INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

April 2024

The total zero-day vulnerabilities count for April month: 260

Command Injection	CSRF	Local File Inclusion	SQLi	Malicious File Upload	Cross-site Scripting
12	17	9	112	10	100

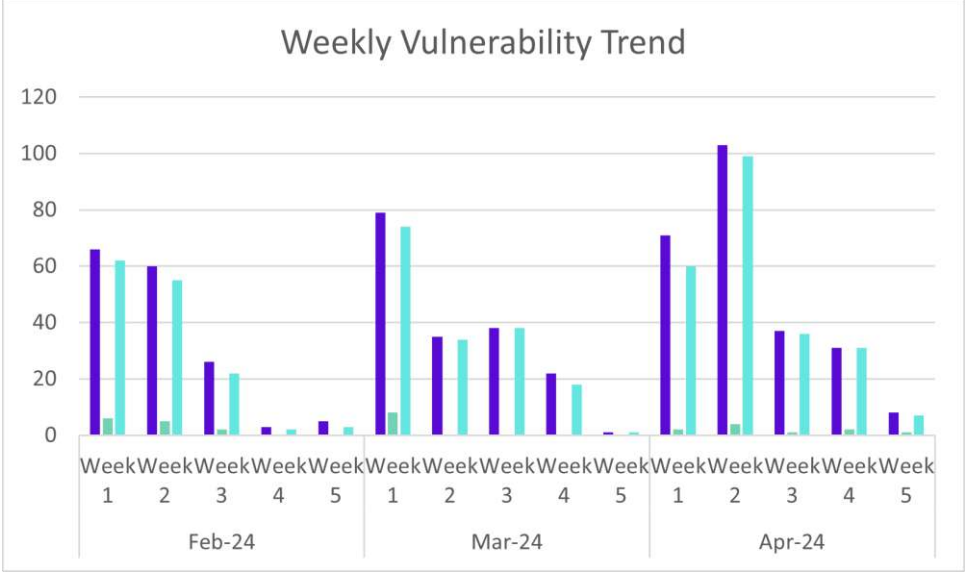
Zero-day vulnerabilities protected through core rules	250
Zero-day vulnerabilities protected through custom rules	10
Zero-day vulnerabilities for which protection cannot be done	0
Zero-day vulnerabilities found by Indusface WAS	233

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

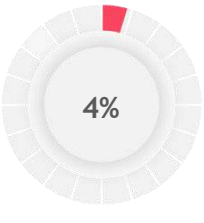
Vulnerability Trend:

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

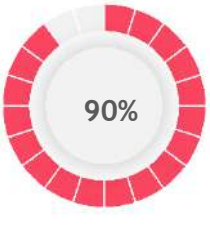
Weekly Vulnerability Trend



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

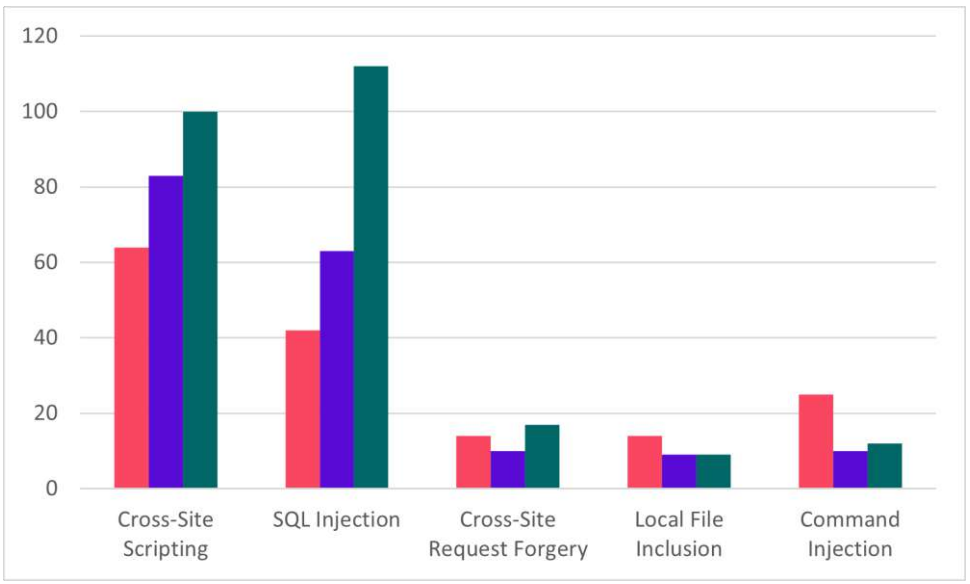


of the zero-day vulnerabilities were protected by the custom rules in the last month



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-2024-2897	Tenda AC7 15.03.06.44 /goform/WriteFacMac formWriteFacMac mac os command injection	A vulnerability classified as critical has been found in Tenda AC7 15.03.06.44. Affected is the function formWriteFacMac of the file /goform/WriteFacMac. The manipulation of the argument mac leads to os command injection. This vulnerability is traded as CVE-2024-2897. It is possible to launch the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-3009	Tenda FH1205 2.0.0.7(775) /goform/WriteFacMac formWriteFacMac mac command injection	A vulnerability has been found in Tenda FH1205 2.0.0.7 and classified as critical. Affected by this vulnerability is the function formWriteFacMac of the file /goform/WriteFacMac. The manipulation of the argument mac leads to command injection.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is known as CVE-2024-3009. 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.		
CVE-2024-1540	gradio-app gradio CI command injection	A vulnerability classified as critical has been found in gradio-app gradio. This affects an unknown part of the component CI. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2024-1540. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y
CVE-2024-30645	Tenda AC15V1.0 15.03.20_multi /goform/setUsbUnload doSystemCmd deviceName command injection	A vulnerability which was classified as critical was found in Tenda AC15V1.0 15.03.20_multi. Affected is the function doSystemCmd of the file /goform/setUsbUnload. The manipulation of the argument deviceName leads to command injection. This vulnerability is traded as CVE-2024-30645. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3273	D-Link DNS-320L/DNS-325/DNS-327L/DNS-340L up to 20240403 HTTP GET Request /cgi-bin/nas_sharing.cgi system command injection	A vulnerability which was classified as critical was found in D-Link DNS-320L DNS-325 DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. This vulnerability is traded as CVE-2024-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		3273. It is possible to launch the attack remotely. Furthermore there is an exploit available. Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. It is recommended to replace the affected component with an alternative.		
CVE-2024-30565	SeaCMS 12.9 /admin_notify.php code injection	A vulnerability has been found in SeaCMS 12.9 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin_notify.php. The manipulation leads to code injection. This vulnerability is known as CVE-2024-30565. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-30891	Tenda AC18 15.03.05.05 /goform/exeCommand cmdinput command injection	A vulnerability was found in Tenda AC18 15.03.05.05. It has been rated as critical. Affected by this issue is some unknown functionality of the file /goform/exeCommand. The manipulation of the argument cmdinput leads to command injection. This vulnerability is handled as CVE-2024-30891. The attack can only be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-3346	Byzro Smart S80 up to 20240328 /log/webmailattach.php mail_file_path os command injection	A vulnerability was found in Byzro Smart S80 up to 20240328. It has been declared as critical. This vulnerability affects unknown code of the file /log/webmailattach.php. The manipulation of the argument mail_file_path leads to os command injection. This vulnerability was named CVE-2024-3346.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The attack can be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-30665	ScriROS Melodic Morenia os command injection	A vulnerability which was classified as critical has been found in ScriROS Melodic Morenia. This issue affects some unknown processing. The manipulation leads to os command injection. The identification of this vulnerability is CVE-2024-30665. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-29269	Telesquare TLR-2005Ksh 1.0.0/1.1.4 Cmd command injection	A vulnerability classified as critical has been found in Telesquare TLR-2005Ksh 1.0.0/1.1.4. This affects an unknown part. The manipulation of the argument Cmd leads to command injection. This vulnerability is uniquely identified as CVE-2024-29269. Access to the local network is required for this attack to succeed. There is no exploit available.	Patched by core rule	Y
CVE-2024-3400	Palo Alto Networks PAN-OS GlobalProtect command injection	A vulnerability which was classified as very critical was found in Palo Alto Networks PAN-OS. This affects an unknown part of the component GlobalProtect. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2024-3400. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y
CVE-2024-32314	Tenda AC500 2.0.1.9(1307) formexeCommand cmdinput command	A vulnerability which was classified as critical was found in Tenda AC500 2.0.1.9. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	affects the function formexeCommand. The manipulation of the argument cmdinput leads to command injection. This vulnerability is uniquely identified as CVE-2024-32314. It is possible to initiate the attack remotely. There is no exploit available.		

