INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

November 2025

The total zero-day vulnerabilities count for November month: 227

Command Injection	SQL Injection	SSRF	Path Traversal	Cross-Site Scripting	Arbitrary Upload/ RCE
2	63	11	8	118	25

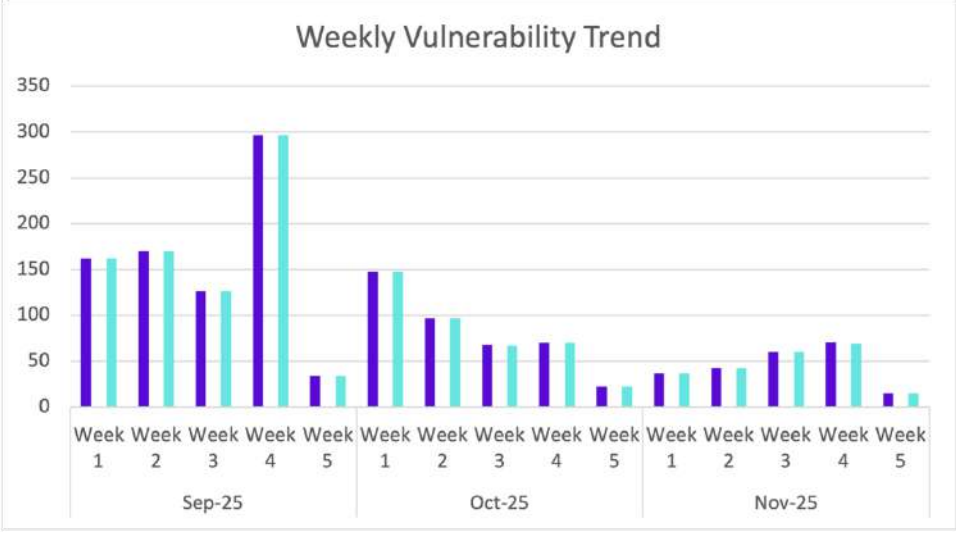
Zero-day vulnerabilities protected through core rules	225
Zero-day vulnerabilities protected through custom rules	2
Zero-day vulnerabilities found by Indusface WAS	223

- 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

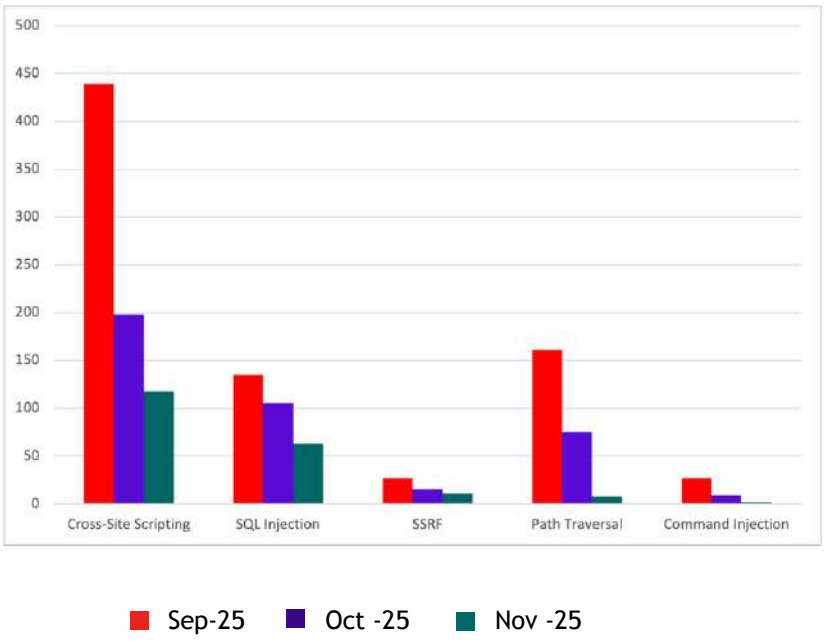


of the zero-day vulnerabilities were protected by the core rules in the last month

of the zero-day vulnerabilities were protected by the custom 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-2025-13562	D-Link DIR-852 gena.cgi command injection	A vulnerability was identified in D-Link DIR-852 1.00. This issue affects some unknown processing of the file /gena.cgi. Such manipulation of the argument service leads to command injection. The attack can be executed remotely. The exploit is publicly available and might be used. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-12296	D-Link DAP-2695 Firmware Update sub_4174B0 os command injection	A security vulnerability has been detected in D-Link DAP-2695 2.00RC13. The impacted element is the function sub_4174B0 of the component Firmware Update Handler. The manipulation leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y

Path Traversal Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-13435	Dreampie Resty HttpClient HttpClient.java request path traversal	A security vulnerability has been detected in Dreampie Resty up to 1.3.1.SNAPSHOT. This affects the function Request of the file /resty-httpclient/src/main/java/cn/dreampie/client/HttpClient.java of the component HttpClient Module. Such manipulation of the argument filename leads to path traversal. The attack may be performed from remote. Attacks of this nature are highly complex. The exploitability is reported as difficult. 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-2025-12089	Data Tables Generator by Supsystic <= 1.10.45 - Authenticated (Admin+) Arbitrary File Deletion	The Data Tables Generator by Supsystic plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the cleanCache() function in all versions up to, and including, 1.10.45. 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
CVE-2025-12923	liweiyi ChestnutCMS download resourceDownload path traversal	A vulnerability was determined in liweiyi ChestnutCMS up to 1.5.8. This vulnerability affects the function resourceDownload of the file /dev-api/common/download. 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.	Patched by core rule	Y
CVE-2025-12922	OpenClinica Community Edition CRF Data Import ImportCRFData path traversal	A vulnerability was found in OpenClinica Community Edition up to 3.12.2/3.13. This affects an unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		part of the file /ImportCRFData?action=confirm of the component CRF Data Import. Performing manipulation of the argument xml_file 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.		
CVE-2025-12092	CYAN Backup <= 2.5.4 - Authenticated (Admin+) Arbitrary File Deletion	The CYAN Backup plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the 'delete' functionality in all versions up to, and including, 2.5.4. 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
CVE-2025-12000	WPFunnels <= 3.6.2 - Authenticated (Administrator+) Arbitrary File Deletion via Path Traversal	The WPFunnels plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the wpfnl_delete_log() function in all versions up to, and including, 3.6.2. 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
CVE-2025-12493	ShopLentor <= 3.2.5 - Unauthenticated Local PHP File Inclusion via 'load_template'	The ShopLentor – WooCommerce Builder for Elementor & Gutenberg +21 Modules – All in One Solution (formerly WooLentor) plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 3.2.5 via the 'load_template' function. This makes it possible for unauthenticated attackers to include and execute arbitrary .php files on the server, allowing the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.		
CVE-2025-12250	OpenWGA TMLScript API WGA.File path traversal	A flaw has been found in OpenWGA 7.11.12 Build 737. This affects an unknown function of the file WGA.File of the component TMLScript API. Executing manipulation can lead to path traversal. It is possible to launch the attack 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

