: from n/a through 0.7.4.	Patched by core rule	Y
CVE-2025-46446	WordPress Libro de Reclamaciones <= 1.0.1 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ivanrojas Libro de Reclamaciones allows Stored XSS. This issue affects Libro de Reclamaciones: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-46448	WordPress Document Management System <= 1.24 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in reifsnyderb Document Management System allows Reflected XSS. This issue affects Document Management System: from n/a through 1.24.	Patched by core rule	Y
CVE-2025-46456	WordPress Theme Blvd Sliders plugin <= 1.2.5 - Reflected Cross Site Scripting (XSS)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	vulnerability	Jason Theme Blvd Sliders allows Reflected XSS. This issue affects Theme Blvd Sliders: from n/a through 1.2.5.		
CVE-2025-46487	WordPress EC Authorize.net plugin <= 0.3.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sftranna EC Authorize.net allows Reflected XSS. This issue affects EC Authorize.net: from n/a through 0.3.3.	Patched by core rule	Y
CVE-2025-46493	WordPress Crossword Compiler Puzzles <= 5.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wordwebsoftware Crossword Compiler Puzzles allows Stored XSS. This issue affects Crossword Compiler Puzzles: from n/a through 5.3.	Patched by core rule	Y
CVE-2025-46515	WordPress Category Widget plugin <= 2.0.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in M A Vinoth Kumar Category Widget allows Reflected XSS. This issue affects Category Widget: from n/a through 2.0.2.	Patched by core rule	Y
CVE-2025-46518	WordPress IGIT Related Posts With Thumb Image After Posts <= 4.5.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in phpaddicted IGIT Related Posts With Thumb Image After Posts allows Stored XSS. This issue affects IGIT Related Posts With Thumb Image After Posts: from n/a through 4.5.3.	Patched by core rule	Y
CVE-2025-46526	WordPress My Custom Widgets plugin <= 2.0.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in janekniefeldt My Custom Widgets allows Reflected XSS. This issue affects My Custom Widgets: from n/a through 2.0.5.	Patched by core rule	Y
CVE-2025-46537	WordPress Section Widget plugin <= 3.3.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ctltwp Section Widget allows Reflected XSS. This issue affects Section Widget: from n/a through 3.3.1.	Patched by core rule	Y
CVE-2025-47458	WordPress B2i Investor Tools plugin <= 1.0.7.9 - Reflected Cross Site	Improper Neutralization of Input During Web Page Generation ('Cross-site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Scripting (XSS) vulnerability	Scripting') vulnerability in B2itech B2i Investor Tools allows Reflected XSS. This issue affects B2i Investor Tools: from n/a through 1.0.7.9.		
CVE-2025-47611	WordPress User Meta plugin <= 3.1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Khaled User Meta allows Reflected XSS. This issue affects User Meta: from n/a through 3.1.2.	Patched by core rule	Y
CVE-2025-47613	WordPress School Management System for Wordpress plugin <= 92.0.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mojoomla School Management allows Reflected XSS. This issue affects School Management: from n/a through 92.0.0.	Patched by core rule	Y
CVE-2025-47618	WordPress BMI Adult & Kid Calculator plugin <= 1.2.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mortgage Calculator BMI Adult & Kid Calculator allows Reflected XSS. This issue affects BMI Adult & Kid Calculator: from n/a through 1.2.2.	Patched by core rule	Y
CVE-2025-47673	WordPress Arconix Shortcodes plugin <= 2.1.16 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tychesoftwares Arconix Shortcodes allows Reflected XSS. This issue affects Arconix Shortcodes: from n/a through 2.1.16.	Patched by core rule	Y
CVE-2025-47678	WordPress FunnelCockpit plugin <= 1.4.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FunnelCockpit FunnelCockpit allows Reflected XSS. This issue affects FunnelCockpit: from n/a through 1.4.2.	Patched by core rule	Y
CVE-2025-47680	WordPress xili-tidy-tags plugin <= 1.12.06 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michel - xiligroup dev xili-tidy-tags allows Reflected XSS. This issue affects xili-tidy-tags: from n/a through 1.12.06.	Patched by core rule	Y
CVE-2025-48241	WordPress Verge3D plugin <= 4.9.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Soft8Soft LLC Verge3D	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		allows Reflected XSS. This issue affects Verge3D: from n/a through 4.9.3.		
CVE-2025-48245	WordPress Quick Contact Form plugin <= 8.2.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fullworks Quick Contact Form allows Reflected XSS. This issue affects Quick Contact Form : from n/a through 8.2.1.	Patched by core rule	Y
CVE-2025-48286	WordPress ReDi Restaurant Reservation plugin <= 24.1209 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in catkin ReDi Restaurant Reservation allows Reflected XSS. This issue affects ReDi Restaurant Reservation: from n/a through 24.1209.	Patched by core rule	Y
CVE-2025-5127	FLIR AX8 prod.php cross site scripting	A vulnerability, which was classified as problematic, has been found in FLIR AX8 up to 1.46.16. This issue affects some unknown processing of the file /prod.php. The manipulation of the argument cmd 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-2025-5138	Bitwarden PDF File cross site scripting	A vulnerability was found in Bitwarden up to 2.25.1. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component PDF File Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y

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