Weekly Zero-Day Vulnerability Coverage Bulletin

(21st May – 27th May)

Summary:

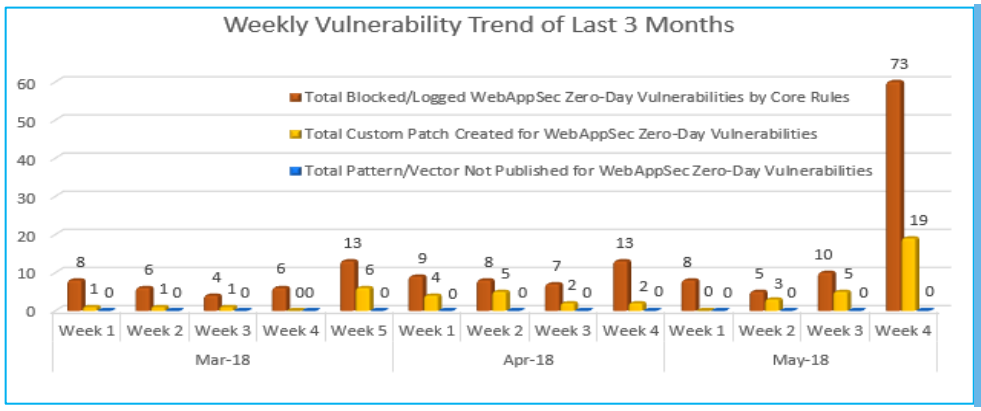
Total **92 Zero-Day Vulnerabilities** were discovered in **4 Categories** previous week

21	52	3	16
Cross Site Scripting	SQL Injection	Arbitrary File Upload	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	73
Zero-Day Vulnerabilities Protected through Custom Rules	19*
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

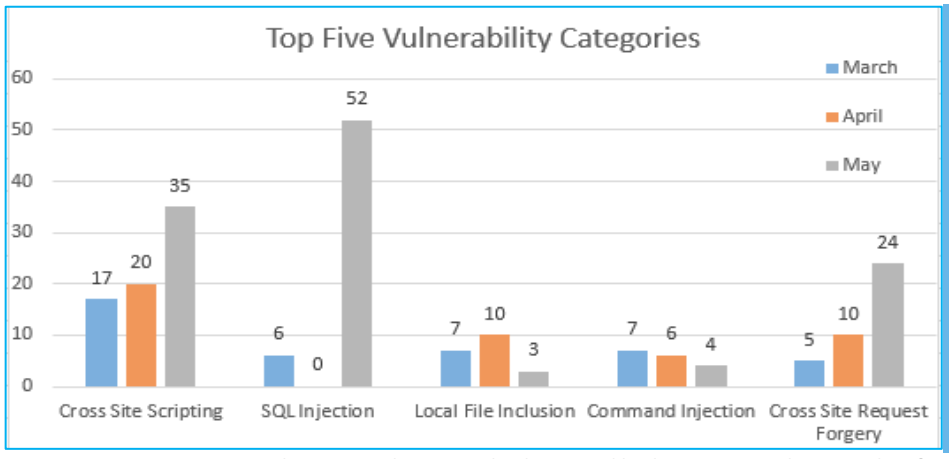
Vulnerability Trend:



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

79% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

21% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



From the graph, we infer that moderate no. of Cross Site Scripting Vulnerabilities are detected in all 3 months.

SQL Injection is 0 in April and multiple vulnerabilities were discovered in May.

