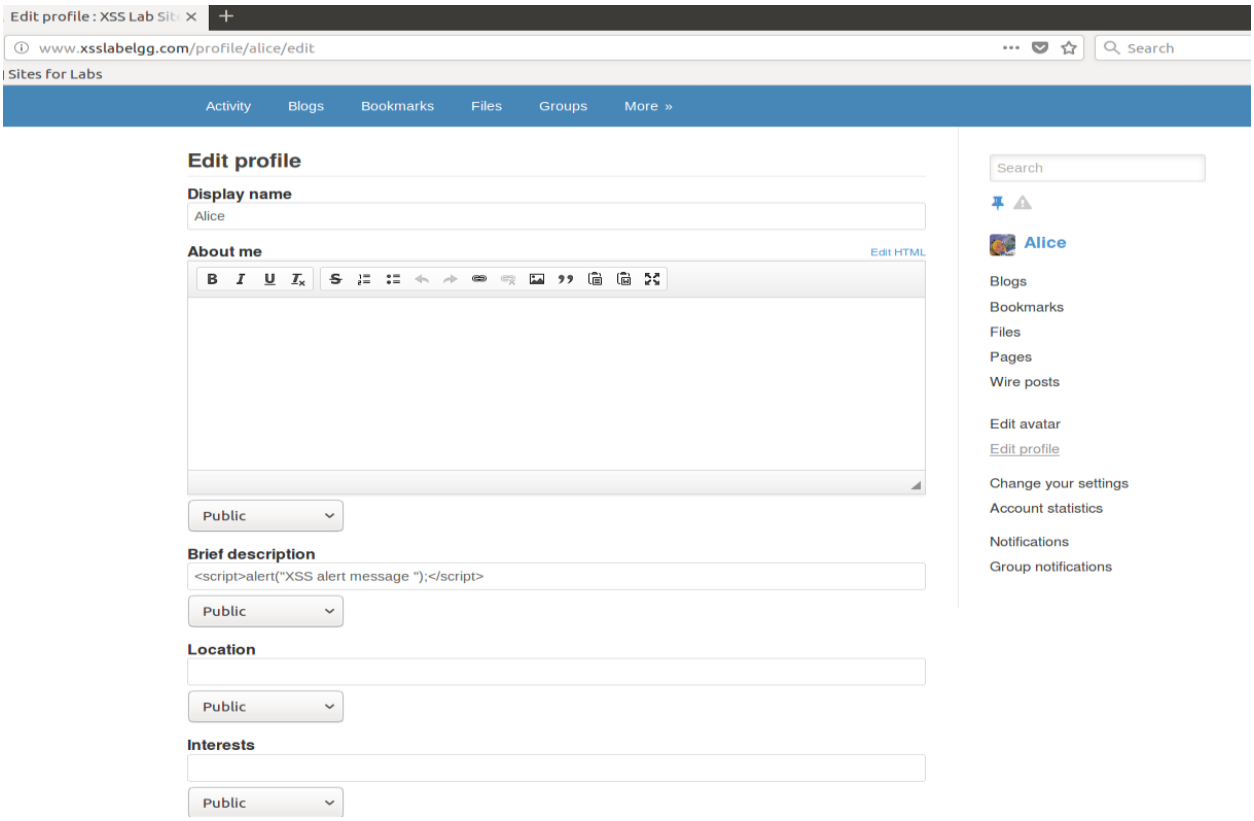
Lab 6 XSS vulnerability

Pramod kumar

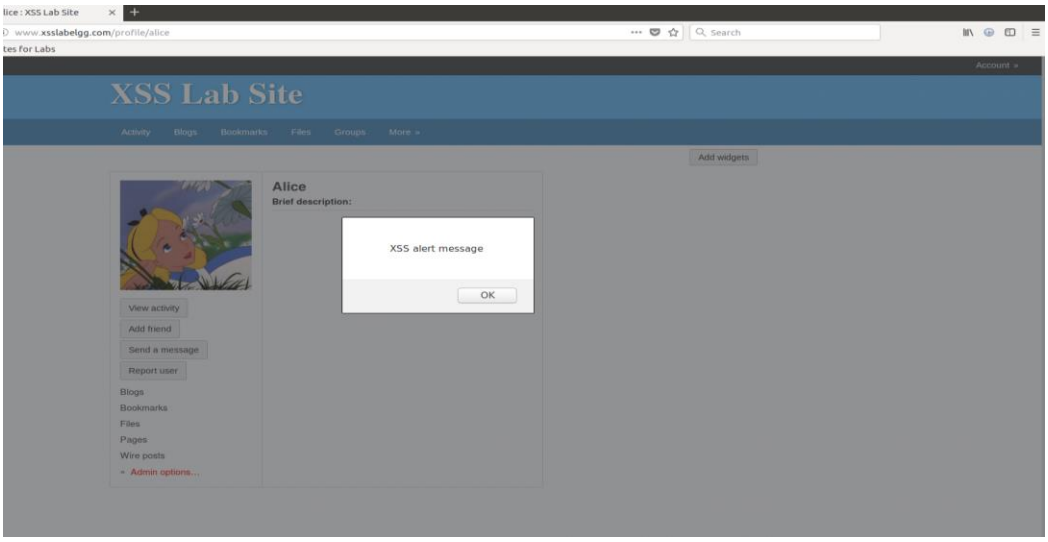
Task1:

Step 1: Edit Alice profile and add desired script in description box.



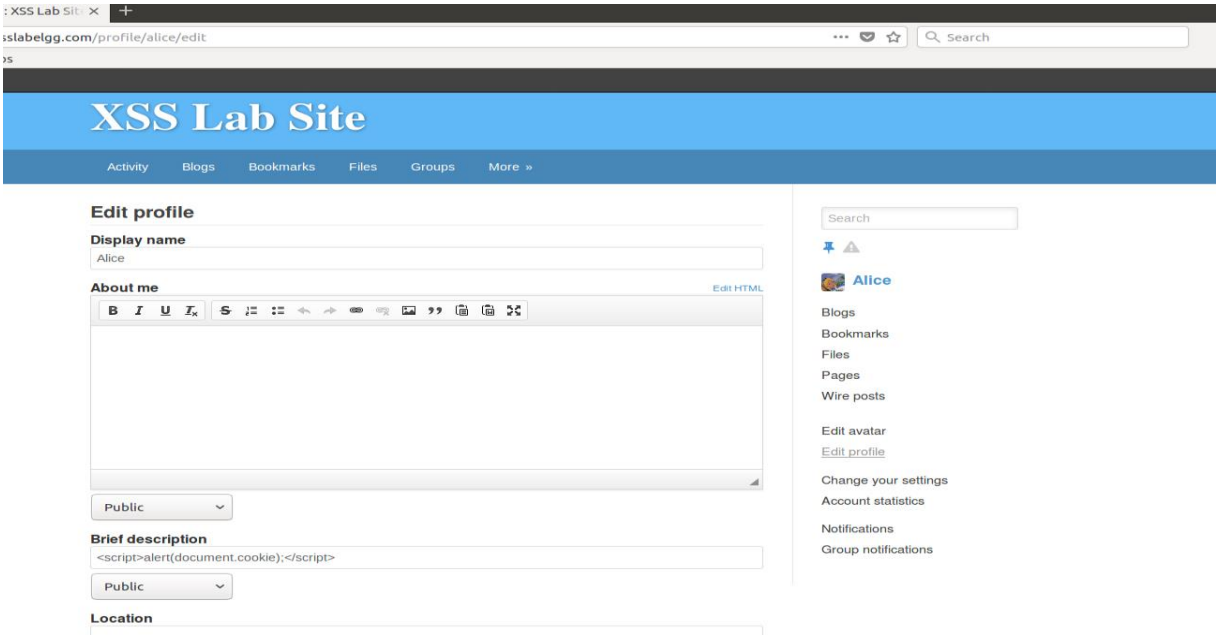
Step 2: Visit alice profile from other user(even with alice visiting it will also execute the script)

Visiting from admin profile:



Task 2:

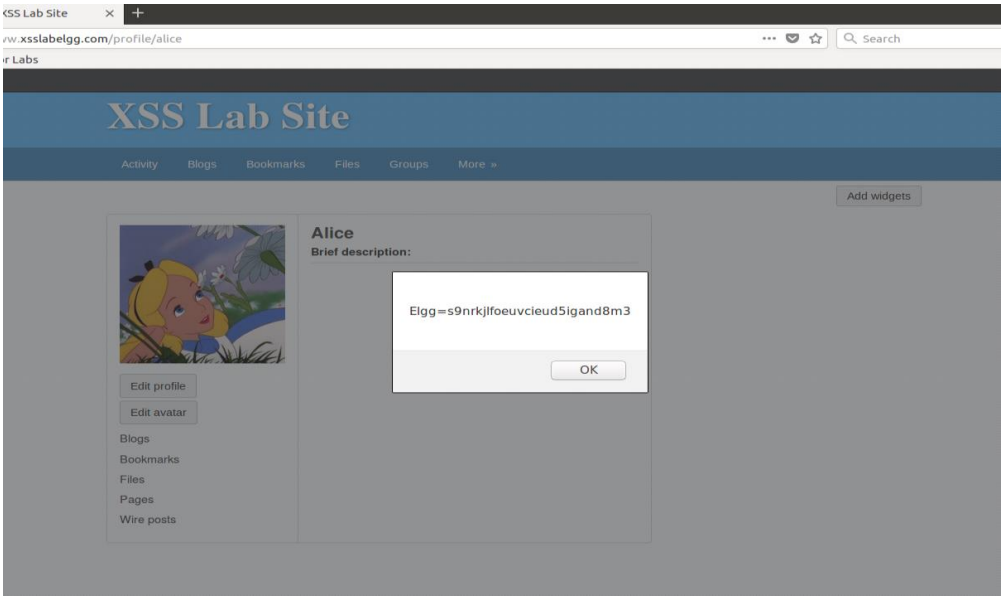
Step1: Again, edit alice profile to display cookies



