INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

May 2022

Total Zero-Day Vulnerabilities Found: 271

Command Injection	CSRF	Local File Inclusion	Cross-Site Scripting	SQL Injection
19	6	17	109	120

Zero-Day vulnerabilities protected through core rules	271
Zero-Day vulnerabilities protected through custom rules	0*
Zero-Day vulnerabilities for which protection cannot be determined	0**
Zero-Day vulnerabilities found by Indusface WAS	265

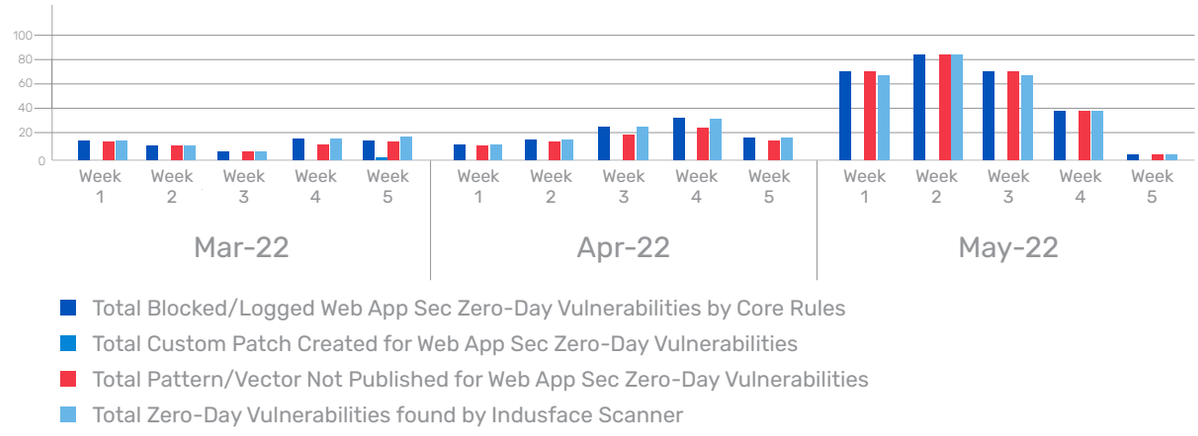
* To enable the custom rules, please contact support@indusface.com

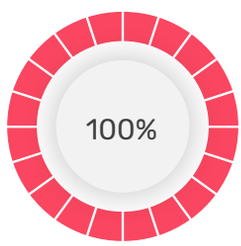
** Since the attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.

Vulnerability Trend:

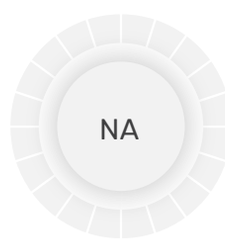
The weekly trend displays the total number of vulnerabilities discovered to the type of protection provided for the last quarter.

Weekly Vulnerability Trend of Last 3 Months

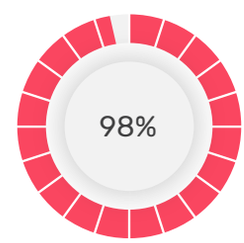




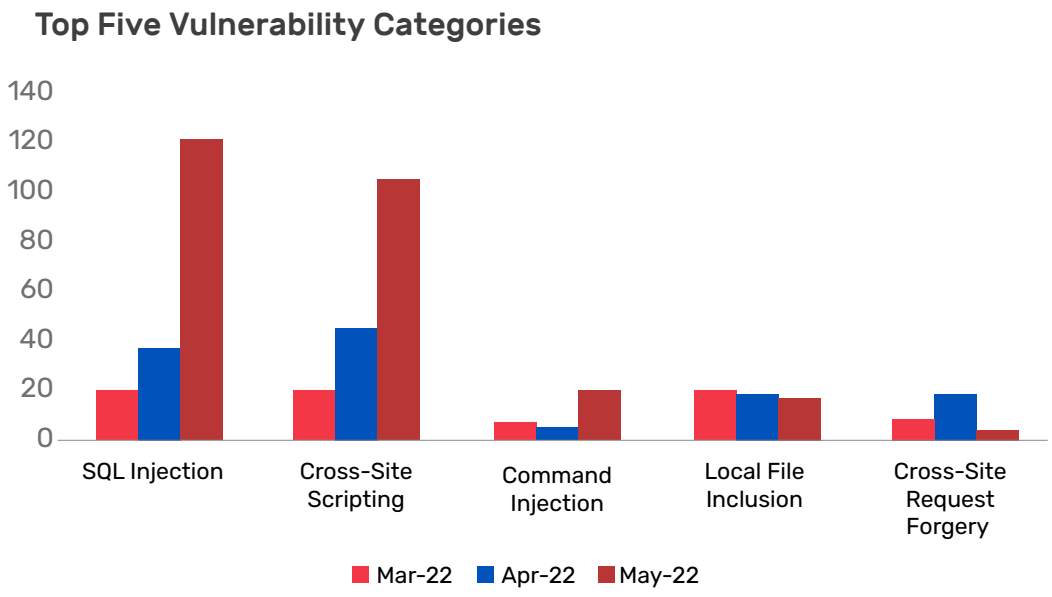
of the zero-day vulnerabilities were protected by the **core rules** in this month



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



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



Vulnerability Details:

1. Vulnerability Type: Command Injection

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-21189	dexie up to 3.2.1/4.0.0-alpha.2 setByKeyPath code injection	A vulnerability classified as critical has been found in dexie up to 3.2.1/4.0.0-alpha.2. This affects the function setByKeyPath. The manipulation leads to privilege escalation. This vulnerability is uniquely identified as CVE-2022-21189. 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 the Command Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-25301	js-gui-lang-es-sentials code injection	A vulnerability was found in js-gui-lang-essentials and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to privilege escalation. This vulnerability is handled as CVE-2022-25301. Access to the local network is required for this attack. There is no exploit available.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.
CVE-2022-24437	git-pull-or-clone up to 2.0.1 spawn outpath command injection (SNYK-JS-GIT-PULLOR-CLONE-2434307)	A vulnerability was found in git-pull-or-clone up to 2.0.1. It has been classified as critical. Affected is the function spawn. The manipulation of the argument outpath leads to privilege escalation. This vulnerability is traded as CVE-2022-24437. 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 the Command Injection attack.
CVE-2022-22143	convict up to 6.2.1 parentKey code injection (SNYK-JS-CONVICT-2340604)	A vulnerability, which was classified as critical, was found in convict up to 6.2.1. Affected is an unknown function. The manipulation of the argument parentKey leads to privilege escalation. This vulnerability is traded as CVE-2022-22143. 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 the Command Injection attack.
CVE-2022-25645	dset DSET Mode/ Merge Mode code injection	A vulnerability was found in dset. It has been declared as critical. This vulnerability affects unknown code of the component DSET Mode/Merge Mode. The manipulation leads to privilege escalation. This vulnerability was named CVE-2022-25645. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-42165	MitraStar GPT-2541GNAC-N1 100VNZ0b33 path os command injection (ID 164333 / EDB-50351)	A vulnerability was found in MitraStar GPT-2541GNAC-N1 100VNZ0b33. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument path leads to privilege escalation. The identification of this vulnerability is CVE-2021-42165. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.
CVE-2021-41739 | Artica Proxy 4.30.000000 cyrus.events.php logs/rp os command injection	Artica Proxy 4.30.000000 cyrus.events.php logs/rp os command injection	A vulnerability classified as critical was found in Artica Proxy 4.30.000000. Affected by this vulnerability is an unknown functionality of the file cyrus.events.php. The manipulation of the argument logs/rp leads to privilege escalation. This vulnerability is known as CVE-2021-41739. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.
CVE-2022-23332	Shenzhen Ejoin ACOM508/ ACOM516/ ACOM532 609-915-041-100-020 Manual Ping Form command injection	A vulnerability classified as critical was found in Shenzhen Ejoin ACOM508, ACOM516 and ACOM532 609-915-041-100-020. This vulnerability affects unknown code of the component Manual Ping Form. The manipulation leads to privilege escalation. This vulnerability was named CVE-2022-23332. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.
CVE-2022-27224	Galleon NTS-6002 Web-Management Interface ping_address/ trace_address/ nslookup_address os command injection	A vulnerability classified as critical has been found in Galleon NTS-6002. This affects an unknown part of the component Web-Management Interface. The manipulation of the argument ping_address/trace_address/ nslookup_address leads to privilege escalation. This vulnerability is uniquely identified as CVE-2022-27224. It is possible to initiate the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-42581	Ramda up to 0.27.0 mapObjIndexed code injection	A vulnerability classified as critical was found in Ramda up to 0.27.0. Affected by this vulnerability is the function mapObjIndexed. The manipulation leads to privilege escalation. This vulnerability is known as CVE-2021-42581. The attack needs to be initiated within the local network. Furthermore, there is an exploit available. It is recommended to apply a patch to fix this issue.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.
CVE-2022-29307	IonizeCMS 1.0.8.1 lang_model.php copy_lang_content command injection (ID 405)	A vulnerability was found in IonizeCMS 1.0.8.1. It has been rated as critical. This issue affects the function copy_lang_content of the file application/models/lang_model.php. The manipulation leads to privilege escalation. The identification of this vulnerability is CVE-2022-29307. Access to the local network is required for this attack. There is no exploit available.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.
CVE-2021-42969	Anaconda 2021.05 usercustomize.py os command injection	A vulnerability has been found in Anaconda 2021.05 and classified as critical. Affected by this vulnerability is an unknown functionality of the file usercustomize.py. The manipulation leads to privilege escalation. This vulnerability is known as CVE-2021-42969. The attack can only be initiated within the local network. There is no exploit available.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.
CVE-2022-29303	SolarView Compact 6.00 conf_mail.php command injection	A vulnerability has been found in SolarView Compact 6.00 and classified as critical. Affected by this vulnerability is an unknown functionality of the file conf_mail.php. The manipulation leads to privilege escalation. This vulnerability is known as CVE-2022-29303. Access to the local network is required for this attack. There is no exploit available.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.
CVE-2022-25862	sds 0.0.0 js/set.js set code injection (SNYK-JS-SDS-2385944)	A vulnerability classified as critical was found in sds 0.0.0. Affected by this vulnerability is the function set of the file js/set.js. The manipulation leads to privilege escalation. This vulnerability is known as CVE-2022-25862. It is possible to launch the attack on the local host. There is no exploit available.	Protected by Core Rules	Detected by the scanner as the Command Injection attack.

