INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

December 2022

The total zero-day vulnerabilities count for December month : 230

Command Injection	CSRF	Local File Inclusion	Malicious File Upload	SQL Injection	XSS Injection	XXE Attack
19	24	12	14	42	118	1

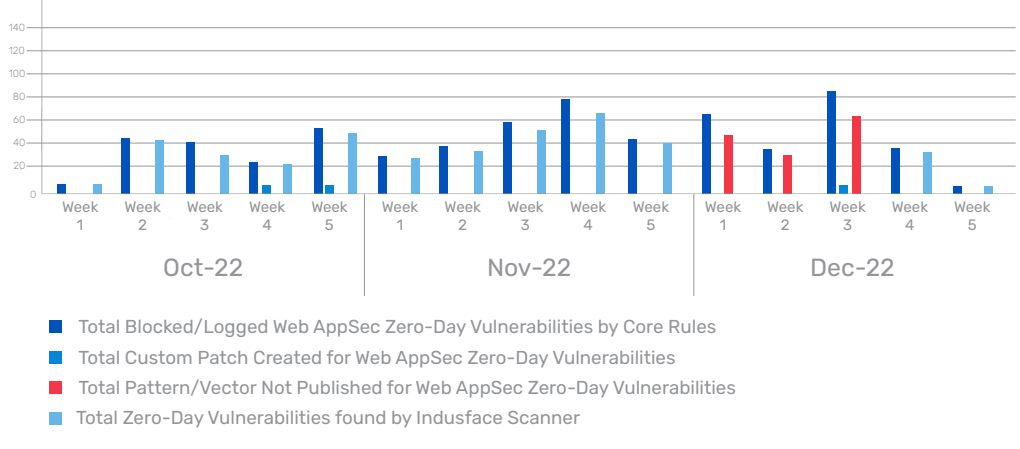
Zero-day vulnerabilities protected through core rules	226
Zero-day vulnerabilities protected through custom rules	4
Zero-day vulnerabilities for which protection can not be done	0
Zero-day vulnerabilities found by Indusface WAS	192

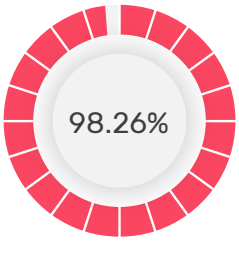
- To enable custom rules, please contact support@indusface.com
- Since the attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.

Vulnerability Trend:

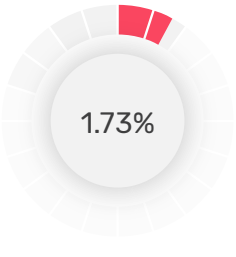
The weekly trend displays the total number of vulnerabilities discovered to the type of protection provided for the last quarter.

Weekly Vulnerability Trend

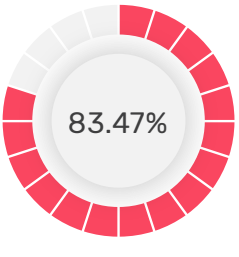




of the zero-day vulnerabilities were protected by the **core rules** in the last month.

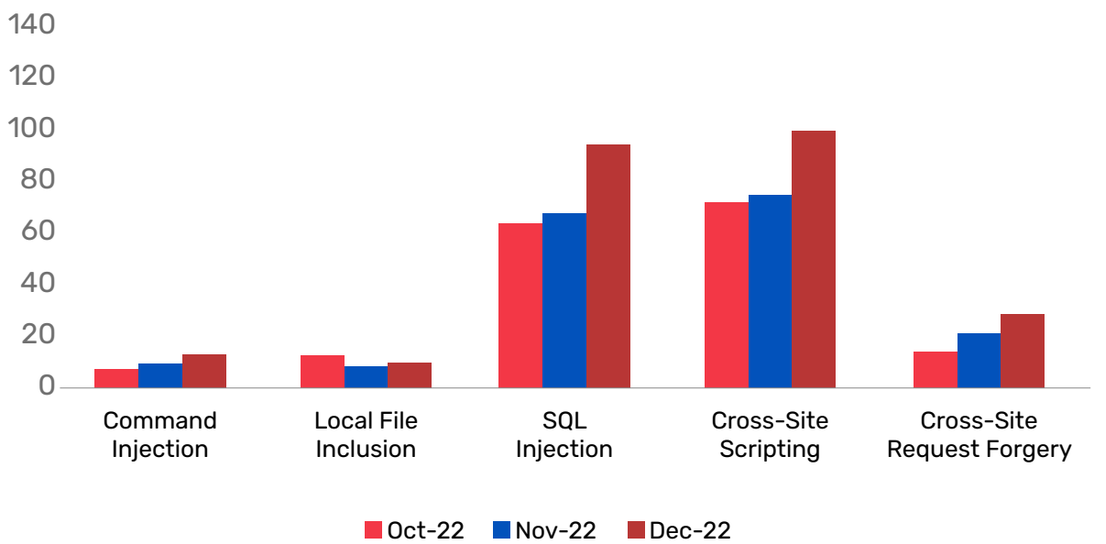


of the zero-day vulnerabilities were protected by the **custom rules** in the last month.



