Zero-Day Vulnerability Report - January 2023

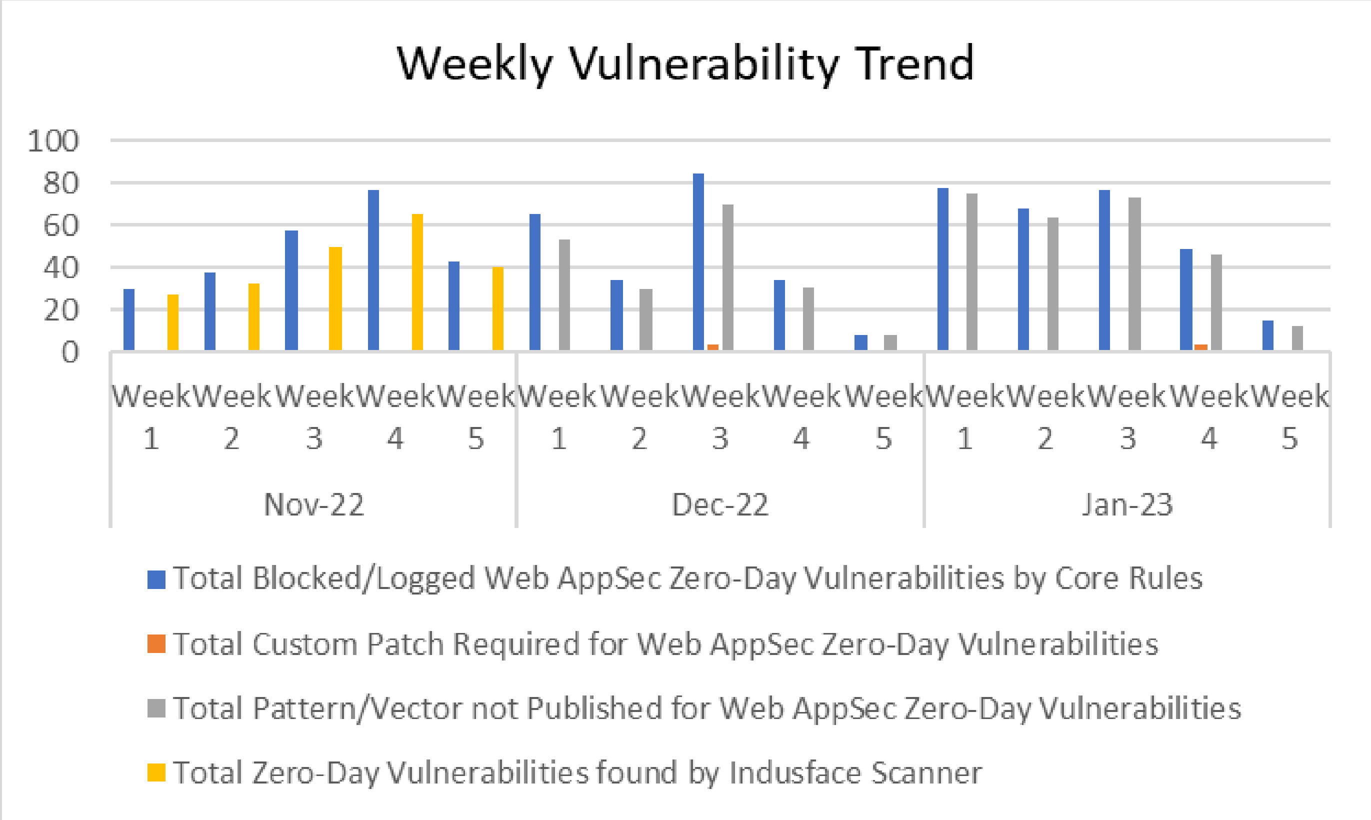
Command Injection	CSRF	Local File Inclusion	Http Request Smuggling	Malicious File Upload	SQL Injection	XSS Injection	XXE Attack
29	17	17	1	7	76	146	1

> *The total zero-day vulnerabilities count for December month : 294*
>
> *Zero-day vulnerabilities protected through core rules: 287*
>
> *Zero-day vulnerabilities protected through custom rules: 7*
>
> *Zero-day vulnerabilities for which protection can not be done: 0*
>
> *Zero-day vulnerabilities found by Indusface WAS: 270*

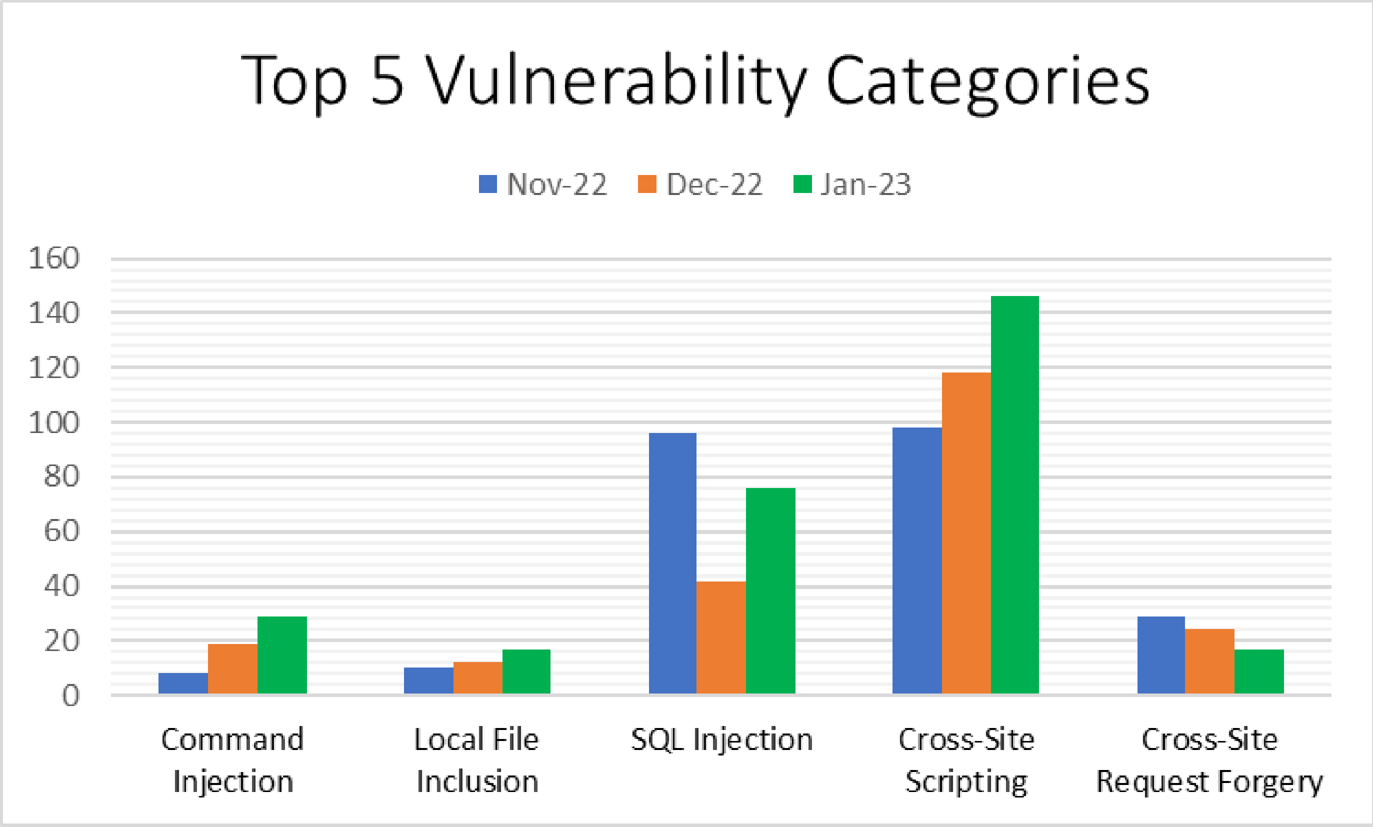
- To enable custom rules, please contact support@indusface.com
- Since the attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.

Vulnerability Trend

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



98%	**of the zero-day vulnerabilities were protected by the core rules in the last month.**	**2%**	**of the zero-day vulnerabilities were protected by the custom rules in the last month.**	**92%**	**of the zero-day vulnerabilities were reported by Indusface Scanner in the last month.**



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0048	lirantal daloradius code injection	A vulnerability classified as critical was found in lirantal daloradius. This vulnerability affects unknown code. The manipulation leads to code injection. This vulnerability was named CVE-2023-0048. The attack can be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2022-44149	Nexxt Amp300 ARN02304U8 42.103.1.5095 Web Service goform /sysTools telnetd os command injection (WLB-2023010006)	A vulnerability which was classified as critical has been found in Nexxt Amp300 ARN02304U8 42.103.1.5095. Affected by this issue is some unknown functionality of the file goform/sysTools of the component Web Service. The manipulation of the argument telnetd leads to os command injection. This vulnerability is handled as CVE-2022-44149. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack

CVE-2022-25923	exec-local-bin up to 1.1.x theProcess command injection	A vulnerability was found in exec-local-bin up to 1.1.x. It has been classified as critical. This affects the function theProcess. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2022-25923. The attack needs to be approached locally. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-22671	NSA Ghidra up to 10.2.2 launch.sh analyzeHeadless command injection (ID 4869)	A vulnerability was found in NSA Ghidra up to 10.2.2. It has been rated as critical. Affected by this issue is the function analyzeHeadless of the file Ghidra/RuntimeScripts/Linux/support/launch.sh. The manipulation leads to command injection. This vulnerability is handled as CVE-2023-22671. The attack needs to be done within the local network. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2022-44877	Centos Panel 7 prior 0.9.8.1147 HTTP Request /login/index.php Remote Code Execution	A vulnerability classified as critical was found in Centos Panel 7. This vulnerability affects unknown code of the file /login/index.php of the component HTTP Request Handler. The manipulation leads to Remote Code Execution. This vulnerability was named CVE-2022-44877. The attack can only be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2022-25890	wifey connect command injection (SNYK-JS-WIFEY-3175615)	A vulnerability which was classified as critical has been found in wifey. Affected by this issue is the function connect. The manipulation leads to command injection. This vulnerability is handled as CVE-2022-25890. Attacking locally is a requirement. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack

CVE-2022-43973	Linksys WRT54GL up to 4.30.18.006 httpd /apply.cgi Check_TSSI os command injection	A vulnerability which was classified as critical has been found in Linksys WRT54GL up to 4.30.18.006. Affected by this issue is the function Check_TSSI of the file /apply.cgi of the component httpd. The manipulation leads to os command injection. This vulnerability is handled as CVE-2022-43973. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2022-43971	Linksys WUMC710 up to 1.0.02 httpd /setNTP.cgi do_setNTP os command injection	A vulnerability has been found in Linksys WUMC710 up to 1.0.02 and classified as critical. This vulnerability affects the function do_setNTP of the file /setNTP.cgi of the component httpd. The manipulation leads to os command injection. This vulnerability was named CVE-2022-43971. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2022-48252	jokob-sk Pi.Alert prior 22.12.20 nmap_scan.php scan os command injection (GHSA-vhg3-f6gv-j89r)	A vulnerability was found in jokob-sk Pi.Alert. It has been rated as critical. Affected by this issue is the function nmap_scan.php. The manipulation of the argument scan leads to os command injection. This vulnerability is handled as CVE-2022-48252. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-22496	Netdata prior 1.36.0-409/1.37 health_alarm_execute command injection (GHSA-xg38-3vmw-2978)	A vulnerability classified as critical was found in Netdata. Affected by this vulnerability is the function health_alarm_execute. The manipulation leads to command injection. This vulnerability is known as CVE-2023-22496. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-0315	froxlor up to 2.0.7 command injection	A vulnerability was found in froxlor up to 2.0.7. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to command injection. The identification of this vulnerability is CVE-2023-0315. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection attack

CVE-2022-47853	TOTOlink A7100RU 7.4cu.2313_B20191024 httpd Service command injection	A vulnerability which was classified as critical was found in TOTOlink A7100RU 7.4cu.2313_B20191024. This affects an unknown part of the component httpd Service. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2022-47853. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-0164	OrangeScrum 2.0.11 injection	A vulnerability was found in OrangeScrum 2.0.11. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation leads to injection. This vulnerability is handled as CVE-2023-0164. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2022-46476	D-Link DIR-859 A1 1.05 soapcgi_main service command injection	A vulnerability which was classified as critical was found in D-Link DIR-859 A1 1.05. This affects the function soapcgi_main. The manipulation of the argument service leads to command injection. This vulnerability is uniquely identified as CVE-2022-46476. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2022-48123	TOTOLINK A7100RU 7.4cu.2313_B20191024 Setting delStaticDhcpRules servername command injection	A vulnerability classified as critical was found in TOTOLINK A7100RU 7.4cu.2313_B20191024. Affected by this vulnerability is the function delStaticDhcpRules of the component Setting Handler. The manipulation of the argument servername leads to command injection. This vulnerability is known as CVE-2022-48123. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-23596	jc21 NGINX Proxy Manager up to 2.9.19 Access List os command injection	A vulnerability classified as critical has been found in jc21 NGINX Proxy Manager up to 2.9.19. This affects an unknown part of the component Access List Handler. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2023-23596. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack

CVE-2022-48121	TOTOlink A7100RU 7.4cu. 2313_B20191024 delStaticDhcpRules rsabits command injection	A vulnerability was found in TOTOlink A7100RU 7.4cu. 2313_B20191024. It has been rated as critical. This issue affects some unknown processing of the file setting /delStaticDhcpRules. The manipulation of the argument rsabits leads to command injection. The identification of this vulnerability is CVE-2022-48121. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2022-48122	TOTOlink A7100RU 7.4cu. 2313_B20191024 Setting delStaticDhcpRules dayvalid command injection	A vulnerability classified as critical has been found in TOTOlink A7100RU 7.4cu. 2313_B20191024. Affected is the function delStaticDhcpRules of the component Setting Handler. The manipulation of the argument dayvalid leads to command injection. This vulnerability is traded as CVE-2022-48122. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2022-48125	TOTOLINK A7100RU 7.4cu. 2313_B20191024 Setting setOpenVpnCertGenerationCfg password command injection	A vulnerability which was classified as critical was found in TOTOLINK A7100RU 7.4cu. 2313_B20191024. This affects the function setOpenVpnCertGenerationCfg of the component Setting Handler. The manipulation of the argument password leads to command injection. This vulnerability is uniquely identified as CVE-2022-48125. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2022-48126	TOTOLINK A7100RU 7.4cu. 2313_B20191024 Setting setOpenVpnCertGenerationCfg username command injection	A vulnerability has been found in TOTOLINK A7100RU 7.4cu. 2313_B20191024 and classified as critical. This vulnerability affects the function setOpenVpnCertGenerationCfg of the component Setting Handler. The manipulation of the argument username leads to command injection. This vulnerability was named CVE-2022-48126. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack

CVE-2022-48124	TOTOLINK A7100RU 7.4cu.2313_B20191024 Setting setOpenVpnCertGenerationCfg FileName command injection	A vulnerability which was classified as critical has been found in TOTOLINK A7100RU 7.4cu.2313_B20191024. Affected by this issue is the function setOpenVpnCertGenerationCfg of the component Setting Handler. The manipulation of the argument FileName leads to command injection. This vulnerability is handled as CVE-2022-48124. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2020-36655	Yii Yii2 Gii up to 2.2.1 Generator.php messageCategory code injection (ID 433)	A vulnerability which was classified as critical has been found in Yii Yii2 Gii up to 2.2.1. This issue affects some unknown processing of the file Generator.php. The manipulation of the argument messageCategory leads to code injection. The identification of this vulnerability is CVE-2020-36655. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-24044	Plesk Obsidian up to 18.0.49 Login Page Host injection	A vulnerability was found in Plesk Obsidian up to 18.0.49. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Login Page. The manipulation of the argument Host leads to injection. This vulnerability is known as CVE-2023-24044. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2022-37718	EdgeNexus ADC up to 4.2.8 Management Portal command injection	A vulnerability classified as critical has been found in EdgeNexus ADC up to 4.2.8. Affected is an unknown function of the component Management Portal. The manipulation leads to command injection. This vulnerability is traded as CVE-2022-37718. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack

CVE-2022-48070	Phicomm K2 22.6.534.263 Automatic Upgrade autoUpTime command injection	A vulnerability was found in Phicomm K2 22.6.534.263. It has been classified as critical. Affected is an unknown function of the component Automatic Upgrade Handler. The manipulation of the argument autoUpTime leads to command injection. This vulnerability is traded as CVE-2022-48070. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2022-48072	Phicomm K2G 22.6.3.20 Automatic Upgrade autoUpTime command injection	A vulnerability was found in Phicomm K2G 22.6.3.20. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Automatic Upgrade Handler. The manipulation of the argument autoUpTime leads to command injection. This vulnerability is known as CVE-2022-48072. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2022-48069	Totolink A830R 4.1.2cu.5182 QUERY_STRING command injection	A vulnerability was found in Totolink A830R 4.1.2cu.5182 and classified as critical. This issue affects some unknown processing. The manipulation of the argument QUERY_STRING leads to command injection. The identification of this vulnerability is CVE-2022-48069. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-0493	btcpayserver up to 1.7.4 equivalent special elements	A vulnerability was found in btcpayserver up to 1.7.4. It has been classified as problematic. This affects an unknown part. The manipulation leads to improper neutralization of equivalent special elements. This vulnerability is uniquely identified as CVE-2023-0493. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2022-25908	create-choo-electron devInstall command injection (SNYK-JS-CREATECHOOELECTRON-3157953)	A vulnerability was found in create-choo-electron. It has been rated as critical. Affected by this issue is the function devInstall. The manipulation leads to command injection. This vulnerability is handled as CVE-2022-25908. An attack has to be approached locally. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3911	iubenda All-in-one Compliance for GDPR CCPA Cookie Consent Plugin AJAX Action cross-site request forgery	A vulnerability was found in iubenda All-in-one Compliance for GDPR CCPA Cookie Consent Plugin up to 3.3.2. It has been classified as problematic. This affects an unknown part of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-3911. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-0088	Swifty Page Manager Plugin up to 3.0.1 on WordPress cross-site request forgery	A vulnerability was found in Swifty Page Manager Plugin up to 3.0.1. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-0088. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-22457	XWiki CKEditor. HTMLConverter up to 1.64.2 cross-site request forgery (GHSA-6mjp-2rm6-9g85)	A vulnerability was found in XWiki CKEditor. HTMLConverter up to 1.64.2. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-22457. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-4368	WP CSV Plugin up to 1.8.0.0 on WordPress CSV Import cross-site request forgery	A vulnerability was found in WP CSV Plugin up to 1.8.0.0 and classified as problematic. Affected by this issue is some unknown functionality of the component CSV Import. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-4368. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA

CVE-2022-4103	Royal Elementor Addons Plugin up to 1.3.55 on WordPress cross-site request forgery	A vulnerability classified as problematic has been found in Royal Elementor Addons Plugin up to 1.3.55. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-4103. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-4102	Royal Elementor Addons Plugin up to 1.3.55 on WordPress cross-site request forgery	A vulnerability has been found in Royal Elementor Addons Plugin up to 1.3.55 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-4102. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-0297	pyload prior 0.5.0b3.dev31 code injection	A vulnerability was found in pyload. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation leads to code injection. This vulnerability is handled as CVE-2023-0297. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-4549	Tickera Plugin up to 3.5.0.x on WordPress Setting cross-site request forgery	A vulnerability classified as problematic has been found in Tickera Plugin up to 3.5.0.x. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-4549. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA

CVE-2023-0398	modoboa up to 2.0.3 cross-site request forgery	A vulnerability was found in modoboa up to 2.0.3. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-0398. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-0406	modoboa up to 2.0.3 cross-site request forgery	A vulnerability which was classified as problematic has been found in modoboa up to 2.0.3. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-0406. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-0403	Social Warfare Plugin up to 4.4.0 on WordPress cross-site request forgery	A vulnerability which was classified as problematic was found in Social Warfare Plugin up to 4.4.0. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-0403. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-4443	BruteBank Plugin up to 1.8 on WordPress Setting cross-site request forgery	A vulnerability classified as problematic has been found in BruteBank Plugin up to 1.8. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-4443. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA

CVE-2022-4548	Optimize images ALT Text & Names for SEO using AI Plugin Setting cross-site request forgery	A vulnerability was found in Optimize images ALT Text & Names for SEO using AI Plugin up to 2.0.7 and classified as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-4548. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-0438	modoboa up to 2.0.3 cross-site request forgery	A vulnerability classified as problematic was found in modoboa up to 2.0.3. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-0438. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-4872	Chained Products Plugin up to 2.11.x on WordPress cross-site request forgery	A vulnerability which was classified as problematic was found in Chained Products Plugin up to 2.11.x. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-4872. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-4552	FL3R FeelBox Plugin up to 8.1 on WordPress cross-site request forgery	A vulnerability has been found in FL3R FeelBox Plugin up to 8.1 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-4552. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-4553	FL3R FeelBox Plugin up to 8.1 on WordPress cross-site request forgery	A vulnerability which was classified as problematic was found in FL3R FeelBox Plugin up to 8.1. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-4553. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-4340	BookingPress Plugin up to 1.0.30 on WordPress appointment_id authorization	A vulnerability was found in BookingPress Plugin up to 1.0.30. It has been rated as problematic. This issue affects some unknown processing. The manipulation of the argument appointment_id leads to authorization bypass. The identification of this vulnerability is CVE-2022-4340. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local file inclusion attack.
CVE-2022-4298	Wholesale Market Plugin up to 2.2.0 on WordPress path traversal	A vulnerability was found in Wholesale Market Plugin up to 2.2.0. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to path traversal. This vulnerability was named CVE-2022-4298. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local file inclusion attack.
CVE-2022-4236	Welcart e-Commerce Plugin up to 2.8.4 on WordPress file access	A vulnerability was found in Welcart e-Commerce Plugin up to 2.8.4. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to files or directories accessible. This vulnerability is handled as CVE-2022-4236. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local file inclusion attack.
CVE-2022-4140	Welcart e-Commerce Plugin up to 2.8.4 on WordPress file access	A vulnerability was found in Welcart e-Commerce Plugin up to 2.8.4. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to files or directories accessible. This vulnerability is known as CVE-2022-4140. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local file inclusion attack.

CVE-2022-4109	Wholesale Market for WooCommerce Plugin up to 1.x on WordPress path traversal	A vulnerability was found in Wholesale Market for WooCommerce Plugin up to 1.x. It has been classified as problematic. Affected is an unknown function. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-4109. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local file inclusion attack.
CVE-2022-44036	b2evolution 7.2.5 unrestricted upload (ID 121)	A vulnerability has been found in b2evolution 7.2.5 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2022-44036. The attack can be initiated remotely. There is no exploit available. The real existence of this vulnerability is still doubted at the moment. It is recommended to change the configuration settings.	Protected by core rules	Detected by scanner as Local file inclusion attack.
CVE-2022-4880	stakira OpenUtau prior 0.0.991 ZIP Archive VoicebankInstaller.cs VoicebankInstaller path traversal (ID 544)	A vulnerability was found in stakira OpenUtau. It has been classified as critical. This affects the function VoicebankInstaller of the file OpenUtau.Core/Classic/VoicebankInstaller.cs of the component ZIP Archive Handler. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-4880. The attack can only be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local file inclusion attack.
CVE-2022-48253	Nostromo up to 2.0 nhttpd path traversal	A vulnerability classified as critical was found in Nostromo up to 2.0. This vulnerability affects unknown code of the component nhttpd. The manipulation leads to path traversal. This vulnerability was named CVE-2022-48253. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local file inclusion attack.

CVE-2022-23532	APOC path traversal (GHSA-5v8v-gwmw-qw97)	A vulnerability classified as critical has been found in APOC. This affects an unknown part. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-23532. It is possible to initiate the attack remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Local file inclusion attack.
CVE-2022-4101	Images Optimize and Upload CF7 Plugin up to 2.1.4 on WordPress AJAX Action path traversal	A vulnerability classified as critical has been found in Images Optimize and Upload CF7 Plugin up to 2.1.4. Affected is an unknown function of the component AJAX Action Handler. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-4101. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Local file inclusion attack.
CVE-2023-0316	froxlor up to 2.0.0 path traversal	A vulnerability classified as problematic has been found in froxlor up to 2.0.0. Affected is an unknown function. The manipulation leads to path traversal: &039;\..\filename&039;. This vulnerability is traded as CVE-2023-0316. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local file inclusion attack.
CVE-2020-36651	youngerheart nodeserver nodeserver.js path traversal	A vulnerability has been found in youngerheart nodeserver and classified as critical. Affected by this vulnerability is an unknown functionality of the file nodeserver.js. The manipulation leads to path traversal. This vulnerability is known as CVE-2020-36651. Access to the local network is required for this attack. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Local file inclusion attack.

CVE-2022-45925	OpenText Content Suite Platform 22.1 requestContext information disclosure	A vulnerability classified as problematic was found in OpenText Content Suite Platform 22.1. Affected by this vulnerability is an unknown functionality. The manipulation of the argument requestContext leads to information disclosure. This vulnerability is known as CVE-2022-45925. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local file inclusion attack.
CVE-2022-47747	uber kraken up to 0.1.4 testfs path traversal (ID 333)	A vulnerability classified as problematic has been found in uber kraken up to 0.1.4. Affected is an unknown function of the component testfs. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-47747. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Local file inclusion attack.
CVE-2022-46959	Sonic 1.0.4 /admin/backups /work-dir path traversal (ID 56)	A vulnerability has been found in Sonic 1.0.4 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/backups/work-dir. The manipulation leads to path traversal. This vulnerability is known as CVE-2022-46959. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Local file inclusion attack.
CVE-2022-31706	VMware vRealize Log Insight path traversal (VMSA-2023-0001)	A vulnerability classified as critical has been found in VMware vRealize Log Insight. This affects an unknown part. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-31706. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local file inclusion attack.
CVE-2022-47615	LMS Plugin up to 4.1.7.3.2 on WordPress file inclusion	A vulnerability was found in LMS Plugin up to 4.1.7.3.2. It has been classified as critical. This affects an unknown part. The manipulation leads to file inclusion. This vulnerability is uniquely identified as CVE-2022-47615. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local file inclusion attack.

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage

CVE-2022-3416	WPtouch Plugin up to 4.3.44 on WordPress Image unrestricted upload	A vulnerability was found in WPtouch Plugin up to 4.3.44 and classified as problematic. This issue affects some unknown processing of the component Image Handler. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2022-3416. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by custom rules	NA
CVE-2022-47766	PopojiCMS 2.0.1 Backend Plugin unrestricted upload (ID 35)	A vulnerability which was classified as critical was found in PopojiCMS 2.0.1. Affected is an unknown function of the component Backend Plugin Handler. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2022-47766. The attack can only be initiated within the local network. There is no exploit available.	Protected by custom rules	NA
CVE-2022-0316	WeStand Theme up to 2.0 on WordPress lang_upload.php unrestricted upload	A vulnerability which was classified as critical has been found in WeStand Theme footysquare Theme aidreform Theme statfort Theme club-theme Theme kingclub-theme Theme spikes Theme spikes-black Theme soundblast Theme and bolster Theme up to 2.0. Affected by this issue is some unknown functionality of the file lang_upload.php. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2022-0316. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by custom rules	NA
CVE-2023-23314	zdir 3.2.0 SSH File /api/upload unrestricted upload (ID 90)	A vulnerability was found in zdir 3.2.0. It has been classified as critical. This affects an unknown part of the file /api/upload of the component SSH File Handler. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-23314. Access to the local network is required for this attack. There is no exploit available.	Protected by custom rules	NA

CVE-2022-48008	LimeSurvey 5.4.15 Plugin Manager unrestricted upload	A vulnerability was found in LimeSurvey 5.4.15. It has been declared as problematic. This vulnerability affects unknown code of the component Plugin Manager. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2022-48008. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by custom rules	NA
CVE-2022-40035	Rawchen blog-ssm 1.0 /uploadFileList unrestricted upload	A vulnerability which was classified as critical has been found in Rawchen blog-ssm 1.0. This issue affects some unknown processing of the file /uploadFileList. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2022-40035. Access to the local network is required for this attack. There is no exploit available.	Protected by custom rules	NA
CVE-2022-4395	Membership For WooCommerce Plugin up to 2.1.6 on WordPress unrestricted upload	A vulnerability has been found in Membership For WooCommerce Plugin up to 2.1.6 and classified as critical. This vulnerability affects unknown code. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2022-4395. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by custom rules	NA

HTTP Request Smuggling Vulnerability

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-41721	h2c Package MaxBytesHandler request smuggling	A vulnerability was found in h2c Package and classified as critical. Affected by this issue is the function MaxBytesHandler. The manipulation leads to http request smuggling. This vulnerability is handled as CVE-2022-41721. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as HTTP smuggling attack.

XML External Entity Vulnerability

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage

CVE-2023-23595	BlueCat Device Registration Portal 2.2 xml external entity reference	A vulnerability which was classified as problematic has been found in BlueCat Device Registration Portal 2.2. Affected by this issue is some unknown functionality. The manipulation leads to xml external entity reference. This vulnerability is handled as CVE-2023-23595. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules.	Detected by scanner as XML External Entity attack.

