Monthly Zero-Day Vulnerability Coverage Bulletin

April 2022

Total Zero-Day Vulnerabilities Found: 109

Command Injection	CSRF	Local File Inclusion	Cross - Site Scripting	SQL Injection
7	17	17	36	32

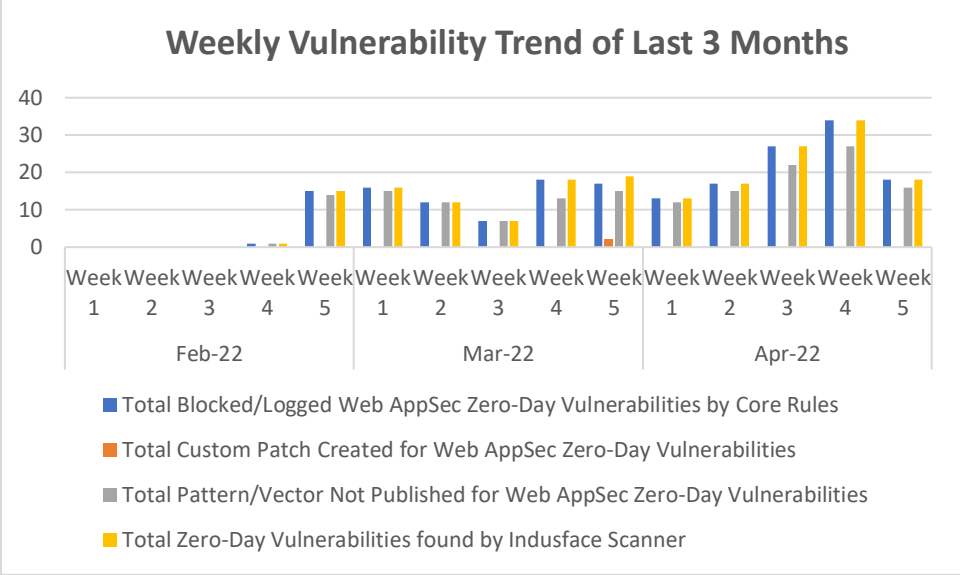
Zero-Day vulnerabilities protected through core rules	109
Zero-Day vulnerabilities protected through custom rules	0 *
Zero-Day vulnerabilities for which protection cannot be determined	0 **
Zero-Day vulnerabilities found by Indusface WAS	92

* To enable custom rules, please contact support@indusface.com

** Since the attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.

Vulnerability Trend:

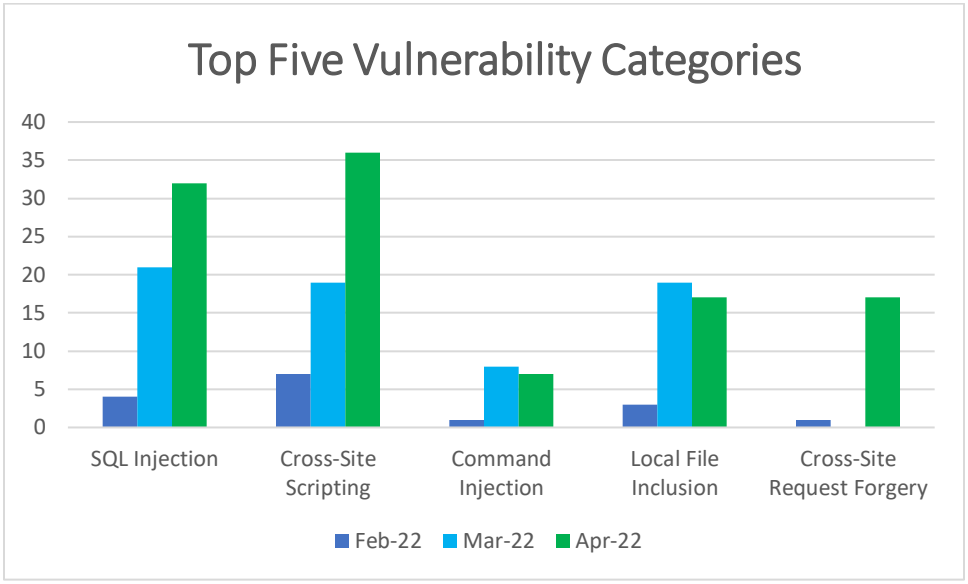
The weekly trend displays the total number of vulnerabilities discovered to the type of protection provided for the last quarter.



100% of the zero-day vulnerabilities were protected by the **core rules** in the last quarter

NA of the zero-day vulnerabilities were protected by the **custom rules** in the last quarter

84% of the zero-day vulnerabilities were reported by **Indusface Scanner** in the 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 round-the-clock protection for customer sites.

