INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

December 2024

The total zero-day vulnerabilities count for December month: 101

Command Injection	SQL Injection	SSRF	Local File Inclusion	Cross-Site Scripting	XML External Entity
6	35	1	5	52	2

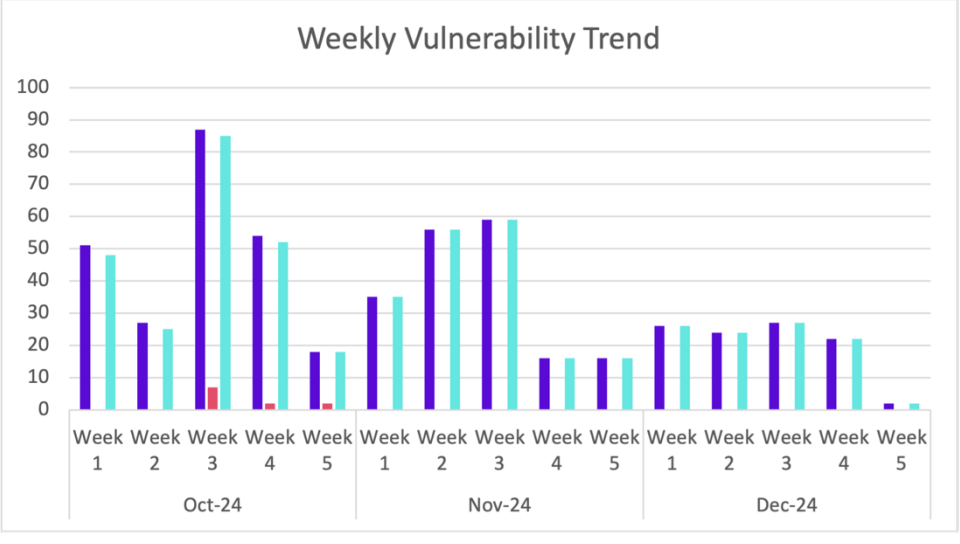
Zero-day vulnerabilities protected through core rules	101
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities found by Indusface WAS	101

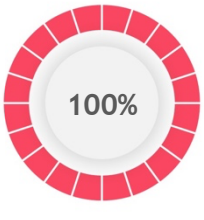
- To enable custom rules, please contact support@indusface.com
- Learn more about zero-day vulnerabilities, detection, and prevention, here

Vulnerability Trend:

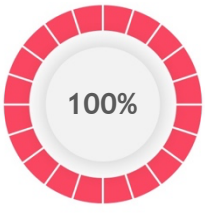
The weekly trend displays the total number of vulnerabilities discovered and the type of protection provided for the last quarter.

Weekly Vulnerability Trend



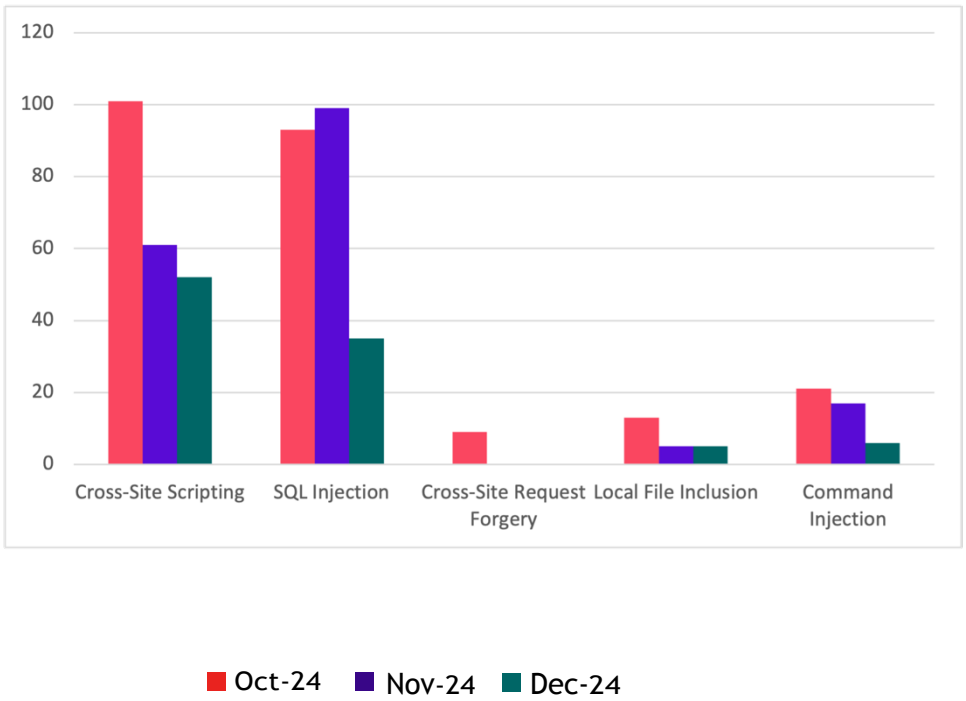


of the zero-day vulnerabilities were protected by the core rules in the last month