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-29684	DedeCMS 5.7 makehtml_homepage.php cross-site request forgery	A vulnerability classified as problematic has been found in DedeCMS 5.7. Affected is an unknown function of the file /src/dede/makehtml_homepage.php. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-29684. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-2911	Tianjin PubliCMS 4.0.202302.e cross-site request forgery	A vulnerability which was classified as problematic was found in Tianjin PubliCMS 4.0.202302.e. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2024-2911. It is possible to initiate the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	N
CVE-2024-3089	PHPGurukul Emergency Ambulance Hiring Portal 1.0 Manage Ambulance Page manage-ambulance.php del cross-site request forgery	A vulnerability has been found in PHPGurukul Emergency Ambulance Hiring Portal 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/manage-ambulance.php of the component Manage Ambulance Page. The manipulation of the argument del leads to cross-site request forgery. This vulnerability was named CVE-2024-3089. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	N
CVE-2024-3147	DedeCMS 5.7 makehtml_map.php cross-site request forgery	A vulnerability classified as problematic was found in DedeCMS 5.7. This vulnerability affects unknown code of the file	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/src/dede/makehtml_map.php. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2024-3147. The attack can be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-3142	Clavister E10/E80 up to 20240323 Setting cross-site request forgery	A vulnerability was found in Clavister E10 and E80 up to 20240323 and classified as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-3142. 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.	Patched by core rule	N
CVE-2024-3146	DedeCMS 5.7 makehtml_rss_action.php cross-site request forgery	A vulnerability classified as problematic has been found in DedeCMS 5.7. This affects an unknown part of the file /src/dede/makehtml_rss_action.php. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2024-3146. It is possible to initiate the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	N
CVE-2024-3144	DedeCMS 5.7 makehtml_spec.php cross-site request forgery	A vulnerability was found in DedeCMS 5.7. It has been declared as problematic. Affected by this vulnerability is an	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown functionality of the file /src/dede/makehtml_spec.php. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2024-3144. 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.		
CVE-2024-3143	DedeCMS 5.7 member_rank.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 /src/dede/member_rank.php. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-3143. It is possible to launch the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	N
CVE-2024-3145	DedeCMS 5.7 makehtml_js_action.php cross-site request forgery	A vulnerability was found in DedeCMS 5.7. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /src/dede/makehtml_js_action.php. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2024-3145. The attack may be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	N
CVE-2024-2262	WP-FeedStats Themify Plugin up to 1.4.3 on WordPress cross-site request	A vulnerability has been found in WP-FeedStats Themify Plugin up to 1.4.3 on WordPress and	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	forgery	classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2024-2262. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-3135	mudler LocalAI cross-site request forgery	A vulnerability was found in mudler LocalAI and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2024-3135. The attack may be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-30965	DedeCMS 5.7 member_scores.php cross-site request forgery	A vulnerability has been found in DedeCMS 5.7 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /src/dede/member_scores.php. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2024-30965. The attack can be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-30946	DedeCMS 5.7 /src/dede/co_do.php cross-site request forgery	A vulnerability was found in DedeCMS 5.7 and classified as problematic. Affected by this issue is some unknown functionality of the file /src/dede/co_do.php. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2024-30946. The attack may be launched remotely. There is no exploit available.	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-2322	WooCommerce Cart Abandonment Recovery Plugin up to 1.2.26 on WordPress Email Template cross-site request forgery	A vulnerability was found in WooCommerce Cart Abandonment Recovery Plugin up to 1.2.26 on WordPress. It has been rated as problematic. This issue affects some unknown processing of the component Email Template Handler. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-2322. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	N
CVE-2024-3076	MM-email2image Plugin up to 0.2.5 on WordPress cross-site request forgery	A vulnerability which was classified as problematic was found in MM-email2image Plugin up to 0.2.5 on WordPress. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-3076. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2023-6385	Ping Optimizer Plugin up to 2.35.1.3.0 on WordPress cross-site request forgery	A vulnerability has been found in Ping Optimizer Plugin up to 2.35.1.3.0 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-6385. The attack can be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-1756	WooCommerce Customers Manager Plugin up to 29.7 on WordPress Ajax Action cross-site request forgery	A vulnerability was found in WooCommerce Customers Manager Plugin up to 29.7 on WordPress and classified as problematic. Affected by this issue is some unknown functionality of the component Ajax Action Handler. The	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2024-1756. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-3218	Shibang Communications IP Network Intercom Broadcasting System 1.0 busyscreenshotpush.php jsondata[callee]/jsondata[imagename] path traversal	A vulnerability classified as critical has been found in Shibang Communications IP Network Intercom Broadcasting System 1.0. This affects an unknown part of the file /php/busyscreenshotpush.php. The manipulation of the argument jsondata[callee]/jsondata[imagename] leads to path traversal: &039;../filedir&039;. This vulnerability is uniquely identified as CVE-2024-3218. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3227	Panwei eoffice OA up to 9.5 Backend save_image.php image_type path traversal	A vulnerability was found in Panwei eoffice OA up to 9.5. It has been declared as critical. This vulnerability affects unknown code of the file /general/system/interface/theme_set/save_image.php of the component Backend. The manipulation of the argument image_type leads to path traversal: &039;../filedir&039;. This vulnerability was named CVE-2024-3227. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-31011	beescms 4.0 admin_template.php path traversal	A vulnerability classified as critical has been found in beescms 4.0. Affected is an unknown function of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		admin_template.php. The manipulation leads to path traversal. This vulnerability is traded as CVE-2024-31011. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-0549	mintplex-labs anything-llm up to 0.x File path traversal	A vulnerability which was classified as problematic has been found in mintplex-labs anything-llm up to 0.x. This issue affects some unknown processing of the component File Handler. The manipulation leads to relative path traversal. The identification of this vulnerability is CVE-2024-0549. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-1593	mlflow URL Parameter path traversal	A vulnerability was found in mlflow and classified as critical. This issue affects some unknown processing of the component URL Parameter Handler. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2024-1593. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-1560	mlflow local_file_uri_to_path path traversal	A vulnerability classified as critical has been found in mlflow. This affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the function local_file_uri_to_path. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2024-1560. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-1594	mlflow Experiment Creation artifact_location path traversal	A vulnerability was found in mlflow and classified as critical. Affected by this issue is some unknown functionality of the component Experiment Creation Handler. The manipulation of the argument artifact_location leads to path traversal. This vulnerability is handled as CVE-2024-1594. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-1558	mlflow server/handlers.py _create_model_version path traversal	A vulnerability was found in mlflow. It has been classified as critical. Affected is the function _create_model_version of the file server/handlers.py. The manipulation leads to path traversal. This vulnerability is traded as CVE-2024-1558. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-1483	mlflow HTTP POST Request artifact_location/source path traversal	A vulnerability was found in mlflow. It has been rated as critical. Affected by this issue is some unknown functionality of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component HTTP POST Request Handler. The manipulation of the argument artifact_location/source leads to path traversal. This vulnerability is handled as CVE-2024-1483. The attack may be launched remotely. There is no exploit available.		

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-2930	SourceCodester Music Gallery Site 1.0 Master.php unrestricted upload	A vulnerability was found in SourceCodester Music Gallery Site 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file classes/Master.phpfsave_music. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2024-2930. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by custom rule	N
CVE-2024-3129	SourceCodester Image Accordion Gallery App 1.0 /endpoint/add-image.php image_name unrestricted upload	A vulnerability was found in SourceCodester Image Accordion Gallery App 1.0. It has been classified as critical. This affects an unknown part of the file /endpoint/add-image.php. The manipulation of the argument image_name leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2024-3129. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by custom rule	N
CVE-2024-30849	SourceCodester Complete E-Commerce Site 1.0 admin/products_photo.php filename unrestricted upload	A vulnerability has been found in SourceCodester Complete E-Commerce Site 1.0 and classified as critical. This vulnerability affects unknown code of the file admin/products_photo.php. The manipulation of the	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument filename leads to unrestricted upload. This vulnerability was named CVE-2024-30849. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-3437	SourceCodester Prison Management System 1.0 Avatar /Admin/add-admin.php avatar unrestricted upload	A vulnerability was found in SourceCodester Prison Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /Admin/add-admin.php of the component Avatar Handler. The manipulation of the argument avatar leads to unrestricted upload. The identification of this vulnerability is CVE-2024-3437. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by custom rule	N
CVE-2024-3436	SourceCodester Prison Management System 1.0 Avatar /Admin/edit-photo.php avatar unrestricted upload	A vulnerability was found in SourceCodester Prison Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /Admin/edit-photo.php of the component Avatar Handler. The manipulation of the argument avatar leads to unrestricted upload. This vulnerability was named CVE-2024-3436. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-3444	Wangshen SecGate 3600 up to 20240408 ?g=net_pro_keyword_import_save reqfile unrestricted upload	A vulnerability was found in Wangshen SecGate 3600 up to 20240408. It has been classified as critical. This affects an unknown part of the file /gnet_pro_keyword_import_save. The manipulation of the argument reqfile leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2024-3444. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by custom rule	N
CVE-2024-29399	GNU Savane up to 3.13 File upload.php unrestricted upload	A vulnerability which was classified as critical has been found in GNU Savane up to 3.13. This issue affects some unknown processing of the file upload.php of the component File Handler. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2024-29399. The attack may be initiated remotely. There is no exploit available.	Patched by custom rule	N
CVE-2024-32161	jizhiCMS 2.5 unrestricted upload	A vulnerability which was classified as critical was found in jizhiCMS 2.5. This affects an unknown part. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2024-32161. It is possible to initiate the attack remotely. There is no exploit available.	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-3948	SourceCodester Home Clean Service System 1.0 Photo \admin\student.add.php unrestricted upload	A vulnerability was found in SourceCodester Home Clean Service System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file \admin\student.add.php of the component Photo Handler. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2024-3948. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by custom rule	N
CVE-2024-31610	code-projects Simple School Management System 1.0 File unrestricted upload	A vulnerability which was classified as critical has been found in code-projects Simple School Management System 1.0. This issue affects some unknown processing of the component File Handler. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2024-31610. The attack may be initiated remotely. There is no exploit available.	Patched by custom rule	N