Vulnerability Details:

S.no	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
1	Command Injection	CVE-2022-0999	mySCADA myPRO prior 8.26 command injection (icsa-22-083-02)	A vulnerability classified as critical has been found in mySCADA myPRO. This affects an unknown part. The manipulation leads to privilege escalation. This vulnerability is uniquely identified as CVE-2022-0999. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the Command Injection attack.
		CVE-2022-25017	Hitron CHITA 7.2.2.0.3b6-CD ddnsUsername command injection	A vulnerability was found in Hitron CHITA 7.2.2.0.3b6-CD. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation of the argument ddnsUsername leads to privilege escalation. This vulnerability is known as CVE-2022-25017. The attack can be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Command Injection attack.
		CVE-2022-24066	simple-git up to 3.4.x Incomplete	A vulnerability has been found in simple-git up to 3.4.x and classified as critical.	Protected by core rules.	Detected by the scanner as

		Fix CVE-2022-24433 command injection	This vulnerability affects unknown code of the component Incomplete Fix CVE-2022-24433. The manipulation leads to privilege escalation. This vulnerability was named CVE-2022-24066. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		the Command Injection attack.
	CVE-2021-32933	MDT Autosave prior 6.02.06 API command injection (icsa-21-189-02)	A vulnerability, which was classified as very critical, was found in MDT Autosave. This affects an unknown part of the component API. The manipulation leads to privilege escalation. This vulnerability is uniquely identified as CVE-2021-32933. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the Command Injection attack.
	CVE-2022-24279	madlib-object-utils up to 0.1.7 Incomplete Fix CVE-2020-7701 setValue code injection	A vulnerability, which was classified as critical, has been found in madlib-object-utils up to 0.1.7. This issue affects the function setValue of the component Incomplete Fix CVE-2020-7701. The manipulation leads to privilege escalation. The identification of this vulnerability is CVE-2022-24279. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the Command Injection attack.
	CVE-2022-27427	Chamilo LMS 1.11.13 Plugin configuration.php code injection	A vulnerability was found in Chamilo LMS 1.11.13. It has been rated as critical. Affected by this issue is some unknown functionality of the file configuration.php of the component Plugin Handler. The manipulation leads to privilege escalation. This vulnerability is handled as CVE-2022-27427. The attack may be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Command Injection attack.
	NA	Telesquare SDT-CW3B1 1.1.0 os command injection	A vulnerability classified as critical was found in Telesquare SDT-CW3B1 1.1.0. This vulnerability affects unknown code. The manipulation leads to privilege escalation. This vulnerability was named CVE-2021-46422. The attack can be initiated remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Command Injection attack.

2	Cross- Site Request Forgery	CVE-2022-0088	yourls up to 1.8.2 cross-site request forgery	A vulnerability classified as problematic was found in yourls up to 1.8.2. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-0088. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	NA
		CVE-2022-26588	IceHrm 31.0.0.OS app/service.php cross-site request forgery (ID 166627)	A vulnerability, which was classified as problematic, has been found in IceHrm 31.0.0.OS. This issue affects some unknown processing of the file app/service.php. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022-26588. The attack may be initiated remotely. There is no exploit available.	Protected by core rules.	NA
		CVE-2022-26180	qdPM 9.2 update cross-site request forgery (ID 166630)	A vulnerability was found in qdPM 9.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file index.php/myAccount/update. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-26180. The attack can be launched remotely. There is no exploit available.	Protected by core rules.	NA
		CVE-2021-32156	Webmin 1.973 Scheduled Cron Job cross-site request forgery	A vulnerability classified as problematic was found in Webmin 1.973. Affected by this vulnerability is an unknown functionality of the component Scheduled Cron Job Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2021-32156. The attack can be launched remotely. There is no exploit available.	Protected by core rules.	NA
		CVE-2021-32162	Webmin up to 1.973 File Manager cross-site request forgery	A vulnerability was found in Webmin up to 1.973. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component File Manager. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2021-32162. The attack can be launched remotely. There is no exploit available.	Protected by core rules.	NA

	CVE-2021-32159	Webmin 1.973 Upload/Download cross-site request forgery	A vulnerability has been found in Webmin 1.973 and classified as problematic. This vulnerability affects unknown code of the component Upload/Download. The manipulation leads to cross- site request forgery. This vulnerability was named CVE-2021-32159. The attack can be initiated remotely. There is no exploit available.	Protected by core rules.	NA
	CVE-2021-34250	baijiacms v4 cross-site request forgery	A vulnerability was found in baijiacms v4 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2021-34250. The attack may be initiated remotely. There is no exploit available.	Protected by core rules.	NA
	CVE-2022-27850	Simple Ajax Chat Plugin up to 20220115 on WordPress Chat Message cross-site request forgery	A vulnerability was found in Simple Ajax Chat Plugin up to 20220115 and classified as problematic. Affected by this issue is some unknown functionality of the component Chat Message Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-27850. The attack may be launched remotely. There is no exploit available.	Protected by core rules.	NA
	CVE-2022-23976	Access Demo Importer Plugin up to 1.0.7 on WordPress cross-site request forgery	A vulnerability was found in Access Demo Importer Plugin up to 1.0.7. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-23976. The attack can be launched remotely. There is no exploit available.	Protected by core rules.	NA
	CVE-2022-23975	Access Demo Importer Plugin up to 1.0.7 on WordPress cross-site request forgery	A vulnerability was found in Access Demo Importer Plugin up to 1.0.7. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Plugin Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-23975. The attack may be launched remotely. There is no exploit available.	Protected by core rules.	NA
	CVE-2022-0707	Easy Digital Downloads Plugin up to 2.11.5 on WordPress cross-site request	A vulnerability, which was classified as problematic, has been found in Easy Digital Downloads Plugin up to 2.11.5. This issue affects some unknown processing. The manipulation leads to cross- site request forgery.	Protected by core rules.	NA

