INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

September 2023

The total zero-day vulnerabilities count for **September** month**: 222**

Command Injection	CSRF	Local File Inclusion	Malicious File Upload	SQL Injection	Cross-site Scripting	XML External Entity
10	10	17	8	74	102	1

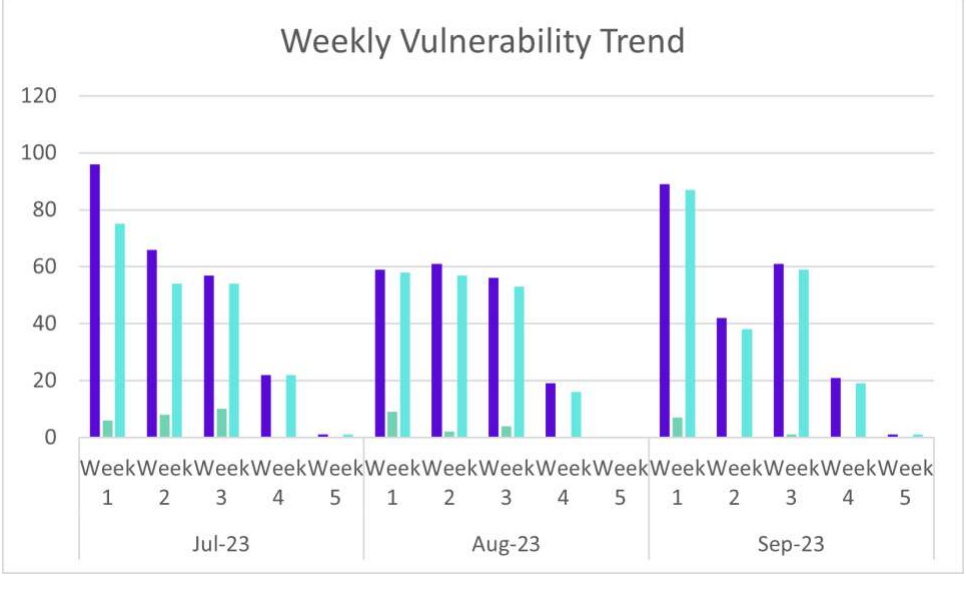
Zero-day vulnerabilities protected through **core rules**	**214**
Zero-day vulnerabilities protected through **custom rules**	**8**
Zero-day vulnerabilities for which protection cannot be done	0
Zero-day vulnerabilities **found by Indusface WAS**	**204**

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

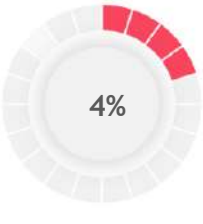
Vulnerability Trend:

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

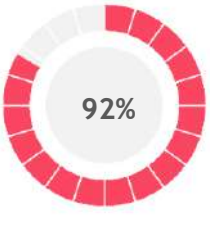
Weekly Vulnerability Trend



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

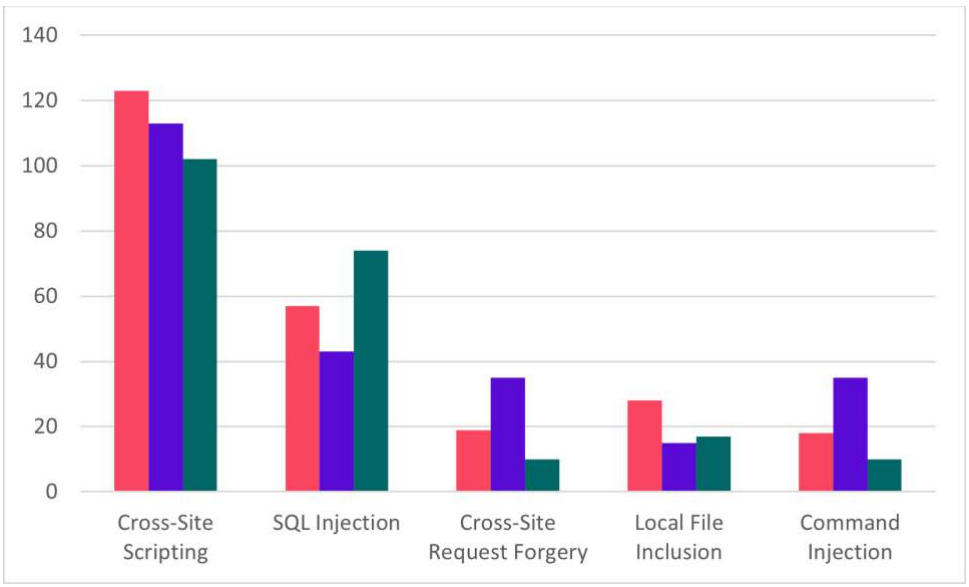


of the zero-day vulnerabilities were protected by the custom rules in the last month



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

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-40796	Phicomm k2 22.6.529.216 command injection	A vulnerability was found in Phicomm k2 22.6.529.216 and classified as critical. This issue affects some unknown processing. The manipulation leads to command injection. The identification of this vulnerability is CVE-2023-40796. 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-2019-13690	Google Chrome prior 75.0.3770.80 on ChromeOS File Remote Code Execution	A vulnerability has been found in Google Chrome on ChromeOS and classified as critical. Affected by this vulnerability is an unknown functionality of the component File Handler. The manipulation leads to Remote Code Execution. This vulnerability is known as CVE-2019-13690. 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 command injection attack.
CVE-2023-41109	SmartNode SN200 3.21.2-23021 os command injection (SYSS-2023-019)	A vulnerability classified as critical has been found in SmartNode SN200 3.21.2-23021. This affects an unknown part. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2023-41109. 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-2023-4711	D-Link DAR-8000-10 up to 20230819 /log/decodmail.php file os command injection	A vulnerability which was classified as critical has been found in D-Link DAR-8000-10 up to 20230819. Affected by	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		this issue is some unknown functionality of the file /log/decodmail.php. The manipulation of the argument file leads to os command injection. This vulnerability is handled as CVE-2023-4711. 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.		
CVE-2023-4873	Beijing Baichuo Smart S45F Multi-Service Secure Gateway Intelligent Management Platform /importexport.php os command injection	A vulnerability which was classified as critical was found in Beijing Baichuo Smart S45F Multi-Service Secure Gateway Intelligent Management Platform up to 20230906. Affected is an unknown function of the file /importexport.php. The manipulation of the argument sql leads to os command injection. This vulnerability is traded as CVE-2023-4873. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-41011	China Mobile Communications China Mobile Intelligent Home Gateway v.HG6543C4 shortcut_telnet.cg command injection	A vulnerability which was classified as critical has been found in China Mobile Communications China Mobile Intelligent Home Gateway v.HG6543C4. Affected by this issue is some unknown functionality of the file shortcut_telnet.cg. The manipulation leads to command injection. This vulnerability is handled as CVE-2023-41011. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-39638	D-Link DIR-859 A1 1.05/1.06B01 Beta01 /htdocs/cgibin lxmldbc_system command injection	A vulnerability was found in D-Link DIR-859 A1 1.05/1.06B01 Beta01. It has been classified as critical. Affected is the function lxmldbc_system of the file /htdocs/cgibin. The manipulation leads to command injection. This vulnerability is traded as CVE-2023-39638. 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-2023-43207	D-Link DWL-6610 4.3.0.8B003C config_upload_handler configRestore command injection	A vulnerability was found in D-Link DWL-6610 4.3.0.8B003C. It has been classified as critical. This affects the function config_upload_handler. The manipulation of the argument configRestore leads to command injection. This vulnerability is uniquely identified as CVE-2023-43207. 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-2023-43137	TP-Link TL-ER5120G 2.0.0	A vulnerability classified as	Protected by	Detected by

