Weekly Zero-Day Vulnerability Coverage Bulletin

(20th May – 26th May)

Summary:

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

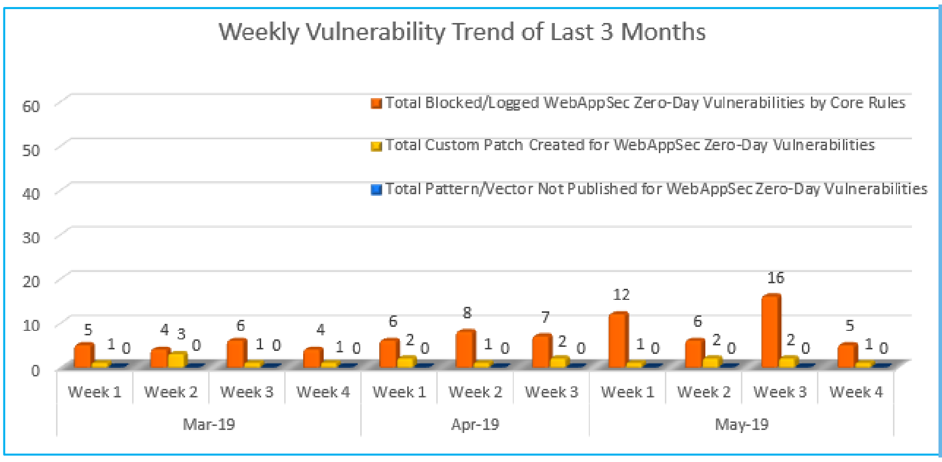
2	**2**	**1**	**1**
Cross Site Scripting	SQL Injection	Cross Site Request Forgery	Directory Traversal

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

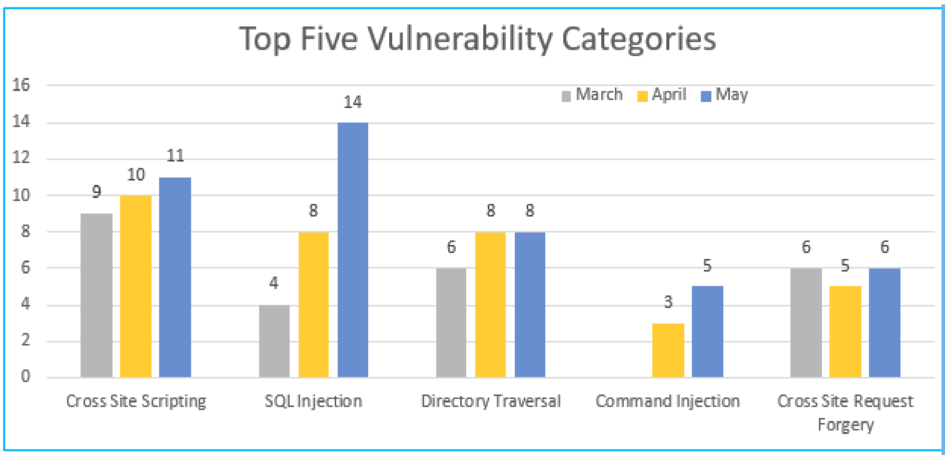
Vulnerability Trend:



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

83% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

17% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



From the graph, we infer that maximum no. of Cross Site Scripting and SQL Injection vulnerabilities are discovered in May compared to other months.

No Command Injection vulnerabilities are found in March

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-2019-11809	Joomla CMS up to 3.9.5 com_users cross site scripting	A vulnerability, which was classified as problematic, has been found in Joomla CMS up to 3.9.5 (Content Management System). This issue affects some functionality of the component *com_users*. The manipulation with an unknown input leads to a cross site scripting vulnerability. 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. This would alter the appearance.	Protected by Default Rules.
		CVE-2019-112	CMS Made Simple up to 2.2.10 m1_title Persistent cross site scripting [Disputed]	A vulnerability, which was classified as problematic, was found in CMS Made Simple up to 2.2.10 (Content Management System). Affected is a function. The manipulation of the argument m1_title with an unknown input leads to a cross site scripting vulnerability (Persistent). CWE is classifying the issue as CWE-80. This is going to have an impact on integrity. An attacker might be able to inject arbitrary html and script code into the website. This would alter the appearance.	Protected by Default Rules.
2.	SQL Injection	CVE-2019-12251	UCMS 1.4.7 sadmin/ceditpost.php cvalue sql injection	A vulnerability was found in UCMS 1.4.7. It has been classified as critical. Affected is code of the file *sadmin/ceditpost.php*. The manipulation of the argument cvalue 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,	Protected by Default Rules.

				and availability. An attacker might be able inject and/or alter existing SQL statements which would influence the database exchange. The weakness was shared in 05/21/2019.	
		CVE-2019-12239	WP Booking System 1.5.1 on WordPress sql injection [CVE-2019-12239]	A vulnerability was found in WP Booking System 1.5.1 on WordPress (WordPress Plugin) and classified as critical. Affected by this issue is a part. The manipulation with an unknown input lead 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 shared in 05/20/2019. This vulnerability is handled as CVE-2019-12239.	Protected by Default Rules.
3.	Cross Site Request Forgery	CVE-2019-12253	My Little Forum up to 2.4.19 Post cross site request forgery	A vulnerability was found in My Little Forum up to 2.4.19 (Forum Software). It has been declared as problematic. Affected by this vulnerability is a code block of the component *Post Handler*. 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 and availability. An attacker might be able force legitimate users to initiate unwanted actions within the web.	Protected by Custom Rules.

4.	Directory Traversal	CVE-2019-9892	Open Ticket Request System up to 5.0.34/6.0.17/7.0.6 Report directory traversal	A vulnerability was found in Open Ticket Request System up to 5.0.34/6.0.17/7.0.6 (Ticket Tracking Software). It has been declared as critical. This vulnerability affects a code block of the component *Report Handler*. The manipulation with an unknown input leads to a directory traversal vulnerability. The CWE definition for the vulnerability is CWE-91. As an impact it is known to affect confidentiality. The weakness was shared in 05/22/2019. The advisory is shared for download at community.otrs.com. This vulnerability was named as CVE-2019-9892.	Protected by Default Rules.