INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

June 2023

The total zero-day vulnerabilities count for June month : 266

Command Injection	CSRF	Local File Inclusion	Malicious File Upload	SQL Injection	Cross-site Scripting	XML External Entity
18	19	28	20	57	123	1

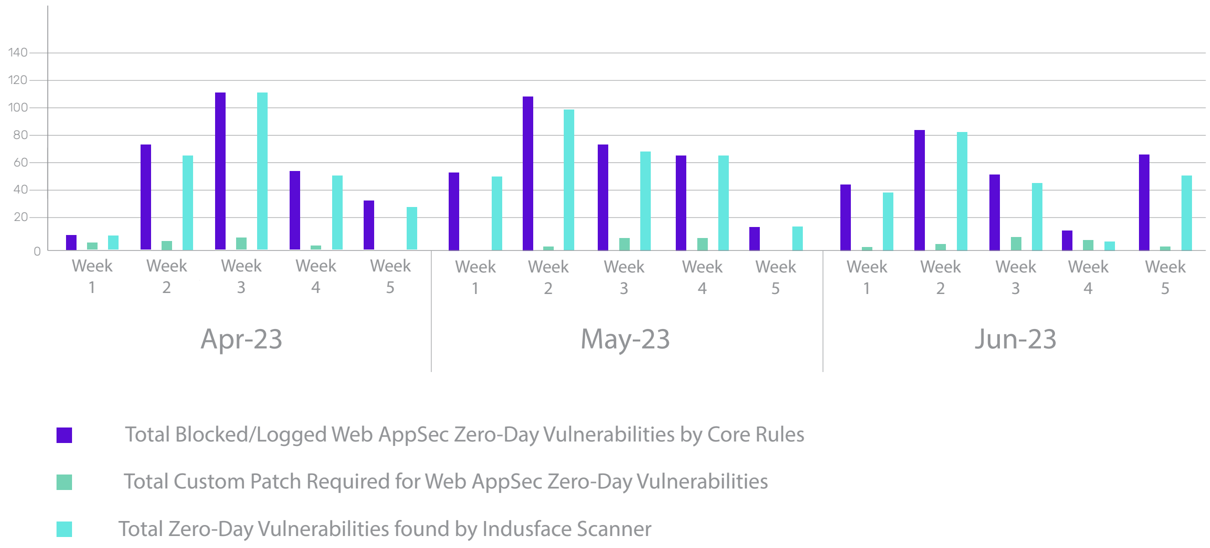
Zero-day vulnerabilities protected through core rules	248
Zero-day vulnerabilities protected through custom rules	18
Zero-day vulnerabilities for which protection can not be done	0
Zero-day vulnerabilities found by Indusface WAS	227

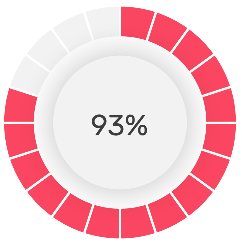
- To enable custom rules, please contact support@indusface.com
- Since the attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.

Vulnerability Trend:

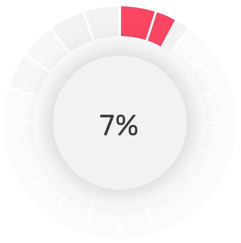
The weekly trend displays the total number of vulnerabilities discovered to the type of protection provided for the last quarter.

Weekly Vulnerability Trend

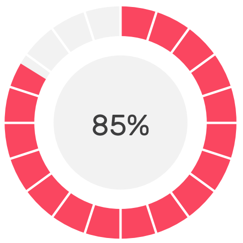




of the zero-day vulnerabilities were protected by the **core rules** in the last month.

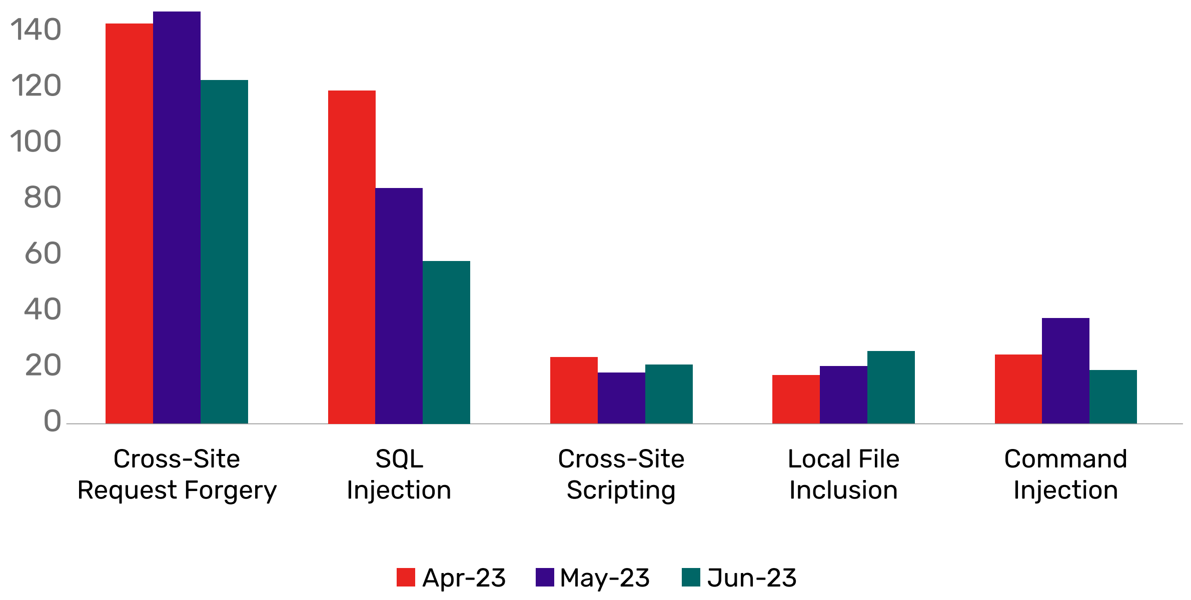


of the zero-day vulnerabilities were protected by the **custom rules** in the last month.



