INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

December 2023

The total zero-day vulnerabilities count for December month: 222

Command Injection	CSRF	Local File Inclusion	CRLF Injection	Malicious File Upload	XML External Entity	SQL Injection	Cross-site Scripting
25	32	18	2	7	1	49	88

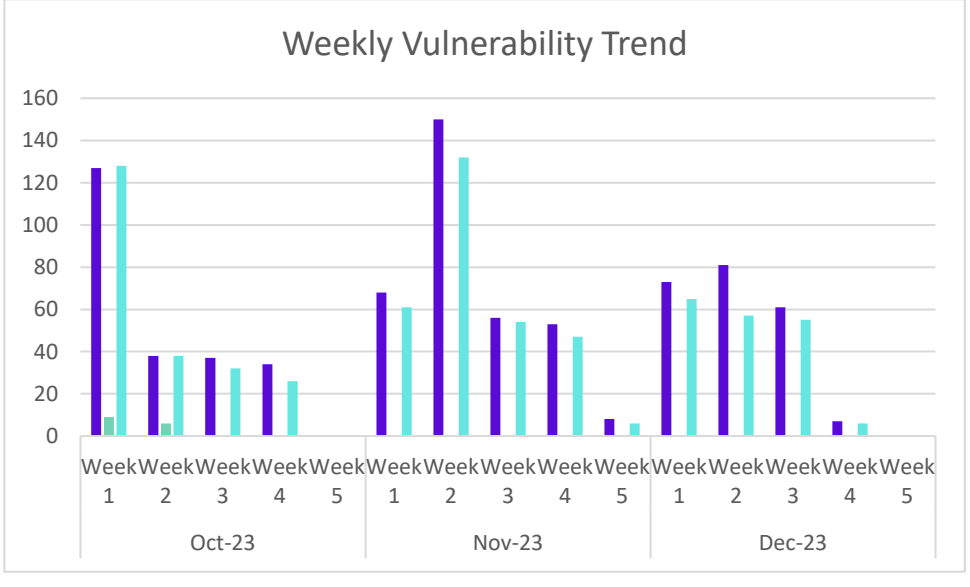
Zero-day vulnerabilities protected through core rules	222
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities for which protection cannot be done	0
Zero-day vulnerabilities found by Indusface WAS	183

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

Vulnerability Trend:

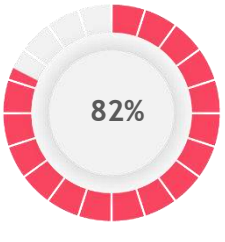
The weekly trend displays the total number of vulnerabilities discovered and the type of protection provided for the last quarter.

Weekly Vulnerability Trend



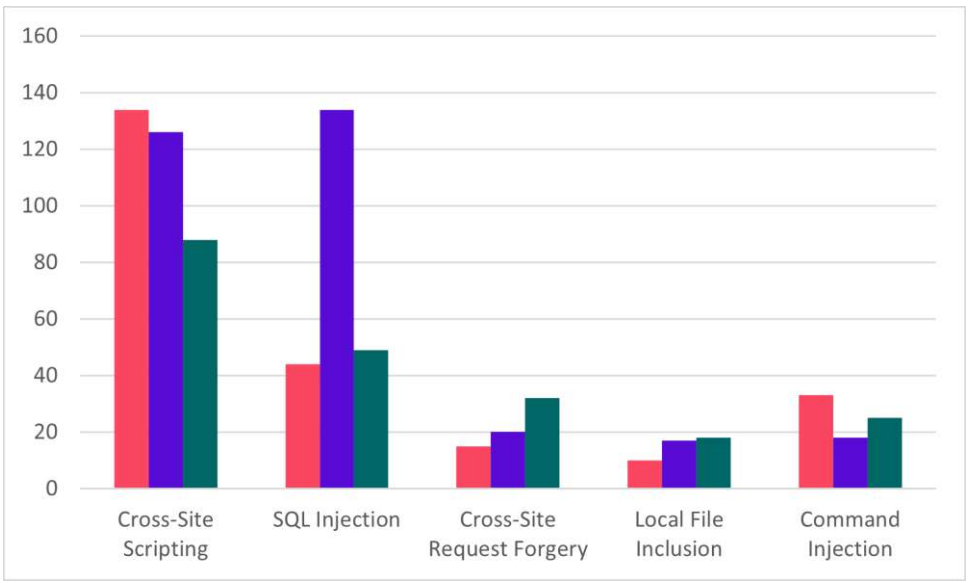
of the zero-day vulnerabilities were protected by the core rules in the last month

