WEB APPLICATION SECURITY REPORT

Title: JWT FORGERY EXPLOIT REPORT OSWAP JUICE SHOP

Submitted By:

Sushant Sudhakar Biranje

Role: Cyber Security Internship

Organization: Future Inters

Date of Submission: 09/07/2025

➢ OVERVIEW

Task : Web Application Security Testing. The task involved testing a sample web application for common vulnerabilities such as SQL injection, Burp Suit.

Target : HTTPS://DEMO.OWASP-JUICESHOP

➢ OBJECTIVE

The objective of this report is to demonstrate the exploitation of a vulnerability in the OSWAP juice shop application by forging by a JSON Web token to escalate Privileges.

This assessment aims to highlight the risks associated with insecure JWT implementation, Illustrate practical ethical hacking technique and provide actionable mitigation for securing token based authentication system.

➢ TOOL'S

- Kali Linux
- Burp Suit
- Firefox (web browser configured with Burp Proxy)
- Damn Vulnerable Web Application (DVWA)

➢ VULNERABILITY TESTING

❖ SQL INJECTION

✓ Inject malicious payload into user id : "1".
✓ Intercepted the request using Burp Suit.
✓ Bypass the Query.
✓ Successfully validated SQL injection.

❖ BURP SUIT

- ✓ Performed this attack using Burp Suit Intruder.
- ✓ The user name: “admin” is fixed, Testing multiple password.
- ✓ Successfully Login .

➢ OUTCOMES

- Logged in Successfully with the real password.
- Gained hands on experience in testing web application vulnerabilities.
- Learned to use SQL Injection, Burp Suit, XSS and Brut force.

➢ CONCLUSON

This assessment Successfully demonstrate a complete JWT forgery exploit chain in the OWASP juice shop application.