

Scan Report

CoE - ICHOM Lung Quest ionnaire

Grouped By: Vulnerability Type
Scanned Branch Name: N/A
Project Created: 08 Apr, 2025 | 3:34 AM UTC+0
Last Scanned: 08 Apr, 2025 | 3:35 AM UTC+0
Scanners: SAST, SCA, Containers, IaC

C

2

H

7

M

9

Shield




18

Table of Contents

| | |
|-------------------------------|----|
| Filtered By | 3 |
| Scan Information | 3 |
| Project & Scan Tags | 3 |
| Scan Results Overview | 4 |
| By Scanner | 4 |
| By Status | 4 |
| By Severity | 4 |
| By State | 4 |
| By Language | 4 |
| By Technology | 4 |
| By Package | 4 |
| By SAST Vulnerability | 5 |
| Top 10 SAST Vulnerabilities | 5 |
| Top 10 SAST Vulnerable Files | 5 |
| 5 Oldest SAST Vulnerabilities | 5 |
| SAST Vulnerabilities | 6 |
| By Severity | 6 |
| SAST Scan Results | 6 |
| Use_Of_Hardcoded_Password | 6 |
| Missing_HSTS_Header | 8 |
| IaC Vulnerabilities | 9 |
| By Severity | 9 |
| IaC Scan Results | 9 |
| SCA Vulnerabilities | 10 |
| By Severity | 10 |
| SCA Scan Results | 10 |
| Npm-datatables.net-1.10.19 | 10 |
| Npm-moment-timezone-0.5.34 | 10 |
| Npm-moment-2.24.0 | 11 |
| Npm-datatables-1.10.18 | 12 |
| Python-Django-5.1.2 | 12 |
| Npm-jquery-3.4.1 | 14 |
| Python-cryptography-44.0.0 | 14 |
| SAST Resolved Vulnerabilities | 16 |
| Categories | 17 |
| ASA Premium | 17 |
| ASD STIG 6.1 | 17 |
| CWE top 25 | 17 |
| FISMA 2014 | 17 |
| MOIS(KISA) Secure Coding 2021 | 17 |
| NIST SP 800-53 | 17 |
| OWASP ASVS | 17 |
| OWASP Top 10 2021 | 18 |

| | |
|---------------------------------|----|
| OWASP Top 10 API | 18 |
| OWASP Top 10 API 2023 | 18 |
| PCI DSS v4.0 | 18 |
| SANS top 25 | 18 |
| Vulnerability Details | 19 |
| Use_Of_Hardcoded_Password | 19 |
| Missing_HSTS_Header | 19 |

Filtered By

Severity:   

Excluded: Low, Information

Result State: [To Verify](#), [Confirmed](#), [Urgent](#)

Excluded: Not Exploitable, Proposed Not Exploitable

Status: [New](#), [Recurrent](#)

Excluded: None

Scanners: [SAST](#), [SCA](#), [Containers](#), [IaC](#)

Excluded: None

Queries: [Link](#)