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-2024-52800	Potential XXE (XML External Entity Injection) vulnerability in veraPDF CLI	veraPDF is an open source PDF/A validation library. Executing policy checks using custom schematron files via the CLI invokes an XSL transformation that may theoretically lead to a remote code execution (RCE) vulnerability. This doesn't affect the standard validation and policy checks functionality, veraPDF's common use cases. Most veraPDF users don't insert any custom XSLT code into policy profiles, which are based on Schematron syntax rather than direct XSL transforms. For users who do, only load custom policy files from sources you trust. This issue has not yet been patched. Users are advised to be cautious of XSLT code until a patch is available.	Patched by core rule	Y
CVE-2022-41137	Apache Hive: Deserialization of untrusted data when fetching partitions from the Metastore	Apache Hive Metastore (HMS) uses SerializationUtilities#deserializeObjectWithTypeInformation method when filtering and fetching partitions that is unsafe and can	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		lead to Remote Code Execution (RCE) since it allows the deserialization of arbitrary data. In real deployments, the vulnerability can be exploited only by authenticated users/clients that were able to successfully establish a connection to the Metastore. From an API perspective any code that calls the unsafe method may be vulnerable unless it performs additional prerechecks on the input arguments.		
CVE-2024-12350	JFinalCMS Template TemplateController.java update command injection	A vulnerability was found in JFinalCMS 1.0. It has been rated as critical. Affected by this issue is the function update of the file \src\main\java\com\cms\controller\admin\TemplateController.java of the component Template Handler. The manipulation of the argument content leads to 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-2024-12358	WeiYe-Jing datax-web add os command injection	A vulnerability was found in WeiYe-Jing datax-web 2.1.1. It has been classified as critical. This affects an unknown part of the file /api/job/add/. The manipulation of the argument glueSource leads to os command 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-2024-12356	Command Injection Vulnerability in Remote Support(RS) & Privileged Remote Access (PRA)	A critical vulnerability has been discovered in Privileged Remote Access (PRA) and Remote Support (RS) products which can allow an unauthenticated attacker to inject commands that are run as a site user.	Patched by core rule	Y
CVE-2024-56145	RCE when PHP `register_argc_argv`	Craft is a flexible, user-friendly CMS for	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	config setting is enabled in craftcms/cms	creating custom digital experiences on the web and beyond. Users of affected versions are affected by this vulnerability if their php.ini configuration has `register_argc_argv` enabled. For these users an unspecified remote code execution vector is present. Users are advised to update to version 4.13.2 or 5.5.2. Users unable to upgrade should disable `register_argc_argv` to mitigate the issue.		

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-55602	PenDoc vulnerable to Arbitrary File Read on updating and downloading templates using Path Traversal	PwnDoc is a penetration test report generator. Prior to commit 1d4219c596f4f518798492e48386a20c6e9a2fe6, an authenticated user who is able to update and download templates can inject path traversal (`../`) sequences into the file extension property to read arbitrary files on the system. Commit 1d4219c596f4f518798492e48386a20c6e9a2fe6 contains a patch for the issue.	Patched by core rule	Y
CVE-2024-12482	cjbi wetech-cms Database Backup BackupFileUtil.java backup path traversal	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been rated as problematic. Affected by this issue is the function backup of the file wetech-cms-master\wetech-basic-common\src\main\java\tech\wetech\basic\util\BackupFileUtil.java of the component Database Backup Handler. The manipulation of the argument name leads to path traversal: '../filedir'. 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-2024-55657	SiYuan has an arbitrary file read via /api/template/render	SiYuan is a personal knowledge management system. Prior to version	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		3.1.16, an arbitrary file read vulnerability exists in Siyuan's `/api/template/render` endpoint. The absence of proper validation on the path parameter allows attackers to access sensitive files on the host system. Version 3.1.16 contains a patch for the issue.		
CVE-2024-55658	SiYuan has an arbitrary file read and path traversal via /api/export/exportResources	SiYuan is a personal knowledge management system. Prior to version 3.1.16, SiYuan's /api/export/exportResources endpoint is vulnerable to arbitary file read via path traversal. It is possible to manipulate the paths parameter to access and download arbitrary files from the host system by traversing the workspace directory structure. Version 3.1.16 contains a patch for the issue.	Patched by core rule	Y
CVE-2024-38819	N/A	Applications serving static resources through the functional web frameworks WebMvc.fn or WebFlux.fn are vulnerable to path traversal attacks. An attacker can craft malicious HTTP requests and obtain any file on the file system that is also accessible to the process in which the Spring application is running.	Patched by core rule	Y