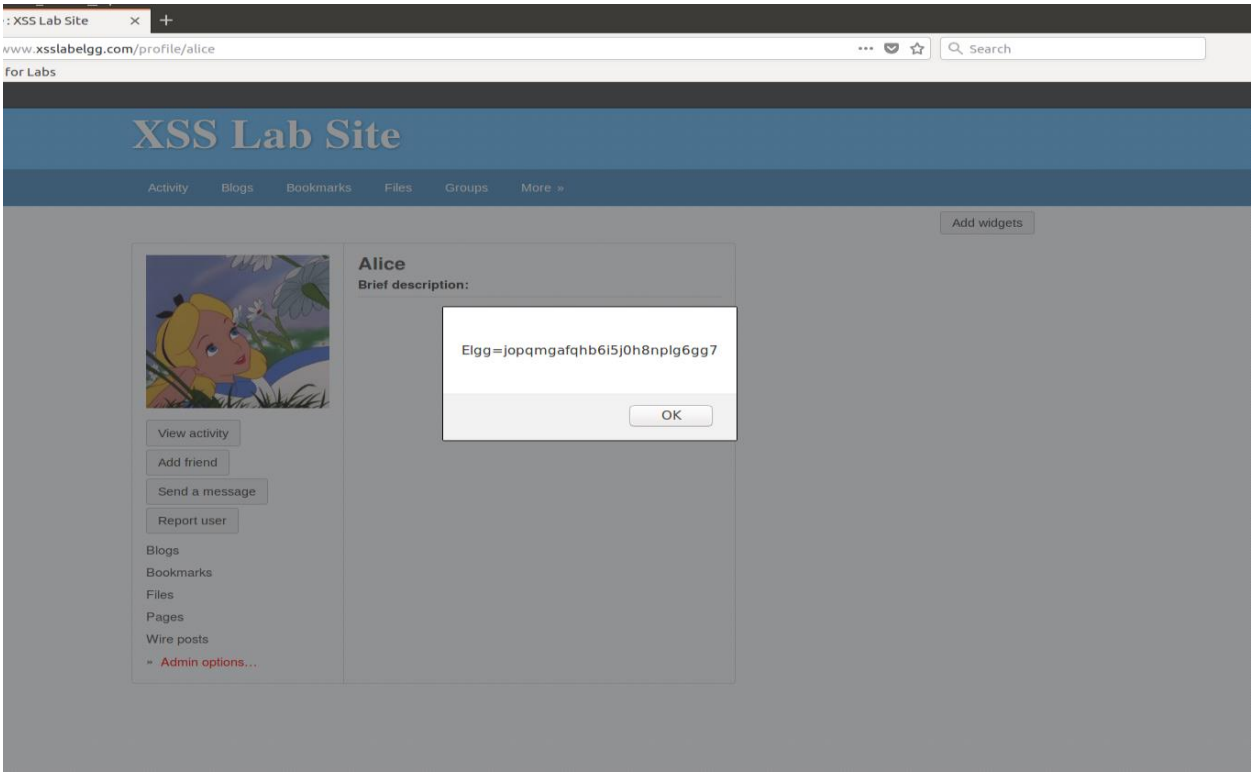
Step 2: Visit alice profile

1) With alice herself
2) From admins account

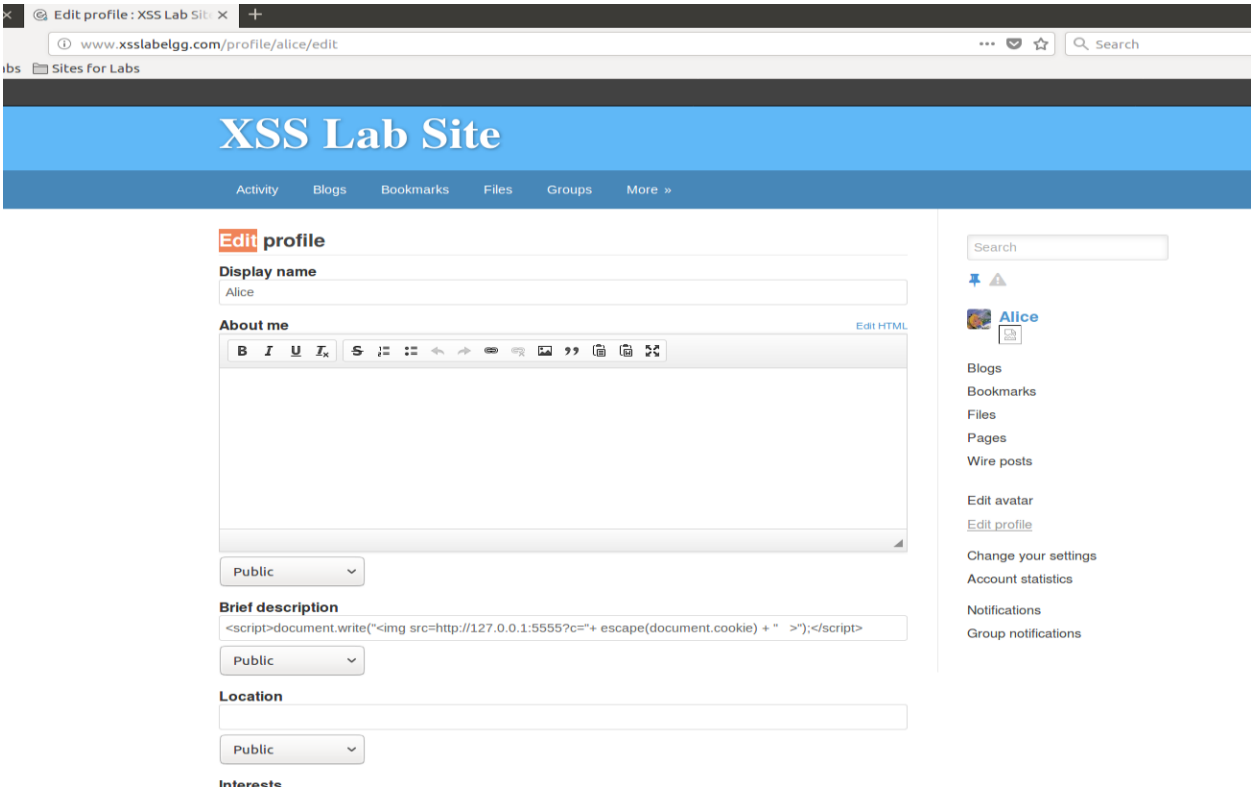
1)