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-2018-11245	MISP 2.4.91 APP/WEBROOT /JS/MISP.JS CROSS SITE SCRIPTING	Affected is an unknown function of the file app/webroot/js/mis p.js. The manipulation with an unknown input leads to a Cross-Site Scripting vulnerability (DOM-Based).	Protected by Default Rules.
		EDB-ID: 147710	Oracle Cross Site Scripting	eventreg.oracle.com suffers from a Cross-Site Scripting vulnerability.	Protected by Default Rules.
		CVE-2018-9163	ManageEngine Recovery Manager Plus 5.3 - Persistent Cross-Site Scripting	In the Add New Technician (s) section on the /admin/technicians page of the Manage Engine Recovery Manager Plus 5.3 (Build 5330) application, allows remote authenticated users with the Login Name parameter is vulnerable to Cross-Site Scripting. The parameters entered are written in the database and effect all users.	Protected by Default Rules.
		EDB-ID: 44683	Wchat PHP AJAX Chat Script 1.5 - Persistent Cross-Site Scripting	Wchat PHP AJAX Chat Script 1.5 - Persistent Cross-Site Scripting.	Protected by Default Rules.
		EDB-ID: 44661	Superfood 1.0 - Multiple Vulnerabilities	Superfood - Restaurants & Online Food Order System 1.0 suffers from multiple vulnerabilities	Protected by Default Rules.
		EDB-ID: 44662	Private Message PHP Script 2.0 - Persistent Cross-Site Scripting	Private Message PHP Script 2.0 suffers from persistent cross site scripting. You can put your malicious JavaScript payload. When target opens your massage, payload will be executed before self-destruction.	Protected by Default Rules.
		EDB-ID: 44663	Flippy DamnFacts - Viral Fun Facts Sharing Script 1.1.0 - Persistent Cross-Site Scripting / Cross-Site Request Forgery	Flippy DamnFacts - Viral Fun Facts Sharing Script 1.1.0 - Persistent Cross-Site Scripting / Cross site request forgery	Protected by Default Rules.
		EDB-ID: 44664	Zenar Content Management System - Cross-Site Scripting	Zenar Content Management System - Cross-Site Scripting	Protected by Default Rules.

EDB-ID: 44679	Auto Dealership & Vehicle Showroom WebSys 1.0 - Persistent Cross-Site Scripting / Cross-Site Request Forgery / Admin Panel Authentication Bypass	Auto Dealership & Vehicle Showroom WebSys 1.0 suffers from multiple vulnerabilities.	Protected by Default Rules.
EDB-ID: 44682	Model Agency Media House & Model Gallery 1.0 - Persistent Cross-Site Scripting / Cross-Site Request Forgery / Authentication bypass	Model Agency - Media House & Model Gallery 1.0 suffers from multiple vulnerabilities.	Protected by Default Rules.
EDB-ID: 147714	Auto Dealership and Vehicle Showroom WebSys 1.0 XSS / CSRF / SQL Injection	Auto Dealership and Vehicle Showroom WebSys 1.0 suffers from multiple vulnerabilities.	Protected by Default Rules.
EDB-ID: 13376	Model Agency Media House and Media Gallery 1.0 XSS / CSRF / SQL Injection	Media House & Model Gallery 1.0 suffers from multiple vulnerabilities.	Protected by Default Rules.
EDB-ID: 44686	WebSocket Live Chat - Cross-Site Scripting	WebSocket Live Chat - Cross-Site Scripting.	Protected by Default Rules.
CVE-2014-2908	Siemens SIMATIC S7-1200 CPU - Cross-Site Scripting	Siemens SIMATIC S7-1200 CPU - Cross-Site Scripting.	Protected by Default Rules.
EDB-ID: 44692	iSocial 1.2.0 - Cross-Site Scripting / Cross-Site Request Forgery	iSocial 1.2.0 - Cross-Site Scripting / Cross-Site Request Forgery.	Protected by Default Rules.
EDB-ID: 44699	Auto Car 1.2 - 'car_title' SQL Injection / Cross-Site Scripting	Auto car 1.2 - 'car_title' SQL Injection / Cross-Site Scripting.	Protected by Default Rules.
EDB-ID: 44703	Easy File Uploader 1.7 - SQL Injection / Cross-Site Scripting	Easy File Uploader 1.7 - SQL Injection / Cross-Site.	Protected by Default Rules.
EDB-ID: 44754	MyBB Moderator Log Notes Plugin 1.1	The plugin allows moderators to save notes and display them in a list in the modCP.	Protected by Default Rules.

