INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

July 2023

The total zero-day vulnerabilities count for July month 266

Command Injection	CSRF	Local File Inclusion	Malicious File Upload	SQL Injection	Cross-site Scripting	HTTP Request Smuggling
35	35	15	24	43	113	1

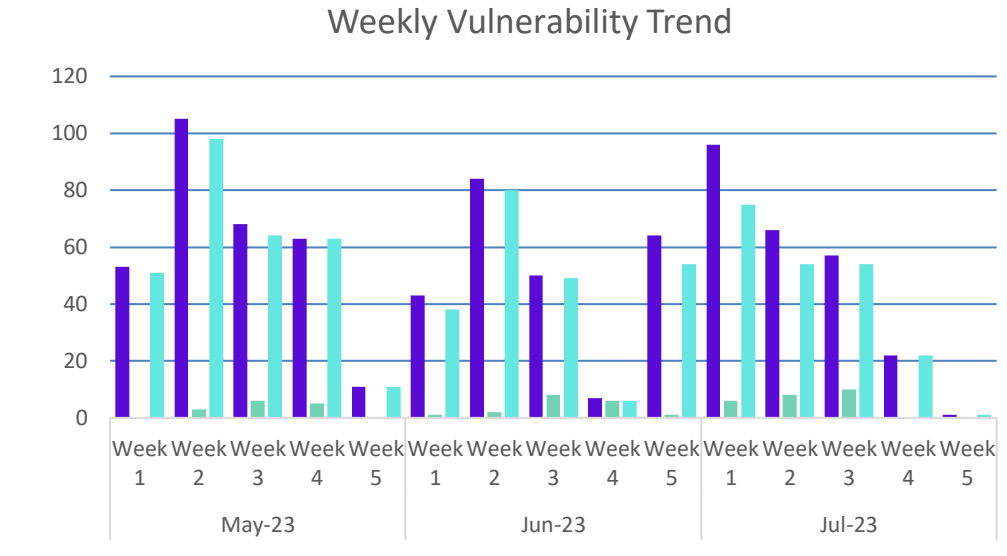
Zero-day vulnerabilities protected through core rules	242
Zero-day vulnerabilities protected through custom rules	24
Zero-day vulnerabilities for which protection cannot be done	0
Zero-day vulnerabilities found by Indusface WAS	206

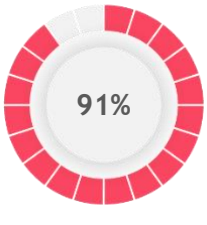
- To enable custom rules, please contact support@indusface.com
- Since the attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.

Vulnerability Trend:

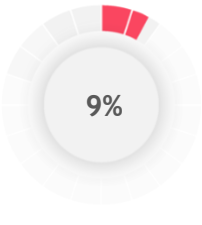
The weekly trend displays the total number of vulnerabilities discovered to the type of protection provided for the last quarter.

Weekly Vulnerability Trend

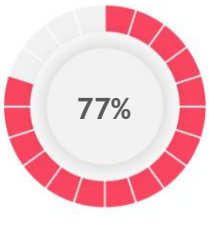




of the zero-day vulnerabilities were protected by the core rules in the last month

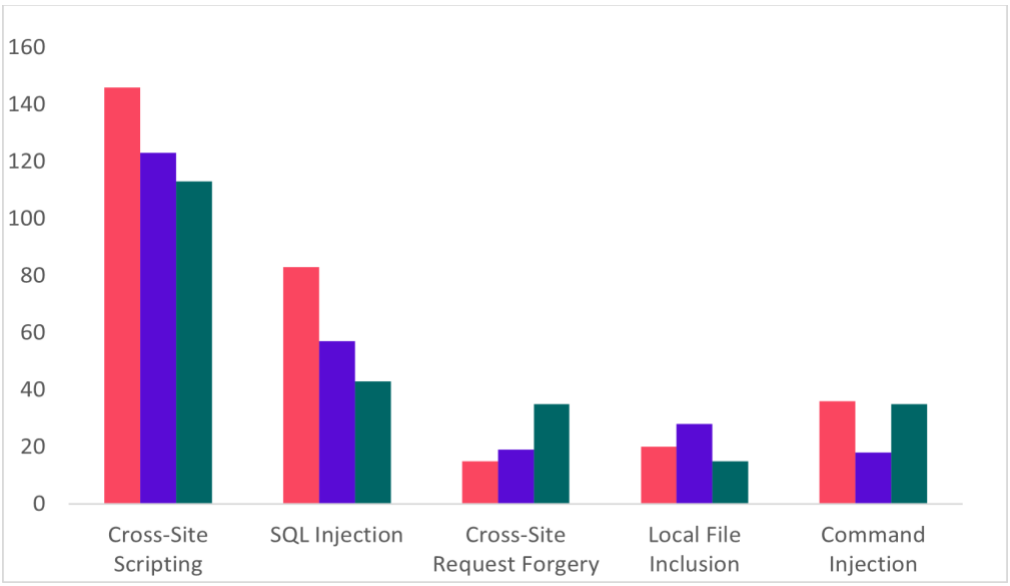


of the zero-day vulnerabilities were protected by the custom rules in the last month



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-2023-33298	Perimeter81 10.0.0.19 on macOS com.perimeter81.osx.HelperTool usingCAPath os command injection	A vulnerability which was classified as critical was found in Perimeter81 10.0.0.19 on macOS. Affected is the function usingCAPath of the component com.perimeter81.osx.HelperTool. The manipulation leads to os command injection. This vulnerability is traded as CVE-2023-33298. An attack has to be approached locally. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-24520	Milesight UR32L 32.3.0.5 Network Request vtysh_ubus toolsh_excute.constprop.1 os command injection (TALOS-2023-1706)	A vulnerability was found in Milesight UR32L 32.3.0.5. It has been declared as critical. This vulnerability affects the function toolsh_excute.constprop.1 of the file vtysh_ubus of the component Network Request Handler. The manipulation leads to os command injection. This vulnerability was named CVE-2023-24520. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-24582	Milesight UR32L up to 32.3.0.5 Network Request urvpn_client cmd_name_action os command injection (TALOS-2023-1710)	A vulnerability was found in Milesight UR32L up to 32.3.0.5. It has been rated as critical. This issue affects the function cmd_name_action of the file urvpn_client of the component Network Request Handler. The manipulation leads to os command injection. The identification of this vulnerability is CVE-2023-24582. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-23550	Milesight UR32L 32.3.0.5 Network Request ys_thirdparty user_delete os command injection (TALOS-2023-1694)	A vulnerability classified as critical was found in Milesight UR32L 32.3.0.5. This vulnerability affects the function user_delete of the file ys_thirdparty of the component Network Request Handler. The manipulation leads to os command injection. This vulnerability was named CVE-2023-23550. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-36458	1Panel up to 1.3.5 command injection (GHSA-7x2c-fgx6-xf9h)	A vulnerability was found in 1Panel up to 1.3.5. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to command injection. The identification of this vulnerability is CVE-2023-36458. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-25583	Milesight UR32L 32.3.0.5 Network Request zebra vlan_name os command injection (TALOS-2023-1723)	A vulnerability classified as critical was found in Milesight UR32L 32.3.0.5. This vulnerability affects the function vlan_name of the file zebra of the component Network Request Handler. The manipulation leads to os command injection. This vulnerability was named CVE-2023-25583. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-36622	Loxone Miniserver Go Gen.2 prior 14.1.5.9 Websocket Configuration Endpoint timezone os command injection (SYSS-2023-012)	A vulnerability which was classified as critical was found in Loxone Miniserver Go Gen.2. This affects an unknown part of the component Websocket Configuration Endpoint. The manipulation of the argument timezone leads to os command injection. This vulnerability is uniquely identified as CVE-2023-36622. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-25582	Milesight UR32L 32.3.0.5 Network Request vlan_name os command injection (TALOS-2023-1723)	A vulnerability was found in Milesight UR32L 32.3.0.5. It has been classified as critical. Affected is the function vlan_name of the component Network Request Handler. The manipulation leads to os command injection. This vulnerability is traded as CVE-2023-25582. Access to the local network is required for this attack. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-24595	Milesight UR32L 32.3.0.5 Network Request ys_thirdparty system_user_script os command injection (TALOS-2023-1713)	A vulnerability classified as critical was found in Milesight UR32L 32.3.0.5. Affected by this vulnerability is the function system_user_script of the file ys_thirdparty of the component Network Request Handler. The manipulation leads to os	Protected by core rules	Detected by scanner as Command Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		command injection. This vulnerability is known as CVE-2023-24595. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2023-36457	1Panel up to 1.3.5 Container Repository command injection (GHSA-q2mx-gpjf-3h8x)	A vulnerability was found in 1Panel up to 1.3.5. It has been declared as critical. This vulnerability affects unknown code of the component Container Repository Handler. The manipulation leads to command injection. This vulnerability was named CVE-2023-36457. 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 Command Injection attack.
CVE-2023-24583	Milesight UR32L 32.3.0.5 Network Request urvpn_client cmd_name_action os command injection (TALOS-2023-1710)	A vulnerability classified as critical has been found in Milesight UR32L 32.3.0.5. Affected is the function cmd_name_action of the file urvpn_client of the component Network Request Handler. The manipulation leads to os command injection. This vulnerability is traded as CVE-2023-24583. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-24519	Milesight UR32L 32.3.0.5 Network Request vtysh_ubus toolsh_excute.constprop .1 command injection (TALOS-2023-1706)	A vulnerability was found in Milesight UR32L 32.3.0.5. It has been classified as critical. This affects the function toolsh_excute.constprop.1 of the file vtysh_ubus of the component Network Request Handler. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2023-24519. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-37149	Totolink LR350 9.3.5u.6369_B20220309 setUploadSetting FileName command injection	A vulnerability was found in Totolink LR350 9.3.5u.6369_B20220309 and classified as critical. This issue affects the function setUploadSetting. The manipulation of the argument FileName leads to command injection. The identification of this vulnerability is CVE-2023-37149. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-37144	Tenda AC10 15.03.06.26 formWriteFacMac mac command injection	A vulnerability classified as critical was found in Tenda AC10 15.03.06.26. Affected by this vulnerability is the function formWriteFacMac. The manipulation of the argument mac leads to command injection. This vulnerability is known as CVE-2023-37144. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-37148	Totolink LR350 9.3.5u.6369_B20220309 setUssd ussd command	A vulnerability has been found in Totolink LR350 9.3.5u.6369_B20220309	Protected by core rules	Detected by scanner as Command