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-2022-4221	Asus NAS-M25 up to 1.0.1.7 Cookie os command injection	A vulnerability has been found in Asus NAS-M25 up to 1.0.1.7 and classified as very critical. This vulnerability affects unknown code of the component Cookie Handler. The manipulation leads to os command injection. This vulnerability was named CVE-2022-4221. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command injection attack
CVE-2022-4257	C-DATA Web Management System GET Parameter cgibin/jumpto.php hostname argument injection	A vulnerability was found in C-DATA Web Management System. It has been rated as critical. This issue affects some unknown processing of the file cgi-bin/jumpto.php of the component GET Parameter Handler. The manipulation of the argument hostname leads to argument injection. The identification of this vulnerability is CVE-2022-4257. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Command injection attack
CVE-2022-44928	D-Link DVG-G5402SP GE_1.03 Maintenance command injection	A vulnerability classified as critical was found in DLink DVG-G5402SP GE_1.03. This vulnerability affects unknown code of the component Maintenance. The manipulation leads to command injection. This vulnerability was named CVE-2022-44928. Access to the local network is required for this attack. Furthermore there is an 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-2022-44930	D-Link DHP-W310AV 3.10 EU command injection	A vulnerability was found in D-Link DHP-W310AV 3.10EU and classified as critical. This issue affects some unknown processing. The manipulation leads to command injection. The identification of this vulnerability is CVE-2022-44930. The attack needs to be approached within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-43325	Telos Alliance Omnia MPX Node 1.3.x/1.4.x Product License Validation command injection	A vulnerability which was classified as critical has been found in Telos Alliance Omnia MPX Node 1.3.x/1.4.x. Affected by this issue is some unknown functionality of the component Product License Validation. The manipulation leads to command injection. This vulnerability is handled as CVE-2022-43325. The attack needs to be initiated within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-45915	ILIAS up to 7.15 os-command injection	A vulnerability was found in ILIAS up to 7.15. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to os command injection. This vulnerability is known as CVE-2022-45915. 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 the scanner as command injection attack
CVE-2022-45025	Markdown Preview Enhanced PDF File Import command injection (ID 639)	A vulnerability which was classified as critical was found in Markdown Preview Enhanced. This affects an unknown part of the component PDF File Import Handler. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE2022-45025. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by the scanner as command injection attack
CVE-2022-4364	Teledyne FLIR AX8 up to 1.46.16 Web Service palette.php palette command injection	A vulnerability classified as critical has been found in Teledyne FLIR AX8 up to 1.46.16. Affected is an unknown function of the file palette.php of the component Web Service Handler. The manipulation of the argument palette leads to command injection. This vulnerability is traded as CVE-2022-4364. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by the scanner as command injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-45506	Tenda W30E 1.0.1.25/ goform/delFileName- fileNameMit com- mand injection	A vulnerability which was classified as critical has been found in Tenda W30E 1.0.1.25. Affected by this issue is some un- known functionality of the file/goform/delFileName. The manipulation of the argument fileNameMit leads to command injec- tion. This vulnerability is han- dled as CVE-2022-45506. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2022-45497	Tenda W6-S 1.0.0.4 / goform/exeCommand tpi_get_ping_output command injection	A vulnerability classified as critical was found in Tenda W6-S 1.0.0.4. This vulner- ability affects the function tpi_get_ping_output of the file /goform/ex- eCommand. The manipu- lation leads to command injection. This vulnerability was named CVE-2022-45497. The attack can only be done within the local net- work. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2022-45005	IP-COM EW9 15.11.0.14 cmd_get_ping_out- put command injection	A vulnerability was found in IP-COM EW9 15.11.0.14. It has been rated as critical. Affected by this issue is the function cmd_get_ ping_output. The manip- ulation leads to command injection. This vulnerability is han- dled as CVE-2022-45005. Access to the local net- work is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2022-46634	TOTOLINK A7100RU 7.4cu.2313_ B20191024 setting/ setWiFiWpsCfg wsc- Disabled command injection	A vulnerability has been found in TOTOLINK A7100RU 7.4cu.2313_ B20191024 and classified as critical. This vulnerabili- ty affects unknown code of the file setting/setWiFi- WpsCfg. The manipulation of the argument wscDis- abled leads to command injection. This vulnerability was named CVE-2022-46634. The attack needs to be done within the local net- work. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2022-46631	TOTOLINK A7100RU 7.4cu.2313_ B20191024 setting/ setWiFiSignalCfg wscDisabled com- mand injection	A vulnerability which was classified as critical was found in TOTOLINK A7100RU 7.4cu.2313_ B20191024. This affects an unknown part of the file setting/setWiFiSig- nalCfg. The manipulation of the argument wscDis- abled leads to command injection. This vulnerability is uniquely identified as CVE2022-46631. The attack can only be initiated within the local network. There is no exploit avail- able.	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-23474	Editor.js up to 2.25.x processHTML code injection (GHSL-2022-028)	A vulnerability was found in Editor.js up to 2.25.x. It has been classified as critical. Affected is the function processHTML of the file Editor.js. The manipulation leads to code injection. This vulnerability is traded as CVE-2022-23474. 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 command injection attack.
CVE-2022-25171	The package p4 before 0.0.7 are vulnerable to Command Injection via the run() function due to improper input sanitization	The package p4 before 0.0.7 are vulnerable to Command Injection via the run() function due to improper input sanitization	Protected by core rules	Detected by scanner as command injection attack.
CVE-2022-40624	pfSense pfBlockerNGthrough 2.1.4_27 allows remote attackers to execute arbitrary OS commands as root via the HTTP Host header, a different vulnerability than CVE-2022-31814.	pfSense pfBlockerNG through 2.1.4_27 allows remote attackers to execute arbitrary OS commands as root via the HTTP Host header, a different vulnerability than CVE-2022-31814.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2022-46538	Tenda F1203 V2.0.1.6 was discovered to contain a command injection vulnerability via the mac parameter at /goform/WriteFacMac.	Tenda F1203 V2.0.1.6 was discovered to contain a command injection vulnerability via the mac parameter at /goform/WriteFacMac.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2022-24431	All versions of package abacus-ext-cmdline are vulnerable to Command Injection via the execute function due to improper user-input sanitization.	All versions of package abacus-ext-cmdline are vulnerable to Command Injection via the execute function due to improper user-input sanitization.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2021-24942	Menu Item Visibility Control Plugin up to 0.5 on WordPress code injection	A vulnerability has been found in Menu Item Visibility Control Plugin up to 0.5 and classified as critical. This vulnerability affects unknown code. The manipulation leads to code injection. This vulnerability was named CVE-2021-24942. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-40489	ThinkCMF 6.0.7 crosssite request forgery (ID 736)	A vulnerability was found in ThinkCMF 6.0.7. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-40489. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-45674	Tenda AC6 15.03.05.19 fromSysToolReboot cross-site request forgery	A vulnerability was found in Tenda AC6 15.03.05.19. It has been classified as problematic. This affects the function fromSysToolReboot. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-45674. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-45668	Tenda i22 1.0.0.3 fromSysToolReboot cross-site request forgery	A vulnerability has been found in Tenda i22 1.0.0.3 and classified as problematic. Affected by this vulnerability is the function fromSysToolReboot. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-45668. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-45667	Tenda i22 1.0.0.3 fromSysToolRestoreSet cross-site request forgery	A vulnerability which was classified as problematic was found in Tenda i22 1.0.0.3. Affected is the function fromSysToolRestoreSet. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-45667. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-45673	Tenda AC6 15.03.05.19 fromSysToolRestoreSet cross-site request forgery	A vulnerability was found in Tenda AC6 15.03.05.19 and classified as problematic. Affected by this issue is the function fromSysToolRestoreSet. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-45673. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-4220	Chained Quiz Plugin up to 1.3.2.4 on WordPress list_questions cross-site request forgery	A vulnerability classified as problematic was found in Chained Quiz Plugin up to 1.3.2.4. Affected by this vulnerability is the function list_questions. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-4220. 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-2022-4218	Chained Quiz Plugin up to 1.3.2.4 on WordPress list_quizzes cross-site request forgery	A vulnerability classified as problematic has been found in Chained Quiz Plugin up to 1.3.2.4. Affected is the function list_quizzes. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-4218. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-4219	Chained Quiz Plugin up to 1.3.2.4 on WordPress manage cross-site request forgery	A vulnerability was found in Chained Quiz Plugin up to 1.3.2.4. It has been declared as problematic. Affected by this vulnerability is the function manage. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-4219. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-44849	MetInfo 7.7 Administrator List crosssite request forgery	A vulnerability was found in MetInfo 7.7. It has been classified as problematic. This affects an unknown part of the component Administrator List. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-44849. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-4349	CTF-hacker pwn delete.html cross-site request forgery	A vulnerability classified as problematic has been found in CTF-hacker pwn. This affects an unknown part of the file delete.html. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-4349. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2022-45228	Dragino Lora LG01 18ed40 IoT 4.3.4 Logout Page cross-site request forgery	A vulnerability was found in Dragino Lora LG01 18ed40 IoT 4.3.4. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Logout Page. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-45228. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-46059	AeroCMS 0.0.1 cross-site request forgery	A vulnerability which was classified as problematic has been found in AeroCMS 0.0.1. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-46059. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-46062	Gym Management System 0.0.1 cross-site request forgery	A vulnerability classified as problematic was found in Gym Management System 0.0.1. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-46062. The attack can belaunched remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3883	Block Bad Bots and Stop Bad Bots Crawlers and Spiders and Anti Spam Protection Plugin AJAX Action cross-site request forgery	A vulnerability was found in Block Bad Bots and Stop Bad Bots Crawlers and Spiders and Anti Spam Protection Plugin up to 7.23. It has been declared as problematic. This vulnerability affects unknown code of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-3883. 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-2022-45980	Tenda AX12 22.03.01.21_CN SysToolRestoreSet cross-site request forgery	A vulnerability was found in Tenda AX12 22.03.01.21_CN. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /goform/SysToolRestoreSet. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-45980. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-4004	Donation Button Plugin up to 4.0.0 on WordPress donation_button_twilio_send_test_sms cross-site request forgery	A vulnerability which was classified as problematic has been found in Donation Button Plugin up to 4.0.0. This issue affects the function donation_button_twilio_send_test_sms. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022-4004. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-3879	Car Dealer and Vehicle Sales Plugin up to 3.04 on WordPress AJAX Action cross-site request forgery	A vulnerability was found in Car Dealer and Vehicle Sales Plugin up to 3.04 and classified as problematic. Affected by this issue is some unknown functionality of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-3879. 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-2022-4016	Booster for WooCommerce Plugin on WordPress cross-site request forgery	A vulnerability was found in Booster for WooCommerce Plugin Booster Plus for WooCommerce Plugin and Booster Elite for WooCommerce Plugin and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-4016. The attack may be launched 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-2022-3946	Welcart e-Commerce Plugin up to 2.8.3 on WordPress AJAX Action cross-site request forgery	A vulnerability was found in Welcart e-Commerce Plugin up to 2.8.3 and classified as problematic. This issue affects some unknown processing of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022-3946. 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-2022-3880	Disable Json API, Login Lockdown, XMLRPC, Pingback, Stop User Enumeration Anti Hacker Scan Plugin AJAX Action cross-site request forgery	A vulnerability was found in Disable Json API Login Lockdown XMLRPC Pingback Stop User Enumeration Anti Hacker Scan Plugin up to 4.19. It has been classified as problematic. This affects an unknown part of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-3880. 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-2022-46074	oretnom23 Helmet Store Showroom 1.0 cross-site request forgery	A vulnerability was found in oretnom23 Helmet Store Showroom 1.0 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-46074. The attack may belaunched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-3427	Corner Ad Plugin up to 1.0.56 on WordPress corner_ad_settings_page cross-site request forgery	A vulnerability was found in Corner Ad Plugin up to 1.0.56. It has been rated as problematic. Affected by this issue is the function corner_ad_settings_page. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-3427. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-4124	The Popup Manager WordPress plugin through 1.6.6 does not have authorisation and CSRF checks when deleting popups, which could allow unauthenticated users to delete them	The Popup Manager WordPress plugin through 1.6.6 does not have authorisation and CSRF checks when deleting popups, which could allow unauthenticated users to delete them	Protected by core rules	NA
CVE-2022-4024	The Registration Forms WordPress plugin before 3.8.1.3 does not have authorization and CSRF when deleting users via an init action handler, allowing unauthenticated attackers to delete arbitrary users (along with their posts)	The Registration Forms WordPress plugin before 3.8.1.3 does not have authorization and CSRF when deleting users via an init action handler, allowing unauthenticated attackers to delete arbitrary users (along with their posts)	Protected by core rules	NA

