INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

September 2025

The total zero-day vulnerabilities count for September month: 789

Command Injection	SQL Injection	SSRF	Path Traversal	Cross-Site Scripting
27	135	27	161	439

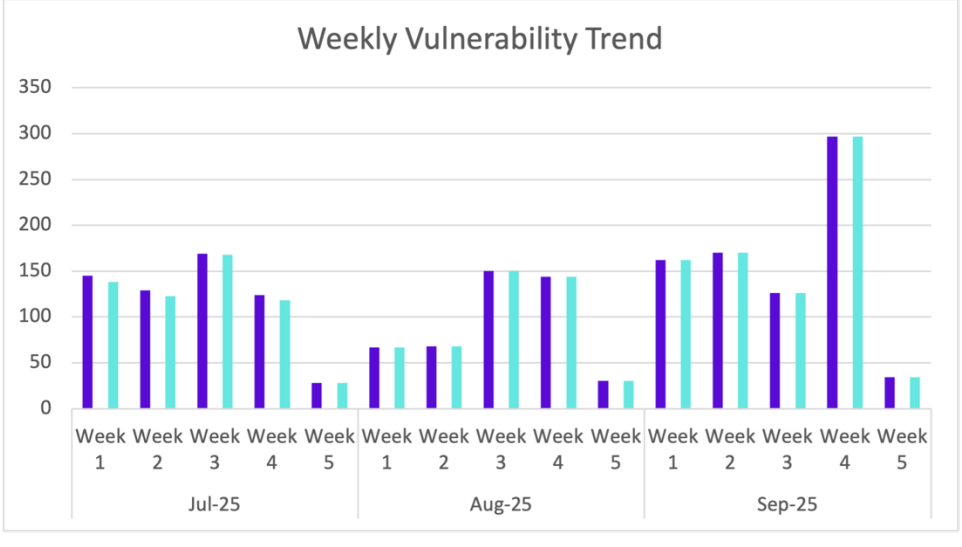
Zero-day vulnerabilities protected through core rules	789
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities found by Indusface WAS	789

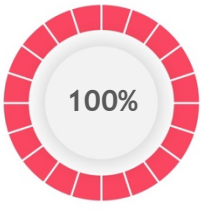
- To enable custom rules, please contact support@indusface.com
- Learn more about zero-day vulnerabilities, detection, and prevention, here

Vulnerability Trend:

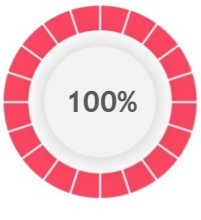
The weekly trend displays the total number of vulnerabilities discovered and the type of protection provided for the last quarter.

Weekly Vulnerability Trend



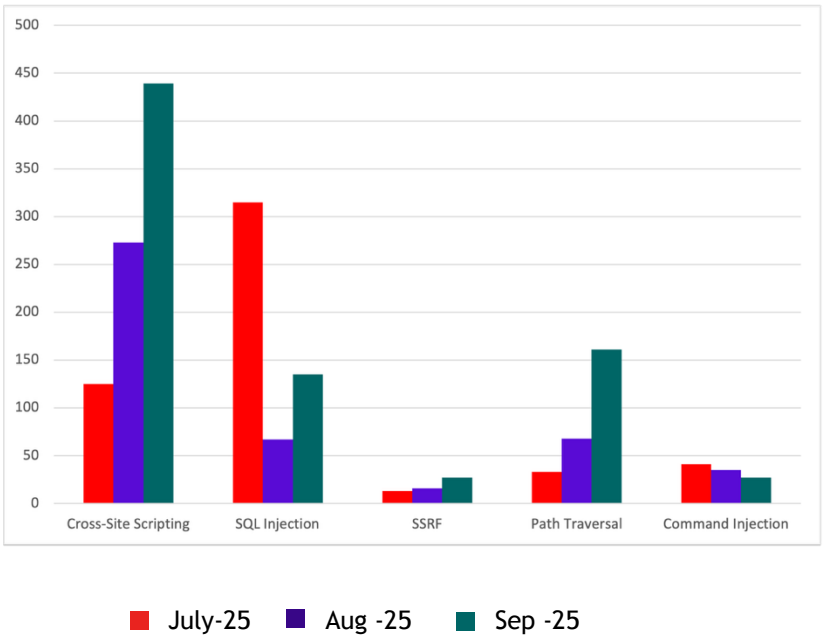


of the zero-day vulnerabilities were protected by the core rules in the last month



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

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-29157	CVE-2025-29157 - An issue in petstore v.1.0.7 allows a remote attacker to execute arbitrary code via accessing a non-...	An issue in petstore v.1.0.7 allows a remote attacker to execute arbitrary code via accessing a non-existent endpoint/cart, the server returns a 404-error page exposing sensitive information including the Servlet name (default) and server version	Patched by core rule	Y
CVE-2025-29155	CVE-2025-29155 - An issue in petstore v.1.0.7 allows a remote attacker to execute arbitrary code via the DELETE endpo...	An issue in petstore v.1.0.7 allows a remote attacker to execute arbitrary code via the DELETE endpoint	Patched by core rule	Y
CVE-2025-45326	CVE-2025-45326 - An issue in PocketVJ CP PocketVJ-CP-v3 pvj 3.9.1 allows remote attackers to execute arbitrary code v...	An issue in PocketVJ CP PocketVJ-CP-v3 pvj 3.9.1 allows remote attackers to execute arbitrary code via the submit_size.php component.	Patched by core rule	Y
CVE-2025-29083	CVE-2025-29083 - SQL Injection vulnerability in CSZ-CMS v.1.3.0 allows a remote attacker to execute arbitrary code vi...	SQL Injection vulnerability in CSZ-CMS v.1.3.0 allows a remote attacker to execute arbitrary code via the execSqlFile function in the Plugin_Manager.php file.	Patched by core rule	Y
CVE-2025-43953	CVE-2025-43953 - In 2wcom IP-4c 2.16, the web interface allows admin and manager users to execute arbitrary code as r...	In 2wcom IP-4c 2.16, the web interface allows admin and manager users to execute arbitrary code as root via a ping or traceroute field on the TCP/IP screen.	Patched by core rule	Y
CVE-2025-57296	CVE-2025-57296 - Tenda AC6 router firmware 15.03.05.19 contains a command injection vulnerability in the formSetIptv ...	Tenda AC6 router firmware 15.03.05.19 contains a command injection vulnerability in the formSetIptv function, which processes requests to the /goform/SetIPTVCfg web interface. When handling the list and vlanId parameters, the sub_ADBC0 helper function	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		concatenates these user-supplied values into nvram set system commands using doSystemCmd, without validating or sanitizing special characters (e.g., ;, ", #). An unauthenticated or authenticated attacker can exploit this by submitting a crafted POST request, leading to arbitrary system command execution on the affected device.		
CVE-2025-56706	CVE-2025-56706 - Edimax BR-6473AX v1.0.28 was discovered to contain a remote code execution (RCE) vulnerability via t...	Edimax BR-6473AX v1.0.28 was discovered to contain a remote code execution (RCE) vulnerability via the Object parameter in the openwrt_getConfig function.	Patched by core rule	Y
CVE-2025-52053	CVE-2025-52053 - TOTOLINK X6000R V9.4.0cu.1360_B20241207 was found to contain a command injection vulnerability in th...	TOTOLINK X6000R V9.4.0cu.1360_B20241207 was found to contain a command injection vulnerability in the sub_417D74 function via the file_name parameter. This vulnerability allows unauthenticated attackers to execute arbitrary commands via a crafted request.	Patched by core rule	Y
CVE-2025-10442	CVE-2025-10442 - A vulnerability was determined in Tenda AC9 and AC15 15.03.05.14. This affects the function formexeC...	A vulnerability was determined in Tenda AC9 and AC15 15.03.05.14. This affects the function formexeCommand of the file /goform/exeCommand. This manipulation of the argument cmdinput causes os command injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-10441	CVE-2025-10441 - A vulnerability was found in D-Link DI-8100G, DI-8200G and DI-8003G 17.12.20A1/19.12.10A1. Affected ...	A vulnerability was found in D-Link DI-8100G, DI-8200G and DI-8003G 17.12.20A1/19.12.10A1. Affected by this issue is the function sub_433F7C of the file version_upgrade.asp of the component jhttpd. The manipulation of the argument path results in os command injection. The attack may be launched remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2025-10440	CVE-2025-10440 - A vulnerability has been found in D-Link DI-8100, DI-8100G, DI-8200, DI-8200G, DI-8003 and DI-8003G ...	A vulnerability has been found in D-Link DI-8100, DI-8100G, DI-8200, DI-8200G, DI-8003 and DI-8003G 16.07.26A1/17.12.20A1/19.12.10A1. Affected by this vulnerability is the function sub_4621DC of the file usb_paswd.asp of the component jhttpd. The manipulation of the argument hname leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-10328	CVE-2025-10328 - A security vulnerability has been detected in MiczFlor RPi-Jukebox-RFID up to 2.8.0. Affected by thi...	A security vulnerability has been detected in MiczFlor RPi-Jukebox-RFID up to 2.8.0. Affected by this issue is some unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		functionality of the file /htdocs/api/playlist/playsinglefile.php. The manipulation of the argument File leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-10327	CVE-2025-10327 - A weakness has been identified in MiczFlor RPi-Jukebox-RFID up to 2.8.0. Affected by this vulnerabil...	A weakness has been identified in MiczFlor RPi-Jukebox-RFID up to 2.8.0. Affected by this vulnerability is an unknown functionality of the file /htdocs/api/playlist/shuffle.php. Executing manipulation of the argument playlist can lead to os command injection. The attack can be launched remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-10326	CVE-2025-10326 - A security flaw has been discovered in MiczFlor RPi-Jukebox-RFID up to 2.8.0. Affected is an unknown...	A security flaw has been discovered in MiczFlor RPi-Jukebox-RFID up to 2.8.0. Affected is an unknown function of the file /htdocs/api/playlist/single.php. Performing manipulation of the argument playlist results in os command injection. The attack can be initiated remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-59045	CVE-2025-59045 - Stalwart is a mail and collaboration server. Starting in version 0.12.0 and prior to version 0.13.3,...	Stalwart is a mail and collaboration server. Starting in version 0.12.0 and prior to version 0.13.3, a memory exhaustion vulnerability exists in Stalwart's CalDAV implementation that allows authenticated attackers to cause denial-of-service by triggering unbounded memory consumption through recurring event expansion. An authenticated attacker can crash the Stalwart server by creating recurring events with large payloads and triggering their expansion through CalDAV REPORT requests. A single malicious request expanding 300 events with 1000-character descriptions can consume up to 2 GB of memory. The vulnerability exists in the `ArchivedCalendarEventData.expand` function, which processes CalDAV `REPORT` requests with event expansion. When a client requests recurring events in their expanded form using the `<C:expand>` element, the server stores all expanded event instances in memory without enforcing	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		size limits. Users should upgrade to Stalwart version 0.13.3 or later to receive a fix. If immediate upgrading is not possible, implement memory limits at the container/system level; monitor server memory usage for unusual spikes; consider rate limiting CalDAV REPORT requests; and restrict CalDAV access to trusted users only.		
CVE-2025-57633	CVE-2025-57633 - A command injection vulnerability in FTP-Flask-python through 5173b68 allows unauthenticated remote ...	A command injection vulnerability in FTP-Flask-python through 5173b68 allows unauthenticated remote attackers to execute arbitrary OS commands. The /ftp.html endpoint's "Upload File" action constructs a shell command from the ftp_file parameter and executes it using os.system() without sanitization or escaping.	Patched by core rule	Y
CVE-2025-57285	CVE-2025-57285 - codeceptjs 3.7.3 contains a command injection vulnerability in the emptyFolder function (lib/utils.j...	codeceptjs 3.7.3 contains a command injection vulnerability in the emptyFolder function (lib/utils.js). The execSync command directly concatenates the user-controlled directoryPath parameter without sanitization or escaping, allowing attackers to execute arbitrary commands.	Patched by core rule	Y
CVE-2014-125127	CVE-2014-125127 - The mikecao/flight PHP framework in versions prior to v1.2 is vulnerable to Denial of Service (DoS) ...	The mikecao/flight PHP framework in versions prior to v1.2 is vulnerable to Denial of Service (DoS) attacks due to eager loading of request bodies in the Request class constructor. The framework automatically reads the entire request body on every HTTP request, regardless of whether the application needs it. An attacker can exploit this by sending requests with large payloads, causing excessive memory consumption and potentially exhausting available server memory, leading to application crashes or service unavailability. The vulnerability was fixed in v1.2 by implementing lazy loading of request bodies.	Patched by core rule	Y
CVE-2025-55824	CVE-2025-55824 - ModStartCMS v9.5.0 has an arbitrary file write vulnerability, which allows attackers to write malici...	ModStartCMS v9.5.0 has an arbitrary file write vulnerability, which allows attackers to write malicious files and execute malicious commands to obtain sensitive data on the server.	Patched by core rule	Y
CVE-2025-50757	CVE-2025-50757 - Wavlink WN535K3 20191010 was found to contain a command injection vulnerability in the set_sys_adm f...	Wavlink WN535K3 20191010 was found to contain a command injection vulnerability in the set_sys_adm function via the username parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	Patched by core rule	Y
CVE-2025-50755	CVE-2025-50755 - Wavlink	Wavlink WN535K3	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	WN535K3 20191010 was found to contain a command injection vulnerability in the set_sys_cmd f...	20191010 was found to contain a command injection vulnerability in the set_sys_cmd function via the command parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	rule	
CVE-2024-48705	CVE-2024-48705 - Wavlink AC1200 with firmware versions M32A3_V1410_230602 and M32A3_V1410_240222 are vulnerable to a ...	Wavlink AC1200 with firmware versions M32A3_V1410_230602 and M32A3_V1410_240222 are vulnerable to a post-authentication command injection while resetting the password. This vulnerability is specifically found within the "set_sys_adm" function of the "adm.cgi" binary, and is due to improper santization of the user provided "newpass" field	Patched by core rule	Y
CVE-2025-9727	CVE-2025-9727 - A weakness has been identified in D-Link DIR-816L 206b01. Affected by this issue is the function soa...	A weakness has been identified in D-Link DIR-816L 206b01. Affected by this issue is the function soapcgi_main of the file /soap.cgi. This manipulation of the argument service causes os command injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-9580	CVE-2025-9580 - A security vulnerability has been detected in LB-LINK BL-X26 1.2.8. This affects an unknown function...	A security vulnerability has been detected in LB-LINK BL-X26 1.2.8. This affects an unknown function of the file /goform/set_blacklist of the component HTTP Handler. Such manipulation of the argument mac leads to os command injection. The attack can be launched remotely. The exploit has been disclosed publicly 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-2025-9579	CVE-2025-9579 - A weakness has been identified in LB-LINK BL-X26 1.2.8. The impacted element is an unknown function ...	A weakness has been identified in LB-LINK BL-X26 1.2.8. The impacted element is an unknown function of the file /goform/set_hidessid_cfg of the component HTTP Handler. This manipulation of the argument enable causes os command injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-9575	CVE-2025-9575 - A vulnerability was determined in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013....	A vulnerability was determined in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This issue affects the function cgiMain of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/cgi-bin/upload.cgi. Executing manipulation of the argument filename can lead to os command injection. The attack may be performed from a remote location. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-9528	CVE-2025-9528 - A vulnerability was determined in Linksys E1700 1.0.0.4.003. This vulnerability affects the function...	A vulnerability was determined in Linksys E1700 1.0.0.4.003. This vulnerability affects the function systemCommand of the file /goform/systemCommand. Executing manipulation of the argument command can lead to os command injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y

