INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

November 2024

The total **zero-day vulnerabilities** count for November month: 182

Command Injection	SQL Injection	Local File Inclusion	Cross-Site Scripting
17	99	5	61

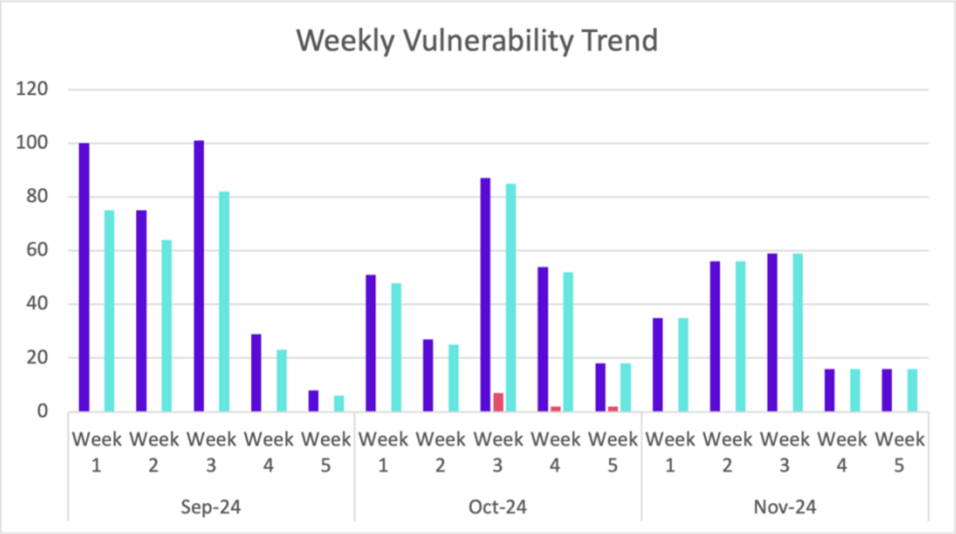
Zero-day vulnerabilities protected through core rules	182
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities found by Indusface WAS	182

- To enable custom rules, please contact support@indusface.com
- Learn more about zero-day vulnerabilities, detection, and prevention, here

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



🟪 Total Blocked/Logged Web AppSec Zero-Day Vulnerabilities by Core Rules

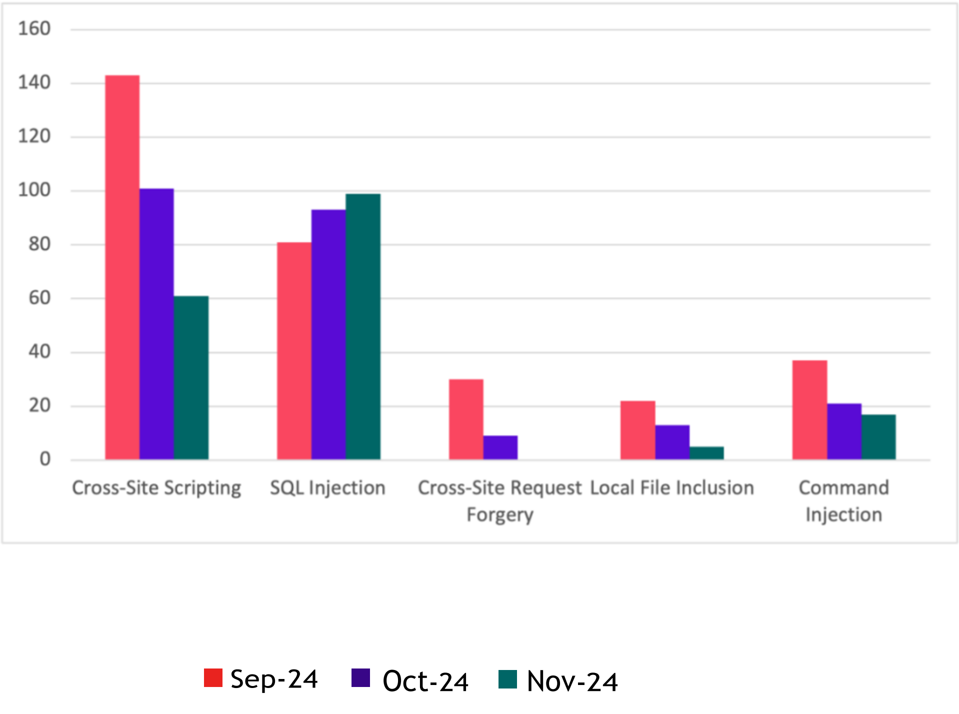
🟩 Total Custom Patch Required for Web AppSec Zero-Day Vulnerabilities

🟦 Total Zero-Day Vulnerabilities found by Indusface Scanner

of the zero-day vulnerabilities were protected by the core 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-2024-50498	WordPress WP Query Console plugin <= 1.0 - Remote Code Execution (RCE) vulnerability	Improper Control of Generation of Code ('Code Injection') vulnerability in LUBUS WP Query Console allows Code Injection.This issue affects WP Query Console: from n/a through 1.0.	Patched by core rule	Y
CVE-2024-51735	Stored Cross-site Scripting to RCE on Osmedeus Web Server	Osmedeus is a Workflow Engine for Offensive Security. Cross-site Scripting (XSS) occurs on the Osmedues web server when viewing results from the workflow, allowing commands to be executed on the server. When using a workflow that contains the summary module, it generates reports in HTML and Markdown formats. The default report is based on the `general-template.md` template.The contents of the files are read and used to generate the report. However, the file contents are not properly filtered, leading to XSS. This may lead to commands executed on the host as well. This issue is not yet resolved. Users are advised to add their own filtering or to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		reach out to the developer to aid in developing a patch.		
CVE-2024-10914	D-Link DNS-320/DNS-320LW/DNS-325/DNS-340L account_mgr.cgi cgi_user_add os command injection	A vulnerability was found in D-Link DNS-320, DNS-320LW, DNS-325 and DNS-340L up to 20241028. It has been declared as critical. Affected by this vulnerability is the function cgi_user_add of the file /cgi-bin/account_mgr.cgi?cmd=cgi_user_add. The manipulation of the argument name leads to os command injection. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10919	didi Super-Jacoco triggerUnitCover os command injection	A vulnerability has been found in didi Super-Jacoco 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /cov/triggerUnitCover. The manipulation of the argument uuid leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10966	TOTOLINK X18 cstecgi.cgi os command injection	A vulnerability, which was classified as critical, has been found in TOTOLINK X18 9.1.0cu.2024_B20220329. Affected by this issue is some unknown functionality of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument enable leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11046	D-Link DI-8003 upgrade_filter.asp upgrade_filter_asp os command injection	A vulnerability was found in D-Link DI-8003 16.07.16A1. It has been classified as critical. Affected is the function upgrade_filter_asp of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the file /upgrade_filter.asp. The manipulation of the argument path leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-49379	Remote Code Execution (RCE) via Cross-Site Scripting (XSS) in Umbrel	Umbrel is a home server OS for self-hosting. The login functionality of Umbrel before version 1.2.2 contains a reflected cross-site scripting (XSS) vulnerability in use-auth.tsx. An attacker can specify a malicious redirect query parameter to trigger the vulnerability. If a JavaScript URL is passed to the redirect parameter the attacker provided JavaScript will be executed after the user entered their password and clicked on login. This vulnerability is fixed in 1.2.2.	Patched by core rule	Y
CVE-2024-52803	LLama Factory Remote OS Command Injection Vulnerability	LLama Factory enables fine-tuning of large language models. A critical remote OS command injection vulnerability has been identified in the LLama Factory training process. This vulnerability arises from improper handling of user input, allowing malicious actors to execute arbitrary OS commands on the host system. The issue is caused by insecure usage of the `Popen` function with `shell=True`, coupled with unsanitized user input. Immediate remediation is required to mitigate the risk. This vulnerability is fixed in 0.9.1.	Patched by core rule	Y
CVE-2024-11665	Unauthenticated Remote Command Injection	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in hardy-barth cph2_echarge_firmware allows OS Command	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Injection.This issue affects cph2_echarge_firmware: through 2.0.4.		
