Web Application Security Testing – Task 1 Report

Cyber Security Internship – Future Interns
Intern Name: *Ankit Bhoya*
Track: Cyber Security (CS)
Task: Web Application Security Testing
Date: *nov 2025*

---

1. Introduction

The objective of this task was to perform **Web Application Security Testing** on a vulnerable web application to identify potential security risks and weaknesses. The assessment was conducted to understand how attackers exploit web vulnerabilities and how such issues can be mitigated to protect real-world applications. This task aligns with the **OWASP Top 10 Web Application Security Risks**.

---

2. Tools Used

Tool	Purpose
OWASP ZAP	Automated scanning & manual testing
Burp Suite	Intercepting and modifying HTTP requests
Browser Developer Tools	Inspecting web elements & responses
GitHub	Documentation & version control

---

3. Target Application

Application Tested: *OWASP Juice Shop*
This application is intentionally vulnerable and used for practicing ethical hacking techniques in a safe environment.

---

4. Testing Methodology

1. **Reconnaissance:** Understanding application structure and endpoints
2. **Scanning:** Automated scanning using OWASP ZAP
3. **Manual Testing:** Attempting exploitation of discovered vulnerabilities

4. **Documentation:** Recording findings with screenshots and remediation steps

---

5. Vulnerabilities Identified

5.1 SQL Injection

- **Description:** The application failed to validate user inputs in SQL queries.
- **Impact:** Attackers can extract or modify sensitive database data.
- **Recommendation:** Use parameterized queries and input sanitization.

5.2 Cross-Site Scripting (XSS)

- **Description:** The application reflected user input directly to the browser without encoding.
- **Impact:** Allows execution of malicious scripts in victim browser sessions.
- **Recommendation:** Implement output encoding and proper input validation.

