INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

January 2025

The total zero-day vulnerabilities count for January month: 275

Command Injection	SQL Injection	SSRF	Malicious File Upload	Cross-Site Scripting	XML External Entity
8	127	9	27	102	2

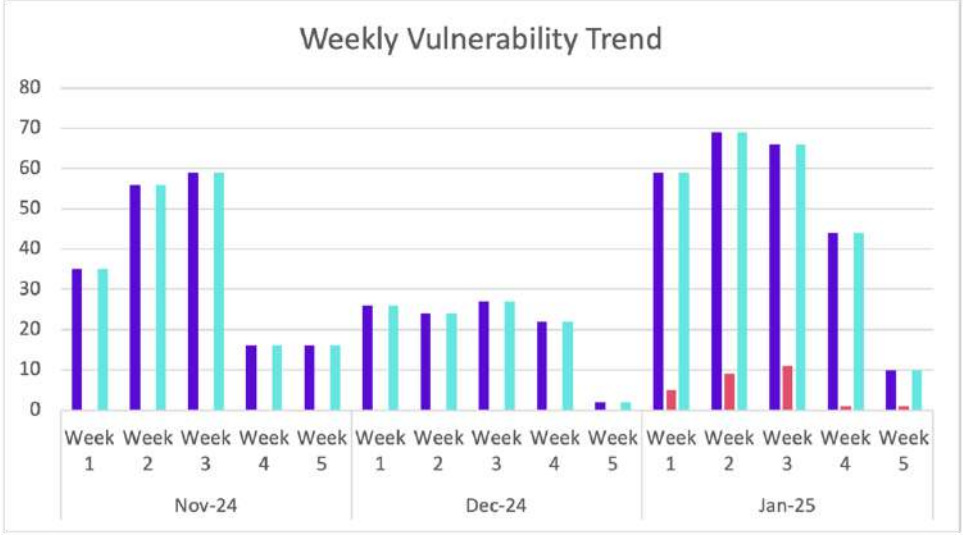
Zero-day vulnerabilities protected through core rules	248
Zero-day vulnerabilities protected through custom rules	27
Zero-day vulnerabilities found by Indusface WAS	248

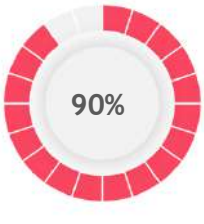
- To enable custom rules, please contact support@indusface.com
- Learn more about zero-day vulnerabilities, detection, and prevention, here

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



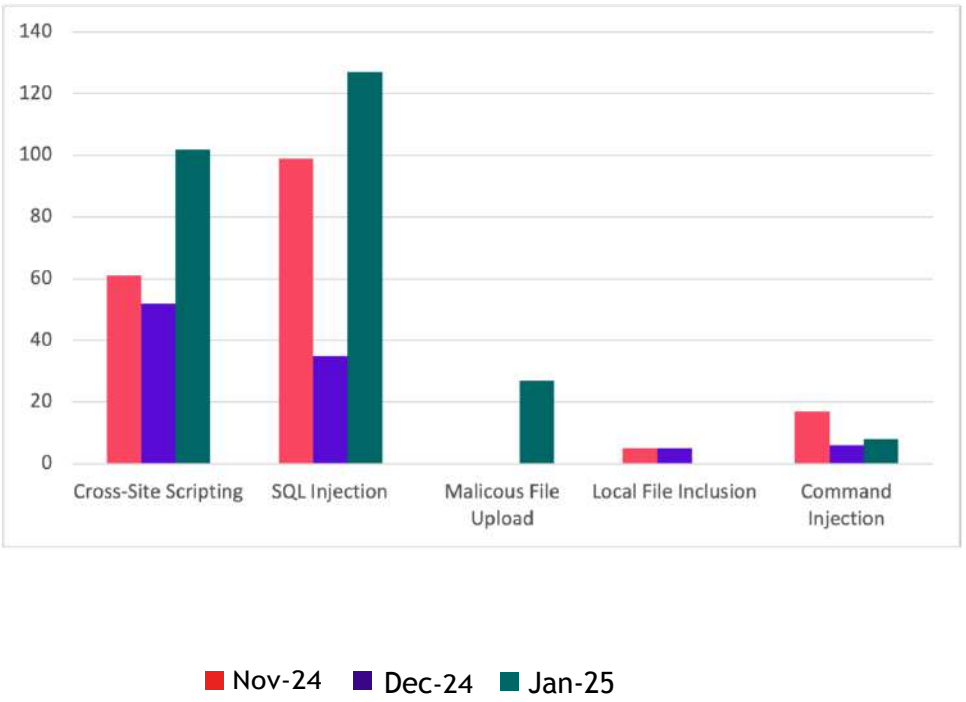


of the zero-day vulnerabilities were protected by the core rules in the last month

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

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

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-12828	Webmin CGI Command Injection Remote Code Execution Vulnerability	Webmin CGI Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Webmin. Authentication is required to exploit this vulnerability. The specific flaw exists within the handling of CGI requests. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-22346.	Patched by core rule	Y
CVE-2024-12952	melMass comfy_mtb Dependency endpoint.py run_command code injection	A vulnerability classified as critical was found in melMass comfy_mtb up to 0.1.4. Affected by this vulnerability is the function run_command of the file comfy_mtb/endpoint.py of the component Dependency Handler.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The manipulation leads to code injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The patch is named d6e004cce2c32f8e48b868e66b89f82da4887dc3. It is recommended to apply a patch to fix this issue.		
CVE-2024-13187	Kingsoft WPS Office TCC code injection	A vulnerability was found in Kingsoft WPS Office 6.14.0 on macOS. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component TCC Handler. The manipulation leads to code injection. It is possible to launch the attack on the local host. 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-2024-46981	Redis' Lua library commands may lead to remote code execution	Redis is an open source, in-memory database that persists on disk. An authenticated user may use a specially crafted Lua script to manipulate the garbage collector and potentially lead to remote code execution. The problem is fixed in 7.4.2, 7.2.7, and 6.2.17. An additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from executing Lua scripts. This can be done using ACL to restrict EVAL and EVALSHA commands.	Patched by core rule	Y
CVE-2024-49375	Remote Code Execution via Remote Model Loading in Rasa	Open source machine learning framework. A vulnerability has been identified in Rasa that enables an attacker who has the ability to load a maliciously	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		crafted model remotely into a Rasa instance to achieve Remote Code Execution. The prerequisites for this are: 1. The HTTP API must be enabled on the Rasa instance eg with `--enable-api`. This is not the default configuration. 2. For unauthenticated RCE to be exploitable, the user must not have configured any authentication or other security controls recommended in our documentation. 3. For authenticated RCE, the attacker must posses a valid authentication token or JWT to interact with the Rasa API. This issue has been addressed in rasa version 3.6.21 and all users are advised to upgrade. Users unable to upgrade should ensure that they require authentication and that only trusted users are given access.		
CVE-2024-56137	MaxKB RCE vulnerability in function library	MaxKB, which stands for Max Knowledge Base, is an open source knowledge base question-answering system based on a large language model and retrieval-augmented generation (RAG). Prior to version 1.9.0, a remote command execution vulnerability exists in the module of function library. The vulnerability allow privileged users to execute OS command in custom scripts. The vulnerability has been fixed in v1.9.0.	Patched by core rule	Y
CVE-2025-0528	Tenda AC8/AC10/AC18 HTTP Request telnet command injection	A vulnerability, which was classified as critical, has been found in Tenda AC8, AC10 and AC18 16.03.10.20. Affected by this issue is some unknown functionality of the file /goform/telnet of the component HTTP Request Handler. The manipulation leads to command injection.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-23209	Potential RCE with a compromised security key in craft/cms	Craft is a flexible, user-friendly CMS for creating custom digital experiences on the web and beyond. This is an remote code execution (RCE) vulnerability that affects Craft 4 and 5 installs where your security key has already been compromised. Anyone running an unpatched version of Craft with a compromised security key is affected. This vulnerability has been patched in Craft 5.5.8 and 4.13.8. Users who cannot update to a patched version, should rotate their security keys and ensure their privacy to help migitgate the issue.	Patched by core rule	Y

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-12951	1000 Projects Portfolio Management System MCA add_personal_details.php unrestricted upload	A vulnerability classified as critical has been found in 1000 Projects Portfolio Management System MCA 1.0. Affected is an unknown function of the file /add_personal_details.php. The manipulation of the argument profile leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by custom rule	N
CVE-2024-12953	1000 Projects Portfolio Management System MCA update_pd_process.php unrestricted upload	A vulnerability, which was classified as critical, has been found in 1000 Projects Portfolio Management System MCA 1.0. Affected by this issue is some unknown functionality of the file /update_pd_process.php. The manipulation of the argument profile leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by custom rule	N
CVE-2024-12954	1000 Projects Portfolio Management System MCA update_ach.php unrestricted upload	A vulnerability, which was classified as critical, was found in 1000 Projects Portfolio Management System MCA 1.0. This affects an unknown part of the file /update_ach.php. The manipulation of	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the argument ach_certy leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-12956	1000 Projects Portfolio Management System MCA add_achievement_details.php unrestricted upload	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 /add_achievement_details.php. The manipulation of the argument ach_certy leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by custom rule	N
CVE-2024-13022	taisan tarzan-cms Article Management UploadController.java UploadResponse unrestricted upload	A vulnerability, which was classified as critical, was found in taisan tarzan-cms 1.0.0. This affects the function UploadResponse of the file src/main/java/com/tarzan/cms/modules/admin/controller/common/UploadController.java of the component Article Management. The manipulation of the argument file leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by custom rule	N
CVE-2024-13133	ZeroWdd studentmanager StudentController.	A vulnerability, which was classified as critical, has been	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	java editStudent unrestricted upload	found in ZeroWdd studentmanager 1.0. This issue affects the function addStudent/editStudent of the file src/main/Java/com/wdd/studentmanager/controller/StudentController. java. The manipulation of the argument file leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-13134	ZeroWdd studentmanager TeacherController. java editTeacher unrestricted upload	A vulnerability, which was classified as critical, was found in ZeroWdd studentmanager 1.0. Affected is the function addTeacher/editTeacher of the file src/main/Java/com/wdd/studentmanager/controller/TeacherController. java. The manipulation of the argument file leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by custom rule	N
CVE-2024-13138	wangl1989 mysiteforme LocalUploadServiceImpl upload unrestricted upload	A vulnerability was found in wangl1989 mysiteforme 1.0. It has been declared as critical. This vulnerability affects the function upload of the file src/main/java/com/mysiteform/admin/service/ipl/LocalUploadServiceImpl. The manipulation of the argument test leads to unrestricted upload. The attack	Patched by custom rule	N