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-28421	Razor 0.8.0 channelmodle.php ChannelModel::updateapk sql injection (Issue 178)	A vulnerability was found in Razor 0.8.0. It has been rated as critical. This issue affects the function ChannelModel::updateapk of the file channelmodle.php. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2024-28421. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-2934	SourceCodester Todo List in Kanban Board 1.0 delete-todo.php list sql injection	A vulnerability classified as critical was found in SourceCodester Todo List in Kanban Board 1.0. Affected by this vulnerability is an unknown functionality of the file /endpoint/delete-todo.php. The manipulation of the argument list leads to sql injection. This vulnerability is known as CVE-2024-2934. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2942	Campcodes Online Examination System 1.0 deleteQuestionExe.php id sql injection	A vulnerability which was classified as critical was found in Campcodes Online Examination System 1.0. This affects an unknown part of the file /adminpanel/admin/query/deleteQuestionExe.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2024-2942. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-2944	Campcodes Online Examination System 1.0 deleteCourseExe.php id sql injection	A vulnerability was found in Campcodes Online Examination System 1.0 and classified as critical. This issue affects some unknown processing of the file /adminpanel/admin/query/deleteCourseExe.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-2944. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2943	Campcodes Online Examination System 1.0 deleteExamExe.php id sql injection	A vulnerability has been found in Campcodes Online Examination System 1.0 and classified as critical. This vulnerability affects unknown code of the file /adminpanel/admin/query/deleteExamExe.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-2943. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2945	Campcodes Online Examination System 1.0 updateExaminee.php id sql injection	A vulnerability was found in Campcodes Online Examination System 1.0. It has been classified as critical. Affected is an unknown function of the file /adminpanel/admin/facebox_modal/updateExaminee.php. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-2945. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2024-2938	Campcodes Online Examination System 1.0 updateCourse.php id sql injection	A vulnerability was found in Campcodes Online Examination System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /adminpanel/admin/facebox_modal/updateCourse.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-2938. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2941	Campcodes Online Examination System 1.0 loginExe.php pass sql injection	A vulnerability which was classified as critical has been found in Campcodes Online Examination System 1.0. Affected by this issue is some unknown functionality of the file /adminpanel/admin/query/loginExe.php. The manipulation of the argument pass leads to sql injection. This vulnerability is handled as CVE-2024-2941. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3000	code-projects Online Book System 1.0 /index.php username/password	A vulnerability classified as critical was found in code-projects Online Book System	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	/login_username/login_password sql injection	1.0. This vulnerability affects unknown code of the file /index.php. The manipulation of the argument username/password/login_username/login_password leads to sql injection. This vulnerability was named CVE-2024-3000. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-3002	code-projects Online Book System 1.0 /description.php ID sql injection	A vulnerability which was classified as critical was found in code-projects Online Book System 1.0. Affected is an unknown function of the file /description.php. The manipulation of the argument ID leads to sql injection. This vulnerability is traded as CVE-2024-3002. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2999	Campcodes Online Art Gallery Management System 1.0 /admin/adminHome.php uname sql injection	A vulnerability classified as critical has been found in Campcodes Online Art Gallery Management System 1.0. This affects an unknown part of the file /admin/adminHome.php. The manipulation of the argument uname leads to sql injection. This vulnerability is uniquely identified as CVE-2024-2999. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3001	code-projects Online Book System	A vulnerability which was classified as critical	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	1.0 /Product.php value sql injection	has been found in code-projects Online Book System 1.0. This issue affects some unknown processing of the file /Product.php. The manipulation of the argument value leads to sql injection. The identification of this vulnerability is CVE-2024-3001. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-3003	code-projects Online Book System 1.0 /cart.php quantity/remove sql injection	A vulnerability has been found in code-projects Online Book System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /cart.php. The manipulation of the argument quantity/remove leads to sql injection. This vulnerability is known as CVE-2024-3003. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3015	SourceCodester Simple Subscription Website 1.0 manage_plan.php id sql injection	A vulnerability classified as critical was found in SourceCodester Simple Subscription Website 1.0. Affected by this vulnerability is an unknown functionality of the file manage_plan.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2024-3015. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-3014	SourceCodester Simple Subscription Website 1.0 Actions.php title sql injection	A vulnerability classified as critical has been found in SourceCodester Simple Subscription Website 1.0. Affected is an unknown function of the file Actions.php. The manipulation of the argument title leads to sql injection. This vulnerability is traded as CVE-2024-3014. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3041	Netentsec NS-ASG Application Security Gateway 6.3 listloginfo.php sql injection	A vulnerability has been found in Netentsec NS-ASG Application Security Gateway 6.3 and classified as critical. This vulnerability affects unknown code of the file /protocol/log/listloginfo.php. The manipulation leads to sql injection. This vulnerability was named CVE-2024-3041. 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.	Patched by core rule	Y
CVE-2024-3042	SourceCodester Simple Subscription Website 1.0 manage_user.php id sql injection	A vulnerability was found in SourceCodester Simple Subscription Website 1.0 and classified as critical. This issue affects some unknown processing of the file manage_user.php. The manipulation of the argument id leads to sql injection.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The identification of this vulnerability is CVE-2024-3042. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-3040	Netentsec NS-ASG Application Security Gateway 6.3 /admin/list_crl_conf CRLId sql injection	A vulnerability which was classified as critical was found in Netentsec NS-ASG Application Security Gateway 6.3. This affects an unknown part of the file /admin/list_crl_conf. The manipulation of the argument CRLId leads to sql injection. This vulnerability is uniquely identified as CVE-2024-3040. It is possible to initiate the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-24407	SourceCodester Barangay Population Monitoring System 1.0 print_pdets.php sql injection	A vulnerability classified as critical has been found in SourceCodester Barangay Population Monitoring System 1.0. This affects an unknown part of the file print_pdets.php. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2024-24407. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-3088	PHPGurukul Emergency Ambulance Hiring Portal 1.0 Forgot Password Page	A vulnerability which was classified as critical was found in PHPGurukul Emergency Ambulance Hiring	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	forgot-password.php username sql injection	Portal 1.0. This affects an unknown part of the file /admin/forgot-password.php of the component Forgot Password Page. The manipulation of the argument username leads to sql injection. This vulnerability is uniquely identified as CVE-2024-3088. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-3087	PHPGurukul Emergency Ambulance Hiring Portal 1.0 Ambulance Tracking Page ambulance-tracking.php searchdata sql injection	A vulnerability which was classified as critical has been found in PHPGurukul Emergency Ambulance Hiring Portal 1.0. Affected by this issue is some unknown functionality of the file ambulance-tracking.php of the component Ambulance Tracking Page. The manipulation of the argument searchdata leads to sql injection. This vulnerability is handled as CVE-2024-3087. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3085	PHPGurukul Emergency Ambulance Hiring Portal 1.0 Admin Login Page /admin/login.php username sql injection	A vulnerability classified as critical has been found in PHPGurukul Emergency Ambulance Hiring Portal 1.0. Affected is an unknown function of the file /admin/login.php of the component Admin Login Page. The manipulation of the argument username leads to sql injection. This vulnerability is traded as CVE-2024-3085. It is possible to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		launch the attack remotely. Furthermore there is an exploit available.		
CVE-2024-30872	Netentsec NS-ASG Application Security Gateway 6.3 /include/authrp.php 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 /include/authrp.php. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2024-30872. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-30866	Netentsec NS-ASG Application Security Gateway 6.3 /3g/menu.php 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 /3g/menu.php. The manipulation leads to sql injection. This vulnerability is handled as CVE-2024-30866. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-30858	Netentsec NS-ASG Application Security Gateway 6.3 edit_fire_wall.php sql injection	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3 and classified as critical. This issue affects some unknown processing of the file /admin/edit_fire_wall.php. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2024-30858. The attack may be initiated remotely. There is no	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit available.		
CVE-2024-30859	Netentsec NS-ASG Application Security Gateway 6.3 config_ISCGroupSSLCert.php sql injection	A vulnerability classified as critical was found in Netentsec NS-ASG Application Security Gateway 6.3. Affected by this vulnerability is an unknown functionality of the file /admin/config_ISCGroupSSLCert.php. The manipulation leads to sql injection. This vulnerability is known as CVE-2024-30859. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-30870	Netentsec NS-ASG Application Security Gateway 6.3 address_interpret.php sql injection	A vulnerability which was classified as critical has been found in Netentsec NS-ASG Application Security Gateway 6.3. Affected by this issue is some unknown functionality of the file /admin/address_interpret.php. The manipulation leads to sql injection. This vulnerability is handled as CVE-2024-30870. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-30862	Netentsec NS-ASG Application Security Gateway 6.3 /3g/index.php sql injection	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3. It has been rated as critical. Affected by this issue is some unknown functionality of the file /3g/index.php. The manipulation leads to sql injection. This vulnerability is handled as CVE-2024-30862. The attack may	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		be launched remotely. There is no exploit available.		
CVE-2024-30861	Netentsec NS-ASG Application Security Gateway 6.3 ipsec_guide_1.php sql injection	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3. It has been classified as critical. Affected is an unknown function of the file /admin/configguide/ipsec_guide_1.php. The manipulation leads to sql injection. This vulnerability is traded as CVE-2024-30861. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-30867	Netentsec NS-ASG Application Security Gateway 6.3 edit_virtual_site_info.php sql injection	A vulnerability which was classified as critical was found in Netentsec NS-ASG Application Security Gateway 6.3. Affected is an unknown function of the file /admin/edit_virtual_site_info.php. The manipulation leads to sql injection. This vulnerability is traded as CVE-2024-30867. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-3148	DedeCMS 5.7.112 makehtml_archives_action.php sql injection	A vulnerability which was classified as critical has been found in DedeCMS 5.7.112. This issue affects some unknown processing of the file dede/makehtml_archives_action.php. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2024-3148. The attack may be initiated remotely. Furthermore	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-30865	Netentsec NS-ASG Application Security Gateway 6.3 edit_user_login.php sql injection	A vulnerability has been found in Netentsec NS-ASG Application Security Gateway 6.3 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/edit_user_login.php. The manipulation leads to sql injection. This vulnerability is known as CVE-2024-30865. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-30863	Netentsec NS-ASG Application Security Gateway 6.3 /WebPages/history.php sql injection	A vulnerability which was classified as critical has been found in Netentsec NS-ASG Application Security Gateway 6.3. This issue affects some unknown processing of the file /WebPages/history.php. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2024-30863. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-30864	Netentsec NS-ASG Application Security Gateway 6.3 config_ISCGroupTimePolicy.php sql injection	A vulnerability classified as critical was found in Netentsec NS-ASG Application Security Gateway 6.3. This vulnerability affects unknown code of the file /admin/config_ISCGroupTimePolicy.php. The manipulation leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		sql injection. This vulnerability was named CVE-2024-30864. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-30860	Netentsec NS-ASG Application Security Gateway 6.3 export_excel_user.php sql injection	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/export_excel_user.php. The manipulation leads to sql injection. This vulnerability is known as CVE-2024-30860. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-30868	Netentsec NS-ASG Application Security Gateway 6.3 /admin/add_getlogin.php sql injection	A vulnerability which was classified as critical was found in Netentsec NS-ASG Application Security Gateway 6.3. This affects an unknown part of the file /admin/add_getlogin.php. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2024-30868. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-30871	Netentsec NS-ASG Application Security Gateway 6.3 applyhardware.php sql injection	A vulnerability has been found in Netentsec NS-ASG Application Security Gateway 6.3 and classified as critical. This vulnerability affects unknown code of the file /WebPages/applyhardware.php. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation leads to sql injection. This vulnerability was named CVE-2024-30871. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-3131	SourceCodester Computer Laboratory Management System 1.0 Master.php id sql injection	A vulnerability was found in SourceCodester Computer Laboratory Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /classes/Master.phpfsave_category. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-3131. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3226	Campcodes Online Patient Record Management System 1.0 /admin/login.php password sql injection	A vulnerability was found in Campcodes Online Patient Record Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/login.php. The manipulation of the argument password leads to sql injection. This vulnerability is uniquely identified as CVE-2024-3226. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3225	SourceCodester PHP Task Management System 1.0 edit-task.php task_id sql injection	A vulnerability was found in SourceCodester PHP Task Management System 1.0 and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		classified as critical. Affected by this issue is some unknown functionality of the file edit-task.php. The manipulation of the argument task_id leads to sql injection. This vulnerability is handled as CVE-2024-3225. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-3224	SourceCodester PHP Task Management System 1.0 task-details.php task_id sql injection	A vulnerability has been found in SourceCodester PHP Task Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file task-details.php. The manipulation of the argument task_id leads to sql injection. This vulnerability is known as CVE-2024-3224. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3223	SourceCodester PHP Task Management System 1.0 admin-manage-user.php admin_id sql injection	A vulnerability which was classified as critical was found in SourceCodester PHP Task Management System 1.0. Affected is an unknown function of the file admin-manage-user.php. The manipulation of the argument admin_id leads to sql injection. This vulnerability is traded as CVE-2024-3223. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3221	SourceCodester PHP	A vulnerability	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Task Management System 1.0 attendance-info.php user_id sql injection	classified as critical was found in SourceCodester PHP Task Management System 1.0. This vulnerability affects unknown code of the file attendance-info.php. The manipulation of the argument user_id leads to sql injection. This vulnerability was named CVE-2024-3221. The attack can be initiated remotely. Furthermore there is an exploit available.	core rule	
CVE-2024-3222	SourceCodester PHP Task Management System 1.0 admin-password-change.php admin_id sql injection	A vulnerability which was classified as critical has been found in SourceCodester PHP Task Management System 1.0. This issue affects some unknown processing of the file admin-password-change.php. The manipulation of the argument admin_id leads to sql injection. The identification of this vulnerability is CVE-2024-3222. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-30998	PHPGurukul Men Salon Management System 2.0 index.php email sql injection	A vulnerability classified as critical has been found in PHPGurukul Men Salon Management System 2.0. Affected is an unknown function of the file index.php. The manipulation of the argument email leads to sql injection. This vulnerability is traded as CVE-2024-30998. It is possible to launch the attack remotely. There is no	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit available.		
CVE-2024-3256	SourceCodester Internship Portal Management System 1.0 admin/edit_activity.php activity_id sql injection	A vulnerability has been found in SourceCodester Internship Portal Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file admin/edit_activity.php. The manipulation of the argument activity_id leads to sql injection. This vulnerability is known as CVE-2024-3256. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3258	SourceCodester Internship Portal Management System 1.0 admin/add_activity.php title/description/start/end sql injection	A vulnerability was found in SourceCodester Internship Portal Management System 1.0. It has been classified as critical. This affects an unknown part of the file admin/add_activity.php. The manipulation of the argument title/description/start/end leads to sql injection. This vulnerability is uniquely identified as CVE-2024-3258. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3259	SourceCodester Internship Portal Management System 1.0 delete_activity.php activity_id sql injection	A vulnerability was found in SourceCodester Internship Portal Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file admin/delete_activity.php. The manipulation of the argument activity_id leads to sql injection. This vulnerability was named CVE-2024-3259. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-3255	SourceCodester Internship Portal Management System 1.0 edit_admin_query.php username/password/name/admin_id sql injection	A vulnerability which was classified as critical was found in SourceCodester Internship Portal Management System 1.0. Affected is an unknown function of the file admin/edit_admin_query.php. The manipulation of the argument username/password/name/admin_id leads to sql injection. This vulnerability is traded as CVE-2024-3255. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3254	SourceCodester Internship Portal Management System 1.0 admin/edit_admin.php admin_id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Internship Portal Management System 1.0. This issue affects some unknown processing of the file admin/edit_admin.php. The manipulation of the argument admin_id leads to sql injection. The identification of this vulnerability is CVE-2024-3254. The attack may be initiated remotely. Furthermore there is an exploit	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		available.		
CVE-2024-3253	SourceCodester Internship Portal Management System 1.0 admin/add_admin.php name/username/password sql injection	A vulnerability classified as critical was found in SourceCodester Internship Portal Management System 1.0. This vulnerability affects unknown code of the file admin/add_admin.php. The manipulation of the argument name/username/password leads to sql injection. This vulnerability was named CVE-2024-3253. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-31009	SEMCMS 4.8 Banner.php lgid sql injection	A vulnerability classified as critical has been found in SEMCMS 4.8. This affects an unknown part of the file Banner.php. The manipulation of the argument lgid leads to sql injection. This vulnerability is uniquely identified as CVE-2024-31009. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-3252	SourceCodester Internship Portal Management System 1.0 admin/check_admin.php username/password sql injection	A vulnerability classified as critical has been found in SourceCodester Internship Portal Management System 1.0. This affects an unknown part of the file admin/check_admin.php. The manipulation of the argument username/password leads to sql injection. This vulnerability is uniquely identified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2024-3252. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-3257	SourceCodester Internship Portal Management System 1.0 edit_activity_query.php title/description/start/end sql injection	A vulnerability was found in SourceCodester Internship Portal Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file admin/edit_activity_query.php. The manipulation of the argument title/description/start/end leads to sql injection. This vulnerability is handled as CVE-2024-3257. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3251	SourceCodester Computer Laboratory Management System 1.0 id sql injection	A vulnerability was found in SourceCodester Computer Laboratory Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/pageborrow/view_borrow. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-3251. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-31010	SEMCMS 4.8 Banner.php ID sql injection	A vulnerability classified as critical was found in SEMCMS 4.8. This vulnerability affects unknown code of the file Banner.php. The manipulation of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the argument ID leads to sql injection. This vulnerability was named CVE-2024-31010. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-3316	SourceCodester Computer Laboratory Management System 1.0 view_category.php id sql injection	A vulnerability was found in SourceCodester Computer Laboratory Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/category/view_category.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2024-3316. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3315	SourceCodester Computer Laboratory Management System 1.0 classes/user.php id sql injection	A vulnerability was found in SourceCodester Computer Laboratory Management System 1.0. It has been classified as critical. Affected is an unknown function of the file classes/user.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-3315. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-36645	ITB-GmbH TradePro 9.5 oordershow customer bestellid sql injection	A vulnerability classified as critical was found in ITB-GmbH TradePro 9.5. Affected	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		by this vulnerability is the function customer of the component oordershow. The manipulation of the argument bestellid leads to sql injection. This vulnerability is known as CVE-2023-36645. The attack can be launched remotely. There is no exploit available.		
CVE-2024-31025	ECshop 4.x file/article.php sql injection	A vulnerability was found in ECshop 4.x. It has been classified as critical. This affects an unknown part of the file file/article.php. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2024-31025. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-3349	SourceCodester Aplaya Beach Resort Online Reservation System 1.0 admin/login.php email sql injection	A vulnerability classified as critical was found in SourceCodester Aplaya Beach Resort Online Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file admin/login.php. The manipulation of the argument email leads to sql injection. This vulnerability is known as CVE-2024-3349. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3362	SourceCodester Online Library System 1.0 controller.php IBSN sql injection	A vulnerability was found in SourceCodester Online Library System 1.0 and classified as critical. Affected by this issue is some unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		functionality of the file admin/books/controller.php. The manipulation of the argument IBSN leads to sql injection. This vulnerability is handled as CVE-2024-3362. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-3352	SourceCodester Aplaya Beach Resort Online Reservation System 1.0 index.php id sql injection	A vulnerability has been found in SourceCodester Aplaya Beach Resort Online Reservation System 1.0 and classified as critical. This vulnerability affects unknown code of the file admin/mod_comments/index.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-3352. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3354	SourceCodester Aplaya Beach Resort Online Reservation System 1.0 index.php id sql injection	A vulnerability was found in SourceCodester Aplaya Beach Resort Online Reservation System 1.0. It has been classified as critical. Affected is an unknown function of the file admin/mod_users/index.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-3354. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-3351	SourceCodester Aplaya Beach Resort Online Reservation System 1.0 index.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Aplaya Beach Resort Online Reservation System 1.0. This affects an unknown part of the file admin/mod_roomtype/index.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-3351. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3348	SourceCodester Aplaya Beach Resort Online Reservation System 1.0 booking/index.php log_email/log_pword sql injection	A vulnerability classified as critical has been found in SourceCodester Aplaya Beach Resort Online Reservation System 1.0. Affected is an unknown function of the file booking/index.php. The manipulation of the argument log_email/log_pword leads to sql injection. This vulnerability is traded as CVE-2024-3348. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3347	SourceCodester Airline Ticket Reservation System 1.0 activate_jet_details_form_handler.php jet_id sql injection	A vulnerability was found in SourceCodester Airline Ticket Reservation System 1.0. It has been rated as critical. This issue affects some unknown processing of the file activate_jet_details_form_handler.php. The manipulation of the argument jet_id leads	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to sql injection. The identification of this vulnerability is CVE-2024-3347. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-3353	SourceCodester Aplaya Beach Resort Online Reservation System 1.0 index.php categ/end sql injection	A vulnerability was found in SourceCodester Aplaya Beach Resort Online Reservation System 1.0 and classified as critical. This issue affects some unknown processing of the file admin/mod_reports/index.php. The manipulation of the argument categ/end leads to sql injection. The identification of this vulnerability is CVE-2024-3353. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3360	SourceCodester Online Library System 1.0 admin/books/index.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Online Library System 1.0. Affected is an unknown function of the file admin/books/index.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-3360. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3359	SourceCodester Online Library System 1.0 admin/login.php user_email sql injection	A vulnerability which was classified as critical has been found in SourceCodester Online Library System 1.0. This issue affects some unknown processing of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the file admin/login.php. The manipulation of the argument user_email leads to sql injection. The identification of this vulnerability is CVE-2024-3359. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-3361	SourceCodester Online Library System 1.0 deweydecimal.php category sql injection	A vulnerability has been found in SourceCodester Online Library System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file admin/books/deweydecimal.php. The manipulation of the argument category leads to sql injection. This vulnerability is known as CVE-2024-3361. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3363	SourceCodester Online Library System 1.0 admin/borrowed/index.php BookPublisher/BookTitle sql injection	A vulnerability was found in SourceCodester Online Library System 1.0. It has been classified as critical. This affects an unknown part of the file admin/borrowed/index.php. The manipulation of the argument BookPublisher/BookTitle leads to sql injection. This vulnerability is uniquely identified as CVE-2024-3363. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3350	SourceCodester Aplaya Beach Resort	A vulnerability which was classified as critical	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Online Reservation System 1.0 admin/mod_room/index.php id sql injection	has been found in SourceCodester Aplaya Beach Resort Online Reservation System 1.0. Affected by this issue is some unknown functionality of the file admin/mod_room/index.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-3350. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-3355	SourceCodester Aplaya Beach Resort Online Reservation System 1.0 controller.php name sql injection	A vulnerability was found in SourceCodester Aplaya Beach Resort Online Reservation System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file admin/mod_users/controller.phpactionadd. The manipulation of the argument name leads to sql injection. This vulnerability is known as CVE-2024-3355. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3356	SourceCodester Aplaya Beach Resort Online Reservation System 1.0 controller.php type sql injection	A vulnerability was found in SourceCodester Aplaya Beach Resort Online Reservation System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file admin/mod_settings/controller.phpactionadd. The manipulation of the argument type leads to sql injection.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is handled as CVE-2024-3356. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-3417	SourceCodester Online Courseware 1.0 admin/saveeditt.php contact sql injection	A vulnerability which was classified as critical has been found in SourceCodester Online Courseware 1.0. This issue affects some unknown processing of the file admin/saveeditt.php. The manipulation of the argument contact leads to sql injection. The identification of this vulnerability is CVE-2024-3417. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3419	SourceCodester Online Courseware 1.0 admin/edit.php id sql injection	A vulnerability has been found in SourceCodester Online Courseware 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file admin/edit.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2024-3419. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3418	SourceCodester Online Courseware 1.0 deactivateteach.php selector sql injection	A vulnerability which was classified as critical was found in SourceCodester Online Courseware 1.0. Affected is an unknown function of the file admin/deactivateteach.php. The manipulation of the argument	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		selector leads to sql injection. This vulnerability is traded as CVE-2024-3418. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2024-3423	SourceCodester Online Courseware 1.0 admin/activateteach.php selector sql injection	A vulnerability was found in SourceCodester Online Courseware 1.0. It has been rated as critical. This issue affects some unknown processing of the file admin/activateteach.php. The manipulation of the argument selector leads to sql injection. The identification of this vulnerability is CVE-2024-3423. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3425	SourceCodester Online Courseware 1.0 admin/activateall.php selector sql injection	A vulnerability classified as critical was found in SourceCodester Online Courseware 1.0. Affected by this vulnerability is an unknown functionality of the file admin/activateall.php. The manipulation of the argument selector leads to sql injection. This vulnerability is known as CVE-2024-3425. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3421	SourceCodester Online Courseware 1.0 admin/deactivatestud.php selector sql injection	A vulnerability was found in SourceCodester Online Courseware 1.0. It has been classified as critical. This affects an	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown part of the file admin/deactivatestud.php. The manipulation of the argument selector leads to sql injection. This vulnerability is uniquely identified as CVE-2024-3421. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-3416	SourceCodester Online Courseware 1.0 admin/editt.php id sql injection	A vulnerability classified as critical was found in SourceCodester Online Courseware 1.0. This vulnerability affects unknown code of the file admin/editt.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-3416. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3420	SourceCodester Online Courseware 1.0 admin/saveedit.php id sql injection	A vulnerability was found in SourceCodester Online Courseware 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file admin/saveedit.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-3420. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3422	SourceCodester Online Courseware 1.0 admin/activatestud.php selector sql	A vulnerability was found in SourceCodester Online Courseware 1.0. It has been declared as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	critical. This vulnerability affects unknown code of the file admin/activatestud.php. The manipulation of the argument selector leads to sql injection. This vulnerability was named CVE-2024-3422. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-3424	SourceCodester Online Courseware 1.0 admin/listscore.php title sql injection	A vulnerability classified as critical has been found in SourceCodester Online Courseware 1.0. Affected is an unknown function of the file admin/listscore.php. The manipulation of the argument title leads to sql injection. This vulnerability is traded as CVE-2024-3424. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3413	SourceCodester Human Resource Information System 1.0 login_process.php hr_email/hr_password sql injection	A vulnerability has been found in SourceCodester Human Resource Information System 1.0 and classified as critical. This vulnerability affects unknown code of the file initialize/login_process.php. The manipulation of the argument hr_email/hr_password leads to sql injection. This vulnerability was named CVE-2024-3413. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3457	Netentsec NS-ASG Application Security	A vulnerability classified as critical has	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Gateway 6.3 config_ISCGroupNoCache.php GroupId sql injection	been found in Netentsec NS-ASG Application Security Gateway 6.3. This affects an unknown part of the file /admin/config_ISCGroupNoCache.php. The manipulation of the argument GroupId leads to sql injection. This vulnerability is uniquely identified as CVE-2024-3457. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-3466	SourceCodester Laundry Management System 1.0 Pengeluaran.php laporan_filter dari/sampai sql injection	A vulnerability was found in SourceCodester Laundry Management System 1.0. It has been declared as critical. Affected by this vulnerability is the function laporan_filter of the file /application/controller/Pengeluaran.php. The manipulation of the argument dari/sampai leads to sql injection. This vulnerability is known as CVE-2024-3466. Access to the local network is required for this attack. There is no exploit available.	Patched by core rule	Y
CVE-2024-3456	Netentsec NS-ASG Application Security Gateway 6.3 config_Anticrack.php GroupId sql injection	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/config_Anticrack.php. The manipulation of the argument GroupId leads to sql injection. This vulnerability is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		handled as CVE-2024-3456. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-3455	Netentsec NS-ASG Application Security Gateway 6.3 /admin/add_postlogin.php SingleLoginId sql injection	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/add_postlogin.php. The manipulation of the argument SingleLoginId leads to sql injection. This vulnerability is known as CVE-2024-3455. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3465	SourceCodester Laundry Management System 1.0 Transaki.php laporan_filter dari/sampai sql injection	A vulnerability was found in SourceCodester Laundry Management System 1.0. It has been classified as critical. Affected is the function laporan_filter of the file /application/controller/Transaki.php. The manipulation of the argument dari/sampai leads to sql injection. This vulnerability is traded as CVE-2024-3465. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3458	Netentsec NS-ASG Application Security Gateway 6.3 /admin/add_ikev2.php TunnelId sql injection	A vulnerability classified as critical was found in Netentsec NS-ASG Application Security Gateway 6.3. This vulnerability affects unknown code of the file /admin/add_ikev2.php.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The manipulation of the argument TunnelId leads to sql injection. This vulnerability was named CVE-2024-3458. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-3445	SourceCodester Laundry Management System 1.0 /karyawan/laporan_filter data_karyawan sql injection	A vulnerability was found in SourceCodester Laundry Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /karyawan/laporan_filter. The manipulation of the argument data_karyawan leads to sql injection. This vulnerability was named CVE-2024-3445. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3464	SourceCodester Laundry Management System 1.0 Pelanggan.php laporan_filter jeniskelamin sql injection	A vulnerability was found in SourceCodester Laundry Management System 1.0 and classified as critical. This issue affects the function laporan_filter of the file /application/controller/Pelanggan.php. The manipulation of the argument jeniskelamin leads to sql injection. The identification of this vulnerability is CVE-2024-3464. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3440	SourceCodester Prison Management System 1.0 /Admin/edit_profile.	A vulnerability was found in SourceCodester Prison Management System	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	php sql injection	1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /Admin/edit_profile.php. The manipulation leads to sql injection. This vulnerability is known as CVE-2024-3440. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2024-3442	SourceCodester Prison Management System 1.0 delete_leave.php sql injection	A vulnerability classified as critical has been found in SourceCodester Prison Management System 1.0. This affects an unknown part of the file /Employee/delete_leave.php. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2024-3442. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3438	SourceCodester Prison Management System 1.0 /Admin/login.php sql injection	A vulnerability was found in SourceCodester Prison Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /Admin/login.php. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2024-3438. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3439	SourceCodester Prison Management	A vulnerability was found in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System 1.0 /Account/login.php sql injection	SourceCodester Prison Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /Account/login.php. The manipulation leads to sql injection. This vulnerability is traded as CVE-2024-3439. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2024-3441	SourceCodester Prison Management System 1.0 edit-profile.php sql injection	A vulnerability was found in SourceCodester Prison Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /Employee/edit-profile.php. The manipulation leads to sql injection. This vulnerability is handled as CVE-2024-3441. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-31507	SourceCodester Online Graduate Tracer System 1.0 admin/fetch_gendercs.php request sql injection	A vulnerability has been found in SourceCodester Online Graduate Tracer System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file admin/fetch_gendercs.php. The manipulation of the argument request leads to sql injection. This vulnerability is known as CVE-2024-31507. The attack can be launched remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		There is no exploit available.		
