INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

October 2022

Total No. of Zero-Day Vulnerabilities Found: 193

Command Injection	Local File Inclusion	SQL Injection	Malicious File Upload	Cross-Site Scripting	Cross-Site Request Forgery
7	15	65	13	74	19

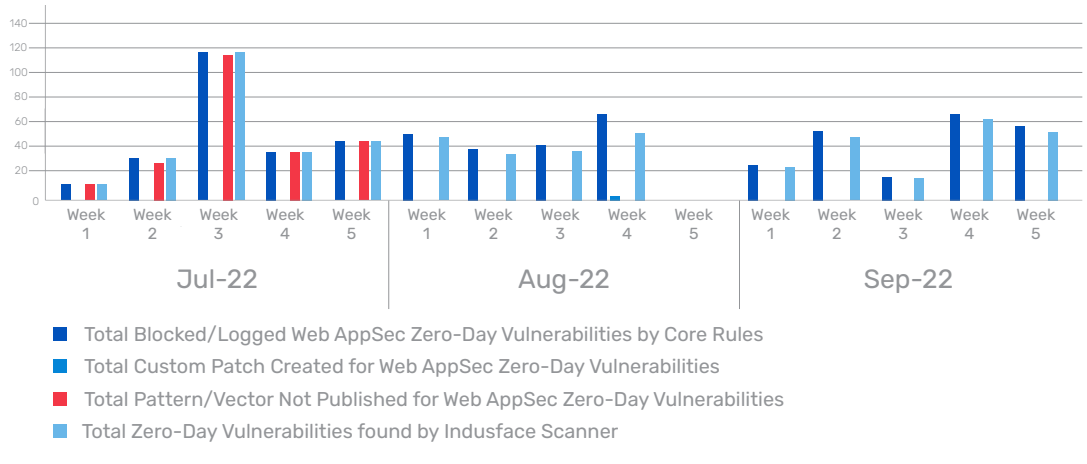
Zero-day vulnerabilities protected through core rules	180
Zero-day vulnerabilities protected through custom rules	13
Zero-day vulnerabilities for which protection can not be done	0
Zero-day vulnerabilities found by Indusface WAS	161

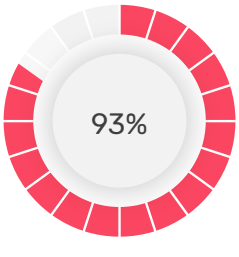
- To enable custom rules, please contact support@indusface.com
- Since the attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.

Vulnerability Trend:

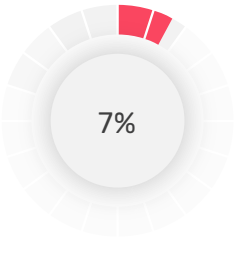
The weekly trend displays the total number of vulnerabilities discovered to the type of protection provided for the last quarter.

Weekly Vulnerability Trend

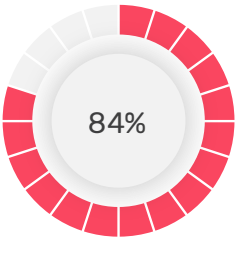




of the zero-day vulnerabilities were protected by the **core rules** in the last month.

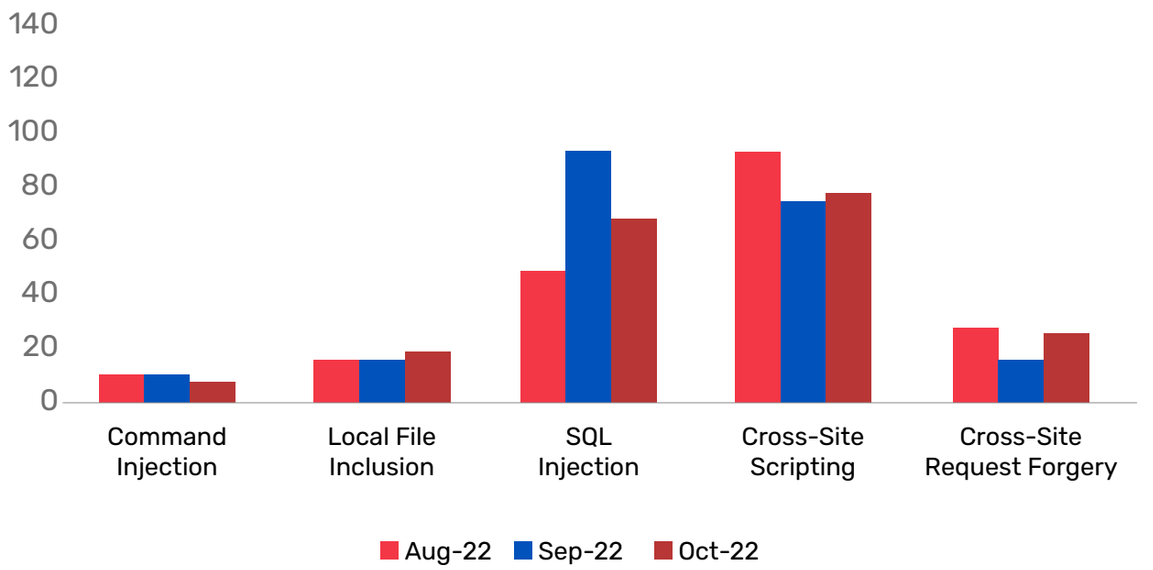


of the zero-day vulnerabilities were protected by the **custom rules** in the last month.



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

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-41443	phpipam 1.5.0 Header ripe-query.php injection	A vulnerability was found in phpipam 1.5.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/subnets/ripe-query.php of the component Header Handler. The manipulation leads to injection. This vulnerability was named CVE-2022-41443. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command injection attack
CVE-2022-41518	TOTOLINK NR1800X 9.1.0u.6279_B20210910 /cgibin/cstecgi.cgi UploadFirmwareFile command injection	A vulnerability was found in TOTOLINK NR1800X 9.1.0u.6279_B20210910. It has been rated as critical. This issue affects the function UploadFirmwareFile of the file /cgi-bin/cstecgi.cgi. The manipulation leads to command injection. The identification of this vulnerability is CVE-2022-41518. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command injection attack
CVE-2022-41525	TOTOLINK NR1800X 9.1.0u.6279_B20210910 /cgibin/cstecgi.cgi OpModeCfg command injection	A vulnerability was found in TOTOLINK NR1800X 9.1.0u.6279_B20210910 and classified as critical. This issue affects the function OpModeCfg of the file /cgibin/cstecgi.cgi. The manipulation leads to command injection. The identification of this vulnerability is CVE-2022-41525. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-35132	Usermin up to 1.850 GPG Module os command injection	A vulnerability was found in Usermin up to 1.850 and classified as critical. This issue affects some unknown processing of the component GPG Module. The manipulation leads to os command injection. The identification of this vulnerability is CVE-2022-35132. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-42055	GL.iNet GoodCloud IoT Device Management System 1.00.220412.00 Ping/Traceroute command injection	A vulnerability which was classified as problematic has been found in GL.iNet GoodCloud IoT Device Management System 1.00.220412.00. This issue affects some unknown processing of the component Ping/Traceroute. The manipulation leads to command injection. The identification of this vulnerability is CVE-2022-42055. 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 command injection attack
CVE-2022-31898	gl-inet GL-MT300N-V2 Mango/GLAX1800 Flint ping_addr/trace_addr command injection	A vulnerability was found in gl-inet GL-MT300N-V2 Mango and GL-AX1800 Flint and classified as critical. Affected by this issue is some unknown functionality. The manipulation of the argument ping_addr/trace_addr leads to command injection. This vulnerability is handled as CVE-2022-31898. The attack can only be initiated within the local network. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-44019	total.js Metacharacter /api/common/ping host os command injection (ID 12 / 0e5ace7)	A vulnerability has been found in total.js and classified as critical. This vulnerability affects unknown code of the file /api/common/ping of the component Metacharacter Handler. The manipulation of the argument host leads to os command injection. This vulnerability was named CVE-2022-44019. 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 the scanner as command injection attack