CVE-2024-11651	EnGenius ENH1350EXT/ENS500-AC/ENS620EXT wifi_schedule command injection	A vulnerability was found in EnGenius ENH1350EXT, ENS500-AC and ENS620EXT up to 20241118. It has been classified as critical. Affected is an unknown function of the file /admin/network/wifi_schedule. The manipulation of the argument wifi_schedule_day_em_5 leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-11653	EnGenius ENH1350EXT/ENS500-AC/ENS620EXT diag_traceroute command injection	A vulnerability was found in EnGenius ENH1350EXT, ENS500-AC and ENS620EXT up to 20241118. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/network/diag_traceroute. The manipulation of the argument diag_traceroute leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-11654	EnGenius ENH1350EXT/ENS500-AC/ENS620EXT diag_traceroute6 command injection	A vulnerability classified as critical has been found in EnGenius ENH1350EXT, ENS500-AC and ENS620EXT up to 20241118. This affects an unknown part of the file /admin/network/diag_traceroute6. The manipulation of the argument diag_traceroute6 leads to command injection. It is possible to initiate the attack remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-11655	EnGenius ENH1350EXT/ENS500-AC/ENS620EXT diag_pinginterface command injection	A vulnerability classified as critical was found in EnGenius ENH1350EXT, ENS500-AC and ENS620EXT up to 20241118. This vulnerability affects unknown code of the file /admin/network/diag_pinginterface. The manipulation of the argument diag_ping leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-11656	EnGenius ENH1350EXT/ENS500-AC/ENS620EXT diag_ping6 command injection	A vulnerability, which was classified as critical, has been found in EnGenius ENH1350EXT, ENS500-AC and ENS620EXT up to 20241118. This issue affects some unknown processing of the file /admin/network/diag_ping6. The manipulation of the argument diag_ping6 leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-11657	EnGenius ENH1350EXT/ENS500-AC/ENS620EXT diag_nslookup command injection	A vulnerability, which was classified as critical, was found in EnGenius ENH1350EXT, ENS500-AC and ENS620EXT up to 20241118. Affected is an unknown function of the file /admin/network/diag_nslookup. The manipulation of the argument diag_nslookup leads to command injection. It	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-11658	EnGenius ENH1350EXT/ENS500-AC/ENS620EXT ajax_getChannelList command injection	A vulnerability has been found in EnGenius ENH1350EXT, ENS500-AC and ENS620EXT up to 20241118 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/network/ajax_getChannelList. The manipulation of the argument countryCode leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-11659	EnGenius ENH1350EXT/ENS500-AC/ENS620EXT diag_iperf command injection	A vulnerability was found in EnGenius ENH1350EXT, ENS500-AC and ENS620EXT up to 20241118 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/network/diag_iperf. The manipulation of the argument iperf leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-7475	Improper Access Control in lunary-ai/lunary	An improper access control vulnerability in lunary-ai/lunary version 1.3.2 allows an attacker to update the SAML configuration without authorization. This vulnerability can lead to manipulation of authentication processes, fraudulent login requests, and theft of user information. Appropriate access controls should be implemented to ensure that the SAML configuration can only be updated by authorized users.	Patched by core rule	Y
CVE-2024-11123	Lingdang CRM pdf.php path traversal	A vulnerability, which was classified as problematic, was found in Lingdang CRM up to 8.6.4.3. This affects an unknown part of the file /crm/data/pdf.php. The manipulation of the argument url with the input ../config.inc.php leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-11210	EyouCMS FilemanagerLogic.php editFile path traversal	A vulnerability was found in EyouCMS 1.51. It has been rated as critical. This issue affects the function editFile of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		application/admin/logic/FilemanagerLogic.php. The manipulation of the argument activepath leads to path traversal. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-11238	Landray EKP sysUiComponent.do delPreviewFile path traversal	A vulnerability, which was classified as critical, was found in Landray EKP up to 16.0. This affects the function delPreviewFile of the file /sys/ui/sys_ui_component/sysUiComponent.do?method=delPreviewFile. The manipulation of the argument directoryPath leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-11239	Landray EKP API Interface import.do deleteFile path traversal	A vulnerability has been found in Landray EKP up to 16.0 and classified as critical. This vulnerability affects the function deleteFile of the file /sys/common/import.do?method=deleteFile of the component API Interface. The manipulation of the argument folder leads to path traversal. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-10408	code-projects Blood Bank Management abs.php sql injection	A vulnerability has been found in code-projects Blood Bank Management up to 1.0 and classified as critical. This vulnerability affects unknown code of the file /abs.php. The manipulation of the argument search leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10409	code-projects Blood Bank Management accept.php sql injection	A vulnerability was found in code-projects Blood Bank Management 1.0 and classified as critical. This issue affects some unknown processing of the file /file/accept.php. The manipulation of the argument reqid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10415	code-projects Blood Bank Management System accept.php sql injection	A vulnerability has been found in code-projects Blood Bank Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /file/accept.php. The manipulation of the argument reqid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10416	code-projects Blood Bank Management System cancel.php	A vulnerability was found in code-projects Blood Bank	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	sql injection	Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /file/cancel.php. The manipulation of the argument reqid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-10417	code-projects Blood Bank Management System delete.php sql injection	A vulnerability was found in code-projects Blood Bank Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /file/delete.php. The manipulation of the argument bid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10418	code-projects Blood Bank Management System infoAdd.php sql injection	A vulnerability was found in code-projects Blood Bank Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /file/infoAdd.php. The manipulation of the argument bg leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10423	Project Worlds Student Project Allocation System Project Selection Page project_selection.ph	A vulnerability, which was classified as critical, was found in Project Worlds Student Project Allocation System 1.0. Affected is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	p sql injection	an unknown function of the file /student/project_selection/project_selection.php of the component Project Selection Page. The manipulation of the argument project_id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-10424	Project Worlds Student Project Allocation System Project Selection Page remove_project.php sql injection	A vulnerability has been found in Project Worlds Student Project Allocation System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /student/project_selection/remove_project.php of the component Project Selection Page. The manipulation of the argument no leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10425	Project Worlds Student Project Allocation System Project Selection Page move_up_project.php sql injection	A vulnerability was found in Project Worlds Student Project Allocation System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /student/project_selection/move_up_project.php of the component Project Selection Page. The manipulation of the argument up leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-10426	Codezips Pet Shop Management System animalsadd.php sql injection	A vulnerability was found in Codezips Pet Shop Management System 1.0. It has been classified as critical. This affects an unknown part of the file /animalsadd.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions the parameter "refno" to be affected. But further inspection indicates that the name of the affected parameter is "id".	Patched by core rule	Y
CVE-2024-10427	Codezips Pet Shop Management System deleteanimal.php sql injection	A vulnerability was found in Codezips Pet Shop Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /deleteanimal.php. The manipulation of the argument t1 leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions the parameter "refno" to be affected. But further inspection indicates that the name of the affected parameter is "t1".	Patched by core rule	Y
