INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

March 2025

The total zero-day vulnerabilities count for March month: 667

Command Injection	SQL Injection	SSRF	Path Traversal	Cross-Site Scripting	Malicious File Upload	XXE
87	178	15	61	324	1	1

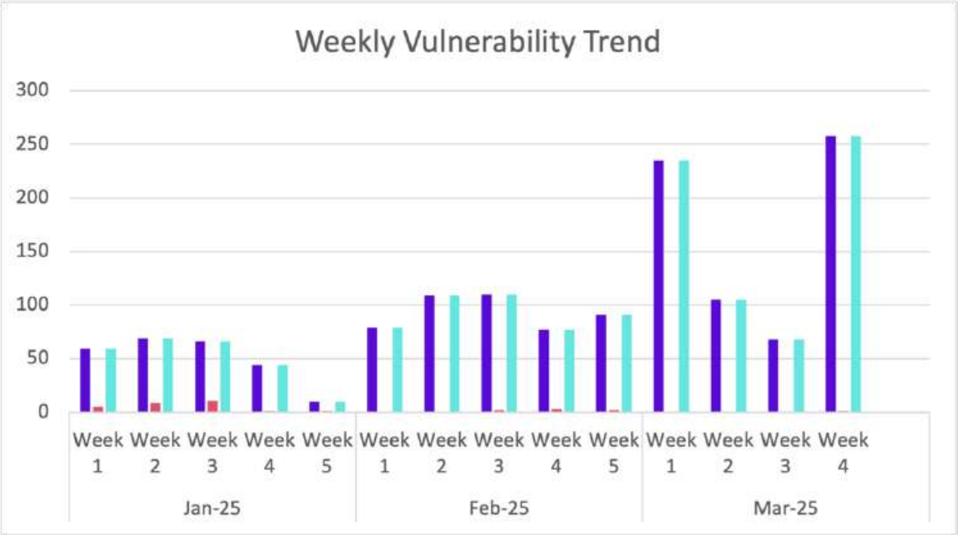
Zero-day vulnerabilities protected through core rules	666
Zero-day vulnerabilities protected through custom rules	1
Zero-day vulnerabilities found by Indusface WAS	666

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

Vulnerability Trend:

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

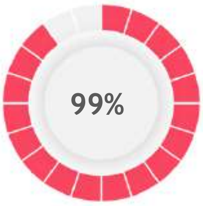
Weekly Vulnerability Trend



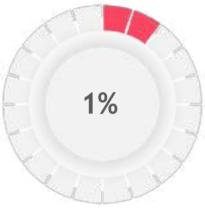
🟪 Total Blocked/Logged Web AppSec Zero-Day Vulnerabilities by Core Rules

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

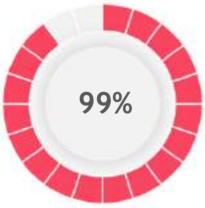
🟦 Total Zero-Day Vulnerabilities found by Indusface Scanner



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

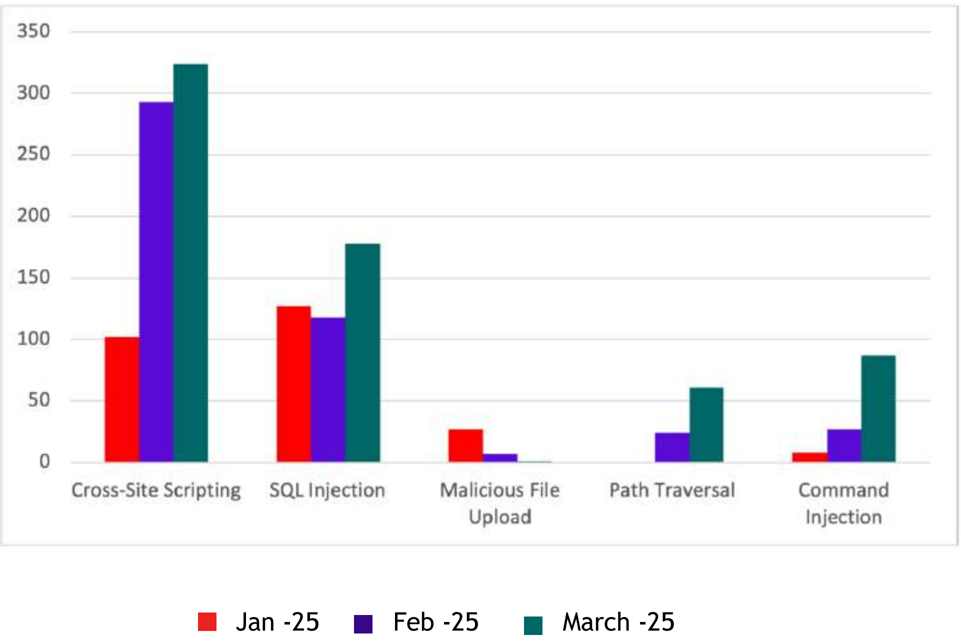


of the zero-day vulnerabilities were protected by the custom rules in the last month



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

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-38693	RCE in Lucee REST endpoint	Lucee Server (or simply Lucee) is a dynamic, Java based, tag and scripting language used for rapid web application development. The Lucee REST endpoint is vulnerable to RCE via an XML XXE attack. This vulnerability is fixed in Lucee 5.4.3.2, 5.3.12.1, 5.3.7.59, 5.3.8.236, and 5.3.9.173.	Patched by core rule	Y
CVE-2024-10019	Path Traversal and OS Command Injection in parisneo/lollms-webui	A vulnerability in the `start_app_server` function of parisneo/lollms-webui V12 (Strawberry) allows for path traversal and OS command injection. The function does not properly sanitize the `app_name` parameter, enabling an attacker to upload a malicious `server.py` file and execute arbitrary code by exploiting the path traversal vulnerability.	Patched by core rule	Y
CVE-2024-10096	Remote Unauthorized Pickle Deserialization Command Execution in dask/dask	Dask versions <=2024.8.2 contain a vulnerability in the Dask Distributed Server where the use of pickle serialization allows attackers to craft malicious objects. These objects can be serialized on the client side and sent to the server for deserialization, leading to remote command execution and potentially granting full control over the Dask server.	Patched by core rule	Y
CVE-2024-10190	Unauthenticated Remote Code Execution in ElasticRendezvousHandler in horovod/horovod	Horovod versions up to and including v0.28.1 are vulnerable to unauthenticated remote code execution. The vulnerability is due to improper handling of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		base64-encoded data in the `ElasticRendezvousHandler`, a subclass of `KVStoreHandler`. Specifically, the `_put_value` method in `ElasticRendezvousHandler` calls `codec.loads_base64(value)`, which eventually invokes `cloudpickle.loads(decoded)`. This allows an attacker to send a malicious pickle object via a PUT request, leading to arbitrary code execution on the server.		
CVE-2024-10252	Code Injection in langgenius/dify	A vulnerability in langgenius/dify versions <=v0.9.1 allows for code injection via internal SSRF requests in the Dify sandbox service. This vulnerability enables an attacker to execute arbitrary Python code with root privileges within the sandbox environment, potentially leading to the deletion of the entire sandbox service and causing irreversible damage.	Patched by core rule	Y
CVE-2024-10835	Arbitrary File Write via SQL Injection in eosphoros-ai/db-gpt	In eosphoros-ai/db-gpt version v0.6.0, the web API `POST /api/v1/editor/sql/run` allows execution of arbitrary SQL queries without any access control. This vulnerability can be exploited by attackers to perform Arbitrary File Write using DuckDB SQL, enabling them to write arbitrary files to the victim's file system. This can potentially lead to Remote Code Execution (RCE).	Patched by core rule	Y
CVE-2024-10901	Arbitrary File Write via DuckDB SQL Injection in eosphoros-ai/db-gpt	In eosphoros-ai/db-gpt version v0.6.0, the web API `POST /api/v1/editor/chart/run` allows execution of arbitrary SQL queries without any access control. This vulnerability can be exploited by attackers to perform Arbitrary File Write, enabling them to write arbitrary files to the victim's file system. This can potentially lead to Remote Code Execution (RCE) by writing malicious files such as `__init__.py` in the Python's `/site-packages/` directory.	Patched by core rule	Y
CVE-2024-10902	Arbitrary File Upload with Path Traversal in eosphoros-ai/db-gpt	In eosphoros-ai/db-gpt version v0.6.0, the web API `POST /v1/personal/agent/upload` is vulnerable to Arbitrary File Upload with Path Traversal. This vulnerability allows unauthorized attackers to upload arbitrary files to the victim's file system at any location. The impact of this vulnerability includes the potential for remote code execution (RCE) by writing malicious files, such as a malicious `__init__.py` in the Python's `/site-packages/`	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		directory.		
CVE-2024-10950	Code Injection in binary-husky/gpt_academic	In binary-husky/gpt_academic version <= 3.83, the plugin `CodeInterpreter` is vulnerable to code injection caused by prompt injection. The root cause is the execution of user-provided prompts that generate untrusted code without a sandbox, allowing the execution of parts of the LLM-generated code. This vulnerability can be exploited by an attacker to achieve remote code execution (RCE) on the application backend server, potentially gaining full control of the server.	Patched by core rule	Y
CVE-2024-10954	Prompt Injection Leading to RCE in binary-husky/gpt_academic Plugin `manim`	In the `manim` plugin of binary-husky/gpt_academic, versions prior to the fix, a vulnerability exists due to improper handling of user-provided prompts. The root cause is the execution of untrusted code generated by the LLM without a proper sandbox. This allows an attacker to perform remote code execution (RCE) on the app backend server by injecting malicious code through the prompt.	Patched by core rule	Y
CVE-2024-11039	Deserialization of Untrusted Data in binary-husky/gpt_academic	A pickle deserialization vulnerability exists in the Latex English error correction plug-in function of binary-husky/gpt_academic versions up to and including 3.83. This vulnerability allows attackers to achieve remote command execution by deserializing untrusted data. The issue arises from the inclusion of numpy in the deserialization whitelist, which can be exploited by constructing a malicious compressed package containing a merge_result.pkl file and a merge_proofread_en.tex file. The vulnerability is fixed in commit 91f5e6b.	Patched by core rule	Y
CVE-2024-11041	Remote Code Execution in vllm-project/vllm	vllm-project vllm version v0.6.2 contains a vulnerability in the MessageQueue.dequeue() API function. The function uses pickle.loads to parse received sockets directly, leading to a remote code execution vulnerability. An attacker can exploit this by sending a malicious payload to the MessageQueue, causing the victim's machine to execute arbitrary code.	Patched by core rule	Y
CVE-2024-12029	Remote Code Execution via Model Deserialization in invoke-ai/invokeai	A remote code execution vulnerability exists in invoke-ai/invokeai versions 5.3.1 through 5.4.2 via the /api/v2/models/install API. The vulnerability arises from unsafe deserialization of model files using torch.load without proper validation. Attackers can exploit this by	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		embedding malicious code in model files, which is executed upon loading. This issue is fixed in version 5.4.3.		
CVE-2024-12044	Remote Code Execution by Pickle Deserialization in open-mmlab/mmdetection	A remote code execution vulnerability exists in open-mmlab/mmdetection version v3.3.0. The vulnerability is due to the use of the `pickle.loads()` function in the `all_reduce_dict()` distributed training API without proper sanitization. This allows an attacker to execute arbitrary code by broadcasting a malicious payload to the distributed training network.	Patched by core rule	Y
CVE-2024-12433	Remote Code Execution in infiniflow/ragflow	A vulnerability in infiniflow/ragflow versions v0.12.0 allows for remote code execution. The RPC server in RagFlow uses a hard-coded AuthKey 'authkey=b'infiniflow-token4kevinhu'' which can be easily fetched by attackers to join the group communication without restrictions. Additionally, the server processes incoming data using pickle deserialization via `pickle.loads()` on `connection.recv()`, making it vulnerable to remote code execution. This issue is fixed in version 0.14.0.	Patched by core rule	Y
CVE-2024-12450	RCE, Full Read SSRF, and Arbitrary File Read in infiniflow/ragflow	In infiniflow/ragflow versions 0.12.0, the `web_crawl` function in `document_app.py` contains multiple vulnerabilities. The function does not filter URL parameters, allowing attackers to exploit Full Read SSRF by accessing internal network addresses and viewing their content through the generated PDF files. Additionally, the lack of restrictions on the file protocol enables Arbitrary File Read, allowing attackers to read server files. Furthermore, the use of an outdated Chromium headless version with --no-sandbox mode enabled makes the application susceptible to Remote Code Execution (RCE) via known Chromium v8 vulnerabilities. These issues are resolved in version 0.14.0.	Patched by core rule	Y
CVE-2024-12866	Local File Inclusion in netease-youdao/qanything	A local file inclusion vulnerability exists in netease-youdao/qanything version v2.0.0. This vulnerability allows an attacker to read arbitrary files on the file system, which can lead to remote code execution by retrieving private SSH keys, reading private files, source code, and configuration files.	Patched by core rule	Y
CVE-2024-47051	Remote Code Execution & File Deletion in Asset Uploads	This advisory addresses two critical security vulnerabilities present in Mautic versions before	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		5.2.3. These vulnerabilities could be exploited by authenticated users. * Remote Code Execution (RCE) via Asset Upload: A Remote Code Execution vulnerability has been identified in the asset upload functionality. Insufficient enforcement of allowed file extensions allows an attacker to bypass restrictions and upload executable files, such as PHP scripts. * Path Traversal File Deletion: A Path Traversal vulnerability exists in the upload validation process. Due to improper handling of path components, an authenticated user can manipulate the file deletion process to delete arbitrary files on the host system.		
CVE-2024-55551	N/A	An issue was discovered in Exasol jdbc driver 24.2.0. Attackers can inject malicious parameters into the JDBC URL, triggering JNDI injection during the process when the JDBC Driver uses this URL to connect to the database. This can further lead to remote code execution vulnerability.	Patched by core rule	Y
CVE-2024-5752	Path Traversal in stitionai/devika	A path traversal vulnerability exists in stitionai/devika, specifically in the project creation functionality. In the affected version beacf6edaa205a5a5370525407a6db45137873b3, the project name is not validated, allowing an attacker to create a project with a crafted name that traverses directories. This can lead to arbitrary file overwrite when the application generates code and saves it to the specified project directory, potentially resulting in remote code execution.	Patched by core rule	Y
CVE-2024-6825	Remote Code Execution in BerriAI/litellm	BerriAI/litellm version 1.40.12 contains a vulnerability that allows remote code execution. The issue exists in the handling of the 'post_call_rules' configuration, where a callback function can be added. The provided value is split at the final '.' mark, with the last part considered the function name and the remaining part appended with the '.py' extension and imported. This allows an attacker to set a system method, such as 'os.system', as a callback, enabling the execution of arbitrary commands when a chat response is processed.	Patched by core rule	Y
CVE-2024-6982	Remote Code Execution in Calculate Function in parisneo/lollms	A remote code execution vulnerability exists in the Calculate function of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		parisneo/lollms version 9.8. The vulnerability arises from the use of Python's `eval()` function to evaluate mathematical expressions within a Python sandbox that disables `__builtins__` and only allows functions from the `math` module. This sandbox can be bypassed by loading the `os` module using the `_frozen_importlib.BuiltinImporter` class, allowing an attacker to execute arbitrary commands on the server. The issue is fixed in version 9.10.		
CVE-2024-7034	Remote Code Execution due to Arbitrary File Write in open-webui/open-webui	In open-webui version 0.3.8, the endpoint `/models/upload` is vulnerable to arbitrary file write due to improper handling of user-supplied filenames. The vulnerability arises from the usage of `file_path = f"{UPLOAD_DIR}/{file.filename}"` without proper input validation or sanitization. An attacker can exploit this by manipulating the `file.filename` parameter to include directory traversal sequences, causing the resulting `file_path` to escape the intended `UPLOAD_DIR` and potentially overwrite arbitrary files on the system. This can lead to unauthorized modifications of system binaries, configuration files, or sensitive data, potentially enabling remote command execution.	Patched by core rule	Y
CVE-2024-7053	Session Fixation in open-webui/open-webui	A vulnerability in open-webui/open-webui version 0.3.8 allows an attacker with a user-level account to perform a session fixation attack. The session cookie for all users is set with the default `SameSite=Lax` and does not have the `Secure` flag enabled, allowing the session cookie to be sent over HTTP to a cross-origin domain. An attacker can exploit this by embedding a malicious markdown image in a chat, which, when viewed by an administrator, sends the admin's session cookie to the attacker's server. This can lead to a stealthy administrator account takeover, potentially resulting in remote code execution (RCE) due to the elevated privileges of administrator accounts.	Patched by core rule	Y
CVE-2024-7776	Arbitrary File Overwrite in onnx/onnx	A vulnerability in the `download_model` function of the onnx/onnx framework, before and including version 1.16.1, allows for arbitrary file overwrite due to inadequate prevention of path traversal attacks in malicious tar files.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability can be exploited by an attacker to overwrite files in the user's directory, potentially leading to remote command execution.		
CVE-2024-7804	Deserialization of Untrusted Data in pytorch/pytorch	A deserialization vulnerability exists in the Pytorch RPC framework (torch.distributed.rpc) in pytorch/pytorch versions <=2.3.1. The vulnerability arises from the lack of security verification during the deserialization process of PythonUDF objects in pytorch/torch/distributed/rpc/internal.py. This flaw allows an attacker to execute arbitrary code remotely by sending a malicious serialized PythonUDF object, leading to remote code execution (RCE) on the master node.	Patched by core rule	Y
CVE-2024-7959	SSRF in open-webui/open-webui	The \`/openai/models\` endpoint in open-webui/open-webui version 0.3.8 is vulnerable to Server-Side Request Forgery (SSRF). An attacker can change the OpenAI URL to any URL without checks, causing the endpoint to send a request to the specified URL and return the output. This vulnerability allows the attacker to access internal services and potentially gain command execution by accessing instance secrets.	Patched by core rule	Y
CVE-2024-8019	Arbitrary File Write/Overwrite in lightning-ai/pytorch-lightning	In lightning-ai/pytorch-lightning version 2.3.2, a vulnerability exists in the \`LightningApp\` when running on a Windows host. The vulnerability occurs at the \`/api/v1/upload_file/\` endpoint, allowing an attacker to write or overwrite arbitrary files by providing a crafted filename. This can lead to potential remote code execution (RCE) by overwriting critical files or placing malicious files in sensitive locations.	Patched by core rule	Y
CVE-2024-8060	Remote Code Execution in OpenWebUI via Arbitrary File Upload	OpenWebUI version 0.3.0 contains a vulnerability in the audio API endpoint \`/audio/api/v1/transcriptions\` that allows for arbitrary file upload. The application performs insufficient validation on the \`file.content_type\` and allows user-controlled filenames, leading to a path traversal vulnerability. This can be exploited by an authenticated user to overwrite critical files within the Docker container, potentially leading to remote code execution as the root user.	Patched by core rule	Y
CVE-2024-8156	Command Injection in significant-gravitas/autogpt	A command injection vulnerability exists in the workflow-checker.yml workflow of significant-gravitas/autogpt. The untrusted user input	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		`github.head.ref` is used insecurely, allowing an attacker to inject arbitrary commands. This vulnerability affects versions up to and including the latest version. An attacker can exploit this by creating a branch name with a malicious payload and opening a pull request, potentially leading to reverse shell access or theft of sensitive tokens and keys.		
CVE-2024-8402	Improper Neutralization of Special Elements used in a Command ('Command Injection') in GitLab	An issue was discovered in GitLab EE affecting all versions starting from 17.2 before 17.7.7, all versions starting from 17.8 before 17.8.5, all versions starting from 17.9 before 17.9.2. An input validation issue in the Google Cloud IAM integration feature could have enabled a Maintainer to introduce malicious code.	Patched by core rule	Y
CVE-2024-8502	Remote Code Execution via Deserialization in modelscope/agentscope	A vulnerability in the RpcAgentServerLauncher class of modelscope/agentscope v0.0.6a3 allows for remote code execution (RCE) via deserialization of untrusted data using the dill library. The issue occurs in the AgentServerServicer.create_agent method, where serialized input is deserialized using dill.loads, enabling an attacker to execute arbitrary commands on the server.	Patched by core rule	Y
CVE-2024-8958	Unrestricted File Write and Read in composiohq/composio	In composiohq/composio version 0.4.3, there is an unrestricted file write and read vulnerability in the filetools actions. Due to improper validation of file paths, an attacker can read and write files anywhere on the server, potentially leading to privilege escalation or remote code execution.	Patched by core rule	Y
CVE-2024-9016	Unauthenticated Remote Command Execution in man-group/dtale	man-group dtale version <= 3.13.1 contains a vulnerability where the query parameters from the request are directly passed into the run_query function without proper sanitization. This allows for unauthenticated remote command execution via the df.query method when the query engine is set to 'python'.	Patched by core rule	Y
CVE-2024-9052	Remote Code Execution by Pickle Deserialization in vllm-project/vllm	vllm-project vllm version 0.6.0 contains a vulnerability in the distributed training API. The function vllm.distributed.GroupCoordinator.recv_object() deserializes received object bytes using pickle.loads() without sanitization, leading to a remote code execution vulnerability.	Patched by core rule	Y
CVE-2024-9053	Remote Code Execution in vllm-project/vllm	vllm-project vllm version 0.6.0 contains a vulnerability in the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		AsyncEngineRPCServer() RPC server entrypoints. The core functionality run_server_loop() calls the function _make_handler_coro(), which directly uses cloudpickle.loads() on received messages without any sanitization. This can result in remote code execution by deserializing malicious pickle data.		
CVE-2024-9415	Path Traversal in transformeroptimus/superagi	A Path Traversal vulnerability exists in the file upload functionality of transformeroptimus/superagi version 0.0.14. This vulnerability allows an attacker to upload an arbitrary file to the server, potentially leading to remote code execution or overwriting any file on the server.	Patched by core rule	Y
CVE-2024-9439	Remote Code Execution in transformeroptimus/superagi	SuperAGI is vulnerable to remote code execution in the latest version. The `agent template update` API allows attackers to control certain parameters, which are then fed to the eval function without any sanitization or checks in place. This vulnerability can lead to full system compromise.	Patched by core rule	Y
CVE-2024-9701	Remote Code Execution in kedro-org/kedro	A Remote Code Execution (RCE) vulnerability has been identified in the Kedro ShelveStore class (version 0.19.8). This vulnerability allows an attacker to execute arbitrary Python code via deserialization of malicious payloads, potentially leading to a full system compromise. The ShelveStore class uses Python's shelve module to manage session data, which relies on pickle for serialization. Crafting a malicious payload and storing it in the shelve file can lead to RCE when the payload is deserialized.	Patched by core rule	Y
CVE-2024-9880	Command Injection in pandas-dev/pandas	A command injection vulnerability exists in the `pandas.DataFrame.query` function of pandas-dev/pandas versions up to and including v2.2.2. This vulnerability allows an attacker to execute arbitrary commands on the server by crafting a malicious query. The issue arises from the improper validation of user-supplied input in the `query` function when using the 'python' engine, leading to potential remote command execution.	Patched by core rule	Y
CVE-2024-9920	Unrestricted File Upload and Execution in parisneo/lollms-webui	In version v12 of parisneo/lollms-webui, the 'Send file to AL' function allows uploading files with various extensions, including potentially dangerous ones like .py, .sh, .bat, and more. Attackers can exploit this by	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		uploading files with malicious content and then using the '/open_file' API endpoint to execute these files. The vulnerability arises from the use of 'subprocess.Popen' to open files without proper validation, leading to potential remote code execution.		
CVE-2025-0185	Pandas Query Injection in langgenius/dify	A vulnerability in the Dify Tools' Vanna module of the langgenius/dify repository allows for a Pandas Query Injection in the latest version. The vulnerability occurs in the function `vn.get_training_plan_generic(df_information_schema)`, which does not properly sanitize user inputs before executing queries using the Pandas library. This can potentially lead to Remote Code Execution (RCE) if exploited.	Patched by core rule	Y
CVE-2025-0655	Remote Code Execution via Global State Override in man-group/dtale	A vulnerability in man-group/dtale versions 3.15.1 allows an attacker to override global state settings to enable the `enable_custom_filters` feature, which is typically restricted to trusted environments. Once enabled, the attacker can exploit the /test-filter endpoint to execute arbitrary system commands, leading to remote code execution (RCE). This issue is addressed in version 3.16.1.	Patched by core rule	Y
CVE-2025-0912	GiveWP – Donation Plugin and Fundraising Platform <= 3.19.4 - Unauthenticated PHP Object Injection	The Donations Widget plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.19.4 via deserialization of untrusted input from the Donation Form through the 'card_address' parameter. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain allows attackers to achieve remote code execution.	Patched by core rule	Y
CVE-2025-1040	Server-Side Template Injection (SSTI) in significant-gravitas/autogpt	AutoGPT versions 0.3.4 and earlier are vulnerable to a Server-Side Template Injection (SSTI) that could lead to Remote Code Execution (RCE). The vulnerability arises from the improper handling of user-supplied format strings in the `AgentOutputBlock` implementation, where malicious input is passed to the Jinja2 templating engine without adequate security measures. Attackers can exploit this flaw to execute arbitrary commands on the host system. The issue is fixed in version 0.4.0.	Patched by core rule	Y
CVE-2025-1497	Remote Code Execution in PlotAI	A vulnerability, that could result in Remote Code Execution (RCE), has been found in PlotAI. Lack of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		validation of LLM-generated output allows attacker to execute arbitrary Python code. Vendor commented out vulnerable line, further usage of the software requires uncommenting it and thus accepting the risk. The vendor does not plan to release a patch to fix this vulnerability.		
CVE-2025-1800	D-Link DAR-7000 HTTP POST Request sxh_vpnlic.php get_ip_addr_details command injection	A vulnerability has been found in D-Link DAR-7000 3.2 and classified as critical. This vulnerability affects the function get_ip_addr_details of the file /view/vpn/sxh_vpn/sxh_vpnlic.php of the component HTTP POST Request Handler. The manipulation of the argument ethname leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-1819	Tenda AC7 1200M telnet TendaTelnet os command injection	A vulnerability, which was classified as critical, was found in Tenda AC7 1200M 15.03.06.44. Affected is the function TendaTelnet of the file /goform/telnet. The manipulation of the argument lan_ip leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1829	TOTOLINK X18 cstecgi.cgi setMtknatCfg os command injection	A vulnerability was found in TOTOLINK X18 9.1.0cu.2024_B20220329. It has been declared as critical. This vulnerability affects the function setMtknatCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument mtkhnatEnable leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-1845	ESAFENET DSM examExportPDF command injection	A vulnerability has been found in ESAFENET DSM 3.1.2 and classified as critical. Affected by this vulnerability is the function examExportPDF of the file /admin/plan/examExportPDF. The manipulation of the argument s leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-1946	hzmanyun Education and Training System	A vulnerability was found in hzmanyun Education and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	exportPDF command injection	Training System 2.1. It has been rated as critical. Affected by this issue is the function exportPDF of the file /user/exportPDF. The manipulation of the argument id leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-1947	hzmanyun Education and Training System UploadImageController.java scorm command injection	A vulnerability classified as critical has been found in hzmanyun Education and Training System 2.1.3. This affects the function scorm of the file UploadImageController.java. The manipulation of the argument param leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-2094	TOTOLINK EX1800T cstecgi.cgi setWiFiExtenderConfig os command injection	A vulnerability was found in TOTOLINK EX1800T 9.1.0cu.2112_B20220316. It has been rated as critical. Affected by this issue is the function setWiFiExtenderConfig of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument apcliKey/key leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-2095	TOTOLINK EX1800T cstecgi.cgi setDmzCfg os command injection	A vulnerability classified as critical has been found in TOTOLINK EX1800T 9.1.0cu.2112_B20220316. This affects the function setDmzCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ip leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-2096	TOTOLINK EX1800T cstecgi.cgi setRebootScheCfg os command injection	A vulnerability classified as critical was found in TOTOLINK EX1800T 9.1.0cu.2112_B20220316. This vulnerability affects the function setRebootScheCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument mode/week/minute/recHour leads to os command 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-2025-24813	Apache Tomcat: Potential RCE and/or information disclosure and/or information corruption with partial PUT	Path Equivalence: 'file.Name' (Internal Dot) leading to Remote Code Execution and/or Information disclosure and/or malicious content added to uploaded files via write enabled Default Servlet in Apache Tomcat. This issue affects Apache	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Tomcat: from 11.0.0-M1 through 11.0.2, from 10.1.0-M1 through 10.1.34, from 9.0.0.M1 through 9.0.98. If all of the following were true, a malicious user was able to view security sensitive files and/or inject content into those files: - writes enabled for the default servlet (disabled by default) - support for partial PUT (enabled by default) - a target URL for security sensitive uploads that was a sub-directory of a target URL for public uploads - attacker knowledge of the names of security sensitive files being uploaded - the security sensitive files also being uploaded via partial PUT If all of the following were true, a malicious user was able to perform remote code execution: - writes enabled for the default servlet (disabled by default) - support for partial PUT (enabled by default) - application was using Tomcat's file based session persistence with the default storage location - application included a library that may be leveraged in a deserialization attack Users are recommended to upgrade to version 11.0.3, 10.1.35 or 9.0.98, which fixes the issue.		
CVE-2025-2512	File Away <= 3.9.9.0.1 - Missing Authorization to Unauthenticated File Upload via upload Function	The File Away plugin for WordPress is vulnerable to arbitrary file uploads due to a missing capability check and missing file type validation in the upload() function in all versions up to, and including, 3.9.9.0.1. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	Patched by core rule	Y
CVE-2025-26924	WordPress Ohio Theme Extra plugin <= 3.4.7 - Shortcode Injection vulnerability	Improper Control of Generation of Code ('Code Injection') vulnerability in NotFound Ohio Extra allows Code Injection. This issue affects Ohio Extra: from n/a through 3.4.7.	Patched by core rule	Y
CVE-2025-26936	WordPress Fresh Framework plugin <= 1.70.0 - Unauthenticated Remote Code Execution (RCE) vulnerability	Improper Control of Generation of Code ('Code Injection') vulnerability in NotFound Fresh Framework allows Code Injection. This issue affects Fresh Framework: from n/a through 1.70.0.	Patched by core rule	Y
CVE-2025-26970	WordPress Ark Theme Core plugin <= 1.70.0 - Unauthenticated Remote Code Execution (RCE) vulnerability	Improper Control of Generation of Code ('Code Injection') vulnerability in NotFound Ark Theme Core allows Code Injection. This issue affects Ark Theme	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Core: from n/a through 1.70.0.		
CVE-2025-2701	AMTT Hotel Broadband Operation System port_setup.php popen os command injection	A vulnerability classified as critical was found in AMTT Hotel Broadband Operation System 1.0. This vulnerability affects the function popen of the file /manager/network/port_setup.php. The manipulation of the argument SwitchVersion/SwitchWrite/SwitchIP/SwitchIndex/SwitchState leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2717	D-Link DIR-823X HTTP POST Request diag_nslookup sub_41710C os command injection	A vulnerability, which was classified as critical, has been found in D-Link DIR-823X 240126/240802. This issue affects the function sub_41710C of the file /goform/diag_nslookup of the component HTTP POST Request Handler. The manipulation of the argument target_addr leads to os command 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-2025-2725	H3C Magic BE18000 HTTP POST Request auth command injection	A vulnerability classified as critical was found in H3C Magic NX15, Magic NX30 Pro, Magic NX400, Magic R3010 and Magic BE18000 up to V100R014. Affected by this vulnerability is an unknown functionality of the file /api/login/auth of the component HTTP POST Request Handler. The manipulation leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2726	H3C Magic BE18000 HTTP POST Request esps command injection	A vulnerability, which was classified as critical, has been found in H3C Magic NX15, Magic NX30 Pro, Magic NX400, Magic R3010 and Magic BE18000 up to V100R014. Affected by this issue is some unknown functionality of the file /api/esps of the component HTTP POST Request Handler. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2727	H3C Magic NX30 Pro HTTP POST Request getNetworkStatus command injection	A vulnerability, which was classified as critical, was found in H3C Magic NX30 Pro up to V100R007. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects an unknown part of the file /api/wizard/getNetworkStatus of the component HTTP POST Request Handler. The manipulation leads to command injection. 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.		
CVE-2025-2728	H3C Magic NX30 Pro/Magic NX400 getNetworkConf command injection	A vulnerability has been found in H3C Magic NX30 Pro and Magic NX400 up to V100R014 and classified as critical. This vulnerability affects unknown code of the file /api/wizard/getNetworkConf. The manipulation leads to command injection. The attack can be initiated remotely. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2729	H3C Magic BE18000 HTTP POST Request networkSetup command injection	A vulnerability was found in H3C Magic NX15, Magic NX30 Pro, Magic NX400, Magic R3010 and Magic BE18000 up to V100R014 and classified as critical. This issue affects some unknown processing of the file /api/wizard/networkSetup of the component HTTP POST Request Handler. The manipulation leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2730	H3C Magic BE18000 HTTP POST Request getssidname command injection	A vulnerability was found in H3C Magic NX15, Magic NX30 Pro, Magic NX400, Magic R3010 and Magic BE18000 up to V100R014. It has been classified as critical. Affected is an unknown function of the file /api/wizard/getssidname of the component HTTP POST Request Handler. The manipulation leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2731	H3C Magic BE18000 HTTP POST Request getDualbandSync command injection	A vulnerability was found in H3C Magic NX15, Magic NX30 Pro, Magic NX400, Magic R3010 and Magic BE18000 up to V100R014. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /api/wizard/getDualbandSync of the component HTTP POST Request Handler. The manipulation leads to command injection. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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-2025-2732	H3C Magic BE18000 HTTP POST Request getWifiNeighbour command injection	A vulnerability was found in H3C Magic NX15, Magic NX30 Pro, Magic NX400, Magic R3010 and Magic BE18000 up to V100R014. It has been rated as critical. Affected by this issue is some unknown functionality of the file /api/wizard/getWifiNeighbour of the component HTTP POST Request Handler. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-27407	Remote code execution when loading a crafted GraphQL schema	graphql-ruby is a Ruby implementation of GraphQL. Starting in version 1.11.5 and prior to versions 1.11.8, 1.12.25, 1.13.24, 2.0.32, 2.1.14, 2.2.17, and 2.3.21, loading a malicious schema definition in `GraphQL::Schema.from_introspection` (or `GraphQL::Schema::Loader.load`) can result in remote code execution. Any system which loads a schema by JSON from an untrusted source is vulnerable, including those that use GraphQL::Client to load external schemas via GraphQL introspection. Versions 1.11.8, 1.12.25, 1.13.24, 2.0.32, 2.1.14, 2.2.17, and 2.3.21 contain a patch for the issue.	Patched by core rule	Y
CVE-2025-27410	PwnDoc Arbitrary File Write to RCE using Path Traversal in backup restore as admin	PwnDoc is a penetration test reporting application. Prior to version 1.2.0, the backup restore functionality is vulnerable to path traversal in the TAR entry's name, allowing an attacker to overwrite any file on the system with their content. By overwriting an included `.js` file and restarting the container, this allows for Remote Code Execution as an administrator. The remote code execution occurs because any user with the `backups:create` and `backups:update` (only administrators by default) is able to overwrite any file on the system. Version 1.2.0 fixes the issue.	Patched by core rule	Y
CVE-2025-27413	PwnDoc Arbitrary File Write to RCE using Path Traversal in template update from backup templates.json	PwnDoc is a penetration test reporting application. Prior to version 1.2.0, the backup restore functionality allows an administrator to import raw data into the database, including Path Traversal (`../`) sequences. This is problematic for the template	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		update functionality as it uses the path from the database to write arbitrary content to, potentially overwriting source code to achieve Remote Code Execution. Any user with the `backups:create`, `backups:update` and `templates:update` permissions (only administrators by default) can write arbitrary content to anywhere on the filesystem. By overwriting source code, it is possible to achieve Remote Code Execution. Version 1.2.0 fixes the issue.		
CVE-2025-27510	RCE in the package conda-forge-metadata	conda-forge-metadata provides programatic access to conda-forge's metadata. conda-forge-metadata uses an optional dependency - "conda-oci-mirror" which was neither present on the PyPi repository nor registered by any entity. If conda-oci-mirror is taken over by a threat actor, it can result in remote code execution.	Patched by core rule	Y
CVE-2025-27519	Cognita Arbitrary File Write	Cognita is a RAG (Retrieval Augmented Generation) Framework for building modular, open source applications for production by TrueFoundry. A path traversal issue exists at /v1/internal/upload-to-local-directory which is enabled when the Local env variable is set to true, such as when Cognita is setup using Docker. Because the docker environment sets up the backend uvicorn server with auto reload enabled, when an attacker overwrites the /app/backend/__init__.py file, the file will automatically be reloaded and executed. This allows an attacker to get remote code execution in the context of the Docker container. This vulnerability is fixed in commit a78bd065e05a1b30a53a3386cc02e08c317d2243.	Patched by core rule	Y
CVE-2025-27607	Python JSON Logger has a Potential RCE via missing `msgspec-python313-pre` dependency	Python JSON Logger is a JSON Formatter for Python Logging. Between 30 December 2024 and 4 March 2025 Python JSON Logger was vulnerable to RCE through a missing dependency. This occurred because msgspec-python313-pre was deleted by the owner leaving the name open to being claimed by a third party. If the package was claimed, it would allow them RCE on any Python JSON Logger user who installed the development dependencies on Python 3.13 (e.g. pip install python-json-logger[dev]). This issue has been resolved with 3.3.0.	Patched by core rule	Y
CVE-2025-27616	Vela Server has	Vela is a Pipeline	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Insufficient Webhook Payload Data Verification	Automation (CI/CD) framework built on Linux container technology written in Golang. Prior to versions 0.25.3 and 0.26.3, by spoofing a webhook payload with a specific set of headers and body data, an attacker could transfer ownership of a repository and its repo level secrets to a separate repository. These secrets could be exfiltrated by follow up builds to the repository. Users with an enabled repository with access to repo level CI secrets in Vela are vulnerable to the exploit, and any user with access to the CI instance and the linked source control manager can perform the exploit. Versions 0.25.3 and 0.26.3 fix the issue. No known workarounds are available.	rule	
CVE-2025-27774	Applio allows SSRF and file write in model_download.py	Applio is a voice conversion tool. Versions 3.2.7 and prior are vulnerable to server-side request forgery (SSRF) and file write in `model_download.py` (line 156 in 3.2.7). The blind SSRF allows for sending requests on behalf of Applio server and can be leveraged to probe for other vulnerabilities on the server itself or on other back-end systems on the internal network, that the Applio server can reach. The blind SSRF can also be coupled with the an arbitrary file read (e.g., CVE-2025-27784) to read files from hosts on the internal network, that the Applio server can reach, which would make it a full SSRF. The file write allows for writing files on the server, which can be coupled with other vulnerabilities, for example an unsafe deserialization, to achieve remote code execution on the Applio server. As of time of publication, no known patches are available.	Patched by core rule	Y
CVE-2025-27775	Applio allows SSRF and file write in model_download.py	Applio is a voice conversion tool. Versions 3.2.7 and prior are vulnerable to server-side request forgery (SSRF) and file write in `model_download.py` (line 143 in 3.2.7). The blind SSRF allows for sending requests on behalf of Applio server and can be leveraged to probe for other vulnerabilities on the server itself or on other back-end systems on the internal network, that the Applio server can reach. The file write allows for writing files on the server, which can be coupled with other vulnerabilities, for example an unsafe deserialization, to achieve remote code execution on the Applio server. As of time of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		publication, no known patches are available.		
CVE-2025-27776	Applio allows SSRF and file write in model_download.py	Applio is a voice conversion tool. Versions 3.2.7 and prior are vulnerable to server-side request forgery (SSRF) and file write in `model_download.py` (line 240 in 3.2.7). The blind SSRF allows for sending requests on behalf of Applio server and can be leveraged to probe for other vulnerabilities on the server itself or on other back-end systems on the internal network, that the Applio server can reach. The blind SSRF can also be coupled with the arbitrary file read CVE-2025-27784 to read files from hosts on the internal network, that the Applio server can reach, which would make it a full SSRF. The file write allows for writing files on the server, which can be coupled with other vulnerabilities, for example an unsafe deserialization, to achieve remote code execution on the Applio server. As of time of publication, no known patches are available.	Patched by core rule	Y
CVE-2025-27778	Applio allows unsafe deserialization in infer.py	Applio is a voice conversion tool. Versions 3.2.8-bugfix and prior are vulnerable to unsafe deserialization in `infer.py`. The issue can lead to remote code execution. As of time of publication, a fix is available on the `main` branch of the Applio repository but not attached to a numbered release.	Patched by core rule	Y
CVE-2025-27779	Applio allows unsafe deserialization in model_blender.py	Applio is a voice conversion tool. Versions 3.2.8-bugfix and prior are vulnerable to unsafe deserialization in `model_blender.py` lines 20 and 21. `model_fusion_a` and `model_fusion_b` from voice_blender.py take user-supplied input (e.g. a path to a model) and pass that value to the `run_model_blender_script` and later to `model_blender` function, which loads these two models with `torch.load` in `model_blender.py (on lines 20-21 in 3.2.8-bugfix), which is vulnerable to unsafe deserialization. The issue can lead to remote code execution. A patch is available on the `main` branch of the Applio repository.	Patched by core rule	Y
CVE-2025-27780	Applio allows unsafe deserialization in model_information.py	Applio is a voice conversion tool. Versions 3.2.8-bugfix and prior are vulnerable to unsafe deserialization in model_information.py. `model_name` in model_information.py takes user-supplied input (e.g. a path to a model) and pass that value to the `run_model_information_script` and later to `model_information`	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		function, which loads that model with `torch.load` in rvc/train/process/model_information.py (on line 16 in 3.2.8-bugfix), which is vulnerable to unsafe deserialization. The issue can lead to remote code execution. A patch is available in the `main` branch of the repository.		
CVE-2025-27781	Applio allows unsafe deserialization in inference.py	Applio is a voice conversion tool. Versions 3.2.8-bugfix and prior are vulnerable to unsafe deserialization in inference.py. `model_file` in inference.py as well as `model_file` in tts.py take user-supplied input (e.g. a path to a model) and pass that value to the `change_choices` and later to `get_speakers_id` function, which loads that model with `torch.load` in inference.py (line 326 in 3.2.8-bugfix), which is vulnerable to unsafe deserialization. The issue can lead to remote code execution. A patch is available on the `main` branch of the repository.	Patched by core rule	Y
CVE-2025-27782	Applio allows arbitrary file write in inference.py	Applio is a voice conversion tool. Versions 3.2.8-bugfix and prior are vulnerable to arbitrary file write in inference.py. This issue may lead to writing arbitrary files on the Applio server. It can also be used in conjunction with an unsafe deserialization to achieve remote code execution. As of time of publication, no known patches are available.	Patched by core rule	Y
CVE-2025-27783	Applio allows arbitrary file write in train.py	Applio is a voice conversion tool. Versions 3.2.8-bugfix and prior are vulnerable to arbitrary file write in train.py. This issue may lead to writing arbitrary files on the Applio server. It can also be used in conjunction with an unsafe deserialization to achieve remote code execution. As of time of publication, no known patches are available.	Patched by core rule	Y
CVE-2025-29783	vLLM Allows Remote Code Execution via Mooncake Integration	vLLM is a high-throughput and memory-efficient inference and serving engine for LLMs. When vLLM is configured to use Mooncake, unsafe deserialization exposed directly over ZMQ/TCP on all network interfaces will allow attackers to execute remote code on distributed hosts. This is a remote code execution vulnerability impacting any deployments using Mooncake to distribute KV across distributed hosts. This vulnerability is fixed in 0.8.0.	Patched by core rule	Y

