Weekly Zero-Day Vulnerability Coverage Bulletin

(13th May – 19th May)

Summary:

Total **18 Zero-Day Vulnerabilities** were discovered in **6 Categories** previous week

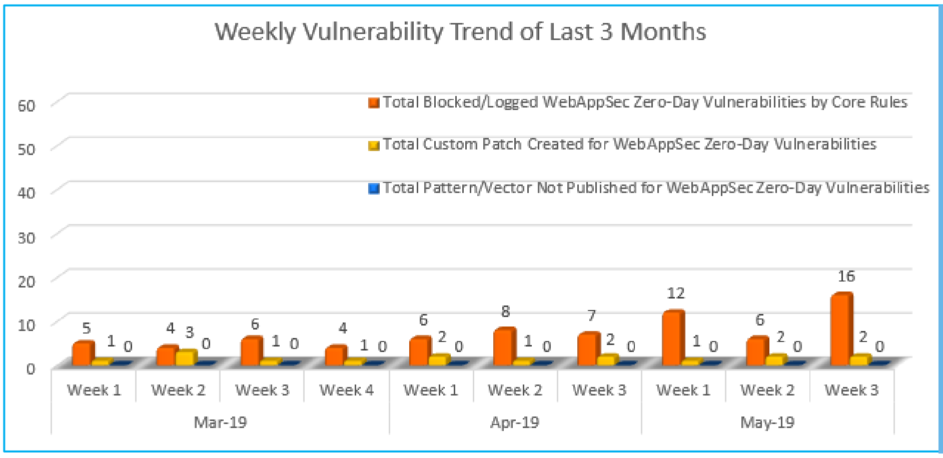
4	**1**	**6**	**4**	**2**	**1**
Cross Site Scripting	PHP Injection	SQL Injection	Directory Traversal	Cross Site Request Forgery	Command Injection

Zero-Day Vulnerabilities Protected through Core Rules	16
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

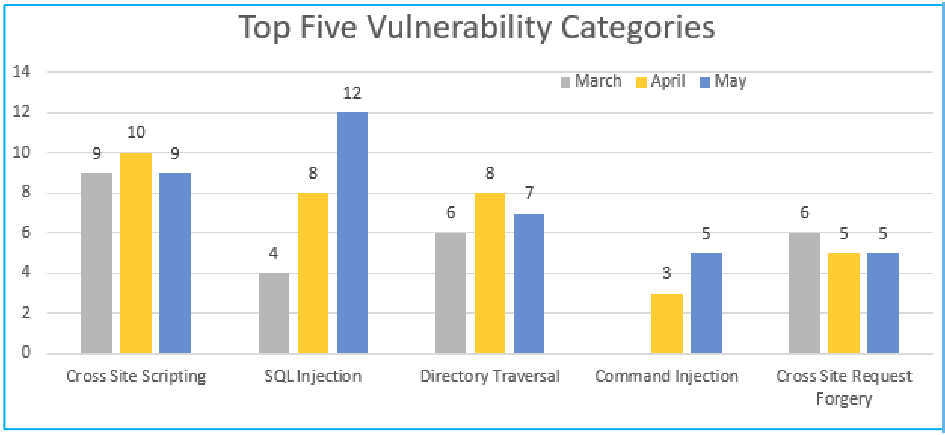
Vulnerability Trend:



Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a 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 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-2018-16139	BIBLIOsoft BIBLIOpac 2018 bin/wxis.exe/bibliopac/ db/action cross site scripting	A vulnerability was found in BIBLIOsoft BIBLIOpac 2018 and classified as problematic. This issue affects a part of the file *bin/wxis.exe/bibliopac/*. The manipulation of the argument db/action as part of a *Parameter* 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	Protected by Default Rules.
		CVE-2019-8391	qdPM 9.1 configuration type cross site scripting	A vulnerability was found in qdPM 9.1. It has been rated as problematic. This issue affects some processing of the file *configuration*. The manipulation of the argument type as part of a *Parameter* 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	Protected by Default Rules.
		CVE-2019-8390	qdPM 9.1 search[keywords] cross site scripting	A vulnerability was found in qdPM 9.1. It has been declared as problematic. This vulnerability affects a code block. The manipulation of the argument search[keywords] as part of a *Parameter* leads to a cross site scripting	Protected by Default Rules.

