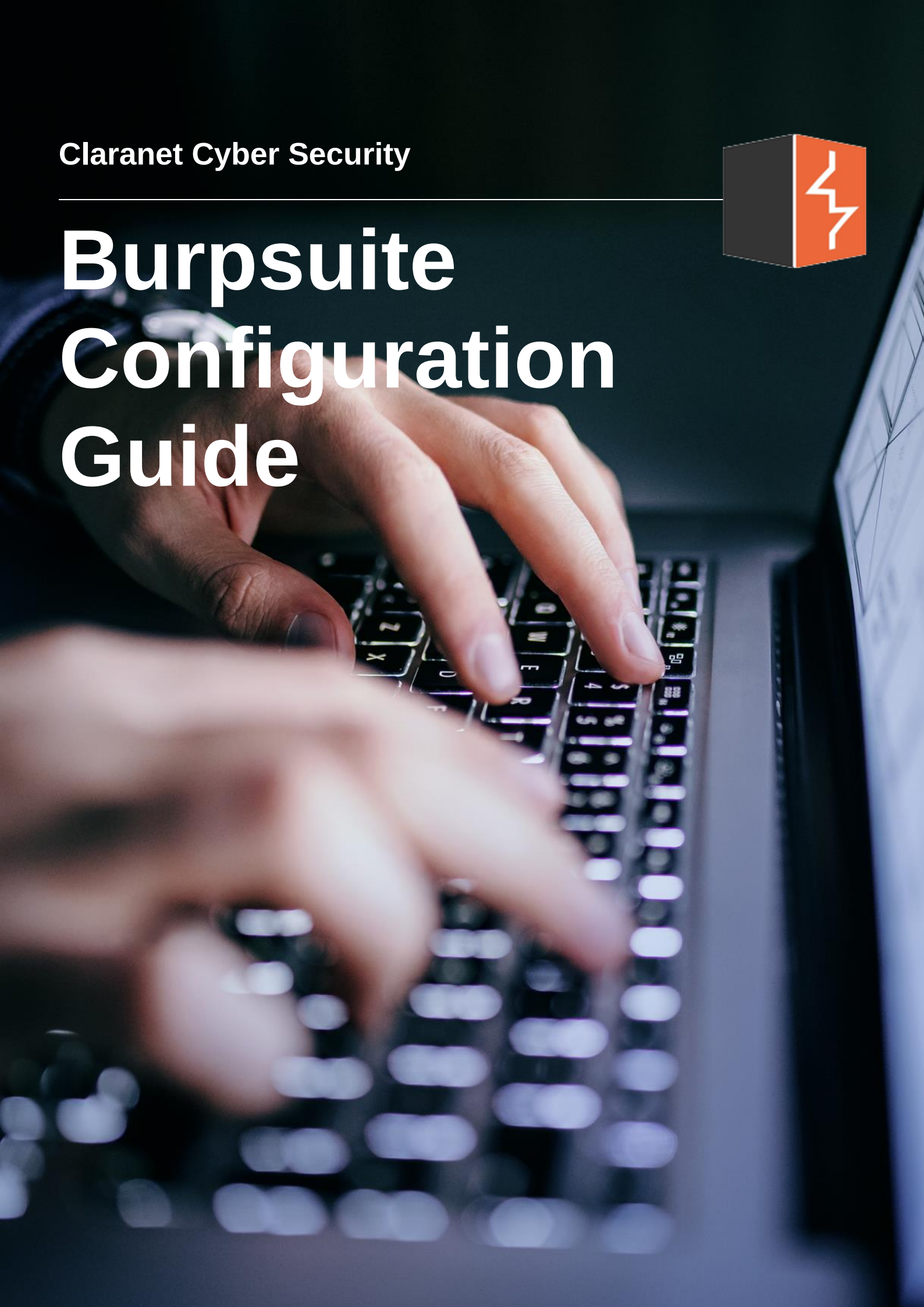
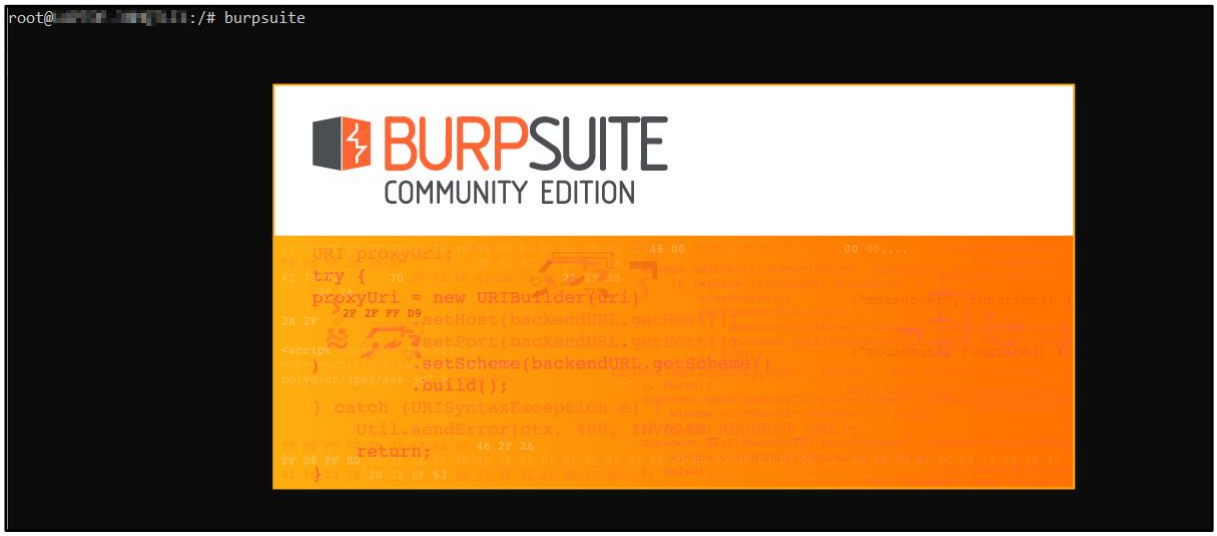
Claranet Cyber Security

