INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

May 2023

The total zero-day vulnerabilities count for May month : 314

Command Injection	CSRF	Local File Inclusion	Malicious File Upload	SQL Injection	Cross-site Scripting	XML External Entity
36	15	20	12	83	146	2

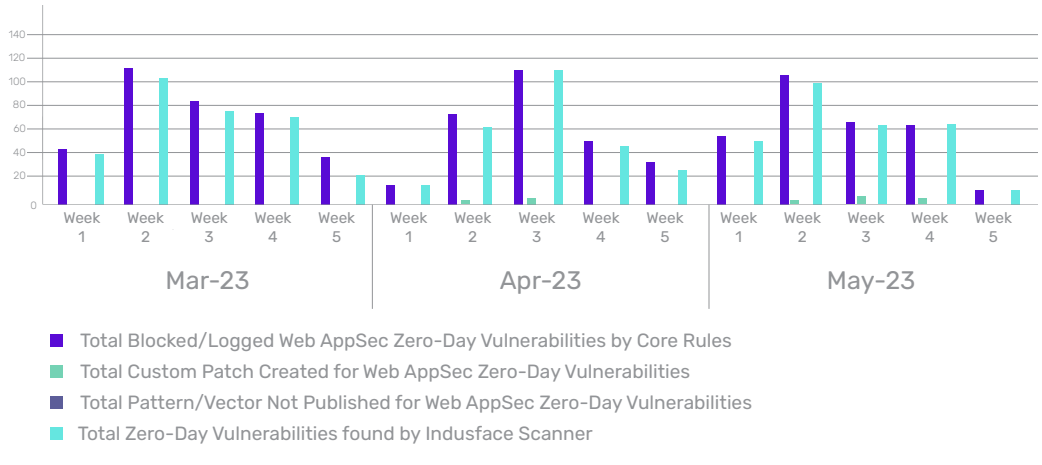
Zero-day vulnerabilities protected through core rules	300
Zero-day vulnerabilities protected through custom rules	14
Zero-day vulnerabilities for which protection can not be done	0
Zero-day vulnerabilities found by Indusface WAS	287

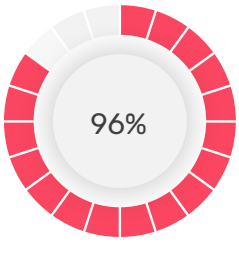
- To enable custom rules, please contact support@indusface.com
- Since the attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.

Vulnerability Trend:

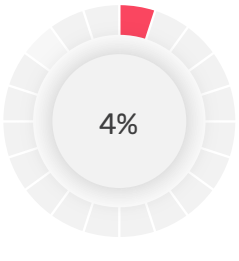
The weekly trend displays the total number of vulnerabilities discovered to the type of protection provided for the last quarter.

Weekly Vulnerability Trend

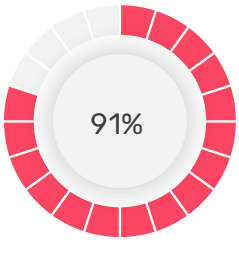




of the zero-day vulnerabilities were protected by the **core rules** in the last month.

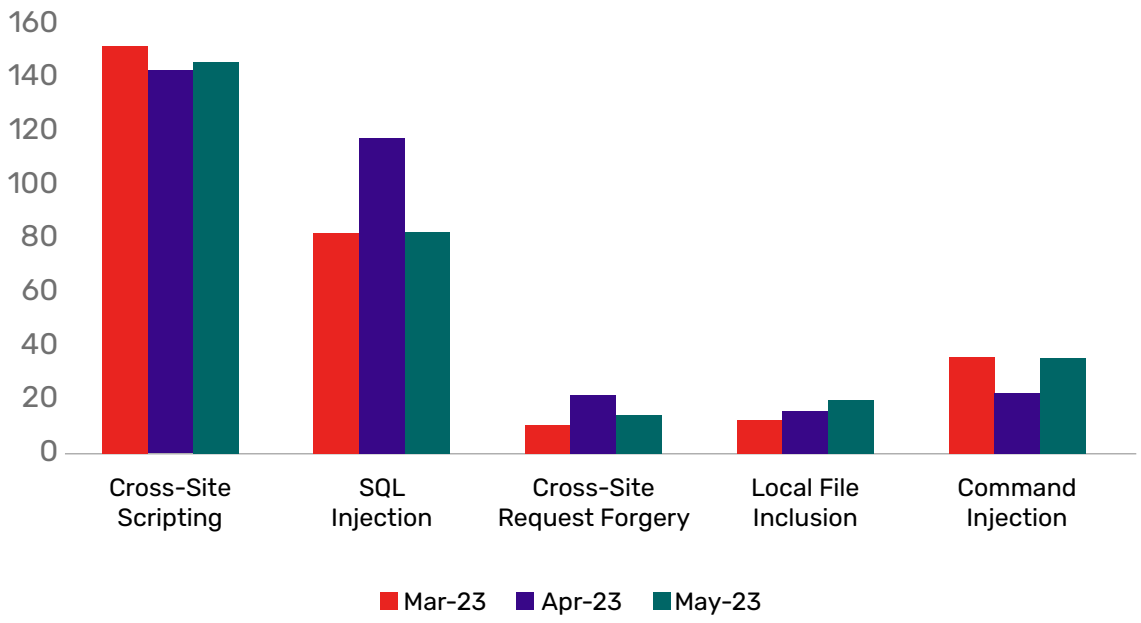


of the zero-day vulnerabilities were protected by the **custom rules** in the last month.



