INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

December 2021

Total Zero-Day Vulnerabilities Found: 66

Command Injection	Dos Attack	Code Injection	CSRF	Local File Inclusion	Malicious File Upload	SQL Injection	Cross-Site Scripting
3	1	1	7	4	1	11	38

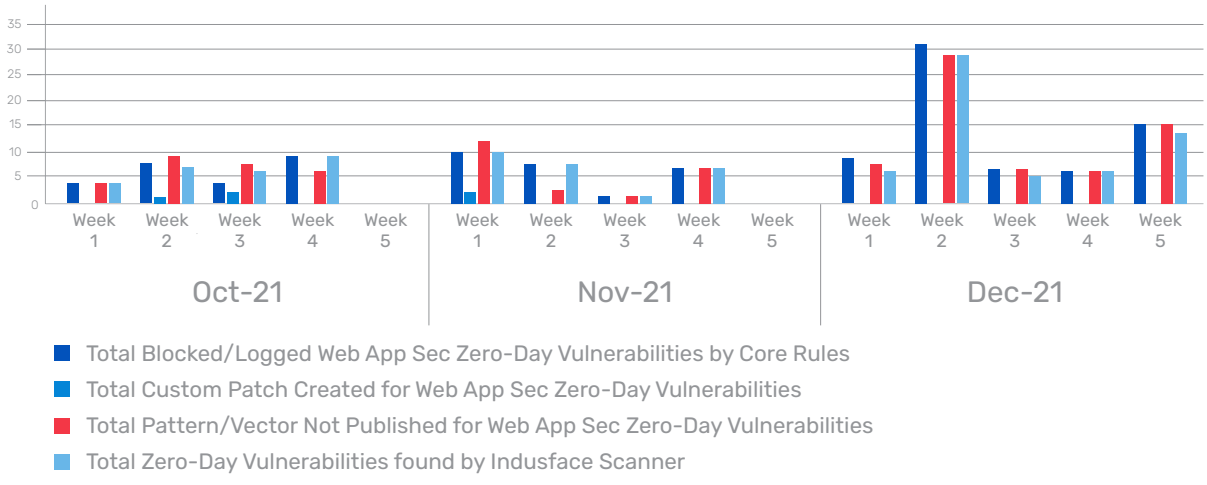
Zero-Day vulnerabilities protected through core rules	66
Zero-Day vulnerabilities protected through custom rules	0*
Zero-Day vulnerabilities for which protection cannot be determined	0**
Zero-Day vulnerabilities found by Indusface WAS	59

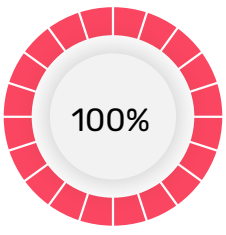
* To enable the custom rules, please contact support@indusface.com

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

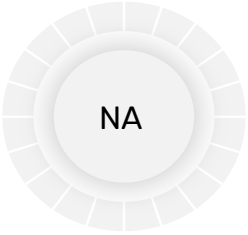
Vulnerability Trend:

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

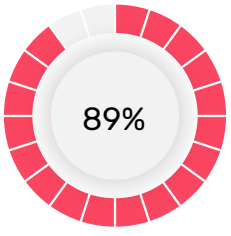




of the zero-day vulnerabilities were protected by the **core rules** in the last quarter