Path Traversal Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-25773	Relative Path Traversal in assets file upload	This advisory addresses a file placement vulnerability that could allow assets to be uploaded to unintended directories on the server. * Improper Limitation of a Pathname to a Restricted Directory: A vulnerability exists in the asset upload functionality that allows users to upload files to directories outside of the intended temporary directory.	Patched by core rule	Y
CVE-2024-10330	Improper Access Control in lunary-ai/lunary	In lunary-ai/lunary version 1.5.6, the `/v1/evaluators/` endpoint lacks proper access control, allowing any user associated with a project to fetch all evaluator data regardless of their role. This vulnerability permits low-privilege users to access potentially sensitive evaluation data.	Patched by core rule	Y
CVE-2024-10553	Jdbc Deserialization in h2oai/h2o-3	A vulnerability in the h2oai/h2o-3 REST API versions 3.46.0.4 allows unauthenticated remote attackers to execute arbitrary code via deserialization of untrusted data. The vulnerability exists in the endpoints POST /99/ImportSQLTable and POST /3/SaveToHiveTable, where user-controlled JDBC URLs are passed to DriverManager.getConnection, leading to deserialization if a MySQL or PostgreSQL driver is available in the classpath. This issue is fixed in version 3.47.0.	Patched by core rule	Y
CVE-2024-10830	Path Traversal in eosphoros-ai/db-gpt	A Path Traversal vulnerability exists in the eosphoros-ai/db-gpt version 0.6.0 at the API endpoint `/v1/resource/file/delete`. This vulnerability allows an attacker to delete any file on the server by manipulating the `file_key` parameter. The `file_key` parameter is not properly sanitized, enabling an	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attacker to specify arbitrary file paths. If the specified file exists, the application will delete it.		
CVE-2024-10833	Arbitrary File Write in eosphoros-ai/db-gpt	eosphoros-ai/db-gpt version 0.6.0 is vulnerable to an arbitrary file write through the knowledge API. The endpoint for uploading files as 'knowledge' is susceptible to absolute path traversal, allowing attackers to write files to arbitrary locations on the target server. This vulnerability arises because the 'doc_file.filename' parameter is user-controllable, enabling the construction of absolute paths.	Patched by core rule	Y
CVE-2024-10834	Arbitrary File Write in eosphoros-ai/db-gpt	eosphoros-ai/db-gpt version 0.6.0 contains a vulnerability in the RAG-knowledge endpoint that allows for arbitrary file write. The issue arises from the ability to pass an absolute path to a call to \`os.path.join\`, enabling an attacker to write files to arbitrary locations on the target server. This vulnerability can be exploited by setting the \`doc_file.filename\` to an absolute path, which can lead to overwriting system files or creating new SSH-key entries.	Patched by core rule	Y
CVE-2024-11137	IDOR Vulnerability in PATCH \`/v1/runs/:id/score\` Endpoint in lunary-ai/lunary	An Insecure Direct Object Reference (IDOR) vulnerability exists in the \`PATCH /v1/runs/:id/score\` endpoint of lunary-ai/lunary version 1.6.0. This vulnerability allows an attacker to update the score data of any run by manipulating the id parameter in the request URL, which corresponds to the \`runId_score\` in the database. The endpoint does not sufficiently validate whether the authenticated user has permission to modify the specified runId, enabling an attacker with a valid account to modify other users' runId scores by specifying different id values. This issue was fixed	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		in version 1.6.1.		
CVE-2024-12380	Generation of Error Message Containing Sensitive Information in GitLab	An issue was discovered in GitLab EE/CE affecting all versions starting from 11.5 before 17.7.7, all versions starting from 17.8 before 17.8.5, all versions starting from 17.9 before 17.9.2. Certain user inputs in repository mirroring settings could potentially expose sensitive authentication information.	Patched by core rule	Y
CVE-2024-12880	Partial Account Takeover due to Insecure Data Querying in infiniflow/ragflow	A vulnerability in infiniflow/ragflow version RAGFlow-0.13.0 allows for partial account takeover via insecure data querying. The issue arises from the way tenant IDs are handled in the application. If a user has access to multiple tenants, they can manipulate their tenant access to query and access API tokens of other tenants. This vulnerability affects the following endpoints: /v1/system/token_list, /v1/system/new_token, /v1/api/token_list, /v1/api/new_token, and /v1/api/rm. An attacker can exploit this to access other tenants' API tokens, perform actions on behalf of other tenants, and access their data.	Patched by core rule	Y
CVE-2024-6583	Path Traversal in stangirard/quivr	A path traversal vulnerability exists in the latest version of stangirard/quivr. This vulnerability allows an attacker to upload files to arbitrary paths in an S3 bucket by manipulating the file path in the upload request.	Patched by core rule	Y
CVE-2024-7039	Improper Privilege Management in open-webui/open-webui	In open-webui/open-webui version v0.3.8, there is an improper privilege management vulnerability. The application allows an attacker, acting as an admin, to delete other administrators via the API endpoint `http://0.0.0.0:8080/api/v1/users/{uuid_administrator}`. This action is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		restricted by the user interface but can be performed through direct API calls.		
CVE-2024-8438	Path Traversal in modelscope/agentscope	A path traversal vulnerability exists in modelscope/agentscope version v.0.0.4. The API endpoint `/api/file` does not properly sanitize the `path` parameter, allowing an attacker to read arbitrary files on the server.	Patched by core rule	Y
CVE-2024-8524	Directory Traversal in modelscope/agentscope	A directory traversal vulnerability exists in modelscope/agentscope version 0.0.4. An attacker can exploit this vulnerability to read any local JSON file by sending a crafted POST request to the /read-examples endpoint.	Patched by core rule	Y
CVE-2024-8551	Path Traversal in modelscope/agentscope	A path traversal vulnerability exists in the save-workflow and load-workflow functionality of modelscope/agentscope versions prior to the fix. This vulnerability allows an attacker to read and write arbitrary JSON files on the filesystem, potentially leading to the exposure or modification of sensitive information such as configuration files, API keys, and hardcoded passwords.	Patched by core rule	Y
CVE-2024-8581	Path Traversal in parisneo/lollms-webui	A vulnerability in the `upload_app` function of parisneo/lollms-webui V12 (Strawberry) allows an attacker to delete any file or directory on the system. The function does not implement user input filtering with the `filename` value, causing a Path Traversal error.	Patched by core rule	Y
CVE-2024-8616	Arbitrary File Overwrite in h2oai/h2o-3	In h2oai/h2o-3 version 3.46.0, the `/99/Models/{name}/json` endpoint allows for arbitrary file overwrite on the target server. The vulnerability arises from the `exportModelDetails` function in `ModelsHandler.java`, where the user-controllable `mexport.dir` parameter is used to specify the file path for	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		writing model details. This can lead to overwriting files at arbitrary locations on the host system.		
CVE-2024-8898	Path Traversal in parisneo/lollms-webui	A path traversal vulnerability exists in the \`install\` and \`uninstall\` API endpoints of parisneo/lollms-webui version V12 (Strawberry). This vulnerability allows attackers to create or delete directories with arbitrary paths on the system. The issue arises due to insufficient sanitization of user-supplied input, which can be exploited to traverse directories outside the intended path.	Patched by core rule	Y
CVE-2024-8999	Improper Access Control in lunary-ai/lunary	lunary-ai/lunary version v1.4.25 contains an improper access control vulnerability in the POST /api/v1/data-warehouse/bigquery endpoint. This vulnerability allows any user to export the entire database data by creating a stream to Google BigQuery without proper authentication or authorization. The issue is fixed in version 1.4.26.	Patched by core rule	Y
CVE-2024-9095	Improper Authorization in lunary-ai/lunary	In lunary-ai/lunary version v1.4.28, the /bigquery API route lacks proper access control, allowing any logged-in user to create a Datastream to Google BigQuery and export the entire database. This includes sensitive data such as password hashes and secret API keys. The route is protected by a config check (\`config.DATA_WAREHOUSE_EXPORTS_ALLOWED\`), but it does not verify the user's access level or implement any access control middleware. This vulnerability can lead to the extraction of sensitive data, disruption of services, credential compromise, and service integrity breaches.	Patched by core rule	Y
CVE-2024-9096	Improper Authorization in lunary-ai/lunary	In lunary-ai/lunary version 1.4.28, the /checklists/:id route allows low-privilege users to modify checklists	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		by sending a PATCH request. The route lacks proper access control, such as middleware to ensure that only authorized users (e.g., project owners or admins) can modify checklist data. This vulnerability allows any user associated with the project, regardless of their role, to modify checklists, including changing the slug or data fields, which can lead to tampering with essential project workflows, altering business logic, and introducing errors that undermine integrity.		
CVE-2024-9597	Path Traversal in parisneo/lollms	A Path Traversal vulnerability exists in the `/wipe_database` endpoint of parisneo/lollms version v12, allowing an attacker to delete any directory on the system. The vulnerability arises from improper validation of the `key` parameter, which is used to construct file paths. An attacker can exploit this by sending a specially crafted HTTP request to delete arbitrary directories.	Patched by core rule	Y
CVE-2024-9617	IDOR in danswer-ai/danswer	An IDOR vulnerability in danswer-ai/danswer v0.3.94 allows an attacker to view any files. The application does not verify whether the attacker is the creator of the file, allowing the attacker to directly call the GET /api/chat/file/{file_id} interface to view any user's file.	Patched by core rule	Y
CVE-2025-0452	Arbitrary File Deletion in eosphoros-ai/DB-GPT	eosphoros-ai/DB-GPT version latest is vulnerable to arbitrary file deletion on Windows systems via the '/v1/agent/hub/update' endpoint. The application fails to properly filter the '\' character, which is commonly used as a separator in Windows paths. This vulnerability allows attackers to delete any files on the host system by manipulating the 'plugin_repo_name' variable.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-0495	Secrets leakage to telemetry endpoint via cache backend configuration via buildx	Buildx is a Docker CLI plugin that extends build capabilities using BuildKit. Cache backends support credentials by setting secrets directly as attribute values in cache-to/cache-from configuration. When supplied as user input, these secure values may be inadvertently captured in OpenTelemetry traces as part of the arguments and flags for the traced CLI command. OpenTelemetry traces are also saved in BuildKit daemon's history records. This vulnerability does not impact secrets passed to the Github cache backend via environment variables or registry authentication.	Patched by core rule	Y
CVE-2025-1743	zyx0814 Pichome index.php path traversal	A vulnerability, which was classified as critical, was found in zyx0814 Pichome 2.1.0. This affects an unknown part of the file /index.php?mod=textviewer. The manipulation of the argument src leads to path traversal. 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-2025-1833	zj1983 zz HTTP Request Customer_noticeAction.java sendNotice server-side request forgery	A vulnerability, which was classified as critical, has been found in zj1983 zz up to 2024-8. Affected by this issue is the function sendNotice of the file src/main/java/com/futvan/z/erp/customer_notice/Customer_noticeAction.java of the component HTTP Request Handler. The manipulation of the argument url leads to server-side request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-2032	ChestnutCMS rename renameFile path traversal	A vulnerability classified as problematic was found in ChestnutCMS 1.5.2. This vulnerability affects the function renameFile of the file /cms/file/rename. The manipulation of the argument rename leads to path traversal. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-2116	Beijing Founder Electronics Founder Enjoys All-Media Acquisition and Editing System File Protocol imageProxy.do server-side request forgery	A vulnerability has been found in Beijing Founder Electronics Founder Enjoys All-Media Acquisition and Editing System 3.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /newsedit/newsedit/xy/imageProxy.do of the component File Protocol Handler. The manipulation of the argument xyImgUrl leads to server-side request forgery. 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-2025-2193	MRCMS org.marker.mushroom.controller.FileController delete.do delete path traversal	A vulnerability has been found in MRCMS 3.1.2 and classified as critical. This vulnerability affects the function delete of the file /admin/file/delete.do of the component org.marker.mushroom.controller.FileController. The manipulation of the argument path/name leads to path traversal. 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-2025-2215	Doufox s=doudou path traversal	A vulnerability classified as critical was found in Doufox up to 0.2.0. Affected by this vulnerability is an unknown functionality of the file /?s=doudou&c=file&a=list. The manipulation of the argument dir leads to path	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		traversal. 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-2025-25122	WordPress WizShop Plugin <= 3.0.2 - Local File Inclusion vulnerability	Path Traversal vulnerability in NotFound WizShop allows PHP Local File Inclusion. This issue affects WizShop: from n/a through 3.0.2.	Patched by core rule	Y
CVE-2025-25130	WordPress Delete Comments By Status plugin <= 1.5.3 - Local File Inclusion vulnerability	Relative Path Traversal vulnerability in NotFound Delete Comments By Status allows PHP Local File Inclusion. This issue affects Delete Comments By Status: from n/a through 2.1.1.	Patched by core rule	Y
CVE-2025-25162	WordPress Sports Rankings and Lists plugin <= 2.3 - Arbitrary File Download vulnerability	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in NotFound Sports Rankings and Lists allows Absolute Path Traversal. This issue affects Sports Rankings and Lists: from n/a through 1.0.2.	Patched by core rule	Y
CVE-2025-2546	D-Link DIR-618/DIR-605L Firewall Service formAdvFirewall access control	A vulnerability classified as problematic was found in D-Link DIR-618 and DIR-605L 2.02/3.02. This vulnerability affects unknown code of the file /goform/formAdvFirewall of the component Firewall Service. The manipulation leads to improper access controls. The attack needs to be approached within the local network. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-2547	D-Link DIR-618/DIR-605L formAdvNetwork access control	A vulnerability, which was classified as problematic, has been found in D-Link DIR-618 and DIR-605L 2.02/3.02. This issue affects some unknown processing of the file /goform/formAdvNetwork . The manipulation leads to improper access controls. The attack can only be done within the local network. The exploit has been disclosed to the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.		
CVE-2025-2548	D-Link DIR-618/DIR-605L formSetDomainFilter access control	A vulnerability, which was classified as problematic, was found in D-Link DIR-618 and DIR-605L 2.02/3.02. Affected is an unknown function of the file /goform/formSetDomainFilter. The manipulation leads to improper access controls. The attack can only be initiated within the local network. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-2549	D-Link DIR-618/DIR-605L formSetPassword access control	A vulnerability has been found in D-Link DIR-618 and DIR-605L 2.02/3.02 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /goform/formSetPassword. The manipulation leads to improper access controls. The attack needs to be done within the local network. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-2550	D-Link DIR-618/DIR-605L DDNS Service formSetDDNS access control	A vulnerability was found in D-Link DIR-618 and DIR-605L 2.02/3.02 and classified as problematic. Affected by this issue is some unknown functionality of the file /goform/formSetDDNS of the component DDNS Service. The manipulation leads to improper access controls. The attack needs to be initiated within the local network. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-2551	D-Link DIR-618/DIR-605L formSetPortTr access control	A vulnerability was found in D-Link DIR-618 and DIR-605L 2.02/3.02. It has been classified as problematic. This affects an unknown part of the file /goform/formSetPortTr. The manipulation leads to improper access controls. Access to the local network is required for this attack. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-2552	D-Link DIR-618/DIR-605L formTcpipSetup access control	A vulnerability was found in D-Link DIR-618 and DIR-605L 2.02/3.02. It has been declared as problematic. This vulnerability affects unknown code of the file /goform/formTcpipSetup. The manipulation leads to improper access controls. Access to the local network is required for this attack to succeed. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-2553	D-Link DIR-618/DIR-605L formVirtualServ access control	A vulnerability was found in D-Link DIR-618 and DIR-605L 2.02/3.02. It has been rated as problematic. This issue affects some unknown processing of the file /goform/formVirtualServ. The manipulation leads to improper access controls. The attack needs to be approached within the local network. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-26534	WordPress Helloprint Plugin <= 2.0.7 - Arbitrary File Deletion vulnerability	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in NotFound Helloprint allows Path Traversal. This issue affects Helloprint: from n/a through 2.0.7.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-26540	WordPress Helloprint Plugin <= 2.0.7 - Arbitrary File Deletion vulnerability	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in NotFound Helloprint allows Path Traversal. This issue affects Helloprint: from n/a through 2.0.7.	Patched by core rule	Y
CVE-2025-26885	WordPress Assistant Plugin <= 1.5.1 - PHP Object Injection vulnerability	Deserialization of Untrusted Data vulnerability in Brent Jett Assistant allows Object Injection. This issue affects Assistant: from n/a through 1.5.1.	Patched by core rule	Y
CVE-2025-26921	WordPress Booking and Rental Manager Plugin <= 2.2.6 - PHP Object Injection vulnerability	Deserialization of Untrusted Data vulnerability in magepeopleteam Booking and Rental Manager allows Object Injection. This issue affects Booking and Rental Manager: from n/a through 2.2.6.	Patched by core rule	Y
CVE-2025-26940	WordPress Pie Register Premium plugin <= 3.8.3.2 - Path Traversal to Non-Arbitrary File Deletion vulnerability	Path Traversal vulnerability in NotFound Pie Register Premium. This issue affects Pie Register Premium: from n/a through 3.8.3.2.	Patched by core rule	Y
CVE-2025-26967	WordPress Events Calendar for GeoDirectory plugin <= 2.3.14 - PHP Object Injection vulnerability	Deserialization of Untrusted Data vulnerability in Stiofan Events Calendar for GeoDirectory allows Object Injection. This issue affects Events Calendar for GeoDirectory: from n/a through 2.3.14.	Patched by core rule	Y
CVE-2025-26999	WordPress ProfileGrid Plugin <= 5.9.4.3 - PHP Object Injection vulnerability	Deserialization of Untrusted Data vulnerability in Metagauss ProfileGrid allows Object Injection. This issue affects ProfileGrid : from n/a through 5.9.4.3.	Patched by core rule	Y
CVE-2025-2707	zhijiantianya ruoyi-vue-pro Front-End Store Interface upload path traversal	A vulnerability, which was classified as critical, has been found in zhijiantianya ruoyi-vue-pro 2.4.1. Affected by this issue is some unknown functionality of the file /app-api/infra/file/upload of the component Front-End Store Interface. The manipulation of the argument path leads to path traversal. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		early about this disclosure but did not respond in any way.		
CVE-2025-2708	zhijiantianya ruoyi-vue-pro Backend File Upload Interface upload path traversal	A vulnerability, which was classified as critical, was found in zhijiantianya ruoyi-vue-pro 2.4.1. This affects an unknown part of the file /admin-api/infra/file/upload of the component Backend File Upload Interface. The manipulation of the argument path leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2716	China Mobile P22g-CIac Samba Path path traversal	A vulnerability classified as problematic was found in China Mobile P22g-CIac 1.0.00.488. This vulnerability affects unknown code of the component Samba Path Handler. The manipulation leads to path traversal. 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-2025-27274	WordPress GPX Viewer plugin <= 2.2.11 - Path Traversal vulnerability	Path Traversal vulnerability in NotFound GPX Viewer allows Path Traversal. This issue affects GPX Viewer: from n/a through 2.2.11.	Patched by core rule	Y
CVE-2025-2742	zhijiantianya ruoyi-vue-pro Material Upload Interface upload-permanent path traversal	A vulnerability classified as critical was found in zhijiantianya ruoyi-vue-pro 2.4.1. This vulnerability affects unknown code of the file /admin-api/mp/material/upload-permanent of the component Material Upload Interface. The manipulation of the argument File leads to path traversal. 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		respond in any way.		
CVE-2025-2743	zhijiantianya ruoyi-vue-pro Material Upload Interface upload-temporary path traversal	A vulnerability, which was classified as problematic, has been found in zhijiantianya ruoyi-vue-pro 2.4.1. This issue affects some unknown processing of the file /admin-api/mp/material/upload-temporary of the component Material Upload Interface. The manipulation of the argument File leads to path traversal. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2744	zhijiantianya ruoyi-vue-pro Material Upload Interface upload-news-image path traversal	A vulnerability, which was classified as critical, was found in zhijiantianya ruoyi-vue-pro 2.4.1. Affected is an unknown function of the file /admin-api/mp/material/upload-news-image of the component Material Upload Interface. The manipulation of the argument File leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-27506	NocoDB Vulnerable to Reflected Cross-Site Scripting on Reset Password Page	NocoDB is software for building databases as spreadsheets. The API endpoint related to the password reset function is vulnerable to Reflected Cross-Site-Scripting. The endpoint /api/v1/db/auth/password/reset/:tokenId is vulnerable to Reflected Cross-Site-Scripting. The flaw occurs due to implementation of the client-side template engine ejs, specifically on file resetPassword.ts where the template is using the insecure function “<%-“, which is rendered	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		by the function renderPasswordReset. This vulnerability is fixed in 0.258.0.		
CVE-2025-27610	Local File Inclusion in Rack::Static	Rack provides an interface for developing web applications in Ruby. Prior to versions 2.2.13, 3.0.14, and 3.1.12, `Rack::Static` can serve files under the specified `root:` even if `urls:` are provided, which may expose other files under the specified `root:` unexpectedly. The vulnerability occurs because `Rack::Static` does not properly sanitize user-supplied paths before serving files. Specifically, encoded path traversal sequences are not correctly validated, allowing attackers to access files outside the designated static file directory. By exploiting this vulnerability, an attacker can gain access to all files under the specified `root:` directory, provided they are able to determine then path of the file. Versions 2.2.13, 3.0.14, and 3.1.12 contain a patch for the issue. Other mitigations include removing usage of `Rack::Static`, or ensuring that `root:` points at a directory path which only contains files which should be accessed publicly. It is likely that a CDN or similar static file server would also mitigate the issue.	Patched by core rule	Y
CVE-2025-29789	OpenEMR Has Directory Traversal in Load Code feature	OpenEMR is a free and open source electronic health records and medical practice management application. Versions prior to 7.3.0 are vulnerable to Directory Traversal in the Load Code feature. Version 7.3.0 contains a patch for the issue.	Patched by core rule	Y
CVE-2025-29930	imFAQ allows local file inclusion in seo.php	imFAQ is an advanced questions and answers management system for ImpressCMS. Prior to 1.0.1, if the $_GET['seoOp'] parameter is manipulated to include malicious input (e.g., seoOp=php://filter/read=c	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		onvert.base64-encode/resource=/var/www/html/config.php), the application could allow an attacker to read sensitive files on the server (Local File Inclusion, LFI). The $_GET['seoOp'] and $_GET['seoArg'] parameters are directly used without sanitization or validation. This is partly mitigated by the fact that the ImpressCMS sensitive files are stored outside the web root, in a folder with a randomized name. The issue has been resolved in imFaq 1.0.1.		
CVE-2025-30567	WordPress WP01 <= 2.6.2 - Arbitrary File Download Vulnerability	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in wp01ru WP01 allows Path Traversal. This issue affects WP01: from n/a through 2.6.2.	Patched by core rule	Y
CVE-2025-30609	WordPress AppExperts – WordPress to Mobile App – WooCommerce to iOs and Android Apps - <= <= 1.4.3 Sensitive Data Exposure Vulnerability	Insertion of Sensitive Information Into Sent Data vulnerability in AppExperts AppExperts – WordPress to Mobile App – WooCommerce to iOs and Android Apps allows Retrieve Embedded Sensitive Data. This issue affects AppExperts – WordPress to Mobile App – WooCommerce to iOs and Android Apps: from n/a through 1.4.3.	Patched by core rule	Y