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-2021-45039	Uniview IPC_G6103 Service Port 7788 os command injection	A vulnerability was found in Uniview IPC_G6103 IPC_G61 IPC21 IPC23 IPC32 IPC36 IPC62 and IPC_HCMN. It has been classified as critical. This affects an unknown part of the component Service Port 7788. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2021-45039. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-3097	KylinSoft kylin-software-properties prior 0.0.1-130 on KylinOS setMainSource os command injection	A vulnerability was found in KylinSoft kylin-software-properties on KylinOS. It has been rated as critical. This issue affects the function setMainSource. The manipulation leads to os command injection. The identification of this vulnerability is CVE-2023-3097. Local access is required to approach this attack. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-31569	TOTOLINK X5000R 9.1.0cu.2350_B20230313 setWanCfg command injection	“A vulnerability was found in TOTOLINK X5000R 9.1.0cu.2350_B20230313 and classified as critical. Affected by this issue is the function setWanCfg. The manipulation leads to command injection. This vulnerability is handled as CVE-2023-31569. 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-2023-34111	taosdata grafanaplugin GitHub Action command injection (GHSA-23wp-p848-hcgr)	"A vulnerability has been found in taosdata grafanaplugin and classified as critical. Affected by this vulnerability is an unknown functionality of the component GitHub Action Handler. The manipulation leads to command injection. This vulnerability is known as CVE-2023-34111. The attack can be launched remotely. There is no exploit available."	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-33532	Netgear R6250 1.0.4.48 Web Management command injection	"A vulnerability which was classified as critical was found in Netgear R6250 1.0.4.48. Affected is an unknown function of the component Web Management. The manipulation leads to command injection. This vulnerability is traded as CVE-2023-33532. 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-2023-33533	Netgear D6220/ D8500/R6700/R6900 Web Management command injection	"A vulnerability has been found in Netgear D6220 D8500 R6700 and R6900 and classified as critical. Affected by this vulnerability is an unknown functionality of the component Web Management. The manipulation leads to command injection. This vulnerability is known as CVE-2023-33533. 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-2023-33381	MitraStar GPT-2741GNAC AR_g5.8_110WVN0b7_2 Ping command injection	"A vulnerability was found in MitraStar GPT-2741GNAC AR_g5.8_110WVN0b7_2. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Ping Handler. The manipulation leads to command injection. This vulnerability is known as CVE-2023-33381. 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-2023-30400	Anyka AK3918EV300 MCU 18 WiFi command injection	"A vulnerability has been found in Anyka AK3918EV300 MCU 18 and classified as critical. Affected by this vulnerability is an unknown functionality of the component WiFi Handler. The manipulation leads to command injection. This vulnerability is known as CVE-2023-30400. 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-2023-33538	TP-LINK TL-WR940N/TL-WR841N/TL-WR740N /userRpm/WlanNetworkRpm command injection	"A vulnerability which was classified as critical has been found in TP-LINK TL-WR940N TL-WR841N and TL-WR740N. Affected by this issue is some unknown functionality of the file /userRpm/WlanNetworkRpm. The manipulation leads to command injection. This vulnerability is handled as CVE-2023-33538. 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-2023-33782	D-Link DIR-842V2 1.0.3 iperf3 command injection	"A vulnerability was found in D-Link DIR-842V2 1.0.3. It has been declared as critical. This vulnerability affects unknown code of the component iperf3. The manipulation leads to command injection. This vulnerability was named CVE-2023-33782. 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-2023-33556	TOTOLINK A7100RU 7.4cu.2313_B20191024 /setting/setWanleCfg staticGw command injection	"A vulnerability was found in TOTOLINK A7100RU 7.4cu.2313_B20191024. It has been rated as critical. This issue affects some unknown processing of the file /setting/setWanleCfg. The manipulation of the argument staticGw leads to command injection. The identification of this vulnerability is CVE-2023-33556. The attack can only be initiated within the local network. There is no exploit available."	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-34112	JavaCPP Presets up to 1.5.8 Commit Message github.event.head_commit.message code injection (GHSA-36rx-hq22-	"A vulnerability was found in JavaCPP Presets up to 1.5.8 and classified as critical. Affected by this issue is some unknown functionality of the component Commit Message Handler. The manipulation of the argument github.event.head_commit.message leads to code injection. This vulnerability is handled as CVE-2023-34112. 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-2023-34105	SRS prior 5.0-b1/5.0.157/6.0.48 POST Request /api/v1/snapshots os command injection (GHSA-vpr5-779c-cx62)	"A vulnerability was found in SRS and classified as critical. This issue affects some unknown processing of the file /api/v1/snapshots of the component POST Request Handler. The manipulation leads to os command injection. The identification of this vulnerability is CVE-2023-34105. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component."	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-33625	D-Link DIR-600 2.18 lxmldbc_system ST command injection	"A vulnerability was found in D-Link DIR-600 2.18 and classified as critical. This issue affects the function lxmldbc_system. The manipulation of the argument ST leads to command injection. The identification of this vulnerability is CVE-2023-33625. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-27836	TP-LINK TL-WPA8630P 171011 sub_40A80C devicePwd command injection	"A vulnerability classified as critical was found in TP-LINK TL-WPA8630P 171011. This vulnerability affects the function sub_40A80C. The manipulation of the argument devicePwd leads to command injection. This vulnerability was named CVE-2023-27836. 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-2023-27837	TP-LINK TL-WPA8630P 171011 sub_40A774 key command injection	"A vulnerability which was classified as critical has been found in TP-LINK TL-WPA8630P 171011. Affected by this issue is the function sub_40A774. The manipulation of the argument key leads to command injection. This vulnerability is handled as CVE-2023-27837. The attack can only be initiated within the local network. There is no exploit available."	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-34800	D-Link Go-RT-AC750 101b03 genacgi_main service command injection	"A vulnerability classified as critical was found in D-Link Go-RT-AC750 101b03. Affected by this vulnerability is the function genacgi_main. The manipulation of the argument service leads to command injection. This vulnerability is known as CVE-2023-34800. 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-2023-1721	Yoga Class Registration System 1.0 command injection	A vulnerability was found in Yoga Class Registration System 1.0. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to command injection. This vulnerability was named CVE-2023-1721. The attack can be initiated remotely. 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-2023-3029	Guangdong Pythagorean OA Office System up to 4.50.31 /note/index/delete id cross-site request forgery (I74VRG)	A vulnerability has been found in Guangdong Pythagorean OA Office System up to 4.50.31 and classified as problematic. This vulnerability affects unknown code of the file /note/index/delete. The manipulation of the argument id leads to cross-site request forgery. This vulnerability was named CVE-2023-3029. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-2405	vcita CRM and Lead Management Plugin up to 2.6.2 on WordPress cross-site request forgery	A vulnerability classified as problematic was found in vcita CRM and Lead Management Plugin up to 2.6.2 on WordPress. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-2405. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-2407	vcita Event Registration Calendar Plugin up to 1.3.1/3.9.1 on WordPress cross-site request forgery	A vulnerability was found in vcita Event Registration Calendar Plugin up to 1.3.1/3.9.1 on WordPress and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-2407. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-3075	tsolucio corebos up to 7 cross-site request forgery	A vulnerability has been found in tsolucio corebos up to 7 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-3075. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-2416	vcita Online Booking & Scheduling Calendar Plugin up to 4.2.10 on WordPress vcita_logout_callback cross-site request forgery	A vulnerability has been found in vcita Online Booking & Scheduling Calendar Plugin up to 4.2.10 on WordPress and classified as problematic. This vulnerability affects the function vcita_logout_callback. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-2416. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-2601	WP Brutal AI Plugin up to 1.x on WordPress cross-site request forgery	"A vulnerability which was classified as problematic was found in WP Brutal AI Plugin up to 1.x on WordPress. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-2601. 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-2020-36717	Kali Forms Plugin up to 2.1.1 on WordPress cross-site request forgery	"A vulnerability was found in Kali Forms Plugin up to 2.1.1 on WordPress. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2020-36717. It is possible to launch the attack remotely. There is no exploit available."	Protected by core rules	NA
CVE-2021-4349	Process Steps Template Designer Plugin up to 1.2.1 on WordPress cross-site request forgery	"A vulnerability was found in Process Steps Template Designer Plugin up to 1.2.1 on WordPress and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2021-4349. The attack may 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-2021-4342	Plugins on WordPress cross-site request forgery	"A vulnerability has been found in Plugins on WordPress and classified as critical. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2021-4342. The attack can be initiated remotely. There is no exploit available."	Protected by core rules	NA
CVE-2023-2277	WP Directory Kit Plugin up to 1.1.9 on WordPress Setting cross-site request forgery	"A vulnerability was found in WP Directory Kit Plugin up to 1.1.9 on WordPress. It has been classified as problematic. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-2277. It is possible to initiate the attack remotely. There is no exploit available."	Protected by core rules	NA
CVE-2023-2628	KiviCare Plugin up to 3.2.0 on WordPress AJAX Action cross-site request forgery	A vulnerability was found in KiviCare Plugin up to 3.2.0 on WordPress and classified as problematic. Affected by this issue is some unknown functionality of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-2628. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-2627	KiviCare Plugin up to 3.2.0 on WordPress Setting cross-site request forgery	A vulnerability was found in KiviCare Plugin up to 3.2.0 on WordPress. It has been rated as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-2627. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-3320	WP Sticky Social Plugin up to 1.0.1 on WordPress cross-site request forgery	A vulnerability was found in WP Sticky Social Plugin up to 1.0.1 on WordPress and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-3320. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2020-21366	GreenCMS 2.3 index.php adduser cross-site request forgery (Issue 115)	A vulnerability was found in GreenCMS 2.3. It has been rated as problematic. Affected by this issue is the function adduser of the file index.php. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2020-21366. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2020-21252	Neeke HongCMS 3.0.0 updateusers cross-site request forgery (Issue 13)	A vulnerability was found in Neeke HongCMS 3.0.0 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument updateusers leads to cross-site request forgery. This vulnerability is handled as CVE-2020-21252. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2020-20502	yzCMS 2.0 Token Check cross-site request forgery (Issue 27)	A vulnerability which was classified as problematic was found in yzCMS 2.0. This affects an unknown part of the component Token Check Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2020-20502. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-34927	Casdoor up to 1.331.0 URL /api/set-password cross-site request forgery (Issue 1531)	A vulnerability which was classified as problematic was found in Casdoor up to 1.331.0. This affects an unknown part of the file /api/set-password of the component URL Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-34927. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-36345	POS Codekop 2.0 cross-site request forgery	A vulnerability was found in POS Codekop 2.0. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-36345. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-1722	Yoga Class Registration System 1.0 cross-site request forgery	A vulnerability was found in Yoga Class Registration System 1.0. 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-2023-1722. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-29159	Starlette up to 0.26.x path traversal (GHSA-v5gw-mw7f-84px)	A vulnerability which was classified as critical has been found in Starlette up to 0.26.x. Affected by this issue is some unknown functionality. The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-29159. 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-2023-33544	hawtio 2.17.2 ZIP Decompression path traversal (Issue 2832)	A vulnerability was found in hawtio 2.17.2. It has been classified as critical. This affects an unknown part of the component ZIP Decompression Handler. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-33544. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-27640	tshirtecommerce 2.1.4 on PrestaShop POST Parameter fonts.php type path traversal	A vulnerability was found in tshirtecommerce 2.1.4 on PrestaShop and classified as critical. This issue affects some unknown processing of the file /tshirtecommerce/fonts.php of the component POST Parameter Handler. The manipulation of the argument type leads to path traversal. The identification of this vulnerability is CVE-2023-27640. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-27639	tshirtecommerce 2.1.4 on PrestaShop POST Parameter ajax.php file_name path traversal	A vulnerability has been found in tshirtecommerce 2.1.4 on PrestaShop and classified as critical. This vulnerability affects unknown code of the file tshirtecommerce/ajax.phptypesvg of the component POST Parameter Handler. The manipulation of the argument file_name leads to path traversal. This vulnerability was named CVE-2023-27639. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-3056	YFCMF up to 3.0.4 index.php path traversal	A vulnerability was found in YFCMF up to 3.0.4. It has been declared as problematic. This vulnerability affects unknown code of the file index.php. The manipulation leads to path traversal: &039;../filedir&039;. This vulnerability was named CVE-2023-3056. The attack can be initiated remotely. Furthermore there is an 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-2023-3057	YFCMF up to 3.0.4 Ajax.php controllername path traversal	A vulnerability was found in YFCMF up to 3.0.4. It has been rated as problematic. This issue affects some unknown processing of the file app/admin/controller/Ajax.php. The manipulation of the argument controllername leads to path traversal: &039;../filedir&039;. The identification of this vulnerability is CVE-2023-3057. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-29736	Keyboard Themes 1.275.1.164 on Android path traversal	A vulnerability was found in Keyboard Themes 1.275.1.164 on Android. It has been classified as critical. This affects an unknown part. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-29736. Attacking locally is a requirement. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-3031	King-Avis prior 17.3.15 on Prestashop Download Token path traversal	A vulnerability was found in King-Avis on Prestashop. It has been classified as problematic. This affects an unknown part of the component Download Token Handler. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-3031. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-33690	SonicJS up to 0.7.0 Backup path traversal	A vulnerability was found in SonicJS up to 0.7.0. It has been rated as critical. Affected by this issue is some unknown functionality of the component Backup Handler. The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-33690. The attack can only be done within the local network. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-3098	KylinSoft youker-assistant prior 3.0.2-0kylin6k70-23 on KylinOS restore_all_sound_file path traversal	A vulnerability classified as critical has been found in KylinSoft youker-assistant on KylinOS. Affected is the function restore_all_sound_file. The manipulation leads to path traversal: &039;../filedir&039;. This vulnerability is traded as CVE-2023-3098. Attacking locally is a requirement. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-34407	Harbinger Offline Player 4.0.6.0.2 OfflinePlayerService.exe path traversal	A vulnerability has been found in Harbinger Offline Player 4.0.6.0.2 and classified as critical. Affected by this vulnerability is an unknown functionality of the file OfflinePlayerService.exe. The manipulation leads to path traversal: &039;..\filedir&039;. This vulnerability is known as CVE-2023-34407. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-33747	CloudPanel 2.2.2 path traversal	"A vulnerability was found in CloudPanel 2.2.2. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to path traversal. This vulnerability was named CVE-2023-33747. The attack needs to be done within the local network. There is no exploit available. It is recommended to upgrade the affected component."	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2020-36728	Adning Advertising Plugin up to 1.5.5 on WordPress path traversal	"A vulnerability was found in Adning Advertising Plugin up to 1.5.5 on WordPress. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to path traversal. This vulnerability was named CVE-2020-36728. The attack can be initiated remotely. Furthermore there is an exploit available."	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-34096	sni Thruk up to 3.06/3.06.2 http://panorama.pm path traversal (GHSA-vh-qc-649h-994h)	"A vulnerability was found in sni Thruk up to 3.06/3.06.2. It has been rated as critical. Affected by this issue is some unknown functionality of the file http://panorama.pm . The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-34096. The attack may be launched remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue."	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-34238	Gatsby path traversal (GHSA-c6f8-8r25-c4gc)	"A vulnerability was found in Gatsby and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-34238. 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-2023-3172	froxlor up to 2.0.19 path traversal	"A vulnerability classified as critical was found in froxlor up to 2.0.19. Affected by this vulnerability is an unknown functionality. The manipulation leads to path traversal. This vulnerability is known as CVE-2023-3172. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component."	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-3241	OTCMS up to 6.62 read.php url path traversal	"A vulnerability was found in OTCMS up to 6.62 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/read.phpmudiannounContent. The manipulation of the argument url leads to path traversal. This vulnerability is handled as CVE-2023-3241. The attack can only be done within the local network. Furthermore there is an exploit available."	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-3239	OTCMS up to 6.62 readDeal.php img path traversal	"A vulnerability which was classified as problematic was found in OTCMS up to 6.62. Affected is an unknown function of the file admin/readDeal.phpmudireadQrCode. The manipulation of the argument img leads to path traversal: &039;../filedir&039;. This vulnerability is traded as CVE-2023-3239. Access to the local network is required for this attack to succeed. Furthermore there is an 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-2023-3240	OTCMS up to 6.62 usersNews_deal.php file path traversal	"A vulnerability has been found in OTCMS up to 6.62 and classified as problematic. Affected by this unknown functionality of the file usersNews_deal.php. The manipulation of the argument file leads to path traversal: &039;../filedir&039;. This vulnerability is known as CVE-2023-3240. The attack needs to be approached within the local network. Furthermore there is an exploit available."	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-34865	UJCMS 6.0.2 Rename path traversal	"A vulnerability was found in UJCMS 6.0.2 and classified as critical. Affected by this issue is some unknown functionality of the component Rename Handler. The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-34865. 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 local file inclusion attack.
CVE-2023-34880	cmseasy 7.7.7.7 language_admin.php add_action path traversal	"A vulnerability classified as critical has been found in cmseasy 7.7.7.7. Affected is the function add_action in the library lib/admin/language_admin.php. The manipulation leads to path traversal. This vulnerability is traded as CVE-2023-34880. 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.
CVE-2023-34645	Jfinal CMS 5.1.0 path traversal (Issue 57)	"A vulnerability which was classified as problematic has been found in Jfinal CMS 5.1.0. This issue affects some unknown processing. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-34645. The attack can only be initiated within the local network. There is no exploit available."	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-36612	com.basecamp.bc3 up to 4.2.0 on Android Deeplink Scheme path traversal	A vulnerability has been found in com.basecamp.bc3 up to 4.2.0 on Android and classified as critical. This vulnerability affects unknown code of the component Deeplink Scheme Handler. The manipulation leads to path traversal. This vulnerability was named CVE-2023-36612. 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 local file inclusion attack.
CVE-2023-32521	Trend Micro Mobile Security 9.8 SP5 path traversal	A vulnerability which was classified as critical has been found in Trend Micro Mobile Security 9.8 SP5. This issue affects some unknown processing. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-32521. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-32522	Trend Micro Mobile Security 9.8 SP5 path traversal	A vulnerability was found in Trend Micro Mobile Security 9.8 SP5. It has been classified as critical. This affects an unknown part. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-32522. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2020-20718	PluckCMS 4.7.10 Image File save_file unrestricted upload (Issue 79)	A vulnerability was found in PluckCMS 4.7.10. It has been classified as critical. This affects the function save_file of the component Image File Handler. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2020-20718. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-35843	NocoDB up to 0.109.1 /download path information disclosure	A vulnerability was found in NocoDB up to 0.109.1. It has been classified as problematic. Affected is an unknown function of the file /download. The manipulation of the argument path leads to information disclosure. This vulnerability is traded as CVE-2023-35843. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-23678	WP Cookie Notice for GDPR, CCPA & ePrivacy Consent Plugin csv injection	A vulnerability has been found in WP Cookie Notice for GDPR CCPA & ePrivacy Consent Plugin up to 2.2.5 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to csv injection. This vulnerability is known as CVE-2023-23678. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-2068	File Manager Advanced Shortcode Plugin up to 2.3.2 on WordPress unrestricted upload	A vulnerability was found in File Manager Advanced Shortcode Plugin up to 2.3.2 on WordPress. It has been classified as critical. Affected is an unknown function of the component Shortcode Handler. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2023-2068. It is possible to launch the attack remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2020-36705	Adning Advertising Plugin up to 1.5.5 on WordPress _ning_upload_image unrestricted upload	"A vulnerability was found in Adning Advertising Plugin up to 1.5.5 on WordPress and classified as critical. Affected by this issue is the function _ning_upload_image. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2020-36705. The attack may be launched remotely. Furthermore there is an exploit available."	Protected by custom rules	NA
CVE-2023-3187	PHPGurukul Teachers Record Management System 1.0 Profile Picture /changeimage.php newpic unrestricted upload	"A vulnerability which was classified as critical has been found in PHPGurukul Teachers Record Management System 1.0. Affected by this issue is some unknown functionality of the file /changeimage.php of the component Profile Picture Handler. The manipulation of the argument newpic leads to unrestricted upload. This vulnerability is handled as CVE-2023-3187. The attack may be launched remotely. Furthermore there is an exploit available."	Protected by custom rules	NA
CVE-2023-33253	LabCollector 6.0/6.15 message unrestricted upload	"A vulnerability has been found in LabCollector 6.0/6.15 and classified as critical. Affected by this vulnerability is the function message. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2023-33253. The attack can be launched remotely. There is no exploit available."	Protected by custom rules	NA
CVE-2023-3049	TMT Lockcell up to 14 unrestricted upload	"A vulnerability was found in TMT Lockcell up to 14. It has been classified as critical. This affects an unknown part. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-3049. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component."	Protected by custom rules	NA
CVE-2023-31541	CKeditor 1.2.3 on Redmine Browse/Upload Images unrestricted upload	"A vulnerability was found in CKeditor 1.2.3 on Redmine and classified as critical. Affected by this issue is some unknown functionality of the component Browse/Upload Images. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-31541. The attack needs to be done within the local network. There is no exploit available."	Protected by custom rules	NA
CVE-2023-34747	UJCMS 6.0.2 upload unrestricted upload	"A vulnerability was found in UJCMS 6.0.2. It has been classified as critical. This affects an unknown part of the file /api/backend/core/web-file-upload/upload. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-34747. The attack needs to be approached within the local network. There is no exploit available."	Protected by custom rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-3274	code-projects Supplier Management System 1.0 Picture btn_functions.php unrestricted upload	"A vulnerability classified as critical has been found in code-projects Supplier Management System 1.0. Affected is an unknown function of the file btn_functions.php of the component Picture Handler. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2023-3274. It is possible to launch the attack remotely. Furthermore there is an exploit available."	Protected by custom rules	NA
CVE-2023-34833	ThinkAdmin 6 File / api/upload.php unrestricted upload	"A vulnerability classified as critical has been found in ThinkAdmin 6. This affects an unknown part of the file /api/upload. php of the component File Handler. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-34833. The attack needs to be approached within the local network. There is no exploit available."	Protected by custom rules	NA
CVE-2023-34845	Bludit 3.14.1 SVG File / admin/new-content unrestricted upload (Issue 1508)	"A vulnerability was found in Bludit 3.14.1 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/new-content of the component SVG File Handler. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-34845. The attack needs to be done within the local network. There is no exploit available."	Protected by custom rules	NA
CVE-2023-34660	jeecg-boot 3.5.0 upload unrestricted upload (Issue 4990)	"A vulnerability was found in jeecg-boot 3.5.0. It has been classified as critical. This affects an unknown part of the file /jeecg-boot/jmreport/upload. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-34660. Access to the local network is required for this attack to succeed. There is no exploit available."	Protected by custom rules	NA
