
Project 2 :Mini Penetration Testing Report

Target Applications

- Damn Vulnerable Web Application (DVWA)
- OWASP Juice Shop

---

1. Executive Summary

A controlled mini penetration test was conducted on two intentionally vulnerable web applications: Damn Vulnerable Web Application (DVWA) and OWASP Juice Shop. The objective of this assessment was to identify common web application vulnerabilities using standard penetration testing methodologies and tools.

The testing included reconnaissance, scanning, directory enumeration, web server vulnerability assessment, and manual exploitation. Several critical and high-risk vulnerabilities were identified, including SQL Injection, Broken Authentication (Brute Force), Command Injection, Insecure Direct Object References (IDOR), information disclosure, and security misconfigurations. These vulnerabilities could allow attackers to gain unauthorized access, expose sensitive information, or execute system-level commands.

---

2. Scope & Methodology

2.1 Scope

- DVWA hosted locally on Apache (Port 80)
- OWASP Juice Shop hosted locally via Docker (Port 3000)
- Testing restricted strictly to local lab environment (127.0.0.1)

2.2 Methodology

The penetration test followed these phases:

- Environment setup
- Reconnaissance
- Scanning
- Directory enumeration

- Web server vulnerability assessment
- Vulnerability exploitation
- Vulnerability comparison
- Reporting and remediation

---

3. Reconnaissance & Scanning

3.1 Nmap Scan

Command Used:

nmap -sV -p- 127.0.0.1

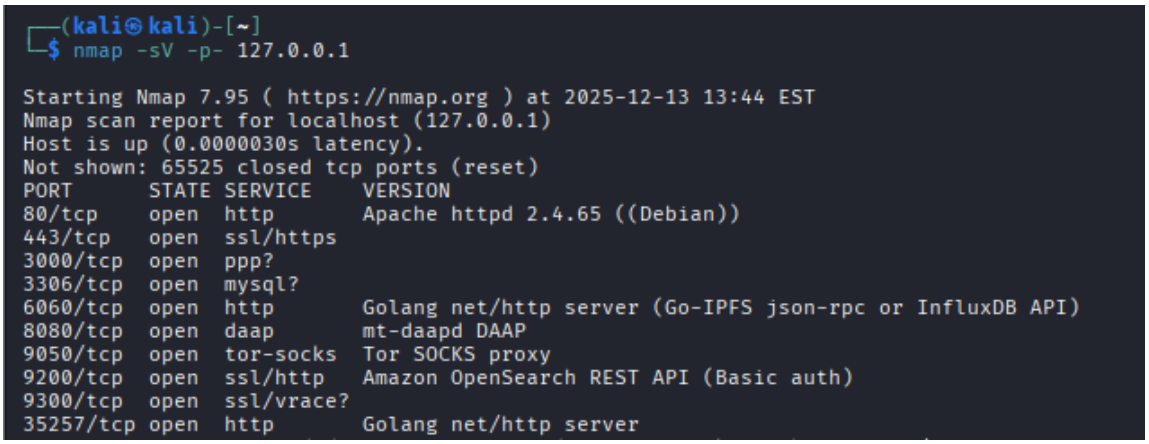
Purpose:
To identify open ports, running services, and service versions on the target system.

Findings:

Port	State	Service	Description
80	Open	HTTP	Apache 2.4.65 hosting DVWA
3000	Open	HTTP	OWASP Juice Shop

Note:
Other open ports identified during the scan were out of scope for this assessment and have been intentionally omitted to focus on the target applications.

Impact:
Exposed web services increase the attack surface and allow attackers to enumerate and exploit web-based vulnerabilities.



Nmap scan showing open HTTP services hosting DVWA and OWASP Juice Shop.

