

Monthly Zero-Day Vulnerability Coverage Report

June 2024

# The total zero-day vulnerabilities count for June month: 215

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Command Injection | CSRF | Local File  Inclusion | SQLi | Malicious File Upload | XSS | XXE |
| 17 | 22 | 27 | 69 | 3 | 75 | 2 |

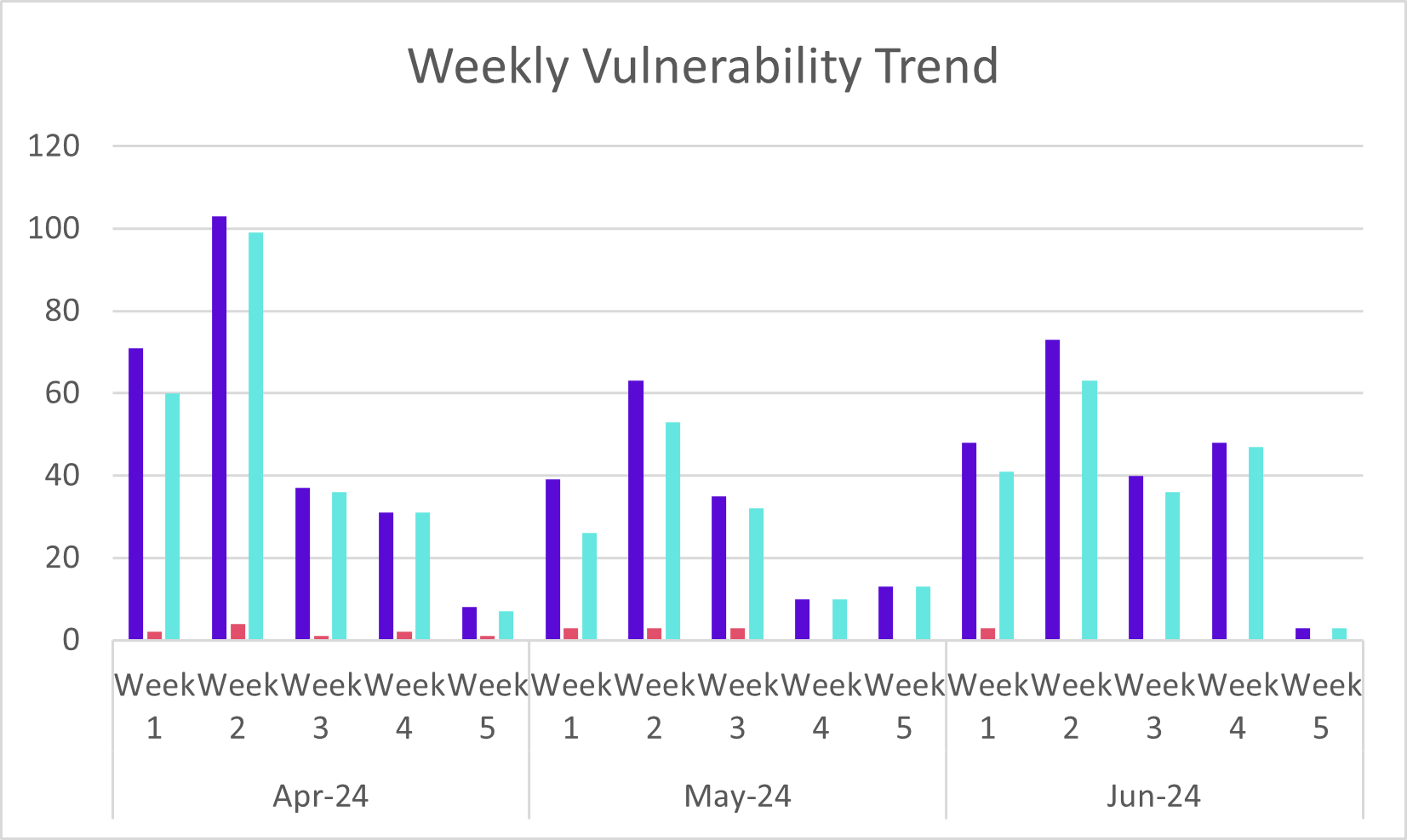
|  |  |
| --- | --- |
| Zero-day vulnerabilities protected through core rules | 212 |
| Zero-day vulnerabilities protected through custom rules | 3 |
| Zero-day vulnerabilities for which protection cannot be done | 0 |
| Zero-day vulnerabilities found by Indusface WAS | 190 |

* To enable custom rules, please contact [support@indusface.com](mailto:support@indusface.com)
* Learn more about [zero-day vulnerabilities, detection, and prevention, here](https://www.indusface.com/blog/zero-day-vulnerability)

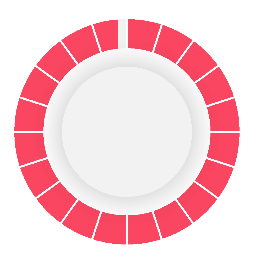
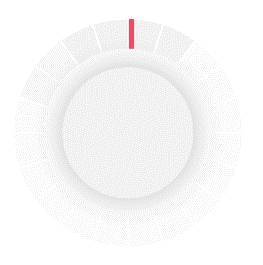
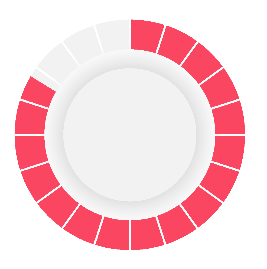
# Vulnerability Trend:

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

# Weekly Vulnerability Trend



Total Blocked/Logged Web AppSec Zero-Day Vulnerabilities by Core Rules Total Custom Patch Required for Web AppSec Zero-Day Vulnerabilities Total Zero-Day Vulnerabilities found by Indusface Scanner

**88%**

**1%**

**99%**

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

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

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

# Top Five Vulnerability Categories

# 

# 

April-24

May-24

June-24

# Vulnerability Details

# Command Injection Vulnerabilities

| **Public ID** | **Vulnerability Name** | **Vulnerability Description** | **AppTrana Coverage** | **Indusface WAS Coverage** |
| --- | --- | --- | --- | --- |
| CVE-2024-34852 | F-logic DataCube3 1.0 transceiver\_schedule.php command injection | A vulnerability was found in F-logic DataCube3 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/transceiver\_schedule.php. The manipulation leads to command injection.  This vulnerability is known as CVE-2024-34852. The attack can be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-36604 | Tenda O3V2 1.0.0.12(3880) SetStp stpEn command injection | A vulnerability classified as critical was found in Tenda O3V2 1.0.0.12. This vulnerability affects the function SetStp. The manipulation of the argument stpEn leads to command injection.  This vulnerability was named CVE-2024-36604. The attack can only be initiated within the local network. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-4253 | gradio up to 4.28.x test-functional.yml command injection | A vulnerability classified as critical has been found in gradio up to 4.28.x. This affects an unknown part of the file test-functional.yml. The manipulation leads to command injection.  This vulnerability is uniquely identified as CVE-2024-4253. It is possible to initiate the attack remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-5480 | PyTorch up to 2.2.1 command injection | A vulnerability which was classified as very critical was found in PyTorch up to 2.2.1. Affected is an unknown function. The manipulation leads to command injection.  This vulnerability is traded as CVE-2024-5480. It is possible to launch the attack remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-2359 | parisneo lollms-webui /execute\_code os command injection | A vulnerability classified as very critical has been found in parisneo lollms-webui. This affects an unknown part of the file /execute\_code. The manipulation leads to os command injection.  This vulnerability is uniquely identified as CVE-2024-2359. It is possible to initiate the attack remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-2171 | zenml-io ZenML up to 0.56.1 logo\_url cross site scripting | A vulnerability was found in zenml-io ZenML up to 0.56.1 and classified as problematic. This issue affects some unknown processing. The manipulation of the argument logo\_url leads to cross site scripting.  The identification of this vulnerability is CVE-2024-2171. The attack may be initiated remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-3102 | mintplex-labs anything-llm up to 0.x JSON /api/request-token username values | A vulnerability classified as problematic has been found in mintplex-labs anything-llm up to 0.x. Affected is an unknown function of the file /api/request-token of the component JSON Handler. The manipulation of the argument username leads to improper handling of values.  This vulnerability is traded as CVE-2024-3102. It is possible to launch the attack remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-1880 | significant-gravitas AutoGPT up to 5.1.0 MacOSTTS os command injection | A vulnerability which was classified as critical was found in significant-gravitas AutoGPT up to 5.1.0. Affected is the function MacOSTTS. The manipulation leads to os command injection.  This vulnerability is traded as CVE-2024-1880. Local access is required to approach this attack. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-5087 | Minimal Coming Soon Plugin up to 2.38 on WordPress Setting authorization | A vulnerability was found in Minimal Coming Soon Plugin up to 2.38 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to missing authorization.  This vulnerability is known as CVE-2024-5087. The attack can be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-4577 | PHP up to 8.1.28/8.2.19/8.3.7 on Windows Unicode Character argument injection | A vulnerability has been found in PHP up to 8.1.28/8.2.19/8.3.7 on Windows and classified as critical. Affected by this vulnerability is an unknown functionality of the component Unicode Character Handler. The manipulation leads to argument injection.  This vulnerability is known as CVE-2024-4577. The attack can be launched remotely. Furthermore there is an exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-37570 | Mitel 6869i 4.5.0.41 Manual Firmware Update upgrade.html username/path command injection | A vulnerability classified as critical has been found in Mitel 6869i 4.5.0.41. Affected is an unknown function of the file upgrade.html of the component Manual Firmware Update Handler. The manipulation of the argument username/path leads to command injection.  This vulnerability is traded as CVE-2024-37570. The attack needs to be approached within the local network. Furthermore there is an exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-37569 | Mitel 6869i up to 4.5.0.41/5.0.0.1018 provis.html hostname os command injection | A vulnerability was found in Mitel 6869i up to 4.5.0.41/5.0.0.1018. It has been rated as critical. This issue affects some unknown processing of the file provis.html. The manipulation of the argument hostname leads to os command injection.  The identification of this vulnerability is CVE-2024-37569. The attack may be initiated remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-5585 | PHP up to 8.1.28/8.2.19/8.3.7 Trailing Space proc\_open argument injection | A vulnerability was found in PHP up to 8.1.28/8.2.19/8.3.7. It has been declared as critical. Affected by this vulnerability is the function proc\_open of the component Trailing Space Handler. The manipulation leads to argument injection.  This vulnerability is known as CVE-2024-5585. The attack can be launched remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-37393 | SecurEnvoy MFA prior 9.4.514 Desktop Service /secserver ldap injection | A vulnerability has been found in SecurEnvoy MFA and classified as critical. Affected by this vulnerability is an unknown functionality of the file /secserver of the component Desktop Service. The manipulation leads to ldap injection.  This vulnerability is known as CVE-2024-37393. The attack can be launched remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-6186 | Ruijie RG-UAC 1.0 commit.php ad\_log\_name os command injection | A vulnerability which was classified as critical was found in Ruijie RG-UAC 1.0. This affects an unknown part of the file /view/userAuthentication/SSO/commit.php. The manipulation of the argument ad\_log\_name leads to os command injection.  This vulnerability is uniquely identified as CVE-2024-6186. It is possible to initiate the attack remotely. Furthermore there is an exploit available.  The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |
| CVE-2024-6185 | Ruijie RG-UAC 1.0 commit.php get\_ip\_addr\_details ethname os command injection | A vulnerability which was classified as critical has been found in Ruijie RG-UAC 1.0. Affected by this issue is the function get\_ip\_addr\_details of the file /view/dhcp/dhcpConfig/commit.php. The manipulation of the argument ethname leads to os command injection.  This vulnerability is handled as CVE-2024-6185. The attack may be launched remotely. Furthermore there is an exploit available.  The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |
| CVE-2024-6187 | Ruijie RG-UAC 1.0 sub\_commit.php key os command injection | A vulnerability has been found in Ruijie RG-UAC 1.0 and classified as critical. This vulnerability affects unknown code of the file /view/vpn/autovpn/sub\_commit.php. The manipulation of the argument key leads to os command injection.  This vulnerability was named CVE-2024-6187. The attack can be initiated remotely. Furthermore there is an exploit available.  The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |

Cross-Site Request Forgery Vulnerabilities

| **Public ID** | **Vulnerability Name** | **Vulnerability Description** | **AppTrana Coverage** | **Indusface WAS Coverage** |
| --- | --- | --- | --- | --- |
| CVE-2024-4535 | KKProgressbar2 Free Plugin up to 1.1.4.2 on WordPress cross-site request forgery | A vulnerability was found in KKProgressbar2 Free Plugin up to 1.1.4.2 on WordPress. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site request forgery.  This vulnerability is traded as CVE-2024-4535. It is possible to launch the attack remotely. There is no exploit available. | Patched by core rule | N |
| CVE-2024-4532 | Business Card Plugin up to 1.0.0 on WordPress cross-site request forgery | A vulnerability was found in Business Card Plugin up to 1.0.0 on WordPress and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery.  The identification of this vulnerability is CVE-2024-4532. The attack may be initiated remotely. There is no exploit available. | Patched by core rule | N |
| CVE-2024-4530 | Business Card Plugin up to 1.0.0 on WordPress cross-site request forgery | A vulnerability which was classified as problematic was found in Business Card Plugin up to 1.0.0 on WordPress. This affects an unknown part. The manipulation leads to cross-site request forgery.  This vulnerability is uniquely identified as CVE-2024-4530. It is possible to initiate the attack remotely. There is no exploit available. | Patched by core rule | N |
| CVE-2024-4531 | Business Card Plugin up to 1.0.0 on WordPress cross-site request forgery | A vulnerability has been found in Business Card Plugin up to 1.0.0 on WordPress and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery.  This vulnerability was named CVE-2024-4531. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | N |
| CVE-2024-4534 | KKProgressbar2 Free Plugin up to 1.1.4.2 on WordPress cross-site request forgery | A vulnerability which was classified as problematic has been found in KKProgressbar2 Free Plugin up to 1.1.4.2 on WordPress. This issue affects some unknown processing. The manipulation leads to cross-site request forgery.  The identification of this vulnerability is CVE-2024-4534. The attack may be initiated remotely. There is no exploit available. | Patched by core rule | N |
| CVE-2024-4529 | Business Card Plugin up to 1.0.0 on WordPress cross-site request forgery | A vulnerability which was classified as problematic has been found in Business Card Plugin up to 1.0.0 on WordPress. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery.  This vulnerability is handled as CVE-2024-4529. The attack may be launched remotely. There is no exploit available. | Patched by core rule | N |
| CVE-2024-5428 | SourceCodester Simple Online Bidding System 1.0 HTTP POST Request index.php save\_product cross-site request forgery | A vulnerability classified as problematic was found in SourceCodester Simple Online Bidding System 1.0. Affected by this vulnerability is the function save\_product of the file /admin/index.phppagemanage\_product of the component HTTP POST Request Handler. The manipulation leads to cross-site request forgery.  This vulnerability is known as CVE-2024-5428. The attack can be launched remotely. There is no exploit available. | Patched by core rule | N |
| CVE-2024-36550 | idcCMS 1.35 vpsCompany\_deal.php cross-site request forgery | A vulnerability classified as problematic has been found in idcCMS 1.35. Affected is an unknown function of the file /admin/vpsCompany\_deal.phpmudiadd&amp;nohrefStrclose. The manipulation leads to cross-site request forgery.  This vulnerability is traded as CVE-2024-36550. It is possible to launch the attack remotely. There is no exploit available. | Patched by core rule | N |
| CVE-2024-36548 | idcCMS 1.35 vpsCompany\_deal.php cross-site request forgery | A vulnerability has been found in idcCMS 1.35 and classified as problematic. This vulnerability affects unknown code of the file admin/vpsCompany\_deal.phpmudidel. The manipulation leads to cross-site request forgery.  This vulnerability was named CVE-2024-36548. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | N |
| CVE-2024-36549 | idcCMS 1.35 vpsCompany\_deal.php cross-site request forgery | A vulnerability was found in idcCMS 1.35. It has been rated as problematic. This issue affects some unknown processing of the file /admin/vpsCompany\_deal.phpmudirev&amp;nohrefStrclose. The manipulation leads to cross-site request forgery.  The identification of this vulnerability is CVE-2024-36549. The attack may be initiated remotely. There is no exploit available. | Patched by core rule | N |
| CVE-2024-36547 | idcCMS 1.35 vpsClass\_deal.php cross-site request forgery | A vulnerability classified as problematic was found in idcCMS 1.35. Affected by this vulnerability is an unknown functionality of the file admin/vpsClass\_deal.phpmudiadd. The manipulation leads to cross-site request forgery.  This vulnerability is known as CVE-2024-36547. The attack can be launched remotely. There is no exploit available. | Patched by core rule | N |
| CVE-2024-36667 | idcCMS 1.35 idcProType\_deal.php cross-site request forgery | A vulnerability was found in idcCMS 1.35. It has been classified as problematic. This affects an unknown part of the file /admin/idcProType\_deal.phpmudiadd&amp;nohrefStrclose. The manipulation leads to cross-site request forgery.  This vulnerability is uniquely identified as CVE-2024-36667. It is possible to initiate the attack remotely. There is no exploit available. | Patched by core rule | N |
| CVE-2024-36668 | idcCMS 1.35 type\_deal.php cross-site request forgery | A vulnerability was found in idcCMS 1.35. It has been declared as problematic. This vulnerability affects unknown code of the file admin/type\_deal.phpmudidel. The manipulation leads to cross-site request forgery.  This vulnerability was named CVE-2024-36668. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | N |
| CVE-2024-36670 | idcCMS 1.35 vpsClass\_deal.php cross-site request forgery | A vulnerability was found in idcCMS 1.35 and classified as problematic. Affected by this issue is some unknown functionality of the file admin/vpsClass\_deal.phpmudidel. The manipulation leads to cross-site request forgery.  This vulnerability is handled as CVE-2024-36670. The attack may be launched remotely. There is no exploit available. | Patched by core rule | N |
| CVE-2024-36669 | idcCMS 1.35 type\_deal.php cross-site request forgery | A vulnerability has been found in idcCMS 1.35 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file admin/type\_deal.phpmudiadd. The manipulation leads to cross-site request forgery.  This vulnerability is known as CVE-2024-36669. The attack can be launched remotely. There is no exploit available. | Patched by core rule | N |
| CVE-2024-1879 | significant-gravitas AutoGPT up to 5.0 cross-site request forgery | A vulnerability has been found in significant-gravitas AutoGPT up to 5.0 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery.  This vulnerability was named CVE-2024-1879. The attack can be initiated remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | N |
| CVE-2024-2288 | parisneo lollms-webui up to 9.2 Profile Picture cross-site request forgery | A vulnerability was found in parisneo lollms-webui up to 9.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Profile Picture Handler. The manipulation leads to cross-site request forgery.  This vulnerability is known as CVE-2024-2288. The attack can be launched remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | N |
| CVE-2024-31612 | Emlog Pro 2.3 twitter.php cross-site request forgery | A vulnerability was found in Emlog Pro 2.3. It has been classified as problematic. Affected is an unknown function of the file twitter.php. The manipulation leads to cross-site request forgery.  This vulnerability is traded as CVE-2024-31612. It is possible to launch the attack remotely. There is no exploit available. | Patched by core rule | N |
| CVE-2024-4403 | parisneo lollms-webui up to 9.6 restart\_program cross-site request forgery | A vulnerability which was classified as problematic has been found in parisneo lollms-webui up to 9.6. Affected by this issue is the function restart\_program. The manipulation leads to cross-site request forgery.  This vulnerability is handled as CVE-2024-4403. The attack may be launched remotely. There is no exploit available. | Patched by core rule | N |
| CVE-2024-4328 | parisneo lollms-webui up to 9.6 Requests clear\_personality\_files\_list cross-site request forgery | A vulnerability which was classified as problematic was found in parisneo lollms-webui up to 9.6. This affects the function clear\_personality\_files\_list of the component Requests Handler. The manipulation leads to cross-site request forgery.  This vulnerability is uniquely identified as CVE-2024-4328. It is possible to initiate the attack remotely. There is no exploit available. | Patched by core rule | N |
| CVE-2024-31613 | BOSSCMS 3.10 cross-site request forgery | A vulnerability which was classified as problematic has been found in BOSSCMS 3.10. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery.  This vulnerability is handled as CVE-2024-31613. The attack may be launched remotely. There is no exploit available. | Patched by core rule | N |
| CVE-2024-4969 | Widget Bundle Plugin up to 2.0.0 on WordPress cross-site request forgery | A vulnerability has been found in Widget Bundle Plugin up to 2.0.0 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery.  This vulnerability is known as CVE-2024-4969. The attack can be launched remotely. There is no exploit available. | Patched by core rule | N |