CVE-2023-36630	CloudPanel up to 2.3.0 unrestricted upload	A vulnerability was found in CloudPanel up to 2.3.0 and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-36630. 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-2020-20210	Bludit 3.9.2 upload-images unrestricted upload (Issue 1079)	A vulnerability was found in Bludit 3.9.2. It has been classified as critical. Affected is an unknown function of the file /admin/ajax/upload-images. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2020-20210. It is possible to launch the attack remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2023-33404	Blogengine.NET up to 3.3.8.0 UploadControlled.cs unrestricted upload	A vulnerability classified as critical was found in Blogengine.NET up to 3.3.8.0. This vulnerability affects unknown code of the file UploadControlled. cs. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-33404. The attack can be initiated remotely. There is no exploit available.	Protected by custom rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-34738	Chemex up to 3.7.1 unrestricted upload (Issue 64)	A vulnerability was found in Chemex up to 3.7.1. It has been classified as critical. This affects an unknown part. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-34738. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by custom rules	NA
CVE-2023-34736	Guantang Equipment Management System 4.12 unrestricted upload	A vulnerability was found in Guantang Equipment Management System 4.12 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-34736. Access to the local network is required for this attack. Furthermore there is an exploit available.	Protected by custom rules	NA
CVE-2023-2359	Slider Revolution Plugin up to 6.6.12 on WordPress Image File unrestricted upload	A vulnerability was found in Slider Revolution Plugin up to 6.6.12 on WordPress. It has been rated as critical. Affected by this issue is some unknown functionality of the component Image File Handler. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-2359. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2020-20067	ebCMS 1.1.0 type unrestricted upload	A vulnerability which was classified as critical was found in ebCMS 1.1.0. Affected is an unknown function. The manipulation of the argument type leads to unrestricted upload. This vulnerability is traded as CVE-2020-20067. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2020-20919	Pluck CMS 4.7.10-dev2 theme.php unrestricted upload (Issue 85)	A vulnerability classified as critical was found in Pluck CMS 4.7.10-dev2. Affected by this vulnerability is an unknown functionality of the file theme.php. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2020-20919. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2020-20969	PluckCMS 4.7.10 trashcan_restoreitem.php unrestricted upload (Issue 86)	A vulnerability which was classified as critical has been found in PluckCMS 4.7.10. Affected by this issue is some unknown functionality of the file trashcan_restoreitem.php. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2020-20969. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-30149	ebewe Autocomplete Module on PrestaShop type/input_name/q sql injection	A vulnerability classified as critical was found in ebewe Autocomplete Module on PrestaShop. Affected by this vulnerability is an unknown functionality. The manipulation of the argument type/input_name/q leads to sql injection. This vulnerability is known as CVE-2023-30149. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-3059	SourceCodester Online Exam Form Submission 1.0 /admin/update_s6.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Online Exam Form Submission 1.0. This affects an unknown part of the file /admin/update_s6.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-3059. 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-2023-3062	code-projects Agro-School Management System 1.0 index.php password sql injection	A vulnerability was found in code-projects Agro-School Management System 1.0. It has been classified as critical. Affected is an unknown function of the file index.php. The manipulation of the argument password leads to sql injection. This vulnerability is traded as CVE-2023-3062. 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-2023-3068	Campcodes Retro Cellphone Online Store 1.0 modal_add_product.php category sql injection	A vulnerability classified as critical has been found in Campcodes Retro Cellphone Online Store 1.0. Affected is an unknown function of the file /admin/modal_add_product.php. The manipulation of the argument category leads to sql injection. This vulnerability is traded as CVE-2023-3068. 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-2023-33762	eMedia simpleRedak up to 2.47.23.05 Activity sql injection	A vulnerability was found in eMedia simpleRedak up to 2.47.23.05. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument Activity leads to sql injection. The identification of this vulnerability is CVE-2023-33762. 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-2023-3094	code-projects Agro-School Management System 1.0 btn_functions.php doUpdateQuestion question_id sql injection	A vulnerability classified as critical has been found in code-projects Agro-School Management System 1.0. Affected is the function doUpdateQuestion of the file btn_functions.php. The manipulation of the argument question_id leads to sql injection. This vulnerability is traded as CVE-2023-3094. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0900	Pricing Table Builder Plugin up to 1.1.6 on WordPress sql injection	A vulnerability was found in Pricing Table Builder Plugin up to 1.1.6 on WordPress. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-0900. 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-2023-3100	IBOS 4.5.5 del actionDel id sql injection	A vulnerability which was classified as critical has been found in IBOS 4.5.5. Affected by this issue is the function actionDel of the file rdashboard/approval/del. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-3100. Access to the local network is required for this attack. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-3120	SourceCodester Service Provider Management System 1.0 view_service.php id sql injection	"A vulnerability which was classified as critical was found in SourceCodester Service Provider Management System 1.0. This affects an unknown part of the file view_service.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-3120. 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-2023-3119	SourceCodester Service Provider Management System 1.0 view.php id sql injection	"A vulnerability which was classified as critical has been found in SourceCodester Service Provider Management System 1.0. Affected by this issue is some unknown functionality of the file view.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-3119. The attack may be launched remotely. Furthermore there is an exploit available."	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-3152	SourceCodester Online Discussion Forum Site 1.0 view_post.php sql injection	"A vulnerability classified as critical has been found in SourceCodester Online Discussion Forum Site 1.0. This affects an unknown part of the file admin\posts\view_post.php. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-3152. 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-2023-3148	SourceCodester Online Discussion Forum Site 1.0 manage_post.php id sql injection	"A vulnerability was found in SourceCodester Online Discussion Forum Site 1.0 and classified as critical. This issue affects some unknown processing of the file admin\posts\manage_post.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2023-3148. The attack may be initiated remotely. Furthermore there is an exploit available."	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-3150	SourceCodester Online Discussion Forum Site 1.0 posts\manage_post.php id sql injection	"A vulnerability was found in SourceCodester Online Discussion Forum Site 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file posts\manage_post.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-3150. 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-2023-3147	SourceCodester Online Discussion Forum Site 1.0 view_category.php id sql injection	"A vulnerability has been found in SourceCodester Online Discussion Forum Site 1.0 and classified as critical. This vulnerability affects unknown code of the file admin\categories\view_category.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-3147. The attack can be initiated remotely. Furthermore there is an exploit available."	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-3151	SourceCodester Online Discussion Forum Site 1.0 user\manage_user.php id sql injection	"A vulnerability was found in SourceCodester Online Discussion Forum Site 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file user\manage_user.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-3151. The attack may be launched remotely. Furthermore there is an exploit available."	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-3146	SourceCodester Online Discussion Forum Site 1.0 manage_category.php id sql injection	"A vulnerability which was classified as critical was found in SourceCodester Online Discussion Forum Site 1.0. This affects an unknown part of the file admin\categories\manage_category.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-3146. 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-2023-3149	SourceCodester Online Discussion Forum Site 1.0 manage_user.php id sql injection	"A vulnerability was found in SourceCodester Online Discussion Forum Site 1.0. It has been classified as critical. Affected is an unknown function of the file admin\user\manage_user.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-3149. 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-2021-4340	uListing Plugin up to 1.6.6 on WordPress listing_id sql injection	"A vulnerability was found in uListing Plugin up to 1.6.6 on WordPress. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation of the argument listing_id leads to sql injection. This vulnerability is known as CVE-2021-4340. The attack can be launched remotely. There is no exploit available."	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-3145	SourceCodester Online Discussion Forum Site 1.0 Users.php username sql injection	"A vulnerability which was classified as critical has been found in SourceCodester Online Discussion Forum Site 1.0. Affected by this issue is some unknown functionality of the file classes\Users.phpfregistration. The manipulation of the argument username leads to sql injection. This vulnerability is handled as CVE-2023-3145. The attack may be launched remotely. Furthermore there is an exploit available."	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-33557	Fuel CMS 1.5.2 /controllers/Blocks.php id sql injection (Issue 604)	"A vulnerability which was classified as critical has been found in Fuel CMS 1.5.2. This issue affects some unknown processing of the file /controllers/Blocks.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2023-33557. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-3177	SourceCodester Lost and Found Information System 1.0 view_inquiry.php sql injection	"A vulnerability has been found in SourceCodester Lost and Found Information System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file admin\inquiries\view_inquiry.php. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-3177. The attack can be launched remotely. Furthermore there is an exploit available."	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-3176	SourceCodester Lost and Found Information System 1.0 manage_user.php id sql injection	"A vulnerability which was classified as critical was found in SourceCodester Lost and Found Information System 1.0. Affected is an unknown function of the file admin\user\manage_user.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-3176. 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-2023-3208	RoadFlow Visual Process Engine .NET Core Mvc 2.13.3 Login Query sidx/sord sql injection	"A vulnerability which was classified as critical has been found in RoadFlow Visual Process Engine .NET Core Mvc 2.13.3. Affected by this issue is some unknown functionality of the file / Log/Queryapid0B736354-9473-4D66-B9C0-15CAC149EB05&tabid-tab_0B73635494734D-66B9C015CAC149EB05 of the component Login. The manipulation of the argument sidx/sord leads to sql injection. This vulnerability is handled as CVE-2023-3208. The attack may be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way."	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-3047	TMT Lockcell up to 14 sql injection	"A vulnerability has been found in TMT Lockcell up to 14 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-3047. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component."	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-33817	HotelDruid Hotel Management Software 3.0.5 sql injection	"A vulnerability classified as critical has been found in HotelDruid Hotel Management Software 3.0.5. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-33817. 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-2023-34751	bloofox 0.5.2.1 index.php gid sql injection	"A vulnerability was found in bloofox 0.5.2.1. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file admin/index.phpmode-user&pagegroups&actionedit. The manipulation of the argument gid leads to sql injection. This vulnerability is known as CVE-2023-34751. 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-2023-34754	bloofox 0.5.2.1 index.php pid sql injection	"A vulnerability was found in bloofox 0.5.2.1. It has been classified as critical. Affected is an unknown function of the file admin/index.phpmodesettings&pageplugins&actionedit. The manipulation of the argument pid leads to sql injection. This vulnerability is traded as CVE-2023-34754. 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-2023-34750	bloofox 0.5.2.1 index.php cid sql injection	“A vulnerability classified as critical has been found in bloofox 0.5.2.1. This affects an unknown part of the file admin/index.phpmodesettings&pageprojects&actionedit. The manipulation of the argument cid leads to sql injection. This vulnerability is uniquely identified as CVE-2023-34750. 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-2023-34756	bloofox 0.5.2.1 index.php cid sql injection	“A vulnerability was found in bloofox 0.5.2.1 and classified as critical. This issue affects some unknown processing of the file admin/index.phpmodesettings&pagecharset&actionedit. The manipulation of the argument cid leads to sql injection. The identification of this vulnerability is CVE-2023-34756. 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-2023-34755	bloofox 0.5.2.1 index.php userid sql injection	“A vulnerability was found in bloofox 0.5.2.1. It has been rated as critical. Affected by this issue is some unknown functionality of the file admin/index.phpmodeuser&actionedit. The manipulation of the argument userid leads to sql injection. This vulnerability is handled as CVE-2023-34755. 