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2839	Zephyr Project Manager Plugin up to 3.2.54 on WordPress AJAX Action cross-site request forgery	A vulnerability classified as problematic was found in Zephyr Project Manager Plugin up to 3.2.54. Affected by this vulnerability is an unknown functionality of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-2839. 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 crosssite request forgery attack.
CVE-2022-39290	ZoneMinder HTTP GET Request crosssite request forgery (GHSA-xgv6-qv6c399q)	A vulnerability classified as problematic was found in ZoneMinder. This vulnerability affects unknown code of the component HTTP GET Request Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-39290. 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 crosssite request forgery attack.
CVE-2022-3154	Woo Billingo Plus Plugin on WordPress AJAX Action Szamlazz.hu cross-site request forgery	A vulnerability which was classified as problematic was found in Woo Billingo Plus Plugin Integration for Billingo & Gravity Forms Plugin and Integration for Szamlazz.hu & Gravity Forms Plugin. Affected is an unknown function of the file Szamlazz.hu of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-3154. 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 crosssite request forgery attack.
CVE-2022-3208	Simple File List Plugin up to 4.4.11 on WordPress cross-site request forgery	A vulnerability was found in Simple File List Plugin up to 4.4.11 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-3208. 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 crosssite request forgery attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-42087	Tenda AX1803 US_AX1803v2.0br_ v1.0.0.1_2994_CN_ ZGYD01_4 fromSys-ToolReboot crosssite request forgery	A vulnerability was found in Tenda AX1803 US_AX1803v2.0br_ v1.0.0.1_2994_CN_ ZGYD01_4. It has been rated as problematic. Affected by this issue is the function fromSysTool-Reboot. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-42087. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as crosssite request forgery attack.
CVE-2022-34020	ResIOT IOT Platform/ LoRaWAN Net-work Server up to 4.1.1000114 cross-site request forgery	A vulnerability classi-fied as problematic has been found in ResIOT IOT Platform and LoRaWAN Network Server up to 4.1.1000114. This affects an unknown part. The manip-ulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-34020. It is possible to initiate the attack re-motely. There is no exploit available.	Protected by core rules	Detected by scanner as crosssite request forgery attack.
CVE-2022-42078	Tenda fromSysTool-RestoreSet crosssite request forgery	A vulnerability was found in Tenda US_AC1206V1.0RTL_ V15.03.06.23_multi_TD01. It has been classified as problematic. Affected is the function fromSysTool-RestoreSet. The manipu-lation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-42078. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as crosssite request forgery attack.
CVE-2022-41475	RPCMS 3.0.2 cross-site request forgery	A vulnerability which was classified as problematic was found in RPCMS 3.0.2. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-41475. It is possible to initiate the attack re-motely. There is no exploit available.	Protected by core rules	Detected by scanner as crosssite request forgery attack.
CVE-2022-41489	WAYOS LQ_09 22.03.17V Usb_up-load.htm cross-site request forgery	A vulnerability classified as problematic has been found in WAYOS LQ_09 22.03.17V. Affected is an unknown function of the file Usb_upload.htm. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-41489. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as crosssite request forgery attack.
CVE-2022-41474	RPCMS 3.0.2 cross-site request forgery	A vulnerability which was classified as problematic has been found in RPCMS 3.0.2. Affected by this issue is some unknown functionality. The manip-ulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-41474. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as crosssite request forgery attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-42077	Tenda AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01 fromSysToolReboot cross-site request forgery	A vulnerability was found in Tenda AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01 and classified as problematic. This issue affects the function fromSysToolReboot. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022-42077. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as crosssite request forgery attack.
CVE-2022-42086	Tenda AX1803 US_AX1803v2.0br_v1.0.0.1_2994_CN_ZGYD01_4 TendaAteMode cross-site request forgery	A vulnerability was found in Tenda AX1803 US_AX1803v2.0br_v1.0.0.1_2994_CN_ZGYD01_4. It has been declared as problematic. Affected by this vulnerability is the function TendaAteMode. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-42086. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as crosssite request forgery attack.
CVE-2022-42070	Online Birth Certificate Management System 1.0 cross-site request forgery (ID 168522)	A vulnerability which was classified as problematic has been found in Online Birth Certificate Management System 1.0. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-42070. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as crosssite request forgery attack.
CVE-2022-41500	EyouCMS 1.5.9 Members Center crosssite request forgery (ID 27)	A vulnerability was found in EyouCMS 1.5.9 and classified as problematic. Affected by this issue is some unknown functionality of the component Members Center/Editorial Membership/Points Recharge. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-41500. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as crosssite request forgery attack.
CVE-2022-42199	Simple Exam Reviewer Management System 1.0 Exam List cross-site request forgery	A vulnerability which was classified as problematic was found in Simple Exam Reviewer Management System 1.0. Affected is an unknown function of the component Exam List Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-42199. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as crosssite request forgery attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2762	AdminPad Plugin up to 2.1 on WordPress Note cross-site request forgery	A vulnerability which was classified as problematic has been found in AdminPad Plugin up to 2.1. Affected by this issue is some unknown functionality of the component Note Handler. The manipulation leads to crosssite request forgery. This vulnerability is handled as CVE-2022-2762. 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 crosssite request forgery attack.
CVE-2022-3097	LBStopAttack Plugin up to 1.1.2 on WordPress Setting cross-site request forgery	A vulnerability classified as problematic was found in LBStopAttack Plugin up to 1.1.2. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-3097. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as crosssite request forgery attack.
CVE-2022-43340	dzzoffice 2.02.1_SC_UTF8 cross-site request forgery (ID 223)	A vulnerability classified as problematic was found in dzzoffice 2.02.1_SC_UTF8. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-43340. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as crosssite request forgery attack.
CVE-2022-3419	Automatic User Roles Switcher Plugin up to 1.1.1 on WordPress cross-site	A vulnerability has been found in Automatic User Roles Switcher Plugin up to 1.1.1 and classified as problematic. This vulnerability affects unknown code.	Protected by core rules	Detected by scanner as crosssite request forgery attack.