		forgery (ID 2697388)	The identification of this vulnerability is CVE-2022-0707. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
	CVE-2022-1112	Autolinks Plugin up to 1.0.1 on WordPress cross-site request forgery	A vulnerability, which was classified as problematic, was found in Autolinks Plugin up to 1.0.1. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-1112. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules.	NA
	CVE-2022-28108	Selenium Server up to 3.x Non-JSON Content Type cross-site request forgery	A vulnerability was found in Selenium Server up to 3.x. It has been declared as problematic. This vulnerability affects unknown code of the component Non-JSON Content Type Handler. The manipulation leads to cross- site request forgery. This vulnerability was named CVE-2022-28108. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	NA
	CVE-2022-27629	MicroPayments Plugin up to 1.9.5 on WordPress cross-site request forgery	A vulnerability was found in MicroPayments Plugin up to 1.9.5. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross- site request forgery. This vulnerability is traded as CVE-2022-27629. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	NA
	NA	CVE-2022-27340 | MCMS 5.2.7 saveOrUpdateRole.do cross-site request forgery	A vulnerability, which was classified as problematic, has been found in MCMS 5.2.7. Affected by this issue is some unknown functionality of the file /role/saveOrUpdateRole.do. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-27340. The attack may be launched remotely. There is no exploit available.	Protected by core rules.	NA

		CVE-2022-29412	Hermit Plugin up to 3.1.6 on WordPress cross-site request forgery	A vulnerability was found in Hermit Plugin up to 3.1.6. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-29412. The attack can be initiated remotely. There is no exploit available.	Protected by core rules.	NA
		CVE-2022-29905	FanBoxes Extension up to 1.37.2 on MediaWiki cross-site request forgery	A vulnerability, which was classified as problematic, was found in FanBoxes Extension up to 1.37.2. Affected is an unknown function. The manipulation leads to cross- site request forgery. This vulnerability is traded as CVE-2022-29905. It is possible to launch the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules.	NA
3	Local File Inclusion	CVE-2021-32949	MDT AutoSave prior 6.02.06 path traversal (icsa-21-189-02)	A vulnerability classified as critical was found in MDT AutoSave. Affected by this vulnerability is an unknown functionality. The manipulation leads to directory traversal. This vulnerability is known as CVE-2021-32949. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
		CVE-2022-26233	Barco Control Room Management up to 2.9 Build 0275 pathname traversal	A vulnerability was found in Barco Control Room Management up to 2.9 Build 0275. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to directory traversal. The identification of this vulnerability is CVE-2022-26233. The attack can only be done within the local network. There is no exploit available.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
		CVE-2022-23732	GitHub Enterprise Server up to 3.1.18/3.2.10/3.3.5/3.4.0 Management Console path traversal	A vulnerability was found in GitHub Enterprise Server up to 3.1.18/3.2.10/3.3.5/3.4.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Management Console. The manipulation leads to directory traversal. This vulnerability is known as CVE-2022-23732. The attack can be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.

		It is recommended to upgrade the affected component.		
CVE-2021-36288	Dell VNX2 up to 8.1.21.266 path traversal (dsa-2021-164)	A vulnerability was found in Dell VNX2 up to 8.1.21.266. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to directory traversal. The identification of this vulnerability is CVE-2021-36288. The attack may be initiated remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
CVE-2022-27043	Yearning 2.3.1/2.3.2/2.3.4/ 2.3.5/2.3.6 pathname traversal	A vulnerability, which was classified as critical, was found in Yearning 2.3.1/2.3.2/2.3.4/2.3.5/2.3.6. This affects an unknown part. The manipulation leads to directory traversal. This vulnerability is uniquely identified as CVE-2022-27043. The attack needs to be initiated within the local network. Furthermore, there is an exploit available.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
CVE-2022-1119	Simple File List Plugin up to 3.2.7 on WordPress ee-downloader.php eeFile path traversal	A vulnerability was found in Simple File List Plugin up to 3.2.7. It has been declared as critical. This vulnerability affects unknown code of the file ~/includes/ee-downloader.php. The manipulation of the argument eeFile leads to directory traversal. This vulnerability was named CVE-2022-1119. The attack can be initiated remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
CVE-2022-27925	Synacor Zimbra Collaboration 8.8.15/9.0 mboximport pathname traversal	A vulnerability, which was classified as critical, has been found in Synacor Zimbra Collaboration 8.8.15/9.0. This issue affects some unknown processing of the component mboximport Handler. The manipulation leads to directory traversal. The identification of this vulnerability is CVE-2022-27925. The attack may be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
CVE-2022-24424	Dell EMC AppSync up to 4.3 Server path traversal	A vulnerability, which was classified as critical, was found in Dell EMC AppSync up to 4.3. Affected is an unknown function of the component Server. The manipulation leads to directory traversal. This vulnerability is traded as CVE-2022-	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.

