INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

June 2025

The total zero-day vulnerabilities count for June month: 527

Command Injection	SQL Injection	SSRF	Path Traversal	Cross-Site Scripting	XXE
54	305	10	51	104	3

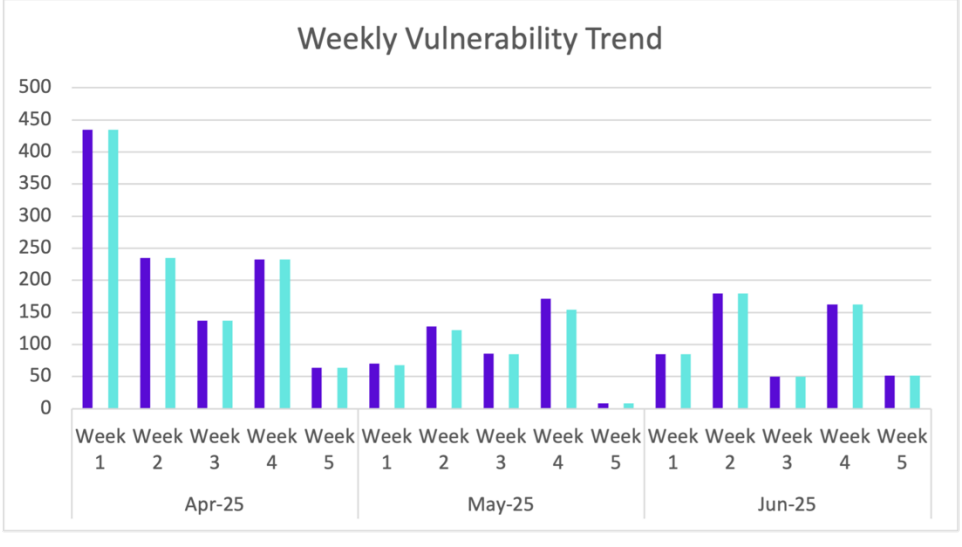
Zero-day vulnerabilities protected through core rules	527
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities found by Indusface WAS	527

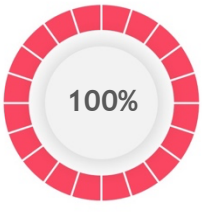
- To enable custom rules, please contact support@indusface.com
- Learn more about zero-day vulnerabilities, detection, and prevention, here

Vulnerability Trend:

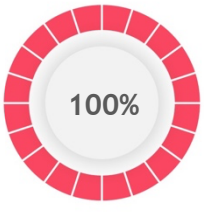
The weekly trend displays the total number of vulnerabilities discovered and the type of protection provided for the last quarter.

Weekly Vulnerability Trend



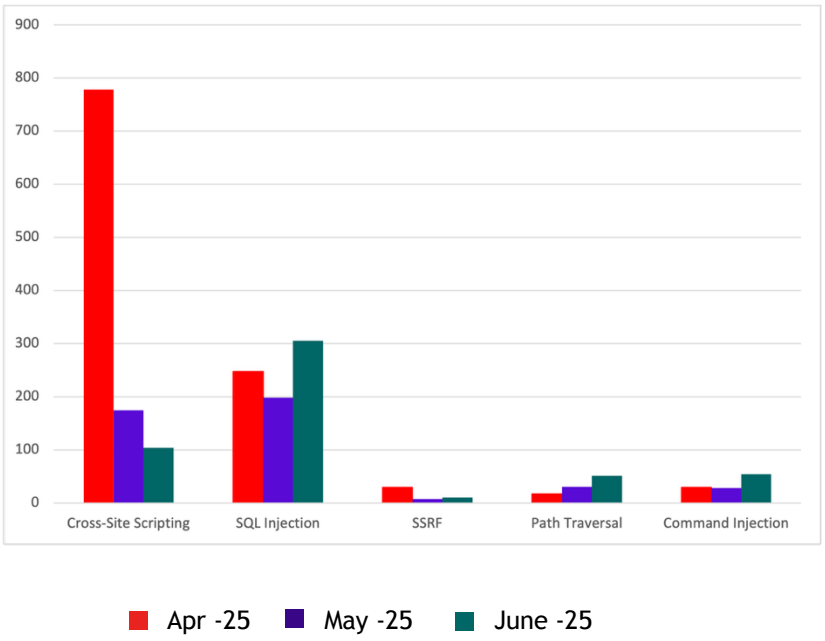


of the zero-day vulnerabilities were protected by the core rules in the last month



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

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-1753	Command Injection in LLama-Index CLI in run-llama/llama_index	LLama-Index CLI version v0.12.20 contains an OS command injection vulnerability. The vulnerability arises from the improper handling of the `--files` argument, which is directly passed into `os.system`. An attacker who controls the content of this argument can inject and execute arbitrary shell commands. This vulnerability can be exploited locally if the attacker has control over the CLI arguments, and remotely if a web application calls the LLama-Index CLI with a user-controlled filename. This issue can lead to arbitrary code execution on the affected system.	Patched by core rule	Y
CVE-2025-48390	FreeScout Vulnerable to Remote Code Execution (RCE)	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.178, FreeScout is vulnerable to code injection due to insufficient validation of user input in the php_path parameter. The backticks characters are not removed, as well as tabulation is not removed. When checking user input, the file_exists function is also called to check for the presence of such a file (folder) in the file system. A user with the administrator role can create a translation for the language, which will create a folder in the file system. Further in tools.php, the user can specify the path to this folder as php_path, which will lead to the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		execution of code in backticks. This issue has been patched in version 1.8.178.		
CVE-2025-48471	FreeScout Vulnerable to Arbitrary File Upload	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.179, the application does not check or performs insufficient checking of files uploaded to the application. This allows files to be uploaded with the phtml and phar extensions, which can lead to remote code execution if the Apache web server is used. This issue has been patched in version 1.8.179.	Patched by core rule	Y
CVE-2025-48492	GetSimple CMS RCE in Edit component	GetSimple CMS is a content management system. In versions starting from 3.3.16 to 3.3.21, an authenticated user with access to the Edit component can inject arbitrary PHP into a component file and execute it via a crafted query string, resulting in Remote Code Execution (RCE). This issue is set to be patched in version 3.3.22.	Patched by core rule	Y
CVE-2024-57783	N/A	The desktop application in Dot through 0.9.3 allows XSS and resultant command execution because user input and LLM output are appended to the DOM with innerHTML (in render.js), and because the Electron window can access Node.js APIs.	Patched by core rule	Y
CVE-2025-48710	N/A	kro (Kube Resource Orchestrator) 0.1.0 before 0.2.1 allows users (with permission to create or modify ResourceGraphDefinition resources) to supply arbitrary container images. This can lead to a confused-deputy scenario where kro's controllers deploy and run attacker-controlled images, resulting in unauthenticated remote code execution on cluster nodes.	Patched by core rule	Y
CVE-2025-49004	Hijacking Caido instance during the initial setup via DNS Rebinding to achieve RCE	Caido is a web security auditing toolkit. Prior to version 0.48.0, due to the lack of protection for DNS rebinding, Caido can be loaded on an attacker-controlled domain. This allows a malicious website to hijack the authentication flow of Caido and achieve code execution. A malicious website loaded in the browser can hijack the locally running Caido instance and achieve remote command execution during the initial setup. Even if the Caido instance is already configured, an attacker can initiate the authentication flow by performing DNS rebinding. In this case, the victim needs to authorize the request on dashboard.caido.io. Users	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		should upgrade to version 0.48.0 to receive a patch.		
CVE-2025-49008	Atheos Improper Input Validation Vulnerability Enables RCE in Common.php	Atheos is a self-hosted browser-based cloud integrated development environment. Prior to version 6.0.4, improper use of `escapeshellcmd()` in `/components/codegit/traits/execute.php` allows argument injection, leading to arbitrary command execution. Atheos administrators and users of vulnerable versions are at risk of data breaches or server compromise. Version 6.0.4 introduces a `Common::safe_execute` function that sanitizes all arguments using `escapeshellarg()` prior to execution and migrated all components potentially vulnerable to similar exploits to use this new templated execution system.	Patched by core rule	Y
CVE-2025-49013	WilderForge vulnerable to code Injection via GitHub Actions Workflows	WilderForge is a Wildermyth coremodding API. A critical vulnerability has been identified in multiple projects across the WilderForge organization. The issue arises from unsafe usage of `${{ github.event.review.body }}` and other user controlled variables directly inside shell script contexts in GitHub Actions workflows. This introduces a code injection vulnerability: a malicious actor submitting a crafted pull request review containing shell metacharacters or commands could execute arbitrary shell code on the GitHub Actions runner. This can lead to arbitrary command execution with the permissions of the workflow, potentially compromising CI infrastructure, secrets, and build outputs. Developers who maintain or contribute to the repos WilderForge/WilderForge, WilderForge/ExampleMod, WilderForge/WilderWorkspace, WilderForge/WildermythGameProvider, WilderForge/AutoSplitter, WilderForge/SpASM, WilderForge/thrixlvault, WilderForge/MassHash, and/or WilderForge/DLC_Disabler; as well as users who fork any of the above repositories and reuse affected GitHub Actions workflows, are affected. End users of any the above software and users who only install pre-built releases or artifacts are not affected. This vulnerability does not impact runtime behavior of the software or compiled outputs unless those outputs were produced	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		during exploitation of this vulnerability. A current workaround is to disable GitHub Actions in affected repositories, or remove the affected workflows.		
CVE-2025-49113	N/A	Roundcube Webmail before 1.5.10 and 1.6.x before 1.6.11 allows remote code execution by authenticated users because the _from parameter in a URL is not validated in program/actions/settings/upload.php, leading to PHP Object Deserialization.	Patched by core rule	Y
CVE-2025-49141	HaxCMS-PHP Command Injection Vulnerability	HAX CMS PHP allows users to manage their microsite universe with a PHP backend. Prior to version 11.0.3, the `gitImportSite` functionality obtains a URL string from a POST request and insufficiently validates user input. The `set_remote` function later passes this input into `proc_open`, yielding OS command injection. An authenticated attacker can craft a URL string that bypasses the validation checks employed by the `filter_var` and `strpos` functions in order to execute arbitrary OS commands on the backend server. The attacker can exfiltrate command output via an HTTP request. Version 11.0.3 contains a patch for the issue.	Patched by core rule	Y
CVE-2025-5438	Linksys RE6500/RE6250/RE6300/RE6350/RE7000/RE9000 WPS command injection	A vulnerability was found in Linksys RE6500, RE6250, RE6300, RE6350, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. It has been declared as critical. Affected by this vulnerability is the function WPS of the file /goform/WPS. The manipulation of the argument PIN 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-2025-5439	Linksys RE6500/RE6250/RE6300/RE6350/RE7000/RE9000 verifyFacebookLike os command injection	A vulnerability was found in Linksys RE6500, RE6250, RE6300, RE6350, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. It has been rated as critical. Affected by this issue is the function verifyFacebookLike of the file /goform/verifyFacebookLike. The manipulation of the argument uid/accessToken leads to os 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		but did not respond in any way.		
CVE-2025-5440	Linksys RE6500/RE6250/RE6300/RE6350/RE7000/RE9000 NTP os command injection	A vulnerability classified as critical has been found in Linksys RE6500, RE6250, RE6300, RE6350, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This affects the function NTP of the file /goform/NTP. The manipulation of the argument manual_year_select/manual_month_select/manual_day_select/manual_hour_select/manual_min_select/manual_sec_select 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. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-5441	Linksys RE6500/RE6250/RE6300/RE6350/RE7000/RE9000 setDeviceURL os command injection	A vulnerability classified as critical was found in Linksys RE6500, RE6250, RE6300, RE6350, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This vulnerability affects the function setDeviceURL of the file /goform/setDeviceURL. The manipulation of the argument DeviceURL 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-2025-5442	Linksys RE6500/RE6250/RE6300/RE6350/RE7000/RE9000 RP_pingGatewayByBBS os command injection	A vulnerability, which was classified as critical, has been found in Linksys RE6500, RE6250, RE6300, RE6350, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This issue affects the function RP_pingGatewayByBBS of the file /goform/RP_pingGatewayByBBS. The manipulation of the argument ip/nm/gw leads to os 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-2025-5443	Linksys RE6500/RE6250/RE6300/RE6350/RE7000/RE9000 wirelessAdvancedHidden os command injection	A vulnerability, which was classified as critical, was found in Linksys RE6500, RE6250, RE6300, RE6350, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. Affected is the function wirelessAdvancedHidden of the file /goform/wirelessAdvancedHidden. The manipulation of the argument ExtChSelector/24GSelector/5GSelector leads to os	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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.		
CVE-2025-5444	Linksys RE6500/RE6250/RE6300/RE6350/RE7000/RE9000 RP_UpgradeFWByBBS os command injection	A vulnerability has been found in Linksys RE6500, RE6250, RE6300, RE6350, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001 and classified as critical. Affected by this vulnerability is the function RP_UpgradeFWByBBS of the file /goform/RP_UpgradeFWByBBS. The manipulation of the argument type/ch/ssidhex/security/extch/pwd/mode/ip/nm/gw leads to os 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-2025-5445	Linksys RE6500/RE6250/RE6300/RE6350/RE7000/RE9000 RP_checkFWByBBS os command injection	A vulnerability was found in Linksys RE6500, RE6250, RE6300, RE6350, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001 and classified as critical. Affected by this issue is the function RP_checkFWByBBS of the file /goform/RP_checkFWByBBS. The manipulation of the argument type/ch/ssidhex/security/extch/pwd/mode/ip/nm/gw leads to os 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-2025-5446	Linksys RE6500/RE6250/RE6300/RE6350/RE7000/RE9000 RP_checkCredentialsByBBS os command injection	A vulnerability was found in Linksys RE6500, RE6250, RE6300, RE6350, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. It has been classified as critical. This affects the function RP_checkCredentialsByBBS of the file /goform/RP_checkCredentialsByBBS. The manipulation of the argument pwd 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. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-5447	Linksys RE6500/RE6250/RE6300/RE6350/RE7000/RE9000 ssid1MACFilter os	A vulnerability was found in Linksys RE6500, RE6250, RE6300, RE6350, RE7000 and RE9000	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	command injection	1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. It has been declared as critical. This vulnerability affects the function ssid1MACFilter of the file /goform/ssid1MACFilter. The manipulation of the argument apselect_%d/newap_text_%d 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.		
CVE-2025-5502	TOTOLINK X15 formMapReboot command injection	A vulnerability, which was classified as critical, has been found in TOTOLINK X15 1.0.0-B20230714.1105. Affected by this issue is the function formMapReboot of the file /boafrm/formMapReboot. The manipulation of the argument deviceMacAddr 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-2025-5504	TOTOLINK X2000R formWsc command injection	A vulnerability has been found in TOTOLINK X2000R 1.0.0-B20230726.1108 and classified as critical. This vulnerability affects unknown code of the file /boafrm/formWsc. The manipulation of the argument peerRptPin leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-5515	TOTOLINK X2000R formMapDel command injection	A vulnerability, which was classified as critical, has been found in TOTOLINK X2000R 1.0.0-B20230726.1108. Affected by this issue is some unknown functionality of the file /boafrm/formMapDel. The manipulation of the argument devicemac1 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-2025-5525	Jrohy trojan linux.go LogChan os command injection	A vulnerability was found in Jrohy trojan up to 2.15.3. It has been declared as critical. This vulnerability affects the function LogChan of the file trojan/util/linux.go. The manipulation of the argument c leads to os command injection. The attack can be initiated remotely. The complexity of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used.		
CVE-2025-5571	D-Link DCS-932L setSystemAdmin os command injection	A vulnerability was found in D-Link DCS-932L 2.18.01. It has been classified as critical. Affected is the function setSystemAdmin of the file /setSystemAdmin. The manipulation of the argument AdminID 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. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-5573	D-Link DCS-932L setSystemWizard setSystemControl os command injection	A vulnerability was found in D-Link DCS-932L 2.18.01. It has been rated as critical. Affected by this issue is the function setSystemWizard/setSystemControl of the file /setSystemWizard. The manipulation of the argument AdminID leads to os command injection. The attack may be launched 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-2025-5620	D-Link DIR-816 setipsec_config os command injection	A vulnerability, which was classified as critical, was found in D-Link DIR-816 1.10CNB05. Affected is the function setipsec_config of the file /goform/setipsec_config. The manipulation of the argument localIP/remoteIP 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. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-5621	D-Link DIR-816 qosClassifier os command injection	A vulnerability has been found in D-Link DIR-816 1.10CNB05 and classified as critical. Affected by this vulnerability is the function qosClassifier of the file /goform/qosClassifier. The manipulation of the argument dip_address/sip_address leads to os command injection. The attack can be launched 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-2025-5695	FLIR AX8 Backend subscriptions.php subscribe_to_alarm	A vulnerability classified as critical has been found in FLIR AX8 up to 1.46.16. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	command injection	affects the function subscribe_to_spot/subscribe_to_delta/subscribe_to_alarm of the file /usr/www/application/models/subscriptions.php of the component Backend. 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. Upgrading to version 1.55.16 is able to address this issue. It is recommended to upgrade the affected component.		
CVE-2025-5763	Tenda CP3 apollo sub_F3C8C command injection	A vulnerability has been found in Tenda CP3 11.10.00.2311090948 and classified as critical. Affected by this vulnerability is the function sub_F3C8C of the file apollo. The manipulation leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-1243	Remote code execution and local privilege escalation in Wazuh Windows agent via NetNTLMv2 hash theft	Improper input validation in the Wazuh agent for Windows prior to version 4.8.0 allows an attacker with control over the Wazuh server or agent key to configure the agent to connect to a malicious UNC path. This results in the leakage of the machine account NetNTLMv2 hash, which can be relayed for remote code execution or used to escalate privileges to SYSTEM via AD CS certificate forging and other similar attacks.	Patched by core rule	Y
CVE-2025-2172	N/A	Aviatrix Controller versions prior to 7.1.4208, 7.2.5090, and 8.0.0 fail to sanitize user input prior to passing the input to command line utilities, allowing command injection via special characters in filenames	Patched by core rule	Y
CVE-2025-34030	sar2html OS Command Injection	An OS command injection vulnerability exists in sar2html version 3.2.2 and prior via the plot parameter in index.php. The application fails to sanitize user-supplied input before using it in a system-level context. Remote, unauthenticated attackers can inject shell commands by appending them to the plot parameter (e.g., ?plot=;id) in a crafted GET request. The output of the command is displayed in the application's interface after interacting with the host selection UI. Successful exploitation leads to arbitrary command execution on the underlying system.	Patched by core rule	Y
CVE-2025-3515	Drag and Drop Multiple File Upload for Contact Form 7 <= 1.3.8.9 - Unauthenticated Arbitrary File Upload via Insufficient Blacklist Checks	The Drag and Drop Multiple File Upload for Contact Form 7 plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in all	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		versions up to, and including, 1.3.8.9. This makes it possible for unauthenticated attackers to bypass the plugin's blacklist and upload .phar or other dangerous file types on the affected site's server, which may make remote code execution possible on the servers that are configured to handle .phar files as executable PHP scripts, particularly in default Apache+mod_php configurations where the file extension is not strictly validated before being passed to the PHP interpreter.		
CVE-2025-49596	MCP Inspector proxy server lacks authentication between the Inspector client and proxy	The MCP inspector is a developer tool for testing and debugging MCP servers. Versions of MCP Inspector below 0.14.1 are vulnerable to remote code execution due to lack of authentication between the Inspector client and proxy, allowing unauthenticated requests to launch MCP commands over stdio. Users should immediately upgrade to version 0.14.1 or later to address these vulnerabilities.	Patched by core rule	Y
CVE-2025-49597	handcraftedinthealps goodby-csv Potential Gadget Chain allowing Remote Code Execution	handcraftedinthealps goodby-csv is a highly memory efficient, flexible and extendable open-source CSV import/export library. Prior to 1.4.3, goodby-csv could be used as part of a chain of methods that is exploitable when an insecure deserialization vulnerability exists in an application. This so-called "gadget chain" presents no direct threat but is a vector that can be used to achieve remote code execution if the application deserializes untrusted data due to another vulnerability. The problem is patched with Version 1.4.3.	Patched by core rule	Y
CVE-2025-49824	conda-smithy Insecure Encryption Vulnerable to Oracle Padding Attack	conda-smithy is a tool for combining a conda recipe with configurations to build using freely hosted CI services into a single repository. Prior to version 3.47.1, the travis_encrypt_binstar_token implementation in the conda-smithy package has been identified as vulnerable to an Oracle Padding Attack. This vulnerability results from the use of an outdated and insecure padding scheme during RSA encryption. A malicious actor with access to an oracle system can exploit this flaw by iteratively submitting modified ciphertexts and analyzing responses to infer the plaintext without possessing the private key. This issue has been patched in version 3.47.1.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-50201	WeGIA OS Command Injection in debug_info.php parameter 'branch'	WeGIA is a web manager for charitable institutions. Prior to version 3.4.2, an OS Command Injection vulnerability was identified in the /html/configuracao/debug_info.php endpoint. The branch parameter is not properly sanitized before being concatenated and executed in a shell command on the server's operating system. This flaw allows an unauthenticated attacker to execute arbitrary commands on the server with the privileges of the web server user (www-data). This issue has been patched in version 3.4.2.	Patched by core rule	Y
CVE-2025-52480	Registrator.jl Argument Injection Vulnerability	Registrator is a GitHub app that automates creation of registration pull requests for julia packages to the General registry. Prior to version 1.9.5, if the clone URL returned by GitHub is malicious (or can be injected using upstream vulnerabilities), an argument injection is possible in the `gettreesha()` function. This can then lead to a potential remote code execution. Users should upgrade immediately to v1.9.5 to receive a patch. All prior versions are vulnerable. No known workarounds are available.	Patched by core rule	Y
CVE-2025-52483	Registrator.jl Vulnerable to Argument Injection and Command Injection	Registrator is a GitHub app that automates creation of registration pull requests for julia packages to the General registry. Prior to version 1.9.5, if the clone URL returned by GitHub is malicious (or can be injected using upstream vulnerabilities) a shell script injection can occur within the `withpasswd` function. Alternatively, an argument injection is possible in the `gettreesha `function. either of these can then lead to a potential RCE. Users should upgrade immediately to v1.9.5 to receive a fix. All prior versions are vulnerable. No known workarounds are available.	Patched by core rule	Y
CVE-2025-52572	Hikka vulnerable to RCE through dangling web interface	Hikka, a Telegram userbot, has vulnerability affects all users on all versions of Hikka. Two scenarios are possible. 1. Web interface does not have an authenticated session: attacker can use his own Telegram account to gain RCE to the server by authorizing in the dangling web interface. 2. Web interface does have an authenticated session: due to insufficient warning in the authentication message, users were tempted to click "Allow" in the "Allow web application ops" menu. This gave an attacker access not	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		only to remote code execution, but also to Telegram accounts of owners. Scenario number 2 is known to have been exploited in the wild. No known patches are available, but some workarounds are available. Use `--no-web` flag and do not start userbot without it; after authorizing in the web interface, close the port on the server and/or start the userbot with `--no-web` flag; and do not click "Allow" in your helper bot unless it is your explicit action that needs to be allowed.		
CVE-2025-5309	Remote Support & Privileged Remote Access server side template injection	The chat feature within Remote Support (RS) and Privileged Remote Access (PRA) is vulnerable to a Server-Side Template Injection vulnerability which can lead to remote code execution.	Patched by core rule	Y
CVE-2025-6102	Wifi-soft UniBox Controller logout.php os command injection	A vulnerability classified as critical was found in Wifi-soft UniBox Controller up to 20250506. Affected by this vulnerability is an unknown functionality of the file /authentication/logout.php. The manipulation of the argument mac_address leads to os 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-2025-6103	Wifi-soft UniBox Controller test_accesscodelogin.php os command injection	A vulnerability, which was classified as critical, has been found in Wifi-soft UniBox Controller up to 20250506. Affected by this issue is some unknown functionality of the file /billing/test_accesscodelogin.php. The manipulation of the argument Password leads to os 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-2025-6104	Wifi-soft UniBox Controller pms_check.php os command injection	A vulnerability, which was classified as critical, was found in Wifi-soft UniBox Controller up to 20250506. This affects an unknown part of the file /billing/pms_check.php. The manipulation of the argument ipaddress 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. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-6218	RARLAB WinRAR Directory	RARLAB WinRAR Directory	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Traversal Remote Code Execution Vulnerability	Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of RARLAB WinRAR. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of file paths within archive files. A crafted file path can cause the process to traverse to unintended directories. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-27198.	rule	
CVE-2025-6220	Ultimate Addons for Contact Form 7 <= 3.5.12 - Authenticated (Administrator+) Arbitrary File Upload via 'save_options'	The Ultra Addons for Contact Form 7 plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'save_options' function in all versions up to, and including, 3.5.12. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	Patched by core rule	Y
CVE-2025-6335	DedeCMS Template dedetag.class.php command injection	A vulnerability was found in DedeCMS up to 5.7.2 and classified as critical. This issue affects some unknown processing of the file /include/dedetag.class.php of the component Template Handler. The manipulation of the argument notes leads to 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-2025-6485	TOTOLINK A3002R formWlSiteSurvey os command injection	A vulnerability was found in TOTOLINK A3002R 1.1.1-B20200824.0128. It has been classified as critical. This affects the function formWlSiteSurvey of the file /boafrm/formWlSiteSurvey. The manipulation of the argument wlanif 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-2025-6618	TOTOLINK CA300-PoE wps.so SetWLanApcliSettings os command injection	A vulnerability was found in TOTOLINK CA300-PoE 6.2c.884. It has been classified as critical. Affected is the function SetWLanApcliSettings of the file wps.so. The manipulation of the argument PIN 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-2025-6619	TOTOLINK CA300-PoE	A vulnerability was found in	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	upgrade.so setUpgradeFW os command injection	TOTOLINK CA300-PoE 6.2c.884. It has been declared as critical. Affected by this vulnerability is the function setUpgradeFW of the file upgrade.so. The manipulation of the argument FileName leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	rule	
CVE-2025-6620	TOTOLINK CA300-PoE upgrade.so setUpgradeUboot os command injection	A vulnerability was found in TOTOLINK CA300-PoE 6.2c.884. It has been rated as critical. Affected by this issue is the function setUpgradeUboot of the file upgrade.so. The manipulation of the argument FileName 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-2025-6621	TOTOLINK CA300-PoE ap.so QuickSetting os command injection	A vulnerability classified as critical has been found in TOTOLINK CA300-PoE 6.2c.884. This affects the function QuickSetting of the file ap.so. The manipulation of the argument hour/minute 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