Results limited to: 10000

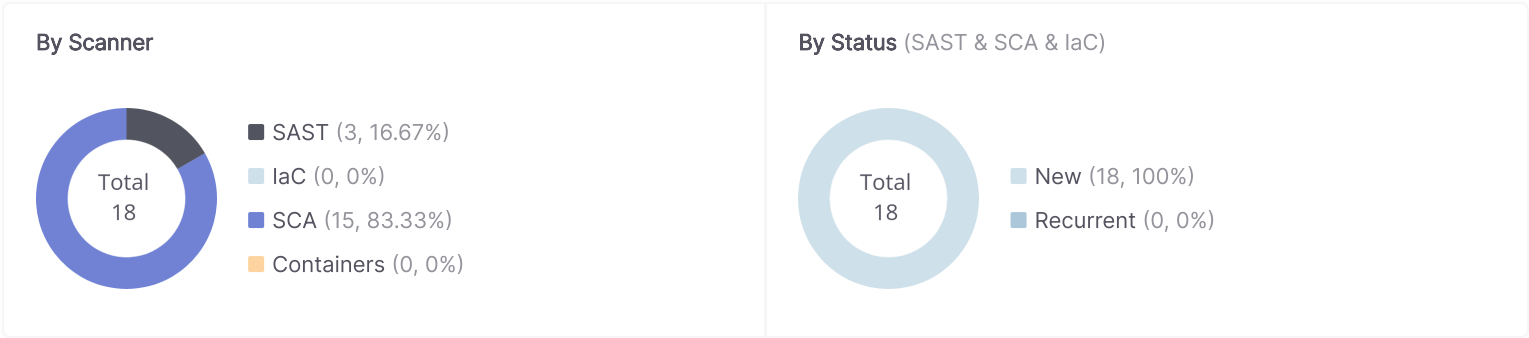
Scan Information

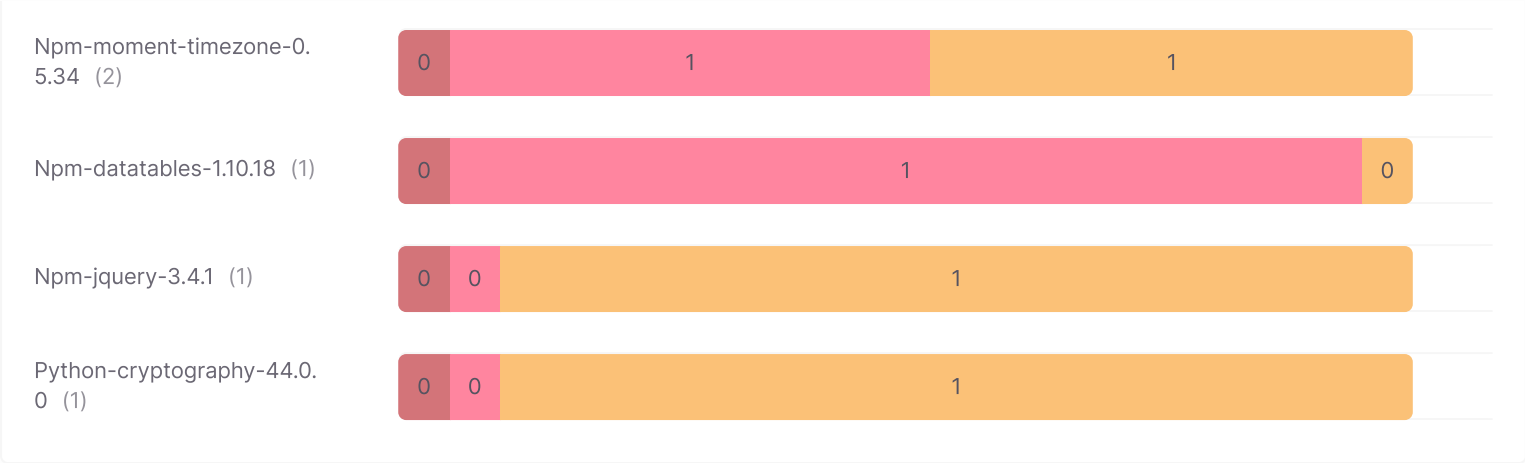
| | |
|---|--|
| <ul style="list-style-type: none">▪ Scan Id: 37e0b680-68a0-4916-b476-621508c41c6f▪ Scan Duration: 0h 2m 23s▪ Preset: ASA Premium▪ LOC Scanned: 1318486<ul style="list-style-type: none">▪ SAST: 657102▪ IaC: 661384▪ Files Scanned: 625<ul style="list-style-type: none">▪ SAST: 597▪ IaC: 28▪ Density: 0<ul style="list-style-type: none">▪ SAST: 0▪ IaC: 0▪ Initiator: songchai.du@bdms.co.th▪ Online Results: Link | <ul style="list-style-type: none">▪ Source Origin: zip▪ Main Branch: N/A▪ Scan Type: Full Scan▪ Scanned Branch Name: N/A▪ Groups: GLS Sec▪ Scanner Status:<ul style="list-style-type: none">▪ IaC: Completed▪ Containers: Completed▪ SAST: Completed▪ SCA: Completed |
|---|--|