			24424. It is possible to launch the attack remotely. There is no exploit available.		
	CVE-2022-20790	Cisco Unified Communications Manager Web-based Management Interface path traversal (cisco-sa-ucm-file-read-h8h4HEJ3)	A vulnerability was found in Cisco Unified Communications Manager and Unified Communications Manager Session Management Edition. It has been declared as problematic. This vulnerability affects unknown code of the component Web-based Management Interface. The manipulation leads to directory traversal. This vulnerability was named CVE-2022-20790. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
	CVE-2021-40680	Artica Proxy up to 4.30.000000 SP255 /cgi-bin/main.cgi filename pathname traversal	A vulnerability, which was classified as critical, was found in Artica Proxy up to 4.30.000000 SP255. Affected is an unknown function of the file /cgi-bin/main.cgi. The manipulation of the argument filename leads to directory traversal. This vulnerability is traded as CVE-2021-40680. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
	CVE-2022-1390	Admin Word Count Column Plugin up to 2.2 on WordPress Phar Deserialization readfile path path traversal (ID 166476)	A vulnerability was found in Admin Word Count Column Plugin up to 2.2. It has been rated as critical. This issue affects the function readfile of the component Phar Deserialization. The manipulation of the argument path leads to directory traversal. The identification of this vulnerability is CVE-2022-1390. The attack may be initiated remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
	CVE-2022-23457	ESAPI up to 2.2.x Validator.getValidDirectoryPath path traversal (GHSA-8m5h-hrqm-pxm2)	A vulnerability was found in ESAPI up to 2.2.x. It has been rated as critical. Affected by this issue is the function Validator.getValidDirectoryPath. The manipulation leads to directory traversal. This vulnerability is handled as CVE-2022-23457. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
	CVE-2022-1392	Videos Sync PDF Plugin up to 1.7.4 on WordPress	A vulnerability was found in Videos Sync PDF Plugin up to 1.7.4. It has been rated as critical. This issue affects some unknown processing. The manipulation	Protected by core rules.	Detected by the scanner as Local File

			path traversal (ID 166534)	of the argument p leads to directory traversal. The identification of this vulnerability is CVE-2022-1392. The attack needs to be initiated within the local network. There is no exploit available.		Inclusion attack.
		NA	Franklin Fueling Systems TS-550 EVO 2.23.4.8936 pathname traversal	A vulnerability was found in Franklin Fueling Systems TS-550 EVO 2.23.4.8936 and classified as critical. This issue affects some unknown processing. The manipulation leads to directory traversal. The identification of this vulnerability is CVE-2021-46420. The attack can only be done within the local network. There is no exploit available.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
		CVE-2021-26629	Tobesoft XPlatform File Creation path traversal	A vulnerability was found in Tobesoft XPlatform and classified as critical. Affected by this issue is some unknown functionality of the component File Creation Handler. The manipulation leads to directory traversal. This vulnerability is handled as CVE-2021-26629. The attack may be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
		NA	Franklin Fueling Systems FFS T5 1.8.7.7299 pathname traversal	A vulnerability was found in Franklin Fueling Systems FFS T5 1.8.7.7299. It has been classified as critical. Affected is an unknown function. The manipulation leads to directory traversal. This vulnerability is traded as CVE-2021-46421. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
		CVE-2021-43930	Elcomplus SmartPTT up to 2.3.3 Download Request path traversal (icsa-22-109-04)	A vulnerability was found in Elcomplus SmartPTT up to 2.3.3 and classified as problematic. Affected by this issue is some unknown functionality of the component Download Request Handler. The manipulation leads to directory traversal. This vulnerability is handled as CVE-2021-43930. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
4	SQL Injection	CVE-2021-44135	Pagekit Comment Listing injection	A vulnerability was found in Pagekit. It has been rated as critical. This issue affects some unknown processing of the component Comment Listing Handler. The manipulation leads to SQL injection.	Protected by core rules.	Detected by the scanner as the SQL