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	and classified as critical. This vulnerability affects the function setUssd. The manipulation of the argument ussd leads to command injection. This vulnerability was named CVE-2023-37148. Access to the local network is required for this attack to succeed. There is no exploit available.		Injection attack.
CVE-2023-37146	Totolink LR350 9.3.5u.6369_B20220309 UploadFirmwareFile FileName command injection	A vulnerability which was classified as critical was found in Totolink LR350 9.3.5u.6369_B20220309. This affects the function UploadFirmwareFile. The manipulation of the argument FileName leads to command injection. This vulnerability is uniquely identified as CVE-2023-37146. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-37145	Totolink LR350 9.3.5u.6369_B20220309 setOpModeCfg hostname command injection	A vulnerability which was classified as critical has been found in Totolink LR350 9.3.5u.6369_B20220309. Affected by this issue is the function setOpModeCfg. The manipulation of the argument hostname leads to command injection. This vulnerability is handled as CVE-2023-37145. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-37172	Totolink A3300R 17.0.0cu.557_B20221024 setDiagnosisCfg ip command injection	A vulnerability classified as critical has been found in Totolink A3300R 17.0.0cu.557_B20221024. This affects the function setDiagnosisCfg. The manipulation of the argument ip leads to command injection. This vulnerability is uniquely identified as CVE-2023-37172. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-37171	Totolink A3300R 17.0.0cu.557_B20221024 setPasswordCfg admuser command injection	A vulnerability was found in Totolink A3300R 17.0.0cu.557_B20221024. It has been rated as critical. Affected by this issue is the function setPasswordCfg. The manipulation of the argument admuser leads to command injection. This vulnerability is handled as CVE-2023-37171. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-37173	Totolink A3300R 17.0.0cu.557_B20221024 setTracerouteCfg command command injection	A vulnerability classified as critical was found in Totolink A3300R 17.0.0cu.557_B20221024. This vulnerability affects the function setTracerouteCfg. The manipulation of the argument command leads to command injection. This vulnerability was named CVE-2023-37173. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-3606	TamronOS up to 20230703 /api/ping host	A vulnerability was found in TamronOS up to	Protected by core rules	Detected by scanner as

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	os command injection	20230703. It has been classified as critical. This affects an unknown part of the file /api/ping. The manipulation of the argument host leads to os command injection. This vulnerability is uniquely identified as CVE-2023-3606. 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.		Command Injection attack.
CVE-2023-3607	kodbox 1.26 WebConsole Plug-In webconsole.php.txt Execute os command injection	A vulnerability was found in kodbox 1.26. It has been declared as critical. This vulnerability affects the function Execute of the file webconsole.php.txt of the component WebConsole Plug-In. The manipulation leads to os command injection. This vulnerability was named CVE-2023-3607. Access to the local network is required for this attack. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-3608	Ruijie BCR810W 2.5.10 Tracert Page os command injection	A vulnerability was found in Ruijie BCR810W 2.5.10. It has been rated as critical. This issue affects some unknown processing of the component Tracert Page. The manipulation leads to os command injection. The identification of this vulnerability is CVE-2023-3608. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-36884	Microsoft Windows up to Server 2022 HTML Remote Code Execution	A vulnerability was found in Microsoft Windows. It has been rated as critical. Affected by this issue is some unknown functionality of the component HTML. The manipulation leads to Remote Code Execution. This vulnerability is handled as CVE-2023-36884. The attack may be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-36887	Microsoft Edge Remote Code Execution	A vulnerability classified as critical has been found in Microsoft Edge. This affects an unknown part. The manipulation leads to Remote Code Execution. This vulnerability is uniquely identified as CVE-2023-36887. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-37794	WAYOS FBM-291W 19.09.11V /upgrade_filter.asp command injection	A vulnerability which was classified as critical has been found in WAYOS FBM-291W 19.09.11V. Affected by this issue is some unknown functionality of the file /upgrade_filter.asp. The manipulation leads to command injection. This vulnerability is handled as CVE-2023-37794. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-38336	rsh-client 0.17-24 netkit-rcp /bin/sh command injection	A vulnerability has been found in rsh-client 0.17-24 and classified as critical. This vulnerability affects unknown code of the file /bin/sh of the component netkit-rcp. The manipulation leads to command injection. This vulnerability was named CVE-2023-38336. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-38378	RIGOL SO5000 Digital Oscilloscope 00.01.03.00.03 Web Interface changepwd.cgi pass1 os command injection	A vulnerability was found in RIGOL SO5000 Digital Oscilloscope 00.01.03.00.03. It has been declared as critical. This vulnerability affects unknown code of the file changepwd.cgi of the component Web Interface. The manipulation of the argument pass1 leads to os command injection. This vulnerability was named CVE-2023-38378. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-37477	1Panel up to 1.4.2 HTTP Request /hosts/firewall/ip os command injection (GHSA-p9xf-74xh-mhw5)	A vulnerability classified as critical has been found in 1Panel up to 1.4.2. Affected is an unknown function of the file /hosts/firewall/ip of the component HTTP Request Handler. The manipulation leads to os command injection. This vulnerability is traded as CVE-2023-37477. 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 Command Injection attack.
CVE-2022-1471	Oracle PeopleSoft Enterprise PeopleTools 8.59/8.60 Elastic Search Remote Code Execution	A vulnerability has been found in Oracle PeopleSoft Enterprise PeopleTools 8.59/8.60 and classified as very critical. This vulnerability affects unknown code of the component Elastic Search. The manipulation leads to Remote Code Execution. This vulnerability was named CVE-2022-1471. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2022-1471	Oracle Utilities Testing Accelerator up to 7.0.0.0 Tools Remote Code Execution	A vulnerability was found in Oracle Utilities Testing Accelerator up to 7.0.0.0 and classified as very critical. Affected by this issue is some unknown functionality of the component Tools. The manipulation leads to Remote Code Execution. This vulnerability is handled as CVE-2022-	Protected by core rules	Detected by scanner as Command Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		1471. The attack may be launched remotely. There is no exploit available.		
CVE-2022-37434	Oracle Retail Advanced Inventory Planning 15.0/16.0 Operations/Maintenance Remote Code Execution	A vulnerability was found in Oracle Retail Advanced Inventory Planning 15.0/16.0. It has been classified as very critical. This affects an unknown part of the component Operations/Maintenance. The manipulation leads to Remote Code Execution. This vulnerability is uniquely identified as CVE-2022-37434. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2022-1471	Oracle Siebel CRM up to 23.4 EAI Remote Code Execution	A vulnerability was found in Oracle Siebel CRM up to 23.4. It has been rated as very critical. Affected by this issue is some unknown functionality of the component EAI. The manipulation leads to Remote Code Execution. This vulnerability is handled as CVE-2022-1471. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2022-27404	Oracle AutoVue up to 21.0.2.7 Security Remote Code Execution	A vulnerability classified as very critical has been found in Oracle AutoVue up to 21.0.2.7. Affected is an unknown function of the component Security. The manipulation leads to Remote Code Execution. This vulnerability is traded as CVE-2022-27404. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack.
CVE-2023-38673	Paddle up to 2.4.x fs.py os command injection (pdsa-2023-005)	A vulnerability classified as critical was found in Paddle up to 2.4.x. Affected by this vulnerability is an unknown functionality of the file fs.py. The manipulation leads to os command injection. This vulnerability is known as CVE-2023-38673. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection attack.

