Weekly Zero-Day Vulnerability Coverage Bulletin

October 2020

Total Zero Day Vulnerabilities found: 20

Injection Attack	BOT Attack	CSRF	HTML Application Attack	SQL Injection	Cross Site Scripting	XML External Entity
1	1	1	1	3	12	1

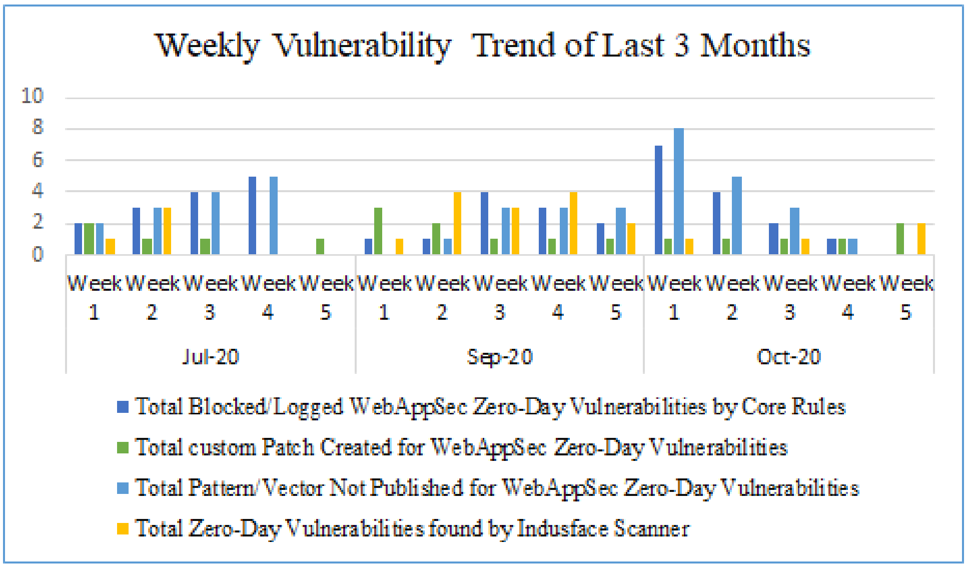
Zero-Day Vulnerabilities Protected through Core Rules	14
Zero-Day Vulnerabilities Protected through Custom Rules	6 *
Zero-Day Vulnerabilities for which protection cannot be determined	0 **
Zero-Day Vulnerabilities found by Indusface WAS	17

* 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:

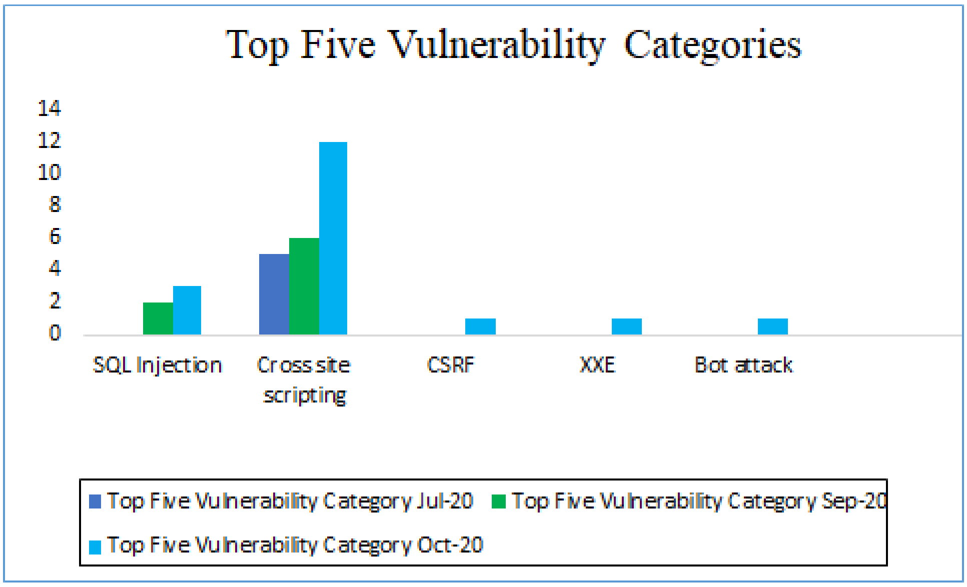
Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.



70% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

30% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

85% Of Zero-Day Vulnerabilities were reported by Indusface Scanner in last quarter



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.

S. No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
1	A1: Injection	CVE-2020-14882	Attackers Exploiting WebLogic Servers via CVE-2020-14882 to install Cobalt Strike,https://github.com/chacka0101/exploits/blob/master/CVE-2020-14882/README.md	Starting late last week, we observed a large number of scans against our WebLogic honeypots to detect if they are vulnerable to CVE-2020-14882. CVE-2020-14882 was patched about two weeks ago as part of Oracle's quarterly critical patch update. In addition to scans simply enumerating vulnerable servers, we saw a small number of scans starting on Friday (Oct. 30th) attempting to install crypto-mining tools [1].	Protected by custom rules	NA

2	Bot Attack	NA	KashmirBlack Botnet Attacked Popular CMSs Like WordPress & Joomla	In this digital age, several websites get attacked daily due to data breach, brute force, vulnerabilities, or any other reasons. A variety of attacks occur on different platforms of different types, scope, and volume. And one such is a highly advanced botnet called KashmirBlack that has mainly infected hundreds of thousands of websites by attacking popular CMS (Content Management System) platforms like WordPress, Joomla, and Drupal.	Protected by custom rules	NA
3	CSRF	CVE-2020-15299	WordPress File Manager plugin flaw causing website hijack exploited in the wild	WordPress File Manager plugin flaw causing website hijack exploited in the wild	Protected by custom rules	NA
4	HTML Application Attack	NA	New Snort, ClamAV coverage strikes back against Cobalt Strike	We recently released a more granular set of updated SNORT® and ClamAV® detection signatures to detect attempted obfuscation and exfiltration of data via Cobalt Strike, a common toolkit often used by	Protected by custom rules.	NA

5	XML External Entity Attack	CVE-2020-21524	WordPress XXE vulnerability	There is a XML external entity (XXE) vulnerability in halo v1.1.3, The function of importing other blogs in the background(/api/admin/migrations/wordpress) needs to parse the xml file, but it is not used for security defense, This vulnerability can detect the intranet, read files, enable ddos attacks, etc. exp:https://github.com/halo-dev/halo/issues/423	Protected by custom rules.	NA
6	SQL Injection	CVE-2020-15487	Re:Desk 2.3 Password Reset Ticket.php getBaseCriteria() folder sql injection	A vulnerability classified as critical was found. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by scanner as SQL Injection attack.
		CVE-2020-24569	MB Connect Line mymbCONNECT24 /mbCONNECT24 up to 2.6.1 knximport sql injection	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.1. There is a blind SQL injection in the knximport component via an advanced attack vector, allowing logged in attackers to discover arbitrary information.	Protected by core rules.	Detected by scanner as SQL Injection attack.

	CVE-2012-2311, CVE-2012-1823	Top 10 most common CVE numbers involved	From May 1-July 21, 2020, Unit 42 researchers captured global network traffic from firewalls around the world and then analyzed the data to examine the latest network attack trends. The majority of attacks we observed were classified as high severity (56.7%), and nearly one quarter (23%) were classified as critical. The most common vulnerabilities exploited were CVE-2012-2311 and CVE-2012-1823, both command injection vulnerabilities in PHP CGI scripts. This indicates that attackers are looking for exploits with high impact.	Protected by custom rules.	Detected by scanner as SQL Injection attack.

