INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

October 2025

The total zero-day vulnerabilities count for October month: 404

Command Injection	SQL Injection	SSRF	Path Traversal	Remote Code Execution	Cross-Site Scripting
9	106	15	75	1	198

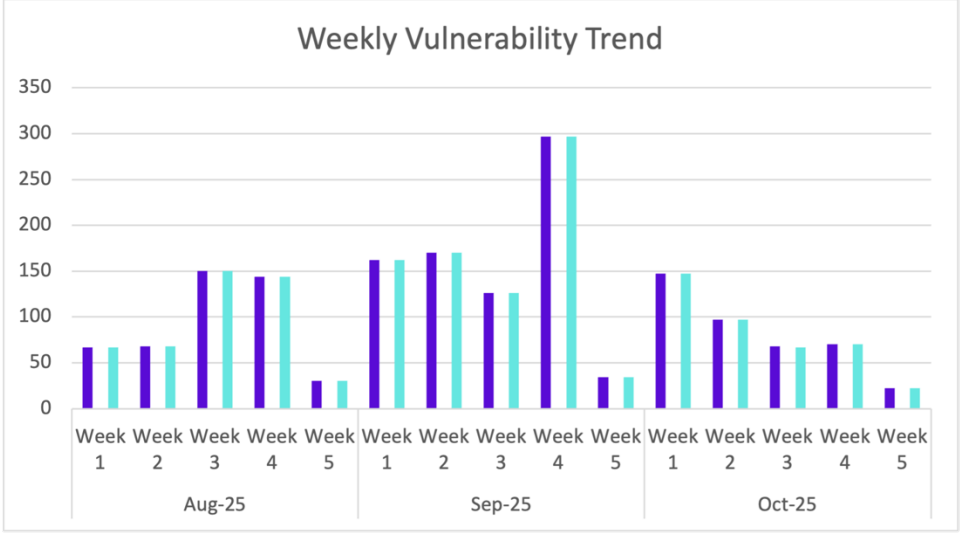
Zero-day vulnerabilities protected through core rules	404
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities found by Indusface WAS	403

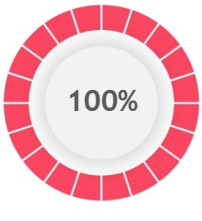
- To enable custom rules, please contact support@indusface.com
- Learn more about zero-day vulnerabilities, detection, and prevention, here

Vulnerability Trend:

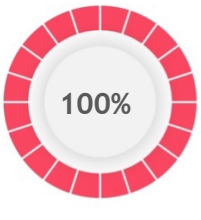
The weekly trend displays the total number of vulnerabilities discovered and the type of protection provided for the last quarter.

Weekly Vulnerability Trend



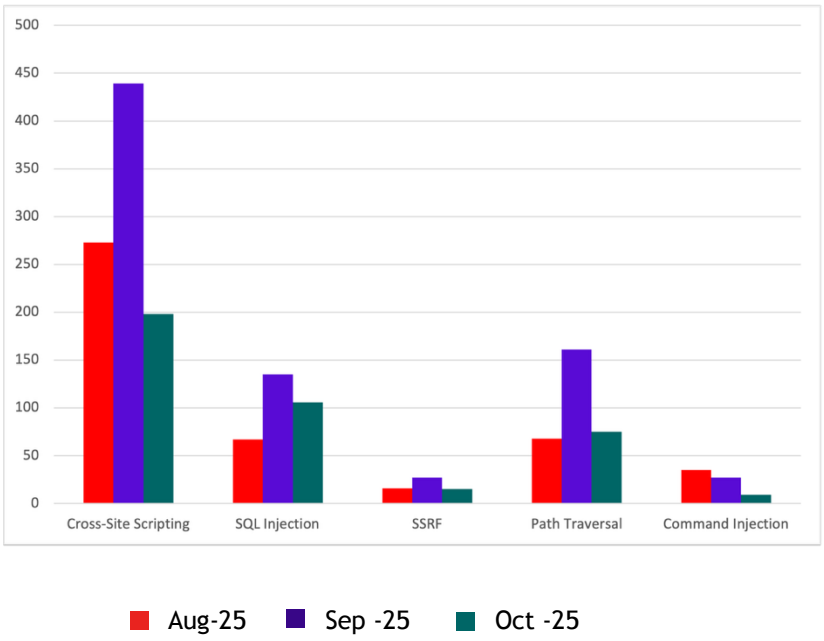


of the zero-day vulnerabilities were protected by the core rules in the last month



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

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-56799	CVE-2025-56799 - Reolink desktop application 8.18.12 contains a command injection vulnerability in its scheduled cach...	Reolink desktop application 8.18.12 contains a command injection vulnerability in its scheduled cache-clearing mechanism via a crafted folder name. NOTE: this is disputed by the Supplier because a crafted folder name would arise only if the local user were attacking himself.	Patched by core rule	Y
CVE-2025-57521	CVE-2025-57521 - Bambu Studio 2.1.1.52 and earlier is affected by a vulnerability that allows arbitrary code executio...	Bambu Studio 2.1.1.52 and earlier is affected by a vulnerability that allows arbitrary code execution during application startup. The application loads a network plugin without validating its digital signature or verifying its authenticity. A local attacker can exploit this behavior by placing a malicious component in the expected location, which is controllable by the attacker (e.g., under %APPDATA%), resulting in code execution within the context of the user. The main application is digitally signed, which may allow a malicious component to inherit trust and evade detection by security solutions that rely on signed parent processes.	Patched by core rule	Y
CVE-2025-56223	CVE-2025-56223 - A lack of rate limiting in the component /Home/UploadStreamDocument of SigningHub v8.6.8 allows atta...	A lack of rate limiting in the component /Home/UploadStreamDocument of SigningHub v8.6.8 allows attackers to cause a Denial of Service (DoS) via uploading an excessive number of files.	Patched by core rule	Y
CVE-2025-61514	CVE-2025-61514 - An	An arbitrary file upload	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	arbitrary file upload vulnerability in SageMath, Inc CoCalc before commit 0d2ff58 allows attacker...	vulnerability in SageMath, Inc CoCalc before commit 0d2ff58 allows attackers to execute arbitrary code via uploading a crafted SVG file.	rule	
CVE-2025-11665	CVE-2025-11665 - A vulnerability was detected in D-Link DAP-2695 2.00RC131. This affects the function fwupdater_main ...	A vulnerability was detected in D-Link DAP-2695 2.00RC131. This affects the function fwupdater_main of the file rgbin of the component Firmware Update Handler. Performing manipulation results in os command injection. The attack may be initiated remotely. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-60838	CVE-2025-60838 - An arbitrary file upload vulnerability in MCMS v6.0.1 allows attackers to execute arbitrary code via...	An arbitrary file upload vulnerability in MCMS v6.0.1 allows attackers to execute arbitrary code via uploading a crafted file.	Patched by core rule	Y
CVE-2025-61045	CVE-2025-61045 - TOTOLINK X18 V9.1.0cu.2053_B20230309 was discovered to contain a command injection vulnerability via...	TOTOLINK X18 V9.1.0cu.2053_B20230309 was discovered to contain a command injection vulnerability via the mac parameter in the setEasyMeshAgentCfg function.	Patched by core rule	Y
CVE-2025-61044	CVE-2025-61044 - TOTOLINK X18 V9.1.0cu.2053_B20230309 was discovered to contain a command injection vulnerability via...	TOTOLINK X18 V9.1.0cu.2053_B20230309 was discovered to contain a command injection vulnerability via the agentName parameter in the setEasyMeshAgentCfg function.	Patched by core rule	Y
CVE-2025-55848	CVE-2025-55848 - An issue was discovered in DIR-823 firmware 20250416. There is an RCE vulnerability in the set_cassw...	An issue was discovered in DIR-823 firmware 20250416. There is an RCE vulnerability in the set_cassword settings interface, as the http_casswd parameter is not filtered by '&'to allow injection of reverse connection commands.	Patched by core rule	Y

Remote Code Execution Vulnerability

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-59287	CVE-2025-59287 - Deserialization of untrusted data in Windows Server Update Service allows an unauthorized attacker t...	Deserialization of untrusted data in Windows Server Update Service allows an unauthorized attacker to execute code over a network.	Patched by core rule	NA

