CSE 406

Computer Security Sessional

Assignment 2

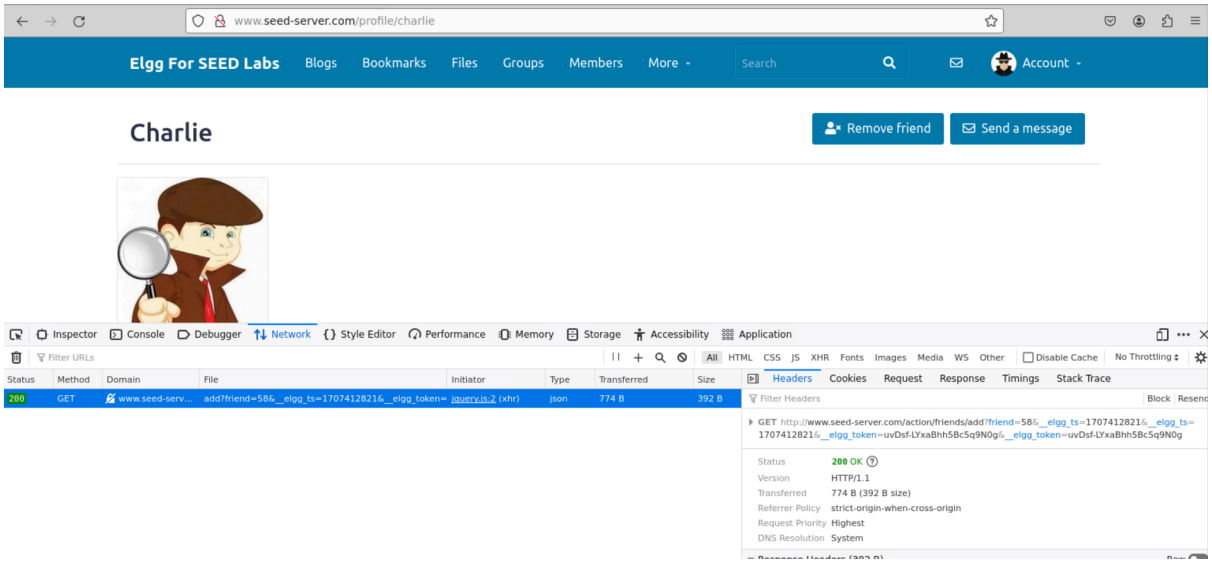
Cross-Site Scripting (XSS) Attack

Name : Sushmita Paul

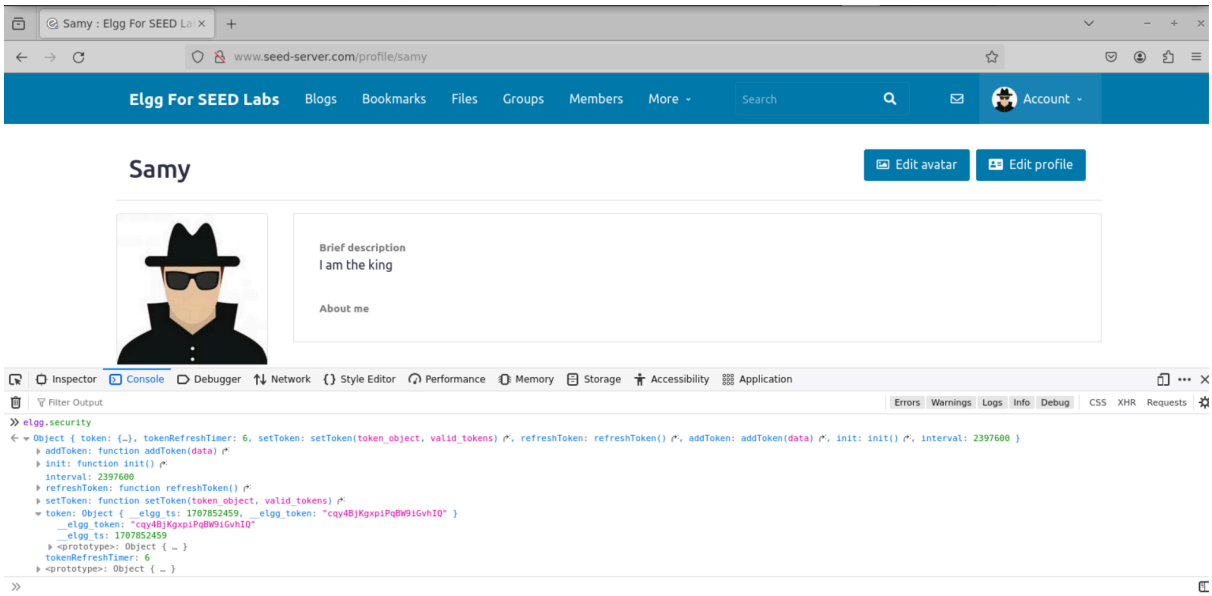
Student ID : 1905086

Task-1: Becoming the Victim's Friend

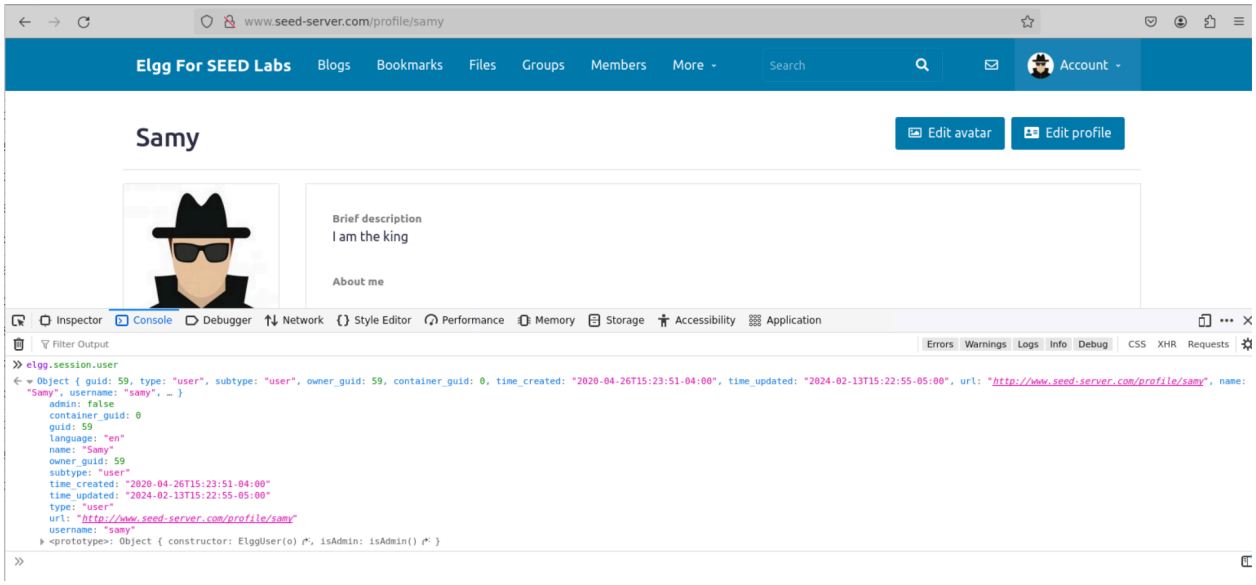
