Web Application Penetration Testing Report

Target Application: OWASP Juice Shop
Prepared By: Purna Kishore
Version: 1.0

1. Executive Summary

1.1 Summary

A penetration test was conducted on the OWASP Juice Shop web application to identify vulnerabilities aligned with the OWASP Top 10. The assessment revealed critical security issues, including SQL Injection, Reflected Cross-Site Scripting (XSS), authentication weaknesses, and security misconfigurations. These vulnerabilities could allow attackers to gain unauthorized access, extract sensitive data, and disrupt application availability1.

1.2 Strengths

- The application uses some modern frameworks and exposes RESTful endpoints, which can simplify security hardening.
- Security scanning tools (e.g., Retire.js) were able to identify third-party dependencies, aiding in vulnerability management1.
- Proxy tools and technology fingerprinting (Paralyzer) provided clear insights into the application stack, supporting targeted testing1.

1.3 Weaknesses

- SQL Injection vulnerabilities in authentication forms allowed bypassing login and extracting user data.
- Reflected XSS was exploitable with multiple payloads, including <iframe src=JavaScript: alert.
- Lack of rate limiting and account lockout enabled brute-force attacks with common passwords.
- Directory listing and insecure credentials were exposed due to security misconfiguration.
- Open-source components with known vulnerabilities were detected by Retire.js.

1.4 Business Impact

If exploited in a production environment, these vulnerabilities could result in:

- Compromise of user data, including email addresses and credentials.

- Unauthorized access to user accounts and sensitive application functions.
- Service disruption due to denial-of-service (DoS) attacks.
- Regulatory non-compliance and reputational damage.

2. Technical Summary

2.1 Scope & Objective

The assessment focused on the OWASP Juice Shop instance, aiming to identify and exploit OWASP Top 10 vulnerabilities using a combination of automated and manual techniques. The primary objectives were to demonstrate exploitability and provide actionable remediation guidance1.

2.2 Testing Environment

- **Target:** OWASP Juice Shop (local/cloud instance)
- **Tools Used:**
    - Burp Suite Community Edition (manual testing, request interception)
    - Wappalyzer (technology fingerprinting)
    - Retire.js (component vulnerability scanning)
    - Common password lists (for brute-force testing)
- **Test Date:** June 25, 2025

2.3 Technical Impact

- SQL Injection enabled authentication bypass and data extraction.
- Reflected XSS allowed execution of arbitrary JavaScript in users' browsers.
- Brute-force attacks revealed weak authentication controls.
- Security misconfigurations exposed sensitive directories and credentials.
- Vulnerable third-party components increased the attack surface.

2.4 Table of Findings

S. No	Tool/Technique	Description	Severity	Status
01	Wappalyzer	Identified backend technologies and components	Informational	NF
02	SQL Injection (Login)	Bypassed authentication, extracted user emails	Critical	NF
03	Reflected XSS	Executed JavaScript via unsensitized input	High	NF
04	Retire.js	Detected vulnerable open-source dependencies	Medium	NF
05	Brute-force (DoS)	No rate limiting, 100 common passwords tested	High	NF
06	Security Misconfiguration	Directory listing and insecure credentials exposed	High	NF

Severity Key:

- Critical – Full compromise or remote code execution
- High – Sensitive data exposure or account takeover
- Medium – Privilege escalation or information disclosure
- Informational – Contextual, not directly exploitable

Juice shop Installation: https://hub.docker.com/r/bkimminich/juice-shop

1. **Quickest Method (Docker)**:

   `docker pull bkimminich/juice-shop && docker run -p 3000:3000 bkimminich/juice-shop`

   Access at `http://localhost:3000`.
2. **From Source**:

   Clone the repo, run `npm install && npm start`. Requires Node.js.
3. **Pre-Packaged**:

   Download the latest release ZIP/tgz, extract, and run `npm start`.
4. **Cloud Deploy**:

   One-click deploy on **Heroku** or use **AWS/Azure/GCP** scripts for instant hosting.
5. **Vagrant**:

   `cd vagrant && vagrant up` to launch a VM (requires VirtualBox).

3. Technical Findings

Passive Reconnaissance:

DNS Enumeration:

Used command - `dnsenum juiceshop.com.` (`dnsenum example.com`)

```
┌──(kali㉿kali)-[~]
└─$ dnsenum juiceshop.com
dnsenum VERSION:1.3.1

-----   juiceshop.com   -----

Host's addresses:
__________________

juiceshop.com.                           3600     IN    A        23.227.38.32

Name Servers:
______________

ns70.domaincontrol.com.                  171008   IN    A        173.201.72.45
ns69.domaincontrol.com.                  171009   IN    A        97.74.104.45

Mail (MX) Servers:
___________________

alt1.aspmx.l.google.com.                 293      IN    A        172.253.116.27
alt2.aspmx.l.google.com.                 293      IN    A        173.194.76.27
aspmx.l.google.com.                      293      IN    A        142.251.111.27
aspmx2.googlemail.com.                   239      IN    A        172.253.116.27
aspmx3.googlemail.com.                   209      IN    A        173.194.76.27

Trying Zone Transfers and getting Bind Versions:
________________________________________________

Trying Zone Transfer for juiceshop.com on ns70.domaincontrol.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for juiceshop.com on ns69.domaincontrol.com ...
AXFR record query failed: corrupt packet

Brute forcing with /usr/share/dnsenum/dns.txt:
______________________________________________

abc.juiceshop.com.                       600      IN    CNAME    juiceshop-production.herokuapp.com.
juiceshop-production.herokuapp.com.      42       IN    A        18.208.60.216
juiceshop-production.herokuapp.com.      42       IN    A        54.159.116.102
juiceshop-production.herokuapp.com.      42       IN    A        54.165.58.209
juiceshop-production.herokuapp.com.      42       IN    A        52.5.82.174
ftp.juiceshop.com.                       3600     IN    CNAME    juiceshop.com.
juiceshop.com.                           3600     IN    A        23.227.38.32
mail.juiceshop.com.                      3600     IN    CNAME    pop.secureserver.net.
pop.secureserver.net.                    3481     IN    CNAME    pop.vox.secureserver.net.
pop.vox.secureserver.net.                164      IN    CNAME    pop.eu-central.vox.secureserver.net.
pop.eu-central.vox.secureserver.net.     464      IN    A        92.204.80.24
pop.juiceshop.com.                       3600     IN    CNAME    pop.secureserver.net.
pop.secureserver.net.                    3236     IN    CNAME    pop.vox.secureserver.net.
pop.vox.secureserver.net.                267      IN    CNAME    pop.eu-central.vox.secureserver.net.
pop.eu-central.vox.secureserver.net.     189      IN    A        92.204.80.24
smtp.juiceshop.com.                      3600     IN    CNAME    smtp.secureserver.net.
smtp.secureserver.net.                   300      IN    A        216.69.141.84
smtp.secureserver.net.                   300      IN    A        216.69.141.71
smtp.secureserver.net.                   300      IN    A        216.69.141.113
test.juiceshop.com.                      600      IN    CNAME            (
```

DNS Enumeration Report Summary – juiceshop.com

Summary: The scan reveals multiple exposed subdomains (e.g., ftp., test., smtp.) and CNAMEs pointing to third-party services like Heroku and secureserver.net, posing a risk of subdomain takeover. Zone transfers are blocked but excessive DNS exposure increases the attack surface.

