Assignment: Web Application Security Testing

1. Spidering the Target Site

- **Step 1**: Open Burp Suite.
- **Step 2**: Go to the site http://testphp.vulnweb.com.
- **Step 3**: In Burp Suite, go to the **Target** tab and add the site to the scope.
- **Step 4**: Go to the **Spider** tab and start spidering the target site.

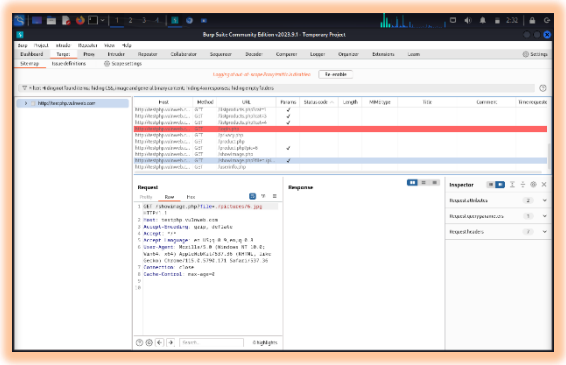
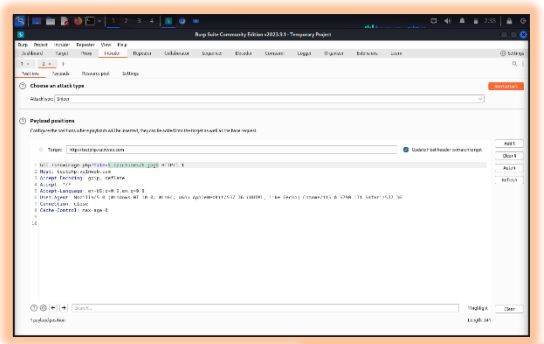
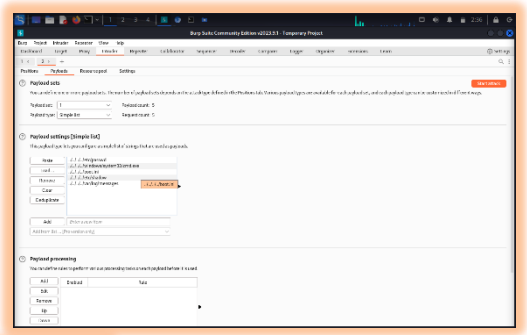


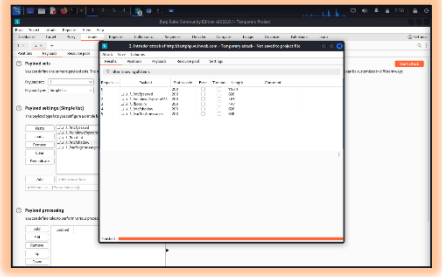
Figure 1

2. Intruder Attack on Parametric URLs

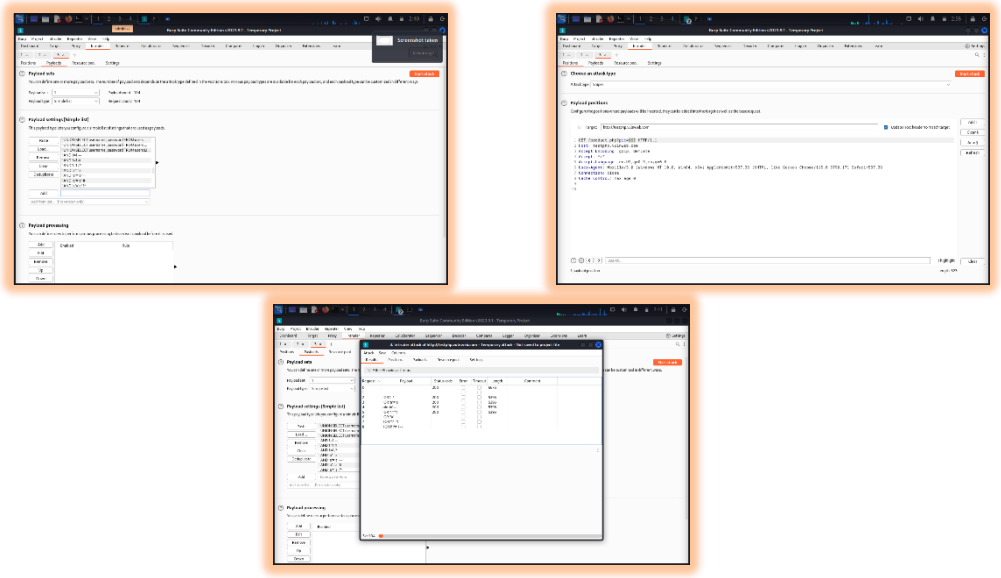
- **Step 1**: After spidering, I select two different urls for parametric attack, One for directory traversal and other for SQL Injection
- **Step 2**: Right-click on the request and send it to **Intruder**.
- **Step 3**: Set the payload positions and choose payloads for SQL Injection and Directory Traversal.
    - ✓ **Directory Traversal Payload**:





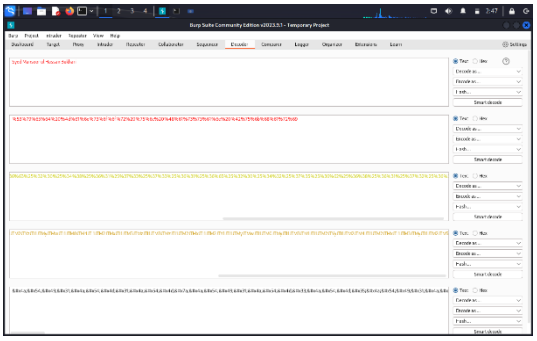


- ✓ **SQL Injection Payload**: 1' OR '1'='1

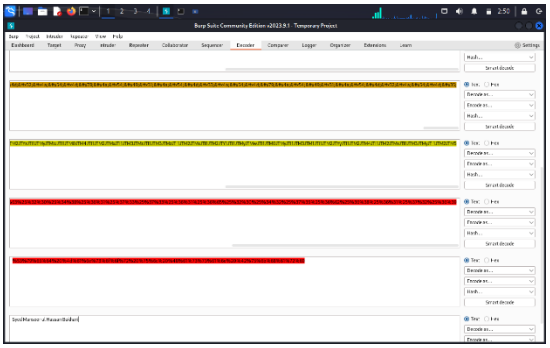


3. Encoding and Decoding in Decoder

- **Step 1**: Go to the **Decoder** tab in Burp Suite.
- **Step 2**: Write your name.
- **Step 3**: Perform the following encodings:
  - **2x URL Encoding**
  - **1x Base64 Encoding**
  - **1x HTML Encoding**
- **Step 4**: Decode in reverse order



Encoding



Decoding

4. HTTP Request Methods with Body Message

- **HTTP Request Methods**: The HTTP methods that can have a body message include:
  - ➢ **POST**
  - ➢ **PUT**

- **PATCH**
- **DELETE**