Burp Suite Professional 2023 Installation Guideline for Kali Linux

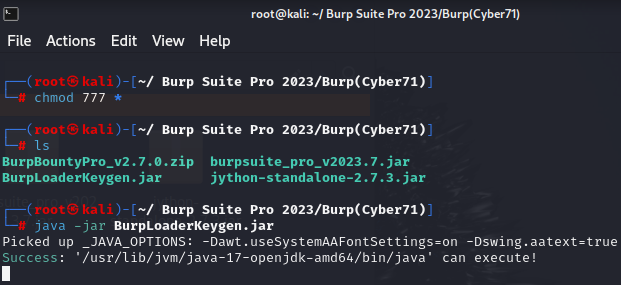
# Installation

1. File name: Burp(Cyber71)-20230726T032814Z-001.zip
2. Open kali Linux.
3. Create a new folder in /root, i.e., “Burp Suite Pro 2023”.
4. Paste and extract the zip file to “Burp Suite Pro 2023” folder.
5. Open terminal to “/root/ Burp Suite Pro 2023/Burp(Cyber71)”.
6. Give 777 (read, write and execute) permission to all the files:

>> chmod 777 \*

1. Run BurpLoaderKeygen.jar

>> java -jar BurpLoaderKeygen.jar

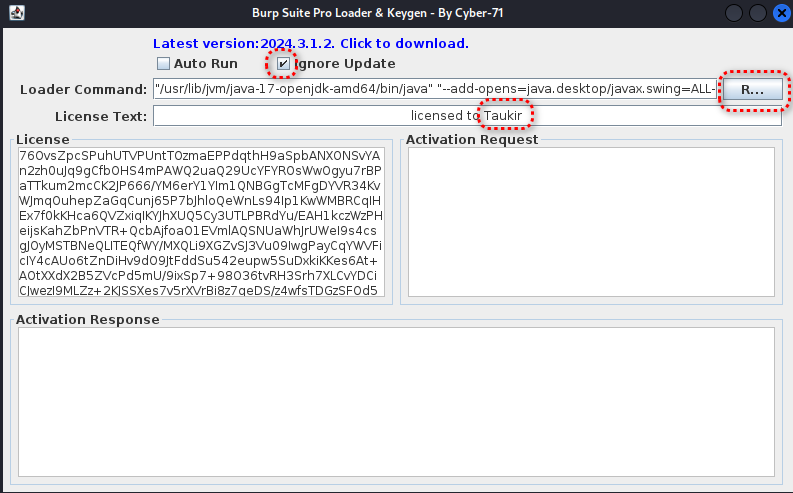


1. Then the following window will appear:

Here, change 2 options:

1. Check the “Ignore Update”.
2. Change the License owner name (optional).

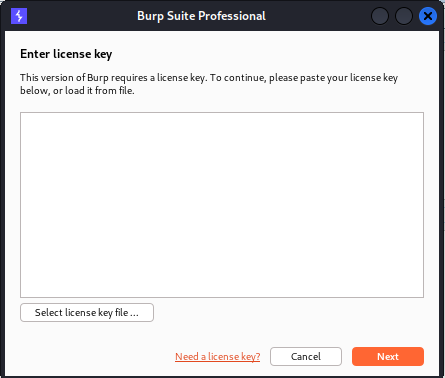
Then Run the program.