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-2023-6309	moses-smt mosesdecoder up to 4.0 trans_result.php input1 os command injection	A vulnerability which was classified as critical was found in moses-smt mosesdecoder up to 4.0. This affects an unknown part of the file contrib/iSenWeb/trans_result.php. The manipulation of the argument input1 leads to os command injection. This vulnerability is uniquely identified as CVE-2023-6309. The attack can only be done within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-6304	Tecno 4G Portable WiFi TR118 TR118-M30E-RR-D-EnFrArSwHaPo-OP-V008-20220830 Ping Tool goform_get_cmd_process url os command injection	A vulnerability was found in Tecno 4G Portable WiFi TR118 TR118-M30E-RR-D-EnFrArSwHaPo-OP-V008-20220830. It has been declared as critical. This vulnerability affects unknown code of the file /goform/goform_get_cmd_process of the component Ping Tool. The manipulation of the argument url leads to os command injection.	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability was named CVE-2023-6304. The attack can be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2023-3368	Chamilo LMS up to 1.11.20 additional_webservices.php os command injection	A vulnerability which was classified as critical was found in Chamilo LMS up to 1.11.20. Affected is an unknown function of the file /main/webservices/additional_webservices.php. The manipulation leads to os command injection. This vulnerability is traded as CVE-2023-3368. 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 command injection attack.
CVE-2023-4221	Chamilo LMS up to 1.11.24 openoffice_presentation.class.php os command injection	A vulnerability classified as critical was found in Chamilo LMS up to 1.11.24. This vulnerability affects unknown code of the file main/lp/openoffice_presentation.class.php. The manipulation leads to os command injection. This vulnerability was named CVE-2023-4221. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-4222	Chamilo LMS up to 1.11.24 openoffice_text_document.class.php os command injection	A vulnerability which was classified as critical has been found in Chamilo LMS up to 1.11.24. This issue affects some unknown processing of the file main/lp/openoffice_text_document.class.php. The manipulation leads to os command injection. The identification of this vulnerability is CVE-2023-4222. The attack may be initiated	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. There is no exploit available.		
CVE-2023-48842	D-Link Go-RT-AC750 revA_v101b03 hedwig.cgi service command injection	A vulnerability was found in D-Link Go-RT-AC750 revA_v101b03. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file hedwig.cgi. The manipulation of the argument service leads to command injection. This vulnerability is known as CVE-2023-48842. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-48849	Ruijie EG up to EG_3.0(1)B11P216 Filter Remote Code Execution	A vulnerability which was classified as critical was found in Ruijie EG up to EG_3.0B11P216. This affects an unknown part of the component Filter. The manipulation leads to Remote Code Execution. This vulnerability is uniquely identified as CVE-2023-48849. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-49435	Tenda AX9 22.03.01.46 command injection	A vulnerability was found in Tenda AX9 22.03.01.46 and classified as critical. This issue affects some unknown processing. The manipulation leads to command injection. The identification of this vulnerability is CVE-2023-49435. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-49999	Tenda W30E 16.01.0.12(4843) setUmountUSBPartition command injection	A vulnerability has been found in Tenda W30E 16.01.0.12 and classified as critical. Affected by this vulnerability is the function setUmountUSBPartition. The manipulation leads to command injection. This vulnerability is known as CVE-2023-49999. Access to the	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		local network is required for this attack. There is no exploit available.		
CVE-2023-49436	Tenda AX9 22.03.01.46 SetNetControlList list command injection	A vulnerability was found in Tenda AX9 22.03.01.46. It has been declared as critical. This vulnerability affects unknown code of the file /goform/SetNetControlList. The manipulation of the argument list leads to command injection. This vulnerability was named CVE-2023-49436. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-49431	Tenda AX9 22.03.01.46 /goform/SetOnlineDevName mac command injection	A vulnerability which was classified as critical has been found in Tenda AX9 22.03.01.46. Affected by this issue is some unknown functionality of the file /goform/SetOnlineDevName. The manipulation of the argument mac leads to command injection. This vulnerability is handled as CVE-2023-49431. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-49403	Tenda W30E 16.01.0.12(4843) setFixTools command injection	A vulnerability was found in Tenda W30E 16.01.0.12. It has been declared as critical. This vulnerability affects the function setFixTools. The manipulation leads to command injection. This vulnerability was named CVE-2023-49403. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-49437	Tenda AX12 22.03.01.46 SetNetControlList list command injection	A vulnerability classified as critical was found in Tenda AX12 22.03.01.46. This vulnerability affects unknown code of the file /goform/SetNetControlList. The manipulation of the argument list leads to command	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		injection. This vulnerability was named CVE-2023-49437. Access to the local network is required for this attack. There is no exploit available.		
CVE-2023-49428	Tenda AX12 22.03.01.46 /goform/SetOnlineDevName mac command injection	A vulnerability has been found in Tenda AX12 22.03.01.46 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /goform/SetOnlineDevName. The manipulation of the argument mac leads to command injection. This vulnerability is known as CVE-2023-49428. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-49429	Tenda AX9 22.03.01.46 /goform/setModules setDeviceInfo mac command injection	A vulnerability was found in Tenda AX9 22.03.01.46 and classified as critical. Affected by this issue is the function setDeviceInfo of the file /goform/setModules. The manipulation of the argument mac leads to command injection. This vulnerability is handled as CVE-2023-49429. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-6612	Totolink X5000R 9.1.0cu.2300_B20230112 /cgi-bin/cstecgi.cgi os command injection	A vulnerability was found in Totolink X5000R 9.1.0cu.2300_B20230112. It has been rated as critical. This issue affects the function setDdnsCfg/setDynamicRoute/setFirewallType/setIPSecCfg/setIpPortFilterRules/setLancfg/setLoginPasswordCfg/setMacFilterRules/setMtknatCfg/setNetworkConfig/setPortForwardRules/setRemoteCfg/setSSServer/setScheduleCfg/setSmartQosCfg/setStaticDhcpRules/setStaticRoute/setVpnAccountCfg/setVpnPassCfg/setVpn	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		User/setWiFiAclAddConfig/setWiFiEasyGuestCfg/setWiFiGuestCfg/setWiFiRepeaterConfig/setWiFiScheduleCfg/setWizardCfg of the file /cgi-bin/cstecgi.cgi. The manipulation leads to os command injection. The identification of this vulnerability is CVE-2023-6612. The attack needs to be approached within the local network. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2023-47254	DrayTek Vigor167 5.2.2 CLI os command injection (SYSS-2023-023)	A vulnerability classified as critical was found in DrayTek Vigor167 5.2.2. Affected by this vulnerability is an unknown functionality of the component CLI. The manipulation leads to os command injection. This vulnerability is known as CVE-2023-47254. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2022-48616	Huawei AR6000 os command injection	A vulnerability classified as critical has been found in Huawei AR6000 V300R019C10SPC300/V300R019C13SPC200/V300R021C00SPC200/V300R021C10SPC100. This affects an unknown part. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2022-48616. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-50710	honojs hono up to 3.11.6 path code injection	A vulnerability which was classified as critical was found in honojs hono up to 3.11.6. Affected is an unknown function. The manipulation of the argument path leads to	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		code injection. This vulnerability is traded as CVE-2023-50710. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-48702	Jellyfin up to 10.8.12 Path ProcessStartInfo command injection (GHSA-rr9h-w522-cvmr)	A vulnerability was found in Jellyfin up to 10.8.12 and classified as critical. Affected by this issue is the function ProcessStartInfo of the file /System/MediaEncoder/Path. The manipulation leads to command injection. This vulnerability is handled as CVE-2023-48702. 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 command injection attack.
CVE-2023-50089	Netgear WNR2000v4 1.0.0.70 HTTP for SOAP Authentication command injection	A vulnerability has been found in Netgear WNR2000v4 1.0.0.70 and classified as critical. This vulnerability affects unknown code of the component HTTP for SOAP Authentication. The manipulation leads to command injection. This vulnerability was named CVE-2023-50089. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-50917	MajorDoMo thumb.php os command injection	A vulnerability which was classified as critical has been found in MajorDoMo. Affected by this issue is some unknown functionality of the file thumb.php. The manipulation leads to os command injection. This vulnerability is handled as CVE-2023-50917. The attack can only be initiated within the local network.	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		There is no exploit available. It is recommended to apply a patch to fix this issue.		
CVE-2023-6901	codelyfe Stupid Simple CMS up to 1.2.3 HTTP POST Request handle-command.php command os command injection	A vulnerability which was classified as critical was found in codelyfe Stupid Simple CMS up to 1.2.3. This affects an unknown part of the file /terminal/handle-command.php of the component HTTP POST Request Handler. The manipulation of the argument command with the input whoami leads to os command injection. This vulnerability is uniquely identified as CVE-2023-6901. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-50989	Tenda i29 1.0.0.5 pingSet command injection	A vulnerability was found in Tenda i29 1.0.0.5. It has been classified as critical. Affected is the function pingSet. The manipulation leads to command injection. This vulnerability is traded as CVE-2023-50989. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-50983	Tenda i29 1.0.0.5 sysScheduleRebootSet command injection	A vulnerability has been found in Tenda i29 1.0.0.5 and classified as critical. This vulnerability affects the function sysScheduleRebootSet. The manipulation leads to command injection. This vulnerability was named CVE-2023-50983. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-5611	Seraphinite Accelerator Plugin up to 2.20.31 on WordPress Setting cross-site request forgery	A vulnerability classified as problematic was found in Seraphinite Accelerator Plugin up to 2.20.31 on WordPress. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-5611. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-5882	WP ALL Export Pro Plugin on WordPress cross-site request forgery	A vulnerability was found in WP ALL Export Pro Plugin on WordPress. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-5882. 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-2023-5886	Export Any Data to XML Plugin on WordPress Phar Deserialization cross-site request forgery	A vulnerability was found in Export Any Data to XML Plugin on WordPress. It has been declared as problematic. This vulnerability affects unknown code of the component Phar Deserialization. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-5886. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-48912	Dreamer CMS 4.1.3 /admin/archives/edit cross-site request forgery	A vulnerability which was classified as problematic was found in Dreamer CMS 4.1.3. Affected is an unknown function of the file /admin/archives/edit. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-48912. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-48913	Dreamer CMS 4.1.3 /admin/archives/delete cross-site request forgery	A vulnerability has been found in Dreamer CMS 4.1.3 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/archives/delete. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-48913. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-48914	Dreamer CMS 4.1.3 /admin/archives/add cross-site request forgery	A vulnerability was found in Dreamer CMS 4.1.3 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/archives/add. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-48914. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-49076	Pimcore customer-data-framework up to 4.0.4 cross-site request forgery	A vulnerability classified as problematic was found in Pimcore customer-data-framework up to 4.0.4. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-49076. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		It is recommended to upgrade the affected component.		
