Project Guide: Active Penetration Testing - SQL Injection on DVWA

1. Project Overview

This lab demonstrates an **Active Penetration Test** focused entirely on identifying and exploiting **SQL Injection (SQLi)** vulnerabilities within the **Damn Vulnerable Web Application (DVWA)** platform. The objective was to successfully exploit the application's database access layer at varying security levels to prove unauthorized data access and understand the impact of developer security choices.

Key Skills Demonstrated

- **Manual Exploitation:** Executing classical SQL Injection payloads (e.g., ' OR '1'='1) to bypass authentication and extract data.
- **Security Context Analysis:** Demonstrating the difference between a "Low" security setting (no defense) and a "Medium" setting (basic defense) and successfully circumventing the medium-level filter.
- **Remediation & Defense:** Providing specific, defense-focused recommendations, including the necessity of **Parameterized Queries** and strict **Input Validation**.
- **Risk Reporting:** Documenting the direct link between a successful exploit and critical business risk (unauthorized data access).

2. Target and Scope

- **Target:** DVWA running on a local, isolated virtual machine (192.168.163.130/dvwa/).
- **Scope:** Focused exclusively on the **SQL Injection** and related parameter tampering modules within DVWA.
- **Authorization:** The target is a designated training environment where explicit exploitation is encouraged and authorized.

3. Report Division and Purpose

Report File	Target Audience	Primary Focus
Formal_Report.md	Non-Technical Management, Executives	Business risk (Data Theft, System Access), high-level mitigation strategies.
Technical_Report.md	Security Engineers / Developers	Specific payloads, successful exploitation

		steps, and defensive code examples (e.g., using prepared statements).
Project_Guide.md (This file)	Peers, Hiring Managers	Project objective, detailed skill showcase, and methodology for active testing.