**CSRF Lab 2.0**

Contents

[Environment Setup: 3](#_Toc119796149)

[Task 1 7](#_Toc119796150)

[Task 2 8](#_Toc119796151)

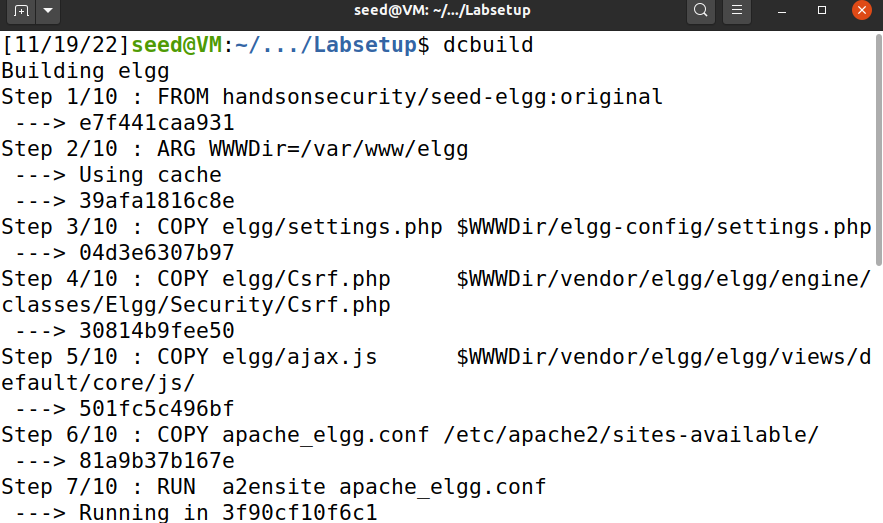
[Task 3 13](#_Toc119796152)

[Task 4 18](#_Toc119796153)

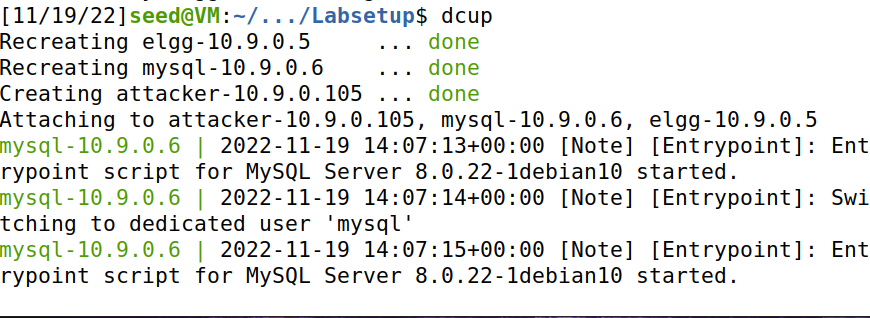
[Task 5 21](#_Toc119796154)

# Environment Setup:

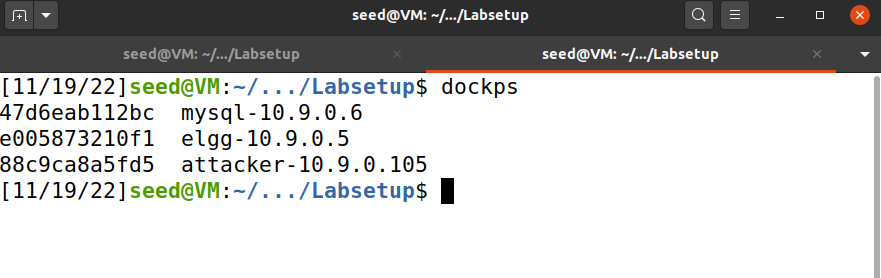
After downloading docker .yml file the docker is setup using commands as follows:

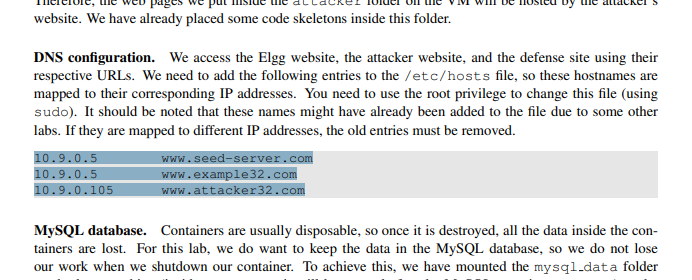


Dcup is then ran to get the container up and running

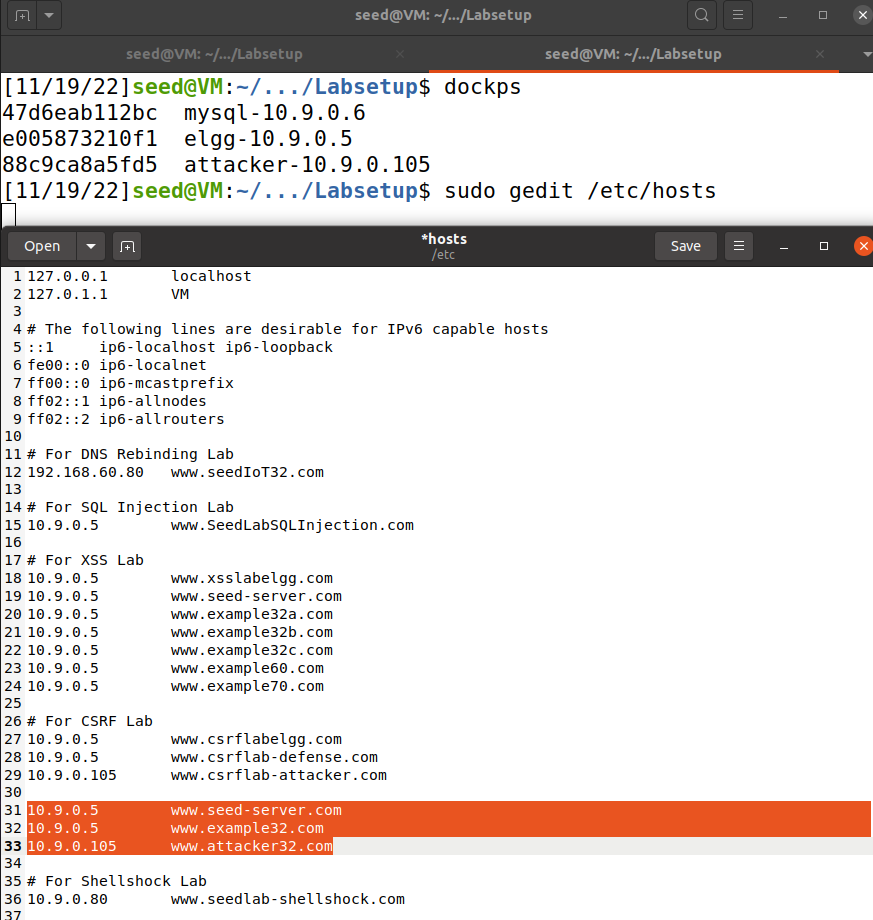


For DNS config we can check DNS setted up that will be used in our labs

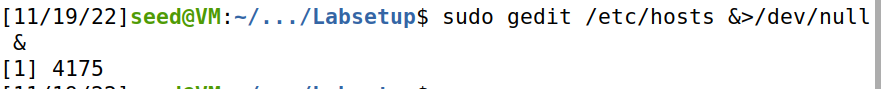




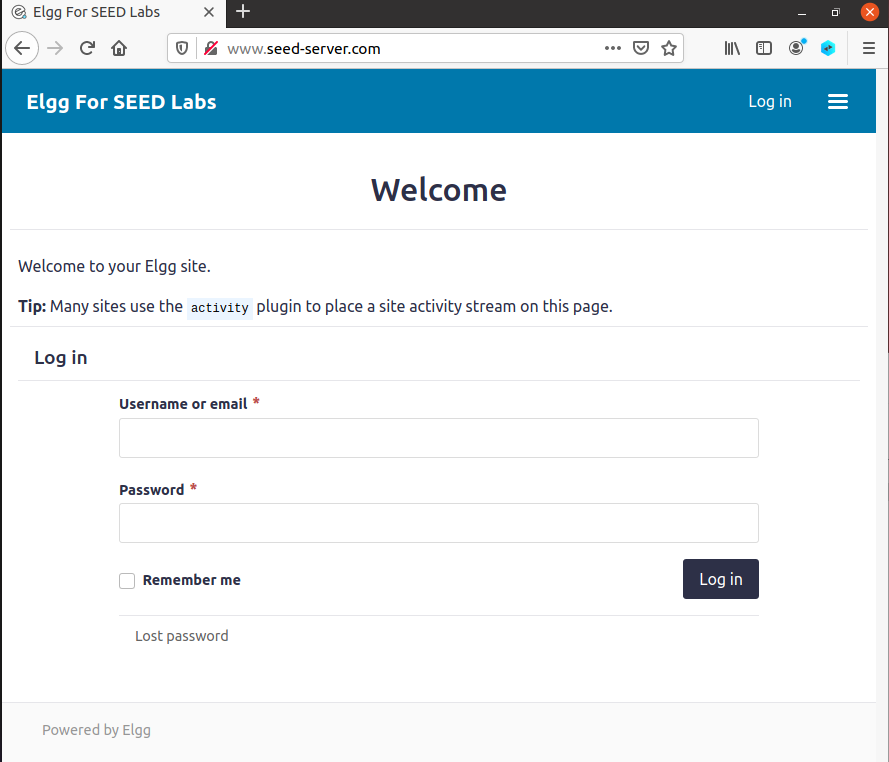
These new DNS are updated into the hosts file.



The host file is updated and is saved to be used as the same alias as the set up lab.

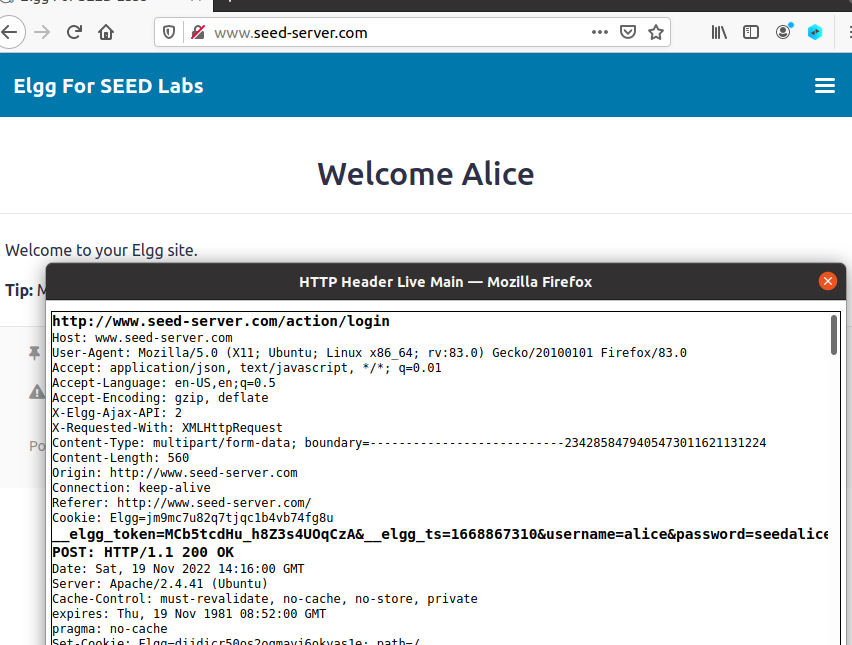


Now I have loaded the web server for CSRF lab provided in lab setup.



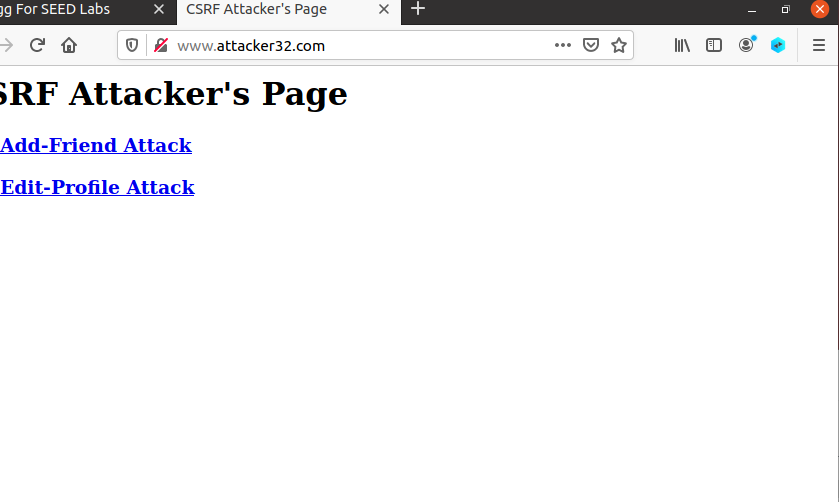
# Task 1

First we add http live header to check all the requests where it is visible that the login credentials have been caught in the header.