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2020-36739	Feed Them Social Plugin up to 2.8.6 on WordPress my_fts_fb_load_more cross-site request forgery	A vulnerability was found in Feed Them Social Plugin up to 2.8.6 on WordPress. It has been rated as problematic. Affected by this issue is the function my_fts_fb_load_more. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2020-36739. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2020-36749	Easy Testimonials Plugin up to 3.6.1 on WordPress saveCustomFields cross-site request forgery	A vulnerability was found in Easy Testimonials Plugin up to 3.6.1 on WordPress. It has been rated as problematic. Affected by this issue is the function saveCustomFields. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2020-36749. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2021-4392	eCommerce Product Catalog Plugin up to 2.9.43 on WordPress implecode_save_products_meta cross-site request forgery	A vulnerability which was classified as problematic was found in eCommerce Product Catalog Plugin up to 2.9.43 on WordPress. This affects the function implecode_save_products_meta. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2021-4392. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2021-4393	eCommerce Product Catalog Plugin up to 3.0.17 on WordPress save cross-site request forgery	A vulnerability has been found in eCommerce Product Catalog Plugin up to 3.0.17 on WordPress and classified as problematic. This vulnerability affects the function save. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2021-4393. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2020-36735	WP ERP Plugin up to 1.6.3 on WordPress Setting cross-site request forgery	A vulnerability was found in WP ERP Plugin up to 1.6.3 on WordPress. It has been rated as problematic. This issue affects the function handle_leave_calendar_filter/add_enable_disable_option_save/leave_policies/process_bulk_action/process_crm_contact of the component Setting Handler. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2020-36735. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2021-4389	WP Travel Plugin up to 4.4.6 on WordPress save_meta_data cross-site request forgery	A vulnerability which was classified as problematic has been found in WP Travel Plugin up to 4.4.6 on WordPress. Affected by this issue is the function save_meta_data. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2021-4389. The attack may be launched	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2020-36736	CartFlows WooCommerce Checkout & Funnel Builder Plugin up to 1.5.15 on WordPress Setting export_json/import_json/status_logs_file cross-site request forgery (ID 2368446)	A vulnerability classified as problematic has been found in CartFlows WooCommerce Checkout & Funnel Builder Plugin up to 1.5.15 on WordPress. Affected is the function export_json/import_json/status_logs_file of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2020-36736. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2021-4387	Opal Estate Plugin up to 1.6.11 on WordPress cross-site request forgery	A vulnerability which was classified as problematic was found in Opal Estate Plugin up to 1.6.11 on WordPress. Affected is the function opalestate_set_feature_property/opalestate_remove_feature_property. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2021-4387. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2020-36738	Cool Timeline Plugin up to 2.0.2 on WordPress ctl_save cross-site request forgery	A vulnerability was found in Cool Timeline Plugin up to 2.0.2 on WordPress. It has been declared as problematic. Affected by this vulnerability is the function ctl_save. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2020-36738. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2020-36737	Import Export Customizer Settings Plugin up to 1.0.3 on WordPress astra_admin_errors cross-site request forgery	A vulnerability was found in Import Export Customizer Settings Plugin up to 1.0.3 on WordPress. It has been classified as problematic. Affected is the function astra_admin_errors. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2020-36737. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2020-36747	Lightweight Sidebar Manager Plugin up to 1.1.4 on WordPress metabox_save cross-site request forgery	A vulnerability was found in Lightweight Sidebar Manager Plugin up to 1.1.4 on WordPress. It has been classified as problematic. Affected is the function metabox_save. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2020-36747. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2021-4390	Contact Form 7 Style Plugin up to 3.2 on WordPress manage_wp_posts_be_qe_save_post cross-site request forgery	A vulnerability classified as problematic was found in Contact Form 7 Style Plugin up to 3.2 on WordPress. Affected by this vulnerability is the function manage_wp_posts_be_qe_save_post. The manipulation leads to cross-site request forgery.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is known as CVE-2021-4390. The attack can be launched remotely. There is no exploit available.		
CVE-2020-36748	Dokan Plugin up to 3.0.8 on WordPress handle_order_export cross-site request forgery	A vulnerability was found in Dokan Plugin up to 3.0.8 on WordPress. It has been declared as problematic. Affected by this vulnerability is the function handle_order_export. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2020-36748. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2021-4394	Locations Plugin up to 3.2.1 on WordPress saveCustomFields cross-site request forgery	A vulnerability which was classified as problematic was found in Locations Plugin up to 3.2.1 on WordPress. This affects the function saveCustomFields. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2021-4394. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2020-36746	Menu Swapper Plugin up to 1.1.0.2 on WordPress mswp_save_meta cross-site request forgery	A vulnerability was found in Menu Swapper Plugin up to 1.1.0.2 on WordPress and classified as problematic. This issue affects the function mswp_save_meta. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2020-36746. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2021-4391	Ultimate Gift Cards for WooCommerce Plugin up to 2.1.1 on WooCommerce mwb_wgm_save_post cross-site request forgery	A vulnerability which was classified as problematic has been found in Ultimate Gift Cards for WooCommerce Plugin up to 2.1.1 on WooCommerce. Affected by this issue is the function mwb_wgm_save_post. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2021-4391. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-36162	ZZCMS 2023 adminlist.php add cross-site request forgery	A vulnerability which was classified as problematic was found in ZZCMS 2023. Affected is the function add of the file adminlist.php. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-36162. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-37131	YznCMS 1.1.0 POST Request update.html cross-site request forgery	A vulnerability which was classified as problematic was found in YznCMS 1.1.0. Affected is an unknown function of the file /public/admin/profile/update.html of the component POST Request Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-37131. It is possible to launch the	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack remotely. There is no exploit available.		
CVE-2023-25201	MultiTech Conduit AP MTCAP2-L4E1 MTCAP2-L4E1-868-042A 6.0.0 cross-site request forgery	A vulnerability was found in MultiTech Conduit AP MTCAP2-L4E1 MTCAP2-L4E1-868-042A 6.0.0 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-25201. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-36256	Online Examination System Project 1.0 cross-site request forgery (EDB-51511)	A vulnerability has been found in Online Examination System Project 1.0 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-2023-36256. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-3209	MStore API Plugin up to 3.9.6 on WordPress AJAX Action cross-site request forgery	A vulnerability classified as problematic was found in MStore API Plugin up to 3.9.6 on WordPress. This vulnerability affects unknown code of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-3209. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-3627	SalesAgility SuiteCRM up to 8.3.0 cross-site request forgery	A vulnerability was found in SalesAgility SuiteCRM up to 8.3.0. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-3627. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-37596	Issabel PBX 4.0.0-6 deleteuser cross-site request forgery	A vulnerability was found in Issabel PBX 4.0.0-6. It has been classified as problematic. This affects the function deleteuser. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-37596. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-37597	issabel PBX 4.0.0-6 grouplist cross-site request forgery	A vulnerability was found in issabel PBX 4.0.0-6. It has been declared as problematic. This vulnerability affects the function grouplist. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-37597. The attack can be initiated	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. There is no exploit available.		
CVE-2020-36760	Ocean Extra Plugin up to 1.6.5 on WordPress add_core_extensions_bundle_validation cross-site request forgery	A vulnerability has been found in Ocean Extra Plugin up to 1.6.5 on WordPress and classified as problematic. Affected by this vulnerability is the function add_core_extensions_bundle_validation. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2020-36760. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2020-36752	Coming Soon & Maintenance Mode Page Plugin up to 1.57 on WordPress save_meta_box cross-site request forgery	A vulnerability which was classified as problematic has been found in Coming Soon & Maintenance Mode Page Plugin up to 1.57 on WordPress. This issue affects the function save_meta_box. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2020-36752. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2021-4427	Vuukle Comments, Reactions, Share Bar, Revenue Plugin Setting cross-site request forgery	A vulnerability was found in Vuukle Comments Reactions Share Bar Revenue Plugin up to 3.4.31 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/partials/free-comments-for-wordpress-vuukle-admin-display.php of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2021-4427. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2021-4425	Defender Security Plugin up to 2.4.6 on WordPress verify_otp_login_time cross-site request forgery	A vulnerability which was classified as problematic was found in Defender Security Plugin up to 2.4.6 on WordPress. Affected is the function verify_otp_login_time. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2021-4425. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2021-4426	Absolute Reviews Plugin up to 1.0.8 on WordPress metabox_review_save cross-site request forgery	A vulnerability was found in Absolute Reviews Plugin up to 1.0.8 on WordPress and classified as problematic. Affected by this issue is the function metabox_review_save. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2021-4426. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2021-4417	Forminator Plugin up to 1.13.4 on WordPress listen_for_saving_export_schedule cross-site request forgery	A vulnerability classified as problematic was found in Forminator Plugin up to 1.13.4 on WordPress. This vulnerability affects the function listen_for_saving_export_schedule. The manipulation leads to cross-site request forgery.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability was named CVE-2021-4417. The attack can be initiated remotely. There is no exploit available.		
CVE-2020-36761	Top 10 Plugin up to 2.10.4 on WordPress tptn_export_tables cross-site request forgery	A vulnerability which was classified as problematic has been found in Top 10 Plugin up to 2.10.4 on WordPress. This issue affects the function tptn_export_tables. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2020-36761. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-37598	Issabel PBX 4.0.0-6 Virtual Fax cross-site request forgery	A vulnerability was found in Issabel PBX 4.0.0-6. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Virtual Fax Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-37598. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-4023	3DPrint Plugin prior 3.5.6.9 on WordPress cross-site request forgery	A vulnerability has been found in 3DPrint Plugin 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-2022-4023. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-3179	POST SMTP Mailer Plugin up to 2.5.6 on WordPress manage_postman_smtp cross-site request forgery	A vulnerability classified as problematic has been found in POST SMTP Mailer Plugin up to 2.5.6 on WordPress. Affected is the function manage_postman_smtp. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-3179. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-37650	Cockpit CMS 2.5.2 cross-site request forgery	A vulnerability classified as problematic has been found in Cockpit CMS 2.5.2. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-37650. 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

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-36819	Knowage up to 8.1.7 Template importTemplateFile_ _templateName_ path traversal (GHSA-jw99-hxxj-75g2)	A vulnerability which was classified as critical was found in Knowage up to 8.1.7. Affected is an unknown function of the file _/knowage/restful-services/dossier/importTemplateFile_ of the component Template Handler. The manipulation of the argument _templateName_ leads to path traversal. This vulnerability is traded as CVE-2023-36819. 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-2023-1273	ND Shortcodes Plugin up to 6.x on WordPress Shortcode Attribute path traversal	A vulnerability was found in ND Shortcodes Plugin up to 6.x on WordPress and classified as critical. This issue affects some unknown processing of the component Shortcode Attribute Handler. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-1273. The attack needs to be initiated within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack
CVE-2023-24256	NIO EC6 Aspen up to 3.2.x com.nextev.datastatistic path traversal	A vulnerability has been found in NIO EC6 Aspen up to 3.2.x and classified as critical. Affected by this vulnerability is an unknown functionality of the component com.nextev.datastatistic. The manipulation leads to path traversal. This vulnerability is known as CVE-2023-24256. The attack can only be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack
CVE-2023-36822	Uptime Kuma up to 1.22.0 Plugin Installation path traversal (GHSA-vr8x-74pm-6vj7)	A vulnerability was found in Uptime Kuma up to 1.22.0 and classified as critical. This issue affects some unknown processing of the component Plugin Installation Handler. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-36822. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack
CVE-2020-21862	DuxCMS 2.1 /admin/AdminBackup/del path traversal	A vulnerability which was classified as critical has been found in DuxCMS 2.1. This issue affects some unknown processing of the file /admin/AdminBackup/del.	Protected by core rules	Detected by scanner as Local File Inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The manipulation leads to path traversal. The identification of this vulnerability is CVE-2020-21862. The attack needs to be approached within the local network. There is no exploit available.		
CVE-2023-23907	Milesight VPN 2.0.2 Network Request server.js start path traversal (TALOS-2023-1702)	A vulnerability which was classified as critical was found in Milesight VPN 2.0.2. Affected is the function start of the file server.js of the component Network Request Handler. The manipulation leads to path traversal. This vulnerability is traded as CVE-2023-23907. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack
CVE-2023-34259	Kyocera TASKalfa 4053ci up to 2VG_S000.002.561 Web Service path traversal	A vulnerability classified as critical has been found in Kyocera TASKalfa 4053ci up to 2VG_S000.002.561. This affects an unknown part of the component Web Service Handler. The manipulation leads to path traversal: &039;../filedir&039;. This vulnerability is uniquely identified as CVE-2023-34259. Access to the local network is required for this attack. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack
CVE-2023-26563	Syncfusion EJ2 Node File Provider 0102271 on Windows filesystem-server.js path traversal	A vulnerability was found in Syncfusion EJ2 Node File Provider 0102271 on Windows. It has been declared as critical. This vulnerability affects unknown code of the file filesystem-server.js. The manipulation leads to path traversal. This vulnerability was named CVE-2023-26563. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack
CVE-2023-26564	Syncfusion EJ2 ASPCore File Provider 3ac357f PhysicalFileProvider.cs path traversal	A vulnerability was found in Syncfusion EJ2 ASPCore File Provider 3ac357f. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file Models/PhysicalFileProvider.cs. The manipulation leads to path traversal. This vulnerability is known as CVE-2023-26564. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack
CVE-2023-37474	Copyparty up to 1.8.1 .cpr/ path traversal (GHSA-pxfv-7rr3-2qjg)	A vulnerability which was classified as critical has been found in Copyparty up to 1.8.1. This issue affects some unknown processing of the file .cpr/. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-37474. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		It is recommended to upgrade the affected component.		
CVE-2023-37781	EMQX 4.3.8 emqx_sn Plugin path traversal (Issue 10419)	A vulnerability classified as critical was found in EMQX 4.3.8. This vulnerability affects unknown code of the component emqx_sn Plugin. The manipulation leads to path traversal. This vulnerability was named CVE-2023-37781. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack
CVE-2023-37461	Metersphere 2.10.3 belongType path traversal (GHSA-xfr9-jgfp-fx3v)	A vulnerability which was classified as critical was found in Metersphere 2.10.3. This affects an unknown part. The manipulation of the argument belongType leads to path traversal: &039;../filedir&039;. This vulnerability is uniquely identified as CVE-2023-37461. 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-2023-3765	mlflow up to 2.4.x absolute path traversal	A vulnerability which was classified as critical was found in mlflow up to 2.4.x. Affected is an unknown function. The manipulation leads to absolute path traversal. This vulnerability is traded as CVE-2023-3765. 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-2023-31461	SteelSeries GG 36.0.0 API Listener path traversal	A vulnerability was found in SteelSeries GG 36.0.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component API Listener. The manipulation leads to path traversal. This vulnerability is known as CVE-2023-31461. The attack needs to be done within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack
CVE-2023-35081	Ivanti Endpoint Manager Mobile 11.8/11.9/11.10 File path traversal (ID 000087119)	A vulnerability has been found in Ivanti Endpoint Manager Mobile 11.8/11.9/11.10 and classified as critical. This vulnerability affects unknown code of the component File Handler. The manipulation leads to path traversal. This vulnerability was named CVE-2023-35081. The attack can 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 Local File Inclusion attack

