INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

February 2023

The total zero-day vulnerabilities count for February month : 311

Command Injection	CSRF	Local File Inclusion	Http Request Smuggling	SQL Injection	XSS Injection	CRLF Injection	XXE Attack	Malicious File Upload
36	11	13	1	82	152	1	3	12

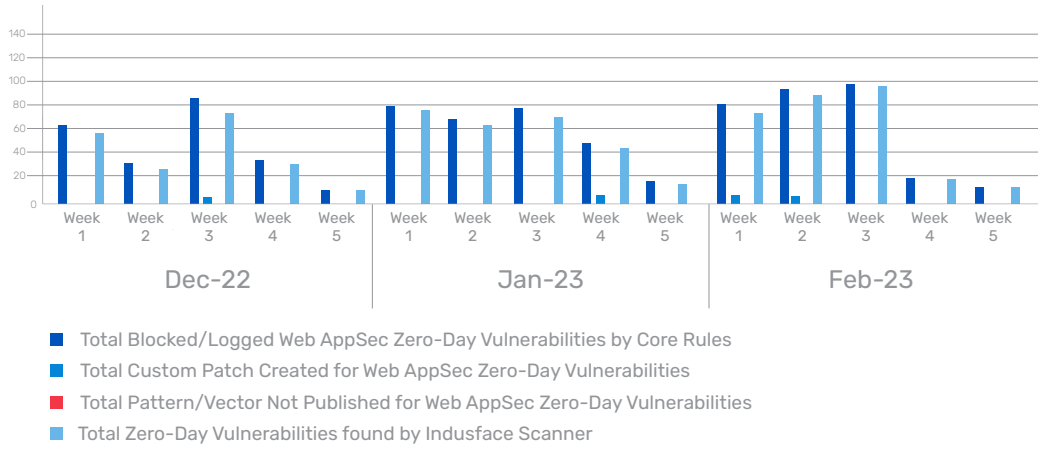
Zero-day vulnerabilities protected through core rules	300
Zero-day vulnerabilities protected through custom rules	11
Zero-day vulnerabilities for which protection can not be done	0
Zero-day vulnerabilities found by Indusface WAS	289

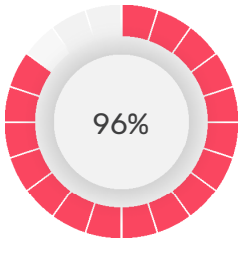
- To enable custom rules, please contact support@indusface.com
- Since the attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.

Vulnerability Trend:

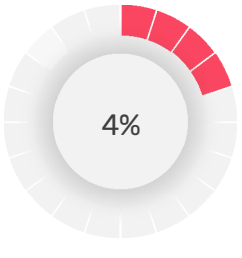
The weekly trend displays the total number of vulnerabilities discovered to the type of protection provided for the last quarter.

Weekly Vulnerability Trend

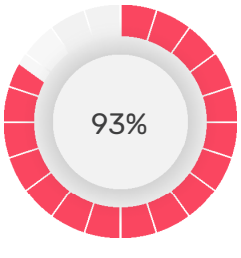




of the zero-day vulnerabilities were protected by the **core rules** in the last month.

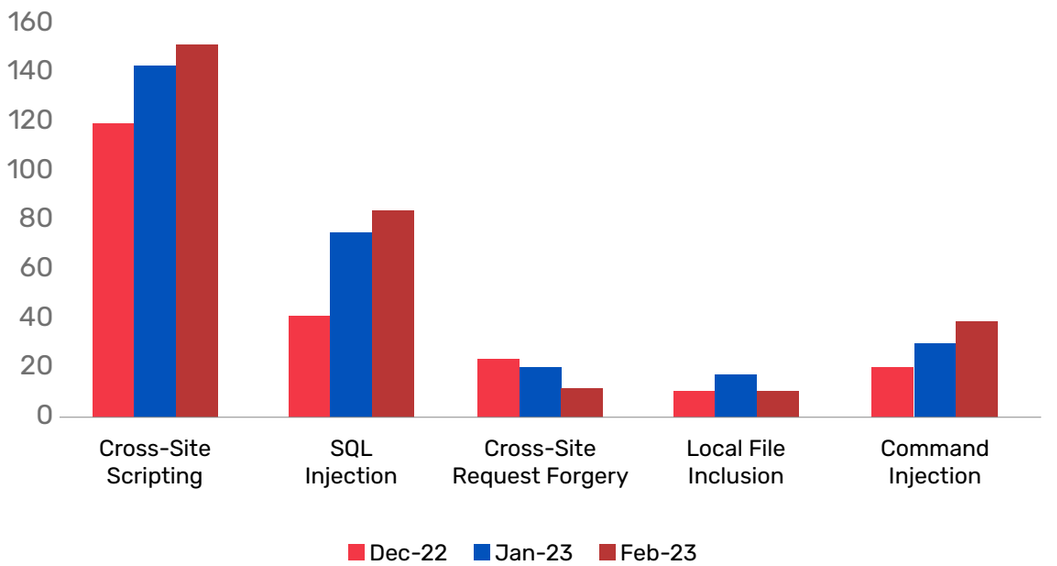


of the zero-day vulnerabilities were protected by the **custom rules** in the last month.



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

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-25906	is-http2 isH2 command injection	A vulnerability classified as critical was found in ishttp2. Affected by this vulnerability is the function isH2. The manipulation leads to command injection. This vulnerability is known as CVE-2022-25906. The attack needs to be approached locally. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-0611	TRENDnet TEW-652BRP 3.04B01 Web Management Interface get_set.ccp command injection	A vulnerability which was classified as critical has been found in TRENDnet TEW-652BRP 3.04B01. This issue affects some unknown processing of the file get_set.ccp of the component Web Management Interface. The manipulation leads to command injection. The identification of this vulnerability is CVE-2023-0611. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-0646	dst-admin 1.5.0 / home /cavesConsole command command injection	A vulnerability classified as critical was found in dstadmin 1.5.0. Affected by this vulnerability is an unknown functionality of the file /home /cavesConsole. The manipulation of the argument command leads to command injection. This vulnerability is known as CVE-2023-0646. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Command Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0647	dst-admin 1.5.0 / home /kickPlayer userId command injection	A vulnerability which was classified as critical has been found in dst-admin 1.5.0. Affected by this issue is some unknown functionality of the file /home /kickPlayer. The manipulation of the argument userId leads to command injection. This vulnerability is handled as CVE-2023-0647. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-0648	dst-admin 1.5.0 / home /masterConsole command command injection	A vulnerability which was classified as critical was found in dst-admin 1.5.0. This affects an unknown part of the file /home/masterConsole. The manipulation of the argument command leads to command injection. This vulnerability is uniquely identified as CVE-2023-0648. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-0649	dst-admin 1.5.0 / home /sendBroadcast message command injection	A vulnerability has been found in dst-admin 1.5.0 and classified as critical. This vulnerability affects unknown code of the file / home/sendBroadcast. The manipulation of the argument message leads to command injection. This vulnerability was named CVE-2023-0649. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-0640	TRENDnet TEW-652BRP 3.04b01 Web Interface ping. ccp command injection	A vulnerability was found in TRENDnet TEW-652BRP 3.04b01. It has been classified as critical. Affected is an unknown function of the file ping.ccp of the component Web Interface. The manipulation leads to command injection. This vulnerability is traded as CVE-2023-0640. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-24138	TOTOLINK CA300-PoE 6.2c. 884 NTPSyncWithHost host_time command injection	A vulnerability classified as critical has been found in TOTOLINK CA300-PoE 6.2c.884. This affects the function NTPSyncWithHost. The manipulation of the argument host_time leads to command injection. This vulnerability is uniquely identified as CVE-2023-24138. 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-24139	TOTOLINK CA300-PoE 6.2c. 884 setNetworkDiag NetDiagHost command injection	A vulnerability classified as critical was found in TOTOLINK CA300-PoE 6.2c.884. This vulnerability affects the function setNetworkDiag. The manipulation of the argument NetDiagHost leads to command injection. This vulnerability was named CVE-2023-24139. 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-2023-24140	TOTOLINK CA300-PoE 6.2c.884 setNetworkDiag NetDiagPingNum command injection	A vulnerability which was classified as critical was found in TOTOLINK CA300-PoE 6.2c.884. This affects the function setNetworkDiag. The manipulation of the argument NetDiagPingNum leads to command injection. This vulnerability is uniquely identified as CVE-2023-24140. 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-2023-24142	TOTOLINK CA300-PoE 6.2c.884 setNetworkDiag NetDiagPingSize command injection	A vulnerability which was classified as critical was found in TOTOLINK CA300-PoE 6.2c.884. Affected is the function setNetworkDiag. The manipulation of the argument NetDiagPingSize leads to command injection. This vulnerability is traded as CVE-2023-24142. 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-2023-24141	TOTOLINK CA300-PoE 6.2c.884 setNetworkDiag NetDiagPingTimeOut command injection	A vulnerability which was classified as critical has been found in TOTOLINK CA300-PoE 6.2c.884. This issue affects the function setNetworkDiag. The manipulation of the argument NetDiagPingTimeOut leads to command injection. The identification of this vulnerability is CVE-2023-24141. 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-2023-24143	TOTOLINK CA300-PoE 6.2c.884 setNetworkDiag NetDiagTracertHop command injection	A vulnerability has been found in TOTOLINK CA300-PoE 6.2c.884 and classified as critical. Affected by this vulnerability is the function setNetworkDiag. The manipulation of the argument NetDiagTracertHop leads to command injection. This vulnerability is known as CVE-2023-24143. 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-24144	TOTOLINK CA300-PoE 6.2c.884 setRebootScheCfg hour command injection	A vulnerability was found in TOTOLINK CA300-PoE 6.2c.884 and classified as critical. Affected by this issue is the function setRebootScheCfg. The manipulation of the argument hour leads to command injection. This vulnerability is handled as CVE-2023-24144. 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-2023-24146	TOTOLINK CA300-PoE 6.2c.884 setRebootScheCfg minute command injection	A vulnerability was found in TOTOLINK CA300-PoE 6.2c.884. It has been classified as critical. This affects the function setRebootScheCfg. The manipulation of the argument minute leads to command injection. This vulnerability is uniquely identified as CVE-2023-24146. 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-2023-24145	TOTOLINK CA300-PoE 6.2c.884 setUnloadUserData plugin_version command injection	A vulnerability was found in TOTOLINK CA300-PoE 6.2c.884. It has been declared as critical. This vulnerability affects the function setUnloadUserData. The manipulation of the argument plugin_version leads to command injection. This vulnerability was named CVE-2023-24145. 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-2023-24148	TOTOLINK CA300-PoE 6.2c.884 setUploadUserData FileName command injection	A vulnerability was found in TOTOLINK CA300-PoE 6.2c.884. It has been rated as critical. This issue affects the function setUploadUserData. The manipulation of the argument FileName leads to command injection. The identification of this vulnerability is CVE-2023-24148. 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-2023-24150	TOTOLINK T8 4.1.5cu MQTT Packet meshSlaveDlfw serverIp command injection	A vulnerability has been found in TOTOLINK T8 4.1.5cu and classified as critical. Affected by this vulnerability is the function meshSlaveDlfw of the component MQTT Packet Handler. The manipulation of the argument serverIp leads to command injection. This vulnerability is known as CVE-2023-24150. 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-24152	TOTOLINK T8 4.1.5cu MQTT Packet meshSlaveUpdate serverIp command injection	A vulnerability was found in TOTOLINK T8 4.1.5cu. It has been classified as critical. This affects the function meshSlaveUpdate of the component MQTT Packet Handler. The manipulation of the argument serverIp leads to command injection. This vulnerability is uniquely identified as CVE-2023-24152. 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-2023-24151	TOTOLINK T8 4.1.5cu MQTT Packet recvSlaveCloudCheckStatus ip command injection	A vulnerability was found in TOTOLINK T8 4.1.5cu and classified as critical. Affected by this issue is the function recvSlaveCloudCheckStatus of the component MQTT Packet Handler. The manipulation of the argument ip leads to command injection. This vulnerability is handled as CVE-2023-24151. 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-2023-24153	TOTOLINK T8 4.1.5cu MQTT Packet recvSlaveCloudCheckStatus version command injection	A vulnerability was found in TOTOLINK T8 4.1.5cu. It has been declared as critical. This vulnerability affects the function recvSlaveCloudCheckStatus of the component MQTT Packet Handler. The manipulation of the argument version leads to command injection. This vulnerability was named CVE-2023-24153. 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-2023-24156	TOTOLINK T8 4.1.5cu MQTT Packet recvSlaveUpgstatus ip command injection	A vulnerability was found in TOTOLINK T8 4.1.5cu. It has been rated as critical. This issue affects the function recvSlaveUpgstatus of the component MQTT Packet Handler. The manipulation of the argument ip leads to command injection. The identification of this vulnerability is CVE-2023-24156. 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-2023-24157	TOTOLINK T8 4.1.5cu MQTT Packet updateWifiInfo serverIp command injection	A vulnerability classified as critical has been found in TOTOLINK T8 4.1.5cu. Affected is the function updateWifiInfo of the component MQTT Packet Handler. The manipulation of the argument serverIp leads to command injection. This vulnerability is traded as CVE-2023-24157. 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-24154	TOTOLINK T8 4.1.5cu setUpgradeFW slaveIpList command injection	A vulnerability classified as critical has been found in TOTOLINK T8 4.1.5cu. Affected is the function setUpgradeFW. The manipulation of the argument slaveIpList leads to command injection. This vulnerability is traded as CVE-2023-24154. The attack needs to be initiated 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-2022-25855	create-choo-app3 devInstall command injection (SNYKJS-CREATE-CHOOAPP3-3157951)	A vulnerability has been found in create-choo-app3 and classified as critical. This vulnerability affects the function devInstall. The manipulation leads to command injection. This vulnerability was named CVE-2022-25855. An attack has to be approached locally. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2022-25853	semver-tags getGitTagsRemote command injection	A vulnerability was found in semver-tags and classified as critical. This issue affects the function getGitTagsRemote. The manipulation leads to command injection. The identification of this vulnerability is CVE-2022-25853. Local access is required to approach this attack. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-24276	TOTOLINK A7100RU 7.4cu.2313_B20191024 delStaticDhcpRules country command injection	A vulnerability which was classified as critical was found in TOTOLINK A7100RU 7.4cu.2313_B20191024. Affected is an unknown function of the file setting/delStaticDhcpRules. The manipulation of the argument country leads to command injection. This vulnerability is traded as CVE-2023-24276. 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-2023-22643	libzypp-plugin-appdata on SuSE REPO os command injection	A vulnerability has been found in libzypp-pluginappdata and classified as critical. This vulnerability affects unknown code of the component REPO Handler. The manipulation leads to os command injection. This vulnerability was named CVE-2023-22643. 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-23333	SolarView Compact up to 6.00 Restrictions downloader.php command injection	A vulnerability classified as critical has been found in SolarView Compact up to 6.00. Affected is an unknown function of the file downloader.php of the component Restrictions Handler. The manipulation leads to command injection. This vulnerability is traded as CVE-2023-23333. 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-2022-45768	Edimax N300 BR428nS v3 formWlanMP command injection	A vulnerability which was classified as critical was found in Edimax N300 BR-428nS v3. This affects the function formWlanMP. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2022-45768. 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-2022-45699	APSystems ECU-R 5203 Administration Interface timezone command injection	A vulnerability has been found in APSystems ECU-R 5203 and classified as very critical. This vulnerability affects unknown code of the component Administration Interface. The manipulation of the argument timezone leads to command injection. This vulnerability was named CVE-2022-45699. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-24816	IPython up to 8.0.x on Windows set_term_title os command injection (GHSA-29gw-9793-fvw7)	A vulnerability was found in IPython up to 8.0.x. It has been rated as critical. Affected by this issue is the function set_term_title. The manipulation leads to os command injection. This vulnerability is handled as CVE-2023-24816. 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-2023-0127	D-Link DWL-2600AP 4.2.0.17 firmware_update command injection	A vulnerability was found in D-Link DWL-2600AP 4.2.0.17. It has been rated as critical. This issue affects the function firmware_update. The manipulation leads to command injection. The identification of this vulnerability is CVE-2023-0127. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0792	thorsten phpmyfaq up to 3.1.10 code injection	A vulnerability classified as critical was found in thorsten phpmyfaq up to 3.1.10. This vulnerability affects unknown code. The manipulation leads to code injection. This vulnerability was named CVE-2023-0792. Access to the local network is required for this attack to succeed. 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-2023-24238	TOTOLINK A7100RU 7.4cu.2313_B20191024 delStaticDhcpRules city command injection	A vulnerability which was classified as critical has been found in TOTOLINK A7100RU 7.4cu.2313_B20191024. Affected by this issue is some unknown functionality of the file setting /delStaticDhcpRules. The manipulation of the argument city leads to command injection. This vulnerability is handled as CVE-2023-24238. 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-2023-24236	TOTOLINK A7100RU 7.4cu.2313_B20191024 delStaticDhcpRules province command injection	A vulnerability classified as critical was found in TOTOLINK A7100RU 7.4cu.2313_B20191024. Affected by this vulnerability is an unknown functionality of the file setting/delStaticDhcpRules. The manipulation of the argument province leads to command injection. This vulnerability is known as CVE-2023-24236. 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