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.		
CVE-2024-13144	zhenfeng13 My-Blog BlogController.java uploadFileByEditomd unrestricted upload	A vulnerability classified as critical has been found in zhenfeng13 My-Blog 1.0. Affected is the function uploadFileByEditomd of the file src/main/java/com/site/blog/my/core/controller/admin/BlogController.java. The manipulation of the argument editormd-image-file leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by custom rule	N
CVE-2024-13145	zhenfeng13 My-Blog uploadController.java upload unrestricted upload	A vulnerability classified as critical was found in zhenfeng13 My-Blog 1.0. Affected by this vulnerability is the function upload of the file src/main/java/com/site/blog/my/core/controller/admin/uploadController. java. The manipulation of the argument file leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by custom rule	N
CVE-2024-13191	ZeroWdd myblog uploadController.java upload unrestricted upload	A vulnerability, which was classified as critical, has been found in ZeroWdd myblog 1.0. This issue affects the function upload of the file src/main/java/com/w	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		dd/myblog/controller/admin/uploadController.java. The manipulation of the argument file leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-13201	wander-chu SpringBoot-Blog Admin Attachment AttachtController.java upload unrestricted upload	A vulnerability has been found in wander-chu SpringBoot-Blog 1.0 and classified as critical. This vulnerability affects the function upload of the file src/main/java/com/my/blog/website/controller/admin/AttachtController.java of the component Admin Attachment Handler. The manipulation of the argument file leads to unrestricted upload. 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 custom rule	N
CVE-2024-13210	donglight bookstore电商书城系统说明 AdminBookController. java uploadPicture unrestricted upload	A vulnerability was found in donglight bookstore电商书城系统说明 1.0. It has been declared as critical. Affected by this vulnerability is the function uploadPicture of the file src/main/java/org/zdd/bookstore/web/controller/admin/AdminBookController.java. The	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument pictureFile leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-13212	SingMR HouseRent AddHouseControlle r.java upload unrestricted upload	A vulnerability classified as critical has been found in SingMR HouseRent 1.0. This affects the function singleUpload/upload of the file src/main/java/com/ho use/wym/controller/ AddHouseController. java. The manipulation of the argument file leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by custom rule	N
CVE-2025-0211	Campcodes School Faculty Scheduling System index.php file inclusion	A vulnerability was found in Campcodes School Faculty Scheduling System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/index.php. The manipulation of the argument page leads to file inclusion. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by custom rule	N
CVE-2025-0213	Campcodes Project Management System update_forms.php unrestricted upload	A vulnerability was found in Campcodes Project Management System 1.0. It has been declared as critical. This	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability affects unknown code of the file /forms/update_forms.php?action=change_pic2&id=4. The manipulation of the argument file leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-0335	code-projects Online Bike Rental System Change Image unrestricted upload	A vulnerability was found in code-projects Online Bike Rental System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the component Change Image Handler. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other endpoints might be affected as well.	Patched by custom rule	N
CVE-2025-0341	CampCodes Computer Laboratory Management System edit unrestricted upload	A vulnerability, which was classified as critical, has been found in CampCodes Computer Laboratory Management System 1.0. Affected by this issue is some unknown functionality of the file /class/edit/edit. The manipulation of the argument e_photo leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		used.		
CVE-2025-0346	code-projects Content Management System Publish News Page publishnews.php unrestricted upload	A vulnerability was found in code-projects Content Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/publishnews.php of the component Publish News Page. The manipulation of the argument image leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by custom rule	N
CVE-2025-0399	StarSea99 starsea-mall uploadController.java UploadController unrestricted upload	A vulnerability was found in StarSea99 starsea-mall 1.0. It has been declared as critical. This vulnerability affects the function UploadController of the file src/main/java/com/siro/mall/controller/common/uploadController.java. The manipulation of the argument file leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by custom rule	N
CVE-2025-0402	1902756969 reggie CommonController.java upload unrestricted upload	A vulnerability classified as critical was found in 1902756969 reggie 1.0. Affected by this vulnerability is the function upload of the file src/main/java/com/ith	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		eima/reggie/controller/CommonController.java. The manipulation of the argument file leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-0460	Blog Botz for Journal Theme blog_add unrestricted upload	A vulnerability, which was classified as critical, was found in Blog Botz for Journal Theme 1.0 on OpenCart. This affects an unknown part of the file /index.php?route=extension/module/blog_add. The manipulation of the argument image leads to unrestricted upload. 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 custom rule	N
CVE-2025-0463	Shanghai Lingdang Information Technology Lingdang CRM index.php unrestricted upload	A vulnerability was found in Shanghai Lingdang Information Technology Lingdang CRM up to 8.6.0.0. It has been classified as critical. Affected is an unknown function of the file /crm/weixinmp/index.php?userid=123&module=Users&usid=1&action=UsersAjax&minipro_const_type=1&related_module=Singin. The manipulation of the argument name	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		leads to unrestricted upload. 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.		
CVE-2025-0474	Invoice Ninja PDF Rendering Server Side Request Forgery	Invoice Ninja is vulnerable to authenticated Server-Side Request Forgery (SSRF) allowing for arbitrary file read and network resource requests as the application user. This issue affects Invoice Ninja: from 5.8.56 through 5.11.23.	Patched by custom rule	N
CVE-2025-0582	itsourcecode Farm Management System add-pig.php unrestricted upload	A vulnerability classified as critical was found in itsourcecode Farm Management System up to 1.0. This vulnerability affects unknown code of the file /add-pig.php. The manipulation of the argument pigphoto leads to unrestricted upload. The attack can be initiated remotely.	Patched by custom rule	N
CVE-2025-0702	JoeyBling bootplus SysFileController.java unrestricted upload	A vulnerability classified as critical was found in JoeyBling bootplus up to 247d5f6c209be1a5cf10cd0fa18e1d8cc63cf55d. This vulnerability affects unknown code of the file src/main/java/io/github/controller/SysFileController.java. The manipulation of the argument portraitFile leads to	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available.		
CVE-2025-21624	ClipBucket V5 Playlist Cover File Upload to Remote Code Execution	ClipBucket V5 provides open source video hosting with PHP. Prior to 5.5.1 - 239, a file upload vulnerability exists in the Manage Playlist functionality of the application, specifically surrounding the uploading of playlist cover images. Without proper checks, an attacker can upload a PHP script file instead of an image file, thus allowing a webshell or other malicious files to be stored and executed on the server. This attack vector exists in both the admin area and low-level user area. This vulnerability is fixed in 5.5.1 - 239.	Patched by custom rule	N

Server-side Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-13029	Antabot White-Jotter Edit Book book server-side request forgery	A vulnerability, which was classified as problematic, was found in Antabot White-Jotter up to 0.2.2. Affected is an unknown function of the file /admin/content/book of the component Edit Book Handler. The manipulation leads to server-side request forgery. 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-2024-13032	Antabot White-Jotter Article Editor editor server-side request forgery	A vulnerability classified as problematic was found in Antabot White-Jotter up to 0.2.2. Affected by this vulnerability is an unknown functionality of the file /admin/content/editor of the component Article Editor. The manipulation of the argument articleCover leads to server-side request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-13139	wangl1989 mysiteforme FileController doContent server-side request forgery	A vulnerability was found in wangl1989 mysiteforme 1.0. It has been rated as critical. This issue affects the function doContent of the file src/main/java/com/mysiteform/admin/controller/system/FileController. The manipulation of the argument content leads to server-side request	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-13195	donglight bookstore电商书城系统说明 HttpUtil.java getHtml server-side request forgery	A vulnerability was found in donglight bookstore电商书城系统说明 1.0.0. It has been classified as critical. This affects the function getHtml of the file src/main/java/org/zdd/bookstore/rawl/HttpUtil.java. The manipulation of the argument url leads to server-side request forgery. 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-2024-52594	Server-Side Request Forgery (SSRF) on redirects and federation in gomatrixserverlib	Gomatrixserverlib is a Go library for matrix federation. Gomatrixserverlib is vulnerable to server-side request forgery, serving content from a private network it can access, under certain conditions. The commit `c4f1e01` fixes this issue. Users are advised to upgrade. Users unable to upgrade should use a local firewall to limit the network segments and hosts the service using gomatrixserverlib can access.	Patched by core rule	Y
CVE-2024-52602	Server-Side Request Forgery (SSRF) on redirects and federation in Matrix Media Repo	Matrix Media Repo (MMR) is a highly configurable multi-homeserver media repository for Matrix. Matrix Media Repo (MMR) is vulnerable to server-side request	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		forgery, serving content from a private network it can access, under certain conditions. This is fixed in MMR v1.3.8. Users are advised to upgrade. Restricting which hosts MMR is allowed to contact via (local) firewall rules or a transparent proxy and may provide a workaround for users unable to upgrade.		
CVE-2024-56800	Firecrawl has SSRF Vulnerability via malicious scrape target	Firecrawl is a web scraper that allows users to extract the content of a webpage for a large language model. Versions prior to 1.1.1 contain a server-side request forgery (SSRF) vulnerability. The scraping engine could be exploited by crafting a malicious site that redirects to a local IP address. This allowed exfiltration of local network resources through the API. The cloud service was patched on December 27th, 2024, and the maintainers have checked that no user data was exposed by this vulnerability. Scraping engines used in the open sourced version of Firecrawl were patched on December 29th, 2024, except for the playwright services which the maintainers have determined to be un-patchable. All users of open-source software (OSS) Firecrawl should upgrade to v1.1.1. As a workaround, OSS Firecrawl users should supply the playwright	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		services with a secure proxy. A proxy can be specified through the `PROXY_SERVER` env in the environment variables. Please refer to the documentation for instructions. Ensure that the proxy server one is using is setup to block all traffic going to link-local IP addresses.		
CVE-2025-0480	wuzhicms config.php test server-side request forgery	A vulnerability classified as problematic has been found in wuzhicms 4.1.0. This affects the function test of the file coreframe/app/search/admin/config.php. The manipulation of the argument sphinxhost/sphinxport leads to server-side request forgery. 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-2025-21385	Microsoft Purview Information Disclosure Vulnerability	A Server-Side Request Forgery (SSRF) vulnerability in Microsoft Purview allows an authorized attacker to disclose information over a network.	Patched by core rule	Y