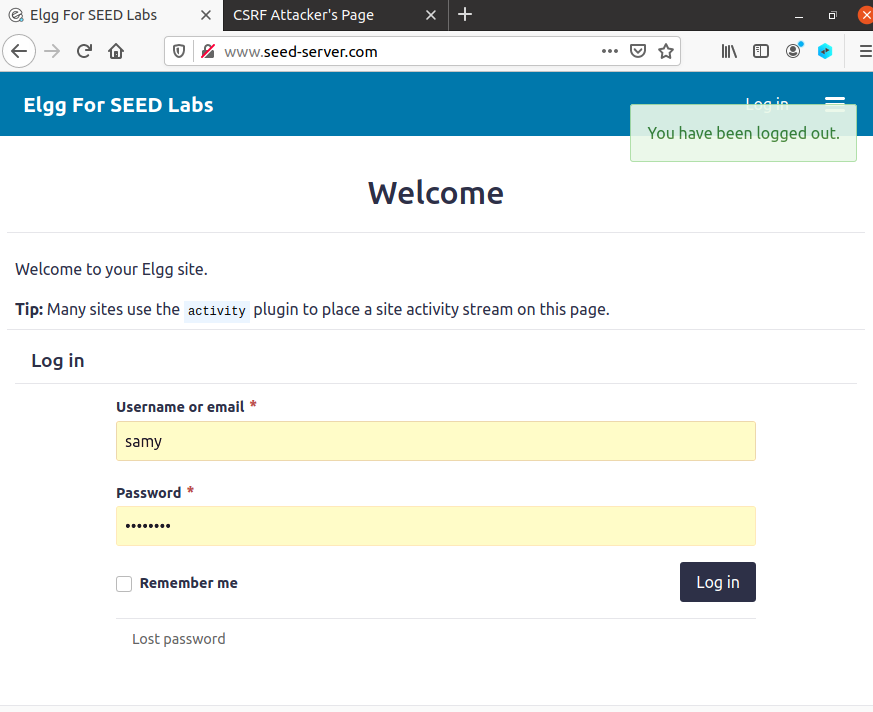


# Task 2

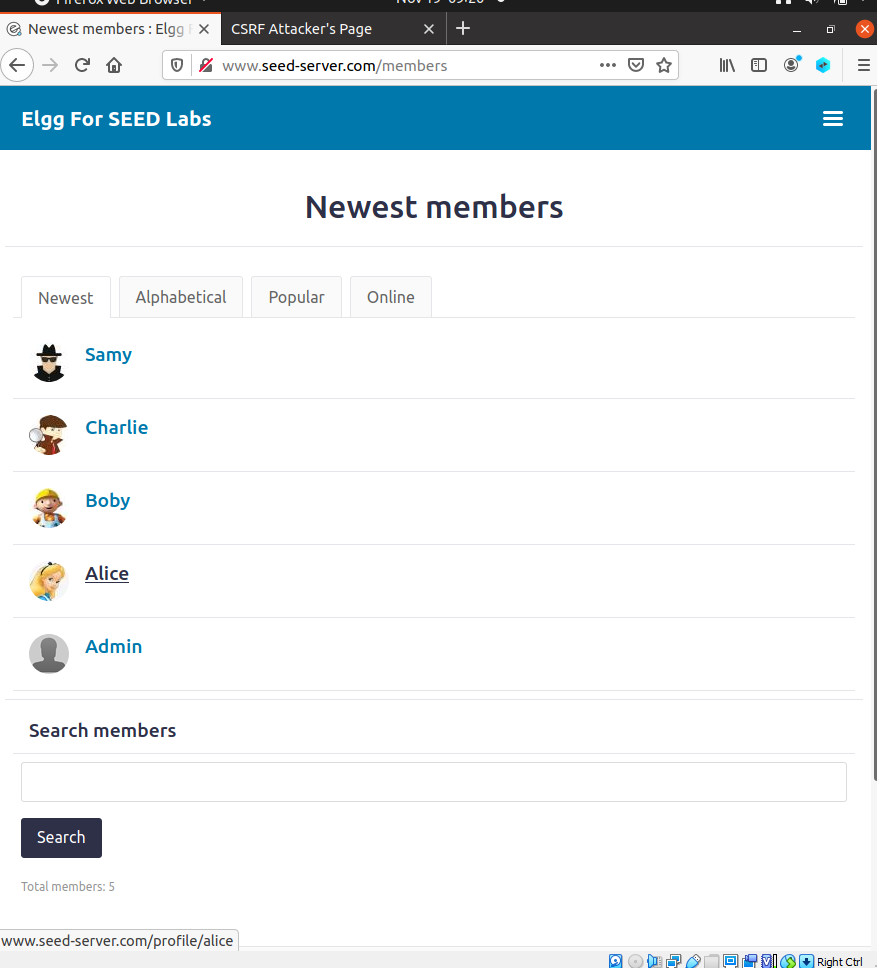
Now we will use attack32 web page to launch attack.



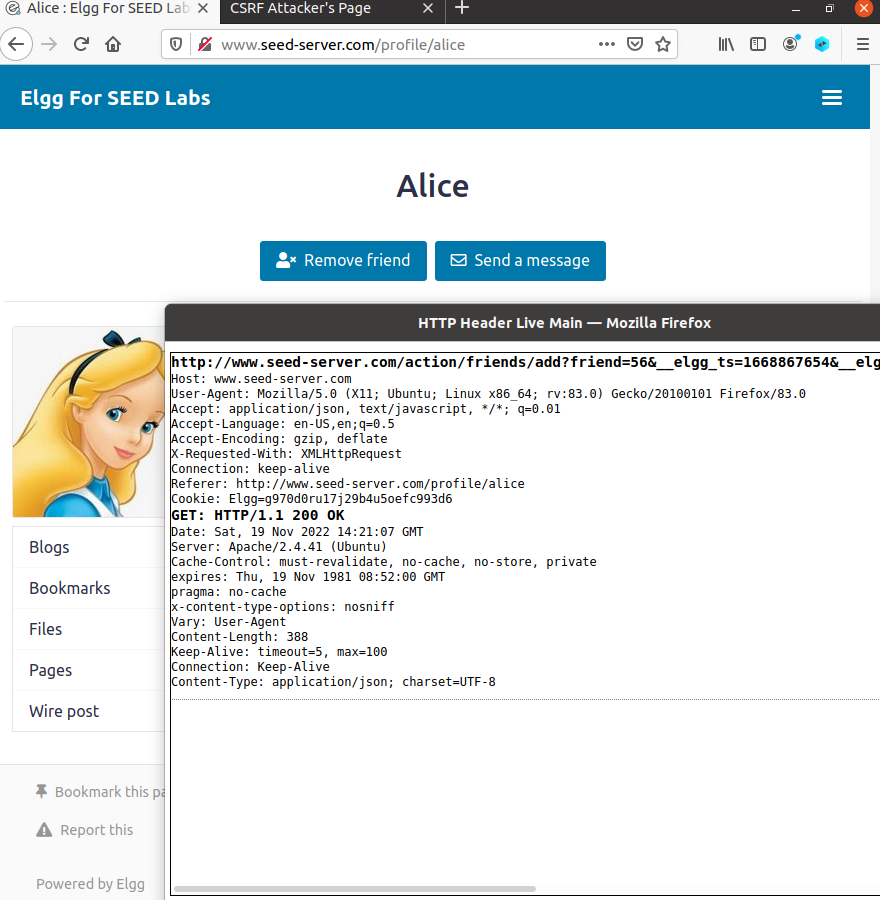
Logging in as Samy who is the victim here.



