INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

July 2022

Total Zero-Day Vulnerabilities Found: 231

Command Injection	Cross-Site Request Forgery	Local File Inclusion	SQL Injection	Cross-Site Scripting	XML External Entity
20	3	90	35	80	3

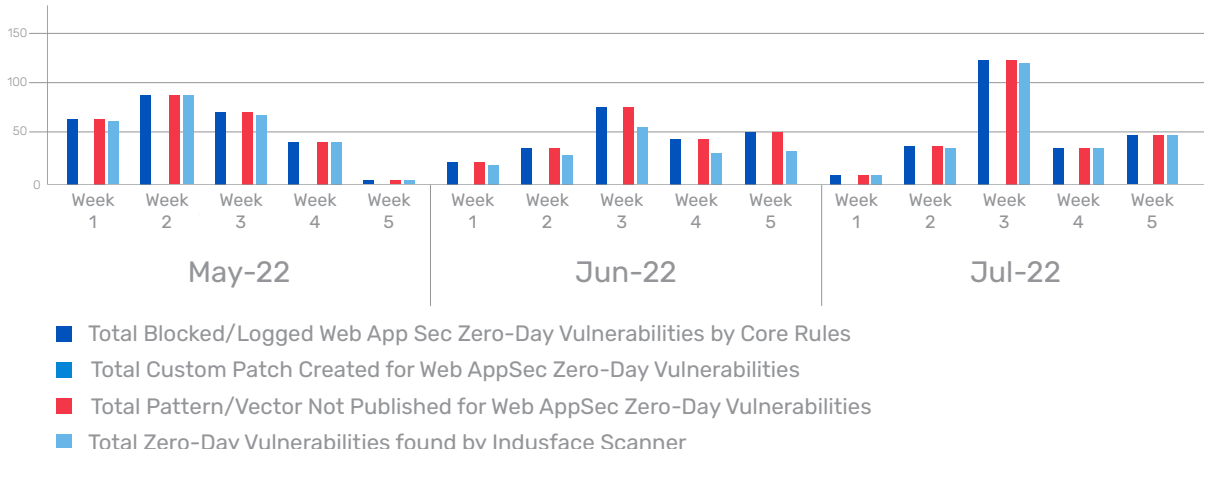
Zero-day vulnerabilities protected through core rules	231
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities for which protection can not be done	0
Zero-day vulnerabilities found by Indusface WAS	228

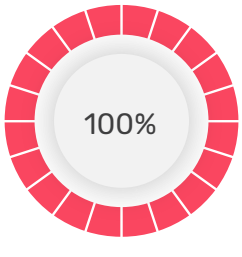
- To enable custom rules, please contact support@indusface.com
- Since the attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.

Vulnerability Trend:

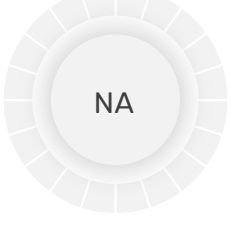
The weekly trend displays the total number of vulnerabilities discovered to the type of protection provided for the last quarter.

Weekly Vulnerability Trend

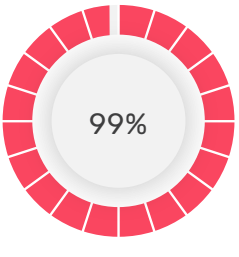




of the zero-day vulnerabilities were protected by the **core rules** in the last month.

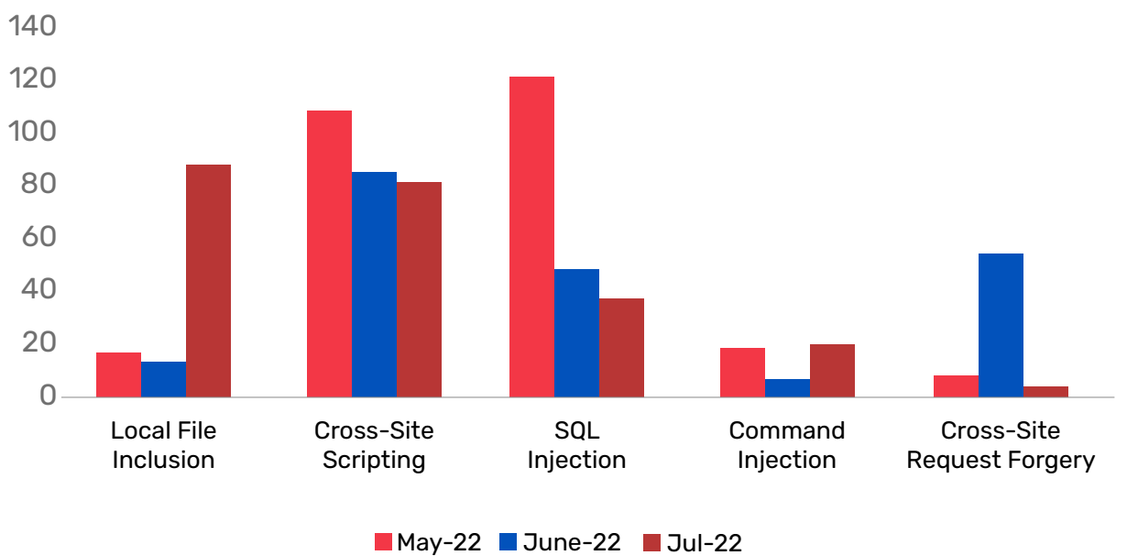


of the zero-day vulnerabilities were protected by the **custom rules** in the last month.



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

Top Five Vulnerability Categories



XML External Entity Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-41042	Eclipse Lyo up to 4.1.0 RDF xml external entity reference (ID 287)	A vulnerability was found in Eclipse Lyo up to 4.1.0. It has been classified as problematic. Affected is an unknown function of the component RDF Handler. The manipulation leads to xml external entity reference. This vulnerability is traded as CVE-2021-41042. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as XML External Entity Attack.
CVE-2015-8031	cPanel Hudson up to 3.3.1 xml external entity reference (GHSA-j3h2-8mf8-j5r2)	A vulnerability was found in cPanel Hudson up to 3.3.1. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to xml external entity reference. This vulnerability is known as CVE-2015-8031. Access to the local network is required for this attack. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as XML External Entity Attack.
CVE-2022-34001	Unit4 ERP up to 7.9 ExecuteServerProcessAsynchronously xml external entity reference	A vulnerability was found in Unit4 ERP up to 7.9. It has been classified as problematic. This affects the function ExecuteServerProcessAsynchronously. The manipulation leads to xml external entity reference. This vulnerability is uniquely identified as CVE-2022-34001. The attack needs to be approached within the local network. Furthermore, there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as XML External Entity Attack.

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-31677	PESCMS 2.3.3 cross-site request forgery	A vulnerability has been found in PESCMS 2.3.3 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2021-31677. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-2144	Jquery Validation for Contact Form 7 Plugin up to 5.2 on WordPress cross-site request forgery	A vulnerability classified as problematic has been found in Jquery Validation for Contact Form 7 Plugin up to 5.2. This affects an unknown part. The manipulation leads to crosssite request forgery. This vulnerability is uniquely identified as CVE-2022-2144. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-1672	Insights from Google PageSpeed Plugin up to 4.0.6 on WordPress cross-site request forgery	A vulnerability classified as problematic has been found in Insights from Google PageSpeed Plugin up to 4.0.6. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-1672. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA

Command Injection Attack Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-25900	git-clone command-injection	A vulnerability was found in git-clone. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to command injection. This vulnerability was named CVE-2022-25900. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-2268	Import any XML or CSV File to Plugin up to 3.6.7 on WordPress ZIP File code injection	A vulnerability classified as critical was found in Import any XML or CSV File to Plugin up to 3.6.7. Affected by this vulnerability is an unknown functionality of the component ZIP File Handler. The manipulation leads to code injection. This vulnerability is known as CVE-2022-2268. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2015-3173	custom-content-typemanager Plugin on WordPress code injection	A vulnerability which was classified as critical was found in custom-content-type-manager Plugin. Affected is an unknown function. The manipulation leads to code injection. This vulnerability is traded as CVE-2015-3173. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-25048	CWP 0.9.8.1126 command injection	A vulnerability classified as critical has been found in CWP 0.9.8.1126. This affects an unknown part. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2022-25048. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31137	Hap-WI Roxy-WI up to 6.1.0.x /app/options.py subprocess_execute os command injection (GHSA-53r2-mq99-f532)	A vulnerability which was classified as critical was found in Hap-WI Roxy-WI up to 6.1.0.x. Affected is the function subprocess_execute of the file /app/options.py. The manipulation leads to os command injection. This vulnerability is traded as CVE-2022-31137. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-2099	WooCommerce Plugin up to 6.5.x on WordPress Payment Gateway Title injection	A vulnerability which was classified as problematic has been found in WooCommerce Plugin up to 6.5.x. Affected by this issue is some unknown functionality of the component Payment Gateway Title Handler. The manipulation leads to injection. This vulnerability is handled as CVE-2022-2099. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-26482	Poly EagleEye Director II up to 2.2.2.0 os.system os command injection	A vulnerability was found in Poly EagleEye Director II up to 2.2.2.0. It has been classified as critical. This affects the function os.system. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2022-26482. Access to the local network is required for this attack to succeed. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-31201	SoftGuard Web up to 5.1.4 injection	A vulnerability which was classified as problematic has been found in SoftGuard Web up to 5.1.4. This issue affects some unknown processing. The manipulation leads to injection. The identification of this vulnerability is CVE-2022-31201. Access to the local network is required for this attack to succeed. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as command injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-26481	Poly Studio up to 3.6.x CSR Action CN command injection	A vulnerability was found in Poly Studio up to 3.6.x and classified as critical. Affected by this issue is some unknown functionality of the component CSR Action Handler. The manipulation of the argument CN leads to command injection. This vulnerability is handled as CVE-2022-26481. Access to the local network is required for this attack. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-34538	Digital Watchdog DW MEGApix IP Camera A7.2.2_20211029 POST Request addacph.cgi command injection	A vulnerability classified as critical has been found in Digital Watchdog DW MEGApix IP Camera A7.2.2_20211029. Affected is an unknown function of the file /admin/vca/bia/addacph.cgi of the component POST Request Handler. The manipulation leads to command injection. This vulnerability is traded as CVE-2022-34538. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-2488	WAVLINK WN535K2/WN535K3 touchlist_sync.cgi IP os command injection	A vulnerability was found in WAVLINK WN535K2 and WN535K3 and classified as critical. This issue affects some unknown processing of the file /cgi-bin/touchlist_sync.cgi. The manipulation of the argument IP leads to os command injection. The identification of this vulnerability is CVE-2022-2488. 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-2022-27483	Fortinet FortiManager/FortiAnalyzer up to 6.0.x/6.2.x/6.4.7/7.0.3 CLI Command os command injection	A vulnerability was found in Fortinet FortiManager and FortiAnalyzer up to 6.0.x/6.2.x/6.4.7/7.0.3. It has been classified as critical. Affected is an unknown function of the component CLI Command Handler. The manipulation leads to os command injection. This vulnerability is traded as CVE-2022-27483. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
Null	Dell PowerStore up to 2.x PowerStore T Environment os command injection	A vulnerability which was classified as critical has been found in Dell PowerStore up to 2.x. Affected by this issue is some unknown functionality of the component PowerStore T Environment. The manipulation leads to os command injection. This vulnerability is handled as CVE-2022-33923. Attacking locally is a requirement. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as command injection attack
Null	Dell EMC PowerStore os command injection	A vulnerability classified as critical has been found in Dell EMC PowerStore. Affected is an unknown function. The manipulation leads to os command injection. This vulnerability is traded as CVE-2022-22555. An attack has to be approached locally. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2020-28459	markdown-it-decorate Event code injection (SNYK-JSMARKDOWNITDECORATE-1044068)	A vulnerability classified as critical has been found in markdown-it-decorate. This affects an unknown part of the component Event Handler. The manipulation leads to code injection. This vulnerability is uniquely identified as CVE-2020-28459. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2020-28446	ntesseract up to 0.2.8 lib/tesseract.js command injection	A vulnerability was found in ntesseract up to 0.2.8. It has been classified as critical. Affected is an unknown function in the library lib/tesseract.js. The manipulation leads to command injection. This vulnerability is traded as CVE-2020-28446. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-23100	OX Software OX App Suite up to 7.10.6 Email Attachment Documentconverter os command injection	A vulnerability was found in OX Software OX App Suite up to 7.10.6 and classified as critical. Affected by this issue is the function Documentconverter of the component Email Attachment Handler. The manipulation leads to os command injection. This vulnerability is handled as CVE-2022-23100. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2550	hestiacp up to 1.6.4 os command injection	A vulnerability which was classified as critical was found in hestiacp up to 1.6.4. Affected is an unknown function. The manipulation leads to os command injection. This vulnerability is traded as CVE-2022-2550. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-24405	OX Software OX App Suite up to 7.10.6 Documentconverter API os command injection	A vulnerability was found in OX Software OX App Suite up to 7.10.6. It has been classified as critical. This affects an unknown part of the component Documentconverter API. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2022-24405. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2016-4991	nodepdf 1.3.0 Pdf os command injection	A vulnerability was found in nodepdf 1.3.0. It has been classified as critical. This affects the function Pdf. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2016-4991. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-32095	Hospital Management System 1.0 orders.php editid sql injection	A vulnerability was found in Hospital Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file orders.php. The manipulation of the argument editid leads to sql injection. This vulnerability was named CVE-2022-32095. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-32093	Hospital Management System 1.0 adminlogin.php loginid sql injection	A vulnerability was found in Hospital Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file adminlogin.php. The manipulation of the argument loginid leads to sql injection. This vulnerability is handled as CVE-2022-32093. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-32094	Hospital Management System 1.0 doctor-login.php loginid sql injection	A vulnerability was found in Hospital Management System 1.0. It has been classified as critical. This affects an unknown part of the file doctorlogin.php. The manipulation of the argument loginid leads to sql injection. This vulnerability is uniquely identified as CVE-2022-32094. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-2298	SourceCodester Clinics Patient Management System 2.0 Login Page /pms / index.php user_name sql injection	A vulnerability has been found in SourceCodester Clinics Patient Management System 2.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /pms/index.php of the component Login Page. The manipulation of the argument user_name with the input admin&039; or &039;1&039; &039;1 leads to sql injection. This vulnerability is known as CVE-2022-2298. The attack can be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2021-44915	Taocms 3.0.2 Edit Category sql injection	A vulnerability was found in Taocms 3.0.2. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Edit Category Handler. The manipulation leads to sql injection. This vulnerability is known as CVE-2021-44915. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-32311	SourceCodester Ingredient Stock Management System 1.0 view_stock.php id sql injection (ID 167290)	A vulnerability classified as critical was found in SourceCodester Ingredient Stock Management System 1.0. This vulnerability affects unknown code of the file /isms/admin /stocks/view_stock.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-32311. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-31856	Newsletter Module on OpenCart /index.php zemez_newsletter_email sql injection (ID50942 / EDB-50942)	A vulnerability classified as critical has been found in Newsletter Module. This affects an unknown part of the file/index.php. The manipulation of the argument zemez_newsletter_email leads to sql injection. This vulnerability is uniquely identified as CVE-2022-31856. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-34972	So Filter Shop 3.x on OpenCart sql injection (ID 167605)	A vulnerability which was classified as critical has been found in So Filter Shop 3.x. This issue affects some unknown processing of the file /index.phprouteextension/module /so_filter_shop_by/filter_data. The manipulation of the argument att_value_id / manu_value_id /opt_value_id /subcate_value_id leads to sql injection. The identification of this vulnerability is CVE-2022-34972. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-32055	Inout Homestay 2.2 guests sql injection	A vulnerability which was classified as critical was found in Inout Homestay 2.2. This affects an unknown part of the file /index.phppagesearch/rentals. The manipulation of the argument guests leads to sql injection. This vulnerability is uniquely identified as CVE-2022-32055. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-32056	Online Accreditation Management 1.0 process.php USERNAME sql injection	A vulnerability has been found in Online Accreditation Management 1.0 and classified as critical. This vulnerability affects unknown code of the file process.php. The manipulation of the argument USERNAME leads to sql injection. This vulnerability was named CVE-2022-32056. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2021-35283	atoms183 CMS 1.0 product_admin.php Name/Fname/ID sql injection	A vulnerability classified as critical was found in atoms183 CMS 1.0. Affected by this vulnerability is an unknown functionality of the file product_admin.php. The manipulation of the argument Name/Fname/ID leads to sql injection. This vulnerability is known as CVE-2021-35283. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-32415	oretnom23 Product Show Room Site 1.0 id sql injection	A vulnerability was found in oretnom23 Product Show Room Site 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /psrs/pproducts/view_product. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-32415. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-32297	Piwigo 12.2.0 Search sql injection	A vulnerability classified as critical has been found in Piwigo 12.2.0. Affected is an unknown function of the component Search. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-32297. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-32416	oretnom23 Product Show Room Site 1.0 Master.php sql injection	A vulnerability was found in oretnom23 Product Show Room Site 1.0. It has been classified as critical. Affected is an unknown function of the file /psrs/classes/Master.phpfdelete_product. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-32416. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-27434	Unit4 Teta Mobile Edition up to 29.5.HF16 errorReporting Page ProfileName sql injection	A vulnerability was found in Unit4 Teta Mobile Edition up to 29.5.HF16. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component errorReporting Page. The manipulation of the argument ProfileName leads to sql injection. This vulnerability is known as CVE-2022-27434. The attack can be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-24691	DSK DSKNet 2.16.136.0/2.17.136.5 HTTP Request sql injection	A vulnerability classified as critical was found in DSK DSKNet 2.16.136.0/2.17.136.5. Affected by this vulnerability is an unknown functionality of the component HTTP Request Handler. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-24691. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-2468	SourceCodester Garage Management System 1.0 / editbrand.php id sql injection	A vulnerability was found in SourceCodester Garage Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /editbrand.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-2468. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2467	SourceCodester Garage Management System 1.0 /login.php username sql injection	A vulnerability has been found in SourceCodester Garage Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /login.php. The manipulation of the argument username with the input 1a.com&039; AND)) LwLu) AND &039; hsvT&039;&039;hsvT leads to sql injection. This vulnerability was named CVE-2022-2467. The attack can be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-24690	DSK DSKNet 2.16.136.0/2. 17.136.5 HTTP Request PresAbs.php sql injection	A vulnerability which was classified as critical has been found in DSK DSKNet 2.16.136.0/2.17.136.5. This issue affects some unknown processing of the file PresAbs.php of the component HTTP Request Handler. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-24690. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-2491	SourceCodester Library Management System 1.0 lab.php Section sql injection	A vulnerability has been found in SourceCodester Library Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file lab.php. The manipulation of the argument Section with the input 1&039; UNION ALL SELECT NULLNULLNULLNULLNULLCONCATNULLNULLNULLNULL leads to sql injection. This vulnerability was named CVE-2022-2491. The attack can be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-2492	SourceCodester Library ManagementSystem 1.0 / index.php RollNo sql injection	A vulnerability was found in SourceCodester Library Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /index.php. The manipulation of the argument RollNo with the input admin&039; AND)) MdIL) AND &039; KXmq&039; &039; KXmq& Password1231312312 leads to sql injection. The identification of this vulnerability is CVE-2022-2492. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-34023	Barangay Management System 1.0 / officials/officials.php hidden_id sql injection	A vulnerability was found in Barangay Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /officials /officials.php. The manipulation of the argument hidden_id leads to sql injection. This vulnerability is known as CVE-2022-34023. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-2490	SourceCodester Simple E-Learning System 1.0 search.php classCode sql injection	A vulnerability classified as critical has been found in SourceCodester Simple E-Learning System 1.0. Affected is an unknown function of the file search.php. The manipulation of the argument classCode with the input 1&039; CONCAT)) 0x71717a-7071FLOOR2)) x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)) &039; leads to sql injection. This vulnerability is traded as CVE-2022-2490. It is possible to launch the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-2489	SourceCodester Simple E-Learning System 1.0 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 classRoom.php. The manipulation of the argument classCode with the input 1&039; CONCAT))0x-717a7a7671FLOOR2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a))&039; leads to sql injection. The identification of this vulnerability is CVE-2022-2489. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-34590	itsourcecode Hospital Management System 1.0 /HMS/admin.php editid sql injection	A vulnerability was found in itsourcecode Hospital Management System 1.0. It has been classified as critical. This affects an unknown part of the file /HMS/admin.php. The manipulation of the argument editid leads to sql injection. This vulnerability is uniquely identified as CVE-2022-34590. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-34586	itsourcecode Advanced School Management System 1.0 student_grade_ wise.php grade sql injection	A vulnerability has been found in itsourcecode Advanced School Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /school/view/student_grade_ wise.php. The manipulation of the argument grade leads to sql injection. This vulnerability is known as CVE-2022-34586. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-34588	itsourcecode Advanced School Management System 1.0 timetable_insert_form. php grade sql injection	A vulnerability was found in itsourcecode Advanced School Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file / school/view /timetable_insert_form.php. The manipulation of the argument grade leads to sql injection. This vulnerability is handled as CVE-2022-34588. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-34114	Dataease 1.11.1 dataSourceId sql injection (ID 2430)	A vulnerability which was classified as critical was found in Dataease 1.11.1. This affects an unknown part. The manipulation of the argument dataSourceId leads to sql injection. This vulnerability is uniquely identified as CVE-2022-34114. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-34115	Dataease 1.11.1 dataSourceId sql injection (ID 2428)	A vulnerability has been found in Dataease 1.11.1 and classified as critical. This vulnerability affects unknown code. The manipulation of the argument dataSourceId leads to sql injection. This vulnerability was named CVE-2022-34115. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-31879	oretnom23 Online Fire Reporting System 1.0 Parameter date sql injection	A vulnerability was found in oretnom23 Online Fire Reporting System 1.0 and classified as critical. This issue affects some unknown processing of the component Parameter Handler. The manipulation of the argument date leads to sql injection. The identification of this vulnerability is CVE-2022-31879. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-36161	Orange Station 1.0 username sql injection	A vulnerability was found in Orange Station 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation of the argument username leads to sql injection. This vulnerability is known as CVE-2022-36161. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-34067	Warehouse Management System 1.0 cari sql injection	A vulnerability was found in Warehouse Management System 1.0. It has been classified as critical. Affected is an unknown function. The manipulation of the argument cari leads to sql injection. This vulnerability is traded as CVE-2022-34067. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-34989	Fruits Bazar 1.0 user_password_recover.php recover_email sql injection	A vulnerability has been found in Fruits Bazar 1.0 and classified as critical. This vulnerability affects unknown code of the file user_password_recover.php. The manipulation of the argument recover_email leads to sql injection. This vulnerability was named CVE-2022-34989. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-2577	SourceCodester Garage Management System 1.0 /edituser.php id sql injection	A vulnerability classified as critical was found in SourceCodester Garage Management System 1.0. This vulnerability affects unknown code of the file /edituser.php. The manipulation of the argument id with the input -2&039;%20UNION%20select%2011user333444--+ leads to sql injection. This vulnerability was named CVE-2022-2577. The attack can be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack
CVE-2022-34557	Barangay Management System 1.0 / pages/permit / permit.php hidden_id sql injection	A vulnerability was found in Barangay Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /pages/permit/permit.php. The manipulation of the argument hidden_id leads to sql injection. The identification of this vulnerability is CVE-2022-34557. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as SQL Injection attack

