INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

August 2022

Total Zero-Day Vulnerabilities Found: 188

Command Injection	Injection Attack	Remote Code Execution	Cross-Site Request Forgery	Local File Inclusion	SQL Injection	Cross-Site Scripting	XML External Entity
9	2	2	23	13	48	90	1

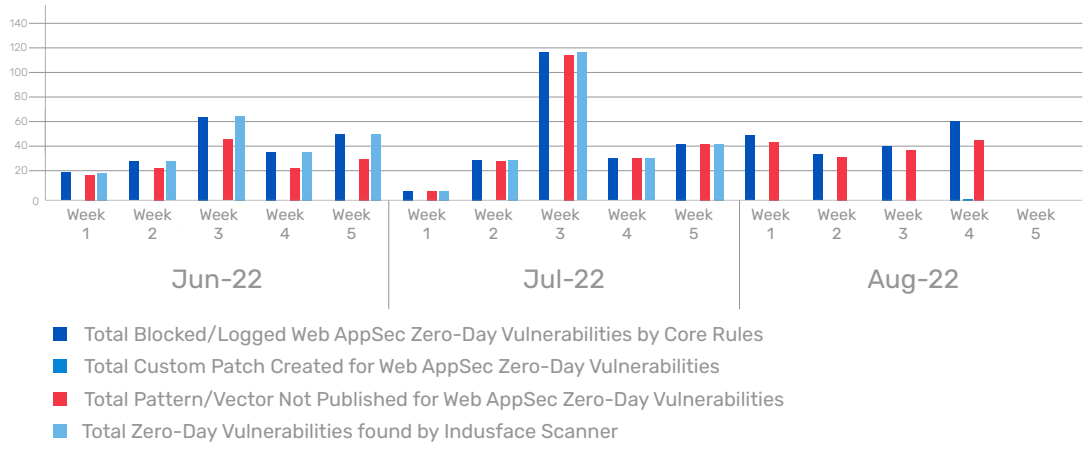
Zero-day vulnerabilities protected through core rules	186
Zero-day vulnerabilities protected through custom rules	2
Zero-day vulnerabilities for which protection can not be done	0
Zero-day vulnerabilities found by Indusface WAS	163

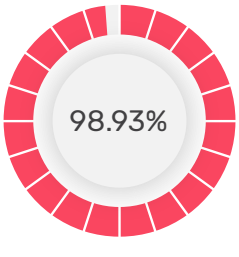
- To enable custom rules, please contact support@indusface.com
- Since the attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.

Vulnerability Trend:

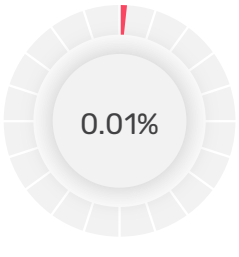
The weekly trend displays the total number of vulnerabilities discovered to the type of protection provided for the last quarter.

Weekly Vulnerability Trend

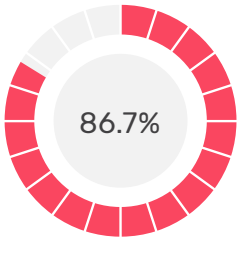




of the zero-day vulnerabilities were protected by the **core rules** in the last month.

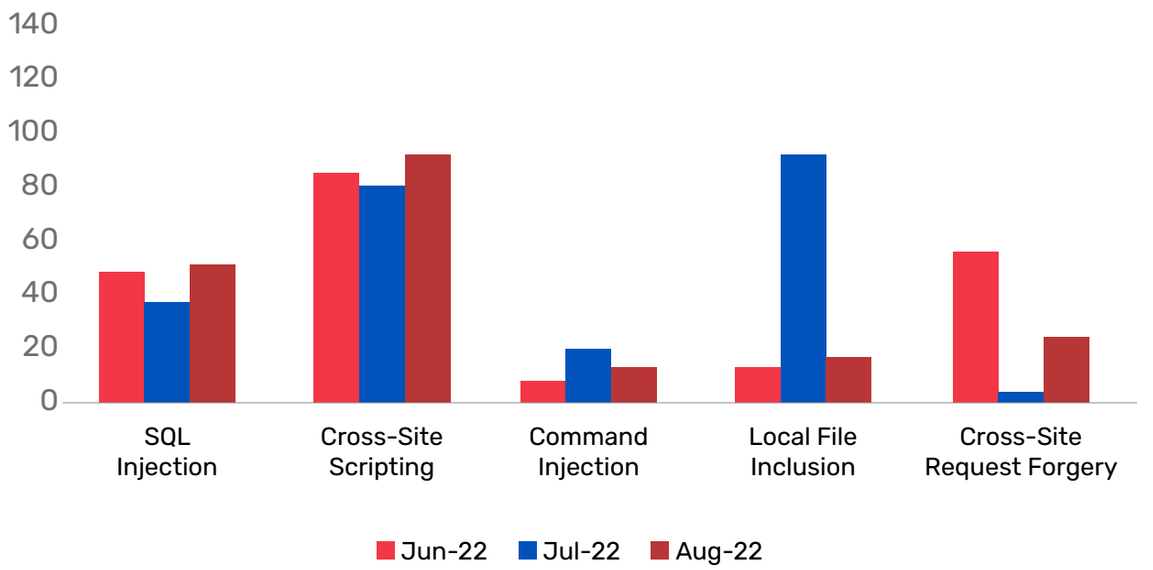


of the zero-day vulnerabilities were protected by the **custom rules** in the last month.



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-2020-7795	get-npm-package-version up to 1.0.6 index.js main command injection	A vulnerability classified as critical was found in get-npmpackage-version up to 1.0.6. Affected by this vulnerability is the function main of the file index.js. The manipulation leads to command injection. This vulnerability is known as CVE-2020-7795. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command injection attack
CVE-2022-21186	acrontum filesystem-template up to 0.0.1 fetchRepo API href command injection	A vulnerability which was classified as critical has been found in acrontum filesystem-template up to 0.0.1. This issue affects some unknown processing of the component fetchRepo API. The manipulation of the argument href leads to command injection. The identification of this vulnerability is CVE-2022-21186. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command injection attack
CVE-2022-36267	Airspan AirSpot 5410 up to 0.3.4.1-4 Ping diagnostics.cgi command injection	A vulnerability classified as critical has been found in Airspan AirSpot 5410 up to 0.3.4.1-4. Affected is an unknown function of the file /home/www/cgi-bin/diagnostics.cgi of the component Ping Handler. The manipulation leads to command injection. This vulnerability is traded as CVE-2022-36267. It is possible to launch the attack remotely. 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-2022-2354	WP-DBManager Plugin up to 2.80.7 on WordPress code injection	A vulnerability classified as critical was found in WPDBManager Plugin up to 2.80.7. Affected by this vulnerability is an unknown functionality. The manipulation leads to code injection. This vulnerability is known as CVE-2022-2354. 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 the scanner as command injection attack
CVE-2022-2314	VR Calendar Plugin up to 2.2.2 on WordPress os command injection	A vulnerability was found in VR Calendar Plugin up to 2.2.2. It has been classified as critical. This affects an unknown part. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2022-2314. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-35948	undici up to 5.8.0 on Node.js Content-Type Header crlf injection (GHSA-f772-66g8-q5h3)	A vulnerability which was classified as critical has been found in undici up to 5.8.0. Affected by this issue is some unknown functionality of the component Content-Type Header Handler. The manipulation leads to crlf injection. This vulnerability is handled as CVE-2022-35948. The attack may be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-36309	Airspan AirVelocity 1500 up to 15.18.00.2510 Web Management UI recoverySubmit.cgi ActiveBank command injection (GHSA-p295-2jh6-g6g4)	A vulnerability was found in Airspan AirVelocity 1500 up to 15.18.00.2510. It has been classified as critical. This affects an unknown part of the file recoverySubmit.cgi of the component Web Management UI. The manipulation of the argument ActiveBank leads to command injection. This vulnerability is uniquely identified as CVE-2022-36309. 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 the scanner as command injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-37061	FLIR AX8 up to 1.46.16 POST Parameter res. php id os command injection	A vulnerability was found in FLIR AX8 up to 1.46.16. It has been classified as very critical. This affects an unknown part of the file res.php of the component POST Parameter Handler. The manipulation of the argument id leads to os command injection. This vulnerability is uniquely identified as CVE-2022-37061. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-36633	Teleport 9.3.6 URL command injection (ID 168137)	A vulnerability classified as critical was found in Teleport 9.3.6. Affected by this vulnerability is an unknown functionality of the component URL Handler. The manipulation leads to command injection. This vulnerability is known as CVE-2022-36633. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack

Injection Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-37240	MDaemon SecurityGateway for Email Servers 8.5.2 format response splitting	A vulnerability classified as critical was found in MDaemon SecurityGateway for Email Servers 8.5.2. Affected by this vulnerability is an unknown functionality. The manipulation of the argument format leads to http response splitting. This vulnerability is known as CVE-2022-37240. 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-2022-37242	MDaemon SecurityGateway for Email Servers 8.5.2 data response splitting	A vulnerability which was classified as critical has been found in MDaemon SecurityGateway for Email Servers 8.5.2. Affected by this issue is some unknown functionality. The manipulation of the argument data leads to http response splitting. This vulnerability is handled as CVE-2022-37242. 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	NA

Remote Code Execution Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-25812	Transposh Translation Plugin up to 1.0.7 on WordPress Debug Setting code injection	A vulnerability classified as critical has been found in Transposh Translation Plugin up to 1.0.7. Affected is an unknown function of the component Debug Setting Handler. The manipulation leads to code injection. This vulnerability is traded as CVE-2022-25812. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2018-14520	Kirby 2.5.12 HTTP Request Remote Code Execution (EDB-45068)	A vulnerability was found in Kirby 2.5.12 and classified as critical. Affected by this issue is some unknown functionality of the component HTTP Request Handler. The manipulation leads to Remote Code Execution. This vulnerability is handled as CVE-2018-14520. The attack may be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	NA

Cross-site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2184	CAPTCHA 4WP Plugin up to 7.0.x on WordPress Admin Template require_once crosssite request forgery	A vulnerability which was classified as problematic was found in CAPTCHA 4WP Plugin up to 7.0.x. This affects the function require_once of the component Admin Template Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-2184. 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-2022-2171	Progressive License Plugin up to 1.1.0 on WordPress cross-site request forgery	A vulnerability has been found in Progressive License Plugin up to 1.1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-2171. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2241	Featured Image from URL Plugin up to 4.0.0 on WordPress cross-site request forgery	A vulnerability was found in Featured Image from URL Plugin up to 4.0.0 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-2022-2241. 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-2022-2260	GiveWP Plugin up to 2.21.2 on WordPress exporting cross-site request forgery	A vulnerability was found in GiveWP Plugin up to 2.21.2. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument exporting leads to cross-site request forgery. This vulnerability is handled as CVE-2022-2260. 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-2022-2245	Counter Box Plugin up to 1.2.0 on WordPress crosssite request forgery	A vulnerability was found in Counter Box Plugin up to 1.2.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-2245. 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-2022-2355	Easy Username Updater Plugin up to 1.0.4 on WordPress cross-site request forgery	A vulnerability which was classified as problematic has been found in Easy Username Updater Plugin up to 1.0.4. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-2355. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-35943	CodeIgniter Shield up to 1.0.0-beta.1 cross-site request forgery (GHSA-5hm8-vh6r-2cjq)	A vulnerability was found in CodeIgniter Shield up to 1.0.0-beta.1. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-35943. 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-2022-38359	Eyes of Network index.php cross-site request forgery	A vulnerability which was classified as problematic has been found in Eyes of Network. This issue affects some unknown processing of the file /module/admin_user/index. phpDataTables_Table_0_length10&user_selected%5B%5D1&user_mgt_listdelete_user&actionsubmit. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022-38359. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-36225	EyouCMS 1.5.8-UTF8-SP1 Column Management crosssite request forgery (ID 26)	A vulnerability was found in EyouCMS 1.5.8-UTF8-SP1 and classified as problematic. This issue affects some unknown processing of the component Column Management. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022-36225. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-36224	XunRuiCMS 4.5.6 cross-site request forgery	A vulnerability has been found in XunRuiCMS 4.5.6 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-36224. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-36577	JIZHICMS 2.3.1 cross-site request forgery (ID 77)	A vulnerability classified as problematic was found in JIZHICMS 2.3.1. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-36577. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2312	Student Result or Employee Database Plugin up to 1.7.4 on WordPress AJAX Action cross-site request forgery	A vulnerability has been found in Student Result or Employee Database Plugin up to 1.7.4 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-2312. 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-2022-2555	Yotpo Reviews for WooCommerce Plugin up to 2.0.4 on WordPress Setting cross-site request forgery	A vulnerability was found in Yotpo Reviews for WooCommerce Plugin up to 2.0.4. It has been classified as problematic. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-2555. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-2382	Product Slider for WooCommerce Plugin up to 2.5.6 on WordPress AJAX Action cross-site request forgery	A vulnerability has been found in Product Slider for WooCommerce Plugin up to 2.5.6 and classified as problematic. This vulnerability affects unknown code of the component AJAX Action Handler. The manipulation leads to crosssite request forgery. This vulnerability was named CVE-2022-2382. 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-2022-1251	Ask Me Theme up to 6.8.3 on WordPress Edit Profile Page cross-site request forgery	A vulnerability which was classified as problematic has been found in Ask Me Theme up to 6.8.3. Affected by this issue is some unknown functionality of the component Edit Profile Page. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-1251. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2275	WP Edit Menu Plugin up to 1.4.x on WordPress AJAX Action cross-site request forgery	A vulnerability classified as problematic was found in WP Edit Menu Plugin up to 1.4.x. Affected by this vulnerability is an unknown functionality of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-2275. 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-2022-2377	Directorist Plugin up to 7.2.x on WordPress AJAX Action cross-site request forgery	A vulnerability has been found in Directorist Plugin up to 7.2.x and classified as problematic. This vulnerability affects unknown code of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-2377. 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-2022-2172	LinkWorth Plugin up to 3.3.3 on WordPress cross-site request forgery	A vulnerability classified as problematic has been found in LinkWorth Plugin up to 3.3.3. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-2172. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-2276	WP Edit Menu Plugin up to 1.4.x on WordPress AJAX Action cross-site request forgery	A vulnerability which was classified as problematic has been found in WP Edit Menu Plugin up to 1.4.x. Affected by this issue is some unknown functionality of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-2276. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2389	Autonami Abandoned Cart Recovery for WooCommerce, Follow Up Emails, Newsletter Builder & Marketing Automation Plugin AJAX Action cross-site request forgery	A vulnerability was found in Autonami Abandoned Cart Recovery for WooCommerce Follow Up Emails Newsletter Builder & Marketing Automation Plugin up to 2.1.1 and classified as problematic. This issue affects some unknown processing of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022-2389. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2018-14519	Kirby 2.5.12 Delete Page cross-site request forgery (ID 45090 / EDB-45090)	A vulnerability classified as problematic has been found in Kirby 2.5.12. Affected is an unknown function of the component Delete Page Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2018-14519. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2021-39394	mm-wiki 0.2.1 cross-site request forgery (ID 316)	A vulnerability was found in mm-wiki 0.2.1. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2021-39394. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-36546	edoc-doctor-appointmentsystem 1.0.1 /patient/settings.php cross-site request forgery	A vulnerability which was classified as problematic was found in edoc-doctor-appointment-system 1.0.1. This affects an unknown part of the file /patient/settings.php. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-36546. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA

XML External Entity Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-29805	Fishbowl Inventory prior 2022.4.1 XML deserialization	A vulnerability was found in Fishbowl Inventory. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component XML Handler. The manipulation leads to deserialization. This vulnerability is known as CVE-2022-29805. 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 XML External Entity Attack

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-35920	Sanic server /framework path traversal (GHSA-8cw9-5hmv-77w6)	A vulnerability was found in Sanic. It has been rated as critical. This issue affects some unknown processing of the file server/framework. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-35920. 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-2022-2653	Planka Environment Variable /proc/self / environ path traversal	A vulnerability was found in Planka. It has been rated as critical. Affected by this issue is some unknown functionality of the file / proc /self/environ of the component Environment Variable Handler. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-2653. The attack may be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Local file inclusion attack
CVE-2022-36264	Airspan AirSpot 5410 up to 0.3.4.1-4 File Upload path traversal	A vulnerability has been found in Airspan AirSpot 5410 up to 0.3.4.1-4 and classified as problematic. This vulnerability affects unknown code of the component File Upload Handler. The manipulation leads to relative path traversal. This vulnerability was named CVE-2022-36264. 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-2022-38129	Keysight Sensor Management Server path traversal	A vulnerability classified as critical has been found in Keysight Sensor Management Server. This affects the function com.keysight.tentacle.licensing.LicenseManager.addLicenseFile. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-38129. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local file inclusion attack
CVE-2022-37423	Neo4j APOC up to 4.3.0.6/4.4.0.7 apoc.log.stream pathname traversal (GHSA-78f9-745f-278p)	A vulnerability has been found in Neo4j APOC up to 4.3.0.6/4.4.0.7 and classified as critical. Affected by this vulnerability is the function apoc.log.stream. The manipulation leads to pathname traversal. This vulnerability is known as CVE-2022-37423. 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-2022-36007	Venice up to 1.10.17 path traversal (GHSA-4mmh-5vw7-rgvj)	A vulnerability was found in Venice up to 1.10.17. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-36007. 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 Local file inclusion attack
CVE-2022-35204	Vitejs Vite up to 2.9.12 URL pathname traversal (ID 8498)	A vulnerability classified as critical has been found in Vitejs Vite up to 2.9.12. Affected is an unknown function of the component URL Handler. The manipulation leads to pathname traversal. This vulnerability is traded as CVE-2022-35204. The attack needs to be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local file inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2557	Team Plugin up to 4.1.1 on WordPress path traversal	A vulnerability was found in Team Plugin up to 4.1.1. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-2557. The attack can only be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local file inclusion attack
CVE-2022-2558	Simple Job Board Plugin up to 2.9.x on WordPress exposure of information through directory listing	A vulnerability classified as problematic has been found in Simple Job Board Plugin up to 2.9.x. This affects an unknown part. The manipulation leads to exposure of information through directory listing. This vulnerability is uniquely identified as CVE-2022-2558. 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-2019-25075	Gravitee API Management up to 1.25.2 register path traversal	A vulnerability classified as critical has been found in Gravitee API Management up to 1.25.2. This affects an unknown part of the file /management/users/register. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2019-25075. The attack can only be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local file inclusion attack
CVE-2022-36261	taocms 3.0.2 admin.php path path traversal	A vulnerability was found in taocms 3.0.2. It has been classified as problematic. This affects an unknown part of the file admin.phpaction-file&ctrldel. The manipulation of the argument path leads to relative path traversal. This vulnerability is uniquely identified as CVE-2022-36261. 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-36168	Wuzhicms 4.1.0 index.php pathname traversal	A vulnerability classified as critical has been found in Wuzhicms 4.1.0. Affected is an unknown function of the file /coreframe/app/attachment/admin/index.php. The manipulation leads to pathname traversal. This vulnerability is traded as CVE-2022-36168. 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-2022-38794	Zaver up to 2020-12-15 pathname traversal (ID 22)	A vulnerability was found in Zaver up to 2020-12-15. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to pathname traversal. The identification of this vulnerability is CVE-2022-38794. 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

