Web Application Security Testing – XSS & SQL Injection

Project Overview
This project focused on identifying and exploiting common web application vulnerabilities, specifically Cross-Site Scripting (XSS) and SQL Injection (SQLi). The exercises were performed in a controlled ethical hacking environment to demonstrate how attackers can compromise poorly secured web applications. **Steps Undertaken**

- Conducted penetration testing on simulated web applications.
- Tested forms and input fields for XSS vulnerabilities.
- Executed payloads to capture cookies and inject client-side scripts.
- Used Burp Suite to intercept, modify, and replay HTTP requests.
- Applied SQLMap to automate SQL injection testing.
- Attempted manual injection of malicious SQL queries in parameters and forms.
- Documented findings with evidence of exploitation.

Tools Used

- Burp Suite (interception & payload injection).
- SQLMap (automated SQLi testing).
- Kali Linux (penetration testing OS).
- Chromium (manual XSS testing).

Frameworks Applied

- OWASP Top 10 (A03:2021 Injection, A07:2021 Identification & Authentication Failures).
- Penetration Testing Execution Standard (PTES).
- NIST Cybersecurity Framework (Identify, Protect, Detect).

Skills Demonstrated

- Web application penetration testing.
- Exploiting XSS and SQL injection vulnerabilities.
- Payload crafting and encoding techniques.
- Manual vs automated vulnerability exploitation.
- Reporting and documenting vulnerabilities for stakeholders.