Scancrypt Vulnerability Report

Scan Report for: http://localhost:8081

Date: 2026-01-16 04:09:47

Executive Summary

Critical: 4

High: 2

Medium: 3

Low: 27

Info: 6

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

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

Param: cmd

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.

---

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).

---

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. [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.

---

9. [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.

---

10. [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.

---

11. [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.

---

12. [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).

---

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. [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.

---

17. [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.

---

18. [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).

---

19. [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).

---

20. [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).

---

21. [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).

---

22. [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.

---

23. [Low] Unknown Issue

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

Param: name

Payload: *; echo 'sc_rce_test'*

Description:

Remediation:

---

24. [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.

25. [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.

26. [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).

27. [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).

28. [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).

29. [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).

---

30. [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.

---

31. [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.

---

32. [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).

---

33. [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).

---

34. [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).

---

35. [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).

---

36. [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.

---

37. [High] SQL Injection

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

Param: id

Payload: '

Description:

The application allows untrusted user input to interfere with a database query. This could allow an attacker to view, modify, or delete data.

Remediation:

Use parameterized queries (Prepared Statements) for all database access. Validate and sanitize all user input.

---

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

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

Param: id

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.

---

39. [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).

---

40. [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).

---

41. [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).

---

42. [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).