Path Traversal Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-10377	CVE-2025-10377 - The System Dashboard plugin for WordPress is vulnerable to Cross-Site Request Forgery in all version...	The System Dashboard plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.8.20. This is due to missing nonce validation on the sd_toggle_logs() function. This makes it possible for unauthenticated attackers to toggle critical logging settings including Page Access Logs, Error Logs, and Email Delivery Logs via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-10752	CVE-2025-10752 - The OAuth Single Sign On – SSO (OAuth Client) plugin for WordPress is vulnerable to Cross-Site Reque...	The OAuth Single Sign On – SSO (OAuth Client) plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 6.26.12. This is due to using a predictable state parameter (base64 encoded app name) without any randomness in the OAuth flow. This makes it possible for unauthenticated attackers to forge OAuth authorization requests and potentially hijack the OAuth flow via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-56816	CVE-2025-56816 - Datart 1.0.0-rc.3 is vulnerable to Directory Traversal. The configuration file handling of the appli...	Datart 1.0.0-rc.3 is vulnerable to Directory Traversal. The configuration file handling of the application allows attackers to upload arbitrary YAML files to the config/jdbc-driver-ext.yml path. The application parses this file using SnakeYAML's unsafe load() or loadAs() method without input sanitization. This allows deserialization of attacker-controlled YAML content, leading to arbitrary class instantiation. Under	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		certain conditions, this can be exploited to achieve remote code execution (RCE).		
CVE-2025-56815	CVE-2025-56815 - Datart 1.0.0-rc.3 is vulnerable to Directory Traversal in the POST /viz/image interface, since the s...	Datart 1.0.0-rc.3 is vulnerable to Directory Traversal in the POST /viz/image interface, since the server directly uses MultipartFile.transferTo() to save the uploaded file to a path controllable by the user, and lacks strict verification of the file name.	Patched by core rule	Y
CVE-2025-59572	CVE-2025-59572 - Cross-Site Request Forgery (CSRF) vulnerability in purethemes WorkScout-Core allows Cross Site Reque...	Cross-Site Request Forgery (CSRF) vulnerability in purethemes WorkScout-Core allows Cross Site Request Forgery. This issue affects WorkScout-Core: from n/a through n/a.	Patched by core rule	Y
CVE-2025-59568	CVE-2025-59568 - Cross-Site Request Forgery (CSRF) vulnerability in Zoho Flow Zoho Flow allows Cross Site Request For...	Cross-Site Request Forgery (CSRF) vulnerability in Zoho Flow Zoho Flow allows Cross Site Request Forgery. This issue affects Zoho Flow: from n/a through 2.14.1.	Patched by core rule	Y
CVE-2025-58956	CVE-2025-58956 - Cross-Site Request Forgery (CSRF) vulnerability in loopus WP Attractive Donations System allows Stor...	Cross-Site Request Forgery (CSRF) vulnerability in loopus WP Attractive Donations System allows Stored XSS. This issue affects WP Attractive Donations System: from n/a through n/a.	Patched by core rule	Y
CVE-2025-58690	CVE-2025-58690 - Cross-Site Request Forgery (CSRF) vulnerability in ptibogxiv Doliconnect allows Stored XSS. This iss...	Cross-Site Request Forgery (CSRF) vulnerability in ptibogxiv Doliconnect allows Stored XSS. This issue affects Doliconnect: from n/a through 9.5.7.	Patched by core rule	Y
CVE-2025-58688	CVE-2025-58688 - Cross-Site Request Forgery (CSRF) vulnerability in Casengo Casengo Live Chat Support allows Stored X...	Cross-Site Request Forgery (CSRF) vulnerability in Casengo Casengo Live Chat Support allows Stored XSS. This issue affects Casengo Live Chat Support: from n/a through 2.1.4.	Patched by core rule	Y
CVE-2025-58687	CVE-2025-58687 - Cross-Site Request Forgery (CSRF) vulnerability in WP CMS Ninja Current Age Plugin allows Stored XSS...	Cross-Site Request Forgery (CSRF) vulnerability in WP CMS Ninja Current Age Plugin allows Stored XSS. This issue affects Current Age Plugin: from n/a through 1.6.	Patched by core rule	Y
CVE-2025-58677	CVE-2025-58677 - Cross-Site Request Forgery (CSRF) vulnerability in puravida1976 ShrinkTheWeb (STW) Website Previews ...	Cross-Site Request Forgery (CSRF) vulnerability in puravida1976 ShrinkTheWeb (STW) Website Previews allows Stored XSS. This issue	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects ShrinkTheWeb (STW) Website Previews: from n/a through 2.8.5.		
CVE-2025-58676	CVE-2025-58676 - Cross-Site Request Forgery (CSRF) vulnerability in extendyourweb HORIZONTAL SLIDER allows Stored XSS...	Cross-Site Request Forgery (CSRF) vulnerability in extendyourweb HORIZONTAL SLIDER allows Stored XSS. This issue affects HORIZONTAL SLIDER: from n/a through 2.4.	Patched by core rule	Y
CVE-2025-58675	CVE-2025-58675 - Cross-Site Request Forgery (CSRF) vulnerability in tryinteract Interact: Embed A Quiz On Your Site a...	Cross-Site Request Forgery (CSRF) vulnerability in tryinteract Interact: Embed A Quiz On Your Site allows Cross Site Request Forgery. This issue affects Interact: Embed A Quiz On Your Site: from n/a through 3.1.	Patched by core rule	Y
CVE-2025-58670	CVE-2025-58670 - Cross-Site Request Forgery (CSRF) vulnerability in Shankaranand Maurya WP Content Protection allows ...	Cross-Site Request Forgery (CSRF) vulnerability in Shankaranand Maurya WP Content Protection allows Stored XSS. This issue affects WP Content Protection: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-58657	CVE-2025-58657 - Cross-Site Request Forgery (CSRF) vulnerability in EdwardBock Grid allows Stored XSS. This issue aff...	Cross-Site Request Forgery (CSRF) vulnerability in EdwardBock Grid allows Stored XSS. This issue affects Grid: from n/a through 2.3.1.	Patched by core rule	Y
CVE-2025-58270	CVE-2025-58270 - Cross-Site Request Forgery (CSRF) vulnerability in NIX Solutions Ltd NIX Anti-Spam Light allows Cros...	Cross-Site Request Forgery (CSRF) vulnerability in NIX Solutions Ltd NIX Anti-Spam Light allows Cross Site Request Forgery. This issue affects NIX Anti-Spam Light: from n/a through 0.0.4.	Patched by core rule	Y
CVE-2025-58268	CVE-2025-58268 - Cross-Site Request Forgery (CSRF) vulnerability in WPMK WPMK PDF Generator allows Stored XSS. This i...	Cross-Site Request Forgery (CSRF) vulnerability in WPMK WPMK PDF Generator allows Stored XSS. This issue affects WPMK PDF Generator: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-58267	CVE-2025-58267 - Cross-Site Request Forgery (CSRF) vulnerability in Aftabul Islam Stock Message allows Stored XSS. Th...	Cross-Site Request Forgery (CSRF) vulnerability in Aftabul Islam Stock Message allows Stored XSS. This issue affects Stock Message: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-58262	CVE-2025-58262 - Cross-Site Request Forgery (CSRF) vulnerability in wpdirectorykit Sweet Energy Efficiency allows Sto...	Cross-Site Request Forgery (CSRF) vulnerability in wpdirectorykit Sweet Energy Efficiency allows Stored XSS. This issue affects Sweet Energy	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Efficiency: from n/a through 1.0.6.		
CVE-2025-58261	CVE-2025-58261 - Cross-Site Request Forgery (CSRF) vulnerability in PressPage Entertainment Inc Mavis HTTPS to HTTP R...	Cross-Site Request Forgery (CSRF) vulnerability in PressPage Entertainment Inc Mavis HTTPS to HTTP Redirection allows Stored XSS. This issue affects Mavis HTTPS to HTTP Redirection: from n/a through 1.4.3.	Patched by core rule	Y
CVE-2025-58259	CVE-2025-58259 - Cross-Site Request Forgery (CSRF) vulnerability in scriptsbundle Nokri allows Cross Site Request For...	Cross-Site Request Forgery (CSRF) vulnerability in scriptsbundle Nokri allows Cross Site Request Forgery. This issue affects Nokri: from n/a through 1.6.4.	Patched by core rule	Y
CVE-2025-58255	CVE-2025-58255 - Cross-Site Request Forgery (CSRF) vulnerability in yonisink Custom Post Type Images allows Code Inje...	Cross-Site Request Forgery (CSRF) vulnerability in yonisink Custom Post Type Images allows Code Injection. This issue affects Custom Post Type Images: from n/a through 0.5.	Patched by core rule	Y
CVE-2025-58250	CVE-2025-58250 - Cross-Site Request Forgery (CSRF) vulnerability in ApusTheme Findgo allows Authentication Bypass. Th...	Cross-Site Request Forgery (CSRF) vulnerability in ApusTheme Findgo allows Authentication Bypass. This issue affects Findgo: from n/a through 1.3.55.	Patched by core rule	Y
CVE-2025-58244	CVE-2025-58244 - Cross-Site Request Forgery (CSRF) vulnerability in Anps Constructo allows Object Injection. This iss...	Cross-Site Request Forgery (CSRF) vulnerability in Anps Constructo allows Object Injection. This issue affects Constructo: from n/a through 4.3.9.	Patched by core rule	Y
CVE-2025-58236	CVE-2025-58236 - Cross-Site Request Forgery (CSRF) vulnerability in Mayo Moriyama Force Update Translations allows Cr...	Cross-Site Request Forgery (CSRF) vulnerability in Mayo Moriyama Force Update Translations allows Cross Site Request Forgery. This issue affects Force Update Translations: from n/a through 0.5.	Patched by core rule	Y
CVE-2025-58224	CVE-2025-58224 - Cross-Site Request Forgery (CSRF) vulnerability in Printeers Printeers Print & Ship allows Cross Sit...	Cross-Site Request Forgery (CSRF) vulnerability in Printeers Printeers Print & Ship allows Cross Site Request Forgery. This issue affects Printeers Print & Ship: from n/a through 1.17.0.	Patched by core rule	Y
CVE-2025-58219	CVE-2025-58219 - Cross-Site Request Forgery (CSRF) vulnerability in LIJE Show Pages List allows Cross Site Request Fo...	Cross-Site Request Forgery (CSRF) vulnerability in LIJE Show Pages List allows Cross Site Request Forgery. This issue affects Show Pages List: from n/a through 1.2.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-58200	CVE-2025-58200 - Cross-Site Request Forgery (CSRF) vulnerability in Bage Flexible FAQ allows Cross Site Request Forge...	Cross-Site Request Forgery (CSRF) vulnerability in Bage Flexible FAQ allows Cross Site Request Forgery. This issue affects Flexible FAQ: from n/a through 0.2.	Patched by core rule	Y
CVE-2025-58199	CVE-2025-58199 - Cross-Site Request Forgery (CSRF) vulnerability in Fastly Fastly allows Cross Site Request Forgery. ...	Cross-Site Request Forgery (CSRF) vulnerability in Fastly Fastly allows Cross Site Request Forgery. This issue affects Fastly: from n/a through 1.2.28.	Patched by core rule	Y
CVE-2025-58032	CVE-2025-58032 - Cross-Site Request Forgery (CSRF) vulnerability in Bytes.co WP Compiler allows Cross Site Request Fo...	Cross-Site Request Forgery (CSRF) vulnerability in Bytes.co WP Compiler allows Cross Site Request Forgery. This issue affects WP Compiler: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-58014	CVE-2025-58014 - Cross-Site Request Forgery (CSRF) vulnerability in Ays Pro Quiz Maker allows Cross Site Request Forg...	Cross-Site Request Forgery (CSRF) vulnerability in Ays Pro Quiz Maker allows Cross Site Request Forgery. This issue affects Quiz Maker: from n/a through 6.7.0.61.	Patched by core rule	Y
CVE-2025-58013	CVE-2025-58013 - Cross-Site Request Forgery (CSRF) vulnerability in pebas CouponXxL allows Privilege Escalation. This...	Cross-Site Request Forgery (CSRF) vulnerability in pebas CouponXxL allows Privilege Escalation. This issue affects CouponXxL: from n/a through 4.5.0.	Patched by core rule	Y
CVE-2025-58010	CVE-2025-58010 - Cross-Site Request Forgery (CSRF) vulnerability in straightvisions GmbH SV Proven Expert allows Cros...	Cross-Site Request Forgery (CSRF) vulnerability in straightvisions GmbH SV Proven Expert allows Cross Site Request Forgery. This issue affects SV Proven Expert: from n/a through 2.0.06.	Patched by core rule	Y
CVE-2025-57992	CVE-2025-57992 - Cross-Site Request Forgery (CSRF) vulnerability in InterServer Mail Baby SMTP allows Cross Site Requ...	Cross-Site Request Forgery (CSRF) vulnerability in InterServer Mail Baby SMTP allows Cross Site Request Forgery. This issue affects Mail Baby SMTP: from n/a through 2.8.	Patched by core rule	Y
CVE-2025-57983	CVE-2025-57983 - Cross-Site Request Forgery (CSRF) vulnerability in Damian BP Disable Activation Reloaded allows Acce...	Cross-Site Request Forgery (CSRF) vulnerability in Damian BP Disable Activation Reloaded allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects BP Disable Activation Reloaded: from n/a through 1.2.1.	Patched by core rule	Y
CVE-2025-57978	CVE-2025-57978 - Cross-Site Request Forgery (CSRF) vulnerability in themespride Advanced Appointment Booking	Cross-Site Request Forgery (CSRF) vulnerability in themespride Advanced Appointment Booking & Scheduling allows	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	& Sc...	Cross Site Request Forgery. This issue affects Advanced Appointment Booking & Scheduling: from n/a through 1.9.		
CVE-2025-57977	CVE-2025-57977 - Cross-Site Request Forgery (CSRF) vulnerability in wpdesk Flexible PDF Invoices for WooCommerce &amp...	Cross-Site Request Forgery (CSRF) vulnerability in wpdesk Flexible PDF Invoices for WooCommerce & WordPress allows Cross Site Request Forgery. This issue affects Flexible PDF Invoices for WooCommerce & WordPress: from n/a through 6.0.13.	Patched by core rule	Y
CVE-2025-57970	CVE-2025-57970 - Cross-Site Request Forgery (CSRF) vulnerability in SALESmanago SALESmanago & Leadoo allows Cross Sit...	Cross-Site Request Forgery (CSRF) vulnerability in SALESmanago SALESmanago & Leadoo allows Cross Site Request Forgery.This issue affects SALESmanago & Leadoo: from n/a through 3.8.1.	Patched by core rule	Y
CVE-2025-57960	CVE-2025-57960 - Cross-Site Request Forgery (CSRF) vulnerability in TravelMap Travel Map allows Cross Site Request Fo...	Cross-Site Request Forgery (CSRF) vulnerability in TravelMap Travel Map allows Cross Site Request Forgery. This issue affects Travel Map: from n/a through 1.0.3.	Patched by core rule	Y
CVE-2025-57946	CVE-2025-57946 - Cross-Site Request Forgery (CSRF) vulnerability in Loc Bui payOS allows Cross Site Request Forgery. ...	Cross-Site Request Forgery (CSRF) vulnerability in Loc Bui payOS allows Cross Site Request Forgery. This issue affects payOS: from n/a through 1.0.61.	Patched by core rule	Y
CVE-2025-57942	CVE-2025-57942 - Cross-Site Request Forgery (CSRF) vulnerability in andy_moyle Emergency Password Reset allows Cross ...	Cross-Site Request Forgery (CSRF) vulnerability in andy_moyle Emergency Password Reset allows Cross Site Request Forgery. This issue affects Emergency Password Reset: from n/a through 9.0.	Patched by core rule	Y
CVE-2025-57934	CVE-2025-57934 - Cross-Site Request Forgery (CSRF) vulnerability in Aurélien LWS LWS Affiliation allows Cross Site Re...	Cross-Site Request Forgery (CSRF) vulnerability in Aurélien LWS LWS Affiliation allows Cross Site Request Forgery. This issue affects LWS Affiliation: from n/a through 2.3.6.	Patched by core rule	Y
CVE-2025-57933	CVE-2025-57933 - Cross-Site Request Forgery (CSRF) vulnerability in piotnetdotcom Piotnet Forms allows Cross Site Req...	Cross-Site Request Forgery (CSRF) vulnerability in piotnetdotcom Piotnet Forms allows Cross Site Request Forgery. This issue affects Piotnet Forms: from n/a through 1.0.30.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-57930	CVE-2025-57930 - Cross-Site Request Forgery (CSRF) vulnerability in kanwei_doublethedonation Double the Donation allo...	Cross-Site Request Forgery (CSRF) vulnerability in kanwei_doublethedonation Double the Donation allows Cross Site Request Forgery. This issue affects Double the Donation: from n/a through 2.0.0.	Patched by core rule	Y
CVE-2025-57927	CVE-2025-57927 - Cross-Site Request Forgery (CSRF) vulnerability in Stephanie Leary Dashboard Notepad allows Cross Si...	Cross-Site Request Forgery (CSRF) vulnerability in Stephanie Leary Dashboard Notepad allows Cross Site Request Forgery. This issue affects Dashboard Notepad: from n/a through 1.42.	Patched by core rule	Y
CVE-2025-57924	CVE-2025-57924 - Cross-Site Request Forgery (CSRF) vulnerability in Automattic Developer allows Cross Site Request Fo...	Cross-Site Request Forgery (CSRF) vulnerability in Automattic Developer allows Cross Site Request Forgery. This issue affects Developer: from n/a through 1.2.6.	Patched by core rule	Y
CVE-2025-57918	CVE-2025-57918 - Cross-Site Request Forgery (CSRF) vulnerability in ERA404 LinkedInclude allows Stored XSS. This issu...	Cross-Site Request Forgery (CSRF) vulnerability in ERA404 LinkedInclude allows Stored XSS. This issue affects LinkedInclude: from n/a through 3.0.4.	Patched by core rule	Y
CVE-2025-57915	CVE-2025-57915 - Cross-Site Request Forgery (CSRF) vulnerability in César Martín TOCHAT.BE allows Cross Site Request ...	Cross-Site Request Forgery (CSRF) vulnerability in César Martín TOCHAT.BE allows Cross Site Request Forgery. This issue affects TOCHAT.BE: from n/a through 1.3.4.	Patched by core rule	Y
CVE-2025-57914	CVE-2025-57914 - Cross-Site Request Forgery (CSRF) vulnerability in Matat Technologies Deliver via Shipos for WooComm...	Cross-Site Request Forgery (CSRF) vulnerability in Matat Technologies Deliver via Shipos for WooCommerce allows Cross Site Request Forgery. This issue affects Deliver via Shipos for WooCommerce: from n/a through 3.0.2.	Patched by core rule	Y
CVE-2025-57905	CVE-2025-57905 - Cross-Site Request Forgery (CSRF) vulnerability in Amin Y AgreeMe Checkboxes For WooCommerce allows ...	Cross-Site Request Forgery (CSRF) vulnerability in Amin Y AgreeMe Checkboxes For WooCommerce allows Cross Site Request Forgery. This issue affects AgreeMe Checkboxes For WooCommerce: from n/a through 1.1.3.	Patched by core rule	Y
CVE-2025-57902	CVE-2025-57902 - Cross-Site Request Forgery (CSRF) vulnerability in Md Taufiqur Rahman RIS Version Switcher – D...	Cross-Site Request Forgery (CSRF) vulnerability in Md Taufiqur Rahman RIS Version Switcher – Downgrade or Upgrade WP Versions Easily allows	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Cross Site Request Forgery. This issue affects RIS Version Switcher – Downgrade or Upgrade WP Versions Easily: from n/a through 1.0.		
CVE-2025-53456	CVE-2025-53456 - Cross-Site Request Forgery (CSRF) vulnerability in activewebsight SEO Backlink Monitor allows Cross ...	Cross-Site Request Forgery (CSRF) vulnerability in activewebsight SEO Backlink Monitor allows Cross Site Request Forgery. This issue affects SEO Backlink Monitor: from n/a through 1.6.0.	Patched by core rule	Y
CVE-2025-53451	CVE-2025-53451 - Cross-Site Request Forgery (CSRF) vulnerability in mihdan Mihdan: No External Links allows Cross Sit...	Cross-Site Request Forgery (CSRF) vulnerability in mihdan Mihdan: No External Links allows Cross Site Request Forgery. This issue affects Mihdan: No External Links: from n/a through 5.1.4.	Patched by core rule	Y
CVE-2025-57682	CVE-2025-57682 - Directory Traversal vulnerability in Papermark 0.20.0 and prior allows authenticated attackers to re...	Directory Traversal vulnerability in Papermark 0.20.0 and prior allows authenticated attackers to retrieve arbitrary files from an S3 bucket through its CloudFront distribution via the "POST /api/file/s3/get-presigned-get-url-proxy" API	Patched by core rule	Y
CVE-2025-9887	CVE-2025-9887 - The Custom Login And Signup Widget plugin for WordPress is vulnerable to Cross-Site Request Forgery ...	The Custom Login And Signup Widget plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing or incorrect nonce validation in the /frndzk_adminclsw.php file. This makes it possible for unauthenticated attackers to change the email and username settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-9883	CVE-2025-9883 - The Browser Sniff plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions u...	The Browser Sniff plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.3. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		granted they can trick a site administrator into performing an action such as clicking on a link.		
CVE-2025-9882	CVE-2025-9882 - The osTicket WP Bridge plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versi...	The osTicket WP Bridge plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.9.2. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-9949	CVE-2025-9949 - The Internal Links Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in all v...	The Internal Links Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.0.1. This is due to missing or incorrect nonce validation on the link deletion functionality in the process_bulk_action() function. This makes it possible for unauthenticated attackers to delete SEO links via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-43809	CVE-2025-43809 - Cross-Site Request Forgery (CSRF) vulnerability in the server (license) registration page in Liferay...	Cross-Site Request Forgery (CSRF) vulnerability in the server (license) registration page in Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.7, 2023.Q3.1 through 2023.Q3.9, 7.4 GA through update 92, and older unsupported versions allows remote attackers to register a server license via the 'orderUuid' parameter.	Patched by core rule	Y
CVE-2025-59352	CVE-2025-59352 - Dragonfly is an open source P2P-based file distribution and image acceleration system. Prior to 2.1....	Dragonfly is an open source P2P-based file distribution and image acceleration system. Prior to 2.1.0, the gRPC API and HTTP APIs allow peers to send requests that force	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the recipient peer to create files in arbitrary file system locations, and to read arbitrary files. This allows peers to steal other peers' secret data and to gain remote code execution (RCE) capabilities on the peer's machine.This vulnerability is fixed in 2.1.0.		
CVE-2025-9215	CVE-2025-9215 - The StoreEngine – Powerful WordPress eCommerce Plugin for Payments, Memberships, Affiliates, Sales &...	The StoreEngine – Powerful WordPress eCommerce Plugin for Payments, Memberships, Affiliates, Sales & More plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.5.0 via the file_download() function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	Patched by core rule	Y
CVE-2025-10188	CVE-2025-10188 - The The Hack Repair Guy's Plugin Archiver plugin for WordPress is vulnerable to Cross-Site Request F...	The The Hack Repair Guy's Plugin Archiver plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.4. This is due to missing or incorrect nonce validation on the bulk_remove() function. This makes it possible for unauthenticated attackers to arbitrary directory deletion in /wp-content via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-9891	CVE-2025-9891 - The User Sync – Remote User Sync plugin for WordPress is vulnerable to Cross-Site Request Forgery in...	The User Sync – Remote User Sync plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.2. This is due to missing or incorrect nonce validation on the mo_user_sync_form_handler() function. This makes it possible for unauthenticated attackers to deactivate the plugin via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-9629	CVE-2025-9629 - The USS Upyun plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to...	The USS Upyun plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.5.0. This is due to missing or incorrect nonce validation on the uss_setting_page function when processing the uss_set form type. This makes it possible for unauthenticated attackers to modify critical Upyun cloud storage settings including bucket name, operator credentials, upload paths, and image processing parameters via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-10050	CVE-2025-10050 - The Developer Loggers for Simple History plugin for WordPress is vulnerable to Local File Inclusion ...	The Developer Loggers for Simple History plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 0.5 via the enabled_loggers parameter. This makes it possible for authenticated attackers, with Administrator-level access and above, to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.	Patched by core rule	Y
CVE-2025-49089	CVE-2025-49089 - wangxutech MoneyPrinterTurbo 1.2.6 allows path traversal via /api/v1/download/ URIs such as /api/v1/...	wangxutech MoneyPrinterTurbo 1.2.6 allows path traversal via /api/v1/download/ URIs such as /api/v1/download//etc/passwd.	Patched by core rule	Y
CVE-2025-10176	CVE-2025-10176 - The The Hack Repair Guy's Plugin Archiver plugin for WordPress is vulnerable to arbitrary file delet...	The The Hack Repair Guy's Plugin Archiver plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the prepare_items function in all versions up to, and including, 2.0.4. This makes it possible for authenticated attackers, with Administrator-level access and above, to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).		
CVE-2025-9881	CVE-2025-9881 - The Ultimate Blogroll plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versio...	The Ultimate Blogroll plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.5.2. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-9880	CVE-2025-9880 - The Side Slide Responsive Menu plugin for WordPress is vulnerable to Cross-Site Request Forgery in a...	The Side Slide Responsive Menu plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-9693	CVE-2025-9693 - The User Meta – User Profile Builder and User management plugin plugin for WordPress is vulnerable t...	The User Meta – User Profile Builder and User management plugin plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the postInsertUserProcess function in all versions up to, and including, 3.1.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	Patched by core rule	Y
CVE-2025-9635	CVE-2025-9635 - The Analytics Reduce Bounce Rate plugin for	The Analytics Reduce Bounce Rate plugin for WordPress is vulnerable to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	WordPress is vulnerable to Cross-Site Request Forgery in...	Cross-Site Request Forgery in all versions up to, and including, 2.3. This is due to missing or incorrect nonce validation on the unbounce_options function. This makes it possible for unauthenticated attackers to modify Google Analytics tracking settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.		
CVE-2025-9634	CVE-2025-9634 - The Plugin updates blocker plugin for WordPress is vulnerable to Cross-Site Request Forgery in all v...	The Plugin updates blocker plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.2. This is due to missing or incorrect nonce validation on the pub_save action handler. This makes it possible for unauthenticated attackers to disable or enable plugin updates via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-9633	CVE-2025-9633 - The LH Signing plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up t...	The LH Signing plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.83. This is due to missing or incorrect nonce validation on the plugin_options function. This makes it possible for unauthenticated attackers to modify plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-9632	CVE-2025-9632 - The PhpList Subber plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions ...	The PhpList Subber plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1. This is due to missing or incorrect nonce validation on the bulk_action_handler function. This makes it possible for unauthenticated attackers to trigger bulk synchronization of subscription forms via a forged request granted they can trick a site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		administrator into performing an action such as clicking on a link.		
CVE-2025-9631	CVE-2025-9631 - The AutoCatSet plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up t...	The AutoCatSet plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.1.4. This is due to missing or incorrect nonce validation on the autocatset_ajax function. This makes it possible for unauthenticated attackers to trigger automatic recategorization of posts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-9628	CVE-2025-9628 - The The integration of the AMO.CRM plugin for WordPress is vulnerable to Cross-Site Request Forgery ...	The The integration of the AMO.CRM plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.1. This is due to missing or incorrect nonce validation on the settings_page function. This makes it possible for unauthenticated attackers to modify critical API connection settings including the AMO.CRM API URL, login credentials, and API hash key via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-9627	CVE-2025-9627 - The Run Log plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, ...	The Run Log plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.7.10. This is due to missing or incorrect nonce validation on the oirl_plugin_options function. This makes it possible for unauthenticated attackers to modify plugin settings including distance units, pace display preferences, style themes, and display positions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-9623	CVE-2025-9623 - The Admin in English with Switch plugin for WordPress is vulnerable	The Admin in English with Switch plugin for WordPress is vulnerable to Cross-Site Request Forgery	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	to Cross-Site Request Forgery in...	in all versions up to, and including, 1.1. This is due to missing or incorrect nonce validation on the enable_eng function. This makes it possible for unauthenticated attackers to modify administrator language settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.		
