Lab 3: Web Application Security Fundamentals with OWASP Juice Shop

Course: FSCT 8540 – Network Security
Instructor: Dr. Maryam R. Aliabadi
Lab Duration: 3 hours

Learning Objectives

- Deploy a vulnerable web application in an isolated Docker environment.
- Configure an interception proxy to inspect and modify HTTP traffic.
- Exploit common web vulnerabilities aligned with OWASP Top 10.
- Analyze application-layer traffic at the network level.
- Explain mitigation strategies for observed vulnerabilities.

Background

Web applications are frequent targets of cyberattacks due to insecure design, misconfigurations, and weak input validation. OWASP Juice Shop is a deliberately vulnerable application designed for security education. Docker is used to ensure an ephemeral and safe testing environment.

Phase 1: Lab Environment Setup

1.1 Install Docker

Run the following commands in Kali Linux:

```
sudo apt update && sudo apt upgrade -y
sudo apt install -y docker.io
sudo systemctl enable docker --now
```

1.2 Deploy OWASP Juice Shop

Pull and run the official Juice Shop image:

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

Verify by visiting http://localhost:3000 in Firefox. You should see the OWASP Juice Shop storefront.

Phase 2: Interception Proxy Setup (Burp Suite)

Configure Burp Suite and Firefox using FoxyProxy to intercept HTTP traffic.

2.1 Launch Burp Suite

- Open **Burp Suite** from the Kali Applications menu.
- Select **Temporary Project → Use Burp Defaults → Start Burp**.

2.2 Configure Firefox with FoxyProxy

1. Install **FoxyProxy Standard** in Firefox.
2. Add a new proxy with the following settings:
    - Type: HTTP
    - IP Address: 127.0.0.1
    - Port: 8080
3. Enable the proxy using the FoxyProxy icon.

2.3 Install Burp CA Certificate

1. With the proxy enabled, visit:
   http://burp
2. Download the **CA Certificate**.
3. In Firefox:
    - Settings → Privacy & Security → Certificates → View Certificates
    - Authorities → Import
    - Trust the certificate to identify websites.

Phase 3: Lab Tasks

Task 1: Information Gathering (OWASP Security Misconfiguration)

Goal: Discover exposed resources and metadata through passive reconnaissance.

Steps:

1. In Burp Suite, ensure **Proxy → Intercept is OFF**.
2. Browse multiple pages of the Juice Shop application.
3. In Burp, go to **Target → Site Map**.
4. Right-click the Juice Shop host and select:
    - **Engagement Tools → Find References**.

Observe:

1. Hidden paths (e.g., /ftp, /api)
2. References to files like data.json
3. Developer comments or unused endpoints

Question1: Why is information disclosure dangerous even without authentication?

Task 2: SQL Injection (OWASP Injection)

Goal: Exploit improper input handling in authentication logic.

Steps:

1. Navigate to the **Login** page in Juice Shop.
2. In Burp, turn **Intercept ON**.
3. Enter any email and password, then click **Login**.
4. When Burp intercepts the request, modify the email field to:

' OR 1=1 --

5. Click **Forward**.

Question2: Explain how this input bypasses authentication**.**

Task 3: Network Traffic Analysis

Goal: Observe application-layer data at the network level.

Steps:

1. Launch Wireshark as root:

sudo wireshark

2. Select the **Loopback (lo)** interface.
3. Apply the display filter:

http

4. Perform an action in Juice Shop (e.g., add an item to the basket).

Observe:

1. HTTP headers
2. Cookies
3. Request URLs

Question 3: What sensitive information could an attacker extract if HTTPS were not used?

Phase 4: Cleanup

Stop and remove the Docker container:

```
sudo docker ps
sudo docker stop <Container_ID>
```

Ethics & Academic Integrity

This lab must only be conducted on the provided environment. Unauthorized attacks against real systems are illegal and unethical.

Learning Resources

- OWASP Juice Shop Official Documentation: https://owasp.org/www-project-juice-shop/
- Docker Documentation: https://docs.docker.com/
- Burp Suite Documentation: https://portswigger.net/burp/documentation
- Wireshark User Guide: https://www.wireshark.org/docs/wsug_html/
- FoxyProxy Browser Extension: https://www.foxyproxy.org /
- "Web Application Security Testing with OWASP Juice Shop" - Practical Guide (Book/Online Tutorials)

Deliverables

1. Short answers to Questions 1–3.
2. Screenshots showing:
    - Burp Site Map entries
    - Successful SQL injection login
    - Wireshark HTTP capture
3. A brief reflection (5–7 sentences) on how these vulnerabilities map to real-world attacks.

Submit items 1-3 in one pdf file through the Learning Hub in the following format:

File Name: Lab3-FirstName-Lastname-StdNo.PDF

Good luck!

Lab Grading Rubric (Total: 100 points)

Criterion	Points	Description
Environment Setup	15	Docker & Juice Shop deployed correctly and verified access. Full points if fully functional without errors.
Information Gathering	20	Hidden resources discovered and documented thoroughly. All relevant endpoints and files captured.
SQL Injection Exploit	20	Payload successfully executed; clear explanation of the mechanism and defenses.
Network Traffic Analysis	15	Correct filters applied; network traffic captured and analyzed with insightful observations.
Documentation & Reflection	20	Complete screenshots, answers to questions, and reflective summary connecting lab to real-world security issues.
Ethics & Compliance	10	Lab performed ethically; all instructions followed and no unauthorized systems tested.