Path Traversal Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-11976	CVE-2025-11976 - The FuseWP – WordPress User Sync to Email List & Marketing Automation (Mailchimp, Constant Contact, ...	The FuseWP – WordPress User Sync to Email List & Marketing Automation (Mailchimp, Constant Contact, ActiveCampaign etc.) plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.23.0. This is due to missing or incorrect nonce validation on the save_changes function. This makes it possible for unauthenticated attackers to add or edit sync rules 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-2025-10488	CVE-2025-10488 - The Directorist: AI-Powered Business Directory Plugin with Classified Ads Listings plugin for WordPr...	The Directorist: AI-Powered Business Directory Plugin with Classified Ads Listings plugin for WordPress is vulnerable to arbitrary file move due to insufficient file path validation in the add_listing_action AJAX action in all versions up to, and including, 8.4.8. This makes it possible for unauthenticated attackers to move arbitrary files on the server, which can easily lead to remote code execution when the right file is moved (such as wp-config.php).	Patched by core rule	Y
CVE-2025-12095	CVE-2025-12095 - The Simple Registration for WooCommerce plugin for WordPress is vulnerable to Cross-Site Request For...	The Simple Registration for WooCommerce plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.5.8. This is due to missing nonce validation on the role requests admin page handler in the includes/display-role-admin.php file. This makes it possible for unauthenticated attackers to approve pending role requests and escalate user privileges via a forged request granted they can trick a site administrator into performing an action	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		such as clicking on a link.		
CVE-2025-12072	CVE-2025-12072 - The Disable Content Editor For Specific Template plugin for WordPress is vulnerable to Cross-Site Re...	The Disable Content Editor For Specific Template plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0. This is due to missing nonce validation on template configuration updates. This makes it possible for unauthenticated attackers to add or delete template configurations via a forged request granted they can trick an administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-12028	CVE-2025-12028 - The IndieAuth plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to...	The IndieAuth plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.5.4. This is due to missing nonce verification on the `login_form_indieauth()` function and the authorization endpoint at wp-login.php?action=indieauth. This makes it possible for unauthenticated attackers to force authenticated users to approve OAuth authorization requests for attacker-controlled applications via a forged request granted they can trick a user into performing an action such as clicking on a link or visiting a malicious page while logged in. The attacker can then exchange the stolen authorization code for an access token, effectively taking over the victim's account with the granted scopes (create, update, delete).	Patched by core rule	Y
CVE-2025-62254	CVE-2025-62254 - The ComboServlet in Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Life...	The ComboServlet in Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.2, 2023.Q3.1 through 2023.Q3.5, 7.4 GA through update 92, 7.3 GA through update 35, and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		older unsupported versions does not limit the number or size of the files it will combine, which allows remote attackers to create very large responses that lead to a denial of service attack via the URL query string.		
CVE-2025-10588	CVE-2025-10588 - The PixelYourSite – Your smart PIXEL (TAG) & API Manager plugin for WordPress is vulnerable to Cross...	The PixelYourSite – Your smart PIXEL (TAG) & API Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 11.1.2. This is due to missing or incorrect nonce validation on the adminEnableGdprAjax() function. This makes it possible for unauthenticated attackers to modify GDPR 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-2025-11939	CVE-2025-11939 - A vulnerability was determined in ChurchCRM up to 5.18.0. This issue affects some unknown processing...	A vulnerability was determined in ChurchCRM up to 5.18.0. This issue affects some unknown processing of the file src/ChurchCRM/Backup/RestoreJob.php of the component Backup Restore Handler. Executing manipulation of the argument restoreFile can lead to path traversal. 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
CVE-2025-9890	CVE-2025-9890 - The Theme Editor plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up...	The Theme Editor plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.0. This is due to missing or incorrect nonce validation on the 'theme_editor_theme' page. This makes it possible for unauthenticated attackers to achieve remote code execution 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-2025-11914	CVE-2025-11914 - A vulnerability was found in Shenzhen Ruiming Technology Streamax Crocus 1.3.40. Affected by this is...	A vulnerability was found in Shenzhen Ruiming Technology Streamax Crocus 1.3.40. Affected by this issue is the function Download of the file /DeviceFileReport.do?Action=Download. Performing manipulation of the argument FilePath results in path traversal. The attack may be initiated remotely. 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-2025-11913	CVE-2025-11913 - A vulnerability has been found in Shenzhen Ruiming Technology Streamax Crocus 1.3.40. Affected by th...	A vulnerability has been found in Shenzhen Ruiming Technology Streamax Crocus 1.3.40. Affected by this vulnerability is the function Download of the file /Service.do?Action=Download. Such manipulation of the argument Path leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-11849	CVE-2025-11849 - Versions of the package mammoth from 0.3.25 and before 1.11.0; versions of the package mammoth from ...	Versions of the package mammoth from 0.3.25 and before 1.11.0; versions of the package mammoth from 0.3.25 and before 1.11.0; versions of the package mammoth before 1.11.0; versions of the package org.zwobble.mammoth:mammoth before 1.11.0 are vulnerable to Directory Traversal due to the lack of path or file type validation when processing a docx file containing an image with an external link (r:link attribute instead of embedded r:embed). The library resolves the URI to a file path and after reading, the content is encoded as base64 and included in the HTML output as a data URI. An attacker can read arbitrary files on the system where the conversion is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		performed or cause an excessive resources consumption by crafting a docx file that links to special device files such as /dev/random or /dev/zero.		
CVE-2025-10700	CVE-2025-10700 - The Ally – Web Accessibility & Usability plugin for WordPress is vulnerable to Cross-Site Request Fo...	The Ally – Web Accessibility & Usability plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.8.0. This is due to missing or incorrect nonce validation on the enable_unfiltered_files_upload function. This makes it possible for unauthenticated attackers to enable unfiltered file upload and add svg files to the upload list 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-2025-10312	CVE-2025-10312 - The Theme Importer plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions ...	The Theme Importer plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing nonce validation when processing form submissions in the theme-importer.php file. This makes it possible for unauthenticated attackers to trigger arbitrary file downloads and potentially execute malicious operations 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-2025-10301	CVE-2025-10301 - The FunKItools plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up t...	The FunKItools 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 saveFields() function. This makes it possible for unauthenticated attackers to update 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-10300	CVE-2025-10300 - The TopBar plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, a...	The TopBar plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.0. This is due to missing or incorrect nonce validation on the fme_nb_topbar_save_settings() function. This makes it possible for unauthenticated attackers to update the plugin's 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-2025-60535	CVE-2025-60535 - A Cross-Site Request Forgery (CSRF) in the component /endpoints/currency/currency of Wallos v4.1.1 a...	A Cross-Site Request Forgery (CSRF) in the component /endpoints/currency/currency of Wallos v4.1.1 allows attackers to execute arbitrary operations via a crafted GET request.	Patched by core rule	Y
CVE-2025-11631	CVE-2025-11631 - A vulnerability was determined in RainyGao DocSys up to 2.02.36. Affected by this vulnerability is a...	A vulnerability was determined in RainyGao DocSys up to 2.02.36. Affected by this vulnerability is an unknown functionality of the file /Doc/deleteDoc.do. Executing manipulation of the argument path can lead to path traversal. The attack can 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
CVE-2025-11630	CVE-2025-11630 - A vulnerability was found in RainyGao DocSys up to 2.02.36. Affected is the function updateRealDoco...	A vulnerability was found in RainyGao DocSys up to 2.02.36. Affected is the function updateRealDoc of the file /Doc/uploadDoc.do of the component File Upload. Performing manipulation of the argument path results in path traversal. The attack can be initiated remotely. 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-2025-9950	CVE-2025-9950 - The Error Log Viewer by BestWebSoft plugin for WordPress is vulnerable	The Error Log Viewer by BestWebSoft plugin for WordPress is vulnerable to Directory Traversal in all	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	to Directory Traversal in all...	versions up to, and including, 1.1.6 via the rrrlgvwr_get_file function. This makes it possible for authenticated attackers, with Administrator-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.		
CVE-2025-9626	CVE-2025-9626 - The Page Blocks plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up ...	The Page Blocks plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.0. This is due to missing or incorrect nonce validation on the admin_process_widget_page_change function. This makes it possible for unauthenticated attackers to modify widget page block configurations 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-2025-9621	CVE-2025-9621 - The WidgetPack Comment System plugin for WordPress is vulnerable to Cross-Site Request Forgery in al...	The WidgetPack Comment System plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.6.1. This is due to missing or incorrect nonce validation on the wpcmt_sync action in the wpcmt_request_handler function. This makes it possible for unauthenticated attackers to trigger comment synchronization events 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-2025-8606	CVE-2025-8606 - The GSheetConnector For Gravity Forms plugin for WordPress is vulnerable to Cross-Site Request Forge...	The GSheetConnector For Gravity Forms plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions less than, or equal to, 1.3.23. This is due to missing or incorrect nonce validation on the activate_plugin and deactivate_plugin functions. This makes it possible for attackers to trick authenticated administrators into activating or deactivating specified plugins via a forged request, such as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		clicking on a malicious link or visiting a compromised page.		
CVE-2025-10376	CVE-2025-10376 - The Course Redirects for Learndash plugin for WordPress is vulnerable to Cross-Site Request Forgery ...	The Course Redirects for Learndash plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.4. This is due to missing nonce validation when processing form submissions on the settings page. 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-2025-10375	CVE-2025-10375 - The Web Accessibility By accessiBe plugin for WordPress is vulnerable to Cross-Site Request Forgery ...	The Web Accessibility By accessiBe plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.10. This is due to missing nonce validation on multiple AJAX actions including accessibe_signup, accessibe_login, accessibe_license_trial, accessibe_modify_config, and accessibe_add_verification_page. This makes it possible for unauthenticated attackers to modify plugin settings and create verification files 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-2025-62245	CVE-2025-62245 - Cross-site request forgery (CSRF) vulnerability in Liferay Portal 7.4.1 through 7.4.3.112, and Lifer...	Cross-site request forgery (CSRF) vulnerability in Liferay Portal 7.4.1 through 7.4.3.112, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.10, and 7.4 GA through update 92 allows remote attackers to add and edit publication comments.	Patched by core rule	Y
CVE-2025-7526	CVE-2025-7526 - The WP Travel Engine – Tour Booking Plugin – Tour Operator Software plugin for WordPress is vulnerab...	The WP Travel Engine – Tour Booking Plugin – Tour Operator Software plugin for WordPress is vulnerable to arbitrary file deletion (via renaming)	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		due to insufficient file path validation in the set_user_profile_image function in all versions up to, and including, 6.6.7. This makes it possible for unauthenticated attackers 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).		
CVE-2025-11166	CVE-2025-11166 - The WP Go Maps (formerly WP Google Maps) plugin for WordPress is vulnerable to Cross-Site Request Fo...	The WP Go Maps (formerly WP Google Maps) plugin for WordPress is vulnerable to Cross-Site Request Forgery (CSRF) in all versions up to, and including, 9.0.46. This is due to the plugin exposing state-changing REST actions through an AJAX bridge without proper CSRF token validation, and having destructive logic reachable via GET requests with no permission_callback. This makes it possible for unauthenticated attackers to force logged-in administrators to create, update, or delete markers and geometry features via CSRF attacks, and allows anonymous users to trigger mass deletion of markers via unsafe GET requests.	Patched by core rule	Y
CVE-2025-9886	CVE-2025-9886 - The Trinity Audio – Text to Speech AI audio player to convert content into audio plugin for WordPres...	The Trinity Audio – Text to Speech AI audio player to convert content into audio plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 5.20.2. This is due to missing or incorrect nonce validation in the '/admin/inc/post-management.php' file. This makes it possible for unauthenticated attackers to activate/deactivate 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-2025-9945	CVE-2025-9945 - The Optimize More! – CSS plugin for WordPress is vulnerable to Cross-Site Request Forgery in all ver...	The Optimize More! – CSS plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.3. This is due	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to missing or incorrect nonce validation on the reset_plugin function. This makes it possible for unauthenticated attackers to reset the plugin's optimization settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.		
CVE-2025-9897	CVE-2025-9897 - The AP Background plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions u...	The AP Background plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.8.2. This is due to missing or incorrect nonce validation on the advParallaxBackAdminSaveSlider function. This makes it possible for unauthenticated attackers to create or modify background sliders 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-2025-9895	CVE-2025-9895 - The Notification Bar plugin for WordPress is vulnerable to Cross-Site Request Forgery in all version...	The Notification Bar plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.2. This is due to missing or incorrect nonce validation on the 'subscriber-list-empty.php' file. This makes it possible for unauthenticated attackers to empty the subscriber list 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-2025-9892	CVE-2025-9892 - The Restrict User Registration plugin for WordPress is vulnerable to Cross-Site Request Forgery in a...	The Restrict User Registration 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 update() function. This makes it possible for unauthenticated attackers to update the plugin's 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-2025-9889	CVE-2025-9889 - The ContentMX Content Publisher plugin for WordPress is vulnerable to Cross-Site Request Forgery in ...	The ContentMX Content Publisher plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.6. This is due to missing or incorrect nonce validation on the cmx_activate_connection function. This makes it possible for unauthenticated attackers to bind their own ContentMX connection 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-2025-9885	CVE-2025-9885 - The MPWizard – Create Mercado Pago Payment Links plugin for WordPress is vulnerable to Cross-Site Re...	The MPWizard – Create Mercado Pago Payment Links plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.1. This is due to missing or incorrect nonce validation in the '/includes/admin/class-mpwizard-table.php' file. This makes it possible for unauthenticated attackers to delete arbitrary 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-2025-9884	CVE-2025-9884 - The Mobile Site Redirect plugin for WordPress is vulnerable to Cross-Site Request Forgery in all ver...	The Mobile Site Redirect plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.1. 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-2025-9630	CVE-2025-9630 - The WP SinoType plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up ...	The WP SinoType 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 the sinotype_config function.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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.		
CVE-2025-9213	CVE-2025-9213 - The TextBuilder plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions 1.0.0 t...	The TextBuilder plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions 1.0.0 to 1.1.1. This is due to missing or incorrect nonce validation on the 'handleToken' function. This makes it possible for unauthenticated attackers to update a user's authorization token via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Once the token is updated, an attacker can update the user's password and email address.	Patched by core rule	Y
CVE-2025-10311	CVE-2025-10311 - The Comment Info Detector plugin for WordPress is vulnerable to Cross-Site Request Forgery in all ve...	The Comment Info Detector plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.5. This is due to missing nonce validation on the options.php file when handling form submissions. 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-2025-10309	CVE-2025-10309 - The PayPal Forms plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up...	The PayPal Forms plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.3. This is due to missing nonce validation on the form creation and management functions. This makes it possible for unauthenticated attackers to create new PayPal forms and modify PayPal payment settings via a forged request granted they can trick a site administrator into	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		performing an action such as clicking on a link.		
CVE-2025-10302	CVE-2025-10302 - The Ultimate Viral Quiz plugin for WordPress is vulnerable to Cross-Site Request Forgery in all vers...	The Ultimate Viral Quiz 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 thesave_options() function. This makes it possible for unauthenticated attackers to update the plugin's 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-2025-9948	CVE-2025-9948 - The Chat by Chatwee plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions...	The Chat by Chatwee plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.1.3. This is due to missing or incorrect nonce validation on the admin settings page. 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-2025-9946	CVE-2025-9946 - The LockerPress – WordPress Security Plugin plugin for WordPress is vulnerable to Cross-Site Request...	The LockerPress – WordPress Security Plugin 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-2025-7052	CVE-2025-7052 - The LatePoint plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to...	The LatePoint plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 5.1.94. This is due to missing nonce validation on the change_password()	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		function of its customer_cabinet__change_password AJAX route. The plugin hooks this endpoint via wp_ajax and wp_ajax_nopriv but does not verify a nonce or user capability before resetting the user's password. This makes it possible for unauthenticated attackers who trick a logged-in customer (or, with "WP users as customers" enabled, an administrator) into visiting a malicious link to take over their account.		
CVE-2025-43813	CVE-2025-43813 - Possible path traversal vulnerability and denial-of-service in the ComboServlet in Liferay Portal 7....	Possible path traversal vulnerability and denial-of-service in the ComboServlet in Liferay Portal 7.4.0 through 7.4.3.107, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.4, 2023.Q3.1 through 2023.Q3.8, 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions allows remote attackers to access arbitrary CSS and JSS files and load the files multiple times via the query string in a URL.	Patched by core rule	Y
CVE-2025-11139	CVE-2025-11139 - A vulnerability was determined in Bjskzy Zhiyou ERP up to 11.0. Affected is the function uploadStudi...	A vulnerability was determined in Bjskzy Zhiyou ERP up to 11.0. Affected is the function uploadStudioFile of the component com.artery.form.services.FormStudioUpdater. This manipulation of the argument filepath causes path traversal. Remote exploitation of the attack is possible. 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-2025-9944	CVE-2025-9944 - The Professional Contact Form plugin for WordPress is vulnerable to Cross-Site Request Forgery in al...	The Professional Contact Form plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.0. This is due to missing or incorrect nonce validation on the watch_for_contact_form_submit function. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		makes it possible for unauthenticated attackers to trigger test email sending via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.		
CVE-2025-9899	CVE-2025-9899 - The Trust Reviews plugin for Google, Tripadvisor, Yelp, Airbnb and other platforms plugin for WordPr...	The Trust Reviews plugin for Google, Tripadvisor, Yelp, Airbnb and other platforms 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 the feed_save function. This makes it possible for unauthenticated attackers to create or modify feed entries 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-2025-9898	CVE-2025-9898 - The cForms – Light speed fast Form Builder plugin for WordPress is vulnerable to Cross-Site Request ...	The cForms – Light speed fast Form Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.0.0. This is due to missing or incorrect nonce validation on the cforms_api function. This makes it possible for unauthenticated attackers to modify forms and their 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-2025-9896	CVE-2025-9896 - The HidePost plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to,...	The HidePost plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.3.8. This is due to missing or incorrect nonce validation on the options.php settings page. 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-2025-9894	CVE-2025-9894 - The Sync Feedly plugin for WordPress is vulnerable to Cross-Site Request	The Sync Feedly plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Forgery in all versions up ...	including, 1.0.1. This is due to missing or incorrect nonce validation on the crsf_cron_job_func function. This makes it possible for unauthenticated attackers to trigger content synchronization from Feedly, potentially creating multiple posts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.		
CVE-2025-9893	CVE-2025-9893 - The VM Menu Reorder plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all v...	The VM Menu Reorder plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.0. This is due to missing or incorrect nonce validation on the vm_set_to_default function. This makes it possible for unauthenticated attackers to reset all menu reordering 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-2025-10499	CVE-2025-10499 - The Ninja Forms – The Contact Form Builder That Grows With You plugin for WordPress is vulnerable to...	The Ninja Forms – The Contact Form Builder That Grows With You plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.12.0. This is due to missing or incorrect nonce validation on the maybe_opt_in() function. This makes it possible for unauthenticated attackers to opt an affected site into usage statistics collection 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-2025-10498	CVE-2025-10498 - The Ninja Forms – The Contact Form Builder That Grows With You plugin for WordPress is vulnerable to...	The Ninja Forms – The Contact Form Builder That Grows With You plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.12.0. This is due to missing or incorrect nonce validation when exporting CSV files. This makes it possible for unauthenticated attackers to delete those files	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		granted they can trick an administrator into performing an action such as clicking on a link.		
CVE-2025-11034	CVE-2025-11034 - A vulnerability was found in Dibo Data Decision Making System up to 2.7.0. The affected element is t...	A vulnerability was found in Dibo Data Decision Making System up to 2.7.0. The affected element is the function downloadImpTemplet of the file /common/dep/common_dep.action.jsp. The manipulation of the argument filePath results in path traversal. It is possible to launch the attack remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2025-11031	CVE-2025-11031 - A flaw has been found in DataTables up to 1.10.13. The affected element is an unknown function of th...	A flaw has been found in DataTables up to 1.10.13. The affected element is an unknown function of the file /examples/resources/examples.php. This manipulation of the argument src causes path traversal. It is possible to initiate the attack remotely. The exploit has been published and may be used. Upgrading to version 1.10.15 is sufficient to fix this issue. Patch name: 3b24f99ac4ddb7f9072076b0d07f0b1a408f177a. Upgrading the affected component is advised. This vulnerability was initially reported for code-projects Faculty Management System but appears to affect DataTables as an upstream component instead. The vendor of DataTables explains: "I would suggest that the author upgrade to the latest versions of DataTables (actually, they shouldn't really be deploying that file to their own server at all - it is only relevant for the DataTables examples)."	Patched by core rule	Y
CVE-2025-11029	CVE-2025-11029 - A weakness has been identified in givanz Vvveb up to 1.0.7.2. This vulnerability affects unknown cod...	A weakness has been identified in givanz Vvveb up to 1.0.7.2. This vulnerability affects unknown code. Executing manipulation can lead to cross-site request forgery. The attack can be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		executed remotely. The exploit has been made available to the public and could be exploited. Once again the project maintainer reacted very professional: "I accept the existence of these vulnerabilities. (...) I fixed the code to remove these vulnerabilities and will push the code to github and make a new release."		
CVE-2025-60173	CVE-2025-60173 - Cross-Site Request Forgery (CSRF) vulnerability in Ashwani kumar GST for WooCommerce allows Stored X...	Cross-Site Request Forgery (CSRF) vulnerability in Ashwani kumar GST for WooCommerce allows Stored XSS. This issue affects GST for WooCommerce: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-60172	CVE-2025-60172 - Cross-Site Request Forgery (CSRF) vulnerability in flytedesk Flytedesk Digital allows Stored XSS. Th...	Cross-Site Request Forgery (CSRF) vulnerability in flytedesk Flytedesk Digital allows Stored XSS. This issue affects Flytedesk Digital: from n/a through 20181101.	Patched by core rule	Y
CVE-2025-60171	CVE-2025-60171 - Cross-Site Request Forgery (CSRF) vulnerability in yourplugins Conditional Cart Messages for WooComm...	Cross-Site Request Forgery (CSRF) vulnerability in yourplugins Conditional Cart Messages for WooCommerce – YourPlugins.com allows Stored XSS. This issue affects Conditional Cart Messages for WooCommerce – YourPlugins.com: from n/a through 1.2.10.	Patched by core rule	Y
CVE-2025-60170	CVE-2025-60170 - Cross-Site Request Forgery (CSRF) vulnerability in Taraprasad Swain HTACCESS IP Blocker allows Store...	Cross-Site Request Forgery (CSRF) vulnerability in Taraprasad Swain HTACCESS IP Blocker allows Stored XSS. This issue affects HTACCESS IP Blocker: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-60169	CVE-2025-60169 - Cross-Site Request Forgery (CSRF) vulnerability in W3S Cloud Technology W3SCloud Contact Form 7 to Z...	Cross-Site Request Forgery (CSRF) vulnerability in W3S Cloud Technology W3SCloud Contact Form 7 to Zoho CRM allows Stored XSS. This issue affects W3SCloud Contact Form 7 to Zoho CRM: from n/a through 3.0.	Patched by core rule	Y
CVE-2025-60164	CVE-2025-60164 - Cross-Site Request Forgery (CSRF) vulnerability in NewsMAN NewsmanApp allows Stored XSS. This issue ...	Cross-Site Request Forgery (CSRF) vulnerability in NewsMAN NewsmanApp allows Stored XSS. This issue affects NewsmanApp: from n/a through 2.7.7.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-60156	CVE-2025-60156 - Cross-Site Request Forgery (CSRF) vulnerability in webandprint AR For WordPress allows Upload a Web ...	Cross-Site Request Forgery (CSRF) vulnerability in webandprint AR For WordPress allows Upload a Web Shell to a Web Server. This issue affects AR For WordPress: from n/a through 7.98.	Patched by core rule	Y
CVE-2025-60145	CVE-2025-60145 - Cross-Site Request Forgery (CSRF) vulnerability in yonifre Lenix scss compiler allows Cross Site Req...	Cross-Site Request Forgery (CSRF) vulnerability in yonifre Lenix scss compiler allows Cross Site Request Forgery. This issue affects Lenix scss compiler: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-60139	CVE-2025-60139 - Cross-Site Request Forgery (CSRF) vulnerability in Joovii Sendle Shipping allows Cross Site Request ...	Cross-Site Request Forgery (CSRF) vulnerability in Joovii Sendle Shipping allows Cross Site Request Forgery. This issue affects Sendle Shipping: from n/a through 6.02.	Patched by core rule	Y
CVE-2025-60137	CVE-2025-60137 - Cross-Site Request Forgery (CSRF) vulnerability in Galaxy Weblinks Post Featured Video allows Cross ...	Cross-Site Request Forgery (CSRF) vulnerability in Galaxy Weblinks Post Featured Video allows Cross Site Request Forgery. This issue affects Post Featured Video: from n/a through 1.7.	Patched by core rule	Y
CVE-2025-60117	CVE-2025-60117 - Cross-Site Request Forgery (CSRF) vulnerability in TangibleWP Vehica Core allows Cross Site Request ...	Cross-Site Request Forgery (CSRF) vulnerability in TangibleWP Vehica Core allows Cross Site Request Forgery. This issue affects Vehica Core: from n/a through 1.0.100.	Patched by core rule	Y
CVE-2025-60115	CVE-2025-60115 - Cross-Site Request Forgery (CSRF) vulnerability in instapagedev Instapage Plugin allows Cross Site R...	Cross-Site Request Forgery (CSRF) vulnerability in instapagedev Instapage Plugin allows Cross Site Request Forgery. This issue affects Instapage Plugin: from n/a through 3.5.12.	Patched by core rule	Y
CVE-2025-60113	CVE-2025-60113 - Cross-Site Request Forgery (CSRF) vulnerability in grooni Groovy Menu allows Cross Site Request Forg...	Cross-Site Request Forgery (CSRF) vulnerability in grooni Groovy Menu allows Cross Site Request Forgery. This issue affects Groovy Menu: from n/a through 1.4.3.	Patched by core rule	Y
CVE-2025-60111	CVE-2025-60111 - Cross-Site Request Forgery (CSRF) vulnerability in javothemes Javo Core allows Authentication Bypass...	Cross-Site Request Forgery (CSRF) vulnerability in javothemes Javo Core allows Authentication Bypass. This issue affects Javo Core: from n/a through 3.0.0.266.	Patched by core rule	Y
CVE-2025-60093	CVE-2025-60093 - Cross-Site Request Forgery (CSRF) vulnerability in Shahjada Download Manager allows Cross	Cross-Site Request Forgery (CSRF) vulnerability in Shahjada Download Manager allows Cross Site Request Forgery. This issue	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Site Reque...	affects Download Manager: from n/a through 3.3.24.		
CVE-2025-59002	CVE-2025-59002 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in SeaT...	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in SeaTheme BM Content Builder allows Path Traversal. This issue affects BM Content Builder: from n/a through n/a.	Patched by core rule	Y
CVE-2025-58914	CVE-2025-58914 - Cross-Site Request Forgery (CSRF) vulnerability in Di Themes Di Themes Demo Site Importer allows Cro...	Cross-Site Request Forgery (CSRF) vulnerability in Di Themes Di Themes Demo Site Importer allows Cross Site Request Forgery. This issue affects Di Themes Demo Site Importer: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-10307	CVE-2025-10307 - The Backuply – Backup, Restore, Migrate and Clone plugin for WordPress is vulnerable to arbitrary fi...	The Backuply – Backup, Restore, Migrate and Clone plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete backup functionality in all versions up to, and including, 1.4.8. This makes it possible for authenticated attackers, with Administrator-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

