Monthly Zero-Day Vulnerability Coverage Bulletin

February 2022

Total Zero-Day Vulnerabilities Found: 16

Command Injection	Redirection	SQL Injection	CSRF	Cross - Site Scripting
2	1	3	4	6

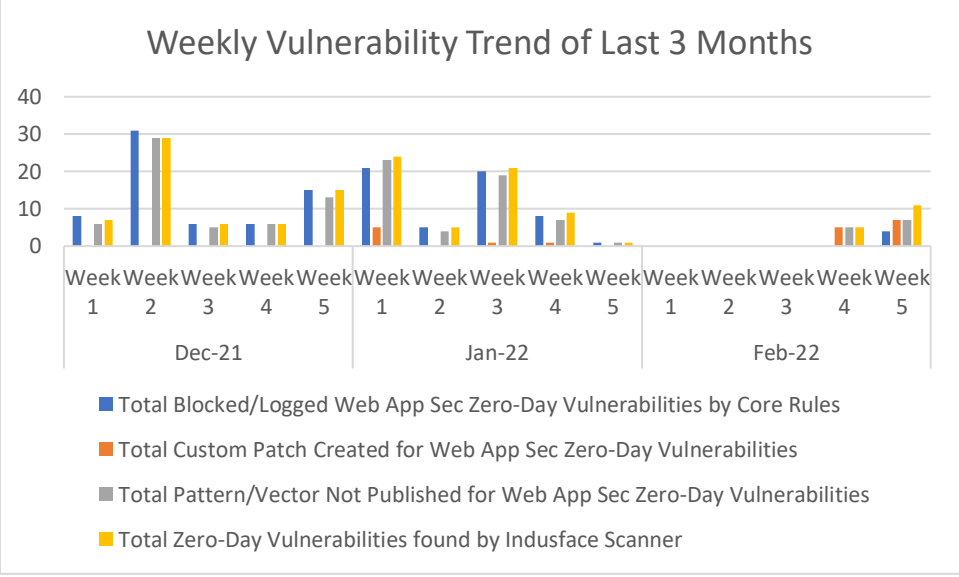
Zero-Day vulnerabilities protected through core rules	4
Zero-Day vulnerabilities protected through custom rules	12 *
Zero-Day vulnerabilities for which protection cannot be determined	0 **
Zero-Day vulnerabilities found by Indusface WAS	12

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

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

Vulnerability Trend:

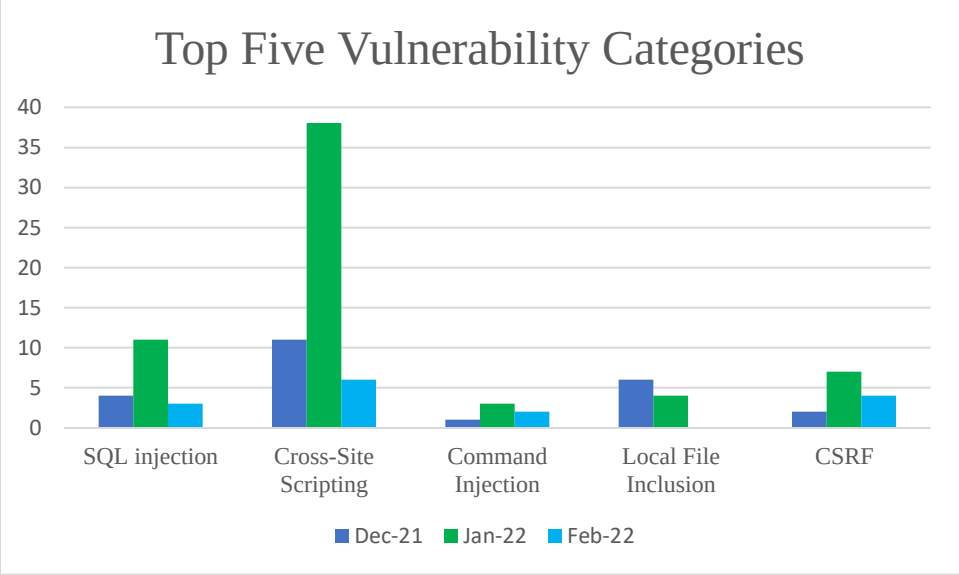
The weekly trend displays the total number of vulnerabilities discovered to the type of protection provided for the last quarter.



25% of the zero-day vulnerabilities were protected by the **core rules** in the last quarter

75% of the zero-day vulnerabilities were protected by the **custom rules** in the last quarter

75% 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	Command Injection	CVE-2022-25095	Home Owners Collection Management System 1.0 POST Request Remote Code Execution	A vulnerability has been found in Home Owners Collection Management System 1.0 and classified as critical. 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 custom rules.	Detected by the scanner as the Command Injection attack.
		CVE-2022-0764	strapi up to 4.0.x command injection [CVE-2022-0764]	A vulnerability has been found in strapi up to 4.0.x and classified as critical. Affected by this vulnerability is some unknown functionality. Upgrading to version 4.1.0 eliminates this vulnerability. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by custom rules.	Detected by the scanner as the Command Injection attack.