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-12939	code-projects Job Recruitment _all_edits.php add_edu sql injection	A vulnerability was found in code-projects Job Recruitment 1.0. It has been rated as critical. This issue affects the function add_edu of the file /_parse/_all_edits.php. The manipulation of the argument degree leads to sql injection. 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-2024-12940	1000 Projects Attendance Tracking Management System student_action.php sql injection	A vulnerability has been found in 1000 Projects Attendance Tracking Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/student_action.php. The manipulation of the argument student_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-2024-12941	CodeAstro Blood Donor Management System deletedannounce.php sql injection	A vulnerability was found in CodeAstro Blood Donor Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /pages/deletedannounce.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the public and may be used.		
CVE-2024-12942	1000 Projects Portfolio Management System MCA admin_login.php sql injection	A vulnerability was found in 1000 Projects Portfolio Management System MCA 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/admin_login.php. The manipulation of the argument username/password 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-2024-12943	CodeAstro House Rental Management System ownersignup.php sql injection	A vulnerability was found in CodeAstro House Rental Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /ownersignup.php. The manipulation of the argument f/e/p/m/o/n/c/s/ci/a leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "m" to be affected. But it must be assumed that many other parameters are affected as well.	Patched by core rule	Y
CVE-2024-12944	CodeAstro House Rental Management System signin.php sql injection	A vulnerability was found in CodeAstro House Rental Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the file /signin.php. The manipulation of the argument u/p leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-12945	code-projects Simple Car Rental System account.php sql injection	A vulnerability classified as critical was found in code-projects Simple Car Rental System 1.0. This vulnerability affects unknown code of the file /account.php. The manipulation of the argument email/pass 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-2024-12946	1000 Projects Attendance Tracking Management System admin_action.php sql injection	A vulnerability, which was classified as critical, has been found in 1000 Projects Attendance Tracking Management System 1.0. This issue affects some unknown processing of the file /admin/admin_action.php. The manipulation of the argument admin_user_name 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-2024-12947	Codezips Hospital Management System invo.php sql injection	A vulnerability was found in Codezips Hospital Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /invo.php. The manipulation of the argument dname leads to sql injection.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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-2024-12958	1000 Projects Portfolio Management System MCA update_pro_details.php sql injection	A vulnerability classified as critical has been found in 1000 Projects Portfolio Management System MCA 1.0. This affects an unknown part of the file /update_pro_details.php. The manipulation of the argument q 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-2024-12959	1000 Projects Portfolio Management System MCA update_personal_details.php sql injection	A vulnerability classified as critical was found in 1000 Projects Portfolio Management System MCA 1.0. This vulnerability affects unknown code of the file /update_personal_details.php. The manipulation of the argument q 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-2024-12960	1000 Projects Portfolio Management System MCA update_edu_details.php sql injection	A vulnerability, which was classified as critical, has been found in 1000 Projects Portfolio Management System MCA 1.0. This issue affects some unknown processing of the file /update_edu_details.php. The manipulation of the argument q	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-12961	1000 Projects Portfolio Management System MCA update_ach_details.php sql injection	A vulnerability, which was classified as critical, was found in 1000 Projects Portfolio Management System MCA 1.0. Affected is an unknown function of the file /update_ach_details.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.	Patched by core rule	Y
CVE-2024-12962	code-projects Job Recruitment _all_edits.php sql injection	A vulnerability has been found in code-projects Job Recruitment 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /_parse/_all_edits.php. The manipulation of the argument skillset 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-2024-12963	code-projects Job Recruitment _all_edits.php add_xp sql injection	A vulnerability was found in code-projects Job Recruitment 1.0 and classified as critical. Affected by this issue is the function add_xp of the file /_parse/_all_edits.php. The manipulation of the argument job_company leads to sql injection. The attack may be launched 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. Other parameters might be affected as well.		
CVE-2024-12964	1000 Projects Daily College Class Work Report Book login.php sql injection	A vulnerability was found in 1000 Projects Daily College Class Work Report Book 1.0. It has been classified as critical. This affects an unknown part of the file /login.php. The manipulation of the argument user 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-2024-12965	1000 Projects Portfolio Management System MCA update_ex_detail.php sql injection	A vulnerability was found in 1000 Projects Portfolio Management System MCA 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /update_ex_detail.php. The manipulation of the argument q 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-2024-12966	code-projects Job Recruitment _all_edits.php cn_update sql injection	A vulnerability was found in code-projects Job Recruitment 1.0. It has been rated as critical. This issue affects the function cn_update of the file /_parse/_all_edits.php. The manipulation of the argument cname/url leads to sql injection. The attack may be initiated 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-2024-12967	code-projects Job Recruitment _all_edits.php fln_update sql injection	A vulnerability classified as critical has been found in code-projects Job Recruitment 1.0. Affected is the function fln_update of the file /_parse/_all_edits.php. The manipulation of the argument fname/lname 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-2024-12968	code-projects Job Recruitment _all_edits.php edit_jobpost sql injection	A vulnerability classified as critical was found in code-projects Job Recruitment 1.0. Affected by this vulnerability is the function edit_jobpost of the file /_parse/_all_edits.php. The manipulation of the argument jobtype 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-2024-12969	code-projects Hospital Management System Login index.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Hospital Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/index.php of the component Login. The manipulation of the argument username/password leads to sql injection. The attack may be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-12976	CodeZips Hospital Management System staff.php sql injection	A vulnerability, which was classified as critical, has been found in CodeZips Hospital Management System 1.0. Affected by this issue is some unknown functionality of the file /staff.php. The manipulation of the argument tel 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.	Patched by core rule	Y
CVE-2024-12977	PHPGurukul Complaint Management System state.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Complaint Management System 1.0. This affects an unknown part of the file /admin/state.php. The manipulation of the argument state 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-2024-12978	code-projects Job Recruitment _all_edits.php add_req sql injection	A vulnerability has been found in code-projects Job Recruitment 1.0 and classified as critical. This vulnerability affects the function add_req of the file /_parse/_all_edits.php. The manipulation of the argument jid/limit leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and may be used.		
CVE-2024-12981	CodeAstro Car Rental System bookingconfirm.php sql injection	A vulnerability was found in CodeAstro Car Rental System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /bookingconfirm.php. The manipulation of the argument driver_id_from_dropdown 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-2024-13002	1000 Projects Bookstore Management System order_process.php sql injection	A vulnerability was found in 1000 Projects Bookstore Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /order_process.php. The manipulation of the argument fnm 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-2024-13003	1000 Projects Portfolio Management System MCA update_ed.php sql injection	A vulnerability was found in 1000 Projects Portfolio Management System MCA 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /update_ed.php. The manipulation of the argument e_id leads to sql injection. The attack may be launched 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-2024-13004	PHPGurukul Complaint Management System category.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Complaint Management System 1.0. This affects an unknown part of the file /admin/category.php. The manipulation of the argument state 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-2024-13005	1000 Projects Attendance Tracking Management System attendance_action.php sql injection	A vulnerability classified as critical was found in 1000 Projects Attendance Tracking Management System 1.0. This vulnerability affects unknown code of the file /admin/attendance_action.php. The manipulation of the argument attendance_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-2024-13006	1000 Projects Human Resource Management System employeeview.php sql injection	A vulnerability, which was classified as critical, has been found in 1000 Projects Human Resource Management System 1.0. This issue affects some unknown processing of the file /employeeview.php. The manipulation of the argument search leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and may be used.		
CVE-2024-13007	Codezips Event Management System contact.php sql injection	A vulnerability, which was classified as critical, was found in Codezips Event Management System 1.0. Affected is an unknown function of the file /contact.php. The manipulation of the argument title 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-2024-13008	code-projects Responsive Hotel Site newsletter.php sql injection	A vulnerability has been found in code-projects Responsive Hotel Site 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/newsletter.php. The manipulation of the argument eid 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-2024-13024	Codezips Blood Bank Management System campaign.php sql injection	A vulnerability was found in Codezips Blood Bank Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /campaign.php. The manipulation of the argument cname leads to sql injection. 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-2024-13025	Codezips College	A vulnerability was	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Management System faculty.php sql injection	found in Codezips College Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /Front-end/faculty.php. The manipulation of the argument book_name/book_author 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-2024-13037	1000 Projects Attendance Tracking Management System report.php attendance_report sql injection	A vulnerability was found in 1000 Projects Attendance Tracking Management System 1.0. It has been classified as critical. Affected is the function attendance_report of the file /admin/report.php. The manipulation of the argument course_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-2024-13038	CodeAstro Simple Loan Management System Login index.php sql injection	A vulnerability was found in CodeAstro Simple Loan Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /index.php of the component Login. The manipulation of the argument email leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and may be used.		
CVE-2024-13039	code-projects Simple Chat System add_user.php sql injection	A vulnerability was found in code-projects Simple Chat System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /add_user.php. The manipulation of the argument name/email/password/number 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-2024-13070	CodeAstro Online Food Ordering System Update User Page update_users.php sql injection	A vulnerability was found in CodeAstro Online Food Ordering System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/update_users.php of the component Update User Page. The manipulation of the argument user_upd 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-2024-13072	1000 Projects Beauty Parlour Management System Customer Detail add-customer-services.php sql injection	A vulnerability was found in 1000 Projects Beauty Parlour Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/add-customer-services.php of the component Customer Detail Handler. The manipulation of the argument sids[] leads	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-13092	code-projects Job Recruitment Job Post search_ajax.php sql injection	A vulnerability classified as critical was found in code-projects Job Recruitment 1.0. This vulnerability affects unknown code of the file /_parse/_call_job/search_ajax.php of the component Job Post Handler. The manipulation of the argument n 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-2024-13093	code-projects Job Recruitment Seeker Profile _call_main_search_ajax.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 /_parse/_call_main_search_ajax.php of the component Seeker Profile Handler. The manipulation of the argument s1 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-2024-13193	SEMCMS Image Library Management Page SEMCMS_Images.php sql injection	A vulnerability has been found in SEMCMS up to 4.8 and classified as critical. Affected by this vulnerability is an unknown functionality of the file SEMCMS_Images.php of the component	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Image Library Management Page. The manipulation 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.		
CVE-2024-13194	Sucms admin_members.php sql injection	A vulnerability was found in Sucms 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/admin_members.php?ac=search. 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-2024-13426	WP-Polls <= 2.77.2 - Unauthenticated SQL Injection to Stored Cross-Site Scripting	The WP-Polls plugin for WordPress is vulnerable to SQL Injection via COOKIE in all versions up to, and including, 2.77.2 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. Those queries are stored and results are not displayed to the attacker, which means they cannot be exploited to obtain any additional information about the database. However, a properly configured payload allows for the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		injection of malicious JavaScript resulting in Stored Cross-Site Scripting.		
CVE-2024-45600	Fields GLPI plugin has an Authenticated SQL Injection	Fields is a GLPI plugin that allows users to add custom fields on GLPI items forms. Prior to 1.21.13, an authenticated user can perform a SQL injection when the plugin is active. The vulnerability is fixed in 1.21.13.	Patched by core rule	Y
CVE-2024-56801	Tasklists has Blind SQL Injection in /ajax/reorder.php	Tasklists provides plugin tasklists for GLPI. Versions prior to 2.0.4 have a blind SQL injection vulnerability. Version 2.0.4 contains a patch for the vulnerability.	Patched by core rule	Y
CVE-2025-0168	code-projects Job Recruitment _feedback_system.php sql injection	A vulnerability classified as critical has been found in code-projects Job Recruitment 1.0. This affects an unknown part of the file /_parse/_feedback_system.php. The manipulation of the argument person 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-2025-0171	code-projects Chat System deleteuser.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Chat System 1.0. Affected is an unknown function of the file /admin/deleteuser.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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-0172	code-projects Chat System deleteroom.php sql injection	A vulnerability has been found in code-projects Chat System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/deleteroom.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-2025-0173	SourceCodester Online Eyewear Shop view_order.php sql injection	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /orders/view_order.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-2025-0174	code-projects Point of Sales and Inventory Management System Parameter search_result2.php sql injection	A vulnerability was found in code-projects Point of Sales and Inventory Management System 1.0. It has been classified as critical. This affects an unknown part of the file /user/search_result2.php of the component Parameter Handler. The manipulation of the argument search 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-0176	code-projects Point of Sales and Inventory Management System add_cart.php sql injection	A vulnerability was found in code-projects Point of Sales and Inventory Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /user/add_cart.php. The manipulation of the argument id/qty 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-2025-0195	code-projects Point of Sales and Inventory Management System del_product.php sql injection	A vulnerability was found in code-projects Point of Sales and Inventory Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /user/del_product.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-2025-0196	code-projects Point of Sales and Inventory Management System plist.php sql injection	A vulnerability classified as critical has been found in code-projects Point of Sales and Inventory Management System 1.0. This affects an unknown part of the file /user/plist.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-2025-0197	code-projects Point of Sales and	A vulnerability classified as critical	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Inventory Management System search.php sql injection	was found in code-projects Point of Sales and Inventory Management System 1.0. This vulnerability affects unknown code of the file /user/search.php. The manipulation of the argument name leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-0198	code-projects Point of Sales and Inventory Management System search_result.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Point of Sales and Inventory Management System 1.0. This issue affects some unknown processing of the file /user/search_result.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-2025-0199	code-projects Point of Sales and Inventory Management System minus_cart.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Point of Sales and Inventory Management System 1.0. Affected is an unknown function of the file /user/minus_cart.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-2025-0200	code-projects Point of Sales and Inventory	A vulnerability has been found in code-projects Point of Sales	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Management System search_num.php sql injection	and Inventory Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /user/search_num.php. The manipulation of the 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-2025-0201	code-projects Point of Sales and Inventory Management System update_account.php sql injection	A vulnerability was found in code-projects Point of Sales and Inventory Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /user/update_account.php. The manipulation of the argument username 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-2025-0203	code-projects Student Management System DbFunction.php showSubject1 sql injection	A vulnerability was found in code-projects Student Management System 1.0. It has been declared as critical. This vulnerability affects the function showSubject1 of the file /config/DbFunction.php. The manipulation of the argument sid 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-0204	code-projects Online Shoe Store details.php sql injection	A vulnerability was found in code-projects Online Shoe Store 1.0. It has been rated as critical. This issue affects some unknown processing of the file /details.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-2025-0205	code-projects Online Shoe Store details2.php sql injection	A vulnerability classified as critical has been found in code-projects Online Shoe Store 1.0. Affected is an unknown function of the file /details2.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-2025-0207	code-projects Online Shoe Store login.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Online Shoe Store 1.0. Affected by this issue is some unknown functionality of the file /function/login.php. The manipulation of the argument password 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-2025-0208	code-projects Online Shoe Store summary.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Online Shoe Store 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 /summary.php. The manipulation of the argument tid 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-2025-0210	Campcodes School Faculty Scheduling System ajax.php sql injection	A vulnerability has been found in Campcodes School Faculty Scheduling System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/ajax.php?action=login. 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-2025-0212	Campcodes Student Grading System view_students.php sql injection	A vulnerability was found in Campcodes Student Grading System 1.0. It has been classified as critical. This affects an unknown part of the file /view_students.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-2025-0214	TMD Custom Header Menu index.php sql injection	A vulnerability was found in TMD Custom Header Menu 4.0.0.1 on OpenCart. It has been rated as problematic. This issue affects some unknown processing of the file /admin/index.php. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument headermenu_id leads to sql injection. The attack may be initiated remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component.		