# Local File Inclusion Vulnerabilities

| **Public ID** | **Vulnerability Name** | **Vulnerability Description** | **AppTrana Coverage** | **Indusface WAS Coverage** |
| --- | --- | --- | --- | --- |
| CVE-2024-5154 | cri-o up to 1.28.6/1.29.4/1.30.0 /proc/mounts symlink | A vulnerability was found in cri-o up to 1.28.6/1.29.4/1.30.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /proc/mounts. The manipulation leads to symlink following.  This vulnerability is handled as CVE-2024-5154. Attacking locally is a requirement. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-4330 | parisneo lollms-webui up to latest list\_personalities category path traversal | A vulnerability was found in parisneo lollms-webui up to latest. It has been rated as problematic. Affected by this issue is the function list\_personalities. The manipulation of the argument category leads to relative path traversal.  This vulnerability is handled as CVE-2024-4330. It is possible to launch the attack on the local host. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-35429 | ZKTeco ZKBio CVSecurity 6.1.1 eventRecord path traversal | A vulnerability which was classified as critical was found in ZKTeco ZKBio CVSecurity 6.1.1. Affected is an unknown function. The manipulation of the argument eventRecord leads to path traversal.  This vulnerability is traded as CVE-2024-35429. The attack needs to be approached within the local network. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-35431 | ZKTeco ZKBio CVSecurity 6.1.1 photoBase64 path traversal | A vulnerability has been found in ZKTeco ZKBio CVSecurity 6.1.1 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation of the argument photoBase64 leads to path traversal.  This vulnerability is known as CVE-2024-35431. The attack can be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-35428 | ZKTeco ZKBio CVSecurity 6.1.1 BaseMediaFile path traversal | A vulnerability was found in ZKTeco ZKBio CVSecurity 6.1.1. It has been classified as critical. This affects an unknown part. The manipulation of the argument BaseMediaFile leads to path traversal.  This vulnerability is uniquely identified as CVE-2024-35428. It is possible to initiate the attack remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-2178 | parisneo lollms-webui lollms\_personalities\_infos.py copy\_to\_custom\_personas name path traversal | A vulnerability which was classified as problematic has been found in parisneo lollms-webui. This issue affects the function copy\_to\_custom\_personas of the file lollms\_personalities\_infos.py. The manipulation of the argument name leads to path traversal: &039;\..\filename&039;.  The identification of this vulnerability is CVE-2024-2178. The attack may be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-36857 | Jan 0.4.12 /v1/app/readFileSync path traversal | A vulnerability classified as problematic was found in Jan 0.4.12. Affected by this vulnerability is an unknown functionality of the file /v1/app/readFileSync. The manipulation leads to path traversal.  This vulnerability is known as CVE-2024-36857. The attack needs to be initiated within the local network. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-2914 | deepjavalibrary djl up to 0.26.x files\_util.py path traversal | A vulnerability was found in deepjavalibrary djl up to 0.26.x. It has been declared as critical. This vulnerability affects unknown code of the file files\_util.py. The manipulation leads to path traversal: &039;\..\filename&039;.  This vulnerability was named CVE-2024-2914. The attack can be initiated remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-5550 | h2oai h2o-3 up to 3.40.0.4 information disclosure | A vulnerability was found in h2oai h2o-3 up to 3.40.0.4. It has been classified as problematic. This affects an unknown part. The manipulation leads to information disclosure.  This vulnerability is uniquely identified as CVE-2024-5550. It is possible to initiate the attack remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-2928 | MLflow up to 2.11.2 Query String path traversal | A vulnerability was found in MLflow up to 2.11.2. It has been classified as problematic. Affected is an unknown function of the component Query String Handler. The manipulation leads to path traversal: &039;\..\filename&039;.  This vulnerability is traded as CVE-2024-2928. It is possible to launch the attack remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-4881 | parisneo lollms up to 5.8.x on Windows Request /user\_infos absolute path traversal | A vulnerability was found in parisneo lollms up to 5.8.x on Windows and classified as problematic. Affected by this issue is some unknown functionality of the file /user\_infos of the component Request Handler. The manipulation leads to absolute path traversal.  This vulnerability is handled as CVE-2024-4881. The attack may be launched remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-2624 | parisneo lollms-webui up to 9.3 /switch\_personal\_path path traversal | A vulnerability was found in parisneo lollms-webui up to 9.3. It has been classified as critical. This affects an unknown part of the file /switch\_personal\_path. The manipulation of the argument path leads to path traversal: &039;\..\filename&039;.  This vulnerability is uniquely identified as CVE-2024-2624. It is possible to initiate the attack remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-4941 | gradio up to 4.31.3 JSON Component json\_component.py postprocess input validation | A vulnerability classified as problematic has been found in gradio up to 4.31.3. Affected is the function postprocess of the file gradio/components/json\_component.py of the component JSON Component. The manipulation leads to improper input validation.  This vulnerability is traded as CVE-2024-4941. It is possible to launch the attack remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-2360 | parisneo lollms-webui discussion\_db\_name/pdf\_latex\_path path traversal | A vulnerability was found in parisneo lollms-webui and classified as very critical. This issue affects some unknown processing. The manipulation of the argument discussion\_db\_name/pdf\_latex\_path leads to path traversal: &039;\..\filename&039;.  The identification of this vulnerability is CVE-2024-2360. The attack may be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-3322 | parisneo lollms-webui up to 9.4 processor.py' path traversal | A vulnerability was found in parisneo lollms-webui up to 9.4. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file lollms-webui/zoos/personalities\_zoo/cyber\_security/codeguard/scripts/processor.py&039;. The manipulation leads to path traversal.  This vulnerability is known as CVE-2024-3322. Local access is required to approach this attack. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-4320 | parisneo lollms-webui /install\_extension ExtensionBuilder name path traversal | A vulnerability has been found in parisneo lollms-webui and classified as very critical. Affected by this vulnerability is the function ExtensionBuilder of the file /install\_extension. The manipulation of the argument name leads to path traversal: &039;\..\filename&039;.  This vulnerability is known as CVE-2024-4320. The attack can be launched remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-3429 | parisneo lollms up to 9.5 on Windows sanitize\_path\_from\_endpoint/sanitize\_path path traversal | A vulnerability was found in parisneo lollms up to 9.5 on Windows. It has been rated as very critical. Affected by this issue is the function sanitize\_path\_from\_endpoint/sanitize\_path. The manipulation leads to path traversal: &039;\..\filename&039;.  This vulnerability is handled as CVE-2024-3429. The attack may be launched remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-5187 | onnx up to 1.16.0 TAR File download\_model\_with\_test\_data path traversal | A vulnerability which was classified as critical has been found in onnx up to 1.16.0. Affected by this issue is the function download\_model\_with\_test\_data of the component TAR File Handler. The manipulation leads to path traversal.  This vulnerability is handled as CVE-2024-5187. The attack may be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-2362 | parisneo lollms-webui up to 9.3 on Windows Request del\_preset absolute path traversal | A vulnerability which was classified as critical was found in parisneo lollms-webui up to 9.3 on Windows. This affects an unknown part of the file del\_preset of the component Request Handler. The manipulation leads to absolute path traversal.  This vulnerability is uniquely identified as CVE-2024-2362. It is possible to initiate the attack remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-3234 | gaizhenbiao chuanhuchatgpt prior 20240305 web\_assets path traversal | A vulnerability classified as critical was found in gaizhenbiao chuanhuchatgpt. Affected by this vulnerability is an unknown functionality of the file web\_assets. The manipulation leads to path traversal.  This vulnerability is known as CVE-2024-3234. The attack can be launched remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-2548 | parisneo lollms-webui up to 9.4 on Windows Request Path(path).is\_absolute absolute path traversal | A vulnerability has been found in parisneo lollms-webui up to 9.4 on Windows and classified as problematic. This vulnerability affects the function Path.is\_absolute of the component Request Handler. The manipulation leads to absolute path traversal.  This vulnerability was named CVE-2024-2548. The attack can be initiated remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-36821 | Linksys Velop WiFi 5 1.1.13.202617 path traversal | A vulnerability which was classified as critical has been found in Linksys Velop WiFi 5 1.1.13.202617. This issue affects some unknown processing. The manipulation leads to path traversal.  The identification of this vulnerability is CVE-2024-36821. The attack can only be initiated within the local network. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-4315 | parisneo lollms up to 9.7 sanitize\_path\_from\_endpoint filename control | A vulnerability was found in parisneo lollms up to 9.7. It has been declared as critical. Affected by this vulnerability is the function sanitize\_path\_from\_endpoint. The manipulation leads to improper control of filename for include/require statement in php program .  This vulnerability is known as CVE-2024-4315. The attack can be launched remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-5211 | mintplex-labs anything-llm up to 0.x anythingllm.db normalizePath path traversal | A vulnerability was found in mintplex-labs anything-llm up to 0.x. It has been declared as critical. Affected by this vulnerability is the function normalizePath of the file anythingllm.db. The manipulation leads to path traversal: &039;\..\filename&039;.  This vulnerability is known as CVE-2024-5211. The attack can be launched remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-38449 | KasmVNC path traversal | A vulnerability was found in KasmVNC up to 1.3.1.230e50f7b89663316c70de7b0e3db6f6b9340489. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation leads to path traversal.  This vulnerability is handled as CVE-2024-38449. The attack may be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-5182 | mudler localai up to 2.15.x model path traversal | A vulnerability which was classified as critical has been found in mudler localai up to 2.15.x. This issue affects some unknown processing. The manipulation of the argument model leads to path traversal.  The identification of this vulnerability is CVE-2024-5182. The attack may be initiated remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-4841 | parisneo lollms-webui up to 9.6 HTTP Request add\_reference\_to\_local\_model add\_reference\_to\_local\_mode path path traversal | A vulnerability was found in parisneo lollms-webui up to 9.6. It has been rated as problematic. Affected by this issue is the function add\_reference\_to\_local\_mode of the file /add\_reference\_to\_local\_model of the component HTTP Request Handler. The manipulation of the argument path leads to path traversal: &039;\..\filename&039;.  This vulnerability is handled as CVE-2024-4841. An attack has to be approached locally. There is no exploit available. | Patched by core rule | Y |