Cross-Site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2290	zadam trilium up to 0.52.3/0.53.0 cross-site scripting	A vulnerability classified as problematic has been found in zadam trilium up to 0.52.3/0.53.0. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2290. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2292	SourceCodester Hotel Management System 2.0 Room Edit Page 1 massageroomDetails cross-site scripting	A vulnerability classified as problematic has been found in SourceCodester Hotel Management System 2.0. Affected is an unknown function of the file / ci_hms/massage_room/edit/1 of the component Room Edit Page. The manipulation of the argument massageroomDetails with the input "><script>alert< /script> leads to cross-site scripting. This vulnerability is traded as CVE-2022-2292. It is possible to launch the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2293	SourceCodester Simple Sales Management System 1.0 create customer_name cross-site scripting	A vulnerability classified as problematic was found in SourceCodester Simple Sales Management System 1.0. Affected by this vulnerability is an unknown functionality of the file / ci_ssms /index.php/orders/create. The manipulation of the argument customer_name with the input <script>alert</script> leads to cross-site scripting. This vulnerability is known as CVE-2022-2293. The attack can be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2291	SourceCodester Hotel Management System 2.0 Search /ci_hms/search crosssite scripting	A vulnerability was found in SourceCodester Hotel Management System 2.0. It has been rated as problematic. This issue affects some unknown processing of the file /ci_hms/search of the component Search. The manipulation of the argument search with the input "><script>alert</script> leads to crosssite scripting. The identification of this vulnerability is CVE-2022-2291. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2300	Microweber up to 1.2.18 cross-site scripting	A vulnerability was found in Microweber up to 1.2.18. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2300. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2021-25066	Ninja Forms Contact Form Plugin up to 3.6.9 on WordPress Data Import cross-site scripting	A vulnerability which was classified as problematic was found in Ninja Forms Contact Form Plugin up to 3.6.9. This affects an unknown part of the component Data Import Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2021-25066. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2021-25056	Ninja Forms Contact Form Plugin up to 3.6.9 Field Label cross-site scripting	A vulnerability which was classified as problematic has been found in Ninja Forms Contact Form Plugin up to 3.6.9. Affected by this issue is some unknown functionality of the component Field Label Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2021-25056. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-0250	Redirection for Contact Form 7 Plugin up to 2.4.x on WordPress Attribute cross-site scripting	A vulnerability has been found in Redirection for Contact Form 7 Plugin up to 2.4.x and classified as problematic. This vulnerability affects unknown code of the component Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-0250. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1301	WP Contact Slider Plugin up to 2.4.6 on WordPress Text to Display Settings cross-site scripting	A vulnerability was found in WP Contact Slider Plugin up to 2.4.6 and classified as problematic. This issue affects some unknown processing of the component Text to Display Settings. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1301. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-33075	SourceCodester Zoo Management System 1.0 Add Classification cross-site scripting (ID 167603)	A vulnerability was found in SourceCodester Zoo Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Add Classification. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-33075. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-34007	EQS Integrity Line up to 2022-07-01 Whistleblower Entry cross-site scripting	A vulnerability which was classified as problematic has been found in EQS Integrity Line up to 2022-07-01. Affected by this issue is some unknown functionality of the component Whistleblower Entry Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-34007. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2021-31676	PESCMS 2.3.3 cross-site scripting	A vulnerability which was classified as problematic was found in PESCMS 2.3.3. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2021-31676. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-31127	NextAuth.js up to 3.29.7/4.8.x Email Signin Endpoint crosssite scripting (GHSApg-jx-7f9g-9463)	A vulnerability was found in NextAuth.js up to 3.29.7/4.8.x. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Email Signin Endpoint. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-31127. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-32567	Appfire Jira Misc Custom Fields App 2.4.6 on Atlassian Project Name cross-site scripting (SYSS-2022-039)	A vulnerability was found in Appfire Jira Misc Custom Fields App 2.4.6. It has been classified as problematic. This affects an unknown part of the component Project Name Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-32567. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2015-3172	EidoGo SGF crosssite scripting (ID 27)	A vulnerability was found in EidoGo. It has been rated as problematic. This issue affects some unknown processing of the component SGF Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2015-3172. 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 the scanner as cross-site scripting attack
CVE-2022-2342	outline up to 0.64.3 cross-site scripting	A vulnerability classified as problematic has been found in outline up to 0.64.3. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-2342. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-31290	Known 1.2.2 +2020061101 Your Name cross-site scripting	A vulnerability classified as problematic was found in Known 1.2.2 +2020061101. Affected by this vulnerability is an unknown functionality. The manipulation of the argument Your Name leads to cross-site scripting. This vulnerability is known as CVE-2022-31290. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2363	SourceCodester Simple Parking Management System 1.0 search cross-site scripting	A vulnerability which was classified as problematic has been found in SourceCodester Simple Parking Management System 1.0. Affected by this issue is some unknown functionality of the file /ci_spms/admin/search/searching/. The manipulation of the argument search with the input "><script>alert< /script> leads to cross-site scripting. This vulnerability is handled as CVE-2022-2363. The attack may be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2364	SourceCodester Simple Parking Management System 1.0 / ci_spms/admin /category vehicle_type crosssite scripting	A vulnerability which was classified as problematic was found in SourceCodester Simple Parking Management System 1.0. This affects an unknown part of the file /ci_spms/admin/category. The manipulation of the argument vehicle_type with the input "><script>alert</script> leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2364. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2353	Microweber 1.2.20 cross-site scripting	A vulnerability has been found in Microweber 1.2.20 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2353. 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 cross-site scripting attack
CVE-2022-35416	H3C SSL VPN up to 2022-07-10 wnm/login /login.json svpnlang cross-site scripting	A vulnerability which was classified as problematic was found in H3C SSL VPN up to 2022-07-10. Affected is an unknown function of the file wnm/login/login.json. The manipulation of the argument svpnlang leads to cross-site scripting. This vulnerability is traded as CVE-2022-35416. It is possible to launch the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2365	zadam trilium up to 0.53.2 cross-site scripting	A vulnerability classified as problematic was found in zadam trilium up to 0.53.2. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2365. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-32274	Transition Scheduler Add-on 6.5.0 on Atlassian Project Name cross-site scripting (SYSS-2022-040)	A vulnerability was found in Transition Scheduler Add-on 6.5.0 and classified as problematic. This issue affects some unknown processing of the component Project Name Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-32274. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2396	SourceCodester Simple e-Learning System 1.0 /vcs / claire_blake Bio cross-site scripting	A vulnerability classified as problematic was found in SourceCodester Simple e-Learning System 1.0. Affected by this vulnerability is an unknown functionality of the file /vcs/claire_blake. The manipulation of the argument Bio with the input "><script>alert</script> leads to cross-site scripting. This vulnerability is known as CVE-2022-2396. The attack can be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-30517	Mogu Blog 5.2 cross-site scripting (ID 65)	A vulnerability was found in Mogu Blog 5.2. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-30517. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-34094	Portal do Software Publico Brasileiro i3geo 7.0.5 request_token.php cross-site scripting	A vulnerability classified as problematic has been found in Portal do Software Publico Brasileiro i3geo 7.0.5. This affects an unknown part of the file request_token.php. The manipulation leads to crosssite scripting. This vulnerability is uniquely identified as CVE-2022-34094. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-32118	Arox School ERP Pro 1.0 backoffice.inc.php dispatchcategory cross-site scripting	A vulnerability classified as problematic has been found in Arox School ERP Pro 1.0. Affected is an unknown function of the file backoffice.inc.php. The manipulation of the argument dispatchcategory leads to cross-site scripting. This vulnerability is traded as CVE-2022-32118. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2020-36550	SourceCodester Multi Restaurant Table Reservation System 1.0 table-list.php Table Name cross-site scripting (EDB-49135)	A vulnerability was found in SourceCodester Multi Restaurant Table Reservation System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /dashboard/tablelist. php. The manipulation of the argument Table Name leads to cross-site scripting. This vulnerability is handled as CVE-2020-36550. The attack may be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-25869	Angular Cache cross-site scripting	A vulnerability was found in Angular. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Cache Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-25869. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2020-35261	SourceCodester Multi Restaurant Table Reservation System 1.0 /dashboard/profile. php Restaurant Name cross-site scripting (EDB-49135)	A vulnerability classified as problematic was found in SourceCodester Multi Restaurant Table Reservation System 1.0. This vulnerability affects unknown code of the file /dashboard/profile. php. The manipulation of the argument Restaurant Name leads to cross-site scripting. This vulnerability was named CVE-2020-35261. The attack can be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2020-36552	SourceCodester Multi Restaurant Table Reservation System 1.0 /dashboard/menulist. php Made crosssite scripting (EDB-49135)	A vulnerability was found in SourceCodester Multi Restaurant Table Reservation System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /dashboard/menu-list. php. The manipulation of the argument Made leads to cross-site scripting. This vulnerability was named CVE-2020-36552. The attack can be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2020-36551	SourceCodester Multi Restaurant Table Reservation System 1.0 /dashboard/ menulist.php Item Name cross-site scripting (EDB-49135)	A vulnerability was found in SourceCodester Multi Restaurant Table Reservation System 1.0. It has been classified as problematic. This affects an unknown part of the file / dashboard/menu-list.php. The manipulation of the argument Item Name leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2020-36551. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2020-36553	SourceCodester Multi Restaurant Table Reservation System 1.0 /dashboard/ menulist. php Area (food_type) cross-site scripting (EDB-49135)	A vulnerability was found in SourceCodester Multi Restaurant Table Reservation System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /dashboard/menu-list. php. The manipulation of the argument Area leads to cross-site scripting. The identification of this vulnerability is CVE-2020-36553. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2169	Loading Page with Loading Screen Plugin up to 1.0.82 on WordPress cross-site scripting	A vulnerability was found in Loading Page with Loading Screen Plugin up to 1.0.82 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-2169. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2187	zadam trilium up to 0.52.3/0.53.0 cross-site scripting	A vulnerability classified as problematic has been found in zadam trilium up to 0.52.3/0.53.0. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2290. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2168	SourceCodester Hotel Management System 2.0 Room Edit Page 1 massageroomDetails cross-site scripting	A vulnerability classified as problematic has been found in SourceCodester Hotel Management System 2.0. Affected is an unknown function of the file /ci_hms/massage_room/edit/1 of the component Room Edit Page. The manipulation of the argument massageroomDetails with the input "><script>alert< /script> leads to cross-site scripting. This vulnerability is traded as CVE-2022-2292. It is possible to launch the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2173	SourceCodester Simple Sales Management System 1.0 create customer_name cross-site scripting	A vulnerability classified as problematic was found in SourceCodester Simple Sales Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /ci_ssms /index.php/orders/create. The manipulation of the argument customer_name with the input <script>alert</script> leads to cross-site scripting. This vulnerability is known as CVE-2022-2293. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2090	SourceCodester Hotel Management System 2.0 Search /ci_hms/search crosssite scripting	A vulnerability was found in SourceCodester Hotel Management System 2.0. It has been rated as problematic. This issue affects some unknown processing of the file /ci_hms/search of the component Search. The manipulation of the argument search with the input "><script>alert</script> leads to crosssite scripting. The identification of this vulnerability is CVE-2022-2291. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2186	Microweber up to 1.2.18 cross-site scripting	A vulnerability was found in Microweber up to 1.2.18. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2300. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2194	Ninja Forms Contact Form Plugin up to 3.6.9 on WordPress Data Import cross-site scripting	A vulnerability which was classified as problematic was found in Ninja Forms Contact Form Plugin up to 3.6.9. This affects an unknown part of the component Data Import Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2021-25066. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2151	Ninja Forms Contact Form Plugin up to 3.6.9 Field Label cross-site scripting	A vulnerability which was classified as problematic has been found in Ninja Forms Contact Form Plugin up to 3.6.9. Affected by this issue is some unknown functionality of the component Field Label Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2021-25056. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2146	Redirection for Contact Form 7 Plugin up to 2.4.x on WordPress Attribute cross-site scripting	A vulnerability has been found in Redirection for Contact Form 7 Plugin up to 2.4.x and classified as problematic. This vulnerability affects unknown code of the component Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-0250. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1933	WP Contact Slider Plugin up to 2.4.6 on WordPress Text to Display Settings cross-site scripting	A vulnerability was found in WP Contact Slider Plugin up to 2.4.6 and classified as problematic. This issue affects some unknown processing of the component Text to Display Settings. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1301. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2149	SourceCodester Zoo Management System 1.0 Add Classification cross-site scripting (ID 167603)	A vulnerability was found in SourceCodester Zoo Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Add Classification. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-33075. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2148	EQS Integrity Line up to 2022-07-01 Whistleblower Entry cross-site scripting	A vulnerability which was classified as problematic has been found in EQS Integrity Line up to 2022-07-01. Affected by this issue is some unknown functionality of the component Whistleblower Entry Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-34007. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2118	PESCMS 2.3.3 cross-site scripting	A vulnerability which was classified as problematic was found in PESCMS 2.3.3. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2021-31676. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2100	NextAuth.js up to 3.29.7/4.8.x Email Signin Endpoint crosssite scripting (GHSApg-jx-7f9g-9463)	A vulnerability was found in NextAuth.js up to 3.29.7/4.8.x. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Email Signin Endpoint. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-31127. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2114	Appfire Jira Misc Custom Fields App 2.4.6 on Atlassian Project Name cross-site scripting (SYSS-2022-039)	A vulnerability was found in Appfire Jira Misc Custom Fields App 2.4.6. It has been classified as problematic. This affects an unknown part of the component Project Name Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-32567. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-30982	EidoGo SGF crosssite scripting (ID 27)	A vulnerability was found in EidoGo. It has been rated as problematic. This issue affects some unknown processing of the component SGF Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2015-3172. 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 the scanner as cross-site scripting attack
CVE-2022-2101	outline up to 0.64.3 cross-site scripting	A vulnerability classified as problematic has been found in outline up to 0.64.3. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-2342. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-24692	Known 1.2.2 +2020061101 Your Name cross-site scripting	A vulnerability classified as problematic was found in Known 1.2.2 +2020061101. Affected by this vulnerability is an unknown functionality. The manipulation of the argument Your Name leads to cross-site scripting. This vulnerability is known as CVE-2022-31290. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-36131	SourceCodester Simple Parking Management System 1.0 search cross-site scripting	A vulnerability which was classified as problematic has been found in SourceCodester Simple Parking Management System 1.0. Affected by this issue is some unknown functionality of the file /ci_spms/admin/search/searching/. The manipulation of the argument search with the input "><script>alert< /script> leads to cross-site scripting. This vulnerability is handled as CVE-2022-2363. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2470	SourceCodester Simple Parking Management System 1.0 / ci_spms/admin /category vehicle_type crosssite scripting	A vulnerability which was classified as problematic was found in SourceCodester Simple Parking Management System 1.0. This affects an unknown part of the file /ci_spms/admin/category. The manipulation of the argument vehicle_type with the input "> <script>alert</script> leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2364. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2115	Microweber 1.2.20 cross-site scripting	A vulnerability has been found in Microweber 1.2.20 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2353. 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 cross-site scripting attack
CVE-2022-2189	H3C SSL VPN up to 2022-07-10 wnm/login.json svpnlang cross-site scripting	A vulnerability which was classified as problematic was found in H3C SSL VPN up to 2022-07-10. Affected is an unknown function of the file wnm/login/login.json. The manipulation of the argument svpnlang leads to cross-site scripting. This vulnerability is traded as CVE-2022-35416. It is possible to launch the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2219	zadam trilium up to 0.53.2 cross-site scripting	A vulnerability classified as problematic was found in zadam trilium up to 0.53.2. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2365. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-0899	Transition Scheduler Add-on 6.5.0 on Atlassian Project Name cross-site scripting (SYSS-2022-040)	A vulnerability was found in Transition Scheduler Add-on 6.5.0 and classified as problematic. This issue affects some unknown processing of the component Project Name Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-32274. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2239	SourceCodester Simple e-Learning System 1.0 /vcs / claire_blake Bio cross-site scripting	A vulnerability classified as problematic was found in SourceCodester Simple e-Learning System 1.0. Affected by this vulnerability is an unknown functionality of the file /vcs/claire_blake. The manipulation of the argument Bio with the input "><script>alert</script> leads to cross-site scripting. This vulnerability is known as CVE-2022-2396. The attack can be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2514	Mogu Blog 5.2 cross-site scripting (ID 65)	A vulnerability was found in Mogu Blog 5.2. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-30517. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-34991	Portal do Software Publico Brasileiro i3geo 7.0.5 request_token.php cross-site scripting	A vulnerability classified as problematic has been found in Portal do Software Publico Brasileiro i3geo 7.0.5. This affects an unknown part of the file request_token.php. The manipulation leads to crosssite scripting. This vulnerability is uniquely identified as CVE-2022-34094. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-34988	Arox School ERP Pro 1.0 backoffice.inc.php dispatchcategory cross-site scripting	A vulnerability classified as problematic has been found in Arox School ERP Pro 1.0. Affected is an unknown function of the file backoffice.inc.php. The manipulation of the argument dispatchcategory leads to cross-site scripting. This vulnerability is traded as CVE-2022-32118. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2523	SourceCodester Multi Restaurant Table Reservation System 1.0 table-list.php Table Name cross-site scripting (EDB-49135)	A vulnerability was found in SourceCodester Multi Restaurant Table Reservation System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /dashboard/tablelist. php. The manipulation of the argument Table Name leads to cross-site scripting. This vulnerability is handled as CVE-2020-36550. The attack may be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-34962	Angular Cache cross-site scripting	A vulnerability was found in Angular. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Cache Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-25869. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2299	SourceCodester Multi Restaurant Table Reservation System 1.0 /dashboard/profile. php Restaurant Name cross-site scripting (EDB-49135)	A vulnerability classified as problematic was found in SourceCodester Multi Restaurant Table Reservation System 1.0. This vulnerability affects unknown code of the file /dashboard/profile. php. The manipulation of the argument Restaurant Name leads to cross-site scripting. This vulnerability was named CVE-2020-35261. The attack can be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-23099	SourceCodester Multi Restaurant Table Reservation System 1.0 /dashboard/menulist. php Made crosssite scripting (EDB-49135)	A vulnerability was found in SourceCodester Multi Restaurant Table Reservation System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /dashboard/menu-list. php. The manipulation of the argument Made leads to cross-site scripting. This vulnerability was named CVE-2020-36552. The attack can be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-34550	SourceCodester Multi Restaurant Table Reservation System 1.0 /dashboard/menulist.php Item Name cross-site scripting (EDB-49135)	A vulnerability was found in SourceCodester Multi Restaurant Table Reservation System 1.0. It has been classified as problematic. This affects an unknown part of the file /dashboard/menu-list.php. The manipulation of the argument Item Name leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2020-36551. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-34594	SourceCodester Multi Restaurant Table Reservation System 1.0 /dashboard/menulist. php Area (food_type) cross-site scripting (EDB-49135)	A vulnerability was found in SourceCodester Multi Restaurant Table Reservation System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /dashboard/menu-list. php. The manipulation of the argument Area leads to cross-site scripting. The identification of this vulnerability is CVE-2020-36553. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-34611	Loading Page with Loading Screen Plugin up to 1.0.82 on WordPress cross-site scripting	A vulnerability was found in Loading Page with Loading Screen Plugin up to 1.0.82 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-2169. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-27105	zadam trilium up to 0.52.3/0.53.0 cross-site scripting	A vulnerability classified as problematic has been found in zadam trilium up to 0.52.3/0.53.0. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2290. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-23101	SourceCodester Hotel Management System 2.0 Room Edit Page 1 massageroomDetails cross-site scripting	A vulnerability classified as problematic has been found in SourceCodester Hotel Management System 2.0. Affected is an unknown function of the file / ci_hms/massage_room/edit/1 of the component Room Edit Page. The manipulation of the argument massageroomDetails with the input "><script>alert< /script> leads to cross-site scripting. This vulnerability is traded as CVE-2022-2292. It is possible to launch the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2021-33371	SourceCodester Simple Sales Management System 1.0 create customer_name cross-site scripting	A vulnerability classified as problematic was found in SourceCodester Simple Sales Management System 1.0. Affected by this vulnerability is an unknown functionality of the file / ci_ssms /index.php/orders/create. The manipulation of the argument customer_name with the input <script>alert</script> leads to cross-site scripting. This vulnerability is known as CVE-2022-2293. The attack can be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-34009	SourceCodester Hotel Management System 2.0 Search /ci_hms/ search crosssite scripting	A vulnerability was found in SourceCodester Hotel Management System 2.0. It has been rated as problematic. This issue affects some unknown processing of the file /ci_hms/search of the component Search. The manipulation of the argument search with the input "><script>alert</script> leads to crosssite scripting. The identification of this vulnerability is CVE-2022-2291. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2016-2138	Microweber up to 1.2.18 cross-site scripting	A vulnerability was found in Microweber up to 1.2.18. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2300. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-34140	Ninja Forms Contact Form Plugin up to 3.6.9 on WordPress Data Import cross-site scripting	A vulnerability which was classified as problematic was found in Ninja Forms Contact Form Plugin up to 3.6.9. This affects an unknown part of the component Data Import Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2021-25066. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2016-2139	Ninja Forms Contact Form Plugin up to 3.6.9 Field Label cross-site scripting	A vulnerability which was classified as problematic has been found in Ninja Forms Contact Form Plugin up to 3.6.9. Affected by this issue is some unknown functionality of the component Field Label Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2021-25056. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-29360	Redirection for Contact Form 7 Plugin up to 2.4.x on WordPress Attribute cross-site scripting	A vulnerability has been found in Redirection for Contact Form 7 Plugin up to 2.4.x and classified as problematic. This vulnerability affects unknown code of the component Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-0250. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-34580	WP Contact Slider Plugin up to 2.4.6 on WordPress Text to Display Settings cross-site scripting	A vulnerability was found in WP Contact Slider Plugin up to 2.4.6 and classified as problematic. This issue affects some unknown processing of the component Text to Display Settings. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1301. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2579	SourceCodester Zoo Management System 1.0 Add Classification cross-site scripting (ID 167603)	A vulnerability was found in SourceCodester Zoo Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Add Classification. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-33075. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2016-3709	EQS Integrity Line up to 2022-07-01 Whistleblower Entry cross-site scripting	A vulnerability which was classified as problematic has been found in EQS Integrity Line up to 2022-07-01. Affected by this issue is some unknown functionality of the component Whistleblower Entry Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-34007. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-33994	PESCMS 2.3.3 cross-site scripting	A vulnerability which was classified as problematic was found in PESCMS 2.3.3. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2021-31676. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2290	NextAuth.js up to 3.29.7/4.8.x Email Signin Endpoint crosssite scripting (GHSApg-jx-7f9g-9463)	A vulnerability was found in NextAuth.js up to 3.29.7/4.8.x. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Email Signin Endpoint. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-31127. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2292	Appfire Jira Misc Custom Fields App 2.4.6 on Atlassian Project Name cross-site scripting (SYSS-2022-039)	A vulnerability was found in Appfire Jira Misc Custom Fields App 2.4.6. It has been classified as problematic. This affects an unknown part of the component Project Name Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-32567. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2293	EidoGo SGF crosssite scripting (ID 27)	A vulnerability was found in EidoGo. It has been rated as problematic. This issue affects some unknown processing of the component SGF Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2015-3172. 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 the scanner as cross-site scripting attack