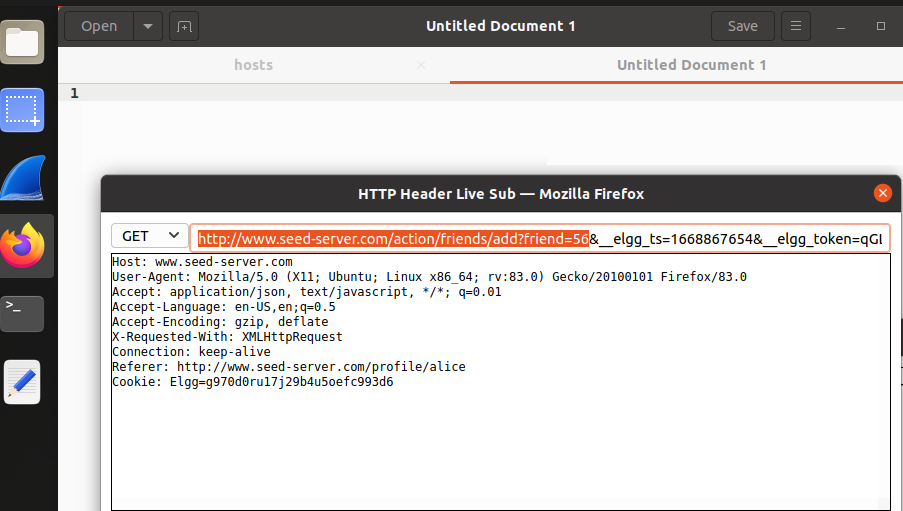
Checking members and locating Alice.



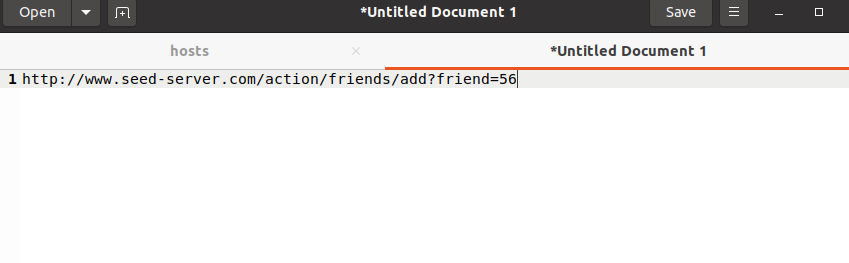
Now we add a friend into Samy’s friend list and take the request sent to add friend. Here, Alice’s guid is also taken and from the request we will now then change the request guid from that of Alice to Samy so the request will make Alice add Samy.



Taking out the selected portion for the purpose of Attack.



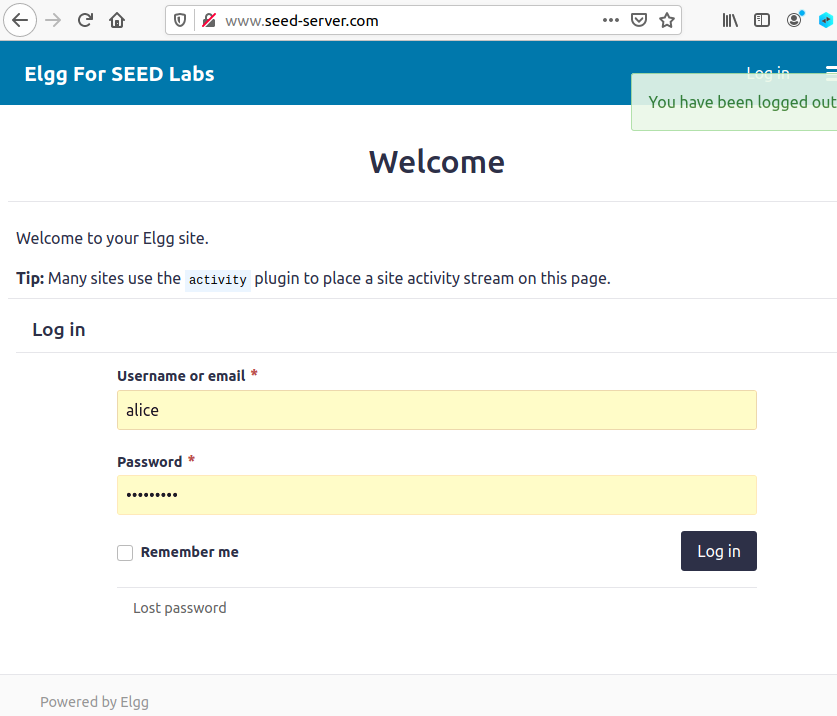
Placing the information here.



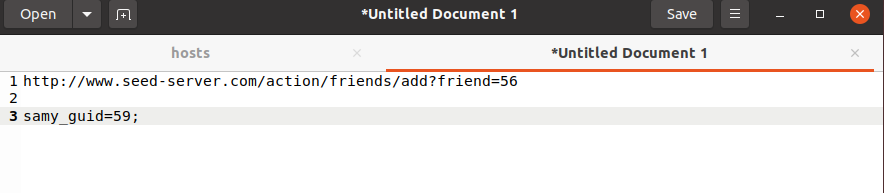
Now checking Samy’s guid to target Samy.



Logging in as Alice now.

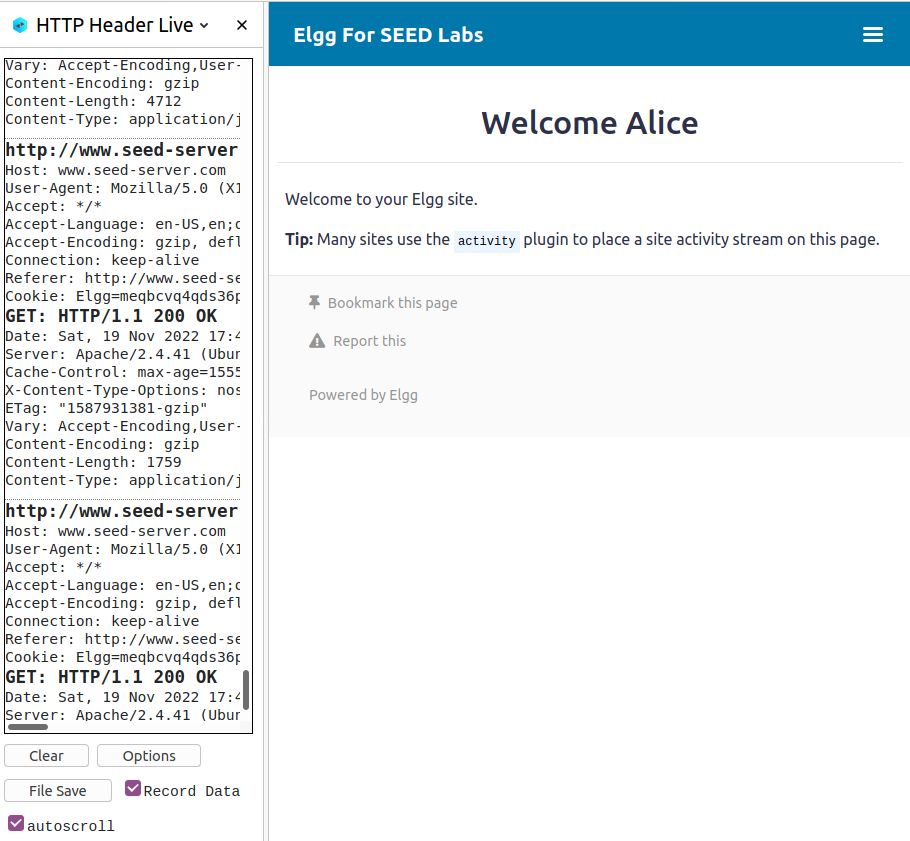


Placing information in a document temporarily which I gathered above.