			The identification of this vulnerability is CVE-2021-44135. The attack may be initiated remotely. There is no exploit available.		Injection attack.
	CVE-2021-36625	Dolibarr ERP/CRM 13.0.2 UPDATE Statement country_id SQL injection	A vulnerability was found in Dolibarr ERP and CRM 13.0.2. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component UPDATE Statement Handler. The manipulation of the argument country_id leads to SQL sinjection. This vulnerability is known as CVE-2021-36625. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	CVE-2021-32953	MDT Autosave prior 6.02.06 SQLinjection (icsa-21-189-02)	A vulnerability was found in MDT Autosave. It has been classified as critical. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is traded as CVE-2021-32953. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	CVE-2021-32957	MDT Autosave prior 6.02.06 SQL injection (icsa-21-189-02)	A vulnerability was found in MDT Autosave. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to SQL injection. This vulnerability is known as CVE-2021-32957. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	CVE-2022-26986	ImpressCMS up to 1.4.3 SQL injection	A vulnerability has been found in ImpressCMS up to 1.4.3 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-26986. The attack can be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	CVE-2022-26585	mingsoft MCMS 5.2.7 /cms/content/list SQL injection	A vulnerability was found in mingsoft MCMS 5.2.7. It has been rated as critical. Affected by this issue is some unknown functionality of the file /cms/content/list. The manipulation leads to SQL injection.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.

			This vulnerability is handled as CVE-2022-26585. The attack may be launched remotely. There is no exploit available.		
	CVE-2022-24231	Student Information System 1.0 Add Student SQL injection	A vulnerability was found in Student Information System 1.0. It has been classified as critical. Affected is an unknown function of the component Add Student Handler. The manipulation leads to SQL Injection. This vulnerability is traded as CVE-2022-24231. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	CVE-2021-46436	zzcms 2021 ad_manage.php SQL injection	A vulnerability classified as critical was found in zzcms 2021. Affected by this vulnerability is an unknown functionality of the file ad_manage.php. The manipulation leads to SQL injection. This vulnerability is known as CVE-2021-46436. The attack can be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	CVE-2022-27126	zbzcms 1.0 /include/make.php art SQL injection	A vulnerability classified as critical was found in zbzcms 1.0. Affected by this vulnerability is an unknown functionality of the file /include/make.php. The manipulation of the argument art leads to SQL injection. This vulnerability is known as CVE-2022-27126. The attack can be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	CVE-2022-27127	zbzcms 1.0 /php/ajax.php id sql injection	A vulnerability, which was classified as critical, has been found in zbzcms 1.0. Affected by this issue is some unknown functionality of the file /php/ajax.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-27127. The attack may be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	CVE-2022-1023	Podcast Importer SecondLine Plugin up to 1.3.7 on WordPress Import sql injection (ID 2696254)	A vulnerability was found in Podcast Importer SecondLine Plugin up to 1.3.7. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Import Handler. The manipulation leads to SQL injection. This vulnerability is known as CVE-2022-1023. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.

	CVE-2022-27041	OS4Ed openSIS Classic 8.0 Student.php student_id SQL injection (ID 248)	A vulnerability classified as critical has been found in OS4Ed openSIS Classic 8.0. Affected is an unknown function of the file /modules/eligibility/Student.php. The manipulation of the argument student_id leads to SQL injection. This vulnerability is traded as CVE-2022-27041. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	CVE-2022-27367	CSCMS 4.2 dance_Topic.php_del SQL injection (ID 14)	A vulnerability was found in CSCMS 4.2. It has been rated as critical. Affected by this issue is some unknown functionality of the file dance_Topic.php_del. The manipulation leads to SQL injection. This vulnerability is handled as CVE-2022-27367. The attack may be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	CVE-2022-27366	CSCMS 4.2 dance_Dance.php_hy sql injection (ID 13)	A vulnerability was found in CSCMS 4.2. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file dance_Dance.php_hy. The manipulation leads to SQL injection. This vulnerability is known as CVE-2022-27366. The attack can be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	CVE-2022-27423	Chamilo LMS 1.11.13 /blog/blog.php blog_id SQL injection	A vulnerability was found in Chamilo LMS 1.11.13. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /blog/blog.php. The manipulation of the argument blog_id leads to SQL injection. This vulnerability is known as CVE-2022-27423. The attack can be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	NA	phpGACL 3.3.7 HTTP Request SQL injection (TALOS-2020-1179)	A vulnerability was found in phpGACL 3.3.7. It has been classified as critical. Affected is an unknown function of the component HTTP Request Handler. The manipulation leads to SQL injection. This vulnerability is traded as CVE-2020-13567. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	NA	Zoho ManageEngine ManageEngine OpManager 125602/up to 125587 Inventory Reports Module SQL injection	A vulnerability classified as critical was found in Zoho ManageEngine ManageEngine OpManager up to 125587/125602. Affected by this vulnerability is an unknown functionality of the component Inventory Reports Module. The manipulation leads to SQL injection.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.