Server-side Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-12068	Server-Side Request Forgery in haotian-liu/llava	A Server-Side Request Forgery (SSRF) vulnerability was discovered in haotian-liu/llava, affecting version git c121f04. This vulnerability allows an attacker to make the server perform HTTP requests to arbitrary URLs, potentially accessing sensitive data that is only accessible from the server, such as AWS metadata credentials.	Patched by core rule	Y
CVE-2024-12376	Server Side Request Forgery in lm-sys/fastchat	A Server-Side Request Forgery (SSRF) vulnerability was identified in the lm-sys/fastchat web server, specifically in the affected version git 2c68a13. This vulnerability allows an attacker to access internal server resources and data that are otherwise inaccessible, such as AWS metadata credentials.	Patched by core rule	Y
CVE-2024-12392	Server-Side Request Forgery (SSRF) in binary-husky/gpt_academic	A Server-Side Request Forgery (SSRF) vulnerability exists in binary-husky/gpt_academic version git 310122f. The application has a functionality to download papers from arxiv.org, but the URL validation is incomplete. An attacker can exploit this vulnerability to make the application access any URL, including internal services, and read the response. This can be used to access data that are only accessible from the server, such as AWS metadata credentials, and can escalate local exploits to network-based attacks.	Patched by core rule	Y
CVE-2024-8952	SSRF in composiohq/composio	A Server-Side Request Forgery (SSRF) vulnerability exists in composiohq/composio version v0.4.2, specifically in the /api/actions/execute/WEBTOOL_SCRAPE_WEBSITE_CONTENT endpoint. This vulnerability allows an attacker to read files, access AWS metadata, and interact with local services on the system.	Patched by core rule	Y
CVE-2025-0184	Server-Side Request Forgery (SSRF) in langgenius/dify	A Server-Side Request Forgery (SSRF) vulnerability was identified in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		langgenius/dify version 0.10.2. The vulnerability occurs in the 'Create Knowledge' section when uploading DOCX files. If an external relationship exists in the DOCX file, the reltype value is requested as a URL using the 'requests' module instead of the 'ssrf_proxy', leading to an SSRF vulnerability. This issue was fixed in version 0.11.0.		
CVE-2025-1799	Zorlan SkyCaiji Tool.php previewAction server-side request forgery	A vulnerability, which was classified as critical, was found in Zorlan SkyCaiji 2.9. This affects the function previewAction of the file vendor/skycaiji/app/admin/controller/Tool.php. The manipulation of the argument data 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-2025-1848	zj1983 zz import_data_check server-side request forgery	A vulnerability classified as critical has been found in zj1983 zz up to 2024-8. Affected is an unknown function of the file /import_data_check. The manipulation of the argument url 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. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-1849	zj1983 zz import_data_todb server-side request forgery	A vulnerability classified as critical was found in zj1983 zz up to 2024-8. Affected by this vulnerability is an unknown functionality of the file /import_data_todb. The manipulation of the argument url leads to server-side request forgery. 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-2025-2109	WP Compress <= 6.30.15 - Unauthenticated Server-Side Request Forgery via init Function	The WP Compress – Instant Performance & Speed Optimization plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		including, 6.30.15 via the init() function. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query information from internal services.		
CVE-2025-22603	AutoGPT SSRF vulnerability	AutoGPT is a platform that allows users to create, deploy, and manage continuous artificial intelligence agents that automate complex workflows. Versions prior to autogpt-platform-beta-v0.4.2 contains a server-side request forgery (SSRF) vulnerability inside component (or block) `Send Web Request`. The root cause is that IPV6 address is not restricted or filtered, which allows attackers to perform a server side request forgery to visit an IPV6 service. autogpt-platform-beta-v0.4.2 fixes the issue.	Patched by core rule	Y
CVE-2025-25303	Server-Side Request Forgery (SSRF) in MouseTooltipTranslator	The MouseTooltipTranslator Chrome extension allows mouseover translation of any language at once. The MouseTooltipTranslator browser extension is vulnerable to SSRF attacks. The pdf.mjs script uses the URL parameter from the current URL as the file to download and display to the extension user. Because pdf.mjs is imported in viewer.html and viewer.html is accessible to all URLs, an attacker can force the user's browser to make a request to any arbitrary URL. After discussion with maintainer, patching this issue would require disabling a major feature of the extension in exchange for a low severity vulnerability. Decision to not patch issue.	Patched by core rule	Y
CVE-2025-27136	LocalS3 CreateBucketConfiguration Endpoint XML External Entity (XXE) Injection	LocalS3 is an Amazon S3 mock service for testing and local development. Prior to version 1.21, the LocalS3 service's bucket creation endpoint is vulnerable to XML External Entity (XXE) injection. When processing the CreateBucketConfiguration	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		XML document during bucket creation, the service's XML parser is configured to resolve external entities. This allows an attacker to declare an external entity that references an internal URL, which the server will then attempt to fetch when parsing the XML. The vulnerability specifically occurs in the location constraint processing, where the XML parser resolves external entities without proper validation or restrictions. When the external entity is resolved, the server makes an HTTP request to the specified URL and includes the response content in the parsed XML document. This vulnerability can be exploited to perform server-side request forgery (SSRF) attacks, allowing an attacker to make requests to internal services or resources that should not be accessible from external networks. The server will include the responses from these internal requests in the resulting bucket configuration, effectively leaking sensitive information. The attacker only needs to be able to send HTTP requests to the LocalS3 service to exploit this vulnerability.		
CVE-2025-27152	Possible SSRF and Credential Leakage via Absolute URL in axios Requests	axios is a promise based HTTP client for the browser and node.js. The issue occurs when passing absolute URLs rather than protocol-relative URLs to axios. Even if baseURL is set, axios sends the request to the specified absolute URL, potentially causing SSRF and credential leakage. This issue impacts both server-side and client-side usage of axios. This issue is fixed in 1.8.2.	Patched by core rule	Y
CVE-2025-27501	Server Side Request Forgery in Ziti Console	OpenZiti is a free and open source project focused on bringing zero trust to any application. An endpoint on the admin panel can be accessed without any form of authentication. This endpoint accepts a user-supplied URL parameter to connect to an OpenZiti	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Controller and performs a server-side request, resulting in a potential Server-Side Request Forgery (SSRF) vulnerability. The fixed version has moved the request to the external controller from the server side to the client side, thereby eliminating the identity of the node from being used to gain any additional permissions. This vulnerability is fixed in 3.7.1.		
CVE-2025-27600	FastGPT SSRF	FastGPT is a knowledge-based platform built on the LLMs. Since the web crawling plug-in does not perform intranet IP verification, an attacker can initiate an intranet IP request, causing the system to initiate a request through the intranet and potentially obtain some private data on the intranet. This issue is fixed in 4.9.0.	Patched by core rule	Y