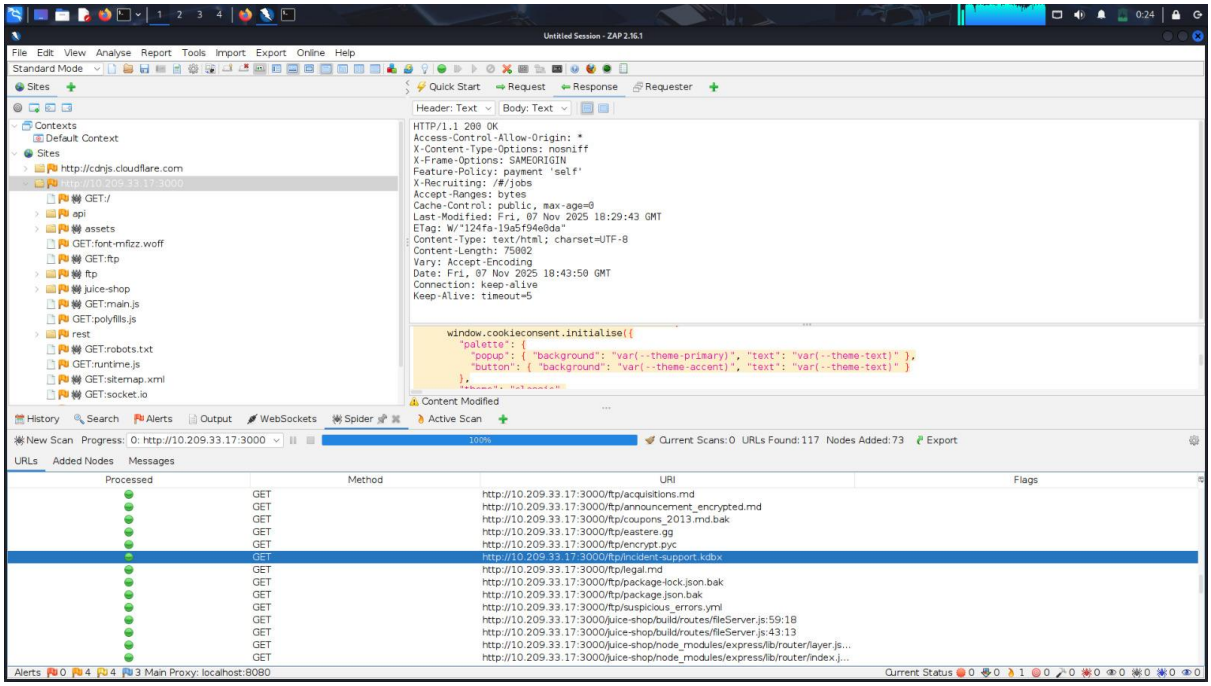
5.3 Broken Authentication

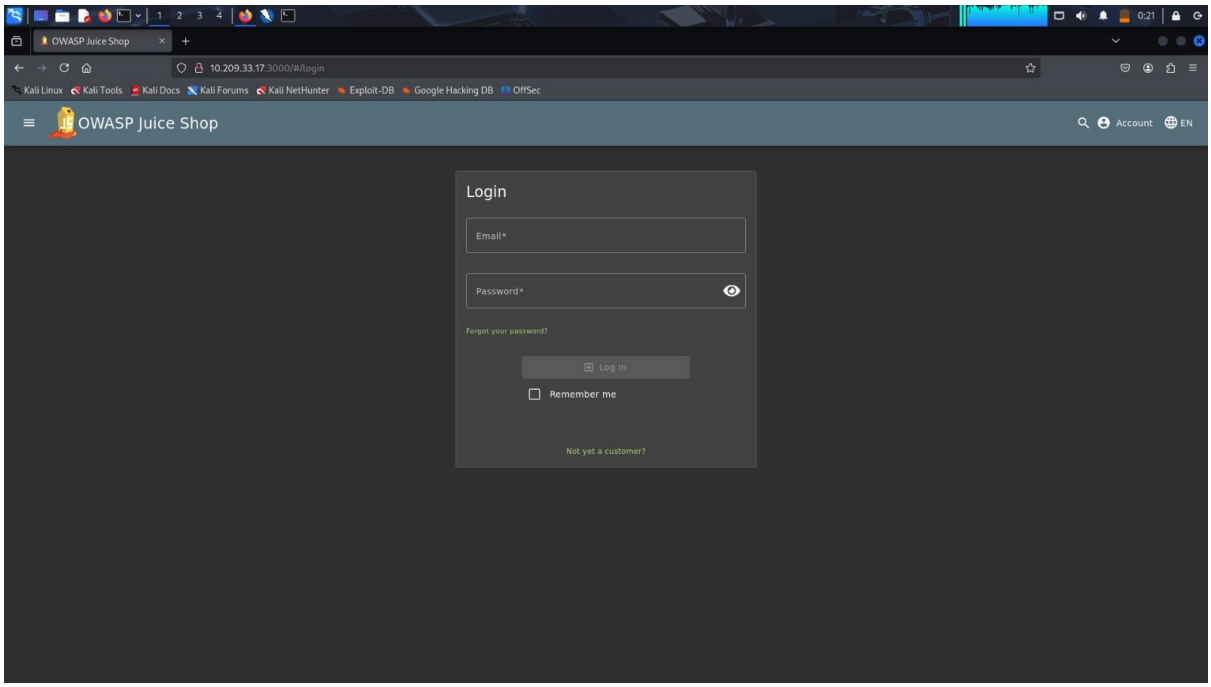
- **Description:** Weak login/session handling made user accounts vulnerable.
- **Impact:** Unauthorized access to user accounts.
- **Recommendation:** Enforce strong password policies and secure session tokens.

