Scancrypt Vulnerability Report

Scan Report for: http://localhost:8081

Date: 2026-01-16 14:42:57

Executive Summary

Critical: 6

High: 5

Medium: 2

Low: 67

Info: 12

Detailed Findings

1. [Info] Technology Stack Disclosure

URL: http://localhost:8081/rce?cmd=echo 'hello'

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. [Low] Unknown Issue

URL: http://localhost:8081/rce?cmd=echo 'hello'

Param: cmd

Payload: *; echo 'sc_rce_test'*

Description:

Remediation:

---

3. [High] Broken Access Control (BAC)

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

Scancrypt Vulnerability Report

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():
    ...
```

---

4. [Low] Missing Security Header

URL: http://localhost:8081/rce?cmd=echo 'hello'

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).

---

5. [Low] Missing Security Header

URL: http://localhost:8081/rce?cmd=echo 'hello'

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/rce?cmd=echo 'hello'

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).

Scancrypt Vulnerability Report

7. [Low] Missing Security Header

URL: http://localhost:8081/rce?cmd=echo 'hello'

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] Insecure Cookie Flags

URL: http://localhost:8081/rce?cmd=echo 'hello'

Param: session_id

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')
```

---

9. [Info] Technology Stack Disclosure

URL: http://localhost:8081/lfi?file=test.txt

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.

---

10. [Critical] Local File Inclusion (LFI)

URL: http://localhost:8081/lfi?file=test.txt

Param: file

Payload: *../../../../etc/passwd*

Description:

The application allows reading arbitrary files from the server via path traversal sequences.

Remediation:

Validate user input against a whitelist of permitted filenames. Disable 'allow_url_include' in PHP.

Scancrypt Vulnerability Report

11. [Critical] Local File Inclusion (LFI)

URL: http://localhost:8081/lfi?file=test.txt

Param: file

Payload: *../../../../windows/win.ini*

Description:

The application allows reading arbitrary files from the server via path traversal sequences.

Remediation:

Validate user input against a whitelist of permitted filenames. Disable 'allow_url_include' in PHP.

---

12. [Critical] Local File Inclusion (LFI)

URL: http://localhost:8081/lfi?file=test.txt

Param: file

Payload: *....//....//....//etc/passwd*

Description:

The application allows reading arbitrary files from the server via path traversal sequences.

Remediation:

Validate user input against a whitelist of permitted filenames. Disable 'allow_url_include' in PHP.

---

13. [Low] Missing Security Header

URL: http://localhost:8081/lfi?file=test.txt

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).

---

14. [Low] Missing Security Header

URL: http://localhost:8081/lfi?file=test.txt

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).

---

15. [Low] Missing Security Header

URL: http://localhost:8081/lfi?file=test.txt

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).

---

16. [Low] Missing Security Header

URL: http://localhost:8081/lfi?file=test.txt

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).

---

17. [Low] Insecure Cookie Flags

URL: http://localhost:8081/lfi?file=test.txt

Param: session_id

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')
```

---

18. [Info] Technology Stack Disclosure

URL: http://localhost:8081/cookie-insecure

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.

---

19. [Low] Missing Security Header

URL: http://localhost:8081/cookie-insecure

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).

---

20. [Low] Missing Security Header

URL: http://localhost:8081/cookie-insecure

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).

---

21. [Low] Missing Security Header

URL: http://localhost:8081/cookie-insecure

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).

---

22. [Low] Missing Security Header

URL: http://localhost:8081/cookie-insecure

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).

---

23. [Low] Insecure Cookie Flags

URL: http://localhost:8081/cookie-insecure

Param: session_id

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')
```

---

24. [Info] Technology Stack Disclosure

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

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.

---

25. [Low] Missing Security Header

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

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).

---

26. [Low] Missing Security Header

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

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).

---

27. [Low] Missing Security Header

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

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).

---

28. [Low] Missing Security Header

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

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).

