INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

April 2023

The total zero-day vulnerabilities count for April month : 287

Command Injection	CSRF	Local File Inclusion	SQL Injection	XSS Injection	XXE Attack	Malicious File Upload
21	16	23	106	109	1	11

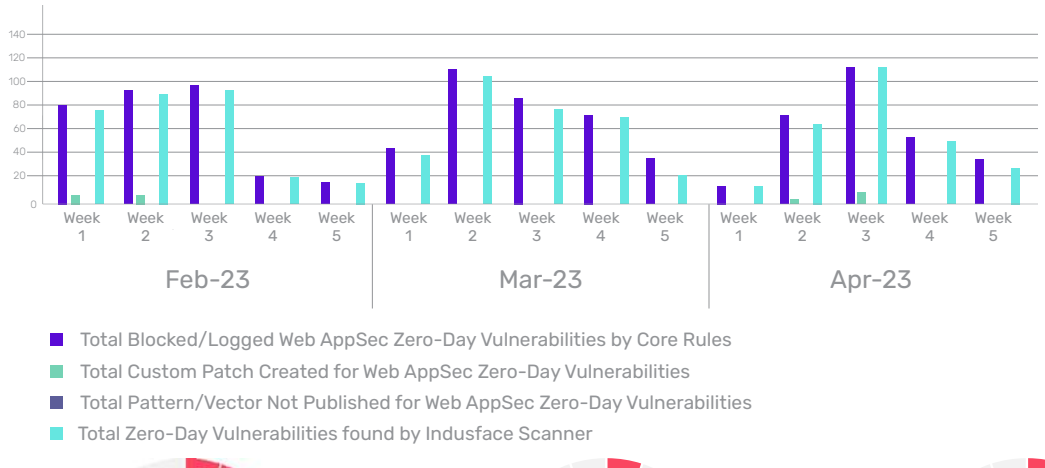
Zero-day vulnerabilities protected through core rules	274
Zero-day vulnerabilities protected through custom rules	12
Zero-day vulnerabilities for which protection can not be done	0
Zero-day vulnerabilities protected by default in SaaS	1
Zero-day vulnerabilities found by Indusface WAS	258

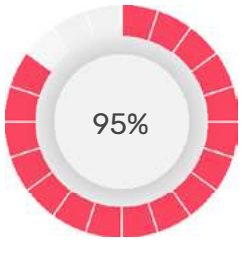
- To enable custom rules, please contact support@indusface.com
- Since the attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.

Vulnerability Trend:

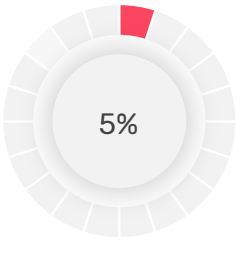
The weekly trend displays the total number of vulnerabilities discovered to the type of protection provided for the last quarter.

Weekly Vulnerability Trend

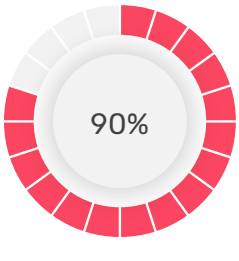




of the zero-day vulnerabilities were protected by the **core rules** in the last month.

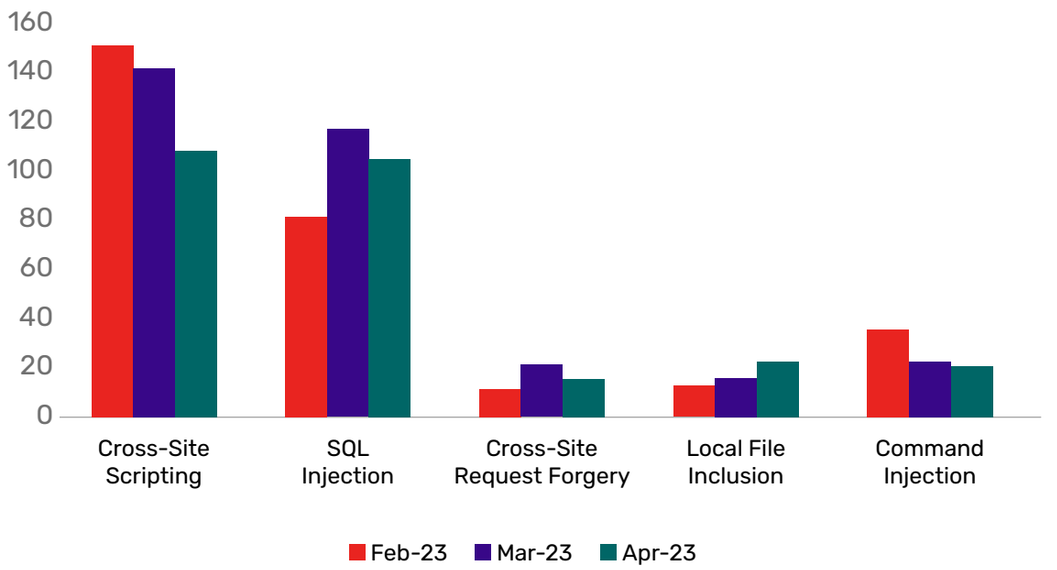


of the zero-day vulnerabilities were protected by the **custom rules** in the last month.