Malicious File Upload Vulnerabilities

| **Public ID** | **Vulnerability Name** | **Vulnerability Description** | **AppTrana Coverage** | **Indusface WAS Coverage** |
| --- | --- | --- | --- | --- |
| CVE-2024-34854 | F-logic DataCube3 1.0 transceiver\_schedule.php unrestricted upload | A vulnerability which was classified as critical has been found in F-logic DataCube3 1.0. This issue affects some unknown processing of the file /admin/transceiver\_schedule.php. The manipulation leads to unrestricted upload.  The identification of this vulnerability is CVE-2024-34854. The attack may be initiated remotely. There is no exploit available. | Patched by custom rule | N |
| CVE-2024-35510 | DedeCMS 5.7.114 file\_manage\_control.php unrestricted upload | A vulnerability which was classified as critical was found in DedeCMS 5.7.114. This affects an unknown part of the file /dede/file\_manage\_control.php. The manipulation leads to unrestricted upload.  This vulnerability is uniquely identified as CVE-2024-35510. It is possible to initiate the attack remotely. There is no exploit available. | Patched by custom rule | N |
| CVE-2024-5518 | itsourcecode Online Discussion Forum 1.0 change\_profile\_picture.php image unrestricted upload | A vulnerability classified as critical has been found in itsourcecode Online Discussion Forum 1.0. This affects an unknown part of the file change\_profile\_picture.php. The manipulation of the argument image leads to unrestricted upload.  This vulnerability is uniquely identified as CVE-2024-5518. It is possible to initiate the attack remotely. Furthermore there is an exploit available. | Patched by custom rule | N |

XML External Entity Vulnerabilities

| **Public ID** | **Vulnerability Name** | **Vulnerability Description** | **AppTrana Coverage** | **Indusface WAS Coverage** |
| --- | --- | --- | --- | --- |
| CVE-2024-37388 | lxml up to 4.9.0 XML ebookmeta.get\_metadata xml external entity reference (Issue 16) | A vulnerability which was classified as problematic was found in lxml up to 4.9.0. Affected is the function ebookmeta.get\_metadata of the component XML Handler. The manipulation leads to xml external entity reference.  This vulnerability is traded as CVE-2024-37388. The attack needs to be done within the local network. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-36827 | ebookmeta up to 1.2.7 XML ebookmeta.get\_metadata xml external entity reference (Issue 16) | A vulnerability which was classified as problematic has been found in ebookmeta up to 1.2.7. This issue affects the function ebookmeta.get\_metadata of the component XML Handler. The manipulation leads to xml external entity reference.  The identification of this vulnerability is CVE-2024-36827. The attack can only be initiated within the local network. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |

# SQL Injection Vulnerabilities

| **Public ID** | **Vulnerability Name** | **Vulnerability Description** | **AppTrana Coverage** | **Indusface WAS Coverage** |
| --- | --- | --- | --- | --- |
| CVE-2024-5397 | itsourcecode Online Student Enrollment System 1.0 instructorSubjects.php instructorId sql injection | A vulnerability classified as critical was found in itsourcecode Online Student Enrollment System 1.0. Affected by this vulnerability is an unknown functionality of the file instructorSubjects.php. The manipulation of the argument instructorId leads to sql injection.  This vulnerability is known as CVE-2024-5397. The attack can be launched remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-5396 | itsourcecode Online Student Enrollment System 1.0 newfaculty.php name sql injection | A vulnerability classified as critical has been found in itsourcecode Online Student Enrollment System 1.0. Affected is an unknown function of the file newfaculty.php. The manipulation of the argument name leads to sql injection.  This vulnerability is traded as CVE-2024-5396. It is possible to launch the attack remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-35181 | Meshery up to 0.7.21 API kinds sql injection (GHSL-2024-013) | A vulnerability which was classified as critical was found in Meshery up to 0.7.21. This affects an unknown part of the file /api/system/meshsync/resources/kinds of the component API. The manipulation leads to sql injection.  This vulnerability is uniquely identified as CVE-2024-35181. It is possible to initiate the attack remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-35182 | Meshery up to 0.7.21 API /api/v2/events sql injection (GHSL-2024-013) | A vulnerability has been found in Meshery up to 0.7.21 and classified as critical. This vulnerability affects unknown code of the file /api/v2/events of the component API. The manipulation leads to sql injection.  This vulnerability was named CVE-2024-35182. The attack can be initiated remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-4533 | KKProgressbar2 Free Plugin up to 1.1.4.2 on WordPress sql injection | A vulnerability has been found in KKProgressbar2 Free Plugin up to 1.1.4.2 on WordPress and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection.  This vulnerability is known as CVE-2024-4533. The attack can be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-33402 | Campcodes Complete Web-Based School Management System 1.0 approve\_petty\_cash.php id sql injection | A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /model/approve\_petty\_cash.php. The manipulation of the argument id leads to sql injection.  This vulnerability is handled as CVE-2024-33402. The attack may be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-33807 | campcodes Complete Web-Based School Management System 1.0 get\_teacher\_timetable.php grade sql injection | A vulnerability was found in campcodes Complete Web-Based School Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /model/get\_teacher\_timetable.php. The manipulation of the argument grade leads to sql injection.  This vulnerability was named CVE-2024-33807. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-33799 | campcodes Complete Web-Based School Management System 1.0 /model/get\_teacher.php id sql injection | A vulnerability was found in campcodes Complete Web-Based School Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /model/get\_teacher.php. The manipulation of the argument id leads to sql injection.  The identification of this vulnerability is CVE-2024-33799. The attack may be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-33805 | campcodes Complete Web-Based School Management System 1.0 /model/get\_student.php id sql injection | A vulnerability was found in campcodes Complete Web-Based School Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /model/get\_student.php. The manipulation of the argument id leads to sql injection.  This vulnerability is handled as CVE-2024-33805. The attack may be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-36428 | OrangeHRM 3.3.3 admin/viewProjects sortOrder sql injection | A vulnerability which was classified as critical has been found in OrangeHRM 3.3.3. This issue affects some unknown processing of the file admin/viewProjects. The manipulation of the argument sortOrder leads to sql injection.  The identification of this vulnerability is CVE-2024-36428. The attack may be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-35511 | PHPGurukul Men Salon Management System 2.0 /msms/admin/index.php username sql injection | A vulnerability was found in PHPGurukul Men Salon Management System 2.0. It has been declared as critical. This vulnerability affects unknown code of the file /msms/admin/index.php. The manipulation of the argument username leads to sql injection.  This vulnerability was named CVE-2024-35511. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-35469 | SourceCodester Codester Human Resource Management System 1.0 /hrm/user/ password sql injection | A vulnerability which was classified as critical has been found in SourceCodester Codester Human Resource Management System 1.0. Affected by this issue is some unknown functionality of the file /hrm/user/. The manipulation of the argument password leads to sql injection.  This vulnerability is handled as CVE-2024-35469. The attack may be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-35469 | SourceCodester Codester Human Resource Management System 1.0 /hrm/user/ password sql injection | A vulnerability which was classified as critical has been found in SourceCodester Codester Human Resource Management System 1.0. Affected by this issue is some unknown functionality of the file /hrm/user/. The manipulation of the argument password leads to sql injection.  This vulnerability is handled as CVE-2024-35469. The attack may be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-35468 | SourceCodester Codester Human Resource Management System 1.0 /index.php password sql injection | A vulnerability classified as critical was found in SourceCodester Codester Human Resource Management System 1.0. This vulnerability affects unknown code of the file /index.php. The manipulation of the argument password leads to sql injection.  This vulnerability was named CVE-2024-35468. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-5515 | SourceCodester Stock Management System 1.0 createBrand.php brandName sql injection | A vulnerability was found in SourceCodester Stock Management System 1.0. It has been classified as critical. Affected is an unknown function of the file createBrand.php. The manipulation of the argument brandName leads to sql injection.  This vulnerability is traded as CVE-2024-5515. It is possible to launch the attack remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-5519 | ItsourceCode Learning Management System Project In PHP 1.0 login.php user\_email sql injection | A vulnerability classified as critical was found in ItsourceCode Learning Management System Project In PHP 1.0. This vulnerability affects unknown code of the file login.php. The manipulation of the argument user\_email leads to sql injection.  This vulnerability was named CVE-2024-5519. The attack can be initiated remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-5522 | HTML5 Video Player Plugin up to 2.5.26 on WordPress sql injection | A vulnerability was found in HTML5 Video Player Plugin up to 2.5.26 on WordPress. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection.  This vulnerability is known as CVE-2024-5522. The attack can be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-5588 | itsourcecode Learning Management System 1.0 processscore.php LessonID sql injection | A vulnerability was found in itsourcecode Learning Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file processscore.php. The manipulation of the argument LessonID leads to sql injection.  This vulnerability is known as CVE-2024-5588. The attack can be launched remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-5590 | Netentsec NS-ASG Application Security Gateway 6.3 JSON Content uploadiscuser.php messagecontent sql injection | A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3. It has been declared as critical. This vulnerability affects unknown code of the file /protocol/iscuser/uploadiscuser.php of the component JSON Content Handler. The manipulation of the argument messagecontent leads to sql injection.  This vulnerability was named CVE-2024-5590. The attack can be initiated remotely. Furthermore there is an exploit available.  The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |
| CVE-2024-5589 | Netentsec NS-ASG Application Security Gateway 6.3 config\_MT.php Mid sql injection | A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3. It has been classified as critical. This affects an unknown part of the file /admin/config\_MT.phpactiondelete. The manipulation of the argument Mid leads to sql injection.  This vulnerability is uniquely identified as CVE-2024-5589. It is possible to initiate the attack remotely. Furthermore there is an exploit available.  The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |
| CVE-2024-36568 | SourceCodester Gas Agency Management System 1.0 /gasmark/editbrand.php id sql injection | A vulnerability was found in SourceCodester Gas Agency Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /gasmark/editbrand.php. The manipulation of the argument id leads to sql injection.  This vulnerability is known as CVE-2024-36568. The attack can be launched remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-34987 | PHPGurukul Online Fire Reporting System 1.2 ofrs/admin/index.php username sql injection | A vulnerability which was classified as critical has been found in PHPGurukul Online Fire Reporting System 1.2. Affected by this issue is some unknown functionality of the file ofrs/admin/index.php. The manipulation of the argument username leads to sql injection.  This vulnerability is handled as CVE-2024-34987. The attack may be launched remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-5636 | itsourcecode Bakery Online Ordering System 1.0 report/index.php procduct sql injection | A vulnerability was found in itsourcecode Bakery Online Ordering System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file report/index.php. The manipulation of the argument procduct leads to sql injection.  This vulnerability is handled as CVE-2024-5636. The attack may be launched remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-36800 | SEMCMS 4.8 Download.php ID sql injection | A vulnerability which was classified as critical was found in SEMCMS 4.8. Affected is an unknown function of the file Download.php. The manipulation of the argument ID leads to sql injection.  This vulnerability is traded as CVE-2024-36800. It is possible to launch the attack remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-5635 | itsourcecode Bakery Online Ordering System 1.0 index.php txtsearch sql injection | A vulnerability was found in itsourcecode Bakery Online Ordering System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file index.php. The manipulation of the argument txtsearch leads to sql injection.  This vulnerability is known as CVE-2024-5635. The attack can be launched remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-36801 | SEMCMS 4.8 Download.php lgid sql injection | A vulnerability classified as critical was found in SEMCMS 4.8. Affected by this vulnerability is an unknown functionality of the file Download.php. The manipulation of the argument lgid leads to sql injection.  This vulnerability is known as CVE-2024-36801. The attack can be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-5653 | Chanjet Smooth T+system 3.5 keyEdit.aspx KeyID sql injection | A vulnerability which was classified as critical has been found in Chanjet Smooth T+system 3.5. This issue affects some unknown processing of the file /tplus/UFAQD/keyEdit.aspx. The manipulation of the argument KeyID leads to sql injection.  The identification of this vulnerability is CVE-2024-5653. The attack may be initiated remotely. Furthermore there is an exploit available.  The vendor was contacted early about this disclosure but did not respond in any way.  It is recommended to apply restrictive firewalling. | Patched by core rule | Y |
| CVE-2024-36837 | CRMEB 5.2.2 ProductController.php getProductList information disclosure | A vulnerability classified as problematic was found in CRMEB 5.2.2. Affected by this vulnerability is the function getProductList of the file ProductController.php. The manipulation leads to information disclosure.  This vulnerability is known as CVE-2024-36837. The attack can be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-5225 | berriai litellm api\_key sql injection | A vulnerability classified as critical was found in berriai litellm. This vulnerability affects unknown code. The manipulation of the argument api\_key leads to sql injection.  This vulnerability was named CVE-2024-5225. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-36779 | SourceCodester Stock Management System 1.0 editCategories.php sql injection (Issue 42) | A vulnerability was found in SourceCodester Stock Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file editCategories.php. The manipulation leads to sql injection.  The identification of this vulnerability is CVE-2024-36779. The attack may be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-4890 | berriai litellm up to up to 1.27.14 user\_id sql injection | A vulnerability was found in berriai litellm up to up to 1.27.14. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation of the argument user\_id leads to sql injection.  This vulnerability is handled as CVE-2024-4890. The attack may be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-36673 | SourceCodester Pharmacy Medical Store Point of Sale System 1.0 password sql injection (Issue 39) | A vulnerability classified as critical has been found in SourceCodester Pharmacy Medical Store Point of Sale System 1.0. This affects an unknown part. The manipulation of the argument password leads to sql injection.  This vulnerability is uniquely identified as CVE-2024-36673. It is possible to initiate the attack remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-5733 | itsourcecode Online Discussion Forum 1.0 register\_me.php eaddress sql injection | A vulnerability was found in itsourcecode Online Discussion Forum 1.0. It has been rated as critical. This issue affects some unknown processing of the file register\_me.php. The manipulation of the argument eaddress leads to sql injection.  The identification of this vulnerability is CVE-2024-5733. The attack may be initiated remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-5772 | Netentsec NS-ASG Application Security Gateway 6.3 deleteiscuser.php messagecontent sql injection | A vulnerability which was classified as critical has been found in Netentsec NS-ASG Application Security Gateway 6.3. This issue affects some unknown processing of the file /protocol/iscuser/deleteiscuser.php. The manipulation of the argument messagecontent leads to sql injection.  The identification of this vulnerability is CVE-2024-5772. The attack may be initiated remotely. Furthermore there is an exploit available.  The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |
| CVE-2024-5773 | Netentsec NS-ASG Application Security Gateway 6.3 deletemacbind.php messagecontent sql injection | A vulnerability which was classified as critical was found in Netentsec NS-ASG Application Security Gateway 6.3. Affected is an unknown function of the file /protocol/firewall/deletemacbind.php. The manipulation of the argument messagecontent leads to sql injection.  This vulnerability is traded as CVE-2024-5773. It is possible to launch the attack remotely. Furthermore there is an exploit available.  The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |
| CVE-2024-5774 | SourceCodester Stock Management System 1.0 Login index.php username/password sql injection | A vulnerability has been found in SourceCodester Stock Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file index.php of the component Login. The manipulation of the argument username/password leads to sql injection.  This vulnerability is known as CVE-2024-5774. The attack can be launched remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-5775 | SourceCodester Vehicle Management System 1.0 updatebill.php id sql injection | A vulnerability was found in SourceCodester Vehicle Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file updatebill.php. The manipulation of the argument id leads to sql injection.  This vulnerability is handled as CVE-2024-5775. The attack may be launched remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-32501 | Centreon prior 22.04.24/22.10.22/23.04.18/23.10.12/24.04.0 updateServiceHost\_MC sql injection | A vulnerability was found in Centreon. It has been classified as critical. This affects the function updateServiceHost\_MC. The manipulation leads to sql injection.  This vulnerability is uniquely identified as CVE-2024-32501. It is possible to initiate the attack remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-1839 | Intrado 911 Emergency Gateway sql injection (icsa-24-163-04) | A vulnerability classified as critical was found in Intrado 911 Emergency Gateway. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection.  This vulnerability is known as CVE-2024-1839. The attack can be launched remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-22261 | Harbor up to 2.8.5/2.9.3/2.10.1 Task ID sql injection (GHSA-vw63-824v-qf2j) | A vulnerability which was classified as critical was found in Harbor up to 2.8.5/2.9.3/2.10.1. Affected is an unknown function of the component Task ID Handler. The manipulation leads to sql injection.  This vulnerability is traded as CVE-2024-22261. It is possible to launch the attack remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-5894 | SourceCodester Online Eyewear Shop 1.0 manage\_product.php id sql injection | A vulnerability classified as critical was found in SourceCodester Online Eyewear Shop 1.0. This vulnerability affects unknown code of the file manage\_product.php. The manipulation of the argument id leads to sql injection.  This vulnerability was named CVE-2024-5894. The attack can be initiated remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-5895 | SourceCodester Employee and Visitor Gate Pass Logging System 1.0 Users.php delete\_users id sql injection | A vulnerability which was classified as critical has been found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. This issue affects the function delete\_users of the file /classes/Users.phpfdelete. The manipulation of the argument id leads to sql injection.  The identification of this vulnerability is CVE-2024-5895. The attack may be initiated remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-5893 | SourceCodester Cab Management System 1.0 Users.php id sql injection | A vulnerability classified as critical has been found in SourceCodester Cab Management System 1.0. This affects an unknown part of the file /cms/classes/Users.phpfdelete\_client. The manipulation of the argument id leads to sql injection.  This vulnerability is uniquely identified as CVE-2024-5893. It is possible to initiate the attack remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-5896 | SourceCodester Employee and Visitor Gate Pass Logging System 1.0 Users.php save\_users id sql injection | A vulnerability which was classified as critical was found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. Affected is the function save\_users of the file /classes/Users.phpfsave. The manipulation of the argument id leads to sql injection.  This vulnerability is traded as CVE-2024-5896. It is possible to launch the attack remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-5898 | itsourcecode Payroll Management System 1.0 print\_payroll.php id sql injection | A vulnerability was found in itsourcecode Payroll Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file print\_payroll.php. The manipulation of the argument id leads to sql injection.  This vulnerability is handled as CVE-2024-5898. The attack may be launched remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-5983 | itsourcecode Online Bookstore 1.0 bookPerPub.php pubid sql injection | A vulnerability was found in itsourcecode Online Bookstore 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file bookPerPub.php. The manipulation of the argument pubid leads to sql injection.  This vulnerability is known as CVE-2024-5983. The attack can be launched remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-5985 | SourceCodester Best Online News Portal 1.0 /admin/index.php username sql injection | A vulnerability classified as critical has been found in SourceCodester Best Online News Portal 1.0. This affects an unknown part of the file /admin/index.php. The manipulation of the argument username leads to sql injection.  This vulnerability is uniquely identified as CVE-2024-5985. It is possible to initiate the attack remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-5976 | SourceCodester Employee and Visitor Gate Pass Logging System 1.0 Master.php log\_employee employee\_code sql injection | A vulnerability was found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. It has been classified as critical. Affected is the function log\_employee of the file /classes/Master.phpflog\_employee. The manipulation of the argument employee\_code leads to sql injection.  This vulnerability is traded as CVE-2024-5976. It is possible to launch the attack remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-6009 | itsourcecode Event Calendar 1.0 process.php regConfirm/regDelete userId sql injection | A vulnerability has been found in itsourcecode Event Calendar 1.0 and classified as critical. Affected by this vulnerability is the function regConfirm/regDelete of the file process.php. The manipulation of the argument userId leads to sql injection.  This vulnerability is known as CVE-2024-6009. The attack can be launched remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-6013 | itsourcecode Online Book Store 1.0 admin\_delete.php bookisbn sql injection | A vulnerability was found in itsourcecode Online Book Store 1.0. It has been rated as critical. This issue affects some unknown processing of the file admin\_delete.php. The manipulation of the argument bookisbn leads to sql injection.  The identification of this vulnerability is CVE-2024-6013. The attack may be initiated remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-6014 | itsourcecode Document Management System 1.0 edithis.php id sql injection | A vulnerability classified as critical has been found in itsourcecode Document Management System 1.0. Affected is an unknown function of the file edithis.php. The manipulation of the argument id leads to sql injection.  This vulnerability is traded as CVE-2024-6014. It is possible to launch the attack remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-6007 | Netentsec NS-ASG Application Security Gateway 6.3 deleteiscgwrouteconf.php messagecontent sql injection | A vulnerability classified as critical has been found in Netentsec NS-ASG Application Security Gateway 6.3. This affects an unknown part of the file /protocol/iscgwtunnel/deleteiscgwrouteconf.php. The manipulation of the argument messagecontent leads to sql injection.  This vulnerability is uniquely identified as CVE-2024-6007. It is possible to initiate the attack remotely. Furthermore there is an exploit available.  The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |
| CVE-2024-6043 | SourceCodester Best House Rental Management System 1.0 admin\_class.php login username sql injection | A vulnerability classified as critical has been found in SourceCodester Best House Rental Management System 1.0. This affects the function login of the file admin\_class.php. The manipulation of the argument username leads to sql injection.  This vulnerability is uniquely identified as CVE-2024-6043. It is possible to initiate the attack remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-6042 | itsourcecode Real Estate Management System 1.0 property-detail.php id sql injection | A vulnerability was found in itsourcecode Real Estate Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file property-detail.php. The manipulation of the argument id leads to sql injection.  This vulnerability is handled as CVE-2024-6042. The attack may be launched remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-6041 | itsourcecode Gym Management System 1.0 manage\_user.php id sql injection | A vulnerability was found in itsourcecode Gym Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file manage\_user.php. The manipulation of the argument id leads to sql injection.  This vulnerability is known as CVE-2024-6041. The attack can be launched remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-37848 | Online Bookstore 1.0 admin\_delete.php sql injection (Issue 13) | A vulnerability which was classified as critical was found in Online Bookstore 1.0. This affects an unknown part of the file admin\_delete.php. The manipulation leads to sql injection.  This vulnerability is uniquely identified as CVE-2024-37848. Local access is required to approach this attack. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-6067 | SourceCodester Music Class Enrollment System 1.0 id sql injection | A vulnerability classified as critical was found in SourceCodester Music Class Enrollment System 1.0. Affected by this vulnerability is an unknown functionality of the file /mces/pclass/view\_class. The manipulation of the argument id leads to sql injection.  This vulnerability is known as CVE-2024-6067. The attack can be launched remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-6065 | itsourcecode Bakery Online Ordering System 1.0 index.php user\_email sql injection | A vulnerability was found in itsourcecode Bakery Online Ordering System 1.0. It has been rated as critical. This issue affects some unknown processing of the file index.php. The manipulation of the argument user\_email leads to sql injection.  The identification of this vulnerability is CVE-2024-6065. The attack may be initiated remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-37840 | itsourcecode Learning Management System 1.0 processscore.php LessonID sql injection | A vulnerability was found in itsourcecode Learning Management System 1.0. It has been classified as critical. Affected is an unknown function of the file processscore.php. The manipulation of the argument LessonID leads to sql injection.  This vulnerability is traded as CVE-2024-37840. It is possible to launch the attack remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-6066 | SourceCodester Best House Rental Management System 1.0 payment\_report.php month\_of sql injection | A vulnerability classified as critical has been found in SourceCodester Best House Rental Management System 1.0. Affected is an unknown function of the file payment\_report.php. The manipulation of the argument month\_of leads to sql injection.  This vulnerability is traded as CVE-2024-6066. It is possible to launch the attack remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-38347 | CodeProjects Health Care Hospital Management System 1.0 Room Information Module id sql injection | A vulnerability classified as critical has been found in CodeProjects Health Care Hospital Management System 1.0. Affected is an unknown function of the component Room Information Module. The manipulation of the argument id leads to sql injection.  This vulnerability is traded as CVE-2024-38347. It is possible to launch the attack remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-6113 | itsourcecode Monbela Tourist Inn Online Reservation System 1.0 login.php email sql injection | A vulnerability was found in itsourcecode Monbela Tourist Inn Online Reservation System 1.0. It has been rated as critical. This issue affects some unknown processing of the file login.php. The manipulation of the argument email leads to sql injection.  The identification of this vulnerability is CVE-2024-6113. The attack may be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-6111 | itsourcecode Pool of Bethesda Online Reservation System 1.0 login.php email sql injection | A vulnerability classified as critical has been found in itsourcecode Pool of Bethesda Online Reservation System 1.0. This affects an unknown part of the file login.php. The manipulation of the argument email leads to sql injection.  This vulnerability is uniquely identified as CVE-2024-6111. It is possible to initiate the attack remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-37799 | CodeProjects Restaurant Reservation System 1.0 view\_reservations.php reserv\_id sql injection | A vulnerability has been found in CodeProjects Restaurant Reservation System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file view\_reservations.php. The manipulation of the argument reserv\_id leads to sql injection.  This vulnerability is known as CVE-2024-37799. The attack can be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-38348 | CodeProjects Health Care Hospital Management System 1.0 Staff Info Module searvalu sql injection | A vulnerability classified as critical was found in CodeProjects Health Care Hospital Management System 1.0. Affected by this vulnerability is an unknown functionality of the component Staff Info Module. The manipulation of the argument searvalu leads to sql injection.  This vulnerability is known as CVE-2024-38348. The attack can be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-37802 | CodeProjects Health Care hospital Management System 1.0 Patient Info Module searvalu sql injection | A vulnerability which was classified as critical was found in CodeProjects Health Care hospital Management System 1.0. This affects an unknown part of the component Patient Info Module. The manipulation of the argument searvalu leads to sql injection.  This vulnerability is uniquely identified as CVE-2024-37802. It is possible to initiate the attack remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-6190 | itsourcecode Farm Management System 1.0 Login index.php username sql injection | A vulnerability was found in itsourcecode Farm Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file index.php of the component Login. The manipulation of the argument username leads to sql injection.  This vulnerability is handled as CVE-2024-6190. The attack may be launched remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-6192 | itsourcecode Loan Management System 1.0 Login Page login.php username sql injection | A vulnerability classified as critical was found in itsourcecode Loan Management System 1.0. This vulnerability affects unknown code of the file login.php of the component Login Page. The manipulation of the argument username leads to sql injection.  This vulnerability was named CVE-2024-6192. The attack can be initiated remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-6241 | Pear Admin Boot up to 2.0.2 getDictItems sql injection | A vulnerability was found in Pear Admin Boot up to 2.0.2 and classified as critical. This issue affects the function getDictItems of the file /system/dictData/getDictItems/. The manipulation with the input user11 leads to sql injection.  The identification of this vulnerability is CVE-2024-6241. The attack may be initiated remotely. Furthermore there is an exploit available. | Patched by core rule | Y |