CVE-2024-10430	Codezips Pet Shop Management System animalsupdate.php sql injection	A vulnerability, which was classified as critical, has been found in Codezips Pet Shop Management System 1.0. This issue affects some unknown processing of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/animalsupdate.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-10431	Codezips Pet Shop Management System deletebird.php sql injection	A vulnerability, which was classified as critical, was found in Codezips Pet Shop Management System 1.0. Affected is an unknown function of the file /deletebird.php. The manipulation of the argument t1 leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10432	Project Worlds Simple Web-Based Chat Application index.php sql injection	A vulnerability has been found in Project Worlds Simple Web-Based Chat Application 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /index.php. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10446	Project Worlds Online Time Table Generator admindashboard.php sql injection	A vulnerability classified as critical has been found in Project Worlds Online Time Table Generator 1.0. Affected is an unknown function of the file /timetable/admin/admindashboard.php?info=add_course. The manipulation of the argument c leads to sql	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-10447	Project Worlds Online Time Table Generator staffdashboard.php sql injection	A vulnerability classified as critical was found in Project Worlds Online Time Table Generator 1.0. Affected by this vulnerability is an unknown functionality of the file /timetable/staff/staffdashboard.php?info=updateprofile. The manipulation of the argument n leads to sql injection. The attack can be launched remotely.	Patched by core rule	Y
CVE-2024-10449	Codezips Hospital Appointment System loginAction.php sql injection	A vulnerability, which was classified as critical, was found in Codezips Hospital Appointment System 1.0. This affects an unknown part of the file /loginAction.php. The manipulation of the argument Username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10450	SourceCodester Kortex Lite Advocate Office Management System POST Parameter edit_profile.php sql injection	A vulnerability has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /kortex_lite/control/edit_profile.php of the component POST Parameter Handler. The manipulation of the argument id leads to sql injection. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-10506	code-projects Blood Bank System B-.php sql injection	A vulnerability classified as critical has been found in code-projects Blood Bank System 1.0. This affects an unknown part of the file /admin/blood/update/B-.php. The manipulation of the argument Bloodname leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10507	Codezips Free Exam Hall Seating Management System login.php sql injection	A vulnerability classified as critical was found in Codezips Free Exam Hall Seating Management System 1.0. This vulnerability affects unknown code of the file /login.php. The manipulation of the argument email leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10509	Codezips Online Institute Management System login.php sql injection	A vulnerability, which was classified as critical, has been found in Codezips Online Institute Management System 1.0. This issue affects some unknown processing of the file /login.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10556	Codezips Pet Shop	A vulnerability, which	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Management System birdsadd.php sql injection	was classified as critical, was found in Codezips Pet Shop Management System 1.0. Affected is an unknown function of the file birdsadd.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	core rule	
CVE-2024-10561	Codezips Pet Shop Management System birdsupdate.php sql injection	A vulnerability was found in Codezips Pet Shop Management System 1.0. It has been classified as critical. This affects an unknown part of the file birdsupdate.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10607	code-projects Courier Management System track-result.php sql injection	A vulnerability was found in code-projects Courier Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /track-result.php. The manipulation of the argument Consignment leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10608	code-projects Courier Management System login.php sql injection	A vulnerability was found in code-projects Courier Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /login.php. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument txtusername leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-10609	itsourcecode Tailoring Management System Project typeadd.php sql injection	A vulnerability, which was classified as critical, was found in itsourcecode Tailoring Management System Project 1.0. This affects an unknown part of the file typeadd.php. The manipulation of the argument sex leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10699	code-projects Wazifa System logincontrol.php sql injection	A vulnerability was found in code-projects Wazifa System 1.0. It has been classified as critical. This affects an unknown part of the file /controllers/logincontrol.php. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10700	code-projects University Event Management System submit.php sql injection	A vulnerability was found in code-projects University Event Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file submit.php. The manipulation of the argument name/email/title/Year/gender/fromdate/todate/people leads to sql injection. The attack	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		can be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "name" to be affected. But it must be assumed that a variety of other parameters is affected too.		
CVE-2024-10702	code-projects Simple Car Rental System signup.php sql injection	A vulnerability classified as critical has been found in code-projects Simple Car Rental System 1.0. Affected is an unknown function of the file /signup.php. The manipulation of the argument fname leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10733	code-projects Restaurant Order System login.php sql injection	A vulnerability was found in code-projects Restaurant Order System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /login.php. The manipulation of the argument uid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10734	Project Worlds Life Insurance Management System editPayment.php sql injection	A vulnerability was found in Project Worlds Life Insurance Management System 1.0. It has been classified as critical. This affects an unknown part of the file /editPayment.php. The manipulation of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the argument recipt_no leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-10735	Project Worlds Life Insurance Management System editNominee.php sql injection	A vulnerability was found in Project Worlds Life Insurance Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /editNominee.php. The manipulation of the argument nominee_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10736	Codezips Free Exam Hall Seating Management System student.php sql injection	A vulnerability was found in Codezips Free Exam Hall Seating Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /student.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10737	Codezips Free Exam Hall Seating Management System teacher.php sql injection	A vulnerability classified as critical has been found in Codezips Free Exam Hall Seating Management System 1.0. Affected is an unknown function of the file /teacher.php. The manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The exploit has been disclosed to the public and may be used.		
CVE-2024-10738	itsourcecode Farm Management System manage-breed.php sql injection	A vulnerability classified as critical was found in itsourcecode Farm Management System 1.0. Affected by this vulnerability is an unknown functionality of the file manage-breed.php. The manipulation of the argument breed leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10742	code-projects Wazifa System control.php sql injection	A vulnerability was found in code-projects Wazifa System 1.0 and classified as critical. This issue affects some unknown processing of the file /controllers/control.php. The manipulation of the argument to leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10751	Codezips ISP Management System pay.php sql injection	A vulnerability was found in Codezips ISP Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file pay.php. The manipulation of the argument customer leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10752	Codezips Pet Shop Management System productsadd.php sql	A vulnerability was found in Codezips Pet Shop Management System 1.0. It has been	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	classified as critical. This affects an unknown part of the file /productsadd.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions contradicting file names to be affected.		
CVE-2024-10758	code-projects/anirbandutta9 Content Management System/News-Buzz index.php sql injection	A vulnerability, which was classified as critical, was found in code-projects/anirbandutta9 Content Management System and News-Buzz 1.0. This affects an unknown part of the file /index.php. The manipulation of the argument user_name leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This product is distributed under two entirely different names.	Patched by core rule	Y
CVE-2024-10759	itsourcecode Farm Management System edit-pig.php sql injection	A vulnerability has been found in itsourcecode Farm Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /edit-pig.php. The manipulation of the argument pigno/weight/arrived/breed/remark/status leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		advisory only mentions the parameter "pigno" to be affected. But it must be assumed that other parameters are affected as well.		