Project & Scan Tags

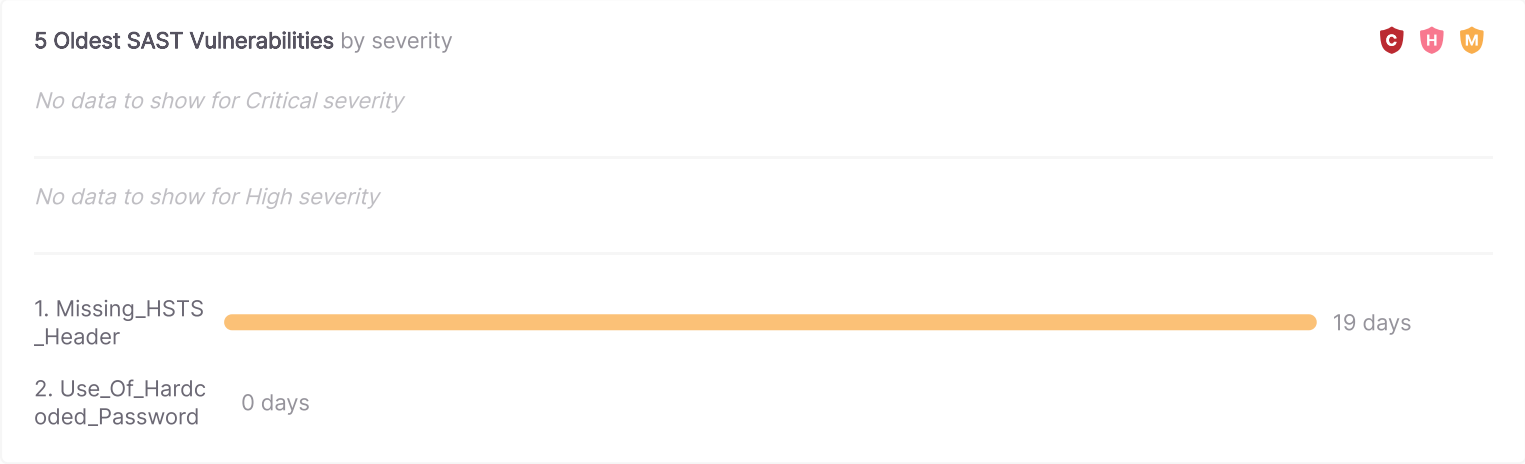
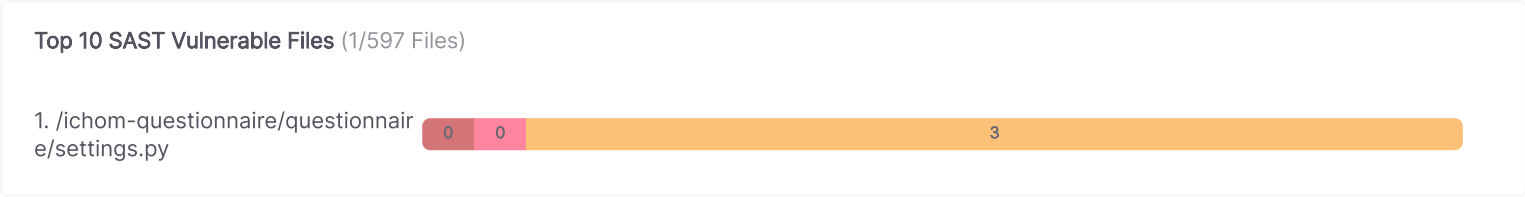
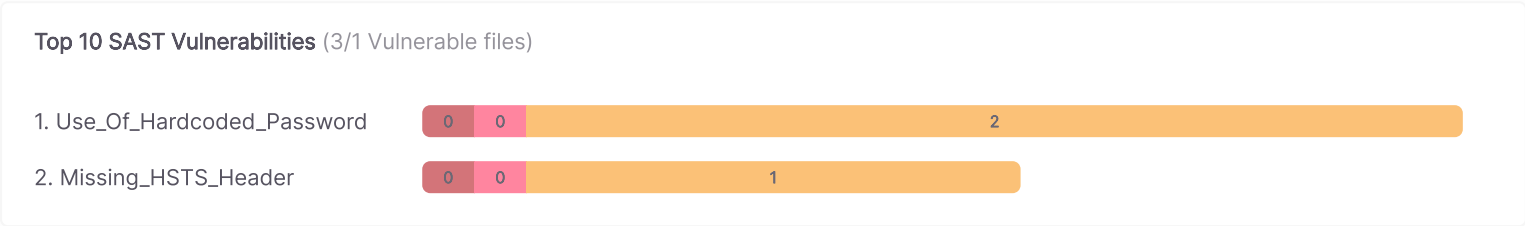
| |
|----------------------------------|
| <p>Project Tags:</p> <p>None</p> |
| <p>Scan Tags:</p> <p>None</p> |

Scan Results Overview





| By SAST Vulnerability | | | | |
|-----------------------|---|---|---|---|
| | Vulnerability Type | | | |
| | Use_Of_Hardcoded_Password In 1 Files | 0 | 0 | 2 |
| | Missing_HSTS_Header In 1 Files | 0 | 0 | 1 |
| | Total In 1 Files | 0 | 0 | 3 |



By Severity



SAST Scan Results (3)

Use_Of_Hardcoded_Password (Type)

Query Path: Python/Python_Medium_Threat/Use_Of_Hardcoded_Password

CWE Id: 259

Total results: 2

Description: The application uses the hard-coded password @SourceElement for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line @SourceLine of @SourceFile appears in the code, implying it is accessible to anyone with source code access, and cannot be changed without rebuilding the application.

Category:

- ASA Premium: ASA Premium
- ASD STIG 6.1: APSC-DV-001740 - CAT I The application must only store cryptographic representations of passwords.
- CWE top 25: CWE top 25
- FISMA 2014: Identification And Authentication
- MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
- NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
- OWASP ASVS: V02 Authentication
- OWASP Top 10 2021: A7-Identification and Authentication Failures
- OWASP Top 10 API: API2-Broken Authentication
- PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development
- SANS top 25: SANS top 25

Result 1 of 2

Medium • Link • New • To Verify • Similarity Id: -1531631419 • Found First: 08 Apr, 2025 • Found Last: 08 Apr, 2025
First Scan ID: 37e0b680-68a0-4916-b476-621508c41c6f

| Source | Destination |
|---|---|
| File Name: /ichom-questionnaire/questionnaire/settings.py | File Name: /ichom-questionnaire/questionnaire/settings.py |
| Method: | Method: |
| Element: "django-insecure-@6*(pt1&tgt1=kcg^po5kczbj(*!7n!rs-+4ajb*asao-c3%6i" | Element: "django-insecure-@6*(pt1&tgt1=kcg^po5kczbj(*!7n!rs-+4ajb*asao-c3%6i" |