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Build 210817 Rel.80868n ACL Rule name command injection	critical was found in TP-Link TL-ER5120G 2.0.0 Build 210817 Rel.80868n. Affected by this vulnerability is an unknown functionality of the component ACL Rule Handler. The manipulation of the argument name leads to command injection. This vulnerability is known as CVE-2023-43137. The attack needs to be done within the local network. There is no exploit available.	core rules	scanner as command injection attack.
CVE-2023-43138	TP-Link TL-ER5120G 2.0.0 Build 210817 Rel.80868n NAPT Rule command injection	A vulnerability which was classified as critical has been found in TP-Link TL-ER5120G 2.0.0 Build 210817 Rel.80868n. Affected by this issue is some unknown functionality of the component NAPT Rule Handler. The manipulation leads to command injection. This vulnerability is handled as CVE-2023-43138. 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-2023-3356	Subscribers Text Counter Plugin up to 1.7.0 on WordPress cross-site request forgery	A vulnerability which was classified as problematic has been found in Subscribers Text Counter Plugin up to 1.7.0 on WordPress. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-3356. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-4013	GDPR Cookie Compliance Plugin up to 4.12.4 on WordPress cross-site request forgery	A vulnerability classified as problematic was found in GDPR Cookie Compliance Plugin up to 4.12.4 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-4013. 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-2023-4059	Profile Builder Plugin up to 3.9.7 on WordPress cross-site request forgery	A vulnerability has been found in Profile Builder Plugin up to 3.9.7 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-4059. 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-2023-4868	SourceCodester Contact Manager App 1.0 add.php cross-site request forgery	A vulnerability was found in SourceCodester Contact Manager App 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file add.php. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-4868. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-4869	SourceCodester Contact Manager App 1.0 update.php cross-site request forgery	A vulnerability was found in SourceCodester Contact Manager App 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file update.php. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-4869. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-4865	SourceCodester Take-Note App 1.0 cross-site request forgery	A vulnerability has been found in SourceCodester Take-Note App 1.0 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-4865. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-42270	Grocy up to 4.0.2 cross-site request forgery	A vulnerability has been found in Grocy up to 4.0.2 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-42270. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-40868	mooSocial cross-site request forgery	A vulnerability has been found in mooSocial and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-40868. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-5036	usememos up to 0.15.0 cross-site request forgery	A vulnerability was found in usememos memos up to 0.15.0 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-5036. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-2508	Papercut Mobility Print 1.0.3512 cross-site request forgery	A vulnerability which was classified as problematic has been found in Papercut Mobility Print 1.0.3512. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-2508. 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-2023-39810	busybox 1.30.1/1.33.2 CPIO Archive path traversal	A vulnerability classified as critical was found in busybox 1.30.1/1.33.2. This vulnerability affects unknown code of the component CPIO Archive Handler. The manipulation leads to path traversal. This vulnerability was named CVE-2023-39810. An attack has to be approached locally. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-41040	GitPython path traversal (GHSA-cwvm-v4w8-q58c)	A vulnerability which was classified as critical was found in GitPython. Affected is an unknown function. The manipulation leads to path traversal. This vulnerability is traded as CVE-2023-41040. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-39135	Zip 2.1.2 path traversal (Issue 245)	A vulnerability was found in Zip 2.1.2 and classified as critical. This issue affects some unknown processing of the component Zip Handler. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-39135. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-39138	ZIPFoundation 0.9.16 ZIP File path traversal (Issue 282)	A vulnerability was found in ZIPFoundation 0.9.16. It has been rated as critical. Affected by this issue is some unknown functionality of the component ZIP File Handler. The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-39138. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-39139	Archive 3.3.7 ZIP File path traversal (Issue 265)	A vulnerability classified as critical has been found in Archive 3.3.7. This affects an unknown part of the component ZIP File Handler. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-39139. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-39138	ZIPFoundation 0.9.16 ZIP File path traversal (Issue 282)	A vulnerability was found in ZIPFoundation 0.9.16. It has been rated as critical. Affected by this issue is some unknown functionality of the component ZIP File Handler. The	Protected by core rules	Detected by scanner as local file inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation leads to path traversal. This vulnerability is handled as CVE-2023-39138. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2023-41044	Graylog up to 5.1.2 Support Bundle data_dir path traversal (GHSA-2q4p-f6gf-mqr5)	A vulnerability which was classified as problematic has been found in Graylog up to 5.1.2. Affected by this issue is the function data_dir of the component Support Bundle. The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-41044. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-4749	SourceCodester Inventory Management System 1.0 index.php page file inclusion	A vulnerability which was classified as critical was found in SourceCodester Inventory Management System 1.0. Affected is an unknown function of the file index.php. The manipulation of the argument page leads to file inclusion. This vulnerability is traded as CVE-2023-4749. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-4748	Yongyou UFIDA-NC PrintTemplateFileServlet.java filePath path traversal	A vulnerability which was classified as critical has been found in Yongyou UFIDA-NC. This issue affects some unknown processing of the file PrintTemplateFileServlet.java. The manipulation of the argument filePath leads to path traversal. The identification of this vulnerability is CVE-2023-4748. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-41057	hyper-bump-it up to 0.5.0 path traversal (GHSA-xc27-f9q3-4448)	A vulnerability was found in hyper-bump-it up to 0.5.0. It has been classified as problematic. Affected is an unknown function. The manipulation leads to path traversal. This vulnerability is traded as CVE-2023-41057. An attack has to be approached locally. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-4634	Media Library Assistant Plugin up to 3.09 on WordPress file inclusion	A vulnerability was found in Media Library Assistant Plugin up to 3.09 on WordPress and classified as critical. This issue affects some unknown processing. The manipulation	Protected by core rules	Detected by scanner as local file inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		leads to file inclusion. The identification of this vulnerability is CVE-2023-4634. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-41578	jeecg-boot up to 3.5.3 /testConnection path traversal	A vulnerability which was classified as problematic has been found in jeecg-boot up to 3.5.3. Affected by this issue is some unknown functionality of the file /testConnection. The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-41578. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-40924	SolarView Compact up to 5.x path traversal	A vulnerability which was classified as critical has been found in SolarView Compact up to 5.x. This issue affects some unknown processing. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-40924. The attack needs to be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-41886	OpenRefine Database up to 3.7.4 Project Import path traversal	A vulnerability was found in OpenRefine Database up to 3.7.4. It has been classified as critical. This affects an unknown part of the component Project Import Handler. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-41886. 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 local file inclusion attack.
CVE-2023-4914	cecilapp cecil up to 7.47.0 path traversal	A vulnerability was found in cecilapp cecil up to 7.47.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to relative path traversal. This vulnerability is known as CVE-2023-4914. 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-2023-37739	i-doit pro 25 path traversal	A vulnerability which was classified as critical has been found in i-doit pro 25. Affected by this issue is some unknown	Protected by core rules	Detected by scanner as local file inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		functionality. The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-37739. Access to the local network is required for this attack. There is no exploit available.		
CVE-2023-40930	Skyworth 3.0 path traversal	A vulnerability was found in Skyworth 3.0. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-40930. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-4596	Forminator Plugin up to 1.24.6 on WordPress unrestricted upload	A vulnerability was found in Forminator Plugin up to 1.24.6 on WordPress. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-4596. The attack can be initiated remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2023-4238	Prevent Files Access Plugin up to 2.5.1 on WordPress mo_media_restrict_page unrestricted upload	A vulnerability was found in Prevent Files Access Plugin up to 2.5.1 on WordPress and classified as problematic. This issue affects the function mo_media_restrict_page. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2023-4238. The attack needs to be initiated within the local network. There is no exploit available.	Protected by custom rules	NA
CVE-2023-41717	Zscaler Proxy up to 3.6.1.25 File unrestricted upload	A vulnerability which was classified as problematic was found in Zscaler Proxy up to 3.6.1.25. This affects an unknown part of the component File Handler. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-41717. The attack needs to be approached locally. There is no exploit available.	Protected by custom rules	NA
CVE-2023-41638	GruppoSCAI RealGimm 1.1.37p38 Documentale Module unrestricted upload	A vulnerability has been found in GruppoSCAI RealGimm 1.1.37p38 and classified as problematic. This vulnerability affects unknown code of the component Documentale Module. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-41638. The attack needs to be done within the local network. There is no exploit available.	Protected by custom rules	NA
CVE-2023-41637	GruppoSCAI RealGimm 1.1.37p38 Carica Immagine unrestricted upload	A vulnerability was found in GruppoSCAI RealGimm 1.1.37p38. It has been declared as problematic. This vulnerability affects unknown code of the component Carica	Protected by custom rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Immagine Handler. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-41637. The attack needs to be initiated within the local network. There is no exploit available.		
CVE-2023-40980	wkeyuan DWSurvey up to 3.2.0 action/UploadAction.java saveimage/saveFile unrestricted upload (Issue 107)	A vulnerability classified as critical was found in wkeyuan DWSurvey up to 3.2.0. Affected by this vulnerability is the function saveimage/saveFile of the file action/UploadAction.java. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2023-40980. The attack can be launched remotely. There is no exploit available.	Protected by custom rules	NA
CVE-2023-4739	Beijing Baichuo Smart S85F Management Platform up to 20230820 on Smart /sysmanage/updateos.php 1_file_upload unrestricted upload	A vulnerability which was classified as critical has been found in Beijing Baichuo Smart S85F Management Platform up to 20230820 on Smart. Affected by this issue is some unknown functionality of the file /sysmanage/updateos.php. The manipulation of the argument 1_file_upload leads to unrestricted upload. This vulnerability is handled as CVE-2023-4739. 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 custom rules	NA
CVE-2023-42180	lenosp 1.0-1.2.0 JPG File /user/upload unrestricted upload	A vulnerability was found in lenosp 1.0-1.2.0. It has been classified as critical. This affects an unknown part of the file /user/upload of the component JPG File Handler. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-42180. The attack needs to be done within the local network. There is no exploit available.	Protected by custom rules	NA
CVE-2023-4596	Forminator Plugin up to 1.24.6 on WordPress unrestricted upload	A vulnerability was found in Forminator Plugin up to 1.24.6 on WordPress. It has been declared as	Protected by custom rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		critical. This vulnerability affects unknown code. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-4596. The attack can be initiated remotely. There is no exploit available.		