			This vulnerability is known as CVE-2022-27908. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
	CVE-2022-0785	Daily Prayer Time Plugin prior 2022.03.01 on WordPress SQL Statement get_monthly_timetable month SQL injection	A vulnerability was found in Daily Prayer Time Plugin. It has been classified as critical. Affected is the function get_monthly_timetable of the component SQL Statement Handler. The manipulation of the argument month leads to sql injection. This vulnerability is traded as CVE-2022-0785. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	CVE-2020-13590	Rukovoditel Project Management App up to 2.7.2 HTTP Request entities/fields SQL injection (TALOS-2020-1199)	A vulnerability classified as critical was found in Rukovoditel Project Management App up to 2.7.2. Affected by this vulnerability is an unknown functionality of the file entities/fields of the component HTTP Request Handler. The manipulation leads to SQL injection. This vulnerability is known as CVE-2020-13590. The attack can be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	CVE-2022-27104	Forma LMS up to 1.4.2 SQL injection	A vulnerability was found in Forma LMS up to 1.4.2. It has been classified as critical. This affects an unknown part. The manipulation leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-27104. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	CVE-2022-29498	Blazer up to 2.5.x Query SQL injection (ID 392)	A vulnerability, which was classified as critical, has been found in Blazer up to 2.5.x. Affected by this issue is some unknown functionality of the component Query Handler. The manipulation leads to SQL injection. This vulnerability is handled as CVE-2022-29498. The attack may be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.

			It is recommended to upgrade the affected component.		
	NA	SourceCodester Attendance and Payroll System 1.0 attendance_delete.php SQL injection	A vulnerability, which was classified as critical, has been found in SourceCodester Attendance and Payroll System 1.0. This issue affects some unknown processing of the file \admin\attendance_delete.php. The manipulation leads to SQL injection. The identification of this vulnerability is CVE-2022-28008. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	NA	NetWave System 1.0 Master.php SQL injection	A vulnerability was found in NetWave System 1.0. It has been classified as critical. This affects an unknown part of the file /cdsms/classes/Master.php?f=delete_package. The manipulation leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-28412. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	NA	Car Driving School Management System 1.0 Master.php SQL injection	A vulnerability was found in Car Driving School Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /cdsms/classes/Master.php?f=delete_enrollment. The manipulation leads to SQL injection. This vulnerability was named CVE-2022-28413. The attack can be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	NA	SourceCodester Baby Care System 1.0 /admin/posts.php find SQL injection	A vulnerability, which was classified as critical, was found in SourceCodester Baby Care System 1.0. This affects an unknown part of the file /admin/posts.php. The manipulation of the argument finds leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-28424. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	NA	SourceCodester Baby Care System 1.0 admin.php SQL injection	A vulnerability classified as critical has been found in SourceCodester Baby Care System 1.0. Affected is an unknown function of the file /admin.php?id=posts&action=display&value=1&postid=. The manipulation leads to SQL injection.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.

			This vulnerability is traded as CVE-2022-28421. It is possible to launch the attack remotely. Furthermore, there is an exploit available.		
	CVE-2022-28020	SourceCodester Attendance and Payroll System 1.0 \admin\position_edit.php SQL injection	A vulnerability was found in SourceCodester Attendance and Payroll System 1.0 and classified as critical. This issue affects some unknown processing of the file \admin\position_edit.php. The manipulation leads to SQL injection. The identification of this vulnerability is CVE-2022-28020. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	CVE-2022-28025	Student Grading System 1.0 rms.php SQL injection	A vulnerability classified as critical has been found in Student Grading System 1.0. This affects an unknown part of the file /student-grading-system/rms.php?page=school_year. The manipulation leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-28025. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	NA	Simple Real Estate Portal System 1.0 Users.php SQL injection	A vulnerability was found in Simple Real Estate Portal System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /reps/classes/Users.php?f=delete_agent. The manipulation leads to SQL injection. This vulnerability is handled as CVE-2022-28410. The attack may be launched remotely. Furthermore, there is an exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	CVE-2022-27985	CuppaCMS 1.0 alertLightbox.php SQL injection (ID 31)	A vulnerability, which was classified as critical, has been found in CuppaCMS 1.0. Affected by this issue is some unknown functionality of the file /administrator/alerts/alertLightbox.php. The manipulation leads to SQL injection. This vulnerability is handled as CVE-2022-27985. The attack may be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
	CVE-2022-29411	Hermit Plugin up to 3.1.6 on WordPress id SQL injection	A vulnerability was found in Hermit Plugin up to 3.1.6. It has been classified as critical. This affects an unknown part. The manipulation of the argument id leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-29411. It is possible to initiate	Protected by core rules.	Detected by the scanner as the SQL Injection attack.