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-2023-29778	GL.iNet MT3000 4.1.0 Release 2 logread os command injection	A vulnerability was found in GL.iNet MT3000 4.1.0 Release 2. It has been declared as critical. Affected by this vulnerability is an unknown functionality in the library /usr/lib/oui-httpd/rpc/logread. The manipulation leads to os command injection. This vulnerability is known as CVE-2023-29778. 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 vulnerabilities
CVE-2023-2479	Appium Desktop prior 1.22.3-4 os command injection	A vulnerability which was classified as very critical has been found in Appium Desktop. This issue affects some unknown processing. The manipulation leads to os command injection. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. The identification of this vulnerability is CVE-2023-2479. 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 vulnerabilities
CVE-2023-2522	Chengdu VEC40G 3.0 Network Detection send_order.cgi COUNT os command injection	A vulnerability was found in Chengdu VEC40G 3.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /send_order.cgiparameteraccess_detect of the component Network Detection. The manipulation of the argument COUNT with the input 3 netstat -an leads to os command injection. This vulnerability is known as CVE-2023-2522. The attack can 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 Command Injection vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-30135	Tenda AC18 15.03.05.19(6318_)_cn setUsbUnload deviceName command injection	A vulnerability was found in Tenda AC18 15.03.05.19_cn. It has been classified as critical. Affected is the function setUsbUnload. The manipulation of the argument deviceName leads to command injection. This vulnerability is traded as CVE-2023-30135. 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 vulnerabilities
CVE-2023-2564	sbs20 scanservjs prior 2.27.0 os command injection	A vulnerability was found in sbs20 scanservjs and classified as critical. This issue affects some unknown processing. The manipulation leads to os command injection. The identification of this vulnerability is CVE-2023-2564. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by custom rules	Detected by scanner as Command Injection vulnerabilities
CVE-2023-2573	Advantech EKI-1524/EKI-1522/EKI-1521 up to 1.21 NTP Server os command injection	A vulnerability was found in Advantech EKI-1524 EKI-1522 and EKI-1521 up to 1.21. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component NTP Server. The manipulation leads to os command injection. This vulnerability is known as CVE-2023-2573. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection vulnerabilities
CVE-2023-2574	Advantech EKI-1524/EKI-1522/EKI-1521 up to 1.21 device name os command injection	A vulnerability was found in Advantech EKI-1524 EKI-1522 and EKI-1521 up to 1.21. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation of the argument device name leads to os command injection. This vulnerability is handled as CVE-2023-2574. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection vulnerabilities
CVE-2021-27280	mblog 3.5.0 Theme os command injection (Issue 44)	A vulnerability was found in mblog 3.5.0. It has been classified as critical. This affects an unknown part of the component Theme Handler. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2021-27280. 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 vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-31472	GL.iNet Device prior 3.216 command injection	A vulnerability was found in GL.iNet Device and classified as critical. This issue affects some unknown processing. The manipulation leads to command injection. The identification of this vulnerability is CVE-2023-31472. 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 Command Injection vulnerabilities
CVE-2023-31473	GL.iNet Device prior 3.216 command injection	A vulnerability was found in GL.iNet Device. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to command injection. This vulnerability is known as CVE-2023-31473. Access to the local network is required for this attack to succeed. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection vulnerabilities
CVE-2023-2649	Tenda AC23 16.03.07.45_cn Service Port 7329 / bin/ate v2 command injection	A vulnerability was found in Tenda AC23 16.03.07.45_cn. It has been declared as critical. This vulnerability affects unknown code of the file / bin/ate of the component Service Port 7329. The manipulation of the argument v2 leads to command injection. This vulnerability was named CVE-2023-2649. The attack can be initiated remotely. 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 applying a restrictive firewalling.	Protected by core rules	Detected by scanner as Command Injection vulnerabilities
CVE-2023-2647	Weaver E-Office 9.5 File Upload utility_all.php command injection	A vulnerability was found in Weaver E-Office 9.5 and classified as critical. Affected by this issue is some unknown functionality of the file /webroot/inc/utility_all.php of the component File Upload Handler. The manipulation leads to command injection. This vulnerability is handled as CVE-2023-2647. 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 Command Injection vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-31985	Edimax Wireless Router N300 BR-6428NS_v4 /bin/webs formAccept command injection	A vulnerability was found in Edimax Wireless Router N300 BR-6428NS_v4. It has been declared as critical. Affected by this vulnerability is the function formAccept of the file /bin/webs. The manipulation leads to command injection. This vulnerability is known as CVE-2023-31985. 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 vulnerabilities
CVE-2023-31529	Motorola CX2L Router 1.0.1 system_time_timezone command injection	A vulnerability was found in Motorola CX2L Router 1.0.1. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument system_time_timezone leads to command injection. The identification of this vulnerability is CVE-2023-31529. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection vulnerabilities
CVE-2023-31528	Motorola CX2L Router 1.0.1 staticroute_list command injection	A vulnerability was found in Motorola CX2L Router 1.0.1. It has been declared as critical. This vulnerability affects unknown code. The manipulation of the argument staticroute_list leads to command injection. This vulnerability was named CVE-2023-31528. 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 vulnerabilities
CVE-2023-31530	Motorola CX2L Router 1.0.1 smartqos_priority_devices command injection	A vulnerability was found in Motorola CX2L Router 1.0.1. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation of the argument smartqos_priority_devices leads to command injection. This vulnerability is handled as CVE-2023-31530. 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 vulnerabilities
CVE-2020-13378	http://Loadbalancer.org Enterprise VA MAX up to 8.3.8 os command injection	A vulnerability classified as critical has been found in http://Loadbalancer.org Enterprise VA MAX up to 8.3.8. Affected is an unknown function. The manipulation leads to os command injection. This vulnerability is traded as CVE-2020-13378. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-31531	Motorola CX2L Router 1.0.1 tomography_ping_number command injection	A vulnerability was found in Motorola CX2L Router 1.0.1. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation of the argument tomography_ping_number leads to command injection. This vulnerability is handled as CVE-2023-31531. 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 vulnerabilities
CVE-2022-47879	Jedox 2020.2.5 / be/rpc.php code injection	A vulnerability which was classified as critical has been found in Jedox 2020.2.5. This issue affects some unknown processing of the file /be/rpc.php. The manipulation leads to code injection. The identification of this vulnerability is CVE-2022-47879. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection vulnerabilities
CVE-2023-32073	World Wide Broadcast Network AVideo up to 12.4 CloneSite Plugin cloneClient.json.php command injection (GHSA-2mhh-27v7-3vcx)	A vulnerability was found in World Wide Broadcast Network AVideo up to 12.4. It has been classified as critical. This affects an unknown part of the file plugin/CloneSite/cloneClient.json.php of the component CloneSite Plugin. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2023-32073. 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 Command Injection vulnerabilities
CVE-2023-31983	Edimax Wireless Router N300 BR-6428NS_v4 /bin/webs mp command injection	A vulnerability was found in Edimax Wireless Router N300 BR-6428NS_v4. It has been declared as critical. This vulnerability affects the function mp of the file /bin/webs. The manipulation leads to command injection. This vulnerability was named CVE-2023-31983. 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 vulnerabilities
CVE-2023-31986	Edimax Wireless Router N300 BR-6428NS_v4 /bin/webs setWAN command injection	A vulnerability classified as critical was found in Edimax Wireless Router N300 BR-6428NS_v4. This vulnerability affects the function setWAN of the file /bin/webs. The manipulation leads to command injection. This vulnerability was named CVE-2023-31986. 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 vulnerabilities
CVE-2023-31856	TOTOLINK CP300+ 5.2cu.7594_B20200910 HTTP Packet NTPSyncWithHostof hostTime command injection	A vulnerability which was classified as critical has been found in TOTOLINK CP300+ 5.2cu.7594_B20200910. This issue affects the function NTPSyncWithHostof of the component HTTP Packet Handler. The manipulation of the argument hostTime leads to command injection. The identification of this vulnerability is CVE-2023-31856. 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 vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-31701	TP-LINK TL-WPA4530 KIT V2 (EU)_161115/ (EU)_170406 _httpRpmPlcDevice-Remove command injection	A vulnerability classified as critical has been found in TP-LINK TL-WPA4530 KIT V2 _170406/_161115. Affected is the function _httpRpmPlcDeviceR-emove. The manipula-tion leads to command injection. This vulnerability is traded as CVE-2023-31701. The attack can only be initiated within the local network. There is no exploit avail-able.	Protected by core rules	Detected by scanner as Com-mand Injection vulnerabilities
CVE-2023-31700	TP-LINK TL-WPA4530 KIT V2 (EU)_161115/ (EU)_170406 _httpRpmPlcDe-viceAdd command injection	A vulnerability was found in TP-LINK TL-WPA4530 KIT V2 _170406/_161115. It has been rated as critical. This issue affects the function _httpRpmPlc-DeviceAdd. The manipu-lation leads to command injection. The identification of this vulnerability is CVE-2023-31700. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Com-mand Injection vulnerabilities
CVE-2023-24805	cups-filters Back-end Error beh.c os command injection (GHSA-gpxc-v2m8-fr3x)	A vulnerability was found in cups-filters. It has been classified as critical. This affects an unknown part of the file beh.c of the component Backend Error Handler. The manipula-tion leads to os command injection. This vulnerability is uniquely identified as CVE-2023-24805. It is possible to initiate the attack re-motely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Com-mand Injection vulnerabilities
CVE-2023-31756	TP-Link Archer VR1600V Adminis-trative Web Portal X_ TP_IfName command injection	A vulnerability which was classified as critical was found in TP-Link Archer VR1600V. This affects an unknown part of the com-ponent Administrative Web Portal. The manipulation of the argument X_TP_If-Name leads to command injection. This vulnerability is uniquely identified as CVE-2023-31756. It is possible to initiate the attack re-motely. There is no exploit available.	Protected by core rules	Detected by scanner as Com-mand Injection vulnerabilities
CVE-2023-31742	Linksys WRT54GL 4.30.18.006 POST Request Start_EPI wl_ant/wl_rate/WL_ atten_ctl/ttcp_num/ ttcp_size command injection	A vulnerability was found in Linksys WRT54GL 4.30.18.006. It has been rated as critical. This issue affects the function Start_EPI of the com-ponent POST Request Handler. The manipulation of the argument wl_ant/ wl_rate/WL_atten_ctl/ ttcp_num/ttcp_size leads to command injection. The identification of this vulnerability is CVE-2023-31742. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as Com-mand Injection vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-33294	KaiOS 3.0 Web Server tctweb_server os command injection	A vulnerability has been found in KaiOS 3.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /system/bin/tctweb_server of the component Web Server. The manipulation leads to os command injection. This vulnerability is known as CVE-2023-33294. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection vulnerabilities
CVE-2023-31740	Linksys E2000 1.0.06 POST Request apply.cgi WL_atten_bb/WL_atten_radio/WL_atten_ctl command injection	A vulnerability was found in Linksys E2000 1.0.06. It has been rated as critical. This issue affects some unknown processing of the file apply.cgi of the component POST Request Handler. The manipulation of the argument WL_atten_bb/WL_atten_radio/WL_atten_ctl leads to command injection. The identification of this vulnerability is CVE-2023-31740. 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 vulnerabilities
CVE-2023-31741	Linksys E2000 1.0.06 POST Request Start_EPI command injection	A vulnerability classified as critical has been found in Linksys E2000 1.0.06. Affected is the function Start_EPI of the component POST Request Handler. The manipulation of the argument wl_ssid/wl_ant/wl_rate/WL_atten_ctl/ttcp_num/ttcp_size leads to command injection. This vulnerability is traded as CVE-2023-31741. 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 vulnerabilities
CVE-2023-33617	Parks Fiberlink 210 2.1.14_X000 /boaform/admin/formPing target_addr os command injection	A vulnerability which was classified as critical has been found in Parks Fiberlink 210 2.1.14_X000. This issue affects some unknown processing of the file /boaform/admin/formPing. The manipulation of the argument target_addr leads to os command injection. The identification of this vulnerability is CVE-2023-33617. 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 vulnerabilities
CVE-2023-33248	Amazon Alexa 8960323972 on Echo Dot Voice command injection	A vulnerability which was classified as critical was found in Amazon Alexa 8960323972 on Echo Dot. Affected is an unknown function of the component Voice Handler. The manipulation leads to command injection. This vulnerability is traded as CVE-2023-33248. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-26129	bwm-ng bwm-ng.js check command injection (SNYK-JS-BWMNG-3175876)	A vulnerability has been found in bwm-ng and classified as critical. Affected by this vulnerability is the function check of the file bwm-ng.js. The manipulation leads to command injection. This vulnerability is known as CVE-2023-26129. It is possible to launch the attack on the local host. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection vulnerabilities
CVE-2023-26128	keep-module-latest installModule command injection	A vulnerability which was classified as critical was found in keep-module-latest. Affected is the function installModule. The manipulation leads to command injection. This vulnerability is traded as CVE-2023-26128. Attacking locally is a requirement. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection vulnerabilities
CVE-2022-24630	AudioCodes Device Manager Express up to 7.8.20002.47752 POST Request BrowseFiles.php ssh_command command injection	A vulnerability has been found in AudioCodes Device Manager Express up to 7.8.20002.47752 and classified as critical. Affected by this vulnerability is an unknown functionality of the file BrowseFiles.php of the component POST Request Handler. The manipulation of the argument ssh_command leads to command injection. This vulnerability is known as CVE-2022-24630. 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 vulnerabilities