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

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-26822	D-Link Go-RT-AC750 101b03 soapcgi.main service command injection	A vulnerability which was classified as critical has been found in D-Link Go-RT-AC750 101b03. This issue affects some unknown processing of the file soapcgi.main. The manipulation of the argument service leads to command injection. The identification of this vulnerability is CVE-2023-26822. 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-2023-26921	quectel AG550QCN ql_atfwd os command injection	A vulnerability classified as critical has been found in quectel AG550QCN. This affects the function ql_atfwd. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2023-26921. 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-2023-26978	TOTOLINK A7100RU 7.4cu.2313_B20191024 Setting / setting/setWanIeCfg pppoeAcName command injection	A vulnerability was found in TOTOLINK A7100RU 7.4cu.2313_B20191024 and classified as critical. Affected by this issue is some unknown functionality of the file /setting/setWanIeCfg of the component Setting Handler. The manipulation of the argument pppoeAcName leads to command injection. This vulnerability is handled as CVE-2023-26978. 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1947	taoCMS 3.0.2 /admin/admin.php code injection	A vulnerability was found in taoCMS 3.0.2. It has been classified as critical. Affected is an unknown function of the file/admin/admin.php. The manipulation leads to code injection. This vulnerability is traded as CVE-2023-1947. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-26848	TOTOLINK A7100RU 7.4cu.2313_B20191024 delStaticDhcpRules org command injection	A vulnerability has been found in TOTOLINK A7100RU 7.4cu.2313_B20191024 and classified as critical. Affected by this vulnerability is an unknown functionality of the file setting/delStaticDhcpRules. The manipulation of the argument org leads to command injection. This vulnerability is known as CVE-2023-26848. 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-2023-1406	JetEngine Plugin prior 3.1.3.1 on WordPress code injection	A vulnerability which was classified as critical was found in JetEngine Plugin. This affects an unknown part. The manipulation leads to code injection. This vulnerability is uniquely identified as CVE-2023-1406. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by custom rules	NA
CVE-2023-26788	Veritas Appliance 4.1.0.1 HTTP Host Header injection	A vulnerability which was classified as critical was found in Veritas Appliance 4.1.0.1. This affects an unknown part of the component HTTP Host Header Handler. The manipulation leads to injection. This vulnerability is uniquely identified as CVE-2023-26788. 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-2023-27826	SeowonIntech SWC 5100W WIMAX Bootloader 1.18.19.0 doSystem os command injection (ID 51311 / EDB-51311)	A vulnerability was found in SeowonIntech SWC 5100W WIMAX Bootloader 1.18.19.0 and classified as critical. This issue affects the function doSystem. The manipulation leads to os command injection. The identification of this vulnerability is CVE-2023-27826. The attack can only be initiated within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-29803	TOTOLINK X18 9.1.0cu.2024_B20220329 disconnectVPN pid command injection	A vulnerability was found in TOTOLINK X18 9.1.0cu.2024_B20220329. It has been rated as critical. Affected by this issue is the function disconnectVPN. The manipulation of the argument pid leads to command injection. This vulnerability is handled as CVE-2023-29803. 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-2023-29805	IO DATA WFS-SR03 1.0.3 pro_stor_canceltrans_handler_part_19 command injection	A vulnerability classified as critical was found in IO DATA WFS-SR03 1.0.3. This vulnerability affects the function pro_stor_canceltrans_handler_part_19. The manipulation leads to command injection. This vulnerability was named CVE-2023-29805. 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-2023-29801	TOTOLINK X18 9.1.0cu.2024_B20220329 setSyslogCfg rtLogEnabled/rtLogServer command injection	A vulnerability was found in TOTOLINK X18 9.1.0cu.2024_B20220329. It has been classified as critical. Affected is the function setSyslogCfg. The manipulation of the argument rtLogEnabled/rtLogServer leads to command injection. This vulnerability is traded as CVE-2023-29801. 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-2023-29802	TOTOLINK X18 9.1.0cu.2024_B20220329 setDiagnosisCfg ip command injection	A vulnerability was found in TOTOLINK X18 9.1.0cu.2024_B20220329. It has been declared as critical. Affected by this vulnerability is the function setDiagnosisCfg. The manipulation of the argument ip leads to command injection. This vulnerability is known as CVE-2023-29802. 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-2023-29800	TOTOLINK X18 9.1.0cu.2024_B20220329 UploadFirmwareFile FileName command injection	A vulnerability was found in TOTOLINK X18 9.1.0cu.2024_B20220329 and classified as critical. This issue affects the function UploadFirmwareFile. The manipulation of the argument FileName leads to command injection. The identification of this vulnerability is CVE-2023-29800. 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-29798	TOTOLINK X18 9.1.0cu.2024_ B20220329 setTracerouteCfg command command injection	A vulnerability which was classified as critical was found in TOTOLINK X18 9.1.0cu.2024_B20220329. This affects the function setTracerouteCfg. The manipulation of the argument command leads to command injection. This vulnerability is uniquely identified as CVE-2023-29798. 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-2023-29799	TOTOLINK X18 9.1.0cu.2024_ B20220329 setOpModeCfg hostname command injection	A vulnerability has been found in TOTOLINK X18 9.1.0cu.2024_B20220329 and classified as critical. This vulnerability affects the function setOpModeCfg. The manipulation of the argument hostname leads to command injection. This vulnerability was named CVE-2023-29799. 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-2023-2056	DedeCMS up to 5.7.87 module_main.php GetSystemFile code injection	A vulnerability was found in DedeCMS up to 5.7.87 and classified as critical. This issue affects the function GetSystemFile of the file module_main.php. The manipulation leads to code injection. The identification of this vulnerability is CVE-2023-2056. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-29804	IO DATA WFS-SR03 1.0.3 sys_smb_pwdmod command injection	A vulnerability classified as critical has been found in IO DATA WFS-SR03 1.0.3. This affects the function sys_smb_pwdmod. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2023-29804. 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-2023-2091	KylinSoft youker-assistant prior 3.1.4.13 on KylinOS adjust_cpufreq_scaling_governer os command injection	A vulnerability classified as critical was found in KylinSoft youker-assistant on KylinOS. Affected by this vulnerability is the function adjust_cpufreq_scaling_governer. The manipulation leads to os command injection. This vulnerability is known as CVE-2023-2091. It is possible to launch the attack on the local host. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-38841	Linksys AX3200 1.1.00 Diagnostics Traceroute Page os command injection (ID 171433)	A vulnerability classified as critical was found in Linksys AX3200 1.1.00. This vulnerability affects unknown code of the component Diagnostics Traceroute Page. The manipulation leads to os command injection. This vulnerability was named CVE-2022-38841. 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-2020-29007	Score Extension up to 0.3.0 on MediaWiki GNU LilyPond Remote Code Execution	A vulnerability was found in Score Extension up to 0.3.0 on MediaWiki. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component GNU LilyPond. The manipulation leads to Remote Code Execution. This vulnerability is known as CVE-2020-29007. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2022-23305	Oracle Utilities Application Framework 4.2.0.3.0 General Remote Code Execution	A vulnerability classified as very critical was found in Oracle Utilities Application Framework 4.2.0.3.0. Affected by this vulnerability is an unknown functionality of the component General. The manipulation leads to Remote Code Execution. This vulnerability is known as CVE-2022-23305. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0820	BestWebSoft User Role Plugin up to 1.6.6 on WordPress cross-site request forgery	A vulnerability has been found in BestWebSoft User Role Plugin up to 1.6.6 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-2023-0820. 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-2020-19278	Phachon mm-wiki 0.1.2 system/user/save cross-site request forgery (ID 68)	A vulnerability which was classified as problematic has been found in Phachon mm-wiki 0.1.2. This issue affects some unknown processing. The manipulation of the argument system/user/save leads to cross-site request forgery. The identification of this vulnerability is CVE-2020-19278. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1330	Redirection Plugin up to 1.1.3 on WordPress cross-site request forgery	A vulnerability was found in Redirection Plugin up to 1.1.3 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-1330. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-29003	SvelteKit up to 1.15.0 is_form_content_type cross-site request forgery (GHSA-5p75-vc5g-8rv2)	A vulnerability was found in SvelteKit up to 1.15.0. It has been declared as problematic. This vulnerability affects the function is_form_content_type. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-29003. 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-2023-0480	Telesoft VitalPBX 3.2.3-8 cross-site request forgery	A vulnerability was found in Telesoft VitalPBX 3.2.3-8. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-0480. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-1937	zhenfeng13 My-Blog userInfo yourAvatar/yourName/yourEmail cross-site request forgery (I6PV4U)	A vulnerability which was classified as problematic was found in zhenfeng13 My-Blog. Affected is an unknown function of the file /admin/configurations/userInfo. The manipulation of the argument yourAvatar/yourName/yourEmail leads to cross-site request forgery. This vulnerability is traded as CVE-2023-1937. It is possible to launch the attack remotely. Furthermore there is an exploit available. This product is using a rolling release to provide continious delivery. Therefore no version details for affected nor updated releases are available.	Protected by core rules	NA
CVE-2023-25411	Aten PE8108 2.4.232 cross-site request forgery	A vulnerability was found in Aten PE8108 2.4.232. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-25411. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1331	Redirection Plugin up to 1.1.4 on WordPress cross-site request forgery	A vulnerability was found in Redirection Plugin up to 1.1.4 on WordPress. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-1331. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-0889	Themeflection Numbers Plugin up to 2.0.0 on WordPress cross-site request forgery	A vulnerability has been found in Themeflection Numbers Plugin up to 2.0.0 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-0889. 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-2023-2228	modoboa up to 2.0.x cross-site request forgery	A vulnerability classified as problematic was found in modoboa up to 2.0.x. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-2228. 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-2023-31061	Repetier Server up to 1.4.10 cross-site request forgery	A vulnerability classified as problematic was found in Repetier Server up to 1.4.10. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-31061. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-26841	ChurchCRM 4.5.3 Password cross-site request forgery	A vulnerability was found in ChurchCRM 4.5.3. It has been rated as problematic. This issue affects some unknown processing of the component Password Handler. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-26841. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-26840	ChurchCRM 4.5.3 User cross-site request forgery	A vulnerability was found in ChurchCRM 4.5.3. It has been declared as problematic. This vulnerability affects unknown code of the component User Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-26840. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-26839	ChurchCRM 4.5.3 People cross-site request forgery	A vulnerability was found in ChurchCRM 4.5.3. It has been classified as problematic. This affects an unknown part of the component People Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-26839. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-1623	Custom Post Type UI Plugin up to 1.13.4 on WordPress Email Address cross-site request forgery	A vulnerability has been found in Custom Post Type UI Plugin up to 1.13.4 on WordPress and classified as problematic. This vulnerability affects unknown code of the component Email Address Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-1623. 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-2023-2307	builderio qwik prior 0.104.0 cross-site request forgery	A vulnerability which was classified as problematic was found in builderio qwik. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-2307. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1800	sjqzhang go-fastdfs up to 1.4.3 File Upload /group1/uploa upload path traversal	A vulnerability which was classified as critical has been found in sjqzhang go-fastdfs up to 1.4.3. Affected by this issue is the function upload of the file /group1/uploa of the component File Upload Handler. The manipulation leads to path traversal: &039;../filedir&039;. This vulnerability is handled as CVE-2023-1800. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-25305	PolyMC Launcher up to 1.4.3 mrpack File path traversal (GHSA-3rfr-g9g9-7gx2)	A vulnerability which was classified as critical has been found in PolyMC Launcher up to 1.4.3. Affected by this issue is some unknown functionality of the component mrpack File Handler. The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-25305. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-25303	ATLauncher up to 3.4.26.0 mrpack File path traversal (GHSA-7cff-8xv4-mvx6)	A vulnerability classified as critical was found in ATLauncher up to 3.4.26.0. Affected by this vulnerability is an unknown functionality of the component mrpack File Handler. The manipulation leads to path traversal. This vulnerability is known as CVE-2023-25303. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-1124	Shopping Cart & eCommerce Store Plugin up to 5.4.2 on WordPress HTTP Request file inclusion	A vulnerability was found in Shopping Cart & eCommerce Store Plugin up to 5.4.2. It has been rated as critical. This issue affects some unknown processing of the component HTTP Request Handler. The manipulation leads to file inclusion. The identification of this vulnerability is CVE-2023-1124. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-26820	siteproxy 1.0 index.js path traversal (ID 67)	A vulnerability which was classified as critical was found in siteproxy 1.0. Affected is an unknown function of the file index.js. The manipulation leads to path traversal. This vulnerability is traded as CVE-2023-26820. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-29478	BiblioCraft up to 2.4.5 Filename path traversal	A vulnerability was found in BiblioCraft up to 2.4.5. It has been classified as critical. This affects an unknown part of the component Filename Handler. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-29478. Access to the local network is required for this attack. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1956	SourceCodester Online Computer and Laptop Store 1.0 Image Master.php path path traversal	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 /classes/Master.phpfdelete_img of the component Image Handler. The manipulation of the argument path leads to path traversal. This vulnerability is known as CVE-2023-1956. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-0156	All-In-One Security Plugin up to 5.1.4 on WordPress Setting path traversal	A vulnerability was found in All-In-One Security Plugin up to 5.1.4 and classified as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-0156. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-1478	Hummingbird Plugin up to 3.4.1 on WordPress Cache path traversal	A vulnerability classified as critical has been found in Hummingbird Plugin up to 3.4.1. This affects an unknown part of the component Cache Handler. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-1478. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-2059	DedeCMS 5.7.87 select_templets.php path traversal	A vulnerability was found in DedeCMS 5.7.87. It has been rated as problematic. Affected by this issue is some unknown functionality of the file uploads/include/dialog/select_templets.php. The manipulation leads to path traversal: &039;..\filedir&039;. This vulnerability is handled as CVE-2023-2059. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-27648	Timmystudios T-ME Studios Change Color of Keypad 1.275.1.277 DEX File path traversal	A vulnerability was found in Timmystudios T-ME Studios Change Color of Keypad 1.275.1.277. It has been rated as critical. This issue affects some unknown processing of the component DEX File Handler. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-27648. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-47027	Timmystudios Fast Typing Keyboard 1.275.1.162 path traversal	A vulnerability was found in Timmystudios Fast Typing Keyboard 1.275.1.162. It has been classified as critical. This affects an unknown part. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-47027. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-26969	Atropim 1.5.26 path traversal	A vulnerability classified as critical has been found in Atropim 1.5.26. This affects an unknown part. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-26969. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-2101	moxi624 Mogu Blog v2 up to 5.2 uploadPicsByUrl uploadPictureByUrl urlList absolute path traversal (ID 97)	A vulnerability which was classified as problematic has been found in moxi624 Mogu Blog v2 up to 5.2. This issue affects the function uploadPictureByUrl of the file /mogu-picture/file/uploadPicsByUrl. The manipulation of the argument urlList leads to absolute path traversal. The identification of this vulnerability is CVE-2023-2101. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2021-33990	Liferay Portal 6.2.5 absolute path traversal (Exploit 171701)	A vulnerability was found in Liferay Portal 6.2.5. It has been declared as problematic. This vulnerability affects unknown code of the file Command-FileUpload&Type-File&CurrentFolder/. The manipulation leads to path traversal: &039;/absolute/pathname/here&039;. This vulnerability was named CVE-2021-33990. The attack can only be done within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-1274	Pricing Tables for WPBakery Page Builder Plugin up to 2.x on WordPress Shortcode Attribute path traversal	A vulnerability which was classified as critical has been found in Pricing Tables for WPBakery Page Builder Plugin up to 2.x on WordPress. Affected by this issue is some unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-1274. The attack can only be initiated within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-1427	10Web Photo Gallery Plugin up to 1.8.14 on WordPress File Upload path traversal	A vulnerability has been found in 10Web Photo Gallery Plugin up to 1.8.14 on WordPress and classified as critical. This vulnerability affects unknown code of the component File Upload. The manipulation leads to path traversal. This vulnerability was named CVE-2023-1427. The attack needs to be initiated within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-29004	Hap-WI Roxy-wi 6.3.9.0 Web Interface /app/options.py config_file_name path traversal (GHSA-7qqj-xhvr-46fv)	A vulnerability was found in Hap-WI Roxy-wi 6.3.9.0. It has been declared as critical. This vulnerability affects unknown code of the file /app/options.py of the component Web Interface Handler. The manipulation of the argument config_file_name leads to path traversal. This vulnerability was named CVE-2023-29004. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-29887	spreadsheet-reader 0.5.11 test.php File file inclusion	A vulnerability was found in spreadsheet-reader 0.5.11. It has been rated as critical. This issue affects some unknown processing of the file test.php. The manipulation of the argument File leads to file inclusion. The identification of this vulnerability is CVE-2023-29887. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-29586	Code Sector TeraCopy 3.9.7 path traversal	A vulnerability which was classified as critical was found in Code Sector TeraCopy 3.9.7. Affected is an unknown function of the component Copy Handler. The manipulation leads to path traversal. This vulnerability is traded as CVE-2023-29586. 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-2014-4650	Python 2.7.5/3.3.4 CGIHTTPServer Module path traversal	A vulnerability was found in Python 2.7.5/3.3.4 and classified as critical. Affected by this issue is some unknown functionality of the component CGIHTTPServer Module. The manipulation leads to path traversal. This vulnerability is handled as CVE-2014-4650. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2013-3738	Zabbix 2.0.6 CGI Script file inclusion	A vulnerability was found in Zabbix 2.0.6 and classified as critical. This issue affects some unknown processing of the component CGI Script. The manipulation leads to file inclusion. The identification of this vulnerability is CVE-2013-3738. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-31059	Repetier Server up to 1.4.10 connectionLost.php path traversal	A vulnerability was found in Repetier Server up to 1.4.10 and classified as problematic. This issue affects some unknown processing of the file connectionLost.php. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-31059. The attack needs to be approached within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1797	OTCMS 6.0.1 sysCheckFile.php unrestricted upload	A vulnerability classified as critical was found in OTCMS 6.0.1. Affected by this vulnerability is an unknown functionality of the file sysCheckFile.phpmudisql. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2023-1797. 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-2021-3267	KiteCMS 1.1 uploadFile unrestricted upload	A vulnerability which was classified as critical has been found in KiteCMS 1.1. Affected by this issue is the function uploadFile. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2021-3267. The attack may be launched remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2023-0265	Uvdesk 1.1.1 Profile Picture unrestricted upload	A vulnerability which was classified as critical has been found in Uvdesk 1.1.1. Affected by this issue is some unknown functionality of the component Profile Picture Handler. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-0265. The attack may be launched remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2023-26857	Dynamic Transaction Queuing System 1.0 ajax.php unrestricted upload	A vulnerability has been found in Dynamic Transaction Queuing System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/ajax.phpactionsave_uploads. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-26857. The attack needs to be done within the local network. There is no exploit available.	Protected by custom rules	NA
CVE-2023-1970	yuan1994 tpAdmin 1.3.12 Upload.php Upload file unrestricted upload	A vulnerability which was classified as problematic has been found in yuan1994 tpAdmin 1.3.12. This issue affects the function Upload of the file application\admin\controller\Upload.php. The manipulation of the argument file leads to unrestricted upload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. The identification of this vulnerability is CVE-2023-1970. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by custom rules	NA
CVE-2023-26852	Textpattern up to 4.8.8 Upload Plugin unrestricted upload	A vulnerability was found in Textpattern up to 4.8.8. It has been classified as critical. This affects an unknown part of the component Upload Plugin. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-26852. Access to the local network is required for this attack. There is no exploit available.	Protected by custom rules	NA
CVE-2023-29625	Employee Performance Evaluation System 1.0 unrestricted upload	A vulnerability was found in Employee Performance Evaluation System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-29625. The attack may be launched remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2023-29621	Purchase Order Management 1.0 unrestricted upload	A vulnerability was found in Purchase Order Management 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2023-29621. The attack can be launched remotely. There is no exploit available.	Protected by custom rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-29627	Online Pizza Ordering 1.0 unrestricted upload	A vulnerability was found in Online Pizza Ordering 1.0 and classified as critical. This issue affects some unknown processing. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2023-29627. The attack may be initiated remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2023-2034	froxlor up to 2.0.13 unrestricted upload	A vulnerability was found in froxlor up to 2.0.13. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-2034. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by custom rules	NA
CVE-2023-2246	SourceCodester Online Pizza Ordering System 1.0 ajax.php img unrestricted upload	A vulnerability has been found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. This vulnerability affects unknown code of the file admin/ajax.phpactionsave_settings. The manipulation of the argument img leads to unrestricted upload. This vulnerability was named CVE-2023-2246. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by custom rules	NA