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-34324	Sage XRT Business Exchange 12.4.302 Add Currencies/Payment Order /Transfer History sql injection	A vulnerability was found in Sage XRT Business Exchange 12.4.302 and classified as critical. This issue affects some unknown processing of the component Add Currencies/Payment Order/Transfer History. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-34324. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-4352	Qe SEO Handyman Plugin up to 1.0 on WordPress sql injection	A vulnerability classified as critical was found in Qe SEO Handyman Plugin up to 1.0. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-4352. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-4358	WP RSS by Publishers Plugin up to 0.1 on WordPress sql injection	A vulnerability was found in WP RSS by Publishers Plugin up to 0.1 and classified as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-4358. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-4359	WP RSS by Publishers Plugin up to 0.1 on WordPress sql injection	A vulnerability which was classified as critical was found in WP RSS by Publishers Plugin up to 0.1. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-4359. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

CVE-2022-4360	WP RSS by Publishers Plugin up to 0.1 on WordPress sql injection	A vulnerability was found in WP RSS by Publishers Plugin up to 0.1. It has been classified as critical. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-4360. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-4383	CBX Petition Plugin up to 1.0.3 on WordPress sql injection	A vulnerability which was classified as critical has been found in CBX Petition Plugin up to 1.0.3. Affected by this issue is some unknown functionality. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-4383. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-4230	WP Statistics Plugin up to 13.2.8 sql injection	A vulnerability which was classified as critical was found in WP Statistics Plugin up to 13.2.8. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-4230. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-4371	Web Invoice Plugin up to 2.1.3 on WordPress Configuration sql injection	A vulnerability has been found in Web Invoice Plugin up to 2.1.3 and classified as critical. This vulnerability affects unknown code of the component Configuration Handler. The manipulation leads to sql injection. This vulnerability was named CVE-2022-4371. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-4059	Cryptocurrency Widgets Pack Plugin up to 1.8.1 on WordPress sql injection	A vulnerability which was classified as critical was found in Cryptocurrency Widgets Pack Plugin up to 1.8.1. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-4059. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

CVE-2022-4547	Conditional Payment Methods for WooCommerce Plugin sql injection	A vulnerability was found in Conditional Payment Methods for WooCommerce Plugin up to 1.0 and classified as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-4547. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-4297	WP AutoComplete Search Plugin up to 1.0.4 on WordPress sql injection	A vulnerability was found in WP AutoComplete Search Plugin up to 1.0.4. It has been classified as critical. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-4297. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-4351	Qe SEO Handyman Plugin up to 1.0 on WordPress sql injection	A vulnerability classified as critical has been found in Qe SEO Handyman Plugin up to 1.0. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-4351. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-4049	WP User Plugin up to 7.0 on WordPress sql injection	A vulnerability which was classified as critical has been found in WP User Plugin up to 7.0. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-4049. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-3860	Visual Email Designer for WooCommerce Plugin up to 1.7.1 on WordPress sql injection	A vulnerability was found in Visual Email Designer for WooCommerce Plugin up to 1.7.1 and classified as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-3860. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.

CVE-2022-4099	Joy Of Text Lite Plugin up to 2.3.0 on WordPress sql injection	A vulnerability has been found in Joy Of Text Lite Plugin up to 2.3.0 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-4099. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-3241	Build App Online Plugin up to 1.0.18 on WordPress sql injection	A vulnerability was found in Build App Online Plugin up to 1.0.18 and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-3241. The attack needs to be approached within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-38627	Nortek Linear eMerge E3 up to 0.32-09c idt sql injection	A vulnerability classified as critical has been found in Nortek Linear eMerge E3 up to 0.32-09c. This affects an unknown part. The manipulation of the argument idt leads to sql injection. This vulnerability is uniquely identified as CVE-2022-38627. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-40049	SourceCodester Theme Park Ticketing System 1.0 /tpts/manage_user.php id information disclosure	A vulnerability classified as problematic has been found in SourceCodester Theme Park Ticketing System 1.0. This affects an unknown part of the file /tpts/manage_user.php. The manipulation of the argument id leads to information disclosure. This vulnerability is uniquely identified as CVE-2022-40049. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

CVE-2022-47790	SourceCodester Dynamic Transaction Queuing System 1.0 index.php id sql injection	A vulnerability classified as critical has been found in SourceCodester Dynamic Transaction Queuing System 1.0. Affected is an unknown function of the file /queuing /index.phppagedisplay. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-47790. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-47859	SourceCodester Lead Management System 1.0 changePassword.php user_id sql injection	A vulnerability was found in SourceCodester Lead Management System 1.0. It has been classified as critical. This affects an unknown part of the file changePassword. php. The manipulation of the argument user_id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-47859. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-22959	WebChess up to 1.0.0.rc2 mainmenu.php txtFirstName /txtLastName sql injection	A vulnerability classified as critical has been found in WebChess up to 1.0.0.rc2. This affects an unknown part of the file mainmenu.php. The manipulation of the argument txtFirstName/txtLastName leads to sql injection. This vulnerability is uniquely identified as CVE-2023-22959. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-47866	SourceCodester Lead Management System 1.0 removeBrand.php id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Lead Management System 1.0. This issue affects some unknown processing of the file removeBrand.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-47866. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-47865	SourceCodester Lead Management System 1.0 removeOrder.php id sql injection	A vulnerability classified as critical was found in SourceCodester Lead Management System 1.0. This vulnerability affects unknown code of the file removeOrder.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-47865. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

CVE-2022-47861	SourceCodester Lead Management System 1.0 removeLead.php id sql injection	A vulnerability was found in SourceCodester Lead Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file removeLead.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-47861. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-47864	SourceCodester Lead Management System 1.0 removeCategories.php id sql injection	A vulnerability classified as critical was found in SourceCodester Lead Management System 1.0. Affected by this vulnerability is an unknown functionality of the file removeCategories.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-47864. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-47860	SourceCodester Lead Management System 1.0 removeProduct.php id sql injection	A vulnerability was found in SourceCodester Lead Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file removeProduct.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-47860. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-47862	SourceCodester Lead Management System 1.0 ajax_represent.php customer_id sql injection	A vulnerability classified as critical has been found in SourceCodester Lead Management System 1.0. Affected is an unknown function of the file ajax_represent.php. The manipulation of the argument customer_id leads to sql injection. This vulnerability is traded as CVE-2022-47862. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

CVE-2023-0244	TuziCMS 2.0.6 KefuController.class.php delall id sql injection	A vulnerability classified as critical was found in TuziCMS 2.0.6. This vulnerability affects the function delall of the file \App\Manage\Controller\KefuController.class.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-0244. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-0245	SourceCodester Online Flight Booking Management System add_contestant.php add_contestant sql injection	A vulnerability which was classified as critical has been found in SourceCodester Online Flight Booking Management System. This issue affects some unknown processing of the file add_contestant.php. The manipulation of the argument add_contestant leads to sql injection. The identification of this vulnerability is CVE-2023-0245. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-0243	TuziCMS 2.0.6 Article Module ArticleController.class.php index id sql injection	A vulnerability classified as critical has been found in TuziCMS 2.0.6. This affects the function index of the file App\Manage\Controller\ArticleController.class.php of the component Article Module. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-0243. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-46471	Online Health Care System 1.0 consulting_detail.php consulting_id sql injection	A vulnerability which was classified as critical was found in Online Health Care System 1.0. This affects an unknown part of the file /healthcare/Admin/consulting_detail.php. The manipulation of the argument consulting_id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-46471. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

CVE-2022-46956	Dynamic Transaction Queuing System 1.0 /admin /manage_user.php id sql injection	A vulnerability which was classified as critical was found in Dynamic Transaction Queuing System 1.0. This affects an unknown part of the file /admin/manage_user.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-46956. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-46623	Judging Management System 1.0.0 username sql injection	A vulnerability was found in Judging Management System 1.0.0. It has been classified as critical. This affects an unknown part. The manipulation of the argument username leads to sql injection. This vulnerability is uniquely identified as CVE-2022-46623. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-0283	SourceCodester Online Flight Booking Management System POST Parameter review_search.php txtsearch sql injection	A vulnerability classified as critical has been found in SourceCodester Online Flight Booking Management System. This affects an unknown part of the file review_search.php of the component POST Parameter Handler. The manipulation of the argument txtsearch leads to sql injection. This vulnerability is uniquely identified as CVE-2023-0283. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-46953	Dynamic Transaction Queuing System 1.0 ajax.php id sql injection	A vulnerability classified as critical has been found in Dynamic Transaction Queuing System 1.0. Affected is an unknown function of the file /admin/ajax.phpactionsave_window. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-46953. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

CVE-2022-46952	Dynamic Transaction Queuing System 1.0 ajax.php id sql injection	A vulnerability was found in Dynamic Transaction Queuing System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/ajax.phpactiondelete_user. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-46952. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-0281	SourceCodester Online Flight Booking Management System judge_panel.php subevent_id sql injection	A vulnerability was found in SourceCodester Online Flight Booking Management System. It has been rated as critical. Affected by this issue is some unknown functionality of the file judge_panel.php. The manipulation of the argument subevent_id leads to sql injection. This vulnerability is handled as CVE-2023-0281. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-46946	Helmet Store Showroom Site 1.0 Master.php id sql injection	A vulnerability classified as critical was found in Helmet Store Showroom Site 1.0. This vulnerability affects unknown code of the file /classes/Master.phpfdelete_brand. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-46946. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-46947	Helmet Store Showroom Site 1.0 Master.php id sql injection	A vulnerability which was classified as critical has been found in Helmet Store Showroom Site 1.0. This issue affects some unknown processing of the file /classes/Master.phpfdelete_category. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-46947. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

CVE-2022-46472	Helmet Store Showroom Site 1.0 Users.php id sql injection	A vulnerability which was classified as critical has been found in Helmet Store Showroom Site 1.0. Affected by this issue is some unknown functionality of the file /hss/classes/Users. phpfdelete. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-46472. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-46502	Online Student Enrollment System 1.0 login.php username sql injection	A vulnerability has been found in Online Student Enrollment System 1.0 and classified as critical. This vulnerability affects unknown code of the file /student_enrollment/admin /login.php. The manipulation of the argument username leads to sql injection. This vulnerability was named CVE-2022-46502. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-46950	Dynamic Transaction Queuing System 1.0 ajax. php id sql injection	A vulnerability was found in Dynamic Transaction Queuing System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/ajax. phpactiondelete_window. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-46950. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-46951	Dynamic Transaction Queuing System 1.0 ajax. php id sql injection	A vulnerability was found in Dynamic Transaction Queuing System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/ajax. phpactiondelete_uploads. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-46951. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

CVE-2022-46949	Helmet Store Showroom Site 1.0 Master.php id sql injection	A vulnerability which was classified as critical was found in Helmet Store Showroom Site 1.0. Affected is an unknown function of the file /classes/Master. phpfdelete_helmet. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-46949. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-48090	Tramyardg hotel-mgmt-system 2022.4 /app/dao /CustomerDAO.php sql injection (ID 21)	A vulnerability has been found in Tramyardg hotel-mgmt-system 2022.4 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /app/dao/CustomerDAO. php. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-48090. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-46093	Hospital Management System 1.0 sql injection	A vulnerability was found in Hospital Management System 1.0. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to sql injection. This vulnerability was named CVE-2022-46093. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-23490	Survey Maker Plugin up to 3.1.1 on WordPress sql injection	A vulnerability which was classified as critical was found in Survey Maker Plugin up to 3.1.1. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-23490. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-23489	Easy Digital Downloads Plugin up to 3.1.0.3 on WordPress sql injection	A vulnerability which was classified as critical has been found in Easy Digital Downloads Plugin up to 3.1.0.3. Affected by this issue is some unknown functionality. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-23489. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.