Code Snippets

```
19 | SECRET_KEY = 'django-insecure-@6*(pt1&tgt1=kcg^po5kczbj(*!7n!rs-+4ajb*asao-c3%6i'
```

Result 2 of 2

Medium • [Link](#) • New • To Verify • Similarity Id: 923699815 • Found First: 08 Apr, 2025 • Found Last: 08 Apr, 2025
First Scan ID: 37e0b680-68a0-4916-b476-621508c41c6f

| | |
|--|---|
| Source File Name: /ichom-questionnaire/questionnaire/settings.py Method: Element: "CGi[]506uj9X" | Destination File Name: /ichom-questionnaire/questionnaire/settings.py Method: Element: "CGi[]506uj9X" |
| Code Snippets <div>122 'PASSWORD': 'CGi[]506uj9X',</div> | |

Missing_HSTS_Header (Type)

Query Path: [Python/Python_Medium_Threat/Missing_HSTS_Header](#)

CWE Id: [346](#)

Total results: 1

Description: The web-application does not define an HSTS header, leaving it vulnerable to attack.

Category:

- ASA Premium: [ASA Premium](#)
- OWASP ASVS: [V14 Configuration](#)
- OWASP Top 10 2021: [A7-Identification and Authentication Failures](#)
- OWASP Top 10 API 2023: [API8-Security Misconfiguration](#)
- PCI DSS v4.0: [PCI DSS \(4.0\) - 6.2.4 Vulnerabilities in software development](#)

Result 1 of 1

[Medium](#) • [Link](#) • [New](#) • [To Verify](#) • Similarity Id: [673611729](#) • Found First: [08 Apr, 2025](#) • Found Last: [08 Apr, 2025](#)
First Scan ID: [b7c5bceb-928b-4cad-a588-6100089a98aa](#)

Source

File Name: [/ichom-questionnaire/questionnaire/settings.py](#)
Method:
Element: [CxPYNS_7a6be4d4](#)

Destination

File Name: [/ichom-questionnaire/questionnaire/settings.py](#)
Method:
Element: [CxPYNS_7a6be4d4](#)

Code Snippets

1 |

laC Vulnerabilities

No data to show

laC Scan Results (0)

No data to show

SCA Vulnerabilities

By Severity



SCA Scan Results (15 Results)

Npm-datatables.net-1.10.19 (2 Results)

Package Name: [datatables.net](#)

Version: [1.10.19](#)

Total Results: 1

Category: [CWE-1321](#)
Total Results: 1

Result 1 of 1 - Vulnerability
High • New • To Verify • Outdated: yes • Found First: 08 Apr, 2025 • Found Last: 08 Apr, 2025 •
Result ID: hmMu6ZLu0VD+FwtpYBWzBeqKF/gmpY373wnHtKfvvw4= •
First Scan ID: 37e0b680-68a0-4916-b476-621508c41c6f

CVE: [CVE-2020-28458](#)
Description: All versions prior to version 1.10.23, and version 2.1.1 of packages [datatables.net](#) and [data tables](#) are vulnerable to Prototype Pollution due to an incomplete fix for <https://snyk.io/vuln/SNYK-JS-DATATABLESNET-598806>.
References: [Advisory](#) • [Commit](#) • [POC/Exploit](#) • [Vulnerable code](#)

Package Name: [datatables.net](#)

Version: [1.10.19](#)

Total Results: 1

Category: [CWE-79](#)
Total Results: 1

Result 1 of 1 - Vulnerability
Medium • New • To Verify • Outdated: yes • Found First: 08 Apr, 2025 • Found Last: 08 Apr, 2025 •
Result ID: CA0JWoDtL9NfVqD7DYchK9+D+zgxAI9jfaODT6Fwsf0= •
First Scan ID: 37e0b680-68a0-4916-b476-621508c41c6f

CVE: [CVE-2021-23445](#)
Description: A Cross-site Scripting (XSS) vulnerability affects the package [datatables.net](#) before 1.11.3 and 2.1.1. If an array is passed to the HTML escape entities function, it would not have its contents escaped.
References: [Advisory](#) • [Commit](#) • [Release Note](#)

Npm-moment-timezone-0.5.34 (2 Results)

Package Name: [moment-timezone](#)

Version: [0.5.34](#)

Total Results: 1

Category: [CWE-78](#)
Total Results: 1

Result 1 of 1 - Vulnerability

High • New • To Verify • Outdated: yes • Found First: 08 Apr, 2025 • Found Last: 08 Apr, 2025 •
Result ID: mNpDUNTcuBpHT0Vp+umJm1JLN0HE1arg8T1tmkI3/Cc= •
First Scan ID: 37e0b680-68a0-4916-b476-621508c41c6f