Server-side Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-10861	CVE-2025-10861 - The Popup builder with Gamification, Multi-Step Popups, Page-Level Targeting, and WooCommerce Trigge...	The Popup builder with Gamification, Multi-Step Popups, Page-Level Targeting, and WooCommerce Triggers plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 2.1.4. This is due to insufficient validation on the URLs supplied via the URL parameter. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services, as well as conduct network reconnaissance. The vulnerability was partially patched in version 2.1.4.	Patched by core rule	Y
CVE-2025-12136	CVE-2025-12136 - The Real Cookie Banner: GDPR & ePrivacy Cookie Consent plugin for WordPress is vulnerable to Server-...	The Real Cookie Banner: GDPR & ePrivacy Cookie Consent plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 5.2.4. This is due to insufficient validation on the user-supplied URL in the '/scanner/scan-without-login' REST API endpoint. This makes it possible for authenticated attackers, with administrator-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services via the `url` parameter.	Patched by core rule	Y
CVE-2025-11128	CVE-2025-11128 - The RSS Aggregator by Feedzy – Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator plu...	The RSS Aggregator by Feedzy – Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 5.1.0 via the 'feedzy_sanitize_feeds' function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to make web requests to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		arbitrary locations originating from the web application and can be used to query information from internal services.		
CVE-2025-10705	CVE-2025-10705 - The MxChat – AI Chatbot for WordPress plugin for WordPress is vulnerable to Blind Server-Side Reques...	The MxChat – AI Chatbot for WordPress plugin for WordPress is vulnerable to Blind Server-Side Request Forgery in all versions up to, and including, 2.4.6. This is due to insufficient validation of user-supplied URLs in the PDF processing functionality. This makes it possible for unauthenticated attackers to make the WordPress server perform HTTP requests to arbitrary destinations via the mxchat_handle_chat_request AJAX action.	Patched by core rule	Y
CVE-2025-11536	CVE-2025-11536 - The Element Pack Addons for Elementor plugin for WordPress is vulnerable to Blind Server-Side Reques...	The Element Pack Addons for Elementor plugin for WordPress is vulnerable to Blind Server-Side Request Forgery in all versions up to, and including, 8.2.5 via the wp_ajax_import_elementor_template action. This makes it possible for authenticated attackers, with Subscriber-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	Patched by core rule	Y
CVE-2025-11361	CVE-2025-11361 - The Gutenberg Essential Blocks – Page Builder for Gutenberg Blocks & Patterns plugin for WordPress i...	The Gutenberg Essential Blocks – Page Builder for Gutenberg Blocks & Patterns plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 5.7.1 via the eb_save_ai_generated_image function. This makes it possible for authenticated attackers, with Author-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	Patched by core rule	Y
CVE-2025-60279	CVE-2025-60279 - A server-side request forgery (SSRF) vulnerability in Illia Cloud illia-Builder before v4.8.5 allows...	A server-side request forgery (SSRF) vulnerability in Illia Cloud illia-Builder before v4.8.5 allows authenticated users to send arbitrary requests to internal services via the API. An attacker can	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		leverage this to enumerate open ports based on response discrepancies and interact with internal services.		
CVE-2025-11864	CVE-2025-11864 - A vulnerability was identified in NucleoidAI Nucleoid up to 0.7.10. The impacted element is the func...	A vulnerability was identified in NucleoidAI Nucleoid up to 0.7.10. The impacted element is the function extension.apply of the file /src/cluster.ts of the component Outbound Request Handler. Such manipulation of the argument https/ip/port/path/headers leads to server-side request forgery. The attack may be performed from remote.	Patched by core rule	Y
CVE-2025-60540	CVE-2025-60540 - karakeep v0.26.0 to v0.7.0 was discovered to contain a Server-Side Request Forgery (SSRF).	karakeep v0.26.0 to v0.7.0 was discovered to contain a Server-Side Request Forgery (SSRF).	Patched by core rule	Y
CVE-2025-11648	CVE-2025-11648 - A vulnerability has been found in Tomofun Furbo 360 and Furbo Mini. Impacted is an unknown function ...	A vulnerability has been found in Tomofun Furbo 360 and Furbo Mini. Impacted is an unknown function of the file TF_FQDN.json of the component GATT Interface URL Handler. Such manipulation leads to server-side request forgery. The attack may be performed from remote. Attacks of this nature are highly complex. The exploitability is considered difficult. The firmware versions determined to be affected are Furbo 360 up to FB0035_FW_036 and Furbo Mini up to MC0020_FW_074. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-9975	CVE-2025-9975 - The WP Scraper plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up ...	The WP Scraper plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 5.8.1 via the wp_scraper_extract_content function. This makes it possible for authenticated attackers, with Administrator-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. On Cloud instances, this issue allows for	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		metadata retrieving.		
CVE-2025-55971	CVE-2025-55971 - TCL 65C655 Smart TV, running firmware version V8-R75PT01-LF1V269.001116 (Android TV, Kernel 5.4.242+...	TCL 65C655 Smart TV, running firmware version V8-R75PT01-LF1V269.001116 (Android TV, Kernel 5.4.242+), is vulnerable to a blind, unauthenticated Server-Side Request Forgery (SSRF) vulnerability via the UPnP MediaRenderer service (AVTransport:1). The device accepts unauthenticated SetAVTransportURI SOAP requests over TCP/16398 and attempts to retrieve externally referenced URIs, including attacker-controlled payloads. The blind SSRF allows for sending requests on behalf of the TV, which can be leveraged to probe for other internal or external services accessible by the device (e.g., 127.0.0.1:16XXX, LAN services, or internet targets), potentially enabling additional exploit chains.	Patched by core rule	Y
CVE-2025-10735	CVE-2025-10735 - The Block For Mailchimp – Easy Mailchimp Form Integration plugin for WordPress is vulnerable to Blin...	The Block For Mailchimp – Easy Mailchimp Form Integration plugin for WordPress is vulnerable to Blind Server-Side Request Forgery in all versions up to, and including, 1.1.12 via the mcbSubmit_Form_Data(). This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	Patched by core rule	Y
CVE-2025-60181	CVE-2025-60181 - Server-Side Request Forgery (SSRF) vulnerability in silence Silencesoft RSS Reader allows Server Sid...	Server-Side Request Forgery (SSRF) vulnerability in silence Silencesoft RSS Reader allows Server Side Request Forgery. This issue affects Silencesoft RSS Reader: from n/a through 0.6.	Patched by core rule	Y
CVE-2025-60161	CVE-2025-60161 - Server-Side Request Forgery (SSRF) vulnerability in BdThemes ZoloBlocks zoloblocks allows Server Sid...	Server-Side Request Forgery (SSRF) vulnerability in BdThemes ZoloBlocks zoloblocks allows Server Side Request Forgery.This issue affects ZoloBlocks: from n/a through 2.3.11.	Patched by core rule	Y