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-2023-34753	bloofox 0.5.2.1 index.php tid sql injection	“A vulnerability classified as critical was found in bloofox 0.5.2.1. This vulnerability affects unknown code of the file admin/index.phpmodesettings&pagetmpl&actionedit. The manipulation of the argument tid leads to sql injection. This vulnerability was named CVE-2023-34753. 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-2023-34752	bloofox 0.5.2.1 index.php lid sql injection	“A vulnerability which was classified as critical has been found in bloofox 0.5.2.1. This issue affects some unknown processing of the file admin/index.phpmodesettings&pagelang&actionedit. The manipulation of the argument lid leads to sql injection. The identification of this vulnerability is CVE-2023-34752. 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-2023-31672	Length, Weight or Volume Sell up to 2.4.2 on PrestaShop sql injection	“A vulnerability which was classified as critical was found in Length Weight or Volume Sell up to 2.4.2 on PrestaShop. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-31672. 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-2023-34626	Piwigo 13.7.0 Users sql injection (Issue 1924)	“A vulnerability was found in Piwigo 13.7.0. It has been classified as critical. This affects an unknown part of the component Users Handler. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-34626. 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-2023-30625	rudder-server up to 1.2.x sql injection (GHSL-2022-097)	“A vulnerability classified as critical has been found in rudder-server up to 1.2.x. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-30625. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-34659	jeecg-boot 3.5.0/3.5.1 show id sql injection (Issue 4976)	“A vulnerability was found in jeecg-boot 3.5.0/3.5.1 and classified as critical. Affected by this issue is some unknown functionality of the file /jeecg-boot/jmreport/show. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-34659. 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-2023-34548	Simple Customer Relationship Management 1.0 Parameter email sql injection	“A vulnerability classified as critical was found in Simple Customer Relationship Management 1.0. This vulnerability affects unknown code of the component Parameter Handler. The manipulation of the argument email leads to sql injection. This vulnerability was named CVE-2023-34548. 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-2023-3310	code-projects Agro-School Management System 1.0 loaddata.php subject/course sql injection	“A vulnerability which was classified as critical has been found in code-projects Agro-School Management System 1.0. Affected by this issue is some unknown functionality of the file loaddata.php. The manipulation of the argument subject/course leads to sql injection. This vulnerability is handled as CVE-2023-3310. The attack may be launched remotely. Furthermore there is an exploit available.”	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-3307	miniCal 1.0.0 /booking/show_bookings/ search_query sql injection	“A vulnerability was found in miniCal 1.0.0. It has been rated as critical. This issue affects some unknown processing of the file /booking/show_bookings/. The manipulation of the argument search_query leads to sql injection. The identification of this vulnerability is CVE-2023-3307. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.”	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2744	ERP Plugin up to 1.12.3 on WordPress REST API Endpoint people type sql injection	A vulnerability classified as critical was found in ERP Plugin up to 1.12.3 on WordPress. This vulnerability affects unknown code of the file erp/v1/accounting/v1/people of the component REST API Endpoint Handler. The manipulation of the argument type leads to sql injection. This vulnerability was named CVE-2023-2744. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-34602	JeecgBoot up to 3.5.1 queryTableDictItemsByCode sql injection (Issue 4983)	A vulnerability classified as critical was found in JeecgBoot up to 3.5.1. Affected by this vulnerability is the function queryTableDictItemsByCode. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-34602. 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-2023-34603	JeecgBoot up to 3.5.1 queryFilterTableDictInfo sql injection (Issue 4984)	A vulnerability which was classified as critical has been found in JeecgBoot up to 3.5.1. Affected by this issue is the function queryFilterTableDictInfo. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-34603. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-2527	Contact Form 7 Plugin up to 1.2.3 on WordPress Setting sql injection	A vulnerability was found in Contact Form 7 Plugin up to 1.2.3 on WordPress. It has been declared as critical. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to sql injection. This vulnerability was named CVE-2023-2527. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2719	SupportCandy Plugin up to 3.1.6 on WordPress REST API sql injection	A vulnerability classified as critical was found in SupportCandy Plugin up to 3.1.6 on WordPress. This vulnerability affects unknown code of the component REST API. The manipulation leads to sql injection. This vulnerability was named CVE-2023-2719. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2221	WP Custom Cursors Plugin up to 3.1 on WordPress sql injection	A vulnerability classified as critical has been found in WP Custom Cursors Plugin up to 3.1 on WordPress. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2221. 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-2023-2805	SupportCandy Plugin up to 3.1.6 on WordPress set_add_agent_leaves agents[] sql injection	A vulnerability which was classified as critical was found in SupportCandy Plugin up to 3.1.6 on WordPress. Affected is the function set_add_agent_leaves. The manipulation of the argument agents[] leads to sql injection. This vulnerability is traded as CVE-2023-2805. 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-2020-20491	OpenCart up to 3.0.3.2 Fba Plugin upload/admin/index.php sql injection (Issue 7612)	A vulnerability which was classified as critical was found in OpenCart up to 3.0.3.2. This affects an unknown part of the file upload/admin/index.php of the component Fba Plugin. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2020-20491. 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-2023-34600	Adiscon LogAnalyzer up to 4.1.13 sql injection	A vulnerability which was classified as critical has been found in Adiscon LogAnalyzer up to 4.1.13. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-34600. 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-2020-21486	PHPOK 5.4 phpok_call.php _userlist sql injection	A vulnerability classified as critical has been found in PHPOK 5.4. Affected is the function _userlist of the file framework/phpok_call.php. The manipulation leads to sql injection. This vulnerability is traded as CVE-2020-21486. 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-2020-21400	PHPMyWind 5.6 modify id sql injection (Issue 11)	A vulnerability was found in PHPMyWind 5.6. It has been rated as critical. This issue affects the function modify. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2020-21400. The attack may 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-2023-3339	code-projects Agro-School Management System 1.0 exam-delete.php test_id sql injection	A vulnerability has been found in code-projects Agro-School Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file exam-delete.php. The manipulation of the argument test_id leads to sql injection. This vulnerability is known as CVE-2023-3339. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-3340	SourceCodester Online School Fees System 1.0 GET Parameter ajx.php name_startsWith sql injection	A vulnerability was found in SourceCodester Online School Fees System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file ajx.php of the component GET Parameter Handler. The manipulation of the argument name_startsWith leads to sql injection. This vulnerability is handled as CVE-2023-3340. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-33584	SourceCodester Enrollment System Project 1.0 username/password sql injection (ID 172718)	A vulnerability classified as critical was found in SourceCodester Enrollment System Project 1.0. Affected by this vulnerability is an unknown functionality. The manipulation of the argument username/password leads to sql injection. This vulnerability is known as CVE-2023-33584. 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-2023-34601	Jeesite /act/ActDao.xml sql injection (Issue 515 / 10742d3)	A vulnerability which was classified as critical has been found in Jeesite. This issue affects some unknown processing of the file /act/ActDao.xml. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-34601. The attack can only be done within the local network. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-3383	SourceCodester Game Result Matrix System 1.0 GET Parameter athlete-profile.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Game Result Matrix System 1.0. This affects an unknown part of the file /dipam/athlete-profile.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-3383. 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-2023-3391	SourceCodester Human Resource Management System 1.0 detailview.php employeeid sql injection	A vulnerability was found in SourceCodester Human Resource Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file detailview.php. The manipulation of the argument employeeid leads to sql injection. This vulnerability was named CVE-2023-3391. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-36284	Webkul QloApps 1.6.0 date_from/date_to/id_product sql injection	A vulnerability classified as critical was found in Webkul QloApps 1.6.0. Affected by this vulnerability is an unknown functionality. The manipulation of the argument date_from/date_to/id_product leads to sql injection. This vulnerability is known as CVE-2023-36284. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Cross-site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-3020	mkucej i-librarian-free up to 5.10.3 cross-sire scripting	A vulnerability which was classified as problematic was found in mkucej i-librarian-free up to 5.10.3. Affected is an unknown function. The manipulation leads to cross-sire scripting. This vulnerability is traded as CVE-2023-3020. 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-2023-33971	ormcreator up to 2.13.5 cross-sire scripting (GHSA-777g-3848-8r3g)	A vulnerability classified as problematic has been found in Formcreator up to 2.13.5. Affected is an unknown function. The manipulation leads to cross-sire scripting. This vulnerability is traded as CVE-2023-33971. 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-2023-30758	Implem Pleasanter up to 1.3.38.1 cross-sire scripting (Issue 474)	A vulnerability was found in Implem Pleasanter up to 1.3.38.1. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-sire scripting. This vulnerability is handled as CVE-2023-30758. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-3035	Guangdong Pythagorean OA Office System up to 4.50.31 Schedule description cross-sire scripting (I74ZPU)	A vulnerability has been found in Guangdong Pythagorean OA Office System up to 4.50.31 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Schedule Handler. The manipulation of the argument description leads to cross-sire scripting. This vulnerability is known as CVE-2023-3035. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-3021	mkucej i-librarian-free up to 5.10.3 cross-sire scripting	A vulnerability has been found in mkucej i-librarian-free up to 5.10.3 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-sire scripting. This vulnerability is known as CVE-2023-3021. 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-2023-2404	vcita CRM and Lead Management Plugin up to 2.6.2 on WordPress cross-sire scripting	A vulnerability was found in vcita CRM and Lead Management Plugin up to 2.6.2 on WordPress. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-sire scripting. This vulnerability was named CVE-2023-2404. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-33764	eMedia simpleRedak up to 2.47.23.05 cross-sire scripting	A vulnerability was found in eMedia simpleRedak up to 2.47.23.05. It has been classified as problematic. Affected is an unknown function of the file /de/casting/show/detail/. The manipulation leads to cross-sire scripting. This vulnerability is traded as CVE-2023-33764. 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-2023-2406	vcita Event Registration Calendar Plugin up to 1.3.1/3.9.1 on WordPress cross-sire scripting	A vulnerability classified as problematic has been found in vcita Event Registration Calendar Plugin up to 1.3.1/3.9.1 on WordPress. This affects an unknown part. The manipulation leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-2406. 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-2023-2835	WP Directory Kit Plugin up to 1.2.3 on WordPress search cross-sire scripting	A vulnerability has been found in WP Directory Kit Plugin up to 1.2.3 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument search leads to cross-sire scripting. This vulnerability is known as CVE-2023-2835. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-33731	MicroWorld eScan Management Console 14.0.1400.2281 URL cross-sire scripting	A vulnerability which was classified as problematic has been found in MicroWorld eScan Management Console 14.0.1400.2281. Affected by this issue is some unknown functionality of the component URL Handler. The manipulation leads to cross-sire scripting. This vulnerability is handled as CVE-2023-33731. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-3067	zadam trilium up to 0.59.3 cross-sire scripting	A vulnerability has been found in zadam trilium up to 0.59.3 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-sire scripting. This vulnerability was named CVE-2023-3067. 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-2023-3058	07FLY CRM up to 1.2.0 User Profile cross-sire scripting (I76K4N)	A vulnerability was found in 07FLY CRM up to 1.2.0. It has been declared as problematic. This vulnerability affects unknown code of the component User Profile Handler. The manipulation leads to cross-sire scripting. This vulnerability was named CVE-2023-3058. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-45938	Comcast microeisbss up to 2021 Inventory Management Device ID cross-sire scripting	A vulnerability which was classified as problematic has been found in Comcast microeisbss up to 2021. This issue affects some unknown processing of the component Inventory Management. The manipulation of the argument Device ID leads to cross-sire scripting. The identification of this vulnerability is CVE-2022-45938. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-3060	code-projects Agro-School Management System 1.0 btn_functions.php doAddQuestion cross-sire scripting	A vulnerability has been found in code-projects Agro-School Management System 1.0 and classified as problematic. This vulnerability affects the function doAddQuestion of the file btn_functions.php. The manipulation of the argument Question leads to cross-sire scripting. This vulnerability was named CVE-2023-3060. 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-2023-3074	tsolucio corebos up to 7 cross-sire scripting	A vulnerability which was classified as problematic was found in tsolucio corebos up to 7. This affects an unknown part. The manipulation leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-3074. 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-2023-33763	eMedia simpleRedak up to 2.47.23.05 / scheduler/index.php cross-sire scripting	A vulnerability classified as problematic has been found in eMedia simpleRedak up to 2.47.23.05. This affects an unknown part of the file /scheduler/index.php. The manipulation leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-33763. 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-2023-3086	nilsteampassnet teampass up to 3.0.8 cross-sire scripting	A vulnerability has been found in nilsteampassnet teampass up to 3.0.8 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-sire scripting. This vulnerability is known as CVE-2023-3086. 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-2023-33761	eMedia simpleRedak up to 2.47.23.05 / view/cb/format_642.php cross-sire scripting	A vulnerability was found in eMedia simpleRedak up to 2.47.23.05. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /view/cb/format_642.php. The manipulation leads to cross-sire scripting. This vulnerability is handled as CVE-2023-33761. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-3071	tsolucio corebos up to 7 cross-sire scripting	A vulnerability which was classified as problematic has been found in tsolucio corebos up to 7. Affected by this issue is some unknown functionality. The manipulation leads to cross-sire scripting. This vulnerability is handled as CVE-2023-3071. 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-2023-3083	nilsteampassnet teampass up to 3.0.8 cross-sire scripting	A vulnerability was found in nilsteampassnet teampass up to 3.0.8 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-sire scripting. The identification of this vulnerability is CVE-2023-3083. 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-2023-3070	tsolucio corebos up to 7 cross-sire scripting	A vulnerability classified as problematic was found in tsolucio corebos up to 7. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-sire scripting. This vulnerability is known as CVE-2023-3070. 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-2023-3073	tsolucio corebos up to 7 cross-sire scripting	A vulnerability was found in tsolucio corebos up to 7 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-sire scripting. The identification of this vulnerability is CVE-2023-3073. 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-2023-3084	nilsteampassnet teampass up to 3.0.8 cross-sire scripting	A vulnerability was found in nilsteampassnet teampass up to 3.0.8 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-sire scripting. This vulnerability is handled as CVE-2023-3084. 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-2023-2472	Sendinblue Newsletter, SMTP, Email Marketing and Subscribe Forms Plugin Admin Dashboard cross-sire scripting	A vulnerability classified as problematic was found in Sendinblue Newsletter SMTP Email Marketing and Subscribe Forms Plugin up to 3.1.60 on WordPress. Affected by this vulnerability is an unknown functionality of the component Admin Dashboard. The manipulation leads to cross-sire scripting. This vulnerability is known as CVE-2023-2472. 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-2023-2488	Stop Spammers Security Plugin prior 2023 on WordPress Admin Dashboard cross-sire scripting	A vulnerability was found in Stop Spammers Security Plugin on WordPress. It has been declared as problematic. This vulnerability affects unknown code of the component Admin Dashboard. The manipulation leads to cross-sire scripting. This vulnerability was named CVE-2023-2488. 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-2023-2337	ConvertKit Plugin up to 2.2.0 on WordPress Attribute cross-sire scripting	A vulnerability classified as problematic has been found in ConvertKit Plugin up to 2.2.0 on WordPress. This affects an unknown part of the component Attribute Handler. The manipulation leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-2337. 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-2023-3109	admidio up to 4.2.7 cross-sire scripting	A vulnerability classified as problematic has been found in admidio up to 4.2.7. This affects an unknown part. The manipulation leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-3109. 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-2023-2489	Stop Spammers Security Plugin prior 2023 on WordPress Setting cross-sire scripting	A vulnerability which was classified as problematic has been found in Stop Spammers Security Plugin on WordPress. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross-sire scripting. This vulnerability is handled as CVE-2023-2489. 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-2023-2571	Quiz Maker Plugin prior 6.4.2.7 on WordPress Attribute cross-sire scripting	A vulnerability has been found in Quiz Maker Plugin on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Attribute Handler. The manipulation leads to cross-sire scripting. This vulnerability is known as CVE-2023-2571. 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-2023-2572	Survey Maker Plugin up to 3.4.6 on WordPress Attribute cross-sire scripting	A vulnerability was found in Survey Maker Plugin up to 3.4.6 on WordPress. It has been classified as problematic. This affects an unknown part of the component Attribute Handler. The manipulation leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-2572. 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-2023-2503	10Web Social Post Feed Plugin up to 1.2.8 on WordPress cross-sire scripting	A vulnerability which was classified as problematic was found in 10Web Social Post Feed Plugin up to 1.2.8 on WordPress. This affects an unknown part. The manipulation leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-2503. 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-2023-34408	DokuWiki prior 2023-04-04a RSS Title cross-sire scripting	A vulnerability was found in DokuWiki and classified as problematic. Affected by this issue is some unknown functionality of the component RSS Title Handler. The manipulation leads to cross-sire scripting. This vulnerability is handled as CVE-2023-34408. 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-2023-33969	Kanboard up to 1.2.29 cross-sire scripting (GHSA-8qvf-9847-gpc9)	A vulnerability was found in Kanboard up to 1.2.29. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-sire scripting. This vulnerability was named CVE-2023-33969. 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-2023-2224	10Web SEO Plugin up to 1.2.6 on WordPress Setting cross-sire scripting	A vulnerability which was classified as problematic was found in 10Web SEO Plugin up to 1.2.6 on WordPress. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-sire scripting. This vulnerability is traded as CVE-2023-2224. 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-2023-0545	Hostel Plugin prior 1.1.5.2 on WordPress Setting cross-sire scripting	A vulnerability classified as problematic has been found in Hostel Plugin on WordPress. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-sire scripting. This vulnerability is traded as CVE-2023-0545. 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-2023-2605	WP Brutal AI Plugin up to 2.0.0 on WordPress cross-sire scripting	"A vulnerability was found in WP Brutal AI Plugin up to 2.0.0 on WordPress and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-sire scripting. The identification of this vulnerability is CVE-2023-2605. 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-2023-33977	Kiwi TCMS up to 12.3 cross-sire scripting (GHSA-2fqm-m4r2-fh98)	"A vulnerability was found in Kiwi TCMS up to 12.3. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-33977. 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-2022-46165	Syncthing up to 1.23.4 Setting cross-sire scripting (GHSA-9rp6-23gf-4c3h)	"A vulnerability has been found in Syncthing up to 1.23.4 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-sire scripting. This vulnerability is known as CVE-2022-46165. 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-2020-36722	Visual Composer Plugin up to 26.0 on WordPress cross-sire scripting	"A vulnerability was found in Visual Composer Plugin up to 26.0 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-sire scripting. This vulnerability is known as CVE-2020-36722. The attack can be launched remotely. There is no exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2021-4363	WP Quick FrontEnd Editor Plugin up to 5.5 on WordPress save_content_front cross-sire scripting	"A vulnerability classified as problematic has been found in WP Quick FrontEnd Editor Plugin up to 5.5 on WordPress. This affects the function save_content_front. The manipulation leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2021-4363. 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-2021-4378	WP Quick FrontEnd Editor Plugin up to 5.5 on WordPress cross-sire scripting	"A vulnerability has been found in WP Quick FrontEnd Editor Plugin up to 5.5 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-sire scripting. This vulnerability is known as CVE-2021-4378. The attack can be launched remotely. There is no exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2021-4372	WooCommerce Dynamic Pricing and Discounts Plugin up to 2.4.1 on WordPress Setting import cross-sire scripting	"A vulnerability was found in WooCommerce Dynamic Pricing and Discounts Plugin up to 2.4.1 on WordPress. It has been classified as problematic. This affects the function import of the component Setting Handler. The manipulation leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2021-4372. 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-2019-25150	Email Templates Plugin up to 1.3 on WordPress cross-sire scripting	"A vulnerability which was classified as problematic has been found in Email Templates Plugin up to 1.3 on WordPress. Affected by this issue is some unknown functionality. The manipulation leads to basic cross-sire scripting. This vulnerability is handled as CVE-2019-25150. The attack may be launched remotely. There is no exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2019-25140	WordPress Coming Soon Page & Maintenance Mode Plugin cross-sire scripting	"A vulnerability was found in WordPress Coming Soon Page & Maintenance Mode Plugin up to 1.8.1 on WordPress. It has been rated as problematic. This issue affects some unknown processing. The manipulation of the argument logo_width/logo_height/rcsp_logo_url/home_sec_link_txt/rcsp_headline/rcsp_description leads to cross-sire scripting. The identification of this vulnerability is CVE-2019-25140. The attack may be initiated remotely. There is no exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2019-25147	Pretty Links Plugin up to 2.1.9 on WordPress Referer Header track_link cross-sire scripting	"A vulnerability classified as problematic was found in Pretty Links Plugin up to 2.1.9 on WordPress. Affected by this vulnerability is the function track_link of the component Referer Header Handler. The manipulation leads to cross-sire scripting. This vulnerability is known as CVE-2019-25147. The attack can be launched remotely. There is no exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2020-36731	Flexible Checkout Fields for WooCommerce Plugin up to 2.3.1 on WooCommerce Setting updateSettingsAction cross-sire scripting	"A vulnerability was found in Flexible Checkout Fields for WooCommerce Plugin up to 2.3.1 on WooCommerce. It has been declared as problematic. This vulnerability affects the function updateSettingsAction of the component Setting Handler. The manipulation leads to cross-sire scripting. This vulnerability was named CVE-2020-36731. The attack can be initiated remotely. There is no exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2020-36703	Elementor Website Builder Plugin up to 2.9.7 on WordPress SVG Image Upload upload_files cross-sire scripting	"A vulnerability which was classified as problematic was found in Elementor Website Builder Plugin up to 2.9.7 on WordPress. This affects the function upload_files of the component SVG Image Upload Handler. The manipulation leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2020-36703. 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-2021-4358	WP DSGVO Tools Plugin up to 3.1.23 on WordPress cross-sire scripting	"A vulnerability was found in WP DSGVO Tools Plugin up to 3.1.23 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-sire scripting. This vulnerability is handled as CVE-2021-4358. The attack may be launched remotely. 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-2021-4367	Easy Drag & Drop Form Builder Plugin up to 1.0.35 on WordPress Options Change flo_import_forms_options cross-sire scripting	"A vulnerability which was classified as problematic has been found in Easy Drag & Drop Form Builder Plugin up to 1.0.35 on WordPress. This issue affects the function flo_import_forms_options of the component Options Change Handler. The manipulation leads to cross-sire scripting. The identification of this vulnerability is CVE-2021-4367. The attack may be initiated remotely. There is no exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2020-36711	Avada Theme up to 6.2.3 on WordPress update_layout cross-sire scripting	"A vulnerability was found in Avada Theme up to 6.2.3 on WordPress. It has been declared as problematic. This vulnerability affects the function update_layout. The manipulation leads to cross-sire scripting. This vulnerability was named CVE-2020-36711. The attack can be initiated remotely. There is no exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2021-4365	Frontend File Manager Plugin up to 18.2 on WordPress wpfm_edit_file_title_desc cross-sire scripting	"A vulnerability classified as problematic was found in Frontend File Manager Plugin up to 18.2 on WordPress. This vulnerability affects the function wpfm_edit_file_title_desc. The manipulation leads to cross-sire scripting. This vulnerability was named CVE-2021-4365. The attack can be initiated remotely. There is no exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2019-25148	WP HTML Mail Plugin up to 2.9.0.3 on WordPress cross-sire scripting	"A vulnerability classified as problematic has been found in WP HTML Mail Plugin up to 2.9.0.3 on WordPress. This affects an unknown part. The manipulation leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2019-25148. 