INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

November 2022

The total zero-day vulnerabilities count for November month : 246

Command Injection	Local File Inclusion	SQL Injection	Malicious File Upload	Cross-Site Scripting	Cross-Site Request Forgery	XML External Entity
8	10	96	3	98	29	2

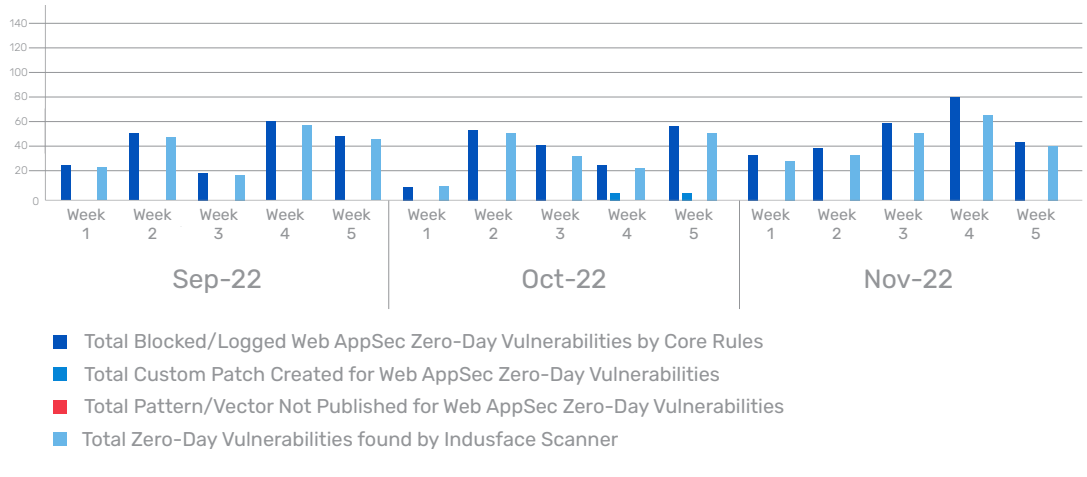
Zero-day vulnerabilities protected through core rules	246
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities for which protection can not be done	0
Zero-day vulnerabilities found by Indusface WAS	214

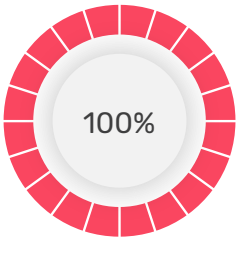
- To enable custom rules, please contact support@indusface.com
- Since the attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.

Vulnerability Trend:

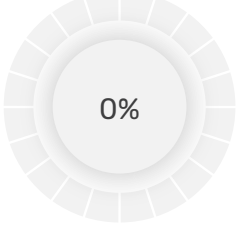
The weekly trend displays the total number of vulnerabilities discovered to the type of protection provided for the last quarter.

Weekly Vulnerability Trend

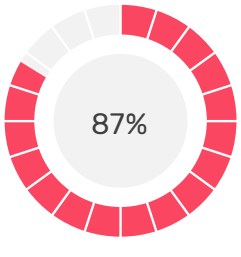




of the zero-day vulnerabilities were protected by the **core rules** in the last month.

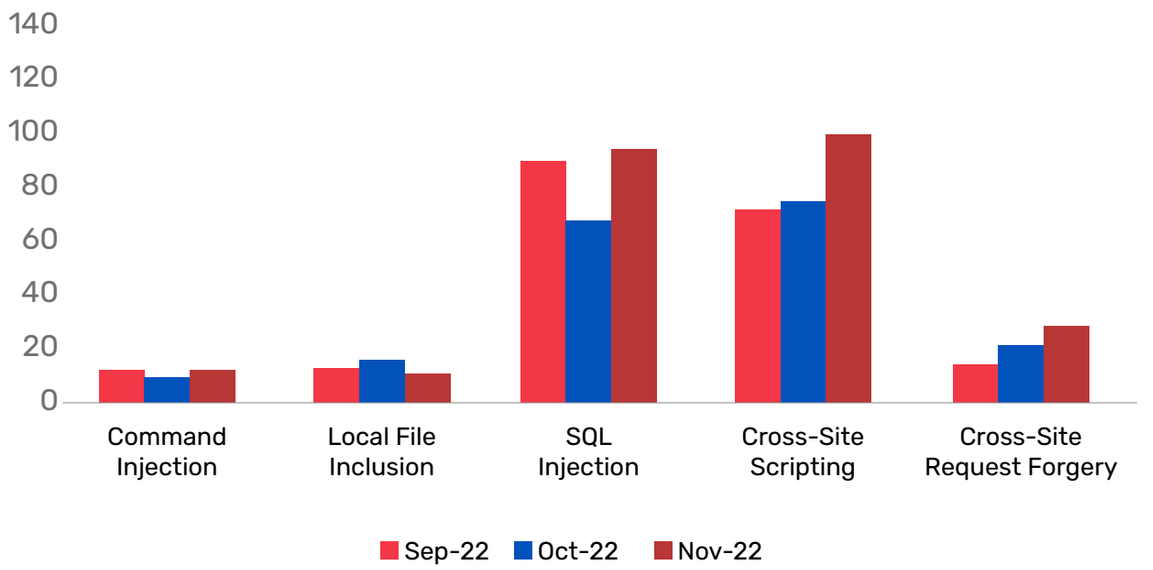


of the zero-day vulnerabilities were protected by the **custom rules** in the last month.



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-2022-43109	D-Link DIR-823G 1.0.2 Packet SetNetworkTomography-Settings command injection	A vulnerability has been found in D-Link DIR-823G 1.0.2 and classified as critical. Affected by this vulnerability is the function SetNetworkTomography-Settings of the component Packet Handler. The manipulation leads to command injection. This vulnerability is known as CVE-2022-43109. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command injection attack
CVE-2022-40847	Tenda AC1200 15.11.0.10 (1576) formSetFixTools hostname command injection	A vulnerability classified as critical was found in Tenda AC1200 15.11.0.10. Affected by this vulnerability is the function formSetFixTools. The manipulation of the argument hostname leads to command injection. This vulnerability is known as CVE-2022-40847. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command injection attack
CVE-2022-41395	Tenda AC1200 15.11.0.10 (1576) setDMZ dmzHost command injection	A vulnerability classified as critical has been found in Tenda AC1200 15.11.0.10. Affected is the function setDMZ. The manipulation of the argument dmzHost leads to command injection. This vulnerability is traded as CVE-2022-41395. 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-41396	Tenda AC1200 15.11.0.10 (1576) setIPsecTunnelList IPsecLocalNet / IPsecRemoteNet command injection	A vulnerability was found in Tenda AC1200 15.11.0.10. It has been declared as critical. Affected by this vulnerability is the function setIPsecTunnelList. The manipulation of the argument IPsecLocalNet /IPsecRemoteNet leads to command injection. This vulnerability is known as CVE-2022-41396. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-42053	Tenda AC1200 15.11.0.10 (1576) setPortMapping PortMappingServer command injection	A vulnerability classified as critical was found in Tenda AC1200 15.11.0.10. Affected by this vulnerability is the function setPortMapping. The manipulation of the argument PortMappingServer leads to command injection. This vulnerability is known as CVE-2022-42053. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-40881	Contec SolarView Compact 6.00 network_test.php command injection	A vulnerability classified as critical has been found in Contec SolarView Compact 6.00. This affects an unknown part of the file network_test.php. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2022-40881. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-40870	Parallels Remote Application Server 18.0 Web Client injection	A vulnerability which was classified as critical was found in Parallels Remote Application Server 18.0. Affected is an unknown function of the component Web Client. The manipulation leads to injection. This vulnerability is traded as CVE-2022-40870. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-40282	Hirschmann BAT-C2 prior 09.13.01.00R04 Web Server FsCreateDir dir command injection	A vulnerability has been found in Hirschmann BAT-C2 and classified as critical. This vulnerability affects the function FsCreateDir of the component Web Server. The manipulation of the argument dir leads to command injection. This vulnerability was named CVE-2022-40282. Access to the local network is required for this attack. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by the scanner as command injection attack