XML External Entity Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-41635	GruppoSCAI RealGimm 1.1.37p38 XML File VerifichePeriodiche.aspx xml external entity reference	A vulnerability classified as problematic was found in GruppoSCAI RealGimm 1.1.37p38. This vulnerability affects unknown code of the file VerifichePeriodiche.aspx of the component XML File Handler. The manipulation leads to xml external entity reference. This vulnerability was named CVE-2023-41635. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as XML external entity attack.

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-4556	SourceCodester Online Graduate Tracer System 1.0 sexit.php mysqli_query id sql injection	A vulnerability was found in SourceCodester Online Graduate Tracer System 1.0 and classified as critical. Affected by this issue is the function mysqli_query of the file sexit.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-4556. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-4557	SourceCodester Inventory Management System 1.0 search_purchase_paymen_report.php customer sql injection	A vulnerability classified as critical has been found in SourceCodester Inventory Management System 1.0. Affected is an unknown function of the file app/ajax/search_purchase_paymen_report.php. The manipulation of the argument customer leads to sql injection. This vulnerability is traded as CVE-2023-4557. 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-2023-4558	SourceCodester Inventory Management System 1.0 staff_data.php columns[0][data] sql injection	A vulnerability classified as critical was found in SourceCodester Inventory Management System 1.0. Affected by this vulnerability is an unknown functionality of the file staff_data.php. The manipulation of the argument columns[0][data] leads to sql injection. This vulnerability is known as CVE-2023-4558. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-40749	PHP Jabbers Food Delivery Script 3.0 index.php column sql injection	A vulnerability was found in PHP Jabbers Food Delivery Script 3.0 and classified as critical. This issue affects some unknown processing of the file index.php. The manipulation of the argument column leads to sql injection. The identification of this vulnerability is CVE-2023-40749. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-40748	PHP Jabbers Food Delivery Script 3.0 index.php q sql injection	A vulnerability classified as critical was found in PHP Jabbers Food Delivery Script 3.0. This vulnerability affects unknown code of the file index.php. The manipulation of the argument q leads to sql injection. This vulnerability was named CVE-2023-40748. 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-2023-39650	Theme Volty CMS Blog up to 4.0.1 /tvcmsblog/single id sql injection	A vulnerability was found in Theme Volty CMS Blog up to 4.0.1. It has been declared as critical. This vulnerability affects unknown code of the file /tvcmsblog/single. The	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-39650. The attack can only be done within the local network. There is no exploit available.		
CVE-2023-39560	ECTouch 2 insert.php arr['id'] sql injection	A vulnerability which was classified as critical was found in ECTouch 2. This affects an unknown part of the file \default\helpers\insert.php. The manipulation of the argument arr[&039;id&039;] leads to sql injection. This vulnerability is uniquely identified as CVE-2023-39560. 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-2023-41539	PHP Jabbers Business Directory Script 3.2 column sql injection	A vulnerability has been found in PHP Jabbers Business Directory Script 3.2 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation of the argument column leads to sql injection. This vulnerability is known as CVE-2023-41539. 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-2021-3262	TripSpark VEO Transportation POST Body sql injection	A vulnerability classified as critical was found in TripSpark VEO Transportation 2.2.x-XP_BB-20201123-184084 NovusEDU-2.2.x-XP_BB-20201123-184084. This vulnerability affects unknown code of the component POST Body Handler. The manipulation leads to sql injection. This vulnerability was named CVE-2021-3262. 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-2023-31714	Chitor-CMS up to 1.1.1 sql injection (EDB-51383)	A vulnerability classified as critical was found in Chitor-CMS up to 1.1.1. This vulnerability affects unknown code. The manipulation leads to sql injection. This vulnerability was named CVE-2023-31714. The attack needs to be approached within the local network. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-31714	Chitor-CMS up to 1.1.1 sql injection (EDB-51383)	A vulnerability classified as critical was found in Chitor-CMS up to 1.1.1. This vulnerability affects unknown code. The manipulation leads to sql injection. This vulnerability was named CVE-2023-31714. The attack needs to be approached within the local network.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Furthermore there is an exploit available. It is recommended to upgrade the affected component.		
CVE-2023-41640	GruppoSCAI RealGimm 1.1.37p38 ErroreNonGestito.aspx sql injection	A vulnerability was found in GruppoSCAI RealGimm 1.1.37p38 and classified as critical. This issue affects some unknown processing of the file ErroreNonGestito.aspx. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-41640. 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-2023-41636	GruppoSCAI RealGimm 1.1.37p38 dal sql injection	A vulnerability has been found in GruppoSCAI RealGimm 1.1.37p38 and classified as critical. This vulnerability affects unknown code. The manipulation of the argument dal leads to sql injection. This vulnerability was named CVE-2023-41636. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-41364	tine up to 2023.01.14.325 /index.php sort sql injection	A vulnerability which was classified as critical was found in tine up to 2023.01.14.325. Affected is an unknown function of the file /index.php. The manipulation of the argument sort leads to sql injection. This vulnerability is traded as CVE-2023-41364. 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-2023-4712	Xintian Smart Table Integrated Management System 5.6.9 AddUpdateRole.aspx txtRoleName sql injection	A vulnerability which was classified as critical was found in Xintian Smart Table Integrated Management System 5.6.9. This affects an unknown part of the file /SysManage/AddUpdateRole.aspx. The manipulation of the argument txtRoleName leads to sql injection. This vulnerability is uniquely identified as CVE-2023-4712. The attack can only be done 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-2023-4713	IBOS OA 4.5.5 addcomment addComment touid sql injection	A vulnerability has been found in IBOS OA 4.5.5 and classified as critical. This vulnerability affects the function addComment of the file rweibo/comment/addcomment. The manipulation of the argument touid leads to sql injection. This vulnerability was named CVE-2023-4713. The attack can only be initiated within	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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-2023-40970	Senayan Library Management Systems 9.6.1 loan_rules.php sql injection (Issue 205)	A vulnerability was found in Senayan Library Management Systems 9.6.1. It has been classified as critical. This affects an unknown part of the file admin/modules/circulation/loan_rules.php. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-40970. 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-2023-40771	DataEase 1.18.9 Blacklist sql injection (Issue 5861)	A vulnerability classified as critical was found in DataEase 1.18.9. This vulnerability affects unknown code of the component Blacklist Handler. The manipulation leads to sql injection. This vulnerability was named CVE-2023-40771. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-4708	Infosoftbd Clcknshop 1.0.0 GET Parameter /collection/all tag sql injection	A vulnerability was found in Infosoftbd Clcknshop 1.0.0. It has been rated as critical. This issue affects some unknown processing of the file /collection/all of the component GET Parameter Handler. The manipulation of the argument tag leads to sql injection. The identification of this vulnerability is CVE-2023-4708. 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 SQL injection attack.
CVE-2023-36076	smanga up to 3.1.9 php/history/add.php mediaId/mangaId/userId sql injection (Issue 100)	A vulnerability has been found in smanga up to 3.1.9 and classified as critical. Affected by this vulnerability is an unknown functionality of the file php/history/add.php. The manipulation of the argument mediaId/mangaId/userId leads to sql injection. This vulnerability is known as CVE-2023-36076. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-4745	Beijing Baichuo Smart S45F Multi-Service Secure Gateway Intelligent Management Platform /importexport.php sql injection	A vulnerability was found in Beijing Baichuo Smart S45F Multi-Service Secure Gateway Intelligent Management Platform up to 20230822. It has been rated as critical. Affected by this issue is some unknown functionality of the file /importexport.php. The manipulation leads to sql	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		injection. This vulnerability is handled as CVE-2023-4745. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2023-4740	IBOS OA 4.5.5 Delete Draft delDraft&archiveId=0 sql injection	A vulnerability which was classified as critical was found in IBOS OA 4.5.5. This affects an unknown part of the file remail/api/delDraft&archiveId0 of the component Delete Draft Handler. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-4740. 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.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-4742	IBOS OA 4.5.5 export&uid=X sql injection	A vulnerability was found in IBOS OA 4.5.5 and classified as critical. This issue affects some unknown processing of the file rdashboard/user/export&uidX. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-4742. 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 SQL injection attack.
CVE-2023-4741	IBOS OA 4.5.5 Delete Logs ?r=diary/default/del sql injection	A vulnerability has been found in IBOS OA 4.5.5 and classified as critical. This vulnerability affects unknown code of the file rdiary/default/del of the component Delete Logs Handler. The manipulation leads to sql injection. This vulnerability was named CVE-2023-4741. 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.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-41507	Super Store Finder 3.6 index.php products/distance/lat/lng sql injection	A vulnerability classified as critical was found in Super Store Finder 3.6. This vulnerability affects unknown code of the file index.php. The manipulation of the argument products/distance/lat/lng leads to sql injection. This vulnerability was named CVE-2023-41507. The attack needs to be approached within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-39654	abupy up to 0.4.0 abupy.MarketBu.ABuSymbol.search_to_symbol_	A vulnerability was found in abupy up to 0.4.0. It has been rated as critical.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	sql injection	Affected by this issue is the function abupy.MarketBu.ABuSymbol.search_to_symbol_. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-39654. Access to the local network is required for this attack. There is no exploit available.		
CVE-2021-45811	osTicket 1.15.x Search tickets.php keywords/topic_id sql injection	A vulnerability has been found in osTicket 1.15.x and classified as critical. This vulnerability affects unknown code of the file tickets.php of the component Search. The manipulation of the argument keywords/topic_id leads to sql injection. This vulnerability was named CVE-2021-45811. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-4852	IBOS OA 4.5.5 optimize sql injection	A vulnerability was found in IBOS OA 4.5.5 and classified as critical. This issue affects some unknown processing of the file rdashboard/database/optimize. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-4852. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-4848	SourceCodester Simple Book Catalog App 1.0 delete_book.php delete sql injection	A vulnerability classified as critical was found in SourceCodester Simple Book Catalog App 1.0. Affected by this vulnerability is an unknown functionality of the file delete_book.php. The manipulation of the argument delete leads to sql injection. This vulnerability is known as CVE-2023-4848. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-4849	IBOS OA 4.5.5 trash&op=del fids sql injection	A vulnerability which was classified as critical has been found in IBOS OA 4.5.5. Affected by this issue is some unknown functionality of the file rfile/dashboard/trash&opdel. The manipulation of the argument fids leads to sql injection. This vulnerability is handled as CVE-2023-4849. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-4844	SourceCodester Simple Membership System 1.0 club_edit_query.php club_id sql injection	A vulnerability was found in SourceCodester Simple Membership System 1.0. It has been classified as critical. This affects an unknown part of the file club_edit_query.php. The manipulation of the argument club_id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-4844. It is possible to initiate the	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack remotely. Furthermore there is an exploit available.		
