Security Assessment Report for OWASP Juice Shop Using Burp Suite

Internship At: Future Interns

Submitted by: Anuj Maharjan

Table of Contents

1. Executive Summary

This report summarizes the findings from a web application security assessment conducted on OWASP Juice Shop, an intentionally vulnerable application used for penetration testing and cybersecurity learning. Using Burp Suite, I identified and analyzed several vulnerabilities in alignment with the OWASP Top 10 security risks. Each finding is documented with the corresponding impact, evidence, and recommended mitigation strategies.

2. Scope

The scope of the assessment includes:

Target: OWASP Juice Shop (localhost instance)
Tools Used:
- Burp Suite (Community Edition)
- Browser with Burp Proxy
- OWASP Juice Shop

Assessment Type: Black-box Testing

3. Methodology

The assessment was conducted using the following steps:

Reconnaissance via Burp Suite Spider
Vulnerability Scanning using Intruder, Repeater, and Scanner tools
Manual exploitation for confirmation
Mapping to OWASP Top 10
Risk Rating based on CVSS v3.1 (where applicable)

4. Key Findings

Vulnerability	OWASP Category	Risk Level	Status
SQL Injection on login	A1: Injection	High	Confirmed
Reflected XSS	A7: Cross-Site Scripting	Medium	Confirmed
Insecure Direct Object Reference (IDOR)	A4: IDOR	High	Confirmed
Security Misconfiguration	A6: Misconfiguration	Medium	Confirmed
Missing Rate Limiting on Login	A10: SSRF/Insufficient Logging & Monitoring	Low	Confirmed

5. Vulnerability Details

SQL Injection on Login Form

Description	' OR '1'='1
Evidence	Login succeeded without valid credentials
Impact	Unauthorized access to user accounts
Mitigation	Use parameterized queries or ORM frameworks

Reflected Cross-Site Scripting (XSS)

Description	/search?q=<script>alert(1)</script>
Evidence	Script executed in browser
Impact	Session hijacking or phishing
Mitigation	Encode output, use CSP headers

Insecure Direct Object Reference (IDOR)

Description	Changed userId parameter
Evidence	Accessed other users' data via ID manipulation
Impact	Data leakage
Mitigation	Implement authorization checks on backend

Security Misconfiguration

Description	Verbose error messages
Evidence	Displayed detailed error messages
Impact	Information disclosure
Mitigation	Disable detailed error messages in production

Missing Rate Limiting on Login

Description	Brute force attempts not blocked
Evidence	Repeated login requests not denied
Impact	Increased risk of credential stuffing
Mitigation	Implement rate limiting and lockouts

6. OWASP Top 10 Compliance Mapping

OWASP Risk	Status
A1: Injection	✅ Found
A2: Broken Auth	⚠️ Partial
A3: Sensitive Data Exposure	❌ Not observed
A4: IDOR	✅ Found
A5: Security Misconfig	✅ Found
A6: XSS	✅ Found
A7: Broken Access Control	✅ Found

A8: CSRF	❌ Not found
A9: Components w/ Known Vuln	⚠️ Not tested
A10: Insufficient Logging/Monitoring	⚠️ Observed

7. Tools Used and Logs

Burp Suite Logs:

- Proxy history
- Intruder payloads
- Scanner issues list

Screenshots:

- Injection and XSS payload success
- Burp Suite Scanner Results
- Response showing misconfiguration

8. Conclusion & Recommendations

This assessment revealed several critical vulnerabilities in the target application. While OWASP Juice Shop is designed to be insecure, this simulation provided valuable experience in vulnerability discovery, risk analysis, and ethical hacking methodology. The use of Burp Suite enabled effective exploitation and verification of findings.