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2711	Import any XML or CSV File to Plugin up to 3.6.8 on WordPress ZIP Archive path traversal	A vulnerability was found in Import any XML or CSV File to Plugin up to 3.6.8. It has been declared as critical. This vulnerability affects unknown code of the component ZIP Archive Handler. The manipulation leads to path traversal. This vulnerability was named CVE-2022-2711. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2022-43319	oretnom23 Simple ELearning System 1.0 path traversal	A vulnerability was found in oretnom23 Simple ELearning System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file vcs/downloadFiles.phpdownload./search.php. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-43319. 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-2022-43753	SUSE Linux Enterprise Module for SUSE Manager Server path traversal	A vulnerability which was classified as critical has been found in SUSE Linux Enterprise Module for SUSE Manager Server. This issue affects some unknown processing. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-43753. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2022-43264	Arobas Music Guitar Pro up to 1.10.1 on iPhone/iPad Web Request pathname traversal	A vulnerability was found in Arobas Music Guitar Pro up to 1.10.1. It has been rated as problematic. This issue affects some unknown processing of the component Web Request Handler. The manipulation leads to pathname traversal. The identification of this vulnerability is CVE-2022-43264. The attack can only be initiated within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3762	Booster for Woo-Commerce Plugin on WordPress path traversal	A vulnerability which was classified as critical was found in Booster for Woo-Commerce Plugin Booster Plus for WooCommerce Plugin and Booster Elite for WooCommerce Plugin. This affects an unknown part. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2022-3762. It is possible to initiate the attack re-motely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclu-sion attack.
CVE-2022-44786	Appalti & Contratti 9.12.2 Apr iPagina.do href file inclusion	A vulnerability was found in Appalti & Contratti 9.12.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file ApriPag ina.do. The manipulation of the argu-ment href leads to file inclusion. This vulnerability is known as CVE-2022-44786. Access to the local net-work is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclu-sion attack.
CVE-2022-44784	Appalti & Contratti 9.12.2 LFS/DL229 WEB-INF/web.xml file inclusion	A vulnerability was found in Appalti & Contratti 9.12.2 and classified as prob-lematic. Affected by this issue is some unknown functionality of the file WEB-INF/web.xml of the component LFS/DL229. The manipulation leads to file inclusion. This vulnerability is handled as CVE-2022-44784. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclu-sion attack.
CVE-2022-45866	qpress up to 11.3 qp File pathname traversal	A vulnerability was found in qpress up to 11.3. It has been declared as critical. Affected by this vulner-ability is an unknown functionality of the com-ponent qp File Handler. The manipulation leads to pathname traversal. This vulnerability is known as CVE-2022-45866. The attack needs to be done within the local network. There is no exploit avail-able. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclu-sion attack.
CVE-2022-25848	static-dev-server path traversal	A vulnerability classified as problematic was found in static-dev-server. Affect-ed by this vulnerability is an unknown functionality. The manipulation leads to relative path traversal. This vulnerability is known as CVE-2022-25848. The attack can be launched re-motely. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclu-sion attack.
CVE-2022-3361	Ultimate Member Plugin up to 2.5.0 on WordPress Short-code template path traversal	A vulnerability has been found in Ultimate Member Plugin up to 2.5.0 and classified as problematic. This vulnerability affects unknown code of the com-ponent Shortcode Handler. The manipulation of the argument template leads to path traversal. This vulnerability was named CVE-2022-3361. The attack can be initiated remotely. There is no ex-ploit available.	Protected by core rules	Detected by scanner as Local File Inclu-sion attack.