CVE-2025-9620	CVE-2025-9620 - The Seo Monster plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up ...	The Seo Monster plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.3.3. This is due to missing or incorrect nonce validation on the check_integration() function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-9617	CVE-2025-9617 - The Publish approval plugin for WordPress is vulnerable to Cross-Site Request Forgery in all version...	The Publish approval plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1. This is due to missing or incorrect nonce validation on the publish_save_option function. This makes it possible for unauthenticated attackers to modify plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-8481	CVE-2025-8481 - The Blog Designer For Elementor – Post Slider, Post Carousel, Post Grid plugin for WordPress is vuln...	The Blog Designer For Elementor – Post Slider, Post Carousel, Post Grid plugin for WordPress is vulnerable to Cross-Site Request Forgery in version 1.1.7. This is due to missing or incorrect nonce validation on the bdfe_install_activate_rswpbs_only function. This makes it possible for unauthenticated attackers to install the 'rs-wp-books-showcase' plugin via a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		forged request granted they can trick a site administrator into performing an action such as clicking on a link.		
CVE-2025-8479	CVE-2025-8479 - The Zoho Flow plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, an...	The Zoho Flow plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.14.1. This is due to missing or incorrect nonce validation on the zoho_flow_deactivate_plugin function. This makes it possible for unauthenticated attackers to modify typography settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-10236	CVE-2025-10236 - A vulnerability has been found in binary-husky gpt_academic up to 3.91. Impacted is the function mer...	A vulnerability has been found in binary-husky gpt_academic up to 3.91. Impacted is the function merge_tex_files_ of the file crazy_functions/latex_fns/latex_toolbox.py of the component LaTeX File Handler. Such manipulation of the argument \input{} leads to path traversal. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-10233	CVE-2025-10233 - A security vulnerability has been detected in kalcaddle kodbox 1.61. This affects the function fileG...	A security vulnerability has been detected in kalcaddle kodbox 1.61. This affects the function fileGet/fileSave of the file app/controller/explorer/editor.class.php. The manipulation of the argument path leads to path traversal. The attack can be initiated remotely. The exploit has been disclosed publicly 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-2025-10232	CVE-2025-10232 - A weakness has been identified in 299ko up to 2.0.0. Affected by this issue is the function	A weakness has been identified in 299ko up to 2.0.0. Affected by this issue is the function getSentDir/delete of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	getSentD...	file plugin/filemanager/controllers/FileManagerAPIController.php. Executing manipulation can lead to path traversal. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-29592	CVE-2025-29592 - oasys v1.1 is vulnerable to Directory Traversal in ProcedureController.	oasys v1.1 is vulnerable to Directory Traversal in ProcedureController.	Patched by core rule	Y
CVE-2025-9888	CVE-2025-9888 - The Maspik – Ultimate Spam Protection plugin for WordPress is vulnerable to Cross-Site Request Forge...	The Maspik – Ultimate Spam Protection plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.5.6. This is due to missing or incorrect nonce validation on the clear_log function. This makes it possible for unauthenticated attackers to clear all spam logs via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-9622	CVE-2025-9622 - The WP Blast | SEO & Performance Booster plugin for WordPress is vulnerable to Cross-Site Request Fo...	The WP Blast | SEO & Performance Booster plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.8.6. This is due to missing or incorrect nonce validation on multiple administrative actions in the Settings class. This makes it possible for unauthenticated attackers to trigger cache purging, sitemap clearing, plugin data purging, and score resetting operations via forged requests granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-58997	CVE-2025-58997 - Cross-Site Request Forgery (CSRF) vulnerability in Frenify Mow allows Code Injection. This issue aff...	Cross-Site Request Forgery (CSRF) vulnerability in Frenify Mow allows Code Injection. This issue affects Mow: from n/a through 4.10.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-58991	CVE-2025-58991 - Cross-Site Request Forgery (CSRF) vulnerability in Cristiano Zanca WooCommerce Booking Bundle Hours ...	Cross-Site Request Forgery (CSRF) vulnerability in Cristiano Zanca WooCommerce Booking Bundle Hours allows Stored XSS. This issue affects WooCommerce Booking Bundle Hours: from n/a through 0.7.4.	Patched by core rule	Y
CVE-2025-58975	CVE-2025-58975 - Cross-Site Request Forgery (CSRF) vulnerability in Helmut Wandl Advanced Settings allows Cross Site ...	Cross-Site Request Forgery (CSRF) vulnerability in Helmut Wandl Advanced Settings allows Cross Site Request Forgery. This issue affects Advanced Settings: from n/a through 3.1.1.	Patched by core rule	Y
CVE-2024-48341	CVE-2024-48341 - dingfanzu CMS V1.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /...	dingfanzu CMS V1.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/doAdminAction.php?act=addShop	Patched by core rule	Y
CVE-2025-48317	CVE-2025-48317 - Path Traversal vulnerability in Stefan Keller WooCommerce Payment Gateway for Saferpay allows Path T...	Path Traversal vulnerability in Stefan Keller WooCommerce Payment Gateway for Saferpay allows Path Traversal. This issue affects WooCommerce Payment Gateway for Saferpay: from n/a through 0.4.9.	Patched by core rule	Y
CVE-2025-48104	CVE-2025-48104 - Cross-Site Request Forgery (CSRF) vulnerability in ericzane Floating Window Music Player allows Stor...	Cross-Site Request Forgery (CSRF) vulnerability in ericzane Floating Window Music Player allows Stored XSS. This issue affects Floating Window Music Player: from n/a through 3.4.2.	Patched by core rule	Y
CVE-2025-27003	CVE-2025-27003 - Cross-Site Request Forgery (CSRF) vulnerability in fullworks Quick Paypal Payments allows Cross Site...	Cross-Site Request Forgery (CSRF) vulnerability in fullworks Quick Paypal Payments allows Cross Site Request Forgery. This issue affects Quick Paypal Payments: from n/a through 5.7.46.	Patched by core rule	Y
CVE-2025-58878	CVE-2025-58878 - Cross-Site Request Forgery (CSRF) vulnerability in usamafarooq Woocommerce Gifts Product allows Cros...	Cross-Site Request Forgery (CSRF) vulnerability in usamafarooq Woocommerce Gifts Product allows Cross Site Request Forgery. This issue affects Woocommerce Gifts Product: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-58869	CVE-2025-58869 - Cross-Site Request Forgery (CSRF) vulnerability in Simasicher SimaCookie allows Stored XSS. This iss...	Cross-Site Request Forgery (CSRF) vulnerability in Simasicher SimaCookie allows Stored XSS. This issue affects SimaCookie: from n/a through 1.3.2.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-58865	CVE-2025-58865 - Cross-Site Request Forgery (CSRF) vulnerability in reimund Compact Admin allows Cross Site Request F...	Cross-Site Request Forgery (CSRF) vulnerability in reimund Compact Admin allows Cross Site Request Forgery. This issue affects Compact Admin: from n/a through 1.3.0.	Patched by core rule	Y
CVE-2025-58861	CVE-2025-58861 - Cross-Site Request Forgery (CSRF) vulnerability in WP Corner Quick Event Calendar allows Stored XSS....	Cross-Site Request Forgery (CSRF) vulnerability in WP Corner Quick Event Calendar allows Stored XSS. This issue affects Quick Event Calendar: from n/a through 1.4.9.	Patched by core rule	Y
CVE-2025-58860	CVE-2025-58860 - Cross-Site Request Forgery (CSRF) vulnerability in KaizenCoders Enable Latex allows Stored XSS. This...	Cross-Site Request Forgery (CSRF) vulnerability in KaizenCoders Enable Latex allows Stored XSS. This issue affects Enable Latex: from n/a through 1.2.16.	Patched by core rule	Y
CVE-2025-58859	CVE-2025-58859 - Cross-Site Request Forgery (CSRF) vulnerability in David Merinas Add to Feedly allows Stored XSS. Th...	Cross-Site Request Forgery (CSRF) vulnerability in David Merinas Add to Feedly allows Stored XSS. This issue affects Add to Feedly: from n/a through 1.2.11.	Patched by core rule	Y
CVE-2025-58856	CVE-2025-58856 - Cross-Site Request Forgery (CSRF) vulnerability in ablancodev Woocommerce Notify Updated Product all...	Cross-Site Request Forgery (CSRF) vulnerability in ablancodev Woocommerce Notify Updated Product allows Stored XSS. This issue affects Woocommerce Notify Updated Product: from n/a through 1.6.	Patched by core rule	Y
CVE-2025-58854	CVE-2025-58854 - Cross-Site Request Forgery (CSRF) vulnerability in Samer Bechara Ultimate AJAX Login allows Reflecte...	Cross-Site Request Forgery (CSRF) vulnerability in Samer Bechara Ultimate AJAX Login allows Reflected XSS. This issue affects Ultimate AJAX Login: from n/a through 1.2.1.	Patched by core rule	Y
CVE-2025-58853	CVE-2025-58853 - Cross-Site Request Forgery (CSRF) vulnerability in OTWthemes Popping Sidebars and Widgets Light allo...	Cross-Site Request Forgery (CSRF) vulnerability in OTWthemes Popping Sidebars and Widgets Light allows Reflected XSS. This issue affects Popping Sidebars and Widgets Light: from n/a through 1.27.	Patched by core rule	Y
CVE-2025-58852	CVE-2025-58852 - Cross-Site Request Forgery (CSRF) vulnerability in Mark O'Donnell MSTW League Manager allows Stored ...	Cross-Site Request Forgery (CSRF) vulnerability in Mark O'Donnell MSTW League Manager allows Stored XSS. This issue affects MSTW League Manager: from n/a through 2.10.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-58849	CVE-2025-58849 - Cross-Site Request Forgery (CSRF) vulnerability in Deepak S Hide Real Download Path allows Stored XS...	Cross-Site Request Forgery (CSRF) vulnerability in Deepak S Hide Real Download Path allows Stored XSS. This issue affects Hide Real Download Path: from n/a through 1.6.	Patched by core rule	Y
CVE-2025-58848	CVE-2025-58848 - Cross-Site Request Forgery (CSRF) vulnerability in aakash1911 WP likes allows Reflected XSS. This is...	Cross-Site Request Forgery (CSRF) vulnerability in aakash1911 WP likes allows Reflected XSS. This issue affects WP likes: from n/a through 3.1.1.	Patched by core rule	Y
CVE-2025-58847	CVE-2025-58847 - Cross-Site Request Forgery (CSRF) vulnerability in Yaidier WN Flipbox Pro allows Reflected XSS. This...	Cross-Site Request Forgery (CSRF) vulnerability in Yaidier WN Flipbox Pro allows Reflected XSS. This issue affects WN Flipbox Pro: from n/a through 2.1.	Patched by core rule	Y
CVE-2025-58846	CVE-2025-58846 - Cross-Site Request Forgery (CSRF) vulnerability in Dejan Markovic WordPress Buffer – HYPESocial. Soc...	Cross-Site Request Forgery (CSRF) vulnerability in Dejan Markovic WordPress Buffer – HYPESocial. Social Media Auto Post, Social Media Auto Publish and Schedule allows Reflected XSS. This issue affects WordPress Buffer – HYPESocial. Social Media Auto Post, Social Media Auto Publish and Schedule: from n/a through 2020.1.0.	Patched by core rule	Y
CVE-2025-58845	CVE-2025-58845 - Cross-Site Request Forgery (CSRF) vulnerability in ChrisHurst Bulk Watermark allows Reflected XSS. T...	Cross-Site Request Forgery (CSRF) vulnerability in ChrisHurst Bulk Watermark allows Reflected XSS. This issue affects Bulk Watermark: from n/a through 1.6.10.	Patched by core rule	Y
CVE-2025-58844	CVE-2025-58844 - Cross-Site Request Forgery (CSRF) vulnerability in Subhash Kumar Database to Excel allows Stored XSS...	Cross-Site Request Forgery (CSRF) vulnerability in Subhash Kumar Database to Excel allows Stored XSS. This issue affects Database to Excel: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-58843	CVE-2025-58843 - Cross-Site Request Forgery (CSRF) vulnerability in David Merinas Auto Last Youtube Video allows Stor...	Cross-Site Request Forgery (CSRF) vulnerability in David Merinas Auto Last Youtube Video allows Stored XSS. This issue affects Auto Last Youtube Video: from n/a through 1.0.7.	Patched by core rule	Y
CVE-2025-58833	CVE-2025-58833 - Cross-Site Request Forgery (CSRF) vulnerability in INVELITY Invelity MyGLS connect allows Object Inj...	Cross-Site Request Forgery (CSRF) vulnerability in INVELITY Invelity MyGLS connect allows Object Injection. This issue affects Invelity MyGLS connect: from n/a through 1.1.1.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-58831	CVE-2025-58831 - Cross-Site Request Forgery (CSRF) vulnerability in snagysandor Parallax Scrolling Enllax.js allows C...	Cross-Site Request Forgery (CSRF) vulnerability in snagysandor Parallax Scrolling Enllax.js allows Cross Site Request Forgery. This issue affects Parallax Scrolling Enllax.js: from n/a through 0.0.6.	Patched by core rule	Y
CVE-2025-58818	CVE-2025-58818 - Cross-Site Request Forgery (CSRF) vulnerability in SwiftNinjaPro Developer Tools Blocker allows Cros...	Cross-Site Request Forgery (CSRF) vulnerability in SwiftNinjaPro Developer Tools Blocker allows Cross Site Request Forgery. This issue affects Developer Tools Blocker: from n/a through 3.2.1.	Patched by core rule	Y
CVE-2025-58809	CVE-2025-58809 - Cross-Site Request Forgery (CSRF) vulnerability in Nick Ciske To Lead For Salesforce allows Reflecte...	Cross-Site Request Forgery (CSRF) vulnerability in Nick Ciske To Lead For Salesforce allows Reflected XSS. This issue affects To Lead For Salesforce: from n/a through 2.7.3.9.	Patched by core rule	Y
CVE-2025-58807	CVE-2025-58807 - Cross-Site Request Forgery (CSRF) vulnerability in Dsingh Purge Varnish Cache allows Stored XSS. Thi...	Cross-Site Request Forgery (CSRF) vulnerability in Dsingh Purge Varnish Cache allows Stored XSS. This issue affects Purge Varnish Cache: from n/a through 2.6.	Patched by core rule	Y
CVE-2025-58806	CVE-2025-58806 - Cross-Site Request Forgery (CSRF) vulnerability in imjoehaines WordPress Error Monitoring by Bugsnag...	Cross-Site Request Forgery (CSRF) vulnerability in imjoehaines WordPress Error Monitoring by Bugsnag allows Stored XSS. This issue affects WordPress Error Monitoring by Bugsnag: from n/a through 1.6.3.	Patched by core rule	Y
CVE-2025-58804	CVE-2025-58804 - Cross-Site Request Forgery (CSRF) vulnerability in brijrajs WooCommerce Single Page Checkout allows ...	Cross-Site Request Forgery (CSRF) vulnerability in brijrajs WooCommerce Single Page Checkout allows Cross Site Request Forgery. This issue affects WooCommerce Single Page Checkout: from n/a through 1.2.7.	Patched by core rule	Y
CVE-2025-58802	CVE-2025-58802 - Cross-Site Request Forgery (CSRF) vulnerability in michalzagdan TrustMate.io – WooCommerce integrati...	Cross-Site Request Forgery (CSRF) vulnerability in michalzagdan TrustMate.io – WooCommerce integration allows Cross Site Request Forgery. This issue affects TrustMate.io – WooCommerce integration: from n/a through 1.14.0.	Patched by core rule	Y
CVE-2025-58801	CVE-2025-58801 - Cross-Site Request Forgery (CSRF) vulnerability in KCS Responder allows	Cross-Site Request Forgery (CSRF) vulnerability in KCS Responder allows Cross Site Request Forgery. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Cross Site Request Forgery. ...	issue affects Responder: from n/a through 4.3.8.		
CVE-2025-58800	CVE-2025-58800 - Cross-Site Request Forgery (CSRF) vulnerability in Steve Truman WP Email Template allows Cross Site ...	Cross-Site Request Forgery (CSRF) vulnerability in Steve Truman WP Email Template allows Cross Site Request Forgery. This issue affects WP Email Template: from n/a through 2.8.3.	Patched by core rule	Y
CVE-2025-58799	CVE-2025-58799 - Cross-Site Request Forgery (CSRF) vulnerability in themelocation Custom WooCommerce Checkout Fields ...	Cross-Site Request Forgery (CSRF) vulnerability in themelocation Custom WooCommerce Checkout Fields Editor allows Cross Site Request Forgery. This issue affects Custom WooCommerce Checkout Fields Editor: from n/a through 1.3.4.	Patched by core rule	Y
CVE-2025-58798	CVE-2025-58798 - Cross-Site Request Forgery (CSRF) vulnerability in Bjorn Manintveld BCM Duplicate Menu allows Cross ...	Cross-Site Request Forgery (CSRF) vulnerability in Bjorn Manintveld BCM Duplicate Menu allows Cross Site Request Forgery. This issue affects BCM Duplicate Menu: from n/a through 1.1.2.	Patched by core rule	Y
CVE-2025-58794	CVE-2025-58794 - Cross-Site Request Forgery (CSRF) vulnerability in rainafarai Notification for Telegram allows Cross...	Cross-Site Request Forgery (CSRF) vulnerability in rainafarai Notification for Telegram allows Cross Site Request Forgery. This issue affects Notification for Telegram: from n/a through 3.4.6.	Patched by core rule	Y
CVE-2025-58792	CVE-2025-58792 - Cross-Site Request Forgery (CSRF) vulnerability in WPKube Authors List allows Cross Site Request For...	Cross-Site Request Forgery (CSRF) vulnerability in WPKube Authors List allows Cross Site Request Forgery. This issue affects Authors List: from n/a through 2.0.6.1.	Patched by core rule	Y
CVE-2025-9616	CVE-2025-9616 - The PopAd plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, an...	The PopAd plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.4. This is due to missing or incorrect nonce validation on the PopAd_reset_cookie_time function. This makes it possible for unauthenticated attackers to reset cookie time settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-58611	CVE-2025-58611 - Cross-Site Request Forgery (CSRF) vulnerability in Tickera Tickera allows Cross Site Request Forgery...	Cross-Site Request Forgery (CSRF) vulnerability in Tickera Tickera allows Cross Site Request Forgery. This issue affects Tickera: from n/a through 3.5.5.6.	Patched by core rule	Y
CVE-2025-9618	CVE-2025-9618 - The Related Posts Lite plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versi...	The Related Posts Lite plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.12. This is due to missing or incorrect nonce validation on the settings update functionality. This makes it possible for unauthenticated attackers to modify plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-4956	CVE-2025-4956 - Path Traversal: '.../...//' vulnerability in AA-Team Pro Bulk Watermark Plugin for WordPress allows ...	Path Traversal: '.../...//' vulnerability in AA-Team Pro Bulk Watermark Plugin for WordPress allows Path Traversal.This issue affects Pro Bulk Watermark Plugin for WordPress: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-9650	CVE-2025-9650 - A vulnerability has been found in yeqifu carRental up to 3fabb7eae93d209426638863980301d6f99866b3. T...	A vulnerability has been found in yeqifu carRental up to 3fabb7eae93d209426638863980301d6f99866b3. This affects the function removeFileByPath of the file src/main/java/com/yeqifu/sys/utils/AppFileUtils.java. The manipulation of the argument carimg leads to path traversal. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. This product adopts a rolling release strategy to maintain continuous delivery	Patched by core rule	Y
CVE-2025-54029	CVE-2025-54029 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in exte...	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in extendons WooCommerce csv import export allows Path Traversal. This issue affects WooCommerce csv import export: from n/a through 2.0.6.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-53588	CVE-2025-53588 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Dmit...	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Dmitry V. (CEO of "UKR Solution") UPC/EAN/GTIN Code Generator allows Path Traversal. This issue affects UPC/EAN/GTIN Code Generator: from n/a through 2.0.2.	Patched by core rule	Y
CVE-2025-48363	CVE-2025-48363 - Cross-Site Request Forgery (CSRF) vulnerability in Metin Saraç Popup for CF7 with Sweet Alert allows...	Cross-Site Request Forgery (CSRF) vulnerability in Metin Saraç Popup for CF7 with Sweet Alert allows Cross Site Request Forgery. This issue affects Popup for CF7 with Sweet Alert: from n/a through 1.6.5.	Patched by core rule	Y
CVE-2025-48362	CVE-2025-48362 - Cross-Site Request Forgery (CSRF) vulnerability in Saeed Sattar Beglou Hesabfa Accounting allows Cro...	Cross-Site Request Forgery (CSRF) vulnerability in Saeed Sattar Beglou Hesabfa Accounting allows Cross Site Request Forgery. This issue affects Hesabfa Accounting: from n/a through 2.2.4.	Patched by core rule	Y
CVE-2025-48359	CVE-2025-48359 - Cross-Site Request Forgery (CSRF) vulnerability in thaihavnn07 ATT YouTube Widget allows Stored XSS....	Cross-Site Request Forgery (CSRF) vulnerability in thaihavnn07 ATT YouTube Widget allows Stored XSS. This issue affects ATT YouTube Widget: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-48357	CVE-2025-48357 - Cross-Site Request Forgery (CSRF) vulnerability in Theme Century Century ToolKit allows Cross Site R...	Cross-Site Request Forgery (CSRF) vulnerability in Theme Century Century ToolKit allows Cross Site Request Forgery. This issue affects Century ToolKit: from n/a through 1.2.1.	Patched by core rule	Y
CVE-2025-48353	CVE-2025-48353 - Cross-Site Request Forgery (CSRF) vulnerability in dactum Clickbank WordPress Plugin (Niche Storefro...	Cross-Site Request Forgery (CSRF) vulnerability in dactum Clickbank WordPress Plugin (Niche Storefront) allows Stored XSS. This issue affects Clickbank WordPress Plugin (Niche Storefront): from n/a through 1.3.5.	Patched by core rule	Y
CVE-2025-48351	CVE-2025-48351 - Cross-Site Request Forgery (CSRF) vulnerability in PluginsPoint Kento Splash Screen allows Stored XS...	Cross-Site Request Forgery (CSRF) vulnerability in PluginsPoint Kento Splash Screen allows Stored XSS. This issue affects Kento Splash Screen: from n/a through 1.4.	Patched by core rule	Y
CVE-2025-48343	CVE-2025-48343 - Cross-Site Request Forgery (CSRF) vulnerability in Aaron Axelsen WPMU Ldap Authentication	Cross-Site Request Forgery (CSRF) vulnerability in Aaron Axelsen WPMU Ldap Authentication allows Stored XSS. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	allows Sto...	issue affects WPMU Ldap Authentication: from n/a through 5.0.1.		
CVE-2025-48325	CVE-2025-48325 - Cross-Site Request Forgery (CSRF) vulnerability in shmish111 WP Admin Theme allows Stored XSS. This ...	Cross-Site Request Forgery (CSRF) vulnerability in shmish111 WP Admin Theme allows Stored XSS. This issue affects WP Admin Theme: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-48321	CVE-2025-48321 - Cross-Site Request Forgery (CSRF) vulnerability in dyiosah Ultimate twitter profile widget allows St...	Cross-Site Request Forgery (CSRF) vulnerability in dyiosah Ultimate twitter profile widget allows Stored XSS. This issue affects Ultimate twitter profile widget: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-48320	CVE-2025-48320 - Cross-Site Request Forgery (CSRF) vulnerability in cuckoohello 百度分享按钮 allows Stored XSS. This issue ...	Cross-Site Request Forgery (CSRF) vulnerability in cuckoohello 百度分享按钮 allows Stored XSS. This issue affects 百度分享按钮: from n/a through 1.0.6.	Patched by core rule	Y
CVE-2025-48318	CVE-2025-48318 - Cross-Site Request Forgery (CSRF) vulnerability in shen2 多说社会化评论框 allows Cross Site Request Forgery....	Cross-Site Request Forgery (CSRF) vulnerability in shen2 多说社会化评论框 allows Cross Site Request Forgery. This issue affects 多说社会化评论框: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-48311	CVE-2025-48311 - Cross-Site Request Forgery (CSRF) vulnerability in OffClicks Invisible Optin allows Stored XSS. This...	Cross-Site Request Forgery (CSRF) vulnerability in OffClicks Invisible Optin allows Stored XSS. This issue affects Invisible Optin: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-48310	CVE-2025-48310 - Cross-Site Request Forgery (CSRF) vulnerability in wptableeditor Table Editor allows Cross Site Requ...	Cross-Site Request Forgery (CSRF) vulnerability in wptableeditor Table Editor allows Cross Site Request Forgery. This issue affects Table Editor: from n/a through 1.6.4.	Patched by core rule	Y
CVE-2025-48309	CVE-2025-48309 - Cross-Site Request Forgery (CSRF) vulnerability in web-able BetPress allows Stored XSS. This issue a...	Cross-Site Request Forgery (CSRF) vulnerability in web-able BetPress allows Stored XSS. This issue affects BetPress: from n/a through 1.0.1 Lite.	Patched by core rule	Y
CVE-2025-48308	CVE-2025-48308 - Cross-Site Request Forgery (CSRF) vulnerability in nonletter Newsletter subscription optin module al...	Cross-Site Request Forgery (CSRF) vulnerability in nonletter Newsletter subscription optin module allows Stored XSS. This issue affects Newsletter subscription optin module:	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		from n/a through 1.2.9.		
CVE-2025-48307	CVE-2025-48307 - Cross-Site Request Forgery (CSRF) vulnerability in kasonzhao SEO For Images allows Stored XSS. This ...	Cross-Site Request Forgery (CSRF) vulnerability in kasonzhao SEO For Images allows Stored XSS. This issue affects SEO For Images: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-48306	CVE-2025-48306 - Cross-Site Request Forgery (CSRF) vulnerability in developers savyour Savyour Affiliate Partner allo...	Cross-Site Request Forgery (CSRF) vulnerability in developers savyour Savyour Affiliate Partner allows Stored XSS. This issue affects Savyour Affiliate Partner: from n/a through 2.1.4.	Patched by core rule	Y
CVE-2025-48304	CVE-2025-48304 - Cross-Site Request Forgery (CSRF) vulnerability in Gary Illyes Google XML News Sitemap plugin allows...	Cross-Site Request Forgery (CSRF) vulnerability in Gary Illyes Google XML News Sitemap plugin allows Stored XSS. This issue affects Google XML News Sitemap plugin: from n/a through 0.02.	Patched by core rule	Y
CVE-2025-48109	CVE-2025-48109 - Cross-Site Request Forgery (CSRF) vulnerability in Xavier Media XM-Backup allows Stored XSS. This is...	Cross-Site Request Forgery (CSRF) vulnerability in Xavier Media XM-Backup allows Stored XSS. This issue affects XM-Backup: from n/a through 0.9.1.	Patched by core rule	Y
CVE-2025-9345	CVE-2025-9345 - The File Manager, Code Editor, and Backup by Managefy plugin for WordPress is vulnerable to Path Tra...	The File Manager, Code Editor, and Backup by Managefy plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.4.8 via the ajax_downloadfile() function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to perform actions on files outside of the originally intended directory.	Patched by core rule	Y
CVE-2025-7812	CVE-2025-7812 - The Video Share VOD – Turnkey Video Site Builder Script plugin for WordPress is vulnerable to Cross-...	The Video Share VOD – Turnkey Video Site Builder Script plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.7.6. This is due to missing or incorrect nonce validation on the adminExport() function. This makes it possible for unauthenticated attackers to update settings and execute remote code when the Server command execution setting is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		enabled via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.		
CVE-2024-13981	CVE-2024-13981 - LiveBOS, an object-oriented business architecture middleware suite developed by Apex Software Co., L...	LiveBOS, an object-oriented business architecture middleware suite developed by Apex Software Co., Ltd., contains an arbitrary file upload vulnerability in its UploadFile.do;.js.jsp endpoint. This flaw affects the LiveBOS Server component and allows unauthenticated remote attackers to upload crafted files outside the intended directory structure via path traversal in the filename parameter. Successful exploitation may lead to remote code execution on the server, enabling full system compromise. The vulnerability is presumed to affect builds released prior to August 2024 and is said to be remediated in newer versions of the product, though the exact affected range remains undefined. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-08-23 UTC.	Patched by core rule	Y
CVE-2025-58217	CVE-2025-58217 - Cross-Site Request Forgery (CSRF) vulnerability in GeroNikolov Instant Breaking News allows Stored X...	Cross-Site Request Forgery (CSRF) vulnerability in GeroNikolov Instant Breaking News allows Stored XSS. This issue affects Instant Breaking News: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-58202	CVE-2025-58202 - Cross-Site Request Forgery (CSRF) vulnerability in Plugins and Snippets Simple Page Access Restricti...	Cross-Site Request Forgery (CSRF) vulnerability in Plugins and Snippets Simple Page Access Restriction allows Cross Site Request Forgery. This issue affects Simple Page Access Restriction: from n/a through 1.0.32.	Patched by core rule	Y
CVE-2025-54598	CVE-2025-54598 - The Bevy Event service through 2025-07-22, as used for eBay Seller Events and other activities, allo...	The Bevy Event service through 2025-07-22, as used for eBay Seller Events and other activities, allows CSRF to delete all notifications via the /notifications/delete/ URI.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-48081	CVE-2025-48081 - Path Traversal: '.../...//' vulnerability in Printeers Printeers Print & Ship allows Path Traversal....	Path Traversal: '.../...//' vulnerability in Printeers Printeers Print & Ship allows Path Traversal.This issue affects Printeers Print & Ship: from n/a through 1.17.0.	Patched by core rule	Y
CVE-2025-49040	CVE-2025-49040 - Cross-Site Request Forgery (CSRF) vulnerability in Backup Bolt allows Cross Site Request Forgery.Thi...	Cross-Site Request Forgery (CSRF) vulnerability in Backup Bolt allows Cross Site Request Forgery.This issue affects Backup Bolt: from n/a through 1.4.1.	Patched by core rule	Y
CVE-2025-50971	CVE-2025-50971 - Directory traversal vulnerability in AbanteCart version 1.4.2 allows unauthenticated attackers to ga...	Directory traversal vulnerability in AbanteCart version 1.4.2 allows unauthenticated attackers to gain access to sensitive system files via the template parameter to index.php.	Patched by core rule	Y

