INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

September 2022

Total Zero-Day Vulnerabilities Found: 202

Command Injection	Local File Inclusion	SQL Injection	Cross-Site Scripting	Cross-Site Request Forgery
9	13	94	73	13

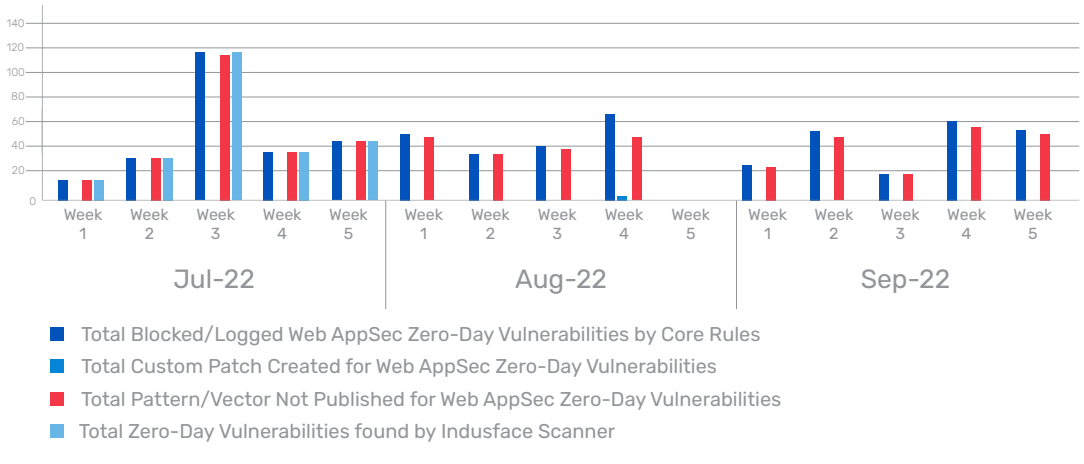
Zero-day vulnerabilities protected through core rules	202
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities for which protection can not be done	0
Zero-day vulnerabilities found by Indusface WAS	189

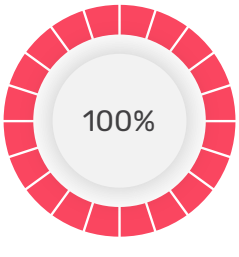
- To enable custom rules, please contact support@indusface.com
- Since the attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.

Vulnerability Trend:

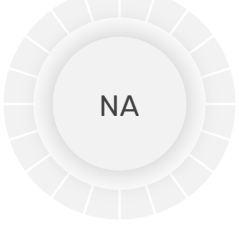
The weekly trend displays the total number of vulnerabilities discovered to the type of protection provided for the last quarter.

Weekly Vulnerability Trend

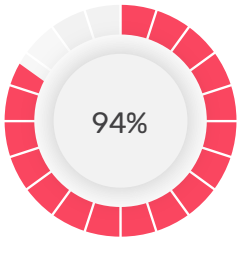




of the zero-day vulnerabilities were protected by the **core rules** in the last month.

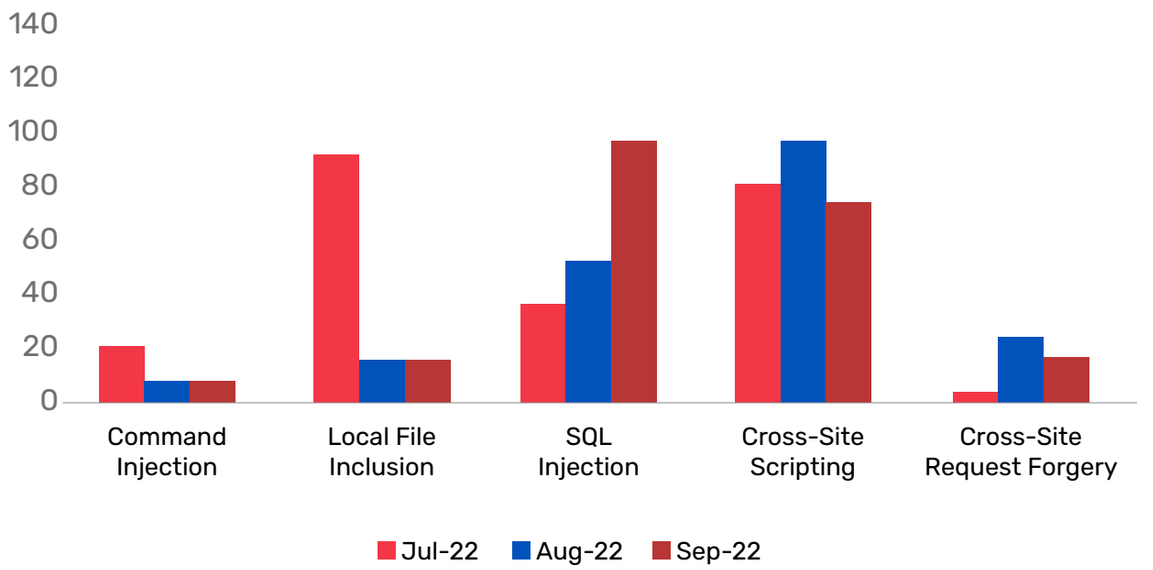


of the zero-day vulnerabilities were protected by the **custom rules** in the last month.



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

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-36566	yogeshojha Rengine 1.3.0 Scan Engine command injection	A vulnerability has been found in yogeshojha Rengine 1.3.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the component Scan Engine. The manipulation leads to command injection. This vulnerability is known as CVE-2022-36566. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as Command injection attack
CVE-2022-3008	tinygltf up to 2.5.x Backtick wordexp os command injection (ID 368)	A vulnerability classified as critical was found in tinygltf up to 2.5.x. This vulnerability affects the function wordexp of the component Backtick Handler. The manipulation leads to os command injection. This vulnerability was named CVE-2022-3008. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command injection attack
CVE-2022-31814	pfSense pfBlockerNG up to 2.1.4 HTTP Header Host os command injection	A vulnerability classified as critical has been found in pfSense pfBlockerNG up to 2.1.4. Affected is an unknown function of the component HTTP Header Handler. The manipulation of the argument Host leads to os command injection. This vulnerability is traded as CVE-2022-31814. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-30079	Netgear R6200 up to 1.0.3.12 /sbin/acos_ service command injection	A vulnerability was found in Netgear R6200 up to 1.0.3.12 and classified as critical. Affected by this issue is some unknown functionality of the file / sbin/acos_service. The manipulation leads to command injection. This vulnerability is handled as CVE-2022-30079. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-25765	pdfkit URL command injection	A vulnerability which was classified as critical was found in pdfkit. This affects an unknown part of the component URL Handler. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2022-25765. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-3133	jgraph drawio up to 20.2.x os command injection	A vulnerability classified as critical was found in jgraph drawio up to 20.2.x. Affected by this vulnerability is an unknown functionality. The manipulation leads to os command injection. This vulnerability is known as CVE-2022-3133. An attack has to be approached locally. 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-2022-39224	Arr-pm up to 0.0.11 RPM RPM::File os command injection (GHSA-88cv-mj24-8w3q)	A vulnerability was found in Arr-pm up to 0.0.11. It has been declared as critical. This vulnerability affects the function RPM::File of the component RPM Handler. The manipulation leads to os command injection. This vulnerability was named CVE-2022-39224. 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 command injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-39243	NuProcess up to 2.0.4 Command Line Argument Java_java_lang_UNIXProcess_forkAndExec command injection (GHSA-cxgf-v2p8-7ph7)	A vulnerability was found in NuProcess up to 2.0.4. It has been rated as critical. Affected by this issue is the function Java_java_lang_UNIXProcess_forkAndExec of the component Command Line Argument Handler. The manipulation leads to command injection. This vulnerability is handled as CVE-2022-39243. 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-2022-40785	mIPC 5.3.1.2003161406 os command injection	A vulnerability which was classified as critical has been found in mIPC 5.3.1.2003161406. This issue affects some unknown processing. The manipulation leads to os command injection. The identification of this vulnerability is CVE-2022-40785. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack

Cross-Site Request Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-36076	NodeBB up to 1.17.1 SSO cross-site request forgery (GHSA-xmgg-fx9p-prq6)	A vulnerability was found in NodeBB up to 1.17.1. It has been rated as problematic. This issue affects some unknown processing of the component SSO. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022-36076. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-36373	Simon Ward MP3 jPlayer Plugin up to 2.7.3 on WordPress cross-site request forgery	A vulnerability has been found in Simon Ward MP3 jPlayer Plugin up to 2.7.3 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-36373. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA

Remote Code Execution Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2432	Ecwid Ecommerce Shopping Cart Plugin up to 6.10.23 on WordPress ecwid_update_plugin_params cross-site request forgery	A vulnerability was found in Ecwid Ecommerce Shopping Cart Plugin up to 6.10.23. It has been rated as problematic. Affected by this issue is the function ecwid_update_plugin_params. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-2432. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-37730	ftcms 2.1 cross-site request forgery	A vulnerability which was classified as problematic was found in ftcms 2.1. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-37730. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-3232	ikus060 rdiffweb up to 2.4.4 cross-site request forgery	A vulnerability classified as problematic was found in ikus060 rdiffweb up to 2.4.4. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-3232. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-1591	Ping Optimizer Plugin prior 2.35.1.3.0 on WordPress Setting cross-site request forgery	A vulnerability has been found in Ping Optimizer Plugin and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-1591. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-35196	TestLink 1.9.20 /lib/plan/planView.php cross-site request forgery	A vulnerability which was classified as problematic has been found in TestLink 1.9.20. Affected by this issue is some unknown functionality in the library /lib/plan/planView.php. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-35196. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3233	us060 rdiffweb up to 2.4.5 crosssite request forgery	A vulnerability was found in ikus060 rdiffweb up to 2.4.5. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-3233. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-3274	ikus060 rdiffweb up to 2.4.6 crosssite request forgery	A vulnerability classified as problematic was found in ikus060 rdiffweb up to 2.4.6. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-3274. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-2405	WP Popup Builder Plugin up to 1.2.8 on WordPress AJAX Action crosssite request forgery	A vulnerability which was classified as problematic was found in WP Popup Builder Plugin up to 1.2.8. Affected is an unknown function of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-2405. It is possible to launch the attack remotely. There is no exploit available	Protected by core rules	NA
CVE-2022-2987	Active Directory Integration Plugin up to 3.0.1 on WordPress Setting crosssite request forgery	A vulnerability has been found in Active Directory Integration Plugin up to 3.0.1 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-2987. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-3098	Login Block IPs Plugin up to 1.0.0 on WordPress Setting cross-site request forgery	A vulnerability classified as problematic has been found in Login Block IPs Plugin up to 1.0.0. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-3098. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-24890	Scripts Organizer Plugin up to 2.x on WordPress AJAX Action saveScript cross-site request forgery	A vulnerability classified as problematic was found in Scripts Organizer Plugin up to 2.x. Affected by this vulnerability is the function saveScript of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2021-24890. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA

Local File Inclusion vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-36582	SourceCodester Garage Management System 1.0 createProduct.php unrestricted upload	A vulnerability was found in SourceCodester Garage Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /php_action/createProduct.php. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2022-36582. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-37122	Carel pCOWeb HVAC BACnet Gateway GET Parameter logdownload.cgi file pathname traversal (ID 167684)	A vulnerability was found in Carel pCOWeb HVAC BACnet Gateway. It has been classified as critical. Affected is an unknown function of the file logdownload.cgi of the component GET Parameter Handler. The manipulation of the argument file leads to pathname traversal. This vulnerability is traded as CVE-2022-37122. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-36580	anobe Online Ordering System 2.3.2 controller.php unrestricted upload	A vulnerability was found in janobe Online Ordering System 2.3.2. It has been classified as critical. This affects an unknown part of the file /admin/products/controller.phpactionadd. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2022-36580. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-3129	codeprojects Online Driving School/registration.php unrestricted upload	A vulnerability was found in codeprojects Online Driving School. It has been rated as critical. Affected by this issue is some unknown functionality of the file /registration.php. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2022-3129. The attack may be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2431	Download Manager Plugin up to 3.2.50 on WordPress Packages.php deleteFiles file inclusion	A vulnerability was found in Download Manager Plugin up to 3.2.50. It has been rated as critical. This issue affects the function deleteFiles of the file ~/Admin/Menu/Packages.php. The manipulation leads to file inclusion. The identification of this vulnerability is CVE-2022-2431. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-2945	Infinite Scroll Plugin up to 5.5.3 on WordPress alm_get_layout type path traversal	A vulnerability which was classified as problematic has been found in Infinite Scroll Plugin up to 5.5.3. Affected by this issue is the function alm_get_layout. The manipulation of the argument type leads to path traversal. This vulnerability is handled as CVE-2022-2945. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-37299	Shirne CMS 1.2.0 controller.php path traversal	A vulnerability classified as critical was found in Shirne CMS 1.2.0. Affected by this vulnerability is an unknown functionality of the file /static/ueditor/php/controller.php. The manipulation leads to path traversal. This vulnerability is known as CVE-2022-37299. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-40443	ZZCMS 2022 GET Request /one/siteinfo.php path traversal	A vulnerability was found in ZZCMS 2022. It has been classified as problematic. Affected is an unknown function of the file /one/siteinfo.php of the component GET Request Handler. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-40443. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-40089	Simple College Website 1.0 file inclusion	A vulnerability which was classified as critical has been found in Simple College Website 1.0. Affected by this issue is some unknown functionality. The manipulation leads to file inclusion. This vulnerability is handled as CVE-2022-40089. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2926	Download Manager Plugin up to 3.2.54 on WordPress Setting path traversal	A vulnerability classified as problematic has been found in Download Manager Plugin up to 3.2.54. This affects an unknown part of the component Setting Handler. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-2926. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-41343	Dompdf up to 2.0.0 Font Registration FontMetrics.php registerFont file inclusion (ID 2994)	A vulnerability which was classified as critical has been found in Dompdf up to 2.0.0. Affected by this issue is the function registerFont of the file FontMetrics.php of the component Font Registration Handler. The manipulation leads to file inclusion. This vulnerability is handled as CVE-2022-41343. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-40082	Hertz 0.3.0 normalizePath path traversal (ID 228)	A vulnerability has been found in Hertz 0.3.0 and classified as critical. This vulnerability affects the function normalizePath. The manipulation leads to path traversal. This vulnerability was named CVE-2022-40082. Access to the local network is required for this attack. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Local File Inclusion Attack
CVE-2022-2922	DNN up to 9.10.x path traversal	A vulnerability was found in DNN up to 9.10.x. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to relative path traversal. The identification of this vulnerability is CVE-2022-2922. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion Attack