CVE-2023-6474	PHPGurukul Nipah Virus Testing Management System 1.0 manage-phlebotomist.php pid cross-site request forgery	A vulnerability has been found in PHPGurukul Nipah Virus Testing Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file manage-phlebotomist.php. The manipulation of the argument pid leads to cross-site request forgery. This vulnerability was named CVE-2023-6474. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-49382	JFinalCMS 5.0.0 /admin/div/delete cross-site request forgery	A vulnerability which was classified as problematic was found in JFinalCMS 5.0.0. This affects an unknown part of the file /admin/div/delete. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-49382. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-49375	JFinalCMS 5.0.0 update cross-site request forgery	A vulnerability which was classified as problematic has been found in JFinalCMS 5.0.0. Affected by this issue is some unknown functionality of the file /admin/friend_link/update. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-49375. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-49397	JFinalCMS 5.0.0 updateStatus cross-site request forgery	A vulnerability which was classified as problematic has been found in JFinalCMS 5.0.0. This issue affects some unknown processing of the file /admin/category/updateStatus. The manipulation leads to cross-site	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		request forgery. The identification of this vulnerability is CVE-2023-49397. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2023-49446	JFinalCMS 5.0.0 /admin/nav/save cross-site request forgery	A vulnerability classified as problematic has been found in JFinalCMS 5.0.0. This affects an unknown part of the file /admin/nav/save. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-49446. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-49447	JFinalCMS 5.0.0 /admin/nav/update cross-site request forgery	A vulnerability was found in JFinalCMS 5.0.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/nav/update. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-49447. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-49373	JFinalCMS 5.0.0 /admin/slide/delete cross-site request forgery	A vulnerability was found in JFinalCMS 5.0.0. It has been classified as problematic. Affected is an unknown function of the file /admin/slide/delete. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-49373. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-49381	JFinalCMS 5.0.0 /admin/div/update cross-site request forgery	A vulnerability has been found in JFinalCMS 5.0.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/div/update. The	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-49381. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2023-49448	JFinalCMS 5.0.0 admin/nav/delete cross-site request forgery	A vulnerability was found in JFinalCMS 5.0.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file admin/nav/delete. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-49448. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-49395	JFinalCMS 5.0.0 /admin/category/update cross-site request forgery	A vulnerability has been found in JFinalCMS 5.0.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/category/update. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-49395. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-49374	JFinalCMS 5.0.0 /admin/slide/update cross-site request forgery	A vulnerability was found in JFinalCMS 5.0.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/slide/update. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-49374. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-49372	JFinalCMS 5.0.0 /admin/slide/save cross-site request forgery	A vulnerability was found in JFinalCMS 5.0.0 and classified as problematic. This issue affects some unknown	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		processing of the file /admin/slide/save. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-49372. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2023-49396	JFinalCMS 5.0.0 /admin/category/save cross-site request forgery	A vulnerability classified as problematic was found in JFinalCMS 5.0.0. This vulnerability affects unknown code of the file /admin/category/save. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-49396. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-49376	JFinalCMS 5.0.0 /admin/tag/delete cross-site request forgery	A vulnerability was found in JFinalCMS 5.0.0. It has been classified as problematic. This affects an unknown part of the file /admin/tag/delete. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-49376. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-49398	JFinalCMS 5.0.0 /admin/category/delete cross-site request forgery	A vulnerability which was classified as problematic was found in JFinalCMS 5.0.0. Affected is an unknown function of the file /admin/category/delete. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-49398. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-49379	JFinalCMS 5.0.0 /admin/friend_link/save cross-site request forgery	A vulnerability was found in JFinalCMS 5.0.0. It has been rated as problematic. This	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		issue affects some unknown processing of the file /admin/friend_link/save. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-49379. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2023-49377	JFinalCMS 5.0.0 /admin/tag/update cross-site request forgery	A vulnerability classified as problematic was found in JFinalCMS 5.0.0. Affected by this vulnerability is an unknown functionality of the file /admin/tag/update. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-49377. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-49380	JFinalCMS 5.0.0 delete cross-site request forgery	A vulnerability was found in JFinalCMS 5.0.0. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/friend_link/delete. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-49380. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-49383	JFinalCMS 5.0.0 /admin/tag/save cross-site request forgery	A vulnerability classified as problematic has been found in JFinalCMS 5.0.0. Affected is an unknown function of the file /admin/tag/save. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-49383. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-49378	JFinalCMS 5.0.0 /admin/form/save cross-site request	A vulnerability was found in JFinalCMS 5.0.0. It has been	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	forgery	classified as problematic. This affects an unknown part of the file /admin/form/save. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-49378. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2023-6653	PHPGurukul Teacher Subject Allocation Management System 1.0 Create a new Subject /admin/subject.php cid cross-site request forgery	A vulnerability was found in PHPGurukul Teacher Subject Allocation Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/subject.php of the component Create a new Subject. The manipulation of the argument cid leads to cross-site request forgery. This vulnerability is handled as CVE-2023-6653. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-6766	PHPGurukul Teacher Subject Allocation Management System 1.0 Delete Course /admin/course.php delid cross-site request forgery	A vulnerability classified as problematic has been found in PHPGurukul Teacher Subject Allocation Management System 1.0. Affected is an unknown function of the file /admin/course.php of the component Delete Course Handler. The manipulation of the argument delid leads to cross-site request forgery. This vulnerability is traded as CVE-2023-6766. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-47322	Silverpeas Core 6.3.1 userModify cross-site request forgery	A vulnerability which was classified as problematic has been found in Silverpeas Core 6.3.1. This issue affects some unknown processing of the component userModify Handler. The	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-47322. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-47326	Silverpeas Core 6.3.1 Domain SQL Create cross-site request forgery	A vulnerability has been found in Silverpeas Core 6.3.1 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Domain SQL Create Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-47326. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-50017	Dreamer CMS 4.1.3 /admin/database/backup cross-site request forgery	A vulnerability was found in Dreamer CMS 4.1.3. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/database/backup. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-50017. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-4922	wpb-show-core Plugin up to 2.2 on WordPress path path traversal	A vulnerability was found in wpb-show-core Plugin up to 2.2 on WordPress. It has been classified as critical. This affects an unknown part. The manipulation of the argument path leads to path traversal. This vulnerability is uniquely identified as CVE-2023-4922. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-42000	Arcserve UDP up to 9.1 path traversal	A vulnerability was found in Arcserve UDP up to 9.1. It has been declared as critical. This vulnerability affects unknown code of the component com.ca.arcflash.ui.server.servlet.FileHandlingServlet.doUpload. The manipulation leads to path traversal. This vulnerability was named CVE-2023-42000. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-3533	Chamilo LMS up to 1.11.20 File Upload additional_webservices.php path traversal	A vulnerability was found in Chamilo LMS up to 1.11.20 and classified as critical. Affected by this issue is some unknown functionality of the file /main/webservices/additional_webservices.php of the component File Upload. The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-3533. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		It is recommended to apply a patch to fix this issue.		