CVE-2023-0304	SourceCodester Online Food Ordering System Signup Module admin_class.php email sql injection	A vulnerability classified as critical has been found in SourceCodester Online Food Ordering System. This affects an unknown part of the file admin_class.php of the component Signup Module. The manipulation of the argument email leads to sql injection. This vulnerability is uniquely identified as CVE-2023-0304. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-0303	SourceCodester Online Food Ordering System view_prod.php id sql injection	A vulnerability was found in SourceCodester Online Food Ordering System. It has been rated as critical. Affected by this issue is some unknown functionality of the file view_prod.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-0303. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-0305	SourceCodester Online Food Ordering System Login Module admin_class.php username sql injection	A vulnerability classified as critical was found in SourceCodester Online Food Ordering System. This vulnerability affects unknown code of the file admin_class.php of the component Login Module. The manipulation of the argument username leads to sql injection. This vulnerability was named CVE-2023-0305. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-0324	SourceCodester Online Tours & Travels Management System 1.0 admin/page-login.php email sql injection	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file admin/page-login.php. The manipulation of the argument email leads to sql injection. This vulnerability is handled as CVE-2023-0324. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-4447	Fontsy Plugin up to 1.8.6 on WordPress sql injection	A vulnerability which was classified as critical was found in Fontsy Plugin up to 1.8.6. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-4447. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

CVE-2023-0332	SourceCodester Online Food Ordering System 2.0 admin/manage_user.php id sql injection	A vulnerability was found in SourceCodester Online Food Ordering System 2.0. It has been classified as critical. Affected is an unknown function of the file admin/manage_user.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-0332. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2020-35326	inxedu 2.0.6 WebsiteImagesMapper.xml id sql injection	A vulnerability which was classified as critical has been found in inxedu 2.0.6. This issue affects some unknown processing of the file /inxedu/demo_inxedu_open/src/main/resources/mybatis/inxedu/website/WebsiteImagesMapper.xml. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2020-35326. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-47105	Jeecg-boot 3.4.4 /sys/dict/queryTableData sql injection (ID 4393)	A vulnerability classified as critical has been found in Jeecg-boot 3.4.4. This affects an unknown part of the file /sys/dict/queryTableData. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-47105. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-47745	EasyCorp ZenTao PMS up to 18.0.beta1 sql injection (ID 106)	A vulnerability has been found in EasyCorp ZenTao PMS up to 18.0.beta1 and classified as critical. This vulnerability affects unknown code. The manipulation leads to sql injection. This vulnerability was named CVE-2022-47745. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-47740	Seltmann Content Management System 6 /index.php sql injection	A vulnerability classified as critical was found in Seltmann Content Management System 6. Affected by this vulnerability is an unknown functionality of the file /index.php. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-47740. Access to the local network is required for this attack. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

CVE-2022-46887	NexusPHP up to 1.7.32 sql injection	A vulnerability has been found in NexusPHP up to 1.7.32 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-46887. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-23492	Login with Phone Number Plugin up to 1.4.1 on WordPress lwp_forgot_password ID sql injection	A vulnerability was found in Login with Phone Number Plugin up to 1.4.1 and classified as critical. Affected by this issue is the function lwp_forgot_password. The manipulation of the argument ID leads to sql injection. This vulnerability is handled as CVE-2023-23492. Access to the local network is required for this attack. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-48152	RemoteClinic 2.0 /medicines /profile.php id sql injection (ID 20)	A vulnerability which was classified as critical was found in RemoteClinic 2.0. Affected is an unknown function of the file /medicines /profile.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-48152. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-48120	Hospital Management System /search.php contact /doctor sql injection (ID 32)	A vulnerability was found in Hospital Management System. It has been classified as critical. Affected is an unknown function of the file /search.php. The manipulation of the argument contact/doctor leads to sql injection. This vulnerability is traded as CVE-2022-48120. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

CVE-2020-21152	SQL SQL Injection vulnerability in inxedu 2.0.6 /saverolefunction functionIds sql injection	A vulnerability which was classified as critical has been found in SQL SQL Injection vulnerability in inxedu 2.0.6. Affected by this issue is some unknown functionality of the file /saverolefunction. The manipulation of the argument functionIds leads to sql injection. This vulnerability is handled as CVE-2020-21152. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2020-29297	tourist5 Online-food-ordering-system 1.0 sql injection	A vulnerability which was classified as critical was found in tourist5 Online-food-ordering-system 1.0. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2020-29297. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-22630	IzyBat Orange Casiers prior 20221102_1 getCasier.php taille sql injection (GHSA-j94f-5cg6-6j9j)	A vulnerability classified as critical was found in IzyBat Orange Casiers. This vulnerability affects unknown code of the file getCasier.php. The manipulation of the argument taille leads to sql injection. This vulnerability was named CVE-2023-22630. Access to the local network is required for this attack. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-23331	Amano Xoffice Parking Solutions 7.1.3879 sql injection	A vulnerability classified as critical has been found in Amano Xoffice Parking Solutions 7.1.3879. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-23331. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-45808	LearnPress Plugin up to 4.1.7.3.2 on WordPress sql injection	A vulnerability was found in LearnPress Plugin up to 4.1.7.3.2. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to sql injection. This vulnerability was named CVE-2022-45808. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.

CVE-2023-0516	SourceCodester Online Tours & Travels Management System 1.0 Parameter user /forget_password.php email sql injection	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0. It has been classified as critical. Affected is an unknown function of the file user/forget_password.php of the component Parameter Handler. The manipulation of the argument email leads to sql injection. This vulnerability is traded as CVE-2023-0516. Access to the local network is required for this attack. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-0515	SourceCodester Online Tours & Travels Management System 1.0 Parameter forget_password.php email sql injection	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0 and classified as critical. This issue affects some unknown processing of the file admin /forget_password.php of the component Parameter Handler. The manipulation of the argument email leads to sql injection. The identification of this vulnerability is CVE-2023-0515. The attack needs to be initiated within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-44297	SiteServer CMS 7.1.3 sql injection (ID 3490)	A vulnerability has been found in SiteServer CMS 7.1.3 and classified as critical. This vulnerability affects unknown code. The manipulation leads to sql injection. This vulnerability was named CVE-2022-44297. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-0532	SourceCodester Online Tours & Travels Management System 1.0 disapprove_user.php id sql injection	A vulnerability classified as critical was found in SourceCodester Online Tours & Travels Management System 1.0. Affected by this vulnerability is an unknown functionality of the file admin /disapprove_user.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-0532. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

CVE-2022-44298	SiteServer CMS 7.1.3 sql injection (ID 3492)	A vulnerability was found in SiteServer CMS 7.1.3. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-44298. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-0562	PHPGurukul Bank Locker Management System 1.0 Login index.php username sql injection	A vulnerability was found in PHPGurukul Bank Locker Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file index.php of the component Login. The manipulation of the argument username leads to sql injection. This vulnerability is handled as CVE-2023-0562. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-0561	SourceCodester Online Tours & Travels Management System 1.0 /user/s.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Online Tours & Travels Management System 1.0. Affected is an unknown function of the file /user/s.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-0561. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-0560	SourceCodester Online Tours & Travels Management System 1.0 admin/practice_pdf.php id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Online Tours & Travels Management System 1.0. This issue affects some unknown processing of the file admin/practice_pdf.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2023-0560. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