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-9322	CVE-2025-9322 - The Stripe Payment Forms by WP Full Pay – Accept Credit Card Payments, Donations & Subscriptions plu...	The Stripe Payment Forms by WP Full Pay – Accept Credit Card Payments, Donations & Subscriptions plugin for WordPress is vulnerable to SQL Injection via the 'wpfs-form-name' parameter in all versions up to, and including, 8.3.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-8416	CVE-2025-8416 - The Product Filter by WBW plugin for WordPress is vulnerable to SQL Injection via the 'filtersDataBa...	The Product Filter by WBW plugin for WordPress is vulnerable to SQL Injection via the 'filtersDataBackend' parameter in all versions up to, and including, 2.9.7. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-4203	CVE-2025-4203 - The wpForo Forum plugin for WordPress is vulnerable to error-based or time-based SQL Injection via t...	The wpForo Forum plugin for WordPress is vulnerable to error-based or time-based SQL Injection via the get_members() function in all versions up to, and including, 2.4.8 due to missing integer validation on the 'offset' and 'row_count' parameters. The function blindly interpolates 'row_count' into a 'LIMIT offset,row_count' clause using esc_sql() rather than enforcing numeric values. MySQL 5.x's grammar allows a 'PROCEDURE ANALYSE' clause immediately after a LIMIT clause. Unauthenticated attackers controlling 'row_count' can append a stored-procedure call, enabling error-based or time-based blind SQL	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		injection that can be used to extract sensitive information from the database.		
CVE-2025-11893	CVE-2025-11893 - The Charitable – Donation Plugin for WordPress – Fundraising with Recurring Donations & More plugin ...	The Charitable – Donation Plugin for WordPress – Fundraising with Recurring Donations & More plugin for WordPress is vulnerable to SQL Injection via the donation_ids parameter in all versions up to, and including, 1.8.8.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation of the vulnerability requires a paid donation.	Patched by core rule	Y
CVE-2025-10748	CVE-2025-10748 - The RapidResult plugin for WordPress is vulnerable to SQL Injection via the 's' parameter in all ver...	The RapidResult plugin for WordPress is vulnerable to SQL Injection via the 's' parameter in all versions up to, and including, 1.2. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with contributor-level permissions and above to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-10740	CVE-2025-10740 - The URL Shortener Plugin For WordPress plugin for WordPress is vulnerable to unauthorized access to ...	The URL Shortener Plugin For WordPress plugin for WordPress is vulnerable to unauthorized access to functionality provided by the API due to a missing capability check on the verifyRequest function in all versions up to, and including, 3.0.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify links.	Patched by core rule	Y
CVE-2025-61194	CVE-2025-61194 - daicuocms V1.3.13 contains a SQL injection vulnerability in the file library\think\db\Builder.	daicuocms V1.3.13 contains a SQL injection vulnerability in the file library\think\db\Builder.php .	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	php.			
CVE-2025-56450	CVE-2025-56450 - Log2Space Subscriber Management Software 1.1 is vulnerable to unauthenticated SQL injection via the ...	Log2Space Subscriber Management Software 1.1 is vulnerable to unauthenticated SQL injection via the `lead_id` parameter in the `/l2s/api/selfcareLeadHistory` endpoint. A remote attacker can exploit this by sending a specially crafted POST request, resulting in the execution of arbitrary SQL queries. The backend fails to sanitize the user input, allowing enumeration of database schemas, table names, and potentially leading to full database compromise.	Patched by core rule	Y
CVE-2025-61455	CVE-2025-61455 - SQL Injection vulnerability exists in Bhabishya-123 E-commerce 1.0, specifically within the signup.i...	SQL Injection vulnerability exists in Bhabishya-123 E-commerce 1.0, specifically within the signup.inc.php endpoint. The application directly incorporates unsanitized user inputs into SQL queries, allowing unauthenticated attackers to bypass authentication and gain full access.	Patched by core rule	Y
CVE-2025-11691	CVE-2025-11691 - The PPOM – Product Addons & Custom Fields for WooCommerce plugin for WordPress is vulnerable to SQL ...	The PPOM – Product Addons & Custom Fields for WooCommerce plugin for WordPress is vulnerable to SQL Injection via the PPOM_Meta::get_fields_by_id() function in all versions up to, and including, 33.0.15 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This is only exploitable when the Enable Legacy Price Calculations setting is enabled.	Patched by core rule	Y
CVE-2025-10187	CVE-2025-10187 - The GSpeech TTS – WordPress Text To Speech Plugin plugin for WordPress is vulnerable to SQL Injectio...	The GSpeech TTS – WordPress Text To Speech Plugin plugin for WordPress is vulnerable to SQL Injection via the 'field' parameter in all versions up to, and including, 3.17.13 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.		
CVE-2025-11912	CVE-2025-11912 - A flaw has been found in Shenzhen Ruiming Technology Streamax Crocus 1.3.40. Affected is the functio...	A flaw has been found in Shenzhen Ruiming Technology Streamax Crocus 1.3.40. Affected is the function Query of the file /DeviceState.do?Action=Query. This manipulation of the argument orderField causes sql injection. The attack can 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-2025-11911	CVE-2025-11911 - A vulnerability was detected in Shenzhen Ruiming Technology Streamax Crocus 1.3.40. This impacts the...	A vulnerability was detected in Shenzhen Ruiming Technology Streamax Crocus 1.3.40. This impacts the function Query of the file /DeviceFault.do?Action=Query. The manipulation of the argument sortField results in sql injection. It is possible to launch the attack 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.	Patched by core rule	Y
CVE-2025-11910	CVE-2025-11910 - A security vulnerability has been detected in Shenzhen Ruiming Technology Streamax Crocus 1.3.40. Th...	A security vulnerability has been detected in Shenzhen Ruiming Technology Streamax Crocus 1.3.40. This affects the function Query of the file /MemoryState.do?Action=Query. The manipulation of the argument orderField leads to sql injection. It is possible to initiate the attack 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-2025-56316	CVE-2025-56316 - A SQL injection vulnerability in the content_title parameter of the /cms/content/list endpoint in MC...	A SQL injection vulnerability in the content_title parameter of the /cms/content/list endpoint in MCMS 5.5.0 allows remote attackers to execute arbitrary SQL queries via unsanitized input in the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		FreeMarker template rendering.		
CVE-2025-11909	CVE-2025-11909 - A weakness has been identified in Shenzhen Ruiming Technology Streamax Crocus 1.3.40. The impacted e...	A weakness has been identified in Shenzhen Ruiming Technology Streamax Crocus 1.3.40. The impacted element is the function queryLast of the file /RepairRecord.do?Action=QueryLast. Executing manipulation of the argument orderField can lead to sql injection. The attack may be performed from remote. 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-2025-11905	CVE-2025-11905 - A vulnerability was found in yanyutao0402 ChanCMS up to 3.3.2. This vulnerability affects the functi...	A vulnerability was found in yanyutao0402 ChanCMS up to 3.3.2. This vulnerability affects the function getArticle of the file app\modules\cms\controller\gather.js. The manipulation results in code injection. The attack may be launched remotely. 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-2025-11904	CVE-2025-11904 - A vulnerability has been found in yanyutao0402 ChanCMS up to 3.3.2. This affects the function hasUse...	A vulnerability has been found in yanyutao0402 ChanCMS up to 3.3.2. This affects the function hasUse of the file /cms/model/hasUse. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-11903	CVE-2025-11903 - A flaw has been found in yanyutao0402 ChanCMS up to 3.3.2. Affected by this issue is the function up...	A flaw has been found in yanyutao0402 ChanCMS up to 3.3.2. Affected by this issue is the function update of the file /cms/article/update. Executing manipulation of the argument cid can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used. The vendor was contacted early	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		about this disclosure but did not respond in any way.		
CVE-2025-11902	CVE-2025-11902 - A vulnerability was detected in yanyutao0402 ChanCMS up to 3.3.2. Affected by this vulnerability is ...	A vulnerability was detected in yanyutao0402 ChanCMS up to 3.3.2. Affected by this vulnerability is the function findField of the file /cms/article/findField. Performing manipulation of the argument cid results in sql injection. The attack can be initiated 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.	Patched by core rule	Y
CVE-2025-56700	CVE-2025-56700 - Boolean SQL injection vulnerability in the web app of Base Digitale Group spa product Centrax Open P...	Boolean SQL injection vulnerability in the web app of Base Digitale Group spa product Centrax Open PSIM version 6.1 allows a low level priviliged user that has access to the platform, to execute arbitrary SQL commands via the datafine parameter.	Patched by core rule	Y
CVE-2025-56699	CVE-2025-56699 - SQL injection vulnerability in the cmd component of Base Digitale Group spa product Centrax Open PSI...	SQL injection vulnerability in the cmd component of Base Digitale Group spa product Centrax Open PSIM version 6.1 allows an unauthenticated user to execute arbitrary SQL commands via the sender parameter.	Patched by core rule	Y
CVE-2025-61540	CVE-2025-61540 - SQL injection vulnerability in Ultimate PHP Board 2.2.7 via the username field in lostpassword.php.	SQL injection vulnerability in Ultimate PHP Board 2.2.7 via the username field in lostpassword.php.	Patched by core rule	Y
CVE-2025-11365	CVE-2025-11365 - The WP Google Map Plugin plugin for WordPress is vulnerable to blind SQL Injection via the 'id' para...	The WP Google Map Plugin plugin for WordPress is vulnerable to blind SQL Injection via the 'id' parameter of the 'google_map' shortcode in all versions up to, and including, 1.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-11177	CVE-2025-11177 - The External Login plugin for	The External Login 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 SQL Injection via the 'log' parameter in al...	SQL Injection via the 'log' parameter in all versions up to, and including, 1.11.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database when a PostgreSQL or MSSQL database is configured as the external authentication database.		
CVE-2025-10743	CVE-2025-10743 - The Outdoor plugin for WordPress is vulnerable to SQL Injection via the 'edit' action in all version...	The Outdoor plugin for WordPress is vulnerable to SQL Injection via the 'edit' action in all versions up to, and including, 1.3.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-10730	CVE-2025-10730 - The Wp tabber widget plugin for WordPress is vulnerable to SQL Injection via the 'wp-tabber-widget' ...	The Wp tabber widget plugin for WordPress is vulnerable to SQL Injection via the 'wp-tabber-widget' shortcode in all versions up to, and including, 4.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-10682	CVE-2025-10682 - The TARIFFUXX plugin for WordPress is vulnerable to SQL Injection in versions up to, and including, ...	The TARIFFUXX plugin for WordPress is vulnerable to SQL Injection in versions up to, and including, 1.4. This is due to insufficient neutralization of user-supplied input used directly in SQL queries. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject additional SQL into	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		queries and extract sensitive information from the database via a crafted id attribute in the 'tariffuxx_configurator' shortcode.		
CVE-2025-10660	CVE-2025-10660 - The WP Dashboard Chat plugin for WordPress is vulnerable to SQL Injection via the ‘id’ parameter in ...	The WP Dashboard Chat plugin for WordPress is vulnerable to SQL Injection via the ‘id’ parameter in all versions up to, and including, 1.0.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-10575	CVE-2025-10575 - The WP jQuery Pager plugin for WordPress is vulnerable to SQL Injection via the 'ids' shortcode attr...	The WP jQuery Pager plugin for WordPress is vulnerable to SQL Injection via the 'ids' shortcode attribute parameter handled by the WPJqueryPaged::get_gallery_page_imgs() function in all versions up to, and including, 1.4.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-10310	CVE-2025-10310 - The Rich Snippet Site Report plugin for WordPress is vulnerable to SQL Injection via the 'last' par...	The Rich Snippet Site Report plugin for WordPress is vulnerable to SQL Injection via the 'last' parameter in all versions up to, and including, 2.0.0105 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This can also be exploited via CSRF.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-11501	CVE-2025-11501 - The Dynamically Display Posts plugin for WordPress is vulnerable to SQL Injection via the 'tax_query...	The Dynamically Display Posts plugin for WordPress is vulnerable to SQL Injection via the 'tax_query' parameter in all versions up to, and including, 1.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-11629	CVE-2025-11629 - A vulnerability has been found in RainyGao DocSys up to 2.02.36. This impacts the function getUserLi...	A vulnerability has been found in RainyGao DocSys up to 2.02.36. This impacts the function getUserList of the file /Manage/getUserList.do. Such manipulation leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-11615	CVE-2025-11615 - A security flaw has been discovered in SourceCodester Best Salon Management System 1.0. This affects...	A security flaw has been discovered in SourceCodester Best Salon Management System 1.0. This affects an unknown part of the file /panel/add_invoice.php. Performing manipulation of the argument ServiceId results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited.	Patched by core rule	Y
CVE-2025-11608	CVE-2025-11608 - A security vulnerability has been detected in code-projects E-Banking System 1.0. This affects an un...	A security vulnerability has been detected in code-projects E-Banking System 1.0. This affects an unknown function of the file /register.php of the component POST Parameter Handler. The manipulation of the argument username/password leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2025-11597	CVE-2025-11597 - A vulnerability was identified in code-	A vulnerability was identified in code-projects E-Commerce Website 1.0. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	projects E-Commerce Website 1.0. The impacted element is an u...	impacted element is an unknown function of the file /pages/product_add_qty.php. The manipulation of the argument prod_id leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.		
CVE-2025-9947	CVE-2025-9947 - The Custom 404 Pro plugin for WordPress is vulnerable to time-based SQL Injection via the 'path' par...	The Custom 404 Pro plugin for WordPress is vulnerable to time-based SQL Injection via the 'path' parameter in all versions up to, and including, 3.12.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-11596	CVE-2025-11596 - A vulnerability was determined in code-projects E-Commerce Website 1.0. The affected element is an u...	A vulnerability was determined in code-projects E-Commerce Website 1.0. The affected element is an unknown function of the file /pages/delete_order_details.php. Executing manipulation of the argument order_id can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-10185	CVE-2025-10185 - The NEX-Forms – Ultimate Forms Plugin for WordPress plugin for WordPress is vulnerable to SQL Inject...	The NEX-Forms – Ultimate Forms Plugin for WordPress plugin for WordPress is vulnerable to SQL Injection via the 'orderby' parameter in the action nf_load_form_entries in all versions up to, and including, 9.1.6 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This may be exploitable by lower-level	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		users if access is granted by a site administrator.		
CVE-2025-10048	CVE-2025-10048 - The My auctions allegro plugin for WordPress is vulnerable to SQL Injection via the 'order' paramete...	The My auctions allegro plugin for WordPress is vulnerable to SQL Injection via the 'order' parameter in all versions up to, and including, 3.6.31 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-60307	CVE-2025-60307 - code-projects Computer Laboratory System 1.0 has a SQL injection vulnerability, where entering a uni...	code-projects Computer Laboratory System 1.0 has a SQL injection vulnerability, where entering a universal password in the Password field on the login page can bypass login attempts.	Patched by core rule	Y
CVE-2025-11556	CVE-2025-11556 - A flaw has been found in code-projects Simple Leave Manager 1.0. This vulnerability affects unknown ...	A flaw has been found in code-projects Simple Leave Manager 1.0. This vulnerability affects unknown code of the file /user.php. This manipulation of the argument table causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2025-60316	CVE-2025-60316 - SourceCodester Pet Grooming Management Software 1.0 is vulnerable to SQL Injection in admin/view_cus...	SourceCodester Pet Grooming Management Software 1.0 is vulnerable to SQL Injection in admin/view_customer.php via the ID parameter.	Patched by core rule	Y
CVE-2025-11551	CVE-2025-11551 - A vulnerability was determined in code-projects Student Result Manager 1.0. This affects an unknown ...	A vulnerability was determined in code-projects Student Result Manager 1.0. This affects an unknown function of the file src/students/Database.java. This manipulation of the argument roll/name/gpa causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-10862	CVE-2025-10862 - The Popup builder with Gamification, Multi-Step Popups, Page-Level	The Popup builder with Gamification, Multi-Step Popups, Page-Level Targeting, and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Targeting, and WooCommerce Trigge...	WooCommerce Triggers plugin for WordPress is vulnerable to SQL Injection in all versions up to, and including, 2.1.3. This is due to insufficient escaping on the 'id' parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.		
CVE-2025-11523	CVE-2025-11523 - A vulnerability was detected in Tenda AC7 15.03.06.44. This vulnerability affects unknown code of th...	A vulnerability was detected in Tenda AC7 15.03.06.44. This vulnerability affects unknown code of the file /goform/AdvSetLanip. The manipulation of the argument lanIp results in command injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-10586	CVE-2025-10586 - The Community Events plugin for WordPress is vulnerable to SQL Injection via the ‘event_venue’ param...	The Community Events plugin for WordPress is vulnerable to SQL Injection via the ‘event_venue’ parameter in all versions up to, and including, 1.5.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-11513	CVE-2025-11513 - A vulnerability was determined in code-projects E-Commerce Website 1.0. This affects an unknown part...	A vulnerability was determined in code-projects E-Commerce Website 1.0. This affects an unknown part of the file /pages/supplier_update.php . This manipulation of the argument supp_id causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-11511	CVE-2025-11511 - A flaw has been found in code-projects E-Commerce Website 1.0. Affected is an unknown function of th...	A flaw has been found in code-projects E-Commerce Website 1.0. Affected is an unknown function of the file /pages/supplier_add.php. Executing manipulation of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the argument supp_email can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.		
CVE-2025-11509	CVE-2025-11509 - A vulnerability was detected in code-projects E-Commerce Website 1.0. This impacts an unknown functi...	A vulnerability was detected in code-projects E-Commerce Website 1.0. This impacts an unknown function of the file /pages/product_add.php. Performing manipulation of the argument prod_name results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-60311	CVE-2025-60311 - ProjectWorlds Gym Management System1.0 is vulnerable to SQL Injection via the "id" parameter in the ...	ProjectWorlds Gym Management System1.0 is vulnerable to SQL Injection via the "id" parameter in the profile/edit.php page	Patched by core rule	Y
CVE-2025-10649	CVE-2025-10649 - The Welcart e-Commerce plugin for WordPress is vulnerable to SQL Injection via the cookie in all ver...	The Welcart e-Commerce plugin for WordPress is vulnerable to SQL Injection via the cookie in all versions up to, and including, 2.11.21 due to insufficient escaping on the user supplied value and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Author-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-11204	CVE-2025-11204 - The RegistrationMagic – Custom Registration Forms, User Registration, Payment, and User Login plugin...	The RegistrationMagic – Custom Registration Forms, User Registration, Payment, and User Login plugin for WordPress is vulnerable to SQL Injection in all versions up to, and including, 6.0.6.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator access or higher, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. An unauthenticated attacker could utilize an injected	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Cross-Site Scripting via user-agent on form submission to leverage this to achieve Reflected Cross-Site Scripting.		