CVE-2024-10760	code-projects University Event Management System dodelete.php sql injection	A vulnerability was found in code-projects University Event Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /dodelete.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10791	Codezips Hospital Appointment System doctorAction.php sql injection	A vulnerability, which was classified as critical, has been found in Codezips Hospital Appointment System 1.0. This issue affects some unknown processing of the file /doctorAction.php. The manipulation of the argument Name leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions contradicting file and parameter names to be affected.	Patched by core rule	Y
CVE-2024-10805	code-projects University Event Management System doedit.php sql injection	A vulnerability was found in code-projects University Event Management System 1.0. It has been classified as critical. This affects an unknown part of the file doedit.php. The manipulation of the argument id leads to sql injection. It is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions a confusing product name to be affected. Other parameters might be affected as well.		
CVE-2024-10808	code-projects E-Health Care System req_detail.php sql injection	A vulnerability has been found in code-projects E-Health Care System 1.0 and classified as critical. This vulnerability affects unknown code of the file Admin/req_detail.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10809	code-projects E-Health Care System chat.php sql injection	A vulnerability was found in code-projects E-Health Care System 1.0 and classified as critical. This issue affects some unknown processing of the file /Doctor/chat.php. The manipulation of the argument name/message leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "name" to be affected. But it must be assumed that the parameter "message" is affected as well.	Patched by core rule	Y
CVE-2024-10810	code-projects E-Health Care System app_request.php sql	A vulnerability was found in code-projects E-Health Care System	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	1.0. It has been classified as critical. Affected is an unknown function of the file Doctor/app_request.php. The manipulation of the argument app_id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-10841	romadebrian WEB-Sekolah Mail Proses_Kirim.php sql injection	A vulnerability classified as critical was found in romadebrian WEB-Sekolah 1.0. Affected by this vulnerability is an unknown functionality of the file /Proses_Kirim.php of the component Mail Handler. The manipulation of the argument Name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2024-10844	1000 Projects Bookstore Management System search.php sql injection	A vulnerability, which was classified as critical, was found in 1000 Projects Bookstore Management System 1.0. This affects an unknown part of the file search.php. The manipulation of the argument s leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10845	1000 Projects Bookstore Management System book_detail.php sql	A vulnerability has been found in 1000 Projects Bookstore Management System 1.0 and classified 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 book_detail.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-10967	code-projects E-Health Care System delete_user_appointment_request.php sql injection	A vulnerability was found in code-projects E-Health Care System 1.0. It has been classified as critical. Affected is an unknown function of the file /Doctor/delete_user_appointment_request.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10987	code-projects E-Health Care System user_appointment.php sql injection	A vulnerability was found in code-projects E-Health Care System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /Doctor/user_appointment.php. The manipulation of the argument schedule_id/schedule_date/schedule_day/start_time/end_time/booking leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10988	code-projects E-Health Care System doctor_login.php sql injection	A vulnerability was found in code-projects E-Health Care System 1.0. It has been rated	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		as critical. Affected by this issue is some unknown functionality of the file /Doctor/doctor_login.php. The manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.		
CVE-2024-10989	code-projects E-Health Care System detail.php sql injection	A vulnerability classified as critical has been found in code-projects E-Health Care System 1.0. This affects an unknown part of the file /Admin/detail.php. The manipulation of the argument s_id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory confuses the vulnerability class of this issue.	Patched by core rule	Y
CVE-2024-10990	SourceCodester Online Veterinary Appointment System view_service.php sql injection	A vulnerability classified as critical was found in SourceCodester Online Veterinary Appointment System 1.0. This vulnerability affects unknown code of the file /admin/services/view_service.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10991	Codezips Hospital Appointment System	A vulnerability, which was classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	editBranchResult.php sql injection	critical, has been found in Codezips Hospital Appointment System 1.0. This issue affects some unknown processing of the file /editBranchResult.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-10995	Codezips Hospital Appointment System removeDoctorResult.php sql injection	A vulnerability was found in Codezips Hospital Appointment System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /removeDoctorResult.php. The manipulation of the argument Name leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10996	1000 Projects Bookstore Management System process_category_edit.php sql injection	A vulnerability was found in 1000 Projects Bookstore Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/process_category_edit.php. The manipulation of the argument cat leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10997	1000 Projects Bookstore Management System book_list.php sql	A vulnerability was found in 1000 Projects Bookstore Management System 1.0. It has been	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	declared as critical. This vulnerability affects unknown code of the file /book_list.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-10998	1000 Projects Bookstore Management System process_category_add.php sql injection	A vulnerability was found in 1000 Projects Bookstore Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/process_category_add.php. The manipulation of the argument cat leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11055	1000 Projects Beauty Parlour Management System admin-profile.php sql injection	A vulnerability, which was classified as critical, has been found in 1000 Projects Beauty Parlour Management System 1.0. This issue affects some unknown processing of the file /admin/admin-profile.php. The manipulation of the argument adminname leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11057	Codezips Hospital Appointment System removeBranchResult.php sql injection	A vulnerability has been found in Codezips Hospital Appointment System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the file /removeBranchResult.php. The manipulation of the argument ID/Name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-11058	CodeAstro Real Estate Management System About Us Page aboutedit.php sql injection	A vulnerability was found in CodeAstro Real Estate Management System up to 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /aboutedit.php of the component About Us Page. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11060	Jinher Network Collaborative Management Platform 金和数字化智能办公平台 AcceptShow.aspx sql injection	A vulnerability classified as critical has been found in Jinher Network Collaborative Management Platform 金和数字化智能办公平台 1.0. Affected is an unknown function of the file /C6/JHSoft.Web.AcceptAip/AcceptShow.aspx/. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11074	itsourcecode Tailoring Management System incadd.php sql injection	A vulnerability classified as critical was found in itsourcecode Tailoring Management System 1.0. This vulnerability affects unknown code of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file /incadd.php. The manipulation of the argument inccat/desc/date/amount leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "inccat" to be affected. But it must be assumed "desc", "date", and "amount" are affected as well.		