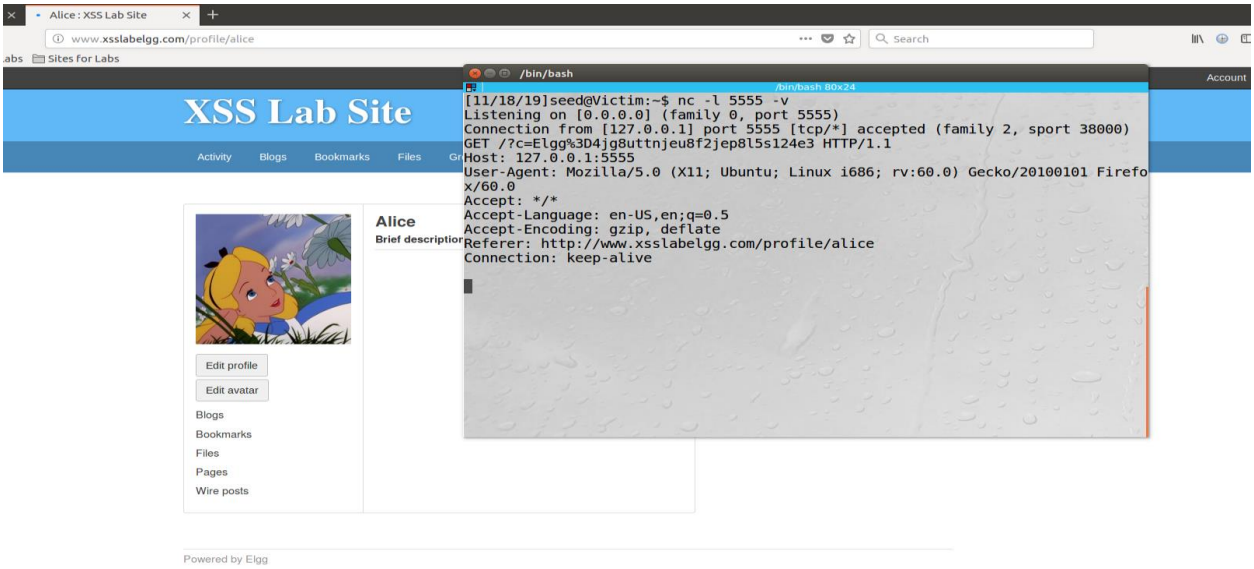
2) From admin login -> alice profile



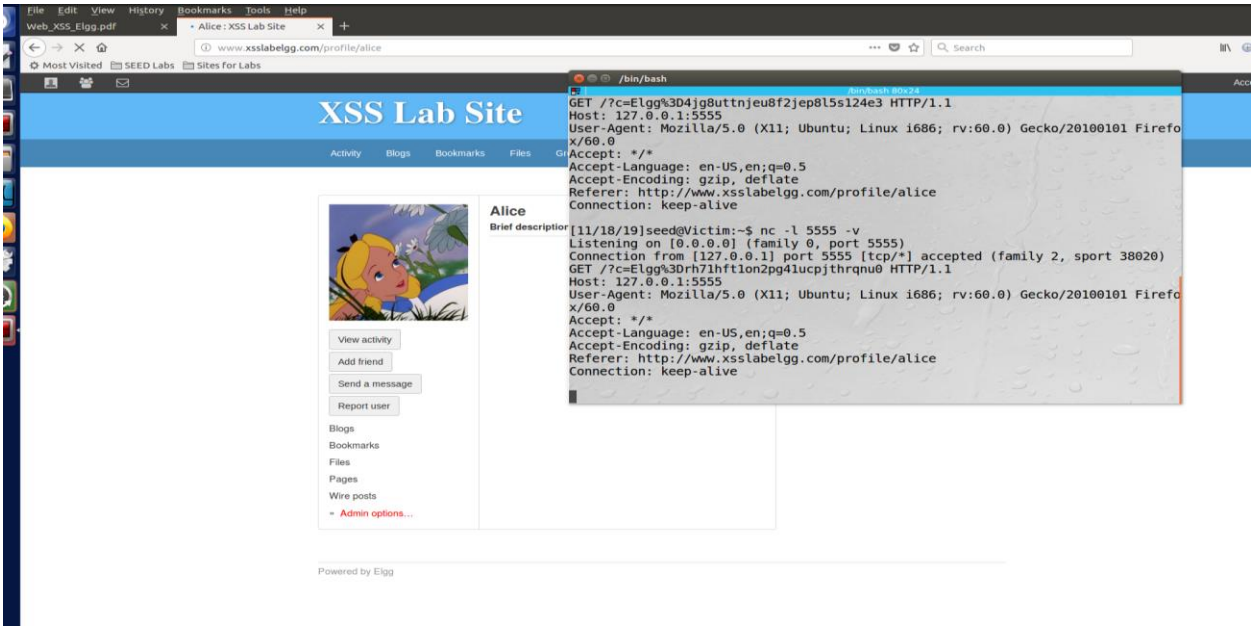
Task 3:



Visit Alice profile using Alice and check the TCP server



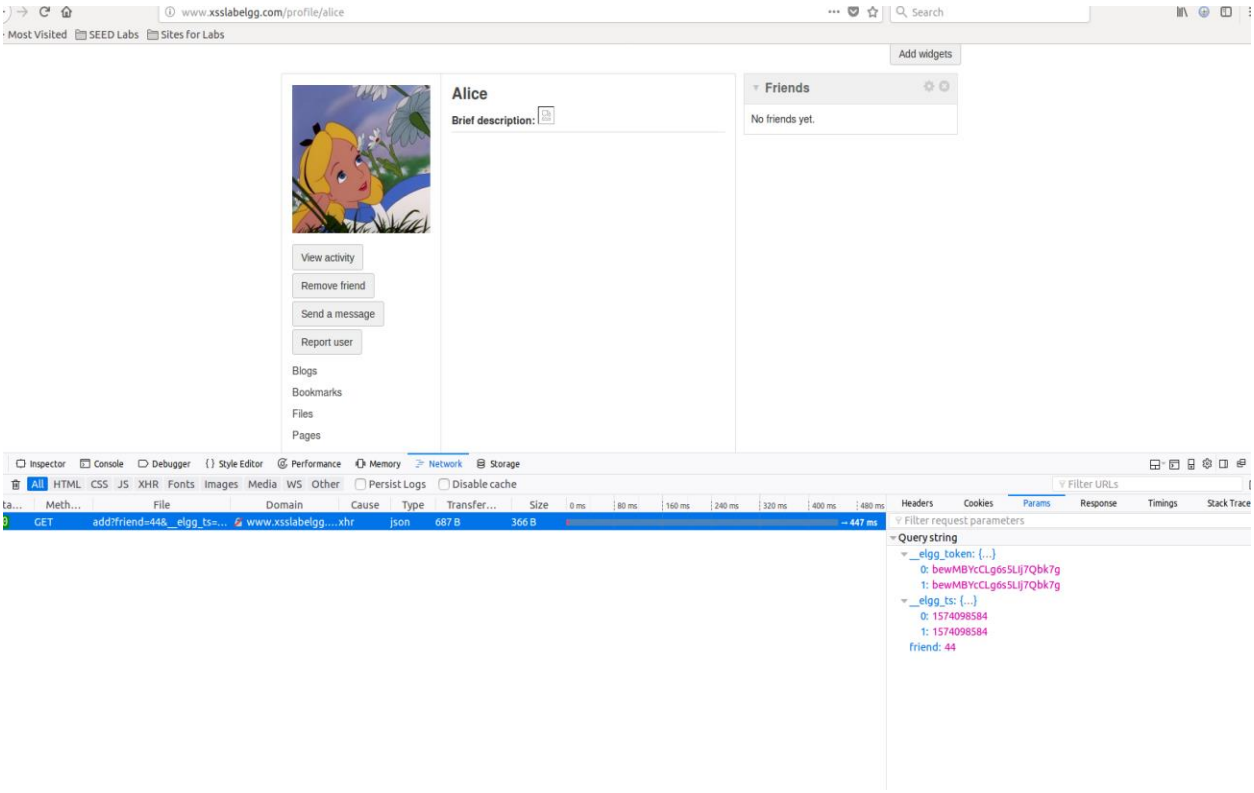
Now visit alice profile from Admin login, we will see different cookies



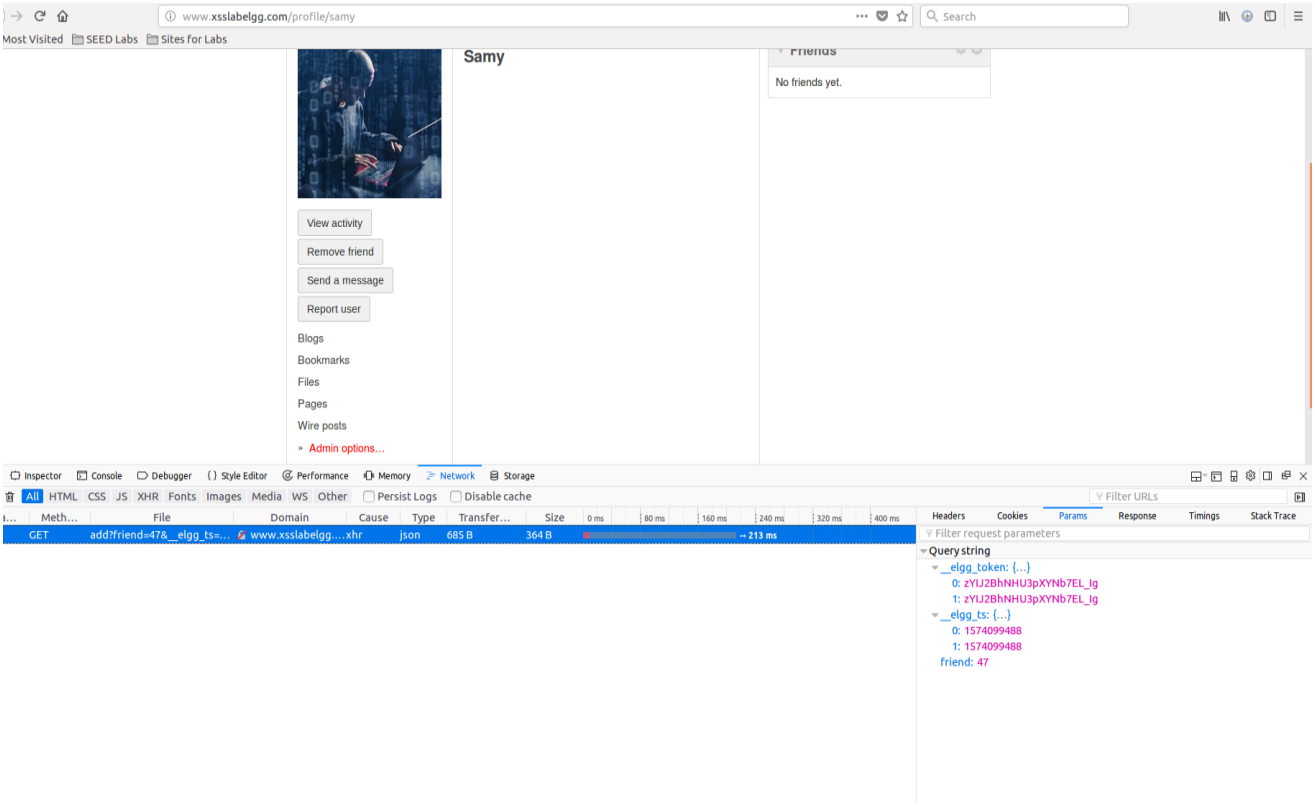
Task4:

Step1: Find pattern in sending friend request.

Visiting alice profile show that alice firend id is 44 and 4 token is sent along with the cookies in the get request.