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0642	squidex up to 7.3.x cross-site request forgery	A vulnerability was found in squidex up to 7.3.x. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-0642. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-47131	Academy LMS up to 5.9 crosssite request forgery	A vulnerability was found in Academy LMS up to 5.9. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-47131. 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-2022-47130	Academy LMS up to 5.9 crosssite request forgery	A vulnerability which was classified as problematic was found in Academy LMS up to 5.9. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-47130. 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-2021-36570	Fuel CMS 1.4.13 /permissions /delete/2--- cross-site request forgery (ID 579)	A vulnerability was found in Fuel CMS 1.4.13. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /permissions/delete/2---. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2021-36570. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2021-36569	Fuel CMS 1.4.13 / users/delete/2 cross-site request forgery (ID 578)	A vulnerability was found in Fuel CMS 1.4.13. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file / users/delete/2. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2021-36569. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-36443	imcat 5.4 cross-site request forgery	A vulnerability was found in imcat 5.4. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2021-36443. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-0674	XXL-JOB 2.3.1 New Password /user/updatePwd cross-site request forgery	A vulnerability which was classified as problematic has been found in XXL-JOB 2.3.1. Affected by this issue is some unknown functionality of the file /user /updatePwd of the component New Password Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-0674. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2022-2933	0mk Shortener Plugin up to 0.2 on WordPress zeromk_options_page zeromk_user/zeromk_apikluc cross-site request forgery	A vulnerability classified as problematic has been found in 0mk Shortener Plugin up to 0.2. Affected is the function zeromk_options_page. The manipulation of the argument zeromk_user/zeromk_apikluc leads to cross-site request forgery. This vulnerability is traded as CVE-2022-2933. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-0735	wallabag up to 2.5.3 cross-site request forgery	A vulnerability has been found in wallabag up to 2.5.3 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-0735. 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-2022-4745	WP Customer Area Plugin up to 8.1.3 on WordPress cross-site request forgery	A vulnerability was found in WP Customer Area Plugin up to 8.1.3. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-4745. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-4386	Intuitive Custom Post Order Plugin up to 3.1.3 on Word-Press AJAX Action update-menu-order cross-site request forgery	A vulnerability was found in Intuitive Custom Post Order Plugin up to 3.1.3. It has been declared as problematic. This vulnera-bility affects the function update-menu-order of the component AJAX Ac-tion Handler. The manip-ulation leads to cross-site request forgery. This vulnerability was named CVE-2022-4386. The attack can be initiated remotely. There is no ex-ploit available.	Protected by core rules	Detected by scanner as Cross-Site Re-quest Forgery attack.

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-48094	Imxcms 1.41 Tem-plateAction. class. php path traversal	A vulnerability was found in Imxcms 1.41. It has been rated as problematic. This issue affects some unknown processing of the file TemplateAction.class. php. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-48094. 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-2022-47768	Serenissima Infor-matica Fast Checkin 1.0 path traversal	A vulnerability was found in Serenissima Informat-ica Fast Checkin 1.0. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-47768. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2021-37317	ASUS AC68U prior 3.0.0.4.386.41634 path traversal	A vulnerability was found in ASUS AC68U. It has been classified as critical. Affected is an unknown function. The manipulation leads to path traversal. This vulnerability is traded as CVE-2021-37317. 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-2021-36425	PHPCMS 1.9.25 act_ftptakeover. php unlink file path traversal (ID 311)	A vulnerability was found in PHPCMS 1.9.25. It has been rated as critical. This issue affects the function unlink of the file include/ inc_act /act_ftptakeover. php. The manipulation of the argument file leads to path traversal. The identification of this vulnerability is CVE-2021-36425. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-47762	Gin-Vue-Admin up to 2.5.4 Download Module path traversal (ID 1309)	A vulnerability was found in Gin-Vue-Admin up to 2.5.4 and classified as critical. Affected by this issue is some unknown functionality of the component Download Module. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-47762. 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 Local File Inclusion attack.
CVE-2023-24815	Vert.x-Web on Windows path traversal (GHSA-53jx-vvf9-4x38)	A vulnerability was found in Vert.x-Web and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-24815. The attack may 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 Local File Inclusion attack.
CVE-2023-0159	Extensive VC Addons for WPBakery Page Builder Plugin Template path traversal	A vulnerability which was classified as critical was found in Extensive VC Addons for WPBakery Page Builder Plugin up to 1.8.x. This affects an unknown part of the component Template Handler. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-0159. 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 Local File Inclusion attack.
CVE-2022-25937	glance up to 3.0.8 path traversal	A vulnerability was found in glance up to 3.0.8. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-25937. 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-2023-24804	ownCloud App up to 2.x on Android Internal File path traversal (GHSL-2022-059)	A vulnerability classified as problematic was found in ownCloud App up to 2.x. This vulnerability affects unknown code of the component Internal File Handler. The manipulation leads to path traversal. This vulnerability was named CVE-2023-24804. An attack has 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 Local File Inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-48323	Sunlogin Sunflower Simplified 1.0.1.43315 HTTP Request /check cmd path traversal	A vulnerability classified as critical has been found in Sunlogin Sunflower Simplified 1.0.1.43315. This affects an unknown part of the file /check of the component HTTP Request Handler. The manipulation of the argument cmd with the input ping../ leads to path traversal. This vulnerability is uniquely identified as CVE-2022-48323. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-22855	Kardex Mlog MCC 5.7.12+0-a203c2a213-master Web Interface Path. Combine path traversal	A vulnerability classified as critical has been found in Kardex Mlog MCC 5.7.12+0-a203c2a213-master. Affected is the function Path.Combine of the component Web Interface Handler. The manipulation leads to path traversal. This vulnerability is traded as CVE-2023-22855. It is possible to launch the attack remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-22629	TitanFTP up to 1.94.1205 movefile newPath path traversal	A vulnerability has been found in TitanFTP up to 1.94.1205 and classified as critical. This vulnerability affects the function movefile. The manipulation of the argument newPath leads to path traversal. This vulnerability was named CVE-2023-22629. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2022-44299	SiteServerCMS 7.1.3 information disclosure (ID 3491)	A vulnerability was found in SiteServerCMS 7.1.3. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to information disclosure. The identification of this vulnerability is CVE-2022-44299. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.

