INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

August 2023

The total zero-day vulnerabilities count for August month: 210

Command Injection	CSRF	Local File Inclusion	Malicious File Upload	SQL Injection	Cross-site Scripting	XML External Entity
20	11	16	15	48	99	1

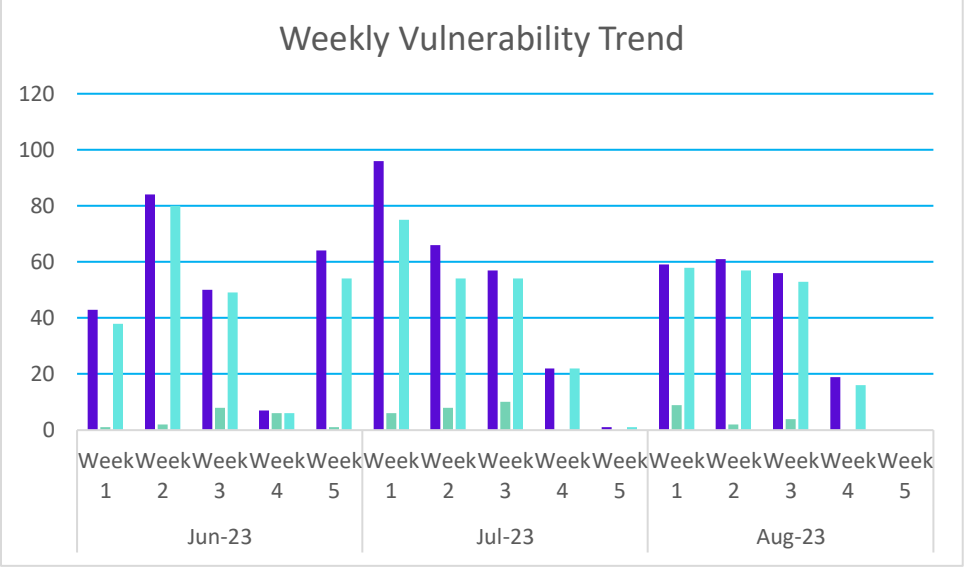
Zero-day vulnerabilities protected through core rules	195
Zero-day vulnerabilities protected through custom rules	15
Zero-day vulnerabilities for which protection cannot be done	0
Zero-day vulnerabilities found by Indusface WAS	184

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

Vulnerability Trend

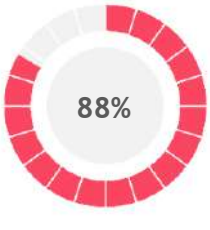
The weekly trend displays the total number of vulnerabilities discovered to the type of protection provided for the last quarter.

Weekly Vulnerability Trend



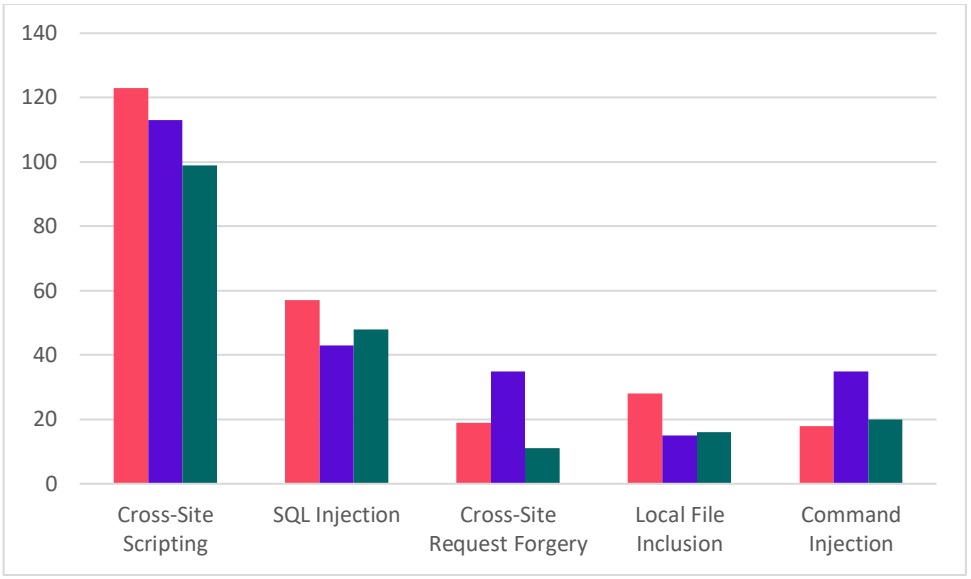
of the zero-day vulnerabilities were protected by the core rules in the last month

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



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

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-39986	raspap-webgui up to 2.8.7 activate_ovpncfg.php cfg_id command injection	A vulnerability was found in raspap-webgui up to 2.8.7 and classified as critical. This issue affects some unknown processing of the file /ajax/openvpn/activate_ovpncfg.php. The manipulation of the argument cfg_id leads to command injection. The identification of this vulnerability is CVE-2022-39986. 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-2023-34960	Chamilo LMS up to 1.11.18 wsConvertPpt command injection	A vulnerability classified as critical was found in Chamilo LMS up to 1.11.18. This vulnerability affects unknown code of the component wsConvertPpt. The manipulation leads to command injection. This vulnerability was named CVE-2023-34960. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2022-39987	RaspAP raspap-webgui up to 2.9.2 POST Parameter get_wgkey.php entity command injection	A vulnerability has been found in RaspAP raspap-webgui up to 2.9.2 and classified as critical. This vulnerability affects unknown code of the file /ajax/networking/get_wgkey.php of the component POST Parameter Handler. The manipulation of the argument entity leads to command injection. This vulnerability was named CVE-2022-39987. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-36255	Eramba Community Edition/Enterprise Edition 3.19.1 download-test-pdf path code injection	A vulnerability was found in Eramba Community Edition and Enterprise Edition 3.19.1. It has been declared as critical. This vulnerability affects unknown code of the file /settings/download-test-pdf. The manipulation of the argument path leads to code injection. This vulnerability was named CVE-2023-36255. The attack can be initiated remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-3739	Google Chrome prior 115.0.5790.98 on ChromeOS Shell Script Remote Code Execution	A vulnerability has been found in Google Chrome on ChromeOS and classified as critical. Affected by this vulnerability is an unknown functionality of the component Shell Script Handler. The manipulation leads to Remote Code Execution. This vulnerability is known as CVE-2023-3739. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-4120	Beijing Baichuo Smart S85F Management Platform up to 20230722 importhtml.php sql command injection	A vulnerability was found in Beijing Baichuo Smart S85F Management Platform up to 20230722 and classified as critical. This issue affects some unknown processing of the file importhtml.php. The manipulation of the argument sql leads to command injection. The identification of this vulnerability is CVE-2023-4120. 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-2023-38692	CloudExplorer Lite up to 1.3.0 Module Management os command injection (GHSA-7wrc-f42m-9v5w)	A vulnerability was found in CloudExplorer Lite up to 1.3.0. It has been rated as critical. Affected by this issue is some unknown functionality of the component Module Management. The manipulation leads to os command injection. This vulnerability is handled as CVE-2023-38692. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-37569	ESDS Emagic Data Center Management Suit Ping os command injection (CIVN-2023-0226)	A vulnerability was found in ESDS Emagic Data Center Management Suit. It has been rated as critical. This	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		issue affects some unknown processing of the component Ping. The manipulation leads to os command injection. The identification of this vulnerability is CVE-2023-37569. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-39001	OPNsense up to 23.6 Backup Configuration File diag_backup.php command injection	A vulnerability was found in OPNsense up to 23.6. It has been declared as critical. This vulnerability affects unknown code of the file diag_backup.php of the component Backup Configuration File Handler. The manipulation leads to command injection. This vulnerability was named CVE-2023-39001. The attack needs to be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-39008	OPNsense up to 23.6 command injection	A vulnerability has been found in OPNsense up to 23.6 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /api/cron/settings/setJob/. The manipulation leads to command injection. This vulnerability is known as CVE-2023-39008. The attack can only be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-40293	Harman Infotainment 20190525031613 D-Bus Connection Object command injection	A vulnerability was found in Harman Infotainment 20190525031613 and classified as critical. This issue affects some unknown processing of the component D-Bus Connection Object Handler. The manipulation leads to command injection. The identification of this vulnerability is CVE-2023-40293. 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-2023-38865	Comfast CF-XR11 2.7.2 POST Request /usr/bin/webmgnt sub_4143F0 timestr command injection	A vulnerability which was classified as critical was found in Comfast CF-XR11 2.7.2. This affects the function sub_4143F0 of the file /usr/bin/webmgnt of the component POST Request Handler. The manipulation of the argument timestr leads to command injection. This vulnerability is uniquely identified as CVE-2023-38865. 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-2023-38866	Comfast CF-XR11 2.7.2	A vulnerability was found in	Protected by	Detected by