CVE-2023-4851	IBOS OA 4.5.5 edit&op=member sql injection	A vulnerability has been found in IBOS OA 4.5.5 and classified as critical. This vulnerability affects unknown code of the file rdashboard/position/edit&opmember. The manipulation leads to sql injection. This vulnerability was named CVE-2023-4851. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-4845	SourceCodester Simple Membership System 1.0 account_edit_query.php admin_id sql injection	A vulnerability was found in SourceCodester Simple Membership System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file account_edit_query.php. The manipulation of the argument admin_id leads to sql injection. This vulnerability was named CVE-2023-4845. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-4846	SourceCodester Simple Membership System 1.0 delete_member.php mem_id sql injection	A vulnerability was found in SourceCodester Simple Membership System 1.0. It has been rated as critical. This issue affects some unknown processing of the file delete_member.php. The manipulation of the argument mem_id leads to sql injection. The identification of this vulnerability is CVE-2023-4846. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-4850	IBOS OA 4.5.5 del sql injection	A vulnerability which was classified as critical was found in IBOS OA 4.5.5. This affects an unknown part of the file rdashboard/position/del. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-4850. 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-2023-41594	Dairy Farm Shop Management System 1.1 Login Username/Password sql injection	A vulnerability which was classified as critical was found in Dairy Farm Shop Management System 1.1. This affects an unknown part of the component Login. The manipulation of the argument Username/Password leads to sql injection. This vulnerability is uniquely identified as CVE-2023-41594. 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-2023-42268	jeecg-boot up to 3.5.3 show sql injection (Issue 5311)	A vulnerability was found in jeecg-boot up to 3.5.3. It has been rated as critical. This issue affects some unknown processing of the file /jeecg-boot/jmreport/show. The	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-42268. Access to the local network is required for this attack to succeed. There is no exploit available.		
CVE-2023-4867	Xintian Smart Table Integrated Management System 5.6.9 Added Site Page AddUpdateSites.aspx TbxSiteName sql injection	A vulnerability was found in Xintian Smart Table Integrated Management System 5.6.9. It has been classified as critical. Affected is an unknown function of the file /SysManage/AddUpdateSites.aspx of the component Added Site Page. The manipulation of the argument TbxSiteName leads to sql injection. This vulnerability is traded as CVE-2023-4867. 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-2023-4872	SourceCodester Contact Manager App 1.0 add.php contact/contactName sql injection	A vulnerability which was classified as critical has been found in SourceCodester Contact Manager App 1.0. This issue affects some unknown processing of the file add.php. The manipulation of the argument contact/contactName leads to sql injection. The identification of this vulnerability is CVE-2023-4872. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-4871	SourceCodester Contact Manager App 1.0 delete.php contact/contactName sql injection	A vulnerability classified as critical was found in SourceCodester Contact Manager App 1.0. This vulnerability affects unknown code of the file delete.php. The manipulation of the argument contact/contactName leads to sql injection. This vulnerability was named CVE-2023-4871. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-4866	SourceCodester Online Tours & Travels Management System 1.0 booking.php exec id sql injection	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0 and classified as critical. This issue affects the function exec of the file booking.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2023-4866. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-40945	Sourcecodester Doctor Appointment System 1.0 doctors\myDetails.php userid sql injection	A vulnerability was found in Sourcecodester Doctor Appointment System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file doctors\myDetails.php. The	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument userid leads to sql injection. This vulnerability is known as CVE-2023-40945. The attack needs to be done within the local network. There is no exploit available.		
CVE-2023-40946	Schoolmate 1.3 ValidateLogin.php username sql injection	A vulnerability was found in Schoolmate 1.3 and classified as critical. This issue affects some unknown processing of the file ValidateLogin.php. The manipulation of the argument username leads to sql injection. The identification of this vulnerability is CVE-2023-40946. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-40944	Schoolmate 1.3 ~\header.php schoolname sql injection	A vulnerability has been found in Schoolmate 1.3 and classified as critical. This vulnerability affects unknown code of the file ~\header.php. The manipulation of the argument schoolname leads to sql injection. This vulnerability was named CVE-2023-40944. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-4928	InstantSoft icms2 up to 2.16.0 sql injection	A vulnerability which was classified as critical has been found in InstantSoft icms2 up to 2.16.0. Affected by this issue is some unknown functionality. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-4928. Access to the local network is required for this attack. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-42178	Lenosp up to 1.2.0 Log Query Module sql injection	A vulnerability was found in Lenosp up to 1.2.0 and classified as critical. Affected by this issue is some unknown functionality of the component Log Query Module. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-42178. 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-2023-39641	Active Design psaffiliate up to 1.9.7 on PrestaShop initContent sql injection	A vulnerability classified as critical has been found in Active Design psaffiliate up to 1.9.7 on PrestaShop. This affects the function PsaffiliateGetaffiliatesdetailsModuleFrontController::initContent. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-39641. Access to the local network is required for this attack. There is no exploit available. It is recommended to	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		upgrade the affected component.		
CVE-2023-40958	Didotech Engineering & Lifecycle Management Parameter models/base_client.py query sql injection	A vulnerability was found in Didotech Engineering & Lifecycle Management. It has been declared as critical. This vulnerability affects unknown code of the file models/base_client.py of the component Parameter Handler. The manipulation of the argument query leads to sql injection. This vulnerability was named CVE-2023-40958. The attack can be initiated remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-39642	Carts Guru cartsguru up to 2.4.2 on PrestaShop display sql injection	A vulnerability classified as critical was found in Carts Guru cartsguru up to 2.4.2 on PrestaShop. This vulnerability affects the function CartsGuruCatalogModuleFrontController::display. The manipulation leads to sql injection. This vulnerability was named CVE-2023-39642. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-39639	LeoTheme LeoBlog up to 3.1.2 on PrestaShop getListBlogs sql injection	A vulnerability was found in LeoTheme LeoBlog up to 3.1.2 on PrestaShop. It has been declared as critical. Affected by this vulnerability is the function LeoBlogBlog::getListBlogs. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-39639. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-39643	Bl Modules xmlfeeds up to 3.9.7 on PrestaShop SearchApiXml::Xmlfeeds sql injection	A vulnerability which was classified as critical has been found in Bl Modules xmlfeeds up to 3.9.7 on PrestaShop. This issue affects the function SearchApiXml::Xmlfeeds. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-39643. 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-2023-40955	Didotech Engineering & Lifecycle Management models/base_client.py select sql injection	A vulnerability has been found in Didotech Engineering & Lifecycle Management and classified as critical. Affected by this vulnerability is an unknown functionality of the file models/base_client.py. The manipulation of the argument select leads to sql injection. This vulnerability is known as CVE-2023-40955. The	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack can be launched remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.		
CVE-2023-40956	Cloudroits Website Job Search 15.0 controllers/main.py name sql injection	A vulnerability was found in Cloudroits Website Job Search 15.0 and classified as critical. Affected by this issue is some unknown functionality of the file controllers/main.py. The manipulation of the argument name leads to sql injection. This vulnerability is handled as CVE-2023-40956. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-38912	Super Store Finder 3.6 username sql injection (ID 173302)	A vulnerability classified as critical has been found in Super Store Finder 3.6. This affects an unknown part. The manipulation of the argument username leads to sql injection. This vulnerability is uniquely identified as CVE-2023-38912. 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-2023-42405	FIT2CLOUD RackShift 1.7.1 sort sql injection (Issue 79)	A vulnerability was found in FIT2CLOUD RackShift 1.7.1. It has been rated as critical. This issue affects the function taskService.list/bareMetalService.list/switchService.list. The manipulation of the argument sort leads to sql injection. The identification of this vulnerability is CVE-2023-42405. 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-2023-40957	Didotech Engineering & Lifecycle Management Request Parameter models/base_client.py request sql injection	A vulnerability was found in Didotech Engineering & Lifecycle Management. It has been classified as critical. This affects an unknown part of the file models/base_client.py of the component Request Parameter Handler. The manipulation of the argument request leads to sql injection. This vulnerability is uniquely identified as CVE-2023-40957. It is possible to initiate the attack remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5023	Tongda OA 2017 delete.php RELATIVES_ID sql injection	A vulnerability was found in Tongda OA 2017 and classified as critical. Affected by this issue is some unknown functionality of the file general/hr/manage/staff_relatives/delete.php. The manipulation of the argument RELATIVES_ID leads to sql 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 handled as CVE-2023-5023. The attack can only be initiated within the local network. Furthermore there is an exploit available.		