CVE-2025-0229	code-projects Travel Management System enquiry.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Travel Management System 1.0. This issue affects some unknown processing of the file /enquiry.php. The manipulation of the argument pid/t1/t2/t3/t4/t5/t6/t7 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-2025-0230	code-projects Responsive Hotel Site print.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Responsive Hotel Site 1.0. Affected is an unknown function of the file /admin/print.php. The manipulation of the argument pid 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-2025-0231	Codezips Gym Management System submit_payments.php sql injection	A vulnerability has been found in Codezips Gym Management System 1.0 and classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		critical. Affected by this vulnerability is an unknown functionality of the file /dashboard/admin/submit_payments.php. The manipulation of the argument m_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-0232	Codezips Blood Bank Management System successadmin.php sql injection	A vulnerability was found in Codezips Blood Bank Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /successadmin.php. The manipulation of the argument psw 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-2025-0233	Codezips Project Management System course.php sql injection	A vulnerability was found in Codezips Project Management System 1.0. It has been classified as critical. This affects an unknown part of the file /pages/forms/course.php. The manipulation of the argument course_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.	Patched by core rule	Y
CVE-2025-0294	SourceCodester Home Clean Services Management System process.php sql injection	A vulnerability has been found in SourceCodester Home Clean Services Management System 1.0 and classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		critical. Affected by this vulnerability is an unknown functionality of the file /public_html/admin/process.php. The manipulation of the argument type/length/business 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-2025-0296	code-projects Online Book Shop booklist.php sql injection	A vulnerability was found in code-projects Online Book Shop 1.0. It has been classified as critical. This affects an unknown part of the file /booklist.php. The manipulation of the argument subcatid 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-2025-0297	code-projects Online Book Shop detail.php sql injection	A vulnerability was found in code-projects Online Book Shop 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /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-2025-0298	code-projects Online Book Shop process_login.php sql injection	A vulnerability was found in code-projects Online Book Shop 1.0. It has been rated as critical. 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
		/process_login.php. The manipulation of the argument usernm leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-0299	code-projects Online Book Shop search_result.php sql injection	A vulnerability classified as critical has been found in code-projects Online Book Shop 1.0. Affected is an unknown function of the file /search_result.php. The manipulation of the argument s 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-2025-0300	code-projects Online Book Shop subcat.php sql injection	A vulnerability classified as critical was found in code-projects Online Book Shop 1.0. Affected by this vulnerability is an unknown functionality of the file /subcat.php. The manipulation of the argument cat 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-2025-0333	leiyuxi cy-fast listData sql injection	A vulnerability, which was classified as critical, was found in leiyuxi cy-fast 1.0. Affected is the function listData of the file /sys/role/listData. The manipulation of the argument order leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and may be used.		
CVE-2025-0334	leiyuxi cy-fast listData sql injection	A vulnerability has been found in leiyuxi cy-fast 1.0 and classified as critical. Affected by this vulnerability is the function listData of the file /sys/user/listData. The manipulation of the argument order 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-2025-0336	Codezips Project Management System teacher.php sql injection	A vulnerability was found in Codezips Project Management System 1.0. It has been classified as critical. This affects an unknown part of the file /pages/forms/teacher.php. The manipulation of the argument 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.	Patched by core rule	Y
CVE-2025-0344	leiyuxi cy-fast listData sql injection	A vulnerability has been found in leiyuxi cy-fast 1.0 and classified as critical. Affected by this vulnerability is the function listData of the file /commpara/listData. The manipulation of the argument order 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-2025-0345	leiyuxi cy-fast listData sql injection	A vulnerability was found in leiyuxi cy-fast 1.0 and classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		critical. Affected by this issue is the function listData of the file /sys/menu/listData. The manipulation of the argument order leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-0347	code-projects Admission Management System Login index.php sql injection	A vulnerability was found in code-projects Admission Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file index.php of the component Login. The manipulation of the argument u_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-2025-0391	Guangzhou Huayi Intelligent Technology Jeewms CgFormBuildController. java saveOrUpdate sql injection	A vulnerability, which was classified as critical, has been found in Guangzhou Huayi Intelligent Technology Jeewms up to 20241229. This issue affects the function saveOrUpdate of the file org/jeecgframework/web/cgform/controller/build/CgFormBuildController. java. The manipulation leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 20250101 is able to address this issue. It is recommended to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		upgrade the affected component.		
CVE-2025-0392	Guangzhou Huayi Intelligent Technology Jeewms graphReportControll er.do datagridGraph sql injection	A vulnerability, which was classified as critical, was found in Guangzhou Huayi Intelligent Technology Jeewms up to 20241229. Affected is the function datagridGraph of the file /graphReportControlle r.do. The manipulation of the argument store_code leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 20250101 is able to address this issue. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-0404	liujianview gymxmjpa CoachController.jav a CoachController sql injection	A vulnerability has been found in liujianview gymxmjpa 1.0 and classified as critical. This vulnerability affects the function CoachController of the file src/main/java/com/liuji an/gymxmjpa/controll er/CoachController.jav a. The manipulation of the argument coachName 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-2025-0405	liujianview gymxmjpa GoodsController.jav a GoodsDaoImpl sql injection	A vulnerability was found in liujianview gymxmjpa 1.0 and classified as critical. This issue affects the function GoodsDaoImpl of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file src/main/java/com/liujian/gymxmjpa/controller/GoodsController.java. The manipulation of the argument goodsName leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-0406	liujianview gymxmjpa SubjectController.java SubjectDaoImpl sql injection	A vulnerability was found in liujianview gymxmjpa 1.0. It has been classified as critical. Affected is the function SubjectDaoImpl of the file src/main/java/com/liujian/gymxmjpa/controller/SubjectController.java. The manipulation of the argument subname 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-2025-0407	liujianview gymxmjpa EquipmentController.java EquipmentDaoImpl sql injection	A vulnerability was found in liujianview gymxmjpa 1.0. It has been declared as critical. Affected by this vulnerability is the function EquipmentDaoImpl of the file src/main/java/com/liujian/gymxmjpa/controller/EquipmentController.java. The manipulation of the argument hyname 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-2025-0408	liujianview gymxmjpa	A vulnerability was found in liujianview	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	LoosController.java LoosDaoImpl sql injection	gymxmjpa 1.0. It has been rated as critical. Affected by this issue is the function LoosDaoImpl of the file src/main/java/com/liujian/gymxmjpa/controller/LoosController.java. The manipulation of the argument loosName leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-0409	liujianview gymxmjpa MembertypeController.java MembertypeDaoImpl sql injection	A vulnerability classified as critical has been found in liujianview gymxmjpa 1.0. This affects the function MembertypeDaoImpl of the file src/main/java/com/liujian/gymxmjpa/controller/MembertypeController.java. The manipulation of the argument typeName 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-2025-0410	liujianview gymxmjpa MenberConntroller.java MenberDaoInpl sql injection	A vulnerability classified as critical was found in liujianview gymxmjpa 1.0. This vulnerability affects the function MenberDaoInpl of the file src/main/java/com/liujian/gymxmjpa/controller/MenberConntroller.java. The manipulation of the argument hyname leads to sql injection. The attack can be initiated 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-2025-0462	Shanghai Lingdang Information Technology Lingdang CRM index.php sql injection	A vulnerability was found in Shanghai Lingdang Information Technology Lingdang CRM up to 8.6.0.0 and classified as critical. This issue affects some unknown processing of the file /crm/weixinmp/index.php?userid=123&module=Users&usid=1&action=UsersAjax&minipro_const_type=1. The manipulation of the argument searchcontent leads to sql 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-2025-0486	Fanli2012 native-php-cms login.php sql injection	A vulnerability was found in Fanli2012 native-php-cms 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /fladmin/login.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-2025-0487	Fanli2012 native-php-cms cat_edit.php sql injection	A vulnerability was found in Fanli2012 native-php-cms 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /fladmin/cat_edit.php. The manipulation of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-0488	Fanli2012 native-php-cms product_list.php sql injection	A vulnerability classified as critical has been found in Fanli2012 native-php-cms 1.0. This affects an unknown part of the file product_list.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-2025-0489	Fanli2012 native-php-cms friendlink_dodel.php sql injection	A vulnerability classified as critical was found in Fanli2012 native-php-cms 1.0. This vulnerability affects unknown code of the file /fladmin/friendlink_dodel.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-2025-0490	Fanli2012 native-php-cms article_dodel.php sql injection	A vulnerability, which was classified as critical, has been found in Fanli2012 native-php-cms 1.0. This issue affects some unknown processing of the file /fladmin/article_dodel.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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-0491	Fanli2012 native-php-cms cat_dodel.php sql injection	A vulnerability, which was classified as critical, was found in Fanli2012 native-php-cms 1.0. Affected is an unknown function of the file /fladmin/cat_dodel.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-2025-0527	code-projects Admission Management System signupconfirm.php sql injection	A vulnerability classified as critical was found in code-projects Admission Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /signupconfirm.php. The manipulation of the argument in_eml 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-2025-0531	code-projects Chat System leaveroom.php sql injection	A vulnerability was found in code-projects Chat System 1.0 and classified as critical. This issue affects some unknown processing of the file /user/leaveroom.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-2025-0532	Codezips Gym Management System	A vulnerability was found in Codezips Gym Management System	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	new_submit.php sql injection	1.0. It has been classified as critical. Affected is an unknown function of the file /dashboard/admin/new_submit.php. The manipulation of the argument m_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-2025-0533	1000 Projects Campaign Management System Platform for Women sc_login.php sql injection	A vulnerability was found in 1000 Projects Campaign Management System Platform for Women 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /Code/sc_login.php. The manipulation of the argument uname 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-2025-0534	1000 Projects Campaign Management System Platform for Women loginnew.php sql injection	A vulnerability was found in 1000 Projects Campaign Management System Platform for Women 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /Code/loginnew.php. The manipulation of the argument Username 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-2025-0535	Codezips Gym	A vulnerability	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Management System edit_mem_submit.php sql injection	classified as critical has been found in Codezips Gym Management System 1.0. This affects an unknown part of the file /dashboard/admin/edit_mem_submit.php. The manipulation of the argument uid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	core rule	
CVE-2025-0536	1000 Projects Attendance Tracking Management System edit_action.php sql injection	A vulnerability classified as critical was found in 1000 Projects Attendance Tracking Management System 1.0. This vulnerability affects unknown code of the file /admin/edit_action.php. The manipulation of the argument attendance_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-2025-0540	itsourcecode Tailoring Management System expadd.php sql injection	A vulnerability has been found in itsourcecode Tailoring Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /expadd.php. The manipulation of the argument expcat 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-2025-0541	Codezips Gym Management System	A vulnerability was found in Codezips Gym Management System	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	edit_member.php sql injection	1.0 and classified as critical. This issue affects some unknown processing of the file /dashboard/admin/edit_member.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. Other parameters might be affected as well.		
CVE-2025-0558	TDuckCloud tduck-platform QueryProThemeRequest.java QueryProThemeRequest sql injection	A vulnerability classified as critical was found in TDuckCloud tduck-platform up to 4.0. This vulnerability affects the function QueryProThemeRequest of the file src/main/java/com/tduck/cloud/form/request/QueryProThemeRequest.java. The manipulation of the argument color 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-2025-0561	itsourcecode Farm Management System add-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 /add-pig.php. The manipulation of the argument pigno leads to sql injection. The attack can be initiated 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-2025-0562	Codezips Gym Management System health_status_entry .php sql injection	A vulnerability was found in Codezips Gym Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /dashboard/admin/hea lth_status_entry.php. The manipulation of the argument usrid 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-2025-0563	code-projects Fantasy-Cricket update.php sql injection	A vulnerability was found in code-projects Fantasy-Cricket 1.0. It has been classified as critical. Affected is an unknown function of the file /dash/update.php. The manipulation of the argument uname 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-2025-0564	code-projects Fantasy-Cricket authenticate.php sql injection	A vulnerability was found in code-projects Fantasy-Cricket 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /authenticate.php. The manipulation of the argument uname 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-2025-0565	ZZCMS index.php sql injection	A vulnerability was found in ZZCMS 2023. It has been rated as critical. Affected by	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		this issue is some unknown functionality of the file /index.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.		
CVE-2025-0579	Shiprocket Module REST API Module restapi sql injection	A vulnerability was found in Shiprocket Module 3/4 on OpenCart. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /index.php?route=extension/shiprocket/module/restapi of the component REST API Module. The manipulation of the argument x-username 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-2025-0698	JoeyBling bootplus list sql injection	A vulnerability was found in JoeyBling bootplus up to 247d5f6c209be1a5cf10cd0fa18e1d8cc63cf55d. It has been classified as critical. Affected is an unknown function of the file /admin/sys/menu/list. The manipulation of the argument sort/order leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		releases is used by this product. Therefore, no version details of affected nor updated releases are available.		
CVE-2025-0699	JoeyBling bootplus list sql injection	A vulnerability was found in JoeyBling bootplus up to 247d5f6c209be1a5cf10cd0fa18e1d8cc63cf55d. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/sys/role/list. The manipulation of the argument sort leads to sql injection. The attack can be launched 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.	Patched by core rule	Y
CVE-2025-0700	JoeyBling bootplus list sql injection	A vulnerability was found in JoeyBling bootplus up to 247d5f6c209be1a5cf10cd0fa18e1d8cc63cf55d. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/sys/log/list. The manipulation of the argument logId leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-0701	JoeyBling bootplus list sql injection	A vulnerability classified as critical has been found in JoeyBling bootplus up to 247d5f6c209be1a5cf10cd0fa18e1d8cc63cf55d. This affects an unknown part of the file /admin/sys/user/list. The manipulation of the argument sort 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 takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available.	Patched by core rule	Y
CVE-2025-22140	WeGIA SQL Injection (Blind Time-Based) endpoint 'dependente_listar_um.php' parameter 'id_dependente'	WeGIA is a web manager for charitable institutions. A SQL Injection vulnerability was identified in the /html/funcionario/dependente_listar_um.php endpoint, specifically in the id_dependente parameter. This vulnerability allows attackers to execute arbitrary SQL commands, compromising the confidentiality, integrity, and availability of the database. This vulnerability is fixed in 3.2.8.	Patched by core rule	Y
CVE-2025-22141	WeGIA SQL Injection (Blind Time-Based) endpoint 'verificar_recursos_cargo.php' parameter 'cargo'	WeGIA is a web manager for charitable institutions. A SQL Injection vulnerability was identified in the /dao/verificar_recursos_cargo.php endpoint, specifically in the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cargo parameter. This vulnerability allows attackers to execute arbitrary SQL commands, compromising the confidentiality, integrity, and availability of the database. This vulnerability is fixed in 3.2.8.		
CVE-2025-22214	N/A	Landray EIS 2001 through 2006 allows Message/fi_message_receiver.aspx?replyid= SQL injection.	Patched by core rule	Y
CVE-2025-22710	WordPress Smart Manager Plugin <= 8.52.0 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in StoreApps Smart Manager allows Blind SQL Injection. This issue affects Smart Manager: from n/a through 8.52.0.	Patched by core rule	Y
CVE-2025-23218	WeGIA has a SQL Injection endpoint 'adicionar_especie.php' parameter 'especie'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A SQL Injection vulnerability was identified in the WeGIA application, specifically in the adicionar_especie.php endpoint. This vulnerability allows attackers to execute arbitrary SQL commands in the database, allowing unauthorized access to sensitive information. During the exploit, it was possible to perform a complete dump of the application's database, highlighting the severity of the flaw. This vulnerability	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		is fixed in 3.2.10.		
CVE-2025-23219	WeGIA has a SQL Injection endpoint 'adicionar_cor.php' parameter 'cor'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A SQL Injection vulnerability was identified in the WeGIA application, specifically in the adicionar_cor.php endpoint. This vulnerability allows attackers to execute arbitrary SQL commands in the database, allowing unauthorized access to sensitive information. During the exploit, it was possible to perform a complete dump of the application's database, highlighting the severity of the flaw. This vulnerability is fixed in 3.2.10.	Patched by core rule	Y
CVE-2025-23220	WeGIA has a SQL Injection endpoint 'adicionar_raca.php' parameter 'raca'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A SQL Injection vulnerability was identified in the WeGIA application, specifically in the adicionar_raca.php endpoint. This vulnerability allows attackers to execute arbitrary SQL commands in the database, allowing unauthorized access to sensitive information. During the exploit, it was possible to perform a complete dump of the application's database, highlighting the severity of the flaw. This vulnerability	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		is fixed in 3.2.10.		

