Day 47

Topic: SQL Injection

Objective: To understand and execute SQL Injection (SQLi) attacks to manipulate backend databases.

Theoretical Concepts:
SQLi occurs when user input is concatenated directly into a database query without sanitization. We discussed the impact: authentication bypass, data theft, and data deletion. We learned about In-band SQLi (Error-based) and Blind SQLi.

Practical Work:
We used the "DVWA" (Damn Vulnerable Web App) lab. 1. Manual: We entered *' OR 1=1 --* into a login field, successfully logging in as admin without a password. 2. Automated: We used **SQLmap** to dump the entire database. command: *sqlmap -u [url] --dbs*. We extracted the table names and column data containing dummy user passwords.

Tools Used: Burp Suite, SQLmap.

Outcome: Ability to detect and exploit SQL injection flaws to retrieve sensitive database information.