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1950	Youzify Plugin up to 1.1. x on WordPress sql injection	A vulnerability which was classified as critical was found in Youzify Plugin up to 1.1.x. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-1950. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-34955	Pligg CMS 2.0.2 load_data_for_topusers.php page_size sql injection (ID 261)	A vulnerability was found in Pligg CMS 2.0.2 and classified as critical. This issue affects some unknown processing of the file load_data_for_topusers.php. The manipulation of the argument page_size leads to sql injection. The identification of this vulnerability is CVE-2022-34955. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-34949	Pharmacy Management System 1.0 login.php email /password sql injection	A vulnerability was found in Pharmacy Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file login.php. The manipulation of the argument email /password leads to sql injection. This vulnerability was named CVE-2022-34949. The attack can 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-2022-35422	Web Based Quiz System 1.0 update.php qid sql injection	A vulnerability has been found in Web Based Quiz System 1.0 and classified as critical. This vulnerability affects unknown code of the file update.php. The manipulation of the argument qid leads to sql injection. This vulnerability was named CVE-2022-35422. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-35421	Online Tours And Travels Management System 1.0 packages.php pname sql injection	A vulnerability which was classified as critical has been found in Online Tours And Travels Management System 1.0. This issue affects some unknown processing of the file / admin/operations /packages.php. The manipulation of the argument pname leads to sql injection. The identification of this vulnerability is CVE-2022-35421. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-34928	JFinal CMS 5.1.0 /system/user sql injection (ID 43)	A vulnerability classified as critical has been found in JFinal CMS 5.1.0. This affects an unknown part of the file /system/user. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-34928. 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-2022-2644	SourceCodester Online Admission System GET Parameter eid sql injection	A vulnerability was found in SourceCodester Online Admission System and classified as critical. This issue affects some unknown processing of the component GET Parameter Handler. The manipulation of the argument eid leads to sql injection. The identification of this vulnerability is CVE-2022-2644. The attack needs to be done within the local network. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-2648	SourceCodester Multi Language Hotel Management Software room_id sql injection	A vulnerability was found in SourceCodester Multi Language Hotel Management Software. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument room_id leads to sql injection. The identification of this vulnerability is CVE-2022-2648. 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-2022-31197	PostgreSQL JDBC Driver up to 42.2.25/42.4.0 java.sql.ResultRow.refreshRow sql injection (GHSA-r38f-c4h4-hqq2)	A vulnerability was found in PostgreSQL JDBC Driver up to 42.2.25 /42.4.0. It has been declared as critical. Affected by this vulnerability is the function java.sql.ResultRow.refreshRow. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-31197. 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-2022-2676	SourceCodester Electronic Medical Records System POST Request user_email sql injection	A vulnerability was found in SourceCodester Electronic Medical Records System and classified as critical. Affected by this issue is some unknown functionality of the component POST Request Handler. The manipulation of the argument user_email leads to sql injection. This vulnerability is handled as CVE-2022-2676. The attack may be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-2679	SourceCodester Interview Management System 1.0 / viewReport. php id sql injection	A vulnerability was found in SourceCodester Interview Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /viewReport.php. The manipulation of the argument id with the input))0x7162766a71)7319)) leads to sql injection. The identification of this vulnerability is CVE-2022-2679. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-2677	SourceCodester Apartment Visitor Management System 1.0 index.php username sql injection	A vulnerability was found in SourceCodester Apartment Visitor Management System 1.0. It has been classified as critical. This affects an unknown part of the file index.php. The manipulation of the argument username with the input &039; AND))RSzF) AND &039; htiy&039;&039;htiy leads to sql injection. This vulnerability is uniquely identified as CVE-2022-2677. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2667	SourceCodester Loan Management System delete_lplan.php lplan_id sql injection	A vulnerability was found in SourceCodester Loan Management System and classified as critical. This issue affects some unknown processing of the file delete_lplan.php. The manipulation of the argument lplan_id leads to sql injection. The identification of this vulnerability is CVE-2022-2667. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-2680	SourceCodeste Church Management System 1.0 /login.php username sql injection	A vulnerability classified as critical has been found in SourceCodester Church Management System 1.0. Affected is an unknown function of the file /login.php. The manipulation of the argument username with the input &039; OR CONCAT))0x716b707871FLOOR2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- jURL leads to sql injection. This vulnerability is traded as CVE-2022-2680. 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-2022-2693	SourceCodester Electronic Medical Records System UPDATE Statement register.php pconsultation sql injection	A vulnerability has been found in SourceCodester Electronic Medical Records System and classified as critical. This vulnerability affects unknown code of the file register.php of the component UPDATE Statement Handler. The manipulation of the argument pconsultation leads to sql injection. This vulnerability was named CVE-2022-2693. The attack can be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-2687	SourceCodester Gym Management System user_pass sql injection	A vulnerability which was classified as critical was found in SourceCodester Gym Management System. Affected is an unknown function. The manipulation of the argument user_pass leads to sql injection. This vulnerability is traded as CVE-2022-2687. 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-2022-2697	SourceCodester Simple E-Learning System comment_frame.php post_id sql injection	A vulnerability was found in SourceCodester Simple E-Learning System. It has been classified as critical. Affected is an unknown function of the file comment_frame.php. The manipulation of the argument post_id leads to sql injection. This vulnerability is traded as CVE-2022-2697. It is possible to launch the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2705	SourceCodester Simple Student Information System manage_department.php id sql injection	A vulnerability was found in SourceCodester Simple Student Information System. It has been rated as critical. This issue affects some unknown processing of the file admin/departments /manage_department.php. The manipulation of the argument id with the input -5756%27%20UNION%20ALL%20SELECT%20NULLdatabaseuserNULLNULLNULL-NULL--%20- leads to sql injection. The identification of this vulnerability is CVE-2022-2705. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-2707	SourceCodester Online Class and Exam 1.0 /pages/faculty_sched.php faculty sql injection	A vulnerability classified as critical was found in SourceCodester Online Class and Exam Scheduling System 1.0. Affected by this vulnerability is an unknown functionality of the file /pages /faculty_sched.php. The manipulation of the argument faculty with the input &039; OR CONCAT))0x717a706a-71FLOOR2)) x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- uYCM leads to sql injection. This vulnerability is known as CVE-2022-2707. The attack can be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-2715	SourceCodester Employee Management System eloginwel.php id sql injection	A vulnerability has been found in SourceCodester Employee Management System and classified as critical. This vulnerability affects unknown code of the file eloginwel.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-2715. 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-2022-2269	Website File Changes Monitor Plugin up to 1.8.2 on WordPress sql injection	A vulnerability was found in Website File Changes Monitor Plugin up to 1.8.2. It has been classified as critical. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-2269. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-2460	WPDating Plugin up to 7.1.9 on WordPress sql injection	A vulnerability classified as critical was found in WPDating Plugin up to 7.1.9. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-2460. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-2766	SourceCodester Loan Management System /index.php password sql injection	A vulnerability was found in SourceCodester Loan Management System. It has been rated as critical. Affected by this issue is some unknown functionality of the file /index.php. The manipulation of the argument password leads to sql injection. This vulnerability is handled as CVE-2022-2766. The attack may be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-2803	SourceCodester Zoo Management System /pages/animals.php class_id sql injection	A vulnerability was found in SourceCodester Zoo Management System and classified as critical. This issue affects some unknown processing of the file /pages/animals.php. The manipulation of the argument class_id leads to sql injection. The identification of this vulnerability is CVE-2022-2803. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-2812	SourceCodester Guest Management System index.php username /pass sql injection	A vulnerability classified as critical was found in SourceCodester Guest Management System. This vulnerability affects unknown code of the file index.php. The manipulation of the argument username /pass leads to sql injection. This vulnerability was named CVE-2022-2812. 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-2022-2876	SourceCodester Student Management System index.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Student Management System. Affected is an unknown function of the file index.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-2876. 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-2022-36578	jizhicms 2.3.1 sql injection (ID 78)	A vulnerability which was classified as critical was found in jizhicms 2.3.1. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-36578. 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-2022-36605	Yimioa 6.1 orderby sql injection (ID 24)	A vulnerability which was classified as critical was found in Yimioa 6.1. Affected is an unknown function. The manipulation of the argument orderby leads to sql injection. This vulnerability is traded as CVE-2022-36605. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-25228	CandidATS 3.0.0 Beta /index.php userID/candidateID/jobOrderID/companyID sql injection	A vulnerability was found in CandidATS 3.0.0 Beta and classified as critical. This issue affects some unknown processing of the file /index.php. The manipulation of the argument userID/candidateID/jobOrderID/companyID leads to sql injection. The identification of this vulnerability is CVE-2022-25228. 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-2022-36606	Ywoa up to 6.0 checkPool sql injection (ID 25)	A vulnerability has been found in Ywoa up to 6.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /oa/setup/checkPooldatabase. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-36606. 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-36727	SourceCodester Library Management System 1.0 /staff/delete.php bookId sql injection	A vulnerability which was classified as critical has been found in SourceCodester Library Management System 1.0. Affected by this issue is some unknown functionality of the file /staff/delete.php. The manipulation of the argument bookId leads to sql injection. This vulnerability is handled as CVE-2022-36727. The attack may be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-36198	PHPGurukul Bus Pass Management System 1.0 view-enquiry.php sql injection	A vulnerability has been found in PHPGurukul Bus Pass Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file buspassms/admin/view-enquiry.php. The manipulation leads to sql injection. This vulnerability was named CVE-2022-36198. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-25811	Transposh Translation Plugin up to 1.0.8 on WordPress order / orderby sql injection	A vulnerability classified as critical was found in Transposh Translation Plugin up to 1.0.8. This vulnerability affects unknown code. The manipulation of the argument order/orderby leads to sql injection. This vulnerability was named CVE-2022-25811. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-2593	Better Search Replace Plugin up to 1.4.0 on WordPress sql injection	A vulnerability which was classified as critical has been found in Better Search Replace Plugin up to 1.4.0. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-2593. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-37111	BlueCMS 1.6 admin / article.php sql injection	A vulnerability classified as critical was found in BlueCMS 1.6. This vulnerability affects unknown code of the file admin/article.php. The manipulation leads to sql injection. This vulnerability was named CVE-2022-37111. The attack can 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-2022-37178	72crm 9.0 Task Calendar sql injection (ID 34)	A vulnerability has been found in 72crm 9.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the component Task Calendar. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-37178. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-36719	SourceCodester Library Management System 1.0 /admin/history.php system ok sql injection	A vulnerability was found in SourceCodester Library Management System 1.0. It has been classified as critical. This affects the function system of the file /admin/history.php. The manipulation of the argument ok leads to sql injection. This vulnerability is uniquely identified as CVE-2022-36719. 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-2022-36692	Ingredients Stock Management System 1.0 Master.php id sql injection	A vulnerability was found in Ingredients Stock Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /classes/Master.phpfdelete_category. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-36692. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2021-43329	Mumara Classic up to 2.93 license_update. php license sql injection (ID 164947 / EDB- 50518)	A vulnerability was found in Mumara Classic up to 2.93. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file license_update.php. The manipulation of the argument license leads to sql injection. This vulnerability is known as CVE-2021-43329. The attack can be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-36681	oretnom23 Simple Task Scheduling System 1.0 Master.php id sql injection	A vulnerability was found in oretnom23 Simple Task Scheduling System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /classes/Master.phpfdelete_account. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-36681. 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-2022-37152	SourceCodester Online Diagnostic Lab Management System 1.0 Users.php dob sql injection	A vulnerability which was classified as critical has been found in Source-Codester Online Diagnostic Lab Management System 1.0. This issue affects some unknown processing of the file /classes /Users. phpfsave_client. The ma-nipulation of the argument dob leads to sql injection. The identification of this vulnerability is CVE-2022-37152. 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-2022-36679	oretnom23 Simple Task Scheduling System 1.0 id sql injection	A vulnerability which was classified as critical was found in oretnom23 Simple Task Scheduling System 1.0. Affected is an un-known function of the file / admin/pageuser/manage_ user. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-36679. 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-2022-36703	Ingredients Stock Management System 1.0 manage_stockin. php id sql injection	A vulnerability was found in Ingredients Stock Management System 1.0. It has been classified as critical. Affected is an un-known function of the file /stocks/manage_stockin. php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-36703. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-36721	SourceCodester Library Management System 1.0 /admin / modify.php Textbook sql injection	A vulnerability was found in SourceCodester Library Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/modify.php. The manipulation of the argument Textbook leads to sql injection. The identification of this vulnerability is CVE-2022-36721. 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-2022-36529	Kensite CMS 1.0 DB-Mapper.xml name / oldname sql injection	A vulnerability which was classified as critical has been found in Kensite CMS 1.0. This issue affects some unknown processing of the file /framework/mod/db/DBMapper.xml. The manipulation of the argument name/oldname leads to sql injection. The identification of this vulnerability is CVE-2022-36529. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-36544	edoc-doctorappointment-system 1.0.1 / patient/booking.php id sql injection	A vulnerability was found in edoc-doctor-appointment-system 1.0.1. It has been rated as critical. This issue affects some unknown processing of the file /patient/booking.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-36544. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-3012	oretnom23 Fast Food Ordering System index. php date sql injection	A vulnerability was found in oretnom23 Fast Food Ordering System. It has been rated as critical. Affected by this issue is some unknown functionality of the file ffos/admin/reports/index.php. The manipulation of the argument date leads to sql injection. This vulnerability is handled as CVE-2022-3012. The attack may be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-3013	SourceCodester Simple Task Managing System /loginVaLidation.php login sql injection	A vulnerability classified as critical has been found in SourceCodester Simple Task Managing System. This affects an unknown part of the file /loginVaLidation.php. The manipulation of the argument login leads to sql injection. This vulnerability is uniquely identified as CVE-2022-3013. 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