XML External Entity Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-52807	XXE vulnerability in XSLT parsing in `org.hl7.fhir.publisher`	The HL7 FHIR IG publisher is a tool to take a set of inputs and create a standard FHIR IG. Prior to version 1.7.4, XSLT transforms performed by various components are vulnerable to XML external entity injections. A processed XML file with a malicious DTD tag `( ]>` could produce XML containing data from the host system. This impacts use cases where org.hl7.fhir.publisher is being used to within a host where external clients can submit XML. A previous release provided an incomplete solution revealed by new testing. This issue has been patched as of version 1.7.4. No known workarounds are available.	Patched by core rule	Y
CVE-2024-56322	GoCD vulnerable to XXE injection via abuse of unused XML configuration repository functionality	GoCD is a continuous deliver server. GoCD versions 16.7.0 through 24.4.0 (inclusive) can allow GoCD admins to abuse a hidden/unused configuration repository (pipelines as code) feature to allow XML External Entity (XXE) injection on the GoCD Server which will be executed when GoCD periodically scans configuration repositories for pipeline updates, or is triggered by an administrator or config repo admin. In	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		practice the impact of this vulnerability is limited, in most cases without combining with another vulnerability, as only GoCD (super) admins have the ability to abuse this vulnerability. Typically a malicious GoCD admin can cause much larger damage than that they can do with XXE injection. The issue is fixed in GoCD 24.5.0. As a workaround, prevent external access from the GoCD server to arbitrary locations using some kind of environment egress control.		