Burpsuite Configuration Guide

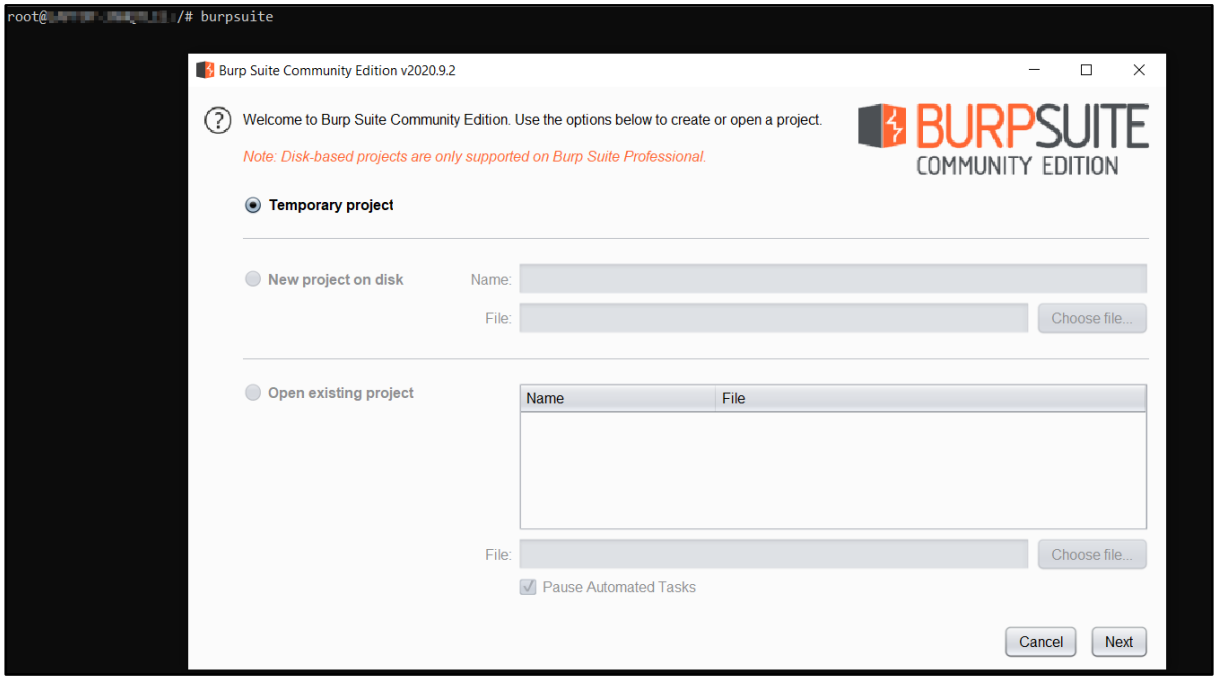


Burpsuite Configuration

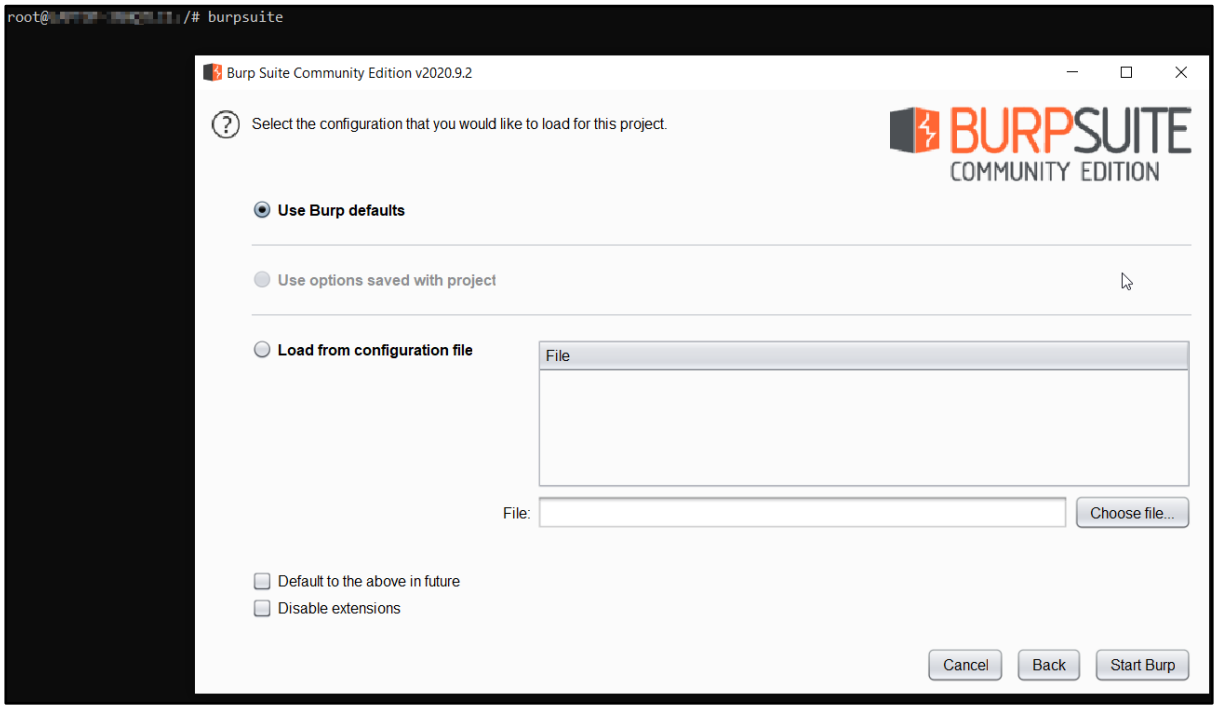
Step 1: Open a Command Prompt