Risks: Subdomain takeover, reconnaissance for phishing/spam, staging environment exposure.

Remediation:

- Remove or secure unused/test subdomains
- Audit and delete outdated CNAMEs
- Implement SPF/DKIM/DMARC for email
- Enable DNSSEC and monitor DNS logs

Nmap (Active Recon):

Used Command: `sudo nmap -sS -sV -O -p- juiceshop.com`

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -O -p- juiceshop.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-11 17:33 EDT
Stats: 0:12:56 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 44.51% done; ETC: 18:02 (0:16:07 remaining)
Stats: 0:21:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 63.33% done; ETC: 18:07 (0:12:30 remaining)
Stats: 0:28:34 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 78.48% done; ETC: 18:09 (0:07:50 remaining)
Stats: 0:37:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 97.15% done; ETC: 18:11 (0:01:06 remaining)
Nmap scan report for juiceshop.com (23.227.38.32)
Host is up (0.036s latency).
rDNS record for 23.227.38.32: myshopify.com
Not shown: 65522 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Cloudflare http proxy
443/tcp  open  ssl/http Cloudflare http proxy
2052/tcp open  http     Cloudflare http proxy
2053/tcp open  ssl/http nginx
2082/tcp open  http     Cloudflare http proxy
2083/tcp open  ssl/http nginx
2086/tcp open  http     Cloudflare http proxy
2087/tcp open  ssl/http nginx
2095/tcp open  http     Cloudflare http proxy
2096/tcp open  ssl/http nginx
8080/tcp open  http     Cloudflare http proxy
8443/tcp open  ssl/http Cloudflare http proxy
8880/tcp open  http     Cloudflare http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Apple iOS 14.0 - 15.6 or tvOS 14.3 - 16.1 (Darwin 20.0.0 - 22.1.0) (89%), Apple macOS 11 (Big Sur) -
 13 (Ventura) or iOS 16 (Darwin 20.6.0 - 22.4.0) (89%), FreeBSD 11.0-STABLE (89%), FreeBSD 11.1-STABLE (89%), Apple iOS 15.
7 (Darwin 21.7.0) (88%), Apple macOS 12 (Monterey) (Darwin 21.2.0) (88%), Apple macOS 13 (Ventura) (Darwin 22.0.0) (88%), F
reeBSD 11.0-RELEASE (88%), FreeBSD 11.3-RELEASE (88%), FreeBSD 12.0-RELEASE - 12.1-RELEASE (88%)
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2327.07 seconds
```

Nmap Reconnaissance Report – Open Services Exposure

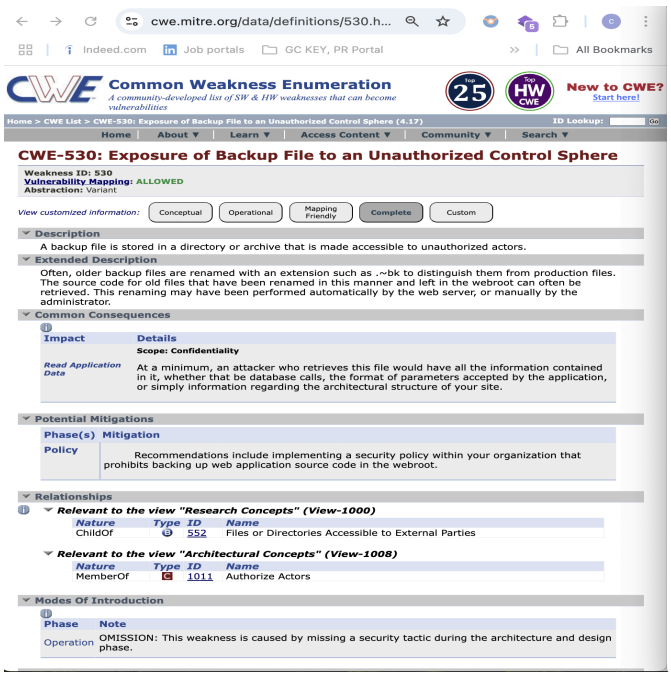
Summary:
An Nmap scan on `juiceshop.com` revealed multiple open ports (80, 443, 8080–8090, 8443) with web services behind Cloudflare. Some high-numbered ports may indicate additional services or admin panels.

Impact: Increases the attack surface; unused or unsecured services may be exploited.

Remediation: Close unused ports, implement firewall rules, audit services on open ports, and harden server configurations behind Cloudflare.

Nikto: Scanned the OWASP Juice shop web application at http://192.168.2.141:3000 and Nikto was executed with the command `nikto -h http://192.168.2.141:3000 -o nikto_output.txt` to access web applications on juice shop instance detected:
Missing Security Headers (`X-Content-Type-Options`), Information Disclosure via Headers (`access-control-allow-origin`), robots.txt Exposes Sensitive Paths, Dangerous Backup/Certificate Files Exposed Over 100 files like:

```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://192.168.2.141:3000 -o nikto_output.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.2.141
+ Target Hostname:    192.168.2.141
+ Target Port:        3000
+ Start Time:         2025-07-11 18:54:29 (GMT-4)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: Retrieved access-control-allow-origin header: *.
+ /: Uncommon header 'x-recruiting' found, with contents: /#/jobs.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/ftp/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-
scanner/vulnerabilities/missing-content-type-header/
+ /backup.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /168.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /2.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192168.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192168.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192_168_2_141.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /1921682.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192168.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.2.141.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /141.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192_168_2_141.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /141.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /1921682.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.2.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /141.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192_168_2_141.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.2.141.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /1921682141.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /2.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.2.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.2.141.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /2.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /2.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /168.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192168.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /192.168.2.141.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
```




