**Lab 7- How to use Burp Suite to intercept client-side requests**

### 

**Objective:**Learn to use Burp Suite's local proxy feature to intercept, analyze, and manipulate client-side requests.

### **Key Concepts**

* **Burp Suite:** A penetration testing tool for web applications, particularly useful for intercepting and modifying web traffic between a client and a server.
* **Proxy Tab:** Allows traffic inspection and manipulation.
* **Intercept Mode:** Enables Burp Suite to capture requests before sending them to the server.

### **Lab Walkthrough**

#### **Task 1: Setting Up Burp Suite**

1. Launch Burp Suite in Kali Linux: burpsuite
2. Choose **"Temporary Project"** and click **Next**.
3. Select **"Use Burp defaults"** and press **"Start Burp"**.

#### **Task 2: Navigating the Interface**

1. Open the **Proxy** tab in Burp Suite.
2. Confirm **"Intercept is on"** mode is active (indicated by a colored button).
   * If intercepting is not required, toggle it off.

#### 

#### **Task 3: Configuring Burp with Firefox**

1. Go to the **Proxy** > **Options** tab.
2. Export Burp's CA Certificate:
   * Click **"Import/export CA Certificate"**.
   * Save the certificate with a **.der** extension to a location in the Kali VM.
3. Open Firefox and configure network settings:
   * Navigate to **Preferences** > Search for **Proxy**.
   * Select **Manual Proxy Configuration** and enter:
     + HTTP Proxy: 127.0.0.1
     + Port: 8080
4. Import the CA Certificate into Firefox:
   * Go to **Preferences** > **Privacy & Security** > **Certificates** > **View Certificates** > **Import**.
   * Select the .der file saved earlier.
   * Choose to trust Burp for both email and website interception.

#### **Task 4: Intercepting Traffic**

1. In Firefox, visit a test site such as:  
   <http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F>.
2. Ensure Burp Suite’s **Intercept** mode is ON.
3. Enter any username and password combination and click **Login**.
   * The page will remain in a loading state as Burp intercepts the request.

#### **Task 5: Analyzing and Modifying Requests**

1. In Burp Suite, view the intercepted request.
   * It contains the username and password parameters sent to the server.
2. Modify request data, e.g., change:
   * tfUName=admin
   * tfUPass=none
3. Press the **Forward** button to send the altered request to the server.
4. Observe the results in Firefox (e.g., accessing a new page if the credentials were valid).

### 

### **Takeaways**

* **Burp Suite Capabilities:**
  + Intercepting and manipulating requests provides insights into how web applications handle client-server interactions.
  + Detects potential vulnerabilities like weak authentication mechanisms.
* **Use Cases:**
  + Testing for SQL injection, XSS, and other vulnerabilities.
  + Bypassing authentication by manipulating requests.
* **Ethical Considerations:**
  + Ensure permission is granted before testing any systems.
  + Use tools like Burp Suite responsibly within legal and ethical boundaries.

This lab demonstrated the practical application of Burp Suite’s proxy feature, a critical skill for web application penetration testers.