Weekly Zero-Day Vulnerability Coverage Bulletin

(1st October – 7th October)

Summary:

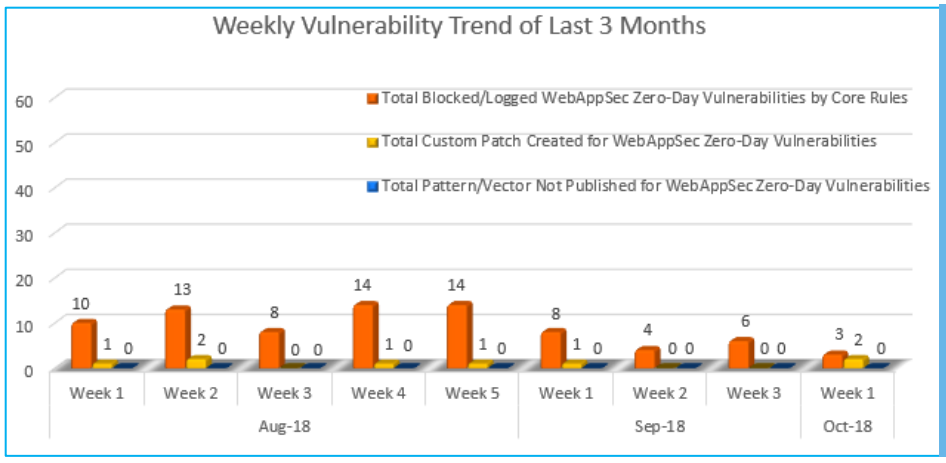
Total **5 Zero-Day Vulnerabilities** were discovered in **3 Categories** this week

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

Zero-Day Vulnerabilities Protected through Core Rules	3
Zero-Day Vulnerabilities Protected through Custom Rules	2*
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

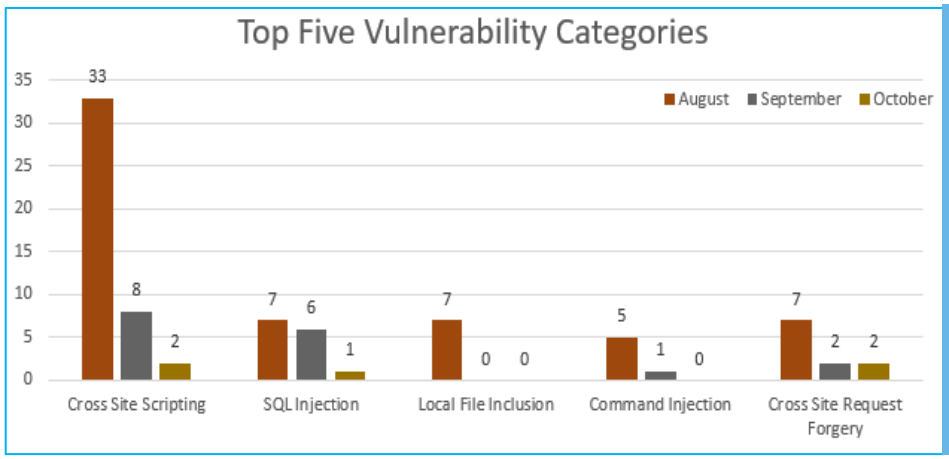
Vulnerability Trend:



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

87% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

13% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



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

Medium no. of SQL Injection attacks was found in August and September.

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-2018-17593	AirTies Air 5453 1.0.0.18 top.html productboardtype cross site scripting	A vulnerability was found in AirTies Air 5453 1.0.0.18. It has been declared as problematic. This vulnerability affects an unknown function of the file *top.html*. The manipulation of the argument productboardtype 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-2018-1602	IBM Rational Quality Manager up to 6.0.6 Web UI cross site scripting	A vulnerability, which was classified as problematic, has been found in IBM Rational Quality Manager up to 6.0.6. Affected by this issue is an unknown function of the component *Web UI*. 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.	Protected by Default Rules.
2.	SQL Injection	CVE-2018-17852	WUZHI CMS 4.1.0 card.php groupname sql injection	A vulnerability was found in WUZHI CMS 4.1.0 and classified as critical. This issue affects an unknown function of the file *coreframe/app/coupon/admin/card.php*. The manipulation of the argument groupname 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	Protected by Default Rules.

				database exchange. The weakness was disclosed in 10/01/2018.	
3.	Cross Site Request Forgery	CVE-2018-17826	HisiPHP 1.0.8 adduser.html cross site request forgery	A vulnerability was found in HisiPHP 1.0.8. It has been rated as problematic. Affected by this issue is an unknown function of the file *admin.php/admin/user/adduser.html*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. Using CWE to declare the problem leads to CWE-352. Impacted is integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness was disclosed 10/01/2018. This vulnerability is handled as CVE-2018-17826 since 09/30/2018.	Protected by Custom Rules.
		CVE-2018-17869	Dasan H660GW cross site request forgery [CVE-2018-17869]	A vulnerability was found in Dasan H660GW (the affected version is unknown). It has been classified as problematic. Affected is an unknown function. 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 10/01/2018. This vulnerability is traded as CVE-2018-17869	Protected by Custom Rules.