Cross-Site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2305	Popup Plugin up to 1.9.3.8 on WordPress Setting crosssite scripting	A vulnerability classified as problematic was found in Popup Plugin up to 1.9.3.8. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2305. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site Scripting attack
CVE-2022-2170	Microsoft Advertising Universal Event Tracking Plugin Setting cross-site scripting	A vulnerability which was classified as problematic has been found in Microsoft Advertising Universal Event Tracking Plugin up to 1.0.3. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to crosssite scripting. The identification of this vulnerability is CVE-2022-2170. 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-2022-0598	Login with Phone Number Plugin up to 1.3.7 on WordPress Setting cross-site scripting	A vulnerability was found in Login with Phone Number Plugin up to 1.3.7. It has been rated as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-0598. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site Scripting attack
CVE-2022-2325	Invitation Based Registrations Plugin up to 2.2.84 on WordPress Setting cross-site scripting	A vulnerability which was classified as problematic has been found in Invitation Based Registrations Plugin up to 2.2.84. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-2325. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site Scripting attack
CVE-2022-2215	GiveWP Plugin up to 2.21.2 on WordPress Currency Setting cross-site scripting	A vulnerability has been found in GiveWP Plugin up to 2.21.2 and classified as problematic. This vulnerability affects unknown code of the component Currency Setting Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2215. 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-2022-2328	Flexi Quote Rotator Plugin up to 0.9.4 on WordPress Setting cross-site scripting	A vulnerability which was classified as problematic was found in Flexi Quote Rotator Plugin up to 0.9.4. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-2328. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site Scripting attack
CVE-2022-2278	Featured Image from URL Plugin up to 4.0.0 on WordPress cross-site scripting	A vulnerability classified as problematic has been found in Featured Image from URL Plugin up to 4.0.0. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2278. 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-2022-1324	Event Timeline Plugin up to 1.1.5 on WordPress Timeline Text cross-site scripting	A vulnerability classified as problematic has been found in Event Timeline Plugin up to 1.1.5. Affected is an unknown function of the component Timeline Text Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-1324. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site Scripting attack
CVE-2022-1906	Copyright Proof Plugin up to 4.16 on WordPress AJAX Action cross-site scripting	A vulnerability classified as problematic was found in Copyright Proof Plugin up to 4.16. Affected by this vulnerability is an unknown functionality of the component AJAX Action Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-1906. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site Scripting attack
CVE-2022-2181	Advanced Reset Plugin up to 1.5 on WordPress Admin Dashboard href cross-site scripting	A vulnerability which was classified as problematic has been found in Advanced Reset Plugin up to 1.5. Affected by this issue is some unknown functionality of the component Admin Dashboard. The manipulation of the argument href leads to cross-site scripting. This vulnerability is handled as CVE-2022-2181. 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-2022-2589	beancount fava up to 1.22.2 cross-site scripting	A vulnerability was found in beancount fava up to 1.22.2 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-2589. 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-2022-34618	Mealie 1.0.0beta3 recipe description cross-site scripting	A vulnerability which was classified as problematic was found in Mealie 1.0.0beta3. This affects an unknown part. The manipulation of the argument recipe description leads to crosssite scripting. This vulnerability is uniquely identified as CVE-2022-34618. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2683	SourceCodester Simple Food Ordering System 1.0 /login.php email/password cross-site scripting	A vulnerability which was classified as problematic was found in SourceCodester Simple Food Ordering System 1.0. This affects an unknown part of the file /login.php. The manipulation of the argument email/password with the input "><ScRiPt>alert</sCrIpT> leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2683. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2681	SourceCodester Online Student Admission System Student User Page editprofile.php cross-site scripting	A vulnerability classified as problematic was found in SourceCodester Online Student Admission System. Affected by this vulnerability is an unknown functionality of the file editprofile. php of the component Student User Page. The manipulation with the input <script>alert</script> leads to cross-site scripting. This vulnerability is known as CVE-2022-2681. The attack can be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2685	SourceCodester Interview Management System 1.0 / addQuestion.php question cross-site scripting	A vulnerability was found in SourceCodester Interview Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file /addQuestion.php. The manipulation of the argument question with the input <script>alert</script> leads to cross-site scripting. The identification of this vulnerability is CVE-2022-2685. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2684	SourceCodester Apartment Visitor Management System 1.0 /manage-apartment.php Apartment Number crosssite scripting	A vulnerability has been found in SourceCodester Apartment Visitor Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /manage apartment.php. The manipulation of the argument Apartment Number with the input <script>alert</script> leads to cross-site scripting. This vulnerability was named CVE-2022-2684. 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-2022-2682	SourceCodester Alphaware Simple E-Commerce System stockin.php id cross-site scripting	A vulnerability which was classified as problematic has been found in SourceCodester Alphaware Simple E-Commerce System. Affected by this issue is some unknown functionality of the file stockin.php. The manipulation of the argument id with the input &039;"><script>alert</script> leads to cross-site scripting. This vulnerability is handled as CVE-2022-2682. The attack may be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-35144	Renato 0.17.0 cross-site scripting	A vulnerability which was classified as problematic has been found in Renato 0.17.0. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-35144. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2686	oretnom23 Fast Food Ordering System Menu List Page Description cross-site scripting	A vulnerability which was classified as problematic was found in oretnom23 Fast Food Ordering System. This affects an unknown part of the component Menu List Page. The manipulation of the argument Description leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2686. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2689	SourceCodester Wedding Hall Booking System Contact Page /whbs/ Message crosssite scripting	A vulnerability classified as problematic has been found in SourceCodester Wedding Hall Booking System. Affected is an unknown function of the file /whbs/pagecontact_us of the component Contact Page. The manipulation of the argument Message leads to cross-site scripting. This vulnerability is traded as CVE-2022-2689. It is possible to launch the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-35163	Complete Online Job Search System 1.0 controller.php U_NAME cross-site scripting	A vulnerability was found in Complete Online Job Search System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /category/controller.phpactionedit. The manipulation of the argument U_NAME leads to cross-site scripting. This vulnerability is handled as CVE-2022-35163. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site Scripting attack
CVE-2022-2701	SourceCodester Simple ELearning System /claire_blake Bio cross-site scripting	A vulnerability classified as problematic was found in SourceCodester Simple E-Learning System. This vulnerability affects unknown code of the file /claire_blake. The manipulation of the argument Bio leads to cross-site scripting. This vulnerability was named CVE-2022-2701. The attack can be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2372	YaySMTP Plugin up to 2.2.1 on WordPress Setting crosssite scripting	A vulnerability has been found in YaySMTP Plugin up to 2.2.1 and classified as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2372. 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 the scanner as cross-site scripting attack
CVE-2022-2425	WP DS Blog Map Plugin up to 3.1.3 on WordPress Setting cross-site scripting	A vulnerability was found in WP DS Blog Map Plugin up to 3.1.3. It has been classified as problematic. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2425. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2395	weForms Plugin up to 1.6.13 on WordPress Setting cross-site scripting	A vulnerability was found in weForms Plugin up to 1.6.13. It has been classified as problematic. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-2395. 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 the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2426	Thinkific Uploader Plugin up to 1.0.0 on WordPress Setting cross-site scripting	A vulnerability was found in Thinkific Uploader Plugin up to 1.0.0. 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-2022-2426. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site Scripting attack