CVE-2024-3620	SourceCodester Kortex Lite Advocate Office Management System 1.0 /control/adds.php name/gender/dob/email/mobile/address sql injection	A vulnerability was found in SourceCodester Kortex Lite Advocate Office Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /control/adds.php. The manipulation of the argument name/gender/dob/email/mobile/address leads to sql injection. This vulnerability is handled as CVE-2024-3620. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3619	SourceCodester Kortex Lite Advocate Office Management System 1.0 addcase_stage.php cname sql injection	A vulnerability has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /control/addcase_stage.php. The manipulation of the argument cname leads to sql injection. This vulnerability is known as CVE-2024-3619. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3617	SourceCodester Kortex Lite Advocate Office Management System 1.0 deactivate_case.php id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0. This issue affects some unknown processing of the file /control/deactivate_case.php. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-3617. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-3621	SourceCodester Kortex Lite Advocate Office Management System 1.0 register_case.php sql injection	A vulnerability was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. It has been classified as critical. This affects an unknown part of the file /control/register_case.php. The manipulation of the argument title/case_no/client_name/court/case_type/case_stage/legel_acts/description/filling_date/hearing_date/opposite_lawyer/total_fees/unpaid leads to sql injection. This vulnerability is uniquely identified as CVE-2024-3621. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3618	SourceCodester Kortex Lite Advocate Office Management System 1.0 activate_case.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. Affected is an unknown function of the file /control/activate_case.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-3618. It is possible to launch the attack	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. Furthermore there is an exploit available.		
CVE-2024-3690	PHPGurukul Small CRM 3.0 Change Password sql injection	A vulnerability classified as critical was found in PHPGurukul Small CRM 3.0. Affected by this vulnerability is an unknown functionality of the component Change Password Handler. The manipulation leads to sql injection. This vulnerability is known as CVE-2024-3690. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3697	Campcodes House Rental Management System 1.0 manage_tenant.php id sql injection	A vulnerability was found in Campcodes House Rental Management System 1.0. It has been classified as critical. Affected is an unknown function of the file manage_tenant.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-3697. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3698	Campcodes House Rental Management System 1.0 manage_payment.php id sql injection	A vulnerability was found in Campcodes House Rental Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file manage_payment.php. The manipulation of the argument id leads to sql injection.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is known as CVE-2024-3698. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2024-3769	PHPGurukul Student Record System 3.20 /login.php id/password sql injection	A vulnerability which was classified as critical was found in PHPGurukul Student Record System 3.20. Affected is an unknown function of the file /login.php. The manipulation of the argument id/password leads to sql injection. This vulnerability is traded as CVE-2024-3769. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3767	PHPGurukul News Portal 4.1 /admin/edit-post.php posttitle sql injection	A vulnerability classified as critical was found in PHPGurukul News Portal 4.1. This vulnerability affects unknown code of the file /admin/edit-post.php. The manipulation of the argument posttitle leads to sql injection. This vulnerability was named CVE-2024-3767. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3768	PHPGurukul News Portal 4.1 search.php searchtitle sql injection	A vulnerability which was classified as critical has been found in PHPGurukul News Portal 4.1. This issue affects some unknown processing of the file search.php. The manipulation of the argument searchtitle leads to sql injection. The identification of this vulnerability is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2024-3768. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-28558	SourceCodester Petrol Pump Management Software 1.0 admin/app/web_crud.php sql injection	A vulnerability has been found in SourceCodester Petrol Pump Management Software 1.0 and classified as critical. This vulnerability affects unknown code of the file admin/app/web_crud.php. The manipulation leads to sql injection. This vulnerability was named CVE-2024-28558. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-2940	Campcodes Online Examination System 1.0 updateCourse.php id cross site scripting	A vulnerability classified as problematic was found in Campcodes Online Examination System 1.0. Affected by this vulnerability is an unknown functionality of the file /adminpanel/admin/facebox_modal/updateCourse.php. The manipulation of the argument id leads to cross site scripting. This vulnerability is known as CVE-2024-2940. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2939	Campcodes Online Examination System 1.0 updateExaminee.php id cross site scripting	A vulnerability classified as problematic has been found in Campcodes Online Examination System 1.0. Affected is an unknown function of the file /adminpanel/admin/facebox_modal/updateExaminee.php. The manipulation of the argument id leads to cross site scripting. This vulnerability is traded as CVE-2024-2939. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2935	SourceCodester Todo List in Kanban Board 1.0 Add ToDo cross site scripting	A vulnerability which was classified as problematic has been found in SourceCodester Todo List in Kanban Board 1.0. Affected by this issue is some unknown functionality of the component Add ToDo.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The manipulation of the argument Todo leads to cross site scripting. This vulnerability is handled as CVE-2024-2935. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-3004	code-projects Online Book System 1.0 /Product.php value cross site scripting	A vulnerability was found in code-projects Online Book System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /Product.php. The manipulation of the argument value leads to cross site scripting. This vulnerability is handled as CVE-2024-3004. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-31065	Insurance Mangement System up to 1.0.0 City cross site scripting	A vulnerability was found in Insurance Mangement System up to 1.0.0. It has been classified as problematic. Affected is an unknown function. The manipulation of the argument City leads to cross site scripting. This vulnerability is traded as CVE-2024-31065. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-31064	Insurance Mangement System up to 1.0.0 First Name cross site scripting	A vulnerability was found in Insurance Mangement System up to 1.0.0 and classified as problematic. This issue affects some unknown processing. The manipulation of the argument First	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Name leads to cross site scripting. The identification of this vulnerability is CVE-2024-31064. The attack may be initiated remotely. There is no exploit available.		
CVE-2024-31061	Insurance Mangement System up to 1.0.0 Last Name cross site scripting	A vulnerability which was classified as problematic was found in Insurance Mangement System up to 1.0.0. This affects an unknown part. The manipulation of the argument Last Name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-31061. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-31062	Insurance Mangement System up to 1.0.0 Street cross site scripting	A vulnerability which was classified as problematic has been found in Insurance Mangement System up to 1.0.0. Affected by this issue is some unknown functionality. The manipulation of the argument Street leads to cross site scripting. This vulnerability is handled as CVE-2024-31062. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-31063	Insurance Mangement System up to 1.0.0 Email cross site scripting	A vulnerability has been found in Insurance Mangement System up to 1.0.0 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument Email leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability was named CVE-2024-31063. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-3091	PHPGurukul Emergency Ambulance Hiring Portal 1.0 Search Request Page /admin/search.php cross site scripting	A vulnerability was found in PHPGurukul Emergency Ambulance Hiring Portal 1.0. It has been classified as problematic. Affected is an unknown function of the file /admin/search.php of the component Search Request Page. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-3091. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3090	PHPGurukul Emergency Ambulance Hiring Portal 1.0 Add Ambulance Page /admin/add-ambulance.php Ambulance Reg No/Driver Name cross site scripting	A vulnerability was found in PHPGurukul Emergency Ambulance Hiring Portal 1.0 and classified as problematic. This issue affects some unknown processing of the file /admin/add-ambulance.php of the component Add Ambulance Page. The manipulation of the argument Ambulance Reg No/Driver Name leads to cross site scripting. The identification of this vulnerability is CVE-2024-3090. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3086	PHPGurukul Emergency Ambulance Hiring Portal 1.0	A vulnerability classified as problematic was found in PHPGurukul	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Ambulance Tracking Page ambulance-tracking.php searchdata cross site scripting	Emergency Ambulance Hiring Portal 1.0. Affected by this vulnerability is an unknown functionality of the file ambulance-tracking.php of the component Ambulance Tracking Page. The manipulation of the argument searchdata leads to cross site scripting. This vulnerability is known as CVE-2024-3086. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2024-3084	PHPGurukul Emergency Ambulance Hiring Portal 1.0 Hire an Ambulance Page cross site scripting	A vulnerability was found in PHPGurukul Emergency Ambulance Hiring Portal 1.0. It has been rated as problematic. This issue affects some unknown processing of the component Hire an Ambulance Page. The manipulation of the argument Patient Name/Relative Name/Relative Phone Number/City/State/Message leads to cross site scripting. The identification of this vulnerability is CVE-2024-3084. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3141	Clavister E10/E80 up to 20240323 Misc Settings Page MiscSettings cross site scripting	A vulnerability has been found in Clavister E10 and E80 up to 20240323 and classified as problematic. This vulnerability affects unknown code of the file /PageNode&OBJ/System/AdvancedSettings/DeviceSettings/Misc	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Settings of the component Misc Settings Page. The manipulation of the argument WatchdogTimerTime/BufFloodRebootTime/MaxPipeUsers/AVCacheLifetime/HTTPipeliningMaxReq/ReassemblyMaxConnections/ReassemblyMaxProcessingMem/ScrSaveTime leads to cross site scripting. This vulnerability was named CVE-2024-3141. The attack can be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-3140	SourceCodester Computer Laboratory Management System 1.0 Users.php middlename cross site scripting	A vulnerability which was classified as problematic was found in SourceCodester Computer Laboratory Management System 1.0. This affects an unknown part of the file /classes/Users.phpfsave. The manipulation of the argument middlename leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-3140. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3125	Zebra ZTC GK420d 1.0 Alert Setup Page /settings Address cross site scripting	A vulnerability classified as problematic was found in Zebra ZTC GK420d 1.0. This vulnerability affects unknown code of the file /settings of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the component Alert Setup Page. The manipulation of the argument Address leads to cross site scripting. This vulnerability was named CVE-2024-3125. The attack can be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-2278	WP-FeedStats Themify Plugin up to 1.4.3 on WordPress Setting cross site scripting	A vulnerability was found in WP-FeedStats Themify Plugin up to 1.4.3 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-2024-2278. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-2263	WP-FeedStats Themify Plugin up to 1.4.3 on WordPress cross site scripting	A vulnerability which was classified as problematic was found in WP-FeedStats Themify Plugin up to 1.4.3 on WordPress. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-2263. It is possible to initiate the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-1274	Joseph C Dolson My Calendar Plugin up to 3.4.23 on WordPress cross site scripting	A vulnerability was found in Joseph C Dolson My Calendar Plugin up to 3.4.23 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-2024-1274. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-3320	SourceCodester eLearning System 1.0 page cross site scripting	A vulnerability was found in SourceCodester eLearning System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument page leads to cross site scripting. This vulnerability is handled as CVE-2024-3320. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-3321	SourceCodester eLearning System 1.0 Maintenance Module Subject Code/Description cross site scripting	A vulnerability classified as problematic has been found in SourceCodester eLearning System 1.0. This affects an unknown part of the component	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Maintenance Module. The manipulation of the argument Subject Code/Description leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-3321. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-25503	Advanced REST Client 17.0.9 New Project cross site scripting	A vulnerability which was classified as problematic was found in Advanced REST Client 17.0.9. Affected is an unknown function of the component New Project Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-25503. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-27705	Leantime 3.0.6 PDF File cross site scripting	A vulnerability was found in Leantime 3.0.6. It has been declared as problematic. This vulnerability affects unknown code of the component PDF File Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-27705. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-29413	Webasyst 2.9.9 Contact Info Instant messenger cross site scripting	A vulnerability was found in Webasyst 2.9.9 and classified as problematic. Affected by this issue is some unknown functionality of the component Contact Info. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument Instant messenger leads to cross site scripting. This vulnerability is handled as CVE-2024-29413. The attack may be launched remotely. There is no exploit available.		