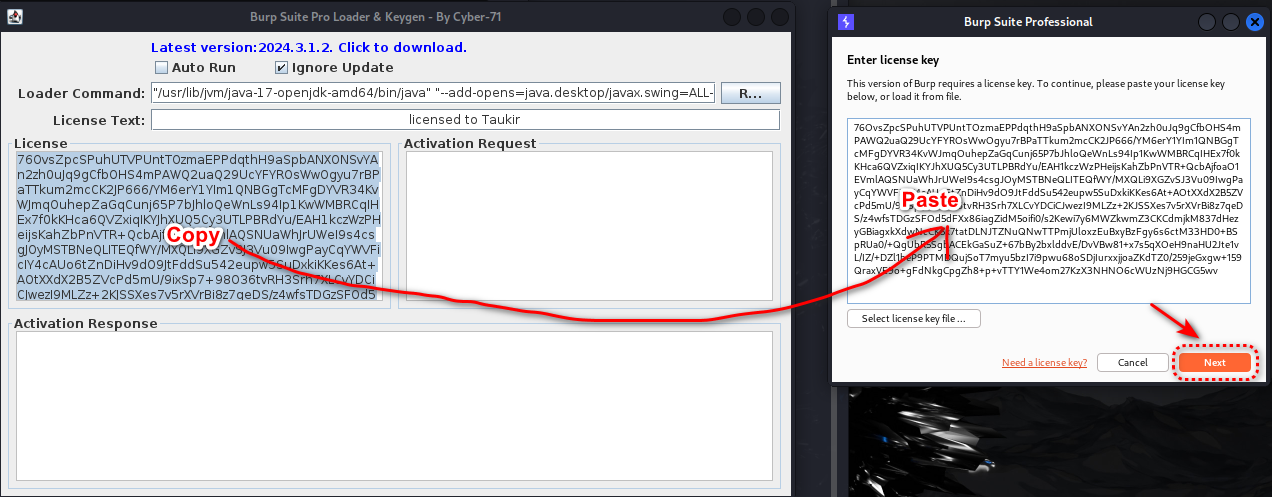
1. Then follow accordingly:

|  |  |
| --- | --- |
|  |  |

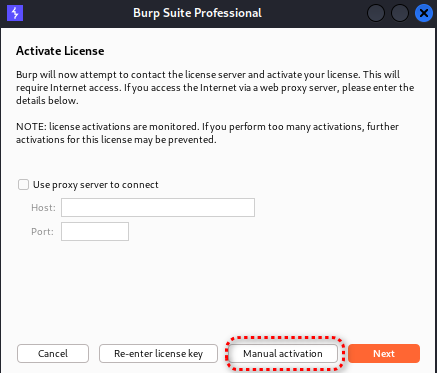
1. License key window will appear:



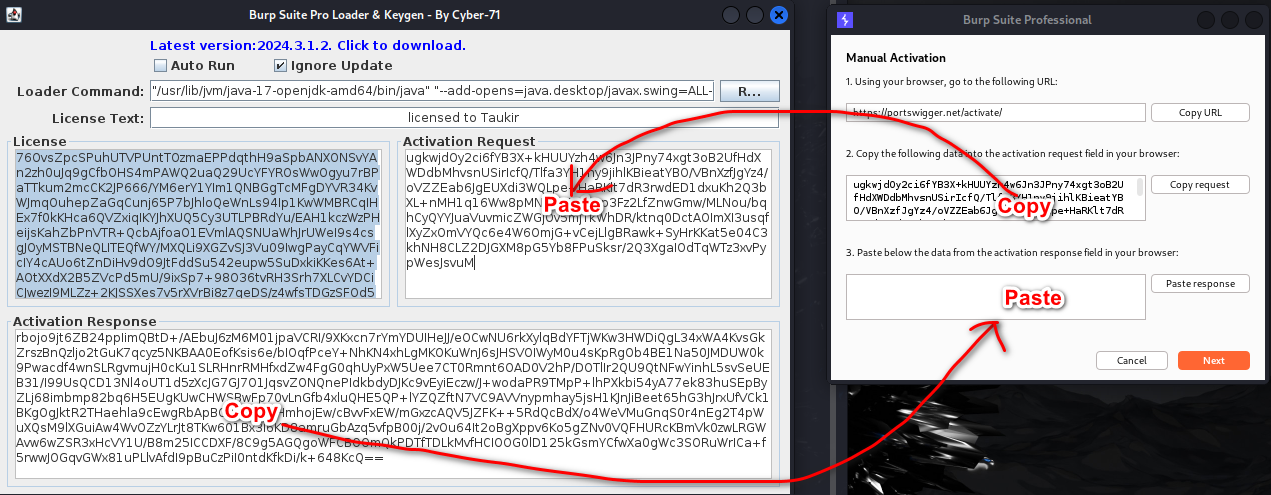
1. Follow accordingly:



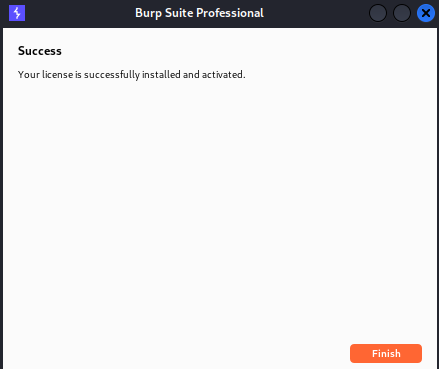
1. Click on “Manual activation”.



1. Follow accordingly:



1. Click on Next and the license will be successfully installed.



1. Now open a Temporary Project.

|  |  |
| --- | --- |
|  |  |
|  | |

1. Now close Burp Suite.
2. To run it again, we need to go to “/root/ Burp Suite Pro 2023/Burp(Cyber71)” and run the following command again:

>> **java -jar BurpLoaderKeygen.jar**

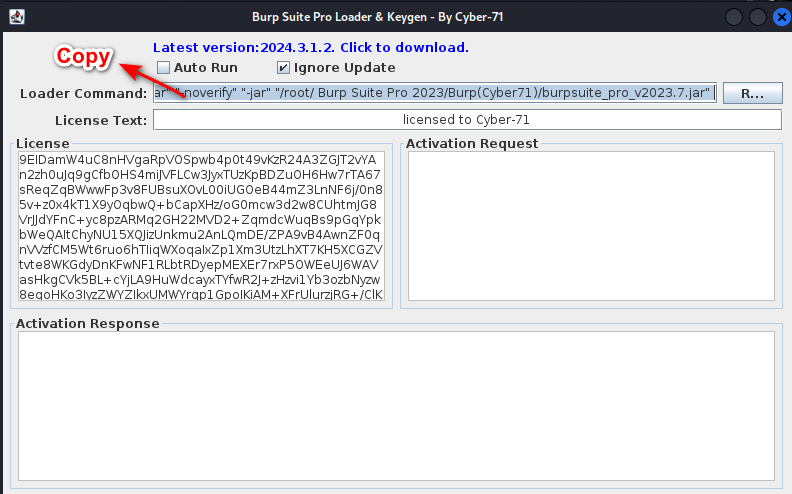
1. This starting process is not convenient. So we need to start a launcher for Burp Suite for easy opening.

# Creating Launcher for Burp Suite

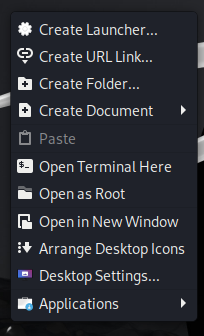
1. Go to “/root/ Burp Suite Pro 2023/Burp(Cyber71)” and create a document named “RunBurp.sh”
2. Now run Burp Suite pro 2023 with terminal using the following command:

>> **java -jar BurpLoaderKeygen.jar**

Copy the “Loader Command”.



1. Then paste the loader command to **RunBurp.sh** and save it.
2. Now in terminal, give executable permission to **RunBurp.sh** with the following command  
   >> chmod +x RunBurp.sh
3. And run Burp Suite  
   >> ./RunBurp.sh
4. If it opens Burp Suite then go to browser and download an icon of Burp Suite.
5. Go to Desktop. Right click and click on “Create Launcher”.