Path Traversal Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-48370	auth-js Vulnerable to Insecure Path Routing from Malformed User Input	auth-js is an isomorphic Javascript library for Supabase Auth. Prior to version 2.69.1, the library functions getUserById, deleteUser, updateUserById, listFactors and deleteFactor did not require the user supplied values to be valid UUIDs. This could lead to a URL path traversal, resulting in the wrong API function being called. Implementations that follow security best practice and validate user controlled inputs, such as the userId are not affected by this. This issue has been patched in version 2.69.1.	Patched by core rule	Y
CVE-2025-5160	H3C SecCenter SMP-E1114P02 download path traversal	A vulnerability classified as problematic has been found in H3C SecCenter SMP-E1114P02 up to 20250513. Affected is the function Download of the file /packetCaptureStrategy/download. The manipulation of the argument Name 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-2025-5161	H3C SecCenter SMP-E1114P02 download operationDailyOut path traversal	A vulnerability classified as problematic was found in H3C SecCenter SMP-E1114P02 up to 20250513. Affected by this vulnerability is the function operationDailyOut of the file /safeEvent/download. The manipulation of the argument filename leads to path 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.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-5328	chshcms mccms Backups.php restore_del path traversal	A vulnerability was found in chshcms mccms 2.7. It has been declared as critical. This vulnerability affects the function restore_del of the file /sys/apps/controllers/admin/Backups.php. The manipulation of the argument dirs 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-2025-5380	ashinigit 天青一白 XueShengZhuSu 学生住宿管理系统 Image File Upload upload path traversal	A vulnerability, which was classified as critical, has been found in ashinigit 天青一白 XueShengZhuSu 学生住宿管理系统 up to 4d3f0ada0e71482c1e51fd5f5615e5a3d8bcbfbb. This issue affects some unknown processing of the file /upload/ of the component Image File Upload. 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. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available.	Patched by core rule	Y
CVE-2025-5381	Yifang CMS Admin Panel downloadFile path traversal	A vulnerability, which was classified as problematic, was found in Yifang CMS up to 2.0.2. Affected is the function downloadFile of the file /api/File/downloadFile of the component Admin Panel. 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.	Patched by core rule	Y
CVE-2025-5385	JeeWMS cgformTemplateController.do doAdd path traversal	A vulnerability was found in JeeWMS up to 20250504. It has been declared as critical. This vulnerability affects the function doAdd of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/cgformTemplateController.do?doAdd. The manipulation leads to path traversal. The attack can be initiated remotely. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available.		

CVE-2011-10007	File::Find::Rule through 0.34 for Perl is vulnerable to Arbitrary Code Execution when `grep()` encounters a crafted file name	File::Find::Rule through 0.34 for Perl is vulnerable to Arbitrary Code Execution when `grep()` encounters a crafted filename.
		
		A file handle is opened with the 2 argument form of `open()` allowing an attacker controlled filename to provide the MODE parameter to `open()`, turning the filename into a command to be executed.
		
		Example:
		
		$ mkdir /tmp/poc; echo > "/tmp/poc/|id"
		$ perl -MFile::Find::Rule \
		-E 'File::Find::Rule->grep("foo")->in("/tmp/poc")'
		uid=1000(user) gid=1000(user) groups=1000(user),100(users)
			Patched by core rule	Y

CVE-2024-12718	Bypass extraction filter to modify file metadata outside extraction directory	Allows modifying some file metadata (e.g. last modified) with filter="data" or file permissions (chmod) with filter="tar" of files outside the extraction directory. You are affected by this vulnerability if using the tarfile module to extract untrusted tar archives using TarFile.extractall() or TarFile.extract() using the filter= parameter with a value of "data" or "tar". See the tarfile extraction filters documentation https://docs.python.org/3/library/tarfile.html#tarfile-extraction-filter for more information. Only Python versions 3.12 or later are affected by these vulnerabilities, earlier versions don't include the extraction filter feature.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Note that for Python 3.14 or later the default value of filter= changed from "no filtering" to `"data", so if you are relying on this new default behavior then your usage is also affected. Note that none of these vulnerabilities significantly affect the installation of source distributions which are tar archives as source distributions already allow arbitrary code execution during the build process. However when evaluating source distributions it's important to avoid installing source distributions with suspicious links.		
CVE-2025-4138	Bypassing extraction filter to create symlinks to arbitrary targets outside extraction directory	Allows the extraction filter to be ignored, allowing symlink targets to point outside the destination directory, and the modification of some file metadata. You are affected by this vulnerability if using the tarfile module to extract untrusted tar archives using TarFile.extractall() or TarFile.extract() using the filter= parameter with a value of "data" or "tar". See the tarfile extraction filters documentation https://docs.python.org/3/library/tarfile.html#tarfile-extraction-filter for more information. Only Python versions 3.12 or later are affected by these vulnerabilities, earlier versions don't include the extraction filter feature. Note that for Python 3.14 or later the default value of filter= changed from "no filtering" to `"data", so if you are relying on this new default behavior then your usage is also affected. Note that none of these vulnerabilities significantly affect the installation of source distributions which are tar archives as source distributions already allow arbitrary code execution	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		during the build process. However when evaluating source distributions it's important to avoid installing source distributions with suspicious links.		
CVE-2025-4330	Extraction filter bypass for linking outside extraction directory	Allows the extraction filter to be ignored, allowing symlink targets to point outside the destination directory, and the modification of some file metadata. You are affected by this vulnerability if using the tarfile module to extract untrusted tar archives using TarFile.extractall() or TarFile.extract() using the filter= parameter with a value of "data" or "tar". See the tarfile extraction filters documentation https://docs.python.org/3/library/tarfile.html#tarfile-extraction-filter for more information. Only Python versions 3.12 or later are affected by these vulnerabilities, earlier versions don't include the extraction filter feature. Note that for Python 3.14 or later the default value of filter= changed from "no filtering" to `"data", so if you are relying on this new default behavior then your usage is also affected. Note that none of these vulnerabilities significantly affect the installation of source distributions which are tar archives as source distributions already allow arbitrary code execution during the build process. However when evaluating source distributions it's important to avoid installing source distributions with suspicious links.	Patched by core rule	Y
CVE-2025-4517	Arbitrary writes via tarfile realpath overflow	Allows arbitrary filesystem writes outside the extraction directory during extraction with filter="data". You are affected by this	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability if using the tarfile module to extract untrusted tar archives using TarFile.extractall() or TarFile.extract() using the filter= parameter with a value of "data" or "tar". See the tarfile extraction filters documentation https://docs.python.org/3/library/tarfile.html#tarfile-extraction-filter for more information. Only Python versions 3.12 or later are affected by these vulnerabilities, earlier versions don't include the extraction filter feature. Note that for Python 3.14 or later the default value of filter= changed from "no filtering" to `"data", so if you are relying on this new default behavior then your usage is also affected. Note that none of these vulnerabilities significantly affect the installation of source distributions which are tar archives as source distributions already allow arbitrary code execution during the build process. However when evaluating source distributions it's important to avoid installing source distributions with suspicious links.		
CVE-2025-5421	juzaweb CMS Plugin Editor Page editor access control	A vulnerability, which was classified as critical, has been found in juzaweb CMS up to 3.4.2. Affected by this issue is some unknown functionality of the file /admin-cp/plugin/editor of the component Plugin Editor Page. The manipulation leads to improper access controls. 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-2025-5422	juzaweb CMS Email Logs Page email access control	A vulnerability, which was classified as problematic, was found in juzaweb CMS up to 3.4.2. This affects an unknown part of the file /admin-cp/logs/email of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the component Email Logs Page. The manipulation leads to improper access controls. 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-2025-5423	juzaweb CMS General Setting Page general access control	A vulnerability has been found in juzaweb CMS up to 3.4.2 and classified as critical. This vulnerability affects unknown code of the file /admin-cp/setting/system/general of the component General Setting Page. The manipulation leads to improper access controls. 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-2025-5424	juzaweb CMS Media Page media access control	A vulnerability was found in juzaweb CMS up to 3.4.2 and classified as critical. This issue affects some unknown processing of the file /admin-cp/media of the component Media Page. The manipulation leads to improper access controls. 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-2025-5425	juzaweb CMS Theme Editor Page default access control	A vulnerability was found in juzaweb CMS up to 3.4.2. It has been classified as critical. Affected is an unknown function of the file /admin-cp/theme/editor/default of the component Theme Editor Page. The manipulation leads to improper access controls. 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		disclosure but did not respond in any way.		
CVE-2025-5426	juzaweb CMS Menu Page menus access control	A vulnerability was found in juzaweb CMS up to 3.4.2. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin-cp/menus of the component Menu Page. The manipulation leads to improper access controls. 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-2025-5427	juzaweb CMS Permalinks Page permalinks access control	A vulnerability was found in juzaweb CMS up to 3.4.2. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin-cp/permalinks of the component Permalinks Page. The manipulation leads to improper access controls. 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-2025-5428	juzaweb CMS Error Logs Page log-viewer access control	A vulnerability classified as critical has been found in juzaweb CMS up to 3.4.2. This affects an unknown part of the file /admin-cp/log-viewer of the component Error Logs Page. The manipulation leads to improper access controls. 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-2025-5429	juzaweb CMS Plugins Page install access control	A vulnerability classified as critical was found in juzaweb CMS up to 3.4.2. This vulnerability affects unknown code of the file /admin-cp/plugin/install of the component Plugins Page. The manipulation	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		leads to improper access controls. 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-2025-5497	slackero phpwcms Feedimport Module processing.inc.php deserialization	A vulnerability was found in slackero phpwcms up to 1.9.45/1.10.8. It has been declared as critical. This vulnerability affects unknown code of the file include/inc_module/mod_feedimport/inc/processing.inc.php of the component Feedimport Module. The manipulation of the argument cnt_text leads to deserialization. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.9.46 and 1.10.9 is able to address this issue. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-5498	slackero phpwcms Custom Source Tab cnt21.readform.inc.php is_file deserialization	A vulnerability was found in slackero phpwcms up to 1.9.45/1.10.8. It has been rated as critical. This issue affects the function file_get_contents/is_file of the file include/inc_lib/content/cnt21.readform.inc.php of the component Custom Source Tab. The manipulation of the argument cpage_custom leads to deserialization. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.9.46 and 1.10.9 is able to address this issue. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-5499	slackero phpwcms image_resized.php getimagesize deserialization	A vulnerability classified as critical has been found in slackero phpwcms up to 1.9.45/1.10.8. Affected is the function is_file/getimagesize of the file image_resized.php. The manipulation of the argument imgfile leads to deserialization. It is possible to launch the attack remotely. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit has been disclosed to the public and may be used. Upgrading to version 1.9.46 and 1.10.9 is able to address this issue. It is recommended to upgrade the affected component.		
CVE-2025-5509	quequnlong shiyi-blog upload path traversal	A vulnerability classified as critical has been found in quequnlong shiyi-blog up to 1.2.1. This affects an unknown part of the file /api/file/upload. The manipulation of the argument file/source 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-2025-5522	jack0240 魏 bskms 蓝天幼儿园管理系统 User Creation addUser improper authorization	A vulnerability was found in jack0240 魏 bskms 蓝天幼儿园管理系统 up to dffe6640b5b54d8e29da6f060e0493fea74b3fad. It has been rated as critical. Affected by this issue is some unknown functionality of the file /sa/addUser of the component User Creation Handler. The manipulation leads to improper authorization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available.	Patched by core rule	Y
CVE-2025-5544	aaluoxiang oa_system UserpanelController.java image path traversal	A vulnerability was found in aaluoxiang oa_system up to 5b445a6227b51cee287bd0c7c33ed94b801a82a5. It has been rated as problematic. Affected by this issue is the function image of the file src/main/java/cn/gson/oasys/controller/user/UserpanelController.java. The manipulation leads to path traversal. The attack may be launched remotely. The exploit has been disclosed to the public and may be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available.		
CVE-2025-5545	aaluoxiang oa_system ProcedureController.java image path traversal	A vulnerability classified as problematic has been found in aaluoxiang oa_system up to 5b445a6227b51cee287bd0c7c33ed94b801a82a5. This affects the function image of the file src/main/java/cn/gson/oasys/controller/process/ProcedureController.java. The manipulation leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.	Patched by core rule	Y
CVE-2025-5598	WF Steuerungstechnik GmbH - airleader MASTER - Path Traversal	Path Traversal vulnerability in WF Steuerungstechnik GmbH airleader MASTER allows Retrieve Embedded Sensitive Data.This issue affects airleader MASTER: 3.0046.	Patched by core rule	Y
CVE-2025-5714	SoluçõesCoop iSoluçõesWEB Profile Information Update up.upload.php path traversal	A vulnerability was found in SoluçõesCoop iSoluçõesWEB up to 20250516. It has been classified as problematic. This affects an unknown part of the file /sys/up.upload.php of the component Profile Information Update. The manipulation of the argument nomeArquivo leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-2828	SSRF Vulnerability in RequestsToolkit in langchain-ai/langchain	A Server-Side Request Forgery (SSRF) vulnerability exists in the RequestsToolkit component of the langchain-community package (specifically, langchain_community.age	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		nt_toolkits.openapi.toolkit .RequestsToolkit) in langchain-ai/langchain version 0.0.27. This vulnerability occurs because the toolkit does not enforce restrictions on requests to remote internet addresses, allowing it to also access local addresses. As a result, an attacker could exploit this flaw to perform port scans, access local services, retrieve instance metadata from cloud environments (e.g., Azure, AWS), and interact with servers on the local network. This issue has been fixed in version 0.0.28.		
CVE-2025-4278	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) in GitLab	An issue has been discovered in GitLab CE/EE affecting all versions starting with 18.0 before 18.0.2. Under certain conditions html injection in new search page could lead to account takeover.	Patched by core rule	Y
CVE-2025-4748	Absolute path traversal in zip:unzip/1,2	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Erlang OTP (stdlib modules) allows Absolute Path Traversal, File Manipulation. This vulnerability is associated with program files lib/stdlib/src/zip.erl and program routines zip:unzip/1, zip:unzip/2, zip:extract/1, zip:extract/2 unless the memory option is passed. This issue affects OTP from OTP 17.0 until OTP 28.0.1, OTP 27.3.4.1 and OTP 26.2.5.13, corresponding to stdlib from 2.0 until 7.0.1, 6.2.2.1 and 5.2.3.4.	Patched by core rule	Y
CVE-2025-50178	GitForge.jl lacks validation for user provided fields	GitForge.jl is a unified interface for interacting with Git "forges." Versions prior to 0.4.3 lack input validation for user provided values in certain functions. In the `GitForge.get_repo` function for GitHub, the user can provide any string for the owner and repo fields. These inputs are not validated or safely	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		encoded and are sent directly to the server. This means a user can add path traversal patterns like `../` in the input to access any other endpoints on api.github.com that were not intended. Version 0.4.3 contains a patch for the issue. No known workarounds are available.		
CVE-2025-50202	Lychee Path Traversal Vulnerability	Lychee is a free photo-management tool. In versions starting from 6.6.6 to before 6.6.10, an attacker can leak local files including environment variables, nginx logs, other user's uploaded images, and configuration secrets due to a path traversal exploit in SecurePathController.php. This issue has been patched in version 6.6.10.	Patched by core rule	Y
CVE-2025-52479	HTTP.jl vulnerable to CR/LF Injection in URIs	HTTP.jl provides HTTP client and server functionality for Julia, and URIs.jl parses and works with Uniform Resource Identifiers (URIs). URIs.jl prior to version 1.6.0 and HTTP.jl prior to version 1.10.17 allows the construction of URIs containing CR/LF characters. If user input was not otherwise escaped or protected, this can lead to a CRLF injection attack. Users of HTTP.jl should upgrade immediately to HTTP.jl v1.10.17, and users of URIs.jl should upgrade immediately to URIs.jl v1.6.0. The check for valid URIs is now in the URI.jl package, and the latest version of HTTP.jl incorporates that fix. As a workaround, manually validate any URIs before passing them on to functions in this package.	Patched by core rule	Y
CVE-2025-52562	Convey Panel Directory Traversal in LocaleController leading to Remote Code Execution	Convoy is a KVM server management panel for hosting businesses. In versions 3.9.0-rc3 to before 4.4.1, there is a directory traversal vulnerability in the LocaleController component of Performave Convoy. An unauthenticated remote	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attacker can exploit this vulnerability by sending a specially crafted HTTP request with malicious locale and namespace parameters. This allows the attacker to include and execute arbitrary PHP files on the server. This issue has been patched in version 4.4.1. A temporary workaround involves implementing strict Web Application Firewall (WAF) rules to incoming requests targeting the vulnerable endpoints.		
CVE-2025-52569	GitHub.jl lacks validation for user-provided fields	GitForge.jl is a unified interface for interacting with Git "forges." Versions prior to 5.9.1 lack input validation of input validation for user-provided values in certain functions. In the `GitHub.repo()` function, the user can provide any string for the `repo_name` field. These inputs are not validated or safely encoded and are sent directly to the server. This means a user can add path traversal patterns like `../` in the input to access any other endpoints on `api.github.com` that were not intended. Users should upgrade immediately to v5.9.1 or later to receive a patch. All prior versions are vulnerable. No known workarounds are available.	Patched by core rule	Y
CVE-2025-52574	SysmonElixir path traversal in /read endpoint allows arbitrary file read	SysmonElixir is a system monitor HTTP service in Elixir. Prior to version 1.0.1, the /read endpoint reads any file from the server's /etc/passwd by default. In v1.0.1, a whitelist was added that limits reading to only files under priv/data. This issue has been patched in version 1.0.1.	Patched by core rule	Y
CVE-2025-52922	N/A	Innoshop through 0.4.1 allows directory traversal via FileManager API endpoints. An authenticated attacker with access to the admin panel could abuse this to: (1) fully map the filesystem structure via the /api/file_manager/files?ba	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		se_folder= endpoint, (2) create arbitrary directories on the server via the /api/file_manager/directories endpoint, (3) read arbitrary files from the server by copying the file to a readable location within the application via the /api/file_manager/copy_files endpoint, {4) delete arbitrary files from the server via a DELETE request to /api/file_manager/files, or (5) create arbitrary files on the server by uploading them and then leveraging the /api/file_manager/move_files endpoint to move them anywhere in the filesystem.		
CVE-2025-6108	hansonwang99 Spring-Boot-In-Action File Upload ImageUploadService.java watermarkTest path traversal	A vulnerability was found in hansonwang99 Spring-Boot-In-Action up to 807fd37643aa774b94fd004cc3adbd29ca17e9aa. It has been declared as critical. Affected by this vulnerability is the function watermarkTest of the file /springbt_watermark/src/main/java/cn/codesheep/springbt_watermark/service/ImageUploadService.java of the component File Upload. The manipulation of the argument filename leads to path traversal. 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.	Patched by core rule	Y
CVE-2025-6109	javahongxi whatsmars InitializrController.java initialize path traversal	A vulnerability was found in javahongxi whatsmars 2021.4.0. It has been rated as problematic. Affected by this issue is the function initialize of the file /whatsmars-archetypes/whatsmars-initializr/src/main/java/org	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/hongxi/whatsmars/initializr/controller/InitializrController.java. The manipulation of the argument artifactId 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 early about this disclosure but did not respond in any way.		
CVE-2025-6152	Steel Browser files.routes.ts handleFileUpload path traversal	A vulnerability, which was classified as critical, was found in Steel Browser up to 0.1.3. This affects the function handleFileUpload of the file api/src/modules/files/files.routes.ts. The manipulation of the argument filename leads to path traversal. It is possible to initiate the attack remotely. The patch is named 7ba93a10000fb77ee01731478ef40551a27bd5b9. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y
CVE-2025-6166	frdel Agent-Zero image_get.py image_get path traversal	A vulnerability was found in frdel Agent-Zero up to 0.8.4. It has been rated as problematic. This issue affects the function image_get of the file /python/api/image_get.py. The manipulation of the argument path leads to path traversal. Upgrading to version 0.8.4.1 is able to address this issue. The identifier of the patch is 5db74202d632306a883ccce7339c5bdba0d16c5a. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-6167	themanojdesai python-a2a api.py create_workflow path traversal	A vulnerability classified as critical has been found in themanojdesai python-a2a up to 0.5.5. Affected is the function create_workflow of the file python_a2a/agent_flow/server/api.py. The manipulation leads to path traversal. Upgrading to version 0.5.6 is able to address this issue. It is recommended to upgrade the affected component.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-6278	Upsonic server.py os.path.join path traversal	A vulnerability classified as critical was found in Upsonic up to 0.55.6. This vulnerability affects the function os.path.join of the file markdown/server.py. The manipulation of the argument file.filename leads to path traversal. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6280	TransformerOptimus SuperAGI EmailToolKit read_email.py download_attachment path traversal	A vulnerability, which was classified as critical, was found in TransformerOptimus SuperAGI up to 0.0.14. Affected is the function download_attachment of the file SuperAGI/superagi/helper/read_email.py of the component EmailToolKit. The manipulation of the argument filename leads to path traversal. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6281	OpenBMB XAgent community path traversal	A vulnerability has been found in OpenBMB XAgent up to 1.0.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /conv/community. The manipulation leads to path traversal. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6282	xlang-ai OpenAgents file.py create_upload_file path traversal	A vulnerability was found in xlang-ai OpenAgents up to ff2e46440699af1324eb25655b622c4a131265bb and classified as critical. Affected by this issue is the function create_upload_file of the file backend/api/file.py. The manipulation leads to path traversal. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The reported GitHub issue was closed automatically with the label "not planned" by a bot.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-6283	xataio Xata Agent route.ts GET path traversal	A vulnerability was found in xataio Xata Agent up to 0.3.0. It has been classified as problematic. This affects the function GET of the file apps/dbagent/src/app/api/evals/route.ts. The manipulation of the argument passed leads to path traversal. Upgrading to version 0.3.1 is able to address this issue. The patch is named 03f27055e0cf5d4fa7e874d34ce8c74c7b9086cc. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-6453	diyhi bbs API ForumManageAction.java add path traversal	A vulnerability classified as critical has been found in diyhi bbs 6.8. Affected is the function Add of the file /src/main/java/cms/web/action/template/ForumManageAction.java of the component API. The manipulation of the argument dirName leads to path traversal. 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