Local File Inclusion vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-44900	py7zr up to 0.20.0 7z File SevenZipFile. extractall pathname traversal	A vulnerability which was classified as critical was found in py7zr up to 0.20.0. Affected is the function SevenZipFile.extractall of the component 7z File Handler. The manipulation leads to pathname traversal. This vulnerability is traded as CVE-2022-44900. The attack needs to be done within the local network. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2022-45269	Gmao Linx Sphere SCS.Web.Server.SPI pathname traversal	A vulnerability which was classified as problematic was found in Gmao Linx Sphere. This affects an unknown part of the component SCS.Web.Server.SPI. The manipulation leads to pathname traversal. This vulnerability is uniquely identified as CVE-2022-45269. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2022-4511	RainyGao DocSys path traversal (I66A3V)	A vulnerability has been found in RainyGao DocSys and classified as critical. Affected by this vulnerability is an unknown functionality of the component com.DocSystem.controller. UserControllergetUserImg. The manipulation leads to path traversal: &039;../filedir&039;. This vulnerability is known as CVE-2022-4511. The attack can be launched remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2022-29511	Lansweeper 10.1.1.0 HTTP Request KnowledgebasePage Actions.aspx ImportArticles path traversal (TALOS2022-1530)	A vulnerability classified as problematic has been found in Lansweeper 10.1.1.0. Affected is the function ImportArticles of the file KnowledgebasePageActions. aspx of the component HTTP Request Handler. The manipulation leads to path traversal. This vulnerability is traded as CVE-2022-29511. 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 local file inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-23512	MeterSphere up to 2.4.0 /&quot deleteBodyFiles path traversal (GHSA5m-wp-xw7p-5j27)	A vulnerability was found in MeterSphere up to 2.4.0. It has been declared as critical. Affected by this vulnerability is the function ApiTestCaseService:: deleteBodyFiles of the file /&quot. The manipulation leads to path traversal. This vulnerability is known as CVE-2022-23512. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2022-29517	Lansweeper 10.1.1.0 HTTP Request HelpdeskActions.aspx edittemplate path traversal (TALOS-2022-1529)	A vulnerability classified as critical was found in Lansweeper 10.1.1.0. Affected by this vulnerability is the function edittemplate of the file HelpdeskActions.aspx of the component HTTP Request Handler. The manipulation leads to path traversal. This vulnerability is known as CVE-2022-29517. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2022-32573	Lansweeper 10.1.1.0 HTTP Request AssetActions.aspx addDoc path traversal (TALOS2022-1528)	A vulnerability which was classified as critical has been found in Lansweeper 10.1.1.0. Affected by this issue is the function addDoc of the file AssetActions.aspx of the component HTTP Request Handler. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-32573. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2020-24855	easywebpack-cli up to 4.5.1 GET Request pathname traversal (ID 25)	A vulnerability was found in easywebpack-cli up to 4.5.1 and classified as problematic. This issue affects some unknown processing of the component GET Request Handler. The manipulation leads to pathname traversal. The identification of this vulnerability is CVE-2020-24855. The attack needs to be initiated within the local network. There is no exploit available. It is recommended to upgrade the affected component	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2022-45969	Alist 3.4.0 pathname traversal (ID 2449)	A vulnerability classified as critical has been found in Alist 3.4.0. This affects an unknown part. The manipulation leads to pathname traversal. This vulnerability is uniquely identified as CVE-2022-45969. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-4606	PHP Remote File Inclusion in GitHub repository flatpress-blog /flatpress prior to 1.3.	PHP Remote File Inclusion in GitHub repository flatpressblog/flatpress prior to 1.3.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2022-36221	Nokia Fastmile 3tg00118abad52 is affected by an authenticated path traversal vulnerability which allows attackers to read any named pipe file on the system.	Nokia Fastmile 3tg00118abad52 is affected by an authenticated path traversal vulnerability which allows attackers to read any named pipe file on the system.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2022-47945	ThinkPHP Framework before 6.0.14 allows local file inclusion via the lang parameter when the language pack feature is enabled (lang_switch_on=true). An unauthenticated and remote attacker can exploit this to execute arbitrary operating system commands, as demonstrated by including pearcmd.php.	ThinkPHP Framework before 6.0.14 allows local file inclusion via the lang parameter when the language pack feature is enabled (lang_switch_on=true). An unauthenticated and remote attacker can exploit this to execute arbitrary operating system commands, as demonstrated by including pearcmd.php.	Protected by core rules	Detected by scanner as local file inclusion attack.

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-36431	Rocket TRUfusion Enterprise prior 7.9.6.1 JSP File unrestricted upload	A vulnerability which was classified as critical was found in Rocket TRUfusion Enterprise. This affects an unknown part of the component JSP File Handler. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2022-36431. 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	NA
CVE-2022-4272	FeMiner wms savenewproduct.php upfile unrestricted upload	A vulnerability which was classified as critical has been found in FeMiner wms. Affected by this issue is some unknown functionality of the file /product/savenewproduct.phpflag1. The manipulation of the argument upfile leads to unrestricted upload. This vulnerability is handled as CVE-2022-4272. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2022-4273	SourceCodester Human Resource Management System 1.0 Content-Type employee.php pfimg unrestricted upload	A vulnerability which was classified as critical has been found in SourceCodester Human Resource Management System 1.0. This issue affects some unknown processing of the file /hrm/controller/employee.php of the component Content-Type Handler. The manipulation of the argument pfimg leads to unrestricted upload. The identification of this vulnerability is CVE-2022-4273. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-4276	House Rental System POST Request tenant-engine.php id_photo unrestricted upload	A vulnerability was found in House Rental System and classified as critical. Affected by this issue is some unknown functionality of the file tenant-engine.php of the component POST Request Handler. The manipulation of the argument id_photo leads to unrestricted upload. This vulnerability is handled as CVE-2022-4276. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2022-45009	oretnom23 Online Leave Management System 1.0 SystemSettings.php unrestricted upload	A vulnerability was found in oretnom23 Online Leave Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /leave_system/classes/SystemSettings. php?fupdate_settings. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2022-45009. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-45548	AyaCMS 3.1.2 unrestricted upload	A vulnerability classified as critical was found in AyaCMS 3.1.2. This vulnerability affects unknown code. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2022-45548. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	NA
CVE-2022-3989	Motors Plugin up to 1.4.3 on WordPress AJAX Action unrestricted upload	A vulnerability which was classified as critical was found in Motors Plugin up to 1.4.3. Affected is an unknown function of the component AJAX Action Handler. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2022-3989. 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-2022-3921	Listingo Theme up to 3.2.6 AJAX Action unrestricted upload	A vulnerability has been found in Listingo Theme up to 3.2.6 and classified as critical. This vulnerability affects unknown code of the component AJAX Action Handler. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2022-3921. 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-2022-46135	In AeroCms v0.0.1, there is an arbitrary file upload vulnerability at /admin/posts. php?source=edit_post, through which we can upload webshell and control the web server.	In AeroCms v0.0.1, there is an arbitrary file upload vulnerability at /admin/posts. php?source=edit_post, through which we can upload webshell and control the web server.	Protected by core rules	NA
CVE-2022-45968	Alist 3.4.0 unrestricted upload (ID 2444)	A vulnerability classified as critical has been found in Alist 3.4.0. This affects an unknown part. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2022-45968. The attack needs to be initiated within the local network. There is no exploit available.	Protected by custom rules.	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-4061	The JobBoardWP WordPress plugin before 1.2.2 does not properly validate file names and types in its file upload functionalities, allowing unauthenticated users to upload arbitrary files such as PHP.	The JobBoardWP WordPress plugin before 1.2.2 does not properly validate file names and types in its file upload functionalities, allowing unauthenticated users to upload arbitrary files such as PHP.	Protected by core rules	NA
CVE-2022-4506	OpenEMR up to 7.0.0.1 unrestricted upload	A vulnerability was found in OpenEMR up to 7.0.0.1. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2022-4506. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by custom rules	NA
CVE-2021-36573	Feehi CMS 2.1.1 Image unrestricted upload (ID 59)	A vulnerability classified as critical was found in Feehi CMS 2.1.1. This vulnerability affects unknown code of the component Image Handler. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2021-36573. The attack can only be initiated within the local network. There is no exploit available.	Protected by custom rules.	NA
CVE-2020-20588	zhimengzhe iBarn 1.5 Avatar action/Core. class.php upload unrestricted upload (ID 13)	A vulnerability classified as critical has been found in zhimengzhe iBarn 1.5. Affected is the function upload of the file action/Core. class.php of the component Avatar Handler. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2020-20588. It is possible to launch the attack remotely. There is no exploit available.	Protected by custom rules	NA