1| checking out friend request url



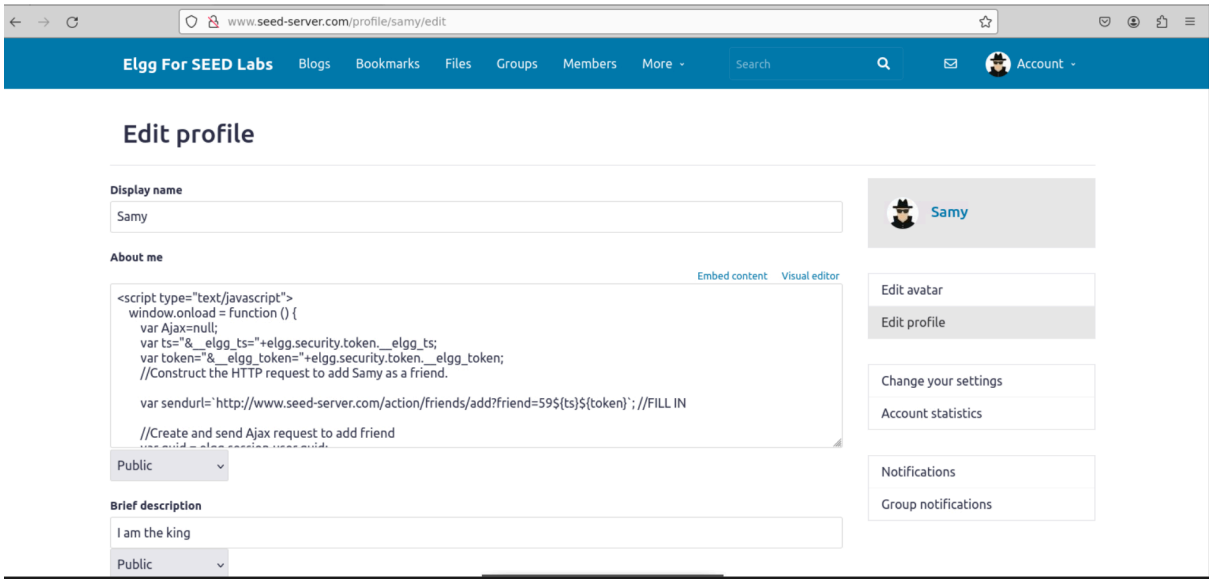
2| Finding __elgg_token & __elgg_ts



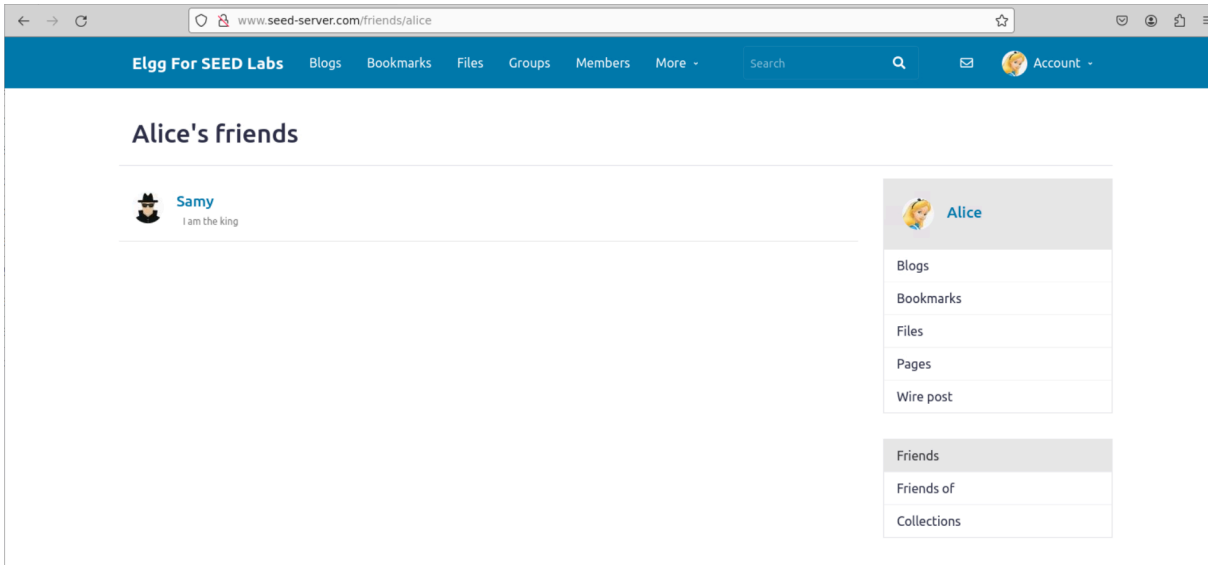
3| Finding samy's guid



4|Pasting malicious script code in samy's about me section and save it.