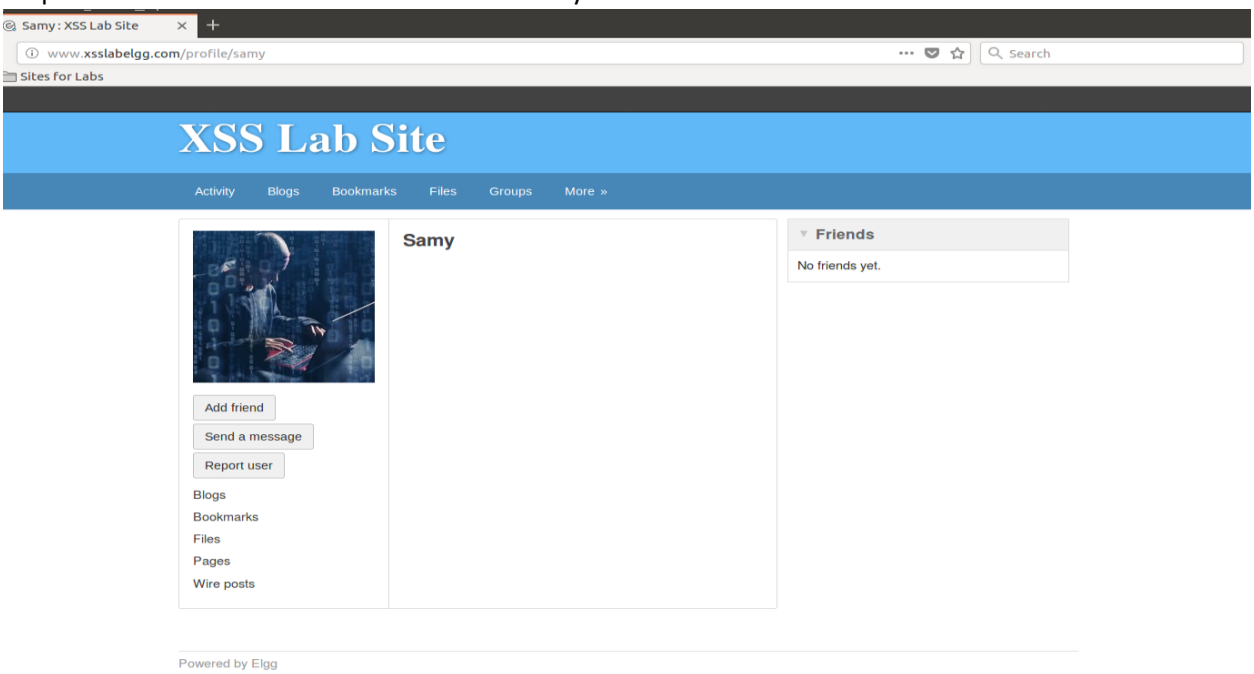
Visiting samy profile: Same has 47 as ID and token are different each time friend request sent, they are stored in elgg_ts and elgg_token variable in the code.



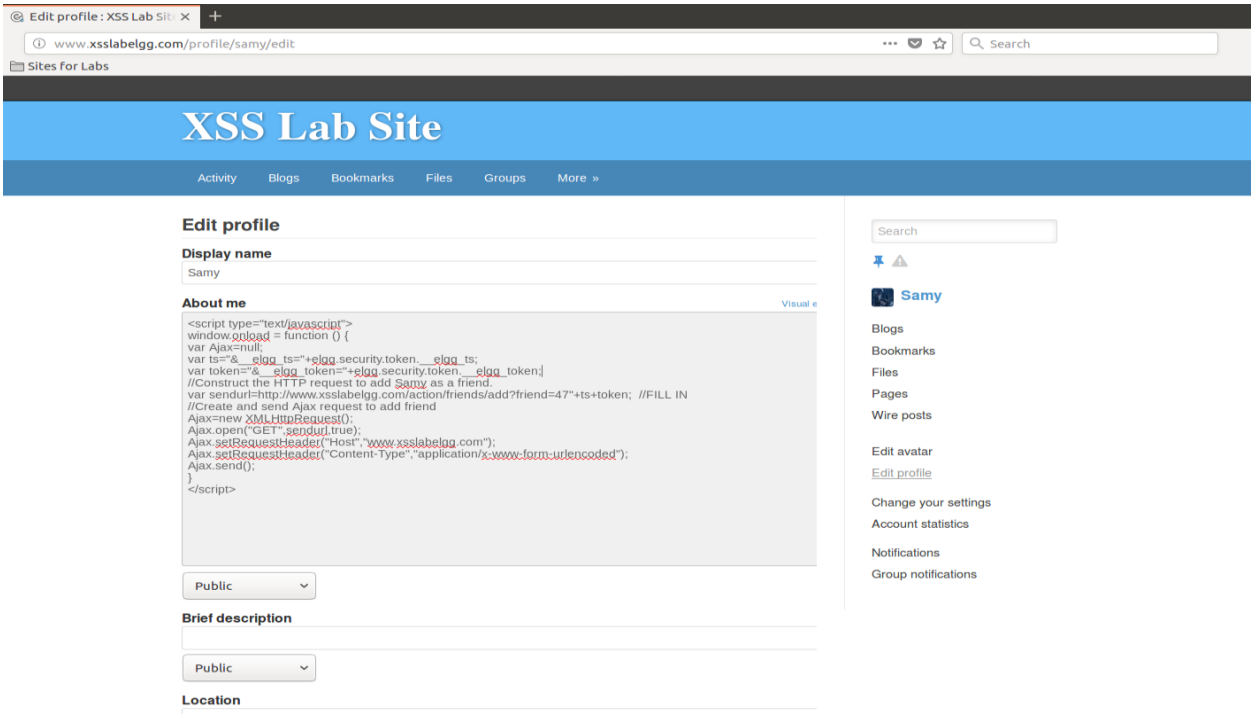
Attack: Now we know that our desired URL will have friend id 47 and paramters

```
"http://www.xsslabelgg.com/action/friends/add?friend=47"+ts+token;
```

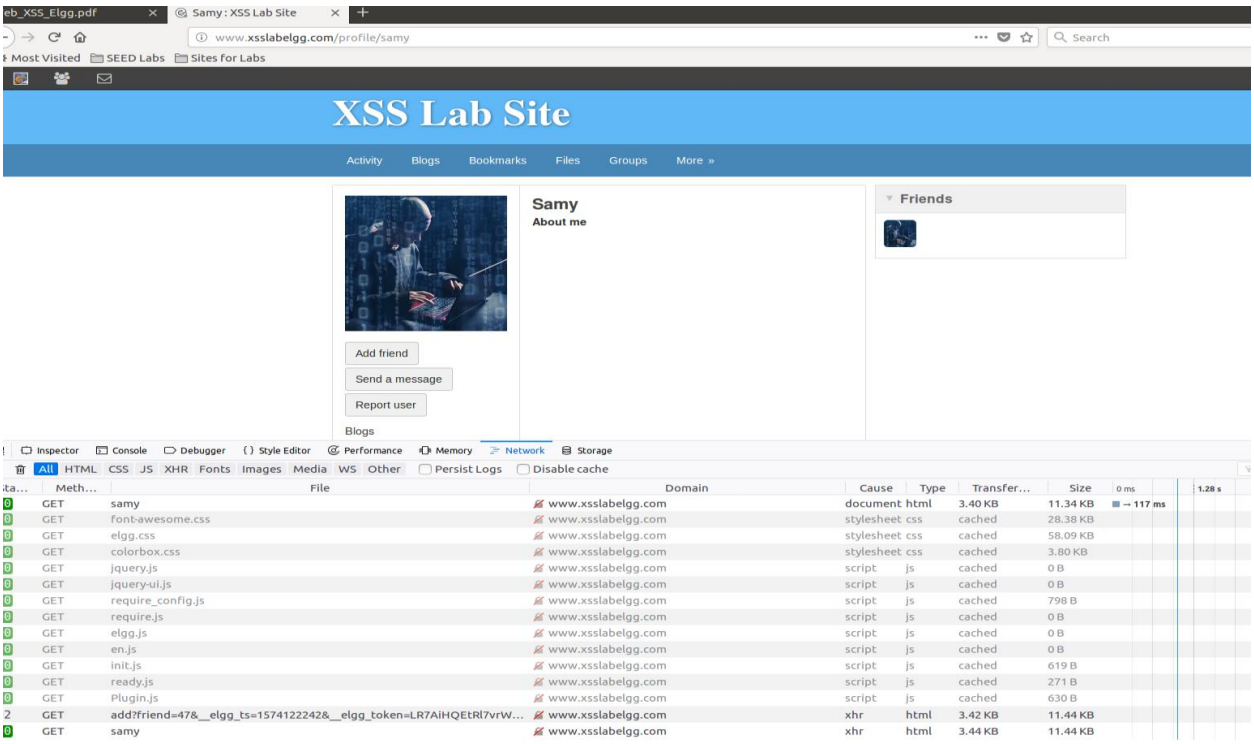
Step1: we can see that alice is not friend of samy



Step 2: Samy will edit its about me with the script

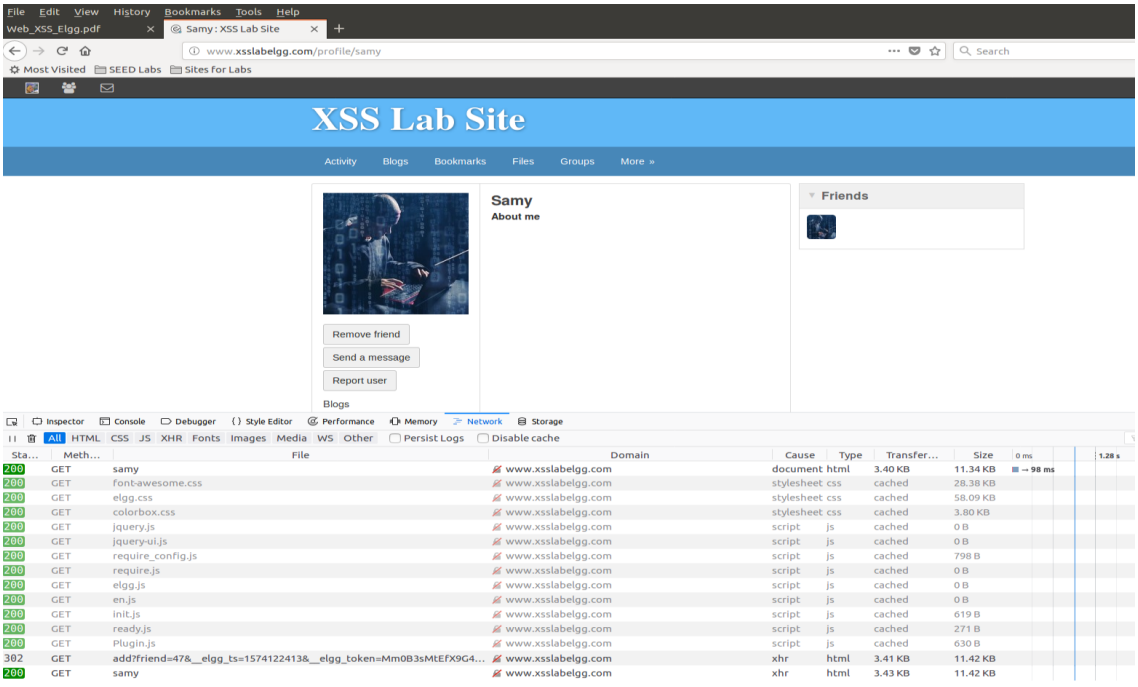


STEP3: Now login with alice and visit samy profile



In network console we can see that add friend url is executed. We can see that samy is friend with himself, as same url was executed for himself when samy edited about me.