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-30528	asith-eranga ISIC Tour Booking controller.php username sql injection	A vulnerability was found in asith-eranga ISIC Tour Booking. It has been classified as critical. Affected is an unknown function of the file /system/user/modules/mod_users /controller.php. The manipulation of the argument username leads to sql injection. This vulnerability is traded as CVE-2022-30528. 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-2022-4248	Movie Ticket Booking System editBooking. php id sql injection	A vulnerability which was classified as critical has been found in Movie Ticket Booking System. This issue affects some unknown processing of the file editBooking.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-4248. 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-2022-4247	Movie Ticket Booking System booking.php id sql injection	A vulnerability classified as critical was found in Movie Ticket Booking System. This vulnerability affects unknown code of the file booking.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-4247. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-44347	Sanitization Management System 1.0 id sql injection	A vulnerability has been found in Sanitization Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /php-sms /admin/pageinquiries/ view_inquiry. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-44347. 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-2022-44348	Sanitization Management System 1.0 update_status.php id sql injection	A vulnerability was found in Sanitization Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /php-sms/admin/ orders /update_status. php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-44348. 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-2022-44945	Rukovoditel 3.2.1 heading_field_id sql injection (ID 16)	A vulnerability which was classified as critical has been found in Rukovoditel 3.2.1. Affected by this issue is some unknown functionality. The manipulation of the argument heading_field_id leads to sql injection. This vulnerability is handled as CVE-2022-44945. 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-2022-44277	Sanitization Management System 1.0 Master.php sql injection	A vulnerability which was classified as critical has been found in Sanitization Management System 1.0. This issue affects some unknown processing of the file /php-sms /classes/ Master.phpfdelete_product. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-44277. 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-2022-44290	webTareas 2.4p5 deleteapprovalstages. php id sql injection	A vulnerability was found in webTareas 2.4p5. It has been declared as critical. This vulnerability affects unknown code of the file deleteapprovalstages.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-44290. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-44291	webTareas 2.4p5 phasesets.php id sql injection	A vulnerability was found in webTareas 2.4p5. It has been rated as critical. This issue affects some unknown processing of the file phasesets.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-44291. 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-2022-44345	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 /php-sms/admin/pagequotes/view_quote. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-44345. 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-2022-4277	Shaoxing Background Management System /Default/Bd id sql injection	A vulnerability was found in Shaoxing Background Management System. It has been declared as critical. This vulnerability affects unknown code of the file /Default/Bd. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-4277. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-4274	House Rental System /view-property.php property_id sql injection	A vulnerability which was classified as critical was found in House Rental System. Affected is an unknown function of the file /view-property.php. The manipulation of the argument property_id leads to sql injection. This vulnerability is traded as CVE-2022-4274. 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-2022-4278	SourceCodester Human Resource Management System 1.0 /hrm /employee-add.php empid sql injection	A vulnerability was found in SourceCodester Human Resource Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /hrm/employeeadd.php. The manipulation of the argument empid leads to sql injection. The identification of this vulnerability is CVE-2022-4278. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-4275	House Rental System POST Request searchproperty.php search_property sql injection	A vulnerability has been found in House Rental System and classified as critical. Affected by this vulnerability is an unknown functionality of the file search-property.php of the component POST Request Handler. The manipulation of the argument search_property leads to sql injection. This vulnerability is known as CVE-2022-4275. The attack can 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-2022-45010	Simple Phone Book App 1.0 Book/Directory editid sql injection	A vulnerability has been found in Simple Phone Book App 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file Book/Directory. The manipulation of the argument editid leads to sql injection. This vulnerability is known as CVE-2022-45010. 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-2022-44393	oretnom23 Sanitization Management System 1.0 id sql injection	A vulnerability was found in oretnom23 Sanitization Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /php-sms/admin/pageservices/view_service. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-44393. 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-2022-4375	Mingsoft MCMS up to 5.2.9 /cms/category/list sqlWhere sql injection	A vulnerability was found in Mingsoft MCMS up to 5.2.9. It has been classified as critical. Affected is an unknown function of the file /cms/category/list. The manipulation of the argument sqlWhere leads to sql injection. This vulnerability is traded as CVE-2022-4375. It is possible to launch the attack remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-44838	Automotive Shop Management System 1.0 view_service.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 /services/view_service.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-44838. 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-2022-4403	SourceCodester Canteen Management System ajax_represent. php customer_id sql injection	A vulnerability classified as critical was found in SourceCodester Canteen Management System. This vulnerability affects unknown code of the file ajax_represent. php. The manipulation of the argument customer_id leads to sql injection. This vulnerability was named CVE-2022-4403. 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-2022-4416	RainyGao DocSys getRe posAllUsers. do getReposAllUsers searchWord/reposId sql injection (I65QEE)	A vulnerability was found in RainyGao DocSys. It has been declared as critical. This vulnerability affects the function getReposAllUsers of the file /DocSystem/Repos / getReposAllUsers.do. The manipulation of the argument searchWord/reposId leads to sql injection. This vulnerability was named CVE-2022-4416. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-46051	AeroCMS 0.0.1 approve sql injection	A vulnerability which was classified as critical was found in AeroCMS 0.0.1. Affected is an unknown function. The manipulation of the argument approve leads to sql injection. This vulnerability is traded as CVE-2022-46051. 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-2022-3915	Dokan Plugin up to 3.7.5 on WordPress SQL Statement sql injection	A vulnerability was found in Dokan Plugin up to 3.7.5. It has been rated as critical. Affected by this issue is some unknown functionality of the component SQL Statement Handler. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-3915. 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-2022-3925	buddybadges Plugin up to 1.0.0 on WordPress SQL Statement sql injection	A vulnerability classified as critical has been found in buddybadges Plugin up to 1.0.0. This affects an unknown part of the component SQL Statement Handler. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-3925. 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-2022-46122	oretnom23 Helmet Store Showroom Site 1.0 view_category. php id sql injection	A vulnerability classified as critical was found in oretnom23 Helmet Store Showroom Site 1.0. Affected by this vulnerability is an unknown functionality of the file /hss/admin /categories/view_category.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-46122. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-46123	oretnom23 Helmet Store Showroom Site 1.0 manage_catego-ry.php id sql injection	A vulnerability which was classified as critical has been found in oretnom23 Helmet Store Showroom Site 1.0. Affected by this issue is some unknown functionality of the file /hss/admin/catego-ries/manage_category. php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-46123. 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-2022-46127	oretnom23 Helmet Store Showroom Site 1.0 Master.php sql injection	A vulnerability has been found in oretnom23 Helmet Store Showroom Site 1.0 and classified as critical. This vulnerability affects unknown code of the file /hss/classes /Mas-ter.phpfdelete_product. The manipulation leads to sql injection. This vulnerability was named CVE-2022-46127. The attack needs to be ap-proached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-46126	oretnom23 Helmet Store Showroom Site 1.0 manage_brand. php id sql injection	A vulnerability which was classified as critical was found in oretnom23 Helmet Store Showroom Site 1.0. This affects an unknown part of the file / hss/admin/brands/man-age_brand. php. The ma-nipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-46126. Access to the local network is required for this attack to suc-ceed. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-46118	oretnom23 Helmet Store Showroom Site 1.0 id sql injection	A vulnerability which was classified as critical has been found in oretnom23 Helmet Store Showroom Site 1.0. This issue affects some unknown processing of the file /hss /pageprod-uct_per_brand. The ma-nipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-46118. 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-2022-46125	oretnom23 Helmet Store Showroom Site 1.0 id sql injection	A vulnerability was found in oretnom23 Helmet Store Showroom Site 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /hss/admin /pageclient/ manage_client. The ma-nipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-46125. Access to the local net-work is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-46443	mesinkasir Bangres-to 1.0 itemqty sql injection	A vulnerability was found in mesinkasir Bangresto 1.0. It has been rated as critical. This issue affects some unknown process-ing. The manipulation of the argument itemqty leads to sql injection. The identification of this vulnerability is CVE-2022-46443. 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-2022-46117	oretnom23 Helmet Store Showroom Site 1.0 /hss/ id sql injection	A vulnerability classified as critical was found in oretnom23 Helmet Store Showroom Site 1.0. This vulnerability affects unknown code of the file / hss/pageview_product. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-46117. 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-2022-46124	oretnom23 Helmet Store Showroom Site 1.0 id sql injection	A vulnerability was found in oretnom23 Helmet Store Showroom Site 1.0. It has been classified as critical. This affects an unknown part of the file /hss/admin/ pageuser /manage_user. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-46124. 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-2022-46121	oretnom23 Helmet Store Showroom Site 1.0 id sql injection	A vulnerability was found in oretnom23 Helmet Store Showroom Site 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /hss/admin /pageproducts/manage_ product. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2022-46121. 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-2022-46120	oretnom23 Helmet Store Showroom Site 1.0 id sql injection	A vulnerability has been found in oretnom23 Helmet Store Showroom Site 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /hss/admin/page-products/view_product. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-46120. 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-2022-46071	oretnom23 Helmet Store Showroom 1.0 Login Page sql injection	A vulnerability was found in oretnom23 Helmet Store Showroom 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the component Login Page. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-46071. 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-2022-46119	oretnom23 Helmet Store Showroom Site 1.0 /hss/c sql injection	A vulnerability which was classified as critical was found in oretnom23 Helmet Store Showroom Site 1.0. Affected is an unknown function of the file / hss/pagecategories. The manipulation of the argument c leads to sql injection. This vulnerability is traded as CVE-2022-46119. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-38488	logrocket-oauth2-example up to 2020-05-27 /auth/register username sql injection	A vulnerability classified as critical was found in logrocketoauth2-example up to 2020-05-27. Affected by this vulnerability is an unknown functionality of the file /auth /register. The manipulation of the argument username leads to sql injection. This vulnerability is known as CVE-2022-38488. 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-2022-46072	oretnom23 Helmet Store Showroom 1.0 sql injection	A vulnerability classified as critical has been found in oretnom23 Helmet Store Showroom 1.0. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-46072. 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-2022-4566	A vulnerability, which was classified as critical, has been found in y_project RuoYi 4.7.5. This issue affects some unknown processing of the file com/ruoyi/generator/controller /GenController. The manipulation leads to sql injection. The name of the patch is 167970e5c-4da7bb46217f 576dc50622b-83f32b40. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-215975.	A vulnerability, which was classified as critical, has been found in y_project RuoYi 4.7.5. This issue affects some unknown processing of the file com/ruoyi/generator/controller /GenController. The manipulation leads to sql injection. The name of the patch is 167970e5c-4da7bb46217f576d-c50622b83f32b40. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-215975.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-45041	SQL Injection exits in xinhu < 2.5.0	SQL Injection exits in xinhu < 2.5.0	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2022-4050	The JoomSport WordPress plugin before 5.2.8 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by unauthenticated users	The JoomSport WordPress plugin before 5.2.8 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by unauthenticated users	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2020-24600	Shilpisoft capexweb 1.1 GET Request capexweb. cap_sendMail sql injection	A vulnerability was found in Shilpisoft capexweb 1.1 and classified as critical. Affected by this issue is some unknown functionality of the file servlet/capexweb.cap_sendMail of the component GET Request Handler. The manipulation leads to sql injection. This vulnerability is handled as CVE-2020-24600. 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.