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-11958	SQL Injection in run-llama/llama_index	A SQL injection vulnerability exists in the `duckdb_retriever` component of the run-llama/llama_index repository, specifically in the latest version. The vulnerability arises from the construction of SQL queries without using prepared statements, allowing an attacker to inject arbitrary SQL code. This can lead to remote code execution (RCE) by installing the shellfs extension and executing malicious commands.	Patched by core rule	Y
CVE-2024-12909	SQL Injection to RCE in run-llama/llama_index	A vulnerability in the FinanceChatLlamaPack of the run-llama/llama_index repository, versions up to v0.12.3, allows for SQL injection in the `run_sql_query` function of the `database_agent`. This vulnerability can be exploited by an attacker to inject arbitrary SQL queries, leading to remote code execution (RCE) through the use of PostgreSQL's large object functionality. The issue is fixed in version 0.3.0.	Patched by core rule	Y
CVE-2024-13844	Post SMTP <= 3.1.2 - Authenticated (Administrator+) SQL Injection via columns Parameter	The Post SMTP plugin for WordPress is vulnerable to generic SQL Injection via the 'columns' parameter in all versions up to, and including, 3.1.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2024-7764	SQL Injection in vanna-ai/vanna	Vanna-ai v0.6.2 is vulnerable to SQL Injection due to insufficient protection against injecting additional SQL commands from user requests. The vulnerability occurs when the `generate_sql` function calls `extract_sql` with the LLM response. An attacker can include a semi-colon	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		between a search data field and their own command, causing the `extract_sql` function to remove all LLM generated SQL and execute the attacker's command if it passes the `is_sql_valid` function. This allows the execution of user-defined SQL beyond the expected boundaries, notably the trained schema.		
CVE-2024-8055	Local File Read (LFI) by Prompt Injection via SnowFlake SQL in vanna-ai/vanna	Vanna v0.6.3 is vulnerable to SQL injection via Snowflake database in its file staging operations using the `PUT` and `COPY` commands. This vulnerability allows unauthenticated remote users to read arbitrary local files on the victim server, such as `/etc/passwd`, by exploiting the exposed SQL queries through a Python Flask API.	Patched by core rule	Y
CVE-2025-1702	Ultimate Member <= 2.10.0 - Unauthenticated SQL Injection via search Parameter	The Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to time-based SQL Injection via the 'search' parameter in all versions up to, and including, 2.10.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-1797	Hunan Zhonghe Baiyi Information Technology Baiyiyun Asset Management and Operations System anyUserBoundHouse.php sql injection	A vulnerability, which was classified as critical, has been found in Hunan Zhonghe Baiyi Information Technology Baiyiyun Asset Management and Operations System up to 20250217. Affected by this issue is some unknown functionality of the file /wuser/anyUserBoundHouse.php. The manipulation of the argument huid 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-2025-1808	Pixsoft E-Saphira Login Endpoint servlet sql	A vulnerability has been found in Pixsoft E-Saphira	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	1.7.24 and classified as critical. This vulnerability affects unknown code of the file /servlet?act=login&tipo=1 of the component Login Endpoint. The manipulation of the argument txtUsuario 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.		
CVE-2025-1809	Pixsoft Sol Login Endpoint servlet sql injection	A vulnerability was found in Pixsoft Sol up to 7.6.6c and classified as critical. This issue affects some unknown processing of the file /pix_projetos/servlet?act=login&submit=1&evento=0&pixrnd=0125021816444195731041 of the component Login Endpoint. The manipulation of the argument txtUsuario 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-2025-1811	AT Software Solutions ATSVD Login Endpoint login.aspx sql injection	A vulnerability was found in AT Software Solutions ATSVD up to 3.4.1. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /login.aspx of the component Login Endpoint. The manipulation of the argument txtUsuario leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.4.2 is able to address this issue. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-1812	zj1983 zz SuperZ.java GetUserOrg sql injection	A vulnerability classified as critical has been found in zj1983 zz up to 2024-08. Affected is the function GetUserOrg of the file com/futvan/z/framework/core/SuperZ.java. The manipulation of the argument userId leads to sql injection. It is possible to launch the attack remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-1820	zj1983 zz ZworkflowAction.java getOaWid sql injection	A vulnerability has been found in zj1983 zz up to 2024-8 and classified as critical. Affected by this vulnerability is the function getOaWid of the file src/main/java/com/futvan/z/system/zworkflow/ZworkflowAction.java. The manipulation of the argument tableId 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-2025-1821	zj1983 zz ZorgAction.java getUserOrgForUserId sql injection	A vulnerability was found in zj1983 zz up to 2024-8 and classified as critical. Affected by this issue is the function getUserOrgForUserId of the file src/main/java/com/futvan/z/system/zorg/ZorgAction.java. The manipulation of the argument userID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-1831	zj1983 zz ZorgAction.java GetDBUser sql injection	A vulnerability classified as critical has been found in zj1983 zz up to 2024-8. Affected is the function GetDBUser of the file src/main/java/com/futvan/z/system/zorg/ZorgAction.java. The manipulation of the argument user_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. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-1832	zj1983 zz ZroleAction.java getUserList sql injection	A vulnerability classified as critical was found in zj1983 zz up to 2024-8. Affected by this vulnerability is the function getUserList of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file src/main/java/com/futvan/z/system/zrole/ZroleAction.java. The manipulation of the argument roleid 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-2025-1840	ESAFENET CDG updateorg.jsp sql injection	A vulnerability was found in ESAFENET CDG 5.6.3.154.205. It has been rated as critical. Affected by this issue is some unknown functionality of the file /CDGServer3/workflowE/useractivate/updateorg.jsp. The manipulation of the argument flowId 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-2025-1841	ESAFENET CDG ClientSortLog.jsp sql injection	A vulnerability classified as critical has been found in ESAFENET CDG 5.6.3.154.205. This affects an unknown part of the file /CDGServer3/logManagement/ClientSortLog.jsp. The manipulation of the argument startDate/endDate 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-2025-1843	Mini-Tmall ProductMapper.java select sql injection	A vulnerability, which was classified as critical, has been found in Mini-Tmall up to 20250211. This issue affects the function select of the file com/xq/tmall/dao/ProductMapper.java. The manipulation of the argument orderBy 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-2025-1844	ESAFENET CDG backupLogDetail.jsp sql injection	A vulnerability, which was classified as critical, was found in ESAFENET CDG 5.6.3.154.205_20250114. Affected is an unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		function of the file /CDGServer3/logManagement/backupLogDetail.jsp. The manipulation of the argument logTaskId leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-1850	Codezips College Management System university.php sql injection	A vulnerability, which was classified as critical, has been found in Codezips College Management System 1.0. Affected by this issue is some unknown functionality of the file /university.php. The manipulation of the argument book_name leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1854	Codezips Gym Management System del_member.php sql injection	A vulnerability was found in Codezips Gym Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /dashboard/admin/del_member.php. The manipulation of the argument name leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1855	PHPGurukul Online Shopping Portal product-details.php sql injection	A vulnerability was found in PHPGurukul Online Shopping Portal 2.1. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /product-details.php. The manipulation of the argument quality/price/value/name/summary/review 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-2025-1856	Codezips Gym Management System gen_invoice.php sql injection	A vulnerability was found in Codezips Gym Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /dashboard/admin/gen_invoice.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-2025-1857	PHPGurukul Nipah Virus Testing Management System check_availability.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Nipah Virus Testing Management System 1.0. This affects an unknown part of the file /check_availability.php. The manipulation of the argument employeeid 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-2025-1858	Codezips Online Shopping Website success.php sql injection	A vulnerability classified as critical was found in Codezips Online Shopping Website 1.0. This vulnerability affects unknown code of the file /success.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-2025-1859	PHPGurukul News Portal login.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul News Portal 4.1. This issue affects some unknown processing of the file /login.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-2025-1894	PHPGurukul Restaurant Table Booking System search-result.php sql injection	A vulnerability was found in PHPGurukul Restaurant Table Booking System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /search-result.php. The manipulation of the argument searchdata 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-2025-1900	PHPGurukul Restaurant Table Booking System add-table.php sql injection	A vulnerability was found in PHPGurukul Restaurant Table Booking System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /add-table.php.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The manipulation of the argument tableno leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-1901	PHPGurukul Restaurant Table Booking System check_availability.php sql injection	A vulnerability was found in PHPGurukul Restaurant Table Booking System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/check_availability.php. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1902	PHPGurukul Student Record System password-recovery.php sql injection	A vulnerability was found in PHPGurukul Student Record System 3.2. It has been declared as critical. This vulnerability affects unknown code of the file /password-recovery.php. The manipulation of the argument emailid 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-2025-1903	Codezips Online Shopping Website cart_add.php sql injection	A vulnerability was found in Codezips Online Shopping Website 1.0. It has been rated as critical. This issue affects some unknown processing of the file /cart_add.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-2025-1906	PHPGurukul Restaurant Table Booking System profile.php sql injection	A vulnerability has been found in PHPGurukul Restaurant Table Booking System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/profile.php. The manipulation of the argument mobilenumber leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-1952	PHPGurukul Restaurant Table Booking System password-recovery.php	A vulnerability, which was classified as critical, was found in PHPGurukul	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	sql injection	Restaurant Table Booking System 1.0. Affected is an unknown function of the file /admin/password-recovery.php. The manipulation of the argument username/mobileno 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-2025-1954	PHPGurukul Human Metapneumovirus Testing Management System login.php sql injection	A vulnerability was found in PHPGurukul Human Metapneumovirus Testing Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /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-2025-1958	aaluoxiang oa_system address-mapper.xml sql injection	A vulnerability, which was classified as critical, has been found in aaluoxiang oa_system 1.0. This issue affects some unknown processing of the file src/main/resources/mappers/address-mapper.xml. The manipulation of the argument outtype 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-2025-1959	Codezips Gym Management System change_s_pwd.php sql injection	A vulnerability, which was classified as critical, was found in Codezips Gym Management System 1.0. Affected is an unknown function of the file /change_s_pwd.php. The manipulation of the argument login_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-2025-1961	SourceCodester Best Church Management Software web_crud.php sql injection	A vulnerability has been found in SourceCodester Best Church Management Software 1.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/app/web_crud.php. The manipulation of the argument encryption leads	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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-2025-1962	projectworlds Online Hotel Booking addroom.php sql injection	A vulnerability was found in projectworlds Online Hotel Booking 1.0. It has been classified as critical. This affects an unknown part of the file /admin/addroom.php. The manipulation of the argument roomname 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-2025-1963	projectworlds Online Hotel Booking reservation.php sql injection	A vulnerability was found in projectworlds Online Hotel Booking 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /reservation.php. The manipulation of the argument checkin 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-2025-1964	projectworlds Online Hotel Booking booknow.php sql injection	A vulnerability was found in projectworlds Online Hotel Booking 1.0. It has been rated as critical. This issue affects some unknown processing of the file /booknow.php?roomname=Duplex. The manipulation of the argument checkin 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-2025-1965	projectworlds Online Hotel Booking login.php sql injection	A vulnerability classified as critical has been found in projectworlds Online Hotel Booking 1.0. Affected is an unknown function of the file /admin/login.php. The manipulation of the argument emailusername 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-2025-1966	PHPGurukul Pre-School Enrollment System	A vulnerability classified as critical was found in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	index.php sql injection	PHPGurukul Pre-School Enrollment System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/index.php. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-2030	Seeyon Zhiyuan Interconnect FE Collaborative Office Platform addUser.jsp sql injection	A vulnerability was found in Seeyon Zhiyuan Interconnect FE Collaborative Office Platform up to 20250224. It has been rated as critical. Affected by this issue is some unknown functionality of the file /security/addUser.jsp. The manipulation of the argument groupId leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2033	code-projects Blood Bank Management System view_donor.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Blood Bank Management System 1.0. Affected is an unknown function of the file /user_dashboard/view_donor.php. The manipulation of the argument donor_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-2025-2034	PHPGurukul Pre-School Enrollment System edit-class.php sql injection	A vulnerability has been found in PHPGurukul Pre-School Enrollment System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/edit-class.php?cid=1. The manipulation of the argument classname/capacity 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-2025-2037	code-projects Blood Bank Management System delete_requester.php sql injection	A vulnerability was found in code-projects Blood Bank Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/user_dashboard/delete_requester.php. The manipulation of the argument requester_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-2039	code-projects Blood Bank Management System delete_members.php sql injection	A vulnerability classified as critical has been found in code-projects Blood Bank Management System 1.0. Affected is an unknown function of the file /admin/delete_members.php. The manipulation of the argument member_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-2025-2044	code-projects Blood Bank Management System delete_bloodGroup.php sql injection	A vulnerability was found in code-projects Blood Bank Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/delete_bloodGroup.php. The manipulation of the argument blood_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-2025-2046	SourceCodester Best Employee Management System print1.php sql injection	A vulnerability was found in SourceCodester Best Employee Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/print1.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-2025-2050	PHPGurukul User Registration & Login and User Management System login.php sql injection	A vulnerability classified as critical was found in PHPGurukul User Registration & Login and User Management System 3.3. Affected by this vulnerability is an unknown functionality of the file /login.php. The manipulation of the argument email leads to sql injection. The attack can 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-2025-2051	PHPGurukul Apartment Visitors Management System search-visitor.php sql injection	A vulnerability has been found in PHPGurukul Apartment Visitors Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /search-visitor.php. The manipulation of the argument searchdata leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-2052	PHPGurukul Apartment Visitors Management System forgot-password.php sql injection	A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /forgot-password.php. The manipulation of the argument contactno 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-2025-2053	PHPGurukul Apartment Visitors Management System visitor-detail.php sql injection	A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /visitor-detail.php. The manipulation of the argument editid 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-2025-2054	code-projects Blood Bank Management System edit_state.php sql injection	A vulnerability was found in code-projects Blood Bank Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/edit_state.php. The manipulation of the argument state_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-2025-2057	PHPGurukul Emergency Ambulance Hiring Portal about-us.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Emergency Ambulance Hiring Portal 1.0. Affected is an unknown function of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file /admin/about-us.php. The manipulation of the argument pagedes 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-2025-2058	PHPGurukul Emergency Ambulance Hiring Portal search.php sql injection	A vulnerability has been found in PHPGurukul Emergency Ambulance Hiring Portal 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/search.php. The manipulation of the argument searchdata 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-2025-2059	PHPGurukul Emergency Ambulance Hiring Portal booking-details.php sql injection	A vulnerability was found in PHPGurukul Emergency Ambulance Hiring Portal 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/booking-details.php. The manipulation of the argument ambulanceregnum 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-2025-2060	PHPGurukul Emergency Ambulance Hiring Portal admin-profile.php sql injection	A vulnerability was found in PHPGurukul Emergency Ambulance Hiring Portal 1.0. It has been classified as critical. This affects an unknown part of the file /admin/admin-profile.php. The manipulation of the argument contactnumber 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-2025-2062	projectworlds Life Insurance Management System clientStatus.php sql injection	A vulnerability classified as critical has been found in projectworlds Life Insurance Management System 1.0. Affected is an unknown function of the file /clientStatus.php. The manipulation of the argument client_id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		may be used.		
CVE-2025-2063	projectworlds Life Insurance Management System deleteNominee.php sql injection	A vulnerability classified as critical was found in projectworlds Life Insurance Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /deleteNominee.php. The manipulation of the argument nominee_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-2025-2064	projectworlds Life Insurance Management System deletePayment.php sql injection	A vulnerability, which was classified as critical, has been found in projectworlds Life Insurance Management System 1.0. Affected by this issue is some unknown functionality of the file /deletePayment.php. The manipulation of the argument recipt_no 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-2025-2065	projectworlds Life Insurance Management System editAgent.php sql injection	A vulnerability, which was classified as critical, was found in projectworlds Life Insurance Management System 1.0. This affects an unknown part of the file /editAgent.php. The manipulation of the argument agent_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-2025-2066	projectworlds Life Insurance Management System updateAgent.php sql injection	A vulnerability has been found in projectworlds Life Insurance Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /updateAgent.php. The manipulation of the argument agent_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-2025-2067	projectworlds Life Insurance Management System search.php sql injection	A vulnerability was found in projectworlds Life Insurance Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /search.php. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument key leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-2088	PHPGurukul Pre-School Enrollment System profile.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Pre-School Enrollment System up to 1.0. Affected is an unknown function of the file /admin/profile.php. The manipulation of the argument fullname/emailid/mobileNumber 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-2025-2106	Arielbrailovsky-Viralad <= 1.0.8 - Unauthenticated SQL Injection	The ArielBrailovsky-ViralAd plugin for WordPress is vulnerable to SQL Injection via the 'text' and 'id' parameters of the limpia() function in all versions up to, and including, 1.0.8 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This only appears to be exploitable on very old versions of WordPress.	Patched by core rule	Y
CVE-2025-2107	Arielbrailovsky-Viralad <= 1.0.8 - Unauthenticated SQL Injection	The ArielBrailovsky-ViralAd plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter of the printResultAndDie() function in all versions up to, and including, 1.0.8 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This only appears to be exploitable on very old versions of WordPress.	Patched by core rule	Y
CVE-2025-2112	user-xiangpeng yaoqishan	A vulnerability was found in user-xiangpeng yaoqishan	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	MediaInfoService.java getMediaLisByFilter sql injection	up to a47fec4a31cbd13698c592dfdc938c8824dd25e4. It has been declared as critical. Affected by this vulnerability is the function getMediaLisByFilter of the file cn/javaex/yaoqishan/service/media_info/MediaInfoService.java. The manipulation of the argument typeId leads to sql injection. The attack can be launched 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. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-2113	AT Software Solutions ATSVD Esqueceu a senha sql injection	A vulnerability was found in AT Software Solutions ATSVD up to 3.4.1. It has been rated as critical. Affected by this issue is some unknown functionality of the component Esqueceu a senha. The manipulation of the argument txtCPF leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.4.2 is able to address this issue. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-2117	Beijing Founder Electronics Founder Enjoys All-Media Acquisition and Editing System reportCenter.do electricDocList sql injection	A vulnerability was found in Beijing Founder Electronics Founder Enjoys All-Media Acquisition and Editing System 3.0 and classified as critical. Affected by this issue is the function electricDocList of the file /newsedit/report/reportCenter.do. The manipulation of the argument fvID/catID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2118	Quantico Tecnologia PRMV Login Endpoint login.php sql injection	A vulnerability was found in Quantico Tecnologia PRMV 6.48. It has been classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		critical. This affects an unknown part of the file /admin/login.php of the component Login Endpoint. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-2132	ftcms Search ajax_all_lists sql injection	A vulnerability classified as critical has been found in ftcms 2.1. Affected is an unknown function of the file /admin/index.php/web/ajax_all_lists of the component Search. The manipulation of the argument name leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-21619	GLPI allows SQL injection through the rules configuration	GLPI is a free asset and IT management software package. An administrator user can perfom a SQL injection through the rules configuration forms. This vulnerability is fixed in 10.0.18.	Patched by core rule	Y
CVE-2025-2186	Recover WooCommerce Cart Abandonment, Newsletter, Email Marketing, Marketing Automation By FunnelKit <= 3.5.1 - Unauthenticated SQL Injection via 'automationId'	The Recover WooCommerce Cart Abandonment, Newsletter, Email Marketing, Marketing Automation By FunnelKit plugin for WordPress is vulnerable to SQL Injection via the 'automationId' parameter in all versions up to, and including, 3.5.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-2217	zzskzy Warehouse Refinement Management System getAdyData.ashx ProcessRequest sql injection	A vulnerability, which was classified as critical, was found in zzskzy Warehouse Refinement Management System 1.3. This affects the function ProcessRequest of the file /getAdyData.ashx. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument showid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-22212	Extension - tassos.gr - SQL injection in ConvertForms component version 1.0.0-1.0.0 - 4.4.9 for Joomla	A SQL injection vulnerability in the ConvertForms component versions 1.0.0-1.0.0 - 4.4.9 for Joomla allows authenticated attackers (administrator) to execute arbitrary SQL commands in the submission management area in backend.	Patched by core rule	Y