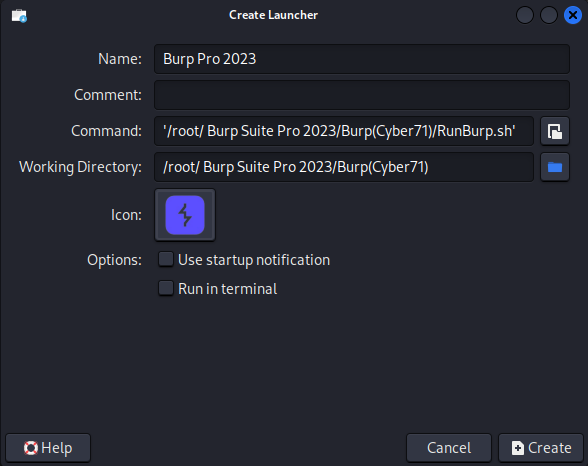


1. **Name**: Anything  
   **Command**: Path to RunBurp.sh

**Working Directory**: Path to the directory of RunBurp.sh

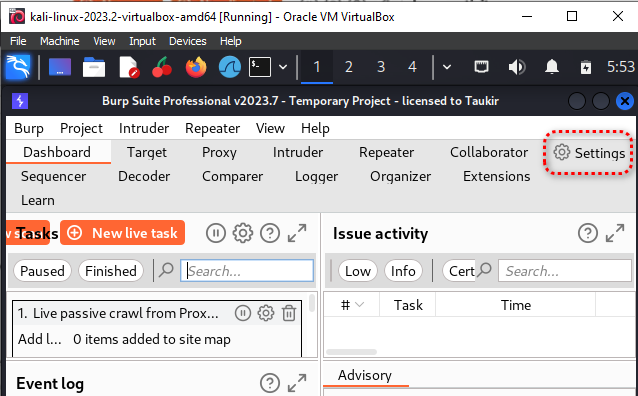
**Icon**: No Icon > Image File > Path to the downloaded Burp suite icon

Then Click on Create and open the Burp Suite Pro 2023 from Desktop.