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-3491	fossbilling up to 0.5.2 unrestricted upload	A vulnerability classified as problematic was found in fossbilling up to 0.5.2. This vulnerability affects unknown code. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-3491. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by custom rules	No
CVE-2023-31543	pipreqs up to 0.4.11 PyPI Package unrestricted upload	A vulnerability was found in pipreqs up to 0.4.11. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component PyPI Package Handler. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2023-31543. The attack can only be initiated within the local network. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by custom rules	No
CVE-2020-22151	Fuel CMS 1.4.6 ZIP File upload assests permission (Issue 551)	A vulnerability classified as critical has been found in Fuel CMS 1.4.6. Affected is the function upload of the component ZIP File Handler. The manipulation of the argument assests leads to permission issues. This vulnerability is traded as CVE-2020-22151. It is possible to launch the attack remotely. There is no exploit available.	Protected by custom rules	No
CVE-2020-22153	Fuel CMS 1.4.6 navigation upload unrestricted upload (Issue 553)	A vulnerability has been found in Fuel CMS 1.4.6 and classified as critical. This vulnerability affects the function navigation. The manipulation of the argument upload leads to unrestricted upload. This vulnerability was named CVE-2020-22153. The attack can be initiated remotely. There is no exploit available.	Protected by custom rules	No
CVE-2023-3503	SourceCodester Shopping Website 1.0 insert-product.php unrestricted upload	A vulnerability has been found in SourceCodester Shopping Website 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file insert-product.php. The manipulation leads to unrestricted upload.	Protected by custom rules	No

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is known as CVE-2023-3503. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2023-36969	CMS Made Simple 2.2.17 unrestricted upload	A vulnerability classified as critical was found in CMS Made Simple 2.2.17. This vulnerability affects unknown code. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-36969. The attack can be initiated remotely. There is no exploit available.	Protected by custom rules	No
CVE-2023-37152	Projectworlds Online Art Gallery Project 1.0 adminHome.php unrestricted upload (Exploit 51524 / EDB-51524)	A vulnerability classified as critical was found in Projectworlds Online Art Gallery Project 1.0. This vulnerability affects unknown code of the file adminHome.php. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-37152. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by custom rules	No
CVE-2023-37151	SourceCodester Online Pizza Ordering System 1.0 unrestricted upload (Exploit 51431 / EDB-51431)	A vulnerability was found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. This issue affects some unknown processing. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2023-37151. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by custom rules	No
CVE-2023-37629	Online Piggery Management System 1.0 POST Request add-pig.php unrestricted upload	A vulnerability was found in Online Piggery Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file add-pig.php of the component POST Request Handler. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2023-37629. The attack can only be initiated within the local network. There is no exploit available.	Protected by custom rules	No
CVE-2023-3342	User Registration Plugin up to 3.0.2/3.0.2.1 on WordPress ur_upload_profile_pic unrestricted upload	A vulnerability which was classified as critical has been found in User Registration Plugin up to 3.0.2/3.0.2.1 on WordPress. This issue affects the function ur_upload_profile_pic. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2023-3342. The attack may be initiated	Protected by custom rules	No

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. There is no exploit available.		
CVE-2023-37839	DedeCMS 5.7.109 PHP File file_manage_control.php unrestricted upload	A vulnerability classified as critical was found in DedeCMS 5.7.109. This vulnerability affects unknown code of the file /dede/file_manage_control.php of the component PHP File Handler. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-37839. The attack can be initiated remotely. There is no exploit available.	Protected by custom rules	No
CVE-2023-36119	PHPGurukul Online Security Guards Hiring System 1.0 PHP File unrestricted upload	A vulnerability which was classified as critical has been found in PHPGurukul Online Security Guards Hiring System 1.0. This issue affects some unknown processing of the component PHP File Handler. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2023-36119. The attack may be initiated remotely. There is no exploit available.	Protected by custom rules	No
CVE-2023-30791	Plane 0.7.1-dev Avatar unrestricted upload	A vulnerability was found in Plane 0.7.1-dev. It has been classified as problematic. Affected is an unknown function of the component Avatar Handler. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2023-30791. It is possible to launch the attack remotely. There is no exploit available.	Protected by custom rules	No
CVE-2023-3692	admidio up to 4.2.9 unrestricted upload	A vulnerability classified as problematic has been found in admidio up to 4.2.9. This affects an unknown part. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-3692. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by custom rules	No
CVE-2020-22159	EVERTZ 3080IPX/7801FC/7890IXG unrestricted upload	A vulnerability was found in EVERTZ 3080IPX 7801FC and 7890IXG. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation leads to unrestricted upload. This vulnerability is	Protected by custom rules	No

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		handled as CVE-2020-22159. The attack needs to be done within the local network. There is no exploit available.		
CVE-2023-37733	tduck-platform 4.0 HTML File unrestricted upload (Issue 17)	A vulnerability classified as critical was found in tduck-platform 4.0. This vulnerability affects unknown code of the component HTML File Handler. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-37733. The attack needs to be initiated within the local network. There is no exploit available.	Protected by custom rules	No
CVE-2023-3802	Chengdu Flash Flood Disaster Monitoring and Warning System Ajaxfileupload.ashx unrestricted upload	A vulnerability was found in Chengdu Flash Flood Disaster Monitoring and Warning System 2.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /Controller/Ajaxfileupload.ashx. The manipulation of the argument file leads to unrestricted upload. This vulnerability is handled as CVE-2023-3802. The attack needs to be done within the local network. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by custom rules	No
CVE-2023-3806	SourceCodester House Rental and Property Listing System 1.0 btn_functions.php unrestricted upload	A vulnerability which was classified as critical was found in SourceCodester House Rental and Property Listing System 1.0. Affected is an unknown function of the file btn_functions.php. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2023-3806. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by custom rules	No
CVE-2023-3804	Chengdu Flash Flood Disaster Monitoring and Warning System FileHandler.ashx unrestricted upload	A vulnerability classified as problematic was found in Chengdu Flash Flood Disaster Monitoring and Warning System 2.0. This vulnerability affects unknown code of the file /Service/FileHandler.ashx. The manipulation of the argument userFile leads to unrestricted upload. This vulnerability was named CVE-2023-3804. Access to the local network is required for this attack. Furthermore there is an exploit	Protected by custom rules	No

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2023-3798	Chengdu Flash Flood Disaster Monitoring and Warning System upload.aspx unrestricted upload	A vulnerability has been found in Chengdu Flash Flood Disaster Monitoring and Warning System 2.0 and classified as critical. This vulnerability affects unknown code of the file /App_Resource/UEditor/server/upload.aspx. The manipulation of the argument file leads to unrestricted upload. This vulnerability was named CVE-2023-3798. Access to the local network is required for this attack to succeed. 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	No
CVE-2023-37602	Alkacon OpenCMS 15.0 PNG File /workplace#!explorer unrestricted upload (Exploit 51564 / EDB-51564)	A vulnerability which was classified as problematic was found in Alkacon OpenCMS 15.0. Affected is an unknown function of the file /workplace!explorer of the component PNG File Handler. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2023-37602. The attack can only be done within the local network. Furthermore there is an exploit available.	Protected by custom rules	No
CVE-2023-3797	Gen Technology Four Mountain Torrent Disaster Prevention and Control of Monitoring and Early Warning System UploadFloodPlanFileUpdate.ashx unrestricted upload	A vulnerability which was classified as critical was found in Gen Technology Four Mountain Torrent Disaster Prevention and Control of Monitoring and Early Warning System up to 20230712. This affects an unknown part of the file /Duty/AjaxHandle/UploadFloodPlanFileUpdate.ashx. The manipulation of the argument Filedata leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-3797. Access to the local network is required for this attack. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by custom rules	No
CVE-2023-3836	Dahua Smart Park Management up to 20230713 devicePoint_addImgIco upload unrestricted upload	A vulnerability classified as critical was found in Dahua Smart Park Management up to 20230713. This vulnerability affects	Protected by custom rules	No

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown code of the file /emap/devicePoint_addImglcohasSubsystemtrue. The manipulation of the argument upload leads to unrestricted upload. This vulnerability was named CVE-2023-3836. 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.		
CVE-2023-3852	OpenRapid RapidCMS up to 1.3.1 /admin/upload.php file unrestricted upload	A vulnerability was found in OpenRapid RapidCMS up to 1.3.1. It has been declared as critical. This vulnerability affects unknown code of the file /admin/upload.php. The manipulation of the argument file leads to unrestricted upload. This vulnerability was named CVE-2023-3852. The attack can be initiated remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue.	Protected by custom rules	No

HTTP Request Smuggling Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-30589	Node.js up to 20.2.0 HTTP Module header request smuggling	A vulnerability which was classified as critical has been found in Node.js up to 20.2.0. This issue affects some unknown processing of the component HTTP Module. The manipulation of the argument header leads to http request smuggling. The identification of this vulnerability is CVE-2023-30589. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as HTTP Request Smuggling Attack

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-3490	fossbilling up to 0.5.2 sql injection	A vulnerability classified as critical has been found in fossbilling up to 0.5.2. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-3490. 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-2023-3502	SourceCodester Shopping Website 1.0 search-result.php product sql injection	A vulnerability which was classified as critical was found in SourceCodester Shopping Website 1.0. Affected is an unknown function of the file search-result.php. The manipulation of the argument product leads to sql injection. This vulnerability is traded as CVE-2023-3502. 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-2023-36813	Kanboard up to 1.2.30 PicoDB sql injection (GHSA-9gvq-78jp-jxcx)	A vulnerability classified as critical was found in Kanboard up to 1.2.30. This vulnerability affects unknown code of the component PicoDB. The manipulation leads to sql injection. This vulnerability was named CVE-2023-36813. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2023-36968	Food Ordering System 1.0 ID sql injection	A vulnerability was found in Food Ordering System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation of the argument ID leads to sql injection. This vulnerability is known as CVE-2023-36968. 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-2023-36189	LangChain 0.0.64 SQLDatabaseChain sql injection (Issue 5923)	A vulnerability was found in LangChain 0.0.64. It has been rated as critical. Affected by this issue is some unknown functionality of the component SQLDatabaseChain. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-36189. The attack may be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2023-3534	SourceCodester Shopping Website 1.0 check_availability.php email sql injection	A vulnerability was found in SourceCodester Shopping Website 1.0. It has been classified as critical. Affected is an unknown function of the file check_availability.php. The manipulation of the argument email leads to sql injection. This vulnerability is traded	Protected by core rules	Detected by scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		as CVE-2023-3534. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2023-37270	Piwigo up to 13.7.x Login sql injection (GHSA-934w-qj9p-3qcx)	A vulnerability was found in Piwigo up to 13.7.x. It has been declared as critical. This vulnerability affects unknown code of the component Login. The manipulation leads to sql injection. This vulnerability was named CVE-2023-37270. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2023-33664	ai-dev aicombinationsonfly up to 0.3.0 on PrestaShop /includes/ajax.php sql injection	A vulnerability which was classified as critical was found in ai-dev aicombinationsonfly up to 0.3.0 on PrestaShop. Affected is an unknown function of the file /includes/ajax.php. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-33664. 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-2023-27845	lekerawen_ocs up to 1.4.0 on PrestaShop resetCheckoutSessionData sql injection	A vulnerability was found in lekerawen_ocs up to 1.4.0 on PrestaShop and classified as critical. Affected by this issue is the function KerawenHelper::setCartOperationInfo/KerawenHelper::resetCheckoutSessionData. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-27845. 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-2023-2493	All In One Redirection Plugin up to 2.1.x on WordPress sql injection	A vulnerability was found in All In One Redirection Plugin up to 2.1.x on WordPress. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-2493. 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-2023-37627	codeprojects Online Restaurant Management System 1.0 Admin Panel sql injection	A vulnerability was found in codeprojects Online Restaurant Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the component Admin Panel. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-37627. 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-2023-37628	Online Piggery Management System	A vulnerability has been found in Online Piggery	Protected by core rules	Detected by scanner as SQL

