

# Scancrypt Vulnerability Report

## Scan Report for: http://localhost:8081

Date: 2026-01-16 13:23:56

### Executive Summary

Critical: 6

High: 6

Medium: 3

Low: 40

Info: 9

### Detailed Findings

#### 1. [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.

---

#### 2. [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:**

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

---

#### 3. [Low] Missing Security Header

**URL:** http://localhost:8081/cors

**Description:**

# Scancrypt Vulnerability Report

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).

---

## 4. [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).

---

## 5. [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).

---

## 6. [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).

---

## 7. [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.

---

# Scancrypt Vulnerability Report

## 8. [Low] Unknown Issue

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

**Param:** name

**Payload:** ; echo 'sc\_rce\_test'

**Description:**

**Remediation:**

---

## 9. [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.

---

## 10. [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'.

---

## 11. [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.

# Scancrypt Vulnerability Report

## 12. [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).

---

## 13. [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).

---

## 14. [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).

---

## 15. [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).

---

## 16. [Info] Technology Stack Disclosure

**URL:** http://localhost:8081/auth/secret?id=1

**Description:**

# Scancrypt Vulnerability Report

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

**URL:** http://localhost:8081/auth/secret?id=1

**Param:** id

**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.

---

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

**URL:** http://localhost:8081/auth/secret?id=1

**Param:** id

**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'.

---

## 19. [Low] Missing Security Header

**URL:** http://localhost:8081/auth/secret?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).

---

## 20. [Low] Missing Security Header

**URL:** http://localhost:8081/auth/secret?id=1

**Description:**

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

# Scancrypt Vulnerability Report

**Remediation:**

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

---

## 21. [Low] Missing Security Header

**URL:** http://localhost:8081/auth/secret?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).

---

## 22. [Low] Missing Security Header

**URL:** http://localhost:8081/auth/secret?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).

---

## 23. [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.

---

## 24. [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.

---

## 25. [Low] Missing Security Header

# Scancrypt Vulnerability Report

**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).

---

## 26. [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).

---

## 27. [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).

---

## 28. [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).

---

## 29. [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.

# Scancrypt Vulnerability Report

**Remediation:**

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

---

## 30. [Low] Unknown Issue

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

**Param:** search

**Payload:** ; echo 'sc\_rce\_test'

**Description:****Remediation:**

---

## 31. [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'.

---

## 32. [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.

---

## 33. [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.



# Scancrypt Vulnerability Report

**Remediation:**

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

---

## 34. [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).

---

## 35. [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).

---

## 36. [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).

---

## 37. [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.

---

# Scancrypt Vulnerability Report

## 38. [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.

---

## 39. [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.

---

## 40. [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.

---

## 41. [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).

---

# Scancrypt Vulnerability Report

## 42. [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).

---

## 43. [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).

---

## 44. [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).

---

## 45. [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.

---

## 46. [Critical] Blind Remote Code Execution

**URL:** http://localhost:8081/blind\_rce?cmd=echo 'test'

**Param:** cmd

**Payload:** ; sleep 5

# Scancrypt Vulnerability Report

**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.

---

**47. [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).

---

**48. [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).

---

**49. [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).

---

**50. [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

## 51. [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.

---

## 52. [Low] Unknown Issue

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

**Param:** cmd

**Payload:** ; echo 'sc\_rce\_test'

**Description:**

**Remediation:**

---

## 53. [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).

---

## 54. [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).

---

## 55. [Low] Missing Security Header

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

# Scancrypt Vulnerability Report

**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/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).

---

## 57. [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.

---

## 58. [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.

---

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

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

**Param:** id

**Payload:** {{7\*7}}

# Scancrypt Vulnerability Report

**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'.

---

## 60. [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.

---

## 61. [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).

---

## 62. [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).

---

## 63. [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.

# Scancrypt Vulnerability Report

**Remediation:**

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

---

## 64. [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).

---