Terminal and type “burpsuite”.



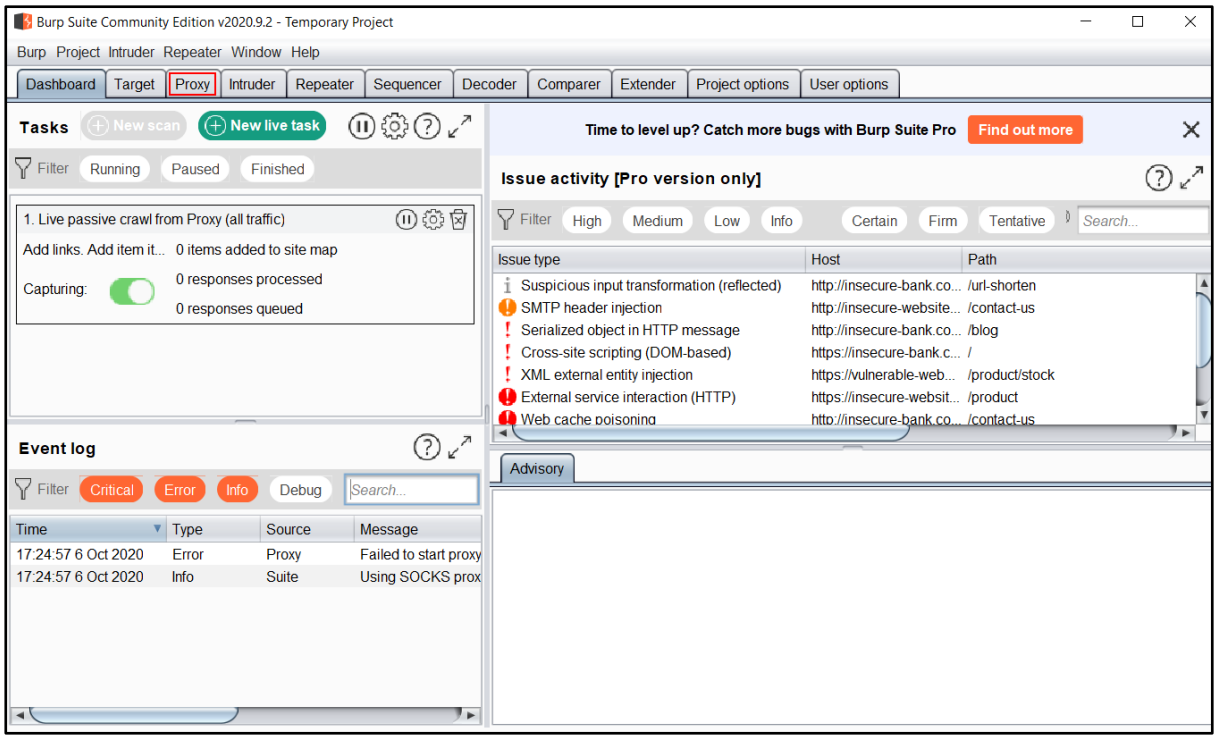
Step 2: Ignore any warning or update notification and select “Temporary Project” and click Next.