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	1.0 sql injection	Management System 1.0 and classified as critical. This vulnerability affects unknown code. The manipulation leads to sql injection. This vulnerability was named CVE-2023-37628. Access to the local network is required for this attack to succeed. There is no exploit available.		Injection attack
CVE-2023-30151	Boxtal Module 3.1.10 on PrestaShop GET Parameter key sql injection	A vulnerability classified as critical has been found in Boxtal Module 3.1.10 on PrestaShop. Affected is an unknown function of the component GET Parameter Handler. The manipulation of the argument key leads to sql injection. This vulnerability is traded as CVE-2023-30151. 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-2023-3673	pimcore up to 10.5.23 sql injection	A vulnerability classified as critical has been found in pimcore up to 10.5.23. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-3673. 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-2023-37472	Knowage Server up to 8.1.7 HQL Query listDocument_ _countBIObjects_ _label_ sql injection (GHSA-2j3f-f696-7rgj)	A vulnerability was found in Knowage Server up to 8.1.7 and classified as critical. Affected by this issue is the function _countBIObjects_ of the file _/knowage/restful-services/2.0/documents/listDocument_ of the component HQL Query Handler. The manipulation of the argument _label_ leads to sql injection. This vulnerability is handled as CVE-2023-37472. 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-2023-3695	Campcodes Beauty Salon Management System 1.0 add-product.php category sql injection	A vulnerability classified as critical has been found in Campcodes Beauty Salon Management System 1.0. Affected is an unknown function of the file add-product.php. The manipulation of the argument category leads to sql injection. This vulnerability is traded as CVE-2023-3695. 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-2023-3694	SourceCodester House Rental and Property Listing 1.0 index.php keywords/location sql injection	A vulnerability which was classified as critical has been found in SourceCodester House Rental and Property Listing 1.0. This issue affects some unknown processing of the file index.php. The manipulation of the argument keywords/location leads to sql injection. The identification of this vulnerability is CVE-2023-3694. The attack may be initiated remotely.	Protected by core rules	Detected by scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Furthermore there is an exploit available.		
CVE-2023-3693	SourceCodester Life Insurance Management System 1.0 login.php username sql injection	A vulnerability classified as critical was found in SourceCodester Life Insurance Management System 1.0. This vulnerability affects unknown code of the file login.php. The manipulation of the argument username leads to sql injection. This vulnerability was named CVE-2023-3693. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2021-37522	HKing2802 Locke-Bot 2.0.2 String /src/db.js sql injection	A vulnerability was found in HKing2802 Locke-Bot 2.0.2 and classified as critical. This issue affects some unknown processing of the file /src/db.js of the component String Handler. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2021-37522. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2023-30153	Payplug Module up to 3.7.1 on PrestaShop ajax.php sql injection	A vulnerability was found in Payplug Module up to 3.7.1 on PrestaShop. It has been rated as critical. This issue affects some unknown processing of the file ajax.php. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-30153. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2023-2843	MultiParcels Shipping for WooCommerce Plugin up to 1.14.12 on WordPress id sql injection	A vulnerability was found in MultiParcels Shipping for WooCommerce Plugin up to 1.14.12 on WordPress. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2023-2843. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2023-31753	eNdonesia 8.7 diskusi.php rid sql injection	A vulnerability which was classified as critical has been found in eNdonesia 8.7. Affected by this issue is some unknown functionality of the file diskusi.php. The manipulation of the argument rid leads to sql injection. This vulnerability is handled as CVE-2023-31753. 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-2023-3799	IBOS OA 4.5.5 Delete Category ?r=article/category/del sql injection	A vulnerability was found in IBOS OA 4.5.5 and classified as critical. This issue affects some unknown processing of the file rarticle/category/del of the component Delete Category Handler. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-3799. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure	Protected by core rules	Detected by scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		but did not respond in any way.		
CVE-2023-3808	Hospital Management System 1.0 patientforgotpassword.php sql injection	A vulnerability was found in Hospital Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file patientforgotpassword.php. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-3808. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2023-3811	Hospital Management System 1.0 patientprofile.php address sql injection	A vulnerability was found in Hospital Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file patientprofile.php. The manipulation of the argument address leads to sql injection. The identification of this vulnerability is CVE-2023-3811. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2023-3807	Campcodes Beauty Salon Management System 1.0 edit_product.php id sql injection	A vulnerability has been found in Campcodes Beauty Salon Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file edit_product.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-3807. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2023-3809	Hospital Management System 1.0 patient.php address sql injection	A vulnerability was found in Hospital Management System 1.0. It has been classified as critical. This affects an unknown part of the file patient.php. The manipulation of the argument address leads to sql injection. This vulnerability is uniquely identified as CVE-2023-3809. 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-2023-3810	Hospital Management System 1.0 patientappointment.php sql injection	A vulnerability was found in Hospital Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file patientappointment.php. The manipulation of the argument loginid/password/mobileno/appointmentdate/appointmenttime/patiente/dob/doct/city leads to sql injection. This vulnerability was named CVE-2023-3810. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2023-3820	pimcore up to 10.6.3 sql injection	A vulnerability classified as critical was found in pimcore up to 10.6.3. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-3820. Access to the local network is required for this attack.	Protected by core rules	Detected by scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-3839	DedeBIZ 6.2.10 /admin/sys_sql_query.php sqlquery sql injection	A vulnerability which was classified as problematic has been found in DedeBIZ 6.2.10. Affected by this issue is some unknown functionality of the file /admin/sys_sql_query.php . The manipulation of the argument sqlquery leads to sql injection. This vulnerability is handled as CVE-2023-3839. The attack may be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2023-3878	Campcodes Beauty Salon Management System 1.0 /admin/about-us.php pagedes sql injection	A vulnerability was found in Campcodes Beauty Salon Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/about-us.php. The manipulation of the argument pagedes leads to sql injection. This vulnerability was named CVE-2023-3878. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2023-3881	Campcodes Beauty Salon Management System 1.0 forgot-password.php contactno sql injection	A vulnerability classified as critical was found in Campcodes Beauty Salon Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/forgot-password.php. The manipulation of the argument contactno leads to sql injection. This vulnerability is known as CVE-2023-3881. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2023-3874	Campcodes Beauty Salon Management System 1.0 /admin/admin-profile.php adminname sql injection	A vulnerability which was classified as critical was found in Campcodes Beauty Salon Management System 1.0. Affected is an unknown function of the file /admin/admin-profile.php. The manipulation of the argument adminname leads to sql injection. This vulnerability is traded as CVE-2023-3874. 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-2023-3873	Campcodes Beauty Salon Management System 1.0 /admin/index.php username sql injection	A vulnerability which was classified as critical has been found in Campcodes Beauty Salon Management System 1.0. This issue affects some unknown processing of the file /admin/index.php. The manipulation of the argument username leads to sql injection. The identification of this vulnerability is CVE-2023-3873. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2023-3875	Campcodes Beauty Salon Management System 0.1.0	A vulnerability has been found in Campcodes Beauty Salon Management	Protected by core rules	Detected by scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	/admin/del_feedback.php id sql injection	System 0.1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/del_feedback.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-3875. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2023-3880	Campcodes Beauty Salon Management System 1.0 /admin/del_service.php editid sql injection	A vulnerability classified as critical has been found in Campcodes Beauty Salon Management System 1.0. Affected is an unknown function of the file /admin/del_service.php. The manipulation of the argument editid leads to sql injection. This vulnerability is traded as CVE-2023-3880. 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-2023-3882	Campcodes Beauty Salon Management System 1.0 edit-accepted-appointment.php contactno sql injection	A vulnerability which was classified as critical has been found in Campcodes Beauty Salon Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/edit-accepted-appointment.php. The manipulation of the argument contactno leads to sql injection. This vulnerability is handled as CVE-2023-3882. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2023-3877	Campcodes Beauty Salon Management System 1.0 /admin/add-services.php cost sql injection	A vulnerability was found in Campcodes Beauty Salon Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/add-services.php. The manipulation of the argument cost leads to sql injection. This vulnerability is uniquely identified as CVE-2023-3877. 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-2023-3879	Campcodes Beauty Salon Management System 1.0 /admin/del_category.php id sql injection	A vulnerability was found in Campcodes Beauty Salon Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/del_category.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2023-3879. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2023-3871	Campcodes Beauty Salon Management System 1.0 /admin/edit_category.php id sql injection	A vulnerability classified as critical has been found in Campcodes Beauty Salon Management System 1.0. This affects an unknown part of the file /admin/edit_category.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-3871. It is	Protected by core rules	Detected by scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2023-3872	Campcodes Beauty Salon Management System 1.0 /admin/edit-services.php editid sql injection	A vulnerability classified as critical was found in Campcodes Beauty Salon Management System 1.0. This vulnerability affects unknown code of the file /admin/edit-services.php. The manipulation of the argument editid leads to sql injection. This vulnerability was named CVE-2023-3872. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2023-3876	Campcodes Beauty Salon Management System 1.0 search-appointment.php searchdata sql injection	A vulnerability was found in Campcodes Beauty Salon Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/search-appointment.php. The manipulation of the argument searchdata leads to sql injection. This vulnerability is handled as CVE-2023-3876. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2023-2761	User Activity Log Plugin up to 1.6.2 on WordPress txtsearch sql injection	A vulnerability was found in User Activity Log Plugin up to 1.6.2 on WordPress and classified as critical. Affected by this issue is some unknown functionality. The manipulation of the argument txtsearch leads to sql injection. This vulnerability is handled as CVE-2023-2761. 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