Server-side Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-58962	CVE-2025-58962 - Server-Side Request Forgery (SSRF) vulnerability in publitio Publitio allows Server Side Request For...	Server-Side Request Forgery (SSRF) vulnerability in publitio Publitio allows Server Side Request Forgery. This issue affects Publitio: from n/a through 2.2.1.	Patched by core rule	Y
CVE-2025-58011	CVE-2025-58011 - Server-Side Request Forgery (SSRF) vulnerability in Alex Content Mask allows Server Side Request For...	Server-Side Request Forgery (SSRF) vulnerability in Alex Content Mask allows Server Side Request Forgery. This issue affects Content Mask: from n/a through 1.8.5.2.	Patched by core rule	Y
CVE-2025-58005	CVE-2025-58005 - Server-Side Request Forgery (SSRF) vulnerability in SmartDataSoft DriCub allows Server Side Request ...	Server-Side Request Forgery (SSRF) vulnerability in SmartDataSoft DriCub allows Server Side Request Forgery. This issue affects DriCub: from n/a through 2.9.	Patched by core rule	Y
CVE-2025-57984	CVE-2025-57984 - Server-Side Request Forgery (SSRF) vulnerability in Pratik Ghela MakeStories (for Google Web Stories...	Server-Side Request Forgery (SSRF) vulnerability in Pratik Ghela MakeStories (for Google Web Stories) allows Server Side Request Forgery. This issue affects MakeStories (for Google Web Stories): from n/a through 3.0.4.	Patched by core rule	Y
CVE-2025-57943	CVE-2025-57943 - Server-Side Request Forgery (SSRF) vulnerability in Skimlinks Skimlinks Affiliate Marketing Tool all...	Server-Side Request Forgery (SSRF) vulnerability in Skimlinks Skimlinks Affiliate Marketing Tool allows Server Side Request Forgery. This issue affects Skimlinks Affiliate Marketing Tool: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-53461	CVE-2025-53461 - Server-Side Request Forgery (SSRF) vulnerability in Binsaifullah Beaf allows Server Side Request For...	Server-Side Request Forgery (SSRF) vulnerability in Binsaifullah Beaf allows Server Side Request Forgery. This issue affects Beaf: from n/a through 1.6.2.	Patched by core rule	Y
CVE-2025-53457	CVE-2025-53457 - Server-Side Request Forgery (SSRF) vulnerability in activewebsight SEO Backlink Monitor allows Serve...	Server-Side Request Forgery (SSRF) vulnerability in activewebsight SEO Backlink Monitor allows Server Side Request Forgery. This issue affects SEO Backlink Monitor: from n/a through 1.6.0.	Patched by core rule	Y
CVE-2025-10764	CVE-2025-10764 - A vulnerability was identified in SeriaWei ZKEACMS up to 4.3. This affects the function Edit of the ...	A vulnerability was identified in SeriaWei ZKEACMS up to 4.3. This affects the function Edit of the file src/ZKEACMS.EventAction/Controllers/PendingTaskController.cs of the component Event Action System. Such manipulation of the argument Data leads to server-side request forgery. The attack may be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		performed from remote. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-10760	CVE-2025-10760 - A flaw has been found in Harness 3.3.0. This impacts the function LookupRepo of the file app/api/con...	A flaw has been found in Harness 3.3.0. This impacts the function LookupRepo of the file app/api/controller/gitspace/lookup_repo.go. Executing manipulation of the argument url can lead to server-side request forgery. The attack may be launched remotely. The exploit has been published 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-2025-59346	CVE-2025-59346 - Dragonfly is an open source P2P-based file distribution and image acceleration system. Versions prio...	Dragonfly is an open source P2P-based file distribution and image acceleration system. Versions prior to 2.1.0 contain a server-side request forgery (SSRF) vulnerability that enables users to force DragonFly2's components to make requests to internal services that are otherwise not accessible to them. The issue arises because the Manager API accepts a user-supplied URL when creating a Preheat job with weak validation, peers can trigger other peers to fetch an arbitrary URL through pieceManager.DownloadSource, and internal HTTP clients follow redirects, allowing a request to a malicious server to be redirected to internal services. This can be used to probe or access internal HTTP endpoints. The vulnerability is fixed in version 2.1.0.	Patched by core rule	Y
CVE-2025-57055	CVE-2025-57055 - WonderCMS 3.5.0 is vulnerable to Server-Side Request Forgery (SSRF) in the custom module installatio...	WonderCMS 3.5.0 is vulnerable to Server-Side Request Forgery (SSRF) in the custom module installation functionality. An authenticated administrator can supply a malicious URL via the pluginThemeUrl POST parameter. The server fetches the provided URL using curl_exec() without sufficient validation, allowing the attacker to force internal or external	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		HTTP requests.		
CVE-2025-10471	CVE-2025-10471 - A vulnerability was detected in ZKEACMS 4.3. Impacted is the function Proxy of the file src/ZKEACMS/...	A vulnerability was detected in ZKEACMS 4.3. Impacted is the function Proxy of the file src/ZKEACMS/Controllers/MediaController.cs. Performing manipulation of the argument url results in server-side request forgery. It is possible to initiate the attack remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-10397	CVE-2025-10397 - A vulnerability was identified in Magicblack MacCMS 2025.1000.4050. This affects an unknown part of ...	A vulnerability was identified in Magicblack MacCMS 2025.1000.4050. This affects an unknown part of the component API Handler. The manipulation of the argument cjurl leads to server-side request forgery. The attack can be initiated remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2025-10395	CVE-2025-10395 - A vulnerability was found in Magicblack MacCMS 2025.1000.4050. Affected by this vulnerability is the...	A vulnerability was found in Magicblack MacCMS 2025.1000.4050. Affected by this vulnerability is the function col_url of the component Scheduled Task Handler. Performing manipulation of the argument cjurl results in server-side request forgery. It is possible to initiate the attack remotely.	Patched by core rule	Y
CVE-2025-10391	CVE-2025-10391 - A security vulnerability has been detected in CRMEB up to 5.6.1. The impacted element is the functio...	A security vulnerability has been detected in CRMEB up to 5.6.1. The impacted element is the function testOutUrl of the file app/services/out/OutAccountServices.php. The manipulation of the argument push_token_url leads to server-side request forgery. Remote exploitation of the attack is possible. The exploit has been disclosed publicly 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-2025-10329	CVE-2025-10329 - A vulnerability was detected in cdevroe unmark up to 1.9.3. This affects an unknown part of the file...	A vulnerability was detected in cdevroe unmark up to 1.9.3. This affects an unknown part of the file /application/controllers/Marks.php. The manipulation of the argument url results in server-side request forgery. The attack may be launched	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-10211	CVE-2025-10211 - A security vulnerability has been detected in yanyutao0402 ChanCMS 3.3.0. The affected element is th...	A security vulnerability has been detected in yanyutao0402 ChanCMS 3.3.0. The affected element is the function CollectController of the file /cms/collect/getArticle. The manipulation of the argument taskUrl leads to server-side request forgery. The attack may be initiated remotely. The exploit has been disclosed publicly 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-2025-58977	CVE-2025-58977 - Server-Side Request Forgery (SSRF) vulnerability in Rhys Wynne WP eBay Product Feeds allows Server S...	Server-Side Request Forgery (SSRF) vulnerability in Rhys Wynne WP eBay Product Feeds allows Server Side Request Forgery. This issue affects WP eBay Product Feeds: from n/a through 3.4.8.	Patched by core rule	Y
CVE-2025-49430	CVE-2025-49430 - Server-Side Request Forgery (SSRF) vulnerability in FWDesign Ultimate Video Player allows Server Sid...	Server-Side Request Forgery (SSRF) vulnerability in FWDesign Ultimate Video Player allows Server Side Request Forgery. This issue affects Ultimate Video Player: from n/a through 10.1.	Patched by core rule	Y
CVE-2025-47437	CVE-2025-47437 - Server-Side Request Forgery (SSRF) vulnerability in LiteSpeed Technologies LiteSpeed Cache. This iss...	Server-Side Request Forgery (SSRF) vulnerability in LiteSpeed Technologies LiteSpeed Cache. This issue affects LiteSpeed Cache: from n/a through 7.0.1.	Patched by core rule	Y
CVE-2025-43763	CVE-2025-43763 - A server-side request forgery (SSRF) vulnerability exist in the Liferay Portal 7.4.0 through 7.4.3....	A server-side request forgery (SSRF) vulnerability exist in the Liferay Portal 7.4.0 through 7.4.3.131, and Liferay DXP 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13 and 2024.Q1.1 through 2024.Q1.20 that affects custom object attachment fields. This flaw allows an attacker to manipulate the application into making unauthorized requests to other instances, creating new object entries that link to external resources.	Patched by core rule	Y
CVE-2025-58829	CVE-2025-58829 - Server-	Server-Side Request Forgery	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Side Request Forgery (SSRF) vulnerability in aitool Ai Auto Tool Content Writing Assistant (G...	(SSRF) vulnerability in aitool Ai Auto Tool Content Writing Assistant (Gemini Writer, ChatGPT) All in One allows Server Side Request Forgery. This issue affects Ai Auto Tool Content Writing Assistant (Gemini Writer, ChatGPT) All in One: from n/a through 2.2.6.	rule	
CVE-2025-58641	CVE-2025-58641 - Server-Side Request Forgery (SSRF) vulnerability in kamleshyadav Exit Intent Popup allows Server Sid...	Server-Side Request Forgery (SSRF) vulnerability in kamleshyadav Exit Intent Popup allows Server Side Request Forgery. This issue affects Exit Intent Popup: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-58615	CVE-2025-58615 - Server-Side Request Forgery (SSRF) vulnerability in gfazioli WP Bannerize Pro allows Server Side Req...	Server-Side Request Forgery (SSRF) vulnerability in gfazioli WP Bannerize Pro allows Server Side Request Forgery. This issue affects WP Bannerize Pro: from n/a through 1.10.0.	Patched by core rule	Y
CVE-2025-53250	CVE-2025-53250 - Server-Side Request Forgery (SSRF) vulnerability in Chartbeat Chartbeat allows Server Side Request F...	Server-Side Request Forgery (SSRF) vulnerability in Chartbeat Chartbeat allows Server Side Request Forgery. This issue affects Chartbeat: from n/a through 2.0.7.	Patched by core rule	Y
CVE-2025-48364	CVE-2025-48364 - Server-Side Request Forgery (SSRF) vulnerability in vEnCa-X rajce allows Server Side Request Forgery...	Server-Side Request Forgery (SSRF) vulnerability in vEnCa-X rajce allows Server Side Request Forgery. This issue affects rajce: from n/a through 0.4.2.	Patched by core rule	Y
CVE-2025-58203	CVE-2025-58203 - Server-Side Request Forgery (SSRF) vulnerability in solacewp Solace Extra allows Server Side Request...	Server-Side Request Forgery (SSRF) vulnerability in solacewp Solace Extra allows Server Side Request Forgery. This issue affects Solace Extra: from n/a through 1.3.2.	Patched by core rule	Y