Server-side Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-55875	http4k has a potential XXE (XML External Entity Injection) vulnerability	http4k is a functional toolkit for Kotlin HTTP applications. Prior to version 5.41.0.0, there is a potential XXE (XML External Entity Injection) vulnerability when http4k handling malicious XML contents within requests, which might allow attackers to read local sensitive information on server, trigger Server-side Request Forgery and even execute code under some circumstances. Version 5.41.0.0 contains a patch for the issue.	Patched by core rule	Y

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-11968	code-projects Farmacia pagamento.php sql injection	A vulnerability was found in code-projects Farmacia up to 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file pagamento.php. The manipulation of the argument notaFiscal leads to sql injection. The attack can be launched remotely.	Patched by core rule	Y
CVE-2024-11998	code-projects Farmacia visualizer-forneccedor.chp sql injection	A vulnerability was found in code-projects Farmacia 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /visualizer-forneccedor.chp. 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-2024-12007	code-projects Farmacia visualizar-produto.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Farmacia 1.0. This affects an unknown part of the file /visualizar-produto.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-2024-12187	1000 Projects Library Management System showbook.php sql injection	A vulnerability was found in 1000 Projects Library Management System 1.0. It has been classified as critical. Affected is an unknown function of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/showbook.php. The manipulation of the argument q 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-2024-12188	1000 Projects Library Management System stu.php sql injection	A vulnerability was found in 1000 Projects Library Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /brains/stu.php. The manipulation of the argument useri 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-2024-12228	PHPGurukul Complaint Management System user-search.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Complaint Management System 1.0. Affected is an unknown function of the file /admin/user-search.php. The manipulation of the argument search 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-2024-12229	PHPGurukul Complaint Management System complaint-search.php sql injection	A vulnerability classified as critical was found in PHPGurukul Complaint Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/complaint-search.php. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument search leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-12230	PHPGurukul Complaint Management System subcategory.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Complaint Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/subcategory.php. The manipulation of the argument category 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-2024-12231	CodeZips Project Management System index.php sql injection	A vulnerability, which was classified as critical, was found in CodeZips Project Management System 1.0. This affects an unknown part of the file /index.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-2024-12234	1000 Projects Beauty Parlour Management System edit-customer-detailed.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/edit-customer-detailed.php. The manipulation of the argument name leads to sql injection. It is possible to launch the attack remotely. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit has been disclosed to the public and may be used. Other parameters might be affected as well.		
CVE-2024-12351	JFinalCMS File Content ContentModel.java findPage sql injection	A vulnerability classified as critical has been found in JFinalCMS 1.0. This affects the function findPage of the file src\main\java\com\cms\entity\ContentModel.java of the component File Content Handler. The manipulation of the argument name leads to sql injection. It is possible to initiate the attack remotely.	Patched by core rule	Y
CVE-2024-12360	code-projects Online Class and Exam Scheduling System class_update.php sql injection	A vulnerability was found in code-projects Online Class and Exam Scheduling System 1.0. It has been rated as critical. This issue affects some unknown processing of the file class_update.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-2024-12479	cjbi wetech-cms TopicDao.java searchTopicByKeyword sql injection	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2 and classified as critical. This issue affects the function searchTopicByKeyword of the file wetech-cms-master\wetech-core\src\main\java\tech\wetech\cms\dao\TopicDao.java. The manipulation of the argument keyword leads to sql injection. The attack may be initiated 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. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-12480	cjbi wetech-cms TopicDao.java searchTopic sql injection	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been classified as critical. Affected is the function searchTopic of the file wetech-cms-master\wetech-core\src\main\java\tech\wetech\cms\dao\TopicDao.java. The manipulation of the argument con 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 vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-12481	cjbi wetech-cms UserDao.java findUser sql injection	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been declared as critical. Affected by this vulnerability is the function findUser of the file wetech-cms-master\wetech-core\src\main\java\tech\wetech\cms\dao\UserDao.java. The manipulation of the argument searchValue/gId/rId 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-2024-12484	Codezips Technical Discussion Forum	A vulnerability classified as critical was	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	signuppost.php sql injection	found in Codezips Technical Discussion Forum 1.0. This vulnerability affects unknown code of the file /signuppost.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. Other parameters might be affected as well.		
