VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

CSE3501 INFORMATION SECURITY ANALYSIS AND AUDIT
EXERCISE – 5

DATE: 20.09.2020

Installing, Understanding and Exploring the functionalities of Burp Suite

www.portswigger.net **-Community Edition**

Use inside Kali Linux installed in VMWare

A. Confirm Whether Burp Proxy Listener is Active

- Open Burp → Select Temporary project → Use Burp defaults
- Navigate to the proxy → **Options** tab
- Verify that the proxy listener is active and set to 127.0.0.1:8080

B. Configure Proxy in Web Browser

For Firefox:

- Navigate to **Preferences**
- Search "proxy" → Go to **Connection Settings**
- Turn on **Manual proxy configuration**, set to the same proxy as Burp (127.0.0.1 on Port 8080)

Exercises:

1. **Intercept the browser HTTP traffic**
    - Open the web browser (Internet Explorer, Firefox, Chrome)
    - Modify the web browser connection properties and set the proxy web's address and port (e.g. address 127.0.0.1 port 8080)
    - Open Burp Suite
    - Try to navigate on a http page (e.g. demo.testfire.net) with the web browser and analyze the intercepted traffic with the application you chose.
2. **Intercept the browser HTTPS traffic**
    - Open the web browser (Internet Explorer, Firefox, Chrome)
    - Modify the web browser connection properties and set the proxy web's address and port (e.g. address 127.0.0.1 port 8080)
    - Try to navigate on a https page (e.g. https://www.google.com) with the web browser and analyze the intercepted traffic.

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

CSE3501 INFORMATION SECURITY ANALYSIS AND AUDIT
EXERCISE – 5

DATE: 20.09.2020

- Installing Burp SSL Certificate

  A. Download certificates:

  - Navigate to http://burp
  - Download the certificate by clicking the **CA Certificate** on the right.

  B. Import certificates to browser.

  For Firefox:

  - Navigate to **Settings**
  - Search "certificates" → Open **Certificate Manager → Authorities**
  - Import the certificate you downloaded and checkmark all the boxes.

- Open Burp Suite
- Try to navigate on a https page (e.g. https://www.google.com) with the web browser and analyze the intercepted traffic.

3. **Use a Proxy Switcher : Foxyproxy Plugin**
   - Download and install foxyproxy plugin for Firefox browser (Standar Version)
   - Switch between Burp Suite and Foxyproxy - Show the usage via Fixyproxy

   a. https://null-byte.wonderhowto.com/how-to/use-burp-foxyproxy-easily-switch-between-proxy-settings-0196630/

   b. https://medium.com/@futaacmcyber/setting-up-burpsuite-for-your-web-penetration-testing-1657fa670304

4. **Burp Repeater**
   - Browse a login page in the Firefox (Mind that Intercept is on)
   - Open Burpsuite and Right Click and choose Send to Repeater option
   - Goto Repeater tab and investigate the request and response tabs of each of the page request.

5. **Burp Target Scoping**

   a. Perform Target Scoping using Burp Suite oprions

http://codegrazer.com/tutorial/burp-tutorial-beginner.html#target