CVE-2025-11431	CVE-2025-11431 - A vulnerability was determined in code-projects Web-Based Inventory and POS System 1.0. The impacted...	A vulnerability was determined in code-projects Web-Based Inventory and POS System 1.0. The impacted element is an unknown function of the file /transaction.php. This manipulation of the argument shopid causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-10587	CVE-2025-10587 - The Community Events plugin for WordPress is vulnerable to SQL Injection via the event_category para...	The Community Events plugin for WordPress is vulnerable to SQL Injection via the event_category parameter in all versions up to, and including, 1.5.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-11424	CVE-2025-11424 - A vulnerability was determined in code-projects Web-Based Inventory and POS System 1.0. This impacts...	A vulnerability was determined in code-projects Web-Based Inventory and POS System 1.0. This impacts an unknown function of the file /login.php. Executing manipulation of the argument emailid can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-52021	CVE-2025-52021 - A SQL Injection vulnerability exists in the edit_product.php file of PuneethReddyHC Online Shopping ...	A SQL Injection vulnerability exists in the edit_product.php file of PuneethReddyHC Online Shopping System Advanced 1.0. The product_id GET parameter is unsafely passed to a SQL query without proper validation or parameterization.	Patched by core rule	Y
CVE-2025-57515	CVE-2025-57515 - A SQL injection vulnerability has been identified in Uniclare Student Portal	A SQL injection vulnerability has been identified in Uniclare Student Portal v2. This flaw allows remote	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	v2. This flaw allows re...	attackers to inject arbitrary SQL commands via vulnerable input fields, enabling the execution of time-delay functions to infer database responses.		
CVE-2025-11343	CVE-2025-11343 - A security vulnerability has been detected in code-projects Student Crud Operation 3.3. Affected is ...	A security vulnerability has been detected in code-projects Student Crud Operation 3.3. Affected is an unknown function of the file delete.php. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2025-11317	CVE-2025-11317 - A vulnerability was identified in Tipray 厦门天锐科技股份有限公司 Data Leakage Prevention System 天锐数据泄露防护系统 1.0....	A vulnerability was identified in Tipray 厦门天锐科技股份有限公司 Data Leakage Prevention System 天锐数据泄露防护系统 1.0. This affects the function findRolePage of the file findSingConfigPage.do. The manipulation of the argument sort leads to sql injection. 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-2025-11316	CVE-2025-11316 - A vulnerability was determined in Tipray 厦门天锐科技股份有限公司 Data Leakage Prevention System 天锐数据泄露防护系统 1.0....	A vulnerability was determined in Tipray 厦门天锐科技股份有限公司 Data Leakage Prevention System 天锐数据泄露防护系统 1.0. Affected by this issue is the function findCategoryPage of the file findCategoryPage.do. Executing manipulation of the argument tenantId can lead to sql injection. 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-2025-11315	CVE-2025-11315 - A vulnerability was found in Tipray 厦门天锐科技股份有限公司 Data Leakage Prevention	A vulnerability was found in Tipray 厦门天锐科技股份有限公司 Data Leakage Prevention System 天锐数	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System 天锐数据泄露防护系统 1.0. Affe...	据泄露防护系统 1.0. Affected by this vulnerability is the function findUserPage of the file findUserPage.do. Performing manipulation of the argument sort results in sql injection. 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.		
CVE-2025-11314	CVE-2025-11314 - A vulnerability has been found in Tipray 厦门天锐科技股份有限公司 Data Leakage Prevention System 天锐数据泄露防护系统 1.0....	A vulnerability has been found in Tipray 厦门天锐科技股份有限公司 Data Leakage Prevention System 天锐数据泄露防护系统 1.0. Affected is the function findRolePage of the file findSingConfigPage.do. Such manipulation of the argument sort leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-11313	CVE-2025-11313 - A flaw has been found in Tipray 厦门天锐科技股份有限公司 Data Leakage Prevention System 天锐数据泄露防护系统 1.0. This imp...	A flaw has been found in Tipray 厦门天锐科技股份有限公司 Data Leakage Prevention System 天锐数据泄露防护系统 1.0. This impacts the function findRolePage of the file findRolePage.do. This manipulation of the argument sort causes sql injection. 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-2025-11312	CVE-2025-11312 - A vulnerability was detected in Tipray 厦门天锐科技股份有限公司 Data Leakage Prevention System 天锐数据泄露防护系统 1.0. T...	A vulnerability was detected in Tipray 厦门天锐科技股份有限公司 Data Leakage Prevention System 天锐数据泄露防护系统 1.0. This affects the function findModulePage of the file findModulePage.do. The manipulation of the argument sort results in sql injection. The attack can be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		launched 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-2025-11311	CVE-2025-11311 - A security vulnerability has been detected in Tipray 厦门天锐科技股份有限公司 Data Leakage Prevention System 天锐数...	A security vulnerability has been detected in Tipray 厦门天锐科技股份有限公司 Data Leakage Prevention System 天锐数据泄露防护系统 1.0. The impacted element is the function findTenantPage of the file findTenantPage.do. The manipulation of the argument sort leads to sql injection. 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-2025-11310	CVE-2025-11310 - A weakness has been identified in Tipray 厦门天锐科技股份有限公司 Data Leakage Prevention System 天锐数据泄露防护系统 1.0....	A weakness has been identified in Tipray 厦门天锐科技股份有限公司 Data Leakage Prevention System 天锐数据泄露防护系统 1.0. The affected element is the function findFileServerPage of the file findFileServerPage.do. Executing manipulation of the argument sort can lead to sql injection. 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.	Patched by core rule	Y
CVE-2025-11309	CVE-2025-11309 - A security flaw has been discovered in Tipray 厦门天锐科技股份有限公司 Data Leakage Prevention System 天锐数据泄露防护系统...	A security flaw has been discovered in Tipray 厦门天锐科技股份有限公司 Data Leakage Prevention System 天锐数据泄露防护系统 1.0. Impacted is the function doFilter of the file findDeptPage.do. Performing manipulation of the argument sort results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		about this disclosure but did not respond in any way.		
CVE-2025-11303	CVE-2025-11303 - A vulnerability was detected in Belkin F9K1015 1.00.10. Affected is an unknown function of the file ...	A vulnerability was detected in Belkin F9K1015 1.00.10. Affected is an unknown function of the file /goform/mp. Performing manipulation of the argument command results in command injection. The attack may be initiated 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.	Patched by core rule	Y
CVE-2025-11298	CVE-2025-11298 - A vulnerability was determined in Belkin F9K1015 1.00.10. Impacted is an unknown function of the fil...	A vulnerability was determined in Belkin F9K1015 1.00.10. Impacted is an unknown function of the file /goform/formSetWanStatic. Executing manipulation of the argument m_wan_ipaddr can lead to command injection. The attack may be performed from remote. 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-2025-11292	CVE-2025-11292 - A weakness has been identified in Belkin F9K1015 1.00.10. Affected is an unknown function of the fil...	A weakness has been identified in Belkin F9K1015 1.00.10. Affected is an unknown function of the file /goform/formBSSetSitesurvey. Executing manipulation of the argument wan_ipaddr can lead to 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-2025-11288	CVE-2025-11288 - A security flaw has been discovered in CRMEB up to 5.6. This issue affects some unknown processing o...	A security flaw has been discovered in CRMEB up to 5.6. This issue affects some unknown processing of the file /adminapi/product/product of the component GET Parameter Handler. Performing manipulation of the argument cate_id results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited. The vendor was contacted early	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		about this disclosure but did not respond in any way.		
CVE-2025-9199	CVE-2025-9199 - The Woo superb slideshow transition gallery with random effect plugin for WordPress is vulnerable to...	The Woo superb slideshow transition gallery with random effect plugin for WordPress is vulnerable to SQL Injection via the 'woo-superb-slideshow' shortcode in all versions up to, and including, 9.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-9198	CVE-2025-9198 - The Wp cycle text announcement plugin for WordPress is vulnerable to SQL Injection via the 'cycle-te...	The Wp cycle text announcement plugin for WordPress is vulnerable to SQL Injection via the 'cycle-text' shortcode in all versions up to, and including, 8.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-10726	CVE-2025-10726 - The WPRecovery plugin for WordPress is vulnerable to SQL Injection via the 'data[id]' parameter in a...	The WPRecovery plugin for WordPress is vulnerable to SQL Injection via the 'data[id]' parameter in all versions up to, and including, 2.0. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Additionally, the result of this SQL injection is passed directly to PHP's unlink() function, allowing attackers to delete arbitrary files on the server by injecting file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		paths through the SQL query.		
CVE-2025-10582	CVE-2025-10582 - The WP Dispatcher plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter in all ...	The WP Dispatcher plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter in all versions up to, and including, 1.2.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-56162	CVE-2025-56162 - YOSHOP 2.0 suffers from an unauthenticated SQL injection in the goodsIds parameter of the /api/goods...	YOSHOP 2.0 suffers from an unauthenticated SQL injection in the goodsIds parameter of the /api/goods/listByIds endpoint. The getListByIds function concatenates user input into orderRaw('field(goods_id, ...)'), allowing attackers to: (a) enumerate or modify database data, including dumping admin password hashes; (b) write web-shell files or invoke xp_cmdshell, leading to remote code execution on servers configured with sufficient DB privileges.	Patched by core rule	Y
CVE-2025-61096	CVE-2025-61096 - PHPGurukul Online Shopping Portal Project v2.1 is vulnerable to SQL Injection in /shopping/login.php...	PHPGurukul Online Shopping Portal Project v2.1 is vulnerable to SQL Injection in /shopping/login.php via the fullname parameter.	Patched by core rule	Y
CVE-2025-56381	CVE-2025-56381 - ERPNEXT v15.67.0 was discovered to contain multiple SQL injection vulnerabilities in the /api/method...	ERPNEXT v15.67.0 was discovered to contain multiple SQL injection vulnerabilities in the /api/method/frappe.desk.reportview.get endpoint via the order_by and group_by parameters.	Patched by core rule	Y
CVE-2025-56380	CVE-2025-56380 - Frappe Framework v15.72.4 was discovered to contain a SQL injection vulnerability via the fieldname ...	Frappe Framework v15.72.4 was discovered to contain a SQL injection vulnerability via the fieldname parameter in the frappe.client.get_value API endpoint and a crafted script to the fieldname parameter	Patched by core rule	Y
CVE-2025-52042	CVE-2025-52042 - In Frappe ERPNext 15.57.5, the function	In Frappe ERPNext 15.57.5, the function get_rfq_containing_supplier(	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	get_rfq_containing_supplier() at erpnext/buying/doctype/requ...	) at erpnext/buying/doctype/request_for_quotation/request_for_quotation.py is vulnerable to SQL Injection, which allows an attacker to extract all information from databases by injecting SQL query via the txt parameter.		
CVE-2025-52041	CVE-2025-52041 - In Frappe ERPNext 15.57.5, the function get_stock_balance_for() at erpnext/stock/doctype/stock_recon...	In Frappe ERPNext 15.57.5, the function get_stock_balance_for() at erpnext/stock/doctype/stock_reconciliation/stock_reconciliation.py is vulnerable to SQL Injection, which allows an attacker to extract all information from databases by injecting a SQL query into the inventory_dimensions_dict parameter.	Patched by core rule	Y
CVE-2025-52040	CVE-2025-52040 - In Frappe ERPNext 15.57.5, the function get_blanket_orders() at erpnext/controllers/queries.py is vu...	In Frappe ERPNext 15.57.5, the function get_blanket_orders() at erpnext/controllers/queries.py is vulnerable to SQL Injection, which allows an attacker can extract all information from databases by injecting a SQL query into the blanket_order_type parameter.	Patched by core rule	Y
CVE-2025-52039	CVE-2025-52039 - In Frappe ERPNext 15.57.5, the function get_material_requests_based_on_supplier() at erpnext/stock/d...	In Frappe ERPNext 15.57.5, the function get_material_requests_based_on_supplier() at erpnext/stock/doctype/material_request/material_request.py is vulnerable to SQL Injection, which allows an attacker to extract all information from databases by injecting a SQL query into the txt parameter.	Patched by core rule	Y
CVE-2025-57254	CVE-2025-57254 - An SQL injection vulnerability in user-login.php and index.php of Karthikg1908 Hospital Management S...	An SQL injection vulnerability in user-login.php and index.php of Karthikg1908 Hospital Management System (HMS) 1.0 allows remote attackers to execute arbitrary SQL queries via the username and password POST parameters. The application fails to properly sanitize input before embedding it into SQL queries, leading to unauthorized access or potential data breaches. This can result in privilege escalation, account takeover, or exposure of sensitive medical data.	Patched by core rule	Y
CVE-2025-52050	CVE-2025-52050 - In	In Frappe ERPNext 15.57.5,	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Frappe ERPNext 15.57.5, the function get_loyalty_program_details_with_points() at erpnext/account...	the function get_loyalty_program_details_with_points() at erpnext/accounts/doctype/loyalty_program/loyalty_program.py is vulnerable to SQL Injection, which allows an attacker to extract all information from databases by injecting a SQL query into the expiry_date parameter.	rule	
CVE-2025-52049	CVE-2025-52049 - In Frappe ErpNext v15.57.5, the function get_timesheet_detail_rate() at erpnext/projects/doctype/tim...	In Frappe ErpNext v15.57.5, the function get_timesheet_detail_rate() at erpnext/projects/doctype/timesheet/timesheet.py is vulnerable to SQL Injection, which allows an attacker to extract all information from databases by injecting SQL query into the timelog parameter.	Patched by core rule	Y
CVE-2025-52047	CVE-2025-52047 - In Frappe ErpNext v15.57.5, the function get_income_account() at erpnext/controllers/queries.py is v...	In Frappe ErpNext v15.57.5, the function get_income_account() at erpnext/controllers/queries.py is vulnerable to SQL Injection, which allows an attacker to extract all information from databases by injecting a SQL query into the filters.disabled parameter.	Patched by core rule	Y
CVE-2025-52043	CVE-2025-52043 - In Frappe ERPNext v15.57.5, the function import_coa() at erpnext/accounts/doctype/chart_of_accounts_...	In Frappe ERPNext v15.57.5, the function import_coa() at erpnext/accounts/doctype/chart_of_accounts_importer/chart_of_accounts_importer.py is vulnerable to SQL injection, which allows an attacker to extract all information from databases by injecting a SQL query into the company parameter.	Patched by core rule	Y
CVE-2025-11121	CVE-2025-11121 - A security vulnerability has been detected in Tenda AC18 15.03.05.19. The impacted element is an unk...	A security vulnerability has been detected in Tenda AC18 15.03.05.19. The impacted element is an unknown function of the file /goform/AdvSetLanip. The manipulation of the argument lanIp leads to command injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2025-11100	CVE-2025-11100 - A vulnerability was identified in D-Link DIR-823X 250416. This affects the function uci_set of the f...	A vulnerability was identified in D-Link DIR-823X 250416. This affects the function uci_set of the file /goform/set_wifi_blacklists. Such manipulation leads to command injection. It is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		possible to launch the attack remotely. The exploit is publicly available and might be used.		
CVE-2025-11099	CVE-2025-11099 - A vulnerability was determined in D-Link DIR-823X 250416. The impacted element is the function uci_d...	A vulnerability was determined in D-Link DIR-823X 250416. The impacted element is the function uci_del of the file /goform/delete_prohibiting. This manipulation of the argument delvalue causes command injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-11098	CVE-2025-11098 - A vulnerability was found in D-Link DIR-823X 250416. The affected element is an unknown function of ...	A vulnerability was found in D-Link DIR-823X 250416. The affected element is an unknown function of the file /goform/set_wifi_blacklists. The manipulation of the argument macList results in command injection. The attack may be performed from remote. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2025-11097	CVE-2025-11097 - A vulnerability has been found in D-Link DIR-823X 250416. Impacted is an unknown function of the fil...	A vulnerability has been found in D-Link DIR-823X 250416. Impacted is an unknown function of the file /goform/set_device_name. The manipulation of the argument mac leads to command injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-11096	CVE-2025-11096 - A flaw has been found in D-Link DIR-823X 250416. This issue affects some unknown processing of the f...	A flaw has been found in D-Link DIR-823X 250416. This issue affects some unknown processing of the file /goform/diag_traceroute. Executing manipulation of the argument target_addr can lead to command injection. The attack can be executed remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2025-11095	CVE-2025-11095 - A vulnerability was detected in D-Link DIR-823X 250416. This vulnerability affects unknown code of t...	A vulnerability was detected in D-Link DIR-823X 250416. This vulnerability affects unknown code of the file /goform/delete_offline_device. Performing manipulation of the argument delvalue results in command injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-11074	CVE-2025-11074 - A flaw has been found in code-projects Project Monitoring System 1.0. The impacted element is an unk...	A flaw has been found in code-projects Project Monitoring System 1.0. The impacted element is an unknown function of the file /login.php. This manipulation of the argument username/password causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2025-11073	CVE-2025-11073 - A vulnerability was detected in Keyfactor RG-EW5100BE EW_3.0B11P280_EW5100BE-PRO_12183019. The affec...	A vulnerability was detected in Keyfactor RG-EW5100BE EW_3.0B11P280_EW5100BE-PRO_12183019. The affected element is an unknown function of the file /cgi-bin/luci/api/cmd of the component HTTP POST Request Handler. The manipulation of the argument url results in command injection. The attack can be launched remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-11066	CVE-2025-11066 - A flaw has been found in code-projects Online Bidding System 1.0. This impacts an unknown function o...	A flaw has been found in code-projects Online Bidding System 1.0. This impacts an unknown function of the file /administrator/bidlist.php. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2025-11037	CVE-2025-11037 - A security flaw has been discovered in code-projects E-Commerce Website 1.0. This impacts an unknown...	A security flaw has been discovered in code-projects E-Commerce Website 1.0. This impacts an unknown function of the file /pages/admin_index_search.php. Performing manipulation of the argument Search results in sql injection. The attack may be initiated remotely. The exploit has been released to the public and may be exploited.	Patched by core rule	Y
CVE-2025-11036	CVE-2025-11036 - A vulnerability was identified in code-projects E-Commerce Website 1.0. This affects an unknown func...	A vulnerability was identified in code-projects E-Commerce Website 1.0. This affects an unknown function of the file /pages/admin_account_update.php. Such manipulation of the argument user_id leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		be used.		
CVE-2025-60118	CVE-2025-60118 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i...	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Potenzaglobalsolutions PGS Core allows SQL Injection. This issue affects PGS Core: from n/a through 5.9.0.	Patched by core rule	Y
CVE-2025-60110	CVE-2025-60110 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i...	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup AllInOne - Banner Rotator allows SQL Injection. This issue affects AllInOne - Banner Rotator: from n/a through 3.8.	Patched by core rule	Y
CVE-2025-60109	CVE-2025-60109 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i...	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup LambertGroup - AllInOne - Content Slider allows Blind SQL Injection. This issue affects LambertGroup - AllInOne - Content Slider: from n/a through 3.8.	Patched by core rule	Y
CVE-2025-60108	CVE-2025-60108 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i...	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup LambertGroup - AllInOne - Banner with Thumbnails allows Blind SQL Injection. This issue affects LambertGroup - AllInOne - Banner with Thumbnails: from n/a through 3.8.	Patched by core rule	Y
CVE-2025-60107	CVE-2025-60107 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i...	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup LambertGroup - AllInOne - Banner with Playlist allows Blind SQL Injection. This issue affects LambertGroup - AllInOne - Banner with Playlist: from n/a through 3.8.	Patched by core rule	Y

