Cybersecurity Daily Dairy

Day 27: SQL Injection and SQLMap

Date: July 19, 2025

Topics Covered:

- Understanding SQL Injection
- Introduction to SQLMap Tool

SQL Injection

Definition:
SQL Injection is a type of attack that enables an attacker to interfere with the queries that an application sends to its database. It is one of the most common and dangerous web application vulnerabilities.

Objectives:

- Bypass authentication mechanisms
- Extract sensitive data from the database
- Perform unauthorized actions such as modifying or deleting records

This payload tricks the backend SQL query into returning true, often bypassing login checks.

SQLMap

Definition:
SQLMap is an open-source penetration testing tool designed to automate the detection and exploitation of SQL injection vulnerabilities in web applications.

This command scans the specified URL and lists the names of the databases if the site is vulnerable.

Common SQLMap Options:

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