CVE-2023-0570	SourceCodester Online Tours & Travels Management System 1.0 payment_operation.php booking_id sql injection	A vulnerability which was classified as critical was found in SourceCodester Online Tours & Travels Management System 1.0. This affects an unknown part of the file user\operations\payment_operation.php. The manipulation of the argument booking_id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-0570. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Cross- Site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0028	linagora twake prior 2023. Q1.1200+ cross site scripting	A vulnerability was found in linagora twake. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-0028. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2021-41823	Kemp LoadMaster 7.2.54.1 Web Application Firewall protection mechanism	A vulnerability has been found in Kemp LoadMaster 7.2.54.1 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Web Application Firewall. The manipulation leads to protection mechanism failure. This vulnerability is known as CVE-2021-41823. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-34323	XRT Business Exchange 12.4.302 Display Model DOWNLOADFRS cross site scripting	A vulnerability was found in XRT Business Exchange 12.4.302. It has been rated as problematic. Affected by this issue is some unknown functionality in the library /OnlineBanking/cgi/isapi.dll /DOWNLOADFRS of the component Display Model Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2022-34323. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-34322	Sage Enterprise Intelligence 2021 R1.1 Notification cross site scripting	A vulnerability was found in Sage Enterprise Intelligence 2021 R1.1. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Notification Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2022-34322. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-40711	PrimeKey EJBCA 7.9.0.2 End Entity Section cross site scripting	A vulnerability was found in PrimeKey EJBCA 7.9.0.2 and classified as problematic. Affected by this issue is some unknown functionality of the component End Entity Section. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2022-40711. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-37787	WeBankPartners WeCube 3.2.2 Plugin Database Execution Page cross site scripting (ID 2328)	A vulnerability was found in WeBankPartners WeCube 3.2.2. It has been classified as problematic. This affects an unknown part of the component Plugin Database Execution Page. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2022-37787. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4484	Super Socializer Plugin up to 7.13.43 on WordPress Shortcode cross site scripting	A vulnerability which was classified as problematic has been found in Super Socializer Plugin up to 7.13.43. This issue affects some unknown processing of the component Shortcode Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2022-4484. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4663	Members Import Plugin up to 1.4.2 on WordPress cross site scripting	A vulnerability was found in Members Import Plugin up to 1.4.2. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2022-4663. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-4482	Carousel, Slider, Gallery by WP Carousel Plugin up to 2.5.2 on WordPress Shortcode cross site scripting	A vulnerability was found in Carousel Slider Gallery by WP Carousel Plugin up to 2.5.2. It has been rated as problematic. This issue affects some unknown processing of the component Shortcode Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2022-4482. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0038	Survey Maker Plugin up to 3.1.3 on WordPress cross site scripting	A vulnerability was found in Survey Maker Plugin up to 3.1.3 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-0038. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4624	Ticker, Grid, List, Table & Filter Views Plugin up to 3.3.7 on WordPress Shortcode cross site scripting	A vulnerability has been found in Ticker Grid List Table & Filter Views Plugin up to 3.3.7 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Shortcode Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2022-4624. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4545	Sitemap Plugin up to 4.3 on WordPress Shortcode cross site scripting	A vulnerability classified as problematic was found in Sitemap Plugin up to 4.3. This vulnerability affects unknown code of the component Shortcode Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2022-4545. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-4142	Filter Gallery Plugin up to 0.1.5 on WordPress Setting ufg_gallery_filters cross site scripting	A vulnerability was found in Filter Gallery Plugin up to 0.1.5 and classified as problematic. Affected by this issue is the function ufg_gallery_filters of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2022-4142. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4650	Notification Bar Plugin up to 1.3.5 on WordPress Shortcode cross site scripting	A vulnerability has been found in Notification Bar Plugin up to 1.3.5 and classified as problematic. This vulnerability affects unknown code of the component Shortcode Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2022-4650. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4648	Real Testimonials Plugin up to 2.5.11 on WordPress Shortcode cross site scripting	A vulnerability was found in Real Testimonials Plugin up to 2.5.11. It has been declared as problematic. This vulnerability affects unknown code of the component Shortcode Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2022-4648. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4329	Product List Widget for Woocommerce Plugin up to 1.0 on WordPress a cross site scripting	A vulnerability has been found in Product List Widget for Woocommerce Plugin up to 1.0 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument a leads to cross site scripting. This vulnerability was named CVE-2022-4329. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-4307	Pardakht DelkhahPlugin up to 2.9.2 on WordPress cross site scripting	A vulnerability classified as problematic has been found in Pardakht DelkhahPlugin up to 2.9.2. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-4307. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4668	Easy Appointments Plugin up to 3.10.7 Shortcode cross site scripting	A vulnerability classified as problematic has been found in Easy Appointments Plugin up to 3.10.7. This affects an unknown part of the component Shortcode Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2022-4668. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4627	ShiftNav Plugin up to 1.7.1 on WordPress Shortcode cross site scripting	A vulnerability was found in ShiftNav Plugin up to 1.7.1. It has been classified as problematic. Affected is an unknown function of the component Shortcode Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-4627. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4369	WP-Lister Lite for Amazon Plugin up to 2.4.3 on WordPress cross site scripting	A vulnerability was found in WP-Lister Lite for Amazon Plugin up to 2.4.3 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2022-4369. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-4362	Popup Maker Plugin up to 1.16.8 on WordPress Shortcode Attribute cross site scripting	A vulnerability has been found in Popup Maker Plugin up to 1.16.8 and classified as problematic. This vulnerability affects unknown code of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2022-4362. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4260	WP-Ban Plugin up to 1.69.0 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic was found in WP-Ban Plugin up to 1.69.0. This affects an unknown part of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2022-4260. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4256	All-in-One Addons for Elementor Plugin up to 2.4.3 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic has been found in All-in-One Addons for Elementor Plugin up to 2.4.3. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2022-4256. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4200	Login with Cognito Plugin up to 1.4.8 on WordPress Setting cross site scripting	A vulnerability classified as problematic was found in Login with Cognito Plugin up to 1.4.8. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2022-4200. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-4119	Image Optimizer, Resizer and CDN Plugin up to 6.8.0 on WordPress Setting cross site scripting	A vulnerability was found in Image Optimizer Resizer and CDN Plugin up to 6.8.0. It has been rated as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2022-4119. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4381	Popup Maker Plugin up to 1.16.8 on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in Popup Maker Plugin up to 1.16.8. It has been classified as problematic. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-4381. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-3936	Team Members Plugin up to 5.2.0 on WordPress Setting cross site scripting	A vulnerability was found in Team Members Plugin up to 5.2.0. It has been declared as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2022-3936. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4474	Easy Social Feed up to 6.3.9 on WordPress Shortcode cross site scripting	A vulnerability was found in Easy Social Feed up to 6.3.9. It has been classified as problematic. This affects an unknown part of the component Shortcode Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2022-4474. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-4114	Superio Theme on WordPress cross site scripting	A vulnerability classified as problematic has been found in Superio Theme. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2022-4114. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4198	WP Social Sharing Plugin up to 2.2 on WordPress Setting cross site scripting	A vulnerability classified as problematic has been found in WP Social Sharing Plugin up to 2.2. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-4198. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4675	Mongoose Page Plugin up to 1.8.3 on WordPress Shortcode cross site scripting	A vulnerability which was classified as problematic was found in Mongoose Page Plugin up to 1.8.3. Affected is an unknown function of the component Shortcode Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-4675. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4475	Collapse-O-Matic Plugin up to 1.8.2 on WordPress Shortcode cross site scripting	A vulnerability which was classified as problematic has been found in Collapse-O-Matic Plugin up to 1.8.2. Affected by this issue is some unknown functionality of the component Shortcode Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2022-4475. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4578	Video Conferencing with Zoom Plugin up to 4.0.9 on WordPress Shortcode cross site scripting	A vulnerability was found in Video Conferencing with Zoom Plugin up to 4.0.9 and classified as problematic. Affected by this issue is some unknown functionality of the component Shortcode Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2022-4578. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-4509	Content Control Plugin up to 1.1.9 on WordPress cross site scripting	A vulnerability was found in Content Control Plugin up to 1.1.9. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2022-4509. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-22461	sanitize-svg up to 0.3.x cross site scripting (GHSA-h857-2g56-468g)	A vulnerability classified as problematic has been found in sanitize-svg up to 0.3.x. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-22461. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-42710	Nice Linear eMerge up to 0.32-09c cross site scripting	A vulnerability was found in Nice Linear eMerge up to 0.32-09c. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2022-42710. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0087	Swifty Page Manager Plugin up to 3.0.1 on WordPress spm_plugin_options_page_tree_max_width cross site scripting	A vulnerability was found in Swifty Page Manager Plugin up to 3.0.1 and classified as problematic. This issue affects some unknown processing. The manipulation of the argument spm_plugin_options_page_tree_max_width leads to cross site scripting. The identification of this vulnerability is CVE-2023-0087. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2021-32828	Nuxeo 11.5.109 REST API cross site scripting (GHSL-2021-072)	A vulnerability which was classified as problematic has been found in Nuxeo 11.5.109. This issue affects some unknown processing of the component REST API. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2021-32828. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-44870	Maccms10 2022.1000.3032 AD Management Module Name cross site scripting (ID 986)	A vulnerability was found in Maccms10 2022.1000.3032. It has been declared as problematic. This vulnerability affects unknown code of the component AD Management Module. The manipulation of the argument Name leads to cross site scripting. This vulnerability was named CVE-2022-44870. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0108	usememos up to 0.9.x cross site scripting	A vulnerability classified as problematic has been found in usememos memos up to 0.9.x. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-0108. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0110	usememos up to 0.9.x cross site scripting	A vulnerability classified as problematic was found in usememos memos up to 0.9.x. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-0110. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0112	usememos up to 0.9.x cross site scripting	A vulnerability which was classified as problematic was found in usememos memos up to 0.9.x. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-0112. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0106	usememos up to 0.9.x cross site scripting	A vulnerability was found in usememos memos up to 0.9.x. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-0106. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2023-0111	usememos up to 0.9.x cross site scripting	A vulnerability which was classified as problematic has been found in usememos memos up to 0.9.x. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-0111. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0107	usememos up to 0.9.x cross site scripting	A vulnerability was found in usememos memos up to 0.9.x. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-0107. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-22464	ViewVC up to 1.1.29/1.2.2 cross site scripting (ID 311)	A vulnerability has been found in ViewVC up to 1.1.29/1.2.2 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-22464. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4301	Sunshine Photo Cart Plugin up to 2.9.14 on WordPress cross site scripting	A vulnerability was found in Sunshine Photo Cart Plugin up to 2.9.14. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2022-4301. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4374	Bg Bible References Plugin up to 3.8.14 on WordPress cross site scripting	A vulnerability classified as problematic has been found in Bg Bible References Plugin up to 3.8.14. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-4374. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-4392	iPanorama 360 Virtual Tour Builder Plugin up to 1.6.29 on WordPress Setting cross site scripting	A vulnerability classified as problematic has been found in iPanorama 360 Virtual Tour Builder Plugin up to 1.6.29. This affects an unknown part of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2022-4392. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4393	ImageLinks Interactive Image Builder for Plugin up to 1.5.3 on WordPress Setting cross site scripting	A vulnerability was found in ImageLinks Interactive Image Builder for Plugin up to 1.5.3. 