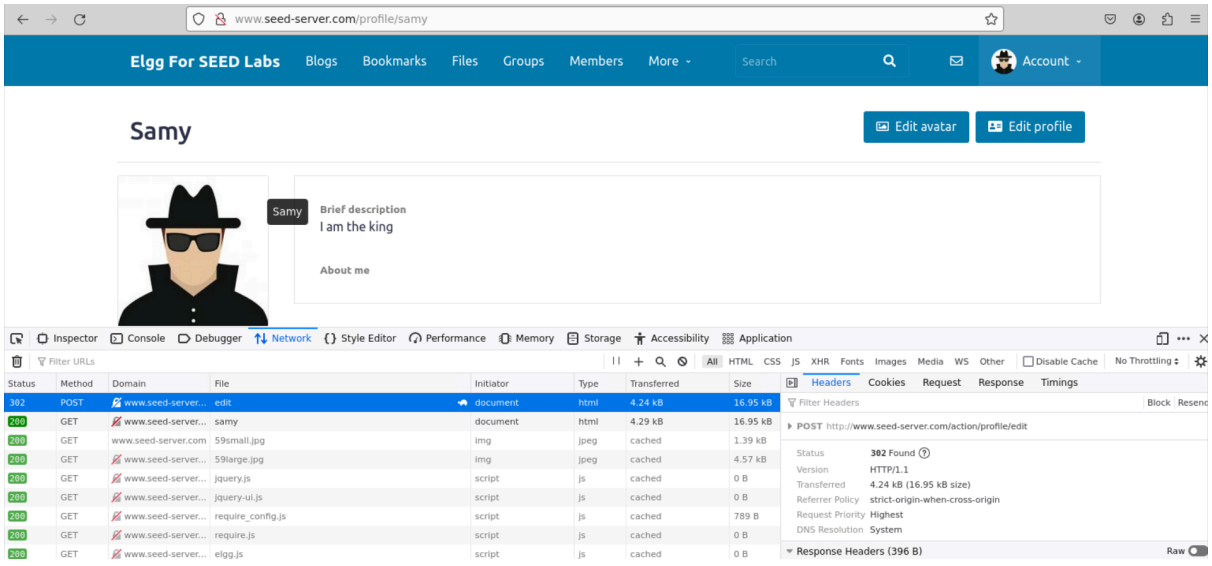


5|Now when alice browse samy's account Samy automatically added to alice's friend list

