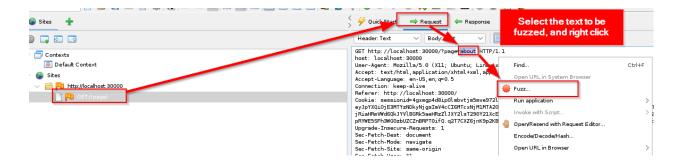
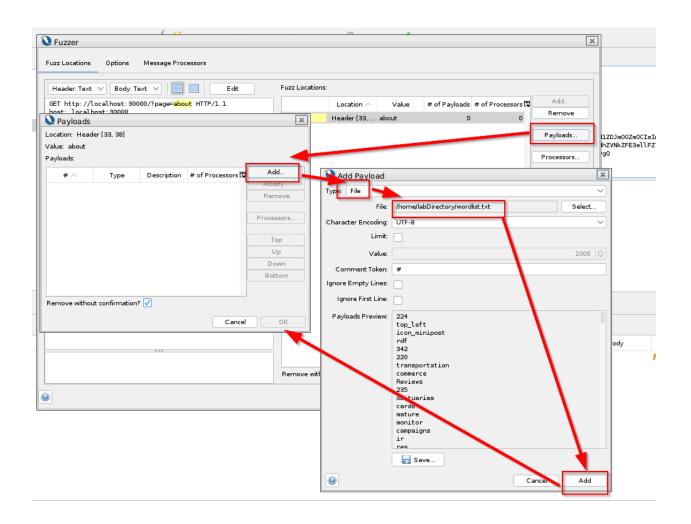
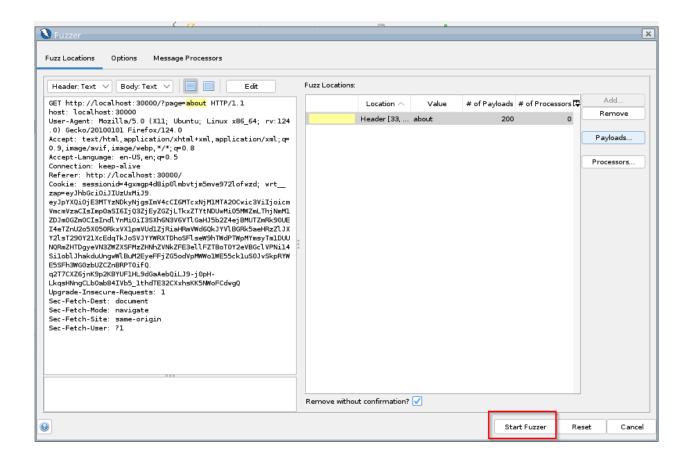
FUZZING through ZAP

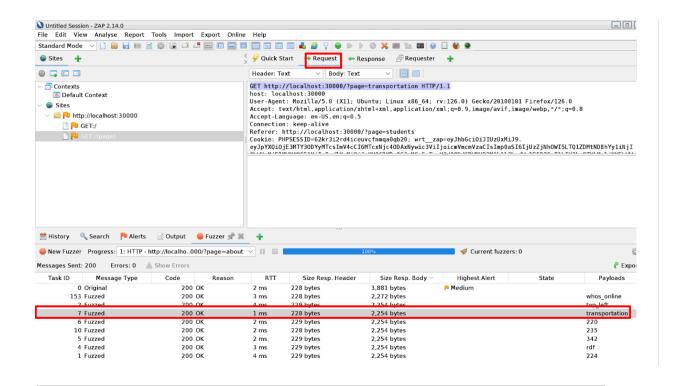
- Ensure FoxyProxy is disabled first. This is important, since without ZAP running, it won't know where to forward traffic
- Then visit http://localhost:30004/zap/ (this can take a few minutes), followed by http://localhost:30000/
- Then in ZAP, ensure HUD is disabled and also enable FoxyProxy now with the right pattern to forward the traffic of http://localhost:30000/ to ZAP (as covered in activity 1)
- Now navigate through the website http://localhost:30000/ so that it appears under Sites.
- Identify the GET request that deals with page GET:/(page). Then follow the below screens. We are essentially feeding a wordlist, where in







Post this, you will see a lot of requests made by ZAP of the type "GET http://localhost:30000/?page=xxx HTTP/1.1" (where xxx is taken from the word list). You can select any request and see what was sent under "Request" in the top window.



Now to see if any hidden page is there, we need to check if there is any difference in response across all payloads. So, let us sort based on response size. See below. Once you obtain the right URL which is hidden, visit it via browser to get the flag! Submit the flab in the cLab app.