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. This vulnerability is handled as CVE-2022-4393. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-46603	Inkdrop 5.4.1 Markdown File unrestricted upload	A vulnerability classified as problematic was found in Inkdrop 5.4.1. Affected by this vulnerability is an unknown functionality of the component Markdown File Handler. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2022-46603. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4497	Jetpack CRM Plugin up to 5.4 on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in Jetpack CRM Plugin up to 5.4. It has been classified as problematic. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-4497. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4196	Multi Step Form Plugin up to 1.7.7 on WordPress cross site scripting	A vulnerability was found in Multi Step Form Plugin up to 1.7.7 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2022-4196. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-4468	WP Recipe Maker Plugin up to 8.6.0 on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in WP Recipe Maker Plugin up to 8.6.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2022-4468. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2021-36603	Tasmota 6.5.0 Friendly Name 1 cross site scripting (ID 12221)	A vulnerability which was classified as problematic was found in Tasmota 6.5.0. This affects an unknown part. The manipulation of the argument Friendly Name 1 leads to cross site scripting. This vulnerability is uniquely identified as CVE-2021-36603. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-3855	404 to Start Plugin up to 1.6.1 on WordPress Setting cross site scripting	A vulnerability was found in 404 to Start Plugin up to 1.6.1. It has been classified as problematic. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-3855. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-22911	MediaWiki up to 1.35.8/1.38.4/1.39.0 E-Widget cross site scripting	A vulnerability has been found in MediaWiki up to 1.35.8/1.38.4/1.39.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component E-Widget. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-22911. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-42967	Caret Markdown cross site scripting	A vulnerability which was classified as problematic was found in Caret. Affected is an unknown function of the component Markdown Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-42967. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-46503	Online Student Enrollment System 1.0 /admin/register.php name cross site scripting	A vulnerability was found in Online Student Enrollment System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/register.php. The manipulation of the argument name leads to cross site scripting. This vulnerability was named CVE-2022-46503. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0246	earclink ESPCMS P8.21120101 Content cross site scripting	A vulnerability which was classified as problematic was found in earclink ESPCMS P8.21120101. Affected is an unknown function of the component Content Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-0246. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-47102	Student Study Center Management System V 1.0 name cross site scripting	A vulnerability classified as problematic was found in Student Study Center Management System V 1.0. Affected by this vulnerability is an unknown functionality. The manipulation of the argument name leads to cross site scripting. This vulnerability is known as CVE-2022-47102. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0287	ityouknow favorites-web Comment cross site scripting (I684L9)	A vulnerability was found in ityouknow favorites-web. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Comment Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-0287. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-46438	DouPHP 1.7 20221118 article_category.php description cross site scripting	A vulnerability was found in DouPHP 1.7 20221118 and classified as problematic. This issue affects some unknown processing of the file /admin/article_category.php. The manipulation of the argument description leads to cross site scripting. The identification of this vulnerability is CVE-2022-46438. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-48091	Tramyardg hotel-mgmt-system 2022.4 process_update_profile.php cross site scripting (ID 22)	A vulnerability was found in Tramyardg hotel-mgmt-system 2022.4 and classified as problematic. Affected by this issue is some unknown functionality of the file process_update_profile.php. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2022-48091. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0289	craigk5n webcalendar cross site scripting	A vulnerability was found in craigk5n webcalendar. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-0289. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0300	alfio-event http://alf.io prior 2.0-M4-2301 cross site scripting	A vulnerability was found in alfio-event http://alf.io . It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-0300. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0301	alfio-event http://alf.io prior 2.0-M4-2301 cross site scripting	A vulnerability was found in alfio-event http://alf.io . It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-0301. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-4655	Welcart e-Commerce Plugin up to 2.8.8 on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in Welcart e-Commerce Plugin up to 2.8.8 and classified as problematic. This issue affects some unknown processing of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2022-4655. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4295	Show All Comments Plugin up to 7.0.0 on WordPress cross site scripting	A vulnerability was found in Show All Comments Plugin up to 7.0.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2022-4295. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4330	WP Attachments Plugin up to 5.0.5 on WordPress Setting cross site scripting	A vulnerability was found in WP Attachments Plugin up to 5.0.5. 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. This vulnerability is handled as CVE-2022-4330. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4199	Link Library Plugin up to 7.4.0 on WordPress Setting cross site scripting	A vulnerability has been found in Link Library Plugin up to 7.4.0 and classified as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2022-4199. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-2658	WP Spell Check Plugin up to 9.12 on WordPress Ignored Words cross site scripting	A vulnerability was found in WP Spell Check Plugin up to 9.12. It has been classified as problematic. Affected is an unknown function of the component Ignored Words Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-2658. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4465	WP Video Lightbox Plugin up to 1.9.6 on WordPress Shortcode Attribute cross site scripting	A vulnerability which was classified as problematic was found in WP Video Lightbox Plugin up to 1.9.6. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-4465. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4507	Real Cookie Banner Plugin up to 3.4.9 on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in Real Cookie Banner Plugin up to 3.4.9. It has been classified as problematic. This affects an unknown part of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2022-4507. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4464	Themify Portfolio Post Plugin up to 1.2.0 on WordPress Shortcode Attribute cross site scripting	A vulnerability classified as problematic has been found in Themify Portfolio Post Plugin up to 1.2.0. This affects an unknown part of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2022-4464. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-4453	3D FlipBook Plugin up to 1.13.2 on WordPress Shortcode Attribute cross site scripting	A vulnerability classified as problematic was found in 3D FlipBook Plugin up to 1.13.2. This vulnerability affects unknown code of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2022-4453. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-3904	MonsterInsights Plugin up to 8.9.0 on WordPress Title cross site scripting	A vulnerability which was classified as problematic has been found in MonsterInsights Plugin up to 8.9.0. Affected by this issue is some unknown functionality of the component Title Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2022-3904. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4487	Easy Accordion Plugin up to 2.1.x on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in Easy Accordion Plugin up to 2.1.x and classified as problematic. Affected by this issue is some unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2022-4487. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0323	pimcore up to 10.5.13 cross site scripting	A vulnerability which was classified as problematic has been found in pimcore up to 10.5.13. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-0323. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-4508	ConvertKit Plugin up to 2.0.4 on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in ConvertKit Plugin up to 2.0.4. It has been declared as problematic. This vulnerability affects unknown code of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2022-4508. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4480	Click to Chat Plugin up to 3.18.0 on WordPress Shortcode Attribute cross site scripting	A vulnerability has been found in Click to Chat Plugin up to 3.18.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2022-4480. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4460	CodeLights Sidebar Widgets Plugin up to 1.4 on WordPress Shortcode Attribute cross site scripting	A vulnerability which was classified as problematic has been found in CodeLights Sidebar Widgets Plugin up to 1.4. This issue affects some unknown processing of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2022-4460. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0337	lirantal daloradius cross site scripting	A vulnerability was found in lirantal daloradius. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-0337. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2023-0338	lirantal daloradius cross site scripting	A vulnerability was found in lirantal daloradius. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-0338. The attack can be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-23637	IMPatienT up to 1.5.1 Ontology Builder cross site scripting (ID 101)	A vulnerability classified as problematic has been found in IMPatienT up to 1.5.1. Affected is an unknown function of the component Ontology Builder. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-23637. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-45613	Book Store Management System 1.0 /bsms_ci/index.php/book publisher cross site scripting	A vulnerability has been found in Book Store Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /bsms_ci/index.php/book. The manipulation of the argument publisher leads to cross site scripting. This vulnerability was named CVE-2022-45613. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-40704	phoronix-test-suite phoromatic_r_add_test_details.php cross site scripting (ID 650)	A vulnerability has been found in phoronix-test-suite and classified as problematic. Affected by this vulnerability is an unknown functionality of the file phoromatic_r_add_test_details.php. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2022-40704. The attack can be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-45928	OpenText Content Suite Platform 22.1 htmlFile cross site scripting	A vulnerability classified as problematic has been found in OpenText Content Suite Platform 22.1. This affects an unknown part. The manipulation of the argument htmlFile leads to cross site scripting. This vulnerability is uniquely identified as CVE-2022-45928. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-47194	Ghost 5.9.4 Post Creation cross site scripting (TALOS-2022-1686)	A vulnerability was found in Ghost 5.9.4 and classified as problematic. This issue affects some unknown processing of the component Post Creation Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2022-47194. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-46888	NexusPHP up to 1.7.32 Query Parameter cross site scripting	A vulnerability was found in NexusPHP up to 1.7.32. It has been classified as problematic. This affects an unknown part of the component Query Parameter Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2022-46888. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-47197	Ghost 5.9.4 Post Creation codeinjection_foot cross site scripting (TALOS-2022-1686)	A vulnerability was found in Ghost 5.9.4. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Post Creation Handler. The manipulation of the argument codeinjection_foot leads to cross site scripting. This vulnerability is handled as CVE-2022-47197. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-47196	Ghost 5.9.4 Post Creation codeinjection_head cross site scripting (TALOS-2022-1686)	A vulnerability was found in Ghost 5.9.4. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Post Creation Handler. The manipulation of the argument codeinjection_head leads to cross site scripting. This vulnerability is known as CVE-2022-47196. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-47195	Ghost 5.9.4 cross site scripting (TALOS-2022-1686)	A vulnerability was found in Ghost 5.9.4. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-47195. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-41441	ReQlogic 11.3 POBatch /WaitDuration cross site scripting	A vulnerability was found in ReQlogic 11.3 and classified as problematic. This issue affects some unknown processing. The manipulation of the argument POBatch /WaitDuration leads to cross site scripting. The identification of this vulnerability is CVE-2022-41441. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-23012	craigrodway classroombookings 2.6.4 Weeks.php bgcol cross site scripting (ID 52)	A vulnerability was found in craigrodway classroombookings 2.6.4. It has been declared as problematic. This vulnerability affects unknown code of the file Weeks.php. The manipulation of the argument bgcol leads to cross site scripting. This vulnerability was named CVE-2023-23012. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-23491	Quick Event Manager Plugin up to 9.7.4 on WordPress qem_ajax_calendar category cross site scripting	A vulnerability which was classified as problematic has been found in Quick Event Manager Plugin up to 9.7.4. Affected by this issue is the function qem_ajax_calendar. The manipulation of the argument category leads to cross site scripting. This vulnerability is handled as CVE-2023-23491. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-23014	InventorySystem InventorySystem.php edit_store_name/edit_active cross site scripting (ID 23)	A vulnerability which was classified as problematic was found in InventorySystem. This affects an unknown part of the file InventorySystem.php. The manipulation of the argument edit_store_name /edit_active leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-23014. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-45557	Hundredrabbits Left 7.1.5 on macOS File Name cross site scripting (ID 167)	A vulnerability which was classified as problematic has been found in Hundredrabbits Left 7.1.5. Affected by this issue is some unknown functionality of the component File Name Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2022-45557. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-45542	EyouCMS up to 1.6.0 FileManager filename cross site scripting (ID 33)	A vulnerability classified as problematic was found in EyouCMS up to 1.6.0. Affected by this vulnerability is an unknown functionality of the component FileManager. The manipulation of the argument filename leads to cross site scripting. This vulnerability is known as CVE-2022-45542. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-45538	EyouCMS up to 1.6.0 Article ENV_GOBACK_URL cross site scripting (ID 35)	A vulnerability has been found in EyouCMS up to 1.6.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Article Handler. The manipulation of the argument ENV_GOBACK_URL leads to cross site scripting. This vulnerability is known as CVE-2022-45538. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-45540	EyouCMS up to 1.6.0 Article Type name cross site scripting (ID 37)	A vulnerability was found in EyouCMS up to 1.6.0. It has been classified as problematic. This affects an unknown part of the component Article Type Handler. The manipulation of the argument name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2022-45540. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2023-23010	Ecommerce-CodeIgniter-Bootstrap add_product.php languages/trans_load cross site scripting (ID 242)	A vulnerability which was classified as problematic has been found in Ecommerce-CodeIgniter-Bootstrap. This issue affects some unknown processing of the file add_product.php. The manipulation of the argument languages/trans_load leads to cross site scripting. The identification of this vulnerability is CVE-2023-23010. The attack may be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-45558	Hundredrabbits Left 7.1.5 on macOS cross site scripting (ID 168)	A vulnerability classified as problematic has been found in Hundredrabbits Left 7.1.5. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-45558. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-45539	EyouCMS up to 1.6.0 FileManager activepath cross site scripting (ID 38)	A vulnerability was found in EyouCMS up to 1.6.0 and classified as problematic. Affected by this issue is some unknown functionality of the component FileManager. The manipulation of the argument activepath leads to cross site scripting. This vulnerability is handled as CVE-2022-45539. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-22910	MediaWiki up to 1.35.8/1.38.4/1.39.0 cross site scripting	A vulnerability was found in MediaWiki up to 1.35.8/1.38.4/1.39.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-22910. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-23024	Book Store Management System 1.0 /bsms_ci/index.php/book writer cross site scripting	A vulnerability has been found in Book Store Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /bsms_ci/index.php/book. The manipulation of the argument writer leads to cross site scripting. This vulnerability is known as CVE-2023-23024. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-45537	EyouCMS up to 1.6.0 Article ENV_LIST_URL cross site scripting (ID 34)	A vulnerability which was classified as problematic was found in EyouCMS up to 1.6.0. Affected is an unknown function of the component Article Handler. The manipulation of the argument ENV_LIST_URL leads to cross site scripting. This vulnerability is traded as CVE-2022-45537. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-45541	EyouCMS up to 1.6.0 Attribute Editor value cross site scripting (ID 36)	A vulnerability was found in EyouCMS up to 1.6.0. It has been rated as problematic. This issue affects some unknown processing of the component Attribute Editor. The manipulation of the argument value leads to cross site scripting. The identification of this vulnerability is CVE-2022-45541. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-23015	Kalkun 0.8.0 User_model.php username cross site scripting (ID 487)	A vulnerability has been found in Kalkun 0.8.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file User_model.php. The manipulation of the argument username leads to cross site scripting. This vulnerability is known as CVE-2023-23015. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4832	Store Locator Plugin up to 1.4.8 on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in Store Locator Plugin up to 1.4.8. It has been classified as problematic. This affects an unknown part of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2022-4832. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-4467	Search & Filter Plugin up to 1.2.15 on WordPress Shortcode Attribute cross site scripting	A vulnerability classified as problematic was found in Search & Filter Plugin up to 1.2.15. This vulnerability affects unknown code of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2022-4467. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4485	Page-list Plugin up to 5.2 on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in Page-list Plugin up to 5.2. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2022-4485. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4542	Compact WP Audio Player Plugin up to 1.9.7 on WordPress Shortcode Attribute cross site scripting	A vulnerability which was classified as problematic has been found in Compact WP Audio Player Plugin up to 1.9.7. This issue affects some unknown processing of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2022-4542. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4576	Easy Bootstrap Shortcode Plugin up to 4.5.4 on WordPress Shortcode Attribute cross site scripting	A vulnerability which was classified as problematic was found in Easy Bootstrap Shortcode Plugin up to 4.5.4. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-4576. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-4672	Simple Shopping Cart Plugin up to 4.6.1 on WordPress Shortcode Attribute cross site scripting	A vulnerability which was classified as problematic was found in Simple Shopping Cart Plugin up to 4.6.1. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-4672. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2021-43446	ONLYOFFICE Server 2021-11-08 Macros cross site scripting	A vulnerability which was classified as problematic was found in ONLYOFFICE Server 2021-11-08. This affects an unknown part of the component Macros Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2021-43446. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4789	WPZOOM Portfolio Plugin up to 1.2.1 on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in WPZOOM Portfolio Plugin up to 1.2.1 and classified as problematic. Affected by this issue is some unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2022-4789. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4673	Rate My Post Plugin up to 3.3.8 on WordPress Shortcode Attribute cross site scripting	A vulnerability has been found in Rate My Post Plugin up to 3.3.8 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2022-4673. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-4625	Login Logout Menu Plugin up to 1.3.x on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in Login Logout Menu Plugin up to 1.3.x. It has been classified as problematic. This affects an unknown part of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2022-4625. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-40034	Rawchen blog-ssm 1.0 notifyInfo cross site scripting	A vulnerability classified as problematic was found in Rawchen blog-ssm 1.0. Affected by this vulnerability is an unknown functionality. The manipulation of the argument notifyInfo leads to cross site scripting. This vulnerability is known as CVE-2022-40034. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0448	WP Helper Premium Plugin up to 4.2.0 on WordPress cross site scripting	A vulnerability which was classified as problematic was found in WP Helper Premium Plugin up to 4.2.0. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-0448. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-47073	Small CRM 3.0 Create Ticket Page Subject cross site scripting	A vulnerability was found in Small CRM 3.0. It has been declared as problematic. This vulnerability affects unknown code of the component Create Ticket Page. The manipulation of the argument Subject leads to cross site scripting. This vulnerability was named CVE-2022-47073. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2021-24452	W3 Total Cache Plugin up to 2.1.4 on WordPress Setting extension cross site scripting	A vulnerability was found in W3 Total Cache Plugin up to 2.1.4. It has been rated as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation of the argument extension leads to cross site scripting. The identification of this vulnerability is CVE-2021-24452. The attack may be initiated remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0488	pyload up to 0.5.0b3.dev41 cross site scripting	A vulnerability which was classified as problematic was found in pyload up to 0.5.0b3.dev41. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-0488. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0470	modoboa up to 2.0.3 cross site scripting	A vulnerability which was classified as problematic has been found in modoboa up to 2.0.3. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-0470. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2021-36686	yapi 1.9.1 Edit Page /interface/api cross site scripting (ID 2190)	A vulnerability classified as problematic was found in yapi 1.9.1. Affected by this vulnerability is an unknown functionality of the file /interface/api of the component Edit Page. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2021-36686. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-46957	SourceCodester Online Graduate Tracer System 1.0.0 cross site scripting	A vulnerability was found in SourceCodester Online Graduate Tracer System 1.0.0. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2022-46957. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0519	modoboa up to 2.0.3 cross site scripting	A vulnerability has been found in modoboa up to 2.0.3 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-0519. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-48007	Piwigo 13.4.0 identification.php User-Agent cross site scripting (ID 1835)	A vulnerability was found in Piwigo 13.4.0 and classified as problematic. Affected by this issue is some unknown functionality of the file identification.php. The manipulation of the argument User-Agent leads to cross site scripting. This vulnerability is handled as CVE-2022-48007. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-48013	Opencats 0.9.7 index.php Description/Title cross site scripting	A vulnerability has been found in Opencats 0.9.7 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /opencats/index.phpmcalendar. The manipulation of the argument Description/Title leads to cross site scripting. This vulnerability is known as CVE-2022-48013. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-48010	LimeSurvey 5.4.15 rendersidemenulink Description/Welcome-message cross site scripting	A vulnerability which was classified as problematic was found in LimeSurvey 5.4.15. Affected is an unknown function of the file /index.php/surveyAdministration/rendersidemenulinksubactionsurveytexts. The manipulation of the argument Description/Welcome-message leads to cross site scripting. This vulnerability is traded as CVE-2022-48010. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2023-0563	PHPGurukul Bank Locker Management System 1.0 Assign Locker add-locker-form.php ahname cross site scripting	A vulnerability classified as problematic has been found in PHPGurukul Bank Locker Management System 1.0. This affects an unknown part of the file add-locker-form.php of the component Assign Locker. The manipulation of the argument ahname leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-0563. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-46968	Revenue Collection System 1.0 Message /index.php cross site scripting (ID 169917)	A vulnerability classified as problematic was found in Revenue Collection System 1.0. This vulnerability affects unknown code of the file /index.phppagehelp of the component Message Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2022-46968. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0571	SourceCodester Canteen Management System 1.0 Add Customer createcustomer.php name cross site scripting	A vulnerability has been found in SourceCodester Canteen Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file createcustomer.php of the component Add Customer. The manipulation of the argument name leads to cross site scripting. This vulnerability was named CVE-2023-0571. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-46087	CloudSchool up to 3.0.1 Notification cross site scripting	A vulnerability was found in CloudSchool up to 3.0.1. It has been declared as problematic. This vulnerability affects unknown code of the component Notification Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2022-46087. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-4470	Widgets for Google Reviews Plugin up to 9.7 on WordPress Shortcode Attribute cross site scripting	A vulnerability which was classified as problematic was found in Widgets for Google Reviews Plugin up to 9.7. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-4470. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4787	Themify Shortcodes Plugin up to 2.0.7 on WordPress Shortcode Attribute cross site scripting	A vulnerability classified as problematic was found in Themify Shortcodes Plugin up to 2.0.7. This vulnerability affects unknown code of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2022-4787. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4828	Bold Timeline Lite Plugin up to 1.1.4 on WordPress Shortcode Attribute cross site scripting	A vulnerability which was classified as problematic has been found in Bold Timeline Lite Plugin up to 1.1.4. This issue affects some unknown processing of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2022-4828. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4781	Accordion Shortcodes Plugin up to 2.4.2 on WordPress Shortcode Attribute cross site scripting	A vulnerability classified as problematic has been found in Accordion Shortcodes Plugin up to 2.4.2. This affects an unknown part of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2022-4781. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-4765	Portfolio for Elementor Plugin up to 2.3.0 on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in Portfolio for Elementor Plugin up to 2.3.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2022-4765. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4667	Feedzy RSS Aggregator Plugin up to 4.1.0 on WordPress cross site scripting	A vulnerability was found in Feedzy RSS Aggregator Plugin up to 4.1.0. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-4667. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4472	Simple Sitemap Plugin up to 3.5.7 on WordPress Shortcode Attribute cross site scripting	A vulnerability which was classified as problematic has been found in Simple Sitemap Plugin up to 3.5.7. Affected by this issue is some unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2022-4472. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4651	Justified Gallery Plugin up to 1.7.0 on WordPress Shortcode Attribute cross site scripting	A vulnerability has been found in Justified Gallery Plugin up to 1.7.0 and classified as problematic. This vulnerability affects unknown code of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2022-4651. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.

CVE-2022-4654	Pricing Tables Plugin up to 3.2.2 on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in Pricing Tables Plugin up to 3.2.2 and classified as problematic. This issue affects some unknown processing of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2022-4654. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4763	Icon Widget Plugin up to 1.2. x on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in Icon Widget Plugin up to 1.2. x. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2022-4763. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4306	Panda Pods Repeater Field Plugin up to 1.5.3 on WordPress cross site scripting	A vulnerability classified as problematic was found in Panda Pods Repeater Field Plugin up to 1.5.3. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2022-4306. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.