Server-side Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-13588	lKinderBueno Streamity Xtream IPTV Player proxy.php server-side request forgery	A vulnerability was found in lKinderBueno Streamity Xtream IPTV Player up to 2.8. The impacted element is an unknown function of the file public/proxy.php. Performing manipulation results in server-side request forgery. The attack can be initiated remotely. The exploit has been made public and could be used. Upgrading to version 2.8.1 is sufficient to resolve this issue. The patch is named c70bfb8d36b47bfd64c5ec73917e1d9ddb97af92. It is suggested to upgrade the affected component.	Patched by core rule	Y
CVE-2025-12800	WP Shortcodes Plugin — Shortcodes Ultimate <= 7.4.5 - Authenticated (Administrator+) Server-Side Request Forgery	The WP Shortcodes Plugin — Shortcodes Ultimate plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 7.4.5 via the su_shortcode_csv_table 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. If the 'Unsafe features' option is explicitly enabled by an administrator, this issue becomes exploitable by Contributor+ attackers	Patched by core rule	Y
CVE-2025-12359	Responsive Lightbox & Gallery <= 2.5.3 - Authenticated (Author+) Server-Side Request Forgery	The Responsive Lightbox & Gallery plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 2.5.3 via the 'get_image_size_by_url' function. This is due to insufficient validation of user-supplied URLs when determining image dimensions for gallery items. 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 which can be used to query and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		modify information from internal services.		
CVE-2025-12376	Icon List Block – Add Icon-Based Lists with Custom Styles <= 1.2.1 - Authenticated (Subscriber+) Server-Side Request Forgery	The Icon List Block – Add Icon-Based Lists with Custom Styles plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.2.1 via the fs_api_request function. 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. Only valid JSON objects are rendered in the response.	Patched by core rule	Y
CVE-2025-8084	AI Engine <= 3.1.8 - Authenticated (Editor+) Server-Side Request Forgery	The AI Engine plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 3.1.8 via the rest_helpers_create_images function. This makes it possible for authenticated attackers, with Editor-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 metadata retrieving.	Patched by core rule	Y
CVE-2025-11427	WP Migrate Lite <= 2.7.6 - Unauthenticated Blind Server-Side Request Forgery	The WP Migrate Lite – WordPress Migration Made Easy plugin for WordPress is vulnerable to Blind Server-Side Request Forgery in all versions up to, and including, 2.7.6 via the wpmdb_flush AJAX action. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to obtain information about internal services.	Patched by core rule	Y
CVE-2025-12962	Local Syndication <= 1.5a - Authenticated (Contributor+) Server-Side Request Forgery via Shortcode	The Local Syndication plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.5a via the `url` parameter in the `[syndicate_local]` shortcode. This is due to the use of `wp_remote_get()`	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		instead of `wp_safe_remote_get()` which lacks protections against requests to internal/private IP addresses and localhost. This makes it possible for authenticated attackers, with Contributor-level access and above, to make web requests to arbitrary locations originating from the web application, which can be used to query and modify information from internal services, scan internal networks, and access resources that should not be accessible from external networks.		
CVE-2025-12560	Blog2Social: Social Media Auto Post & Scheduler <= 8.6.0 - Authenticated (Subscriber+) Blind Server-Side Request Forgery via post_url	The Blog2Social: Social Media Auto Post & Scheduler plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 8.6.0 via the getFullContent() function. 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-2025-12388	B Carousel Block – Responsive Image and Content Carousel <= 1.1.5 - Missing Authorization to Authenticated (Subscriber+) Server-Side Request Forgery	The B Carousel Block – Responsive Image and Content Carousel plugin for WordPress is vulnerable to Server-Side Request Forgery in versions up to, and including, 1.1.5. This is due to the plugin not validating user-supplied URLs before passing them to the wp_remote_request() function. 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-2025-11917	WPeMatico RSS Feed Fetcher <= 2.8.11 - Authenticated (Subscriber+) Server-Side Request Forgery via wpematico_test_feed	The WPeMatico RSS Feed Fetcher plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 2.8.11 via the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		wpematico_test_feed() function. 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.		
CVE-2025-10145	Auto Featured Image (Auto Post Thumbnail) <= 4.1.7 - Authenticated (Author+) Server-Side Request Forgery	The Auto Featured Image (Auto Post Thumbnail) plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 4.1.7 via the upload_to_library 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. On Cloud instances, this issue allows for metadata retrieval.	Patched by core rule	Y