CVE-2022-2291	outline up to 0.64.3 cross-site scripting	A vulnerability classified as problematic has been found in outline up to 0.64.3. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-2342. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2300	Known 1.2.2 +2020061101 Your Name cross-site scripting	A vulnerability classified as problematic was found in Known 1.2.2 +2020061101. Affected by this vulnerability is an unknown functionality. The manipulation of the argument Your Name leads to cross-site scripting. This vulnerability is known as CVE-2022-31290. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-25066	SourceCodester Management System 1.0 search cross-site scripting	A vulnerability which was classified as problematic has been found in Source-Codester Simple Parking Management System 1.0. Affected by this issue is some unknown function-ality of the file /ci_spms/admin/search/searching/. The manipulation of the argument search with the input "><scrip t>alert< /script> leads to cross-site script-ing. This vulnerability is handled as CVE-2022-2363. The attack may be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2021-25056	SourceCodester Simple Parking Man-agement System 1.0 / ci_spms/admin /cat-egory vehicle_type crosssite scripting	A vulnerability which was classified as problematic was found in Source-Codester Simple Parking Management System 1.0. This affects an unknown part of the file /ci_spms/admin/category. The manipulation of the argument vehicle_type with the input "> <script>alert</ script> leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2364. It is possible to initiate the attack re-motely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-0250	Microweber 1.2.20 cross-site scripting	A vulnerability has been found in Microweber 1.2.20 and classified as prob-lematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2353. The attack can be initiated remotely. There is no ex-ploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-1301	H3C SSL VPN up to 2022-07-10 wnm/ login /login.json svpnlang cross-site scripting	A vulnerability which was classified as problematic was found in H3C SSL VPN up to 2022-07-10. Affected is an unknown function of the file wnm/login/login. json. The manipulation of the argument svpnlang leads to cross-site script-ing. This vulnerability is traded as CVE-2022-35416. It is possible to launch the attack remotely. Further-more, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-33075	zadam trilium up to 0.53.2 cross-site scripting	A vulnerability classified as problematic was found in zadam trilium up to 0.53.2. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2365. The attack can be initiated remotely. There is no ex-ploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-34007	Transition Scheduler Add-on 6.5.0 on Atlassian Project Name cross-site scripting (SYSS-2022-040)	A vulnerability was found in Transition Scheduler Add-on 6.5.0 and classified as problematic. This issue affects some unknown processing of the component Project Name Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-32274. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2021-31676	SourceCodester Simple e-Learning System 1.0 /vcs / claire_blake Bio cross-site scripting	A vulnerability classified as problematic was found in SourceCodester Simple e-Learning System 1.0. Affected by this vulnerability is an unknown functionality of the file /vcs/claire_blake. The manipulation of the argument Bio with the input "><script>alert</script> leads to cross-site scripting. This vulnerability is known as CVE-2022-2396. The attack can be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-31127	Mogu Blog 5.2 cross-site scripting (ID 65)	A vulnerability was found in Mogu Blog 5.2. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-30517. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-32567	Portal do Software Publico Brasileiro i3geo 7.0.5 request_token.php cross-site scripting	A vulnerability classified as problematic has been found in Portal do sileiro i3geo 7.0.5. This affects an unknown part of the file request_token.php. The manipulation leads to crosssite scripting. This vulnerability is uniquely identified as CVE-2022-34094. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2015-3172	Arox School ERP Pro 1.0 backoffice.inc.php dispatchcategory cross-site scripting	A vulnerability classified as problematic has been found in Arox School ERP Pro 1.0. Affected is an unknown function of the file backoffice.inc.php. The manipulation of the argument dispatchcategory leads to cross-site scripting. This vulnerability is traded as CVE-2022-32118. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2342	SourceCodester Multi Restaurant Table Reservation System 1.0 table-list.php Table Name cross-site scripting (EDB-49135)	A vulnerability was found in SourceCodester Multi Restaurant Table Reservation System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /dashboard/tablelist. php. The manipulation of the argument Table Name leads to cross-site scripting. This vulnerability is handled as CVE-2020-36550. The attack may be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-31290	Angular Cache cross-site scripting	A vulnerability was found in Angular. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Cache Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-25869. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2363	SourceCodester Multi Restaurant Table Reservation System 1.0 /dashboard/profile.php Restaurant Name cross-site scripting (EDB-49135)	A vulnerability classified as problematic was found in SourceCodester Multi Restaurant Table Reservation System 1.0. This vulnerability affects unknown code of the file /dashboard/profile. php. The manipulation of the argument Restaurant Name leads to cross-site scripting. This vulnerability was named CVE-2020-35261. The attack can be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2364	SourceCodester Multi Restaurant Table Reservation System 1.0 /dashboard/menulist. php Made crosssite scripting (EDB-49135)	A vulnerability was found in SourceCodester Multi Restaurant Table Reservation System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /dashboard/menulist. php. The manipulation of the argument Made leads to cross-site scripting. This vulnerability was named CVE-2020-36552. The attack can be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2353	SourceCodester Multi Restaurant Table Reservation System 1.0 /dashboard/menulist. php Item Name cross-site scripting (EDB-49135)	A vulnerability was found in SourceCodester Multi Restaurant Table Reservation System 1.0. It has been classified as problematic. This affects an unknown part of the file /dashboard/menu-list.php. The manipulation of the argument Item Name leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2020-36551. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-35416	SourceCodester Multi Restaurant Table Reservation System 1.0 /dashboard/menulist.php Area (food_type) cross-site scripting (EDB-49135)	A vulnerability was found in SourceCodester Multi Restaurant Table Reservation System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /dashboard/menulist.php. The manipulation of the argument Area leads to cross-site scripting. The identification of this vulnerability is CVE-2020-36553. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2365	Loading Page with Loading Screen Plugin up to 1.0.82 on WordPress cross-site scripting	A vulnerability was found in Loading Page with Loading Screen Plugin up to 1.0.82 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-2169. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-32274	zadam trilium up to 0.52.3/0.53.0 cross-site scripting	A vulnerability classified as problematic has been found in zadam trilium up to 0.52.3/0.53.0. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2290. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2396	SourceCodester Hotel Management System 2.0 Room Edit Page 1 massageroomDetails cross-site scripting	A vulnerability classified as problematic has been found in SourceCodester Hotel Management System 2.0. Affected is an unknown function of the file /ci_hms/massage_room/edit/1 of the component Room Edit Page. The manipulation of the argument massageroomDetails with the input "><script>alert< /script> leads to cross-site scripting. This vulnerability is traded as CVE-2022-2292. It is possible to launch the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-30517	SourceCodester Simple Sales Management System 1.0 create customer_name cross-site scripting	A vulnerability classified as problematic was found in SourceCodester Simple Sales Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /ci_ssms /index.php/orders/create. The manipulation of the argument customer_name with the input <script>alert</script> leads to cross-site scripting. This vulnerability is known as CVE-2022-2293. The attack can be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-34094	SourceCodester Hotel Management System 2.0 Search /ci_hms/search crosssite scripting	A vulnerability was found in SourceCodester Hotel Management System 2.0. It has been rated as problematic. This issue affects some unknown processing of the file /ci_hms/search of the component Search. The manipulation of the argument search with the input "><script>alert</script> leads to crosssite scripting. The identification of this vulnerability is CVE-2022-2291. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-32118	Microweber up to 1.2.18 cross-site scripting	A vulnerability was found in Microweber up to 1.2.18. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2300. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2020-36550	Ninja Forms Contact Form Plugin up to 3.6.9 on WordPress Data Import cross-site scripting	A vulnerability which was classified as problematic was found in Ninja Forms Contact Form Plugin up to 3.6.9. This affects an unknown part of the component Data Import Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2021-25066. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-25869	Ninja Forms Contact Form Plugin up to 3.6.9 Field Label cross-site scripting	vulnerability which was classified as problematic has been found in Ninja Forms Contact Form Plugin up to 3.6.9. Affected by this issue is some unknown functionality of the component Field Label Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2021-25056. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2020-35261	Redirection for Contact Form 7 Plugin up to 2.4.x on WordPress Attribute cross-site scripting	A vulnerability has been found in Redirection for Contact Form 7 Plugin up to 2.4.x and classified as problematic. This vulnerability affects unknown code of the component Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-0250. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2020-36552	WP Contact Slider Plugin up to 2.4.6 on WordPress Text to Display Settings cross-site scripting	A vulnerability was found in WP Contact Slider Plugin up to 2.4.6 and classified as problematic. This issue affects some unknown processing of the component Text to Display Settings. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1301. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2020-36551	SourceCodester Zoo Management System 1.0 Add Classification (ID 167603)	A vulnerability was found in SourceCodester Zoo Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Add Classification. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-33075. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2020-36553	EQS Integrity Line up to 2022-07-01 Whistleblower Entry cross-site scripting	A vulnerability which was classified as problematic has been found in EQS Integrity Line up to 2022-07-01. Affected by this issue is some unknown functionality of the component Whistleblower Entry Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-34007. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2169	PESCMS 2.3.3 cross-site scripting	A vulnerability which was classified as problematic was found in PESCMS 2.3.3. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2021-31676. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2187	Contact Form 7 Captcha Plugin up to 0.1.1 on WordPress Web Browser REQUEST_URI cross-site scripting	A vulnerability was found in Contact Form 7 Captcha Plugin up to 0.1.1. It has been rated as problematic. This issue affects some unknown processing of the component Web Browser Handler. The manipulation of the argument REQUEST_URI leads to cross-site scripting. The identification of this vulnerability is CVE-2022-2187. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2168	Download Manager Plugin up to 3.2.43 on WordPress History Dashboard cross-site scripting	A vulnerability has been found in Download Manager Plugin up to 3.2.43 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component History Dashboard. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-2168. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2173	Advanced Database Cleaner Plugin up to 3.1.0 on WordPress Admin Dashboard cross-site scripting	A vulnerability was found in Advanced Database Cleaner Plugin up to 3.1.0. It has been classified as problematic. This affects an unknown part of the component Admin Dashboard. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2173. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2090	Discount Rules for WooCommerce Plugin up to 2.4.1 on WordPress a crosssite scripting	A vulnerability classified as problematic was found in Discount Rules for WooCommerce Plugin up to 2.4.1. Affected by this vulnerability is an unknown functionality. The manipulation of the argument a lead to cross-site scripting. This vulnerability is known as CVE-2022-2090. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2186	Simple Post Notes Plugin up to 1.7.5 on WordPress cross-site scripting	A vulnerability was found in Simple Post Notes Plugin up to 1.7.5. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2186. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2194	Accept Stripe Payments Plugin up to 2.0.63 on WordPress Setting cross-site scripting	A vulnerability classified as problematic has been found in Accept Stripe Payments Plugin up to 2.0.63. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-2194. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2151	Best Contact Management Software Plugin up to 3.7.3 on WordPress cross-site scripting	A vulnerability which was classified as problematic was found in Best Contact Management Software Plugin up to 3.7.3. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-2151. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2146	Import CSV Files Plugin up to 1.0 on WordPress cross-site scripting	A vulnerability classified as problematic was found in Import CSV Files Plugin up to 1.0. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-2146. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-1933	CDI Plugin up to 5.1.8 on WordPress AJAX Action cross-site scripting	A vulnerability was found in CDI Plugin up to 5.1.8 and classified as problematic. This issue affects some unknown processing of the component AJAX Action Handler. The manipulation leads to crosssite scripting. The identification of this vulnerability is CVE-2022-1933. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2149	Very Simple Breadcrumb Plugin up to 1.0 on WordPress cross-site scripting	A vulnerability which was classified as problematic has been found in Very Simple Breadcrumb Plugin up to 1.0. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-2149. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2148	LinkedIn Company Updates Plugin up to 1.5.3 on WordPress Setting cross-site scripting	A vulnerability classified as problematic was found in LinkedIn Company Updates Plugin up to 1.5.3. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2148. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2118	404s Plugin up to 3.5.0 on WordPress Field cross-site scripting	A vulnerability was found in 404s Plugin up to 3.5.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Field Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-2118. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2100	Page Generator Plugin up to 1.6.4 on WordPress Setting cross-site scripting	A vulnerability was found in Page Generator Plugin up to 1.6.4. It has been classified as problematic. Affected is an unknown function of the component Setting Handler. The manipulation leads to crosssite scripting. This vulnerability is traded as CVE-2022-2100. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2114	Supsystic Data Tables Generator Plugin up to 1.10.19 on WordPress crosssite scripting	A vulnerability was found in Supsystic Data Tables Generator Plugin up to 1.10.19. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-2114. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-30982	Gentics CMS up to 5.43.0 profile description/username cross-site scripting	A vulnerability classified as problematic was found in Gentics CMS up to 5.43.0. This vulnerability affects unknown code. The manipulation of the argument profile description/username leads to cross-site scripting. This vulnerability was named CVE-2022-30982. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2101	Download Manager Plugin up to 3.2.46 on WordPress file[files][] cross-site scripting	A vulnerability has been found in Download Manager Plugin up to 3.2.46 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument file[files][] leads to cross-site scripting. This vulnerability was named CVE-2022-2101. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-24692	DSK DSKNet 2.16.136.0/2.17.136.5 cross-site scripting	A vulnerability was found in DSK DSKNet 2.16.136.0/2.17.136.5. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-24692. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-36131	Better PDF Exporter Add-on 10.0.0 on Jira PDF Templates Overview Page description cross-site scripting (SYSS-2022-038)	A vulnerability was found in Better PDF Exporter Add-on 10.0.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component PDF Templates Overview Page. The manipulation of the argument description leads to crosssite scripting. This vulnerability is handled as CVE-2022-36131. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2470	Microweber up to 1.2.20 cross-site scripting	A vulnerability classified as problematic has been found in Microweber up to 1.2.20. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-2470. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2115	Popup Anything Plugin up to 2.1.6 on WordPress Frontend Page cross-site scripting	A vulnerability which was classified as problematic was found in Popup Anything Plugin up to 2.1.6. Affected is an unknown function of the component Frontend Page. The manipulation leads to crosssite scripting. This vulnerability is traded as CVE-2022-2115. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2189	WP Video Lightbox Plugin up to 1.9.4 on WordPress REQUEST_URI cross-site scripting	A vulnerability has been found in WP Video Lightbox Plugin up to 1.9.4 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument REQUEST_URI leads to cross-site scripting. This vulnerability is known as CVE-2022-2189. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2219	Unyson Plugin up to 2.7.26 on WordPress cross-site scripting	A vulnerability was found in Unyson Plugin up to 2.7.26. 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-2022-2219. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-0899	Header Footer Code Manager Plugin up to 1.1.23 on WordPress Admin Page crosssite scripting	A vulnerability which was classified as problematic has been found in Header Footer Code Manager Plugin up to 1.1.23. This issue affects some unknown processing of the component Admin Page. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-0899. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2239	Request a Quote Plugin up to 2.3.7 on WordPress Setting cross-site scripting	A vulnerability was found in Request a Quote Plugin up to 2.3.7. 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-2022-2239. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2514	Fava up to 1.21 Error Message time/filter cross-site scripting	A vulnerability classified as problematic was found in Fava up to 1.21. This vulnerability affects unknown code of the component Error Message Handler. The manipulation of the argument time/filter leads to cross-site scripting. This vulnerability was named CVE-2022-2514. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-34991	Paymoney 3.3 first_name/last_name cross-site scripting	A vulnerability was found in Paymoney 3.3. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument first_name /last_name leads to cross-site scripting. This vulnerability is known as CVE-2022-34991. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-34988	Inout Blockchain AltExchanger 1.2.1 / admin/js cross-site scripting	A vulnerability was found in Inout Blockchain AltExchanger 1.2.1. It has been classified as problematic. Affected is an unknown function of the file /admin/js. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-34988. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2523	beancount fava up to 1.22.1 cross-site scripting	A vulnerability was found in beancount fava up to 1.22.1 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-2523. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-34962	OpenTeknik OSSN Open Source Social Network 6.3 LTS Group Timeline Module cross-site scripting	A vulnerability which was classified as problematic has been found in Open Teknik OSSN Open Source Social Network 6.3 LTS. This issue affects some unknown processing of the component Group Timeline Module. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-34962. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2299	Allow SVG Files Plugin up to 1.1 on WordPress cross-site scripting	A vulnerability was found in Allow SVG Files Plugin up to 1.1. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2299. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-23099	OX Software OX App Suite up to 7.10.6 cross-site scripting	A vulnerability was found in OX Software OX App Suite up to 7.10.6. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-23099. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-34550	Sims 1.0 /addNotifyServlet notifyInfo cross-site scripting	A vulnerability has been found in Sims 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file / addNotifyServlet. The manipulation of the argument notifyInfo leads to cross-site scripting. This vulnerability is known as CVE-2022-34550. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-34594	Advanced School Management System 1.0 update_subject.php Edit Subject cross-site scripting	A vulnerability which was classified as problematic was found in Advanced School Management System 1.0. This affects an unknown part of the file ip/school/moudel/update_subject.php. The manipulation of the argument Edit Subject leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-34594. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-34611	Online Fire Reporting System 1.0 /index.php/ Contac # cross-site scripting	A vulnerability was found in Online Fire Reporting System 1.0 and classified as problematic. This issue affects some unknown processing of the file / index.php/preport. The manipulation of the argument Contac leads to cross-site scripting. The identification of this vulnerability is CVE-2022-34611. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-27105	InMailX Outlook Plugin prior 3.22.0101 Connection Name cross-site scripting	A vulnerability which was classified as problematic was found in InMailX Outlook Plugin. Affected is an unknown function of the component Connection Name Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-27105. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-23101	OX Software OX App Suite up to 7.10.6 EMail Message appHandler cross-site scripting	A vulnerability classified as problematic has been found in OX Software OX App Suite up to 7.10.6. This affects the function appHandler of the component E-Mail Message Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-23101. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2021-33371	Student Management System 1.0 Chat Box /nav_bar_action.php (ID 49865 / EDB-49865)	A vulnerability was found in Student Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /nav_bar_action.php of the component Chat Box. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2021-33371. The attack can be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-34009	Fossil 2.18 on Windows Ticket crosssite scripting	A vulnerability was found in Fossil 2.18. It has been classified as problematic. Affected is an unknown function of the component Ticket Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-34009. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2016-2138	kippo-graph up to 1.5.0 KippoInput.class.php xss_clean cross-site scripting (ID 35)	A vulnerability classified as problematic was found in kippo-graph up to 1.5.0. Affected by this vulnerability is the function xss_clean of the file class/KippoInput.class.php. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2016-2138. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-34140	Feehi CMS 2.1.1 index.php username cross-site scripting (ID 61)	A vulnerability classified as problematic was found in Feehi CMS 2.1.1. Affected by this vulnerability is an unknown functionality of the file /index.phpr-site%2Fsignup. The manipulation of the argument username leads to cross-site scripting. This vulnerability is known as CVE-2022-34140. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2016-2139	kippo-graph up to 1.5.0 KippoInput.class.php file_link cross-site scripting (ID 35)	A vulnerability classified as problematic has been found in kippograph up to 1.5.0. Affected is an unknown function of the file class /KippoInput.class.php. The manipulation of the argument file_link leads to cross-site scripting. This vulnerability is traded as CVE-2016-2139. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-29360	RainLoop up to 1.6.0 Email Viewer cross-site scripting	A vulnerability which was classified as problematic was found in RainLoop up to 1.6.0. This affects an unknown part of the component Email Viewer. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-29360. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-34580	itsourcecode Advanced School Management System 1.0 ip/school/index.php address crosssite scripting	A vulnerability was found in itsourcecode Advanced School Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file ip /school/index.php. The manipulation of the argument address leads to cross-site scripting. This vulnerability is known as CVE-2022-34580. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2022-2579	SourceCodester Garage Management System 1.0 createUser.php userName cross-site scripting	A vulnerability which was classified as problematic was found in SourceCodester Garage Management System 1.0. Affected is an unknown function of the file /php_action/createUser.php. The manipulation of the argument userName with the input lala<img src"" onerroralert> leads to cross-site scripting. This vulnerability is traded as CVE-2022-2579. It is possible to launch the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack
CVE-2016-3709	libxml 960f0e2 crosssite scripting	A vulnerability was found in libxml 960f0e2. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2016-3709. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-33994	Gutenberg Plugin up to 13.7.3 on Word-Press SVG Document cross-site scripting	A vulnerability which was classified as problematic was found in Gutenberg Plugin up to 13.7.3. This affects an unknown part of the component SVG Document Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-33994. It is possible to initiate the attack re-motely. There is no exploit available.	Protected by core rules	Detected by the scanner as cross-site scripting attack