2. Vulnerability Type: Cross-Site Request Forgery

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-0191	Ad Invalid Click Protector Plugin up to 1.2.6 on WordPress cross-site request forgery (ID 2705068)	A vulnerability was found in Ad Invalid Click Protector Plugin up to 1.2.6. 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-2022-0191. 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-2022-23904	Rainworx Auctionworx Enterprise/Auctionworx Events Edition up to 3.1R1 Admin Control Panel cross-site request forgery	A vulnerability was found in Rainworx Auctionworx Enterprise and Auctionworx Events Edition up to 3.1R1. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Admin Control Panel. The manipulation leads to cross site request forgery. This vulnerability is known as CVE-2022-23904. 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-2022-25778	Secomea GateManager Web UI cross-site request forgery	A vulnerability, which was classified as problematic, was found in Secomea GateManager. This affects an unknown part of the component Web UI. The manipulation leads to cross site request forgery. This vulnerability is uniquely identified as CVE-2022-25778. It is possible to initiate the attack remotely. There is no exploit available.	Protected by Core Rules	NA
CVE-2022-30953	Blue Ocean Plugin up to 1.25.3 on Jenkins HTTP Server cross-site request forgery	A vulnerability was found in Blue Ocean Plugin up to 1.25.3. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component HTTP Server. The manipulation leads to cross site request forgery. This vulnerability is known as CVE-2022-30953. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	NA
CVE-2022-28921	BlogEngine.NET 3.3.8.0 cross-site request forgery	A vulnerability, which was classified as problematic, was found in BlogEngine.NET 3.3.8.0. Affected is an unknown function. The manipulation leads to cross site request forgery. This vulnerability is traded as CVE-2022-28921. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-29427	Aftab Muni Disable Right Click for WP Plugin up to 1.1.6 on WordPress cross-site request forgery	A vulnerability was found in Aftab Muni Disable Right Click for WP Plugin up to 1.1.6. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross site request forgery. The identification of this vulnerability is CVE-2022-29427. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	NA
CVE-2022-0191	Ad Invalid Click Protector Plugin up to 1.2.6 on WordPress cross-site request forgery (ID 2705068)	A vulnerability was found in Ad Invalid Click Protector Plugin up to 1.2.6. 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-2022-0191. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	NA

3. Vulnerability Type: Local File Inclusion

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-25842	com.alibaba.oneagent:one-java-agent-plugin ZIP File path-name traversal	A vulnerability was found in com.alibaba.oneagent:one-java-agent-plugin. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component ZIP File Handler. The manipulation leads to directory traversal. This vulnerability is known as CVE-2022-25842. The attack can be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
CVE-2022-26068	pistache prior 0.0.3.20220425 path traversal	A vulnerability was found in pistache. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to directory traversal. The identification of this vulnerability is CVE-2022-26068. 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 Local File Inclusion Attack
CVE-2022-1554	clinical-genomics scout up to 4.51 send_file path traversal	A vulnerability was found in clinical-genomics scout up to 4.51. It has been classified as critical. Affected is the function send_file. The manipulation leads to directory traversal. This vulnerability is traded as CVE-2022-1554. 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 Local File Inclusion Attack
CVE-2022-24897	xwiki-commons up to 12.6.6/12.10.2 API path traversal (GHSA-cvx5-m8vg-vxgc)	A vulnerability has been found in xwiki-commons up to 12.6.6/12.10.2 and classified as critical. Affected by this vulnerability is an unknown functionality of the component API. The manipulation leads to directory traversal. This vulnerability is known as CVE-2022-24897. 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 Local File Inclusion Attack
CVE-2021-42183	MasaCMS 7.2.1 path traversal	A vulnerability was found in MasaCMS 7.2.1. It has been classified as critical. This affects an unknown part of the file /index.cfm/_api/asset/image/. The manipulation leads to directory traversal. This vulnerability is uniquely identified as CVE-2021-42183. The attack needs to be initiated within the local network. There is no exploit available.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-45783	Bookeen Notea BK_R_1.0.5_ 20210608 pathname traversal	A vulnerability, which was classified as problematic, was found in Bookeen Notea BK_R_1.0.5_20210608. This affects an unknown part. The manipulation leads to directory traversal. This vulnerability is uniquely identified as CVE-2021-45783. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
CVE-2022-30062	ftcms up to 2.1 tp.php path traversal	A vulnerability was found in ftcms up to 2.1. It has been rated as problematic. Affected by this issue is some unknown functionality of the file tp.php. The manipulation leads to directory traversal. This vulnerability is handled as CVE-2022-30062. The attack can only be initiated within the local network. There is no exploit available.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
CVE-2022-30061	ftcms up to 2.1 tp pathname traversal	A vulnerability classified as critical has been found in ftcms up to 2.1. Affected is an unknown function. The manipulation of the argument tp leads to directory traversal. This vulnerability is traded as CVE-2022-30061. The attack needs to be initiated within the local network. There is no exploit available.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
CVE-2021-34605	XINJE PLC Program Tool up to 3.5.1 Project File path traversal	A vulnerability, which was classified as problematic, was found in XINJE PLC Program Tool up to 3.5.1. This affects an unknown part of the component Project File Handler. The manipulation leads to directory traversal. This vulnerability is uniquely identified as CVE-2021-34605. It is possible to initiate the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-29596	MicroStrategy Enterprise Manager 2022 Uid pathname traversal	A vulnerability classified as critical was found in MicroStrategy Enterprise Manager 2022. Affected by this vulnerability is an unknown functionality. The manipulation of the argument Uid leads to directory traversal. This vulnerability is known as CVE-2022-29596. Access to the local network is required for this attack to succeed. Furthermore, there is an exploit available.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
CVE-2022-1560	Amministrazione Aperta Plugin up to 3.7.3 on WordPress open path traversal	A vulnerability was found in Amministrazione Aperta Plugin up to 3.7.3 and classified as critical. This issue affects some unknown processing. The manipulation of the argument open leads to directory traversal. The identification of this vulnerability is CVE-2022-1560. The attack can only be done within the local network. There is no exploit available.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
CVE-2022-1721	jgraph drawio up to 18.0.4 WellKnownServlet path traversal	A vulnerability classified as critical was found in jgraph drawio up to 18.0.4. Affected by this vulnerability is an unknown functionality of the component WellKnownServlet. The manipulation leads to directory traversal. This vulnerability is known as CVE-2022-1721. 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 Local File Inclusion Attack
CVE-2022-29446	Counter Box Plugin up to 1.1.1 file inclusion	A vulnerability was found in Counter Box Plugin up to 1.1.1. It has been classified as critical. Affected is an unknown function. The manipulation leads to privilege escalation. This vulnerability is traded as CVE-2022-29446. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-29447	Wow-Company Hover Effects Plugin up to 2.1 on WordPress file inclusion	A vulnerability, which was classified as critical, was found in Wow-Company Hover Effects Plugin up to 2.1. Affected is an unknown function. The manipulation leads to privilege escalation. This vulnerability is traded as CVE-2022-29447. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
CVE-2022-29448	Wow-Company Herd Effects Plugin up to 5.2 on WordPress file inclusion	A vulnerability has been found in Wow-Company Herd Effects Plugin up to 5.2 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to privilege escalation. This vulnerability is known as CVE-2022-29448. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
CVE-2022-31268	Gitblit 1.9.3 /resources//../ path traversal	A vulnerability was found in Gitblit 1.9.3. It has been declared as critical. This vulnerability affects unknown code of the file /resources//../. The manipulation leads to directory traversal. This vulnerability was named CVE-2022-31268. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as Local File Inclusion Attack
CVE-2022-1850	filegator up to 7.7.x path traversal	A vulnerability classified as critical has been found in filegator up to 7.7.x. Affected is an unknown function. The manipulation leads to directory traversal. This vulnerability is traded as CVE-2022-1850. 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 Local File Inclusion Attack

