INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

November
2023

The total zero-day vulnerabilities count for **November** month: 334

Command Injection	CSRF	Local File Inclusion	HTTP Request Smuggling	Malicious File Upload	XML External Entity	SQL Injection	Cross-site Scripting
18	20	17	4	14	1	134	126

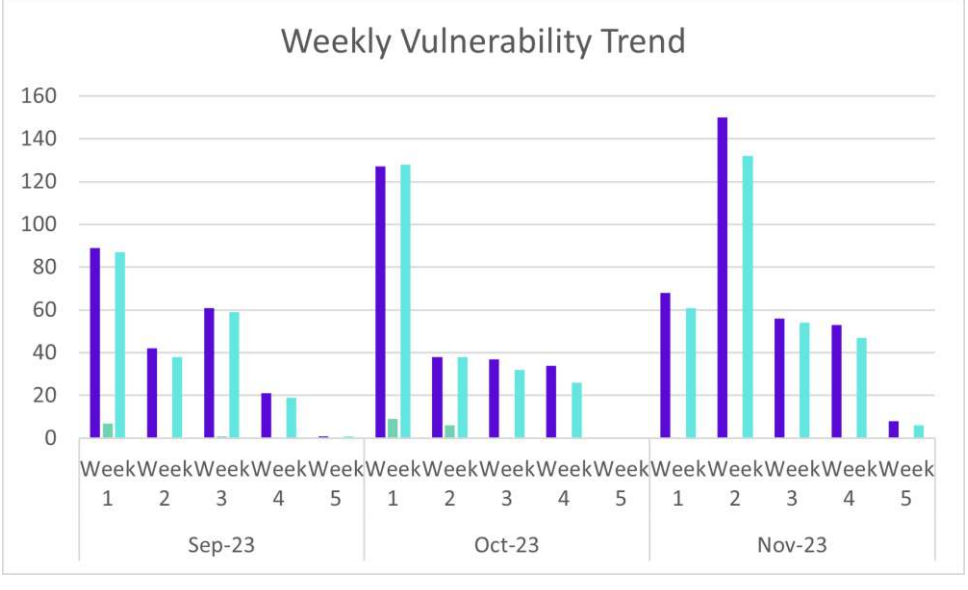
Zero-day vulnerabilities protected through core rules	334
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities for which protection cannot be done	0
Zero-day vulnerabilities found by Indusface WAS	300

- 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 and the type of protection provided for the last quarter.

Weekly Vulnerability Trend

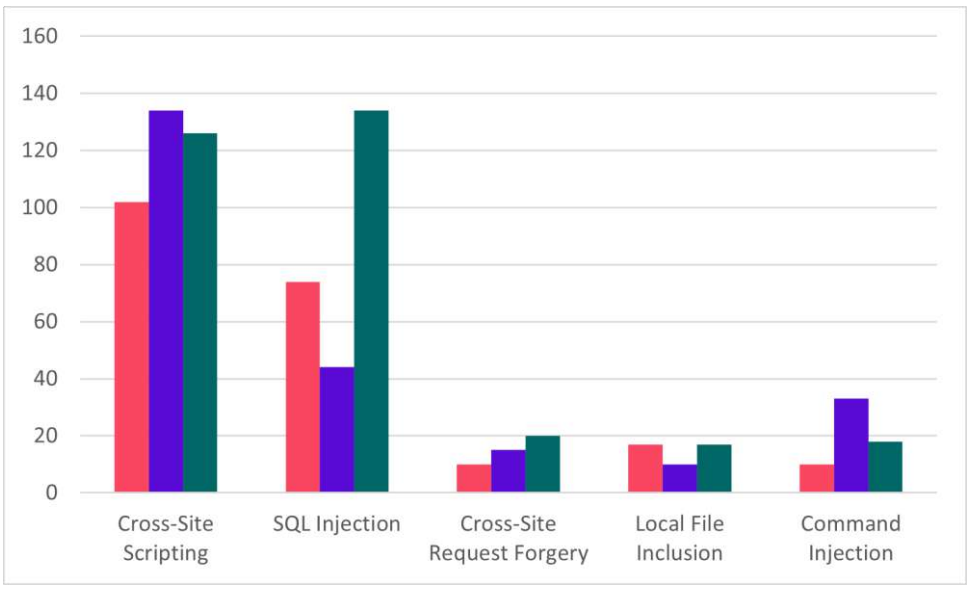


of the zero-day vulnerabilities were protected by the core rules in the last month

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

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

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-45869	ILIAS 7.25 class.ilUtil.php execQuoted command injection	A vulnerability classified as critical was found in ILIAS 7.25. This vulnerability affects the function execQuoted of the file /Services/Utilities/classes/class.ilUtil.php. The manipulation leads to command injection. This vulnerability was named CVE-2023-45869. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-43208	NextGen Healthcare Mirth Connect up to 4.4.0 on CVE Remote Code Execution	A vulnerability classified as critical was found in NextGen Healthcare Mirth Connect up to 4.4.0 on CVE. Affected by this vulnerability is an unknown functionality. The manipulation leads to Remote Code Execution. This vulnerability is known as CVE-2023-43208. 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-2018-17879	ABUS TVIP Camera CGI system injection	A vulnerability classified as very critical has been found in ABUS TVIP Camera. This affects the function system of the component CGI. The manipulation leads to injection. This vulnerability is uniquely identified as CVE-2018-17879. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-45498	Vinchin Backup & Recovery 5.0/6.0/6.7/7.0 command injection	A vulnerability classified as critical was found in Vinchin Backup & Recovery 5.0/6.0/6.7/7.0. Affected by this vulnerability is an	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown functionality. The manipulation leads to command injection. This vulnerability is known as CVE-2023-45498. The attack can only be done within the local network. There is no exploit available.		
CVE-2023-5839	HestiaCP up to 1.8.8 privilege chaining	A vulnerability was found in HestiaCP up to 1.8.8 and classified as critical. This issue affects some unknown processing. The manipulation leads to privilege chaining. The identification of this vulnerability is CVE-2023-5839. The attack needs 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 command injection attack.
CVE-2023-47104	tinyfiledialogs up to 3.14.x os command injection	A vulnerability was found in tinyfiledialogs up to 3.14.x. It has been classified as critical. Affected is an unknown function. The manipulation leads to os command injection. This vulnerability is traded as CVE-2023-47104. The attack needs to be initiated within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2020-36767	tinyfiledialogs up to 3.7.x os command injection	A vulnerability was found in tinyfiledialogs up to 3.7.x. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to os command injection. This vulnerability is known as CVE-2020-36767. 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 command injection attack.
CVE-2023-5843	datafeedr.com Ads Plugin up to 1.1.3 on WordPress Remote Code Execution	A vulnerability was found in datafeedr.com Ads Plugin up to 1.1.3 on WordPress. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to Remote Code Execution. This vulnerability is known as CVE-2023-5843. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-46976	A3300R 17.0.0cu.557_B20221024 UploadFirmwareFile file_name command injection	A vulnerability was found in A3300R 17.0.0cu.557_B20221024 and classified as critical. This issue affects the function UploadFirmwareFile. The manipulation of the argument file_name leads to command injection. The identification of this vulnerability is CVE-2023-	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		46976. Access to the local network is required for this attack. There is no exploit available.		
CVE-2023-46993	Totolink A3300R 17.0.0cu.557_B20221024 setLedCfg enable command injection	A vulnerability was found in Totolink A3300R 17.0.0cu.557_B20221024. It has been rated as critical. Affected by this issue is the function setLedCfg. The manipulation of the argument enable leads to command injection. This vulnerability is handled as CVE-2023-46993. 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-2023-46979	Totolink X6000R 9.4.0cu.852_B20230719 setLedCfg enable command injection	A vulnerability was found in Totolink X6000R 9.4.0cu.852_B20230719. It has been declared as critical. Affected by this vulnerability is the function setLedCfg. The manipulation of the argument enable leads to command injection. This vulnerability is known as CVE-2023-46979. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-46248	sourcegraph cody .vscode/cody.json unknown vulnerability (GHSA-8wmq-fwv7-xmwq)	A vulnerability has been found in sourcegraph cody and classified as critical. Affected by this vulnerability is an unknown functionality of the file .vscode/cody.json. The manipulation leads to external control of system or configuration setting. This vulnerability is known as CVE-2023-46248. 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-2023-46947	Intelliants Subrion 4.2.1 code injection (Issue 909)	A vulnerability has been found in Intelliants Subrion 4.2.1 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to code injection. This vulnerability is known as CVE-2023-46947. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-46404	PCRS up to 3.11 Questions Page/Code Editor sandbox	A vulnerability was found in PCRS up to 3.11. It has been rated as critical. This issue affects some unknown processing of the component Questions Page/Code Editor. The manipulation leads to sandbox issue. The identification of this vulnerability is CVE-2023-46404. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-47253	Qualitor up to 8.20 processVariavel.php gridValoresPopHidden code injection	A vulnerability which was classified as critical has been found in Qualitor up to 8.20. Affected by this issue is some unknown functionality	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the file html/ad/adpesquisasql/request/processVariavel.php. The manipulation of the argument gridValoresPopHidden leads to code injection. This vulnerability is handled as CVE-2023-47253. The attack may be launched remotely. There is no exploit available.		
CVE-2023-47397	WebID up to 1.2.2 categoriestrans.php code injection	A vulnerability was found in WebID up to 1.2.2. It has been rated as critical. Affected by this issue is some unknown functionality of the file admin/categoriestrans.php. The manipulation leads to code injection. This vulnerability is handled as CVE-2023-47397. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-26156	node-chromedriver up to 119.0.0 Setting chromedriver.path os command injection	A vulnerability classified as critical was found in node-chromedriver up to 119.0.0. This vulnerability affects unknown code of the component Setting Handler. The manipulation of the argument chromedriver.path leads to os command injection. This vulnerability was named CVE-2023-26156. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2023-6019	ray URL Parameter cpu_profile os command injection	A vulnerability classified as very critical has been found in ray. This affects an unknown part of the component URL Parameter Handler. The manipulation of the argument cpu_profile leads to os command injection. This vulnerability is uniquely identified as CVE-2023-6019. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-42188	The cosy IceCMS 2.0.1 cross-site request forgery (Issue 17)	A vulnerability which was classified as problematic was found in Thecosy IceCMS 2.0.1. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-42188. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-46375	ZenTao Biz up to 4.1.3 cross-site request forgery	A vulnerability was found in ZenTao Biz up to 4.1.3. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-46375. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-42323	DouHaocms 3.3 adminAction.class.php cross-site request forgery	A vulnerability was found in DouHaocms 3.3. It has been rated as problematic. This issue affects some unknown processing of the file adminAction.class.php. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-42323. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-4251	EventPrime Plugin up to 3.1.x on WordPress cross-site request forgery (Duplicate CVE-2023-5519)	A vulnerability classified as problematic has been found in EventPrime Plugin up to 3.1.x on WordPress. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-4251. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		It is recommended to upgrade the affected component. It looks like this entry got a duplicate CVE-2023-5519 assigned.		
CVE-2023-45670	blakeblackshear frigate up to 0.13.0-beta2 Endpoint cross-site request forgery (GHSA-xq49-hv88-jr6h)	A vulnerability was found in blakeblackshear frigate up to 0.13.0-beta2 and classified as problematic. This issue affects some unknown processing of the component Endpoint. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-45670. 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-2023-5898	pkp-lib prior 3.3.0-16 cross-site request forgery	A vulnerability was found in pkp-lib. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-5898. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-5897	pkp customLocale prior 1.2.0-1 cross-site request forgery	A vulnerability which was classified as problematic has been found in pkp customLocale. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-5897. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-5902	pkp-lib prior 3.3.0-	A vulnerability was	Protected by	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	16 cross-site request forgery	found in pkp-lib. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-5902. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	core rules	
CVE-2023-5893	pkp-lib prior 3.3.0-16 cross-site request forgery	A vulnerability which was classified as problematic was found in pkp-lib. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-5893. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-5899	pkp-lib prior 3.3.0-16 cross-site request forgery	A vulnerability was found in pkp-lib. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-5899. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-5945	Video Carousel Slider with Lightbox Plugin 1.0 on WordPress cross-site request forgery	A vulnerability which was classified as problematic has been found in Video Carousel Slider with Lightbox Plugin 1.0 on WordPress. This issue affects some unknown processing. The manipulation leads to cross-site request forgery.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The identification of this vulnerability is CVE-2023-5945. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-45884	NASA Openmct up to 3.1.0 flexibleLayout Plugin cross-site request forgery	A vulnerability classified as problematic has been found in NASA Openmct up to 3.1.0. This affects an unknown part of the component flexibleLayout Plugin. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-45884. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-48058	Dreamer CMS 4.1.3 /admin/task/run cross-site request forgery	A vulnerability was found in Dreamer CMS 4.1.3. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/task/run. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-48058. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-48060	Dreamer CMS 4.1.3 /admin/task/add cross-site request forgery	A vulnerability was found in Dreamer CMS 4.1.3. It has been classified as problematic. Affected is an unknown function of the file /admin/task/add. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-48060. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-48063	Dreamer CMS 4.1.3 Theme Project /admin/category/delete cross-site request forgery	A vulnerability was found in Dreamer CMS 4.1.3 and classified as problematic. This issue affects some unknown processing of the file /admin/category/delete of the component Theme Project Handler. The manipulation leads	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to cross-site request forgery. The identification of this vulnerability is CVE-2023-48063. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-6022	prefect up to latest API cross-site request forgery	A vulnerability classified as problematic has been found in prefect up to latest. Affected is an unknown function of the component API. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-6022. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-43275	DedeCMS 5.7 Backend Management Interface /catalog_add.php cross-site request forgery	A vulnerability was found in DedeCMS 5.7. It has been classified as problematic. Affected is an unknown function of the file /catalog_add.php of the component Backend Management Interface. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-43275. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-48017	Dreamer CMS 4.1.3 Permission Management cross-site request forgery	A vulnerability was found in Dreamer CMS 4.1.3. It has been rated as problematic. This issue affects some unknown processing of the component Permission Management. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-48017. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-4824	WooHoo Newspaper Magazine Theme up to 2.5.3 on WordPress Setting cross-site request forgery	A vulnerability classified as problematic was found in WooHoo Newspaper Magazine Theme up to 2.5.3 on WordPress. Affected by this vulnerability is an	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown functionality of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-4824. The attack can be launched remotely. There is no exploit available.		
CVE-2023-5651	WP Hotel Booking Plugin up to 2.0.7 on WordPress cross-site request forgery	A vulnerability classified as problematic was found in WP Hotel Booking Plugin up to 2.0.7 on WordPress. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-5651. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-45867	ILIAS 2013-09-12 ScormAicc file path traversal	A vulnerability which was classified as critical was found in ILIAS 2013-09-12. Affected is an unknown function of the component ScormAicc. The manipulation of the argument file leads to path traversal. This vulnerability is traded as CVE-2023-45867. 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-2023-45868	ILIAS 7.25 Learning Module rename old_name/new_name path traversal	A vulnerability classified as critical has been found in ILIAS 7.25. This affects the function rename of the component Learning Module. The manipulation of the argument old_name/new_name leads to path traversal. This vulnerability is uniquely identified as CVE-2023-45868. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2018-16739	ABUS TVIP /opt/cgi/admin/filewrite path traversal	A vulnerability was found in ABUS TVIP and classified as critical. Affected by this issue is some unknown functionality of the file /opt/cgi/admin/filewrite. The manipulation leads to path traversal. This vulnerability is handled as CVE-2018-16739. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-27170	Xpand IT Write-Back Manager 2.3.1 siteName path traversal	A vulnerability has been found in Xpand IT Write-Back Manager 2.3.1 and classified as critical. This vulnerability affects unknown code. The manipulation of the argument siteName leads to path traversal.	Protected by core rules	Detected by scanner as local file inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability was named CVE-2023-27170. The attack needs to be initiated within the local network. There is no exploit available.		
CVE-2023-46468	juzawebCMS up to 3.4 Custom Plugin code injection	A vulnerability was found in juzawebCMS up to 3.4. It has been rated as critical. Affected by this issue is some unknown functionality of the component Custom Plugin Handler. The manipulation leads to code injection. This vulnerability is handled as CVE-2023-46468. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-5199	PHP to Page Plugin up to 0.3 on WordPress Shortcode file inclusion	A vulnerability classified as critical has been found in PHP to Page Plugin up to 0.3 on WordPress. This affects an unknown part of the component Shortcode Handler. The manipulation leads to file inclusion. This vulnerability is uniquely identified as CVE-2023-5199. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-46863	Peppermint Ticket Management up to 0.2.3 POST Request download filepath path traversal (Issue 108)	A vulnerability was found in Peppermint Ticket Management up to 0.2.3. It has been rated as problematic. This issue affects some unknown processing of the file /api/v1/users/file/download of the component POST Request Handler. The manipulation of the argument filepath leads to relative path traversal. The identification of this vulnerability is CVE-2023-46863. The attack may be initiated remotely. There is no exploit available. It is recommended to	Protected by core rules	Detected by scanner as local file inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		upgrade the affected component.		
CVE-2023-46864	Peppermint Ticket Management up to 0.2.4 POST Request download filepath path traversal	A vulnerability classified as problematic has been found in Peppermint Ticket Management up to 0.2.4. Affected is an unknown function of the file /api/v1/ticket/1/file/download of the component POST Request Handler. The manipulation of the argument filepath leads to relative path traversal. This vulnerability is traded as CVE-2023-46864. 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-2023-4591	WPN-XM Serverstack 0.8.6 GET Request index.php page unknown vulnerability	A vulnerability has been found in WPN-XM Serverstack 0.8.6 and classified as problematic. This vulnerability affects unknown code of the file /tools/webinterface/index.php of the component GET Request Handler. The manipulation of the argument page leads to inclusion of functionality from untrusted control sphere. This vulnerability was named CVE-2023-4591. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-34259	Kyocera TASKalfa 4053ci up to 2VG_S000.002.561 Incomplete Fix CVE-2020-23575 wlmdeu%2f%2e%2e%2f%2e%2e path traversal	A vulnerability classified as problematic has been found in Kyocera TASKalfa 4053ci up to 2VG_S000.002.561. Affected is an unknown function of the file /wlmdeu%2f%2e%2e%2f%2e%2e of the component Incomplete Fix CVE-2020-23575. The manipulation leads to path traversal. This vulnerability is traded as CVE-2023-34259. Access to the local network is required for this attack to succeed.	Protected by core rules	Detected by scanner as local file inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		There is no exploit available.		
CVE-2023-46253	Squidex prior 7.9.0 GetFileName path traversal (GHSA-phqq-8g7v-3pg5)	A vulnerability was found in Squidex and classified as critical. This issue affects the function GetFileName. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-46253. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-47246	SysAid On-Premise prior 23.3.36 path traversal	A vulnerability has been found in SysAid On-Premise and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to path traversal. This vulnerability is known as CVE-2023-47246. The attack can only be initiated within the local network. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-45880	GibbonEdu Gibbon up to 25.0.0 Report Template Builder templateFileDestination path traversal (usd-2023-0022)	A vulnerability classified as critical has been found in GibbonEdu Gibbon up to 25.0.0. This affects an unknown part of the component Report Template Builder. The manipulation of the argument templateFileDestination leads to path traversal. This vulnerability is uniquely identified as CVE-2023-45880. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-5245	MLeap prior 0.23.1 Tensorflow Model FileUtil.extract path	A vulnerability which was classified as critical has been found in MLeap.	Protected by core rules	Detected by scanner as local file inclusion

