INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

October
2023

The total zero-day vulnerabilities count for October month: 251

Command Injection	CSRF	Local File Inclusion	Malicious File Upload	SQL Injection	Cross-site Scripting
33	15	10	15	44	134

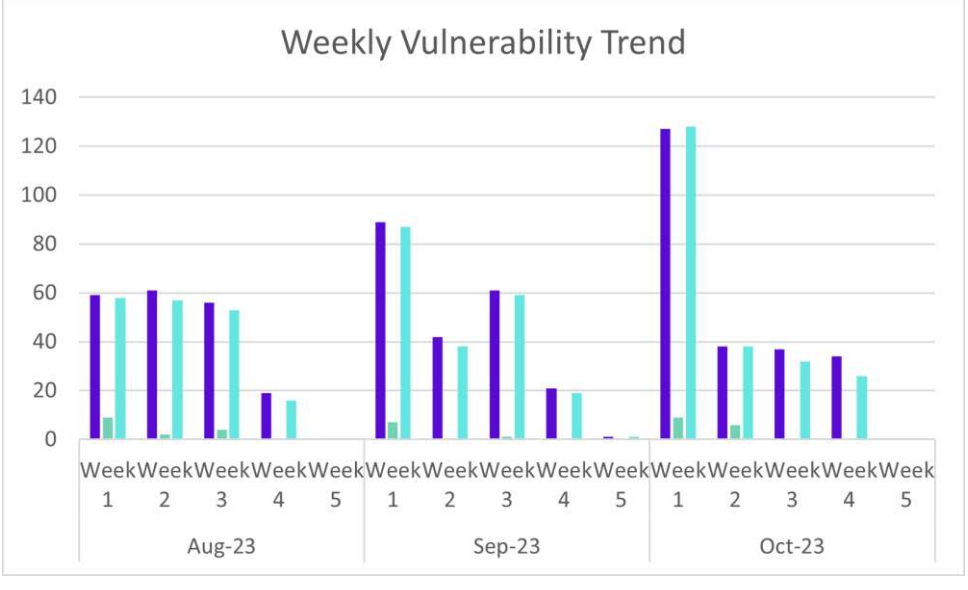
Zero-day vulnerabilities protected through core rules	236
Zero-day vulnerabilities protected through custom rules	15
Zero-day vulnerabilities for which protection cannot be done	0
Zero-day vulnerabilities found by Indusface WAS	221

- 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 and the type of protection provided for the last quarter.

Weekly Vulnerability Trend

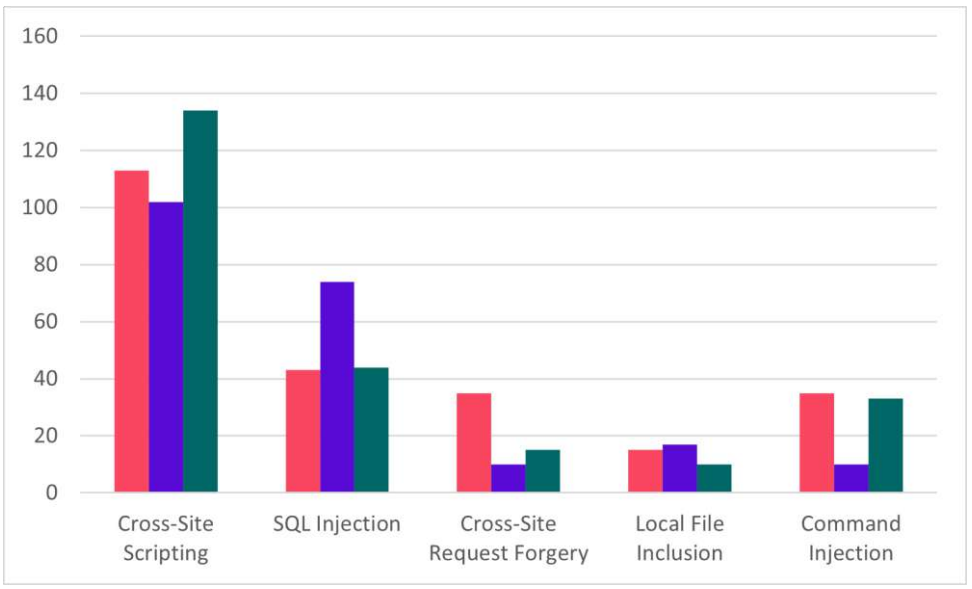


of the zero-day vulnerabilities were protected by the core rules in the last month

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

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

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-40581	yt-dlp prior 2023.09.24.003044 os command injection (GHSA-42h4-v29r-42qg)	A vulnerability was found in yt-dlp. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation leads to os command injection. This vulnerability is handled as CVE-2023-40581. 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-2023-26145	pydash up to 5.x pydash.objects.invoke command injection	A vulnerability classified as critical has been found in pydash up to 5.x. This affects the function pydash.objects.invoke. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2023-26145. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-43651	JumpServer prior 2.28.20/3.7.1 code injection (GHSA-4r5x-x283-wm96)	A vulnerability was found in JumpServer. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation leads to code injection. This vulnerability is handled as CVE-2023-43651. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component.		
CVE-2023-5301	DedeCMS 5.7.111 album_add.php AddMyAddon albumUploadFiles os command injection	A vulnerability classified as critical was found in DedeCMS 5.7.111. This vulnerability affects the function AddMyAddon of the file album_add.php. The manipulation of the argument albumUploadFiles leads to os command injection. This vulnerability was named CVE-2023-5301. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-26148	ithewei libhv Request Header injection	A vulnerability was found in ithewei libhv. It has been classified as critical. This affects an unknown part of the component Request Header Handler. The manipulation leads to injection. This vulnerability is uniquely identified as CVE-2023-26148. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-43890	Netis N3Mv2 1.0.1.865 Diagnostic Tools Page command injection	A vulnerability was found in Netis N3Mv2 1.0.1.865. It has been classified as critical. Affected is an unknown function of the component Diagnostic Tools Page. The manipulation leads to command injection. This vulnerability is traded as CVE-2023-43890. 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-2023-43892	Netis N3Mv2 1.0.1.865 WAN Setting Hostname command injection	A vulnerability classified as critical was found in Netis N3Mv2 1.0.1.865. This vulnerability affects unknown code of the component WAN Setting Handler. The manipulation of the argument Hostname leads to command injection. This vulnerability was named CVE-2023-43892. 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-2023-43835	Super Store Finder up to 3.7 Setting config.inc.php code injection (ID 174756)	A vulnerability was found in Super Store Finder up to 3.7 and classified as critical. This issue affects some unknown processing of the file config.inc.php of the component Setting Handler. The manipulation leads to code injection. The identification of this vulnerability is CVE-2023-43835. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-43893	Netis N3Mv2 1.0.1.865 Wake-On-LAN wakeup_mac command injection	A vulnerability which was classified as critical has been found in Netis N3Mv2 1.0.1.865. This issue affects some unknown processing of the component Wake-On-LAN. The manipulation of the argument wakeup_mac leads to command injection.	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The identification of this vulnerability is CVE-2023-43893. Access to the local network is required for this attack. There is no exploit available.		
CVE-2023-43891	Netis N3Mv2 1.0.1.865 command injection	A vulnerability classified as critical has been found in Netis N3Mv2 1.0.1.865. This affects an unknown part. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2023-43891. 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-2023-33271	DTS Monitoring 3.57.0 SSL Certificate Check common_name os command injection	A vulnerability has been found in DTS Monitoring 3.57.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the component SSL Certificate Check. The manipulation of the argument common_name leads to os command injection. This vulnerability is known as CVE-2023-33271. 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-2023-33269	DTS Monitoring 3.57.0 WGET Check options os command injection	A vulnerability which was classified as critical has been found in DTS Monitoring 3.57.0. This issue affects some unknown processing of the component WGET Check. The manipulation of the argument options leads to os command injection. The identification of this vulnerability is CVE-2023-33269. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-33273	DTS Monitoring 3.57.0 WGET Check url os command injection	A vulnerability was found in DTS Monitoring 3.57.0. It has been classified as critical. This affects an unknown part of the component WGET Check. The manipulation of the argument url leads to os command injection. This vulnerability is uniquely identified as CVE-2023-33273. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-33268	DTS Monitoring 3.57.0 SSL Certificate port os command injection	A vulnerability classified as critical was found in DTS Monitoring 3.57.0. This vulnerability affects unknown code of the component SSL Certificate Handler. The manipulation of the argument port leads to os command injection. This vulnerability was named CVE-2023-33268. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-33270	DTS Monitoring 3.57.0 Curl Check os command injection	A vulnerability which was classified as critical was found in DTS Monitoring	Protected by core rules	Detected by scanner as command injection