Now reload the page to see if ALICE is friend now?
Answer: **“Remove friend” is coming on samy profile**



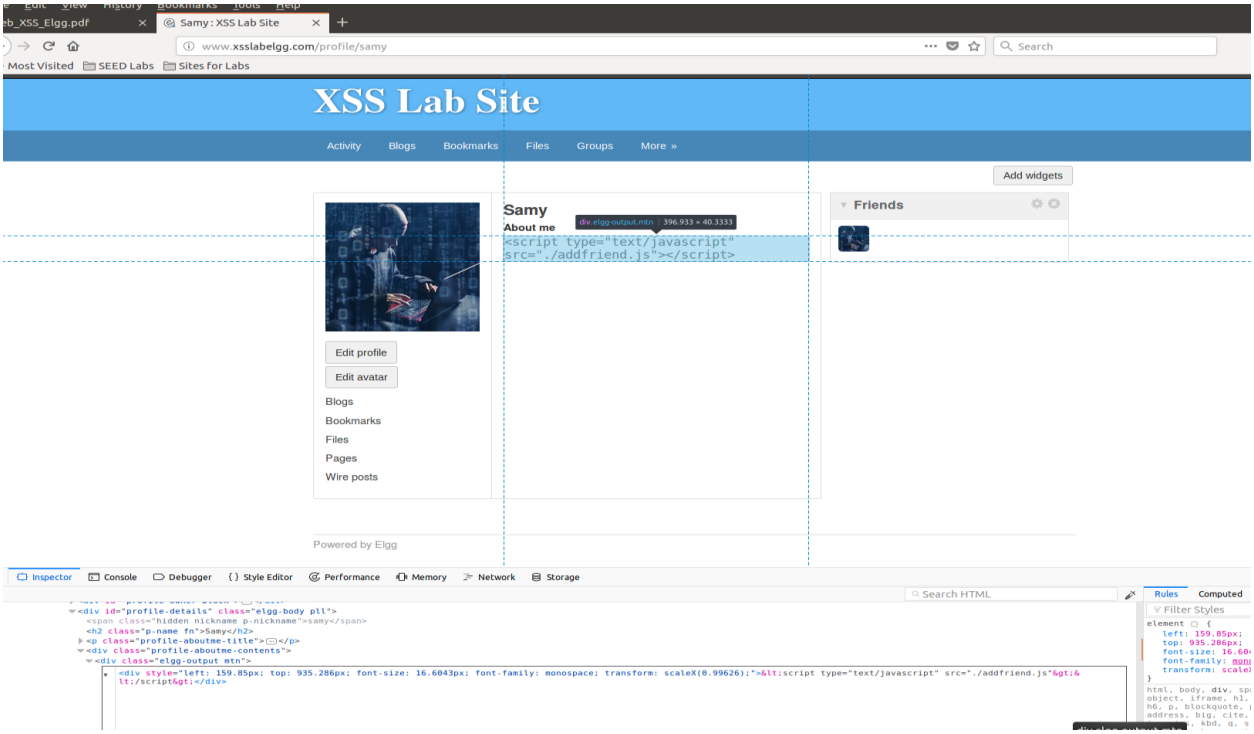
Observations :

1) Explain the purpose of Lines `1` and `2`, why are they are needed?

Answer: line 1 and 2 trying to build _elgg_ts and __elgg_token by reading those variables, which we will use in our HTTP url.

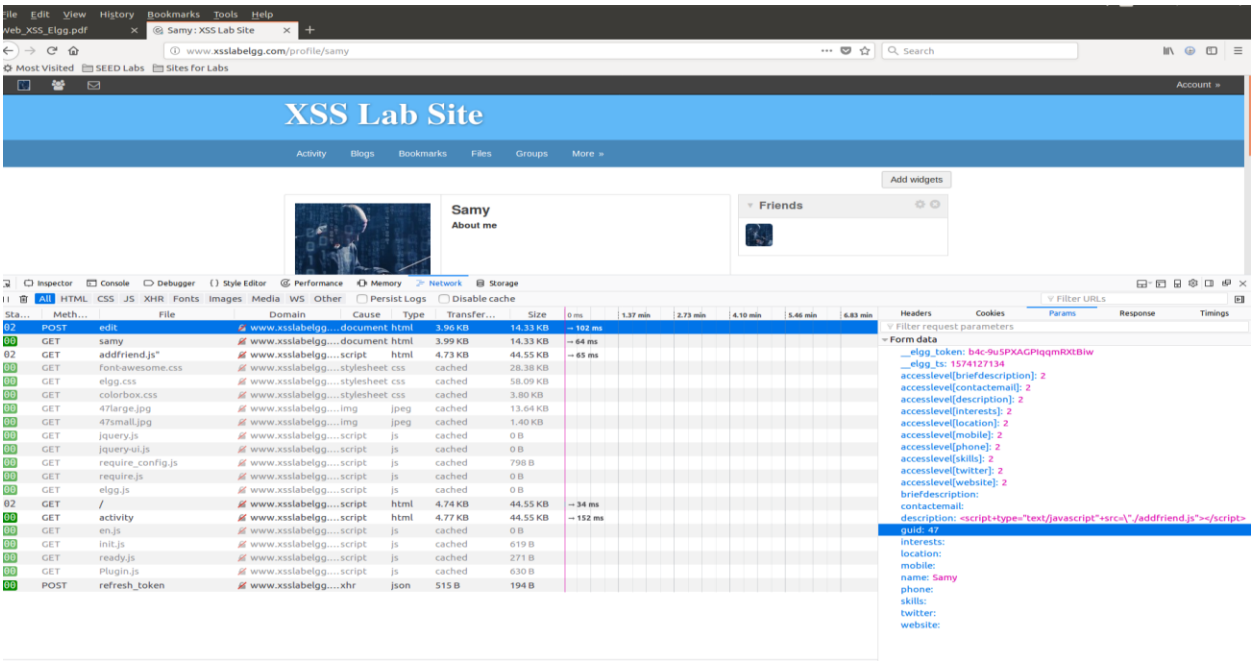
2) If the`Elgg`application only provide the Editor mode for the"`About Me`"field, i.e.,you cannot switch to the Text mode, can you still launch a successful attack?

Answer: Method tried

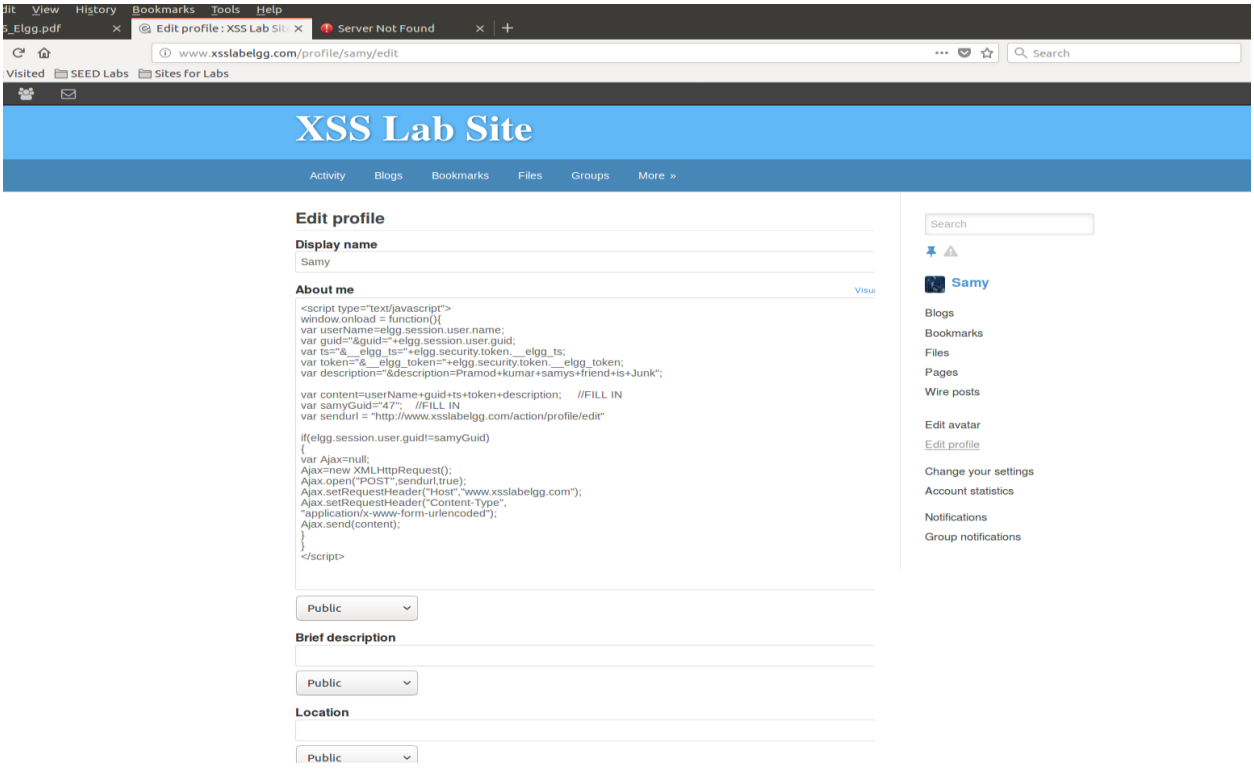
1) Make whole script in one line, but again everything was converted to html tags
2) Create a JS file with out script and add just one line to fetch the script. But as we can see in the editor, it was converted into html tags. "<" converted to "&gt". Hence, html will process &gt not as "<" and it wont recognize it as script.
3) 