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-2023-3142	microweber up to 1.x cross-sire scripting	"A vulnerability was found in microweber up to 1.x. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-sire scripting. This vulnerability was named CVE-2023-3142. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2021-46889	10Web Photo Gallery Plugin up to 1.5.69 on WordPress bwg_frontend_data theme_id cross-sire scripting (ID 162227)	"A vulnerability was found in 10Web Photo Gallery Plugin up to 1.5.69 on WordPress and classified as problematic. Affected by this issue is the function bwg_frontend_data. The manipulation of the argument theme_id leads to cross-sire scripting. This vulnerability is handled as CVE-2021-46889. The attack may be launched remotely. There is no exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-3143	SourceCodester Online Discussion Forum Site 1.0 manage_post.php content cross-sire scripting	"A vulnerability classified as problematic has been found in SourceCodester Online Discussion Forum Site 1.0. Affected is an unknown function of the file admin\posts\manage_post.php. The manipulation of the argument content leads to cross-sire scripting. This vulnerability is traded as CVE-2023-3143. It is possible to launch the attack remotely. Furthermore there is an exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2019-25144	WP HTML Mail Plugin up to 2.2.10 on WordPress cross-sire scripting	"A vulnerability was found in WP HTML Mail Plugin up to 2.2.10 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to basic cross-sire scripting. This vulnerability is handled as CVE-2019-25144. 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-2020-36704	Fruitful Theme up to 3.8.1 on WordPress AJAX Action fruitful_theme_options_action cross-sire scripting	"A vulnerability classified as problematic was found in Fruitful Theme up to 3.8.1 on WordPress. Affected by this vulnerability is the function fruitful_theme_options_action of the component AJAX Action Handler. The manipulation leads to cross-sire scripting. This vulnerability is known as CVE-2020-36704. The attack can be launched remotely. There is no exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2020-36709	KingComposer Plugin up to 2.9.3 on WordPress cross-sire scripting	"A vulnerability was found in KingComposer Plugin up to 2.9.3 on WordPress and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-sire scripting. The identification of this vulnerability is CVE-2020-36709. 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-2019-25146	DELUCKS SEO Plugin up to 2.1.7 on WordPress Setting saveSettings cross-sire scripting (ID 2161211)	"A vulnerability classified as problematic has been found in DELUCKS SEO Plugin up to 2.1.7 on WordPress. Affected is the function saveSettings of the component Setting Handler. The manipulation leads to cross-sire scripting. This vulnerability is traded as CVE-2019-25146. It is possible to launch the attack remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-3144	SourceCodester Online Discussion Forum Site 1.0 manage_post.php title cross-sire scripting	"A vulnerability classified as problematic was found in SourceCodester Online Discussion Forum Site 1.0. Affected by this vulnerability is an unknown functionality of the file admin\posts\manage_post.php. The manipulation of the argument title leads to cross-sire scripting. This vulnerability is known as CVE-2023-3144. The attack can be launched remotely. Furthermore there is an exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-2711	Ultimate Product Catalog Plugin up to 5.2.5 on WordPress cross-sire scripting	"A vulnerability classified as problematic was found in Ultimate Product Catalog Plugin up to 5.2.5 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-sire scripting. This vulnerability is known as CVE-2023-2711. The attack can be launched remotely. There is no exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-3165	SourceCodester Life Insurance Management System 1.0 POST Parameter insertNominee.php nominee_id cross-sire scripting	"A vulnerability was found in SourceCodester Life Insurance Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file insertNominee.php of the component POST Parameter Handler. The manipulation of the argument nominee_id leads to cross-sire scripting. This vulnerability is known as CVE-2023-3165. The attack can be launched remotely. Furthermore there is an exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-3184	SourceCodester Sales Tracker Management System 1.0 Users.php firstname/middlename/lastname/username cross-sire scripting	"A vulnerability was found in SourceCodester Sales Tracker Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /classes/Users.phpfsave. The manipulation of the argument firstname/middlename/lastname/username leads to cross-sire scripting. This vulnerability is handled as CVE-2023-3184. The attack may be launched remotely. Furthermore there is an exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-3183	SourceCodester Performance Indicator System 1.0 /admin/addproduct.php prodname cross-sire scripting	"A vulnerability was found in SourceCodester Performance Indicator System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/addproduct.php. The manipulation of the argument prodname leads to cross-sire scripting. This vulnerability is known as CVE-2023-3183. The attack can be launched remotely. Furthermore there is an exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-29712	Vade Secure Gateway X-Rewrite-URL cross-sire scripting	"A vulnerability was found in Vade Secure Gateway. It has been classified as problematic. This affects an unknown part. The manipulation of the argument X-Rewrite-URL leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-29712. 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-2023-3191	nilsteampassnet teampass up to 3.0.8 cross-sire scripting	"A vulnerability classified as problematic has been found in nilsteampassnet teampass up to 3.0.8. This affects an unknown part. The manipulation leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-3191. 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-2023-3190	nilsteampassnet teampass up to 3.0.8 cross-sire scripting	"A vulnerability was found in nilsteampassnet teampass up to 3.0.8. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to basic cross-sire scripting. This vulnerability is handled as CVE-2023-3190. 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-2023-34856	D-Link DI-7500G-CI 19.05.29A HTML File / auth_pic.cgi cross-sire scripting	"A vulnerability classified as problematic has been found in D-Link DI-7500G-CI 19.05.29A. Affected is an unknown function of the file /auth_pic.cgi of the component HTML File Handler. The manipulation leads to cross-sire scripting. This vulnerability is traded as CVE-2023-34856. 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-2023-2398	Icegram Engage Plugin up to 3.1.11 on WordPress cross-sire scripting	"A vulnerability was found in Icegram Engage Plugin up to 3.1.11 on WordPress and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-sire scripting. This vulnerability is handled as CVE-2023-2398. 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-2023-33492	EyouCMS 1.6.2 cross-sire scripting (Issue 42)	"A vulnerability classified as problematic has been found in EyouCMS 1.6.2. Affected is an unknown function. The manipulation leads to cross-sire scripting. This vulnerability is traded as CVE-2023-33492. 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-2023-34855	Youxun AC Centralized Management Platform 1.02.040 HTML File /upfile.cgi cross-sire scripting	"A vulnerability was found in Youxun AC Centralized Management Platform 1.02.040. It has been classified as problematic. This affects an unknown part of the file /upfile.cgi of the component HTML File Handler. The manipulation leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-34855. 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-2023-34941	Asus RT-N10LX 2.0.0.39 urlFilterList URL Keyword List cross-sire scripting	"A vulnerability was found in Asus RT-N10LX 2.0.0.39. It has been rated as problematic. Affected by this issue is the function urlFilterList. The manipulation of the argument URL Keyword List leads to cross-sire scripting. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is handled as CVE-2023-34941. The attack may be launched remotely. There is no exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-2718	Contact Form Email Plugin up to 1.3.37 on WordPress submitted cross-sire scripting	"A vulnerability classified as problematic has been found in Contact Form Email Plugin up to 1.3.37 on WordPress. Affected is an unknown function. The manipulation of the argument submitted leads to cross-sire scripting. This vulnerability is traded as CVE-2023-2718. 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-2023-2568	Ays Photo Gallery Plugin up to 5.1.6 on WordPress cross-sire scripting	"A vulnerability has been found in Ays Photo Gallery Plugin up to 5.1.6 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-sire scripting. This vulnerability is known as CVE-2023-2568. 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-2023-3189	SourceCodester Online School Fees System 1.0 POST Parameter /paysystem/branch.php branch cross-sire scripting	"A vulnerability which was classified as problematic was found in SourceCodester Online School Fees System 1.0. This affects an unknown part of the file /paysystem/branch.php of the component POST Parameter Handler. The manipulation of the argument branch leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-3189. 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-2023-34537	HotelDruid 3.0.5 cross-sire scripting	"A vulnerability was found in HotelDruid 3.0.5. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-sire scripting. The identification of this vulnerability is CVE-2023-34537. The attack may be initiated remotely. There is no exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2021-31280	tp5cms up to 2017-05-25 set.html keywords cross-sire scripting	"A vulnerability was found in tp5cms up to 2017-05-25. It has been declared as problematic. This vulnerability affects unknown code of the file admin.php/system/set.html. The manipulation of the argument keywords leads to cross-sire scripting. This vulnerability was named CVE-2021-31280. The attack can be initiated remotely. There is no exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-34565	Netbox 3.5.1 Create Wireless LAN Groups cross-sire scripting	"A vulnerability which was classified as problematic was found in Netbox 3.5.1. Affected is an unknown function of the component Create Wireless LAN Groups Handler. The manipulation leads to cross-sire scripting. This vulnerability is traded as CVE-2023-34565. 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-2023-34452	Grav up to 1.7.42 /forgot_password email cross-sire scripting (GHSA-xcr8-cc2j-62fc)	"A vulnerability which was classified as problematic has been found in Grav up to 1.7.42. Affected by this issue is some unknown functionality of the file /forgot_password. The manipulation of the argument email leads to cross-sire scripting. This vulnerability is handled as CVE-2023-34452. The attack may be launched remotely. There is no exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-35048	Booking and Rental Manager Plugin up to 1.2.1 on WordPress Administrator cross-sire scripting	"A vulnerability was found in Booking and Rental Manager Plugin up to 1.2.1 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Administrator Handler. The manipulation leads to cross-sire scripting. This vulnerability is handled as CVE-2023-35048. The attack may be launched remotely. There is no exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-33515	SoftExpert Excellence Suite 2.1.9 Query Screen cross-sire scripting	"A vulnerability which was classified as problematic has been found in SoftExpert Excellence Suite 2.1.9. This issue affects some unknown processing of the component Query Screen Handler. The manipulation leads to cross-sire scripting. The identification of this vulnerability is CVE-2023-33515. The attack may be initiated remotely. There is no exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-3294	saleor react-storefront cross-sire scripting (ebb-4289-411)	"A vulnerability classified as problematic has been found in saleor react-storefront. This affects an unknown part. The manipulation leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-3294. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue."	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-3293	SalesAgility SuiteCRM up to 8.2.x cross-sire scripting	"A vulnerability was found in SalesAgility SuiteCRM up to 8.2.x. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-sire scripting. This vulnerability is handled as CVE-2023-3293. 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-2023-34666	PHPGurukul Cyber Cafe Management System 1.0 username cross-sire scripting (Exploit 49204 / EDB-49204)	"A vulnerability which was classified as problematic was found in PHPGurukul Cyber Cafe Management System 1.0. Affected is an unknown function. The manipulation of the argument username leads to cross-sire scripting. This vulnerability is traded as CVE-2023-34666. It is possible to launch the attack remotely. Furthermore there is an exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-26527	WPIndeed Debug Assistant Plugin up to 1.4 on WordPress cross-sire scripting	"A vulnerability was found in WPIndeed Debug Assistant Plugin up to 1.4 on WordPress. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-26527. 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-2023-33438	Wolters Kluwer TeamMate+ 35.0.11.0 cross-sire scripting	"A vulnerability was found in Wolters Kluwer TeamMate+ 35.0.11.0. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-sire scripting. The identification of this vulnerability is CVE-2023-33438. The attack may be initiated remotely. There is no exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-3309	SourceCodester Resort Reservation System 1.0 Manage Room Page ?page=rooms Cottage Number cross-sire scripting	"A vulnerability classified as problematic was found in SourceCodester Resort Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file pagerooms of the component Manage Room Page. The manipulation of the argument Cottage Number leads to cross-sire scripting. This vulnerability is known as CVE-2023-3309. The attack can be launched remotely. Furthermore there is an exploit available."	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-3311	SourceCodester Advance Charity Management System 1.0 addsuppliers.php First name cross-sire scripting	"A vulnerability which was classified as problematic was found in SourceCodester Advance Charity Management System 1.0. This affects an unknown part of the file addsuppliers.php. The manipulation of the argument First name leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-3311. 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-2023-37255	CheckUser Extension up to 1.39.3 on MediaWiki HTTP Request Header injection	A vulnerability which was classified as critical was found in CheckUser Extension up to 1.39.3 on MediaWiki. This affects an unknown part of the component HTTP Request Header Handler. The manipulation leads to injection. This vulnerability is uniquely identified as CVE-2023-37255. 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-2023-33570	Webkul Bagisto 1.5.1 Template injection	A vulnerability was found in Webkul Bagisto 1.5.1. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Template Handler. The manipulation leads to injection. This vulnerability is handled as CVE-2023-33570. 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 cross-site scripting attack