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-43353	oretnom23 Sanitization Management System 1.0 id sql injection	A vulnerability which was classified as critical has been found in oretnom23 Sanitization Management System 1.0. This issue affects some unknown processing of the file /admin/pageorders /view_order. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-43353. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-3789	Tim Campus Confession Wall share.php post_id sql injection	A vulnerability has been found in Tim Campus Confession Wall and classified as critical. Affected by this vulnerability is an unknown functionality of the file share.php. The manipulation of the argument post_id leads to sql injection. This vulnerability is known as CVE-2022-3789. The attack needs to be approached within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-43355	oretnom23 Sanitization Management System 1.0 Master.php id sql injection	A vulnerability classified as critical has been found in oretnom23 Sanitization Management System 1.0. This affects an unknown part of the file /php-sms/classes /Master.phpfdelete_service. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022- 43355. 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-2022-43354	Sanitization Management System 1.0 id sql injection	A vulnerability which was classified as critical was found in Sanitization Management System 1.0. Affected is an unknown function of the file /admin /pageorders /manage_request. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-43354. 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-2022-43226	oretnom23 Online Diagnostic Lab Management System 1.0 id sql injection	A vulnerability classified as critical has been found in oretnom23 Online Diagnostic Lab Management System 1.0. This affects an unknown part of the file /odlms /page-appointments /view_appointment. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-43226. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-43227	oretnom23 Online Diagnostic Lab Management System 1.0 id sql injection	A vulnerability classified as critical was found in oretnom23 Online Diagnostic Lab Management System 1.0. This vulnerability affects unknown code of the file /odlms/admin /page-appointments /view_appointment. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-43227. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-41551	Garage Management System 1.0 /garage/editorder.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/editorder.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-41551. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-3825	Huaxia ERP 2.3 User Management login sql injection	A vulnerability was found in Huaxia ERP 2.3 and classified as critical. Affected by this issue is some unknown functionality of the component User Management. The manipulation of the argument login leads to sql injection. This vulnerability is handled as CVE-2022-3825. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-43066	oretnom23 Online Diagnostic Lab Management System 1.0 Master.php id sql injection	A vulnerability classified as critical has been found in oretnom23 Online Diagnostic Lab Management System 1.0. Affected is an unknown function of the file /odlms/classes/Master. phpfdelete_message. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-43066. 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-2022-43068	oretnom23 Online Diagnostic Lab Management System 1.0 Master.php id sql injection	A vulnerability classified as critical was found in oretnom23 Online Diagnostic Lab Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /classes /Master. phpfdelete_reservation. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-43068. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-43062	Online Diagnostic Lab Management System 1.0 Master.php id sql injection	A vulnerability has been found in Online Diagnostic Lab Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /classes/Master. phpfdelete_appointment. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-43062. 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-2022-43063	Online Diagnostic Lab Management System 1.0 Users.php id sql injection	A vulnerability was found in Online Diagnostic Lab Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /classes/Users. phpfdelete_client. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-43063. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-42744	CandidATS 3.0.0 CRUD Operation entriesPerPage sql injection	A vulnerability classified as critical has been found in CandidATS 3.0.0. Affected is an unknown function of the component CRUD Operation Handler. The manipulation of the argument entriesPerPage leads to sql injection. This vulnerability is traded as CVE-2022-42744. 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-2022-3481	WooCommerce Dropshipping Plugin up to 4.3 on WordPress REST Endpoint sql injection	A vulnerability was found in WooCommerce Dropshipping Plugin up to 4.3. It has been classified as critical. This affects an unknown part of the component REST Endpoint. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-3481. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-3494	Complianz Plugin/ Complianz Premium Plugin on WordPress Translation sql injection	A vulnerability classified as critical has been found in Complianz Plugin and Complianz Premium Plugin. Affected is an unknown function of the component Translation Handler. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-3494. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-43318	oretnom23 Human Resource Management System 1.0 / hrm/state.php stateedit sql injection	A vulnerability was found in oretnom23 Human Resource Management System 1.0 and classified as critical. This issue affects some unknown processing of the file / hrm/state.php. The manipulation of the argument stateedit leads to sql injection. The identification of this vulnerability is CVE-2022-43318. 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-2022-43350	oretnom23 Sanitization Management System 1.0 Master.php id sql injection	A vulnerability classified as critical has been found in oretnom23 Sanitization Management System 1.0. This affects an unknown part of the file /php-sms/classes /Master.phpfdelete_inquiry. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-43350. 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-2022-43352	oretnom23 Sanitization Management System 1.0 Master.php id sql injection	A vulnerability which was classified as critical has been found in oretnom23 Sanitization Management System 1.0. This issue affects some unknown processing of the file /php-sms/classes /Master.phpfdelete_quote. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-43352. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-3878	Maxon ERP browse_data tb_search sql injection	A vulnerability classified as critical has been found in Maxon ERP. This affects an unknown part of the file /index.php/purchase_order/browse_data. The manipulation of the argument tb_search leads to sql injection. This vulnerability is uniquely identified as CVE-2022-3878. 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-2022-42990	oretnom23 Food Ordering Management System 1.0 allorders.php sql injection	A vulnerability was found in oretnom23 Food Ordering Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /foms/allorders.phpstatusCancelled%20by%20Customer. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-42990. 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-2022-43292	Canteen Management System 1.0 /youthappam / editfood.php id sql injection	A vulnerability was found in Canteen Management System 1.0 and classified as critical. This issue affects some unknown processing of the file / youthappam/editfood.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-43292. 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-2022-43278	Canteen Management System 1.0 fetchSelectedCategories.php categoriesId sql injection	A vulnerability which was classified as critical has been found in Canteen Management System 1.0. Affected by this issue is some unknown functionality of the file /php_action/fetchSelectedCategories.php. The manipulation of the argument categoriesId leads to sql injection. This vulnerability is handled as CVE-2022-43278. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-43291	Canteen Management System 1.0 editclient.php id sql injection	A vulnerability has been found in Canteen Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /youthappam/editclient.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-43291. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-43290	Canteen Management System 1.0 editcategory.php id sql injection	A vulnerability which was classified as critical was found in Canteen Management System 1.0. This affects an unknown part of the file /youthappam/editcategory.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-43290. 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-2022-3948	eolinker goku_lite / plugin /getList route/keyword sql injection	A vulnerability classified as critical was found in eolinker goku_lite. This vulnerability affects unknown code of the file /plugin/getList. The manipulation of the argument route/keyword leads to sql injection. This vulnerability was named CVE-2022-3948. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-44727	EU Cookie Law GDPR Module up to 2.1.2 on PrestaShop lgcookieslaw/__lglaw sql injection	A vulnerability was found in EU Cookie Law GDPR Module up to 2.1.2. It has been declared as critical. This vulnerability affects unknown code of the component Cookie Handler. The manipulation of the argument lgcookieslaw/__lglaw leads to sql injection. This vulnerability was named CVE-2022-44727. 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-2022-3956	tsruban HHIMS 2.1 Patient Portrait PID sql injection	A vulnerability classified as critical has been found in tsruban HHIMS 2.1. Affected is an unknown function of the component Patient Portrait Handler. The manipulation of the argument PID leads to sql injection. This vulnerability is traded as CVE-2022-3956. It is possible to launch the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-3955	tholum crm42 Login class.user.php user_name sql injection	A vulnerability was found in tholum crm42. It has been rated as critical. This issue affects some unknown processing of the file crm42\class\class.user.php of the component Login. The manipulation of the argument user_name leads to sql injection. The identification of this vulnerability is CVE-2022-3955. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-3947	eolinker goku_lite / balance /service/list route/keyword sql injection	A vulnerability classified as critical has been found in eolinker goku_lite. This affects an unknown part of the file /balance/service/list. The manipulation of the argument route/keyword leads to sql injection. This vulnerability is uniquely identified as CVE-2022-3947. 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-2022-3972	Pingkon HMS-PHP admin/adminlogin.php uname/pass sql injection	A vulnerability was found in Pingkon HMS-PHP. It has been rated as critical. This issue affects some unknown processing of the file admin /adminlogin.php. The manipulation of the argument uname/pass leads to sql injection. The identification of this vulnerability is CVE-2022-3972. 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-2022-3973	Pingkon HMS-PHP Data Pump Metada-ta /admin /admin. php uname/pass sql injection	A vulnerability classified as critical has been found in Pingkon HMS-PHP. Affect-ed is an unknown function of the file /admin /admin. php of the component Data Pump Metadata. The manipulation of the argu-ment uname/pass leads to sql injection. This vulnerability is traded as CVE-2022-3973. It is possible to launch the attack remotely. Further-more there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-43288	Rukovoditel 3.2.1 or-der_by sql injection	A vulnerability which was classified as critical has been found in Rukovodi-tel 3.2.1. Affected by this issue is some unknown functionality of the file / rukovoditel/index. php-modulelogs/view& typephp. The manipulation of the argument order_by leads to sql injection. This vulnerability is handled as CVE-2022-43288. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-3998	MonikaBrzica scm uredi_korisnika.php id sql injection	A vulnerability which was classified as critical was found in MonikaBrzi-ca scm. This affects an unknown part of the file uredi_korisnika.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-3998. It is possible to initiate the attack remotely. Furthermore there is an exploit avail-able.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-3997	MonikaBrzica scm upis_u_bazu.php email /lozinka/ime/id sql injection	A vulnerability which was classified as critical has been found in MonikaBrzi-ca scm. Affected by this issue is some unknown functionality of the file upis_u_bazu.php. The manipulation of the argu-ment email/lozinka/ime/id leads to sql injection. This vulnerability is handled as CVE-2022-3997. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-43262	Human Resource Management System 1.0 login.php pass-word sql injection	A vulnerability has been found in Human Resource Management System 1.0 and classified as critical. Affected by this vulner-ability is an unknown functionality of the file / hrm/controller/login.php. The manipulation of the argument password leads to sql injection. This vulnerability is known as CVE-2022-43262. The attack can be launched re-motely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-43256	SeaCms up to 12.5 in-dex. php sql injection (ID 23)	A vulnerability was found in SeaCms up to 12.5. It has been classified as critical. This affects an unknown part of the file / js/player/dmplayer /dmku/ index.php. The manipula-tion leads to sql injection. This vulnerability is uniquely identified as CVE-2022-43256. It is possible to initiate the attack re-motely. 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-2022-4012	Hospital Management Center patient-info. php pt_id sql injection	A vulnerability classified as critical has been found in Hospital Management Center. Affected is an unknown function of the file patient-info.php. The manipulation of the argument pt_id leads to sql injection. This vulnerability is traded as CVE-2022-4012. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-43279	LimeSurvey 5.4.4 update. php sql injection	A vulnerability which was classified as critical was found in LimeSurvey 5.4.4. Affected is an unknown function of the file / application /views/themeOptions/update. php. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-43279. 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-2022-4015	Sports Club Management System 119 admin /make_payments.php m_id / plan sql injection	A vulnerability which was classified as critical was found in Sports Club Management System 119. This affects an unknown part of the file admin /make_payments.php. The manipulation of the argument m_id/plan leads to sql injection. This vulnerability is uniquely identified as CVE-2022-4015. 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-2022-44403	Automotive Shop Management System 1.0 id sql injection	A vulnerability has been found in Automotive Shop Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file / asms/admin /pageuser/ manage_user. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-44403. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-44402	oretnom23 Automotive Shop Management System 1.0 Master.php sql injection	A vulnerability was found in oretnom23 Automotive Shop Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /asms/classes/ Master. phpfdelete_transaction. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-44402. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-44003	BACKCLICK Professional 5.9.63 sql injection (SYSS-2022-029)	A vulnerability which was classified as critical was found in BACKCLICK Professional 5.9.63. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-44003. 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-2022-4052	Student Attendance Management System /Admin /createClass. php Id sql injection	A vulnerability was found in Student Attendance Management System and classified as critical. This issue affects some unknown processing of the file /Admin /createClass. php. The manipulation of the argument Id leads to sql injection. The identification of this vulnerability is CVE-2022-4052. 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-2022-43135	Online Diagnostic Lab Management System 1.0 /diagnostic/login.php username sql injection	A vulnerability which was classified as critical has been found in Online Diagnostic Lab Management System 1.0. Affected by this issue is some unknown functionality of the file /diagnostic/login.php. The manipulation of the argument username leads to sql injection. This vulnerability is handled as CVE-2022-43135. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-42245	Dreamer CMS 4.0.01 sql injection	A vulnerability was found in Dreamer CMS 4.0.01. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-42245. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-4051	Hostel Searching Project view-property.php property_id sql injection	A vulnerability has been found in Hostel Searching Project and classified as critical. This vulnerability affects unknown code of the file view-property.php. The manipulation of the argument property_id leads to sql injection. This vulnerability was named CVE-2022-4051. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-43179	Online Leave Management System 1.0 id sql injection	A vulnerability classified as critical was found in Online Leave Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin /pageuser/manage_user. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-43179. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-43162	Online Diagnostic Lab Management System 1.0 /tests/view_test.php id sql injection	A vulnerability which was classified as critical was found in Online Diagnostic Lab Management System 1.0. Affected is an unknown function of the file /tests /view_test.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-43162. 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-2022-44378	Automotive Shop Management System 1.0 Master.php sql injection	A vulnerability was found in Automotive Shop Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /asms/classes/Master. phpfdelete_mechanic. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-44378. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-43163	Online Diagnostic Lab Management System 1.0 /clients/ view_client.php id sql injection	A vulnerability has been found in Online Diagnostic Lab Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file / clients/view_client. php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-43163. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-44379	Automotive Shop Management System 1.0 Master.php sql injection	A vulnerability was found in Automotive Shop Management System 1.0. It has been classified as critical. This affects an unknown part of the file / asms/classes /Master. phpfdelete_service. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-44379. 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-2022-44414	Automotive Shop Management System 1.0 manage_service. php id sql injection	A vulnerability was found in Automotive Shop Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /asms/admin/ services /manage_service.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-44414. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-44413	Automotive Shop Management System 1.0 manage_mechanic.php id sql injection	A vulnerability has been found in Automotive Shop Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file / asms/admin/mechanics / manage_mechanic.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-44413. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-44820	Automotive Shop Management System 1.0 id sql injection	A vulnerability classified as critical was found in Automotive Shop Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /asms/admin / pagetransactions /manage_transaction. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-44820. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-44415	Automotive Shop Management System 1.0 view_mechanic. php id sql injection	A vulnerability was found in Automotive Shop Management System 1.0. It has been classified as critical. This affects an unknown part of the file / asms/admin /mechanics/ view_mechanic. php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-44415. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-4093	Dolibarr 16.0.1/16.0.2 sql injection	A vulnerability was found in Dolibarr 16.0.1/16.0.2. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-4093. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-3720	Event Monster Plugin up to 1.1.x on WordPress sql injection	A vulnerability was found in Event Monster Plugin up to 1.1.x and classified as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-3720. 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-2022-42098	KLiK SocialMediaWebsite 1.0.1 profile.php sql injection	A vulnerability which was classified as critical was found in KLiK SocialMediaWebsite 1.0.1. This affects an unknown part of the file profile.php. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-42098. 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-2022-44785	Appalti & Contratti 9.12.2 Get ListaEnti.do cfamm sql injection	A vulnerability which was classified as critical has been found in Appalti & Contratti 9.12.2. Affected by this issue is some unknown functionality of the file GetListaEnti.do. The manipulation of the argument cfamm leads to sql injection. This vulnerability is handled as CVE-2022-44785. 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-2022-43212	Billing System Project 1.0 fetchOrderData.php orderId sql injection	A vulnerability was found in Billing System Project 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file fetchOrderData.php. The manipulation of the argument orderId leads to sql injection. This vulnerability is handled as CVE-2022-43212. 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-2022-43214	SourceCodester Billing System Project 1.0 printOrder.php orderId sql injection	A vulnerability was found in SourceCodester Billing System Project 1.0. It has been classified as critical. This affects an unknown part of the file printOrder.php. The manipulation of the argument orderId leads to sql injection. This vulnerability is uniquely identified as CVE-2022-43214. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-43215	SourceCodester Billing System Project 1.0 getOrderReport. php getOrderReport endDate sql injection	A vulnerability was found in SourceCodester Billing System Project 1.0. It has been declared as critical. This vulnerability affects the function getOrderReport of the file getOrderReport.php. The manipulation of the argument endDate leads to sql injection. This vulnerability was named CVE-2022-43215. 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-2022-43213	Billing System Project 1.0 editorder.php id sql injection	A vulnerability was found in Billing System Project 1.0. It has been classified as critical. Affected is an unknown function of the file editorder. php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-43213. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-45536	AeroCMS 0.0.1\admin\post_comments. php id sql injection	A vulnerability has been found in AeroCMS 0.0.1 and classified as critical. This vulnerability affects unknown code of the file \admin\post_comments. php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-45536. 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-2022-45330	AeroCMS 0.0.1 \category. php Category sql injection	A vulnerability was found in AeroCMS 0.0.1 and classified as critical. Affected by this issue is some unknown functionality of the file \category.php. The manipulation of the argument Category leads to sql injection. This vulnerability is handled as CVE-2022-45330. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-45535	AeroCMS 0.0.1 \admin\categories.php edit sql injection	A vulnerability which was classified as critical was found in AeroCMS 0.0.1. This affects an unknown part of the file \admin\categories.php.The manipulation of the argument edit leads to sql injection. This vulnerability is uniquely identified as CVE-2022-45535. 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-2022-44139	oretnom23 Apartment Visitor Management System 1.0 / avms/index.php sql injection	A vulnerability classified as critical was found in oretnom23 Apartment Visitor Management System 1.0. This vulnerability affects unknown code of the file /avms/index.php. The manipulation leads to sql injection. This vulnerability was named CVE-2022-44139. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-37773	Maarch RM 2.8 /statistics/retrieve filter sql injection	A vulnerability was found in Maarch RM 2.8. It has been classified as critical. Affected is an unknown function of the file /statistics/retrieve. The manipulation of the argument filter leads to sql injection. This vulnerability is traded as CVE-2022-37773. 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-2022-45529	AeroCMS 0.0.1 edit_post. php post_category_id sql injection	A vulnerability which was classified as critical has been found in AeroCMS 0.0.1. Affected by this issue is some unknown functionality of the file \admin\includes\edit_post. php. The manipulation of the argument post_category_id leads to sql injection. This vulnerability is handled as CVE-2022-45529. 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-2022-44278	oretnom23 Sanitization Management System 1.0 id sql injection	A vulnerability which was classified as critical has been found in oretnom23 Sanitization Management System 1.0. This issue affects some unknown processing of the file /php-sms/admin /pageuser/manage_user. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-44278. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-45331	AeroCMS 0.0.1 \post. php p_id sql injection	A vulnerability was found in AeroCMS 0.0.1. It has been classified as critical. This affects an unknown part of the file \post.php. The manipulation of the argument p_id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-45331. 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-2022-4088	rickxy Stock Management System /pages/processlogin.php user/password sql injection	A vulnerability was found in rickxy Stock Management System and classified as critical. Affected by this issue is some unknown functionality of the file /pages/processlogin. php. The manipulation of the argument user/password leads to sql injection. This vulnerability is handled as CVE-2022-4088. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-45278	Jizhicms 2.3.3 get_fields. html sql injection (ID 83)	A vulnerability classified as critical was found in Jizhicms 2.3.3. This vulnerability affects unknown code of the file /index.php/admins/Fields /get_fields. html. The manipulation leads to sql injection. This vulnerability was named CVE-2022-45278. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-44140	Jizhicms 2.3.3 / Member /membered-it.html sql injection (ID 81)	A vulnerability which was classified as critical was found in Jizhicms 2.3.3. Affected is an unknown function of the file / Member /memberedit.html. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-44140. 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-2022-44860	Automotive Shop Management System 1.0 update_status. php id sql injection	A vulnerability has been found in Automotive Shop Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file / admin /transactions/update_status. php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-44860. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-44859	Automotive Shop Management System 1.0 manage_product. php id sql injection	A vulnerability which was classified as critical was found in Automotive Shop Management System 1.0. This affects an unknown part of the file /asms/admin /products/manage_ product. php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-44859. 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-2022-44858	Automotive Shop Management System 1.0 view_product.php id sql injection	A vulnerability which was classified as critical has been found in Automotive Shop Management System 1.0. Affected by this issue is some unknown functionality of the file /asms/products /view_product. php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-44858. 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-2022-45205	Jeecg-boot 3.4.3 / sys/dict /queryTableData sql injection (ID 4128)	A vulnerability which was classified as critical was found in Jeecg-boot 3.4.3. Affected is an unknown function of the file /sys/dict /queryTableData. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-45205. 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-2022-45206	Jeecg-boot 3.4.3 / sys /duplicate/check sql injection (ID 4129)	A vulnerability has been found in Jeecg-boot 3.4.3 and classified as critical. Affected by this vulnerability is an unknown functionality of the file / sys/duplicate/check. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-45206. 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-2022-45207	Jeecg-boot 3.4.3 updateNullByEmptyString sql injection (ID 4127)	A vulnerability was found in Jeecg-boot 3.4.3 and classified as critical. Affected by this issue is the function updateNullByEmptyString. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-45207. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-45208	Jeecg-boot 3.4.3 / sys/user /putRecycleBin sql injection (ID 4126)	A vulnerability was found in Jeecg-boot 3.4.3. It has been classified as critical. This affects an unknown part of the file /sys/user /putRecycleBin. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-45208. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-45210	Jeecg-boot 3.4.3 deleteRecycleBin sql injection (ID 4125)	A vulnerability was found in Jeecg-boot 3.4.3. It has been declared as critical. This vulnerability affects unknown code of the file /sys/user /deleteRecycleBin. The manipulation leads to sql injection. This vulnerability was named CVE-2022-45210. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-45932	OpenDaylight up to 0.16.4 RoleStore.java deleteRole sql injection	A vulnerability which was classified as critical has been found in OpenDaylight up to 0.16.4. This issue affects the function deleteRole of the file aaa-idm-store-h2/src/main /java/org/opendaylight/aaa /datastore/h2/RoleStore.java. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-45932. The attack needs to be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-45930	OpenDaylight up to 0.16.4 AAA DomainStore.java deleteDomain sql injection	A vulnerability classified as critical has been found in OpenDaylight up to 0.16.4. This affects the function deleteDomain of the file aaaidm-store-h2/src/main/java/org/opendaylight/aaa/datastore/h2/DomainStore.java of the component AAA. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-45930. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-44399	Poultry Farm Management System 1.0 category.php del sql injection	A vulnerability which was classified as critical was found in Poultry Farm Management System 1.0. Affected is an unknown function of the file/Redcock- Farm/farm/category.php. The manipulation of the argument del leads to sql injection. This vulnerability is traded as CVE-2022-44399. 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-2022-3769	OWM Weather Plugin up to 5.6.8 on WordPress sql injection	A vulnerability has been found in OWM Weather Plugin up to 5.6.8 and classified as critical. This vulnerability affects unknown code. The manipulation leads to sql injection. This vulnerability was named CVE-2022-3769. 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-2022-3768	WPSmartContracts Plugin up to 1.3.11 on WordPress sql injection	A vulnerability which was classified as critical was found in WPSmartContracts Plugin up to 1.3.11. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-3768. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-36193	School Management System 1.0 sql injection	A vulnerability classified as critical has been found in School Management System 1.0. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-36193. 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-2022-3865	WP User Merger Plugin up to 1.5.2 on WordPress sql injection	A vulnerability was found in WP User Merger Plugin up to 1.5.2. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-3865. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-3849	WP User Merger Plugin up to 1.5.2 on WordPress sql injection	A vulnerability was found in WP User Merger Plugin up to 1.5.2. It has been classified as critical. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-3849. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3848	WP User Merger Plugin up to 1.5.2 on WordPress sql injection	A vulnerability was found in WP User Merger Plugin up to 1.5.2 and classified as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-3848. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-3689	HTML Forms Plugin up to 1.3.24 on WordPress sql injection	A vulnerability which was classified as critical has been found in HTML Forms Plugin up to 1.3.24. Affected by this issue is some unknown functionality. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-3689. 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-2022-45329	AeroCMS 0.0.1 Search sql injection	A vulnerability has been found in AeroCMS 0.0.1 and classified as critical. This vulnerability affects unknown code. The manipulation of the argument Search leads to sql injection. This vulnerability was named CVE-2022-45329. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-42109	PuneethReddyHC onlineshopping-system-advanced 1.0 / shopping/product.php sql injection	A vulnerability was found in PuneethReddyHC onlineshopping- system-advanced 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /shopping/product.php. The manipulation of the argument p leads to sql injection. This vulnerability was named CVE-2022-42109. 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-2022-4222	SourceCodester Canteen Management System POST Request ajax_invoice.php query search sql injection	A vulnerability was found in SourceCodester Canteen Management System. It has been rated as critical. This issue affects the function query of the file ajax_invoice. php of the component POST Request Handler. The manipulation of the argument search leads to sql injection. The identification of this vulnerability is CVE-2022-4222. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2022-45328	Church Management System 1.0 /admin / edit_members.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_members. php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-45328. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Cross- Site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-40840	NdkAdvancedCustomization Fields 3.5.0 createPdf.php cross-site scripting	A vulnerability was found in NdkAdvancedCustomizatio nFields 3.5.0. It has been classified as problematic. This affects an unknown part of the file createPdf.php. The manipulation leads to crosssite scripting. This vulnerability is uniquely identified as CVE-2022-40840. 