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-26858	faqs 3.1.6 on PrestaShop displayAjaxGenerateBudget sql injection	A vulnerability was found in faqs 3.1.6. It has been rated as critical. Affected by this issue is the function faqsBudgetModuleFrontController::displayAjaxGenerateBudget. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-26858. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1793	SourceCodester Police Crime Record Management System 1.0 GET Parameter /officer/assigncase.php caseid sql injection	A vulnerability was found in SourceCodester Police Crime Record Management System 1.0. It has been classified as critical. This affects an unknown part of the file /officer/assigncase.php of the component GET Parameter Handler. The manipulation of the argument caseid leads to sql injection. This vulnerability is uniquely identified as CVE-2023-1793. 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-2023-1792	SourceCodester Simple Mobile Comparison Website 1.0 GET Parameter manage_field.php id sql injection	A vulnerability was found in SourceCodester Simple Mobile Comparison Website 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/fields/manage_field.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-1792. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2020-20913	Ming-Soft MCMS 4.7.2 basic_title sql injection (ID 27)	A vulnerability was found in Ming-Soft MCMS 4.7.2. It has been classified as critical. This affects an unknown part. The manipulation of the argument basic_title leads to sql injection. This vulnerability is uniquely identified as CVE-2020-20913. 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-2020-20914	sanluan PublicCMS 4.0 sql sql injection (ID 29)	A vulnerability was found in sanluan PublicCMS 4.0. It has been declared as critical. This vulnerability affects unknown code. The manipulation of the argument sql leads to sql injection. This vulnerability was named CVE-2020-20914. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-38922	BluePage CMS up to 3.9 Cookie Header sql injection	A vulnerability which was classified as critical has been found in BluePage CMS up to 3.9. Affected by this issue is some unknown functionality of the component Cookie Header Handler. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-38922. 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-2023-1827	SourceCodester Centralized Covid Vaccination Records System 1.0 GET Parameter manage_location.php sql injection	A vulnerability has been found in SourceCodester Centralized Covid Vaccination Records System 1.0 and classified as critical. This vulnerability affects unknown code of the file /vaccinated/admin/maintenance/manage_location.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-1827. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-38923	BluePage CMS up to 3.9 HTTP Header User-Agent sql injection	A vulnerability classified as critical was found in BluePage CMS up to 3.9. Affected by this vulnerability is an unknown functionality of the component HTTP Header Handler. The manipulation of the argument User-Agent leads to sql injection. This vulnerability is known as CVE-2022-38923. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2020-20915	sanluan PublicCMS 4.0 SysSiteAdminControl sql sql injection (ID 29)	A vulnerability was found in sanluan PublicCMS 4.0. It has been rated as critical. This issue affects the function SysSiteAdminCon-trol. The manipulation of the argument sql leads to sql injection. The identification of this vulnerability is CVE-2020-20915. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1850	SourceCodester Online Payroll System 1.0 /admin/login.php username sql injection	A vulnerability was found in SourceCodester Online Payroll System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/login.php. The manipulation of the argument username leads to sql injection. This vulnerability is handled as CVE-2023-1850. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1856	SourceCodester Air Cargo Management System 1.0 GET Parameter track_ shipment.php id sql injection	A vulnerability has been found in SourceCodester Air Cargo Management System 1.0 and classified as critical. Affected by this vulnerability is an un-known functionality of the file /admin/transactions/ track_shipment.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-1856. The attack can be launched re-motely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-25330	MyBatis Plus up to 3.5.3.0 sql injection	A vulnerability was found in MyBatis Plus up to 3.5.3.0 and classi-fied as critical. Affected by this issue is some unknown function-ality. The ma-nipulation leads to sql injection. This vulnerability is handled as CVE-2023-25330. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1849	SourceCodester Online Payroll System 1.0 cashad-vance_row.php id sql injection	A vulnerability was found in SourceCodester Online Payroll Sys-tem 1.0. It has been declared as critical. Affected by this vul-nera-bility is an unknown functionality of the file / admin/cashadvance_row. php. The manipulation of the argu-ment id leads to sql injection. This vulnerability is known as CVE-2023-1849. The attack can be launched re-motely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-26856	Dynamic Transaction Queuing System 1.0 ajax.php name sql injection	A vulnerability was found in Dynamic Transaction Queuing Sys-tem 1.0 and classified as critical. This issue affects some un-known processing of the file /admin/ajax.phpac-tionlogin. The manipu-la-tion of the argument name leads to sql injection. The identification of this vulnerability is CVE-2023-26856. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1847	SourceCodester Online Pay-roll Sys-tem 1.0 attend-ance. php employee sql injection	A vulnerability was found in SourceCodester Online Payroll System 1.0 and classified as critical. This issue affects some unknown processing of the file attendance.php. The manipulation of the argument employee leads to sql injection. The identification of this vulnerability is CVE-2023-1847. The attack may be initiated remotely. Further-more there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1845	SourceCodester Online Payroll System 1.0 /admin/employ-ee_row.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Online Payroll System 1.0. This affects an un-known part of the file /admin/ employee_row.php. The manipu-lation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-1845. It is possible to initiate the attack remote-ly. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1846	SourceCodester Online Payroll System 1.0 /admin/deduc-tion_row.php id sql injection	A vulnerability has been found in SourceCodester Online Payroll System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/deduction_row. php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-1846. The attack can be initiated remotely. Furthermore there is an exploit avail-able.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1848	SourceCodester Online Pay-roll System 1.0 attend-ance_row.php id sql injection	A vulnerability was found in SourceCodester Online Payroll System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/attendance_row.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-1848. 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-2023-1941	SourceCodester Simple and Beautiful Shopping Cart System 1.0 login.php username/password sql injection	A vulnerability which was classified as critical has been found in SourceCodester Simple and Beautiful Shopping Cart System 1.0. This issue affects some unknown processing of the file login.php. The manipulation of the argument username/password leads to sql injection. The identification of this vulnerability is CVE-2023-1941. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1940	SourceCodester Simple and Beautiful Shopping Cart System 1.0 delete_user_query.php user_id sql injection	A vulnerability classified as critical was found in SourceCodester Simple and Beautiful Shopping Cart System 1.0. This vulnerability affects unknown code of the file delete_user_query.php. The manipulation of the argument user_id leads to sql injection. This vulnerability was named CVE-2023-1940. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1909	PHPGurukul BP Monitoring Management System 1.0 User Profile Update profile.php name/mobno sql injection	A vulnerability which was classified as critical was found in PHPGurukul BP Monitoring Management System 1.0. Affected is an unknown function of the file profile.php of the component User Profile Update Handler. The manipulation of the argument name/mobno leads to sql injection. This vulnerability is traded as CVE-2023-1909. 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-2020-36074	SourceCodester Tailor Mangement System 1.0 title sql injection	A vulnerability classified as critical was found in SourceCodester Tailor Mangement System 1.0. This vulnerability affects unknown code. The manipulation of the argument title leads to sql injection. This vulnerability was named CVE-2020-36074. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2020-36072	SourceCodester Tailor Management System 1.0 id sql injection	A vulnerability classified as critical has been found in SourceCodester Tailor Management System 1.0. This affects an unknown part. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2020-36072. 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-2023-1959	SourceCodester Online Computer and Laptop Store 1.0 Master.php category sql injection	A vulnerability has been found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. This vulnerability affects unknown code of the file /classes/Master.phpfsave_category. The manipulation of the argument category leads to sql injection. This vulnerability was named CVE-2023-1959. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1954	SourceCodester Online Computer and Laptop Store 1.0 manage.php save_inventory id sql injection	A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0. It has been rated as critical. This issue af-fects the function save_inventory of the file /admin/product/manage.php. The manipulation of the argu-ment id leads to sql injection. The identification of this vulnerability is CVE-2023-1954. The at-tack may be initiated remotely. Further-more there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1955	SourceCodester Online Computer and Laptop Store 1.0 User Registration login.php email sql injection	A vulnerability classified as critical has been found in SourceCodester Online Computer and Laptop Store 1.0. Affected is an unknown function of the file login.php of the com-ponent User Registration. The manipulation of the argument email leads to sql injection. This vulnerability is traded as CVE-2023-1955. It is possible to launch the attack remotely. Further-more there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1952	SourceCodester Online Computer and Laptop Store 1.0 Product Search /?p=products search sql injection	A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0. It has been classified as critical. This affects an unknown part of the file /pproducts of the component Product Search. The manipulation of the argument search leads to sql injection. This vulnerability is uniquely identified as CVE-2023-1952. It is possible to initiate the attack remote-ly. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1949	PHPGurukul BP Monitoring Manage-ment System 1.0 Change Password change-password.php password sql injection	A vulnerability which was classified as critical was found in PHPGurukul BP Monitoring Management System 1.0. Affected is an unknown function of the file change-password.php of the component Change Password Handler. The manipulation of the argument password leads to sql injection. This vulnerability is traded as CVE-2023-1949. It is possible to launch the attack remotely. Further-more there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1950	PHPGurukul BP Mon-itoring Management System 1.0 Password Recovery pass-word-recovery.php emailid/contactno sql injection	A vulnerability has been found in PHPGurukul BP Monitoring Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file password-recov-ery.php of the component Password Recovery. The manipulation of the argu-ment emailid/contactno leads to sql injection. This vulnerability is known as CVE-2023-1950. The attack can be launched re-motely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1953	SourceCodester Online Computer and Laptop Store 1.0 /ad-min/sales/index.php date_start/date_end sql injection	A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0. It has been de-clared as critical. This vul-nerability affects unknown code of the file /admin/sales/index.php. The ma-nipulation of the argument date_start/date_end leads to sql injection. This vulnerability was named CVE-2023-1953. The attack can be initiated remotely. Furthermore there is an exploit avail-able.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1957	SourceCodester Online Computer and Laptop Store 1.0 Subcategory Master.php sub_category sql injection	A vulnerability which was classified as critical has been found in Source-Codester Online Computer and Laptop Store 1.0. Affected by this issue is some unknown function-ality of the file /classes/Master.phpfsave_sub_category of the compo-nent Subcategory Handler. The manipulation of the argument sub_category leads to sql injection. This vulnerability is handled as CVE-2023-1957. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1960	SourceCodester Online Computer and Laptop Store 1.0 Master.php id sql injection	A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. This issue affects some unknown processing of the file /classes/Master.phpfdelete_category. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2023-1960. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1958	SourceCodester Online Computer and Laptop Store 1.0 Master.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Online Computer and Laptop Store 1.0. This affects an unknown part of the file /classes/Master.phpfdelete_sub_category. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-1958. 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-2023-1951	SourceCodester Online Computer and Laptop Store 1.0 brand.php delete_brand id sql injection	A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. Affected by this issue is the function delete_brand of the file /admin/maintenance/brand.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-1951. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1964	PHPGurukul Bank Locker Management System 1.0 Password Reset recovery.php uname/mobile sql injection	A vulnerability classified as critical has been found in PHPGurukul Bank Locker Management System 1.0. Affected is an unknown function of the file recovery.php of the component Password Reset. The manipulation of the argument uname/mobile leads to sql injection. This vulnerability is traded as CVE-2023-1964. 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-2023-1962	SourceCodester Best Online News Portal 1.0 POST Parameter forgot-password.php username sql injection	A vulnerability classified as critical was found in SourceCodester Best Online News Portal 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/forgot-password.php of the component POST Parameter Handler. The manipulation of the argument username leads to sql injection. This vulnerability is known as CVE-2023-1962. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1963	PHPGurukul Bank Locker Management System 1.0 Search index.php searchinput sql injection	A vulnerability was found in PHPGurukul Bank Locker Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file index.php of the component Search. The manipulation of the argument searchinput leads to sql injection. The identification of this vulnerability is CVE-2023-1963. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1969	SourceCodester Online Eyewear Shop 1.0 GET Parameter manage_stock.php id sql injection	A vulnerability classified as critical was found in SourceCodester Online Eyewear Shop 1.0. This vulnerability affects unknown code of the file /admin/inventory/manage_stock.