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	POST Request /usr/bin/webmgnt sub_415588 display_name command injection	Comfast CF-XR11 2.7.2 and classified as critical. Affected by this issue is the function sub_415588 of the file /usr/bin/webmgnt of the component POST Request Handler. The manipulation of the argument display_name leads to command injection. This vulnerability is handled as CVE-2023-38866. The attack needs to be initiated within the local network. There is no exploit available.	core rules	scanner as command injection attack.
CVE-2023-4412	TOTOLINK EX1200L EN_V9.3.5u.6146_B20201023 setWanCfg os command injection	A vulnerability was found in TOTOLINK EX1200L EN_V9.3.5u.6146_B20201023 and classified as critical. This issue affects the function setWanCfg. The manipulation leads to os command injection. The identification of this vulnerability is CVE-2023-4412. 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-2023-4411	TOTOLINK EX1200L EN_V9.3.5u.6146_B20201023 setTracerouteCfg os command injection	A vulnerability has been found in TOTOLINK EX1200L EN_V9.3.5u.6146_B20201023 and classified as critical. This vulnerability affects the function setTracerouteCfg. The manipulation leads to os command injection. This vulnerability was named CVE-2023-4411. The attack can be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-4414	Beijing Baichuo Smart S85F Management Platform up to 20230807 /log/decodmail.php file command injection	A vulnerability was found in Beijing Baichuo Smart S85F Management Platform up to 20230807. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /log/decodmail.php. The manipulation of the argument file leads to command injection. This vulnerability is known as CVE-2023-4414. The attack can be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-4410	TOTOLINK EX1200L EN_V9.3.5u.6146_B20201023 setDiagnosisCfg os command injection	A vulnerability which was classified as critical was found in TOTOLINK EX1200L EN_V9.3.5u.6146_B20201023. This affects the function setDiagnosisCfg. The manipulation leads to os command injection.	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is uniquely identified as CVE-2023-4410. 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.		
CVE-2022-24989	TerraMaster NAS up to 4.2.30 on PHP Shell Metacharacter raidtype/diskstring os command injection	A vulnerability was found in TerraMaster NAS up to 4.2.30 on PHP. It has been rated as critical. Affected by this issue is some unknown functionality of the file api.phpmobile/createRaid of the component Shell Metacharacter Handler. The manipulation of the argument raidtype/diskstring leads to os command injection. This vulnerability is handled as CVE-2022-24989. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-39834	PbootCMS up to 3.1.x create_function command injection	A vulnerability was found in PbootCMS up to 3.1.x. It has been declared as critical. Affected by this vulnerability is the function create_function. The manipulation leads to command injection. This vulnerability is known as CVE-2023-39834. The attack can only be initiated within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-37469	IceWhaleTech CasaOS up to 0.4.3 SMB command injection (GHSL-2022-119)	A vulnerability was found in IceWhaleTech CasaOS up to 0.4.3. It has been classified as critical. Affected is an unknown function of the component SMB Handler. The manipulation leads to command injection. This vulnerability is traded as CVE-2023-37469. 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.

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-3720	Upload Media by URL Plugin up to 1.0.7 on WordPress umbu_download cross-site request forgery	A vulnerability has been found in Upload Media by URL Plugin up to 1.0.7 on WordPress and classified as problematic. Affected by this vulnerability is the function umbu_download. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-3720. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-38348	LWsystems Benno MailArchiv 2.10.1 cross-site request forgery	A vulnerability which was classified as problematic has been found in LWsystems Benno MailArchiv 2.10.1. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-38348. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-38999	OPNsense up to 23.6 System Halt API /system/halt cross-site request forgery	A vulnerability has been found in OPNsense up to 23.6 and classified as problematic. This vulnerability affects unknown code of the file /system/halt of the component System Halt API. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-38999. 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-2020-23595	yzmcms 5.6 sitemodel/add.html cross-site request forgery (Issue 47)	A vulnerability which was classified as problematic has been found in yzmcms 5.6. Affected by this issue is some unknown functionality of the file sitemodel/add.html. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2020-23595. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2020-24922	Xuxueli xxl-job 2.2.0 xxl-job-admin/user/add cross-site request forgery (Issue 1921)	A vulnerability classified as problematic has been found in Xuxueli xxl-job 2.2.0. Affected is an unknown function of the file xxl-job-admin/user/add. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2020-24922. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-2271	Tiempo.com Plugin up to 0.1.2 on WordPress cross-site request forgery	A vulnerability was found in Tiempo.com Plugin up to 0.1.2 on WordPress. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-2271. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0551	REST API TO MiniProgram Plugin up to 4.6.1 on WordPress AJAX Action cross-site request forgery	A vulnerability has been found in REST API TO MiniProgram Plugin up to 4.6.1 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-0551. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-0058	Tiempo.com Plugin up to 0.1.2 on WordPress Shortcode cross-site request forgery	A vulnerability classified as problematic has been found in Tiempo.com Plugin up to 0.1.2 on WordPress. Affected is an unknown function of the component Shortcode Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-0058. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-4455	wallabag up to 2.6.2 cross-site request forgery	A vulnerability was found in wallabag up to 2.6.2. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-4455. 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-2023-4454	wallabag up to 2.6.2 cross-site request forgery	A vulnerability was found in wallabag up to 2.6.2. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-4454. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-3366	MultiParcels Shipping For WooCommerce Plugin up to 1.15.1 on WordPress cross-site request forgery	A vulnerability classified as problematic was found in MultiParcels Shipping For WooCommerce Plugin up to 1.15.1 on WordPress. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-3366. The attack can be initiated 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-2023-39143	Papercut NG/MF up to 22.1.2 path traversal	A vulnerability was found in Papercut NG and MF up to 22.1.2. It has been classified as critical. Affected is an unknown function. The manipulation leads to path traversal. This vulnerability is traded as CVE-2023-39143. The attack needs to be approached within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack
CVE-2023-38702	Knowage up to 8.1.7 importTemplateFile path traversal (GHSA-7mjh-73q3-c3fc)	A vulnerability was found in Knowage up to 8.1.7. It has been rated as critical. This issue affects some unknown processing of the file /knowage/restful-services/dossier/importTemplateFile. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-38702. 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-2023-4171	Chengdu Flash Flood Disaster Monitoring and Warning System FileDownload.ashx path traversal	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\FileDownload.ashx. The manipulation of the argument Files leads to path traversal: &039;../filedir&039;. This vulnerability was named CVE-2023-4171. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack
CVE-2023-4172	Chengdu Flash Flood Disaster Monitoring and Warning System FileHandler.ashx absolute path traversal	A vulnerability which was classified as problematic has been found in Chengdu Flash Flood Disaster Monitoring and Warning System 2.0. This issue affects some unknown processing of the file \Service\FileHandler.ashx. The manipulation of the argument FileDirectory leads to absolute path traversal. The identification of this vulnerability is CVE-2023-4172. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack
CVE-2023-4191	SourceCodester Resort Reservation System 1.0 index.php page file	A vulnerability which was classified as critical has been found in SourceCodester Resort	Protected by core rules	Detected by scanner as local file inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	inclusion	Reservation System 1.0. Affected by this issue is some unknown functionality of the file index.php. The manipulation of the argument page leads to file inclusion. This vulnerability is handled as CVE-2023-4191. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2023-4195	cockpit up to 2.6.2 file inclusion	A vulnerability was found in cockpit up to 2.6.2 and classified as critical. This issue affects some unknown processing. The manipulation leads to file inclusion. The identification of this vulnerability is CVE-2023-4195. 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-2023-36220	Textpattern CMS 4.8.8 Plugin Upload path traversal (ID 172967)	A vulnerability was found in Textpattern CMS 4.8.8. It has been declared as critical. This vulnerability affects unknown code of the component Plugin Upload Handler. The manipulation leads to path traversal. This vulnerability was named CVE-2023-36220. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack
CVE-2023-39964	1Panel 1.4.3/1.5.0 Configuration File api/v1/file.go LoadFromFile path traversal (GHSA-pv7q-v9mv-9mh5)	A vulnerability was found in 1Panel 1.4.3/1.5.0. It has been rated as critical. This issue affects the function LoadFromFile of the file api/v1/file.go of the component Configuration File Handler. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-39964. 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-2023-38997	OPNsense up to 23.6 Captive Portal Template path traversal	A vulnerability was found in OPNsense up to 23.6. It has been classified as critical. Affected is an unknown function of the component Captive Portal Template Handler. The manipulation leads to path traversal. This vulnerability is traded as CVE-2023-38997. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		It is recommended to upgrade the affected component.		
CVE-2020-27514	ZrLog 2.1.15 admin.api.TemplateController delete path traversal (Issue 66)	A vulnerability was found in ZrLog 2.1.15. It has been declared as critical. This vulnerability affects the function delete of the component admin.api.TemplateController. The manipulation leads to path traversal. This vulnerability was named CVE-2020-27514. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack
CVE-2023-40274	zola up to 0.17.2 handle_request path traversal (Issue 2257)	A vulnerability classified as problematic was found in zola up to 0.17.2. This vulnerability affects the function handle_request. The manipulation leads to path traversal: &039;../filedir&039;. This vulnerability was named CVE-2023-40274. The attack needs to be initiated within the local network. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as local file inclusion attack
CVE-2020-26037	Even Balance Punkbuster 1.902/1.903/1.904 Server path traversal	A vulnerability was found in Even Balance Punkbuster 1.902/1.903/1.904. It has been classified as critical. Affected is an unknown function of the component Server. The manipulation leads to path traversal. This vulnerability is traded as CVE-2020-26037. 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-2023-26469	Jorani 1.0.0 path traversal	A vulnerability was found in Jorani 1.0.0 and classified as critical. This issue affects some unknown processing. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-26469. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack
CVE-2023-2316	Typora up to 1.6.6 on Windows/Linux Typora Scheme path traversal	A vulnerability has been found in Typora up to 1.6.6 on Windows/Linux and classified as critical. This vulnerability affects unknown code of the component Typora Scheme Handler. The manipulation leads to path traversal. This vulnerability was named CVE-2023-2316. The attack can 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-2023-2110	Obsidian Desktop up to 1.2.7 App Scheme path traversal	A vulnerability which was classified as critical was found in Obsidian Desktop up to 1.2.7. This affects an unknown part of the component App Scheme Handler. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-2110. 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-2023-2971	Typora up to 1.6.x on Windows/Linux Typora Scheme path traversal	A vulnerability was found in Typora up to 1.6.x on Windows/Linux and classified as critical. This issue affects some unknown processing of the component Typora Scheme Handler. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-2971. 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