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-2022-39262	GLPI up to 10.0.3 Rich-Text Content cross-site scripting (GHSA-4x48-q2wr-cpg4)	A vulnerability which was classified as problematic has been found in GLPI up to 10.0.3. This issue affects some unknown processing of the component Rich-Text Content Handler. The manipulation leads to crosssite scripting. The identification of this vulnerability is CVE-2022-39262. The attack may 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-2022-41435	OpenWRT LuCI 22.140.66206-02913be Public Key Comment /system / sshkeys.js cross-site scripting	A vulnerability was found in OpenWRT LuCI 22.140.66206-02913be. It has been classified as problematic. This affects an unknown part of the file /system/sshkeys.js of the component Public Key Comment Handler. The manipulation leads to crosssite scripting. This vulnerability is uniquely identified as CVE-2022-41435. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-42749	CandidATS 3.0.0 ajax.php page cross-site scripting	A vulnerability classified as problematic was found in CandidATS 3.0.0. This vulnerability affects unknown code of the file ajax.php. The manipulation of the argument page leads to cross-site scripting. This vulnerability was named CVE-2022-42749. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-42748	CandidATS 3.0.0 ajax.php sortDirection cross-site scripting	A vulnerability classified as problematic has been found in CandidATS 3.0.0. This affects the function sortDirection of the file ajax.php. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-42748. 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-2022-43372	Emlog Pro 1.7.1 /admin /store.php cross-site scripting (ID 195)	A vulnerability which was classified as problematic has been found in Emlog Pro 1.7.1. Affected by this issue is some unknown functionality of the file /admin/store.php. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-43372. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-42753	SalonERP 3.0.2 page crosssite scripting	A vulnerability was found in SalonERP 3.0.2 and classified as problematic. This issue affects some unknown processing. The manipulation of the argument page leads to cross-site scripting. The identification of this vulnerability is CVE-2022-42753. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-39277	GLPI up to 10.0.3 External Link cross-site scripting (GHSA-rh-cw-8r7g-8pwc)	A vulnerability was found in GLPI up to 10.0.3 and classified as problematic. Affected by this issue is some unknown functionality of the component External Link Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-39277. The attack may be launched remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-43561	Scripts Enterprise up to 8.1.11/8.2.8/9.0.1 Web crosssite scripting	A vulnerability which was classified as problematic has been found in Scripts Enterprise up to 8.1.11/8.2.8 /9.0.1. This issue affects some unknown processing of the component Web. The manipulation leads to crosssite scripting. The identification of this vulnerability is CVE-2022-43561. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-43568	Splunk Enterprise up to 8.1.11/8.2.8/9.0.1 JSON cross-site scripting	A vulnerability classified as problematic was found in Splunk Enterprise up to 8.1.11/8.2.8/9.0.1. This vulnerability affects unknown code of the component JSON Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-43568. 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-2022-43569	Splunk Enterprise up to 8.1.11/8.2.8/9.0.1 Data Model cross-site scripting	A vulnerability was found in Splunk Enterprise up to 8.1.11/8.2.8/9.0.1. It has been classified as problematic. This affects an unknown part of the component Data Model Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-43569. 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-2022-3873	jgraph drawio up to 20.5.1 cross-site scripting	A vulnerability which was classified as problematic has been found in jgraph drawio up to 20.5.1. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-3873. 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-2022-3462	Highlight Focus Plugin up to 1.1 on WordPress Setting cross-site scripting	A vulnerability has been found in Highlight Focus Plugin up to 1.1 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-2022-3462. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-43317	oretnom23 Human Resource Management System 1.0 / hrm/index.php cross-site scripting	A vulnerability was found in oretnom23 Human Resource Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file / hrm/index.phpmsg. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-43317. 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-2022-43118	flatCore-CMS 2.1.0 Username cross-site scripting (ID 86)	A vulnerability was found in flatCore-CMS 2.1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument Username leads to cross-site scripting. This vulnerability is known as CVE-2022-43118. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-43144	SourceCodester Canteen Management System 1.0 cross-site scripting	A vulnerability was found in SourceCodester Canteen Management System 1.0 and classified as problematic. This issue affects some unknown processing. The manipulation leads to crosssite scripting. The identification of this vulnerability is CVE-2022-43144. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-43120	Intelliants Subrion CMS 4.2.1 /panel/fields/add crosssite scripting (ID 894)	A vulnerability was found in Intelliants Subrion CMS 4.2.1 and classified as problematic. This issue affects some unknown processing of the file /panel /fields/add. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-43120. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-43321	Shopwind 3.4.3 / common /library/ Page.php cross-site scripting	A vulnerability has been found in Shopwind 3.4.3 and classified as problematic. Affected by this vulnerability is an unknown functionality in the library /common/library /Page.php. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-43321. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-43320	FeehiCMS 2.1.1 index.php id cross-site scripting	A vulnerability was found in FeehiCMS 2.1.1. It has been classified as problematic. This affects an unknown part of the file /web /admin/index.phprlog% 2Fview-layer. The manipulation of the argument id leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-43320. 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-2022-43119	Clansphere CMS 2011.4 Username cross-site scripting	A vulnerability has been found in Clansphere CMS 2011.4 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument Username leads to cross-site scripting. This vulnerability was named CVE-2022-43119. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-43121	Intelliants Subrion CMS 4.2.1 cross-site scripting (ID 895)	A vulnerability was found in Intelliants Subrion CMS 4.2.1. It has been classified as problematic. Affected is an unknown function. The manipulation leads to crosssite scripting. This vulnerability is traded as CVE-2022-43121. 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-2022-26088	BMC Remedy up to 22.0 Incident Forwarding To crosssite scripting	A vulnerability classified as problematic was found in BMC Remedy up to 22.0. This vulnerability affects unknown code of the component Incident Forwarding. The manipulation of the argument To leads to cross-site scripting. This vulnerability was named CVE-2022-26088. 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-2022-3578	ProfileGrid Plugin up to 5.1.0 on WordPress a cross-site scripting	A vulnerability which was classified as problematic has been found in ProfileGrid Plugin up to 5.1.0. Affected by this issue is some unknown functionality. The manipulation of the argument a leads to cross-site scripting. This vulnerability is handled as CVE-2022-3578. 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-2022-3469	WP Attachments Plugin up to 5.0.4 on WordPress Setting cross-site scripting	A vulnerability was found in WP Attachments Plugin up to 5.0.4. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-3469. 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-2022-3415	Chat Bubble Plugin up to 2.2 on WordPress Contact Parameter contact cross-site scripting	A vulnerability was found in Chat Bubble Plugin up to 2.2. It has been classified as problematic. Affected is an unknown function of the component Contact Parameter Handler. The manipulation of the argument contact leads to cross-site scripting. This vulnerability is traded as CVE-2022-3415. 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-2022-3539	Testimonials Plugin on WordPress Setting cross-site scripting	A vulnerability has been found in Testimonials Plugin and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-3539. 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-2022-43342	Eramba GRC 2.8.1 KPI Title Add cross-site scripting	A vulnerability has been found in Eramba GRC 2.8.1 and classified as problematic. This vulnerability affects the function Add of the component KPI Title Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-43342. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-3484	WPB Show Core Plugin on WordPress cross-site scripting	A vulnerability classified as problematic was found in WPB Show Core Plugin. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-3484. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-3631	DigitialPixies OAuth Client Plugin up to 1.1.0 on WordPress Setting cross-site scripting	A vulnerability was found in DigitialPixies OAuth Client Plugin up to 1.1.0 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-2022-3631. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-40846	Tenda AC1200 15.11.0.10 (1576) hostname cross-site scripting	A vulnerability classified as problematic was found in Tenda AC1200 15.11.0.10. This vulnerability affects unknown code. The manipulation of the argument hostname leads to cross-site scripting. This vulnerability was named CVE-2022-40846. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-40844	Tenda AC1200 15.11.0.10 (1576) cross-site scripting	A vulnerability classified as problematic has been found in Tenda AC1200 15.11.0.10. This affects an unknown part. The manipulation leads to crosssite scripting. This vulnerability is uniquely identified as CVE-2022-40844. 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-2022-44071	Zenario CMS 9.3.57186 Profile cross-site scripting	A vulnerability which was classified as problematic has been found in Zenario CMS 9.3.57186. Affected by this issue is some unknown functionality of the component Profile Handler. The manipulation leads to crosssite scripting. This vulnerability is handled as CVE-2022-44071. 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-2022-44069	Zenario CMS 9.3.57186 Nest Library Module cross-site scripting	A vulnerability classified as problematic has been found in Zenario CMS 9.3.57186. Affected is an unknown function of the component Nest Library Module. The manipulation leads to crosssite scripting. This vulnerability is traded as CVE-2022-44069. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scipting attack.
CVE-2022-44073	Zenario CMS 9.3.57186 User cross-site scripting	A vulnerability which was classified as problematic was found in Zenario CMS 9.3.57186. This affects an unknown part of the component User Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-44073. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scipting attack.
CVE-2022-43263	Arobas Music Guitar Pro up to 1.10.1 on iPhone/iPad cross-site scripting	A vulnerability was found in Arobas Music Guitar Pro up to 1.10.1. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-43263. 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 Cross-site scipting attack.
CVE-2022-30768	ZoneMinder 1.36.12 Logout Username cross-site scripting	A vulnerability has been found in ZoneMinder 1.36.12 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Logout. The manipulation of the argument Username leads to cross-site scripting. This vulnerability is known as CVE-2022-30768. 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 scipting attack.
CVE-2022-44070	Zenario CMS 9.3.57186 News Article cross-site scripting	A vulnerability classified as problematic was found in Zenario CMS 9.3.57186. Affected by this vulnerability is an unknown functionality of the component News Article Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-44070. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scipting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-43142	Password Storage Application 1.0 add-fee.php cmddept cross-site scripting	A vulnerability was found in Password Storage Application 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file add-fee.php. The manipulation of the argument cmddept leads to cross-site scripting. This vulnerability is known as CVE-2022-43142. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-36432	Amasty Blog Pro Plugin 2.10.3 on Magento Preview cross-site scripting	A vulnerability was found in Amasty Blog Pro Plugin 2.10.3 and classified as problematic. Affected by this issue is some unknown functionality of the component Preview Handler. The manipulation leads to crosssite scripting. This vulnerability is handled as CVE-2022-36432. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-4053	Student Attendance Management System createClass.php className cross-site scripting	A vulnerability was found in Student Attendance Management System. It has been classified as problematic. Affected is an unknown function of the file createClass.php. The manipulation of the argument className leads to cross-site scripting. This vulnerability is traded as CVE-2022-4053. It is possible to launch the attack remotely. Furthermore there is an exploit	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-42187	Hustoj 22.09.22 /admin /problem_judge.php crosssite scripting (ID 866)	A vulnerability was found in Hustoj 22.09.22. It has been classified as problematic. Affected is an unknown function of the file /admin/problem_judge.php. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-42187. 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-2022-4068	LibreNMS Admin User View cross-site scripting	A vulnerability classified as problematic was found in LibreNMS. This vulnerability affects unknown code of the component Admin User View. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-4068. The attack can be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-3690	Popup Maker Plugin up to 1.16.10 on WordPress crosssite scripting	A vulnerability which was classified as problematic has been found in Popup Maker Plugin up to 1.16.10. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-3690. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-40470	Phpgurukul Blood Donor Management System 1.0 Add Blood Group Name cross-site scripting	A vulnerability which was classified as problematic was found in Phpgurukul Blood Donor Management System 1.0. This affects an unknown part of the component Add Blood Group Name Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-40470. 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-2022-3618	Spacer Plugin up to 3.0.6 on WordPress cross-site scripting	A vulnerability classified as problematic has been found in Spacer Plugin up to 3.0.6. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-3618. 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-2022-3753	Evaluate Plugin up to 1.0 on WordPress cross-site scripting	A vulnerability which was classified as problematic was found in Evaluate Plugin up to 1.0. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-3753. 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-2022-43117	SourceCodester Password Storage Application 1.0 Name /Username/Description/Site Feature cross-site scripting	A vulnerability was found in SourceCodester Password Storage Application 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument Name/Username/Description /Site Feature leads to crosssite scripting. This vulnerability is known as CVE-2022-43117. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-45017	WBCE CMS 1.5.4 Overview Page Settings Module Post Loop cross-site scripting (ID 525)	A vulnerability has been found in WBCE CMS 1.5.4 and classified as problematic. This vulnerability affects unknown code of the component Overview Page Settings Module. The manipulation of the argument Post Loop leads to cross-site scripting. This vulnerability was named CVE-2022-45017. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-42096	Backdrop CMS 1.23.0 Post Content cross-site scripting	A vulnerability classified as problematic was found in Backdrop CMS 1.23.0. Affected by this vulnerability is an unknown functionality of the component Post Content Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-42096. 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-2022-44787	Appalti & Contratti 9.12.2 idPagina cross-site scripting	A vulnerability which was classified as problematic has been found in Appalti & Contratti 9.12.2. This issue affects some unknown processing. The manipulation of the argument idPagina leads to cross-site scripting. The identification of this vulnerability is CVE-2022-44787. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-36180	Fusiondirectory 1.3 index.php message/plug cross-site scripting	A vulnerability was found in Fusiondirectory 1.3. It has been rated as problematic. This issue affects some unknown processing of the file /fusiondirectory/index.php. The manipulation of the argument message/plug leads to cross-site scripting. The identification of this vulnerability is CVE-2022-36180. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-38724	SilverStripe Assets /Framework Shortcode crosssite scripting	A vulnerability was found in SilverStripe Assets and Framework. It has been declared as problematic. This vulnerability affects unknown code of the component Shortcode Handler. The manipulation leads to crosssite scripting. This vulnerability was named CVE-2022-38724. 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-2022-41445	PHPGurukul Teachers Record Management System 1.0 Add Subject Page crosssite scripting	A vulnerability classified as problematic has been found in PHPGurukul Teachers Record Management System 1.0. This affects an unknown part of the component Add Subject Page. The manipulation leads to crosssite scripting. This vulnerability is uniquely identified as CVE-2022-41445. 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-2022-4105	Kiwi Test Plan cross-site scripting	A vulnerability classified as problematic was found in Kiwi. This vulnerability affects unknown code of the component Test Plan. The manipulation leads to crosssite scripting. This vulnerability was named CVE-2022-4105. The attack can be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-42097	Backdrop CMS 1.23.0 Comment cross-site scripting	A vulnerability has been found in Backdrop CMS 1.23.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Comment Handler. The manipulation leads to crosssite scripting. This vulnerability is known as CVE-2022-42097. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scipting attack.