CVE-2022-2409	Rough Chart Plugin up to 1.0.0 on WordPress Data Label cross-site scripting	A vulnerability classified as problematic was found in Rough Chart Plugin up to 1.0.0. This vulnerability affects unknown code of the component Data Label Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2409. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2410	mTouch Quiz Plugin up to 3.1.3 on WordPress Setting cross-site scripting	A vulnerability which was classified as problematic has been found in mTouch Quiz Plugin up to 3.1.3. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-2410. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2391	Inspiro PRO Plugin on WordPress description crosssite scripting	A vulnerability classified as problematic has been found in Inspiro PRO Plugin. Affected is an unknown function. The manipulation of the argument description leads to cross-site scripting. This vulnerability is traded as CVE-2022-2391. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2424	Google Maps Anywhere Plugin up to 1.2.6.3 on WordPress cross-site scripting	A vulnerability has been found in Google Maps Anywhere Plugin up to 1.2.6.3 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-2022-2424. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-35493	eShop Multipurpose Ecommerce Store Website 3.0.4 search cross-site scripting	A vulnerability which was classified as problematic was found in eShop Multipurpose Ecommerce Store Website 3.0.4. This affects an unknown part. The manipulation of the argument search leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-35493. 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-2022-2423	DW Promobar Plugin up to 1.0.4 on WordPress Setting cross-site scripting	A vulnerability was found in DW Promobar Plugin up to 1.0.4 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-2022-2423. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2386	Crowdsignal Dashboard Plugin up to 3.0.7 on WordPress cross-site scripting	A vulnerability was found in Crowdsignal Dashboard Plugin up to 3.0.7 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-2386. 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 the scanner as cross-site scripting attack
CVE-2022-2398	Comments Fields Plugin up to 4.0 on WordPress Field Error Message cross-site scripting	A vulnerability classified as problematic has been found in Comments Fields Plugin up to 4.0. This affects an unknown part of the component Field Error Message Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2398. 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 the scanner as cross-site scripting attack
CVE-2022-2412	Better Tag Cloud Plugin up to 0.99.5 on WordPress Setting cross-site scripting	A vulnerability has been found in Better Tag Cloud Plugin up to 0.99.5 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-2412. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2411	Auto More Tag Plugin up to 4.0.0 on WordPress Setting cross-site scripting	A vulnerability which was classified as problematic was found in Auto More Tag Plugin up to 4.0.0. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-2411. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site Scripting attack
CVE-2022-36266	Airspan AirSpot 5410 up to 0.3.4.1-4 Binary File login.cgi cross-site scripting	A vulnerability classified as problematic was found in Airspan AirSpot 5410 up to 0.3.4.1-4. This vulnerability affects unknown code of the file /home/www/cgi-bin/login.cgi of the component Binary File Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-36266. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2767	SourceCodester Online Admission System /index.php student_add cross-site scripting	A vulnerability classified as problematic has been found in SourceCodester Online Admission System. This affects an unknown part of the file /index.php. The manipulation of the argument student_add leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2767. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2769	SourceCodester Company Website CMS /dashboard / contact phone cross-site scripting	A vulnerability which was classified as problematic has been found in SourceCodester Company Website CMS. This issue affects some unknown processing of the file / dashboard /contact. The manipulation of the argument phone leads to cross-site scripting. The identification of this vulnerability is CVE-2022-2769. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2777	microweber up to 1.3.0 cross-site scripting	A vulnerability which was classified as problematic has been found in microweber up to 1.3.0. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-2777. 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 the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-35509	EyouCMS 1.5.8 title crosssite scripting (ID 25)	A vulnerability has been found in EyouCMS 1.5.8 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument title leads to cross-site scripting. This vulnerability was named CVE-2022-35509. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site Scripting attack
CVE-2021-42750	ThingsBoard 3.3.1 Rule Engine title cross-site scripting (ID 167999)	A vulnerability was found in ThingsBoard 3.3.1 and classified as problematic. Affected by this issue is some unknown functionality of the component Rule Engine. The manipulation of the argument title leads to cross-site scripting. This vulnerability is handled as CVE-2021-42750. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-35585	ForkCMS 5.9.3 start_date cross-site scripting	A vulnerability was found in ForkCMS 5.9.3. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument start_date leads to cross-site scripting. This vulnerability is known as CVE-2022-35585. The attack can be launched remotely. There is no exploit available.		Detected by the scanner as cross-site scripting attack
CVE-2022-35587	Fork 5.9.3 publish_on_date cross-site scripting	A vulnerability was found in Fork 5.9.3. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument publish_on_date leads to crosssite scripting. This vulnerability was named CVE-2022-35587. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2814	SourceCodester Simple and Nice Shopping Cart Script /mkshope/login.php msg cross-site scripting	A vulnerability has been found in SourceCodester Simple and Nice Shopping Cart Script and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /mkshope/login.php. The manipulation of the argument msg leads to cross-site scripting. This vulnerability is known as CVE-2022-2814. The attack can be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2811	SourceCodester Guest Management System myform. php name cross-site scripting	A vulnerability classified as problematic has been found in SourceCodester Guest Management System. This affects an unknown part of the file myform.php. The manipulation of the argument name leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2811. 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-2022-2384	Supsystic Digital Publications Plugin up to 1.7.3 on WordPress Setting cross-site scripting	A vulnerability was found in Supsystic Digital Publications Plugin up to 1.7.3. It has been classified as problematic. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-2384. 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 the scanner as cross-site scripting attack
CVE-2022-2378	Easy Student Results Plugin up to 2.2.8 on WordPress a cross-site scripting	A vulnerability has been found in Easy Student Results Plugin up to 2.2.8 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument a lead to cross-site scripting. This vulnerability was named CVE-2022-2378. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2152	Duplicate Page and Post Plugin up to 2.7 on WordPress Setting cross-site scripting	A vulnerability which was classified as problematic was found in Duplicate Page and Post Plugin up to 2.7. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2152. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2116	Contact Form DB Plugin up to 1.7.x on WordPress Attribute cross-site scripting	A vulnerability which was classified as problematic has been found in Contact Form DB Plugin up to 1.7.x. Affected by this issue is some unknown functionality of the component Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-2116. 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 the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-36530	rageframe2 2.6.37 User-Agent info.php cross-site scripting (ID 106)	A vulnerability which was classified as problematic was found in Auto More Tag Plugin up to 4.0.0. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-2411. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site Scripting attack
CVE-2022-24654	Intelbras ATA 200 up to 74.19.10.21 Field Server Address cross-site scripting (ID 168064)	A vulnerability which was classified as problematic has been found in Intelbras ATA 200 up to 74.19.10.21. Affected by this issue is some unknown functionality. The manipulation of the argument Field Server Address leads to cross-site scripting. This vulnerability is handled as CVE-2022-24654. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-38357	Eyes of Network Parameter index.php url cross-site scripting	A vulnerability has been found in Eyes of Network and classified as problematic. Affected by this vulnerability is an unknown functionality of the file / module/module_frame/ index. php of the component Parameter Handler. The manipulation of the argument url leads to cross-site scripting. This vulnerability is known as CVE-2022-38357. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2871	NotrinosERP up to 0.6 crosssite scripting	A vulnerability which was classified as problematic has been found in NotrinosERP up to 0.6. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-2871. 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 the scanner as cross-site scripting attack
CVE-2022-35117	Clinics Patient Management System 1.0 Update Medical Details update_medicine_details.php Packing cross-site scripting	A vulnerability was found in Clinics Patient Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file update_medicine_ details. php of the component Update Medical Details. The manipulation of the argument Packing leads to cross-site scripting. The identification of this vulnerability is CVE-2022-35117. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-35151	kkFileView 4.1.0 OnlinePreviewController.java urls/currentUrl cross-site scripting (ID 366)	A vulnerability was found in kkFileView 4.1.0. It has been rated as problematic. This issue affects some unknown processing of the file /controller/OnlinePreviewController.java. The manipulation of the argument urls/currentUrl leads to cross-site scripting. The identification of this vulnerability is CVE-2022-35151. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site Scripting attack
CVE-2020-23466	PHPGurukul Online Marriage Registration System 1.0 wzipcode cross-site scripting (ID 48522 / EDB-48522)	A vulnerability was found in PHPGurukul Online Marriage Registration System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument wzipcode leads to cross-site scripting. This vulnerability is known as CVE-2020-23466. The attack can be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-35174	Kirby Starterkit 3.7.0.2 Tags cross-site scripting	A vulnerability which was classified as problematic was found in Kirby Starterkit 3.7.0.2. This affects an unknown part. The manipulation of the argument Tags leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-35174. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2021-32862	Jupyter nbconvert cross-site scripting (GHSA-9jmq-rx5f-8jwq)	A vulnerability was found in Jupyter nbconvert and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2021-32862. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-35910	Jellyfin up to 10.7 Access Token cross-site scripting	A vulnerability which was classified as problematic has been found in Jellyfin up to 10.7. Affected by this issue is some unknown functionality of the component Access Token Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-35910. 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 the scanner as cross-site scripting attack