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-55757	CVE-2025-55757 - A unauthenticated reflected XSS vulnerability in VirtueMart 1.0.0-4.4.10 for Joomla was discovered.	A unauthenticated reflected XSS vulnerability in VirtueMart 1.0.0-4.4.10 for Joomla was discovered.	Patched by core rule	Y
CVE-2025-12034	CVE-2025-12034 - The Fast Velocity Minify plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin...	The Fast Velocity Minify plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.5.1 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-2025-11875	CVE-2025-11875 - The SpendeOnline.org plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugi...	The SpendeOnline.org plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'spendeonline' shortcode in all versions up to, and including, 3.0.1 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-2025-10580	CVE-2025-10580 - The Widget Options – The #1 WordPress Widget & Block Control Plugin plugin for WordPress is vulnerab...	The Widget Options – The #1 WordPress Widget & Block Control Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple functions in all versions up to, and including, 4.1.2 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-8666	CVE-2025-8666 - The Testimonial Carousel For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scrip...	The Testimonial Carousel For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple parameters in versions less than, or equal to, 11.6.2 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-2025-8588	CVE-2025-8588 - The Gutenberg Blocks – PublishPress Blocks plugin for WordPress is vulnerable to Stored Cross-Site S...	The Gutenberg Blocks – PublishPress Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Marker Title' and 'Marker Description' parameters for the Maps block in versions up to, and including, 3.3.4 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-2025-11238	CVE-2025-11238 - The Watu Quiz plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the HTTP Referer...	The Watu Quiz plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the HTTP Referer header in versions less than, or equal to, 3.4.4 due to insufficient input sanitization and output escaping when the "Save source URL" option is enabled. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever an user accesses an injected page.	Patched by core rule	Y
CVE-2025-12096	CVE-2025-12096 - The Simple Excel Pricelist for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site S...	The Simple Excel Pricelist for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'pricelist' shortcode in all versions up to, and including, 1.13 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		pages that will execute whenever a user accesses an injected page.		
CVE-2025-10701	CVE-2025-10701 - The Time Clock – A WordPress Employee & Volunteer Time Clock Plugin for WordPress is vulnerable to S...	The Time Clock – A WordPress Employee & Volunteer Time Clock Plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'data' parameter in all versions up to, and including, 1.3.1. This is due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with Time Clock user credentials to inject arbitrary web scripts in pages that will execute whenever a user accesses an affected page.	Patched by core rule	Y
CVE-2025-7730	CVE-2025-7730 - The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘per...	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘percentage’ parameter in all versions up to, and including, 5.4.5 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-2025-62255	CVE-2025-62255 - Self Cross-site scripting (XSS) vulnerability on the edit Knowledge Base article page in Liferay Por...	Self Cross-site scripting (XSS) vulnerability on the edit Knowledge Base article page in Liferay Portal 7.4.0 through 7.4.3.101, and older unsupported versions, and Liferay DXP 2023.Q3.1 through 2023.Q3.5, 7.4 GA through update 92, and older unsupported versions allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into an attachment's filename.	Patched by core rule	Y
CVE-2025-60837	CVE-2025-60837 - A reflected cross-site scripting (XSS) vulnerability in MCMS v6.0.1 allows attackers to execute arbi...	A reflected cross-site scripting (XSS) vulnerability in MCMS v6.0.1 allows attackers to execute arbitrary Javascript in the context of a user's browser via a crafted payload.	Patched by core rule	Y
CVE-2025-61413	CVE-2025-61413 - A stored cross-site scripting (XSS) vulnerability in the /manager/pages component of Piranha	A stored cross-site scripting (XSS) vulnerability in the /manager/pages component of Piranha CMS v12.0 allows attackers to execute	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	CMS v12...	arbitrary web scripts or HTML via creating a page and injecting a crafted payload into the Markdown blocks.		
CVE-2025-62248	CVE-2025-62248 - A reflected cross-site scripting (XSS) vulnerability, resulting from a regression, has been identif...	A reflected cross-site scripting (XSS) vulnerability, resulting from a regression, has been identified in Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.9, 2025.Q1.0 through 2025.Q1.16, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.1 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.19 allows a remote, authenticated attacker to inject and execute JavaScript code via the _com_liferay_dynamic_data_mapping_web_portlet_DDMPortlet_definition parameter. The malicious payload is executed within the victim's browser when they access a URL that includes the crafted parameter.	Patched by core rule	Y
CVE-2025-11883	CVE-2025-11883 - The Responsive Progress Bar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via th...	The Responsive Progress Bar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's rprogress shortcode in versions less than, or equal to, 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-2025-11880	CVE-2025-11880 - The SM CountDown Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the pl...	The SM CountDown Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's smcountdown shortcode in versions less than, or equal to, 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		injected page.		
CVE-2025-11878	CVE-2025-11878 - The ST Categories Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the p...	The ST Categories Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's st-categories shortcode in versions less than, or equal to, 1.0.0. 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-2025-11872	CVE-2025-11872 - The Material Design Iconic Font Integration plugin for WordPress is vulnerable to Stored Cross-Site ...	The Material Design Iconic Font Integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'mdiconic' shortcode in all versions up to, and including, 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-2025-11870	CVE-2025-11870 - The Simple Business Data plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'simp...	The Simple Business Data plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'simple_business_data' shortcode attributes in all versions up to, and including, 1.0.1. This is due to the plugin not properly sanitizing user input or escaping output when embedding the `type` attribute into the `class` attribute in rendered HTML. 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-2025-11867	CVE-2025-11867 - The Bg Book Publisher plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `boo...	The Bg Book Publisher plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `book_author` post meta, rendered through the `[book_author]` shortcode, in all versions up to, and including, 1.25. This is due to the plugin not properly	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		escaping the meta value before output. 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-2025-11866	CVE-2025-11866 - The Photographers galleries plugin for WordPress is vulnerable to Stored Cross-Site Scripting via mu...	The Photographers galleries plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple shortcode attributes (`w`, `h`, `raw_css`, `look`, etc.) in all versions up to, and including, 1.1.8. This is due to the plugin not properly sanitizing user input or escaping output when inserting these values into HTML attributes and inline styles. 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-2025-11834	CVE-2025-11834 - The WP AD Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'startin...	The WP AD Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'startindex' parameter of the ad-gallery shortcode in all versions up to, and including, 1.3. This is 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-2025-11830	CVE-2025-11830 - The WP Restaurant Listings plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the...	The WP Restaurant Listings plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'align' parameter of the restaurant_summary shortcode in all versions up to, and including, 1.0.2. This is 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-2025-11827	CVE-2025-11827 - The	The Oboxmedia Ads plugin	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Oboxmedia Ads plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'before_...	for WordPress is vulnerable to Stored Cross-Site Scripting via the 'before_widget' and 'after_widget' parameters of the oboxads-ad-widget shortcode in all versions up to, and including, 1.9.8. This is 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-2025-11825	CVE-2025-11825 - The Playerzbr plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'urlmeta' po...	The Playerzbr plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'urlmeta' post meta field in all versions up to, and including, 1.6 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-2025-11824	CVE-2025-11824 - The Cinza Grid plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'cgrid_skin...	The Cinza Grid plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'cgrid_skin_content' post meta field in all versions up to, and including, 1.2.1 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-2025-11819	CVE-2025-11819 - The WP-Thumbnail plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'roboshot...	The WP-Thumbnail plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'roboshot' shortcode in all versions up to, and including, 1.1. 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-2025-11818	CVE-2025-11818 - The	The WP Responsive Meet	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	WP Responsive Meet The Team plugin for WordPress is vulnerable to Stored Cross-Site Scripting vi...	The Team plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wprm_team' shortcode in all versions up to, and including, 1.0.1. 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.	rule	
CVE-2025-11817	CVE-2025-11817 - The Simple Tableau Viz plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ta...	The Simple Tableau Viz plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tableau' shortcode in all versions up to, and including, 2.0. 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-2025-11813	CVE-2025-11813 - The Responsive iframe GoogleMap plugin for WordPress is vulnerable to Stored Cross-Site Scripting vi...	The Responsive iframe GoogleMap plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'responsive_map' shortcode in all versions up to, and including, 1.0.2. This is due to insufficient input sanitization and output escaping on the 'width' and 'height' 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-2025-11811	CVE-2025-11811 - The Simple Youtube Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via t...	The Simple Youtube Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'embed_youtube' shortcode in all versions up to, and including, 1.1.3. This is due to insufficient input sanitization and output escaping on the 'id' attribute. 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-2025-11810	CVE-2025-11810 - The Print Button Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the...	The Print Button Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'print-button' shortcode in all versions up to, and including, 1.0.1. This is due to insufficient input sanitization and output escaping on the 'target' attribute. 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-2025-11809	CVE-2025-11809 - The WP-Force Images Download plugin for WordPress is vulnerable to Stored Cross-Site Scripting via t...	The WP-Force Images Download plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpfid' shortcode in all versions up to, and including, 1.8. This is due to insufficient input sanitization and output escaping on the 'class' attribute. 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-2025-11807	CVE-2025-11807 - The Mixlr Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'mixlr...	The Mixlr Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'mixlr' shortcode in all versions up to, and including, 1.0.1. This is due to insufficient input sanitization and output escaping on the 'url' attribute. 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-2025-11804	CVE-2025-11804 - The JB News Ticker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' sh...	The JB News Ticker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' shortcode attribute of the 'jbticker' shortcode in all versions up to, and including, 1.0. This is due to insufficient input sanitization and output	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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.		
CVE-2025-10138	CVE-2025-10138 - The This-or-That plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's ...	The This-or-That plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'thisorthat' shortcode in all versions up to, and including, 1.0.4 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-2025-12033	CVE-2025-12033 - The Simple Banner – Easily add multiple Banners/Bars/Notifications/Announcements to the top or botto...	The Simple Banner – Easily add multiple Banners/Bars/Notifications/Announcements to the top or bottom of your website plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'pro_version_activation_code' parameter in all versions up to, and including, 3.0.10 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-2025-10651	CVE-2025-10651 - The Welcart e-Commerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'or...	The Welcart e-Commerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'order_mail' setting in versions up to, and including, 2.11.22. This is due to insufficient sanitization on the order_mail field and a lack of escaping on output. This makes it possible for authenticated attackers, with Editor-level permissions and above, to inject arbitrary web scripts via the General	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Setting page that will execute when an administrator accesses the E-mail Setting page.		
CVE-2025-62249	CVE-2025-62249 - A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, ...	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q3.0 through 2025.Q3.2, 2025.Q2.0 through 2025.Q2.12, 2025.Q1.0 through 2025.Q1.17, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.20, and 2023.Q4.0 through 2023.Q4.10 allows an remote non-authenticated attacker to inject JavaScript into the google_gadget.	Patched by core rule	Y
CVE-2025-61457	CVE-2025-61457 - code16 Sharp v9.6.6 is vulnerable to Cross Site Scripting (XSS) src/Form/Fields/SharpFormUploadField...	code16 Sharp v9.6.6 is vulnerable to Cross Site Scripting (XSS) src/Form/Fields/SharpFormUploadField.php.	Patched by core rule	Y
CVE-2025-61255	CVE-2025-61255 - Bank Locker Management System by PHPGurukul is affected by a Cross-Site Scripting (XSS) vulnerabilit...	Bank Locker Management System by PHPGurukul is affected by a Cross-Site Scripting (XSS) vulnerability via the /search parameter, where unsanitized input allows arbitrary HTML and JavaScript injection, potentially resulting in information disclosure and user redirection.	Patched by core rule	Y
CVE-2025-60280	CVE-2025-60280 - Cross-Site Scripting (XSS) vulnerability in Bang Resto v1.0 could allow an attacker to inject malici...	Cross-Site Scripting (XSS) vulnerability in Bang Resto v1.0 could allow an attacker to inject malicious JavaScript code into the application's web pages. This vulnerability exists due to insufficient input sanitization or output encoding, allowing attacker-controlled input to be rendered directly in the browser. When exploited, an attacker can steal session cookies, redirect users to malicious sites, perform actions on behalf of the user, or deface the website. This can lead to user data compromise, loss of user trust, and a broader attack surface for more advanced exploitation techniques.	Patched by core rule	Y
CVE-2025-61456	CVE-2025-61456 - A Cross-Site Scripting (XSS)	A Cross-Site Scripting (XSS) vulnerability exists in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	vulnerability exists in Bhabishya-123 E-commerce 1.0, specifically with...	Bhabishya-123 E-commerce 1.0, specifically within the index endpoint. Unsanitized input in the /index parameter is directly reflected back into the response HTML, allowing attackers to execute arbitrary JavaScript in the browser of a user who visits a malicious link or submits a crafted request.		
CVE-2025-61417	CVE-2025-61417 - Cross-Site Scripting (XSS) vulnerability exists in TastyIgniter 3.7.7, affecting the /admin/media_ma...	Cross-Site Scripting (XSS) vulnerability exists in TastyIgniter 3.7.7, affecting the /admin/media_manager component. Attackers can upload a malicious SVG file containing JavaScript code. When an administrator previews the file, the code executes in their browser context, allowing the attacker to perform unauthorized actions such as modifying the admin account credentials.	Patched by core rule	Y
CVE-2025-61454	CVE-2025-61454 - A Cross-Site Scripting (XSS) vulnerability exists in Bhabishya-123 E-commerce 1.0, specifically with...	A Cross-Site Scripting (XSS) vulnerability exists in Bhabishya-123 E-commerce 1.0, specifically within the search endpoint. Unsanitized input in the /search parameter is directly reflected back into the response HTML, allowing attackers to execute arbitrary JavaScript in the browser of a user who visits a malicious link or submits a crafted request.	Patched by core rule	Y
CVE-2025-11946	CVE-2025-11946 - A security flaw has been discovered in LogicalDOC Community Edition up to 9.2.1. This issue affects ...	A security flaw has been discovered in LogicalDOC Community Edition up to 9.2.1. This issue affects some unknown processing of the file /frontend.jsp of the component Add Contact Page. Performing manipulation of the argument First Name/Last Name/Company/Address/Phone/Mobile results in cross site scripting. Remote exploitation of the attack is possible. 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-2025-11926	CVE-2025-11926 - The Related Posts Lite plugin for WordPress is vulnerable to Stored	The Related Posts Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Cross-Site Scripting via admin s...	versions up to, and including, 1.12 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.		
CVE-2025-9562	CVE-2025-9562 - The Redirection for Contact Form 7 plugin for WordPress is vulnerable to Stored Cross-Site Scripting...	The Redirection for Contact Form 7 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's qs_date shortcode in all versions up to, and including, 3.2.6 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-2025-11270	CVE-2025-11270 - The Gutenberg Essential Blocks – Page Builder for Gutenberg Blocks & Patterns plugin for WordPress i...	The Gutenberg Essential Blocks – Page Builder for Gutenberg Blocks & Patterns plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'titleTag' attribute in all versions up to, and including, 5.7.1 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-2025-11857	CVE-2025-11857 - The XX2WP Integration Tools plugin for WordPress is vulnerable to Stored Cross-Site Scripting via th...	The XX2WP Integration Tools plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'mxp_fb2wp_display_embed' shortcode in all versions up to, and including, 1.9.9. This is due to the plugin not properly sanitizing user input and output of the 'post_id' parameter. This makes it possible for authenticated attackers, with contributor-level access	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2020-36853	CVE-2020-36853 - The 10WebMapBuilder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Plugin Set...	The 10WebMapBuilder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Plugin Settings Change in versions up to, and including, 1.0.63 due to insufficient input sanitization and output escaping and a lack of capability checks. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-61539	CVE-2025-61539 - Cross site scripting (XSS) vulnerability in Ultimate PHP Board 2.2.7 via the u_name parameter in los...	Cross site scripting (XSS) vulnerability in Ultimate PHP Board 2.2.7 via the u_name parameter in lostpassword.php.	Patched by core rule	Y
CVE-2025-11814	CVE-2025-11814 - The Ultimate Addons for WPBakery plugin for WordPress is vulnerable to Stored Cross-Site Scripting i...	The Ultimate Addons for WPBakery plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to 3.21.1 (exclusive) due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-10194	CVE-2025-10194 - The Shortcode Button plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugi...	The Shortcode Button plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'button' 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-2025-10141	CVE-2025-10141 - The Digiseller plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'd...	The Digiseller plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ds' shortcode in all versions up to, and including, 1.3.0 due to insufficient input sanitization and output	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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-2025-10140	CVE-2025-10140 - The Quick Social Login plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plu...	The Quick Social Login plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'quick-login' shortcode in all versions up to, and including, 1.4.6 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-2025-10139	CVE-2025-10139 - The WP BookWidgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin'...	The WP BookWidgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'bw_link' shortcode in all versions up to, and including, 0.9 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-2025-10133	CVE-2025-10133 - The URLYar URL Shortner plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the pl...	The URLYar URL Shortner plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'urlyar_shortlink' shortcode in all versions up to, and including, 1.1.0 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-2025-10132	CVE-2025-10132 - The Dhivehi Text plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's ...	The Dhivehi Text plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'dhivehi' shortcode in all versions up to, and including, 0.1 due to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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-2025-60374	CVE-2025-60374 - Stored Cross-Site Scripting (XSS) in Perfex CRM chatbot before 3.3.1 allows attackers to inject arbi...	Stored Cross-Site Scripting (XSS) in Perfex CRM chatbot before 3.3.1 allows attackers to inject arbitrary HTML/JavaScript. The payload is executed in the browsers of users viewing the chat, resulting in client-side code execution, potential session token theft, and other malicious actions. A different vulnerability than CVE-2024-8867.	Patched by core rule	Y
CVE-2025-62246	CVE-2025-62246 - Multiple stored cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.4.0 through 7.4.3.111...	Multiple stored cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, 7.4 GA through update 92, and older unsupported versions allow remote authenticated users to inject arbitrary web script or HTML via a crafted payload injected into a user's first, middle or last name text field to (1) page comments widget, (2) blog entry comments, (3) document and media document comments, (4) message board messages, (5) wiki page comments or (6) other widgets/apps that supports mentions.	Patched by core rule	Y