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		3.57.0. Affected is an unknown function of the component Curl Check. The manipulation of the argument url leads to os command injection. This vulnerability is traded as CVE-2023-33270. The attack needs to be done within the local network. There is no exploit available.		attack.
CVE-2023-33272	DTS Monitoring 3.57.0 Ping Check ip os command injection	A vulnerability was found in DTS Monitoring 3.57.0 and classified as critical. Affected by this issue is some unknown functionality of the component Ping Check. The manipulation of the argument ip leads to os command injection. This vulnerability is handled as CVE-2023-33272. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-36820	micronaut-security-oauth2 Remote Code Execution	A vulnerability was found in micronaut-security-oauth2. It has been classified as problematic. This affects an unknown part. The manipulation leads to Remote Code Execution. This vulnerability is uniquely identified as CVE-2023-36820. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-26153	geokit-rails up to 2.4.x YAML geo_location command injection	A vulnerability was found in geokit-rails up to 2.4.x and classified as critical. This issue affects some unknown processing of the component YAML Handler. The manipulation of the argument geo_location leads to command injection. The identification of this vulnerability is CVE-2023-26153. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-22515	Atlassian Confluence Server/Confluence Data Center up to 8.5.1 Remote Code Execution	A vulnerability which was classified as very critical was found in Atlassian Confluence Server and Confluence Data Center up to 8.5.1. This affects an unknown part. The manipulation leads to Remote Code Execution. This vulnerability is uniquely identified as CVE-2023-22515. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-45208	D-Link DAP-X1860 up to 1.01b05-01 SSID libcgifunc.so	A vulnerability which was classified as critical has been found in D-Link DAP-X1860	Protected by core rules	Detected by scanner as command injection

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	parsing_xml_stasurvey os command injection	up to 1.01b05-01. Affected by this issue is the function parsing_xml_stasurvey in the library libcgifunc.so of the component SSID Handler. The manipulation leads to os command injection. This vulnerability is handled as CVE-2023-45208. The attack needs to be initiated within the local network. There is no exploit available.		attack.
CVE-2023-5494	Beijing Baichuo Smart S45F Multi-Service Secure Gateway Intelligent Management Platform /log/download.php os command injection	A vulnerability was found in Beijing Baichuo Smart S45F Multi-Service Secure Gateway Intelligent Management Platform up to 20230928 and classified as critical. Affected by this issue is some unknown functionality of the file /log/download.php. The manipulation of the argument file leads to os command injection. This vulnerability is handled as CVE-2023-5494. The attack may be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-35194	Peplink Surf SOHO HW1 6.3.5 HTTP Request api.cgi system os command injection (TALOS-2023-1782)	A vulnerability was found in Peplink Surf SOHO HW1 6.3.5. It has been classified as critical. This affects the function system of the file /web/MANGA/cgi-bin/api.cgi of the component HTTP Request Handler. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2023-35194. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-35193	Peplink Surf SOHO HW1 6.3.5 HTTP Request api.cgi os command injection (TALOS-2023-1782)	A vulnerability was found in Peplink Surf SOHO HW1 6.3.5 and classified as critical. Affected by this issue is some unknown functionality of the file /web/MANGA/cgi-bin/api.cgi of the component HTTP Request Handler. The manipulation leads to os command injection. This vulnerability is handled as CVE-2023-35193. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-27380	Peplink Surf SOHO HW1 6.3.5 HTTP Request admin.cgi USSD_send os command injection (TALOS-2023-1780)	A vulnerability which was classified as critical was found in Peplink Surf SOHO HW1 6.3.5. This affects the function USSD_send of the file admin.cgi of the component HTTP Request Handler. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2023-27380. It is possible to initiate the attack remotely.	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		There is no exploit available.		
CVE-2023-34356	Peplink Surf SOHO HW1 6.3.5 HTTP Request data.cgi xfer_dns os command injection (TALOS-2023-1778)	A vulnerability classified as critical has been found in Peplink Surf SOHO HW1 6.3.5. This affects the function xfer_dns of the file data.cgi of the component HTTP Request Handler. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2023-34356. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-28381	Peplink Surf SOHO HW1 6.3.5 HTTP Request admin.cgi MVPN_trial_init os command injection (TALOS-2023-1779)	A vulnerability has been found in Peplink Surf SOHO HW1 6.3.5 and classified as critical. This vulnerability affects the function MVPN_trial_init of the file admin.cgi of the component HTTP Request Handler. The manipulation leads to os command injection. This vulnerability was named CVE-2023-28381. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-45466	Netis N3Mv2 1.0.1.865 WPS Setting pin_host command injection	A vulnerability was found in Netis N3Mv2 1.0.1.865. It has been rated as critical. Affected by this issue is some unknown functionality of the component WPS Setting Handler. The manipulation of the argument pin_host leads to command injection. This vulnerability is handled as CVE-2023-45466. 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-2023-45465	Netis N3Mv2 1.0.1.865 Dynamic DNS Setting ddnsDomainName command injection	A vulnerability was found in Netis N3Mv2 1.0.1.865 and classified as critical. This issue affects some unknown processing of the component Dynamic DNS Setting Handler. The manipulation of the argument ddnsDomainName leads to command injection. The identification of this vulnerability is CVE-2023-45465. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-45467	Netis N3Mv2 1.0.1.865 Time Setting ntpServIP command injection	A vulnerability was found in Netis N3Mv2 1.0.1.865. It has been classified as critical. Affected is an unknown function of the component Time Setting Handler. The manipulation of the argument ntpServIP leads to command injection. This vulnerability is traded as CVE-2023-45467. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-26155	node-qpdf API encrypt command injection (Issue 23)	A vulnerability has been found in node-qpdf and classified as critical. Affected by this vulnerability is the function encrypt of the	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component API. The manipulation leads to command injection. This vulnerability is known as CVE-2023-26155. The attack can be launched remotely. There is no exploit available.		
CVE-2023-45852	Viessmann Vitogate 300 2.1.3.0 /cgi-bin/vitogate.cgi ipaddr os command injection	A vulnerability which was classified as critical has been found in Viessmann Vitogate 300 2.1.3.0. Affected by this issue is the function ipaddr of the file /cgi-bin/vitogate.cgi. The manipulation leads to os command injection. This vulnerability is handled as CVE-2023-45852. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-36954	Totolink CP300+ up to 5.2cu.7594_B20200910 command injection	A vulnerability classified as critical has been found in Totolink CP300+ up to 5.2cu.7594_B20200910. Affected is an unknown function. The manipulation leads to command injection. This vulnerability is traded as CVE-2023-36954. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-36953	Totolink CP300+ up to 5.2cu.7594_B20200910 command injection	A vulnerability was found in Totolink CP300+ up to 5.2cu.7594_B20200910. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to command injection. The identification of this vulnerability is CVE-2023-36953. 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.