---

4. Web Server Vulnerability Assessment (Nikto)

4.1 Nikto Scan – DVWA

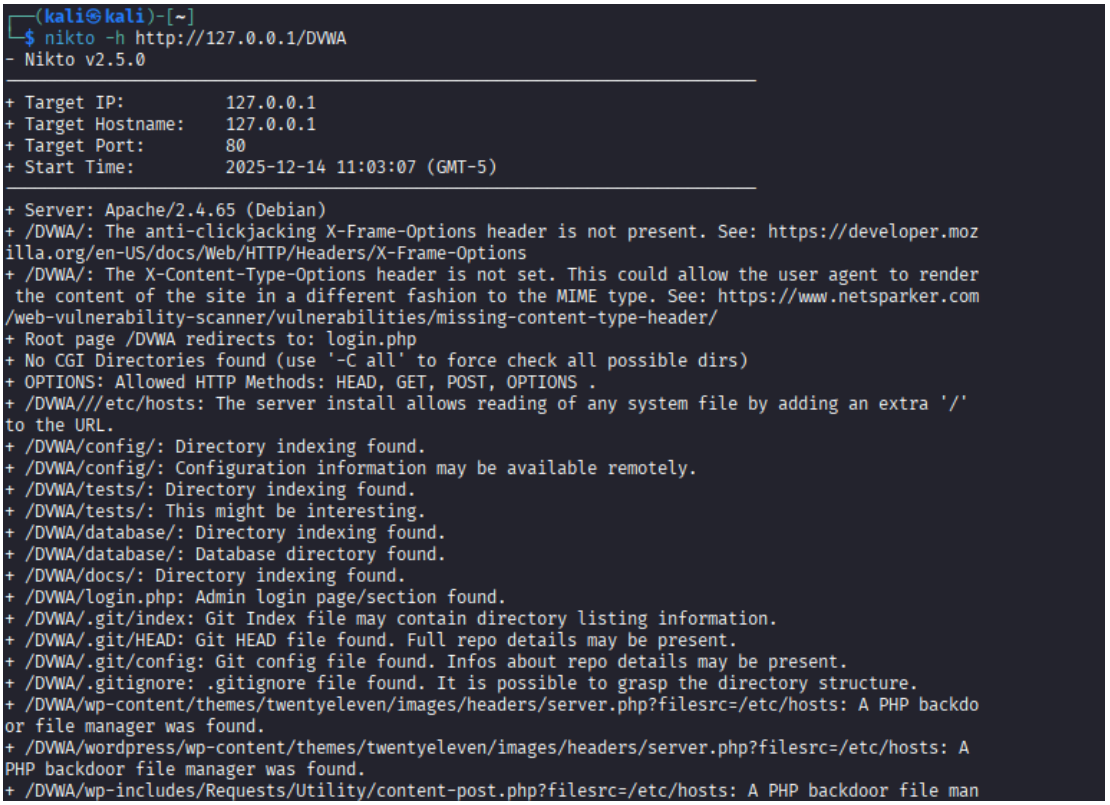
Command Used:

nikto -h http://127.0.0.1/DVWA

Findings:

- Missing security headers such as:
  - X-Frame-Options
  - X-Content-Type-Options
- Directory indexing enabled on sensitive directories:
  - /config/
  - /database/
  - /docs/
  - /tests/
- Exposure of sensitive files and resources:
  - .git repository files
  - Configuration and database directories
- Information disclosure due to insecure server configuration

Impact:
These issues could allow attackers to gather sensitive information, access internal files, and assist in further exploitation.



Nikto scan results showing missing security headers and exposed directories in DVWA.

4.2 Nikto Scan – OWASP Juice Shop

Command Used:

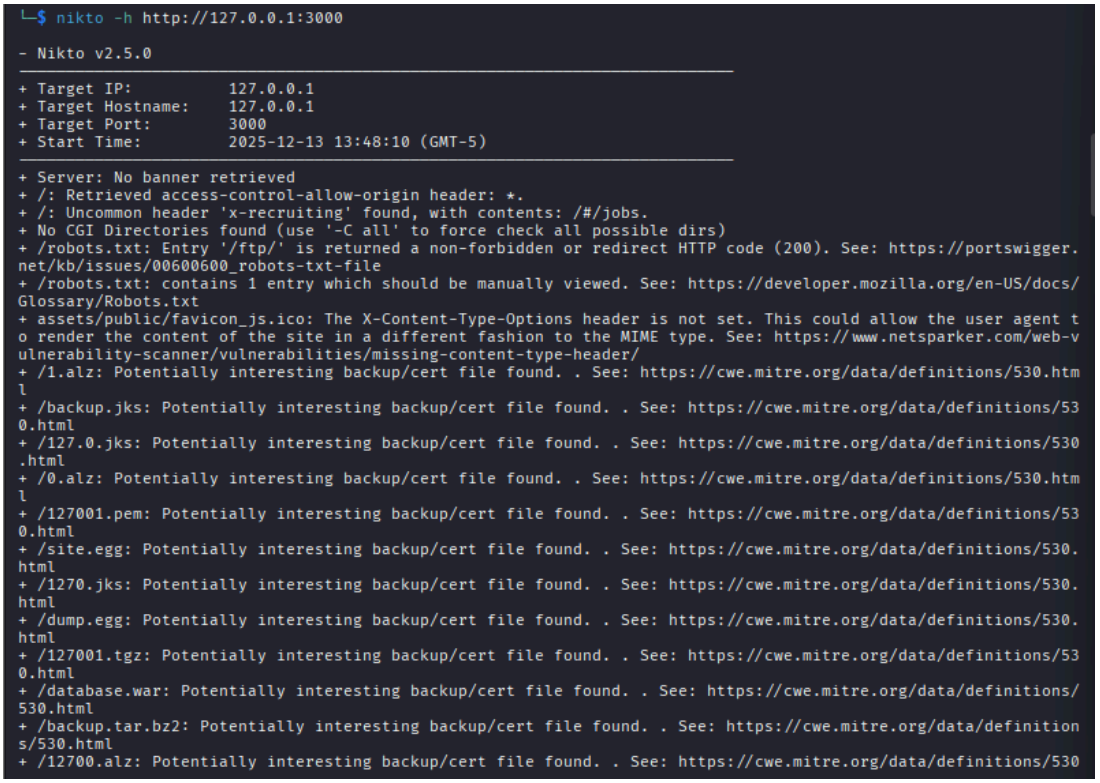
nikto -h http://127.0.0.1:3000

Findings:

- Missing recommended HTTP security headers such as:
  - X-Frame-Options
  - X-Content-Type-Options
- Information disclosure through HTTP response headers
- Identification of application framework and technologies in use
- No critical server-side vulnerabilities detected by Nikto, indicating that most flaws are application-level rather than server-level

Impact:

While no direct high-risk server misconfigurations were identified, missing security headers and information disclosure increase the attack surface and assist attackers during reconnaissance and exploitation phases.