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-40341	mojoPortal 2.7 PNG File unrestricted upload	A vulnerability was found in mojoPortal 2.7. It has been declared as critical. This vulnerability affects unknown code of the component PNG File Handler. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2022-40341. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-40123	mojoPortal 2.7 CssEditor.aspx f path traversal	A vulnerability was found in mojoPortal 2.7 and classified as problematic. This issue affects some unknown processing of the file /DesignTools/CssEditor.aspx. The manipulation of the argument f leads to path traversal. The identification of this vulnerability is CVE-2022-40123. The attack needs to be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-40721	CreativeDream PHP Uploader unrestricted upload (ID 23)	A vulnerability which was classified as critical has been found in CreativeDream PHP Uploader. This issue affects some unknown processing. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2022-40721. The attack can only be initiated within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-3125	Frontend File Manager Plugin up to 21.2 on WordPress unrestricted upload	A vulnerability classified as critical was found in Frontend File Manager Plugin up to 21.2. This vulnerability affects unknown code. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2022-3125. 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 Local File Inclusion Attack
CVE-2022-3389	ikus060 rdiffweb path traversal	A vulnerability has been found in ikus060 rdiffweb and classified as critical. This vulnerability affects unknown code. The manipulation leads to path traversal. This vulnerability was named CVE-2022-3389. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-41379	Online Leave Management System 1.0 Users.php unrestricted upload	A vulnerability was found in Online Leave Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /leave_system/classes/Users.phpfsave. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2022-41379. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-41512	Online Diagnostic Lab Management System 1.0 /php_action/editFile.php unrestricted upload	A vulnerability was found in Online Diagnostic Lab Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /php_action/editFile.php. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2022-41512. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-2554	Enable Media Replace Plugin up to 3.x on WordPress path traversal	A vulnerability was found in Enable Media Replace Plugin up to 3.x and classified as critical. This issue affects some unknown processing. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-2554. The attack needs to be initiated within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-42234	UCMS 1.6 Template Management Module file inclusion	A vulnerability was found in UCMS 1.6. It has been rated as critical. Affected by this issue is some unknown functionality of the component Template Management Module. The manipulation leads to file inclusion. This vulnerability is handled as CVE-2022-42234. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-41547	MobSF Mobile Security Framework up to 0.9.2 HTTP Request StaticAnalyzer/views.py file inclusion	A vulnerability classified as problematic was found in MobSF Mobile Security Framework up to 0.9.2. Affected by this vulnerability is an unknown functionality of the file StaticAnalyzer/views.py of the component HTTP Request Handler. The manipulation leads to file inclusion. This vulnerability is known as CVE-2022-41547. Access to the local network is required for this attack to succeed. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Local File Inclusion Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-42188	Lavalite 9.0.0 Cookie XSRFTOKEN path traversal	A vulnerability has been found in Lavalite 9.0.0 and classified as problematic. This vulnerability affects unknown code of the component Cookie Handler. The manipulation of the argument XSRF-TOKEN leads to path traversal. This vulnerability was named CVE-2022-42188. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-39345	Gin-Vue-Admin up to 2.5.3 File Upload path traversal (GHSA-7gc4-r5jr-9hxv)	A vulnerability classified as critical has been found in Gin-Vue-Admin up to 2.5.3. This affects an unknown part of the component File Upload Handler. The manipulation leads to relative path traversal. This vulnerability is uniquely identified as CVE-2022-39345. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-33897	Robustel R1510 3.1.16 Web Server /ajax/remove/ path traversal (TALOS-2022-1579)	A vulnerability was found in Robustel R1510 3.1.16. It has been classified as critical. Affected is an unknown function of the file /ajax/remove/ of the component Web Server. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-33897. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-0072	Litespeed Technologies OpenLiteSpeed up to 1.5.12/1.6.20.1/1.7.16.0 Web Server Dashboard path traversal	A vulnerability was found in Litespeed Technologies OpenLiteSpeed up to 1.5.12/1.6.20.1/1.7.16.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Web Server Dashboard. The manipulation leads to path traversal. This vulnerability is known as CVE-2022-0072. 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 Local File Inclusion Attack

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-41504	Billing System Project 1.0 editProductImage.php unrestricted upload	A vulnerability was found in Billing System Project 1.0 and classified as critical. This issue affects some unknown processing of the file/php_action/editProductImage.php. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2022-41504. The attack needs to be done within the local network. There is no exploit available.	Protected by Custom rules	NA
CVE-2022-41537	Online Tours & Travels Management System 1.0 profile.php unrestricted upload	A vulnerability classified as critical has been found in Online Tours & Travels Management System 1.0. This affects an unknown part of the file /user_operations/profile.php. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2022-41537. The attack needs to be done within the local network. There is no exploit available.	Protected by Custom rules	NA
CVE-2022-42198	Simple Exam Reviewer Management System 1.0 User List unrestricted upload	A vulnerability classified as critical was found in Simple Exam Reviewer Management System 1.0. This vulnerability affects unknown code of the component User List Handler. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2022-42198. The attack can only be initiated within the local network. There is no exploit available.	Protected by Custom rules	NA
CVE-2022-42201	Simple Exam Reviewer Management System 1.0 unrestricted upload	A vulnerability which was classified as critical has been found in Simple Exam Reviewer Management System 1.0. This issue affects some unknown processing. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2022-42201. The attack needs to be done within the local network. There is no exploit available.	Protected by Custom rules	NA
CVE-2022-42189	Emlog Pro 1.6.0 Plugin Upload unrestricted upload	A vulnerability was found in Emlog Pro 1.6.0 and classified as critical. This issue affects some unknown processing of the component Plugin Upload Handler. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2022-42189. The attack may be initiated remotely. There is no exploit available.	Protected by Custom rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-39305	Gin-vue-admin up to 2.5.3 fileMd5/fileName unrestricted upload (GHSA-wrmq-4v4c-gxp2)	A vulnerability was found in Gin-vue-admin up to 2.5.3 and classified as critical. Affected by this issue is some unknown functionality. The manipulation of the argument fileMd5/fileName leads to unrestricted upload. This vulnerability is handled as CVE-2022-39305. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by Custom rules	NA
CVE-2022-41711	Badaso 2.6.0 unrestricted upload (ID 802)	A vulnerability classified as critical was found in Badaso 2.6.0. Affected by this vulnerability is an unknown functionality. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2022-41711. The attack can be launched remotely. There is no exploit available.	Protected by Custom rules	NA
CVE-2022-43275	Canteen Management System 1.0 editProductImage.php unrestricted upload	A vulnerability was found in Canteen Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /youthappam/php_action/editProductImage.php. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2022-43275. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by Custom rules	NA
CVE-2022-39977	Online Pet Shop We App up to 1.0 User Module unrestricted upload	A vulnerability which was classified as critical was found in Online Pet Shop We App up to 1.0. This affects an unknown part of the component User Module. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2022-39977. Access to the local network is required for this attack. There is no exploit available.	Protected by Custom rules	NA
CVE-2022-39978	Online Pet Shop We App up to 1.0 List Module unrestricted upload	A vulnerability has been found in Online Pet Shop We App up to 1.0 and classified as critical. This vulnerability affects unknown code of the component List Module. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2022-39978. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by Custom rules	NA
CVE-2022-43231	Canteen Management System 1.0 manage_website.php unrestricted upload	A vulnerability classified as critical was found in Canteen Management System 1.0. This vulnerability affects unknown code of the file /youthappam/manage_website.php. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2022-43231. The attack can be initiated remotely. There is no exploit available.	Protected by Custom rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3770	Yunjing CMS upload_ img.html file unrestricted upload	A vulnerability classified as critical was found in Yunjing CMS. This vulnerability affects unknown code of the file /index/user/upload_img.html. The manipulation of the argument file leads to unrestricted upload. This vulnerability was named CVE-2022-3770. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by Custom rules	NA
CVE-2022-40471	Clinic Patient Management System 1.0 Profile Picture users. php unrestricted upload	A vulnerability was found in Clinic Patient Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file users.php of the component Profile Picture Handler. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2022-40471. The attack can be initiated remotely. There is no exploit available.	Protected by Custom rules	NA