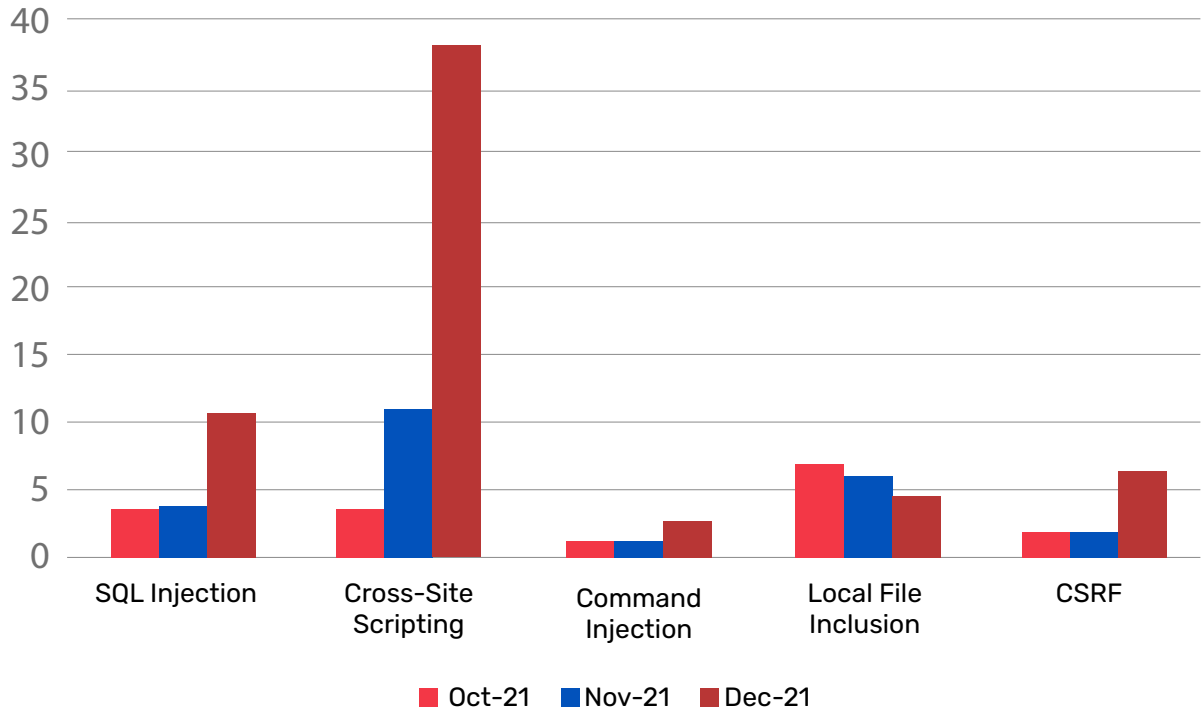


None of the zero-day vulnerabilities were protected by the **custom rules** in the last quarter



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

Top Five Vulnerability Categories



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.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
1	Local File Inclusion	CVE-2021-43795	Armeria 1.13.4 path traversal [CVE-2021-43795]	A vulnerability, which was classified as critical, was found in Armeria 1.13.4. Affected is an unknown code block. Applying the patch e2697a575e9df6692b423e02d731f293c1313284 is able to eliminate this problem.	Protected by core rules.	Detected by the scanner as the Local File Inclusion attack.
		CVE-2021-43798	Grafana up to 8.0.6/8.1.7/8.2.6/8.3.0 / public/plugins/ path traversal	A vulnerability was found in Grafana up to 8.0.6/8.1.7/8.2.6/8.3.0. It has been declared as critical. Affected by this vulnerability is some unknown functionality of the file. Upgrading to version 8.0.7, 8.1.8, 8.2.7, or 8.3.1 eliminates this vulnerability. Applying the patch c798c0e958d15d9cc7f27c72113d572fa58545ce is able to 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 Local File Inclusion attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2021-23797	http-server-node pathname traversal [CVE-2021-23797]	A vulnerability was found in http-server-node and classified as critical. This issue affects an unknown part. 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-2021-44548	Apache Solr up to 8.11.0 SMB DataImportHandler path traversal	A vulnerability was found in Apache Solr up to 8.11.0. It has been rated as critical. Affected by this issue is the function of the component. Upgrading to version 8.11.1 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Local File Inclusion attack.
2	Command Injection	CVE-2021-44684	naholyr github-todos 3.1.0 Argument _hook range command injection	A vulnerability classified as critical was found in naholyr github-todos 3.1.0. Affected by this vulnerability is the function 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.
		CVE-2021-27453	Marmind Web Application 3.0 Cookie authentication bypass	A vulnerability was found in Marmind Web Application 3.0. It has been classified as critical. Affected is an unknown code block 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
		CVE-2021-44832	Apache Log4j up to 2.17.0 Logging Configuration File injection	A vulnerability was found in Apache Log4j up to 2.17.0. It has been rated as critical. Affected by this issue is some unknown functionality of the component. Upgrading to version 2.3.2, 2.12.4, or 2.17.1 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Command Injection attack.
3	Cross-Site Request Forgery	CVE-2021-3993	ShowDoc cross-site request forgery [CVE-2021-3993]	A vulnerability was found in ShowDoc. It has been classified as problematic. Affected is an unknown code. Applying the patch 654e871a3923e79076818a9a03533fe88222c871 can eliminate this problem.	Protected by core rules.	NA
		CVE-2021-4017	ShowDoc cross-site request forgery [CVE-2021-4017]	A vulnerability was found in ShowDoc. It has been rated as problematic. Affected by this issue is some unknown processing. Applying the patch 654e871a3923e79076818a9a03533fe88222c871 can eliminate this problem.	Protected by core rules.	NA
		CVE-2021-24914	Tawk.To Live Chat Plugin up to 0.5.x on WordPress AJAX Action tawkto_setwidget/tawkto_removewidget authorization	A vulnerability was found in Tawk.To Live Chat Plugin up to 0.5. It has been declared as problematic. Affected by this vulnerability is the function of the component. Upgrading to version 0.6.0 eliminates this vulnerability.	Protected by core rules.	NA
		CVE-2021-31631	b2evolution CMS 7.2.3 User Login Page cross-site request forgery	A vulnerability has been found in b2evolution CMS 7.2.3 and classified as problematic. This vulnerability affects an unknown function 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.	NA