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-10037	SQL Injection	CVE-2025-10037 - The Featured Image from URL (FIFU) plugin for WordPress is vulnerable to SQL Injection via the get_p...	Patched by core rule	Y
CVE-2025-10036	SQL Injection	CVE-2025-10036 - The Featured Image from URL (FIFU) plugin for WordPress is vulnerable to SQL Injection via the get_a...	Patched by core rule	Y
CVE-2025-10964	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10964 - A weakness has been identified in Wavlink NU516U1. Affected by this vulnerability is the function su...	Patched by core rule	Y
CVE-2025-10963	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10963 - A security flaw has been discovered in Wavlink NU516U1 M16U1_V240425. Affected is the function sub_4...	Patched by core rule	Y
CVE-2025-10962	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10962 - A vulnerability was identified in Wavlink NU516U1 M16U1_V240425. This impacts the function sub_40319...	Patched by core rule	Y
CVE-2025-10961	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10961 - A vulnerability was determined in Wavlink NU516U1 M16U1_V240425. This affects the function sub_4030C...	Patched by core rule	Y
CVE-2025-10960	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10960 - A vulnerability was found in Wavlink NU516U1 M16U1_V240425. The impacted element is the function sub...	Patched by core rule	Y
CVE-2025-10959	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10959 - A vulnerability has been found in Wavlink NU516U1 M16U1_V240425. The affected element is the functio...	Patched by core rule	Y
CVE-2025-10958	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10958 - A flaw has been found in Wavlink NU516U1 M16U1_V240425. Impacted is the function sub_403010 of the f...	Patched by core rule	Y
CVE-2025-29084	SQL Injection	CVE-2025-29084 - SQL Injection vulnerability in CSZ-CMS v.1.3.0 allows a remote attacker to execute arbitrary code vi...	Patched by core rule	Y
CVE-2025-10846	Improper Neutralization of Special Elements in	CVE-2025-10846 - A vulnerability was	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Output Used by a Downstream Component(SQL Injection)	determined in Portabilis i-Educar up to 2.10. This vulnerability affects unknown...		
CVE-2025-10845	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10845 - A vulnerability was found in Portabilis i-Educar up to 2.10. This affects an unknown part of the fil...	Patched by core rule	Y
CVE-2025-10844	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10844 - A vulnerability has been found in Portabilis i-Educar up to 2.10. Affected by this issue is some unk...	Patched by core rule	Y
CVE-2025-10842	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10842 - A vulnerability was detected in code-projects Online Bidding System 1.0. Affected is an unknown func...	Patched by core rule	Y
CVE-2025-10841	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10841 - A security vulnerability has been detected in code-projects Online Bidding System 1.0. This impacts ...	Patched by core rule	Y
CVE-2025-10840	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10840 - A weakness has been identified in SourceCodester Pet Grooming Management Software 1.0. This affects ...	Patched by core rule	Y
CVE-2025-10839	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10839 - A security flaw has been discovered in SourceCodester Pet Grooming Management Software 1.0. The impa...	Patched by core rule	Y
CVE-2025-10836	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10836 - A weakness has been identified in SourceCodester Pet Grooming Management Software 1.0. Affected is a...	Patched by core rule	Y
CVE-2025-10835	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10835 - A security flaw has been discovered in SourceCodester Pet Grooming Management Software 1.0. This imp...	Patched by core rule	Y
CVE-2025-10832	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10832 - A vulnerability was found in SourceCodester Pet Grooming Management Software 1.0. The affected eleme...	Patched by core rule	Y
CVE-2025-10828	Improper Neutralization of Special Elements in Output Used by a Downstream	CVE-2025-10828 - A security vulnerability has been detected in SourceCodester Pet Grooming Management	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Component(SQL Injection)	Software 1.0. T...		
CVE-2025-10826	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10826 - A security flaw has been discovered in Campcodes Online Beauty Parlor Management System 1.0. Affecte...	Patched by core rule	Y
CVE-2025-10825	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10825 - A vulnerability was identified in Campcodes Online Beauty Parlor Management System 1.0. Affected is ...	Patched by core rule	Y
CVE-2025-10814	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10814 - A vulnerability was determined in D-Link DIR-823X 240126/240802/250416. Affected by this vulnerabili...	Patched by core rule	Y
CVE-2025-59570	SQL Injection	CVE-2025-59570 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i...	Patched by core rule	Y
CVE-2025-58686	SQL Injection	CVE-2025-58686 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i...	Patched by core rule	Y
CVE-2025-53468	SQL Injection	CVE-2025-53468 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i...	Patched by core rule	Y
CVE-2025-55885	SQL Injection	CVE-2025-55885 - SQL Injection vulnerability in Alpes Recherche et Developpement ARD GEC en Lign before v.2025-04-23 ...	Patched by core rule	Y
CVE-2025-10807	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10807 - A security flaw has been discovered in Campcodes Online Beauty Parlor Management System 1.0. This is...	Patched by core rule	Y
CVE-2025-10806	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10806 - A vulnerability was identified in Campcodes Online Beauty Parlor Management System 1.0. This vulnera...	Patched by core rule	Y
CVE-2025-10805	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10805 - A vulnerability was determined in Campcodes Online Beauty Parlor Management System 1.0. This affects...	Patched by core rule	Y
CVE-2025-10804	Improper Neutralization of Special Elements in Output Used by a	CVE-2025-10804 - A vulnerability was found in Campcodes Online Beauty	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Downstream Component(SQL Injection)	Parlor Management System 1.0. Affected by this ...		
CVE-2025-10802	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10802 - A flaw has been found in code-projects Online Bidding System 1.0. Affected is an unknown function of...	Patched by core rule	Y
CVE-2025-56075	SQL Injection	CVE-2025-56075 - A SQL Injection vulnerability was discovered in the normal-bwdates-reports-details.php file of PHPGu...	Patched by core rule	Y
CVE-2025-56074	SQL Injection	CVE-2025-56074 - A SQL Injection vulnerability was discovered in the foreigner-bwdates-reports-details.php file of PH...	Patched by core rule	Y
CVE-2025-10795	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10795 - A vulnerability has been found in code-projects Online Bidding System 1.0. This affects an unknown p...	Patched by core rule	Y
CVE-2025-10793	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10793 - A vulnerability was detected in code-projects E-Commerce Website 1.0. Affected by this vulnerability...	Patched by core rule	Y
CVE-2025-10791	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10791 - A weakness has been identified in code-projects Online Bidding System 1.0. This impacts an unknown f...	Patched by core rule	Y
CVE-2025-10788	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10788 - A vulnerability was determined in SourceCodester Online Hotel Reservation System 1.0. The affected e...	Patched by core rule	Y
CVE-2025-10002	SQL Injection	CVE-2025-10002 - The ClickWhale – Link Manager, Link Shortener and Click Tracker for Affiliate Links & Link Pages plu...	Patched by core rule	Y
CVE-2025-10652	SQL Injection	CVE-2025-10652 - The Robcore Netatmo plugin for WordPress is vulnerable to SQL Injection via the 'module_id' attribut...	Patched by core rule	Y
CVE-2025-10689	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10689 - A vulnerability was identified in D-Link DIR-645 105B01. This issue affects the function soapcgi_mai...	Patched by core rule	Y
CVE-2025-10688	Improper Neutralization of Special Elements in	CVE-2025-10688 - A vulnerability was	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Output Used by a Downstream Component(SQL Injection)	determined in SourceCodester Pet Grooming Management Software 1.0. This vulnerab...		
CVE-2025-10662	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10662 - A vulnerability has been found in SeaCMS up to 13.3. The impacted element is an unknown function of ...	Patched by core rule	Y
CVE-2025-10634	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10634 - A weakness has been identified in D-Link DIR-823X 240126/240802/250416. The impacted element is the ...	Patched by core rule	Y
CVE-2025-10623	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10623 - A vulnerability was identified in SourceCodester Hotel Reservation System 1.0. The impacted element ...	Patched by core rule	Y
CVE-2025-10621	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10621 - A vulnerability was determined in SourceCodester Hotel Reservation System 1.0. The affected element ...	Patched by core rule	Y
CVE-2025-10620	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10620 - A flaw has been found in itsourcecode Online Clinic Management System 1.0. This vulnerability affect...	Patched by core rule	Y
CVE-2025-10618	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10618 - A security vulnerability has been detected in itsourcecode Online Clinic Management System 1.0. Affe...	Patched by core rule	Y
CVE-2025-10599	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10599 - A security flaw has been discovered in itsourcecode Web-Based Internet Laboratory Management System ...	Patched by core rule	Y
CVE-2025-10592	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10592 - A security vulnerability has been detected in itsourcecode Online Public Access Catalog OPAC 1.0. Th...	Patched by core rule	Y
CVE-2025-10042	SQL Injection	CVE-2025-10042 - The Quiz Maker plugin for WordPress is vulnerable to SQL Injection via spoofed IP headers in all ver...	Patched by core rule	Y
CVE-2025-57631	SQL Injection	CVE-2025-57631 - SQL Injection vulnerability in TDuckCloud v.5.1 allows a remote attacker to execute	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		arbitrary code v...		
CVE-2025-52044	SQL Injection	CVE-2025-52044 - In Frappe ERPNext v15.57.5, the function get_stock_balance() at erpnext/stock/utils.py is vulnerable...	Patched by core rule	Y
CVE-2025-44034	SQL Injection	CVE-2025-44034 - SQL injection vulnerability in oa_system oasys v.1.1 allows a remote attacker to execute arbitrary c...	Patched by core rule	Y
CVE-2025-10473	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10473 - A security flaw has been discovered in yangzongzhuan RuoYi up to 4.8.1. This impacts the function fi...	Patched by core rule	Y
CVE-2025-57104	SQL Injection	CVE-2025-57104 - Teampel 5.1.6 is vulnerable to SQL Injection in /Common/login.aspx.	Patched by core rule	Y
CVE-2025-52048	SQL Injection	CVE-2025-52048 - In Frappe 15.x.x before 15.72.0 and 14.x.x before 14.96.10, in the function add_tag() at `frappe/des...	Patched by core rule	Y
CVE-2025-10431	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10431 - A vulnerability has been found in SourceCodester Pet Grooming Management Software 1.0. This affects ...	Patched by core rule	Y
CVE-2025-10430	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10430 - A flaw has been found in SourceCodester Pet Grooming Management Software 1.0. Affected by this issue...	Patched by core rule	Y
CVE-2025-10429	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10429 - A vulnerability was detected in SourceCodester Pet Grooming Management Software 1.0. Affected by thi...	Patched by core rule	Y
CVE-2025-10401	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10401 - A vulnerability was detected in D-Link DIR-823x up to 250416. The affected element is an unknown fun...	Patched by core rule	Y
CVE-2025-10396	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10396 - A vulnerability was determined in SourceCodester Pet Grooming Management Software 1.0. Affected by t...	Patched by core rule	Y
CVE-2025-10387	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL	CVE-2025-10387 - A vulnerability was determined in codesiddhant Jasmin Ransomware up to 1.0.1. This vulnerability aff...	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Injection)			
CVE-2025-10325	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10325 - A vulnerability was identified in Wavlink WL-WN578W2 221110. This impacts the function sub_401340/su...	Patched by core rule	Y
CVE-2025-9807	SQL Injection	CVE-2025-9807 - The The Events Calendar plugin for WordPress is vulnerable to time-based SQL Injection via the ‘s’ p...	Patched by core rule	Y
CVE-2025-9451	SQL Injection	CVE-2025-9451 - The Smartcat Translator for WPML plugin for WordPress is vulnerable to time-based SQL Injection via ...	Patched by core rule	Y
CVE-2025-9073	SQL Injection	CVE-2025-9073 - The All in one Minifier plugin for WordPress is vulnerable to SQL Injection via the 'post_id' parame...	Patched by core rule	Y
CVE-2025-8692	SQL Injection	CVE-2025-8692 - The Coupon API plugin for WordPress is vulnerable to SQL Injection via the ‘log_duration’ parameter ...	Patched by core rule	Y
CVE-2025-9776	SQL Injection	CVE-2025-9776 - The CatFolders – Tame Your WordPress Media Library by Category plugin for WordPress is vulnerable to...	Patched by core rule	Y
CVE-2025-10210	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10210 - A weakness has been identified in yanyutao0402 ChanCMS up to 3.3.0. Impacted is the function Search ...	Patched by core rule	Y
CVE-2025-56407	SQL Injection	CVE-2025-56407 - A vulnerability has been found in HuangDou UTCMS V9 and classified as critical. This vulnerability a...	Patched by core rule	Y
CVE-2025-9463	SQL Injection	CVE-2025-9463 - The Payments Plugin and Checkout Plugin for WooCommerce: Stripe, PayPal, Square, Authorize.net plugi...	Patched by core rule	Y
CVE-2025-6189	SQL Injection	CVE-2025-6189 - The Duplicate Page and Post plugin for WordPress is vulnerable to time-based SQL Injection via the ‘...	Patched by core rule	Y
CVE-2025-10142	SQL Injection	CVE-2025-10142 - The PagBank / PagSeguro Connect para WooCommerce plugin for WordPress is vulnerable to SQL Injection...	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-10197	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10197 - A vulnerability was found in HJSoft HCM Human Resources Management System up to 20250822. Affected b...	Patched by core rule	Y
CVE-2025-59008	SQL Injection	CVE-2025-59008 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i...	Patched by core rule	Y
CVE-2025-58993	SQL Injection	CVE-2025-58993 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i...	Patched by core rule	Y
CVE-2025-47569	SQL Injection	CVE-2025-47569 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i...	Patched by core rule	Y
CVE-2025-10107	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10107 - A vulnerability has been found in TRENDnet TEW-831DR 1.0 (601.130.1.1410). Impacted is an unknown fu...	Patched by core rule	Y
CVE-2025-10123	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10123 - A vulnerability was determined in D-Link DIR-823X up to 250416. Affected by this vulnerability is th...	Patched by core rule	Y
CVE-2025-10122	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10122 - A vulnerability was found in Maccms10 2025.1000.4050. Affected is the function rep of the file appli...	Patched by core rule	Y
CVE-2025-10046	SQL Injection	CVE-2025-10046 - The ELEX WooCommerce Google Shopping (Google Product Feed) plugin for WordPress is vulnerable to SQL...	Patched by core rule	Y
CVE-2025-9085	SQL Injection	CVE-2025-9085 - The User Registration & Membership plugin for WordPress is vulnerable to SQL Injection via the 's' p...	Patched by core rule	Y
CVE-2025-10003	SQL Injection	CVE-2025-10003 - The UsersWP – Front-end login form, User Registration, User Profile & Members Directory plugin for W...	Patched by core rule	Y
CVE-2025-58628	SQL Injection	CVE-2025-58628 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i...	Patched by core rule	Y
CVE-2025-58780	SQL Injection	CVE-2025-58780 - index.em7 in ScienceLogic SL1 before	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		12.1.1 allows SQL Injection via a parameter in a request. NOTE:...		
CVE-2025-10012	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10012 - A security vulnerability has been detected in Portabilis i-Educar up to 2.10. The impacted element i...	Patched by core rule	Y
CVE-2025-58881	SQL Injection	CVE-2025-58881 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i...	Patched by core rule	Y
CVE-2025-58789	SQL Injection	CVE-2025-58789 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i...	Patched by core rule	Y
CVE-2025-58788	SQL Injection	CVE-2025-58788 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i...	Patched by core rule	Y
CVE-2025-10011	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-10011 - A weakness has been identified in Portabilis i-Educar up to 2.10. The affected element is an unknown...	Patched by core rule	Y
CVE-2025-9935	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9935 - A vulnerability was determined in TOTOLINK N600R 4.3.0cu.7866_B20220506. This vulnerability affects ...	Patched by core rule	Y
CVE-2025-9934	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9934 - A vulnerability was found in TOTOLINK X5000R 9.1.0cu.2415_B20250515. This affects the function sub_4...	Patched by core rule	Y
CVE-2025-58604	SQL Injection	CVE-2025-58604 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i...	Patched by core rule	Y
CVE-2025-50565	SQL Injection	CVE-2025-50565 - Doubo ERP 1.0 has an SQL injection vulnerability due to a lack of filtering of user input, which can...	Patched by core rule	Y
CVE-2025-9790	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9790 - A security flaw has been discovered in SourceCodester Hotel Reservation System 1.0. This affects an ...	Patched by core rule	Y
CVE-2025-9789	Improper Neutralization of Special Elements in Output Used by a	CVE-2025-9789 - A vulnerability was identified in SourceCodester Online	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Downstream Component(SQL Injection)	Hotel Reservation System 1.0. Affected by th...		
CVE-2025-9771	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9771 - A security vulnerability has been detected in SourceCodester Eye Clinic Management System 1.0. Affec...	Patched by core rule	Y
CVE-2025-9770	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9770 - A weakness has been identified in Campcodes Hospital Management System 1.0. Affected by this vulnera...	Patched by core rule	Y
CVE-2025-9758	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9758 - A vulnerability was identified in deepakmisal24 Chemical Inventory Management System up to 1.0. Affe...	Patched by core rule	Y
CVE-2025-9749	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9749 - A vulnerability was identified in HKritesh009 Grocery List Management Web App up to f491b681eb70d465...	Patched by core rule	Y
CVE-2025-9743	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9743 - A security flaw has been discovered in code-projects Human Resource Integrated System 1.0. Impacted ...	Patched by core rule	Y
CVE-2025-9742	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9742 - A vulnerability was identified in code-projects Human Resource Integrated System 1.0. This issue aff...	Patched by core rule	Y
CVE-2025-9741	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9741 - A vulnerability was determined in code-projects Human Resource Integrated System 1.0. This vulnerabi...	Patched by core rule	Y
CVE-2025-9740	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9740 - A vulnerability was found in code-projects Human Resource Integrated System 1.0. This affects an unk...	Patched by core rule	Y
CVE-2025-9733	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9733 - A security flaw has been discovered in code-projects Human Resource Integrated System 1.0. This impa...	Patched by core rule	Y
CVE-2025-9686	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL	CVE-2025-9686 - A security flaw has been discovered in Portabilis i-Educar up to 2.10. This issue affects some unkno...	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Injection)			
CVE-2025-9685	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9685 - A vulnerability was identified in Portabilis i-Educar up to 2.10. This vulnerability affects unknown...	Patched by core rule	Y
CVE-2025-9684	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9684 - A vulnerability was determined in Portabilis i-Educar up to 2.10. This affects an unknown part of th...	Patched by core rule	Y
CVE-2025-44033	SQL Injection	CVE-2025-44033 - SQL injection vulnerability in oa_system oasys v.1.1 allows a remote attacker to execute arbitrary c...	Patched by core rule	Y
CVE-2025-9441	SQL Injection	CVE-2025-9441 - The iATS Online Forms plugin for WordPress is vulnerable to time-based SQL Injection via the ‘order'...	Patched by core rule	Y
CVE-2025-9608	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9608 - A vulnerability has been found in Portabilis i-Educar up to 2.10. This affects an unknown part of th...	Patched by core rule	Y
CVE-2025-9607	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9607 - A flaw has been found in Portabilis i-Educar up to 2.10. Affected by this issue is some unknown func...	Patched by core rule	Y
CVE-2025-9606	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9606 - A vulnerability was detected in Portabilis i-Educar up to 2.10. Affected by this vulnerability is an...	Patched by core rule	Y
CVE-2025-9603	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9603 - A vulnerability was determined in Telesquare TLR-2005KSH 1.2.4. The affected element is an unknown f...	Patched by core rule	Y
CVE-2025-9586	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9586 - A vulnerability was identified in Comfast CF-N1 2.6.0. This vulnerability affects the function wirel...	Patched by core rule	Y
CVE-2025-9585	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9585 - A vulnerability was determined in Comfast CF-N1 2.6.0. This affects the function wifilith_delete_pic...	Patched by core rule	Y
CVE-2025-9584	Improper Neutralization of Special Elements in	CVE-2025-9584 - A vulnerability was found in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Output Used by a Downstream Component(SQL Injection)	Comfast CF-N1 2.6.0. Affected by this issue is the function update_inte...		
CVE-2025-57819	SQL Injection	CVE-2025-57819 - FreePBX is an open-source web-based graphical user interface. FreePBX 15, 16, and 17 endpoints are v...	Patched by core rule	Y
CVE-2025-51972	SQL Injection	CVE-2025-51972 - A SQL Injection vulnerability exists in the login.php of PuneethReddyHC Online Shopping System Advan...	Patched by core rule	Y
CVE-2025-51971	SQL Injection	CVE-2025-51971 - A reflected Cross-Site Scripting (XSS) vulnerability exists in register.php of PuneethReddyHC Online...	Patched by core rule	Y
CVE-2025-51969	SQL Injection	CVE-2025-51969 - A SQL Injection vulnerability exists in the product.php page of PuneethReddyHC Online Shopping Syste...	Patched by core rule	Y
CVE-2025-51968	SQL Injection	CVE-2025-51968 - A SQL Injection vulnerability exists in the action.php file of PuneethReddyHC Online Shopping System...	Patched by core rule	Y
CVE-2025-54720	SQL Injection	CVE-2025-54720 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i...	Patched by core rule	Y
CVE-2025-49404	SQL Injection	CVE-2025-49404 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i...	Patched by core rule	Y
CVE-2025-39496	SQL Injection	CVE-2025-39496 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i...	Patched by core rule	Y
CVE-2025-8977	SQL Injection	CVE-2025-8977 - The Simple Download Monitor plugin for WordPress is vulnerable to time-based SQL Injection via the o...	Patched by core rule	Y
CVE-2024-13979	SQL Injection	CVE-2024-13979 - A SQL injection vulnerability exists in the St. Joe ERP system ("圣乔ERP系统") that allows unauthenticat...	Patched by core rule	Y
CVE-2025-51667	SQL Injection	CVE-2025-51667 - An issue was discovered in simple-admin-core v1.2.0 thru v1.6.7. The /sys-api/role/update interface ...	Patched by core rule	Y
CVE-2025-50979	SQL Injection	CVE-2025-50979 - NodeBB	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		v4.3.0 is vulnerable to SQL injection in its search-categories API endpoint (/api/v3/search/c...	rule	
CVE-2025-50984	SQL Injection	CVE-2025-50984 - diskover-web v2.3.0 Community Edition is vulnerable to multiple boolean-based blind SQL injection fl...	Patched by core rule	Y
CVE-2025-50983	SQL Injection	CVE-2025-50983 - SQL Injection vulnerability exists in the sortKey parameter of the GET /api/v1/wanted/cutoff API end...	Patched by core rule	Y
CVE-2025-50972	SQL Injection	CVE-2025-50972 - SQL Injection vulnerability in AbanteCart 1.4.2, allows unauthenticated attackers to execute arbitra...	Patched by core rule	Y
CVE-2025-9532	Improper Neutralization of Special Elements in Output Used by a Downstream Component(SQL Injection)	CVE-2025-9532 - A flaw has been found in Portabilis i-Educar up to 2.10. This impacts an unknown function of the fil...	Patched by core rule	Y