CVE-2025-2358	Shenzhen Mingyuan Cloud Technology Mingyuan Real Estate ERP System HTTP Header Service.asmx sql injection	A vulnerability was found in Shenzhen Mingyuan Cloud Technology Mingyuan Real Estate ERP System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /Kfxt/Service.asmx of the component HTTP Header Handler. The manipulation of the argument X-Forwarded-For 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-2025-2362	PHPGurukul Pre-School Enrollment System contact-us.php sql injection	A vulnerability was found in PHPGurukul Pre-School Enrollment System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/contact-us.php. The manipulation of the argument mobnum 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-2025-2372	PHPGurukul Human Metapneumovirus Testing Management System Password Recovery Page password-recovery.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Human Metapneumovirus Testing Management System 1.0. This affects an unknown part of the file /password-recovery.php of the component Password Recovery Page. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-2373	PHPGurukul Human Metapneumovirus Testing Management System check_availability.php sql injection	A vulnerability classified as critical was found in PHPGurukul Human Metapneumovirus Testing Management System 1.0. This vulnerability affects unknown code of the file /check_availability.php. The manipulation of the argument mobnumber/employeeid 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-2025-2374	PHPGurukul Human Metapneumovirus Testing Management System profile.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Human Metapneumovirus Testing Management System 1.0. This issue affects some unknown processing of the file /profile.php. The manipulation of the argument aid/adminname/mobilenumber/email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-2378	PHPGurukul Medical Card Generation System download-medical-cards.php sql injection	A vulnerability was found in PHPGurukul Medical Card Generation System 1.0. It has been classified as critical. This affects an unknown part of the file /download-medical-cards.php. The manipulation of the argument searchdata 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-2025-2379	PHPGurukul Apartment Visitors Management System create-pass.php sql injection	A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /create-pass.php. The manipulation of the argument visname leads to sql injection. The attack can 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-2025-2380	PHPGurukul Apartment Visitors Management System admin-profile.php sql injection	A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin-profile.php. The manipulation of the argument mobilenumber 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-2025-2381	PHPGurukul Curfew e-Pass Management System search-pass.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Curfew e-Pass Management System 1.0. Affected is an unknown function of the file /admin/search-pass.php. The manipulation of the argument searchdata 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-2025-2382	PHPGurukul Online Banquet Booking System booking-search.php sql injection	A vulnerability classified as critical was found in PHPGurukul Online Banquet Booking System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/booking-search.php. The manipulation of the argument searchdata 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-2025-2383	PHPGurukul Doctor Appointment Management System search.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Doctor Appointment Management System 1.0. Affected by this issue is some unknown functionality of the file /doctor/search.php. The manipulation of the argument searchdata 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-2025-2384	code-projects Real Estate Property Management System Parameter	A vulnerability, which was classified as critical, was found in code-projects Real	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	InsertCustomer.php sql injection	Estate Property Management System 1.0. This affects an unknown part of the file /InsertCustomer.php of the component Parameter Handler. The manipulation of the argument txtName/txtAddress/cmbCity/txtEmail/cmbGender/txtBirthDate/txtUserName2/txtPassword2 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-2025-2385	code-projects Modern Bag login.php sql injection	A vulnerability has been found in code-projects Modern Bag 1.0 and classified as critical. This vulnerability affects unknown code of the file /login.php. The manipulation of the argument userEmail/userPassword 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-2025-2386	PHPGurukul Local Services Search Engine Management System serviceman-search.php sql injection	A vulnerability was found in PHPGurukul Local Services Search Engine Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /serviceman-search.php. The manipulation of the argument location 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-2025-2387	SourceCodester Online Food Ordering System ajax.php sql injection	A vulnerability was found in SourceCodester Online Food Ordering System 2.0. It has been classified as critical. Affected is an unknown function of the file /admin/ajax.php?action=add_to_cart. 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-2025-2389	code-projects Blood Bank Management System add_city.php sql injection	A vulnerability was found in code-projects Blood Bank 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 /admin/add_city.php. The manipulation leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-2390	code-projects Blood Bank Management System add_donor.php sql injection	A vulnerability classified as critical has been found in code-projects Blood Bank Management System 1.0. This affects an unknown part of the file /user_dashboard/add_donor.php. The manipulation 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-2025-2391	code-projects Blood Bank Management System Admin Login Page admin_login.php sql injection	A vulnerability classified as critical was found in code-projects Blood Bank Management System 1.0. This vulnerability affects unknown code of the file /admin/admin_login.php of the component Admin Login Page. The manipulation leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-2392	code-projects Online Class and Exam Scheduling System activate.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Online Class and Exam Scheduling System 1.0. This issue affects some unknown processing of the file /pages/activate.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-2025-2393	code-projects Online Class and Exam Scheduling System salut_del.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Online Class and Exam Scheduling System 1.0. Affected is an unknown function of the file /pages/salut_del.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-2025-2419	code-projects Real Estate Property Management	A vulnerability classified as critical has been found in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System InsertFeedback.php sql injection	code-projects Real Estate Property Management System 1.0. Affected is an unknown function of the file /InsertFeedback.php. The manipulation of the argument txtName/txtEmail/txtMobile /txtFeedback 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-2025-2471	PHPGurukul Boat Booking System boat-details.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Boat Booking System 1.0. Affected is an unknown function of the file /boat-details.php. The manipulation of the argument bid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-2472	PHPGurukul Apartment Visitors Management System Sign In index.php sql injection	A vulnerability has been found in PHPGurukul Apartment Visitors Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /index.php of the component Sign In. 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-2025-2473	PHPGurukul Company Visitor Management System Sign In index.php sql injection	A vulnerability was found in PHPGurukul Company Visitor Management System 2.0 and classified as critical. Affected by this issue is some unknown functionality of the file /index.php of the component Sign In. 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-2025-2478	Code Clone <= 0.9 - Authenticated (Administrator+) SQL Injection via snippetId Parameter	The Code Clone plugin for WordPress is vulnerable to time-based SQL Injection via the 'snippetId' parameter in all versions up to, and including, 0.9 due to insufficient escaping on the user supplied parameter and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.		
CVE-2025-24799	GLPI allows unauthenticated SQL injection through the inventory endpoint	GLPI is a free asset and IT management software package. An unauthenticated user can perform a SQL injection through the inventory endpoint. This vulnerability is fixed in 10.0.18.	Patched by core rule	Y
CVE-2025-2511	AHAthat Plugin <= 1.6 - Authenticated (Administrator+) SQL Injection via id Parameter	The AHAthat Plugin plugin for WordPress is vulnerable to time-based SQL Injection via the 'id' parameter in all versions up to, and including, 1.6 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-25112	WordPress Social Links plugin <= 1.2 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in NotFound Social Links allows Blind SQL Injection. This issue affects Social Links: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-25150	Directory Listings WordPress uListing plugin <= 2.1.6 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Stylemix uListing allows Blind SQL Injection. This issue affects uListing: from n/a through 2.1.6.	Patched by core rule	Y
CVE-2025-2587	Jinher OA C6 IncentivePlanFulfillAppprove.aspx sql injection	A vulnerability, which was classified as critical, was found in Jinher OA C6 1.0. This affects an unknown part of the file IncentivePlanFulfillAppprove.aspx. The manipulation of the argument httpOID leads to sql injection. It is possible to initiate the attack remotely. The exploit has	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		been disclosed to the public and may be used.		
CVE-2025-2593	FastCMS list sql injection	A vulnerability has been found in FastCMS up to 0.1.5 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /api/client/article/list. The manipulation of the argument orderBy 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-2025-2601	SourceCodester Kortex Lite Advocate Office Management System activate_reg.php sql injection	A vulnerability, which was classified as critical, was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. This affects an unknown part of the file activate_reg.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-2025-2602	SourceCodester Kortex Lite Advocate Office Management System deactivate_reg.php sql injection	A vulnerability has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file deactivate_reg.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-2025-2603	SourceCodester Kortex Lite Advocate Office Management System deactivate.php sql injection	A vulnerability was found in SourceCodester Kortex Lite Advocate Office Management System 1.0 and classified as critical. This issue affects some unknown processing of the file deactivate.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-2025-2604	SourceCodester Kortex Lite Advocate Office Management System edit_act.php sql injection	A vulnerability was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. It has been classified as critical. Affected is an unknown function of the file edit_act.php. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-2608	PHPGurukul Banquet Booking System view-user-queries.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Banquet Booking System 1.2. This affects an unknown part of the file /admin/view-user-queries.php. The manipulation of the argument viewid 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-2025-2624	westboy CicadasCMS save sql injection	A vulnerability was found in westboy CicadasCMS 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /system/cms/content/save. The manipulation of the argument content/fujian/laiyuan 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-2025-2625	westboy CicadasCMS page sql injection	A vulnerability classified as critical has been found in westboy CicadasCMS 1.0. This affects an unknown part of the file /system/cms/content/page. The manipulation of the argument orderField/orderDirection 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-2025-2626	SourceCodester Kortex Lite Advocate Office Management System edit_case.php sql injection	A vulnerability classified as critical was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. This vulnerability affects unknown code of the file edit_case.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-2025-2627	PHPGurukul Art Gallery	A vulnerability, which was	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Management System contactus.php sql injection	classified as critical, has been found in PHPGurukul Art Gallery Management System 1.0. This issue affects some unknown processing of the file /admin/contactus.php. The manipulation of the argument pagetitle leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	rule	
CVE-2025-2628	PHPGurukul Art Gallery Management System art-enquiry.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Art Gallery Management System 1.1. Affected is an unknown function of the file /art-enquiry.php. The manipulation of the argument eid 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-2025-2640	PHPGurukul Doctor Appointment Management System appointment-bwdates-reports-details.php sql injection	A vulnerability was found in PHPGurukul Doctor Appointment Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /doctor/appointment-bwdates-reports-details.php. The manipulation of the argument fromdate/todate 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-2025-2641	PHPGurukul Art Gallery Management System edit-artist-detail.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Art Gallery Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/edit-artist-detail.php?editid=1. The manipulation of the argument Name leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-2642	PHPGurukul Art Gallery Management System edit-art-product-detail.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Art Gallery Management System 1.0. This affects an unknown part of the file /admin/edit-art-product-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		detail.php?editid=2. The manipulation of the argument editide/sprice/description 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-2025-2643	PHPGurukul Art Gallery Management System edit-art-type-detail.php sql injection	A vulnerability has been found in PHPGurukul Art Gallery Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/edit-art-type-detail.php?editid=1. The manipulation of the argument arttype 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-2025-2644	PHPGurukul Art Gallery Management System add-art-product.php sql injection	A vulnerability was found in PHPGurukul Art Gallery Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/add-art-product.php. The manipulation of the argument arttype 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-2025-2646	PHPGurukul Art Gallery Management System admin-profile.php sql injection	A vulnerability was found in PHPGurukul Art Gallery Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/admin-profile.php. The manipulation of the argument contactnumber 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-2025-2647	PHPGurukul Art Gallery Management System search.php sql injection	A vulnerability was found in PHPGurukul Art Gallery Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /search.php. The manipulation of the argument Search leads to sql injection. The attack may be launched remotely. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit has been disclosed to the public and may be used.		
CVE-2025-2648	PHPGurukul Art Gallery Management System view-enquiry-detail.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Art Gallery Management System 1.0. This affects an unknown part of the file /admin/view-enquiry-detail.php. The manipulation of the argument viewid 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-2025-2649	PHPGurukul Doctor Appointment Management System check-appointment.php sql injection	A vulnerability classified as critical was found in PHPGurukul Doctor Appointment Management System 1.0. This vulnerability affects unknown code of the file /check-appointment.php. The manipulation of the argument searchdata leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-26535	WordPress Bitcoin / AltCoin Payment Gateway for WooCommerce & Multivendor store / shop plugin <= 1.7.6 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in NotFound Bitcoin / AltCoin Payment Gateway for WooCommerce allows Blind SQL Injection. This issue affects Bitcoin / AltCoin Payment Gateway for WooCommerce: from n/a through 1.7.6.	Patched by core rule	Y
CVE-2025-2654	SourceCodester AC Repair and Services System manage_service.php sql injection	A vulnerability was found in SourceCodester AC Repair and Services System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/services/manage_service.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-2025-2655	SourceCodester AC Repair and Services System Users.php save_users sql injection	A vulnerability was found in SourceCodester AC Repair and Services System 1.0. It has been declared as critical. This vulnerability affects the function save_users of the file /classes/Users.php. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.		
CVE-2025-2656	PHPGurukul Zoo Management System login.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Zoo Management System 2.1. Affected is an unknown function of the file /admin/login.php. The manipulation of the argument Username 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-2025-2657	projectworlds Apartment Visitors Management System front.php sql injection	A vulnerability classified as critical was found in projectworlds Apartment Visitors Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /front.php. The manipulation of the argument rid 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-2025-2658	PHPGurukul Online Security Guards Hiring System search-request.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Online Security Guards Hiring System 1.0. Affected by this issue is some unknown functionality of the file /search-request.php. The manipulation of the argument searchdata 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-2025-2659	Project Worlds Online Time Table Generator index.php sql injection	A vulnerability, which was classified as critical, was found in Project Worlds Online Time Table Generator 1.0. This affects an unknown part of the file /student/index.php. The manipulation of the argument e 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-2025-2660	Project Worlds Online	A vulnerability has been	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Time Table Generator index.php sql injection	found in Project Worlds Online Time Table Generator 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/index.php. The manipulation of the argument e leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	rule	
CVE-2025-2661	Project Worlds Online Time Table Generator index.php sql injection	A vulnerability was found in Project Worlds Online Time Table Generator 1.0 and classified as critical. This issue affects some unknown processing of the file /staff/index.php. The manipulation of the argument e 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-2025-2662	Project Worlds Online Time Table Generator studentdashboard.php sql injection	A vulnerability was found in Project Worlds Online Time Table Generator 1.0. It has been classified as critical. Affected is an unknown function of the file student/studentdashboard.php. The manipulation of the argument course 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-2025-2663	PHPGurukul Bank Locker Management System search-locker-details.php sql injection	A vulnerability has been found in PHPGurukul Bank Locker Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /search-locker-details.php. The manipulation of the argument searchinput 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-2025-2664	CodeZips Hospital Management System suadpeted.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 /suadpeted.php. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit has been disclosed to the public and may be used.		
CVE-2025-2665	PHPGurukul Online Security Guards Hiring System bwdates-reports-details.php sql injection	A vulnerability was found in PHPGurukul Online Security Guards Hiring System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/bwdates-reports-details.php. The manipulation of the argument fromdate/todate 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-2025-2672	code-projects Payroll Management System add_deductions.php sql injection	A vulnerability was found in code-projects Payroll Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /add_deductions.php. The manipulation of the argument bir 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-2025-2674	PHPGurukul Bank Locker Management System aboutus.php sql injection	A vulnerability classified as critical was found in PHPGurukul Bank Locker Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /aboutus.php. The manipulation of the argument pagetitle 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-2025-2675	PHPGurukul Bank Locker Management System add-lockertype.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Bank Locker Management System 1.0. Affected by this issue is some unknown functionality of the file /add-lockertype.php. The manipulation of the argument lockerprice 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-2025-2676	PHPGurukul Bank Locker Management System add-subadmin.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Bank Locker Management System 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 /add-subadmin.php. The manipulation of the argument sadminusername 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-2025-2677	PHPGurukul Bank Locker Management System changeidproof.php sql injection	A vulnerability has been found in PHPGurukul Bank Locker Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /changeidproof.php. The manipulation of the argument editid 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-2025-2678	PHPGurukul Bank Locker Management System changeimage1.php sql injection	A vulnerability was found in PHPGurukul Bank Locker Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /changeimage1.php. The manipulation of the argument editid 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-2025-2679	PHPGurukul Bank Locker Management System contact-us.php sql injection	A vulnerability was found in PHPGurukul Bank Locker Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /contact-us.php. The manipulation of the argument pagetitle 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-2025-2680	PHPGurukul Bank Locker Management System edit-assign-locker.php sql injection	A vulnerability was found in PHPGurukul Bank Locker Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /edit-assign-locker.php?ltid=1. The manipulation of the argument mobilenumber 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-2025-2681	PHPGurukul Bank Locker	A vulnerability was found in	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Management System edit-locker.php sql injection	PHPGurukul Bank Locker Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /edit-locker.php?ltid=6. The manipulation of the argument lockersize leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	rule	
CVE-2025-2682	PHPGurukul Bank Locker Management System edit-subadmin.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Bank Locker Management System 1.0. This affects an unknown part of the file /edit-subadmin.php?said=3. The manipulation of the argument mobilenumber 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-2025-2683	PHPGurukul Bank Locker Management System profile.php sql injection	A vulnerability classified as critical was found in PHPGurukul Bank Locker Management System 1.0. This vulnerability affects unknown code of the file /profile.php. The manipulation of the argument mobilenumber 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-2025-2684	PHPGurukul Bank Locker Management System search-report-details.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Bank Locker Management System 1.0. This issue affects some unknown processing of the file /search-report-details.php. The manipulation of the argument searchinput 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-2025-26875	WordPress Multiple Shipping And Billing Address For Woocommerce Plugin <= 1.3 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in silverplugins217 Multiple Shipping And Billing Address For Woocommerce allows SQL Injection. This issue affects Multiple Shipping	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		And Billing Address For Woocommerce: from n/a through 1.3.		
CVE-2025-26886	WordPress PublishPress Authors plugin <= 4.7.3 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in PublishPress PublishPress Authors allows SQL Injection. This issue affects PublishPress Authors: from n/a through 4.7.3.	Patched by core rule	Y
CVE-2025-26976	WordPress PrivateContent plugin <= 8.11.4 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Aldo Latino PrivateContent. This issue affects PrivateContent: from n/a through 8.11.4.	Patched by core rule	Y
CVE-2025-26978	WordPress FS Poster plugin <= 6.5.8 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in NotFound FS Poster. This issue affects FS Poster: from n/a through 6.5.8.	Patched by core rule	Y
CVE-2025-26988	WordPress SMS Alert Order Notifications – WooCommerce plugin <= 3.7.8 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Cozy Vision SMS Alert Order Notifications – WooCommerce allows SQL Injection. This issue affects SMS Alert Order Notifications – WooCommerce: from n/a through 3.7.8.	Patched by core rule	Y
CVE-2025-27018	Apache Airflow MySQL Provider: SQL injection in MySQL provider core function	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Airflow MySQL Provider. When user triggered a DAG with dump_sql or load_sql functions they could pass a table parameter from a UI, that could cause SQL injection by running SQL that was not intended. It could lead to data corruption, modification and others. This issue affects Apache Airflow MySQL Provider: before 6.2.0. Users are recommended to upgrade to version 6.2.0, which fixes the issue.	Patched by core rule	Y
CVE-2025-27263	WordPress Doctor	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Appointment Booking Plugin <= 1.0.0 - SQL Injection vulnerability	Special Elements used in an SQL Command ('SQL Injection') vulnerability in NotFound Doctor Appointment Booking allows SQL Injection. This issue affects Doctor Appointment Booking: from n/a through 1.0.0.	rule	
CVE-2025-27268	WordPress Small Package Quotes – Worldwide Express Edition Plugin <= 5.2.18 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in enituretechnology Small Package Quotes – Worldwide Express Edition allows SQL Injection. This issue affects Small Package Quotes – Worldwide Express Edition: from n/a through 5.2.18.	Patched by core rule	Y
CVE-2025-27281	WordPress All In Menu Plugin <= 1.1.5 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in cookforweb All In Menu allows Blind SQL Injection. This issue affects All In Menu: from n/a through 1.1.5.	Patched by core rule	Y
CVE-2025-2734	PHPGurukul Old Age Home Management System aboutus.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Old Age Home Management System 1.0. Affected is an unknown function of the file /admin/aboutus.php. The manipulation of the argument pagetitle 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-2025-2735	PHPGurukul Old Age Home Management System add-services.php sql injection	A vulnerability has been found in PHPGurukul Old Age Home Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/add-services.php. The manipulation of the argument sertitle 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-2025-2736	PHPGurukul Old Age Home Management System bwdates-report-details.php sql injection	A vulnerability was found in PHPGurukul Old Age Home Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/bwdates-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		report-details.php. The manipulation of the argument fromdate leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.		
CVE-2025-2737	PHPGurukul Old Age Home Management System contactus.php sql injection	A vulnerability was found in PHPGurukul Old Age Home Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/contactus.php. The manipulation of the argument pagetitle 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-2025-2738	PHPGurukul Old Age Home Management System manage-scdetails.php sql injection	A vulnerability was found in PHPGurukul Old Age Home Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/manage-scdetails.php. The manipulation of the argument namesc 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-2025-2739	PHPGurukul Old Age Home Management System manage-services.php sql injection	A vulnerability was found in PHPGurukul Old Age Home Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/manage-services.php. The manipulation of the argument sertitle 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-2025-2740	PHPGurukul Old Age Home Management System eligibility.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Old Age Home Management System 1.0. Affected is an unknown function of the file /admin/eligibility.php. The manipulation of the argument pagetitle 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-2025-27617	Pimcore Vulnerable to SQL Injection in getRelationFilterCondition	Pimcore is an open source data and experience management platform. Prior to version 11.5.4, authenticated users can craft a filter string used to cause a SQL injection. Version 11.5.4 fixes the issue.	Patched by core rule	Y
CVE-2025-28904	WordPress Web Directory Free plugin <= 1.7.6 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Shamalli Web Directory Free allows Blind SQL Injection. This issue affects Web Directory Free: from n/a through 1.7.6.	Patched by core rule	Y
CVE-2025-29980	Blind SQL Injection vulnerability in eTRAKiT.Net	A SQL injection issue has been discovered in eTRAKiT.net release 3.2.1.77. Due to improper input validation, a remote unauthenticated attacker can run arbitrary commands as the current MS SQL server account. It is recommended that the CRM feature is turned off while on eTRAKiT.net release 3.2.1.77. eTRAKiT.Net is no longer supported, and users are recommended to migrate to the latest version of CentralSquare Community Development.	Patched by core rule	Y
CVE-2025-30212	Frappe has possibility of SQL injection due to improper validations	Frappe is a full-stack web application framework. An SQL Injection vulnerability has been identified in Frappe Framework prior to versions 14.89.0 and 15.51.0 which could allow a malicious actor to access sensitive information. Versions 14.89.0 and 15.51.0 fix the issue. Upgrading is required; no other workaround is present.	Patched by core rule	Y
CVE-2025-30523	WordPress Super Simple Subscriptions plugin <= 1.1.0 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Marcel-NL Super Simple Subscriptions allows SQL Injection. This issue affects Super Simple Subscriptions: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-30525	WordPress WP Profitshare plugin <= 1.4.9 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ProfitShare.ro WP Profitshare allows SQL	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Injection. This issue affects WP Profitshare: from n/a through 1.4.9.		
CVE-2025-30569	WordPress WP Featured Entries - <= <= 1.0 SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Jahertor WP Featured Entries allows SQL Injection. This issue affects WP Featured Entries: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-30570	WordPress دکمه، شبکه اجتماعی خرید - <= <= 2.0.6 SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AliRezaMohammadi دکمه، شبکه اجتماعی خرید allows SQL Injection. This issue affects دکمه، شبکه اجتماعی خرید: from n/a through 2.0.6.	Patched by core rule	Y
CVE-2025-30571	WordPress STEdb Forms - <= <= 1.0.4 SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in STEdb Corp. STEdb Forms allows SQL Injection. This issue affects STEdb Forms: from n/a through 1.0.4.	Patched by core rule	Y
CVE-2025-30590	WordPress Flickr set slideshows - <= <= 0.9 SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Dourou Flickr set slideshows allows SQL Injection. This issue affects Flickr set slideshows: from n/a through 0.9.	Patched by core rule	Y
CVE-2025-30604	WordPress JiangQie Official Website Mini Program plugin <= 1.8.2 - SQL Injection Vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in jiangqie JiangQie Official Website Mini Program allows Blind SQL Injection. This issue affects JiangQie Official Website Mini Program: from n/a through 1.8.2.	Patched by core rule	Y