7	Cross Site Scripting	CVE-2020-21527	Halo CMS up to 1.1.3 Backup File directory traversal	A vulnerability was found in Content Management System. It has been declared as critical. Affected by this vulnerability is some unknown functionality of the component Backup File Handler. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2020-24861	GetSimple CMS 3.3.16 Settings Page permalink Persistent cross site scripting	A vulnerability was found in CMS 3.3.1Content Management System and classified as problematic. This issue affects an unknown functionality of the component Settings Page. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2020-8238	Pulse Connect Secure/Pulse Policy Secure up to 9.1R8.1 Web Interface cross site scripting	A vulnerability was found in Pulse Connect Sec. It has been declared as problematic. This vulnerability affects an unknown functionality of the component Web Interface.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.

		Upgrading to version 9.1R8.2 eliminates this vulnerability.		
CVE-2019-20921	bootstrap-select up to 1.13.5 OPTION Element cross site scripting	A vulnerability was found and classified as problematic. Affected by this issue is an unknown code of the component. Upgrading to version 1.13.6 eliminates this vulnerability.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
CVE-2020-14223	HCL Digital Experience 8.5/9.0/9.5 Reflected cross site scripting	HCL Digital Experience 8.5, 9.0, 9.5 is susceptible to cross-site scripting (XSS). The vulnerability could be employed in a reflected or non-persistent XSS attack.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
CVE-2020-26166	qdPM 9.1 File Upload cross site scripting	The file upload functionality in qdPM 9.1 doesn't check the file description, which allows remote authenticated attackers to inject web script or HTML via the attachments info parameter, aka XSS. This can occur during creation of a ticket, project, or task.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
CVE-2020-7741	hellojs Package up to 1.18.5 oauth_redirect cross site scripting	This affects the package hellojs before 1.18.6. The code get the param oauth_redirect from url and pass it to	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.

			location.assign without any check and sanitisation. So we can simply pass some XSS payloads into the url param oauth_redirect, such as javascript:alert(1) .		
	NA	Post Grid WordPress Plugin Flaws Allow Site Takeovers	Two high-severity vulnerabilities in Post Grid, a WordPress plugin with more than 60,000 installations, opens the door to site takeovers, according to researchers. To boot, nearly identical bugs are also found in Post Grid's sister plug-in, Team Showcase, which has 6,000 installations.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
	CVE-2020-26934	phpMyAdmin up to 4.9.5/5.0.2 Transformation Feature cross site scripting	A vulnerability was found in phpMyAdmin up to 4.9.5/5.0.2 (Database Administration Software). It has been rated as problematic. This issue affects an unknown functionality of the component Transformation Feature. The manipulation with an unknown input leads to a cross site scripting vulnerability.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.

			Using CWE to declare the problem leads to CWE-79. 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 against site visitors. The summary by CVE is:		
	CVE-2020-14184	Atlassian JIRA Server up to 8.5.8/8.12.2/8.13.0 Issue Filter Export File cross site scripting	A vulnerability was found in Atlassian JIRA Server up to 8.5.8/8.12.2/8.13.0 (Bug Tracking Software) and classified as problematic. This issue affects an unknown function of the component Issue Filter Export File Handler. The manipulation with an unknown input leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to CWE-79. Impacted is integrity. An attacker might be able to inject arbitrary html and script code into the web site.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.

			This would alter the appearance and would make it possible to initiate further attacks against site visitors. The summary by CVE is:		
	CVE-2020-8820	Webmin up to 1.941 Cluster Shell Commands Endpoint cross site scripting	A vulnerability was found in Webmin up to 1.941 (Software Management Software). It has been rated as problematic. Affected by this issue is an unknown functionality of the component Cluster Shell Commands Endpoint. The manipulation with an unknown input leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to CWE-79. 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 against site visitors. CVE summarizes:	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
	NA	Cross-site Scripting in React Web Applications	React is a popular JavaScript	Protected by core rules.	Detected by scanner as Cross Site

	framework for building user interfaces. This article shows why it was developed, how it handles user-controlled inputs, and what you should do to prevent cross-site scripting when working with React’s type, props, and children attributes.	Scripting attack.