Server-side Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-52588	Strapi allows Server-Side Request Forgery in Webhook function	Strapi is an open-source content management system. Prior to version 4.25.2, inputting a local domain into the Webhooks URL field leads to the application fetching itself, resulting in a server side request forgery (SSRF). This issue has been patched in version 4.25.2.	Patched by core rule	Y
CVE-2025-5186	thinkgem JeeSite URI Scheme form ResourceLoader.getResource server-side request forgery	A vulnerability was found in thinkgem JeeSite up to 5.11.1. It has been rated as critical. Affected by this issue is the function ResourceLoader.getResource of the file /cms/fileTemplate/form of the component URI Scheme Handler. The manipulation of the argument Name leads to server-side request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-5327	chshcms mccms Gf.php index server-side request forgery	A vulnerability was found in chshcms mccms 2.7. It has been classified as critical. This affects the function index of the file sys/apps/controllers/api/Gf.php. The manipulation of the argument pic 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. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-29198	GeoServer Vulnerable to Unauthenticated SSRF via TestWfsPost	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. It possible to achieve Service Side Request Forgery (SSRF) via the Demo request endpoint if Proxy Base URL has not been set. Upgrading to GeoServer 2.24.4, or 2.25.2, removes the TestWfsPost servlet resolving this issue.	Patched by core rule	Y
CVE-2025-5510	quequnlong shiyi-blog optimize server-side request forgery	A vulnerability classified as critical was found in quequnlong shiyi-blog up to 1.2.1. This vulnerability	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects unknown code of the file /app/sys/article/optimize. The manipulation of the argument url leads to server-side request forgery. 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-2024-51980	Unauthenticated Server Side Request Forgery (SSRF) via WS-Addressing affecting multiple models from Brother Industries, Ltd, FUJIFILM Business Innovation, RICOH, and Toshiba Tec.	An unauthenticated attacker may perform a limited server side request forgery (SSRF), forcing the target device to open a TCP connection to an arbitrary port number on an arbitrary IP address. This SSRF leverages the WS-Addressing ReplyTo element in a Web service (HTTP TCP port 80) SOAP request. The attacker can not control the data sent in the SSRF connection, nor can the attacker receive any data back. This SSRF is suitable for TCP port scanning of an internal network when the Web service (HTTP TCP port 80) is exposed across a network segment.	Patched by core rule	Y
CVE-2024-51981	Unauthenticated Server Side Request Forgery (SSRF) via WS-Eventing affecting multiple models from Brother Industries, Ltd, FUJIFILM Business Innovation, RICOH, and Toshiba Tec.	An unauthenticated attacker may perform a blind server side request forgery (SSRF), due to a CLRF injection issue that can be leveraged to perform HTTP request smuggling. This SSRF leverages the WS-Addressing feature used during a WS-Eventing subscription SOAP operation. The attacker can control all the HTTP data sent in the SSRF connection, but the attacker can not receive any data back from this connection.	Patched by core rule	Y
CVE-2025-47293	PowSyBl Core XML Reader allows XXE and SSRF	PowSyBl (Power System Blocks) is a framework to build power system oriented software. Prior to version 6.7.2, in certain places, powsybl-core XML parsing is vulnerable to an XML external entity (XXE) attack and to a server-side request forgery (SSRF) attack. This allows an attacker to elevate their privileges to read files that they do not have permissions to, including sensitive files on the system.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The vulnerable class is com.powsybl.commons.xml.XmlReader which is considered to be untrusted in use cases where untrusted users can submit their XML to the vulnerable methods. This can be a multi-tenant application that hosts many different users perhaps with different privilege levels. This issue has been patched in com.powsybl:powsybl-commons: 6.7.2.		
CVE-2025-52888	Allure 2's xunit-xml-plugin Vulnerable to Improper XXE Restriction	Allure 2 is the version 2.x branch of Allure Report, a multi-language test reporting tool. A critical XML External Entity (XXE) vulnerability exists in the xunit-xml-plugin used by Allure 2 prior to version 2.34.1. The plugin fails to securely configure the XML parser (`DocumentBuilderFactory`) and allows external entity expansion when processing test result .xml files. This allows attackers to read arbitrary files from the file system and potentially trigger server-side request forgery (SSRF). Version 2.34.1 contains a patch for the issue.	Patched by core rule	Y
CVE-2025-6517	Dromara MaxKey Meta URL SAML20DetailsController.java add server-side request forgery	A vulnerability was found in Dromara MaxKey up to 4.1.7 and classified as critical. This issue affects the function Add of the file maxkey-webs\maxkey-web-mgt\src\main\java\org\dromara\maxkey\web\apps\contorller\SAML20DetailsController.java of the component Meta URL Handler. The manipulation of the argument post leads to server-side request forgery. 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