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2020-19682	zzzcms 1.7.1 save.php save_user cross-site request forgery	A vulnerability, which was classified as problematic, has been found in zzzcms 1.7.1. This issue affects the function 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.	NA
		CVE-2020-20943	Qibosoft 7 Article post.php cross-site request forgery	A vulnerability has been found in Qibosoft 7 and classified as problematic. Affected by this vulnerability is 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.	NA
		CVE-2020-20945	Qibosoft 7 index.php cross-site request forgery	A vulnerability was found in Qibosoft 7. It has been declared as problematic. This vulnerability affects an unknown code block 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.	NA
4	SQL Injection	CVE-2020-35012	Events Manager Plugin up to 5.9.7 on WordPress SQL Injection	A vulnerability has been found in the Events Manager Plugin up to 5.9.7 on WordPress and classified as critical. Affected by this vulnerability is an unknown functionality. Upgrading to version 5.9.8 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-2021-43451	PHPGurukul Employee Record Management System 1.2 POST Parameter /forget-password.php Email SQL Injection	A vulnerability was found in PHPGurukul Employee Record Management System 1.2. It has been classified as critical. This affects an unknown function of the file 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 SQL Injection attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2021-24866	WP Data Access Plugin up to 4.x on WordPress backup_date SQL Injection	A vulnerability, which was classified as critical, has been found in WP Data Access Plugin up to 4.xon WordPress. Affected by this issue is an unknown code. Upgrading to version 5.0.0 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2021-24943	Registrations for the Events Calendar Plugin up to 2.7.5 on Word-Press rtec_ send_un-register_link event_id SQL Injection	A vulnerability has been found in Registrations for the Events Calendar Plugin up to 2.7.5 on WordPress Calen-dar Software and classified as critical. This vulnerability affects the function. Upgrading to version 2.7.6 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2021-3817	wbce_cms SQL Injection [CVE-2021-3817]	A vulnerability was found in wbce_cms. It has been classi-fied as critical. This affects an unknown functionality. Apply-ing the patch 6ca63f-0cad5f0cd606fd-b69a372f09b7d23 8f1d7 can eliminate this problem.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2021-40279	zzcms 8.2/8.3/2020/ 2021 Param-eter admin/ bad.php id SQL Injection	A vulnerability has been found inzzcms 8.2/8.3/2020/2021 and classified as crit-ical. This vulnerability affects an unknown functionality of the file. There is no infor-mation about possi-ble 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-2021-40281	zzcms 8.2/8.3/2020/ 2021 dl/dl_ print.php SQL Injection	A vulnerability was found in zzcms 8.2/8.3/2020/2021. It has been rated as critical. Affected by this issue is some unknown functional-ity of the file. There is no information about possible counter-measures known. It may be suggested to replace the affected object with an alter-native 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-2021-40282	zzcms 8.2/8.3/2020/2021 dl/dl_download.php SQL Injection	A vulnerability classified as critical has been found in zzcms 8.2/8.3/2020/2021. This affects 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 SQL Injection attack.
		CVE-2021-40280	zzcms 8.2/8.3/2020/2021 Parameter admin/dl_sendmail.php id SQL Injection	A vulnerability was found in zzcms 8.2/8.3/2020/2021 and classified as critical. 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-2020-18081	SEMCMS up to 3.8 SQL Query information disclosure	A vulnerability was found in SEMCMS up to 3.8 and classified as problematic. This issue affects some unknown processing 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 SQL Injection attack.
		CVE-2021-24753	Rich Reviews Plugin up to 1.9.5 on WordPress GET Parameter orderby SQL Injection	A vulnerability has been found in Rich Reviews Plugin up to 1.9.5 on WordPress and classified as critical. Affected by this vulnerability is an unknown code block of the component. Upgrading to version 1.9.6 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.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