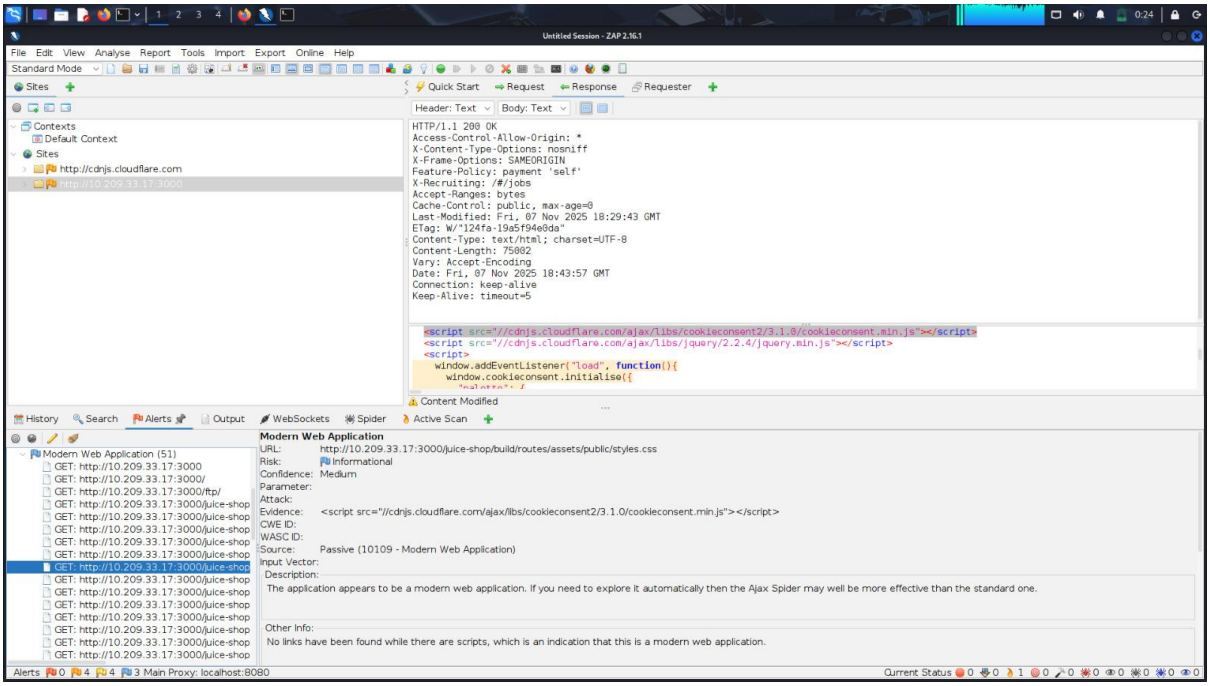
5.4 Security Misconfiguration

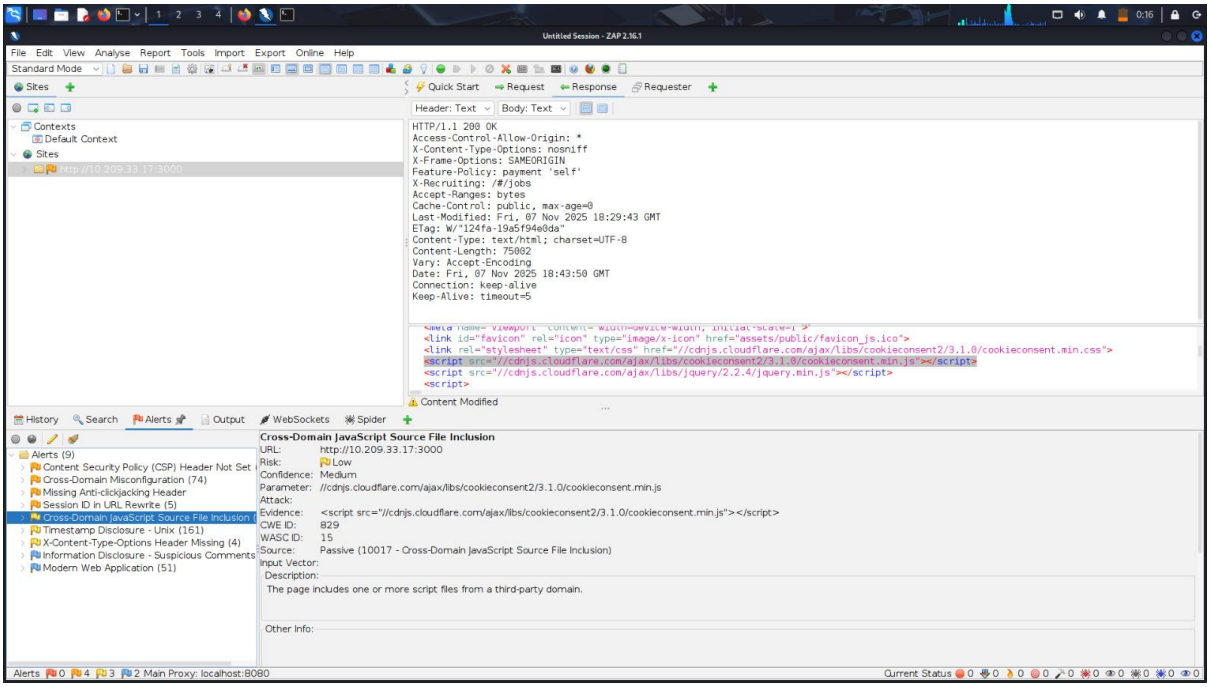
- **Description:** Application revealed debug/error messages exposing internal details.
- **Impact:** Attackers can use these details to perform targeted attacks.
- **Recommendation:** Disable debugging mode and configure secure error handling.