HTTP Request Smuggling Vulnerability

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-25725	HAProxy up to 2.7.2 Header Field request smuggling	A vulnerability was found in HAProxy up to 2.7.2 and classified as critical. Affected by this issue is some unknown functionality of the component Header Field Handler. The manipulation leads to http request smuggling. This vulnerability is handled as CVE-2023-25725. 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.

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-24241	Forget Heart Message Box 1.1 /admin/loginpost.php name sql injection	A vulnerability was found in Forget Heart Message Box 1.1. It has been classified as critical. This affects an unknown part of the file /admin /loginpost.php. The manipulation of the argument name leads to sql injection. This vulnerability is uniquely identified as CVE-2023-24241. 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-2023-24956	Forget Heart Message Box 1.1 /cha.php name sql injection	A vulnerability was found in Forget Heart Message Box 1.1. It has been declared as critical. This vulnerability affects unknown code of the file /cha.php. The manipulation of the argument name leads to sql injection. This vulnerability was named CVE-2023-24956. 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-2022-47770	Serenissima Informatica Fast Checkin 1.0 sql injection	A vulnerability classified as critical has been found in Serenissima Informatica Fast Checkin 1.0. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-47770. 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-2022-45297	tlfyyds EQ up to 2.2.0 UserPwd sql injection	A vulnerability has been found in tlfyyds EQ up to 2.2.0 and classified as critical. This vulnerability affects unknown code. The manipulation of the argument UserPwd leads to sql injection. This vulnerability was named CVE-2022-45297. 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-2022-46965	totadministrativemandate Module up to 1.7.0 on PrestaShop sql injection (GHSA-hg7m-23j3-rf56)	A vulnerability was found in totadministrativemandate Module up to 1.7.0 and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-46965. 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-2021-37316	ASUS AC68U prior 3.0.0.4.386.41634 Cloud Disk sql injection	A vulnerability was found in ASUS AC68U. It has been classified as critical. Affected is an unknown function of the component Cloud Disk. The manipulation leads to sql injection. This vulnerability is traded as CVE-2021-37316. 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 SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0663	Calendar Event Management System 2.3.0 Login Page name/pwd sql injection	A vulnerability was found in Calendar Event Management System 2.3.0. It has been rated as critical. This issue affects some unknown processing of the component Login Page. The manipulation of the argument name/pwd leads to sql injection. The identification of this vulnerability is CVE-2023-0663. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2021-36484	JIZHICMS 1.9.5 Article sql injection	A vulnerability was found in JIZHICMS 1.9.5. It has been classified as critical. Affected is an unknown function of the component Article Handler. The manipulation leads to sql injection. This vulnerability is traded as CVE-2021-36484. 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-2021-36434	jocms 0.8 getmask.php jo_json_check sql injection	A vulnerability classified as critical was found in jocms 0.8. Affected by this vulnerability is the function jo_json_check of the file jocms /apps/mask/inc/getmask.php. The manipulation leads to sql injection. This vulnerability is known as CVE-2021-36434. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2021-36433	jocms 0.8 jocms/apps/mask /mask.php jo_delete_mask sql injection	A vulnerability which was classified as critical has been found in jocms 0.8. This issue affects the function jo_delete_mask of the file jocms/apps/mask/mask.php. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2021-36433. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2021-36432	jocms 0.8 jocms/apps/mask /mask.php jo_set_mask sql injection	A vulnerability classified as critical was found in jocms 0.8. This vulnerability affects the function jo_set_mask of the file jocms/apps/mask /mask.php. The manipulation leads to sql injection. This vulnerability was named CVE-2021-36432. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2021-36431	jocms 0.8 mask.php jo_json_check sql injection	A vulnerability classified as critical has been found in jocms 0.8. Affected is the function jo_json_check of the file jocms/apps/mask/inc /mask.php. The manipulation leads to sql injection. This vulnerability is traded as CVE-2021-36431. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-36503	native-php-cms 1.0 /list.php cat sql injection	A vulnerability which was classified as critical was found in native-php-cms 1.0. Affected is an unknown function of the file /list.php. The manipulation of the argument cat leads to sql injection. This vulnerability is traded as CVE-2021-36503. 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-2021-37497	PbootCMS 3.0.5 GET Request sql injection	A vulnerability was found in PbootCMS 3.0.5 and classified as critical. This issue affects some unknown processing of the component GET Request Handler. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2021-37497. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-48114	y_project RuoYi up to 4.7.5 /tool/gen/createTable sql injection	A vulnerability was found in y_project RuoYi up to 4.7.5 and classified as critical. Affected by this issue is some unknown functionality of the file /tool/gen/createTable. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-48114. 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-2023-0675	Calendar Event Management System 2.3.0 start/end sql injection	A vulnerability which was classified as critical was found in Calendar Event Management System 2.3.0. This affects an unknown part. The manipulation of the argument start/end leads to sql injection. This vulnerability is uniquely identified as CVE-2023-0675. 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-2022-4681	Hide My WP Plugin up to 6.2.8 on WordPress sql injection	A vulnerability was found in Hide My WP Plugin up to 6.2.8 and classified as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-4681. 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-2023-0679	SourceCodester Canteen Management System 1.0 removeUser.php id sql injection	A vulnerability was found in SourceCodester Canteen Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file removeUser.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-0679. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-24197	SourceCodester Online Food Ordering System v2 view_order.php id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Online Food Ordering System v2. Affected by this issue is some unknown functionality of the file view_order.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-24197. 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-2023-24199	SourceCodester Raffle Draw System 1.0 delete_ticket.php id sql injection	A vulnerability has been found in SourceCodester Raffle Draw System 1.0 and classified as critical. This vulnerability affects unknown code of the file delete_ticket. php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-24199. 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-2023-24201	SourceCodester Raffle Draw System 1.0 get_ticket.php id sql injection	A vulnerability was found in SourceCodester Raffle Draw System 1.0. It has been classified as critical. Affected is an unknown function of the file get_ticket.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-24201. 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-2023-24200	SourceCodester Raffle Draw System 1.0 save_ticket.php id sql injection	A vulnerability was found in SourceCodester Raffle Draw System 1.0 and classified as critical. This issue affects some unknown processing of the file save_ticket.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2023-24200. 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-2023-24198	SourceCodester Raffle Draw System 1.0 save_winner.php ticket_id/draw sql injection	A vulnerability which was classified as critical was found in SourceCodester Raffle Draw System 1.0. This affects an unknown part of the file save_winner.php. The manipulation of the argument ticket_id/draw leads to sql injection. This vulnerability is uniquely identified as CVE-2023-24198. 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-2011-10002	weblabyrinth 0.3.1 labyrinth. inc.php Labyrinth sql injection	A vulnerability classified as critical has been found in weblabyrinth 0.3.1. This affects the function Labyrinth of the file labyrinth. inc.php. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2011-10002. 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 SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-45526	Future-Depth IMS 1.0 login_transfer.php ad sql injection	A vulnerability was found in Future-Depth IMS 1.0. It has been classified as critical. This affects an unknown part of the file / admin_area /login_transfer.php. The manipulation of the argument ad leads to sql injection. This vulnerability is uniquely identified as CVE-2022-45526. 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-2023-0771	ampache up to 5.5.6 sql injection	A vulnerability was found in ampache up to 5.5.6 and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-0771. 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-2023-24685	ChurchCRM up to 4.5.3 Event Attendance Reports Module sql injection	A vulnerability which was classified as critical was found in ChurchCRM up to 4.5.3. Affected is an unknown function of the component Event Attendance Reports Module. The manipulation of the argument Event leads to sql injection. This vulnerability is traded as CVE-2023-24685. 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-2023-24684	ChurchCRM up to 4.5.3 GetText.php EID sql injection	A vulnerability which was classified as critical was found in ChurchCRM up to 4.5.3. This affects an unknown part of the file GetText.php. The manipulation of the argument EID leads to sql injection. This vulnerability is uniquely identified as CVE-2023-24684. 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-2023-0774	SourceCodester Medical Certificate Generator App 1.0 action.php lastname sql injection	A vulnerability has been found in SourceCodester Medical Certificate Generator App 1.0 and classified as critical. This vulnerability affects unknown code of the file action.php. The manipulation of the argument lastname leads to sql injection. This vulnerability was named CVE-2023-0774. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-23162	Art Gallery Management System 1.0 product.php cid sql injection	A vulnerability classified as critical was found in Art Gallery Management System 1.0. This vulnerability affects unknown code of the file product.php. The manipulation of the argument cid leads to sql injection. This vulnerability was named CVE-2023-23162. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-23163	Art Gallery Management System Project 1.0 editid sql injection	A vulnerability classified as critical was found in Art Gallery Management System Project 1.0. This vulnerability affects unknown code. The manipulation of the argument editid leads to sql injection. This vulnerability was named CVE-2023-23163. 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-2023-0781	SourceCodester Canteen Management System 1.0 removeOrder.php query id sql injection	A vulnerability was found in SourceCodester Canteen Management System 1.0. It has been declared as critical. This vulnerability affects the function query of the file removeOrder.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-0781. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-0784	SourceCodester Best Online News Portal 1.0 Login Page username sql injection	A vulnerability classified as critical has been found in SourceCodester Best Online News Portal 1.0. Affected is an unknown function of the component Login Page. The manipulation of the argument username leads to sql injection. This vulnerability is traded as CVE-2023-0784. 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-2022-4445	FL3R FeelBox Plugin up to 8.1 on WordPress sql injection	A vulnerability was found in FL3R FeelBox Plugin up to 8.1. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-4445. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-23948	ownCloud App 2.21.1/3.0 on Android FileContentProvider.kt sql injection (GHSL-2022-059)	A vulnerability which was classified as critical has been found in ownCloud App 2.21.1/3.0. This issue affects some unknown processing of the file FileContentProvider.kt. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-23948. Local access is required to approach this attack. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-0220	Pinpoint Booking System Plugin prior 2.9.9.2.9 on WordPress Shortcode Attribute sql injection	A vulnerability classified as critical was found in Pinpoint Booking System Plugin. This vulnerability affects unknown code of the component Shortcode Attribute Handler. The manipulation leads to sql injection. This vulnerability was named CVE-2023-0220. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0098	Simple URLs Plugin up to 114 on WordPress sql injection	A vulnerability classified as critical has been found in Simple URLs Plugin up to 114. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-0098. 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-2023-0259	WP Google Review Slider Plugin up to 11.7 on WordPress sql injection	A vulnerability was found in WP Google Review Slider Plugin up to 11.7 and classified as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-0259. 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-2023-0260	WP Review Slider Plugin up to 12.1 on WordPress sql injection	A vulnerability which was classified as critical has been found in WP Review Slider Plugin up to 12.1. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-0260. 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-2023-0263	WP Yelp Review Slider Plugin up to 7.0 on WordPress sql injection	A vulnerability which was classified as critical was found in WP Yelp Review Slider Plugin up to 7.0. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-0263. 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 SQL Injection attack.