CVE-2024-11076	code-projects Job Recruitment activation.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Job Recruitment 1.0. This issue affects some unknown processing of the file /activation.php. The manipulation of the argument e_hash leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11077	code-projects Job Recruitment index.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Job Recruitment 1.0. Affected is an unknown function of the file /index.php. The manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11096	code-projects Task Manager newProject.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Task Manager 1.0. This affects an unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		part of the file /newProject.php. The manipulation of the argument projectName leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-11099	code-projects Job Recruitment login.php sql injection	A vulnerability was found in code-projects Job Recruitment 1.0 and classified as critical. This issue affects some unknown processing of the file /login.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11100	1000 Projects Beauty Parlour Management System index.php sql injection	A vulnerability was found in 1000 Projects Beauty Parlour Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /index.php. The manipulation of the argument name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11101	1000 Projects Beauty Parlour Management System search-invoices.php sql injection	A vulnerability was found in 1000 Projects Beauty Parlour Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/search-invoices.php. The manipulation of the argument searchdata	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-11121	上海灵当信息科技有限公司 Lingdang CRM index.php sql injection	A vulnerability classified as critical was found in 上海灵当信息科技有限公司 Lingdang CRM up to 8.6.4.3. Affected by this vulnerability is an unknown functionality of the file /crm/WeiXinApp/marketing/index.php?module=Users&action=getActionList. The manipulation of the argument userid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-11124	TimGeyssens UIOMatic uioMaticObject.r sql injection	A vulnerability has been found in TimGeyssens UIOMatic 5 and classified as critical. This vulnerability affects unknown code of the file /src/UIOMatic/wwwroot/backoffice/resources/uioMaticObject.r. The manipulation leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11127	code-projects Job Recruitment admin.php sql injection	A vulnerability was found in code-projects Job Recruitment up to 1.0. It has been declared as critical. Affected by this vulnerability is an	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown functionality of the file admin.php. The manipulation of the argument userid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-43415	Decidim-Awesome: SQL injection in AdminAccountability	An improper neutralization of special elements used in an SQL command in the papertrail/version-model of the decidim_awesome-module <= v0.11.1 (> 0.9.0) allows an authenticated admin user to manipulate sql queries to disclose information, read and write files or execute commands.	Patched by core rule	Y
CVE-2024-11212	SourceCodester Best Employee Management System fetch_product_details.php sql injection	A vulnerability, which was classified as critical, has been found in SourceCodester Best Employee Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/fetch_product_details.php. The manipulation of the argument barcode leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11213	SourceCodester Best Employee Management System edit_role.php sql injection	A vulnerability, which was classified as critical, was found in SourceCodester Best Employee Management System 1.0. This affects an unknown part of the file /admin/edit_role.php. The manipulation of the argument id leads	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-11241	code-projects Job Recruitment reset.php sql injection	A vulnerability was found in code-projects Job Recruitment 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file reset.php. The manipulation of the argument e leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11242	ZZCMS Keyword Filtering ad_list.php sql injection	A vulnerability was found in ZZCMS 2023. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/ad_list.php?action=pass of the component Keyword Filtering. The manipulation of the argument keyword leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11244	code-projects Farmacia editar-cliente.php sql injection	A vulnerability classified as critical was found in code-projects Farmacia 1.0. This vulnerability affects unknown code of the file /editar-cliente.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11245	code-projects	A vulnerability, which	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Farmacia editar-produto.php sql injection	was classified as critical, has been found in code-projects Farmacia 1.0. This issue affects some unknown processing of the file /editar-produto.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	core rule	
CVE-2024-11250	code-projects Inventory Management editProduct.php sql injection	A vulnerability was found in code-projects Inventory Management up to 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /model/editProduct.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11251	erzhongxmu Jeewms AuthInterceptor cgReportController.do sql injection	A vulnerability was found in erzhongxmu Jeewms up to 20241108. It has been rated as critical. This issue affects some unknown processing of the file cgReportController.do of the component AuthInterceptor. The manipulation of the argument begin_date leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. Other	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		parameters might be affected as well.		
CVE-2024-11256	1000 Projects Portfolio Management System MCA login.php sql injection	A vulnerability was found in 1000 Projects Portfolio Management System MCA 1.0 and classified as critical. This issue affects some unknown processing of the file /login.php. The manipulation of the argument username leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11257	1000 Projects Beauty Parlour Management System forgot-password.php sql injection	A vulnerability classified as critical has been found in 1000 Projects Beauty Parlour Management System 1.0. This affects an unknown part of the file /admin/forgot-password.php. The manipulation of the argument email leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11258	1000 Projects Beauty Parlour Management System index.php sql injection	A vulnerability classified as critical was found in 1000 Projects Beauty Parlour Management System 1.0. This vulnerability affects unknown code of the file /admin/index.php. The manipulation of the argument username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-9887	Login using WordPress Users (WP as SAML IDP) <= 1.15.6 -	The Login using WordPress Users (WP as SAML IDP) plugin for WordPress is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Authenticated (Administrator+) SQL Injection	vulnerable to time-based SQL Injection via the 'id' parameter in all versions up to, and including, 1.15.6 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.		
CVE-2024-11305	Altenergy Power Control Software status_zigbee get_status_zigbee sql injection	A vulnerability classified as critical was found in Altenergy Power Control Software up to 20241108. This vulnerability affects the function get_status_zigbee of the file /index.php/display/status_zigbee. The manipulation of the argument date leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-11589	itsourcecode Tailoring Management System expcatedit.php sql injection	A vulnerability classified as critical was found in itsourcecode Tailoring Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /expcatedit.php. The manipulation of the argument id leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-11590	1000 Projects Bookstore Management System forget_password_process.php sql injection	A vulnerability, which was classified as critical, has been found in 1000 Projects Bookstore Management System 1.0. Affected by this issue is some unknown functionality of the file /forget_password_process.php. The manipulation of the argument unm leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11591	1000 Projects Beauty Parlour Management System add-services.php sql injection	A vulnerability, which was classified as critical, was found in 1000 Projects Beauty Parlour Management System 1.0. This affects an unknown part of the file /admin/add-services.php. The manipulation of the argument sername leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11592	1000 Projects Beauty Parlour Management System about-us.php sql injection	A vulnerability has been found in 1000 Projects Beauty Parlour Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/about-us.php. The manipulation of the argument pagetitle leads to sql injection. The attack can be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2023-7299	DataGear resolveSql sql injection	A vulnerability was found in DataGear up to 4.60. It has been declared as critical. This vulnerability affects unknown code of the file /dataSet/resolveSql. The manipulation of the argument sql leads to sql injection. The attack can be initiated remotely. Upgrading to version 4.7.0 is able to address this issue. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-11631	itsourcecode Tailoring Management System expedit.php sql injection	A vulnerability was found in itsourcecode Tailoring Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /expedit.php. The manipulation of the argument expcat leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11632	code-projects Simple Car Rental System book_car.php sql injection	A vulnerability was found in code-projects Simple Car Rental System 1.0. It has been classified as critical. Affected is an unknown function of the file /book_car.php. The manipulation of the argument fname/id_no/gender/email/phone/location leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		initial researcher advisory only mentions the parameter "fname" to be affected. Further analysis indicates that other arguments might be affected as well.		
CVE-2024-11646	1000 Projects Beauty Parlour Management System edit-services.php sql injection	A vulnerability classified as critical was found in 1000 Projects Beauty Parlour Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/edit-services.php. The manipulation of the argument sername leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11647	1000 Projects Beauty Parlour Management System view-appointment.php sql injection	A vulnerability, which was classified as critical, has been found in 1000 Projects Beauty Parlour Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/view-appointment.php. The manipulation of the argument viewid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11648	1000 Projects Beauty Parlour Management System add-customer.php sql injection	A vulnerability, which was classified as critical, was found in 1000 Projects Beauty Parlour Management System 1.0. This affects an unknown part of the file /admin/add-customer.php. The manipulation of the argument name leads to sql injection. It is possible to initiate the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-11649	1000 Projects Beauty Parlour Management System search-appointment.php sql injection	A vulnerability has been found in 1000 Projects Beauty Parlour Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/search-appointment.php. The manipulation of the argument searchdata leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11663	Codezips E-Commerce Site search.php sql injection	A vulnerability classified as critical was found in Codezips E-Commerce Site 1.0. Affected by this vulnerability is an unknown functionality of the file search.php. The manipulation of the argument keywords leads to sql injection. The attack can be launched remotely. The exploit has disclosed to the public and may be used.	Patched by core rule	Y

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-10414	PHPGurukul Vehicle Record System edit-brand.php cross site scripting	A vulnerability, which was classified as problematic, was found in PHPGurukul Vehicle Record System 1.0. This affects an unknown part of the file /admin/edit-brand.php. The manipulation of the argument Brand Name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions the parameter "phone_number" to be affected. But this might be a mistake because the textbox field label is "Brand Name".	Patched by core rule	Y
CVE-2024-10419	code-projects Blood Bank Management System bloodrequest.php cross site scripting	A vulnerability was found in code-projects Blood Bank Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /bloodrequest.php. The manipulation of the argument msg leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10433	Project Worlds Simple Web-Based Chat Application index.php cross site scripting	A vulnerability was found in Project Worlds Simple Web-Based Chat Application 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /index.php. The manipulation of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the argument Name/Comment leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions different parameters to be affected which do not correlate with the screenshots of a successful attack.		