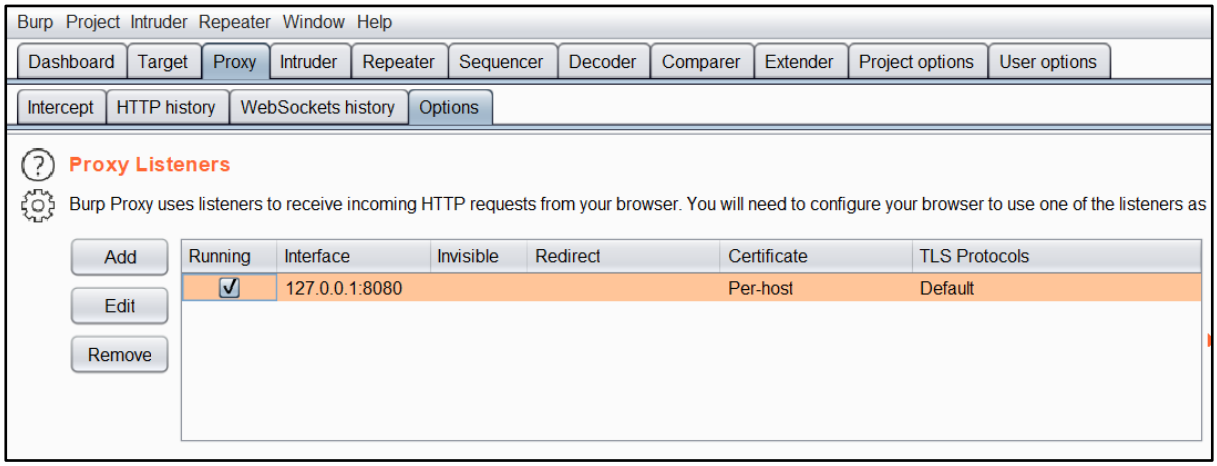
Step 3: Keep the default selection, " Use Burp defaults" and click on "Start Burp".



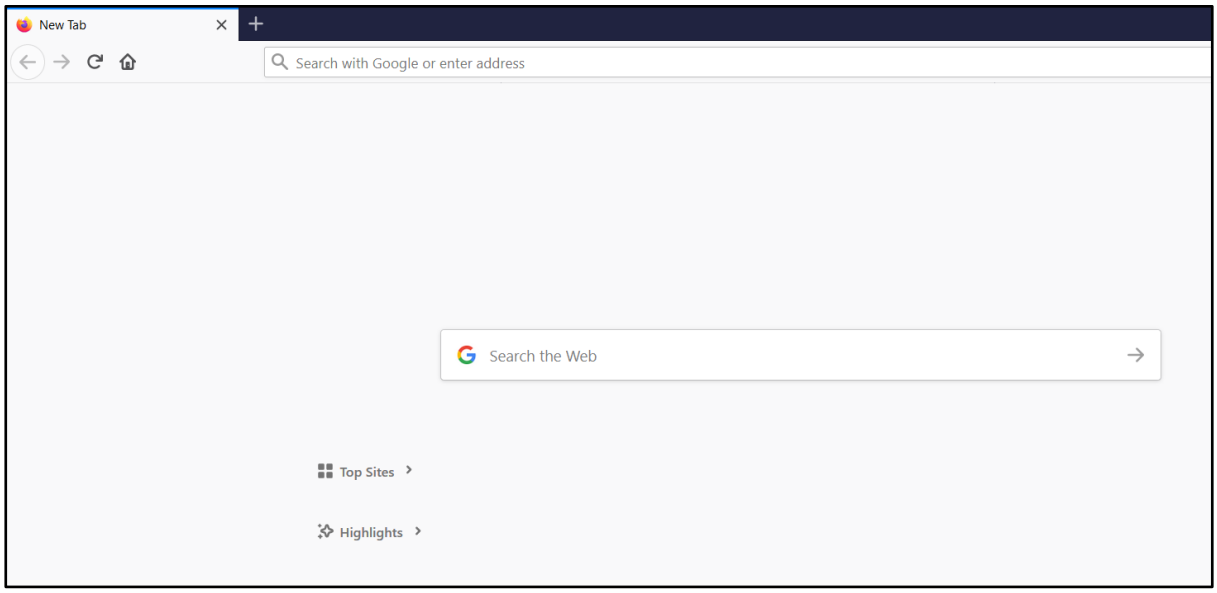
Step 4: Burp Suite has now been started and you should have the below window. Click on the "Proxy" Tab.



Step 5: Under the Proxy tab confirm the below default settings. Use the “Edit” button in case you wish to change the default settings. By default Burp is configured to listen over the localhost interface of port 8080. Feel free to change it to another port number and update the browser settings.