4. Vulnerability Type: Cross-Site Scripting

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-23060	Shopizer up to 2.17.0 Manage Files filename cross-site scripting	A vulnerability, which was classified as problematic, was found in Shopizer up to 2.17.0. This affects an unknown part of the component Manage Files. The manipulation of the argument filename leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-23060. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-25349	materialize-css cross-site scripting	A vulnerability was found in materialize-css. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-25349. 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-2022-0418	Event List Plugin up to 0.8.7 on WordPress Setting cross-site scripting	A vulnerability was found in Event List Plugin up to 0.8.7. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-0418. 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-2021-31673	Cyclos Pro up to 14.7 Account Registration groupId cross-site scripting	A vulnerability classified as problematic has been found in Cyclos Pro up to 14.7. This affects an unknown part of the component Account Registration Handler. The manipulation of the argument groupId leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2021-31673. 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-2022-0649	AdRotate Plugin up to 5.8.22 on WordPress Group Name cross-site scripting	A vulnerability classified as problematic was found in AdRotate Plugin up to 5.8.22. This vulnerability affects unknown code of the component Group Name Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-0649. The attack can be initiated remotely. There is no Protected by Core Rules 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-2022-1255	Import and Export Users and Customers Plugin up to 1.19.2.0 on WordPress CSV Data cross-site scripting	A vulnerability was found in Import and Export Users and Customers Plugin up to 1.19.2.0. It has been classified as problematic. This affects an unknown part of the component CSV Data Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1255. 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-2022-1250	LifterLMS PayPal Plugin up to 1.3.x on WordPress Payment Confirmation Page cross-site scripting	A vulnerability was found in LifterLMS PayPal Plugin up to 1.3.x and classified as problematic. Affected by this issue is some unknown functionality of the component Payment Confirmation Page. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-1250. 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-2021-25102	All In One WP Security & Firewall Plugin up to 4.4.10 on WordPress Location Header redirect_ to cross-site scripting	A vulnerability was found in All In One WP Security & Firewall Plugin up to 4.4.10. It has been classified as problematic. Affected is an unknown function of the component Location Header Handler. The manipulation of the argument redirect to leads to cross-site scripting. This vulnerability is traded as CVE-2021-25102. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-0428	Content Egg Plugin up to 5.2.x on WordPress Autoblogging Admin Dashboard page cross-site scripting	A vulnerability classified as problematic has been found in Content Egg Plugin up to 5.2.x. This affects an unknown part of the component Autoblogging Admin Dashboard. The manipulation of the argument page leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-0428. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1046	Visual Form Builder Plugin up to 3.0.6 on WordPress Email to cross-site scripting	A vulnerability has been found in Visual Form Builder Plugin up to 3.0.6 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument email to leads to cross-site scripting. This vulnerability is known as CVE-2022-1046. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1282	10Web Photo Gallery Plugin up to 1.6.2 on WordPress AJAX Action image_url cross-site scripting	A vulnerability has been found in 10Web Photo Gallery Plugin up to 1.6.2 and classified as problematic. This vulnerability affects unknown code of the component AJAX Action Handler. The manipulation of the argument image_url leads to cross-site scripting. This vulnerability was named CVE-2022-1282. 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-2021-25086	Advanced Page Visit Counter Plugin up to 5.0.8 on WordPress Admin Dashboard Page cross-site scripting	A vulnerability was found in Advanced Page Visit Counter Plugin up to 5.0.8 and classified as problematic. This issue affects some unknown processing of the component Admin Dashboard Page. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2021-25086. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2021-31674	Cyclos Pro up to 4.14.7 Error cross-site scripting	A vulnerability was found in Cyclos Pro up to 4.14.7. It has been classified as problematic. Affected is an unknown function of the component Error Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2021-31674. 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-2022-0662	AdRotate Plugin up to 5.8.22 on WordPress Advert Name cross-site scripting	A vulnerability, which was classified as problematic, has been found in AdRotate Plugin up to 5.8.22. This issue affects some unknown processing of the component Advert Name Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-0662. 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-29969	RSS Extension on MediaWiki RSS Element cross-site scripting	A vulnerability was found in RSS Extension and classified as problematic. This issue affects some unknown processing of the component RSS Element Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-29969. 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-2022-23065	Vendure up to 1.5.1 SVG File cross-site scripting	A vulnerability has been found in Vendure up to 1.5.1 and classified as problematic. This vulnerability affects unknown code of the component SVG File Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-23065. The attack can be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1269	Fast Flow Plugin up to 1.2.10 on WordPress Admin Dashboard page cross-site scripting	A vulnerability was found in Fast Flow Plugin up to 1.2.10. It has been declared as problematic. This vulnerability affects unknown code of the component Admin Dashboard. The manipulation of the argument page leads to cross-site scripting. This vulnerability was named CVE-2022-1269. 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-2021-36844	MyThemeShop WP Subscribe Plugin up to 1.2.12 on WordPress cross-site scripting	A vulnerability, which was classified as problematic, has been found in MyThemeShop WP Subscribe Plugin up to 1.2.12. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2021-36844. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-28589	Pixelimity 1.0 pages.php Title cross-site scripting (ID 23)	A vulnerability classified as problematic has been found in Pixelimity 1.0. This affects an unknown part of the file admin/pages.php?action=add_new. The manipulation of the argument Title leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-28589. 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-2021-39390	PartKeepr 1.4.0 API Endpoint name cross-site scripting (ID 1237)	A vulnerability, which was classified as problematic, has been found in PartKeepr 1.4.0. This issue affects some unknown processing of the component API Endpoint Handler. The manipulation of the argument name leads to cross-site scripting. The identification of this vulnerability is CVE-2021-39390. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-28588	SpringBootMovie up to 1.2 Movie Name cross-site scripting	A vulnerability was found in SpringBootMovie up to 1.2. It has been classified as problematic. This affects an unknown part of the component Movie Name Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-28588. 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-2022-1555	Microweber up to 1.2.15 cross-site scripting	A vulnerability classified as problematic has been found in Microweber up to 1.2.15. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-1555. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-27330	SourceCodester E-Commerce Website 1.0 index.php Product Title cross-site scripting	A vulnerability was found in SourceCodester E-Commerce Website 1.0 and classified as problematic. This issue affects some unknown processing of the file /public/admin/index.php?add_product. The manipulation of the argument Product Title leads to cross-site scripting. The identification of this vulnerability is CVE-2022-27330. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-28508	MantisBT up to 2.25.1 Hidden Input Field browser_ search_plugin. php return cross-site scripting	A vulnerability classified as problematic has been found in MantisBT up to 2.25.1. This affects an unknown part of the file browser_search_plugin.php of the component Hidden Input Field Handler. The manipulation of the argument return leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-28508. 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-2022-1571	neorazorx facturascripts prior 2022.07 Create Subac-count cross-site scripting	A vulnerability classified as prob-lematic was found in neorazorx facturascripts. Affected by this vulnerability is an unknown functionality of the component Create Subaccount Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-1571. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1584	microweber up to 1.2.15 cross-site scripting	A vulnerability was found in microweber up to 1.2.15. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1584. 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-2022-1590	Bludit 3.13.1 New Content Module / admin/new-con-tent cross-site scripting	A vulnerability was found in Bludit 3.13.1. It has been declared as problematic. This vulnera-bility affects unknown code of the file /admin/new-content of the component New Content Module. The manipulation of the argument content with the input <script>alert(1)</ script> leads to cross-site scripting. This vulnerability was named CVE-2022-1590. The attack can be initiated remotely. Further-more, there is an exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1575	jgraph drawio up to 17.x cross-site scripting	A vulnerability was found in jgraph drawio up to 17.x. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-1575. 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-2022-29939	LibreHealth EHR 2.0.0 GET Parameter sl_eob_process.php debug/InsId cross-site scripting	A vulnerability was found in LibreHealth EHR 2.0.0. It has been classified as problematic. Affected is an unknown function of the file interface\billing\sl_eob_process.php of the component GET Parameter Handler. The manipulation of the argument debug/InsId leads to cross-site scripting. This vulnerability is traded as CVE-2022-29939. 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-2022-1047	Themify Post Type Builder Search Addon Plugin up to 1.3.x on WordPress cross-site scripting	A vulnerability was found in Themify Post Type Builder Search Addon Plugin up to 1.3.x. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-1047. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-0898	IgniteUp Plugin up to 3.4.1 on WordPress cross-site scripting	A vulnerability was found in IgniteUp Plugin up to 3.4.1. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-0898. 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-2022-0625	Admin Menu Editor Plugin up to 1.0.4 on WordPress cross-site scripting	A vulnerability has been found in Admin Menu Editor Plugin up to 1.0.4 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-0625. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1171	Vertical Scroll Recent Post Plugin up to 13.x on WordPress cross-site scripting	A vulnerability classified as problematic has been found in Vertical Scroll Recent Post Plugin up to 13.x. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1171. 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-2022-0874	WP Social Buttons Plugin up to 2.1 on WordPress cross-site scripting	A vulnerability was found in WP Social Buttons Plugin up to 2.1 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-0874. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1338	Easily Generate Rest API Url Plugin up to 1.0.0 on WordPress cross-site scripting	A vulnerability, which was classified as problematic, has been found in Easily Generate Rest API Url Plugin up to 1.0.0. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1338. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1104	Popup Maker Plugin up to 1.16.4 on WordPress cross-site scripting	A vulnerability was found in Popup Maker Plugin up to 1.16.4. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-1104. 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-2022-27308	PHProjekt PhpSimplyGest 1.3.0 Project Title cross-site scripting (ID 166966)	A vulnerability classified as problematic was found in PHProjekt PhpSimplyGest 1.3.0. Affected by this vulnerability is an unknown functionality of the component Project Title Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-27308. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1567	WP-JS Plugin up to 2.0.6 on WordPress wp-js.php wp_js_admin cross-site scripting	A vulnerability was found in WP-JS Plugin up to 2.0.6. It has been rated as problematic. This issue affects the function wp_js_admin of the file wp-js.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1567. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-29727	Survey Sparrow Enterprise Survey Software 2022 Signup cross-site scripting	A vulnerability, which was classified as problematic, has been found in Survey Sparrow Enterprise Survey Software 2022. This issue affects some unknown processing. The manipulation of the argument Signup leads to cross-site scripting. The identification of this vulnerability is CVE-2022-29727. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2021-42648	CDR code-server up to 3.11.x URL cross-site scripting (ID 4355)	A vulnerability was found in CDR code-server up to 3.11.x. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component URL Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2021-42648. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2021-31330	Review Board up to 3.0.20/4.0 RC1 Markdown cross-site scripting	A vulnerability was found in Review Board up to 3.0.20/4.0 RC1. It has been classified as problematic. Affected is an unknown function of the component Markdown Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2021-31330. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2021-22531	Micro Focus NetIQ Access Manager 4.5/5.0 cross-site scripting	A vulnerability was found in Micro Focus NetIQ Access Manager 4.5/5.0. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2021-22531. 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1062	th23 Social Plugin up to 1.2.0 on WordPress cross-site scripting	A vulnerability classified as problematic was found in th23 Social Plugin up to 1.2.0. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-1062. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1216	Advanced Image Sitemap Plugin up to 1.2 on WordPress Admin Page cross-site scripting	A vulnerability was found in Advanced Image Sitemap Plugin up to 1.2. It has been rated as problematic. This issue affects some unknown processing of the component Admin Page. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1216. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1559	Clipr Plugin up to 1.2.3 on WordPress API Key Setting cross-site scripting	A vulnerability has been found in Clipr Plugin up to 1.2.3 and classified as problematic. This vulnerability affects unknown code of the component API Key Setting Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-1559. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1408	VikBooking Hotel Booking Engine & PMS Plugin up to 1.5.7 on WordPress cross-site scripting	A vulnerability was found in VikBooking Hotel Booking Engine & PMS Plugin up to 1.5.7. 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-2022-1408. 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-2022-1726	bootstrap-table up to 1.20.1 Table Export Plug-In cross-site scripting	A vulnerability, which was classified as problematic, has been found in bootstrap-table up to 1.20.1. This issue affects some unknown processing of the component Table Export Plug-In. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1726. 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-2022-1465	WPC Smart Wishlist for WooCommerce Plugin up to 2.9.8 on WordPress AJAX Action cross-site scripting	A vulnerability has been found in WPC Smart Wishlist for WooCommerce Plugin up to 2.9.8 and classified as problematic. This vulnerability affects unknown code of the component AJAX Action Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-1465. 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-2022-1726	Admin Menu Editor Plugin up to 1.0.4 on WordPress cross-site scripting	A vulnerability has been found in Admin Menu Editor Plugin up to 1.0.4 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-0625. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1334	WP YouTube Live Plugin up to 1.8.2 on WordPress Setting cross-site scripting	A vulnerability was found in WP YouTube Live Plugin up to 1.8.2 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-2022-1334. 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-2022-1051	WPQA Builder Plugin Plugin up to 5.1 on WordPress cross-site scripting	A vulnerability, which was classified as problematic, was found in WPQA Builder Plugin Plugin up to 5.1. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1051. 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-2022-1265	BulletProof Security Plugin up to 6.0 CAPTCHA Setting cross-site scripting	A vulnerability, which was classified as problematic, was found in BulletProof Security Plugin up to 6.0. Affected is an unknown function of the component CAPTCHA Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-1265. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1436	WPCargo Track & Trace Plugin up to 6.9.4 on WordPress wpcargo_tracking_number cross-site scripting	A vulnerability classified as problematic was found in WPCargo Track & Trace Plugin up to 6.9.4. Affected by this vulnerability is an unknown functionality. The manipulation of the argument wpcargo_tracking_number leads to cross-site scripting. This vulnerability is known as CVE-2022-1436. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-0873	Gmedia Photo Gallery Plugin up to 1.19.x on WordPress Album Name cross-site scripting	A vulnerability classified as problematic has been found in Gmedia Photo Gallery Plugin up to 1.19.x. This affects an unknown part of the component Album Name Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-0873. 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-2022-1217	Custom TinyMCE Shortcode Button Plugin up to 1.1 on WordPress cross-site scripting	A vulnerability classified as problematic has been found in Custom TinyMCE Shortcode Button Plugin up to 1.1. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-1217. 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-2022-1435	WPCargo Track & Trace Plugin up to 6.9.4 on WordPress Setting cross-site scripting	A vulnerability classified as problematic has been found in WPCargo Track & Trace Plugin up to 6.9.4. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-1435. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1455	Call Now Button Plugin up to 1.1.1 on WordPress Attribute cross-site scripting	A vulnerability, which was classified as problematic, has been found in Call Now Button Plugin up to 1.1.1. 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-2022-1455. 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-2022-1089	Bulk Edit and Create User Profiles Plugin up to 1.5.13 on WordPress User Login cross-site scripting	A vulnerability, which was classified as problematic, has been found in Bulk Edit and Create User Profiles Plugin up to 1.5.13. This issue affects some unknown processing of the component User Login. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1089. 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-2022-1393	WP Subtitle Plugin up to 3.4.0 on WordPress wp_subtitle cross-site scripting	A vulnerability was found in WP Subtitle Plugin up to 3.4.0. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument wp_subtitle leads to cross-site scripting. This vulnerability was named CVE-2022-1393. 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-2022-1512	ScrollReveal.js Effects Plugin up to 1.2 on WordPress Setting cross-site scripting	A vulnerability, which was classified as problematic, was found in ScrollReveal.js Effects Plugin up to 1.2. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1512. 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-2022-30013	totaljs CMS 3.4.5 JavaScript Embedded PDF cross-site scripting	A vulnerability was found in totaljs CMS 3.4.5. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component JavaScript Embedded PDF Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-30013. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-30050	Gnuboard 5.55/5.56 bbs/member_confirm.php cross-site scripting	A vulnerability has been found in Gnuboard 5.55/5.56 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file bbs/member_confirm.php. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-30050. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-30776	atmail 6.5.0 index.php/admin/index/error cross-site scripting	A vulnerability classified as problematic has been found in atmail 6.5.0. This affects an unknown part of the file index.php/admin/index/. The manipulation of the argument error leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-30776. 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-2021-42943	IPPlan 4.92b admin/user-manager.php userid cross-site scripting	A vulnerability, which was classified as problematic, has been found in IPPlan 4.92b. This issue affects some unknown processing of the file admin/usermanager.php. The manipulation of the argument userid leads to cross-site scripting. The identification of this vulnerability is CVE-2021-42943. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-30966	Random String Parameter Plugin up to 1.0 on Jenkins cross-site scripting	A vulnerability was found in Random String Parameter Plugin up to 1.0. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-30966. 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-2022-30961	Autocomplete Parameter Plugin up to 1.1 on Jenkins cross-site scripting	A vulnerability classified as problematic was found in Autocomplete Parameter Plugin up to 1.1. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-30961. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-30956	Rundeck Plugin up to 3.6.10 on Jenkins Webhook Submission cross-site scripting	A vulnerability was found in Rundeck Plugin up to 3.6.10. It has been rated as problematic. This issue affects some unknown processing of the component Webhook Submission Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-30956. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1432	OctoPrint up to 1.7.x cross-site scripting	A vulnerability, which was classified as problematic, was found in OctoPrint up to 1.7.x. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-1432. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1782	erudika para up to 1.45.10 cross-site scripting	A vulnerability has been found in erudika para up to 1.45.10 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-2022-1782. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1430	OctoPrint up to 1.7.x cross-site scripting	A vulnerability, which was classified as problematic, has been found in OctoPrint up to 1.7.x. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1430. 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-2022-1730	jgraph drawio up to 18.0.3 cross-site scripting	A vulnerability classified as problematic was found in jgraph drawio up to 18.0.3. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-1730. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-29449	Opal Hotel Room Booking Plugin up to 1.2.7 on WordPress cross-site scripting	A vulnerability was found in Opal Hotel Room Booking Plugin up to 1.2.7. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-29449. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1806	RTX cross-site scripting	A vulnerability classified as problematic has been found in RTX. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1806. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-28959	SPIP up to 3.1.13 /spip.php cross-site scripting	A vulnerability was found in SPIP up to 3.1.13 and classified as problematic. This issue affects some unknown processing of the file / spip.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-28959. The attack may be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-25224	Proton 0.2.0 Markdown File cross-site scripting	A vulnerability was found in Proton 0.2.0 and classified as problematic. This issue affects some unknown processing of the component Markdown File Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-25224. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-29183	GoCD up to 21.3.x Pipeline Comparison Error cross-site scripting (GHSA-3vvq-q4qv-x2gf)	A vulnerability was found in GoCD up to 21.3.x and classified as problematic. This issue affects some unknown processing of the component Pipeline Comparison Error Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-29183. 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-2022-29425	Wham Checkout Files Upload for WooCommerce Plugin up to 2.1.2 on WordPress cross-site scripting	A vulnerability was found in Wham Checkout Files Upload for WooCommerce Plugin up to 2.1.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-29425. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2021-36833	ibericode MC4WP Plugin up to 4.8.6 on WordPress cross-site scripting	A vulnerability was found in ibericode MC4WP Plugin up to 4.8.6 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-2021-36833. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-29430	KubiQ PNG to JPG Plugin up to 4.0 on WordPress jpg_quality cross-site scripting	A vulnerability has been found in KubiQ PNG to JPG Plugin up to 4.0 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument jpg_quality leads to cross-site scripting. This vulnerability was named CVE-2022-29430. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-29426	2J Image Slider Plugin up to 1.3.54 on WordPress cross-site scripting	A vulnerability was found in 2J Image Slider Plugin up to 1.3.54. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-29426. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-29424	Biplob Adhikari Image Hover Effects Ultimate Plugin up to 9.7.1 on WordPress cross-site scripting	A vulnerability was found in Biplob Adhikari Image Hover Effects Ultimate Plugin up to 9.7.1. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-29424. 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-2022-29428	Muneeb WP Slider Plugin up to 1.4.5 on WordPress cross-site scripting	A vulnerability classified as problematic has been found in Muneeb WP Slider Plugin up to 1.4.5. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-29428. 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-2022-29432	TMS-Plugins wpDataTables Plugin up to 2.1.27 on WordPress cross-site scripting	A vulnerability, which was classified as problematic, has been found in TMS-Plugins wpDataTables Plugin up to 2.1.27. Affected by this issue is some unknown functionality. The manipulation of the argument data-link-text/data-link-url/data/data-shortcode/data-star-num leads to cross-site scripting. This vulnerability is handled as CVE-2022-29432. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1816	Zoo Management System 1.0 Content Module view_accounts admin_name cross-site scripting	A vulnerability, which was classified as problematic, has been found in Zoo Management System 1.0. Affected by this issue is some unknown functionality of the file /zoo/admin/public_html/view_accounts?type=zookeeper of the component Content Module. The manipulation of the argument admin_name with the input <script>alert(1)</script> leads to cross-site scripting. This vulnerability is handled as CVE-2022-1816. The attack may be launched remotely. Furthermore, there is an exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1268	Donate Extra Plugin up to 2.02 on WordPress cross-site scripting	A vulnerability, which was classified as problematic, has been found in Donate Extra Plugin up to 2.02. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1268. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1817	Badminton Center Management System Userlist Module username cross-site scripting	A vulnerability, which was classified as problematic, was found in Badminton Center Management System. This affects an unknown part of the file /bcms/admin/?page=user/list of the component Userlist Module. The manipulation of the argument username with the input </td><img src="" onerror="alert(1)"><td>1 leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1817. 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-2022-1093	WP Meta SEO Plugin up to 4.4.6 on WordPress Breadcrumb Separator cross-site scripting	A vulnerability was found in WP Meta SEO Plugin up to 4.4.6. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Breadcrumb Separator Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-1093. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-0346	XML Sitemap Generator for Google Plugin up to 2.0.3 on WordPress Error Message cross-site scripting	A vulnerability has been found in XML Sitemap Generator for Google Plugin up to 2.0.3 and classified as problematic. This vulnerability affects unknown code of the component Error Message Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-0346. 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-2022-1221	Gwyn's Imagemap Selector Plugin up to 0.3.3 on WordPress Attribute cross-site scripting	A vulnerability classified as problematic was found in Gwyn's Imagemap Selector Plugin up to 0.3.3. This vulnerability affects unknown code of the component Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-1221. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1218	Domain Replace Plugin up to 1.3.8 on WordPress Admin Page cross-site scripting	A vulnerability classified as problematic has been found in Domain Replace Plugin up to 1.3.8. This affects an unknown part of the component Admin Page. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1218. 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-2022-1320	Sliderby10Web Plugin up to 1.2.51 on WordPress Setting cross-site scripting	A vulnerability has been found in Sliderby10Web Plugin up to 1.2.51 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-2022-1320. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1192	Turn Off All Comments Plugin up to 1.0 on WordPress Admin Page rows cross-site scripting	A vulnerability was found in Turn Off All Comments Plugin up to 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Admin Page. The manipulation of the argument rows leads to cross-site scripting. This vulnerability is handled as CVE-2022-1192. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1558	Curtain Plugin up to 1.0.2 on WordPress cross-site scripting	A vulnerability was found in Curtain Plugin up to 1.0.2. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1558. 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-2022-1825	collectiveaccess providence up to 1.7 cross-site scripting	A vulnerability, which was classified as problematic, was found in collectiveaccess providence up to 1.7. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1825. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1298	Tabs Plugin up to 2.2.7 on WordPress Tab Description cross-site scripting	A vulnerability, which was classified as problematic, was found in Tabs Plugin up to 2.2.7. Affected is an unknown function of the component Tab Description Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-1298. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1547	Check & Log Email Plugin up to 1.0.5 on WordPress Admin Page cross-site scripting	A vulnerability was found in Check & Log Email Plugin up to 1.0.5 and classified as problematic. Affected by this issue is some unknown functionality of the component Admin Page. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-1547. 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-2022-29005	Online Birth Certificate System 1.2 / obcs/user/profile.php fname/lname cross-site scripting	A vulnerability classified as problematic has been found in Online Birth Certificate System 1.2. Affected is an unknown function of the file /obcs/user/profile.php. The manipulation of the argument fname/lname leads to cross-site scripting. This vulnerability is traded as CVE-2022-29005. 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-2022-30017	SourceCodester Rescue Dispatch Management System 1.0 cross-site scripting	A vulnerability, which was classified as problematic, has been found in SourceCodester Rescue Dispatch Management System 1.0. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-30017. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1840	Home Clean Services Management System 1.0 register.php cross-site scripting	A vulnerability, which was classified as problematic, has been found in Home Clean Services Management System 1.0. This issue affects some unknown processing of the file register.php?link=register-and. The manipulation with the input <script>alert(1)</script> leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1840. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-42233	WonderCMS 3.4.1 Simple Blog Plugin cross-site scripting	A vulnerability was found in WonderCMS 3.4.1. It has been classified as problematic. Affected is an unknown function of the component Simple Blog Plugin. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2021-42233. 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-2022-1819	Student Information System 1.0 Student Roll Module admin/ cross-site scripting	A vulnerability, which was classified as problematic, was found in Student Information System 1.0. Affected is an unknown function of the file admin/?page=students of the component Student Roll Module. The manipulation with the input <script>alert(1)</script> leads to cross-site scripting. This vulnerability is traded as CVE-2022-1819. It is possible to launch the attack remotely. Furthermore, there is an exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2021-42656	SiteServer CMS 6.15.51 cross-site scripting (ID 3238)	A vulnerability was found in SiteServer CMS 6.15.51. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2021-42656. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-29004	Diary Management System 1.0 search-result.php Name cross-site scripting	A vulnerability has been found in Diary Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file search-result.php. The manipulation of the argument Name leads to cross-site scripting. This vulnerability is known as CVE-2022-29004. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-30456	Badminton Center Management System 1.0 Master.php cross-site scripting	A vulnerability, which was classified as problematic, has been found in Badminton Center Management System 1.0. This issue affects some unknown processing of the file /bcms/classes/Master.php?f=save_court_rental. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-30456. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-29362	ZKEACMS 3.5.2 create ParentID cross-site scripting (ID 457)	A vulnerability was found in ZKEACMS 3.5.2. It has been rated as problematic. This issue affects some unknown processing of the file /navigation/create?ParentID=%23. The manipulation of the argument ParentID leads to cross-site scripting. The identification of this vulnerability is CVE-2022-29362. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-30842	Covid-19 Travel Pass Management System 1.0 Users.php firstname cross-site scripting	A vulnerability was found in Covid-19 Travel Pass Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /ctpms/classes/Users.php?f=save. The manipulation of the argument firstname leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-30842. 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-2022-29408	Vsourz Digital Advanced Contact form 7 DB Plugin up to 1.8.7 on WordPress cross-site scripting	A vulnerability was found in Vsourz Digital Advanced Contact form 7 DB Plugin up to 1.8.7. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-29408. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1528	VikBooking Hotel Booking Engine & PMS Plugin up to 1.5.8 on WordPress URL cross-site scripting	A vulnerability was found in VikBooking Hotel Booking Engine & PMS Plugin up to 1.5.8 and classified as problematic. Affected by this issue is some unknown functionality of the component URL Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-1528. 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-2022-1527	WP 2FA Plugin up to 2.2.0 on WordPress Admin Page cross-site scripting	A vulnerability has been found in WP 2FA Plugin up to 2.2.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Admin Page. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-1527. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack
CVE-2022-1456	Poll Maker Plugin up to 4.0.1 on WordPress Setting cross-site scripting	A vulnerability, which was classified as problematic, was found in Poll Maker Plugin up to 4.0.1. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-1456. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Core Rules	Detected by scanner as cross-site scripting attack