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-36477	XWiki Platform CKEditor cross-site scripting (GHSA-793w-g325-hrw2)	A vulnerability was found in XWiki Platform and classified as problematic. Affected by this issue is some unknown functionality of the component CKEditor. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-36477. 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-2023-33276	Gira KNX-IP-Router 3.1.3683.0/3.3.8.0 Web Interface cross-site scripting (SYSS-2023-016)	A vulnerability which was classified as problematic was found in Gira KNX-IP-Router 3.1.3683.0/3.3.8.0. This affects an unknown part of the component Web Interface. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-33276. 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-2023-34840	angular-ui-notification 0.1.0/0.2.0/0.3.6 cross-site scripting	A vulnerability was found in angular-ui-notification 0.1.0/0.2.0/0.3.6. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-34840. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-2320	CF7 Google Sheets Connector Plugin up to 5.0.1 on WordPress cross-site scripting	A vulnerability was found in CF7 Google Sheets Connector Plugin and cf7-google-sheets-connector-pro Plugin up to 5.0.1 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-2023-2320. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2020-22152	Fuel CMS 1.4.6 Pages page title/meta description/meta keywords cross-site scripting (Issue 552)	A vulnerability classified as problematic has been found in Fuel CMS 1.4.6. This affects an unknown part of the component Pages Handler. The manipulation of the argument page title/meta description/meta keywords leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2020-22152. 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-2023-36816	2FA up to 4.0.2 Account service cross-site scripting (GHSA-cwhq-2mcq-pp9q)	A vulnerability classified as problematic was found in 2FA up to 4.0.2. Affected by this vulnerability is an unknown functionality of the component Account Handler. The manipulation of the argument service leads to cross-site	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		scripting. This vulnerability is known as CVE-2023-36816. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-2324	Elementor Forms Google Sheet Connector Plugin up to 1.0.7 on WordPress Attribute cross-site scripting	A vulnerability was found in Elementor Forms Google Sheet Connector Plugin and gsheetconnector-for-elementor-forms-pro Plugin up to 1.0.7 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-2324. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-4623	ND Shortcodes Plugin up to 6.x on WordPress Shortcode Attribute cross-site scripting	A vulnerability classified as problematic has been found in ND Shortcodes Plugin up to 6.x 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-2022-4623. 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-2023-36223	mlogclub bbs-go up to 3.5.5 settings announcements cross-site scripting (Issue 208)	A vulnerability classified as problematic was found in mlogclub bbs-go up to 3.5.5. This vulnerability affects the function settings. The manipulation of the argument announcements leads to cross-site scripting. This vulnerability was named CVE-2023-36223. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-36222	mlogclub bbs-go up to 3.5.5 article comment cross-site scripting (Issue 206)	A vulnerability classified as problematic has been found in mlogclub bbs-go up to 3.5.5. This affects the function article. The manipulation of the argument comment leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-36222. 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-2023-33335	Sophos iView on Windows grpname cross-site scripting	A vulnerability classified as problematic has been found in Sophos iView on Windows. This affects an unknown part. The manipulation of the argument grpname leads to cross-site scripting. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is uniquely identified as CVE-2023-33335. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2020-23452	Selenium Grid 3.141.59 /grid/console hub cross-site scripting (Issue 8259)	A vulnerability was found in Selenium Grid 3.141.59. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /grid/console. The manipulation of the argument hub leads to cross-site scripting. This vulnerability is known as CVE-2020-23452. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-30319	wliang6 ChatEngine fded8e710ad59f816867ad47d7fc4862f6502f3e LoginServlet.java username cross-site scripting	A vulnerability was found in wliang6 ChatEngine fded8e710ad59f816867ad47d7fc4862f6502f3e and classified as problematic. This issue affects some unknown processing of the file /src/chatbotapp/LoginServlet.java. The manipulation of the argument username leads to cross-site scripting. The identification of this vulnerability is CVE-2023-30319. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-34654	taoCMS up to 3.0.2 cross-site scripting	A vulnerability was found in taoCMS up to 3.0.2. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-34654. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-36828	Statamic up to 4.9.x SVG Tag cross-site scripting (GHSA-6r5g-cq4q-327g)	A vulnerability was found in Statamic up to 4.9.x. It has been classified as problematic. Affected is an unknown function of the component SVG Tag Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-36828. 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-2023-30320	wliang6 ChatEngine fded8e710ad59f816867ad47d7fc4862f6502f3e chatWindow.java textMessage cross-site scripting	A vulnerability which was classified as problematic has been found in wliang6 ChatEngine fded8e710ad59f816867ad47d7fc4862f6502f3e. Affected by this issue is some unknown functionality of the file /src/chatbotapp/chatWindow.java. The manipulation of the argument textMessage leads to cross-site scripting. This vulnerability is handled as CVE-2023-30320. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-3344	Auto Location for WP Job Manager via Google Plugin cross-site scripting	A vulnerability was found in Auto Location for WP Job Manager via Google Plugin up to 1.0 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-2023-3344. The attack can be initiated remotely. There	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		is no exploit available.		
CVE-2023-3248	All-in-one Floating Contact Form Plugin up to 2.1.1 on WordPress Setting cross-site scripting	A vulnerability classified as problematic has been found in All-in-one Floating Contact Form Plugin up to 2.1.1 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-2023-3248. 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-2023-24496	Milesight VPN up to 2.0.2 requestHandlers.js detail_device name cross-site scripting (TALOS-2023-1704)	A vulnerability classified as problematic has been found in Milesight VPN up to 2.0.2. Affected is the function detail_device of the file requestHandlers.js. The manipulation of the argument name leads to basic cross-site scripting. This vulnerability is traded as CVE-2023-24496. 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-2023-37124	SeaCms 12.1 Setup Module cross-site scripting (Issue 24)	A vulnerability was found in SeaCms 12.1. It has been classified as problematic. This affects an unknown part of the component Setup Module. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-37124. 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-2023-36995	TravianZ up to 8.3.4 cross-site scripting	A vulnerability has been found in TravianZ up to 8.3.4 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-2023-36995. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-37132	EyouCMS 1.6.3 Custom Variables Module cross-site scripting (Issue 45)	A vulnerability was found in EyouCMS 1.6.3. It has been declared as problematic. This vulnerability affects unknown code of the component Custom Variables Module. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-37132. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-3521	fossbilling up to 0.5.3 cross-site scripting	A vulnerability was found in fossbilling up to 0.5.3. 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-2023-3521. 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-2023-36970	CMS Made Simple 2.2.17 File Upload cross-site scripting	A vulnerability was found in CMS Made Simple 2.2.17 and classified as problematic. Affected by	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		this issue is some unknown functionality of the component File Upload Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-36970. The attack may be launched remotely. There is no exploit available.		
CVE-2023-36809	Kiwi TCMS up to 12.4 tree_view_html cross-site scripting (GHSA-jpgw-2r9m-8qfw)	A vulnerability which was classified as problematic has been found in Kiwi TCMS up to 12.4. Affected by this issue is the function tree_view_html. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-36809. 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-2023-24497	Milesight VPN up to 2.0.2 HTTP Request requestHandlers.js detail_device remote_subnet cross-site scripting (TALOS-2023-1704)	A vulnerability was found in Milesight VPN up to 2.0.2. It has been classified as problematic. Affected is the function detail_device of the file requestHandlers.js of the component HTTP Request Handler. The manipulation of the argument remote_subnet leads to cross-site scripting. This vulnerability is traded as CVE-2023-24497. 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-2023-37125	SeaCms 12.1 Management Custom Label Module cross-site scripting (Issue 25)	A vulnerability was found in SeaCms 12.1 and classified as problematic. Affected by this issue is some unknown functionality of the component Management Custom Label Module. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-37125. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-2309	wpForo Forum Plugin up to 2.1.8 on WordPress wpforo_debug cross-site scripting	A vulnerability was found in wpForo Forum Plugin up to 2.1.8 on WordPress. It has been rated as problematic. Affected by this issue is the function wpforo_debug. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-2309. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-27225	User Registration & Login and User Management System with Admin Panel cross-site scripting	A vulnerability was found in User Registration & Login and User Management System with Admin Panel and classified as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument first name/last name leads to cross-site scripting. This vulnerability is handled as CVE-2023-27225. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-37135	EyouCMS 1.6.3 Image Upload Module cross-site scripting (Issue 48)	A vulnerability classified as problematic has been found in EyouCMS 1.6.3. This affects an unknown part of the component Image Upload Module. The manipulation leads to	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross-site scripting. This vulnerability is uniquely identified as CVE-2023-37135. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2023-37136	EyouCMS 1.6.3 Basic Website Information Module cross-site scripting (Issue 49)	A vulnerability which was classified as problematic has been found in EyouCMS 1.6.3. This issue affects some unknown processing of the component Basic Website Information Module. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-37136. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-37133	EyouCMS 1.6.3 Column Management Module cross-site scripting (Issue 46)	A vulnerability which was classified as problematic was found in EyouCMS 1.6.3. Affected is an unknown function of the component Column Management Module. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-37133. 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-2023-37134	EyouCMS 1.6.3 Information Module cross-site scripting (Issue 47)	A vulnerability was found in EyouCMS 1.6.3. It has been classified as problematic. This affects an unknown part of the component Information Module. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-37134. 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-2023-37122	Bagecms 3.1.0 Custom Settings Module cross-site scripting	A vulnerability classified as problematic was found in Bagecms 3.1.0. This vulnerability affects unknown code of the component Custom Settings Module. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-37122. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-30321	wliang6 ChatEngine fded8e710ad59f816867ad47d7fc4862f6502f3e LoginServlet.java textMessage cross-site scripting	A vulnerability was found in wliang6 ChatEngine fded8e710ad59f816867ad47d7fc4862f6502f3e. It has been rated as problematic. This issue affects some unknown processing of the file /src/chatbotapp/LoginServlet.java. The manipulation of the argument textMessage leads to cross-site scripting. The identification of this vulnerability is CVE-2023-30321. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-3531	nilsteampassnet teampass up to 3.0.9 cross-site scripting	A vulnerability classified as problematic has been found in nilsteampassnet teampass up to 3.0.9. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-3531. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		It is recommended to upgrade the affected component.		
CVE-2023-3532	outline up to 0.70.0 cross-site scripting	A vulnerability classified as problematic was found in outline up to 0.70.0. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-3532. 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-2023-29998	Gis3W g3w-suite 3.5 Content Editor description cross-site scripting	A vulnerability was found in Gis3W g3w-suite 3.5. It has been classified as problematic. Affected is an unknown function of the component Content Editor. The manipulation of the argument description leads to cross-site scripting. This vulnerability is traded as CVE-2023-29998. 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-2023-3418	Querlo Chatbot Plugin up to 1.2.4 on WordPress cross-site scripting	A vulnerability was found in Querlo Chatbot Plugin up to 1.2.4 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-2023-3418. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-3118	Export All URLs Plugin up to 4.5 on WordPress cross-site scripting	A vulnerability has been found in Export All URLs Plugin up to 4.5 on WordPress and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-3118. 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-2023-3129	URL Shortify Plugin up to 1.6.x on WordPress Setting cross-site scripting	A vulnerability was found in URL Shortify Plugin up to 1.6.x 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-2023-3129. 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-2023-2964	Simple Iframe Plugin up to 1.1.x on WordPress Block Attribute cross-site scripting	A vulnerability which was classified as problematic has been found in Simple Iframe Plugin up to 1.1.x on WordPress. Affected by this issue is some unknown functionality of the component Block Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		handled as CVE-2023-2964. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-3175	AI ChatBot Plugin up to 4.6.0 on WordPress Setting cross-site scripting	A vulnerability classified as problematic has been found in AI ChatBot Plugin up to 4.6.0 on WordPress. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-3175. 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-2023-1780	Companion Sitemap Generator Plugin up to 4.5.2 on WordPress cross-site scripting	A vulnerability was found in Companion Sitemap Generator Plugin up to 4.5.2 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-2023-1780. 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-2023-2967	TinyMCE Custom Styles Plugin up to 1.1.3 on WordPress Setting cross-site scripting	A vulnerability which was classified as problematic was found in TinyMCE Custom Styles Plugin up to 1.1.3 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-2023-2967. 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-2023-1119	WP-Optimize Plugin/SrbTransLatin Plugin on WordPress HTML Character cross-site scripting	A vulnerability has been found in WP-Optimize Plugin and SrbTransLatin Plugin on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality of the component HTML Character Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-1119. 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-2023-2635	Call Now Accessibility Button Plugin up to 1.0 on WordPress Setting cross-site scripting	A vulnerability was found in Call Now Accessibility Button Plugin up to 1.0 on WordPress. It has been declared as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-2635.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-36376	PHPGurukul Hostel Management System 2.1 Add Course cross-site scripting	A vulnerability which was classified as problematic has been found in PHPGurukul Hostel Management System 2.1. Affected by this issue is some unknown functionality of the component Add Course. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-36376. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-2028	Call Now Accessibility Button Plugin up to 1.0 on WordPress Setting cross-site scripting	A vulnerability was found in Call Now Accessibility Button Plugin up to 1.0 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-2023-2028. 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-2023-36375	Hostel Management System 2.1 Room Details Page cross-site scripting	A vulnerability has been found in Hostel Management System 2.1 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Room Details Page. The manipulation of the argument Guardian name/Guardian relation/complimentary address/city/permanent address/city leads to cross-site scripting. This vulnerability is known as CVE-2023-36375. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-36939	Hostel Management System 2.1 search booking cross-site scripting	A vulnerability classified as problematic has been found in Hostel Management System 2.1. This affects an unknown part. The manipulation of the argument search booking leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-36939. 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-2023-36940	PHPGurukul Online Fire Reporting System 1.2 search cross-site scripting	A vulnerability classified as problematic was found in PHPGurukul Online Fire Reporting System 1.2. This vulnerability affects unknown code. The manipulation of the argument search leads to cross-site scripting. This vulnerability was named CVE-2023-36940. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-36936	PHPGurukul Online Security Guards Hiring System 1.0 search booking cross-site scripting	A vulnerability which was classified as problematic has been found in PHPGurukul Online Security Guards Hiring	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		System 1.0. This issue affects some unknown processing. The manipulation of the argument search booking leads to cross-site scripting. The identification of this vulnerability is CVE-2023-36936. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-37153	KodExplorer 4.51 Light App Creation Description cross-site scripting	A vulnerability classified as problematic was found in KodExplorer 4.51. Affected by this vulnerability is an unknown functionality of the component Light App Creation. The manipulation of the argument Description leads to cross-site scripting. This vulnerability is known as CVE-2023-37153. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-3565	nilsteampassnet teampass up to 3.0.9 cross-site scripting	A vulnerability was found in nilsteampassnet teampass up to 3.0.9. 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-2023-3565. 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-2023-37191	Issabel PBX 4.0.0-6 Group/Description cross-site scripting	A vulnerability was found in Issabel PBX 4.0.0-6. It has been classified as problematic. Affected is an unknown function. The manipulation of the argument Group/Description leads to cross-site scripting. This vulnerability is traded as CVE-2023-37191. 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-2023-37190	Issabel PBX 4.0.0-6 New Virtual Fax Virtual Fax Name/Caller ID Name cross-site scripting	A vulnerability was found in Issabel PBX 4.0.0-6. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component New Virtual Fax. The manipulation of the argument Virtual Fax Name/Caller ID Name leads to cross-site scripting. This vulnerability is known as CVE-2023-37190. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-37189	Issabel PBX 4 Create New Rate Module index.php Name/Prefix cross-site scripting	A vulnerability classified as problematic was found in Issabel PBX 4. This vulnerability affects unknown code of the file index.phpmenubilling_rates of the component Create New Rate Module. The manipulation of the argument Name/Prefix leads to cross-site scripting. This vulnerability was named CVE-2023-37189. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-3130	Short URL Plugin up to 1.6.4 on WordPress	A vulnerability classified as problematic was found	Protected by core rules	Detected by scanner as Cross-