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-35793	Cassia Access Controller 2.1.1.2303271039 Web SSH Session cross-site request forgery	A vulnerability was found in Cassia Access Controller 2.1.1.2303271039. It has been classified as problematic. Affected is an unknown function of the component Web SSH Session Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-35793. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-41452	phpkobo AjaxNewTicker 1.0.5 index.php txt cross-site request forgery	A vulnerability which was classified as problematic has been found in phpkobo AjaxNewTicker 1.0.5. Affected by this issue is some unknown functionality of the file index.php. The manipulation of the argument txt leads to cross-site request forgery. This vulnerability is handled as CVE-2023-41452. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-5498	chiefonboarding up to 2.0.46 cross-site request forgery	A vulnerability has been found in chiefonboarding up to 2.0.46 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-5498. 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-2023-5511	Snipe-IT up to 6.2.3 cross-site request forgery	A vulnerability classified as problematic was found in Snipe-IT up to 6.2.3. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-5511. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-43147	PHP Jabbers Limo Booking Software 1.0 index.php cross-site request forgery	A vulnerability classified as problematic was found in PHP Jabbers Limo Booking Software 1.0. Affected by this vulnerability is an unknown functionality of the file index.phpcontrollerpjAdminUsers&actionpjActionCreate. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-43147. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-43148	SPA-Cart 1.9.0.3 cross-site request forgery	A vulnerability which was classified as problematic has been found in SPA-Cart 1.9.0.3. This issue affects some unknown processing. The manipulation leads to cross-site request forgery.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The identification of this vulnerability is CVE-2023-43148. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-43149	SPA-Cart 1.9.0.3 cross-site request forgery	A vulnerability classified as problematic was found in SPA-Cart 1.9.0.3. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-43149. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-45901	Dreamer CMS 4.1.3 /admin/category/add cross-site request forgery	A vulnerability has been found in Dreamer CMS 4.1.3 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/category/add. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-45901. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-45907	Dreamer CMS 4.1.3 /admin/variable/delete cross-site request forgery	A vulnerability classified as problematic was found in Dreamer CMS 4.1.3. Affected by this vulnerability is an unknown functionality of the file /admin/variable/delete. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-45907. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-45905	Dreamer CMS 4.1.3 /admin/variable/add cross-site request forgery	A vulnerability was found in Dreamer CMS 4.1.3. It has been rated as problematic. This issue affects some unknown processing of the file /admin/variable/add. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-45905. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-45902	Dreamer CMS 4.1.3 /admin/attachment/delete cross-site request forgery	A vulnerability was found in Dreamer CMS 4.1.3 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/attachment/delete. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-45902. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-45906	Dreamer CMS 4.1.3 /admin/user/add cross-site request forgery	A vulnerability classified as problematic has been found in Dreamer CMS 4.1.3. Affected is an unknown function of the file /admin/user/add. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-45906. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-45904	Dreamer CMS 4.1.3	A vulnerability was found in	Protected by	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	/variable/update cross-site request forgery	Dreamer CMS 4.1.3. It has been declared as problematic. This vulnerability affects unknown code of the file /variable/update. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-45904. The attack can be initiated remotely. There is no exploit available.	core rules	
CVE-2023-45903	Dreamer CMS 4.1.3 /admin/label/delete cross-site request forgery	A vulnerability was found in Dreamer CMS 4.1.3. It has been classified as problematic. This affects an unknown part of the file /admin/label/delete. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-45903. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-5626	pkp ojs up to 3.3.0-15 cross-site request forgery	A vulnerability has been found in pkp ojs up to 3.3.0-15 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-5626. The attack can be launched 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-2023-43662	ShokoServer /api/Image/WithPath System.IO.File.OpenRead serverImagePath path traversal (GHSA-mwcv-ghjq-8f2g)	A vulnerability was found in ShokoServer. It has been rated as critical. Affected by this issue is the function System.IO.File.OpenRead of the file /api/Image/WithPath. The manipulation of the argument serverImagePath leads to path traversal. This vulnerability is handled as CVE-2023-43662. The attack may be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-5257	WhiteHSBG JNDIExploit 1.4 on Windows HTTPServer.java handleFileRequest path traversal	A vulnerability was found in WhiteHSBG JNDIExploit 1.4 on Windows. It has been rated as problematic. Affected by this issue is the function handleFileRequest of the file src/main/java/com/feihong/ldap/HTTPServer.java. The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-5257. The attack needs to be done within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-26152	static-server server.js validPath path traversal	A vulnerability was found in static-server. It has been rated as critical. This issue affects the function validPath of the file server.js. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-26152. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-36123	Hex-Dragon Plain Craft Launcher 2 1.3.9 path traversal	A vulnerability was found in Hex-Dragon Plain Craft Launcher 2 1.3.9. It has been classified as critical. This affects an unknown part. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-36123. Attacking locally is a requirement. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-45855	qdPM 9.2 /uploads path traversal	A vulnerability was found in qdPM 9.2. It has been classified as problematic. This affects an unknown part of the file /uploads. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-45855. The attack needs to be initiated within the local network. There	Protected by core rules	Detected by scanner as local file inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		is no exploit available.		
CVE-2023-45689	South River MFT Server/Titan SFTP Server on Windows path traversal	A vulnerability has been found in South River MFT Server and Titan SFTP Server on Windows and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to path traversal. This vulnerability is known as CVE-2023-45689. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-45686	South River MFT Server/Titan SFTP Server on Linux path traversal	A vulnerability classified as critical was found in South River MFT Server and Titan SFTP Server on Linux. This vulnerability affects unknown code. The manipulation leads to path traversal. This vulnerability was named CVE-2023-45686. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-45685	South River MFT Server/Titan SFTP Server on Windows path traversal	A vulnerability classified as critical has been found in South River MFT Server and Titan SFTP Server on Windows. This affects an unknown part. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-45685. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-45688	South River MFT Server/Titan SFTP Server on Linux SIZE Command path traversal	A vulnerability which was classified as critical was found in South River MFT Server and Titan SFTP Server on Linux. Affected is an unknown function of the component SIZE Command Handler. The manipulation leads to path traversal. This vulnerability is traded as CVE-2023-45688. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-41629	eSST Monitoring 2.147.1 File Download path traversal	A vulnerability which was classified as critical was found in eSST Monitoring 2.147.1. This affects an unknown part of the component File Download Handler. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-41629. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-43226	DedeCMS up to 5.7.111 dede/baidunews.php unrestricted upload	A vulnerability was found in DedeCMS up to 5.7.111. It has been rated as problematic. Affected by this issue is some unknown functionality of the file dede/baidunews.php. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-43226. The attack can only be initiated within the local network. There is no exploit available.	Protected by custom rules	NA
CVE-2023-30415	Sourcecodester Packers and Movers Management System 1.0 view_inquiry.php id sql injection (ID 174758)	A vulnerability was found in Sourcecodester Packers and Movers Management System 1.0. It has been classified as critical. This affects an unknown part of the file /inquiries/view_inquiry.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-30415. Access to the local network is required for this attack. There is no exploit available.	Protected by custom rules	NA
CVE-2023-38874	gugoan Economizzer 0.9-beta1 Cash Book Entry unrestricted upload	A vulnerability was found in gugoan Economizzer 0.9-beta1. It has been rated as critical. This issue affects some unknown processing of the component Cash Book Entry Handler. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2023-38874. The attack may be initiated remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2023-5185	Gym Management System 1.0 profile/i.php file unrestricted upload	A vulnerability was found in Gym Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file profile/i.php. The manipulation of the argument file leads to unrestricted upload. The identification of this vulnerability is CVE-2023-5185. The attack may be initiated remotely. There is no exploit available.	Protected by custom rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-5277	SourceCodester Engineers Online Portal 1.0 student_avatar.php change unrestricted upload	A vulnerability which was classified as critical has been found in SourceCodester Engineers Online Portal 1.0. This issue affects some unknown processing of the file student_avatar.php. The manipulation of the argument change leads to unrestricted upload. The identification of this vulnerability is CVE-2023-5277. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by custom rules	NA
CVE-2023-5284	SourceCodester Engineers Online Portal 1.0 upload_save_student.php uploaded_file unrestricted upload	A vulnerability classified as critical has been found in SourceCodester Engineers Online Portal 1.0. Affected is an unknown function of the file upload_save_student.php. The manipulation of the argument uploaded_file leads to unrestricted upload. This vulnerability is traded as CVE-2023-5284. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by custom rules	NA
CVE-2023-5263	ZZZCMS 2.1.7 Database Backup File /admin/save.php restore permission	A vulnerability was found in ZZZCMS 2.1.7 and classified as critical. Affected by this issue is the function restore of the file /admin/save.php of the component Database Backup File Handler. The manipulation leads to permission issues. This vulnerability is handled as CVE-2023-5263. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by custom rules	NA
CVE-2023-5262	OpenRapid RapidCMS 1.3.1 uploadicon.php isImg fileName unrestricted upload	A vulnerability has been found in OpenRapid RapidCMS 1.3.1 and classified as critical. Affected by this vulnerability is the function isImg of the file /admin/config/uploadicon.php. The manipulation of the argument fileName leads to unrestricted upload. This vulnerability is known as CVE-2023-5262. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by custom rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-43740	Online Book Store 1.0 unrestricted upload	A vulnerability has been found in Online Book Store 1.0 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-43740. The attack can be initiated remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2023-44008	mojoPortal 2.7.0.0 File Manager unrestricted upload	A vulnerability was found in mojoPortal 2.7.0.0. It has been rated as critical. Affected by this issue is some unknown functionality of the component File Manager. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-44008. The attack may be launched remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2023-44009	mojoPortal 2.7.0.0 Skin Management unrestricted upload	A vulnerability classified as critical has been found in mojoPortal 2.7.0.0. This affects an unknown part of the component Skin Management. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-44009. It is possible to initiate the attack remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2023-44974	Emlog Pro 2.2.0 PHP File /admin/plugin.php unrestricted upload	A vulnerability has been found in Emlog Pro 2.2.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/plugin.php of the component PHP File Handler. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2023-44974. The attack needs to be approached within the local network. There is no exploit available.	Protected by custom rules	NA
CVE-2023-44973	Emlog Pro 2.2.0 PHP File /content/templates/ unrestricted upload	A vulnerability which was classified as critical was found in Emlog Pro 2.2.0. Affected is an unknown function of the file /content/templates/ of the component PHP File Handler. The manipulation leads to unrestricted upload.	Protected by custom rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is traded as CVE-2023-44973. Access to the local network is required for this attack to succeed. There is no exploit available.		
CVE-2023-43838	Personal Management System 1.4.64 SVG unrestricted upload	A vulnerability classified as critical has been found in Personal Management System 1.4.64. Affected is an unknown function of the component SVG Handler. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2023-43838. The attack needs to be initiated within the local network. There is no exploit available.	Protected by custom rules	NA
CVE-2023-43321	Digital China Networks DCFW-1800-SDC 3.0 /sbin/cloudadmin.sh wget unrestricted upload	A vulnerability classified as problematic has been found in Digital China Networks DCFW-1800-SDC 3.0. This affects the function wget of the file /sbin/cloudadmin.sh. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-43321. The attack needs to be done within the local network. There is no exploit available.	Protected by custom rules	NA