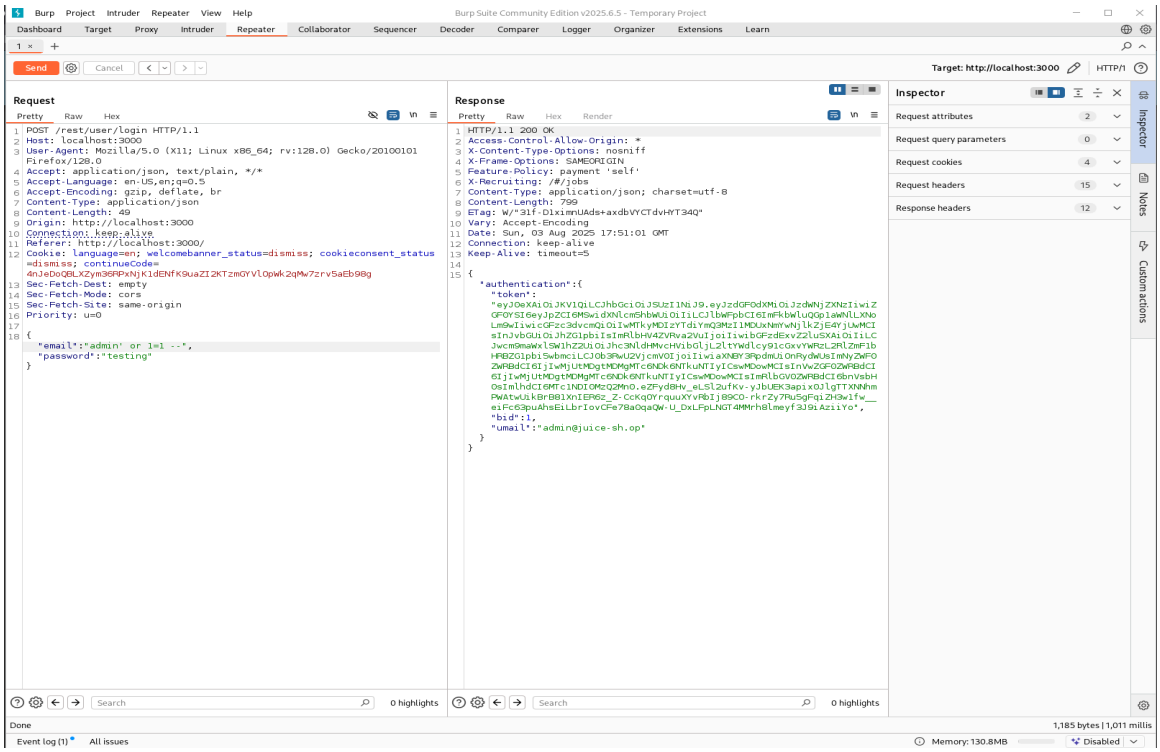
Top Recommendations:

Apply input validation and output encoding
Use secure development frameworks
Enforce strict authorization logic
Enable rate limiting and logging mechanisms