CVE-2024-12485	code-projects Online Class and Exam Scheduling System department.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Online Class and Exam Scheduling System 1.0. This issue affects some unknown processing of the file /pages/department.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-2024-12486	code-projects Online Class and Exam Scheduling System rank_update.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Online Class and Exam Scheduling System 1.0. Affected is an unknown function of the file /pages/rank_update.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-2024-12487	code-projects Online Class and Exam Scheduling System room_update.php	A vulnerability has been found in code-projects Online Class and Exam Scheduling	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	sql injection	System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /pages/room_update.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-12488	code-projects Online Class and Exam Scheduling System subject_update.php sql injection	A vulnerability was found in code-projects Online Class and Exam Scheduling System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /pages/subject_update.php. The manipulation of the argument id 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-2024-12489	code-projects Online Class and Exam Scheduling System term.php sql injection	A vulnerability was found in code-projects Online Class and Exam Scheduling System 1.0. It has been classified as critical. This affects an unknown part of the file /pages/term.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-2024-12490	code-projects Online Class and Exam Scheduling System teacher_save.php sql injection	A vulnerability was found in code-projects Online Class and Exam Scheduling System 1.0. It has been declared as critical. This vulnerability affects unknown code of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file /pages/teacher_save.php. The manipulation of the argument salut leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.		
CVE-2024-12492	code-projects Farmacia visualizar-usuario.php sql injection	A vulnerability was found in code-projects Farmacia 1.0. It has been rated as critical. This issue affects some unknown processing of the file /visualizar-usuario.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-2024-12497	1000 Projects Attendance Tracking Management System check_admin_login.php sql injection	A vulnerability classified as critical has been found in 1000 Projects Attendance Tracking Management System 1.0. Affected is an unknown function of the file /admin/check_admin_login.php. The manipulation of the argument admin_user_name 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-2024-12025	Collapsing Categories <= 3.0.8 - Unauthenticated SQL Injection	The Collapsing Categories plugin for WordPress is vulnerable to SQL Injection via the 'taxonomy' parameter of the /wp-json/collapsing-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		categories/v1/get REST API in all versions up to, and including, 3.0.8 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.		
CVE-2024-12784	itsourcecode Vehicle Management System editbill.php sql injection	A vulnerability was found in itsourcecode Vehicle Management System 1.0. It has been classified as critical. Affected is an unknown function of the file editbill.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-2024-12785	itsourcecode Vehicle Management System sendmail.php sql injection	A vulnerability was found in itsourcecode Vehicle Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file sendmail.php. The manipulation of the argument id 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-2024-12787	1000 Projects Attendance Tracking Management System	A vulnerability has been found in 1000 Projects Attendance Tracking Management	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	check_student_login .php sql injection	System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /student/check_student_login.php. The manipulation of the argument student_emailid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-12791	Codezips E-Commerce Site signin.php sql injection	A vulnerability was found in Codezips E-Commerce Site 1.0. It has been rated as critical. This issue affects some unknown processing of the file signin.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-2024-12792	Codezips E-Commerce Site newadmin.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 newadmin.php. The manipulation of the argument email 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-2024-12794	Codezips E-Commerce Site editorder.php sql injection	A vulnerability, which was classified as critical, was found in Codezips E-Commerce Site 1.0. This affects an unknown part of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file /admin/editorder.php. The manipulation of the argument dstatus/quantity/ddate 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-2024-12898	1000 Projects Attendance Tracking Management System faculty_action.php sql injection	A vulnerability was found in 1000 Projects Attendance Tracking Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/faculty_action.php. The manipulation of the argument faculty_course_id leads to sql injection. The attack can be initiated 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-2024-12899	1000 Projects Attendance Tracking Management System course_action.php sql injection	A vulnerability was found in 1000 Projects Attendance Tracking Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/course_action.php. The manipulation of the argument course_code 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-2024-12926	Codezips Project Management System advanced.php sql injection	A vulnerability classified as critical was found in Codezips Project Management System 1.0. 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 /pages/forms/advanced.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. Other parameters might be affected as well.		
CVE-2024-12927	1000 Projects Attendance Tracking Management System check_faculty_login.php sql injection	A vulnerability, which was classified as critical, has been found in 1000 Projects Attendance Tracking Management System 1.0. Affected by this issue is some unknown functionality of the file /faculty/check_faculty_login.php. The manipulation of the argument faculty_emailid 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