CVE-2022-37063	FLIR AX8 up to 1.46.16 Web Management Interface crosssite scripting	A vulnerability was found in FLIR AX8 up to 1.46.16. It has been classified as problematic. Affected is an unknown function of the component Web Management Interface. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-37063. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-35213	Ecommerce-CodeIgniter-Bootstrap / blog/blogpublish.php base_url cross-site-scripting (ID 219)	A vulnerability was found in Ecommerce-CodeIgniter-Bootstrap. It has been declared as problematic. This vulnerability affects the function base_url of the file /blog/blogpublish.php. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-35213. 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-2022-37254	DolphinPHP 1.5.1 Configuration Management cross-site scripting (ID 42)	A vulnerability was found in DolphinPHP 1.5.1. It has been classified as problematic. Affected is an unknown function of the component Configuration Management. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-37254. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-0542	chatwoot up to 2.6.x crosssite scripting	A vulnerability has been found in chatwoot up to 2.6.x 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-2022-0542. 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 the scanner as cross-site scripting attack
CVE-2022-35554	BPC SmartVista 3.28.0 Error Message cross-site scripting	A vulnerability which was classified as problematic was found in BPC SmartVista 3.28.0. Affected is an unknown function of the component Error Message Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-35554. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2885	yetiforcecrm up to 6.3.x cross-site scripting	A vulnerability which was classified as problematic was found in yetiforcecrm up to 6.3.x. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2885. 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-2022-2375	WP Sticky Button Plugin up to 1.4.0 on WordPress crosssite scripting	A vulnerability was found in WP Sticky Button Plugin up to 1.4.0 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-2022-2375. 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 the scanner as cross-site scripting attack
CVE-2022-2361	WP Social Chat Plugin up to 6.0.4 on WordPress Setting cross-site scripting	A vulnerability which was classified as problematic was found in WP Social Chat Plugin up to 6.0.4. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2361. 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 the scanner as cross-site scripting attack
CVE-2022-2407	WP phpMyAdmin Plugin prior 5.2.0.4 on WordPress Setting cross-site scripting	A vulnerability was found in WP phpMyAdmin Plugin. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-2407. 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 the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-24910	Transposh WordPress Translation Plugin up to 1.0.7 on WordPress AJAX Action cross-site scripting	A vulnerability was found in Transposh WordPress Translation Plugin up to 1.0.7 and classified as problematic. Affected by this issue is some unknown functionality of the component AJAX Action Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2021-24910. 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-2022-1932	Rezgo Online Booking Plugin up to 4.1.7 on WordPress AJAX Action cross-site scripting	A vulnerability which was classified as problematic was found in Rezgo Online Booking Plugin up to 4.1.7. This affects an unknown part of the component AJAX Action Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1932. 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 the scanner as cross-site scripting attack
CVE-2022-2383	Feed Them Social Plugin up to 3.0.0 on WordPress crosssite scripting	A vulnerability was found in Feed Them Social Plugin up to 3.0.0 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-2383. 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 the scanner as cross-site scripting attack
CVE-2022-2362	Download Manager Plugin prior 3.2.50 on WordPress Restrictions cross-site scripting	A vulnerability was found in Download Manager Plugin. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Restrictions Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-2362. 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 the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1322	Coming Soon Under Construction Plugin up to 1.1.9 on WordPress Setting cross-site scripting	A vulnerability was found in Coming Soon Under Construction Plugin up to 1.1.9. It has been rated as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1322. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site Scripting attack
CVE-2022-36251	Clinics Patient Management System 1.0 patients.php cross-site scripting	A vulnerability was found in Clinics Patient Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file patients.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-36251. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-1340	yetiforcecrm up to 6.3.x cross-site scripting	A vulnerability has been found in yetiforcecrm up to 6.3.x and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-1340. 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 the scanner as cross-site scripting attack
CVE-2022-2796	pimcore up to 10.5.3 crosssite scripting	A vulnerability has been found in pimcore up to 10.5.3 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-2022-2796. 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 the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-28598	Frappe ERPNext up to 12.28.x cross-site scripting	A vulnerability was found in Frappe ERPNext up to 12.28.x. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-28598. 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-2022-2956	ConsoleTVs Noxen / Noxenmaster/users.php create_user_username cross-site scripting	A vulnerability classified as problematic has been found in ConsoleTVs Noxen. Affected is an unknown function of the file / Noxen-master/users.php. The manipulation of the argument create_user_username with the input "><script>alert</script> leads to cross-site scripting. This vulnerability is traded as CVE-2022-2956. It is possible to launch the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2932	bustle mobiledoc-kit up to 0.14.1 cross-site scripting	A vulnerability was found in bustle mobiledoc-kit up to 0.14.1. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-2932. 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 the scanner as cross-site scripting attack
CVE-2022-37245	MDaemon SecurityGateway for Email Servers 8.5.2 Blacklist Endpoint cross-site scripting	A vulnerability which was classified as problematic has been found in MDaemon SecurityGateway for Email Servers 8.5.2. This issue affects some unknown processing of the component Blacklist Endpoint. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-37245. 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 the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-37244	MDaemon SecurityGateway for Email Servers 8.5.2 currentRequest response splitting	A vulnerability which was classified as critical was found in MDaemon SecurityGateway for Email Servers 8.5.2. This affects an unknown part. The manipulation of the argument currentRequest leads to http response splitting. This vulnerability is uniquely identified as CVE-2022-37244. 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-2022-37160	Claroline up to 13.5.7 SVG File cross-site scripting	A vulnerability was found in Claroline up to 13.5.7. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component SVG File Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-37160. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-37162	Claroline up to 13.5.7 Calendar Event Location cross-site scripting	A vulnerability was found in Claroline up to 13.5.7 and classified as problematic. This issue affects some unknown processing of the component Calendar Event Handler. The manipulation of the argument Location leads to cross-site scripting. The identification of this vulnerability is CVE-2022-37162. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-37150	SourceCodester Online Diagnostic Lab Management System 1.0 cross-site scripting	A vulnerability has been found in SourceCodester Online Diagnostic Lab Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument firstname /address/middlename/lastname /gender/email/contact leads to cross-site scripting. This vulnerability is known as CVE-2022-37150. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-39393	mm-wiki 0.2.1 Markdown Editor cross-site scripting (ID 315)	A vulnerability was found in mm-wiki 0.2.1. It has been classified as problematic. This affects an unknown part of the component Markdown Editor. The manipulation leads to crosssite scripting. This vulnerability is uniquely identified as CVE-2021-39393. 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-2022-36527	Jfinal CMS 5.1.0 Blog Module cross-site scripting (ID 45)	A vulnerability classified as problematic was found in Jfinal CMS 5.1.0. Affected by this vulnerability is an unknown functionality of the component Blog Module. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-36527. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-3014	SourceCodester Simple Task Managing System student_add cross-site scripting	A vulnerability classified as problematic was found in SourceCodester Simple Task Managing System. This vulnerability affects unknown code. The manipulation of the argument student_add leads to cross-site scripting. This vulnerability was named CVE-2022-3014. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-36548	edoc-doctor-appointmentsystem 1.0.1 /patient/settings.php Name cross-site scripting	A vulnerability was found in edoc-doctor-appointment-system 1.0.1 and classified as problematic. This issue affects some unknown processing of the file /patient/settings.php. The manipulation of the argument Name leads to cross-site scripting. The identification of this vulnerability is CVE-2022-36548. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2021-3427	Deluge Web UI cross-site scripting (ID 3459)	A vulnerability was found in Deluge and classified as problematic. This issue affects some unknown processing of the component Web UI. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2021-3427. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Indusface is a leading application security SaaS company that secures critical Web, Mobile & API applications of 3000+ 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.

CONTACT US - +91 265 6133021 | +1 866 537 8234
EMAIL - sales@indusface.com

Indusface is the Only Vendor To Be Named Gartner® Peer Insights™ Customers' Choice in All the 7 Segments of Voice of Customer WAAP 2022 Report.