INDUSFACE™

Weekly Zero-Day Vulnerability Coverage Bulletin

MARCH 2021

Total Zero Day Vulnerabilities found: 19

SQL Injection	Cross Site Scripting	Direct Traversal	PHP remote Code execution	Insecure Flash Parameter" AllowScript Access" Detected	Cross site request forgery	BOT attack	Weak Authentication
5	5	4	1	1	1	1	1

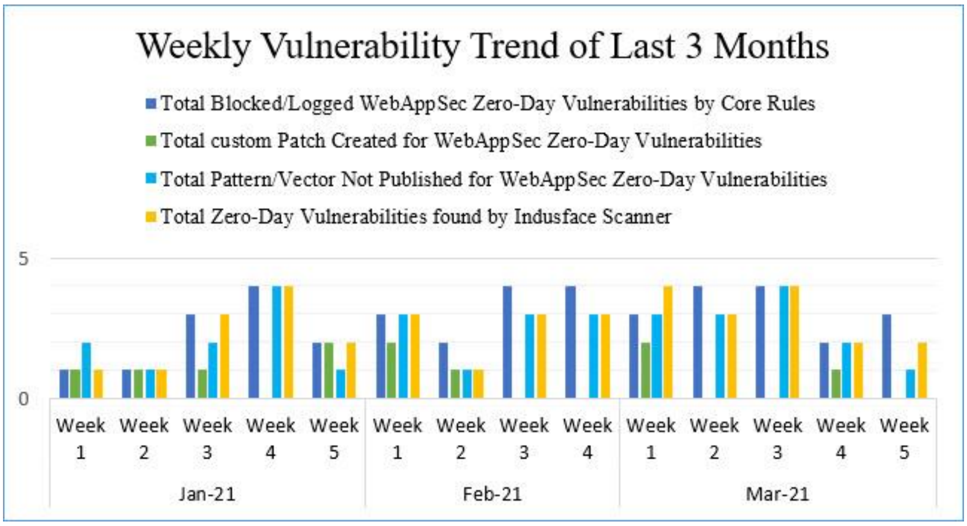
Zero-Day Vulnerabilities Protected through Core Rules	16
Zero-Day Vulnerabilities Protected through Custom Rules	3*
Zero-Day Vulnerabilities for which protection cannot be determined	0 **
Zero-Day Vulnerabilities found by Indusface WAS	16

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

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

Vulnerability Trend:

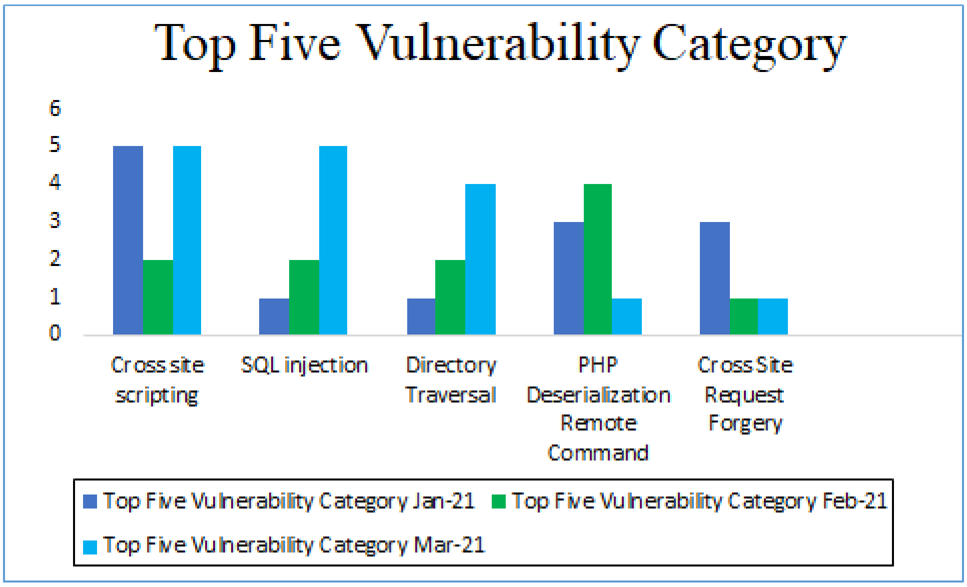
Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.



80% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

20% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

76% Of Zero-Day Vulnerabilities were reported by Indusface Scanner in 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 around the clock protection for customer sites.

Vulnerability Details:

S. No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
1	Cross Site Scripting	CVE-2021-23129	Joomla! up to 3.9.24 Message cross site scripting	A vulnerability was found in Joomla! Up to 3.9.24. It has been rated as problematic. Affected by this issue 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 Core Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2020-23721	Fuel CMS 1.4.7 1 cross site scripting	A vulnerability was found in Fuel CMS 1.4.7.1 and classified as problematic. Affected by this issue is an unknown code block of the file. There is no information about countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Core Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2021-24135	WP Customer Reviews Plugin up to 3.4.2 on WordPress cross site scripting	A vulnerability was found in WP Customer Reviews Plugin up to 3.4.2. It has been classified as problematic. This affects some unknown functionality. Upgrading to	Protected by Core Rules.	Detected by scanner as Cross Site Scripting attack.