			- Cross-Site Scripting	# The Cross-Site Scripting is in the mod notes text area.	
		CVE-2018-2791	Oracle WebCenter Sites 11.1.1.8.0/12.2.1.x - Cross-Site Scripting	The backend of the Content Server is prone to permanent and reflected Cross-Site Scripting attacks. The vulnerability can be used to include HTML- or JavaScript code to the affected web page. The code is executed in the browser of users if they visit the manipulated site. The vulnerability can be used to change the contents of the displayed site, redirect to other sites or steal user credentials. Additionally, Portal users are potential victims of browser exploits and JavaScript Trojans.	Protected by Default Rules.
		CVE-2018-11443	EasyService Billing 1.0 - Cross-Site Scripting	EasyService Billing 1.0 - Cross-Site Scripting.	Protected by Default Rules.
		CVE-2018-11027	Ruckus (Brocade) ICX7450-48 Reflected Cross Site Scripting	Ruckus (Brocade) ICX7450-48 web application has a reflected cross-site scripting vulnerability. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected site and allow the attacker to access sensitive browser-based information.	Protected by Default Rules.
2.	SQL Injection	EDB-ID: 44684	Nordex N149/4.0-4.5 - SQL Injection	Nordex N149/4.0-4.5 Wind Turbine Web Server - SQL Injection	Protected by Default Rules.
		EDB-ID: 44685	Zechat 1.5 - SQL Injection / Cross-Site Request Forgery	Zechat 1.5 - 'hashtag' / 'v' SQL Injection / Cross site request forgery	Protected by Default Rules.
		EDB-ID: 44689	PaulPrinting CMS Printing 1.0 - SQL Injection	Any visitor can run code to exploit css and SQL vulnerabilities in the products and order sections.	Protected by Default Rules.
		EDB-ID: 44700	NewsBee CMS 1.4 - 'home-text-edit.php' SQL Injection	NewsBee CMS 1.4 - 'home-text-edit.php' SQL Injection.	Protected by Default Rules.
		EDB-ID: 44701	Feedy RSS News Ticker 2.0 - 'cat' SQL Injection	Feedy RSS News Ticker 2.0 - 'cat' SQL Injection	Protected by Default Rules.

EDB-ID: 44702	NewsBee CMS 1.4 - 'download.php' SQL Injection	NewsBee CMS 1.4 - 'download .php' SQL Injection.	Protected by Default Rules.
EDB-ID: 44733	Mcard Mobile Card Selling Platform 1 - SQL Injection	Mcard Mobile Card Selling Platform 1 - SQL Injection.	Protected by Default Rules.
EDB-ID: 44730	Wecodex Restaurant CMS 1.0 - 'Login' SQL Injection	Wecodex Restaurant CMS 1.0 - 'Login' SQL Injection.	Protected by Default Rules.
EDB-ID: 44729	Wecodex Hotel CMS 1.0 - 'Admin Login' SQL Injection	Wecodex Hotel CMS 1.0 - 'Admin Login' SQL Injection.	Protected by Default Rules.
EDB-ID: 44728	Library CMS 1.0 - SQL Injection	Library CMS 1.0 - SQL Injection.	Protected by Default Rules.
EDB-ID: 44727	School Management System CMS 1.0 - 'username' SQL Injection	School Management System CMS 1.0 - Admin Login SQL.	Protected by Default Rules.
EDB-ID: 44726	SAT CFDI 3.3 - SQL Injection	SAT CFDI 3.3 - SQL Injection.	Protected by Default Rules.
EDB-ID: 44725	Wecodex Store Paypal 1.0 - SQL Injection	Wecodex Store Paypal 1.0 - SQL Injection.	Protected by Default Rules.
EDB-ID: 44722	Shipping System CMS 1.0 - SQL Injection	Shipping System CMS 1.0 - SQL Injection.	Protected by Default Rules.
EDB-ID: 44720	GPSTracker 1.0 - 'id' SQL Injection	GPSTracker 1.0 - 'id' SQL Injection.	Protected by Default Rules.
EDB-ID: 44719	Online Store System CMS 1.0 - SQL Injection	Online Store System CMS 1.0 - SQL Injection.	Protected by Default Rules.
EDB-ID: 44718	Gigs 2.0 - 'username' SQL Injection	Gigs 2.0 - 'username' SQL Injection.	Protected by Default Rules.
EDB-ID: 147827	PHP Dashboards 4.5 - SQL Injection	PHP Dashboards 4.5 - SQL Injection.	Protected by Default Rules.
EDB-ID: 44714	PHP Dashboards 4.5 - 'email' SQL Injection	PHP Dashboards 4.5 - 'email' SQL Injection.	Protected by Default Rules.
EDB-ID: 44712	MySQL Blob Uploader 1.7 - 'home-filet-edit.php' SQL Injection	MySQL Blob Uploader 1.7 - 'home-filet-edit.php' SQL Injection.	Protected by Default Rules.
EDB-ID:44709	MySQL Blob Uploader 1.7 - 'home-filet-edit.php' SQL Injection /	MySQL Blob Uploader 1.7 - 'home-filet-edit.php' SQL Injection / Cross-Site Scripting.	Protected by Default Rules.