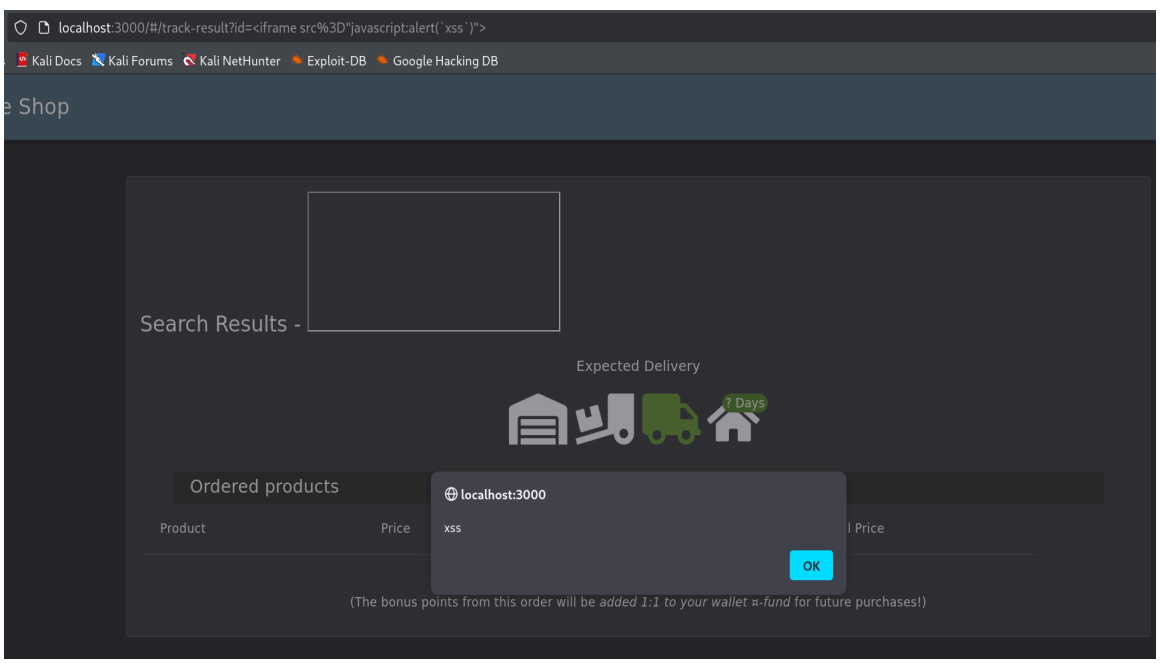
9. Appendix

Screenshots of Attack Execution

SQL Injection on Login Form