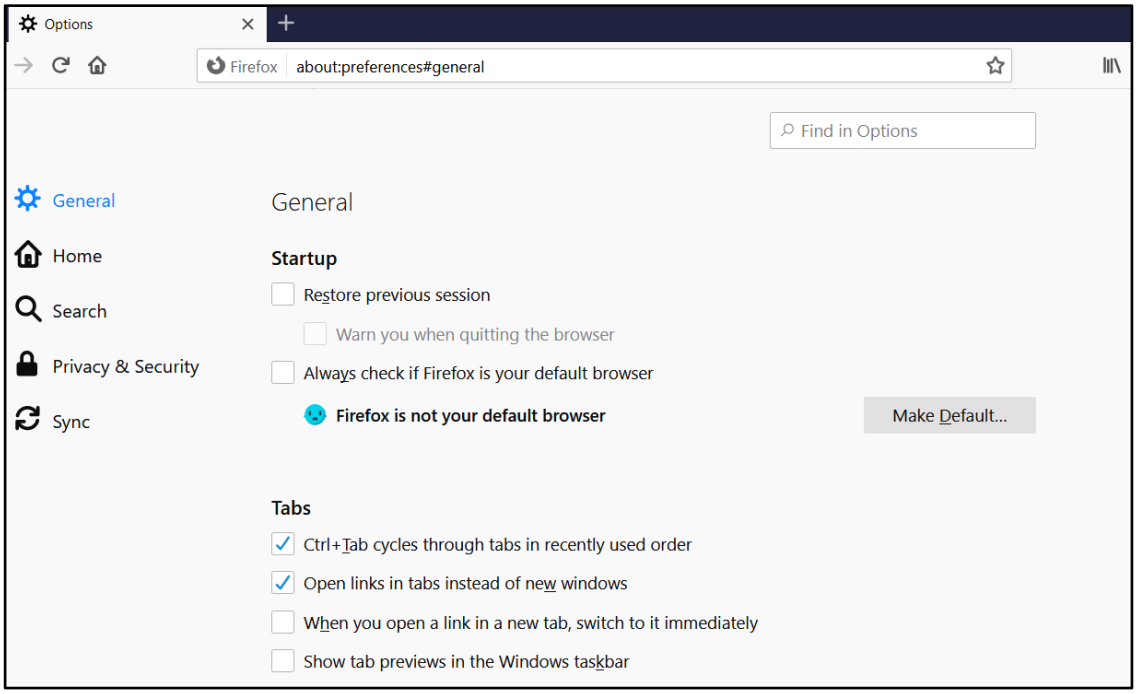


Step 6: Now, open your Firefox browser.

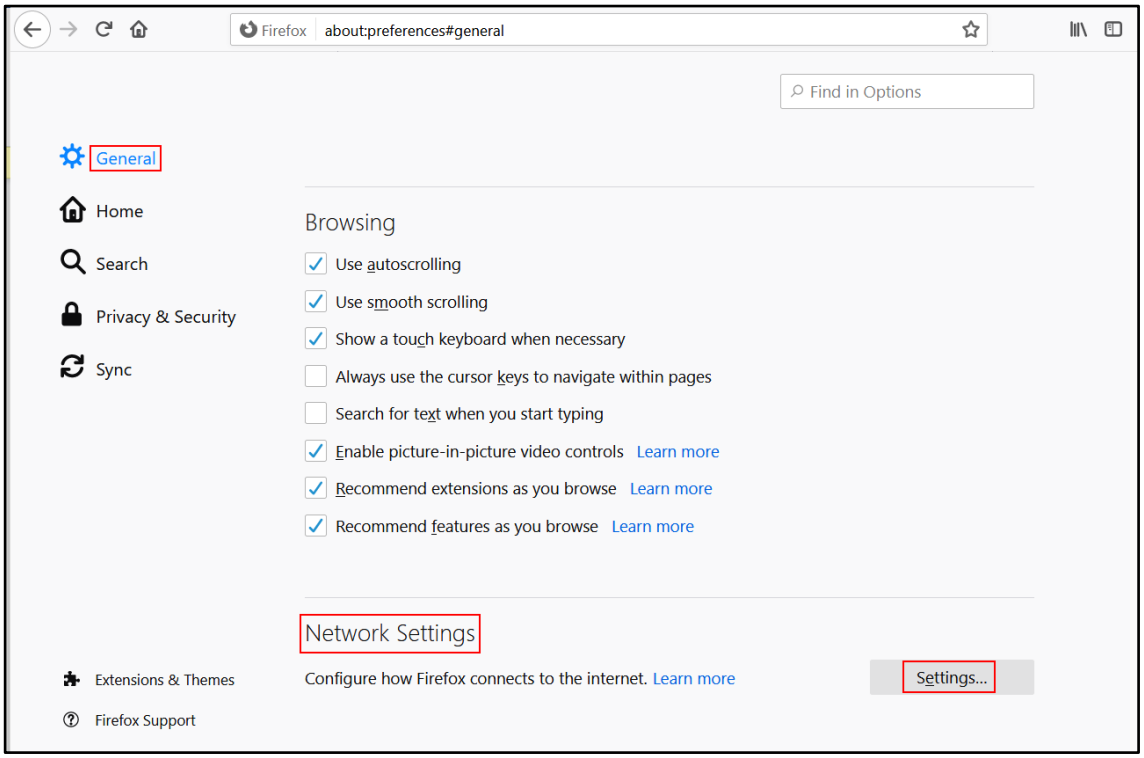


Step 7: Press the “ALT” key in windows/linux or “Option” for mac users to enable viewing of the Browser Tool tab. Click on Edit and Preferences.