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-35156	Bus Pass Management System 1.0 download-pass.php searchdata sql injection (ID 168555)	A vulnerability was found in Bus Pass Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file/buspassms/download-pass. php. The manipulation of the argument searchdata leads to sql injection. The identification of this vulnerability is CVE-2022-35156. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-41439	Billing System Project 1.0 edituser.php id sql injection	A vulnerability was found in Billing System Project 1.0. It has been classified as critical. This affects an unknown part of the file / phpinventory/edituser. php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-41439. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-41440	Billing System Project 1.0 editcategory.php id sql injection	A vulnerability was found in Billing System Project 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /phpinventory/editcategory.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-41440. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-40944	Dairy Farm Shop Management System 1.0 sales-report-ds. php sql injection	A vulnerability which was classified as critical has been found in Dairy Farm Shop Management System 1.0. Affected by this issue is some unknown functionality of the file sales-report-ds.php. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-40944. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-40943	Dairy Farm Shop Management System 1.0 bwdate-report-ds.php sql injection	A vulnerability classified as critical was found in Dairy Farm Shop Management System 1.0. Affected by this vulnerability is an unknown functionality of the file bwdate-report-ds.php. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-40943. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-36635	ZKTeco ZKBiosecurity 4.1.2/baseOpLog.do opTimeBegin/opTimeEnd sql injection	A vulnerability which was classified as critical has been found in ZKTeco ZKBiosecurity 4.1.2. Affected by this issue is some unknown functionality of the file /baseOpLog.do. The manipulation of the argument opTimeBegin/opTimeEnd leads to sql injection. This vulnerability is handled as CVE-2022-36635. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-42241	Simple Cold Storage Management System 1.0 Master.php sql injection	A vulnerability was found in Simple Cold Storage Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /csms/classes/Master.phpfdelete_message. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-42241. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-42250	Simple Cold Storage Management System 1.0 view_details.php id sql injection	A vulnerability classified as critical was found in Simple Cold Storage Management System 1.0. This vulnerability affects unknown code of the file /csms/admin/inquiries/view_details.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-42250. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-42242	Simple Cold Storage Management System 1.0 Master.php sql injection	A vulnerability was found in Simple Cold Storage Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /csms/classes/Master.phpfdelete_booking. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-42242. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-42249	Simple Cold Storage Management System 1.0 view_storage.php id sql injection	A vulnerability classified as critical has been found in Simple Cold Storage Management System 1.0. This affects an unknown part of the file /csms/admin/storages/view_storage.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-42249. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-42243	Simple Cold Storage Management System 1.0 manage_storage.php id sql injection	A vulnerability was found in Simple Cold Storage Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /csms/admin/storages/manage_storage.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-42243. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-40830	CodeIgniter up to 3.1.13 DB_query_builder.php where_not_in sql injection	A vulnerability was found in CodeIgniter up to 3.1.13. It has been classified as critical. Affected is the function where_not_in of the file system\database\DB_query_builder.php. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-40830. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-41355	Online Leave Management System 1.0 Master.php id sql injection	A vulnerability was found in Online Leave Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /leave_system/classes/Master.phpfdelete_department. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-41355. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-40833	CodeIgniter up to 3.1.13 DB_query_builder.php or_where_in sql injection	A vulnerability classified as critical has been found in CodeIgniter up to 3.1.13. This affects the function or_where_in of the file system\database\DB_query_builder.php. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-40833. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-40832	CodeIgniter up to 3.1.13 DB_query_builder.php having sql injection	A vulnerability was found in CodeIgniter up to 3.1.13. It has been rated as critical. Affected by this issue is the function having of the file system\database\DB_query_builder.php. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-40832. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-40835	CodeIgniter up to 3.1.13 DB_query_builder.php sql injection	A vulnerability which was classified as critical has been found in CodeIgniter up to 3.1.13. This issue affects some unknown processing of the file system\database\DB_query_builder.php. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-40835. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3414	SourceCodester Web-Based Student Clearance System POST Parameter /Admin/login.php txtusername sql injection	A vulnerability was found in SourceCodester Web-Based Student Clearance System. It has been classified as critical. Affected is an unknown function of the file /Admin/login.php of the component POST Parameter Handler. The manipulation of the argument txtusername leads to sql injection. This vulnerability is traded as CVE-2022-3414. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-40824	CodeIgniter up to 3.1.13 DB_query_builder.php or_where sql injection	A vulnerability classified as critical has been found in CodeIgniter up to 3.1.13. Affected is the function or_where of the file system\database\DB_query_builder.php. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-40824. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-40826	CodeIgniter up to 3.1.13 DB_query_builder.php or_having sql injection	A vulnerability which was classified as critical has been found in CodeIgniter up to 3.1.13. Affected by this issue is the function or_having of the file system\database\DB_query_builder.php. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-40826. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-40834	CodeIgniter up to 3.1.13 DB_query_builder.php or_not_like sql injection	A vulnerability classified as critical was found in CodeIgniter up to 3.1.13. This vulnerability affects the function or_not_like of the file system\database\DB_query_builder.php. The manipulation leads to sql injection. This vulnerability was named CVE-2022-40834. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-40828	CodeIgniter up to 3.1.13 DB_query_builder.php or_where_not_in sql injection	A vulnerability has been found in CodeIgniter up to 3.1.13 and classified as critical. This vulnerability affects the function or_where_not_in of the file system\database\DB_query_builder.php. The manipulation leads to sql injection. This vulnerability was named CVE-2022-40828. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-40872	SourceCodester Simple E-Learning System 1.0 /vcs/classRoom.php classCode sql injection	A vulnerability was found in SourceCodester Simple E-Learning System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /vcs/classRoom.php. The manipulation of the argument classCode leads to sql injection. The identification of this vulnerability is CVE-2022-40872. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-40829	CodeIgniter up to 3.1.13 DB_query_builder.php or_like sql injection	A vulnerability was found in CodeIgniter up to 3.1.13 and classified as critical. This issue affects the function or_like of the file system\database\DB_query_builder.php. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-40829. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-40825	CodeIgniter up to 3.1.13 DB_query_builder.php where_in sql injection	A vulnerability classified as critical was found in CodeIgniter up to 3.1.13. Affected by this vulnerability is the function where_in of the file system\database\DB_query_builder.php. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-40825. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-40831	CodeIgniter up to 3.1.13 DB_query_builder.php like sql injection	A vulnerability was found in CodeIgniter up to 3.1.13. It has been declared as critical. Affected by this vulnerability is the function like of the file system\database\DB_query_builder.php. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-40831. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-41514	Open Source SACCO Management System 1.0 ajax.php id sql injection	A vulnerability classified as critical was found in Open Source SACCO Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /sacco_shield/ajax.phpactiondelete_loan. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-41514. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-41513	Online Diagnostic Lab Management System 1.0 /diagnostic/edittest.php id sql injection	A vulnerability which was classified as critical was found in Online Diagnostic Lab Management System 1.0. This affects an unknown part of the file /diagnostic/edittest.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-41513. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-41515	Open Source SACCO Management System 1.0 ajax.php id sql injection	A vulnerability which was classified as critical has been found in Open Source SACCO Management System 1.0. Affected by this issue is some unknown functionality of the file /sacco_shield/ajax.phpactiondelete_payment. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-41515. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-42073	Online Diagnostic Lab Management System 1.0 editclient.php id sql injection	A vulnerability was found in Online Diagnostic Lab Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /diagnostic/editclient.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-42073. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-41377	Online Pet Shop We App 1.0 id sql injection	A vulnerability was found in Online Pet Shop We App 1.0. It has been classified as critical. Affected is an unknown function of the file /pet_shop/admin/pagemaintenance/manage_category. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-41377. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-42074	Online Diagnostic Lab Management System 1.0 editcategory.php id sql injection	A vulnerability classified as critical has been found in Online Diagnostic Lab Management System 1.0. This affects an unknown part of the file /diagnostic/editcategory.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-42074. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-41378	Online Pet Shop We App 1.0 id sql injection	A vulnerability was found in Online Pet Shop We App 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /pet_shop/admin/pageinventory/manage_inventory. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-41378. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3473	SourceCodester Human Resource Management System getstatecity.php ci sql injection	A vulnerability classified as critical has been found in SourceCodester Human Resource Management System. This affects an unknown part of the file getstatecity.php. The manipulation of the argument ci leads to sql injection. This vulnerability is uniquely identified as CVE-2022-3473. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-3472	SourceCodester Human Resource Management System city.php cityedit sql injection	A vulnerability was found in SourceCodester Human Resource Management System. It has been rated as critical. Affected by this issue is some unknown functionality of the file city.php. The manipulation of the argument cityedit leads to sql injection. This vulnerability is handled as CVE-2022-3472. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-41407	Online Pet Shop We App 1.0 id sql injection	A vulnerability which was classified as critical was found in Online Pet Shop We App 1.0. This affects an unknown part of the file /admin/pageorders/view_order. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-41407. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-3470	SourceCodester Human Resource Management System getstatecity.php sc sql injection	A vulnerability was found in SourceCodester Human Resource Management System. It has been classified as critical. Affected is an unknown function of the file getstatecity.php. The manipulation of the argument sc leads to sql injection. This vulnerability is traded as CVE-2022-3470. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-3471	SourceCodester Human Resource Management System city.php searccity sql injection	A vulnerability was found in SourceCodester Human Resource Management System. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file city.php. The manipulation of the argument searccity leads to sql injection. This vulnerability is known as CVE-2022-3471. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-41403	OpenCart 3.x Newsletter Custom Popup email sql injection (ID 168412)	A vulnerability which was classified as critical was found in OpenCart 3.x. Affected is an unknown function of the file index.phprouteextension/module/so_newletter_custom_popup/newsletter of the component Newsletter Custom Popup. The manipulation of the argument email leads to sql injection. This vulnerability is traded as CVE-2022-41403. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3495	SourceCodester Simple Online Public Access Catalog 1.0 Admin Login Actions.php username/password sql injection	A vulnerability has been found in SourceCodester Simple Online Public Access Catalog 1.0 and classified as critical. This vulnerability affects unknown code of the file /opac/Actions.phpalogin of the component Admin Login. The manipulation of the argument username/password leads to sql injection. This vulnerability was named CVE-2022-3495. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-37208	JFinal CMS 5.1.0 sql injection	A vulnerability was found in JFinal CMS 5.1.0. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-37208. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-42064	Online Diagnostic Lab Management System 1.0 sql injection (ID 168498)	A vulnerability has been found in Online Diagnostic Lab Management System 1.0 and classified as critical. This vulnerability affects unknown code. The manipulation leads to sql injection. This vulnerability was named CVE-2022-42064. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-41416	Online Tours Travels Management System 1.0 /user/update_booking.php id sql injection	A vulnerability classified as critical has been found in Online Tours Travels Management System 1.0. This affects an unknown part of the file /user/update_booking.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-41416. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-42218	Open Source SACCO Management System 1.0 manage_loan.php sql injection	A vulnerability classified as critical was found in Open Source SACCO Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /sacco_shield/manage_loan.php. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-42218. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-43023	OpenCATS 0.9.6 Import Error importID sql injection	A vulnerability classified as critical has been found in OpenCATS 0.9.6. Affected is an unknown function of the component Import Error Handler. The manipulation of the argument importID leads to sql injection. This vulnerability is traded as CVE-2022-43023. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-42021	Best Student Result Management System 1.0 notice-details.php nid sql injection	A vulnerability was found in Best Student Result Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /upresult/upresult/notice-details.php. The manipulation of the argument nid leads to sql injection. This vulnerability is handled as CVE-2022-42021. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-43022	OpenCATS 0.9.6 Tag Delete tag_id sql injection	A vulnerability was found in OpenCATS 0.9.6. It has been rated as critical. This issue affects some unknown processing of the component Tag Delete Handler. The manipulation of the argument tag_id leads to sql injection. The identification of this vulnerability is CVE-2022-43022. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-43021	OpenCATS 0.9.6 entriesPerPage sql injection	A vulnerability was found in OpenCATS 0.9.6. It has been declared as critical. This vulnerability affects unknown code. The manipulation of the argument entriesPerPage leads to sql injection. This vulnerability was named CVE-2022-43021. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-43020	OpenCATS 0.9.6 Tag Update tag_id sql injection	A vulnerability was found in OpenCATS 0.9.6. It has been classified as critical. This affects an unknown part of the component Tag Update Handler. The manipulation of the argument tag_id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-43020. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-3671	SourceCodester eLearning System 1.0 manage.php id sql injection	A vulnerability classified as critical was found in SourceCodester eLearning System 1.0. This vulnerability affects unknown code of the file /admin/students/manage.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-3671. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-3395	WP All Export Pro Plugin up to 1.7.8 on WordPress POST Parameter cc_sql sql injection	A vulnerability was found in WP All Export Pro Plugin up to 1.7.8. It has been declared as critical. This vulnerability affects unknown code of the component POST Parameter Handler. The manipulation of the argument cc_sql leads to sql injection. This vulnerability was named CVE-2022-3395. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3302	CleanTalk Spam Protection, AntiSpam, FireWall Plugin up to 5.185.0 on WordPress sql injection	A vulnerability was found in CleanTalk Spam Protection AntiSpam FireWall Plugin up to 5.185.0 and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-3302. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-3300	10Web Form Maker Plugin up to 1.15.5 on WordPress sql injection	A vulnerability has been found in 10Web Form Maker Plugin up to 1.15.5 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-3300. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-3246	Blog2Social Social Media Auto Post & Scheduler Plugin up to 6.9.9 on WordPress sql injection	A vulnerability which was classified as critical has been found in Blog2Social Social Media Auto Post & Scheduler Plugin up to 6.9.9. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-3246. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-37202	JFinal CMS 5.1.0 list sql injection	A vulnerability was found in JFinal CMS 5.1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/advicefeedback/list. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-37202. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-43276	Canteen Management System 1.0 fetchSelectedfood.php productId sql injection	A vulnerability classified as critical has been found in Canteen Management System 1.0. Affected is an unknown function of the file /php_action/fetchSelectedfood.php. The manipulation of the argument productId leads to sql injection. This vulnerability is traded as CVE-2022-43276. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3733	SourceCodester Web-Based Student Clearance System Admin/editadmin.php id sql injection	A vulnerability was found in SourceCodester Web-Based Student Clearance System. It has been classified as critical. This affects an unknown part of the file Admin/edit-admin.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-3733. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-39976	SourceCodester School Activity Updates with SMS Notification 1.0 index.php id sql injection	A vulnerability which was classified as critical has been found in SourceCodester School Activity Updates with SMS Notification 1.0. Affected by this issue is some unknown functionality of the file /modules/announcement/index.phpviewedit. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-39976. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-43230	Simple Cold Storage Management System 1.0 id sql injection	A vulnerability classified as critical was found in Simple Cold Storage Management System 1.0. This vulnerability affects unknown code of the file /admin/pagebookings/view_details. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-43230. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-43228	Barangay Management System 1.0 /clearance/clearance.php hidden_id sql injection	A vulnerability was found in Barangay Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /clearance/clearance.php. The manipulation of the argument hidden_id leads to sql injection. This vulnerability is handled as CVE-2022-43228. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-43232	Canteen Management System 1.0 fetchOrderData.php userid sql injection	A vulnerability was found in Canteen Management System 1.0. It has been classified as critical. This affects an unknown part of the file /php_action/fetchOrderData.php. The manipulation of the argument userid leads to sql injection. This vulnerability is uniquely identified as CVE-2022-43232. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-43233	Canteen Management System 1.0 fetchSelectedUser.php userid sql injection	A vulnerability was found in Canteen Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /php_action/fetchSelectedUser.php. The manipulation of the argument userid leads to sql injection. This vulnerability was named CVE-2022-43233. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-43229	Simple Cold Storage Management System 1.0 update_status.php id sql injection	A vulnerability has been found in Simple Cold Storage Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /bookings/update_status.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-43229. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-43168	Rukovoditel 3.2.1 reports_id sql injection	A vulnerability classified as critical was found in Rukovoditel 3.2.1. This vulnerability affects unknown code. The manipulation of the argument reports_id leads to sql injection. This vulnerability was named CVE-2022-43168. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack
CVE-2022-3254	Classifieds Plugin up to 4.2 on WordPress Premium Module sql injection	A vulnerability was found in Classifieds Plugin up to 4.2. It has been rated as critical. This issue affects some unknown processing of the component Premium Module Handler. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-3254. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack

Cross-Site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-37461	Canon Medical Vitrea View up to 7.7.5 / vitrea-view/error/ cross-site scripting	A vulnerability which was classified as problematic was found in Canon Medical Vitrea View up to 7.7.5. Affected is an unknown function of the file /vitreaview/error/. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-37461. 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-2022-35155	Bus Pass Management System 1.0 searchdata cross-site scripting	A vulnerability which was classified as problematic has been found in Bus Pass Management System 1.0. Affected by this issue is some unknown functionality. The manipulation of the argument searchdata leads to cross-site scripting. This vulnerability is handled as CVE-2022-35155. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-3132	Goolytics Plugin up to 1.1.1 on WordPress Setting cross-site scripting	A vulnerability classified as problematic has been found in Goolytics Plugin up to 1.1.1. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-3132. 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-2022-42247	pfSense 2.5.2 File Name browser.php-cross-site scripting	A vulnerability was found in pfSense 2.5.2. It has been rated as problematic. This issue affects some unknown processing of the file browser.php of the component File Name Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-42247. 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-2022-3128	Donation Thermometer Plugin up to 2.1.2 on WordPress Setting cross-site scripting	A vulnerability was found in Donation Thermometer Plugin up to 2.1.2. It has been classified as problematic. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-3128. 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-2022-2628	DSGVO All in One for WP Plugin up to 4.1 on WordPress Setting cross-site scripting	A vulnerability has been found in DSGVO All in One for WP Plugin up to 4.1 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-2022-2628. 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-2022-32173	Orchard CMS up to 1.2.2 HTML Modal Dialog cross-site scripting	A vulnerability was found in Orchard CMS up to 1.2.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component HTML Modal Dialog. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-32173. The attack can be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-2763	WP Socializer Plugin up to 7.2 on WordPress Icon Setting cross-site scripting	A vulnerability was found in WP Socializer Plugin up to 7.2 and classified as problematic. Affected by this issue is some unknown functionality of the component Icon Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-2763. 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-2022-3002	Yetiforce CRM up to 6.3.x cross-site scripting	A vulnerability was found in Yetiforce CRM up to 6.3.x. 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-2022-3002. 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-2022-39988	Centreon 22.04.0 Template service_alias cross-site scripting (ID 168585)	A vulnerability which was classified as problematic has been found in Centreon 22.04.0. Affected by this issue is some unknown functionality of the component Template Handler. The manipulation of the argument service_alias leads to crosssite scripting. This vulnerability is handled as CVE-2022-39988. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-41392	TotalJS 8c2c8909 Website name cross-site scripting (ID 38)	A vulnerability which was classified as problematic has been found in TotalJS 8c2c8909. This issue affects some unknown processing. The manipulation of the argument Website name leads to cross-site scripting. The identification of this vulnerability is CVE-2022-41392. 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-2022-39285	ZoneMinder prior 1.36.27/1.37.24 Log file cross-site scripting (GHSA-h6x-pcvwv-q433)	A vulnerability was found in ZoneMinder. It has been classified as problematic. This affects an unknown part of the component Log Handler. The manipulation of the argument file leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-39285. 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-2022-3434	SourceCodester Web-Based Student Clearance System / Admin/addstudent.php prepare cross-site scripting	A vulnerability was found in SourceCodester Web-Based Student Clearance System. It has been rated as problematic. Affected by this issue is the function prepare of the file / Admin/add-student.php. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-3434. 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-2022-41442	PicUploader 2.6.3 SettingController.php setStorageParams cross-site scripting (ID 80)	A vulnerability which was classified as problematic has been found in PicUploader 2.6.3. This issue affects the function setStorageParams of the file SettingController.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-41442. 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-2022-3442	Crealogix EBICS 7.0 /ebicsserver/ebics.aspx cross-site scripting	A vulnerability was found in Crealogix EBICS 7.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file / ebicsserver/ebics.aspx. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-3442. The attack may be launched remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-2448	reSmush.it Plugin up to 0.4.5 on WordPress Setting cross-site scripting	A vulnerability was found in reSmush.it Plugin up to 0.4.5. 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-2022-2448. 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-2022-3220	Advanced Comment Form Plugin up to 1.2.0 on WordPress Setting crosssite scripting	A vulnerability was found in Advanced Comment Form Plugin up to 1.2.0. It has been declared as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-3220. 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-2022-2629	Top Bar Plugin up to 3.0.3 on WordPress Setting cross-site scripting	A vulnerability classified as problematic has been found in Top Bar Plugin up to 3.0.3. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2629. 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-2022-2823	MetaSlider Slider, Gallery, and Carousel Plugin up to 3.27.8 on WordPress Gallery Image Parameter cross-site scripting	A vulnerability classified as problematic was found in MetaSlider Slider Gallery and Carousel Plugin up to 3.27.8. This vulnerability affects unknown code of the component Gallery Image Parameter. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2823. 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-2022-3207	Simple File List Plugin up to 4.4.11 on WordPress Setting cross-site scripting	A vulnerability has been found in Simple File List Plugin up to 4.4.11 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-2022-3207. 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-2022-3136	Social Rocket Plugin up to 1.3.2 on WordPress cross-site scripting	A vulnerability which was classified as problematic has been found in Social Rocket Plugin up to 1.3.2. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-3136. 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-2022-3209	soledad Theme up to 8.2.4 on WordPress AJAX Action penci_more_slist_post_ajax id/datafilter[type] cross-site scripting	A vulnerability was found in soledad Theme up to 8.2.4. It has been classified as problematic. This affects the function penci_more_slist_post_ajax of the component AJAX Action Handler. The manipulation of the argument id/datafilter[type] leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-3209. 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-2022-42235	Student Clearance System 1.0 Registration Form cross-site scripting	A vulnerability which was classified as problematic was found in Student Clearance System 1.0. This affects an unknown part of the component Registration Form. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-42235. 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-2022-40440	mxGraph 4.2.2 setTooltips cross-site scripting	A vulnerability classified as problematic was found in mxGraph 4.2.2. Affected by this vulnerability is the function setTooltips. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-40440. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-42715	REDCap prior 12.04.18 Alerts crosssite scripting	A vulnerability which was classified as problematic was found in REDCap. This affects an unknown part of the component Alerts Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-42715. 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-2022-40047	Flatpress 1.2.1 / flatpress/admin.php page cross-site scripting (ID 153)	A vulnerability was found in Flatpress 1.2.1. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /flatpress/admin.php. The manipulation of the argument page leads to cross-site scripting. This vulnerability is known as CVE-2022-40047. 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-2022-41473	RPCMS 3.0.2 Search cross-site scripting	A vulnerability classified as problematic was found in RPCMS 3.0.2. Affected by this vulnerability is an unknown functionality of the component Search. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-41473. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-38902	Liferay Portal/DXP 7.3.10 SP3 Blog Module name cross-site scripting	A vulnerability was found in Liferay Portal and DXP 7.3.10 SP3. It has been declared as problematic. This vulnerability affects unknown code of the component Blog Module. The manipulation of the argument name leads to cross-site scripting. This vulnerability was named CVE-2022-38902. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-42069	Online Birth Certificate Management System 1.0 cross-site scripting (ID 168529)	A vulnerability classified as problematic was found in Online Birth Certificate Management System 1.0. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-42069. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-42071	Online Birth Certificate Management System 1.0 cross-site scripting (ID 168533)	A vulnerability which was classified as problematic was found in Online Birth Certificate Management System 1.0. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-42071. 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-2022-3506	barrykooij related-posts-for-wp up to 2.1.2 cross-site scripting	A vulnerability classified as problematic has been found in barrykooij relatedposts-for-wp up to 2.1.2. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-3506. 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-2022-3547	SourceCodester Simple Cold Storage-Management System 1.0 Setting System Name/System Short Name cross-site scripting	A vulnerability was found in SourceCodester Simple Cold Storage Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /csms/admin/pagesystem_info of the component Setting Handler. The manipulation of the argument System Name/System Short Name leads to crosssite scripting. This vulnerability is uniquely identified as CVE-2022-3547. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3548	SourceCodester Simple Cold Storage-Management System 1.0 Add New Storage Name cross-site scripting	A vulnerability was found in SourceCodester Simple Cold Storage Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the component Add New Storage Handler. The manipulation of the argument Name leads to cross-site scripting. This vulnerability was named CVE-2022-3548. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-38901	Liferay DXP 7.3.10 SP3 Document/Media Module description cross-site scripting	A vulnerability has been found in Liferay DXP 7.3.10 SP3 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Document/Media Module. The manipulation of the argument description leads to cross-site scripting. This vulnerability is known as CVE-2022-38901. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-3608	thorsten phpmyfaq up to 3.1.x crosssite scripting	A vulnerability classified as problematic was found in thorsten phpmyfaq up to 3.1.x. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-3608. 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-2022-43016	OpenCATS 0.9.6 Callback cross-site scripting	A vulnerability which was classified as problematic was found in OpenCATS 0.9.6. Affected is an unknown function of the component Callback Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-43016. 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-2022-43014	OpenCATS 0.9.6 jobOrderID cross-site-scripting	A vulnerability classified as problematic was found in OpenCATS 0.9.6. This vulnerability affects unknown code. The manipulation of the argument joborderID leads to cross-site scripting. This vulnerability was named CVE-2022-43014. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-43015	OpenCATS 0.9.6 entriesPerPage-cross-site scripting	A vulnerability which was classified as problematic has been found in OpenCATS 0.9.6. This issue affects some unknown processing. The manipulation of the argument entriesPerPage leads to cross-site scripting. The identification of this vulnerability is CVE-2022-43015. 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-2022-43018	OpenCATS 0.9.6 Check Email email-cross-site scripting	A vulnerability was found in OpenCATS 0.9.6 and classified as problematic. Affected by this issue is some unknown functionality of the component Check Email Handler. The manipulation of the argument email leads to cross-site scripting. This vulnerability is handled as CVE-2022-43018. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-42200	Simple Exam Reviewer Management System 1.0 Exam List cross-site scripting	A vulnerability has been found in Simple Exam Reviewer Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Exam List Handler. The manipulation leads to crosssite scripting. This vulnerability is known as CVE-2022-42200. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-39301	sra-admin 1.1.1 Profile Picture crosssite scripting (GHSA-v7r9-qx74-h3v8)	A vulnerability was found in sra-admin 1.1.1. It has been declared as problematic. This vulnerability affects unknown code of the component Profile Picture Handler. The manipulation leads to basic cross-site scripting. This vulnerability was named CVE-2022-39301. 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-2022-41358	SourceCodester Garage ManagementSystem 1.0 createCategories.phpcategoriesName cross-site scripting	A vulnerability has been found in SourceCodester Garage Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file createCategories.php. The manipulation of the argument categoriesName leads to cross-site scripting. This vulnerability is known as CVE-2022-41358. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-43017	OpenCATS 0.9.6 indexFile Component cross-site scripting	A vulnerability has been found in OpenCATS 0.9.6 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component indexFile Component. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-43017. 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-2022-42205	PHPGurukul Hospital Management System in PHP 4.0 add-patient.php cross-site scripting	A vulnerability which was classified as problematic has been found in PHPGurukul Hospital Management System in PHP 4.0. Affected by this issue is some unknown functionality of the file add-patient.php. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-42205. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-42206	PHPGurukul Hospital Management System in PHP 4.0 doctor/viewpatient.php cross-site scripting	A vulnerability which was classified as problematic was found in PHPGurukul Hospital Management System in PHP 4.0. This affects an unknown part of the file doctor/view-patient.php. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-42206. 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-2022-39350	DependencyTrack Frontend up to 4.6.0 cross-site scripting (GHSA-c33w-pm52-mqvf)	A vulnerability was found in DependencyTrack Frontend up to 4.6.0. 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-2022-39350. 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-2022-3704	Ruby on Rails _table.html.erb crosssite scripting (ID 46244)	A vulnerability classified as problematic has been found in Ruby on Rails. This affects an unknown part of the file actionpack/lib/action_dispatch/middleware/templates/routes/_table.html.erb. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-3704. 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-2022-3350	Contact Bank Plugin up to 3.0.30 on WordPress Form Setting cross-site scripting	A vulnerability was found in Contact Bank Plugin up to 3.0.30 and classified as problematic. This issue affects some unknown processing of the component Form Setting Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-3350. 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-2022-3391	Retain Live Chat Plugin up to 0.1 on WordPress Setting cross-site scripting	A vulnerability was found in Retain Live Chat Plugin up to 0.1. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-3391. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-3392	WP Humans.txt Plugin up to 1.0.6 on WordPress Setting cross-site scripting	A vulnerability was found in WP Humans.txt Plugin up to 1.0.6. 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-2022-3392. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-42992	Train Scheduler App 1.0 Train Code/Train Name/Destination crosssite scripting	A vulnerability classified as problematic has been found in Train Scheduler App 1.0. This affects an unknown part. The manipulation of the argument Train Code/Train Name/Destination leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-42992. 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-2022-39348	Twisted up to 22.9.x HTTP Request-cross-site scripting (GHSA-vg46-2rrj3647)	A vulnerability classified as problematic has been found in Twisted up to 22.9.x. Affected is an unknown function of the component HTTP Request Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-39348. 