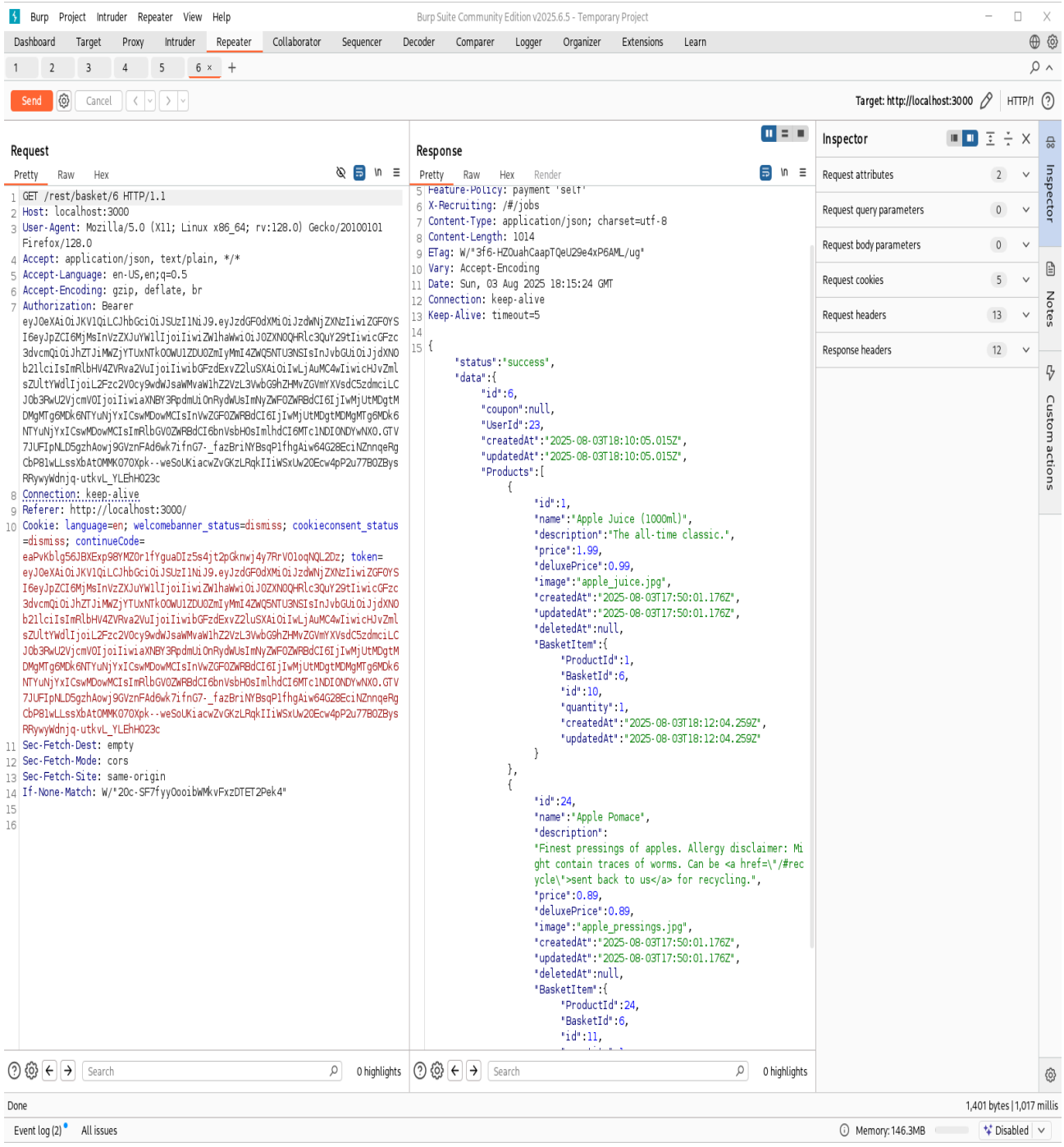


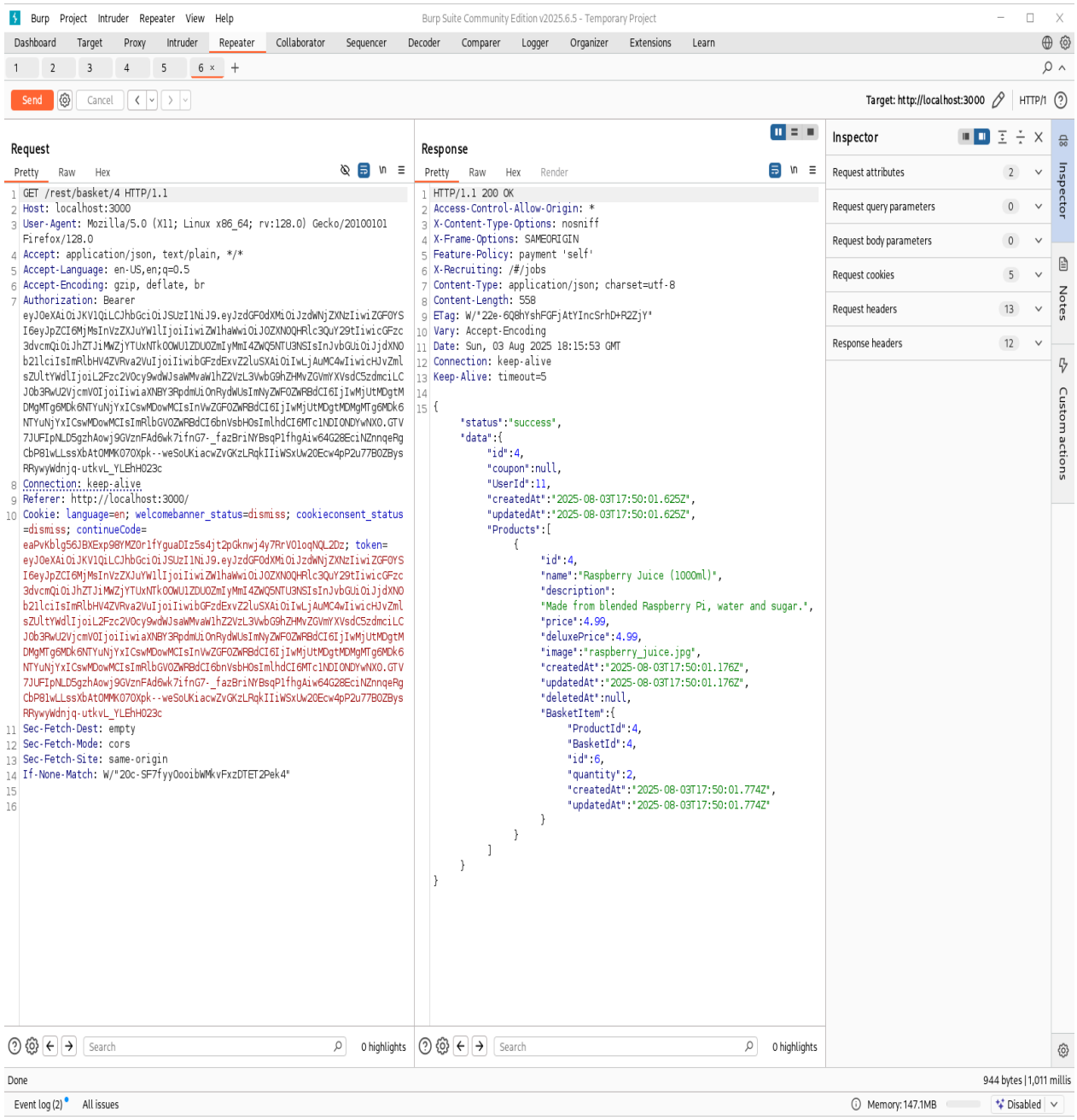
Reflected Cross-Site Scripting (XSS)