	Cross-Site Scripting		
EDB-ID: 44709	MySQL Blob Uploader 1.7 - 'download.php' SQL Injection / Cross-Site Scripting	MySQL Blob Uploader 1.7 - 'download.php' SQL Injection / Cross-Site Scripting	Protected by Default Rules.
EDB-ID: 44708	MySQL Smart Reports 1.0 - 'id' SQL Injection / Cross-Site Scripting	MySQL Smart Reports 1.0 - 'id' SQL Injection / Cross-Site Scripting	Protected by Default Rules.
EDB-ID: 44707	EasyService Billing 1.0 - 'p1' SQL Injection	EasyService Billing 1.0 - 'p1' SQL Injection	Protected by Default Rules.
EDB-ID: 44706	EasyService Billing 1.0 - SQL Injection / Cross-Site Scripting	EasyService Billing 1.0 - SQL Injection / Cross-Site Scripting	Protected by Default Rules.
EDB-ID: 147829	Gigs 2.0 SQL Injection	Gigs version 2.0 suffers from a remote SQL injection vulnerability.	Protected by Default Rules.
EDB-ID: 147830	Online Store System CMS 1.0 SQL Injection	Online Store System CMS version 1.0 suffers from a remote SQL injection vulnerability.	Protected by Default Rules.
EDB-ID: 147831	GPSTracker 1.0 SQL Injection	PHP Dashboards is prone to an SQL-injection vulnerability because it fails to sufficiently sanitize user-supplied data before using it in an SQL query.Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.	Protected by Default Rules.
EDB-ID: 147832	Shipping System CMS 1.0 SQL Injection	HP Dashboards is prone to an SQL-injection vulnerability # because it fails to sufficiently sanitize user-supplied data before using # it in an SQL query.Exploiting this issue could allow an attacker to # compromise the application, access or modify data, or exploit latent # vulnerabilities in the underlying database.	Protected by Default Rules.

EDB-ID: 147833	Wecodex Store Paypal 1.0 SQL Injection	PHP Dashboards is prone to an SQL-injection vulnerability # because it fails to sufficiently sanitize user-supplied data before using # it in an SQL query.Exploiting this issue could allow an attacker to # compromise the application, access or modify data, or exploit latent # vulnerabilities in the underlying database.	Protected by Default Rules.
EDB-ID: 147834	SAT CFDI 3.3 SQL Injection	PHP Dashboards is prone to an SQL-injection vulnerability # because it fails to sufficiently sanitize user-supplied data before using # it in an SQL query.Exploiting this issue could allow an attacker to # compromise the application, access or modify data, or exploit latent # vulnerabilities in the underlying database.	Protected by Default Rules.
EDB-ID: 147835	School Management System CMS 1.0 SQL Injection	PHP Dashboards is prone to an SQL-injection vulnerability # because it fails to sufficiently sanitize user-supplied data before using # it in an SQL query. Exploiting this issue could allow an attacker to # compromise the application, access or modify data, or exploit latent # vulnerabilities in the underlying database.	Protected by Default Rules.
EDB-ID: 147836	Library CMS 1.0 SQL Injection	PHP Dashboards is prone to an SQL-injection vulnerability # because it fails to sufficiently sanitize user-supplied data before using # it in an SQL query. Exploiting this issue could allow an attacker to # compromise the application, access or modify data, or exploit latent # vulnerabilities in the underlying database.	Protected by Default Rules.
EDB-ID: 147845	Wecodex Hotel CMS 1.0 SQL Injection	Wecodex Hotel CMS version 1.0 suffers from a remote SQL injection vulnerability.	Protected by Default Rules.
EDB-ID: 147846	Wecodex Restaurant CMS 1.0 SQL Injection	Wecodex Restaurant CMS version 1.0 suffers from a remote SQL Injection vulnerability.	Protected by Default Rules.