CVE-2022-43143	Beekeeper Studio 3.6.6 Error Modal Container crosssite scripting (ID 1393)	A vulnerability was found in Beekeeper Studio 3.6.6. It has been classified as problematic. This affects an unknown part of the component Error Modal Container. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-43143. It is possible to initiatethe attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scipting attack.
CVE-2022-42094	Backdrop CMS 1.23.0 Content cross-site scripting	A vulnerability which was classified as problematic was found in Backdrop CMS 1.23.0. Affected is an unknown function of the component Content Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-42094. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scipting attack.
CVE-2022-42989	Sankhya ERP prior 4.11b81 Caixa de Entrada cross-site scripting	A vulnerability which was classified as problematic has been found in Sankhya ERP. This issue affects some unknown processing of the component Caixa de Entrada. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-42989. 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 scipting attack.
CVE-2022-42095	Backdrop CMS 1.23.0 Page Content cross-site scripting	A vulnerability was found in Backdrop CMS 1.23.0. It has been classified as problematic. Affected is an unknown function of the component Page Content Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-42095. 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 scipting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-4089	rickxy Stock Management System / pages/processlogin. php user cross-site scripting	A vulnerability was found in rickxy Stock Management System. It has been declared as problematic. This vulnerability affects unknown code of the file / pages /processlogin.php. The manipulation of the argument user leads to cross-site scripting. This vulnerability was named CVE-2022-4089. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-site scipting attack.
CVE-2022-45280	EyouCMS 1.6.0 /login. php Url cross-site scripting (ID 32)	A vulnerability which was classified as problematic has been found in EyouCMS 1.6.0. This issue affects some unknown processing of the file /login.php. The manipulation of the argument Url leads to cross-site scripting. The identification of this vulnerability is CVE-2022-45280. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scipting attack.
CVE-2022-4091	SourceCodester Canteen Management System food. php query product_name cross-site scripting	A vulnerability was found in SourceCodester Canteen Management System. It has been classified as problematic. This affects the function query of the file food. php. The manipulation of the argument product_name leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-4091. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-site scipting attack.
CVE-2022-45040	WBCE CMS 1.5.4 sections_save.php Name Section cross-site scripting	A vulnerability was found in WBCE CMS 1.5.4. It has been classified as problematic. This affects an unknown part of the file /admin/pages/sections_ save. php. The manipulation of the argument Name Section leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-45040. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scipting attack.
CVE-2022-45036	WBCE CMS 1.5.4 Search Settings Module No Results cross-site scripting	A vulnerability classified as problematic has been found in WBCE CMS 1.5.4. Affected is an unknown function of the component Search Settings Module. The manipulation of the argument No Results leads to cross-site scripting. This vulnerability is traded as CVE-2022-45036. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scipting attack.
CVE-2022-45038	WBCE CMS 1.5.4 / admin /settings/save. php Website Footer cross-site scripting	A vulnerability has been found in WBCE CMS 1.5.4 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file / admin/settings/save. php. The manipulation of the argument Website Footer leads to cross-site scripting. This vulnerability is known as CVE-2022-45038. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scipting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-45037	WBCE CMS 1.5.4 / admin /users/index. php Display Name cross-site scripting	A vulnerability which was classified as problem-atic was found in WBCE CMS 1.5.4. Affected is an unknown function of the file /admin /users/index. php. The manipulation of the argument Display Name leads to crosssite scripting. This vulnerability is traded as CVE-2022-45037. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scipt-ing attack.
CVE-2022-37720	Orchard CMS 1.10.3 Blog Post cross-site scripting	A vulnerability was found in Orchard CMS 1.10.3. It has been rated as prob-lematic. This issue affects some unknown processing of the component Blog Post Handler. The manip-ulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-37720. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scipt-ing attack.
CVE-2022-39333	Nextcloud Desktop up to 3.6.0 HTML cross-site scripting (GHSA-92p9-x79h-2mj8)	A vulnerability which was classified as problematic has been found in Next-cloud Desktop up to 3.6.0. Affected by this issue is some unknown function-ality of the component HTML Handler. The manip-ulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-39333. 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 scipt-ing attack.
CVE-2022-39331	Nexcloud Desktop up to 3.6.0 cross-site scripting (GHSA-c3xh-q694-6rc5)	A vulnerability classified as problematic has been found in Nexcloud Desktop up to 3.6.0. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-39331. 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 scipt-ing attack.
CVE-2022-39332	Nextcloud Desktop up to 3.6.0 HTML cross-site script-ing (GHSA-q9f6-4r6rh74p)	A vulnerability classified as problematic was found in Nextcloud Desktop up to 3.6.0. Affected by this vulnerability is an un-known functionality of the component HTML Handler. The manipulation leads to crosssite scripting. This vulnerability is known as CVE-2022-39332. The attack can be launched re-motely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-site scipt-ing attack.
CVE-2022-45225	Book Store Manage-ment System 1.0 / bsms_ci/index. php/ book book_title crosssite scripting	A vulnerability which was classified as problematic was found in Book Store Management System 1.0. Affected is an unknown function of the file / bsms_ci /index.php/book. The manipulation of the argument book_title leads to cross-site scripting. This vulnerability is traded as CVE-2022-45225. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scipt-ing attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-0698	Microweber 1.3.1 select-file cross-site scripting	A vulnerability has been found in Microweber 1.3.1 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument select-file leads to cross-site scripting. This vulnerability was named CVE-2022-0698. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-3822	Donations via PayPal Plugin up to 1.9.8 on WordPress Setting cross-site scripting	A vulnerability was found in Donations via PayPal Plugin up to 1.9.8 and classified as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to crosssite scripting. This vulnerability is handled as CVE-2022-3822. 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-2022-3839	Analytics for WP Plugin up to 1.5.1 on WordPress Setting cross-site scripting	A vulnerability which was classified as problematic has been found in Analytics for WP Plugin up to 1.5.1. 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-2022-3839. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-3833	ThematoSoup Fancier Author Box Plugin up to 1.4 on WordPress Setting crosssite scripting	A vulnerability classified as problematic was found in ThematoSoup Fancier Author Box Plugin up to 1.4. 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-2022-3833. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-3831	reCAPTCHA Plugin up to 1.6 on WordPress Setting cross-site scripting	A vulnerability classified as problematic has been found in reCAPTCHA Plugin up to 1.6. Affected is an unknown function of the component Setting Handler. The manipulation leads to crosssite scripting. This vulnerability is traded as CVE-2022-3831. 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-2022-3824	WP Admin UI Customize Plugin up to 1.5.12 on WordPress cross-site scripting	A vulnerability was found in WP Admin UI Customize Plugin up to 1.5.12. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to crosssite scripting. This vulnerability was named CVE-2022-3824. 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-2022-3828	Video Thumbnails Plugin up to 2.12.3 on WordPress Setting cross-site scripting	A vulnerability was found in Video Thumbnails Plugin up to 2.12.3. It has been rated as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to crosssite scripting. The identification of this vulnerability is CVE-2022-3828. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3610	Jeeng Push Notifications Plugin up to 2.0.3 on WordPress Setting cross-site scripting	A vulnerability has been found in Jeeng Push Notifications Plugin up to 2.0.3 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to crosssite scripting. This vulnerability is known as CVE-2022-3610. 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-2022-2983	Salat Times Plugin up to 3.2.1 on WordPress Setting cross-site scripting	A vulnerability which was classified as problematic has been found in Salat Times Plugin up to 3.2.1. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to crosssite scripting. The identification of this vulnerability is CVE-2022-2983. 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-2022-3834	Google Forms Plugin up to 0.95 on WordPress Setting cross-site scripting	A vulnerability was found in Google Forms Plugin up to 0.95. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to crosssite scripting. This vulnerability is handled as CVE-2022-3834. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-2311	Find and Replace All Plugin up to 1.2 on WordPress Setting Page cross-site scripting	A vulnerability classified as problematic was found in Find and Replace All Plugin up to 1.2. This vulnerability affects unknown code of the component Setting Page. The manipulation leads to crosssite scripting. This vulnerability was named CVE-2022-2311. 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-2022-44284	Dinstar FXO Analog VoIP Gateway DAG2000-160 cross-site scripting (ID 169531)	A vulnerability has been found in Dinstar FXO Analog VoIP Gateway DAG2000-160 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to crosssite scripting. This vulnerability was named CVE-2022-44284. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3601	Image Hover Effects CSS3 Plugin up to 4.5 on WordPress Setting cross-site scripting	A vulnerability which was classified as problematic was found in Image Hover Effects CSS3 Plugin up to 4.5. Affected is an unknown function of the component Setting Handler. The manipulation leads to crosssite scripting. This vulnerability is traded as CVE-2022-3601. 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-2022-36433	Amasty Blog Pro Plugin 2.10.3 on Magento Admin Panel short_content /full_content cross-site scripting	A vulnerability was found in Amasty Blog Pro Plugin 2.10.3. It has been declared as problematic. This vulnerability affects unknown code of the component Admin Panel. The manipulation of the argument short_content /full_content leads to crosssite scripting. This vulnerability was named CVE-2022-36433. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-42100	KLiK SocialMediaWebsite 1.0.1 reply-form cross-site scripting	A vulnerability classified as problematic was found in KLiK SocialMediaWebsite 1.0.1. This vulnerability affects unknown code. The manipulation of the argument reply-form leads to cross-site scripting. This vulnerability was named CVE-2022-42100. 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-2022-46147	XBlock Drag and Drop up to 2.x Image cross-site scripting (GHSA-qv6c-367r-3w6q)	A vulnerability which was classified as problematic was found in XBlock Drag and Drop up to 2.x. Affected is an unknown function of the component Image Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-46147. 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-2022-36136	ChurchCRM 4.4.5 Deposit Comment cross-site scripting	A vulnerability was found in ChurchCRM 4.4.5. It has been classified as problematic. Affected is an unknown function. The manipulation of the argument Deposit Comment leads to cross-site scripting. This vulnerability is traded as CVE-2022-36136. 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-2022-36137	ChurchCRM 4.4.5 sHeader cross-site scripting	A vulnerability was found in ChurchCRM 4.4.5. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument sHeader leads to cross-site scripting. This vulnerability is known as CVE-2022-36137. 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-2022-42099	KLiK SocialMediaWebsite 1.0.1 Forum Subject crosssite scripting	A vulnerability classified as problematic has been found in KLiK SocialMediaWebsite 1.0.1. This affects an unknown part. The manipulation of the argument Forum Subject leads to crosssite scripting. This vulnerability is uniquely identified as CVE-2022-42099. 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-2022-45221	Web-Based Student Clearance System 1.0 changepassword.php txtnew_password cross-site scripting	A vulnerability has been found in Web-Based Student Clearance System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file changepassword.php. The manipulation of the argument txtnew_password leads to cross-site scripting. This vulnerability is known as CVE-2022-45221. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-45223	Web-Based Student Clearance System 1.0 /Admin /add-student.php txtfullname cross-site scripting	A vulnerability was found in Web-Based Student Clearance System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /Admin/add-student.php. The manipulation of the argument txtfullname leads to cross-site scripting. This vulnerability is handled as CVE-2022-45223. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-45214	Sanitization Management System 1.0.0 Login.php username cross-site scripting	A vulnerability was found in Sanitization Management System 1.0.0. It has been rated as problematic. This issue affects some unknown processing of the file /php-sms /classes/Login.php. The manipulation of the argument username leads to cross-site scripting. The identification of this vulnerability is CVE-2022-45214. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-45224	Web-Based Student Clearance System 1.0 Admin /add-admin.php txtfullname cross-site scripting	A vulnerability was found in Web-Based Student Clearance System 1.0. It has been classified as problematic. This affects an unknown part of the file Admin /add-admin.php. The manipulation of the argument txtfullname leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-45224. 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-2022-4234	SourceCodester Canteen Management System youthappam/brand.php builtin_ echo brand_name cross-site scripting	A vulnerability was found in SourceCodester Canteen Management System. It has been rated as problematic. This issue affects the function builtin_echo of the file youthappam/brand.php. The manipulation of the argument brand_name leads to crosssite scripting. The identification of this vulnerability is CVE-2022-4234. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-44355	SolarView Compact 7.0 /network_test.php cross-site scripting	A vulnerability classified as problematic was found in SolarView Compact 7.0. Affected by this vulnerability is an unknown functionality of the file /network_test.php. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-44355. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-3991	Dean Oakley Photospace Gallery Plugin up to 2.3.5 on WordPress Setting update cross-site scripting	A vulnerability classified as problematic was found in Dean Oakley Photospace Gallery Plugin up to 2.3.5. This vulnerability affects the function update of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-3991. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.
CVE-2022-44279	Garage Management System 1.0 createBrand.php cross-site scripting	A vulnerability which was classified as problematic has been found in Garage Management System 1.0. Affected by this issue is some unknown functionality of the file /garage/php_action /createBrand.php. The manipulation leads to crosssite scripting. This vulnerability is handled as CVE-2022-44279. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack.