CVE-2025-10190	CVE-2025-10190 - The WP Easy Toggles plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin...	The WP Easy Toggles plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'toggles' shortcode in all versions up to, and including, 1.9.0 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-10167	CVE-2025-10167 - The Stock History & Reports Manager for WooCommerce plugin for WordPress is vulnerable to Stored Cro...	The Stock History & Reports Manager for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'alg_wc_stock_snapshot_restocked shortcode in all versions up to, and including, 2.2.1 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-2025-10129	CVE-2025-10129 - The WordPress Live Webcam Widget & Shortcode plugin for WordPress is vulnerable to Stored Cross-Site...	The WordPress Live Webcam Widget & Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'webcam' shortcode in all versions up to, and including, 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-2025-9496	CVE-2025-9496 - The Enable Media Replace plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the p...	The Enable Media Replace plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file_modified shortcode in all versions up to, and including, 4.1.6 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-2025-11197	CVE-2025-11197 - 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, 2.6.1 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-2025-9560	CVE-2025-9560 - The Colibri Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the p...	The Colibri Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's colibri_newsletter shortcode in all versions up to, and including, 1.0.334 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-2025-60880	CVE-2025-60880 - An authenticated stored XSS vulnerability exists in the Bagisto 2.3.6 admin panel's product creation...	An authenticated stored XSS vulnerability exists in the Bagisto 2.3.6 admin panel's product creation path, allowing an attacker to upload a crafted SVG file containing malicious JavaScript code. This vulnerability can be exploited by an authenticated admin user to execute arbitrary JavaScript in the browser, potentially leading to session hijacking, data theft, or unauthorized actions.	Patched by core rule	Y
CVE-2025-60308	CVE-2025-60308 - code-projects Simple Online Hotel Reservation System 1.0 has a Cross Site Scripting (XSS) vulnerabil...	code-projects Simple Online Hotel Reservation System 1.0 has a Cross Site Scripting (XSS) vulnerability in the Add Room function of the online hotel reservation system. Malicious JavaScript code is entered in the Description field, which can leak the administrator's cookie information when browsing this room information	Patched by core rule	Y
CVE-2025-60869	CVE-2025-60869 - Publii CMS v0.46.5 (build 17089) allows persistent Cross-Site Scripting (XSS) via unsanitized input ...	Publii CMS v0.46.5 (build 17089) allows persistent Cross-Site Scripting (XSS) via unsanitized input in configuration fields such as "Site Description" and "Footer Follow Buttons". An attacker can inject arbitrary JavaScript, which is stored in the project and executed in the browsers of remote visitors viewing the generated static site.	Patched by core rule	Y
CVE-2025-60378	CVE-2025-60378 - Stored	Stored HTML injection in	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	HTML injection in RISE Ultimate Project Manager & CRM allows authenticated users to inject ar...	RISE Ultimate Project Manager & CRM allows authenticated users to inject arbitrary HTML into invoices and messages. Injected content renders in emails, PDFs, and messaging/chat modules sent to clients or team members, enabling phishing, credential theft, and business email compromise. Automated recurring invoices and messaging amplify the risk by distributing malicious content to multiple recipients.	rule	
CVE-2025-61319	CVE-2025-61319 - ReNgine thru 2.2.0 is vulnerable to a Stored Cross-Site Scripting (XSS) vulnerability in the Vulnera...	ReNgine thru 2.2.0 is vulnerable to a Stored Cross-Site Scripting (XSS) vulnerability in the Vulnerabilities module. When scanning a target with an XSS payload, the unsanitized payload is rendered in the ReNgine web UI, resulting in arbitrary JavaScript execution in the victim's browser. This can be abused to steal session cookies, perform unauthorized actions, or compromise the ReNgine administrator's account.	Patched by core rule	Y
CVE-2025-62239	CVE-2025-62239 - Cross-site scripting (XSS) vulnerability in workflow process builder in Liferay Portal 7.4.3.21 thro...	Cross-site scripting (XSS) vulnerability in workflow process builder in Liferay Portal 7.4.3.21 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, and 7.4 update 21 through update 92 allows remote authenticated attackers to inject arbitrary web script or HTML via the crafted input in a workflow definition.	Patched by core rule	Y
CVE-2025-62238	CVE-2025-62238 - Stored cross-site scripting (XSS) vulnerability on the Membership page in Account Settings in Lifera...	Stored cross-site scripting (XSS) vulnerability on the Membership page in Account Settings in Liferay Portal 7.4.3.21 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, and 7.4 update 21 through update 92 allows remote authenticated attackers to inject arbitrary web script or HTML via a crafted payload injected into a Account's “Name“ text field.	Patched by core rule	Y
CVE-2025-62237	CVE-2025-62237 - 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 Commerce's view order page in Liferay Portal 7.4....	(XSS) vulnerability in Commerce's view order page in Liferay Portal 7.4.3.8 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, and 7.4 update 8 through update 92 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into an Account's "Name" text field.	rule	
CVE-2025-62240	CVE-2025-62240 - Multiple cross-site scripting (XSS) vulnerabilities with Calendar events in Liferay Portal 7.4.3.35 ...	Multiple cross-site scripting (XSS) vulnerabilities with Calendar events in Liferay Portal 7.4.3.35 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.7, 7.4 update 35 through update 92, and 7.3 update 25 through update 36 allow remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a user's (1) First Name, (2) Middle Name or (3) Last Name text field.	Patched by core rule	Y
CVE-2025-60304	CVE-2025-60304 - code-projects Simple Scheduling System 1.0 is vulnerable to Cross Site Scripting (XSS) via the Subje...	code-projects Simple Scheduling System 1.0 is vulnerable to Cross Site Scripting (XSS) via the Subject Description field.	Patched by core rule	Y
CVE-2025-61532	CVE-2025-61532 - Cross Site Scripting vulnerability in SVX Portal v.2.7A to execute arbitrary code via the TG paramet...	Cross Site Scripting vulnerability in SVX Portal v.2.7A to execute arbitrary code via the TG parameter on last_heard_page.php component	Patched by core rule	Y
CVE-2025-60302	CVE-2025-60302 - code-projects Client Details System 1.0 is vulnerable to Cross Site Scripting (XSS). When adding cus...	code-projects Client Details System 1.0 is vulnerable to Cross Site Scripting (XSS). When adding customer information, the client details system fills in malicious JavaScript code in the username field.	Patched by core rule	Y
CVE-2025-56683	CVE-2025-56683 - A cross-site scripting (XSS) vulnerability in the component /app/marketplace.html of Logseq v0.10.9 ...	A cross-site scripting (XSS) vulnerability in the component /app/marketplace.html of Logseq v0.10.9 allows attackers to execute arbitrary code via injecting arbitrary Javascript into a crafted README.md file.	Patched by core rule	Y
CVE-2025-11485	CVE-2025-11485 - A vulnerability was determined in SourceCodester Student	A vulnerability was determined in SourceCodester Student Grades Management System	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Grades Management System 1.0. Affected is t...	1.0. Affected is the function add_user of the file /admin.php of the component Manage Users Page. This manipulation of the argument first_name/last_name causes cross site scripting. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.		
CVE-2025-60318	CVE-2025-60318 - SourceCodester Pet Grooming Management Software 1.0 is vulnerable to Cross Site Scripting (XSS) in /...	SourceCodester Pet Grooming Management Software 1.0 is vulnerable to Cross Site Scripting (XSS) in /admin/profile.php via the fname (First Name) and lname (Last Name) fields.	Patched by core rule	Y
CVE-2025-60313	CVE-2025-60313 - Sourcecodester Link Status Checker 1.0 is vulnerable to a Cross-Site Scripting (XSS) in the Enter UR...	Sourcecodester Link Status Checker 1.0 is vulnerable to a Cross-Site Scripting (XSS) in the Enter URLs to check input field. This allows a remote attacker to execute arbitrary code.	Patched by core rule	Y
CVE-2025-43771	CVE-2025-43771 - Multiple cross-site scripting (XSS) vulnerabilities in the Notifications widget in Liferay Portal 7....	Multiple cross-site scripting (XSS) vulnerabilities in the Notifications widget in Liferay Portal 7.4.3.102 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5 and 2023.Q3.1 through 2023.Q3.10 allow remote attackers to inject arbitrary web script or HTML via a crafted payload injected into (1) a user's "First Name" text field, (2) a user's "Middle Name" text field, (3) a user's "Last Name" text field, (4) the "Other Reason" text field when flagging content, or (5) the name of the flagged content.	Patched by core rule	Y
CVE-2025-61183	CVE-2025-61183 - Cross Site Scripting in vaahcms v.2.3.1 allows a remote attacker to execute arbitrary code via uploa...	Cross Site Scripting in vaahcms v.2.3.1 allows a remote attacker to execute arbitrary code via upload method in the storeAvatar() method of UserBase.php	Patched by core rule	Y
CVE-2025-60314	CVE-2025-60314 - Configuroweb Sistema Web de Inventario 1.0 is vulnerable to a Stored Cross-Site Scripting (XSS) due ...	Configuroweb Sistema Web de Inventario 1.0 is vulnerable to a Stored Cross-Site Scripting (XSS) due to the lack of input sanitization on the product name parameter (Nombre:Producto) allowing an authenticated attacker to inject malicious payloads and execute arbitrary JavaScript.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-43830	CVE-2025-43830 - Stored cross-site scripting (XSS) vulnerability in Forms in Liferay Portal 7.3.2 through 7.4.3.111, ...	Stored cross-site scripting (XSS) vulnerability in Forms in Liferay Portal 7.3.2 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, 7.4 GA through update 92, and 7.3 GA through update 35 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a form with a rich text type field.	Patched by core rule	Y
CVE-2025-43829	CVE-2025-43829 - Stored cross-site scripting (XSS) vulnerability in diagram type products in Commerce in Liferay Port...	Stored cross-site scripting (XSS) vulnerability in diagram type products in Commerce in Liferay Portal 7.4.3.18 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, and 7.4 update 18 through update 92 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a SVG file.	Patched by core rule	Y
CVE-2025-43821	CVE-2025-43821 - Cross-site scripting (XSS) vulnerability in the Commerce Product Comparison Table widget in Liferay ...	Cross-site scripting (XSS) vulnerability in the Commerce Product Comparison Table widget in Liferay Portal 7.4.0 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, and 7.4 GA through update 92 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a Commerce Product's Name text field.	Patched by core rule	Y
CVE-2025-11433	CVE-2025-11433 - A security flaw has been discovered in itsourcecode Leave Management System 1.0. This impacts the fu...	A security flaw has been discovered in itsourcecode Leave Management System 1.0. This impacts the function redirect of the file /module/employee/controller.php?action=reset of the component Query Parameter Handler. Performing manipulation of the argument ID results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited.	Patched by core rule	Y
CVE-2025-43822	CVE-2025-43822 - Multiple stored cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.4.3.15 through	Multiple stored cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.4.3.15 through 7.4.3.111, and Liferay DXP 2023.Q4.0	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	7.4.3....	through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, and 7.4 update 15 through update 92 allow remote attackers to inject arbitrary web script or HTML via crafted payload injected into a Terms and Condition's Name text field to (1) Payment Terms, or (2) the Delivery Term on the view order page.		
CVE-2025-43823	CVE-2025-43823 - Cross-site scripting (XSS) vulnerability in the Commerce Search Result widget in Liferay Portal 7.4....	Cross-site scripting (XSS) vulnerability in the Commerce Search Result widget in Liferay Portal 7.4.0 through 7.4.3.111, and Liferay DXP 2023.Q4 before patch 6, 2023.Q3 before patch 9, and 7.4 GA through update 92 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a Commerce Product's Name text field.	Patched by core rule	Y
CVE-2025-56243	CVE-2025-56243 - A Cross-Site Scripting (XSS) vulnerability was found in the register.php page of PuneethReddyHC Even...	A Cross-Site Scripting (XSS) vulnerability was found in the register.php page of PuneethReddyHC Event Management System 1.0, where the event_id GET parameter is improperly handled. An attacker can craft a malicious URL to execute arbitrary JavaScript in the victim s browser by injecting code into this parameter.	Patched by core rule	Y
CVE-2025-60312	CVE-2025-60312 - Sourcecodester Markdown to HTML Converter v1.0 is vulnerable to a Cross-Site Scripting (XSS) in the ...	Sourcecodester Markdown to HTML Converter v1.0 is vulnerable to a Cross-Site Scripting (XSS) in the "Markdown Input" field, allowing a remote attacker to inject arbitrary HTML/JavaScript code that executes in the victim's browser upon clicking the "Convert to HTML" button.	Patched by core rule	Y
CVE-2025-7400	CVE-2025-7400 - The Featured Image from URL (FIFU) plugin for WordPress is vulnerable to Stored Cross-Site Scripting...	The Featured Image from URL (FIFU) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via a post's Featured Image custom fields in all versions up to, and including, 5.2.7 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		whenever a user accesses an injected page. NOTE: This vulnerability was partially fixed in version 5.2.2.		
CVE-2025-43824	CVE-2025-43824 - The Profile widget in Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Li...	The Profile widget in Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, 7.4 GA through update 92, and older unsupported versions uses a user's name in the "Content-Disposition" header, which allows remote authenticated users to change the file extension when a vCard file is downloaded.	Patched by core rule	Y
CVE-2025-56382	CVE-2025-56382 - A stored Cross-site scripting (XSS) vulnerability exists in the Customer Management Module of LionCo...	A stored Cross-site scripting (XSS) vulnerability exists in the Customer Management Module of LionCoders SalePro POS 5.4.8. An authenticated attacker can inject arbitrary web script or HTML via the 'Customer Name' parameter when creating or editing customer profiles. This malicious input is improperly sanitized before storage and subsequent rendering, leading to script execution in the browsers of users who view the affected customer details.	Patched by core rule	Y
CVE-2025-61224	CVE-2025-61224 - Cross Site Scripting vulnerability in DokuWiki 2025-05-14a 'Librarian'[56.1] allows a remote attacke...	Cross Site Scripting vulnerability in DokuWiki 2025-05-14a 'Librarian'[56.1] allows a remote attacker to execute arbitrary code via the q parameter	Patched by core rule	Y
CVE-2025-61198	CVE-2025-61198 - A stored cross-site scripting (XSS) vulnerability in Optimod 5950 - Optimod 5950HD - Optimod 5750 - ...	A stored cross-site scripting (XSS) vulnerability in Optimod 5950 - Optimod 5950HD - Optimod 5750 - Optimod 5750HD - Optimod Trio - Optimod version 1.0.0.33 - System version 2.5.26, allows remote attackers to execute arbitrary JavaScript in the web browser of a user, by including a malicious payload into the logs which would be returned in logs rendered in the UI.	Patched by core rule	Y
CVE-2025-11308	CVE-2025-11308 - A vulnerability was identified in Vanderlande Baggage 360 7.0.0. This issue affects some unknown pro...	A vulnerability was identified in Vanderlande Baggage 360 7.0.0. This issue affects some unknown processing of the file /api-addons/v1/messages. Such	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument Message leads to cross site scripting. The attack may be 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-2025-11289	CVE-2025-11289 - A vulnerability was determined in westboy CicadasCMS up to 2431154dac8d0735e04f1fd2a3c3556668fc8dab....	A vulnerability was determined in westboy CicadasCMS up to 2431154dac8d0735e04f1fd2a3c3556668fc8dab. The impacted element is the function Save of the file src/main/java/com/zhiliao/common/template/TemplateFileServiceImpl.java of the component Template Management Page. This manipulation causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-11283	CVE-2025-11283 - A vulnerability was determined in Frappe LMS 2.35.0. This affects an unknown function of the compone...	A vulnerability was determined in Frappe LMS 2.35.0. This affects an unknown function of the component Course Handler. Executing manipulation of the argument Description can lead to cross site scripting. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. It is suggested to upgrade the affected component. The vendor was informed early about a total of four security issues and confirmed that those have been fixed. However, the release notes on GitHub do not mention them.	Patched by core rule	Y
CVE-2025-11282	CVE-2025-11282 - A vulnerability was found in Frappe LMS 2.34.x/2.35.0. The impacted element is an unknown function o...	A vulnerability was found in Frappe LMS 2.34.x/2.35.0. The impacted element is an unknown function of the component Incomplete Fix CVE-2025-55006. 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 affected component should be upgraded. The vendor was informed early about a total of four security issues and confirmed that those have	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		been fixed. However, the release notes on GitHub do not mention them.		
CVE-2025-9952	CVE-2025-9952 - The Trinity Audio – Text to Speech AI audio player to convert content into audio plugin for WordPres...	The Trinity Audio – Text to Speech AI audio player to convert content into audio plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'range-date' parameter in all versions up to, and including, 5.20.2 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-2025-10383	CVE-2025-10383 - The Contest Gallery – Upload, Vote & Sell with PayPal and Stripe plugin for WordPress is vulnerable ...	The Contest Gallery – Upload, Vote & Sell with PayPal and Stripe plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple form field parameters in all versions up to, and including, 27.0.2. This is due to insufficient input sanitization and output escaping on user-supplied attributes. This makes it possible for authenticated attackers, with author-level access or higher, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-9030	CVE-2025-9030 - The Majestic Before After Image plugin for WordPress is vulnerable to Stored Cross-Site Scripting vi...	The Majestic Before After Image plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'before_label' and 'after_label' parameters in versions less than, or equal to, 2.0.1 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-2025-8726	CVE-2025-8726 - The WP Photo Album Plus plugin for WordPress is vulnerable to Cross-Site Scripting in all versions u...	The WP Photo Album Plus plugin for WordPress is vulnerable to Cross-Site Scripting in all versions up to, and including, 9.0.11.006 due to insufficient input sanitization and output escaping in the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		wppa_user_upload function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in the photo album descriptions that execute in a victim's browser.		
CVE-2025-9876	CVE-2025-9876 - The Ird Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'i...	The Ird Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'irdslider' shortcode in all versions up to, and including, 1.0.2 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-2025-9875	CVE-2025-9875 - The Event Tickets, RSVPs, Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting...	The Event Tickets, RSVPs, Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ticket_spot' shortcode in all versions up to, and including, 1.0.2 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-2025-9859	CVE-2025-9859 - The Fintelligence Calculator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via t...	The Fintelligence Calculator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'fintelligence-calculator' shortcode in all versions up to, and including, 1.0.3 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-2025-9858	CVE-2025-9858 - The Auto Bulb Finder for WordPress plugin for	The Auto Bulb Finder for WordPress 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 Stored Cross-Site Scripting...	Stored Cross-Site Scripting via the plugin's 'abf_vehicle' shortcode in all versions up to, and including, 2.8.0 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-2025-9854	CVE-2025-9854 - The A Simple Multilanguage Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting ...	The A Simple Multilanguage Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'asmp-switcher' shortcode in all versions up to, and including, 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-2025-9206	CVE-2025-9206 - The Meks Easy Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the post ti...	The Meks Easy Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the post title field in all version up to, and including, 2.1.4. 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 the map containing the malicious post.	Patched by core rule	Y
CVE-2025-9204	CVE-2025-9204 - The X Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the...	The X Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Youtube Video ID field in all versions up to, and including, 1.0.14. This is due to insufficient input sanitization and output escaping on the Youtube Video ID parameter. 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		accesses an affected page.		
CVE-2025-9130	CVE-2025-9130 - The Unify plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin for WordP...	The Unify plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin for WordPress's unify_checkout shortcode in all versions up to, and including, 3.4.7 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-2025-9129	CVE-2025-9129 - The Flexi plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin for WordP...	The Flexi plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin for WordPress's flexi-form-tag shortcode in all versions up to, and including, 4.28 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-2025-9080	CVE-2025-9080 - The Generic Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple ...	The Generic Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple widget fields in version 1.2.4 and earlier. 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-2025-9077	CVE-2025-9077 - The Ultra Addons Lite for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scriptin...	The Ultra Addons Lite for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Animated Text' field of the Typeout Widget in version 1.1.9 and below due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-9045	CVE-2025-9045 - The Easy Elementor Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via seve...	The Easy Elementor Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several widget parameters in versions less than, or equal to, 2.2.8 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-2025-10192	CVE-2025-10192 - The WP Photo Effects plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugi...	The WP Photo Effects plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wppe_effect' shortcode in all versions up to, and including, 1.2.4 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-2025-10165	CVE-2025-10165 - The AP Background plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's...	The AP Background plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'adv_parallax_back' shortcode in all versions up to, and including, 3.8.2 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-2025-56154	CVE-2025-56154 - htmly v3.0.8 is vulnerable to Cross Site Scripting (XSS) in the /author/:name endpoint of the affect...	htmly v3.0.8 is vulnerable to Cross Site Scripting (XSS) in the /author/:name endpoint of the affected application. The name parameter is not properly sanitized before being reflected in the HTML response, allowing attackers to inject arbitrary JavaScript	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		payloads.		