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	traversal	Affected by this issue is the function FileUtil.extract of the component Tensorflow Model Handler. The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-5245. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		attack.
CVE-2023-6038	h2oai h2o-3 Dashboard path traversal	A vulnerability was found in h2oai h2o-3 and classified as problematic. Affected by this issue is some unknown functionality of the component Dashboard. The manipulation leads to path traversal: &039;\..\filename&039;. This vulnerability is handled as CVE-2023-6038. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-6021	ray Log API Endpoint path traversal	A vulnerability has been found in ray and classified as critical. Affected by this vulnerability is an unknown functionality of the component Log API Endpoint. The manipulation leads to path traversal: &039;\..\filename&039;. This vulnerability is known as CVE-2023-6021. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2023-6222	Quttera Web Malware Scanner Plugin up to 3.4.1.48 on WordPress ShowFile path traversal	A vulnerability which was classified as critical has been found in Quttera Web Malware Scanner Plugin up to 3.4.1.48 on WordPress. Affected by this issue is the function ShowFile. The manipulation leads to path traversal.	Protected by core rules	Detected by scanner as local file inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is handled as CVE-2023-6222. The attack needs to be done within the local network. There is no exploit available.		

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-5795	CodeAstro POS System 1.0 Profile Picture /profil unrestricted upload	A vulnerability was found in CodeAstro POS System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /profil of the component Profile Picture Handler. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2023-5795. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-5796	CodeAstro POS System 1.0 Logo /setting unrestricted upload	A vulnerability was found in CodeAstro POS System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /setting of the component Logo Handler. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-5796. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-5790	SourceCodester File Manager App 1.0 endpoint/add-file.php uploadedFileName unrestricted upload	A vulnerability classified as critical was found in SourceCodester File Manager App 1.0. Affected by this vulnerability is an unknown functionality of the file endpoint/add-file.php. The manipulation of the argument uploadedFileName leads to unrestricted	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		upload. This vulnerability is known as CVE-2023-5790. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2023-5812	flusity CMS core/tools/upload.php handleFileUpload uploaded_file unrestricted upload	A vulnerability has been found in flusity CMS and classified as critical. Affected by this vulnerability is the function handleFileUpload of the file core/tools/upload.php. The manipulation of the argument uploaded_file leads to unrestricted upload. This vulnerability is known as CVE-2023-5812. The attack can be launched remotely. Furthermore there is an exploit available. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.	Protected by core rules	NA
CVE-2023-5829	code-projects Admission Management System 1.0 student_avatar.php unrestricted upload	A vulnerability was found in code-projects Admission Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file student_avatar.php. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-5829. 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-2023-46245	Kimai Twig File unrestricted upload	A vulnerability classified as problematic was found in Kimai. Affected by this vulnerability is an unknown functionality of the component Twig File Handler. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2023-46245. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-46865	crater invoice up to 6.0.6 PNG Image upload-logo unrestricted upload (Issue 1267)	A vulnerability was found in crater invoice up to 6.0.6 and classified as problematic. Affected by this issue is some unknown functionality of the file /api/v1/company/upload-logo of the component PNG Image Handler. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-46865. The attack needs to be approached within the local network. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	NA
CVE-2023-5360	Royal Elementor Addons and Templates Plugin prior 1.3.79 on WordPress unrestricted upload	A vulnerability which was classified as critical was found in Royal Elementor Addons and Templates Plugin on WordPress. This affects an unknown part. The manipulation leads to unrestricted upload. This vulnerability is	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		uniquely identified as CVE-2023-5360. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-1720	Bitrix24 up to 22.0.300 MIME Type file.ajax.php unrestricted upload	A vulnerability was found in Bitrix24 up to 22.0.300. It has been declared as critical. This vulnerability affects unknown code of the file /desktop_app/file.ajax.phpactionuploadfile of the component MIME Type Handler. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-1720. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-1713	Bitrix24 up to 22.0.300 Apache HTTP Server instagram.php unrestricted upload	A vulnerability has been found in Bitrix24 up to 22.0.300 and classified as critical. This vulnerability affects unknown code in the library bitrix/modules/crm/lib/order/import/instagram.php of the component Apache HTTP Server. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-1713. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-5901	pkp-lib prior 3.3.0-16 unrestricted upload	A vulnerability classified as problematic has been found in pkp-lib. Affected is an unknown function. The manipulation	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		leads to unrestricted upload. This vulnerability is traded as CVE-2023-5901. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-5919	SourceCodester Company Website CMS 1.0 Create Blog Page /dashboard/createblog unrestricted upload	A vulnerability was found in SourceCodester Company Website CMS 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /dashboard/createblog of the component Create Blog Page. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2023-5919. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	NA
CVE-2023-46428	HadSky 7.12.10 File unrestricted upload	A vulnerability was found in HadSky 7.12.10. It has been classified as critical. This affects an unknown part of the component File Handler. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-46428. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-37790	Jaspersoft Clarity PPM 14.3.0.298 Profile Picture unrestricted upload (ID 173508)	A vulnerability has been found in Jaspersoft Clarity PPM 14.3.0.298 and classified as problematic. Affected	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		by this vulnerability is an unknown functionality of the component Profile Picture Handler. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2023-37790. Access to the local network is required for this attack to succeed. There is no exploit available.		