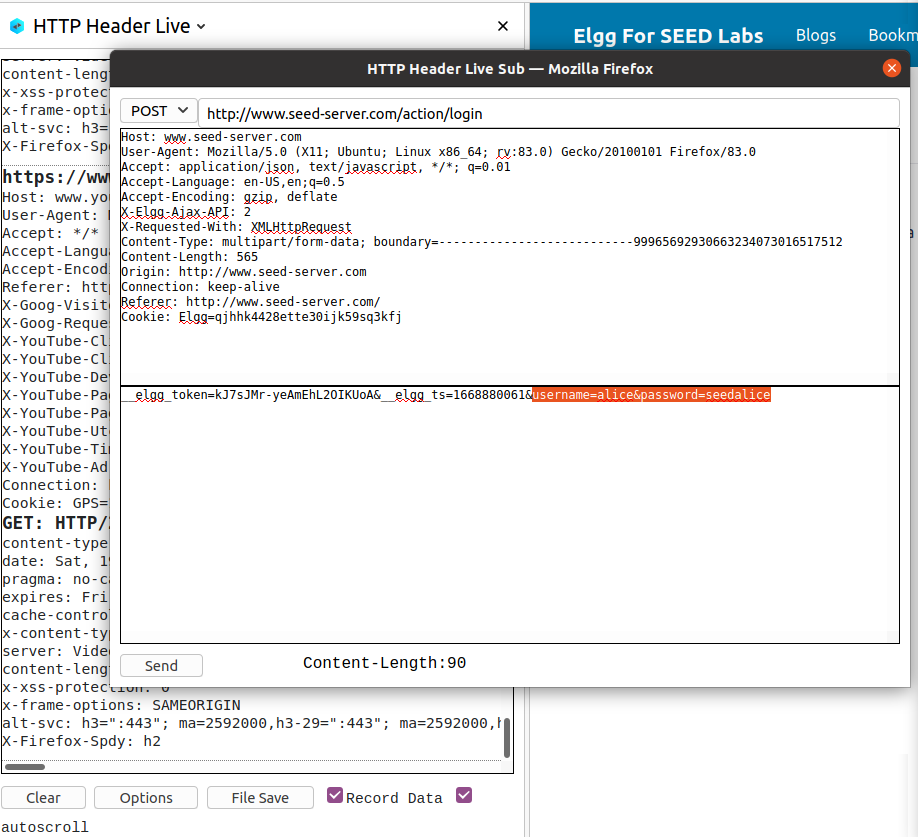


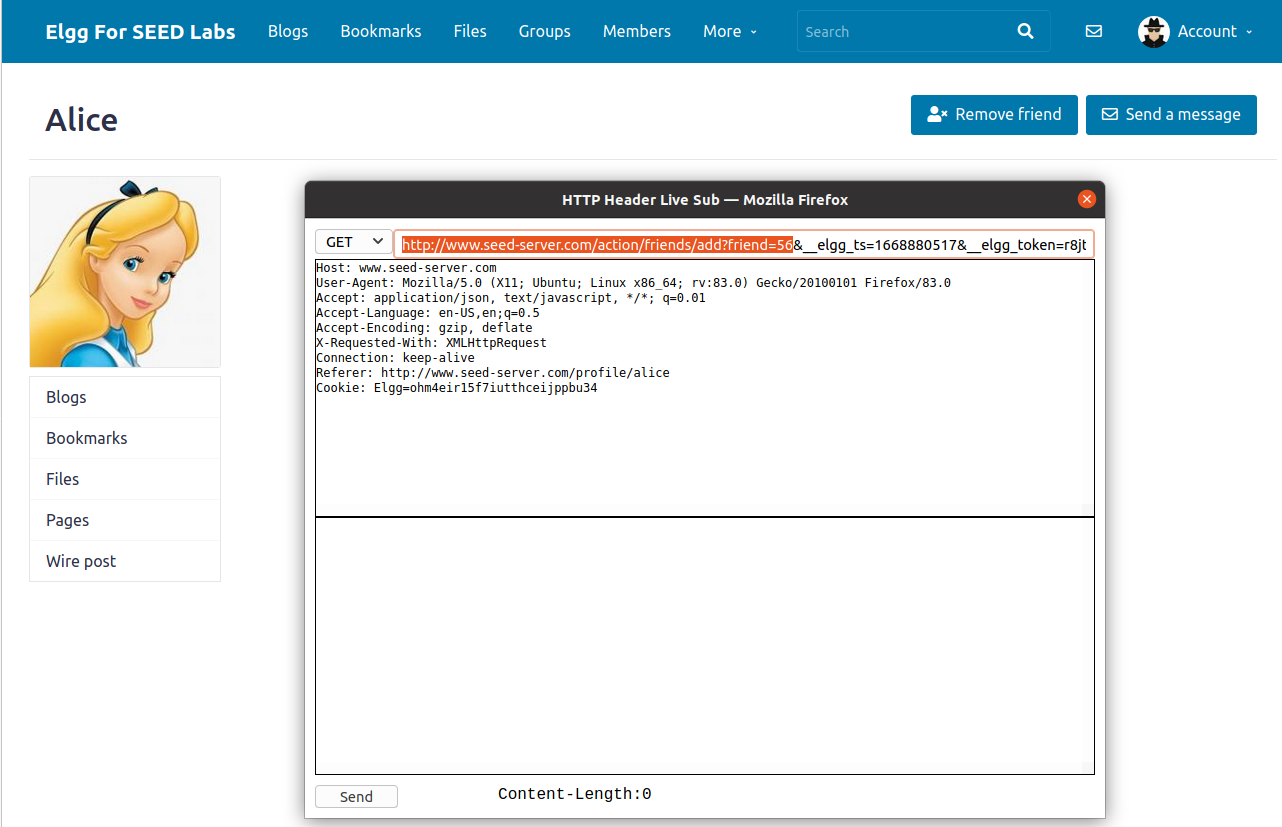
# Task 3

Checking live HTTP Header Activity.