Nikto scan results for OWASP Juice Shop highlighting missing security headers and information disclosure.

---

5. Directory Enumeration

5.1 DIRB Scan – OWASP Juice Shop

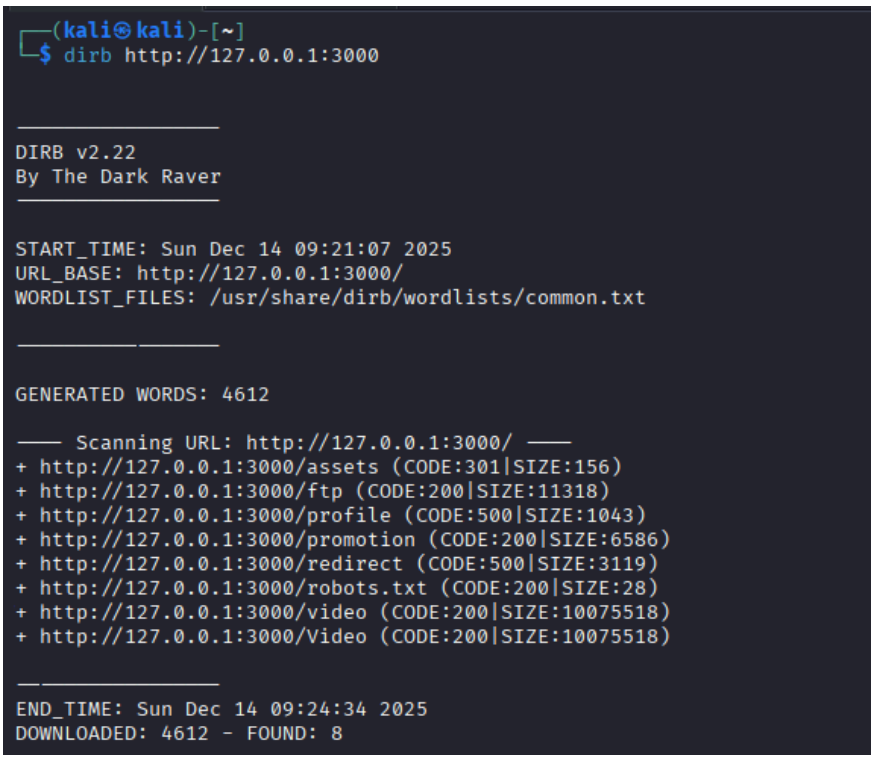
Command Used:

dirb http://127.0.0.1:3000

Findings:

- /ftp – Publicly accessible directory
- /robots.txt – Revealed internal paths
- /profile – Server error (500)
- /redirect – Possible open redirect
- /assets, /video – Exposed static resources

Impact:
Improper access control and information disclosure vulnerabilities were identified.



DIRB scan results for OWASP Juice Shop showing discovered directories.

5.2 DIRB Scan – DVWA

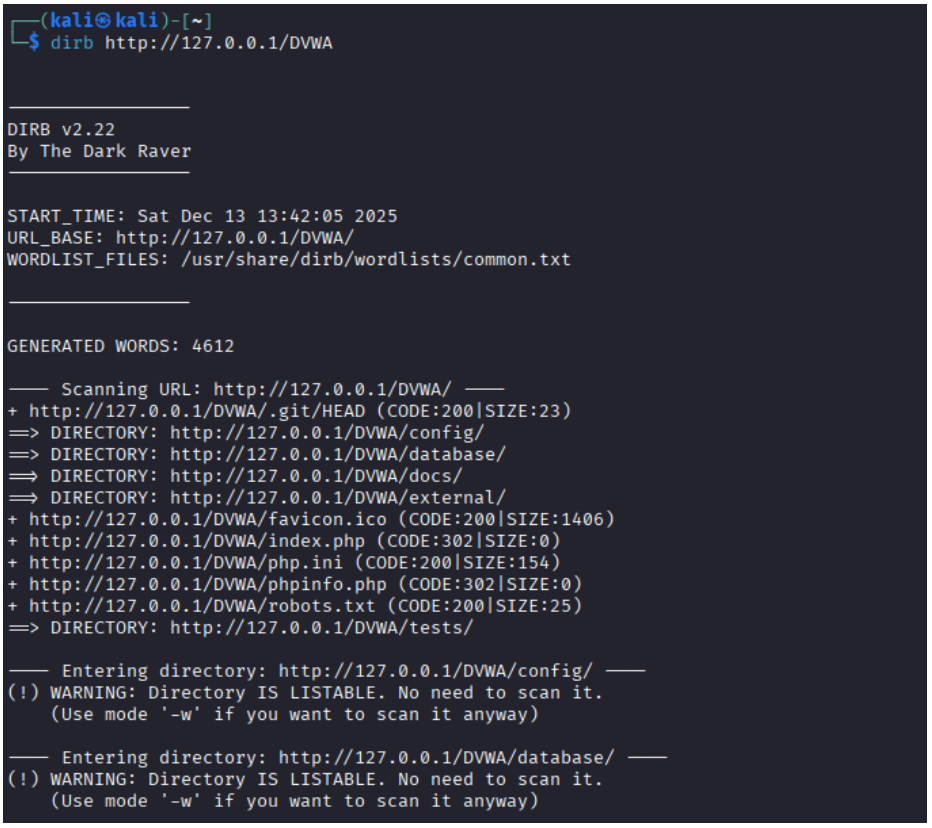
Command Used:

dirb http://127.0.0.1/DVWA

Findings:

- Directory listing enabled:
  - /config/
  - /database/
  - /docs/
  - /tests/
- Sensitive files exposed:
  - php.ini
  - phpinfo.php
  - .git directory

Impact:
These issues could lead to source code disclosure and leakage of sensitive configuration details.



DIRB scan results for DVWA showing exposed directories and sensitive files.

---

6. Vulnerability Assessment & Exploitation

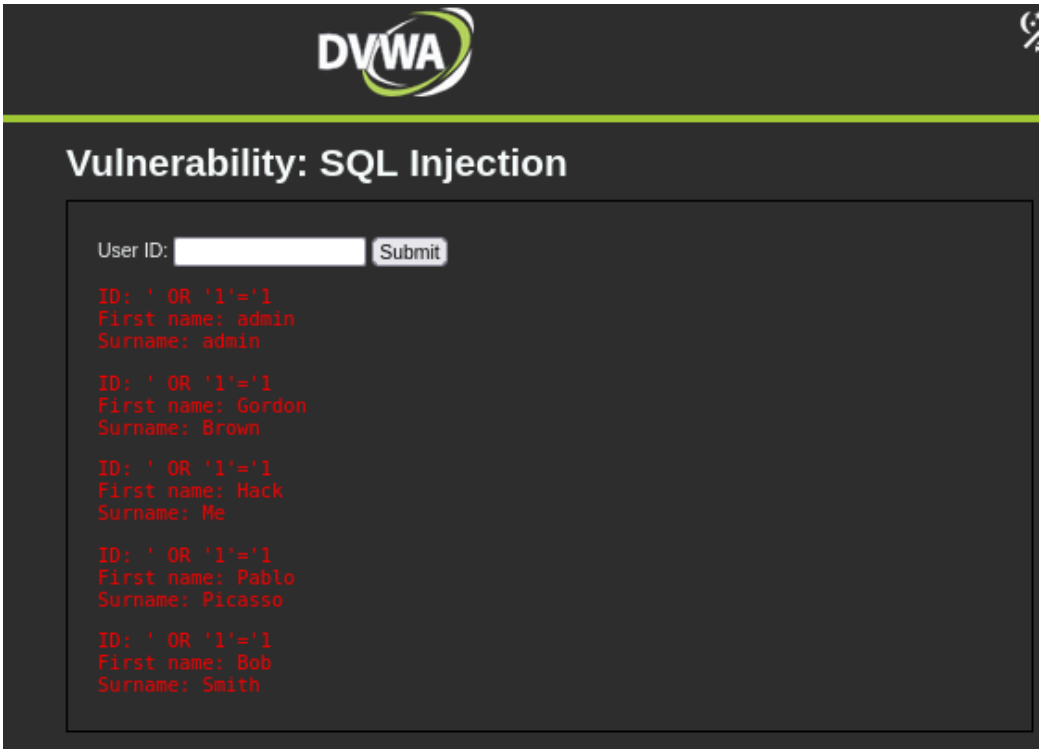
6.1 SQL Injection

- **Application:** DVWA

Payload Used:
' OR '1'='1

Result:
All user records were retrieved, including administrative accounts.

Impact:
Unauthorized access to database contents and potential full database compromise.



SQL Injection exploitation retrieving multiple user records.