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-5792	SourceCodester Sticky Notes App 1.0 endpoint/delete-note.php note sql injection	A vulnerability has been found in SourceCodester Sticky Notes App 1.0 and classified as critical. This vulnerability affects unknown code of the file endpoint/delete-note.php. The manipulation of the argument note leads to sql injection. This vulnerability was named CVE-2023-5792. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5794	PHPGurukul Online Railway Catering System 1.0 Login index.php username sql injection	A vulnerability was found in PHPGurukul Online Railway Catering System 1.0. It has been classified as critical. Affected is an unknown function of the file index.php of the component Login. The manipulation of the argument username leads to sql injection. This vulnerability is traded as CVE-2023-5794. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5804	PHPGurukul Nipah Virus Testing Management System 1.0 login.php username sql injection	A vulnerability was found in PHPGurukul Nipah Virus Testing Management System 1.0 and classified as critical. This issue affects some unknown processing of the file login.php. The manipulation of the argument username leads to sql injection. The identification of this vulnerability is CVE-2023-5804. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5785	Netentsec NS-ASG Application Security Gateway 6.3 addaddress_interpret.php messagecontent sql injection	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3. It has been classified as critical. This affects an unknown part of the file /protocol/firewall/addaddress_interpret.php. The manipulation of	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the argument messagecontent leads to sql injection. This vulnerability is uniquely identified as CVE-2023-5785. Access to the local network is required for this attack. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2023-46584	PHPGurukul Nipah Virus Testing Management System 1.0 Request new-user-testing.php sql injection	A vulnerability which was classified as critical was found in PHPGurukul Nipah Virus Testing Management System 1.0. This affects an unknown part of the file new-user-testing.php of the component Request Handler. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-46584. 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-2023-5787	Shaanxi Chanming Education Technology Score Query System 5.0 stuIdCard sql injection	A vulnerability was found in Shaanxi Chanming Education Technology Score Query System 5.0. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument stuIdCard leads to sql injection. The identification of this vulnerability is CVE-2023-5787. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5783	Tongda OA 2017 up to 11.9 delete.php id/sort_parent sql injection	A vulnerability has been found in Tongda OA 2017 up to 11.9 and classified as critical. Affected by this vulnerability is an unknown functionality of the file general/system/approve_center/flow_sort/flow/delete.php. The manipulation of the argument id/sort_parent leads to	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		sql injection. This vulnerability is known as CVE-2023-5783. 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. It is recommended to upgrade the affected component.		
CVE-2023-5784	Netentsec NS-ASG Application Security Gateway 6.3 uploadfirewall.php messagecontent sql injection	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3 and classified as critical. Affected by this issue is some unknown functionality of the file /protocol/firewall/uploadfirewall.php. The manipulation of the argument messagecontent leads to sql injection. This vulnerability is handled as CVE-2023-5784. The attack needs to be initiated within the local network. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5781	Tongda OA 2017 11.10 delete_webmail.php DELETE_STR sql injection	A vulnerability which was classified as critical has been found in Tongda OA 2017 11.10. This issue affects the function DELETE_STR of the file general/system/res_manage/monitor/delete_webmail.php. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-5781. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-5780	Tongda OA 2017 11.10 delete.php DELETE_STR sql injection	A vulnerability classified as critical was found in Tongda OA 2017 11.10. This vulnerability affects unknown code of the file general/system/approve_center/flow_guide/flow_type/set_print/delete.php. The manipulation of the argument DELETE_STR leads to sql injection. This vulnerability was named CVE-2023-5780. 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-2023-5782	Tongda OA 2017 up to 11.10 General News /manage/delete_query.php NEWS_ID sql injection	A vulnerability which was classified as critical was found in Tongda OA 2017 up to 11.10. Affected is an unknown function of the file /manage/delete_query.php of the component General News. The manipulation of the argument NEWS_ID leads to sql injection. This vulnerability is traded as CVE-2023-5782. The attack can only be initiated within the local network. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-44267	Project Worlds Online Art Gallery 1.0 header.php lnm sql injection	A vulnerability classified as critical has been found in Project Worlds Online Art Gallery 1.0. Affected is an unknown function of the file header.php. The manipulation of the argument lnm leads to sql injection. This vulnerability is traded as CVE-2023-44267. 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-2023-46435	SourceCodester	A vulnerability has	Protected by	Detected by

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Packers and Movers Management System 1.0 id sql injection	been found in SourceCodester Packers and Movers Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file mpms/pservices/view_service. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-46435. Access to the local network is required for this attack to succeed. There is no exploit available.	core rules	scanner as SQL injection attack.
CVE-2023-5805	SourceCodester Simple Real Estate Portal System 1.0 view_estate.php id sql injection	A vulnerability was found in SourceCodester Simple Real Estate Portal System 1.0. It has been classified as critical. Affected is an unknown function of the file view_estate.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-5805. 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-2023-42406	D-Link DAR-7000 V31R02B1413C editrole.php sql injection	A vulnerability which was classified as critical has been found in D-Link DAR-7000 V31R02B1413C. Affected by this issue is some unknown functionality of the file editrole.php. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-42406. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-44375	Online Art Gallery 1.0 header.php add1 sql injection	A vulnerability was found in Online Art Gallery 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file header.php. The manipulation of the argument add1 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-2023-44375. The attack may be launched remotely. There is no exploit available.		
CVE-2023-5826	Netentsec NS-ASG Application Security Gateway 6.3 list_onlineuser.php SessionId sql injection	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/list_onlineuser.php. The manipulation of the argument SessionId leads to sql injection. This vulnerability is handled as CVE-2023-5826. The attack needs to be initiated within the local network. Furthermore there is an exploit available. We tried to contact the vendor early about the disclosure but the official mail address was not working properly.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-44377	Project Worlds Online Art Gallery 1.0 header.php add3 sql injection	A vulnerability which was classified as critical has been found in Project Worlds Online Art Gallery 1.0. Affected by this issue is some unknown functionality of the file header.php. The manipulation of the argument add3 leads to sql injection. This vulnerability is handled as CVE-2023-44377. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-43738	Online Art Gallery 1.0 header.php email sql injection	A vulnerability has been found in Online Art Gallery 1.0 and classified as critical. This vulnerability affects unknown code of the file header.php. The manipulation of the argument email leads to sql injection. This vulnerability was named CVE-2023-43738. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-43737	Online Art Gallery 1.0 header.php fnm	A vulnerability classified as critical has	Protected by core rules	Detected by scanner as SQL

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	sql injection	been found in Online Art Gallery 1.0. Affected is an unknown function of the file header.php. The manipulation of the argument fnm leads to sql injection. This vulnerability is traded as CVE-2023-43737. It is possible to launch the attack remotely. There is no exploit available.		injection attack.
CVE-2023-44162	Online Art Gallery 1.0 header.php contact sql injection	A vulnerability which was classified as critical was found in Online Art Gallery 1.0. This affects an unknown part of the file header.php. The manipulation of the argument contact leads to sql injection. This vulnerability is uniquely identified as CVE-2023-44162. 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-2023-44268	Online Art Gallery 1.0 header.php gender sql injection	A vulnerability classified as critical was found in Online Art Gallery 1.0. Affected by this vulnerability is an unknown functionality of the file header.php. The manipulation of the argument gender leads to sql injection. This vulnerability is known as CVE-2023-44268. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5827	Shanghai CTI Navigation CTI Monitoring and Early Warning System 2.2 UserEdit.aspx ID sql injection	A vulnerability was found in Shanghai CTI Navigation CTI Monitoring and Early Warning System 2.2. It has been classified as critical. This affects an unknown part of the file /Web/SysManage/UserEdit.aspx. The manipulation of the argument ID leads to sql injection. This vulnerability is uniquely identified as CVE-2023-5827. Access to the local network is required for this attack. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5828	Nanning Ontall Longxing Industrial	A vulnerability was found in Nanning	Protected by core rules	Detected by scanner as SQL

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Development Zone Project Construction and Installation Management System login.aspx sql injection	Ontall Longxing Industrial Development Zone Project Construction and Installation Management System up to 20231026. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file login.aspx. The manipulation of the argument tbxUserName leads to sql injection. This vulnerability is known as CVE-2023-5828. The attack can be launched remotely. Furthermore there is an exploit available.		injection attack.
CVE-2023-44376	Project Worlds Online Art Gallery 1.0 header.php add2 sql injection	A vulnerability was found in Project Worlds Online Art Gallery 1.0. It has been rated as critical. This issue affects some unknown processing of the file header.php. The manipulation of the argument add2 leads to sql injection. The identification of this vulnerability is CVE-2023-44376. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-46490	Cacti 1.2.25 managers.php form_actions sql injection (GHSA-f4r3-53jr-654c)	A vulnerability was found in Cacti 1.2.25. It has been declared as critical. Affected by this vulnerability is the function form_actions of the file managers.php. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-46490. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-44480	Project Worlds Leave Management System Project 1.0 admin/setleaves.php setcasualleave sql injection	A vulnerability has been found in Project Worlds Leave Management System Project 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file admin/setleaves.php. The manipulation of the argument setcasualleave leads to	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		sql injection. This vulnerability is known as CVE-2023-44480. The attack can be launched remotely. There is no exploit available.		
CVE-2023-5439	WP Photo Text Slider 50 Plugin up to 8.0 on WordPress Shortcode sql injection	A vulnerability which was classified as critical was found in WP Photo Text Slider 50 Plugin up to 8.0 on WordPress. This affects an unknown part of the component Shortcode Handler. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-5439. 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-2023-5435	Up Down Image Slideshow Gallery Plugin up to 12.0 on WordPress Shortcode sql injection	A vulnerability was found in Up Down Image Slideshow Gallery Plugin up to 12.0 on WordPress. It has been rated as critical. This issue affects some unknown processing of the component Shortcode Handler. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-5435. 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-2023-5436	Vertical Marquee Plugin up to 7.1 on WordPress Shortcode sql injection	A vulnerability classified as critical was found in Vertical Marquee Plugin up to 7.1 on WordPress. Affected by this vulnerability is an unknown functionality of the component Shortcode Handler. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-5436. 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-2023-5430	Jquery News Ticker Plugin up to 3.0 on WordPress Shortcode sql injection	A vulnerability has been found in Jquery News Ticker Plugin up to 3.0 on WordPress and classified as	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		critical. This vulnerability affects unknown code of the component Shortcode Handler. The manipulation leads to sql injection. This vulnerability was named CVE-2023-5430. Access to the local network is required for this attack to succeed. There is no exploit available.		
CVE-2023-5434	Superb Slideshow Gallery up to 13.1 on WordPress Shortcode sql injection	A vulnerability which was classified as critical has been found in Superb Slideshow Gallery up to 13.1 on WordPress. Affected by this issue is some unknown functionality of the component Shortcode Handler. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-5434. 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-2023-5437	WP Fade in Text News Plugin up to 12.0 on WordPress Shortcode sql injection	A vulnerability was found in WP Fade in Text News Plugin up to 12.0 on WordPress. It has been classified as critical. This affects an unknown part of the component Shortcode Handler. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-5437. 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-2023-5429	Information Reel Plugin up to 10.0 on WordPress Shortcode sql injection	A vulnerability classified as critical was found in Information Reel Plugin up to 10.0 on WordPress. This vulnerability affects unknown code of the component Shortcode Handler. The manipulation leads to sql injection. This vulnerability was named CVE-2023-5429. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-5431	Left Right Image Slideshow Gallery Plugin up to 12.0 on WordPress Shortcode sql injection	A vulnerability has been found in Left Right Image Slideshow Gallery Plugin up to 12.0 on WordPress and classified as critical. Affected by this vulnerability is an unknown functionality of the component Shortcode Handler. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-5431. 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-2023-5433	Message Ticker Plugin up to 9.2 on WordPress Shortcode sql injection	A vulnerability was found in Message Ticker Plugin up to 9.2 on WordPress. It has been rated as critical. Affected by this issue is some unknown functionality of the component Shortcode Handler. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-5433. 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-2023-5438	WP Image Slideshow Plugin up to 12.0 on WordPress Shortcode sql injection	A vulnerability classified as critical has been found in WP Image Slideshow Plugin up to 12.0 on WordPress. This affects an unknown part of the component Shortcode Handler. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-5438. 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-2023-5464	Jquery Accordion Slideshow Plugin up to 8.1 on WordPress Shortcode sql injection	A vulnerability which was classified as critical was found in Jquery Accordion Slideshow Plugin up to 8.1 on WordPress. Affected is an unknown function of the component Shortcode Handler. The manipulation 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 traded as CVE-2023-5464. The attack needs to be done within the local network. There is no exploit available.		
CVE-2023-5428	Image Vertical Reel Scroll Slideshow Plugin up to 9.0 on WordPress Shortcode sql injection	A vulnerability was found in Image Vertical Reel Scroll Slideshow Plugin up to 9.0 on WordPress and classified as critical. Affected by this issue is some unknown functionality of the component Shortcode Handler. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-5428. 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-2023-5412	Image Horizontal Reel Scroll Slideshow Plugin up to 13.2 on WordPress Shortcode sql injection	A vulnerability which was classified as critical has been found in Image Horizontal Reel Scroll Slideshow Plugin up to 13.2 on WordPress. This issue affects some unknown processing of the component Shortcode Handler. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-5412. 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-2023-46356	Bl Modules CSV Feeds PRO Module up to 2.6.0 on PrestaShop getProducts sql injection	A vulnerability classified as critical has been found in Bl Modules CSV Feeds PRO Module up to 2.6.0 on PrestaShop. Affected is the function SearchApiCsv::getProducts. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-46356. Access to the local network is required for this attack to succeed. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45996	Senayan SLiMS/Bulian	A vulnerability was found in Senayan	Protected by core rules	Detected by scanner as SQL