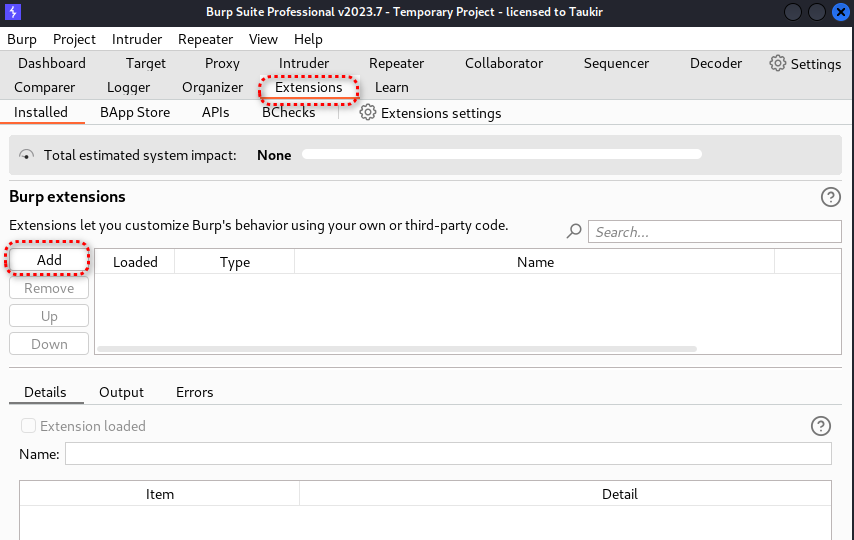


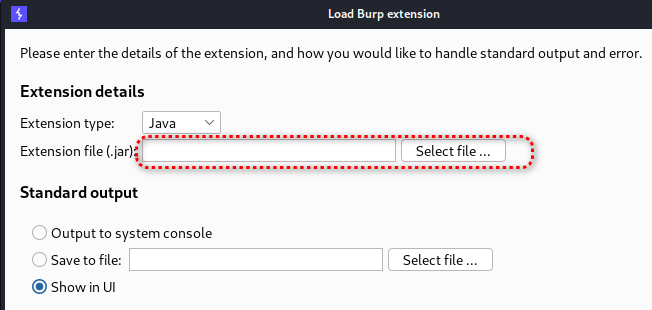
# Burp Suite Extensions

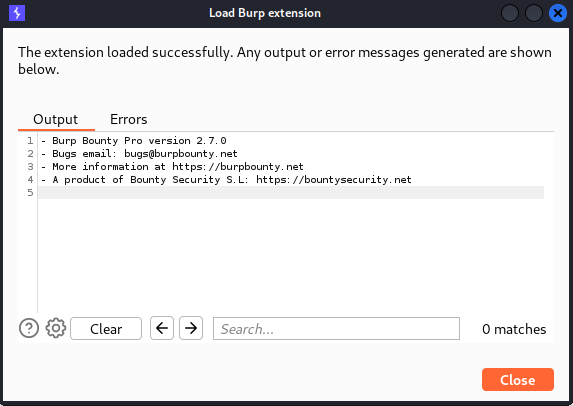
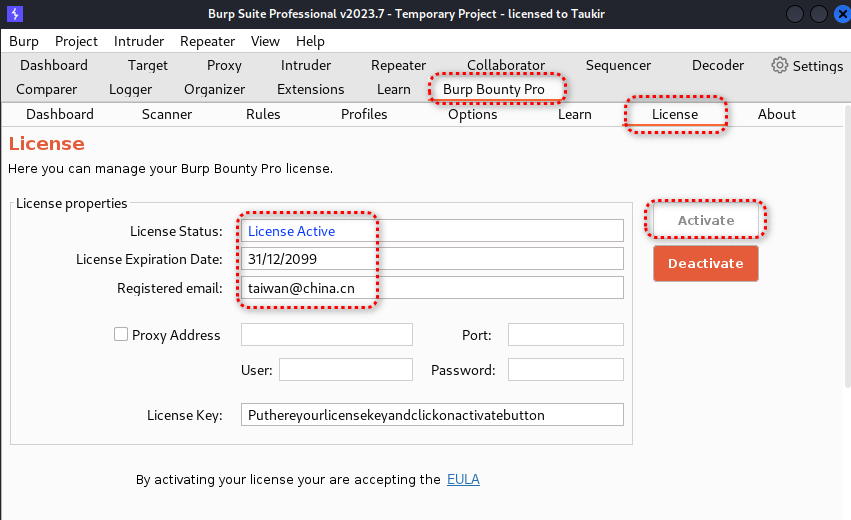
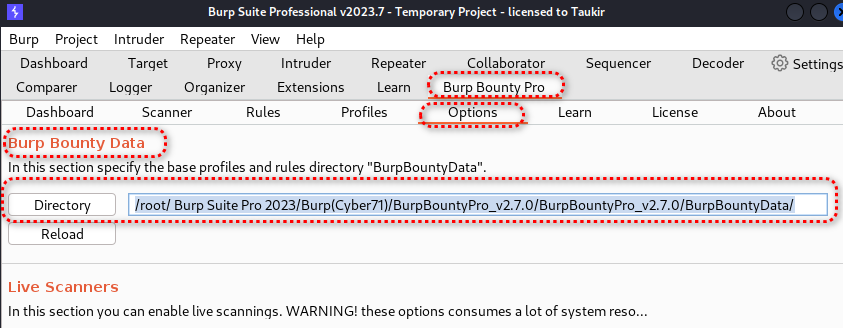
## Burp Bounty Pro

1. Open Burp Suite and go to Settings at top-right corner.  
   
2. Go to Extensions and from Python environment select Jython file located at “/root/ Burp Suite Pro 2023/Burp(Cyber71)/jython-standalone-2.7.3.jar”.