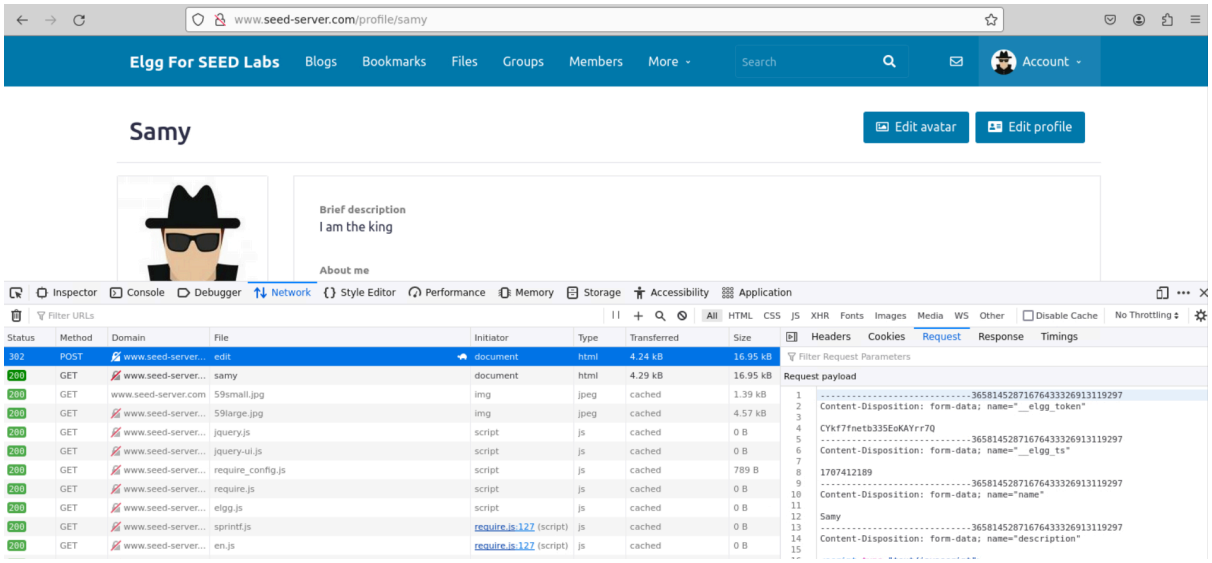


Task-2: Modifying the Victim's Profile

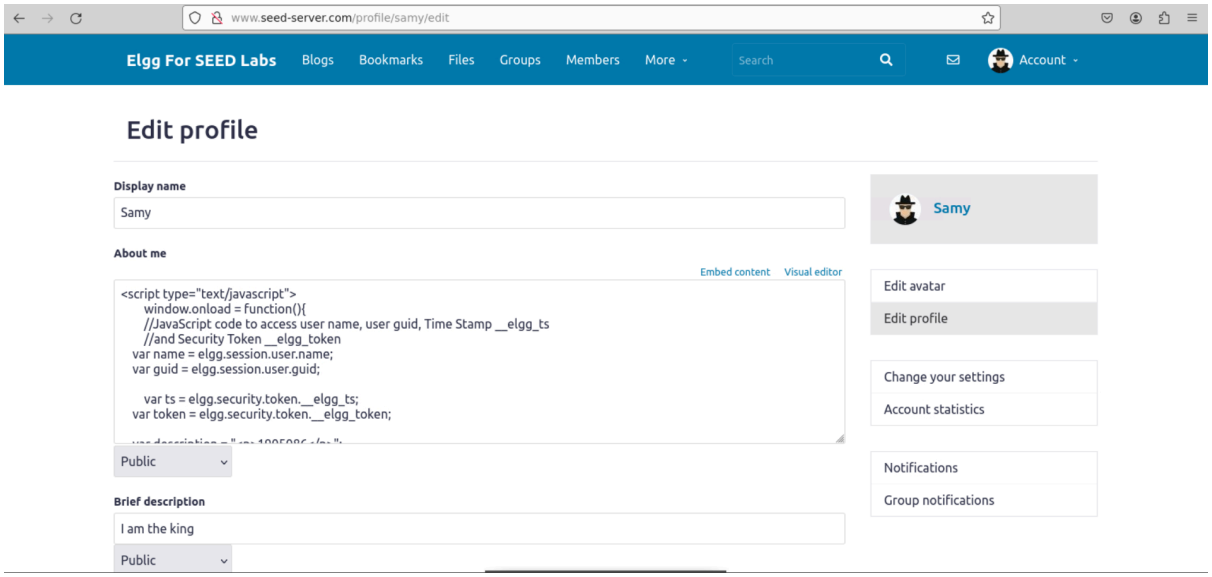
1| Checking out profile editing post method



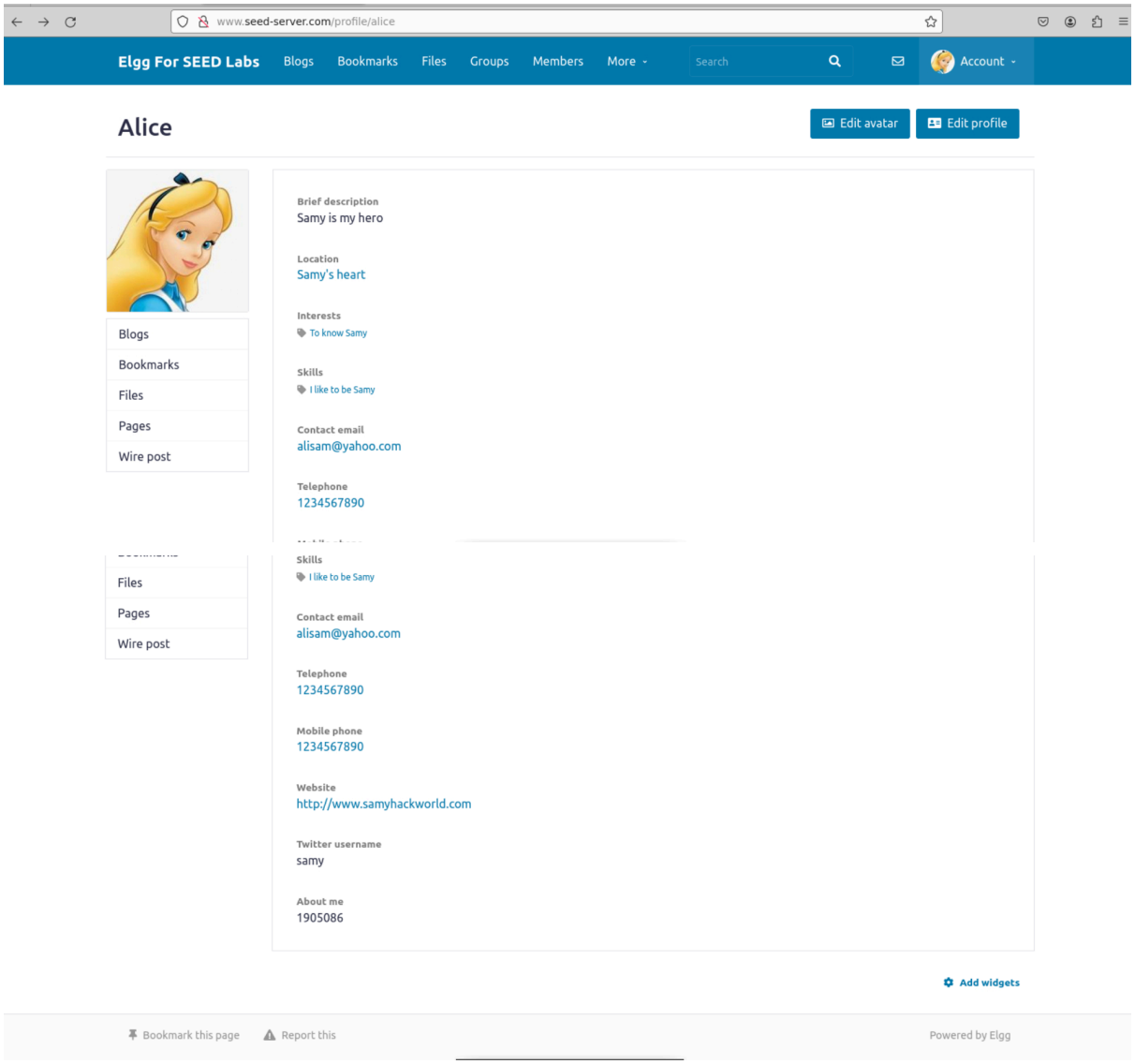
2| Figuring out post request construction for modifying profile



3| Pasting malicious script code in samy's about me section and save it.