CVE-2023-6295	SiteOrigin Widgets Bundle Plugin up to 1.50.x on WordPress file inclusion	A vulnerability classified as problematic was found in SiteOrigin Widgets Bundle Plugin up to 1.50.x on WordPress. This vulnerability affects unknown code. The manipulation leads to file inclusion. This vulnerability was named CVE-2023-6295. Access to the local network is required for this attack to succeed. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-46886	Dreamer CMS up to 4.0.0 Background Template Management path traversal	A vulnerability classified as critical was found in Dreamer CMS up to 4.0.0. Affected by this vulnerability is an unknown functionality of the component Background Template Management. The manipulation leads to path traversal. This vulnerability is known as CVE-2023-46886. 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-2021-35975	Systematica Radius up to 3.9.256.777 SMTP Adapter file absolute path traversal	A vulnerability classified as critical was found in Systematica Radius up to 3.9.256.777. This vulnerability affects unknown code of the component SMTP Adapter. The manipulation of the argument file leads to absolute path traversal. This vulnerability was named CVE-2021-35975. The attack can be initiated	Protected by core rules	Detected by scanner as local file inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. There is no exploit available.		
CVE-2023-6352	Aquaforest TIFF Server up to 4.2.210913 path traversal	A vulnerability was found in Aquaforest TIFF Server up to 4.2.210913. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to path traversal. This vulnerability was named CVE-2023-6352. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-6577	Beijing Baichuo PatrolFlow 2530Pro up to 20231126 /log/mailsendview.php file path traversal	A vulnerability was found in Beijing Baichuo PatrolFlow 2530Pro up to 20231126. It has been rated as problematic. This issue affects some unknown processing of the file /log/mailsendview.php. The manipulation of the argument file with the input /boot/phpConfig/tb_admin.txt leads to path traversal. The identification of this vulnerability is CVE-2023-6577. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-5907	File Manager Plugin up to 6.2 on WordPress path traversal	A vulnerability was found in File Manager Plugin up to 6.2 on WordPress. It has been classified as critical. Affected is an unknown function. The manipulation leads to path traversal. This vulnerability is traded as CVE-2023-5907. It is possible to launch the attack remotely. There is no exploit available. It is recommended to	Protected by core rules	Detected by scanner as local file inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		upgrade the affected component.		
CVE-2023-50449	JFinalCMS 5.0.0 /common/down/file fileKey path traversal	A vulnerability which was classified as critical has been found in JFinalCMS 5.0.0. Affected by this issue is some unknown functionality of the file /common/down/file. The manipulation of the argument fileKey leads to path traversal: &039;../filedir&039;. This vulnerability is handled as CVE-2023-50449. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-47624	advplyr audiobookshelf up to 2.4.3 /hls path traversal (GHSL-2023-203)	A vulnerability classified as critical was found in advplyr audiobookshelf up to 2.4.3. Affected by this vulnerability is an unknown functionality of the file /hls. The manipulation leads to path traversal. This vulnerability is known as CVE-2023-47624. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-6569	h2oai h2o-3 up to latest file inclusion	A vulnerability was found in h2oai h2o-3 up to latest. It has been classified as critical. This affects an unknown part. The manipulation leads to file inclusion. This vulnerability is uniquely identified as CVE-2023-6569. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-6831	mlflow up to 2.9.1 path traversal	A vulnerability was found in mlflow up to 2.9.1. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to path traversal: &039;\..\filename&039;. This vulnerability is known	Protected by core rules	Detected by scanner as local file inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		as CVE-2023-6831. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-50264	morpheus65535 bazarr up to 1.3.0 /system/backup/download/ send_file filename path traversal (GHSL-2023-192)	A vulnerability classified as critical was found in morpheus65535 bazarr up to 1.3.0. This vulnerability affects the function send_file of the file /system/backup/download/. The manipulation of the argument filename leads to path traversal. This vulnerability was named CVE-2023-50264. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-50265	morpheus65535 bazarr up to 1.3.0 /api/swaggerui/static send_file filename path traversal (GHSL-2023-192)	A vulnerability which was classified as critical has been found in morpheus65535 bazarr up to 1.3.0. This issue affects the function send_file of the file /api/swaggerui/static. The manipulation of the argument filename leads to path traversal. The identification of this vulnerability is CVE-2023-50265. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-6900	rmountjoy92 DashMachine 0.5-4 /settings/delete_file path traversal	A vulnerability which was classified as critical has been found in rmountjoy92 DashMachine 0.5-4. Affected by this issue is some unknown functionality of the file /settings/delete_file. The manipulation of the	Protected by core rules	Detected by scanner as local file inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument file leads to path traversal: &039;../filedir&039;. This vulnerability is handled as CVE-2023-6900. The attack needs to be done within the local network. Furthermore there is an exploit available.		
CVE-2023-6893	Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) /php/exportrecord.php downname path traversal	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. This vulnerability is handled as CVE-2023-6893. The attack needs to be initiated within the local network. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-6909	mlflow up to 2.9.1 path traversal	A vulnerability which was classified as critical has been found in mlflow up to 2.9.1. This issue affects some unknown processing. The manipulation leads to path traversal: &039;\..\filename&039;. The identification of this vulnerability is CVE-2023-6909. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-48930	Xinhu Xinhuoa 2.2.1 File Upload unrestricted upload	A vulnerability which was classified as problematic was found in Xinhu Xinhuoa 2.2.1. Affected is an unknown function of the component File Upload Handler. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2023-48930. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	NA
CVE-2023-6574	Beijing Baichuo Smart S20 up to 20231120 HTTP POST Request /sysmanage/updateos.php 1_file_upload unrestricted upload	A vulnerability was found in Beijing Baichuo Smart S20 up to 20231120 and classified as critical. Affected by this issue is some unknown functionality of the file /sysmanage/updateos.php of the component HTTP POST Request Handler. The manipulation of the argument 1_file_upload leads to unrestricted upload. This vulnerability is handled as CVE-2023-6574. The attack may be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	NA
CVE-2023-49444	DoraCMS 2.1.8 User Avatar unrestricted upload	A vulnerability was found in DoraCMS 2.1.8. It has been declared as problematic. Affected	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		by this vulnerability is an unknown functionality of the component User Avatar Handler. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2023-49444. The attack can only be initiated within the local network. There is no exploit available.		
CVE-2023-4122	Kashipara Student Information System 1.0 my-profile Page photo unrestricted upload	A vulnerability classified as critical has been found in Kashipara Student Information System 1.0. Affected is an unknown function of the component my-profile Page. The manipulation of the argument photo leads to unrestricted upload. This vulnerability is traded as CVE-2023-4122. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-6902	codelyfe Stupid Simple CMS up to 1.2.4 /file-manager/upload.php file unrestricted upload	A vulnerability has been found in codelyfe Stupid Simple CMS up to 1.2.4 and classified as critical. This vulnerability affects unknown code of the file /file-manager/upload.php. The manipulation of the argument file leads to unrestricted upload. This vulnerability was named CVE-2023-6902. Access to the local network is required for this attack. Furthermore there is an exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-6887	saysky ForestBlog up to 20220630 Image Upload /admin/upload/img filename unrestricted upload	A vulnerability classified as critical has been found in saysky ForestBlog up to 20220630. This affects an unknown part of the file /admin/upload/img of the component Image Upload Handler. The manipulation of the argument filename leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-6887. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-4311	Vrm 360 3D Model Viewer Plugin up to 1.2.1 on WordPress Shortcode unrestricted upload	A vulnerability was found in Vrm 360 3D Model Viewer Plugin up to 1.2.1 on WordPress. It has been classified as critical. This affects an unknown part of the component Shortcode Handler. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-4311. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-6305	SourceCodester Free and Open Source Inventory Management System 1.0 suppliar_data.php columns sql injection	A vulnerability was found in SourceCodester Free and Open Source Inventory Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file ample/app/ajax/suppliar_data.php. The manipulation of the argument columns leads to sql injection. The identification of this vulnerability is CVE-2023-6305. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-6306	SourceCodester Free and Open Source Inventory Management System 1.0 member_data.php columns sql injection	A vulnerability classified as critical has been found in SourceCodester Free and Open Source Inventory Management System 1.0. Affected is an unknown function of the file /ample/app/ajax/member_data.php. The manipulation of the argument columns leads to sql injection. This vulnerability is traded as CVE-2023-6306. 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-2023-6310	SourceCodester Loan Management System 1.0 deleteBorrower.php delete_borrower borrower_id sql injection	A vulnerability has been found in SourceCodester Loan Management System 1.0 and classified as critical. This vulnerability affects the function delete_borrower of the file	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		deleteBorrower.php. The manipulation of the argument borrower_id leads to sql injection. This vulnerability was named CVE-2023-6310. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2023-6312	SourceCodester Loan Management System 1.0 Users Page deleteUser.php delete_user user_id sql injection	A vulnerability was found in SourceCodester Loan Management System 1.0. It has been classified as critical. Affected is the function delete_user of the file deleteUser.php of the component Users Page. The manipulation of the argument user_id leads to sql injection. This vulnerability is traded as CVE-2023-6312. 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-2023-6311	SourceCodester Loan Management System 1.0 Loan Type Page delete_ltype.php delete_ltype ltype_id sql injection	A vulnerability was found in SourceCodester Loan Management System 1.0 and classified as critical. This issue affects the function delete_ltype of the file delete_ltype.php of the component Loan Type Page. The manipulation of the argument ltype_id leads to sql injection. The identification of this vulnerability is CVE-2023-6311. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-48188	opartdevis Module up to 4.5.18/4.6.12	A vulnerability was found in opartdevis	Protected by core rules	Detected by scanner as SQL