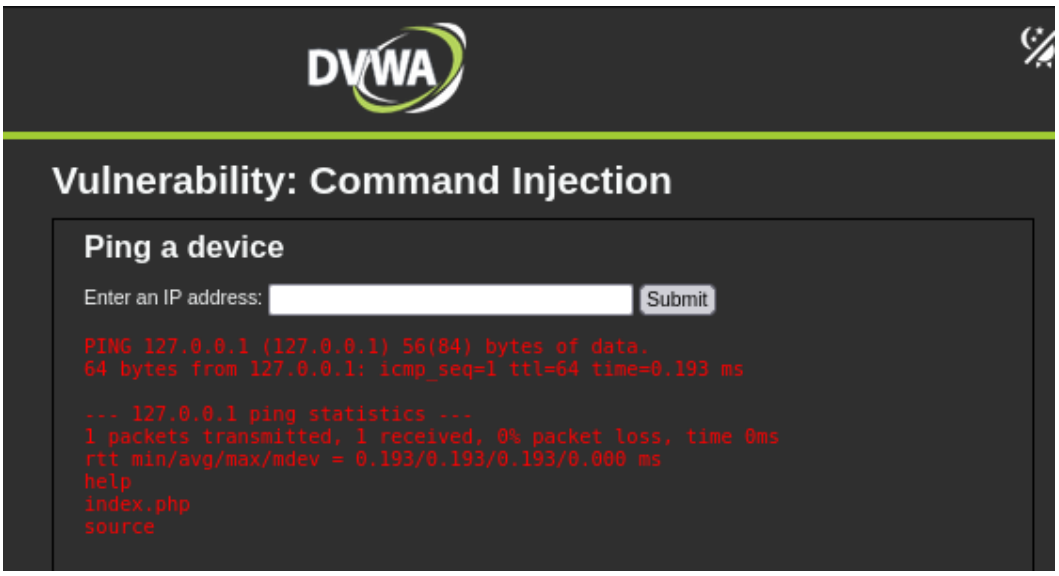
6.2 Command Injection

- **Application:** DVWA

Payload Used:
127.0.0.1 -c 3; ls

Result:
System command execution was successful.

Impact:
Remote command execution leading to complete server compromise.



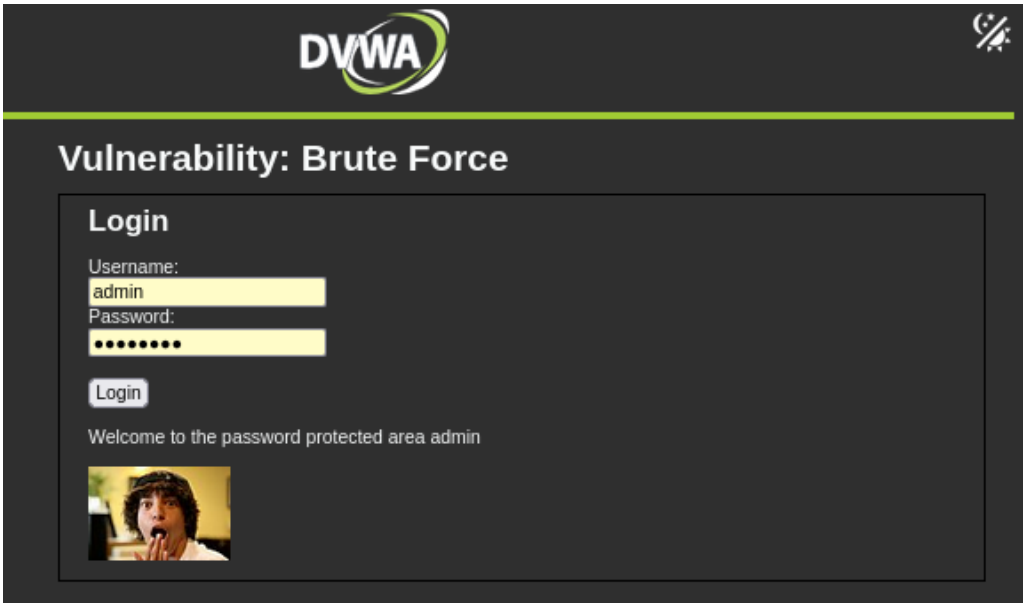
Successful command injection showing command execution output.

6.3 Broken Authentication (Brute Force)

- **Application:** DVWA
- **Credentials Used:**
  - Username: admin
  - Password: password

Result:
Admin login was successful due to lack of rate limiting.

Impact:
Unauthorized administrative access.



Successful brute force login to DVWA admin account.

