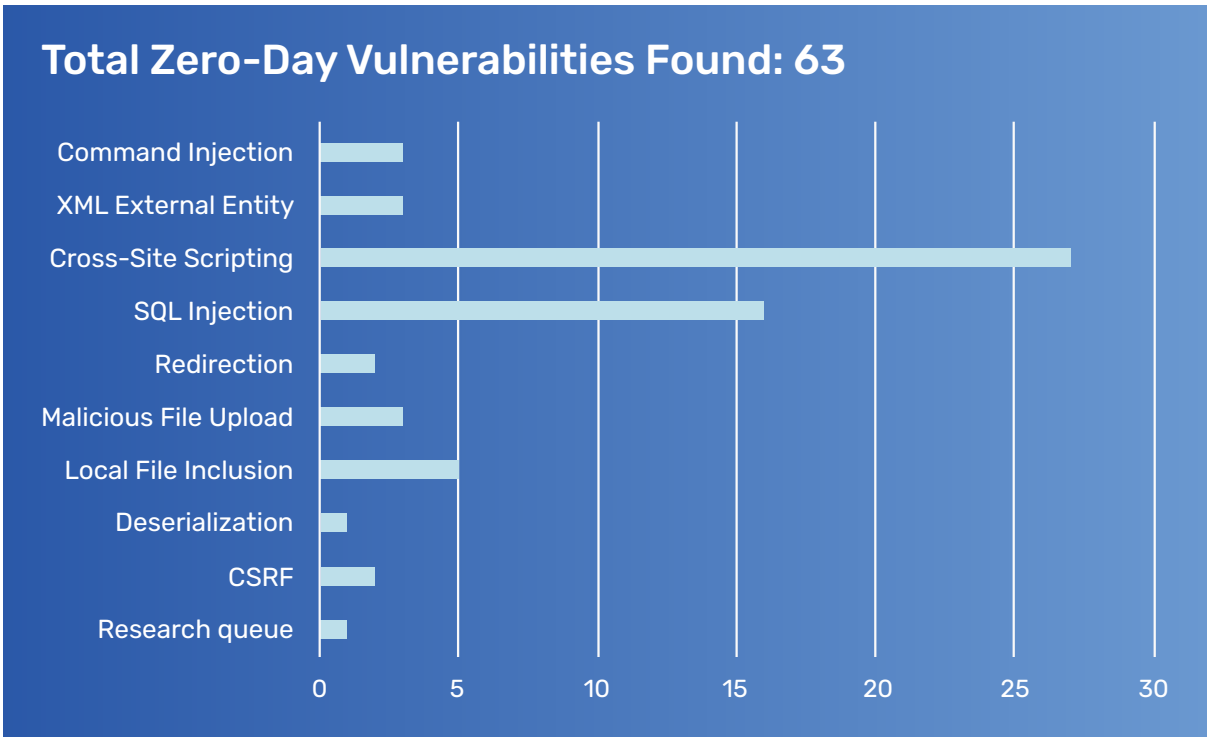
INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

January 2022

Total Zero-Day Vulnerabilities Found: 63



Zero-Day vulnerabilities protected through core rules	55
Zero-Day vulnerabilities protected through custom rules	7*
Zero-Day vulnerabilities for which protection cannot be determined	1**
Zero-Day vulnerabilities found by Indusface WAS	55