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-39147	Uvdesk 1.1.3 Image File unrestricted upload	A vulnerability which was classified as critical has been found in Uvdesk 1.1.3. This issue affects some unknown processing of the component Image File Handler. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2023-39147. The attack needs to be approached within the local network. There is no exploit available.	Protected by custom rules	NA
CVE-2023-4121	Beijing Baichuo Smart S85F Management Platform up to 20230722 file_upload unrestricted upload	A vulnerability was found in Beijing Baichuo Smart S85F Management Platform up to 20230722. It has been classified as critical. Affected is an unknown function. The manipulation of the argument file_upload leads to unrestricted upload. This vulnerability is traded as CVE-2023-4121. 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 custom rules	NA
CVE-2023-38947	WBCE CMS 1.6.1 /languages/install.php unrestricted upload	A vulnerability was found in WBCE CMS 1.6.1. It has been classified as problematic. Affected is an unknown function of the file /languages/install.php. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2023-38947. The attack can only be done within the local network. There is no exploit available.	Protected by custom rules	NA
CVE-2023-36299	Typecho 1.2.1 index.php upload/options-general unrestricted upload	A vulnerability was found in Typecho 1.2.1. It has been classified as critical. This affects an unknown part of the file index.php. The manipulation of the argument upload/options-general leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-36299. It is possible to initiate the attack remotely. There is no	Protected by custom rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit available. It is recommended to upgrade the affected component.		
CVE-2023-36212	Total CMS 1.7.4 unrestricted upload (Exploit 172687 / EDB-51500)	A vulnerability was found in Total CMS 1.7.4 and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-36212. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by custom rules	NA
CVE-2023-36298	DedeCMS 5.7.109 unrestricted upload	A vulnerability has been found in DedeCMS 5.7.109 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2023-36298. The attack can be launched remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2023-4159	omeka omeka-s up to 4.0.2 unrestricted upload	A vulnerability was found in omeka omeka-s up to 4.0.2. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-4159. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by custom rules	NA
CVE-2023-4186	SourceCodester Pharmacy Management System 1.0 manage_website.php unrestricted upload	A vulnerability was found in SourceCodester Pharmacy Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file manage_website.php. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2023-4186. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by custom rules	NA
CVE-2020-23564	SEMCMS 3.9 SEMCMS_Upfile.php	A vulnerability was found in SEMCMS 3.9 and	Protected by custom rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	unrestricted upload	classified as critical. Affected by this issue is some unknown functionality of the file SEMCMS_Upfile.php. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2020-23564. The attack may be launched remotely. There is no exploit available.		
CVE-2023-26961	Alteryx Server 2022.1.1.42590 File Type Verification unrestricted upload	A vulnerability was found in Alteryx Server 2022.1.1.42590. It has been classified as critical. This affects an unknown part of the component File Type Verification Handler. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-26961. The attack needs to be approached within the local network. There is no exploit available.	Protected by custom rules	NA
CVE-2023-39776	PHP Jabbers Ticket Support Script 3.2 unrestricted upload	A vulnerability classified as critical has been found in PHP Jabbers Ticket Support Script 3.2. Affected is an unknown function. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2023-39776. It is possible to launch the attack remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2023-28480	Tigergraph Enterprise 3.7.0 unrestricted upload	A vulnerability was found in Tigergraph Enterprise 3.7.0. It has been classified as critical. Affected is an unknown function. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2023-28480. It is possible to launch the attack remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2023-38915	Wolf-leo EasyAdmin8 1.0 unrestricted upload	A vulnerability was found in Wolf-leo EasyAdmin8 1.0. It has been classified as critical. Affected is an unknown function. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2023-38915. It is possible to launch the attack remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2023-31941	Online Travel Agency System 1.0 PHP File employee_insert.php	A vulnerability was found in Online Travel Agency System 1.0. It has been	Protected by custom rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	unrestricted upload	classified as critical. This affects an unknown part of the file employee_insert.php of the component PHP File Handler. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-31941. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2023-31946	Online Travel Agency System 1.0 PHP File artical.php unrestricted upload	A vulnerability classified as critical was found in Online Travel Agency System 1.0. Affected by this vulnerability is an unknown functionality of the file artical.php of the component PHP File Handler. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2023-31946. The attack can be launched remotely. There is no exploit available.	Protected by custom rules	NA

XML External Entity Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-3823	PHP up to 8.0.29 xml external entity reference	A vulnerability classified as problematic has been found in PHP up to 8.0.29. This affects an unknown part. The manipulation leads to xml external entity reference. This vulnerability is uniquely identified as CVE-2023-3823. Access to the local network is required for this attack. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as XML external entity attack.