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-2474	Rebuild 3.2 cross-site request forgery (I6W4M2)	A vulnerability has been found in Rebuild 3.2 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-2474. The attack can be initiated remotely. Furthermore there is an exploit available. It is recommended to change the configuration settings.	Protected by core rules	NA
CVE-2023-2552	unilogies bumsys up to 2.1.0 cross-site request forgery	A vulnerability was found in unilogies bumsys up to 2.1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-2552. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2020-18131	Bluethrust Clan Scripts 4 Request console.php cross-site request forgery (Issue 27)	A vulnerability was found in Bluethrust Clan Scripts 4. It has been declared as problematic. This vulnerability affects unknown code of the file /members/console.phpcID5 of the component Request Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2020-18131. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-0522	Enable Disable Auto Login when Register Plugin up to 1.1.0 on WordPress Setting cross-site request forgery	A vulnerability has been found in Enable Disable Auto Login when Register Plugin up to 1.1.0 on WordPress and classified as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-0522. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2020-22334	beescms 4 /admin/admin_admin.php cross-site request forgery	A vulnerability was found in beescms 4. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/admin_admin.php. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2020-22334. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2020-36065	sunkaifei FlyCms 1.0 system/admin/admin_save cross-site request forgery	A vulnerability has been found in sunkaifei FlyCms 1.0 and classified as problematic. This vulnerability affects unknown code of the file system/admin/admin_save. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2020-36065. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-1660	AI ChatBot Plugin up to 4.4.8 on WordPress Setting cross-site request forgery	A vulnerability which was classified as problematic was found in AI ChatBot Plugin up to 4.4.8 on WordPress. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-1660. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2020-23363	Verytops Verydows cross-site request forgery (Issue 17)	A vulnerability has been found in Verytops Verydows and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2020-23363. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2021-36444	imcat 5.4 Add Administrator cross-site request forgery	A vulnerability was found in imcat 5.4. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Add Administrator Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2021-36444. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0762	Clock In Portal- Staff & Attendance Management Plugin cross-site request forgery	A vulnerability has been found in Clock In Portal- Staff & Attendance Management Plugin up to 2.1 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-0762. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-0520	RapidExpCart Plugin up to 1.0 on WordPress rapidexpcart Endpoint url cross-site request forgery	A vulnerability which was classified as problematic was found in RapidExpCart Plugin up to 1.0 on WordPress. This affects an unknown part of the component rapidexpcart Endpoint. The manipulation of the argument url leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-0520. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-2179	WooCommerce Order Status Change Notifier Plugin up to 1.1.0 on WordPress AJAX Action cross-site request forgery	A vulnerability which was classified as problematic has been found in WooCommerce Order Status Change Notifier Plugin up to 1.1.0 on WordPress. This issue affects some unknown processing of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-2179. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-0763	Clock In Portal- Staff & Attendance Management Plugin cross-site request forgery	A vulnerability was found in Clock In Portal- Staff & Attendance Management Plugin up to 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-2023-0763. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-31708	EyouCMS 1.6.2 HTML File cross-site request forgery (Issue 41)	A vulnerability classified as problematic has been found in EyouCMS 1.6.2. This affects an unknown part of the component HTML File Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-31708. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-33359	Piwigo 13.6.0 Add Tags cross-site request forgery (Issue 1908)	A vulnerability has been found in Piwigo 13.6.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Add Tags Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-33359. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-48483	3CX Phone System prior 18 Hotfix 1 Build 18.0.3.461 Drive Letter /Electron/download path traversal	A vulnerability classified as critical was found in 3CX Phone System. Affected by this vulnerability is an unknown functionality of the file /Electron/download of the component Drive Letter Handler. The manipulation leads to path traversal. This vulnerability is known as CVE-2022-48483. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2022-48482	3CX Phone System on Windows /Electron/download path traversal	A vulnerability classified as critical has been found in 3CX Phone System on Windows. Affected is an unknown function of the file /Electron/download. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-48482. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2022-47875	Jedox 2020.2.5 / be/erpc.php path traversal	A vulnerability was found in Jedox 2020.2.5. It has been declared as critical. This vulnerability affects unknown code of the file / be/erpc.php. The manipulation leads to path traversal. This vulnerability was named CVE-2022-47875. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2017-20184	Carlo Gavazzi Powersoft up to 2.1.1.1 path traversal (Exploit 42705 / EDB-42705)	A vulnerability which was classified as critical has been found in Carlo Gavazzi Powersoft up to 2.1.1.1. This issue affects some unknown processing. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2017-20184. 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-2023-25289	virtualreception Digital Receptie 6.1.7601.1.0.65792 Web Server path traversal (Exploit 51142 / EDB-51142)	A vulnerability was found in virtualreception Digital Receptie 6.1.7601.1.0.65792. It has been classified as problematic. Affected is an unknown function of the component Web Server. The manipulation leads to path traversal. This vulnerability is traded as CVE-2023-25289. Access to the local network is required for this attack. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-27562	n8n 0.218.0 on Node.js path traversal	A vulnerability has been found in n8n 0.218.0 on Node.js and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to path traversal. This vulnerability is known as CVE-2023-27562. 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-2023-26126	m.static 2.2.0 requestFile path traversal	A vulnerability was found in m.static 2.2.0. It has been declared as critical. Affected by this vulnerability is the function requestFile. The manipulation leads to path traversal. This vulnerability is known as CVE-2023-26126. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-31477	GL.iNet Device prior 3.216 File Sharing / tmp path traversal	A vulnerability which was classified as critical has been found in GL.iNet Device. Affected by this issue is some unknown functionality of the file / tmp of the component File Sharing. The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-31477. The attack needs to be approached within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2020-13377	http://Loadbalancer.org Enterprise VA MAX up to 8.3.8 Web-Services Interface path traversal	A vulnerability which was classified as critical has been found in http://Loadbalancer.org Enterprise VA MAX up to 8.3.8. This issue affects some unknown processing of the component Web-Services Interface. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2020-13377. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-32309	PyMdown Extensions up to 9.x path traversal (GHSA-jh85-wwv9-24hv)	A vulnerability was found in PyMdown Extensions up to 9.x. It has been classified as critical. Affected is an unknown function. The manipulation leads to path traversal. This vulnerability is traded as CVE-2023-32309. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-2765	Weaver OA up to 9.5 downfile.php url absolute path traversal	A vulnerability has been found in Weaver OA up to 9.5 and classified as problematic. This vulnerability affects unknown code of the file /E-mobile/App/System/File/downfile.php. The manipulation of the argument url leads to absolute path traversal. This vulnerability was named CVE-2023-2765. The attack can 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 Local File Inclusion attack.
CVE-2023-2780	mlflow up to 2.3.0 path traversal	A vulnerability was found in mlflow up to 2.3.0. It has been classified as critical. Affected is an unknown function. The manipulation leads to path traversal: &039;\..\filename&039;. This vulnerability is traded as CVE-2023-2780. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-32767	Symcon IP-Symcon prior 6.3 Web Interface path traversal (SYSS-2023-014)	A vulnerability which was classified as critical was found in Symcon IP-Symcon. This affects an unknown part of the component Web Interface Handler. The manipulation leads to path traversal: &039;../filedir&039;. This vulnerability is uniquely identified as CVE-2023-32767. 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-2023-32322	Ombi up to 4.38.1 SystemControllers.cs path traversal (GHSA-28j3-84m7-gpjp)	A vulnerability which was classified as problematic was found in Ombi up to 4.38.1. This affects an unknown part of the file SystemControllers.cs. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-32322. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-27067	Sitecore Experience Platform up to 10.2 download.aspx path traversal	A vulnerability which was classified as critical was found in Sitecore Experience Platform up to 10.2. This affects an unknown part of the file download.aspx. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-27067. 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-2023-27066	Sitecore Experience Platform up to 10.2 Urlhandle path traversal	A vulnerability classified as critical was found in Sitecore Experience Platform up to 10.2. Affected by this vulnerability is the function Urlhandle. The manipulation leads to path traversal. This vulnerability is known as CVE-2023-27066. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-31861	ZLMediaKit 4.0 path traversal	A vulnerability which was classified as critical has been found in ZLMediaKit 4.0. Affected by this issue is some unknown functionality. The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-31861. 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-2023-29380	Warpinator up to 1.5.x top_dir_basenames path traversal	A vulnerability classified as critical has been found in Warpinator up to 1.5.x. This affects the function top_dir_basenames. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-29380. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2022-24632	AudioCodes Device Manager Express up to 7.8.20002.47752 File Download BrowseFiles.php view path traversal	A vulnerability was found in AudioCodes Device Manager Express up to 7.8.20002.47752 and classified as problematic. Affected by this issue is some unknown functionality of the file BrowseFiles.php of the component File Download Handler. The manipulation of the argument view leads to path traversal. This vulnerability is handled as CVE-2022-24632. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2022-24629	AudioCodes Device Manager Express up to 7.8.20002.47752 File Upload BrowseFiles.php dir path traversal	A vulnerability was found in AudioCodes Device Manager Express up to 7.8.20002.47752. It has been rated as critical. Affected by this issue is some unknown functionality of the file BrowseFiles.php of the component File Upload Handler. The manipulation of the argument dir leads to path traversal. This vulnerability is handled as CVE-2022-24629. The attack may 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-2021-34076	PHPOK 5.7.140 ZIP File unrestricted upload	A vulnerability which was classified as critical has been found in PHPOK 5.7.140. This issue affects some unknown processing of the component ZIP File Handler. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2021-34076. The attack may be initiated remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2023-29657	eXtplorer 2.1.15 File Manager unrestricted upload	A vulnerability classified as critical has been found in eXtplorer 2.1.15. This affects an unknown part of the component File Manager. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-29657. The attack needs to be initiated within the local network. There is no exploit available.	Protected by custom rules	NA
CVE-2023-30247	SourceCodester Storage Unit Rental Management System 1.0 update_settings unrestricted upload	A vulnerability classified as critical has been found in SourceCodester Storage Unit Rental Management System 1.0. This affects an unknown part. The manipulation of the argument update_settings leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-30247. It is possible to initiate the attack remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2022-4774	Bit Form Plugin up to 1.8 on WordPress unrestricted upload	A vulnerability classified as critical was found in Bit Form Plugin up to 1.8 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2022-4774. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by custom rules	NA
CVE-2023-31857	Sourcecodester Online Computer and Laptop Store 1.0 Users.php unrestricted upload	A vulnerability was found in Sourcecodester Online Computer and Laptop Store 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /classes/Users.phpfsave. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-31857. The attack may be launched remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2023-31576	Serendipity 2.4-beta1 HTML File unrestricted upload	A vulnerability was found in Serendipity 2.4-beta1. It has been rated as problematic. Affected by this issue is some unknown functionality of the component HTML File Handler. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-31576. The attack needs to be done 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-2023-2738	Tongda OA 11.10 GatewayController.php actionGetdata unrestricted upload	A vulnerability classified as critical has been found in Tongda OA 11.10. This affects the function actionGetdata of the file GatewayController.php. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-2738. It is possible to initiate the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by custom rules	NA
CVE-2023-31903	GuppY CMS 6.00.10 unrestricted upload	A vulnerability was found in GuppY CMS 6.00.10. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-31903. The attack may be launched remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2023-30333	PerfreeBlog 3.1.2 File ThemeController.java unrestricted upload	A vulnerability classified as problematic was found in PerfreeBlog 3.1.2. This vulnerability affects unknown code of the file /admin/ThemeController.java of the component File Handler. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-30333. Access to the local network is required for this attack. There is no exploit available.	Protected by custom rules	NA
CVE-2023-31689	vedees wcms 0.3.2 Request /wcms/wex/html.php finish/textAreaCode unrestricted upload (Issue 15)	A vulnerability was found in vedees wcms 0.3.2. It has been classified as critical. This affects an unknown part of the file /wcms/wex/html.php of the component Request Handler. The manipulation of the argument finish/textAreaCode leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-31689. The attack needs to be done within the local network. There is no exploit available.	Protected by custom rules	NA
CVE-2023-2888	PHPOK 6.4.100 admin.php unrestricted upload (I72D24)	A vulnerability which was classified as problematic was found in PHPOK 6.4.100. This affects an unknown part of the file /admin.phpcupload&fzip&_noCache0.1683794968. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-2888. It is possible to initiate the attack remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2023-29721	SofaWiki up to 3.8.9 unrestricted upload (Issue 27)	A vulnerability was found in SofaWiki up to 3.8.9. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-29721. The attack needs to be initiated within the local network. There is no exploit available.	Protected by custom rules	NA

XML External Entity Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-2806	Weaver e-cology up to 9.0 API RequestInfoByXml xml external entity reference	A vulnerability classified as problematic was found in Weaver e-cology up to 9.0. Affected by this vulnerability is the function RequestInfoByXml of the component API. The manipulation leads to xml external entity reference. This vulnerability is known as CVE-2023-2806. The attack needs to be approached within the local network. There is no 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.
CVE-2022-41221	OpenText Archive Center Administration up to 16.2.3/21.2 xml external entity reference	A vulnerability was found in OpenText Archive Center Administration up to 16.2.3/21.2. It has been classified as problematic. This affects an unknown part. The manipulation leads to xml external entity reference. This vulnerability is uniquely identified as CVE-2022-41221. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules.	Detected by scanner as XML External Entity attack.