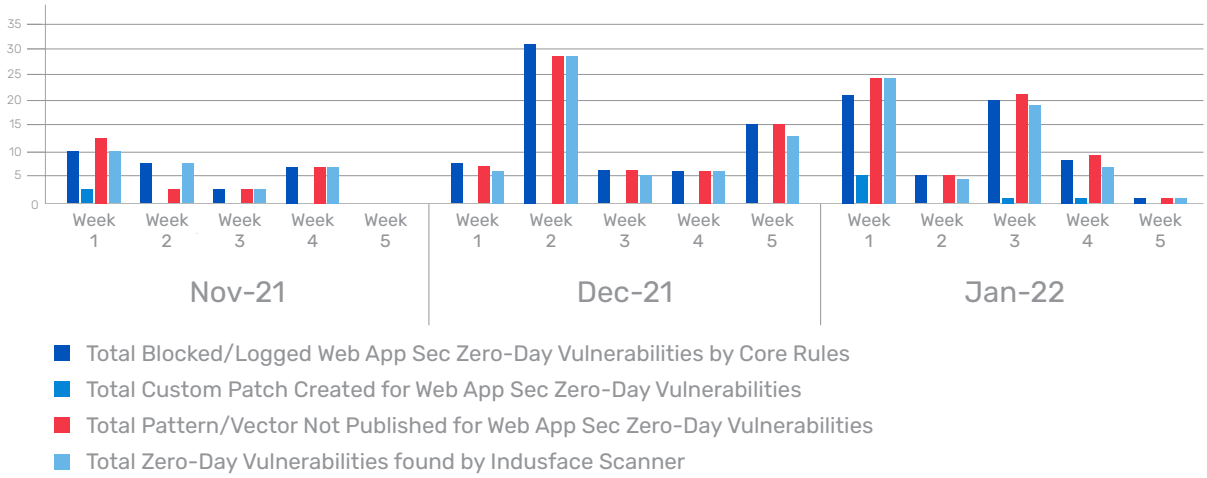
* To enable the custom rules, please contact support@indusface.com

** Since the attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.

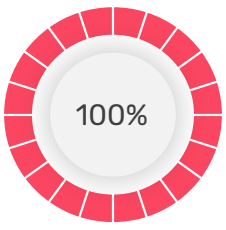
Vulnerability Trend:

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

Weekly Vulnerability Trend

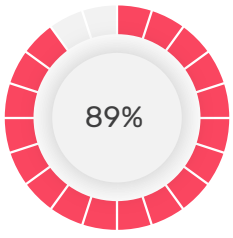


- Total Blocked/Logged Web App Sec Zero-Day Vulnerabilities by Core Rules
- Total Custom Patch Created for Web App Sec Zero-Day Vulnerabilities
- Total Pattern/Vector Not Published for Web App Sec Zero-Day Vulnerabilities
- Total Zero-Day Vulnerabilities found by Indusface Scanner

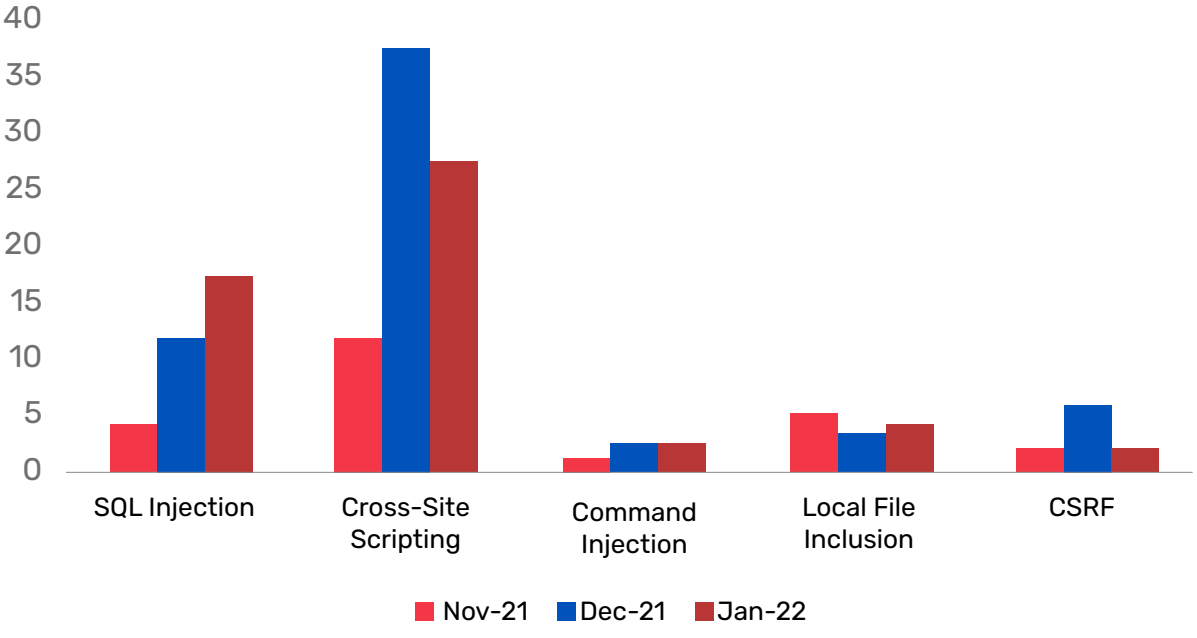


of the zero-day vulnerabilities were protected by the **core rules** in the last quarter

None of the zero-day vulnerabilities were protected by the **custom rules** in the last quarter



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



Note: Our Sig-Dev team constantly monitors the security landscape and leading security websites to identify any new vulnerabilities identified/published and monitors/updates rules to ensure round-the-clock protection for customer sites.