CVE: Cxb5e411c7-17b4
Description: Command Injection in "moment-timezone". This issue affects versions 0.1.0 prior to 0.5.35.
References: [Advisory](#) • [Commit](#) • [Release Note](#)

Package Name: moment-timezone

Version: 0.5.34

Total Results: 1

Category: [CWE-319](#)
Total Results: 1

Result 1 of 1 - Vulnerability

Medium • New • To Verify • Outdated: yes • Found First: 08 Apr, 2025 • Found Last: 08 Apr, 2025 •
Result ID: ASpFRmwK7tKn+b3vMipmX58OdKEXWJmL00y5egrv7Hw= •
First Scan ID: 37e0b680-68a0-4916-b476-621508c41c6f

CVE: Cx88793d01-c25f
Description: Cleartext Transmission of Sensitive Information in moment-timezone. This issue affects versions 0.1.0 through 0.5.34.
References: [Advisory](#) • [Commit](#) • [Release Note](#)

Npm-moment-2.24.0 (3 Results)

Package Name: moment

Version: 2.24.0

Total Results: 1

Category: [CWE-22](#)
Total Results: 1

Result 1 of 1 - Vulnerability

High • New • To Verify • Outdated: yes • Found First: 08 Apr, 2025 • Found Last: 08 Apr, 2025 •
Result ID: mkbcnk30oz2PG1sKLTccQ7tTJ6qWeIJk/B97js+GKco= •
First Scan ID: 37e0b680-68a0-4916-b476-621508c41c6f

CVE: CVE-2022-24785
Description: Moment.js is a JavaScript date library for parsing, validating, manipulating, and formatting dates. A path traversal vulnerability impacts npm (server) users of Moment.js between versions 1.0.1 and 2.29.1, especially if a user-provided locale string is directly used to switch moment locale. This problem is patched in 2.29.2, and the patch can be applied to all affected versions. As a workaround, sanitize the user-provided locale name before passing it to Moment.js.
References: [Advisory](#) • [Commit](#) • [Release Note](#)

Package Name: moment

Version: 2.24.0

Total Results: 2

Category: [CWE-1333](#)
Total Results: 2

Result 1 of 2 - Vulnerability

High • New • To Verify • Outdated: yes • Found First: 08 Apr, 2025 • Found Last: 08 Apr, 2025 •
Result ID: vSCu2FzZ/Zq3OrjGAd61XH6dwwyT7VWkOo3logdcD4c= •
First Scan ID: 37e0b680-68a0-4916-b476-621508c41c6f

CVE: CVE-2022-31129
Description: moment is a JavaScript date library for parsing, validating, manipulating, and formatting dates. Affected versions of moment were found to use an inefficient parsing algorithm. Specifically using string-to-date parsing in moment (more specifically rfc2822 parsing, which is tried by default) has quadratic (N^2) complexity on specific inputs. Users may notice a noticeable slowdown is observed with inputs above 10k characters. Users who pass user-provided strings without sanity length checks to moment constructor are vulnerable to (Re)DoS attacks. The problem is patched in 2.29.4, the patch can be applied to all affected versions with minimal tweaking. Users are advised to upgrade. Users unable to upgrade should consider limiting date lengths accepted from user input. This issue affects versions 2.18.0 through 2.29.3.
References: [Advisory](#) • [Commit](#) • [Pull request](#) • [Disclosure](#) • [Issue](#) • [Release Note](#)

Result 2 of 2 - Vulnerability

High • New • To Verify • Outdated: yes • Found First: 08 Apr, 2025 • Found Last: 08 Apr, 2025 •
Result ID: 9HtVZcRjgizMcrhwWjOqHukBJFR+XlowA+aVsijqZR8= •
First Scan ID: 37e0b680-68a0-4916-b476-621508c41c6f

CVE: Cx62f5bb1b-fa5e
Description: A Regular Expression Denial of Service (ReDoS) in moment 2.18 through 2.29.3 makes the server unavailable when a specially crafted input is provided to the default function "moment()", which nearly matches the pattern being matched. This will cause the regular expression matching to take a long time, all the while occupying the event loop and preventing it from processing other requests.
References: [Issue](#) • [Commit](#) • [Pull request](#) • [Advisory](#)

Npm-datatables-1.10.18 (1 Result)

Package Name: **datatables**
Version: 1.10.18
Total Results: 1

Category: [CWE-1321](#)
Total Results: 1

Result 1 of 1 - Vulnerability

High • New • To Verify • Outdated: no • Found First: 08 Apr, 2025 • Found Last: 08 Apr, 2025 •
Result ID: 9uxZdxKdCJNYjpZKB0vf+Q7GyUBeiHuAmxtlRWyeJ+8= •
First Scan ID: 37e0b680-68a0-4916-b476-621508c41c6f

CVE: CVE-2020-28458
Description: All versions prior to version 1.10.23, and version 2.1.1 of packages datatables.net and datatables are vulnerable to Prototype Pollution due to an incomplete fix for <https://snyk.io/vuln/SNYK-JS-DATATABLESNET-598806>.
References: [Advisory](#) • [Commit](#) • [POC/Exploit](#) • [Vulnerable code](#)