XML External Entity Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-2365	crmeb_java WeChatMessageController.java webHook xml external entity reference	A vulnerability, which was classified as problematic, has been found in crmeb_java up to 1.3.4. Affected by this issue is the function webHook of the file WeChatMessageController.java. The manipulation leads to xml external entity reference. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-10948	Arbitrary File Read via Upload Function in binary-husky/gpt_academic	A vulnerability in the upload function of binary-husky/gpt_academic allows any user to read arbitrary files on the system, including sensitive files such as `config.py`. This issue affects the latest version of the product. An attacker can exploit this vulnerability by intercepting the websocket request during file upload and replacing the file path with the path of the file they wish to read. The server then copies the file to the `private_upload` folder and provides the path to the copied file, which can be accessed via a GET request. This vulnerability can lead to the exposure of sensitive system files, potentially including credentials, configuration files, or sensitive user data.	Patched by custom rule	N

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-0640	Stored XSS in chatwoot/chatwoot	A stored cross-site scripting (XSS) vulnerability exists in chatwoot/chatwoot versions 3.0.0 to 3.5.1. This vulnerability allows an admin user to inject malicious JavaScript code via the dashboard app settings, which can then be executed by another admin user when they access the affected dashboard app. The issue is fixed in version 3.5.2.	Patched by core rule	Y
CVE-2024-10719	Stored Cross-site Scripting (XSS) in phpipam/phpipam	A stored cross-site scripting (XSS) vulnerability exists in phpipam version 1.5.2, specifically in the circuits options functionality. This vulnerability allows an attacker to inject malicious scripts via the 'option' parameter in the POST request to /phpipam/app/admin/circuits/edit-options-submit.php. The injected script can be executed in the context of the user's browser, leading to potential cookie theft and end-user file disclosure. The issue is fixed in version 1.7.0.	Patched by core rule	Y
CVE-2024-10720	Stored Cross-site Scripting (XSS) in phpipam/phpipam	A stored cross-site scripting (XSS) vulnerability exists in phpipam/phpipam version 1.5.2. The vulnerability occurs in the 'Device Management' section under 'Administration' where an attacker can inject malicious scripts into the 'Name' and 'Description' fields when adding a new device type. This can lead to data theft, account compromise, distribution of malware, website defacement, and phishing attacks. The issue is fixed in version 1.7.0.	Patched by core rule	Y
CVE-2024-10721	Store XSS in phpipam/phpipam	A stored cross-site scripting (XSS) vulnerability was discovered in phpipam/phpipam version 1.5.2. This vulnerability allows an attacker to inject malicious scripts into the application, which can be executed in the context of other users who view the affected page. The issue occurs in the circuits options page (https://demo.phpipam.net/tools/circuits/options/). An	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attacker can exploit this vulnerability to steal cookies, gain unauthorized access to user accounts, or redirect users to malicious websites. The vulnerability has been fixed in version 1.7.0.		
CVE-2024-10722	Stored Cross-site Scripting (XSS) in phpipam/phpipam	A stored cross-site scripting (XSS) vulnerability exists in phpipam/phpipam version 1.5.2. The vulnerability allows attackers to inject malicious scripts into the 'Description' field of custom fields in the 'IP RELATED MANAGEMENT' section. This can lead to data theft, account compromise, distribution of malware, website defacement, content manipulation, and phishing attacks. The issue is fixed in version 1.7.0.	Patched by core rule	Y
CVE-2024-10723	Stored XSS in phpipam/phpipam	A stored cross-site scripting (XSS) vulnerability was discovered in phpipam/phpipam version 1.5.2. This vulnerability allows an attacker to inject malicious scripts into the destination address field of the NAT tool, which can be executed when a user interacts with the field. The impact of this vulnerability includes the potential theft of user cookies, unauthorized access to user accounts, and redirection to malicious websites. The issue has been fixed in version 1.7.0.	Patched by core rule	Y
CVE-2024-10724	Stored XSS in IPV6 Section in phpipam/phpipam	A stored cross-site scripting (XSS) vulnerability exists in phpipam/phpipam version 1.5.2, specifically in the Subnet NAT translations section when editing the Destination address. This vulnerability allows an attacker to execute malicious code. The issue is fixed in version 1.7.0.	Patched by core rule	Y
CVE-2024-10725	Stored Cross-site Scripting (XSS) in phpipam/phpipam	A stored cross-site scripting (XSS) vulnerability exists in phpipam/phpipam version 1.5.2. This vulnerability allows an attacker to inject malicious scripts into the application, which are then executed in the context of other users who view the affected pages. The issue occurs when editing the NAT	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		destination address, where user input is not properly sanitized. This can lead to data theft, account compromise, and other malicious activities. The vulnerability is fixed in version 1.7.0.		
CVE-2024-10727	Cross-Site Scripting (XSS) in phpipam/phpipam	A reflected cross-site scripting (XSS) vulnerability exists in phpipam/phpipam versions 1.5.0 through 1.6.0. The vulnerability arises when the application receives data in an HTTP request and includes that data within the immediate response in an unsafe manner. This allows an attacker to execute arbitrary JavaScript in the context of the user's browser, potentially leading to full compromise of the user.	Patched by core rule	Y
CVE-2024-11441	Stored XSS in Serge in serge-chat/serge	A stored cross-site scripting (XSS) vulnerability exists in Serge version 0.9.0. The vulnerability is due to improper neutralization of input during web page generation in the chat prompt. An attacker can exploit this vulnerability by sending a crafted message containing malicious HTML/JavaScript code, which will be stored and executed whenever the chat is accessed, leading to unintended content being shown to the user and potential phishing attacks.	Patched by core rule	Y
CVE-2024-11824	Stored XSS in langgenius/dify	A stored cross-site scripting (XSS) vulnerability exists in langgenius/dify version latest, specifically in the chat log functionality. The vulnerability arises because certain HTML tags like <input> and <form> are not disallowed, allowing an attacker to inject malicious HTML into the log via prompts. When an admin views the log containing the malicious HTML, the attacker could steal the admin's credentials or sensitive information. This issue is fixed in version 0.12.1.	Patched by core rule	Y
CVE-2024-11850	Stored XSS in langgenius/dify	A stored cross-site scripting (XSS) vulnerability exists in the latest version of langgenius/dify. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability is due to improper validation and sanitization of user input in SVG markdown support within the chatbot feature. An attacker can exploit this vulnerability by injecting malicious SVG content, which can execute arbitrary JavaScript code when viewed by an admin, potentially leading to credential theft.		
CVE-2024-12119	FooGallery – Responsive Photo Gallery, Image Viewer, Justified, Masonry & Carousel <= 2.4.29 - Authenticated (Custom+) Stored Cross-Site Scripting via Album Title Size	The FooGallery – Responsive Photo Gallery, Image Viewer, Justified, Masonry & Carousel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the default_gallery_title_size parameter in all versions up to, and including, 2.4.29 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with granted gallery and album creator roles, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2024-12374	Stored XSS in automatic1111/stable-diffusion-webui	A stored cross-site scripting (XSS) vulnerability exists in automatic1111/stable-diffusion-webui version git 82a973c. An attacker can upload an HTML file, which the application interprets as content-type application/html. If a victim accesses the malicious link, it will execute arbitrary JavaScript in the victim's browser.	Patched by core rule	Y
CVE-2024-12870	Stored Cross-site Scripting (XSS) in infiniflow/ragflow	A stored cross-site scripting (XSS) vulnerability exists in infiniflow/ragflow, affecting the latest commit on the main branch (cec2080). The vulnerability allows an attacker to upload HTML/XML files that can host arbitrary JavaScript payloads. These files are served with the 'application/xml' content type, which is automatically rendered by browsers. This can lead to the execution of arbitrary JavaScript in the context of the user's browser, potentially allowing attackers to steal cookies and gain unauthorized	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		access to user files and resources. The vulnerability does not require authentication, making it accessible to anyone with network access to the instance.		
CVE-2024-12871	Stored Cross-site Scripting (XSS) in infiniflow/ragflow	An XSS vulnerability in infiniflow/ragflow version 0.12.0 allows an attacker to upload a malicious PDF file to the knowledge base. When the file is viewed within Ragflow, the payload is executed in the context of the user's browser. This can lead to session hijacking, data exfiltration, or unauthorized actions performed on behalf of the victim, compromising sensitive user data and affecting the integrity of the entire application.	Patched by core rule	Y
CVE-2024-13902	huang-yk student-manage Edit a Student Information Page cross site scripting	A vulnerability, which was classified as problematic, was found in huang-yk student-manage 1.0. This affects an unknown part of the component Edit a Student Information Page. The manipulation of the argument Class leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-13918	Laravel Reflected XSS via Request Parameter in Debug-Mode Error Page	The Laravel framework versions between 11.9.0 and 11.35.1 are susceptible to reflected cross-site scripting due to an improper encoding of request parameters in the debug-mode error page.	Patched by core rule	Y
CVE-2024-13919	Laravel Reflected XSS via Route Parameter in Debug-Mode Error Page	The Laravel framework versions between 11.9.0 and 11.35.1 are susceptible to reflected cross-site scripting due to an improper encoding of route parameters in the debug-mode error page.	Patched by core rule	Y
CVE-2024-4023	Stored XSS in flatpressblog/flatpress	A stored cross-site scripting (XSS) vulnerability exists in flatpressblog/flatpress version 1.3. When a user uploads a file with a `.xsig` extension and directly accesses this file, the server responds with a Content-type of application/octet-stream, leading to the file being processed as an HTML	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file. This allows an attacker to execute arbitrary JavaScript code, which can be used to steal user cookies, perform HTTP requests, and access content of the same origin.		
CVE-2024-52812	LF Edge eKuiper has Stored XSS in Rules Functionality	LF Edge eKuiper is an internet-of-things data analytics and stream processing engine. Prior to version 2.0.8, auser with rights to modify the service (e.g. kuiperUser role) can inject a cross-site scripting payload into the rule `id` parameter. Then, after any user with access to this service (e.g. admin) tries make any modifications with the rule (update, run, stop, delete), a payload acts in the victim's browser. Version 2.0.8 fixes the issue.	Patched by core rule	Y
CVE-2024-53382	N/A	Prism (aka PrismJS) through 1.29.0 allows DOM Clobbering (with resultant XSS for untrusted input that contains HTML but does not directly contain JavaScript), because document.currentScript lookup can be shadowed by attacker-injected HTML elements.	Patched by core rule	Y
CVE-2024-53386	N/A	Stage.js through 0.8.10 allows DOM Clobbering (with resultant XSS for untrusted input that contains HTML but does not directly contain JavaScript), because document.currentScript lookup can be shadowed by attacker-injected HTML elements.	Patched by core rule	Y
CVE-2024-6986	Cross-site Scripting (XSS) in parisneo/lollms-webui	A Cross-site Scripting (XSS) vulnerability exists in the Settings page of parisneo/lollms-webui version 9.8. The vulnerability is due to the improper use of the 'v-html' directive, which inserts the content of the 'full_template' variable directly as HTML. This allows an attacker to execute malicious JavaScript code by injecting a payload into the 'System Template' input field under main configurations.	Patched by core rule	Y
CVE-2024-7044	Stored XSS in open-webui/open-webui	A Stored Cross-Site Scripting (XSS) vulnerability exists in the chat file upload	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		functionality of open-webui/open-webui version 0.3.8. An attacker can inject malicious content into a file, which, when accessed by a victim through a URL or shared chat, executes JavaScript in the victim's browser. This can lead to user data theft, session hijacking, malware distribution, and phishing attacks.		
CVE-2024-7990	Stored Cross-Site Scripting in open-webui/open-webui	A stored cross-site scripting (XSS) vulnerability exists in open-webui/open-webui version 0.3.8. The vulnerability is present in the `/api/v1/models/add` endpoint, where the model description field is improperly sanitized before being rendered in chat. This allows an attacker to inject malicious scripts that can be executed by any user, including administrators, potentially leading to arbitrary code execution.	Patched by core rule	Y
CVE-2024-8017	Cross-site Scripting (XSS) in open-webui/open-webui	An XSS vulnerability exists in open-webui/open-webui versions <= 0.3.8, specifically in the function that constructs the HTML for tooltips. This vulnerability allows attackers to perform operations with the victim's privileges, such as stealing chat history, deleting chats, and escalating their own account to an admin if the victim is an admin.	Patched by core rule	Y
CVE-2024-8027	Stored Cross-Site Scripting (XSS) in netease-youdao/QAnything	A stored Cross-Site Scripting (XSS) vulnerability exists in netease-youdao/QAnything. Attackers can upload malicious knowledge files to the knowledge base, which can trigger XSS attacks during user chats. This vulnerability affects all versions prior to the fix.	Patched by core rule	Y
CVE-2024-8029	Stored XSS in imartinez/privategpt	An XSS vulnerability was discovered in the upload file(s) process of imartinez/privategpt v0.5.0. Attackers can upload malicious SVG files, which execute JavaScript when victims click on the file link. This can lead to user data theft, session hijacking, malware distribution, and phishing attacks.	Patched by core rule	Y
CVE-2024-8101	Stored XSS in	A stored cross-site scripting	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	aimhubio/aim	(XSS) vulnerability exists in the Text Explorer component of aimhubio/aim version 3.23.0. The vulnerability arises due to the use of `dangerouslySetInnerHTML` without proper sanitization, allowing arbitrary JavaScript execution when rendering tracked texts. This can be exploited by injecting malicious HTML content during the training process, which is then rendered unsanitized in the Text Explorer.	rule	
CVE-2024-8186	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 16.6 before 17.7.6, 17.8 before 17.8.4, and 17.9 before 17.9.1. An attacker could inject HMTL into the child item search potentially leading to XSS in certain situations.	Patched by core rule	Y
CVE-2024-8400	Stored XSS in gaizhenbiao/chuanhuchatgpt	A stored cross-site scripting (XSS) vulnerability exists in the latest version of gaizhenbiao/chuanhuchatgpt. The vulnerability allows an attacker to upload a malicious HTML file containing JavaScript code, which is then executed when the file is accessed. This can lead to the execution of arbitrary JavaScript in the context of the user's browser.	Patched by core rule	Y
CVE-2024-8556	Stored XSS in modelscope/agentscope	A stored cross-site scripting (XSS) vulnerability exists in modelscope/agentscope, as of the latest commit 21161fe on the main branch. The vulnerability occurs in the view for inspecting detailed run information, where a user-controllable string (run ID) is appended and rendered as HTML. This allows an attacker to execute arbitrary JavaScript code in the context of the user's browser.	Patched by core rule	Y
CVE-2024-9107	Stored XSS in gaizhenbiao/chuanhuchatgpt	A stored cross-site scripting (XSS) vulnerability exists in the gaizhenbiao/chuanhuchatgpt repository, affecting version git 20b2e02. The vulnerability arises from improper sanitization of HTML tags in chat history	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		uploads. Specifically, the sanitization logic fails to handle HTML tags within code blocks correctly, allowing an attacker to inject malicious scripts. This can lead to the execution of arbitrary JavaScript code in the context of the user's browser, potentially leading to identity theft or other malicious actions.		
CVE-2024-9699	Cross-Site Scripting (XSS) in flatpressblog/flatpress	A vulnerability in the file upload functionality of the FlatPress CMS admin panel (version latest) allows an attacker to upload a file with a JavaScript payload disguised as a filename. This can lead to a Cross-Site Scripting (XSS) attack if the uploaded file is accessed by other users. The issue is fixed in version 1.4.dev.	Patched by core rule	Y
CVE-2024-9901	Storage XSS and CSRF Vulnerability in mudler/localai	LocalAI version v2.19.4 (af0545834fd565ab56af0b9348550ca9c3cb5349) contains a vulnerability where the delete model API improperly neutralizes input during web page generation, leading to a one-time storage cross-site scripting (XSS) vulnerability. This vulnerability allows an attacker to store a malicious payload that executes when a user accesses the homepage. Additionally, the presence of cross-site request forgery (CSRF) can enable automated malicious requests.	Patched by core rule	Y
CVE-2025-0183	Stored XSS in binary-husky/gpt_academic	A stored cross-site scripting (XSS) vulnerability exists in the Latex Proof-Reading Module of binary-husky/gpt_academic version 3.9.0. This vulnerability allows an attacker to inject malicious scripts into the `debug_log.html` file generated by the module. When an admin visits this debug report, the injected scripts can execute, potentially leading to unauthorized actions and data access.	Patched by core rule	Y
CVE-2025-0192	Stored Cross-site Scripting (XSS) in wandb/openui	A stored Cross-site Scripting (XSS) vulnerability exists in the latest version of wandb/openui. The vulnerability is present in the edit HTML functionality,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		where an attacker can inject malicious scripts. When the modified HTML is shared with another user, the XSS payload executes, potentially leading to the theft of user prompt history and other sensitive information.		
CVE-2025-0281	Stored Cross-Site Scripting (XSS) in lunary-ai/lunary	A stored cross-site scripting (XSS) vulnerability exists in lunary-ai/lunary versions 1.6.7 and earlier. An attacker can inject malicious JavaScript into the SAML IdP XML metadata, which is used to generate the SAML login redirect URL. This URL is then set as the value of `window.location.href` without proper validation or sanitization. This vulnerability allows the attacker to execute arbitrary JavaScript in the context of the user's browser, potentially leading to session hijacking, data theft, or other malicious actions. The issue is fixed in version 1.7.10.	Patched by core rule	Y
CVE-2025-0475	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 15.10 prior to 17.7.6, 17.8 prior to 17.8.4, and 17.9 prior to 17.9.1. A proxy feature could potentially allow unintended content rendering leading to XSS under specific circumstances.	Patched by core rule	Y
CVE-2025-0555	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in GitLab	A Cross Site Scripting (XSS) vulnerability in GitLab-EE affecting all versions from 16.6 prior to 17.7.6, 17.8 prior to 17.8.4, and 17.9 prior to 17.9.1 allows an attacker to bypass security controls and execute arbitrary scripts in a users browser under specific conditions.	Patched by core rule	Y
CVE-2025-1517	Sina Extension for Elementor <= 3.6.0 - Authenticated (Contributor+) Stored Cross-Site Scripting via Fancy Text, Countdown Widget, and Login Form Shortcodes	The Sina Extension for Elementor (Slider, Gallery, Form, Modal, Data Table, Tab, Particle, Free Elementor Widgets & Elementor Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Fancy Text, Countdown Widget, and Login Form shortcodes in all versions up to, and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		including, 3.6.0 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.		
CVE-2025-1689	ThemeMakers PayPal Express Checkout <= 1.1.9 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode	The ThemeMakers PayPal Express Checkout plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'paypal' shortcode in versions up to, and including, 1.1.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-1690	ThemeMakers Stripe Checkout <= 1.0.1 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode	The ThemeMakers Stripe Checkout plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'stripe' shortcode in versions up to, and including, 1.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-1742	pihome-shc PiHome home.php cross site scripting	A vulnerability, which was classified as problematic, has been found in pihome-shc PiHome 2.0. Affected by this issue is some unknown functionality of the file /home.php. The manipulation of the argument page_name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-1810	Pixsoft Vivaz Login	A vulnerability was found in	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Endpoint servlet cross site scripting	Pixsoft Vivaz 6.0.11. It has been classified as problematic. Affected is an unknown function of the file /servlet?act=login&submit=1&evento=0&pixrnd=0125021817031859360231 of the component Login Endpoint. The manipulation of the argument sistema leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	rule	
CVE-2025-1817	Mini-Tmall Admin Name admin cross site scripting	A vulnerability classified as problematic was found in Mini-Tmall up to 20250211. This vulnerability affects unknown code of the file /admin of the component Admin Name 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-2025-1830	zj1983 zz Customer Information cross site scripting	A vulnerability was found in zj1983 zz up to 2024-8. It has been rated as problematic. This issue affects some unknown processing of the component Customer Information Handler. The manipulation of the argument Customer Name leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-1892	shishuocms Directory Deletion Page add.json cross site scripting	A vulnerability was found in shishuocms 1.1. It has been classified as problematic. Affected is an unknown function of the file /manage/folder/add.json of the component Directory Deletion Page. The manipulation of the argument folderName 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-2025-1904	code-projects Blood Bank System A+.php cross site scripting	A vulnerability, which was classified as problematic, has been found in code-projects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Blood Bank System 1.0. Affected by this issue is some unknown functionality of the file /Blood/A+.php. The manipulation of the argument Availibility leads to cross site scripting. The attack may be launched remotely.		
CVE-2025-1905	SourceCodester Employee Management System employee.php cross site scripting	A vulnerability, which was classified as problematic, was found in SourceCodester Employee Management System 1.0. This affects an unknown part of the file employee.php. The manipulation of the argument Full 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-2025-1949	ZZCMS URL register_nodb.php cross site scripting	A vulnerability, which was classified as problematic, has been found in ZZCMS 2025. This issue affects some unknown processing of the file /3/ucenter_api/code/register_nodb.php of the component URL Handler. The manipulation of the argument $_SERVER['PHP_SELF'] 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-2025-1957	code-projects Blood Bank System o+.php cross site scripting	A vulnerability classified as problematic was found in code-projects Blood Bank System 1.0. This vulnerability affects unknown code of the file /BBfile/Blood/o+.php. The manipulation of the argument Bloodname 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-2025-1967	code-projects Blood Bank Management System donor.php cross site scripting	A vulnerability, which was classified as problematic, has been found in code-projects Blood Bank Management System 1.0. Affected by this issue is some unknown functionality of the file /user_dashboard/donor.php . The manipulation of the argument name leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-2047	PHPGurukul Art Gallery Management System search.php cross site scripting	A vulnerability was found in PHPGurukul Art Gallery Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /search.php. The manipulation of the argument search leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-2049	code-projects Blood Bank System AB+.php cross site scripting	A vulnerability classified as problematic has been found in code-projects Blood Bank System 1.0. Affected is an unknown function of the file AB+.php. The manipulation of the argument Bloodname 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-2025-2061	code-projects Online Ticket Reservation System passenger.php cross site scripting	A vulnerability was found in code-projects Online Ticket Reservation System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /passenger.php. The manipulation of the argument name 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-2025-2084	PHPGurukul Human Metapneumovirus Testing Management System Search Report Page search-report.php cross site scripting	A vulnerability was found in PHPGurukul Human Metapneumovirus Testing Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file /search-report.php of the component Search Report Page. 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-2025-2085	StarSea99 starsea-mall save cross site scripting	A vulnerability classified as problematic has been found in StarSea99 starsea-mall 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 /admin/carousels/save. The manipulation of the argument redirectUrl 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-2025-2086	StarSea99 starsea-mall update cross site scripting	A vulnerability classified as problematic was found in StarSea99 starsea-mall 1.0. This vulnerability affects unknown code of the file /admin/indexConfigs/update. The manipulation of the argument redirectUrl 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-2025-2087	StarSea99 starsea-mall update cross site scripting	A vulnerability, which was classified as problematic, has been found in StarSea99 starsea-mall 1.0. This issue affects some unknown processing of the file /admin/goods/update. The manipulation of the argument goodsName 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-2025-2108	140+ Widgets | Xpro Addons For Elementor – FREE <= 1.4.7.1 - Authenticated (Contributor+) Stored Cross-Site Scripting via 'Site Title' widget	The 140+ Widgets | Xpro Addons For Elementor – FREE plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘Site Title’ widget's 'title_tag' and 'html_tag' parameters in all versions up to, and including, 1.4.6.8 due to insufficient input sanitization and output escaping. 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-2025-2123	GeSHi CSS cssgen.php get_var cross site scripting	A vulnerability, which was classified as problematic, has been found in GeSHi up to 1.0.9.1. Affected by this issue is the function get_var of the file /contrib/cssgen.php of the component CSS Handler. The manipulation of the argument default-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		styles/keywords-1/keywords-2/keywords-3/keywords-4/comments leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-2124	Control iD RH iD API change_password cross site scripting	A vulnerability, which was classified as problematic, was found in Control iD RH iD 25.2.25.0. This affects an unknown part of the file /v2/customerdb/person.svc/change_password of the component API Handler. 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. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2130	OpenXE Ticket Bearbeiten Page cross site scripting	A vulnerability was found in OpenXE up to 1.12. It has been declared as problematic. This vulnerability affects unknown code of the component Ticket Bearbeiten Page. The manipulation of the argument Notizen leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2131	dayrui XunRuiCMS Friendly Links cross site scripting	A vulnerability was found in dayrui XunRuiCMS up to 4.6.3. It has been rated as problematic. This issue affects some unknown processing of the component Friendly Links Handler. The manipulation of the argument Website Address 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-2025-2133	ftcms edit cross site scripting	A vulnerability classified as problematic was found in ftcms 2.1. Affected by this vulnerability is an unknown functionality of the file /admin/index.php/news/edit. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument title leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-2163	Zoorum Comments <= 0.9 - Cross-Site Request Forgery to Stored Cross-Site Scripting	The Zoorum Comments plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.9. This is due to missing or incorrect nonce validation on the zoorum_set_options() function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-2164	pixelstats <= 0.8.2 - Reflected Cross-Site Scripting	The pixelstats plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'post_id' and 'sortby' parameters in all versions up to, and including, 0.8.2 due to insufficient input sanitization and output escaping. This makes it possible for 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.	Patched by core rule	Y
CVE-2025-2166	CM FAQ – Simplify support with an intuitive FAQ management tool <= 1.2.5 - Reflected Cross-Site Scripting	The CM FAQ – Simplify support with an intuitive FAQ management tool plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.2.5. This makes it possible for 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.	Patched by core rule	Y
CVE-2025-2194	MRCMS org.marker.mushroom.controller.FileController	A vulnerability was found in MRCMS 3.1.2 and classified as problematic. This issue	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	list.do list cross site scripting	affects the function list of the file /admin/file/list.do of the component org.marker.mushroom.controller.FileController. The manipulation of the argument path leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-2195	MRCMS org.marker.mushroom.controller.FileController rename.do rename cross site scripting	A vulnerability was found in MRCMS 3.1.2. It has been classified as problematic. Affected is the function rename of the file /admin/file/rename.do of the component org.marker.mushroom.controller.FileController. The manipulation of the argument name/path leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2196	MRCMS org.marker.mushroom.controller.FileController upload.do upload cross site scripting	A vulnerability was found in MRCMS 3.1.2. It has been declared as problematic. Affected by this vulnerability is the function upload of the file /admin/file/upload.do of the component org.marker.mushroom.controller.FileController. The manipulation of the argument path 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-2025-2206	aitangbao springboot-manager permission cross site scripting	A vulnerability classified as problematic has been found in aitangbao springboot-manager 3.0. This affects an unknown part of the file /sys/permission. The manipulation of the argument name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Other	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		parameters might be affected as well. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-2207	aitangbao springboot-manager dept cross site scripting	A vulnerability classified as problematic was found in aitangbao springboot-manager 3.0. This vulnerability affects unknown code of the file /sys/dept. The manipulation of the argument name leads to cross site scripting. 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. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2208	aitangbao springboot-manager Filename upload cross site scripting	A vulnerability, which was classified as problematic, has been found in aitangbao springboot-manager 3.0. This issue affects some unknown processing of the file /sysFiles/upload of the component Filename Handler. The manipulation of the argument name leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2209	aitangbao springboot-manager add cross site scripting	A vulnerability, which was classified as problematic, was found in aitangbao springboot-manager 3.0. Affected is an unknown function of the file /sysDict/add. 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-2025-2210	aitangbao springboot-manager add cross site scripting	A vulnerability has been found in aitangbao springboot-manager 3.0 and classified as problematic. Affected by this vulnerability	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		is an unknown functionality of the file /sysJob/add. The manipulation of the argument name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-2211	aitangbao springboot-manager add cross site scripting	A vulnerability was found in aitangbao springboot-manager 3.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /sysDictDetail/add. The manipulation of the argument name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2214	Microweber Settings index.php cross site scripting	A vulnerability was found in Microweber 2.0.19. It has been rated as problematic. This issue affects some unknown processing of the file userfiles/modules/settings/group/website_group/index.php of the component Settings Handler. The manipulation of the argument group leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2325	WP Test Email <= 1.1.8 - Unauthenticated Stored Cross-Site Scripting	The WP Test Email plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Email Logs in all versions up to, and including, 1.1.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-2335	Drivin Soluções API registerSchool cross site scripting	A vulnerability classified as problematic was found in Drivin Soluções up to 20250226. This vulnerability affects unknown code of the file /api/school/registerSchool of the component API Handler. The manipulation of the argument message leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2340	otale Tale Blog Site Settings save saveOptions cross site scripting	A vulnerability was found in otale Tale Blog 2.0.5. It has been declared as problematic. This vulnerability affects the function saveOptions of the file /options/save of the component Site Settings. The manipulation of the argument Site Title leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-23425	WordPress Marekkis Watermark plugin <= 0.9.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in marekki Marekkis Watermark allows Reflected XSS. This issue affects Marekkis Watermark: from n/a through 0.9.4.	Patched by core rule	Y