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-38870	gugoan Economizzer 0.9-beta1 category_id sql injection	A vulnerability was found in gugoan Economizzer 0.9-beta1. It has been declared as critical. This vulnerability affects unknown code. The manipulation of the argument category_id leads to sql injection. This vulnerability was named CVE-2023-38870. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-44047	SourceCodester Toll Tax Management System 1.0 sql injection	A vulnerability was found in SourceCodester Toll Tax Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-44047. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-43192	jfinal_cms sql injection	A vulnerability was found in jfinal_cms and classified as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-43192. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-43013	Asset Management System 1.0 index.php email sql injection	A vulnerability was found in Asset Management System 1.0. It has been classified as critical. Affected is an unknown function of the file index.php. The manipulation of the argument email leads to sql injection. This vulnerability is traded as CVE-2023-43013. 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-2023-5267	Tongda OA 2017 prior 11.10 delete.php EXPERT_ID sql injection	A vulnerability has been found in Tongda OA 2017 and classified as critical. This vulnerability affects unknown code of the file general/hr/recruit/hr_pool/delete.php. The manipulation of the argument EXPERT_ID leads to sql injection. This vulnerability was named CVE-2023-5267. The attack needs to be done within the local network. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-5266	DedeBIZ 6.2 /src/admin/tags_main.php ids sql injection	A vulnerability which was classified as critical was found in DedeBIZ 6.2. This affects an unknown part of the file /src/admin/tags_main.php. The manipulation of the argument ids leads to sql	Protected by core rules	Detected by scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		injection. This vulnerability is uniquely identified as CVE-2023-5266. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2023-5265	Tongda OA 2017 prior 11.10 delete.php TRANSFER_ID sql injection	A vulnerability which was classified as critical has been found in Tongda OA 2017. Affected by this issue is some unknown functionality of the file general/hr/manage/staff_transfer/delete.php. The manipulation of the argument TRANSFER_ID leads to sql injection. This vulnerability is handled as CVE-2023-5265. The attack can only be done within the local network. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-5298	Tongda OA 2017 prior 11.10 delete.php REQUIREMENTS_ID sql injection	A vulnerability was found in Tongda OA 2017. It has been rated as critical. Affected by this issue is some unknown functionality of the file general/hr/recruit/requirements/delete.php. The manipulation of the argument REQUIREMENTS_ID leads to sql injection. This vulnerability is handled as CVE-2023-5298. Access to the local network is required for this attack. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-44163	Online Movie Ticket Booking System 1.0 process_search.php search sql injection	A vulnerability classified as critical has been found in Online Movie Ticket Booking System 1.0. This affects an unknown part of the file process_search.php. The manipulation of the argument search leads to sql injection. This vulnerability is uniquely identified as CVE-2023-44163. 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-2023-43739	Online Book Store 1.0 cart.php bookisbn sql injection	A vulnerability classified as critical was found in Online Book Store 1.0. This vulnerability affects unknown code of the file cart.php. The manipulation of the argument bookisbn leads to sql injection. This vulnerability was named CVE-2023-43739. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-44164	Online Movie Ticket Booking System 1.0 process_login.php Email sql injection	A vulnerability which was classified as critical has been found in Online Movie Ticket Booking System 1.0. This issue affects some unknown processing of the file process_login.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 Email leads to sql injection. The identification of this vulnerability is CVE-2023-44164. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-44165	Online Movie Ticket Booking System 1.0 process_login.php Password sql injection	A vulnerability which was classified as critical was found in Online Movie Ticket Booking System 1.0. Affected is an unknown function of the file process_login.php. The manipulation of the argument Password leads to sql injection. This vulnerability is traded as CVE-2023-44165. 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-2023-43014	Asset Management System 1.0 user.php first_name/last_name sql injection	A vulnerability was found in Asset Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file user.php. The manipulation of the argument first_name/last_name leads to sql injection. This vulnerability is known as CVE-2023-43014. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-5283	SourceCodester Engineers Online Portal 1.0 teacher_signup.php firstname/lastname sql injection	A vulnerability was found in SourceCodester Engineers Online Portal 1.0. It has been rated as critical. This issue affects some unknown processing of the file teacher_signup.php. The manipulation of the argument firstname/lastname leads to sql injection. The identification of this vulnerability is CVE-2023-5283. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-5282	SourceCodester Engineers Online Portal 1.0 seed_message_student.php teacher_id sql injection	A vulnerability was found in SourceCodester Engineers Online Portal 1.0. It has been declared as critical. This vulnerability affects unknown code of the file seed_message_student.php. The manipulation of the argument teacher_id leads to sql injection. This vulnerability was named CVE-2023-5282. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-5281	SourceCodester Engineers Online Portal 1.0 remove_inbox_message.php id sql injection	A vulnerability was found in SourceCodester Engineers Online Portal 1.0. It has been classified as critical. This affects an unknown part of the file remove_inbox_message.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-5281.	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-2023-5280	SourceCodester Engineers Online Portal 1.0 my_students.php id sql injection	A vulnerability was found in SourceCodester Engineers Online Portal 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file my_students.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-5280. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-5279	SourceCodester Engineers Online Portal 1.0 my_classmates.php teacher_class_student_id sql injection	A vulnerability has been found in SourceCodester Engineers Online Portal 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file my_classmates.php. The manipulation of the argument teacher_class_student_id leads to sql injection. This vulnerability is known as CVE-2023-5279. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-5278	SourceCodester Engineers Online Portal 1.0 login.php username/password sql injection	A vulnerability which was classified as critical was found in SourceCodester Engineers Online Portal 1.0. Affected is an unknown function of the file login.php. The manipulation of the argument username/password leads to sql injection. This vulnerability is traded as CVE-2023-5278. 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-2023-5276	SourceCodester Engineers Online Portal 1.0 downloadable_student.php id sql injection	A vulnerability classified as critical was found in SourceCodester Engineers Online Portal 1.0. This vulnerability affects unknown code of the file downloadable_student.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-5276. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-5285	Tongda OA 2017 prior 11.10 delete.php RECRUITMENT_ID sql injection	A vulnerability classified as critical was found in Tongda OA 2017. Affected by this vulnerability is an unknown functionality of the file general/hr/recruit/recruitment/delete.php. The manipulation of the argument RECRUITMENT_ID leads to sql injection. This vulnerability is known as CVE-2023-5285. The attack can be launched remotely. Furthermore there is an exploit available. It is recommended to	Protected by core rules	Detected by scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		upgrade the affected component.		
CVE-2023-5268	DedeBIZ 6.2 makehtml_taglist_action.php mktime sql injection	A vulnerability was found in DedeBIZ 6.2 and classified as critical. This issue affects some unknown processing of the file /src/admin/makehtml_taglist_action.php. The manipulation of the argument mktime leads to sql injection. The identification of this vulnerability is CVE-2023-5268. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-5294	ECshop 4.1.1 /admin/order.php goods_id sql injection	A vulnerability has been found in ECshop 4.1.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/order.php. The manipulation of the argument goods_id leads to sql injection. This vulnerability is known as CVE-2023-5294. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-43909	Hospital Management System up to 4770d appsearch.php app_contact sql injection	A vulnerability has been found in Hospital Management System up to 4770d and classified as critical. This vulnerability affects unknown code of the file appsearch.php. The manipulation of the argument app_contact leads to sql injection. This vulnerability was named CVE-2023-43909. 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-2023-5293	ECshop 4.1.5 /admin/leancloud.php id sql injection	A vulnerability which was classified as critical was found in ECshop 4.1.5. Affected is an unknown function of the file /admin/leancloud.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-5293. 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-2023-5269	SourceCodester Best Courier Management System 1.0 GET Parameter parcel_list.php s sql injection	A vulnerability was found in SourceCodester Best Courier Management System 1.0. It has been classified as critical. Affected is an unknown function of the file parcel_list.php of the component GET Parameter Handler. The manipulation of the argument s leads to sql injection. This vulnerability is traded as CVE-2023-5269. Access to the local network is required for this attack. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-5271	SourceCodester Best Courier Management System 1.0 edit_parcel.php email sql	A vulnerability was found in SourceCodester Best Courier Management System 1.0. It has been rated as critical.	Protected by core rules	Detected by scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	Affected by this issue is some unknown functionality of the file edit_parcel.php. The manipulation of the argument email leads to sql injection. This vulnerability is handled as CVE-2023-5271. The attack needs to be approached within the local network. Furthermore there is an exploit available.		
CVE-2023-5264	huakecms 3.0 /admin/cms_content.php cid sql injection	A vulnerability classified as critical was found in huakecms 3.0. Affected by this vulnerability is an unknown functionality of the file /admin/cms_content.php. The manipulation of the argument cid leads to sql injection. This vulnerability is known as CVE-2023-5264. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-5261	Tongda OA 2017 prior 11.10 delete.php EVALUATION_ID sql injection	A vulnerability which was classified as critical was found in Tongda OA 2017. Affected is an unknown function of the file general/hr/manage/staff_title_evaluation/delete.php. The manipulation of the argument EVALUATION_ID leads to sql injection. This vulnerability is traded as CVE-2023-5261. The attack needs to be approached within the local network. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-5260	SourceCodester Simple Membership System 1.0 group_validator.php club_id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Simple Membership System 1.0. This issue affects some unknown processing of the file group_validator.php. The manipulation of the argument club_id leads to sql injection. The identification of this vulnerability is CVE-2023-5260. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-5258	OpenRapid RapidCMS 1.3.1 /resource/addgood.php sql injection	A vulnerability classified as critical has been found in OpenRapid RapidCMS 1.3.1. This affects an unknown part of the file /resource/addgood.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-5258. 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-2023-5270	SourceCodester Best Courier Management System 1.0 view_parcel.php id sql	A vulnerability was found in SourceCodester Best Courier Management System 1.0. It has been declared as critical.	Protected by core rules	Detected by scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	Affected by this vulnerability is an unknown functionality of the file view_parcel.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-5270. Access to the local network is required for this attack to succeed. Furthermore there is an exploit available.		
CVE-2023-5004	Hospital Management System 378c157 sql injection	A vulnerability which was classified as critical has been found in Hospital Management System 378c157. Affected by this issue is some unknown functionality. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-5004. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-44168	Online Movie Ticket Booking System 1.0 process_registration.php phone sql injection	A vulnerability classified as critical has been found in Online Movie Ticket Booking System 1.0. Affected is an unknown function of the file process_registration.php. The manipulation of the argument phone leads to sql injection. This vulnerability is traded as CVE-2023-44168. 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-2023-44167	Online Movie Ticket Booking System 1.0 process_registration.php name sql injection	A vulnerability was found in Online Movie Ticket Booking System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file process_registration.php. The manipulation of the argument name leads to sql injection. This vulnerability is handled as CVE-2023-44167. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-44166	Online Movie Ticket Booking System 1.0 process_registration.php age sql injection	A vulnerability has been found in Online Movie Ticket Booking System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file process_registration.php. The manipulation of the argument age leads to sql injection. This vulnerability is known as CVE-2023-44166. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-5053	Hospital Management System 378c157 sql injection	A vulnerability was found in Hospital Management System 378c157 and classified as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-	Protected by core rules	Detected by scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		5053. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-5272	SourceCodester Best Courier Management System 1.0 GET Parameter edit_parcel.php id sql injection	A vulnerability classified as critical has been found in SourceCodester Best Courier Management System 1.0. This affects an unknown part of the file edit_parcel.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-5272. 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-2023-5322	D-Link DAR-7000 up to 20151231 edit_manageadmin.php id sql injection	A vulnerability was found in D-Link DAR-7000 up to 20151231. It has been rated as critical. Affected by this issue is some unknown functionality of the file /sysmanage/edit_manageadmin.php. The manipulation of the argument id leads to sql injection. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is handled as CVE-2023-5322. The attack may be launched remotely. Furthermore there is an exploit available. Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. It is recommended to disable the affected component.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-43836	JIZHICMS 2.4.9 sql injection	A vulnerability classified as critical was found in JIZHICMS 2.4.9. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-43836. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-5350	SalesAgility SuiteCRM up to 7.14.0 sql injection	A vulnerability was found in SalesAgility SuiteCRM up to 7.14.0. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to sql injection. This vulnerability was named CVE-2023-5350. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2023-5374	SourceCodester Online Computer and Laptop Store 1.0 products.php c sql injection	A vulnerability classified as critical was found in SourceCodester Online Computer and Laptop Store 1.0. Affected by this vulnerability is an unknown functionality of the file products.php. The	Protected by core rules	Detected by scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument c leads to sql injection. This vulnerability is known as CVE-2023-5374. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2023-5373	SourceCodester Online Computer and Laptop Store 1.0 Master.php register email sql injection	A vulnerability classified as critical has been found in SourceCodester Online Computer and Laptop Store 1.0. Affected is the function register of the file Master.php. The manipulation of the argument email leads to sql injection. This vulnerability is traded as CVE-2023-5373. 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-2023-40920	Prixan prixanconnect up to 1.62 on PrestaShop importProducts sql injection	A vulnerability was found in Prixan prixanconnect up to 1.62 on PrestaShop and classified as critical. This issue affects the function CartsGuruCatalogModuleFrontController::importProducts. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-40920. 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

