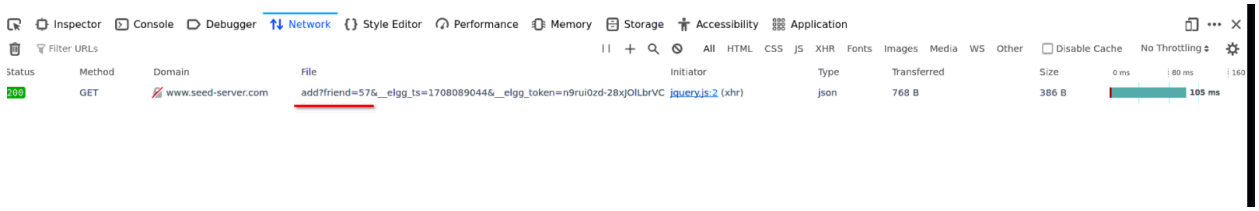
Task 1 :

In task 1 , we have to make sure a friend request is automatically , without clicking on sent to the attacker samy , whenever our victim Alice decides to visit samy's profile. Also , we had to make sure the friend request is not sent to samy whenever he visits his own profile.

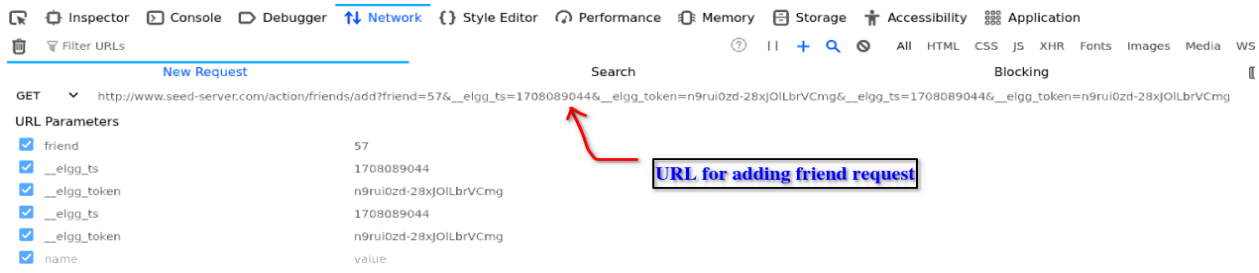
At first , we checked how a legitimate user is added in a friend request , for that we send a friend request and inspect the network section to find the corresponding header information.



From the header , we can see that it is sending a friend ID , along with the elgg_ts and elgg_token as part of URL parameters. So , for our desired URL , we will add :

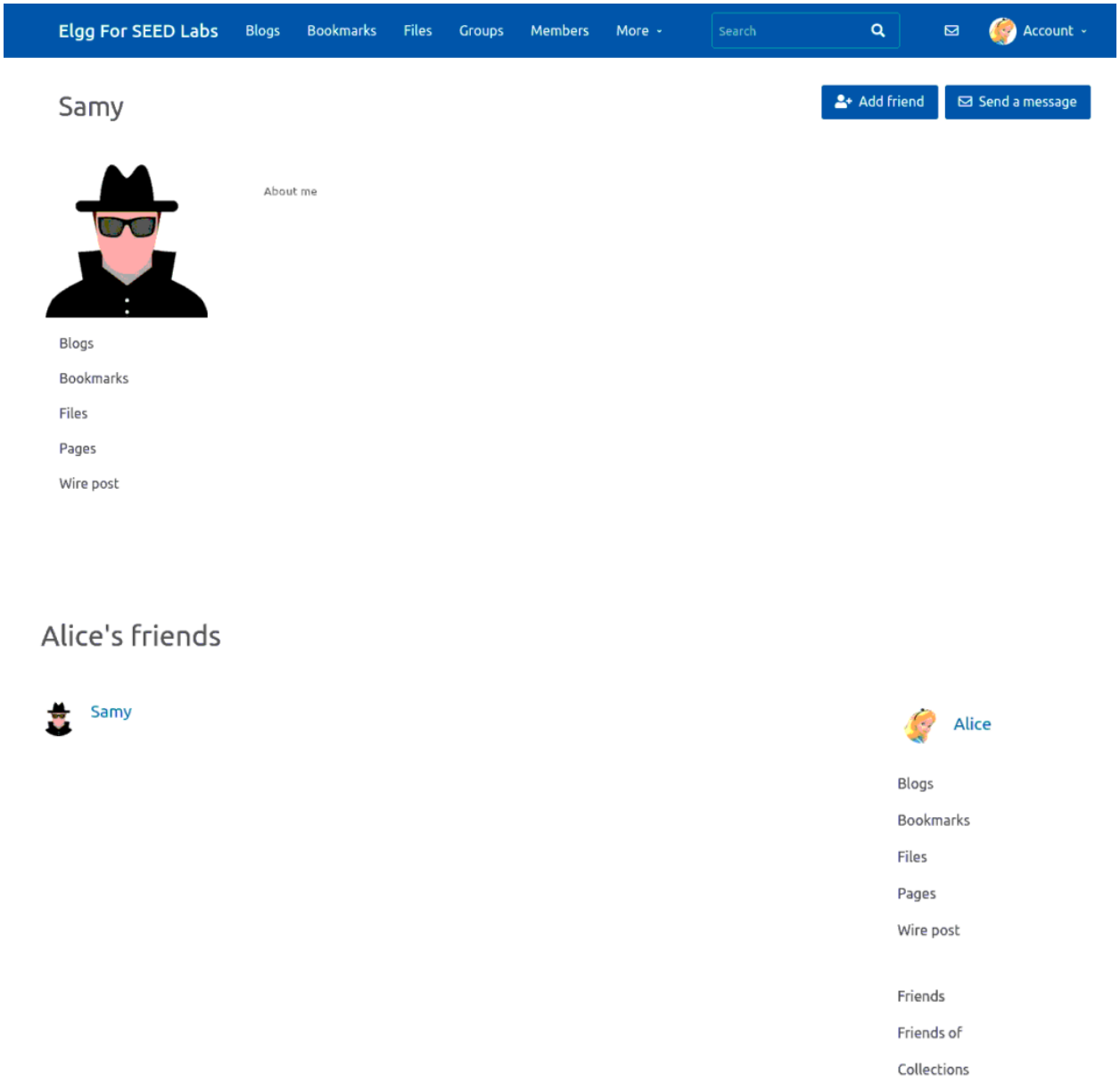
```
"http://www.seed-server.com/action/friends/add?friend=" + samyguid + ts + token;
```