CVE-2025-23433	WordPress vcOS plugin <=1.4.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jnwry vcOS allows Reflected XSS. This issue affects vcOS: from n/a through 1.4.0.	Patched by core rule	Y
CVE-2025-23437	WordPress ntp-header-images plugin <=1.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound ntp-header-images allows Reflected XSS. This issue affects ntp-header-images: from n/a through 1.2.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-23439	WordPress TinyMCE Extended Config plugin <= 0.1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in willshouse TinyMCE Extended Config allows Reflected XSS. This issue affects TinyMCE Extended Config: from n/a through 0.1.0.	Patched by core rule	Y
CVE-2025-23441	WordPress Attach Gallery Posts plugin <= 1.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Attach Gallery Posts allows Reflected XSS. This issue affects Attach Gallery Posts: from n/a through 1.6.	Patched by core rule	Y
CVE-2025-23447	WordPress Smooth Dynamic Slider plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Smooth Dynamic Slider allows Reflected XSS. This issue affects Smooth Dynamic Slider: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23450	WordPress AW WooCommerce Kode Pembayaran plugin <= 1.1.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in agenwebsite AW WooCommerce Kode Pembayaran allows Reflected XSS. This issue affects AW WooCommerce Kode Pembayaran: from n/a through 1.1.4.	Patched by core rule	Y
CVE-2025-23451	WordPress Awesome Twitter Feeds plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Awesome Twitter Feeds allows Reflected XSS. This issue affects Awesome Twitter Feeds: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23464	WordPress Twitter News Feed plugin <= 1.1.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Twitter News Feed allows Reflected XSS. This issue affects Twitter News Feed: from n/a through 1.1.1.	Patched by core rule	Y
CVE-2025-23465	WordPress Vampire Character Manager plugin <= 2.13 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Vampire Character Manager allows Reflected XSS. This issue	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects Vampire Character Manager: from n/a through 2.13.		
CVE-2025-23468	WordPress Essay Wizard (wpCRES) plugin <= 1.0.6.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Essay Wizard (wpCRES) allows Reflected XSS. This issue affects Essay Wizard (wpCRES): from n/a through 1.0.6.4.	Patched by core rule	Y
CVE-2025-23472	WordPress Flexo Slider plugin <= 1.0013 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Flexo Slider allows Reflected XSS. This issue affects Flexo Slider: from n/a through 1.0013.	Patched by core rule	Y
CVE-2025-23473	WordPress Killer Theme Options plugin <= 2.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Killer Theme Options allows Reflected XSS. This issue affects Killer Theme Options: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-23478	WordPress Photo Video Store plugin <= 21.07 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Photo Video Store allows Reflected XSS. This issue affects Photo Video Store: from n/a through 21.07.	Patched by core rule	Y
CVE-2025-23479	WordPress melascrivi plugin <= 1.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound melascrivi allows Reflected XSS. This issue affects melascrivi: from n/a through 1.4.	Patched by core rule	Y
CVE-2025-23480	WordPress RSVP ME plugin <= 1.9.9 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound RSVP ME allows Stored XSS. This issue affects RSVP ME: from n/a through 1.9.9.	Patched by core rule	Y
CVE-2025-23481	WordPress Ni WooCommerce Sales Report Email plugin <= 3.1.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Ni WooCommerce Sales Report Email allows Reflected XSS. This issue affects Ni WooCommerce Sales Report Email: from n/a through 3.1.4.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-23482	WordPress azurecurve Floating Featured Image plugin <= 2.2.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound azurecurve Floating Featured Image allows Reflected XSS. This issue affects azurecurve Floating Featured Image: from n/a through 2.2.0.	Patched by core rule	Y
CVE-2025-23484	WordPress Predict When plugin <= 1.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Predict When allows Reflected XSS. This issue affects Predict When: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-23485	WordPress RS Survey plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in richestsoft RS Survey allows Reflected XSS. This issue affects RS Survey: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23487	WordPress Easy Gallery plugin <= 1.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Easy Gallery allows Reflected XSS. This issue affects Easy Gallery: from n/a through 1.4.	Patched by core rule	Y
CVE-2025-23488	WordPress rng-refresh plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound rng-refresh allows Reflected XSS. This issue affects rng-refresh: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23490	WordPress Browser-Update-Notify plugin <= 0.2.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Browser-Update-Notify allows Reflected XSS. This issue affects Browser-Update-Notify: from n/a through 0.2.1.	Patched by core rule	Y
CVE-2025-23493	WordPress Google Transliteration plugin <= 1.7.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Google Transliteration allows Reflected XSS. This issue affects Google Transliteration: from n/a through 1.7.2.	Patched by core rule	Y
CVE-2025-23494	WordPress Quizzin plugin <= 1.01.4 - Reflected	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Cross Site Scripting (XSS) vulnerability	Generation ('Cross-site Scripting') vulnerability in NotFound Quizzin allows Reflected XSS. This issue affects Quizzin: from n/a through 1.01.4.		
CVE-2025-23496	WordPress WP FPO plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WP FPO allows Reflected XSS. This issue affects WP FPO: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23505	WordPress Pit Login Welcome plugin <= 1.1.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Pit Login Welcome allows Reflected XSS. This issue affects Pit Login Welcome: from n/a through 1.1.5.	Patched by core rule	Y
CVE-2025-23516	WordPress Sale with Razorpay plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Sale with Razorpay allows Reflected XSS. This issue affects Sale with Razorpay: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23517	WordPress Google Map on Post/Page plugin <= 1.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Google Map on Post/Page allows Reflected XSS. This issue affects Google Map on Post/Page: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-23518	WordPress GoogleMapper plugin <= 2.0.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound GoogleMapper allows Reflected XSS. This issue affects GoogleMapper: from n/a through 2.0.3.	Patched by core rule	Y
CVE-2025-23519	WordPress G Web Pro Store Locator plugin <= 2.0.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound G Web Pro Store Locator allows Reflected XSS. This issue affects G Web Pro Store Locator: from n/a through 2.0.1.	Patched by core rule	Y
CVE-2025-2352	StarSea99 starsea-mall Backend save cross site scripting	A vulnerability, which was classified as problematic, has been found in StarSea99 starsea-mall 1.0. This issue affects some unknown processing of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/admin/indexConfigs/save of the component Backend. The manipulation of the argument categoryName leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. Other parameters might be affected as well. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-23520	WordPress Heartland Management Terminal plugin <= 1.3.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SecureSubmit Heartland Management Terminal allows Reflected XSS. This issue affects Heartland Management Terminal: from n/a through 1.3.0.	Patched by core rule	Y
CVE-2025-23521	WordPress Goodlayers Blocks plugin <= 1.0.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Goodlayers Blocks allows Reflected XSS. This issue affects Goodlayers Blocks: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-23524	WordPress ClickBank Storefront WordPress Plugin plugin <= 1.7 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound ClickBank Storefront allows Reflected XSS. This issue affects ClickBank Storefront: from n/a through 1.7.	Patched by core rule	Y
CVE-2025-23526	WordPress Swift Calendar Online Appointment Scheduling plugin <= 1.3.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Swift Calendar Online Appointment Scheduling allows Reflected XSS. This issue affects Swift Calendar Online Appointment Scheduling: from n/a through 1.3.3.	Patched by core rule	Y
CVE-2025-23536	WordPress Track Page Scroll plugin <= 1.0.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Track Page Scroll allows Reflected XSS. This issue affects Track Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Scroll: from n/a through 1.0.2.		
CVE-2025-23538	WordPress WP Contest plugin <= 1.0.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WP Contest allows Reflected XSS. This issue affects WP Contest: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-23539	WordPress Awesome Hooks plugin <= 1.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Awesome Hooks allows Reflected XSS. This issue affects Awesome Hooks: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-23549	WordPress Maniac SEO plugin <= 2.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Maniac SEO allows Reflected XSS. This issue affects Maniac SEO: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-23552	WordPress Texteller plugin <= 1.3.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Texteller allows Reflected XSS. This issue affects Texteller: from n/a through 1.3.0.	Patched by core rule	Y
CVE-2025-23553	WordPress Userbase Access Control plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in David Cramer Userbase Access Control allows Reflected XSS. This issue affects Userbase Access Control: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23555	WordPress Ui Slider Filter By Price plugin <= 1.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Ui Slider Filter By Price allows Reflected XSS. This issue affects Ui Slider Filter By Price: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-23556	WordPress Push Envoy Notifications plugin <= 1.0.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Push Envoy Notifications allows Reflected XSS. This issue affects Push Envoy Notifications: from n/a through 1.0.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-23563	WordPress Explore pages plugin <= 1.01 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Explore pages allows Reflected XSS. This issue affects Explore pages: from n/a through 1.01.	Patched by core rule	Y
CVE-2025-23564	WordPress WP FixTag plugin <= v2.0.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mohsenshahbazi WP FixTag allows Reflected XSS. This issue affects WP FixTag: from n/a through v2.0.2.	Patched by core rule	Y
CVE-2025-23565	WordPress Wibstats plugin <= 0.5.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Wibstats allows Reflected XSS. This issue affects Wibstats: from n/a through 0.5.5.	Patched by core rule	Y
CVE-2025-23570	WordPress WP Social Links plugin <= 0.3.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WP Social Links allows Reflected XSS. This issue affects WP Social Links: from n/a through 0.3.1.	Patched by core rule	Y
CVE-2025-23575	WordPress DX Sales CRM plugin <= 1.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound DX Sales CRM allows Reflected XSS. This issue affects DX Sales CRM: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-23576	WordPress WP Intro.JS Plugin plugin <= 1.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WP Intro.JS allows Reflected XSS. This issue affects WP Intro.JS: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-23579	WordPress DZS Ajaxer Lite plugin <= 1.04 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound DZS Ajaxer Lite allows Stored XSS. This issue affects DZS Ajaxer Lite: from n/a through 1.04.	Patched by core rule	Y
CVE-2025-23584	WordPress Pin Locations on Map plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Pin Locations on Map allows Reflected XSS. This issue affects Pin	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Locations on Map: from n/a through 1.0.		
CVE-2025-23585	WordPress Goo.gl Url Shorter plugin <= 1.0.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CantonBolo Goo.gl Url Shorter allows Reflected XSS. This issue affects Goo.gl Url Shorter: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-23586	WordPress WP Post Category Notifications plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WP Post Category Notifications allows Reflected XSS. This issue affects WP Post Category Notifications: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23587	WordPress all-in-one-box-login plugin <= 2.0.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound all-in-one-box-login allows Reflected XSS. This issue affects all-in-one-box-login: from n/a through 2.0.1.	Patched by core rule	Y
CVE-2025-23595	WordPress Page Health-O-Meter plugin <= 2.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Page Health-O-Meter allows Reflected XSS. This issue affects Page Health-O-Meter: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-23600	WordPress Send to a Friend Addon plugin <= 1.4.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pinal.shah Send to a Friend Addon allows Reflected XSS. This issue affects Send to a Friend Addon: from n/a through 1.4.1.	Patched by core rule	Y
CVE-2025-23616	WordPress Canalplan plugin <= 5.31 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Canalplan allows Reflected XSS. This issue affects Canalplan: from n/a through 5.31.	Patched by core rule	Y
CVE-2025-23619	WordPress Catch Duplicate Switcher plugin <= 2.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Catch Duplicate Switcher allows Reflected XSS. This issue affects Catch Duplicate Switcher: from n/a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		through 2.0.		
CVE-2025-23635	WordPress ePermissions plugin <= 1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mobde3net ePermissions allows Reflected XSS. This issue affects ePermissions: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-23637	WordPress 新淘客WordPress插件 plugin <= 1.1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound 新淘客WordPress插件 allows Reflected XSS. This issue affects 新淘客WordPress插件: from n/a through 1.1.2.	Patched by core rule	Y
CVE-2025-2366	gougucms Add Department Page add cross site scripting	A vulnerability, which was classified as problematic, was found in gougucms 4.08.18. This affects the function add of the file /admin/department/add of the component Add Department Page. The manipulation of the argument title 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-2025-23663	WordPress Contexto plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Adrian Vaquez Contexto allows Reflected XSS. This issue affects Contexto: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23668	WordPress ChatGPT Open AI Images & Content for WooCommerce plugin <= 2.2.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound ChatGPT Open AI Images & Content for WooCommerce allows Reflected XSS. This issue affects ChatGPT Open AI Images & Content for WooCommerce: from n/a through 2.2.0.	Patched by core rule	Y
CVE-2025-23670	WordPress 4 author cheer up donate plugin <= 1.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound 4 author cheer up donate allows Reflected XSS. This issue affects 4 author	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cheer up donate: from n/a through 1.3.		
CVE-2025-23687	WordPress Woo Store Mode plugin <= 1.0.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in simonhunter Woo Store Mode allows Reflected XSS. This issue affects Woo Store Mode: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-23688	WordPress Cobwebo URL Plugin plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Cobwebo URL Plugin allows Reflected XSS. This issue affects Cobwebo URL Plugin: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-2371	PHPGurukul Human Metapneumovirus Testing Management System Registered Mobile Number Search registered-user-testing.php cross site scripting	A vulnerability was found in PHPGurukul Human Metapneumovirus Testing Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /registered-user-testing.php of the component Registered Mobile Number Search. The manipulation of the argument regmobilenumber 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-2025-23716	WordPress Login Watchdog plugin <= 1.0.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Login Watchdog allows Stored XSS. This issue affects Login Watchdog: from n/a through 1.0.4.	Patched by core rule	Y
CVE-2025-23718	WordPress Mancx AskMe Widget plugin <= 0.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Mancx AskMe Widget allows Reflected XSS. This issue affects Mancx AskMe Widget: from n/a through 0.3.	Patched by core rule	Y
CVE-2025-23721	WordPress Mobigate plugin <= 1.0.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Mobigate allows Reflected XSS. This issue affects Mobigate: from n/a through 1.0.3.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-23726	WordPress ComparePress plugin <= 2.0.8 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound ComparePress allows Reflected XSS. This issue affects ComparePress: from n/a through 2.0.8.	Patched by core rule	Y
CVE-2025-23731	WordPress Tax Report for WooCommerce plugin <= 2.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in infosoftplugin Tax Report for WooCommerce allows Reflected XSS. This issue affects Tax Report for WooCommerce: from n/a through 2.2.	Patched by core rule	Y
CVE-2025-23736	WordPress Form To JSON plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Form To JSON allows Reflected XSS. This issue affects Form To JSON: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23738	WordPress Ps Ads Pro plugin <= 1.0.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Ps Ads Pro allows Reflected XSS. This issue affects Ps Ads Pro: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-23739	WordPress WP Ultimate Reviews FREE plugin <= 1.0.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WP Ultimate Reviews FREE allows Reflected XSS. This issue affects WP Ultimate Reviews FREE: from n/a through 1.0.2.	Patched by core rule	Y
CVE-2025-23740	WordPress Easy School Registration plugin <= 3.9.8 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Easy School Registration allows Reflected XSS. This issue affects Easy School Registration: from n/a through 3.9.8.	Patched by core rule	Y
CVE-2025-23741	WordPress Notifications Center plugin <= 1.5.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Notifications Center allows Reflected XSS. This issue affects Notifications Center: from n/a through 1.5.2.	Patched by core rule	Y
CVE-2025-23744	WordPress Random	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Posts, Mp3 Player + ShareButton plugin <= 1.4.1 - Reflected Cross Site Scripting (XSS) vulnerability	Input During Web Page Generation ('Cross-site Scripting') vulnerability in dvs11 Random Posts, Mp3 Player + ShareButton allows Reflected XSS. This issue affects Random Posts, Mp3 Player + ShareButton: from n/a through 1.4.1.	rule	
CVE-2025-2375	PHPGurukul Human Metapneumovirus Testing Management System Admin Profile Page profile.php cross site scripting	A vulnerability, which was classified as problematic, was found in PHPGurukul Human Metapneumovirus Testing Management System 1.0. Affected is an unknown function of the file /profile.php of the component Admin Profile Page. The manipulation of the argument email 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-2025-23753	WordPress DN Sitemap Control plugin <= 1.0.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound DN Sitemap Control allows Reflected XSS. This issue affects DN Sitemap Control: from n/a through 1.0.6.	Patched by core rule	Y
CVE-2025-23762	WordPress DsgnWrks Twitter Importer plugin <= 1.1.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound DsgnWrks Twitter Importer allows Reflected XSS. This issue affects DsgnWrks Twitter Importer: from n/a through 1.1.4.	Patched by core rule	Y
CVE-2025-2377	SourceCodester Vehicle Management System confirmbooking.php cross site scripting	A vulnerability was found in SourceCodester Vehicle Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /confirmbooking.php. The manipulation of the argument id leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions contradicting product names.	Patched by core rule	Y
CVE-2025-23813	WordPress Guten Free Options Plugin <= 0.9.5 - Reflected Cross Site Scripting (XSS)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	vulnerability	NotFound Guten Free Options allows Reflected XSS. This issue affects Guten Free Options: from n/a through 0.9.5.		
CVE-2025-23814	WordPress CRUDLab Like Box Plugin <= 2.0.9 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound CRUDLab Like Box allows Reflected XSS. This issue affects CRUDLab Like Box: from n/a through 2.0.9.	Patched by core rule	Y
CVE-2025-23829	WordPress Woo Update Variations In Cart plugin <= 0.0.9 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Woo Update Variations In Cart allows Stored XSS. This issue affects Woo Update Variations In Cart: from n/a through 0.0.9.	Patched by core rule	Y
CVE-2025-23843	WordPress WP-HR Manager plugin <= 3.1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wphrmanager WP-HR Manager: The Human Resources Plugin for WordPress allows Reflected XSS. This issue affects WP-HR Manager: The Human Resources Plugin for WordPress: from n/a through 3.1.0.	Patched by core rule	Y
CVE-2025-23847	WordPress Site Launcher Plugin <= 0.9.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Site Launcher allows Reflected XSS. This issue affects Site Launcher: from n/a through 0.9.4.	Patched by core rule	Y
CVE-2025-23850	WordPress Mojo Under Construction Plugin <= 1.1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Mojo Under Construction allows Reflected XSS. This issue affects Mojo Under Construction: from n/a through 1.1.2.	Patched by core rule	Y
CVE-2025-23852	WordPress First Comment Redirect plugin <= 1.0.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound First Comment Redirect allows Reflected XSS. This issue affects First Comment Redirect: from n/a through 1.0.3.	Patched by core rule	Y
CVE-2025-23879	WordPress Easy Automatic Newsletter	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Lite Plugin <= 3.2.0 - Reflected Cross Site Scripting (XSS) vulnerability	Generation ('Cross-site Scripting') vulnerability in PillarDev Easy Automatic Newsletter Lite allows Reflected XSS. This issue affects Easy Automatic Newsletter Lite: from n/a through 3.2.0.		
CVE-2025-23881	WordPress LJ Custom Menu Links Plugin <= 2.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound LJ Custom Menu Links allows Reflected XSS. This issue affects LJ Custom Menu Links: from n/a through 2.5.	Patched by core rule	Y
CVE-2025-23883	WordPress Stray Random Quotes Plugin <= 1.9.9 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Stray Random Quotes allows Reflected XSS. This issue affects Stray Random Quotes: from n/a through 1.9.9.	Patched by core rule	Y
CVE-2025-23903	WordPress Local Shipping Labels for WooCommerce Plugin <= 1.0.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Local Shipping Labels for WooCommerce allows Reflected XSS. This issue affects Local Shipping Labels for WooCommerce: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-23904	WordPress Rebrand Fluent Forms Plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Rebrand Fluent Forms allows Reflected XSS. This issue affects Rebrand Fluent Forms: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23956	WordPress WP Easy Post Mailer Plugin <= 0.64 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WP Easy Post Mailer allows Reflected XSS. This issue affects WP Easy Post Mailer: from n/a through 0.64.	Patched by core rule	Y
CVE-2025-24694	WordPress Name: CM E-Mail Registration Blacklist plugin <= 1.5.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CreativeMindsSolutions CM Email Registration Blacklist and Whitelist allows Reflected XSS. This issue affects CM Email Registration Blacklist and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Whitelist: from n/a through 1.5.5.		
CVE-2025-24758	WordPress CM Map Locations plugin <= 2.0.8 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CreativeMindsSolutions CM Map Locations allows Reflected XSS. This issue affects CM Map Locations: from n/a through 2.0.8.	Patched by core rule	Y
CVE-2025-2477	CryoKey <= 2.4 - Reflected Cross-Site Scripting via 'ckemail' Parameter	The CryoKey plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘ckemail’ parameter in all versions up to, and including, 2.4 due to insufficient input sanitization and output escaping. This makes it possible for 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.	Patched by core rule	Y
CVE-2025-2479	Easy Custom Admin Bar <= 1.0 - Reflected Cross-Site Scripting via msg Parameter	The Easy Custom Admin Bar plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘msg’ parameter in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for 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.	Patched by core rule	Y
CVE-2025-2482	Gotcha | Gesture-based Captcha <= 1.0.0 - Reflected Cross-Site Scripting via menu Parameter	The Gotcha | Gesture-based Captcha plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'menu' parameter in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for 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.	Patched by core rule	Y
CVE-2025-2484	Multi Video Box <= 1.5.2 - Reflected Cross-Site Scripting via video_id and group_id Parameters	The Multi Video Box plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'video_id' and 'group_id' parameters in all versions up to, and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		including, 1.5.2 due to insufficient input sanitization and output escaping. This makes it possible for 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-2025-2490	Dromara ujcms File Upload WebFileUploadController.java upload cross site scripting	A vulnerability was found in Dromara ujcms 9.7.5. It has been rated as problematic. Affected by this issue is the function uploadZip/upload of the file /main/java/com/ujcms/cms/ext/web/backendapi/WebFileUploadController.java of the component File Upload. 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.	Patched by core rule	Y
CVE-2025-2491	Dromara ujcms Edit Template File Page WebFileTemplateController.java update cross site scripting	A vulnerability classified as problematic has been found in Dromara ujcms 9.7.5. This affects the function update of the file /main/java/com/ujcms/cms/ext/web/backendapi/WebFileTemplateController.java of the component Edit Template File Page. 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.	Patched by core rule	Y
CVE-2025-25070	WordPress Album Reviewer plugin <= 2.0.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Album Reviewer allows Stored XSS. This issue affects Album Reviewer: from n/a through 2.0.2.	Patched by core rule	Y
CVE-2025-25083	WordPress EP4 More Embeds Plugin <= 1.0.0 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound EP4 More Embeds allows Stored XSS. This issue affects EP4 More Embeds: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-25084	WordPress UniTimetable plugin <= 1.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound UniTimetable allows Stored XSS. This issue affects UniTimetable: from	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		n/a through 1.1.		
CVE-2025-25087	WordPress seekXL Snapr plugin <= 2.0.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound seekXL Snapr allows Reflected XSS. This issue affects seekXL Snapr: from n/a through 2.0.6.	Patched by core rule	Y
CVE-2025-25089	WordPress Image Rotator plugin <= 2.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in appten Image Rotator allows Reflected XSS. This issue affects Image Rotator: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-25090	WordPress Dreamstime Stock Photos plugin <= 4.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Dreamstime Stock Photos allows Reflected XSS. This issue affects Dreamstime Stock Photos: from n/a through 4.0.	Patched by core rule	Y
CVE-2025-25092	WordPress All push notification for WP plugin <= 1.5.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gtlwpdev All push notification for WP allows Reflected XSS. This issue affects All push notification for WP: from n/a through 1.5.3.	Patched by core rule	Y
CVE-2025-25099	WordPress Appointment Buddy Widget By Accrete plugin <= 1.2. - Reflected Cross-Site Scripting vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in accreteinfosolution Appointment Buddy Widget allows Reflected XSS. This issue affects Appointment Buddy Widget: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-25102	WordPress Yahoo BOSS Plugin <= 0.7 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Yahoo BOSS allows Reflected XSS. This issue affects Yahoo BOSS: from n/a through 0.7.	Patched by core rule	Y
CVE-2025-25108	WordPress SW Plus Plugin <= 2.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in shalomworld SW Plus allows Reflected XSS. This issue affects SW Plus: from n/a through 2.1.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-25113	WordPress Implied Cookie Consent plugin <= 1.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Implied Cookie Consent allows Reflected XSS. This issue affects Implied Cookie Consent: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-25114	WordPress User Role plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ehabstar User Role allows Reflected XSS. This issue affects User Role: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-25115	WordPress Like dislike plus counter plugin <= 1.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Like dislike plus counter allows Stored XSS. This issue affects Like dislike plus counter: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-25118	WordPress WPOptin plugin <= 2.0.8 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Top Bar – PopUps – by WPOptin allows Reflected XSS. This issue affects Top Bar – PopUps – by WPOptin: from n/a through 2.0.8.	Patched by core rule	Y
CVE-2025-25119	WordPress Woocommerce osCommerce Sync plugin <= 2.0.20 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Woocommerce osCommerce Sync allows Reflected XSS. This issue affects Woocommerce osCommerce Sync: from n/a through 2.0.20.	Patched by core rule	Y
CVE-2025-25121	WordPress Theme Options Z Plugin <= 1.4 - Cross Site Request Forgery (CSRF) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Theme Options Z allows Stored XSS. This issue affects Theme Options Z: from n/a through 1.4.	Patched by core rule	Y
CVE-2025-25124	WordPress Status Updater Plugin <= 9.21 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in devu Status Updater allows Reflected XSS. This issue affects Status Updater: from n/a through 1.9.2.	Patched by core rule	Y
CVE-2025-25127	WordPress Contact Us By	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Lord Linus Plugin <= 2.6 - Reflected Cross Site Scripting (XSS) vulnerability	Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rohitashv Singhal Contact Us By Lord Linus allows Reflected XSS. This issue affects Contact Us By Lord Linus: from n/a through 2.6.	rule	
CVE-2025-25129	WordPress Callback Request plugin <= 1.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Callback Request allows Reflected XSS. This issue affects Callback Request: from n/a through 1.4.	Patched by core rule	Y
CVE-2025-25131	WordPress RJ Quickcharts plugin <= 0.6.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound RJ Quickcharts allows Stored XSS. This issue affects RJ Quickcharts: from n/a through 0.6.1.	Patched by core rule	Y
CVE-2025-25132	WordPress Visitor Details plugin <= 1.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ravi Singh Visitor Details allows Stored XSS. This issue affects Visitor Details: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-25133	WordPress WP Frontend Submit Plugin <= 1.1.0 - Reflected Cross-Site Scripting vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WP Frontend Submit allows Cross-Site Scripting (XSS). This issue affects WP Frontend Submit: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-25137	WordPress Social Links plugin <= 1.0.11 - Stored Cross-Site Scripting vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Social Links allows Stored XSS. This issue affects Social Links: from n/a through 1.0.11.	Patched by core rule	Y
CVE-2025-25142	WordPress WP Less Compiler plugin <= 1.3.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WP Less Compiler allows Stored XSS. This issue affects WP Less Compiler: from n/a through 1.3.0.	Patched by core rule	Y
CVE-2025-25157	WordPress WP Church Center Plugin <= 1.3.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WP Church Center allows Reflected XSS. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		issue affects WP Church Center: from n/a through 1.3.3.		
CVE-2025-25158	WordPress Uncomplicated SEO plugin <= 1.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Uncomplicated SEO allows Reflected XSS. This issue affects Uncomplicated SEO: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-25161	WordPress WP Find Your Nearest Plugin <= 0.3.1 - CSRF to Settings Change vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WP Find Your Nearest allows Reflected XSS. This issue affects WP Find Your Nearest: from n/a through 0.3.1.	Patched by core rule	Y