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-4646	Simple Posts Ticker Plugin up to 1.1.5 on WordPress Shortcode cross-site scripting	A vulnerability was found in Simple Posts Ticker Plugin up to 1.1.5 on WordPress. It has been classified as problematic. Affected is an unknown function of the component Shortcode Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-4646. 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-2023-4725	Simple Posts Ticker Plugin up to 1.1.5 on WordPress cross-site scripting	A vulnerability has been found in Simple Posts Ticker Plugin up to 1.1.5 on WordPress and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-4725. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-5167	User Activity Log Pro Plugin up to 2.3.3 on WordPress Header User-Agent cross-site scripting	A vulnerability was found in User Activity Log Pro Plugin up to 2.3.3 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Header Handler. The manipulation of the argument User-Agent leads to cross-site scripting. This vulnerability is known as CVE-2023-5167. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-4798	User Avatar Plugin up to 1.2.1 on WordPress Shortcode cross-site scripting	A vulnerability was found in User Avatar Plugin up to 1.2.1 on WordPress and classified as problematic. This issue affects some unknown processing of the component Shortcode Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-4798. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43326	mooSocial 3.1.8 Change Email cross-site scripting	A vulnerability was found in mooSocial 3.1.8. It has been classified as problematic. This affects an unknown part of the component Change Email. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-43326. 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-2023-42426	Froala Editor 4.1.1 Insert Image Insert link cross-site scripting	A vulnerability which was classified as problematic has been found in Froala Editor 4.1.1. This issue affects some unknown processing of the component Insert Image. The manipulation of the argument Insert link 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
		The identification of this vulnerability is CVE-2023-42426. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-43325	mooSocial 3.1.8 URL data[redirect_url] cross-site scripting	A vulnerability was found in mooSocial 3.1.8. It has been rated as problematic. This issue affects some unknown processing of the component URL Handler. The manipulation of the argument data[redirect_url] leads to cross-site scripting. The identification of this vulnerability is CVE-2023-43325. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43458	Resort Reservation System 1.0 room/name/description cross-site scripting	A vulnerability has been found in Resort Reservation System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument room/name/description leads to cross-site scripting. This vulnerability is known as CVE-2023-43458. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43319	Icewarp WebClient 10.3.5 Sign-In Page username cross-site scripting	A vulnerability was found in Icewarp WebClient 10.3.5 and classified as problematic. Affected by this issue is some unknown functionality of the component Sign-In Page. The manipulation of the argument username leads to cross-site scripting. This vulnerability is handled as CVE-2023-43319. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-3746	ActivityPub Plugin up to 0.17.0 on WordPress Post Content cross-site scripting	A vulnerability was found in ActivityPub Plugin up to 0.17.0 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Post Content Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-3746. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43263	Froala Editor 4.1.1 Markdown cross-site scripting	A vulnerability was found in Froala Editor 4.1.1. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Markdown. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-43263. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43857	Dreamer CMS 4.1.3 /admin/u/toIndex cross-	A vulnerability was found in Dreamer CMS 4.1.3 and	Protected by core rules	Detected by scanner as cross-

