Weekly Zero-Day Vulnerability Coverage Bulletin

(28th May – 3rd June)

Summary:

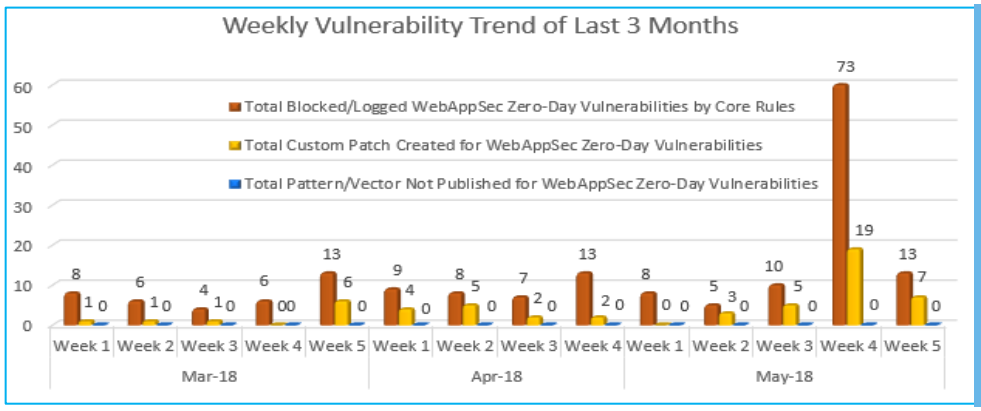
Total **20 Zero-Day Vulnerabilities** were discovered in **5 Categories** previous week

4	7	2	1	6
Cross Site Scripting	SQL Injection	Local File Inclusion	Arbitrary File Upload	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	13
Zero-Day Vulnerabilities Protected through Custom Rules	7*
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

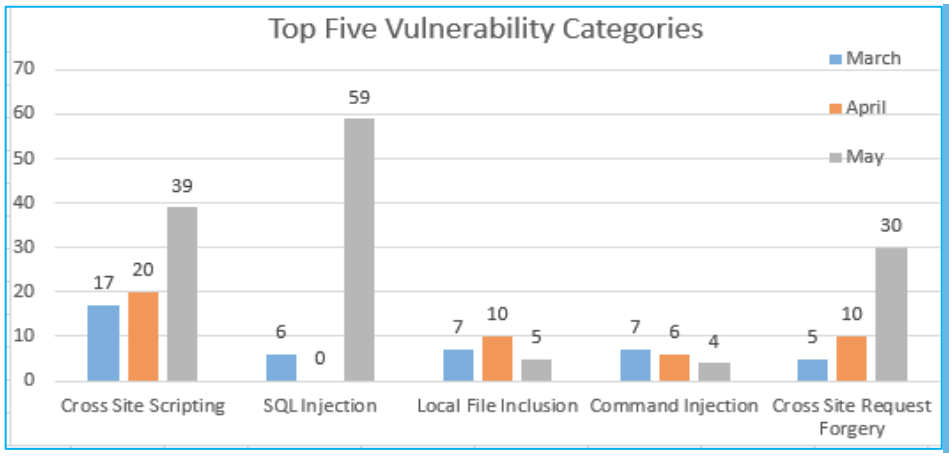
Vulnerability Trend:



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

78% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

22% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



From the graph, we infer that multiple no. of Cross Site Scripting, SQL Injection, and Cross Site Request Forgery vulnerabilities are discovered in May.

Whereas in previous months Cross Site Scripting attacks are more compared to other categories.

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-2018-11512	wityCMS 0.6.1 Website Name cross site scripting	A vulnerability classified as problematic has been found in wityCMS 0.6.1. This affects an unknown function of the component *Website Name Handler*. The manipulation with the input value <scri<script>pt>alert(1)</scri</script>pt> 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 arbitrary html and script code into the web site. This would alter the appearance and would make it possible to initiate.	Protected by Default Rules.
		CVE-2018-11512	wityCMS 0.6.1 - Cross-Site Scripting	A persistent/stored cross-site scripting (XSS) vulnerability in the "Website's name" field found in the "Settings" page under the General" menu in Creatiwity wityCMS 0.6.1 allows remote attackers to inject arbitrary web script or HTML via a crafted website name by going an authenticated POST HTTP request to admin/settings/general.	Protected by Default Rules.
		CVE-2018-11430	Moderator Log Notes Plugin 1.1 on MyBB modCP cross site scripting	A vulnerability, which was classified as problematic, was found in Moderator Log Notes Plugin 1.1 on MyBB. Affected is an unknown function of the component *modCP*. The manipulation with an unknown input 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 arbitrary html and script code into the web site. This would alter the appearance and would make it.	Protected by Default Rules.