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-2451	SourceCodester Online DJ Management System 1.0 GET Parameter view_details.php id sql injection	A vulnerability was found in SourceCodester Online DJ Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/bookings/view_details.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2023-2451. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-31433	evasys up to 8.1/8.x Logbuch welche sql injection	A vulnerability was found in evasys up to 8.1/8.x. It has been rated as critical. Affected by this issue is some unknown functionality of the component Logbuch. The manipulation of the argument welche leads to sql injection. This vulnerability is handled as CVE-2023-31433. 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 SQL Injection attack.
CVE-2023-27568	inSpryker Commerce OS 0.9 customer/order orderSearchForm[searchText] sql injection	A vulnerability was found in inSpryker Commerce OS 0.9 and classified as critical. Affected by this issue is some unknown functionality of the file customer/order. The manipulation of the argument orderSearchForm[searchText] leads to sql injection. This vulnerability is handled as CVE-2023-27568. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-30077	Judging Management System 1.0 review_result.php mainevent_id sql injection	A vulnerability which was classified as critical was found in Judging Management System 1.0. This affects an unknown part of the file /php-jms/review_result.php. The manipulation of the argument mainevent_id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-30077. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-29842	ChurchCRM 4.5.4 POST Parameter / EditEventTypes.php EN_tyid sql injection	A vulnerability was found in ChurchCRM 4.5.4. It has been classified as critical. Affected is an unknown function of the file /EditEventTypes.php of the component POST Parameter Handler. The manipulation of the argument EN_tyid leads to sql injection. This vulnerability is traded as CVE-2023-29842. 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-2023-30203	Judging Management System 1.0 result_sheet.php event_id sql injection	A vulnerability which was classified as critical was found in Judging Management System 1.0. Affected is an unknown function of the file /php-jms/result_sheet.php. The manipulation of the argument event_id leads to sql injection. This vulnerability is traded as CVE-2023-30203. 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-2023-1408	Video List Manager Plugin up to 1.7 on WordPress sql injection	A vulnerability was found in Video List Manager Plugin up to 1.7 on WordPress. It has been classified as critical. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-1408. 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-2023-31038	Apache Log4cxx prior 1.1.0 ODBC Appender sql injection	A vulnerability classified as critical has been found in Apache Log4cxx. Affected is an unknown function of the component ODBC Appender. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-31038. The attack needs to be approached within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-30018	Judging Management System 1.0 review_se_result.php mainevent_id sql injection	A vulnerability classified as critical was found in Judging Management System 1.0. This vulnerability affects unknown code of the file /php-jms/review_se_result.php. The manipulation of the argument mainevent_id leads to sql injection. This vulnerability was named CVE-2023-30018. 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-2023-30092	SourceCodester Online Pizza Ordering System 1.0 QTY sql injection	A vulnerability has been found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. This vulnerability affects unknown code. The manipulation of the argument QTY leads to sql injection. This vulnerability was named CVE-2023-30092. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-4118	Bitcoin AltCoin Payment Gateway for WooCommerce & Multivendor Store Plugin sql injection	A vulnerability has been found in Bitcoin AltCoin Payment Gateway for WooCommerce & Multivendor Store Plugin up to 1.7.1 on WordPress and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-4118. The attack can be launched 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-2023-0768	Avirato Hotels Online Booking Engine Plugin up to 5.0.5 on WordPress Shortcode Attribute sql injection	A vulnerability was found in Avirato Hotels Online Booking Engine Plugin up to 5.0.5 on WordPress and classified as critical. Affected by this issue is some unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-0768. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2021-28999	CMS Made Simple up to 2.2.15 function. admin_articlestab. php m1_sortby sql injection	A vulnerability which was classified as critical was found in CMS Made Simple up to 2.2.15. Affected is an unknown function of the file modules/News/function.admin_articlestab. php. The manipulation of the argument m1_sortby leads to sql injection. This vulnerability is traded as CVE-2021-28999. 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-2020-23966	Victor CMS 1.0 GET /post.php post sql injection (Issue 15)	A vulnerability classified as critical was found in Victor CMS 1.0. This vulnerability affects unknown code of the file /post.php of the component GET Handler. The manipulation of the argument post leads to sql injection. This vulnerability was named CVE-2020-23966. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2114	NEX-Forms Plugin up to 8.3 on WordPress table sql injection	A vulnerability has been found in NEX-Forms Plugin up to 8.3 on WordPress and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation of the argument table leads to sql injection. This vulnerability is known as CVE-2023-2114. 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-2023-2596	SourceCodester Online Reviewer System 1.0 GET Parameter user-update.php user_id sql injection	A vulnerability was found in SourceCodester Online Reviewer System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /reviewer/system/system/admins/manage/users/user-update.php of the component GET Parameter Handler. The manipulation of the argument user_id leads to sql injection. This vulnerability is handled as CVE-2023-2596. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2595	SourceCodester Billing Management System 1.0 POST Parameter ajax_service. php drop_services sql injection	A vulnerability has been found in SourceCodester Billing Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file ajax_service.php of the component POST Parameter Handler. The manipulation of the argument drop_services leads to sql injection. This vulnerability is known as CVE-2023-2595. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2619	SourceCodester Online Tours & Travels Management System 1.0 disapprove_delete.php exec id sql injection	A vulnerability which was classified as critical was found in SourceCodester Online Tours & Travels Management System 1.0. This affects the function exec of the file disapprove_delete.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2619. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-29863	Medical Systems Medisys Weblab Products 19.4.03 WSDL File tem:statement sql injection	A vulnerability classified as critical has been found in Medical Systems Medisys Weblab Products 19.4.03. This affects an unknown part of the component WSDL File Handler. The manipulation of the argument tem:statement leads to sql injection. This vulnerability is uniquely identified as CVE-2023-29863. 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-2023-2659	SourceCodester Online Computer and Laptop Store 1.0 view_product.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Online Computer and Laptop Store 1.0. This affects an unknown part of the file view_product.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2659. 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-2023-2653	SourceCodester Lost and Found Information System 1.0 items/index.php cid sql injection	A vulnerability classified as critical was found in SourceCodester Lost and Found Information System 1.0. Affected by this vulnerability is an unknown functionality of the file items/index.php. The manipulation of the argument cid leads to sql injection. This vulnerability is known as CVE-2023-2653. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2661	SourceCodester Online Computer and Laptop Store 1.0 / classes/Master.php id sql injection	A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. This issue affects some unknown processing of the file /classes/Master.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2023-2661. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-30194	posstaticfooter up to 1.0.0 on Prestashop getPosCurrentHook sql injection	A vulnerability has been found in posstaticfooter up to 1.0.0 on Prestashop and classified as critical. This vulnerability affects the function posstaticfooter::getPosCurrentHook. The manipulation leads to sql injection. This vulnerability was named CVE-2023-30194. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2660	SourceCodester Online Computer and Laptop Store 1.0 view_categories.php c sql injection	A vulnerability has been found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. This vulnerability affects unknown code of the file view_categories.php. The manipulation of the argument c leads to sql injection. This vulnerability was named CVE-2023-2660. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2643	SourceCodester File Tracker Manager System 1.0 POST Parameter update_password.php new_password sql injection	A vulnerability classified as critical was found in SourceCodester File Tracker Manager System 1.0. This vulnerability affects unknown code of the file register/update_password.php of the component POST Parameter Handler. The manipulation of the argument new_password leads to sql injection. This vulnerability was named CVE-2023-2643. The attack can be initiated 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-2023-2641	SourceCodester Online Internship Management System 1.0 POST Parameter admin/login.php email sql injection	A vulnerability was found in SourceCodester Online Internship Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file admin/login.php of the component POST Parameter Handler. The manipulation of the argument email leads to sql injection. This vulnerability is handled as CVE-2023-2641. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2656	SourceCodester AC Repair and Services System 1.0 Master.php id sql injection	A vulnerability classified as critical has been found in SourceCodester AC Repair and Services System 1.0. Affected is an unknown function of the file /classes/Master.phpfdelete_service. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-2656. 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-2023-2658	SourceCodester Online Computer and Laptop Store 1.0 products.php c sql injection	A vulnerability which was classified as critical has been found in SourceCodester Online Computer and Laptop Store 1.0. Affected by this issue is some unknown functionality of the file products.php. The manipulation of the argument c leads to sql injection. This vulnerability is handled as CVE-2023-2658. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2642	SourceCodester Online Exam System 1.0 GET Parameter updateCourse.php id sql injection	A vulnerability classified as critical has been found in SourceCodester Online Exam System 1.0. This affects an unknown part of the file adminpanel/admin/facebox_modal/updateCourse.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2642. 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-2023-2652	SourceCodester Lost and Found Information System 1.0 Master.php sql injection	A vulnerability classified as critical has been found in SourceCodester Lost and Found Information System 1.0. Affected is an unknown function of the file /classes/Master.phpfdelete_item. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-2652. 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-2023-30192	possearchproducts 1.7 on Prestashop PosSearch::find sql injection	A vulnerability classified as critical was found in possearchproducts 1.7 on Prestashop. This vulnerability affects the function PosSearch::find. The manipulation leads to sql injection. This vulnerability was named CVE-2023-30192. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-29809	Maximilian Vogt companymaps 8.0 sql injection (Exploit 172146 / EDB-51422)	A vulnerability classified as critical was found in Maximilian Vogt companymaps 8.0. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-29809. 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-2023-30246	Judging Management System 1.0 contestant_id sql injection	A vulnerability was found in Judging Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality. The manipulation of the argument contestant_id leads to sql injection. This vulnerability is handled as CVE-2023-30246. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1934	SDG PnPSCADA 2.x PostgreSQL hitlogcsv.jsp sql injection (icsa-23-131-12)	A vulnerability classified as critical was found in SDG PnPSCADA 2.x. Affected by this vulnerability is an unknown functionality of the file hitlogcsv.jsp of the component PostgreSQL. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-1934. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2677	SourceCodester Covid-19 Contact Tracing System 1.0 manage.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Covid-19 Contact Tracing System 1.0. This affects an unknown part of the file admin/establishment/manage.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2677. 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-2023-2669	SourceCodester Lost and Found Information System 1.0 GET Parameter id sql injection	A vulnerability was found in SourceCodester Lost and Found Information System 1.0. It has been classified as critical. This affects an unknown part of the file admin/pagecategories/view_category of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2669. 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-2023-2668	SourceCodester Lost and Found Information System 1.0 GET Parameter manager_category id sql injection	A vulnerability was found in SourceCodester Lost and Found Information System 1.0 and classified as critical. Affected by this issue is the function manager_category of the file admin/pagecategories/manage_category of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-2668. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2672	SourceCodester Lost and Found Information System 1.0 GET Parameter items/view.php id sql injection	A vulnerability classified as critical has been found in SourceCodester Lost and Found Information System 1.0. Affected is an unknown function of the file items/view.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-2672. 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-2023-2693	SourceCodester Online Exam System 1.0 POST Parameter /mahasiswa/data columns[1][data] sql injection	A vulnerability was found in SourceCodester Online Exam System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /mahasiswa/data of the component POST Parameter Handler. The manipulation of the argument columns[1][data] leads to sql injection. This vulnerability is handled as CVE-2023-2693. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2695	SourceCodester Online Exam System 1.0 POST Parameter /kelas/data columns[1][data] sql injection	A vulnerability was found in SourceCodester Online Exam System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /kelas/data of the component POST Parameter Handler. The manipulation of the argument columns[1][data] leads to sql injection. This vulnerability was named CVE-2023-2695. The attack can be initiated 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-2023-2694	SourceCodester Online Exam System 1.0 POST Parameter /dosen/data columns[1][data] sql injection	A vulnerability was found in SourceCodester Online Exam System 1.0. It has been classified as critical. This affects an unknown part of the file /dosen/data of the component POST Parameter Handler. The manipulation of the argument columns[1][data] leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2694. 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-2023-2699	SourceCodester Lost and Found Information System 1.0 GET Parameter id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Lost and Found Information System 1.0. Affected by this issue is some unknown functionality of the file admin/pageitems/view_item of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-2699. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2696	SourceCodester Online Exam System 1.0 POST Parameter /matkul/data columns[1][data] sql injection	A vulnerability was found in SourceCodester Online Exam System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /matkul/data of the component POST Parameter Handler. The manipulation of the argument columns[1][data] leads to sql injection. The identification of this vulnerability is CVE-2023-2696. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2689	SourceCodester Billing Management System 1.0 GET Parameter editproduct.php id sql injection	A vulnerability classified as critical was found in SourceCodester Billing Management System 1.0. This vulnerability affects unknown code of the file editproduct.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-2689. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2690	SourceCodester Personnel Property Equipment System 1.0 GET Parameter returned_reuse_form.php client_id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Personnel Property Equipment System 1.0. This issue affects some unknown processing of the file admin/returned_reuse_form.php of the component GET Parameter Handler. The manipulation of the argument client_id leads to sql injection. The identification of this vulnerability is CVE-2023-2690. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2698	SourceCodester Lost and Found Information System 1.0 GET Parameter id sql injection	A vulnerability classified as critical was found in SourceCodester Lost and Found Information System 1.0. Affected by this vulnerability is an unknown functionality of the file admin/pageitems/manage_item of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-2698. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2697	SourceCodester Online Exam System 1.0 POST Parameter /jurusan/data columns[1][data] sql injection	A vulnerability classified as critical has been found in SourceCodester Online Exam System 1.0. Affected is an unknown function of the file /jurusan/data of the component POST Parameter Handler. The manipulation of the argument columns[1][data] leads to sql injection. This vulnerability is traded as CVE-2023-2697. 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-2023-30245	SourceCodester Judging Management System 1.0 edit_criteria.php the crit_id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Judging Management System 1.0. Affected by this issue is the function the of the file edit_criteria.php. The manipulation of the argument crit_id leads to sql injection. This vulnerability is handled as CVE-2023-30245. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-31843	SourceCodester Faculty Evaluation System 1.0 view_faculty.php id sql injection	A vulnerability was found in SourceCodester Faculty Evaluation System 1.0 and classified as critical. This issue affects some unknown processing of the file /eval/admin/view_faculty.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2023-31843. 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-2023-31842	SourceCodester Faculty Evaluation System 1.0 index.php id sql injection	A vulnerability has been found in SourceCodester Faculty Evaluation System 1.0 and classified as critical. This vulnerability affects unknown code of the file /eval/index.phppage-edit_faculty. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-31842. 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-2023-31844	SourceCodester Faculty Evaluation System 1.0 manage_subject.php id sql injection	A vulnerability was found in SourceCodester Faculty Evaluation System 1.0. It has been classified as critical. Affected is an unknown function of the file /eval/admin/manage_subject.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-31844. 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-2023-31845	Sourcecodester Faculty Evaluation System 1.0 manage_class.php id sql injection	A vulnerability was found in Sourcecodester Faculty Evaluation System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /eval/admin/manage_class.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-31845. 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-2023-0600	WP Visitor Statistics Plugin up to 6.8 on WordPress sql injection	A vulnerability was found in WP Visitor Statistics Plugin up to 6.8 on WordPress. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-0600. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-31519	Pharmacy Management System 1.0 Parameter login_core.php email sql injection	A vulnerability was found in Pharmacy Management System 1.0. It has been classified as critical. This affects an unknown part of the file login_core.php of the component Parameter Handler. The manipulation of the argument email leads to sql injection. This vulnerability is uniquely identified as CVE-2023-31519. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-2770	SourceCodester Online Exam System 1.0 /kelasdosen/data columns[1][data] sql injection	A vulnerability classified as critical was found in SourceCodester Online Exam System 1.0. This vulnerability affects unknown code of the file /kelasdosen/data. The manipulation of the argument columns[1][data] leads to sql injection. This vulnerability was named CVE-2023-2770. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2772	SourceCodester Budget and Expense Tracker System 1.0 GET Parameter manage_budget.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Budget and Expense Tracker System 1.0. Affected is an unknown function of the file /admin/budget/manage_budget.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-2772. 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-2023-2775	code-projects Bus Dispatch and Information System 1.0 adminHome.php reach_city sql injection	A vulnerability was found in code-projects Bus Dispatch and Information System 1.0. It has been classified as critical. This affects an unknown part of the file adminHome.php. The manipulation of the argument reach_city leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2775. 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-2023-2771	SourceCodester Online Exam System 1.0 /jurusanmatkul/data columns[1][data] sql injection	A vulnerability which was classified as critical has been found in SourceCodester Online Exam System 1.0. This issue affects some unknown processing of the file /jurusanmatkul/data. The manipulation of the argument columns[1][data] leads to sql injection. The identification of this vulnerability is CVE-2023-2771. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2769	SourceCodester Service Provider Management System 1.0 Master.php id sql injection	A vulnerability classified as critical has been found in SourceCodester Service Provider Management System 1.0. This affects an unknown part of the file /classes/Master.phpfdelete_service. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2769. 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-2023-27742	Dolibarr ERP CRM 1 /api/login sql injection	A vulnerability which was classified as critical has been found in Dolibarr ERP CRM 1. This issue affects some unknown processing of the file /api/login. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-27742. 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-2023-30189	posstaticblocks up to 1.0.0 on PrestaShop getPosCurrentHook sql injection	A vulnerability was found in posstaticblocks up to 1.0.0 on PrestaShop and classified as critical. This issue affects the function posstaticblocks::getPosCurrentHook. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-30189. 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-2023-2774	code-projects Bus Dispatch and Information System 1.0 view_branch.php branchid sql injection	A vulnerability was found in code-projects Bus Dispatch and Information System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file view_branch.php. The manipulation of the argument branchid leads to sql injection. This vulnerability is handled as CVE-2023-2774. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-31702	MicroWorld eScan Management Console 14.0.1400.2281 View User Profile sql injection	A vulnerability was found in MicroWorld eScan Management Console 14.0.1400.2281. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component View User Profile. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-31702. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2756	pimcore customer-data-framework up to 3.3.9 sql injection	A vulnerability which was classified as critical was found in pimcore customer-data-framework up to 3.3.9. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-2756. 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 SQL Injection attack.
CVE-2023-30191	cdesigner up to 3.1.8 on PrestaShop initContent sql injection	A vulnerability was found in cdesigner up to 3.1.8 on PrestaShop and classified as critical. This issue affects the function CdesignerTraitementModuleFrontController::initContent. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-30191. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-27233	Piwigo 13.5.0 user_list_backend.php order[0][dir] sql injection	A vulnerability was found in Piwigo 13.5.0. It has been declared as critical. This vulnerability affects unknown code of the file user_list_backend.php. The manipulation of the argument order[0][dir] leads to sql injection. This vulnerability was named CVE-2023-27233. 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-2023-29985	SourceCodester Student Study Center Desk Management System 1.0 index.php#date_from sql injection	A vulnerability which was classified as critical has been found in SourceCodester Student Study Center Desk Management System 1.0. This issue affects some unknown processing of the file admin\reports\index.php-date_from. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-29985. 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-2023-31707	SEMCMS 1.5 Ant_ Rponse.php sql injection	A vulnerability was found in SEMCMS 1.5. It has been classified as critical. Affected is an unknown function of the file Ant_ Rponse.php. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-31707. 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-2023-2815	SourceCodester Online Jewelry Store 1.0 POST Parameter supplier.php suppid sql injection	A vulnerability classified as critical was found in SourceCodester Online Jewelry Store 1.0. Affected by this vulnerability is an unknown functionality of the file supplier.php of the component POST Parameter Handler. The manipulation of the argument suppid leads to sql injection. This vulnerability is known as CVE-2023-2815. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2823	SourceCodester Class Scheduling System 1.0 GET Parameter / admin/edit_subject. php id sql injection	A vulnerability was found in SourceCodester Class Scheduling System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/edit_subject. php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-2823. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-2832	unilogies bumsys up to 2.1.x sql injection	A vulnerability classified as critical has been found in unilogies bumsys up to 2.1.x. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2832. 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-2023-33362	Piwigo 13.6.0 profile sql injection (Issue 1911)	A vulnerability classified as critical was found in Piwigo 13.6.0. This vulnerability affects the function profile. The manipulation leads to sql injection. This vulnerability was named CVE-2023-33362. 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-2023-33338	Old Age Home Management 1.0 username sql injection	A vulnerability classified as critical has been found in Old Age Home Management 1.0. This affects an unknown part. The manipulation of the argument username leads to sql injection. This vulnerability is uniquely identified as CVE-2023-33338. 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-2023-33361	Piwigo 13.6.0 /admin/ permalinks.php sql injection (Issue 1910)	A vulnerability was found in Piwigo 13.6.0 and classified as critical. This issue affects some unknown processing of the file / admin/permalinks.php. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-33361. 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-2023-2865	SourceCodester Theme Park Ticketing System 1.0 GET Parameter print_ticket.php id sql injection	A vulnerability was found in SourceCodester Theme Park Ticketing System 1.0. It has been classified as critical. This affects an unknown part of the file print_ticket.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2865. 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-2023-31752	SourceCodester Employee and Visitor Gate Pass Logging System 1.0 Login.php sql injection	A vulnerability which was classified as critical has been found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. This issue affects some unknown processing of the file /employee_gatepass/classes/Login.php. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-31752. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-30025	Tredence Analytics iDEAL Wealth and Funds 1.0 /Framewrk/Home.jsp v sql injection	A vulnerability has been found in Tredence Analytics iDEAL Wealth and Funds 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /Framewrk/Home.jsp. The manipulation of the argument v leads to sql injection. This vulnerability is known as CVE-2022-30025. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-33439	Sourcecodester Faculty Evaluation System 1.0 /admin/manage_task.php id sql injection	A vulnerability has been found in Sourcecodester Faculty Evaluation System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/manage_task.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-33439. 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-2023-2955	SourceCodester Students Online Internship Timesheet System 1.0 GET Parameter rendered_report.php sid sql injection	A vulnerability which was classified as critical was found in SourceCodester Students Online Internship Timesheet System 1.0. Affected is an unknown function of the file rendered_report.php of the component GET Parameter Handler. The manipulation of the argument sid leads to sql injection. This vulnerability is traded as CVE-2023-2955. 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-2023-2962	SourceCodester Faculty Evaluation System 1.0 index.php id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Faculty Evaluation System 1.0. Affected by this issue is some unknown functionality of the file index.phppage-edit_user. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-2962. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-0329	Elementor Website Builder Plugin up to 3.12.1 on WordPress Tools Module sql injection	A vulnerability was found in Elementor Website Builder Plugin up to 3.12.1 on WordPress. It has been classified as critical. Affected is an unknown function of the component Tools Module. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-0329. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-24628	AudioCodes Device Manager Express up to 7.8.20002.47752 IPPhoneFirmwa-reEdit.php id sql injection	A vulnerability which was classified as critical was found in AudioCodes Device Manager Express up to 7.8.20002.47752. Affected is an unknown function of the file IP-PhoneFirmwareEdit.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-24628. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-24627	AudioCodes Device Manager Express up to 7.8.20002.47752 process_login.php sql injection	A vulnerability which was classified as critical has been found in AudioCodes Device Manager Express up to 7.8.20002.47752. This issue affects some unknown processing of the file process_login.php. The manipulation of the argument p leads to sql injection. The identification of this vulnerability is CVE-2022-24627. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Cross-Site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-4782	ClickFunnels Plugin up to 3.1.1 on Word-Press Shortcode cross site scripting	A vulnerability was found in ClickFunnels Plugin up to 3.1.1 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Shortcode Handler. The manipula-tion leads to cross site scripting. This vulnerability is known as CVE-2022-4782. The attack can be launched re-motely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1465	WP EasyPay Plugin up to 4.0.4 on WordPress cross site scripting	A vulnerability which was classified as problematic was found in WP Ea-syPay Plugin up to 4.0.4 on WordPress. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-1465. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-47877	Jedox 2020.2.5 Logs Page cross site scripting	A vulnerability classified as problematic has been found in Jedox 2020.2.5. This affects an unknown part of the component Logs Page. The manipu-lation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2022-47877. It is possible to initiate the attack re-motely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-29643	PerfreeBlog 3.1.2 Post cross site scripting (Issue 14)	A vulnerability was found in PerfreeBlog 3.1.2. It has been rated as problematic. Affected by this issue is some unknown functional-ity of the component Post Handler. The manipula-tion leads to cross site scripting. This vulnerability is handled as CVE-2023-29643. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1525	Site Reviews Plugin up to 6.7.0 on Word-Press Setting cross site scripting	A vulnerability classified as problematic has been found in Site Reviews Plugin up to 6.7.0 on WordPress. This affects an unknown part of the com-ponent Setting Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-1525. It is possible to initiate the attack re-motely. 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-2023-29636	zhenfeng13 My-Blog Blog Management Page title cross site scripting (Issue 131)	A vulnerability has been found in zhenfeng13 My-Blog and classified as problematic. This vulnerability affects unknown code of the component Blog Management Page. The manipulation of the argument title leads to cross site scripting. This vulnerability was named CVE-2023-29636. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1546	MyCryptoCheckout Plugin prior 2.124 on WordPress URL cross site scripting	A vulnerability was found in MyCryptoCheckout Plugin on WordPress. It has been classified as problematic. This affects an unknown part of the component URL Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-1546. 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-2023-29641	Pandao http://editor.md up to 1.5.0 Markdown cross site scripting (Issue 985)	A vulnerability was found in Pandao http://editor.md up to 1.5.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Markdown Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-29641. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-29638	WinterChenS my-site Blog Article cross site scripting (Issue 74)	A vulnerability classified as problematic has been found in WinterChenS my-site. Affected is an unknown function of the component Blog Article Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-29638. It is possible to launch the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-31434	evasys prior 8.2 Build 2286/9.0 Build 2401 nutzer_titel/nutzer_vn/nutzer_nn/langID/ONLINEID cross site scripting	A vulnerability was found in evasys and classified as problematic. This issue affects some unknown processing. The manipulation of the argument nutzer_titel/nutzer_vn/nutzer_nn/langID/ONLINEID leads to cross site scripting. The identification of this vulnerability is CVE-2023-31434. 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-2023-29639	zhenfeng13 My-Blog Blog Article Page cross site scripting (Issue 131)	A vulnerability was found in zhenfeng13 My-Blog and classified as problematic. This issue affects some unknown processing of the component Blog Article Page. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-29639. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1554	Quick Paypal Payments Plugin prior 5.7.26.4 on WordPress Setting cross site scripting	A vulnerability has been found in Quick Paypal Payments Plugin on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-1554. 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-2023-0891	StagTools Plugin up to 2.3.6 on WordPress Shortcode Attribute cross site scripting (fee-9768-462)	A vulnerability which was classified as problematic was found in StagTools Plugin up to 2.3.6 on WordPress. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-0891. 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-2023-29637	Qbian61 forum-java Article Editor Page cross site scripting (Issue 13)	A vulnerability was found in Qbian61 forum-java. It has been classified as problematic. Affected is an unknown function of the component Article Editor Page. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-29637. 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-2023-2477	Funadmin up to 3.2.3 Cx.php tagLoad file cross site scripting (I6W2YL)	A vulnerability was found in Funadmin up to 3.2.3. It has been declared as problematic. Affected by this vulnerability is the function tagLoad of the file Cx.php. The manipulation of the argument file leads to cross site scripting. This vulnerability is known as CVE-2023-2477. 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-2023-2476	Dromara J2eeFAST up to 2.6.0 Announcement 系统工具/公告管理 cross site scripting (I6W380)	A vulnerability was found in Dromara J2eeFAST up to 2.6.0. It has been classified as problematic. Affected is an unknown function of the component Announcement Handler. The manipulation of the argument 系统工具/公告管理 leads to cross site scripting. This vulnerability is traded as CVE-2023-2476. 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-2023-29772	ASUS RT-AC51U up to 3.0.0.4.380.8591 Network Request cross site scripting	A vulnerability classified as problematic was found in ASUS RT-AC51U up to 3.0.0.4.380.8591. This vulnerability affects unknown code of the component Network Request Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-29772. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1090	SMTP Mailing Queue Plugin up to 2.0.0 on WordPress Setting cross site scripting	A vulnerability was found in SMTP Mailing Queue Plugin up to 2.0.0 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-1090. 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-2023-1021	amr ical Events Lists Plugin up to 6.6 on WordPress Setting cross site scripting	A vulnerability was found in amr ical Events Lists Plugin up to 6.6 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-1021. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-30860	World Wide Broadcast Network AVideo prior 12.4 Schedule Meet topic cross site scripting	A vulnerability was found in World Wide Broadcast Network AVideo. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Schedule. The manipulation of the argument Meet topic with the input "><img srcx onerroralert> leads to cross site scripting. This vulnerability is handled as CVE-2023-30860. 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-2023-2475	Dromara J2eeFAST up to 2.6.0 System Message 主题 cross site scripting (I6W390)	A vulnerability was found in Dromara J2eeFAST up to 2.6.0 and classified as problematic. This issue affects some unknown processing of the component System Message Handler. The manipulation of the argument 主题 leads to cross site scripting. The identification of this vulnerability is CVE-2023-2475. The attack may be initiated 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-2023-29839	Hotel Druid 3.0.4 Document Surname/Name/Nickname cross site scripting	A vulnerability was found in Hotel Druid 3.0.4. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Document Handler. The manipulation of the argument Surname/Name/Nickname leads to cross site scripting. This vulnerability is handled as CVE-2023-29839. The attack may be launched remotely. There is no exploit available	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-24744	Rediker AdminPlus 6.1.91.00 onload cross site scripting	A vulnerability classified as problematic has been found in Rediker AdminPlus 6.1.91.00. Affected is the function onload. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-24744. 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-2023-27075	Microbin 1.2.0 microbin/src/pasta.rs cross site scripting (Issue 142)	A vulnerability classified as problematic was found in Microbin 1.2.0. Affected by this vulnerability is an unknown functionality of the file microbin/src/pasta.rs. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-27075. The attack can be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-30184	Typecho 1.2.0 comment url cross site scripting (Issue 1546)	A vulnerability was found in Typecho 1.2.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /index.php/archives/1/comment. The manipulation of the argument url leads to cross site scripting. This vulnerability is handled as CVE-2023-30184. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1839	PPOM for WooCommerce Plugin up to 32.0.5 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic was found in PPOM for WooCommerce Plugin up to 32.0.5 on WordPress. This affects an unknown part of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-1839. 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-2023-30094	TotalJS Flow 10 Settings Module platform name cross site scripting (Issue 100)	A vulnerability was found in TotalJS Flow 10. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Settings Module. The manipulation of the argument platform name leads to cross site scripting. This vulnerability is known as CVE-2023-30094. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-30096	TotalJS Messenger b6cf1c9 information cross site scripting (Issue 10)	A vulnerability classified as problematic has been found in TotalJS Messenger b6cf1c9. Affected is an unknown function. The manipulation of the argument information leads to cross site scripting. This vulnerability is traded as CVE-2023-30096. 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-2023-30097	TotalJS Messenger b6cf1c9 task cross site scripting	A vulnerability classified as problematic was found in TotalJS Messenger b6cf1c9. Affected by this vulnerability is an unknown functionality. The manipulation of the argument task leads to cross site scripting. This vulnerability is known as CVE-2023-30097. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-30095	TotalJS Messenger b6cf1c9 description cross site scripting (Issue 11)	A vulnerability was found in TotalJS Messenger b6cf1c9. It has been rated as problematic. This issue affects some unknown processing. The manipulation of the argument description leads to cross site scripting. The identification of this vulnerability is CVE-2023-30095. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-2550	thorsten phpmyfaq up to 3.1.12 cross site scripting	A vulnerability has been found in thorsten phpmyfaq up to 3.1.12 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-2550. 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-2023-2427	thorsten phpmyfaq up to 3.1.12 cross site scripting	A vulnerability which was classified as problematic was found in thorsten phpmyfaq up to 3.1.12. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-2427. 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-2023-2553	unilogies bumsys up to 2.1.x cross site scripting	A vulnerability was found in unilogies bumsys up to 2.1.x. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-2553. 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-2023-2516	nilsteampassnet teampass up to 3.0.6 cross site scripting	A vulnerability was found in nilsteampassnet teampass up to 3.0.6. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-2516. 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-2023-2565	SourceCodester Multi Language Hotel Management Software 1.0 POST Parameter ajax.php complaint_type cross site scripting	A vulnerability has been found in SourceCodester Multi Language Hotel Management Software 1.0 and classified as problematic. This vulnerability affects unknown code of the file ajax.php of the component POST Parameter Handler. The manipulation of the argument complaint_type with the input <script>alert</script> leads to cross site scripting. This vulnerability was named CVE-2023-2565. 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-2023-2566	OpenEMR up to 7.0.0 cross site scripting	A vulnerability was found in OpenEMR up to 7.0.0. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-2566. 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-2023-0537	Product Slider for WooCommerce Lite Plugin up to 1.1.7 on WordPress Shortcode Attribute cross site scripting	A vulnerability classified as problematic has been found in Product Slider for WooCommerce Lite Plugin up to 1.1.7 on WordPress. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-0537. 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-2023-0268	Mega Addons for WPBakery Page Builder Plugin up to 4.2.x on WordPress Shortcode Attribute cross site scripting	A vulnerability classified as problematic was found in Mega Addons for WPBakery Page Builder Plugin up to 4.2.x on WordPress. This vulnerability affects unknown code of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-0268. 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-2023-0267	Ultimate Carousel for WPBakery Page Builder Plugin Shortcode Attribute cross site scripting	A vulnerability classified as problematic was found in Ultimate Carousel for WPBakery Page Builder Plugin up to 2.6 on WordPress. Affected by this vulnerability is an unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-0267. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0514	Membership Database Plugin up to 1.0 on WordPress cross site scripting	A vulnerability which was classified as problematic was found in Membership Database Plugin up to 1.0 on WordPress. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-0514. 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-2023-0526	Post Shortcode Plugin up to 2.0.9 on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in Post Shortcode Plugin up to 2.0.9 on WordPress and classified as problematic. This issue affects some unknown processing of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-0526. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1905	WP Popups Plugin up to 2.1.5.0 on WordPress Shortcode Attribute cross site scripting	A vulnerability classified as problematic has been found in WP Popups Plugin up to 2.1.5.0 on WordPress. This affects an unknown part of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-1905. 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-2020-18282	nangge NoneCms 1.3.0 Feedback cross site scripting (Issue 23)	A vulnerability which was classified as problematic was found in nangge NoneCms 1.3.0. This affects an unknown part of the component Feedback Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2020-18282. 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-2023-0536	Wp-D3 Plugin up to 2.4.1 on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in Wp-D3 Plugin up to 2.4.1 on WordPress. It has been classified as problematic. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-0536. 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-2023-0280	Ultimate Carousel for Elementor Plugin up to 2.1.7 on WordPress Block Option cross site scripting	A vulnerability which was classified as problematic has been found in Ultimate Carousel for Elementor Plugin up to 2.1.7 on WordPress. Affected by this issue is some unknown functionality of the component Block Option Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-0280. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0603	Sloth Logo Customizer Plugin up to 2.0.2 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic has been found in Sloth Logo Customizer Plugin up to 2.0.2 on WordPress. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-0603. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2020-18132	sansanyun MIPCMS 3.6.0 categoryEdit category name cross site scripting	A vulnerability which was classified as problematic has been found in sansanyun MIPCMS 3.6.0. Affected by this issue is the function categoryEdit. The manipulation of the argument category name leads to cross site scripting. This vulnerability is handled as CVE-2020-18132. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0544	WP Login Box Plugin up to 2.0.2 on WordPress Setting cross site scripting	A vulnerability was found in WP Login Box Plugin up to 2.0.2 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-0544. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0948	Japanized for WooCommerce plugin up to 2.5.7 on WordPress cross site scripting	A vulnerability was found in Japanized for WooCommerce plugin up to 2.5.7 on WordPress and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-0948. 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-2023-0542	Custom Post Type List Shortcode Plugin up to 1.4.4 on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in Custom Post Type List Shortcode Plugin up to 1.4.4 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-0542. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2021-31711	Trippo Responsive-Filemanager up to 9.14.0 dialog.php sort_by cross site scripting (Issue 661)	A vulnerability which was classified as problematic has been found in Trippo ResponsiveFilemanager up to 9.14.0. Affected by this issue is some unknown functionality of the file dialog.php. The manipulation of the argument sort_by leads to cross site scripting. This vulnerability is handled as CVE-2021-31711. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-30334	AsmBB 2.9.1 MiniMag.asm/bbcode.asm cross site scripting	A vulnerability classified as problematic was found in AsmBB 2.9.1. This vulnerability affects unknown code in the library MiniMag.asm/bbcode.asm. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-30334. 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-2023-30777	Advanced Custom Fields Pro Plugin up to 6.1.5 on WordPress post_status cross site scripting	A vulnerability classified as problematic was found in Advanced Custom Fields Pro Plugin up to 6.1.5 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation of the argument post_status leads to cross site scripting. This vulnerability is known as CVE-2023-30777. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2020-18280	Phodal MD 1.0 cross site scripting (Issue 20)	A vulnerability which was classified as problematic was found in Phodal MD 1.0. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2020-18280. 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-2023-2616	pimcore up to 10.5.20 cross site scripting	A vulnerability was found in pimcore up to 10.5.20. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-2616. 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-2023-2630	pimcore up to 10.5.20 cross site scripting	A vulnerability classified as problematic was found in pimcore up to 10.5.20. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-2630. 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-2023-32070	XWiki Platform up to 14.5 cross site scripting (GHSA-6gf5-c898-7rxp)	A vulnerability which was classified as problematic has been found in XWiki Platform up to 14.5. Affected by this issue is some unknown functionality. The manipulation leads to improper neutralization of script in attributes in a web page. This vulnerability is handled as CVE-2023-32070. 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-2023-2614	pimcore up to 10.5.20 cross site scripting	A vulnerability classified as problematic has been found in pimcore up to 10.5.20. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-2614. 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-2023-30057	FICO Origination Manager Decision Module 4.8.1 cross site scripting	A vulnerability was found in FICO Origination Manager Decision Module 4.8.1. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-30057. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-2615	pimcore up to 10.5.20 cross site scripting	A vulnerability classified as problematic was found in pimcore up to 10.5.20. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-2615. 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-2023-30256	Webkil QloApps 1.5.2 AuthController.php email_create cross site scripting	A vulnerability was found in Webkil QloApps 1.5.2. It has been classified as problematic. Affected is an unknown function of the file AuthController.php. The manipulation of the argument email_create leads to cross site scripting. This vulnerability is traded as CVE-2023-30256. 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-2023-25309	Fetlife rollout-ui 0.5 URL cross site scripting	A vulnerability classified as problematic was found in Fetlife rollout-ui 0.5. This vulnerability affects unknown code of the component URL Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-25309. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-2657	SourceCodester Online Computer and Laptop Store 1.0 products.php search cross site scripting	A vulnerability classified as problematic was found in SourceCodester Online Computer and Laptop Store 1.0. Affected by this vulnerability is an unknown functionality of the file products.php. The manipulation of the argument search leads to cross site scripting. This vulnerability is known as CVE-2023-2657. 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-2023-2667	SourceCodester Lost and Found Information System 1.0 admin/ page cross site scripting	A vulnerability has been found in SourceCodester Lost and Found Information System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file admin/. The manipulation of the argument page leads to cross site scripting. This vulnerability is known as CVE-2023-2667. 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-2023-31508	PrestaShop 1.7.7.4 contactform.php message cross site scripting	A vulnerability was found in PrestaShop 1.7.7.4. It has been classified as problematic. Affected is an unknown function of the file /contactform/contactform.php. The manipulation of the argument message leads to cross site scripting. This vulnerability is traded as CVE-2023-31508. 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-2023-29983	Maximilian Vogt companymaps 8.0 token cross site scripting (Exploit 172075 / EDB-51417)	A vulnerability which was classified as problematic has been found in Maximilian Vogt companymaps 8.0. Affected by this issue is some unknown functionality. The manipulation of the argument token leads to cross site scripting. This vulnerability is handled as CVE-2023-29983. 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-2023-2678	SourceCodester File Tracker Manager System 1.0 POST Parameter save_user.php firstname cross site scripting	A vulnerability has been found in SourceCodester File Tracker Manager System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /file_manager/admin/save_user.php of the component POST Parameter Handler. The manipulation of the argument firstname leads to cross site scripting. This vulnerability was named CVE-2023-2678. The attack can be initiated 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-2023-29808	Maximilian Vogt companymaps 8.0 cross site scripting	A vulnerability was found in Maximilian Vogt companymaps 8.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-29808. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-2634	Get Your Number Plugin up to 1.1.3 on WordPress cross site scripting	A vulnerability classified as problematic has been found in Get Your Number Plugin up to 1.1.3 on WordPress. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-2634. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-48020	Vinteo VCC 2.36.4 conference cross site scripting	A vulnerability was found in Vinteo VCC 2.36.4. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument conference leads to cross site scripting. This vulnerability is handled as CVE-2022-48020. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-2691	SourceCodester Personnel Property Equipment System 1.0 POST Parameter admin/add_item.php item_name cross site scripting	A vulnerability which was classified as problematic was found in SourceCodester Personnel Property Equipment System 1.0. Affected is an unknown function of the file admin/add_item.php of the component POST Parameter Handler. The manipulation of the argument item_name leads to cross site scripting. This vulnerability is traded as CVE-2023-2691. 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-2023-2692	SourceCodester ICT Laboratory Management System 1.0 GET Parameter views/room_info.php name cross site scripting	A vulnerability has been found in SourceCodester ICT Laboratory Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file views/room_info.php of the component GET Parameter Handler. The manipulation of the argument name leads to cross site scripting. This vulnerability is known as CVE-2023-2692. 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-2023-1890	Tablesome Plugin up to 1.0.8 on WordPress URL cross site scripting	A vulnerability has been found in Tablesome Plugin up to 1.0.8 on WordPress and classified as problematic. This vulnerability affects unknown code of the component URL Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-1890. 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-2023-0152	WP Multi Store Locator Plugin up to 2.4 on WordPress cross site scripting	A vulnerability has been found in WP Multi Store Locator Plugin up to 2.4 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-0152. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1915	Thumbnail Carousel Slider Plugin up to 1.1.9 on WordPress cross site scripting	A vulnerability was found in Thumbnail Carousel Slider Plugin up to 1.1.9 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-1915. 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-2023-2009	Pretty Url plugin up to 1.5.4 on WordPress Setting cross site scripting	A vulnerability was found in Pretty Url plugin up to 1.5.4 on WordPress and classified as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-2009. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0490	fx TOC Plugin up to 1.1.0 on WordPress Shortcode Attribute cross site scripting	A vulnerability which was classified as problematic was found in fx TOC Plugin up to 1.1.0 on WordPress. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-0490. 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-2023-1596	tagDiv Composer Plugin up to 3.x on WordPress cross site scripting	A vulnerability classified as problematic has been found in tagDiv Composer Plugin up to 3.x on WordPress. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-1596. 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-2023-23682	Snap Creek EZP Maintenance Mode Plugin up to 1.0.1 on WordPress cross site scripting	A vulnerability which was classified as problematic has been found in Snap Creek EZP Maintenance Mode Plugin up to 1.0.1 on WordPress. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-23682. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0892	BizLibrary Plugin up to 1.1 on WordPress Setting cross site scripting	A vulnerability was found in BizLibrary Plugin up to 1.1 on WordPress. It has been classified as problematic. This affects an unknown part of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-0892. 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-2023-1835	Ninja Forms Contact Form Plugin up to 3.6.21 on WordPress cross site scripting	A vulnerability classified as problematic was found in Ninja Forms Contact Form Plugin up to 3.6.21 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-1835. 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-2023-1019	Help Desk WP Plugin up to 1.2.0 on WordPress cross site scripting	A vulnerability was found in Help Desk WP Plugin up to 1.2.0 on WordPress. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-1019. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-2740	SourceCodester Guest Management System 1.0 GET Parameter dateTest.php name cross site scripting	A vulnerability which was classified as problematic has been found in SourceCodester Guest Management System 1.0. Affected by this issue is some unknown functionality of the file dateTest.php of the component GET Parameter Handler. The manipulation of the argument name leads to cross site scripting. This vulnerability is handled as CVE-2023-2740. 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-2023-29439	FooPlugins Foo-Gallery Plugin up to 2.2.35 on WordPress cross site scripting	A vulnerability has been found in FooPlugins Foo-Gallery Plugin up to 2.2.35 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-29439. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-2752	thorsten phpmyfaq up to 3.1.x cross site scripting	A vulnerability classified as problematic has been found in thorsten phpmyfaq up to 3.1.x. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-2752. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2021-27131	Moodle 3.10.1 Additional HTML Section Header/Footer cross site scripting	A vulnerability was found in Moodle 3.10.1. It has been classified as problematic. This affects an unknown part of the component Additional HTML Section. The manipulation of the argument Header/Footer leads to cross site scripting. This vulnerability is uniquely identified as CVE-2021-27131. 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-2023-31703	MicroWorld eScan Management Console 14.0.1400.2281 Edit User Form from cross site scripting	A vulnerability which was classified as problematic has been found in MicroWorld eScan Management Console 14.0.1400.2281. This issue affects some unknown processing of the component Edit User Form. The manipulation of the argument from leads to cross site scripting. The identification of this vulnerability is CVE-2023-31703. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-2768	Sucms 1.0 admin_ads.php intro cross site scripting	A vulnerability was found in Sucms 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file admin_ads.phpactionadd. The manipulation of the argument intro leads to cross site scripting. This vulnerability is handled as CVE-2023-2768. 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-2023-31698	Bludit 3.14.1 Site Logo cross site scripting (Issue 1509)	A vulnerability was found in Bludit 3.14.1 and classified as problematic. Affected by this issue is some unknown functionality of the component Site Logo Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-31698. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-45144	Algoo Tracim up to 4.4.1 HTML File Upload cross site scripting	A vulnerability has been found in Algoo Tracim up to 4.4.1 and classified as problematic. This vulnerability affects unknown code of the component HTML File Upload Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2022-45144. 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-2023-31699	ChurchCRM 4.5.4 Image File cross site scripting (Issue 6471)	A vulnerability was found in ChurchCRM 4.5.4. It has been classified as problematic. This affects an unknown part of the component Image File Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-31699. 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-2023-31544	Alkacon OpenCMS 11.0.0.0 Upload Image Module Title cross site scripting (Issue 652)	A vulnerability was found in Alkacon OpenCMS 11.0.0.0. It has been rated as problematic. This issue affects some unknown processing of the component Upload Image Module. The manipulation of the argument Title leads to cross site scripting. The identification of this vulnerability is CVE-2023-31544. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-2753	thorsten phpmyfaq up to 3.1.x cross site scripting	A vulnerability classified as problematic was found in thorsten phpmyfaq up to 3.1.x. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-2753. 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-2023-30124	Lavalite 9.0.0 cross site scripting (Issue 389)	A vulnerability classified as problematic has been found in Lavalite 9.0.0. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-30124. 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-2023-31862	jizhicms 2.4.6 Article cross site scripting (Issue 86)	A vulnerability classified as problematic has been found in jizhicms 2.4.6. This affects an unknown part of the component Article Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-31862. 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-2023-29720	SofaWiki up to 3.8.9 index.php cross site scripting (Issue 26)	A vulnerability has been found in SofaWiki up to 3.8.9 and classified as problematic. This vulnerability affects unknown code of the file index.php. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-29720. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-31757	DedeCMS up to 5.7.108 sys_info.php edit___cfg_powerby/edit___cfg_beian cross site scripting	A vulnerability was found in DedeCMS up to 5.7.108. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file sys_info.php. The manipulation of the argument edit___cfg_powerby/edit___cfg_beian leads to cross site scripting. This vulnerability is known as CVE-2023-31757. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-2814	SourceCodester Class Scheduling System 1.0 POST Parameter /admin/save_teacher.php Academic_Rank cross site scripting	A vulnerability classified as problematic has been found in SourceCodester Class Scheduling System 1.0. Affected is an unknown function of the file /admin/save_teacher.php of the component POST Parameter Handler. The manipulation of the argument Academic_Rank leads to cross site scripting. This vulnerability is traded as CVE-2023-2814. 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-2023-2824	SourceCodester Dental Clinic Appointment Reservation System 1.0 POST Parameter /admin/service.php service cross site scripting	A vulnerability was found in SourceCodester Dental Clinic Appointment Reservation System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/service.php of the component POST Parameter Handler. The manipulation of the argument service leads to cross site scripting. This vulnerability is handled as CVE-2023-2824. 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-2023-2822	Ellucian Ethos Identity up to 5.10.5 /cas/logout url cross site scripting	A vulnerability was found in Ellucian Ethos Identity up to 5.10.5. It has been classified as problematic. Affected is an unknown function of the file /cas/logout. The manipulation of the argument url leads to cross site scripting. This vulnerability is traded as CVE-2023-2822. It is possible to launch the attack remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-2826	SourceCodester Class Scheduling System 1.0 POST Parameter search_teacher_result.php teacher cross site scripting	A vulnerability has been found in SourceCodester Class Scheduling System 1.0 and classified as problematic. This vulnerability affects unknown code of the file search_teacher_result.php of the component POST Parameter Handler. The manipulation of the argument teacher leads to cross site scripting. This vulnerability was named CVE-2023-2826. The attack can be initiated 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-2021-46888	hledger up to 1.22 toBloodhoundJson cross site scripting (Issue 1525)	A vulnerability which was classified as problematic was found in hledger up to 1.22. Affected is the function toBloodhoundJson. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2021-46888. 