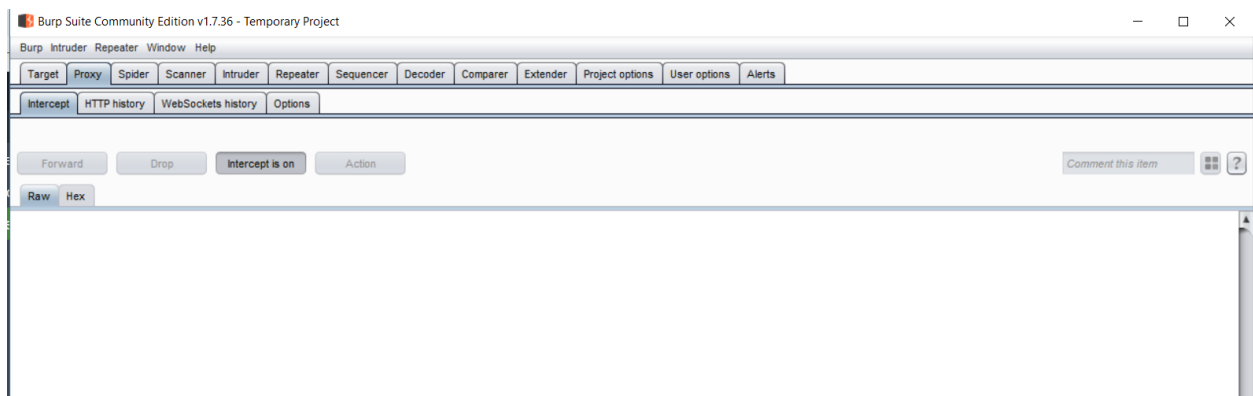
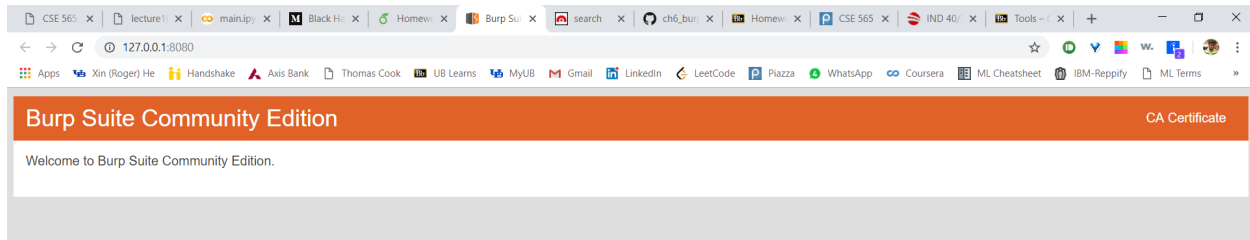


- After adding the python file to the extension, we have to make sure to point your browser to the proxy address: 127.0.0.1:8080.
- This is the default configuration in Burp Suite. Once the site is loaded, I ran a search with `â€œfuzzâ€œ`.
- My intention is to intercept and mutate/ fuzz the `â€œfuzzâ€œ` payload to `â€œbuz-zâ€œ`.
- The IP address will open a website as follows. The mutation is possible only if we open this website. Only then the Burp Suite's Intercept will be switched on. The screenshots of both the website and the Intercept is given below.





- Now we open the vulnerable site and search for the keyword "fuzz".
- Burp has intercepted the HTTP request.
- This intercepted request can be sent to Intruder available in BURP.
- You can go to the Payloads tab and make sure our python extender is selected and click on "Start Attack" after changing the query from fuzz to buzz
- The resulting webpage in the response will search for the keyword "buzz" and hence the Fuzzing Mutation is Successful.
- The screenshots of the attack are attached here.

