Manual on Performing SQL Injection Using BurpSuite

Introduction

SQL Injection is a code injection technique that might destroy your database. It is one of the most common web hacking techniques. This manual will guide you through performing an SQL injection using BurpSuite.

Prerequisites

- Basic understanding of SQL and web applications.
- BurpSuite installed and configured.
- A vulnerable web application for testing (e.g., DVWA, bWAPP).

Steps to Perform SQL Injection Using BurpSuite

Step 1: Setting Up BurpSuite

1. **Launch BurpSuite**: Open BurpSuite and go to the "Proxy" tab.
2. **Configure Browser**: Ensure your browser is configured to use BurpSuite as the proxy. You can do this by setting the browser proxy settings to `127.0.0.1:8080`.

Step 2: Identifying the Vulnerable Input

1. **Navigate to Target**: Use the browser to navigate to the target web application.
2. **Find User Input Fields**: Look for user input fields such as login forms, search boxes, etc., where SQL queries might be executed.

Step 3: Intercepting the Request

1. **Enable Intercept**: In BurpSuite, under the "Proxy" tab, ensure the intercept is on.
2. **Submit Input**: Enter a basic input (e.g., `' OR 1=1 --`) in the target input field and submit it.
3. **Intercept the Request**: BurpSuite will intercept the HTTP request containing the input.

Step 4: Analyzing the Request

1. **Send to Repeater**: Right-click on the intercepted request and select "Send to Repeater."

2. **Modify the Request**: In the Repeater tab, modify the input parameters to include SQL injection payloads. For example, change `username=admin` to `username=' OR 1=1 --`.

Step 5: Executing the SQL Injection

1. **Execute the Request**: Click on "Send" in the Repeater tab to execute the modified request.
2. **Analyze the Response**: Check the response for any indications of successful SQL injection, such as bypassing login restrictions or accessing unauthorized data.

Step 6: Automating SQL Injection Detection

1. **Scanner**: BurpSuite Professional version includes a scanner that can automate the detection of SQL injection vulnerabilities. Navigate to the "Scanner" tab.
2. **Active Scan**: Right-click on the target site in the "Target" tab and select "Scan." Configure the scan settings to check for SQL injection.

Example: Exploiting a Login Form

1. **Initial Setup**:
    - Target: Login form with fields `username` and `password`.
2. **Basic SQL Injection**:
    - Input: `username=admin' --` and leave the password field empty.
3. **Intercept Request**:
    - Intercept the request and send it to Repeater.
4. **Modify and Send**:
    - Modify the request to include SQL payloads and send it.

Tips and Best Practices

- Always use SQL injection testing on legal and authorized applications.
- Use parameterized queries or ORM frameworks to mitigate SQL injection risks in your applications.

Conclusion

Performing SQL injection using BurpSuite involves identifying vulnerable inputs, intercepting and modifying requests, and analyzing responses. This manual provides a step-by-step approach to using BurpSuite for SQL injection testing.

Reference Link :- https://youtu.be/qf4Cr6n1l4w?si=amHsqVYIWEtmd5f4