CVE-2023-37255	CheckUser Extension up to 1.39.3 on MediaWiki HTTP Request Header injection	A vulnerability which was classified as critical was found in CheckUser Extension up to 1.39.3 on MediaWiki. This affects an unknown part of the component HTTP Request Header Handler. The manipulation leads to injection. This vulnerability is uniquely identified as CVE-2023-37255. 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-2023-2684	File Renaming on Upload Plugin up to 2.5.1 on WordPress Setting cross-sire scripting	A vulnerability classified as problematic has been found in File Renaming on Upload Plugin up to 2.5.1 on WordPress. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-sire scripting. This vulnerability is traded as CVE-2023-2684. 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-2023-2742	AI ChatBot Plugin up to 4.5.4 on WordPress Setting cross-sire scripting	A vulnerability classified as problematic was found in AI ChatBot Plugin up to 4.5.4 on WordPress. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-sire scripting. This vulnerability is known as CVE-2023-2742. 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-2023-2811	AI ChatBot Plugin up to 4.5.5 on WordPress Setting cross-sire scripting	A vulnerability was found in AI ChatBot Plugin up to 4.5.5 on WordPress and classified as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross-sire scripting. The identification of this vulnerability is CVE-2023-2811. 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-2023-3318	SourceCodester Resort Management System 1.0 page cross-sire scripting	A vulnerability was found in SourceCodester Resort Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument page leads to cross-sire scripting. This vulnerability is known as CVE-2023-3318. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-2399	QuBot Plugin up to 1.1.5 on WordPress Chat cross-sire scripting	A vulnerability has been found in QuBot Plugin up to 1.1.5 on WordPress and classified as problematic. This vulnerability affects unknown code of the component Chat Handler. The manipulation leads to cross-sire scripting. This vulnerability was named CVE-2023-2399. 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-2023-2812	Ultimate Dashboard Plugin up to 3.7.5 on WordPress Setting cross-sire scripting	A vulnerability which was classified as problematic was found in Ultimate Dashboard Plugin up to 3.7.5 on WordPress. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-2812. 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-2023-2779	Social Share, Social Login and Social Comments Plugin cross-sire scripting	A vulnerability which was classified as problematic has been found in Social Share Social Login and Social Comments Plugin on WordPress. Affected by this issue is some unknown functionality. The manipulation leads to cross-sire scripting. This vulnerability is handled as CVE-2023-2779. 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-2023-2600	Custom Base Terms Plugin up to 1.0.2 on WordPress Setting cross-sire scripting	A vulnerability was found in Custom Base Terms Plugin up to 1.0.2 on WordPress. It has been classified as problematic. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-2600. 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-2023-2654	Conditional Menus Plugin up to 1.2.0 on WordPress Attribute cross-sire scripting	A vulnerability was found in Conditional Menus Plugin up to 1.2.0 on WordPress. It has been rated as problematic. This issue affects some unknown processing of the component Attribute Handler. The manipulation leads to cross-sire scripting. The identification of this vulnerability is CVE-2023-2654. 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-2020-20725	taogogo taoCMS 2.5 beta5.1 admin.php name cross-sire scripting	A vulnerability was found in taogogo taoCMS 2.5 beta5.1 and classified as problematic. This issue affects some unknown processing of the file admin.php. The manipulation of the argument name leads to cross-sire scripting. The identification of this vulnerability is CVE-2020-20725. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2020-21485	Alluxio 1.8.1 Browse Board path cross-sire scripting (Issue 10552)	A vulnerability which was classified as problematic has been found in Alluxio 1.8.1. Affected by this issue is some unknown functionality of the component Browse Board. The manipulation of the argument path leads to cross-sire scripting. This vulnerability is handled as CVE-2020-21485. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2020-20070	wkeyuan DWSurvey 1.0 qu-multi-fill-blank!answers.action thequltemId cross-sire scripting (Issue 48)	A vulnerability was found in wkeyuan DWSurvey 1.0. It has been classified as problematic. Affected is an unknown function of the file qu-multi-fill-blank!answers.action. The manipulation of the argument thequltemId leads to cross-sire scripting. This vulnerability is traded as CVE-2020-20070. 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-2020-21268	EasySoft ZenTao PMS 11.6.4 lastComment cross-sire scripting (Issue 40)	A vulnerability classified as problematic has been found in EasySoft ZenTao PMS 11.6.4. Affected is an unknown function. The manipulation of the argument lastComment leads to cross-sire scripting. This vulnerability is traded as CVE-2020-21268. 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-2020-20697	khodakhah NodCMS 3.0 address cross-sire scripting (Issue 41)	A vulnerability classified as problematic has been found in khodakhah NodCMS 3.0. This affects an unknown part. The manipulation of the argument address leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2020-20697. 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-2020-21058	Typora 0.9.79 mermaid Syntax cross-sire scripting (Issue 2959)	A vulnerability was found in Typora 0.9.79. It has been declared as problematic. This vulnerability affects unknown code of the component mermaid Syntax Handler. The manipulation leads to cross-sire scripting. This vulnerability was named CVE-2020-21058. 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-2020-21246	YiiCMS 1.0 news cross-sire scripting	A vulnerability has been found in YiiCMS 1.0 and classified as problematic. Affected by this vulnerability is the function news. The manipulation leads to cross-sire scripting. This vulnerability is known as CVE-2020-21246. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-33495	Craft CMS up to 4.4.9 cross-sire scripting	A vulnerability which was classified as problematic has been found in Craft CMS up to 4.4.9. This issue affects some unknown processing. The manipulation leads to basic cross-sire scripting. The identification of this vulnerability is CVE-2023-33495. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-35155	XWiki Platform Email target cross-sire scripting	A vulnerability was found in XWiki Platform and classified as problematic. This issue affects some unknown processing of the component Email Handler. The manipulation of the argument target leads to cross-sire scripting. The identification of this vulnerability is CVE-2023-35155. 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-2023-35153	XWiki Platform ClassEditSheet Page name cross-sire scripting	A vulnerability was found in XWiki Platform. It has been classified as problematic. Affected is an unknown function of the component ClassEditSheet Page. The manipulation of the argument name leads to cross-sire scripting. This vulnerability is traded as CVE-2023-35153. 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-2023-34464	XWiki Platform Wiki Document cross-sire scripting	A vulnerability was found in XWiki Platform. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Wiki Document Handler. The manipulation leads to cross-sire scripting. This vulnerability is known as CVE-2023-34464. 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-2023-36093	EyouCMS 1.6.3 Basic Information Tab cross-sire scripting (Issue 44)	A vulnerability was found in EyouCMS 1.6.3. It has been classified as problematic. Affected is an unknown function of the component Basic Information Tab. The manipulation leads to cross-sire scripting. This vulnerability is traded as CVE-2023-36093. 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-2023-29707	GBCOM LAC WEB Control Center 1.3.x cross-sire scripting	A vulnerability was found in GBCOM LAC WEB Control Center 1.3.x. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-sire scripting. This vulnerability is traded as CVE-2023-29707. 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-2019-25152	Abandoned Cart Lite for WooCommerce Plugin on WordPress Admin Dashboard cross-sire scripting (ID 2033212)	A vulnerability was found in Abandoned Cart Lite for WooCommerce Plugin and Abandoned Cart Pro for WooCommerce Plugin on WordPress and classified as problematic. Affected by this issue is some unknown functionality of the component Admin Dashboard. The manipulation leads to cross-sire scripting. This vulnerability is handled as CVE-2019-25152. 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-34796	dmarcts-report-viewer 1.1 org_name/domain cross-sire scripting	A vulnerability which was classified as problematic has been found in dmarcts-report-viewer 1.1. This issue affects some unknown processing. The manipulation of the argument org_name/domain leads to cross-sire scripting. The identification of this vulnerability is CVE-2023-34796. The attack may be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-2796	EventON Plugin up to 2.1 on WordPress Event authorization	A vulnerability classified as critical was found in EventON Plugin up to 2.1 on WordPress. Affected by this vulnerability is an unknown functionality of the component Event Handler. The manipulation leads to missing authorization. This vulnerability is known as CVE-2023-2796. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-3381	SourceCodester Online School Fees System 1.0 GET Parameter /paysystem/datatable.php doj cross-sire scripting	A vulnerability classified as problematic was found in SourceCodester Online School Fees System 1.0. Affected by this vulnerability is an unknown functionality of the file /paysystem/datatable.php of the component GET Parameter Handler. The manipulation of the argument doj leads to cross-sire scripting. This vulnerability is known as CVE-2023-3381. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-3382	SourceCodester Game Result Matrix System 1.0 GET Parameter save-delegates.php del_name cross-sire scripting	A vulnerability which was classified as problematic has been found in SourceCodester Game Result Matrix System 1.0. Affected by this issue is some unknown functionality of the file /dipam/save-delegates.php of the component GET Parameter Handler. The manipulation of the argument del_name leads to cross-sire scripting. This vulnerability is handled as CVE-2023-3382. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-36289	Webkul QloApps 1.6.0 email_create/back cross-sire scripting	A vulnerability has been found in Webkul QloApps 1.6.0 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument email_create/back leads to cross-sire scripting. This vulnerability was named CVE-2023-36289. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-36288	Webkul QloApps 1.6.0 configure cross-sire scripting	A vulnerability which was classified as problematic was found in Webkul QloApps 1.6.0. This affects an unknown part. The manipulation of the argument configure leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-36288. 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-2023-36346	POS Codekop 2.0 print.php nm_member cross-sire scripting	A vulnerability classified as problematic has been found in POS Codekop 2.0. This affects an unknown part of the file print.php. The manipulation of the argument nm_member leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-36346. 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-2023-36287	Webkul QloApps 1.6.0 controller cross-sire scripting	A vulnerability was found in Webkul QloApps 1.6.0. It has been classified as problematic. This affects an unknown part. The manipulation of the argument controller leads to cross-sire scripting. This vulnerability is uniquely identified as CVE-2023-36287. 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-2023-1724	Faveo Helpdesk Enterprise 6.0.1 Permissions cross-sire scripting	A vulnerability classified as problematic was found in Faveo Helpdesk Enterprise 6.0.1. Affected by this vulnerability is an unknown functionality of the component Permissions Handler. The manipulation leads to cross-sire scripting. This vulnerability is known as CVE-2023-1724. The attack can be launched remotely. There is no exploit available.	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-2023-3276	Dromara HuTool up to 5.8.19 XML Parsing Module XmlUtil.java readBySax xml external entity reference	"A vulnerability which was classified as problematic has been found in Dromara HuTool up to 5.8.19. Affected by this issue is the function readBySax of the file XmlUtil.java of the component XML Parsing Module. The manipulation leads to xml external entity reference. This vulnerability is handled as CVE-2023-3276. The attack needs to be done within the local network. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way."	Protected by core rules	Detected by scanner as XML external entity attack.

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.

Gartner Peer Insights Customers' Choice 2023™

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™

CONTACT US - +91 265 6133021 | +1 866 537 8234

EMAIL - sales@indusface.com