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-9044	CVE-2025-9044 - The Mapster WP Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple f...	The Mapster WP Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple fields in versions up to, and including, 1.20.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor-level permissions and above to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-8906	CVE-2025-8906 - The Widgets for Tiktok Feed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via th...	The Widgets for Tiktok Feed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'trustindex-feed' shortcode in all versions up to, and including, 1.7.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-8200	CVE-2025-8200 - The Mega Elements – Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scr...	The Mega Elements – Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Countdown Timer widget in all versions up to, and including, 1.3.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-10178	CVE-2025-10178 - The CM Business Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ...	The CM Business Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'cmbd_featured_image' shortcode in all versions up to, and including, 1.5.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-29156	CVE-2025-29156 - Cross Site Scripting vulnerability in petstore v.1.0.7 allows a remote attacker to execute arbitrary...	Cross Site Scripting vulnerability in petstore v.1.0.7 allows a remote attacker to execute arbitrary code via a crafted script to the /api/v3/pet	Patched by core rule	Y
CVE-2025-59832	CVE-2025-59832 - Horilla is a free and open source Human Resource Management System (HRMS). Prior to version 1.4.0, t...	Horilla is a free and open source Human Resource Management System (HRMS). Prior to version 1.4.0, there is a stored XSS vulnerability in the ticket comment editor. A low-privilege authenticated user could run arbitrary JavaScript in an admin's browser, exfiltrate the admin's cookies/CSRF token, and hijack their session. This issue has been patched in version 1.4.0.	Patched by core rule	Y
CVE-2025-59525	CVE-2025-59525 - Horilla is a free and open source Human Resource Management System (HRMS). Prior to version 1.4.0, i...	Horilla is a free and open source Human Resource Management System (HRMS). Prior to version 1.4.0, improper sanitization across the application allows XSS via uploaded SVG (and via allowed <embed>), which can be chained to execute JavaScript whenever users view impacted content (e.g., announcements). This can result in admin account takeover. This issue has been patched in version 1.4.0.	Patched by core rule	Y
CVE-2025-59524	CVE-2025-59524 - Horilla is a free and open source Human Resource Management System (HRMS). Prior to version 1.4.0, t...	Horilla is a free and open source Human Resource Management System (HRMS). Prior to version 1.4.0, the file upload flow performs validation only in the browser and does not enforce server-side checks. An attacker can bypass the client-side validation (for example, with an intercepting proxy or by submitting a crafted request) to store an executable HTML document on the server. When an administrator or other privileged user views the uploaded file, the embedded script runs in their context and sends session cookies (or other credentials) to an	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attacker-controlled endpoint. The attacker then reuses those credentials to impersonate the admin. This issue has been patched in version 1.4.0.		
CVE-2025-9353	CVE-2025-9353 - The Themify Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several pa...	The Themify Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several parameters in all versions up to, and including, 7.6.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The vulnerability was partially patched in version 7.6.9.	Patched by core rule	Y
CVE-2025-43779	CVE-2025-43779 - A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.112, ...	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.112, and Liferay DXP 2024.Q1.1 through 2024.Q1.18 and 7.4 GA through update 92 allows a remote authenticated attacker to inject JavaScript code via _com_liferay_commerce_product_definitions_web_internal_portlet_CPDefinitionsPortlet_productTypeName parameter. This malicious payload is then reflected and executed within the user's browser.	Patched by core rule	Y
CVE-2025-58674	CVE-2025-58674 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WordPress allows Stored XSS. WordPress core security team is aware of the issue and working on a fix. This is low severity vulnerability that requires an attacker to have Author or higher user privileges to execute the attack vector.This issue affects WordPress: from 6.8 through 6.8.2, from 6.7 through 6.7.3, from 6.6 through 6.6.3, from 6.5 through 6.5.6, from 6.4 through 6.4.6, from 6.3 through 6.3.6, from 6.2 through 6.2.7, from 6.1 through 6.1.8, from 6.0 through 6.0.10, from 5.9 through 5.9.11, from 5.8	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		through 5.8.11, from 5.7 through 5.7.13, from 5.6 through 5.6.15, from 5.5 through 5.5.16, from 5.4 through 5.4.17, from 5.3 through 5.3.19, from 5.2 through 5.2.22, from 5.1 through 5.1.20, from 5.0 through 5.0.23, from 4.9 through 4.9.27, from 4.8 through 4.8.26, from 4.7 through 4.7.30.		
CVE-2025-10837	CVE-2025-10837 - A security vulnerability has been detected in code-projects Simple Food Ordering System 1.0. Affecte...	A security vulnerability has been detected in code-projects Simple Food Ordering System 1.0. Affected by this vulnerability is an unknown functionality of the file /ordersimple/order.php. The manipulation of the argument ID leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2025-58915	CVE-2025-58915 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Emarket-design YouTube Showcase youtube-showcase allows Stored XSS.This issue affects YouTube Showcase: from n/a through 3.5.0.	Patched by core rule	Y
CVE-2025-59592	CVE-2025-59592 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fernando Acosta Make Column Clickable Elementor allows Stored XSS. This issue affects Make Column Clickable Elementor: from n/a through 1.6.0.	Patched by core rule	Y
CVE-2025-59590	CVE-2025-59590 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in David Lingren Media Library Assistant allows Stored XSS. This issue affects Media Library Assistant: from n/a through 3.28.	Patched by core rule	Y
CVE-2025-59589	CVE-2025-59589 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Soledad allows DOM-Based XSS. This issue affects Soledad: from n/a through 8.6.8.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-59587	CVE-2025-59587 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Shortcodes & Performance allows DOM-Based XSS. This issue affects Penci Shortcodes & Performance: from n/a through n/a.	Patched by core rule	Y
CVE-2025-59586	CVE-2025-59586 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Portfolio allows DOM-Based XSS. This issue affects Penci Portfolio: from n/a through 3.5.	Patched by core rule	Y
CVE-2025-59585	CVE-2025-59585 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Recipe allows DOM-Based XSS. This issue affects Penci Recipe: from n/a through 4.0.	Patched by core rule	Y
CVE-2025-59584	CVE-2025-59584 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Podcast allows DOM-Based XSS. This issue affects Penci Podcast: from n/a through 1.6.	Patched by core rule	Y
CVE-2025-59583	CVE-2025-59583 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Filter Everything allows DOM-Based XSS. This issue affects Penci Filter Everything: from n/a through n/a.	Patched by core rule	Y
CVE-2025-59574	CVE-2025-59574 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Travel Engine WP Travel Engine allows Stored XSS. This issue affects WP Travel Engine: from n/a through 1.4.2.	Patched by core rule	Y
CVE-2025-59569	CVE-2025-59569 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Emraan Cheema CubeWP allows Stored XSS. This issue affects CubeWP: from n/a through 1.1.26.	Patched by core rule	Y
CVE-2025-59565	CVE-2025-59565 - Improper Neutralization of Input During Web Page	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
	Generation ('Cross-site Scripting') vulnerability i...	Scripting') vulnerability in WP Swings Upsell Order Bump Offer for WooCommerce allows Stored XSS. This issue affects Upsell Order Bump Offer for WooCommerce: from n/a through 3.0.7.		
CVE-2025-59553	CVE-2025-59553 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Coderz Studio Custom iFrame for Elementor allows DOM-Based XSS. This issue affects Custom iFrame for Elementor: from n/a through 1.0.13.	Patched by core rule	Y
CVE-2025-59552	CVE-2025-59552 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pdfcrowd Dev Team Save as PDF allows Stored XSS. This issue affects Save as PDF: from n/a through 4.5.2.	Patched by core rule	Y
CVE-2025-59549	CVE-2025-59549 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fatcatapps GetResponse Forms allows Stored XSS. This issue affects GetResponse Forms: from n/a through 2.6.0.	Patched by core rule	Y
CVE-2025-58992	CVE-2025-58992 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in impleCode Product Catalog Simple allows Stored XSS. This issue affects Product Catalog Simple: from n/a through 1.8.2.	Patched by core rule	Y
CVE-2025-58974	CVE-2025-58974 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in StellarWP WPComplete allows Stored XSS. This issue affects WPComplete: from n/a through 2.9.5.2.	Patched by core rule	Y
CVE-2025-58965	CVE-2025-58965 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Agency Dominion Inc. Fusion Page Builder : Extension – Gallery allows Stored XSS. This issue affects Fusion Page Builder : Extension – Gallery: from n/a through 1.7.6.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-58960	CVE-2025-58960 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in brijeshk89 IP Based Login allows Stored XSS. This issue affects IP Based Login: from n/a through 2.4.3.	Patched by core rule	Y
CVE-2025-58704	CVE-2025-58704 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ren Ventura WP Delete User Accounts allows Stored XSS. This issue affects WP Delete User Accounts: from n/a through 1.2.4.	Patched by core rule	Y
CVE-2025-58703	CVE-2025-58703 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skyword Skyword API Plugin allows Stored XSS. This issue affects Skyword API Plugin: from n/a through 2.5.3.	Patched by core rule	Y
CVE-2025-58702	CVE-2025-58702 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebWizards MarketKing allows Stored XSS. This issue affects MarketKing: from n/a through 2.0.92.	Patched by core rule	Y
CVE-2025-58691	CVE-2025-58691 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Russell Jamieson Genesis Club Lite allows Stored XSS. This issue affects Genesis Club Lite: from n/a through 1.17.	Patched by core rule	Y
CVE-2025-58689	CVE-2025-58689 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tapfiliate Tapfiliate allows Stored XSS. This issue affects Tapfiliate: from n/a through 3.2.2.	Patched by core rule	Y
CVE-2025-58684	CVE-2025-58684 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themepoints Logo Showcase allows Stored XSS. This issue affects Logo Showcase: from n/a through 3.0.9.	Patched by core rule	Y
CVE-2025-58683	CVE-2025-58683 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Luke Mlsna Last Updated	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	i...	Shortcode allows Stored XSS. This issue affects Last Updated Shortcode: from n/a through 1.0.1.		
CVE-2025-58682	CVE-2025-58682 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Timur Kamaev Kama Click Counter allows Stored XSS. This issue affects Kama Click Counter: from n/a through 4.0.4.	Patched by core rule	Y
CVE-2025-58671	CVE-2025-58671 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in morganrichards Auction Feed allows Stored XSS. This issue affects Auction Feed: from n/a through 1.1.3.	Patched by core rule	Y
CVE-2025-58669	CVE-2025-58669 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Modern Minds Magento 2 WordPress Integration allows Stored XSS. This issue affects Magento 2 WordPress Integration: from n/a through 1.4.1.	Patched by core rule	Y
CVE-2025-58665	CVE-2025-58665 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tmontg1 Form Generator for WordPress allows Stored XSS. This issue affects Form Generator for WordPress: from n/a through 1.5.2.	Patched by core rule	Y
CVE-2025-58661	CVE-2025-58661 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eZee Technosys eZee Online Hotel Booking Engine allows Stored XSS. This issue affects eZee Online Hotel Booking Engine: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-58659	CVE-2025-58659 - Use of Hard-coded Credentials vulnerability in Essekia Helpie FAQ allows Retrieve Embedded Sensitive...	Use of Hard-coded Credentials vulnerability in Essekia Helpie FAQ allows Retrieve Embedded Sensitive Data. This issue affects Helpie FAQ: from n/a through 1.39.	Patched by core rule	Y
CVE-2025-58658	CVE-2025-58658 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Proof Factor LLC Proof Factor – Social Proof Notifications allows Stored	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		XSS. This issue affects Proof Factor – Social Proof Notifications: from n/a through 1.0.5.		
CVE-2025-58656	CVE-2025-58656 - Use of Hard-coded Credentials vulnerability in Risto Niinemets Estonian Shipping Methods for WooComm...	Use of Hard-coded Credentials vulnerability in Risto Niinemets Estonian Shipping Methods for WooCommerce allows Retrieve Embedded Sensitive Data. This issue affects Estonian Shipping Methods for WooCommerce: from n/a through 1.7.2.	Patched by core rule	Y
CVE-2025-58655	CVE-2025-58655 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mattia Roccoberton Category Featured Images allows Stored XSS. This issue affects Category Featured Images: from n/a through 1.1.8.	Patched by core rule	Y
CVE-2025-58654	CVE-2025-58654 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michel - xiligroup dev xili-language allows DOM-Based XSS. This issue affects xili-language: from n/a through 2.21.3.	Patched by core rule	Y
CVE-2025-58653	CVE-2025-58653 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in JS Morisset JSM file_get_contents() Shortcode allows Stored XSS. This issue affects JSM file_get_contents() Shortcode: from n/a through 2.7.1.	Patched by core rule	Y
CVE-2025-58652	CVE-2025-58652 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themepoints Carousel Ultimate allows Stored XSS. This issue affects Carousel Ultimate: from n/a through 1.8.	Patched by core rule	Y
CVE-2025-58651	CVE-2025-58651 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PlayerJS PlayerJS allows DOM-Based XSS. This issue affects PlayerJS: from n/a through 2.24.	Patched by core rule	Y
CVE-2025-58648	CVE-2025-58648 - Improper Neutralization	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Generation ('Cross-site Scripting') vulnerability in Nicu Micle Simple JWT Login allows Stored XSS. This issue affects Simple JWT Login: from n/a through 3.6.4.		
CVE-2025-58647	CVE-2025-58647 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Will.I.am Simple Restaurant Menu allows Stored XSS. This issue affects Simple Restaurant Menu: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-58646	CVE-2025-58646 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in chtombleson Mobi2Go allows Stored XSS. This issue affects Mobi2Go: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-58645	CVE-2025-58645 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Gravitate Gravitate Automated Tester allows Stored XSS. This issue affects Gravitate Automated Tester: from n/a through 1.4.5.	Patched by core rule	Y
CVE-2025-58271	CVE-2025-58271 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AnyClip Video Platform AnyClip Luminous Studio allows Stored XSS. This issue affects AnyClip Luminous Studio: from n/a through 1.3.3.	Patched by core rule	Y
CVE-2025-58269	CVE-2025-58269 - Use of Hard-coded Credentials vulnerability in weDevs WP Project Manager allows Retrieve Embedded Se...	Use of Hard-coded Credentials vulnerability in weDevs WP Project Manager allows Retrieve Embedded Sensitive Data. This issue affects WP Project Manager: from n/a through 2.6.25.	Patched by core rule	Y
CVE-2025-58266	CVE-2025-58266 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fumiki Takahashi Gianism allows Stored XSS. This issue affects Gianism: from n/a through 5.2.2.	Patched by core rule	Y
CVE-2025-58265	CVE-2025-58265 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Stonehenge Creations Events Manager – OpenStreetMaps allows	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Stored XSS. This issue affects Events Manager – OpenStreetMaps: from n/a through 4.2.1.		
CVE-2025-58264	CVE-2025-58264 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	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 4.10.1.	Patched by core rule	Y
CVE-2025-58263	CVE-2025-58263 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BuddyDev BuddyPress Notification Widget allows Stored XSS. This issue affects BuddyPress Notification Widget: from n/a through 1.3.3.	Patched by core rule	Y
CVE-2025-58260	CVE-2025-58260 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ronald Huereca Highlight and Share – Social Text and Image Sharing allows Stored XSS. This issue affects Highlight and Share – Social Text and Image Sharing: from n/a through 5.1.1.	Patched by core rule	Y
CVE-2025-58257	CVE-2025-58257 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Picture-Planet GmbH Verowa Connect allows Stored XSS. This issue affects Verowa Connect: from n/a through 3.2.3.	Patched by core rule	Y
CVE-2025-58256	CVE-2025-58256 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jonathan Brinley DOAJ Export allows Stored XSS. This issue affects DOAJ Export: from n/a through 1.0.4.	Patched by core rule	Y
CVE-2025-58254	CVE-2025-58254 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in dtbaker StylePress for Elementor allows Stored XSS. This issue affects StylePress for Elementor: from n/a through 1.2.1.	Patched by core rule	Y
CVE-2025-58253	CVE-2025-58253 - Improper Neutralization of Input During Web Page Generation ('Cross-site	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
	Scripting') vulnerability i...	Rameez Iqbal Real Estate Manager allows DOM-Based XSS. This issue affects Real Estate Manager: from n/a through 7.3.		
CVE-2025-58248	CVE-2025-58248 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in codefish Pinterest Pinboard Widget allows Stored XSS. This issue affects Pinterest Pinboard Widget: from n/a through 1.0.7.	Patched by core rule	Y
CVE-2025-58245	CVE-2025-58245 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bestweblayout Portfolio allows DOM-Based XSS. This issue affects Portfolio : from n/a through 2.58.	Patched by core rule	Y
CVE-2025-58242	CVE-2025-58242 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vadim Bogaiskov Bg Church Memos allows DOM-Based XSS. This issue affects Bg Church Memos: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-58241	CVE-2025-58241 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in snapwidget SnapWidget Social Photo Feed Widget allows DOM-Based XSS. This issue affects SnapWidget Social Photo Feed Widget: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-58240	CVE-2025-58240 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michel - xiligroup dev xili-tidy-tags allows Stored XSS. This issue affects xili-tidy-tags: from n/a through 1.12.06.	Patched by core rule	Y
CVE-2025-58239	CVE-2025-58239 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chandrika Sista WP Category Dropdown allows Stored XSS. This issue affects WP Category Dropdown: from n/a through 1.9.	Patched by core rule	Y
CVE-2025-58238	CVE-2025-58238 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ONTRAPORT PilotPress	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	i...	allows Stored XSS. This issue affects PilotPress: from n/a through 2.0.35.		
CVE-2025-58237	CVE-2025-58237 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Niaj Morshed LC Wizard allows Stored XSS. This issue affects LC Wizard: from n/a through 1.3.0.	Patched by core rule	Y
CVE-2025-58235	CVE-2025-58235 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rustaurius Front End Users allows Stored XSS. This issue affects Front End Users: from n/a through 3.2.33.	Patched by core rule	Y
CVE-2025-58234	CVE-2025-58234 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in JoomSky JS Job Manager allows Stored XSS. This issue affects JS Job Manager: from n/a through 2.0.2.	Patched by core rule	Y
CVE-2025-58233	CVE-2025-58233 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Guaven Labs SQL Chart Builder allows DOM-Based XSS. This issue affects SQL Chart Builder: from n/a through 2.3.7.2.	Patched by core rule	Y
CVE-2025-58232	CVE-2025-58232 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ickata Image Editor by Pixo allows DOM-Based XSS. This issue affects Image Editor by Pixo: from n/a through 2.3.8.	Patched by core rule	Y
CVE-2025-58231	CVE-2025-58231 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bitlydeveloper Bitly allows Stored XSS. This issue affects Bitly: from n/a through 2.7.4.	Patched by core rule	Y
CVE-2025-58230	CVE-2025-58230 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bdthemes ZoloBlocks allows DOM-Based XSS. This issue affects ZoloBlocks: from n/a through 2.3.9.	Patched by core rule	Y
CVE-2025-58229	CVE-2025-58229 - Improper Neutralization of Input During Web Page	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
	Generation ('Cross-site Scripting') vulnerability i...	Scripting') vulnerability in webvitaly Sitekit allows Stored XSS. This issue affects Sitekit: from n/a through 2.0.		
CVE-2025-58228	CVE-2025-58228 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ShapedPlugin LLC Quick View for WooCommerce allows Stored XSS. This issue affects Quick View for WooCommerce: from n/a through 2.2.16.	Patched by core rule	Y
CVE-2025-58227	CVE-2025-58227 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alexander Lueken Podlove Subscribe button allows Stored XSS. This issue affects Podlove Subscribe button: from n/a through 1.3.11.	Patched by core rule	Y
CVE-2025-58223	CVE-2025-58223 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chris Taylor VoucherPress allows Stored XSS. This issue affects VoucherPress: from n/a through 1.5.7.	Patched by core rule	Y
CVE-2025-58220	CVE-2025-58220 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Techeshta Card Elements for WPBakery allows DOM-Based XSS. This issue affects Card Elements for WPBakery: from n/a through 1.0.8.	Patched by core rule	Y
CVE-2025-58033	CVE-2025-58033 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in leeshadle Draft allows Stored XSS. This issue affects Draft: from n/a through 3.0.9.	Patched by core rule	Y
CVE-2025-58031	CVE-2025-58031 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nextendweb Nextend Facebook Connect allows Stored XSS. This issue affects Nextend Facebook Connect : from n/a through 3.1.19.	Patched by core rule	Y
CVE-2025-58030	CVE-2025-58030 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webvitaly Page-list allows	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	i...	Stored XSS. This issue affects Page-list: from n/a through 5.7.		
CVE-2025-58028	CVE-2025-58028 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aum Watcharapon Designil PDPA Thailand allows Stored XSS. This issue affects Designil PDPA Thailand: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-58027	CVE-2025-58027 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	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 3.4.3.	Patched by core rule	Y
CVE-2025-58026	CVE-2025-58026 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in termageddon Termageddon: Cookie Consent & Privacy Compliance allows Stored XSS. This issue affects Termageddon: Cookie Consent & Privacy Compliance: from n/a through 1.8.1.	Patched by core rule	Y
CVE-2025-58025	CVE-2025-58025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in averta Master Slider allows Stored XSS. This issue affects Master Slider: from n/a through 3.11.0.	Patched by core rule	Y
CVE-2025-58023	CVE-2025-58023 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in akdevs Genealogical Tree allows Stored XSS. This issue affects Genealogical Tree: from n/a through 2.2.5.	Patched by core rule	Y
CVE-2025-58022	CVE-2025-58022 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in maxpagels ShortCode allows Stored XSS. This issue affects ShortCode: from n/a through 0.8.1.	Patched by core rule	Y
CVE-2025-58021	CVE-2025-58021 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in douglaskarr List Child Pages Shortcode allows Stored XSS. This issue affects List Child	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Pages Shortcode: from n/a through 1.3.1.		
CVE-2025-58020	CVE-2025-58020 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeroen Schmit Theater for WordPress allows Stored XSS. This issue affects Theater for WordPress: from n/a through 0.18.8.	Patched by core rule	Y
CVE-2025-58019	CVE-2025-58019 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Search Atlas Search Atlas SEO allows Stored XSS. This issue affects Search Atlas SEO: from n/a through 2.5.4.	Patched by core rule	Y
CVE-2025-58018	CVE-2025-58018 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Richard Leishman Mail Subscribe List allows Stored XSS. This issue affects Mail Subscribe List: from n/a through 2.1.10.	Patched by core rule	Y
CVE-2025-58017	CVE-2025-58017 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bdthemes Ultimate Store Kit Elementor Addons allows Stored XSS. This issue affects Ultimate Store Kit Elementor Addons: from n/a through 2.8.2.	Patched by core rule	Y
CVE-2025-58008	CVE-2025-58008 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in xnau webdesign Participants Database allows Stored XSS. This issue affects Participants Database: from n/a through 2.7.6.3.	Patched by core rule	Y
CVE-2025-58002	CVE-2025-58002 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Milan Petrovic GD bbPress Tools allows DOM-Based XSS. This issue affects GD bbPress Tools: from n/a through 3.5.3.	Patched by core rule	Y
CVE-2025-58001	CVE-2025-58001 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Noumaan Yaqoob Compact Archives allows Stored XSS. This issue affects Compact Archives: from n/a through	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		4.1.0.		
CVE-2025-57999	CVE-2025-57999 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpkoithemes WPKoi Templates for Elementor allows DOM-Based XSS. This issue affects WPKoi Templates for Elementor: from n/a through 3.4.1.	Patched by core rule	Y
CVE-2025-57998	CVE-2025-57998 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hamid Reza Yazdani E-namad & Shamed Logo Manager allows Stored XSS. This issue affects E-namad & Shamed Logo Manager: from n/a through 2.2.	Patched by core rule	Y
CVE-2025-57996	CVE-2025-57996 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in matthewordie Buckets allows Stored XSS. This issue affects Buckets: from n/a through 0.3.9.	Patched by core rule	Y
CVE-2025-57993	CVE-2025-57993 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Benjamin Pick Geolocation IP Detection allows Stored XSS. This issue affects Geolocation IP Detection: from n/a through 5.5.0.	Patched by core rule	Y
CVE-2025-57989	CVE-2025-57989 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brajesh Singh WordPress Widgets Shortcode allows Stored XSS. This issue affects WordPress Widgets Shortcode: from n/a through 1.0.3.	Patched by core rule	Y
CVE-2025-57988	CVE-2025-57988 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	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 3.0.7.3.	Patched by core rule	Y
CVE-2025-57986	CVE-2025-57986 - Improper Neutralization of Input During Web Page Generation ('Cross-site	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
	Scripting') vulnerability i...	husani WP Subtitle allows Stored XSS. This issue affects WP Subtitle: from n/a through 3.4.1.		
CVE-2025-57982	CVE-2025-57982 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPBean Advance Portfolio Grid allows Stored XSS. This issue affects Advance Portfolio Grid: from n/a through 1.07.6.	Patched by core rule	Y
CVE-2025-57981	CVE-2025-57981 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in catchsquare WP Social Widget allows Stored XSS. This issue affects WP Social Widget: from n/a through 2.3.1.	Patched by core rule	Y
CVE-2025-57980	CVE-2025-57980 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tomas Cordero Safety Exit allows Stored XSS. This issue affects Safety Exit: from n/a through 1.8.0.	Patched by core rule	Y
CVE-2025-57979	CVE-2025-57979 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Russell Jamieson AuthorSure allows Stored XSS. This issue affects AuthorSure: from n/a through 2.3.	Patched by core rule	Y
CVE-2025-57974	CVE-2025-57974 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tuyennv TZ PlusGallery allows Stored XSS. This issue affects TZ PlusGallery: from n/a through 1.5.5.	Patched by core rule	Y
CVE-2025-57973	CVE-2025-57973 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chad Butler WP-Members allows Stored XSS. This issue affects WP-Members: from n/a through 3.5.4.2.	Patched by core rule	Y
CVE-2025-57968	CVE-2025-57968 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e4jvikwp VikRestaurants Table Reservations and Take-Away allows Reflected XSS. This issue affects VikRestaurants Table Reservations and Take-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Away: from n/a through 1.4.		
CVE-2025-57967	CVE-2025-57967 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPBean WPB Quick View for WooCommerce allows Stored XSS. This issue affects WPB Quick View for WooCommerce: from n/a through 2.1.8.	Patched by core rule	Y
CVE-2025-57966	CVE-2025-57966 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GhozyLab Gallery Lightbox allows Stored XSS. This issue affects Gallery Lightbox: from n/a through 1.0.0.41.	Patched by core rule	Y
CVE-2025-57965	CVE-2025-57965 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP CodeUs WP Proposals allows Stored XSS. This issue affects WP Proposals: from n/a through 2.3.	Patched by core rule	Y
CVE-2025-57964	CVE-2025-57964 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in photonicgnostic Library Bookshelves allows Stored XSS. This issue affects Library Bookshelves: from n/a through 5.11.	Patched by core rule	Y
CVE-2025-57963	CVE-2025-57963 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zoho Subscriptions Zoho Billing allows DOM-Based XSS. This issue affects Zoho Billing: from n/a through 4.1.	Patched by core rule	Y
CVE-2025-57962	CVE-2025-57962 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e4jvikwp VikRestaurants Table Reservations and Take-Away allows Stored XSS. This issue affects VikRestaurants Table Reservations and Take-Away: from n/a through 1.4.	Patched by core rule	Y
CVE-2025-57959	CVE-2025-57959 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tmatsuur Slightly troublesome permalink allows Stored XSS. This issue affects Slightly troublesome	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		permalink: from n/a through 1.2.0.		
CVE-2025-57956	CVE-2025-57956 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpcraft WooMS allows Stored XSS. This issue affects WooMS: from n/a through 9.12.	Patched by core rule	Y
CVE-2025-57954	CVE-2025-57954 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ays Pro Poll Maker allows DOM-Based XSS. This issue affects Poll Maker: from n/a through 6.0.1.	Patched by core rule	Y
CVE-2025-57953	CVE-2025-57953 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 100plugins Open User Map allows DOM-Based XSS. This issue affects Open User Map: from n/a through 1.4.14.	Patched by core rule	Y
CVE-2025-57952	CVE-2025-57952 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in icopydoc Maps for WP allows Stored XSS. This issue affects Maps for WP: from n/a through 1.2.5.	Patched by core rule	Y
CVE-2025-57951	CVE-2025-57951 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ken107 SiteNarrator Text-to-Speech Widget allows Stored XSS. This issue affects SiteNarrator Text-to-Speech Widget: from n/a through 1.9.	Patched by core rule	Y
CVE-2025-57950	CVE-2025-57950 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Glen Scott Plugin Security Scanner allows Stored XSS. This issue affects Plugin Security Scanner: from n/a through 2.0.2.	Patched by core rule	Y
CVE-2025-57948	CVE-2025-57948 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e-plugins Directory Pro allows DOM-Based XSS. This issue affects Directory Pro: from n/a through 2.5.5.	Patched by core rule	Y
CVE-2025-57947	CVE-2025-57947 -	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ays Pro Photo Gallery by Ays allows DOM-Based XSS. This issue affects Photo Gallery by Ays: from n/a through 6.3.6.	rule	
CVE-2025-57945	CVE-2025-57945 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cedcommerce WP Advanced PDF allows Stored XSS. This issue affects WP Advanced PDF: from n/a through 1.1.7.	Patched by core rule	Y
CVE-2025-57941	CVE-2025-57941 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in JonathanMH Append Link on Copy allows Stored XSS. This issue affects Append Link on Copy: from n/a through 0.2.	Patched by core rule	Y
CVE-2025-57940	CVE-2025-57940 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Suresh Kumar Mukhiya Append extensions on Pages allows Stored XSS. This issue affects Append extensions on Pages: from n/a through 1.1.2.	Patched by core rule	Y
CVE-2025-57938	CVE-2025-57938 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themewant Easy Hotel Booking allows DOM-Based XSS. This issue affects Easy Hotel Booking: from n/a through 1.6.9.	Patched by core rule	Y
CVE-2025-57935	CVE-2025-57935 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ricky Dawn Bot Block – Stop Spam Referrals in Google Analytics allows Stored XSS. This issue affects Bot Block – Stop Spam Referrals in Google Analytics: from n/a through 2.6.	Patched by core rule	Y
CVE-2025-57932	CVE-2025-57932 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Diego Pereira PowerFolio allows Stored XSS. This issue affects PowerFolio: from n/a through 3.2.1.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-57929	CVE-2025-57929 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kanwei_doublethedonation Double the Donation allows Stored XSS. This issue affects Double the Donation: from n/a through 2.0.0.	Patched by core rule	Y
CVE-2025-57926	CVE-2025-57926 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Chill Passster allows Stored XSS. This issue affects Passster: from n/a through 4.2.18.	Patched by core rule	Y
CVE-2025-57920	CVE-2025-57920 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CK MacLeod Category Featured Images Extended allows Stored XSS. This issue affects Category Featured Images Extended: from n/a through 1.52.	Patched by core rule	Y
CVE-2025-57913	CVE-2025-57913 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eleopard Behance Portfolio Manager allows Stored XSS. This issue affects Behance Portfolio Manager: from n/a through 1.7.4.	Patched by core rule	Y
CVE-2025-57912	CVE-2025-57912 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in dialogity Dialogity Free Live Chat allows Stored XSS. This issue affects Dialogity Free Live Chat: from n/a through 1.0.3.	Patched by core rule	Y
CVE-2025-57911	CVE-2025-57911 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Adverts allows DOM-Based XSS. This issue affects Adverts: from n/a through 1.4.	Patched by core rule	Y
CVE-2025-57910	CVE-2025-57910 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AnyClip Video Platform AnyClip Luminous Studio allows Stored XSS. This issue affects AnyClip Luminous Studio: from n/a through 1.3.3.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-57908	CVE-2025-57908 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	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 1.6.4.	Patched by core rule	Y
CVE-2025-57906	CVE-2025-57906 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in epeken Epeken All Kurir allows Stored XSS. This issue affects Epeken All Kurir: from n/a through 2.0.2.	Patched by core rule	Y
CVE-2025-57904	CVE-2025-57904 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP-EXPERTS.IN Sales Count Manager for WooCommerce allows Stored XSS. This issue affects Sales Count Manager for WooCommerce: from n/a through 2.5.	Patched by core rule	Y
CVE-2025-57903	CVE-2025-57903 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPSuperiors Developer WooCommerce Additional Fees On Checkout (Free) allows Stored XSS. This issue affects WooCommerce Additional Fees On Checkout (Free): from n/a through 1.5.0.	Patched by core rule	Y
CVE-2025-57901	CVE-2025-57901 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DAEXT Import Markdown allows Stored XSS. This issue affects Import Markdown: from n/a through 1.14.	Patched by core rule	Y
CVE-2025-57900	CVE-2025-57900 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ataur R GutenKit allows Stored XSS. This issue affects GutenKit: from n/a through 2.4.2.	Patched by core rule	Y
CVE-2025-57898	CVE-2025-57898 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jose Vega WP Frontend Admin allows Stored XSS. This issue affects WP	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Frontend Admin: from n/a through 1.22.6.		
CVE-2025-55887	CVE-2025-55887 - Cross-Site Scripting (XSS) vulnerability was discovered in the meal reservation service ARD. The vul...	Cross-Site Scripting (XSS) vulnerability was discovered in the meal reservation service ARD. The vulnerability exists in the transactionID GET parameter on the transaction confirmation page. Due to improper input validation and output encoding, an attacker can inject malicious JavaScript code that is executed in the context of a user s browser. This can lead to session hijacking, theft of cookies, and other malicious actions performed on behalf of the victim.	Patched by core rule	Y
CVE-2025-53570	CVE-2025-53570 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	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 2.7.0.	Patched by core rule	Y
CVE-2025-53469	CVE-2025-53469 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mortgage Calculator BMI Adult & Kid Calculator allows Stored XSS. This issue affects BMI Adult & Kid Calculator: from n/a through 1.2.2.	Patched by core rule	Y
CVE-2025-53467	CVE-2025-53467 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webvitaly Login-Logout allows Stored XSS. This issue affects Login-Logout: from n/a through 3.8.	Patched by core rule	Y
CVE-2025-53466	CVE-2025-53466 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodeSolz Better Find and Replace allows Stored XSS. This issue affects Better Find and Replace: from n/a through 1.7.6.	Patched by core rule	Y
CVE-2025-53464	CVE-2025-53464 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ironikus WP Mailto Links allows Stored XSS. This issue affects WP Mailto Links: from n/a through 3.1.4.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-53463	CVE-2025-53463 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HT Plugins HT Mega – Absolute Addons for WPBakery Page Builder allows DOM-Based XSS. This issue affects HT Mega – Absolute Addons for WPBakery Page Builder: from n/a through 1.0.9.	Patched by core rule	Y
CVE-2025-53462	CVE-2025-53462 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SAPO SAPO Feed allows Stored XSS. This issue affects SAPO Feed: from n/a through 2.4.2.	Patched by core rule	Y
CVE-2025-53460	CVE-2025-53460 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Syed Balkhi AffiliateWP – External Referral Links allows Stored XSS. This issue affects AffiliateWP – External Referral Links: from n/a through 1.2.0.	Patched by core rule	Y
CVE-2025-53459	CVE-2025-53459 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ads by WPQuads Ads by WPQuads allows Stored XSS. This issue affects Ads by WPQuads: from n/a through 2.0.92.	Patched by core rule	Y
CVE-2025-53458	CVE-2025-53458 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in davaxi Goracash allows Stored XSS. This issue affects Goracash: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-53455	CVE-2025-53455 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CashBill CashBill.pl – Płatności WooCommerce allows Stored XSS. This issue affects CashBill.pl – Płatności WooCommerce: from n/a through 3.2.1.	Patched by core rule	Y
CVE-2025-53454	CVE-2025-53454 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rustaurius Ultimate WP Mail allows Stored XSS. This issue affects Ultimate WP Mail: from n/a through 1.3.8.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-55888	CVE-2025-55888 - Cross-Site Scripting (XSS) vulnerability was discovered in the Ajax transaction manager endpoint of ...	Cross-Site Scripting (XSS) vulnerability was discovered in the Ajax transaction manager endpoint of ARD. An attacker can intercept the Ajax response and inject malicious JavaScript into the accountName field. This input is not properly sanitized or encoded when rendered, allowing script execution in the context of users browsers. This flaw could lead to session hijacking, cookie theft, and other malicious actions.	Patched by core rule	Y
CVE-2025-43807	CVE-2025-43807 - Stored cross-site scripting (XSS) vulnerability in the notifications widget in Liferay Portal 7.4.0 ...	Stored cross-site scripting (XSS) vulnerability in the notifications widget in Liferay Portal 7.4.0 through 7.4.3.112, and Liferay DXP 2023.Q4.0 through 2023.Q4.8, 2023.Q3.1 through 2023.Q3.10, and 7.4 GA through update 92 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a publication’s “Name” text field.	Patched by core rule	Y
CVE-2025-57602	CVE-2025-57602 - Insufficient hardening of the proxyuser account in the AiKaan IoT management platform, combined with...	Insufficient hardening of the proxyuser account in the AiKaan IoT management platform, combined with the use of a shared, hardcoded SSH private key, allows remote attackers to authenticate to the cloud controller, gain interactive shell access, and pivot into other connected IoT devices. This can lead to remote code execution, information disclosure, and privilege escalation across customer environments.	Patched by core rule	Y
CVE-2025-57601	CVE-2025-57601 - AiKaan Cloud Controller uses a single hardcoded SSH private key and the username `proxyuser` for rem...	AiKaan Cloud Controller uses a single hardcoded SSH private key and the username `proxyuser` for remote terminal access to all managed IoT/edge devices. When an administrator initiates "Open Remote Terminal" from the AiKaan dashboard, the controller sends this same static private key to the target device. The device then uses it to establish a reverse SSH tunnel to a remote access server, enabling browser-based SSH access for the administrator. Because the same `proxyuser` account	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and SSH key are reused across all customer environments: - An attacker who obtains the key (e.g., by intercepting it in transit, extracting it from the remote access server, or from a compromised admin account) can impersonate any managed device. - They can establish unauthorized reverse SSH tunnels and interact with devices without the owner's consent. This is a design flaw in the authentication model: compromise of a single key compromises the trust boundary between the controller and devices.		