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	cross-site scripting	in Short URL Plugin up to 1.6.4 on WordPress. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-3130. The attack can be initiated remotely. There is no exploit available.		Site Scripting attack
CVE-2023-3292	Grid Kit Premium Plugin up to 2.1.x on WordPress cross-site scripting	A vulnerability which was classified as problematic has been found in Grid Kit Premium Plugin up to 2.1.x on WordPress. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-3292. 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-2023-0602	Twittee Text Tweet Plugin up to 1.0.8 on WordPress cross-site scripting	A vulnerability was found in Twittee Text Tweet Plugin up to 1.0.8 on WordPress. 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-2023-0602. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-37630	Online Piggery Management System 1.0 manage-breed.php cross-site scripting	A vulnerability was found in Online Piggery Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file manage-breed.php. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-37630. 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-2023-37787	Geeklog 2.2.2 /admin/router.php Route cross-site scripting	A vulnerability was found in Geeklog 2.2.2. It has been rated as problematic. This issue affects some unknown processing of the file /admin/router.php. The manipulation of the argument Route leads to cross-site scripting. The identification of this vulnerability is CVE-2023-37787. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-37785	ImpressCMS up to 1.4.5 /editprofile.php smile_code cross-site scripting	A vulnerability which was classified as problematic was found in ImpressCMS up to 1.4.5. This affects an unknown part of the file /editprofile.php. The manipulation of the argument smile_code leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-37785. 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-2023-31705	Sourcecodester Task Reminder System 1.0 page cross-site scripting	A vulnerability classified as problematic has been found in Sourcecodester Task Reminder System 1.0. This affects an unknown part. The manipulation of the argument page leads to cross-site scripting.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is uniquely identified as CVE-2023-31705. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2023-37786	Geeklog 2.2.2 /admin/configuration.php cross-site scripting	A vulnerability was found in Geeklog 2.2.2. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/configuration.php. The manipulation of the argument Mail Settings[backend]/Mail Settings[host]/Mail Settings[port]/Mail Settings[auth] leads to cross-site scripting. This vulnerability was named CVE-2023-37786. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-2082	Buy Me a Coffee Plugin up to 3.6 on WordPress cross-site scripting	A vulnerability was found in Buy Me a Coffee Plugin up to 3.6 on WordPress. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-2082. 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-2023-3660	Campcodes Retro Cellphone Online Store 1.0 add_user_modal.php un cross-site scripting	A vulnerability was found in Campcodes Retro Cellphone Online Store 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/add_user_modal.php. The manipulation of the argument un leads to cross-site scripting. This vulnerability is handled as CVE-2023-3660. 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-2023-3672	plaidweb webmention.js up to 0.5.4 cross-site scripting	A vulnerability classified as problematic was found in plaidweb webmention.js up to 0.5.4. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-3672. 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-2023-2507	CleverTap Cordova Plugin 2.6.2 Deeplink cross-site scripting	A vulnerability was found in CleverTap Cordova Plugin 2.6.2 and classified as problematic. This issue affects some unknown processing of the component Deeplink Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-2507. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-38350	PNP4Nagios up to 0.6.26 Basket API cross-site scripting	A vulnerability was found in PNP4Nagios up to 0.6.26. It has been classified as problematic. Affected is an unknown function of the component Basket API. The manipulation leads to cross-site scripting. This vulnerability is traded	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		as CVE-2023-38350. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2023-3691	layui up to v2.8.0-rc.16 HTML Attribute title cross-site scripting (I7HDXZ)	A vulnerability which was classified as problematic was found in layui up to v2.8.0-rc.16. This affects an unknown part of the component HTML Attribute Handler. The manipulation of the argument title leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-3691. 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-2023-3681	Campcodes Retro Cellphone Online Store 1.0 modal_add_product.php description cross-site scripting	A vulnerability classified as problematic was found in Campcodes Retro Cellphone Online Store 1.0. This vulnerability affects unknown code of the file /admin/modal_add_product.php. The manipulation of the argument description leads to cross-site scripting. This vulnerability was named CVE-2023-3681. 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-2023-31852	Cudy LT400 1.13.4 config iface cross-site scripting	A vulnerability was found in Cudy LT400 1.13.4. It has been classified as problematic. Affected is an unknown function of the file cgi-bin/luci/admin/network/wireless/config. The manipulation of the argument iface leads to cross-site scripting. This vulnerability is traded as CVE-2023-31852. 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-2023-31851	Cudy LT400 1.13.4 status iface cross-site scripting	A vulnerability classified as problematic was found in Cudy LT400 1.13.4. This vulnerability affects unknown code of the file /cgi-bin/luci/admin/network/wireless/status. The manipulation of the argument iface leads to cross-site scripting. This vulnerability was named CVE-2023-31851. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-31853	Cudy LT400 1.13.4 bandwidth icon cross-site scripting	A vulnerability which was classified as problematic has been found in Cudy LT400 1.13.4. This issue affects some unknown processing of the file /cgi-bin/luci/admin/network/bandwidth. The manipulation of the argument icon leads to cross-site scripting. The identification of this vulnerability is CVE-2023-31853. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-36656	Jaegertracing Jaeger UI up to 1.30.x KeyValuesTable Component cross-site scripting (GHSA-vv24-rm95-q56r)	A vulnerability classified as problematic has been found in Jaegertracing Jaeger UI up to 1.30.x. This affects an unknown part of the component KeyValuesTable Component. The manipulation leads to	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross-site scripting. This vulnerability is uniquely identified as CVE-2023-36656. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-3182	Membership Plugin up to 3.2.2 on WordPress cross-site scripting	A vulnerability classified as problematic was found in Membership Plugin up to 3.2.2 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-3182. 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-2023-1893	Login Configurator Plugin up to 2.1 on WordPress URL Parameter cross-site scripting	A vulnerability was found in Login Configurator Plugin up to 2.1 on WordPress. It has been classified as problematic. This affects an unknown part of the component URL Parameter Handler. The manipulation of the argument URL leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-1893. 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-2023-0439	NEX-Forms Plugin up to 8.4.3 on WordPress cross-site scripting	A vulnerability was found in NEX-Forms Plugin up to 8.4.3 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-2023-0439. 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-2023-0604	WP Food Manager Plugin up to 1.0.3 on WordPress cross-site scripting	A vulnerability classified as problematic was found in WP Food Manager Plugin up to 1.0.3 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-0604. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-3671	MultiParcels Shipping for WooCommerce Plugin up to 1.15 on WordPress cross-site scripting	A vulnerability classified as problematic has been found in MultiParcels Shipping for WooCommerce Plugin up to 1.15 on WordPress. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-3671. 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-2023-3815	y_project RuoYi up to 4.7.7 File Upload uploadFilesPath originalFilenames cross-site scripting	A vulnerability which was classified as problematic has been found in y_project RuoYi up to 4.7.7. Affected by this	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		issue is the function uploadFilesPath of the component File Upload. The manipulation of the argument originalFilenames leads to cross-site scripting. This vulnerability is handled as CVE-2023-3815. The attack may be launched remotely. There is no exploit available.		
CVE-2023-3785	PaulPrinting CMS 2018 firstname/lastname/address/city/state cross-site scripting	A vulnerability was found in PaulPrinting CMS 2018. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument firstname/lastname/address/city/state leads to cross-site scripting. This vulnerability is handled as CVE-2023-3785. 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-2023-3790	Boom CMS 8.0.7 assets-manager add title/description cross-site scripting	A vulnerability has been found in Boom CMS 8.0.7 and classified as problematic. Affected by this vulnerability is the function add of the component assets-manager. The manipulation of the argument title/description leads to cross-site scripting. This vulnerability is known as CVE-2023-3790. 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-2023-3783	Webile 1.0.1 HTTP POST Request new_file_name/c cross-site scripting	A vulnerability was found in Webile 1.0.1. It has been classified as problematic. Affected is an unknown function of the component HTTP POST Request Handler. The manipulation of the argument new_file_name/c leads to cross-site scripting. This vulnerability is traded as CVE-2023-3783. 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-2023-3787	Codecanyon Tiva Events Calender 1.4 name cross-site scripting	A vulnerability classified as problematic was found in Codecanyon Tiva Events Calender 1.4. This vulnerability affects unknown code. The manipulation of the argument name leads to cross-site scripting. This vulnerability was named CVE-2023-3787. The attack can be initiated remotely. Furthermore there is an exploit available. It is recommended to apply the suggested workaround.