CVE-2024-3364	SourceCodester Online Library System 1.0 admin/books/index.php id cross site scripting	A vulnerability was found in SourceCodester Online Library System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file admin/books/index.php. The manipulation of the argument id leads to cross site scripting. This vulnerability was named CVE-2024-3364. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3365	SourceCodester Online Library System 1.0 controller.php user_name cross site scripting	A vulnerability was found in SourceCodester Online Library System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file admin/users/controller.php. The manipulation of the argument user_name leads to cross site scripting. The identification of this vulnerability is CVE-2024-3365. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2509	Kadence Gutenberg Blocks Plugin up to 3.2.25 on WordPress Option cross site scripting	A vulnerability was found in Kadence Gutenberg Blocks Plugin up to 3.2.25 on WordPress. It has been classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		problematic. This affects an unknown part of the component Option Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-2509. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-3378	iboss Secure Web Gateway up to 10.1 Login Portal /login redirectUrl cross site scripting	A vulnerability has been found in iboss Secure Web Gateway up to 10.1 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /login of the component Login Portal. The manipulation of the argument redirectUrl leads to cross site scripting. This vulnerability is known as CVE-2024-3378. The attack can be launched remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-3377	SourceCodester Computer Laboratory Management System 1.0 SystemSettings.php name cross site scripting	A vulnerability classified as problematic was found in SourceCodester Computer Laboratory Management System 1.0. This vulnerability affects unknown code of the file /classes/SystemSettings.phpfupdate_settings. The manipulation of the argument name	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		leads to cross site scripting. This vulnerability was named CVE-2024-3377. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-3358	SourceCodester Aplaya Beach Resort Online Reservation System 1.0 /index.php to cross site scripting	A vulnerability classified as problematic was found in SourceCodester Aplaya Beach Resort Online Reservation System 1.0. This vulnerability affects unknown code of the file /index.php. The manipulation of the argument to leads to cross site scripting. This vulnerability was named CVE-2024-3358. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3357	SourceCodester Aplaya Beach Resort Online Reservation System 1.0 index.php end cross site scripting	A vulnerability classified as problematic has been found in SourceCodester Aplaya Beach Resort Online Reservation System 1.0. This affects an unknown part of the file admin/mod_reports/index.php. The manipulation of the argument end leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-3357. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2444	Inline Related Posts Plugin up to 3.4.x on WordPress Setting cross site scripting	A vulnerability has been found in Inline Related Posts Plugin up to 3.4.x on WordPress and classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-2444. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-3075	MM-email2image Plugin up to 0.2.5 on WordPress Shortcode cross site scripting	A vulnerability classified as problematic was found in MM-email2image Plugin up to 0.2.5 on WordPress. This vulnerability affects unknown code of the component Shortcode Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-3075. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-3048	Bannerlid Plugin up to 1.1.0 on WordPress cross site scripting	A vulnerability which was classified as problematic has been found in Bannerlid Plugin up to 1.1.0 on WordPress. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-3048. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-28741	EginDemirbilek Northstar C2 1 login.php cross site	A vulnerability was found in EginDemirbilek	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	scripting	Northstar C2 1. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file login.php. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-28741. The attack can be launched remotely. There is no exploit available.		
CVE-2024-3427	SourceCodester Online Courseware 1.0 addq.php id cross site scripting	A vulnerability which was classified as problematic was found in SourceCodester Online Courseware 1.0. This affects an unknown part of the file addq.php. The manipulation of the argument id leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-3427. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3426	SourceCodester Online Courseware 1.0 editt.php id cross site scripting	A vulnerability which was classified as problematic has been found in SourceCodester Online Courseware 1.0. Affected by this issue is some unknown functionality of the file editt.php. The manipulation of the argument id leads to cross site scripting. This vulnerability is handled as CVE-2024-3426. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3428	SourceCodester Online Courseware	A vulnerability has been found in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	1.0 edit.php id cross site scripting	SourceCodester Online Courseware 1.0 and classified as problematic. This vulnerability affects unknown code of the file edit.php. The manipulation of the argument id leads to cross site scripting. This vulnerability was named CVE-2024-3428. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-3415	SourceCodester Human Resource Information System 1.0 addbranches_process.php branches_name cross site scripting	A vulnerability was found in SourceCodester Human Resource Information System 1.0. It has been classified as problematic. Affected is an unknown function of the file Superadmin_Dashboard/process/addbranches_process.php. The manipulation of the argument branches_name leads to cross site scripting. This vulnerability is traded as CVE-2024-3415. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3414	SourceCodester Human Resource Information System 1.0 addcorporate_process.php corporate_name cross site scripting	A vulnerability was found in SourceCodester Human Resource Information System 1.0 and classified as problematic. This issue affects some unknown processing of the file Superadmin_Dashboard/process/addcorporate_process.php. The manipulation of the argument corporate_name leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The identification of this vulnerability is CVE-2024-3414. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-1588	SendPress Newsletters Plugin up to 1.23.11.6 on WordPress Setting cross site scripting	A vulnerability has been found in SendPress Newsletters Plugin up to 1.23.11.6 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-1588. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-1292	WP-FeedStats wpb-show-core Plugin up to 2.5 on WordPress cross site scripting	A vulnerability which was classified as problematic was found in WP-FeedStats wpb-show-core Plugin up to 2.5 on WordPress. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-1292. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-3443	SourceCodester Prison Management System 1.0 apply_leave.php txtstart_date/txtend_date cross site scripting	A vulnerability classified as problematic was found in SourceCodester Prison Management System 1.0. This vulnerability affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown code of the file /Employee/apply_leave.php. The manipulation of the argument txtstart_date/txtend_date leads to cross site scripting. This vulnerability was named CVE-2024-3443. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-1752	Font Farsi Plugin up to 1.6.6 on WordPress Setting cross site scripting	A vulnerability was found in Font Farsi Plugin up to 1.6.6 on WordPress. It has been classified as problematic. This affects an unknown part of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-1752. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-1958	WP-FeedStats wpb-show-core Plugin up to 2.6 on WordPress cross site scripting	A vulnerability was found in WP-FeedStats wpb-show-core Plugin up to 2.6 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-2024-1958. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-1956	WP-FeedStats wpb-show-core Plugin up to 2.6 on WordPress	A vulnerability was found in WP-FeedStats wpb-show-core Plugin	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	the cross site scripting	up to 2.6 on WordPress. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument the leads to cross site scripting. This vulnerability was named CVE-2024-1956. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-3463	SourceCodester Laundry Management System 1.0 /karyawan/edit karyawan cross site scripting	A vulnerability has been found in SourceCodester Laundry Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /karyawan/edit. The manipulation of the argument karyawan leads to cross site scripting. This vulnerability was named CVE-2024-3463. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-1589	SendPress Newsletters Plugin up to 1.23.11.6 on WordPress Setting cross site scripting	A vulnerability was found in SendPress Newsletters Plugin up to 1.23.11.6 on WordPress and classified as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		1589. The attack may be launched remotely. There is no exploit available.		
CVE-2024-1664	Responsive Gallery Grid Plugin up to 2.3.10 on WordPress Setting cross site scripting	A vulnerability classified as problematic was found in Responsive Gallery Grid Plugin up to 2.3.10 on WordPress. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-1664. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-31544	Computer Laboratory Management System 1.0 Master.php remarks/borrower_name/faculty_department cross site scripting	A vulnerability classified as problematic was found in Computer Laboratory Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /classes/Master.phpfsave_record. The manipulation of the argument remarks/borrower_name/faculty_department leads to cross site scripting. This vulnerability is known as CVE-2024-31544. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-2428	Ultimate Video Plugin up to 2.2.2 on WordPress REST Route cross site	A vulnerability was found in Ultimate Video Plugin up to 2.2.2 on WordPress. It	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	scripting	has been classified as problematic. This affects an unknown part of the component REST Route Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-2428. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-3093	khl32 Font Farsi Plugin up to 1.6.6 on WordPress Setting cross site scripting	A vulnerability was found in khl32 Font Farsi Plugin up to 1.6.6 on WordPress. It has been classified as problematic. This affects an unknown part of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-3093. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-3570	mintplex-labs anything-llm dangerouslySetInnerHTML cross site scripting	A vulnerability was found in mintplex-labs anything-llm and classified as problematic. This issue affects the function dangerouslySetInnerHTML. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-3570. The attack may be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-3616	SourceCodester Warehouse Management System 1.0 pengguna.php admin_user/admin_nama/admin_alamat/admin_telepon cross site scripting	A vulnerability classified as problematic was found in SourceCodester Warehouse Management System 1.0. This vulnerability affects unknown code of the file pengguna.php. The manipulation of the argument admin_user/admin_nama/admin_alamat/admin_telepon leads to cross site scripting. This vulnerability was named CVE-2024-3616. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3614	SourceCodester Warehouse Management System 1.0 customer.php nama_customer/alamat_customer/notelp_customer cross site scripting	A vulnerability classified as problematic has been found in SourceCodester Warehouse Management System 1.0. This affects an unknown part of the file customer.php. The manipulation of the argument nama_customer/alamat_customer/notelp_customer leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-3614. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-3613	SourceCodester Warehouse Management System 1.0 supplier.php nama_supplier/alamat_supplier/notelp_supplier cross site scripting	A vulnerability was found in SourceCodester Warehouse Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		supplier.php. The manipulation of the argument nama_supplier/alamat_supplier/notelp_supplier leads to cross site scripting. This vulnerability is handled as CVE-2024-3613. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-3612	SourceCodester Warehouse Management System 1.0 barang.php nama_barang/merek cross site scripting	A vulnerability was found in SourceCodester Warehouse Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file barang.php. The manipulation of the argument nama_barang/merek leads to cross site scripting. This vulnerability is known as CVE-2024-3612. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-30884	Discuz X3.4 20220811 misc.php primarybegin cross site scripting (Issue 28)	A vulnerability was found in Discuz X3.4 20220811. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file misc.php. The manipulation of the argument primarybegin leads to cross site scripting. This vulnerability is known as CVE-2024-30884. The attack can be launched remotely. There is no exploit	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		available.		
CVE-2024-30880	RageFrame2 2.6.43 Image Crop cross site scripting (Issue 114)	A vulnerability has been found in RageFrame2 2.6.43 and classified as problematic. This vulnerability affects unknown code of the component Image Crop Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-30880. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-30883	RageFrame2 2.6.43 aspectRatio cross site scripting (Issue 114)	A vulnerability which was classified as problematic was found in RageFrame2 2.6.43. This affects an unknown part. The manipulation of the argument aspectRatio leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-30883. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-29504	Summernote up to 0.8.18 codeview cross site scripting	A vulnerability was found in Summernote up to 0.8.18. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument codeview leads to cross site scripting. This vulnerability is handled as CVE-2024-29504. The attack may be launched remotely. There is no exploit available. It is recommended to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		apply a patch to fix this issue.		