XML External Entity Attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-39353	xmldom prior 0.7.7/0.8.4/0.9.0-beta.4 improper validation of consistency within input (ID 150)	A vulnerability was found in xmldom. It has been classified as critical. This affects an unknown part. The manipulation leads to improper validation of consistency within input. This vulnerability is uniquely identified as CVE-2022- 39353. 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 XML External Entity attack
CVE-2022-42745	CandidATS 3.0.0 xml external entity reference	A vulnerability classified as problematic was found in CandidATS 3.0.0. Affected by this vulnerability is an unknown functionality. The manipulation leads to xml external entity reference. This vulnerability is known as CVE-2022-42745. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as XML External Entity attack

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-43061	Online Tours & Travels Management System 1.0 travellers.php unrestricted upload	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 / operations /travellers.php. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2022-43061. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Malicious File Upload attack
CVE-2022-42750	CandidATS 3.0.0 Cookie unrestricted upload	A vulnerability was found in CandidATS 3.0.0. It has been rated as critical. Affected by this issue is some unknown functionality of the component Cookie Handler. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2022-42750. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Malicious File Upload attack
CVE-2022-3993	kareadita kavita up to 0.6.0.2 authentication bypass	A vulnerability was found in kareadita kavita up to 0.6.0.2. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to authentication bypass by primary weakness. This vulnerability is known as CVE-2022-3993. 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 Malicious File Upload attack