5. Vulnerability Type: SQL Injection

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-27466	mingSoft MCMS 5.2.27 /dict/list.do orderBy SQL injection (ID 90)	A vulnerability, which was classified as critical, was found in mingSoft MCMS 5.2.27. Affected is an unknown function of the file /dict/list.do. The manipulation of the argument orderBy leads to SQL injection. This vulnerability is traded as CVE-2022-27466. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-1281	10Web Photo Gallery Plugin up to 1.6.3 on WordPress filter_tag SQL injection (ID 2706797)	A vulnerability, which was classified as critical, was found in 10Web Photo Gallery Plugin up to 1.6.3. This affects an unknown part. The manipulation of the argument filter_tag leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-1281. It is possible to initiate the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-0783	Multiple Shipping Address Woocommerce Plugin up to 1.x on WordPress SQL injection	A vulnerability was found in Multiple Shipping Address Woocommerce Plugin up to 1.x. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to SQL injection. This vulnerability was named CVE-2022-0783. 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 SQL injection attack
CVE-2022-0771	SiteSuperCharger Plugin up to 5.1.x on WordPress SQL injection	A vulnerability classified as critical has been found in SiteSuperCharger Plugin up to 5.1.x. Affected is an unknown function. The manipulation leads to SQL injection. This vulnerability is traded as CVE-2022-0771. 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 SQL injection attack
CVE-2022-0773	Documentor Plugin up to 1.5.3 on WordPress SQL injection	A vulnerability classified as critical was found in Documentor Plugin up to 1.5.3. Affected by this vulnerability is an unknown functionality. The manipulation leads to SQL injection. This vulnerability is known as CVE-2022-0773. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-27962	Bluecms 1.6 Cookie SQL injection	A vulnerability, which was classified as critical, was found in Bluecms 1.6. Affected is an unknown function of the component Cookie Handler. The manipulation leads to SQL injection. This vulnerability is traded as CVE-2022-27962. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-28505	jfinal_cms 5.1.0 com.jflyfox.system.log.LogController.java SQL injection (ID 33)	A vulnerability has been found in jfinal_cms 5.1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file com.jflyfox.system.log.LogController.java. The manipulation leads to SQL injection. This vulnerability is known as CVE-2022-28505. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-28585	EmpireCMS 7.5 AdClass.php SQL injection	A vulnerability, which was classified as critical, was found in EmpireCMS 7.5. Affected is an unknown function of the file AdClass.php. The manipulation leads to SQL injection. This vulnerability is traded as CVE-2022-28585. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-27413	Hospital Management System 1.0 admin.php adminname SQL injection	A vulnerability has been found in Hospital Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file admin.php. The manipulation of the argument adminname leads to SQL injection. This vulnerability was named CVE-2022-27413. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2021-42185	wdja 2.1 Foreground Search SQL injection (ID 12)	A vulnerability, which was classified as critical, was found in wdja 2.1. This affects an unknown part of the component Foreground Search. The manipulation leads to SQL injection. This vulnerability is uniquely identified as CVE-2021-42185. It is possible to initiate the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-28099	Poultry Farm Management System 1.0 / farm/store.php Item SQL injection	A vulnerability was found in Poultry Farm Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file / farm/store.php. The manipulation of the argument Item leads to SQL injection. This vulnerability is handled as CVE-2022-28099. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-28552	Cscms 4.1 Song Module SQL injection (ID 10)	A vulnerability classified as critical was found in Cscms 4.1. Affected by this vulnerability is an unknown functionality of the component Song Module. The manipulation leads to SQL injection. This vulnerability is known as CVE-2022-28552. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-27431	Wuzhicms 4.1.0 group.php groupid SQL injection (ID 200)	A vulnerability was found in Wuzhicms 4.1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /coreframe/app/member/admin/group.php. The manipulation of the argument groupid leads to SQL injection. This vulnerability is handled as CVE-2022-27431. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-27420	Hospital Management System 1.0 patientsearch.php patient_contact SQL injection (ID 19)	A vulnerability was found in Hospital Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file patientsearch.php. The manipulation of the argument patient_contact leads to SQL injection. This vulnerability is known as CVE-2022-27420. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-28512	Sourcecodester Fantastic Blog CMS 1.0 single.php id SQL injection	A vulnerability classified as critical was found in Sourcecodester Fantastic Blog CMS 1.0. This vulnerability affects unknown code of the file /fantasticblog/single.php. The manipulation of the argument id leads to SQL injection. This vulnerability was named CVE-2022-28512. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-28111	MyBatis PageHelper up to 5.x orderBy SQL injection	A vulnerability was found in MyBatis PageHelper up to 5.x. It has been declared as critical. This vulnerability affects unknown code. The manipulation of the argument orderBy leads to SQL injection. This vulnerability was named CVE-2022-28111. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-28461	mingyuefusu SQL injection	A vulnerability, which was classified as critical, was found in mingyuefusu. Affected is an unknown function. The manipulation leads to SQL injection. This vulnerability is traded as CVE-2022-28461. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-29938	LibreHealth EHR 2.0.0 GET Parameter new_payment.php payment_id SQL injection	A vulnerability was found in LibreHealth EHR 2.0.0. It has been rated as critical. This issue affects some unknown processing of the file interface\billing\new_payment.php of the component GET Parameter Handler. The manipulation of the argument payment_id leads to SQL injection. The identification of this vulnerability is CVE-2022-29938. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-27360	SpringBlade up to 3.2.0 customSqlSegment SQL injection	A vulnerability was found in SpringBlade up to 3.2.0 and classified as critical. Affected by this issue is some unknown functionality. The manipulation of the argument customSqlSegment leads to SQL injection. This vulnerability is handled as CVE-2022-27360. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-28079	College Management System 1.0 course_code SQL injection	A vulnerability was found in College Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation of the argument course_code leads to SQL injection. This vulnerability is handled as CVE-2022-28079. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30047	mingSoft MCMS 5.2.7 listExcludeApp orderBy SQL injection	A vulnerability was found in mingSoft MCMS 5.2.7. It has been declared as critical. This vulnerability affects unknown code of the file /mdiy/dict/listExcludeApp. The manipulation of the argument orderBy leads to SQL injection. This vulnerability was named CVE-2022-30047. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-29006	Directory Management System 1.0 username/password SQL injection (ID 50370 / EDB-50370)	A vulnerability was found in Directory Management System 1.0. It has been classified as critical. Affected is an unknown function. The manipulation of the argument username/password leads to SQL injection. This vulnerability is traded as CVE-2022-29006. The attack needs to be done within the local network. Furthermore, there is an exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30451	waimairenCMS up to 9.0 SQL injection	A vulnerability was found in waimairenCMS up to 9.0. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to SQL injection. This vulnerability was named CVE-2022-30451. 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 SQL injection attack
CVE-2022-30048	mingSoft MCMS 5.2.7 /mdiy/dict/list orderBy SQL injection	A vulnerability was found in mingSoft MCMS 5.2.7. It has been rated as critical. This issue affects some unknown processing of the file /mdiy/dict/list. The manipulation of the argument orderBy leads to SQL injection. The identification of this vulnerability is CVE-2022-30048. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-29306	IonizeCMS 1.0.8.1 article_model.php id_page SQL injection (ID 404)	A vulnerability was found in IonizeCMS 1.0.8.1. It has been declared as critical. This vulnerability affects unknown code of the file application/models/article_model.php. The manipulation of the argument id_page leads to SQL injection. This vulnerability was named CVE-2022-29306. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-29985	Online Sports Complex Booking System 1.0 Master.php SQL injection	A vulnerability has been found in Online Sports Complex Booking System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file \scbs\classes\Master.php?f=delete_category. The manipulation leads to SQL injection. This vulnerability is known as CVE-2022-29985. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-29979	Simple Client Management System 1.0 Master.php SQL injection	A vulnerability was found in Simple Client Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /cms/classes/Master.php?f=delete_designation. The manipulation leads to SQL injection. The identification of this vulnerability is CVE-2022-29979. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-29988	Online Sports Complex Booking System 1.0 Master.php SQL injection	A vulnerability classified as critical was found in Online Sports Complex Booking System 1.0. Affected by this vulnerability is an unknown functionality of the file \scbs\classes\Master.php?f=delete. The manipulation leads to SQL injection. This vulnerability is known as CVE-2022-29988. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-29741	Money Transfer Management System 1.0 Master.php SQL injection	A vulnerability was found in Money Transfer Management System 1.0. It has been classified as critical. Affected is an unknown function of the file \mtms\classes\Master.php?f=delete_fee. The manipulation leads to SQL injection. This vulnerability is traded as CVE-2022-29741. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-29999	Insurance Management System 1.0 editClient.php client_id SQL injection	A vulnerability classified as critical was found in Insurance Management System 1.0. This vulnerability affects unknown code of the file /insurance/editClient.php. The manipulation of the argument client_id leads to SQL injection. This vulnerability was named CVE-2022-29999. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30000	Insurance Management System 1.0 editPayment.php recipt_no SQL injection	A vulnerability, which was classified as critical, has been found in Insurance Management System 1.0. This issue affects some unknown processing of the file /insurance/editPayment.php. The manipulation of the argument recipt_no leads to SQL injection. The identification of this vulnerability is CVE-2022-30000. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-29993	Online Sports Complex Booking System 1.0 view_booking.php id SQL injection	A vulnerability was found in Online Sports Complex Booking System 1.0 and classified as critical. This issue affects some unknown processing of the file /scbs/admin/bookings/view_booking.php. The manipulation of the argument id leads to SQL injection. The identification of this vulnerability is CVE-2022-29993. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-29981	Simple Client Management System 1.0 Users.php SQL injection	A vulnerability classified as critical has been found in Simple Client Management System 1.0. Affected is an unknown function of the file /cms/classes/Users.php?f=delete. The manipulation leads to SQL injection. This vulnerability is traded as CVE-2022-29981. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-29749	Simple Client Management System 1.0 Master.php SQL injection	A vulnerability was found in Simple Client Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /cms/classes/Master.php?f=delete_invoice. The manipulation leads to SQL injection. This vulnerability is handled as CVE-2022-29749. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-29750	Simple Client Management System 1.0 Master.php SQL injection	A vulnerability was found in Simple Client Management System 1.0. It has been classified as critical. This affects an unknown part of the file /cms/classes/Master.php?f=delete_service. The manipulation leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-29750. It is possible to initiate the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-29751	Simple Client Management System 1.0 Master.php SQL injection	A vulnerability was found in Simple Client Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /cms/classes/Master.php?f=delete_client. The manipulation leads to SQL injection. This vulnerability was named CVE-2022-29751. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-29745	Money Transfer Management System 1.0 Master.php SQL injection	A vulnerability was found in Money Transfer Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file \mtms\classes\Master.php?f=delete_transaction. The manipulation leads to SQL injection. This vulnerability is known as CVE-2022-29745. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-29746	Money Transfer Management System 1.0 Users.php SQL injection	A vulnerability was found in Money Transfer Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /mtms/classes/Users.php?f=delete. The manipulation leads to SQL injection. This vulnerability is handled as CVE-2022-29746. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-29986	Booking Online Sports Complex Booking System 1.0 Master.php SQL injection	A vulnerability classified as critical has been found in Booking Online Sports Complex Booking System 1.0. Affected is an unknown function of the file \scbs\classes\Master.php?f=delete_facility. The manipulation leads to SQL injection. This vulnerability is traded as CVE-2022-29986. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-29998	Insurance Management System 1.0 clientStatus.php client_id SQL injection	A vulnerability classified as critical has been found in Insurance Management System 1.0. This affects an unknown part of the file /insurance/clientStatus.php. The manipulation of the argument client_id leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-29998. It is possible to initiate the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30002	Insurance Management System 1.0 editNominee.php nominee_id SQL injection	A vulnerability has been found in Insurance Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /insurance/editNominee.php. The manipulation of the argument nominee_id leads to SQL injection. This vulnerability is known as CVE-2022-30002. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30001	Insurance Management System 1.0 /insurance/editAgent.php agent_id SQL injection	A vulnerability, which was classified as critical, was found in Insurance Management System 1.0. Affected is an unknown function of the file /insurance/editAgent.php. The manipulation of the argument agent_id leads to SQL injection. This vulnerability is traded as CVE-2022-30001. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-29982	Simple Client Management System 1.0 manage_service.php id SQL injection	A vulnerability classified as critical was found in Simple Client Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /cms/admin/maintenance/manage_service.php. The manipulation of the argument id leads to SQL injection. This vulnerability is known as CVE-2022-29982. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-29989	Booking Online Sports Complex Booking System 1.0 Master.php SQL injection	A vulnerability, which was classified as critical, has been found in Booking Online Sports Complex Booking System 1.0. Affected by this issue is some unknown functionality of the file \scbs\classes\Master.php?f=delete_booking. The manipulation leads to SQL injection. This vulnerability is handled as CVE-2022-29989. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-29992	Online Sports Complex Booking System 1.0 manage_category.php id SQL injection	A vulnerability has been found in Online Sports Complex Booking System 1.0 and classified as critical. This vulnerability affects unknown code of the file /scbs/admin/categories/manage_category.php. The manipulation of the argument id leads to SQL injection. This vulnerability was named CVE-2022-29992. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30399	Merchandise Online Store 1.0 id SQL injection	A vulnerability, which was classified as critical, has been found in Merchandise Online Store 1.0. Affected by this issue is some unknown functionality of the file /vloggers_merch/admin/?page=-maintenance/manage_category. The manipulation of the argument id leads to SQL injection. This vulnerability is handled as CVE-2022-30399. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30373	Air Cargo Management System 1.0 manage_cargo_type.php id SQL injection	A vulnerability classified as critical has been found in Air Cargo Management System 1.0. This affects an unknown part of the file /acms/admin/cargo_types/manage_cargo_type.php. The manipulation of the argument id leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-30373. It is possible to initiate the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30385	Merchandise Online Store 1.0 Master.php SQL injection	A vulnerability, which was classified as critical, has been found in Merchandise Online Store 1.0. Affected by this issue is some unknown functionality of the file /vloggers_merch/classes/Master.php?f=delete_order. The manipulation leads to SQL injection. This vulnerability is handled as CVE-2022-30385. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-30401	Merchandise Online Store 1.0 id SQL injection	A vulnerability, which was classified as critical, was found in Merchandise Online Store 1.0. This affects an unknown part of the file /vloggers_merch/?p=view_product. The manipulation of the argument id leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-30401. It is possible to initiate the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30386	Merchandise Online Store 1.0 Master.php SQL injection	A vulnerability, which was classified as critical, was found in Merchandise Online Store 1.0. This affects an unknown part of the file /vloggers_merch/classes/Master.php?f=delete_featured. The manipulation leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-30386. It is possible to initiate the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30372	Air Cargo Management System 1.0 Master.php SQL injection	A vulnerability was found in Air Cargo Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /acms/classes/Master.php?f=delete_cargo. The manipulation leads to SQL injection. This vulnerability is handled as CVE-2022-30372. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30384	Merchandise Online Store 1.0 Master.php SQL injection	A vulnerability classified as critical was found in Merchandise Online Store 1.0. Affected by this vulnerability is an unknown functionality of the file /vloggers_merch/classes/Master.php?f=delete_inventory. The manipulation leads to SQL injection. This vulnerability is known as CVE-2022-30384. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30371	Air Cargo Management System 1.0 view_cargo_type.php id SQL injection	A vulnerability was found in Air Cargo Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /acms/admin/cargo_types/view_cargo_type.php. The manipulation of the argument id leads to SQL injection. This vulnerability is known as CVE-2022-30371. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-30374	Air Cargo Management System 1.0 id SQL injection	A vulnerability, which was classified as critical, has been found in Air Cargo Management System 1.0. This issue affects some unknown processing of the file /acms/admin/?page=transactions/manage_transaction. The manipulation of the argument id leads to SQL injection. The identification of this vulnerability is CVE-2022-30374. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30393	Merchandise Online Store 1.0 id SQL injection	A vulnerability was found in Merchandise Online Store 1.0. It has been rated as critical. This issue affects some unknown processing of the file /vloggers_merch/admin/?page=product/manage_product. The manipulation of the argument id leads to SQL injection. The identification of this vulnerability is CVE-2022-30393. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30398	Merchandise Online Store 1.0 id SQL injection	A vulnerability classified as critical was found in Merchandise Online Store 1.0. Affected by this vulnerability is an unknown functionality of the file /vloggers_merch/admin/?page=orders/view_order. The manipulation of the argument id leads to SQL injection. This vulnerability is known as CVE-2022-30398. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30417	Covid-19 Travel Pass Management System 1.0 id SQL injection	A vulnerability was found in Covid-19 Travel Pass Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file ctpms/admin/?page=user/manage_user. The manipulation of the argument id leads to SQL injection. This vulnerability is handled as CVE-2022-30417. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30414	Covid-19 Travel Pass Management System 1.0 id SQL injection	A vulnerability was found in Covid-19 Travel Pass Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /ctpms/admin/?page=applications/view_application. The manipulation of the argument id leads to SQL injection. This vulnerability is known as CVE-2022-30414. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-30370	Air Cargo Management System 1.0 Master.php SQL injection	A vulnerability was found in Air Cargo Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /acms/classes/Master.php?f=delete_cargo_type. The manipulation leads to SQL injection. This vulnerability is traded as CVE-2022-30370. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30376	Sourcecodester Simple Social Networking Site 1.0 view_member.php id SQL injection	A vulnerability was found in Sourcecodester Simple Social Networking Site 1.0. It has been rated as critical. This issue affects some unknown processing of the file /sns/admin/members/view_member.php. The manipulation of the argument id leads to SQL injection. The identification of this vulnerability is CVE-2022-30376. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-28530	NCDC Covid-19 Directory on Vaccination 1.0 cmdcategory SQL injection (ID 166481)	A vulnerability, which was classified as critical, has been found in NCDC Covid-19 Directory on Vaccination 1.0. This issue affects some unknown processing. The manipulation of the argument cmdcategory leads to SQL injection. The identification of this vulnerability is CVE-2022-28530. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-28080	Royal Event Management System 1.0 todate SQL injection	A vulnerability classified as critical has been found in Royal Event Management System 1.0. This affects an unknown part. The manipulation of the argument todate leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-28080. It is possible to initiate the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-28533	SourceCodester Medical Hub Directory Site 1.0 view_details.php SQL injection (ID 166539)	A vulnerability, which was classified as critical, was found in SourceCodester Medical Hub Directory Site 1.0. Affected is an unknown function of the file /mhds/clinic/view_details.php. The manipulation leads to SQL injection. This vulnerability is traded as CVE-2022-28533. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2020-19213	Piwigo 2.9.5 cat_move.php move_categories selection SQL injection (ID 1010)	A vulnerability was found in Piwigo 2.9.5 and classified as critical. This issue affects the function move_categories of the file cat_move.php. The manipulation of the argument selection leads to SQL injection. The identification of this vulnerability is CVE-2020-19213. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2020-19217	Piwigo 2.9.5 admin/batch_manager.php filter_category SQL injection (ID 1012)	A vulnerability was found in Piwigo 2.9.5. It has been rated as critical. Affected by this issue is some unknown functionality of the file admin/batch_manager.php. The manipulation of the argument filter_category leads to SQL injection. This vulnerability is handled as CVE-2020-19217. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2020-19216	Piwigo 2.9.5 admin/user_perm.php cat_false SQL injection (ID 1011)	A vulnerability was found in Piwigo 2.9.5. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file admin/user_perm.php. The manipulation of the argument cat_false leads to SQL injection. This vulnerability is known as CVE-2020-19216. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2020-19212	Piwigo 2.9.5 admin/group_list.php group SQL injection (ID 1009)	A vulnerability has been found in Piwigo 2.9.5 and classified as critical. This vulnerability affects unknown code of the file admin/group_list.php. The manipulation of the argument group leads to SQL injection. This vulnerability was named CVE-2020-19212. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-0592	MapSVG Plugin up to 6.2.19 on WordPress REST Endpoint SQL injection	A vulnerability was found in MapSVG Plugin up to 6.2.19. It has been rated as critical. This issue affects some unknown processing of the component REST Endpoint. The manipulation leads to SQL injection. The identification of this vulnerability is CVE-2022-0592. 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 SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-0826	WP Video Gallery Plugin up to 1.7.1 on WordPress SQL injection	A vulnerability classified as critical was found in WP Video Gallery Plugin up to 1.7.1. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-0826. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-0817	BadgeOS Plugin up to 3.7.0 on WordPress SQL injection	A vulnerability classified as critical has been found in BadgeOS Plugin up to 3.7.0. Affected is an unknown function. The manipulation leads to SQL injection. This vulnerability is traded as CVE-2022-0817. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-0948	Order Listener for WooCommerce Plugin up to 3.2.1 on WordPress id SQL injection (ID 2707223)	A vulnerability was found in Order Listener for WooCommerce Plugin up to 3.2.1. It has been classified as critical. This affects an unknown part. The manipulation of the argument id leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-0948. 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 SQL injection attack
CVE-2022-1013	Personal Dictionary Plugin up to 1.3.3 on WordPress SQL injection	A vulnerability, which was classified as critical, was found in Personal Dictionary Plugin up to 1.3.3. This affects an unknown part. The manipulation leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-1013. 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 SQL injection attack
CVE-2022-0836	SEMA API Plugin up to 3.64 on WordPress AJAX Action SQL injection	A vulnerability, which was classified as critical, has been found in SEMA API Plugin up to 3.64. Affected by this issue is some unknown functionality of the component AJAX Action Handler. The manipulation leads to SQL injection. This vulnerability is handled as CVE-2022-0836. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-28110	Hotel Management System 1.0 Login Page username SQL injection	A vulnerability, which was classified as critical, was found in Hotel Management System 1.0. This affects an unknown part of the component Login Page. The manipulation of the argument username leads to sql injection. This vulnerability is uniquely identified as CVE-2022-28110. It is possible to initiate the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-0814	Ubigeo de Perú para Woocommerce Plugin up to 3.6.3 on WordPress AJAX Action SQL injection	A vulnerability has been found in Ubigeo de Perú para Woocommerce Plugin up to 3.6.3 and classified as critical. Affected by this vulnerability is an unknown functionality of the component AJAX Action Handler. The manipulation leads to SQL injection. This vulnerability is known as CVE-2022-0814. 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 SQL injection attack
CVE-2022-27412	Explore CMS 1.0 /page.php id SQL injection (ID 166694)	A vulnerability was found in Explore CMS 1.0. It has been rated as critical. This issue affects some unknown processing of the file /page.php. The manipulation of the argument id leads to SQL injection. The identification of this vulnerability is CVE-2022-27412. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30452	Shopwind up to 3.4.2 Database.php SQL injection	A vulnerability, which was classified as critical, was found in Shopwind up to 3.4.2. Affected is an unknown function of the file Database.php. The manipulation leads to SQL injection. This vulnerability is traded as CVE-2022-30452. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30449	Hospital Management System in PHP 1.0 room.php editid SQL injection	A vulnerability classified as critical was found in Hospital Management System in PHP 1.0. Affected by this vulnerability is an unknown functionality of the file room.php. The manipulation of the argument editid leads to SQL injection. This vulnerability is known as CVE-2022-30449. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-29007	PHPGurukul Dairy Farm Shop Management System 1.0 Admin Panel username/password SQL injection (ID 50365 / EDB-50365)	A vulnerability was found in PHPGurukul Dairy Farm Shop Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Admin Panel. The manipulation of the argument username/password leads to SQL injection. This vulnerability is known as CVE-2022-29007. The attack needs to be initiated within the local network. Furthermore, there is an exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-29009	Cyber Cafe Management System Project 1.0 username/password SQL injection (ID 50355 / EDB-50355)	A vulnerability classified as critical has been found in Cyber Cafe Management System Project 1.0. This affects an unknown part. The manipulation of the argument username/password leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-29009. Access to the local network is required for this attack to succeed. Furthermore, there is an exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30407	Pharmacy Sales and Inventory System 1.0 manage_user.php id SQL injection	A vulnerability classified as critical was found in Pharmacy Sales and Inventory System 1.0. This vulnerability affects unknown code of the file /pharmacy-sales-and-inventory-system/manage_user.php. The manipulation of the argument id leads to SQL injection. This vulnerability was named CVE-2022-30407. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30395	Merchandise Online Store 1.0 Master.php SQL injection	A vulnerability was found in Merchandise Online Store 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /vloggers_merch/classes/Master.php?f=delete_cart. The manipulation leads to SQL injection. This vulnerability is known as CVE-2022-30395. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30387	Merchandise Online Store 1.0 Master.php SQL injection	A vulnerability has been found in Merchandise Online Store 1.0 and classified as critical. This vulnerability affects unknown code of the file /vloggers_merch/classes/Master.php?f=pay_order. The manipulation leads to SQL injection. This vulnerability was named CVE-2022-30387. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-30404	College Management System 1.0 display-teacher.php teacher_id SQL injection	A vulnerability classified as critical has been found in College Management System 1.0. This affects an unknown part of the file /College_Management_System/admin/display-teacher.php. The manipulation of the argument teacher_id leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-30404. It is possible to initiate the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30392	Merchandise Online Store 1.0 Master.php SQL injection	A vulnerability was found in Merchandise Online Store 1.0. It has been classified as critical. Affected is an unknown function of the file /vloggers_merch/classes/Master.php?f=delete_sub_category. The manipulation leads to SQL injection. This vulnerability is traded as CVE-2022-30392. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2021-41965	ChurchCRM up to 4.4.5 Edit EN_tyid/theID/EID SQL injection	A vulnerability, which was classified as critical, was found in ChurchCRM up to 4.4.5. Affected is an unknown function of the component Edit Handler. The manipulation of the argument EN_tyid/theID/EID leads to SQL injection. This vulnerability is traded as CVE-2021-41965. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-28930	ERP-Pro 3.7.5 SysEveMenuAuthPointMapper.xml SQL injection	A vulnerability was found in ERP-Pro 3.7.5 and classified as critical. Affected by this issue is some unknown functionality of the file /base/SysEveMenuAuthPointMapper.xml. The manipulation leads to SQL injection. This vulnerability is handled as CVE-2022-28930. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-1182	Visual Slide Box Builder Plugin up to 3.2.9 on WordPress SQL injection	A vulnerability was found in Visual Slide Box Builder Plugin up to 3.2.9. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to SQL injection. This vulnerability is known as CVE-2022-1182. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-30012	HMS 1.0 POST Request appointment.php SQL injection	A vulnerability has been found in HMS 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file appointment.php of the component POST Request Handler. The manipulation leads to SQL injection. This vulnerability is known as CVE-2022-30012. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-28929	Hospital Management System 1.0 viewtreatmentrecord.php delid SQL injection	A vulnerability has been found in Hospital Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file viewtreatmentrecord.php. The manipulation of the argument delid leads to SQL injection. This vulnerability is known as CVE-2022-28929. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-0867	Pricing Table Plugin up to 3.6.0 on WordPress SQL injection	A vulnerability was found in Pricing Table Plugin up to 3.6.0. It has been classified as critical. Affected is an unknown function. The manipulation leads to SQL injection. This vulnerability is traded as CVE-2022-0867. 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 SQL injection attack
CVE-2022-30011	HMS up to 1.0 appointment.php SQL injection	A vulnerability, which was classified as critical, was found in HMS up to 1.0. Affected is an unknown function of the file appointment.php. The manipulation leads to SQL injection. This vulnerability is traded as CVE-2022-30011. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-24391	Fidelis Network and Deception up to 9.4.4 Web Interface SQL injection	A vulnerability was found in Fidelis Network and Deception up to 9.4.4. It has been classified as critical. Affected is an unknown function of the component Web Interface. The manipulation leads to SQL injection. This vulnerability is traded as CVE-2022-24391. 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 SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-30054	Covid 19 Travel Pass Management 1.0 code SQL injection	A vulnerability has been found in Covid 19 Travel Pass Management 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation of the argument code leads to SQL injection. This vulnerability is known as CVE-2022-30054. The attack can be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30053	Toll Tax Management System 1.0 id SQL injection	A vulnerability, which was classified as critical, was found in Toll Tax Management System 1.0. Affected is an unknown function. The manipulation of the argument id leads to SQL injection. This vulnerability is traded as CVE-2022-30053. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30052	Home Clean Service System 1.0 password SQL injection	A vulnerability, which was classified as critical, has been found in Home Clean Service System 1.0. This issue affects some unknown processing. The manipulation of the argument password leads to SQL injection. The identification of this vulnerability is CVE-2022-30052. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-28962	Online Sports Complex Booking System 1.0 Users.php SQL injection (ID 166598)	A vulnerability, which was classified as critical, has been found in Online Sports Complex Booking System 1.0. Affected by this issue is some unknown functionality of the file /scbs/classes/Users.php?f=delete_client. The manipulation leads to SQL injection. This vulnerability is handled as CVE-2022-28962. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2021-37413	GRANDCOM DynWEB up to 4.1 Admin Login Interface SQL injection	A vulnerability classified as critical has been found in GRANDCOM DynWEB up to 4.1. Affected is an unknown function of the component Admin Login Interface. The manipulation leads to SQL injection. This vulnerability is traded as CVE-2021-37413. 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 SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-28105	Online Sports Complex Booking System 1.0 / scbs/view_facility.php id SQL injection	A vulnerability was found in Online Sports Complex Booking System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /scbs/view_facility.php. The manipulation of the argument id leads to SQL injection. This vulnerability is handled as CVE-2022-28105. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-26632	Multi-Vendor Online Groceries Management System 1.0 view_product.php id SQL injection (ID 50739 / EDB-50739)	A vulnerability, which was classified as critical, was found in Multi-Vendor Online Groceries Management System 1.0. Affected is an unknown function of the file /products/view_product.php. The manipulation of the argument id leads to SQL injection. This vulnerability is traded as CVE-2022-26632. It is possible to launch the attack remotely. Furthermore, there is an exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30886	School Dormitory Management System 1.0 daily_collection_report.php month SQL injection (ID 167001)	A vulnerability, which was classified as critical, has been found in School Dormitory Management System 1.0. This issue affects some unknown processing of the file /dms/admin/reports/daily_collection_report.php. The manipulation of the argument month leads to SQL injection. The identification of this vulnerability is CVE-2022-30886. The attack may be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-28961	SPIP up to 3.1.13 / ecrire lier_trad/ where SQL injection	A vulnerability, which was classified as critical, was found in SPIP up to 3.1.13. This affects an unknown part of the file /ecrire. The manipulation of the argument lier_trad/where leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-28961. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-29652	Online Sports Complex Booking System 1.0 Users.php SQL injection (ID 166641)	A vulnerability has been found in Online Sports Complex Booking System 1.0 and classified as critical. This vulnerability affects unknown code of the file /scbs/classes/Users.php?f=save_client. The manipulation leads to SQL injection. This vulnerability was named CVE-2022-29652. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-29304	Online Sports Complex Booking System 1.0 master.php delete_facility SQL injection	A vulnerability, which was classified as critical, was found in Online Sports Complex Booking System 1.0. This affects the function delete_facility of the file /classes/master.php?f=delete_facility. The manipulation leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-29304. It is possible to initiate the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-28531	Sourcecodester Covid-19 Directory on Vaccination 1.0 admin/login.php txtusername SQL injection (ID 166481)	A vulnerability, which was classified as critical, was found in Sourcecodester Covid-19 Directory on Vaccination 1.0. This affects an unknown part of the file admin/login.php. The manipulation of the argument txtusername leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-28531. It is possible to initiate the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-1014	WP Contacts Manager Plugin up to 2.2.4 on WordPress SQL injection	A vulnerability was found in WP Contacts Manager Plugin up to 2.2.4. It has been classified as critical. Affected is an unknown function. The manipulation leads to SQL injection. This vulnerability is traded as CVE-2022-1014. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-0781	Nirweb Support Plugin up to 2.8.1 on WordPress SQL injection	A vulnerability was found in Nirweb Support Plugin up to 2.8.1 and classified as critical. This issue affects some unknown processing. The manipulation leads to SQL injection. The identification of this vulnerability is CVE-2022-0781. 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 SQL injection attack
CVE-2022-30454	Merchandise Online Store 1.0 Master.php SQL injection	A vulnerability classified as critical has been found in Merchandise Online Store 1.0. This affects an unknown part of the file /vloggers_merch/classes/Master.php?f=delete_product. The manipulation leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-30454. It is possible to initiate the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31487	Inout Blockchain AltExchanger master.php symbol SQL injection	A vulnerability was found in Inout Blockchain AltExchanger and Inout Blockchain FiatExchanger and classified as critical. Affected by this issue is some unknown functionality of the file Chart/TradingView/chart_content/master.php. The manipulation of the argument symbol leads to SQL injection. This vulnerability is handled as CVE-2022-31487. The attack may be launched remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-1839	Home Clean Services Management System 1.0 login.php email SQL injection	A vulnerability classified as critical was found in Home Clean Services Management System 1.0. This vulnerability affects unknown code of the file login.php. The manipulation of the argument email with the input admin%'/**/AND/**/(SELECT/**/5383/**/FROM/**/(SELECT(SLEEP(2)))JPeh)/**/AND/**/'-frfq%'='frfq leads to SQL injection. This vulnerability was named CVE-2022-1839. The attack can be initiated remotely. Furthermore, there is an exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2021-42655	SiteServer CMS 6.15.51 SQL injection (ID 3237)	A vulnerability was found in SiteServer CMS 6.15.51. It has been classified as critical. This affects an unknown part. The manipulation leads to SQL injection. This vulnerability is uniquely identified as CVE-2021-42655. It is possible to initiate the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-1838	Home Clean Services Management System 1.0 admin/login.php username SQL injection	A vulnerability classified as critical has been found in Home Clean Services Management System 1.0. This affects an unknown part of the file admin/login.php. The manipulation of the argument username with the input admin%'/**/AND/**/(SELECT/**/5383/**/FROM/**/(SELECT(SLEEP(5)))JPeh)/**/AND/**/'-frfq%'='frfq leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-1838. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-30455	Badminton Center Management System 1.0 Master.php SQL injection	A vulnerability classified as critical was found in Badminton Center Management System 1.0. This vulnerability affects unknown code of the file /bcms/classes/Master.php?f=delete_court_rental. The manipulation leads to SQL injection. This vulnerability was named CVE-2022-30455. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-29305	imgurl 2.31 / upload/localhost SQL injection (ID 75)	A vulnerability was found in imgurl 2.31 and classified as critical. Affected by this issue is some unknown functionality of the file / upload/localhost. The manipulation leads to SQL injection. This vulnerability is handled as CVE-2022-29305. The attack needs to be approached within the local network. Furthermore, there is an exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-30461	water-billing-management-system 1.0 Master.php id SQL injection	A vulnerability classified as critical was found in water-billing-management-system 1.0. Affected by this vulnerability is an unknown functionality of the file / wbms/classes/Master.php?f=delete_client. The manipulation of the argument id leads to SQL injection. This vulnerability is known as CVE-2022-30461. The attack can be launched remotely. Furthermore, there is an exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-1883	camptocamp terraboard up to 2.1.x SQL injection	A vulnerability, which was classified as critical, was found in camptocamp terraboard up to 2.1.x. This affects an unknown part. The manipulation leads to SQL injection. This vulnerability is uniquely identified as CVE-2022-1883. 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 SQL injection attack
CVE-2022-28862	ARCHIBUS Web Central up to 26.1 workflow.runWorkflowRule.dwr SQL injection	A vulnerability was found in ARCHIBUS Web Central up to 26.1 and classified as critical. This issue affects some unknown processing of the file dwr/call/plaincall/workflow.runWorkflowRule.dwr. The manipulation leads to SQL injection. The identification of this vulnerability is CVE-2022-28862. 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 SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-29650	Online Food Ordering System 1.0 food-search.php Search SQL injection	A vulnerability has been found in Online Food Ordering System 1.0 and classified as critical. This vulnerability affects unknown code of the file /online-food-order/food-search.php. The manipulation of the argument Search leads to SQL injection. This vulnerability was named CVE-2022-29650. The attack can be initiated remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-29667	CSCMS Music Portal System 4.2 Photo hy SQL injection (ID 26)	A vulnerability, which was classified as critical, was found in CSCMS Music Portal System 4.2. Affected is an unknown function of the file /admin.php/pic/admin/pic/hy of the component Photo Handler. The manipulation leads to SQL injection. This vulnerability is traded as CVE-2022-29667. It is possible to launch the attack remotely. There is no exploit available.	Protected by Core Rules	Detected by the scanner as SQL injection attack
CVE-2022-1556	STAFFLIST PLUGIN UP TO 3.1.4 ON WORDPRESS ADMIN DASHBOARD SQL INJECTION	A vulnerability, which was classified as critical, has been found in StaffList Plugin up to 3.1.4. Affected by this issue is some unknown functionality of the component Admin Dashboard. The manipulation leads to SQL injection. This vulnerability is handled as CVE-2022-1556. 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 SQL injection 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

Gartner Peer Insights Customers' Choice 2022™

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.