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	site scripting	classified as problematic. This issue affects some unknown processing of the file /admin/u/toIndex. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-43857. The attack may be initiated remotely. There is no exploit available.		site scripting attack
CVE-2023-44275	OPNsense up to 23.7.4 Lobby Dashboard index.php column_count cross-site scripting	A vulnerability which was classified as problematic has been found in OPNsense up to 23.7.4. This issue affects some unknown processing of the file index.php of the component Lobby Dashboard. The manipulation of the argument column_count leads to cross-site scripting. The identification of this vulnerability is CVE-2023-44275. 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-2023-44276	OPNsense up to 23.7.4 Lobby Dashboard index.php cross-site scripting	A vulnerability which was classified as problematic was found in OPNsense up to 23.7.4. Affected is an unknown function of the file index.php of the component Lobby Dashboard. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-44276. 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-2023-41445	phpkobo AjaxNewTicker 1.0.5 index.php cross-site scripting	A vulnerability which was classified as problematic has been found in phpkobo AjaxNewTicker 1.0.5. Affected by this issue is some unknown functionality of the file index.php. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-41445. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43191	jfinal_cms cross-site scripting	A vulnerability was found in jfinal_cms. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-43191. 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-2023-43876	October 3.4.16 Installation dbhost cross-site scripting	A vulnerability classified as problematic was found in October 3.4.16. Affected by this vulnerability is an unknown functionality of the component Installation. The manipulation of the argument dbhost leads to	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross-site scripting. This vulnerability is known as CVE-2023-43876. The attack can be launched remotely. There is no exploit available.		
CVE-2023-26149	quill-mention up to 3.x renderList cross-site scripting (Issue 255)	A vulnerability was found in quill-mention up to 3.x. It has been declared as problematic. This vulnerability affects the function renderList. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-26149. 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-2023-43879	Rite CMS 3.0 Administration Menu cross-site scripting	A vulnerability classified as problematic has been found in Rite CMS 3.0. Affected is an unknown function of the component Administration Menu. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-43879. 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-2023-43884	Subrion 4.2.1 Reference ID cross-site scripting	A vulnerability was found in Subrion 4.2.1. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument Reference ID leads to cross-site scripting. This vulnerability was named CVE-2023-43884. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43878	Rite CMS 3.0 Administration Menu cross-site scripting	A vulnerability was found in Rite CMS 3.0. It has been rated as problematic. This issue affects some unknown processing of the component Administration Menu. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-43878. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-41448	phpkobo AjaxNewTicker 1.0.5 index.php ID cross-site scripting	A vulnerability classified as problematic has been found in phpkobo AjaxNewTicker 1.0.5. Affected is an unknown function of the file index.php. The manipulation of the argument ID leads to cross-site scripting. This vulnerability is traded as CVE-2023-41448. 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-2023-43871	WBCE 1.6.1 File Upload cross-site scripting	A vulnerability was found in WBCE 1.6.1. It has been rated as problematic. This issue affects some unknown processing of the component File Upload 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
		The identification of this vulnerability is CVE-2023-43871. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-43874	e017 CMS 2.3.2 Meta/Custom Tags Menu Copyright/Author cross-site scripting	A vulnerability was found in e017 CMS 2.3.2. It has been declared as problematic. This vulnerability affects unknown code of the component Meta/Custom Tags Menu. The manipulation of the argument Copyright/Author leads to cross-site scripting. This vulnerability was named CVE-2023-43874. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43872	CMS Made Simple 2.2.18 File Upload cross-site scripting	A vulnerability classified as problematic has been found in CMS Made Simple 2.2.18. Affected is an unknown function of the component File Upload Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-43872. 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-2023-41447	phpkobo AjaxNewTicker 1.0.5 index.php subcmd cross-site scripting	A vulnerability was found in phpkobo AjaxNewTicker 1.0.5 and classified as problematic. This issue affects some unknown processing of the file index.php. The manipulation of the argument subcmd leads to cross-site scripting. The identification of this vulnerability is CVE-2023-41447. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-41446	phpkobo AjaxNewTicker 1.0.5 index.php title cross-site scripting	A vulnerability has been found in phpkobo AjaxNewTicker 1.0.5 and classified as problematic. This vulnerability affects unknown code of the file index.php. The manipulation of the argument title leads to cross-site scripting. This vulnerability was named CVE-2023-41446. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-41453	phpkobo AjaxNewTicker 1.0.5 index.php cmd cross-site scripting	A vulnerability which was classified as problematic was found in phpkobo AjaxNewTicker 1.0.5. This affects an unknown part of the file index.php. The manipulation of the argument cmd leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-41453. 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-2023-41451	phpkobo AjaxNewTicker 1.0.5 index.php txt cross-site scripting	A vulnerability classified as problematic was found in phpkobo AjaxNewTicker 1.0.5. Affected by this vulnerability is an unknown functionality of the file index.php. The manipulation	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the argument txt leads to cross-site scripting. This vulnerability is known as CVE-2023-41451. The attack can be launched remotely. There is no exploit available.		
CVE-2023-43873	e017 CMS 2.3.2 Manage Menu Name cross-site scripting	A vulnerability classified as problematic was found in e017 CMS 2.3.2. Affected by this vulnerability is an unknown functionality of the component Manage Menu. The manipulation of the argument Name leads to cross-site scripting. This vulnerability is known as CVE-2023-43873. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-44048	SourceCodester Expense Tracker App 1.0 Add Category cross-site scripting	A vulnerability was found in SourceCodester Expense Tracker App 1.0. It has been classified as problematic. This affects an unknown part of the component Add Category Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-44048. 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-2023-5302	SourceCodester Best Courier Management System 1.0 Manage Account Page First Name cross-site scripting	A vulnerability which was classified as problematic has been found in SourceCodester Best Courier Management System 1.0. This issue affects some unknown processing of the component Manage Account Page. The manipulation of the argument First Name leads to cross-site scripting. The identification of this vulnerability is CVE-2023-5302. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-5273	SourceCodester Best Courier Management System 1.0 manage_parcel_status.php id cross-site scripting	A vulnerability classified as problematic was found in SourceCodester Best Courier Management System 1.0. This vulnerability affects unknown code of the file manage_parcel_status.php. The manipulation of the argument id leads to cross-site scripting. This vulnerability was named CVE-2023-5273. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-39308	UserFeedback User Feedback Plugin up to 1.0.7 on WordPress cross-site scripting	A vulnerability was found in UserFeedback User Feedback Plugin up to 1.0.7 on WordPress and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-39308. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-43944	SourceCodester Task Management System 1.0 index.php cross-site scripting	A vulnerability was found in SourceCodester Task Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file index.phppageproject_list. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-43944. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-5287	BEECMS 4.0 admin_content_tag.php tag cross-site scripting	A vulnerability which was classified as problematic was found in BEECMS 4.0. This affects an unknown part of the file /admin/admin_content_tag.phpactionsave_content. The manipulation of the argument tag leads to cross-site scripting. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is uniquely identified as CVE-2023-5287. 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-2023-44174	Online Movie Ticket Booking System 1.0 cross-site scripting	A vulnerability was found in Online Movie Ticket Booking System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-44174. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-44173	Online Movie Ticket Booking System 1.0 cross-site scripting	A vulnerability was found in Online Movie Ticket Booking System 1.0. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-44173. 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-2023-26146	ithewei libhv File Name cross-site scripting	A vulnerability classified as problematic has been found in ithewei libhv. Affected is an unknown function of the component File Name Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-26146. 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-2023-43705	Os Commerce translation_value[1] cross-site scripting	A vulnerability classified as problematic was found in Os Commerce. This vulnerability affects unknown code. The manipulation of the argument translation_value[1] leads to cross-site scripting. This vulnerability was named	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2023-43705. The attack can be initiated remotely. There is no exploit available.		
CVE-2023-5057	ActivityPub Plugin up to 0.17.0 on WordPress Metadata cross-site scripting	A vulnerability which was classified as problematic was found in ActivityPub Plugin up to 0.17.0 on WordPress. This affects an unknown part of the component Metadata Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-5057. 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-2023-43706	Os Commerce email_templates_key cross-site scripting	A vulnerability which was classified as problematic has been found in Os Commerce. This issue affects some unknown processing. The manipulation of the argument email_templates_key leads to cross-site scripting. The identification of this vulnerability is CVE-2023-43706. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43704	Os Commerce title cross-site scripting	A vulnerability classified as problematic has been found in Os Commerce. This affects an unknown part. The manipulation of the argument title leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-43704. 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-2023-43702	Os Commerce 4.12.56860 tracking_number cross-site scripting	A vulnerability was found in Os Commerce 4.12.56860. It has been classified as problematic. Affected is an unknown function. The manipulation of the argument tracking_number leads to cross-site scripting. This vulnerability is traded as CVE-2023-43702. 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-2023-43703	Os Commerce product_info[][name] cross-site scripting	A vulnerability was found in Os Commerce and classified as problematic. This issue affects some unknown processing. The manipulation of the argument product_info[][name] leads to cross-site scripting. The identification of this vulnerability is CVE-2023-43703. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43707	Os Commerce CatalogsPageDescriptionForm[1][name] cross-site scripting	A vulnerability classified as problematic has been found in Os Commerce. Affected is an unknown function. The manipulation of the argument CatalogsPageDescriptionForm[1][name] leads to cross-site scripting. This vulnerability is traded as CVE-2023-43707. It is	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		possible to launch the attack remotely. There is no exploit available.		
CVE-2023-43708	Os Commerce cross-site scripting	A vulnerability classified as problematic was found in Os Commerce. Affected by this vulnerability is an unknown functionality. The manipulation of the argument configuration_title[1] leads to cross-site scripting. This vulnerability is known as CVE-2023-43708. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43709	Os Commerce configuration_title[1](MODULE) cross-site scripting	A vulnerability which was classified as problematic has been found in Os Commerce. Affected by this issue is some unknown functionality. The manipulation of the argument configuration_title[1] leads to cross-site scripting. This vulnerability is handled as CVE-2023-43709. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43711	Os Commerce admin_firstname cross-site scripting	A vulnerability has been found in Os Commerce and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument admin_firstname leads to cross-site scripting. This vulnerability was named CVE-2023-43711. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43710	Os Commerce cross-site scripting	A vulnerability which was classified as problematic was found in Os Commerce. This affects an unknown part. The manipulation of the argument configuration_title[1][MODULE_SHIPPING_PERCENT_TEXT_TITLE] leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-43710. 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-2023-43944	SourceCodester Task Management System 1.0 index.php cross-site scripting	A vulnerability was found in SourceCodester Task Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file index.phppageproject_list. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-43944. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43708	Os Commerce cross-site scripting	A vulnerability classified as problematic was found in Os Commerce. Affected by this vulnerability is an unknown functionality. The manipulation of the argument	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		configuration_title[1] leads to cross-site scripting. This vulnerability is known as CVE-2023-43708. The attack can be launched remotely. There is no exploit available.		