CVE-2023-24084	ChiKoi 1.0 load_file sql injection	A vulnerability was found in ChiKoi 1.0. It has been declared as critical. Affected by this vulnerability is the function load_file. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-24084. 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-2022-45962	Open Solutions for Education openSIS Community Edition up to 8.0 CalendarModal.php sql injection	A vulnerability was found in Open Solutions for Education openSIS Community Edition up to 8.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file CalendarModal.php. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-45962. Access to the local network is required for this attack to succeed. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-24647	SourceCodester Food Ordering System 2.0 Parameter email sql injection	A vulnerability was found in SourceCodester Food Ordering System 2.0. It has been rated as critical. Affected by this issue is some unknown functionality of the component Parameter Handler. The manipulation of the argument email leads to sql injection. This vulnerability is handled as CVE-2023-24647. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-38239	Dataease up to 1.1.x /api /sys_msg/ list/1/10 orders sql injection (ID 510)	A vulnerability was found in Dataease up to 1.1.x and classified as critical. This issue affects some unknown processing of the file /api /sys_msg/ list/1/10. The manipulation of the argument orders leads to sql injection. The identification of this vulnerability is CVE-2021-38239. Access to the local network is required for this attack to succeed. 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-2022-38868	Ehoney 2.0.0 models /protocol.go sql injection (ID 59)	A vulnerability was found in Ehoney 2.0.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file models/protocol.go. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-38868. 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-2020-21119	Kliqqi-CMS 2.0.2 admin_update_module_widg ets.php recordIDValue sql injection (ID 259)	A vulnerability was found in Kliqqi-CMS 2.0.2. It has been declared as critical. This vulnerability affects unknown code of the file admin /admin_update_module_widg ets.php. The manipulation of the argument recordIDValue leads to sql injection. This vulnerability was named CVE-2020-21119. 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-2021-33925	nitinparashar30 cms-corephp up to bda-be52ef282846823b-da102728a-35506d0ec8f9 Login sql injection	A vulnerability was found in nitinparashar30 cms-corephp up to bda-be52ef282846823bda102728a35506d0ec8f9. It has been classified as critical. This affects an unknown part of the component Login Handler. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2021-33925. 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-2023-25047	RSVPMaker Plugin up to 9.9.3 on WordPress delete sql injection	A vulnerability was found in RSVPMaker Plugin up to 9.9.3. It has been classified as critical. This affects an unknown part. The manipulation of the argument delete leads to sql injection. This vulnerability is uniquely identified as CVE-2023-25047. 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-2023-25045	RSVPMaker Plugin up to 9.9.3 on WordPress email sql injection	A vulnerability was found in RSVPMaker Plugin up to 9.9.3. It has been declared as critical. This vulnerability affects unknown code. The manipulation of the argument email leads to sql injection. This vulnerability was named CVE-2023-25045. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-38867	rttys 4.0.0/4.0.1/4.0.2 api.go sql injection (ID 117)	A vulnerability was found in rttys 4.0.0/4.0.1/4.0.2. It has been classified as critical. Affected is an unknown function of the file api.go. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-38867. 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-2021-34117	SEO Panel 4.9.0 api/user. api.php getUserName username sql injection (ID 219)	A vulnerability was found in SEO Panel 4.9.0. It has been rated as critical. This issue affects the function getUserName of the file api/user.api.php. The manipulation of the argument username leads to sql injection. The identification of this vulnerability is CVE-2021-34117. 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-2020-21120	UQCMS 2.1.3 cart.class.php cookie_cart sql injection	A vulnerability which was classified as critical has been found in UQCMS 2.1.3. Affected by this issue is some unknown functionality of the file home\controls\cart.class. php. The manipulation of the argument cookie_cart leads to sql injection. This vulnerability is handled as CVE-2020-21120. 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-2022-40347	Intern Record System 1.0 /intern/controller.php email /deptType/name sql injection	A vulnerability was found in Intern Record System 1.0. It has been classified as critical. Affected is an unknown function of the file /intern /controller.php. The manipulation of the argument email/deptType/name leads to sql injection. This vulnerability is traded as CVE-2022-40347. 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-2023-24221	LuckyframeWEB 3.5 / system /DeptMapper.xml dataScope sql injection (ID 23)	A vulnerability was found in LuckyframeWEB 3.5. It has been rated as critical. Affected by this issue is some unknown functionality of the file /system/DeptMapper.xml. The manipulation of the argument dataScope leads to sql injection. This vulnerability is handled as CVE-2023-24221. 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-2023-24220	LuckyframeWEB 3.5 / system /RoleMapper.xml dataScope sql injection (ID 22)	A vulnerability was found in LuckyframeWEB 3.5. It has been classified as critical. Affected is an unknown function of the file /system /RoleMapper.xml. The manipulation of the argument dataScope leads to sql injection. This vulnerability is traded as CVE-2023-24220. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-24219	LuckyframeWEB 3.5 / system /UserMapper. xml dataScope sql injection (ID 24)	A vulnerability was found in LuckyframeWEB 3.5 and classified as critical. This issue affects some un-known processing of the file /system /UserMapper. xml. The manipulation of the argument dataScope leads to sql injection. The identification of this vulnerability is CVE-2023-24219. 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-2022-40032	Simple Task Managing System 1.0 login.php username/password information disclo-sure	A vulnerability was found in Simple Task Managing System 1.0. It has been declared as problematic. Affected by this vulnera-bility is an unknown func-tionality of the file login. php. The manipulation of the argument username/ password leads to infor-mation disclosure. This vulnerability is known as CVE-2022-40032. The attack needs to be done within the local network. There is no exploit avail-able.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-23279	Canteen Manage-ment System 1.0 getOrderReport. php sql injection	A vulnerability was found in Canteen Management System 1.0. It has been classified as critical. This affects an unknown part of the file /php_action /ge-tOrderReport.php. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-23279. 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-2023-23007	earclink ESPCMS 8.211201 Members sql injection	A vulnerability was found in earclink ESPCMS 8.211201. It has been rated as critical. Affected by this issue is some unknown functionality of the com-ponent Members Handler. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-23007. 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-2021-33948	FantasticLBP Hotels Server 1.0 username sql injection (ID 14)	A vulnerability classified as critical was found in Fan-tasticLBP Hotels Server 1.0. Affected by this vul-nerability is an unknown functionality. The manip-ulation of the argument username leads to sql injection. This vulnerability is known as CVE-2021-33948. Ac-cess 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-2020-29168	Projectworlds Online Doctor Appointment Booking System getuser.php q sql injection (ID 49059 / EDB- 49059)	A vulnerability which was classified as critical was found in Projectworlds On-line Doctor Appointment Booking System. Affected is an unknown function of the file getuser.php. The manipulation of the argument q leads to sql injection. This vulnerability is traded as CVE-2020-29168. Ac-cess 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0913	SourceCodester Auto Dealer Management System 1.0 id sql injection	A vulnerability classified as critical was found in SourceCodester Auto Dealer Management System 1.0. This vulnerability affects unknown code of the file /adms/admin/pagevehicles /sell_vehicle. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-0913. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-0912	SourceCodester Auto Dealer Management System 1.0 id sql injection	A vulnerability classified as critical has been found in SourceCodester Auto Dealer Management System 1.0. This affects an unknown part of the file /adms/admin /pagevehicles /view_transaction. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-0912. 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-2023-0903	SourceCodester Employee Task Management System 1.0 edit-task.php task_id sql injection	A vulnerability was found in SourceCodester Employee Task Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file edit-task.php. The manipulation of the argument task_id leads to sql injection. This vulnerability was named CVE-2023-0903. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-0904	SourceCodester Employee Task Management System 1.0 task-details.php task_id sql injection	A vulnerability was found in SourceCodester Employee Task Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file task-details.php. The manipulation of the argument task_id leads to sql injection. The identification of this vulnerability is CVE-2023-0904. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-0915	SourceCodester Auto Dealer Management System 1.0 id sql injection	A vulnerability classified as critical has been found in SourceCodester Auto Dealer Management System 1.0. Affected is an unknown function of the file /adms /admin/pageuser /manage_user. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-0915. 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-2023-0917	SourceCodester Simple Customer Relationship Management System 1.0 /php-scrm/login.php Password sql injection	A vulnerability which was classified as critical was found in SourceCodester Simple Customer Relationship Management System 1.0. This affects an unknown part of the file /phpscrm/login.php. The manipulation of the argument Password leads to sql injection. This vulnerability is uniquely identified as CVE-2023-0917. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0938	SourceCodester Music Gallery Site 1.0 GET Request music_list.php cid sql injection	A vulnerability classified as critical has been found in SourceCodester Music Gallery Site 1.0. This affects an unknown part of the file music_list.php of the component GET Request Handler. The manipulation of the argument cid leads to sql injection. This vulnerability is uniquely identified as CVE-2023-0938. 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-2023-1035	SourceCodester Clinics Patient Management System 1.0 update_user.php user_id sql injection	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been classified as critical. Affected is an unknown function of the file update_user.php. The manipulation of the argument user_id leads to sql injection. This vulnerability is traded as CVE-2023-1035. 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-2023-24651	SourceCodester Simple Customer Relationship Management System 1.0 Registration Page name sql injection	A vulnerability which was classified as critical was found in SourceCodester Simple Customer Relationship Management System 1.0. This affects an unknown part of the component Registration Page. The manipulation of the argument name leads to sql injection. This vulnerability is uniquely identified as CVE-2023-24651. 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-2023-24656	SourceCodester Simple Customer Relationship Management System 1.0 Create Ticket subject sql injection	A vulnerability was found in SourceCodester Simple Customer Relationship Management System 1.0. It has been classified as critical. Affected is an unknown function of the component Create Ticket Handler. The manipulation of the argument subject leads to sql injection. This vulnerability is traded as CVE-2023-24656. 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-2023-24364	SourceCodester Simple Customer Relationship Management System 1.0 Admin Panel username sql injection	A vulnerability which was classified as critical has been found in SourceCodester Simple Customer Relationship Management System 1.0. Affected by this issue is some unknown functionality of the component Admin Panel. The manipulation of the argument username leads to sql injection. This vulnerability is handled as CVE-2023-24364. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-24653	SourceCodester Simple Customer Relationship Management System 1.0 Change Password oldpass sql injection	A vulnerability has been found in SourceCodester Simple Customer Relationship Management System 1.0 and classified as critical. This vulnerability affects unknown code of the component Change Password Handler. The manipulation of the argument oldpass leads to sql injection. This vulnerability was named CVE-2023-24653. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-24654	SourceCodester Simple Customer Relationship Management System 1.0 Request a Quote name sql injection	A vulnerability was found in SourceCodester Simple Customer Relationship Management System 1.0 and classified as critical. This issue affects some unknown processing of the component Request a Quote. The manipulation of the argument name leads to sql injection. The identification of this vulnerability is CVE-2023-24654. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-24652	SourceCodester Simple Customer Relationship Management System 1.0 Create Ticket Description sql injection	A vulnerability classified as critical was found in SourceCodester Simple Customer Relationship Management System 1.0. This vulnerability affects unknown code of the component Create Ticket Handler. The manipulation of the argument Description leads to sql injection. This vulnerability was named CVE-2023-24652. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1059	SourceCodester Doctors Appointment System 1.0 Parameter /admin/doctors. php search sql injection	A vulnerability classified as critical was found in SourceCodester Doctors Appointment System 1.0. This vulnerability affects unknown code of the file /admin/doctors. php of the component Parameter Handler. The manipulation of the argument search leads to sql injection. This vulnerability was named CVE-2023-1059. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1062	SourceCodester Doctors Appointment System 1.0 Parameter /admin/add-new. php email sql injection	A vulnerability which was classified as critical was found in SourceCodester Doctors Appointment System 1.0. Affected is an unknown function of the file /admin/addnew. php of the component Parameter Handler. The manipulation of the argument email leads to sql injection. This vulnerability is traded as CVE-2023-1062. 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-2023-1061	SourceCodester Doctors Appointment System 1.0 /admin/edit-doc.php oldmail sql injection	A vulnerability which was classified as critical has been found in SourceCodester Doctors Appointment System 1.0. This issue affects some unknown processing of the file /admin/edit-doc. php. The manipulation of the argument oldmail leads to sql injection. The identification of this vulnerability is CVE-2023-1061. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1056	SourceCodester Doctors Appointment System 1.0 /edoc/doctor/patient.php search12 sql injection	A vulnerability was found in SourceCodester Doctors Appointment System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /edoc/doctor/patient. php. The manipulation of the argument search12 leads to sql injection. This vulnerability is known as CVE-2023-1056. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1057	SourceCodester Doctors Appointment System 1.0 login.php edoc usermail sql injection	A vulnerability was found in SourceCodester Doctors Appointment System 1.0. It has been rated as critical. Affected by this issue is the function edoc of the file login. php. The manipulation of the argument usermail leads to sql injection. This vulnerability is handled as CVE-2023-1057. 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-2023-1058	SourceCodester Doctors Appointment System 1.0 create-account. php newemail sql injection	A vulnerability classified as critical has been found in SourceCodester Doctors Appointment System 1.0. This affects an unknown part of the file create-account.php. The manipulation of the argument newemail leads to sql injection. This vulnerability is uniquely identified as CVE-2023-1058. 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-2023-1063	SourceCodester Doctors Appointment System 1.0 Parameter /admin/patient. php search sql injection	A vulnerability has been found in SourceCodester Doctors Appointment System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/patient. php of the component Parameter Handler. The manipulation of the argument search leads to sql injection. This vulnerability is known as CVE-2023-1063. The attack can be launched 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-2023-0606	ampache up to 5.5.6 cross-site scripting	A vulnerability which was classified as problematic has been found in ampache up to 5.5.6. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-0606. 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-2023-0608	microweber up to 1.3.1 cross-site scripting	A vulnerability has been found in microweber up to 1.3.1 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-0608. 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-2023-0607	projectsend prior r1606 cross-site scripting	A vulnerability which was classified as problematic was found in projectsend. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-0607. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2546	All-in-One WP Migration Plugin up to 7.62 on WordPress Content Type ai1wm_export cross-site scripting	A vulnerability was found in All-in-One WP Migration Plugin up to 7.62. It has been rated as problematic. Affected by this issue is the function ai1wm_export of the component Content Type Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-2546. 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-2022-46934	kkFileView 4.1.0 OnlinePreviewController.java url cross-site scripting (ID 411)	A vulnerability was found in kkFileView 4.1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /controller/OnlinePreviewController.java. The manipulation of the argument url leads to cross-site scripting. This vulnerability is handled as CVE-2022-46934. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0650	YAFNET up to 3.1.11 Signature cross-site scripting	A vulnerability was found in YAFNET up to 3.1.11 and classified as problematic. This issue affects some unknown processing of the component Signature Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-0650. 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-2022-4897	BackupBuddy Plugin up to 8.8.2 on WordPress cross-site scripting	A vulnerability was found in BackupBuddy Plugin up to 8.8.2 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-2022-4897. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0380	Easy Digital Downloads Plugin up to 3.1.0.4 on WordPress Shortcode cross-site scripting	A vulnerability which was classified as problematic has been found in Easy Digital Downloads Plugin up to 3.1.0.4. 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-2023-0380. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0371	EmbedSocial Plugin 1.1.27 on WordPress Shortcode cross-site scripting	A vulnerability has been found in EmbedSocial Plugin 1.1.27 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-2023-0371. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0372	EmbedStories Plugin up to 0.7.4 on WordPress Shortcode cross-site scripting	A vulnerability was found in EmbedStories Plugin up to 0.7.4. 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-2023-0372. 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-2021-36538	Gurock TestRail up to 7.1.1 reference/ description cross-site scripting	A vulnerability which was classified as problematic was found in Gurock TestRail up to 7.1.1. This affects an unknown part. The manipulation of the argument reference/description leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2021-36538. 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-2023-23635	Jellyfin up to 10.8.3 Collection Name cross-site scripting (ID 3788)	A vulnerability classified as problematic has been found in Jellyfin up to 10.8.3. This affects an unknown part of the component Collection Name Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-23635. 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-2023-23636	Jellyfin up to 10.8.3 Playlist Name cross-site scripting (ID 3788)	A vulnerability classified as problematic was found in Jellyfin up to 10.8.3. This vulnerability affects unknown code of the component Playlist Name Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-23636. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0285	Real Media Library Plugin up to 4.18.28 on WordPress cross-site scripting	A vulnerability was found in Real Media Library Plugin up to 4.18.28. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-0285. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2021-37502	Site automad 1.7.5 Add User name cross-site scripting (ID 29)	A vulnerability classified as problematic has been found in Site automad 1.7.5. This affects an unknown part of the component Add User Handler. The manipulation of the argument name leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2021-37502. 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-2021-37374	Teradek Clip System Information Settings Friendly Name cross-site scripting	A vulnerability classified as problematic was found in Teradek Clip. Affected by this vulnerability is an unknown functionality of the component System Information Settings. The manipulation of the argument Friendly Name leads to cross-site scripting. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is known as CVE-2021-37374. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2021-37378	Teradek Cube/Cube Pro up to 7.3. x System Information Settings Friendly Name cross-site scripting	A vulnerability which was classified as problematic was found in Teradek Cube and Cube Pro up to 7.3.x. This affects an unknown part of the component System Information Settings. The manipulation of the argument Friendly Name leads to cross-site scripting. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is uniquely identified as CVE-2021-37378. 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-2021-37373	Teradek Slice up to 7.3.x Friendly Name cross-site scripting	A vulnerability classified as problematic has been found in Teradek Slice up to 7.3.x. Affected is an unknown function. The manipulation of the argument Friendly Name leads to cross-site scripting. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is traded as CVE-2021-37373. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-37379	Teradek Sphere System Information Settings Friendly Name cross-site scripting	A vulnerability has been found in Teradek Sphere and classified as problematic. This vulnerability affects unknown code of the component System Information Settings. The manipulation of the argument Friendly Name leads to cross-site scripting. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability was named CVE-2021-37379. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2021-37375	Teradek VidiU/VidiU Mini up to 3.0.8 System Information Settings Friendly Name cross-site scripting	A vulnerability which was classified as problematic has been found in Teradek VidiU and VidiU Mini up to 3.0.8. Affected by this issue is some unknown functionality of the component System Information Settings. The manipulation of the argument Friendly Name leads to cross-site scripting. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is handled as CVE-2021-37375. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2021-37518	Vimium up to 1.66 omnibar crosssite scripting (ID 3832)	A vulnerability classified as problematic was found in Vimium up to 1.66. This vulnerability affects unknown code of the component omnibar. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2021-37518. 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-2022-4714	WP Dark Mode up to 3.0.6 on WordPress Shortcode cross-site scripting	A vulnerability which was classified as problematic was found in WP Dark Mode up to 3.0.6. Affected is an unknown function of the component Shortcode Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-4714. 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-2017-20175	DaSchTour matomo-mediawikiextension up to 2.4.2 on MediaWiki Username Piwik.hooks.php crosssite scripting (ID 17)	A vulnerability classified as problematic has been found in DaSchTour matomo-mediawiki-extension up to 2.4.2. This affects an unknown part of the file Piwik.hooks.php of the component Username Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2017-20175. It is possible to initiate the attack 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-22975	jfinal_cms 5.1.0 cross-site scripting (ID 53)	A vulnerability was found in jfinal_cms 5.1.0. 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-2023-22975. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0676	phpipam up to 1.5.0 cross-site scripting	A vulnerability was found in phpipam up to 1.5.0. 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-2023-0676. 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-2023-0677	phpipam up to 1.5.0 cross-site scripting	A vulnerability was found in phpipam up to 1.5.0. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to crosssite scripting. This vulnerability is handled as CVE-2023-0677. 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-2021-37376	Teradek Bond/Bond 2/Bond Pro up to 7.3.x System Information Settings Friendly Name cross-site scripting	A vulnerability was found in Teradek Bond Bond 2 and Bond Pro up to 7.3.x and classified as problematic. This issue affects some unknown processing of the component System Information Settings. The manipulation of the argument Friendly Name leads to cross-site scripting. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. The identification of this vulnerability is CVE-2021-37376. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2021-37377	Teradek Brik up to 7.2.x System Information Settings Friendly Name cross-site scripting	A vulnerability has been found in Teradek Brik up to 7.2.x and classified as problematic. This vulnerability affects unknown code of the component System Information Settings. The manipulation of the argument Friendly Name leads to cross-site scripting. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability was named CVE-2021-37377. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-36712	yzmcms 6.1 Image Clipping crosssite scripting	A vulnerability classified as problematic has been found in yzmcms 6.1. Affected is an unknown function of the component Image Clipping Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2021-36712. 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-2022-4836	Breadcrumb Plugin up to 1.5.32 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in Breadcrumb Plugin up to 1.5.32. 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-2022-4836. 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-2023-0252	Contextual Related Posts Plugin up to 3.3.0 on WordPress Block Option cross-site scripting	A vulnerability was found in Contextual Related Posts Plugin up to 3.3.0. It has been classified as problematic. Affected is an unknown function of the component Block Option Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-0252. 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-2023-0147	Flexible Captcha Plugin up to 4.1 on WordPress Shortcode Attribute cross-site scripting	A vulnerability classified as problematic was found in Flexible Captcha Plugin up to 4.1. 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-2023-0147. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0148	Gallery Factory Lite Plugin up to 2.0.0 on WordPress Shortcode Attribute cross-site scripting	A vulnerability which was classified as problematic has been found in Gallery Factory Lite Plugin up to 2.0.0. 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-2023-0148. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0154	GamiPress Plugin up to 1.0.8 on WordPress Shortcode Attribute cross-site scripting	A vulnerability has been found in GamiPress Plugin up to 1.0.8 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-2023-0154. 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-2022-4674	Ibtana Plugin up to 1.1.8.7 on WordPress Shortcode Attribute cross-site scripting	A vulnerability which was classified as problematic has been found in Ibtana Plugin up to 1.1.8.7. 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-2022-4674. 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-2022-4664	Logo Slider Plugin up to 3.5.x on WordPress Shortcode Attribute cross-site scripting	A vulnerability classified as problematic was found in Logo Slider Plugin up to 3.5.x. This vulnerability affects unknown code of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-4664. 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-2022-4762	Materialis Companion Plugin up to 1.3.39 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in Materialis Companion Plugin up to 1.3.39 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-2022-4762. 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-2022-4756	My YouTube Channel Plugin up to 3.22.x on WordPress Shortcode Attribute cross-site scripting	A vulnerability has been found in My YouTube Channel Plugin up to 3.22.x 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-2022-4756. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0146	Naver Map Plugin up to 1.1.0 on WordPress Shortcode Attribute cross-site scripting	A vulnerability classified as problematic has been found in Naver Map Plugin up to 1.1.0. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-0146. 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-2022-4321	PDF Generator for Plugin up to 1.1.1 on WordPress dompdf Example cross-site scripting	A vulnerability was found in PDF Generator for Plugin up to 1.1.1. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component dompdf Example. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-4321. 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-2022-4747	Post Category Image With Grid and Slider Plugin up to 1.4.7 on WordPress Shortcode Attribute cross-site scripting	A vulnerability which was classified as problematic was found in Post Category Image With Grid and Slider Plugin up to 1.4.7. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-4747. 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-2022-4657	Restaurant Menu Plugin up to 2.3.5 on WordPress Shortcode Attribute cross-site scripting	A vulnerability classified as problematic has been found in Restaurant Menu Plugin up to 2.3.5. 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-2022-4657. 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-2022-4826	Simple Tooltips Plugin up to 2.1.3 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in Simple Tooltips Plugin up to 2.1.3. 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-2022-4826. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-48085	Softr 2.0 Work Space Name crosssite scripting	A vulnerability which was classified as problematic has been found in Softr 2.0. This issue affects some unknown process-ing. The manipulation of the argument Work Space Name leads to cross-site scripting. The identification of this vulnerability is CVE-2022-48085. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-24195	SourceCodester Online Food Ordering System v2 index. php page cross-site scripting	A vulnerability classified as problematic was found in SourceCodester Online Food Ordering System v2. This vulnerability affects unknown code of the file index.php. The manip-ulation of the argument page leads to crosssite scripting. This vulnerability was named CVE-2023-24195. The attack can be initiated remotely. There is no ex-ploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-24192	SourceCodester Online Food Ordering System v2 login.php login redirect cross-site scripting	A vulnerability was found in SourceCodester Online Food Ordering System v2. It has been rated as problematic. Affected by this issue is the function login of the file login. php. The manipulation of the argument redirect leads to cross-site scripting. This vulnerability is handled as CVE-2023-24192. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-24194	SourceCodester Online Food Ordering System v2 navbar. php page cross-site scripting	A vulnerability classified as problematic has been found in SourceCodester Online Food Ordering System v2. This affects an unknown part of the file navbar.php. The manipula-tion of the argument page leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-24194. It is possible to initiate the attack re-motely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-24191	SourceCodester Online Food Ordering System v2 signup. php redirect cross-site scripting	A vulnerability classified as problematic was found in SourceCodester Online Food Ordering System v2. Affected by this vulner-ability is an unknown functionality of the file signup.php. The manip-ulation of the argument redirect leads to cross-site scripting. This vulnerability is known as CVE-2023-24191. The attack can be launched re-motely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0236	Tutor LMS Plugin up to 2.0.9 on WordPress Attribute reset_key /user_id cross-site scripting	A vulnerability was found in Tutor LMS Plugin up to 2.0.9 and classified as problematic. This issue affects some unknown processing of the compo-nent Attribute Handler. The manipulation of the argument reset_key/ user_id leads to cross-site scripting. The identification of this vulnerability is CVE-2023-0236. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0072	WC Vendors Marketplace Plugin up to 2.4.4 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in WC Vendors Marketplace Plugin up to 2.4.4. It has been rated 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-2023-0072. 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-2023-0149	WordPrezi Plugin up to 0.8.2 on WordPress Shortcode Attribute cross-site scripting	A vulnerability which was classified as problematic was found in WordPrezi Plugin up to 0.8.2. 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-2023-0149. 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-2022-4459	WP Show Posts Plugin up to 1.1.3 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in WP Show Posts Plugin up to 1.1.3. 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-2022-4459. 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-2023-0282	YourChannel Plugin up to 1.2.1 on WordPress cross-site scripting	A vulnerability was found in YourChannel Plugin up to 1.2.1. 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-2023-0282. 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-2022-48311	HP Deskjet 2540 CEP1FN1418BR Configuration Page cross-site scripting	A vulnerability classified as problematic has been found in HP Deskjet 2540 CEP1FN1418BR. Affected is an unknown function of the component Configuration Page. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-48311. 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-2022-41312	Moxa DS-3008 2.1 HTTP Request cross-site scripting	A vulnerability which was classified as problematic has been found in Moxa DS-3008 2.1. This issue affects some unknown processing of the component HTTP Request Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-41312. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-41311	Moxa DS-3008 2.1 HTTP Request cross-site scripting	A vulnerability classified as problematic was found in Moxa DS-3008 2.1. This vulnerability affects unknown code of the component HTTP Request Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-41311. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-41313	Moxa DS-3008 2.1 Web Application cross-site scripting	A vulnerability which was classified as problematic was found in Moxa DS-3008 2.1. Affected is an unknown function of the component Web Application Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-41313. 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-2022-21948	openSUSE paste SVG File crosssite scripting	A vulnerability was found in openSUSE paste. It has been classified as problematic. Affected is an unknown function of the component SVG File Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-21948. 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-2023-24814	TYPO3 getIndpEnv cross-site scripting (GHSA-r4f8-f93x-5qh3)	A vulnerability classified as problematic was found in TYPO3. Affected by this vulnerability is the function GeneralUtility::getIndpEnv. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-24814. 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-2023-0740	answerdev answer up to 1.0.3 cross-site scripting	A vulnerability was found in answerdev answer up to 1.0.3 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-0740. 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-2023-0741	answerdev answer up to 1.0.3 cross-site scripting	A vulnerability was found in answerdev answer up to 1.0.3. It has been classified as problematic. Affected is an unknown function. The manipulation leads to crosssite scripting. This vulnerability is traded as CVE-2023-0741. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0742	answerdev answer up to 1.0.3 cross-site scripting	A vulnerability was found in answerdev answer up to 1.0.3. 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-2023-0742. 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-2023-0743	answerdev answer up to 1.0.3 cross-site scripting	A vulnerability was found in answerdev answer up to 1.0.3. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-0743. 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-2023-0747	btcpayserver up to 1.7.5 cross-site scripting	A vulnerability classified as problematic was found in btcpayserver up to 1.7.5. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-0747. 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-2022-45755	EyouCMS 1.6.0 Home Page Description cross-site scripting (ID 39)	A vulnerability was found in EyouCMS 1.6.0. It has been classified as problematic. Affected is an unknown function of the component Home Page Description Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-45755. 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-2023-23011	InvoicePlane 1.6 modal_product_lookups. php filter_product cross-site scripting	A vulnerability was found in InvoicePlane 1.6 and classified as problematic. Affected by this issue is the function filter_product of the file modal_product_lookups. php. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-23011. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-47417	LogicalDOC Community Edition / Enterprise Edition Document File Name cross-site scripting	A vulnerability which was classified as problematic has been found in LogicalDOC Community Edition and Enterprise Edition. This issue affects some unknown processing of the component Document File Name Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-47417. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-47418	LogicalDOC Community Edition / Enterprise Edition Document Version Comment cross-site scripting	A vulnerability which was classified as problematic was found in LogicalDOC Community Edition and Enterprise Edition. Affected is an unknown function of the component Document Version Comment Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-47418. 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-2022-47415	LogicalDOC Community Edition /Enterprise Edition In-App Messaging System subject/body cross-site scripting	A vulnerability has been found in LogicalDOC Community Edition and Enterprise Edition and classified as problematic. This vulnerability affects unknown code of the component In-App Messaging System. The manipulation of the argument subject/body leads to crosssite scripting. This vulnerability was named CVE-2022-47415. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-47416	LogicalDOC Enterprise In-App Chat System cross-site scripting	A vulnerability classified as problematic was found in LogicalDOC Enterprise. This vulnerability affects unknown code of the component In-App Chat System. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-47416. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-47419	Mayan EDMS DMS In-Product Tagging System cross-site scripting	A vulnerability was found in Mayan EDMS DMS. It has been classified as problematic. Affected is an unknown function of the component In-Product Tagging System. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-47419. 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-2022-47412	ONLYOFFICE Workspace DMS Document cross-site scripting	A vulnerability classified as problematic has been found in ONLYOFFICE Workspace DMS. This affects an unknown part of the component Document Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-47412. 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-2022-47414	OpenKM Console cross-site scripting	A vulnerability was found in OpenKM. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Console. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-47414. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-47413	OpenKM DMS cross-site scripting	A vulnerability was found in OpenKM DMS. 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-2022-47413. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-23026	SourceCodester Sales Management System 1.0 print.php product_name/product_price crosssite scripting	A vulnerability classified as problematic has been found in SourceCodester Sales Management System 1.0. This affects an unknown part of the file print.php. The manipulation of the argument product_name /product_price leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-23026. 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-2023-0736	wallabag up to 2.5.3 cross-site scripting	A vulnerability was found in wallabag up to 2.5.3 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to crosssite scripting. This vulnerability is handled as CVE-2023-0736. 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-2022-2094	Yellow Yard Searchbar Plugin up to 2.8.1 on WordPress URL Parameter cross-site scripting	A vulnerability classified as problematic was found in Yellow Yard Searchbar Plugin up to 2.8.1. Affected by this vulnerability is an unknown functionality of the component URL Parameter Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-2094. 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-2023-24687	Mojoportal 2.7.0.0 Company Info Settings txtCompanyName crosssite scripting	A vulnerability was found in Mojoportal 2.7.0.0. It has been declared as problematic. This vulnerability affects unknown code of the component Company Info Settings. The manipulation of the argument txtCompanyName leads to cross-site scripting. This vulnerability was named CVE-2023-24687. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-24322	mojoPortal 2.7.0.0 FileDialog.aspx tbi cross-site scripting	A vulnerability classified as problematic has been found in mojoPortal 2.7.0.0. This affects an unknown part of the file FileDialog.aspx. The manipulation of the argument tbi leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-24322. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-24690	ChurchCRM up to 4.5.3 family cross-site scripting	A vulnerability was found in ChurchCRM up to 4.5.3. It has been declared as problematic. This vulnerability affects unknown code of the file /api/public/register /family. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-24690. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-24230	Formwork 1.12.1 dashboard Page title cross-site scripting	A vulnerability was found in Formwork 1.12.1. It has been classified as problematic. This affects an unknown part of the file /formwork/panel/dashboard. The manipulation of the argument Page title leads to crosssite scripting. This vulnerability is uniquely identified as CVE-2023-24230. 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-2023-24234	Inventory Management System v1 brand.php Brand Name cross-site scripting	A vulnerability which was classified as problematic has been found in Inventory Management System v1. This issue affects some unknown processing of the file phpinventory-management-system/brand.php. The manipulation of the argument Brand Name leads to crosssite scripting. The identification of this vulnerability is CVE-2023-24234. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-24231	Inventory Management System v1 categories.php Categories Name cross-site scripting	A vulnerability was found in Inventory Management System v1. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /phpinventory-management-system/categories.php. The manipulation of the argument Categories Name leads to cross-site scripting. This vulnerability is handled as CVE-2023-24231. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-24233	Inventory Management System v1 orders.php Client Name cross-site scripting	A vulnerability classified as problematic was found in Inventory Management System v1. This vulnerability affects unknown code of the file /php-inventorymanagement-system/orders.phpoadd. The manipulation of the argument Client Name leads to cross-site scripting. This vulnerability was named CVE-2023-24233. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-24232	Inventory Management System v1 product.php Product Name crosssite scripting	A vulnerability classified as problematic has been found in Inventory Management System v1. This affects an unknown part of the file /php-inventory-managementsystem/product.php. The manipulation of the argument Product Name leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-24232. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-23286	Provide up to 14.4 Login Form username cross-site scripting	A vulnerability was found in Provide up to 14.4. It has been rated as problematic. This issue affects some unknown processing of the component Login Form. The manipulation of the argument username leads to crosssite scripting. The identification of this vulnerability is CVE-2023-23286. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-23161	Art Gallery Management System 1.0 Navigation Bar artname crosssite scripting	A vulnerability has been found in Art Gallery Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Navigation Bar. The manipulation of the argument artname leads to cross-site scripting. This vulnerability is known as CVE-2023-23161. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-44261	Avery Dennison Monarch Printer M9855 cross-site scripting	A vulnerability was found in Avery Dennison Monarch Printer M9855. 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-2022-44261. 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-2023-0787	thorsten phpmyfaq up to 3.1.10 cross-site scripting	A vulnerability has been found in thorsten phpmyfaq up to 3.1.10 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-2023-0787. 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-2023-0786	thorsten phpmyfaq up to 3.1.10 cross-site scripting	A vulnerability which was classified as problematic was found in thorsten phpmyfaq up to 3.1.10. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-0786. 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-2023-0075	Amazon JS Plugin up to 0.10 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in Amazon JS Plugin up to 0.10 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-2023-0075. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-4458	amr Shortcode Any Widget plugin up to 4.0 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in amr Shortcode Any Widget plugin up to 4.0. 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-2022-4458. 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-2023-0810	btcpayserver up to 1.7.10 crosssite scripting	A vulnerability was found in btcpayserver up to 1.7.10. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to crosssite scripting. The identification of this vulnerability is CVE-2023-0810. 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-2023-0275	Easy Accept Payments for PayPal Plugin up to 4.9.9 on WordPress Shortcode Attribute cross-site scripting	A vulnerability classified as problematic was found in Easy Accept Payments for PayPal Plugin up to 4.9.9. 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-2023-0275. 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-2022-4628	Easy PayPal Buy Now Button Plugin up to 1.7.3 on WordPress Shortcode Attribute cross-site scripting	A vulnerability has been found in Easy PayPal Buy Now Button Plugin up to 1.7.3 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-2022-4628. 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-2022-4759	GigPress Plugin up to 2.3.27 on WordPress Shortcode Attribute cross-site scripting	A vulnerability classified as problematic has been found in GigPress Plugin up to 2.3.27. 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-2022-4759. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0034	JetWidgets for Elementor Plugin up to 1.0.13 on WordPress Shortcode Attribute cross-site scripting	A vulnerability which was classified as problematic was found in JetWidgets for Elementor Plugin up to 1.0.13. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-0034. 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-2023-0061	http://Judge.me Product Reviews for WooCommerce Plugin up to 1.3.20 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in http://Judge.me Product Reviews for WooCommerce Plugin up to 1.3.20 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-2023-0061. 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-2022-4682	Lightbox Gallery Plugin up to 0.9.4 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in Lightbox Gallery Plugin up to 0.9.4. 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-2022-4682. 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-2022-4562	Meks Flexible Shortcodes Plugin up to 1.3.4 on WordPress Shortcode Attribute cross-site scripting	A vulnerability which was classified as problematic has been found in Meks Flexible Shortcodes Plugin up to 1.3.4. 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-2022-4562. 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-2022-4830	Paid Memberships Pro Plugin up to 2.9.8 on WordPress Shortcode Attribute cross-site scripting	A vulnerability which was classified as problematic has been found in Paid Memberships Pro Plugin up to 2.9.8. 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-2022-4830. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0060	Responsive Gallery Grid Plugin up to 2.3.8 on WordPress Shortcode Attribute page/post cross-site scripting	A vulnerability has been found in Responsive Gallery Grid Plugin up to 2.3.8 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file page/post of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-0060. 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-2022-4551	Rich Table of Contents Plugin up to 1.3.7 on WordPress Shortcode Attribute cross-site scripting	A vulnerability classified as problematic was found in Rich Table of Contents Plugin up to 1.3.7. 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-2022-4551. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0099	Simple URLs Plugin up to 114 on WordPress cross-site scripting	A vulnerability was found in Simple URLs Plugin up to 114. 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-2023-0099. 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-2023-0379	Spotlight Social Feeds Plugin up to 1.4.2 on WordPress Block Option cross-site scripting	A vulnerability which was classified as problematic was found in Spotlight Social Feeds Plugin up to 1.4.2. This affects an unknown part of the component Block Option Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-0379. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-4678	TemplatesNext ToolKit Plugin up to 3.2.7 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in TemplatesNext ToolKit Plugin up to 3.2.7 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-2022-4678. 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-2023-0362	Themify Portfolio Post Plugin up to 1.2.1 on WordPress Shortcode Attribute cross-site scripting	A vulnerability which was classified as problematic has been found in Themify Portfolio Post Plugin up to 1.2.1. 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-2023-0362. 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-2022-4580	Twenty20 Image Before-After Plugin up to 1.5.9 on WordPress Shortcode Attribute cross-site scripting	A vulnerability which was classified as problematic was found in Twenty20 Image Before-After Plugin up to 1.5.9. 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-2022-4580. 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-2023-0151	uTubeVideo Gallery Plugin up to 2.0.7 on WordPress Shortcode Attribute page/post cross-site scripting	A vulnerability was found in uTubeVideo Gallery Plugin up to 2.0.7. It has been declared as problematic. This vulnerability affects unknown code of the file page/post of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-0151. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-45285	Vsourz Digital Advanced Contact Form 7 DB 1.7.2/1.9.1 cross-site scripting	A vulnerability classified as problematic has been found in Vsourz Digital Advanced Contact Form 7 DB 1.7.2/1.9.1. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-45285. 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-2022-4473	Widget Shortcode Plugin up to 0.3.5 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in Widget Shortcode Plugin up to 0.3.5. It has been rated 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-2022-4473. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-4488	Widgets on Pages Plugin up to 1.6.0 on WordPress Shortcode Attribute cross-site scripting	A vulnerability classified as problematic has been found in Widgets on Pages Plugin up to 1.6.0. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-4488. 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-2022-4656	WP Visitor Statistics Plugin up to 6.4 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in WP Visitor Statistics Plugin up to 6.4. 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-2022-4656. 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-2023-0177	WpDevArt Social Like Box and Page Plugin prior 0.8.41 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in WpDevArt Social Like Box and Page Plugin. It has been rated 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-2023-0177. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0270	YaMaps for Plugin prior 0.6.26 on WordPress Shortcode Attribute cross-site scripting	A vulnerability classified as problematic has been found in YaMaps for Plugin. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-0270. 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-2022-4471	YARPP Plugin up to 5.30.1 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in YARPP Plugin up to 5.30.1. 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-2022-4471. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-4783	Youtube Channel Gallery Plugin up to 2.4 on WordPress Shortcode Attribute cross-site scripting	A vulnerability classified as problematic was found in Youtube Channel Gallery Plugin up to 2.4. This vulnerability affects unknown code of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-4783. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-25241	bgERP 22.31 Parameter Search cross-site scripting	A vulnerability has been found in bgERP 22.31 and classified as problematic. This vulnerability affects unknown code of the component Parameter Handler. The manipulation of the argument Search leads to crosssite scripting. This vulnerability was named CVE-2023-25241. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0827	pimcore up to 1.5.16 cross-site scripting	A vulnerability was found in pimcore up to 1.5.16. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-0827. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-25572	react-admin up to 3.19.11/4.7.5 Custom Fields cross-site scripting (GHSA-5jcr-82fh-339v)	A vulnerability which was classified as problematic was found in react-admin up to 3.19.11/4.7.5. Affected is an unknown function of the component Custom Fields Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-25572. 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-2023-24086	SLIMS 9.5.2 loan_by_class.php cross-site scripting	A vulnerability which was classified as problematic has been found in SLIMS 9.5.2. Affected by this issue is some unknown functionality of the file /customs /loan_by_class.phpreportView. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-24086. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-22933	Splunk Enterprise up to 8.1.12/8.2.9/9.0.3 XML layoutPanel crosssite scripting (SVD-2023-0203)	A vulnerability has been found in Splunk Enterprise up to 8.1.12/8.2.9/9.0.3 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component XML Handler. The manipulation of the argument layoutPanel leads to cross-site scripting. This vulnerability is known as CVE-2023-22933. 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-2023-24648	Zstore 6.6.0 /index.php cross-site scripting	A vulnerability which was classified as problematic was found in Zstore 6.6.0. This affects an unknown part of the file /index.php. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-24648. 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-2022-45543	DiscuzX 3.4 Audit Search datetline / title/tpp/username cross-site scripting	A vulnerability which was classified as problematic was found in DiscuzX 3.4. This affects an unknown part of the component Audit Search. The manipulation of the argument datetline/title/tpp/username leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-45543. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-25978	usememos cross-site scripting (ID 1026)	A vulnerability was found in usememos memos. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-25978. 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-2023-0879	btcpayserver up to 1.7.11 crosssite scripting	A vulnerability which was classified as problematic has been found in btcpayserver up to 1.7.11. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-0879. 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-2021-40555	flatCore-CMS 2.2.15 New Page Creation Form description crosssite scripting (ID 56)	A vulnerability which was classified as problematic was found in flatCore-CMS 2.2.15. This affects an unknown part of the component New Page Creation Form. The manipulation of the argument description leads to crosssite scripting. This vulnerability is uniquely identified as CVE-2021-40555. 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-2022-48324	Mapos 4.39.0 Arquivos.php crosssite scripting (ID 2010)	A vulnerability was found in Mapos 4.39.0 and classified as problematic. Affected by this issue is some unknown functionality of the file application/controllers/Arquivos. php. The manipulation of the argument pesquisa/data / data2/nome/descricao/ idDocumentos/id leads to crosssite scripting. This vulnerability is handled as CVE-2022-48324. The attack may 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-2022-48325	Mapos 4.39.0 Mapos. php crosssite scripting (ID 2010)	A vulnerability was found in Mapos 4.39.0. It has been classified as problematic. Affected is an unknown function of the file application/controllers/ Mapos.php. The manipulation of the argument year/ oldSenha/novaSenha/termo/nome/cnpj/ie/cep/logradouro/numero/bairro/ cidade /uf/telefone/email/ id/app_name/per_page/ app_theme/os_notification/email_automatico/ control_estoque/notifica_whats/control_baixa/ control_editos/control_edit_vendas/control_datatable/pix_key /os_status_list/control_2vias/status/start/ end leads to cross-site scripting. This vulnerability is traded as CVE-2022-48325. It is possible to launch the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-48326	Mapos 4.39.0 Permissoes.php cross-site scripting (ID 2010)	A vulnerability has been found in Mapos 4.39.0 and classified as problematic. This vulnerability affects unknown code of the file application/controllers /Permissoes.php. The manipulation of the argument nome/aCliente/eCliente/dCliente/vCliente/aProduto/eProduto/dProduto/vProduto/aServico/eServico/dServico/vServico/aOs/eOs/dOs/vOs/aVenda/eVenda/dVenda/vVenda/aGarantia/eGarantia/dGarantia/vGarantia/aArquivo/eArquivo/dArquivo/vArquivo/aPagamento /ePagamento/dPagamento/vPagamento/aLancamento/eLancamento/dLancamento/vLancamento/cUsuario/cEmitente/cPermissao/cBackup/cAuditoria/cEmail /cSistema/rCliente/rProduto/rServico/rOs/rVenda /rFinanceiro/aCobranca/eCobranca/dCobranca /vCobranca/situacao/idPermissao/id leads to cross-site scripting. This vulnerability was named CVE-2022-48326. 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-2022-48327	Mapos 4.39.0 Relatorios.php cross-site scripting (ID 2010)	A vulnerability was found in Mapos 4.39.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file application/controllers /Relatorios.php. The manipulation of the argument dataInicial/dataFinal/tipocliente/format/precoInicial /precoFinal/estoqueInicial/estoqueFinal/de_id/ate_id /clientes_id/origem/cliente/responsavel/status/tipo /situacao leads to cross-site scripting. This vulnerability is known as CVE-2022-48327. 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-2019-17003	Mozilla Firefox on iOS QR Code Parser cross-site scripting	A vulnerability was found in Mozilla Firefox and classified as problematic. Affected by this issue is some unknown functionality of the component QR Code Parser. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2019-17003. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0878	nuxt framework up to 3.2.0 crosssite scripting	A vulnerability classified as problematic was found in nuxt framework up to 3.2.0. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-0878. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-24769	Changedetection.io up to 0.40.1.0 Add a new change detection watch URL cross-site scripting (ID 1358)		Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-48115	jspreadsheet up to 4.5.x Dropdown Menu cross-site scripting (ID 1587)	A vulnerability was found in jspreadsheet up to 4.5.x and classified as problematic. Affected by this issue is some unknown functionality of the component Dropdown Menu. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-48115. 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-2023-0902	SourceCodester Simple Food Ordering System 1.0 process_order.php order cross-site scripting	A vulnerability was found in SourceCodester Simple Food Ordering System 1.0. It has been classified as problematic. This affects an unknown part of the file process_order.php. The manipulation of the argument order leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-0902. 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-2023-24369	UJCMS 4.1.3 Add New Articles URL cross-site scripting	A vulnerability which was classified as problematic has been found in UJCMS 4.1.3. This issue affects some unknown processing of the component Add New Articles. The manipulation of the argument URL leads to crosssite scripting. The identification of this vulnerability is CVE-2023-24369. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-4754	Easy Social Box Plugin up to 4.1.2 on WordPress Shortcode Attribute cross-site scripting	A vulnerability classified as problematic has been found in Easy Social Box Plugin up to 4.1.2. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-4754. 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-2023-0378	Greenshift Plugin up to 4.x on WordPress Block Option cross-site scripting	A vulnerability was found in Greenshift Plugin up to 4.x. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Block Option Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-0378. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-4784	Hueman Addons Plugin up to 2.3.3 on WordPress Shortcode Attribute cross-site scripting	A vulnerability which was classified as problematic was found in Hueman Addons Plugin up to 2.3.3. 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-2022-4784. 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-2023-0366	Loan Comparison Plugin up to 1.5.2 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in Loan Comparison Plugin up to 1.5.2. 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-2023-0366. 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-2023-0442	Loan Comparison Plugin up to 1.5.2 on WordPress Shortcode cross-site scripting	A vulnerability was found in Loan Comparison Plugin up to 1.5.2 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-2023-0442. 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-2022-4622	Login Logout Menu Plugin up to 1.3.3 on WordPress Shortcode Attribute cross-site scripting	A vulnerability which was classified as problematic was found in Login Logout Menu Plugin up to 1.3.3. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-4622. 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-2022-4752	Opening Hours Plugin up to 2.3.0 on WordPress Shortcode Attribute cross-site scripting	A vulnerability which was classified as problematic has been found in Opening Hours Plugin up to 2.3.0. 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-2022-4752. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-4761	Post Views Count Plugin up to 3.0.2 on WordPress Shortcode Attribute cross-site scripting	A vulnerability classified as problematic was found in Post Views Count Plugin up to 3.0.2. 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-2022-4761. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-4791	Product Slider and Carousel with Category for Woo-Commerce Plugin Shortcode Attribute crosssite scripting	A vulnerability was found in Product Slider and Carousel with Category for WooCommerce Plugin up to 2.7. It has been rated as problematic. This issue affects some unknown processing of the compo-nent Shortcode Attribute Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-4791. 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-2022-4764	Simple File Down-loader Plugin up to 1.0.4 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in Simple File Downloader Plugin up to 1.0.4. It has been classified as prob-lematic. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-4764. It is possible to launch the at-tack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2020-36656	Spectra Plugin up to 1.14.x on WordPress Gutenberg Block crosssite scripting	A vulnerability which was classified as problem-atic has been found in Spectra Plugin up to 1.14.x. This issue affects some unknown processing of the component Gutenberg Block Handler. The manip-ulation leads to cross-site scripting. The identification of this vulnerability is CVE-2020-36656. 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-2022-4785	Video Sidebar Widgets Plugin up to 6.1 on WordPress Shortcode Attribute cross-site scripting	A vulnerability has been found in Video Sidebar Widgets Plugin up to 6.1 and classified as prob-lematic. This vulnerability affects unknown code of the component Short-code Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-4785. The attack can be initiated remotely. There is no ex-ploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-4786	Video.js Plugin up to 4.5.0 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in Video.js Plugin up to 4.5.0 and classified as problematic. This issue affects some unknown processing of the compo-nent Shortcode Attribute Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-4786. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0966	SourceCodester On-line Eyewear Shop 1.0 id cross-site scripting	A vulnerability classified as problematic was found in SourceCodester Online Eyewear Shop 1.0. Affected by this vulnerability is an unknown functionality of the file admin/pageorders/view_order. The manip-ulation of the argument id leads to cross-site scripting. This vulnerability is known as CVE-2023-0966. The attack can be launched re-motely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1067	pimcore up to 10.5.17 cross-site scripting	A vulnerability was found in pimcore up to 10.5.17. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to crosssite scripting. The identification of this vulnerability is CVE-2023-1067. 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.