Cross-Site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-25046	CWP 0.9.8.1122 POST Request loader. php path traversal	A vulnerability was found in CWP 0.9.8.1122 and clas-sified as critical. This issue affects some unknown processing of the file loader.php of the com-ponent POST Request Handler. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-25046. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-35410	Metadata Anonymi-sation Toolkit up to 0.12.x ZIP Archive path traversal (ID 174)	A vulnerability was found in Metadata Anonymisa-tion Toolkit up to 0.12.x. It has been rated as prob-lematic. This issue affects some unknown processing of the component ZIP Archive Handler. The manipulation leads to path traversal: &039;../file-dir&039;. The identification of this vulnerability is CVE-2022-35410. 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 the scanner as Local File Inclusion attack
CVE-2022-31565	yogson syrabond up to 2020-05-25 send_file path tra-versal (ID 669)	A vulnerability was found in yogson syrabond up to 2020-05-25. It has been declared as critical. Affect-ed by this vulnerability is the function send_file. The manipulation leads to path traversal. This vulnerability is known as CVE-2022-31565. The attack needs to be ap-proached within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31551	pleomax00 flaskmon-go-skel up to 2012-11-01 send_file path traversal (ID 669)	A vulnerability which was classified as critical has been found in pleomax00 flask-mongo-skel up to 2012-11-01. This issue affects the function send_file. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-31551. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31579	ralphjzhang iasset up to 2022-05-04 send_file path traversal (ID 669)	A vulnerability classified as critical has been found in ralphjzhang iasset up to 2022-05-04. Affected is the function send_file. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-31579. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31559	tsileo flask-yeoman up to 2013-09-13 send_file path traversal (ID 669)	A vulnerability classified as critical was found in tsileo flaskyeoman up to 2013-09-13. Affected by this vulnerability is the function send_file. The manipulation leads to path traversal. This vulnerability is known as CVE-2022-31559. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31568	Rexians rex-web up to 2022-06-05 send_file path traversal (ID 669)	A vulnerability classified as critical has been found in Rexians rex-web up to 2022-06-05. This affects the function send_file. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-31568. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31558	tooxie shiva-server up to 0.10.0 send_file path traversal (ID 669)	A vulnerability classified as critical has been found in tooxie shiva-server up to 0.10.0. Affected is the function send_file. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-31558. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31545	ml-inory ModelConverter up to 2021-04-26 send_file path traversal (ID 669)	A vulnerability was found in ml-inory ModelConverter up to 2021-04-26 and classified as critical. This issue affects the function send_file. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-31545. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31530	csm up to 3.5 send_file path traversal (ID 669)	A vulnerability classified as critical has been found in csm up to 3.5. This affects the function send_file. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-31530. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31566	DSAB up to 2019-02- 18 send_file path traversal (ID 669)	A vulnerability which was classified as critical has been found in DSAB up to 2019-02-18. This issue affects the function send_file. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-31566. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31556	rusyasoft TrainEnergyServer up to 2017-08-03 send_file path traversal (ID 669)	A vulnerability was found in rusyasoft TrainEnergyServer up to 2017-08-03. It has been declared as critical. This vulnerability affects the function send_file. The manipulation leads to path traversal. This vulnerability was named CVE-2022-31556. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31557	seveas golem up to 2016-05-17 send_file path traversal (ID 669)	A vulnerability was found in seveas golem up to 2016-05-17. It has been rated as critical. This issue affects the function send_file. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-31557. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31567	DSABenchmark DSAB up to 2.1 send_file path traversal (ID 669)	A vulnerability was found in DSABenchmark DSAB up to 2.1. It has been rated as critical. Affected by this issue is the function send_file. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-31567. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31561	varijkapil13 Sphere_ImageBackend up to 2019-10-03 send_file path traversal (ID 669)	A vulnerability which was classified as critical was found in varijkapil13 Sphere_ImageBackend up to 2019-10-03. This affects the function send_file. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-31561. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31569	RipudamanKaushikDal projects up to 2022-04-03 send_file path traversal (ID 669)	A vulnerability classified as critical was found in RipudamanKaushikDal projects up to 2022-04-03. This vulnerability affects the function send_file. The manipulation leads to path traversal. This vulnerability was named CVE-2022-31569. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31586	unizar-30226-2019-06 ChangePop-Back up to 2019-06-04 send_file path traversal (ID 669)	A vulnerability was found in unizar-30226-2019-06 ChangePop-Back up to 2019-06-04. It has been classified as critical. Affected is the function send_file. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-31586. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31546	nlpweb glance up to 2014-06-27 send_file path traversal (ID 669)	A vulnerability was found in nlpweb glance up to 2014-06-27. It has been classified as critical. Affected is the function send_file. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-31546. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31552	anuvaad corpus up to 2020-11-23 send_file path traversal (ID 669)	A vulnerability which was classified as critical was found in anuvaad corpus up to 2020-11-23. Affected is the function send_file. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-31552. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31563	whmacmac vprj up to 2022-04-06 send_file path traversal (ID 669)	A vulnerability was found in whmacmac vprj up to 2022-04-06 and classified as critical. This issue affects the function send_file. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-31563. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31570	adriankoczuruek ceneo-web-scrapper up to 2021-03-15 send_file path traversal (ID 669)	A vulnerability which was classified as critical has been found in adriankoczuruek ceneo-web-scrapper up to 2021-03-15. This issue affects the function send_file. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-31570. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31583	sravaniboinepelli AutomatedQuizEval up to 2020-04-27 send_file path traversal (ID 669)	A vulnerability has been found in sravaniboinepelli AutomatedQuizEval up to 2020-04-27 and classified as critical. This vulnerability affects the function send_file. The manipulation leads to path traversal. This vulnerability was named CVE-2022-31583. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31553	rainsoupah sleeplearner up to 2021-02-21 send_file path traversal (ID 669)	A vulnerability has been found in rainsoupah sleep-learner up to 2021-02-21 and classified as critical. Affected by this vulnerability is the function send_file. The manipulation leads to path traversal. This vulnerability is known as CVE-2022-31553. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31550	olmax99 pyathenastack up to 2019-11-08 send_file path traversal (ID 669)	A vulnerability classified as critical was found in olmax99 pyathenastack up to 2019-11-08. This vulnerability affects the function send_file. The manipulation leads to path traversal. This vulnerability was named CVE-2022-31550. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31562	waveyan internshipsystem up to 2018-05-22 send_file path traversal (ID 669)	A vulnerability has been found in waveyan internshipsystem up to 2018-05-22 and classified as critical. This vulnerability affects the function send_file. The manipulation leads to path traversal. This vulnerability was named CVE-2022-31562. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31549	olmax99 helm-flask-celery prior 2022-05-25 send_file path traversal (ID 669)	A vulnerability classified as critical has been found in olmax99 helm-flask-celery. This affects the function send_file. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-31549. Access to the local network is required for this attack. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31580	sanojtharindu caretakerr-api up to 2021-05-17 send_file path traversal (ID 669)	A vulnerability classified as critical was found in sanojtharindu caretakerr-api up to 2021-05-17. Affected by this vulnerability is the function send_file. The manipulation leads to path traversal. This vulnerability is known as CVE-2022-31580. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31587	yuriyouzhou KGfashion-chatbot up to 2018-05-22 send_file path traversal (ID 669)	A vulnerability was found in yuriyouzhou KG-fashion-chatbot up to 2018-05-22. It has been declared as critical. Affected by this vulnerability is the function send_file. The manipulation leads to path traversal. This vulnerability is known as CVE-2022-31587. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31560	uncleYiba photo_tag up to 2020-08-31 send_file path traversal (ID 669)	A vulnerability which was classified as critical has been found in uncleYiba photo_tag up to 2020-08-31. Affected by this issue is the function send_file. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-31560. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31588	zippies testplatform up to 2016-07-19 send_file path traversal (ID 669)	A vulnerability was found in zippies testplatform up to 2016-07-19. It has been rated as critical. Affected by this issue is the function send_file. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-31588. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31577	longmaoteamtf audio_aligner_app up to 2020-01-10 send_file path traversal (ID 669)	A vulnerability was found in longmaoteamtf audio_aligner_app up to 2020-01-10. It has been declared as critical. This vulnerability affects the function send_file. The manipulation leads to path traversal. This vulnerability was named CVE-2022-31577. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31582	shaolo1 VideoServer up to 2019-09-21 send_file path traversal (ID 669)	A vulnerability which was classified as critical was found in shaolo1 VideoServer up to 2019-09-21. This affects the function send_file. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-31582. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31564	woduq1414 munhakmoa prior 2022-05-03 send_file path traversal (ID 669)	A vulnerability was found in woduq1414 munhak-moa. It has been classified as critical. Affected is the function send_file. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-31564. Access to the local network is required for this attack to succeed. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as Local File Inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31573	chainer chainer-rlvisualizer up to 0.1.1 send_file path traversal (ID 669)	A vulnerability has been found in chainer chainer-rl-visualizer up to 0.1.1 and classified as critical. Affected by this vulnerability is the function send_file. The manipulation leads to path traversal. This vulnerability is known as CVE-2022-31573. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31554	rohitnayak moviere-view- sentimentanal-ysis up to 2017-05-07 send_file path traversal (ID 669)	A vulnerability was found in rohitnayak movie-review-sentimentanalysis up to 2017-05-07 and classified as critical. Affected by this issue is the function send_file. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-31554. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31578	piaoyunsoft bt_lnmp up to 2019-10-10 send_file path traversal (ID 669)	A vulnerability was found in piaoyunsoft bt_lnmp up to 2019-10-10. It has been rated as critical. This issue affects the function send_file. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-31578. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31576	heidi-luong1109 shackerpanel up to 2021-05-25 send_file path traversal (ID 669)	A vulnerability was found in heidi-luong1109 shackerpanel up to 2021-05-25. It has been classified as critical. This affects the function send_file. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-31576. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31574	deepaliupadhyay RealEstate up to 2018-11-30 send_file path traversal (ID 669)	A vulnerability was found in Deepali Upadhyay RealEstate up to 2018-11-30 and classified as critical. Affected by this issue is the function send_file. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-31574. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31584	stonethree s3label up to 2019-08-14 send_file path traversal (ID 669)	A vulnerability was found in stonethree s3label up to 2019-08-14 and classified as critical. This issue affects the function send_file. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-31584. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31581	scorelab OpenMF prior 2022-05-03 send_file path traversal (ID 669)	A vulnerability which was classified as critical has been found in scorelab OpenMF. Affected by this issue is the function send_file. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-31581. Access to the local network is required for this attack to succeed. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31572	ceee-vip cockybook up to 2015-04-16 send_file path traversal (ID 669)	A vulnerability which was classified as critical was found in ceee-vip cockybook up to 2015-04-16. Affected is the function send_file. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-31572. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31555	romain20100 nursequest up to 2018-02-22 send_file path traversal (ID 669)	A vulnerability was found in romain20100 nursequest up to 2018-02-22. It has been classified as critical. This affects the function send_file. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-31555. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31547	noamezekiel sphere up to 2020-05-31 send_file path traversal (ID 669)	A vulnerability was found in noamezekiel sphere up to 2020-05- 31. It has been declared as critical. Affected by this vulnerability is the function send_file. The manipulation leads to path traversal. This vulnerability is known as CVE-2022-31547. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31521	Niyaz-Mohamed mosaic up to 1.0.0 send_file path traversal (ID 669)	A vulnerability classified as critical was found in Niyaz-Mohamed mosaic up to 1.0.0. Affected by this vulnerability is the function send_file. The manipulation leads to path traversal. This vulnerability is known as CVE-2022-31521. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31502	operatorequals wormnest up to 0.4.7 send_file path traversal (ID 669)	A vulnerability was found in operatorequals wormnest up to 0.4.7. It has been declared as critical. This vulnerability affects the function send_file. The manipulation leads to path traversal. This vulnerability was named CVE-2022-31502. The attack needs to be approached within the local network. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31524	PureStorage-OpenConnect swagger up to 1.1.5 send_file path traversal (ID 669)	A vulnerability has been found in PureStorage-OpenConnect swagger up to 1.1.5 and classified as critical. This vulnerability affects the function send_file. The manipulation leads to path traversal. This vulnerability was named CVE-2022-31524. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31505	cheo0 MercadoEnLineaBack up to 2022-05-04 send_file path traversal (ID 669)	A vulnerability was found in cheo0 MercadoEnLineaBack up to 2022-05-04. It has been declared as critical. Affected by this vulnerability is the function send_file. The manipulation leads to path traversal. This vulnerability is known as CVE-2022-31505. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31513	BolunHan Krypton up to 2021-06-03 send_file path traversal (ID 669)	A vulnerability was found in BolunHan Krypton up to 2021-06-03 and classified as critical. Affected by this issue is the function send_file. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-31513. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31526	ThundeRatz ThunderDocs up to 2020-05-01 send_file path traversal (ID 669)	A vulnerability was found in ThundeRatz ThunderDocs up to 2020-05-01. It has been classified as critical. Affected is the function send_file. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-31526. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31507	ganga up to 8.5.9 send_file path traversal (ID 669)	A vulnerability classified as critical has been found in ganga up to 8.5.9. This affects the function send_file. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-31507. 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 the scanner as Local File Inclusion attack