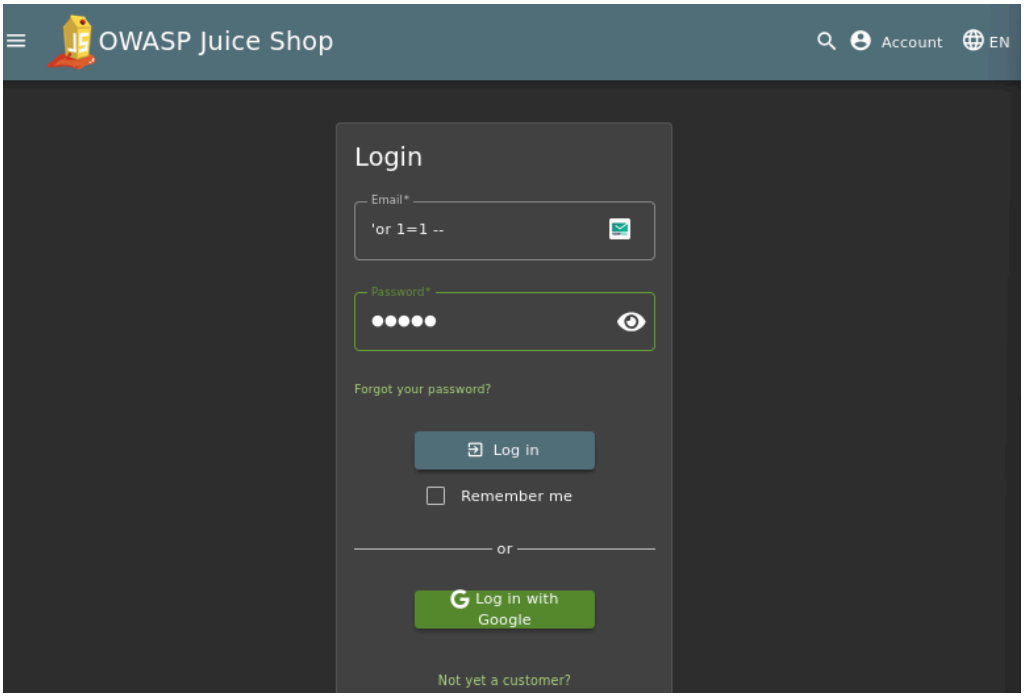
6.4 SQL Injection – OWASP Juice Shop

- **Application:** OWASP Juice Shop

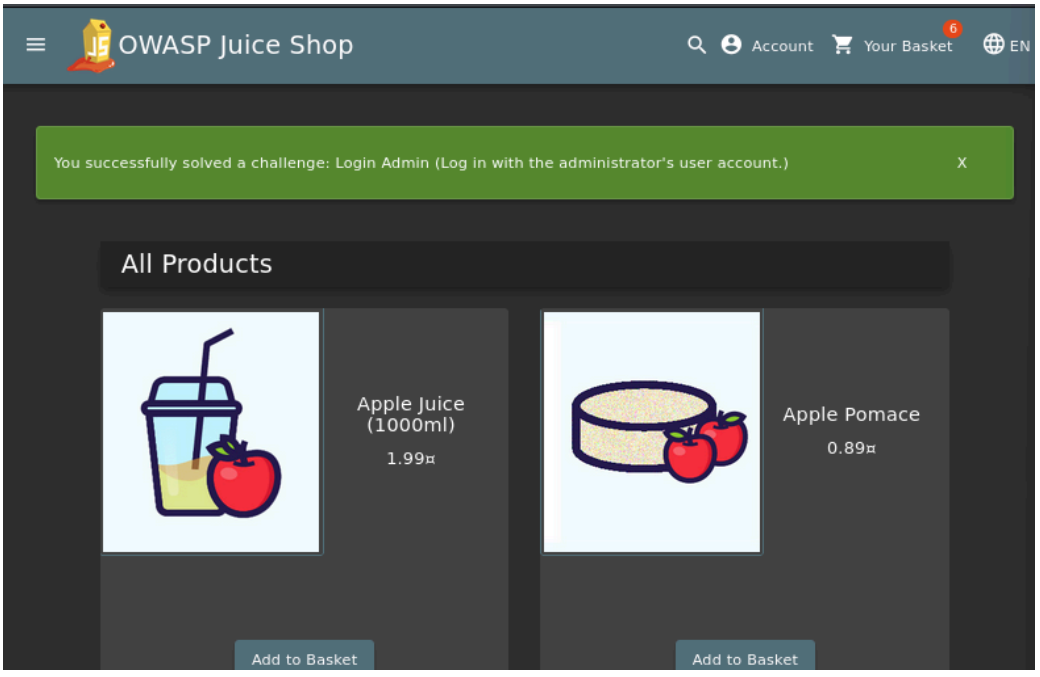
Payload Used:
' OR 1=1--

Result:
Authentication bypass was achieved.

Impact:
Account takeover and unauthorized access.



Authentication bypass using SQL Injection in OWASP Juice Shop



Logged in as Admin.