				version 3.4.3 eliminates this vulnerability.		
		CVE-2021-25919	Open EMR up to 6.0.0 Create New User cross site scripting	A vulnerability has been found in Open EMR up to 6.0.0 and classified as problematic. This vulnerability affects an unknown part of the component. Applying a patch can eliminate this problem.	Protected by Core Rules.	Detected by scanner as Cross Site Scripting attack.
		NA	Moodle flaw exposed users to account takeover	Moodle is an open-source educational platform used by 179,000 sites and has 242 million users. It allows universities to distribute content to students and teachers. It allows teachers to easily communicate with students, organize and post links, documents, assignments, quizzes, and grades.	Protected by Core Rules.	Detected by scanner as Cross Site Scripting attack.
2	SQL Injection	CVE-2021-27314	Doctor Appointment System 1.0 admin.php username sql injection	A vulnerability was found in Doctor Appointment System 1.0 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 scanner as SQL Injection attack.
		CVE-2020-24791	Fuel CMS 1.4.8 pages/replace/1 fuel_replace_id sql injection	A vulnerability was found in Fuel CMS 1.4.8. It has been declared as critical. This vulnerability affects an unknown function of the file. Upgrading to version 1.4.9 eliminates this vulnerability.	Protected by Core Rules.	Detected by scanner as SQL Injection attack.
		CVE-2021-27947	MyBB up to 1.8.25 Forum Management sql injection	A vulnerability MyBB up to 1.8.25, which was classified as critical, has been found in Content Management System. Affected by this issue is an unknown code of the component. Upgrading to version 1.8.26 eliminates this vulnerability.	Protected by Core Rules.	Detected by scanner as SQL Injection attack.

		CVE-2021-28419	Seo Panel 4.8.0 archive.php order_col sql injection	A vulnerability has been found in Seo Panel 4.8.0 and classified as critical. This vulnerability affects some unknown processing of the file. There is no information about countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Core Rules.	Detected by scanner as SQL Injection attack.
		CVE-2020-35337	ThinkSAAS up to 3.37 topic.php title sql injection	A vulnerability was found in ThinkSAAS up to 3.37. It has been rated as critical. This issue affects an unknown code of the file. Upgrading to version 3.38 eliminates this vulnerability.	Protected by Core Rules.	Detected by scanner as SQL Injection attack.
3	Directory Traversal/File Inclusion	CVE-2020-36240	Crowd up to 4.0.3/4.1.1 ResourceDownloadRewriteRule path traversal	The ResourceDownloadRewriteRule class in Crowd before version 4.0.4, and from version 4.1.0 before 4.1.2 allowed unauthenticated remote attackers to read arbitrary files within WEB-INF and META-INF directories via an incorrect path access check.	Protected by Core Rules.	Detected by scanner as Local File Injection attack.
		CVE-2021-28918, CVE-2021-29418	Universal "netmask" npm package, used by 270,000+ projects, vulnerable to octal input data: server-side request forgery, remote file inclusion, local file inclusion, and more	The following research outlines a vulnerability discovered in netmask npm package that is currently used by 278,722+ other projects. The vulnerability has been present for 9 years. Since this package is so incredibly widespread, I would suggest every nodejs developer to check their package.jsons to see if they use netmask... and upgrade immediately!	Protected by Core Rules.	Detected by scanner as Local File Injection attack.
		CVE-2020-29555	Grav CMS up to 1.7.0-rc.17 path traversal [CVE-2020-29555]	The Backup Delete functionality in Grav CMS through 1.7.0-rc.17 allows an authenticated attacker to delete arbitrary files on the underlying server by exploiting a path-traversal technique. (This vulnerability can also be exploited by an unauthenticated attacker due to a lack of CSRF protection.)	Protected by Core Rules.	Detected by scanner as Local File Injection attack.

		CVE-2021-29417	gitjacker prior 0.1.0. git Directory pathname traversal	A vulnerability, which was classified as critical, was found in gitjacker before 0.1.0 allows remote attackers to execute arbitrary code via a crafted. git directory traversal. Upgrading to version 0.1.0 eliminates this vulnerability.	Protected by Core Rules.	Detected by scanner as Local File Injection attack.
4	Cross site request forgery	CVE-2020-29599	ImageMagick vulnerability	ImageMagick before 6.9.11-40 and 7.x before 7.0.10-40 mishandles the -authenticate option, which allows setting a password for password-protected PDF files. The user-controlled password was not properly escaped/sanitized, and it was therefore possible to inject additional shell commands via coders/pdf.c.	Protected by Core Rules.	NA
5	Bot attacks	NA	Golang Bot Starts Targeting WordPress Websites	Bitdefender researchers have identified a new version of an already-known vulnerability scanner that looks for a specific flaw in the "Ultimate GDPR & CCPA Compliance Toolkit" plugin for WordPress.	Protected by Core Rules.	NA
6	Weak Authentication	CVE-2021-24219	Recently Patched Vulnerability in Thrive Themes Actively Exploited in the Wild	The plugins and themes register a REST API endpoint associated with Zapier functionality. While this endpoint was intended to require an API key to access, it was possible to access it by supplying an empty api_key parameter in vulnerable versions if Zapier was not enabled. Attackers could use this endpoint to add arbitrary data to a predefined option in the wp_options table.	Protected by custom rules.	NA
7	PHP Deserialization Remote Command Execution Vulnerability	CVE-2021-24217	Two Vulnerabilities Patched in Facebook for WordPress Plugin	The run action function of the Facebook for WordPress plugin before 3.0.0 deserializes user supplied data making it possible for PHP objects to be supplied creating an Object Injection vulnerability. There was also a useable magic method in the plugin that could be used to achieve remote code execution.	Protected by custom rules.	Detected by scanner as PHP Deserialization Remote Command Execution Vulnerability

8	Insecure Flash Parameter "AllowScriptAccess" Detected	CVE-2021-24207	Vulnerabilities Patched in WP Page Builder	By default, the WP Page Builder WordPress plugin before 1.2.4 allows subscriber-level users to edit and make changes to all posts pages - user roles must be specifically blocked from editing posts and pages.	Protected by custom rules.	Detected by scanner as Insecure Flash Parameter "AllowScript Access" Detected