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-5172	Econtrata valida sql injection	A vulnerability, which was classified as critical, was found in Econtrata up to 20250516. Affected is an unknown function of the file /valida. The manipulation of the argument usuario 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-2025-5205	1000 Projects Daily College Class Work Report Book dcwr_entry.php sql injection	A vulnerability classified as critical has been found in 1000 Projects Daily College Class Work Report Book 1.0. Affected is an unknown function of the file /dcwr_entry.php. The manipulation of the argument Date 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-2025-5206	Pixelimity Installation index.php sql injection	A vulnerability classified as critical was found in Pixelimity 1.0. Affected by this vulnerability is an unknown functionality of the file /install/index.php of the component Installation. The manipulation of the argument site_description 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-2025-5207	SourceCodester Client Database Management System superadmin_update_profile.php sql injection	A vulnerability, which was classified as critical, has been found in SourceCodester Client Database Management System 1.0. Affected by this issue is some unknown functionality of the file /superadmin_update_profile.php. The manipulation of the argument nickname/email 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-2025-5208	SourceCodester Online Hospital Management System	A vulnerability, which was classified as critical, was found in SourceCodester	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	check_availability.php sql injection	Online Hospital Management System 1.0. This affects an unknown part of the file /admin/check_availability.php. The manipulation of the argument emailid 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-2025-5210	PHPGurukul Employee Record Management System loginerms.php sql injection	A vulnerability has been found in PHPGurukul Employee Record Management System 1.3 and classified as critical. This vulnerability affects unknown code of the file /loginerms.php. The manipulation of the argument Email leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-5211	PHPGurukul Employee Record Management System myprofile.php sql injection	A vulnerability was found in PHPGurukul Employee Record Management System 1.3 and classified as critical. This issue affects some unknown processing of the file /myprofile.php. The manipulation of the argument EmpCode 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-2025-5212	PHPGurukul Employee Record Management System editempexp.php sql injection	A vulnerability was found in PHPGurukul Employee Record Management System 1.3. It has been classified as critical. Affected is an unknown function of the file /admin/editempexp.php. The manipulation of the argument emp1name 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-2025-5213	projectworlds Responsive E-Learning System delete_file.php sql injection	A vulnerability was found in projectworlds Responsive E-Learning System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/delete_file.php. The manipulation of the argument ID leads to sql injection. The attack can 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-2025-5214	Kashipara Responsive Online Learing Platform course_detail_user_new.php sql injection	A vulnerability was found in Kashipara Responsive Online Learing Platform 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /courses/course_detail_user_new.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. The name of the affected product appears to have a typo in it.	Patched by core rule	Y
CVE-2025-5216	PHPGurukul Student Record System login.php sql injection	A vulnerability classified as critical was found in PHPGurukul Student Record System 3.20. This vulnerability affects unknown code of the file /login.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-2025-5224	Campcodes Online Hospital Management System add-doctor.php sql injection	A vulnerability classified as critical has been found in Campcodes Online Hospital Management System 1.0. Affected is an unknown function of the file /admin/add-doctor.php. The manipulation of the argument Doctorspecialization 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-2025-5225	Campcodes Advanced Online Voting System index.php sql injection	A vulnerability, which was classified as critical, was found in Campcodes Advanced Online Voting System 1.0. This affects an unknown part of the file /index.php. The manipulation of the argument voter 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-2025-5226	PHPGurukul Small CRM change-password.php sql injection	A vulnerability has been found in PHPGurukul Small CRM 3.0 and classified as critical. This vulnerability affects unknown code of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file /admin/change-password.php. The manipulation of the argument oldpass 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-2025-5227	PHPGurukul Small CRM manage-tickets.php sql injection	A vulnerability was found in PHPGurukul Small CRM 3.0 and classified as critical. This issue affects some unknown processing of the file /admin/manage-tickets.php. The manipulation of the argument aremark 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-2025-5229	Campcodes Online Hospital Management System view-patient.php sql injection	A vulnerability was found in Campcodes Online Hospital Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/view-patient.php. The manipulation of the argument viewid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-5230	PHPGurukul Online Nurse Hiring System bwdates-report-details.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Online Nurse Hiring System 1.0. This affects an unknown part of the file /admin/bwdates-report-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-2025-5231	PHPGurukul Company Visitor Management System forgot-password.php sql injection	A vulnerability classified as critical was found in PHPGurukul Company Visitor Management System 1.0. This vulnerability affects unknown code of the file /forgot-password.php. The manipulation of the argument email leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-5232	PHPGurukul Student Study Center Management System report.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Student Study Center Management System 1.0. This issue affects some unknown processing of the file /admin/report.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-2025-5246	Campcodes Online Hospital Management System query-details.php sql injection	A vulnerability classified as critical was found in Campcodes Online Hospital Management System 1.0. This vulnerability affects unknown code of the file /hms/admin/query-details.php. The manipulation of the argument adminremark 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-2025-5248	PHPGurukul Company Visitor Management System bwdates-reports-details.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Company Visitor Management System 1.0. Affected is an unknown function of the file /bwdates-reports-details.php. The manipulation of the argument fromdate/todate 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-2025-5249	PHPGurukul News Portal Project add-category.php sql injection	A vulnerability has been found in PHPGurukul News Portal Project 4.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/add-category.php. The manipulation of the argument Category 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-2025-5250	PHPGurukul News Portal Project edit-category.php sql injection	A vulnerability was found in PHPGurukul News Portal Project 4.1 and classified as critical. Affected by this issue is some unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		functionality of the file /admin/edit-category.php. The manipulation of the argument Category leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-5251	PHPGurukul News Portal Project edit-subcategory.php sql injection	A vulnerability was found in PHPGurukul News Portal Project 4.1. It has been classified as critical. This affects an unknown part of the file /admin/edit-subcategory.php. The manipulation of the argument Category 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-2025-5252	PHPGurukul News Portal Project edit-subadmin.php sql injection	A vulnerability was found in PHPGurukul News Portal Project 4.1. It has been declared as critical. This vulnerability affects unknown code of the file /admin/edit-subadmin.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-2025-5298	Campcodes Online Hospital Management System betweendates-detailsreports.php sql injection	A vulnerability, which was classified as critical, was found in Campcodes Online Hospital Management System 1.0. Affected is an unknown function of the file /admin/betweendates-detailsreports.php. The manipulation of the argument fromdate/todate 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-2025-5332	1000 Projects Online Notice Board index.php sql injection	A vulnerability was found in 1000 Projects Online Notice Board 1.0 and classified as critical. This issue affects some unknown processing of the file /index.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-5358	PHPGurukul/Campcodes Cyber Cafe Management System bwdates-reports-	A vulnerability was found in PHPGurukul/Campcodes Cyber Cafe Management	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	details.php sql injection	System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /bwdates-reports-details.php. The manipulation of the argument fromdate/todate leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-5359	Campcodes Online Hospital Management System appointment-history.php sql injection	A vulnerability classified as critical has been found in Campcodes Online Hospital Management System 1.0. This affects an unknown part of the file /appointment-history.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-2025-5360	Campcodes Online Hospital Management System book-appointment.php sql injection	A vulnerability classified as critical was found in Campcodes Online Hospital Management System 1.0. This vulnerability affects unknown code of the file /book-appointment.php. The manipulation of the argument doctor 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-2025-5361	Campcodes Online Hospital Management System contact.php sql injection	A vulnerability, which was classified as critical, has been found in Campcodes Online Hospital Management System 1.0. This issue affects some unknown processing of the file /contact.php. The manipulation of the argument fullname 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-2025-5362	Campcodes Online Hospital Management System doctor-specilization.php sql injection	A vulnerability, which was classified as critical, was found in Campcodes Online Hospital Management System 1.0. Affected is an unknown function of the file /admin/doctor-specilization.php. The manipulation of the argument doctorspecilization leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-5363	Campcodes Online Hospital Management System index.php sql injection	A vulnerability has been found in Campcodes Online Hospital Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /doctor/index.php. The manipulation of the argument Username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-5364	Campcodes Online Hospital Management System add-patient.php sql injection	A vulnerability was found in Campcodes Online Hospital Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /doctor/add-patient.php. The manipulation of the argument patname 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-2025-5365	Campcodes Online Hospital Management System patient-search.php sql injection	A vulnerability was found in Campcodes Online Hospital Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/patient-search.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-2025-5367	PHPGurukul Online Shopping Portal Project category.php sql injection	A vulnerability was found in PHPGurukul Online Shopping Portal Project 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /category.php. The manipulation of the argument Product 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-2025-5368	PHPGurukul Daily Expense Tracker System expense-yearwise-reports-detailed.php sql injection	A vulnerability was found in PHPGurukul Daily Expense Tracker System 1.1. It has been rated as critical. This issue affects some unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		processing of the file /expense-yearwise-reports-detailed.php. The manipulation of the argument todate leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-5369	SourceCodester PHP Display Username After Login login.php sql injection	A vulnerability classified as critical has been found in SourceCodester PHP Display Username After Login 1.0. Affected is an unknown function of the file /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-2025-5370	PHPGurukul News Portal forgot-password.php sql injection	A vulnerability classified as critical was found in PHPGurukul News Portal 4.1. Affected by this vulnerability is an unknown functionality of the file /admin/forgot-password.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-2025-5371	SourceCodester Health Center Patient Record Management System admin.php sql injection	A vulnerability, which was classified as critical, has been found in SourceCodester Health Center Patient Record Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/admin.php. The manipulation of the argument Username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-5373	PHPGurukul Online Birth Certificate System users-applications.php sql injection	A vulnerability has been found in PHPGurukul Online Birth Certificate System 2.0 and classified as critical. This vulnerability affects unknown code of the file /admin/users-applications.php. The manipulation of the argument userid 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-5374	PHPGurukul Online Birth Certificate System all-applications.php sql injection	A vulnerability was found in PHPGurukul Online Birth Certificate System 2.0 and classified as critical. This issue affects some unknown processing of the file /admin/all-applications.php. The manipulation of the argument del 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-2025-5375	PHPGurukul HPGurukul Online Birth Certificate System registered-users.php sql injection	A vulnerability was found in PHPGurukul HPGurukul Online Birth Certificate System 2.0. It has been classified as critical. Affected is an unknown function of the file /admin/registered-users.php. The manipulation of the argument del 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-2025-5376	SourceCodester Health Center Patient Record Management System patient.php sql injection	A vulnerability was found in SourceCodester Health Center Patient Record Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /patient.php. The manipulation of the argument itr_no leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-5384	JeeWMS cgAutoListController.do CgAutoListController sql injection	A vulnerability was found in JeeWMS up to 20250504. It has been classified as critical. This affects the function CgAutoListController of the file /cgAutoListController.do?datagrid. The manipulation leads to sql injection. It is possible to initiate the attack remotely. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available.	Patched by core rule	Y
CVE-2025-5386	JeeWMS cgformTransController.do transEditor sql injection	A vulnerability was found in JeeWMS up to 20250504. It has been rated as critical. This issue affects the function transEditor of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/cgformTransController.do?transEditor. The manipulation leads to sql injection. The attack may be initiated remotely. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.		
CVE-2025-5388	JeeWMS generateController.do dogenerate sql injection	A vulnerability classified as critical was found in JeeWMS up to 20250504. Affected by this vulnerability is the function dogenerate of the file /generateController.do?dogenerate. The manipulation leads to sql injection. The attack can be launched remotely. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available.	Patched by core rule	Y
CVE-2025-1750	SQL Injection in run-llama/llama_index	An SQL injection vulnerability exists in the delete function of DuckDBVectorStore in run-llama/llama_index version v0.12.19. This vulnerability allows an attacker to manipulate the ref_doc_id parameter, enabling them to read and write arbitrary files on the server, potentially leading to remote code execution (RCE).	Patched by core rule	Y
CVE-2025-1793	SQL Injection in run-llama/llama_index	Multiple vector store integrations in run-llama/llama_index version v0.12.21 have SQL injection vulnerabilities. These vulnerabilities allow an attacker to read and write data using SQL, potentially leading to unauthorized access to data of other users depending on the usage of the llama-index library in a web application.	Patched by core rule	Y
CVE-2025-5400	chaitak-gorai Blogbook GET Parameter user.php sql injection	A vulnerability was found in chaitak-gorai Blogbook up to 92f5cf90f8a7e6566b576fe0952e14e1c6736513. It has been classified as critical. Affected is an unknown function of the file /user.php of the component GET Parameter Handler. The manipulation of the argument u_id 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. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-5401	chaitak-gorai Blogbook GET Parameter post.php sql injection	A vulnerability was found in chaitak-gorai Blogbook up to 92f5cf90f8a7e6566b576fe0952e14e1c6736513. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /post.php of the component GET Parameter Handler. The manipulation of the argument p_id 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.	Patched by core rule	Y
CVE-2025-5402	chaitak-gorai Blogbook GET Parameter edit_post.php sql injection	A vulnerability was found in chaitak-gorai Blogbook up to 92f5cf90f8a7e6566b576fe0952e14e1c6736513. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/includes/edit_post.php of the component GET Parameter Handler. The manipulation of the argument edit_post_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-5403	chaitak-gorai Blogbook GET Parameter view_all_posts.php sql	A vulnerability classified as critical has been found in chaitak-gorai Blogbook up to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	92f5cf90f8a7e6566b576fe0952e14e1c6736513. This affects an unknown part of the file /admin/view_all_posts.php of the component GET Parameter Handler. The manipulation of the argument post_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. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-5430	AssamLook CMS product.php sql injection	A vulnerability, which was classified as critical, has been found in AssamLook CMS 1.0. This issue affects some unknown processing of the file /product.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. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-5431	AssamLook CMS department-profile.php sql injection	A vulnerability, which was classified as critical, was found in AssamLook CMS 1.0. Affected is an unknown function of the file /department-profile.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. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-5432	AssamLook CMS view_tender.php sql injection	A vulnerability has been found in AssamLook CMS 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /view_tender.php. The manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. 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-2025-5433	Fengoffice Feng Office index.php sql injection	A vulnerability was found in Fengoffice Feng Office 3.5.1.5 and classified as critical. Affected by this issue is some unknown functionality of the file /index.php?c=account&a=set_timezone. The manipulation of the argument tz_offset 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-2025-5434	Aem Solutions CMS page.php sql injection	A vulnerability was found in Aem Solutions CMS up to 1.0. It has been classified as critical. This affects an unknown part of the file /page.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-5435	Marwal Infotech CMS page.php sql injection	A vulnerability was found in Marwal Infotech CMS 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /page.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. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-5546	PHPGurukul Daily Expense Tracker System expense-reports-detailed.php sql injection	A vulnerability classified as critical was found in PHPGurukul Daily Expense Tracker System 1.1. This vulnerability affects unknown code of the file /expense-reports-detailed.php. The manipulation of the argument fromdate/todate leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and may be used.		
CVE-2025-5553	PHPGurukul Rail Pass Management System download-pass.php sql injection	A vulnerability classified as critical was found in PHPGurukul Rail Pass Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /download-pass.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-2025-5554	PHPGurukul Rail Pass Management System pass-bwdates-reports-details.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Rail Pass Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/pass-bwdates-reports-details.php. The manipulation of the argument fromdate/todate 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-2025-5556	PHPGurukul Teacher Subject Allocation Management System edit-teacher-info.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Teacher Subject Allocation Management System 1.0. This affects an unknown part of the file /admin/edit-teacher-info.php. The manipulation of the argument editid 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-2025-5557	PHPGurukul Teacher Subject Allocation Management System edit-course.php sql injection	A vulnerability has been found in PHPGurukul Teacher Subject Allocation Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/edit-course.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-2025-5558	PHPGurukul Teacher Subject Allocation Management System changeimage.php sql	A vulnerability was found in PHPGurukul Teacher Subject Allocation Management System 1.0 and classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	critical. This issue affects some unknown processing of the file /admin/changeimage.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.		
CVE-2025-5560	PHPGurukul Curfew e-Pass Management System index.php sql injection	A vulnerability was found in PHPGurukul Curfew e-Pass Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /index.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-2025-5561	PHPGurukul Curfew e-Pass Management System view-pass-detail.php sql injection	A vulnerability was found in PHPGurukul Curfew e-Pass Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/view-pass-detail.php. The manipulation of the argument viewid 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-2025-5562	PHPGurukul Curfew e-Pass Management System edit-category-detail.php sql injection	A vulnerability was found in PHPGurukul Curfew e-Pass Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/edit-category-detail.php. The manipulation of the argument editid 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-2025-5566	PHPGurukul Notice Board System search-notice.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Notice Board System 1.0. This affects an unknown part of the file /search-notice.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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-5569	IdeaCMS getList.html Goods sql injection	A vulnerability was found in IdeaCMS up to 1.7 and classified as critical. This issue affects the function Article/Goods of the file /api/v1.index.article/getList.html. The manipulation of the argument Field leads to sql injection. The attack may be initiated remotely. Upgrading to version 1.8 is able to address this issue. The patch is named 935aceb4c21338633de6d41e13332f7b9db4fa6a. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-5574	PHPGurukul Dairy Farm Shop Management System add-company.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Dairy Farm Shop Management System 1.3. This affects an unknown part of the file /add-company.php. The manipulation of the argument companyname 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-2025-5575	PHPGurukul Dairy Farm Shop Management System add-product.php sql injection	A vulnerability classified as critical was found in PHPGurukul Dairy Farm Shop Management System 1.3. This vulnerability affects unknown code of the file /add-product.php. The manipulation of the argument productname 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-2025-5576	PHPGurukul Dairy Farm Shop Management System bwdate-report-details.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Dairy Farm Shop Management System 1.3. This issue affects some unknown processing of the file /bwdate-report-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-2025-5577	PHPGurukul Dairy Farm Shop Management System profile.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Dairy Farm Shop Management	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		System 1.3. Affected is an unknown function of the file /profile.php. The manipulation of the argument 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.		
CVE-2025-5578	PHPGurukul Dairy Farm Shop Management System sales-report-details.php sql injection	A vulnerability has been found in PHPGurukul Dairy Farm Shop Management System 1.3 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /sales-report-details.php. The manipulation of the argument fromdate/todate 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-2025-5579	PHPGurukul Dairy Farm Shop Management System search-product.php sql injection	A vulnerability was found in PHPGurukul Dairy Farm Shop Management System 1.3 and classified as critical. Affected by this issue is some unknown functionality of the file /search-product.php. The manipulation of the argument productname 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-2025-5580	CodeAstro Real Estate Management System login.php sql injection	A vulnerability was found in CodeAstro Real Estate Management System 1.0. It has been classified as critical. This affects an unknown part of the file /login.php. The manipulation of the argument email leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-5581	CodeAstro Real Estate Management System index.php sql injection	A vulnerability was found in CodeAstro Real Estate Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/index.php. The manipulation of the argument User leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the public and may be used.		
CVE-2025-5582	CodeAstro Real Estate Management System profile.php sql injection	A vulnerability was found in CodeAstro Real Estate Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /profile.php. The manipulation of the argument content 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-2025-5583	CodeAstro Real Estate Management System register.php sql injection	A vulnerability classified as critical has been found in CodeAstro Real Estate Management System 1.0. Affected is an unknown function of the file /register.php. The manipulation 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-2025-5599	PHPGurukul Student Result Management System editmyexp.php sql injection	A vulnerability classified as critical was found in PHPGurukul Student Result Management System 1.3. This vulnerability affects unknown code of the file /editmyexp.php. The manipulation of the argument emp1ctc 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-2025-5602	Campcodes Hospital Management System registration.php sql injection	A vulnerability, which was classified as critical, was found in Campcodes Hospital Management System 1.0. Affected is an unknown function of the file /admin/registration.php. The manipulation of the argument full_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-2025-5603	Campcodes Hospital Management System registration.php sql injection	A vulnerability has been found in Campcodes Hospital Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /registration.php. The manipulation of the argument	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		full_name/username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-5604	Campcodes Hospital Management System user-login.php sql injection	A vulnerability was found in Campcodes Hospital Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /user-login.php. The manipulation of the argument Username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-5610	CodeAstro Real Estate Management System submitpropertydelete.php sql injection	A vulnerability, which was classified as critical, has been found in CodeAstro Real Estate Management System 1.0. Affected by this issue is some unknown functionality of the file /submitpropertydelete.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-2025-5611	CodeAstro Real Estate Management System submitpropertyupdate.php sql injection	A vulnerability, which was classified as critical, was found in CodeAstro Real Estate Management System 1.0. This affects an unknown part of the file /submitpropertyupdate.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-2025-5612	PHPGurukul Online Fire Reporting System reporting.php sql injection	A vulnerability has been found in PHPGurukul Online Fire Reporting System 1.2 and classified as critical. This vulnerability affects unknown code of the file /reporting.php. The manipulation of the argument fullname 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-2025-5613	PHPGurukul Online Fire Reporting System request-details.php sql	A vulnerability was found in PHPGurukul Online Fire Reporting System 1.2 and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	classified as critical. This issue affects some unknown processing of the file /request-details.php. The manipulation of the argument requestid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-5614	PHPGurukul Online Fire Reporting System search-report-result.php sql injection	A vulnerability was found in PHPGurukul Online Fire Reporting System 1.2. It has been classified as critical. Affected is an unknown function of the file /search-report-result.php. The manipulation of the argument serachdata 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-2025-5615	PHPGurukul Online Fire Reporting System details.php sql injection	A vulnerability was found in PHPGurukul Online Fire Reporting System 1.2. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /details.php. The manipulation of the argument requestid 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-2025-5616	PHPGurukul Online Fire Reporting System profile.php sql injection	A vulnerability was found in PHPGurukul Online Fire Reporting System 1.2. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/profile.php. The manipulation of the argument mobilenumber leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-5617	PHPGurukul Online Fire Reporting System manage-teams.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Online Fire Reporting System 1.2. This affects an unknown part of the file /admin/manage-teams.php. The manipulation of the argument teamid leads to sql injection. It is possible to initiate the attack remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The exploit has been disclosed to the public and may be used.		