		CVE-2018-11532	MyBB ChangUonDyU Plugin 1.0.2 - Cross-Site Scripting	This plugin displays advanced statistics on the index page such as latest posts with auto refresh using AJAX.	Protected by Default Rules.
2.	SQL Injection	EDB-ID: 44785	Wordpress Plugin Events Calendar - SQL Injection	Wordpress Plugin Events Calendar - SQL Injection.	Protected by Default Rules.
		EDB-ID: 44786	Joomla! Component Full Social 1.1.0 - 'search_query' SQL Injection	Joomla! Component Full Social 1.1.0 - 'search_query' SQL Injection.	Protected by Default Rules.
		EDB-ID: 44799	Facebook Clone Script 1.0.5 - 'search' SQL Injection	Facebook Clone Script 1.0.5 - 'search' SQL Injection.	Protected by Default Rules.
		CVE-2018-11535	Sitemakin SLAC 1.0 - 'my_item_search' SQL Injection	Sitemakin SLAC 1.0 - 'my_item_search' SQL Injection.	Protected by Default Rules.
		EDB-ID: 44792	IssueTrak 7.0 - SQL Injection	IssueTrak 7.0 - SQL Injection.	Protected by Default Rules.
		CVE-2018-10094	Dolibarr 7.0.0 - SQL Injection	Dolibarr is an "Open Source ERP & CRM for Business" used by many companies worldwide.	Protected by Default Rules.
		EDB-ID: 44823	Smartshop 1 - 'id' SQL Injection	Smartshop 1 suffers from sql injection which attacker can inject sql commands.	Protected by Default Rules.
3.	Local File Inclusion	CVE-2018-11522	Yosoro 1.0.4 - Remote Code Execution	Yosoro 1.0.4 - Remote Code Execution.	Protected by Default Rules.
		EDB-ID: 44809	TAC Xenta 511/911 - Directory Traversal	Devices are not indexed by crawlers like Shodan or Censys due to ancient SSL configuration, needed to use old browser to support it not even s_client, curl or ncat could connect).	Protected by Default Rules.
4.	Arbitrary File Upload	CVE-2018-11523	NUUO NVRmini2 / NVRsolo - Arbitrary File Upload	Recetly, I found an Arbitrary File Upload Vulnerability in 'NUUO NVRmini2' program, NVRmini2 is widely used all over the world.	Protected by Custom Rules.
5.	Cross Site Request Forgery	EDB-ID: 44788	Joomla! Component jCart for OpenCart 2.3.0.2 - Cross-Site Request Forgery	Joomla! Component jCart for OpenCart 2.3.0.2 - Cross-Site Request Forgery.	Protected by Custom Rules.

EDB-ID: 44789	Joomla! Component JoomOCShop 1.0 - Cross-Site Request Forgery	Joomla! Component JoomOCShop 1.0 - Cross-Site Request Forgery.	Protected by Custom Rules.
EDB-ID: 44800	Facebook Clone Script 1.0.5 - Cross-Site Request Forgery	Facebook Clone Script 1.0.5 has CSRF vulnerability which attacker can easily change user information.	Protected by Custom Rules.
CVE-2018-11538	SearchBlox 8.6.6 - Cross-Site Request Forgery	Using Cross-Site Request Forgery (CSRF), an attacker can force a user who is currently authenticated with a web application to execute an unwanted action. The attacker can trick the user into loading a page which may send a request to perform the unwanted action in the background. In the case of Searchblox, we can use CSRF to perform actions on the admin dashboard by targeting an administrator.	Protected by Custom Rules.
EDB-ID: 44824	Smartshop 1 - Cross-Site Request Forgery	Smartshop 1 - Cross-Site Request Forgery.	Protected by Custom Rules.
CVE-2018-11671	GreenCMS 2.3.0603 - Cross-Site Request Forgery (Add Admin)	n issue was discovered in GreenCMS v2.3.0603. There is a CSRF vulnerability that can add an admin account via index.php?m=admin&c=access&a=adduserhandle.	Protected by Custom Rules.