Vulnerability Details:

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
1	Local File Inclusion	CVE-2021-3845	ws-scrcpy file inclusion [CVE-2021-3845]	A vulnerability classified as problematic has been found in ws-scrcpy. Affected is some unknown functionality. Applying the patch e83cf65438be-f83a3503b25358b-ba97bcc156fef can eliminate this problem.	Protected by core rules.	Detected by the scanner as the Local File Inclusion attack.
		CVE-2022-21682	Flatpak up to 1.10.5/1.12.2 path traversal [CVE-2022-21682]	A vulnerability was found in Flatpak up to 1.10.5/1.12.2. It has been declared as critical. Affected by this vulnerability is an unknown code. Upgrading to version 1.10.6 or 1.12.3 eliminates this vulnerability. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by core rules.	Detected by the scanner as the Local File Inclusion attack.
		CVE-2021-46104	webp_server_go 0.4.0 pathname traversal [CVE-2021-46104]	A vulnerability has been found in webp_server_go 0.4.0 and classified as problematic. Affected by this vulnerability is an unknown code block. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the Local File Inclusion attack.
		CVE-2021-46203	Taocms 3.0.2 path path traversal	A vulnerability has been found in Taocms 3.0.2 and classified as problematic. This vulnerability affects an unknown function. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the Local File Inclusion attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2021-34805	Land FAUST iServer prior 9.0.019.019.7 URL Request path traversal	A vulnerability has been found in Land FAUST iServer and classified as critical. This vulnerability affects an unknown function of the component. Upgrading to version 9.0.019.019.7 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Local File Inclusion attack.
2	Command Injection	CVE-2021-32650	October CMS up to 1.0.472/1.1.5 Theme Import injection	A vulnerability has been found in October CMS up to 1.0.472/1.1.5 and classified as critical. Affected by this vulnerability is an unknown code of the component. Upgrading to version 1.0.473 or 1.1.6 eliminates this vulnerability. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by core rules.	Detected by the scanner as the Command Injection attack.
		CVE-2021-32649	October CMS up to 1.0.472/1.1.5 Twig Code injection	A vulnerability, which was classified as critical, was found in October CMS up to 1.0.472/1.1.5. Affected is an unknown part of the component. Upgrading to version 1.0.473 or 1.1.6 eliminates this vulnerability. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by core rules.	Detected by the scanner as the Command Injection attack.
		CVE-2020-28885	Liferay Portal Server 7.2.0 GA1/7.3.5 GA6 Gogo Shell os command injection	A vulnerability, which was classified as critical, has been found in Liferay Portal Server 7.3.5 GA6/7.2.0 GA1. This issue affects some unknown functionality of the component. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the Command Injection attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
3	Cross-Site Request Forgery	CVE-2021-4164	Calibre-Web cross-site request forgery [CVE-2021-4164]	A vulnerability, which was classified as problematic, has been found in Calibre-Web. Affected by this issue is an unknown code block.	Protected by core rules.	NA
		CVE-2021-24936	WP Extra File Types Plugin up to 0.5.0 on WordPress cross-site request forgery	A vulnerability was found in WP Extra File Types Plugin up to 0.5.0 and classified as problematic. Affected by this issue is some unknown processing. Upgrading to version 0.5.1 eliminates this vulnerability.	Protected by core rules.	NA
4	SQL Injection	CVE-2021-25023	PageSpeed Optimization Suite up to 4.3.3.0 on WordPress SQL Statement sbp_convert_table_name SQL injection	A vulnerability was found in PageSpeed Optimization Suite up to 4.3.3.0. It has been classified as critical. This affects an unknown part of the component. Upgrading to version 4.3.3.1 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2021-25030	Events Made Easy Plugin up to 2.2.35 on WordPress SQL Statement eme_searchmail search_text SQL injection	A vulnerability was found in Events Made Easy Plugin up to 2.2.35. It has been declared as critical. This vulnerability affects the function of the component. Upgrading to version 2.2.36 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2021-24786	Download Monitor Plugin up to 4.4.4 on WordPress GET Parameter orderby SQL injection	A vulnerability has been found in Download Monitor Plugin up to 4.4.4 on WordPress and classified as critical. Affected by this vulnerability is an unknown functionality of the component. Upgrading to version 4.4.5 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2022-21661	WordPress Core 5.8.2 - 'WP_Query' SQL Injection	A vulnerability allows remote malicious users to disclose sensitive information on affected installations of WordPress Core. Authentication is not required to exploit this vulnerability.	Protected custom rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2022-21664	WordPress up to 5.8.2 SQL injection [CVE-2022-21664]	A vulnerability was found in WordPress up to 5.8.2. It has been declared as critical. Affected by this vulnerability is an unknown code block. Upgrading to version 5.8.3 eliminates this vulnerability. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2022-21661	WordPress up to 5.8.2 WP_Query SQL injection	A vulnerability was found in WordPress up to 5.8.2. It has been rated as critical. Affected by this issue is the function. Upgrading to version 5.8.3 eliminates this vulnerability. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2022-23305	SQL injection in JDBC Appender in Apache Log4j V1	By design, the JDBCAppender in Log4j 1.2.x accepts an SQL statement as a configuration parameter where the values to be inserted are converters from PatternLayout. The message converter, %m, is likely to always be included. This allows attackers to manipulate the SQL by entering crafted strings into input fields or headers of an application that are logged allowing unint233ended SQL queries to be executed. Note this issue only affects Log4j 1.x when specifically configured to use the JDBCAppender, which is not the default	Protected by custom rules.	Detected by the scanner as the SQL Injection attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2021-25037	All in One SEO Plugin prior 4.1.5.3 on WordPress SQL injection	A vulnerability was found in the All-in-One SEO Plugin. It has been rated as critical. Affected by this issue is an unknown function. Upgrading to version 4.1.5.3 eliminates this vulnerability. Applying a patch can eliminate this problem. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2022-23046	PhpIPAM 1.4.4 edit-bgp-mapping-search.php subnet SQL injection	A vulnerability was found in PhpIPAM 1.4.4. It has been classified as critical. This affects an unknown code of the file. Upgrading to version 1.4.5 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2021-46204	Taocms 3.0.2 Article.php path SQL injection	A vulnerability was found in Taocms 3.0.2. It has been rated as problematic. This issue affects some unknown functionality of the file. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2021-44593	Source-Codester Simple College Website 1.0 File Upload /admin/login.php username SQL injection	A vulnerability classified as critical was found in Source-Codester Simple College Website 1.0. Affected by this vulnerability is an unknown functionality of the file. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2021-46024	projectworlds online-shopping-web-vsite-in-php 1.0 cart_add.php id SQL injection	A vulnerability, which was classified as critical, has been found in projectworlds online-shopping-web-vsite-in-php 1.0. This issue affects some unknown functionality of the file. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2021-24858	Cookie Notification Plugin for Plugin up to 1.0.8 on WordPress GET Parameter id SQL injection	A vulnerability was found in Cookie Notification Plugin for Plugin up to 1.0.8 on WordPress. It has been rated as critical. Affected by this issue is an unknown part of the component. Upgrading to version 1.0.9 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2022-0362	ShowDoc up to 2.10.2 sql injection [CVE-2022-0362]	A vulnerability was found in ShowDoc up to 2.10.2 and classified as critical. This issue affects some unknown processing. Upgrading to version 2.10.3 eliminates this vulnerability. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2021-46377	cszcms 1.2.9 Front-End Member.php#viewUser SQL injection	A vulnerability was found in cszcms 1.2.9. It has been rated as critical. Affected by this issue is an unknown code of the file. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2020-25905	Source-codester Mobile Shop System in PHP MySQL 1.0 login.php email SQL injection	A vulnerability was found in Source-codester Mobile Shop System in PHP MySQL 1.0. It has been classified as critical. This affects some unknown processing of the file. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
5	Deserialization	CVE-2021-42321	Microsoft urges Exchange admins to patch bugs exploited in the wild	A remote code execution (RCE) vulnerability in Microsoft Exchange that affects on-premises servers running Microsoft Exchange 2016 and 2019, including those using Exchange Hybrid mode. This exploit enables authenticated threat actors to execute code remotely on vulnerable servers and launch an attack.	Protected by the custom rules.	NA
6	Malicious File Upload	CVE-2021-4080	crater unrestricted upload	A vulnerability, which was classified as critical, has been found in the crater. This issue affects some unknown functionality.	Protected by the core rules.	NA
		CVE-2022-22929	mingSoft MCMS 5.2.4 New Template Module unrestricted upload	A vulnerability was found in mingSoft MCMS 5.2.4. It has been classified as critical. Affected is an unknown code of the component. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by the custom rules.	NA
		CVE-2021-46386	mingsoft MCMS up to 5.2.5 unrestricted upload	A vulnerability was found in mingsoft MCMS up to 5.2.5. It has been declared as critical. This vulnerability affects some unknown processing. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by the custom rules.	NA