CVE-2024-10701	PHPGurukul Car Rental Portal search.php cross site scripting	A vulnerability was found in PHPGurukul Car Rental Portal 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /search.php. The manipulation of the argument searchdata leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10743	PHPGurukul Online Shopping Portal editable_ajax.php cross site scripting	A vulnerability was found in PHPGurukul Online Shopping Portal 2.0. It has been classified as problematic. Affected is an unknown function of the file /shopping/admin/assets/plugins/DataTables/examples/examples_support/editable_ajax.php. The manipulation of the argument value leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10744	PHPGurukul Online Shopping Portal complex_header_2.p	A vulnerability was found in PHPGurukul Online Shopping Portal	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	hp cross site scripting	2.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/assets/plugins/DataTables/media/unit_testing/templates/complex_header_2.php. The manipulation of the argument scripts leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-10745	PHPGurukul Online Shopping Portal deferred_table.php cross site scripting	A vulnerability was found in PHPGurukul Online Shopping Portal 2.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/assets/plugins/DataTables/media/unit_testing/templates/deferred_table.php. The manipulation of the argument scripts leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10746	PHPGurukul Online Shopping Portal dom_data.php cross site scripting	A vulnerability classified as problematic has been found in PHPGurukul Online Shopping Portal 2.0. This affects an unknown part of the file /admin/assets/plugins/DataTables/media/unit_testing/templates/dom_data.php. The manipulation of the argument scripts leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		disclosed to the public and may be used.		
CVE-2023-34443	Cross-site Scripting vulnerability in the run_query.php page in Combodo iTop	Combodo iTop is a simple, web based IT Service Management tool. When displaying page Run queries Cross-site Scripting (XSS) are possible for scripts outside of script tags. This has been fixed in versions 2.7.9, 3.0.4, 3.1.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2023-34444	Cross-site Scripting vulnerability on pages/ajax.searchform.php in Combodo iTop	Combodo iTop is a simple, web based IT Service Management tool. When displaying pages/ajax.searchform.php XSS are possible for scripts outside of script tags. This issue has been fixed in versions 2.7.9, 3.0.4, 3.1.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2023-34445	Cross-site Scripting vulnerability on pages/ajax.render.php in Combodo iTop	Combodo iTop is a simple, web based IT Service Management tool. When displaying pages/ajax.render.php XSS are possible for scripts outside of script tags. This issue has been fixed in versions 2.7.9, 3.0.4, 3.1.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2024-10747	PHPGurukul Online Shopping Portal dom_data_th.php cross site scripting	A vulnerability classified as problematic was found in PHPGurukul Online Shopping Portal 2.0. This vulnerability affects unknown code of the file /admin/assets/plugins/DataTables/media/unit	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		_testing/templates/dom_data_th.php. The manipulation of the argument scripts leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-10753	PHPGurukul Online Shopping Portal dom_data_two_headers.php cross site scripting	A vulnerability was found in PHPGurukul Online Shopping Portal 2.0. It has been declared as problematic. This vulnerability affects unknown code of the file admin/assets/plugins/DataTables/media/unit_testing/templates/dom_data_two_headers.php. The manipulation of the argument scripts leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10754	PHPGurukul Online Shopping Portal dymanic_table.php cross site scripting	A vulnerability was found in PHPGurukul Online Shopping Portal 2.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/assets/plugins/DataTables/media/unit_testing/templates/dymanic_table.php. The manipulation of the argument scripts leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10755	PHPGurukul Online Shopping Portal empty_table.php cross site scripting	A vulnerability classified as problematic has been found in PHPGurukul	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Online Shopping Portal 2.0. Affected is an unknown function of the file /admin/assets/plugins/DataTables/media/unit_testing/templates/empty_table.php. The manipulation of the argument scripts leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-10756	PHPGurukul Online Shopping Portal html_table.php cross site scripting	A vulnerability classified as problematic was found in PHPGurukul Online Shopping Portal 2.0. Affected by this vulnerability is an unknown functionality of the file /admin/assets/plugins/DataTables/media/unit_testing/templates/html_table.php. The manipulation of the argument scripts leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10757	PHPGurukul Online Shopping Portal js_data.php cross site scripting	A vulnerability, which was classified as problematic, has been found in PHPGurukul Online Shopping Portal 2.0. Affected by this issue is some unknown functionality of the file /admin/assets/plugins/DataTables/media/unit_testing/templates/js_data.php. The manipulation of the argument scripts leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-10768	PHPGurukul Online Shopping Portal two_tables.php cross site scripting	A vulnerability classified as problematic was found in PHPGurukul Online Shopping Portal 2.0. This vulnerability affects unknown code of the file /admin/assets/plugins/DataTables/media/unit_testing/templates/two_tables.php. The manipulation of the argument scripts leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-31448	Cross-site Scripting vulnerability in link CSV import in Combodo iTop	Combodo iTop is a simple, web based IT Service Management tool. By filling malicious code in a CSV content, an Cross-site Scripting (XSS) attack can be performed when importing this content. This issue has been fixed in versions 3.1.2 and 3.2.0. All users are advised to upgrade. Users unable to upgrade should validate CSV content before importing it.	Patched by core rule	Y
CVE-2024-10806	PHPGurukul Hospital Management System betweendates-detailsreports.php cross site scripting	A vulnerability was found in PHPGurukul Hospital Management System 4.0. It has been declared as problematic. This vulnerability affects unknown code of the file betweendates-detailsreports.php. The manipulation of the argument fromdate/todate leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-10807	PHPGurukul Hospital Management System search.php cross site scripting	A vulnerability was found in PHPGurukul Hospital Management System 4.0. It has been rated as problematic. This issue affects some unknown processing of the file hms/doctor/search.php. The manipulation of the argument searchdata leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10840	romadebrian WEB-Sekolah Backend akun_edit.php cross site scripting	A vulnerability classified as problematic has been found in romadebrian WEB-Sekolah 1.0. Affected is an unknown function of the file /Admin/akun_edit.php of the component Backend. The manipulation of the argument kode leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-10842	romadebrian WEB-Sekolah Backend Proses_Edit_Akun.php cross site scripting	A vulnerability, which was classified as problematic, has been found in romadebrian WEB-Sekolah 1.0. Affected by this issue is some unknown functionality of the file /Admin/Proses_Edit_Akun.php of the component Backend. The manipulation of the argument Username_Baru/Password leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		used.		