6.5 Insecure Direct Object Reference (IDOR)

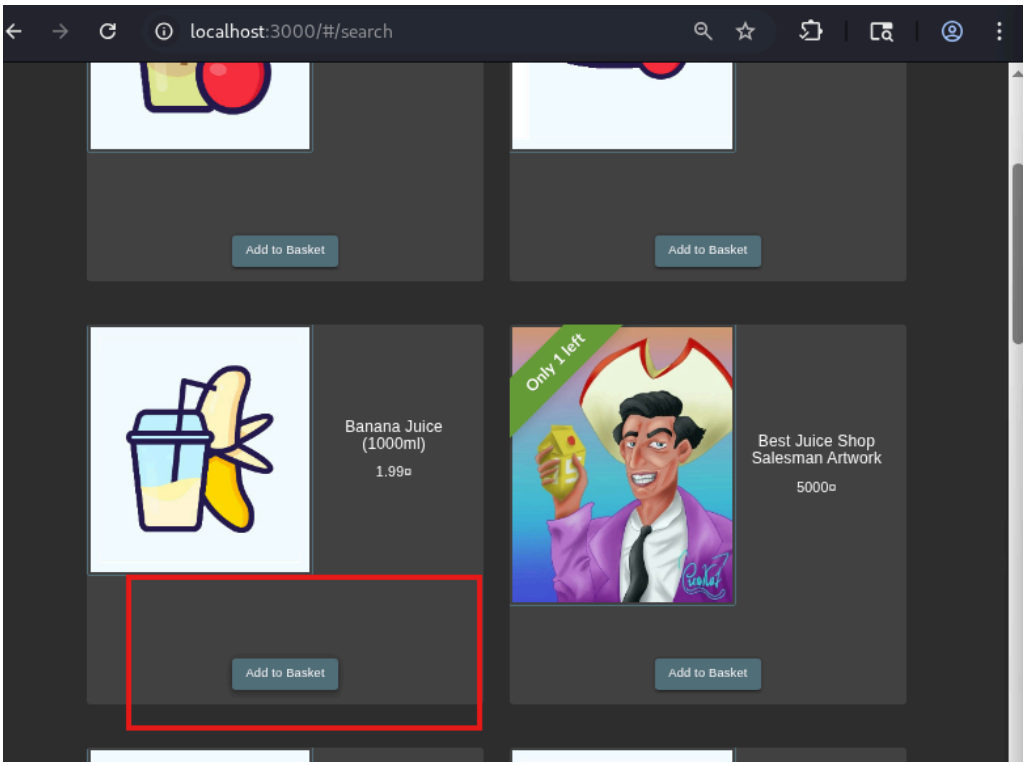
- **Application:** OWASP Juice Shop

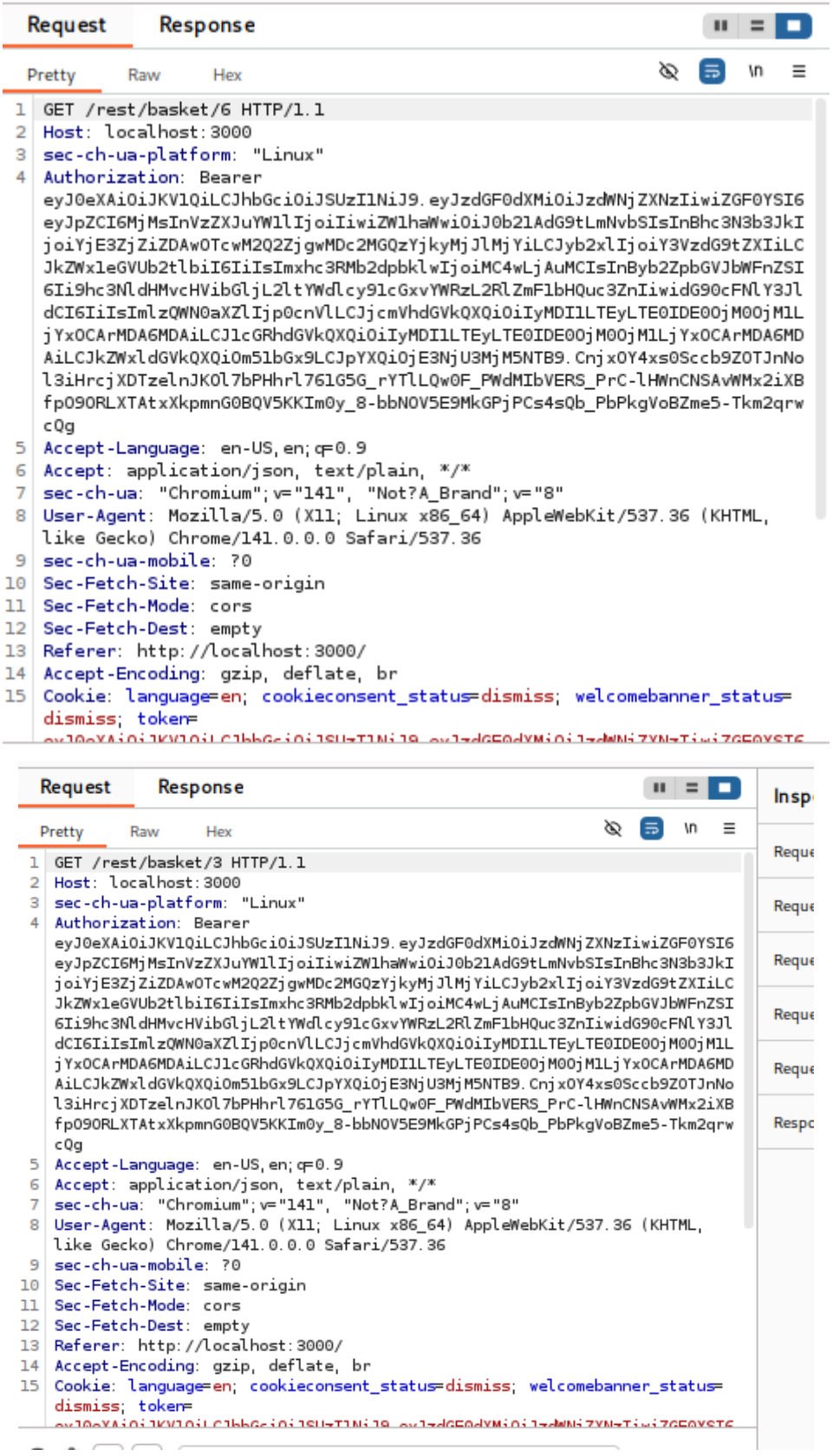
Tool Used:
Burp Suite

Technique:
The IDOR vulnerability was identified by intercepting and modifying HTTP requests using Burp Suite. Object identifiers (such as user IDs) within the intercepted requests were manually altered and forwarded to the server without proper authorization checks.

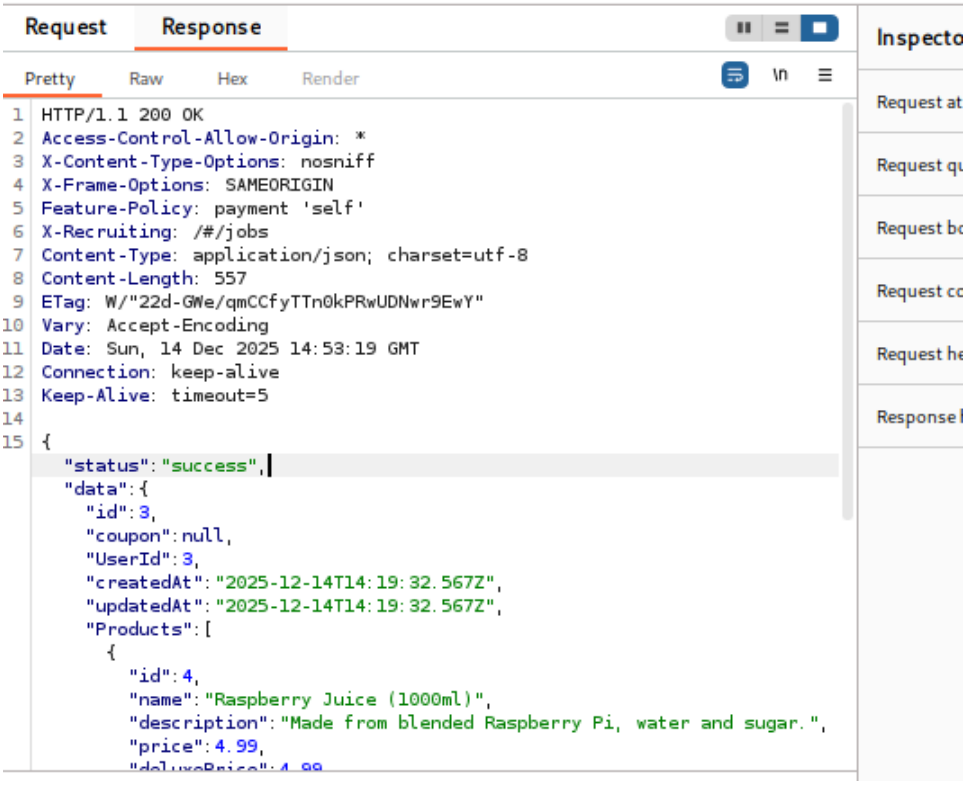
Result:
The application returned data belonging to other users without enforcing access control, confirming the presence of an Insecure Direct Object Reference vulnerability.

Impact:
This vulnerability allows unauthorized access to sensitive user information, leading to privacy violations, data exposure, and potential account compromise.





*Burp Suite request showing basket ID changed from **6 to 3**.*



*Server response returns **HTTP 200 OK** after basket ID modification.*

IDOR exploitation in OWASP Juice Shop using Burp Suite by modifying object identifiers in intercepted requests.

---

7. Vulnerability Comparison

Vulnerability	DVWA	OWASP Juice Shop
SQL Injection	✅	✅
Broken Authentication	✅	✅
Command Injection	✅	❌
IDOR	❌	✅
Information Disclosure	✅	✅

Observation:
DVWA focuses on direct, beginner-level vulnerabilities, while OWASP Juice Shop demonstrates real-world logical and access control flaws.

---

8. Remediation Recommendations

- Use prepared statements and parameterized queries
- Implement strong authentication controls and rate limiting
- Disable directory listing and remove sensitive files
- Validate and sanitize all user input
- Apply proper authorization checks for object access
- Enable security headers (CSP, HSTS, X-Frame-Options)
- Conduct regular security audits and code reviews

---

9. Conclusion

The mini penetration test successfully identified multiple critical vulnerabilities across both DVWA and OWASP Juice Shop. These findings demonstrate how weak input validation, insecure configurations, and poor access controls can lead to severe security risks. Implementing the recommended remediation measures will significantly improve the overall security posture of the applications.