2	Cross-Site Request Forgery	CVE-2022-0328	Simple Membership Plugin up to 4.0.8 on WordPress Member Delete cross-site request forgery	Simple Membership Plugin up to 4.0.8 on WordPress Member Delete cross-site request forgery	Protected by custom rules.	NA
		CVE-2022-0345	Customize Emails and Alerts Plugin up to 1.8.6 on WordPress AJAX Action bnfw_search_users cross-site request forgery	Customize Emails and Alerts Plugin up to 1.8.6 on WordPress AJAX Action bnfw_search_users cross-site request forgery	Protected by custom rules.	NA
		CVE-2021-24803	Core Tweaks WP Setup Plugin up to 4.1 on WordPress cross-site request forgery	Core Tweaks WP Setup Plugin up to 4.1 on WordPress cross-site request forgery	Protected by custom rules.	NA
		CVE-2021-24913	Logo Showcase with Slick Slider Plugin up to 2.0.0 on WordPress AJAX Action lswss_save_attachment_data cross-site request forgery	Logo Showcase with Slick Slider Plugin up to 2.0.0 on WordPress AJAX Action lswss_save_attachment_data cross-site request forgery	Protected by custom rules.	NA

3	SQL Injection	CVE-2022-0412	TI WooCommerce Wishlist Plugin up to 1.40.0 REST Endpoint wishlist/remove_product item_id SQL injection	A vulnerability, which was classified as critical, was found in TI WooCommerce Wishlist Plugin and TI WooCommerce Wishlist Pro Plugin up to 1.40.0. Affected is an unknown code block of the file. Upgrading to version 1.40.1 eliminates this vulnerability. Applying a patch is able to eliminate this problem. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by custom rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2022-0383	WP Review Slider Plugin up to 10.x on WordPress pid SQL injection	A vulnerability, which was classified as critical, has been found in WP Review Slider Plugin up to 10.x on WordPress. This issue affects an unknown code. Upgrading to version 11.0 eliminates this vulnerability. Applying a patch is able to eliminate this problem. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by custom rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2021-24864	WP Cloudy Plugin up to 4.4.8 on WordPress Admin Dashboard post_id SQL injection	A vulnerability classified as critical has been found in WP Cloudy Plugin up to 4.4.8. Affected is an unknown code of the component. Upgrading to version 4.4.9 eliminates this vulnerability.	Protected by custom rules.	Detected by the scanner as the SQL Injection attack.

				Applying a patch is able to eliminate this problem. The best possible mitigation is suggested to be upgrading to the latest version.		
4	Redirection	CVE-2021-23495	karma up to 6.3.15 Query Parameter return_url redirect	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 custom rules.	Detected by the scanner as the Code Injection attack.
5	Cross-Site Scripting	CVE-2021-37504	jQuery-Upload-File 4.0.11 fileNameStr cross-site scripting	A vulnerability classified as problematic was found in jQuery-Upload-File 4.0.11. Affected by this vulnerability 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 custom rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2022-26146	Tricentis qTest up to 10.3 cross-site scripting	A vulnerability classified as problematic has	Protected by custom rules.	Detected by the scanner as the Cross-Site

		[CVE-2022-26146]	been found in Tricentis qTest up to 10.3. Affected is an unknown function. Upgrading to version 10.4 eliminates this vulnerability.		Scripting attack.
	CVE-2021-43945	Atlassian JIRA Server/Data Center up to 8.20.2 hierarchyConfiguration cross-site scripting	A vulnerability, which was classified as problematic, was found in Atlassian JIRA Server and Data Center up to 8.20.2. This affects an unknown part of the file. Upgrading to version 8.20.3 eliminates this vulnerability.	Protected by custom rules.	Detected by the scanner as the Cross-Site Scripting attack.
	CVE-2022-0772	librenms up to 22.2.1 cross-site scripting [CVE-2022-0772]	A vulnerability, which was classified as problematic, has been found in librenms up to 22.2.1. Affected by this issue is some unknown functionality. Upgrading to version 22.2.2 eliminates this vulnerability. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by custom rules.	Detected by the scanner as the Cross-Site Scripting attack.
	CVE-2022-0360	WP Ultimate CSV Importer Plugin up to 6.4.2 on WordPress Comment cross-site scripting	A vulnerability has been found in WP Ultimate CSV Importer Plugin up to 6.4.2 and classified as problematic. This vulnerability affects an unknown code block of the component. Upgrading to version 6.4.3 eliminates this vulnerability. Applying a patch is able to eliminate this problem. The best possible mitigation is	Protected by custom rules.	Detected by the scanner as the Cross-Site Scripting attack.

			suggested to be upgrading to the latest version.		
	CVE-2021-25034	WP User Plugin up to 6.x on WordPress wp_user Shortcode cross-site scripting	A vulnerability was found in WP User Plugin up to 6.x on WordPress. It has been classified as problematic. This affects an unknown code block of the component. Upgrading to version 7.0 eliminates this vulnerability.	Protected by custom rules.	Detected by the scanner as the Cross-Site Scripting attack.