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
7	Redirection	CVE-2021-25074	WebP Converter for Media Plugin up to 4.0.2 on WordPress passthru.php src redirect	A vulnerability has been found in WebP Converter for Media Plugin up to 4.0.2 on WordPress and classified as problematic. This vulnerability affects some unknown processing of the file. Upgrading to version 4.0.3 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Dos attack.
		CVE-2021-25028	Event Tickets Plugin up to 5.2.1 on WordPress tribe_tickets_redirect_to	A vulnerability, which was classified as problematic, has been found in the Event Tickets Plugin up to 5.2.1 on WordPress.This issue affects some unknown processing. Upgrading to version 5.2.2 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Dos attack.
8	Cross-Site Scripting	CVE-2021-24680	WP Travel Engine Plugin up to 5.3.0 on WordPress Description cross-site scripting	A vulnerability was found in WP Travel Engine Plugin up to 5.3.0. It has been rated as problematic. This issue affects an unknown code block. Upgrading to version 5.3.1 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-25027	PowerPack Addons for Elementor Plugin up to 2.6.1 on WordPress Admin Dashboard tab cross-site scripting	A vulnerability was found in PowerPack Addons for Elementor Plugin up to 2.6.1. Upgrading to version 2.6.2 eliminates this vulnerability. Applying a patch can eliminate this problem. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-24828	Loan Calculator Plugin up to 1.5.16 on WordPress Shortcode cross-site scripting	A vulnerability classified as problematic has been found in Loan Calculator Plugin up to 1.5.16. Affected is some unknown processing of the component Shortcode Handler. Upgrading to version 1.5.17 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2021-25022	UpdraftPlus Backup Plugin prior 1.16.66 on WordPress Admin Page backup_timestamp/job_id cross-site scripting	A vulnerability was found in UpdraftPlus Backup Plugin and classified as problematic. This issue affects an unknown code of the component. Upgrading to version 1.16.66 eliminates this vulnerability. Applying a patch can eliminate this problem. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-24963	LiteSpeed Cache Plugin up to 4.4.3 on WordPress Admin Page qc_res cross site scripting	A vulnerability classified as problematic was found in LiteSpeed Cache Plugin up to 4.4.3. Affected by this vulnerability is an unknown function of the component. Upgrading to version 4.4.4 eliminates this vulnerability. Applying a patch can eliminate this problem. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-25016	Chaty Plugin Plugin/Chaty Pro Plugin on WordPress Admin Dashboard search cross-site scripting	A vulnerability has been found in Chaty Plugin Plugin and Chaty Pro Plugin on WordPress and classified as problematic. This vulnerability affects an unknown part of the component. Upgrading eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-24991	WooCommerce PDF Invoices & Packing Slips Plugin up to 2.10.4 on WordPress Attribute tab/section cross-site scripting	A vulnerability classified as problematic has been found in WooCommerce PDF Invoices &amp, Packing Slips Plugin up to 2.10.4 on WordPress. This affects an unknown code of the component. Upgrading to version 2.10.5 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2021-24999	Booster for WooCommerce Plugin up to 5.4.8 on WordPress PDF Invoicing Module wcj_notice cross-site scripting	A vulnerability classified as problematic was found in Booster for WooCommerce Plugin up to 5.4.8 on WordPress. This vulnerability affects an unknown code block of the component. Upgrading to version 5.4.9 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-24964	LiteSpeed Cache Plugin up to 4.4.3 on WordPress HTTP Header X-Forwarded-For cross-site scripting	A vulnerability, which was classified as problematic, has been found in LiteSpeed Cache Plugin up to 4.4.3 on WordPress. Affected by this issue is an unknown functionality of the component. Upgrading to version 4.4.4 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-25000	Booster for WooCommerce Plugin up to 5.4.8 on WordPress Admin Dashboard wcj_delete_role cross-site scripting	A vulnerability, which was classified as problematic, has been found in Booster for WooCommerce Plugin up to 5.4.8 on WordPress E-Commerce Management Software. This