# Cross-site Scripting Vulnerabilities

| **Public ID** | **Vulnerability Name** | **Vulnerability Description** | **AppTrana Coverage** | **Indusface WAS Coverage** |
| --- | --- | --- | --- | --- |
| CVE-2024-3939 | Ditty Plugin up to 3.1.35 on WordPress Setting cross site scripting | A vulnerability classified as problematic was found in Ditty Plugin up to 3.1.35 on WordPress. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting.  This vulnerability is known as CVE-2024-3939. The attack can be launched remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-35236 | advplyr audiobookshelf up to 2.9.0 File cross site scripting (GHSA-7j99-76cj-q9pg) | A vulnerability which was classified as problematic has been found in advplyr audiobookshelf up to 2.9.0. This issue affects some unknown processing of the component File Handler. The manipulation leads to cross site scripting.  The identification of this vulnerability is CVE-2024-35236. The attack may be initiated remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-36109 | sagemathinc cocalc Markdown Parser cross site scripting (GHSA-8w44-hggw-p5rf) | A vulnerability was found in sagemathinc cocalc and classified as problematic. This issue affects some unknown processing of the component Markdown Parser. The manipulation leads to cross site scripting.  The identification of this vulnerability is CVE-2024-36109. The attack may be initiated remotely. There is no exploit available.  It is recommended to apply a patch to fix this issue. | Patched by core rule | Y |
| CVE-2024-5437 | SourceCodester Simple Online Bidding System 1.0 index.php save\_category name cross site scripting | A vulnerability was found in SourceCodester Simple Online Bidding System 1.0. It has been classified as problematic. Affected is the function save\_category of the file /admin/index.phppagecategories. The manipulation of the argument name leads to cross site scripting.  This vulnerability is traded as CVE-2024-5437. It is possible to launch the attack remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-36110 | ansibleguy webui up to 0.0.20 cross site scripting (ID 44) | A vulnerability has been found in ansibleguy webui up to 0.0.20 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting.  This vulnerability was named CVE-2024-36110. The attack can be initiated remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-35583 | SourceCodester Laboratory Management System 1.0 Remarks cross site scripting | A vulnerability was found in SourceCodester Laboratory Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument Remarks leads to cross site scripting.  This vulnerability is handled as CVE-2024-35583. The attack may be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-35582 | SourceCodester Laboratory Management System 1.0 Department cross site scripting | A vulnerability was found in SourceCodester Laboratory Management System 1.0. It has been classified as problematic. Affected is an unknown function. The manipulation of the argument Department leads to cross site scripting.  This vulnerability is traded as CVE-2024-35582. It is possible to launch the attack remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-35240 | Umbraco Umbraco.Commerce.Issues prior 10.0.5/12.1.4 Print cross site scripting | A vulnerability classified as problematic was found in Umbraco Umbraco.Commerce.Issues. This vulnerability affects unknown code of the component Print Handler. The manipulation leads to cross site scripting.  This vulnerability was named CVE-2024-35240. The attack can be initiated remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-35581 | SourceCodester Laboratory Management System 1.0 Borrower Name cross site scripting | A vulnerability was found in SourceCodester Laboratory Management System 1.0. It has been classified as problematic. This affects an unknown part. The manipulation of the argument Borrower Name leads to cross site scripting.  This vulnerability is uniquely identified as CVE-2024-35581. It is possible to initiate the attack remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-3921 | Gianism Plugin up to 5.1.0 on WordPress Setting cross site scripting | A vulnerability has been found in Gianism Plugin up to 5.1.0 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting.  This vulnerability is known as CVE-2024-3921. The attack can be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-3937 | Playlist for Youtube Plugin up to 1.32 on WordPress Setting cross site scripting | A vulnerability was found in Playlist for Youtube Plugin up to 1.32 on WordPress and classified as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting.  This vulnerability is handled as CVE-2024-3937. The attack may be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-25976 | HAWKI LDAP Authentication login.php $\_SERVER['PHP\_SELF'] cross site scripting | A vulnerability which was classified as problematic has been found in University of Applied Sciences and Arts Hildesheim HAWKI. Affected by this issue is some unknown functionality of the file login.php of the component LDAP Authentication Handler. The manipulation of the argument $\_SERVER[&039;PHP\_SELF&039;] leads to cross site scripting.  This vulnerability is handled as CVE-2024-25976. The attack may be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-35432 | ZKTeco ZKBio CVSecurity 6.1.1 Audio File cross site scripting | A vulnerability has been found in ZKTeco ZKBio CVSecurity 6.1.1 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Audio File Handler. The manipulation leads to cross site scripting.  This vulnerability is known as CVE-2024-35432. The attack can be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-35504 | FineSoft 8.0 URL errorname cross site scripting | A vulnerability was found in FineSoft 8.0. It has been declared as problematic. This vulnerability affects unknown code of the component URL Handler. The manipulation of the argument errorname leads to cross site scripting.  This vulnerability was named CVE-2024-35504. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-35432 | ZKTeco ZKBio CVSecurity 6.1.1 Audio File cross site scripting | A vulnerability has been found in ZKTeco ZKBio CVSecurity 6.1.1 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Audio File Handler. The manipulation leads to cross site scripting.  This vulnerability is known as CVE-2024-35432. The attack can be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2022-25038 | wanEditor 4.7.11 Video Upload cross site scripting (Issue 3872) | A vulnerability classified as problematic was found in wanEditor 4.7.11. Affected by this vulnerability is an unknown functionality of the component Video Upload. The manipulation leads to cross site scripting.  This vulnerability is known as CVE-2022-25038. The attack can be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2022-25037 | wanEditor 4.7.11 Image Upload cross site scripting (Issue 3870) | A vulnerability was found in wanEditor 4.7.11. It has been rated as problematic. This issue affects some unknown processing of the component Image Upload. The manipulation leads to cross site scripting.  The identification of this vulnerability is CVE-2022-25037. The attack may be initiated remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-36123 | StarCitizenTools mediawiki-skins-Citizen up to 2.15.x cross site scripting (GHSA-jhm6-qjhq-5mf9) | A vulnerability has been found in StarCitizenTools mediawiki-skins-Citizen up to 2.15.x and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting.  This vulnerability is known as CVE-2024-36123. The attack can be launched remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-36674 | LyLme\_spage 1.9.5 admin/link.php cross site scripting (Issue 91) | A vulnerability classified as problematic has been found in LyLme\_spage 1.9.5. Affected is an unknown function of the file admin/link.php. The manipulation leads to cross site scripting.  This vulnerability is traded as CVE-2024-36674. It is possible to launch the attack remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-4749 | WP-FeedStats wp-eMember Plugin up to 10.3.8 on WordPress fieldId cross site scripting | A vulnerability was found in WP-FeedStats wp-eMember Plugin up to 10.3.8 on WordPress. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument fieldId leads to cross site scripting.  This vulnerability was named CVE-2024-4749. The attack can be initiated remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-4857 | FS Product Inquiry Plugin up to 1.1.1 on WordPress Form Submission cross site scripting | A vulnerability classified as problematic was found in FS Product Inquiry Plugin up to 1.1.1 on WordPress. This vulnerability affects unknown code of the component Form Submission Handler. The manipulation leads to cross site scripting.  This vulnerability was named CVE-2024-4857. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-4180 | Events Calendar Plugin up to 6.4.0.0 on WordPress cross site scripting | A vulnerability which was classified as problematic has been found in Events Calendar Plugin up to 6.4.0.0 on WordPress. This issue affects some unknown processing. The manipulation leads to cross site scripting.  The identification of this vulnerability is CVE-2024-4180. The attack may be initiated remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-2470 | Simple Ajax Chat Plugin prior 20240412 on WordPress Setting cross site scripting | A vulnerability was found in Simple Ajax Chat Plugin on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting.  This vulnerability is known as CVE-2024-2470. The attack can be launched remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-4856 | FS Product Inquiry Plugin up to 1.1.1 on WordPress cross site scripting | A vulnerability was found in FS Product Inquiry Plugin up to 1.1.1 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting.  This vulnerability is handled as CVE-2024-4856. The attack may be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-0756 | Insert or Embed Articulate Content into WordPress Plugin cross site scripting | A vulnerability was found in Insert or Embed Articulate Content into WordPress Plugin up to 4.3000000023 on WordPress and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to basic cross site scripting.  This vulnerability is handled as CVE-2024-0756. The attack may be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-30889 | audimex audimexEE up to 15.1.3.8 service/method/widget\_type/request\_id cross site scripting | A vulnerability has been found in audimex audimexEE up to 15.1.3.8 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument service/method/widget\_type/request\_id leads to cross site scripting.  This vulnerability was named CVE-2024-30889. The attack can be initiated remotely. Furthermore there is an exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-3166 | mintplex-labs anything-llm up to 1.4.1 cross site scripting | A vulnerability was found in mintplex-labs anything-llm up to 1.4.1. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting.  This vulnerability was named CVE-2024-3166. The attack can be initiated remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-5478 | lunary-ai lunary up to 1.2.7 cross site scripting | A vulnerability which was classified as problematic was found in lunary-ai lunary up to 1.2.7. This affects an unknown part of the file /auth/saml/${org.id}/metadata. The manipulation leads to cross site scripting.  This vulnerability is uniquely identified as CVE-2024-5478. It is possible to initiate the attack remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-3110 | mintplex-labs anything-llm up to 0.x cross site scripting | A vulnerability classified as problematic has been found in mintplex-labs anything-llm up to 0.x. Affected is an unknown function. The manipulation leads to cross site scripting.  This vulnerability is traded as CVE-2024-3110. It is possible to launch the attack remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-3402 | gaizhenbiao chuanhuchatgpt up to 20240121 cross site scripting | A vulnerability classified as problematic was found in gaizhenbiao chuanhuchatgpt up to 20240121. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting.  This vulnerability is known as CVE-2024-3402. The attack can be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-36773 | Monstra CMS 3.0.4 index.php Themes cross site scripting | A vulnerability was found in Monstra CMS 3.0.4. It has been rated as problematic. This issue affects some unknown processing of the file index.php. The manipulation of the argument Themes leads to cross site scripting.  The identification of this vulnerability is CVE-2024-36773. The attack may be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-37160 | Formwork up to 1.13.0/2.0.0-beta.1 /panel/options/site cross site scripting (GHSA-5pxr-7m4j-jjc6) | A vulnerability which was classified as problematic has been found in Formwork up to 1.13.0/2.0.0-beta.1. This issue affects some unknown processing of the file /panel/options/site. The manipulation leads to cross site scripting.  The identification of this vulnerability is CVE-2024-37160. The attack may be initiated remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-4621 | ARForms Plugin up to 6.5 on WordPress Setting cross site scripting | A vulnerability which was classified as problematic has been found in ARForms Plugin up to 6.5 on WordPress. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting.  This vulnerability is handled as CVE-2024-4621. The attack may be launched remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-36775 | Monstra CMS 3.0.4 Profile Page About Me cross site scripting | A vulnerability has been found in Monstra CMS 3.0.4 and classified as problematic. This vulnerability affects unknown code of the component Profile Page. The manipulation of the argument About Me leads to cross site scripting.  This vulnerability was named CVE-2024-36775. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-5851 | playSMS up to 1.4.7 SMS Schedule index.php name/message cross site scripting | A vulnerability classified as problematic has been found in playSMS up to 1.4.7. Affected is an unknown function of the file /index.phpappmain&amp;incfeature\_schedule&amp;oplist of the component SMS Schedule Handler. The manipulation of the argument name/message leads to basic cross site scripting.  This vulnerability is traded as CVE-2024-5851. It is possible to launch the attack remotely. Furthermore there is an exploit available.  The code maintainer was contacted early about this disclosure and was eager to prepare a fix as quickly as possible.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-5897 | SourceCodester Employee and Visitor Gate Pass Logging System 1.0 Master.php name cross site scripting | A vulnerability has been found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /classes/Master.phpflog\_visitor. The manipulation of the argument name leads to cross site scripting.  This vulnerability is known as CVE-2024-5897. The attack can be launched remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-37629 | SummerNote 0.8.18 Code View cross site scripting (Issue 4642) | A vulnerability classified as problematic has been found in SummerNote 0.8.18. Affected is an unknown function of the component Code View. The manipulation leads to cross site scripting.  This vulnerability is traded as CVE-2024-37629. It is possible to launch the attack remotely. Furthermore there is an exploit available. | Patched by core rule | Y |