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-56361	Stored Cross-Site Scripting (XSS) in lgsl v7.0	LGSL (Live Game Server List) provides online status for games. Before 7.0.0, a stored cross-site scripting (c) vulnerability was identified in lgsl. The function lgsl_query_40 in lgsl_protocol.php has implemented an HTTP crawler. This function makes a request to the registered game server, and upon crawling the malicious /info endpoint with our payload, will render our javascript on the info page. This information is being displayed via lgsl_details.php. This vulnerability is fixed in 7.0.0.	Patched by core rule	Y
CVE-2024-12979	code-projects Job Recruitment _all_edits.php cn_update cross site scripting	A vulnerability was found in code-projects Job Recruitment 1.0 and classified as problematic. This issue affects the function cn_update of the file /_parse/_all_edits.php. The manipulation of the argument cname 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-2024-12980	code-projects Job Recruitment _all_edits.php fln_update cross site scripting	A vulnerability was found in code-projects Job Recruitment 1.0. It has been classified as problematic. Affected is the function fln_update of the file /_parse/_all_edits.php. The manipulation of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the argument fname/lname 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-2024-12983	code-projects Hospital Management System Edit Doctor Details Page manage-doctors.php cross site scripting	A vulnerability classified as problematic has been found in code-projects Hospital Management System 1.0. This affects an unknown part of the file /hospital/hms/admin/manage-doctors.php of the component Edit Doctor Details Page. The manipulation of the argument Doctor 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. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2024-12991	Beijing Longda Jushang Technology DBShop 商城系统 home-order cross site scripting	A vulnerability was found in Beijing Longda Jushang Technology DBShop商城系统 3.3 Release 231225. It has been declared as problematic. This vulnerability affects unknown code of the file /home-order. The manipulation of the argument orderStatus with the input %22%3E%3Csvg%20onload=alert(5888)%3E 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		this disclosure but did not respond in any way.		
CVE-2024-56507	Reflected Cross-Site Scripting (XSS) Vulnerability in LinkAce	LinkAce is a self-hosted archive to collect links of your favorite websites. Prior to 1.15.6, a reflected cross-site scripting (XSS) vulnerability exists in the LinkAce. This issue occurs in the "URL" field of the "Edit Link" module, where user input is not properly sanitized or encoded before being reflected in the HTML response. This allows attackers to inject and execute arbitrary JavaScript in the context of the victim's browser, leading to potential session hijacking, data theft, and unauthorized actions. This vulnerability is fixed in 1.15.6.	Patched by core rule	Y
CVE-2024-12995	ruifang-tech Rebuild Project Tasks Section tasks cross site scripting	A vulnerability classified as problematic has been found in ruifang-tech Rebuild 3.8.6. This affects an unknown part of the file /project/050-900000000000001/tasks of the component Project Tasks Section. The manipulation of the argument description 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 respond in any way.	Patched by core rule	Y
CVE-2024-13021	SourceCodester Road Accident Map	A vulnerability, which was classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Marker add-mark.php cross site scripting	problematic, has been found in SourceCodester Road Accident Map Marker 1.0. Affected by this issue is some unknown functionality of the file /endpoint/add-mark.php. The manipulation of the argument mark_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.		
CVE-2024-13031	Antabot White-Jotter Article Content Editor editor cross site scripting	A vulnerability classified as problematic has been found in Antabot White-Jotter up to 0.2.2. Affected is an unknown function of the file /admin/content/editor of the component Article Content Editor. 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.	Patched by core rule	Y
CVE-2024-56517	LGSL has a reflected XSS at /lgsl_files/lgsl_list.php	LGSL (Live Game Server List) provides online status lists for online video games. Versions up to and including 6.2.1 contain a reflected cross-site scripting vulnerability in the `Referer` HTTP header. The vulnerability allows attackers to inject arbitrary JavaScript code, which is reflected in the HTML response without proper sanitization. When crafted	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		malicious input is provided in the `Referer` header, it is echoed back into an HTML attribute in the application's response. Commit 7ecb839df9358d21f64cdbff5b2536af25a77de1 contains a patch for the issue.		
CVE-2024-56733	Password Pusher Allows Session Token Interception Leading to Potential Hijacking	Password Pusher is an open source application to communicate sensitive information over the web. A vulnerability has been reported in versions 1.50.3 and prior where an attacker can copy the session cookie before a user logs out, potentially allowing session hijacking. Although the session token is replaced and invalidated upon logout, if an attacker manages to capture the session cookie before this process, they can use the token to gain unauthorized access to the user's session until the token expires or is manually cleared. This vulnerability hinges on the attacker's ability to access the session cookie during an active session, either through a man-in-the-middle attack, by exploiting another vulnerability like XSS, or via direct access to the victim's device. Although there is no direct resolution to this vulnerability, it is recommended to always use the latest version of Password Pusher to best mitigate risk. If self-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		hosting, ensure Password Pusher is hosted exclusively over SSL connections to encrypt traffic and prevent session cookies from being intercepted in transit. Additionally, implement best practices in local security to safeguard user systems, browsers, and data against unauthorized access.		
CVE-2024-13069	SourceCodester Multi Role Login System add-user.php cross site scripting	A vulnerability was found in SourceCodester Multi Role Login System 1.0. It has been classified as problematic. Affected is an unknown function of the file /endpoint/add-user.php. The manipulation of the argument name 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-2024-56365	PhpSpreadsheet vulnerable to unauthorized reflected XSS in the constructor of the Downloader class	PhpSpreadsheet is a PHP library for reading and writing spreadsheet files. Versions prior to 3.7.0, 2.3.5, 2.1.6, and 1.29.7 are vulnerable to unauthorized reflected cross-site scripting in the constructor of the `Downloader` class. Using the `/vendor/phpoffice/phpspreadsheet/samples/download.php` script, an attacker can perform a cross-site scripting attack. Versions 3.7.0, 2.3.5, 2.1.6, and 1.29.7 contain a patch for the issue.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-56366	PhpSpreadsheet vulnerable to unauthorized reflected XSS in the Accounting.php file	PhpSpreadsheet is a PHP library for reading and writing spreadsheet files. Versions prior to 3.7.0, 2.3.5, 2.1.6, and 1.29.7 are vulnerable to unauthorized reflected cross-site scripting in the `Accounting.php` file. Using the `/vendor/phpoffice/phpspreadsheet/samples/Wizards/NumberFormat/Accounting.php` script, an attacker can perform a cross-site scripting attack. Versions 3.7.0, 2.3.5, 2.1.6, and 1.29.7 contain a patch for the issue.	Patched by core rule	Y
CVE-2024-56408	PhpSpreadsheet allows unauthorized reflected XSS in `Convert-Online.php` file	PhpSpreadsheet is a PHP library for reading and writing spreadsheet files. Versions prior to 3.7.0, 2.3.5, 2.1.6, and 1.29.7 have no sanitization in the `/vendor/phpoffice/phpspreadsheet/samples/Engineering/Convert-Online.php` file, which leads to the possibility of a cross-site scripting attack. Versions 3.7.0, 2.3.5, 2.1.6, and 1.29.7 contain a patch for the issue.	Patched by core rule	Y
CVE-2024-56409	PhpSpreadsheet vulnerable to unauthorized reflected XSS in Currency.php file	PhpSpreadsheet is a PHP library for reading and writing spreadsheet files. Versions prior to 3.7.0, 2.3.5, 2.1.6, and 1.29.7 are vulnerable to unauthorized reflected cross-site scripting in the `Currency.php` file. Using the `/vendor/phpoffice/phpspreadsheet/samples/Wizards/NumberForm	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		at/Currency.php` script, an attacker can perform a cross-site scripting attack. Versions 3.7.0, 2.3.5, 2.1.6, and 1.29.7 contain a patch for the issue.		
CVE-2024-56410	PhpSpreadsheet has Cross-Site Scripting (XSS) vulnerability in custom properties	PhpSpreadsheet is a PHP library for reading and writing spreadsheet files. Versions prior to 3.7.0, 2.3.5, 2.1.6, and 1.29.7 have a cross-site scripting (XSS) vulnerability in custom properties. The HTML page is generated without clearing custom properties. Versions 3.7.0, 2.3.5, 2.1.6, and 1.29.7 contain a patch for the issue.	Patched by core rule	Y
CVE-2024-56411	PhpSpreadsheet has Cross-Site Scripting (XSS) vulnerability of the hyperlink base in the HTML page header	PhpSpreadsheet is a PHP library for reading and writing spreadsheet files. Versions prior to 3.7.0, 2.3.5, 2.1.6, and 1.29.7 have a cross-site scripting (XSS) vulnerability of the hyperlink base in the HTML page header. The HTML page is formed without sanitizing the hyperlink base. Versions 3.7.0, 2.3.5, 2.1.6, and 1.29.7 contain a patch for the issue.	Patched by core rule	Y
CVE-2024-56412	PhpSpreadsheet vulnerable to bypass of the XSS sanitizer using the javascript protocol and special characters	PhpSpreadsheet is a PHP library for reading and writing spreadsheet files. Versions prior to 3.7.0, 2.3.5, 2.1.6, and 1.29.7 are vulnerable to bypass of the cross-site scripting sanitizer using the javascript protocol and special characters. An	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attacker can use special characters, so that the library processes the javascript protocol with special characters and generates an HTML link. Versions 3.7.0, 2.3.5, 2.1.6, and 1.29.7 contain a patch for the issue.		
CVE-2025-0175	code-projects Online Shop view.php cross site scripting	A vulnerability was found in code-projects Online Shop 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /view.php. The manipulation of the argument name/details 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-2025-21610	Trix allows Cross-site Scripting via `javascript:` url in a link	Trix is a what-you-see-is-what-you-get rich text editor for everyday writing. Versions prior to 2.1.12 are vulnerable to cross-site scripting when pasting malicious code in the link field. An attacker could trick the user to copy&paste a malicious `javascript:` URL as a link 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 2.1.12 or later to receive a patch. In addition to upgrading, affected	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		users can disallow browsers that don't support a Content Security Policy (CSP) as a workaround for this and other cross-site scripting vulnerabilities. Set CSP policies such as script-src 'self' to ensure that only scripts hosted on the same origin are executed, and explicitly prohibit inline scripts using script-src-elem.		
CVE-2024-13132	Emlog Pro Subpage article.php cross site scripting	A vulnerability classified as problematic was found in Emlog Pro up to 2.4.3. This vulnerability affects unknown code of the file /admin/article.php of the component Subpage Handler. 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-2024-13135	Emlog Pro Subpage twitter.php cross site scripting	A vulnerability has been found in Emlog Pro 2.4.3 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/twitter.php of the component Subpage Handler. The manipulation 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-2024-13137	wangl1989 mysiteforme SiteController RestResponse cross site scripting	A vulnerability was found in wangl1989 mysiteforme 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
		affects the function RestResponse of the file src/main/java/com/mysiteforme/admin/controller/system/SiteController. 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-2024-13140	Emlog Pro Cover Upload article.php cross site scripting	A vulnerability classified as problematic has been found in Emlog Pro up to 2.4.3. Affected is an unknown function of the file /admin/article.php?action=upload_cover of the component Cover Upload Handler. The manipulation of the argument image 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-2024-13141	osuuu LightPicture SVG File Upload upload cross site scripting	A vulnerability classified as problematic was found in osuuu LightPicture up to 1.2.2. This vulnerability affects unknown code of the file /api/upload of the component SVG File Upload Handler. The manipulation of the argument file 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-2024-13142	ZeroWdd studentmanager RoleController. java submitAddRole	A vulnerability was found in ZeroWdd studentmanager 1.0. It has been declared as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	cross site scripting	problematic. This vulnerability affects the function submitAddRole of the file src/main/java/com/zero/system/controller/RoleController. java. The manipulation of the argument name leads to cross site scripting. The attack can be initiated remotely.		
CVE-2024-13143	ZeroWdd studentmanager PermissionController. java submitAddPermission cross site scripting	A vulnerability was found in ZeroWdd studentmanager 1.0. It has been rated as problematic. This issue affects the function submitAddPermission of the file src/main/java/com/zero/system/controller/PermissionController. java. The manipulation of the argument url 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-2025-0220	Trimble SPS851 Ethernet Configuration Menu cross site scripting	A vulnerability, which was classified as problematic, was found in Trimble SPS851 488.01. This affects an unknown part of the component Ethernet Configuration Menu. The manipulation of the argument Hostname 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 respond in any way.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-21612	Cross-site Scripting in TabberTransclude in Extension:TabberNeue	TabberNeue is a MediaWiki extension that allows the wiki to create tabs. Prior to 2.7.2, TabberTransclude.php doesn't escape the user-supplied page name when outputting, so an XSS payload as the page name can be used here. This vulnerability is fixed in 2.7.2.	Patched by core rule	Y
CVE-2025-21616	Plane has a Cross-site scripting (XSS) via SVG image upload	Plane is an open-source project management tool. A cross-site scripting (XSS) vulnerability has been identified in Plane versions prior to 0.23. The vulnerability allows authenticated users to upload SVG files containing malicious JavaScript code as profile images, which gets executed in victims' browsers when viewing the profile image.	Patched by core rule	Y
CVE-2025-0295	code-projects Online Book Shop booklist.php cross site scripting	A vulnerability was found in code-projects Online Book Shop 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /booklist.php?subcatid=1. The manipulation of the argument subcatnm 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-2025-0301	code-projects Online Book Shop subcat.php cross site scripting	A vulnerability, which was classified as problematic, has been found in code-projects Online Book Shop 1.0. Affected by this issue is some unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		functionality of the file /subcat.php. The manipulation of the argument catnm leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-22132	WeGIA has a Cross-Site Scripting (XSS) in File Upload Field	WeGIA is a web manager for charitable institutions. A Cross-Site Scripting (XSS) vulnerability was identified in the file upload functionality of the WeGIA/html/socio/sistema/controller/controla_xlsx.php endpoint. By uploading a file containing malicious JavaScript code, an attacker can execute arbitrary scripts in the context of a victim's browser. This can lead to information theft, session hijacking, and other forms of client-side exploitation. This vulnerability is fixed in 3.2.7.	Patched by core rule	Y
CVE-2024-13192	ZeroWdd myblog BlogController.java update cross site scripting	A vulnerability, which was classified as problematic, was found in ZeroWdd myblog 1.0. Affected is the function update of the file src/main/java/com/wdd/myblog/controller/admin/BlogController.java. 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.	Patched by core rule	Y
CVE-2025-22139	WeGIA Cross-Site Scripting (XSS) Reflected endpoint `configuracao_geral	WeGIA is a web manager for charitable institutions. A Reflected Cross-Site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	.php` parameter `msg`	Scripting (XSS) vulnerability was identified in the configuracao_geral.php endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the msg_c parameter. This vulnerability is fixed in 3.2.8.		
CVE-2025-22143	WeGIA Cross-Site Scripting (XSS) Reflected endpoint 'listar_permissoes.php' parameter 'msg_e'	WeGIA is a web manager for charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the listar_permissoes.php endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the msg_e parameter. This vulnerability is fixed in 3.2.8.	Patched by core rule	Y