CVE-2023-5057	ActivityPub Plugin up to 0.17.0 on WordPress Metadata cross-site scripting	A vulnerability which was classified as problematic was found in ActivityPub Plugin up to 0.17.0 on WordPress. This affects an unknown part of the component Metadata Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-5057. 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-2023-43732	Os Commerce tax_class_title cross-site scripting	A vulnerability was found in Os Commerce and classified as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument tax_class_title leads to cross-site scripting. This vulnerability is handled as CVE-2023-43732. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43726	Os Commerce orders_products_status_manual_name_long[1] cross-site scripting	A vulnerability was found in Os Commerce. It has been classified as problematic. Affected is an unknown function. The manipulation of the argument orders_products_status_manual_name_long[1] leads to cross-site scripting. This vulnerability is traded as CVE-2023-43726. 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-2023-43729	Os Commerce xsell_type_name[1] cross-site scripting	A vulnerability classified as problematic has been found in Os Commerce. This affects an unknown part. The manipulation of the argument xsell_type_name[1] leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-43729. 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-2023-43728	Os Commerce stock_delivery_terms_text[1] cross-site scripting	A vulnerability has been found in Os Commerce and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument stock_delivery_terms_text[1] leads to cross-site scripting. This vulnerability is known as CVE-2023-43728. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-5111	Os Commerce featured_type_name[1] cross-site scripting	A vulnerability classified as problematic has been found in Os Commerce. Affected is an unknown function. The manipulation of the argument	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		featured_type_name[1] leads to cross-site scripting. This vulnerability is traded as CVE-2023-5111. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2023-43731	Os Commerce zone_name cross-site scripting	A vulnerability which was classified as problematic has been found in Os Commerce. This issue affects some unknown processing. The manipulation of the argument zone_name leads to cross-site scripting. The identification of this vulnerability is CVE-2023-43731. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43715	Os Commerce ENTRY_FIRST_NAME_MIN_LENGTH_TITLE[1] cross-site scripting	A vulnerability was found in Os Commerce and classified as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument ENTRY_FIRST_NAME_MIN_LENGTH_TITLE[1] leads to cross-site scripting. This vulnerability is handled as CVE-2023-43715. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43722	Os Commerce orders_status_groups_name[1] cross-site scripting	A vulnerability classified as problematic was found in Os Commerce. This vulnerability affects unknown code. The manipulation of the argument orders_status_groups_name[1] leads to cross-site scripting. This vulnerability was named CVE-2023-43722. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43734	Os Commerce name cross-site scripting	A vulnerability was found in Os Commerce. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument name leads to cross-site scripting. This vulnerability was named CVE-2023-43734. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43733	Os Commerce company_address cross-site scripting	A vulnerability was found in Os Commerce. It has been classified as problematic. This affects an unknown part. The manipulation of the argument company_address leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-43733. 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-2023-43713	Os Commerce add-submit title cross-site scripting	A vulnerability which was classified as problematic was found in Os Commerce. Affected is an unknown function of the file /admin/admin-menu/add-submit. The manipulation of	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the argument title leads to cross-site scripting. This vulnerability is traded as CVE-2023-43713. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2023-43724	Os Commerce up to 4.oastif cross-site scripting	A vulnerability which was classified as problematic was found in Os Commerce up to 4.oastif. Affected is an unknown function. The manipulation of the argument derb6zmklgtjuhh2cn5chn2qjbm2stgmfa4.oastify.comscription[1][name] leads to cross-site scripting. This vulnerability is traded as CVE-2023-43724. 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-2023-43725	Os Commerce orders_products_status_name_long[1] cross-site scripting	A vulnerability was found in Os Commerce and classified as problematic. This issue affects some unknown processing. The manipulation of the argument orders_products_status_name_long[1] leads to cross-site scripting. The identification of this vulnerability is CVE-2023-43725. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43714	Os Commerce SKIP_CART_PAGE_TITLE[1] cross-site scripting	A vulnerability was found in Os Commerce. It has been classified as problematic. This affects an unknown part. The manipulation of the argument SKIP_CART_PAGE_TITLE[1] leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-43714. 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-2023-43717	Os Commerce MSEARCH_HIGHLIGHT_ENABLE_TITLE[1] cross-site scripting	A vulnerability which was classified as problematic has been found in Os Commerce. Affected by this issue is some unknown functionality. The manipulation of the argument MSEARCH_HIGHLIGHT_ENABLE_TITLE[1] leads to cross-site scripting. This vulnerability is handled as CVE-2023-43717. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43716	Os Commerce MAX_DISPLAY_NEW_PRODUCTS_TITLE[1] cross-site scripting	A vulnerability was found in Os Commerce. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument MAX_DISPLAY_NEW_PRODUCTS_TITLE[1] leads to cross-site scripting. This vulnerability was named CVE-2023-43716. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-43718	Os Commerce MSEARCH_ENABLE_TITLE [1] cross-site scripting	A vulnerability was found in Os Commerce. It has been rated as problematic. This issue affects some unknown processing. The manipulation of the argument MSEARCH_ENABLE_TITLE[1] leads to cross-site scripting. The identification of this vulnerability is CVE-2023-43718. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43721	Os Commerce PACKING_SLIPS_SUMMARY_TITLE[1] cross-site scripting	A vulnerability classified as problematic was found in Os Commerce. Affected by this vulnerability is an unknown functionality. The manipulation of the argument PACKING_SLIPS_SUMMARY_TITLE[1] leads to cross-site scripting. This vulnerability is known as CVE-2023-43721. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43712	Os Commerce access_levels_name cross-site scripting	A vulnerability has been found in Os Commerce and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument access_levels_name leads to cross-site scripting. This vulnerability is known as CVE-2023-43712. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43730	Os Commerce countries_name[1] cross-site scripting	A vulnerability was found in Os Commerce. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument countries_name[1] leads to cross-site scripting. This vulnerability is handled as CVE-2023-43730. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43735	Os Commerce formats_titles[7] cross-site scripting	A vulnerability was found in Os Commerce. It has been rated as problematic. This issue affects some unknown processing. The manipulation of the argument formats_titles[7] leads to cross-site scripting. The identification of this vulnerability is CVE-2023-43735. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43720	Os Commerce BILLING_GENDER_TITLE[1] cross-site scripting	A vulnerability which was classified as problematic was found in Os Commerce. This affects an unknown part. The manipulation of the argument BILLING_GENDER_TITLE[1] leads to cross-site scripting. This vulnerability is uniquely identified as 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
		43720. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2023-43723	Os Commerce orders_status_name[1] cross-site scripting	A vulnerability was found in Os Commerce. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument orders_status_name[1] leads to cross-site scripting. This vulnerability is known as CVE-2023-43723. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43727	Os Commerce stock_indication_text[1] cross-site scripting	A vulnerability has been found in Os Commerce and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument stock_indication_text[1] leads to cross-site scripting. This vulnerability was named CVE-2023-43727. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43719	Os Commerce SHIPPING_GENDER_TITLE [1] cross-site scripting	A vulnerability classified as problematic has been found in Os Commerce. Affected is an unknown function. The manipulation of the argument SHIPPING_GENDER_TITLE[1] leads to cross-site scripting. This vulnerability is traded as CVE-2023-43719. 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-2023-5112	Os Commerce specials_type_name[1] cross-site scripting	A vulnerability classified as problematic was found in Os Commerce. Affected by this vulnerability is an unknown functionality. The manipulation of the argument specials_type_name[1] leads to cross-site scripting. This vulnerability is known as CVE-2023-5112. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-5351	SalesAgility SuiteCRM up to 7.14.0 cross-site scripting	A vulnerability was found in SalesAgility SuiteCRM up to 7.14.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-5351. 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-2023-44012	mojoPortal 2.7.0.0 Help.aspx helpkey cross-site scripting	A vulnerability classified as problematic has been found in mojoPortal 2.7.0.0. Affected is an unknown function of the file Help.aspx. The manipulation of the argument helpkey	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 traded as CVE-2023-44012. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2023-27121	Pleasant Password Server 7.11.41.0 humanize cronString cross-site scripting	A vulnerability classified as problematic has been found in Pleasant Password Server 7.11.41.0. Affected is an unknown function of the file /framework/cron/action/humanize. The manipulation of the argument cronString leads to cross-site scripting. This vulnerability is traded as CVE-2023-27121. 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-2023-44075	Small CRM 3.0 Address cross-site scripting	A vulnerability was found in Small CRM 3.0 and classified as problematic. This issue affects some unknown processing. The manipulation of the argument Address leads to cross-site scripting. The identification of this vulnerability is CVE-2023-44075. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-42808	Common Voice 1.88.2 Path Expression cross-site scripting (GHSL-2023-026)	A vulnerability was found in Common Voice 1.88.2. It has been rated as problematic. This issue affects some unknown processing of the component Path Expression Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-42808. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-43877	Rite CMS 3.0 Administration Menu cross-site scripting	A vulnerability which was classified as problematic has been found in Rite CMS 3.0. Affected by this issue is some unknown functionality of the component Administration Menu. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-43877. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-44766	Concrete CMS 9.2.1 SEO Settings cross-site scripting	A vulnerability was found in Concrete CMS 9.2.1. It has been classified as problematic. This affects an unknown part of the component SEO Settings. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-44766. 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-2023-44758	GDidees CMS 3.0 Page Title cross-site scripting	A vulnerability classified as problematic has been found in GDidees CMS 3.0. This affects an unknown part. The manipulation of the argument Page Title leads to cross-site scripting.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is uniquely identified as CVE-2023-44758. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2023-43260	Milesight UR5X/UR32L/UR32/UR35/UR41 prior 35.3.0.7 Admin Panel cross-site scripting	A vulnerability has been found in Milesight UR5X UR32L UR32 UR35 and UR41 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-2023-43260. 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-2023-43343	OpenSolution Quick CMS 6.7 Pages Menu Component Description cross-site scripting	A vulnerability which was classified as problematic was found in OpenSolution Quick CMS 6.7. Affected is an unknown function of the component Pages Menu Component. The manipulation of the argument Description leads to cross-site scripting. This vulnerability is traded as CVE-2023-43343. 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-2023-44771	Zenario CMS 9.4.59197 Page Layout cross-site scripting	A vulnerability classified as problematic has been found in Zenario CMS 9.4.59197. Affected is an unknown function of the component Page Layout Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-44771. 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-2023-1259	Hotjar Plugin up to 1.0.15 on WordPress cross-site scripting	A vulnerability which was classified as problematic was found in Hotjar Plugin up to 1.0.15 on WordPress. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-1259. 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-2023-44764	Concrete CMS 9.2.1 Settings SITE cross-site scripting	A vulnerability classified as problematic was found in Concrete CMS 9.2.1. This vulnerability affects unknown code of the component Settings. The manipulation of the argument SITE leads to cross-site scripting. This vulnerability was named CVE-2023-44764. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-44761	Concrete CMS 9.2.1 Data Object cross-site scripting	A vulnerability was found in Concrete CMS 9.2.1. It has been rated as problematic.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This issue affects some unknown processing of the component Data Object Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-44761. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-44770	Zenario CMS 9.4.59197 Organizer cross-site scripting	A vulnerability was found in Zenario CMS 9.4.59197. It has been declared as problematic. This vulnerability affects unknown code of the component Organizer Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-44770. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-44762	Concrete CMS 9.2.1 Settings Tags cross-site scripting	A vulnerability was found in Concrete CMS 9.2.1 and classified as problematic. Affected by this issue is some unknown functionality of the component Settings Tags Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-44762. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-44765	Concrete CMS 9.2.1 Plural cross-site scripting	A vulnerability which was classified as problematic has been found in Concrete CMS 9.2.1. This issue affects some unknown processing of the component Plural Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-44765. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-5452	Snipe-IT up to 6.2.1 cross-site scripting	A vulnerability was found in Snipe-IT up to 6.2.1. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-5452. 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-2023-44393	Piwigo up to 14.0.0.beta3 admin.php cross-site scripting (GHSA-qg85-957m-7vgg)	A vulnerability classified as problematic has been found in Piwigo up to 14.0.0.beta3. This affects an unknown part of the file /admin.phppageplugins&tabnew&installstatusok&plugin_id[here. The manipulation leads to basic cross-site scripting. This vulnerability is uniquely identified as CVE-2023-44393. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		It is recommended to upgrade the affected component.		
CVE-2023-43643	AntiSamy up to 1.7.3 cross-site scripting	A vulnerability was found in AntiSamy up to 1.7.3. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-43643. 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-2023-44812	mooSocial 3.1.8 admin_redirect_url cross-site scripting	A vulnerability was found in mooSocial 3.1.8. It has been rated as problematic. This issue affects some unknown processing. The manipulation of the argument admin_redirect_url leads to cross-site scripting. The identification of this vulnerability is CVE-2023-44812. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-44763	Concrete CMS 9.2.1 Thumbnail cross-site scripting	A vulnerability classified as problematic was found in Concrete CMS 9.2.1. This vulnerability affects unknown code of the component Thumbnail Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-44763. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-44826	ZenTaoPMS 18.6 cross-site scripting	A vulnerability was found in ZenTaoPMS 18.6. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-44826. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2020-18336	Typora 0.9.65 PDF File Export cross-site scripting (Issue 2232)	A vulnerability was found in Typora 0.9.65 and classified as problematic. This issue affects some unknown processing of the component PDF File Export. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2020-18336. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-44813	mooSocial 3.1.8 Invite Friend Login mode cross-site scripting	A vulnerability classified as problematic was found in mooSocial 3.1.8. Affected by this vulnerability is an unknown functionality of the component Invite Friend Login. The manipulation of the argument mode leads to cross-site scripting. This vulnerability is known	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		as CVE-2023-44813. The attack can be launched remotely. There is no exploit available.		
CVE-2023-34354	Peplink Surf SOHO HW1 6.3.5 HTTP Request upload_brand.cgi cross-site scripting (TALOS-2023-1781)	A vulnerability was found in Peplink Surf SOHO HW1 6.3.5. It has been classified as problematic. Affected is an unknown function of the file upload_brand.cgi of the component HTTP Request Handler. The manipulation leads to basic cross-site scripting. This vulnerability is traded as CVE-2023-34354. 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-2023-36126	PHP Jabbers Appointment Scheduler 3.0 preview.php theme cross-site scripting	A vulnerability was found in PHP Jabbers Appointment Scheduler 3.0. It has been rated as problematic. This issue affects some unknown processing of the file preview.php. The manipulation of the argument theme leads to cross-site scripting. The identification of this vulnerability is CVE-2023-36126. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-5556	structurizr onpremises up to 3193 cross-site scripting	A vulnerability which was classified as problematic was found in structurizr onpremises up to 3193. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-5556. 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-2023-5555	frappe lms cross-site scripting	A vulnerability which was classified as problematic has been found in frappe lms. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-5555. The attack may be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-5581	SourceCodester Medicine Tracker System 1.0 index.php page cross-site scripting	A vulnerability classified as problematic was found in SourceCodester Medicine Tracker System 1.0. This vulnerability affects unknown code of the file index.php. The manipulation of the argument page leads to cross-site scripting. This vulnerability was named CVE-2023-5581. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-5582	ZZZCMS 2.2.0 Personal Profile Page cross-site	A vulnerability which was classified as problematic has	Protected by core rules	Detected by scanner as cross-

