SQL MAPPING

Sqlmap is a python based tool, which means it will usually run on any system with python. Python comes already installed in Ubuntu. This is the same tool we use on our online sql injection test site.

SQLmap can be used to test and exploit SQL Injection, doing things such as extracting data from databases, updating tables, and even popping shells on remote hosts if all the commands are organized and next steps are scheduled.

What is SQL Injection Software?

SQL Injection is a code injection technique where an attacker executes malicious SQL queries that control a web application's database. With the right set of queries, a user can gain access to information stored in databases. SQLMAP tests whether a 'GET' parameter is vulnerable to SQL Injection.

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

Using SQLMAP to test a website for SQL Injection vulnerability:

Step 1: List information about the existing databases

Step 2: List information about Tables present in a particular Database

Step 3: List information about the columns of a particular table

Step 4: Dump the data from the columns

Features:

1. Full support for MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB and many more database management systems.
2. Full support for six SQL injection techniques: boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries and out-of-band.
3. Full support for six SQL injection techniques: boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries and out-of-band.
4. Support to enumerate users, password hashes, privileges, roles, databases, tables and columns.
5. Automatic recognition of password hash formats and support for cracking them using a dictionary-based attack
6. Support to dump database tables entirely, a range of entries or specific columns as per user's choice. The user can also choose to dump only a range of characters from each column's entry.
7. Support to search for specific database names, specific tables across all databases or specific columns across all databases' tables. This is useful, for instance, to identify tables containing custom application credentials where relevant columns' names contain string like name and pass.
8. Support to download and upload any file from the database server underlying file system when the database software is MySQL, PostgreSQL or Microsoft SQL Server.
9. Support to execute arbitrary commands and retrieve their standard output on MySQL, PostgreSQL or Microsoft SQL Server.

10. Support to establish an out-of-band stateful TCP connection between the attacker machine and the database server underlying operating system. This channel can be an interactive command prompt, a Meterpreter session or a graphical user interface (VNC) session as per user's choice.