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-37772	PHPGurukul Online Shopping Portal 3.1 Parameter /shopping/login.php Email sql injection	A vulnerability was found in PHPGurukul Online Shopping Portal 3.1. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /shopping/login.php of the component Parameter Handler. The manipulation of the argument Email leads to sql injection. This vulnerability is known as CVE-2023-37772. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-39122	BMC Control-M 9.0.20.200 /report/deleteReport report-id sql injection	A vulnerability which was classified as critical has been found in BMC Control-M 9.0.20.200. This issue affects some unknown processing of the file /report/deleteReport. The manipulation of the argument report-id leads to sql injection. The identification of this vulnerability is CVE-2023-39122. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-36213	MotoCMS 3.4.3 search keyword sql injection (Exploit 172698 / EDB-51504)	A vulnerability classified as critical has been found in MotoCMS 3.4.3. Affected is the function search. The manipulation of the argument keyword leads to sql injection. This vulnerability is traded as CVE-2023-36213. 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-2023-39121	Emlog 2.1.9 /admin/user.php sql injection	A vulnerability was found in Emlog 2.1.9. It has been classified as critical. This affects an unknown part of the file /admin/user.php. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-39121. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-4165	Tongda OA prior 11.10 delete_seal.php DELETE_STR sql injection	A vulnerability which was classified as critical was found in Tongda OA. This affects an unknown part of the file general/system/seal_manage/iweboffice/delete_seal.php. The manipulation of the argument DELETE_STR leads to sql injection. This vulnerability is uniquely identified as CVE-2023-4165. The attack can only be done within the local network. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	Detected by scanner as sql injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		It is recommended to upgrade the affected component.		
CVE-2023-4166	Tongda OA prior 11.10 delete_log.php DELETE_STR sql injection	A vulnerability has been found in Tongda OA and classified as critical. This vulnerability affects unknown code of the file general/system/seal_manage/dianju/delete_log.php. The manipulation of the argument DELETE_STR leads to sql injection. This vulnerability was named CVE-2023-4166. The attack can only be initiated 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. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-39551	PHPGurukul Online Security Guards Hiring System 1.0 osghs/admin/search.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Online Security Guards Hiring System 1.0. Affected is an unknown function of the file osghs/admin/search.php. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-39551. 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-2023-39344	social-media-skeleton sql injection (GHSA-857x-p6fq-mgfh)	A vulnerability which was classified as critical has been found in social-media-skeleton. Affected by this issue is some unknown functionality. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-39344. 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-2023-4180	SourceCodester Free Hospital Management System for Small Practices /vm/login.php sql injection	A vulnerability classified as critical was found in SourceCodester Free Hospital Management System for Small Practices 1.0. Affected by this vulnerability is an unknown functionality of the file /vm/login.php. The manipulation of the argument useremail/userpassword leads to sql injection. This vulnerability is known as CVE-2023-4180. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-4185	SourceCodester Online Hospital Management System 1.0 patientlogin.php loginid/password sql injection	A vulnerability was found in SourceCodester Online Hospital Management System 1.0. It has been classified as critical. Affected is an unknown function of the file patientlogin.php. The manipulation of the	Protected by core rules	Detected by scanner as sql injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument loginid/password leads to sql injection. This vulnerability is traded as CVE-2023-4185. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2023-4179	SourceCodester Free Hospital Management System for Small Practices doctors.php sql injection	A vulnerability classified as critical has been found in SourceCodester Free Hospital Management System for Small Practices 1.0. Affected is an unknown function of the file /vm/doctor/doctors.phpactionview. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-4179. 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-2023-4176	SourceCodester Hospital Management System 1.0 appointmentapproval.php time sql injection	A vulnerability was found in SourceCodester Hospital Management System 1.0. It has been classified as critical. This affects an unknown part of the file appointmentapproval.php. The manipulation of the argument time leads to sql injection. This vulnerability is uniquely identified as CVE-2023-4176. 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-2023-4193	SourceCodester Resort Reservation System 1.0 view_fee.php id sql injection	A vulnerability has been found in SourceCodester Resort Reservation System 1.0 and classified as critical. This vulnerability affects unknown code of the file view_fee.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-4193. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-4188	instantsoft icms2 up to 2.16.0 sql injection	A vulnerability classified as critical has been found in instantsoft icms2 up to 2.16.0. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-4188. 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-2023-4192	SourceCodester Resort Reservation System 1.0 manage_user.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Resort Reservation System 1.0. This affects an unknown part of the file manage_user.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-4192.	Protected by core rules	Detected by scanner as sql injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2023-4201	SourceCodester Inventory Management System 1.0 ex_catagory_data.php columns[1][data] sql injection	A vulnerability was found in SourceCodester Inventory Management System 1.0 and classified as critical. This issue affects some unknown processing of the file ex_catagory_data.php. The manipulation of the argument columns[1][data] leads to sql injection. The identification of this vulnerability is CVE-2023-4201. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-4199	SourceCodester Inventory Management System 1.0 catagory_data.php columns[1][data] sql injection	A vulnerability which was classified as critical was found in SourceCodester Inventory Management System 1.0. This affects an unknown part of the file catagory_data.php. The manipulation of the argument columns[1][data] leads to sql injection. This vulnerability is uniquely identified as CVE-2023-4199. 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-2023-4200	SourceCodester Inventory Management System 1.0 product_data.php. columns[1][data] sql injection	A vulnerability has been found in SourceCodester Inventory Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file product_data.php.. The manipulation of the argument columns[1][data] leads to sql injection. This vulnerability was named CVE-2023-4200. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-4219	SourceCodester Doctors Appointment System 1.0 login.php useremail sql injection	A vulnerability was found in SourceCodester Doctors Appointment System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file login.php. The manipulation of the argument useremail leads to sql injection. This vulnerability is known as CVE-2023-4219. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-37689	Maid Hiring Management System 1.0 Booking Request Page sql injection	A vulnerability has been found in Maid Hiring Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the component Booking Request Page. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-37689. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-37682	Judging Management System 1.0	A vulnerability which was classified as critical has been	Protected by core rules	Detected by scanner as sql