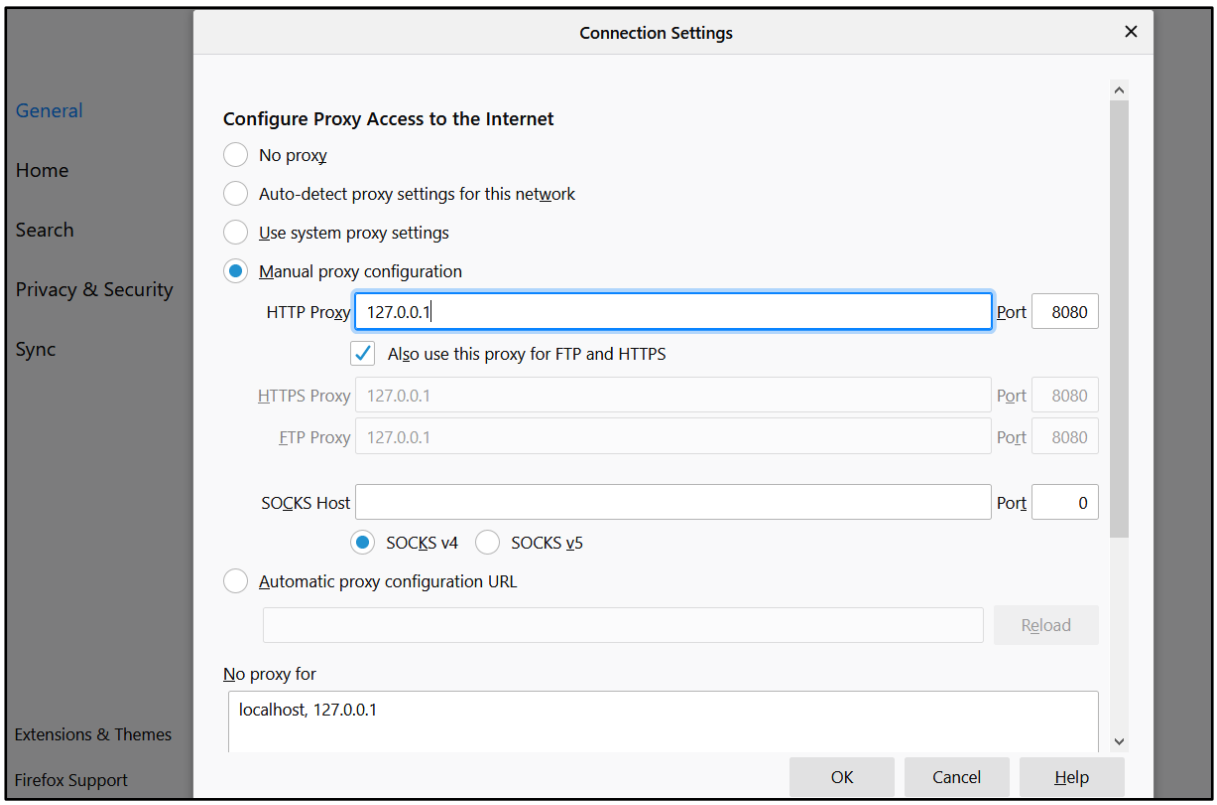
Alternatively press the below keys in quick succession → “ALT/Option + E + N”.



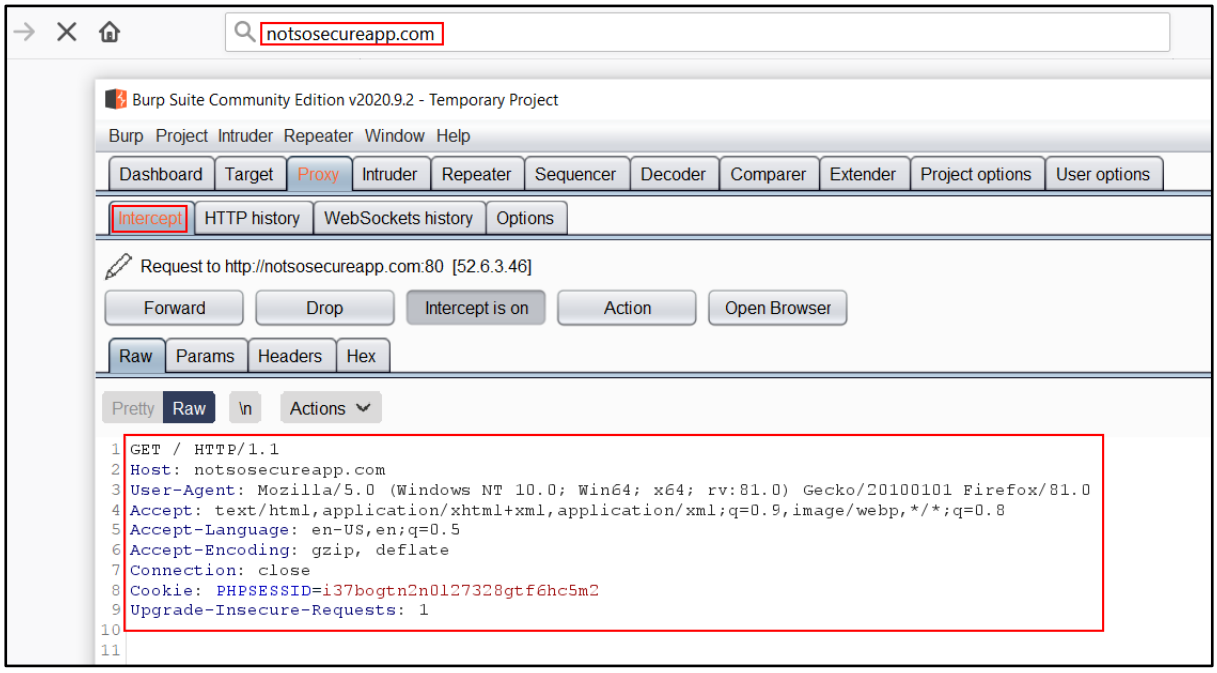
Step 8: Click on “Advanced” -> Network -> Settings



