SQLMap

Saif Ansari

SQL Injection

- Injection or insertion of an SQL query from input data of web application
- Can read sensitive data from the database
- Can modify the database
- Execute operation on a database
- Quote from OWASP
  - "SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands"

https://www.owasp.org/index.php/SQL_Injection

SQLMap – What is it

- Penetration Testing Tool
- Developed in python
- Developed by Bernardo Damele and Miroslav Stampar
- Open source
- Part of the tools available in Kali Linux

SQLMap – Supported DBMS

- PostgreSQL
- MySQL
- Microsoft SQL Server
- Oracle
- SAP
- Microsoft Access
- IBM DB2

SQLMap - Features

- Can connect to database directly without a SQL injection using login details of the DBMS, among various other methods
- Can create table entries locally after extraction for readability
- Supports various SQL injection techniques:
  - Union query
  - Time based blind
  - Error based
  - Boolean based

https://github.com/sqlmapproject/sqlmap/wiki/Features

SQLMap Demo

- Go to /virtual
- Open the Kali Linux VM (ends with SQLMAP)
- Open the Ubuntu804Server (ends with SQLMAP)

SQL Injection Prevention

- Input Sanitization
- Prepared Statements
- Configure the DBMS based on the least amount of privileges to be handed out
- Do not pass errors to the user.