CVE-2024-49377	Jinja2 Templates are vulnerable to XSS attacks due to their configuration in OctoPrint	OctoPrint provides a web interface for controlling consumer 3D printers. OctoPrint versions up until and including 1.10.2 contain reflected XSS vulnerabilities in the login dialog and the standalone application key confirmation dialog. An attacker who successfully talked a victim into clicking on a specially crafted login link, or a malicious app running on a victim's computer triggering the application key workflow with specially crafted parameters and then redirecting the victim to the related standalone confirmation dialog could use this to retrieve or modify sensitive configuration settings, interrupt prints or otherwise interact with the OctoPrint instance in a malicious way. The above mentioned specific vulnerabilities of the login dialog and the standalone application key confirmation dialog have been patched in the bugfix release 1.10.3 by individual escaping of the detected locations. A global change throughout all of OctoPrint's templating system with the upcoming 1.11.0 release will handle this further, switching to globally enforced automatic escaping and thus reducing the attack surface in general. The latter will	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		also improve the security of third party plugins. During a transition period, third party plugins will be able to opt into the automatic escaping. With OctoPrint 1.13.0, automatic escaping will be switched over to be enforced even for third party plugins, unless they explicitly opt-out.		
CVE-2024-10927	MonoCMS Account Information Page account.php cross site scripting	A vulnerability was found in MonoCMS up to 20240528. It has been classified as problematic. Affected is an unknown function of the file /monofiles/account.php of the component Account Information Page. The manipulation of the argument userid leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-10928	MonoCMS Posts Page opensaved.php cross site scripting	A vulnerability was found in MonoCMS up to 20240528. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /monofiles/opensaved.php of the component Posts Page. The manipulation of the argument filtcategory/filtstatus leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		contacted early about this disclosure but did not respond in any way.		
CVE-2024-11070	Sanluan PublicCMS Tag Type save cross site scripting	A vulnerability, which was classified as problematic, has been found in Sanluan PublicCMS 5.202406.d. This issue affects some unknown processing of the file /admin/cmsTagType/save of the component Tag Type Handler. The manipulation of the argument name leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11078	code-projects Job Recruitment register.php cross site scripting	A vulnerability has been found in code-projects Job Recruitment 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /register.php. The manipulation of the argument e leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-51486	Stored Cross-Site Scripting in Ampache	Ampache is a web based audio/video streaming application and file manager. The vulnerability exists in the interface section of the Ampache menu, where users can change the "Custom URL - Favicon". This section is not properly sanitized, allowing for the input of strings that can execute JavaScript. This issue has been	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		addressed in version 7.0.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2024-51490	Stored Cross-Site Scripting in Ampache	Ampache is a web based audio/video streaming application and file manager. This vulnerability exists in the interface section of the Ampache menu, where users can change "Custom URL - Logo". This section is not properly sanitized, allowing for the input of strings that can execute JavaScript. This issue has been addressed in version 7.0.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2024-52286	Self Cross Site Scripting (XSS) In Merge Functionality in Stirling-PDF	Stirling-PDF is a locally hosted web application that allows you to perform various operations on PDF files. In affected versions the Merge functionality takes untrusted user input (file name) and uses it directly in the creation of HTML pages allowing any unauthenticated to execute JavaScript code in the context of the user. The issue stems to the code starting at \`Line 24\` in \`src/main/resources/static/js/merge.js\`. The file name is directly being input into InnerHTML with no sanitization on the file name, allowing a malicious user to be able to upload files with names containing HTML tags. As HTML tags can include	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		JavaScript code, this can be used to execute JavaScript code in the context of the user. This is a self-injection style attack and relies on a user uploading the malicious file themselves and it impact only them, not other users. A user might be social engineered into running this to launch a phishing attack. Nevertheless, this breaks the expected security restrictions in place by the application. This issue has been addressed in version 0.32.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2024-11102	SourceCodester Hospital Management System edit-doc.php cross site scripting	A vulnerability was found in SourceCodester Hospital Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /vm/doctor/edit-doc.php. The manipulation of the argument name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2024-11130	ZZCMS msg.php cross site scripting	A vulnerability was found in ZZCMS up to 2023. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/msg.php. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument keyword leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-52300	macro-pdfviewer has a XSS through the width parameter	macro-pdfviewer is a PDF Viewer Macro for XWiki using Mozilla pdf.js. The width parameter of the PDF viewer macro isn't properly escaped, allowing XSS for any user who can edit a page. XSS can impact the confidentiality, integrity and availability of the whole XWiki installation when an admin visits the page with the malicious code. This is fixed in 2.5.6.	Patched by core rule	Y
CVE-2024-1097	Stored XSS in craigk5n/webcalendar	A stored cross-site scripting (XSS) vulnerability exists in craigk5n/webcalendar version 1.3.0. The vulnerability occurs in the 'Report Name' input field while creating a new report. An attacker can inject malicious scripts, which are then executed in the context of other users who view the report, potentially leading to the theft of user accounts and cookies.	Patched by core rule	Y
CVE-2024-11243	code-projects Online Shop Store signup.php cross site scripting	A vulnerability classified as problematic has been found in code-projects Online Shop Store 1.0. This affects an unknown part of the file /signup.php. The manipulation of the argument m2 with the input	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		<svg%20onload=alert(document.cookie)> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-11246	code-projects Farmacia adicionar-cliente.php cross site scripting	A vulnerability, which was classified as problematic, was found in code-projects Farmacia 1.0. Affected is an unknown function of the file /adicionar-cliente.php. The manipulation of the argument nome/cpf/dataNascimento leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions the parameter "nome" to be affected. But further inspection indicates that other parameters might be affected as well.	Patched by core rule	Y
CVE-2024-11247	SourceCodester Online Eyewear Shop Inventory Page Master.php cross site scripting	A vulnerability has been found in SourceCodester Online Eyewear Shop 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /oews/classes/Master.php?f=save_product of the component Inventory Page. The manipulation of the argument brand leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		might be affected as well.		
CVE-2024-11259	code-projects Farmacia fornecedores.php cross site scripting	A vulnerability, which was classified as problematic, has been found in code-projects Farmacia 1.0. This issue affects some unknown processing of the file /fornecedores.php. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-49754	LibreNMS has a stored XSS ('Cross-site Scripting') in librenms/includes/html/pages/api-access.inc.php	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the API-Access page allows authenticated users to inject arbitrary JavaScript through the "token" parameter when creating a new API token. This vulnerability can result in the execution of malicious code in the context of other users' sessions, compromising their accounts and enabling unauthorized actions. This vulnerability is fixed in 24.10.0.	Patched by core rule	Y
CVE-2024-49758	LibreNMS has a stored XSS in ExamplePlugin with Device's Notes	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. User with Admin role can add Notes to a device, the application did not properly sanitize the user input, when the ExamplePlugin enable, if java script code is inside the device's	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Notes, its will be trigger. This vulnerability is fixed in 24.10.0.		
CVE-2024-49759	LibreNMS has a Stored XSS ('Cross-site Scripting') in librenms/includes/html/pages/edituser.inc.php	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Manage User Access" page allows authenticated users to inject arbitrary JavaScript through the "bill_name" parameter when creating a new bill. This vulnerability can lead to the execution of malicious code when visiting the "Bill Access" dropdown in the user's "Manage Access" page, potentially compromising user sessions and allowing unauthorized actions. This vulnerability is fixed in 24.10.0.	Patched by core rule	Y
CVE-2024-49764	LibreNMS has a Stored XSS ('Cross-site Scripting') in librenms/includes/html/pages/device/capture.inc.php	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Capture Debug Information" page allows authenticated users to inject arbitrary JavaScript through the "hostname" parameter when creating a new device. This vulnerability results in the execution of malicious code when the "Capture Debug Information" page is visited, redirecting the user and sending non-httponly cookies to an attacker-controlled	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		domain. This vulnerability is fixed in 24.10.0.		