CVE-2025-61087	CVE-2025-61087 - SourceCodester Pet Grooming Management Software 1.0 is vulnerable to Cross Site Scripting (XSS) via ...	SourceCodester Pet Grooming Management Software 1.0 is vulnerable to Cross Site Scripting (XSS) via the Customer Name field under Customer Management Section.	Patched by core rule	Y
CVE-2025-56379	CVE-2025-56379 - A stored cross-site scripting (XSS) vulnerability in the blog post feature of ERPNEXT v15.67.0 allow...	A stored cross-site scripting (XSS) vulnerability in the blog post feature of ERPNEXT v15.67.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the content field.	Patched by core rule	Y
CVE-2025-57389	CVE-2025-57389 - A reflected cross-site scripting (XSS) vulnerability in the /admin/system/packages endpoint of Luci ...	A reflected cross-site scripting (XSS) vulnerability in the /admin/system/packages endpoint of Luci OpenWRT v18.06.2 allows attackers to execute arbitrary Javascript in the context of a user's browser via a crafted payload. This vulnerability was fixed in OpenWRT v19.07.0.	Patched by core rule	Y
CVE-2025-60991	CVE-2025-60991 - A reflected cross-site scripted (XSS) vulnerability in Codazon Magento Themes v1.1.0.0 to v2.4.7 all...	A reflected cross-site scripted (XSS) vulnerability in Codazon Magento Themes v1.1.0.0 to v2.4.7 allows attackers to execute arbitrary Javascript in the context of a user's browser via a crafted payload injected into the cat parameter.	Patched by core rule	Y
CVE-2025-57393	CVE-2025-57393 - A stored cross-site scripting (XSS) in Kissflow Work Platform Kissflow Application Versions 7337 Acc...	A stored cross-site scripting (XSS) in Kissflow Work Platform Kissflow Application Versions 7337 Account v2.0 to v4.2vallows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload.	Patched by core rule	Y
CVE-2024-57494	CVE-2024-57494 - Cross Site Scripting vulnerability in Neto E-Commerce CMS v.6.313.0 through v.6.3115 allows a remote...	Cross Site Scripting vulnerability in Neto E-Commerce CMS v.6.313.0 through v.6.3115 allows a remote attacker to escalate privileges via the kw parameter.	Patched by core rule	Y
CVE-2025-56515	CVE-2025-56515 - File upload vulnerability in Fiora chat application 1.0.0 through user avatar upload functionality. ...	File upload vulnerability in Fiora chat application 1.0.0 through user avatar upload functionality. The application fails to validate SVG file content, allowing malicious SVG files with embedded foreignObject	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		elements containing iframe tags and JavaScript event handlers (onmouseover) to be uploaded and stored. When rendered, these SVG files execute arbitrary JavaScript, enabling attackers to steal user sessions, cookies, and perform unauthorized actions in the context of users viewing affected profiles.		
CVE-2025-56514	CVE-2025-56514 - Cross Site Scripting (XSS) vulnerability in Fiora chat application 1.0.0 allows executes arbitrary J...	Cross Site Scripting (XSS) vulnerability in Fiora chat application 1.0.0 allows executes arbitrary JavaScript when malicious SVG files are rendered by other users.	Patched by core rule	Y
CVE-2025-9075	CVE-2025-9075 - The ZoloBlocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple Gutenb...	The ZoloBlocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple Gutenberg blocks in versions up to, and including, 2.3.10. This is due to insufficient input sanitization and output escaping on user-supplied attributes within multiple block components including Google Maps markers, Lightbox captions, Image Gallery data attributes, Progress Pie prefix/suffix fields, and Text Path URL fields. 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-2025-43826	CVE-2025-43826 - Stored cross-site scripting (XSS) vulnerabilities in Web Content translation in Liferay Portal 7.4.0...	Stored cross-site scripting (XSS) vulnerabilities in Web Content translation in Liferay Portal 7.4.0 through 7.4.3.112, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.8, 2023.Q3.1 through 2023.Q3.10, 7.4 GA through update 92, and older unsupported versions allow remote attackers to inject arbitrary web script or HTML via any rich text field in a web content article.	Patched by core rule	Y
CVE-2025-56200	CVE-2025-56200 - A URL validation bypass vulnerability exists in validator.js through version 13.15.15. The isURL() f...	A URL validation bypass vulnerability exists in validator.js through version 13.15.15. The isURL() function uses '://' as a delimiter to parse protocols, while browsers use ':' as the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		delimiter. This parsing difference allows attackers to bypass protocol and domain validation by crafting URLs leading to XSS and Open Redirect attacks.		
CVE-2025-28016	CVE-2025-28016 - A Reflected Cross-Site Scripting (XSS) vulnerability was found in loginsystem/edit-profile.php of th...	A Reflected Cross-Site Scripting (XSS) vulnerability was found in loginsystem/edit-profile.php of the PHPGurukul User Registration & Login and User Management System V3.3. This vulnerability allows remote attackers to execute arbitrary JavaScript code via the fname, lname, and contact parameters.	Patched by core rule	Y
CVE-2025-9852	CVE-2025-9852 - The Yoga Schedule Momoyoga plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the...	The Yoga Schedule Momoyoga plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'momoyoga-schedule' shortcode in all versions up to, and including, 2.9.0 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-2025-8608	CVE-2025-8608 - The Mihdan: Elementor Yandex Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting ...	The Mihdan: Elementor Yandex Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's block attributes in all versions up to, and including, 1.6.11 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-2025-6941	CVE-2025-6941 - The LatePoint – Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerab...	The LatePoint – Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter of the 'latepoint_resources' shortcode in all versions up to, and including, 5.1.94 due to insufficient input	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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.		
CVE-2025-6815	CVE-2025-6815 - The LatePoint – Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerab...	The LatePoint – Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'service[name]' parameter in all versions up to, and including, 5.1.94 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-2025-10191	CVE-2025-10191 - The Big Post Shipping for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Script...	The Big Post Shipping for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wooboigpost_shipping_status' shortcode in all versions up to, and including, 2.1.1 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-2025-10189	CVE-2025-10189 - The BP Direct Menus plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin...	The BP Direct Menus plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'bpdm_login' 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		injected page.		
CVE-2025-10182	CVE-2025-10182 - The dbview plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'dbvie...	The dbview plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'dbview' shortcode in all versions up to, and including, 0.5.5 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-2025-10179	CVE-2025-10179 - The My AskAI plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'mya...	The My AskAI plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'myaskai' 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-2025-10168	CVE-2025-10168 - The Any News Ticker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin...	The Any News Ticker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'any-ticker' shortcode in all versions up to, and including, 3.1.1 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-2025-10131	CVE-2025-10131 - The All Social Share Options plugin for WordPress is vulnerable to Stored Cross-Site Scripting via t...	The All Social Share Options plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'sc' shortcode in all versions up to, and including, 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	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-2025-10130	CVE-2025-10130 - The Layers plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'webca...	The Layers plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'webcam' shortcode in all versions up to, and including, 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-2025-43817	CVE-2025-43817 - Multiple reflected cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.4.3.74 through 7.4...	Multiple reflected cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.4.3.74 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.6, 2023.Q3.1 through 2023.Q3.8, and 7.4 update 74 through update 92 allow remote attackers to inject arbitrary web script or HTML via the `redirect` parameter to (1) Announcements, or (2) Alerts.	Patched by core rule	Y
CVE-2025-43812	CVE-2025-43812 - Cross-site scripting (XSS) vulnerability in web content template in Liferay Portal 7.4.3.4 through 7...	Cross-site scripting (XSS) vulnerability in web content template in Liferay Portal 7.4.3.4 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.4, 2023.Q3.1 through 2023.Q3.8, and 7.4 GA through update 92 allows remote authenticated users to inject arbitrary web script or HTML via a crafted payload injected into a web content structure's Name text field	Patched by core rule	Y
CVE-2025-43820	CVE-2025-43820 - Multiple cross-site scripting (XSS) vulnerabilities in the Calendar widget when inviting users to a ...	Multiple cross-site scripting (XSS) vulnerabilities in the Calendar widget when inviting users to a event in Liferay Portal 7.4.3.35 through 7.4.3.110, and Liferay DXP 2023.Q4.0 through 2023.Q4.4, 2023.Q3.1 through 2023.Q3.6, 7.4 update 35 through update 92, and 7.3 update 25 through update 35 allow remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a user's (1) First	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Name, (2) Middle text, or (3) Last Name text fields.		
CVE-2025-43818	CVE-2025-43818 - Cross-site scripting (XSS) vulnerability in the Calendar widget in Liferay Portal 7.4.3.35 through 7...	Cross-site scripting (XSS) vulnerability in the Calendar widget in Liferay Portal 7.4.3.35 through 7.4.3.110, and Liferay DXP 2023.Q4.0 through 2023.Q4.4, 2023.Q3.1 through 2023.Q3.6, 7.4 update 35 through update 92, and 7.3 update 25 through update 36 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a Calendar's “Name” text field	Patched by core rule	Y
CVE-2025-43815	CVE-2025-43815 - Reflected cross-site scripting (XSS) vulnerability on the page configuration page in Liferay Portal ...	Reflected cross-site scripting (XSS) vulnerability on the page configuration page in Liferay Portal 7.4.3.102 through 7.4.3.110, and Liferay DXP 2023.Q4.0 through 2023.Q4.2, and 2023.Q3.5 allows remote attackers to inject arbitrary web script or HTML via the com_liferay_layout_admin_web_portlet_GroupPagesPortlet_backURLTitle parameter.	Patched by core rule	Y
CVE-2025-43811	CVE-2025-43811 - Multiple stored cross-site scripting (XSS) vulnerability in the related asset selector in Liferay Po...	Multiple stored cross-site scripting (XSS) vulnerability in the related asset selector in Liferay Portal 7.4.3.50 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.4, 2023.Q3.1 through 2023.Q3.7, and 7.4 update 50 through update 92 allows remote authenticated attackers to inject arbitrary web script or HTML via a crafted payload injected into an asset author’s (1) First Name, (2) Middle Name, or (3) Last Name text field.	Patched by core rule	Y
CVE-2025-57483	CVE-2025-57483 - A reflected cross-site scripting (XSS) vulnerability in tawk.to chatbox widget v4 allows attackers t...	A reflected cross-site scripting (XSS) vulnerability in tawk.to chatbox widget v4 allows attackers to execute arbitrary Javascript in the context of the user's browser via injecting a crafted payload into the vulnerable parameter.	Patched by core rule	Y
CVE-2025-56807	CVE-2025-56807 - A cross-site scripting (XSS) vulnerability in FairSketch RISE Ultimate Project Manager & CRM 3.9.4 a...	A cross-site scripting (XSS) vulnerability in FairSketch RISE Ultimate Project Manager & CRM 3.9.4 allows an administrator to store a JavaScript payload using the file explorer in the admin dashboard when creating	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		new folders.		
CVE-2025-56795	CVE-2025-56795 - Mealie 3.0.1 and earlier is vulnerable to Stored Cross-Site Scripting (XSS) in the recipe creation f...	Mealie 3.0.1 and earlier is vulnerable to Stored Cross-Site Scripting (XSS) in the recipe creation functionality. Unsanitized user input in the "note" and "text" fields of the "/api/recipes/{recipe_name}" endpoint is rendered in the frontend without proper escaping leading to persistent XSS.	Patched by core rule	Y
CVE-2025-11124	CVE-2025-11124 - A vulnerability has been found in code-projects Project Monitoring System 1.0. Affected is an unknow...	A vulnerability has been found in code-projects Project Monitoring System 1.0. Affected is an unknown function of the file /onlineJobSearchEngine/postjob.php. Such manipulation of the argument txtapplyto leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-11069	CVE-2025-11069 - A vulnerability was determined in westboy CicadasCMS 1.0. Affected by this issue is some unknown fun...	A vulnerability was determined in westboy CicadasCMS 1.0. Affected by this issue is some unknown functionality of the file /system/org/save of the component Add Department Handler. This manipulation of the argument Name causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-11068	CVE-2025-11068 - A vulnerability was found in westboy CicadasCMS 1.0. Affected by this vulnerability is an unknown fu...	A vulnerability was found in westboy CicadasCMS 1.0. Affected by this vulnerability is an unknown functionality of the file /system/cms/category/save. The manipulation of the argument categoryName results in cross site scripting. The attack can be executed remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2025-9816	CVE-2025-9816 - The WP Statistics – The Most Popular Privacy-Friendly Analytics Plugin plugin for WordPress is vulne...	The WP Statistics – The Most Popular Privacy-Friendly Analytics Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the User-Agent Header in all versions up to, and including, 14.5.4 due to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-8440	CVE-2025-8440 - The Team Members plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the first and...	The Team Members plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the first and last name fields in all versions up to, and including, 5.3.5 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-2025-57692	CVE-2025-57692 - PiranhaCMS 12.0 allows stored XSS in the Text content block of Standard and Standard Archive Pages v...	PiranhaCMS 12.0 allows stored XSS in the Text content block of Standard and Standard Archive Pages via /manager/pages, enabling execution of arbitrary JavaScript in another user s browser.	Patched by core rule	Y
CVE-2025-26258	CVE-2025-26258 - Sourcecodester Employee Management System v1.0 is vulnerable to Cross Site Scripting (XSS) via 'Add ...	Sourcecodester Employee Management System v1.0 is vulnerable to Cross Site Scripting (XSS) via 'Add Designation.'	Patched by core rule	Y
CVE-2025-11027	CVE-2025-11027 - A vulnerability was identified in givanz Vvveb up to 1.0.7.2. Affected by this issue is some unknown...	A vulnerability was identified in givanz Vvveb up to 1.0.7.2. Affected by this issue is some unknown functionality of the component SVG File Handler. Such manipulation leads to cross site scripting. The attack may be launched remotely. The exploit is publicly available and might be used. Once again the project maintainer reacted very professional: "I accept the existence of these vulnerabilities. (...) I fixed the code to remove these vulnerabilities and will push the code to github and make a new release."	Patched by core rule	Y
CVE-2025-60186	CVE-2025-60186 - 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 Alex Moss Google+ Comments allows Stored XSS. This issue affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Google+ Comments: from n/a through 1.0.		
CVE-2025-60185	CVE-2025-60185 - 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 kontur.us kontur Admin Style allows Stored XSS. This issue affects kontur Admin Style: from n/a through 1.0.4.	Patched by core rule	Y
CVE-2025-60184	CVE-2025-60184 - 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 Terry L. SEO Search Permalink allows Stored XSS. This issue affects SEO Search Permalink: from n/a through 1.0.3.	Patched by core rule	Y
CVE-2025-60179	CVE-2025-60179 - 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 Space Studio Click & Tweet allows Stored XSS. This issue affects Click & Tweet: from n/a through 0.8.9.	Patched by core rule	Y
CVE-2025-60177	CVE-2025-60177 - 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 rozx Recaptcha – wp allows Stored XSS. This issue affects Recaptcha – wp: from n/a through 0.2.6.	Patched by core rule	Y
CVE-2025-60163	CVE-2025-60163 - 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 Robin W bbp topic count allows DOM-Based XSS. This issue affects bbp topic count: from n/a through 3.1.	Patched by core rule	Y
CVE-2025-60162	CVE-2025-60162 - 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 PickPlugins Job Board Manager allows DOM-Based XSS. This issue affects Job Board Manager: from n/a through 2.1.61.	Patched by core rule	Y
CVE-2025-60160	CVE-2025-60160 - 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 sharkthemes Smart Related Products allows Stored XSS. This issue affects Smart Related Products: from n/a through 2.0.5.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-60158	CVE-2025-60158 - 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 webmaniabr Nota Fiscal Eletrônica WooCommerce allows Stored XSS. This issue affects Nota Fiscal Eletrônica WooCommerce: from n/a through 3.4.0.6.	Patched by core rule	Y
CVE-2025-60157	CVE-2025-60157 - 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 WP Ticket Customer Service Software & Support Ticket System allows Stored XSS. This issue affects WP Ticket Customer Service Software & Support Ticket System: from n/a through 6.0.2.	Patched by core rule	Y
CVE-2025-60154	CVE-2025-60154 - 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 Jennifer Moss MWW Disclaimer Buttons allows Stored XSS. This issue affects MWW Disclaimer Buttons: from n/a through 3.41.	Patched by core rule	Y
CVE-2025-60149	CVE-2025-60149 - 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 Michael Ott Notely allows Stored XSS. This issue affects Notely: from n/a through 1.8.0.	Patched by core rule	Y
CVE-2025-60147	CVE-2025-60147 - 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 Feed allows Stored XSS. This issue affects HT Feed: from n/a through 1.3.0.	Patched by core rule	Y
CVE-2025-60146	CVE-2025-60146 - 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 Amit Verma Map Categories to Pages allows Stored XSS. This issue affects Map Categories to Pages: from n/a through 1.3.2.	Patched by core rule	Y
CVE-2025-60144	CVE-2025-60144 - 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 yonifre Lenix scss compiler allows Stored XSS. This issue affects Lenix scss compiler: from n/a through 1.2.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-60142	CVE-2025-60142 - 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 DaganLev Simple Meta Tags allows DOM-Based XSS. This issue affects Simple Meta Tags: from n/a through 1.5.	Patched by core rule	Y
CVE-2025-60141	CVE-2025-60141 - 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 thetechtribe The Tribal allows Stored XSS. This issue affects The Tribal: from n/a through 1.3.3.	Patched by core rule	Y
CVE-2025-60138	CVE-2025-60138 - 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 sonalsinha21 SKT Blocks allows Stored XSS. This issue affects SKT Blocks: from n/a through 2.5.	Patched by core rule	Y
CVE-2025-60136	CVE-2025-60136 - 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 cartpauj User Notes allows Stored XSS. This issue affects User Notes: from n/a through 1.0.2.	Patched by core rule	Y
CVE-2025-60133	CVE-2025-60133 - 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 DJ-Extensions.com PE Easy Slider allows Stored XSS. This issue affects PE Easy Slider: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-60124	CVE-2025-60124 - 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 Ryan Hellyer Simple Colorbox allows Stored XSS. This issue affects Simple Colorbox: from n/a through 1.6.1.	Patched by core rule	Y
CVE-2025-60112	CVE-2025-60112 - 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 aThemes Addons for Elementor allows Stored XSS. This issue affects aThemes Addons for Elementor: from n/a through 1.1.3.	Patched by core rule	Y
CVE-2025-60105	CVE-2025-60105 - 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...	metaphorcreations Ditty allows Stored XSS. This issue affects Ditty: from n/a through 3.1.58.		
CVE-2025-60104	CVE-2025-60104 - 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 Jordy Meow Gallery Custom Links allows Stored XSS. This issue affects Gallery Custom Links: from n/a through 2.2.5.	Patched by core rule	Y
CVE-2025-60102	CVE-2025-60102 - 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 Syam Mohan WPFront User Role Editor allows Stored XSS. This issue affects WPFront User Role Editor: from n/a through 4.2.3.	Patched by core rule	Y
CVE-2025-60101	CVE-2025-60101 - 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 Woostify Woostify allows Stored XSS. This issue affects Woostify: from n/a through 2.4.2.	Patched by core rule	Y
CVE-2025-60099	CVE-2025-60099 - 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 awsm.in Embed Any Document allows Stored XSS. This issue affects Embed Any Document: from n/a through 2.7.7.	Patched by core rule	Y
CVE-2025-60040	CVE-2025-60040 - 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 fkrauthan wp-mpdf allows Stored XSS. This issue affects wp-mpdf: from n/a through 3.9.1.	Patched by core rule	Y
CVE-2025-59012	CVE-2025-59012 - 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 shinetheme Traveler allows Reflected XSS. This issue affects Traveler: from n/a through n/a.	Patched by core rule	Y
CVE-2025-58917	CVE-2025-58917 - 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 Nick Verwymeren Quantities and Units for WooCommerce allows Stored XSS. This issue affects Quantities and Units for	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		WooCommerce: from n/a through 1.0.13.		
CVE-2025-4957	CVE-2025-4957 - 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 Metagauss ProfileGrid allows Reflected XSS. This issue affects ProfileGrid : from n/a through 5.9.5.7.	Patched by core rule	Y
CVE-2025-48107	CVE-2025-48107 - 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 undsgn Uncode allows Reflected XSS. This issue affects Uncode: from n/a through n/a.	Patched by core rule	Y
CVE-2025-27006	CVE-2025-27006 - 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 themeplugs Authorsy allows Stored XSS. This issue affects Authorsy: from n/a through 1.0.5.	Patched by core rule	Y
CVE-2025-10490	CVE-2025-10490 - The Zephyr Project Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via adm...	The Zephyr Project Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.3.202 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-2025-10180	CVE-2025-10180 - The Markdown Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plu...	The Markdown Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'markdown' shortcode in all versions up to, and including, 0.2.1 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-2025-9490	CVE-2025-9490 - The	The Popup Maker plugin for	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Popup Maker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title' pa...	WordPress is vulnerable to Stored Cross-Site Scripting via the 'title' parameter in all versions up to, and including, 1.20.6 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	

INDUSFACE™

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

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

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

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

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