Task 5:

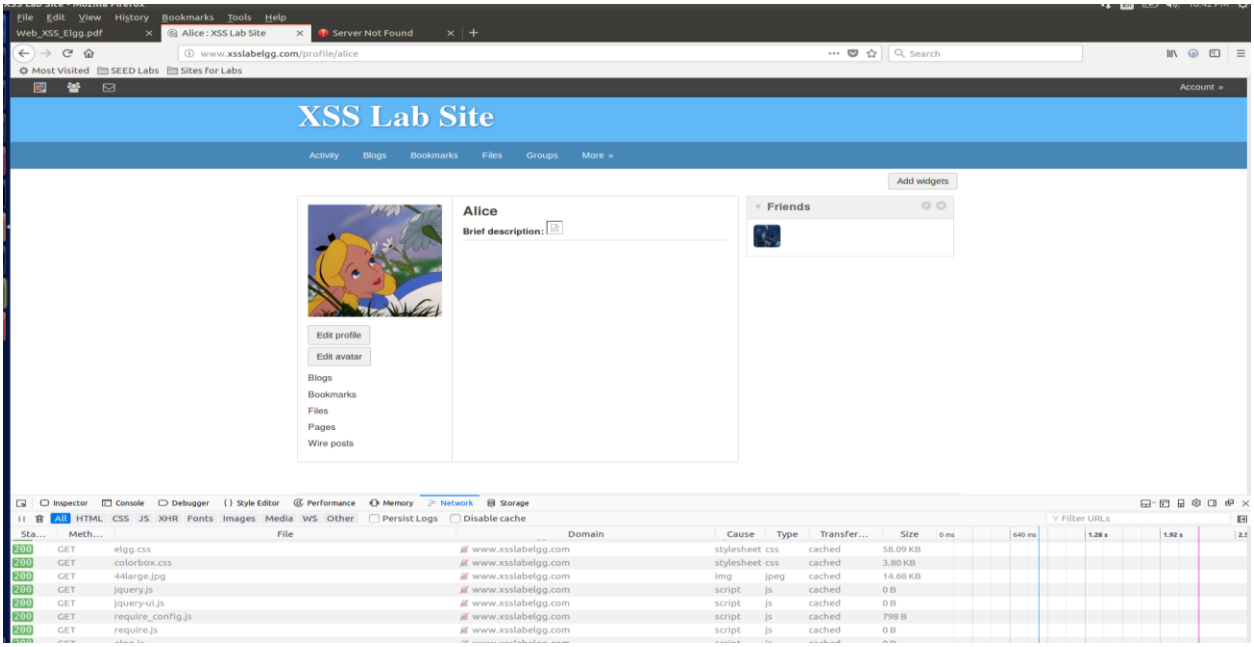
Step1: Find the pattern/URL which used to edit about me in the server.



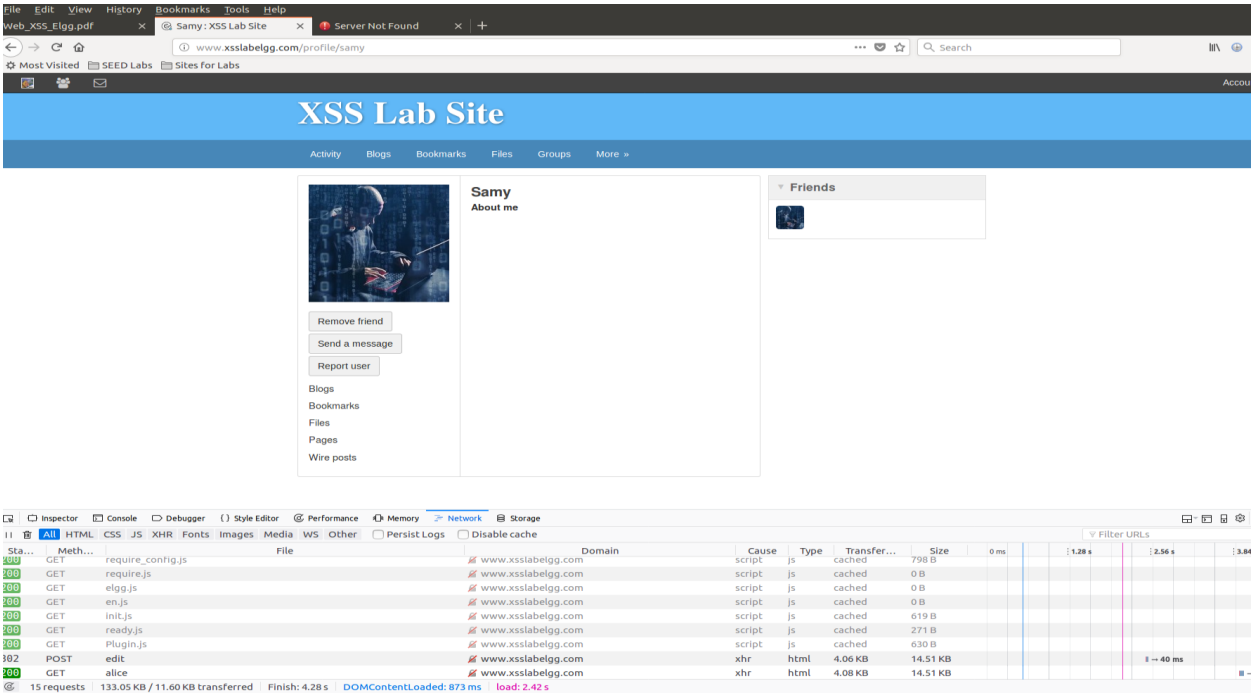
Now we know the URl and its parameter. Write a script and past in about me



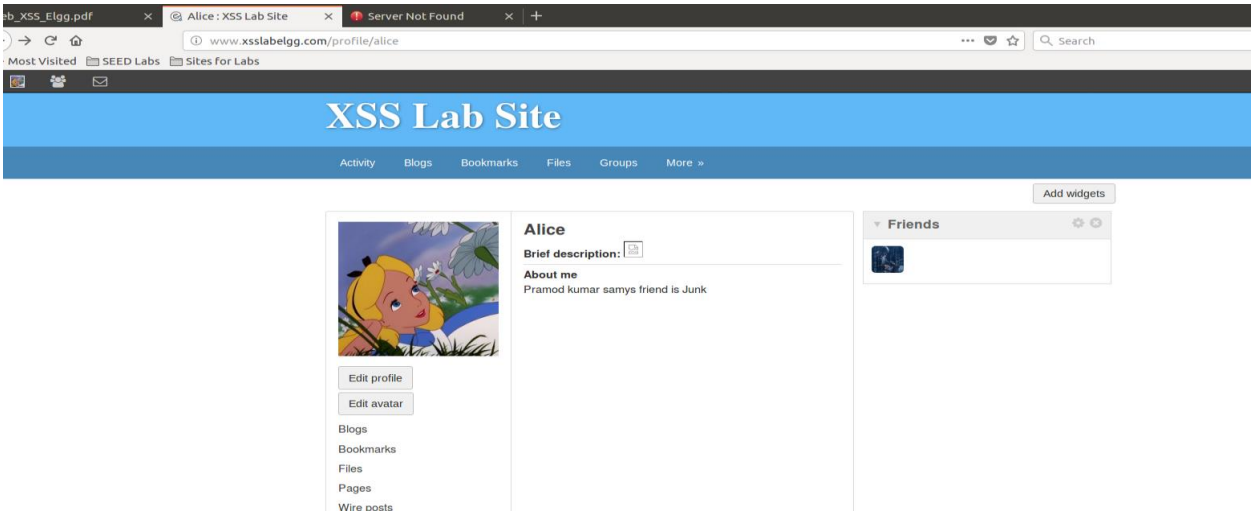
Alice profile before visiting



Now visit Samy profil, We can see in he below screenshot that our script in disccription got executed.