Insecure Direct Object Reference (IDOR)

First one is original basket of the user and below is the modified request + response showing other user's items in basket

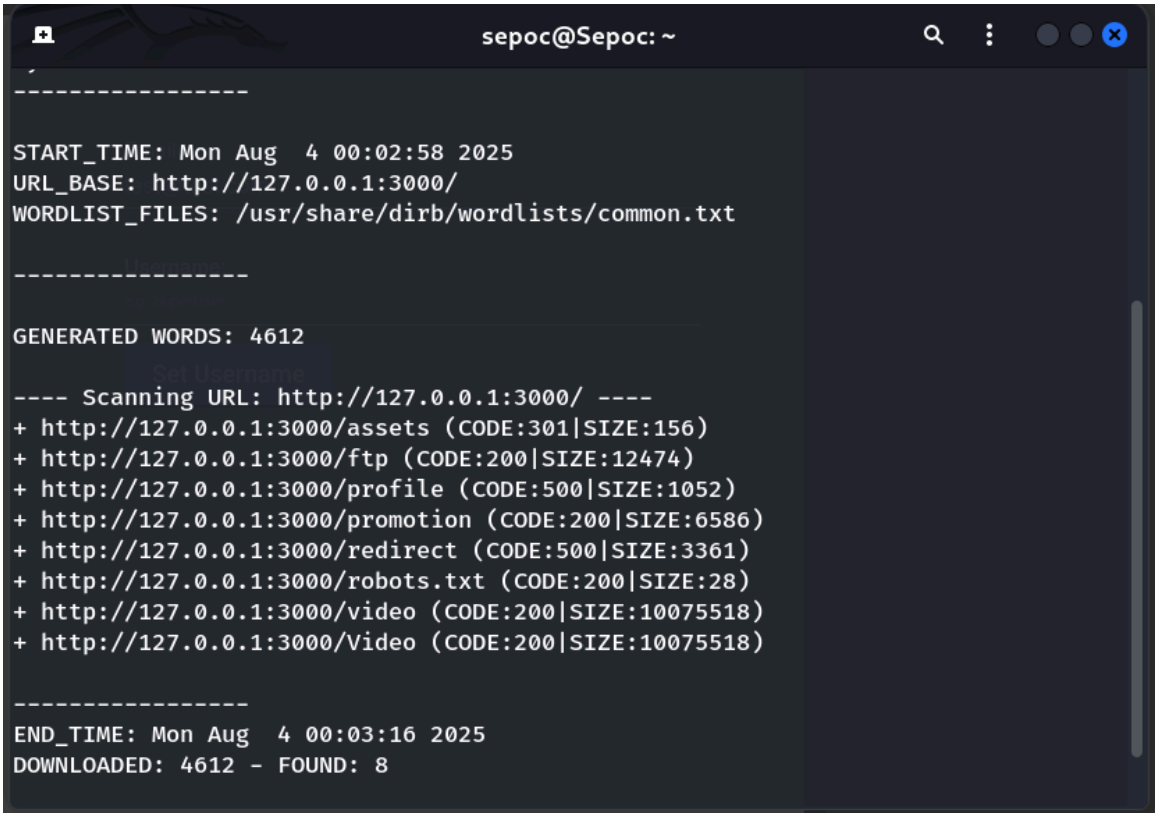


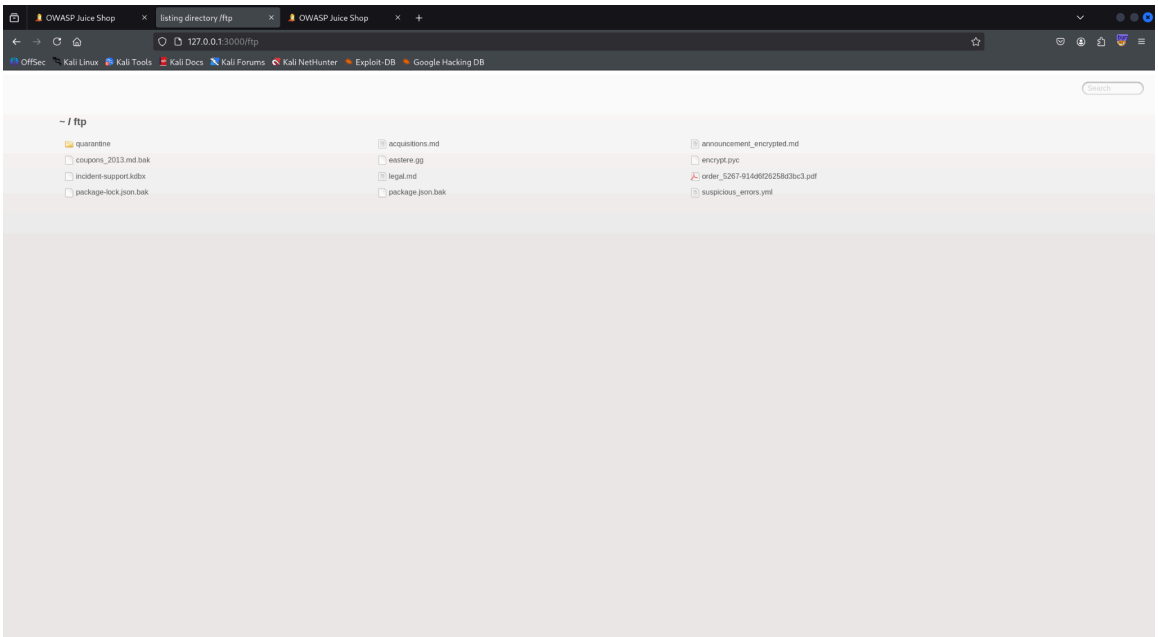


Security Misconfiguration

Juice Shop, by design, simulates multiple misconfigurations, including default error pages showing stack traces, Unsecured endpoints (/ftp, /debug, /profile), Verbose