

Monthly Zero-Day Vulnerability Coverage Bulletin

May 2022

Total Zero-Day Vulnerabilities Found: 271

Command Injection	CSRF	Local File Inclusion	Cross-Site Scripting	SQL Injection
19	6	17	109	120

Zero-Day vulnerabilities protected through core rules	271
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	265

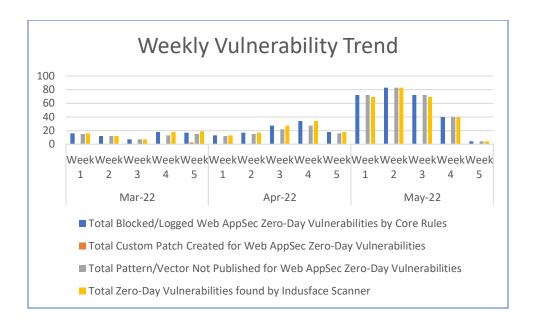
^{*} To enable custom rules, please contact support@indusface.com

^{**} 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%

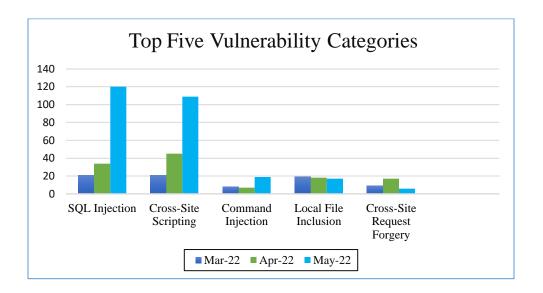
of the zero-day vulnerabilities were protected by the **core rules** in the last month.

NA

of the zero-day vulnerabilities were protected by the **custom rules** in the last month. 98%

of the zero-day vulnerabilities were reported by Indusface Scanner in the last month.







Vulnerability Details

1. Vulnerability Type: Command Injection

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-21189	dexie up to 3.2.1/4.0.0-alpha.2 setByKeyPath code injection	A vulnerability classified as critical has been found in dexie up to 3.2.1/4.0.0-alpha.2. This affects the function setByKeyPath. The manipulation leads to privilege escalation. This vulnerability is uniquely identified as CVE-2022-21189. It is possible to initiate the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.
		It is recommended to upgrade the affected component.		
CVE-2022-25301	jsgui-lang-essentials code injection	A vulnerability was found in jsgui-langessentials and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to privilege escalation. This vulnerability is handled as CVE-2022-25301. Access to the local network is	Protected by Core Rules	Detected by the scanner as the Command Injection attack.
		required for this attack. There is no exploit available.		
CVE-2022-24437	git-pull-or-clone up to 2.0.1 spawn outpath command injection (SNYK-JS- GITPULLORCLONE- 2434307)	A vulnerability was found in git-pull-or- clone up to 2.0.1. It has been classified as critical. Affected is the function spawn. The manipulation of the argument outpath leads to privilege escalation. This vulnerability is traded as CVE-2022- 24437. It is possible to launch the attack	Protected by Core Rules	Detected by the scanner as the Command Injection attack.
		remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		
CVE-2022-22143	convict up to 6.2.1 parentKey code injection (SNYK-JS- CONVICT-2340604)	A vulnerability, which was classified as critical, was found in convict up to 6.2.1. Affected is an unknown function. The manipulation of the argument parentKey leads to privilege escalation.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.



		This vulnerability is traded as CVE-2022-22143. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2022-25645	dset DSET Mode/Merge Mode code injection	A vulnerability was found in dset. It has been declared as critical. This vulnerability affects unknown code of the component DSET Mode/Merge Mode. The manipulation leads to privilege escalation. This vulnerability was named CVE-2022-	Protected by Core Rules	Detected by the scanner as the Command Injection attack.
		25645. The attack can be initiated remotely. There is no exploit available.		
CVE-2021-42165	MitraStar GPT- 2541GNAC-N1 100VNZ0b33 path os command injection (ID 164333 / EDB- 50351)	A vulnerability was found in MitraStar GPT-2541GNAC-N1 100VNZ0b33. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument path leads to privilege escalation.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.
		The identification of this vulnerability is CVE-2021-42165. The attack may be initiated remotely. Furthermore, there is an exploit available.		
CVE-2021-41739 Artica Proxy 4.30.000000 cyrus.events.php logs/rp os command injection	Artica Proxy 4.30.000000 cyrus.events.php logs/rp os command injection	A vulnerability classified as critical was found in Artica Proxy 4.30.000000. Affected by this vulnerability is an unknown functionality of the file cyrus.events.php. The manipulation of the argument logs/rp leads to privilege escalation.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.
		This vulnerability is known as CVE-2021-41739. The attack can be launched remotely. There is no exploit available.		
CVE-2022-23332	Shenzhen Ejoin ACOM508/ACOM516 /ACOM532 609-915- 041-100-020 Manual Ping Form command injection	A vulnerability classified as critical was found in Shenzhen Ejoin ACOM508, ACOM516 and ACOM532 609-915-041-100-020. This vulnerability affects unknown code of the component Manual Ping Form. The manipulation leads to privilege escalation.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.
		This vulnerability was named CVE-2022- 23332. The attack can be initiated remotely. There is no exploit available.		
CVE-2022-27224	Galleon NTS-6002 Web-Management Interface ping_address/trace_a ddress/nslookup_add	A vulnerability classified as critical has been found in Galleon NTS-6002. This affects an unknown part of the component Web-Management Interface. The manipulation of the argument ping_address/trace_address/nslookup_add	Protected by Core Rules	Detected by the scanner as the Command Injection attack.



	ress os command injection	ress leads to privilege escalation.		
	·	This vulnerability is uniquely identified as CVE-2022-27224. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2021-42581	Ramda up to 0.27.0 mapObjIndexed code injection	A vulnerability classified as critical was found in Ramda up to 0.27.0. Affected by this vulnerability is the function mapObjIndexed. The manipulation leads to privilege escalation.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.
		This vulnerability is known as CVE-2021-42581. The attack needs to be initiated within the local network. Furthermore, there is an exploit available.		
		It is recommended to apply a patch to fix this issue.		
CVE-2022-29307	lonizeCMS 1.0.8.1 lang_model.php copy_lang_content command injection (ID 405)	A vulnerability was found in IonizeCMS 1.0.8.1. It has been rated as critical. This issue affects the function copy_lang_content of the file application/models/lang_model.php. The manipulation leads to privilege escalation.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.
		The identification of this vulnerability is CVE-2022-29307. Access to the local network is required for this attack. There is no exploit available.		
CVE-2021-42969	Anaconda 2021.05 usercustomize.py os command injection	A vulnerability has been found in Anaconda 2021.05 and classified as critical. Affected by this vulnerability is an unknown functionality of the file usercustomize.py. The manipulation leads to privilege escalation.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.
		This vulnerability is known as CVE-2021-42969. The attack can only be initiated within the local network. There is no exploit available.		
CVE-2022-29303	SolarView Compact 6.00 conf_mail.php command injection	A vulnerability has been found in SolarView Compact 6.00 and classified as critical. Affected by this vulnerability is an unknown functionality of the file conf_mail.php. The manipulation leads to privilege escalation.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.
		This vulnerability is known as CVE-2022-29303. Access to the local network is required for this attack. There is no exploit available.		
CVE-2022-25862	sds 0.0.0 js/set.js set code injection (SNYK- JS-SDS-2385944)	A vulnerability classified as critical was found in sds 0.0.0. Affected by this vulnerability is the function set of the file	Protected by Core Rules	Detected by the scanner as the Command



js/set.js. The manipulation leads to privilege escalation.

Injection attack.

This vulnerability is known as CVE-2022-25862. It is possible to launch the attack on the local host. There is no exploit available.



2. <u>Vulnerability Type: Cross- Site Request Forgery</u>

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-0191	Ad Invalid Click Protector Plugin up to 1.2.6 on WordPress cross-site request forgery (ID 2705068)	A vulnerability was found in Ad Invalid Click Protector Plugin up to 1.2.6. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site request forgery.	Protected by Core Rules	NA
		This vulnerability is known as CVE-2022-0191. The attack can be launched remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		
CVE-2022-23904	Rainworx Auctionworx Enterprise/Auctionworx Events Edition up to 3.1R1 Admin Control Panel cross- site request forgery	A vulnerability was found in Rainworx Auctionworx Enterprise and Auctionworx Events Edition up to 3.1R1. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Admin Control Panel. The manipulation leads to cross site request forgery. This vulnerability is known as CVE-	Protected by Core Rules	NA
		2022-23904. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2022-25778	Secomea GateManager Web UI cross-site request forgery	A vulnerability, which was classified as problematic, was found in Secomea GateManager. This affects an unknown part of the component Web UI. The manipulation leads to cross site request forgery.	Protected by Core Rules	NA
		This vulnerability is uniquely identified as CVE-2022-25778. It is possible to initiate the attack		



		remotely. There is no exploit available.		
CVE-2022-30953	Blue Ocean Plugin up to 1.25.3 on Jenkins HTTP Server cross-site request forgery	A vulnerability was found in Blue Ocean Plugin up to 1.25.3. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component HTTP Server. The manipulation leads to cross site request forgery.	Protected by Core Rules	NA
		This vulnerability is known as CVE- 2022-30953. The attack can be launched remotely. There is no exploit available.		
CVE-2022-28921	BlogEngine.NET 3.3.8.0 cross-site request forgery	A vulnerability, which was classified as problematic, was found in BlogEngine.NET 3.3.8.0. Affected is an unknown function. The manipulation leads to cross site request forgery.	Protected by Core Rules	NA
		This vulnerability is traded as CVE- 2022-28921. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2022-29427	Aftab Muni Disable Right Click for WP Plugin up to 1.1.6 on WordPress cross- site request forgery	A vulnerability was found in Aftab Muni Disable Right Click for WP Plugin up to 1.1.6. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross site request forgery.	Protected by Core Rules	NA
		The identification of this vulnerability is CVE-2022-29427. The attack may be initiated remotely. There is no exploit available.		
CVE-2022-0191	Ad Invalid Click Protector Plugin up to 1.2.6 on WordPress cross-site request forgery (ID 2705068)	A vulnerability was found in Ad Invalid Click Protector Plugin up to 1.2.6. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site request forgery.	Protected by Core Rules	NA
		This vulnerability is known as CVE-2022-0191. The attack can be launched remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		



3. <u>Vulnerability Type: Local File Inclusion</u>

Public ID	Vulnerability Type	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-25842	com.alibaba.oneagent:one-java- agent-plugin ZIP File pathname traversal	A vulnerability was found in com.alibaba.oneagent:one-java-agent-plugin. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component ZIP File Handler. The manipulation leads to directory traversal.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
		This vulnerability is known as CVE-2022-25842. The attack can be launched remotely. There is no exploit available.		
		It is recommended to apply a patch to fix this issue.		
CVE-2022-26068	pistache prior 0.0.3.20220425 path traversal	A vulnerability was found in pistache. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to directory traversal.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
		The identification of this vulnerability is CVE-2022-26068. The attack may be initiated remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		
CVE-2022-1554	clinical-genomics scout up to 4.51 send_file path traversal	A vulnerability was found in clinical-genomics scout up to 4.51. It has been classified as critical. Affected is the function send_file. The manipulation leads to directory traversal.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
		This vulnerability is traded as CVE-2022-1554. It is possible to launch the attack remotely. There is no exploit available.		



		It is recommended to upgrade the affected component.		
CVE-2022-24897	xwiki-commons up to 12.6.6/12.10.2 API path traversal (GHSA-cvx5-m8vg-vxgc)	A vulnerability has been found in xwiki-commons up to 12.6.6/12.10.2 and classified as critical. Affected by this vulnerability is an unknown functionality of the component API. The manipulation leads to directory traversal. This vulnerability is known as CVE-2022-24897. 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-2021-42183	MasaCMS 7.2.1 path traversal	A vulnerability was found in MasaCMS 7.2.1. It has been classified as critical. This affects an unknown part of the file /index.cfm/_api/asset/image/. The manipulation leads to directory traversal.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
		This vulnerability is uniquely identified as CVE-2021-42183. The attack needs to be initiated within the local network. There		
CVE-2021-45783	Bookeen Notea BK_R_1.0.5_20210608 pathname traversal	is no exploit available. A vulnerability, which was classified as problematic, was found in Bookeen Notea BK_R_1.0.5_20210608. This affects an unknown part. The manipulation leads to directory traversal.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
		This vulnerability is uniquely identified as CVE-2021-45783. Access to the local network is required for this attack to succeed. There is no exploit available.		
CVE-2022-30062	ftcms up to 2.1 tp.php path traversal	A vulnerability was found in ftcms up to 2.1. It has been rated as problematic. Affected by this issue is some unknown functionality of the file tp.php. The manipulation leads to directory traversal.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
		This vulnerability is handled as CVE-2022-30062. The attack		



		can only be initiated within the local network. There is no exploit available.		
CVE-2022-30061	ftcms up to 2.1 tp pathname traversal	A vulnerability classified as critical has been found in ftcms up to 2.1. Affected is an unknown function. The manipulation of the argument tp leads to directory traversal.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
		This vulnerability is traded as CVE-2022-30061. The attack needs to be initiated within the local network. There is no exploit available.		
CVE-2021-34605	XINJE PLC Program Tool up to 3.5.1 Project File path traversal	A vulnerability, which was classified as problematic, was found in XINJE PLC Program Tool up to 3.5.1. This affects an unknown part of the component Project File Handler. The manipulation leads to directory traversal.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
		This vulnerability is uniquely identified as CVE-2021-34605. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-29596	MicroStrategy Enterprise Manager 2022 Uid pathname traversal	A vulnerability classified as critical was found in MicroStrategy Enterprise Manager 2022. Affected by this vulnerability is an unknown functionality. The manipulation of the argument Uid leads to directory traversal.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
		This vulnerability is known as CVE-2022-29596. Access to the local network is required for this attack to succeed. Furthermore, there is an exploit available.		
CVE-2022-1560	Amministrazione Aperta Plugin up to 3.7.3 on WordPress open path traversal	A vulnerability was found in Amministrazione Aperta Plugin up to 3.7.3 and classified as critical. This issue affects some unknown processing. The manipulation of the argument open leads to directory traversal.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
		The identification of this vulnerability is CVE-2022-1560.		



		The attack can only be done within the local network. There is no exploit available.		
CVE-2022-1721	jgraph drawio up to 18.0.4 WellKnownServlet path traversal	A vulnerability classified as critical was found in jgraph drawio up to 18.0.4. Affected by this vulnerability is an unknown functionality of the component WellKnownServlet. The manipulation leads to directory traversal.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
		This vulnerability is known as CVE-2022-1721. The attack can be launched remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		
CVE-2022-29446	Counter Box Plugin up to 1.1.1 file inclusion	A vulnerability was found in Counter Box Plugin up to 1.1.1. It has been classified as critical. Affected is an unknown function. The manipulation leads to privilege escalation.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
		This vulnerability is traded as CVE-2022-29446. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2022-29447	Wow-Company Hover Effects Plugin up to 2.1 on WordPress file inclusion	A vulnerability, which was classified as critical, was found in Wow-Company Hover Effects Plugin up to 2.1. Affected is an unknown function. The manipulation leads to privilege escalation.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
		This vulnerability is traded as CVE-2022-29447. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2022-29448	Wow-Company Herd Effects Plugin up to 5.2 on WordPress file inclusion	A vulnerability has been found in Wow-Company Herd Effects Plugin up to 5.2 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to privilege escalation.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
		This vulnerability is known as CVE-2022-29448. The attack can be launched remotely. There is no exploit available.		



CVE-2022-31268	Gitblit 1.9.3 /resources/// path traversal	A vulnerability was found in Gitblit 1.9.3. It has been declared as critical. This vulnerability affects unknown code of the file /resources///. The manipulation leads to directory traversal.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
		This vulnerability was named CVE-2022-31268. The attack can be initiated remotely. There is no exploit available.		
CVE-2022-1850	filegator up to 7.7.x path traversal	A vulnerability classified as critical has been found in filegator up to 7.7.x. Affected is an unknown function. The manipulation leads to directory traversal.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
		This vulnerability is traded as CVE-2022-1850. It is possible to launch the attack remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		



4. Vulnerability Type: Cross-Site Scripting

Public ID	Vulnerability Name	Vulnerability Description	AppTrana WAF Coverage	Indusface WAS Coverage
		A vulnerability, which was classified as problematic, was found in Shopizer up to 2.17.0. This affects an unknown part of the component Manage Files. The manipulation of the argument filename leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
		This vulnerability is uniquely identified as CVE-2022-23060. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-23060	Shopizer up to 2.17.0 Manage Files filename cross-site scripting	It is recommended to apply a patch to fix this issue.		
		A vulnerability was found in materializecss. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-25349	materialize-css cross-site scripting	This vulnerability is uniquely identified as CVE-2022-25349. It is possible to initiate the attack remotely. There is no exploit available.		
		A vulnerability was found in Event List Plugin up to 0.8.7. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
	For the Physics and the O. 7.	This vulnerability is handled as CVE-2022-0418. The attack may be launched remotely. There is no exploit available.		
CVE-2022-0418	Event List Plugin up to 0.8.7 on WordPress Setting cross-site scripting	It is recommended to upgrade the affected component.		
	Cyclos Pro up to 14.7	A vulnerability classified as problematic has been found in Cyclos Pro up to 14.7. This affects an unknown part of the component Account Registration Handler. The manipulation of the	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2021-31673	Account Registration groupId cross-site scripting	argument groupId leads to cross-site scripting.		