XML External Entity Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-52596	SimpleSAMLphp xml-common XXE vulnerability	SimpleSAMLphp xml-common is a common classes for handling XML-structures. When loading an (untrusted) XML document, for example the SAMLResponse, it's possible to induce an XXE. This vulnerability is fixed in 1.19.0.	Patched by core rule	Y
CVE-2024-52806	SimpleSAMLphp SAML2 has an XXE in parsing SAML messages	SimpleSAMLphp SAML2 library is a PHP library for SAML2 related functionality. When loading an (untrusted) XML document, for example the SAMLResponse, it's possible to induce an XXE. This vulnerability is fixed in 4.6.14 and 5.0.0-alpha.18.	Patched by core rule	Y

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-11742	SourceCodester Best House Rental Management System ajax.php cross site scripting	A vulnerability, which was classified as problematic, has been found in SourceCodester Best House Rental Management System 1.0. This issue affects some unknown processing of the file /rental/ajax.php?action=save_tenant. The manipulation of the argument lastname/firstname/middlename leads to cross site scripting. The attack may be initiated 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-2024-11678	CodeAstro Hospital Management System his_doc_register_patient.php cross site scripting	A vulnerability was found in CodeAstro Hospital Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /backend/doc/his_doc_register_patient.php. The manipulation of the argument pat_fname/pat_ailment/pat_lname/pat_age/pat_dob/pat_number/pat_phone/pat_type/pat_addr 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-2024-11677	CodeAstro Hospital Management System Add Vendor Details Page his_admin_add_vendor.php cross site	A vulnerability was found in CodeAstro Hospital Management System 1.0. It has been classified as problematic. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	scripting	affects an unknown part of the file /backend/admin/his_admin_add_vendor.php of the component Add Vendor Details Page. The manipulation of the argument v_name/v_adr/v_number/v_email/v_phone/v_desc 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-2024-11676	CodeAstro Hospital Management System Add Laboratory Equipment Page his_admin_add_lab_equipment.php cross site scripting	A vulnerability was found in CodeAstro Hospital Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /backend/admin/his_admin_add_lab_equipment.php of the component Add Laboratory Equipment Page. The manipulation of the argument eqp_code/eqp_name/eqp_vendor/eqp_desc/eqp_dept/eqp_status/eqp_qty 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-2024-11675	CodeAstro Hospital Management System Add Patient Details Page his_admin_register_patient.php cross site scripting	A vulnerability has been found in CodeAstro Hospital Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /backend/admin/his_admin_register_patient.php of the component Add Patient Details Page. The manipulation	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the argument pat_fname/pat_ailment/pat_lname/pat_age/pat_dob/pat_number/pat_phone/pat_type/pat_addr leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-11820	code-projects Crud Operation System add.php cross site scripting	A vulnerability, which was classified as problematic, has been found in code-projects Crud Operation System 1.0. This issue affects some unknown processing of the file /add.php. The manipulation of the argument saddress leads to cross site scripting. The attack may be initiated 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-2024-11971	Guizhou Xiaoma Technology jpress Avatar upload cross site scripting	A vulnerability classified as problematic was found in Guizhou Xiaoma Technology jpress 5.1.2. Affected by this vulnerability is an unknown functionality of the file /commons/attachment/upload of the component Avatar Handler. The manipulation of the argument files 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-2024-11995	code-projects Farmacia pagamento.php	A vulnerability has been found in code-projects Farmacia 1.0	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	cross site scripting	and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /pagamento.php. The manipulation of the argument total leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-52809	Cross-site Scripting vulnerability with prototype pollution in vue-i18n	vue-i18n is an internationalization plugin for Vue.js. In affected versions vue-i18n can be passed locale messages to `createI18n` or `useI18n`. When locale message ASTs are generated in development mode there is a possibility of Cross-site Scripting attack. This issue has been addressed in versions 9.14.2, and 10.0.5. Users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2024-53864	Cross-site Scripting in a field that is used in the Content name pattern in ibexa/admin-ui	Ibexa Admin UI Bundle is all the necessary parts to run the Ibexa DXP Back Office interface. The Content name pattern is used to build Content names from one or more fields. An XSS vulnerability has been found in this mechanism. Content edit permission is required to exploit it. After the fix, any existing injected XSS will not run. This issue has been patched in version 4.6.14. All users are advised to upgrade. There are no known workarounds for this	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability.		
CVE-2024-11995	code-projects Farmacia pagamento.php cross site scripting	A vulnerability has been found in code-projects Farmacia 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /pagamento.php. The manipulation of the argument total 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-2024-11996	code-projects Farmacia editar-fornecedor.php cross site scripting	A vulnerability was found in code-projects Farmacia 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /editar-fornecedor.php. The manipulation of the argument cidade 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-2024-11997	code-projects Farmacia vendas.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 /vendas.php. The manipulation of the argument notaFiscal 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