Python-Django-5.1.2 (5 Results)

Package Name: **Django**
Version: 5.1.2
Total Results: 3

Category: [CWE-770](#)
Total Results: 3

Result 1 of 3 - Vulnerability

High • New • To Verify • Outdated: yes • Found First: 08 Apr, 2025 • Found Last: 08 Apr, 2025 •
Result ID: kcPicRE3yyRIZ88d/w7mEY9q1itOEeCh7×9T/czE3fA= •
First Scan ID: 37e0b680-68a0-4916-b476-621508c41c6f

CVE: CVE-2024-53907
Description: An issue was discovered in Django versions 1.6.3 through 4.2.16, 5.0a1 through 5.0.9, and 5.1a1 through 5.1.3. The `strip_tags()` method and `striptags` template filter are subject to a potential Denial-of-service attack via certain inputs containing large sequences of nested incomplete HTML entities.
References: [Advisory](#) • [Advisory](#) • [Commit](#) • [Release Note](#) • [Mail Thread](#)

Result 2 of 3 - Vulnerability

Medium • New • To Verify • Outdated: yes • Found First: 08 Apr, 2025 • Found Last: 08 Apr, 2025 •
Result ID: W4MU5PnNp0xBOqvdX40/PJ8YTkmaKPM6U3VB9TbzSU= •
First Scan ID: 37e0b680-68a0-4916-b476-621508c41c6f

CVE: CVE-2025-26699
Description: An issue was discovered in Django versions 4.2.x prior to 4.2.20, 5.0.x prior to 5.0.13, 5.1.x prior to 5.1.7, 5.2.a1, and 5.2b1. The 'django.utils.text.wrap()' method and wordwrap template filter are subject to a potential Denial-of-Service (DoS) attack when used with very long strings.
References: [Advisory](#) • [Release Note](#) • [Mail Thread](#) • [Commit](#)

Result 3 of 3 - Vulnerability

Medium • New • To Verify • Outdated: yes • Found First: 08 Apr, 2025 • Found Last: 08 Apr, 2025 •
Result ID: XZ+WzBZqcBGeFv+HUBVslavno2v8F9t15EGrF7YVAvE= •
First Scan ID: 37e0b680-68a0-4916-b476-621508c41c6f

CVE: CVE-2024-56374
Description: An issue was discovered in Django 4.2.x prior to 4.2.18, 5.0.x prior to 5.0.11, and 5.1.x prior to 5.1.5. Lack of upper-bound limit enforcement in strings passed when performing IPv6 validation could lead to a potential denial-of-service attack. The undocumented and private functions `clean_ipv6_address` and `is_valid_ipv6_address` are vulnerable, as is the `django.forms.GenericIPAddressField` form field. (The `django.db.models.GenericIPAddressField` model field is not affected.)
References: [Advisory](#) • [Release Note](#) • [Commit](#) • [Blog Post](#)

Package Name: Django

Version: 5.1.2

Total Results: 1

Category: [CWE-1269](#)
Total Results: 1

Result 1 of 1 - Vulnerability

Critical • New • To Verify • Outdated: yes • Found First: 08 Apr, 2025 • Found Last: 08 Apr, 2025 •
Result ID: xyubqQ5KANOXJ6FV1mxOKwMRwVrp+J1Kv7uaOgxPyIM= •
First Scan ID: 37e0b680-68a0-4916-b476-621508c41c6f

CVE: CVE-2023-5457
Description: A CWE-1269 "Product Released in Non-Release Configuration" vulnerability in the Django web framework used by the web application (due to the "debug" configuration parameter set to "True") allows a remote unauthenticated attacker to access critical information and have other unspecified impacts to the confidentiality, integrity, and availability of the application. This issue affects all versions of Django if and only if the user makes the debug configuration to "True".
References: [Advisory](#) • [Advisory](#)

Package Name: Django

Version: 5.1.2

Total Results: 1

Category: [CWE-89](#)
Total Results: 1

Result 1 of 1 - Vulnerability

Critical • New • To Verify • Outdated: yes • Found First: 08 Apr, 2025 • Found Last: 08 Apr, 2025 •
Result ID: 6OpTMADq6BSJLQyi0MNsWP6EjX+/WkP0I+6U07FNGB0= •
First Scan ID: 37e0b680-68a0-4916-b476-621508c41c6f

CVE: [CVE-2024-53908](#)
Description: An issue was discovered in Django versions 3.1a1 through 4.2.16, 5.0a1 through 5.0.9, and 5.1a1 through 5.1.3. Direct usage of the ``django.db.models.fields.json.HasKey`` lookup, when an Oracle database is used, is subject to SQL injection if untrusted data is used as an ``lhs`` value. (Applications that use the ``jsonfield.has_key`` lookup via ``__`` are unaffected.)
References: [Advisory](#) • [Release Note](#) • [Commit](#) • [Advisory](#)