CVE-2023-5027	SourceCodester Simple Membership System 1.0 club_validator.php club sql injection	A vulnerability classified as critical was found in SourceCodester Simple Membership System 1.0. Affected by this vulnerability is an unknown functionality of the file club_validator.php. The manipulation of the argument club leads to sql injection. This vulnerability is known as CVE-2023-5027. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5020	07FLY CRM V2 Administrator Login Page account sql injection	A vulnerability which was classified as critical has been found in 07FLY CRM V2. This issue affects some unknown processing of the file /index.php/sysmanage/Login/login_auth/ of the component Administrator Login Page. The manipulation of the argument account leads to sql injection. The identification of this vulnerability is CVE-2023-5020. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5019	Tongda OA prior 11.10 delete.php REINSTATEMENT_ID sql injection	A vulnerability classified as critical was found in Tongda OA. This vulnerability affects unknown code of the file general/hr/manage/staff_reinstatement/delete.php. The manipulation of the argument REINSTATEMENT_ID leads to sql injection. This vulnerability was named CVE-2023-5019. The attack can be initiated remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5014	Sakshi2610 Food Ordering Website 1.0 categoryfood.php id sql injection	A vulnerability was found in Sakshi2610 Food Ordering Website 1.0 and classified as critical. This issue affects some unknown processing of the file categoryfood.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2023-5014. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5033	OpenRapid RapidCMS 1.3.1 cate-edit-run.php sql injection	A vulnerability classified as critical has been found in OpenRapid RapidCMS 1.3.1. This affects an unknown part of the file /admin/category/cate-edit-run.php. The manipulation of the argument id leads to sql 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 uniquely identified as CVE-2023-5033. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2023-5032	OpenRapid RapidCMS 1.3.1 article-edit-run.php sql injection	A vulnerability was found in OpenRapid RapidCMS 1.3.1. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/article/article-edit-run.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-5032. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5030	Tongda OA up to 11.10 delete.php PLAN_ID sql injection	A vulnerability has been found in Tongda OA up to 11.10 and classified as critical. This vulnerability affects unknown code of the file general/hr/recruit/plan/delete.php. The manipulation of the argument PLAN_ID leads to sql injection. This vulnerability was named CVE-2023-5030. The attack needs to be done within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5029	mccms 2.6 1 sql injection	A vulnerability which was classified as critical was found in mccms 2.6. This affects an unknown part of the file /category/order/hits/copyright/46/finish/1/list/1. The manipulation with the input &039;"1 leads to sql injection. This vulnerability is uniquely identified as CVE-2023-5029. 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-2023-5031	OpenRapid RapidCMS 1.3.1 article-add.php sql injection	A vulnerability was found in OpenRapid RapidCMS 1.3.1. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/article/article-add.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-5031. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-42359	Exam Form Submission 1.0 /index.php val-username sql injection	A vulnerability was found in Exam Form Submission 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /index.php. The manipulation of the argument val-username leads to sql injection. This vulnerability is known as CVE-2023-42359. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-43371	Hoteldruid 3.0.5 creaprezzi.php numcaselle sql injection	A vulnerability was found in Hoteldruid 3.0.5. It has been rated as critical. This issue affects some unknown processing of the file /hoteldruid/creaprezzi.php. The manipulation of the argument numcaselle leads to sql injection. The identification of this vulnerability is CVE-2023-43371. 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-2023-43373	Hoteldruid 3.0.5 interconnessioni.php n_utente_agg sql injection	A vulnerability classified as critical has been found in Hoteldruid 3.0.5. Affected is an unknown function of the file /hoteldruid/interconnessioni.php. The manipulation of the argument n_utente_agg leads to sql injection. This vulnerability is traded as CVE-2023-43373. 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-2023-43374	Hoteldruid 3.0.5 personalizza.php id_utente_log sql injection	A vulnerability classified as critical was found in Hoteldruid 3.0.5. Affected by this vulnerability is an unknown functionality of the file /hoteldruid/personalizza.php. The manipulation of the argument id_utente_log leads to sql injection. This vulnerability is known as CVE-2023-43374. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-34575	opartsavecart up to 2.0.7 on PrestaShop displayAjaxSendCartByEmail(sql injection	A vulnerability was found in opartsavecart up to 2.0.7 on PrestaShop and classified as critical. Affected by this issue is the function OpartSaveCartDefaultModuleFrontController::initContent/OpartSaveCartDefaultModuleFrontController::displayAjaxSendCartByEmail(. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-34575. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-43274	PHP Jabbers PHP Shopping Cart 4.2 id sql injection	A vulnerability classified as critical has been found in PHP Jabbers PHP Shopping Cart 4.2. This affects an unknown part. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-43274. 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-2023-39675	SimpleImportProduct Module 6.2.9 on Prestashop send.php key sql injection	A vulnerability which was classified as critical has been found in SimpleImportProduct Module 6.2.9 on Prestashop. This issue affects some unknown processing of the	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file send.php. The manipulation of the argument key leads to sql injection. The identification of this vulnerability is CVE-2023-39675. The attack can only be initiated within the local network. There is no exploit available.		
CVE-2023-34577	opartplannedpopup up to 1.4.11 on PrestaShop prepareHook sql injection	A vulnerability which was classified as critical was found in opartplannedpopup up to 1.4.11 on PrestaShop. Affected is the function OpartPlannedPopupModuleFrontController::prepareHook. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-34577. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-39600	IceWarp 11.4.6.0 color cross-site scripting	A vulnerability which was classified as problematic has been found in IceWarp 11.4.6.0. This issue affects some unknown processing. The manipulation of the argument color leads to cross-site scripting. The identification of this vulnerability is CVE-2023-39600. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-39707	Free and Open Source Inventory Management System 1.0 Expense Section Add Expense cross-site scripting	A vulnerability has been found in Free and Open Source Inventory Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the component Expense Section. The manipulation of the argument Add Expense leads to cross-site scripting. This vulnerability was named CVE-2023-39707. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-4555	SourceCodester Inventory Management System 1.0 suppliar_data.php name/company cross-site scripting	A vulnerability has been found in SourceCodester Inventory Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file suppliar_data.php. The manipulation of the argument name/company leads to cross-site scripting. This vulnerability is known as CVE-2023-4555. 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-2023-40752	PHP Jabbers Make an Offer Widget 1.0 index.php action cross-site scripting	A vulnerability was found in PHP Jabbers Make an Offer Widget 1.0. It has been classified as problematic. Affected is an unknown function of the file index.php. The manipulation of the argument action leads to cross-site scripting. This vulnerability is traded as CVE-2023-40752. 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-2023-40750	PHP Jabbers Yacht Listing Script 1.0 index.php action cross-site scripting	A vulnerability was found in PHP Jabbers Yacht Listing Script 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file index.php. The manipulation of the argument action leads to cross-site scripting. This vulnerability is known as CVE-2023-40750. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-40755	PHP Jabbers Callback Widget 1.0 preview.php theme cross-site scripting	A vulnerability was found in PHP Jabbers Callback Widget 1.0. It has been rated as problematic. Affected by this issue is some unknown	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		functionality of the file preview.php. The manipulation of the argument theme leads to cross-site scripting. This vulnerability is handled as CVE-2023-40755. The attack may be launched remotely. There is no exploit available.		
CVE-2023-4561	omeka-s omeka up to 4.0.3 cross-site scripting	A vulnerability which was classified as problematic was found in omeka-s omeka up to 4.0.3. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-4561. 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-2023-40753	PHP Jabbers Ticket Support Script 3.2 index.php message cross-site scripting	A vulnerability was found in PHP Jabbers Ticket Support Script 3.2. It has been classified as problematic. This affects an unknown part of the file index.php. The manipulation of the argument message leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-40753. 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-2023-40751	PHP Jabbers Fundraising Script 1.0 index.php action cross-site scripting	A vulnerability has been found in PHP Jabbers Fundraising Script 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file index.php. The manipulation of the argument action leads to cross-site scripting. This vulnerability is known as CVE-2023-40751. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-39708	SourceCodester Inventory Management System 1.0 index.php Add New cross-site scripting	A vulnerability was found in SourceCodester Inventory Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /index.phppagebuy_product. The manipulation of the argument Add New leads to cross-site scripting. This vulnerability was named CVE-2023-39708. 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-2023-41362	MyBB up to 1.8.35 Template code injection (GHSA-pr74-wvp3-q6f5)	A vulnerability was found in MyBB up to 1.8.35. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Template Handler. The manipulation leads to code injection. This vulnerability is known as CVE-2023-41362. The attack needs to be	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		approached within the local network. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-2995	Leyka Plugin up to 3.30.3 on WordPress cross-site scripting	A vulnerability classified as problematic was found in Leyka Plugin up to 3.30.3 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-2995. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-39578	Zenario CMS 9.4 Menu Navigation cross-site scripting	A vulnerability was found in Zenario CMS 9.4. It has been rated as problematic. This issue affects some unknown processing of the component Menu Navigation Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-39578. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-39062	Spipu HTML2PDF up to 5.2.7 forms.php cross-site scripting	A vulnerability which was classified as problematic has been found in Spipu HTML2PDF up to 5.2.7. This issue affects some unknown processing of the file forms.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-39062. 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-2023-38969	Badaso 2.9.7 Book title cross-site scripting	A vulnerability was found in Badaso 2.9.7 and classified as problematic. Affected by this issue is some unknown functionality of the component Book Handler. The manipulation of the argument title leads to cross-site scripting. This vulnerability is handled as CVE-2023-38969. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-39709	SourceCodester Inventory Management System 1.0 Add Member Section Name/Address/Company cross-site scripting	A vulnerability was found in SourceCodester Inventory Management System 1.0. It has been classified as problematic. This affects an unknown part of the component Add Member Section. The manipulation of the argument Name/Address/Company leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-39709. 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-2023-34032	Pascal Casier bbPress Toolkit Plugin up to	A vulnerability which was classified as problematic has	Protected by core rules	Detected by scanner as cross-

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	1.0.12 on WordPress cross-site scripting	been found in Pascal Casier bbPress Toolkit Plugin up to 1.0.12 on WordPress. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-34032. The attack may be launched remotely. There is no exploit available.		site scripting attack.
CVE-2023-34022	Rakib Hasan Dynamic QR Code Generator Plugin up to 0.0.5 on WordPress cross-site scripting	A vulnerability classified as problematic was found in Rakib Hasan Dynamic QR Code Generator Plugin up to 0.0.5 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-34022. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-34173	Alexander Semikashev Yandex Metrica Counter Plugin up to 1.4.3 on WordPress cross-site scripting	A vulnerability which was classified as problematic was found in Alexander Semikashev Yandex Metrica Counter 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-2023-34173. 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-2023-32294	Radical Web Design GDPR Cookie Consent Notice Box Plugin up to 1.1.6 on WordPress cross-site scripting	A vulnerability was found in Radical Web Design GDPR Cookie Consent Notice Box Plugin up to 1.1.6 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-2023-32294. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-25466	Mahlamusa Who Hit The Page Plugin up to 1.4.14.3 on WordPress cross-site scripting	A vulnerability was found in Mahlamusa Who Hit The Page Plugin up to 1.4.14.3 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-25466. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-25471	Webcodin WCP OpenWeather Plugin up to 2.5.0 on WordPress cross-site scripting	A vulnerability was found in Webcodin WCP OpenWeather Plugin up to 2.5.0 on WordPress. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-25471. It is possible to launch the attack	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. There is no exploit available.		
CVE-2023-28692	Kevon Adonis WP Abstracts Plugin up to 2.6.3 on WordPress cross-site scripting	A vulnerability was found in Kevon Adonis WP Abstracts Plugin up to 2.6.3 on WordPress and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-28692. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-24401	Davidsword Mobile Call Now & Map Buttons Plugin up to 1.5.0 on WordPress cross-site scripting	A vulnerability has been found in Davidsword Mobile Call Now & Map Buttons Plugin up to 1.5.0 on WordPress and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-24401. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-34172	Miled Social Login Plugin up to 3.0.4 on WordPress cross-site scripting	A vulnerability which was classified as problematic has been found in Miled Social Login Plugin up to 3.0.4 on WordPress. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-34172. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-27621	MrDemonWolf Livestream Notice Plugin up to 1.2.0 on WordPress cross-site scripting	A vulnerability classified as problematic has been found in MrDemonWolf Livestream Notice Plugin up to 1.2.0 on WordPress. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-27621. 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-2023-34004	WooCommerce Box Office Plugin up to 1.1.50 on WordPress cross-site scripting	A vulnerability which was classified as problematic was found in WooCommerce Box Office Plugin up to 1.1.50 on WordPress. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-34004. 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-2023-34008	weDevs WP ERP Plugin up to 1.12.3 on WordPress cross-site scripting	A vulnerability classified as problematic has been found in weDevs WP ERP Plugin up to 1.12.3 on WordPress. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-34008. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-28415	XootiX Side Cart Woocommerce Plugin up to 2.2 on WordPress cross-site scripting	A vulnerability classified as problematic has been found in XootiX Side Cart Woocommerce Plugin up to 2.2 on WordPress. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-28415. 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-2023-34023	Miled Social Login Plugin up to 3.0.4 on WordPress cross-site scripting	A vulnerability was found in Miled Social Login Plugin up to 3.0.4 on WordPress. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-34023. 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-2023-39678	BDCOM OLT P3310D-2AC 10.1.0F Build 69083 Device WeI interface username cross-site scripting	A vulnerability classified as problematic was found in BDCOM OLT P3310D-2AC 10.1.0F Build 69083. Affected by this vulnerability is an unknown functionality of the component Device WeI interface. The manipulation of the argument username leads to cross-site scripting. This vulnerability is known as CVE-2023-39678. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-41537	PHP Jabbers Business Directory Script 3.2 keyword cross-site scripting	A vulnerability classified as problematic was found in PHP Jabbers Business Directory Script 3.2. Affected by this vulnerability is an unknown functionality. The manipulation of the argument keyword leads to cross-site scripting. This vulnerability is known as CVE-2023-41537. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-41538	PHP Jabbers PHP Forum Script 3.0 keyword cross-site scripting	A vulnerability which was classified as problematic has been found in PHP Jabbers PHP Forum Script 3.0. Affected by this issue is some unknown functionality. The manipulation of the argument keyword leads to cross-site scripting. This vulnerability is handled as CVE-2023-41538. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-4109	Ninja Forms Contact Form Plugin up to 3.6.25 on WordPress cross-site scripting	A vulnerability which was classified as problematic was found in Ninja Forms Contact Form Plugin up to 3.6.25 on WordPress. Affected is an unknown function. The manipulation leads to basic cross-site scripting. This vulnerability is traded as CVE-2023-4109. It is possible	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-3501	FormCraft Plugin up to 1.2.6 on WordPress Setting cross-site scripting	A vulnerability was found in FormCraft Plugin up to 1.2.6 on WordPress. It has been declared as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-3501. 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-2023-39558	AudimexEE 15.0 Show Kai Data Component cross-site scripting	A vulnerability which was classified as problematic has been found in AudimexEE 15.0. Affected by this issue is some unknown functionality of the component Show Kai Data Component. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-39558. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-38971	Badaso up to 2.9.7 Add New Rack rack number cross-site scripting	A vulnerability which was classified as problematic has been found in Badaso up to 2.9.7. This issue affects some unknown processing of the component Add New Rack Handler. The manipulation of the argument rack number leads to cross-site scripting. The identification of this vulnerability is CVE-2023-38971. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-4652	instantsoft icms2 up to 2.16.0 cross-site scripting	A vulnerability was found in instantsoft icms2 up to 2.16.0. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-4652. 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-2023-4653	instantsoft icms2 up to 2.16.0 cross-site scripting	A vulnerability was found in instantsoft icms2 up to 2.16.0. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-4653. The attack can be initiated 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-2023-4655	instantsoft icms2 up to 2.16.0 cross-site scripting	A vulnerability was found in instantsoft icms2 up to 2.16.0. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-4655. 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-2023-38970	Badaso up to 2.9.7 Add New Member cross-site scripting	A vulnerability was found in Badaso up to 2.9.7. It has been rated as problematic. This issue affects some unknown processing of the component Add New Member. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-38970. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-4653	instantsoft icms2 up to 2.16.0 cross-site scripting	A vulnerability was found in instantsoft icms2 up to 2.16.0. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-4653. 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-2023-38970	Badaso up to 2.9.7 Add New Member cross-site scripting	A vulnerability was found in Badaso up to 2.9.7. It has been rated as problematic. This issue affects some unknown processing of the component Add New Member. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-38970. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-41642	GruppoSCAI RealGimm 1.1.37p38 ErroreNonGestito.aspx VIEWSTATE cross-site scripting	A vulnerability was found in GruppoSCAI RealGimm 1.1.37p38. It has been classified as problematic. Affected is an unknown function of the file ErroreNonGestito.aspx. The manipulation of the argument VIEWSTATE leads to cross-site scripting. This vulnerability is traded as CVE-2023-41642. 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-2023-4707	Infosoftbd Clcknshop 1.0.0 /collection/all q cross-site scripting	A vulnerability was found in Infosoftbd Clcknshop 1.0.0. It has been declared as problematic. This vulnerability affects unknown code of the file /collection/all. 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 q leads to cross-site scripting. This vulnerability was named CVE-2023-4707. 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-2023-24675	Bludit CMS 3.14.1 Categories Friendly URL cross-site scripting	A vulnerability which was classified as problematic has been found in Bludit CMS 3.14.1. This issue affects some unknown processing of the component Categories Friendly URL. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-24675. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-39710	Inventory Management System 1.0 Add Customer Section Name/Address/Company cross-site scripting	A vulnerability was found in Inventory Management System 1.0. It has been classified as problematic. Affected is an unknown function of the component Add Customer Section. The manipulation of the argument Name/Address/Company leads to cross-site scripting. This vulnerability is traded as CVE-2023-39710. 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-2023-39703	Typora 1.6.7 Markdown Editor cross-site scripting	A vulnerability which was classified as problematic was found in Typora 1.6.7. Affected is an unknown function of the component Markdown Editor. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-39703. 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-2023-39714	Inventory Management System 1.0 Add Member Section Name/Address/Company cross-site scripting	A vulnerability classified as problematic has been found in Inventory Management System 1.0. This affects an unknown part of the component Add Member Section. The manipulation of the argument Name/Address/Company leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-39714. 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-2023-3499	Photo Gallery, Images, Slider in Rbs Image Gallery Plugin Setting cross-site scripting	A vulnerability which was classified as problematic was found in Photo Gallery Images Slider in Rbs Image Gallery Plugin up to 3.2.15 on WordPress. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2023-3499. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-4151	Store Locator Plugin up to 1.4.12 on WordPress AJAX cross-site scripting	A vulnerability was found in Store Locator Plugin up to 1.4.12 on WordPress and classified as problematic. Affected by this issue is some unknown functionality of the component AJAX Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-4151. 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-2023-4636	File Sharing Plugin up to 2.0.3 on WordPress cross-site scripting	A vulnerability classified as problematic has been found in File Sharing Plugin up to 2.0.3 on WordPress. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-4636. 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-2023-34637	IsarNet IsarFlow 5.23 Portal dashboard title cross-site scripting	A vulnerability was found in IsarNet IsarFlow 5.23. It has been declared as problematic. This vulnerability affects unknown code of the component Portal. The manipulation of the argument dashboard title leads to cross-site scripting. This vulnerability was named CVE-2023-34637. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-39598	IceWarp WebClient 10.2.1 mid cross-site scripting	A vulnerability classified as problematic was found in IceWarp WebClient 10.2.1. Affected by this vulnerability is an unknown functionality. The manipulation of the argument mid leads to cross-site scripting. This vulnerability is known as CVE-2023-39598. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-41107	TEF Portal 2023-07-17 cross-site scripting (SYSS-2023-020)	A vulnerability has been found in TEF Portal 2023-07-17 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-2023-41107. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-41009	bolo-solo 2.6 cross-site scripting	A vulnerability classified as problematic has been found in bolo-solo 2.6. This affects an unknown part. The manipulation leads to cross-	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		site scripting. This vulnerability is uniquely identified as CVE-2023-41009. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2023-39511	Cacti up to 1.2.24 reports_admin.php cross-site scripting (GHSA-5hpr-4hhc-8q42)	A vulnerability which was classified as problematic has been found in Cacti up to 1.2.24. This issue affects some unknown processing of the file reports_admin.php. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-39511. 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-2023-41601	CSZ CMS 1.3.0 Database Host Parameter install/index.php cross-site scripting	A vulnerability classified as problematic has been found in CSZ CMS 1.3.0. Affected is an unknown function of the file install/index.php of the component Database Host Parameter Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-41601. 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-2023-39711	Inventory Management System 1.0 Subtotal/Paidbill cross-site scripting	A vulnerability which was classified as problematic was found in Inventory Management System 1.0. Affected is an unknown function. The manipulation of the argument Subtotal/Paidbill leads to cross-site scripting. This vulnerability is traded as CVE-2023-39711. 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-2023-37798	Vanderbilt REDCap 13.1.35 project title cross-site scripting	A vulnerability was found in Vanderbilt REDCap 13.1.35 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument project title leads to cross-site scripting. This vulnerability is handled as CVE-2023-37798. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-41316	Tolgee up to 3.29.1 cross-site scripting (GHSA-gx3w-rwh5-w5cg)	A vulnerability which was classified as problematic has been found in Tolgee up to 3.29.1. This issue affects some unknown processing. The manipulation leads to basic cross-site scripting. The identification of this vulnerability is CVE-2023-41316. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-39676	SimpleImportProduct Module 1.0.0 on Prestashop ajax.php callback cross-site scripting	A vulnerability which was classified as problematic was found in SimpleImportProduct Module 1.0.0 on Prestashop. Affected is an unknown function of the file ajax.php. The manipulation of the argument callback leads to cross-site scripting. This vulnerability is traded as CVE-2023-39676. 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-2023-4847	SourceCodester Simple Book Catalog App 1.0 Update Book Form book_title/book_author cross-site scripting	A vulnerability classified as problematic has been found in SourceCodester Simple Book Catalog App 1.0. Affected is an unknown function of the component Update Book Form. The manipulation of the argument book_title/book_author leads to cross-site scripting. This vulnerability is traded as CVE-2023-4847. 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-2023-4864	SourceCodester Take-Note App 1.0 index.php noteContent cross-site scripting	A vulnerability which was classified as problematic was found in SourceCodester Take-Note App 1.0. This affects an unknown part of the file index.php. The manipulation of the argument noteContent with the input <script>alert</script > leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-4864. 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-2023-4870	SourceCodester Contact Manager App 1.0 Contact Information index.php contactID cross-site scripting	A vulnerability classified as problematic has been found in SourceCodester Contact Manager App 1.0. This affects an unknown part of the file index.php of the component Contact Information Handler. The manipulation of the argument contactID with the input "><sCrIpT>alert</ScRiPt> leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-4870. 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-2023-4879	InstantSoft icms2 up to 2.16.0 cross-site scripting	A vulnerability which was classified as problematic has been found in InstantSoft icms2 up to 2.16.0. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-4879. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		It is recommended to upgrade the affected component.		
CVE-2023-4913	cecilapp cecil up to 7.47.0 cross-site scripting	A vulnerability classified as problematic was found in cecilapp cecil up to 7.47.0. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-4913. 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-2023-4841	Feeds for YouTube Plugin up to 2.1 on WordPress Shortcode cross-site scripting	A vulnerability was found in Feeds for YouTube Plugin up to 2.1 on WordPress and classified as problematic. Affected by this issue is some unknown functionality of the component Shortcode Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-4841. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-41423	WP Githuber MD Plugin 1.16.2 on WordPress New Article cross-site scripting (Issue 316)	A vulnerability which was classified as problematic was found in WP Githuber MD Plugin 1.16.2 on WordPress. This affects an unknown part of the component New Article. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-41423. 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-2023-4973	Academy LMS 6.2 on Windows GET Parameter /academy/tutor/filter cross-site scripting	A vulnerability was found in Academy LMS 6.2 on Windows. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /academy/tutor/filter of the component GET Parameter Handler. The manipulation of the argument searched_word/searched_tution_class_type[]/searched_price_type[]/searched_duration[] leads to cross-site scripting. This vulnerability is known as CVE-2023-4973. The attack can 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 cross-site scripting attack.
CVE-2023-40984	Webmin 2.100 File Manager cross-site scripting	A vulnerability was found in Webmin 2.100. It has been classified as problematic. This affects an unknown part of the component File Manager. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-40984. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-40986	Webmin 2.100 Usermin Configuration cross-site scripting	A vulnerability was found in Webmin 2.100. It has been declared as problematic. This vulnerability affects unknown code of the component Usermin Configuration. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-40986. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-41160	Usermin 2.001 SSH Configuration Tab key name cross-site scripting	A vulnerability was found in Usermin 2.001 and classified as problematic. This issue affects some unknown processing of the component SSH Configuration Tab. The manipulation of the argument key name leads to cross-site scripting. The identification of this vulnerability is CVE-2023-41160. 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-2023-40985	Webmin 2.100 File Manager cross-site scripting	A vulnerability which was classified as problematic was found in Webmin 2.100. Affected is an unknown function of the component File Manager. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-40985. 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-2023-40869	mooSocial 3.1.6/3.1.7 edit_menu/copuon/group_categorias cross-site scripting	A vulnerability which was classified as problematic was found in mooSocial 3.1.6/3.1.7. This affects the function edit_menu/copuon/group_categorias. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-40869. 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-2023-4977	librenms up to 23.8.x librenms/librenms code injection	A vulnerability was found in librenms up to 23.8.x. It has been rated as critical. This issue affects some unknown processing in the library librenms/librenms. The manipulation leads to code injection. The identification of this vulnerability is CVE-2023-4977. 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-2023-40983	Webmin 2.100 Find in Results File cross-site scripting	A vulnerability which was classified as problematic has been found in Webmin 2.100. Affected by this issue is some unknown functionality of the component Find in Results File Handler. 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 handled as CVE-2023-40983. The attack may be launched remotely. There is no exploit available.		
CVE-2023-40982	Webmin 2.100 module name cross-site scripting	A vulnerability classified as problematic was found in Webmin 2.100. Affected by this vulnerability is an unknown functionality. The manipulation of the argument module name leads to cross-site scripting. This vulnerability is known as CVE-2023-40982. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-4981	librenms up to 23.8.x cross-site scripting	A vulnerability classified as problematic was found in librenms up to 23.8.x. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-4981. 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-2023-4980	librenms up to 23.8.x cross-site scripting	A vulnerability which was classified as problematic has been found in librenms up to 23.8.x. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-4980. 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-2023-4978	librenms up to 23.8.x cross-site scripting	A vulnerability which was classified as problematic was found in librenms up to 23.8.x. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-4978. 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-2023-4982	librenms up to 23.8.x cross-site scripting	A vulnerability has been found in librenms up to 23.8.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-2023-4982. 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-2023-41592	Froala Editor up to 4.1.1 cross-site scripting	A vulnerability was found in Froala Editor up to 4.1.1. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-41592. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-41588	Time to SLA Plugin 10.13.5 durationFormat cross-site scripting	A vulnerability was found in Time to SLA Plugin 10.13.5. It has been classified as problematic. Affected is an unknown function. The manipulation of the argument durationFormat leads to cross-site scripting. This vulnerability is traded as CVE-2023-41588. 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-2023-4979	librenms up to 23.8.x cross-site scripting	A vulnerability classified as problematic has been found in librenms up to 23.8.x. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-4979. 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-2023-39777	vBulletin 5.7.5/6.0.0 Admin Control Panel /login.php url cross-site scripting	A vulnerability classified as problematic was found in vBulletin 5.7.5/6.0.0. Affected by this vulnerability is an unknown functionality of the file /login.phpdologin of the component Admin Control Panel. The manipulation of the argument url leads to cross-site scripting. This vulnerability is known as CVE-2023-39777. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-39612	FileBrowser up to 2.22.x cross-site scripting (Issue 2570)	A vulnerability was found in FileBrowser up to 2.22.x. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-39612. 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-2023-41436	CSZCMS 1.3.0 Pages Content Menu Additional Meta Tag cross-site scripting	A vulnerability was found in CSZCMS 1.3.0. It has been rated as problematic. This issue affects some unknown processing of the component Pages Content Menu. The manipulation of the argument Additional	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Meta Tag leads to cross-site scripting. The identification of this vulnerability is CVE-2023-41436. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-5026	Tongda OA 11.10 menu_code.php OA_SUB_WINDOW cross-site scripting	A vulnerability classified as problematic has been found in Tongda OA 11.10. Affected is an unknown function of the file /general/ipanel/menu_code.phpMENU_TYPEFAV. The manipulation of the argument OA_SUB_WINDOW leads to cross-site scripting. This vulnerability is traded as CVE-2023-5026. 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-2023-5025	KOHA up to 23.05.03 MARC search.pl cross-site scripting	A vulnerability was found in KOHA up to 23.05.03. It has been declared as problematic. This vulnerability affects unknown code of the file /cgi-bin/koha/catalogue/search.pl of the component MARC. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-5025. 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-2023-5024	Planno 23.04.04 Comment cross-site scripting	A vulnerability was found in Planno 23.04.04. It has been classified as problematic. This affects an unknown part of the component Comment Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-5024. 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-2023-5015	UCMS 1.4.7 ajax.php strdefault cross-site scripting	A vulnerability was found in UCMS 1.4.7. It has been classified as problematic. Affected is an unknown function of the file ajax.phpdostrarraylist. The manipulation of the argument strdefault leads to cross-site scripting. This vulnerability is traded as CVE-2023-5015. 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-2023-5013	Pluck CMS 4.7.18 Installation install.php contents cross-site scripting	A vulnerability has been found in Pluck CMS 4.7.18 and classified as problematic. This vulnerability affects unknown code of the file install.php of the component Installation Handler. The manipulation of the argument contents with the input <script>alert</script > leads to cross-site scripting. This vulnerability was named CVE-2023-5013. The attack	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		can be initiated remotely. Furthermore there is an exploit available.		
CVE-2023-38040	Revive Adserver up to 5.4.1 cross-site scripting	A vulnerability was found in Revive Adserver up to 5.4.1. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-38040. 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-2023-42253	code-projects Vehicle Management 1.0 Add Accounts Invoice No/To/Mammul cross-site scripting	A vulnerability classified as problematic was found in code-projects Vehicle Management 1.0. This vulnerability affects unknown code of the component Add Accounts. The manipulation of the argument Invoice No/To/Mammul leads to cross-site scripting. This vulnerability was named CVE-2023-42253. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-43376	Hoteldruid 3.0.5 /hoteldruid/clienti.php nometipotariffa1 cross-site scripting	A vulnerability which was classified as problematic was found in Hoteldruid 3.0.5. This affects an unknown part of the file /hoteldruid/clienti.php. The manipulation of the argument nometipotariffa1 leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-43376. 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-2023-43377	Hoteldruid 3.0.5 visualizza_contratto.php destinatario_email1 cross-site scripting	A vulnerability has been found in Hoteldruid 3.0.5 and classified as problematic. This vulnerability affects unknown code of the file /hoteldruid/visualizza_contratto.php. The manipulation of the argument destinatario_email1 leads to cross-site scripting. This vulnerability was named CVE-2023-43377. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-36234	Netbox 3.5.1 device-roles/add Name cross-site scripting	A vulnerability has been found in Netbox 3.5.1 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file device-roles/add. The manipulation of the argument Name leads to cross-site scripting. This vulnerability is known as CVE-2023-36234. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-43309	Webmin up to 2.002 Cluster Cron Job Tab cross-site scripting	A vulnerability which was classified as problematic was found in Webmin up to 2.002. This affects an unknown part of the component Cluster Cron Job Tab. The manipulation leads to cross-site scripting. This vulnerability is uniquely	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		identified as CVE-2023-43309. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2023-41614	Zoo Management System 1.0 Description of Animal cross-site scripting	A vulnerability which was classified as problematic has been found in Zoo Management System 1.0. This issue affects some unknown processing. The manipulation of the argument Description of Animal leads to cross-site scripting. The identification of this vulnerability is CVE-2023-41614. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-41616	Student Management System up to 1.2.3 cross-site scripting	A vulnerability which was classified as problematic was found in Student Management System up to 1.2.3. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-41616. 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-2023-43456	Service Provider Management System 1.0 firstname/middlename/lastname cross-site scripting	A vulnerability was found in Service Provider Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /php-spms/admin/pageuser. The manipulation of the argument firstname/middlename/lastname leads to cross-site scripting. This vulnerability is handled as CVE-2023-43456. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting 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™