CVE-2024-13196	donglight bookstore电商书城系统说明 BookInfoController.java BookSearchList cross site scripting	A vulnerability was found in donglight bookstore电商书城系统说明 1.0.0. It has been declared as problematic. This vulnerability affects the function BookSearchList of the file src/main/java/org/zdd/bookstore/web/controller/BookInfoController.java. The manipulation of the argument keywords 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-2024-13197	donglight bookstore电商书城	A vulnerability was found in donglight	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	系统说明 AdminUserControlle.java updateUser cross site scripting	bookstore电商书城系统说明 1.0.0. It has been rated as problematic. This issue affects the function updateUser of the file src/main/Java/org/zdd/bookstore/web/controller/admin/AdminUserControlle.java. 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.		
CVE-2024-13199	langhsu Mblog Blog System Search Bar search cross site scripting	A vulnerability classified as problematic was found in langhsu Mblog Blog System 3.5.0. Affected by this vulnerability is an unknown functionality of the file /search of the component Search Bar. The manipulation of the argument kw 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.	Patched by core rule	Y
CVE-2024-13202	wander-chu SpringBoot-Blog Blog Article PageController.java modifiyArticle cross site scripting	A vulnerability was found in wander-chu SpringBoot-Blog 1.0 and classified as problematic. This issue affects the function modifiyArticle of the file src/main/java/com/my/blog/website/controller/admin/PageController.java of the component Blog Article Handler. The manipulation of the argument content	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-13213	SingMR HouseRent toAdminUpdateHousePage cross site scripting	A vulnerability classified as problematic was found in SingMR HouseRent 1.0. This vulnerability affects unknown code of the file /toAdminUpdateHousePage?hID=30. 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-2024-56376	N/A	A stored cross-site scripting (XSS) vulnerability in the built-in messenger of REDCap 14.9.6 allows authenticated users to inject malicious scripts into the message field. When a user click on the received message, the crafted payload is executed, potentially enabling the execution of arbitrary web scripts.	Patched by core rule	Y
CVE-2024-56377	N/A	A stored cross-site scripting (XSS) vulnerability in survey titles of REDCap 14.9.6 allows authenticated users to inject malicious scripts into the Survey Title field or Survey Instructions. When a user receives a survey and clicks anywhere on the survey page to enter data, the crafted payload (which has been injected into all survey fields) is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		executed, potentially enabling the execution of arbitrary web scripts.		
CVE-2025-0342	CampCodes Computer Laboratory Management System edit cross site scripting	A vulnerability, which was classified as problematic, was found in CampCodes Computer Laboratory Management System 1.0. This affects an unknown part of the file /class/edit/edit. The manipulation of the argument s_lname 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. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-0348	CampCodes DepEd Equipment Inventory System add_employee.php cross site scripting	A vulnerability was found in CampCodes DepEd Equipment Inventory System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /data/add_employee.php. The manipulation of the argument data 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-2024-13183	Orbit Fox by ThemeIsle <= 2.10.43 - Authenticated (Contributor+) Stored Cross-Site Scripting via title_tag Parameter	The Orbit Fox by ThemeIsle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title_tag' parameter in all versions up to, and including, 2.10.43 due to insufficient input sanitization and output escaping. This makes it possible for authenticated	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-0311	Orbit Fox by ThemeIsle <= 2.10.43 - Authenticated (Contributor+) Stored Cross-Site Scripting via Pricing Table Widget	The Orbit Fox by ThemeIsle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Pricing Table widget in all versions up to, and including, 2.10.43 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-22596	WeGIA has a Cross-Site Scripting (XSS) Reflected endpoint 'modulos_visiveis.php' parameter'msg_c'	WeGIA is a web manager for charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the modulos_visiveis.php endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the msg_c parameter. This vulnerability is fixed in 3.2.8.	Patched by core rule	Y
CVE-2025-22597	WeGIA has a Cross-Site Scripting (XSS) Stored endpoint 'CobrancaController.php' parameter 'local_recepcao'	WeGIA is a web manager for charitable institutions. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the CobrancaController.ph	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		p endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts into the local_recepcao parameter. The injected scripts are stored on the server and executed automatically whenever the affected page is accessed by users, posing a significant security risk. This vulnerability is fixed in 3.2.8.		
CVE-2025-22598	WeGIA has a Cross-Site Scripting (XSS) Stored endpoint 'cadastrarSocio.php' parameter 'nome'	WeGIA is a web manager for charitable institutions. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the cadastrarSocio.php endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts into the local_recepcao parameter. The injected scripts are stored on the server and executed automatically whenever the affected page is accessed by users, posing a significant security risk. This vulnerability is fixed in 3.2.8.	Patched by core rule	Y
CVE-2025-22599	WeGIA has a Cross-Site Scripting (XSS) Reflected endpoint `home.php` parameter `msg_c`	WeGIA is a web manager for charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the home.php endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the msg_c parameter. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability is fixed in 3.2.8.		
CVE-2025-22600	WeGIA has a Cross-Site Scripting (XSS) Reflected endpoint `configuracao_doacao.php` parameter `avulso`	WeGIA is a web manager for charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the configuracao_doacao.php endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the avulso parameter. This vulnerability is fixed in 3.2.8.	Patched by core rule	Y
CVE-2025-23110	N/A	An issue was discovered in REDCap 14.9.6. A Reflected cross-site scripting (XSS) vulnerability in the email-subject field exists while performing an upload of a CSV file containing a list of alert configurations. An attacker can send the victim a CSV file containing the XSS payload in the email-subject. Once the victim uploads the file, he automatically lands on a page to view the uploaded data. If the victim clicks on the email-subject value, it triggers the XSS payload.	Patched by core rule	Y
CVE-2025-23112	N/A	An issue was discovered in REDCap 14.9.6. A stored cross-site scripting (XSS) vulnerability allows authenticated users to inject malicious scripts into the Survey field name of Survey. When a user receive the survey, if he clicks on the field name, it triggers the XSS	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		payload.		
CVE-2025-0397	reckcn SPPanAdmin edit cross site scripting	A vulnerability, which was classified as problematic, was found in reckcn SPPanAdmin 1.0. Affected is an unknown function of the file /;/admin/role/edit. The manipulation of the argument name 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. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-0398	longpi1 warehouse Backend updateInport cross site scripting	A vulnerability has been found in longpi1 warehouse 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /resources/..;/inport/updateInport of the component Backend. The manipulation of the argument remark 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-2025-0400	StarSea99 starsea-mall update cross site scripting	A vulnerability was found in StarSea99 starsea-mall 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/categories/update. The manipulation of the argument categoryName leads	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-22613	WeGIA Cross-Site Scripting (XSS) Stored endpoint 'informacao_adicional.php' parameter 'descricao'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the `informacao_adicional.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts into the `descricao` parameter. The injected scripts are stored on the server and executed automatically whenever the affected page is accessed by users, posing a significant security risk. The application fails to properly validate and sanitize user inputs in the `informacao_adicional.php` parameter. This lack of validation allows attackers to inject malicious scripts, which are then stored on the server. Whenever the affected page is accessed, the malicious payload is executed in the victim's browser, potentially compromising the user's data and system. This issue has been addressed in version 3.2.6 and all users are advised to upgrade. There are no known workarounds	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		for this vulnerability.		
CVE-2025-22614	WeGIA Cross-Site Scripting (XSS) Stored endpoint 'dependente_editarInfoPessoal.php ' parameters 'nome' 'SobrenomeForm'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the `dependente_editarInfoPessoal.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts into the `nome` and `SobrenomeForm`parameters. The injected scripts are stored on the server and executed automatically whenever the affected page is accessed by users, posing a significant security risk. The application fails to properly validate and sanitize user inputs in the `dependente_editarInfoPessoal.php` parameters. This lack of validation allows attackers to inject malicious scripts, which are then stored on the server. Whenever the affected page is accessed, the malicious payload is executed in the victim's browser, potentially compromising the user's data and system. This issue has been addressed in version 3.2.6 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-22615	WeGIA Cross-Site Scripting (XSS) Reflected endpoint 'Cadastro_Atendido.php' parameter 'cpf'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the `Cadastro_Atendido.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the `cpf` parameter. The application fails to validate and sanitize user inputs in the `cpf` parameter. This lack of validation permits the injection of malicious payloads, which are reflected back to the user's browser in the server's response and executed within the context of the victim's browser. This issue has been addressed in version 3.2.6 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-22616	WeGIA Cross-Site Scripting (XSS) Stored endpoint 'dependente_parentesco_adicionar.php' parameter 'descricao'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the `dependente_parentesco_adicionar.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts into the `descricao` parameter. The injected scripts are stored on the server and executed	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		automatically whenever the affected page is accessed by users, posing a significant security risk. The application fails to properly validate and sanitize user inputs in the `dependente_parentesco_adicionar.php` parameter. This lack of validation allows attackers to inject malicious scripts, which are then stored on the server. Whenever the affected page is accessed, the malicious payload is executed in the victim's browser, potentially compromising the user's data and system. This issue has been addressed in version 3.2.6 and all users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-22617	WeGIA Cross-Site Scripting (XSS) Reflected endpoint 'editar_socio.php' parameter 'socio'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the `editar_socio.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the `socio` parameter. The application fails to validate and sanitize user inputs in the `socio` parameter. This lack of validation permits the injection	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of malicious payloads, which are reflected back to the user's browser in the server's response and executed within the context of the victim's browser. This issue has been addressed in version 3.2.7 and all users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-22618	WeGIA Cross-Site Scripting (XSS) Stored endpoint 'adicionar_cargo.php' parameter 'cargo'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the `adicionar_cargo.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts into the `cargo` parameter. The injected scripts are stored on the server and executed automatically whenever the affected page is accessed by users, posing a significant security risk. The application fails to properly validate and sanitize user inputs in the `adicionar_cargo.php` parameter. This lack of validation allows attackers to inject malicious scripts, which are then stored on the server. Whenever the affected page is accessed, the malicious payload is executed in the victim's browser, potentially	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		compromising the user's data and system. This issue has been addressed in release version 3.2.6 and all users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-22619	WeGIA Cross-Site Scripting (XSS) Reflected endpoint 'editar_permissoes.php' parameter 'msg_c'	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the `editar_permissoes.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the `msg_c` parameter. The application fails to validate and sanitize user inputs in the `msg_c` parameter. This lack of validation permits the injection of malicious payloads, which are reflected back to the user's browser in the server's response and executed within the context of the victim's browser. This issue has been addressed in release version 3.2.6. All users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-23026	HTML templates containing Javascript template strings are subject to XSS in jte	jte (Java Template Engine) is a secure and lightweight template engine for Java and Kotlin. In affected versions Jte HTML templates with `script` tags or script	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attributes that include a Javascript template string (backticks) are subject to XSS. The `javaScriptBlock` and `javaScriptAttribute` methods in the `Escape` class do not escape backticks, which are used for Javascript template strings. Dollar signs in template strings should also be escaped as well to prevent undesired interpolation. HTML templates rendered by Jte's `OwaspHtmlTemplate Output` in versions less than or equal to `3.1.15` with `script` tags or script attributes that contain Javascript template strings (backticks) are vulnerable. Users are advised to upgrade to version 3.1.16 or later to resolve this issue. There are no known workarounds for this vulnerability.		
CVE-2025-23030	Cross-Site Scripting (XSS) Reflected endpoint 'cadastro_funcionario.php' parameter 'cpf' in WeGIA	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the `cadastro_funcionario.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the `cpf` parameter. The application fails to validate and sanitize user inputs in the `cpf` parameter. This lack of validation permits the injection of malicious	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		payloads, which are reflected back to the user's browser in the server's response and executed within the context of the victim's browser. This issue has been addressed in version 3.2.6. All users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-23031	Cross-Site Scripting (XSS) Stored endpoint 'adicionar_alergia.php' parameter 'nome' in WeGIA	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the `adicionar_alergia.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts into the `nome` parameter. The injected scripts are stored on the server and executed automatically whenever the affected page is accessed by users, posing a significant security risk. The application fails to properly validate and sanitize user inputs in the `adicionar_alergia.php` parameter. This lack of validation allows attackers to inject malicious scripts, which are then stored on the server. Whenever the affected page is accessed, the malicious payload is executed in the victim's browser, potentially compromising the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		user's data and system. This issue has been addressed in version 3.2.6. All users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-23032	Cross-Site Scripting (XSS) Stored endpoint 'adicionar_escala.php' parameter 'escala' in WeGIA	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the `adicionar_escala.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts into the `escala` parameter. The injected scripts are stored on the server and executed automatically whenever the affected page is accessed by users, posing a significant security risk. The application fails to properly validate and sanitize user inputs in the `adicionar_escala.php` parameter. This lack of validation allows attackers to inject malicious scripts, which are then stored on the server. Whenever the affected page is accessed, the malicious payload is executed in the victim's browser, potentially compromising the user's data and system. This issue has been addressed in version 3.2.6. All users are advised to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-23033	Cross-Site Scripting (XSS) Stored endpoint 'adicionar_situacao.php' parameter 'situacao' in WeGIA	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the `adicionar_situacao.