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-42751	CandidATS 3.0.0 cross-site request forgery	A vulnerability has been found in CandidATS 3.0.0 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to crosssite request forgery. This vulnerability was named CVE-2022-42751. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-3451	Product Stock Manager Plugin up to 1.0.4 on WordPress AJAX Action cross-site request forgery	A vulnerability which was classified as problematic was found in Product Stock Manager Plugin up to 1.0.4. This affects an unknown part of the component AJAX Action Handler. The manipulation leads to crosssite request forgery. This vulnerability is uniquely identified as CVE-2022-3451. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-3489	WP Hide Plugin up to 0.0.2 on WordPress custom_wpadmin_slug Setting cross-site request forgery	A vulnerability was found in WP Hide Plugin up to 0.0.2 and classified as problematic. This issue affects some unknown processing of the component custom_wpadmin_slug Setting Handler. The manipulation leads to crosssite request forgery. The identification of this vulnerability is CVE-2022-3489. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-2387	Easy Digital Downloads Plugin up to 2.x on WordPress Payment History cross-site request forgery	A vulnerability which was classified as problematic has been found in Easy Digital Downloads Plugin up to 2.x. Affected by this issue is some unknown functionality of the component Payment History Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-2387. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-43031	DedeCMS 6.1.9 cross-site request forgery	A vulnerability classified as problematic has been found in DedeCMS 6.1.9. This affects an unknown part. The manipulation leads to crosssite request forgery. This vulnerability is uniquely identified as CVE-2022-43031. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-45130	Plesk Obsidian REST API /api/v2/cli/commands crosssite request forgery	A vulnerability has been found in Plesk Obsidian and classified as problematic. This vulnerability affects unknown code of the file /api/v2/cli /commands of the component REST API. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-45130. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3978	NodeBB up to 2.5.7 / register /abort cross-site request forgery (ID 11017)	A vulnerability which was classified as problematic was found in NodeBB up to 2.5.7. This affects an unknown part of the file / register/abort. The manipulation leads to crosssite request forgery. This vulnerability is uniquely identified as CVE-2022-3978. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-2449	reSmush.it Only Free Image Optimizer & Compress Plugin Plugin AJAX Action cross-site request forgery	A vulnerability was found in re Smush.it Only Free Image Optimizer & Compress Plugin Plugin up to 0.4.3 and classified as problematic. This issue affects some unknown processing of the component AJAX Action Handler. The manipulation leads to crosssite request forgery. The identification of this vulnerability is CVE-2022-2449. 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-2022-3632	DigitialPixies OAuth Client Plugin up to 1.1.0 on WordPress cross-site request forgery	A vulnerability which was classified as problematic was found in DigitialPixies OAuth Client Plugin up to 1.1.0. This affects an unknown part. The manipulation leads to crosssite request forgery. This vulnerability is uniquely identified as CVE-2022-3632. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-3538	Webmaster Tools Verification Plugin up to 1.2 on WordPress cross-site request forgery	A vulnerability classified as problematic was found in Webmaster Tools Verification Plugin up to 1.2. This vulnerability affects unknown code. The manipulation leads to crosssite request forgery. This vulnerability was named CVE-2022-3538. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-3240	Follow Me Plugin up to 3.1.1 on WordPress FollowMeIgniteSocialMedia_options_page cross-site request forgery	A vulnerability was found in Follow Me Plugin up to 3.1.1. It has been classified as problematic. Affected is the function FollowMeIgniteSocialMedia_options_page. The manipulation leads to crosssite request forgery. This vulnerability is traded as CVE-2022-3240. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-43323	EyouCMS 1.5.9-UTF8-SP1 Top Up Balance cross-site request forgery (ID 28)	A vulnerability which was classified as problematic has been found in EyouCMS 1.5.9-UTF8-SP1. Affected by this issue is some unknown functionality of the component Top Up Balance. The manipulation leads to crosssite request forgery. This vulnerability is handled as CVE-2022-43323. 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-2022-4013	Hospital Management Center appointment. php cross-site request forgery	A vulnerability classified as problematic was found in Hospital Management Center. Affected by this vulnerability is an unknown functionality of the file appointment.php. The manipulation leads to crosssite request forgery. This vulnerability is known as CVE-2022-4013. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2022-42246	Doufox 0.0.4 cross-site request forgery	A vulnerability classified as problematic has been found in Doufox 0.0.4. Affected is an unknown function. The manipulation leads to crosssite request forgery. This vulnerability is traded as CVE-2022-42246. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-3763	Booster for WooCommerce Plugin on WordPress crosssite request forgery	A vulnerability was found in Booster for WooCommerce Plugin Booster Plus for WooCommerce Plugin and Booster Elite for WooCommerce Plugin. It has been classified as problematic. Affected is an unknown function. The manipulation leads to crosssite request forgery. This vulnerability is traded as CVE-2022-3763. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-3750	Ask Me Plugin prior 6.8.7 cross-site request forgery	A vulnerability classified as problematic has been found in Ask Me Plugin. Affected is an unknown function. The manipulation leads to crosssite request forgery. This vulnerability is traded as CVE-2022-3750. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-1578	My wpdb Plugin up to 2.4 on WordPress cross-site request forgery	A vulnerability was found in My wpdb Plugin up to 2.4. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to crosssite request forgery. This vulnerability was named CVE-2022-1578. 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-2022-3688	WPQA Builder Plugin up to 5.8 on WordPress cross-site request forgery	A vulnerability classified as problematic was found in WPQA Builder Plugin up to 5.8. This vulnerability affects unknown code. The manipulation leads to crosssite request forgery. This vulnerability was named CVE-2022-3688. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3336	Event Monster Plugin up to 1.1.x on WordPress crosssite request forgery	A vulnerability was found in Event Monster Plugin up to 1.1.x. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to crosssite request forgery. This vulnerability is handled as CVE-2022-3336. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-41925	Tailscale up to 1.32.2 crosssite request forgery (GHSAqccm-wmcq-pwr6)	A vulnerability which was classified as problematic has been found in Tailscale up to 1.32.2. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022-41925. 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-2022-4090	rickxy Stock Management System us_transac.php cross-site request forgery	A vulnerability was found in rickxy Stock Management System and classified as problematic. This issue affects some unknown processing of the file us_transac.phpactionadd. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022-4090. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2022-3747	BeCustom Plugin prior 1.0.5.3 on Wordpress crosssite request forgery	A vulnerability classified as problematic has been found in BeCustom Plugin. Affected is an unknown function. The manipulation leads to crosssite request forgery. This vulnerability is traded as CVE-2022-3747. 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	NA
CVE-2022-41924	Tailscale up to 1.32.2 on Windows tailscaled cross-site request forgery (GHSA-vqp6-rc3h-83cp)	A vulnerability has been found in Tailscale up to 1.32.2 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component tailscaled. The manipulation leads to crosssite request forgery. This vulnerability is known as CVE-2022-41924. 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-2022-23044	Tiny File Manager 2.4.8 cross-site request forgery	A vulnerability was found in Tiny File Manager 2.4.8. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to crosssite request forgery. This vulnerability is known as CVE-2022-23044. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-45476	Tiny File Manager 2.4.8 cross-site request forgery	A vulnerability was found in Tiny File Manager 2.4.8. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to crosssite request forgery. This vulnerability is handled as CVE-2022-45476. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-45475	Tiny File Manager 2.4.8 cross-site request forgery	A vulnerability was found in Tiny File Manager 2.4.8. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to crosssite request forgery. This vulnerability is known as CVE-2022-45475. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-3847	Showing URL in QR Code Plugin up to 0.0.1 on WordPress Setting cross-site request forgery	A vulnerability was found in Showing URL in QR Code Plugin up to 0.0.1. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-3847. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-3850	Find and Replace All Plugin up to 1.2 on WordPress cross-site request forgery	A vulnerability which was classified as problematic was found in Find and Replace All Plugin up to 1.2. This affects an unknown part. The manipulation leads to crosssite request forgery. This vulnerability is uniquely identified as CVE-2022-3850. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-44937	Wenzhou Huoyin BossCMS 2.0.0 Administrator List Module Add cross-site request forgery	A vulnerability which was classified as problematic has been found in Wenzhou Huoyin BossCMS 2.0.0. This issue affects the function Add of the component Administrator List Module. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022-44937. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA

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.