```
itions/530.html
+ /192_168_2_141.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.o
rg/data/definitions/530.html
+ /dump.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/d
efinitions/530.html
+ /192168.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/dat
a/definitions/530.html
+ /192168.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/def
initions/530.html
+ /192.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/defini
tions/530.html
+ /backup.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/def
initions/530.html
+ /dump.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/defin
itions/530.html
+ /192.168.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/de
finitions/530.html
+ /141.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/defini
tions/530.html
+ /168.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/defini
tions/530.html
+ /backup.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/def
initions/530.html
+ /backup.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data
/definitions/530.html
+ /site.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/
definitions/530.html
+ /192.168.2.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/
definitions/530.html
+ /192.168.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/de
finitions/530.html
+ /192.168.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/dat
a/definitions/530.html
+ /192168.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/def
initions/530.html
+ /1921682.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/de
finitions/530.html
+ /1921682.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/de
finitions/530.html
+ /backup.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/def
initions/530.html
+ /1921682141.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data
/definitions/530.html
+ /192.168.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/da
ta/definitions/530.html
+ /1921682141.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data
/definitions/530.html
+ /192_168_2_141.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/d
ata/definitions/530.html
+ /archive.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/de
finitions/530.html
+ /archive.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/de
finitions/530.html
+ /192.168.2.141.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/d
ata/definitions/530.html
+ /2.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/def
initions/530.html
+ /192.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/defini
tions/530.html
+ /141.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/defini
tions/530.html
+ /dump.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/
```

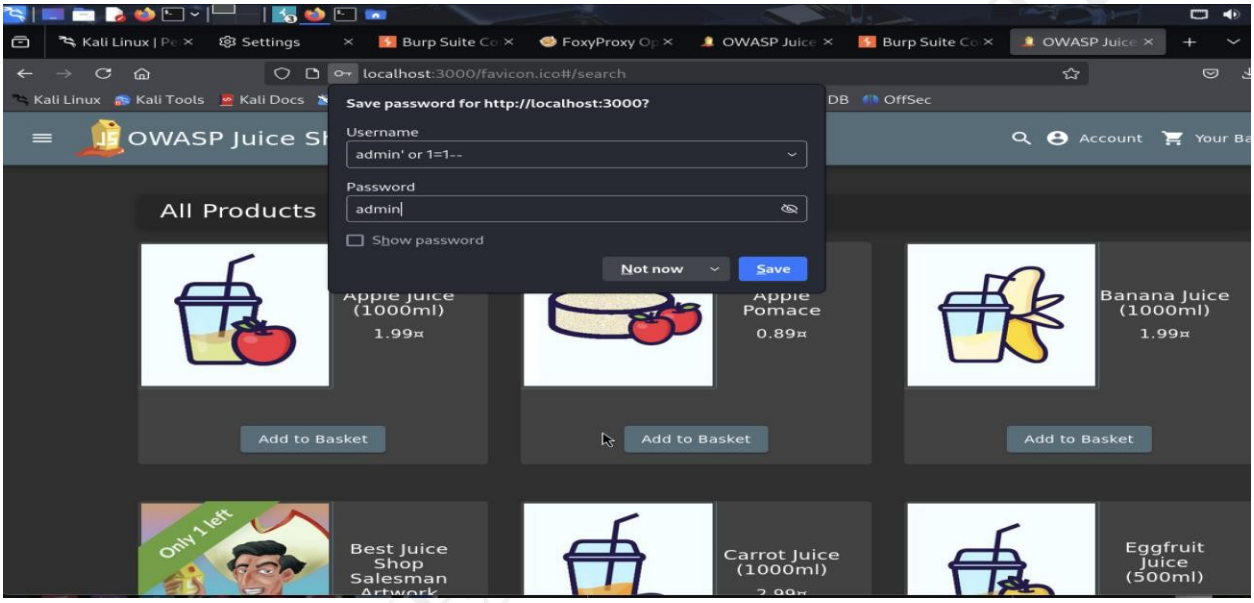
Vulnerability Report – CWE-530: Exposure of Backup Files