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	on PrestaShop getModuleTranslation sql injection	Module up to 4.5.18/4.6.12 on PrestaShop. It has been rated as critical. This issue affects the function getModuleTranslation. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-48188. The attack may be initiated remotely. There is no exploit available.		injection attack.
CVE-2023-49030	in32ns KLive up to 2019-1-19 web/user.php sql injection	A vulnerability was found in in32ns KLive up to 2019-1-19. It has been rated as critical. Affected by this issue is some unknown functionality of the file web/user.php. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-49030. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-6360	My Calendar Plugin up to 3.4.21 on WordPress /my-calendar/v1/events sql injection	A vulnerability classified as critical has been found in My Calendar Plugin up to 3.4.21 on WordPress. Affected is an unknown function of the file /my-calendar/v1/events. The manipulation of the argument to leads to sql injection. This vulnerability is traded as CVE-2023-6360. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-6402	PHPGurukul Nipah	A vulnerability which	Protected by	Detected by

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Virus Testing Management System 1.0 add-phlebotomist.php empid sql injection	was classified as critical was found in PHPGurukul Nipah Virus Testing Management System 1.0. This affects an unknown part of the file add-phlebotomist.php. The manipulation of the argument empid leads to sql injection. This vulnerability is uniquely identified as CVE-2023-6402. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	core rules	scanner as SQL injection attack.
CVE-2023-48016	Restaurant Table Booking System 1.0 rtbs/admin/index.php username sql injection	A vulnerability which was classified as critical has been found in Restaurant Table Booking System 1.0. Affected by this issue is some unknown functionality of the file rtbs/admin/index.php. The manipulation of the argument username leads to sql injection. This vulnerability is handled as CVE-2023-48016. 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-2023-6464	SourceCodester User Registration and Login System 1.0 /endpoint/add-user.php user sql injection	A vulnerability was found in SourceCodester User Registration and Login System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /endpoint/add-user.php. The manipulation of the argument user leads to sql injection. This vulnerability is handled as CVE-2023-6464. The attack may	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		be launched remotely. Furthermore there is an exploit available.		
CVE-2023-48813	Senayan SLiMS 9.6.1 fines_report.php sql injection	A vulnerability has been found in Senayan SLiMS 9.6.1 and classified as critical. This vulnerability affects unknown code of the file admin/modules/reporting/customs/fines_report.php. The manipulation leads to sql injection. This vulnerability was named CVE-2023-48813. 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-2023-48893	Senayan SLiMS 9.6.1 staff_act.php sql injection	A vulnerability was found in Senayan SLiMS 9.6.1 and classified as critical. This issue affects some unknown processing of the file admin/modules/reporting/customs/staff_act.php. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-48893. 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-2023-49371	RuoYi up to 4.6 /system/dept/edit sql injection	A vulnerability was found in RuoYi up to 4.6. It has been classified as critical. Affected is an unknown function of the file /system/dept/edit. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-49371. The attack needs to be done within the local network. There is no	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit available.		
CVE-2023-46956	Packers and Movers Management System 1.0 sql injection	A vulnerability classified as critical has been found in Packers and Movers Management System 1.0. This affects an unknown part of the file /mpms/admin/pageuser/manage_user&id. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-46956. 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-2023-48863	SEMCMS 3.9 sql injection	A vulnerability classified as critical has been found in SEMCMS 3.9. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-48863. 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-2023-6575	Beijing Baichuo S210 up to 20231121 HTTP POST Request /Tool/repair.php txt sql injection	A vulnerability was found in Beijing Baichuo S210 up to 20231121. It has been classified as critical. This affects an unknown part of the file /Tool/repair.php of the component HTTP POST Request Handler. The manipulation of the argument txt leads to sql injection. This vulnerability is uniquely identified as CVE-2023-6575. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2023-6579	osCommerce 4 POST Parameter shopping-cart estimate[country_id] sql injection	A vulnerability which was classified as critical has been found in osCommerce 4. Affected by this issue is some unknown functionality of the file /b2b-supermarket/shopping-cart of the component POST Parameter Handler. The manipulation of the argument estimate[country_id] leads to sql injection. This vulnerability is handled as CVE-2023-6579. The attack may be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-6581	D-Link DAR-7000 up to 20231126 /user/inc/workidajax .php id sql injection	A vulnerability has been found in D-Link DAR-7000 up to 20231126 and classified as critical. This vulnerability affects unknown code of the file /user/inc/workidajax.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-6581. Access to the local network is required for this attack to succeed. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		not respond in any way.		
CVE-2023-48823	GaatiTrack Courier Management System 1.0 Login ajax.php email sql injection (ID 176030)	A vulnerability has been found in GaatiTrack Courier Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file ajax.php of the component Login. The manipulation of the argument email leads to sql injection. This vulnerability was named CVE-2023-48823. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5008	Kashipara Student Information System 1.0 index.php regno sql injection	A vulnerability was found in Kashipara Student Information System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file index.php. The manipulation of the argument regno leads to sql injection. This vulnerability was named CVE-2023-5008. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-6619	SourceCodester Simple Student Attendance System 1.0 /modals/class_form.php id sql injection	A vulnerability was found in SourceCodester Simple Student Attendance System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /modals/class_form.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-6619. The attack can	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		only be initiated within the local network. Furthermore there is an exploit available.		
CVE-2023-6608	Tongda OA 2017 up to 11.9 delete.php DELETE_STR sql injection	A vulnerability was found in Tongda OA 2017 up to 11.9 and classified as critical. Affected by this issue is some unknown functionality of the file general/notify/manage/delete.php. The manipulation of the argument DELETE_STR leads to sql injection. This vulnerability is handled as CVE-2023-6608. The attack needs to be initiated within the local network. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-6607	Tongda OA 2017 up to 11.10 delete.php TERM_ID_STR sql injection	A vulnerability has been found in Tongda OA 2017 up to 11.10 and classified as critical. Affected by this vulnerability is an unknown functionality of the file general/wiki/cp/manage/delete.php. The manipulation of the argument TERM_ID_STR leads to sql injection. This vulnerability is known as CVE-2023-6607. The attack needs to be done within the local network. Furthermore there is an exploit available. The vendor was	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		contacted early about this disclosure but did not respond in any way.		
CVE-2023-6611	Tongda OA 2017 up to 11.9 pda/pad/email/delete.php EMAIL_ID sql injection	A vulnerability was found in Tongda OA 2017 up to 11.9. It has been declared as critical. This vulnerability affects unknown code of the file pda/pad/email/delete.php. The manipulation of the argument EMAIL_ID leads to sql injection. This vulnerability was named CVE-2023-6611. Access to the local network is required for this attack to succeed. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-6373	ArtPlacer Widget Plugin up to 2.20.6 on WordPress sql injection	A vulnerability was found in ArtPlacer Widget Plugin up to 2.20.6 on WordPress. It has been classified as critical. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-6373. 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-2023-6617	SourceCodester Simple Student Attendance System 1.0 attendance.php class_id sql injection	A vulnerability was found in SourceCodester Simple Student Attendance System 1.0. It has been	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		classified as critical. Affected is an unknown function of the file attendance.php. The manipulation of the argument class_id leads to sql injection. This vulnerability is traded as CVE-2023-6617. The attack needs to be approached within the local network. Furthermore there is an exploit available.		
CVE-2023-50429	IzyBat Orange Casiers prior 20230803_1 getEnsemble.php sql injection (GHSA-mc3w-rv8p-f9xf)	A vulnerability has been found in IzyBat Orange Casiers and classified as critical. This vulnerability affects unknown code of the file getEnsemble.php. The manipulation leads to sql injection. This vulnerability was named CVE-2023-50429. The attack can only be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-6652	code-projects Matrimonial Site 1.0 /register.php register sql injection	A vulnerability was found in code-projects Matrimonial Site 1.0. It has been declared as critical. Affected by this vulnerability is the function register of the file /register.php. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-6652. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-6648	PHPGurukul Nipah Virus Testing Management	A vulnerability which was classified as critical was found in	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System 1.0 password-recovery.php username sql injection	PHPGurukul Nipah Virus Testing Management System 1.0. This affects an unknown part of the file password-recovery.php. The manipulation of the argument username leads to sql injection. This vulnerability is uniquely identified as CVE-2023-6648. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2023-6651	code-projects Matrimonial Site 1.0 /auth/auth.php username sql injection	A vulnerability was found in code-projects Matrimonial Site 1.0. It has been classified as critical. Affected is an unknown function of the file /auth/auth.phpuser1. The manipulation of the argument username leads to sql injection. This vulnerability is traded as CVE-2023-6651. 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-2023-6647	AMTT HiBOS 1.0 Type sql injection	A vulnerability which was classified as critical has been found in AMTT HiBOS 1.0. Affected by this issue is some unknown functionality. The manipulation of the argument Type leads to sql injection. This vulnerability is handled as CVE-2023-6647. The attack may be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		this disclosure but did not respond in any way.		