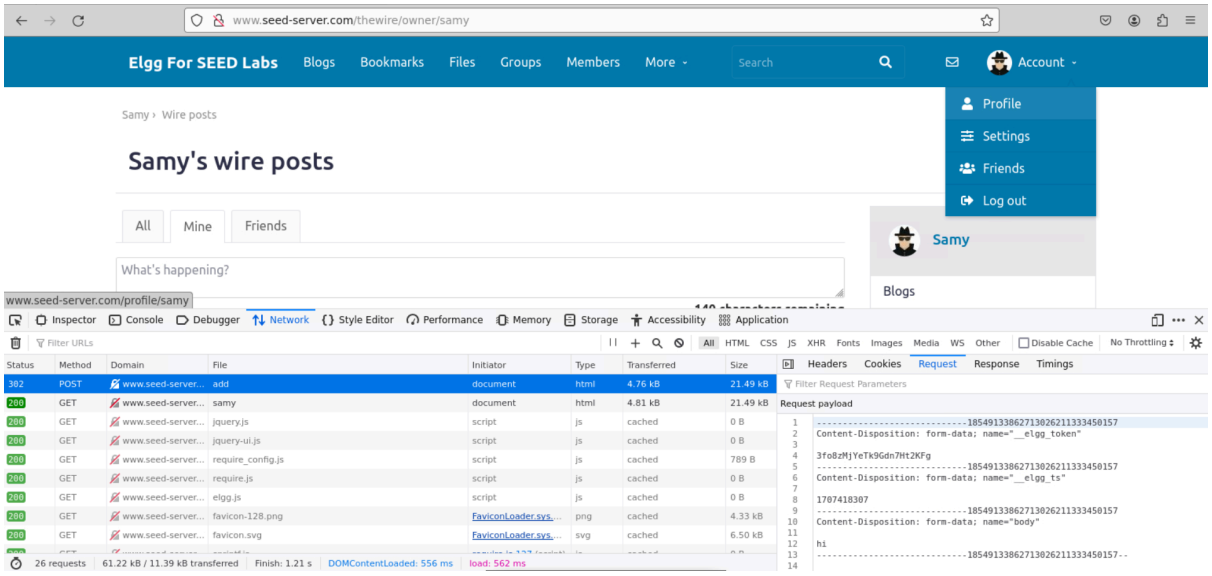


4| Now when Alice browses Samy's profile, Alice's profile gets edited.

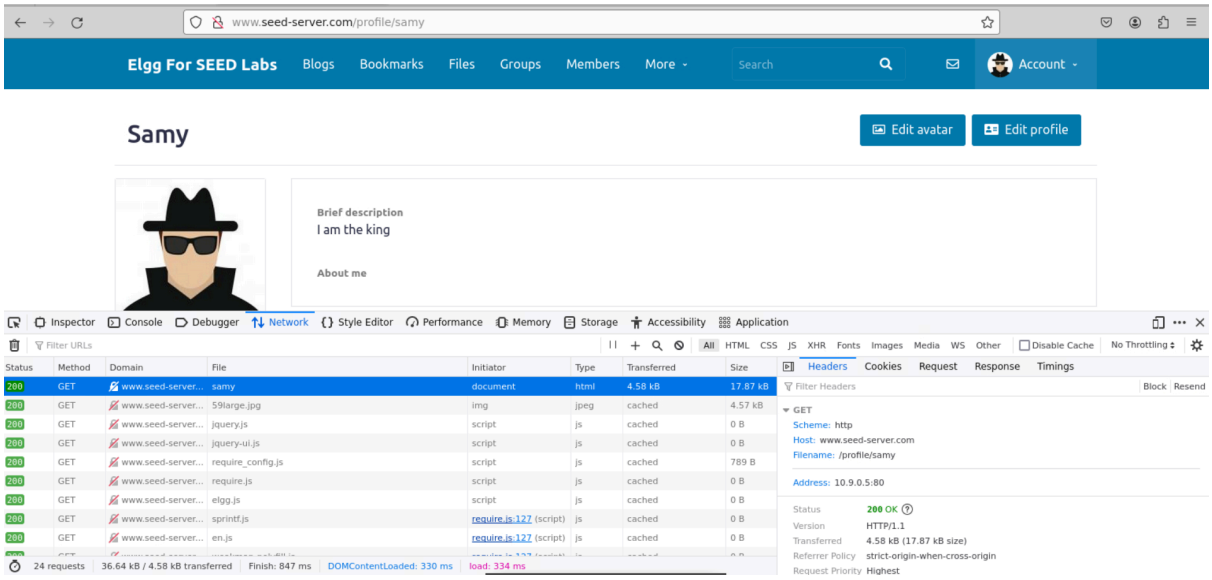


Task-3: Posting on the Wire on Behalf of the Victim

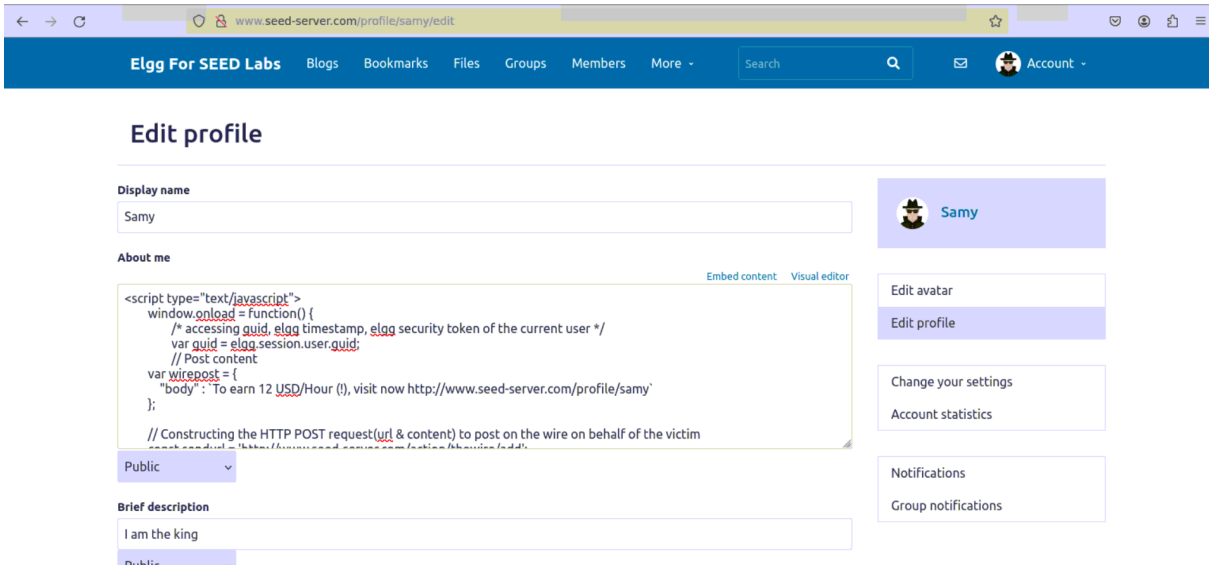
1| Figuring out post request construction for wire posting



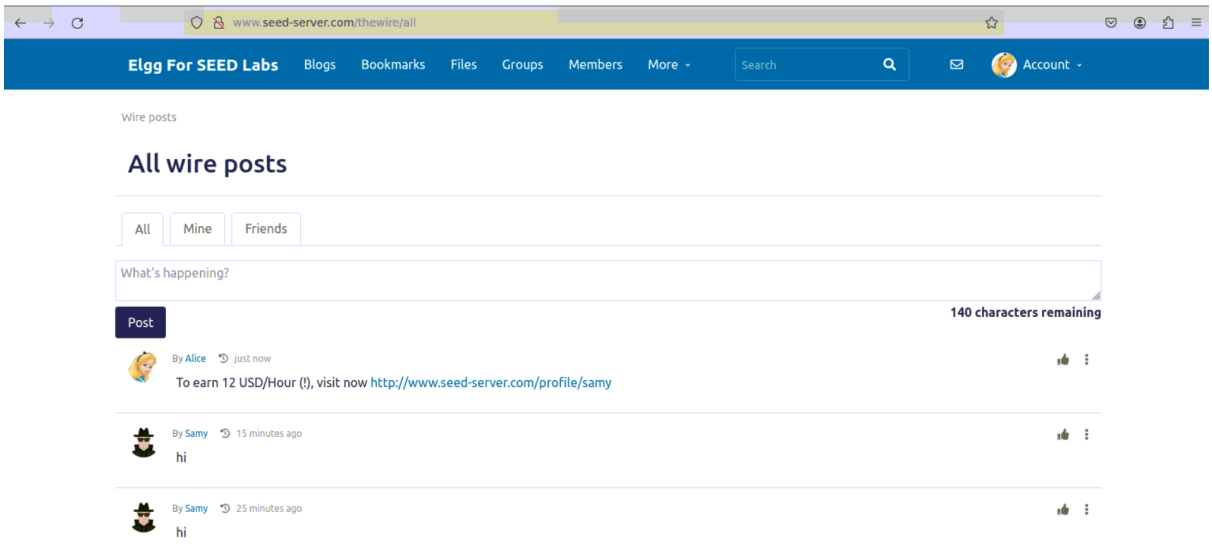
2| Checking out url of visiting user profile



3| Pasting malicious script code in samy's about me section and save it.

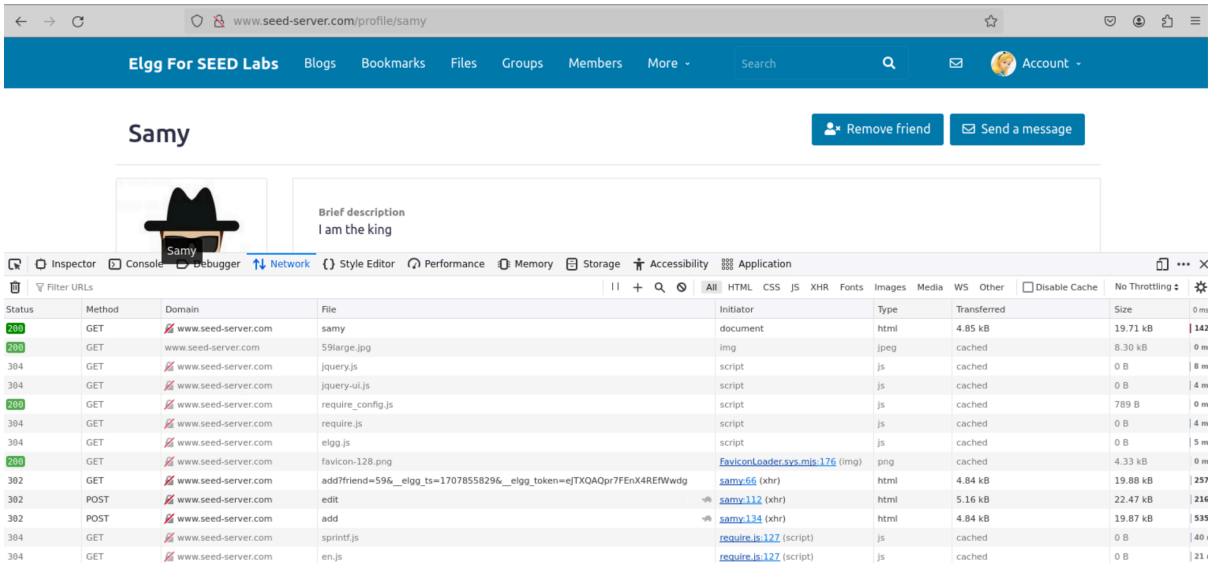


4| Now when Alice browses Samy's profile, Samy posted on the wire on behalf of Alice.