		This vulnerability is uniquely identified as CVE-2021-31673. It is possible to initiate the attack remotely. There is no exploit available.		
		A vulnerability classified as problematic was found in AdRotate Plugin up to 5.8.22. This vulnerability affects unknown code of the component Group Name Handler. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
		This vulnerability was named CVE-2022-0649. The attack can be initiated remotely. There is no Protected by Core Rules exploit available.		
CVE-2022-0649	AdRotate Plugin up to 5.8.22 on WordPress Group Name cross-site scripting	It is recommended to upgrade the affected component.		
	. 0	A vulnerability was found in Import and Export Users and Customers Plugin up to 1.19.2.0. It has been classified as problematic. This affects an unknown part of the component CSV Data Handler. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
	Import and Export Users	This vulnerability is uniquely identified as CVE-2022-1255. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-1255	and Customers Plugin up to 1.19.2.0 on WordPress CSV Data cross-site scripting	It is recommended to upgrade the affected component.		
		A vulnerability was found in LifterLMS PayPal Plugin up to 1.3.x and classified as problematic. Affected by this issue is some unknown functionality of the component Payment Confirmation Page. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
	LifterLMS PayPal Plugin up to 1.3.x on WordPress	This vulnerability is handled as CVE-2022-1250. The attack may be launched remotely. There is no exploit available.		
CVE-2022-1250	Payment Confirmation Page cross-site scripting	It is recommended to upgrade the affected component.		
CVE-2021-25102	All In One WP Security & Firewall Plugin up to 4.4.10 on WordPress Location Header redirect_to cross- site scripting	A vulnerability was found in All In One WP Security & Firewall Plugin up to 4.4.10. It has been classified as problematic. Affected is an unknown function of the component Location Header Handler. The manipulation of the	Protected by Core Rules	Detected by scanner as cross-site scripting attack
		•		



		argument redirect to leads to cross-site scripting.		
		This vulnerability is traded as CVE-2021-		
		25102. It is possible to launch the attack		
		remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		
		A vulnerability classified as problematic	Protected	Detected by
		has been found in Content Egg Plugin up	by Core	scanner as
		to 5.2.x. This affects an unknown part of	Rules	cross-site
		the component Autoblogging Admin		scripting
		Dashboard. The manipulation of the		attack
		argument page leads to cross-site scripting.		
		This vulnerability is uniquely identified as		
		CVE-2022-0428. It is possible to initiate		
	Content Egg Plugin up to	the attack remotely. There is no exploit		
	5.2.x on WordPress	available.		
	Autoblogging Admin	It is recommended to ungrade the		
CVE-2022-0428	Dashboard page cross-site scripting	It is recommended to upgrade the affected component.		
012 2022 0 120	30.16.11.9	A vulnerability has been found in Visual	Protected	Detected by
		Form Builder Plugin up to 3.0.6 and	by Core	scanner as
		classified as problematic. Affected by this	Rules	cross-site
		vulnerability is an unknown functionality.		scripting
		The manipulation of the argument email		attack
		to leads to cross-site scripting.		
		This vulnerability is known as CVE-2022-		
		1046. The attack can be launched		
		remotely. There is no exploit available.		
	Visual Form Builder Plugin			
	up to 3.0.6 on WordPress	It is recommended to upgrade the		
CVE-2022-1046	Email to cross-site scripting	affected component.		
		A vulnerability has been found in 10Web	Protected	Detected by
		Photo Gallery Plugin up to 1.6.2 and	by Core	scanner as
		classified as problematic. This vulnerability affects unknown code of the	Rules	cross-site scripting
		component AJAX Action Handler. The		attack
		manipulation of the argument image_url		attaan
		leads to cross-site scripting.		
		This vulnerability was named CVE-2022-		
	10Web Photo Gallery	1282. The attack can be initiated		
	Plugin up to 1.6.2 on	remotely. There is no exploit available.		
	WordPress AJAX Action	W to		
CVE 2022 1202	image_url cross-site	It is recommended to upgrade the		
CVE-2022-1282	scripting Advanced Page Visit	affected component. A vulnerability was found in Advanced	Protected	Detected by
	Counter Plugin up to 5.0.8	Page Visit Counter Plugin up to 5.0.8 and	by Core	scanner as
CVE-2021-25086	on WordPress Admin	classified as problematic. This issue	Rules	cross-site



	Dashboard Page cross-site scripting	affects some unknown processing of the component Admin Dashboard Page. The manipulation leads to cross-site scripting.		scripting attack
		The identification of this vulnerability is CVE-2021-25086. The attack may be initiated remotely. There is no exploit available.		
		A vulnerability was found in Cyclos Pro up to 4.14.7. It has been classified as problematic. Affected is an unknown function of the component Error Handler. The manipulation leads to crosssite scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2021-31674	Cyclos Pro up to 4.14.7 Error cross-site scripting	This vulnerability is traded as CVE-2021-31674. It is possible to launch the attack remotely. There is no exploit available.		
		A vulnerability, which was classified as problematic, has been found in AdRotate Plugin up to 5.8.22. This issue affects some unknown processing of the component Advert Name Handler. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
	AdRotate Plugin up to 5.8.22 on WordPress	The identification of this vulnerability is CVE-2022-0662. The attack may be initiated remotely. There is no exploit available.		
CVE-2022-0662	Advert Name cross-site scripting	It is recommended to upgrade the affected component.		
		A vulnerability was found in RSS Extension and classified as problematic. This issue affects some unknown processing of the component RSS Element Handler. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
		The identification of this vulnerability is CVE-2022-29969. The attack may be initiated remotely. There is no exploit available.		
CVE-2022-29969	RSS Extension on MediaWiki RSS Element cross-site scripting	It is recommended to upgrade the affected component.		
		A vulnerability has been found in Vendure up to 1.5.1 and classified as problematic. This vulnerability affects unknown code of the component SVG File Handler. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-23065	Vendure up to 1.5.1 SVG File cross-site scripting	This vulnerability was named CVE-2022-		



		23065. The attack can be initiated		
		remotely. There is no exploit available.		
		It is recommended to apply a patch to fix		
		this issue.		
		A vulnerability was found in Fast Flow	Protected	Detected by
		Plugin up to 1.2.10. It has been declared	by Core	scanner as
		as problematic. This vulnerability affects	Rules	cross-site
		unknown code of the component Admin		scripting
		Dashboard. The manipulation of the		attack
		argument page leads to cross-site scripting.		
		scripting.		
		This vulnerability was named CVE-2022-		
		1269. The attack can be initiated		
	Fast Flow Plugin up to	remotely. There is no exploit available.		
	1.2.10 on WordPress Admin			
	Dashboard page cross-site	It is recommended to upgrade the		
CVE-2022-1269	scripting	affected component.		
		A vulnerability, which was classified as	Protected	Detected by
		problematic, has been found in	by Core	scanner as
		MyThemeShop WP Subscribe Plugin up	Rules	cross-site
		to 1.2.12. Affected by this issue is some		scripting
		unknown functionality. The manipulation		attack
		leads to cross-site scripting.		
	MyThemeShop WP	This could near hill the in heard like in CVF 2024		
	Subscribe Plugin up to	This vulnerability is handled as CVE-2021-		
CVE-2021-36844	1.2.12 on WordPress cross-	36844. The attack may be launched		
CVE-2021-30644	site scripting	remotely. There is no exploit available. A vulnerability classified as problematic	Protected	Detected by
		has been found in Pixelimity 1.0. This	by Core	scanner as
		affects an unknown part of the file	Rules	cross-site
		admin/pages.php?action=add_new. The	raics	scripting
		manipulation of the argument Title leads		attack
		to cross-site scripting.		
CVE-2022-28589		This vulnerability is uniquely identified as		
	Pixelimity 1.0 pages.php	CVE-2022-28589. It is possible to initiate		
	Title cross-site scripting (ID	the attack remotely. There is no exploit		
	23)	available. A vulnerability, which was classified as	Protected	Detected by
		problematic, has been found in	by Core	scanner as
		PartKeepr 1.4.0. This issue affects some	Rules	cross-site
		unknown processing of the component	Naics	scripting
		API Endpoint Handler. The manipulation		attack
		of the argument name leads to cross-site		actaon
		scripting.		
		The identification of this vulnerability is		
	PartKeepr 1.4.0 API	CVE-2021-39390. The attack may be		
<u> </u>	Endpoint name cross-site	initiated remotely. There is no exploit		
CVE-2021-39390	scripting (ID 1237)	available.		



SpringBootMovie up to 1.2. It has been unknown part of the component Movie Name Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-28588. It is possible to initiate the attack remotely. There is no exploit available. EVE-2022-28588 Microweber up to 1.2. If is recommended to upgrade the affected component. Microweber up to 1.2.15. Affected is an unknown function. The manipulation leads to cross-site scripting attact of the size per found in Microweber up to the attack remotely. There is no exploit available. Wilderability is traded as CVE-2022-1555. It is possible to launch the attack remotely. There is no exploit available. Wilderability is traded as CVE-2022-1555. It is possible to launch the attack remotely. There is no exploit available. Wilderability was found in SourceCodester E-Commerce Website 1.0 and classified as problematic. This issue affects some unknown processing of the file /public/admin/index.php?add_product. The manipulation of the argument Product Title leads to cross-site scripting. SourceCodester E-Commerce Website 1.0 index.php Product Title leads to cross-site scripting. SourceCodester E-Commerce Website 1.0 index.php Product Title leads to cross-site scripting. SourceCodester E-Commerce Website 1.0 index.php Product Title leads to cross-site scripting. A vulnerability classified as problematic has been found in MantisBT up to 2.25.1. This affects an unknown part of the file browser_sacrh_pulgin.php for the component tildden input field handler. The manipulation of the argument return leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-28508. It is possible to initiate the attack remotely. There is no exploit available. WantisBT up to 2.25.1 Hidden input Field browser_sacrh_pulgin.php for the corpose. The corpose of the file browser_sacrh_pulgin.php for the corpose of the file browser_sacrh_pulgin.php for the corpose of the file browser_sacrh_pulgin.php for the corpose of the file brow	CVE-2022-1571	neorazorx facturascripts prior 2022.07 Create	A vulnerability classified as problematic was found in neorazorx facturascripts. Affected by this vulnerability is an	Protected by Core Rules	Detected by scanner as cross-site
SpringBootMovie up to 1.2. It has been classified as problematic. This affects an unknown part of the component Movie Name Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-28588 to pringBootMovie up to 1.2 Movie Name cross-site wheat tack remotely. There is no exploit available. CVE-2022-28588 to pring SpringBootMovie up to 1.2 CVE-2022-28588. It is possible to initiate the attack remotely. There is no exploit available. A vulnerability classified as problematic has been found in Microweber up to 1.2.15. Affected is an unknown function. The manipulation leads to cross-site scripting. Microweber up to 1.2.15 CVE-2022-1555 to it is possible to launch the attack remotely. There is no exploit available. Microweber up to 1.2.15 CVE-2022-1555 to a fire scripting attack remotely. There is no exploit available. Microweber up to 1.2.15 CVE-2022-1555 to a fire scripting affected component. A vulnerability was found in SourceCodester E-Commerce Website 1.0 and classified as problematic. This issue affects some unknown processing of the file public/admin/index.php?add_product. The manipulation of the argument Product Title leads to cross-site scripting. SourceCodester E-Commerce Website 1.0 index.php Product Title cross-site scripting. SourceCodester E-Commerce Website 1.0 index.php Product Title cross-site scripting. A vulnerability classified as problematic has been found in MantisBT up to 2.25.1. This affects an unknown part of the file browser_search_plugin.php of the component Hidden Input Field Handler. The manipulation of the argument return leads to cross-site scripting. A vulnerability is uniquely identified as CVE-2022-228508. It is possible to initiate the attack remotely. There is no exploit available.	CVE-2022-28508		affected component.	Drotoctod	Dotostad b
SpringBootMovie up to 1.2. It has been by Core classified as problematic. This affects an unknown part of the component Movie was been found in Microweber up to 1.2 that sheen by Core scan cVE-2022-28588. It is possible to initiate the attack remotely. There is no exploit available. Protected by Core scan available. Wilcroweber up to 1.2.15. Affected is an unknown function. The manipulation leads to cross-site scripting. Microweber up to 1.2.15. It is possible to initiate the attack remotely. There is no exploit available. Wilcroweber up to 1.2.15. It is possible to a nunknown function. The manipulation leads to cross-site scripting. Microweber up to 1.2.15 ti is possible to launch the attack remotely. There is no exploit available. Wilcroweber up to 1.2.15 ti is possible to launch the attack remotely. There is no exploit available. Wilcroweber up to 1.2.15 affected component. A vulnerability was found in SourceCodester E-Commerce Website 1.0 and classified as problematic. This issue affects some unknown processing of the file /public/admin/index.php?add_product. The manipulation of the argument Product Title leads to cross-site scripting. SourceCodester E-Commerce Website 1.0 index.php Product Title leads to cross-site scripting. A vulnerability classified as problematic. This issue affects some unknown processing of the file /public/admin/index.php?add_product. The manipulation of the argument Product Title leads to cross-site scripting. A vulnerability classified as problematic has been found in MantisBr up to 2.25.1. This affects an unknown part of the file browser_search_plugin.php of the component Hidden Input Field Handler. The manipulation of the argument return.		Hidden Input Field	CVE-2022-28508. It is possible to initiate the attack remotely. There is no exploit		
SpringBootMovie up to 1.2. It has been classified as problematic. This affects an unknown part of the component Movie scripting. This vulnerability is uniquely identified as to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-28588. It is possible to initiate the attack remotely. There is no exploit available. CVE-2022-28588 A vulnerability classified as problematic has been found in Microweber up to 1.2.15. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-1555. It is possible to initiate the attack remotely. There is no exploit available. Microweber up to 1.2.15 This vulnerability is traded as CVE-2022-1555. It is possible to launch the attack remotely. There is no exploit available. Microweber up to 1.2.15 It is recommended to upgrade the affected component. A vulnerability was found in Protected by Core scan SourceCodester E-Commerce Website 1.0 and classified as problematic. This issue affects some unknown processing of the file [public/admin/index.php?add_product. The manipulation of the argument Product Title leads to cross-site scripting. SourceCodester E-Commerce Website 1.0 CVE-2022-27330. The attack may be index.php Product Title initiated remotely. Furthermore, there is an exploit available.			has been found in MantisBT up to 2.25.1. This affects an unknown part of the file browser_search_plugin.php of the component Hidden Input Field Handler. The manipulation of the argument return	by Core	Detected by scanner as cross-site scripting attack
SpringBootMovie up to 1.2. It has been classified as problematic. This affects an unknown part of the component Movie scripting. SpringBootMovie up to 1.2 Movie Name Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as VCVE-2022-28588. It is possible to initiate the attack remotely. There is no exploit available. CVE-2022-28588 scripting A vulnerability classified as problematic has been found in Microweber up to by Core scani The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-1555. It is possible to launch the attack remotely. There is no exploit available. Microweber up to 1.2.15 This vulnerability is traded as CVE-2022-1555. It is possible to launch the attack remotely. There is no exploit available. Microweber up to 1.2.15 A vulnerability was found in SourceCodester E-Commerce Website by Core scani feeted component. A vulnerability was found in Protected Dete SourceCodester E-Commerce Website by Core scani 1.0 and classified as problematic. This is sulnerability was found in SourceCodester E-Commerce Website by Core scani Sissue affects some unknown processing of the file /public/admin/index.php?add_product. The manipulation of the argument	CVE-2022-27330	Commerce Website 1.0 index.php Product Title	CVE-2022-27330. The attack may be initiated remotely. Furthermore, there is an exploit available.		
SpringBootMovie up to 1.2. It has been classified as problematic. This affects an unknown part of the component Movie Name Handler. The manipulation leads to cross-site scripting. SpringBootMovie up to 1.2 CVE-2022-28588. It is possible to initiate the attack remotely. There is no exploit available. A vulnerability classified as problematic has been found in Microweber up to 1.2.15. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-28588. It is possible to initiate the attack remotely. There is no exploit available. Protected by Core scans 1.2.15. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-1555. It is possible to launch the attack remotely. There is no exploit available. Microweber up to 1.2.15 It is recommended to upgrade the affected component.			1.0 and classified as problematic. This issue affects some unknown processing of the file /public/admin/index.php?add_product. The manipulation of the argument	•	scanner as cross-site scripting attack
SpringBootMovie up to 1.2. It has been classified as problematic. This affects an unknown part of the component Movie Name Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-28588. It is possible to initiate the attack remotely. There is no exploit available. A vulnerability classified as problematic has been found in Microweber up to 1.2.15. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-21555. It is possible to launch the attack	CVE-2022-1555	•	affected component.	Protected	Detected by
SpringBootMovie up to 1.2. It has been by Core scans classified as problematic. This affects an unknown part of the component Movie Name Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as SpringBootMovie up to 1.2 CVE-2022-28588. It is possible to initiate Movie Name cross-site the attack remotely. There is no exploit available. CVE-2022-28588 scripting A vulnerability classified as problematic has been found in Microweber up to by Core scans 1.2.15. Affected is an unknown function. Rules cross The manipulation leads to cross-site scripting scripting has been found in leads to cross-site scripting.			1555. It is possible to launch the attack		
SpringBootMovie up to 1.2. It has been by Core scans classified as problematic. This affects an unknown part of the component Movie scripting. This vulnerability is uniquely identified as SpringBootMovie up to 1.2 Movie Name cross-site the attack remotely. There is no exploit available.			has been found in Microweber up to 1.2.15. Affected is an unknown function. The manipulation leads to cross-site	by Core	Detected by scanner as cross-site scripting attack
SpringBootMovie up to 1.2. It has been by Core scans classified as problematic. This affects an Rules cross unknown part of the component Movie script Name Handler. The manipulation leads attactions attacted the component Movie script Name Handler.	CVE-2022-28588	Movie Name cross-site	CVE-2022-28588. It is possible to initiate the attack remotely. There is no exploit available.		
A vulnerability was found in Protected Dete			SpringBootMovie up to 1.2. It has been classified as problematic. This affects an unknown part of the component Movie Name Handler. The manipulation leads	by Core	Detected by scanner as cross-site scripting attack