CVE-2025-10181	CVE-2025-10181 - The Draft List plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'd...	The Draft List plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'drafts' shortcode in all versions up to, and including, 2.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-56762	CVE-2025-56762 - Paracrawl KeOPs v2 is vulnerable to Cross Site Scripting (XSS) in error.php.	Paracrawl KeOPs v2 is vulnerable to Cross Site Scripting (XSS) in error.php.	Patched by core rule	Y
CVE-2025-52159	CVE-2025-52159 - Hardcoded credentials in default configuration of PPress 0.0.9.	Hardcoded credentials in default configuration of PPress 0.0.9.	Patched by core rule	Y
CVE-2025-10146	CVE-2025-10146 - The Download Manager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'u...	The Download Manager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'user_ids' parameter in all versions up to, and including, 3.3.23 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-2025-57452	CVE-2025-57452 - In realme BackupRestore app v15.1.12_2810c08_25031	In realme BackupRestore app v15.1.12_2810c08_250314, improper URI scheme	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	4, improper URI scheme handling in com.coloros.pc....	handling in com.coloros.pc.PcToolMainActivity allows local attackers to cause a crash and potential XSS via crafted ADB intents.		
CVE-2025-9992	CVE-2025-9992 - The Ghost Kit – Page Builder Blocks, Motion Effects & Extensions plugin for WordPress is vulnerable ...	The Ghost Kit – Page Builder Blocks, Motion Effects & Extensions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the custom JS field in all versions up to, and including, 3.4.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-10632	CVE-2025-10632 - A security flaw has been discovered in itsourcecode Online Petshop Management System 1.0. The affect...	A security flaw has been discovered in itsourcecode Online Petshop Management System 1.0. The affected element is an unknown function of the file availableframe.php of the component Admin Dashboard. The manipulation of the argument name/address results in cross site scripting. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	Patched by core rule	Y
CVE-2025-10631	CVE-2025-10631 - A vulnerability was identified in itsourcecode Online Petshop Management System 1.0. Impacted is an ...	A vulnerability was identified in itsourcecode Online Petshop Management System 1.0. Impacted is an unknown function of the file addcnp.php of the component Available Products Page. The manipulation of the argument name/description leads to cross site scripting. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2025-10606	CVE-2025-10606 - A weakness has been identified in Portabilis i-Educar up to 2.10. This issue affects some unknown pr...	A weakness has been identified in Portabilis i-Educar up to 2.10. This issue affects some unknown processing of the file /module/Configuracao/ConfiguracaoMovimentoGeral. This manipulation of the argument tipoacao causes cross site scripting. Remote	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.		
CVE-2025-10605	CVE-2025-10605 - A security flaw has been discovered in Portabilis i-Educar up to 2.10. This vulnerability affects un...	A security flaw has been discovered in Portabilis i-Educar up to 2.10. This vulnerability affects unknown code of the file /agenda_preferencias.php. The manipulation of the argument tipoacao results in cross site scripting. The attack may be launched remotely. The exploit has been released to the public and may be exploited.	Patched by core rule	Y
CVE-2025-10591	CVE-2025-10591 - A weakness has been identified in Portabilis i-Educar up to 2.10. This affects an unknown function o...	A weakness has been identified in Portabilis i-Educar up to 2.10. This affects an unknown function of the file /intranet/educar_funcao_cad.php of the component Editar Função Page. This manipulation of the argument abreviatura/tipoacao causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	Patched by core rule	Y
CVE-2025-10590	CVE-2025-10590 - A security flaw has been discovered in Portabilis i-Educar up to 2.10. The impacted element is an un...	A security flaw has been discovered in Portabilis i-Educar up to 2.10. The impacted element is an unknown function of the file /intranet/educar_usuario_det.php. The manipulation of the argument ref_pessoa results in cross site scripting. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	Patched by core rule	Y
CVE-2025-9565	CVE-2025-9565 - The Blocksy Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plug...	The Blocksy Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's blocksy_newsletter_subscribe shortcode in all versions up to, and including, 2.1.10 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		injected page.		
CVE-2025-9203	CVE-2025-9203 - The Media Player Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Script...	The Media Player Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'subtitle_ssize', 'track_title', and 'track_artist_name' parameters in version 1.0.5. This is due to insufficient input sanitization and output escaping on user-supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-10584	CVE-2025-10584 - A vulnerability was identified in Portabilis i-Educar up to 2.10. Impacted is an unknown function of...	A vulnerability was identified in Portabilis i-Educar up to 2.10. Impacted is an unknown function of the file /intranet/educar_calendario_anotacao_cad.php. Such manipulation of the argument nm_anotacao/descricao leads to cross site scripting. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2025-9851	CVE-2025-9851 - The Appointmind plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's '...	The Appointmind plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'appointmind_calendar' shortcode in all versions up to, and including, 4.1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-8394	CVE-2025-8394 - The Productive Style plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugi...	The Productive Style plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's display_productive_breadcrumb shortcode in all versions up to, and including, 1.1.23 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-10166	CVE-2025-10166 - The Social Media Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via th...	The Social Media Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'twitter' shortcode in all versions up to, and including, 1.3.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-43804	CVE-2025-43804 - Cross-site scripting (XSS) vulnerability in Search widget in Liferay Portal 7.4.3.93 through 7.4.3.111, and Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_portal_search_web_portlet_SearchPortlet_userId parameter.	Cross-site scripting (XSS) vulnerability in Search widget in Liferay Portal 7.4.3.93 through 7.4.3.111, and Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_portal_search_web_portlet_SearchPortlet_userId parameter.	Patched by core rule	Y
CVE-2025-57145	CVE-2025-57145 - A cross-site scripting (XSS) vulnerability exists in the search-autootaxi.php endpoint of the ATSMS ...	A cross-site scripting (XSS) vulnerability exists in the search-autootaxi.php endpoint of the ATSMS web application. The application fails to properly sanitize user input submitted through a form field, allowing an attacker to inject arbitrary JavaScript code. The malicious payload is stored in the backend and executed when a user or administrator accesses the affected report page. This allows attackers to exfiltrate session cookies, hijack user sessions, and perform unauthorized actions in the context of the victims browser.	Patched by core rule	Y
CVE-2025-56293	CVE-2025-56293 - code-projects Human Resource Integrated System 1.0 is vulnerable to Cross Site Scripting (XSS) in th...	code-projects Human Resource Integrated System 1.0 is vulnerable to Cross Site Scripting (XSS) in the Add Child Information section in the Childs Name field.	Patched by core rule	Y
CVE-2025-56289	CVE-2025-56289 - code-projects Document Management System 1.0	code-projects Document Management System 1.0 has a Cross Site Scripting (XSS)	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	has a Cross Site Scripting (XSS) vulnerability, where a...	vulnerability, where attackers can leak admin's cookie information by entering malicious XSS code in the Company field when adding files.		
CVE-2025-56280	CVE-2025-56280 - code-projects Food Ordering Review System 1.0 is vulnerable to Cross Site Scripting (XSS) in the are...	code-projects Food Ordering Review System 1.0 is vulnerable to Cross Site Scripting (XSS) in the area where users submit reservation information.	Patched by core rule	Y
CVE-2025-56276	CVE-2025-56276 - code-projects Food Ordering Review System 1.0 is vulnerable to Cross Site Scripting (XSS) in the reg...	code-projects Food Ordering Review System 1.0 is vulnerable to Cross Site Scripting (XSS) in the registration function. An attacker enters malicious JavaScript code as a username, which triggers the XSS vulnerability when the admin views user information, resulting in the disclosure of the admin's cookie information.	Patched by core rule	Y
CVE-2025-55834	CVE-2025-55834 - A Cross Site Scripting vulnerability in JeeWMS v.3.7 and before allows a remote attacker to obtain s...	A Cross Site Scripting vulnerability in JeeWMS v.3.7 and before allows a remote attacker to obtain sensitive information via the logController.do component	Patched by core rule	Y
CVE-2025-10485	CVE-2025-10485 - A vulnerability has been found in pojoin h3blog up to 5bf704425ebc11f4c24da51f32f36bb17ae20489. Affe...	A vulnerability has been found in pojoin h3blog up to 5bf704425ebc11f4c24da51f32f36bb17ae20489. Affected by this issue is the function ppt_log of the file /login of the component HTTP Header Handler. Such manipulation of the argument X-Forwarded-For leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed.	Patched by core rule	Y
CVE-2025-57117	CVE-2025-57117 - A Clickjacking vulnerability exists in Rems' Employee Management System 1.0. This flaw allows remote...	A Clickjacking vulnerability exists in Rems' Employee Management System 1.0. This flaw allows remote attackers to execute arbitrary JavaScript on the department.php page by injecting a malicious payload into the Department Name field under Add Department.	Patched by core rule	Y
CVE-2025-43802	CVE-2025-43802 - Stored cross-site scripting (XSS)	Stored cross-site scripting (XSS) vulnerability in a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	vulnerability in a custom object's /o/c/<object-name> API endpoint...	custom object's /o/c/<object-name> API endpoint in Liferay Portal 7.4.3.51 through 7.4.3.109, and Liferay DXP 2023.Q3.1 through 2023.Q3.4, 7.4 update 51 through update 92, and 7.3 update 33 through update 35. allows remote attackers to inject arbitrary web script or HTML via the externalReferenceCode parameter.		
CVE-2025-43800	CVE-2025-43800 - Cross-site scripting (XSS) vulnerability in Objects in Liferay Portal 7.4.3.20 through 7.4.3.111, an...	Cross-site scripting (XSS) vulnerability in Objects in Liferay Portal 7.4.3.20 through 7.4.3.111, and Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4 and 7.4 GA through update 92 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into an object with a rich text type field.	Patched by core rule	Y
CVE-2025-52344	CVE-2025-52344 - Multiple Cross Site Scripting (XSS) vulnerabilities in input fields in Explorance Blue 8.1.2 allows ...	Multiple Cross Site Scripting (XSS) vulnerabilities in input fields in Explorance Blue 8.1.2 allows attackers to inject arbitrary JavaScript code on the user's browser via the Group name and Project Description input fields.	Patched by core rule	Y
CVE-2025-43791	CVE-2025-43791 - Multiple cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.3.0 through 7.4.3.111, and L...	Multiple cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.3.0 through 7.4.3.111, and Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92 and 7.3 GA through update 36 allow remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a "Rich Text" type field to (1) a web content structure, (2) a Documents and Media Document Type , or (3) custom assets that uses the Data Engine's module Rich Text field.	Patched by core rule	Y
CVE-2025-56252	CVE-2025-56252 - Cross Site Scripting (xss) vulnerability in ServitiumCRM 2.10 allowing attackers to execute arbitrar...	Cross Site Scripting (xss) vulnerability in ServitiumCRM 2.10 allowing attackers to execute arbitrary code via a crafted URL to the mobile parameter.	Patched by core rule	Y
CVE-2025-43794	CVE-2025-43794 - Stored cross-site scripting (XSS) vulnerability in Liferay	Stored cross-site scripting (XSS) vulnerability in Liferay Portal 7.4.0 through	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Portal 7.4.0 through 7.4.3.111, and older...	7.4.3.111, and older unsupported versions, and Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions allows remote authenticated attackers with the instance administrator role to inject arbitrary web script or HTML into all pages via a crafted payload injected into the Instance Configuration's (1) CDN Host HTTP text field or (2) CDN Host HTTPS text field.		
CVE-2025-10434	CVE-2025-10434 - A vulnerability was identified in IbuyuCMS up to 2.6.3. Impacted is an unknown function of the file ...	A vulnerability was identified in IbuyuCMS up to 2.6.3. Impacted is an unknown function of the file /admin/article.php?a=mod of the component Add Article Page. The manipulation of the argument Title leads to cross site scripting. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2025-10388	CVE-2025-10388 - A vulnerability was identified in Selleo Mentingo 2025.08.27. This issue affects some unknown proces...	A vulnerability was identified in Selleo Mentingo 2025.08.27. This issue affects some unknown processing of the file /api/course/enroll-course of the component Create New Course Basic Settings. Such manipulation of the argument Description leads to cross site scripting. The attack can be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-10373	CVE-2025-10373 - A security vulnerability has been detected in Portabilis i-Educar up to 2.10. The affected element i...	A security vulnerability has been detected in Portabilis i-Educar up to 2.10. The affected element is an unknown function of the file /intranet/educar_turma_tipo_cad.php. Such manipulation of the argument nm_tipo leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2025-10372	CVE-2025-10372 - A	A weakness has been	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	weakness has been identified in Portabilis i-Educar up to 2.10. Impacted is an unknown function of...	identified in Portabilis i-Educar up to 2.10. Impacted is an unknown function of the file /intranet/educar_modulo_cad.php. This manipulation of the argument nm_tipo/descricao causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited.	rule	
CVE-2025-10370	CVE-2025-10370 - A vulnerability was identified in MiczFlor RPi-Jukebox-RFID up to 2.8.0. This vulnerability affects ...	A vulnerability was identified in MiczFlor RPi-Jukebox-RFID up to 2.8.0. This vulnerability affects unknown code of the file /htdocs/userScripts.php. The manipulation of the argument Custom script leads to cross site scripting. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-10369	CVE-2025-10369 - A vulnerability was determined in MiczFlor RPi-Jukebox-RFID up to 2.8.0. This affects an unknown par...	A vulnerability was determined in MiczFlor RPi-Jukebox-RFID up to 2.8.0. This affects an unknown part of the file /htdocs/cardRegisterNew.php. Executing manipulation can lead to cross site scripting. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-10368	CVE-2025-10368 - A vulnerability was found in MiczFlor RPi-Jukebox-RFID up to 2.8.0. Affected by this issue is some u...	A vulnerability was found in MiczFlor RPi-Jukebox-RFID up to 2.8.0. Affected by this issue is some unknown functionality of the file /htdocs/manageFilesFolders.php. Performing manipulation results in cross site scripting. Remote exploitation of the attack is possible. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-10367	CVE-2025-10367 - A vulnerability has been found in MiczFlor RPi-Jukebox-RFID up to 2.8.0.	A vulnerability has been found in MiczFlor RPi-Jukebox-RFID up to 2.8.0. Affected by this vulnerability	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Affected by this vulnerabil...	is an unknown functionality of the file /htdocs/cardEdit.php. Such manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-10366	CVE-2025-10366 - A flaw has been found in MiczFlor RPi-Jukebox-RFID up to 2.8.0. Affected is an unknown function of t...	A flaw has been found in MiczFlor RPi-Jukebox-RFID up to 2.8.0. Affected is an unknown function of the file /htdocs/inc.setWlanIpMail.php. This manipulation of the argument Email address causes cross site scripting. The attack may be initiated remotely. The exploit has been published 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-2025-10340	CVE-2025-10340 - A vulnerability was determined in WhatCD Gazelle up to 63b337026d49b5cf63ce4be20fdabdc880112fa3. The...	A vulnerability was determined in WhatCD Gazelle up to 63b337026d49b5cf63ce4be20fdabdc880112fa3. The affected element is an unknown function of the file /sections/tools/managers/change_log.php of the component Commit Message Handler. Executing manipulation of the argument Message can lead to cross site scripting. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed.	Patched by core rule	Y
CVE-2025-10332	CVE-2025-10332 - A vulnerability was found in cdevroe unmark up to 1.9.3. Impacted is an unknown function of the file...	A vulnerability was found in cdevroe unmark up to 1.9.3. Impacted is an unknown function of the file application/views/marks/info.php. Performing manipulation of the argument Title results in cross site scripting. The attack is possible to be carried out remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		but did not respond in any way.		
CVE-2025-10331	CVE-2025-10331 - A vulnerability has been found in cdevroe unmark up to 1.9.3. This issue affects some unknown proces...	A vulnerability has been found in cdevroe unmark up to 1.9.3. This issue affects some unknown processing of the file /application/controllers/Marks.php. Such manipulation of the argument Title leads to cross site scripting. The attack can be executed 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-2025-10330	CVE-2025-10330 - A flaw has been found in cdevroe unmark up to 1.9.3. This vulnerability affects unknown code of the ...	A flaw has been found in cdevroe unmark up to 1.9.3. This vulnerability affects unknown code of the file application/views/layouts/topbar/searchform.php. This manipulation of the argument q causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been published 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-2025-52074	CVE-2025-52074 - PHPGURUKUL Online Shopping Portal 2.1 is vulnerable to Cross Site Scripting (XSS) due to lack of inp...	PHPGURUKUL Online Shopping Portal 2.1 is vulnerable to Cross Site Scripting (XSS) due to lack of input sanitization in the quantity parameter when adding a product to the cart.	Patched by core rule	Y
CVE-2025-43787	CVE-2025-43787 - A Stored cross-site scripting vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Life...	A Stored cross-site scripting vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q3.0, 2025.Q2.0 through 2025.Q2.12, 2025.Q1.0 through 2025.Q1.17, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13 and 2024.Q1.1 through 2024.Q1.20 allows an remote authenticated attacker to inject JavaScript through the organization site names. The malicious payload is stored and executed without proper sanitization or escaping.	Patched by core rule	Y
CVE-2025-57579	CVE-2025-57579 - An issue in TOTOLINK Wi-Fi 6 Router Series Device	An issue in TOTOLINK Wi-Fi 6 Router Series Device X2000R-Gh-V2.0.0 allows a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	X2000R-Gh-V2.0.0 allows a remote attacker to execu...	remote attacker to execute arbitrary code via the default password		
CVE-2025-57578	CVE-2025-57578 - An issue in H3C Magic M Device M2V100R006 allows a remote attacker to execute arbitrary code via the...	An issue in H3C Magic M Device M2V100R006 allows a remote attacker to execute arbitrary code via the default password	Patched by core rule	Y
CVE-2025-57577	CVE-2025-57577 - An issue in H3C Device R365V300R004 allows a remote attacker to execute arbitrary code via the defau...	An issue in H3C Device R365V300R004 allows a remote attacker to execute arbitrary code via the default password. NOTE: the Supplier's position is that their "product lines enforce or clearly prompt users to change any initial credentials upon first use. At most, this would be a case of misconfiguration if an administrator deliberately ignored the prompts, which is outside the scope of CVE definitions."	Patched by core rule	Y
CVE-2025-9879	CVE-2025-9879 - The Spotify Embed Creator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ...	The Spotify Embed Creator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'spotify' shortcode in all versions up to, and including, 1.0.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-9877	CVE-2025-9877 - The Embed Google Datastudio plugin for WordPress is vulnerable to Stored Cross-Site Scripting via th...	The Embed Google Datastudio plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'egds' shortcode in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-9861	CVE-2025-9861 - The ThemeLoom Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via	The ThemeLoom Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'los_showposts' shortcode in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	the plug...	all versions up to, and including, 1.8.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-9860	CVE-2025-9860 - The Mixtape plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'mixt...	The Mixtape plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'mixtape' shortcode in all versions up to, and including, 1.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-9855	CVE-2025-9855 - The Enhanced BibliPlug plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plu...	The Enhanced BibliPlug plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'bibliplug_authors' shortcode in all versions up to, and including, 1.3.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-9850	CVE-2025-9850 - The Evenium plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'even...	The Evenium plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'evenium_single_event' shortcode in all versions up to, and including, 1.3.11 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-9128	CVE-2025-9128 - The eID	The eID Easy plugin for	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Easy plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' paramete...	WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter in all versions up to, and including, 4.9.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	rule	
CVE-2025-8445	CVE-2025-8445 - The Countdown Timer for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting ...	The Countdown Timer for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'countdown_label' Parameter in all versions up to, and including, 1.3.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-5801	CVE-2025-5801 - The Digital Events Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via th...	The Digital Events Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'column' parameter in all versions up to, and including, 1.0.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-43783	CVE-2025-43783 - Reflected cross-site scripting (XSS) vulnerability in Liferay Portal 7.4.3.73 through 7.4.3.128, and...	Reflected cross-site scripting (XSS) vulnerability in Liferay Portal 7.4.3.73 through 7.4.3.128, and Liferay DXP 2024.Q3.0 through 2024.Q3.1, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.12, 7.4 update 73 through update 92 allows remote attackers to inject arbitrary web script or HTML via the /c/portal/comment/discussion/get_editor path.	Patched by core rule	Y
CVE-2025-43785	CVE-2025-43785 - Stored	Stored cross-site scripting	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	cross-site scripting (XSS) vulnerability in Liferay Portal 7.4.3.45 through 7.4.3.128, and Li...	(XSS) vulnerability in Liferay Portal 7.4.3.45 through 7.4.3.128, and Liferay DXP 2024 Q2.0 through 2024.Q2.9, 2024.Q1.1 through 2024.Q1.12, and 7.4 update 45 through update 92 allows remote attackers to execute an arbitrary web script or HTML in the My Workflow Tasks page.	rule	
CVE-2025-56466	CVE-2025-56466 - Hardcoded credentials in Dietly v1.25.0 for android allows attackers to gain sensitive information.	Hardcoded credentials in Dietly v1.25.0 for android allows attackers to gain sensitive information.	Patched by core rule	Y
CVE-2025-9857	CVE-2025-9857 - The Heateor Login – Social Login Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scri...	The Heateor Login – Social Login Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'Heateor_Facebook_Login' shortcode in all versions up to, and including, 1.1.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-9367	CVE-2025-9367 - The Welcart e-Commerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via setting...	The Welcart e-Commerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via settings in all versions up to, and including, 2.11.20 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with editor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	Patched by core rule	Y
CVE-2025-10126	CVE-2025-10126 - The MyBrain Utilities plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plug...	The MyBrain Utilities plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugins's 'mbumap' shortcode in all versions up to, and including, 1.0.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-8388	CVE-2025-8388 - The PowerPack Elementor Addons (Free Widgets, Extensions and Templates) plugin for WordPress is vuln...	The PowerPack Elementor Addons (Free Widgets, Extensions and Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'cursor_url' parameter in all versions up to, and including, 2.9.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-43786	CVE-2025-43786 - Enumeration of ERC from object entry in Liferay Portal 7.4.0 through 7.4.3.128, and Liferay DXP 2024...	Enumeration of ERC from object entry in Liferay Portal 7.4.0 through 7.4.3.128, and Liferay DXP 2024.Q3.0 through 2024.Q3.1, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.12, 2023.Q4.0 and 7.4 GA through update 92 allow attackers to determine existent ERC in the application by exploit the time response.	Patched by core rule	Y
CVE-2025-43781	CVE-2025-43781 - Reflected cross-site scripting (XSS) vulnerability in Liferay Portal 7.4.3.110 through 7.4.3.128, an...	Reflected cross-site scripting (XSS) vulnerability in Liferay Portal 7.4.3.110 through 7.4.3.128, and Liferay DXP 2024.Q3.1 through 2024.Q3.8, 2024.Q2.0 through 2024.Q2.13 and 2024.Q1.1 through 2024.Q1.12 allows remote attackers to inject arbitrary web script or HTML via the URL in search bar portlet	Patched by core rule	Y
CVE-2025-43775	CVE-2025-43775 - Stored cross-site scripting (XSS) vulnerability in Liferay Portal 7.4.0 through 7.4.3.128, and Lifer...	Stored cross-site scripting (XSS) vulnerability in Liferay Portal 7.4.0 through 7.4.3.128, and Liferay DXP 2024.Q3.0 through 2024.Q3.5, 2024.Q2.0 through 2024.Q2.12, 2024.Q1.1 through 2024.Q1.12, and 7.4 GA through update 92 allows remote attackers to inject arbitrary web script or HTML via remote app title field.	Patched by core rule	Y
CVE-2025-58990	CVE-2025-58990 -	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Input During Web Page Generation ('Cross-site Scripting') vulnerability in HasTech ShopLentor allows Stored XSS. This issue affects ShopLentor: from n/a through 3.2.0.	rule	
CVE-2025-58989	CVE-2025-58989 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in silverplugins217 Dynamic Text Field For Contact Form 7 allows Stored XSS. This issue affects Dynamic Text Field For Contact Form 7: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-58988	CVE-2025-58988 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Joe Dolson My Tickets allows Stored XSS. This issue affects My Tickets: from n/a through 2.0.22.	Patched by core rule	Y
CVE-2025-58987	CVE-2025-58987 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AntoineH Football Pool allows Stored XSS. This issue affects Football Pool: from n/a through 2.12.6.	Patched by core rule	Y
CVE-2025-58985	CVE-2025-58985 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Additional Custom Product Tabs for WooCommerce allows Stored XSS. This issue affects Additional Custom Product Tabs for WooCommerce: from n/a through 1.7.3.	Patched by core rule	Y
CVE-2025-58984	CVE-2025-58984 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in nanbu Welcart e-Commerce allows Stored XSS. This issue affects Welcart e-Commerce: from n/a through 2.11.20.	Patched by core rule	Y
CVE-2025-58983	CVE-2025-58983 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Stefano Lissa Include Me allows Stored XSS. This issue affects Include Me: from n/a through 1.3.2.	Patched by core rule	Y
CVE-2025-58982	CVE-2025-58982 - Improper Neutralization of Input During Web Page	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
	Generation ('Cross-site Scripting') vulnerability i...	Scripting') vulnerability in pixeline Pixeline's Email Protector allows Stored XSS. This issue affects Pixeline's Email Protector: from n/a through 1.3.8.		
CVE-2025-47694	CVE-2025-47694 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in solwin Blog Designer PRO. This issue affects Blog Designer PRO: from n/a through 3.4.7.	Patched by core rule	Y
CVE-2025-47570	CVE-2025-47570 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in villatheme WooCommerce Photo Reviews. This issue affects WooCommerce Photo Reviews: from n/a through 1.3.13.	Patched by core rule	Y
CVE-2025-30875	CVE-2025-30875 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alexandre Froger WP Weixin allows Stored XSS. This issue affects WP Weixin: from n/a through 1.3.16.	Patched by core rule	Y
CVE-2025-52277	CVE-2025-52277 - Cross Site Scripting vulnerability in YesWiki v.4.54 allows a remote attacker to execute arbitrary c...	Cross Site Scripting vulnerability in YesWiki v.4.54 allows a remote attacker to execute arbitrary code via a crafted payload to the meta configuration robots field	Patched by core rule	Y
CVE-2025-43778	CVE-2025-43778 - A Stored cross-site scripting vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Life...	A Stored cross-site scripting vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.11, 2025.Q1.0 through 2025.Q1.16, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13 and 2024.Q1.1 through 2024.Q1.20 allows an remote authenticated attacker to inject JavaScript through the name of a fieldset in Kaleo Forms Admin. The malicious payload is stored and executed without proper sanitization or escaping.	Patched by core rule	Y
CVE-2025-10099	CVE-2025-10099 - A weakness has been identified in Portabilis i-Educar up to 2.10.	A weakness has been identified in Portabilis i-Educar up to 2.10. Affected by this vulnerability is an	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Affected by this vulnerability is ...	unknown functionality of the file /intranet/educar_usuario_cad.php of the component Editar usuário Page. This manipulation of the argument email/data_inicial/data_expiracao causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited.		
CVE-2025-55998	CVE-2025-55998 - A cross-site scripting (XSS) vulnerability in Smart Search & Filter Shopify and BigCommerce apps all...	A cross-site scripting (XSS) vulnerability in Smart Search & Filter Shopify and BigCommerce apps allows a remote attacker to execute arbitrary JavaScript in the web browser of a user, by including a malicious payload into several filter parameter	Patched by core rule	Y
CVE-2014-125128	CVE-2014-125128 - 'sanitize-html' prior to version 1.0.3 is vulnerable to Cross-site Scripting (XSS). The function 'na...	'sanitize-html' prior to version 1.0.3 is vulnerable to Cross-site Scripting (XSS). The function 'naughtyHref' doesn't properly validate the hyperreference (`href`) attribute in anchor tags (`<a>`), allowing bypasses that contain different casings, whitespace characters, or hexadecimal encodings.	Patched by core rule	Y
CVE-2019-25225	CVE-2019-25225 - `sanitize-html` prior to version 2.0.0-beta is vulnerable to Cross-site Scripting (XSS). The `saniti...	`sanitize-html` prior to version 2.0.0-beta is vulnerable to Cross-site Scripting (XSS). The `sanitizeHtml()` function in `index.js` does not sanitize content when using the custom `transformTags` option, which is intended to convert attribute values into text. As a result, malicious input can be transformed into executable code.	Patched by core rule	Y
CVE-2025-10074	CVE-2025-10074 - A vulnerability was identified in Portabilis i-Educar up to 2.10. The affected element is an unknown...	A vulnerability was identified in Portabilis i-Educar up to 2.10. The affected element is an unknown function of the file /usuarios/tipos/. The manipulation of the argument Tipos de Usuário/Descrição leads to cross site scripting. The attack can be initiated remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2025-10067	CVE-2025-10067 - A vulnerability was detected in itsourcecode	A vulnerability was detected in itsourcecode POS Point of Sale System 1.0. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	POS Point of Sale System 1.0. The impacted element is a...	impacted element is an unknown function of the file /inventory/main/vendors/datatables/unit_testing/templates/empty_table.php. Performing manipulation of the argument scripts results in cross site scripting. It is possible to initiate the attack remotely. The exploit is now public and may be used.		
CVE-2025-10066	CVE-2025-10066 - A security vulnerability has been detected in itsourcecode POS Point of Sale System 1.0. The affecte...	A security vulnerability has been detected in itsourcecode POS Point of Sale System 1.0. The affected element is an unknown function of the file /inventory/main/vendors/datatables/unit_testing/templates/dymanic_table.php. Such manipulation of the argument scripts leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2025-10065	CVE-2025-10065 - A weakness has been identified in itsourcecode POS Point of Sale System 1.0. Impacted is an unknown ...	A weakness has been identified in itsourcecode POS Point of Sale System 1.0. Impacted is an unknown function of the file /inventory/main/vendors/datatables/unit_testing/templates/dom_data_th.php. This manipulation of the argument scripts causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	Patched by core rule	Y
CVE-2025-10064	CVE-2025-10064 - A security flaw has been discovered in itsourcecode POS Point of Sale System 1.0. This issue affects...	A security flaw has been discovered in itsourcecode POS Point of Sale System 1.0. This issue affects some unknown processing of the file /inventory/main/vendors/datatables/unit_testing/templates/dom_data_two_headers.php. The manipulation of the argument scripts results in cross site scripting. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	Patched by core rule	Y
CVE-2025-10063	CVE-2025-10063 - A vulnerability was identified in itsourcecode POS Point of Sale System 1.0. This vulnerability affe...	A vulnerability was identified in itsourcecode POS Point of Sale System 1.0. This vulnerability affects unknown code of the file /inventory/main/vendors/da	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		tatables/unit_testing/templates/deferred_table.php. The manipulation of the argument scripts leads to cross site scripting. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.		
CVE-2025-10029	CVE-2025-10029 - A security flaw has been discovered in itsourcecode POS Point of Sale System 1.0. This vulnerability...	A security flaw has been discovered in itsourcecode POS Point of Sale System 1.0. This vulnerability affects unknown code of the file /inventory/main/vendors/datatables/unit_testing/templates/complex_header_2.php. Performing manipulation of the argument scripts results in cross site scripting. The attack may be initiated remotely. The exploit has been released to the public and may be exploited.	Patched by core rule	Y
CVE-2025-10028	CVE-2025-10028 - A vulnerability was identified in itsourcecode POS Point of Sale System 1.0. This affects an unknown...	A vulnerability was identified in itsourcecode POS Point of Sale System 1.0. This affects an unknown part of the file /inventory/main/vendors/datatables/unit_testing/templates/6776.php. Such manipulation of the argument scripts leads to cross site scripting. The attack can be launched remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2025-6757	CVE-2025-6757 - The Recent Posts Widget Extended plugin for WordPress is vulnerable to Stored Cross-Site Scripting v...	The Recent Posts Widget Extended plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'rpwe' shortcode in all versions up to, and including, 2.0.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-9493	CVE-2025-9493 - The Admin Menu Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'pla...	The Admin Menu Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'placeholder' parameter in all versions up to, and including, 1.14 due to insufficient input sanitization and output escaping. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-9442	CVE-2025-9442 - The StreamWeasels Kick Integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting...	The StreamWeasels Kick Integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'vodsChannel' parameter in all versions up to, and including, 1.1.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-9126	CVE-2025-9126 - The Smart Table Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'i...	The Smart Table Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter in all versions up to, and including, 1.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-8722	CVE-2025-8722 - The Content Views plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's...	The Content Views plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Grid and List widgets in all versions up to, and including, 4.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-8564	CVE-2025-8564 - The SKT Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via m...	The SKT Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple widgets in all versions up to, and including, 3.7 due to insufficient input sanitization and output escaping on user	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-8149	CVE-2025-8149 - The aThemes Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting v...	The aThemes Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Countdown widget in all versions up to, and including, 1.1.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-9853	CVE-2025-9853 - The Optio Dentistry plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin...	The Optio Dentistry plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'optio-lightbox' shortcode in all versions up to, and including, 2.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-8360	CVE-2025-8360 - The LA-Studio Element Kit for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scri...	The LA-Studio Element Kit for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several of the plugin's widgets in all versions up to, and including, 1.5.5.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-9849	CVE-2025-9849 - The Html Social share buttons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via ...	The Html Social share buttons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'zm_sh_btn' shortcode in all versions up	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to, and including, 2.1.16 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-6067	CVE-2025-6067 - The Easy Social Feed – Social Photos Gallery – Post Feed – Like Box plugin for WordPress is vulnerab...	The Easy Social Feed – Social Photos Gallery – Post Feed – Like Box plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `data-caption` and `data-linktext` parameters in all versions up to, and including, 6.6.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-10027	CVE-2025-10027 - A vulnerability was determined in itsourcecode POS Point of Sale System 1.0. Affected by this issue ...	A vulnerability was determined in itsourcecode POS Point of Sale System 1.0. Affected by this issue is some unknown functionality of the file /inventory/main/vendors/datatables/unit_testing/templates/2512.php. This manipulation of the argument scripts causes cross site scripting. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-10026	CVE-2025-10026 - A vulnerability was found in itsourcecode POS Point of Sale System 1.0. Affected by this vulnerabili...	A vulnerability was found in itsourcecode POS Point of Sale System 1.0. Affected by this vulnerability is an unknown functionality of the file /inventory/main/vendors/datatables/unit_testing/templates/-complex_header.php. The manipulation of the argument scripts results in cross site scripting. It is possible to launch the attack remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2025-53307	CVE-2025-53307 - Improper Neutralization	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Generation ('Cross-site Scripting') vulnerability in Brent Jett Assistant allows Reflected XSS. This issue affects Assistant: from n/a through 1.5.2.		
CVE-2025-48105	CVE-2025-48105 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vincent Boiardt Easy Flash Embed allows Stored XSS. This issue affects Easy Flash Embed: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-48103	CVE-2025-48103 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mulscully Today's Date Inserter allows Stored XSS. This issue affects Today's Date Inserter: from n/a through 1.2.1.	Patched by core rule	Y
CVE-2025-48102	CVE-2025-48102 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gourl GoUrl Bitcoin Payment Gateway & Paid Downloads & Membership allows Stored XSS. This issue affects GoUrl Bitcoin Payment Gateway & Paid Downloads & Membership: from n/a through 1.6.6.	Patched by core rule	Y
CVE-2025-58887	CVE-2025-58887 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Course Finder | andré martin - it solutions & research UG Course Booking Platform allows Stored XSS. This issue affects Course Booking Platform: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-58886	CVE-2025-58886 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tan Nguyen Instant Locations allows Stored XSS. This issue affects Instant Locations: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-58884	CVE-2025-58884 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ivan Drago vipdrv allows Stored XSS. This issue affects vipdrv: from n/a through	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		1.0.3.		
CVE-2025-58883	CVE-2025-58883 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Thomas Harris Search Cloud One allows Stored XSS. This issue affects Search Cloud One: from n/a through 2.2.5.	Patched by core rule	Y
CVE-2025-58882	CVE-2025-58882 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in w1zzard Simple Text Slider allows Stored XSS. This issue affects Simple Text Slider: from n/a through 1.0.5.	Patched by core rule	Y
CVE-2025-58880	CVE-2025-58880 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in reubenthiessen Translate This gTranslate Shortcode allows Stored XSS. This issue affects Translate This gTranslate Shortcode: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-58876	CVE-2025-58876 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ali Aghdam Aparat Video Shortcode allows Stored XSS. This issue affects Aparat Video Shortcode: from n/a through 0.2.4.	Patched by core rule	Y