CVE-2025-5618	PHPGurukul Online Fire Reporting System edit-team.php sql injection	A vulnerability classified as critical was found in PHPGurukul Online Fire Reporting System 1.2. This vulnerability affects unknown code of the file /admin/edit-team.php. The manipulation of the argument teamid 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-2025-5625	Campcodes Online Teacher Record Management System search-teacher.php sql injection	A vulnerability was found in Campcodes Online Teacher Record Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /search-teacher.php. The manipulation of the argument searchteacher 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-2025-5626	Campcodes Online Teacher Record Management System edit-subjects-detail.php sql injection	A vulnerability classified as critical has been found in Campcodes Online Teacher Record Management System 1.0. Affected is an unknown function of the file /admin/edit-subjects-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-2025-5627	code-projects Patient Record Management System sputum_form.php sql injection	A vulnerability classified as critical was found in code-projects Patient Record Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /sputum_form.php. The manipulation of the argument itr_no leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-5631	code-projects/anirbandutta9 Content Management System/News-Buzz publicposts.php sql injection	A vulnerability was found in code-projects/anirbandutta9 Content Management System and News-Buzz 1.0. It has been classified as critical. Affected is an	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown function of the file /publicposts.php. The manipulation of the argument post 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-2025-5632	code-projects/anirbandutta9 Content Management System/News-Buzz users.php sql injection	A vulnerability was found in code-projects/anirbandutta9 Content Management System and News-Buzz 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/users.php. The manipulation of the argument change_to_admin 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-2025-5633	code-projects/anirbandutta9 Content Management System/News-Buzz users.php sql injection	A vulnerability was found in code-projects/anirbandutta9 Content Management System and News-Buzz 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/users.php. The manipulation of the argument delete 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-2025-5638	PHPGurukul Notice Board System admin-profile.php sql injection	A vulnerability has been found in PHPGurukul Notice Board System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin-profile.php. 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. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-5639	PHPGurukul Notice Board System forgot-password.php sql injection	A vulnerability was found in PHPGurukul Notice Board System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /forgot-password.php. The manipulation of the argument email leads to sql injection. The attack may be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-5650	1000projects Online Notice Board register.php sql injection	A vulnerability classified as critical was found in 1000projects Online Notice Board 1.0. This vulnerability affects unknown code of the file /register.php. The manipulation of the argument fname 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-2025-5652	PHPGurukul Complaint Management System between-date-complaintreport.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Complaint Management System 2.0. Affected is an unknown function of the file /admin/between-date-complaintreport.php. The manipulation of the argument fromdate/todate 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-2025-5653	PHPGurukul Complaint Management System between-date-userreport.php sql injection	A vulnerability has been found in PHPGurukul Complaint Management System 2.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/between-date-userreport.php. The manipulation of the argument fromdate/todate 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-2025-5654	PHPGurukul Complaint Management System edit-state.php sql injection	A vulnerability was found in PHPGurukul Complaint Management System 2.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/edit-state.php. The manipulation of the argument description 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-2025-5655	PHPGurukul Complaint Management System edit-subcategory.php sql	A vulnerability was found in PHPGurukul Complaint Management System 2.0. It	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	has been classified as critical. This affects an unknown part of the file /admin/edit-subcategory.php. The manipulation of the argument subcategory 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-2025-5656	PHPGurukul Complaint Management System edit-category.php sql injection	A vulnerability was found in PHPGurukul Complaint Management System 2.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/edit-category.php. The manipulation of the argument description 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-2025-5657	PHPGurukul Complaint Management System manage-users.php sql injection	A vulnerability was found in PHPGurukul Complaint Management System 2.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/manage-users.php. The manipulation of the argument uid 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-2025-5658	PHPGurukul Complaint Management System updatecomplaint.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Complaint Management System 2.0. Affected is an unknown function of the file /admin/updatecomplaint.php. The manipulation of the argument Status 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-2025-5659	PHPGurukul Complaint Management System profile.php sql injection	A vulnerability classified as critical was found in PHPGurukul Complaint Management System 2.0. Affected by this vulnerability is an unknown functionality of the file /user/profile.php. The manipulation of the argument pincode leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the public and may be used.		
CVE-2025-5660	PHPGurukul Complaint Management System register-complaint.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Complaint Management System 2.0. Affected by this issue is some unknown functionality of the file /user/register-complaint.php. The manipulation of the argument noc 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-2025-5663	PHPGurukul Auto Taxi Stand Management System search-autoortaxi.php sql injection	A vulnerability has been found in PHPGurukul Auto Taxi Stand Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/search-autoortaxi.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-2025-5668	PHPGurukul Medical Card Generation System readenq.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Medical Card Generation System 1.0. This affects an unknown part of the file /admin/readenq.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-2025-5669	PHPGurukul Medical Card Generation System unreadenq.php sql injection	A vulnerability classified as critical was found in PHPGurukul Medical Card Generation System 1.0. This vulnerability affects unknown code of the file /admin/unreadenq.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-2025-5670	PHPGurukul Medical Card Generation System manage-card.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Medical Card Generation System 1.0. This issue affects some unknown processing	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the file /admin/manage-card.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-5674	code-projects Patient Record Management System urinalysis_form.php sql injection	A vulnerability was found in code-projects Patient Record Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file urinalysis_form.php. The manipulation of the argument urinalysis_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-2025-5675	Campcodes Online Teacher Record Management System bwdates-reports-details.php sql injection	A vulnerability was found in Campcodes Online Teacher Record Management System 1.0. It has been classified as critical. This affects an unknown part of the file /trms/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-2025-5676	Campcodes Online Recruitment Management System ajax.php sql injection	A vulnerability was found in Campcodes Online Recruitment Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/ajax.php?action=login. The manipulation of the argument Username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-5677	Campcodes Online Recruitment Management System ajax.php sql injection	A vulnerability was found in Campcodes Online Recruitment Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/ajax.php?action=save_application. The manipulation of the argument position_id leads to sql injection. The attack may be initiated remotely. The exploit has been		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		disclosed to the public and may be used.		
CVE-2025-5693	PHPGurukul Human Metapneumovirus Testing Management System bwdates-report-result.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 /bwdates-report-result.php. The manipulation of the argument fromdate/todate 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-2025-5694	PHPGurukul Human Metapneumovirus Testing Management System search-report-result.php sql injection	A vulnerability was found in PHPGurukul Human Metapneumovirus Testing Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /search-report-result.php. The manipulation of the argument serachdata 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-2025-5696	Brilliance Golden Link Secondary System rentChangeCheckInfoPage.htm sql injection	A vulnerability classified as critical was found in Brilliance Golden Link Secondary System up to 20250424. This vulnerability affects unknown code of the file /storagework/rentChangeCheckInfoPage.htm. The manipulation of the argument clientname 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-2025-5697	Brilliance Golden Link Secondary System tcCustDeferPosiQuery.htm sql injection	A vulnerability, which was classified as critical, has been found in Brilliance Golden Link Secondary System up to 20250424. This issue affects some unknown processing of the file /reprotframework/tcCustDeferPosiQuery.htm. The manipulation of the argument custTradeId 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-2025-5698	Brilliance Golden Link	A vulnerability, which was	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Secondary System logSelect.htm sql injection	classified as critical, was found in Brilliance Golden Link Secondary System up to 20250424. Affected is an unknown function of the file /sysframework/logSelect.htm. The manipulation of the argument nodename leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	rule	
CVE-2025-5704	code-projects Real Estate Property Management System User.php sql injection	A vulnerability was found in code-projects Real Estate Property Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /Admin/User.php. The manipulation of the argument txtUserName leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-5705	code-projects Real Estate Property Management System Property.php sql injection	A vulnerability was found in code-projects Real Estate Property Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /Admin/Property.php. The manipulation of the argument cmbCat 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-2025-5706	PHPGurukul Human Metapneumovirus Testing Management System new-user-testing.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 /new-user-testing.php. The manipulation of the argument state 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-2025-5707	PHPGurukul Human Metapneumovirus Testing Management System registered-user-testing.php sql injection	A vulnerability was found in PHPGurukul Human Metapneumovirus Testing Management System 1.0. It has been rated as critical. Affected by this issue is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		some unknown functionality of the file /registered-user-testing.php. The manipulation of the argument testtype 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-2025-5708	code-projects Real Estate Property Management System NewsReport.php sql injection	A vulnerability classified as critical has been found in code-projects Real Estate Property Management System 1.0. This affects an unknown part of the file /Admin/NewsReport.php. The manipulation of the argument txtFrom 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-2025-5709	code-projects Real Estate Property Management System InsertCategory.php sql injection	A vulnerability classified as critical was found in code-projects Real Estate Property Management System 1.0. This vulnerability affects unknown code of the file /Admin/InsertCategory.php. The manipulation of the argument txtCategoryName 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-2025-5710	code-projects Real Estate Property Management System InsertState.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Real Estate Property Management System 1.0. This issue affects some unknown processing of the file /Admin/InsertState.php. The manipulation of the argument txtStateName 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-2025-5711	code-projects Real Estate Property Management System InsertCity.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Real Estate Property Management System 1.0. Affected is an unknown function of the file /Admin/InsertCity.php. The manipulation of the argument cmbState leads to sql injection. It is possible to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		launch the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-5712	SourceCodester Open Source Clinic Management System appointment.php sql injection	A vulnerability has been found in SourceCodester Open Source Clinic Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /appointment.php. The manipulation of the argument patient 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-2025-5716	SourceCodester Open Source Clinic Management System login.php sql injection	A vulnerability classified as critical has been found in SourceCodester Open Source Clinic Management System 1.0. Affected is an unknown function of the file /login.php. The manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-5729	code-projects Health Center Patient Record Management System birthing_record.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Health Center Patient Record Management System 1.0. Affected is an unknown function of the file /birthing_record.php. The manipulation of the argument itr_no 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-2025-5755	SourceCodester Open Source Clinic Management System email_config.php sql injection	A vulnerability was found in SourceCodester Open Source Clinic Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /email_config.php. The manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-5756	code-projects Real Estate Property Management System EditCity.php sql injection	A vulnerability was found in code-projects Real Estate Property Management System 1.0. It has been	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		declared as critical. Affected by this vulnerability is an unknown functionality of the file /Admin/EditCity.php. The manipulation leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-5758	SourceCodester Open Source Clinic Management System doctor.php sql injection	A vulnerability classified as critical has been found in SourceCodester Open Source Clinic Management System 1.0. This affects an unknown part of the file /doctor.php. The manipulation of the argument doctorname leads to sql injection. 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-2025-5759	PHPGurukul Local Services Search Engine Management System edit-person-detail.php sql injection	A vulnerability classified as critical was found in PHPGurukul Local Services Search Engine Management System 2.1. This vulnerability affects unknown code of the file /admin/edit-person-detail.php?editid=2. 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-2025-5761	PHPGurukul BP Monitoring Management System edit-family-member.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul BP Monitoring Management System 1.0. This issue affects some unknown processing of the file /edit-family-member.php. The manipulation of the argument memberage 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-2025-5762	code-projects Patient Record Management System view_hematology.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Patient Record Management System 1.0. Affected is an unknown function of the file view_hematology.php. The manipulation of the argument itr_no leads to sql injection. It is possible to launch the attack remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The exploit has been disclosed to the public and may be used.		
CVE-2025-5778	1000 Projects ABC Courier Management System adminSQL sql injection	A vulnerability, which was classified as critical, was found in 1000 Projects ABC Courier Management System 1.0. Affected is an unknown function of the file /adminSQL. 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-2025-5779	code-projects Patient Record Management System birthing.php sql injection	A vulnerability has been found in code-projects Patient Record Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /birthing.php. The manipulation of the argument itr_no/comp_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-2025-5780	code-projects Patient Record Management System view_dental.php sql injection	A vulnerability was found in code-projects Patient Record Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /view_dental.php. The manipulation of the argument itr_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-2025-5782	PHPGurukul Employee Record Management System resetpassword.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Employee Record Management System 1.3. Affected by this issue is some unknown functionality of the file /resetpassword.php. The manipulation of the argument newpassword 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-2025-5783	PHPGurukul Employee Record Management System editmyexp.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Employee Record	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Management System 1.3. This affects an unknown part of the file /editmyexp.php. The manipulation of the argument emp3workduration 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-2025-5784	PHPGurukul Employee Record Management System myexp.php sql injection	A vulnerability has been found in PHPGurukul Employee Record Management System 1.3 and classified as critical. This vulnerability affects unknown code of the file /myexp.php. The manipulation of the argument emp3ctc 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-2025-5837	PHPGurukul Employee Record Management System allemployees.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Employee Record Management System 1.3. Affected is an unknown function of the file /admin/allemployees.php. The manipulation of the argument delid 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-2025-5838	PHPGurukul Employee Record Management System adminprofile.php sql injection	A vulnerability classified as critical was found in PHPGurukul Employee Record Management System 1.3. Affected by this vulnerability is an unknown functionality of the file /admin/adminprofile.php. The manipulation of the argument AdminName 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-2025-5856	PHPGurukul BP Monitoring Management System registration.php sql injection	A vulnerability has been found in PHPGurukul BP Monitoring Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /registration.php. The manipulation of the argument emailid leads to sql injection. The attack can be initiated 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-2025-5857	code-projects Patient Record Management System urinalysis_record.php sql injection	A vulnerability was found in code-projects Patient Record Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /urinalysis_record.php. The manipulation of the argument itr_no 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-2025-5858	PHPGurukul Nipah Virus Testing Management System patient-report.php sql injection	A vulnerability was found in PHPGurukul Nipah Virus Testing Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /patient-report.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-2025-5859	PHPGurukul Nipah Virus Testing Management System test-details.php sql injection	A vulnerability was found in PHPGurukul Nipah Virus Testing Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /test-details.php. The manipulation of the argument assignto 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-2025-5860	PHPGurukul Maid Hiring Management System search-booking-request.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Maid Hiring Management System 1.0. This affects an unknown part of the file /admin/search-booking-request.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-2025-5881	code-projects Chat System confirm_password.php sql injection	A vulnerability was found in code-projects Chat System up to 1.0 and classified as critical. This issue affects some unknown processing of the file /user/confirm_password.ph	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		p. The manipulation of the argument cid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-5913	PHPGurukul Vehicle Record Management System search-vehicle.php sql injection	A vulnerability was found in PHPGurukul Vehicle Record Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/search-vehicle.php. The manipulation of the argument searchinputdata 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-2025-5971	code-projects School Fees Payment System ajx.php sql injection	A vulnerability was found in code-projects School Fees Payment System 1.0. It has been classified as critical. This affects an unknown part of the file /ajx.php. The manipulation of the argument name_startsWith 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-2025-5977	code-projects School Fees Payment System datatable.php sql injection	A vulnerability was found in code-projects School Fees Payment System 1.0 and classified as critical. This issue affects some unknown processing of the file /datatable.php. The manipulation of the argument sSortDir_0 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-2025-5979	code-projects School Fees Payment System branch.php sql injection	A vulnerability classified as critical has been found in code-projects School Fees Payment System 1.0. This affects an unknown part of the file /branch.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-2025-5980	code-projects Restaurant Order System order.php sql injection	A vulnerability classified as critical was found in code-projects Restaurant Order System 1.0. This vulnerability	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects unknown code of the file /order.php. The manipulation of the argument tabidNoti leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-52474	WeGIA SQL Injection Vulnerability in id Parameter on control.php Endpoint	WeGIA is a web manager for charitable institutions. Prior to version 3.4.2, a SQL Injection vulnerability was identified in the id parameter of the /WeGIA/controle/control.php endpoint. This vulnerability allows attacker to manipulate SQL queries and access sensitive database information, such as table names and sensitive data. This issue has been patched in version 3.4.2.	Patched by core rule	Y
CVE-2025-6005	kiCode111 like-girl aboutPost.php sql injection	A vulnerability classified as critical was found in kiCode111 like-girl 5.2.0. This vulnerability affects unknown code of the file /admin/aboutPost.php. The manipulation of the argument title/aboutimg/info1/info2/info3/btn1/btn2/infox1/infox2/infox3/infox4/infox5/infox6/btnx2/infof1/infof2/infof3/infof4/btnf3/infod1/infod2/infod3/infod4/infod5 leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-6006	kiCode111 like-girl ImgUpdaPost.php sql injection	A vulnerability, which was classified as critical, has been found in kiCode111 like-girl 5.2.0. This issue affects some unknown processing of the file /admin/ImgUpdaPost.php. The manipulation of the argument id/imgText/imgDatd/imgUrl 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-2025-6007	kiCode111 like-girl CopyadminPost.php sql	A vulnerability, which was classified as critical, was	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	found in kiCode111 like-girl 5.2.0. Affected is an unknown function of the file /admin/CopyadminPost.php. The manipulation of the argument icp/Copyright 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-2025-6008	kiCode111 like-girl ImgAddPost.php sql injection	A vulnerability has been found in kiCode111 like-girl 5.2.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/ImgAddPost.php. The manipulation of the argument imgDatd/imgText/imgUrl 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-2025-6009	kiCode111 like-girl ipAddPost.php sql injection	A vulnerability was found in kiCode111 like-girl 5.2.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/ipAddPost.php. The manipulation of the argument bz/ipdz 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-2025-6094	FoxCMS Download.php batchCope sql injection	A vulnerability, which was classified as critical, has been found in FoxCMS up to 1.2.5. This issue affects the function batchCope of the file app/admin/controller/Download.php. The manipulation of the argument ids 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-2025-6095	codesiddhant Jasmin Ransomware checklogin.php sql injection	A vulnerability, which was classified as critical, was found in codesiddhant Jasmin Ransomware 1.0.1.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Affected is an unknown function of the file /checklogin.php. The manipulation of the argument username/password leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-6096	codesiddhant Jasmin Ransomware dashboard.php sql injection	A vulnerability has been found in codesiddhant Jasmin Ransomware up to 1.0.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /dashboard.php. The manipulation of the argument Search leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-6100	realguoshuai open-video-cms list sql injection	A vulnerability was found in realguoshuai open-video-cms 1.0. It has been rated as critical. This issue affects some unknown processing of the file /v1/video/list. The manipulation of the argument sort 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-2025-6116	Das Parking Management System 停车场管理系统 API Search sql injection	A vulnerability was found in Das Parking Management System 停车场管理系统 6.2.0. It has been classified as critical. This affects an unknown part of the file /IntraFieldVehicle/Search of the component API. The manipulation of the argument Value 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-2025-6117	Das Parking Management System 停车场管理系统	A vulnerability was found in Das Parking Management	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	API Search sql injection	System 停车场管理系统 6.2.0. It has been declared as critical. This vulnerability affects unknown code of the file /Reservations/Search of the component API. The manipulation of the argument Value leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6118	Das Parking Management System 停车场管理系统 API search sql injection	A vulnerability was found in Das Parking Management System 停车场管理系统 6.2.0. It has been rated as critical. This issue affects some unknown processing of the file /vehicle/search of the component API. The manipulation of the argument vehicleTypeCode 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-2025-6122	code-projects Restaurant Order System table.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Restaurant Order System 1.0. This affects an unknown part of the file /table.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-2025-6123	code-projects Restaurant Order System payment.php sql injection	A vulnerability has been found in code-projects Restaurant Order System 1.0 and classified as critical. This vulnerability affects unknown code of the file /payment.php. The manipulation of the argument tabidNoti 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-2025-6124	code-projects Restaurant Order System tablelow.php sql injection	A vulnerability was found in code-projects Restaurant Order System 1.0 and classified as critical. This issue affects some unknown processing of the file /tablelow.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the public and may be used.		
CVE-2025-6132	Chanjet CRM departmentsetting.php sql injection	A vulnerability has been found in Chanjet CRM 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /sysconfig/departmentsetting.php. The manipulation of the argument gblOrgID 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-2025-6133	Projectworlds Life Insurance Management System insertagent.php sql injection	A vulnerability was found in Projectworlds Life Insurance Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /insertagent.php. The manipulation of the argument agent_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-2025-6134	Projectworlds Life Insurance Management System insertClient.php sql injection	A vulnerability was found in Projectworlds Life Insurance Management System 1.0. It has been classified as critical. This affects an unknown part of the file /insertClient.php. The manipulation of the argument client_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. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-6135	Projectworlds Life Insurance Management System insertNominee.php sql injection	A vulnerability was found in Projectworlds Life Insurance Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /insertNominee.php. The manipulation of the argument client_id/nominee_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6136	Projectworlds Life Insurance Management System insertPayment.php sql injection	A vulnerability was found in Projectworlds Life Insurance Management System 1.0. It has been rated as critical. This issue affects some	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown processing of the file /insertPayment.php. The manipulation of the argument recipt_no leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6153	PHPGurukul Hostel Management System students.php sql injection	A vulnerability has been found in PHPGurukul Hostel Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/students.php. The manipulation of the argument search_box 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-2025-6154	PHPGurukul Hostel Management System login.inc.php sql injection	A vulnerability was found in PHPGurukul Hostel Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /includes/login.inc.php. The manipulation of the argument student_roll_no 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-2025-6155	PHPGurukul Hostel Management System login-hm.inc.php sql injection	A vulnerability was found in PHPGurukul Hostel Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /includes/login-hm.inc.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-2025-6156	PHPGurukul Nipah Virus Testing Management System bwdates-report-ds.php sql injection	A vulnerability was found in PHPGurukul Nipah Virus Testing Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /bwdates-report-ds.php. The manipulation of the argument testtype 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-2025-6157	PHPGurukul Nipah Virus	A vulnerability was found in	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Testing Management System registered-user-testing.php sql injection	PHPGurukul Nipah Virus Testing Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /registered-user-testing.php. The manipulation of the argument testtype leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	rule	
CVE-2025-6159	code-projects Hostel Management System allocate_room.php sql injection	A vulnerability classified as critical was found in code-projects Hostel Management System 1.0. This vulnerability affects unknown code of the file /allocate_room.php. The manipulation of the argument search_box 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-2025-6160	SourceCodester Client Database Management System user_customer_create_order.php sql injection	A vulnerability, which was classified as critical, has been found in SourceCodester Client Database Management System 1.0. This issue affects some unknown processing of the file /user_customer_create_order.php. The manipulation of the argument user_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-2025-6173	Webkul QloApps ajax_products_list.php sql injection	A vulnerability classified as critical was found in Webkul QloApps 1.6.1. Affected by this vulnerability is an unknown functionality of the file /admin/ajax_products_list.php. The manipulation of the argument packItself leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor confirms the existence of this flaw but considers it a low-level issue due to admin privilege pre-requisites. Still, a fix is planned for a future release.	Patched by core rule	Y