	Subaccount cross-site scripting	unknown functionality of the component Create Subaccount Handler. The manipulation leads to cross-site scripting.		scripting attack
		This vulnerability is known as CVE-2022- 1571. The attack can be launched remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		
		A vulnerability was found in microweber up to 1.2.15. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
		This vulnerability is uniquely identified as CVE-2022-1584. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-1584	microweber up to 1.2.15 cross-site scripting	It is recommended to upgrade the affected component.		
		A vulnerability was found in Bludit 3.13.1. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/newcontent of the component New Content Module. The manipulation of the argument content with the input <script>alert(1)</script> leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1590	Bludit 3.13.1 New Content Module /admin/new- content cross-site scripting	This vulnerability was named CVE-2022- 1590. The attack can be initiated remotely. Furthermore, there is an exploit available.		
	,	A vulnerability was found in jgraph drawio up to 17.x. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
		This vulnerability is handled as CVE-2022- 1575. The attack may be launched remotely. There is no exploit available.		
CVE-2022-1575	jgraph drawio up to 17.x cross-site scripting	It is recommended to upgrade the affected component.		
	LibreHealth EHR 2.0.0 GET Parameter sl_eob_process.php debug/InsId cross-site	A vulnerability was found in LibreHealth EHR 2.0.0. It has been classified as problematic. Affected is an unknown function of the file	Protected by Core Rules	Detected by scanner as cross-site scripting
CVE-2022-29939	scripting	interface\billing\sl_eob_process.php of		attack



		the component GET Parameter Handler.		
		The manipulation of the argument		
		debug/InsId leads to cross-site scripting.		
		This vulnerability is traded as CVE-2022-		
		29939. It is possible to launch the attack		
		remotely. There is no exploit available.		
		A vulnerability was found in Themify Post	Protected	Detected by
		Type Builder Search Addon Plugin up to	by Core	scanner as
		1.3.x. It has been declared as	Rules	cross-site
		problematic. Affected by this		scripting
		vulnerability is an unknown functionality.		attack
		The manipulation leads to cross-site		
		scripting.		
		This vulnerability is known as CVE-2022-		
		1047. The attack can be launched		
	Themify Post Type Builder	remotely. There is no exploit available.		
	Search Addon Plugin up to			
	1.3.x on WordPress cross-	It is recommended to upgrade the		
CVE-2022-1047	site scripting	affected component.		
		A vulnerability was found in IgniteUp	Protected	Detected by
		Plugin up to 3.4.1. It has been classified	by Core	scanner as
		as problematic. Affected is an unknown	Rules	cross-site
		function. The manipulation leads to		scripting
		cross-site scripting.		attack
	IgniteUp Plugin up to 3.4.1	This vulnerability is traded as CVE-2022-		
	on WordPress cross-site	0898. It is possible to launch the attack		
CVE-2022-0898	scripting	remotely. There is no exploit available.		
		A vulnerability has been found in Admin	Protected	Detected by
		Menu Editor Plugin up to 1.0.4 and	by Core	scanner as
		classified as problematic. This	Rules	cross-site
		vulnerability affects unknown code. The		scripting
		manipulation leads to cross-site scripting.		attack
	Admin Menu Editor Plugin	This vulnerability was named CVE-2022-		
	up to 1.0.4 on WordPress	0625. The attack can be initiated		
CVE-2022-0625	cross-site scripting	remotely. There is no exploit available.		
		A vulnerability classified as problematic	Protected	Detected by
		has been found in Vertical Scroll Recent	by Core	scanner as
		Post Plugin up to 13.x. This affects an	Rules	cross-site
		unknown part. The manipulation leads to		scripting
		cross-site scripting.		attack
		This vulnerability is uniquely identified as		
		CVE-2022-1171. It is possible to initiate		
		the attack remotely. There is no exploit		
	Vertical Scroll Recent Post	available.		
	Plugin up to 13.x on			
	WordPress cross-site	It is recommended to upgrade the		
CVE-2022-1171	scripting	affected component.		



		A vulnerability was found in WP Social Buttons Plugin up to 2.1 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-0874	WP Social Buttons Plugin up to 2.1 on WordPress cross- site scripting	The identification of this vulnerability is CVE-2022-0874. The attack may be initiated remotely. There is no exploit available.		
		A vulnerability, which was classified as problematic, has been found in Easily Generate Rest API Url Plugin up to 1.0.0. This issue affects some unknown processing. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1338	Easily Generate Rest API Url Plugin up to 1.0.0 on WordPress cross-site scripting	The identification of this vulnerability is CVE-2022-1338. The attack may be initiated remotely. There is no exploit available.		
		A vulnerability was found in Popup Maker Plugin up to 1.16.4. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
		This vulnerability is handled as CVE-2022- 1104. The attack may be launched remotely. There is no exploit available.		
CVE-2022-1104	Popup Maker Plugin up to 1.16.4 on WordPress cross- site scripting	It is recommended to upgrade the affected component.		
		A vulnerability classified as problematic was found in PHProjekt PhpSimplyGest 1.3.0. Affected by this vulnerability is an unknown functionality of the component Project Title Handler. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-27308	PHProjekt PhpSimplyGest 1.3.0 Project Title cross-site scripting (ID 166966)	This vulnerability is known as CVE-2022-27308. The attack can be launched remotely. There is no exploit available.		
		A vulnerability was found in WP-JS Plugin up to 2.0.6. It has been rated as problematic. This issue affects the function wp_js_admin of the file wp-js.php. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1567	WP-JS Plugin up to 2.0.6 on WordPress wp-js.php wp_js_admin cross-site scripting	The identification of this vulnerability is CVE-2022-1567. The attack may be initiated remotely. There is no exploit available.		



A vulnerability, which was classified as protected by Core grammer Signup leads to cross-site scripting. Survey Sparrow Enterprise 2022. This issue affects some unknown processing. The manipulation of the argument Signup leads to cross-site scripting. The identification of this vulnerability is CVE-2022-29727. The attack may be initiated remotely. There is no exploit available. A vulnerability as found in CDR codeserver up to 3.11.x. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component URL Handler. The manipulation leads to cross-site scripting attack CVE-2021-42648 CVE-2021-42648 CVE-2021-42648 CVE-2021-42648 CVE-2021-42648 CVE-2021-42648 CVE-2021-42649					
Survey Sparrow Enterprise Survey Software 2022 Signup cross-site scripting available. A valuerability was found in CDR codeserver up to 3.11.x. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component URL Handler. The manipulation leads to cross-site scripting. CDR code-server up to 3.11.x URL cross-site scripting (ID 4355) CDR code-server up to 3.11.x URL cross-site scripting (ID 4355) A vulnerability was found in Review Board up to 3.0.20/4.0 RC1. It has been classified as problematic. Affected is an unknown function of the component. A vulnerability was found in Review Board up to 3.0.20/4.0 RC1. It has been classified as problematic. Affected is an unknown function of the component. A vulnerability is traded as CVE-2021-31330. It is possible to launch the attack remotely. There is no exploit available. Review Board up to 3.0.20/4.0 RC1. It has been classified as problematic. Affected is an unknown function of the component. A vulnerability was found in Micro Focus Net(Q Access Manager 4.5/5.0. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. Micro Focus Net(Q Access Manager 4.5/5.0. cross-site scripting. Micro Focus Net(Q Access Manager 4.5/5.0. cross-site scripting. Micro Focus Net(Q Access Manager 4.5/5.0. thas been classified as problematic. Affected with the attack remotely. There is no exploit available. Wilco Focus Net(Q Access Manager 4.5/5.0. thas been classified as problematic. Affected was found in the attack remotely. There is no exploit available. Wilco Focus Net(Q Access Manager 4.5/5.0. cross-site scripting. A vulnerability affects unknown code. The manipulation leads to cross-site scripting. A vulnerability affects unknown code. The manipulation leads to cross-site scripting attack. Protected by Voce Rules Cross-site scripting. Detected by Voce Rules Cross-site scripting. A vulnerability affects unknown code. The manipulation leads to cross-site scri			problematic, has been found in Survey Sparrow Enterprise Survey Software 2022. This issue affects some unknown processing. The manipulation of the argument Signup leads to cross-site	by Core	scanner as cross-site scripting
A vulnerability was found in CDR codeserver up to 3.11.x. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component URL Handler. The manipulation leads to cross-site scripting. CDR code-server up to 3.11.x. URL cross-site scripting. This vulnerability is known as CVE-2021-42648. The attack can be launched remotely. There is no exploit available. CVE-2021-42648 CVE-2021-42648 CVE-2021-42648 CVE-2021-43640 CVE-2021-43640 Review Board up to 3.0.20/4.0 RC1. It has been classified as problematic. Affected is an unknown function of the component Markdown Handler. The manipulation leads to cross-site scripting. Review Board up to 3.0.20/4.0 RC1. It has been classified as problematic. Affected is an unknown function of the component Markdown Handler. The manipulation leads to cross-site scripting. Review Board up to 3.0.20/4.0 RC1. It has been classified as problematic. Affected is an unknown function of the component Markdown Handler. The manipulation leads to cross-site scripting. Review Board up to 3.0.20/4.0 RC1. It has been classified as problematic. Affected by Core Rules Review Board up to 3.0.20/4.0 RC1. It has been classified as problematic. Affected by Core NettQ Access Manager 4.5/5.0. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. Micro Focus NettQ Access Manager 4.5/5.0 cross-site scripting Micro Focus NettQ Access Manager 4.5/5.0 cross-site scripting attack This vulnerability is traded as CVE-2021-22531. It is possible to launch the attack remotely. There is no exploit available. A vulnerability classified as problematic was found in th23 Social Plugin up to 1.2.0. This vulnerability affects unknown code. The manipulation leads to cross-site scripting attack This vulnerability affects unknown code. The manipulation leads to cross-site scripting attack	CVE 2022 20727	Survey Software 2022	CVE-2022-29727. The attack may be initiated remotely. There is no exploit		
CVE-2021-42648 Processing (ID 4355) CDR code-server up to 3.11.x URL cross-site scripting (ID 4355) EVE-2021-42648 Scripting (ID 4355) A vulnerability was found in Review Board up to 3.0.20/4.0 RC1. It has been classified as problematic. Affected is an unknown function of the component Markdown Handler. The manipulation leads to cross-site scripting. Review Board up to 3.0.20/4.0 RC1 was found in Micro Focus NetIQ Access Manager 4.5/5.0 cross-site scripting attack Micro Focus NetIQ Access Manager 4.5/5.0 cross-site scripting attack Which are the manipulation leads to cross-site scripting. Micro Focus NetIQ Access Manager 4.5/5.0 cross-site scripting attack A vulnerability is traded as CVE-2021- been classified as problematic. Affected by Core scanner as cross-site scripting. A vulnerability was found in Micro Focus NetIQ Access Manager 4.5/5.0 thas been classified as problematic. Affected by Core scanner as cross-site scripting. Micro Focus NetIQ Access Manager 4.5/5.0 cross-site scripting attack A vulnerability is traded as CVE-2021- 22531. It is possible to launch the attack remotely. There is no exploit available. A vulnerability is traded as CVE-2021- 22531. It is possible to launch the attack remotely. There is no exploit available. A vulnerability dassified as problematic Affected by Core scanner as cross-site scripting attack Will be a vulnerability is traded as CVE-2021- 22531. It is possible to launch the attack remotely. There is no exploit available. A vulnerability affects unknown code. The manipulation leads to cross- site scripting attack Detected by Core scanner as cross-site scripting.	CVE-2022-29721	signup cross-site scripting	A vulnerability was found in CDR code- server up to 3.11.x. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component URL Handler. The	by Core	scanner as cross-site scripting
A vulnerability is traded as CVE-2021-31330 It is recommended to upgrade the affected component. A vulnerability was found in Review Board up to 3.0.20/4.0 RC1. It has been classified as problematic. Affected is an unknown function of the component Markdown Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2021-31330. It is possible to launch the attack remotely. There is no exploit available. Review Board up to 3.0.20/4.0 RC1 Markdown cross-site scripting. It is recommended to upgrade the affected component. A vulnerability was found in Micro Focus NetlQ Access Manager 4.5/5.0. It has been classified as problematic. Affected Rules Rules Cross-site scripting Rules Cross-site scripting Scripting A vulnerability is traded as CVE-2021-31330 There is no exploit available. Protected by Core scanner as been classified as problematic. Affected Rules Cross-site Scripting A vulnerability is traded as CVE-2021-3134 Rules Cross-site Scripting A vulnerability is traded as CVE-2021-3134 Scripting A vulnerability classified as problematic Protected Detected by Core Creative CVE-2021-22531 There is no exploit available. A vulnerability classified as problematic Protected Detected by Core Creative CVE-2021-3134 Scripting A vulnerability classified as problematic Protected Detected Detected Detected CVE-2021-3134 Scripting Cross-site CVE-2021-3135			42648. The attack can be launched		
Board up to 3.0.20/4.0 RC1. It has been classified as problematic. Affected is an unknown function of the component Markdown Handler. The manipulation leads to cross-site scripting. Review Board up to 3.0.20/4.0 RC1 Markdown It is recommended to upgrade the affected component. A vulnerability as found in Micro Focus NetlQ Access Manager 4.5/5.0 cross-site is an unknown function. The manipulation leads to cross-site scripting. Micro Focus NetlQ Access Manager 4.5/5.0 cross-site scripting attack Micro Focus NetlQ Access Manager 4.5/5.0 cross-site scripting attack This vulnerability is traded as CVE-2021-31330. It is possible to launch the attack remotely. There is no exploit available. Protected by by Core scanner as been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. Micro Focus NetlQ Access Manager 4.5/5.0 cross-site scripting. A vulnerability is traded as CVE-2021-4 scripting. A vulnerability is traded as CVE-2021-4 scripting. A vulnerability affects unknown code. The manipulation leads to cross-site scripting attack Protected by scanner as 1.2.0. This vulnerability affects unknown code. The manipulation leads to cross-site scripting attack	CVE-2021-42648	3.11.x URL cross-site	, -		
Review Board up to 3.0.20/4.0 RC1 Markdown cross-site scripting A vulnerability was found in Micro Focus NetlQ Access Manager 4.5/5.0. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting Micro Focus NetlQ Access Manager 4.5/5.0 trips wilnerability is traded as CVE-2021-Manager 4.5/5.0 cross-site A vulnerability is traded as CVE-2021-Manager 4.5/5.0 cross-site A vulnerability is traded as CVE-2021-Manager 4.5/5.0 cross-site A vulnerability classified as problematic was found in th23 Social Plugin up to 1.2.0. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. A vulnerability affects unknown code. The manipulation leads to cross-site scripting attack			Board up to 3.0.20/4.0 RC1. It has been classified as problematic. Affected is an unknown function of the component Markdown Handler. The manipulation	by Core	scanner as cross-site scripting
Review Board up to 3.0.20/4.0 RC1 Markdown cross-site scripting affected component. A vulnerability was found in Micro Focus NetlQ Access Manager 4.5/5.0. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. Micro Focus NetlQ Access Manager 4.5/5.0 it has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. Micro Focus NetlQ Access Manager 4.5/5.0 cross-site is an unknown function. The manipulation leads to cross-site scripting. Micro Focus NetlQ Access Manager 4.5/5.0 cross-site is an unknown function. The manipulation leads to cross-site scripting. A vulnerability is traded as CVE-2021-22531. It is possible to launch the attack remotely. There is no exploit available. A vulnerability classified as problematic was found in th23 Social Plugin up to 1.2.0. This vulnerability affects unknown code. The manipulation leads to cross-site scripting site scripting.	CVE-2021-31330		31330. It is possible to launch the attack		
A vulnerability was found in Micro Focus Protected Detected by NetIQ Access Manager 4.5/5.0. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. Micro Focus NetIQ Access Manager 4.5/5.0 cross-site scripting. Micro Focus NetIQ Access Manager 4.5/5.0 cross-site scripting. Micro Focus NetIQ Access Manager 4.5/5.0 cross-site scripting. This vulnerability is traded as CVE-2021-22531. It is possible to launch the attack remotely. There is no exploit available. A vulnerability classified as problematic Protected Detected by was found in th23 Social Plugin up to by Core scanner as 1.2.0. This vulnerability affects unknown Rules cross-site code. The manipulation leads to cross-scripting site scripting.		3.0.20/4.0 RC1 Markdown	It is recommended to upgrade the		
Manager 4.5/5.0 cross-site scripting 22531. It is possible to launch the attack remotely. There is no exploit available. A vulnerability classified as problematic was found in th23 Social Plugin up to by Core scanner as 1.2.0. This vulnerability affects unknown code. The manipulation leads to cross-site stripting. th23 Social Plugin up to 1.2.0 on WordPress cross-		·	A vulnerability was found in Micro Focus NetIQ Access Manager 4.5/5.0. It has been classified as problematic. Affected is an unknown function. The	by Core	scanner as cross-site scripting
A vulnerability classified as problematic Protected Detected by was found in th23 Social Plugin up to by Core scanner as 1.2.0. This vulnerability affects unknown Rules cross-site code. The manipulation leads to cross-scripting site scripting. 1.2.0 on WordPress cross-	CVF-2021-22531	Manager 4.5/5.0 cross-site	22531. It is possible to launch the attack		
1.2.0 on WordPress cross-		r - U	A vulnerability classified as problematic was found in th23 Social Plugin up to 1.2.0. This vulnerability affects unknown code. The manipulation leads to cross-	by Core	scanner as cross-site scripting
	CVE-2022-1062	1.2.0 on WordPress cross-			attack