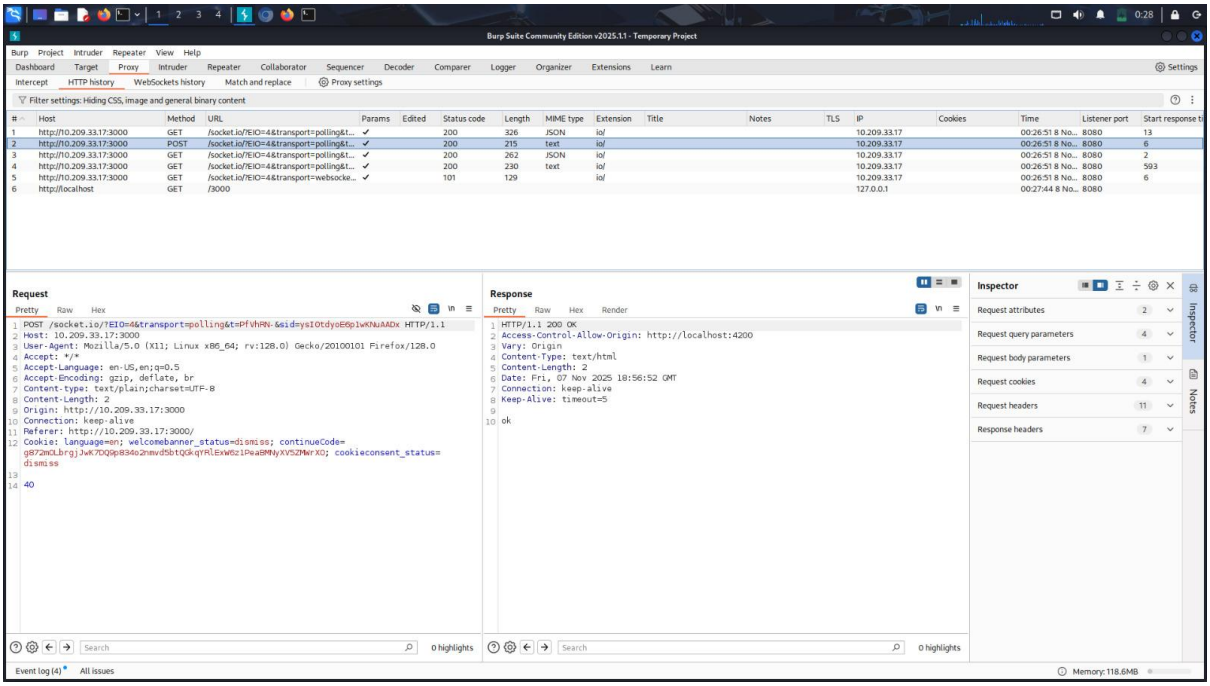
5.Screenshots

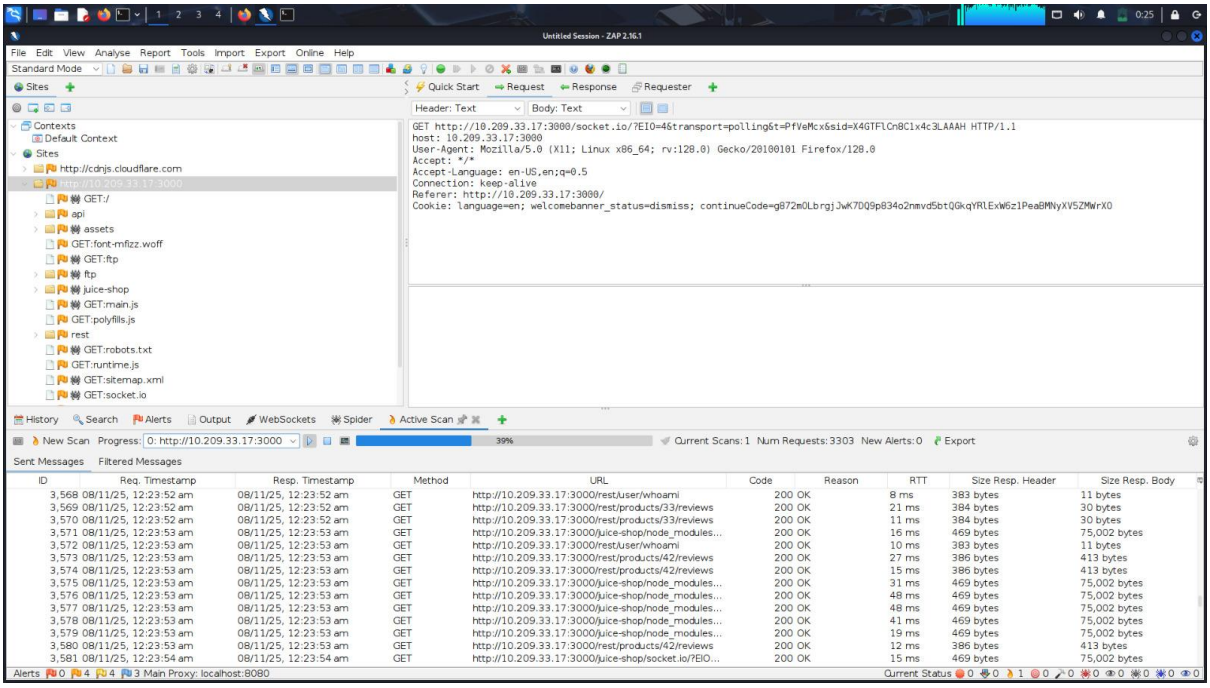





Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
http://cdnjs.cloudflare.com
http://10.209.33.17:3000
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Fri, 07 Nov 2025 18:29:43 GMT
ETag: W/"124fa-19a5f94e0da"
Content-Type: text/html; charset=UTF-8
Content-Length: 75002
Vary: Accept-Encoding
Date: Fri, 07 Nov 2025 18:43:57 GMT
Connection: keep-alive
Keep-Alive: timeout=5
<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
<script>
window.addEventListener("load", function(){
window.cookieconsent.initialise({
Content Modified
History Search Alerts Output WebSockets Spider Active Scan
Modern Web Application (51)
GET: http://10.209.33.17:3000
GET: http://10.209.33.17:3000/
GET: http://10.209.33.17:3000/ftp/
GET: http://10.209.33.17:3000/juice-shop
Modern Web Application
URL: http://10.209.33.17:3000/juice-shop/build/routes/assets/public/styles.css
Risk: Informational
Confidence: Medium
Parameter:
Attack:
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID:
WASC ID:
Source: Passive (10109 - Modern Web Application)
Input Vector:
Description:
The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Other Info:
No links have been found while there are scripts, which is an indication that this is a modern web application.
Alerts 0 4 4 3 Main Proxy: localhost:8080
Current Status


Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Fri, 07 Nov 2025 18:29:43 GMT
ETag: W/"124fa-19a5f94e0da"
Content-Type: text/html; charset=UTF-8
Content-Length: 75002
Vary: Accept-Encoding
Date: Fri, 07 Nov 2025 18:43:50 GMT
Connection: keep-alive
Keep-Alive: timeout=5