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts into the `situacao` parameter. The injected scripts are stored on the server and executed automatically whenever the affected page is accessed by users, posing a significant security risk. The application fails to properly validate and sanitize user inputs in the `adicionar_situacao.php` parameter. This lack of validation allows attackers to inject malicious scripts, which are then stored on the server. Whenever the affected page is accessed, the malicious payload is executed in the victim's browser, potentially compromising the user's data and system. This issue has been addressed in version 3.2.6. All users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-23034	Cross-Site Scripting (XSS) Reflected	WeGIA is an open source web manager	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	endpoint 'tags.php' parameter 'msg_e' in WeGIA	with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the `tags.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the `msg_e` parameter. The application fails to validate and sanitize user inputs in the `msg_e` parameter. This lack of validation permits the injection of malicious payloads, which are reflected back to the user's browser in the server's response and executed within the context of the victim's browser. This issue has been addressed in version 3.2.6. All users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-23035	Cross-Site Scripting (XSS) Stored endpoint 'adicionar_tipo_quadro_horario.php' parameter 'tipo' in WeGIA	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the `adicionar_tipo_quadro_horario.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts into the `tipo` parameter. The injected scripts are stored on the server and executed automatically	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		whenever the affected page is accessed by users, posing a significant security risk. The application fails to properly validate and sanitize user inputs in the `adicionar_tipo_quadro_horario.php` parameter. This lack of validation allows attackers to inject malicious scripts, which are then stored on the server. Whenever the affected page is accessed, the malicious payload is executed in the victim's browser, potentially compromising the user's data and system. This issue has been addressed in version 3.2.6. All users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-23036	Cross-Site Scripting (XSS) Reflected endpoint 'pre_cadastro_funcionario.php' parameter 'msg_e' in WeGIA	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in the `pre_cadastro_funcionario.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the `msg_e` parameter. The application fails to validate and sanitize user inputs in the `msg_e` parameter. This lack of validation permits the injection of malicious payloads,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		which are reflected back to the user's browser in the server's response and executed within the context of the victim's browser. This issue has been addressed in version 3.2.7. All users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-23037	Cross-Site Scripting (XSS) Stored endpoint 'control.php' parameter 'cargo' in WeGIA	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the `control.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts into the `cargo` parameter. The injected scripts are stored on the server and executed automatically whenever the affected page is accessed by users, posing a significant security risk. The application fails to properly validate and sanitize user inputs in the `control.php` parameter. This lack of validation allows attackers to inject malicious scripts, which are then stored on the server. Whenever the affected page is accessed, the malicious payload is executed in the victim's browser, potentially compromising the user's data and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		system. This issue has been addressed in version 3.2.6. All users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-23038	Cross-Site Scripting (XSS) Stored endpoint 'remuneracao.php ' parameter 'descricao' in WeGIA	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the `remuneracao.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts into the `descricao` parameter. The injected scripts are stored on the server and executed automatically whenever the affected page is accessed by users, posing a significant security risk. The application fails to properly validate and sanitize user inputs in the `remuneracao.php` parameter. This lack of validation allows attackers to inject malicious scripts, which are then stored on the server. Whenever the affected page is accessed, the malicious payload is executed in the victim's browser, potentially compromising the user's data and system. This issue has been addressed in version 3.2.6. All users are advised to upgrade. There are no	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		known workarounds for this vulnerability.		
CVE-2024-53277	Cross-site Scripting in form messages in silverstripe framework	Silverstripe Framework is a PHP framework which powers the Silverstripe CMS. In some cases, form messages can contain HTML markup. This is an intentional feature, allowing links and other relevant HTML markup for the given message. Some form messages include content that the user can provide. There are scenarios in the CMS where that content doesn't get correctly sanitised prior to being included in the form message, resulting in an XSS vulnerability. This issue has been addressed in silverstripe/framework version 5.3.8 and users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-0483	Fanli2012 native-php-cms jump.php cross site scripting	A vulnerability has been found in Fanli2012 native-php-cms 1.0 and classified as problematic. This vulnerability affects unknown code of the file /fladmin/jump.php. The manipulation of the argument message/error 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-2025-0485	Fanli2012 native-php-cms sysconfig_doedit.php cross site scripting	A vulnerability was found in Fanli2012 native-php-cms 1.0. It has been classified as problematic. Affected is an unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		function of the file /fladmin/sysconfig_doedit.php. The manipulation of the argument info 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-2024-56144	Stored XSS-LibreNMS-Display Name 2 in librenms	librenms is a community-based GPL-licensed network monitoring system. Affected versions are subject to a stored XSS on the parameters (Replace $DEVICE_ID with your specific $DEVICE_ID value):`/device/$DEVICE_ID/edit` -> param: display. Librenms versions up to 24.11.0 allow remote attackers to inject malicious scripts. When a user views or interacts with the page displaying the data, the malicious script executes immediately, leading to potential unauthorized actions or data exposure. This issue has been addressed in release version 24.12.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-23198	Stored-XSS-LibreNMS-Display-Name in librenms	librenms is a community-based GPL-licensed network monitoring system. Affected versions are subject to a stored XSS on the parameters (Replace $DEVICE_ID with your specific $DEVICE_ID value):`/device/$DEVICE_ID/edit` -> param: display. Librenms	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		versions up to 24.10.1 allow remote attackers to inject malicious scripts. When a user views or interacts with the page displaying the data, the malicious script executes immediately, leading to potential unauthorized actions or data exposure. This issue has been addressed in release version 24.11.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-23199	Stored XSS-LibreNMS-Ports in librenms	librenms is a community-based GPL-licensed network monitoring system. Affected versions are subject to a stored XSS on the parameter: `/ajax_form.php` -> param: descr. Librenms version up to 24.10.1 allow remote attackers to inject malicious scripts. When a user views or interacts with the page displaying the data, the malicious script executes immediately, leading to potential unauthorized actions or data exposure. This issue has been addressed in release version 24.11.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-23200	Stored XSS-LibreNMS-Misc Section in librenms	librenms is a community-based GPL-licensed network monitoring system. Affected versions are subject to a stored XSS on the parameter: `ajax_form.php` ->	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		param: state. Librenms versions up to 24.10.1 allow remote attackers to inject malicious scripts. When a user views or interacts with the page displaying the data, the malicious script executes immediately, leading to potential unauthorized actions or data exposure. This issue has been addressed in release version 24.11.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-23201	Reflected Cross-site Scripting on error alert in librenms	librenms is a community-based GPL-licensed network monitoring system. Affected versions are subject to Cross-site Scripting (XSS) on the parameters:`/addhost` -> param: community. Librenms versions up to 24.10.1 allow remote attackers to inject malicious scripts. When a user views or interacts with the page displaying the data, the malicious script executes immediately, leading to potential unauthorized actions or data exposure. This issue has been addressed in release version 24.11.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-0530	code-projects Job Recruitment _feedback_system.php cross site scripting	A vulnerability has been found in code-projects Job Recruitment 1.0 and classified as problematic. This vulnerability affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown code of the file /_parse/_feedback_system.php. The manipulation of the argument type leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-0537	code-projects Car Rental Management System manage-pages.php cross site scripting	A vulnerability, which was classified as problematic, has been found in code-projects Car Rental Management System 1.0. This issue affects some unknown processing of the file /admin/manage-pages.php. The manipulation of the argument pgdetails 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-2025-0538	code-projects Tourism Management System manage-pages.php cross site scripting	A vulnerability, which was classified as problematic, was found in code-projects Tourism Management System 1.0. Affected is an unknown function of the file /admin/manage-pages.php. The manipulation of the argument pgedetails 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-2025-23039	Cross Site Scripting on URL decode Tooltip in Caido	Caido is a web security auditing toolkit. A Cross-Site Scripting (XSS) vulnerability was identified in Caido	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		v0.45.0 due to improper sanitization in the URL decoding tooltip of HTTP request and response editors. This issue could allow an attacker to execute arbitrary scripts, potentially leading to the theft of sensitive information. This issue has been addressed in version 0.45.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2024-13385	JSM Screenshot Machine Shortcode <= 2.3.0 - Authenticated (Contributor+) Stored Cross-Site Scripting	The JSM Screenshot Machine Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ssm' shortcode in all versions up to, and including, 2.3.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2024-13515	Image Source Control Lite – Show Image Credits and Captions <= 2.28.0 - Reflected Cross-Site Scripting	The Image Source Control Lite – Show Image Credits and Captions plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'path' parameter in all versions up to, and including, 2.28.0 due to insufficient input sanitization and output escaping. This makes it possible for	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.		
CVE-2025-0559	Campcodes School Management Software Create Id Card Page create-id-card cross site scripting	A vulnerability, which was classified as problematic, has been found in Campcodes School Management Software 1.0. This issue affects some unknown processing of the file /create-id-card of the component Create Id Card Page. The manipulation of the argument ID Card Title 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-2025-0560	CampCodes School Management Software Photo Gallery Page photo-gallery cross site scripting	A vulnerability, which was classified as problematic, was found in CampCodes School Management Software 1.0. Affected is an unknown function of the file /photo-gallery of the component Photo Gallery Page. The manipulation of the argument Description 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-2025-0581	CampCodes School Management Software Chat History send cross site scripting	A vulnerability classified as problematic has been found in CampCodes School Management Software 1.0. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects an unknown part of the file /chat/group/send of the component Chat History. The manipulation of the argument message 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-2025-22131	Cross-Site Scripting (XSS) vulnerability in generateNavigation () function	PhpSpreadsheet is a PHP library for reading and writing spreadsheet files. Cross-Site Scripting (XSS) vulnerability in the code which translates the XLSX file into a HTML representation and displays it in the response.	Patched by core rule	Y
CVE-2025-24012	Umbraco Backoffice Components Have XSS/HTML Injection Vulnerability	Umbraco is a free and open source .NET content management system. Starting in version 14.0.0 and prior to versions 14.3.2 and 15.1.2, authenticated users are able to exploit a cross-site scripting vulnerability when viewing certain localized backoffice components. Versions 14.3.2 and 15.1.2 contain a patch.	Patched by core rule	Y
CVE-2025-24017	YesWiki Vulnerable to Unauthenticated DOM Based XSS	YesWiki is a wiki system written in PHP. Versions up to and including 4.4.5 are vulnerable to any end-user crafting a DOM based XSS on all of YesWiki's pages which is triggered when a user clicks on a malicious link. The vulnerability makes use of the search by tag feature. When a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		tag doesn't exist, the tag is reflected on the page and isn't properly sanitized on the server side which allows a malicious user to generate a link that will trigger an XSS on the client's side when clicked. This vulnerability allows any user to generate a malicious link that will trigger an account takeover when clicked, therefore allowing a user to steal other accounts, modify pages, comments, permissions, extract user data (emails), thus impacting the integrity, availability and confidentiality of a YesWiki instance. Version 4.5.0 contains a patch for the issue.		
CVE-2025-24018	YesWiki Vulnerable to Authenticated Stored XSS	YesWiki is a wiki system written in PHP. In versions up to and including 4.4.5, it is possible for an authenticated user with rights to edit/create a page or comment to trigger a stored XSS which will be reflected on any page where the resource is loaded. The vulnerability makes use of the content edition feature and more specifically of the `{{attach}}` component allowing users to attach files/medias to a page. When a file is attached using the `{{attach}}` component, if the resource contained in the `file` attribute doesn't exist, then the server will generate a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file upload button containing the filename. This vulnerability allows any malicious authenticated user that has the right to create a comment or edit a page to be able to steal accounts and therefore modify pages, comments, permissions, extract user data (emails), thus impacting the integrity, availability and confidentiality of a YesWiki instance. Version 4.5.0 contains a patch for the issue.		
CVE-2025-24027	ps_contactinfo has potential XSS due to usage of the nofilter tag in template	ps_contactinfo, a PrestaShop module for displaying store contact information, has a cross-site scripting (XSS) vulnerability in versions up to and including 3.3.2. This can not be exploited in a fresh install of PrestaShop, only shops made vulnerable by third party modules are concerned. For example, if the shop has a third party module vulnerable to SQL injections, then ps_contactinfo might execute a stored cross-site scripting in formatting objects. Commit d60f9a5634b4fc2d3a8831fb08fe2e1f23cbfa39 keeps formatted addresses from displaying a XSS stored in the database, and the fix is expected to be available in version 3.3.3. No workarounds are available aside from applying the fix	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and keeping all modules maintained and update.		
CVE-2025-0314	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 17.2 before 17.6.4, 17.7 before 17.7.3, and 17.8 before 17.8.1. Improper rendering of certain file types lead to cross-site scripting.	Patched by core rule	Y
CVE-2025-0706	JoeyBling bootplus admin.html cross site scripting	A vulnerability was found in JoeyBling bootplus up to 247d5f6c209be1a5cf10cd0fa18e1d8cc63cf55d and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/sys/admin.html. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available.	Patched by core rule	Y
CVE-2025-0708	fumiao opencms Add Model Management Page addOrUpdate cross site scripting	A vulnerability was found in fumiao opencms 2.2. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/model/addOrUpdate of the component Add Model Management Page. The manipulation of the argument 模板前缀 leads to cross site scripting. The attack can be initiated	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-0709	Dcat-Admin Roles Page roles cross site scripting	A vulnerability was found in Dcat-Admin 2.2.1-beta. It has been rated as problematic. This issue affects some unknown processing of the file /admin/auth/roles of the component Roles Page. 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-2025-0710	CampCodes School Management Software Notice Board Page notice-list cross site scripting	A vulnerability classified as problematic has been found in CampCodes School Management Software 1.0. Affected is an unknown function of the file /notice-list of the component Notice Board Page. The manipulation of the argument Notice 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

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™