Npm-jquery-3.4.1 (1 Result)

Package Name: [jquery](#)
Version: [3.4.1](#)
Total Results: 1

Category: [CWE-79](#)
Total Results: 1

Result 1 of 1 - Vulnerability

Medium • New • To Verify • Outdated: yes • Found First: 08 Apr, 2025 • Found Last: 08 Apr, 2025 •
Result ID: J0Ue76LwAWhkXZue5FgBYqaSX9CU+3FUKCQceMgpFtU= •
First Scan ID: 37e0b680-68a0-4916-b476-621508c41c6f

CVE: [CVE-2020-11023](#)
Description: In jQuery versions 1.0.3 through 3.4.1, passing HTML containing `<option>` elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code. This vulnerability also affects jquery-rails versions through 4.3.5.
References: [Advisory](#) • [Release Note](#) • [Pull request](#) • [Commit](#) • [Commit](#) • [Pull request](#) • [Release Note](#) • [Commit](#) • [Issue](#)

Python-cryptography-44.0.0 (1 Result)

Package Name: [cryptography](#)
Version: [44.0.0](#)
Total Results: 1

Category: [CWE-392](#)
Total Results: 1

Result 1 of 1 - Vulnerability

Medium • New • To Verify • Outdated: yes • Found First: 08 Apr, 2025 • Found Last: 08 Apr, 2025 •

Result ID: sEkBG/HUPd72JmT5mwaPnFzsudPnm0G2CNDJAowigRM= •

First Scan ID: 37e0b680-68a0-4916-b476-621508c41c6f

CVE: CVE-2024-12797



Description: Clients using RFC7250 Raw Public Keys (RPKs) to authenticate a server may fail to notice that the server was not authenticated because handshakes don't abort as expected when the "SSL_VERIFY_PEER" verification mode is set. TLS and DTLS connections using raw public keys may be vulnerable to man-in-the-middle attacks when server authentication failure is not detected by clients. RPKs are disabled by default in both TLS clients and TLS servers. The issue only arises when TLS clients explicitly enable RPK use by the server, and the server likewise enables sending an RPK instead of an X.509 certificate chain. The affected clients are those that then rely on the handshake to fail when the server's RPK fails to match one of the expected public keys by setting the verification mode to "SSL_VERIFY_PEER." Clients that enable server-side raw public keys can still find out that raw public key verification failed by calling "SSL_get_verify_result()", and those that do and take appropriate action are not affected. This issue was introduced in the initial implementation of RPK support in OpenSSL 3.2. The FIPS modules in 3.4, 3.3, 3.2, 3.1, and 3.0 are not affected by this issue. This issue affects openssl versions 3.2.x prior to 3.2.4, 3.3.x prior to 3.3.3, and 3.4.x prior to 3.4.1. The versions of OpenSSL included in cryptography 42.0.0 through 44.0.0 are vulnerable to a security issue.




References: [Advisory](#) • [Commit](#) • [Mail Thread](#) • [Advisory](#) • [Commit](#) • [Release Note](#) • [Release Note](#) • [Pull request](#)




SAST Resolved Vulnerabilities




No data to show



Categories




| ASA Premium | | | |
|-------------|---|---|---|
| Category |  |  |  |
| ASA Premium | 0 | 0 | 3 |

| ASD STIG 6.1 | | | |
|--|---|---|---|
| Category |  |  |  |
| APSC-DV-001740 - CAT I The application must only store cryptographic representations of passwords. | 0 | 0 | 2 |




| CWE top 25 | | | |
|------------|---|---|---|
| Category |  |  |  |
| CWE top 25 | 0 | 0 | 2 |

| FISMA 2014 | | | |
|-----------------------------------|---|---|---|
| Category |  |  |  |
| Identification And Authentication | 0 | 0 | 2 |




| MOIS(KISA) Secure Coding 2021 | | | |
|-------------------------------|---|---|---|
| Category |  |  |  |
| MOIS(KISA) Security Functions | 0 | 0 | 2 |

| NIST SP 800-53 | | | |
|--|---|---|---|
| Category |  |  |  |
| SC-28 Protection of Information at Rest (P1) | 0 | 0 | 2 |




| OWASP ASVS | | | |
|------------|--|--|--|
|------------|--|--|--|

| Category |  |  |  |
|--------------------|--|--|--|
| V02 Authentication | 0 | 0 | 2 |
| V14 Configuration | 0 | 0 | 1 |




OWASP Top 10 2021

| Category |  |  |  |
|---|---|---|---|
| A7-Identification and Authentication Failures | 0 | 0 | 3 |




OWASP Top 10 API

| Category |  |  |  |
|----------------------------|---|---|---|
| API2-Broken Authentication | 0 | 0 | 2 |




OWASP Top 10 API 2023

| Category |  |  |  |
|--------------------------------|---|---|---|
| API8-Security Misconfiguration | 0 | 0 | 1 |

PCI DSS v4.0

| Category |  |  |  |
|---|---|---|---|
| PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development | 0 | 0 | 3 |

SANS top 25

| Category |  |  |  |
|-------------|---|---|---|
| SANS top 25 | 0 | 0 | 2 |

Use_Of_Hardcoded_Password (CWE 259)

What Is The Risk

Hardcoded passwords expose the application to password leakage. If an attacker gains access to the source code, she will be able to steal the embedded passwords, and use them to impersonate a valid user. This could include impersonating end users to the application, or impersonating the application to a remote system, such as a database or a remote web service. Once the attacker succeeds in impersonating the user or application, she will have full access to the system, and be able to do anything the impersonated identity could do.