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-1969. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1425	CRM, Email & Marketing Automation Plugin prior 2.7.9.4 on WordPress sql injection	A vulnerability was found in CRM Email & Marketing Automation Plugin. 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-2023-1425. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-26860	Igbudget up to 1.0.3 on PrestaShop displayAjaxGener-ateBudget sql injection	A vulnerability which was classified as critical has been found in Igbudget up to 1.0.3. Affected by this issue is the function LgBudgetBudgetModuleFrontController::displayAjaxGenerateBudget. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-26860. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1730	SupportCandy Plugin up to 3.1.4 on WordPress parse_user_filters sql injection	A vulnerability which was classified as critical has been found in SupportCandy Plugin up to 3.1.4. This issue affects the function parse_user_filters. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-1730. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-29597	bloofox 0.5.2 index.php sql injection	A vulnerability classified as critical has been found in bloofox 0.5.2. This affects an unknown part of the file /index.phpmodecontent&page-pages&actionedit&eid1. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-29597. 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-2023-29598	lmxcms 1.4.1 index.php setbook sql injection	A vulnerability which was classified as critical has been found in lmxcms 1.4.1. This issue affects some unknown processing of the file index.php. The manipulation of the argument set-book leads to sql injection. The identification of this vulnerability is CVE-2023-29598. Ac-cess to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-27779	AM Presencia 3.7.3 Login Form user sql injection	A vulnerability has been found in AM Presencia 3.7.3 and classified as critical. Affected by this vulnerability is an unknown functionality of the component Login Form. The manipulation of the argument user leads to sql injection. This vulnerability is known as CVE-2023-27779. 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-2023-2047	Campcodes Advanced Online Voting System 1.0 login.php voter sql injection	A vulnerability was found in Campcodes Advanced Online Voting System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file login.php. The manipulation of the argument voter leads to sql injection. This vulnerability is handled as CVE-2023-2047. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-2074	Campcodes Online Traffic Offense Management System 1.0 / classes/Master.php id sql injection	A vulnerability was found in Campcodes Online Traffic Offense Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /classes/Master.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-2074. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-29622	Purchase Order Management 1.0 login.php password sql injection	A vulnerability was found in Purchase Order Management 1.0. It has been rated as critical. This issue affects some unknown processing of the file /purchase_order/admin/login.php. The manipulation of the argument password leads to sql injection. The identification of this vulnerability is CVE-2023-29622. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2051	Campcodes Advanced Online Voting System 1.0 /admin/positions_row.php id sql injection	A vulnerability classified as critical has been found in Campcodes Advanced Online Voting System 1.0. Affected is an unknown function of the file /admin/positions_row.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-2051. 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-2023-2073	Campcodes Online Traffic Offense Management System 1.0 /classes/Login.php password sql injection	A vulnerability was found in Campcodes Online Traffic Of-fense Management System 1.0. It has been declared as criti-cal. Affected by this vulnerability is an unknown functionality of the file /classes/Login.php. The manipulation of the argu-ment password leads to sql injection. This vulnerability is known as CVE-2023-2073. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-29626	Yoga Class Registration System 1.0 / admin/login.php cid sql injection	A vulnerability classified as critical has been found in Yoga Class Registration System 1.0. Affected is an unknown function of the file /admin/login.php. The manipulation of the argument cid leads to sql injection. This vulnerability is traded as CVE-2023-29626. 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-2023-2052	Campcodes Advanced Online Voting System 1.0 /admin/ballot_down.php id sql injection	A vulnerability classified as critical was found in Campcodes Advanced Online Voting System 1.0. Affected by this vulnera-bility is an unknown functionality of the file /admin/ballot_down.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-2052. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2035	Campcodes Video Sharing Website 1.0 signup.php id sql injection	A vulnerability has been found in Campcodes Video Sharing Website 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file signup.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-2035. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2054	Campcodes Advanced Online Voting System 1.0 positions_delete.php id sql injection	A vulnerability which was classified as critical was found in Campcodes Advanced Online Voting System 1.0. This affects an unknown part of the file /admin/positions_delete.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2054. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-2075	Campcodes Online Traffic Offense Management System 1.0 view_details.php id sql injection	A vulnerability classified as critical has been found in Campcodes Online Traffic Offense Management System 1.0. This affects an unknown part of the file /admin/offenses/view_details.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2075. 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-2023-2041	novel-plus 3.6.2 list sort sql injection	A vulnerability classified as critical was found in novel-plus 3.6.2. Affected by this vulnerability is an unknown functionality of the file /category/listlimit10&offset0&orderdesc. The manipulation of the argument sort leads to sql injection. This vulnerability is known as CVE-2023-2041. The attack can be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2039	novel-plus 3.6.2 list sort sql injection	A vulnerability was found in novel-plus 3.6.2. It has been rated as critical. This issue affects some unknown processing of the file /author/listlimit10&offset0&orderdesc. The manipulation of the argument sort leads to sql injection. The identification of this vulnerability is CVE-2023-2039. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2036	Campcodes Video Sharing Website 1.0 upload.php id sql injection	A vulnerability was found in Campcodes Video Sharing Web-site 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file upload.php. The manipula-tion of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-2036. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2040	novel-plus 3.6.2 list sort sql injection	A vulnerability classified as critical has been found in novel-plus 3.6.2. Affected is an unknown function of the file /news/listlimit10&offset0&orderdesc. The manipulation of the argument sort leads to sql injection. This vulnerability is traded as CVE-2023-2040. It is possible to launch the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2038	Campcodes Video Sharing Website 1.0 admin_class.php email sql injection	A vulnerability was found in Campcodes Video Sharing Website 1.0. It has been declared as critical. This vulnerability affects unknown code of the file admin_class.php. The manipulation of the argument email leads to sql injection. This vulnerability was named CVE-2023-2038. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2037	Campcodes Video Sharing Website 1.0 watch.php code sql injection	A vulnerability was found in Campcodes Video Sharing Website 1.0. It has been classified as critical. This affects an unknown part of the file watch.php. The manipulation of the argument code leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2037. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-2049	Campcodes Advanced Online Voting System 1.0 /admin/ballot_up.php id sql injection	A vulnerability was found in Campcodes Advanced Online Voting System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/ballot_up-.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-2049. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-27649	Trusted Tools Free Music 1.8.2.43/1.9.1.45/2.0.0.46/2.1.0.47 Search History sql injection	A vulnerability classified as critical has been found in Trusted Tools Free Music 1.8.2.43/1.9.1.45/2.0.0.46/2.1.0.47. Affected is an unknown function of the component Search History Handler. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-27649. 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-2023-2050	Campcodes Advanced Online Voting System 1.0 /admin/positions_add.php description sql injection	A vulnerability was found in Campcodes Advanced Online Voting System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/positions_add.php. The manipulation of the argument description leads to sql injection. The identification of this vulnerability is CVE-2023-2050. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2048	Campcodes Advanced Online Voting System 1.0 /admin/voters_row.php id sql injection	A vulnerability was found in Campcodes Advanced Online Voting System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/voters_row.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2048. 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-2023-2053	Campcodes Advanced Online Voting System 1.0 candidates_row.php id sql injection	A vulnerability which was classified as critical has been found in Campcodes Advanced Online Voting System 1.0. Affected by this issue is some unknown functionality of the file /admin/candidates_row.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-2053. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2094	SourceCodester Vehicle Service Management System 1.0 manage_mechanic.php id sql injection	A vulnerability has been found in SourceCodester Vehicle Service Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/mechanics/manage_mechanic.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-2094. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-45030	rConfig 3.9.7 ajaxCompareGetCmdDates.php command sql injection (ID 171613)	A vulnerability has been found in rConfig 3.9.7 and classified as critical. This vulnerability affects unknown code in the library lib/ajaxHandlers/ajaxCompareGetCmdDates.php. The manipulation of the argument command leads to sql injection. This vulnerability was named CVE-2022-45030. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-2090	SourceCodester Employee and Visitor Gate Pass Logging System 1.0 GET Parameter view_designation.php id sql injection	A vulnerability classified as critical has been found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. Affected is an unknown function of the file /admin/maintenance/view_designation.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-2090. 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-2023-2107	IBOS 4.5.5 del&op=recycle fids sql injection	A vulnerability which was classified as critical was found in IBOS 4.5.5. Affected is an unknown function of the file file/personal/del&opre-cycle. The manipulation of the argument fids leads to sql injection. This vulnerability is traded as CVE-2023-2107. 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-2023-2092	SourceCodester Vehicle Service Management System 1.0 view_service.php id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Vehicle Service Management System 1.0. Affected by this issue is some unknown functionality of the file view_service.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-2092. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2097	SourceCodester Vehicle Service Management System 1.0 /classes/Master.php id sql injection	A vulnerability was found in SourceCodester Vehicle Service Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /classes/Master.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-2097. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2096	SourceCodester Vehicle Service Management System 1.0 manage_inventory.php id sql injection	A vulnerability was found in SourceCodester Vehicle Service Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/service_requests/manage_inventory.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-2096. 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-2023-2093	SourceCodester Vehicle Service Management System 1.0 /classes/Login.php username sql injection	A vulnerability which was classified as critical was found in SourceCodester Vehicle Service Management System 1.0. This affects an unknown part of the file /classes/Login.php. The manipulation of the argument username leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2093. 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-2023-2095	SourceCodester Vehicle Service Management System 1.0 manage_category.php id sql injection	A vulnerability was found in SourceCodester Vehicle Service Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/maintenance/manage_category.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2023-2095. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-36520	I-Tech Trainsmart r1044 assign-evaluation id sql injection (ID 171731)	A vulnerability was found in I-Tech Trainsmart r1044 and classified as critical. This issue affects some unknown processing of the file evaluation/assign-evaluation. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2021-36520. 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-2023-27733	DedeCMS 5.7.106 / dede/sys_sql_query.php sql injection	A vulnerability was found in DedeCMS 5.7.106. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file / dede/sys_sql_query.php. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-27733. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2130	SourceCodester Purchase Order Management Sys-tem 1.0 GET Parameter view_details.php id sql injection	A vulnerability classified as critical has been found in SourceCodester Purchase Order Management System 1.0. Affected is an unknown function of the file /admin/suppliers/view_details.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-2130. 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-2023-0765	BestWebSoft Gallery Plugin up to 4.6.x on WordPress escape sql injection	A vulnerability classified as critical was found in BestWebSoft Gallery Plugin up to 4.6.x on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation of the argument escape leads to sql injection. This vulnerability is known as CVE-2023-0765. The attack can only be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-30558	Archery sql/data_dictionary.py sql injection (GHSA-jwjj-jgfv-x66q)	A vulnerability which was classified as critical has been found in Archery. This issue affects some unknown processing of the file sql/data_dictionary.py. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-30558. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-30605	Archery sql/instance.py sql injection (GHSA-6mqc-w2qp-fvhp)	A vulnerability classified as critical has been found in Archery. Affected is an unknown function of the file sql/instance.py. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-30605. 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-2023-2209	Campcodes Coffee Shop POS System 1.0 view_details.php id sql injection	A vulnerability which was classified as critical was found in Campcodes Coffee Shop POS System 1.0. Affected is an unknown function of the file /admin/sales/view_details.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-2209. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-2210	Campcodes Coffee Shop POS System 1.0 view_category.php id sql injection	A vulnerability has been found in Campcodes Coffee Shop POS System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/categories/view_category.