CVE-2024-30878	RageFrame2 2.6.43 upload_drive cross site scripting (Issue 111)	A vulnerability was found in RageFrame2 2.6.43 and classified as problematic. This issue affects some unknown processing. The manipulation of the argument upload_drive leads to cross site scripting. The identification of this vulnerability is CVE-2024-30878. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-30885	HadSky 7.6.3 chklogin.php cross site scripting (Issue 29)	A vulnerability classified as problematic has been found in HadSky 7.6.3. Affected is an unknown function of the file chklogin.php. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-30885. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-30879	RageFrame2 2.6.43 boxId cross site scripting (Issue 114)	A vulnerability was found in RageFrame2 2.6.43. It has been classified as problematic. Affected is an unknown function. The manipulation of the argument boxId leads to cross site scripting. This vulnerability is traded as CVE-2024-30879. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-3687	bihell Dice 3.1.0 Comment cross site scripting	A vulnerability was found in bihell Dice 3.1.0 and classified as problematic. Affected	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		by this issue is some unknown functionality of the component Comment Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-3687. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-30845	Rainbow External Link Network Disk 5.5 cross site scripting	A vulnerability has been found in Rainbow External Link Network Disk 5.5 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-2024-30845. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-3703	Carousel Slider Plugin up to 2.2.9 on WordPress cross site scripting	A vulnerability which was classified as problematic has been found in Carousel Slider Plugin up to 2.2.9 on WordPress. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-3703. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-3695	SourceCodester Computer Laboratory Management System 1.0 /classes/Users.php id cross site scripting	A vulnerability has been found in SourceCodester Computer Laboratory Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /classes/Users.php.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The manipulation of the argument id leads to cross site scripting. This vulnerability was named CVE-2024-3695. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-2583	WP Shortcodes Plugin up to 7.0.4 on WordPress Shortcode Attribute cross site scripting	A vulnerability has been found in WP Shortcodes Plugin up to 7.0.4 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-2583. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-3575	mindsdb cross site scripting	A vulnerability was found in mindsdb. 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-2024-3575. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-31648	Insurance Management System 1.0 /core/new_category 2 Category Name cross site scripting	A vulnerability was found in Insurance Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the file /core/new_category2. The manipulation of the argument Category Name leads to cross site scripting. This vulnerability is handled as CVE-2024-31648. The attack may be launched remotely. There is no exploit available.		
CVE-2024-31783	Typora up to 1.6.7 Markdown File Creation cross site scripting	A vulnerability was found in Typora up to 1.6.7. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Markdown File Creation Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-31783. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-31650	Cosmetics and Beauty Product Online Store 1.0 Last Name cross site scripting	A vulnerability which was classified as problematic has been found in Cosmetics and Beauty Product Online Store 1.0. Affected by this issue is some unknown functionality. The manipulation of the argument Last Name leads to cross site scripting. This vulnerability is handled as CVE-2024-31650. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-31651	Cosmetics and Beauty Product Online Store 1.0 First Name cross site scripting	A vulnerability has been found in Cosmetics and Beauty Product Online Store 1.0 and classified as problematic. This vulnerability affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown code. The manipulation of the argument First Name leads to cross site scripting. This vulnerability was named CVE-2024-31651. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-32743	WonderCMS 3.4.3 Security Module SITE LANGUAGE CONFIG cross site scripting	A vulnerability was found in WonderCMS 3.4.3. It has been classified as problematic. This affects an unknown part of the component Security Module. The manipulation of the argument SITE LANGUAGE CONFIG leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-32743. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-32746	WonderCMS 3.4.3 Menu Module MENU cross site scripting	A vulnerability was found in WonderCMS 3.4.3 and classified as problematic. Affected by this issue is some unknown functionality of the component Menu Module. The manipulation of the argument MENU leads to cross site scripting. This vulnerability is handled as CVE-2024-32746. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-32745	WonderCMS 3.4.3 Current Page Module PAGE DESCRIPTION cross site scripting	A vulnerability has been found in WonderCMS 3.4.3 and classified as problematic. Affected by this vulnerability is an unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		functionality of the component Current Page Module. The manipulation of the argument PAGE DESCRIPTION leads to cross site scripting. This vulnerability is known as CVE-2024-32745. The attack can be launched remotely. There is no exploit available.		
CVE-2024-32345	CMSimple 5.15 Language Section Configuration cross site scripting	A vulnerability which was classified as problematic has been found in CMSimple 5.15. This issue affects some unknown processing of the component Language Section. The manipulation of the argument Configuration leads to cross site scripting. The identification of this vulnerability is CVE-2024-32345. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-32744	WonderCMS 3.4.3 Current Page Module PAGE KEYWORDS cross site scripting	A vulnerability which was classified as problematic was found in WonderCMS 3.4.3. Affected is an unknown function of the component Current Page Module. The manipulation of the argument PAGE KEYWORDS leads to cross site scripting. This vulnerability is traded as CVE-2024-32744. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-32338	WonderCMS 3.4.3 Current Page Module PAGE TITLE cross site scripting	A vulnerability has been found in WonderCMS 3.4.3 and classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		problematic. This vulnerability affects unknown code of the component Current Page Module. The manipulation of the argument PAGE TITLE leads to cross site scripting. This vulnerability was named CVE-2024-32338. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-32344	CMSimple 5.15 Settings Menu Edit cross site scripting	A vulnerability classified as problematic was found in CMSimple 5.15. This vulnerability affects unknown code of the component Settings Menu. The manipulation of the argument Edit leads to cross site scripting. This vulnerability was named CVE-2024-32344. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-32339	WonderCMS 3.4.3 cross site scripting	A vulnerability was found in WonderCMS 3.4.3 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-32339. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-32342	Boid CMS 2.1.0 Permalink cross site scripting	A vulnerability was found in Boid CMS 2.1.0. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument Permalink leads to cross site scripting. This vulnerability is handled as CVE-2024-32342. The attack may be launched remotely. There is no exploit available.		
CVE-2024-32340	WonderCMS 3.4.3 Menu Module WEBSITE TITLE cross site scripting	A vulnerability was found in WonderCMS 3.4.3. It has been classified as problematic. Affected is an unknown function of the component Menu Module. The manipulation of the argument WEBSITE TITLE leads to cross site scripting. This vulnerability is traded as CVE-2024-32340. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-32343	Boid CMS 2.1.0 Content cross site scripting	A vulnerability classified as problematic has been found in Boid CMS 2.1.0. This affects an unknown part. The manipulation of the argument Content leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-32343. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-32337	WonderCMS 3.4.3 ADMIN LOGIN URL cross site scripting	A vulnerability which was classified as problematic was found in WonderCMS 3.4.3. This affects an unknown part. The manipulation of the argument ADMIN LOGIN URL leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is uniquely identified as CVE-2024-32337. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-30953	Htmly 2.9.5 Menu Editor Module Link Name cross site scripting	A vulnerability which was classified as problematic has been found in Htmly 2.9.5. Affected by this issue is some unknown functionality of the component Menu Editor Module. The manipulation of the argument Link Name leads to cross site scripting. This vulnerability is handled as CVE-2024-30953. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-30951	FUDforum 3.1.3 /adm/admsmiley.php chpos cross site scripting	A vulnerability classified as problematic was found in FUDforum 3.1.3. Affected by this vulnerability is an unknown functionality of the file /adm/admsmiley.php. The manipulation of the argument chpos leads to cross site scripting. This vulnerability is known as CVE-2024-30951. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-30950	FUDforum 3.1.3 /adm/admsql.php statements cross site scripting	A vulnerability was found in FUDforum 3.1.3. It has been declared as problematic. This vulnerability affects unknown code of the file /adm/admsql.php. The manipulation of the argument statements leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross site scripting. This vulnerability was named CVE-2024-30950. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-30952	PESCMS-TEAM 2.3.6 domain cross site scripting	A vulnerability classified as problematic was found in PESCMS-TEAM 2.3.6. This vulnerability affects unknown code of the file /youdoamin/gTeam&mSetting&action. The manipulation of the argument domain leads to cross site scripting. This vulnerability was named CVE-2024-30952. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-2729	Otter Blocks Plugin up to 2.6.5 on WordPress cross site scripting	A vulnerability was found in Otter Blocks Plugin up to 2.6.5 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-2024-2729. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-2761	Genesis Blocks Plugin up to 3.1.2 on WordPress cross site scripting	A vulnerability has been found in Genesis Blocks Plugin up to 3.1.2 on WordPress and classified as problematic. This vulnerability affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-2761. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-27752	CSZ CMS 1.3.0 settings Default Keyword cross site scripting	A vulnerability classified as problematic has been found in CSZ CMS 1.3.0. This affects the function settings. The manipulation of the argument Default Keyword leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-27752. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-30886	HadSky 7.6.3 remotelink url cross site scripting (Issue 30)	A vulnerability classified as problematic has been found in HadSky 7.6.3. Affected is the function remotelink. The manipulation of the argument url leads to cross site scripting. This vulnerability is traded as CVE-2024-30886. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-2972	Floating Chat Widget Plugin up to 3.1.8 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic was found in Floating Chat Widget Plugin up to 3.1.8 on WordPress. Affected is an unknown function of the component Setting Handler. The manipulation leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross site scripting. This vulnerability is traded as CVE-2024-2972. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-1743	WooCommerce Customers Manager Plugin up to 29.7 on WordPress cross site scripting	A vulnerability classified as problematic has been found in WooCommerce Customers Manager Plugin up to 29.7 on WordPress. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-1743. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-2402	Better Comments Plugin up to 1.5.5 on WordPress Setting cross site scripting	A vulnerability classified as problematic was found in Better Comments Plugin up to 1.5.5 on WordPress. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-2402. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-2907	AGCA Plugin up to 7.2.1 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic has been found in AGCA Plugin up to 7.2.1 on WordPress. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-2907. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-31609	BOSSCMS 3.10 Code Configuration cross site scripting	A vulnerability which was classified as problematic was found in BOSSCMS 3.10. Affected is an unknown function of the component Code Configuration Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-31609. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-31574	TWCMS 2.6 cross site scripting	A vulnerability has been found in TWCMS 2.6 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-31574. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y

INDUSFACE™

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 a “Great Place to Work” 2022 Winner in the Mid-Size category in India and is PCI, ISO27001, SOC 2, GDPR certified and has been the recipient of many prestigious start-up awards.

Indusface is the only cloud WAAP (WAF) vendor with 100% customer recommendation for 4 consecutive years

A Customers' Choice from 2022 to 2024 Gartner® Peer Insights™