CVE-2025-6276	Brilliance Golden Link Secondary System rentTakeInfoPage.htm sql injection	A vulnerability was found in Brilliance Golden Link Secondary System up to 20250609. It has been rated	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		as critical. Affected by this issue is some unknown functionality of the file /storagework/rentTakeInfoPage.htm. The manipulation of the argument custTradeName leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6277	Brilliance Golden Link Secondary System custTakeInfoPage.htm sql injection	A vulnerability classified as critical has been found in Brilliance Golden Link Secondary System up to 20250609. This affects an unknown part of the file /storagework/custTakeInfoPage.htm. The manipulation of the argument custTradeName 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-2025-6293	code-projects Hostel Management System contact_manager.php sql injection	A vulnerability was found in code-projects Hostel Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /contact_manager.php. The manipulation of the argument student_roll_no 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-2025-6294	code-projects Hostel Management System contact.php sql injection	A vulnerability was found in code-projects Hostel Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /contact.php. The manipulation of the argument hostel_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-2025-6295	code-projects Hostel Management System allocated_rooms.php sql injection	A vulnerability was found in code-projects Hostel Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /allocated_rooms.php. The manipulation of the argument search_box leads to sql injection. The attack	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6296	code-projects Hostel Management System empty_rooms.php sql injection	A vulnerability was found in code-projects Hostel Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /empty_rooms.php. The manipulation of the argument search_box 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-2025-6300	PHPGurukul Employee Record Management System editempeducation.php sql injection	A vulnerability classified as critical was found in PHPGurukul Employee Record Management System 1.3. This vulnerability affects unknown code of the file /admin/editempeducation.php. The manipulation of the argument yopgra 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-2025-6303	code-projects Online Shoe Store contactus1.php sql injection	A vulnerability has been found in code-projects Online Shoe Store 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /contactus1.php. The manipulation of the argument Message 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-2025-6304	code-projects Online Shoe Store cart.php sql injection	A vulnerability was found in code-projects Online Shoe Store 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /cart.php. The manipulation of the argument qty[] 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-2025-6305	code-projects Online Shoe Store admin_feature.php sql injection	A vulnerability was found in code-projects Online Shoe Store 1.0. It has been classified as critical. This affects an unknown part of the file /admin/admin_feature.php.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The manipulation of the argument product_code 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-2025-6306	code-projects Online Shoe Store admin_index.php sql injection	A vulnerability was found in code-projects Online Shoe Store 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/admin_index.php. The manipulation of the argument Username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6307	code-projects Online Shoe Store edit_customer.php sql injection	A vulnerability was found in code-projects Online Shoe Store 1.0. It has been rated as critical. This issue affects some unknown processing of the file /function/edit_customer.php. The manipulation of the argument firstname 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-2025-6308	PHPGurukul Emergency Ambulance Hiring Portal bwdates-request-report-details.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Emergency Ambulance Hiring Portal 1.0. Affected is an unknown function of the file /admin/bwdates-request-report-details.php. The manipulation of the argument fromdate/todate 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-2025-6309	PHPGurukul Emergency Ambulance Hiring Portal add-ambulance.php sql injection	A vulnerability classified as critical was found in PHPGurukul Emergency Ambulance Hiring Portal 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/add-ambulance.php. The manipulation of the argument ambregnum 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-6310	PHPGurukul Emergency Ambulance Hiring Portal index.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Emergency Ambulance Hiring Portal 1.0. Affected by this issue is some unknown functionality of the file /index.php. The manipulation of the argument Message leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-6311	Campcodes Sales and Inventory System account_add.php sql injection	A vulnerability, which was classified as critical, was found in Campcodes Sales and Inventory System 1.0. This affects an unknown part of the file /pages/account_add.php. The manipulation of the argument id/amount 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-2025-6312	Campcodes Sales and Inventory System cash_transaction.php sql injection	A vulnerability has been found in Campcodes Sales and Inventory System 1.0 and classified as critical. This vulnerability affects unknown code of the file /pages/cash_transaction.php. The manipulation of the argument cid 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-2025-6313	Campcodes Sales and Inventory System cat_add.php sql injection	A vulnerability was found in Campcodes Sales and Inventory System 1.0 and classified as critical. This issue affects some unknown processing of the file /pages/cat_add.php. The manipulation of the argument Category 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-2025-6314	Campcodes Sales and Inventory System cat_update.php sql injection	A vulnerability was found in Campcodes Sales and Inventory System 1.0. It has been classified as critical. Affected is an unknown function of the file /pages/cat_update.php. The manipulation of the argument ID leads to sql	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6315	code-projects Online Shoe Store cart2.php sql injection	A vulnerability was found in code-projects Online Shoe Store 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /cart2.php. The manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6316	code-projects Online Shoe Store admin_running.php sql injection	A vulnerability was found in code-projects Online Shoe Store 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/admin_running.php. The manipulation of the argument qty 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-2025-6317	code-projects Online Shoe Store confirm.php sql injection	A vulnerability classified as critical has been found in code-projects Online Shoe Store 1.0. This affects an unknown part of the file /admin/confirm.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-2025-6318	PHPGurukul Pre-School Enrollment System check_availability.php sql injection	A vulnerability classified as critical was found in PHPGurukul Pre-School Enrollment System 1.0. This vulnerability affects unknown code of the file /admin/check_availability.php. The manipulation of the argument Username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6319	PHPGurukul Pre-School Enrollment System add-teacher.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Pre-School Enrollment System 1.0. This issue affects some unknown processing of the file /admin/add-teacher.php. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument tsubject leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6320	PHPGurukul Pre-School Enrollment System add-class.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Pre-School Enrollment System 1.0. Affected is an unknown function of the file /admin/add-class.php. The manipulation of the argument classname 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-2025-6321	PHPGurukul Pre-School Enrollment System add-subadmin.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/add-subadmin.php. The manipulation of the argument sadminusername 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-2025-6322	PHPGurukul Pre-School Enrollment System visit.php sql injection	A vulnerability was found in PHPGurukul Pre-School Enrollment System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /visit.php. The manipulation of the argument gname 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-2025-6323	PHPGurukul Pre-School Enrollment System enrollment.php sql injection	A vulnerability was found in PHPGurukul Pre-School Enrollment System 1.0. It has been classified as critical. This affects an unknown part of the file /enrollment.php. The manipulation of the argument fathername leads to sql injection. 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-2025-6330	PHPGurukul Directory	A vulnerability classified as	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Management System searchdata.php sql injection	critical has been found in PHPGurukul Directory Management System 1.0. Affected is an unknown function of the file /searchdata.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.	rule	
CVE-2025-6331	PHPGurukul Directory Management System search-directory.php sql injection	A vulnerability classified as critical was found in PHPGurukul Directory Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/search-directory.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-2025-6332	PHPGurukul Directory Management System manage-directory.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Directory Management System 2.0. Affected by this issue is some unknown functionality of the file /admin/manage-directory.php. The manipulation of the argument del 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-2025-6333	PHPGurukul Directory Management System admin-profile.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Directory Management System 2.0. This affects an unknown part of the file /admin/admin-profile.php. The manipulation of the argument adminname 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-2025-6339	ponaravindb Hospital Management System func3.php sql injection	A vulnerability was found in ponaravindb Hospital Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /func3.php. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument username1 leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6342	code-projects Online Shoe Store admin_football.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Online Shoe Store 1.0. This issue affects some unknown processing of the file /admin/admin_football.php. The manipulation of the argument pid 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-2025-6343	code-projects Online Shoe Store admin_product.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Online Shoe Store 1.0. Affected is an unknown function of the file /admin/admin_product.php. The manipulation of the argument pid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6344	code-projects Online Shoe Store contactus.php sql injection	A vulnerability has been found in code-projects Online Shoe Store 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /contactus.php. The manipulation of the argument email leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6346	SourceCodester Advance Charity Management System fundDetails.php sql injection	A vulnerability was found in SourceCodester Advance Charity Management System 1.0. It has been classified as critical. This affects an unknown part of the file /members/fundDetails.php. The manipulation of the argument m06 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-2025-6351	itsourcecode Employee Record Management System editprofile.php sql injection	A vulnerability was found in itsourcecode Employee Record Management System 1.0. It has been rated as critical. This issue affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		some unknown processing of the file /editprofile.php. The manipulation of the argument emp1name leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6354	code-projects Online Shoe Store customer_signup.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Online Shoe Store 1.0. Affected by this issue is some unknown functionality of the file /function/customer_signup.php. The manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6355	SourceCodester Online Hotel Reservation System exceditroom.php sql injection	A vulnerability has been found in SourceCodester Online Hotel Reservation System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/exceditroom.php. The manipulation of the argument userid 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-2025-6356	code-projects Simple Pizza Ordering System addmem.php sql injection	A vulnerability was found in code-projects Simple Pizza Ordering System 1.0 and classified as critical. This issue affects some unknown processing of the file /addmem.php. The manipulation 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-2025-6357	code-projects Simple Pizza Ordering System paymentportal.php sql injection	A vulnerability was found in code-projects Simple Pizza Ordering System 1.0. It has been classified as critical. Affected is an unknown function of the file /paymentportal.php. The manipulation of the argument person 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-2025-6358	code-projects Simple Pizza Ordering System	A vulnerability was found in code-projects Simple Pizza	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	saveorder.php sql injection	Ordering System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /saveorder.php. The manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6359	code-projects Simple Pizza Ordering System cashconfirm.php sql injection	A vulnerability was found in code-projects Simple Pizza Ordering System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /cashconfirm.php. The manipulation of the argument transactioncode 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-2025-6360	code-projects Simple Pizza Ordering System portal.php sql injection	A vulnerability classified as critical has been found in code-projects Simple Pizza Ordering System 1.0. This affects an unknown part of the file /portal.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-2025-6361	code-projects Simple Pizza Ordering System adds.php sql injection	A vulnerability classified as critical was found in code-projects Simple Pizza Ordering System 1.0. This vulnerability affects unknown code of the file /adds.php. The manipulation of the argument userid leads to sql injection. The attack can be initiated remotely.	Patched by core rule	Y
CVE-2025-6362	code-projects Simple Pizza Ordering System editpro.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Simple Pizza Ordering System 1.0. This issue affects some unknown processing of the file /editpro.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely.	Patched by core rule	Y
CVE-2025-6363	code-projects Simple Pizza Ordering System adding-exec.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Simple Pizza Ordering System 1.0. Affected is an unknown function of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/adding-exec.php. The manipulation of the argument ingname leads to sql injection. It is possible to launch the attack remotely.		
CVE-2025-6364	code-projects Simple Pizza Ordering System adduser-exec.php sql injection	A vulnerability has been found in code-projects Simple Pizza Ordering System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /adduser-exec.php. The manipulation of the argument Username leads to sql injection. The attack can be launched remotely.	Patched by core rule	Y
CVE-2025-6394	code-projects Simple Online Hotel Reservation System add_reserve.php sql injection	A vulnerability was found in code-projects Simple Online Hotel Reservation System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /add_reserve.php. The manipulation of the argument firstname 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-2025-6403	code-projects School Fees Payment System student.php sql injection	A vulnerability was found in code-projects School Fees Payment System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /student.php. The manipulation of the argument 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-2025-6404	Campcodes Online Teacher Record Management System search.php sql injection	A vulnerability classified as critical has been found in Campcodes Online Teacher Record Management System 1.0. Affected is an unknown function of the file /admin/search.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-2025-6405	Campcodes Online Teacher Record Management System edit-teacher-detail.php sql injection	A vulnerability classified as critical was found in Campcodes Online Teacher Record Management System 1.0. Affected by this	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability is an unknown functionality of the file /admin/edit-teacher-detail.php. The manipulation of the argument editid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6406	Campcodes Online Hospital Management System forgot-password.php sql injection	A vulnerability, which was classified as critical, has been found in Campcodes Online Hospital Management System 1.0. Affected by this issue is some unknown functionality of the file /hms/forgot-password.php. The manipulation of the argument fullname 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-2025-6407	Campcodes Online Hospital Management System user-login.php sql injection	A vulnerability, which was classified as critical, was found in Campcodes Online Hospital Management System 1.0. This affects an unknown part of the file /user-login.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-2025-6408	Campcodes Online Hospital Management System search.php sql injection	A vulnerability has been found in Campcodes Online Hospital Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /doctor/search.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-2025-6409	PHPGurukul Art Gallery Management System forgot-password.php sql injection	A vulnerability was found in PHPGurukul Art Gallery Management System 1.1 and classified as critical. This issue affects some unknown processing of the file /admin/forgot-password.php. The manipulation of the argument email leads to sql injection. The attack may be initiated 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-2025-6410	PHPGurukul Art Gallery Management System edit-art-medium-detail.php sql injection	A vulnerability was found in PHPGurukul Art Gallery Management System 1.1. It has been classified as critical. Affected is an unknown function of the file /admin/edit-art-medium-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-2025-6411	PHPGurukul Art Gallery Management System changepropic.php sql injection	A vulnerability was found in PHPGurukul Art Gallery Management System 1.1. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/changepropic.php. The manipulation of the argument imageid 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-2025-6412	PHPGurukul Art Gallery Management System changeimage.php sql injection	A vulnerability was found in PHPGurukul Art Gallery Management System 1.1. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/changeimage.php. The manipulation of the argument editid 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-2025-6413	PHPGurukul Art Gallery Management System changeimage1.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Art Gallery Management System 1.1. This affects an unknown part of the file /admin/changeimage1.php. The manipulation of the argument editid 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-2025-6414	PHPGurukul Art Gallery Management System changeimage2.php sql injection	A vulnerability classified as critical was found in PHPGurukul Art Gallery Management System 1.1. This vulnerability affects unknown code of the file /admin/changeimage2.php.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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.		
CVE-2025-6415	PHPGurukul Art Gallery Management System changeimage3.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Art Gallery Management System 1.1. This issue affects some unknown processing of the file /admin/changeimage3.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-2025-6416	PHPGurukul Art Gallery Management System changeimage4.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 /admin/changeimage4.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-2025-6417	PHPGurukul Art Gallery Management System add-artist.php sql injection	A vulnerability has been found in PHPGurukul Art Gallery Management System 1.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/add-artist.php. The manipulation of the argument awarddetails 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-2025-6418	code-projects Simple Online Hotel Reservation System edit_query_account.php sql injection	A vulnerability was found in code-projects Simple Online Hotel Reservation System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/edit_query_account.php. The manipulation of the argument Name leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6419	code-projects Simple Online Hotel Reservation System edit_room.php	A vulnerability was found in code-projects Simple Online Hotel Reservation System	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	sql injection	1.0. It has been classified as critical. This affects an unknown part of the file /admin/edit_room.php. The manipulation of the argument room_type 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-2025-6420	code-projects Simple Online Hotel Reservation System add_room.php sql injection	A vulnerability was found in code-projects Simple Online Hotel Reservation System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/add_room.php. The manipulation of the argument room_type 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-2025-6421	code-projects Simple Online Hotel Reservation System add_account.php sql injection	A vulnerability was found in code-projects Simple Online Hotel Reservation System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/add_account.php. The manipulation of the argument name/admin_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-2025-6446	code-projects Client Details System index.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Client Details System 1.0. This issue affects some unknown processing of the file /clientdetails/admin/index.php. The manipulation of the argument Username leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6447	code-projects Simple Online Hotel Reservation System index.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Simple Online Hotel Reservation System 1.0. Affected is an unknown function of the file /admin/index.php. The manipulation of the argument Username leads to sql injection. It is possible to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		launch the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6448	code-projects Simple Online Hotel Reservation System delete_room.php sql injection	A vulnerability has been found in code-projects Simple Online Hotel Reservation System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/delete_room.php. The manipulation of the argument room_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-2025-6449	code-projects Simple Online Hotel Reservation System checkout_query.php sql injection	A vulnerability was found in code-projects Simple Online Hotel Reservation System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/checkout_query.php. The manipulation of the argument transaction_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-2025-6450	code-projects Simple Online Hotel Reservation System confirm_reserve.php sql injection	A vulnerability was found in code-projects Simple Online Hotel Reservation System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/confirm_reserve.php. The manipulation of the argument transaction_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-2025-6451	code-projects Simple Online Hotel Reservation System delete_pending.php sql injection	A vulnerability was found in code-projects Simple Online Hotel Reservation System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/delete_pending.php. The manipulation of the argument transaction_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-6455	code-projects Online Hotel Reservation System messageexec.php sql injection	A vulnerability classified as critical was found in code-projects Online Hotel Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file /messageexec.php. The manipulation of the argument Name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6456	code-projects Online Hotel Reservation System order.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Online Hotel Reservation System 1.0. Affected by this issue is some unknown functionality of the file /reservation/order.php. The manipulation of the argument Start 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-2025-6457	code-projects Online Hotel Reservation System demo.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Online Hotel Reservation System 1.0. This affects an unknown part of the file /reservation/demo.php. The manipulation of the argument Start 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-2025-6458	code-projects Online Hotel Reservation System execedituser.php sql injection	A vulnerability has been found in code-projects Online Hotel Reservation System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/execedituser.php. The manipulation of the argument userid 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-2025-6467	code-projects Online Bidding System login.php sql injection	A vulnerability was found in code-projects Online Bidding System 1.0. It has been classified as critical. This affects an unknown part of the file /login.php. The manipulation of the argument User leads to sql injection. It is possible to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		initiate the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6468	code-projects Online Bidding System bidnow.php sql injection	A vulnerability was found in code-projects Online Bidding System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /bidnow.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-2025-6469	code-projects Online Bidding System details.php sql injection	A vulnerability was found in code-projects Online Bidding System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /details.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6470	code-projects Online Bidding System bidlog.php sql injection	A vulnerability classified as critical has been found in code-projects Online Bidding System 1.0. Affected is an unknown function of the file /bidlog.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-2025-6471	code-projects Online Bidding System administrator sql injection	A vulnerability classified as critical was found in code-projects Online Bidding System 1.0. Affected by this vulnerability is an unknown functionality of the file /administrator. The manipulation of the argument aduser 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-2025-6472	code-projects Online Bidding System showprod.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Online Bidding System 1.0. Affected by this issue is some unknown functionality of the file /showprod.php. The manipulation of the argument ID leads to sql injection. The attack may be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6474	code-projects Inventory Management System changeUsername.php sql injection	A vulnerability has been found in code-projects Inventory Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /changeUsername.php. The manipulation of the argument user_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-2025-6479	code-projects Simple Pizza Ordering System salesreport.php sql injection	A vulnerability classified as critical has been found in code-projects Simple Pizza Ordering System 1.0. This affects an unknown part of the file /salesreport.php. The manipulation of the argument dayfrom 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-2025-6480	code-projects Simple Pizza Ordering System addcatexec.php sql injection	A vulnerability classified as critical was found in code-projects Simple Pizza Ordering System 1.0. This vulnerability affects unknown code of the file /addcatexec.php. The manipulation of the argument textfield 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-2025-6481	code-projects Simple Pizza Ordering System update.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Simple Pizza Ordering System 1.0. This issue affects some unknown processing of the file /update.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6482	code-projects Simple Pizza Ordering System edituser-exec.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Simple Pizza Ordering System 1.0. Affected is an unknown function of the file /edituser-exec.php. The manipulation of the argument userid leads to sql injection. It is possible to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		launch the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6483	code-projects Simple Pizza Ordering System edituser.php sql injection	A vulnerability has been found in code-projects Simple Pizza Ordering System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /edituser.php. The manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6484	code-projects Online Shopping Store action.php sql injection	A vulnerability was found in code-projects Online Shopping Store 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /action.php. The manipulation of the argument cat_id/brand_id/keyword/proId/pid 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-2025-6489	itsourcecode Agri-Trading Online Shopping System transactionsave.php sql injection	A vulnerability has been found in itsourcecode Agri-Trading Online Shopping System 1.0 and classified as critical. This vulnerability affects unknown code of the file /transactionsave.php. The manipulation of the argument del 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-2025-6500	code-projects Inventory Management System editCategories.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Inventory Management System 1.0. Affected by this issue is some unknown functionality of the file /php_action/editCategories.php. The manipulation of the argument editCategoriesName 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-2025-6501	code-projects Inventory Management System createCategories.php sql injection	A vulnerability, which was classified as critical, was found in code-projects Inventory Management	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		System 1.0. This affects an unknown part of the file /php_action/createCategories.php. The manipulation of the argument categoriesStatus 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-2025-6502	code-projects Inventory Management System changePassword.php sql injection	A vulnerability has been found in code-projects Inventory Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /php_action/changePassword.php. The manipulation of the argument user_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-2025-6503	code-projects Inventory Management System fetchSelectedCategories.php sql injection	A vulnerability was found in code-projects Inventory Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /php_action/fetchSelectedCategories.php. The manipulation of the argument categoriesId 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-2025-6567	Campcodes Online Recruitment Management System view_application.php sql injection	A vulnerability was found in Campcodes Online Recruitment Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file Recruitment/admin/view_application.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-2025-6570	PHPGurukul Hospital Management System search.php sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Hospital Management System 4.0. Affected by this issue is some unknown functionality of the file /doctor/search.php. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument searchdata leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6578	code-projects Simple Online Hotel Reservation System delete_account.php sql injection	A vulnerability was found in code-projects Simple Online Hotel Reservation System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/delete_account.php. The manipulation of the argument admin_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-2025-6579	code-projects Car Rental System message_admin.php sql injection	A vulnerability was found in code-projects Car Rental System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /message_admin.php. The manipulation of the argument Message 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-2025-6580	SourceCodester Best Salon Management System Login sql injection	A vulnerability classified as critical has been found in SourceCodester Best Salon Management System 1.0. Affected is an unknown function of the component Login. 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-2025-6581	SourceCodester Best Salon Management System add-customer.php sql injection	A vulnerability classified as critical was found in SourceCodester Best Salon Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /add-customer.php. The manipulation of the argument name/email/mobilenum/gender/details/dob/marriage_date 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-2025-6582	SourceCodester Best Salon Management	A vulnerability, which was classified as critical, has	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System edit-customer-detailed.php sql injection	been found in SourceCodester Best Salon Management System 1.0. Affected by this issue is some unknown functionality of the file /edit-customer-detailed.php. The manipulation of the argument editid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6583	SourceCodester Best Salon Management System view-appointment.php sql injection	A vulnerability, which was classified as critical, was found in SourceCodester Best Salon Management System 1.0. This affects an unknown part of the file /view-appointment.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-2025-6604	SourceCodester Best Salon Management System add-staff.php sql injection	A vulnerability classified as critical has been found in SourceCodester Best Salon Management System 1.0. This affects an unknown part of the file /panel/add-staff.php. The manipulation of the argument Name leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6605	SourceCodester Best Salon Management System edit-staff.php sql injection	A vulnerability classified as critical was found in SourceCodester Best Salon Management System 1.0. This vulnerability affects unknown code of the file /panel/edit-staff.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-2025-6606	SourceCodester Best Salon Management System add-services.php sql injection	A vulnerability, which was classified as critical, has been found in SourceCodester Best Salon Management System 1.0. This issue affects some unknown processing of the file /panel/add-services.php. The manipulation of the argument Type leads to sql injection. The attack may be initiated remotely. The		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit has been disclosed to the public and may be used.		
CVE-2025-6607	SourceCodester Best Salon Management System stock.php sql injection	A vulnerability, which was classified as critical, was found in SourceCodester Best Salon Management System 1.0. Affected is an unknown function of the file /panel/stock.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-2025-6608	SourceCodester Best Salon Management System edit-services.php sql injection	A vulnerability has been found in SourceCodester Best Salon Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /panel/edit-services.php. The manipulation of the argument editid 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-2025-6609	SourceCodester Best Salon Management System bwdates-reports-details.php sql injection	A vulnerability was found in SourceCodester Best Salon Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /panel/bwdates-reports-details.php. The manipulation of the argument fromdate/todate 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-2025-6610	itsourcecode Employee Management System editempprofile.php sql injection	A vulnerability was found in itsourcecode Employee Management System up to 1.0. It has been classified as critical. This affects an unknown part of the file /admin/editempprofile.php. The manipulation of the argument FirstName 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-2025-6611	code-projects Inventory Management System createBrand.php sql injection	A vulnerability was found in code-projects Inventory 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
		/php_action/createBrand.php. The manipulation of the argument brandStatus leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6612	code-projects Inventory Management System removeCategories.php sql injection	A vulnerability was found in code-projects Inventory Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /php_action/removeCategories.php. The manipulation of the argument categoriesId 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-2025-6665	code-projects Inventory Management System editBrand.php sql injection	A vulnerability has been found in code-projects Inventory Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /php_action/editBrand.php. The manipulation of the argument editBrandStatus 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-2025-6668	code-projects Inventory Management System fetchSelectedBrand.php sql injection	A vulnerability was found in code-projects Inventory Management System 1.0. It has been classified as critical. This affects an unknown part of the file /php_action/fetchSelectedBrand.php. The manipulation of the argument brandId 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