CVE-2024-50350	LibreNMS has a Stored XSS ('Cross-site Scripting') in librenms/app/Http/Controllers/Table/EditPortsController.php	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Port Settings" page allows authenticated users to inject arbitrary JavaScript through the "name" parameter when creating a new Port Group. This vulnerability results in the execution of malicious code when the "Port Settings" page is visited after the affected Port Group is added to a device, potentially compromising user sessions and allowing unauthorized actions. This vulnerability is fixed in 24.10.0.	Patched by core rule	Y
CVE-2024-50351	LibreNMS has a Reflected XSS ('Cross-site Scripting') in librenms/includes/functions.php	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Reflected Cross-Site Scripting (XSS) vulnerability in the "section" parameter of the "logs" tab of a device allows attackers to inject arbitrary JavaScript. This vulnerability results in the execution of malicious code when a user accesses the page with a malicious "section" parameter, potentially compromising their session and enabling unauthorized actions. The issue arises from a lack of sanitization in the "report_this()"	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		function. This vulnerability is fixed in 24.10.0.		
CVE-2024-50352	LibreNMS has a Stored XSS ('Cross-site Scripting') in librenms/includes/html/pages/device/overview/services.inc.php	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Services" section of the Device Overview page allows authenticated users to inject arbitrary JavaScript through the "name" parameter when adding a service to a device. This vulnerability could result in the execution of malicious code in the context of other users' sessions, potentially compromising their accounts and enabling unauthorized actions. This vulnerability is fixed in 24.10.0.	Patched by core rule	Y
CVE-2024-50355	LibreNMS has a Persistent XSS from Insecure Input Sanitization Affects Multiple Endpoints	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. User with Admin role can edit the Display Name of a device, the application did not properly sanitize the user input in the device Display Name, if java script code is inside the name of the device Display Name, its can be trigger from different sources. This vulnerability is fixed in 24.10.0.	Patched by core rule	Y
CVE-2024-51494	LibreNMS has a Stored XSS ('Cross-site Scripting') in librenms/app/Http/Controllers/Table/EditPortsController.php	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS)	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability in the "Port Settings" page allows authenticated users to inject arbitrary JavaScript through the "descr" parameter when editing a device's port settings. This vulnerability can lead to the execution of malicious code when the "Port Settings" page is visited, potentially compromising the user's session and allowing unauthorized actions. This vulnerability is fixed in 24.10.0.		
CVE-2024-51495	LibreNMS has a Stored XSS ('Cross-site Scripting') in librenms/includes/html/dev-overview-data.inc.php	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the Device Overview page allows authenticated users to inject arbitrary JavaScript through the "overwrite_ip" parameter when editing a device. This vulnerability results in the execution of malicious code when the device overview page is visited, potentially compromising the accounts of other users. This vulnerability is fixed in 24.10.0.	Patched by core rule	Y
CVE-2024-51496	LibreNMS has a Reflected XSS ('Cross-site Scripting') in librenms/includes/html/pages/wireless.inc.php	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Reflected Cross-Site Scripting (XSS) vulnerability in the "metric" parameter of the "/wireless" and "/health" endpoints allows attackers to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		inject arbitrary JavaScript. This vulnerability results in the execution of malicious code when a user accesses the page with a malicious "metric" parameter, potentially compromising their session and allowing unauthorized actions. This vulnerability is fixed in 24.10.0.		
CVE-2024-51497	LibreNMS has a Stored XSS ('Cross-site Scripting') in librenms/includes/html/print-customoid.php	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Custom OID" tab of a device allows authenticated users to inject arbitrary JavaScript through the "unit" parameter when creating a new OID. This vulnerability can lead to the execution of malicious code in the context of other users' sessions, compromising their accounts and enabling unauthorized actions. This vulnerability is fixed in 24.10.0.	Patched by core rule	Y
CVE-2024-52526	LibreNMS has a Stored XSS ('Cross-site Scripting') in librenms/includes/html/pages/device/services.inc.php	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Services" tab of the Device page allows authenticated users to inject arbitrary JavaScript through the "descr" parameter when adding a service to a device. This vulnerability could result in the execution	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of malicious code in the context of other users' sessions, potentially compromising their accounts and enabling unauthorized actions. This vulnerability is fixed in 24.10.0.		
CVE-2024-11488	115cms web_user.html cross site scripting	A vulnerability was found in 115cms up to 20240807 and classified as problematic. This issue affects some unknown processing of the file /app/admin/view/web_user.html. The manipulation of the argument ks leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-11489	115cms file.html cross site scripting	A vulnerability was found in 115cms up to 20240807. It has been classified as problematic. Affected is an unknown function of the file /index.php/admin/web/file.html. The manipulation of the argument ks leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-11490	115cms set.html cross site scripting	A vulnerability was found in 115cms up to 20240807. It has been declared as problematic. Affected by this vulnerability is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		an unknown functionality of the file /index.php/admin/web/set.html. The manipulation of the argument type leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-11491	115cms useradmin.html cross site scripting	A vulnerability was found in 115cms up to 20240807. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /index.php/admin/web/useradmin.html. The manipulation of the argument ks leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-11492	115cms appurladd.html cross site scripting	A vulnerability classified as problematic has been found in 115cms up to 20240807. This affects an unknown part of the file /index.php/admin/web/appurladd.html. The manipulation of the argument tid leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		respond in any way.		
CVE-2024-11493	115cms pageAE.html cross site scripting	A vulnerability classified as problematic was found in 115cms up to 20240807. This vulnerability affects unknown code of the file /index.php/setpage/admin/pageAE.html. The manipulation of the argument tid leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-11587	idcCMS classProvCity.php GetCityOptionJs cross site scripting	A vulnerability was found in idcCMS 1.60. It has been classified as problematic. This affects the function GetCityOptionJs of the file /inc/classProvCity.php. The manipulation of the argument idName leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-11660	code-projects Farmacia usuario.php cross site scripting	A vulnerability was found in code-projects Farmacia 1.0. It has been classified as problematic. This affects an unknown part of the file usuario.php. The manipulation of the argument name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Other parameters might be affected as well.		
CVE-2024-53255	Reflected Cross-site Scripting in /admin?page=media via file Parameter in BoidCMS	BoidCMS is a free and open-source flat file CMS for building simple websites and blogs, developed using PHP and uses JSON as a database. In affected versions a reflected Cross-site Scripting (XSS) vulnerability exists in the /admin?page=media endpoint in the file parameter, allowing an attacker to inject arbitrary JavaScript code. This code could be used to steal the user's session cookie, perform phishing attacks, or deface the website. This issue has been addressed in version 2.1.2 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y

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.

Indusface, an institutionally funded firm, is the only vendor to receive 100% customer recommendation rating four years in a row and is a global customer choice in the 2024 Gartner Peer Insights™ Web Application and API Protection (WAAP) Report. Indusface is also a “Great Place to Work” 2024 certified 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™

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