issue affects some unknown processing of the component. Upgrading to version 5.4.9 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-25001	Booster for WooCommerce Plugin up to 5.4.8 on WordPress Product XML Feeds Module wcj_create_products_xml_result cross-site scripting	A vulnerability, which was classified as problematic, was found in Booster for WooCommerce Plugin up to 5.4.8 on WordPress. Affected is an unknown function of the component. Upgrading to version 5.4.9 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-25040	Booking Calendar Plugin up to 8.9.1 on WordPress Admin Page booking_type cross-site scripting	A vulnerability was found in Booking Calendar Plugin up to 8.9.1. It has been declared as problematic. Affected by this vulnerability is some unknown processing of the component. Upgrading to version 8.9.2 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2021-24973	Site Reviews Plugin up to 5.17.2 on WordPress AJAX Action glsr_action site-reviews cross-site scripting	A vulnerability, which was classified as problematic, was found in Site Reviews Plugin up to 5.17.2 on WordPress. Upgrading to version 5.17.3 eliminates this vulnerability. Applying a patch can eliminate this problem. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-42363	WooCommerce Extension – Reflected XSS Vulnerability	A vulnerability was found in Variation Swatches for WooCommerce Plugin up to 2.1.1 on WordPress (E-Commerce Management Software). It has been classified as problematic. Affected is the function tawcvs_save_settings of the file ~/includes/class-menu-page.php. The manipulation with an unknown input led to a cross site scripting vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2022-21662	WordPress up to 5.8.2 cross-site scripting [CVE-2022-21662]	A vulnerability classified as problematic has been found in WordPress up to 5.8. This affects an unknown function. Upgrading to version 5.8.3 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2022-21662	WordPress: Stored XSS through authenticated users	WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Low-privileged authenticated users (like author) in WordPress core are able to execute JavaScript/perform stored XSS attack, which can affect high-privileged users. This has been patched in WordPress version 5.8.3.	Protected by custom rules.	Detected by the scanner as the Cross-Site Scripting attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2022-0218	Unauthen-ticated XSS Vulnerability Patched in HTML Email Template De-signer Plugin	The WP HTML Mail WordPress plugin is vulnerable to unau-thorized access which allows unau-thenti-cated attack-ers to retrieve and modify theme set-tings due to a missing capability check on the /themesettings REST-API endpoint found in the ~/ includes/class-tem-plate-designer.php file, in versions up to and including 3.0.9. This makes it possible for attackers with no privileges to execute the endpoint and add malicious JavaS-cript to a vulnerable Word-Press site.	Protected by custom rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-36920	Download Monitor Plugin up to 4.4.6 on WordPress cross-site scripting	A vulnerability has been found in Down-load Monitor Plugin up to 4.4.6 on Word-Press and classified as problematic. This vulnerability affects an unknown part. There is no informa-tion about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-25061	WP Booking System Plugin prior 2.0.15 on WordPress Admin Page cross-site scripting	A vulnerability was found in WP Booking System Plugin on WordPress. It has been classified as problematic. This affects an unknown function of the com-ponent. Upgrading to version 2.0.15 elimi-nates this vulnerabil-ity. Applying a patch can eliminate this problem. The bugfix is ready for download at lugins.trac.wordpress.org. The best possible mitigation is suggest-ed to be upgrading to the latest version.