EDB-ID: 147848	Mcard Mobile Card Selling Platform 1 SQL Injection	Mcard Mobile Card Selling Platform version 1 suffers from a remote SQL injection vulnerability.	Protected by Default Rules.
EDB-ID: 147855	ASP.NET jVideo Kit 1.0 SQL Injection	ASP.NET jVideo Kit version 1.0 suffers from a remote SQL injection vulnerability.	Protected by Default Rules.
EDB-ID: 147856	OpenDaylight SQL Injection	OpenDaylight suffers from a remote SQL injection vulnerability.	Protected by Default Rules.
CVE-2014-3110	Honeywell XL Web Controller Cross Site Scripting / SQL Injection	Honeywell XL Web Controller suffers from cross site scripting and remote SQL injection vulnerabilities.	Protected by Default Rules.
EDB-ID: 147867	EU MRV Regulatory Complete Solution 1 SQL Injection	EU MRV Regulatory Complete Solution version 1 suffers from a remote SQL injection vulnerability.	Protected by Default Rules.
EDB-ID: 147875	PaulNews 1.0 Cross Site Scripting / SQL Injection	PaulNews version 1.0 suffers from cross site scripting and remote SQL injection vulnerabilities.	Protected by Default Rules.
EDB-ID: 44753	KomSeo Cart 1.3 - 'my_item_search' SQL Injection	The vulnerability allows an attacker to inject sql commands from the user search section with 'my_item_search' parameter.	Protected by Default Rules.
EDB-ID: 44767	easyLetters 1.0 - 'id' SQL Injection	easyLetters 1.0 - 'id' SQL Injection	Protected by Default Rules.
EDB-ID: 44766	mySurvey 1.0 - 'id' SQL Injection	You can see the notifications on the left side when you receive new answers. This url works in 'statistic.php' with 'id' parameter. This 'id' parameter is vulnerable.	Protected by Default Rules.
CVE-2018-11444	EasyService Billing 1.0 - 'q' SQL Injection	EasyService Billing 1.0 - 'q' SQL Injection	Protected by Default Rules.
EDB-ID: 44762	Ajax Full Featured Calendar 2.0 - 'search' SQL Injection	The vulnerability allows an attacker to inject SQL commands from the search section with 'search' parameter.	Protected by Default Rules.
EDB-ID: 44761	Employee Work Schedule 5.9 - 'cal_id' SQL Injection	The vulnerability allows an attacker to inject SQL commands from the search section with 'cal_id' parameter.	Protected by Default Rules.
EDB-ID: 44772	Lyrist - 'id' SQL Injection	Lyrist - Music Lyrics Script - SQL Injection.	Protected by Default Rules.