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-2210. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2213	Campcodes Coffee Shop POS System 1.0 manage_product.php id sql injection	A vulnerability was found in Campcodes Coffee Shop POS System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/products/manage_product.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-2213. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2211	Campcodes Coffee Shop POS System 1.0 manage_category.php id sql injection	A vulnerability was found in Campcodes Coffee Shop POS System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/categories/manage_category.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-2211. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2204	Campcodes Retro Basket-ball Shoes Online Store 1.0 faqs.php id sql injection	A vulnerability was found in Campcodes Retro Basketball Shoes Online Store 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file faqs.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-2204. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2207	Campcodes Retro Basketball Shoes Online Store 1.0 contactus1.php email sql injection	A vulnerability classified as critical was found in Campcodes Retro Basketball Shoes Online Store 1.0. This vulnerability affects unknown code of the file contactus1.php. The manipulation of the argument email leads to sql injection. This vulnerability was named CVE-2023-2207. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2206	Campcodes Retro Basketball Shoes Online Store 1.0 contactus.php email sql injection	A vulnerability classified as critical has been found in Campcodes Retro Basketball Shoes Online Store 1.0. This affects an unknown part of the file contactus.php. The manipulation of the argument email leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2206. 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-2023-2205	Campcodes Retro Basketball Shoes Online Store 1.0 / function/login.php email sql injection	A vulnerability was found in Campcodes Retro Basketball Shoes Online Store 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file / function/login.php. The manipulation of the argument email leads to sql injection. This vulnerability is handled as CVE-2023-2205. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-2215	Campcodes Coffee Shop POS System 1.0 manage_user.php id sql injection	A vulnerability classified as critical has been found in Camp-codes Coffee Shop POS System 1.0. Affected is an unknown function of the file /admin/user/manage_user.php. The ma-nipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-2215. It is possible to launch the attack remotely. Further-more there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2214	Campcodes Coffee Shop POS System 1.0 manage_sale.php id sql injection	A vulnerability was found in Campcodes Coffee Shop POS System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/sales/man-age_sale.php. The manip-ulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2023-2214. The attack may be initiated remotely. Further-more there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2212	Campcodes Coffee Shop POS System 1.0 view_product.php id sql injection	A vulnerability was found in Campcodes Coffee Shop POS System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/products/view_product.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2212. It is possible to initiate the attack remote-ly. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2208	Campcodes Retro Basketball Shoes On-line Store 1.0 details.php id sql injection	A vulnerability which was classified as critical has been found in Campcodes Retro Basketball Shoes Online Store 1.0. This issue affects some unknown processing of the file de-tails.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2023-2208. The attack may be initiated remotely. Further-more there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-30076	Sourcecodester Judging Manage-ment System 1.0 print_judges.php sql injection	A vulnerability was found in Sourcecodester Judging Management System 1.0 and classified as critical. Affected by this issue is some unknown function-ality of the file /php-jms/print_judges.phpprint_judges.php&se_name&sub_event_id. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-30076. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-26876	Piwigo up to 13.5.0 admin.php filter_user_id sql injection	A vulnerability was found in Piwigo up to 13.5.0. It has been classified as critical. Affected is an unknown function of the file admin.phppagehisto-ry&filter_image_id. The manipulation of the argument filter_user_id leads to sql injection. This vulnerability is traded as CVE-2023-26876. 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-2023-2243	SourceCodester Complaint Manage-ment System 1.0 POST Parameter us-ers/registration.php fullname sql injection	A vulnerability was found in SourceCodester Complaint Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file users/registration.php of the component POST Parameter Handler. The manipulation of the argu-ment fullname leads to sql injection. This vulnerability is handled as CVE-2023-2243. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-2244	SourceCodester Online Eyewear Shop 1.0 GET Parameter update_status.php id sql injection	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been classified as critical. This affects an unknown part of the file /admin/orders/update_status.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2244. 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-2023-2242	SourceCodester Online Computer and Laptop Store 1.0 GET Parameter c/s sql injection	A vulnerability has been found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the component GET Parameter Handler. The manipulation of the argument c/s leads to sql injection. This vulnerability is known as CVE-2023-2242. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-26865	bdroppy up to 2.2.12 on PrestaShop importProd-ucts sql injection	A vulnerability which was classified as critical was found in bdroppy up to 2.2.12 on PrestaShop. Affected is the function BdroppyCronModuleFront-Controller::importProducts. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-26865. 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-2023-29849	Bang Resto 1.0 sql injection	A vulnerability which was classified as critical has been found in Bang Resto 1.0. Affected by this issue is some unknown functionality. The manipulation of the argument btnMenu-ItemID/itemID/itemPrice/menuID/staffID/itemqty leads to sql injection. This vulnerability is handled as CVE-2023-29849. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-23753	Visforms Base Package Extension on Joomla sql injection	A vulnerability was found in Visforms Base Package Extension on Joomla. It has been classified as critical. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-23753. 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-2023-1020	Steveas WP Live Chat Shoutbox Plugin up to 1.4.2 on WordPress AJAX Action sql injection	A vulnerability which was classified as critical was found in Steveas WP Live Chat Shoutbox Plugin up to 1.4.2 on WordPress. Affected is an unknown function of the component AJAX Action Handler. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-1020. 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-2023-0388	Random Text Plugin up to 0.3.0 on WordPress sql injection	A vulnerability which was classified as critical has been found in Random Text Plugin up to 0.3.0 on WordPress. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-0388. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-30211	OURPHP up to 7.2.0 sql injection	A vulnerability was found in OURPHP up to 7.2.0 and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-30211. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2348	SourceCodester Service Provider Management System 1.0 manage_user.php id sql injection	A vulnerability was found in SourceCodester Service Provider Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/user/manage_user.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2023-2348. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-2346	SourceCodester Service Provider Management System 1.0 view_inquiry.php id sql injection	A vulnerability was found in SourceCodester Service Provider Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/inquiries/view_inquiry.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-2346. 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-2023-2347	SourceCodester Service Provider Management System 1.0 manage_service.php id sql injection	A vulnerability was found in SourceCodester Service Provider Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/services/manage_service.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-2347. The attack can be initiated remotely. Furthermore there is an 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-2023-1799	EyouCMS up to 1.5.4 login.php tag_tag cross-site scripting	A vulnerability which was classified as problematic was found in EyouCMS up to 1.5.4. This affects an unknown part of the file login.php. The manipulation of the argument tag_tag leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-1799. 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-2023-1798	EyouCMS up to 1.5.4 login.php typename cross-site scripting	A vulnerability which was classified as problematic has been found in EyouCMS up to 1.5.4. Affected by this issue is some unknown functionality of the file login.php. The manipulation of the argument typename leads to cross-site scripting. This vulnerability is handled as CVE-2023-1798. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-1795	SourceCodester Gadget Works Online Ordering System 1.0 GET Parameter index.php view cross-site scripting	A vulnerability was found in SourceCodester Gadget Works Online Ordering System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/products/index.php of the component GET Parameter Handler. The manipulation of the argument view with the input <script>alert</script> leads to cross-site scripting. The identification of this vulnerability is CVE-2023-1795. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1796	SourceCodester Employee Payslip Generator 1.0 Create News Master.php name cross-site scripting	A vulnerability classified as problematic has been found in SourceCodester Employee Payslip Generator 1.0. Affected is an unknown function of the file /classes/Master.phpfsave_position of the component Create News Handler. The manipulation of the argument name with the input <script>alert</script> leads to cross-site scripting. This vulnerability is traded as CVE-2023-1796. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-1794	SourceCodester Police Crime Record Management System 1.0 GET Parameter /admin/casedetails.php id cross-site scripting	A vulnerability was found in SourceCodester Police Crime Record Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/casedetails.php of the component GET Parameter Handler. The manipulation of the argument id with the input "><script>alert</script> leads to cross-site scripting. This vulnerability was named CVE-2023-1794. 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-2023-0399	Image Over Image for WPBakery Page Builder Plugin up to 2.x on WordPress Shortcode Attribute cross-site scripting	A vulnerability classified as problematic has been found in Image Over Image for WPBakery Page Builder Plugin up to 2.x. This affects an unknown part of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-0399. 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-2023-24724	SAS 9.4 User Management Module cross-site scripting	A vulnerability classified as problematic has been found in SAS 9.4. This affects an unknown part of the component User Management Module. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-24724. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-47870	Redgate SQL Monitor 12.1.31.893 returnUrl cross-site scripting (ID 171647)	A vulnerability was found in Redgate SQL Monitor 12.1.31.893. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument returnUrl leads to cross-site scripting. This vulnerability was named CVE-2022-47870. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2020-19277	Phachon mm-wiki 0.1.2 Markdown Editor cross-site scripting (ID 68)	A vulnerability classified as problematic was found in Phachon mm-wiki 0.1.2. This vulnerability affects unknown code of the component Markdown Editor. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2020-19277. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2020-19698	Pandao http://Editor.md 1.5.0 editor cross-site scripting (ID 700)	A vulnerability has been found in Pandao http://Editor.md 1.5.0 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument editor leads to cross-site scripting. This vulnerability is known as CVE-2020-19698. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2020-19699	KOHGYLW Kiftd 1.0.18 Upload File Page cross-site scripting (ID 32)	A vulnerability was found in KOHGYLW Kiftd 1.0.18 and classified as problematic. Affected by this issue is some unknown functionality of the component Upload File Page. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2020-19699. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2020-19697	Pandao http://Editor.md 1.5.0 src cross-site scripting (ID 701)	A vulnerability which was classified as problematic was found in Pandao http://Editor.md 1.5.0. Affected is an unknown function. The manipulation of the argument src leads to cross-site scripting. This vulnerability is traded as CVE-2020-19697. 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-2020-20521	KiteCMS 1.1 comment cross-site scripting	A vulnerability has been found in KiteCMS 1.1 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument comment leads to cross-site scripting. This vulnerability was named CVE-2020-20521. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2020-22533	Zentao lang cross-site scripting	A vulnerability classified as problematic has been found in Zentao. Affected is an unknown function. The manipulation of the argument lang leads to cross-site scripting. This vulnerability is traded as CVE-2020-22533. 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-2020-20522	KiteCMS 1.1 user cross-site scripting	A vulnerability was found in KiteCMS 1.1 and classified as problematic. This issue affects some unknown processing. The manipulation of the argument user leads to cross-site scripting. The identification of this vulnerability is CVE-2020-20522. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-1377	Solidres Plugin up to 0.9.4 on WordPress cross-site scripting	A vulnerability classified as problematic was found in Solidres Plugin up to 0.9.4. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-1377. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-28850	Pimcore Perspective Editor up to 1.5.1 cross-site scripting (GHSA-fq8q-55v3-2986)	A vulnerability has been found in Pimcore Perspective Editor up to 1.5.1 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-2023-28850. The attack can be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0357	Helpy 2.8.0 cross-site scripting	A vulnerability which was classified as problematic was found in Helpy 2.8.0. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-0357. 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-2023-0486	Telesoft VitalPBX 3.2.3-8 cross-site scripting	A vulnerability was found in Telesoft VitalPBX 3.2.3-8 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-2023-0486. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-1853	SourceCodester Online Payroll System 1.0 /admin/employee_edit.php of cross-site scripting	A vulnerability which was classified as problematic has been found in SourceCodester Online Payroll System 1.0. This issue affects some unknown processing of the file /admin/employee_edit.php. The manipulation of the argu-ment of leads to cross-site scripting. The identification of this vulnerability is CVE-2023-1853. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1857	SourceCodester Online Computer and Laptop Store 1.0 Product Name cross-site scripting	A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/page-product/manage_product&id2. The manipulation of the argument Product Name leads to cross-site scripting. This vulnerability is handled as CVE-2023-1857. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0325	Uvdesk 1.1.1 cross-site scripting	A vulnerability which was classified as problematic has been found in Uvdesk 1.1.1. This issue affects some unknown pro-cessing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-0325. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-1851	SourceCodester Online Payroll System 1.0 /admin/employee_add.php of cross-site scripting	A vulnerability classified as problematic has been found in SourceCodester Online Payroll System 1.0. This affects an unknown part of the file /admin/employee_add.php. The manipulation of the argument of leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-1851. 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-2023-1852	SourceCodester Online Payroll System 1.0 deduction_edit.php description cross-site scripting	A vulnerability classified as problematic was found in SourceCodester Online Payroll System 1.0. This vulnerability affects unknown code of the file /admin/deduction_edit.php. The manipulation of the argument description leads to cross-site scripting. This vulnerability was named CVE-2023-1852. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-27620	RoboSoft Image Gallery plugin up to 3.2.12 on WordPress cross-site scripting	A vulnerability classified as problematic was found in RoboSoft Image Gallery plugin up to 3.2.12. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-27620. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-1948	PHPGurukul BP Monitoring Management System 1.0 Add New Family Member add-family-member.php Member Name cross-site scripting	A vulnerability which was classified as problematic has been found in PHPGurukul BP Monitoring Management System 1.0. This issue affects some unknown processing of the file add-family-member.php of the component Add New Family Member Handler. The manipulation of the argument Member Name leads to cross-site scripting. The identification of this vulnerability is CVE-2023-1948. 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-2023-0363	Scheduled Announcements Widget Plugin up to 0.x on WordPress Shortcode Attribute cross-site scripting	A vulnerability which was classified as problematic was found in Scheduled Announcements Widget Plugin up to 0.x. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-0363. 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-2023-26120	Xuxueli xxl-job /xxl-job-admin/user/add cross-site scripting (SNYK-JAVA-COMXUXUELI-3248764)	A vulnerability which was classified as problematic has been found in Xuxueli xxl-job. This issue affects some unknown processing of the file /xxl-job-admin/user/add. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-26120. 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-2023-0423	Amazon S3 Plugin Plugin up to 1.5 on WordPress cross-site scripting	A vulnerability was found in Amazon S3 Plugin Plugin up to 1.5. 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-2023-0423. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-4827	WP Tiles Plugin up to 1.1.2 on WordPress Shortcode Attribute cross-site scripting	A vulnerability which was classified as problematic has been found in WP Tiles Plugin up to 1.1.2. This issue affects some unknown processing of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-4827. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-37462	Cisco Upstream Works Agent Desktop for Cisco Finesse up to 4.2.12/5.0 File Upload AttachmentId cross-site scripting	A vulnerability was found in Cisco Upstream Works Agent Desktop for Cisco Finesse up to 4.2.12/5.0. It has been rated as problematic. This issue affects some unknown processing of the component File Upload Handler. The manipulation of the argument AttachmentId leads to cross-site scripting. The identification of this vulnerability is CVE-2022-37462. 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-2023-0874	Klaviyo Plugin up to 3.0.9 on WordPress Setting cross-site scripting	A vulnerability was found in Klaviyo Plugin up to 3.0.9. It has been rated as problematic. This issue affects some unknown processing of the component Setting Handler. The manipula-tion leads to cross-site scripting. The identification of this vulnerability is CVE-2023-0874. 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-2023-1121	Simple Giveaways Plugin up to 2.45.0 on WordPress Setting cross-site scripting	A vulnerability classified as problematic was found in Simple Giveaways Plugin up to 2.45.0. 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-2023-1121. 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-2023-1122	Simple Giveaways Plugin up to 2.45.0 on WordPress cross-site scripting	A vulnerability which was classified as problematic has been found in Simple Giveaways Plugin up to 2.45.0. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-1122. 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-2023-0893	Time Sheets Plugin up to 1.29.2 on WordPress Setting cross-site scripting	A vulnerability was found in Time Sheets Plugin up to 1.29.2. It has been declared as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-0893. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0157	All-In-One Security Plugin up to 5.1.4 on WordPress Log File cross-site scripting	A vulnerability was found in All-In-One Security Plugin up to 5.1.4. It has been classified as problematic. Affected is an unknown function of the component Log File Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-0157. 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-2023-24181	LuCI Openwrt 22.03 / openvpn/pageswitch.htm cross-site scripting (GHSA-9gqg-pp5p-q9hg)	A vulnerability was found in LuCI Openwrt 22.03. It has been classified as problematic. Affected is an unknown function of the file /openvpn/pageswitch.htm. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-24181. It is possible to launch the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0422	Article Directory Plugin up to 1.3 on WordPress Setting publish_terms_text cross-site scripting	A vulnerability has been found in Article Directory Plugin up to 1.3 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation of the argument publish_terms_text leads to cross-site scripting. This vulnerability is known as CVE-2023-0422. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0983	stylish-cost-calculator-premium Plugin up to 7.8.x on WordPress cross-site scripting	A vulnerability classified as problematic was found in stylish-cost-calculator-premium Plugin up to 7.8.x. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-0983. 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-2023-26919	delight-nashorn-sandbox 0.2.4/0.2.5 Java Process loadWithNewGlobal (ID 135)	A vulnerability was found in delight-nashorn-sandbox 0.2.4/0.2.5 and classified as critical. Affected by this issue is the function loadWithNewGlobal of the component Java Process Handler. The manipulation leads to sandbox issue. This vulnerability is handled as CVE-2023-26919. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-1120	Simple Giveaways Plugin up to 2.45.0 on WordPress Setting cross-site scripting	A vulnerability classified as problematic has been found in Simple Giveaways Plugin up to 2.45.0. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-1120. 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-2023-0605	Auto Rename Media On Upload Plugin up to 1.0.x on WordPress Setting cross-site scripting	A vulnerability was found in Auto Rename Media On Upload Plugin up to 1.0.x 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-2023-0605. 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-2023-26773	Sales Tracker Management System 1.0 Product List Master.php cross-site scripting (ID 171686)	A vulnerability which was classified as problematic has been found in Sales Tracker Management System 1.0. Affected by this issue is some unknown functionality of the file Master.php of the component Product List. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-26773. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-24182	LuCI Openwrt 22.03 /system/sshkeys.js cross-site scripting (GHSA-7vqh-2r8q-rjg2)	A vulnerability was found in LuCI Openwrt 22.03. It has been declared as problematic. This vulnerability affects unknown code of the file /system/sshkeys.js. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-24182. The attack can 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-2023-24721	LiveAction LiveSP 21.1.2 cross-site scripting	A vulnerability was found in LiveAction LiveSP 21.1.2. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-24721. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-27775	LiveAction LiveSP 21.1.2 cross-site scripting	A vulnerability was found in LiveAction LiveSP 21.1.2 and clas-sified as problematic. This issue affects some unknown pro-cessing. The manipulation leads to basic cross-site scripting. The identification of this vulnerability is CVE-2023-27775. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-1804	PixelYourSite Product Catalog Feed Plugin up to 2.1.0 on WordPress cross-site scripting	A vulnerability was found in PixelYourSite Product Catalog Feed Plugin up to 2.1.0 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-1804. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-29206	XWiki xwiki-platform-skin-skinx cross-site scripting	A vulnerability classified as problematic has been found in XWiki xwiki-platform-skin-skinx. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-29206. 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-2023-29506	XWiki xwiki-platform-security-authentication-default cross-site scripting	A vulnerability was found in XWiki xwiki-platform-security-authentication-default. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-29506. 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-2023-2021	nilsteampassnet teampass up to 3.0.2 cross-site scripting	A vulnerability was found in nilsteampassnet teampass up to 3.0.2. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-2021. 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-2023-29207	XWiki xwiki-platform-flamingo/ xwiki-platform-web cross-site scripting	A vulnerability which was classified as problematic was found in XWiki xwiki-platform-flamingo and xwiki-platform-web. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-29207. 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-2023-29205	XWiki xwiki-platform-rendering-xwiki prior 14.8-rc-1 cross-site scripting	A vulnerability has been found in XWiki xwiki-platform-rendering-xwiki 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-2023-29205. 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-2023-29202	XWiki xwiki-platform-rendering-macro-rss cross-site scripting	A vulnerability was found in XWiki xwiki-platform-rendering-macro-rss 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-2023-29202. 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-2023-29201	XWiki xwiki-commons-xml prior 14.6-rc-1 cross-site scripting	A vulnerability was found in XWiki xwiki-commons-xml. 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-2023-29201. 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-2023-2014	microweber up to 1.3.2 cross-site scripting	A vulnerability has been found in microweber up to 1.3.2 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-2023-2014. 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-2023-1805	PixelYourSite Product Catalog Feed Plugin up to 2.1.0 on WordPress page cross-site scripting	A vulnerability has been found in PixelYourSite Product Cata-log Feed Plugin up to 2.1.0 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument page leads to cross-site scripting. This vulnerability was named CVE-2023-1805. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-1861	Limit Login Attempts Plugin up to 1.7.1 on WordPress cross-site scripting	A vulnerability was found in Limit Login Attempts Plugin up to 1.7.1. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-1861. 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-2023-2077	Campcodes Online Traffic Offense Management System 1.0 view_details.php id cross-site scripting	A vulnerability which was classified as problematic has been found in Campcodes Online Traffic Offense Management System 1.0. This issue affects some unknown processing of the file /admin/offenses/view_details.php. The manipulation of the argument id leads to cross-site scripting. The identification of this vulnerability is CVE-2023-2077. 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-2023-26123	raysan5 raylib up to 4.4.x SetClipboardText API emscripten_run_script cross-site scripting (ID 2954)	A vulnerability which was classified as problematic has been found in raysan5 raylib up to 4.4.x. This issue affects the function emscripten_run_script of the component SetClipboardText API. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-26123. 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-2023-2076	Campcodes Online Traffic Offense Management System 1.0 /classes/Users.phpp id cross-site scripting	A vulnerability classified as problematic was found in Campcodes Online Traffic Offense Management System 1.0. This vulnerability affects unknown code of the file /classes/Users.phpp. The manipulation of the argument id leads to cross-site scripting. This vulnerability was named CVE-2023-2076. 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-2023-29847	AeroCMS 0.0.1 /post.php comment_author/comment_content cross-site scripting (ID 11)	A vulnerability classified as problematic was found in AeroCMS 0.0.1. Affected by this vulnerability is an unknown functionality of the file /post.php. The manipulation of the argument comment_author/comment_content leads to cross-site scripting. This vulnerability is known as CVE-2023-29847. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-2058	EyouCms up to 1.6.2 HTTP POST Request web_ico cross-site scripting	A vulnerability was found in EyouCms up to 1.6.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /yxcms/index.phpradmin/extendfield/meseditamp;tabid12amp;id4 of the component HTTP POST Request Handler. The manipulation of the argument web_ico leads to cross-site scripting. This vulnerability is known as CVE-2023-2058. 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-2023-29623	Purchase Order Management 1.0 login.php password cross-site scripting	A vulnerability has been found in Purchase Order Manage-ment 1.0 and classified as problematic. Affected by this vul-nerability is an unknown functionality of the file /purchase_order/classes/login.php. The manipulation of the argument password leads to cross-site scripting. This vulnerability is known as CVE-2023-29623. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-2055	Campcodes Advanced Online Voting System 1.0 /admin/config_save.php title cross-site scripting	A vulnerability has been found in Campcodes Advanced Online Voting System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/config_save.php. The manipulation of the argument title leads to cross-site scripting. This vulnerability was named CVE-2023-2055. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1649	AI ChatBot Plugin up to 4.4.9 on WordPress cross-site scripting	A vulnerability has been found in AI ChatBot Plugin up to 4.4.9 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-2023-1649. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-2057	EyouCms 1.5.4 New Picture login.php litpic_loca cross-site scripting	A vulnerability was found in EyouCms 1.5.4. It has been classi-fied as problematic. Affected is an unknown function of the file login.phpmadmin&-cArctype&aedit of the com-ponent New Picture Handler. The manipulation of the argu-ment litpic_loca leads to cross-site scripting. This vulnerability is traded as CVE-2023-2057. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-2100	SourceCodester Vehicle Service Management System 1.0 / admin/report/index.php date_end cross-site scripting	A vulnerability classified as problematic was found in SourceCodester Vehicle Service Management System 1.0. This vulnerability affects unknown code of the file /admin/report/index.php. The manipulation of the argument date_end leads to cross-site scripting. This vulnerability was named CVE-2023-2100. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-48178	X2CRM Open Source Sales CRM 6.6/6.9 index.php/actions/update cross-site scripting (ID 171792)	A vulnerability was found in X2CRM Open Source Sales CRM 6.6/6.9. It has been declared as problematic. This vulnerability affects unknown code of the file index.php/actions/update. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-48178. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-48177	X2CRM Open Source Sales CRM 6.6/6.9 adin/importModels cross-site scripting (ID 171792)	A vulnerability which was classified as problematic has been found in X2CRM Open Source Sales CRM 6.6/6.9. Affected by this issue is some unknown functionality of the file adin/importModels. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-48177. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-2103	alextselegidis easyappointments up to 1.4.x cross-site scripting	A vulnerability classified as problematic has been found in alextselegidis easyappointments up to 1.4.x. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-2103. 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-2023-2102	alextselegidis easyappointments up to 1.4.x cross-site scripting	A vulnerability was found in alextselegidis easyappointments up to 1.4.x. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-2102. 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-2023-2099	SourceCodester Vehicle Service Management System 1.0 / classes/Users.php id cross-site scripting	A vulnerability classified as problematic has been found in SourceCodester Vehicle Service Management System 1.0. This affects an unknown part of the file /classes/Users.php. The manipulation of the argument id leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-2099. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-2098	SourceCodester Vehicle Service Management System 1.0 /inc/topBarNav.php search cross-site scripting	A vulnerability was found in SourceCodester Vehicle Service Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /inc/topBarNav.php. The manipulation of the argument search leads to cross-site scripting. This vulnerability is handled as CVE-2023-2098. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-45849	Silkalns Activello Theme up to 1.4.4 on WordPress cross-site scripting	A vulnerability which was classified as problematic has been found in Silkalns Activello Theme up to 1.4.4 on WordPress. This issue affects some unknown processing. The manipula-tion leads to cross-site scripting. The identification of this vulnerability is CVE-2022-45849. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-1373	W4 Post List Plugin up to 2.4.5 on WordPress cross-site scripting	A vulnerability was found in W4 Post List Plugin up to 2.4.5 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-2023-1373. 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-2023-1473	MetaSlider Slider, Gallery, and Carousel Plugin 3.29.0 on WordPress cross-site scripting	A vulnerability was found in MetaSlider Slider Gallery and Carousel Plugin 3.29.0 on WordPress. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-1473. 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-2022-44726	TouchDown Timesheet Tracking Component 4.1.4 on Jira Calendar View cross-site scripting (SYSS-2022-050)	A vulnerability has been found in TouchDown Timesheet Tracking Component 4.1.4 on Jira and classified as problematic. This vulnerability affects unknown code of the component Calendar View. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-44726. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-0367	Pricing Tables for WPBakery Page Builder Plugin up to 2.x on WordPress Shortcode Attribute cross-site scripting	A vulnerability which was classified as problematic has been found in Pricing Tables for WPBakery Page Builder Plugin up to 2.x on WordPress. This issue affects some unknown processing of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-0367. 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-2023-1282	Drag and Drop Multiple File Upload Pro Plugin on WordPress cross-site scripting	A vulnerability was found in Drag and Drop Multiple File Upload Pro 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-2023-1282. 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-2023-1413	WP VR Plugin up to 8.2.8 on WordPress cross-site scripting	A vulnerability was found in WP VR Plugin up to 8.2.8 on WordPress. It has been declared as problematic. This vulner-ability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-1413. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0374	W4 Post List Plugin up to 2.4.5 on WordPress Block Option cross-site scripting	A vulnerability which was classified as problematic was found in W4 Post List Plugin up to 2.4.5 on WordPress. Affected is an unknown function of the component Block Option Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-0374. 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-2023-1325	Easy Forms for Mailchimp Plugin up to 6.8.6 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in Easy Forms for Mailchimp Plugin up to 6.8.6 on WordPress and classified as problematic. Affected by this issue is some unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-1325. 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-2023-27776	Online Jewelry Shop 1.0 in-dex.php Category Name cross-site scripting	A vulnerability was found in Online Jewelry Shop 1.0. It has been classified as problematic. This affects an unknown part of the file /index.phppagecatego-ry_list. The manipulation of the argument Category Name leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-27776. 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-2023-1767	Snyk Advisor Website Readme cross-site scripting	A vulnerability was found in Snyk Advisor Website. It has been declared as problematic. This vulnerability affects unknown code of the component Readme Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-1767. 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-2023-2191	azuracast up to 0.17 cross-site scripting	A vulnerability which was classified as problematic was found in azuracast up to 0.17. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-2191. 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-2023-27090	TeaCMS article title cross-site scripting	A vulnerability was found in TeaCMS and classified as problematic. This issue affects some unknown processing. The manipulation of the argument article title leads to cross-site scripting. The identification of this vulnerability is CVE-2023-27090. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-2220	Dream Technology mica up to 3.0.5 Form Object cross-site scripting (I6TGJD)	A vulnerability was found in Dream Technology mica up to 3.0.5. It has been classified as problematic. Affected is an unknown function of the component Form Object Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-2220. It is possible to launch the attack remotely. There is no exploit available. It is recommended to apply the suggested workaround.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2013-3565	VideoLAN VLC Media Player up to 2.0.6 Parameter requests/vlm_cmd.xml command cross-site scripting	A vulnerability classified as problematic has been found in VideoLAN VLC Media Player up to 2.0.6. This affects an unknown part of the file requests/vlm_cmd.xml of the component Parameter Handler. The manipulation of the argument command leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2013-3565. It is possible to initiate the attack remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-2142	Nunjucks prior 3.2.4 cross-site scripting	A vulnerability classified as problematic has been found in Nunjucks. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-2142. 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-2023-1892	sidekiq up to 7.0.7 cross-site scripting	A vulnerability was found in sidekiq up to 7.0.7. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-1892. 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-2023-2216	Campcodes Coffee Shop POS System 1.0 /classes/Users.php firstname cross-site scripting	A vulnerability classified as problematic was found in Campcodes Coffee Shop POS System 1.0. Affected by this vulnerability is an unknown functionality of the file /classes/Users.php. The manipulation of the argument firstname leads to cross-site scripting. This vulnerability is known as CVE-2023-2216. 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-2013-7351	Shaarli index.php importFile cross-site scripting (Issue 134 / XFDB-92215)	A vulnerability classified as problematic was found in Shaarli. This vulnerability affects the function importFile of the file index.php. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2013-7351. The attack can be initiated remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2012-6684	RedCloth Library up to 4.2.9 on Ruby cross-site scripting (ID 243)	A vulnerability which was classified as problematic has been found in RedCloth Library up to 4.2.9 on Ruby. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2012-6684. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-1875	thorsten phpmyfaq up to 3.1.11 cross-site scripting	A vulnerability classified as problematic was found in thorsten phpmyfaq up to 3.1.11. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-1875. 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-2023-29848	Bang Resto 1.0 Add New Menu admin/menu.php itemName cross-site scripting	A vulnerability classified as problematic has been found in Bang Resto 1.0. Affected is an unknown function of the file admin/menu.php of the component Add New Menu. The manipulation of the argument itemName leads to cross-site scripting. This vulnerability is traded as CVE-2023-29848. 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-2023-31045	Backdrop CMS up to 1.24.1 name cross-site scripting (Issue 6065)	A vulnerability has been found in Backdrop CMS up to 1.24.1 and classified as problematic. This vulnerability affects un-known code. The manipulation of the argument name leads to cross-site scripting. This vulnerability was named CVE-2023-31045. The attack can be initiated remotely. There is no exploit available. The real existence of this vulnerability is still doubted at the moment. 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-2023-0420	Custom Post Type and Taxonomy GUI Manager Plugin up to 1.1 on WordPress cross-site scripting	A vulnerability which was classified as problematic has been found in Custom Post Type and Taxono-my GUI Manager Plugin up to 1.1 on WordPress. This issue affects some un-known processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-0420. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site script-ing attack.
CVE-2023-0276	Weaver Xtreme Theme Support Plugin up to 6.2.6 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in Weaver Xtreme Theme Support Plugin up to 6.2.6 on WordPress. It has been rated as problematic. This issue affects some unknown processing of the component Short-code Attribute Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-0276. 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 script-ing attack.
CVE-2023-25347	ChurchCRM 4.5.3 EventEdi-tor.php Title cross-site scripting	A vulnerability was found in ChurchCRM 4.5.3 and classified as problematic. This issue affects some unknown processing of the file EventEditor.php. The manipulation of the argument Title leads to cross-site scripting. The identification of this vulnerability is CVE-2023-25347. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site script-ing attack.
CVE-2023-26843	ChurchCRM 4.5.3 NoteEditor.php cross-site scripting	A vulnerability was found in ChurchCRM 4.5.3. It has been rated as problematic. Affected by this issue is some unknown function-ality of the file NoteEditor. php. The manipulation leads to cross-site script-ing. This vulnerability is handled as CVE-2023-26843. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site script-ing attack.
CVE-2023-0899	Steveas WP Live Chat Shoutbox Plugin up to 1.4.2 on WordPress cross-site scripting	A vulnerability which was classified as problematic has been found in Steveas WP Live Chat Shoutbox Plugin up to 1.4.2 on Word-Press. Affected by this issue is some unknown function-ality. The manip-ulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-0899. 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 script-ing attack.
CVE-2023-1324	Easy Forms for Mailchimp Plugin up to 6.8.7 on Word-Press cross-site scripting	A vulnerability which was classified as problematic was found in Easy Forms for Mailchimp Plugin up to 6.8.7 on WordPress. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-1324. It is possible to initiate the attack re-motely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site script-ing attack.
CVE-2023-25346	ChurchCRM 4.5.3 not-found id cross-site scripting	A vulnerability classified as problematic was found in ChurchCRM 4.5.3. This vulnerability affects unknown code of the file / churchcrm/v2/family/not-found. The manipulation of the argument id leads to cross-site scripting. This vulnerability was named CVE-2023-25346. The attack can be initiated remotely. There is no ex-ploit available.	Protected by core rules	Detected by scanner as cross-site script-ing attack.
CVE-2023-0418	Video Central for Plugin up to 1.3.0 on WordPress Shortcode Attribute cross-site scripting	A vulnerability classified as problematic has been found in Video Central for Plugin up to 1.3.0 on WordPress. Affected is an unknown function of the component Short-code Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-0418. 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 script-ing attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0424	MS-Reviews Plugin up to 1.5 on Word-Press Review cross-site scripting	A vulnerability classified as problematic was found in MS-Reviews Plugin up to 1.5 on WordPress. Affected by this vul-nerability is an unknown functionality of the component Re-view Handler. The manipula-tion leads to cross-site scripting. This vulnerability is known as CVE-2023-0424. The attack can be launched re-motely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site script-ing attack.
CVE-2023-30210	OURPHP up to 7.2.0 our-php_tz.php cross-site scripting	A vulnerability was found in OURPHP up to 7.2.0. It has been rated as problematic. This issue affects some unknown pro-cessing of the file our-php_tz.php. The manipu-lation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-30210. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site script-ing attack.
CVE-2023-20060	Cisco Prime Collab-oration Deployment prior 14SU3 cross-site scripting (cisco-sa-pcd-xss-jDXpjm7)	A vulnerability was found in Cisco Prime Collabo-ration Deployment and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-20060. 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 script-ing attack.
CVE-2023-30212	OURPHP up to 7.2.0 ourphp_out.php cross-site scripting	A vulnerability classi-fied as problematic has been found in OURPHP up to 7.2.0. Affected is an unknown function of the file /client/manage/our-php_out.php. The manip-ulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-30212. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site script-ing attack.
CVE-2023-30338	Emlog Pro 2.0.3 Article Title/Article Summary cross-site scripting (Issue 229)	A vulnerability has been found in Emlog Pro 2.0.3 and classified as prob-lematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument Article Title/ Article Summary leads to cross-site scripting. This vulnerability is known as CVE-2023-30338. The attack can be launched re-motely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site script-ing attack.