XML External Entity Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-48882	PHPOffice Math allows XXE when processing an XML file in the MathML format	PHPOffice Math is a library that provides a set of classes to manipulate different formula file formats. Prior to version 0.3.0, loading XML data using the standard `libxml` extension and the `LIBXML_DTDLOAD` flag without additional filtration, leads to XXE. Version 0.3.0 fixes the vulnerability.	Patched by core rule	Y
CVE-2025-30220	GeoTools, GeoServer, and GeoNetwork XML External Entity (XXE) Processing Vulnerability in XSD schema handling	GeoServer is an open source server that allows users to share and edit geospatial data. GeoTools Schema class use of Eclipse XSD library to represent schema data structure is vulnerable to XML External Entity (XXE) exploit. This impacts whoever exposes XML processing with gt-xsd-core involved in parsing, when the documents carry a reference to an external XML schema. The gt-xsd-core Schemas class is not using the EntityResolver provided by the ParserHandler (if any was configured). This also impacts users of gt-wfs-ng DataStore where the ENTITY_RESOLVER connection parameter was not being used as intended. This vulnerability is fixed in GeoTools 33.1, 32.3, 31.7, and 28.6.1, GeoServer 2.27.1, 2.26.3, and 2.25.7, and GeoNetwork 4.4.8 and 4.2.13.	Patched by core rule	Y
CVE-2025-5877	Fengoffice Feng Office Document Upload ApplicationDataObject.class.php xml external entity reference	A vulnerability, which was classified as problematic, has been found in Fengoffice Feng Office 3.2.2.1. Affected by this issue is some unknown functionality of the file /application/models/ApplicationDataObject.class.php of the component Document Upload Handler. 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. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-1461	Vuetify XSS through 'eventMoreText' prop of VCalendar	Improper neutralization of the value of the 'eventMoreText' property of the 'VCalendar' component in Vuetify allows unsanitized HTML to be inserted into the page. This can lead to a Cross-Site Scripting (XSS) https://owasp.org/www-community/attacks/xss attack. The vulnerability occurs because the default Vuetify translator will return the translation key as the translation, if it can't find an actual translation. This issue affects Vuetify versions greater than or equal to 2.0.0 and less than 3.0.0. Note: Version 2.x of Vuetify is End-of-Life and will not receive any updates to address this issue. For more information see here https://v2.vuetifyjs.com/en/about/eol/ .	Patched by core rule	Y
CVE-2025-3704	WordPress Volunteer Sign Up Sheets plugin < 5.5.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DBAR Productions Volunteer Sign Up Sheets allows Stored XSS.This issue affects Volunteer Sign Up Sheets: from n/a before 5.5.5. The patch is available exclusively on GitHub at https://github.com/dbarproductions/pta-volunteer-sign-up-sheets , as the vendor encounters difficulties using SVN to deploy to the WordPress.org repository.	Patched by core rule	Y
CVE-2025-47933	Argo CD allows cross-site scripting on repositories page	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Prior to versions 2.13.8, 2.14.13, and 3.0.4, an attacker can perform arbitrary actions on behalf of the victim via the API. Due to the improper filtering of URL protocols in the repository page, an attacker can achieve cross-site scripting with permission to edit the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		repository. This issue has been patched in versions 2.13.8, 2.14.13, and 3.0.4.		
CVE-2025-48483	FreeScout Stored XSS leads to CSRF	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.180, the application is vulnerable to Cross-Site Scripting (XSS) attacks due to incorrect input validation and sanitization of user-input data during mail signature sanitization. An attacker can inject arbitrary HTML code, including JavaScript scripts, into the page processed by the user's browser, allowing them to steal sensitive data, hijack user sessions, or conduct other malicious activities. Additionally, if an administrator accesses one of these emails with a modified signature, it could result in a subsequent Cross-Site Request Forgery (CSRF) vulnerability. This issue has been patched in version 1.8.180.	Patched by core rule	Y
CVE-2025-48484	FreeScout Vulnerable to Stored XSS	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.178, the application is vulnerable to Cross-Site Scripting (XSS) attacks due to incorrect input validation and sanitization of user-input data in the conversation POST data body. This issue has been patched in version 1.8.178.	Patched by core rule	Y
CVE-2025-48485	FreeScout Vulnerable to Stored XSS	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.180, the application is vulnerable to Cross-Site Scripting (XSS) attacks due to incorrect input validation and sanitization of user-input data when an authenticated user updates the profile of an arbitrary customer. This issue has been patched in version 1.8.180.	Patched by core rule	Y
CVE-2025-48486	FreeScout Vulnerable to Stored XSS	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.180, the cross-site scripiting (XSS) vulnerability is caused by the lack of input validation and sanitization in both \Session::flash and __, allowing user input to be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		executed without proper filtering. This issue has been patched in version 1.8.180.		
CVE-2025-48487	FreeScout Vulnerable to Stored XSS	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.180, when creating a translation of a phrase that appears in a flash-message after a completed action, it is possible to inject a payload to exploit XSS vulnerability. This issue has been patched in version 1.8.180.	Patched by core rule	Y
CVE-2025-48488	FreeScout Vulnerable to Stored XSS	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.180, deleting the file .htaccess allows an attacker to upload an HTML file containing malicious JavaScript code to the server, which can result in a Cross-Site Scripting (XSS) vulnerability. This issue has been patched in version 1.8.180.	Patched by core rule	Y
CVE-2025-48489	FreeScout Vulnerable to Stored XSS	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.180, the application is vulnerable to Cross-Site Scripting (XSS) attacks due to insufficient data validation and sanitization during data reception. This issue has been patched in version 1.8.180.	Patched by core rule	Y
CVE-2025-48875	FreeScout Vulnerable to Stored XSS	FreeScout is a free self-hosted help desk and shared mailbox. Prior to version 1.8.181, the system's incorrect validation of last_name and first_name during profile data updates allows for the injection of arbitrary JavaScript code, which will be executed in a flesh-message when the data is deleted, potentially leading to a Cross-Site Scripting (XSS) vulnerability. This issue has been patched in version 1.8.181.	Patched by core rule	Y
CVE-2025-48883	Chrome PHP is missing encoding in `CssSelector`	Chrome PHP allows users to start playing with chrome/chromium in headless mode from PHP. Prior to version 1.14.0, CSS Selector expressions are not properly encoded, which can lead to XSS (cross-site scripting) vulnerabilities. This is patched in v1.14.0. As	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		a workaround, users can apply encoding manually to their selectors if they are unable to upgrade.		
CVE-2025-5181	Summer Pearl Group Vacation Rental Management Platform updateListing cross site scripting	A vulnerability, which was classified as problematic, was found in Summer Pearl Group Vacation Rental Management Platform up to 1.0.1. This affects an unknown part of the file /spgpm/updateListing. The manipulation of the argument spgLsTitle 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. Upgrading to version 1.0.2 is able to address this issue. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-5235	OpenSheetMusicDisplay <= 1.4.0 - Authenticated (Contributor+) Stored Cross-Site Scripting via className Parameter	The OpenSheetMusicDisplay plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'className' parameter in all versions up to, and including, 1.4.0 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-2025-5383	Yifang CMS Article Management Module cross site scripting	A vulnerability was found in Yifang CMS up to 2.0.2 and classified as problematic. Affected by this issue is some unknown functionality of the component Article Management Module. The manipulation of the argument Default Value 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-2025-31136	FreshRSS vulnerable to Cross-site Scripting by <iframe>'ing a vulnerable same-origin page in a feed entry	FreshRSS is a self-hosted RSS feed aggregator. Prior to version 1.26.2, it's possible to run arbitrary JavaScript on the feeds page. This occurs by combining a cross-site scripting (XSS) issue that occurs in `f.php` when SVG favicons are downloaded from an attacker-controlled feed	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		containing `<script>` tags inside of them that aren't sanitized, with the lack of CSP in `f.php` by embedding the malicious favicon in an iframe (that has `sandbox="allow-scripts allow-same-origin"` set as its attribute). An attacker needs to control one of the feeds that the victim is subscribed to, and also must have an account on the FreshRSS instance. Other than that, the iframe payload can be embedded as one of two options. The first payload requires user interaction (the user clicking on the malicious feed entry) with default user configuration, and the second payload fires instantly right after the user adds the feed or logs into the account while the feed entry is still visible. This is because of lazy image loading functionality, which the second payload bypasses. An attacker can gain access to the victim's account by exploiting this vulnerability. If the victim is an admin it would be possible to delete all users (cause damage) or execute arbitrary code on the server by modifying the update URL using fetch() via the XSS. Version 1.26.2 has a patch for the issue.		
CVE-2025-32015	FreshRSS vulnerable to Cross-site Scripting by embedding <script> tag inside <iframe srcdoc>	FreshRSS is a self-hosted RSS feed aggregator. Prior to version 1.26.2, HTML is sanitized improperly inside the `<iframe srcdoc>` attribute, which leads to cross-site scripting (XSS) by loading an attacker's UserJS inside `<script src>`. In order to execute the attack, the attacker needs to control one of the victim's feeds and have an account on the FreshRSS instance that the victim is using. An attacker can gain access to the victim's account by exploiting this vulnerability. If the victim is an admin it would be possible to delete all users (cause damage) or execute arbitrary code on the server by modifying the update URL using fetch() via the XSS. Version 1.26.2 contains a patch for the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		issue.		
CVE-2025-4392	Shared Files <= 1.7.48 - Unauthenticated Stored Cross-Site Scripting via sanitize_file Function	The Shared Files – Frontend File Upload Form & Secure File Sharing plugin for WordPress is vulnerable to Stored Cross-Site Scripting via html File uploads in all versions up to, and including, 1.7.48 due to insufficient input sanitization and output escaping within the sanitize_file() function. This makes it possible for unauthenticated attackers to bypass the plugin's MIME-only checks and inject arbitrary web scripts in pages that will execute whenever a user accesses the html file.	Patched by core rule	Y
CVE-2025-48494	Gokapi vulnerable to stored XSS via uploading file with malicious file name	Gokapi is a self-hosted file sharing server with automatic expiration and encryption support. When using end-to-end encryption, a stored cross-site scripting vulnerability can be exploited by uploading a file with JavaScript code embedded in the filename. After upload and every time someone opens the upload list, the script is then parsed. Prior to version 2.0.0, there was no user permission system implemented, therefore all authenticated users were already able to see and modify all resources, even if end-to-end encrypted, as the encryption key had to be the same for all users using a version prior to 2.0.0. If a user is the only authenticated user using Gokapi, they are not affected. This issue has been fixed in v2.0.0. A possible workaround would be to disable end-to-end encryption.	Patched by core rule	Y
CVE-2025-49130	Laravel Translation Manager Vulnerable to Stored Cross-site Scripting	Laravel Translation Manager is a package to manage Laravel translation files. Prior to version 0.6.8, the application is vulnerable to Cross-Site Scripting (XSS) attacks due to incorrect input validation and sanitization of user-input data. An attacker can inject arbitrary HTML code, including JavaScript scripts, into the page processed by the user's browser, allowing	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		them to steal sensitive data, hijack user sessions, or conduct other malicious activities. Only authenticated users with access to the translation manager are impacted. The issue is fixed in version 0.6.8.		
CVE-2025-5116	WP Plugin Info Card <= 5.3.1 - Authenticated (Contributor+) Stored Cross-Site Scripting via containerid Parameter	The WP Plugin Info Card plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'containerid' parameter in all versions up to, and including, 5.3.1 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. This issue is due to an incomplete patch for CVE-2025-31835.	Patched by core rule	Y
CVE-2025-5405	chaitak-gorai Blogbook post.php cross site scripting	A vulnerability, which was classified as problematic, has been found in chaitak-gorai Blogbook up to 92f5cf90f8a7e6566b576fe0952e14e1c6736513. This issue affects some unknown processing of the file /post.php. The manipulation of the argument comment_author/comment_email/comment_content 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 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.	Patched by core rule	Y
CVE-2025-5407	chaitak-gorai Blogbook register_script.php cross site scripting	A vulnerability has been found in chaitak-gorai Blogbook up to 92f5cf90f8a7e6566b576fe0952e14e1c6736513 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /register_script.php. The manipulation of the argument fullname leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. It is recommended to upgrade the affected component. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-5411	Mist Community Edition views.py tag_resources cross site scripting	A vulnerability was found in Mist Community Edition up to 4.7.1. It has been rated as problematic. This issue affects the function tag_resources of the file src/mist/api/tag/views.py. The manipulation of the argument tag leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.7.2 is able to address this issue. The patch is named db10ecb62ac832c1ed4924556d167efb9bc07fad. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-5412	Mist Community Edition Authentication Endpoint views.py login cross site scripting	A vulnerability classified as problematic has been found in Mist Community Edition up to 4.7.1. Affected is the function Login of the file src/mist/api/views.py of the component Authentication Endpoint. The manipulation of the argument return_to 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. Upgrading to version 4.7.2 is able to address this issue. The name of the patch is db10ecb62ac832c1ed4924556d167efb9bc07fad. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-5420	juzaweb CMS Profile Page upload cross site scripting	A vulnerability classified as problematic was found in juzaweb CMS up to 3.4.2. Affected by this vulnerability is an unknown functionality of the file /admin-cp/file-manager/upload of the component Profile Page. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument Upload leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-5505	TOTOLINK A3002RU Virtual Server Page formPortFw cross site scripting	A vulnerability was found in TOTOLINK A3002RU 2.1.1-B20230720.1011 and classified as problematic. This issue affects some unknown processing of the file /boafrm/formPortFw of the component Virtual Server Page. The manipulation of the argument service_type 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-2025-5506	TOTOLINK A3002RU NAT Mapping Page cross site scripting	A vulnerability was found in TOTOLINK A3002RU 2.1.1-B20230720.1011. It has been classified as problematic. Affected is an unknown function of the component NAT Mapping Page. The manipulation of the argument Comment 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-2025-5507	TOTOLINK A3002RU MAC Filtering Page cross site scripting	A vulnerability was found in TOTOLINK A3002RU 2.1.1-B20230720.1011. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component MAC Filtering Page. The manipulation of the argument Comment 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-2025-5508	TOTOLINK A3002RU IP	A vulnerability was found in	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Port Filtering Page cross site scripting	TOTOLINK A3002RU 2.1.1-B20230720.1011. It has been rated as problematic. Affected by this issue is some unknown functionality of the component IP Port Filtering Page. The manipulation of the argument Comment leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	rule	
CVE-2025-5513	quequnlong shiyi-blog add cross site scripting	A vulnerability has been found in quequnlong shiyi-blog up to 1.2.1 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /dev-api/api/comment/add. The manipulation of the argument content 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-2025-5516	TOTOLINK X2000R URL Filtering Page formFilter cross site scripting	A vulnerability, which was classified as problematic, was found in TOTOLINK X2000R 1.0.0-B20230726.1108. This affects an unknown part of the file /boafrm/formFilter of the component URL Filtering Page. The manipulation of the argument URL Address 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-2025-5523	enilu web-flash File Upload upload fileService.upload cross site scripting	A vulnerability classified as problematic has been found in enilu web-flash 1.0. This affects the function fileService.upload of the file src/main/java/cn/enilu/flash/api/controller/FileController/upload of the component File Upload. The manipulation of the argument File leads to cross site scripting. It is possible to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		initiate the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-5542	TOTOLINK X2000R Virtual Server Page formPortFw cross site scripting	A vulnerability was found in TOTOLINK X2000R 1.0.0-B20230726.1108. It has been classified as problematic. Affected is an unknown function of the file /boafrm/formPortFw of the component Virtual Server Page. The manipulation of the argument service_type 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-2025-5543	TOTOLINK X2000R Parent Controls Page cross site scripting	A vulnerability was found in TOTOLINK X2000R 1.0.0-B20230726.1108. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Parent Controls Page. The manipulation of the argument Device Name 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-2025-5568	WpEvently <= 4.4.2 - Authenticated (Contributor+) Stored Cross-Site Scripting	The WpEvently plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple parameters in all versions up to, and including, 4.4.2 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-2025-5584	PHPGurukul Hospital Management System POST Parameter edit-patient.php cross site scripting	A vulnerability was found in PHPGurukul Hospital Management System 4.0. It has been classified as problematic. Affected is an unknown function of the file /doctor/edit-patient.php?editid=2 of the component POST Parameter Handler. The manipulation of the argument patname leads to cross site scripting. It is possible to launch the attack remotely. 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.		
CVE-2025-5628	SourceCodester Food Menu Manager Add Menu index.php cross site scripting	A vulnerability, which was classified as problematic, has been found in SourceCodester Food Menu Manager 1.0. Affected by this issue is some unknown functionality of the file /index.php of the component Add Menu Handler. The manipulation of the argument name/description 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-2025-5651	code-projects Traffic Offense Reporting System saveuser.php cross site scripting	A vulnerability, which was classified as problematic, has been found in code-projects Traffic Offense Reporting System 1.0. This issue affects some unknown processing of the file saveuser.php. The manipulation of the argument user_id/username/email/name/position 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-2025-5661	code-projects Traffic Offense Reporting System Setting save-settings.php cross site scripting	A vulnerability, which was classified as problematic, was found in code-projects Traffic Offense Reporting System 1.0. This affects an unknown part of the file /save-settings.php of the component Setting Handler. The manipulation of the argument site_name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-5713	SoluçõesCoop iSoluçõesWEB Flow fluxos-dashboard cross site scripting	A vulnerability was found in SoluçõesCoop iSoluçõesWEB up to 20250519 and classified as problematic. Affected by this issue is some unknown functionality of the file /fluxos-dashboard of the component Flow Handler. The manipulation of the argument Descrição da solicitação leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. It is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		recommended to upgrade the affected component.		
CVE-2025-5721	SourceCodester Student Result Management System Profile Setting Page update_profile cross site scripting	A vulnerability, which was classified as problematic, was found in SourceCodester Student Result Management System 1.0. This affects an unknown part of the file /script/academic/core/update_profile of the component Profile Setting 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-2025-5722	SourceCodester Student Result Management System Add Academic Term terms cross site scripting	A vulnerability has been found in SourceCodester Student Result Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /script/academic/terms of the component Add Academic Term. The manipulation of the argument Academic Term 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-2025-5723	SourceCodester Student Result Management System Classes Page classes cross site scripting	A vulnerability was found in SourceCodester Student Result Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file /script/academic/classes of the component Classes Page. The manipulation of the argument Class Name leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-5724	SourceCodester Student Result Management System Subjects Page subjects cross site scripting	A vulnerability was found in SourceCodester Student Result Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file /script/academic/subjects of the component Subjects Page. The manipulation of the argument Subject leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and may be used.		