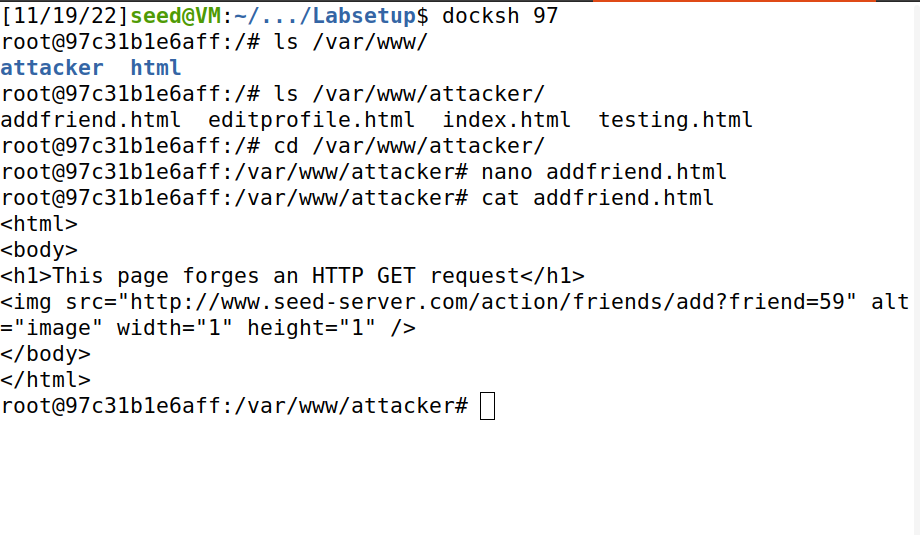


Checking the POST requests while live capture in which login credentials are caught.

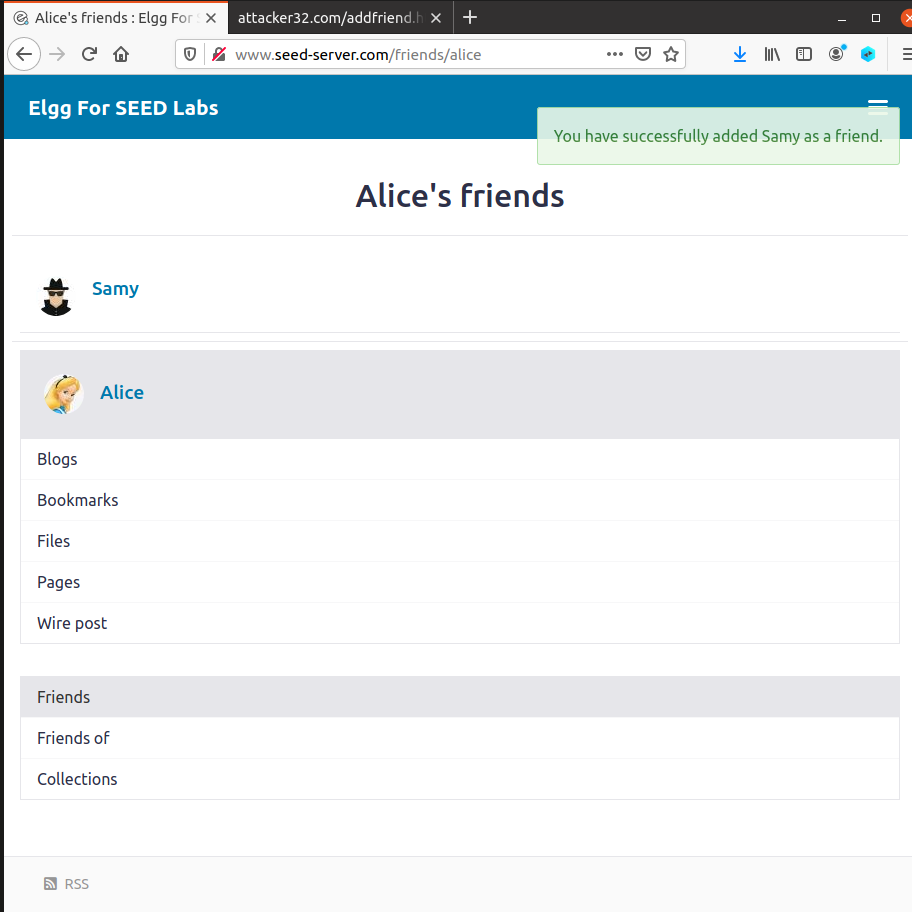




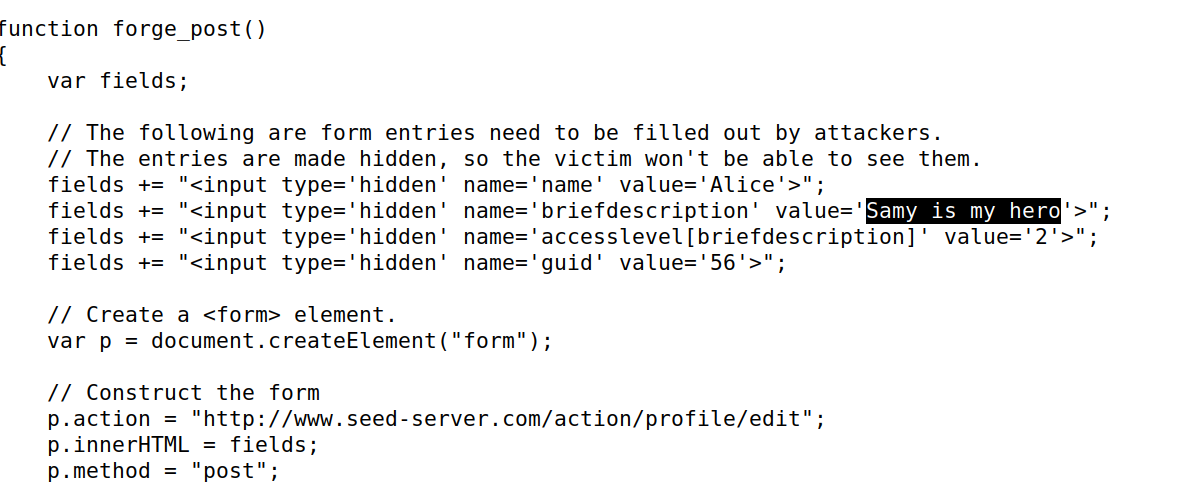
After checking the contents of the file.