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	member_type.php reborrowLimit sql injection (Issue 216)	SLiMS and Bulian. It has been rated as critical. Affected by this issue is some unknown functionality of the file member_type.php. The manipulation of the argument reborrowLimit leads to sql injection. This vulnerability is handled as CVE-2023-45996. The attack may be launched remotely. There is no exploit available.		injection attack.
CVE-2023-46482	wuzhicms 4.1.0 Database Backup index.php sql injection	A vulnerability was found in wuzhicms 4.1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file coreframe/app/database/admin/index.php of the component Database Backup Handler. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-46482. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45113	Project Worlds Online Examination System 1.0 feed.php name sql injection	A vulnerability has been found in Project Worlds Online Examination System 1.0 and classified as critical. This vulnerability affects unknown code of the file feed.php. The manipulation of the argument name leads to sql injection. This vulnerability was named CVE-2023-45113. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45328	Project Worlds Online Food Ordering System 1.0 routers/add-users.php password sql injection	A vulnerability was found in Project Worlds Online Food Ordering System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file routers/add-users.php. The manipulation of the argument password leads to sql injection. This vulnerability was	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		named CVE-2023-45328. The attack can be initiated remotely. There is no exploit available.		
CVE-2023-45327	Project Worlds Online Food Ordering System 1.0 routers/add-users.php name sql injection	A vulnerability has been found in Project Worlds Online Food Ordering System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file routers/add-users.php. The manipulation of the argument name leads to sql injection. This vulnerability is known as CVE-2023-45327. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45114	Project Worlds Online Examination System 1.0 feed.php subject sql injection	A vulnerability was found in Project Worlds Online Examination System 1.0 and classified as critical. This issue affects some unknown processing of the file feed.php. The manipulation of the argument subject leads to sql injection. The identification of this vulnerability is CVE-2023-45114. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45326	Project Worlds Online Food Ordering System 1.0 routers/add-users.php email sql injection	A vulnerability was found in Project Worlds Online Food Ordering System 1.0. It has been classified as critical. This affects an unknown part of the file routers/add-users.php. The manipulation of the argument email leads to sql injection. This vulnerability is uniquely identified as CVE-2023-45326. 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-2023-45331	Project Worlds Online Food Ordering System 1.0 routers/add-users.php contact sql injection	A vulnerability classified as critical was found in Project Worlds Online Food Ordering System 1.0. Affected by this vulnerability is an unknown functionality of the file routers/add-users.php. The manipulation of the	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument contact leads to sql injection. This vulnerability is known as CVE-2023-45331. The attack can be launched remotely. There is no exploit available.		
CVE-2023-45339	Project Worlds Online Food Ordering System 1.0 routers/add-ticket.php type sql injection	A vulnerability classified as critical has been found in Project Worlds Online Food Ordering System 1.0. This affects an unknown part of the file routers/add-ticket.php. The manipulation of the argument type leads to sql injection. This vulnerability is uniquely identified as CVE-2023-45339. 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-2023-45333	Project Worlds Online Food Ordering System 1.0 routers/add-users.php verified sql injection	A vulnerability has been found in Project Worlds Online Food Ordering System 1.0 and classified as critical. This vulnerability affects unknown code of the file routers/add-users.php. The manipulation of the argument verified leads to sql injection. This vulnerability was named CVE-2023-45333. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45323	Project Worlds Online Food Ordering System 1.0 routers/add-item.php name sql injection	A vulnerability which was classified as critical has been found in Project Worlds Online Food Ordering System 1.0. This issue affects some unknown processing of the file routers/add-item.php. The manipulation of the argument name leads to sql injection. The identification of this vulnerability is CVE-2023-45323. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45336	Project Worlds Online Food Ordering System 1.0 routers/router.php password sql	A vulnerability was found in Project Worlds Online Food Ordering System 1.0 and classified as critical.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	This issue affects some unknown processing of the file routers/router.php. The manipulation of the argument password leads to sql injection. The identification of this vulnerability is CVE-2023-45336. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-45340	Project Worlds Online Food Ordering System 1.0 details-router.php phone sql injection	A vulnerability was found in Project Worlds Online Food Ordering System 1.0. It has been rated as critical. This issue affects some unknown processing of the file routers/details-router.php. The manipulation of the argument phone leads to sql injection. The identification of this vulnerability is CVE-2023-45340. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5918	SourceCodester Visitor Management System 1.0 manage_user.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Visitor Management System 1.0. Affected is an unknown function of the file manage_user.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-5918. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5929	Campcodes Simple Student Information System 1.0 manage_academic.php id sql injection	A vulnerability was found in Campcodes Simple Student Information System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/students/manage_academic.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-5929. The attack can only be done	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		within the local network. Furthermore there is an exploit available.		
CVE-2023-45324	Project Worlds Online Food Ordering System 1.0 routers/add-item.php price sql injection	A vulnerability was found in Project Worlds Online Food Ordering System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file routers/add-item.php. The manipulation of the argument price leads to sql injection. This vulnerability is handled as CVE-2023-45324. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45325	Project Worlds Online Food Ordering System 1.0 routers/add-users.php address sql injection	A vulnerability classified as critical was found in Project Worlds Online Food Ordering System 1.0. This vulnerability affects unknown code of the file routers/add-users.php. The manipulation of the argument address leads to sql injection. This vulnerability was named CVE-2023-45325. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5928	Campcodes Simple Student Information System 1.0 manage_department.php id sql injection	A vulnerability was found in Campcodes Simple Student Information System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/departments/manage_department.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-5928. 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-2023-5927	Campcodes Simple Student Information System 1.0 manage_course.php id sql injection	A vulnerability has been found in Campcodes Simple Student Information System 1.0 and classified as critical. Affected by this vulnerability is an	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown functionality of the file /admin/courses/manage_course.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-5927. Access to the local network is required for this attack to succeed. Furthermore there is an exploit available.		
CVE-2023-5926	Campcodes Simple Student Information System 1.0 update_status.php student_id sql injection	A vulnerability which was classified as critical was found in Campcodes Simple Student Information System 1.0. Affected is an unknown function of the file /admin/students/update_status.php. The manipulation of the argument student_id leads to sql injection. This vulnerability is traded as CVE-2023-5926. Access to the local network is required for this attack. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5925	Campcodes Simple Student Information System 1.0 /classes/Master.php f sql injection	A vulnerability which was classified as critical has been found in Campcodes Simple Student Information System 1.0. This issue affects some unknown processing of the file /classes/Master.php. The manipulation of the argument f leads to sql injection. The identification of this vulnerability is CVE-2023-5925. The attack needs to be initiated within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5923	Campcodes Simple Student Information System 1.0 /admin/index.php id sql injection	A vulnerability classified as critical has been found in Campcodes Simple Student Information System 1.0. This affects an unknown part of the file /admin/index.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2023-5923. The attack can only be initiated within the local network. Furthermore there is an exploit available.		
CVE-2023-45335	Project Worlds Online Food Ordering System 1.0 routers/edit-orders.php id sql injection	A vulnerability which was classified as critical was found in Project Worlds Online Food Ordering System 1.0. This affects an unknown part of the file routers/edit-orders.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-45335. 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-2023-45329	Project Worlds Online Food Ordering System 1.0 routers/add-users.php role sql injection	A vulnerability which was classified as critical was found in Project Worlds Online Food Ordering System 1.0. Affected is an unknown function of the file routers/add-users.php. The manipulation of the argument role leads to sql injection. This vulnerability is traded as CVE-2023-45329. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45345	Project Worlds Online Food Ordering System 1.0 routers/user-router.php *_deleted sql injection	A vulnerability which was classified as critical has been found in Project Worlds Online Food Ordering System 1.0. This issue affects some unknown processing of the file routers/user-router.php. The manipulation of the argument _deleted leads to sql injection. The identification of this vulnerability is CVE-2023-45345. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45111	Project Worlds Online Examination System 1.0 feed.php email sql injection	A vulnerability was found in Project Worlds Online Examination System 1.0. It has been classified as critical. Affected is an unknown function of the file feed.php. The manipulation of the	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument email leads to sql injection. This vulnerability is traded as CVE-2023-45111. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2023-45019	Project Worlds Online Bus Booking System 1.0 category.php category sql injection	A vulnerability which was classified as critical was found in Project Worlds Online Bus Booking System 1.0. This affects an unknown part of the file category.php. The manipulation of the argument category leads to sql injection. This vulnerability is uniquely identified as CVE-2023-45019. 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-2023-45013	Project Worlds Online Bus Booking System 1.0 bus_info.php user_query sql injection	A vulnerability was found in Project Worlds Online Bus Booking System 1.0. It has been rated as critical. This issue affects some unknown processing of the file bus_info.php. The manipulation of the argument user_query leads to sql injection. The identification of this vulnerability is CVE-2023-45013. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45017	Project Worlds Online Bus Booking System 1.0 search.php destination sql injection	A vulnerability classified as critical has been found in Project Worlds Online Bus Booking System 1.0. Affected is an unknown function of the file search.php. The manipulation of the argument destination leads to sql injection. This vulnerability is traded as CVE-2023-45017. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45330	Project Worlds Online Food Ordering System 1.0 routers/add-users.php username sql injection	A vulnerability classified as critical has been found in Project Worlds Online Food Ordering System 1.0. Affected is an unknown function of the file routers/add-users.php.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The manipulation of the argument username leads to sql injection. This vulnerability is traded as CVE-2023-45330. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2023-45346	Project Worlds Online Food Ordering System 1.0 routers/user-router.php *_role sql injection	A vulnerability which was classified as critical was found in Project Worlds Online Food Ordering System 1.0. Affected is an unknown function of the file routers/user-router.php. The manipulation of the argument _role leads to sql injection. This vulnerability is traded as CVE-2023-45346. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45334	Project Worlds Online Food Ordering System 1.0 routers/edit-orders.php status sql injection	A vulnerability which was classified as critical has been found in Project Worlds Online Food Ordering System 1.0. Affected by this issue is some unknown functionality of the file routers/edit-orders.php. The manipulation of the argument status leads to sql injection. This vulnerability is handled as CVE-2023-45334. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45344	Project Worlds Online Food Ordering System 1.0 routers/user-router.php *_balance sql injection	A vulnerability was found in Project Worlds Online Food Ordering System 1.0. It has been classified as critical. This affects an unknown part of the file routers/user-router.php. The manipulation of the argument _balance leads to sql injection. This vulnerability is uniquely identified as CVE-2023-45344. 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-2023-45347	Project Worlds Online Food Ordering System 1.0	A vulnerability has been found in Project Worlds Online Food	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	routers/user-router.php *_verified sql injection	Ordering System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file routers/user-router.php. The manipulation of the argument _verified leads to sql injection. This vulnerability is known as CVE-2023-45347. The attack can be launched remotely. There is no exploit available.		
CVE-2023-45012	Project Worlds Online Bus Booking System 1.0 bus_info.php user_email sql injection	A vulnerability which was classified as critical has been found in Project Worlds Online Bus Booking System 1.0. Affected by this issue is some unknown functionality of the file bus_info.php. The manipulation of the argument user_email leads to sql injection. This vulnerability is handled as CVE-2023-45012. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45018	Project Worlds Online Bus Booking System 1.0 includes/login.php username sql injection	A vulnerability classified as critical was found in Project Worlds Online Bus Booking System 1.0. Affected by this vulnerability is an unknown functionality of the file includes/login.php. The manipulation of the argument username leads to sql injection. This vulnerability is known as CVE-2023-45018. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-5924	Campcodes Simple Student Information System 1.0 view_course.php id sql injection	A vulnerability classified as critical was found in Campcodes Simple Student Information System 1.0. This vulnerability affects unknown code of the file /admin/courses/view_course.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-5924. The attack needs to be	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		done within the local network. Furthermore there is an exploit available.		
CVE-2023-45342	Project Worlds Online Food Ordering System 1.0 register-router.php phone sql injection	A vulnerability was found in Project Worlds Online Food Ordering System 1.0. It has been classified as critical. Affected is an unknown function of the file routers/register-router.php. The manipulation of the argument phone leads to sql injection. This vulnerability is traded as CVE-2023-45342. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45338	Project Worlds Online Food Ordering System 1.0 routers/add-ticket.php id sql injection	A vulnerability was found in Project Worlds Online Food Ordering System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file routers/add-ticket.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-45338. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45332	Project Worlds Online Food Ordering System 1.0 routers/add-users.php deleted sql injection	A vulnerability classified as critical has been found in Project Worlds Online Food Ordering System 1.0. This affects an unknown part of the file routers/add-users.php. The manipulation of the argument deleted leads to sql injection. This vulnerability is uniquely identified as CVE-2023-45332. 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-2023-45014	Project Worlds Online Bus Booking System 1.0 bus_info.php bus_id sql injection	A vulnerability was found in Project Worlds Online Bus Booking System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file bus_info.php. The manipulation of the argument bus_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 was named CVE-2023-45014. The attack can be initiated remotely. There is no exploit available.		
CVE-2023-45015	Project Worlds Online Bus Booking System 1.0 bus_info.php date sql injection	A vulnerability was found in Project Worlds Online Bus Booking System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file bus_info.php. The manipulation of the argument date leads to sql injection. This vulnerability is known as CVE-2023-45015. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45341	Project Worlds Online Food Ordering System 1.0 routers/menu-router.php *_price sql injection	A vulnerability was found in Project Worlds Online Food Ordering System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file routers/menu-router.php. The manipulation of the argument _price leads to sql injection. This vulnerability is handled as CVE-2023-45341. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45337	Project Worlds Online Food Ordering System 1.0 routers/router.php username sql injection	A vulnerability was found in Project Worlds Online Food Ordering System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file routers/router.php. The manipulation of the argument username leads to sql injection. This vulnerability is known as CVE-2023-45337. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-45343	Project Worlds Online Food Ordering System 1.0 ticket-message.php	A vulnerability classified as critical was found in Project Worlds Online Food Ordering	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	ticket_id sql injection	System 1.0. This vulnerability affects unknown code of the file routers/ticket-message.php. The manipulation of the argument ticket_id leads to sql injection. This vulnerability was named CVE-2023-45343. The attack can be initiated remotely. There is no exploit available.		
CVE-2023-45112	Project Worlds Online Examination System 1.0 feed.php feedback sql injection	A vulnerability classified as critical has been found in Project Worlds Online Examination System 1.0. This affects an unknown part of the file feed.php. The manipulation of the argument feedback leads to sql injection. This vulnerability is uniquely identified as CVE-2023-45112. 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-2023-45016	Project Worlds Online Bus Booking System 1.0 search.php source sql injection	A vulnerability was found in Project Worlds Online Bus Booking System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file search.php. The manipulation of the argument source leads to sql injection. This vulnerability is handled as CVE-2023-45016. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-46954	Relativity RelativityOne up to 12.1.537.3 Patch 2 name sql injection	A vulnerability classified as critical was found in Relativity RelativityOne up to 12.1.537.3 Patch 2. Affected by this vulnerability is an unknown functionality. The manipulation of the argument name leads to sql injection. This vulnerability is known as CVE-2023-46954. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-46981	Novel-Plus 4.2.0 /common/log/list	A vulnerability which was classified as critical	Protected by core rules	Detected by scanner as SQL