Cross-Site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-4252	SourceCodester Canteen Management System categories.php builtin_echo cross-site scripting	A vulnerability was found in SourceCodester Canteen Management System. It has been classified as problematic. This affects the function builtin_echo of the file categories.php. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-4252. 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-2022-4253	SourceCodester Canteen Management System customer.php builtin_echo cross-site scripting	A vulnerability was found in SourceCodester Canteen Management System. It has been declared as problematic. This vulnerability affects the function builtin_echo of the file customer. php. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-4253. 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-2022-4251	Movie Ticket Booking System editBooking.php cross-site scripting	A vulnerability was found in Movie Ticket Booking System and classified as problematic. Affected by this issue is some unknown functionality of the file editBooking.php. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-4251. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-40849	ThinkCMF 6.0.7 Slideshow Management cross-site scripting (ID 737)	A vulnerability classified as problematic was found in ThinkCMF 6.0.7. Affected by this vulnerability is an unknown functionality of the component Slideshow Management. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-40849. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4249	Movie Ticket Booking System POST Request ORDER_ID cross-site scripting	A vulnerability which was classified as problematic was found in Movie Ticket Booking System. Affected is an unknown function of the component POST Request Handler. The manipulation of the argument ORDER_ID leads to cross-site scripting. This vulnerability is traded as CVE-2022-4249. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4250	Movie Ticket Booking System booking.php id crosssite scripting	A vulnerability has been found in Movie Ticket Booking System and classified as problematic. Affected by this vulnerability is an unknown functionality of the file booking.php. The manipulation of the argument id leads to cross-site scripting. This vulnerability is known as CVE-2022-4250. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-44957	webTareas 2.4p5 / clients /listclients. php Name crosssite scripting (ID 11)	A vulnerability which was classified as problematic has been found in webTareas 2.4p5. This issue affects some unknown processing of the file / clients/listclients.php. The manipulation of the argument Name leads to cross-site scripting. The identification of this vulnerability is CVE-2022-44957. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-44955	webTareas 2.4p5 Chat Messages cross-site scripting	A vulnerability which was classified as problematic was found in webTareas 2.4p5. This affects the function Chat. The manipulation of the argument Messages leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-44955. 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-2022-44961	webTareas 2.4p5 / forums /editforum. php Name crosssite scripting	A vulnerability was found in webTareas 2.4p5 and classified as problematic. Affected by this issue is some unknown functionality of the file /forums/ editforum.php. The manipulation of the argument Name leads to cross-site scripting. This vulnerability is handled as CVE-2022-44961. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-44959	webTareas 2.4p5 listmeetings.php Name crosssite scripting	A vulnerability which was classified as problematic was found in webTareas 2.4p5. Affected is an unknown function of the file /meetings/listmeetings. php. The manipulation of the argument Name leads to cross-site scripting. This vulnerability is traded as CVE-2022-44959. 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-2022-44953	webTareas 2.4p5 listfiles.php Name cross-site scripting	A vulnerability was found in webTareas 2.4p5. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /linkedcontent/listfiles.php. The manipulation of the argument Name leads to cross-site scripting. This vulnerability is handled as CVE-2022-44953. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-44956	webTareas 2.4p5 listprojects. php Name cross-site scripting	A vulnerability classified as problematic was found in webTareas 2.4p5. This vulnerability affects unknown code of the file /projects /listprojects.php. The manipulation of the argument Name leads to cross-site scripting. This vulnerability was named CVE-2022-44956. 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-2022-44960	webTareas 2.4p5 search. php Search cross-site scripting	A vulnerability has been found in webTareas 2.4p5 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /general/search.php-searchtypesimple. The manipulation of the argument Search leads to cross-site scripting. This vulnerability is known as CVE-2022-44960. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-44954	webTareas 2.4p5 listcontacts.php Last Name cross-site scripting (ID 10)	A vulnerability classified as problematic has been found in webTareas 2.4p5. This affects an unknown part of the file /contacts/listcontacts.php. The manipulation of the argument Last Name leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-44954. 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-2022-44962	webTareas 2.4p5 viewcalendar.php Subject cross-site scripting (ID 12)	A vulnerability was found in webTareas 2.4p5. It has been classified as problematic. This affects an unknown part of the file /calendar/viewcalendar.php. The manipulation of the argument Subject leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-44962. 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-2022-4271	osticket up to 1.16.3 crosssite scripting	A vulnerability classified as problematic was found in osticket up to 1.16.3. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-4271. 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-2022-44949	Rukovoditel 3.2.1 Add New Field Short Name cross-site scripting (ID 12)	A vulnerability has been found in Rukovoditel 3.2.1 and classified as problematic. This vulnerability affects unknown code of the file /index.phpmoduleentities/fields&entities_id24 of the component Add New Field Handler. The manipulation of the argument Short Name leads to cross-site scripting. This vulnerability was named CVE-2022-44949. 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-2022-44948	Rukovoditel 3.2.1 Entities Group Name cross-site scripting	A vulnerability which was classified as problematic was found in Rukovoditel 3.2.1. This affects an unknown part of the file at /index.phpmoduleentities/entities_groups of the component Entities Group Handler. The manipulation of the argument Name leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-44948. 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-2022-44944	Rukovoditel 3.2.1 Add Announcement Title crosssite scripting (ID 14)	A vulnerability classified as problematic has been found in Rukovoditel 3.2.1. Affected is an unknown function of the file /index.phpmodulehelp_pages/pages&entities_id24 of the component Add Announcement Handler. The manipulation of the argument Title leads to cross-site scripting. This vulnerability is traded as CVE-2022-44944. 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-2022-44951	Rukovoditel 3.2.1 Add New Form Tab Name cross-site scripting (ID 11)	A vulnerability was found in Rukovoditel 3.2.1. It has been classified as problematic. Affected is an unknown function of the file /index.phpmoduleentities/forms&entities_id24 of the component Add New Form Tab Handler. The manipulation of the argument Name leads to cross-site scripting. This vulnerability is traded as CVE-2022-44951. 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-2022-44952	Rukovoditel 3.2.1 Copyright Text cross-site scripting	A vulnerability was found in Rukovoditel 3.2.1. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /index.phpmodule-configuration /application. The manipulation of the argument Copyright Text leads to cross-site scripting. This vulnerability is known as CVE-2022-44952. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-44950	Rukovoditel 3.2.1 Name cross-site scripting (ID 10)	A vulnerability was found in Rukovoditel 3.2.1 and classified as problematic. This issue affects some unknown processing of the file /index.phpmoduleentities/fields&entities_id24. The manipulation of the argument Name leads to cross-site scripting. The identification of this vulnerability is CVE-2022-44950. 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-2022-44946	Rukovoditel 3.2.1 Add Page Title cross-site scripting (ID 15)	A vulnerability classified as problematic was found in Rukovoditel 3.2.1. Affected by this vulnerability is an unknown functionality of the file /index.phpmodulehelp_pages/pages&entities_id24 of the component Add Page Handler. The manipulation of the argument Title leads to cross-site scripting. This vulnerability is known as CVE-2022-44946. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-44947	Rukovoditel 3.2.1 Highlight Row Note cross-site scripting (ID 13)	A vulnerability which was classified as problematic has been found in Rukovoditel 3.2.1. Affected by this issue is some unknown functionality of the file /index.phpmoduleentities /listing_types&entities_id24 of the component Highlight Row Handler. The manipulation of the argument Note leads to crosssite scripting. This vulnerability is handled as CVE-2022-44947. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4217	Chained Quiz Plugin up to 1.3.2.2 on WordPress api_key cross-site scripting (ID 2824193)	A vulnerability was found in Chained Quiz Plugin up to 1.3.2.2. It has been rated as problematic. This issue affects some unknown processing. The manipulation of the argument api_key leads to cross-site scripting. The identification of this vulnerability is CVE-2022-4217. The attack may be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4216	Chained Quiz Plugin up to 1.3.2.2 on WordPress facebook_appid cross-site scripting	A vulnerability was found in Chained Quiz Plugin up to 1.3.2.2. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument facebook_appid leads to cross-site scripting. This vulnerability was named CVE-2022-4216. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4211	Chained Quiz Plugin up to 1.3.2 on WordPress chainedquiz_list emailf crosssite scripting	A vulnerability which was classified as problematic has been found in Chained Quiz Plugin up to 1.3.2. This issue affects some unknown processing of the file chainedquiz_list. The manipulation of the argument emailf leads to cross-site scripting. The identification of this vulnerability is CVE-2022-4211. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4214	Chained Quiz Plugin up to 1.3.2.3 on WordPress chainedquiz_list ip cross-site scripting	A vulnerability was found in Chained Quiz Plugin up to 1.3.2.3 and classified as problematic. Affected by this issue is some unknown functionality of the file chainedquiz_list. The manipulation of the argument ip leads to cross-site scripting. This vulnerability is handled as CVE-2022-4214. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4212	Chained Quiz Plugin up to 1.3.2 on WordPress chainedquiz_list ipf cross-site scripting	A vulnerability which was classified as problematic was found in Chained Quiz Plugin up to 1.3.2. Affected is an unknown function of the file chainedquiz_list. The manipulation of the argument ipf leads to cross-site scripting. This vulnerability is traded as CVE-2022-4212. 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-2022-4208	Chained Quiz Plugin up to 1.3.2 on WordPress chainedquiz_list datef crosssite scripting	A vulnerability was found in Chained Quiz Plugin up to 1.3.2. It has been rated as problematic. Affected by this issue is some unknown functionality of the file chainedquiz_list. The manipulation of the argument datef leads to cross-site scripting. This vulnerability is handled as CVE-2022-4208. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4210	Chained Quiz Plugin up to 1.3.2 on WordPress chainedquiz_list dnf crosssite scripting	A vulnerability classified as problematic was found in Chained Quiz Plugin up to 1.3.2. This vulnerability affects unknown code of the file chainedquiz_list. The manipulation of the argument dnf leads to cross-site scripting. This vulnerability was named CVE-2022-4210. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4209	Chained Quiz Plugin up to 1.3.2 on WordPress chainedquiz_list pointsf crosssite scripting	A vulnerability classified as problematic has been found in Chained Quiz Plugin up to 1.3.2. This affects an unknown part of the file chainedquiz_list. The manipulation of the argument pointsf leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-4209. 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-2022-4279	SourceCodester Human Resource Management System 1.0 / hrm /employeeview.php search cross-site scripting	A vulnerability classified as problematic has been found in SourceCodester Human Resource Management System 1.0. Affected is an unknown function of the file /hrm/employeeview. php. The manipulation of the argument search leads to cross-site scripting. This vulnerability is traded as CVE-2022-4279. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4215	Chained Quiz Plugin up to 1.3.2.3 on WordPress chainedquiz_list date crosssite scripting	A vulnerability was found in Chained Quiz Plugin up to 1.3.2.3. It has been classified as problematic. This affects an unknown part of the file chainedquiz_list. The manipulation of the argument date leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-4215. 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-2022-43499	SHIRASAGI up to 1.16.1 cross-site scripting	A vulnerability has been found in SHIRASAGI up to 1.16.1 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-43499. 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-2022-43363	Telegram Web 15.3.1 crosssite scripting	A vulnerability was found in Telegram Web 15.3.1. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-43363. The attack may be initiated remotely. There is no exploit available. The real existence of this vulnerability is still doubted at the moment.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-44361	ZZCMS 2022 admin/ad_list.php cross-site scripting	A vulnerability which was classified as problematic has been found in ZZCMS 2022. This issue affects some unknown processing of the file admin/ad_list.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-44361. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4341	csliuwy coder-chain_gdut cross-site scripting	A vulnerability has been found in csliuwy coder-chain_gdut and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /back/index.php/user/User/1. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-4341. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-23475	daloRADIUS up to 1.3 mngdel.php cross-site scripting (GHSA-c9xx-6mvw-9v84)	A vulnerability was found in daloRADIUS up to 1.3. It has been classified as problematic. Affected is an unknown function of the file mng-del.php. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-23475. 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 Cross-site scripting attack
CVE-2022-45217	Book Store Management System 1.0.0 Add New System User Module Level cross-site scripting	A vulnerability has been found in Book Store Management System 1.0.0 and classified as problematic. This vulnerability affects unknown code of the component Add New System User Module. The manipulation of the argument Level leads to crosssite scripting. This vulnerability was named CVE-2022-45217. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-45008	oretnom23 Online Leave Management System 1.0 Create New Module Name cross-site scripting	A vulnerability which was classified as problematic has been found in oretnom23 Online Leave Management System 1.0. Affected by this issue is some unknown functionality of the file /leave_system/admin/pagemaintenance/department of the component Create New Module. The manipulation of the argument Name leads to cross-site scripting. This vulnerability is handled as CVE-2022-45008. 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-2022-44153	Rapid Software Rapid SCADA 5.8.4 cross-site scripting	A vulnerability was found in Rapid Software Rapid SCADA 5.8.4 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-44153. The attack may be launched remotely. There is no exploit available	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-45916	ILIAS up to 7.15 cross-site scripting	A vulnerability has been found in ILIAS up to 7.15 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-45916. 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-2022-4348	y_project RuoYi-Cloud JSON cross-site scripting	A vulnerability was found in y_project RuoYi-Cloud. It has been rated as problematic. Affected by this issue is some unknown functionality of the component JSON Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-4348. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4347	xiandafu beetl-bbs WebUtils.java user cross-site scripting	A vulnerability was found in xiandafu beetl-bbs. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file WebUtils.java. The manipulation of the argument user leads to cross-site scripting. This vulnerability is known as CVE-2022-4347. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4350	Mingsoft MCMS 5.2.8 search .do content_title cross-site scripting	A vulnerability which was classified as problematic was found in Mingsoft MCMS 5.2.8. Affected is an unknown function of the file search.do. The manipulation of the argument content_title leads to cross-site scripting. This vulnerability is traded as CVE-2022-4350. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4354	LinZhaoguan pb-cms 2.0 Message Board /blog /comment cross-site scripting	A vulnerability was found in LinZhaoguan pb-cms 2.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /blog/comment of the component Message Board. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-4354. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-4353	LinZhaoguan pb-cms 2.0 IpUtil.getIpAddr cross-site scripting	A vulnerability has been found in LinZhaoguan pb-cms 2.0 and classified as problematic. Affected by this vulnerability is the function IpUtil.getIpAddr. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-4353. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-44213	ZKTeco ZKBio ECO ADMS up to 3.1-164 cross-site scripting	A vulnerability was found in ZKTeco ZKBio ECO ADMS up to 3.1-164 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-44213. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4401	pallidlight online-courseselection-system cross-site scripting	A vulnerability was found in pallidlight online-course-selectionsystem. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-4401. 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-2022-34297	Yii Yii2 Gii up to 2.2.4 any cross-site scripting	A vulnerability has been found in Yii Yii2 Gii up to 2.2.4 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument any leads to cross-site scripting. This vulnerability was named CVE-2022-34297. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4408	thorsten phpmyfaq up to 3.1.8 cross-site scripting	A vulnerability has been found in thorsten phpmyfaq up to 3.1.8 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-4408. 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-2022-4413	nuxt framework up to 3.0.0-rc.12 cross-site scripting	A vulnerability classified as problematic has been found in nuxt framework up to 3.0.0-rc.12. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-4413. 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-2022-45758	SENS 1.0 getRegister crosssite scripting (ID 19)	A vulnerability which was classified as problematic was found in SENS 1.0. Affected is the function getRegister. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-45758. 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-2022-45028	Arris NVG443B 9.3.0h3d36 HTTP POST /cgi-bin/logs.ha cross-site scripting	A vulnerability classified as problematic has been found in Arris NVG443B 9.3.0h3d36. Affected is an unknown function of the file /cgi-bin/logs.ha of the component HTTP POST Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-45028. 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-2022-44303	Resque Scheduler 1.27.4 {schedule_job} args crosssite scripting	A vulnerability has been found in Resque Scheduler 1.27.4 and classified as problematic. This vulnerability affects unknown code of the file /resque/delayed/jobs/{schedule_job}. The manipulation of the argument args leads to cross-site scripting. This vulnerability was named CVE-2022-44303. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-23519	rails-html-sanitizer cross-site scripting	A vulnerability was found in rails-html-sanitizer. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-23519. 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-2022-23518	rails-html-sanitizer URI cross-site scripting	A vulnerability was found in rails-html-sanitizer. It has been declared as problematic. This vulnerability affects unknown code of the component URI Handler. The manipulation leads to crosssite scripting. This vulnerability was named CVE-2022-23518. 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-2022-23520	rails-html-sanitizer cross-site scripting	A vulnerability was found in rails-html-sanitizer and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-23520. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-3862	Livemesh Addons for Elementor Plugin up to 7.2.3 on WordPress Setting crosssite scripting	A vulnerability has been found in Livemesh Addons for Elementor Plugin up to 7.2.3 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-2022-3862. 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-2022-4000	WooCommerce Shipping Plugin up to 1.2.11 on WordPress Setting cross-site scripting	A vulnerability has been found in WooCommerce Shipping Plugin up to 1.2.11 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-4000. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-3935	Welcart e-Commerce Plugin up to 2.8.3 on WordPress cross-site scripting	A vulnerability which was classified as problematic was found in Welcart e-Commerce Plugin up to 2.8.3. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-3935. 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-2022-3919	Jetpack CRM Plugin up to 5.4.2 on WordPress Setting cross-site scripting	A vulnerability classified as problematic has been found in Jetpack CRM Plugin up to 5.4.2. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-3919. 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-2022-4005	Donation Button Plugin up to 4.0.0 on WordPress crosssite scripting	A vulnerability which was classified as problematic has been found in Donation Button Plugin up to 4.0.0. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-4005. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4010	mage Hover Effects Plugin up to 5.3 on WordPress Setting cross-site scripting	A vulnerability which was classified as problematic was found in Image Hover Effects Plugin up to 5.3. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-4010. 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-2022-3908	Helloprint Plugin up to 1.4.6 on WordPress cross-site scripting	A vulnerability was found in Helloprint Plugin up to 1.4.6. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-3908. 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-2022-3934	Flat PM Plugin up to 2.661 on WordPress cross-site scripting	A vulnerability was found in Flat PM Plugin up to 2.661. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-3934. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-3933	Essential Real Estate Plugin up to 3.9.5 on WordPress some cross-site scripting	A vulnerability classified as problematic was found in Essential Real Estate Plugin up to 3.9.5. Affected by this vulnerability is an unknown functionality. The manipulation of the argument some leads to cross-site scripting. This vulnerability is known as CVE-2022-3933. 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-2022-45970	Alist 3.5.1 Bulletin Board cross-site scripting (ID 2457)	A vulnerability was found in Alist 3.5.1. It has been classified as problematic. Affected is an unknown function of the component Bulletin Board. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-45970. 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-2022-4502	OpenEMR up to 7.0.0.1 cross-site scripting	A vulnerability was found in OpenEMR up to 7.0.0.1. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-4502. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component	Protected by core rules	Detected by scanner as Cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31358	Proxmox Virtual Environment prior 7.2-3 / api2 /html/ cross-site scripting	A vulnerability which was classified as problematic has been found in Proxmox Virtual Environment. This issue affects some unknown processing of the file /api2/html/. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-31358. 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-2022-46073	oretnom23 Helmet Store Showroom 1.0 cross-site scripting	A vulnerability has been found in oretnom23 Helmet Store Showroom 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-46073. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4520	WSO2 carbon-registry up to 4.8.11 Advanced Search advancedSearchFormajaxprocessor.jsp cross-site scripting (ID 404)	A vulnerability was found in WSO2 carbon-registry up to 4.8.11. It has been rated as problematic. Affected by this issue is some unknown functionality of the file components/registry/org.wso2. carbon.registry.search.ui/src/main/resources/web/search /advancedSearchForm-ajaxprocessor.jsp of the component Advanced Search. The manipulation of the argument mediaType /rightOp/leftOp/rightPropertyValue/leftPropertyValue leads to cross-site scripting. This vulnerability is handled as CVE-2022-4520. 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-2022-4503	OpenEMR up to 7.0.0.1 cross-site scripting	A vulnerability was found in OpenEMR up to 7.0.0.1. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-4503. 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-2022-28703	Lansweeper 10.1.1.0 HTTP Request HdConfigActions. aspx altertextlanguages cross-site scripting (TALOS2022-1532)	A vulnerability has been found in Lansweeper 10.1.1.0 and classified as problematic. This vulnerability affects the function altertextlanguages of the file HdConfigActions.aspx of the component HTTP Request Handler. The manipulation leads to basic cross-site scripting. This vulnerability was named CVE-2022-28703. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2020-36607	FeehiCMS up to 2.0.8 HTML Tag lang cross-site scripting (ID 45)	A vulnerability which was classified as problematic was found in FeehiCMS up to 2.0.8. This affects an unknown part of the component HTML Tag Handler. The manipulation of the argument lang leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2020-36607. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2021-39427	188Jianzhan 2.10 / admin /reg.php username cross-site scripting	A vulnerability which was classified as problematic has been found in 188Jianzhan 2.10. This issue affects some unknown processing of the file / admin/reg.php. The manipulation of the argument username leads to cross-site scripting. The identification of this vulnerability is CVE-2021-39427. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-44235	Beijing Zed-3 VoIP Simplicity ASG 8.5.0.17807 cross-site scripting	A vulnerability was found in Beijing Zed-3 VoIP Simplicity ASG 8.5.0.17807 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to crosssite scripting. This vulnerability is handled as CVE-2022-44235. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2021-39428	EyouCMS 1.5.4 Users.php edit_users_head_pic filename cross-site scripting (ID 14)	A vulnerability was found in EyouCMS 1.5.4 and classified as problematic. This issue affects the function edit_users_head_pic of the file Users.php. The manipulation of the argument filename leads to cross-site scripting. The identification of this vulnerability is CVE-2021-39428. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2021-36572	FeehiCMS up to 2.1.1 Login name cross-site scripting (ID 58)	A vulnerability was found in FeehiCMS up to 2.1.1. It has been declared as problematic. This vulnerability affects unknown code of the component Login. The manipulation of the argument name leads to cross-site scripting. This vulnerability was named CVE-2021-36572. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-40001	FeehiCMS up to 2.1.1 Article Page cross-site scripting (ID 65)	A vulnerability classified as problematic has been found in FeehiCMS up to 2.1.1. Affected is an unknown function of the component Article Page. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-40001. 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-2022-45033	Expense Tracker 1.0 Chat Text cross-site scripting	A vulnerability was found in Expense Tracker 1.0. It has been classified as problematic. This affects an unknown part of the component Chat Text Handler. The manipulation leads to crosssite scripting. This vulnerability is uniquely identified as CVE-2022-45033. 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-2022-40373	FeehiCMS up to 2.1.1 XML File cross-site scripting (ID 67)	A vulnerability has been found in FeehiCMS up to 2.1.1 and classified as problematic. This vulnerability affects unknown code of the component XML File Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-40373. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-40000	FeehiCMS up to 2.1.1 Admin Login Page username cross-site scripting (ID 64)	A vulnerability classified as problematic was found in FeehiCMS up to 2.1.1. Affected by this vulnerability is an unknown functionality of the component Admin Login Page. The manipulation of the argument username leads to cross-site scripting. This vulnerability is known as CVE-2022-40000. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-40002	FeehiCMS up to 2.1.1 / cms /notify callback cross-site scripting (ID 66)	A vulnerability was found in FeehiCMS up to 2.1.1. It has been rated as problematic. This issue affects some unknown processing of the file /cms/notify. The manipulation of the argument callback leads to cross-site scripting. The identification of this vulnerability is CVE-2022-40002. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2020-20589	FeehiCMS up to 2.0.8 HTML Tag lang cross-site scripting (ID 45)	A vulnerability which was classified as problematic has been found in FeehiCMS up to 2.0.8. Affected by this issue is some unknown functionality of the component HTML Tag Handler. The manipulation of the argument lang leads to cross-site scripting. This vulnerability is handled as CVE-2020-20589. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4605	Cross-site Scripting (XSS) - Stored in GitHub repository flatpressblog/flatpress prior to 1.3.	Cross-site Scripting (XSS) - Stored in GitHub repository flatpressblog/flatpress prior to 1.3.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4596	A vulnerability, which was classified as problematic, has been found in Shoplazza 1.1. This issue affects some unknown processing of the file /admin/api/admin/articles/ of the component Add Blog Post Handler. The manipulation of the argument Title leads to cross-site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-216191.	A vulnerability, which was classified as problematic, has been found in Shoplazza 1.1. This issue affects some unknown processing of the file /admin/api/admin/articles/ of the component Add Blog Post Handler. The manipulation of the argument Title leads to cross-site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-216191.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4597	A vulnerability, which was classified as problematic, was found in Shoplazza LifeStyle 1.1. Affected is an unknown function of the file /admin/api/admin/v2_products of the component Create Product Handler. The manipulation leads to cross-site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-216192.	A vulnerability, which was classified as problematic, was found in Shoplazza LifeStyle 1.1. Affected is an unknown function of the file /admin/api/admin/v2_products of the component Create Product Handler. The manipulation leads to cross-site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-216192.	Protected by core rules	Detected by scanner as Cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3877	A vulnerability, which was classified as problematic, was found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome. Affected is an unknown function of the component URL Field Handler. The manipulation leads to cross-site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. VDB-216246 is the identifier assigned to this vulnerability.	A vulnerability, which was classified as problematic, was found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome. Affected is an unknown function of the component URL Field Handler. The manipulation leads to crosssite scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. VDB-216246 is the identifier assigned to this vulnerability.