Weekly Zero-Day Vulnerability Coverage Bulletin

(11th March – 17th March)

Summary:

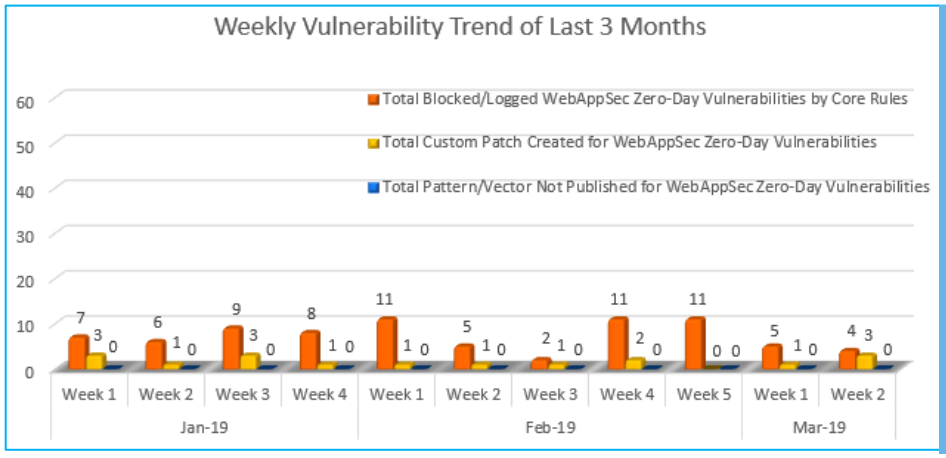
Total **7 Zero-Day Vulnerabilities** were discovered in **4 Categories** previous week

1	1	2	3
Cross Site Scripting	SQL Injection	Directory Traversal	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	4
Zero-Day Vulnerabilities Protected through Custom Rules	3*
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

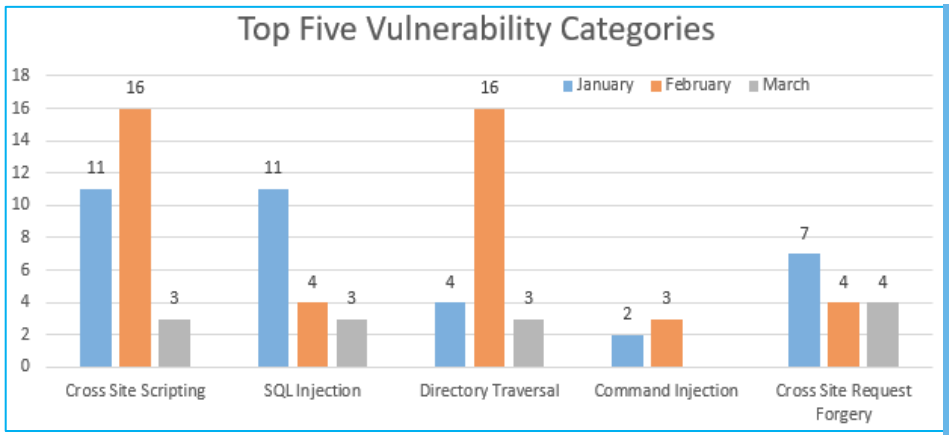
Vulnerability Trend:



Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a quarter.

84% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

16% 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	NA	WordPress shopping sites under attack	The plugin, which we'll be referring to by its slug woocommerce-abandoned-cart, allows the owners of WooCommerce sites to track abandoned shopping carts in order to recover those sales. A lack of sanitation on both input and output allows attackers to inject malicious JavaScript payloads into various data fields, which will execute when a logged-in user with administrator privileges views the list of abandoned carts from their WordPress dashboard.	Protected by Default Rules.
2.	SQL Injection	CVE-2019-9693	CMS Made Simple up to 2.2.9 class.showtime2_data.php Parameter sql injection	A vulnerability was found in CMS Made Simple up to 2.2.9 (Content Management System) and classified as critical. Affected by this issue is a part of the file *class.showtime2_data.php*. The manipulation as part of a *Parameter* leads to a sql injection vulnerability. Using CWE to declare the problem leads to CWE-89. Impacted is confidentiality, integrity, and availability. An attacker might be able inject and/or alter existing SQL statements which would influence the database exchange. The weakness was released 03/11/2019.	Protected by Default Rules.
3.	Directory Traversal	CVE-2019-9686	Pacman up to 5.1.2 Remote Package Installation lib/libalpm/dload.c	A vulnerability was found in Pacman up to 5.1.2 and classified as critical. This issue affects a part in the library *lib/libalpm/dload.c* of	Protected by Default Rules.

			Content-Disposition Header directory traversal	the component *Remote Package Installation*. The manipulation as part of a *Content-Disposition Header* leads to a directory traversal vulnerability (Code Execution). Using CWE to declare the problem leads to CWE-22. Impacted is confidentiality, integrity, and availability. The weakness was shared 03/11/2019. The identification of this vulnerability is CVE-2019-9686 since 03/11/2019. The attack may be initiated remotely.	
		CVE-2019-9662	JTBC(PHP) 3.0.1.8 Cache Management inc.php String directory traversal	A vulnerability, which was classified as problematic, has been found in JTBC(PHP) 3.0.1.8 (Programming Language Software). Affected by this issue is some functionality of the file *inc.php* of the component *Cache Management*. The manipulation with the input value ../ leads to a directory traversal vulnerability. Using CWE to declare the problem leads to CWE-22. Impacted is integrity, and availability. The weakness was released 03/11/2019. This vulnerability is handled as CVE-2019-9662 since 03/10/2019.	Protected by Default Rules.
4.	Cross Site Request Forgery	CVE-2019-9652	SDcms 1.7 filename/t2 cross site request forgery	A vulnerability was found in SDcms 1.7 (Content Management System). It has been classified as problematic. This affects code. The manipulation of the argument filename/t2 as part of a *Parameter* leads to a cross site request forgery vulnerability. CWE is classifying the issue as CWE-352. This is going to have an impact on	Protected by Custom Rules.

			integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness was released 03/11/2019.	
	CVE-2019-9688	sftnow up to 2018-12-29 index.php cross site request forgery	A vulnerability was found in sftnow up to 2018-12-29. It has been declared as problematic. Affected by this vulnerability is a code block of the file *index.php?g=Admin&m=User&a=add_post*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. The CWE definition for the vulnerability is CWE-352. As an impact it is known to affect integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness was released 03/11/2019. This	Protected by Custom Rules.
	CVE-2019-9769	PilusCart 1.4.1 index.php cross site request forgery	A vulnerability was found in PilusCart 1.4.1. It has been classified as problematic. This affects code of the file *index.php?module=users&action=newUser*. 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 released 03/14/2019 as *EDB-ID 46531* as uncorroborated exploit (Exploit-DB).	Protected by Custom Rules.