				the attack remotely. There is no exploit available.		
		CVE-2022-29410	Hermit Plugin up to 3.1.6 on WordPress ids SQL injection	A vulnerability was found in Hermit Plugin up to 3.1.6 and classified as critical. Affected by this issue is some unknown functionality. The manipulation of the argument ids leads to SQL injection. This vulnerability is handled as CVE-2022-29410. The attack may be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
5	Cross- Site Scripting	CVE-2021-42946	htmly 2.8.1 /admin/config Copyright cross-site scripting	A vulnerability classified as problematic was found in htmly 2.8.1. Affected by this vulnerability is an unknown functionality of the file /admin/config. The manipulation of the argument Copyright leads to cross-site scripting. This vulnerability is known as CVE-2021-42946. The attack can be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2022-26565	Totaljs New Page Page Name cross-site scripting (ID 35)	A vulnerability classified as problematic has been found in Totaljs. This affects an unknown part of the component New Page Handler. The manipulation of the argument Page Name leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-26565. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-23288	Eaton Intelligent Power Protector prior 1.69 cross-site scripting	A vulnerability classified as problematic was found in Eaton Intelligent Power Protector. This vulnerability affects unknown code. The manipulation leads to cross- site scripting. This vulnerability was named CVE-2021-23288. The attack needs to be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2022-27436	Ecommerce-Website 1.1.0 index.php username cross-site scripting	A vulnerability was found in Ecommerce-Website 1.1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /public/admin/index.php?add_user. The manipulation of the argument username leads to cross-site scripting. This vulnerability was named CVE-2022-27436. The attack can be initiated remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2022-0830	FormBuilder Plugin up to 1.08 on WordPress cross-site scripting	A vulnerability, which was classified as problematic, was found in FormBuilder Plugin up to 1.08. Affected is an unknown function. The manipulation leads to cross-site scripting.	Protected by core rules.	Detected by the scanner as the

			This vulnerability is traded as CVE-2022-0830. It is possible to launch the attack remotely. There is no exploit available.		Cross-Site Scripting attack.
	CVE-2022-1170	Noo JobMonster Theme prior 4.5.2.9 on WordPress GET Request cross-site scripting	A vulnerability has been found in Noo JobMonster Theme and classified as problematic. This vulnerability affects unknown code of the component GET Request Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-1170. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
	CVE-2022-1168	WP JobSearch Plugin up to 1.5.0 on WordPress cross-site scripting	A vulnerability was found in WP JobSearch Plugin up to 1.5.0. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-1168. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
	NA	Ad Inserter Free Plugin/Ad Inserter Pro Plugin up to 2.7.11 on WordPress Admin Page REQUEST_URI cross-site scripting	A vulnerability, which was classified as problematic, was found in Ad Inserter Free Plugin and Ad Inserter Pro Plugin up to 2.7.11. This affects an unknown part of the component Admin Page. The manipulation of the argument REQUEST_URI leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-0901. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
	CVE-2022-24229	ONLYOFFICE Document Server Example up to 6.x /example/editor cross-site scripting (ID 252)	A vulnerability was found in ONLYOFFICE Document Server Example up to 6.x. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /example/editor. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-24229. The attack can be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.

		It is recommended to upgrade the affected component.		
CVE-2021-46437	ZZCMS 2021 ad_manage.php cross-site scripting	A vulnerability, which was classified as problematic, has been found in ZZCMS 2021. Affected by this issue is some unknown functionality of the file ad_manage.php. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2021-46437. The attack may be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2021-43009	OpMon up to 9.11 search cross-site scripting (ID 166619)	A vulnerability was found in OpMon up to 9.11. It has been classified as problematic. Affected is an unknown function. The manipulation of the argument search leads to cross-site scripting. This vulnerability is traded as CVE-2021-43009. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2021-32157	Webmin 1.973 Scheduled Cron Job cross-site scripting	A vulnerability, which was classified as problematic, has been found in Webmin 1.973. Affected by this issue is some unknown functionality of the component Scheduled Cron Job Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2021-32157. The attack may be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2021-32161	Webmin 1.973 File Manager cross-site scripting	A vulnerability was found in Webmin 1.973. It has been classified as problematic. Affected is an unknown function of the component File Manager. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2021-32161. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2021-32160	Webmin up to 1.973 Add User cross-site scripting	A vulnerability was found in Webmin up to 1.973 and classified as problematic. This issue affects some unknown processing of the component Add User Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2021-32160. The attack may be initiated remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2021-32158	Webmin 1.973 Upload/Download cross-site scripting	A vulnerability, which was classified as problematic, was found in Webmin 1.973. This affects an unknown part of the component Upload/Download. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.

		2021-32158. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-27125	zbzcms 1.0 /php/ajax.php neirong cross-site scripting	A vulnerability has been found in zbzcms 1.0 and classified as problematic. This vulnerability affects unknown code of the file /php/ajax.php. The manipulation of the argument neirong leads to cross-site scripting. This vulnerability was named CVE-2022-27125. The attack can be initiated remotely. There are no exploitations available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2022-27961	OFCMS 1.1.4 Comment /ofcms/company-c-47 cross-site scripting	A vulnerability classified as problematic has been found in OFCMS 1.1.4. This affects an unknown part of the file /ofcms/company-c-47 of the component Comment Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-27961. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2021-36828	WP Maintenance Plugin up to 6.0.4 on WordPress cross-site scripting	A vulnerability has been found in WP Maintenance Plugin up to 6.0.4 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2021-36828. The attack can be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2022-26594	Liferay Portal/DXP cross-site scripting	A vulnerability was found in Liferay Portal and DXP. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-26594. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2022-1231	plantuml prior 1.2022.4 Diagram Embedder cross-site scripting	A vulnerability, which was classified as problematic, has been found in plantuml. Affected by this issue is some unknown functionality of the component Diagram Embedder. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-1231. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
NA	KB Support Plugin up to 1.5.5 on	A vulnerability was found in KB Support Plugin up to 1.5.5. It has been declared as problematic. This vulnerability affects	Protected by	Detected by the scanner