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-2023-31584	cu silicon a9ef36 cross site scripting	A vulnerability classified as problematic has been found in cu silicon a9ef36. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-31584. 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-2023-31664	WSO2 API Manager up to 4.1.x login.do tenantDomain cross site scripting	A vulnerability was found in WSO2 API Manager up to 4.1.x. It has been rated as problematic. This issue affects some unknown processing of the file /authenticationendpoint/login.do. The manipulation of the argument tenantDomain leads to cross site scripting. The identification of this vulnerability is CVE-2023-31664. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-31816	IT Sourcecode Content Management System 1.0.0 search_list.php cross site scripting	A vulnerability was found in IT Sourcecode Content Management System 1.0.0. It has been classified as problematic. Affected is an unknown function of the file /ecodesource/search_list.php. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-31816. 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-2023-25440	CiviCRM 5.59.alpha1 first name/second name cross site scripting	A vulnerability was found in CiviCRM 5.59.alpha1. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument first name/second name leads to cross site scripting. This vulnerability is known as CVE-2023-25440. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-33599	EasyImages up to 2.8.1 viewlog.php cross site scripting (Issue 115)	A vulnerability was found in EasyImages up to 2.8.1. It has been classified as problematic. Affected is an unknown function of the file viewlog.php. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-33599. 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-2023-31860	Wuzhi CMS 3.1.2 Five Finger CMS b2b System cross site scripting	A vulnerability which was classified as problematic has been found in Wuzhi CMS 3.1.2. Affected by this issue is some unknown functionality of the component Five Finger CMS b2b System. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-31860. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-2864	SourceCodester Online Jewelry Store 1.0 POST Parameter customer.php Custid cross site scripting	A vulnerability was found in SourceCodester Online Jewelry Store 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file customer.php of the component POST Parameter Handler. The manipulation of the argument Custid leads to cross site scripting. This vulnerability is handled as CVE-2023-2864. 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-2023-2862	SiteServer CMS up to 7.2.1 /api/stl/actions/search ajaxDivId cross site scripting (I71WJ4)	A vulnerability which was classified as problematic was found in SiteServer CMS up to 7.2.1. Affected is an unknown function of the file /api/stl/actions/search. The manipulation of the argument ajaxDivId leads to cross site scripting. This vulnerability is traded as CVE-2023-2862. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-33789	Netbox 3.5.1 Create Contact Groups / tenancy/con-tact-groups/ Name cross site scripting	A vulnerability classified as problematic was found in Netbox 3.5.1. Affected by this vulnerability is an unknown functional-ity of the file /tenancy/ contact-groups/ of the component Con-tact Groups. The manip-ulation of the argument Name leads to cross site scripting. This vulnerability is known as CVE-2023-33789. The attack can be launched re-motely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-33785	Netbox 3.5.1 /dcim/ rack-roles/ Name cross site scripting	A vulnerability was found in Netbox 3.5.1. It has been classified as problematic. This affects an unknown part of the file /dcim/rack-roles/. The manipulation of the argument Name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-33785. It is possible to initiate the attack re-motely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-42225	Jumpserver up to 2.10.0/2.26.0 cross site scripting	A vulnerability which was classified as problematic has been found in Jump-server up to 2.10.0/2.26.0. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2022-42225. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-33787	Netbox 3.5.1 Create Tenant Groups /ten-ancy/tenant-groups/ Name cross site scripting	A vulnerability was found in Netbox 3.5.1. It has been rated as problematic. This issue affects some unknown processing of the file /tenancy/tenant-groups/ of the component Create Tenant Groups. The manipulation of the argu-ment Name leads to cross site scripting. The identification of this vulnerability is CVE-2023-33787. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-33790	Netbox 3.5.1 Create Locations /dcim/lo-cations/ Name cross site scripting	A vulnerability which was classified as problematic has been found in Netbox 3.5.1. Affected by this issue is some unknown func-tionality of the file /dcim/ locations/ of the compo-nent Create Locations. The manipulation of the argument Name leads to cross site scripting. This vulnerability is handled as CVE-2023-33790. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-33794	Netbox 3.5.1 Create Tenants /tenancy/ tenants/ Name cross site scripting	A vulnerability was found in Netbox 3.5.1. It has been classified as problematic. Affected is an unknown function of the file / tenancy/tenants/ of the component Create Ten-ants. The manipulation of the argument Name leads to cross site scripting. This vulnerability is traded as CVE-2023-33794. 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-2023-33793	Netbox 3.5.1 Create Power Panels /dcim/ power-panels/ Name cross site scripting	A vulnerability has been found in Netbox 3.5.1 and classified as problematic. This vulnerability affects unknown code of the file / dcim/power-panels/ of the component Create Power Panels. The manipulation of the argument Name leads to cross site script-ing. This vulnerability was named CVE-2023-33793. The attack can be initiated remotely. There is no ex-ploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-33788	Netbox 3.5.1 Create Providers /circuits/ providers/ Name cross site scripting	A vulnerability classified as problematic has been found in Netbox 3.5.1. Affected is an unknown function of the file / circuits/providers/ of the component Create Provid-ers. The manipulation of the argument Name leads to cross site scripting. This vulnerability is traded as CVE-2023-33788. 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-2023-33786	Netbox 3.5.1 Create Circuit Types /cir-cuits/circuit-types/ Name cross site scripting	A vulnerability was found in Netbox 3.5.1. It has been declared as problematic. This vulnerability affects unknown code of the file /circuits/circuit-types/ of the component Create Circuit Types. The manip-ulation of the argument Name leads to cross site scripting. This vulnerability was named CVE-2023-33786. The attack can be initiated remotely. There is no ex-ploit 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-2023-33792	Netbox 3.5.1 Create Site Groups /dcim/site-groups/ Name cross site scripting (Issue 10)	A vulnerability was found in Netbox 3.5.1 and classified as problematic. This issue affects some unknown processing of the file /dcim/site-groups/ of the component Create Site Groups. The manipulation of the argument Name leads to cross site scripting. The identification of this vulnerability is CVE-2023-33792. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-33791	Netbox 3.5.1 Create Provider Accounts Name cross site scripting	A vulnerability which was classified as problematic was found in Netbox 3.5.1. This affects an unknown part of the file /circuits/provider-accounts/ of the component Create Provider Accounts. The manipulation of the argument Name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-33791. 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-2023-33750	mipjz 5.0.5 Description cross site scripting (Issue 15)	A vulnerability was found in mipjz 5.0.5 and classified as problematic. Affected by this issue is some unknown functionality of the file /index.phps/article/ApiAdminArticle/itemAdd. The manipulation of the argument Description leads to cross site scripting. This vulnerability is handled as CVE-2023-33750. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-33356	IceCMS 1.0.0 cross site scripting	A vulnerability which was classified as problematic was found in IceCMS 1.0.0. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-33356. 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-2023-33751	mipjz 5.0.5 ApiAdminTagCategory.php name cross site scripting (Issue 14)	A vulnerability was found in mipjz 5.0.5. It has been classified as problematic. This affects an unknown part of the file /app/tag/controller/ApiAdminTagCategory.php. The manipulation of the argument name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-33751. 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-2023-33795	Netbox 3.5.1 Create Contact Roles /tenancy/contact-roles/ Name cross site scripting (Issue 15)	A vulnerability was found in Netbox 3.5.1. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /tenancy/contact-roles/ of the component Create Contact Roles. The manipulation of the argument Name leads to cross site scripting. This vulnerability is known as CVE-2023-33795. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-33829	Cloudogu SCM Manager up to 1.60 Description cross site scripting	A vulnerability was found in Cloudogu SCM Manager up to 1.60. It has been rated as problematic. This issue affects some unknown processing. The manipulation of the argument Description leads to cross site scripting. The identification of this vulnerability is CVE-2023-33829. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-25439	Square Pig Fusion-Invoice 2023-1.0 description/expenses/tasks/customer cross site scripting (ID 172556)	A vulnerability was found in Square Pig Fusion-Invoice 2023-1.0 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument description/expenses/tasks/customer leads to cross site scripting. This vulnerability is handled as CVE-2023-25439. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-33800	Netbox 3.5.1 Create Regions /dcim/regions/ Name cross site scripting (Issue 11)	A vulnerability which was classified as problematic was found in Netbox 3.5.1. Affected is an unknown function of the file /dcim/regions/ of the component Create Regions. The manipulation of the argument Name leads to cross site scripting. This vulnerability is traded as CVE-2023-33800. 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-2023-33799	Netbox 3.5.1 Create Contacts /tenancy/contacts/ Name cross site scripting (Issue 14)	A vulnerability which was classified as problematic has been found in Netbox 3.5.1. This issue affects some unknown processing of the file /tenancy/contacts/ of the component Create Contacts. The manipulation of the argument Name leads to cross site scripting. The identification of this vulnerability is CVE-2023-33799. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-33797	Netbox 3.5.1 Create Sites /dcim/sites/ Name cross site scripting (Issue 12)	A vulnerability classified as problematic has been found in Netbox 3.5.1. This affects an unknown part of the file /dcim/sites/ of the component Create Sites. The manipulation of the argument Name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-33797. 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-2023-33798	Netbox 3.5.1 Create Rack /dcim/rack/ Name cross site scripting (Issue 13)	A vulnerability classified as problematic was found in Netbox 3.5.1. This vulnerability affects unknown code of the file /dcim/rack/ of the component Create Rack. The manipulation of the argument Name leads to cross site scripting. This vulnerability was named CVE-2023-33798. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-33197	Craft CMS indexedVolumes cross site scripting	A vulnerability was found in Craft CMS. It has been classified as problematic. Affected is an unknown function. The manipulation of the argument indexedVolumes leads to cross site scripting. This vulnerability is traded as CVE-2023-33197. 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-2023-33195	Craft CMS RSS Feed Widget cross site scripting	A vulnerability was found in Craft CMS. It has been rated as problematic. Affected by this issue is some unknown functionality of the component RSS Feed Widget. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-33195. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-30145	Camaleon CMS 2.7.0 Template formats injection	A vulnerability was found in Camaleon CMS 2.7.0. It has been classified as problematic. This affects an unknown part of the component Template Handler. The manipulation of the argument formats leads to injection. This vulnerability is uniquely identified as CVE-2023-30145. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-33780	TFDi smartCARS up to 0.7.0 News Article cross site scripting (GHSA-hx8p-f8h7-5h78)	A vulnerability was found in TFDi smartCARS up to 0.7.0 and classified as problematic. Affected by this issue is some unknown functionality of the component News Article Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-33780. 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-2023-33394	Zorlan skycaiji 2.5.4 JSON Data cross site scripting	A vulnerability was found in Zorlan skycaiji 2.5.4. It has been rated as problematic. This issue affects some unknown processing of the component JSON Data Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-33394. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-2925	Webkul krayin crm 1.2.4 Edit Person Page 2 Organization cross site scripting	A vulnerability which was classified as problematic was found in Webkul krayin crm 1.2.4. This affects an unknown part of the file /admin/contacts/organizations/edit/2 of the component Edit Person Page. The manipulation of the argument Organization leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-2925. It is possible to initiate the attack 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 Cross-Site Scripting attack.
CVE-2023-33255	Papaya Viewer 4a42701 DICOM Image cross site scripting	A vulnerability which was classified as problematic has been found in Papaya Viewer 4a42701. This issue affects some unknown processing of the component DICOM Image Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-33255. An attack has to be approached locally. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-2922	SourceCodester Comment System 1.0 GET Parameter index.php msg cross site scripting	A vulnerability classified as problematic has been found in SourceCodester Comment System 1.0. Affected is an unknown function of the file index.php of the component GET Parameter Handler. The manipulation of the argument msg leads to cross site scripting. This vulnerability is traded as CVE-2023-2922. 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-2023-2943	OpenEMR up to 7.0.0 code injection	A vulnerability was found in OpenEMR up to 7.0.0. It has been classified as critical. Affected is an unknown function. The manipulation leads to code injection. This vulnerability is traded as CVE-2023-2943. 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-2023-2949	OpenEMR up to 7.0.0 cross site scripting	A vulnerability which was classified as problematic was found in OpenEMR up to 7.0.0. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-2949. 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-2023-2950	OpenEMR up to 7.0.0 improper authorization	A vulnerability has been found in OpenEMR up to 7.0.0 and classified as critical. This vulnerability affects unknown code. The manipulation leads to improper authorization. This vulnerability was named CVE-2023-2950. 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-2023-2948	OpenEMR up to 7.0.0 cross site scripting	A vulnerability which was classified as problematic has been found in OpenEMR up to 7.0.0. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-2948. 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-2023-2947	OpenEMR up to 7.0.0 cross site scripting	A vulnerability classified as problematic has been found in OpenEMR up to 7.0.0. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-2947. 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-2023-2954	liangliangyy djangoblog cross site scripting	A vulnerability has been found in liangliangyy djangoblog and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-2954. The attack can be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-24631	AudioCodes Device Manager Express up to 7.8.20002.47752 ajaxTenants.php desc cross site scripting	A vulnerability which was classified as problematic has been found in AudioCodes Device Manager Express up to 7.8.20002.47752. Affected by this issue is some unknown functionality of the file ajaxTenants.php. The manipulation of the argument desc leads to cross site scripting. This vulnerability is handled as CVE-2022-24631. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting 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.

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