Multiple sensitive files (e.g., `.tar`, `.pem`, `.jks`, `.war`) were publicly accessible via HTTP, risking exposure of credentials, source code, and app architecture.
Impact: Confidentiality breach, possible full system compromise.
Remediation: Immediately remove or restrict access to backup files, enforce secure DevOps policies, and scan regularly using tools like Nikto or Nuclei.
Reference: CWE-530 – Exposure of Backup File to Unauthorized Control.

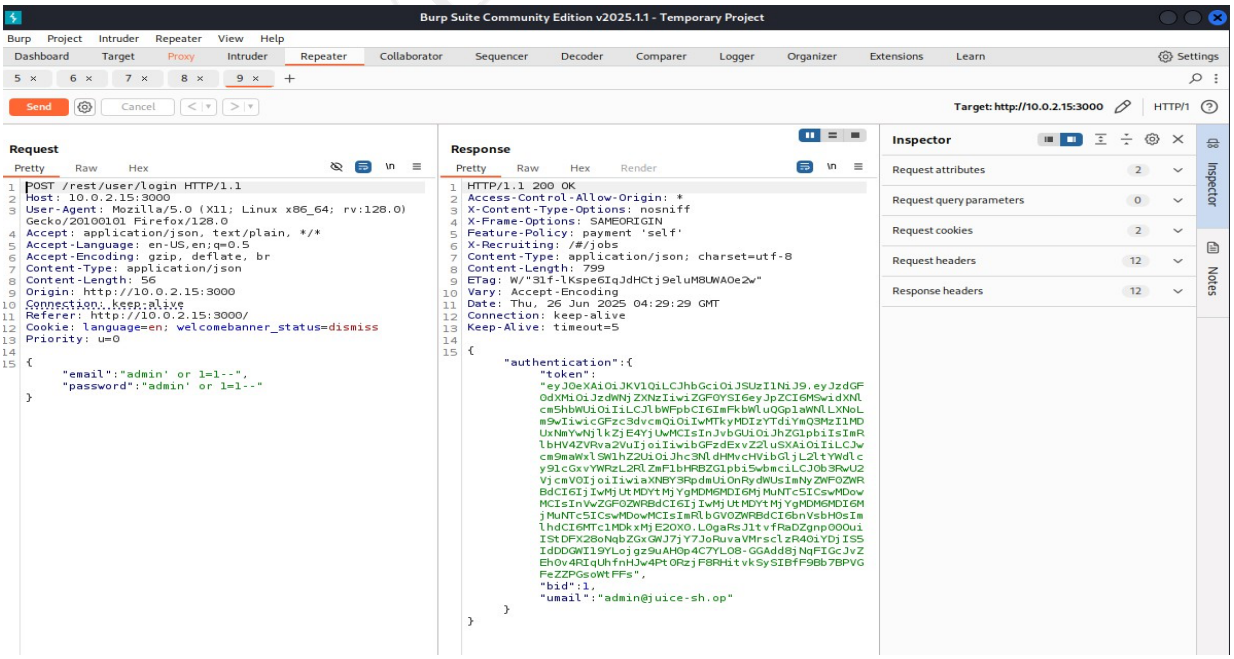
3.1 SQL Injection in Authentication (Critical)

- **Description:**
  The login form was vulnerable to SQL Injection. Using payloads such as ' OR '1'='1 and variants with #, testers could bypass authentication and access user accounts. The attack revealed user email addresses and other sensitive information1.

CVSS Score: 9.8 (Critical)

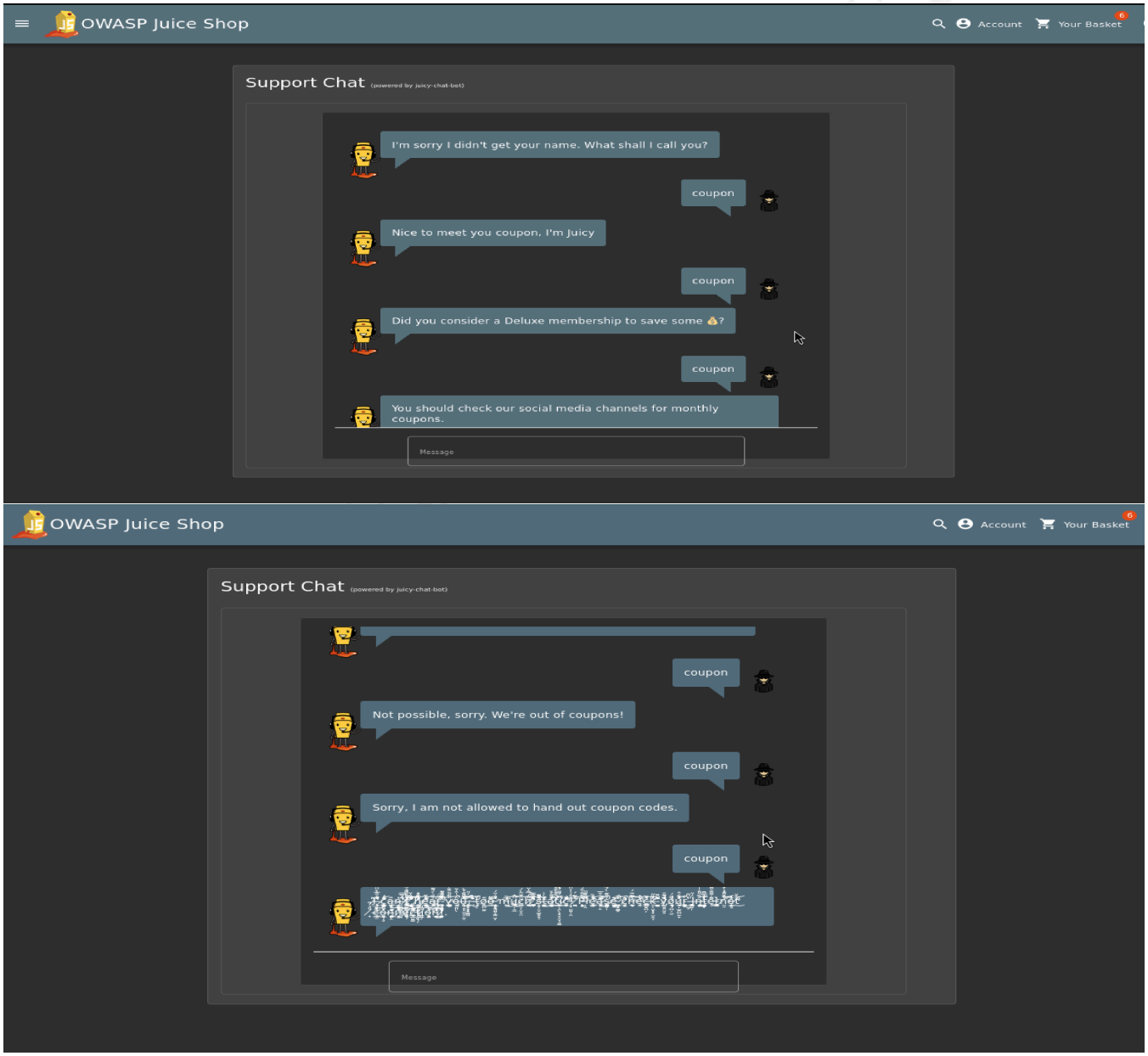
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H





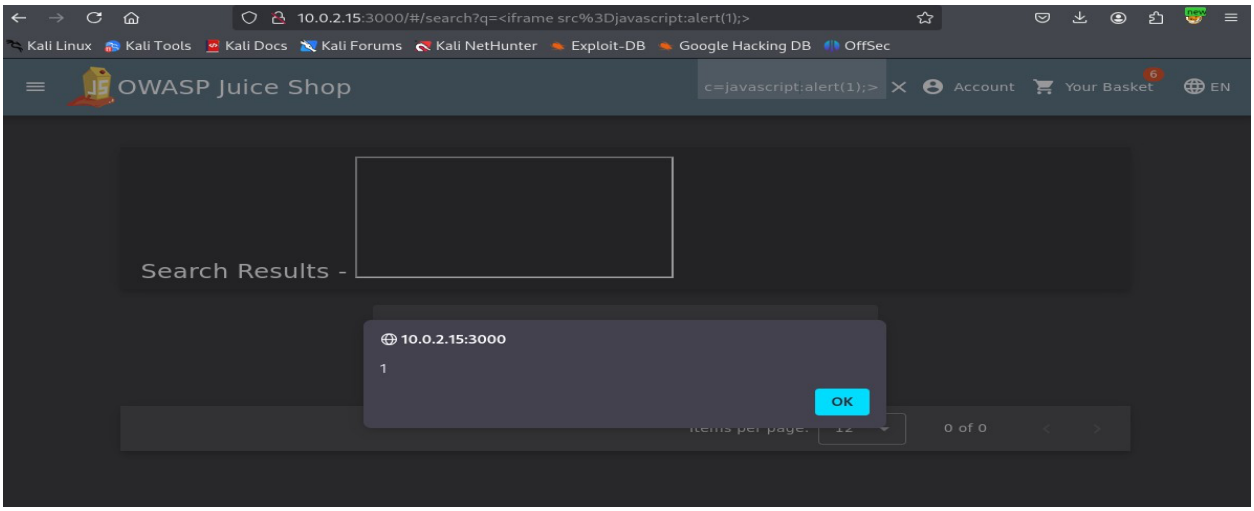
- **Business Impact:**
  Full compromise of user accounts and potential access to administrative functions.
- **Remediation:**
  - Implement parameterized queries (prepared statements).
  - Validate and sanitize all user inputs.
  - Apply least privilege to database accounts

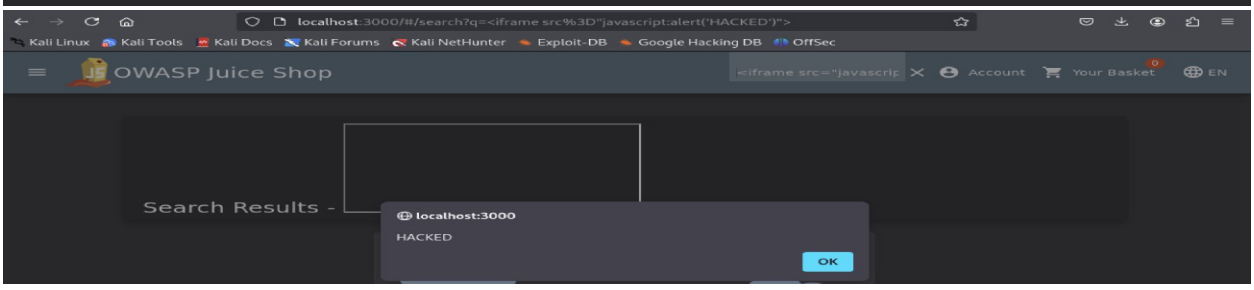
SQL INJECTION : Bullying chatbot

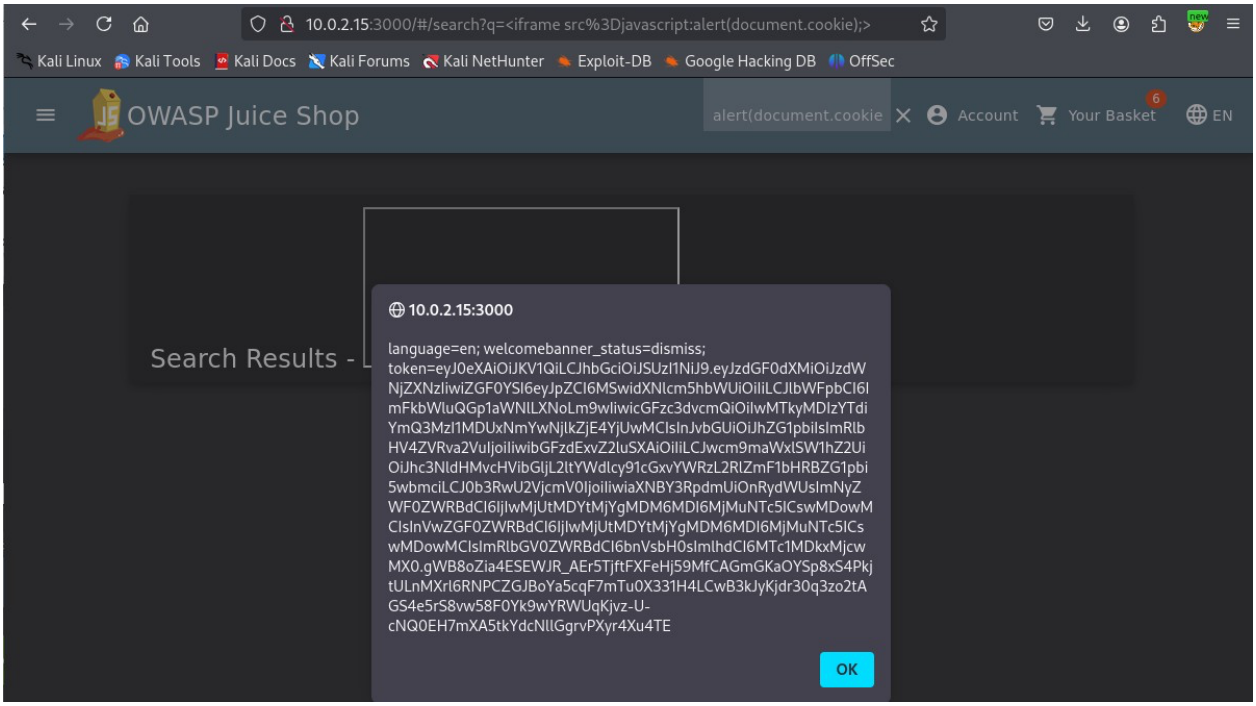