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-2022-42991	Simple Online Public Access Catalog 1.0 Edit Account Full Name cross-site scripting	A vulnerability was found in Simple Online Public Access Catalog 1.0. It has been classified as problematic. Affected is an unknown function of the component Edit Account. The manipulation of the argument Full Name leads to cross-site scripting. This vulnerability is traded as CVE-2022-42991. 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-2022-42993	Password Storage Application 1.0 Setup Page cross-site scripting	A vulnerability was found in Password Storage Application 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Setup Page. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-42993. The attack can be launched 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-2022-32407	Softr 2.0 Create A New Account Module First Name cross-site scripting	A vulnerability was found in Softr 2.0. It has been classified as problematic. This affects an unknown part of the component Create A New Account Module. The manipulation of the argument First Name leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-32407. 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-2022-42054	GL.iNet GoodCloud IoT Device Management System 1.00.220412.00 Company Name/Description cross-site scripting	A vulnerability which was classified as problematic has been found in GL.iNet GoodCloud IoT Device Management System 1.00.220412.00. Affected by this issue is some unknown functionality. The manipulation of the argument Company Name/Description leads to cross-site scripting. This vulnerability is handled as CVE-2022-42054. 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-2022-43164	Rukovoditel 3.2.1 Global Lists Name-cross-site scripting	A vulnerability was found in Rukovoditel 3.2.1. It has been rated as problematic. This issue affects some unknown processing of the file /index.phpmodule-uleglobal_lists/lists of the component Global Lists. The manipulation of the argument Name leads to cross-site scripting. The identification of this vulnerability is CVE-2022-43164. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-43165	Rukovoditel 3.2.1 Global Variables Value cross-site scripting	A vulnerability classified as problematic has been found in Rukovoditel 3.2.1. Affected is an unknown function of the file /index.phpmoduleglobal_vars/vars of the component Global Variables. The manipulation of the argument Value leads to cross-site scripting. This vulnerability is traded as CVE-2022-43165. 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-2022-43166	Rukovoditel 3.2.1 Global Entities Name cross-site scripting	A vulnerability classified as problematic was found in Rukovoditel 3.2.1. Affected by this vulnerability is an unknown functionality of the file /index.phpmoduleentities/entities of the component Global Entities. The manipulation of the argument Name leads to cross-site scripting. This vulnerability is known as CVE-2022-43166. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-43167	Rukovoditel 3.2.1 Users Alerts Title cross-site scripting	A vulnerability which was classified as problematic has been found in Rukovoditel 3.2.1. Affected by this issue is some unknown functionality of the file /index.phpmodule-users_alerts/users_alerts of the component Users Alerts. The manipulation of the argument Title leads to cross-site scripting. This vulnerability is handled as CVE-2022-43167. 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-2022-43169	Rukovoditel 3.2.1 Users Access Groups Name cross-site scripting	A vulnerability which was classified as problematic was found in Rukovoditel 3.2.1. This affects an unknown part of the file /index.phpmoduleusers_groups/users_groups of the component Users Access Groups. The manipulation of the argument Name leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-43169. 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-2022-43170	Rukovoditel 3.2.1 Dashboard Configuration Title cross-site scripting	A vulnerability has been found in Rukovoditel 3.2.1 and classified as problematic. This vulnerability affects unknown code of the file index.phpmoduledashboard_configure/ index of the component Dashboard Configuration. The manipulation of the argument Title leads to cross-site scripting. This vulnerability was named CVE-2022-43170. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-3773	EmbedPress Plugin on WordPress Shortcode post.php cross-site scripting	A vulnerability has been found in EmbedPress Plugin and classified as problematic. Affected by this vulnerability is an unknown functionality of the file post.php of the component Shortcode Handler. The manipulation leads to crosssite scripting. This vulnerability is known as CVE-2022-3773. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-2190	Gallery Plugin for Plugin up to 1.8.4.6 on WordPress Attribute $_SERVER['REQUEST_URI'] cross-site scripting	A vulnerability classified as problematic has been found in Gallery Plugin for Plugin up to 1.8.4.6. Affected is an unknown function of the component Attribute Handler. The manipulation of the argument $_SERVER[&039;REQUEST_URI&039;] leads to cross-site scripting. This vulnerability is traded as CVE-2022-2190. 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-2022-3096	WP Total Hacks Plugin up to 4.7.2 on WordPress Setting cross-site scripting	A vulnerability classified as problematic was found in WP Total Hacks Plugin up to 4.7.2. 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-2022-3096. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-3237	WP Contact Slider Plugin up to 2.4.7 on WordPress Setting cross-site scripting	A vulnerability which was classified as problematic has been found in WP Contact Slider Plugin up to 2.4.7. 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-2022-3237. 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-2022-3408	WP Word Count Plugin up to 3.2.3 on WordPress Setting cross-site scripting	A vulnerability which was classified as problematic was found in WP Word Count Plugin up to 3.2.3. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-3408. 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-2022-3420	Official Integration for Billingo Plugin up to 3.3.x on WordPress cross-site scripting	A vulnerability was found in Official Integration for Billingo Plugin up to 3.3.x and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-3420. 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-2022-3440	Rock Convert Plugin up to 2.10.x on-WordPress Attribute cross-site scripting	A vulnerability was found in Rock Convert Plugin up to 2.10.x. It has been classified as problematic. Affected is an unknown function of the component Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-3440. 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-2022-3441	Rock Convert Plugin up to 2.10.x on WordPress Setting cross-site scripting	A vulnerability was found in Rock Convert Plugin up to 2.10.x. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-3441. 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-2022-2167	Newspaper Theme up to 11 on WordPress AJAX Action cross-site scripting	A vulnerability was found in Newspaper Theme up to 11. It has been rated as problematic. Affected by this issue is some unknown functionality of the component AJAX Action Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-2167. 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-2022-2627	Newspaper Theme up to 11 on WordPress AJAX Action a cross-site scripting	A vulnerability classified as problematic has been found in Newspaper Theme up to 11. This affects an unknown part of the component AJAX Action Handler. The manipulation of the argument a leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2627. 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-2022-3765	thorsten phpmyfaq up to 3.1.7 crosssite scripting	A vulnerability which was classified as problematic has been found in thorsten phpmyfaq up to 3.1.7. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-3765. 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-2022-3766	thorsten phpmyfaq up to 3.1.7 crosssite scripting	A vulnerability which was classified as problematic was found in thorsten phpmyfaq up to 3.1.7. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-3766. 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

Indusface is a leading application security SaaS company that secures critical Web, Mobile & API applications of 3000+ global customers using its award-winning fully managed platform that integrates a web application scanner, web application firewall, DDoS &, BOT Mitigation, CDN, and threat intelligence engine. The company has been funded by Tata Capital Growth Fund, is Great Place to Work certified, mentioned by analysts like Gartner, Forrester, etc in their reports, and has been the recipient of many awards such as the Economic Times Top 25, NASSCOM DSCI Top Security Company, Deloitte Asia Top 100 , and several other such prestigious recognitions.

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

EMAIL - sales@indusface.com

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