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-40435	Employee Performance Evaluation System v1.0 was discovered to contain a persistent cross-site scripting (XSS) vulnerability via adding new entries under the Departments and Designations module.	Employee Performance Evaluation System v1.0 was discovered to contain a persistent cross-site scripting (XSS) vulnerability via adding new entries under the Departments and Designations module.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4614	Cross-site Scripting (XSS) - Stored in GitHub repository alagrede/znote-app prior to 1.7.11.	Cross-site Scripting (XSS) - Stored in GitHub repository alagrede/znote-app prior to 1.7.11.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4615	Cross-site Scripting (XSS) - Reflected in GitHub repository openemr/openemr prior to 7.0.0.2.	Cross-site Scripting (XSS) - Reflected in GitHub repository openemr/openemr prior to 7.0.0.2.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4609	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.9.0.	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.9.0.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4112	The Quizlord WordPress plugin through 2.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	The Quizlord WordPress plugin through 2.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4125	The Popup Manager WordPress plugin through 1.6.6 does not have authorisation and CSRF check when creating / updating popups, and is missing sanitisation as well as escaping, which could allow unauthenticated attackers to create arbitrary popups and add Stored XSS payloads as well	The Popup Manager WordPress plugin through 1.6.6 does not have authorisation and CSRF check when creating/updating popups, and is missing sanitisation as well as escaping, which could allow unauthenticated attackers to create arbitrary popups and add Stored XSS payloads as well	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-3832	The External Media WordPress plugin before 1.0.36 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	The External Media WordPress plugin before 1.0.36 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	Protected by core rules	Detected by scanner as Cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3937	The Easy Video Player WordPress plugin before 1.2.2.3 does not sanitize and escapes some parameters, which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks.	The Easy Video Player WordPress plugin before 1.2.2.3 does not sanitize and escapes some parameters, which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4058	The Photo Gallery by 10Web WordPress plugin before 1.8.3 does not validate and escape some parameters before outputting them back in in JS code later on in another page, which could lead to Stored XSS issue when an attacker makes a logged in admin open a malicious URL or page under their control.	The Photo Gallery by 10Web WordPress plugin before 1.8.3 does not validate and escape some parameters before outputting them back in in JS code later on in another page, which could lead to Stored XSS issue when an attacker makes a logged in admin open a malicious URL or page under their control.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-3985	The Videojs HTML5 Player WordPress plugin before 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	The Videojs HTML5 Player WordPress plugin before 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-3983	The Checkout for PayPal WordPress plugin before 1.0.14 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	The Checkout for PayPal WordPress plugin before 1.0.14 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-3984	The Flowplayer Video Player WordPress plugin before 1.0.5 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	The Flowplayer Video Player WordPress plugin before 1.0.5 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-3987	The Responsive Lightbox2 WordPress plugin before 1.0.4 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	The Responsive Lightbox2 WordPress plugin before 1.0.4 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	Protected by core rules	Detected by scanner as Cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-3986	The WP Stripe Checkout WordPress plugin before 1.2.2.21 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	The WP Stripe Checkout WordPress plugin before 1.2.2.21 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4640	A vulnerability has been found in Mingsoft MCMS 5.2.9 and classified as problematic. Affected by this vulnerability is the function save of the component Article Handler. The manipulation leads to crosssite scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216499.	A vulnerability has been found in Mingsoft MCMS 5.2.9 and classified as problematic. Affected by this vulnerability is the function save of the component Article Handler. The manipulation leads to cross-site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216499.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-46095	Sourcecodester Covid-19 Directory on Vaccination System 1.0 was discovered to contain a Cross-Site Scripting (XSS) vulnerability via verification.php because the program does not verify the txtvaccinationID parameter.	Sourcecodester Covid-19 Directory on Vaccination System 1.0 was discovered to contain a Cross-Site Scripting (XSS) vulnerability via verification.php because the program does not verify the txtvaccinationID parameter.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-46096	A cross-site scripting (XSS) vulnerability in Sourcecodester Online Covid19 Directory on Vaccination System v1.0 allows attackers to execute arbitrary code via the txtfullname parameter or txtphone parameter to register.php without logging in.	A cross-site scripting (XSS) vulnerability in Sourcecodester Online Covid-19 Directory on Vaccination System v1.0 allows attackers to execute arbitrary code via the txtfullname parameter or txtphone parameter to register.php without logging in.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-40841	A cross-site scripting (XSS) vulnerability in NdkAdvancedCustomizationFields v3.5.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payloads injected into the "htmlNodes" parameter.	A cross-site scripting (XSS) vulnerability in NdkAdvancedCustomizationFields v3.5.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payloads injected into the "htmlNodes" parameter.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-25929	The package smoothie from 1.31.0 and before 1.36.1 are vulnerable to Cross-site Scripting (XSS) due to improper user input sanitization in strokeStyle and tooltipLabel properties. Exploiting this vulnerability is possible when the user can control these properties.	The package smoothie from 1.31.0 and before 1.36.1 are vulnerable to Cross-site Scripting (XSS) due to improper user input sanitization in strokeStyle and tooltipLabel properties. Exploiting this vulnerability is possible when the user can control these properties.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-4617	Cross-site Scripting (XSS) - Reflected in GitHub repository microweber/microweber prior to 1.3.2.	Cross-site Scripting (XSS) - Reflected in GitHub repository microweber/microweber prior to 1.3.2.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-46491	A Cross-Site Request Forgery (CSRF) vulnerability in the Add Administrator function of the default version of nbnbk allows attackers to arbitrarily add Administrator accounts.	A Cross-Site Request Forgery (CSRF) vulnerability in the Add Administrator function of the default version of nbnbk allows attackers to arbitrarily add Administrator accounts.	Protected by core rules	Detected by scanner as Cross-site scripting attack
CVE-2022-44380	Snipe-IT before 6.0.14 is vulnerable to cross-site Scripting (XSS) for View Assigned Assets.	Snipe-IT before 6.0.14 is vulnerable to cross-site Scripting (XSS) for View Assigned Assets.	Protected by core rules	Detected by scanner as Cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-30134	php-mod curl up to 2.3.1 post_file_ path_upload.php key cross-site scripting	A vulnerability was found in php-mod curl up to 2.3.1. It has been classified as problematic. Affected is an unknown function of the file post_file_path_upload.php. The manipulation of the argument key leads to cross-site scripting. This vulnerability is traded as CVE-2021-30134. 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-2015-8354	Ultimate Member Plugin up to 1.3.28 on WordPress wpadmin/ users.php _refer crosssite scripting (ID 134601 / ID 803448)	A vulnerability which was classified as problematic was found in Ultimate Member Plugin up to 1.3.28. This affects an unknown part of the file wp-admin/users.php. The manipulation of the argument _refer as part of Parameter leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2015-8354. 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-2015-8353	Role Scoper Plugin up to 1.3.66 on WordPress Edit Page wp-admin/admin.php object_name cross-site scripting (ID 134600 / ID 803448)	A vulnerability which was classified as problematic has been found in Role Scoper Plugin up to 1.3.66. Affected by this issue is some unknown functionality of the file wp-admin/admin.php of the component Edit Page. The manipulation of the argument object_name as part of Parameter leads to cross-site scripting. This vulnerability is handled as CVE-2015-8353. 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-2015-9230	BulletProof Security Plugin up to 52.4 on WordPress Backup db-backup-security. php DBTablePrefix cross-site scripting (ID 135125)	A vulnerability was found in BulletProof Security Plugin up to 52.4. It has been classified as problematic. Affected is an unknown function of the file admin/db-backup-security/db-backupsecurity. php of the component Backup. The manipulation of the argument DBTablePrefix as part of Parameter leads to cross-site scripting. This vulnerability is traded as CVE-2015-9230. 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-2022-4690	usememos up to 0.8.x crosssite scripting	A vulnerability was found in usememos memos up to 0.8.x. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-4690. 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-2022-4692	usememos up to 0.8.x crosssite scripting	A vulnerability was found in usememos memos up to 0.8.x. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-4692. 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

XML External Entity Vulnerabilties

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-45326	Kwoksys Kwok Information Server up to 2.9.5.SP30 xml injection	A vulnerability was found in Kwoksys Kwok Information Server up to 2.9.5.SP30. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to xml injection. This vulnerability was named CVE-2022-45326. 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 external xml entity attack.

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

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

EMAIL - sales@indusface.com

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