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	deductScores.php id sql injection	found in Judging Management System 1.0. This issue affects some unknown processing of the file /php-jms/deductScores.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2023-37682. The attack can only be initiated within the local network. There is no exploit available.		injection attack.
CVE-2023-37688	Maid Hiring Management System 1.0 Admin Page sql injection	A vulnerability was found in Maid Hiring Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the component Admin Page. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-37688. 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-2023-37690	Maid Hiring Management System 1.0 Search Maid Page sql injection	A vulnerability was found in Maid Hiring Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the component Search Maid Page. The manipulation leads to sql injection. This vulnerability was named CVE-2023-37690. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-36311	PHP Jabbers Document Creator 1.0 index.php column sql injection	A vulnerability which was classified as critical has been found in PHP Jabbers Document Creator 1.0. Affected by this issue is some unknown functionality of the file index.php. The manipulation of the argument column leads to sql injection. This vulnerability is handled as CVE-2023-36311. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-37069	code-projects Online Hospital Management System 1.0 Field loginid/password sql injection	A vulnerability classified as critical has been found in code-projects Online Hospital Management System 1.0. Affected is an unknown function of the component Field Handler. The manipulation of the argument loginid/password leads to sql injection. This vulnerability is traded as CVE-2023-37069. 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-2023-37068	code-projects Gym Management System 1.0 Login Form password sql injection	A vulnerability which was classified as critical was found in code-projects Gym Management System 1.0. This affects an unknown part of the component Login Form. The manipulation of the argument password leads to sql injection.	Protected by core rules	Detected by scanner as sql injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is uniquely identified as CVE-2023-37068. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2020-24950	Daylight Studio Fuel CMS 1.4.9 Base_module_model.php list_items col sql injection (Issue 562)	A vulnerability was found in Daylight Studio Fuel CMS 1.4.9. It has been rated as critical. Affected by this issue is the function list_items of the file Base_module_model.php. The manipulation of the argument col leads to sql injection. This vulnerability is handled as CVE-2020-24950. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2021-29378	pear-admin-think 2.1.2 GET Request Crud.php sql injection	A vulnerability has been found in pear-admin-think 2.1.2 and classified as critical. Affected by this vulnerability is an unknown functionality of the file Crud.php of the component GET Request Handler. The manipulation leads to sql injection. This vulnerability is known as CVE-2021-29378. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2020-36034	oretnom23 School Faculty Scheduling System 1.0 manage_user.php id sql injection	A vulnerability was found in oretnom23 School Faculty Scheduling System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file manage_user.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2020-36034. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2020-36136	CSKaza CSZCMS 1.2.9 csz_model.php pm_sendmail sql injection (Issue 26)	A vulnerability was found in CSKaza CSZCMS 1.2.9. It has been classified as critical. Affected is an unknown function of the file csz_model.php. The manipulation of the argument pm_sendmail leads to sql injection. This vulnerability is traded as CVE-2020-36136. 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-2023-38916	eVotingSystem-PHP 1.0 Input Field sql injection	A vulnerability classified as critical has been found in eVotingSystem-PHP 1.0. This affects an unknown part of the component Input Field Handler. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-38916. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-39852	Doctormms 1.0 myAppoinment.php userid sql injection	A vulnerability was found in Doctormms 1.0. It has been classified as critical. This affects an unknown part of the file myAppoinment.php. The manipulation of the	Protected by core rules	Detected by scanner as sql injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument userid leads to sql injection. This vulnerability is uniquely identified as CVE-2023-39852. Access to the local network is required for this attack. There is no exploit available.		
CVE-2023-39851	webchess 1.0 mainmenu.php playerID sql injection	A vulnerability was found in webchess 1.0. It has been declared as critical. This vulnerability affects unknown code of the file mainmenu.php. The manipulation of the argument playerID leads to sql injection. This vulnerability was named CVE-2023-39851. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-39850	Schoolmate 1.3 DeleteFunctions.php courseid/teacherid sql injection	A vulnerability which was classified as critical was found in Schoolmate 1.3. Affected is an unknown function of the file DeleteFunctions.php. The manipulation of the argument courseid/teacherid leads to sql injection. This vulnerability is traded as CVE-2023-39850. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-0579	YARPP Plugin up to 5.30.2 on WordPress Shortcode Attribute sql injection	A vulnerability which was classified as critical was found in YARPP Plugin up to 5.30.2 on WordPress. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-0579. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-31945	Online Travel Agency System 1.0 daily_expenditure_edit.php daily_expenditure_edit id sql injection	A vulnerability was found in Online Travel Agency System 1.0. It has been declared as critical. This vulnerability affects the function daily_expenditure_edit of the file daily_expenditure_edit.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-31945. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-31943	Online Travel Agency System 1.0 ticket_detail.php ticket_detail ticket_id sql injection	A vulnerability which was classified as critical was found in Online Travel Agency System 1.0. Affected is the function ticket_detail of the file ticket_detail.php. The manipulation of the argument ticket_id leads to sql injection. This vulnerability is traded as CVE-2023-31943. It is possible to launch the attack	Protected by core rules	Detected by scanner as sql injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. There is no exploit available.		
CVE-2023-31944	Online Travel Agency System 1.0 employee_edit.php employee_edit emp_id sql injection	A vulnerability was found in Online Travel Agency System 1.0. It has been rated as critical. This issue affects the function employee_edit of the file employee_edit.php. The manipulation of the argument emp_id leads to sql injection. The identification of this vulnerability is CVE-2023-31944. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-31940	Online Travel Agency System 1.0 article_edit.php article_edit page_id sql injection	A vulnerability classified as critical has been found in Online Travel Agency System 1.0. Affected is the function article_edit of the file article_edit.php. The manipulation of the argument page_id leads to sql injection. This vulnerability is traded as CVE-2023-31940. 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-2023-31939	Online Travel Agency System 1.0 customer_edit.php customer_edit costomer_id sql injection	A vulnerability has been found in Online Travel Agency System 1.0 and classified as critical. Affected by this vulnerability is the function customer_edit of the file customer_edit.php. The manipulation of the argument costomer_id leads to sql injection. This vulnerability is known as CVE-2023-31939. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-38905	Jeecg-boot up to 3.5.0 sql injection (Issue 4737)	A vulnerability which was classified as critical was found in Jeecg-boot up to 3.5.0. This affects the function Benchmark/PG_Sleep/DBMS_Lock.Sleep/Waitfor/DECODE/DBMS_PIPE.RECEIVE_MESSAGE. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-38905. An attack has to be approached locally. There is no exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-31938	Online Travel Agency System 1.0 employee_detail.php employee_detail emp_id sql injection	A vulnerability was found in Online Travel Agency System 1.0 and classified as critical. Affected by this issue is the function employee_detail of the file employee_detail.php. The manipulation of the argument emp_id leads to sql injection. This vulnerability is handled as CVE-2023-31938. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-4407	Codecanyon Credit Lite 1.5.4 POST Request account_statement date1/date2 sql injection	A vulnerability classified as critical was found in Codecanyon Credit Lite 1.5.4. Affected by this vulnerability is an unknown functionality of the file /portal/reports/account_statement of the component	Protected by core rules	Detected by scanner as sql injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		POST Request Handler. The manipulation of the argument date1/date2 leads to sql injection. This vulnerability is known as CVE-2023-4407. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2023-38890	Online Shopping Portal Project 3.1 Login Form username sql injection	A vulnerability was found in Online Shopping Portal Project 3.1. It has been declared as critical. This vulnerability affects unknown code of the component Login Form. The manipulation of the argument username leads to sql injection. This vulnerability was named CVE-2023-38890. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-38839	Kidus Minimati 1.0.0 fulldelete.php ID sql injection	A vulnerability was found in Kidus Minimati 1.0.0 and classified as critical. Affected by this issue is some unknown functionality of the file fulldelete.php. The manipulation of the argument ID leads to sql injection. This vulnerability is handled as CVE-2023-38839. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-4436	SourceCodester Inventory Management System 1.0 edit_update.php user_id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Inventory Management System 1.0. This issue affects some unknown processing of the file app/action/edit_update.php. The manipulation of the argument user_id leads to sql injection. The identification of this vulnerability is CVE-2023-4436. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-4446	OpenRapid RapidCMS 1.3.1 category.php sql injection	A vulnerability which was classified as critical was found in OpenRapid RapidCMS 1.3.1. This affects an unknown part of the file template/default/category.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-4446. The attack can only be done within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as sql injection attack.
CVE-2023-4449	SourceCodester Free and Open Source Inventory Management System 1.0 /index.php columns[0][data] sql injection	A vulnerability was found in SourceCodester Free and Open Source Inventory Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /index.phppagemember. The manipulation of the argument	Protected by core rules	Detected by scanner as sql injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		columns[0][data] leads to sql injection. This vulnerability is traded as CVE-2023-4449. It is possible to launch the attack remotely. Furthermore there is an exploit available.		

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-36211	Barebones CMS 2.0.2 Admin Panel cross-site scripting (Exploit 51502 / EDB-51502)	A vulnerability has been found in Barebones CMS 2.0.2 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Admin Panel. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-36211. 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-2023-36210	MotoCMS 3.4.3 Template keyword injection (Exploit 51499 / EDB-51499)	A vulnerability which was classified as problematic was found in MotoCMS 3.4.3. Affected is an unknown function of the component Template Handler. The manipulation of the argument keyword leads to injection. This vulnerability is traded as CVE-2023-36210. The attack can only be done within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-36118	Faculty Evaulation System 1.0 page cross-site scripting (ID 172672)	A vulnerability which was classified as problematic was found in Faculty Evaulation System 1.0. Affected is an unknown function. The manipulation of the argument page leads to cross-site scripting. This vulnerability is traded as CVE-2023-36118. 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-2023-33564	PHP Jabbers Time Slots Booking Calendar 3.3 preview.php theme cross-site scripting	A vulnerability which was classified as problematic has been found in PHP Jabbers Time Slots Booking Calendar 3.3. Affected by this issue is some unknown functionality of the file preview.php. The manipulation of the argument theme leads to cross-site scripting. This vulnerability is handled as CVE-2023-33564. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-33560	PHP Jabbers Time Slots Booking Calendar 3.3 preview.php cid cross-site scripting	A vulnerability classified as problematic was found in PHP Jabbers Time Slots Booking Calendar 3.3. Affected by this vulnerability is an unknown functionality of the file preview.php. The manipulation of the argument cid leads to cross-site scripting. This vulnerability is known as CVE-2023-33560. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-34869	PHP Jabbers Catering System 1.0 index.php cross-site scripting	A vulnerability classified as problematic has been found in PHP Jabbers Catering System 1.0. Affected is an unknown function of the file /index.phpcontrollerpjAdmin&actionpjActionForgo	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		t. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-34869. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2023-36121	e107 CMS 2.3.2 SEO Project description cross-site scripting (Exploit 51449 / EDB-51449)	A vulnerability classified as problematic has been found in e107 CMS 2.3.2. This affects the function description of the component SEO Project. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-36121. 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-2023-4117	PHP Jabbers Rental Property Booking 2.0 /index.php index cross-site scripting	A vulnerability which was classified as problematic has been found in PHP Jabbers Rental Property Booking 2.0. Affected by this issue is some unknown functionality of the file /index.php. The manipulation of the argument index leads to cross-site scripting. This vulnerability is handled as CVE-2023-4117. 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 cross-site scripting attack.
CVE-2023-4113	PHP Jabbers Service Booking Script 1.0 /index.php index cross-site scripting	A vulnerability was found in PHP Jabbers Service Booking Script 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /index.php. The manipulation of the argument index leads to cross-site scripting. This vulnerability was named CVE-2023-4113. The attack can be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-4111	PHP Jabbers Bus Reservation System 1.1 /index.php index/pickup_id cross-site scripting	A vulnerability was found in PHP Jabbers Bus Reservation System 1.1 and classified as problematic. Affected by this issue is some unknown functionality of the file /index.php. The manipulation of the argument index/pickup_id leads to cross-site scripting. This vulnerability is handled as CVE-2023-4111. 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 cross-site scripting attack.
CVE-2023-33257	Verint Engagement Management 15.3	A vulnerability classified as problematic has been found	Protected by core rules	Detected by scanner as cross-