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-13385	Bookme <= 4.2 - Authenticated (Admin+) SQL Injection via 'filter[status]' Parameter	The Bookme – Free Online Appointment Booking and Scheduling Plugin for WordPress is vulnerable to time-based SQL Injection via the `filter[status]` parameter in all versions up to, and including, 4.2 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 admin-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-2025-13370	ProjectList <= 0.3.0 - Authenticated (Editor+) SQL Injection via 'id' Parameter	The ProjectList plugin for WordPress is vulnerable to time-based SQL Injection via the 'id' parameter in all versions up to, and including, 0.3.0 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attackers, with Editor-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-2025-10144	Perfect Brands for WooCommerce <= 3.6.2 - Authenticated (Contributor+) SQL Injection	The Perfect Brands for WooCommerce plugin for WordPress is vulnerable to time-based SQL Injection via the `brands` attribute of the `products` shortcode in all versions up to, and including, 3.6.2 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 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-2025-13575	code-projects Blog Site Category blog.php category_exists sql injection	A security vulnerability has been detected in code-projects Blog Site 1.0. Impacted is the function category_exists of the file /resources/functions/	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		blog.php of the component Category Handler. Such manipulation of the argument name/field leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. Multiple endpoints are affected.		
CVE-2025-13572	projectworlds Advanced Library Management System delete_admin.php sql injection	A vulnerability was identified in projectworlds Advanced Library Management System 1.0. This affects an unknown part of the file /delete_admin.php. The manipulation of the argument admin_id leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2025-12750	Groundhogg <= 4.2.6.1 - Authenticated (Admin+) SQL Injection	The Groundhogg — CRM, Newsletters, and Marketing Automation plugin for WordPress is vulnerable to SQL Injection via the 'term' parameter in all versions up to, and including, 4.2.6.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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-2025-13138	WP Directory Kit <= 1.4.3 - Unauthenticated SQL Injection via select_2_ajax() Function	The WP Directory Kit plugin for WordPress is vulnerable to SQL Injection via the 'columns_search' parameter of the select_2_ajax() function in all versions up to, and including, 1.4.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for 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-2025-12646	Community Events <= 1.5.4 - Unauthenticated SQL Injection	The Community Events plugin for WordPress is vulnerable to SQL Injection via the 'dayofyear' parameter in all versions up to, and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		including, 1.5.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.		
CVE-2025-12411	Premmerce Wholesale Pricing for WooCommerce <= 1.1.10 - Authenticated (Subscriber+) SQL Injection	The Premmerce Wholesale Pricing for WooCommerce plugin for WordPress is vulnerable to SQL Injection via the 'ID' parameter in versions up to, and including, 1.1.10. 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 subscriber level access and above, to manipulate SQL queries that can be used to extract sensitive information from the database and modify price type display names in the database via the admin-post.php "premmerce_update	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		_price_type" action, causing cosmetic corruption of the admin interface. The 'price_type' parameter of the "premmerce_delete_price_type" is also vulnerable.		
CVE-2025-13279	code-projects Nero Social Networking Site profilefriends.php sql injection	A vulnerability was found in code-projects Nero Social Networking Site 1.0. The affected element is an unknown function of the file /profilefriends.php. Performing manipulation of the argument ID results in sql injection. The attack may be initiated remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2025-13278	projectworlds Advanced Library Management System borrowed_book_search.php sql injection	A vulnerability has been found in projectworlds Advanced Library Management System 1.0. Impacted is an unknown function of the file /borrowed_book_search.php. Such manipulation of the argument datefrom/dateto leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-13267	SourceCodester Dental Clinic	A vulnerability was detected in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Appointment Reservation System success.php sql injection	SourceCodester Dental Clinic Appointment Reservation System 1.0. Impacted is an unknown function of the file /success.php. Performing manipulation of the argument username/password results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used.		
CVE-2025-13264	SourceCodester Online Magazine Management System view_magazine.php sql injection	A security flaw has been discovered in SourceCodester Online Magazine Management System 1.0. This affects an unknown part of the file /view_magazine.php. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be exploited.	Patched by core rule	Y
CVE-2025-13263	SourceCodester Online Magazine Management System categories.php sql injection	A vulnerability was identified in SourceCodester Online Magazine Management System 1.0. Affected by this issue is some unknown functionality of the file /categories.php. The manipulation of the argument c leads	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.		
CVE-2025-13256	projectworlds Advanced Library Management System borrow.php sql injection	A weakness has been identified in projectworlds Advanced Library Management System 1.0. Impacted is an unknown function of the file /borrow.php. Executing manipulation of the argument roll_number 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.	Patched by core rule	Y
CVE-2025-13255	projectworlds Advanced Library Management System book_search.php sql injection	A security flaw has been discovered in projectworlds Advanced Library Management System 1.0. This issue affects some unknown processing of the file /book_search.php. Performing manipulation of the argument book_pub/book_title results in sql injection. 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-2025-13254	projectworlds Advanced Library	A vulnerability was identified in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Management System add_member.php sql injection	projectworlds Advanced Library Management System 1.0. This vulnerability affects unknown code of the file /add_member.php. Such manipulation of the argument roll_number leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.		
CVE-2025-13253	projectworlds Advanced Library Management System add_librarian.php sql injection	A vulnerability was determined in projectworlds Advanced Library Management System 1.0. This affects an unknown part of the file /add_librarian.php. This manipulation of the argument Username 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-2025-13251	WeiYe-Jing datax-web sql injection	A flaw has been found in WeiYe-Jing datax-web up to 2.1.2. Affected is an unknown function. Executing manipulation 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-2025-13243	code-projects	A vulnerability was	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Student Information System editprofile.php sql injection	found in code-projects Student Information System 2.0. Impacted is an unknown function of the file /editprofile.php. The manipulation results in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.	core rule	
CVE-2025-13242	code-projects Student Information System register.php sql injection	A vulnerability has been found in code-projects Student Information System 2.0. This issue affects some unknown processing of the file /register.php. The manipulation leads to sql 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-2025-13241	code-projects Student Information System index.php sql injection	A flaw has been found in code-projects Student Information System 2.0. This vulnerability affects unknown code of the file /index.php. Executing manipulation of the argument Username can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-13240	code-projects Student Information System searchquery.php sql injection	A vulnerability was detected in code-projects Student Information System 2.0. This affects an unknown part of the file /searchquery.php. Performing manipulation of the argument s results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-12482	Booking for Appointments and Events Calendar – Amelia <= 1.2.35 - Unauthenticated SQL Injection via search	The Booking for Appointments and Events Calendar – Amelia plugin for WordPress is vulnerable to SQL Injection via the 'search' parameter in all versions up to, and including, 1.2.35 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-2025-13201	code-projects Simple Cafe Ordering System login.php sql	A vulnerability was identified in code-projects Simple Cafe Ordering System 1.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	Affected by this issue is some unknown functionality of the file /login.php. Such manipulation of the argument Username leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.		
CVE-2025-8994	WP Project Manager <= 2.6.26 - Authenticated (Subscriber+) SQL Injection via 'completed_at_operator'	The Project Management, Team Collaboration, Kanban Board, Gantt Charts, Task Manager and More – WP Project Manager plugin for WordPress is vulnerable to time-based SQL Injection via the 'completed_at_operator' parameter in all versions up to, and including, 2.6.26 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-2025-13171	ZZCMS wangkan_list.php	A vulnerability was identified in ZZCMS	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	sql injection	2023. This impacts an unknown function of the file /admin/wangkan_list.php. Such manipulation of the argument keyword leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.		
CVE-2025-13169	code-projects Simple Online Hotel Reservation System add_query_reserve.php sql injection	A security vulnerability has been detected in code-projects Simple Online Hotel Reservation System 1.0. This vulnerability affects unknown code of the file /add_query_reserve.php. Such manipulation of the argument room_id leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2025-13168	ury-erp ury pos_extend.py overrided_past_order_list sql injection	A weakness has been identified in ury-erp ury up to 0.2.0. This affects the function overrided_past_order_list of the file ury/ury/api/pos_extend.py. This manipulation of the argument search_term causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		public and could be exploited. Upgrading to version 0.2.1 is able to mitigate this issue. Patch name: 063384e0dddfd191847cd2d6524c342cc380b058. It is suggested to upgrade the affected component. The vendor replied and reacted very professional.		
CVE-2025-11981	School Management System – WPSchoolPress <= 2.2.23 - Authenticated (Administrator+) SQL Injection	The School Management System – WPSchoolPress plugin for WordPress is vulnerable to SQL Injection via the 'SCodes' parameter in all versions up to, and including, 2.2.23 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-2025-13121	cameasy Liketea API Endpoint StoreController.php list sql injection	A security vulnerability has been detected in cameasy Liketea 1.0.0. Impacted is the function list of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		laravel/app/Http/Controllers/Front/StoreController.php of the component API Endpoint. Such manipulation of the argument lng/lat leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.		