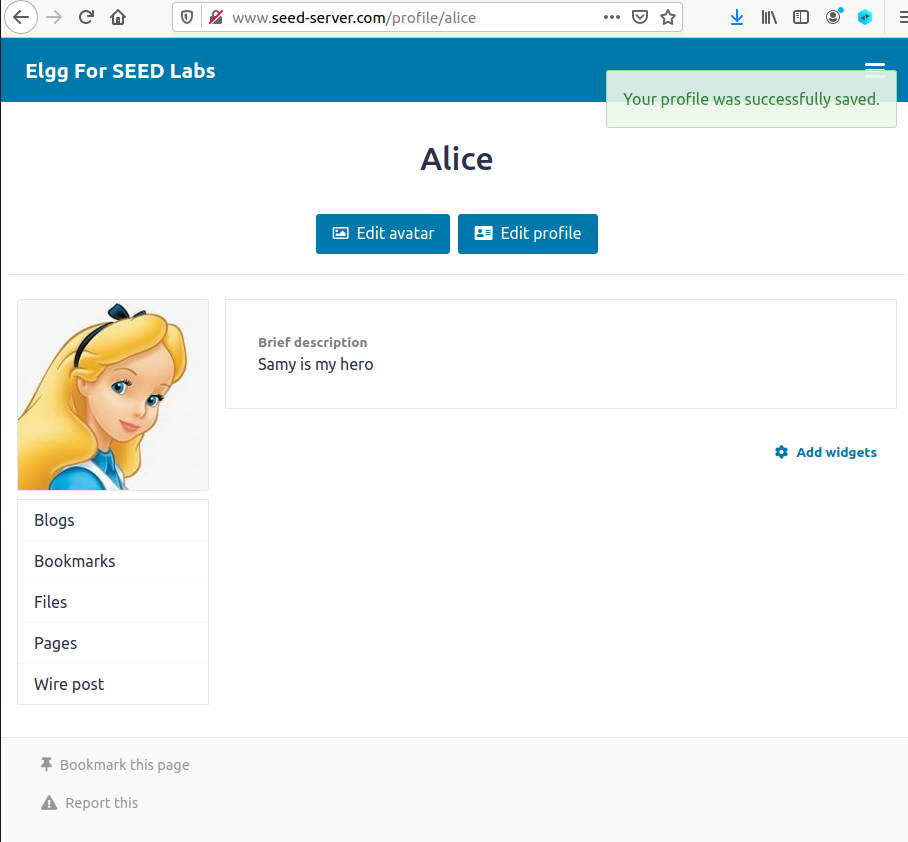


Here u can see the source code is changed and the source request is changed for alice which make samy her friend.



Now similarly we will change the post request and save target in the source code to alices. And set out request to add description of samy is my hero now the req uest will change alice’s prif



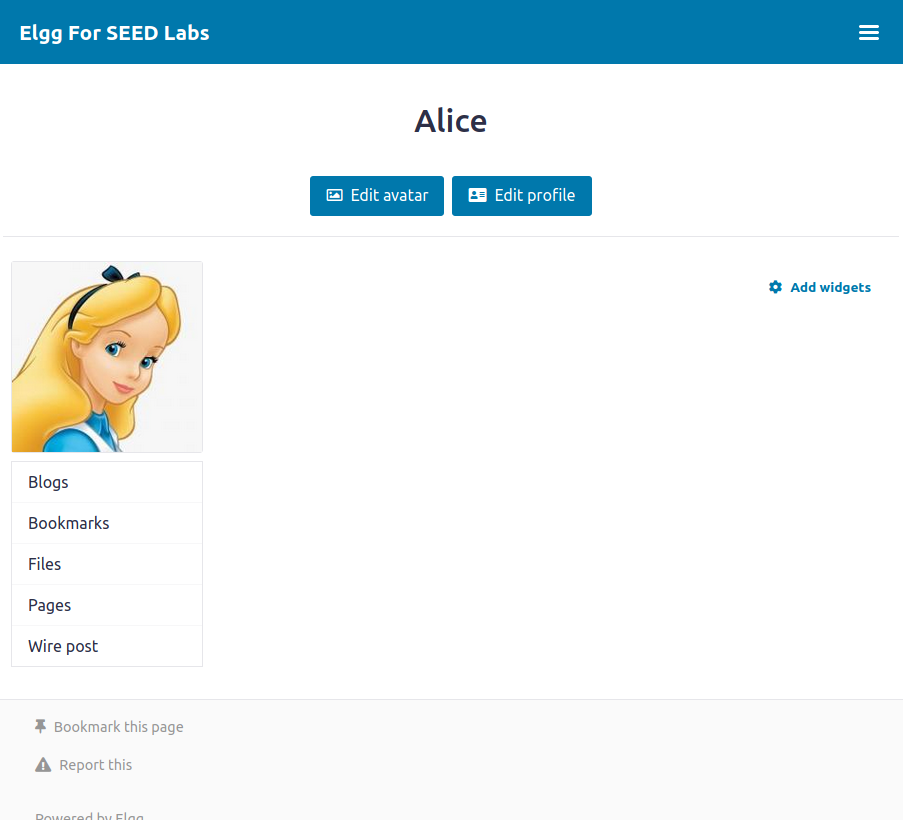


# Task 4

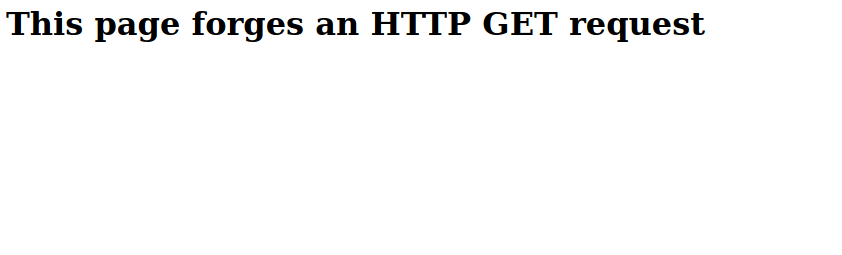
Here counter measure used is we turn off all return tokens from the shown below code we can see the return statement is used to return tokens. If this return statement is removed It will act as countermeasure to all of our above attacks.



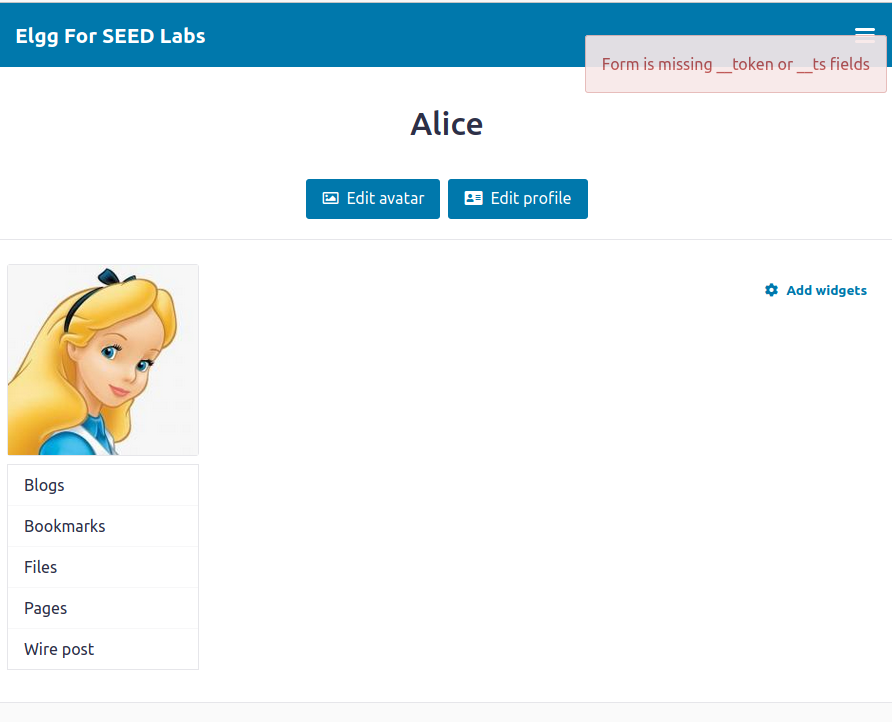
Here we can see alice friend list is again removed and cleared to run attacka again.



