Web Application Security Testing
Task - 1

Internship Report

Submitted By: Priyanshu Shekhar

Cyber Security Intern: Future Interns

Learning Outcome:

Through this task, I gained hands-on experience in identifying and exploiting web application vulnerabilities like SQL Injection, Cross-Site Scripting, and Authentication Flaws using Burp Suite and DVWA. The internship helped reinforce key concepts in penetration testing, payload crafting, and interpreting HTTP responses

1. Task Overview

- Task: Conduct security testing on a sample web application to identify vulnerabilities like SQL Injection, XSS, and Authentication Flaws.
- Skills Gained: Web application security, ethical hacking, penetration testing.
- Tools Used: Burp Suite, DVWA (Damn Vulnerable Web Application), Kali Linux.

2. Environment & Tools Used

- Operating System: Kali Linux (VMware)
- Target Platform: DVWA (Damn Vulnerable Web Application)
- Proxy Tool: Burp Suite Community Edition
- Browser: Firefox (Burp-configured)

3. Vulnerabilities Tested

3.1 SQL Injection

Objective: Test for SQL Injection vulnerability in user ID parameter.
Payload Used: 1'--
Observation: Admin user details revealed in response.
Tool Used: Burp Suite (Proxy + Intercept)
DVWA Response: Displayed first name and surname for injected ID.

3.2 Cross-Site Scripting (XSS)

Objective: Identify reflected XSS vulnerability in input fields.
Payload Used: "><script>alert("XSS")</script>
Observation: JavaScript alert popup triggered in browser.
Tool Used: Burp Suite (Proxy)
DVWA Response: Executed script, confirming reflected XSS.

3.3 Authentication Flaws

Objective: Test login form against brute-force attacks.
Method: Burp Suite Intruder with password list.
Username: admin
Successful Password Found: "**password**"
Observation: Login successful after brute-force attempt.
Tool Used: Burp Suite Intruder