What Can Cause It

The application codebase has string literal passwords embedded in the source code. This hardcoded value is used either to compare to user-provided credentials, or to authenticate downstream to a remote system (such as a database or a remote web service). An attacker only needs to gain access to the source code to reveal the hardcoded password. Likewise, the attacker can reverse engineer the compiled application binaries, and easily retrieve the embedded password. Once found, the attacker can easily use the password in impersonation attacks, either directly on the application or to the remote system. Furthermore, once stolen, this password cannot be easily changed to prevent further misuse, unless a new version of the application is compiled. Moreover, if this application is distributed to numerous systems, stealing the password from one system automatically allows a class break in to all the deployed systems.

General Recommendations

- * Do not hardcode any secret data in source code, especially not passwords.
 - * In particular, user passwords should be stored in a database or directory service, and protected with a strong password hash (e.g. bcrypt, scrypt, PBKDF2, or Argon2). Do not compare user passwords with a hardcoded value.
 - * Sytem passwords should be stored in a configuration file or the database, and protected with strong encryption (e.g. AES-256). Encryption keys should be securely managed, and not hardcoded.

Missing_HSTS_Header (CWE 346)

What Is The Risk

Failure to set an HSTS header and provide it with a reasonable "max-age" value of at least one year may leave users vulnerable to Man-in-the-Middle attacks.

What Can Cause It

Many users browse to websites by simply typing the domain name into the address bar, without the protocol prefix. The browser will automatically assume that the user's intended protocol is HTTP, instead of the encrypted HTTPS protocol. When this initial request is made, an attacker can perform a Man-in-the-Middle attack and manipulate it to redirect users to a malicious web-site of the attacker's choosing. To protect the user from such an occurence, the HTTP Strict Transport Security (HSTS) header instructs the user's browser to disallow use of an unsecure HTTP connection to the the domain associated with the HSTS header. Once a browser that supports the HSTS feature has visited a web-site and the header was set, it will no longer allow communicating with the domain over an HTTP connection. Once an HSTS header was issued for a specific website, the browser is also instructed to prevent users from manually overriding and accepting an untrusted SSL certificate for as long as the "max-age" value still applies. The recommended "max-age" value is for at least one year in seconds, or 31536000.

General Recommendations

- * Before setting the HSTS header - consider the implications it may have:
 - * Forcing HTTPS will prevent any future use of HTTP, which could hinder some testing
 - * Disabling HSTS is not trivial, as once it is disabled on the site, it must also be disabled on the browser
- * Set the HSTS header either explicitly within application code, or using web-server configurations.
- * Ensure the "max-age" value for HSTS headers is set to 31536000 to ensure HSTS is strictly enforced for at least one year.
- * Include the "includeSubDomains" to maximize HSTS coverage, and ensure HSTS is enforced on all sub-domains under the current domain
 - * Note that this may prevent secure browser access to any sub-domains that utilize HTTP; however, use of HTTP is very severe and highly discouraged, even for websites that do not contain any sensitive information, as their contents can still be tampered via Man-in-the-Middle attacks to phish users under the HTTP domain.
- * Once HSTS has been enforced, submit the web-application's address to an HSTS preload list - this will ensure that, even if a client is accessing the web-application for the first time (implying HSTS has not yet been set by the web-application), a browser that respects the HSTS preload list would still treat the web-application as if it had already issued an HSTS header. Note that this requires the server to have a trusted SSL certificate, and issue an HSTS header with a maxAge of 1 year (31536000)
- * Note that this query is designed to return one result per application. This means that if more than one vulnerable response without an HSTS header is identified, only the first identified instance of this issue will be highlighted as a result. If a misconfigured instance of HSTS is identified (has a short lifespan, or is missing the "includeSubDomains" flag), that result will be flagged. Since HSTS is required to be enforced across the entire application to be considered a secure deployment of HSTS functionality, fixing this issue only where the query highlights this result is likely to produce subsequent results in other sections of the application; therefore, when adding this header via code, ensure it is uniformly deployed across the entire application. If this header is added via configuration, ensure that this configuration applies to the entire application.
- * Note that misconfigured HSTS headers that do not contain the recommended max-age value of at least one year or the "includeSubDomains" flag will still return a result for a missing HSTS header.