CVE-2025-25164	WordPress Meta Accelerator plugin <= 1.0.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Meta Accelerator allows Reflected XSS. This issue affects Meta Accelerator: from n/a through 1.0.4.	Patched by core rule	Y
CVE-2025-25165	WordPress Staff Directory Plugin: Company Directory Plugin <= 4.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Staff Directory Plugin: Company Directory allows Stored XSS. This issue affects Staff Directory Plugin: Company Directory: from n/a through 4.3.	Patched by core rule	Y
CVE-2025-25169	WordPress Authors Autocomplete Meta Box plugin <= 1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Authors Autocomplete Meta Box allows Reflected XSS. This issue affects Authors Autocomplete Meta Box: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-25170	WordPress Migrate Posts Plugin <=1.0 - Post Based Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Migrate Posts allows Reflected XSS. This issue affects Migrate Posts: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-25191	Group-Office has a Stored XSS Vulnerability via user's name field	Group-Office is an enterprise CRM and groupware tool. This Stored XSS vulnerability exists where user input in the Name field is not properly sanitized before	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		being stored. This vulnerability is fixed in 6.8.100.		
CVE-2025-2542	Your Simple SVG Support <= 1.0.1 - Authenticated (Author+) Stored Cross-Site Scripting via SVG File Upload	The Your Simple SVG Support plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	Patched by core rule	Y
CVE-2025-2582	SimpleMachines SMF ManageAttachments.php cross site scripting	A vulnerability was found in SimpleMachines SMF 2.1.4 and classified as problematic. Affected by this issue is some unknown functionality of the file ManageAttachments.php. The manipulation of the argument Notice leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure.	Patched by core rule	Y
CVE-2025-2583	SimpleMachines SMF ManageNews.php cross site scripting	A vulnerability was found in SimpleMachines SMF 2.1.4. It has been classified as problematic. This affects an unknown part of the file ManageNews.php. The manipulation of the argument subject/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. The vendor was contacted early about this disclosure.	Patched by core rule	Y
CVE-2025-2590	code-projects Human Resource Management System recruitment.go UpdateRecruitmentById cross site scripting	A vulnerability was found in code-projects Human Resource Management System 1.0.1. It has been classified as problematic. Affected is the function UpdateRecruitmentById of the file \handler\recruitment.go. The manipulation of the argument c leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		may be used.		
CVE-2025-2609	MagnusBilling Stored Cross-Site Scripting in Login Logs	Improper neutralization of input during web page generation vulnerability in MagnusSolution MagnusBilling login logging allows unauthenticated users to store HTML content in the viewable log component accessible at /mbilling/index.php/logUsers/read" cross-site scripting This vulnerability is associated with program files protected/components/MagnusLog.Php. This issue affects MagnusBilling: through 7.3.0.	Patched by core rule	Y
CVE-2025-2610	MagnusBilling Stored Cross-Site Scripting in Alarm Module	Improper neutralization of input during web page generation vulnerability in MagnusSolution MagnusBilling (Alarm Module modules) allows authenticated stored cross-site scripting. This vulnerability is associated with program files protected/components/MagnusLog.Php. This issue affects MagnusBilling: through 7.3.0.	Patched by core rule	Y
CVE-2025-2616	yangyouwang 杨有旺 crud 简约后台管理系统 Role Management Page cross site scripting	A vulnerability classified as problematic has been found in yangyouwang 杨有旺 crud 简约后台管理系统 1.0.0. Affected is an unknown function of the component Role Management Page. 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-2025-2617	yangyouwang 杨有旺 crud 简约后台管理系统 Department Page cross site scripting	A vulnerability classified as problematic was found in yangyouwang 杨有旺 crud 简约后台管理系统 1.0.0. Affected by this vulnerability is an unknown functionality of the component Department Page. The manipulation leads to cross site scripting. The attack can be launched 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-2025-2623	westboy CicadasCMS save cross site scripting	A vulnerability was found in westboy CicadasCMS 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /system/cms/content/save. The manipulation of the argument title/content/laiyuan 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-2025-2645	PHPGurukul Art Gallery Management System product.php cross site scripting	A vulnerability was found in PHPGurukul Art Gallery Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file /product.php. The manipulation of the argument artname 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-2025-2650	PHPGurukul Medical Card Generation System download-medical-cards.php cross site scripting	A vulnerability, which was classified as problematic, has been found in PHPGurukul Medical Card Generation System 1.0. This issue affects some unknown processing of the file /download-medical-cards.php. The manipulation of the argument searchdata leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-26548	WordPress Random Image Selector plugin <= 1.5.6 - Reflected Cross-Site Scripting vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Random Image Selector allows Reflected XSS. This issue affects Random Image Selector: from n/a through 2.4.	Patched by core rule	Y
CVE-2025-26553	WordPress Pre Order Addon for WooCommerce plugin<= 1.0.7 - Reflected Cross-Site Scripting	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Spring Devs Pre Order Addon for WooCommerce – Advance Order/Backorder Plugin allows Reflected XSS. This issue affects Pre Order Addon for WooCommerce –	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Advance Order/Backorder Plugin: from n/a through 2.2.		
CVE-2025-26554	WordPress WP Discord Post Plugin <= 2.1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WP Discord Post allows Reflected XSS. This issue affects WP Discord Post: from n/a through 2.1.0.	Patched by core rule	Y
CVE-2025-26555	WordPress Debug-Bar-Extender Plugin <= 0.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Debug-Bar-Extender allows Reflected XSS. This issue affects Debug-Bar-Extender: from n/a through 0.5.	Patched by core rule	Y
CVE-2025-26556	WordPress WP AntiDDOS Plugin <= 2.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in zzmaster WP AntiDDOS allows Reflected XSS. This issue affects WP AntiDDOS: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-26557	WordPress ViperBar Plugin <= 2.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound ViperBar allows Reflected XSS. This issue affects ViperBar: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-26563	WordPress Rocket Mobile Plugin <= 0.4.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Mobile allows Reflected XSS. This issue affects Mobile: from n/a through 1.3.3.	Patched by core rule	Y
CVE-2025-26585	WordPress DL Leadback Plugin <= 1.2.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound DL Leadback allows Reflected XSS. This issue affects DL Leadback: from n/a through 1.2.1.	Patched by core rule	Y
CVE-2025-26586	WordPress Events Planner Plugin <= 1.3.10 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Events Planner allows Reflected XSS. This issue affects Events Planner: from n/a through 1.3.10.	Patched by core rule	Y
CVE-2025-26587	WordPress sidebarTabs Plugin <= 3.1 - Reflected Cross Site Scripting (XSS)	Improper Neutralization of Input During Web Page Generation ('Cross-site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	vulnerability	Scripting') vulnerability in NotFound sidebarTabs allows Reflected XSS. This issue affects sidebarTabs: from n/a through 3.1.		
CVE-2025-26588	WordPress TTT Crop Plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound TTT Crop allows Reflected XSS. This issue affects TTT Crop: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-26589	WordPress IE CSS3 Support Plugin <= 2.0.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound IE CSS3 Support allows Reflected XSS. This issue affects IE CSS3 Support: from n/a through 2.0.1.	Patched by core rule	Y
CVE-2025-26626	GLPI Inventory Plugin vulnerable to reflective Cross-site Scripting	The GLPI Inventory Plugin handles various types of tasks for GLPI agents for the GLPI asset and IT management software package. Versions prior to 1.5.0 are vulnerable to reflective cross-site scripting, which may lead to executing javascript code. Version 1.5.0 fixes the issue.	Patched by core rule	Y
CVE-2025-2673	code-projects Payroll Management System home_employee.php cross site scripting	A vulnerability classified as problematic has been found in code-projects Payroll Management System 1.0. Affected is an unknown function of the file /home_employee.php. The manipulation of the argument division leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-26742	WordPress Gallery for Social Photo plugin <= 1.0.0.35 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GhozyLab Gallery for Social Photo allows Stored XSS.This issue affects Gallery for Social Photo: from n/a through 1.0.0.35.	Patched by core rule	Y
CVE-2025-26879	WordPress s2Member Plugin <= 241216 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Cristián Lávaque s2Member Pro allows Reflected XSS.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This issue affects s2Member Pro: from n/a through 241216.		
CVE-2025-26895	WordPress m1.DownloadList plugin <= 0.19 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in maennchen1.de m1.DownloadList allows DOM-Based XSS. This issue affects m1.DownloadList: from n/a through 0.19.	Patched by core rule	Y
CVE-2025-26914	WordPress Variable Inspector plugin <= 2.6.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bowo Variable Inspector allows Reflected XSS. This issue affects Variable Inspector: from n/a through 2.6.2.	Patched by core rule	Y
CVE-2025-26917	WordPress WP Templata plugin <= 1.0.7 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HasThemes WP Templata allows Reflected XSS. This issue affects WP Templata: from n/a through 1.0.7.	Patched by core rule	Y
CVE-2025-26918	WordPress Small Package Quotes – Unishippers Edition plugin <= 2.4.9 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in enituretechnology Small Package Quotes – Unishippers Edition allows Reflected XSS. This issue affects Small Package Quotes – Unishippers Edition: from n/a through 2.4.9.	Patched by core rule	Y
CVE-2025-26972	WordPress PrivateContent plugin <= 8.11.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound PrivateContent. This issue affects PrivateContent: from n/a through 8.11.5.	Patched by core rule	Y
CVE-2025-26984	WordPress SMS Alert Order Notifications – WooCommerce plugin <= 3.7.8 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Cozy Vision SMS Alert Order Notifications – WooCommerce allows Reflected XSS. This issue affects SMS Alert Order Notifications – WooCommerce: from n/a through 3.7.8.	Patched by core rule	Y
CVE-2025-26989	WordPress Zigaform – Form Builder Lite plugin <= 7.4.2 - Cross Site	Improper Neutralization of Input During Web Page Generation ('Cross-site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Scripting (XSS) vulnerability	Scripting') vulnerability in softdiscover Zigaform – Form Builder Lite allows Stored XSS. This issue affects Zigaform – Form Builder Lite: from n/a through 7.4.2.		
CVE-2025-2699	GetmeUK ContentTools Image cross site scripting	A vulnerability was found in GetmeUK ContentTools up to 1.6.16. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Image Handler. The manipulation of the argument onload leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-26994	WordPress Zigaform – Price Calculator & Cost Estimation Form Builder Lite plugin <= 7.4.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in softdiscover Zigaform – Price Calculator & Cost Estimation Form Builder Lite allows Stored XSS. This issue affects Zigaform – Price Calculator & Cost Estimation Form Builder Lite: from n/a through 7.4.2.	Patched by core rule	Y
CVE-2025-2700	michelson Dante Editor Insert Link cross site scripting	A vulnerability classified as problematic has been found in michelson Dante Editor up to 0.4.4. This affects an unknown part of the component Insert Link Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2709	Yonyou UFIDA ERP-NC login.jsp cross site scripting	A vulnerability has been found in Yonyou UFIDA ERP-NC 5.0 and classified as problematic. This vulnerability affects unknown code of the file /login.jsp. The manipulation of the argument key/redirect leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		but did not respond in any way.		
CVE-2025-27099	Tuleap allows XSS via the tracker names used in the semantic timeframe deletion message	Tuleap is an Open Source Suite to improve management of software developments and collaboration. Tuleap allows cross-site scripting (XSS) via the tracker names used in the semantic timeframe deletion message. A tracker administrator with a semantic timeframe used by other trackers could use this vulnerability to force other tracker administrators to execute uncontrolled code. This vulnerability is fixed in Tuleap Community Edition 16.4.99.1740067916 and Tuleap Enterprise Edition 16.4-5 and 16.3-10.	Patched by core rule	Y
CVE-2025-2710	Yonyou UFIDA ERP-NC menu.jsp cross site scripting	A vulnerability was found in Yonyou UFIDA ERP-NC 5.0 and classified as problematic. This issue affects some unknown processing of the file /menu.jsp. The manipulation of the argument flag leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2711	Yonyou UFIDA ERP-NC systop.jsp cross site scripting	A vulnerability was found in Yonyou UFIDA ERP-NC 5.0. It has been classified as problematic. Affected is an unknown function of the file /help/systop.jsp. The manipulation of the argument langcode leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-2712	Yonyou UFIDA ERP-NC top.jsp cross site scripting	A vulnerability was found in Yonyou UFIDA ERP-NC 5.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /help/top.jsp. The manipulation of the argument langcode leads to cross site scripting. The attack can be launched	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. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-2715	timschofield webERP Confirm Dispatch and Invoice Page ConfirmDispatch_Invoice.php cross site scripting	A vulnerability classified as problematic has been found in timschofield webERP up to 5.0.0.rc+13. This affects an unknown part of the file ConfirmDispatch_Invoice.php of the component Confirm Dispatch and Invoice Page. The manipulation of the argument Narrative 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. It is recommended to apply a patch to fix this issue. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-27155	In-memory stored Cross-site scripting (XSS) vulnerability in pineconesim	Pinecone is an experimental overlay routing protocol suite which is the foundation of the current P2P Matrix demos. The Pinecone Simulator (pineconesim) included in Pinecone up to commit ea4c337 is vulnerable to stored cross-site scripting. The payload storage is not permanent and will be wiped when restarting pineconesim.	Patched by core rule	Y
CVE-2025-27269	WordPress .htaccess Login block Plugin <= 0.9a - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound .htaccess Login block allows Reflected XSS. This issue affects .htaccess Login block: from n/a through 0.9a.	Patched by core rule	Y
CVE-2025-27271	WordPress DB Tables Import/Export Plugin <= 1.0.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound DB Tables Import/Export allows Reflected XSS. This issue affects DB Tables Import/Export: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-27273	WordPress Affiliate Links Manager Plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in winking Affiliate Links Manager allows Reflected XSS. This issue affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Affiliate Links Manager: from n/a through 1.0.		
CVE-2025-27275	WordPress WOO Codice Fiscale plugin <= 1.6.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in andrew_fisher WOO Codice Fiscale allows Reflected XSS. This issue affects WOO Codice Fiscale: from n/a through 1.6.3.	Patched by core rule	Y
CVE-2025-27278	WordPress AcuGIS Leaflet Maps Plugin <= 5.1.1.0 - Multiple Cross Site Scripting (XSS) vulnerabilities	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound AcuGIS Leaflet Maps allows Reflected XSS. This issue affects AcuGIS Leaflet Maps: from n/a through 5.1.1.0.	Patched by core rule	Y
CVE-2025-27279	WordPress Flashfader Plugin <= 1.1.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Flashfader allows Reflected XSS. This issue affects Flashfader: from n/a through 1.1.1.	Patched by core rule	Y
CVE-2025-27400	Magento vulnerable to stored XSS in theme config fields	Magento Long Term Support (LTS) is an unofficial, community-driven project provides an alternative to the Magento Community Edition e-commerce platform with a high level of backward compatibility. Versions prior to 20.12.3 and 20.13.1 contain a vulnerability that allows script execution in the admin panel which could lead to cross-site scripting against authenticated admin users. The attack requires an admin user with configuration access, so in practicality it is not very likely to be useful given that a user with this level of access is probably already a full admin. Versions 20.12.3 and 20.13.1 contain a patch for the issue.	Patched by core rule	Y
CVE-2025-27412	REDAXO allows Authenticated Reflected Cross Site Scripting - packages installation	REDAXO is a PHP-based CMS. In Redaxo from 5.0.0 through 5.18.2, the rex-api-result parameter is vulnerable to Reflected cross-site scripting (XSS) on the page of AddOns. This vulnerability is fixed in 5.18.3.	Patched by core rule	Y
CVE-2025-27417	WeGIA Contains a Stored Cross-Site Scripting (XSS)	WeGIA is an open source Web Manager for	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	in 'adicionar_status_atendido.php' via the 'status' parameter	Institutions with a focus on Portuguese language users. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the adicionar_status_atendido.php endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts into the status 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 3.2.16.		
CVE-2025-27418	WeGIA contains a Stored Cross-Site Scripting (XSS) in 'adicionar_tipo_atendido.php' via the 'tipo' parameter	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the adicionar_tipo_atendido.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 whenever the affected page is accessed by users, posing a significant security risk. This vulnerability is fixed in 3.2.16.	Patched by core rule	Y
CVE-2025-27420	WeGIA contains a Stored Cross-Site Scripting (XSS) in 'atendido_parentesco_adicionar.php' via the 'descricao' parameter	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the atendido_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 automatically whenever the affected page is accessed by users, posing a significant security risk. This vulnerability fix in 3.2.16.	Patched by core rule	Y
CVE-2025-27499	WeGIA has a stored Cross-Site Scripting (XSS) in 'processa_edicao_socio.php' via the 'socio_nome'	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A Stored Cross-Site Scripting	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	parameter	(XSS) vulnerability was identified in the processa_edicao_socio.php endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts into the socio_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. This vulnerability is fixed in 3.2.10.		
CVE-2025-27500	Cross Site Scripting potential in Ziti Console	OpenZiti is a free and open source project focused on bringing zero trust to any application. An endpoint(/api/upload) on the admin panel can be accessed without any form of authentication. This endpoint accepts an HTTP POST to upload a file which is then stored on the node and is available via URL. This can lead to a stored cross site scripting attack if the file uploaded contains malicious code and is then accessed and executed within the context of the user's browser. This function is no longer necessary as the ziti-console moves from a node server application to a single page application, and has been disabled. The vulnerability is fixed in 3.7.1.	Patched by core rule	Y
CVE-2025-28870	WordPress amoCRM WebForm plugin <= 1.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in amocrm amoCRM WebForm allows DOM-Based XSS. This issue affects amoCRM WebForm: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-28871	WordPress Block Spam By Math Reloaded plugin <= 2.2.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jwpegram Block Spam By Math Reloaded allows Stored XSS. This issue affects Block Spam By Math Reloaded: from n/a through 2.2.4.	Patched by core rule	Y
CVE-2025-28875	WordPress BP Email Assign Templates By shanebp plugin <= 1.6 - Cross-Site Scripting	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	vulnerability	shanebp BP Email Assign Templates allows Stored XSS. This issue affects BP Email Assign Templates: from n/a through 1.6.		
CVE-2025-28878	WordPress Awesome Surveys plugin <= 2.0.10 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Will Brubaker Awesome Surveys allows Stored XSS. This issue affects Awesome Surveys: from n/a through 2.0.10.	Patched by core rule	Y
CVE-2025-28879	WordPress Bee Layer Slider plugin <= 1.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in aumsrini Bee Layer Slider allows Stored XSS. This issue affects Bee Layer Slider: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-28895	WordPress Custom top bar plugin <= 2.0.2 - CSRF to Stored XSS vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sumanbiswas013 Custom top bar allows Stored XSS. This issue affects Custom top bar: from n/a through 2.0.2.	Patched by core rule	Y
CVE-2025-28905	WordPress Featured Posts Grid plugin <= 1.7 - CSRF to Stored XSS vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chaser324 Featured Posts Grid allows Stored XSS. This issue affects Featured Posts Grid: from n/a through 1.7.	Patched by core rule	Y
CVE-2025-28906	WordPress Skitter Slideshow plugin <= 2.5.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Thiago S.F. Skitter Slideshow allows Stored XSS. This issue affects Skitter Slideshow: from n/a through 2.5.2.	Patched by core rule	Y
CVE-2025-28907	WordPress WP Last Modified plugin <= 0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rahul Arora WP Last Modified allows Stored XSS. This issue affects WP Last Modified: from n/a through 0.1.	Patched by core rule	Y
CVE-2025-28908	WordPress pipDisqus plugin <= 1.6 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pipdig pipDisqus allows Stored XSS. This issue affects pipDisqus: from n/a through 1.6.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-28914	WordPress wordpress login form to anywhere plugin <= 0.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ajay Sharma wordpress login form to anywhere allows Stored XSS. This issue affects wordpress login form to anywhere: from n/a through 0.2.	Patched by core rule	Y
CVE-2025-28918	WordPress Featured Image Thumbnail Grid plugin <= 6.6.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in A. Jones Featured Image Thumbnail Grid allows Stored XSS. This issue affects Featured Image Thumbnail Grid: from n/a through 6.6.1.	Patched by core rule	Y
CVE-2025-28919	WordPress Easy Image Display plugin <= 1.2.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Shellbot Easy Image Display allows Stored XSS. This issue affects Easy Image Display: from n/a through 1.2.5.	Patched by core rule	Y
CVE-2025-28926	WordPress Post Read Time plugin <= 1.2.6 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in popeating Post Read Time allows Stored XSS. This issue affects Post Read Time: from n/a through 1.2.6.	Patched by core rule	Y
CVE-2025-28929	WordPress Tabbed Login Widget plugin <= 1.1.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vivek Marakana Tabbed Login Widget allows Stored XSS. This issue affects Tabbed Login Widget: from n/a through 1.1.2.	Patched by core rule	Y
CVE-2025-28930	WordPress List Mixcloud plugin <= 1.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rodolphe MOULIN List Mixcloud allows Stored XSS. This issue affects List Mixcloud: from n/a through 1.4.	Patched by core rule	Y
CVE-2025-28936	WordPress Lunar plugin <= 1.3.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sakurapixel Lunar allows Stored XSS. This issue affects Lunar: from n/a through 1.3.0.	Patched by core rule	Y
CVE-2025-28937	WordPress Lava Ajax Search plugin <= 1.1.9 -	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Cross Site Scripting (XSS) vulnerability	Generation ('Cross-site Scripting') vulnerability in lavacode Lava Ajax Search allows Stored XSS. This issue affects Lava Ajax Search: from n/a through 1.1.9.		
CVE-2025-28943	WordPress DP ALTerminator - Missing ALT manager Plugin <= 1.0.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mylo2h2s DP ALTerminator - Missing ALT manager allows Stored XSS. This issue affects DP ALTerminator - Missing ALT manager: from n/a through 1.0.2.	Patched by core rule	Y
CVE-2025-29771	HtmlSanitizer vulnerable to XSS when used with contentEditable	HtmlSanitizer is a client-side HTML Sanitizer. Versions prior to 2.0.3 have a cross-site scripting vulnerability when the sanitizer is used with a `contentEditable` element to set the elements `innerHTML` to a sanitized string produced by the package. If the code is particularly crafted to abuse the code beautifier, that runs AFTER sanitation. The issue is patched in version 2.0.3.	Patched by core rule	Y
CVE-2025-29782	WeGIA Cross-Site Scripting (XSS) Stored in endpoint `adicionar_tipo_docs_atendido.php` parameter `tipo`	WeGIA is Web manager for charitable institutions A Stored Cross-Site Scripting (XSS) vulnerability was identified in the `adicionar_tipo_docs_atendido.php` endpoint in versions of the WeGIA application prior to 3.2.17. This vulnerability allows attackers to inject malicious scripts into the `tipo` 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. Version 3.2.17 contains a patch for the issue.	Patched by core rule	Y
CVE-2025-29790	Contao allows cross-site scripting through SVG uploads	Contao is an Open Source CMS. Users can upload SVG files with malicious code, which is then executed in the back end and/or front end. This vulnerability is fixed in Contao 4.13.54, 5.3.30, or 5.5.6.	Patched by core rule	Y
CVE-2025-30219	RabbitMQ has XSS Vulnerability in an Error Message in Management UI	RabbitMQ is a messaging and streaming broker. Versions prior to 4.0.3 are vulnerable to a sophisticated attack that could modify virtual host name on disk	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and then make it unrecoverable (with other on disk file modifications) can lead to arbitrary JavaScript code execution in the browsers of management UI users. When a virtual host on a RabbitMQ node fails to start, recent versions will display an error message (a notification) in the management UI. The error message includes virtual host name, which was not escaped prior to open source RabbitMQ 4.0.3 and Tanzu RabbitMQ 4.0.3, 3.13.8. An attack that both makes a virtual host fail to start and creates a new virtual host name with an XSS code snippet or changes the name of an existing virtual host on disk could trigger arbitrary JavaScript code execution in the management UI (the user's browser). Open source RabbitMQ `4.0.3` and Tanzu RabbitMQ `4.0.3` and `3.13.8` patch the issue.		
CVE-2025-30349	N/A	Horde IMP through 6.2.27, as used with Horde Application Framework through 5.2.23, allows XSS that leads to account takeover via a crafted text/html e-mail message with an onerror attribute (that may use base64-encoded JavaScript code), as exploited in the wild in March 2025.	Patched by core rule	Y
CVE-2025-30527	WordPress My Bootstrap Menu plugin <= 1.2.1 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in codetoolbox My Bootstrap Menu allows Stored XSS. This issue affects My Bootstrap Menu: from n/a through 1.2.1.	Patched by core rule	Y
CVE-2025-30530	WordPress AI Preloader plugin <= 1.0.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Atikul AI Preloader allows Stored XSS. This issue affects AI Preloader: from n/a through 1.0.2.	Patched by core rule	Y
CVE-2025-30532	WordPress Weather Layer plugin <= 4.2.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		MorganF Weather Layer allows Stored XSS. This issue affects Weather Layer: from n/a through 4.2.1.		
CVE-2025-30533	WordPress Message ticker plugin <= 9.3 - Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gopiplus Message ticker allows Stored XSS. This issue affects Message ticker: from n/a through 9.3.	Patched by core rule	Y
CVE-2025-30536	WordPress Beautiful Link Preview plugin <= 1.5.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in zeitwesentech Beautiful Link Preview allows Stored XSS. This issue affects Beautiful Link Preview: from n/a through 1.5.0.	Patched by core rule	Y
CVE-2025-30537	WordPress Upload Quota per User - <= <= 1.3 Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Cristian Sarov Upload Quota per User allows Stored XSS. This issue affects Upload Quota per User: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-30539	WordPress BMo Expo plugin <= 1.0.15 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Benedikt Mo BMo Expo allows Stored XSS. This issue affects BMo Expo: from n/a through 1.0.15.	Patched by core rule	Y
CVE-2025-30540	WordPress AvaiBook plugin <= 1.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in avaibook AvaiBook allows Stored XSS. This issue affects AvaiBook: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-30545	WordPress issuuPress plugin <= 1.3.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pixeline issuuPress allows Stored XSS. This issue affects issuuPress: from n/a through 1.3.2.	Patched by core rule	Y
CVE-2025-30551	WordPress Pretty file links plugin <= 0.9 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in smartredfox Pretty file links allows Stored XSS. This issue affects Pretty file links: from n/a through 0.9.	Patched by core rule	Y
CVE-2025-30553	WordPress GMO Font	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Agent plugin <= 1.6 - Cross Site Scripting (XSS) vulnerability	Input During Web Page Generation ('Cross-site Scripting') vulnerability in Z.com byGMO GMO Font Agent allows Stored XSS. This issue affects GMO Font Agent: from n/a through 1.6.	rule	
CVE-2025-30566	WordPress Clink - <= <= 1.2.2 Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aryan Themes Clink allows DOM-Based XSS. This issue affects Clink: from n/a through 1.2.2.	Patched by core rule	Y
CVE-2025-30573	WordPress My Default Post Content - <= <= 0.7.3 Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mrdenny My Default Post Content allows Stored XSS. This issue affects My Default Post Content: from n/a through 0.7.3.	Patched by core rule	Y
CVE-2025-30574	WordPress Mobile Navigation - <= <= 1.5 Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jenst Mobile Navigation allows Stored XSS. This issue affects Mobile Navigation: from n/a through 1.5.	Patched by core rule	Y
CVE-2025-30575	WordPress Login Redirect - <= <= 1.0.5 Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Arefly Login Redirect allows Stored XSS. This issue affects Login Redirect: from n/a through 1.0.5.	Patched by core rule	Y
CVE-2025-30593	WordPress Include URL - <= <= 0.3.5 Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in samsk Include URL allows Stored XSS. This issue affects Include URL: from n/a through 0.3.5.	Patched by core rule	Y
CVE-2025-30595	WordPress include-file - <= <= 1 Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tstafford include-file allows Stored XSS. This issue affects include-file: from n/a through 1.	Patched by core rule	Y
CVE-2025-30597	WordPress IG Shortcodes - <= <= 3.1 Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in iografica IG Shortcodes allows DOM-Based XSS. This issue affects IG Shortcodes: from n/a through 3.1.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-30599	WordPress WP Parallax Content Slider plugin <= 0.9.8 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wp-maverick WP Parallax Content Slider allows Stored XSS. This issue affects WP Parallax Content Slider: from n/a through 0.9.8.	Patched by core rule	Y
CVE-2025-30600	WordPress WP Hotjar plugin <= 0.0.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in thiagogsrwp WP Hotjar allows Stored XSS. This issue affects WP Hotjar: from n/a through 0.0.3.	Patched by core rule	Y
CVE-2025-30602	WordPress Related Posts via Categories plugin <= 2.1.2 - CSRF to Stored XSS vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in alphasis Related Posts via Categories allows Stored XSS. This issue affects Related Posts via Categories: from n/a through 2.1.2.	Patched by core rule	Y
CVE-2025-30606	WordPress Easy Page Transition plugin <= 1.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Logan Carlile Easy Page Transition allows Stored XSS. This issue affects Easy Page Transition: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-30610	WordPress WP Social Widget - <= <= 2.2.6 Cross Site Scripting (XSS) Vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in catchsquare WP Social Widget allows Stored XSS. This issue affects WP Social Widget: from n/a through 2.2.6.	Patched by core rule	Y
CVE-2025-30623	WordPress wA11y – The Web Accessibility Toolbox plugin <= 1.0.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rachel Cherry wA11y – The Web Accessibility Toolbox allows Stored XSS. This issue affects wA11y – The Web Accessibility Toolbox: from n/a through 1.0.3.	Patched by core rule	Y

INDUSFACE™

Indusface is a leading application security SaaS company, securing over 5,000 customers across 95 countries with its award-winning platform. Funded by institutional investors, it has been a category leader in Gartner Peer Insights™ for the past three years.

The industry's only AI-powered, all-in-one AppSec platform helps businesses discover, detect, remediate, and protect web applications and APIs at internet scale, backed by a 100% uptime guarantee.

Gartner
Peer Insights
Customers'
Choice 2024™

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

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

CONTACT US - +91 265 6133021 | +1 866 537 82