CVE-2025-12620	Poll Maker – Versus Polls, Anonymous Polls, Image Polls <= 6.0.7 - Authenticated (Administrator+) SQL Injection via `filterbyauthor` Parameter	The Poll Maker – Versus Polls, Anonymous Polls, Image Polls plugin for WordPress is vulnerable to generic SQL Injection via the 'filterbyauthor' parameter in all versions up to, and including, 6.0.7 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-2025-13076	code-projects Responsive Hotel Site usersetting.php sql	A flaw has been found in code-projects Responsive Hotel Site 1.0. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	affected element is an unknown function of the file /admin/usersetting.php. Executing manipulation of the argument usname can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.		
CVE-2025-13075	code-projects Responsive Hotel Site usersettingdel.php sql injection	A vulnerability was detected in code-projects Responsive Hotel Site 1.0. Impacted is an unknown function of the file /admin/usersettingdel.php. Performing manipulation of the argument eid results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-13060	SourceCodester Survey Application System view_survey.php sql injection	A security vulnerability has been detected in SourceCodester Survey Application System 1.0. This affects an unknown function of the file /view_survey.php. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2025-11454	Specific Content	The Specific Content	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	For Mobile – Customize the mobile version without redirections <= 0.5.5 - Authenticated (Contributor+) SQL Injection	For Mobile – Customize the mobile version without redirections plugin for WordPress is vulnerable to SQL Injection via the eos_scfm_duplicate_post_as_draft() function in all versions up to, and including, 0.5.5 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.	core rule	
CVE-2025-12929	SourceCodester Survey Application System LoginRegistration.php update_user sql injection	A flaw has been found in SourceCodester Survey Application System 1.0. This impacts the function save_user/update_user of the file /LoginRegistration.php. Executing manipulation of the argument fullname can lead to sql injection. The attack may be performed from remote. The exploit has been published and may	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		be used. Other parameters might be affected as well.		
CVE-2025-12928	code-projects Online Job Search Engine login.php sql injection	A vulnerability was detected in code-projects Online Job Search Engine 1.0. This affects an unknown function of the file /login.php. Performing manipulation of the argument username/phone results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-12921	OpenClinica Community Edition CRF Data Import ImportCRFData xml injection	A vulnerability has been found in OpenClinica Community Edition up to 3.12.2/3.13. Affected by this issue is some unknown functionality of the file /ImportCRFData?action=confirm of the component CRF Data Import. Such manipulation of the argument xml_file leads to xml 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-12914	aaPanel BaoTa Backend database sql injection	A vulnerability has been found in aaPanel BaoTa up to 11.2.x. This vulnerability affects unknown code of the file /database?action=GetDatabaseAccess of the component Backend. The manipulation of the argument Name leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 11.3.0 is able to resolve this issue. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-12913	code-projects Responsive Hotel Site roomdel.php sql injection	A flaw has been found in code-projects Responsive Hotel Site 1.0. This affects an unknown part of the file /admin/roomdel.php. Executing manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2025-11980	Quick Featured Images <= 13.7.3 - Authenticated (Editor+) SQL Injection via delete_orphaned	The Quick Featured Images plugin for WordPress is vulnerable to SQL Injection via the 'delete_orphaned' function in all	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		versions up to, and including, 13.7.3 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 Editor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database, granted they can convince an author-level user or higher to add a malicious custom field value.		
CVE-2025-11452	Asgaros Forum <= 3.1.0 - Unauthenticated SQL Injection	The Asgaros Forum plugin for WordPress is vulnerable to SQL Injection via the '$_COOKIE['asgarosforum_unread_exclude']' cookie in all versions up to, and including, 3.1.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		extract sensitive information from the database.		
CVE-2025-12857	code-projects Responsive Hotel Site roombook.php sql injection	A security vulnerability has been detected in code-projects Responsive Hotel Site 1.0. The affected element is an unknown function of the file /admin/roombook.php. Such manipulation of the argument rid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2025-12856	code-projects Responsive Hotel Site reservation.php sql injection	A weakness has been identified in code-projects Responsive Hotel Site 1.0. Impacted is an unknown function of the file /admin/reservation.php. This manipulation of the argument email causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	Patched by core rule	Y
CVE-2025-12855	code-projects Responsive Hotel Site newsletterdel.php sql injection	A security flaw has been discovered in code-projects Responsive Hotel Site 1.0. This issue affects some unknown processing of the file /admin/newsletterdel	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		.php. The manipulation of the argument eid results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.		
CVE-2025-10683	Easy Email Subscription <= 1.3 - Authenticated (Admin+) SQL Injection via uid	The Easy Email Subscription plugin for WordPress is vulnerable to SQL Injection via the 'uid' parameter in all versions up to, and including, 1.3 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 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-2025-12197	The Events Calendar 6.15.1.1 - 6.15.9 - Unauthenticated SQL Injection via s	The The Events Calendar plugin for WordPress is vulnerable to blind SQL Injection via the 's' parameter in versions 6.15.1.1 to 6.15.9 due to insufficient escaping on the user supplied parameter and lack	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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-2025-32786	GLPI Inventory Plugin is Vulnerable to Unauthenticated SQL Injection	The GLPI Inventory Plugin handles network discovery, inventory, software deployment, and data collection for GLPI agents. Versions 1.5.0 and below are vulnerable to SQL Injection. This issue is fixed in version 1.5.1.	Patched by core rule	Y
CVE-2025-12614	SourceCodester Best House Rental Management System admin_class.php delete_payment sql injection	A weakness has been identified in SourceCodester Best House Rental Management System 1.0. Impacted is the function delete_payment of the file /admin_class.php. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	Patched by core rule	Y
CVE-2025-12598	SourceCodester Best House Rental	A flaw has been found in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Management System admin_class.php save_tenant sql injection	SourceCodester Best House Rental Management System 1.0. Affected by this issue is the function save_tenant of the file /admin_class.php. Executing manipulation of the argument firstname can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used. Other parameters might be affected as well.		
CVE-2025-12597	SourceCodester Best House Rental Management System admin_class.php save_category sql injection	A vulnerability was detected in SourceCodester Best House Rental Management System 1.0. Affected by this vulnerability is the function save_category of the file /admin_class.php. Performing manipulation of the argument Name results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-12594	code-projects Simple Online Hotel Reservation System add_account.php sql injection	A security flaw has been discovered in code-projects Simple Online Hotel Reservation System 2.0. This affects an unknown function of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/admin/add_account.php. The manipulation of the argument Name results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be exploited.		
CVE-2025-11740	wpForo Forum <= 2.4.9 - Authenticated (Susbscriber+) SQL Injection	The wpForo Forum plugin for WordPress is vulnerable to SQL Injection via the Subscriptions Manager in all versions up to, and including, 2.4.9 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-2025-4665	CVE-2025-4665 - WordPress plugin Contact Form CFDB7 versions up to and including 1.3.2 are affected by a pre-authent...	WordPress plugin Contact Form CFDB7 versions up to and including 1.3.2 are affected by a pre-authentication SQL injection vulnerability that cascades into insecure	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		deserialization (PHP Object Injection). The weakness arises due to insufficient validation of user input in plugin endpoints, allowing crafted input to influence backend queries in unexpected ways. Using specially crafted payloads, this can escalate into unsafe deserialization, enabling arbitrary object injection in PHP. Although the issue is remotely exploitable without authentication, it does require a crafted interaction with the affected endpoint in order to trigger successfully.		
CVE-2025-11735	HUSKY – Products Filter Professional for WooCommerce <= 1.3.7.1 - Unauthenticated SQL Injection via `phrase` Parameter	The HUSKY – Products Filter Professional for WooCommerce plugin for WordPress is vulnerable to blind SQL Injection via the `phrase` parameter in all versions up to, and including, 1.3.7.1 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		existing queries that can be used to extract sensitive information from the database.		
CVE-2025-12325	SourceCodester Best Salon Management System forgot-password.php sql injection	A vulnerability has been found in SourceCodester Best Salon Management System 1.0. This affects an unknown part of the file /panel/forgot-password.php. The manipulation of the argument email leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-12308	code-projects Nero Social Networking Site deletemessage.php sql injection	A security flaw has been discovered in code-projects Nero Social Networking Site 1.0. Affected by this issue is some unknown functionality of the file /deletemessage.php. Performing manipulation of the argument message_id results in sql injection. 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-2025-12307	code-projects Nero Social Networking Site addfriend.php sql	A vulnerability was identified in code-projects Nero Social Networking Site 1.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	Affected by this vulnerability is an unknown functionality of the file /addfriend.php. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.		
CVE-2025-12306	code-projects Nero Social Networking Site acceptoffres.php sql injection	A vulnerability was determined in code-projects Nero Social Networking Site 1.0. Affected is an unknown function of the file /acceptoffres.php. This manipulation of the argument 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-2025-12287	Bdtask Wholesale Inventory Control and Inventory Management System edit_profile sql injection	A security vulnerability has been detected in Bdtask Wholesale Inventory Control and Inventory Management System up to 20251013. This impacts an unknown function of the file /Admin_dashboard/edit_profile. Such manipulation of the argument first_name/last_name leads to sql injection. The attack may be launched remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-12226	SourceCodester Best House Rental Management System admin_class.php save_house sql injection	A vulnerability was found in SourceCodester Best House Rental Management System 1.0. Impacted is the function save_house of the file /admin_class.php. Performing manipulation of the argument house_no results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	Patched by core rule	Y