5	Code Injection	CVE-2021-44228	Apache log4j up to 2.14.1 JNDI LDAP Server Lookup format string	A vulnerability was found in Apache log4j up to 2.14.1 and classified as critical. This issue affects an unknown part of the component. Upgrading to version 2.15.0 eliminates this vulnerability. The upgrade is hosted for download at logging.apache.org. 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 Code Injection attack.
6	Malicious File Upload	CVE-2021-44228	Apache log4j up to 2.14.1 JNDI LDAP Server Lookup format string	A vulnerability was found in Apache log4j up to 2.14.1 and classified as critical. This issue affects an unknown part of the component. Upgrading to version 2.15.0 eliminates this vulnerability. Applying a patch can eliminate this problem. It is possible to mitigate the problem by applying the configuration setting. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by core rules.	NA
7	Dos Attack	CVE-2021-44228	Apache Log4j up to 2.12.2/2.16.0 Lookup infinite loop	A vulnerability was found in Apache log4j up to 2.14.1 and classified as critical. This issue affects an unknown part of the component. Upgrading to version 2.15.0 eliminates this vulnerability. Applying a patch can eliminate this problem. It is possible to mitigate the problem by applying the configuration setting. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by core rules.	Detected by the scanner as the Dos attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
8	Cross-Site Scripting	CVE-2015-20105	ClickBank Affiliate Ads Plugin up to 1.20 on WordPress cross site scripting	A vulnerability, which was classified as problematic, has been found inClickBank Affiliate Ads Plugin up to 1.20. 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.
		CVE-2021-24969	WordPress Download Manager Plugin prior 3.2.22 on WordPress Template Data wpdm_save_template cross site scripting	A vulnerability, which was classified as problematic, was found in WordPress Download Manager Plugin. This affects the function of the component. Upgrading to version 3.2.22 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-24797	Tickera Plugin prior 3.4.8.3 on WordPress Booked Event cross site scripting	A vulnerability was found in Tickera Plugin and classified as problematic. Affected by this issue is some unknown processing of the component. Upgrading to version 3.4.8.3 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-24979	Paid Memberships Pro Plugin up to 2.6.5 on WordPress Admin Page cross site scripting	A vulnerability was found in Paid Memberships Pro Plugin up to 2.6. It has been rated as problematic. This issue affects some unknown functionality of the component. Upgrading to version 2.6.6 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-2021-24902	Build Beautiful Conversational Forms Plugin up to 1.4.2 on WordPress Publish ID Setting cross site scripting	A vulnerability was found in Build Beautiful Conversational Forms Plugin up to 1.4.2. It has been classified as problematic. This affects an unknown function of the component. Upgrading to version 1.4.3 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-2021-24967	Contact Form & Lead Form Elementor Builder Plugin up to 1.6.3 on WordPress cross site scripting	A vulnerability was found in Contact Form & Lead Form Elementor-Builder Plugin up to 1.6.3. It has been declared as problematic. This vulnerability affects an unknown functionality. Upgrading to version 1.6.4 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-24984	WP RSS Aggregator Plugin prior 4.19.3 on WordPress System Info Admin Dashboard wprss_dismiss_addon_notice cross site scripting	A vulnerability has been found in WP RSS Aggregator Plugin and classified as problematic. This vulnerability affects the function of the component. Upgrading to version 4.19.3 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-24980	Gwolle Guestbook Plugin up to 4.1.x on WordPress Admin Page gwolle_gb_user_email cross site scripting	A vulnerability classified as problematic has been found in Gwolle Guestbook Plugin up to 4.1.x. Affected is an unknown part of the component. Upgrading to version 4.2.0 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-24992	Smart Floating & Sticky Buttons Plugin up to 2.5.4 on WordPress Parameter cross site scripting	A vulnerability, which was classified as problematic, has been found in Smart Floating & Sticky Buttons Plugin up to 2.5.4. Affected by this issue is an unknown code block of the component. Upgrading to version 2.5.5 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2020-20946	