CVE-2025-58875	CVE-2025-58875 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sudar Muthu WP Github Gist allows Stored XSS. This issue affects WP Github Gist: from n/a through 0.5.	Patched by core rule	Y
CVE-2025-58874	CVE-2025-58874 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in josepsitjar StoryMap allows DOM-Based XSS. This issue affects StoryMap: from n/a through 2.1.	Patched by core rule	Y
CVE-2025-58873	CVE-2025-58873 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pusheco Pushe Web Push Notification allows Stored XSS. This issue affects Pushe Web Push Notification: from n/a through 0.5.0.	Patched by core rule	Y
CVE-2025-58871	CVE-2025-58871 -	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Input During Web Page Generation ('Cross-site Scripting') vulnerability in Luis Rock Master Paper Collapse Toggle allows Stored XSS. This issue affects Master Paper Collapse Toggle: from n/a through 1.1.	rule	
CVE-2025-58870	CVE-2025-58870 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DeBAAT WP-GraphViz allows DOM-Based XSS. This issue affects WP-GraphViz: from n/a through 1.5.1.	Patched by core rule	Y
CVE-2025-58868	CVE-2025-58868 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Simasicher SimaCookie allows Stored XSS. This issue affects SimaCookie: from n/a through 1.3.2.	Patched by core rule	Y
CVE-2025-58867	CVE-2025-58867 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Remi Corson Easy Download Media Counter allows Stored XSS. This issue affects Easy Download Media Counter: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-58864	CVE-2025-58864 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in iamroody 金数据 allows Stored XSS. This issue affects 金数据: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-58863	CVE-2025-58863 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SdeWijs Zoomify embed for WP allows Stored XSS. This issue affects Zoomify embed for WP: from n/a through 1.5.2.	Patched by core rule	Y
CVE-2025-58862	CVE-2025-58862 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in George Sexton WordPress Events Calendar Plugin – connectDaily allows Stored XSS. This issue affects WordPress Events Calendar Plugin – connectDaily: from n/a through 1.5.3.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-58858	CVE-2025-58858 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPBean WPB Image Widget allows Stored XSS. This issue affects WPB Image Widget: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-58857	CVE-2025-58857 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in KaizenCoders Table of content allows Stored XSS. This issue affects Table of content: from n/a through 1.5.3.1.	Patched by core rule	Y
CVE-2025-58851	CVE-2025-58851 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DigitalCourt Boxed Content allows Stored XSS. This issue affects Boxed Content: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-58850	CVE-2025-58850 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in marcshowpass Showpass WordPress Extension allows Stored XSS. This issue affects Showpass WordPress Extension: from n/a through 4.0.3.	Patched by core rule	Y
CVE-2025-58842	CVE-2025-58842 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in givecloud Donation Forms WP by Givecloud allows Stored XSS. This issue affects Donation Forms WP by Givecloud: from n/a through 1.0.9.	Patched by core rule	Y
CVE-2025-58840	CVE-2025-58840 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ibnul H. Custom Team Manager allows Stored XSS. This issue affects Custom Team Manager: from n/a through 2.4.2.	Patched by core rule	Y
CVE-2025-58838	CVE-2025-58838 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zakir Smooth Accordion allows Stored XSS. This issue affects Smooth Accordion: from n/a through 2.1.	Patched by core rule	Y
CVE-2025-58837	CVE-2025-58837 -	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Input During Web Page Generation ('Cross-site Scripting') vulnerability in Shiful H SS Font Awesome Icon allows Stored XSS. This issue affects SS Font Awesome Icon: from n/a through 4.1.3.	rule	
CVE-2025-58836	CVE-2025-58836 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tikolan FW Anker allows Stored XSS. This issue affects FW Anker: from n/a through 1.2.6.	Patched by core rule	Y
CVE-2025-58834	CVE-2025-58834 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gugu short.io allows DOM-Based XSS. This issue affects short.io: from n/a through 2.4.0.	Patched by core rule	Y
CVE-2025-58832	CVE-2025-58832 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webvitaly Search by Google allows Stored XSS. This issue affects Search by Google: from n/a through 1.9.	Patched by core rule	Y
CVE-2025-58830	CVE-2025-58830 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in snagysandor Parallax Scrolling Enllax.js allows Stored XSS. This issue affects Parallax Scrolling Enllax.js: from n/a through 0.0.6.	Patched by core rule	Y
CVE-2025-58828	CVE-2025-58828 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in codemstory 코드엠샵 소셜톡 allows Stored XSS. This issue affects 코드엠샵 소셜톡: from n/a through 1.2.1.	Patched by core rule	Y
CVE-2025-58826	CVE-2025-58826 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Eric Mann WP Publication Archive allows Stored XSS. This issue affects WP Publication Archive : from n/a through 3.0.1.	Patched by core rule	Y
CVE-2025-58825	CVE-2025-58825 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Habibur Rahman Comment	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	i...	Form WP – Customize Default Comment Form allows Stored XSS. This issue affects Comment Form WP – Customize Default Comment Form: from n/a through 2.0.0.		
CVE-2025-58823	CVE-2025-58823 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in The African Boss Get Cash allows Stored XSS. This issue affects Get Cash: from n/a through 3.2.2.	Patched by core rule	Y
CVE-2025-58822	CVE-2025-58822 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mndpsingh287 WP Mail allows DOM-Based XSS. This issue affects WP Mail: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-58821	CVE-2025-58821 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpdever WP Notification Bell allows Stored XSS. This issue affects WP Notification Bell: from n/a through 1.4.5.	Patched by core rule	Y
CVE-2025-58820	CVE-2025-58820 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themepoints Carousel Ultimate allows Stored XSS. This issue affects Carousel Ultimate: from n/a through 1.8.	Patched by core rule	Y
CVE-2025-58814	CVE-2025-58814 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ram Ratan Maurya Stagtools allows Stored XSS. This issue affects Stagtools: from n/a through 2.3.8.	Patched by core rule	Y
CVE-2025-58812	CVE-2025-58812 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PriceListo Best Restaurant Menu by PriceListo allows Stored XSS. This issue affects Best Restaurant Menu by PriceListo: from n/a through 1.4.3.	Patched by core rule	Y
CVE-2025-58811	CVE-2025-58811 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP CodeUs Ultimate Client Dash allows Stored XSS. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		issue affects Ultimate Client Dash: from n/a through 4.6.		
CVE-2025-58810	CVE-2025-58810 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jimmywb Simple Link List Widget allows Stored XSS. This issue affects Simple Link List Widget: from n/a through 0.3.2.	Patched by core rule	Y
CVE-2025-58808	CVE-2025-58808 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Babar prettyPhoto allows Stored XSS. This issue affects prettyPhoto: from n/a through 1.2.4.	Patched by core rule	Y
CVE-2025-58805	CVE-2025-58805 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in OTWthemes Widgetize Pages Light allows Stored XSS. This issue affects Widgetize Pages Light: from n/a through 3.0.	Patched by core rule	Y
CVE-2025-58796	CVE-2025-58796 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in dudaster Elementor Element Condition allows Stored XSS. This issue affects Elementor Element Condition: from n/a through 1.0.5.	Patched by core rule	Y
CVE-2025-58793	CVE-2025-58793 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPBean WPB Elementor Addons allows Stored XSS. This issue affects WPB Elementor Addons: from n/a through 1.6.	Patched by core rule	Y
CVE-2025-58791	CVE-2025-58791 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Arjan Olsder SEO Auto Linker allows Stored XSS. This issue affects SEO Auto Linker: from n/a through 1.5.3.	Patched by core rule	Y
CVE-2025-58790	CVE-2025-58790 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPKube Kiwi allows Stored XSS. This issue affects Kiwi: from n/a through 2.1.8.	Patched by core rule	Y
CVE-2025-58787	CVE-2025-58787 - Improper Neutralization	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Generation ('Cross-site Scripting') vulnerability in themifyme Themify Popup allows Stored XSS. This issue affects Themify Popup: from n/a through 1.4.4.		
CVE-2025-58786	CVE-2025-58786 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VW THEMES Ibtana – Ecommerce Product Addons allows DOM-Based XSS. This issue affects Ibtana – Ecommerce Product Addons: from n/a through 0.4.7.4.	Patched by core rule	Y
CVE-2025-58784	CVE-2025-58784 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in arisoft ARI Fancy Lightbox allows Stored XSS. This issue affects ARI Fancy Lightbox: from n/a through 1.4.0.	Patched by core rule	Y
CVE-2025-57576	CVE-2025-57576 - PHPGurukul Online Shopping Portal 2.1 is vulnerable to Cross Site Scripting (XSS) in /admin/updateor...	PHPGurukul Online Shopping Portal 2.1 is vulnerable to Cross Site Scripting (XSS) in /admin/updateorder.php.	Patched by core rule	Y
CVE-2025-9940	CVE-2025-9940 - A vulnerability was detected in CodeAstro Real Estate Management System 1.0. This affects an unknown...	A vulnerability was detected in CodeAstro Real Estate Management System 1.0. This affects an unknown function of the file /feature.php. Performing manipulation of the argument msg results in cross site scripting. The attack can be initiated remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-9939	CVE-2025-9939 - A security vulnerability has been detected in CodeAstro Real Estate Management System 1.0. The impac...	A security vulnerability has been detected in CodeAstro Real Estate Management System 1.0. The impacted element is an unknown function of the file /propertyview.php. Such manipulation of the argument msg leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2025-45805	CVE-2025-45805 - In phpgurukul Doctor Appointment Management System 1.0, an authenticated doctor user can inject arbi...	In phpgurukul Doctor Appointment Management System 1.0, an authenticated doctor user can inject arbitrary JavaScript code into their profile name. This payload is subsequently rendered	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		without proper sanitization, when a user visits the website and selects the doctor to book an appointment.		
CVE-2025-55944	CVE-2025-55944 - Slink v1.4.9 allows stored cross-site scripting (XSS) via crafted SVG uploads. When a user views the...	Slink v1.4.9 allows stored cross-site scripting (XSS) via crafted SVG uploads. When a user views the shared image in a new browser tab, the embedded JavaScript executes. The issue affects both authenticated and unauthenticated users.	Patched by core rule	Y
CVE-2025-58640	CVE-2025-58640 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MatrixAddons Document Engine allows Stored XSS. This issue affects Document Engine: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-58633	CVE-2025-58633 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Deetronix Booking Ultra Pro allows Stored XSS. This issue affects Booking Ultra Pro: from n/a through 1.1.21.	Patched by core rule	Y
CVE-2025-58632	CVE-2025-58632 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dadevarzan Dadevarzan WordPress Common allows Stored XSS. This issue affects Dadevarzan WordPress Common: from n/a through 2.2.2.	Patched by core rule	Y
CVE-2025-58631	CVE-2025-58631 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ZEEN101 IssueM allows DOM-Based XSS. This issue affects IssueM: from n/a through 2.9.0.	Patched by core rule	Y
CVE-2025-58630	CVE-2025-58630 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rbaer Simple Matomo Tracking Code allows Stored XSS. This issue affects Simple Matomo Tracking Code: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-58626	CVE-2025-58626 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RumbleTalk RumbleTalk Live Group Chat allows Stored	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		XSS. This issue affects RumbleTalk Live Group Chat: from n/a through 6.3.5.		
CVE-2025-58625	CVE-2025-58625 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Spiffy Plugins WP Flow Plus allows Stored XSS. This issue affects WP Flow Plus: from n/a through 5.2.5.	Patched by core rule	Y
CVE-2025-58624	CVE-2025-58624 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in falselight Exchange Rates allows Stored XSS. This issue affects Exchange Rates: from n/a through 1.2.5.	Patched by core rule	Y
CVE-2025-58623	CVE-2025-58623 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bohemia Plugins Event Feed for Eventbrite allows DOM-Based XSS. This issue affects Event Feed for Eventbrite: from n/a through 1.3.2.	Patched by core rule	Y
CVE-2025-58621	CVE-2025-58621 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Amuse Labs PuzzleMe for WordPress allows Stored XSS. This issue affects PuzzleMe for WordPress: from n/a through 1.2.0.	Patched by core rule	Y
CVE-2025-58620	CVE-2025-58620 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in add-ons.org PDF for WPForms allows Stored XSS. This issue affects PDF for WPForms: from n/a through 6.2.1.	Patched by core rule	Y
CVE-2025-58618	CVE-2025-58618 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jonathan Jernigan Pie Calendar allows DOM-Based XSS. This issue affects Pie Calendar: from n/a through 1.2.8.	Patched by core rule	Y
CVE-2025-58614	CVE-2025-58614 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jamel.Z Tooltipy allows Stored XSS. This issue affects Tooltipy: from n/a through 5.5.6.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-58612	CVE-2025-58612 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Property Hive PropertyHive allows Stored XSS. This issue affects PropertyHive: from n/a through 2.1.5.	Patched by core rule	Y
CVE-2025-58610	CVE-2025-58610 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Chill Gallery PhotoBlocks allows Stored XSS. This issue affects Gallery PhotoBlocks: from n/a through 1.3.1.	Patched by core rule	Y
CVE-2025-58609	CVE-2025-58609 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Iulia Cazan Latest Post Shortcode allows Stored XSS. This issue affects Latest Post Shortcode: from n/a through 14.0.3.	Patched by core rule	Y
CVE-2025-58607	CVE-2025-58607 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GDPR Info Cookie Notice & Consent Banner for GDPR & CCPA Compliance allows Stored XSS. This issue affects Cookie Notice & Consent Banner for GDPR & CCPA Compliance: from n/a through 1.7.11.	Patched by core rule	Y
CVE-2025-58605	CVE-2025-58605 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Delicious WP Delicious allows Stored XSS. This issue affects WP Delicious: from n/a through 1.8.7.	Patched by core rule	Y
CVE-2025-58602	CVE-2025-58602 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in IfSo Dynamic Content If-So Dynamic Content Personalization allows Stored XSS. This issue affects If-So Dynamic Content Personalization: from n/a through 1.9.4.	Patched by core rule	Y
CVE-2025-58596	CVE-2025-58596 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in properfraction MailOptin allows Stored XSS. This issue affects MailOptin: from n/a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		through 1.2.75.0.		
CVE-2025-58593	CVE-2025-58593 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeisle Orbit Fox by ThemeIsle allows Stored XSS. This issue affects Orbit Fox by ThemeIsle: from n/a through 3.0.0.	Patched by core rule	Y
CVE-2025-9378	CVE-2025-9378 - The Vayu Blocks – Website Builder for the Block Editor plugin for WordPress is vulnerable to Stored ...	The Vayu Blocks – Website Builder for the Block Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple attributes in the Lottie block in all versions up to, and including, 1.3.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-9834	CVE-2025-9834 - A flaw has been found in PHPGurukul Small CRM 4.0. Affected by this issue is some unknown functional...	A flaw has been found in PHPGurukul Small CRM 4.0. Affected by this issue is some unknown functionality of the file /registration.php. Executing manipulation of the argument Username can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2025-9755	CVE-2025-9755 - A vulnerability has been found in Khanakag-17 Library Management System up to 60ed174506094dcd166e34...	A vulnerability has been found in Khanakag-17 Library Management System up to 60ed174506094dcd166e34904a54288e5d10ff24. This affects an unknown function of the file /index.php. The manipulation of the argument msg leads to cross site scripting. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided.	Patched by core rule	Y
CVE-2025-9754	CVE-2025-9754 - A flaw has been found in Campcodes Online	A flaw has been found in Campcodes Online Hospital Management System 1.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Hospital Management System 1.0. The impacted element is an...	The impacted element is an unknown function of the file /edit-profile.php of the component Edit Profile Page. Executing manipulation of the argument Username can lead to cross site scripting. The attack may be launched remotely. The exploit has been published and may be used.		
CVE-2025-9753	CVE-2025-9753 - A vulnerability was detected in Campcodes Online Hospital Management System 1.0. The affected elemen...	A vulnerability was detected in Campcodes Online Hospital Management System 1.0. The affected element is an unknown function of the file /admin/patient-search.php of the component Patient Search Module. Performing manipulation of the argument Search by Name Mobile No results in cross site scripting. The attack may be initiated remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-9724	CVE-2025-9724 - A vulnerability was determined in Portabilis i-Educar up to 2.10. This impacts an unknown function o...	A vulnerability was determined in Portabilis i-Educar up to 2.10. This impacts an unknown function of the file /intranet/educar_nivel_ensino_cad.php. Executing manipulation of the argument nm_nivel/descricao can lead to cross site scripting. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-9723	CVE-2025-9723 - A vulnerability was found in Portabilis i-Educar up to 2.10. This affects an unknown function of the...	A vulnerability was found in Portabilis i-Educar up to 2.10. This affects an unknown function of the file /intranet/educar_tipo_regime_cad.php. Performing manipulation of the argument nm_tipo results in cross site scripting. The attack can be initiated remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2025-9722	CVE-2025-9722 - A vulnerability has been found in Portabilis i-Educar up to 2.10. The impacted element is an unknown...	A vulnerability has been found in Portabilis i-Educar up to 2.10. The impacted element is an unknown function of the file /intranet/educar_tipo_ocorrencia_disciplinar_cad.php. Such manipulation of the argument nm_tipo/descricao leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-9721	CVE-2025-9721 - A flaw has been found in Portabilis i-Educar up to 2.10. The affected element is an unknown function...	A flaw has been found in Portabilis i-Educar up to 2.10. The affected element is an unknown function of the file /module/FormulaMedia/edit. This manipulation of the argument nome/formulaMedia causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2025-9720	CVE-2025-9720 - A vulnerability was detected in Portabilis i-Educar up to 2.10. Impacted is an unknown function of t...	A vulnerability was detected in Portabilis i-Educar up to 2.10. Impacted is an unknown function of the file /module/TabelaArredondamento/edit of the component Cadastrar tabela de arredondamento Page. The manipulation of the argument Nome results in cross site scripting. The attack may be performed from a remote location. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-5083	CVE-2025-5083 - The Amministrazione Trasparente plugin for WordPress is vulnerable to Stored Cross-Site Scripting vi...	The Amministrazione Trasparente plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 9.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	Patched by core rule	Y
CVE-2025-9500	CVE-2025-9500 - The TablePress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'shortcode_...	The TablePress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'shortcode_debug' parameter in all versions up to, and including, 3.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-9499	CVE-2025-9499 - The Ocean Extra plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's o...	The Ocean Extra plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's oceanwp_library shortcode in all versions up to, and including, 2.4.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2023-41471	CVE-2023-41471 - Cross Site Scripting vulnerability in copyparty v.1.9.1 allows a local attacker to execute arbitrary...	Cross Site Scripting vulnerability in copyparty v.1.9.1 allows a local attacker to execute arbitrary code via a crafted payload to the WEEKEND-PLANS function.	Patched by core rule	Y
CVE-2025-55580	CVE-2025-55580 - SolidInvoice 2.3.7 and v.2.3.8 is vulnerable to Cross Site Scripting (XSS) in the client's functiona...	SolidInvoice 2.3.7 and v.2.3.8 is vulnerable to Cross Site Scripting (XSS) in the client's functionality.	Patched by core rule	Y
CVE-2025-55579	CVE-2025-55579 - SolidInvoice 2.3.7 and fixed in v.2.3.8 is vulnerable to Cross Site Scripting (XSS) in the Tax Rate ...	SolidInvoice 2.3.7 and fixed in v.2.3.8 is vulnerable to Cross Site Scripting (XSS) in the Tax Rate functionality.	Patched by core rule	Y
CVE-2025-8150	CVE-2025-8150 - The Events Addon for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via...	The Events Addon for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Typewriter and Countdown widgets in all versions up to, and including, 2.2.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-8619	CVE-2025-8619 - The OSM Map Widget for Elementor plugin for WordPress is vulnerable to Stored Cross-Site	The OSM Map Widget for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Map Block	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Scripting v...	URL in all versions up to, and including, 1.3.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-9590	CVE-2025-9590 - A vulnerability was identified in Weaver E-Mobile Mobile Management Platform up to 20250813. Affecte...	A vulnerability was identified in Weaver E-Mobile Mobile Management Platform up to 20250813. Affected by this vulnerability is an unknown functionality. The manipulation of the argument gohome leads to cross site scripting. The attack can be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-56236	CVE-2025-56236 - FormCms v0.5.5 contains a stored cross-site scripting (XSS) vulnerability in the avatar upload featu...	FormCms v0.5.5 contains a stored cross-site scripting (XSS) vulnerability in the avatar upload feature. Authenticated users can upload .html files containing malicious JavaScript, which are accessible via a public URL. When a privileged user accesses the file, the script executes in their browser context.	Patched by core rule	Y
CVE-2025-51967	CVE-2025-51967 - A Reflected Cross-site Scripting (XSS) vulnerability exists in the themeSet.php file of ProjectsAndP...	A Reflected Cross-site Scripting (XSS) vulnerability exists in the themeSet.php file of ProjectsAndPrograms School Management System 1.0. The application fails to sanitize user-supplied input in the theme POST parameter, allowing an attacker to inject and execute arbitrary JavaScript in a victim's browser.	Patched by core rule	Y
CVE-2025-54724	CVE-2025-54724 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in uxper Golo allows Reflected XSS. This issue affects Golo: from n/a through 1.7.1.	Patched by core rule	Y
CVE-2025-53579	CVE-2025-53579 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in captcha.eu Captcha.eu allows Reflected XSS. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		issue affects Captcha.eu: from n/a through n/a.		
CVE-2025-53289	CVE-2025-53289 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jason Theme Blvd Widget Areas allows Reflected XSS. This issue affects Theme Blvd Widget Areas: from n/a through 1.3.0.	Patched by core rule	Y
CVE-2025-53225	CVE-2025-53225 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eboekhouden e-Boekhouden.nl allows Reflected XSS. This issue affects e-Boekhouden.nl: from n/a through 1.9.3.	Patched by core rule	Y
CVE-2025-53224	CVE-2025-53224 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Koen Schuit NextGEN Gallery Search allows Reflected XSS. This issue affects NextGEN Gallery Search: from n/a through 2.12.	Patched by core rule	Y
CVE-2025-53223	CVE-2025-53223 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in undoIT Theme Switcher Reloaded allows Reflected XSS. This issue affects Theme Switcher Reloaded: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-53220	CVE-2025-53220 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in XmasB XmasB Quotes allows Reflected XSS. This issue affects XmasB Quotes: from n/a through 1.6.1.	Patched by core rule	Y
CVE-2025-53215	CVE-2025-53215 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 8bitkid Yahoo! WebPlayer allows Reflected XSS. This issue affects Yahoo! WebPlayer: from n/a through 2.0.6.	Patched by core rule	Y
CVE-2025-49407	CVE-2025-49407 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in favethemes Houzez allows Reflected XSS. This issue affects Houzez: from n/a through 4.1.1.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-48365	CVE-2025-48365 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in imaprogrammer Custom Comment allows Stored XSS. This issue affects Custom Comment: from n/a through 2.1.6.	Patched by core rule	Y
CVE-2025-48360	CVE-2025-48360 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Razvan Stanga Varnish/Nginx Proxy Caching allows Stored XSS. This issue affects Varnish/Nginx Proxy Caching: from n/a through 1.8.3.	Patched by core rule	Y
CVE-2025-48358	CVE-2025-48358 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in everythingwp Risk Free Cash On Delivery (COD) – WooCommerce allows Stored XSS. This issue affects Risk Free Cash On Delivery (COD) – WooCommerce: from n/a through 1.0.4.	Patched by core rule	Y
CVE-2025-48356	CVE-2025-48356 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Isra Kanpress allows Stored XSS. This issue affects Kanpress: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-48354	CVE-2025-48354 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Smart Widgets Better Post & Filter Widgets for Elementor allows Stored XSS. This issue affects Better Post & Filter Widgets for Elementor: from n/a through 1.6.0.	Patched by core rule	Y
CVE-2025-48352	CVE-2025-48352 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sitesearch-yandex Yandex Site search pinger allows Stored XSS. This issue affects Yandex Site search pinger: from n/a through 1.5.	Patched by core rule	Y
CVE-2025-48349	CVE-2025-48349 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in origincode Video Gallery –	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	i...	Vimeo and YouTube Gallery allows Stored XSS. This issue affects Video Gallery – Vimeo and YouTube Gallery: from n/a through 1.1.7.		
CVE-2025-48347	CVE-2025-48347 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vincent Mimoun-Prat bxSlider integration for WordPress allows Stored XSS. This issue affects bxSlider integration for WordPress: from n/a through 1.7.2.	Patched by core rule	Y
CVE-2025-48324	CVE-2025-48324 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in khashabawy tli.tl auto Twitter poster allows Stored XSS. This issue affects tli.tl auto Twitter poster: from n/a through 3.4.	Patched by core rule	Y
CVE-2025-48323	CVE-2025-48323 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Md Abunaser Khan Advance Food Menu allows Stored XSS. This issue affects Advance Food Menu: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-48322	CVE-2025-48322 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Finn Dohrn Statify Widget allows Stored XSS. This issue affects Statify Widget: from n/a through 1.4.6.	Patched by core rule	Y
CVE-2025-48319	CVE-2025-48319 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gslauraspeck Mesa Mesa Reservation Widget allows Stored XSS. This issue affects Mesa Mesa Reservation Widget: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-48316	CVE-2025-48316 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ItayXD Responsive Mobile-Friendly Tooltip allows Stored XSS. This issue affects Responsive Mobile-Friendly Tooltip: from n/a through 1.6.6.	Patched by core rule	Y
CVE-2025-48315	CVE-2025-48315 - Improper Neutralization	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Generation ('Cross-site Scripting') vulnerability in stanton119 WordPress HTML allows Stored XSS. This issue affects WordPress HTML: from n/a through 0.51.		
CVE-2025-48314	CVE-2025-48314 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in salubrio Add Code To Head allows Stored XSS. This issue affects Add Code To Head: from n/a through 1.17.	Patched by core rule	Y
CVE-2025-48313	CVE-2025-48313 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kevin heath Tripadvisor Shortcode allows Stored XSS. This issue affects Tripadvisor Shortcode: from n/a through 2.2.	Patched by core rule	Y
CVE-2025-48312	CVE-2025-48312 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 文派翻译（WP Chinese Translation） WPAvatar allows Stored XSS. This issue affects WPAvatar: from n/a through 1.9.3.	Patched by core rule	Y
CVE-2025-48305	CVE-2025-48305 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in vikingjs Goal Tracker for Patreon allows Stored XSS. This issue affects Goal Tracker for Patreon: from n/a through 0.4.6.	Patched by core rule	Y
CVE-2025-48110	CVE-2025-48110 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mibuthu Link View allows Stored XSS. This issue affects Link View: from n/a through 0.8.0.	Patched by core rule	Y
CVE-2025-8073	CVE-2025-8073 - The Dynamic AJAX Product Filters for WooCommerce plugin for WordPress is vulnerable to Stored Cross-...	The Dynamic AJAX Product Filters for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'name' parameter in all versions up to, and including, 1.3.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-6255	CVE-2025-6255 - The Dynamic AJAX Product Filters for WooCommerce plugin for WordPress is vulnerable to Stored Cross-...	The Dynamic AJAX Product Filters for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'className' parameter in all versions up to, and including, 1.3.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-9346	CVE-2025-9346 - The Booking Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via settings ...	The Booking Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via settings in all versions up to, and including, 10.14.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-8603	CVE-2025-8603 - The Unlimited Elements For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripti...	The Unlimited Elements For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several widgets in all versions up to, and including, 1.5.148 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-9352	CVE-2025-9352 - The Pronamic Google Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the d...	The Pronamic Google Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the description field in all versions up to, and including, 2.4.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-9344	CVE-2025-9344 - The UsersWP – Front-end login form, User Registration, User Profile & Members Directory plugin for W...	The UsersWP – Front-end login form, User Registration, User Profile & Members Directory plugin for WP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'uwp_profile' and 'uwp_profile_header' shortcodes in all versions up to, and including, 1.2.42 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-8897	CVE-2025-8897 - The Beaver Builder – WordPress Page Builder plugin for WordPress is vulnerable to Reflected Cross-Si...	The Beaver Builder – WordPress Page Builder plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ''fl_builder' parameter in all versions up to, and including, 2.9.2.1 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-2025-55618	CVE-2025-55618 - In Hyundai Navigation App STD5W.EUR.HMC.230516.afa908d, an attacker can inject HTML payloads in the ...	In Hyundai Navigation App STD5W.EUR.HMC.230516.afa908d, an attacker can inject HTML payloads in the profile name field in navigation app which then get rendered.	Patched by core rule	Y
CVE-2025-58216	CVE-2025-58216 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jgwhite33 WP Thumbtack Review Slider allows Stored XSS. This issue affects WP Thumbtack Review Slider: from n/a through 2.6.	Patched by core rule	Y
CVE-2025-58213	CVE-2025-58213 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ameliabooking Booking	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	i...	System Trafft allows Stored XSS. This issue affects Booking System Trafft: from n/a through 1.0.14.		
CVE-2025-58212	CVE-2025-58212 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in epeken Epeken All Kurir allows DOM-Based XSS. This issue affects Epeken All Kurir: from n/a through 2.0.1.	Patched by core rule	Y
CVE-2025-58211	CVE-2025-58211 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in alexvtn Chatbox Manager allows Stored XSS. This issue affects Chatbox Manager: from n/a through 1.2.6.	Patched by core rule	Y
CVE-2025-58209	CVE-2025-58209 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rtCamp Transcoder allows Stored XSS. This issue affects Transcoder: from n/a through 1.4.0.	Patched by core rule	Y
CVE-2025-58208	CVE-2025-58208 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in add-ons.org PDF for Elementor Forms + Drag And Drop Template Builder allows Stored XSS. This issue affects PDF for Elementor Forms + Drag And Drop Template Builder: from n/a through 6.2.0.	Patched by core rule	Y
CVE-2025-58205	CVE-2025-58205 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Element Invader ElementInvader Addons for Elementor allows DOM-Based XSS. This issue affects ElementInvader Addons for Elementor: from n/a through 1.3.6.	Patched by core rule	Y
CVE-2025-58197	CVE-2025-58197 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mra13 / Team Tips and Tricks HQ Simple Download Monitor allows Stored XSS. This issue affects Simple Download Monitor: from n/a through 3.9.34.	Patched by core rule	Y
CVE-2025-58196	CVE-2025-58196 - Improper Neutralization	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Generation ('Cross-site Scripting') vulnerability in uicore UiCore Elements allows Stored XSS. This issue affects UiCore Elements: from n/a through 1.3.4.		
CVE-2025-58195	CVE-2025-58195 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Xpro Xpro Elementor Addons allows Stored XSS. This issue affects Xpro Elementor Addons: from n/a through 1.4.17.	Patched by core rule	Y
CVE-2025-58194	CVE-2025-58194 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	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 5.4.3.	Patched by core rule	Y
CVE-2025-50977	CVE-2025-50977 - A template injection vulnerability leading to reflected cross-site scripting (XSS) has been identifi...	A template injection vulnerability leading to reflected cross-site scripting (XSS) has been identified in version 1.7.1, requiring authenticated admin access for exploitation. The vulnerability exists in the 'r' parameter and allows attackers to inject malicious Angular expressions that execute JavaScript code in the context of the application. The flaw can be exploited through GET requests to the summary endpoint as well as POST requests to specific Wicket interface endpoints, though the GET method provides easier weaponization. This vulnerability enables authenticated administrators to execute arbitrary client-side code, potentially leading to session hijacking, data theft, or further privilege escalation attacks.	Patched by core rule	Y
CVE-2025-50978	CVE-2025-50978 - In Gitblit v1.7.1, a reflected cross-site scripting (XSS) vulnerability exists in the way repository...	In Gitblit v1.7.1, a reflected cross-site scripting (XSS) vulnerability exists in the way repository path names are handled. By injecting a specially crafted path payload an attacker can cause arbitrary JavaScript to execute when a victim views the manipulated URL. This flaw stems from insufficient input sanitization of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		filename elements.		
CVE-2025-50986	CVE-2025-50986 - diskover-web v2.3.0 Community Edition suffers from multiple stored cross-site scripting (XSS) vulner...	diskover-web v2.3.0 Community Edition suffers from multiple stored cross-site scripting (XSS) vulnerabilities in its administrative settings interface. Various configuration fields such as ES_HOST, ES_INDEXREFRESH, ES_PORT, ES_SCROLLSIZE, ES_TRANSLOGSIZE, ES_TRANSLOGSYNCINT, EXCLUDES_FILES, FILE_TYPES[], INCLUDES_DIRS, INCLUDES_FILES, and TIMEZONE do not properly sanitize user-supplied input. Malicious payloads submitted via these parameters are persisted in the application and executed whenever an administrator views or edits the settings page.	Patched by core rule	Y
CVE-2025-50985	CVE-2025-50985 - diskover-web v2.3.0 Community Edition is vulnerable to multiple reflected cross-site scripting (XSS)...	diskover-web v2.3.0 Community Edition is vulnerable to multiple reflected cross-site scripting (XSS) flaws in its web interface. Unsanitized GET parameters including maxage, maxindex, index, path, q (query), and doctype are directly echoed into the HTML response, allowing attackers to inject and execute arbitrary JavaScript when a victim visits a maliciously crafted URL.	Patched by core rule	Y
CVE-2025-49039	CVE-2025-49039 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mibuthu Link View allows Stored XSS.This issue affects Link View: from n/a through 0.8.0.	Patched by core rule	Y
CVE-2025-49035	CVE-2025-49035 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in chaimchaikin Admin Menu Groups allows Stored XSS.This issue affects Admin Menu Groups: from n/a through 0.1.2.	Patched by core rule	Y
CVE-2025-7732	CVE-2025-7732 - The Lazy Load for Videos plugin for WordPress is vulnerable to Stored Cross-Site Scripting via its l...	The Lazy Load for Videos plugin for WordPress is vulnerable to Stored Cross-Site Scripting via its lazy-loading handlers in all	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		versions up to, and including, 2.18.7 due to insufficient input sanitization and output escaping. The plugin's JavaScript registration handlers read the client-supplied 'data-video-title' and 'href' attributes, decode HTML entities by default, and pass them directly into DOM sinks without any escaping or validation. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-8490	CVE-2025-8490 - The All-in-One WP Migration and Backup plugin for WordPress is vulnerable to Stored Cross-Site Scrip...	The All-in-One WP Migration and Backup plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Import in all versions up to, and including, 7.97 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	Patched by core rule	Y
CVE-2025-9277	CVE-2025-9277 - The SiteSEO – SEO Simplified plugin for WordPress is vulnerable to Stored Cross-Site Scripting via t...	The SiteSEO – SEO Simplified plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the broken preg_replace expression in all versions up to, and including, 1.2.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-50975	CVE-2025-50975 - IPFire 2.29 web-based firewall interface (firewall.cgi) fails to sanitize several rule parameters su...	IPFire 2.29 web-based firewall interface (firewall.cgi) fails to sanitize several rule parameters such as PROT, SRC_PORT, TGT_PORT, dnatport, key, ruleremark, src_addr, std_net_tgt, and tgt_addr, allowing an authenticated	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		administrator to inject persistent JavaScript. This stored XSS payload is executed whenever another admin views the firewall rules page, enabling session hijacking, unauthorized actions within the interface, or further internal pivoting. Exploitation requires only high-privilege GUI access, and the complexity of the attack is low.		
CVE-2025-50976	CVE-2025-50976 - IPFire 2.29 DNS management interface (dns.cgi) fails to properly sanitize user-supplied input in the...	IPFire 2.29 DNS management interface (dns.cgi) fails to properly sanitize user-supplied input in the NAMESERVER, REMARK, and TLS_HOSTNAME query parameters, resulting in a reflected cross-site scripting (XSS) vulnerability.	Patched by core rule	Y
CVE-2025-57425	CVE-2025-57425 - A Stored Cross-Site Scripting (XSS) vulnerability in SourceCodester FAQ Management System 1.0 allows...	A Stored Cross-Site Scripting (XSS) vulnerability in SourceCodester FAQ Management System 1.0 allows an authenticated attacker to inject malicious JavaScript into the 'question' and 'answer' fields via the update-faq.php endpoint.	Patched by core rule	Y
CVE-2025-52184	CVE-2025-52184 - Cross Site Scripting vulnerability in Helpy.io v.2.8.0 allows a remote attacker to escalate privileg...	Cross Site Scripting vulnerability in Helpy.io v.2.8.0 allows a remote attacker to escalate privileges via the New Topic Ticket funtion.	Patched by core rule	Y
CVE-2025-52037	CVE-2025-52037 - A vulnerability has been found in NotesCMS and classified as medium. Affected by this vulnerability ...	A vulnerability has been found in NotesCMS and classified as medium. Affected by this vulnerability is the page /index.php?route=sites. The manipulation of the title of the service descriptions leads to a stored XSS vulnerability. The issue was confirmed to be present in the source code as of commit 7d821a0f028b0778b245b99ab3d3bff1ac10e2d3 (dated 2024-05-08), and was fixed in commit 95322c5121dbd7070f3bd54f2848079654a0a8ea (dated 2025-03-31). The attack can be launched remotely. CWE Definition of the Vulnerability: CWE-79.	Patched by core rule	Y
CVE-2025-52036	CVE-2025-52036 - A vulnerability has been found in NotesCMS and classified as medium.	A vulnerability has been found in NotesCMS and classified as medium. Affected by this vulnerability	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Affected by this vulnerability ...	is the page /index.php?route=categories . The manipulation of the title of the service descriptions leads to a stored XSS vulnerability. The issue was confirmed to be present in the source code as of commit 7d821a0f028b0778b245b99ab3d3bff1ac10e2d3 (dated 2024-05-08), and was fixed in commit 95322c5121dbd7070f3bd54f2848079654a0a8ea (dated 2025-03-31). The attack can be launched remotely. CWE Definition of the Vulnerability: CWE-79.		
CVE-2025-52035	CVE-2025-52035 - A vulnerability in NotesCMS and specifically in the page /index.php?route=notes. The manipulation of...	A vulnerability in NotesCMS and specifically in the page /index.php?route=notes. The manipulation of the title of the service descriptions leads to a stored XSS vulnerability. The issue was confirmed to be present in the source code as of commit 7d821a0f028b0778b245b99ab3d3bff1ac10e2d3 (dated 2024-05-08) and was fixed in commit 95322c5121dbd7070f3bd54f2848079654a0a8ea (dated 2025-03-31). The attack can be launched remotely.	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™