XML External Entity Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-38840	Güralp MAN-EAM-0003 3.2.4 XML File Upload cgi-bin/ xmlstatus.cgi xml external entity refer-ence (ID 171439)	A vulnerability which was classified as problematic was found in Güralp MAN-EAM-0003 3.2.4. Affected is an unknown function of the file cgi-bin/xmlstatus. cgi of the component XML File Upload Handler. The manipulation leads to xml external entity reference. This vulnerability is traded as CVE-2022-38840. The attack needs to be initiated within the local network. There is no ex-ploit available.	Protected by core rules	Detected by scanner as XML external entity attack.

Indusface is a leading application security SaaS company that secures critical Web, Mobile & API applications of 5000+ global customers using its award-winning fully managed platform that integrates a web application scanner, web application firewall, DDoS &, BOT Mitigation, CDN, and threat intelligence engine. The company has been funded by Tata Capital Growth Fund, is Great Place to Work certified, mentioned by analysts like Gartner, Forrester, etc in their reports, and has been the recipient of many awards such as the Economic Times Top 25, NASSCOM DSCI Top Security Company, Deloitte Asia Top 100 , and several other such prestigious recognitions.

Indusface is the only cloud WAAP (WAF) vendor with 100% customer recommendation for 3 consecutive years

A Customers' Choice for 2022 and 2023 Gartner® Peer Insights™

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

EMAIL - sales@indusface.com