Qibosoft 7 index.php cross site scripting	A vulnerability was found in Qibosoft 7. It has been rated as problematic. This issue 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 Cross-Site Scripting attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2021-38876	IBM i 7.2/7.3/7.4 Web UI cross site scripting	A vulnerability was found in IBM i 7.2/7.3/7.4. It has been classified as problematic. Affected is an unknown functionality of the component. Upgrading eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-23260	Crafter CMS File Name cross site scripting [CVE-2021-23260]	A vulnerability classified as problematic has been found in Crafter CMS. This affects an unknown code block of the component. Upgrading eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2020-35037	Events Manager Plugin up to 5.9.7 on WordPress Search Parameter cross site scripting	A vulnerability was found in Events Manager Plugin up to 5.9.7 and classified as problematic. Affected by this issue is some unknown functionality of the component. Upgrading to version 5.9.8 eliminates this vulnerability. Applying a patch can eliminate this problem.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-24938	WOOCS Plugin up to 1.3.7.0 on WordPress AJAX Action woocs_update_profiles_data key cross site scripting	A vulnerability classified as problematic was found in WOOCS Plugin up to 1.3.7.0. This vulnerability affects the function of the component. Upgrading to version 1.3.7.1 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-24939	LoginWP Plugin prior 3.0.0.5 on WordPress Admin Page rul_login_url/rul_logout_url cross site scripting	A vulnerability, which was classified as problematic, has been found in LoginWP Plugin. This issue affects some unknown processing of the component. Upgrading to version 3.0.0.5 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-2021-24714	Import any XML or CSV File Plugin up to 3.6.2 on WordPress Admin Page cross site scripting	A vulnerability was found in Import any XML or CSV File Plugin up to 3.6.2 and classified as problematic. Affected by this issue is some unknown functionality of the component. Upgrading to version 3.6.3 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-25041	10Web Photo Gallery Plugin prior 1.5.68 on WordPress AJAX Action bwg_frontend_data bwg_album_breadcrumb_0/ shortcode_id cross site scripting	A vulnerability, which was classified as problematic, was found in 10Web Photo Gallery Plugin. Affected is the function of the component. Upgrading to version 1.5.68 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-2021-24759	PDF.js Viewer Plugin up to 2.0.1 on WordPress Shortcode cross site scripting	A vulnerability was found inPDF.js Viewer Plugin up to 2.0.1 on WordPress. It has been classified as problematic. Affected is an unknown functionality of the component. Upgrading to version 2.0.2 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-24924	Email Log Plugin up to 2.4.7 on WordPress Log Page d cross site scripting	A vulnerability was found in the Email Log Plugin up to 2.4.7 on WordPress. It has been rated as problematic. Affected by this issue is an unknown part of the component. Upgrading to version 2.4.8 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-24930	Online Booking and Scheduling Plugin up to 20.3.0 on WordPress Staff Full Name cross site scripting	A vulnerability classified as problematic has been found in Online Booking and Scheduling Plugin up to 20.3.0 on WordPress. This affects an unknown code. Upgrading to version 20.3.1 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-2021-24718	Contact Form, Survey & Pop-up Form Plugin up to 1.4 on WordPress cross site scripting	A vulnerability was found in Contact Form, Survey & Popup Form Plugin up to 1.4 on WordPress. This issue affects an unknown function. Upgrading to version 1.5 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-24935	WP Google Fonts Plugin up to 3.1.4 on WordPress AJAX Action google-font_action googlefont_ajax_family cross-site scripting	A vulnerability classified as problematic was found in WP Google Fonts Plugin up to 3.1.4 on WordPress. Affected by this vulnerability is the function of the component. Upgrading to version 3.1.5 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-2020-22421	74CMS 6.0.4 index.php cross-site scripting	A vulnerability has been found in 74CMS 6.0.4 and classified as problematic. 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 Cross-Site Scripting attack.