Arbitrary Upload / RCE Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-13574	code-projects Online Bidding System addcategory.php categoryadd unrestricted upload	A weakness has been identified in code-projects Online Bidding System 1.0. This issue affects the function categoryadd of the file /administrator/addcategory.php. This manipulation of the argument catimage causes unrestricted upload. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	Patched by core rule	Y
CVE-2025-13573	projectworlds can pass malicious payloads add_book.php unrestricted upload	A security flaw has been discovered in projectworlds can pass malicious payloads up to 1.0. This vulnerability affects unknown code of the file /add_book.php. The manipulation of the argument image results in unrestricted upload. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	Patched by core rule	Y
CVE-2025-12039	BigBuy Dropshipping Connector for WooCommerce <= 2.0.5 - Unauthenticated IP Spoofing to phpinfo() Exposure	The BigBuy Dropshipping Connector for WooCommerce plugin for WordPress is vulnerable to IP Address Spoofing in all versions up to, and including, 2.0.5 due to insufficient IP address validation and use of user-supplied HTTP headers as a primary method for IP retrieval. This makes it possible for unauthenticated attackers to retrieve the output of phpinfo().	Patched by core rule	Y
CVE-2025-11003	UiPress lite <= 3.5.08 - Missing Authorization to Authenticated (Subscriber+) Stored Cross-Site Scripting	The UiPress lite | Effortless custom dashboards, admin themes and pages plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'uip_save_ui_template' function in all versions up to, and including, 3.5.08. This makes it possible for authenticated attackers, with Subscriber-level access and above, to save templates that contain custom JavaScript.	Patched by core rule	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-13035	Code Snippets <= 3.9.1 - Authenticated (Contributor+) PHP Code Injection via extract() and PHP Filter Chains	The Code Snippets plugin for WordPress is vulnerable to PHP Code Injection in all versions up to, and including, 3.9.1. This is due to the plugin's use of extract() on attacker-controlled shortcode attributes within the `evaluate_shortcode_from_flat_file` method, which can be used to overwrite the `$filepath` variable and subsequently passed to require_once. This makes it possible for authenticated attackers, with Contributor-level access and above, to execute arbitrary PHP code on the server via the `[code_snippet]` shortcode using PHP filter chains granted they can trick an administrator into enabling the "Enable file-based execution" setting and creating at least one active Content snippet.	Patched by core rule	Y
CVE-2025-13145	WP Import – Ultimate CSV XML Importer for WordPress <= 7.33.1 - Authenticated (Administrator+) PHP Object Injection via CSV Import	The WP Import – Ultimate CSV XML Importer for WordPress plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 7.33.1. This is due to deserialization of untrusted data supplied via CSV file imports in the import_single_post_as_csv function within SingleImportExport.php. This makes it possible for authenticated attackers, with administrator-level access or higher, to inject a PHP object. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	Patched by core rule	NA
CVE-2025-7711	Classified Listing – Classified ads & Business Directory Plugin <= 5.0.3 - Authenticated (Subscriber+) Arbitrary Shortcode Execution via Listing Description	The The Classified Listing – Classified ads & Business Directory Plugin plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 5.0.3. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		possible for authenticated attackers, with Subscriber-level access and above, to execute arbitrary shortcodes.		
CVE-2025-13249	Jiusi OA OfficeServer unrestricted upload	A security vulnerability has been detected in Jiusi OA up to 20251102. This affects an unknown function of the file /OfficeServer?isAjaxDownloadTemplate=false of the component OfficeServer Interface. Such manipulation of the argument FileData leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2025-12844	AI Engine <= 3.1.8 - Authenticated (Subscriber+) PHP Object Injection via PHAR Deserialization	The AI Engine plugin for WordPress is vulnerable to PHP Object Injection via PHAR Deserialization in all versions up to, and including, 3.1.8 via deserialization of untrusted input in the 'rest_simpleTranscribeAudio' and 'rest_simpleVisionQuery' functions. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present.	Patched by core rule	Y
CVE-2025-12733	Import any XML, CSV or Excel File to WordPress (WP All Import) <= 3.9.6 - Authenticated (Administrator+) Remote Code Execution via Conditional Logic	The Import any XML, CSV or Excel File to WordPress (WP All Import) plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 3.9.6. This is due to the use of eval() on unsanitized user-supplied input in the pmxi_if function within helpers/functions.php. This makes it possible for authenticated attackers, with import capabilities	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		(typically administrators), to inject and execute arbitrary PHP code on the server via crafted import templates. This can lead to remote code execution.		
CVE-2025-12637	Elastic Theme Editor <= 0.0.3 - Authenticated (Subscriber+) Arbitrary File Upload	The Elastic Theme Editor plugin for WordPress is vulnerable to arbitrary file uploads due to a dynamic code generation feature in the process_theme function in all versions up to, and including, 0.0.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	Patched by core rule	Y
CVE-2025-12813	Holiday class post calendar <= 7.1 - Unauthenticated Remote Code Execution via 'contents'	The Holiday class post calendar plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 7.1 via the 'contents' parameter. This is due to a lack of sanitization of user-supplied data when creating a cache file. This makes it possible for unauthenticated attackers to execute code on the server.	Patched by core rule	Y
CVE-2025-12590	YSlider <= 1.1 - Cross-Site Request Forgery to Stored Cross-Site Scripting	The YSlider plugin for WordPress is vulnerable to Cross-Site Request Forgery to Stored Cross-Site Scripting in all versions up to, and including, 1.1. This is due to missing nonce verification on the content configuration page and insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages via a forged request granted they can trick an administrator into performing an action such as clicking on a link. The injected scripts will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-9334	Better Find and Replace <= 1.7.7 - Authenticated (Subscriber+) Limited Code Injection	The Better Find and Replace – AI-Powered Suggestions plugin for WordPress is vulnerable to Limited Code Injection in all versions up to, and including, 1.7.7. This is due to insufficient input validation and restriction on the 'rtafar_ajax' function. This makes it possible for	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		authenticated attackers, with Subscriber-level access and above, to call arbitrary plugin functions and execute code within those functions.		
CVE-2025-12583	Simple Downloads List <= 1.4.3 - Missing Authorization to Authenticated (Subscriber+) Stored Cross-Site Scripting	The Simple Downloads List plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'wp_ajax_neofix_sdl_edit' AJAX endpoint along with many others in all versions up to, and including, 1.4.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to alter many of the plugin's settings/downloads and inject malicious web scripts.	Patched by core rule	Y
CVE-2025-12563	Blog2Social: Social Media Auto Post & Scheduler <= 8.6.0 - Incorrect Authorization to Video File Upload	The Blog2Social: Social Media Auto Post & Scheduler plugin for WordPress is vulnerable to limited file upload due to an incorrect capability check on theuploadVideo() function in all versions up to, and including, 8.6.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload mp4 files to the 'wp-content/uploads/<YYYY>/<MM>/' directory.	Patched by core rule	Y
CVE-2025-12593	code-projects Simple Online Hotel Reservation System Photo edit_room.php unrestricted upload	A vulnerability was identified in code-projects Simple Online Hotel Reservation System 2.0. The impacted element is an unknown function of the file /admin/edit_room.php of the component Photo Handler. The manipulation leads to unrestricted upload. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2025-10487	Advanced Ads <= 2.0.12 - Unauthenticated Limited Code Execution	The Advanced Ads – Ad Manager & AdSense plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 2.0.12 via the select_one() function. This is due to the endpoint not properly restricting access to the AJAX endpoint or limiting the functions that can be called to safe functions. This makes it possible for unauthenticated	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attackers to call arbitrary functions beginning with get_the_ like get_the_excerpt which can make information exposure possible.		
CVE-2023-7325	Mingyu Operations and Maintenance Audit and Risk Control System xmlrpc.sock SSRF	Anheng Mingyu Operation and Maintenance Audit and Risk Control System up to 2023-08-10 contains a server-side request forgery (SSRF) vulnerability in the xmlrpc.sock handler. The product accepts specially crafted XML-RPC requests that can be used to instruct the server to connect to internal unix socket RPC endpoints and perform privileged XML-RPC methods. An attacker able to send such requests can invoke administrative RPC methods via the unix socket interface to create arbitrary user accounts on the system, resulting in account creation and potential takeover of the bastion host. VulnCheck has observed this vulnerability being exploited in the wild as of 2025-10-30 at 00:30:17.837319 UTC.	Patched by core rule	Y
CVE-2025-62253	CVE-2025-62253 - Open redirect vulnerability in page administration in Liferay Portal 7.4.0 through 7.4.3.97, and old...	Open redirect vulnerability in page administration in Liferay Portal 7.4.0 through 7.4.3.97, and older unsupported versions, and Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions allows remote attackers to redirect users to arbitrary external URLs via the _com_liferay_layout_admin_web_portlet_GroupPagesPortlet_redirect parameter.	Patched by core rule	Y
CVE-2025-12268	LearnHouse Course Thumbnail courses unrestricted upload	A vulnerability has been found in LearnHouse up to 98dfad76aad70711a8113f6c1fdabfccf10509ca. Impacted is an unknown function of the file /api/v1/courses/ of the component Course Thumbnail Handler. The manipulation of the argument thumbnail leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-12223	Bdtask Flight Booking Software Package Information package-information unrestricted upload	A vulnerability was detected in Bdtask Flight Booking Software up to 3.1. This affects an unknown part of the file /b2c/package-information of the component Package Information Module. The manipulation results in unrestricted upload. The attack can be 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.	Patched by core rule	Y
CVE-2025-12222	Bdtask Flight Booking Software Deposit deposit unrestricted upload	A security vulnerability has been detected in Bdtask Flight Booking Software up to 3.1. Affected by this issue is some unknown functionality of the file /admin/transaction/deposit of the component Deposit Handler. The manipulation leads to unrestricted upload. 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-2025-5394	Alone Charity Multipurpose WordPress Theme Arbitrary File Upload	The Alone – Charity Multipurpose Non-profit WordPress Theme theme for WordPress is vulnerable to arbitrary file uploads due to a missing capability check on the alone_import_pack_install_plugin() function in all versions up to, and including, 7.8.3. This makes it possible for unauthenticated attackers to upload zip files containing webshells disguised as plugins from remote locations to achieve remote code execution.	Patched by custom rule	NA
CVE-2024-11972	Hunk Companion WordPress Plugin Improper Authorization on REST API Endpoints	The Hunk Companion WordPress plugin before 1.9.0 does not correctly authorize some REST API endpoints, allowing unauthenticated requests to	Patched by custom rule	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		install and activate arbitrary Hunk Companion WordPress plugin before 1.9.0 from the WordPress.org repo, including vulnerable Hunk Companion WordPress plugin before 1.9.0 that have been closed.		