---

29. [Low] Insecure Cookie Flags

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

Param: session_id

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')
```

---

30. [Info] Technology Stack Disclosure

URL: http://localhost:8081/blind_rce?cmd=echo 'test'

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.

---

31. [Critical] Blind Remote Code Execution

URL: http://localhost:8081/blind_rce?cmd=echo 'test'

Param: cmd

Payload: *; sleep 5*

Description:

The application executes system commands but does not return the output. Detected via time delays.

Remediation:
Avoid using system calls. Validate input strictly against a whitelist.

---

32. [Low] Missing Security Header

URL: http://localhost:8081/blind_rce?cmd=echo 'test'

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).

---

33. [Low] Missing Security Header

URL: http://localhost:8081/blind_rce?cmd=echo 'test'

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).

---

34. [Low] Missing Security Header

URL: http://localhost:8081/blind_rce?cmd=echo 'test'

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).

---

35. [Low] Missing Security Header

URL: http://localhost:8081/blind_rce?cmd=echo 'test'

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).

Scancrypt Vulnerability Report

36. [Low] Insecure Cookie Flags

URL: http://localhost:8081/blind_rce?cmd=echo 'test'

Param: session_id

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')
```

---

37. [Info] Technology Stack Disclosure

URL: http://localhost:8081/csti?search=vue

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.

---

38. [Low] Unknown Issue

URL: http://localhost:8081/csti?search=vue

Param: search

Payload: *; echo 'sc_rce_test'*

Description:

Remediation:

---

39. [High] Client-Side Template Injection (CSTI)

URL: http://localhost:8081/csti?search=vue

Param: search

Payload: *{{7*7}}*

Description:

The application reflects user input that is interpreted by client-side frameworks (Angular, Vue).

Remediation:

Escape user input before embedding it in templates. Use 'ng-non-bindable' or 'v-pre'.

---

40. [Medium] Reflected Cross-Site Scripting (XSS)

URL: http://localhost:8081/csti?search=vue

Param: search

Payload: *<sc_test>*

Description:

The application reflects untrusted data in a web page without proper validation or escaping, allowing execution of malicious scripts.

Remediation:

Context-aware output encoding (escaping) of all user input before rendering it in the browser.

Fix Snippet:

```
# Python (Jinja2) - Auto-escapes by default
{{ user_input }}

# JavaScript (React) - Safe by default
<div>{userInput}</div>
```

---

41. [Low] Missing Security Header

URL: http://localhost:8081/csti?search=vue

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).

---

42. [Low] Missing Security Header

URL: http://localhost:8081/csti?search=vue

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).

---

43. [Low] Missing Security Header

URL: http://localhost:8081/csti?search=vue

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).

---

44. [Low] Missing Security Header

URL: http://localhost:8081/csti?search=vue

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).

---

45. [Low] Insecure Cookie Flags

URL: http://localhost:8081/csti?search=vue

Param: session_id

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')
```

---

46. [Info] Technology Stack Disclosure

URL: http://localhost:8081/sqli?id=1

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.

---

47. [Low] Missing Security Header

URL: http://localhost:8081/sqli?id=1

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).

---

48. [Low] Missing Security Header

URL: http://localhost:8081/sqli?id=1

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).

---

49. [Low] Missing Security Header

URL: http://localhost:8081/sqli?id=1

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).

---

50. [Low] Missing Security Header

URL: http://localhost:8081/sqli?id=1

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).

---

51. [Low] Insecure Cookie Flags

URL: http://localhost:8081/sqli?id=1

Param: session_id

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')
```

---

52. [Info] Technology Stack Disclosure

URL: http://localhost:8081/cors

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.

---

53. [High] CORS Misconfiguration (Insecure Origin)

URL: http://localhost:8081/cors

Payload: *Origin: http://evil-scanner.com*

Description:

The application accepts arbitrary origins (Access-Control-Allow-Origin: * or null), allowing attackers to steal data.

Remediation:

Whiltelist trusted origins. Do not reflect the 'Origin' header blindly.

---

54. [Low] Missing Security Header

URL: http://localhost:8081/cors

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).

---

55. [Low] Missing Security Header

URL: http://localhost:8081/cors

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).

---

56. [Low] Missing Security Header

URL: http://localhost:8081/cors

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).

---

57. [Low] Missing Security Header

URL: http://localhost:8081/cors

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).