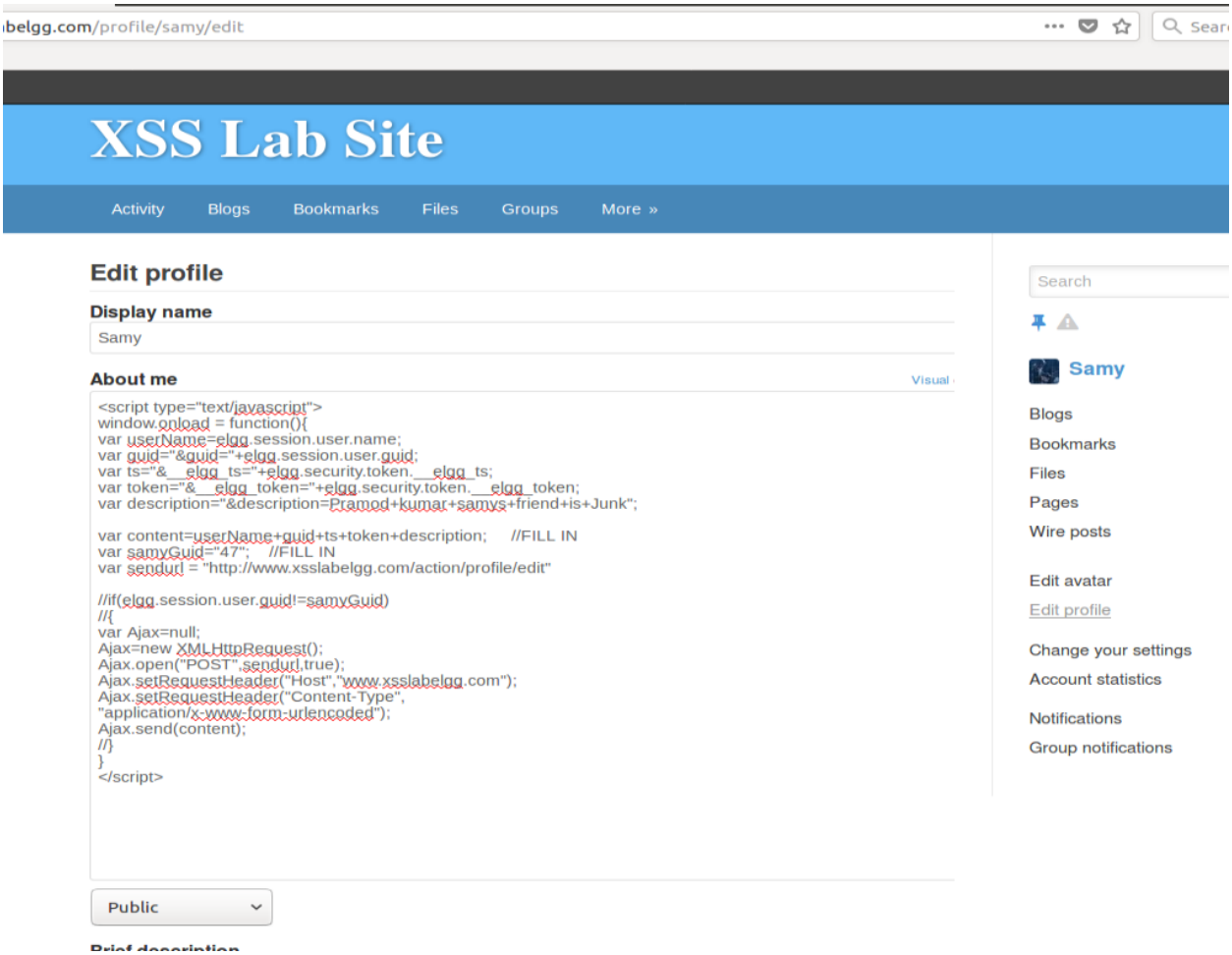


Now Alice profile is edited:

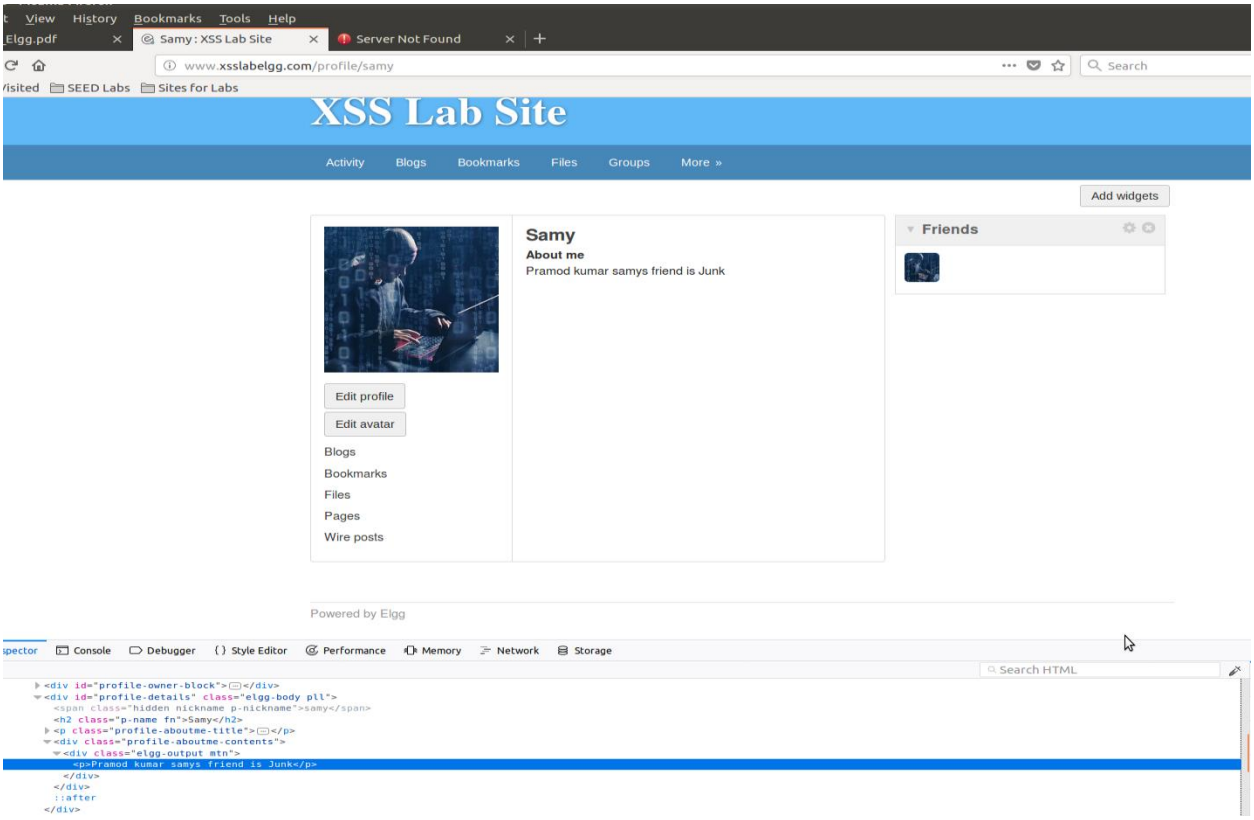


Now remove that line mention in the pdf and repeat the experetment

Observation : purpose of that that line is not to modify smay its own profile, if that happens then whatever we have written in the description will overwrite the script and our attack wont happen.