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-13311	Just Highlight <= 1.0.3 - Authenticated (Administrator+) Stored Cross-Site Scripting via 'Highlight Color' Setting	The Just Highlight plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Highlight Color' setting in all versions up to, and including, 1.0.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the plugin's settings page.	Patched by core rule	Y
CVE-2025-12645	Inline frame – Iframe <= 0.1 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode	The Inline frame – Iframe plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'embedsite' shortcode in all versions up to, and including, 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.	Patched by core rule	Y
CVE-2025-12025	YouTube Subscribe <= 3.0.0 - Authenticated (Admin+) Stored Cross-Site Scripting via Title and Channel ID	The YouTube Subscribe plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	Patched by core rule	Y
CVE-2025-13383	Job Board by BestWebSoft <= 1.2.1 - Cross-Site Request Forgery to Stored Cross-Site Scripting via $_GET Array Storage	The Job Board by BestWebSoft plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 1.2.1. This is due to the plugin storing the entire unsanitized `$_GET`	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		superglobal array directly into the database via `update_user_meta()` when users save search results, and later outputting this data without proper escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that execute whenever a user accesses the saved search or views their profile, granted they can trick the user into performing the search and saving the results.		
CVE-2025-13068	Telegram Bot & Channel <= 4.1 - Unauthenticated Stored Cross-Site Scripting via Telegram Username	The Telegram Bot & Channel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Telegram username in all versions up to, and including, 4.1 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-2025-11186	Cookie Notice & Compliance for GDPR / CCPA <= 2.5.8 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode	The Cookie Notice & Compliance for GDPR / CCPA plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's cookies_accepted shortcode in all versions up to, and including, 2.5.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-12935	FluentCRM - Marketing Automation For WordPress <= 2.9.84 - Authenticated (Contributor+) Stored Cross-Site Scripting via 'fluentcrm_content' Shortcode	The FluentCRM – Email Newsletter, Automation, Email Marketing, Email Campaigns, Optins, Leads, and CRM Solution plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'fluentcrm_content' shortcode in all versions up to, and including, 2.9.84 due to insufficient input sanitization and output escaping on user supplied attributes. 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-2025-12160	Simple User Registration <= 6.6 - Unauthenticated Stored Cross-Site Scripting	The Simple User Registration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpr_admin_msg' parameter in all versions up to, and including, 6.6 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-2025-12066	WP Delete Post Copies <= 6.0.2 - Authenticated (Admin+) Stored Cross-Site Scripting	The WP Delete Post Copies plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 6.0.2 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-2025-12964	Magical Products Display <= 1.1.29 - Authenticated (Contributor+) Stored Cross-Site Scripting via MPD Pricing Table Widget	The Magical Products Display plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'mpdpr_title_tag' and 'mpdpr_subtitle_tag' parameters in the MPD Pricing Table widget in all versions up to, and including, 1.1.29 due to insufficient input sanitization and output escaping on user-supplied HTML tag names. 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-2025-11808	Shortcode for Google Street View <= 0.5.7 - Authenticated (Contributor+) Stored	The Shortcode for Google Street View plugin for WordPress is vulnerable to Stored Cross-Site Scripting	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Cross-Site Scripting via Shortcode	via the 'streetview' shortcode in all versions up to, and including, 0.5.7. 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 inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-13141	HT Mega – Absolute Addons For Elementor <= 3.0.0 - Authenticated (Contributor+) Stored Cross-Site Scripting via Tag Attribute Injection	The HT Mega – Absolute Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Gutenberg blocks in all versions up to, and including, 3.0.0 due to insufficient input validation on user-supplied HTML tag names. This is due to the lack of a tag name whitelist allowing dangerous tags like 'script', 'iframe', and 'object' to be injected even though tag_escape() is used for sanitization. While some blocks use esc_html() for content, this can be bypassed using JavaScript encoding techniques (unquoted strings, backticks, String.fromCharCode()). 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-2025-11826	WP Company Info <= 1.9.0 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode	The WP Company Info plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'class' attribute of the 'social-networks' shortcode in all versions up to, and including, 1.9.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-11803	WPSite Shortcode <= 1.2 - Authenticated (Contributor+) Stored Cross-Site Scripting	The WPSite Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'format' shortcode attribute in the wpsite_y shortcode and the 'before'	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attribute in the wpsite_postauthor shortcode in all versions up to, and including, 1.2. This is due to insufficient input sanitization and output escaping in error messages. 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-2025-11800	Surbma | MiniCRM Shortcode <= 2.0 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Surbma | MiniCRM Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' shortcode attribute of the 'minicrm' shortcode in all versions up to, and including, 2.0. 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-2025-11802	Bulma Shortcodes <= 1.0 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Bulma Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'type' shortcode attribute in the bulma-notification shortcode in all versions up to, and including, 1.0. 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-2025-11763	Display Pages Shortcode <= 1.1 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Display Pages Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'column_count' parameter in the [display-pages] shortcode in all versions up to, and including, 1.1. 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		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		whenever a user accesses an injected page.		
CVE-2025-11764	Shortcodes Bootstrap <= 1.1 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Shortcodes Bootstrap plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'type' parameter in the [notification] shortcode in all versions up to, and including, 1.1. This is due to missing 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-2025-11799	Affiliate AI Lite <= 1.0.1 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Affiliate AI Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'asin' shortcode attribute in the affiai_img shortcode in all versions up to, and including, 1.0.1. 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-2025-13159	Flo Forms – Easy Drag & Drop Form Builder <= 1.0.43 - Unauthenticated Stored Cross-Site Scripting via SVG Upload	The Flo Forms – Easy Drag & Drop Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG file uploads in all versions up to, and including, 1.0.43. This is due to the plugin allowing SVG file uploads via an unauthenticated AJAX endpoint (`flo_form_submit`) without proper file content validation. This makes it possible for unauthenticated attackers to upload malicious SVG files containing JavaScript that executes when an administrator views the uploaded file in the WordPress admin interface, leading to potential full site compromise.	Patched by core rule	Y
CVE-2025-12135	WPBookit <= 1.0.6 - Unauthenticated Stored Cross-Site Scripting	The WPBookit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'css_code' parameter in all versions up to, and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		including, 1.0.6 due to a missing capability check on the save_custome_code() function. 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-2025-11885	EchBay Admin Security <= 1.3.0 - Reflected Cross-Site Scripting	The EchBay Admin Security plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the '_ebnonce' parameter in all versions up to, and including, 1.3.0 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-2025-11768	Islamic Phrases <= 2.12.2015 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Islamic Phrases plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'phrases' shortcode attribute in all versions up to, and including, 2.12.2015. 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-2025-11770	BrightTALK WordPress Shortcode <= 2.4.0 - Authenticated (Contributor+) Stored Cross-Site Scripting	The BrightTALK WordPress Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'format' shortcode attribute in the brighttalk-time shortcode in all versions up to, and including, 2.4.0. 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-2025-11767	Tips Shortcode <= 0.2.1 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Tips Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tip' shortcode in all versions up to, and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		including, 0.2.1. 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.		
CVE-2025-11801	AudioTube <= 0.0.3 - Authenticated (Contributor+) Stored Cross-Site Scripting	The AudioTube plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'caption' shortcode attribute of the 'audiotube' shortcode in all versions up to, and including, 0.0.3. 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-2025-11765	Stock Tools <= 1.1 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Stock Tools plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'image_height' and 'image_width' shortcode attributes in all versions up to, and including, 1.1. 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-2025-12661	Pollcaster Shortcode Plugin <= 1.0 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode	The Pollcaster Shortcode Plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'height' parameter in the 'pollcaster' shortcode in all versions up to, and including, 1.0. 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-2025-12660	Padlet Shortcode <= 1.3 - Authenticated	The Padlet Shortcode plugin for WordPress is vulnerable	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	(Contributor+) Stored Cross-Site Scripting via Shortcode	to Stored Cross-Site Scripting via the 'key' parameter in the 'wallwisher' shortcode in all versions up to, and including, 1.3. 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.		
CVE-2025-12746	Tainacan <= 1.0.0 - Reflected Cross-Site Scripting	The Tainacan plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'search' parameter in all versions up to, and including, 1.0.0 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-2025-5092	Multiple Plugins and Themes <= (Various Versions) - Authenticated (Contributor+) DOM-Based Stored Cross-Site Scripting via lightGallery JavaScript Library	Multiple plugins and/or themes for WordPress are vulnerable to Stored Cross-Site Scripting via the plugin's bundled lightGallery library (<= 2.8.3) in various versions due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-13206	GiveWP - Donation Plugin and Fundraising Platform <= 4.13.0 - Unauthenticated Stored Cross-Site Scripting via 'name'	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘name’ parameter in all versions up to, and including, 4.13.0 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. Avatars must be enabled in the WordPress install in order to exploit the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability.		
CVE-2025-12484	Giveaways and Contests by RafflePress – Get More Website Traffic, Email Subscribers, and Social Followers <= 1.12.19 - Unauthenticated Stored Cross-Site Scripting	The Giveaways and Contests by RafflePress – Get More Website Traffic, Email Subscribers, and Social Followers plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple social media username parameters in all versions up to, and including, 1.12.19 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-2025-12878	FunnelKit – Funnel Builder for WooCommerce Checkout <= 3.13.1.2 - Authenticated (Contributor+) Stored Cross-Site Scripting via wfop_phone Shortcode	The FunnelKit – Funnel Builder for WooCommerce Checkout plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `wfop_phone` shortcode in all versions up to, and including, 3.13.1.2. This is due to insufficient input sanitization and output escaping on the user-supplied `default` 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-2025-13054	User Profile Builder – Beautiful User Registration Forms, User Profiles & User Role Editor <= 3.14.8 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode	The User Profile Builder – Beautiful User Registration Forms, User Profiles & User Role Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wppb-embed shortcode in all versions up to, and including, 3.14.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-12710	Pet-Manager – Petfinder <= 3.6.1 - Authenticated (Contributor+) Stored Cross-Site Scripting via kwm-petfinder Shortcode	The Pet-Manager – Petfinder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the kwm-petfinder shortcode in all	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		versions up to, and including, 3.6.1 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.		
CVE-2025-6251	Royal Elementor Addons and Templates <= 1.7.1036 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via $item['field_id'] in all versions up to, and including, 1.7.1036 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-2025-12457	Enable SVG, WebP, and ICO Upload <= 1.1.2 - Authenticated (Author+) Stored Cross-Site Scripting via SVG File Uploads	The Enable SVG, WebP, and ICO Upload plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.1.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	Patched by core rule	Y
