

Scancrypt Vulnerability Report

Scan Report for: http://localhost:8081/jwt-none

Date: 2026-01-16 14:35:37

Executive Summary

Critical: 1

High: 1

Medium: 0

Low: 6

Info: 1

Detailed Findings

1. [Info] Technology Stack Disclosure

URL: http://localhost:8081/jwt-none

Description:

The application discloses specific technology versions via headers or default files, which aids attackers in finding known exploits.

Remediation:

Configure the server to suppress 'Server' and 'X-Powered-By' headers. Remove default welcome pages.

2. [High] Broken Access Control (BAC)

URL: http://localhost:8081/admin/dashboard

Param: path

Payload: /admin/dashboard

Description:

Unprivileged users can access restricted administrative pages.

Remediation:

Enforce strict role-based access control (RBAC) on all endpoints.

Fix Snippet:

```
# Python (Decorator)
@requires_role('admin')
def admin_dashboard():
    ...
```

Scancrypt Vulnerability Report

3. [Low] Unknown Issue

URL: http://localhost:8081/jwt-none

Param: auth_token

Payload: *JWT Deteced*

Description:

Remediation:

4. [Critical] Insecure JWT (Alg: None)

URL: http://localhost:8081/jwt-none

Param: auth_token

Payload: *eyJhbGciOiJub25lbn0.eyJ1c2VyljoiYWRtaW4ifQ.*

Description:

The application allows JSON Web Tokens with 'alg': 'none', which bypasses signature verification.

Remediation:

Enforce strong algorithms (RS256/HS256) and reject 'none' algorithm.

Fix Snippet:

```
# Python (PyJWT)
payload = jwt.decode(token, key, algorithms=["HS256"])
# Never use verify=False or allow 'none'
```

5. [Low] Missing Security Header

URL: http://localhost:8081/jwt-none

Description:

The application is missing common HTTP security headers that provide protection against attacks like Clickjacking and XSS.

Remediation:

Configure the web server to send strict security headers (CSP, HSTS, X-Frame-Options).

6. [Low] Missing Security Header

URL: http://localhost:8081/jwt-none

Description:

The application is missing common HTTP security headers that provide protection against attacks like Clickjacking and XSS.

Remediation:

Scancrypt Vulnerability Report

Configure the web server to send strict security headers (CSP, HSTS, X-Frame-Options).

7. [Low] Missing Security Header

URL: http://localhost:8081/jwt-none

Description:

The application is missing common HTTP security headers that provide protection against attacks like Clickjacking and XSS.

Remediation:

Configure the web server to send strict security headers (CSP, HSTS, X-Frame-Options).

8. [Low] Missing Security Header

URL: http://localhost:8081/jwt-none

Description:

The application is missing common HTTP security headers that provide protection against attacks like Clickjacking and XSS.

Remediation:

Configure the web server to send strict security headers (CSP, HSTS, X-Frame-Options).

9. [Low] Insecure Cookie Flags

URL: http://localhost:8081/jwt-none

Param: auth_token

Description:

Sensitive cookies are missing 'Secure', 'HttpOnly', or 'SameSite' flags.

Remediation:

Set Secure=True, HttpOnly=True, and SameSite=Strict/Lax for all session cookies.

Fix Snippet:

```
# Python (Flask)
response.set_cookie('session', value, secure=True, httponly=True, samesite='Lax')
```