CVE-2022-31585	umeshpatil-dev Home__internet up to 2020-08-28 send_file path traversal (ID 669)	A vulnerability which was classified as critical was found in umeshpatil-dev Home__internet up to 2020-08-28. Affected is the function send_file. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-31585. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31517	HolgerGraef MSM up to 2021-04-20 send_file path traversal (ID 669)	A vulnerability was found in HolgerGraef MSM up to 2021-04-20. It has been declared as critical. This vulnerability affects the function send_file. The manipulation leads to path traversal. This vulnerability was named CVE-2022-31517. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31520	Luxas98 logstash-management-api up to 2020-05-04 send_file path traversal (ID 669)	A vulnerability classified as critical has been found in Luxas98 logstash-management-api up to 2020-05-04. Affected is the function send_file. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-31520. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31523	PaddlePaddle Anakin up to 0.1.1 send_file path traversal (ID 669)	A vulnerability which was classified as critical was found in PaddlePaddle Anakin up to 0.1.1. This affects the function send_file. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-31523. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31510	sergeKashkin Simple-RAT prior 2022-05-03 send_file path traversal (ID 669)	A vulnerability which was classified as critical was found in sergeKashkin Simple-RAT. Affected is the function send_file. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-31510. The attack needs to be approached within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31506	cmusatyalab opendiamond up to 10.1.1 send_file path traversal (ID 669)	A vulnerability was found in cmusatyalab opendiamond up to 10.1.1. It has been rated as critical. Affected by this issue is the function send_file. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-31506. The attack needs to be done within the local network. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31522	NotVinay karaokey up to 2019-12-11 send_file path traversal (ID 669)	A vulnerability which was classified as critical has been found in NotVinay karaokey up to 2019-12-11. Affected by this issue is the function send_file. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-31522. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31512	Atom02 flask-mvc up to 2020-09-14 send_file path traversal (ID 669)	A vulnerability has been found in Atom02 flask-mvc up to 2020-09-14 and classified as critical. Affected by this vulnerability is the function send_file. The manipulation leads to path traversal. This vulnerability is known as CVE-2022-31512. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31525	SummaLabs DLS up to 0.1.0 send_file path traversal (ID 669)	A vulnerability was found in SummaLabs DLS up to 0.1.0 and classified as critical. This issue affects the function send_file. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-31525. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31504	ChangeWeDer Baidu-WenkuSpider_flaskWeb prior 2021-11- 29 send_file path traversal (ID 669)	A vulnerability was found in ChangeWeDer Baidu-WenkuSpider_flaskWeb. It has been classified as critical. Affected is the function send_file. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-31504. The attack can only be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31509	iedadata usap-dc-website up to 1.0.1 send_file path traversal (ID 669)	A vulnerability which was classified as critical has been found in iedadata usap-dc-website up to 1.0.1. This issue affects the function send_file. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-31509. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31519	Lukasavicus WindMill up to 1.0 send_file path traversal (ID 669)	A vulnerability was found in Lukasavicus WindMill up to 1.0. It has been rated as critical. This issue affects the function send_file. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-31519. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31537	jmcginty15 Solarsystem-simulator up to 2021-07-26 send_file path traversal (ID 669)	A vulnerability was found in jmcginty15 Solar-system-simulator up to 2021-07-26. It has been classified as critical. This affects the function send_file. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-31537. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31575	duducosmos livro_python up to 2018-06-06 send_file path traversal (ID 669)	A vulnerability classified as critical was found in duducosmos livro_python up to 2018-06-06. This vulnerability affects the function send_file. The manipulation leads to path traversal. This vulnerability was named CVE-2022-31575. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31542	mandoku mdweb up to 2015-05-07 send_file path traversal (ID 669)	A vulnerability which was classified as critical has been found in mandoku mdweb up to 2015-05-07. Affected by this issue is the function send_file. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-31542. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31531	dainst cilantro up to 0.0.4 send_file path traversal (ID 669)	A vulnerability classified as critical was found in dainst cilantro up to 0.0.4. This vulnerability affects the function send_file. The manipulation leads to path traversal. This vulnerability was named CVE-2022-31531. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31540	kumardeepak hin-engpreprocess-ing up to 2019-07-16 send_file path traversal (ID 669)	A vulnerability classified as critical has been found in kumardeepak hin-eng-preprocessing up to 2019-07-16. Affected is the function send_file. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-31540. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31528	bonn-activity-maps bam_annotation_ tool up to 2021-08-31 send_file path traversal (ID 669)	A vulnerability was found in bonn-activity-maps bam_annotation_tool up to 2021-08-31. It has been declared as critical. Affect-ed by this vulnerability is the function send_file. The manipulation leads to path traversal. This vulnerability is known as CVE-2022-31528. Ac-cess to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31571	akashtalole python-flask- restful-api up to 2019-09-16 send_file path traversal (ID 669)	A vulnerability classified as critical has been found in akashtalole python-flask-restful-api up to 2019-09-16. This affects the function send_file. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-31571. The attack needs to be approached within the local network. There is no exploit avail-able.	Protected by core rules	Detected by the scanner as Local File Inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31539	kotekan up to 2021.11 send_file path traversal (ID 669)	A vulnerability was found in kotekan up to 2021.11. It has been rated as critical. This issue affects the function send_file. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-31539. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31538	joaopedro-fg mp-m08- interface up to 2020-12- 10 send_file path traversal (ID 669)	A vulnerability was found in joaopedro-fg mp-m08-interface up to 2020-12-10. It has been declared as critical. This vulnerability affects the function send_file. The manipulation leads to path traversal. This vulnerability was named CVE-2022-31538. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31532	dankolbman travel_blahg up to 2016-01-16 send_file path traversal (ID 669)	A vulnerability which was classified as critical has been found in dankolbman travel_blahg up to 2016-01-16. This issue affects the function send_file. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-31532. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31535	freefood89 Fishtank up to 2015-06-24 send_file path traversal (ID 669)	A vulnerability has been found in freefood89 Fishtank up to 2015-06-24 and classified as critical. Affected by this vulnerability is the function send_file. The manipulation leads to path traversal. This vulnerability is known as CVE-2022-31535. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31544	meerstein rbtm up to 1.5 send_file path traversal (ID 669)	A vulnerability has been found in meerstein rbtm up to 1.5 and classified as critical. This vulnerability affects the function send_file. The manipulation leads to path traversal. This vulnerability was named CVE-2022-31544. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31529	cinemaproject monorepo up to 2021-03-03 send_file path traversal (ID 669)	A vulnerability was found in cinemaproject monorepo up to 2021-03-03. It has been rated as critical. Affected by this issue is the function send_file. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-31529. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31541	lyubolp Barry-Voice-Assistant up to 2021-01-18 send_file path traversal (ID 669)	A vulnerability classified as critical was found in lyubolp Barry-Voice-Assistant up to 2021-01-18. Affected by this vulnerability is the function send_file. The manipulation leads to path traversal. This vulnerability is known as CVE-2022-31541. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31533	decentraminds umbral up to 2020-01-15 send_file path traversal (ID 669)	A vulnerability which was classified as critical was found in decentraminds umbral up to 2020-01-15. Affected is the function send_file. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-31533. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31534	echoleegroup PythonWeb up to 2018-10-31 send_file path traversal (ID 669)	A vulnerability was found in echoleegroup PythonWeb up to 2018-10-31. It has been rated as critical. Affected by this issue is the function send_file. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-31534. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31536	jaygarza1982 ytdl-sync up to 2021-01-02 send_file path traversal (ID 669)	A vulnerability was found in jaygarza1982 ytdl-sync up to 2021- 01-02 and classified as critical. Affected by this issue is the function send_file. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-31536. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31543	maxtortime SetupBox up to 1.0 send_file path traversal (ID 669)	A vulnerability which was classified as critical was found in maxtortime SetupBox up to 1.0. This affects the function send_file. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-31543. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31503	orchest prior 2022.05.0 send_file path traversal (ID 669)	A vulnerability was found in orchest and classified as critical. This issue affects the function send_file. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-31503. The attack needs to be approached within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as Local File Inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31501	ChaoticOnyx Onyx-Forum up to 2022-05-04 send_file path traversal (ID 669)	A vulnerability has been found in ChaoticOnyx OnyxForum up to 2022-05-04 and classified as critical. This vulnerability affects the function send_file. The manipulation leads to path traversal. This vulnerability was named CVE-2022-31501. Access to the local network is required for this attack to succeed. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-32409	Portal do Software Publico Brasileiro i3geo 7.0.5 HTTP Request codemirror.php file inclusion	A vulnerability which was classified as critical has been found in Portal do Software Publico Brasileiro i3geo 7.0.5. This issue affects some unknown processing of the file codemirror.php of the component HTTP Request Handler. The manipulation leads to file inclusion. The identification of this vulnerability is CVE-2022-32409. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-31159	AWS SDK for Java up to 1.12.260 S3 TransferManager downloadDirectory path traversal (GHSAc28r-hw5m-5gv3)	A vulnerability classified as critical has been found in AWS SDK for Java up to 1.12.260. This affects the function downloadDirectory of the component S3 TransferManager. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-31159. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-26352	dotCMS up to 22.02 ContentResource API filename pathname traversal (ID 167365)	A vulnerability was found in dotCMS up to 22.02 and classified as critical. This issue affects some unknown processing of the component ContentResource API. The manipulation of the argument filename leads to pathname traversal. The identification of this vulnerability is CVE-2022-26352. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-2400	dompdf up to 1.x file inclusion	A vulnerability was found in dompdf up to 1.x and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to file inclusion. This vulnerability is handled as CVE-2022-2400. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as Local File Inclusion attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-24659	Goldshell ASIC Miner up to 2.2.1 path traversal	A vulnerability was found in Goldshell ASIC Miner up to 2.2.1. It has been classified as critical. This affects an unknown part. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-24659. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2020-7649	snyk-broker up to 4.72.x pathname traversal	A vulnerability which was classified as problematic has been found in snyk-broker up to 4.72.x. This issue affects some unknown processing. The manipulation leads to pathname traversal. The identification of this vulnerability is CVE-2020-7649. The attack can only be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-34551	Sims 1.0 Attachment Download path traversal	A vulnerability which was classified as critical has been found in Sims 1.0. Affected by this issue is some unknown functionality of the component Attachment Download Handler. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-34551. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack
CVE-2022-34121	Cuppa CMS 1.0 right.php file inclusion (ID 18)	A vulnerability was found in Cuppa CMS 1.0. It has been classified as critical. Affected is an unknown function of the file/templates/default/html/windows/right.php. The manipulation leads to file inclusion. This vulnerability is traded as CVE-2022-34121. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as Local File Inclusion attack

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.