CVE-2025-12691	Photonic Gallery & Lightbox for Flickr, SmugMug & Others <= 3.21 - Authenticated (Contributor+) Stored Cross-Site Scripting via Caption Attribute	The Photonic Gallery & Lightbox for Flickr, SmugMug & Others plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's lightbox functionality in all versions up to, and including, 3.21 due to insufficient input sanitization and output escaping on user supplied caption 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 the injected page.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-13196	Element Pack Addons for Elementor <= 8.3.4 - Authenticated (Contributor+) Stored Cross-Site Scripting via Open Street Map widget	The Element Pack Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Open Street Map widget's marker content parameter in all versions up to, and including, 8.3.4. This is due to insufficient input sanitization and output escaping on user-supplied attributes in the render function. 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-2025-4212	Checkout Files Upload for WooCommerce <= 2.2.1 - Unauthenticated Stored Cross-Site Scripting	The Checkout Files Upload for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via file uploads in all versions up to, and including, 2.2.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in image files that will execute whenever a user accesses the injected page.	Patched by core rule	Y
CVE-2025-11868	everviz <= 1.1 - Authenticated (Contributor+) Stored Cross-Site Scripting	The everviz plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `everviz` shortcode attributes in versions up to, and including, 1.1. This is due to the plugin not properly sanitizing user input or escaping output when building a `<div id=...>` from the `type` and `hash` 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-2025-8609	RTMKit Addons <= 1.6.5 - Authenticated (Contributor+) Stored Cross-Site Scripting via Accordion Repeater Block Attribute	The RTMKit Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Accordion Block's attributes in all versions up to, and including, 1.6.1 due to insufficient input sanitization and output escaping on user supplied attributes. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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-2025-13245	code-projects Student Information System editprofile.php cross site scripting	A vulnerability was identified in code-projects Student Information System 2.0. The impacted element is an unknown function of the file /editprofile.php. Such manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2025-13244	code-projects Student Information System register.php cross site scripting	A vulnerability was determined in code-projects Student Information System 2.0. The affected element is an unknown function of the file /register.php. 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-2025-13202	code-projects Simple Cafe Ordering System add_to_cart cross site scripting	A security flaw has been discovered in code-projects Simple Cafe Ordering System 1.0. This affects an unknown part of the file /add_to_cart. Performing manipulation of the argument product_name 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-2025-13186	Bdtask/CodeCanyon Isshue Multi Store eCommerce Shopping Cart Solution manage_customer cross site scripting	A weakness has been identified in Bdtask/CodeCanyon Isshue Multi Store eCommerce Shopping Cart Solution up to 4.0. This impacts an unknown function of the file /dashboard/Ccustomer/manage_customer. This manipulation of the argument Search causes cross site scripting. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-13182	pojoin h3blog addtitle cross site scripting	A vulnerability was identified in pojoin h3blog 1.0. The impacted element is an	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown function of the file /admin/cms/category/addtitle. The manipulation of the argument Title leads to cross site scripting. The attack can be initiated remotely. The exploit is publicly available and might be used.		
CVE-2025-13181	pojoin h3blog add cross site scripting	A vulnerability was determined in pojoin h3blog 1.0. The affected element is an unknown function of the file /admin/cms/material/add. Executing manipulation of the argument Name can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-12904	SNORDIAN's H5PxAPIkatchu <= 0.4.17 - Unauthenticated Stored Cross-Site Scripting via insert_data	The SNORDIAN's H5PxAPIkatchu plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'insert_data' AJAX endpoint in all versions up to, and including, 0.4.17 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-2025-11769	WordPress Content Flipper <= 0.1 - Authenticated (Contributor+) Stored Cross-Site Scripting	The WordPress Content Flipper plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'bgcolor' shortcode attribute of the 'flipper_front' shortcode in all versions up to, and including, 0.1. 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-2025-11994	Easy Email Subscription <= 1.3 - Unauthenticated Stored Cross-Site Scripting	The Easy Email Subscription plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'name' parameter in all versions up to, and including, 1.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		in pages that will execute whenever a user accesses an injected page.		
CVE-2025-12018	MembershipWorks <= 6.14 - Authenticated (Admin+) Stored Cross-Site Scripting	The MembershipWorks – Membership, Events & Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 6.14 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-2025-12667	GitHub Gist Shortcode Plugin <= 0.2 - Authenticated (Contributor+) Stored Cross-Site Scripting	The GitHub Gist Shortcode Plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter of the 'gist' shortcode in all versions up to, and including, 0.2 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-2025-12651	Live Photos on WordPress <= 0.1 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode	The Live Photos on WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'video_src', 'img_src', and 'class' parameters in the livephotos_photo shortcode in all versions up to, and including, 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 when a user accesses an injected page.	Patched by core rule	Y
CVE-2025-12019	Featured Image <= 2.1 - Authenticated (Admin+) Stored Cross-Site Scripting	The Featured Image plugin for WordPress is vulnerable to Stored Cross-Site Scripting via image metadata in all	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		versions up to, and including, 2.1 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.		
CVE-2025-12662	Coon Google Maps <= 1.0 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode	The Coon Google Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'height' parameter in the 'map' shortcode in all versions up to, and including, 1.0. 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-2025-11129	Include fussball.de Widgets <= 4.0.0 - Authenticated (Contributor+) Stored Cross-Site Scripting via 'api' and 'type'	The Include Fussball.de Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'api' and 'type' parameters in all versions up to, and including, 4.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-11882	Simple Donate <= 1.0 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Simple Donate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's simpledonate 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		whenever a user accesses an injected page.		
CVE-2025-12663	Jeba Cute forkit <= 1.0 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode	The Jeba Cute forkit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'text' parameter in the 'jeba_forkit' shortcode in all versions up to, and including, 1.0. 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-2025-11860	Twitter Feed <= 1.3.1 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Twitter Feed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ottwitter_feed' shortcode in all versions up to, and including, 1.3.1. This is due to the plugin not properly sanitizing user input and output of the 'width' and 'height' parameters. 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-2025-11821	Woocommerce – Products By Custom Tax <= 2.2 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode	The Woocommerce – Products By Custom Tax plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'woo_products_custom_tax' shortcode in all versions up to, and including, 2.2. 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-2025-12668	WP Count Down Timer <= 1.0.1 - Authenticated (Contributor+) Stored Cross-Site Scripting	The WP Count Down Timer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple parameters of the 'wp_countdown_timer' shortcode in all versions up to, and including, 1.0.1 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-2025-12658	Preload Current Images <= 1.3 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode	The Preload Current Images plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'complete' parameter in the 'preload_progress_bar' shortcode in all versions up to, and including, 1.3. 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-2025-11859	Paypal Donation Shortcode <= 0.1 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Paypal Donation Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'paypal' shortcode in all versions up to, and including, 0.1. This is due to the plugin not properly sanitizing user input and output of the 'title' and 'text' parameters. 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-2025-12671	WP-Iconics <= 0.0.4 - Authenticated (Contributor+) Stored Cross-Site Scripting	The WP-Iconics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple parameters of the 'wp_iconics' shortcode in all versions up to, and including, 0.0.4 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-2025-11869	Precise Columns <= 1.0 - Authenticated	The Precise Columns plugin for WordPress is vulnerable	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	(Contributor+) Stored Cross-Site Scripting	to Stored Cross-Site Scripting via the `wrap_id` shortcode attribute in all versions up to, and including, 1.0. This is due to the plugin not properly sanitizing user input or escaping output when inserting the wrapper ID into the generated 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.		
CVE-2025-11828	Magazine Companion <= 1.2.3 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Magazine Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'headerHtmlTag' attribute in the bnm-blocks/featured-posts-1 block in all versions up to, and including, 1.2.3. This is due to insufficient input sanitization and output escaping when using user-supplied values as HTML tag names. 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-2025-12711	Share to Google Classroom <= 1.0 - Authenticated (Contributor+) Stored Cross-Site Scripting via share_to_google Shortcode	The Share to Google Classroom plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the share_to_google 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-2025-11856	Eventbee Ticketing Widget <= 1.0 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Eventbee Ticketing Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'eventbeeticketwidget' shortcode in all versions up to, and including, 1.0. This is due to the plugin not properly sanitizing user input and output of several parameters. 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-2025-12021	WP-OAuth <= 0.4.1 - Reflected Cross-Site Scripting	The WP-OAuth plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'error_description' parameter in all versions up to, and including, 0.4.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-12020	Double the Donation <= 2.0.0 - Authenticated (Admin+) Stored Cross-Site Scripting	The Double the Donation – A workplace giving tool to help your fundraising efforts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	Patched by core rule	Y
CVE-2025-12672	Flickr Show <= 1.5 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Flickr Show plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'div_height' parameter of the 'flickrshow' shortcode in all versions up to, and including, 1.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-12754	Geopost <= 1.2 - Authenticated (Contributor+) Stored	The Geopost plugin for WordPress is vulnerable to Stored Cross-Site Scripting	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Cross-Site Scripting via Shortcode	via the 'height' parameter of the 'geopost' shortcode in all versions up to, and including, 1.2. 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.		
CVE-2025-11805	Skip to Timestamp <= 1.4.4 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode	The Skip to Timestamp plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'skipto' shortcode in all versions up to, and including, 1.4.4. This is due to insufficient input sanitization and output escaping on the 'time' 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-2025-12644	Nonaki – Drag and Drop Email Template builder and Newsletter plugin for WordPress <= 1.0.11 - Authenticated (Contributor+) Stored Cross-Site Scripting via Custom Fields	The Nonaki – Drag and Drop Email Template builder and Newsletter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'nonaki' shortcode in all versions up to, and including, 1.0.11. This is due to insufficient input sanitization and output escaping on user supplied custom field values that are retrieved and rendered by the shortcode. 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-2025-11863	My Geo Posts Free <= 1.2 - Authenticated (Contributor+) Stored Cross-Site Scripting	The My Geo Posts Free plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'mygeo_city' shortcode in all versions up to, and including, 1.2. This is due to the plugin not properly sanitizing user input or escaping output of the 'default' shortcode attribute. 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-2025-11829	Five9 Live Chat <= 1.1.2 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Five9 Live Chat plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'toolbar' attribute of the [five9-chat] shortcode in all versions up to, and including, 1.1.2. 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-2025-12652	Ungapped Widgets <= 1 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode	The Ungapped Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'prefillvalues' parameter in the ungapped-form shortcode in all versions up to, and including, 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 when a user accesses an injected page.	Patched by core rule	Y