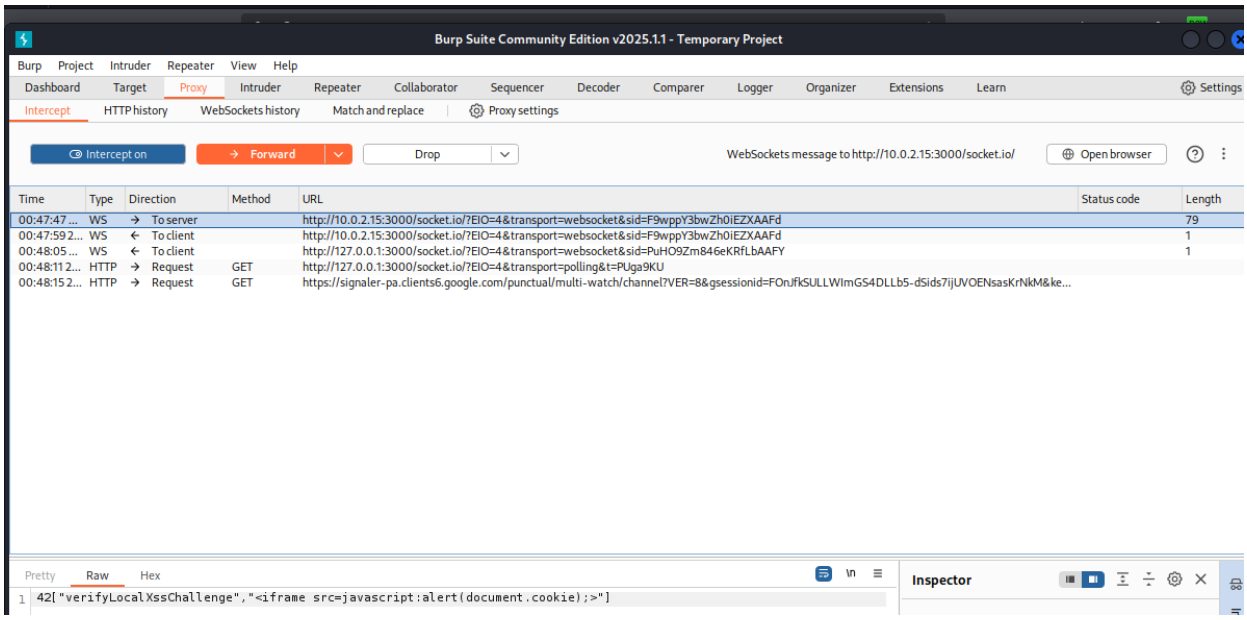
3.2 Reflected Cross-Site Scripting (High)

- **Description:**
  Reflected XSS was confirmed using payloads like <iframe src=javascript:alert(HACKED) <iframe src=javascript:alert(1);> and <iframe src=javascript:alert(document.cookie);>. Unsanitized user input was injected and executed in the browser context.





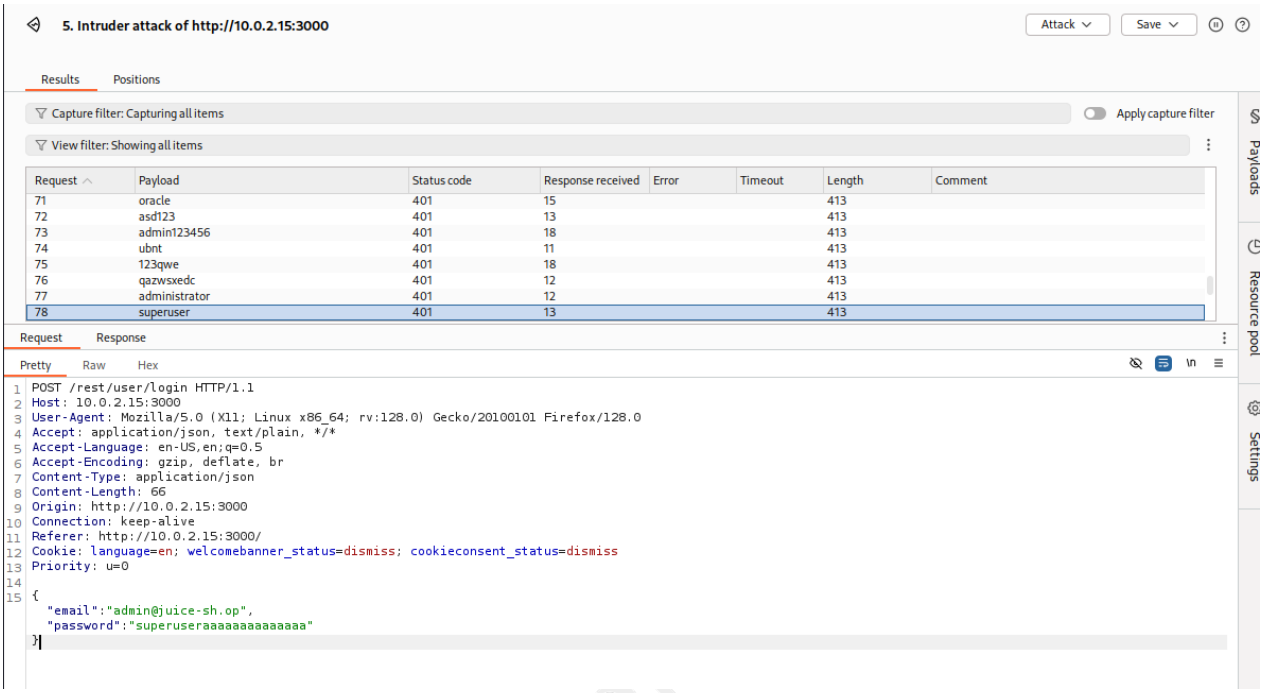


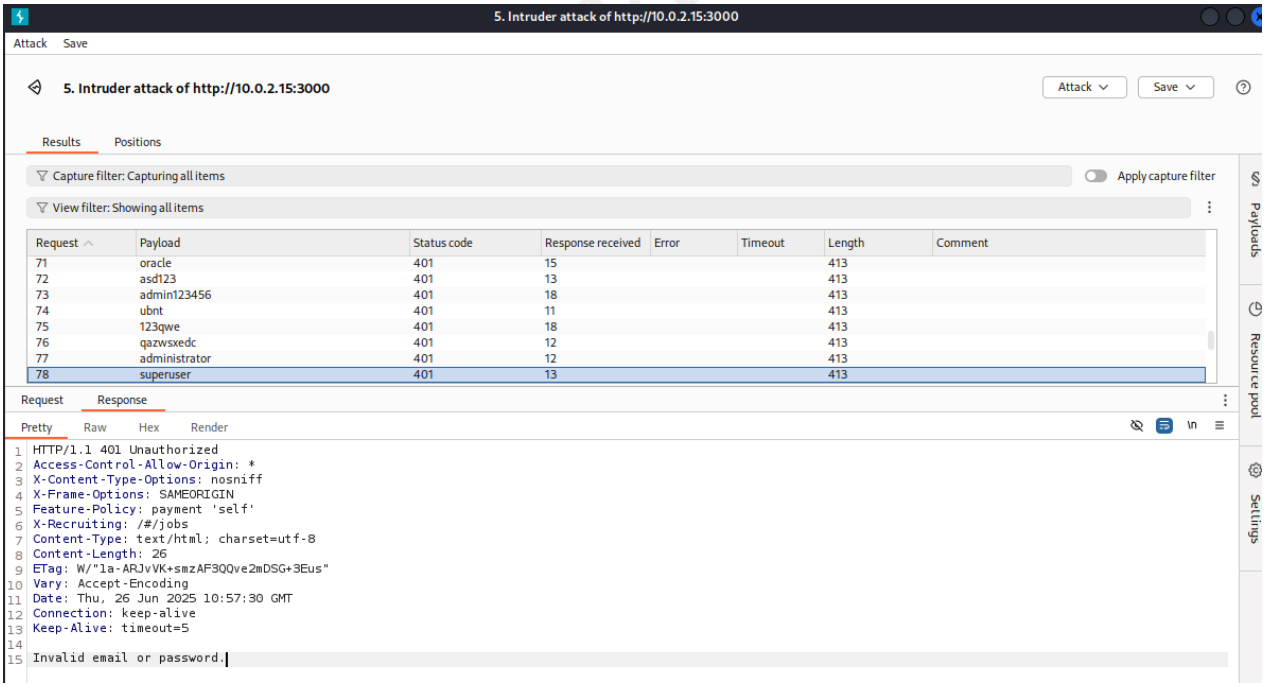


- **Business Impact:**
  could enable session hijacking, phishing, or defacement.
- **Remediation:**
  - Sanitize and encode all user inputs and outputs.
  - Implement Content Security Policy (CSP) header

4. Application Flooding & Broken Authentication (High)

- **Description:**
  Brute-force testing with 100 common passwords revealed lack of account lockout and rate limiting, making the application susceptible to credential stuffing and DoS attacks1.





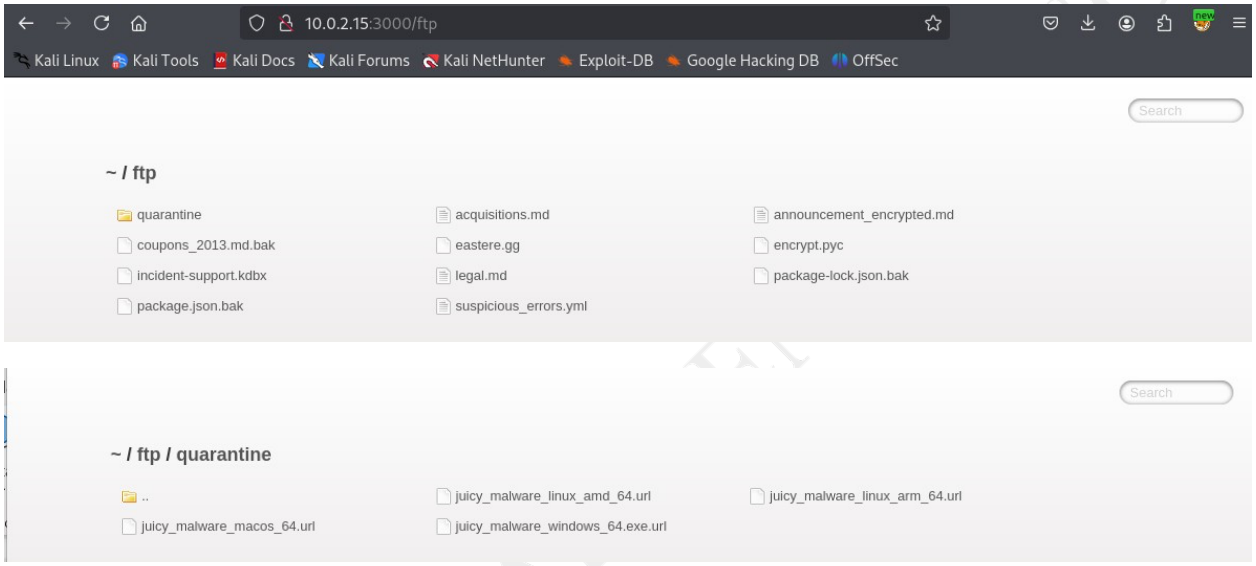
- **Business Impact:**
  Increased risk of unauthorized access and service disruption.

- **Remediation:**

- Implement rate limiting and account lockout mechanisms.
- Enforce strong password policies.

4.2 Security Misconfiguration (High)

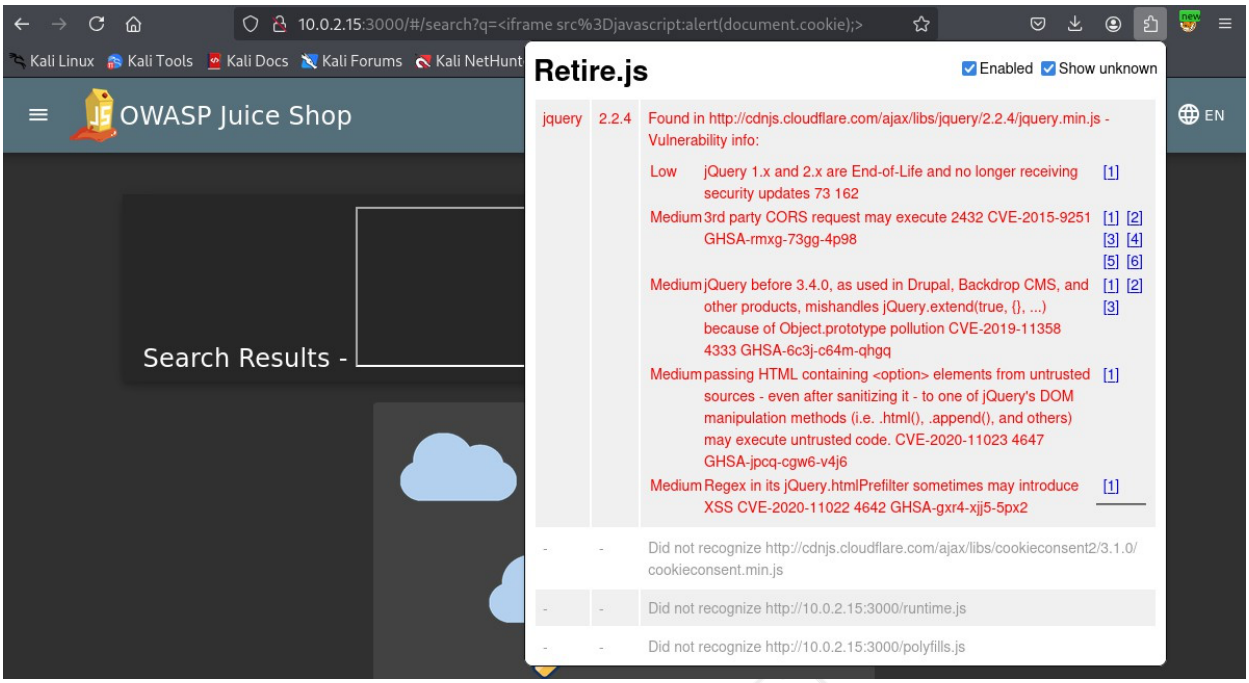
- **Description:**
  Directory listing was enabled, and insecure credentials were found, exposing sensitive files and configuration data.



- **Business Impact:**