		1062. The attack can be initiated remotely. There is no exploit available.		
		A vulnerability was found in Advanced Image Sitemap Plugin up to 1.2. It has been rated as problematic. This issue affects some unknown processing of the component Admin Page. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1216	Advanced Image Sitemap Plugin up to 1.2 on WordPress Admin Page cross-site scripting	The identification of this vulnerability is CVE-2022-1216. The attack may be initiated remotely. There is no exploit available.		
		A vulnerability has been found in Clipr Plugin up to 1.2.3 and classified as problematic. This vulnerability affects unknown code of the component API Key Setting Handler. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1559	Clipr Plugin up to 1.2.3 on WordPress API Key Setting cross-site scripting	This vulnerability was named CVE-2022- 1559. The attack can be initiated remotely. There is no exploit available.		
		A vulnerability was found in VikBooking Hotel Booking Engine & PMS Plugin up to 1.5.7. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
	VikBooking Hotel Booking Engine & PMS Plugin up to	The identification of this vulnerability is CVE-2022-1408. The attack may be initiated remotely. There is no exploit available.		
CVE-2022-1408	1.5.7 on WordPress cross- site scripting	It is recommended to upgrade the affected component.		
		A vulnerability, which was classified as problematic, has been found in bootstrap-table up to 1.20.1. This issue affects some unknown processing of the component Table Export Plug-In. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
		The identification of this vulnerability is CVE-2022-1726. The attack may be initiated remotely. There is no exploit available.		
CVE-2022-1726	bootstrap-table up to 1.20.1 Table Export Plug-In cross-site scripting	It is recommended to upgrade the affected component.		
CVE-2022-1465	WPC Smart Wishlist for WooCommerce Plugin up	A vulnerability has been found in WPC Smart Wishlist for WooCommerce Plugin up to 2.9.8 and classified as problematic.	Protected by Core Rules	Detected by scanner as cross-site



	to 2.9.8 on WordPress AJAX Action cross-site scripting	This vulnerability affects unknown code of the component AJAX Action Handler. The manipulation leads to cross-site scripting.		scripting attack
		This vulnerability was named CVE-2022- 1465. The attack can be initiated remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		
		A vulnerability has been found in Admin Menu Editor Plugin up to 1.0.4 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1726	Admin Menu Editor Plugin up to 1.0.4 on WordPress cross-site scripting	This vulnerability was named CVE-2022-0625. The attack can be initiated remotely. There is no exploit available.		
		A vulnerability was found in WP YouTube Live Plugin up to 1.8.2 and classified as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
	WP YouTube Live Plugin up	This vulnerability is handled as CVE-2022-1334. The attack may be launched remotely. There is no exploit available.		
CVE-2022-1334	to 1.8.2 on WordPress Setting cross-site scripting	It is recommended to upgrade the affected component.		
		A vulnerability, which was classified as problematic, was found in WPQA Builder Plugin Plugin up to 5.1. This affects an unknown part. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
		This vulnerability is uniquely identified as CVE-2022-1051. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-1051	WPQA Builder Plugin Plugin up to 5.1 on WordPress cross-site scripting	It is recommended to upgrade the affected component.		
	, 3	A vulnerability, which was classified as problematic, was found in BulletProof Security Plugin up to 6.0. Affected is an	Protected by Core Rules	Detected by scanner as cross-site
CVE-2022-1265	BulletProof Security Plugin up to 6.0 CAPTCHA Setting cross-site scripting	unknown function of the component CAPTCHA Setting Handler. The manipulation leads to cross-site scripting.		scripting attack



-				
		This vulnerability is traded as CVE-2022-		
		1265. It is possible to launch the attack		
		remotely. There is no exploit available.		
		It is recommended to upgrade the		
		affected component.		
		A vulnerability classified as problematic	Protected	Detected by
		was found in WPCargo Track & Trace	by Core	scanner as
		Plugin up to 6.9.4. Affected by this	Rules	cross-site
		vulnerability is an unknown functionality.		scripting
		The manipulation of the argument		attack
		wpcargo_tracking_number leads to		
		cross-site scripting.		
		This vulnerability is known as CVE-2022-		
	WPCargo Track & Trace	1436. The attack can be launched		
	Plugin up to 6.9.4 on	remotely. There is no exploit available.		
	WordPress			
	wpcargo_tracking_number	It is recommended to upgrade the		
CVE-2022-1436	cross-site scripting	affected component.		
		A vulnerability classified as problematic	Protected	Detected by
		has been found in Gmedia Photo Gallery	by Core	scanner as
		Plugin up to 1.19.x. This affects an unknown part of the component Album	Rules	cross-site scripting
		Name Handler. The manipulation leads		attack
		to cross-site scripting.		attack
		This vulnerability is uniquely identified as		
		CVE-2022-0873. It is possible to initiate		
		the attack remotely. There is no exploit		
	Gmedia Photo Gallery	available.		
	Plugin up to 1.19.x on			
CVE-2022-0873	WordPress Album Name cross-site scripting	It is recommended to upgrade the affected component.		
CVL-2022-0873	cross-site scripting	A vulnerability classified as problematic	Protected	Detected by
		has been found in Custom TinyMCE	by Core	scanner as
		Shortcode Button Plugin up to 1.1.	Rules	cross-site
		Affected is an unknown function. The		scripting
		manipulation leads to cross-site scripting.		attack
	Custom TinyMCE Shortcode			
	Button Plugin up to 1.1 on	This vulnerability is traded as CVE-2022-		
CVE 2022 1217	WordPress cross-site	1217. It is possible to launch the attack		
CVE-2022-1217	scripting	remotely. There is no exploit available. A vulnerability classified as problematic	Protected	Detected by
		has been found in WPCargo Track &	by Core	scanner as
		Trace Plugin up to 6.9.4. Affected is an	Rules	cross-site
		unknown function of the component		scripting
		Setting Handler. The manipulation leads		attack
		to cross-site scripting.		
	WPCargo Track & Trace			
	Plugin up to 6.9.4 on	This vulnerability is traded as CVE-2022-		
CVE-2022-1435	WordPress Setting cross-	1435. It is possible to launch the attack		
	site scripting	remotely. There is no exploit available.		



		It is recommended to upgrade the		
		affected component. A vulnerability, which was classified as problematic, has been found in Call Now Button Plugin up to 1.1.1. Affected by this issue is some unknown functionality of the component Attribute Handler. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
	Call Now Button Plugin up to 1.1.1 on WordPress	This vulnerability is handled as CVE-2022-1455. The attack may be launched remotely. There is no exploit available.		
CVE-2022-1455	Attribute cross-site scripting	It is recommended to upgrade the affected component.		
		A vulnerability, which was classified as problematic, has been found in Bulk Edit and Create User Profiles Plugin up to 1.5.13. This issue affects some unknown processing of the component User Login. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
	Bulk Edit and Create User Profiles Plugin up to 1.5.13	The identification of this vulnerability is CVE-2022-1089. The attack may be initiated remotely. There is no exploit available.		
CVE-2022-1089	on WordPress User Login cross-site scripting	It is recommended to upgrade the affected component.		
CVE-2022-1089	Cross-site scripting	A vulnerability was found in WP Subtitle Plugin up to 3.4.0. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument wp_subtitle leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
	WP Subtitle Plugin up to 3.4.0 on WordPress	This vulnerability was named CVE-2022-1393. The attack can be initiated remotely. There is no exploit available.		
CVE-2022-1393	wp_subtitle cross-site scripting	It is recommended to upgrade the affected component.		
	ScrollReveal.js Effects	A vulnerability, which was classified as problematic, was found in ScrollReveal.js Effects Plugin up to 1.2. This affects an unknown part of the component Setting Handler. The manipulation leads to crosssite scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1512	Plugin up to 1.2 on WordPress Setting cross- site scripting	This vulnerability is uniquely identified as CVE-2022-1512. It is possible to initiate		



		the attack remotely. There is no exploit available.		
		A vulnerability was found in totaljs CMS 3.4.5. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component JavaScript Embedded PDF Handler. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-30013	totaljs CMS 3.4.5 JavaScript Embedded PDF cross-site scripting	This vulnerability is known as CVE-2022-30013. The attack can be launched remotely. There is no exploit available.		
CVE 2022 30013	Scripting	A vulnerability has been found in Gnuboard 5.55/5.56 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file bbs/member_confirm.php. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-30050	Gnuboard 5.55/5.56 bbs/member_confirm.php cross-site scripting	This vulnerability is known as CVE-2022- 30050. The attack can be launched remotely. There is no exploit available.		
		A vulnerability classified as problematic has been found in atmail 6.5.0. This affects an unknown part of the file index.php/admin/index/. The manipulation of the argument error leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-30776	atmail 6.5.0 index.php/admin/index/ error cross-site scripting	This vulnerability is uniquely identified as CVE-2022-30776. It is possible to initiate the attack remotely. There is no exploit available.		
		A vulnerability, which was classified as problematic, has been found in IPPlan 4.92b. This issue affects some unknown processing of the file admin/usermanager.php. The manipulation of the argument userid leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2021-42943	IPPlan 4.92b admin/usermanager.php userid cross-site scripting	The identification of this vulnerability is CVE-2021-42943. The attack may be initiated remotely. There is no exploit available.		
	. 3	A vulnerability was found in Random String Parameter Plugin up to 1.0. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-30966	Random String Parameter Plugin up to 1.0 on Jenkins cross-site scripting	This vulnerability is uniquely identified as CVE-2022-30966. It is possible to initiate		



		the attack remotely. There is no exploit available.		
		A vulnerability classified as problematic was found in Autocomplete Parameter Plugin up to 1.1. This vulnerability affects unknown code. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-30961	Autocomplete Parameter Plugin up to 1.1 on Jenkins cross-site scripting	This vulnerability was named CVE-2022-30961. The attack can be initiated remotely. There is no exploit available.		
		A vulnerability was found in Rundeck Plugin up to 3.6.10. It has been rated as problematic. This issue affects some unknown processing of the component Webhook Submission Handler. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-30956	Rundeck Plugin up to 3.6.10 on Jenkins Webhook Submission cross-site scripting	The identification of this vulnerability is CVE-2022-30956. The attack may be initiated remotely. There is no exploit available.		
		A vulnerability, which was classified as problematic, was found in OctoPrint up to 1.7.x. Affected is an unknown function. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
		This vulnerability is traded as CVE-2022-1432. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2022-1432	OctoPrint up to 1.7.x cross- site scripting	It is recommended to upgrade the affected component.		
		A vulnerability has been found in erudika para up to 1.45.10 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
		This vulnerability is known as CVE-2022- 1782. The attack can be launched remotely. There is no exploit available.		
CVE-2022-1782	erudika para up to 1.45.10 cross-site scripting	It is recommended to upgrade the affected component.		
		A vulnerability, which was classified as problematic, has been found in OctoPrint up to 1.7.x. This issue affects some unknown processing. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1430	OctoPrint up to 1.7.x cross- site scripting	The identification of this vulnerability is		



CVE-2022-1806 CVE-2022-1806 RTX cross-site scripting CVE-2022-28959 SPIP up to 3.1.13 /spip.php The instruction apply a patch to fix A vulnerability is unjuerability is commended to upgrade the affected component. A vulnerability is mount in RTX. This affects an unknown part. The manipulation leads to cross-site scripting. A vulnerability is unjuerability as munknown part. The manipulation leads to cross-site scripting. A vulnerability is unjuerability is unjuerability is unjuerable to initiate the attack remotely. There is no exploit available. CVE-2022-1806 RTX cross-site scripting SPIP up to 3.1.13 /spip.php The identification of this vulnerability is CVE-2022-28959 SPIP up to 3.1.13 /spip.php Tit is recommended to apply a patch to fix A vulnerability is complement. A vulnerability is unjuerability is unjuerability is component. A vulnerability is unjuerability is unjuera					
available. It is recommended to upgrade the affected component. A vulnerability classified as problematic was found in jgraph drawio up to 18.0.3. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability was found in Opal Hotel Room Booking Plugin up to 1.2.7 on WordPress cross-site scripting Opal Hotel Room Booking Plugin up to 1.2.7 on WordPress cross-site scripting A vulnerability is known as CVE-2022-29449 This vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. Opal Hotel Room Booking Plugin up to 1.2.7 on WordPress cross-site or remotely. There is no exploit available. CVE-2022-29449 This vulnerability is shown as CVE-2022-29449. The attack can be launched remotely. There is no exploit available. A vulnerability to shirt is a possible to initiate the attack remotely. There is no exploit available. CVE-2022-1806 RTX cross-site scripting A vulnerability is injudicely identified as CVE-2022-29449. The attack can be launched remotely. There is no exploit available. CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available attack This vulnerability is sundinguely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. The identification of this vulnerability is corressing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is corressing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is corressing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is corressing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is corressing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is corressing of the f			CVE-2022-1430. The attack may be		
It is recommended to upgrade the affected component. A vulnerability classified as problematic was found in jagraph drawiou pto 18.0.3. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting CVE-2022-1730 igraph drawiou up to 18.0.3 cross-site scripting A vulnerability is known as CVE-2022-1730. The attack can be launched remotely. There is no exploit available. CVE-2022-1806 RTX cross-site scripting			initiated remotely. There is no exploit		
affected component. A vulnerability classified as problematic was found in jgraph drawio up to 18.0.3. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-1730. The attack can be launched remotely. There is no exploit available. VE-2022-1730 This vulnerability is was found in Opal Hotel Room Booking Plugin up to 1.2.7 on Wordfress cross-site scripting. Opal Hotel Room Booking Plugin up to 1.2.7 on Wordfress cross-site VE-2022-29449 Opal Hotel Room Booking Plugin up to 1.2.7 on Wordfress cross-site CVE-2022-2949 Opal Hotel Room Booking Plugin up to 1.2.7 on Wordfress cross-site This vulnerability is known as CVE-2022-29449. The attack can be launched remotely. There is no exploit available. Opal Hotel Room Booking Plugin up to 1.2.7 on Wordfress cross-site This vulnerability is snown as CVE-2022-29449. The attack can be launched remotely. There is no exploit available. Opal Hotel Room Booking Plugin up to 1.2.8 on whom as CVE-2022-29449. The attack can be launched remotely. There is no exploit available. Opal Hotel Room Booking Plugin up to 1.2.8 on whom as CVE-2022-29449. The attack can be launched remotely. There is no exploit available. Opal Hotel Room Booking Plugin up to 1.2.8 on whom as CVE-2022-29449. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component. A vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component. A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is considered to protected by Core is canner as cripting attack.			available.		
affected component. A vulnerability classified as problematic was found in jgraph drawio up to 18.0.3. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-1730. The attack can be launched remotely. There is no exploit available. VE-2022-1730 This vulnerability is was found in Opal Hotel Room Booking Plugin up to 1.2.7 on Wordfress cross-site scripting. Opal Hotel Room Booking Plugin up to 1.2.7 on Wordfress cross-site VE-2022-29449 Opal Hotel Room Booking Plugin up to 1.2.7 on Wordfress cross-site CVE-2022-2949 Opal Hotel Room Booking Plugin up to 1.2.7 on Wordfress cross-site This vulnerability is known as CVE-2022-29449. The attack can be launched remotely. There is no exploit available. Opal Hotel Room Booking Plugin up to 1.2.7 on Wordfress cross-site This vulnerability is snown as CVE-2022-29449. The attack can be launched remotely. There is no exploit available. Opal Hotel Room Booking Plugin up to 1.2.8 on whom as CVE-2022-29449. The attack can be launched remotely. There is no exploit available. Opal Hotel Room Booking Plugin up to 1.2.8 on whom as CVE-2022-29449. The attack can be launched remotely. There is no exploit available. Opal Hotel Room Booking Plugin up to 1.2.8 on whom as CVE-2022-29449. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component. A vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component. A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is considered to protected by Core is canner as cripting attack.					
A vulnerability classified as problematic was found in graph drawio up to 18.03. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting This vulnerability is known as CVE-2022- 1730. The attack can be launched remotely. There is no exploit available. VE-2022-1730 Qpal Hotel Room Booking Plugin up to 1.2.7 on WordPress cross-site scripting Opal Hotel Room Booking Plugin up to 1.2.7 on WordPress cross-site scripting CVE-2022-29449 This vulnerability is known as CVE-2022- 29449. The attack can be launched remotely. There is no exploit available. CVE-2022-1806 RTX cross-site scripting Rules Rules Protected by this vulnerability is known as CVE-2022- 29449. The attack can be launched remotely. There is no exploit available. A vulnerability is known as CVE-2022- 29449. The attack can be launched remotely. There is no exploit available. A vulnerability is known as CVE-2022- 29449. The attack can be launched remotely. There is no exploit available. This vulnerability is known as CVE-2022- 29449. The attack can be launched remotely. There is no exploit available. Protected by Core Rules CVE-2022-1806 RTX cross-site scripting Rules This vulnerability is uniquely identified as CVE-2022- 2022-1806. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component. A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is cross-site scripting.			It is recommended to upgrade the		
was found in jigraph drawio up to 18.0.3. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-1730. The attack can be launched remotely. There is no exploit available. CVE-2022-1730 jgraph drawio up to 18.0.3 tis recommended to upgrade the affected component. Protected by Core Scanner as CVE-2022-1730. The attack can be launched remotely. There is no exploit available. Protected by Core Scanner as CVE-2022-1730. The attack can be applied by Core Scanner as CVE-2022-1730. Protected Scripting Scriptin			•		
Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. Igraph drawlo up to 18.0.3 It is recommended to upgrade the affected component.			A vulnerability classified as problematic	Protected	Detected by
unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-1730. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component. A vulnerability was found in Opal Hotel Room Booking Plugin up to 1.2.7 it has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. Opal Hotel Room Booking Plugin up to 1.2.7 on WordPress cross-site scripting. Opal Hotel Room Booking Plugin up to 1.2.7 on WordPress cross-site scripting. This vulnerability is known as CVE-2022-29449. This vulnerability is known as CVE-2022-29449. The attack can be launched remotely. There is no exploit available. Over-2022-29449. The attack can be launched remotely. There is no exploit available. This vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. This vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. The identification of this vulnerability is CVE-2022-1806. The manipulation leads to cross-site scripting. The identification of this vulnerability is component. The iden				by Core	scanner as
leads to cross-site scripting. attack			· · · · · · · · · · · · · · · · · · ·	Rules	
This vulnerability is known as CVE-2022- 1730. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component. A vulnerability was found in Opal Hotel Room Booking Plugin up to 1.2.7. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. Opal Hotel Room Booking Plugin up to 1.2.7 on WordPress cross-site CVE-2022-29449 scripting Opal Hotel Room Booking Plugin up to 1.2.7 on WordPress cross-site Scripting A vulnerability is known as CVE-2022- 29449. The attack can be launched remotely. There is no exploit available. A vulnerability dassified as problematic. This cross-site scripting attack CVE-2022-1806 RTX cross-site scripting RTX cross-site scripting This vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. RTX cross-site scripting This vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28999. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix			·		
1730. The attack can be launched remotely. There is no exploit available.			leads to cross-site scripting.		attack
1730. The attack can be launched remotely. There is no exploit available.					
This vulnerability is no exploit available. Protected by Core coress-site scripting					
igraph drawio up to 18.0.3 It is recommended to upgrade the affected component.					
CVE-2022-1730 cross-site scripting affected component. A vulnerability was found in Opal Hotel Room Booking Plugin up to 1.2.7. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. Opal Hotel Room Booking Plugin up to 1.2.7 on WordPress cross-site scripting. CVE-2022-29449 This vulnerability is known as CVE-2022-29449. The attack can be launched remotely. There is no exploit available. CVE-2022-1806 RTX cross-site scripting CVE-2022-1806 RTX cross-site scripting A vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. CVE-2022-1806 RTX cross-site scripting RTX cross-site scripting A vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. CVE-2022-1806 RTX cross-site scripting RTX cross-site scripting A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is cross-site scripting attack SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix			remotely. There is no exploit available.		
CVE-2022-1730 cross-site scripting affected component. A vulnerability was found in Opal Hotel Room Booking Plugin up to 1.2.7. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. Opal Hotel Room Booking Plugin up to 1.2.7 on WordPress cross-site scripting. CVE-2022-29449 This vulnerability is known as CVE-2022-29449. The attack can be launched remotely. There is no exploit available. CVE-2022-1806 RTX cross-site scripting CVE-2022-1806 RTX cross-site scripting A vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. CVE-2022-1806 RTX cross-site scripting RTX cross-site scripting A vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. CVE-2022-1806 RTX cross-site scripting RTX cross-site scripting A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is cross-site scripting attack SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix		igraph drawio un to 18 0 3	It is recommended to ungrade the		
A vulnerability was found in Opal Hotel Room Booking Plugin up to 1.2.7. It has been declared as problematic. Affected by Core functionality. The manipulation leads to cross-site scripting. Opal Hotel Room Booking Plugin up to 1.2.7 on WordPress cross-site scripting. Opal Hotel Room Booking Plugin up to 1.2.7 on WordPress cross-site scripting. Opal Hotel Room Booking Plugin up to 1.2.7 on WordPress cross-site scripting. A vulnerability is known as CVE-2022-29449 This vulnerability classified as problematic has been found in RTX. This affects an unknown part. The manipulation leads to cross-site scripting. A vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. This vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects occupantly and affected components of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix	CVE-2022-1730				
Room Booking Plugin up to 1.2.7. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. Opal Hotel Room Booking Plugin up to 1.2.7 on WordPress cross-site 29449. The attack can be launched remotely. There is no exploit available. A vulnerability is known as CVE-2022-29449. The attack can be launched remotely. There is no exploit available. A vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. CVE-2022-1806 RTX cross-site scripting RTX		от от от тр. т. в	·	Protected	Detected by
by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. Opal Hotel Room Booking Plugin up to 1.2.7 on WordPress cross-site 29449. The attack can be launched remotely. There is no exploit available. CVE-2022-29449 CVE-2022-1806 RTX cross-site scripting Detected by Scanner as cross-site the attack remotely. There is no exploit available. CVE-2022-1806 RTX cross-site scripting RTX cross-site scripting SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix Vision and the manipulation leads to cross-site scripting. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix VE second attack SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix				by Core	· · · · · · · · · · · · · · · · · · ·
functionality. The manipulation leads to cross-site scripting. Opal Hotel Room Booking Plugin up to 1.2.7 on WordPress cross-site scripting OVE-2022-29449 This vulnerability is known as CVE-2022-29449. The attack can be launched remotely. There is no exploit available. A vulnerability classified as problematic has been found in RTX. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component. A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13/spip.php It is recommended to apply a patch to fix			been declared as problematic. Affected	Rules	cross-site
CVE-2022-29449 CVE-2022-29449 This vulnerability is known as CVE-2022-29449 This vulnerability classified as problematic has been found in RTX. This affects an unknown part. The manipulation leads to cross-site scripting. A vulnerability classified as problematic has been found in RTX. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. EVE-2022-1806 RTX cross-site scripting RTX cross-site scripting A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix			by this vulnerability is an unknown		scripting
Opal Hotel Room Booking Plugin up to 1.2.7 on WordPress cross-site 29449. The attack can be launched remotely. There is no exploit available. A vulnerability classified as problematic has been found in RTX. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. RTX cross-site scripting Rules CVE-2022-1806 by Core Rules CVE-2022-1806 by Core Rules CVE-2022-28959. The manipulation Rules CVE-2022-28959. The attack may be initiated remotely. There is no exploit available.			functionality. The manipulation leads to		attack
This vulnerability is known as CVE-2022- 29449. The attack can be launched remotely. There is no exploit available. A vulnerability classified as problematic has been found in RTX. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. CVE-2022-1806 RTX cross-site scripting RTX cross-site scr			cross-site scripting.		
WordPress cross-site scripting 29449. The attack can be launched remotely. There is no exploit available. A vulnerability classified as problematic has been found in RTX. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. CVE-2022-1806 RTX cross-site scripting RTX cross-site scripting It is recommended to upgrade the affected component. A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix		Opal Hotel Room Booking			
CVE-2022-29449 scripting remotely. There is no exploit available. A vulnerability classified as problematic has been found in RTX. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component. A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix			*		
A vulnerability classified as problematic has been found in RTX. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component. A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix					
has been found in RTX. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component. A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix	CVE-2022-29449	scripting			- · · · · · · · · · · · · · · · · · · ·
unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component. A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13/spip.php It is recommended to apply a patch to fix					· ·
cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component. A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13/spip.php It is recommended to apply a patch to fix				-	
This vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component. A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix				Rules	
This vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component. A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix			cross-site scripting.		
CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component. A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix			This vulnerability is uniquely identified as		attack
the attack remotely. There is no exploit available. It is recommended to upgrade the affected component. A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13/spip.php It is recommended to apply a patch to fix					
available. It is recommended to upgrade the affected component. A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix			·		
CVE-2022-1806 RTX cross-site scripting affected component. A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix					
CVE-2022-1806 RTX cross-site scripting affected component. A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix					
A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This by Core scanner as issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix			It is recommended to upgrade the		
3.1.13 and classified as problematic. This by Core scanner as issue affects some unknown processing of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix	CVE-2022-1806	RTX cross-site scripting	· · · · · · · · · · · · · · · · · · ·		
issue affects some unknown processing Rules cross-site of the file /spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix				Protected	Detected by
of the file /spip.php. The manipulation scripting leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix				•	scanner as
leads to cross-site scripting. attack The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix				Rules	
The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix					
CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix			leads to cross-site scripting.		attack
CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix			The identification of this code contilled		
initiated remotely. There is no exploit available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix					
available. SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix					
SPIP up to 3.1.13 /spip.php It is recommended to apply a patch to fix					
		SPIP up to 3.1.13 /spip.php	It is recommended to apply a patch to fix		
	CVE-2022-28959				



		A vulnerability was found in Proton 0.2.0 and classified as problematic. This issue affects some unknown processing of the component Markdown File Handler. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-25224	Proton 0.2.0 Markdown File cross-site scripting	The identification of this vulnerability is CVE-2022-25224. The attack may be initiated remotely. There is no exploit available.		
		A vulnerability was found in GoCD up to 21.3.x and classified as problematic. This issue affects some unknown processing of the component Pipeline Comparison Error Handler. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
	GoCD up to 21.3.x Pipeline Comparison Error cross-site	The identification of this vulnerability is CVE-2022-29183. The attack may be initiated remotely. There is no exploit available.		
CVE-2022-29183	scripting (GHSA-3vvq-q4qv- x2gf)	It is recommended to upgrade the affected component.		
	Wham Checkout Files	A vulnerability was found in Wham Checkout Files Upload for WooCommerce Plugin up to 2.1.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-29425	Upload for WooCommerce Plugin up to 2.1.2 on WordPress cross-site scripting	This vulnerability is known as CVE-2022-29425. The attack can be launched remotely. There is no exploit available.		
CVE 2022 23423	Scripting	A vulnerability was found in ibericode MC4WP Plugin up to 4.8.6 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2021-36833	ibericode MC4WP Plugin up to 4.8.6 on WordPress cross-site scripting	This vulnerability is handled as CVE-2021-36833. The attack may be launched remotely. There is no exploit available.		
		A vulnerability has been found in KubiQ PNG to JPG Plugin up to 4.0 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument jpg_quality leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-29430	KubiQ PNG to JPG Plugin up to 4.0 on WordPress jpg_quality cross-site scripting	This vulnerability was named CVE-2022-29430. The attack can be initiated remotely. There is no exploit available.		



		A vulnerability was found in 2J Image Slider Plugin up to 1.3.54. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-29426	2J Image Slider Plugin up to 1.3.54 on WordPress cross- site scripting	This vulnerability was named CVE-2022- 29426. The attack can be initiated remotely. There is no exploit available.		
		A vulnerability was found in Biplob Adhikari Image Hover Effects Ultimate Plugin up to 9.7.1. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-29424	Biplob Adhikari Image Hover Effects Ultimate Plugin up to 9.7.1 on WordPress cross-site scripting	This vulnerability is uniquely identified as CVE-2022-29424. It is possible to initiate the attack remotely. There is no exploit available.		
		A vulnerability classified as problematic has been found in Muneeb WP Slider Plugin up to 1.4.5. Affected is an unknown function. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-29428	Muneeb WP Slider Plugin up to 1.4.5 on WordPress cross-site scripting	This vulnerability is traded as CVE-2022-29428. It is possible to launch the attack remotely. There is no exploit available.		
		A vulnerability, which was classified as problematic, has been found in TMS-Plugins wpDataTables Plugin up to 2.1.27. Affected by this issue is some unknown functionality. The manipulation of the argument data-link-text/data-link-url/data/data-shortcode/data-star-num leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-29432	TMS-Plugins wpDataTables Plugin up to 2.1.27 on WordPress cross-site scripting	This vulnerability is handled as CVE-2022-29432. The attack may be launched remotely. There is no exploit available.		
	Zoo Management System	A vulnerability, which was classified as problematic, has been found in Zoo Management System 1.0. Affected by this issue is some unknown functionality of the file /zoo/admin/public_html/view_accounts? type=zookeeper of the component Content Module. The manipulation of the argument admin_name with the	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1816	1.0 Content Module view_accounts admin_name cross-site scripting	input <script>alert(1)</script> leads to cross-site scripting. This vulnerability is handled as CVE-2022-		



		1816. The attack may be launched remotely. Furthermore, there is an exploit available.			
		A vulnerability, which was classified as problematic, has been found in Donate Extra Plugin up to 2.02. This issue affects some unknown processing. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack	
CVE-2022-1268	Donate Extra Plugin up to 2.02 on WordPress crosssite scripting	The identification of this vulnerability is CVE-2022-1268. The attack may be initiated remotely. There is no exploit available.			
	· Ū	A vulnerability, which was classified as problematic, was found in Badminton Center Management System. This affects an unknown part of the file /bcms/admin/?page=user/list of the component Userlist Module. The manipulation of the argument username with the input	1 leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1817	Badminton Center Management System Userlist Module username cross-site scripting	This vulnerability is uniquely identified as CVE-2022-1817. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.			
		A vulnerability was found in WP Meta SEO Plugin up to 4.4.6. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Breadcrumb Separator Handler. The manipulation leads to crosssite scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack	
	WP Meta SEO Plugin up to 4.4.6 on WordPress	This vulnerability is known as CVE-2022-1093. The attack can be launched remotely. There is no exploit available.			
CVE-2022-1093	Breadcrumb Separator cross-site scripting	It is recommended to upgrade the affected component.			
CVL 2022-1073	cross site surpting	A vulnerability has been found in XML Sitemap Generator for Google Plugin up to 2.0.3 and classified as problematic. This vulnerability affects unknown code of the component Error Message Handler. The manipulation leads to cross- site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack	
CVE-2022-0346	XML Sitemap Generator for Google Plugin up to 2.0.3 on WordPress Error Message cross-site scripting	This vulnerability was named CVE-2022-0346. The attack can be initiated remotely. There is no exploit available.			



		It is recommended to upgrade the affected component.		
		A vulnerability classified as problematic was found in Gwyn's Imagemap Selector Plugin up to 0.3.3. This vulnerability affects unknown code of the component Attribute Handler. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1221	Gwyn's Imagemap Selector Plugin up to 0.3.3 on WordPress Attribute cross- site scripting	This vulnerability was named CVE-2022- 1221. The attack can be initiated remotely. There is no exploit available.		
		A vulnerability classified as problematic has been found in Domain Replace Plugin up to 1.3.8. This affects an unknown part of the component Admin Page. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1218	Domain Replace Plugin up to 1.3.8 on WordPress Admin Page cross-site scripting	This vulnerability is uniquely identified as CVE-2022-1218. It is possible to initiate the attack remotely. There is no exploit available.		
		A vulnerability has been found in Sliderby10Web Plugin up to 1.2.51 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
		This vulnerability is known as CVE-2022- 1320. The attack can be launched remotely. There is no exploit available.		
CVE-2022-1320	Sliderby10Web Plugin up to 1.2.51 on WordPress Setting cross-site scripting	It is recommended to upgrade the affected component.		
		A vulnerability was found in Turn Off All Comments Plugin up to 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Admin Page. The manipulation of the argument rows leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
	Turn Off All Comments Plugin up to 1.0 on WordPress Admin Page	This vulnerability is handled as CVE-2022- 1192. The attack may be launched		
CVE-2022-1192	rows cross-site scripting	remotely. There is no exploit available. A vulnerability was found in Curtain Plugin up to 1.0.2. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site	Protected by Core Rules	Detected by scanner as cross-site scripting
CVE-2022-1558	Curtain Plugin up to 1.0.2 on WordPress cross-site scripting	scripting. This vulnerability is uniquely identified as		attack
1000	··P····O	a		



		CVE-2022-1558. It is possible to initiate the attack remotely. There is no exploit available.		
		A vulnerability, which was classified as problematic, was found in collectiveaccess providence up to 1.7. This affects an unknown part. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
		This vulnerability is uniquely identified as CVE-2022-1825. It is possible to initiate the attack remotely. There is no exploit available.		
	collectiveaccess providence			
CVE-2022-1825	up to 1.7 cross-site scripting	It is recommended to upgrade the affected component.		
		A vulnerability, which was classified as problematic, was found in Tabs Plugin up to 2.2.7. Affected is an unknown function of the component Tab Description Handler. The manipulation leads to crosssite scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
	Tabs Plugin up to 2.2.7 on	This vulnerability is traded as CVE-2022-1298. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2022-1298	WordPress Tab Description cross-site scripting	It is recommended to upgrade the affected component.		
		A vulnerability was found in Check & Log Email Plugin up to 1.0.5 and classified as problematic. Affected by this issue is some unknown functionality of the component Admin Page. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
	Check & Log Email Plugin	This vulnerability is handled as CVE-2022-1547. The attack may be launched remotely. There is no exploit available.		
	up to 1.0.5 on WordPress Admin Page cross-site	It is recommended to upgrade the		
CVE-2022-1547	scripting	affected component.		
	Online Birth Certificate System 1.2	A vulnerability classified as problematic has been found in Online Birth Certificate System 1.2. Affected is an unknown function of the file /obcs/user/profile.php. The manipulation of the argument fname/lname leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-29005	/obcs/user/profile.php fname/lname cross-site scripting	This vulnerability is traded as CVE-2022-29005. It is possible to launch the attack remotely. There is no exploit available.		



	SourceCodester Rescue	A vulnerability, which was classified as problematic, has been found in SourceCodester Rescue Dispatch Management System 1.0. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
	Dispatch Management	This vulnerability is handled as CVE-2022-		
	System 1.0 cross-site	30017. The attack may be launched		
CVE-2022-30017	scripting	remotely. There is no exploit available.	Ductostad	Datastad b
		A vulnerability, which was classified as problematic, has been found in Home Clean Services Management System 1.0. This issue affects some unknown processing of the file register.php?link=registerand. The manipulation with the input <script>alert(1)</script> leads to cross-site scripting.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
	Home Clean Services	The identification of this vulnerability is		
CVE-2022-1840	Management System 1.0 register.php cross-site scripting	CVE-2022-1840. The attack may be initiated remotely. Furthermore, there is an exploit available.		
	P 0	A vulnerability was found in WonderCMS	Protected	Detected by
		3.4.1. It has been classified as problematic. Affected is an unknown function of the component Simple Blog Plugin. The manipulation leads to crosssite scripting.	by Core Rules	scanner as cross-site scripting attack
	WonderCMS 3.4.1 Simple Blog Plugin cross-site	This vulnerability is traded as CVE-2021-42233. It is possible to launch the attack		
CVE-2021-42233	scripting	remotely. There is no exploit available. A vulnerability, which was classified as	Protected	Dotoctod by
		problematic, was found in Student Information System 1.0. Affected is an unknown function of the file admin/?page=students of the component Student Roll Module. The manipulation with the input <script>alert(1)</script> leads to cross-site scripting.	by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1819	Student Information System 1.0 Student Roll Module admin/ cross-site scripting	This vulnerability is traded as CVE-2022-1819. It is possible to launch the attack remotely. Furthermore, there is an exploit available.		
	· · · · · · · · · · · · · · · · · ·	A vulnerability was found in SiteServer	Protected	Detected by
CVE 2024 42555	SiteServer CMS 6.15.51 cross-site scripting (ID	CMS 6.15.51. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads	by Core Rules	scanner as cross- site scripting
CVE-2021-42656	3238)	to cross-site scripting.		attack



		This vulnerability was named CVE-2021-		
		42656. The attack can be initiated		
		remotely. There is no exploit available.		
		A vulnerability has been found in Diary	Protected	Detected by
		Management System 1.0 and classified as	by Core	scanner as
		problematic. Affected by this	Rules	cross-site
		vulnerability is an unknown functionality	rtaics	scripting
		of the file search-result.php. The		attack
		manipulation of the argument Name		attack
		leads to cross-site scripting.		
		, ,		
	Diary Management System	This vulnerability is known as CVE-2022-		
	1.0 search-result.php Name	29004. The attack can be launched		
CVE-2022-29004	cross-site scripting	remotely. There is no exploit available.		
		A vulnerability, which was classified as	Protected	Detected by
		problematic, has been found in	by Core	scanner as
		Badminton Center Management System	Rules	cross-site
		1.0. This issue affects some unknown		scripting
		processing of the file		attack
		/bcms/classes/Master.php?f=save_court		
		_rental. The manipulation leads to cross-		
		site scripting.		
	Badminton Center	The identification of this vulnerability is		
	Management System 1.0	CVE-2022-30456. The attack may be		
	Master.php cross-site	initiated remotely. There is no exploit		
CVE-2022-30456	scripting	available.		
		A vulnerability was found in ZKEACMS	Protected	Detected by
		3.5.2. It has been rated as problematic.	by Core	scanner as
		This issue affects some unknown	Rules	cross-site
		processing of the file		scripting
		/navigation/create?ParentID=%23. The		attack
		manipulation of the argument ParentID		
		leads to cross-site scripting.		
		The identification of this vulnerability is		
	ZKEACMS 3.5.2 create	CVE-2022-29362. The attack may be		
	ParentID cross-site scripting	initiated remotely. There is no exploit		
CVE-2022-29362	(ID 457)	available.		
		A vulnerability was found in Covid-19	Protected	Detected b
		Travel Pass Management System 1.0. It	by Core	scanner as
		has been classified as problematic. This	Rules	cross-site
		affects an unknown part of the file		scripting
		/ctpms/classes/Users.php?f=save. The		attack
		manipulation of the argument firstname		
		leads to cross-site scripting.		
	Covid-19 Travel Pass	This vulnerability is uniquely identified as		
	Management System 1.0	CVE-2022-30842. It is possible to initiate		
	Users.php firstname cross-	the attack remotely. There is no exploit		
CVE-2022-30842	site scripting	available.		



		A vulnerability was found in Vsourz Digital Advanced Contact form 7 DB	Protected by Core	Detected by scanner as
		Plugin up to 1.8.7. It has been declared	Rules	cross-site
		as problematic. This vulnerability affects	Rules	scripting
		unknown code. The manipulation leads		attack
		to cross-site scripting.		
	Vsourz Digital Advanced	This was a sale little was a same of CV/F 2022		
	Contact form 7 DB Plugin	This vulnerability was named CVE-2022-		
CVE-2022-29408	up to 1.8.7 on WordPress cross-site scripting	29408. The attack can be initiated		
CVE-2022-29406	cross-site scripting	remotely. There is no exploit available. A vulnerability was found in VikBooking	Protected	Detected b
		Hotel Booking Engine & PMS Plugin up to	by Core	scanner as
		1.5.8 and classified as problematic.	Rules	cross-site
		Affected by this issue is some unknown	Rules	scripting
		functionality of the component URL		attack
		Handler. The manipulation leads to cross-		attack
		site scripting.		
		This vulnerability is handled as CVE-2022-		
		1528. The attack may be launched		
	VikBooking Hotel Booking	remotely. There is no exploit available.		
	Engine & PMS Plugin up to			
	1.5.8 on WordPress URL	It is recommended to upgrade the		
CVE-2022-1528	cross-site scripting	affected component.		
		A vulnerability has been found in WP 2FA	Protected	Detected b
		Plugin up to 2.2.0 and classified as	by Core	scanner as
		problematic. Affected by this	Rules	cross-site
		vulnerability is an unknown functionality		scripting
		of the component Admin Page. The		attack
		manipulation leads to cross-site scripting.		
		This vulnerability is known as CVE-2022-		
		1527. The attack can be launched		
		remotely. There is no exploit available.		
	WP 2FA Plugin up to 2.2.0			
	on WordPress Admin Page	It is recommended to upgrade the		
CVE-2022-1527	cross-site scripting	affected component.		
		A vulnerability, which was classified as	Protected	Detected b
		problematic, was found in Poll Maker	by Core	scanner as
		Plugin up to 4.0.1. Affected is an	Rules	cross-site
		unknown function of the component		scripting
		Setting Handler. The manipulation leads		attack
		to cross-site scripting.		
		This vulnerability is traded as CVE-2022-		
		1456. It is possible to launch the attack		
		remotely. There is no exploit available.		
	Poll Maker Plugin up to	remotely. There is no exploit available.		
	Poll Maker Plugin up to 4.0.1 on WordPress Setting	It is recommended to upgrade the		





5. <u>Vulnerability Type: SQL Injection</u>

Public ID	Vulnerability name	Vulnerability Description	AppTrana WAF Coverage	Indusfac e WAS Coverag e
CVE-2022-27466	mingSoft MCMS 5.2.27 /dict/list.do orderBy SQL injection (ID 90)	A vulnerability, which was classified as critical, was found in mingSoft MCMS 5.2.27. Affected is an unknown function of the file /dict/list.do. The manipulation of the argument orderBy leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is traded as CVE-2022-27466. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2022-1281	10Web Photo Gallery Plugin up to 1.6.3 on WordPress filter_tag SQL injection (ID 2706797)	A vulnerability, which was classified as critical, was found in 10Web Photo Gallery Plugin up to 1.6.3. This affects an unknown part. The manipulation of the argument filter_tag leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is uniquely identified as CVE-2022-1281. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-0783	Multiple Shipping Address Woocommerce Plugin up to 1.x on WordPress SQL injection	A vulnerability was found in Multiple Shipping Address Woocommerce Plugin up to 1.x. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability was named CVE-2022-0783. The attack can be initiated remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		
CVE-2022-0771	SiteSuperCharger Plugin up to 5.1.x on WordPress SQL injection	A vulnerability classified as critical has been found in SiteSuperCharger Plugin up to 5.1.x. Affected is an unknown function. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection
		This vulnerability is traded as CVE-2022-0771. It is possible to launch the attack remotely. There is no exploit available.		attack
		It is recommended to upgrade the affected component.		



CVE-2022-0773	Documentor Plugin up to 1.5.3 on WordPress SQL injection	A vulnerability classified as critical was found in Documentor Plugin up to 1.5.3. Affected by this vulnerability is an unknown functionality. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is known as CVE-2022- 0773. The attack can be launched remotely. There is no exploit available.		
CVE-2022-27962	Bluecms 1.6 Cookie SQL injection	A vulnerability, which was classified as critical, was found in Bluecms 1.6. Affected is an unknown function of the component Cookie Handler. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is traded as CVE-2022-27962. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2022-28505	jfinal_cms 5.1.0 com.jflyfox.system.log.LogC ontroller.java SQL injection (ID 33)	A vulnerability has been found in jfinal_cms 5.1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file com.jflyfox.system.log.LogController.java. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is known as CVE-2022-28505. The attack can be launched remotely. There is no exploit available.		
CVE-2022-28585	EmpireCMS 7.5 AdClass.php SQL injection	A vulnerability, which was classified as critical, was found in EmpireCMS 7.5. Affected is an unknown function of the file AdClass.php. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is traded as CVE-2022-28585. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2022-27413	Hospital Management System 1.0 admin.php adminname SQL injection	A vulnerability has been found in Hospital Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file admin.php. The manipulation of the argument adminname leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability was named CVE-2022-27413. The attack can be initiated remotely. There is no exploit available.		
CVE-2021-42185	wdja 2.1 Foreground Search SQL injection (ID 12)	A vulnerability, which was classified as critical, was found in wdja 2.1. This affects an unknown part of the component Foreground Search. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is uniquely identified as		



		CVE-2021-42185. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-28099	Poultry Farm Management System 1.0 /farm/store.php Item SQL injection	A vulnerability was found in Poultry Farm Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /farm/store.php. The manipulation of the argument Item leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is handled as CVE-2022-28099. The attack may be launched remotely. There is no exploit available.		
CVE-2022-28552	Cscms 4.1 Song Module SQL injection (ID 10)	A vulnerability classified as critical was found in Cscms 4.1. Affected by this vulnerability is an unknown functionality of the component Song Module. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is known as CVE-2022-28552. The attack can be launched remotely. There is no exploit available.		
CVE-2022-27431	Wuzhicms 4.1.0 group.php groupid SQL injection (ID 200)	A vulnerability was found in Wuzhicms 4.1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /coreframe/app/member/admin/group.ph p. The manipulation of the argument groupid leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is handled as CVE-2022-27431. The attack may be launched remotely. There is no exploit available.		
CVE-2022-27420	Hospital Management System 1.0 patientsearch.php patient_contact SQL injection (ID 19)	A vulnerability was found in Hospital Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file patientsearch.php. The manipulation of the argument patient_contact leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is known as CVE-2022-27420. The attack can be launched remotely. There is no exploit available.		
CVE-2022-28512	Sourcecodester Fantastic Blog CMS 1.0 single.php id SQL injection	A vulnerability classified as critical was found in Sourcecodester Fantastic Blog CMS 1.0. This vulnerability affects unknown code of the file /fantasticblog/single.php. The manipulation of the argument id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability was named CVE-2022- 28512. The attack can be initiated remotely. There is no exploit available.		



CVE-2022-28111	MyBatis PageHelper up to 5.x orderBy SQL injection	A vulnerability was found in MyBatis PageHelper up to 5.x. It has been declared as critical. This vulnerability affects unknown code. The manipulation of the argument orderBy leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE 2022 20461	mingulaturu SQL injection	This vulnerability was named CVE-2022-28111. The attack can be initiated remotely. There is no exploit available.	Protected	Datastad
CVE-2022-28461	mingyuefusu SQL injection	A vulnerability, which was classified as critical, was found in mingyuefusu. Affected is an unknown function. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection
		This vulnerability is traded as CVE-2022-28461. It is possible to launch the attack remotely. There is no exploit available.		attack
CVE-2022-29938	LibreHealth EHR 2.0.0 GET Parameter new_payment.php payment_id SQL injection	A vulnerability was found in LibreHealth EHR 2.0.0. It has been rated as critical. This issue affects some unknown processing of the file interface\billing\new_payment.php of the component GET Parameter Handler. The manipulation of the argument payment_id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		The identification of this vulnerability is CVE-2022-29938. The attack may be initiated remotely. There is no exploit available.		
CVE-2022-27360	SpringBlade up to 3.2.0 customSqlSegment SQL injection	A vulnerability was found in SpringBlade up to 3.2.0 and classified as critical. Affected by this issue is some unknown functionality. The manipulation of the argument customSqlSegment leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is handled as CVE-2022- 27360. The attack may be launched remotely. There is no exploit available.		
CVE-2022-28079	College Management System 1.0 course_code SQL injection	A vulnerability was found in College Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation of the argument course_code leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is handled as CVE-2022-28079. The attack may be launched remotely. There is no exploit available.		
CVE-2022-30047	mingSoft MCMS 5.2.7 listExcludeApp orderBy SQL injection	A vulnerability was found in mingSoft MCMS 5.2.7. It has been declared as critical. This vulnerability affects unknown code of the file /mdiy/dict/listExcludeApp. The manipulation of the argument orderBy	Protected by Core Rules	Detected by the scanner as SQL



		leads to SQL injection.		injection attack
		This vulnerability was named CVE-2022-30047. The attack can be initiated remotely. There is no exploit available.		
CVE-2022-29006	Directory Management System 1.0 username/password SQL injection (ID 50370 / EDB- 50370)	A vulnerability was found in Directory Management System 1.0. It has been classified as critical. Affected is an unknown function. The manipulation of the argument username/password leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is traded as CVE-2022-29006. The attack needs to be done within the local network. Furthermore, there is an exploit available.		
CVE-2022-30451	waimairenCMS up to 9.0 SQL injection	A vulnerability was found in waimairenCMS up to 9.0. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection
		This vulnerability was named CVE-2022-30451. The attack can be initiated remotely. There is no exploit available.		attack
		It is recommended to upgrade the affected component.		
CVE-2022-30048	mingSoft MCMS 5.2.7 /mdiy/dict/list orderBy SQL injection	A vulnerability was found in mingSoft MCMS 5.2.7. It has been rated as critical. This issue affects some unknown processing of the file /mdiy/dict/list. The manipulation of the argument orderBy leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		The identification of this vulnerability is CVE-2022-30048. The attack may be initiated remotely. There is no exploit available.		
CVE-2022-29306	IonizeCMS 1.0.8.1 article_model.php id_page SQL injection (ID 404)	A vulnerability was found in IonizeCMS 1.0.8.1. It has been declared as critical. This vulnerability affects unknown code of the file application/models/article_model.php. The manipulation of the argument id_page leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability was named CVE-2022-29306. The attack can be initiated remotely. There is no exploit available.		
CVE-2022-29985	Online Sports Complex Booking System 1.0 Master.php SQL injection	A vulnerability has been found in Online Sports Complex Booking System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file \scbs\classes\Master.php?f=delete_catego	Protected by Core Rules	Detected by the scanner as SQL injection attack



		ry. The manipulation leads to SQL injection.		
		This vulnerability is known as CVE-2022-29985. The attack can be launched remotely. There is no exploit available.		
CVE-2022-29979	Simple Client Management System 1.0 Master.php SQL injection	A vulnerability was found in Simple Client Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /cms/classes/Master.php?f=delete_design ation. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		The identification of this vulnerability is CVE-2022-29979. The attack may be initiated remotely. There is no exploit available.		
CVE-2022-29988	Online Sports Complex Booking System 1.0 Master.php SQL injection	A vulnerability classified as critical was found in Online Sports Complex Booking System 1.0. Affected by this vulnerability is an unknown functionality of the file \scbs\classes\Master.php?f=delete. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is known as CVE-2022-29988. The attack can be launched remotely. There is no exploit available.		
CVE-2022-29741	Money Transfer Management System 1.0 Master.php SQL injection	A vulnerability was found in Money Transfer Management System 1.0. It has been classified as critical. Affected is an unknown function of the file \mtms\classes\Master.php?f=delete_fee. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is traded as CVE-2022-29741. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2022-29999	Insurance Management System 1.0 editClient.php client_id SQL injection	A vulnerability classified as critical was found in Insurance Management System 1.0. This vulnerability affects unknown code of the file /insurance/editClient.php. The manipulation of the argument client_id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability was named CVE-2022-29999. The attack can be initiated remotely. There is no exploit available.		
CVE-2022-30000	Insurance Management System 1.0 editPayment.php recipt_no SQL injection	A vulnerability, which was classified as critical, has been found in Insurance Management System 1.0. This issue affects some unknown processing of the file /insurance/editPayment.php. The manipulation of the argument recipt_no leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack



		The identification of this vulnerability is CVE-2022-30000. The attack may be initiated remotely. There is no exploit available.		
CVE-2022-29993	Online Sports Complex Booking System 1.0 view_booking.php id SQL injection	A vulnerability was found in Online Sports Complex Booking System 1.0 and classified as critical. This issue affects some unknown processing of the file /scbs/admin/bookings/view_booking.php. The manipulation of the argument id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		The identification of this vulnerability is CVE-2022-29993. The attack may be initiated remotely. There is no exploit		
		available.		
Syste	Simple Client Management System 1.0 Users.php SQL injection	A vulnerability classified as critical has been found in Simple Client Management System 1.0. Affected is an unknown function of the file /cms/classes/Users.php?f=delete. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is traded as CVE-2022-29981. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2022-29749	Simple Client Management System 1.0 Master.php SQL injection	A vulnerability was found in Simple Client Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /cms/classes/Master.php?f=delete_invoice . The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is handled as CVE-2022- 29749. The attack may be launched remotely. There is no exploit available.		
CVE-2022-29750	Simple Client Management System 1.0 Master.php SQL injection	A vulnerability was found in Simple Client Management System 1.0. It has been classified as critical. This affects an unknown part of the file /cms/classes/Master.php?f=delete_service . The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is uniquely identified as CVE-2022-29750. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-29751	Simple Client Management System 1.0 Master.php SQL injection	A vulnerability was found in Simple Client Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /cms/classes/Master.php?f=delete_client. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack



		This vulnerability was named CVE-2022-29751. The attack can be initiated remotely. There is no exploit available.		
CVE-2022-29745	Money Transfer Management System 1.0 Master.php SQL injection	A vulnerability was found in Money Transfer Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file \mtms\classes\Master.php?f=delete_trans action. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is known as CVE-2022-29745. The attack can be launched remotely. There is no exploit available.		
CVE-2022-29746	Money Transfer Management System 1.0 Users.php SQL injection	A vulnerability was found in Money Transfer Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /mtms/classes/Users.php?f=delete. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is handled as CVE-2022-29746. The attack may be launched remotely. There is no exploit available.		
CVE-2022-29986	Booking Online Sports Complex Booking System 1.0 Master.php SQL injection	A vulnerability classified as critical has been found in Booking Online Sports Complex Booking System 1.0. Affected is an unknown function of the file \scbs\classes\Master.php?f=delete_facility. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is traded as CVE-2022-29986. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2022-29998	Insurance Management System 1.0 clientStatus.php client_id SQL injection	A vulnerability classified as critical has been found in Insurance Management System 1.0. This affects an unknown part of the file /insurance/clientStatus.php. The manipulation of the argument client_id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is uniquely identified as CVE-2022-29998. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-30002	Insurance Management System 1.0 editNominee.php nominee_id SQL injection	A vulnerability has been found in Insurance Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /insurance/editNominee.php. The manipulation of the argument nominee_id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack



		This vulnerability is known as CVE-2022-30002. The attack can be launched remotely. There is no exploit available.		
CVE-2022-30001	Insurance Management System 1.0 /insurance/editAgent.php agent_id SQL injection	A vulnerability, which was classified as critical, was found in Insurance Management System 1.0. Affected is an unknown function of the file /insurance/editAgent.php. The manipulation of the argument agent_id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is traded as CVE-2022-30001. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2022-29982	Simple Client Management System 1.0 manage_service.php id SQL injection	A vulnerability classified as critical was found in Simple Client Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /cms/admin/maintenance/manage_service .php. The manipulation of the argument id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is known as CVE-2022-29982. The attack can be launched remotely. There is no exploit available.		
CVE-2022-29989	Booking Online Sports Complex Booking System 1.0 Master.php SQL injection	A vulnerability, which was classified as critical, has been found in Booking Online Sports Complex Booking System 1.0. Affected by this issue is some unknown functionality of the file \scbs\classes\Master.php?f=delete_booking. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is handled as CVE-2022-29989. The attack may be launched remotely. There is no exploit available.		
CVE-2022-29992	Online Sports Complex Booking System 1.0 manage_category.php id SQL injection	A vulnerability has been found in Online Sports Complex Booking System 1.0 and classified as critical. This vulnerability affects unknown code of the file /scbs/admin/categories/manage_category. php. The manipulation of the argument id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability was named CVE-2022-29992. The attack can be initiated remotely. There is no exploit available.		
CVE-2022-30399	Merchandise Online Store 1.0 id SQL injection	A vulnerability, which was classified as critical, has been found in Merchandise Online Store 1.0. Affected by this issue is some unknown functionality of the file /vloggers_merch/admin/?page=maintenan ce/manage_category. The manipulation of	Protected by Core Rules	Detected by the scanner as SQL injection attack



		the argument id leads to SQL injection.		
CVE-2022-30373	Air Cargo Management System 1.0 manage_cargo_type.php id SQL injection	This vulnerability is handled as CVE-2022-30399. The attack may be launched remotely. There is no exploit available. A vulnerability classified as critical has been found in Air Cargo Management System 1.0. This affects an unknown part of the file /acms/admin/cargo_types/manage_cargo_type.php. The manipulation of the argument id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is uniquely identified as CVE-2022-30373. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-30385	Merchandise Online Store 1.0 Master.php SQL injection	A vulnerability, which was classified as critical, has been found in Merchandise Online Store 1.0. Affected by this issue is some unknown functionality of the file /vloggers_merch/classes/Master.php?f=del ete_order. The manipulation leads to SQL injection.	Protected by Rore rules	Detected by the scanner as SQL injection attack
		This vulnerability is handled as CVE-2022-30385. The attack may be launched remotely. There is no exploit available.		
CVE-2022-30401	Merchandise Online Store 1.0 id SQL injection	A vulnerability, which was classified as critical, was found in Merchandise Online Store 1.0. This affects an unknown part of the file /vloggers_merch/?p=view_product. The manipulation of the argument id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is uniquely identified as CVE-2022-30401. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-30386	Merchandise Online Store 1.0 Master.php SQL injection	A vulnerability, which was classified as critical, was found in Merchandise Online Store 1.0. This affects an unknown part of the file /vloggers_merch/classes/Master.php?f=del ete_featured. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is uniquely identified as CVE-2022-30386. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-30372	Air Cargo Management System 1.0 Master.php SQL injection	A vulnerability was found in Air Cargo Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file	Protected by Core Rules	Detected by the scanner as SQL



		/acms/classes/Master.php?f=delete_cargo. The manipulation leads to SQL injection.		injection attack
		This vulnerability is handled as CVE-2022-30372. The attack may be launched		
		remotely. There is no exploit available.		
CVE-2022-30384	Merchandise Online Store 1.0 Master.php SQL injection	A vulnerability classified as critical was found in Merchandise Online Store 1.0. Affected by this vulnerability is an unknown functionality of the file /vloggers_merch/classes/Master.php?f=del ete_inventory. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is known as CVE-2022-30384. The attack can be launched remotely. There is no exploit available.		
CVE-2022-30371	Air Cargo Management System 1.0 view_cargo_type.php id SQL injection	A vulnerability was found in Air Cargo Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /acms/admin/cargo_types/view_cargo_type.php. The manipulation of the argument id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is known as CVE-2022-30371. The attack can be launched remotely. There is no exploit available.		
CVE-2022-30374	Air Cargo Management System 1.0 id SQL injection	A vulnerability, which was classified as critical, has been found in Air Cargo Management System 1.0. This issue affects some unknown processing of the file /acms/admin/?page=transactions/manage _transaction. The manipulation of the argument id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		The identification of this vulnerability is CVE-2022-30374. The attack may be initiated remotely. There is no exploit available.		
CVE-2022-30393	Merchandise Online Store 1.0 id SQL injection	A vulnerability was found in Merchandise Online Store 1.0. It has been rated as critical. This issue affects some unknown processing of the file /vloggers_merch/admin/?page=product/m anage_product. The manipulation of the argument id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		The identification of this vulnerability is CVE-2022-30393. The attack may be initiated remotely. There is no exploit available.		



CVE-2022-30398	Merchandise Online Store	A vulnerability classified as critical was	Protected	Detected
	1.0 id SQL injection	found in Merchandise Online Store 1.0.	by Core	by the
		Affected by this vulnerability is an	Rules	scanner
		unknown functionality of the file		as SQL
		/vloggers_merch/admin/?page=orders/vie		injection
		w_order. The manipulation of the		attack
		argument id leads to SQL injection.		
		This vulnerability is known as CVE-2022-		
		30398. The attack can be launched		
		remotely. There is no exploit available.		
CVE-2022-30417	Covid-19 Travel Pass	A vulnerability was found in Covid-19	Protected	Detected
	Management System 1.0 id	Travel Pass Management System 1.0. It has	by Core	by the
	SQL injection	been rated as critical. Affected by this issue	Rules	scanner
		is some unknown functionality of the file		as SQL
		ctpms/admin/?page=user/manage_user.		injection
		The manipulation of the argument id leads		attack
		to SQL injection.		
		This vulnerability is handled as CVE-2022-		
		30417. The attack may be launched		
		remotely. There is no exploit available.		
CVE-2022-30414	Covid-19 Travel Pass	A vulnerability was found in Covid-19	Protected	Detected
	Management System 1.0 id	Travel Pass Management System 1.0. It has	by Core	by the
	SQL injection	been declared as critical. Affected by this	Rules	scanner
		vulnerability is an unknown functionality of		as SQL
		the file		injection
		/ctpms/admin/?page=applications/view_a		attack
		pplication. The manipulation of the		
		argument id leads to SQL injection.		
		This vulnerability is known as CVE-2022-		
		30414. The attack can be launched		
		remotely. There is no exploit available.		
CVE-2022-30370	Air Cargo Management	A vulnerability was found in Air Cargo	Protected	Detected
	System 1.0 Master.php SQL	Management System 1.0. It has been	by Core	by the
	injection	classified as critical. Affected is an	Rules	scanner
		unknown function of the file		as SQL
		/acms/classes/Master.php?f=delete_cargo		injection
		_type. The manipulation leads to SQL		attack
		injection.		
		This vulnerability is traded as CVE-2022-		
		30370. It is possible to launch the attack		
		remotely. There is no exploit available.		
CVE-2022-30376	Sourcecodester Simple	A vulnerability was found in	Protected	Detected
	Social Networking Site 1.0	Sourcecodester Simple Social Networking	by Core	by the
	view_member.php id SQL	Site 1.0. It has been rated as critical. This	Rules	scanner
	that a set and	issue affects some unknown processing of		as SQL
	injection			
	injection	the file		injection
	injection	the file /sns/admin/members/view_member.php.		injection attack
	injection	the file		



		The identification of this vulnerability is CVE-2022-30376. The attack may be initiated remotely. There is no exploit available.		
CVE-2022-28530	NCDC Covid-19 Directory on Vaccination 1.0 cmdcategory SQL injection (ID 166481)	A vulnerability, which was classified as critical, has been found in NCDC Covid-19 Directory on Vaccination 1.0. This issue affects some unknown processing. The manipulation of the argument cmdcategory leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		The identification of this vulnerability is CVE-2022-28530. The attack may be initiated remotely. There is no exploit available.		
CVE-2022-28080	Royal Event Management System 1.0 todate SQL injection	A vulnerability classified as critical has been found in Royal Event Management System 1.0. This affects an unknown part. The manipulation of the argument todate leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is uniquely identified as CVE-2022-28080. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-28533	SourceCodester Medical Hub Directory Site 1.0 view_details.php SQL injection (ID 166539)	A vulnerability, which was classified as critical, was found in SourceCodester Medical Hub Directory Site 1.0. Affected is an unknown function of the file /mhds/clinic/view_details.php. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is traded as CVE-2022-28533. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2020-19213	Piwigo 2.9.5 cat_move.php move_categories selection SQL injection (ID 1010)	A vulnerability was found in Piwigo 2.9.5 and classified as critical. This issue affects the function move_categories of the file cat_move.php. The manipulation of the argument selection leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		The identification of this vulnerability is CVE-2020-19213. The attack may be initiated remotely. There is no exploit available.		
CVE-2020-19217	Piwigo 2.9.5 admin/batch_manager.php filter_category SQL injection (ID 1012)	A vulnerability was found in Piwigo 2.9.5. It has been rated as critical. Affected by this issue is some unknown functionality of the file admin/batch_manager.php. The manipulation of the argument filter_category leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is handled as CVE-2020-		



		19217. The attack may be launched		
CVE-2020-19216	Piwigo 2.9.5 admin/user_perm.php cat_false SQL injection (ID 1011)	remotely. There is no exploit available. A vulnerability was found in Piwigo 2.9.5. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file admin/user_perm.php. The manipulation of the argument cat_false leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is known as CVE-2020- 19216. The attack can be launched remotely. There is no exploit available.		
CVE-2020-19212	Piwigo 2.9.5 admin/group_list.php group SQL injection (ID 1009)	A vulnerability has been found in Piwigo 2.9.5 and classified as critical. This vulnerability affects unknown code of the file admin/group_list.php. The manipulation of the argument group leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability was named CVE-2020- 19212. The attack can be initiated remotely. There is no exploit available.		
CVE-2022-0592	MapSVG Plugin up to 6.2.19 on WordPress REST Endpoint SQL injection	A vulnerability was found in MapSVG Plugin up to 6.2.19. It has been rated as critical. This issue affects some unknown processing of the component REST Endpoint. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		The identification of this vulnerability is CVE-2022-0592. The attack may be initiated remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		
CVE-2022-0826	WP Video Gallery Plugin up to 1.7.1 on WordPress SQL injection	A vulnerability classified as critical was found in WP Video Gallery Plugin up to 1.7.1. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is known as CVE-2022- 0826. The attack can be launched remotely. There is no exploit available.		
CVE-2022-0817	BadgeOS Plugin up to 3.7.0 on WordPress SQL injection	A vulnerability classified as critical has been found in BadgeOS Plugin up to 3.7.0. Affected is an unknown function. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection
		This vulnerability is traded as CVE-2022-0817. It is possible to launch the attack remotely. There is no exploit available.		attack



