Weekly Zero-Day Vulnerability Coverage Bulletin

(4th March – 10th March)

Summary:

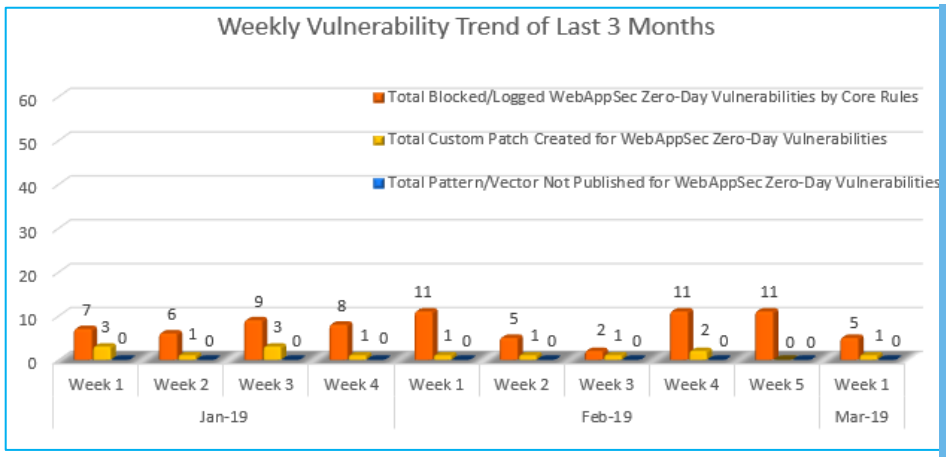
Total **6 Zero-Day Vulnerabilities** were discovered in **4 Categories** previous week

2	2	1	1
Cross Site Scripting	SQL Injection	Directory Traversal	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	5
Zero-Day Vulnerabilities Protected through Custom Rules	1*
Zero-Day Vulnerabilities for which protection cannot be determined	0**

* To enable custom rules please contact support@indusface.com
** Since attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected

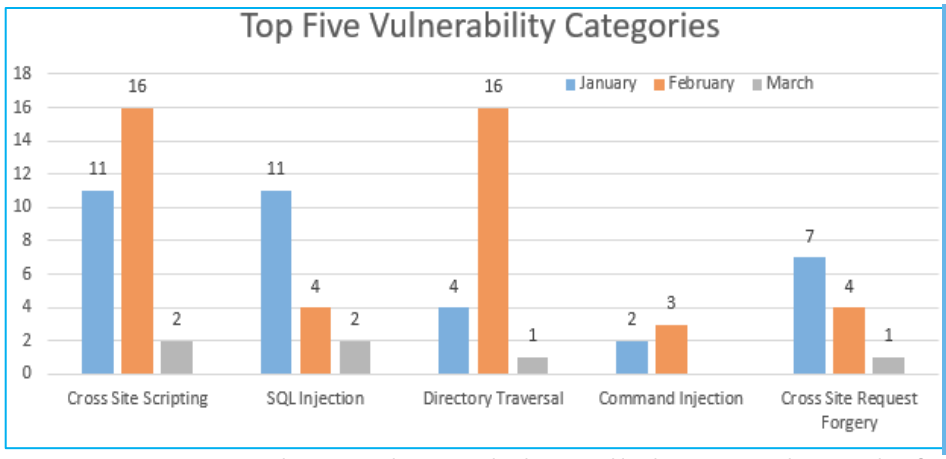
Vulnerability Trend:



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

86% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

14% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



From the graph, we infer that maximum Cross Site Scripting & Directory Traversal vulnerabilities were discovered in December compared to other months and categories so far.

Medium no. of SQL Injection attacks was found in all the months.

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.

Details:

S. No.	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage
1.	Cross Site Scripting	CVE-2019-9550	DhCms up to 2017-09-18 cross site scripting [CVE-2019-9550]	A vulnerability has been found in DhCms up to 2017-09-18 (Content Management System) and classified as problematic. Affected by this vulnerability is a functionality of the file *admin.php?r=admin/Index/index*. The manipulation with an unknown input leads to a cross site scripting vulnerability. The CWE definition for the vulnerability is CWE-80. As an impact it is known to affect integrity. An attacker might be able to inject arbitrary html and script code into the website.	Protected by Default Rules.
		CVE-2019-8279	Vanilla Forums up to 2.4 Message Stored cross site scripting	A vulnerability, which was classified as problematic, has been found in Vanilla Forums up to 2.4 (Forum Software). Affected by this issue is some functionality. The manipulation as part of a *Message* leads to a cross site scripting vulnerability (Stored). Using CWE to declare the problem leads to CWE-80. Impacted is integrity. An attacker might be able to inject arbitrary html and script code into the website.	Protected by Default Rules.
2.	SQL Injection	CVE-2019-4032	IBM 3.1.0 sql injection [CVE-2019-4032]	A vulnerability was found in IBM Financial Transaction Manager for Digital Payments for Multi-Platform 3.1.0 (Financial Software). It has been declared as critical. This vulnerability affects a code block. The manipulation with an unknown input lead to a	Protected by Default Rules.

				sql injection vulnerability. The CWE definition for the vulnerability is CWE-89. As an impact it is known to affect confidentiality, integrity, and availability. An attacker might be able to inject and/or alter existing SQL statements which would influence the database exchange.	
		CVE-2018-17988	LayerBB 1.1.1 Search search.php search_query sql injection	A vulnerability, which was classified as critical, was found in LayerBB 1.1.1. This affects a function of the file *search.php* of the component *Search*. The manipulation of the argument search_query as part of a *Parameter* leads to a sql injection vulnerability. CWE is classifying the issue as CWE-89. This is going to have an impact on confidentiality, integrity, and availability. An attacker might be able inject and/or alter existing SQL statements which would influence the database exchange.	Protected by Default Rules.
3.	Directory Traversal	CVE-2019-9622	eBrigade up to 4.5 showfile.php file directory traversal	A vulnerability, which was classified as problematic, was found in eBrigade up to 4.5. Affected is a function of the file *showfile.php*. The manipulation of the argument file with the input value ../ leads to a directory traversal vulnerability. CWE is classifying the issue as CWE-22. This is going to have an impact on confidentiality. The weakness was disclosed 03/07/2019 as *EDB-ID 46109* as uncorroborated exploit (Exploit-DB). The advisory is shared for download at exploit-db.com.	Protected by Default Rules.

4.	Cross Site Request Forgery	CVE-2019-9549	PopojiCMS 2.0.1 route.php cross site request forgery	A vulnerability, which was classified as problematic, was found in PopojiCMS 2.0.1 (Content Management System). Affected is a function of the file *po-admin/route.php?mod=user&act=addnew*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. CWE is classifying the issue as CWE-352. This is going to have an impact on integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness was shared on 03/03/2019. This vulnerability is traded as CVE-2019-9549.	Protected by Custom Rules.