SQL Injection Demonstration with DVWA & sqlmap

Introduction

This guide demonstrates how an SQL Injection attack can be carried out using Damn Vulnerable Web Application (DVWA) hosted on Metasploitable 2 and automated with sqlmap. It is intended solely for educational use to raise awareness of web vulnerabilities.

Legal and Ethical Notice

This demonstration must only be performed in a lab environment with explicitly authorized targets. Unauthorized use of these techniques on production systems is illegal and unethical.

Tools Required

- Metasploitable 2 VM (with DVWA installed)
- Kali Linux or Parrot OS (Attacker machine)
- Burp Suite (for intercepting HTTP requests)
- sqlmap (SQL injection automation tool)
- Web browser (Firefox or Chromium recommended)

Lab Setup Overview

1. Launch Metasploitable 2 and access DVWA via browser.
2. Use Burp Suite to intercept requests sent to the DVWA.
3. Run sqlmap using captured URL and cookie to automate SQL injection.

Step 1: Access DVWA

Open DVWA in your browser by navigating to http://<target-ip>/dvwa.

Step 2: Submit a Normal Query

Use the form to submit a user ID (e.g., ID=2) and verify functionality.

Step 3: Setup Burp Suite Intercept

SQL Injection Demonstration with DVWA & sqlmap

Open Burp Suite, enable Intercept, and set browser proxy to 127.0.0.1:8080.

Step 4: Capture the Request

Submit the form again and capture the HTTP request in Burp.

Step 5: Copy URL and Cookie

From Burp Suite, extract the URL and Cookie headers needed by sqlmap.

Step 6: Run sqlmap

Use sqlmap with the captured data:

sqlmap -u '<URL>' --cookie='<cookie>'

Step 7: Enumerate Databases

Add `--dbs` to discover available databases.

Step 8: Target DVWA Database

Use `-D DVWA --tables` to find tables inside the DVWA DB.

Step 9: Explore the Users Table

Use `-T users --columns` to list columns in the users table.

Step 10: Dump User Data

Use `--dump` to extract usernames and password hashes.

sqlmap -u '<URL>' --cookie='<cookie>' -D DVWA -T users --dump

Sample Credentials Extracted

These are typical results from an SQL Injection attack on DVWA:

SQL Injection Demonstration with DVWA & sqlmap

Username | Password

--------- | ---------

admin | password

gordonb | abc123

1337 | charley

pablo | letmein

smithy | password

Key Takeaways

- Always use input validation and sanitization.
- Never trust user input; use parameterized queries.
- Test your applications in controlled environments for vulnerabilities.
- Educate developers and security teams about injection risks.