  Attackers could discover and exploit hidden resources.
- **Remediation:**
  - Disable directory listing on the web server.
  - Secure all credentials and configuration files.

4.3 Vulnerable Open-Source Components (Medium)

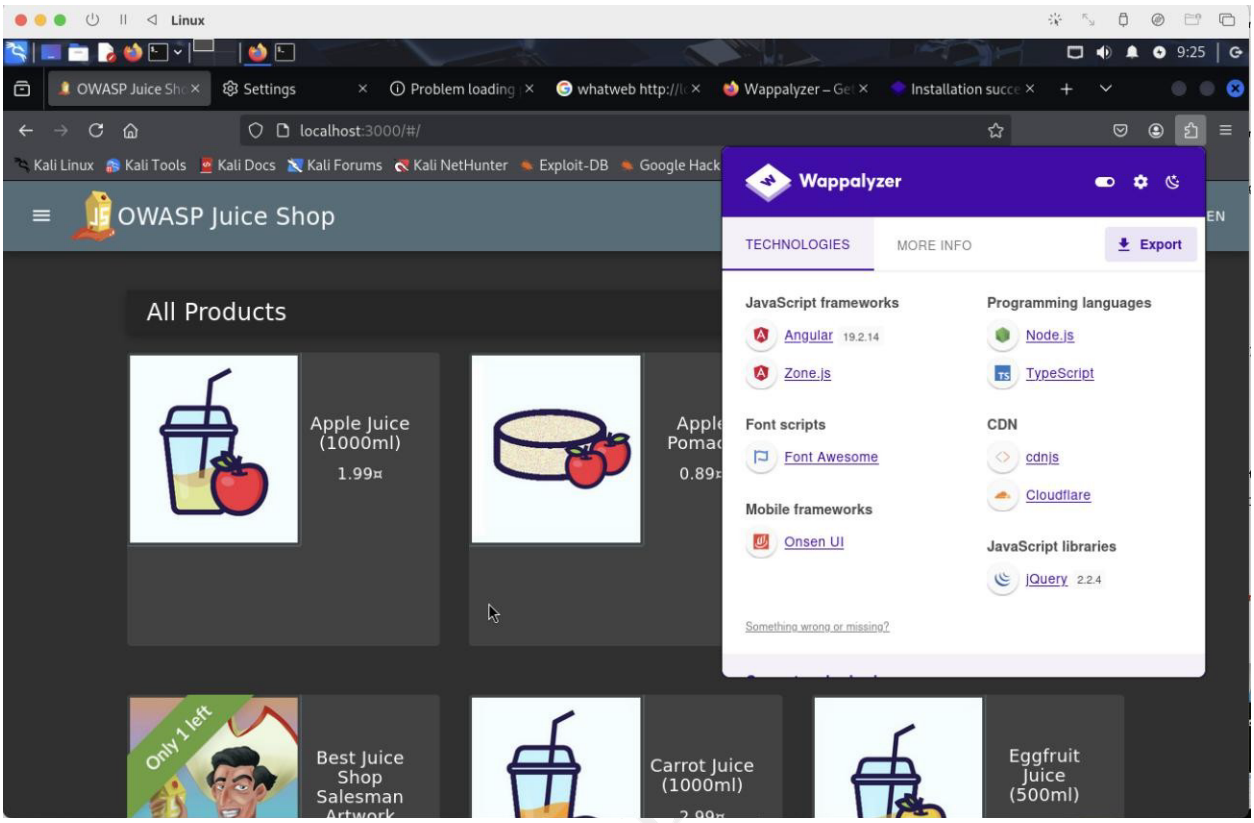
- **Description:**
  Retire.js identified outdated and vulnerable JavaScript libraries in use.



- **Business Impact:**
  Increases risk of exploitation via known vulnerabilities.
- **Remediation:**
  - Regularly update and patch third-party components.
  - Monitor vulnerability advisories for dependencies.

4.4 Technology Fingerprinting via Wappalyzer (Informational)

- **Description:**
  Wappalyzer identified backend technologies including AngularJS, Express.js, and Node.js, revealing the application stack architecture. This reconnaissance enables attackers to target version-specific vulnerabilities in identified components.



- **Business Impact:**
  Exposes potential attack vectors through known framework vulnerabilities.
- **Remediation:**
  - Obfuscate technology headers and disable unnecessary version disclosures.
  - Regularly audit dependencies for known vulnerabilities.

5. Appendix

5.1 Tools List

- Burp Suite Community Edition
- Wappalyzer
- Retire.js
- Common password lists (GitHub)

5.2 Limitations

- Burp Suite Community Edition has limited functionality; some automated attacks were restricted1.