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Update 2023R2 Live Chat cross-site scripting	in Verint Engagement Management 15.3 Update 2023R2. This affects an unknown part of the component Live Chat. The manipulation leads to basic cross-site scripting. This vulnerability is uniquely identified as CVE-2023-33257. It is possible to initiate the attack remotely. There is no exploit available.		site scripting attack.
CVE-2023-4110	PHP Jabbers Availability Booking Calendar 5.0 /index.php session_id cross-site scripting	A vulnerability has been found in PHP Jabbers Availability Booking Calendar 5.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /index.php. The manipulation of the argument session_id leads to cross-site scripting. This vulnerability is known as CVE-2023-4110. 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-2023-4119	Academy LMS 6.0 /academy/home/courses query/sort_by cross-site scripting	A vulnerability has been found in Academy LMS 6.0 and classified as problematic. This vulnerability affects unknown code of the file /academy/home/courses. The manipulation of the argument query/sort_by leads to cross-site scripting. This vulnerability was named CVE-2023-4119. The attack can be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-4116	PHP Jabbers Taxi Booking 2.0 /index.php index cross-site scripting	A vulnerability classified as problematic was found in PHP Jabbers Taxi Booking 2.0. Affected by this vulnerability is an unknown functionality of the file /index.php. The manipulation of the argument index leads to cross-site scripting. This vulnerability is known as CVE-2023-4116. 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-2023-4115	PHP Jabbers Cleaning Business 1.0 /index.php index cross-site scripting	A vulnerability classified as problematic has been found in PHP Jabbers Cleaning Business 1.0. Affected is an unknown function of the file /index.php. The manipulation of the argument index leads to cross-site scripting. This vulnerability is traded as CVE-2023-4115. It is possible	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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.		
CVE-2023-36081	GatesAir Flexiva FAX 150W Web Application Dashboard cross-site scripting	A vulnerability classified as problematic was found in GatesAir Flexiva FAX 150W. This vulnerability affects unknown code of the component Web Application Dashboard. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-36081. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-4114	PHP Jabbers Night Club Booking Software 1.0 /index.php index cross-site scripting	A vulnerability was found in PHP Jabbers Night Club Booking Software 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /index.php. The manipulation of the argument index leads to cross-site scripting. The identification of this vulnerability is CVE-2023-4114. 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 cross-site scripting attack.
CVE-2023-4112	PHP Jabbers Shuttle Booking Software 1.0 /index.php cross-site scripting	A vulnerability was found in PHP Jabbers Shuttle Booking Software 1.0. It has been classified as problematic. This affects an unknown part of the file /index.php. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-4112. It is possible to initiate the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-4035	Simple Blog Card Plugin up to 1.30 on WordPress Shortcode cross-site scripting	A vulnerability was found in Simple Blog Card Plugin up to 1.30 on WordPress and classified as problematic. Affected by this issue is some unknown functionality of the component Shortcode Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-4035. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-36217	Xoops CMS 2.5.10 Category Name cross-site scripting (EDB-51520)	A vulnerability which was classified as problematic has been found in Xoops CMS 2.5.10. Affected by this issue is some unknown functionality of the component Category Name Handler. The manipulation 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 handled as CVE-2023-36217. The attack may be launched remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.		
CVE-2023-4145	pimcore customer-data-framework up to 3.4.1 cross-site scripting	A vulnerability which was classified as problematic was found in pimcore customer-data-framework up to 3.4.1. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-4145. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2020-20808	Qibosoft up to 7 do/search.php starttijd cross-site scripting	A vulnerability which was classified as problematic has been found in Qibosoft up to 7. This issue affects some unknown processing of the file do/search.php. The manipulation of the argument starttijd leads to cross-site scripting. The identification of this vulnerability is CVE-2020-20808. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-39552	PHPGurukul Online Security Guards Hiring System 1.0 cross-site scripting	A vulnerability classified as problematic was found in PHPGurukul Online Security Guards Hiring System 1.0. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-39552. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-36137	PHP Jabbers Class Scheduling System 1.0 preview.php theme cross-site scripting	A vulnerability was found in PHP Jabbers Class Scheduling System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file preview.php. The manipulation of the argument theme leads to cross-site scripting. This vulnerability is handled as CVE-2023-36137. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-1982	WP Front User Submit Plugin up to 4.0.4 on WordPress cross-site scripting	A vulnerability was found in WP Front User Submit Plugin up to 4.0.4 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-2023-1982. 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-2023-38964	Creative Item Academy LMS 6.0 cross-site	A vulnerability has been found in Creative Item	Protected by core rules	Detected by scanner as cross-

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	scripting	Academy LMS 6.0 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-38964. The attack can be initiated remotely. There is no exploit available.		site scripting attack.
CVE-2023-36138	PHP Jabbers Cleaning Business Software 1.0 preview.php theme cross-site scripting	A vulnerability was found in PHP Jabbers Cleaning Business Software 1.0. It has been classified as problematic. This affects an unknown part of the file preview.php. The manipulation of the argument theme leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-36138. 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-2023-36158	SourceCodester Toll Tax Management System 1.0 My Account Page First Name/Last Name cross-site scripting	A vulnerability was found in SourceCodester Toll Tax Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the component My Account Page. The manipulation of the argument First Name/Last Name leads to cross-site scripting. This vulnerability was named CVE-2023-36158. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-4170	DedeBIZ 6.2.10 Article cross-site scripting	A vulnerability was found in DedeBIZ 6.2.10. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Article Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-4170. 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 cross-site scripting attack.
CVE-2023-4167	Media Browser Emby Server 4.7.13.0 /web/ cross-site scripting	A vulnerability was found in Media Browser Emby Server 4.7.13.0 and classified as problematic. This issue affects some unknown processing of the file /web/. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-4167. The attack may be initiated remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-4158	omeka omeka-s up to 4.0.2 cross-site scripting	A vulnerability classified as problematic was found in omeka omeka-s up to 4.0.2. This vulnerability affects unknown code. The manipulation leads to cross-	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		site scripting. This vulnerability was named CVE-2023-4158. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-3992	PostX Gutenberg Post Grid Blocks Plugin up to 3.0.5 on WordPress postx_type cross-site scripting	A vulnerability was found in PostX Gutenberg Post Grid Blocks Plugin up to 3.0.5 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument postx_type leads to cross-site scripting. This vulnerability is known as CVE-2023-3992. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-29689	PyroCMS up to 3.9 Template injection	A vulnerability classified as critical was found in PyroCMS up to 3.9. Affected by this vulnerability is an unknown functionality of the component Template Handler. The manipulation leads to injection. This vulnerability is known as CVE-2023-29689. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-4174	mooSocial mooStore 3.1.6 cross-site scripting	A vulnerability has been found in mooSocial mooStore 3.1.6 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-2023-4174. 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-2023-4173	mooSocial mooStore 3.1.6 /search/index q cross-site scripting	A vulnerability which was classified as problematic was found in mooSocial mooStore 3.1.6. Affected is an unknown function of the file /search/index. The manipulation of the argument q leads to cross-site scripting. This vulnerability is traded as CVE-2023-4173. 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-2023-4187	instantsoft icms2 up to 2.16.0 cross-site scripting	A vulnerability which was classified as problematic has been found in instantsoft icms2 up to 2.16.0. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-4187. 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-2023-4189	instantsoft icms2 up to	A vulnerability which was	Protected by	Detected by

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	2.16.0 cross-site scripting	classified as problematic was found in instantsoft icms2 up to 2.16.0. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-4189. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	core rules	scanner as cross-site scripting attack.
CVE-2023-3524	WPCode Plugin up to 2.0.13.0 on WordPress URL cross-site scripting	A vulnerability was found in WPCode Plugin up to 2.0.13.0 on WordPress and classified as problematic. Affected by this issue is some unknown functionality of the component URL Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-3524. 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-2023-4196	cockpit up to 2.6.2 cross-site scripting	A vulnerability was found in cockpit up to 2.6.2. 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-2023-4196. 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-2023-3650	Bubble Menu Plugin up to 3.0.4 on WordPress Setting cross-site scripting	A vulnerability classified as problematic has been found in Bubble Menu Plugin up to 3.0.4 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-2023-3650. 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-2023-3575	Quiz and Survey Master Plugin up to 8.1.10 on WordPress Question Title cross-site scripting	A vulnerability classified as problematic was found in Quiz and Survey Master Plugin up to 8.1.10 on WordPress. This vulnerability affects unknown code of the component Question Title Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-3575. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component.		
CVE-2023-4203	Advantech EKI-1524/EKI-1522/EKI-1521 up to 1.21 Web Interface cross-site scripting	A vulnerability was found in Advantech EKI-1524 EKI-1522 and EKI-1521 up to 1.21. It has been classified as problematic. Affected is an unknown function of the component Web Interface. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-4203. 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-2023-3526	Phoenix Contact TC Router/TC Cloud Client License Viewer Page cross-site scripting (VDE-2023-017)	A vulnerability was found in Phoenix Contact TC Router and TC Cloud Client. It has been classified as problematic. This affects an unknown part of the component License Viewer Page. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-3526. 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-2023-37685	Online Nurse Hiring System 1.0 Search Report Page cross-site scripting	A vulnerability classified as problematic was found in Online Nurse Hiring System 1.0. Affected by this vulnerability is an unknown functionality of the component Search Report Page. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-37685. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-4202	Advantech EKI-1524/EKI-1522/EKI-1521 up to 1.21 Web Interface device name cross-site scripting	A vulnerability was found in Advantech EKI-1524 EKI-1522 and EKI-1521 up to 1.21 and classified as problematic. This issue affects some unknown processing of the component Web Interface. The manipulation of the argument device name leads to cross-site scripting. The identification of this vulnerability is CVE-2023-4202. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-37684	Online Nurse Hiring System 1.0 Admin Portal cross-site scripting	A vulnerability classified as problematic has been found in Online Nurse Hiring System 1.0. Affected is an unknown function of the component Admin Portal. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-37684. 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-2023-37683	Online Nurse Hiring System 1.0 Profile Page cross-site scripting	A vulnerability was found in Online Nurse Hiring System 1.0. It has been rated as problematic. This issue affects some unknown processing of the	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component Profile Page. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-37683. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-4254	ChatBot Plugin 4.7.7 on WordPress Setting cross-site scripting	A vulnerability classified as problematic was found in ChatBot Plugin 4.7.7 on WordPress. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-4254. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-36309	PHP Jabbers Document Creator 1.0 index.php action cross-site scripting	A vulnerability classified as problematic was found in PHP Jabbers Document Creator 1.0. This vulnerability affects unknown code of the file index.php. The manipulation of the argument action leads to cross-site scripting. This vulnerability was named CVE-2023-36309. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-36310	PHP Jabbers Document Creator 1.0 index.php column cross-site scripting	A vulnerability which was classified as problematic has been found in PHP Jabbers Document Creator 1.0. This issue affects some unknown processing of the file index.php. The manipulation of the argument column leads to cross-site scripting. The identification of this vulnerability is CVE-2023-36310. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-36312	PHP Jabbers Callback Widget 1.0 index.php o_bf_include_timezone cross-site scripting	A vulnerability which was classified as problematic was found in PHP Jabbers Callback Widget 1.0. Affected is an unknown function of the file index.php. The manipulation of the argument o_bf_include_timezone leads to cross-site scripting. This vulnerability is traded as CVE-2023-36312. 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-2023-39002	OPNsense up to 23.6 system_certmanager.php act cross-site scripting	A vulnerability was found in OPNsense up to 23.6. It has been rated as problematic. This issue affects some unknown processing of the file system_certmanager.php. The manipulation of the argument act leads to cross-site scripting. The identification of this vulnerability is CVE-2023-39002. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component.		
CVE-2023-36314	PHP Jabbers Callback Widget 1.0 index.php value-text-o_sms_email_request_message cross-site scripting	A vulnerability was found in PHP Jabbers Callback Widget 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file index.php. The manipulation of the argument value-text-o_sms_email_request_message leads to cross-site scripting. This vulnerability is handled as CVE-2023-36314. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-39007	OPNsense up to 23.6 Cron /ui/cron/item/open cross-site scripting	A vulnerability was found in OPNsense up to 23.6 and classified as problematic. This issue affects some unknown processing of the file /ui/cron/item/open of the component Cron. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-39007. 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-2023-36313	PHP Jabbers Document Creator 1.0 POST Parameter request_feed cross-site scripting	A vulnerability has been found in PHP Jabbers Document Creator 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component POST Parameter Handler. The manipulation of the argument request_feed leads to cross-site scripting. This vulnerability is known as CVE-2023-36313. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-38347	LWsystems Benno MailArchiv 2.10.1 Mailbox cross-site scripting	A vulnerability classified as problematic was found in LWsystems Benno MailArchiv 2.10.1. Affected by this vulnerability is an unknown functionality of the component Mailbox. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-38347. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-36315	PHP Jabbers Document Creator 1.0 index.php action cross-site scripting	A vulnerability was found in PHP Jabbers Document Creator 1.0. It has been classified as problematic. This affects an unknown part of the file index.php. The manipulation of the argument action leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-36315. 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-2023-39000	OPNsense up to 23.6 URL cross-site scripting	A vulnerability which was classified as problematic has been found in OPNsense up	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to 23.6. This issue affects some unknown processing of the file /ui/diagnostics/log/core/ of the component URL Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-39000. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2021-27524	margox braft-editor 2.3.8 Embed Media cross-site scripting (Issue 880)	A vulnerability was found in margox braft-editor 2.3.8. It has been declared as problematic. This vulnerability affects unknown code of the component Embed Media Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2021-27524. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2020-28717	kindsoft kindeditor 4.1.12 demo.jsp content1 cross-site scripting (Issue 321)	A vulnerability was found in kindsoft kindeditor 4.1.12. It has been rated as problematic. This issue affects some unknown processing of the file demo.jsp. The manipulation of the argument content1 leads to cross-site scripting. The identification of this vulnerability is CVE-2020-28717. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2020-19952	jbt Markdown Editor 2252418c27dffbb35147acd8ed324822b8919477 Rendering Engine cross-site scripting (Issue 106)	A vulnerability was found in jbt Markdown Editor 2252418c27dffbb35147acd8ed324822b8919477. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Rendering Engine. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2020-19952. The attack may be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-37625	Netbox 3.4.7 Custom Link Template cross-site scripting (Issue 12205)	A vulnerability classified as problematic was found in Netbox 3.4.7. Affected by this vulnerability is an unknown functionality of the component Custom Link Template Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-37625. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2020-20523	Gila CMS 1.11.3 Installation adm_user cross-site scripting (Issue 41)	A vulnerability classified as problematic was found in Gila CMS 1.11.3. Affected by this vulnerability is an unknown functionality of the component Installation Handler. The manipulation of the argument adm_user	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		leads to cross-site scripting. This vulnerability is known as CVE-2020-20523. The attack can be launched remotely. There is no exploit available.		
CVE-2020-28849	ChurchCRM 4.2.1 View All Deposit Module Add New Deposit cross-site scripting (Issue 5477)	A vulnerability was found in ChurchCRM 4.2.1. It has been classified as problematic. Affected is an unknown function of the component View All Deposit Module. The manipulation of the argument Add New Deposit leads to cross-site scripting. This vulnerability is traded as CVE-2020-28849. 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-2023-37070	code-projects Hospital Information System 1.0 cross-site scripting	A vulnerability classified as problematic has been found in code-projects Hospital Information System 1.0. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-37070. 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-2023-4321	cockpit up to 2.4.2 cross-site scripting	A vulnerability which was classified as problematic was found in cockpit up to 2.4.2. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-4321. 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-2023-38687	Svelecte up to 3.16.2 cross-site scripting (GHSA-7h45-grc5-89wq)	A vulnerability was found in Svelecte up to 3.16.2. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-38687. 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-2023-2606	WP Brutal AI Plugin up to 2.05 on WordPress Setting cross-site scripting	A vulnerability classified as problematic has been found in WP Brutal AI Plugin up to 2.05 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-2023-2606. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-2803	Ultimate Addons for Contact Form 7 Plugin up to 3.1.28 on WordPress cross-site scripting	A vulnerability classified as problematic was found in Ultimate Addons for Contact Form 7 Plugin up to 3.1.28 on WordPress. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-2803. 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-2023-3721	WP-EMail Plugin up to 2.69.0 on WordPress Setting cross-site scripting	A vulnerability was found in WP-EMail Plugin up to 2.69.0 on WordPress and classified 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-2023-3721. 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-2023-40024	ScanCode.io up to 32.5.1 /license/ license_details_view cross-site scripting (GHSA-6xcx-gx7r-rccj)	A vulnerability was found in ScanCode.io up to 32.5.1. It has been classified as problematic. This affects the function license_details_view of the file /license/. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-40024. 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-2023-3645	Contact Form Builder by Bit Form Plugin up to 2.1.x on WordPress Setting cross-site scripting	A vulnerability which was classified as problematic has been found in Contact Form Builder by Bit Form Plugin up to 2.1.x on WordPress. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-3645. 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-2023-2802	Ultimate Addons for Contact Form 7 Plugin up to 3.1.28 on WordPress Setting cross-site scripting	A vulnerability which was classified as problematic was found in Ultimate Addons for Contact Form 7 Plugin up to 3.1.28 on WordPress. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2023-2802. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2022-4953	Elementor Website Builder Plugin up to 3.5.4 on WordPress URL cross-site scripting	A vulnerability which was classified as problematic was found in Elementor Website Builder Plugin up to 3.5.4 on WordPress. Affected is an unknown function of the component URL Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-4953. 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-2023-4347	librenms up to 23.7.x cross-site scripting	A vulnerability which was classified as problematic was found in librenms up to 23.7.x. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-4347. 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-2023-4382	tdevs Hyip Rio 2.1 Profile Settings /user/settings avatar cross-site scripting	A vulnerability which was classified as problematic has been found in tdevs Hyip Rio 2.1. Affected by this issue is some unknown functionality of the file /user/settings of the component Profile Settings. The manipulation of the argument avatar leads to cross-site scripting. This vulnerability is handled as CVE-2023-4382. 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 cross-site scripting attack.
CVE-2023-39115	Campcodes Online Matrimonial Website System Script 3.3 SVG Document upload cross-site scripting (ID 173950)	A vulnerability was found in Campcodes Online Matrimonial Website System Script 3.3. It has been classified as problematic. Affected is an unknown function of the file install/aiz-uploader/upload of the component SVG Document Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-39115. 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-2023-38904	Netlify CMS 2.10.192 the body cross-site scripting (Exploit 51576 / EDB-51576)	A vulnerability was found in Netlify CMS 2.10.192 and classified as problematic. This issue affects the function the. The	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument body leads to cross-site scripting. The identification of this vulnerability is CVE-2023-38904. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2023-1110	Yellow Yard Searchbar Plugin up to 2.8.11 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in Yellow Yard Searchbar Plugin up to 2.8.11 on WordPress and classified as problematic. Affected by this issue is some unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-1110. 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-2023-2272	Tiempo.com Plugin up to 0.1.2 on WordPress page cross-site scripting	A vulnerability was found in Tiempo.com Plugin up to 0.1.2 on WordPress. It has been rated as problematic. This issue affects some unknown processing. The manipulation of the argument page leads to cross-site scripting. The identification of this vulnerability is CVE-2023-2272. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-2122	10web Image Optimizer Plugin up to 1.0.26 on WordPress iowd_tabs_active cross-site scripting	A vulnerability was found in 10web Image Optimizer Plugin up to 1.0.26 on WordPress. It has been classified as problematic. This affects an unknown part. The manipulation of the argument iowd_tabs_active leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-2122. 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-2023-4395	cockpit up to 2.6.3 cross-site scripting	A vulnerability which was classified as problematic has been found in cockpit up to 2.6.3. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-4395. 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-2023-31942	Online Travel Agency System 1.0 insert.php description cross-site scripting	A vulnerability which was classified as problematic has been found in Online Travel Agency System 1.0. Affected	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		by this issue is some unknown functionality of the file insert.php. The manipulation of the argument description leads to cross-site scripting. This vulnerability is handled as CVE-2023-31942. The attack may be launched remotely. There is no exploit available.		
CVE-2023-38910	CSZ CMS 1.3.0 Carousel Wiget cross-site scripting	A vulnerability was found in CSZ CMS 1.3.0. It has been rated as problematic. This issue affects some unknown processing of the component Carousel Wiget. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-38910. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-38911	CSZ CMS 1.3.0 YouTube URL Field Gallery cross-site scripting	A vulnerability which was classified as problematic has been found in CSZ CMS 1.3.0. Affected by this issue is some unknown functionality of the component YouTube URL Field Handler. The manipulation of the argument Gallery leads to cross-site scripting. This vulnerability is handled as CVE-2023-38911. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-2317	Typora up to 1.6.6 on Windows/Linux Markdown File updater/update.html cross-site scripting	A vulnerability was found in Typora up to 1.6.6 on Windows/Linux. It has been classified as problematic. Affected is an unknown function of the file updater/update.html of the component Markdown File Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-2317. 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-2023-2318	r up to 0.17.1 pasteCtrl.js cross-site scripting (ID 3618)	A vulnerability was found in r up to 0.17.1. It has been declared as problematic. Affected by this vulnerability is an unknown functionality in the library src/muya/lib/contentState/pasteCtrl.js. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-2318. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-4432	cockpit up to 2.6.3 cross-site scripting	A vulnerability classified as problematic was found in cockpit up to 2.6.3. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-4432. The	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-4422	cockpit up to 2.6.2 cross-site scripting	A vulnerability classified as problematic has been found in cockpit up to 2.6.2. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-4422. 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-2023-4453	pimcore up to 10.6.7 cross-site scripting	A vulnerability was found in pimcore up to 10.6.7 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-2023-4453. 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-2023-4451	cockpit up to 2.6.3 cross-site scripting	A vulnerability was found in cockpit up to 2.6.3. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-4451. 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-2023-3936	Blog2Social Plugin up to 7.2.0 on WordPress cross-site scripting	A vulnerability was found in Blog2Social Plugin up to 7.2.0 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-2023-3936. 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-2023-3954	MultiParcels Shipping For WooCommerce Plugin up to 1.15.3 on WordPress cross-site scripting	A vulnerability which was classified as problematic has been found in MultiParcels Shipping For WooCommerce Plugin up to 1.15.3 on WordPress. This issue affects some unknown processing. The manipulation 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
		3954. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-39094	ZeroWdd studentmanager 1.0 Student List username cross-site scripting (Issue 12)	A vulnerability classified as problematic has been found in ZeroWdd studentmanager 1.0. This affects an unknown part of the component Student List Handler. The manipulation of the argument username leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-39094. 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-2023-38974	Badaso 2.9.7 Edit Category Title cross-site scripting	A vulnerability was found in Badaso 2.9.7. It has been classified as problematic. Affected is an unknown function of the component Edit Category Handler. The manipulation of the argument Title leads to cross-site scripting. This vulnerability is traded as CVE-2023-38974. 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-2023-40877	DedeCMS up to 5.7.110 /dede/freelist_edit.php title cross-site scripting	A vulnerability classified as problematic was found in DedeCMS up to 5.7.110. Affected by this vulnerability is an unknown functionality of the file /dede/freelist_edit.php. The manipulation of the argument title leads to cross-site scripting. This vulnerability is known as CVE-2023-40877. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-40876	DedeCMS up to 5.7.110 /dede/freelist_add.php title cross-site scripting	A vulnerability classified as problematic has been found in DedeCMS up to 5.7.110. Affected is an unknown function of the file /dede/freelist_add.php. The manipulation of the argument title leads to cross-site scripting. This vulnerability is traded as CVE-2023-40876. 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-2023-40875	DedeCMS up to 5.7.110 /dede/vote_edit.php votename/votenote cross-site scripting	A vulnerability was found in DedeCMS up to 5.7.110. It has been rated as problematic. This issue affects some unknown processing of the file /dede/vote_edit.php. The manipulation of the argument votename/votenote leads to cross-site scripting. The identification of this vulnerability is CVE-2023-40875. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-40874	DedeCMS up to 5.7.110 /dede/vote_add.php votename/voteitem1	A vulnerability was found in DedeCMS up to 5.7.110. It has been declared as	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	problematic. This vulnerability affects unknown code of the file /dede/vote_add.php. The manipulation of the argument votename/voteitem1 leads to cross-site scripting. This vulnerability was named CVE-2023-40874. The attack can be initiated remotely. There is no exploit available.		

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