CVE-2022-0948	Order Listener for WooCommerce Plugin up to 3.2.1 on WordPress id SQL injection (ID 2707223)	A vulnerability was found in Order Listener for WooCommerce Plugin up to 3.2.1. It has been classified as critical. This affects an unknown part. The manipulation of the argument id leads to SQL injection.	Protected by Rore rules	Detected by the scanner as SQL injection attack
		This vulnerability is uniquely identified as CVE-2022-0948. It is possible to initiate the attack remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		
CVE-2022-1013	Personal Dictionary Plugin up to 1.3.3 on WordPress SQL injection	A vulnerability, which was classified as critical, was found in Personal Dictionary Plugin up to 1.3.3. This affects an unknown part. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is uniquely identified as CVE-2022-1013. It is possible to initiate the attack remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		
CVE-2022-0836	SEMA API Plugin up to 3.64 on WordPress AJAX Action SQL injection	A vulnerability, which was classified as critical, has been found in SEMA API Plugin up to 3.64. Affected by this issue is some unknown functionality of the component AJAX Action Handler. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is handled as CVE-2022- 0836. The attack may be launched remotely. There is no exploit available.		
CVE-2022-28110	Hotel Management System 1.0 Login Page username SQL injection	A vulnerability, which was classified as critical, was found in Hotel Management System 1.0. This affects an unknown part of the component Login Page. The manipulation of the argument username leads to sql injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is uniquely identified as CVE-2022-28110. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-0814	Ubigeo de Perú para Woocommerce Plugin up to 3.6.3 on WordPress AJAX Action SQL injection	A vulnerability has been found in Ubigeo de Perú para Woocommerce Plugin up to 3.6.3 and classified as critical. Affected by this vulnerability is an unknown functionality of the component AJAX Action Handler. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack



		This vulnerability is known as CVE-2022-0814. The attack can be launched remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		
CVE-2022-27412	Explore CMS 1.0 /page.php id SQL injection (ID 166694)	A vulnerability was found in Explore CMS 1.0. It has been rated as critical. This issue affects some unknown processing of the file /page.php. The manipulation of the argument id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		The identification of this vulnerability is CVE-2022-27412. The attack may be initiated remotely. There is no exploit available.		
CVE-2022-30452	Shopwind up to 3.4.2 Database.php SQL injection	A vulnerability, which was classified as critical, was found in Shopwind up to 3.4.2. Affected is an unknown function of the file Database.php. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is traded as CVE-2022-30452. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2022-30449	Hospital Management System in PHP 1.0 room.php editid SQL injection	A vulnerability classified as critical was found in Hospital Management System in PHP 1.0. Affected by this vulnerability is an unknown functionality of the file room.php. The manipulation of the argument editid leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is known as CVE-2022-30449. The attack can be launched remotely. There is no exploit available.		
CVE-2022-29007	PHPGurukul Dairy Farm Shop Management System 1.0 Admin Panel username/password SQL injection (ID 50365 / EDB- 50365)	A vulnerability was found in PHPGurukul Dairy Farm Shop Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Admin Panel. The manipulation of the argument username/password leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is known as CVE-2022-29007. The attack needs to be initiated within the local network. Furthermore, there is an exploit available.		
CVE-2022-29009	Cyber Cafe Management System Project 1.0 username/password SQL injection (ID 50355 / EDB- 50355)	A vulnerability classified as critical has been found in Cyber Cafe Management System Project 1.0. This affects an unknown part. The manipulation of the argument username/password leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack



		This vulnerability is uniquely identified as CVE-2022-29009. Access to the local network is required for this attack to succeed. Furthermore, there is an exploit available.		
CVE-2022-30407	Pharmacy Sales and Inventory System 1.0 manage_user.php id SQL injection	A vulnerability classified as critical was found in Pharmacy Sales and Inventory System 1.0. This vulnerability affects unknown code of the file /pharmacy-sales-and-inventory-system/manage_user.php. The manipulation of the argument id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability was named CVE-2022-30407. The attack can be initiated remotely. There is no exploit available.		
CVE-2022-30395	Merchandise Online Store 1.0 Master.php SQL injection	A vulnerability was found in Merchandise Online Store 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /vloggers_merch/classes/Master.php?f=del ete_cart. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is known as CVE-2022-30395. The attack can be launched remotely. There is no exploit available.		
CVE-2022-30387	Merchandise Online Store 1.0 Master.php SQL injection	A vulnerability has been found in Merchandise Online Store 1.0 and classified as critical. This vulnerability affects unknown code of the file /vloggers_merch/classes/Master.php?f=pa y_order. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability was named CVE-2022-30387. The attack can be initiated remotely. There is no exploit available.		
CVE-2022-30404	College Management System 1.0 display- teacher.php teacher_id SQL injection	A vulnerability classified as critical has been found in College Management System 1.0. This affects an unknown part of the file /College_Management_System/admin/dis play-teacher.php. The manipulation of the argument teacher_id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is uniquely identified as CVE-2022-30404. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-30392	Merchandise Online Store 1.0 Master.php SQL injection	A vulnerability was found in Merchandise Online Store 1.0. It has been classified as critical. Affected is an unknown function of the file	Protected by Core Rules	Detected by the scanner as SQL



		/vloggers_merch/classes/Master.php?f=del ete_sub_category. The manipulation leads to SQL injection.		injection attack
		This vulnerability is traded as CVE-2022-30392. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2021-41965	ChurchCRM up to 4.4.5 Edit EN_tyid/theID/EID SQL injection	A vulnerability, which was classified as critical, was found in ChurchCRM up to 4.4.5. Affected is an unknown function of the component Edit Handler. The manipulation of the argument EN_tyid/theID/EID leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is traded as CVE-2021-41965. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2022-28930	ERP-Pro 3.7.5 SysEveMenuAuthPointMap per.xml SQL injection	A vulnerability was found in ERP-Pro 3.7.5 and classified as critical. Affected by this issue is some unknown functionality of the file /base/SysEveMenuAuthPointMapper.xml. The manipulation leads to SQL injection.	Protected by core rules	Detected by the scanner as SQL injection attack
		This vulnerability is handled as CVE-2022-28930. The attack may be launched remotely. There is no exploit available.		
CVE-2022-1182	Visual Slide Box Builder Plugin up to 3.2.9 on WordPress SQL injection	A vulnerability was found in Visual Slide Box Builder Plugin up to 3.2.9. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is known as CVE-2022- 1182. The attack can be launched remotely. There is no exploit available.		
CVE-2022-30012	HMS 1.0 POST Request appointment.php SQL injection	A vulnerability has been found in HMS 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file appointment.php of the component POST Request Handler. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is known as CVE-2022-30012. The attack can be launched remotely. There is no exploit available.		
CVE-2022-28929	Hospital Management System 1.0 viewtreatmentrecord.php delid SQL injection	A vulnerability has been found in Hospital Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file viewtreatmentrecord.php. The manipulation of the argument delid leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack



		This vulnerability is known as CVE-2022- 28929. The attack can be launched remotely. There is no exploit available.		
CVE-2022-0867	Pricing Table Plugin up to 3.6.0 on WordPress SQL injection	A vulnerability was found in Pricing Table Plugin up to 3.6.0. It has been classified as critical. Affected is an unknown function. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection
		This vulnerability is traded as CVE-2022-0867. The attack can only be initiated within the local network. There is no exploit available.		attack
		It is recommended to upgrade the affected component.		
CVE-2022-30011	HMS up to 1.0 appointment.php SQL injection	A vulnerability, which was classified as critical, was found in HMS up to 1.0. Affected is an unknown function of the file appointment.php. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is traded as CVE-2022-30011. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2022-24391	Fidelis Network and Deception up to 9.4.4 Web Interface SQL injection	A vulnerability was found in Fidelis Network and Deception up to 9.4.4. It has been classified as critical. Affected is an unknown function of the component Web Interface. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is traded as CVE-2022-24391. It is possible to launch the attack remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		
CVE-2022-30054	Covid 19 Travel Pass Management 1.0 code SQL injection	A vulnerability has been found in Covid 19 Travel Pass Management 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation of the argument code leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is known as CVE-2022-30054. The attack can be launched remotely. There is no exploit available.		
CVE-2022-30053	Toll Tax Management System 1.0 id SQL injection	A vulnerability, which was classified as critical, was found in Toll Tax Management System 1.0. Affected is an unknown function. The manipulation of the argument id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
				actack



		30053. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2022-30052	Home Clean Service System 1.0 password SQL injection	A vulnerability, which was classified as critical, has been found in Home Clean Service System 1.0. This issue affects some unknown processing. The manipulation of the argument password leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		The identification of this vulnerability is CVE-2022-30052. The attack may be initiated remotely. There is no exploit available.		
CVE-2022-28962	Online Sports Complex Booking System 1.0 Users.php SQL injection (ID 166598)	A vulnerability, which was classified as critical, has been found in Online Sports Complex Booking System 1.0. Affected by this issue is some unknown functionality of the file /scbs/classes/Users.php?f=delete_client. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is handled as CVE-2022-28962. The attack may be launched remotely. There is no exploit available.		
CVE-2021-37413	GRANDCOM DynWEB up to 4.1 Admin Login Interface SQL injection	A vulnerability classified as critical has been found in GRANDCOM DynWEB up to 4.1. Affected is an unknown function of the component Admin Login Interface. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is traded as CVE-2021-37413. It is possible to launch the attack remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		
CVE-2022-28105	Online Sports Complex Booking System 1.0 /scbs/view_facility.php id SQL injection	A vulnerability was found in Online Sports Complex Booking System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /scbs/view_facility.php. The manipulation of the argument id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is handled as CVE-2022-28105. The attack may be launched remotely. There is no exploit available.		
CVE-2022-26632	Multi-Vendor Online Groceries Management System 1.0 view_product.php id SQL injection (ID 50739 / EDB- 50739)	A vulnerability, which was classified as critical, was found in Multi-Vendor Online Groceries Management System 1.0. Affected is an unknown function of the file /products/view_product.php. The manipulation of the argument id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack



		This vulnerability is traded as CVE-2022-26632. It is possible to launch the attack remotely. Furthermore, there is an exploit available.		
CVE-2022-30886	School Dormitory Management System 1.0 daily_collection_report.php month SQL injection (ID 167001)	A vulnerability, which was classified as critical, has been found in School Dormitory Management System 1.0. This issue affects some unknown processing of the file /dms/admin/reports/daily_collection_report.php. The manipulation of the argument month leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		The identification of this vulnerability is CVE-2022-30886. The attack may be initiated remotely. There is no exploit available.		
CVE-2022-28961	SPIP up to 3.1.13 /ecrire lier_trad/where SQL injection	A vulnerability, which was classified as critical, was found in SPIP up to 3.1.13. This affects an unknown part of the file /ecrire. The manipulation of the argument lier_trad/where leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is uniquely identified as CVE-2022-28961. It is possible to initiate the attack remotely. There is no exploit available.		
		It is recommended to apply a patch to fix this issue.		
CVE-2022-29652	Online Sports Complex Booking System 1.0 Users.php SQL injection (ID 166641)	A vulnerability has been found in Online Sports Complex Booking System 1.0 and classified as critical. This vulnerability affects unknown code of the file /scbs/classes/Users.php?f=save_client. The manipulation leads to SQL injection.	Protected by Core Rues	Detected by the scanner as SQL injection attack
		This vulnerability was named CVE-2022-29652. The attack can be initiated remotely. There is no exploit available.		
CVE-2022-29304	Online Sports Complex Booking System 1.0 master.php delete_facility SQL injection	A vulnerability, which was classified as critical, was found in Online Sports Complex Booking System 1.0. This affects the function delete_facility of the file /classes/master.php?f=delete_facility. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is uniquely identified as CVE-2022-29304. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-28531	Sourcecodester Covid-19 Directory on Vaccination 1.0 admin/login.php	A vulnerability, which was classified as critical, was found in Sourcecodester Covid-19 Directory on Vaccination 1.0. This	Protected by Core Rules	Detected by the scanner



	txtusername SQL injection (ID 166481)	affects an unknown part of the file admin/login.php. The manipulation of the argument txtusername leads to SQL injection.	as SQL injection attack	
		This vulnerability is uniquely identified as CVE-2022-28531. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-1014	WP Contacts Manager Plugin up to 2.2.4 on WordPress SQL injection	A vulnerability was found in WP Contacts Manager Plugin up to 2.2.4. It has been classified as critical. Affected is an unknown function. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is traded as CVE-2022- 1014. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2022-0781	Nirweb Support Plugin up to 2.8.1 on WordPress SQL injection	A vulnerability was found in Nirweb Support Plugin up to 2.8.1 and classified as critical. This issue affects some unknown processing. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		The identification of this vulnerability is CVE-2022-0781. The attack may be initiated remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		
CVE-2022-30454	Merchandise Online Store 1.0 Master.php SQL injection	A vulnerability classified as critical has been found in Merchandise Online Store 1.0. This affects an unknown part of the file /vloggers_merch/classes/Master.php?f=del ete_product. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is uniquely identified as CVE-2022-30454. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-31487	Inout Blockchain AltExchanger master.php symbol SQL injection	A vulnerability was found in Inout Blockchain AltExchanger and Inout Blockchain FiatExchanger and classified as critical. Affected by this issue is some unknown functionality of the file Chart/TradingView/chart_content/master. php. The manipulation of the argument symbol leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is handled as CVE-2022-31487. The attack may be launched remotely. There is no exploit available.		



CVE-2022-1839	Home Clean Services Management System 1.0 login.php email SQL injection	A vulnerability classified as critical was found in Home Clean Services Management System 1.0. This vulnerability affects unknown code of the file login.php. The manipulation of the argument email with the input admin%'/**/AND/**/(SELECT/**/53 83/**/FROM/**/(SELECT(SLEEP(2)))JPeh)/* */AND/**/'frfq%'='frfq leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability was named CVE-2022- 1839. The attack can be initiated remotely. Furthermore, there is an exploit available.		
CVE-2021-42655	SiteServer CMS 6.15.51 SQL injection (ID 3237)	A vulnerability was found in SiteServer CMS 6.15.51. It has been classified as critical. This affects an unknown part. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection
		This vulnerability is uniquely identified as CVE-2021-42655. It is possible to initiate the attack remotely. There is no exploit available.		attack
CVE-2022-1838	Home Clean Services Management System 1.0 admin/login.php username SQL injection	A vulnerability classified as critical has been found in Home Clean Services Management System 1.0. This affects an unknown part of the file admin/login.php. The manipulation of the argument username with the input admin%'/**/AND/**/(SELECT/**/53 83/**/FROM/**/(SELECT(SLEEP(5)))JPeh)/* */AND/**/'frfq%'='frfq leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is uniquely identified as CVE-2022-1838. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.		
CVE-2022-30455	Badminton Center Management System 1.0 Master.php SQL injection	A vulnerability classified as critical was found in Badminton Center Management System 1.0. This vulnerability affects unknown code of the file /bcms/classes/Master.php?f=delete_court _rental. The manipulation leads to SQL injection.	Protected by Rore rules	Detected by the scanner as SQL injection attack
		This vulnerability was named CVE-2022-30455. The attack can be initiated remotely. There is no exploit available.		
CVE-2022-29305	imgurl 2.31 /upload/localhost SQL injection (ID 75)	A vulnerability was found in imgurl 2.31 and classified as critical. Affected by this issue is some unknown functionality of the file /upload/localhost. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL



		This vulnerability is handled as CVE-2022-29305. The attack needs to be approached within the local network. Furthermore, there is an exploit available.		injection attack
CVE-2022-30461	water-billing-management- system 1.0 Master.php id SQL injection	A vulnerability classified as critical was found in water-billing-management-system 1.0. Affected by this vulnerability is an unknown functionality of the file /wbms/classes/Master.php?f=delete_client . The manipulation of the argument id leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is known as CVE-2022-30461. The attack can be launched remotely. Furthermore, there is an exploit available.		
CVE-2022-1883	camptocamp terraboard up to 2.1.x SQL injection	A vulnerability, which was classified as critical, was found in camptocamp terraboard up to 2.1.x. This affects an unknown part. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is uniquely identified as CVE-2022-1883. It is possible to initiate the attack remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		
CVE-2022-28862	ARCHIBUS Web Central up to 26.1 workflow.runWorkflowRule .dwr SQL injection	A vulnerability was found in ARCHIBUS Web Central up to 26.1 and classified as critical. This issue affects some unknown processing of the file dwr/call/plaincall/workflow.runWorkflowR ule.dwr. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		The identification of this vulnerability is CVE-2022-28862. The attack may be initiated remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		
CVE-2022-29650	Online Food Ordering System 1.0 food-search.php Search SQL injection	A vulnerability has been found in Online Food Ordering System 1.0 and classified as critical. This vulnerability affects unknown code of the file /online-food-order/food-search.php. The manipulation of the argument Search leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability was named CVE-2022-		



		29650. The attack can be initiated remotely. There is no exploit available.		
CVE-2022-29667	CSCMS Music Portal System 4.2 Photo hy SQL injection (ID 26)	A vulnerability, which was classified as critical, was found in CSCMS Music Portal System 4.2. Affected is an unknown function of the file /admin.php/pic/admin/pic/hy of the component Photo Handler. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is traded as CVE-2022- 29667. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2022-1556	STAFFLIST PLUGIN UP TO 3.1.4 ON WORDPRESS ADMIN DASHBOARD SQL INJECTION	A vulnerability, which was classified as critical, has been found in StaffList Plugin up to 3.1.4. Affected by this issue is some unknown functionality of the component Admin Dashboard. The manipulation leads to SQL injection.	Protected by Core Rules	Detected by the scanner as SQL injection attack
		This vulnerability is handled as CVE-2022- 1556. The attack may be launched remotely. There is no exploit available.		
		It is recommended to upgrade the affected component.		