CVE-2023-6655	Hongjing e-HR 2020 Login Interface loadhistroyorgtree parentid sql injection	A vulnerability which was classified as critical has been found in Hongjing e-HR 2020. Affected by this issue is some unknown functionality of the file /w_selfservice/oauthservlet/%2e./.%2e/general/inform/org/loadhistroyorgtree of the component Login Interface. The manipulation of the argument parentid leads to sql injection. This vulnerability is handled as CVE-2023-6655. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-6657	SourceCodester Simple Student Attendance System 1.0 /modals/student_form.php id sql injection	A vulnerability classified as critical has been found in SourceCodester Simple Student Attendance System 1.0. This affects an unknown part of the file /modals/student_form.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-6657. Access to the local network is required for this attack to succeed. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-6659	Campcodes Web-Based Student Clearance System 1.0 /libsystem/login.php student sql injection	A vulnerability which was classified as critical has been found in Campcodes Web-Based Student Clearance System 1.0. This issue affects some unknown processing of the file /libsystem/login.php. The manipulation of	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the argument student leads to sql injection. The identification of this vulnerability is CVE-2023-6659. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2023-6035	EazyDocs Plugin up to 2.3.3 on WordPress data sql injection	A vulnerability was found in EazyDocs Plugin up to 2.3.3 on WordPress. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation of the argument data leads to sql injection. This vulnerability is handled as CVE-2023-6035. 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-2023-41623	Emlog 2.1.14 /admin/media.php uid sql injection	A vulnerability was found in Emlog 2.1.14. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/media.php. The manipulation of the argument uid leads to sql injection. This vulnerability is known as CVE-2023-41623. 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-2023-6755	DedeBIZ 6.2 content_batchup_action.php endid sql injection	A vulnerability was found in DedeBIZ 6.2 and classified as critical. This issue affects some unknown processing of the file	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/src/admin/content_batchup_action.php. The manipulation of the argument endid leads to sql injection. The identification of this vulnerability is CVE-2023-6755. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2023-6771	SourceCodester Simple Student Attendance System 1.0 actions.class.php save_attendance sid sql injection	A vulnerability which was classified as critical has been found in SourceCodester Simple Student Attendance System 1.0. This issue affects the function save_attendance of the file actions.class.php. The manipulation of the argument sid leads to sql injection. The identification of this vulnerability is CVE-2023-6771. The attack can only be initiated within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-6772	OTCMS 7.01 /admin/ind_backstage.php sqlContent sql injection	A vulnerability which was classified as critical was found in OTCMS 7.01. Affected is an unknown function of the file /admin/ind_backstage.php. The manipulation of the argument sqlContent leads to sql injection. This vulnerability is traded as CVE-2023-6772. It is possible to launch the attack remotely. Furthermore there is an exploit	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		available.		
CVE-2023-6765	SourceCodester Online Tours & Travels Management System 1.0 email_setup.php prepare name sql injection	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0. It has been rated as critical. This issue affects the function prepare of the file email_setup.php. The manipulation of the argument name leads to sql injection. The identification of this vulnerability is CVE-2023-6765. The attack needs to be initiated within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-49363	RockOA up to 2.3.2 reimpAction.php indexAction sql injection	A vulnerability was found in RockOA up to 2.3.2. It has been rated as critical. Affected by this issue is the function indexAction of the file reimpAction.php. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-49363. The attack needs to be approached within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-48050	ZKTeco Cams Biometrics Integration Module with HR Attendance controllers.py sql injection	A vulnerability was found in ZKTeco Cams Biometrics Integration Module with HR Attendance up to 16.0.1 and classified as critical. Affected by this issue is some unknown functionality of the file controllers/controllers.py. The manipulation of the argument db leads	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to sql injection. This vulnerability is handled as CVE-2023-48050. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2023-40954	Grzegorz Marczynski Dynamic Progress Bar models/web_progress.py recency sql injection	A vulnerability has been found in Grzegorz Marczynski Dynamic Progress Bar and classified as critical. Affected by this vulnerability is an unknown functionality of the file models/web_progress.py. The manipulation of the argument recency leads to sql injection. This vulnerability is known as CVE-2023-40954. 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 SQL injection attack.
CVE-2023-48049	Cybrosys Website Blog Search up to 13.0.1.0.1 controllers/main.py name sql injection	A vulnerability was found in Cybrosys Website Blog Search up to 13.0.1.0.1. It has been classified as critical. This affects an unknown part of the file controllers/main.py. The manipulation of the argument name leads to sql injection. This vulnerability is uniquely identified as CVE-2023-48049. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-6898	SourceCodester Best Courier Management System 1.0 manage_user.php id	A vulnerability classified as critical has been found in SourceCodester Best Courier Management	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	sql injection	System 1.0. Affected is an unknown function of the file manage_user.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-6898. The attack can only be done within the local network. Furthermore there is an exploit available.		
CVE-2023-6885	Tongda OA 2017 up to 11.10 delete.php DELETE_STR sql injection	A vulnerability was found in Tongda OA 2017 up to 11.10. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file general/vote/manage/delete.php. The manipulation of the argument DELETE_STR leads to sql injection. This vulnerability is known as CVE-2023-6885. The attack needs to be initiated within the local network. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-6899	rmountjoy92 DashMachine 0.5-4 Config /settings/save_config value_template code injection	A vulnerability classified as problematic was found in rmountjoy92 DashMachine 0.5-4. Affected by this vulnerability is an unknown functionality of the file /settings/save_config of the component Config Handler. The manipulation of the argument value_template leads to code injection.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is known as CVE-2023-6899. The attack can only be initiated within the local network. Furthermore there is an exploit available.		
CVE-2023-6903	Netentsec NS-ASG Application Security Gateway 6.3.1 singlelogin.php loginId sql injection	A vulnerability classified as critical has been found in Netentsec NS-ASG Application Security Gateway 6.3.1. This affects an unknown part of the file /admin/singlelogin.php submit1. The manipulation of the argument loginId leads to sql injection. This vulnerability is uniquely identified as CVE-2023-6903. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-6301	SourceCodester Best Courier Management System 1.0 GET Parameter parcel_list.php id cross site scripting	A vulnerability has been found in SourceCodester Best Courier Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file parcel_list.php of the component GET Parameter Handler. The manipulation of the argument id with the input </TiTlE><ScRiPt >alert</ScRiPt&gt ; leads to cross site scripting. This vulnerability is known as CVE-2023-6301. 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-2023-6300	SourceCodester Best Courier Management System 1.0 page cross site scripting	A vulnerability which was classified as problematic was found in SourceCodester Best Courier Management System 1.0. Affected is an unknown function. The manipulation of the argument page with the input </TiTlE><ScRiPt >alert</ScRiPt&gt ; leads to cross site scripting. This vulnerability is traded as CVE-2023-6300. 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-2023-6303	CSZCMS 1.3.0 Site Settings Page /admin/settings/ Additional Meta Tag cross site scripting	A vulnerability was found in CSZCMS 1.3.0. It has been classified as problematic. This affects an unknown part of the file	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/admin/settings/ of the component Site Settings Page. The manipulation of the argument Additional Meta Tag with the input <svg><animate onbeginalert attributeNamex dur1s> leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-6303. It is possible to initiate the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2023-6313	SourceCodester URL Shortener 1.0 Long URL cross site scripting	A vulnerability was found in SourceCodester URL Shortener 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Long URL Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-6313. 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-2023-6297	PHPGurukul Nipah Virus Testing Management System 1.0 Search Report Page patient-search-report.php Search By Patient Name cross site scripting	A vulnerability classified as problematic has been found in PHPGurukul Nipah Virus Testing Management System 1.0. This affects an unknown part of the file patient-search-report.php of the component Search Report Page. The	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument Search By Patient Name with the input <script>alert</script> leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-6297. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2023-49029	smpn1smg absis up to 2017-10-19 lock/lock.php nama cross site scripting	A vulnerability was found in smpn1smg absis up to 2017-10-19. It has been classified as problematic. Affected is an unknown function of the file lock/lock.php. The manipulation of the argument nama leads to cross site scripting. This vulnerability is traded as CVE-2023-49029. 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-2023-5738	Backup & Migration Plugin up to 1.4.3 on WordPress cross site scripting	A vulnerability which was classified as problematic was found in Backup & Migration Plugin up to 1.4.3 on WordPress. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-5738. 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-2023-5560	WP-UserOnline Plugin up to 2.88.2 on WordPress Header X-	A vulnerability classified as problematic has been found in WP-	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Forwarded-For cross site scripting	UserOnline Plugin up to 2.88.2 on WordPress. Affected is an unknown function of the component Header Handler. The manipulation of the argument X-Forwarded-For leads to cross site scripting. This vulnerability is traded as CVE-2023-5560. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-5325	Woocommerce Vietnam Checkout Plugin up to 2.0.5 on WordPress custom shipping phone cross site scripting	A vulnerability was found in Woocommerce Vietnam Checkout Plugin up to 2.0.5 on WordPress and classified as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument custom shipping phone leads to cross site scripting. This vulnerability is handled as CVE-2023-5325. 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-2023-5942	D. Relton Medialist Plugin up to 1.4.0 on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in D. Relton Medialist Plugin up to 1.4.0 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross site scripting. This vulnerability is handled as CVE-2023-5942. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-5209	Online Booking and Scheduling Plugin up to 22.4 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic has been found in Online Booking and Scheduling Plugin up to 22.4 on WordPress. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-5209. 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-2023-49028	smpn1smg absis up to 2017-10-19 lock/lock.php user cross site scripting	A vulnerability was found in smpn1smg absis up to 2017-10-19. It has been classified as problematic. Affected is an unknown function of the file lock/lock.php. The manipulation of the argument user leads to cross site scripting. This vulnerability is traded as CVE-2023-49028. 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-2023-6225	WP Shortcodes Plugin up to 5.13.3 on WordPress cross	A vulnerability classified as problematic was found	Protected by core rules	Detected by scanner as cross-site

