Web Application Penetration Testing – Vulnerability Assessment

Project Overview
This project focused on conducting a penetration test on a simulated web application environment. The aim was to identify critical vulnerabilities, exploit them ethically, and propose remediation strategies aligned with industry best practices. **Steps Undertaken**
- Performed reconnaissance and enumeration of the target host (semiregular.space).
- Conducted vulnerability discovery using both automated and manual testing methods.
- Exploited identified vulnerabilities to demonstrate real-world risks.
- Documented findings and provided recommendations for remediation.

Vulnerabilities Identified
1. SQL Injection – Extracted database schema and sensitive data.
2. Directory Enumeration – Discovered unsecured directories with sensitive files.
3. User Enumeration & Password Reuse – Weak credential practices across accounts.
4. Insecure Direct Object Reference (IDOR) – Accessed unauthorized user data.
5. Improper Access Control – Retrieved hidden account details.
6. File Upload Vulnerability – Uploaded disguised malicious files.

Tools Used
- Burp Suite (traffic interception and payload injection).
- Gobuster (directory enumeration).
- SQLMap (automated SQLi exploitation).
- Kali Linux (penetration testing platform).

Frameworks Applied
- OWASP Top 10 (2021): Injection, Broken Access Control, Identification & Authentication Failures.
- Penetration Testing Execution Standard (PTES).
- NIST Cybersecurity Framework (CSF): Identify, Protect, Detect, Respond.

Skills Demonstrated
- Web application penetration testing.
- Exploitation of SQL Injection, IDOR, and File Upload flaws.
- Payload crafting and execution.
- Risk analysis and vulnerability prioritisation.
- Clear technical reporting and remediation strategies.