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	scripting	been found in ZZZCMS 2.2.0. This issue affects some unknown processing of the component Personal Profile Page. The manipulation leads to basic cross-site scripting. The identification of this vulnerability is CVE-2023-5582. The attack may be initiated remotely. Furthermore there is an exploit available.		site scripting attack
CVE-2023-5564	froxlor up to 2.0.0 cross-site scripting	A vulnerability which was classified as problematic was found in froxlor up to 2.0.0. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-5564. 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-2023-38000	Gutenberg Plugin on WordPress cross-site scripting	A vulnerability was found in Gutenberg Plugin on WordPress and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-38000. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-4517	hestiacp up to 1.8.5 cross-site scripting	A vulnerability which was classified as problematic has been found in hestiacp up to 1.8.5. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-4517. 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-2023-4829	froxlor up to 2.0.21 cross-site scripting	A vulnerability has been found in froxlor up to 2.0.21 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-2023-4829. 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-2023-45391	Granding UTime Master 9.0.7 Create A New Employee First Name cross-site scripting	A vulnerability classified as problematic was found in Granding UTime Master 9.0.7. This vulnerability affects unknown code of the component Create A New Employee. The manipulation of the argument First Name	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 was named CVE-2023-45391. The attack can be initiated remotely. There is no exploit available.		
CVE-2023-4820	PowerPress Podcasting Plugin up to 11.0.11 on WordPress Media URL cross-site scripting	A vulnerability has been found in PowerPress Podcasting Plugin up to 11.0.11 on WordPress and classified as problematic. This vulnerability affects unknown code of the component Media URL Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-4820. 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-2023-4783	Magee Shortcodes Plugin up to 2.1.1 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in Magee Shortcodes Plugin up to 2.1.1 on WordPress. It has been declared as problematic. This vulnerability affects unknown code of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-4783. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-5087	Pagelayer Plugin up to 1.7.7 on WordPress Post cross-site scripting	A vulnerability was found in Pagelayer Plugin up to 1.7.7 on WordPress. It has been classified as problematic. Affected is an unknown function of the component Post Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-5087. 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-2023-4388	EventON Plugin up to 2.1 on WordPress Setting cross-site scripting	A vulnerability was found in EventON Plugin up to 2.1 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-2023-4388. 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-2023-4811	File Upload Plugin up to 4.23.2 on WordPress Setting cross-site scripting	A vulnerability classified as problematic has been found in File Upload Plugin up to 4.23.2 on WordPress. This affects an unknown part of the component Setting 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 uniquely identified as CVE-2023-4811. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-4862	File Manager Pro Plugin up to 1.8.0 on WordPress cross-site scripting	A vulnerability was found in File Manager Pro Plugin up to 1.8.0 on WordPress and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-4862. 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-2023-4819	Shared Files Plugin up to 1.7.5 on WordPress Header cross-site scripting	A vulnerability which was classified as problematic was found in Shared Files Plugin up to 1.7.5 on WordPress. This affects an unknown part of the component Header Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-4819. 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-2023-4795	Testimonial Slider Shortcode Plugin up to 1.1.8 on WordPress Shortcode Attribute cross-site scripting	A vulnerability classified as problematic was found in Testimonial Slider Shortcode Plugin up to 1.1.8 on WordPress. Affected by this vulnerability is an unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-4795. 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-2023-4950	Interactive Contact Form and Multi Step Form Builder Plugin cross-site scripting	A vulnerability was found in Interactive Contact Form and Multi Step Form Builder Plugin up to 3.3 on WordPress. 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-2023-4950. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-4290	WP Matterport Shortcode Plugin up to 2.1.6 on WordPress cross-site scripting	A vulnerability has been found in WP Matterport Shortcode Plugin up to 2.1.6 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-4290. 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-2023-4620	Booking Calendar Plugin up to 9.7.3.0 on WordPress cross-site scripting	A vulnerability was found in Booking Calendar Plugin up to 9.7.3.0 on WordPress. 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-2023-4620. 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-2023-4687	Pagelayer Plugin up to 1.7.6 on WordPress Post cross-site scripting	A vulnerability which was classified as problematic was found in Pagelayer Plugin up to 1.7.6 on WordPress. Affected is an unknown function of the component Post Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-4687. 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-2023-4805	Tutor LMS Plugin up to 2.2.x on WordPress Setting cross-site scripting	A vulnerability was found in Tutor LMS Plugin up to 2.2.x on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-4805. 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-2023-4289	WP Matterport Shortcode Plugin up to 2.1.7 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in WP Matterport Shortcode Plugin up to 2.1.7 on WordPress. It has been classified as problematic. This affects an unknown part of the component Shortcode Attribute 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 uniquely identified as CVE-2023-4289. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2022-48612	ClassLink OneClick Extension up to 10.7 Regular Expression cross-site scripting	A vulnerability classified as problematic was found in ClassLink OneClick Extension up to 10.7. This vulnerability affects unknown code of the component Regular Expression Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-48612. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-45540	Jorani Leave Management System 1.0.3 List of Leave Requests Page comment cross-site scripting	A vulnerability was found in Jorani Leave Management System 1.0.3. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component List of Leave Requests Page. The manipulation of the argument comment leads to basic cross-site scripting. This vulnerability is known as CVE-2023-45540. 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-2023-40851	PHPGurukul User Registration & Login and User Management System with Admin Panel cross-site scripting (Exploit 51694 / EDB-51694)	A vulnerability was found in PHPGurukul User Registration & Login and User Management System with Admin Panel 3.0. It has been rated as problematic. This issue affects some unknown processing of the component User Registration Handler. The manipulation of the argument fname/lname/email/contact leads to cross-site scripting. The identification of this vulnerability is CVE-2023-40851. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2023-45542	mooSocial 3.1.8 Search q cross-site scripting	A vulnerability was found in mooSocial 3.1.8. It has been classified as problematic. Affected is an unknown function of the component Search. The manipulation of the argument q leads to cross-site scripting. This vulnerability is traded as CVE-2023-45542. 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-2023-5538	MpOperationLogs Plugin up to 1.0.1 on WordPress cross-site scripting	A vulnerability has been found in MpOperationLogs Plugin up to 1.0.1 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-5538. 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.		

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™