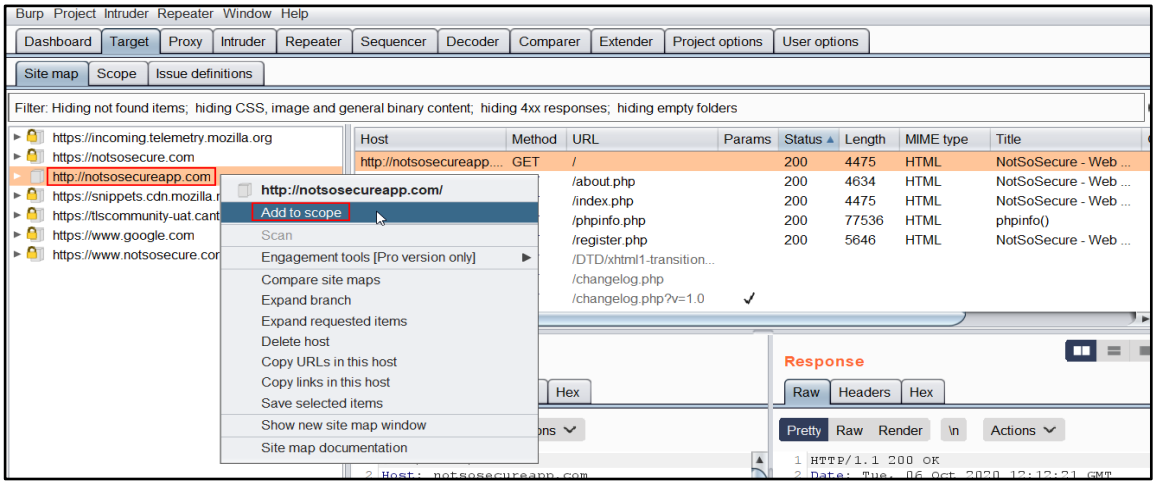
Step 9: Enter the required information. Here we are configuring Firefox to communicate with Burpsuite over port 8080. Click OK and then in new tab open notsosecureapp.com



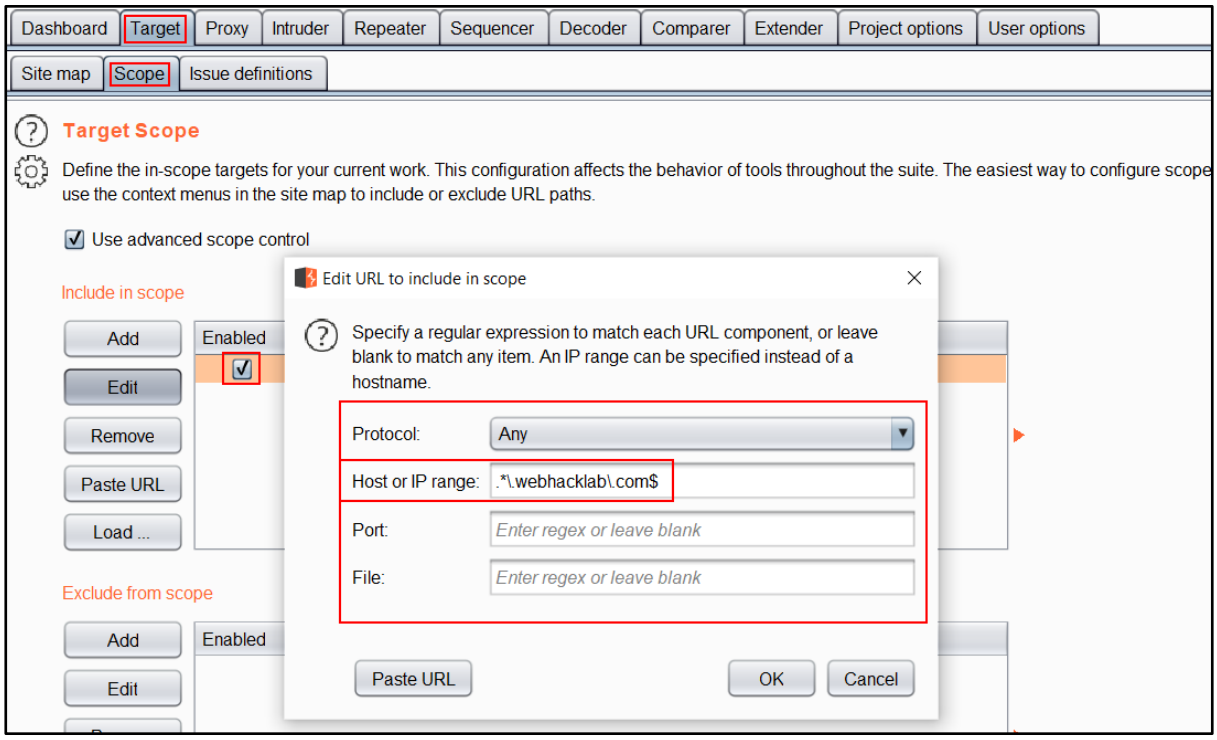
Step 10: Once you have configured your browser, the next step is to test that it is working properly. Go to any HTTP site. If everything works well, you'll see an HTTP request in the intercept tab. Congratulations you have just configured Burpsuite successfully! You are now ready to intercept each HTTP/HTTPS request that the browser is sending to the server(s).