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-3788	ActiveITzone Active Super Shop CMS 2.5 Manage Details Page name/phone/address cross-site scripting	A vulnerability which was classified as problematic has been found in ActiveITzone Active Super Shop CMS 2.5. This issue affects some unknown processing of the component Manage Details Page. The manipulation of the argument name/phone/address leads to cross-site scripting. The identification of this vulnerability is CVE-2023-	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		3788. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2023-3784	Dooblou WiFi File Explorer 1.13.3 search/order/download /mode cross-site scripting	A vulnerability was found in Dooblou WiFi File Explorer 1.13.3. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument search/order/download/mode leads to cross-site scripting. This vulnerability is known as CVE-2023-3784. 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-2023-37600	Office Suite Premium Version 10.9.1.42602 /api id cross-site scripting (ID 173143)	A vulnerability was found in Office Suite Premium Version 10.9.1.42602. It has been declared as problematic. This vulnerability affects unknown code of the file /apipathprofile. The manipulation of the argument id leads to cross-site scripting. This vulnerability was named CVE-2023-37600. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-38617	Office Suite Premium 10.9.1.42602 /api filter cross-site scripting (ID 173143)	A vulnerability was found in Office Suite Premium 10.9.1.42602. It has been rated as problematic. This issue affects some unknown processing of the file /apipathfiles. The manipulation of the argument filter leads to cross-site scripting. The identification of this vulnerability is CVE-2023-38617. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-37164	Diafan CMS 6.0 cat_id cross-site scripting (Exploit 51529 / EDB-51529)	A vulnerability was found in Diafan CMS 6.0. It has been classified as problematic. This affects an unknown part of the file /shop/moduleshop&actionsearch. The manipulation of the argument cat_id leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-37164. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-37728	Icewarp Icearp 10.2.1 cross-site scripting	A vulnerability was found in Icewarp Icearp 10.2.1 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-2023-37728. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-3789	PaulPrinting CMS 2018 Search /account/delivery s cross-site scripting	A vulnerability which was classified as problematic was found in PaulPrinting CMS 2018. Affected is an unknown function of the file /account/delivery of the component Search. The manipulation of the argument s leads to cross-site scripting. This vulnerability is traded as CVE-2023-3789. It is possible to launch the attack remotely.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Furthermore there is an exploit available.		
CVE-2023-3822	pimcore up to 10.6.3 cross-site scripting	A vulnerability which was classified as problematic was found in pimcore up to 10.6.3. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-3822. 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-2023-3821	pimcore up to 10.6.3 cross-site scripting	A vulnerability which was classified as problematic has been found in pimcore up to 10.6.3. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-3821. 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-2023-3847	mooSocial mooDating 1.2 URL /users cross-site scripting	A vulnerability classified as problematic was found in mooSocial mooDating 1.2. This vulnerability affects unknown code of the file /users of the component URL Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-3847. The attack can be initiated remotely. Furthermore there is an exploit available. We tried to contact the vendor early about the disclosure but the official mail address was not working properly.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-3845	mooSocial mooDating 1.2 URL /friends/ajax_invite cross-site scripting	A vulnerability was found in mooSocial mooDating 1.2. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /friends/ajax_invite of the component URL Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-3845. The attack may be launched remotely. Furthermore there is an exploit available. We tried to contact the vendor early about the disclosure but the official mail address was not working properly.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-3846	mooSocial mooDating 1.2 URL /pages cross-site scripting	A vulnerability classified as problematic has been found in mooSocial mooDating 1.2. This affects an unknown part of the file /pages of the component URL Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-3846. It is possible to initiate the attack remotely. Furthermore there is an exploit available. We tried to contact the vendor early about the	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		disclosure but the official mail address was not working properly.		
CVE-2023-3844	mooSocial mooDating 1.2 URL /friends cross-site scripting	A vulnerability was found in mooSocial mooDating 1.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /friends of the component URL Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-3844. The attack can be launched remotely. Furthermore there is an exploit available. We tried to contact the vendor early about the disclosure but the official mail address was not working properly.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-3838	DedeBIZ 6.2.10 /admin/vote_edit.php cross-site scripting	A vulnerability classified as problematic was found in DedeBIZ 6.2.10. Affected by this vulnerability is an unknown functionality of the file /admin/vote_edit.php. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-3838. 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 Cross-Site Scripting attack
CVE-2023-3837	DedeBIZ 6.2.10 /admin/sys_sql_query.php cross-site scripting	A vulnerability classified as problematic has been found in DedeBIZ 6.2.10. Affected is an unknown function of the file /admin/sys_sql_query.php. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-3837. It is possible to launch 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-2023-3843	mooSocial mooDating 1.2 URL /matchmakings/question cross-site scripting	A vulnerability was found in mooSocial mooDating 1.2. It has been classified as problematic. Affected is an unknown function of the file /matchmakings/question of the component URL Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-3843. It is possible to launch the attack remotely. Furthermore there is an exploit available. We tried to contact the vendor early about the disclosure but the official mail address was not working properly.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-3849	mooSocial mooDating 1.2 URL /find-a-match cross-site scripting	A vulnerability which was classified as problematic was found in mooSocial mooDating 1.2. Affected is an unknown function of the file /find-a-match of the component URL Handler. The manipulation leads to cross-site scripting. This vulnerability is traded	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		as CVE-2023-3849. It is possible to launch the attack remotely. Furthermore there is an exploit available. We tried to contact the vendor early about the disclosure but the official mail address was not working properly.		
CVE-2023-3848	mooSocial mooDating 1.2 URL /users/view cross-site scripting	A vulnerability which was classified as problematic has been found in mooSocial mooDating 1.2. This issue affects some unknown processing of the file /users/view of the component URL Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-3848. The attack may be initiated remotely. Furthermore there is an exploit available. We tried to contact the vendor early about the disclosure but the official mail address was not working properly.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-3888	Campcodes Beauty Salon Management System 1.0 /admin/admin-profile.php adminname cross-site scripting	A vulnerability was found in Campcodes Beauty Salon Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/admin-profile.php. The manipulation of the argument adminname leads to cross-site scripting. This vulnerability is handled as CVE-2023-3888. 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-2023-3883	Campcodes Beauty Salon Management System 1.0 /admin/add-category.php name cross-site scripting	A vulnerability which was classified as problematic was found in Campcodes Beauty Salon Management System 1.0. This affects an unknown part of the file /admin/add-category.php. The manipulation of the argument name leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-3883. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-3886	Campcodes Beauty Salon Management System 1.0 /admin/invoice.php inv_id cross-site scripting	A vulnerability was found in Campcodes Beauty Salon Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file /admin/invoice.php. The manipulation of the argument inv_id leads to cross-site scripting. This vulnerability is traded as CVE-2023-3886. 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-2023-3884	Campcodes Beauty Salon Management System 1.0 /admin/edit_product.php id cross-site scripting	A vulnerability has been found in Campcodes Beauty Salon Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/edit_product.php. The manipulation of the argument id leads to cross-site scripting. This vulnerability was	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		named CVE-2023-3884. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2023-3885	Campcodes Beauty Salon Management System 1.0 /admin/edit_category.php id cross-site scripting	A vulnerability was found in Campcodes Beauty Salon Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file /admin/edit_category.php. The manipulation of the argument id leads to cross-site scripting. The identification of this vulnerability is CVE-2023-3885. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-37613	Assembly Trialworks 11.4 src cross-site scripting	A vulnerability which was classified as problematic has been found in Assembly Trialworks 11.4. Affected by this issue is some unknown functionality. The manipulation of the argument src leads to cross-site scripting. This vulnerability is handled as CVE-2023-37613. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-3890	Campcodes Beauty Salon Management System 1.0 edit-accepted-appointment.php id cross-site scripting	A vulnerability classified as problematic has been found in Campcodes Beauty Salon Management System 1.0. This affects an unknown part of the file /admin/edit-accepted-appointment.php. The manipulation of the argument id leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-3890. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2023-3887	Campcodes Beauty Salon Management System 1.0 search-appointment.php searchdata cross-site scripting	A vulnerability was found in Campcodes Beauty Salon Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/search-appointment.php. The manipulation of the argument searchdata leads to cross-site scripting. This vulnerability is known as CVE-2023-3887. The attack can be launched remotely. Furthermore, there is an 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