error messages, Lack of secure headers, Open admin pages or debug interfaces. In the first step, we performed a port scan using **Nmap** to identify open services. Next, we used **Dirb** to enumerate accessible directories and URLs on the web server. This scan revealed confidential files and

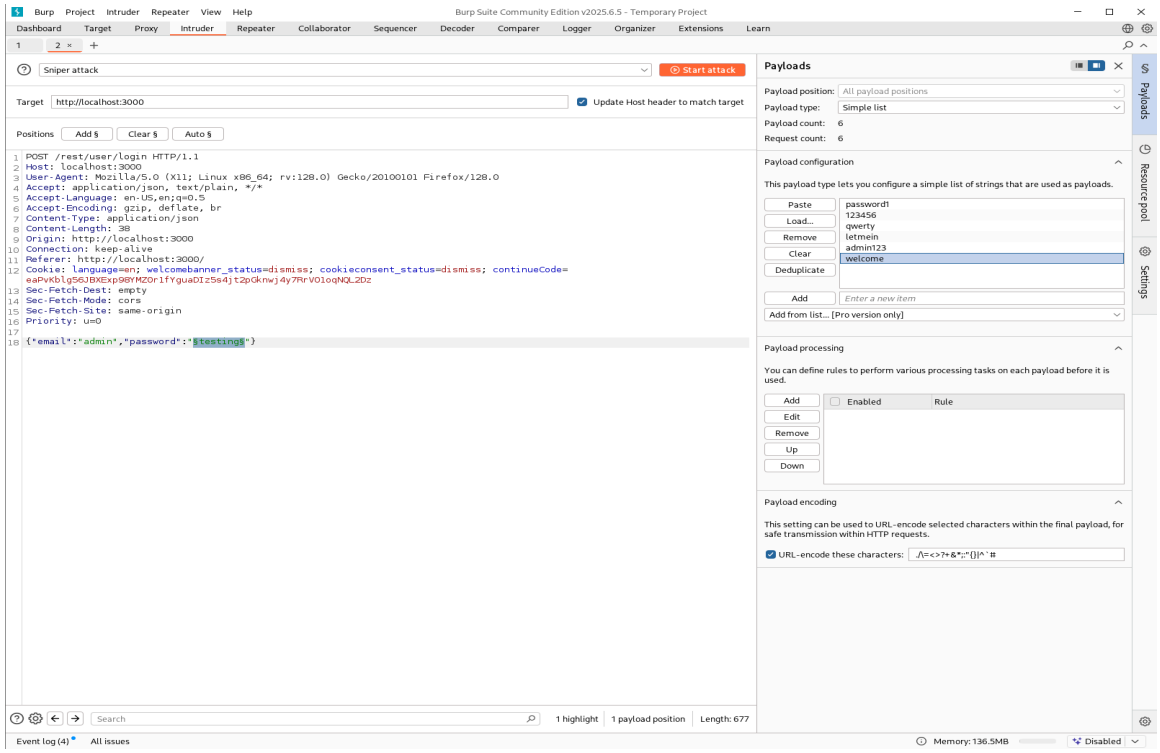
directories that were unintentionally exposed, allowing unauthorized access to sensitive information.

