Weekly Zero-Day Vulnerability Coverage Bulletin

(11th June – 17th June)

Summary:

Total **5 Zero-Day Vulnerabilities** were discovered in **2 Categories** previous week

4

Cross Site Scripting

1

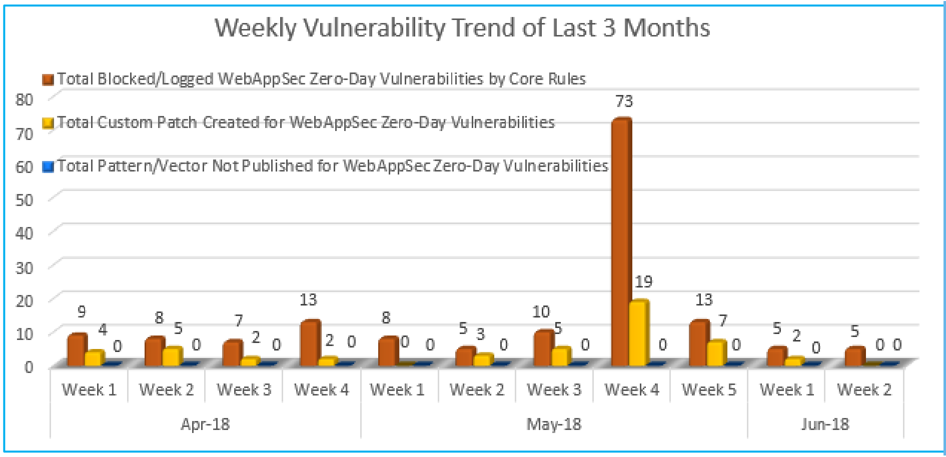
SQL Injection

Zero-Day Vulnerabilities Protected through Core Rules	5
Zero-Day Vulnerabilities Protected through Custom Rules	0*
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:

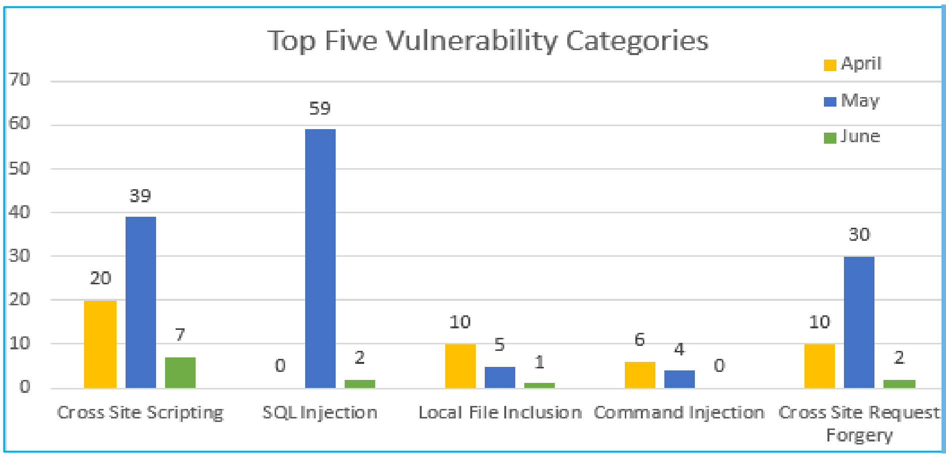


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

May 4th Week has multiple vulnerabilities blocked by Core Rules.

75% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

25% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



From the graph, we infer that multiple SQL Injection vulnerabilities were discovered in May compared to other months and categories.

Medium no. of Cross Site Scripting attacks was found in May compared to June.

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-2018-12099	Grafana up to 5.1 Dashboard cross site scripting	A vulnerability was found in Grafana up to 5.1 and classified as problematic. Affected by this issue is an unknown function of the component *Dashboard*. 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 web site. This would alter the appearance and would make it possible to initiate further attacks.	Protected by Default Rules.
		CVE-2018-12273	Ximdex 4.0 DMS /edit Ciudad/Nombre cross site scripting	A vulnerability was found in Ximdex 4.0. It has been declared as problematic. This vulnerability affects an unknown function of the file */edit* of the component *DMS*. The manipulation of the argument Ciudad/Nombre as part of a *Parameter* 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 web site.	Protected by Default Rules.
		CVE-2018-12272	Ximdex 4.0 xowl/request.php content cross site scripting	A vulnerability was found in Ximdex 4.0. It has been classified as problematic. This affects an unknown function of the file *xowl/request.php*. The manipulation of the argument content as part of a *Parameter* leads to a cross site scripting vulnerability. CWE is classifying the issue as CWE-80. This is going to have an impact on integrity. An attacker might be able to inject	Protected by Default Rules.

				arbitrary html and script code into the web site. This would alter the appearance and would make possible to initiate further attacks.	
		CVE-2018-5754	Open-Xchange OX AppSuite up to 7.8.3-rev11/7.8.4-rev8 Office-Web cross site scripting	A vulnerability classified as critical was found in Open-Xchange OX AppSuite up to 7.8.3-rev11/7.8.4-rev8. Affected by this vulnerability is an unknown function of the component *Office-Web*. 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 confidentiality. An attacker might be able to inject arbitrary html and script code into the web site. This would alter the appearance and would make it possible to initiate further attacks.	Protected by Default Rules.
2.	SQL Injection	CVE-2018-12110	portfolioCMS 1.0.5 admin/portfolio.php preview sql injection	A vulnerability was found in portfolioCMS 1.0.5. It has been rated as critical. This issue affects an unknown function of the file *admin/portfolio.php*. The manipulation of the argument preview 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 disclosed 06/11/2018.	Protected by Default Rules.