- Testing was performed in a controlled environment; findings may differ in production.

6. Recommendations & Secure Code Snippets

- **SQL Injection:**
  Use parameterized queries.

javascript

// Example in Node.js with parameterized query

db.query('SELECT * FROM users WHERE email = ?', [userInput], callback);

- **XSS:**
  Sanitize user input and encode output.

javascript

// Example using DOMPurify for sanitization

const clean = DOMPurify.sanitize(userInput);

- **Authentication:**
  Implement account lockout and rate limiting.

javascript

// Example (pseudo-code)

if (failedAttempts > 5) lockAccount(userId);

- **Security Headers:**
  Add CSP and other headers.

text

Content-Security-Policy: default-src 'self'

7. Before-and-After Security Posture

Vulnerability	**Before (Status)**	**After (Mitigation)**
SQL Injection	Present	Parameterized queries

Reflected XSS	Present	Input/output sanitization
Broken Authentication	Present	Lockout, rate limiting
Directory Listing	Enabled	Disabled

Vulnerability	**Before (Status)**	**After (Mitigation)**
Vulnerable Components	Outdated	Updated

Conclusion:

The Juice Shop application exhibited several critical vulnerabilities. Remediation should prioritize SQL Injection and authentication flaws, followed by XSS and misconfigurations. Regular security assessments and secure development practices are essential to maintain a robust security posture.