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	sort sql injection	has been found in Novel-Plus 4.2.0. This issue affects some unknown processing of the file /common/log/list. The manipulation of the argument sort leads to sql injection. The identification of this vulnerability is CVE-2023-46981. The attack may be initiated remotely. There is no exploit available.		injection attack.
CVE-2023-5709	WD WidgetTwitter Plugin up to 1.0.9 on WordPress Shortcode sql injection	A vulnerability classified as critical was found in WD WidgetTwitter Plugin up to 1.0.9 on WordPress. Affected by this vulnerability is an unknown functionality of the component Shortcode Handler. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-5709. 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-2023-33478	RemoteClinic 2.0 /medicines/stocks.php ID sql injection (Issue 22)	A vulnerability classified as critical has been found in RemoteClinic 2.0. This affects an unknown part of the file /medicines/stocks.php. The manipulation of the argument ID leads to sql injection. This vulnerability is uniquely identified as CVE-2023-33478. 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-2023-42283	Tyk Gateway 5.0.3 api_id sql injection	A vulnerability was found in Tyk Gateway 5.0.3. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument api_id leads to sql injection. The identification of this vulnerability is CVE-2023-42283. 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-2023-33479	RemoteClinic 2.0 /staff/edit.php sql	A vulnerability classified as critical was	Protected by core rules	Detected by scanner as SQL

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection (Issue 23)	found in RemoteClinic 2.0. This vulnerability affects unknown code of the file /staff/edit.php. The manipulation leads to sql injection. This vulnerability was named CVE-2023-33479. The attack can be initiated remotely. There is no exploit available.		injection attack.
CVE-2023-33481	RemoteClinic 2.0 GET Parameter patients/index.php start sql injection (Issue 25)	A vulnerability was found in RemoteClinic 2.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file patients/index.php of the component GET Parameter Handler. The manipulation of the argument start leads to sql injection. This vulnerability is handled as CVE-2023-33481. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-42284	Tyk Gateway 5.0.3 api_version sql injection	A vulnerability classified as critical has been found in Tyk Gateway 5.0.3. Affected is an unknown function. The manipulation of the argument api_version leads to sql injection. This vulnerability is traded as CVE-2023-42284. 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-2023-46677	Project Worlds Online Job Portal 1.0 sign-up.php txt_uname sql injection	A vulnerability was found in Project Worlds Online Job Portal 1.0. It has been declared as critical. This vulnerability affects unknown code of the file sign-up.php. The manipulation of the argument txt_uname leads to sql injection. This vulnerability was named CVE-2023-46677. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-46680	Project Worlds Online Job Portal 1.0 index.php	A vulnerability was found in Project Worlds Online Job Portal 1.0	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	txt_password sql injection	and classified as critical. Affected by this issue is some unknown functionality of the file index.php. The manipulation of the argument txt_password leads to sql injection. This vulnerability is handled as CVE-2023-46680. The attack may be launched remotely. There is no exploit available.		
CVE-2023-46679	Project Worlds Online Job Portal 1.0 index.php txt_uname_email sql injection	A vulnerability has been found in Project Worlds Online Job Portal 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file index.php. The manipulation of the argument txt_uname_email leads to sql injection. This vulnerability is known as CVE-2023-46679. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-46676	Project Worlds Online Job Portal 1.0 sign-up.php filename sql injection	A vulnerability was found in Project Worlds Online Job Portal 1.0. It has been classified as critical. This affects an unknown part of the file sign-up.php. The manipulation of the argument filename leads to sql injection. This vulnerability is uniquely identified as CVE-2023-46676. 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-2023-46796	Project Worlds Online Matrimonial Project 1.0 functions.php register month sql injection	A vulnerability was found in Project Worlds Online Matrimonial Project 1.0 and classified as critical. Affected by this issue is the function register of the file functions.php. The manipulation of the argument month leads to sql injection. This vulnerability is handled as CVE-2023-46796. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-46795	Project Worlds Online Matrimonial	A vulnerability has been found in Project	Protected by core rules	Detected by scanner as SQL

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Project 1.0 functions.php register gender sql injection	Worlds Online Matrimonial Project 1.0 and classified as critical. Affected by this vulnerability is the function register of the file functions.php. The manipulation of the argument gender leads to sql injection. This vulnerability is known as CVE-2023-46795. The attack can be launched remotely. There is no exploit available.		injection attack.
CVE-2023-46793	Project Worlds Online Matrimonial Project 1.0 functions.php register day sql injection	A vulnerability which was classified as critical has been found in Project Worlds Online Matrimonial Project 1.0. This issue affects the function register of the file functions.php. The manipulation of the argument day leads to sql injection. The identification of this vulnerability is CVE-2023-46793. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-46792	Project Worlds Online Matrimonial Project 1.0 functions.php multipart sql injection	A vulnerability classified as critical was found in Project Worlds Online Matrimonial Project 1.0. This vulnerability affects unknown code of the file functions.php. The manipulation of the argument multipart leads to sql injection. This vulnerability was named CVE-2023-46792. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-46800	Project Worlds Online Matrimonial Project 1.0 view_profile.php id sql injection	A vulnerability classified as critical has been found in Project Worlds Online Matrimonial Project 1.0. This affects an unknown part of the file view_profile.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-46800. 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-2023-46789	Project Worlds	A vulnerability	Protected by	Detected by

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Online Matrimonial Project 1.0 functions.php pic1 sql injection	classified as critical was found in Project Worlds Online Matrimonial Project 1.0. Affected by this vulnerability is an unknown functionality of the file functions.php. The manipulation of the argument pic1 leads to sql injection. This vulnerability is known as CVE-2023-46789. The attack can be launched remotely. There is no exploit available.	core rules	scanner as SQL injection attack.
CVE-2023-46678	Project Worlds Online Job Portal 1.0 sign-up.php txt_upass sql injection	A vulnerability was found in Project Worlds Online Job Portal 1.0. It has been rated as critical. This issue affects some unknown processing of the file sign-up.php. The manipulation of the argument txt_upass leads to sql injection. The identification of this vulnerability is CVE-2023-46678. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-46790	Project Worlds Online Matrimonial Project 1.0 functions.php pic2 sql injection	A vulnerability which was classified as critical has been found in Project Worlds Online Matrimonial Project 1.0. Affected by this issue is some unknown functionality of the file functions.php. The manipulation of the argument pic2 leads to sql injection. This vulnerability is handled as CVE-2023-46790. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-46787	Project Worlds Online Matrimonial Project 1.0 auth/auth.php username sql injection	A vulnerability was found in Project Worlds Online Matrimonial Project 1.0 and classified as critical. This issue affects some unknown processing of the file auth/auth.php. The manipulation of the argument username leads to sql injection. The identification of this vulnerability is CVE-2023-46787. The attack may be initiated	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. There is no exploit available.		
CVE-2023-46786	Project Worlds Online Matrimonial Project 1.0 auth/auth.php password sql injection	A vulnerability has been found in Project Worlds Online Matrimonial Project 1.0 and classified as critical. This vulnerability affects unknown code of the file auth/auth.php. The manipulation of the argument password leads to sql injection. This vulnerability was named CVE-2023-46786. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-46785	Project Worlds Online Matrimonial Project 1.0 partner_preference.php id sql injection	A vulnerability which was classified as critical was found in Project Worlds Online Matrimonial Project 1.0. This affects an unknown part of the file partner_preference.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-46785. 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-2023-46797	Project Worlds Online Matrimonial Project 1.0 functions.php register name sql injection	A vulnerability was found in Project Worlds Online Matrimonial Project 1.0. It has been classified as critical. Affected is the function register of the file functions.php. The manipulation of the argument name leads to sql injection. This vulnerability is traded as CVE-2023-46797. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-46794	Project Worlds Online Matrimonial Project 1.0 functions.php register email sql injection	A vulnerability which was classified as critical was found in Project Worlds Online Matrimonial Project 1.0. Affected is the function register of the file functions.php. The manipulation of the argument email leads to sql injection. This vulnerability is traded as CVE-2023-	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		46794. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2023-46799	Project Worlds Online Matrimonial Project 1.0 functions.php register year sql injection	A vulnerability was found in Project Worlds Online Matrimonial Project 1.0. It has been rated as critical. Affected by this issue is the function register of the file functions.php. The manipulation of the argument year leads to sql injection. This vulnerability is handled as CVE-2023-46799. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-46798	Project Worlds Online Matrimonial Project 1.0 functions.php register pass sql injection	A vulnerability was found in Project Worlds Online Matrimonial Project 1.0. It has been declared as critical. Affected by this vulnerability is the function register of the file functions.php. The manipulation of the argument pass leads to sql injection. This vulnerability is known as CVE-2023-46798. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-46788	Project Worlds Online Matrimonial Project 1.0 functions.php uploadphoto id sql injection	A vulnerability classified as critical has been found in Project Worlds Online Matrimonial Project 1.0. Affected is the function uploadphoto of the file functions.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-46788. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-6052	Tongda OA 2017 up to 11.9 delete.php DELETE_STR sql injection	A vulnerability classified as critical has been found in Tongda OA 2017 up to 11.9. Affected is an unknown function of the file general/system/censor_words/module/delete.php. The manipulation of the argument DELETE_STR 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 traded as CVE-2023-6052. Access to the local network is required for this attack. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way. It is recommended to upgrade the affected component.		
CVE-2023-6054	Tongda OA 2017 up to 11.9 lock.php TERM_ID_STR sql injection	A vulnerability which was classified as critical was found in Tongda OA 2017 up to 11.9. This affects an unknown part of the file general/wiki/cp/manage/lock.php. The manipulation of the argument TERM_ID_STR leads to sql injection. This vulnerability is uniquely identified as CVE-2023-6054. 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. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-6053	Tongda OA 2017 up to 11.9 delete.php DELETE_STR sql injection	A vulnerability which was classified as critical has been found in Tongda OA 2017 up to 11.9. Affected by this issue is some unknown functionality of the file general/system/censor_words/manage/delete.php. The manipulation of the argument DELETE_STR leads to sql injection. This vulnerability is handled as CVE-2023-6053. 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.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The vendor was contacted early about this disclosure but did not respond in any way. It is recommended to upgrade the affected component.		
CVE-2023-47128	Piccolo up to 1.1.0 Named Transaction sql injection (GHSA-xq59-7jf3-rjc6)	A vulnerability classified as critical has been found in Piccolo up to 1.1.0. This affects an unknown part of the component Named Transaction Handler. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-47128. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-6084	Tongda OA 2017 up to 11.9 delete.php VU_ID sql injection	A vulnerability was found in Tongda OA 2017 up to 11.9 and classified as critical. Affected by this issue is some unknown functionality of the file general/vehicle/checkup/delete.php. The manipulation of the argument VU_ID leads to sql injection. This vulnerability is handled as CVE-2023-6084. 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. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-46022	code-projects Blood Bank 1.0 delete.php bid sql injection	A vulnerability which was classified as critical has been found in code-projects Blood Bank 1.0. Affected by this issue is some unknown functionality of the file delete.php. The manipulation of the argument bid 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-2023-46022. The attack can only be done within the local network. There is no exploit available.		
CVE-2023-46025	PHPGurukul Teacher Subject Allocation Management System 1.0 teacher-info.php editid sql injection	A vulnerability was found in PHPGurukul Teacher Subject Allocation Management System 1.0. It has been classified as critical. This affects an unknown part of the file teacher-info.php. The manipulation of the argument editid leads to sql injection. This vulnerability is uniquely identified as CVE-2023-46025. 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-2023-46024	PHPGurukul Teacher Subject Allocation Management System 1.0 index.php searchdata sql injection	A vulnerability was found in PHPGurukul Teacher Subject Allocation Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file index.php. The manipulation of the argument searchdata leads to sql injection. The identification of this vulnerability is CVE-2023-46024. 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-2023-46581	Inventory Management 1.0 registration.php name/uname/email sql injection	A vulnerability was found in Inventory Management 1.0. It has been classified as critical. This affects an unknown part of the file registration.php. The manipulation of the argument name/uname/email leads to sql injection. This vulnerability is uniquely identified as CVE-2023-46581. Local access is required to approach this attack. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-46021	code-projects Blood Bank 1.0 cancel.php reqid sql injection	A vulnerability classified as critical has been found in code-projects Blood Bank 1.0. This affects an	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown part of the file cancel.php. The manipulation of the argument reqid leads to sql injection. This vulnerability is uniquely identified as CVE-2023-46021. Access to the local network is required for this attack to succeed. There is no exploit available.		
CVE-2023-46017	code-projects Blood Bank 1.0 receiverLogin.php rpassword sql injection	A vulnerability was found in code-projects Blood Bank 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file receiverLogin.php. The manipulation of the argument rpassword leads to sql injection. This vulnerability is known as CVE-2023-46017. 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-2023-46582	Inventory Management 1.0 deleteProduct.php id sql injection	A vulnerability was found in Inventory Management 1.0. It has been declared as critical. This vulnerability affects unknown code of the file deleteProduct.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-46582. Attacking locally is a requirement. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-46018	code-projects Blood Bank 1.0 receiverReg.php remail sql injection	A vulnerability was found in code-projects Blood Bank 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file receiverReg.php. The manipulation of the argument remail leads to sql injection. This vulnerability is handled as CVE-2023-46018. 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-2023-46014	code-projects Blood Bank 1.0	A vulnerability was found in code-projects	Protected by core rules	Detected by scanner as SQL

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	hospitalLogin.php hemail/hpassword sql injection	Blood Bank 1.0. It has been rated as critical. This issue affects some unknown processing of the file hospitalLogin.php. The manipulation of the argument hemail/hpassword leads to sql injection. The identification of this vulnerability is CVE-2023-46014. The attack needs to be done within the local network. There is no exploit available.		injection attack.
CVE-2023-47637	Pimcore Admin Grid Filter API getFilterConditionExt sql injection	A vulnerability has been found in Pimcore and classified as critical. Affected by this vulnerability is the function Multiselect::getFilterConditionExt of the component Admin Grid Filter API. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-47637. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2021-35437	lmxcms 1.4 TagsAction.class sql injection	A vulnerability which was classified as critical was found in lmxcms 1.4. This affects an unknown part of the file TagsAction.class. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2021-35437. 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-2023-48078	Simple CRUD Functionality 1.0 add.php title sql injection	A vulnerability was found in Simple CRUD Functionality 1.0. It has been classified as critical. Affected is an unknown function of the file add.php. The manipulation of the argument title leads to sql injection. This vulnerability is traded as CVE-2023-48078. 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. There is no exploit available.		
CVE-2023-5652	WP Hotel Booking Plugin up to 2.0.7 on WordPress admin_init sql injection	A vulnerability which was classified as critical has been found in WP Hotel Booking Plugin up to 2.0.7 on WordPress. This issue affects the function admin_init. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-5652. The attack needs to be initiated within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-5789	Dragon Path 707GR1 up to 20231022 Ping Diagnostics Host Address cross-site scripting	A vulnerability classified as problematic has been found in Dragon Path 707GR1 up to 20231022. Affected is an unknown function of the component Ping Diagnostics. The manipulation of the argument Host Address with the input >><img/src/onerroralert> leads to cross-site scripting. This vulnerability is traded as CVE-2023-5789. 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-2023-5793	flusity CMS Dashboard customblock.php loadCustomBlocCreateForm customblock_place cross-site scripting	A vulnerability was found in flusity CMS and classified as problematic. This issue affects the function loadCustomBlocCreateForm of the file /core/tools/customblock.php of the component Dashboard. The manipulation of the argument customblock_place leads to cross-site scripting. The identification of this vulnerability is CVE-2023-5793. The attack may be initiated remotely. Furthermore there is an exploit available. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-5791	SourceCodester Sticky Notes App 1.0 endpoint/add-note.php noteTitle/noteContent cross-site scripting	A vulnerability which was classified as problematic was found in SourceCodester Sticky Notes App 1.0. This affects an unknown part of the file endpoint/add-note.php. The manipulation of the argument noteTitle/noteContent leads to cross-site scripting.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is uniquely identified as CVE-2023-5791. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2023-45137	XWiki Platform Error Message cross-site scripting (GHSA-93gh-jgjj-r929)	A vulnerability which was classified as problematic has been found in XWiki Platform. This issue affects some unknown processing of the component Error Message Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-45137. 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-2023-43906	Xolo CMS 0.11 cross-site scripting	A vulnerability has been found in Xolo CMS 0.11 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-2023-43906. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-5810	flusity CMS core/tools/posts.php loadPostAddForm edit_post_id cross-site scripting	A vulnerability which was classified as problematic has been found in flusity CMS. This issue affects the function loadPostAddForm of the file core/tools/posts.php. The manipulation of the argument edit_post_id leads to cross-site scripting. The identification of this vulnerability is CVE-2023-5810. The attack may be initiated remotely. Furthermore there is an exploit available. This product takes the approach of rolling releases to provide continious delivery. Therefore version	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		details for affected and updated releases are not available. It is recommended to apply a patch to fix this issue.		
CVE-2023-5811	flusity CMS core/tools/posts.php loadPostAddForm menu_id cross-site scripting	A vulnerability which was classified as problematic was found in flusity CMS. Affected is the function loadPostAddForm of the file core/tools/posts.php. The manipulation of the argument menu_id leads to cross-site scripting. This vulnerability is traded as CVE-2023-5811. It is possible to launch the attack remotely. Furthermore there is an exploit available. Continious delivery with rolling releases is used by this product. Therefore no version details of affected nor updated releases are available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-46450	SourceCodester Free and Open Source Inventory Management System 1.0 Add Supplier cross-site scripting	A vulnerability has been found in SourceCodester Free and Open Source Inventory Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Add Supplier Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-46450. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-46583	PHPGurukul Nipah Virus Testing Management System 1.0 State cross-site scripting	A vulnerability has been found in PHPGurukul Nipah Virus Testing Management System 1.0 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument State leads to cross-site scripting. This vulnerability was named CVE-2023-	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		46583. The attack can be initiated remotely. There is no exploit available.		
CVE-2023-5774	Animated Counters Plugin up to 1.7 on WordPress Shortcode cross-site scripting	A vulnerability classified as problematic has been found in Animated Counters Plugin up to 1.7 on WordPress. This affects an unknown part of the component Shortcode Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-5774. 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-2023-46503	YXBOOKCMS 1.0.2 Reader Management cross-site scripting	A vulnerability which was classified as problematic has been found in YXBOOKCMS 1.0.2. This issue affects some unknown processing of the component Reader Management. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-46503. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-46505	FanCMS 1.0.0 demo.php content1 cross-site scripting	A vulnerability was found in FanCMS 1.0.0. It has been declared as problematic. This vulnerability affects unknown code of the file demo.php. The manipulation of the argument content1 leads to cross-site scripting. This vulnerability was named CVE-2023-46505. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-5817	Neon Text Plugin up to 1.1 on WordPress cross-site scripting	A vulnerability classified as problematic was found in Neon Text Plugin up to 1.1 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-5817. The attack can be	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		launched remotely. There is no exploit available.		
CVE-2023-46394	gougucms 4.08.18 /home/user/edit_submit headimgurl cross-site scripting	A vulnerability has been found in gougucms 4.08.18 and classified as problematic. This vulnerability affects unknown code of the file /home/user/edit_submit. The manipulation of the argument headimgurl leads to cross-site scripting. This vulnerability was named CVE-2023-46394. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-46504	YXBOOKCMS 1.0.2 Library Name cross-site scripting	A vulnerability classified as problematic has been found in YXBOOKCMS 1.0.2. This affects an unknown part of the component Library Name Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-46504. It is possible to launch the attack on the physical device. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-46491	ZenTao Biz up to 4.1.3 Version Library cross-site scripting	A vulnerability classified as problematic was found in ZenTao Biz up to 4.1.3. This vulnerability affects unknown code of the component Version Library. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-46491. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-46374	ZenTao Enterprise Edition up to 4.1.3 cross-site scripting	A vulnerability was found in ZenTao Enterprise Edition up to 4.1.3. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-46374. It is possible to	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		launch the attack remotely. There is no exploit available.		
CVE-2023-46467	juzawebCMS up to 3.4 Registration Page username cross-site scripting	A vulnerability which was classified as problematic was found in juzawebCMS up to 3.4. This affects an unknown part of the component Registration Page. The manipulation of the argument username leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-46467. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-34833	Vermeg AgileReporter 21.3 Analysis cross-site scripting	A vulnerability was found in Vermeg AgileReporter 21.3 and classified as problematic. This issue affects some unknown processing of the component Analysis. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-34833. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-5837	AlexanderLivanov FotosCMS2 up to 2.4.3 Cookie profile.php username cross-site scripting	A vulnerability classified as problematic was found in AlexanderLivanov FotosCMS2 up to 2.4.3. This vulnerability affects unknown code of the file profile.php of the component Cookie Handler. The manipulation of the argument username leads to cross-site scripting. This vulnerability was named CVE-2023-5837. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2022-34834	Vermeg AgileReporter 21.3 Add Comment cross-site scripting	A vulnerability classified as problematic was found in Vermeg AgileReporter 21.3. Affected by this vulnerability is an unknown functionality of the component Add Comment. The manipulation leads to cross-site scripting.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is known as CVE-2022-34834. The attack can be launched remotely. There is no exploit available.		
CVE-2023-46858	Moodle 4.3 index.php searchvalue cross-site scripting	A vulnerability was found in Moodle 4.3. It has been rated as problematic. This issue affects some unknown processing of the file /grade/report/grader/index.php. The manipulation of the argument searchvalue leads to cross-site scripting. The identification of this vulnerability is CVE-2023-46858. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-5566	Simple Shortcodes Plugin up to 1.0.20 on WordPress Shortcode cross-site scripting	A vulnerability was found in Simple Shortcodes Plugin up to 1.0.20 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-2023-5566. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-5335	Buzzsprout Podcasting Plugin up to 1.8.3 on WordPress Shortcode cross-site scripting	A vulnerability classified as problematic was found in Buzzsprout Podcasting Plugin up to 1.8.3 on WordPress. This vulnerability affects unknown code of the component Shortcode Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-5335. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-5842	Dolibarr up to 16.0.4 cross-site scripting	A vulnerability has been found in Dolibarr up to 16.0.4 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross-site scripting. This vulnerability was named CVE-2023-5842. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-5666	Accordion Plugin up to 2.6 on WordPress Shortcode cross-site scripting	A vulnerability which was classified as problematic was found in Accordion Plugin up to 2.6 on WordPress. Affected is an unknown function of the component Shortcode Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-5666. 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-2023-4250	EventPrime Plugin up to 3.1.x on WordPress cross-site scripting	A vulnerability was found in EventPrime Plugin up to 3.1.x on WordPress. 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-2023-4250. 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-2023-45671	blakeblackshear frigate up to 0.13.0-beta2 API Endpoint cross-site scripting (GHSA-jjxc-m35j-p56f)	A vulnerability which was classified as problematic was found in blakeblackshear frigate up to 0.13.0-beta2. This affects an unknown part of the component API Endpoint. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-45671. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component.		
CVE-2023-4390	Popup Box Plugin up to 3.7.1 on WordPress cross-site scripting	A vulnerability was found in Popup Box Plugin up to 3.7.1 on WordPress. 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-2023-4390. 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-2023-46040	GetSimpleCMS 3.4.0a components.php cross-site scripting	A vulnerability classified as problematic has been found in GetSimpleCMS 3.4.0a. This affects an unknown part of the file components.php. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-46040. 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-2023-5873	pimcore up to 11.0.x cross-site scripting	A vulnerability classified as problematic has been found in pimcore up to 11.0.x. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-5873. 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-2023-5867	thorsten phpmyfaq up to 3.2.1 cross-site scripting	A vulnerability was found in thorsten phpmyfaq up to 3.2.1 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-5867. The attack may be launched remotely. There is no exploit	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		available. It is recommended to upgrade the affected component.		
CVE-2023-5114	idbbee Plugin up to 1.0 on WordPress Shortcode cross-site scripting	A vulnerability was found in idbbee Plugin up to 1.0 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Shortcode Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-5114. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-5073	iframe Forms Plugin up to 1.0 on WordPress Shortcode cross-site scripting	A vulnerability was found in iframe Forms Plugin up to 1.0 on WordPress. It has been classified as problematic. Affected is an unknown function of the component Shortcode Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-5073. 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-2023-46451	Best Courier Management System 1.0 username cross-site scripting	A vulnerability has been found in Best Courier Management System 1.0 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument username leads to cross-site scripting. This vulnerability was named CVE-2023-46451. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-5861	microweber up to 1.x cross-site scripting	A vulnerability which was classified as problematic was found in microweber up to 1.x. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		uniquely identified as CVE-2023-5861. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-46478	minCal 1.0.0 customer_data cross-site scripting	A vulnerability was found in minCal 1.0.0. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument customer_data leads to cross-site scripting. This vulnerability was named CVE-2023-46478. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-5864	thorsten phpmyfaq up to 3.2.0 cross-site scripting	A vulnerability has been found in thorsten phpmyfaq up to 3.2.0 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-5864. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-5863	thorsten phpmyfaq up to 3.2.1 cross-site scripting	A vulnerability which was classified as problematic was found in thorsten phpmyfaq up to 3.2.1. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-5863. 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-2023-4823	WP Meta and Date Remover Plugin up to 2.1.x on WordPress AJAX Endpoint cross-site scripting	A vulnerability classified as problematic was found in WP Meta and Date Remover Plugin up to 2.1.x on WordPress.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Affected by this vulnerability is an unknown functionality of the component AJAX Endpoint. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-4823. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-5238	EventPrime Plugin prior 3.2.0 on WordPress cross-site scripting	A vulnerability was found in EventPrime Plugin 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-2023-5238. 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-2023-5229	E2Pdf Plugin prior 1.20.20 on WordPress Setting cross-site scripting	A vulnerability classified as problematic has been found in E2Pdf Plugin on WordPress. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-5229. 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-2023-5307	Photos and Files Contest Gallery Plugin prior 21.2.8.1 on WordPress cross-site scripting	A vulnerability classified as problematic was found in Photos and Files Contest Gallery Plugin on WordPress. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-5307.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-5237	Memberlite Shortcodes Plugin prior 1.3.9 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in Memberlite Shortcodes Plugin on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-5237. 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-2023-1716	Bitrix24 up to 22.0.300 Invoice Edit Page cross-site scripting	A vulnerability was found in Bitrix24 up to 22.0.300. It has been rated as problematic. This issue affects some unknown processing of the component Invoice Edit Page. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-1716. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-46911	Jspxcms 10.2.0 choose_style_tree.do cross-site scripting	A vulnerability has been found in Jspxcms 10.2.0 and classified as problematic. This vulnerability affects unknown code of the file choose_style_tree.do. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-46911. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-1717	Bitrix24 up to 22.0.300 script.js cross-site scripting	A vulnerability has been found in Bitrix24 up to 22.0.300 and classified as problematic. Affected by this vulnerability is an unknown	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		functionality of the file bitrix/templates/bitrix24/components/bitrix/menu/left_vertical/script.js. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-1717. The attack can be launched remotely. There is no exploit available.		
CVE-2023-1715	Bitrix24 up to 22.0.300 mb_strpos cross-site scripting	A vulnerability was found in Bitrix24 up to 22.0.300. It has been rated as problematic. Affected by this issue is the function mb_strpos. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-1715. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-47099	Virtualmin 7.7 Create Virtual Server cross-site scripting	A vulnerability was found in Virtualmin 7.7. It has been classified as problematic. Affected is an unknown function of the component Create Virtual Server. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-47099. 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-2023-44485	Project Worlds Online Blood Donation Management System 1.0 users/register.php lastName cross-site scripting	A vulnerability was found in Project Worlds Online Blood Donation Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file users/register.php. The manipulation of the argument lastName leads to cross-site scripting. This vulnerability is known as CVE-2023-44485. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-5895	pkp-lib prior 3.3.0-16 cross-site scripting	A vulnerability has been found in pkp-lib and classified as problematic. Affected	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-5895. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-47094	Virtualmin 7.7 Account Plans Tab Plan Name cross-site scripting	A vulnerability was found in Virtualmin 7.7 and classified as problematic. Affected by this issue is some unknown functionality of the component Account Plans Tab. The manipulation of the argument Plan Name leads to cross-site scripting. This vulnerability is handled as CVE-2023-47094. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-5892	pkp-lib prior 3.3.0-16 cross-site scripting	A vulnerability which was classified as problematic has been found in pkp-lib. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-5892. 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-2023-5894	pkp ojs prior 3.3.0-16 cross-site scripting	A vulnerability has been found in pkp ojs and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-5894. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component.		
CVE-2023-47096	Virtualmin 7.7 Cloudmin Services Client cross-site scripting	A vulnerability which was classified as problematic was found in Virtualmin 7.7. This affects an unknown part of the component Cloudmin Services Client. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-47096. 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-2023-46378	Num-Nine MiniCMS 1.1.1 String /mc-admin/conf.php cross-site scripting	A vulnerability classified as problematic was found in Num-Nine MiniCMS 1.1.1. Affected by this vulnerability is an unknown functionality of the file /mc-admin/conf.php of the component String Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-46378. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-5890	pkp-lib prior 3.3.0-16 cross-site scripting	A vulnerability classified as problematic has been found in pkp-lib. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-5890. 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-2023-44486	Project Worlds Online Blood Donation Management System 1.0 users/register.php address cross-site scripting	A vulnerability was found in Project Worlds Online Blood Donation Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file users/register.php. The manipulation of the argument address leads to cross-site scripting.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The identification of this vulnerability is CVE-2023-44486. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-47098	Virtualmin 7.7 Create Extra Administrator Tab Real name cross-site scripting	A vulnerability was found in Virtualmin 7.7. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Create Extra Administrator Tab. The manipulation of the argument Real name leads to cross-site scripting. This vulnerability is handled as CVE-2023-47098. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-44484	Project Worlds Online Blood Donation Management System 1.0 users/register.php firstName cross-site scripting	A vulnerability was found in Project Worlds Online Blood Donation Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file users/register.php. The manipulation of the argument firstName leads to cross-site scripting. This vulnerability is traded as CVE-2023-44484. 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-2023-5306	Project Worlds Online Blood Donation Management System 1.0 users/register.php city cross-site scripting	A vulnerability has been found in Project Worlds Online Blood Donation Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file users/register.php. The manipulation of the argument city leads to cross-site scripting. This vulnerability was named CVE-2023-5306. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-47097	Virtualmin 7.7 System Settings cross-site scripting	A vulnerability was found in Virtualmin 7.7 and classified as problematic. This issue affects 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
		processing of the component System Settings. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-47097. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-5903	pkp-lib prior 3.3.0-16 cross-site scripting	A vulnerability classified as problematic has been found in pkp-lib. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-5903. 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-2023-47095	Virtualmin 7.7 Custom Fields cross-site scripting	A vulnerability which was classified as problematic has been found in Virtualmin 7.7. Affected by this issue is some unknown functionality of the component Custom Fields Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-47095. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-5896	pkp-lib prior 3.4.0-4 cross-site scripting	A vulnerability was found in pkp-lib and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-5896. 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-2023-5904	pkp-lib prior 3.3.0-16 cross-site scripting	A vulnerability classified as problematic was found in pkp-lib. Affected by	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-5904. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-5891	pkp-lib prior 3.3.0-16 cross-site scripting	A vulnerability classified as problematic was found in pkp-lib. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-5891. 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-2023-5930	Campcodes Simple Student Information System 1.0 manage_academic.php student_id cross-site scripting	A vulnerability was found in Campcodes Simple Student Information System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/students/manage_academic.php. The manipulation of the argument student_id leads to cross-site scripting. This vulnerability was named CVE-2023-5930. 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-2023-43193	Submitty prior 22.06.00 Link cross-site scripting	A vulnerability classified as problematic was found in Submitty. Affected by this vulnerability is an unknown functionality of the component Link Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-43193. The attack can	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-46448	dmpop Mejiro Image Metadata cross-site scripting	A vulnerability was found in dmpop Mejiro and classified as problematic. Affected by this issue is some unknown functionality of the component Image Metadata Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-46448. The attack may be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-44954	BigTree CMS 4.5.7 Developer Settings ID cross-site scripting	A vulnerability classified as problematic was found in BigTree CMS 4.5.7. This vulnerability affects unknown code of the component Developer Settings. The manipulation of the argument ID leads to cross-site scripting. This vulnerability was named CVE-2023-44954. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-46925	Reportico 7.1.21 cross-site scripting (Issue 47)	A vulnerability was found in Reportico 7.1.21. 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-2023-46925. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-46475	ZenTao 18.3 Project name cross-site scripting	A vulnerability has been found in ZenTao 18.3 and classified as problematic. This vulnerability affects unknown code of the component Project Handler. The manipulation of the	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument name leads to cross-site scripting. This vulnerability was named CVE-2023-46475. The attack can be initiated remotely. There is no exploit available.		
CVE-2023-45360	MediaWiki prior 1.35.12/1.39.5/1.40.1 i18n Message MediaWiki:Youhavenewmessagesfromusers youhavenewmessagesmanyusers/youhavenewmessages cross-site scripting	A vulnerability has been found in MediaWiki and classified as problematic. Affected by this vulnerability is the function youhavenewmessagesmanyusers/youhavenewmessages of the file MediaWiki:Youhavenewmessagesfromusers of the component i18n Message Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-45360. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-5707	SEO Slider Plugin up to 1.1.0 on WordPress Shortcode cross-site scripting	A vulnerability which was classified as problematic was found in SEO Slider Plugin up to 1.1.0 on WordPress. Affected is an unknown function of the component Shortcode Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-5707. 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-2023-5354	Awesome Support Plugin up to 6.1.4 on WordPress cross-site scripting	A vulnerability was found in Awesome Support Plugin up to 6.1.4 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-2023-5354. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		It is recommended to upgrade the affected component.		
CVE-2023-5669	Featured Image Caption Plugin up to 0.8.10 on WordPress Shortcode cross-site scripting	A vulnerability was found in Featured Image Caption Plugin up to 0.8.10 on WordPress. It has been rated 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-2023-5669. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-46744	Squidex prior 7.9.0 cross-site scripting	A vulnerability classified as problematic was found in Squidex. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-46744. 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-2023-41425	Wonder CMS up to 3.4.2 installModule cross-site scripting	A vulnerability was found in Wonder CMS up to 3.4.2. It has been classified as problematic. Affected is an unknown function of the component installModule. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-41425. 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-2023-5530	Ninja Forms Contact Form Plugin up to 3.6.33 on WordPress Label Field cross-site scripting	A vulnerability was found in Ninja Forms Contact Form Plugin up to 3.6.33 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Label Field Handler. The manipulation leads to	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross-site scripting. This vulnerability is handled as CVE-2023-5530. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-46998	BootBox.js up to 6.0 alert/confirm/prompt cross-site scripting (Issue 661)	A vulnerability has been found in BootBox.js up to 6.0 and classified as problematic. This vulnerability affects the function alert/confirm/prompt. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-46998. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-4810	Responsive Pricing Table Plugin up to 5.1.7 on WordPress Setting cross-site scripting	A vulnerability was found in Responsive Pricing Table Plugin up to 5.1.7 on WordPress and classified as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-4810. 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-2023-5661	Social Feed Plugin up to 1.5.4.6 on WordPress Shortcode cross-site scripting	A vulnerability was found in Social Feed Plugin up to 1.5.4.6 on WordPress and classified as problematic. This issue affects some unknown processing of the component Shortcode Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-5661. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-5228	User Registration	A vulnerability was	Protected by	Detected by

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Plugin prior 3.0.4.2 on WordPress Setting cross-site scripting	found in User Registration Plugin on WordPress. It has been classified as problematic. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-5228. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	core rules	scanner as cross-site scripting attack.
CVE-2023-5181	WP Discord Invite Plugin up to 2.5.1 on WordPress Setting cross-site scripting	A vulnerability which was classified as problematic was found in WP Discord Invite Plugin up to 2.5.1 on WordPress. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-5181. 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-2023-5660	SendPress Newsletters Plugin up to 1.22.3.31 on WordPress Shortcode cross-site scripting	A vulnerability classified as problematic was found in SendPress Newsletters Plugin up to 1.22.3.31 on WordPress. This vulnerability affects unknown code of the component Shortcode Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-5660. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-46732	XWiki Platform up to 14.10.13/15.5.0/15.6 Parameter rev cross-site scripting (GHSA-j9rc-w3wv-fv62)	A vulnerability was found in XWiki Platform up to 14.10.13/15.5.0/15.6 and classified as problematic. Affected by this issue is some unknown functionality of the component	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Parameter Handler. The manipulation of the argument rev leads to cross-site scripting. This vulnerability is handled as CVE-2023-46732. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-45556	MyBB 1.8.33 Theme Management Theme Name cross-site scripting (GHSA-4xqm-3cm2-5xgf)	A vulnerability was found in MyBB 1.8.33. It has been rated as problematic. This issue affects some unknown processing of the component Theme Management. The manipulation of the argument Theme Name leads to cross-site scripting. The identification of this vulnerability is CVE-2023-45556. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-46252	Squidex prior 7.9.0 editor-sdk.js onValueChanged cross-site scripting (GHSA-7q4f-fprr-5jw8)	A vulnerability classified as problematic has been found in Squidex. This affects the function onValueChanged of the file editor-sdk.js. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-46252. 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-2023-5605	URL Shortify Plugin up to 1.7.8 on WordPress Setting cross-site scripting	A vulnerability classified as problematic has been found in URL Shortify Plugin up to 1.7.8 on WordPress. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-5605. 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-2023-5703	koanleeroy Gift Up Gift Cards Plugin up to 2.20.1 on WordPress Shortcode giftup cross-site scripting	A vulnerability which was classified as problematic was found in koanleeroy Gift Up Gift Cards Plugin up to 2.20.1 on WordPress. This affects the function giftup of the component Shortcode Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-5703. 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-2023-46483	timetec AWDMS 2.0 remark cross-site scripting	A vulnerability has been found in timetec AWDMS 2.0 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument remark leads to cross-site scripting. This vulnerability was named CVE-2023-46483. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-45885	NASA Openmct up to 3.1.0 flexibleLayout Plugin cross-site scripting	A vulnerability which was classified as problematic has been found in NASA Openmct up to 3.1.0. This issue affects some unknown processing of the component flexibleLayout Plugin. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-45885. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-48068	DedeCMS 6.2 spec_add.php cross-site scripting	A vulnerability has been found in DedeCMS 6.2 and classified as problematic. This vulnerability affects unknown code of the file spec_add.php. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-48068. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-4603	Star CloudPRNT for WooCommerce Plugin up to 2.0.3 on WordPress cross-site scripting	A vulnerability was found in Star CloudPRNT for WooCommerce Plugin up to 2.0.3 on WordPress and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-4603. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-46026	PHPGurukul Teacher Subject Allocation Management System 1.0 profile.php email cross-site scripting	A vulnerability which was classified as problematic was found in PHPGurukul Teacher Subject Allocation Management System 1.0. This affects an unknown part of the file profile.php. The manipulation of the argument email leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-46026. 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-2023-45881	GibbonEdu Gibbon up to 25.0.0 File Upload resources_addQuick_ajaxProcess.php imageAsLinks cross-site scripting (usd-2023-0024)	A vulnerability which was classified as problematic has been found in GibbonEdu Gibbon up to 25.0.0. This issue affects some unknown processing of the file /modules/Planner/resources_addQuick_ajaxProcess.php of the component File Upload Handler. The manipulation of the argument imageAsLinks leads to cross-site scripting. The identification of this vulnerability is CVE-2023-45881. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-46019	code-projects Blood Bank 1.0 abs.php error cross-site scripting	A vulnerability classified as problematic was found in code-projects Blood Bank 1.0. This vulnerability affects unknown code of the file abs.php. The manipulation of the argument error leads	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to cross-site scripting. This vulnerability was named CVE-2023-46019. The attack can be initiated remotely. There is no exploit available.		
CVE-2023-46020	code-projects Blood Bank 1.0 updateprofile.php rename/remail/rphone/rcity cross-site scripting	A vulnerability which was classified as problematic has been found in code-projects Blood Bank 1.0. This issue affects some unknown processing of the file updateprofile.php. The manipulation of the argument rename/remail/rphone/rcity leads to cross-site scripting. The identification of this vulnerability is CVE-2023-46020. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-46016	code-projects Blood Bank 1.0 abs.php search cross-site scripting	A vulnerability has been found in code-projects Blood Bank 1.0 and classified as problematic. This vulnerability affects unknown code of the file abs.php. The manipulation of the argument search leads to cross-site scripting. This vulnerability was named CVE-2023-46016. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-46015	code-projects Blood Bank 1.0 index.php msg cross-site scripting	A vulnerability which was classified as problematic was found in code-projects Blood Bank 1.0. This affects an unknown part of the file index.php. The manipulation of the argument msg leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-46015. 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-2023-42327	Netgate pfSense 2.7.0 URL getserviceproviders.php cross-site scripting	A vulnerability classified as problematic was found in Netgate pfSense 2.7.0. Affected by this vulnerability is an unknown functionality of the file	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		getserviceproviders.php of the component URL Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-42327. The attack can be launched remotely. There is no exploit available.		
CVE-2023-46580	Inventory Management 1.0 editProduct.php pname cross-site scripting	A vulnerability was found in Inventory Management 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file editProduct.php. The manipulation of the argument pname leads to cross-site scripting. This vulnerability is handled as CVE-2023-46580. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-31754	Optimizely CMS up to 12.15.x Admin Panel cross-site scripting	A vulnerability was found in Optimizely CMS up to 12.15.x. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Admin Panel. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-31754. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-42325	Netgate pfSense 2.7.0 URL status_logs_filter_dynamic.php cross-site scripting	A vulnerability which was classified as problematic has been found in Netgate pfSense 2.7.0. Affected by this issue is some unknown functionality of the file status_logs_filter_dynamic.php of the component URL Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-42325. The attack may	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		be launched remotely. There is no exploit available.		
CVE-2023-45879	GibbonEdu Gibbon 25.0.0 Messager Component cross-site scripting (usd-2023-0019)	A vulnerability was found in GibbonEdu Gibbon 25.0.0. It has been classified as problematic. Affected is an unknown function of the component Messager Component. The manipulation leads to basic cross-site scripting. This vulnerability is traded as CVE-2023-45879. 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-2023-48088	xxl-job-admin 2.4.0 logDetailPage cross-site scripting (Issue 3329)	A vulnerability classified as problematic was found in xxl-job-admin 2.4.0. This vulnerability affects unknown code of the file /xxl-job-admin/joblog/logDetailPage. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-48088. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-4602	Namaste LMS Plugin up to 2.6.1.1 on WordPress cross-site scripting	A vulnerability has been found in Namaste LMS Plugin up to 2.6.1.1 on WordPress 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-2023-4602. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-41597	EyouCms 1.6.2 twitter.php cross-site scripting	A vulnerability which was classified as problematic has been found in EyouCms 1.6.2. This issue affects some unknown processing of the file /admin/twitter.phpactive_t. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-41597. The	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack may be initiated remotely. There is no exploit available.		
CVE-2023-48200	Grocy 4.0.3 Equipment Description /equipment/ cross-site scripting	A vulnerability was found in Grocy 4.0.3. It has been rated as problematic. This issue affects some unknown processing of the file /equipment/ of the component Equipment Description Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-48200. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-48197	Grocy 4.0.3 manageapikeys cross-site scripting	A vulnerability has been found in Grocy 4.0.3 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component manageapikeys. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-48197. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-48198	Grocy 4.0.3 Product Description api/stock/products cross-site scripting	A vulnerability which was classified as problematic has been found in Grocy 4.0.3. This issue affects some unknown processing of the file api/stock/products of the component Product Description Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-48198. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2020-11448	Bell HomeHub 3000 SG48222070 Login Page email cross-site scripting	A vulnerability was found in Bell HomeHub 3000 SG48222070. It has been declared as problematic. This vulnerability affects unknown code of the component Login Page. The manipulation of the argument email leads to cross-site scripting.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability was named CVE-2020-11448. The attack can be initiated remotely. There is no exploit available.		
CVE-2023-40813	OpenCRX 5.2.0 Activity Saved Search Creation cross-site scripting	A vulnerability which was classified as problematic was found in OpenCRX 5.2.0. Affected is an unknown function of the component Activity Saved Search Creation. The manipulation leads to basic cross-site scripting. This vulnerability is traded as CVE-2023-40813. It is possible to launch the attack remotely. Further more there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-40810	OpenCRX 5.2.0 Product Name cross-site scripting	A vulnerability classified as problematic was found in OpenCRX 5.2.0. This vulnerability affects unknown code. The manipulation of the argument Product Name leads to basic cross-site scripting. This vulnerability was named CVE-2023-40810. 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-2023-40814	OpenCRX 5.2.0 Accounts Name cross-site scripting	A vulnerability has been found in OpenCRX 5.2.0 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument Accounts Name leads to basic cross-site scripting. This vulnerability is known as CVE-2023-40814. 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-2023-44796	LimeSurvey prior 6.2.9-230925 _generaloptions_panel.php cross-site scripting	A vulnerability was found in LimeSurvey. It has been rated as problematic. Affected by this issue is some unknown functionality of the file _generaloptions_panel.php. The manipulation leads to cross-site scripting.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is handled as CVE-2023-44796. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-40816	OpenCRX 5.2.0 Activity Milestone Name cross-site scripting	A vulnerability was found in OpenCRX 5.2.0. It has been classified as problematic. This affects an unknown part. The manipulation of the argument Activity Milestone Name leads to basic cross-site scripting. This vulnerability is uniquely identified as CVE-2023-40816. 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-2023-40817	OpenCRX 5.2.0 Product Configuration Name cross-site scripting	A vulnerability was found in OpenCRX 5.2.0. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument Product Configuration Name leads to basic cross-site scripting. This vulnerability was named CVE-2023-40817. 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-2023-40812	OpenCRX 5.2.0 Accounts Group Name cross-site scripting	A vulnerability which was classified as problematic has been found in OpenCRX 5.2.0. This issue affects some unknown processing. The manipulation of the argument Accounts Group Name leads to basic cross-site scripting. The identification of this vulnerability is CVE-2023-40812. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-40815	OpenCRX 5.2.0 Category Creation Name cross-site	A vulnerability was found in OpenCRX 5.2.0 and classified as	Protected by core rules	Detected by scanner as cross-site

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	scripting	problematic. Affected by this issue is some unknown functionality. The manipulation of the argument Category Creation Name leads to basic cross-site scripting. This vulnerability is handled as CVE-2023-40815. The attack may be launched remotely. Furthermore there is an exploit available.		scripting attack.
CVE-2023-40809	OpenCRX 5.2.0 Activity Search Criteria-Activity Number cross-site scripting	A vulnerability classified as problematic has been found in OpenCRX 5.2.0. This affects an unknown part of the component Activity Search Criteria-Activity Number. The manipulation leads to basic cross-site scripting. This vulnerability is uniquely identified as CVE-2023-40809. 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-2023-5343	Popup Box Plugin up to 3.7.8 on WordPress Setting cross-site scripting	A vulnerability classified as problematic has been found in Popup Box Plugin up to 3.7.8 on WordPress. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-5343. 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-2023-5119	Forminator Plugin up to 1.26.x on WordPress Setting redirect-url cross-site scripting	A vulnerability classified as problematic was found in Forminator Plugin up to 1.26.x on WordPress. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation of the argument redirect-url leads to cross-site scripting.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is known as CVE-2023-5119. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-48300	epiphyt embed-privacy Plugin up to 1.8.0 on WordPress Shortcode embed_privacy_opt_out cross-site scripting (ID 199)	A vulnerability was found in epiphyt embed-privacy Plugin up to 1.8.0 on WordPress. It has been rated as problematic. Affected by this issue is the function embed_privacy_opt_out of the component Shortcode Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-48300. 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-2023-46935	EyouCMS 1.6.4 cross-site scripting	A vulnerability was found in EyouCMS 1.6.4. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-46935. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.

HTTP Request Smuggling Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-46137	Twisted up to 23.9.x HTTP Request request smuggling (GHSA-xc8x-vp79-p3wm)	A vulnerability was found in Twisted up to 23.9.x. It has been declared as problematic. This vulnerability affects unknown code of the component HTTP Request Handler. The manipulation leads to http request smuggling. This vulnerability was named CVE-2023-46137. 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 http request smuggling attack.
CVE-2023-4767	Zoho ManageEngine Desktop Central 9.1.0 HTTP Response InvSWMetering.csv fileName crlf injection	A vulnerability was found in Zoho ManageEngine Desktop Central 9.1.0 and classified as problematic. This issue affects some unknown processing of the file /STATE_ID/1613157927228/InvSWMetering.csv of the component HTTP Response Handler. The manipulation of the argument fileName leads to crlf injection. The identification of this vulnerability is CVE-2023-4767. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as http request smuggling attack.
CVE-2023-4768	Zoho ManageEngine Desktop Central 9.1.0 HTTP Response InvSWMetering.pdf fileName crlf injection	A vulnerability was found in Zoho ManageEngine Desktop Central 9.1.0. It has been classified as problematic. Affected is an unknown function of the file /STATE_ID/1613157927228/InvSWMetering.pdf of the component HTTP Response Handler. The manipulation of the argument fileName leads to crlf injection. This vulnerability is traded as CVE-2023-	Protected by core rules	Detected by scanner as http request smuggling attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		4768. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2023-47627	aio-libs aiohttp up to 3.8.5 HTTP Parser request smuggling	A vulnerability was found in aio-libs aiohttp up to 3.8.5. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component HTTP Parser. The manipulation leads to http request smuggling. This vulnerability is known as CVE-2023-47627. 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 http request smuggling attack.

XML External Entity Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-34832	Vermeg AgileReporter 21.3 Analysis xml external entity reference	A vulnerability which was classified as problematic has been found in Vermeg AgileReporter 21.3. Affected by this issue is some unknown functionality of the component Analysis. The manipulation leads to xml external entity reference. This vulnerability is handled as CVE-2022-34832. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as XML external entity attack.

Indusface is a leading application security SaaS company that secures critical Web, Mobile & API applications of 5000+ global customers using its award-winning fully managed platform that integrates a web application scanner, web application firewall, DDoS &, BOT Mitigation, CDN, and threat intelligence engine. The company has been funded by Tata Capital Growth Fund, is Great Place to Work certified, mentioned by analysts like Gartner, Forrester, etc. in their reports, and has been the recipient of many awards such as the Economic Times Top 25, NASSCOM DSCI Top Security Company, Deloitte Asia Top 100, and several other such prestigious recognitions.

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

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