---

58. [Low] Insecure Cookie Flags

URL: http://localhost:8081/cors

Param: session_id

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')
```

---

59. [Info] Technology Stack Disclosure

URL: http://localhost:8081/api/user/100

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.

---

60. [High] Broken Object Level Authorization (BOLA/IDOR)

URL: http://localhost:8081/api/user/100

Param: path

Payload: *101*

Description:

The application allows access to objects belonging to other users by manipulating IDs.

Remediation:

Implement proper authorization checks for every object access.

Fix Snippet:

```
# Python (Secure)
if document.owner_id != current_user.id:
    abort(403, "Access Denied")
```

---

61. [Low] Missing Security Header

URL: http://localhost:8081/api/user/100

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).

---

62. [Low] Missing Security Header

URL: http://localhost:8081/api/user/100

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).

---

63. [Low] Missing Security Header

URL: http://localhost:8081/api/user/100

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).

---

64. [Low] Missing Security Header

URL: http://localhost:8081/api/user/100

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).

---

65. [Low] Insecure Cookie Flags

URL: http://localhost:8081/api/user/100

Param: session_id

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')
```

---

66. [Info] Technology Stack Disclosure

URL: http://localhost:8081/ssti?name=Guest

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.

---

67. [Low] Unknown Issue

URL: http://localhost:8081/ssti?name=Guest

Param: name

Payload: *; echo 'sc_rce_test'*

Description:

Remediation:

---

68. [Critical] Server-Side Template Injection (SSTI)

URL: http://localhost:8081/ssti?name=Guest

Param: name

Payload: *${{7*7}}*

Description:

The application blindly processes user input inside a template engine. This often leads to RCE.

Remediation:

Do not pass user input directly to templates. Use a 'Sandboxed' environment.

---

69. [High] Client-Side Template Injection (CSTI)

URL: http://localhost:8081/ssti?name=Guest

Param: name

Payload: *{{1+1}}*

Description:

The application reflects user input that is interpreted by client-side frameworks (Angular, Vue).

Remediation:

Escape user input before embedding it in templates. Use 'ng-non-bindable' or 'v-pre'.

---

70. [Medium] Reflected Cross-Site Scripting (XSS)

URL: http://localhost:8081/ssti?name=Guest

Param: name

Payload: *<sc_test>*

Description:

The application reflects untrusted data in a web page without proper validation or escaping, allowing execution of malicious scripts.

Remediation:

Context-aware output encoding (escaping) of all user input before rendering it in the browser.

Fix Snippet:

```
# Python (Jinja2) - Auto-escapes by default
{{ user_input }}

# JavaScript (React) - Safe by default
<div>{userInput}</div>
```

---

71. [Low] Missing Security Header

URL: http://localhost:8081/ssti?name=Guest

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).

---

72. [Low] Missing Security Header

URL: http://localhost:8081/ssti?name=Guest

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).

---

73. [Low] Missing Security Header

URL: http://localhost:8081/ssti?name=Guest

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).

---

74. [Low] Missing Security Header

URL: http://localhost:8081/ssti?name=Guest

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).

---

75. [Low] Insecure Cookie Flags

URL: http://localhost:8081/ssti?name=Guest

Param: session_id

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')
```

---

76. [Info] Technology Stack Disclosure

URL: http://localhost:8081

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.

---

77. [Low] Sensitive Data Exposure

URL: http://localhost:8081

Description:

The application exposes sensitive information (emails, keys, passwords) in its responses.

Remediation:

Ensure sensitive data is not returned in API responses or HTML comments. Use generic error messages.

---

78. [Low] Sensitive Data Exposure

URL: http://localhost:8081

Description:

The application exposes sensitive information (emails, keys, passwords) in its responses.

Remediation:

Ensure sensitive data is not returned in API responses or HTML comments. Use generic error messages.

---

79. [Low] Missing Security Header

URL: http://localhost:8081

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).

---

80. [Low] Missing Security Header

URL: http://localhost:8081

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).

---

81. [Low] Missing Security Header

URL: http://localhost:8081

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).

---

82. [Low] Missing Security Header

URL: http://localhost:8081

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).

---

83. [Low] Insecure Cookie Flags

URL: http://localhost:8081

Param: session_id

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')
```

---

84. [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.

---

85. [Low] Unknown Issue

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

Param: auth_token

Payload: *JWT Deteced*

Description:

Remediation:

---

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

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

Param: auth_token

Payload: *eyJhbGciOiJub25lIn0.eyJ1c2VyIjoiYWRtaW4ifQ.*

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'
```

---

87. [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).

---

88. [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).

---

89. [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).

---

90. [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).

---

91. [Low] Insecure Cookie Flags

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

Param: session_id

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')
```

---

92. [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')
```