XML External Entity Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-24323	Mojoportal 2.7 xml external entity reference	A vulnerability which was classified as problematic has been found in Mojoportal 2.7. This issue affects some unknown processing. The manipulation leads to xml external entity reference. The identification of this vulnerability is CVE-2023-24323. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as XML External Entity Attack.
CVE-2023-24187	ureport 2.2.9 XML saveReportFile xml external entity reference	A vulnerability classified as problematic was found in ureport 2.2.9. Affected by this vulnerability is an unknown functionality of the file /ureport/designer/saveReportFile of the component XML Handler. The manipulation leads to xml external entity reference. This vulnerability is known as CVE-2023-24187. 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 XML External Entity Attack.
CVE-2014-125087	java-xmlbuilder up to 1.1 xml external entity reference	A vulnerability was found in java-xmlbuilder up to 1.1. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to xml external entity reference. This vulnerability is handled as CVE-2014-125087. 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 XML External Entity Attack.

CRLF Injection Vulnerability

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-23936	Undici prior 5.19.1 HTTP Header crlf injection (GHSA-5r9g-qh6m-jxff)	A vulnerability which was classified as critical was found in Undici. Affected is an unknown function of the component HTTP Header Handler. The manipulation leads to crlf injection. This vulnerability is traded as CVE-2023-23936. 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 CRLF Injection attack.

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-23135	Ftdms 3.1.6 JPG File unrestricted upload	A vulnerability was found in Ftdms 3.1.6. It has been classified as critical. Affected is an unknown function of the component JPG File Handler. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2023-23135. The attack can only be initiated within the local network. There is no exploit available.	Protected by custom rules	NA
CVE-2022-47854	i-librarian 4.10 ajaxsupplement.php unrestricted upload (ID 155)	A vulnerability was found in i-librarian 4.10. It has been rated as critical. This issue affects some unknown processing of the file ajaxsupplement.php. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2022-47854. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by custom rules	NA
CVE-2022-47769	Serenissima Informatica Fast Checkin 1.0 unrestricted upload	A vulnerability classified as critical has been found in Serenissima Informatica Fast Checkin 1.0. This affects an unknown part. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2022-47769. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by custom rules	NA
CVE-2023-0587	Trend Micro Apex One Build 11110 Header fcgiOfcDDA.exe Content-Length unrestricted upload	A vulnerability classified as critical was found in Trend Micro Apex One Build 11110. This vulnerability affects unknown code of the file /officescan/console/html/cgi/fcgiOfcDDA.exe of the component Header Handler. The manipulation of the argument Content-Length leads to unrestricted upload. This vulnerability was named CVE-2023-0587. The attack can be initiated remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2022-46604	Tecrail Responsive FileManager up to 9.9.5 File Extension Check unrestricted upload	A vulnerability was found in Tecrail Responsive FileManager up to 9.9.5. It has been rated as problematic. This issue affects some unknown processing of the component File Extension Check. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2022-46604. 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 custom rules	NA
CVE-2021-36426	phpwcms 1.9.25 general.inc.php unrestricted upload (ID 312)	A vulnerability classified as critical has been found in phpwcms 1.9.25. This affects an unknown part in the library include/inc_lib/general.inc.php. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2021-36426. It is possible to initiate the attack remotely. There is no exploit available.	Protected by custom rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-36225	Western Digital My Cloud prior OS5 REST API unrestricted upload	A vulnerability has been found in Western Digital My Cloud and classified as critical. Affected by this vulnerability is an unknown functionality of the component REST API. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2021-36225. Access to the local network is required for this attack. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by custom rules	NA
CVE-2022-45544	SCHLIX CMS 2.2.7-2 tristao unrestricted upload	A vulnerability classified as critical was found in SCHLIX CMS 2.2.7-2. This vulnerability affects unknown code. The manipulation of the argument tristao leads to unrestricted upload. This vulnerability was named CVE-2022-45544. The attack can only be initiated within the local network. There is no exploit available.	Protected by custom rules	NA
CVE-2022-45527	Future-Depth IMS 1.0 File Upload unrestricted upload	A vulnerability has been found in Future- Depth IMS 1.0 and classified as critical. This vulnerability affects unknown code of the component File Upload Handler. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2022-45527. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by custom rules	NA
CVE-2023-0783	EcShop 4.1.5 PHP File template.php unrestricted upload	A vulnerability was found in EcShop 4.1.5. It has been classified as critical. This affects an unknown part of the file /ecshop/admin / template.php of the component PHP File Handler. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-0783. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by custom rules	NA
CVE-2023-0255	Enable Media Replace Plugin up to 4.0.1 on WordPress unrestricted upload	A vulnerability has been found in Enable Media Replace Plugin up to 4.0.1 and classified as critical. This vulnerability affects unknown code. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-0255. The attack can be initiated remotely.There is no exploit available. It is recommended to upgrade the affected component.	Protected by custom rules	NA
CVE-2023-24646	SourceCodester Food Ordering System 2.0 PHP File /fos/admin/ajax.php unrestricted upload	A vulnerability was found in SourceCodester Food Ordering System 2.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /fos/admin /ajax.php of the component PHP File Handler. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-24646. The attack needs to be approached within the local network. There is no exploit available.	Protected by custom rules	NA

Indusface is a leading application security SaaS company that secures critical Web, Mobile & API applications of 5000+ global customers using its award-winning fully managed platform that integrates a web application scanner, web application firewall, DDoS &, BOT Mitigation, CDN, and threat intelligence engine. The company has been funded by Tata Capital Growth Fund, is Great Place to Work certified, mentioned by analysts like Gartner, Forrester, etc in their reports, and has been the recipient of many awards such as the Economic Times Top 25, NASSCOM DSCI Top Security Company, Deloitte Asia Top 100 , and several other such prestigious recognitions.

CONTACT US - +91 265 6133021 | +1 866 537 8234
EMAIL - sales@indusface.com

Indusface is the only cloud WAAP (WAF) vendor with 100% customer recommendation for 3 consecutive years

A Customers' Choice for 2022 and 2023 Gartner® Peer Insights™