<link id="favicon" rel="icon" type="image/x-icon" href="assets/public/favicon_js.ico">
<link rel="stylesheet" type="text/css" href="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css">
<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
<script>
Content Modified
History Search Alerts Output WebSockets Spider
Alerts (9)
Content Security Policy (CSP) Header Not Set
Cross-Domain Misconfiguration (74)
Missing Anti-clickjacking Header
Session ID in URL Rewrite (5)
Cross-Domain JavaScript Source File Inclusion
Timestamp Disclosure - Unix (161)
X-Content-Type-Options Header Missing (4)
Information Disclosure - Suspicious Comments
Modern Web Application (51)
Cross-Domain JavaScript Source File Inclusion
URL: http://10.209.33.17:3000
Risk: Low
Confidence: Medium
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Attack:
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829
WASC ID: 15
Source: Passive (10017 - Cross-Domain JavaScript Source File Inclusion)
Input Vector:
Description:
The page includes one or more script files from a third-party domain.
Other Info:
Alerts 0 4 3 2 Main Proxy: localhost:8080
Current Status


Burp Suite Community Edition v2025.1.1 - Temporary Project
Request
Response
Inspector


Untitled Session - ZAP 2.16.1

.gitkeep

7. Conclusion

This task provided hands-on experience in identifying and analyzing common web application vulnerabilities. It also helped in understanding secure coding practices and mitigation strategies. Completing this task strengthened my skills in **Web Application Penetration Testing, OWASP Awareness, and Security Documentation**.

---

8. GitHub Repository Link

https://github.com/ANKI0310/FUTURE_CS_01/tree/main/Task1_WebAppSecurity/Screenshots