Cross-Site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-37183	Piwigo 12.3.0 created-monthly-list crosssite scripting	A vulnerability was found in Piwigo 12.3.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /search/1940/created-monthly-list. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-37183. The attack may be launched remotely. There is no exploit available	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-3072	francoisjacquet rosariosis up to 8.9.2 cross-site scripting	A vulnerability was found in francoisjacquet rosariosis up to 8.9.2. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-3072. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-38790	Weave GitOps Enterprise up to 0.9.0-rc4 javascript URL cross-site scripting	A vulnerability was found in Weave GitOps Enterprise up to 0.9.0-rc4. It has been classified as problematic. Affected is an unknown function of the component javascript URL Handler. The manipulation leads to crosssite scripting. This vulnerability is traded as CVE-2022-38790. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-36203	SourceCodester Doctors Appointment System 1.0 Admin Panel cross-site scripting	A vulnerability was found in SourceCodester Doctors Appointment System 1.0. It has been classified as problematic. This affects an unknown part of the component Admin Panel. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-36203. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-36583	DedeCMS 5.7.97 / dede/co_do.php dopost/rpok/aid cross-site scripting	A vulnerability was found in DedeCMS 5.7.97. It has been declared as problematic. This vulnerability affects unknown code of the file /dede/co_do.php. The manipulation of the argument dopost/rpok/aid leads to cross-site scripting. This vulnerability was named CVE-2022-36583. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-36600	BlogEngine 3.3.8.0 / blogengine/api/posts Description cross-site scripting (ID 254)	A vulnerability was found in BlogEngine 3.3.8.0. It has been classified as problematic. This affects an unknown part of the file /blogengine/api/posts. The manipulation of the argument Description leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-36600. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-37679	Miniblog.Core 1.0 / blog/edit Excerpt crosssite scripting (ID 178)	A vulnerability was found in Miniblog.Core 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /blog/edit. The manipulation of the argument Excerpt leads to cross-site scripting. This vulnerability was named CVE-2022-37679. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-36637	SourceCodester Garage Management System 1.0 /brand.php brand_name crosssite scripting	A vulnerability classified as problematic was found in SourceCodester Garage Management System 1.0. This vulnerability affects unknown code of the file /brand.php. The manipulation of the argument brand_name leads to cross-site scripting. This vulnerability was named CVE-2022-36637. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-39840	Cotonti Siena 0.9.20 Direct Message cross-site scripting (ID 1660)	A vulnerability classified as problematic has been found in Cotonti Siena 0.9.20. Affected is an unknown function of the component Direct Message Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-39840. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-39049	OTRS URL cross-site scripting	A vulnerability was found in OTRS. It has been classified as problematic. This affects an unknown part of the component URL Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-39049. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-39839	Cotonti Siena 0.9.20 Forum Post cross-site scripting (ID 1661)	A vulnerability was found in Cotonti Siena 0.9.20. It has been rated as problematic. This issue affects some unknown processing of the component Forum Post Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-39839. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-39824	Appsmith up to 1.7.14 List Widget currentItem cross- site scripting	A vulnerability which was classified as problematic has been found in Appsmith up to 1.7.14. Affected by this issue is some unknown functionality of the component List Widget. The manipulation of the argument currentItem leads to cross-site scripting. This vulnerability is handled as CVE-2022-39824. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-3123	DokuWiki prior 2022-07-31a cross-site scripting	A vulnerability was found in DokuWiki. 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-2022-3123. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-2565	Simple Payment Donations & Subscriptions Plugin up to 4.2.0 on WordPress Form cross-site scripting	A vulnerability was found in Simple Payment Donations & Subscriptions Plugin up to 4.2.0. It has been declared as problematic. This vulnerability affects unknown code of the component Form Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2565. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3127	jgraph drawio up to 20.2.7 cross site scripting	A vulnerability was found in jgraph drawio up to 20.2.7. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-3127. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-2775	Fast Flow Plugin up to 1.2.12 on WordPress Widget Setting cross-site scripting	A vulnerability was found in Fast Flow Plugin up to 1.2.12. It has been rated as problematic. This issue affects some unknown processing of the component Widget Setting Handler. The manipulation leads to cross- site scripting. The identification of this vulnerability is CVE-2022-2775. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-37731	ftcms 2.1 poster.PHP cross-site scripting	A vulnerability which was classified as problematic has been found in ftcms 2.1. This issue affects some unknown processing of the file poster.PHP. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-37731. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-2515	Simple Banner Plugin up to 2.11.0 on WordPress pro_version_activation_code cross-site scripting	A vulnerability classified as problematic has been found in Simple Banner Plugin up to 2.11.0. This affects the function pro_version_activation_code. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2515. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-2941	WP-UserOnline Plugin up to 2.88.0 on WordPress Naming Conventions cross-site scripting	A vulnerability which was classified as problematic has been found in WP-UserOnline Plugin up to 2.88.0. This issue affects some unknown processing of the component Naming Conventions Handler. The manipulation leads to cross- site scripting. The identification of this vulnerability is CVE-2022-2941. The attack may be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-36080	Wikmd up to 1.7.0 Markdown cross-site scripting (GHSA-9m4m-6gqx-gfj3)	A vulnerability was found in Wikmd up to 1.7.0. It has been classified as problematic. Affected is an unknown function of the component Markdown Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-36080. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2020-19914	xiunobbs 4.0.4 Attachment Upload cross site scripting	A vulnerability was found in xiunobbs 4.0.4. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Attachment Upload Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2020-19914. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-36098	XWiki Platform Mentions UI prior 13.10.6/14.4 Script cross site scripting (GHSA-c5v8-2q4r-5w9v)	A vulnerability which was classified as problematic was found in XWiki Platform Mentions UI. Affected is an unknown function of the component Script Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-36098. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-2925	appwrite prior 1.0.0-RC1 cross site scripting	A vulnerability has been found in appwrite and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2022-2925. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-36094	XWiki Platform Web Parent POM prior 13.10.6/14.30-rc-1 History cross site scripting (GHSA-mxf2-4r22-5hq9)	A vulnerability classified as problematic has been found in XWiki Platform Web Parent POM. Affected is an unknown function of the component History Handler. The manipulation leads to basic cross site scripting. This vulnerability is traded as CVE-2022-36094. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-40317	OpenKM 6.3.11 javascript Substring cross site scripting	A vulnerability was found in OpenKM 6.3.11. It has been rated as problematic. This issue affects some unknown processing of the component javascript Substring Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2022-40317. The attack may be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-38639	Markdown-Nice 1.8.22 Community Posting cross site scripting (ID 327)	A vulnerability classified as problematic has been found in MarkdownNice 1.8.22. Affected is an unknown function. The manipulation of the argument Community Posting leads to cross site scripting. This vulnerability is traded as CVE-2022-38639. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-37796	SourceCodester Simple Online Book Store System 1.0 /admin_book.php Title/Author/Description cross site scripting	A vulnerability which was classified as problematic has been found in SourceCodester Simple Online Book Store System 1.0. This issue affects some unknown processing of the file /admin_book.php. The manipulation of the argument Title/Author/Description leads to cross site scripting. The identification of this vulnerability is CVE-2022-37796. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-36254	SourceCodester Hotel Management System 1.0 index.php fullname cross site scripting	A vulnerability classified as problematic has been found in SourceCodester Hotel Management System 1.0. This affects an unknown part of the file index.php. The manipulation of the argument fullname leads to cross site scripting. This vulnerability is uniquely identified as CVE-2022-36254. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-38295	Cuppa CMS 1.0 Add New Group cu_user_groups Name cross site scripting (ID 34)	A vulnerability was found in Cuppa CMS 1.0. It has been classified as problematic. Affected is an unknown function of the file /table_manager/view/cu_user_groups of the component Add New Group. The manipulation of the argument Name leads to cross site scripting. This vulnerability is traded as CVE-2022-38295. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-38291	Slims9 Senayan Library Management System 9.4.2 Search Bar cross site scripting (ID 156)	A vulnerability was found in Slims9 Senayan Library Management System 9.4.2 and classified as problematic. This issue affects some unknown processing of the component Search Bar. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2022-38291. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2020-25491	6Kare Emakin 5.0.341.0 Activity Stream Page setProfile DisplayName cross-site scripting	A vulnerability was found in 6Kare Emakin 5.0.341.0. It has been classified as problematic. This affects an unknown part of the file /rpc/membership/setProfile of the component Activity Stream Page. The manipulation of the argument DisplayName leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2020-25491. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-25873	vuetify up to 2.6.9 VCalendar Component eventName cross-site scripting (ID 15757)	A vulnerability has been found in vuetify up to 2.6.9 and classified as problematic. Affected by this vulnerability is the function eventName of the component VCalendar Component. The manipulation leads to crosssite scripting. This vulnerability is known as CVE-2022-25873. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-3231	librenms up to 22.8.x cross-site scripting	A vulnerability classified as problematic has been found in librenms up to 22.8.x. This affects an unknown part. The manipulation leads to crosssite scripting. This vulnerability is uniquely identified as CVE-2022-3231. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-3036	Gettext Override Translations Plugin up to 1.x on WordPress Setting cross-site scripting	A vulnerability classified as problematic was found in Gettext Override Translations Plugin up to 1.x. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-3036. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2753	Ketchup Restaurant Reservations Plugin up to 1.0.0 on WordPress cross-site scripting	A vulnerability was found in Ketchup Restaurant Reservations Plugin up to 1.0.0. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-2753. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-2567	Form Builder CP Plugin up to 1.2.31 on WordPress Setting cross-site scripting	A vulnerability was found in Form Builder CP Plugin up to 1.2.31 and classified as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-2567. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-3021	Slickr Flickr Plugin up to 2.8.1 on WordPress Setting cross-site scripting	A vulnerability classified as problematic has been found in Slickr Flickr Plugin up to 2.8.1. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-3021. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-2710	Scroll to Top Plugin up to 1.4.0 on WordPress Setting cross-site scripting	A vulnerability was found in Scroll to Top Plugin up to 1.4.0. It has been declared as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2710. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-2709	Float to Top Button Plugin up to 2.3.6 on WordPress Setting cross-site scripting	A vulnerability was found in Float to Top Button Plugin up to 2.3.6. It has been classified as problematic. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-2709. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3000	yetiforcecrm up to 6.3.x cross-site scripting	A vulnerability which was classified as problematic was found in yetiforce-crm up to 6.3.x. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-3000. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-2924	yetiforcecrm up to 6.2 cross-site scripting	A vulnerability which was classified as problem-atic has been found in yetiforcecrm up to 6.2. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-2924. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-38527	UCMS 1.6.0 Site Management Page cross-site scripting	A vulnerability was found in UCMS 1.6.0. It has been rated as problematic. This issue affects some un-known processing of the component Site Manage-ment Page. The manipula-tion leads to cross-site scripting. The identification of this vulnerability is CVE-2022-38527. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-38550	Jeesns 2.0.0 /weibo/ list cross-site script-ing	A vulnerability classified as problematic was found in Jeesns 2.0.0. Affected by this vulnerability is an unknown functionality of the file /weibo/list. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-38550. The attack can be launched re-motely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-32167	Cloudreve up to 3.5.3 File Upload crosssite scripting	A vulnerability classified as problematic was found in Cloudreve up to 3.5.3. Affected by this vulnerability is an unknown functionality of the component File Upload. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-32167. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-3255	pimcore cross-site scripting	A vulnerability which was classified as problematic has been found in pimcore. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-3255. The attack may be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-36365	WHA Crossword Plugin up to 1.1.10 on WordPress cross-site scripting	A vulnerability classified as problematic was found in WHA Crossword Plugin up to 1.1.10. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-36365. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-40029	SourceCodester Simple Task Managing System 1.0 newProjectValidation.php shortName cross-site scripting	A vulnerability which was classified as problematic was found in SourceCodester Simple Task Managing System 1.0. Affected is an unknown function of the file newProjectValidation.php. The manipulation of the argument shortName leads to cross-site scripting. This vulnerability is traded as CVE-2022-40029. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-40088	Simple College Website 1.0 index.php page cross-site scripting	A vulnerability which was classified as problematic was found in Simple College Website 1.0. This affects an unknown part of the file /college_website/index.php. The manipulation of the argument page leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-40088. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-23458	Toast UI Grid up to 4.21.2 Cell cross-site scripting (GHSL-2022-029)	A vulnerability was found in Toast UI Grid up to 4.21.2. It has been rated as problematic. This issue affects some unknown processing of the component Cell Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-23458. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-23461	Jodit Editor cross-site scripting (GHSL2022-030)	A vulnerability which was classified as problematic was found in Jodit Editor. Affected is an unknown function. The manipulation leads to crosssite scripting. This vulnerability is traded as CVE-2022-23461. It is possible to launch the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-35251	Rocket.Chat up to 4.x Style cross-site scripting	A vulnerability which was classified as problematic has been found in Rocket.Chat up to 4.x. This issue affects some unknown processing of the component Style Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-35251. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-39240	MyGraph up to 1.0.3 cross-site scripting (GHSA-hj4j-923h-927j)	A vulnerability was found in MyGraph up to 1.0.3 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-2022-39240. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-40358	AjaXplorer 4.2.3 SVG File cross-site scripting	A vulnerability classified as problematic was found in AjaXplorer 4.2.3. Affected by this vulnerability is an unknown functionality of the component SVG File Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-40358. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-40359	kfm up to 1.4.7 GET Request/kfm/index.php cross-site scripting	A vulnerability was found in kfm up to 1.4.7. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /kfm/index.php of the component GET Request Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-40359. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-3062	Simple File List Plugin up to 4.4.11 on WordPress cross-site scripting	A vulnerability was found in Simple File List Plugin up to 4.4.11 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-3062. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-2404	WP Popup Builder Plugin up to 1.2.8 on WordPress cross-site scripting	A vulnerability which was classified as problematic has been found in WP Popup Builder Plugin up to 1.2.8. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-2404. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-1755	SVG Support Plugin up to 2.4 on WordPress URL cross-site scripting	A vulnerability classified as problematic was found in SVG Support Plugin up to 2.4. This vulnerability affects unknown code of the component URL Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-1755. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-3135	SEO Smart Links Plugin up to 3.0.1 on WordPress Setting cross-site scripting	A vulnerability which was classified as problematic has been found in SEO Smart Links Plugin up to 3.0.1. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-3135. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3069	WordLift Plugin up to 3.37.1 on WordPress Setting cross-site scripting	A vulnerability was found in WordLift Plugin up to 3.37.1. It has been classified as problematic. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-3069. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-3070	Generate PDF Plugin up to 3.5 on WordPress Setting cross-site scripting	A vulnerability was found in Generate PDF Plugin up to 3.5. 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-2022-3070. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-3074	Slider Hero Plugin up to 8.4.3 on WordPress Slider Name cross-site scripting	A vulnerability was found in Slider Hero Plugin up to 8.4.3. It has been rated as problematic. This issue affects some unknown processing of the component Slider Name Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-3074. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-3024	Simple Bitcoin Faucets Plugin up to 1.7.0 on WordPress AJAX Action cross-site scripting	A vulnerability which was classified as problematic was found in Simple Bitcoin Faucets Plugin up to 1.7.0. This affects an unknown part of the component AJAX Action Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-3024. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-3025	Bitcoin Altcoin Faucet Plugin up to 1.6.0 on WordPress Setting cross-site scripting	A vulnerability has been found in Bitcoin Altcoin Faucet Plugin up to 1.6.0 and classified as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to crosssite scripting. This vulnerability was named CVE-2022-3025. The attack can be initiated remotely. There is no exploit available.		Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-21169	express-xss-sanitizer up to 1.1.2 allowed-Tags cross-site scripting	A vulnerability classified as problematic was found in express-xsssanitizer up to 1.1.2. This vulnerability affects unknown code. The manipulation of the argument allowedTags leads to cross-site scripting. This vulnerability was named CVE-2022-21169. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-38553	Academy Learning Management System up to 5.9.0 Search cross-site scripting	A vulnerability was found in Academy Learning Management System up to 5.9.0. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument Search leads to crosssite scripting. This vulnerability was named CVE-2022-38553. The attack can be initiated remotely. Furthermore, there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-40044	Centreon 20.10.18 Escalation esc_name cross-site scripting	A vulnerability has been found in Centreon 20.10.18 and classified as problematic. This vulnerability affects unknown code of the component Escalation Handler. The manipulation of the argument esc_ name leads to cross-site scripting. This vulnerability was named CVE-2022-40044. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-30003	SourceCodester Online Market Place Site 1.0 Product Title/ Short Description crosssite scripting (ID 168250)	A vulnerability was found in SourceCodester Online Market Place Site 1.0 and classified as problematic. This issue affects some unknown processing. The manipulation of the argument Product Title/Short Description leads to cross-site scripting. The identification of this vulnerability is CVE-2022-30003. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-38335	Vtiger CRM 7.4.0 E-Mail Template crosssite scripting	A vulnerability was found in Vtiger CRM 7.4.0. It has been classified as problematic. This affects an unknown part of the component E-Mail Template Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-38335. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-40912	ETAP Lighting International NV ETAP Safety Manager 1.0.0.32 GET Parameter cross-site scripting (ZSL-2022-5711)	A vulnerability which was classified as problematic has been found in ETAP Lighting International NV ETAP Safety Manager 1.0.0.32. Affected by this issue is some unknown functionality of the component GET Parameter Handler. The manipulation of the argument GET leads to cross-site scripting. This vulnerability is handled as CVE-2022-40912. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2020-15339	ZyXEL CloudCNM SecuManager 3.1.0/3.1.1 handle_campaign_script_link script_name cross-site scripting	A vulnerability classified as problematic has been found in ZyXEL CloudCNM SecuManager 3.1.0/3.1.1. Affected is an unknown function of the file live/CPEManager/AXCampaignManager/handle_campaign_script_link. The manipulation of the argument script_name leads to cross-site scripting. This vulnerability is traded as CVE-2020-15339. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-3355	inventree up to 0.8.2 cross-site scripting	A vulnerability has been found in inventree up to 0.8.2 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-3355. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2021-45843	glFusion CMS 1.7.9 Title Request Parameter cross-site scripting	A vulnerability has been found in glFusion CMS 1.7.9 and classified as problematic. This vulnerability affects unknown code of the component Title Request Parameter Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2021-45843. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack
CVE-2022-1719	polonel trudesk up to 1.2.1 Ticket Filter cross-site scripting	A vulnerability which was classified as problematic has been found in polonel trudesk up to 1.2.1. Affected by this issue is some unknown functionality of the component Ticket Filter. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-1719. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-38812	AeroCMS 0.1.1 author sql injection	A vulnerability which was classified as critical was found in AeroCMS 0.1.1. Affected is an unknown function. The manipulation of the argument author leads to sql injection. This vulnerability is traded as CVE-2022-38812. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-36676	oretnom23 Simple Task Scheduling System 1.0 view_category.php id sql injection	A vulnerability which was classified as critical was found in oretnom23 Simple Task Scheduling System 1.0. Affected is an unknown function of the file /categories/view_category.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-36676. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-36581	janobe Online Ordering System 2.3.2 /admin/login.php user_email sql injection	A vulnerability classified as critical has been found in janobe Online Ordering System 2.3.2. This affects an unknown part of the file /admin/login.php. The manipulation of the argument user_email leads to sql injection. This vulnerability is uniquely identified as CVE-2022-36581. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-36201	Doctors Appointment System 1.0 booking.php id sql injection	A vulnerability has been found in Doctors Appointment System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file booking.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-36201. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2020-22669	Modsecurity owasp-modsecurity-crs 3.2.0 WAF Protection sql injection (ID 1727)	A vulnerability was found in Modsecurity owasp-modsecurity-crs 3.2.0. It has been declared as critical. This vulnerability affects unknown code of the component WAF Protection. The manipulation leads to sql injection. This vulnerability was named CVE-2020-22669. The attack can be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as SQL Injection Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-36636	SourceCodester Garage Management System 1.0 /print.php id sql injection	A vulnerability was found in SourceCodester Garage Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /print.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-36636. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-36759	Online Food Ordering System 1.0 /dishes.php res_id sql injection	A vulnerability was found in Online Food Ordering System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /dishes.php. The manipulation of the argument res_id leads to sql injection. This vulnerability is handled as CVE-2022-36759. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-36594	Mapper up to 4.2.0 selectByIds ids sql injection (ID 862)	A vulnerability has been found in Mapper up to 4.2.0 and classified as critical. This vulnerability affects the function selectByIds. The manipulation of the argument ids leads to sql injection. This vulnerability was named CVE-2022-36594. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-36754	Expense Management System 1.0/Home/debit_credit_p id sql injection	A vulnerability has been found in Expense Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /Home/debit_credit_p. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-36754. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-3118	Sourcecodehero ERP System Project /pages/processlogin.php user sql injection	A vulnerability was found in Sourcecodehero ERP System Project. It has been rated as critical. This issue affects some unknown processing of the file /pages/processlogin.php. The manipulation of the argument user leads to sql injection. The identification of this vulnerability is CVE-2022-3118. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3120	SourceCodester Clinics Patient Management System Login index.php user_name sql injection	A vulnerability classified as critical was found in SourceCodester Clinics Patient Management System. Affected by this vulnerability is an unknown functionality of the file index.php of the component Login. The manipulation of the argument user_name leads to sql injection. This vulnerability is known as CVE-2022-3120. The attack can be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-3130	codeprojects Online Driving School /login.php username sql injection	A vulnerability classified as critical has been found in codeprojects Online Driving School. This affects an unknown part of the file /login.php. The manipulation of the argument username leads to sql injection. This vulnerability is uniquely identified as CVE-2022-3130. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-3122	SourceCodester Clinics Patient Management System 1.0 medicine_details.php medicine sql injection	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file medicine_details.php. The manipulation of the argument medicine leads to sql injection. This vulnerability is handled as CVE-2022-3122. The attack may be launched remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38255	janobe Interview Management System 1.0 editQuestion.php id sql injection	A vulnerability classified as critical has been found in janobe Interview Management System 1.0. Affected is an unknown function of the file /interview/editQuestion.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-38255. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38269	janobe School Activity Updates with SMS Notification 1.0 index.php id sql injection	A vulnerability was found in janobe School Activity Updates with SMS Notification 1.0 and classified as critical. This issue affects some unknown processing of the file /modules/mod-student/index.phpviewed-it. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-38269. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-38267	janobe School Activity Updates with SMS Notification 1.0 index.php id sql injection	A vulnerability which was classified as critical was found in janobe School Activity Updates with SMS Notification 1.0. This affects an unknown part of the file /modules/user/index.phpviewedit. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-38267. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38277	JFinal CMS 5.1.0 list sql injection (ID 51)	A vulnerability which was classified as critical has been found in JFinal CMS 5.1.0. Affected by this issue is some unknown functionality of the file /admin/folderrollpicture/list. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-38277. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38279	JFinal CMS 5.1.0 / admin/imagealbum/list sql injection (ID 51)	A vulnerability has been found in JFinal CMS 5.1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/imagealbum/list. The manipulation leads to sql injection. This vulnerability was named CVE-2022-38279. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38280	JFinal CMS 5.1.0 / admin/image/list sql injection (ID 51)	A vulnerability was found in JFinal CMS 5.1.0 and classified as critical. This issue affects some unknown processing of the file /admin/image/list. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-38280. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38282	JFinal CMS 5.1.0 /admin/videoalbum/list sql injection (ID 52)	A vulnerability was found in JFinal CMS 5.1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/videoalbum/list. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-38282. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38281	JFinal CMS 5.1.0 / admin/site/list sql injection (ID 51)	A vulnerability was found in JFinal CMS 5.1.0. It has been classified as critical. Affected is an unknown function of the file /admin/site/list. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-38281. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-38284	JFinal CMS 5.1.0 /system/department/list sql injection (ID 52)	A vulnerability classified as critical has been found in JFinal CMS 5.1.0. This affects an unknown part of the file /system/department/list. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-38284. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38278	JFinal CMS 5.1.0 / admin/friendlylink/list sql injection (ID 51)	A vulnerability which was classified as critical was found in JFinal CMS 5.1.0. This affects an unknown part of the file /admin/friendlylink/list. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-38278. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38276	JFinal CMS 5.1.0 / admin/foldernotice/list sql injection (ID 51)	A vulnerability classified as critical was found in JFinal CMS 5.1.0. Affected by this vulnerability is an unknown functionality of the file /admin/foldernotice/list. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-38276. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38285	JFinal CMS 5.1.0 / system/menu/list sql injection (ID 52)	A vulnerability classified as critical was found in JFinal CMS 5.1.0. This vulnerability affects unknown code of the file /system/menu/list. The manipulation leads to sql injection. This vulnerability was named CVE-2022-38285. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38275	JFinal CMS 5.1.0 / admin/contact/list sql injection (ID 51)	A vulnerability classified as critical has been found in JFinal CMS 5.1.0. Affected is an unknown function of the file /admin/contact/list. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-38275. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38283	JFinal CMS 5.1.0 / admin/video/list sql injection (ID 52)	A vulnerability was found in JFinal CMS 5.1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/video/list. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-38283. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-38286	JFinal CMS 5.1.0 / system/role/list sql injection (ID 52)	A vulnerability which was classified as critical has been found in JFinal CMS 5.1.0. This issue affects some unknown processing of the file /system/role/list. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-38286. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38615	SmartVista SVFE2 2.2.22 service_group.jsf UserForm:j_id88/UserForm:j_id90/UserForm:j_id92 sql injection	A vulnerability was found in SmartVista SVFE2 2.2.22. It has been classified as critical. Affected is an unknown function of the file /SVFE2/pages/feegroups/service_group.jsf. The manipulation of the argument UserForm:j_id88/UserForm:j_id90/UserForm:j_id92 leads to sql injection. This vulnerability is traded as CVE-2022-38615. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38272	JFinal CMS 5.1.0 / admin/article/list sql injection (ID 51)	A vulnerability was found in JFinal CMS 5.1.0. It has been classified as critical. This affects an unknown part of the file /admin/article/list. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-38272. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2021-44835	Active Intelligent Visualization 5 Vdc Header sql injection	A vulnerability was found in Active Intelligent Visualization 5. It has been rated as critical. Affected by this issue is some unknown functionality of the component Vdc Header Handler. The manipulation leads to sql injection. This vulnerability is handled as CVE-2021-44835. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38273	JFinal CMS 5.1.0 list_approve sql injection (ID 51)	A vulnerability was found in JFinal CMS 5.1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/article/list_approve. The manipulation leads to sql injection. This vulnerability was named CVE-2022-38273. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-36258	sazanrjb InventoryManagementSystem 1.0 CustomerDAO.java searchTxt sql injection (ID 14)	A vulnerability which was classified as critical has been found in sazanrjb InventoryManagementSystem 1.0. Affected by this issue is some unknown functionality of the file CustomerDAO.java. The manipulation of the argument searchTxt leads to sql injection. This vulnerability is handled as CVE-2022-36258. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-38605	Church Management System 1.0 /admin/edit_event.php id sql injection	A vulnerability which was classified as critical has been found in Church Management System 1.0. This issue affects some unknown processing of the file /admin/edit_event.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-38605. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-2840	Zephyr Project Manager up to 3.2.4 on Wordpress /wpadmin/admin-ajax.php project_id/task_id sql injection	A vulnerability which was classified as critical was found in Zephyr Project Manager up to 3.2.4. Affected is an unknown function of the file /wp-admin/admin-ajax.php. The manipulation of the argument project_id/task_id leads to sql injection. This vulnerability is traded as CVE-2022-2840. It is possible to launch the attack remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38610	Garage Management System 1.0 /garage/editclient.php id sql injection	A vulnerability has been found in Garage Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /garage/editclient.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-38610. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38302	Online Leave Management System 1.0 manage_department.php id sql injection	A vulnerability was found in Online Leave Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /maintenance/manage_department.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-38302. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38304	oretnom23 Online Leave Management System 1.0 manage_leave_type.php id sql injection	A vulnerability was found in oretnom23 Online Leave Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /maintenance/manage_leave_type.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-38304. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-38606	Garage Management System 1.0 /garage/editcategory.php id sql injection	A vulnerability which was classified as critical was found in Garage Management System 1.0. Affected is an unknown function of the file /garage/editcategory.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-38606. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40766	Modern Campus Omni CMS 10.2.4 log-in-page sql injection	A vulnerability which was classified as critical has been found in Modern Campus Omni CMS 10.2.4. This issue affects some unknown processing of the component log-in-page. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-40766. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-3141	Translate Multilingual Sites Plugin up to 2.3.2 on WordPress Settings Page sql injection	A vulnerability which was classified as critical was found in Translate Multilingual Sites Plugin up to 2.3.2. Affected is an unknown function of the component Settings Page. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-3141. The attack can only be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38617	SmartVista SVFE2 2.2.22 voiceaudit.jsf voiceAudit:j_id97 sql injection	A vulnerability which was classified as critical has been found in SmartVista SVFE2 2.2.22. Affected by this issue is some unknown functionality of the file /SVFE2/pages/audit/voiceaudit.jsf. The manipulation of the argument voiceAudit:j_id97 leads to sql injection. This vulnerability is handled as CVE-2022-38617. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-2958	BadgeOS Plugin prior 3.7.1.3 on WordPress SQL Statement sql injection	A vulnerability which was classified as critical has been found in BadgeOS Plugin. This issue affects some unknown processing of the component SQL Statement Handler. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-2958. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-37203	JFinal CMS 5.1.0 sql injection	A vulnerability classified as critical has been found in JFinal CMS 5.1.0. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-37203. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-2754	Ketchup Restaurant Reservations Plugin up to 1.0.0 on WordPress SQL Statement sql injection	A vulnerability classified as critical was found in Ketchup Restaurant Reservations Plugin up to 1.0.0. This vulnerability affects unknown code of the component SQL Statement Handler. The manipulation leads to sql injection. This vulnerability was named CVE-2022-2754. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-3142	NEX-Forms Plugin up to 7.9.6 on WordPress sql injection	A vulnerability which was classified as critical has been found in NEX-Forms Plugin up to 7.9.6. Affected by this issue is some unknown functionality. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-3142. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38509	Wedding Planner 1.0 /admin/budget.php booking_id sql injection	A vulnerability was found in Wedding Planner 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/budget.php. The manipulation of the argument booking_id leads to sql injection. This vulnerability is handled as CVE-2022-38509. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38576	janobe Interview Management System 1.0 delete.php id sql injection	A vulnerability which was classified as critical was found in janobe Interview Management System 1.0. Affected is an unknown function of the file /interview/delete.phpactiondeletecand. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-38576. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-37204	Final CMS 5.1.0 sql injection	A vulnerability has been found in Final CMS 5.1.0 and classified as critical. This vulnerability affects unknown code. The manipulation leads to sql injection. This vulnerability was named CVE-2022-37204. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-37205	JFinal CMS 5.1.0 sql injection	A vulnerability classified as critical has been found in JFinal CMS 5.1.0. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-37205. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-38619	SmartVista SVFE2 2.2.22 mcc_group.jsf UserForm:j_id90 sql injection	A vulnerability has been found in SmartVista SVFE2 2.2.22 and classified as critical. This vulnerability affects unknown code of the file /SVFE2/pages/feegroups/mcc_group.jsf. The manipulation of the argument UserForm:j_id90 leads to sql injection. This vulnerability was named CVE-2022-38619. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40935	oretnom23 Online Pet Shop We App 1.0 Master.php id sql injection	A vulnerability was found in oretnom23 Online Pet Shop We App 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /pet_shop/classes/Master.phpfdelete_category. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-40935. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40026	SourceCodester Simple Task Managing System 1.0 board.php board bookId sql injection	A vulnerability was found in SourceCodester Simple Task Managing System 1.0. It has been rated as critical. Affected by this issue is the function board of the file board.php. The manipulation of the argument bookId leads to sql injection. This vulnerability is handled as CVE-2022-40026. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-40934	oretnom23 Online Pet Shop We App 1.0 Master.php id sql injection	A vulnerability has been found in oretnom23 Online Pet Shop We App 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /pet_shop/classes/Master.phpfdelete_sub_category. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-40934. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40446	ZZCMS 2022 sendmailto.php sql injection	A vulnerability has been found in ZZCMS 2022 and classified as critical. This vulnerability affects unknown code of the file /admin/sendmailto.php-tomail&groupid. The manipulation leads to sql injection. This vulnerability was named CVE-2022-40446. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40447	ZZCMS 2022 /admin/baojia_list.php keyword sql injection	A vulnerability was found in ZZCMS 2022 and classified as critical. This issue affects some unknown processing of the file /admin/baojia_list.php. The manipulation of the argument keyword leads to sql injection. The identification of this vulnerability is CVE-2022-40447. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40030	SourceCodester Simple Task Managing System 1.0 changeStatus.php bookId sql injection	A vulnerability classified as critical has been found in SourceCodester Simple Task Managing System 1.0. This affects an unknown part of the file changeStatus.php. The manipulation of the argument bookId leads to sql injection. This vulnerability is uniquely identified as CVE-2022-40030. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40933	oretnom23 Online Pet Shop We App 1.0 Master.php id sql injection	A vulnerability which was classified as critical was found in oretnom23 Online Pet Shop We App 1.0. Affected is an unknown function of the file /pet_shop/classes/Master.phpfdelete_order. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-40933. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-40093	Online Tours & Travels Management System 1.0 update_tax.php id sql injection	A vulnerability was found in Online Tours & Travels Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /tour/admin/update_tax.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-40093. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40091	Online Tours & Travels Management System 1.0 update_packages.php id sql injection	A vulnerability was found in Online Tours & Travels Management System 1.0. It has been classified as critical. This affects an unknown part of the file /tour/admin/update_packages.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-40091. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40092	Online Tours & Travels Management System 1.0 update_payment.php id sql injection	A vulnerability was found in Online Tours & Travels Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /tour/admin/update_payment.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-40092. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40117	Online Banking System 1.0 delete_customer.php cust_id sql injection (ID 17)	A vulnerability was found in Online Banking System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /net-banking/delete_customer.php. The manipulation of the argument cust_id leads to sql injection. This vulnerability is handled as CVE-2022-40117. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40122	Online Banking System 1.0 edit_customer_action.php cust_id sql injection (ID 15)	A vulnerability classified as critical was found in Online Banking System 1.0. Affected by this vulnerability is an unknown functionality of the file /net-banking/edit_customer_action.php. The manipulation of the argument cust_id leads to sql injection. This vulnerability is known as CVE-2022-40122. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40119	Online Banking System 1.0 transactions.php search_term sql injection (ID 11)	A vulnerability was found in Online Banking System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /net-banking/transactions.php. The manipulation of the argument search_term leads to sql injection. This vulnerability was named CVE-2022-40119. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-40121	Online Banking System 1.0 manage_customers.php search sql injection (ID 12)	A vulnerability classified as critical has been found in Online Banking System 1.0. Affected is an unknown function of the file /net-banking/manage_customers.php. The manipulation of the argument search leads to sql injection. This vulnerability is traded as CVE-2022-40121. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-32211	Rocket.Chat up to 3.18.5/4.4.3/4.7.2 2FA Secret sql injection	A vulnerability has been found in Rocket.Chat up to 3.18.5/4.4.3/4.7.2 and classified as critical. This vulnerability affects unknown code of the component 2FA Secret Handler. The manipulation leads to sql injection. This vulnerability was named CVE-2022-32211. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40120	Online Banking System 1.0 customer_transactions.php search_term sql injection (ID 14)	A vulnerability was found in Online Banking System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /net-banking/customer_transactions.php. The manipulation of the argument search_term leads to sql injection. The identification of this vulnerability is CVE-2022-40120. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40118	Online Banking System 1.0 send_funds_action.php cust_id sql injection (ID 19)	A vulnerability was found in Online Banking System 1.0. It has been classified as critical. This affects an unknown part of the file /net-banking/send_funds_action.php. The manipulation of the argument cust_id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-40118. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40115	Online Banking System 1.0 delete_beneficiary.php cust_id sql injection (ID 10)	A vulnerability which was classified as critical was found in Online Banking System 1.0. Affected is an unknown function of the file /net-banking/delete_beneficiary.php. The manipulation of the argument cust_id leads to sql injection. This vulnerability is traded as CVE-2022-40115. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40116	Online Banking System 1.0 beneficiary.php search sql injection (ID 13)	A vulnerability has been found in Online Banking System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /netbanking/beneficiary.php. The manipulation of the argument search leads to sql injection. This vulnerability is known as CVE-2022-40116. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-40114	Online Banking System 1.0 edit_customer.php cust_id sql injection (ID 16)	A vulnerability which was classified as critical has been found in Online Banking System 1.0. This issue affects some unknown processing of the file /net-banking/edit_customer.php. The manipulation of the argument cust_id leads to sql injection. The identification of this vulnerability is CVE-2022-40114. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40113	Online Banking System 1.0 send_funds.php cust_id sql injection (ID 18)	A vulnerability classified as critical was found in Online Banking System 1.0. This vulnerability affects unknown code of the file /net-banking/send_funds.php. The manipulation of the argument cust_id leads to sql injection. This vulnerability was named CVE-2022-40113. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40928	Online Leave Management System 1.0 Master.php sql injection	A vulnerability was found in Online Leave Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /leave_system/classes/Master.phpfdelete_application. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-40928. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40402	Wedding Planner 1.0 /admin/client_assign.php booking sql injection	A vulnerability which was classified as critical has been found in Wedding Planner 1.0. Affected by this issue is some unknown functionality of the file /admin/client_assign.php. The manipulation of the argument booking leads to sql injection. This vulnerability is handled as CVE-2022-40402. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40927	Online Leave Management System 1.0 Master.php sql injection	A vulnerability was found in Online Leave Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /leave_system/classes/Master.phpfdelete_designation. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-40927. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40926	Online Leave Management System 1.0 Master.php sql injection	A vulnerability was found in Online Leave Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /leave_system/classes/Master.phpfdelete_leave_type. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-40926. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-40403	Wedding Planner 1.0 / admin/feature_edit. php id sql injection	A vulnerability which was classified as critical was found in Wedding Planner 1.0. This affects an unknown part of the file / admin/feature_edit.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-40403. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40404	Wedding Planner 1.0 / admin/select.php id sql injection	A vulnerability has been found in Wedding Planner 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/select.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-40404. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-3332	SourceCodester Food Ordering Management System POST Parameter router. php username sql injection	A vulnerability classified as critical has been found in SourceCodester Food Ordering Management System. This affects an unknown part of the file router.php of the component POST Parameter Handler. The manipulation of the argument username leads to sql injection. This vulnerability is uniquely identified as CVE-2022-3332. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40099	Online Tours & Travels Management System 1.0 update_expense_category.php id sql injection	A vulnerability has been found in Online Tours & Travels Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file/admin/update_expense_category.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-40099. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40098	Online Tours & Travels Management System 1.0 update_expense. php id sql injection	A vulnerability which was classified as critical was found in Online Tours & Travels Management System 1.0. This affects an unknown part of the file /admin/update_expense. php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-40098. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40485	Wedding Planner 1.0 / package_detail.php id sql injection	A vulnerability was found in Wedding Planner 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /package_detail. php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-40485. The attack needs to be approached within the local network. There is no exploit available	Protected by core rules	Detected by scanner as SQL Injection Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-40097	Online Tours & Travels Management System 1.0 update_currency.php id sql injection	A vulnerability which was classified as critical has been found in Online Tours & Travels Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/update_currency.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-40097. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40483	Wedding Planner 1.0 / wedding_details.php id sql injection	A vulnerability was found in Wedding Planner 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /wedding_details.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-40483. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40043	Centreon 20.10.18 Configuration Escalations esc_name sql injection	A vulnerability has been found in Centreon 20.10.18 and classified as critical. Affected by this vulnerability is an unknown functionality of the file Configuration/Notifications/Escalations of the component Configuration Handler. The manipulation of the argument esc_name leads to sql injection. This vulnerability is known as CVE-2022-40043. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40484	Wedding Planner 1.0 /admin/client_edit.php booking sql injection	A vulnerability was found in Wedding Planner 1.0. It has been classified as critical. This affects an unknown part of the file /admin/client_edit.php. The manipulation of the argument booking leads to sql injection. This vulnerability is uniquely identified as CVE-2022-40484. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-30004	SourceCodester Online Market Place Site 1.0 sql injection (ID 168249)	A vulnerability classified as critical has been found in SourceCodester Online Market Place Site 1.0. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-30004. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-37209	JFinal CMS 5.1.0 sql injection	A vulnerability classified as critical was found in JFinal CMS 5.1.0. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-37209. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-40877	Exam Reviewer Management System 1.0 id sql injection (ID 50725 / EDB-50725)	A vulnerability was found in Exam Reviewer Management System 1.0. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-40877. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-3323	Advantech iView 5.7.04.6469 ConfigurationServlet Endpoint check SQLInjection column_value sql injection	A vulnerability was found in Advantech iView 5.7.04.6469. It has been rated as critical. This issue affects the function checkSQLInjection of the component ConfigurationServlet Endpoint. The manipulation of the argument column_value leads to sql injection. The identification of this vulnerability is CVE-2022-3323. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40353	Online Tours & Travels Management System 1.0 /admin/up_booking.php id sql injection	A vulnerability which was classified as critical was found in Online Tours & Travels Management System 1.0. Affected is an unknown function of the file /admin/up_booking.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-40353. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2021-41433	EGavilan Resumes Management and Job Application up to 1.0 Login Form login.php sql injection	A vulnerability was found in EGavilan Resumes Management and Job Application up to 1.0. It has been classified as critical. This affects an unknown part of the file login.php of the component Login Form. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2021-41433. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-40352	Online Tours & Travels Management System 1.0 update_traveller.php id sql injection	A vulnerability which was classified as critical has been found in Online Tours & Travels Management System 1.0. This issue affects some unknown processing of the file /admin/update_traveller.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-40352. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack
CVE-2022-40354	Online Tours & Travels Management System 1.0 update_booking.php id sql injection	A vulnerability has been found in Online Tours & Travels Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/update_booking.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-40354. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection Attack

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

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

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.