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2021-25024	EventCalendar Plugin prior 1.1.51 on WordPress Attribute cross-site scripting	A vulnerability, which was classified as problematic, was found in EventCalendar Plugin on WordPressWordPress Plugin. Affected is an unknown code of the component. Upgrading to version 1.1.51 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-42367	XSS Vulnera-bility Patched in Plugin De-signed to En-hance Woo-Commerce	A vulnerability was found in Variation Swatches for WooCommerce Plugin up to 2.1.1 on WordPress (E-Commerce Management Software). It has been classified as problematic. Affected is the function tawcvs_save_settings of the file ~/includes/class-menu-page.php. The manipulation with an unknown input led to a cross site scripting vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2022-23045	PhpIPAM 1.4.4 Site Settings Site title cross-site scripting	A vulnerability was found in PhpIPAM 1.4.4. It has been declared as problematic. This vulnerability affects an unknown code block of the component. Upgrading to version 1.4.5 eliminates this vulnerability. The upgrade is hosted for download at github.com.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-44299	Navigate CMS 2.9.4 themes.php cross-site scripting	A vulnerability classified as problematic has been found in Navigate CMS 2.9.4. Affected is an unknown part of the file. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2021-44829	AFI WebACMS up to 2.1.0 index.html ID cross-site scripting	A vulnerability was found in AFI WebACMS up to 2.1.0 and classified as problematic. Affected by this issue is some unknown functionali-ty of the file. There is no information about possible counter-measures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-33966	spotweb 1.4.9 Login Page cross-site scripting	A vulnerability was found in spotweb 1.4.9 and classified as problematic. This issue affects an unknown part of the component. There is no information about possible counter-measures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2022-23808	phpMyAdmin up to 5.0/5.1.1 Setup cross-site scripting	A vulnerability was found in phpMyAdmin up to 5.0/5.1.1. It has been declared as problematic. Affected by this vulnerability is an unknown code block of the component. Upgrading to version 5.1.2 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-45380	AppCMS 2.0.101 inc_head.php cross-site scripting	A vulnerability, which was classified as problematic, was found in AppCMS 2.0.101. Affected is an unknown part of the file. There is no in-formation about pos-sible counter-meas-ures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
9	XML External Entity	CVE-2022-0239	corenlp xml external entity reference [CVE-2022-0239]	A vulnerability classified as problematic was found in corenlp. Affected by this vulnerability is an unknown function.	Protected by core rules.	Detected by the scanner as XML External Entity attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2020-4876	IBM Cognos Controller 10.4.0/10.4.1/10.4.2 xml external entity reference	A vulnerability classified as critical has been found in IBM Cognos Controller 10.4.0/10.4.1/10.4.2. This affects some unknown functionality. Upgrading eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as XML External Entity attack.
		CVE-2020-4875	IBM Cognos Controller 10.4.0/10.4.1/10.4.2 xml external entity reference	A vulnerability was found in IBM Cognos Controller 10.4.0/10.4.1/10.4.2. It has been rated as critical. Affected by this issue is an unknown functionality. Upgrading eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as XML External Entity attack.
10	Remote Code Execution	CVE-2022-21907	Microsoft Windows HTTP Protocol Stack Remote Code Execution [CVE-2022-21907]	A vulnerability, which was classified as very critical, was found in Microsoft Windows 10 1809/10 20H2/10 21H1/10 21H2/11/ Server 2019/Server 2022/Server up to 20H2. Affected is an unknown functionality of the component. Applying a patch can eliminate this problem. A possible mitigation has been published immediately after the disclosure of the vulnerability.	Research queue	NA

Indusface is a leading application security SaaS company that secures critical Web, Mobile & API applications of 3000+ global customers using its award-winning fully managed platform that integrates a web application scanner, web application firewall, DDoS &, BOT Mitigation, CDN, and threat intelligence engine. The company has been funded by Tata Capital Growth Fund, is Great Place to Work certified, mentioned by analysts like Gartner, Forrester, etc in their reports, and has been the recipient of many awards such as the Economic Times Top 25, NASSCOM DSCI Top Security Company, Deloitte Asia Top 100 , and several other such prestigious recognitions.

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

EMAIL - sales@indusface.com