| CVE-2024-4924 | Social Sharing Plugin up to 3.3.62 on WordPress Setting cross site scripting | A vulnerability which was classified as problematic was found in Social Sharing Plugin up to 3.3.62 on WordPress. This affects an unknown part of the component Setting Handler. The manipulation leads to cross site scripting.  This vulnerability is uniquely identified as CVE-2024-4924. It is possible to initiate the attack remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-0427 | ARForms Plugin up to 6.4.0 on WordPress cross site scripting | A vulnerability has been found in ARForms Plugin up to 6.4.0 on WordPress and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting.  This vulnerability was named CVE-2024-0427. The attack can be initiated remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-37297 | WooCommerce up to 8.8.4/8.9.2 Sourcebuster.js cross site scripting (GHSA-cv23-q6gh-xfrf) | A vulnerability has been found in WooCommerce up to 8.8.4/8.9.2 and classified as problematic. This vulnerability affects unknown code of the file Sourcebuster.js. The manipulation leads to cross site scripting.  This vulnerability was named CVE-2024-37297. The attack can be initiated remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-36647 | Church CRM 5.8.0 New Family Page Family Name cross site scripting (Issue 7029) | A vulnerability was found in Church CRM 5.8.0 and classified as problematic. This issue affects some unknown processing of the component New Family Page. The manipulation of the argument Family Name leads to cross site scripting.  The identification of this vulnerability is CVE-2024-36647. The attack may be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-3992 | Amen Plugin up to 3.3.1 on WordPress Setting cross site scripting | A vulnerability classified as problematic was found in Amen Plugin up to 3.3.1 on WordPress. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross site scripting.  This vulnerability was named CVE-2024-3992. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-3977 | Jitsi Shortcode Plugin up to 0.1 on WordPress Setting cross site scripting | A vulnerability classified as problematic has been found in Jitsi Shortcode Plugin up to 0.1 on WordPress. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross site scripting.  This vulnerability is traded as CVE-2024-3977. It is possible to launch the attack remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-3966 | Pray for Me Plugin up to 1.0.4 on WordPress cross site scripting | A vulnerability was found in Pray for Me Plugin up to 1.0.4 on WordPress. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting.  The identification of this vulnerability is CVE-2024-3966. The attack may be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-3754 | Alemha Watermarker Plugin up to 1.3.1 on WordPress Setting cross site scripting | A vulnerability was found in Alemha Watermarker Plugin up to 1.3.1 on WordPress. It has been declared as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross site scripting.  This vulnerability was named CVE-2024-3754. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-37888 | mlewand ckeditor-plugin-openlink up to 1.0.4 cross site scripting | A vulnerability was found in mlewand ckeditor-plugin-openlink up to 1.0.4 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting.  This vulnerability is handled as CVE-2024-37888. The attack may be launched remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-3978 | Jitsi Shortcode Plugin up to 0.1 on WordPress Shortcode Attribute cross site scripting | A vulnerability was found in Jitsi Shortcode Plugin up to 0.1 on WordPress. It has been classified as problematic. This affects an unknown part of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting.  This vulnerability is uniquely identified as CVE-2024-3978. It is possible to initiate the attack remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-36656 | MintHCM 4.0.3 cross site scripting | A vulnerability has been found in MintHCM 4.0.3 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting.  This vulnerability was named CVE-2024-36656. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-37624 | Xinhu RockOA 2.6.3 inputChajian.php cross site scripting | A vulnerability classified as problematic was found in Xinhu RockOA 2.6.3. This vulnerability affects unknown code of the file /chajian/inputChajian.php. The manipulation leads to cross site scripting.  This vulnerability was named CVE-2024-37624. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-4305 | Post Grid Gutenberg Blocks and Blog Plugin up to 4.0.x on WordPress Block cross site scripting | A vulnerability which was classified as problematic has been found in Post Grid Gutenberg Blocks and Blog Plugin up to 4.0.x on WordPress. Affected by this issue is some unknown functionality of the component Block Handler. The manipulation leads to cross site scripting.  This vulnerability is handled as CVE-2024-4305. The attack may be launched remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-37619 | StrongShop 1.0 /spec/index.blade.php spec\_group\_id cross site scripting (Issue 45) | A vulnerability was found in StrongShop 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /spec/index.blade.php. The manipulation of the argument spec\_group\_id leads to cross site scripting.  This vulnerability is known as CVE-2024-37619. The attack can be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-38470 | zhimengzhe iBarn 1.5 /own.php search cross site scripting | A vulnerability was found in zhimengzhe iBarn 1.5. It has been classified as problematic. Affected is an unknown function of the file /own.php. The manipulation of the argument search leads to cross site scripting.  This vulnerability is traded as CVE-2024-38470. It is possible to launch the attack remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-37622 | Xinhu RockOA 2.6.3 /flow/flow.php num cross site scripting | A vulnerability has been found in Xinhu RockOA 2.6.3 and classified as problematic. This vulnerability affects unknown code of the file /flow/flow.php. The manipulation of the argument num leads to cross site scripting.  This vulnerability was named CVE-2024-37622. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-38469 | zhimengzhe iBarn 1.5 Parameter /pay.php search cross site scripting | A vulnerability classified as problematic has been found in zhimengzhe iBarn 1.5. This affects an unknown part of the file /pay.php of the component Parameter Handler. The manipulation of the argument search leads to cross site scripting.  This vulnerability is uniquely identified as CVE-2024-38469. It is possible to initiate the attack remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-37620 | PHPVOD 4.0 /view/admin/view.php id cross site scripting | A vulnerability which was classified as problematic has been found in PHPVOD 4.0. This issue affects some unknown processing of the file /view/admin/view.php. The manipulation of the argument id leads to cross site scripting.  The identification of this vulnerability is CVE-2024-37620. The attack may be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-37625 | zhimengzhe iBarn 1.5 Parameter /index.php search cross site scripting | A vulnerability which was classified as problematic has been found in zhimengzhe iBarn 1.5. Affected by this issue is some unknown functionality of the file /index.php of the component Parameter Handler. The manipulation of the argument search leads to cross site scripting.  This vulnerability is handled as CVE-2024-37625. The attack may be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-37623 | Xinhu RockOA 2.6.3 tpl\_kaoqin\_locationchange.html cross site scripting | A vulnerability has been found in Xinhu RockOA 2.6.3 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /kaoqin/tpl\_kaoqin\_locationchange.html. The manipulation leads to cross site scripting.  This vulnerability is known as CVE-2024-37623. The attack can be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-3236 | Popup Builder Plugin up to 1.1.32 on WordPress Notifications cross site scripting | A vulnerability classified as problematic was found in Popup Builder Plugin up to 1.1.32 on WordPress. Affected by this vulnerability is an unknown functionality of the component Notifications Handler. The manipulation leads to cross site scripting.  This vulnerability is known as CVE-2024-3236. The attack can be launched remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-37803 | CodeProjects Health Care Hospital Management System 1.0 Staff Info Page fname/lname cross site scripting | A vulnerability which was classified as problematic has been found in CodeProjects Health Care Hospital Management System 1.0. Affected by this issue is some unknown functionality of the component Staff Info Page. The manipulation of the argument fname/lname leads to cross site scripting.  This vulnerability is handled as CVE-2024-37803. The attack may be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-37800 | CodeProjects Restaurant Reservation System 1.0 index.php Date cross site scripting | A vulnerability was found in CodeProjects Restaurant Reservation System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file index.php. The manipulation of the argument Date leads to cross site scripting.  The identification of this vulnerability is CVE-2024-37800. The attack may be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-3276 | Lightbox & Modal Popup Plugin up to 2.7.27 on WordPress Setting cross site scripting | A vulnerability which was classified as problematic was found in Lightbox & Modal Popup Plugin and foobox-image-lightbox-premium Plugin up to 2.7.27 on WordPress. This affects an unknown part of the component Setting Handler. The manipulation leads to cross site scripting.  This vulnerability is uniquely identified as CVE-2024-3276. It is possible to initiate the attack remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-5172 | Expert Invoice Plugin up to 1.0.2 on WordPress Setting cross site scripting | A vulnerability was found in Expert Invoice Plugin up to 1.0.2 on WordPress and classified as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross site scripting.  The identification of this vulnerability is CVE-2024-5172. The attack may be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-31586 | Computer Laboratory Management System 1.0 Borrower Name/Department/Remarks cross site scripting | A vulnerability was found in Computer Laboratory Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument Borrower Name/Department/Remarks leads to cross site scripting.  This vulnerability was named CVE-2024-31586. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-5475 | Responsive Video Embed Plugin up to 0.5.0 on WordPress Shortcode cross site scripting | A vulnerability classified as problematic has been found in Responsive Video Embed Plugin up to 0.5.0 on WordPress. Affected is an unknown function of the component Shortcode Handler. The manipulation leads to cross site scripting.  This vulnerability is traded as CVE-2024-5475. It is possible to launch the attack remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-5448 | PayPal Pay Now, Buy Now, Donation and Cart Buttons Shortcode Plugin cross site scripting | A vulnerability was found in PayPal Pay Now Buy Now Donation and Cart Buttons Shortcode Plugin up to 1.7 on WordPress. It has been declared as problematic. This vulnerability affects unknown code of the component Shortcode Handler. The manipulation leads to cross site scripting.  This vulnerability was named CVE-2024-5448. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-4381 | CB Plugin up to 0.9.4.18 on WordPress Setting cross site scripting | A vulnerability was found in CB Plugin up to 0.9.4.18 on WordPress. It has been declared as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross site scripting.  This vulnerability was named CVE-2024-4381. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-5447 | PayPal Pay Now, Buy Now, Donation and Cart Buttons Shortcode Plugin cross site scripting | A vulnerability was found in PayPal Pay Now Buy Now Donation and Cart Buttons Shortcode Plugin up to 1.7 on WordPress. It has been classified as problematic. This affects an unknown part of the component Shortcode Handler. The manipulation leads to cross site scripting.  This vulnerability is uniquely identified as CVE-2024-5447. It is possible to initiate the attack remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-4970 | Widget Bundle Plugin up to 2.0.0 on WordPress Setting cross site scripting | A vulnerability was found in Widget Bundle Plugin up to 2.0.0 on WordPress and classified as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting.  This vulnerability is handled as CVE-2024-4970. The attack may be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-4477 | WP Logs Book Plugin up to 1.0.1 on WordPress Admin Dashboard cross site scripting | A vulnerability was found in WP Logs Book Plugin up to 1.0.1 on WordPress and classified as problematic. Affected by this issue is some unknown functionality of the component Admin Dashboard. The manipulation leads to cross site scripting.  This vulnerability is handled as CVE-2024-4477. The attack may be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-4616 | Widget Bundle Plugin up to 2.0.0 on WordPress cross site scripting | A vulnerability was found in Widget Bundle Plugin up to 2.0.0 on WordPress. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross site scripting.  This vulnerability is uniquely identified as CVE-2024-4616. It is possible to initiate the attack remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-4755 | ptz0n Google CSE Plugin up to 1.0.7 on WordPress Setting cross site scripting | A vulnerability was found in ptz0n Google CSE Plugin up to 1.0.7 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting.  This vulnerability is handled as CVE-2024-4755. The attack may be launched remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-37675 | Tessi Docubase Document Management 5.x Note sectionContent cross site scripting | A vulnerability was found in Tessi Docubase Document Management 5.x. It has been declared as problematic. This vulnerability affects unknown code of the component Note Handler. The manipulation of the argument sectionContent leads to cross site scripting.  This vulnerability was named CVE-2024-37675. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-37671 | Tessi Docubase Document Management 5.x page cross site scripting | A vulnerability which was classified as problematic has been found in Tessi Docubase Document Management 5.x. This issue affects some unknown processing. The manipulation of the argument page leads to cross site scripting.  The identification of this vulnerability is CVE-2024-37671. The attack may be initiated remotely. There is no exploit available. | Patched by core rule | Y |
| CVE-2024-4899 | SEOPress Plugin up to 7.7 on WordPress Post Setting cross site scripting | A vulnerability was found in SEOPress Plugin up to 7.7 on WordPress and classified as problematic. This issue affects some unknown processing of the component Post Setting Handler. The manipulation leads to cross site scripting.  The identification of this vulnerability is CVE-2024-4899. The attack may be initiated remotely. There is no exploit available.  It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2024-4759 | Mime Types Extended Plugin up to 0.11 on WordPress SVG File cross site scripting | A vulnerability has been found in Mime Types Extended Plugin up to 0.11 on WordPress and classified as problematic. This vulnerability affects unknown code of the component SVG File Handler. The manipulation leads to cross site scripting.  This vulnerability was named CVE-2024-4759. The attack can be initiated remotely. There is no exploit available. | Patched by core rule | Y |

# 

## 



Monthly Zero-Day Vulnerability Coverage Bulletin June 2024

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

Indusface, an institutionally funded firm, is the only vendor to receive

100% customer recommendation rating four years in a row and is a global customer choice in the 2024 Gartner Peer Insights™ Web Application and API Protection (WAAP) Report. Indusface is also a “Great Place to Work” 2024 certified and is PCI, ISO27001, SOC 2, GDPR certified and has been the recipient of many prestigious start-up awards.

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

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

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