		WordPress cross-site scripting	unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-27852. The attack can be initiated remotely. There is no exploit available.	core rules.	as the Cross-Site Scripting attack.
	CVE-2022-27425	Chamilo LMS 1.11.13 /blog/blog.php cross-site scripting	A vulnerability classified as problematic has been found in Chamilo LMS 1.11.13. This affects an unknown part of the file /blog/blog.php. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-27425. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
	CVE-2022-1380	snipe-it up to 5.4.2 Item name cross-site scripting	A vulnerability, which was classified as problematic, has been found in snipe-it up to 5.4.2. Affected by this issue is some unknown functionality. The manipulation of the argument Item name leads to cross-site scripting. This vulnerability is handled as CVE-2022-1380. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
	CVE-2022-27853	Contest Gallery Plugin up to 13.1.0.9 on WordPress cross-site scripting	A vulnerability classified as problematic has been found in Contest Gallery Plugin up to 13.1.0.9. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-27853. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
	CVE-2022-0780	SearchIQ Plugin up to 3.8 on WordPress siq_ajax customCss cross-site scripting	A vulnerability, which was classified as problematic, has been found in SearchIQ Plugin up to 3.8. Affected by this issue is the function siq_ajax. The manipulation of the argument customCss leads to cross-site scripting. This vulnerability is handled as CVE-2022-0780. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
	CVE-2022-1090	Good & Bad Comments Plugin up to 1.0.0 on WordPress cross-site scripting	A vulnerability classified as problematic has been found in Good & Bad Comments Plugin up to 1.0.0. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-1090.	Protected by core rules.	Detected by the scanner as the Cross-Site

		It is possible to launch the attack remotely. There is no exploit available.		Scripting attack.
CVE-2022-1088	Page Security & Membership Plugin up to 1.5.15 on WordPress cross-site scripting	A vulnerability was found in Page Security & Membership Plugin up to 1.5.15. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1088. The attack may be initiated remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2022-1001	WP Downgrade Plugin up to 1.2.2 on WordPress Target Version Setting cross-site scripting (ID 2696091)	A vulnerability was found in WP Downgrade Plugin up to 1.2.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Target Version Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-1001. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2022-0737	Text Hover Plugin up to 4.1 on WordPress cross-site scripting	A vulnerability, which was classified as problematic, was found in Text Hover Plugin up to 4.1. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-0737. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
Null	SolarWinds Database Performance Monitor 2022.1.7779 SQL Query cross-site scripting	A vulnerability classified as problematic has been found in SolarWinds Database Performance Monitor 2022.1.7779. This affects an unknown part of the component SQL Query Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2021-35229. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2022-28074	Halo 1.5.0 tools cross-site scripting (ID 1769)	A vulnerability was found in Halo 1.5.0. It has been classified as problematic. Affected is an unknown function of the file \admin\index.html#/system/tools. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-28074.	Protected by core rules.	Detected by the scanner as the Cross-Site

		It is possible to launch the attack remotely. There is no exploit available.		Scripting attack.
CVE-2022-1439	Microweber up to 1.2.14 cross-site scripting	A vulnerability classified as problematic has been found in Microweber up to 1.2.14. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-1439. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2022-1503	GetSimple CMS Content Module /admin/edit.php post-content cross-site scripting	A vulnerability, which was classified as problematic, has been found in GetSimple CMS. Affected by this issue is some unknown functionality of the file /admin/edit.php of the component Content Module. The manipulation of the argument post-content with the input <script>alert(1)</script> leads to cross-site scripting. This vulnerability is handled as CVE-2022-1503. The attack may be launched remotely. Furthermore, there is an exploit available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2022-1504	Microweber up to 1.2.14 cross-site scripting	A vulnerability classified as problematic has been found in Microweber up to 1.2.14. This affects an unknown part of the file /demo/module/?module=HERE. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1504. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2022-28102	PHP MySQL Admin Panel Generator 1 /edit-db.php cross-site scripting (ID 19)	A vulnerability has been found in PHP MySQL Admin Panel Generator 1 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /edit-db.php. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-28102. The attack can be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2022-24873	Shopware up to 5.7.8 Storefront cross-site scripting (GHSA-4g29-fccr-p59w)	A vulnerability classified as problematic has been found in Shopware up to 5.7.8. This affects an unknown part of the component Storefront. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-24873. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.

	It is recommended to upgrade the affected component.