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	site scripting	in WP Shortcodes Plugin up to 5.13.3 on WordPress. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-6225. The attack can be initiated remotely. There is no exploit available.		scripting attack.
CVE-2023-5653	WassUp Real Time Analytics Plugin up to 1.9.4.5 on WordPress IP Address cross site scripting	A vulnerability which was classified as problematic has been found in WassUp Real Time Analytics Plugin up to 1.9.4.5 on WordPress. Affected by this issue is some unknown functionality of the component IP Address Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-5653. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-5958	POST SMTP Mailer Plugin up to 2.7.0 on WordPress Email Message Content cross site scripting	A vulnerability was found in POST SMTP Mailer Plugin up to 2.7.0 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Email Message Content Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-5958. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component.		
CVE-2023-49078	zediious raptor-web 0.4.4 Link cross site scripting (GHSA-8r6g-fhh4-xhmq)	A vulnerability was found in zediious raptor-web 0.4.4. It has been classified as problematic. Affected is an unknown function of the component Link Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-49078. 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-2023-48880	EyouCMS 1.6.4-UTF8-SP1 login.php Menu Name cross site scripting (Issue 52)	A vulnerability has been found in EyouCMS 1.6.4-UTF8-SP1 and classified as problematic. This vulnerability affects unknown code of the file /login.phpmadmin&cIndex&achangeTableVal&_ajax1&langcn. The manipulation of the argument Menu Name leads to cross site scripting. This vulnerability was named CVE-2023-48880. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-48881	EyouCMS 1.6.4-UTF8-SP1 login.php Field Title cross site scripting (Issue 53)	A vulnerability was found in EyouCMS 1.6.4-UTF8-SP1 and classified as problematic. This issue affects some unknown processing of the file /login.phpmadmin&cField&aarctype_add&_ajax1&langcn. The manipulation of the	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument Field Title leads to cross site scripting. The identification of this vulnerability is CVE-2023-48881. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-48882	EyouCMS 1.6.4-UTF8 /login.php Document Properties cross site scripting (Issue 54)	A vulnerability was found in EyouCMS 1.6.4-UTF8. It has been classified as problematic. Affected is an unknown function of the file /login.php. The manipulation of the argument Document Properties leads to cross site scripting. This vulnerability is traded as CVE-2023-48882. 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-2023-6440	SourceCodester Book Borrower System 1.0 endpoint/add-book.php Book Title/Book Author cross site scripting	A vulnerability was found in SourceCodester Book Borrower System 1.0 and classified as problematic. This issue affects some unknown processing of the file endpoint/add-book.php. The manipulation of the argument Book Title/Book Author leads to cross site scripting. The identification of this vulnerability is CVE-2023-6440. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-6442	PHPGurukul Nipah Virus Testing Management System 1.0 add-phlebotomist.php empid/fullname	A vulnerability was found in PHPGurukul Nipah Virus Testing Management System 1.0. It has been declared as	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	cross site scripting	problematic. Affected by this vulnerability is an unknown functionality of the file add-phlebotomist.php. The manipulation of the argument empid/fullname leads to cross site scripting. This vulnerability is known as CVE-2023-6442. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2023-47844	Lim Kai Yang Grab & Save Plugin up to 1.0.4 on WordPress cross site scripting	A vulnerability which was classified as problematic was found in Lim Kai Yang Grab & Save Plugin up to 1.0.4 on WordPress. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-47844. 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-2023-47418	o2oa up to 8.1.2 Service Management cross site scripting	A vulnerability was found in o2oa up to 8.1.2. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Service Management. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-47418. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-49052	Microweber 2.0.4 Created Forms cross site scripting	A vulnerability was found in Microweber 2.0.4. It has been classified as problematic. This affects an unknown	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		part of the component Created Forms. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-49052. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2023-47777	Automattic WooCommerce Plugin/WooCommerce Blocks Plugin on WordPress cross site scripting	A vulnerability was found in Automattic WooCommerce Plugin and WooCommerce Blocks Plugin on WordPress. 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-2023-47777. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-47505	Elementor Elementor Plugin up to 3.16.4 on WordPress Elementor.Com cross site scripting	A vulnerability was found in Elementor Elementor Plugin up to 3.16.4 on WordPress. It has been declared as problematic. This vulnerability affects unknown code of the file Elementor.Com. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-47505. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-6439	ZenTao PMS 18.8 cross site scripting	A vulnerability classified as problematic was found in ZenTao PMS 18.8. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is known as CVE-2023-6439. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2023-6461	viliusle minipaint up to 4.13.x cross site scripting	A vulnerability classified as problematic has been found in viliusle minipaint up to 4.13.x. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-6461. 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-2023-6465	PHPGurukul Nipah Virus Testing Management System 1.0 registered-user-testing.php regmobilenumber cross site scripting	A vulnerability was found in PHPGurukul Nipah Virus Testing Management System 1.0. It has been classified as problematic. This affects an unknown part of the file registered-user-testing.php. The manipulation of the argument regmobilenumber leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-6465. 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-2023-6463	SourceCodester User Registration and Login System 1.0 /endpoint/add-user.php first_name cross site scripting	A vulnerability has been found in SourceCodester User Registration and Login System 1.0 and classified as	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		problematic. Affected by this vulnerability is an unknown functionality of the file /endpoint/add-user.php. The manipulation of the argument first_name leads to cross site scripting. This vulnerability is known as CVE-2023-6463. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2023-6466	Thecosy IceCMS 2.0.1 User Comment /planet cross site scripting	A vulnerability was found in Thecosy IceCMS 2.0.1. It has been declared as problematic. This vulnerability affects unknown code of the file /planet of the component User Comment Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-6466. 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-2023-6462	SourceCodester User Registration and Login System 1.0 delete-user.php user cross site scripting	A vulnerability which was classified as problematic was found in SourceCodester User Registration and Login System 1.0. Affected is an unknown function of the file /endpoint/delete-user.php. The manipulation of the argument user leads to cross site scripting. This vulnerability is traded as CVE-2023-6462. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-49276	louislam uptime-kuma up to 1.23.6 cross site scripting (GHSA-v4v2-8h88-65qj)	A vulnerability was found in louislam uptime-kuma up to 1.23.6. 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-2023-49276. 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-2023-6473	SourceCodester Online Quiz System 1.0 take-quiz.php quiz_taker/year_section cross site scripting	A vulnerability which was classified as problematic was found in SourceCodester Online Quiz System 1.0. This affects an unknown part of the file take-quiz.php. The manipulation of the argument quiz_taker/year_section leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-6473. 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-2023-6472	PHPEMS 7.0 Content Section api.cls.php cross site scripting	A vulnerability which was classified as problematic has been found in PHPEMS 7.0. This issue affects some unknown processing of the file app\content\cls\api.cls.php of the component Content Section Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2023-6472. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2023-28875	Afian Filerun 20220202 Share Link cross site scripting	A vulnerability has been found in Afian Filerun 20220202 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Share Link Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-28875. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-48208	Availability Booking Calendar 5.0 index.php cross site scripting (ID 175805)	A vulnerability which was classified as problematic was found in Availability Booking Calendar 5.0. This affects an unknown part of the file index.php. The manipulation of the argument name/plugin_sms_api_key/plugin_sms_country_code/uuid/title/country name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-48208. 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-2023-46857	Squidex up to 7.8.x SVG Document cross site scripting	A vulnerability was found in Squidex up to 7.8.x. It has been declared as problematic. An unknown functionality of the SVG Document Handler is affected by this vulnerability. The manipulation leads to cross-site scripting.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is known as CVE-2023-46857. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-48839	Appointment Scheduler 3.0 cross site scripting (ID 176055)	A vulnerability has been found in Appointment Scheduler 3.0 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument name/plugin_sms_api_key/plugin_sms_country_code/calendar_id/title/country name/customer_name leads to cross site scripting. This vulnerability was named CVE-2023-48839. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-46974	Best Courier Management System 1.000 URL page cross site scripting	A vulnerability classified as problematic has been found in Best Courier Management System 1.000. This affects an unknown part of the component URL Handler. The manipulation of the argument page leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-46974. 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-2023-49493	DedeCMS 5.7.111 selectimages.php v cross site scripting	A vulnerability was found in DedeCMS 5.7.111. It has been rated as problematic.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This issue affects some unknown processing of the file selectimages.php. The manipulation of the argument v leads to cross site scripting. The identification of this vulnerability is CVE-2023-49493. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-48838	Appointment Scheduler 3.0 MS API Key/Default Country Code cross site scripting (ID 176054)	A vulnerability which was classified as problematic was found in Appointment Scheduler 3.0. This affects an unknown part. The manipulation of the argument MS API Key/Default Country Code leads to basic cross site scripting. This vulnerability is uniquely identified as CVE-2023-48838. 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-2023-48836	PHP Jabbers Car Rental Script 3.0 cross site scripting	A vulnerability which was classified as problematic was found in PHP Jabbers Car Rental Script 3.0. Affected is an unknown function. The manipulation of the argument name/plugin_sms_api_key/plugin_sms_country_code/calendar_id/title/country name/customer_name leads to cross site scripting. This vulnerability is traded as CVE-2023-48836. 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-2023-6568	mlflow up to 2.8.x	A vulnerability has	Protected by	Detected by