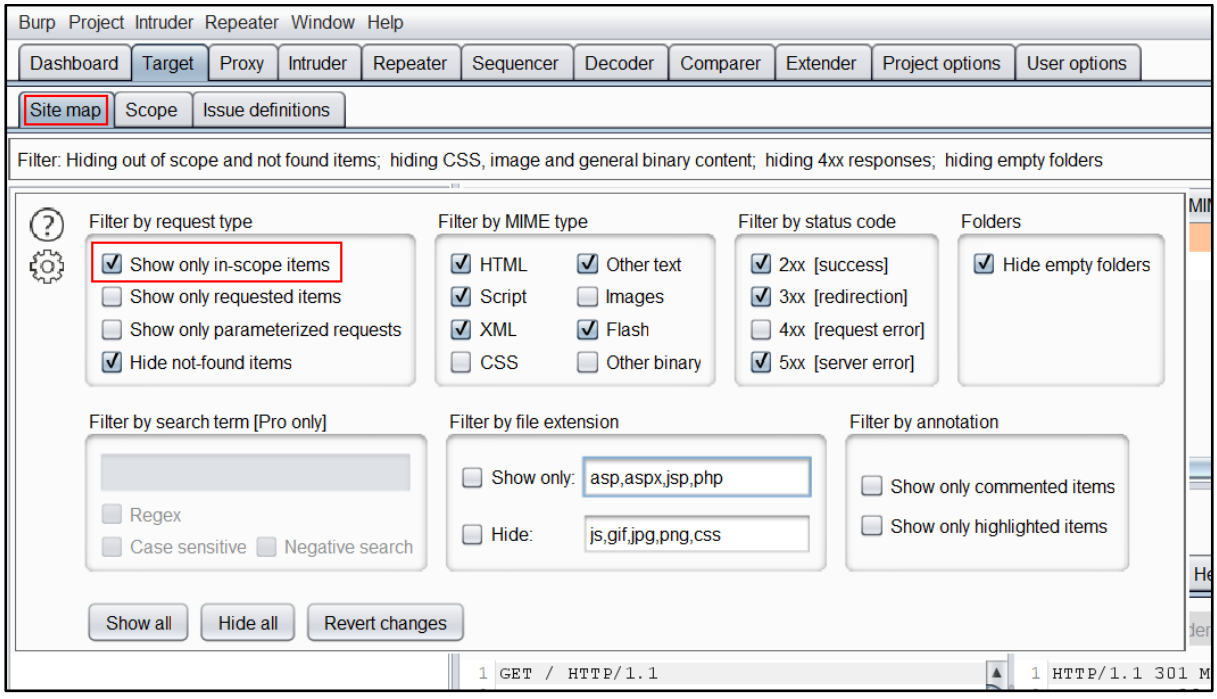
Step 11: Navigate to the "Target" tab , select the URL "http://XXXXXXXXXX.com", right click on "Add to scope". Scope defines to focus our testing to scoped items only, we can use/filter scoped items to Burp components such as interception, proxy history, scanner etc. However, we need to configure few components such as proxy history which is described in next steps.



Step 12: You can also select “Advanced Options” from “Scope” configuration. Add regex “**.*\.webhacklab\.com$**” to Host or IP Range field, this allows all subdomains of webhacklab.com with all ports.



Step 13: Now click on the “Filter” row right below the SiteMap tab in the above image and select the option as “Show only in-scope items” and then click on the Proxy tab.



Step 14: Under the Proxy tab click on the “HTTP history” tab and then again click on the same “Filter” button and select “Show only in-scope items”. This way you’ll be able to view only requests/responses related to our target application in the HTTP History.