CVE-2025-11873	WP BBCode <= 1.8.1 - Authenticated (Contributor+) Stored Cross-Site Scripting	The WP BBCode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'url' shortcode in all versions up to, and including, 1.8.1 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-2025-11822	WP Bootstrap Tabs <= 1.0.4 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode	The WP Bootstrap Tabs plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'bootstrap_tab' shortcode in all versions up to, and including, 1.0.4. This is due to insufficient input	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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-2025-12920	qianfox FoxCMS Product.php edit cross site scripting	A flaw has been found in qianfox FoxCMS up to 1.2.16. Affected by this vulnerability is the function add/edit of the file app/admin/controller/Product.php. This manipulation of the argument Title causes cross site scripting. It is possible to initiate the attack 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-2025-12837	aThemes Addons for Elementor <= 1.1.5 - Authenticated (Contributor+) Stored Cross-Site Scripting via Call To Action Widget	The aThemes Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Call To Action widget in versions up to, and including, 1.1.5 due to insufficient input sanitization and output escaping on user-supplied values. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-12643	Saphali LiqPay for donate <= 1.0.2 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode	The Saphali LiqPay for donate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'saphali_liqpay' shortcode in all versions up to, and including, 1.0.2. 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-2025-12125	HTML Forms <= 1.5.5 - Authenticated (Admin+) Stored Cross-Site	The HTML Forms – Simple WordPress Forms Plugin plugin for WordPress is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Scripting	vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.5.5 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-2025-12112	Insert Headers and Footers Code – HT Script <= 1.1.6 - Authenticated (Author+) Stored Cross-Site Scripting	The Insert Headers and Footers Code – HT Script plugin for WordPress is vulnerable to Stored Cross-Site Scripting via adding scripts in all versions up to, and including, 1.1.6 due to insufficient capability checks. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-12193	Mang Board WP <= 2.3.1 - Reflected Cross-Site Scripting	The Mang Board WP plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'mp' parameter in all versions up to, and including, 2.3.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-12064	WP2Social Auto Publish <= 2.4.7 - Reflected Cross-Site Scripting via PostMessage	The WP2Social Auto Publish plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via PostMessage in all versions up to, and including, 2.4.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-12520	WP Airbnb Review Slider <= 4.2 - Authenticated (Admin+) Stored Cross-Site Scripting	The WP Airbnb Review Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 4.2 due to insufficient URL validation that allows users to pull in a malicious HTML file. 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-2025-11268	Strong Testimonials <= 3.2.16 - Unauthenticated Arbitrary Shortcode Execution	The Strong Testimonials plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 3.2.16. This is due to the software allowing users to submit a testimonial in which a value is not properly validated or sanitized prior to being passed to a do_shortcode call. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes if an administrator previews or publishes a crafted testimonial.	Patched by core rule	Y
CVE-2025-12471	Hubbub Lite <= 1.36.0 - Reflected Cross-Site Scripting	The Hubbub Lite – Fast, free social sharing and follow buttons plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'dpsp_list_attention_search' parameter in all versions up to, and including, 1.36.0 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-2025-11820	Graphina – Elementor Charts and Graphs <= 3.1.8 - Authenticated (Contributor+) Stored Cross-Site Scripting via Chart Widgets	The Graphina – Elementor Charts and Graphs plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple chart widgets in all versions up to, and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		including, 3.1.8 due to insufficient input sanitization and output escaping on data 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. The vulnerability affects multiple chart widgets including Area Chart, Line Chart, Column Chart, Donut Chart, Heatmap Chart, Radar Chart, Polar Chart, Pie Chart, Radial Chart, and Advance Data Table widgets.		
CVE-2025-11162	Spectra <= 2.19.14 - Authenticated (Contributor+) Stored Cross-Site Scripting via Custom CSS	The Spectra Gutenberg Blocks – Website Builder for the Block Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Custom CSS in all versions up to, and including, 2.19.14 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-2025-12580	SMS for WordPress <= 1.1.8 - Reflected Cross-Site Scripting	The SMS for WordPress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'paged' parameter in all versions up to, and including, 1.1.8 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-2025-12045	Orbit Fox Companion <= 3.0.2 - Authenticated (Author+) Stored Cross-Site Scripting via Post Taxonomy	The Orbit Fox: Duplicate Page, Menu Icons, SVG Support, Cookie Notice, Custom Fonts & More plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the category and tag 'name' parameters in all versions up to, and including, 3.0.2 due to insufficient input sanitization and output escaping. This makes it possible for	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-11812	Reuse Builder <= 1.7 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode	The Reuse Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'reuse_builder_single_post_title' shortcode in all versions up to, and including, 1.7. This is due to insufficient input sanitization and output escaping on the 'style' 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-2025-11733	Footnotes Made Easy <= 3.0.7 - Unauthenticated Stored Cross-Site Scripting	The Footnotes Made Easy plugin for WordPress is vulnerable to Stored Cross-Site Scripting via plugin settings in all versions up to, and including, 3.0.7 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-2025-12369	Extensions for Leaflet Map <= 4.7 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Extensions for Leaflet Map plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `geojsonmarker` shortcode in all versions up to, and including, 4.7. 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-2025-12324	TablePress – Tables in WordPress made easy <= 3.2.4 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode Attributes	The TablePress – Tables in WordPress made easy plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `table` shortcode attributes in all versions up to, and including, 3.2.3 due to insufficient input sanitization	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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-2025-11841	Greenshift – animation and page builder blocks <= 12.2.7 - Authenticated (Contributor+) Stored Cross-Site Scripting via Chart Data Attributes	The Greenshift – animation and page builder blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Chart Data attributes in all versions up to, and including, 12.2.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-11502	Schema & Structured Data for WP & AMP <= 1.51 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Schema & Structured Data for WP & AMP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'saswp_tiny_multiple_faq' shortcode in all versions up to, and including, 1.51 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-2025-12090	Employee Spotlight – Team Member Showcase & Meet the Team Plugin <= 5.1.2 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Employee Spotlight – Team Member Showcase & Meet the Team Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Social URLs in all versions up to, and including, 5.1.2 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
CVE-2025-11927	Flying Images: Optimize and Lazy Load Images for	The Flying Images: Optimize and Lazy Load Images for	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Faster Page Speed <= 2.4.14 - Authenticated (Admin+) Stored Cross-Site Scripting	Faster Page Speed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.4.14 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-2025-12118	Schema Scalpel <= 1.6.1 - Authenticated (Contributor+) Stored Cross-Site Scripting via Post Title in JSON-LD Schema	The Schema Scalpel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the post title in all versions up to, and including, 1.6.1 due to insufficient input sanitization and output escaping when outputting user-supplied data into JSON-LD schema markup. 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-2025-11995	Community Events <= 1.5.2 - Unauthenticated Stored Cross-Site Scripting	The Community Events plugin for WordPress is vulnerable to Stored Cross-Site Scripting via event details parameter in all versions up to, and including, 1.5.2 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-2025-11928	CSS & JavaScript Toolbox <= 12.0.5 - Authenticated (Admin+) Stored Cross-Site Scripting	The CSS & JavaScript Toolbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 12.0.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions 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. This only affects multi-site installations and installations where unfiltered_html has been disabled.		
CVE-2025-11922	Inactive Logout <= 3.5.5 - Authenticated (Subscriber+) Stored Cross-Site Scripting	The Inactive Logout plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ina_redirect_page_individual_user' parameter in all versions up to, and including, 3.5.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-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-2025-12547	LogicalDOC Community Edition Admin Login login.jsp excessive authentication	A vulnerability was identified in LogicalDOC Community Edition up to 9.2.1. This vulnerability affects unknown code of the file /login.jsp of the component Admin Login Page. Such manipulation leads to improper restriction of excessive authentication attempts. The attack can be executed remotely. This attack is characterized by high complexity. It is stated that the exploitability is difficult. 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-2025-12546	LogicalDOC Community Edition API Key creation UI cross site scripting	A vulnerability was determined in LogicalDOC Community Edition up to 9.2.1. This affects an unknown part of the component API Key creation UI. This manipulation causes cross site scripting. 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-2025-62267	CVE-2025-62267 - Multiple cross-site scripting (XSS) vulnerabilities in web	Multiple cross-site scripting (XSS) vulnerabilities in web content template's select structure page in Liferay	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	content template's select structure page ...	Portal 7.4.3.35 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.10, 2023.Q3.1 through 2023.Q3.10, 7.4 update 35 through update 92 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.		
CVE-2025-62264	CVE-2025-62264 - Reflected cross-site scripting (XSS) vulnerability in Languauge Override in Liferay Portal 7.4.3.8 t...	Reflected cross-site scripting (XSS) vulnerability in Languauge Override in Liferay Portal 7.4.3.8 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.10, 2023.Q3.1 through 2023.Q3.10, and 7.4 update 4 through update 92 allows remote attackers to inject arbitrary web script or HTML via the `_com_liferay_portal_language_override_web_internal_portlet_PLOPortlet_selectedLanguageId` parameter.	Patched by core rule	Y
CVE-2025-11806	Qzzr Shortcode Plugin <= 1.0.1 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode	The Qzzr Shortcode Plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'qzzr' shortcode in all versions up to, and including, 1.0.1. This is due to insufficient input sanitization and output escaping on the 'quiz' 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-2025-62265	CVE-2025-62265 - Cross-site scripting (XSS) vulnerability in the Blogs widget in Liferay Portal 7.4.0 through 7.4.3.1...	Cross-site scripting (XSS) vulnerability in the Blogs widget in Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.10, 2023.Q3.1 through 2023.Q3.8, 7.4 GA through update 92, 7.3 GA through update 36, and older unsupported versions allows remote attackers to inject arbitrary web script or HTML via a crafted <iframe> injected into a blog entry's "Content" text field The Blogs widget in Liferay DXP does not add the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		sandbox attribute to <iframe> elements, which allows remote attackers to access the parent page via scripts and links in the frame page.		
CVE-2025-12475	Blocksy Companion <= 2.1.14 - Authenticated (Contributor+) Stored Cross-Site Scripting	The Blocksy Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'blocksy_newsletter_subscribe' shortcode in all versions up to, and including, 2.1.14 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-2025-62263	CVE-2025-62263 - Multiple cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.3.7 through 7.4.3.103, and L...	Multiple cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.3.7 through 7.4.3.103, and Liferay DXP 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, 7.3 service pack 3 through update 36 allow remote attackers to inject arbitrary web script or HTML via a crafted payload injected into an Account Role's "Title" text field to (1) view account role page, or (2) select account role page. Multiple cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.3.7 through 7.4.3.103, and Liferay DXP 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, 7.3 service pack 3 through update 36 allow remote attackers to inject arbitrary web script or HTML via a crafted payload injected into an Organization's "Name" text field to (1) view account page, (2) view account organization page, or (3) select account organization page.	Patched by core rule	Y
CVE-2025-12269	LearnHouse Account Setting previews cross site scripting	A vulnerability was found in LearnHouse up to 98dfad76aad70711a8113f6c1fdabfccf10509ca. The affected element is an unknown function of the file /dash/org/settings/previews of the component Account	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Setting Page. The manipulation results in cross site scripting. It is possible to launch the attack remotely. The exploit has been made public and could be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-12251	OpenWGA Admin UI cross site scripting	A vulnerability has been found in OpenWGA 7.11.12 Build 737. This impacts an unknown function of the component Admin UI. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-12244	code-projects Simple E-Banking System register.php cross site scripting	A vulnerability was determined in code-projects Simple E-Banking System 1.0. This affects an unknown part of the file /eBank/register.php. Executing manipulation of the argument Username can lead to cross site scripting. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y

INDUSFACE™

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

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

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

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