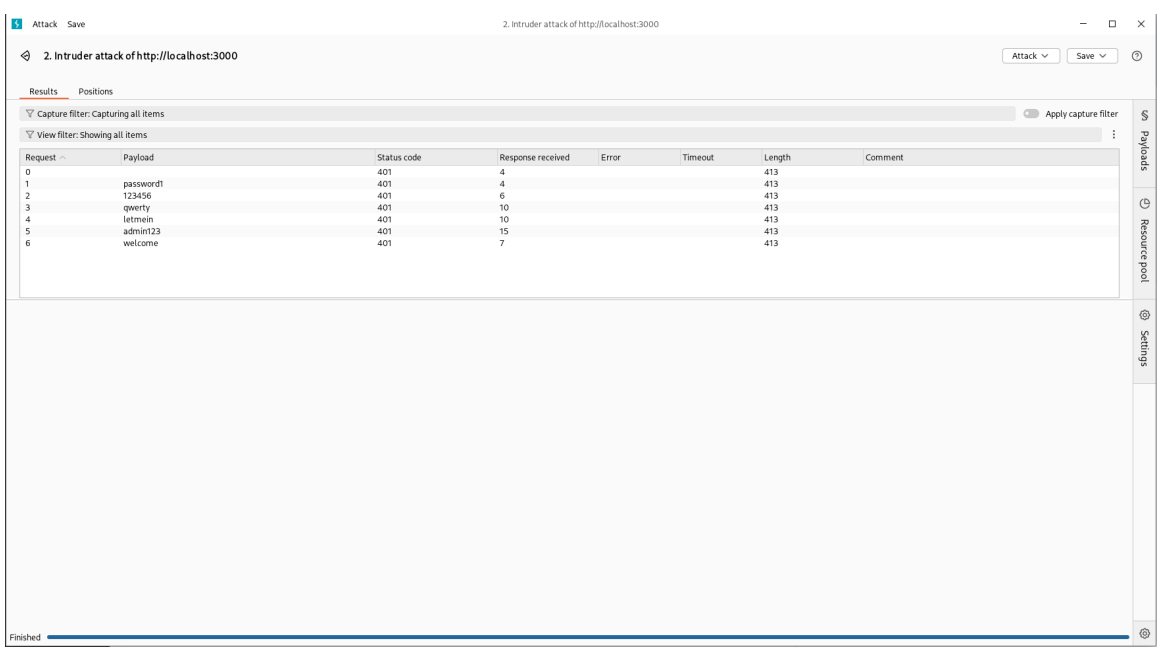




Missing Rate Limiting on Login

In this test, we targeted the login endpoint by first preparing a brute-force attack payload in **Burp Suite Intruder**. The first screenshot shows the configuration where multiple passwords were loaded against a fixed email address. In the second screenshot, the attack was executed, and the server responded with repeated 401 Unauthorized status codes without any delay or blocking mechanism. This confirms that no rate limiting or brute-force protection is in place, exposing the system to credential-based attacks.





10.Bibliography

1. OWASP Foundation. *OWASP Juice Shop Project*. https://owasp.org/www-project-juice-shop/

2. OWASP Foundation. *OWASP Top 10: The Ten Most Critical Web Application Security Risks – 2021*. https://owasp.org/Top10/

3. PortSwigger. *Burp Suite Community Edition Documentation*. https://portswigger.net/burp/documentation

4. OWASP Foundation. *OWASP ZAP (Zed Attack Proxy)*. https://owasp.org/www-project-zap/

5. Nikto Project. *Nikto Web Scanner*. https://cirt.net/Nikto2

6. Nmap.org. *Nmap Reference Guide*. https://nmap.org/book/man.html

7. Mitre Corporation. *Common Vulnerabilities and Exposures (CVE) List*. https://cve.mitre.org/

8. Mozilla. *HTTP Security Headers Guide*. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers