Web Application Vulnerability Assessment Report

Intern Name : SHREYA SHARMA

Target Application : OWASP Juice-shop

Host OS : Kali Linux

Tools used : OWASP ZAP

Track Code: TASK 01

Executive Summary

This report outlines the vulnerabilities identified through an automated security scan using OWASP ZAP. The goal is to uncover weaknesses that align with the OWASP Top 10 and suggest actionable mitigation strategies. The assessment was conducted on:

- `http://127.0.0.1:42000` (main target)
- `http://cdnjs.cloudflare.com` (external JS library source)

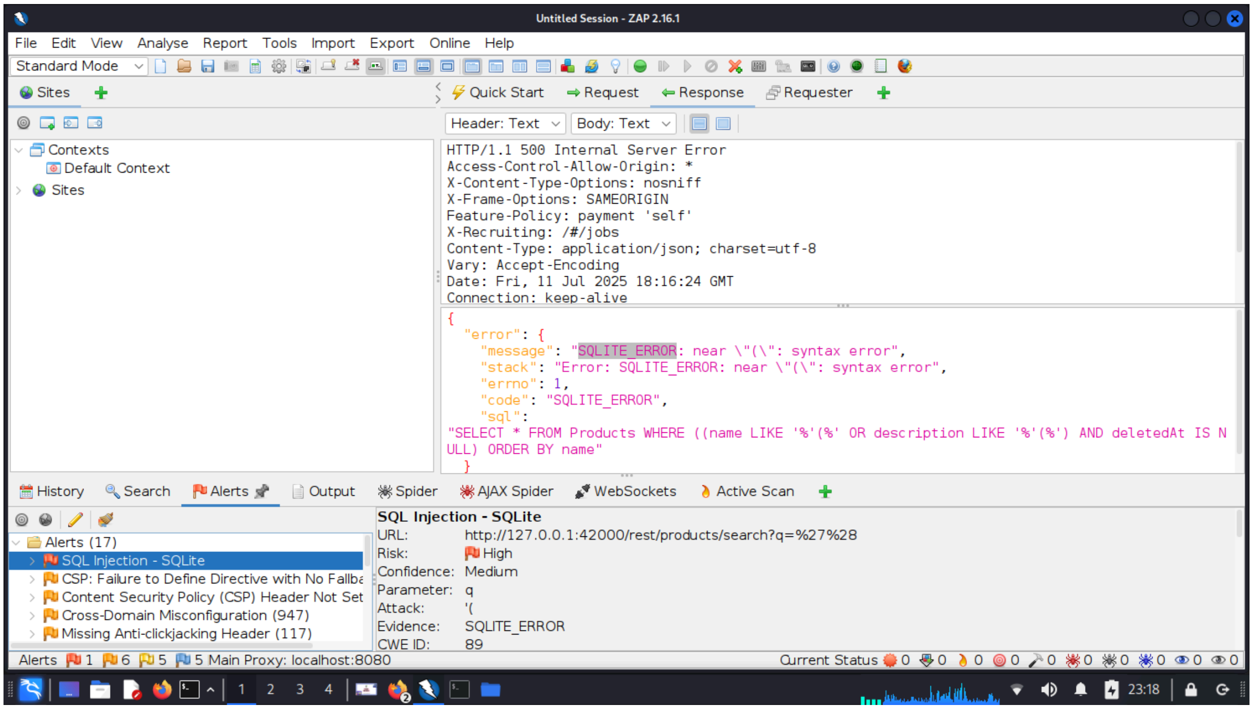
1. SQL Injection (SQLite)

- **Risk Level**: High
- **Confidence**: Medium
- **URL**: `GET /rest/products/search?q=%27%28`
- **OWASP Mapping**: A1:2021 - Injection

Description:

User-controlled input is not properly sanitized before being passed into an SQL query, enabling potential SQL Injection attacks.

Screenshot Placeholder:



```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
Date: Fri, 11 Jul 2025 18:16:24 GMT
Connection: keep-alive
```

```
{
  "error": {
    "message": "SQLITE_ERROR: near \"(\": syntax error",
    "stack": "Error: SQLITE_ERROR: near \"(\": syntax error",
    "errno": 1,
    "code": "SQLITE_ERROR",
    "sql":
"SELECT * FROM Products WHERE ((name LIKE '%'(%' OR description LIKE '%'(%') AND deletedAt IS N
ULL) ORDER BY name"
  }
```

Alerts (17)
- SQL Injection - SQLite
- CSP: Failure to Define Directive with No Fallba
- Content Security Policy (CSP) Header Not Set
- Cross-Domain Misconfiguration (947)
- Missing Anti-clickjacking Header (117)

SQL Injection - SQLite
URL: http://127.0.0.1:42000/rest/products/search?q=%27%28
Risk: High
Confidence: Medium
Parameter: q
Attack: '(
Evidence: SQLITE_ERROR
CWE ID: 89

Alerts 1 6 5 5 Main Proxy: localhost:8080 Current Status 0 0 0 0 0 0 0 0 0 0

Mitigation:

- Use parameterized queries (PreparedStatements)
- Implement input validation and output encoding
- Apply WAF (Web Application Firewall) protection where possible

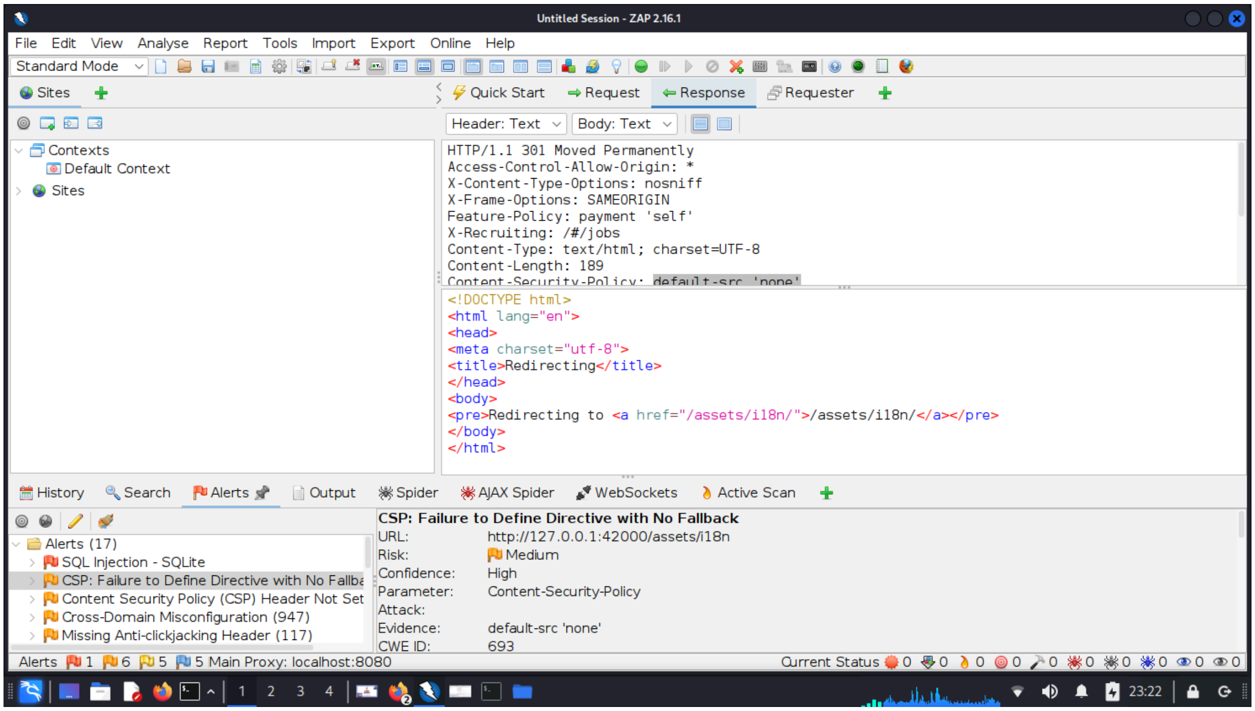
2. Content Security Policy (CSP) Header Not Set

- **Risk Level**: Medium
- **Confidence**: High
- **URL**: `GET /http://127.0.0.1:42000`

Description:

Lack of a CSP allows attackers to inject malicious scripts, increasing risk of XSS or data theft.

Screenshot Placeholder:


Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Contexts
Default Context
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
History
Search
Alerts
Output
Spider
AJAX Spider
WebSockets
Active Scan
Alerts (17)
SQL Injection - SQLite
CSP: Failure to Define Directive with No Fallba
Content Security Policy (CSP) Header Not Set
Cross-Domain Misconfiguration (947)
Missing Anti-clickjacking Header (117)
Alerts 1 6 5 5 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0
1 2 3 4
23:22

```
HTTP/1.1 301 Moved Permanently
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/html; charset=UTF-8
Content-Length: 189
Content-Security-Policy: default-src 'none'
```

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Redirecting</title>
</head>
<body>
<pre>Redirecting to <a href="/assets/i18n/">/assets/i18n/</a></pre>
</body>
</html>
```

CSP: Failure to Define Directive with No Fallback

```
URL:           http://127.0.0.1:42000/assets/i18n
Risk:          Medium
Confidence:    High
Parameter:     Content-Security-Policy
Attack:
Evidence:      default-src 'none'
CWE ID:        693
```

Mitigation:

Add a strong CSP header

OWASP Mapping:

- A5:2021 - Security Misconfiguration
- A7:2021 - Identification and Authentication Failures

3. Session ID in URL Rewrite

- **Risk Level**: Medium
- **Confidence**: High
- **URL**: `/socket.io/?EIO=4...&sid=Rmeo5AxtjmYn02qQAAAE`

Description:

Session IDs in URLs may be logged, cached, or leaked through referrer headers, exposing user sessions.

Mitigation:

- Use cookies (with `HttpOnly` and `Secure` flags) to store session IDs
- Avoid URL-based session management entirely

OWASP Mapping:

- A2:2021 - Broken Authentication

4. Vulnerable JS Library (jQuery 2.2.4)

- **Risk Level**: Medium
- **Confidence**: Medium
- **URL**: `GET https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js`

Description:

Old version of jQuery contains known vulnerabilities that could be exploited through XSS or DOM-based attacks.

Mitigation:

Upgrade to the latest secure version of jQuery, preferably from a trusted CDN.

OWASP Mapping:

- A6:2021 - Vulnerable and Outdated Components

5. Missing Anti-clickjacking Header

- **Risk Level**: Medium
- **Confidence**: Medium
- **URL**: `POST /socket.io/?EIO=4...`

Description:

Absence of the `X-Frame-Options` header makes the site vulnerable to clickjacking attacks.

OWASP Top 10 Coverage

OWASP Category	Covered	Notes
A1:2021 - Broken Access Control	✘	Not detected in scan
A2:2021 - Cryptographic Failures	✘	Not detected
A3:2021 - Injection	✔	SQL Injection vulnerability found
A4:2021 - Insecure Design	✘	Not tested
A5:2021 - Security Misconfiguration	✔	Missing CSP, X-Frame-Options
A6:2021 - Vulnerable Components	✔	Outdated jQuery library
A7:2021 - Identification Failures	✔	Session ID in URL
A8:2021 - Software/Data Integrity Failures	✘	Not detected

A9:2021 - Logging and Monitoring	✘	Not assessed
A10:2021 - SSRF	✘	Not detected

Conclusion

The scan identified critical injection vulnerabilities, missing headers, and use of outdated libraries. Prompt remediation will enhance the app's security posture and align with best practices.