Day 27: SQL Injection and SQLMap

Topics Covered:

- Understanding SQL Injection
- Intro to SQLMap Tool

SQL Injection Definition:

An attack where attackers interfere with database queries. It's a very common and dangerous web vulnerability.

Objectives:

- Bypass logins
- Get sensitive data from the database
- Do unauthorized things like changing or deleting records

This attack tricks the database query into returning true, often skipping login checks.

SQLMap Definition:

An open-source tool for automating SQL injection detection and exploitation. This command scans a URL and lists database names if it's vulnerable.

Common SQLMap Options:

- `--tables`: Lists tables from a database.
- `--columns`: Lists columns from a table.
- `--dump`: Dumps data from a table.