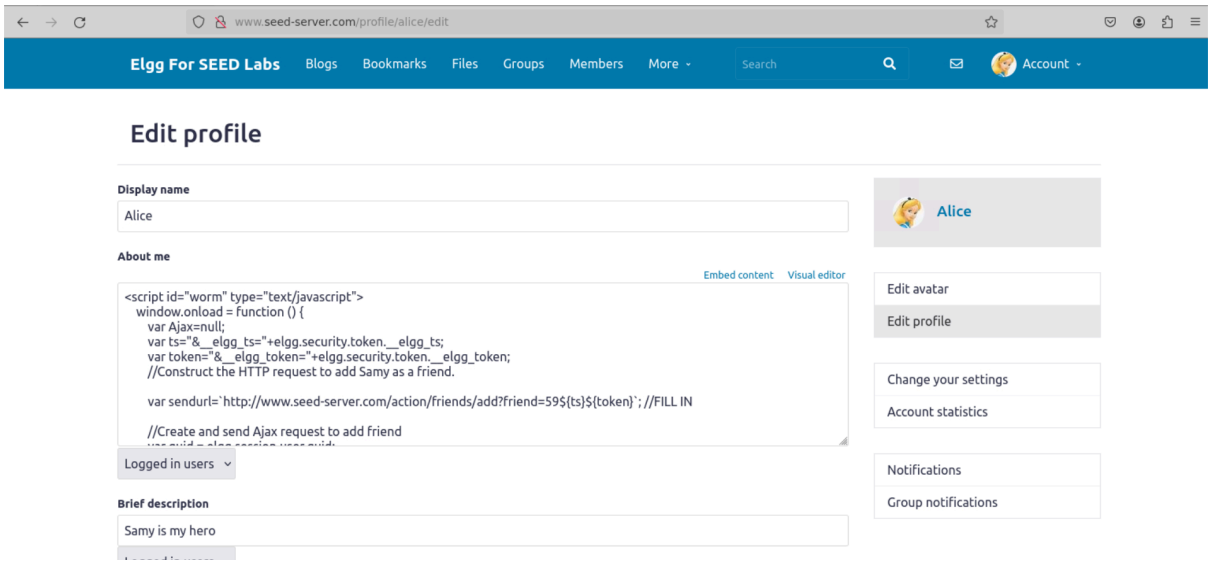


Task 4: Design a Self-Propagating Worm

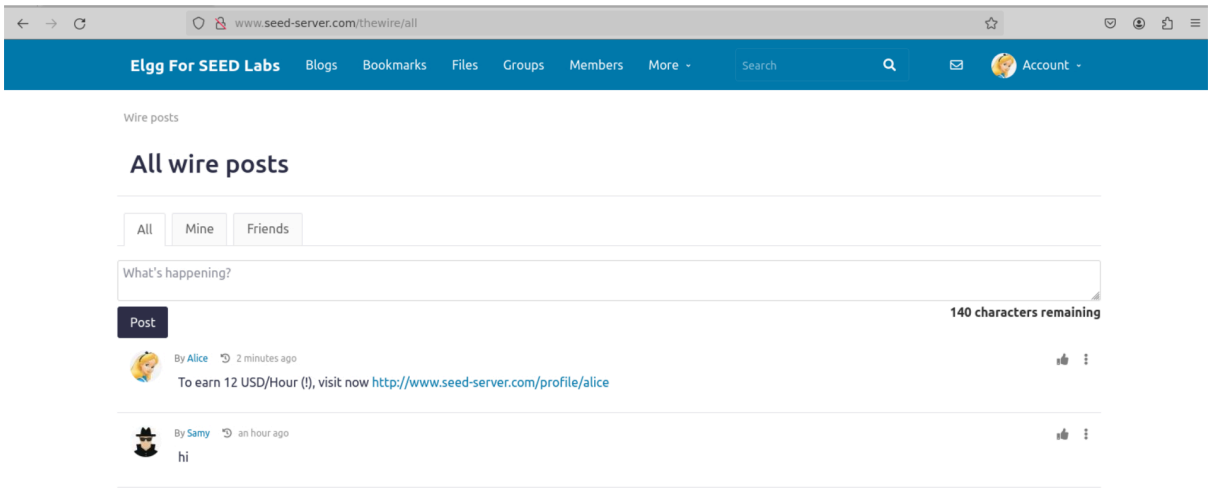
1| Samy put malicious script code in Samy's about me section as before. Now when Alice browses Samy's profile there will be additional 3 requests. These are for sending friend request, editing profile and posting on the wire



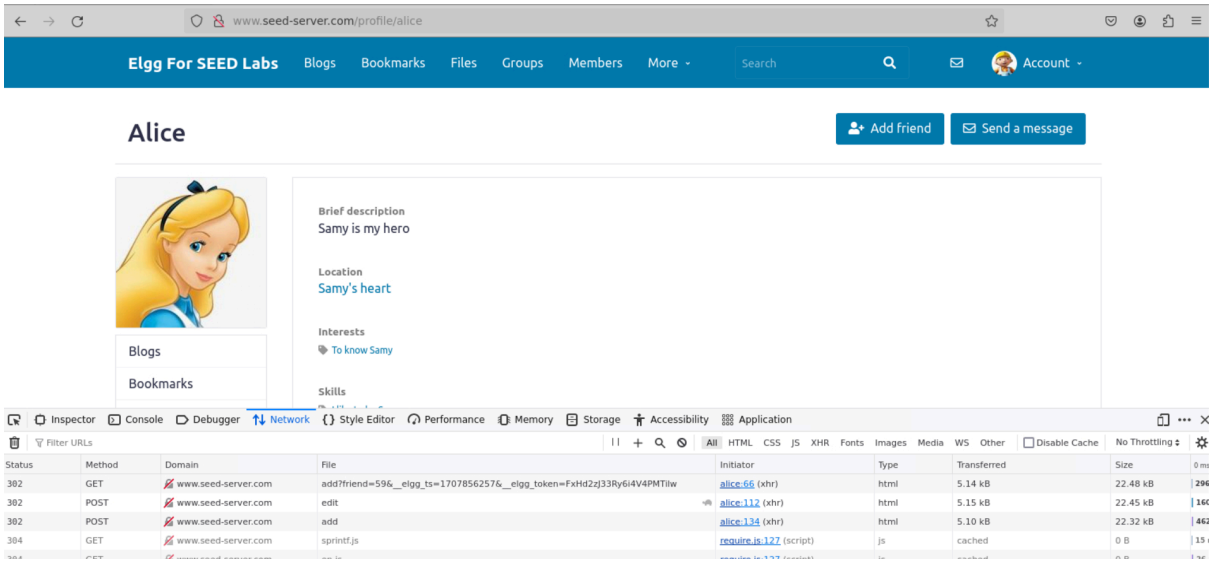
2| Now in Alice's profile malicious script code is placed after visiting Samy's profile automatically.