				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 website. This would alter the appearance and would make it possible.	
		CWE-80	WolfCMS up to 0.8.3.1 User Add name cross site scripting	A vulnerability was found in WolfCMS up to 0.8.3.1. It has been rated as problematic. This issue affects some processing of the file */wolfcms/?/admin/user/add* of the component *User Add*. The manipulation of the argument name 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.	PHP Injection	CVE-2019-11185	Alert logic Uncovers New Vulnerability in WordPress WP Live Chat – CVE-2019-11185 WordPress plugin sees second serious security bug in six weeks	A vulnerability was found in WP Live Chat Support up to 8.0.26 on WordPress (Chat Software). It has been classified as critical. This affects code of the component File Upload. The manipulation as part of a POST Request leads to a privilege escalation vulnerability. CWE is classifying the issue as CWE-269. This is going to have an impact on confidentiality, integrity, and availability. The weakness was released 06/03/2019. This vulnerability is uniquely identified as CVE-2019-11185 since 04/11/2019. It is possible to initiate the	Protected by Default Rules.

				attack remotely. No form of authentication is needed for exploitation. Neither technical details nor an exploit is publicly available. The price for an exploit might be around USD $0-$5k at the moment (estimation calculated on 06/04/2019).	
3.	SQL Injection	CVE-2017-12760	Ynet Interactive Mobiketa 4.0 Code Execution sql injection	A vulnerability was found in Ynet Interactive Mobiketa 4.0. It has been declared as critical. This vulnerability affects a code block. The manipulation with an unknown input lead to a sql injection vulnerability (Code Execution). The CWE definition for the vulnerability is CWE-89. As an impact it is known to affect 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 presented 05/09/2019. This vulnerability was	Protected by Default Rules.
		CVE-2017-12758	Appointment Component 1.1 on Joomla Code Execution sql injection	A vulnerability was found in Appointment Component 1.1 on Joomla (Appointment Software) and classified as critical. Affected by this issue is a part. The manipulation with an unknown input lead to a sql injection vulnerability (Code Execution). 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 released	Protected by Default Rules.

		05/09/2019. This vulnerability is handled as CVE-2017-12758.	
CVE-2017-12757	Ambit Technologies iTech B2B Script Code Execution sql injection	A vulnerability has been found in Ambit Technologies iTech B2B Script, Tech Business Networking Script, Tech Caregiver Script, Tech Classifieds Script, Tech Dating Script, Tech Freelancer Script, Tech Image Sharing Script, Tech Job Script, Tech Movie Script, Tech Multi-Vendor Script and Tech Social Networking Script and classified as critical. Affected by this vulnerability is a functionality. The manipulation with an unknown input lead to a sql injection vulnerability (Code Execution). The CWE definition for the vulnerability is CWE-89.	Protected by Default Rules.
NA	Sqlite3 Window Function Remote Code Execution Vulnerability	An exploitable use after free vulnerability exists in the window function functionality of Sqlite3 3.26.0. A specially crafted SQL command can cause a use after free vulnerability, potentially resulting in remote code execution. An attacker can send a malicious SQL command to trigger this vulnerability.	Protected by Default Rules.
CVE-2019-11600	OpenProject up to 8.3.1 Activities API id sql injection	A vulnerability was found in OpenProject up to 8.3.1 (Project Management Software). It has been rated as critical. Affected by this issue is some processing of the component *Activities API*. The manipulation of the argument id as part of a *Parameter* leads to a sql injection vulnerability. Using CWE to declare the problem leads to CWE-89. Impacted is	Protected by Default Rules.

				confidentiality, integrity, and availability. An attacker might be able inject and/or alter existing SQL statements which would influence the database exchange.	
		CVE-2018-18800	Tubigan Welcome to our Resort 1.0 index.php q sql injection	A vulnerability was found in Tubigan Welcome to our Resort 1.0. It has been classified as critical. This affects code of the file *index.php?p=accomodation*. The manipulation of the argument q with an unknown input lead to a sql injection vulnerability. CWE is classifying the issue as CWE-89. This is going to have an impact on confidentiality, integrity, and availability. An attacker might be able inject and/or alter existing SQL statements which would influence the database exchange.	Protected by Default Rules.
4.	Directory Traversal	CVE-2019-5438	Harp Module up to 0.29.0 on npm Symlink directory traversal	A vulnerability has been found in Harp Module up to 0.29.0 on npm and classified as critical. This vulnerability affects a functionality. The manipulation with an unknown input leads to a directory traversal vulnerability (Symlink). The CWE definition for the vulnerability is CWE-22. As an impact it is known to affect confidentiality, integrity, and availability. CVE summarizes:Path traversal using symlink in npm harp module versions <= 0.29.0.The weakness was published in 05/10/2019. This vulnerability was named as CVE-2019-5438 since 01/04/2019.	Protected by Default Rules.