CVE-2025-5725	SourceCodester Student Result Management System Grading System Page grading-system cross site scripting	A vulnerability was found in SourceCodester Student Result Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /script/academic/grading-system of the component Grading System Page. The manipulation of the argument Remark leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-5726	SourceCodester Student Result Management System Division System Page division-system cross site scripting	A vulnerability was found in SourceCodester Student Result Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /script/academic/division-system of the component Division System Page. The manipulation of the argument Division 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-2025-5727	SourceCodester Student Result Management System Announcement Page announcement cross site scripting	A vulnerability classified as problematic has been found in SourceCodester Student Result Management System 1.0. This affects an unknown part of the file /script/academic/announcement of the component Announcement 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.	Patched by core rule	Y
CVE-2025-5757	code-projects Traffic Offense Reporting System save-reported.php cross site scripting	A vulnerability was found in code-projects Traffic Offense Reporting System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /save-reported.php. The manipulation of the argument offence_id/vehicle_no/driver_license/name/address/gender/officer_reporting/offence leads to cross site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-5764	code-projects Laundry System insert_laundry.php cross site scripting	A vulnerability was found in code-projects Laundry System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /data/insert_laundry.php. The manipulation of the argument Customer 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-2025-5765	code-projects Laundry System edit_laundry.php cross site scripting	A vulnerability was found in code-projects Laundry System 1.0. It has been classified as problematic. This affects an unknown part of the file /data/edit_laundry.php. The manipulation of the argument Customer 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-2025-5796	code-projects Laundry System edit_type.php cross site scripting	A vulnerability has been found in code-projects Laundry System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /data/edit_type.php. The manipulation of the argument Type leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-5797	code-projects Laundry System insert_type.php cross site scripting	A vulnerability was found in code-projects Laundry System 1.0 and classified as problematic. This issue affects some unknown processing of the file /data/insert_type.php. The manipulation of the argument Type 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-2025-5879	WuKongOpenSource WukongCRM File Upload AdminSysConfigController.java cross site scripting	A vulnerability, which was classified as problematic, was found in WuKongOpenSource WukongCRM 9.0. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects an unknown part of the file AdminSysConfigController.java of the component File Upload. The manipulation of the argument File 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.		
CVE-2025-5886	Emlog article.php cross site scripting	A vulnerability was found in Emlog up to 2.5.7 and classified as problematic. This issue affects some unknown processing of the file /admin/article.php. The manipulation of the argument active_post 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-2025-5887	jsnjfz WebStack-Guns File Upload UserMgrController.java cross site scripting	A vulnerability was found in jsnjfz WebStack-Guns 1.0. It has been classified as problematic. Affected is an unknown function of the file UserMgrController.java of the component File Upload. The manipulation of the argument File 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-2025-5970	PHPGurukul Restaurant Table Booking System add-subadmin.php cross site scripting	A vulnerability was found in PHPGurukul Restaurant Table Booking System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/add-subadmin.php. The manipulation of the argument fullname leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-5972	PHPGurukul Restaurant Table Booking System manage-subadmins.php cross site scripting	A vulnerability classified as problematic has been found in PHPGurukul Restaurant Table Booking System 1.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Affected is an unknown function of the file /admin/manage-subadmins.php. The manipulation of the argument fullname 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.		
CVE-2025-5973	PHPGurukul Restaurant Table Booking System add-table.php cross site scripting	A vulnerability classified as problematic was found in PHPGurukul Restaurant Table Booking System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/add-table.php. The manipulation of the argument tableno 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-2025-5974	PHPGurukul Restaurant Table Booking System check-status.php cross site scripting	A vulnerability, which was classified as problematic, has been found in PHPGurukul Restaurant Table Booking System 1.0. Affected by this issue is some unknown functionality of the file /check-status.php. The manipulation of the argument searchdata 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-2025-5975	PHPGurukul Rail Pass Management System download-pass.php cross site scripting	A vulnerability, which was classified as problematic, was found in PHPGurukul Rail Pass Management System 1.0. This affects an unknown part of the file /rpms/download-pass.php. The manipulation of the argument searchdata 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-2025-5976	PHPGurukul Rail Pass Management System add-pass.php cross site scripting	A vulnerability has been found in PHPGurukul Rail Pass Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/add-pass.php. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument fullname 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.		
CVE-2025-2254	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in GitLab	An issue has been discovered in GitLab CE/EE affecting all versions from 17.9 before 17.10.8, 17.11 before 17.11.4, and 18.0 before 18.0.2. Improper output encoding in the snipper viewer functionality lead to Cross-Site scripting attacks.	Patched by core rule	Y
CVE-2025-47943	Gogs stored XSS in PDF renderer	Gogs is an open source self-hosted Git service. In application version 0.14.0+dev and prior, there is a stored cross-site scripting (XSS) vulnerability present in Gogs, which allows client-side Javascript code execution. The vulnerability is caused by the usage of a vulnerable and outdated component: pdfjs-1.4.20 under public/plugins/. This issue has been fixed for gogs.io/gogs in version 0.13.3.	Patched by core rule	Y
CVE-2025-48954	Discourse vulnerable to XSS via user-provided query parameter in oauth failure flow	Discourse is an open-source discussion platform. Versions prior to 3.5.0.beta6 are vulnerable to cross-site scripting when the content security policy isn't enabled when using social logins. Version 3.5.0.beta6 patches the issue. As a workaround, have the content security policy enabled.	Patched by core rule	Y
CVE-2025-48992	Group-Office vulnerable to blind XSS	Group-Office is an enterprise customer relationship management and groupware tool. Prior to versions 6.8.123 and 25.0.27, a stored and blind cross-site scripting (XSS) vulnerability exists in the Name Field of the user profile. A malicious attacker can change their name to a javascript payload, which is executed when a user adds the malicious user to their Synchronization > Address books. This issue has been patched in versions 6.8.123 and 25.0.27.	Patched by core rule	Y
CVE-2025-48993	Group-Office vulnerable to reflected XSS via Look	Group-Office is an enterprise customer relationship	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	and Feel Formatting input	management and groupware tool. Prior to versions 6.8.123 and 25.0.27, a malicious JavaScript payload can be executed via the Look and Feel formatting fields. Any user can update their Look and Feel Formatting input fields, but the web application does not sanitize their input. This could result in a reflected cross-site scripting (XSS) attack. This issue has been patched in versions 6.8.123 and 25.0.27.		
CVE-2025-49126	Visionatrix Vulnerable to Reflected XSS Leading to Exfiltration of Secrets	Visionatrix is an AI Media processing tool using ComfyUI. In versions 1.5.0 to before 2.5.1, the /docs/flows endpoint is vulnerable to a Reflected XSS (Cross-Site Scripting) attack allowing full takeover of the application and exfiltration of secrets stored in the application. The implementation uses the get_swagger_ui_html function from FastAPI. This function does not encode or sanitize its arguments before using them to generate the HTML for the swagger documentation page and is not intended to be used with user-controlled arguments. Any user of this application can be targeted with a one-click attack that can takeover their session and all the secrets that may be contained within it. This issue has been patched in version 2.5.1.	Patched by core rule	Y
CVE-2025-49149	Dify has XSS vulnerability	Dify is an open-source LLM app development platform. In version 1.2.0, there is insufficient filtering of user input by web applications. Attackers can use website vulnerabilities to inject malicious script code into web pages. This may result in a cross-site scripting (XSS) attack when a user browses these web pages. At time of posting, there is no known patched version.	Patched by core rule	Y
CVE-2025-49575	Citizen allows stored XSS in Command Palette tip messages	Citizen is a MediaWiki skin that makes extensions part of the cohesive experience. Multiple system messages are inserted into the CommandPaletteFooter as raw HTML, allowing anybody who can edit those	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		messages to insert arbitrary HTML into the DOM. This impacts wikis where a group has the `editinterface` but not the `editsitejs` user right. This vulnerability is fixed in 3.3.1.		
CVE-2025-49576	Citizen allows stored XSS in search no result messages	Citizen is a MediaWiki skin that makes extensions part of the cohesive experience. The citizen-search-noresults-title and citizen-search-noresults-desc system messages are inserted into raw HTML, allowing anybody who can edit those messages to insert arbitrary HTML into the DOM. This vulnerability is fixed in 3.3.1.	Patched by core rule	Y
CVE-2025-49577	Citizen allows stored XSS in preference menu headings	Citizen is a MediaWiki skin that makes extensions part of the cohesive experience. Various preferences messages are inserted into raw HTML, allowing anybody who can edit those messages to insert arbitrary HTML into the DOM. This vulnerability is fixed in 3.3.1.	Patched by core rule	Y
CVE-2025-49578	Citizen allows stored XSS in user registration date message	Citizen is a MediaWiki skin that makes extensions part of the cohesive experience. Various date messages returned by `Language::userDate` are inserted into raw HTML, allowing anybody who can edit those messages to insert arbitrary HTML into the DOM. This impacts wikis where a group has the `editinterface` but not the `editsitejs` user right. This vulnerability is fixed in 3.3.1.	Patched by core rule	Y
CVE-2025-49579	Citizen allows stored XSS in menu heading message	Citizen is a MediaWiki skin that makes extensions part of the cohesive experience. All system messages in menu headings using the Menu.mustache template are inserted as raw HTML, allowing anybody who can edit those messages to insert arbitrary HTML into the DOM. This impacts wikis where a group has the `editinterface` but not the `editsitejs` user right. This vulnerability is fixed in 3.3.1.	Patched by core rule	Y
CVE-2025-50183	OpenList (frontend) allows XSS Attacks in the built-in Markdown Viewer	OpenList Frontend is a UI component for OpenList. Prior to version 4.0.0-rc.4, a vulnerability exists in the file preview/browsing feature of the application, where files	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		with a .py extension that contain JavaScript code wrapped in <script> tags may be interpreted and executed as HTML in certain modes. This leads to a stored XSS vulnerability. This issue has been patched in version 4.0.0-rc.4.		
CVE-2025-5144	The Events Calendar <= 6.13.2 - Authenticated (Contributor+) DOM-Based Stored Cross-Site Scripting	The The Events Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'data-date-*' parameters in all versions up to, and including, 6.13.2 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-2025-52485	DNN.PLATFORM Allows Stored Cross-Site Scripting (XSS) in Activity Feed	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. In versions 6.0.0 to before 10.0.1, DNN.PLATFORM allows a specially crafted request to inject scripts in the Activity Feed Attachments endpoint which will then render in the feed. This issue has been patched in version 10.0.1.	Patched by core rule	Y
CVE-2025-52486	DNN.PLATFORM Allows Reflected Cross-Site Scripting (XSS) in some TokenReplace situations with SkinObjects	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. In versions 6.0.0 to before 10.0.1, DNN.PLATFORM allows specially crafted content in URLs to be used with TokenReplace and not be properly sanitized by some SkinObjects. This issue has been patched in version 10.0.1.	Patched by core rule	Y
CVE-2025-52552	FastGPT LastRoute Parameter on Login Page Vulnerable to Open Redirect and DOM-based XSS	FastGPT is an AI Agent building platform. Prior to version 4.9.12, the LastRoute Parameter on login page is vulnerable to open redirect and DOM-based XSS. Improper validation and lack of sanitization of this parameter allows attackers execute malicious JavaScript	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		or redirect them to attacker-controlled sites. This issue has been patched in version 4.9.12.		
CVE-2025-52558	ChangeDetection.io XSS in watch overview	changedetection.io is a free open source web page change detection, website watcher, restock monitor and notification service. Prior to version 0.50.4, errors in filters from website page change detection watches were not being filtered resulting in a cross-site scripting (XSS) vulnerability. This issue has been patched in version 0.50.4	Patched by core rule	Y
CVE-2025-52561	HTMLSanitizer.jl Possible XSS	HTMLSanitizer.jl is a Whitelist-based HTML sanitizer. Prior to version 0.2.1, when adding the style tag to the whitelist, content inside the tag is incorrectly unescaped, and closing tags injected as content are interpreted as real HTML, enabling tag injection and JavaScript execution. This could result in possible cross-site scripting (XSS) in any HTML that is sanitized with this library. This issue has been patched in version 0.2.1. A workaround involves adding the math and svg elements to the whitelist manually.	Patched by core rule	Y
CVE-2025-5301	Reflected Cross-Site Scripting in ONLYOFFICE Docs (DocumentServer)	ONLYOFFICE Docs (DocumentServer) in versions equal and below 8.3.1 are affected by a reflected cross-site scripting (XSS) issue when opening files via the WOPI protocol. Attackers could inject malicious scripts via crafted HTTP POST requests, which are then reflected in the server's HTML response.	Patched by core rule	Y
CVE-2025-5700	Simple Logo Carousel <= 1.9.3 - Authenticated (Contributor+) Stored Cross-Site Scripting via id Parameter	The Simple Logo Carousel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter in all versions up to, and including, 1.9.3 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		injected page.		
CVE-2025-5923	Game Review Block <= 4.8.1 - Authenticated (Contributor+) Stored Cross-Site Scripting via className Parameter	The Game Review Block plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'className' parameter in all versions up to, and including, 4.8.1 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-2025-5990	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in Crafty Controller	An input neutralization vulnerability in the Server Name form and API Key form components of Crafty Controller allows a remote, authenticated attacker to perform stored XSS via malicious form input.	Patched by core rule	Y
CVE-2025-6050	Stored Cross-Site Scripting (XSS) in Mezzanine CMS Admin Interface	Mezzanine CMS, in versions prior to 6.1.1, contains a Stored Cross-Site Scripting (XSS) vulnerability in the admin interface. The vulnerability exists in the "displayable_links_js" function, which fails to properly sanitize blog post titles before including them in JSON responses served via "/admin/displayable_links.js ". An authenticated admin user can create a blog post with a malicious JavaScript payload in the title field, then trick another admin user into clicking a direct link to the "/admin/displayable_links.js " endpoint, causing the malicious script to execute in their browser.	Patched by core rule	Y
CVE-2025-6092	comfyanonymous comfyui Incomplete Fix CVE-2024-10099 image cross site scripting	A vulnerability was found in comfyanonymous comfyui up to 0.3.39. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /upload/image of the component Incomplete Fix CVE-2024-10099. The manipulation of the argument image leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-6125	PHPGurukul Rail Pass Management System aboutus.php cross site scripting	A vulnerability was found in PHPGurukul Rail Pass Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file /admin/aboutus.php. The manipulation of the argument pagedes 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-2025-6126	PHPGurukul Rail Pass Management System contact.php cross site scripting	A vulnerability was found in PHPGurukul Rail Pass Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /contact.php. 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.	Patched by core rule	Y
CVE-2025-6127	PHPGurukul Nipah Virus Testing Management System search-report.php cross site scripting	A vulnerability was found in PHPGurukul Nipah Virus Testing Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /search-report.php. The manipulation of the argument serachdata 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-2025-6131	CodeAstro Food Ordering System POST Request Parameter edit cross site scripting	A vulnerability, which was classified as problematic, was found in CodeAstro Food Ordering System 1.0. Affected is an unknown function of the file /admin/store/edit/ of the component POST Request Parameter Handler. The manipulation of the argument Restaurant Name/Address 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-2025-6257	Euro FxRef Currency Converter <= 2.0.2 - Authenticated (Contributor+) Stored Cross-Site Scripting via currency Shortcode	The Euro FxRef Currency Converter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's currency shortcode in all versions up to, and including, 2.0.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-6340	code-projects School Fees Payment System branch.php cross site scripting	A vulnerability classified as problematic has been found in code-projects School Fees Payment System 1.0. This affects an unknown part of the file /branch.php. The manipulation of the argument Branch/Address/Detail 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-2025-6345	SourceCodester My Food Recipe Add Recipe Page add-recipe.php addRecipeModal cross site scripting	A vulnerability was found in SourceCodester My Food Recipe 1.0 and classified as problematic. Affected by this issue is the function addRecipeModal of the file /endpoint/add-recipe.php of the component Add Recipe Page. The manipulation of the argument Name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6347	code-projects Responsive Blog pageViewMembers.php cross site scripting	A vulnerability was found in code-projects Responsive Blog 1.0/1.12.4/3.3.4. It has been declared as problematic. This vulnerability affects unknown code of the file /responsive/resblog/blogadmin/admin/pageViewMembers.php. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6353	code-projects Responsive	A vulnerability classified as	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Blog search.php cross site scripting	problematic was found in code-projects Responsive Blog 1.0. Affected by this vulnerability is an unknown functionality of the file /search.php. The manipulation of the argument keyword leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	rule	
CVE-2025-6452	CodeAstro Patient Record Management System Generate New Report Page cross site scripting	A vulnerability was found in CodeAstro Patient Record Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the component Generate New Report Page. The manipulation of the argument Patient Name/Name leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6473	code-projects School Fees Payment System fees.php cross site scripting	A vulnerability, which was classified as problematic, was found in code-projects School Fees Payment System 1.0. This affects an unknown part of the file /fees.php. The manipulation of the argument transcation_remark 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-2025-6475	SourceCodester Student Result Management System Manage Students Module manage_students cross site scripting	A vulnerability was found in SourceCodester Student Result Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file /script/admin/manage_students of the component Manage Students Module. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-6477	SourceCodester Student Result Management System System Settings Page system cross site scripting	A vulnerability was found in SourceCodester Student Result Management System 1.0. It has been declared as problematic. Affected by this	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability is an unknown functionality of the file /script/admin/system of the component System Settings Page. The manipulation of the argument School Name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-6509	seaswalker spring-analysis SimpleController.java echo cross site scripting	A vulnerability was found in seaswalker spring-analysis up to 4379cce848af96997a9d7ef91d594aa129be8d71. It has been declared as problematic. Affected by this vulnerability is the function echo of the file /src/main/java/controller/SimpleController.java. 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. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available.	Patched by core rule	Y
CVE-2025-6551	java-aodeng Hope-Boot WebController.java login cross site scripting	A vulnerability was found in java-aodeng Hope-Boot 1.0.0 and classified as problematic. This issue affects the function Login of the file /src/main/java/com/hope/controller/WebController.java. The manipulation of the argument errorMsg 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-2025-6569	code-projects School Fees Payment System student.php cross site scripting	A vulnerability classified as problematic was found in code-projects School Fees Payment System 1.0. Affected by this vulnerability is an unknown functionality of the file /student.php. The manipulation of the argument sname/contact/about/emailid/transcation_remark 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.		
CVE-2025-6613	PHPGurukul Hospital Management System manage-patient.php cross site scripting	A vulnerability classified as problematic was found in PHPGurukul Hospital Management System 4.0. Affected by this vulnerability is an unknown functionality of the file /doctor/manage-patient.php. 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.	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.

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™