		EDB-ID: 44773	BookingWizz Booking System 5.5 - 'id' SQL Injection	The service editing on the admin panel is vulnerable. An attacker can exploit the entire database using this vulnerable in the 'id' parameter.	Protected by Default Rules.
		EDB-ID: 44774	Listing Hub CMS 1.0 - SQL Injection	An attacker can use the 'SQLi' attack method on many places.	Protected by Default Rules.
		EDB-ID: 44777	My Directory 2.0 - SQL Injection / Cross-Site Scripting	The vulnerability allows an attacker to inject SQL commands from the user search section with 'business' parameter. Another parameter 'city', has Cross-Site Scripting vulnerability.	Protected by Default Rules.
		EDB-ID: 44778		The vulnerability allows an attacker to inject SQL commands from search section with 'a' parameter.	Protected by Default Rules.
3.	Arbitrary File Upload	EDB-ID: 44737	WordPress Plugin Peugeot Music - Arbitrary File Upload	Wordpress Plugin Peugeot Music - Arbitrary File Upload	Protected by Custom Rules.
		EDB-ID: 147854	WordPress Peugeot Music 1.0 Shell Upload / Cross Site Request Forgery	WordPress Peugeot Music plugin version 1.0 suffers from cross site request forgery and remote shell upload vulnerabilities.	Protected by Custom Rules.
		EDB-ID: 147858	Easy File Uploader 1.7 Shell Upload	Easy File Uploader version 1.7 suffers from a remote shell upload vulnerability.	Protected by Custom Rules.
4.	Cross Site Request Forgery	CVE-2013-0663	Schneider Electric PLCs - Cross-Site Request Forgery	Schneider Electric PLCs - Cross-Site Request Forgery	Protected by Custom Rules.
		CVE-2015- 5698	Siemens SIMATIC S7-1200 CPU - Cross-Site Request Forgery	Siemens SIMATIC S7-1200 CPU - Cross-Site Request Forgery	Protected by Custom Rules.
		EDB-ID: 44681	Merge PACS 7.0 - Cross-Site Request Forgery	Merge PACS 7.0 - Cross-Site Request Forgery	Protected by Custom Rules.
		EDB-ID: 44675	Teradek Cube 7.3.6 - Cross-Site Request Forgery	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges	Protected by Custom Rules.

		if a logged-in user visits a malicious web site.	
EDB-ID: 44676	Teradek Slice 7.3.15 - Cross-Site Request Forgery	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site.	Protected by Custom Rules.
EDB-ID: 147724	Teradek VidiU Pro 3.0.3 Change Password Cross Site Request Forgery	Teradek VidiU Pro version 3.0.3 change password cross site request forgery exploit.	Protected by Custom Rules.
EDB-ID: 44735	NewsBee CMS 1.4 - Cross-Site Request Forgery	NewsBee CMS 1.4 - Cross-Site Request Forgery.	Protected by Custom Rules.
EDB-ID: 44732	eWallet Online Payment Gateway 2 - Cross-Site Request Forgery	eWallet - Online Payment Gateway 2 - Cross-Site Request Forgery.	Protected by Custom Rules.
EDB-ID: 44716	Mobile Card Selling Platform 1 - Cross-Site Request Forgery	Mobile Card Selling Platform 1 - Cross-Site Request Forgery.	Protected by Custom Rules.
CVE-2018-11405	Kliqqi 2.0.2 admin/admin_users.php cross site request forgery	A vulnerability classified as problematic was found in Kliqqi 2.0.2. Affected by this vulnerability is an unknown function of the file *admin/admin_users.php*. 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. The weakness was presented 05/24/2018. This vulnerability is known as CVE-2018-11405.	Protected by Custom Rules.
EDB-ID: 147828	Mcard Mobile Card Selling Platform 1 Cross Site	Mcard Mobile Card Selling Platform version 1 suffers from a cross	Protected by Custom Rules.

	Request Forgery	site request forgery vulnerability.	
EDB-ID: 147859	Timber 1.1 Cross Site Request Forgery	Timber version 1.1 suffers from a cross site request forgery vulnerability.	Protected by Custom Rules.
EDB-ID: 147869	NewsBee CMS 1.4 Cross Site Request Forgery	NewsBee CMS version 1.4 suffers from a cross site request forgery vulnerability.	Protected by Custom Rules.
EDB-ID:147874	LikeSoftware CMS Cross Site Request Forgery / Shell Upload	LikeSoftware CMS suffers from cross site request forgery and remote shell upload vulnerabilities.	Protected by Custom Rules.
EDB-ID: 44763	EasyService Billing 1.0 - Cross-Site Request Forgery	EasyService Billing 1.0 - Cross-Site Request Forgery	Protected by Custom Rules.
EDB-ID: 147915	Sharetronix CMS 3.6.2 Cross Site Request Forgery	Sharetronix CMS 3.6.2 Cross Site Request Forgery	Protected by Custom Rules.