CVE-2019-11831	Drupal core - Moderately critical - Third-party libraries - SA-CORE-2019-007	A vulnerability, which was classified as critical, has been found in PharStreamWrapper up to 2.1.0/3.1.0 on TYPO3. Affected by this issue is some functionality of the component Protection Mechanism. The manipulation with an unknown input lead to a directory traversal vulnerability (Deserialization). Using CWE to declare the problem leads to CWE-22. Impacted is confidentiality, integrity, and availability. The weakness was released 05/09/2019. This vulnerability is handled as CVE-2019-11831 since 05/08/2019. The attack may be launched remotely. No form of authentication is required for exploitation. There are neither technical details nor an exploit publicly available.	Protected by Default Rules.
CVE-2019-8952	Bosch DIVAR IP 2000/DIVAR IP 5000 prior 3.10 Webserver directory traversal	A vulnerability has been found in Bosch DIVAR IP 2000 and DIVAR IP 5000 and classified as critical. Affected by this vulnerability is a functionality of the component *Webserver*. The manipulation with an unknown input leads to a directory traversal vulnerability. The CWE definition for the vulnerability is CWE-22. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was released 05/13/2019. It is possible to read the advisory at media.boschsecurity.com.	Protected by Default Rules.

		CVE-2019-9726	eQ-3 Homematic CCU3 up to 3.43.15 Web Interface directory traversal	A vulnerability classified as critical has been found in eQ-3 Homematic CCU3 up to 3.43.15. Affected is an unknown function of the component *Web Interface*. The manipulation with an unknown input leads to a directory traversal vulnerability. CWE is classifying the issue as CWE-22. This is going to have an impact on confidentiality. The weakness was presented in 05/13/2019. This vulnerability is traded as CVE-2019-9726 since 03/12/2019. It is possible to launch the attack remotely. The exploitation doesn't require any form.	Protected by Default Rules.
5.	Cross Site Request Forgery	CVE-2019-11886	WaspThemes Visual CSS Style Editor Plugin up to 7.2.0 on WordPress cross site request forgery	A vulnerability was found in WaspThemes Visual CSS Style Editor Plugin up to 7.2.0 on WordPress (Plugin Software). It has been declared as problematic. Affected by this vulnerability is a code block. 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. An attacker might be able force legitimate users to initiate unwanted actions within the web application.	Protected by Custom Rules.
			Multiple bugs in several Jenkins plugins	Some of the plugins let users test the credential and connect to a server. These test functions can be protected by authorizing users based on user roles (require Overall/Administer permission) and enforcing POST requests, which will	Protected by Custom Rules.

				always require a CSRF token called Crumb. In these situations, the plugin developers did not enforce POST requests and the plugin becomes vulnerable to CSRF. An attacker could change the hostname in the CSRF payload and trick the administrator in initiating the test connection to a server, which is controlled by the attacker to then capture the credential.	
6.	Command Injection	CVE-2019-12099	php-fusion 9.03.00 Avatar Upload edit_profile.php Remote Code Execution	A vulnerability was found in php-fusion 9.03.00 (Content Management System). It has been classified as critical. Affected is code of the file *edit_profile.php* of the component *Avatar Upload Handler*. The manipulation with an unknown input leads to a privilege escalation vulnerability (Code Execution). CWE is classifying the issue as CWE-269. This is going to have an impact on confidentiality, integrity, and availability. The weakness was disclosed in 05/14/2019. This vulnerability is traded as CVE-2019-12099 since 05/14/2019.	Protected by Default Rules.
		CVE-2018-1335	Exploiting CVE-2018-1335: Command Injection in Apache Tika	This post is a walk-through of steps taken to go from an undisclosed CVE for a command injection vulnerability in the Apache tika-server to a complete exploit. The CVE is https://nvd.nist.gov/vuln/detail/CVE-2018-1335. Since Apache Tika is open source, I was able to take some basic information from the CVE and identify the actual issue by analysing the Apache Tika	Protected by Default Rules.

code. Although a command injection vulnerability is typically straightforward, as you will see in this post there were some hurdles to overcome to achieve full remote code or command execution. This was due to the way Java handles executing operating system commands and some intricacies of the Apache Tika code itself. In the end, it was still possible to get around these blockers using the Windows Script Host (Cscript.exe).