Hands on learning – Burp Suite Community Edition.

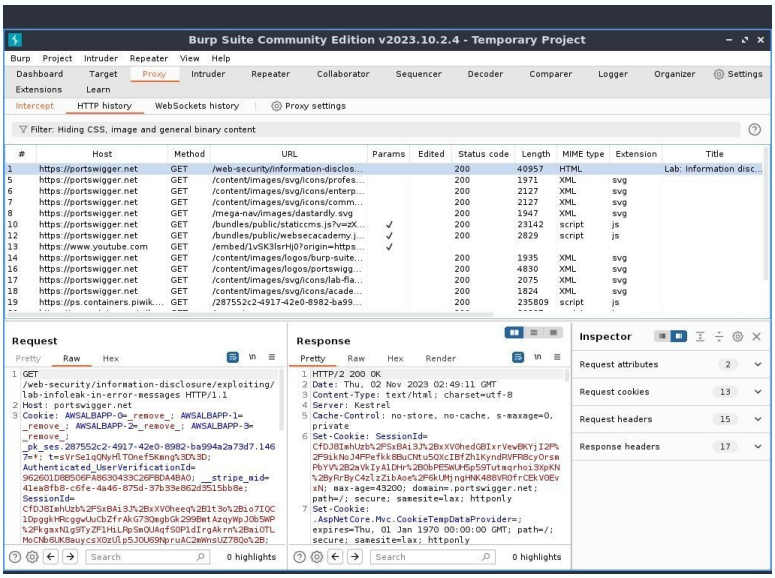
1. I installed Burp Suite on my Lubuntu Linux OS:

- https://portswigger.net/burp/documentation/desktop/getting-started/download-and-install
- save the .sh file to selected folder (I created one for Linux Addons) and run (install) using
    - "cd LinuxAddons"
    - "sudo bash burpsuite_community_linux_v2023_10_2_4.sh"

2. Once Java and the Burp Suite Community Edition were installed I logged out and back on to update the files.

3. Burp Suite has several hands on tutorials and labs under the learn option:

1. The first tutorial uses Burp Suite to intercept http traffic from a vulnerable shopping website and enables you to change the price in the shopping cart item from $1,337 to 1 cent!
2. The next set of tutorials captures and examines the web traffic and uses the repeater option to allow us to send different values to the web server and observe the response.
    1. The lab example shopping site used integer numerical values and correctly processed the data even if the integer was out of scope. HOWEVER, fractional decimal values and text values were not handled securely by the website and it verbosely revealed internal information including the fact that it used an Apache server and the exact version of the server.



3. In another exercise I was able to use Burp Suite to retrieve the contents of the “etc/passwd” file from a website to server query by hijacking the “GET filename= ” and inserting “../../” with the file traversal technique.

4. Vertical and horizontal access control vulnerabililities allowed me to delete a user from the administrator panel. First I appended “/admin” to the site URL but when that did not work I tried the “/robots.txt” to see which subfolders were disallowed. The key entry was “/administrator-panel” instead of “/admin”. Once I accessed the subdirectory I was able to delete the user.