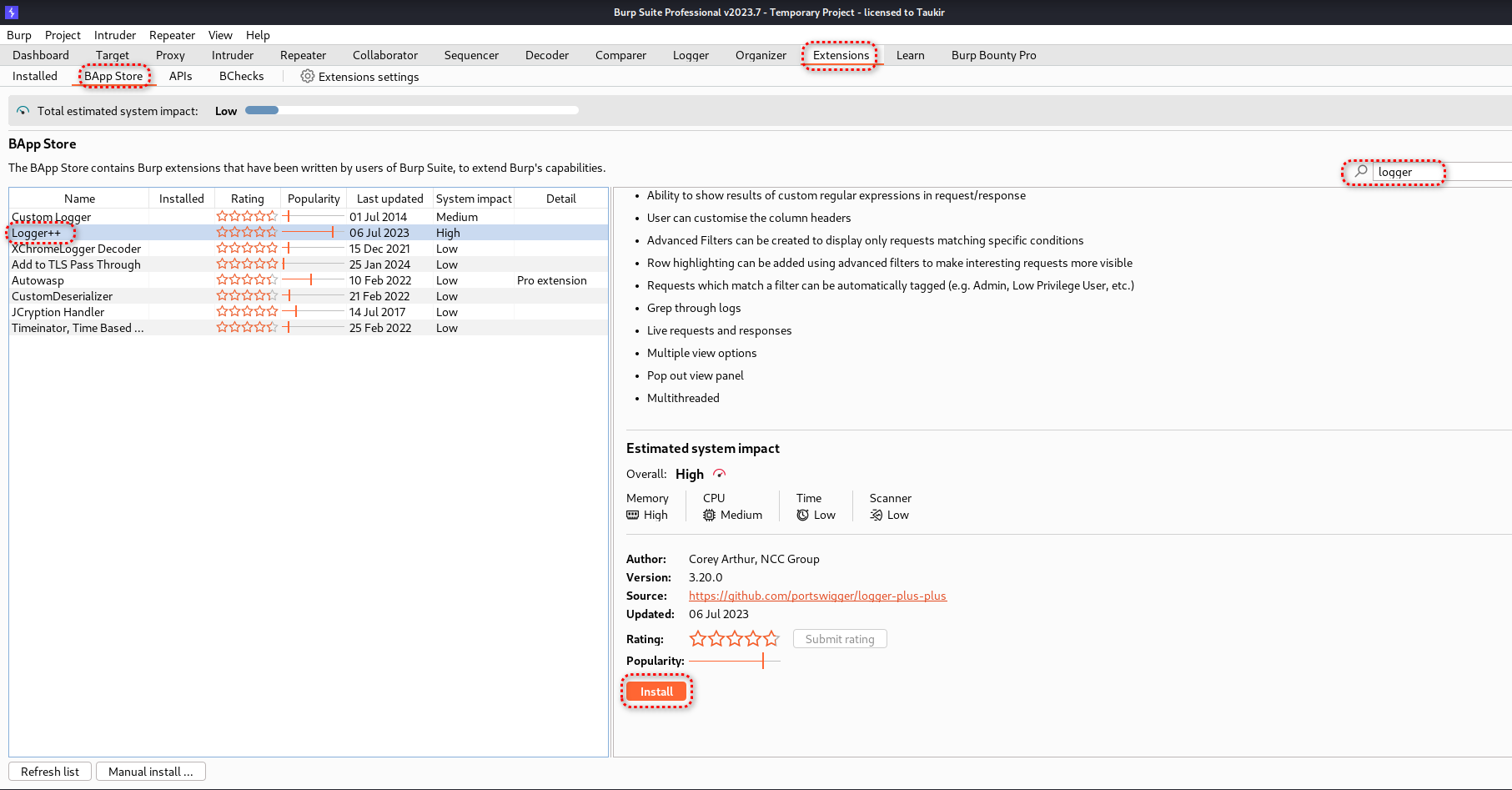
|  |  |
| --- | --- |
|  |  |

1. Close it and go to Extensions > Add  
   
2. From “Extension details”, select “.jar” file from the following path  
   “/root/ Burp Suite Pro 2023/Burp(Cyber71)/BurpBountyPro\_v2.7.0/BurpBountyPro\_v2.7.0/BurpBountyPro.jar”



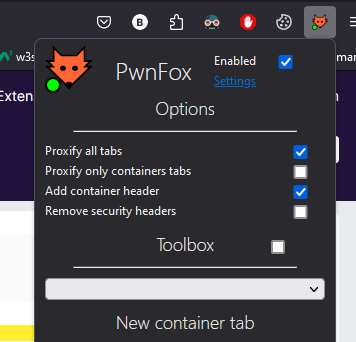
1. Then the following window will appear.  
   
2. Go to Burp Bounty Pro > License.   
   Then press “**Activate”** and we have a lifetime activated license**.**  
   
3. To activate Burp Bounty rules, go to Burp Bounty Pro > Options > Burp Bounty Data > then select the following directory: “/root/ Burp Suite Pro 2023/Burp(Cyber71)/BurpBountyPro\_v2.7.0/BurpBountyPro\_v2.7.0/BurpBountyData/”  
   

## Logger++

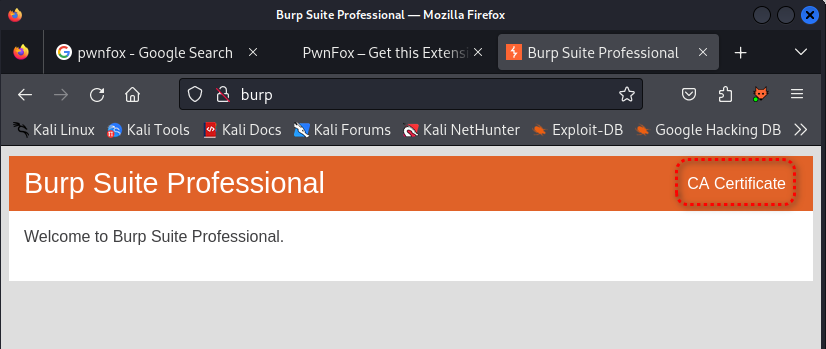
1. Go to Extensions > BApp Store > Search for “Logger++” > Install  
   **Caution: Logger++ has a high system impact**  
   

# Configuring Burp Suite pro 2023

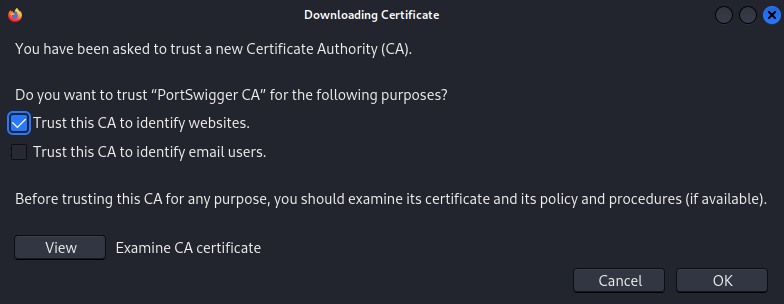
## Installing PwnFox extension

1. Search for PwnFox extension in Firefox browser and install it.
2. Enable PwnFox extension and check “Proxify all tabs”.  
   

## Installing CA Certificate

1. In Burp Suite, Intercept should be closed (Proxy > Intercept > Intercept is off).
2. Go to Firefox browser and enable PwnFox.
3. Search for <http://burp> and download “CA Certificate”.  
   
4. Go to Settings of Firefox and search for “certificate”. Click on View Certificate > Authorities > Import > Select the CA certificate file

|  |  |
| --- | --- |
|  |  |

1. Check “Trust this CA to identify websites” and press OK.  
     
   

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*THE END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*