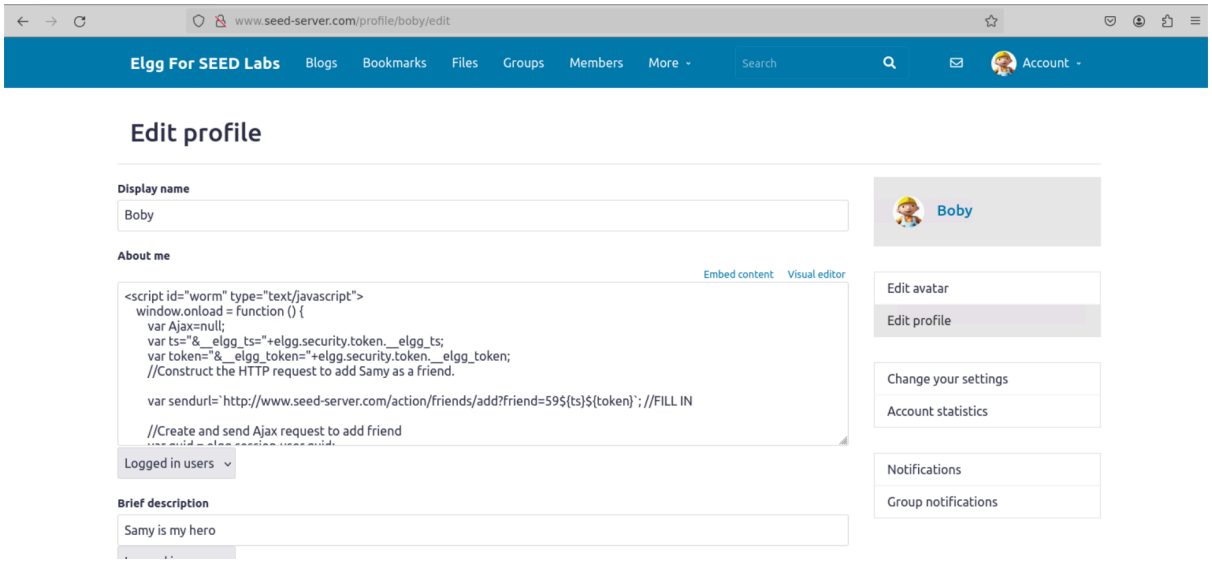
3| Also, the worm posted Alice's profile link on the wire.



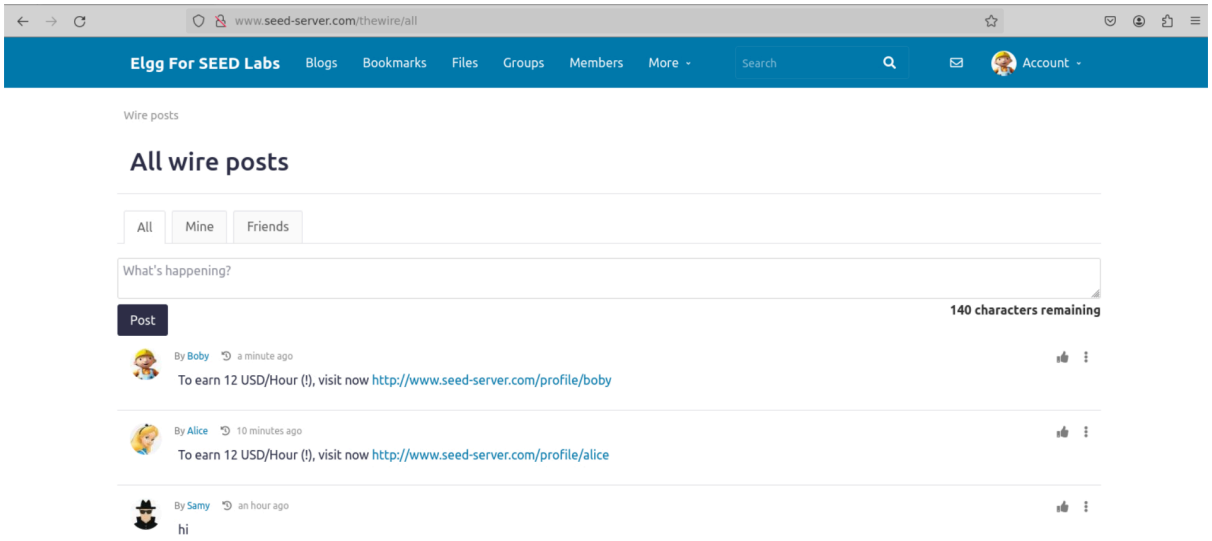
4| Now when Boby browses Alice's profile there will be additional 3 requests. These are for sending friend requests, editing profiles and posting on the wire.



5| As a result, in Boby's profile malicious script code is placed after visiting Alice's profile automatically.



6| Also, the worm posted Boby's profile link on the wire.



DONE!