CVE-2024-12000	code-projects Blood Bank System Setting updatesettings.php cross site scripting	A vulnerability was found in code-projects Blood Bank System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /controllers/updatesettings.php of the component Setting Handler. The manipulation of the argument firstname leads to cross site scripting. The attack may be initiated 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-2024-12001	code-projects Wazifa System Setting updatesettings.php cross site scripting	A vulnerability classified as problematic has been found in code-projects Wazifa System 1.0. Affected is an unknown function of the file /controllers/updatesettings.php of the component Setting Handler. The manipulation of the argument firstname 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. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2024-53985	Possible XSS vulnerability with certain configurations of rails-html-sanitizer 1.6.0	rails-html-sanitizer is responsible for sanitizing HTML fragments in Rails applications. There is a possible XSS vulnerability with certain configurations of Rails::HTML::Sanitizer 1.6.0 when used with Rails >= 7.1.0 and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Nokogiri < 1.15.7, or 1.16.x < 1.16.8. The XSS vulnerability with certain configurations of Rails::HTML::Sanitizer may allow an attacker to inject content if HTML5 sanitization is enabled and the application developer has overridden the sanitizer's allowed tags with both "math" and "style" elements or both both "svg" and "style" elements. This vulnerability is fixed in 1.6.1.		
CVE-2024-53986	Possible XSS vulnerability with certain configurations of rails-html-sanitizer 1.6.0	rails-html-sanitizer is responsible for sanitizing HTML fragments in Rails applications. There is a possible XSS vulnerability with certain configurations of Rails::HTML::Sanitizer 1.6.0 when used with Rails >= 7.1.0. A possible XSS vulnerability with certain configurations of Rails::HTML::Sanitizer may allow an attacker to inject content if HTML5 sanitization is enabled and the application developer has overridden the sanitizer's allowed tags where the "math" and "style" elements are both explicitly allowed. This vulnerability is fixed in 1.6.1.	Patched by core rule	Y
CVE-2024-53987	Possible XSS vulnerability with certain configurations of rails-html-sanitizer 1.6.0	rails-html-sanitizer is responsible for sanitizing HTML fragments in Rails applications. There is a possible XSS vulnerability with certain configurations of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Rails::HTML::Sanitizer 1.6.0 when used with Rails >= 7.1.0. A possible XSS vulnerability with certain configurations of Rails::HTML::Sanitizer may allow an attacker to inject content if HTML5 sanitization is enabled and the application developer has overridden the sanitizer's allowed tags where the "style" element is explicitly allowed and the "svg" or "math" element is not allowed. This vulnerability is fixed in 1.6.1.		
CVE-2024-53988	Possible XSS vulnerability with certain configurations of rails-html-sanitizer 1.6.0	rails-html-sanitizer is responsible for sanitizing HTML fragments in Rails applications. There is a possible XSS vulnerability with certain configurations of Rails::HTML::Sanitizer 1.6.0 when used with Rails >= 7.1.0. A possible XSS vulnerability with certain configurations of Rails::HTML::Sanitizer may allow an attacker to inject content if HTML5 sanitization is enabled and the application developer has overridden the sanitizer's allowed tags where the "math", "mtext", "table", and "style" elements are allowed and either either "mglyph" or "malignmark" are allowed. This vulnerability is fixed in 1.6.1.	Patched by core rule	Y
CVE-2024-53989	Possible XSS vulnerability with	rails-html-sanitizer is responsible for	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	certain configurations of rails-html-sanitizer 1.6.0	sanitizing HTML fragments in Rails applications. There is a possible XSS vulnerability with certain configurations of Rails::HTML::Sanitizer 1.6.0 when used with Rails >= 7.1.0. A possible XSS vulnerability with certain configurations of Rails::HTML::Sanitizer may allow an attacker to inject content if HTML5 sanitization is enabled and the application developer has overridden the sanitizer's allowed tags for the the "noscript" element. This vulnerability is fixed in 1.6.1.		
CVE-2024-53999	Mobile Security Framework (MobSF) Stored Cross-Site Scripting Vulnerability in "Diff or Compare" Functionality	Mobile Security Framework (MobSF) is a pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis. The application allows users to upload files with scripts in the filename parameter. As a result, a malicious user can upload a script file to the system. When users in the application use the "Diff or Compare" functionality, they are affected by a Stored Cross-Site Scripting vulnerability. This vulnerability is fixed in 4.2.9.	Patched by core rule	Y
CVE-2024-12180	DedeCMS article_add.php cross site scripting	A vulnerability classified as problematic has been found in DedeCMS 5.7.116. Affected is an unknown function of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/member/article_add.php. The manipulation of the argument body 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-2024-12181	DedeCMS SWF File uploads_add.php cross site scripting	A vulnerability classified as problematic was found in DedeCMS 5.7.116. Affected by this vulnerability is an unknown functionality of the file /member/uploads_add.php of the component SWF File Handler. The manipulation of the argument mediatype 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-2024-12182	DedeCMS soft_add.php cross site scripting	A vulnerability, which was classified as problematic, has been found in DedeCMS 5.7.116. Affected by this issue is some unknown functionality of the file /member/soft_add.php. The manipulation of the argument body 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-2024-12183	DedeCMS HTTP POST Request carbuyaction.php RemoveXSS cross site scripting	A vulnerability, which was classified as problematic, was found in DedeCMS 5.7.116. This affects the function RemoveXSS of the file /plus/carbuyaction.php	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the component HTTP POST Request Handler. The manipulation 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-2024-12232	code-projects Simple CRUD Functionality index.php cross site scripting	A vulnerability has been found in code-projects Simple CRUD Functionality 1.0 and classified as problematic. This vulnerability affects unknown code of the file /index.php. The manipulation of the argument newtitle/newdescr 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-2024-54001	Kanboard allows a persistent HTML injection site scripting in settings page date format	Kanboard is project management software that focuses on the Kanban methodology. HTML can be injected and stored into the application settings section. The fields application_language, application_date_format,application_timezone and application_time_format allow arbirary user input which is reflected. The vulnerability can become xss if the user input is javascript code that bypass CSP. This vulnerability is fixed in 1.2.41.	Patched by core rule	Y
CVE-2024-12326	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in Jirafeau	Jirafeau normally prevents browser preview for SVG files due to the possibility that manipulated SVG files could be exploited	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		for cross site scripting. This was done by storing the MIME type of a file and preventing the browser preview for MIME type image/svg+xml. This issue was first reported in CVE-2022-30110. However, it was still possible to do a browser preview of a SVG file by sending a manipulated MIME type during the upload, where the case of any letter in image/svg+xml had been changed (like image/svg+XML). The check for image/svg+xml has been changed to be case insensitive.		
CVE-2024-54138	XSS Vulnerability in NuGetGallery's Markdown Autolinks Processing	NuGet Gallery is a package repository that powers nuget.org. The NuGetGallery has a security vulnerability related to its handling of autolinks in Markdown content. While the platform properly filters out JavaScript from standard links, it does not adequately sanitize autolinks. This oversight allows attackers to exploit autolinks as a vector for Cross-Site Scripting (XSS) attacks. This vulnerability is fixed in 2024.12.06.	Patched by core rule	Y
CVE-2024-12348	Guizhou Xiaoma Technology jpress Attachment Upload upload AttachmentUtils.isUnSafe cross site scripting	A vulnerability was found in Guizhou Xiaoma Technology jpress 5.1.2. It has been classified as problematic. Affected is the function AttachmentUtils.isUnSafe of the file /commons/attachment/upload of the component Attachment Upload	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Handler. The manipulation of the argument files[] 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-2024-52599	Tuleap vulnerable to XSS in the Gantt chart of the tracker plugin	Tuleap is an open source suite to improve management of software developments and collaboration. In Tuleap Community Edition prior to version 16.1.99.50 and Tuleap Enterprise Edition prior to versions 16.1-4 and 16.0-7, a malicious user with the ability to create an artifact in a tracker with a Gantt chart could force a victim to execute uncontrolled code. Tuleap Community Edition 16.1.99.50, Tuleap Enterprise Edition 16.1-4, and Tuleap Enterprise Edition 16.0-7 contain a fix.	Patched by core rule	Y
CVE-2024-53847	Trix vulnerable to Cross-site Scripting on copy & paste	The Trix rich text editor, prior to versions 2.1.9 and 1.3.3, is vulnerable to cross-site scripting (XSS) + mutation XSS attacks when pasting malicious code. An attacker could trick a user to copy and paste malicious code that would execute arbitrary JavaScript code within the context of the user's session, potentially leading to unauthorized actions being performed or sensitive information being disclosed. Users should upgrade to Trix editor version 2.1.9 or 1.3.3, which uses DOMPurify to sanitize the pasted content.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-54133	Possible Content Security Policy bypass in Action Dispatch	Action Pack is a framework for handling and responding to web requests. There is a possible Cross Site Scripting (XSS) vulnerability in the `content_security_policy` helper starting in version 5.2.0 of Action Pack and prior to versions 7.0.8.7, 7.1.5.1, 7.2.2.1, and 8.0.0.1. Applications which set Content-Security-Policy (CSP) headers dynamically from untrusted user input may be vulnerable to carefully crafted inputs being able to inject new directives into the CSP. This could lead to a bypass of the CSP and its protection against XSS and other attacks. Versions 7.0.8.7, 7.1.5.1, 7.2.2.1, and 8.0.0.1 contain a fix. As a workaround, applications can avoid setting CSP headers dynamically from untrusted input, or can validate/sanitize that input.	Patched by core rule	Y
CVE-2024-53272	GHSL-2024-109: Reflected XSS in /login in habitica	Habitica is an open-source habit-building program. Versions prior to 5.28.5 are vulnerable to reflected cross-site scripting. The `login` and `social media` function in `RegisterLoginReset.vue` contains two reflected XSS vulnerabilities due to an incorrect sanitization function. An attacker can specify a malicious `redirectTo` parameter to trigger the vulnerability, giving the attacker control of the victim's account	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		when a victim registers or logins with a specially crafted link. Version 5.28.5 contains a patch.		
CVE-2024-53273	GHSL-2024-110: Reflected XSS in /register in habitica	Habitica is an open-source habit-building program. Versions prior to 5.28.5 are vulnerable to reflected cross-site scripting. The `register` function in `RegisterLoginReset.vue` contains a reflected XSS vulnerability due to an incorrect sanitization function. An attacker can specify a malicious `redirectTo` parameter to trigger the vulnerability, giving the attacker control of the victim's account when a victim registers or logins with a specially crafted link. Version 5.28.5 contains a patch.	Patched by core rule	Y
CVE-2024-53274	GHSL-2024-111: Reflected XSS in /home in habitica	Habitica is an open-source habit-building program. Versions prior to 5.28.5 are vulnerable to reflected cross-site scripting. The `register` function in `home.vue` containsa reflected XSS vulnerability due to an incorrect sanitization function. An attacker can specify a malicious `redirectTo` parameter to trigger the vulnerability. Arbitrary javascript can be executed by the attacker in the context of the victim's session. Version 5.28.5 contains a patch.	Patched by core rule	Y
CVE-2024-55659	SiYuan has an arbitrary file write in the host via /api/asset/upload	SiYuan is a personal knowledge management system. Prior to version 3.1.16, the `/api/asset/upload` endpoint in Siyuan is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerable to both arbitrary file write to the host and stored cross-site scripting (via the file write). Version 3.1.16 contains a patch for the issue.		
CVE-2024-12503	ClassCMS Model Management Page admin cross site scripting	A vulnerability classified as problematic was found in ClassCMS 4.8. Affected by this vulnerability is an unknown functionality of the file /index.php/admin of the component Model Management Page. The manipulation of the argument URL 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-2024-55878	Cross-site Scripting vulnerability in SimpleXLSXEx::readXfs and SimpeXLSX::toHTMLEx	SimpleXLSX is software for parsing and retrieving data from Excel XLSx files. Starting in version 1.0.12 and prior to version 1.1.12, when calling the extended toHTMLEx method, it is possible to execute arbitrary JavaScript code. Version 1.1.12 fixes the issue. As a workaround, don't use direct publication via toHTMLEx.	Patched by core rule	Y
CVE-2024-8179	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in GitLab	An issue has been discovered in GitLab CE/EE affecting all versions from 17.3 before 17.4.6, 17.5 before 17.5.4, and 17.6 before 17.6.2. Improper output encoding could lead to XSS if CSP is not enabled.	Patched by core rule	Y
CVE-2024-12664	ruifang-tech Rebuild Project Task Comment cross site	A vulnerability, which was classified as problematic, has been	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	scripting	found in ruifang-tech Rebuild 3.8.5. This issue affects some unknown processing of the component Project Task Comment Handler. 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. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-12665	ruifang-tech Rebuild Task Comment Attachment Upload cross site scripting	A vulnerability, which was classified as problematic, was found in ruifang-tech Rebuild 3.8.5. Affected is an unknown function of the component Task Comment Attachment Upload. The manipulation 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-2024-12783	itsourcecode Vehicle Management System billaction.php cross site scripting	A vulnerability was found in itsourcecode Vehicle Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file /billaction.php. The manipulation of the argument extra-cost 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-12790	code-projects Hostel Management Site room-details.php cross site scripting	A vulnerability was found in code-projects Hostel Management Site 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file room-details.php. The manipulation 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-2024-12841	Emlog Pro tag.php cross site scripting	A vulnerability was found in Emlog Pro up to 2.4.1. It has been classified as problematic. This affects an unknown part of the file /admin/tag.php. The manipulation of the argument keyword 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-2024-12842	Emlog Pro user.php cross site scripting	A vulnerability was found in Emlog Pro up to 2.4.1. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/user.php. The manipulation of the argument keyword 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-2024-12843	Emlog Pro plugin.php cross site scripting	A vulnerability was found in Emlog Pro up to 2.4.1. It has been rated as problematic. This issue affects some unknown processing of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the file /admin/plugin.php. The manipulation of the argument filter leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-12844	Emlog Pro store.php cross site scripting	A vulnerability classified as problematic has been found in Emlog Pro up to 2.4.1. Affected is an unknown function of the file /admin/store.php. The manipulation of the argument tag 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-2024-12845	Emlog Pro common.php cross site scripting	A vulnerability classified as problematic was found in Emlog Pro up to 2.4.1. Affected by this vulnerability is an unknown functionality in the library /include/lib/common.php. The manipulation of the argument msg 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-2024-12846	Emlog Pro link.php cross site scripting	A vulnerability, which was classified as problematic, has been found in Emlog Pro up to 2.4.1. Affected by this issue is some unknown functionality of the file /admin/link.php. The manipulation of the argument siteurl/icon leads to cross site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-12883	code-projects Job Recruitment _email.php cross site scripting	A vulnerability was found in code-projects Job Recruitment 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /_email.php. The manipulation of the argument email 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-2024-12893	Portabilis i-Educar Tipo de Usuário Page 2 cross site scripting	A vulnerability, which was classified as problematic, has been found in Portabilis i-Educar up to 2.9. Affected by this issue is some unknown functionality of the file /usuarios/tipos/2 of the component Tipo de Usuário Page. 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. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y

INDUSFACE™

Indusface is a leading application security SaaS company that secures critical Web, Mobile & API applications of 5000+ global customers using its award-winning fully managed platform that integrates a web application scanner, web application firewall, DDoS &, BOT Mitigation, CDN, and threat intelligence engine.

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™