View of Attacker Web page.



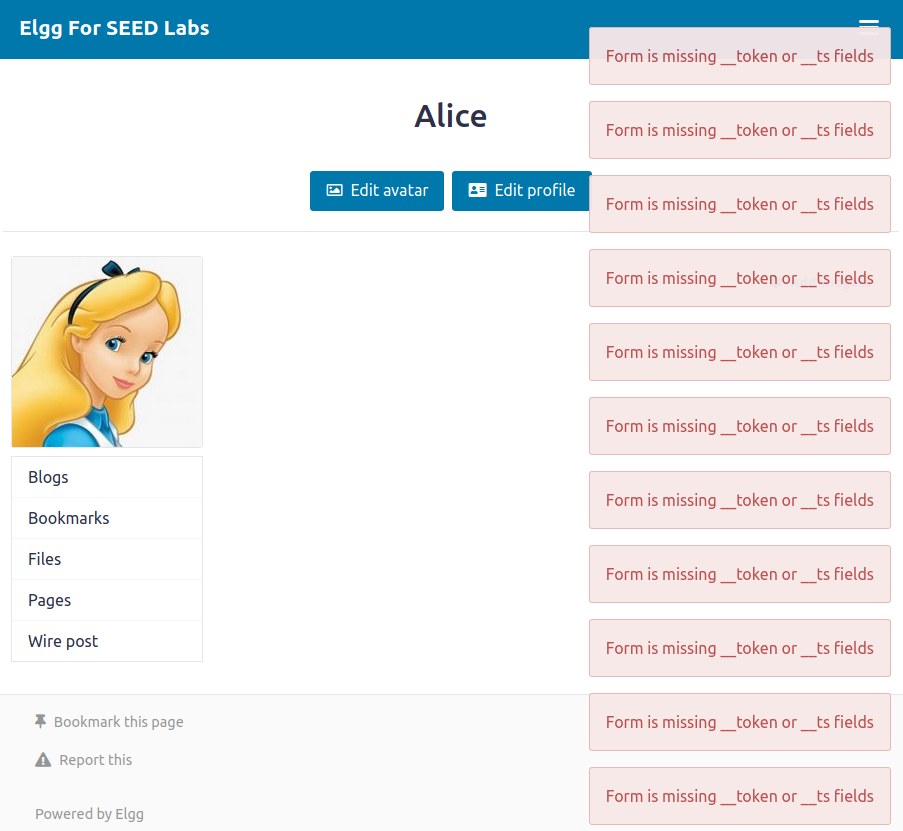
Here the last ran attack now gives error that token are missing and friend list is not added.



Attacker web page again.

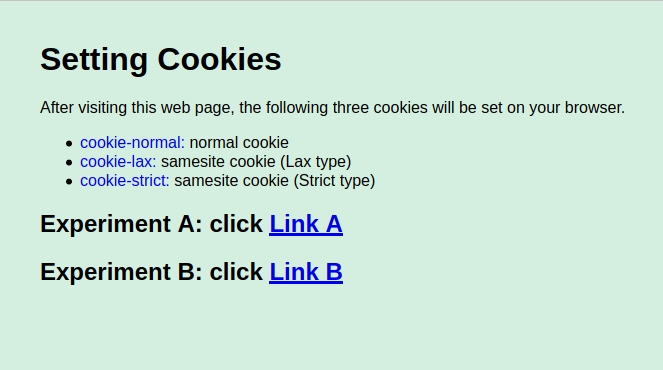


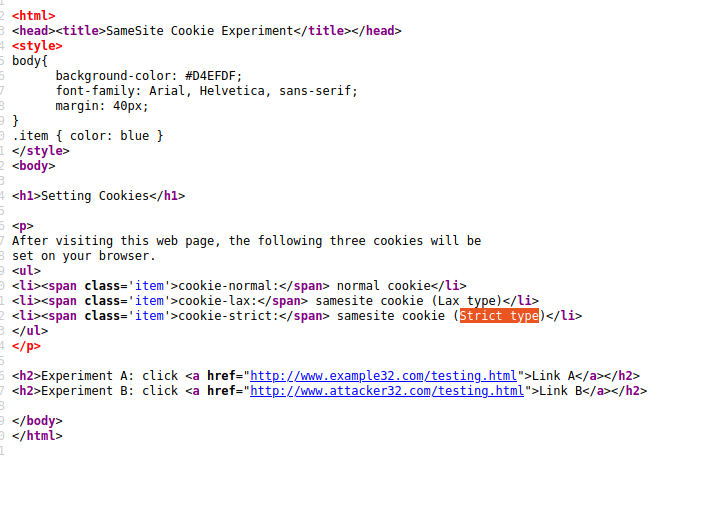
Now again for post multiple errors show up for all the post requests as the tokens are now missing. this is counter measure to CSRF.



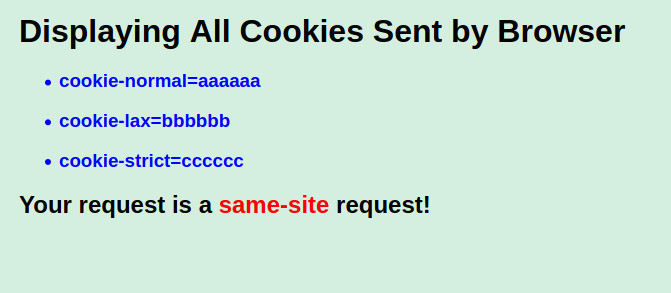
# Task 5

The above shown source code show 2 different cookie type the lax and strict type page.



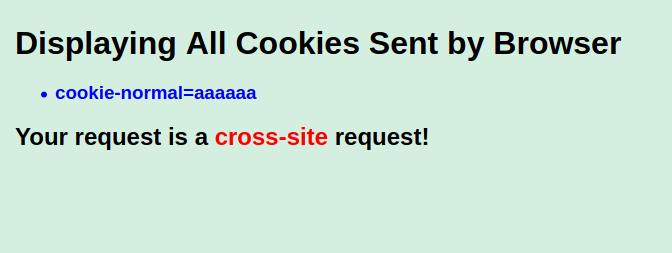




]

Here for lax setting the cookies are displayed for all type.





And for strict setting for of the cookies are missing not taken.