		CVE-2020-27356	debug-meta-data Plugin 1.1.2 on WordPress cross-site scripting	A vulnerability has been found in debug-meta-data Plugin 1.1.2 on WordPress 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 Cross-Site Scripting attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2021-36188	Fortinet FortiWeb up to 6.3.15/6.4.1 Login/Error cross-site scripting	A vulnerability was found in Fortinet FortiWeb up to 6.3.15/6.4.1. It has been declared as problematic. Affected by this vulnerability is some unknown functionality 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-2021-42752	Fortinet FortiWLM up to 8.6.1 Web Page Generation cross-site scripting	A vulnerability was found in Fortinet FortiWLM up to 8.6.1. It has been declared as problematic. This vulnerability affects some unknown functionality 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-2021-41029	Fortinet FortiWLM up to 8.6.1 Web Page Generation cross-site scripting	A vulnerability was found in Fortinet FortiWLM up to 8.6.1. It has been classified as problematic. This affects an unknown functionality 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-2021-43808	Laravel up to 6.20.41/7.30.5/8.74.x Blade Templating Engine cross-site scripting	A vulnerability classified as problematic was found in Laravel up to 6.20.41/7.30.5/8.74.x. Affected by this vulnerability is an unknown part of the component. Upgrading to version 6.20.42, 7.30.6 or 8.75.0 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 Cross-Site Scripting attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2021-4038	McAfee Network Security Manager up to 10.1 Minor 6 Administrator Interface crosssite scripting	A vulnerability was found in McAfee Network Security Manager up to 10.1 Minor 6. It has been rated as problematic. This issue affects an unknown function of the component. Upgrading to version 10.1 Minor 7 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
8	Cross-Site Scripting	CVE-2020-19683	zzzcms 1.7.1 save.php editfile cross-site scripting	A vulnerability, which was classified as problematic, was found in zzzcms 1.7.1. Affected is the function 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
		CVE-2021-36911	Comment Engine Pro Plugin up to 1.0 on WordPress cross-site scripting	A vulnerability classified as problematic has been found in Comment Engine Pro Plugin up to 1.0 on WordPress. Affected is some unknown functionality. 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
		CVE-2021-41962	Source-codester Vehicle Service Management System 1.0 Parameter vehicle_service cross-site scripting	A vulnerability, which was classified as problematic, was found in Source-codester Vehicle Service Management System 1.0. Affected is the function 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 Cross-Site Scripting attack.

S.No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2021-38883	IBM Business Automation Workflow Web UI cross-site scripting	A vulnerability has been found in IBM Business Automation Workflow and Business Process Manager and classified as problematic. This vulnerability affects some unknown processing of the component. Upgrading eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-38966	IBM Cloud Pak for Automation 21.0.2 Web UI cross-site scripting	A vulnerability has been found in IBM Cloud Pak for Automation 21.0.2 and classified as problematic. This vulnerability affects an unknown function of the component. Upgrading eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack
		CVE-2020-19770	Wuzhi CMS 4.1.0 System Bulletin cross-site scripting	A vulnerability, which was classified as problematic, has been found in Wuzhi CMS 4.1.0. Affected by this issue is an unknown code block of the component. There is no information about possible countermeasure-sknown. 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-2021-38893	IBM Business Automation Workflow Web UI cross-site scripting	A vulnerability, which was classified as problematic, was found in IBM Business Automation Workflow and Business Process Manager. This affects some unknown processing of the component. Upgrading eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2020-20605	Blog CMS 1.0 Comment Admin Controller.java cross-site scripting	A vulnerability was found in Blog CMS 1.0. It has been declared as problematic. Affected by this vulnerability 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.

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