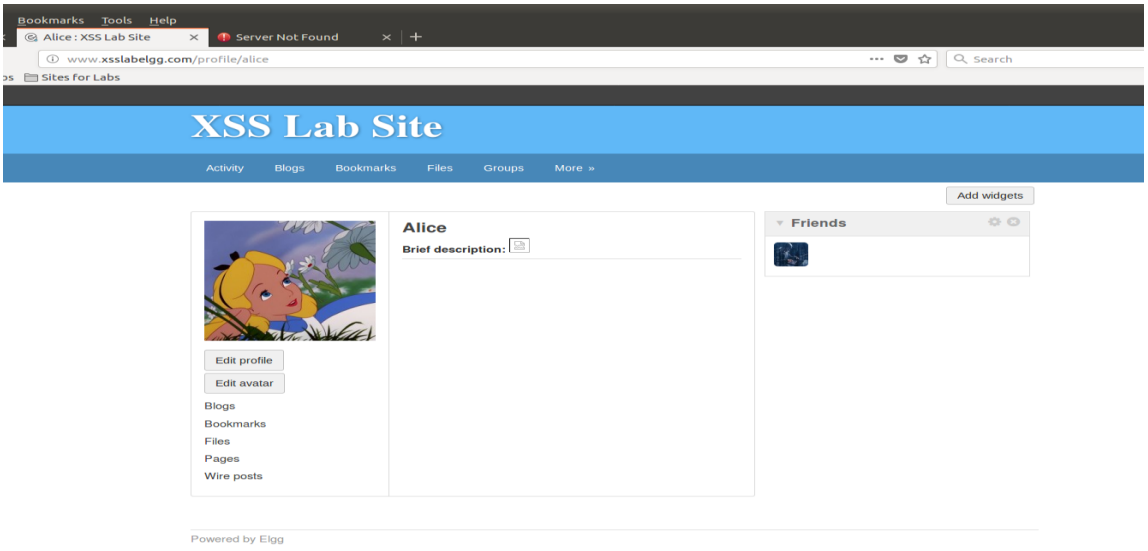


On reloading “samy” profile we can see that script is not longer in the DOM

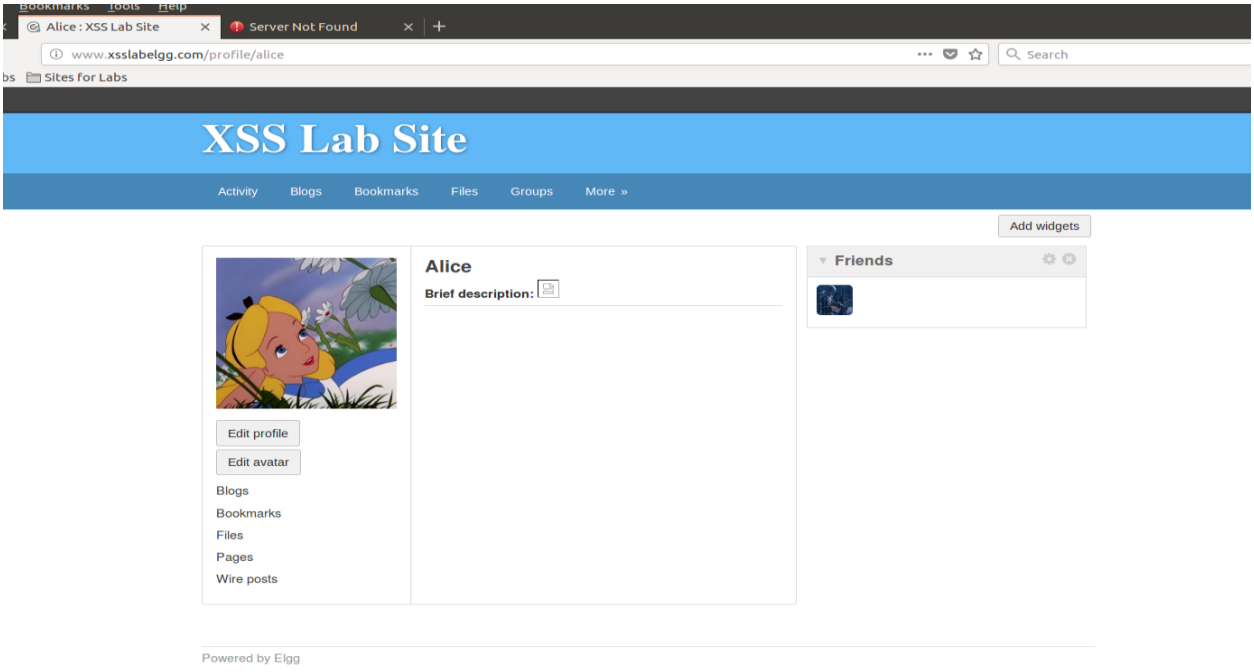


Lets try with alice empty profile and visit the samys profile

Alice profile before visiting samys profile

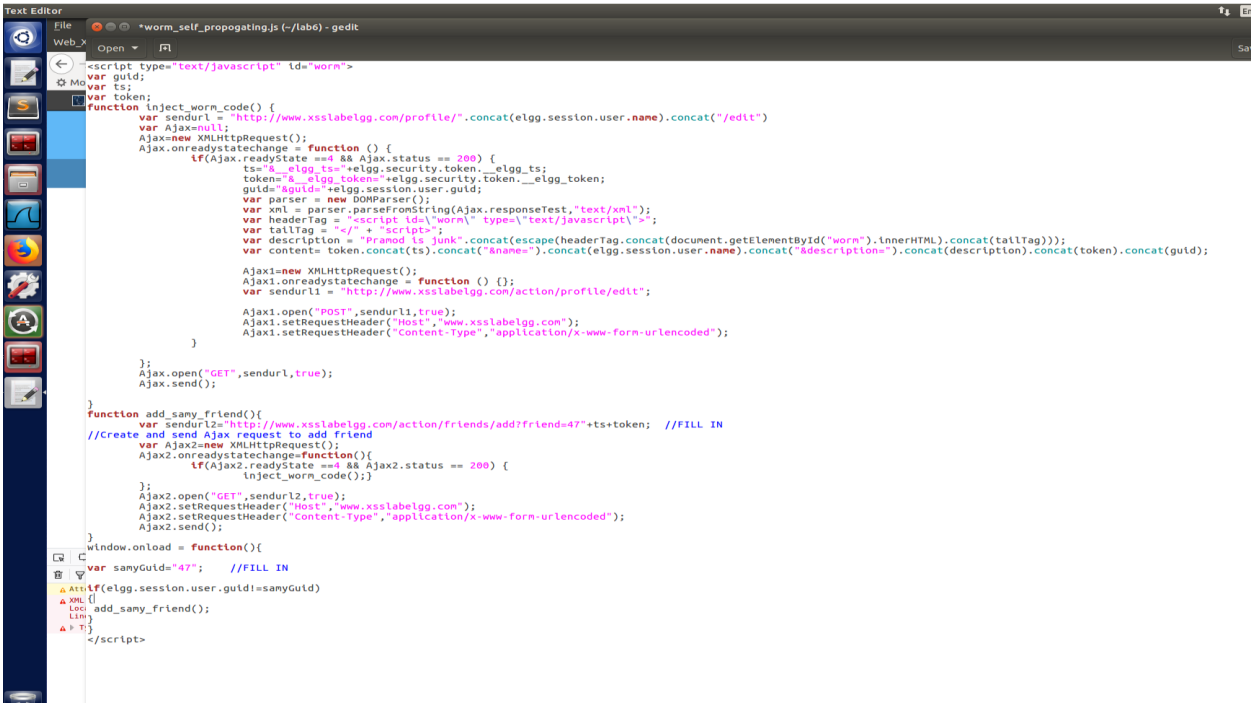


Alice profile after visiting Samy profile.. **Nothing happen**

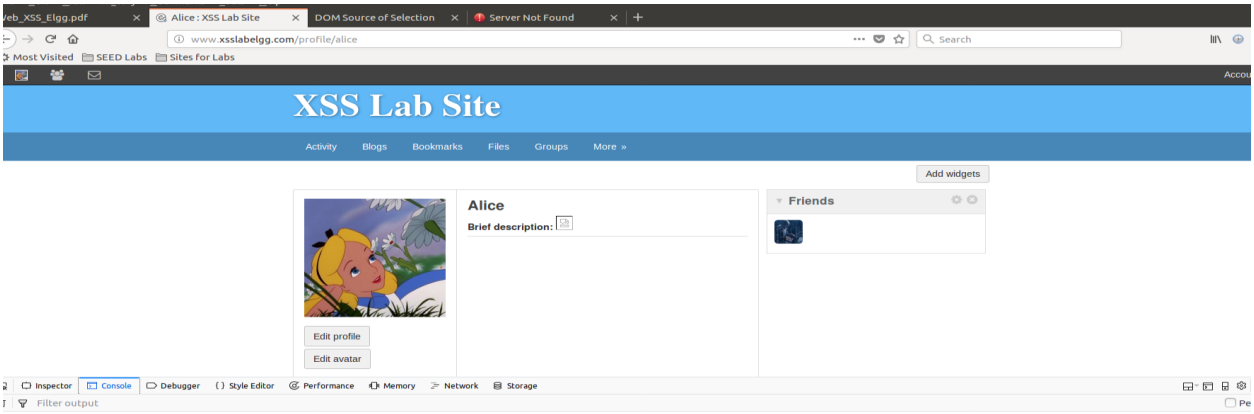


Task 6:

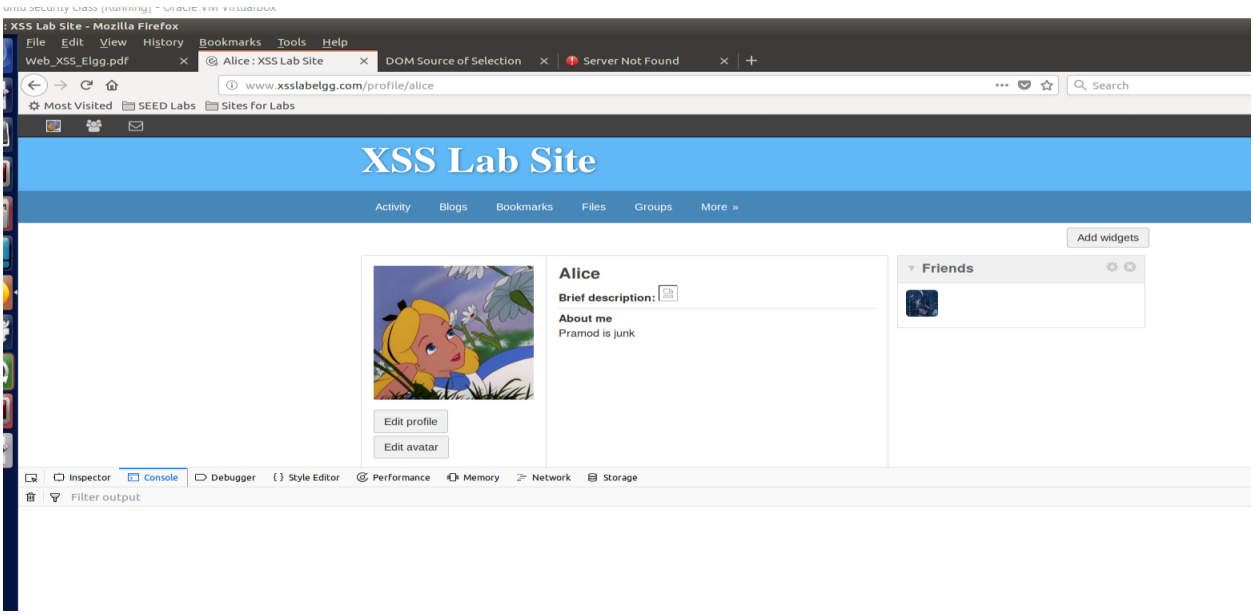
Script used in DOM



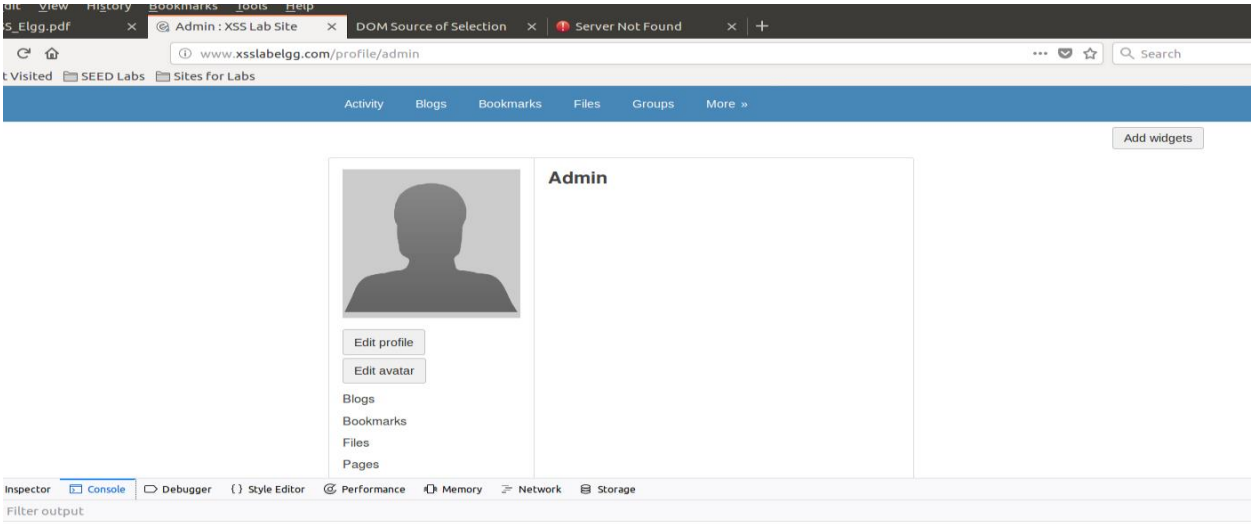
Alice profile



After visiting sam profile



Admin profile before visiting “Alice”



After visiting Alice profile