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	cross site scripting	been found in mlflow up to 2.8.x 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-2023-6568. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	core rules	scanner as cross-site scripting attack.
CVE-2023-48824	BoidCMS 2.0.1 title/subtitle/footer/keywords cross site scripting (ID 176031)	A vulnerability was found in BoidCMS 2.0.1 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument title/subtitle/footer/keywords leads to cross site scripting. This vulnerability is handled as CVE-2023-48824. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-48825	Availability Booking Calendar 5.0 SMS API Key/Default Country Code cross site scripting (ID 176033)	A vulnerability classified as problematic was found in Availability Booking Calendar 5.0. This vulnerability affects unknown code. The manipulation of the argument SMS API Key/Default Country Code leads to basic cross site scripting. This vulnerability was named CVE-2023-48825. 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-2023-48828	PHP Jabbers Time Slots Booking Calendar 4.0 cross site scripting	A vulnerability which was classified as problematic has been found in PHP Jabbers Time Slots Booking Calendar 4.0. This issue affects some unknown processing. The manipulation of the argument name/plugin_sms_api_key/plugin_sms_country_code/calendar_id/title/country name/customer_name leads to cross site scripting. The identification of this vulnerability is CVE-2023-48828. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-48837	PHP Jabbers Car Rental Script 3.0 SMS API Key/Default Country Code cross site scripting	A vulnerability was found in PHP Jabbers Car Rental Script 3.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument SMS API Key/Default Country Code leads to basic cross site scripting. This vulnerability is known as CVE-2023-48837. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-48827	PHP Jabbers Time Slots Booking Calendar 4.0 cross site scripting	A vulnerability classified as problematic was found in PHP Jabbers Time Slots Booking Calendar 4.0. This vulnerability affects unknown code. The manipulation of the argument name/plugin_sms_api_key/plugin_sms_country_code/calendar_id/title/country	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		name/customer_name leads to basic cross site scripting. This vulnerability was named CVE-2023-48827. The attack can be initiated remotely. There is no exploit available.		
CVE-2023-48206	GaatiTrack Courier Management System 1.0 login.php page cross site scripting (ID 175803)	A vulnerability was found in GaatiTrack Courier Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file login.php. The manipulation of the argument page leads to cross site scripting. This vulnerability is handled as CVE-2023-48206. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-49492	DedeCMS 5.7.111 selectimages.php imgstick cross site scripting	A vulnerability classified as problematic has been found in DedeCMS 5.7.111. Affected is an unknown function of the file selectimages.php. The manipulation of the argument imgstick leads to cross site scripting. This vulnerability is traded as CVE-2023-49492. 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-2023-48172	Shuttle Booking Software 2.0 index.php name/description/title/address cross site scripting (ID 175800)	A vulnerability classified as problematic has been found in Shuttle Booking Software 2.0. Affected is an unknown function of the file index.php. The manipulation of the	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument name/description/title/ address leads to cross site scripting. This vulnerability is traded as CVE-2023-48172. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2023-49485	JFinalCMS 5.0.0 Column Management Department cross site scripting	A vulnerability which was classified as problematic has been found in JFinalCMS 5.0.0. This issue affects some unknown processing of the component Column Management Department. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-49485. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-49484	Dreamer CMS 4.1.3 Article Management Department cross site scripting	A vulnerability classified as problematic was found in Dreamer CMS 4.1.3. This vulnerability affects unknown code of the component Article Management Department. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-49484. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-49487	JFinalCMS 5.0.0 Navigation Management Department cross site scripting	A vulnerability classified as problematic has been found in JFinalCMS 5.0.0. This affects an unknown part of the component Navigation Management Department. The	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-49487. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2023-6616	SourceCodester Simple Student Attendance System 1.0 index.php page cross site scripting	A vulnerability was found in SourceCodester Simple Student Attendance System 1.0 and classified as problematic. This issue affects some unknown processing of the file index.php. The manipulation of the argument page leads to cross site scripting. The identification of this vulnerability is CVE-2023-6616. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-49486	JFinalCMS 5.0.0 Model Management Department cross site scripting	A vulnerability was found in JFinalCMS 5.0.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Model Management Department. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-49486. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-6613	Typecho 1.2.1 Logo /admin/options-theme.php cross site scripting	A vulnerability classified as problematic has been found in Typecho 1.2.1. Affected is an unknown function of the file /admin/options-theme.php of the	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component Logo Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-6613. It is possible to launch the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2023-6646	linkding 1.23.0 q cross site scripting	A vulnerability classified as problematic has been found in linkding 1.23.0. Affected is an unknown function. The manipulation of the argument q leads to cross site scripting. This vulnerability is traded as CVE-2023-6646. It is possible to launch the attack remotely. Furthermore there is an exploit available. The vendor was contacted early responded in a very professional manner and immediately released a fixed version of the affected product. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-6650	SourceCodester Simple Invoice Generator System 1.0 login.php cashier cross site scripting	A vulnerability was found in SourceCodester Simple Invoice Generator System 1.0 and classified as problematic. This issue affects some unknown processing of the file login.php. The	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument cashier leads to cross site scripting. The identification of this vulnerability is CVE-2023-6650. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2023-28873	Seafile 9.0.6 Wiki/Discussion Page cross site scripting (usd-2022-0032)	A vulnerability was found in Seafile 9.0.6. It has been declared as problematic. This vulnerability affects unknown code of the component Wiki/Discussion Page. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-28873. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-6649	PHPGurukul Teacher Subject Allocation Management System 1.0 index.php searchdata cross site scripting	A vulnerability has been found in PHPGurukul Teacher Subject Allocation Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file index.php. The manipulation of the argument searchdata with the input <script>alert</script> leads to cross site scripting. This vulnerability was named CVE-2023-6649. 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-2023-5749	EmbedPress Plugin up to 3.9.1 on WordPress cross site scripting (daac-3899-4169)	A vulnerability classified as problematic has been found in EmbedPress Plugin up to 3.9.1 on WordPress. This affects	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-5749. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-5955	Contact Form Email Plugin up to 1.3.43 on WordPress Setting cross site scripting	A vulnerability was found in Contact Form Email Plugin up to 1.3.43 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-5955. 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-2023-50465	Monica 4.0.0 SVG Document cross site scripting	A vulnerability was found in Monica 4.0.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component SVG Document Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-50465. The attack can be launched remotely. There is no exploit available. It is recommended to	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		upgrade the affected component.		
CVE-2023-5750	EmbedPress Plugin up to 3.9.1 on WordPress cross site scripting	A vulnerability classified as problematic was found in EmbedPress Plugin up to 3.9.1 on WordPress. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-5750. 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-2023-5757	WP Crowdfunding Plugin up to 2.1.7 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic has been found in WP Crowdfunding Plugin up to 2.1.7 on WordPress. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-5757. 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-2023-49490	XunRuiCMS 4.5.5 /admin.php cross site scripting	A vulnerability which was classified as problematic was found in XunRuiCMS 4.5.5. This affects an unknown part of the file /admin.php. The manipulation leads to cross site scripting.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is uniquely identified as CVE-2023-49490. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2023-49488	Openfiler ESA 2.99.1 nic cross site scripting	A vulnerability was found in Openfiler ESA 2.99.1. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument nic leads to cross site scripting. This vulnerability is handled as CVE-2023-49488. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-49494	DedeCMS 5.7.111 select_media_post_wangEditor.php cross site scripting	A vulnerability was found in DedeCMS 5.7.111. It has been declared as problematic. This vulnerability affects unknown code of the file select_media_post_wangEditor.php. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-49494. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-49563	Voltronic Power SNMP Web Pro 1.1 cross site scripting	A vulnerability was found in Voltronic Power SNMP Web Pro 1.1 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-49563. The attack may be initiated remotely. There is no	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit available.		
CVE-2023-6774	CodeAstro POS and Inventory Management System 1.0 register_account Username cross site scripting	A vulnerability was found in CodeAstro POS and Inventory Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /accounts_con/register_account. The manipulation of the argument Username with the input <script>alert</script> leads to cross site scripting. This vulnerability is handled as CVE-2023-6774. 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-2023-6775	CodeAstro POS and Inventory Management System 1.0 /item/item_con item_name cross site scripting	A vulnerability was found in CodeAstro POS and Inventory Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /item/item_con. The manipulation of the argument item_name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-6775. 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-2023-47324	Silverpeas Core 6.3.1 Notification cross site scripting	A vulnerability which was classified as problematic was found in Silverpeas Core 6.3.1. Affected is an unknown function of the component Notification Handler. The manipulation leads to cross site scripting.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is traded as CVE-2023-47324. It is possible to launch the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.		
CVE-2023-31546	DedeBIZ 6.0.3 Search Box keyword cross site scripting	A vulnerability was found in DedeBIZ 6.0.3 and classified as problematic. Affected by this issue is some unknown functionality of the component Search Box. The manipulation of the argument keyword leads to cross site scripting. This vulnerability is handled as CVE-2023-31546. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-50100	JFinalcms 5.0.0 Carousel Image Editing cross site scripting	A vulnerability was found in JFinalcms 5.0.0. It has been classified as problematic. Affected is an unknown function of the component Carousel Image Editing. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-50100. 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-2023-50101	JFinalcms 5.0.0 Label Management Editing cross site scripting	A vulnerability has been found in JFinalcms 5.0.0 and classified as problematic. This vulnerability affects unknown code of the component Label Management Editing. The manipulation leads	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to cross site scripting. This vulnerability was named CVE-2023-50101. The attack can be initiated remotely. There is no exploit available.		
CVE-2023-50137	JFinalcms 5.0.0 Site Management Office cross site scripting	A vulnerability was found in JFinalcms 5.0.0. It has been declared as problematic. This vulnerability affects unknown code of the component Site Management Office. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-50137. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-50102	JFinalcms 5.0.0 cross site scripting	A vulnerability was found in JFinalcms 5.0.0 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-50102. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-41621	Emlog Pro 2.1.14 /admin/store.php cross site scripting	A vulnerability was found in Emlog Pro 2.1.14. It has been classified as problematic. Affected is an unknown function of the file /admin/store.php. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-41621. It is possible to launch the attack remotely. There is no	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit available.		
CVE-2023-41618	Emlog Pro 2.1.14 article.php cross site scripting	A vulnerability was found in Emlog Pro 2.1.14 and classified as problematic. This issue affects some unknown processing of the file /admin/article.phpactive_savedraft. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-41618. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-47620	koush scrypted up to 0.55.0 plugin-http.ts owner/pkg cross site scripting (GHSL-2023-218)	A vulnerability classified as problematic was found in koush scrypted up to 0.55.0. Affected by this vulnerability is an unknown functionality of the file plugin-http.ts. The manipulation of the argument owner/pkg leads to cross site scripting. This vulnerability is known as CVE-2023-47620. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-47623	koush scrypted up to 0.55.0 javascript Scheme redirect_uri cross site scripting (GHSL-2023-218)	A vulnerability was found in koush scrypted up to 0.55.0. It has been classified as problematic. This affects an unknown part of the component javascript Scheme Handler. The manipulation of the argument redirect_uri leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-47623. It is possible to initiate the attack remotely. There	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		is no exploit available.		
CVE-2023-6889	thorsten phpmyfaq up to 3.1.16 cross site scripting	A vulnerability which was classified as problematic has been found in thorsten phpmyfaq up to 3.1.16. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-6889. 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-2023-6890	thorsten phpmyfaq up to 3.1.16 cross site scripting	A vulnerability which was classified as problematic was found in thorsten phpmyfaq up to 3.1.16. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-6890. 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-2023-6896	SourceCodester Simple Image Stack Website 1.0 search cross site scripting	A vulnerability was found in SourceCodester Simple Image Stack Website 1.0. It has been rated as problematic. This issue affects some unknown processing. The manipulation of the argument search with the input sy2ap%22%3e%3cscript%3ealert%3c%2fscript%3etkxh1 leads to cross site scripting.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The identification of this vulnerability is CVE-2023-6896. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2023-6778	allegroai clearml-server up to 1.12.x cross site scripting	A vulnerability was found in allegroai clearml-server up to 1.12.x. 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-2023-6778. 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-2023-5348	Product Catalog Mode for WooCommerce Plugin up to 5.0.2 on WordPress Setting cross site scripting	A vulnerability has been found in Product Catalog Mode for WooCommerce Plugin up to 5.0.2 on WordPress 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-2023-5348. 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.

Carriage Return Line Feed (CRLF) Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-49081	aio-libs aiohttp ClientSession crlf injection	A vulnerability was found in aio-libs aiohttp. It has been classified as problematic. This affects an unknown part of the component ClientSession. The manipulation leads to crlf injection. This vulnerability is uniquely identified as CVE-2023-49081. 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 CRLF Injection vulnerability
CVE-2023-49082	aio-libs aiohttp crlf injection	A vulnerability was found in aio-libs aiohttp. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to crlf injection. This vulnerability was named CVE-2023-49082. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner a CRLF Injection vulnerability

XML External Entity Vulnerability

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-6194	Eclipse Memory Analyzer up to 1.14.0 Report Definition xml external entity reference (Issue 15)	A vulnerability has been found in Eclipse Memory Analyzer up to 1.14.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Report Definition Handler. The manipulation leads to xml external entity reference. This vulnerability is known as CVE-2023-6194. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by the scanner as XML external entity attack.

Indusface is a leading application security SaaS company that secures critical Web, Mobile & API applications of 5000+ 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.

Indusface is the only cloud WAAP (WAF) vendor with 100% customer recommendation for 3 consecutive years

A Customers' Choice for 2022 and 2023 Gartner® Peer Insights™