Here, ts and token represents the corresponding elgg token and ts.

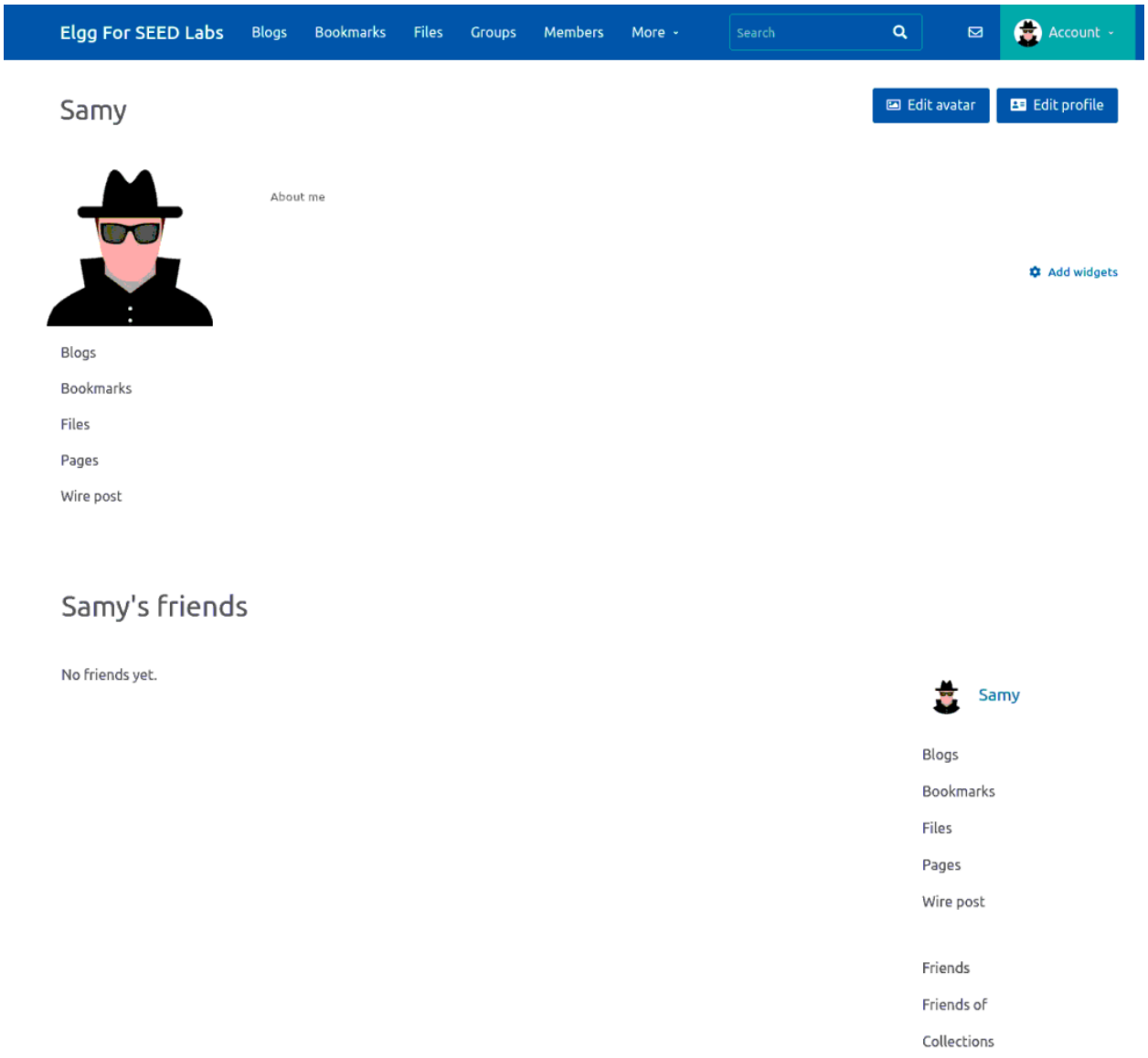


So, to ensure this, we added a script in the "About Me" section of samy. The scripts adds an URL which sends a friend request to the guid of samy along with the timestamp elgg_ts and token elgg_token. The guid of samy was obtained by inspecting the profile of samy

So by modifying the sendurl , we can send a friend request to samy. Now to ensure that samy doesn't receive a friend request when he visits his own page , I added a constraint so that the current session user guid is not the same as samy , `elgg.session.user.guid!=SamyGUID.` . Finally the output will be :



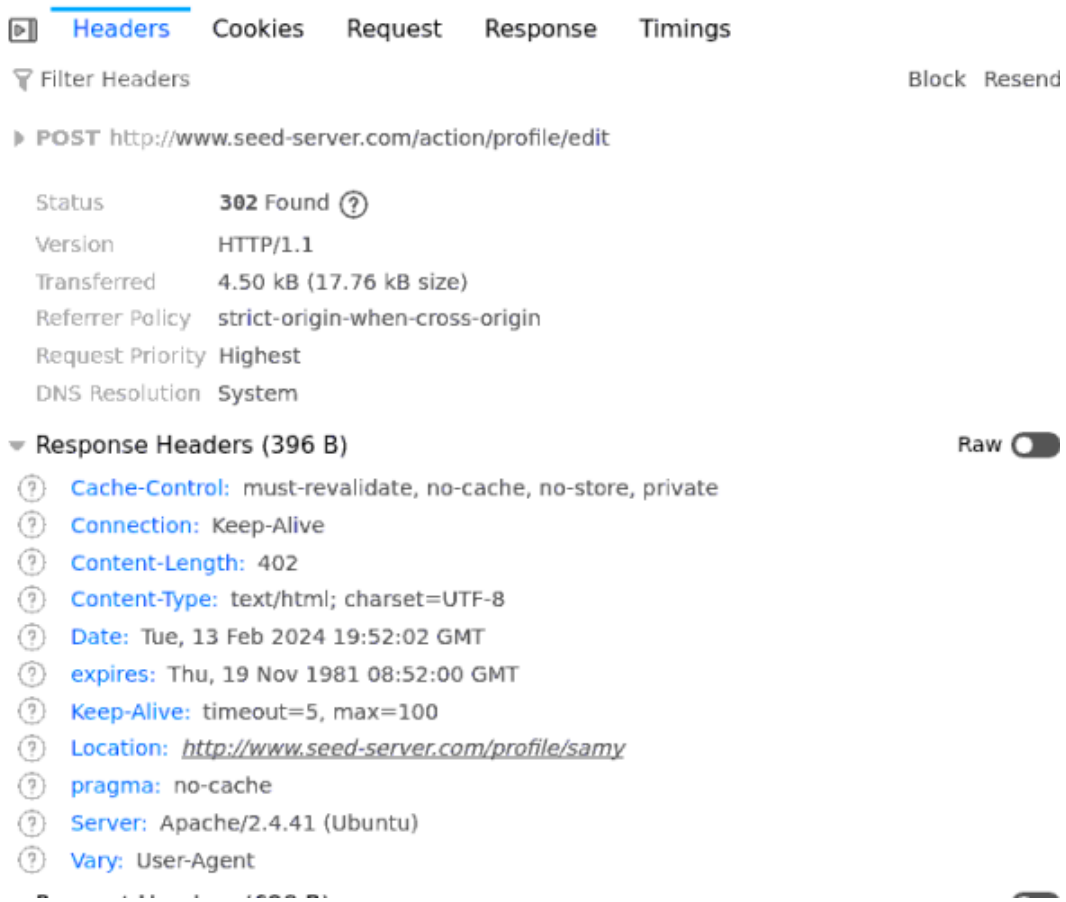
Also made sure that samy doesn't become friend with his own account even if he visits his own account.



Task 2 :

Whenever a victim account , for example , Alice visits the profile of attacker samy , it will modify Alice's own profile. The required modifications are that all the fields' privacy access level will be "Logged In Users" , the description will show my own roll number and all the other fields will show a random string.

At first, I determined the URL associated with the "edit profile" and Ajax sends XMLHttpRequest to that URL. The URL found in edit profile is :



So, from the legitimate request , we can denote that, the URL , where Ajax needs to send a POST request will be :

```
var sendurl = "http://www.seed-server.com/action/profile/edit";
```

In our body of the request , it sends the updated information along with the access level. For a legitimate use of edit profile , the content looks like :

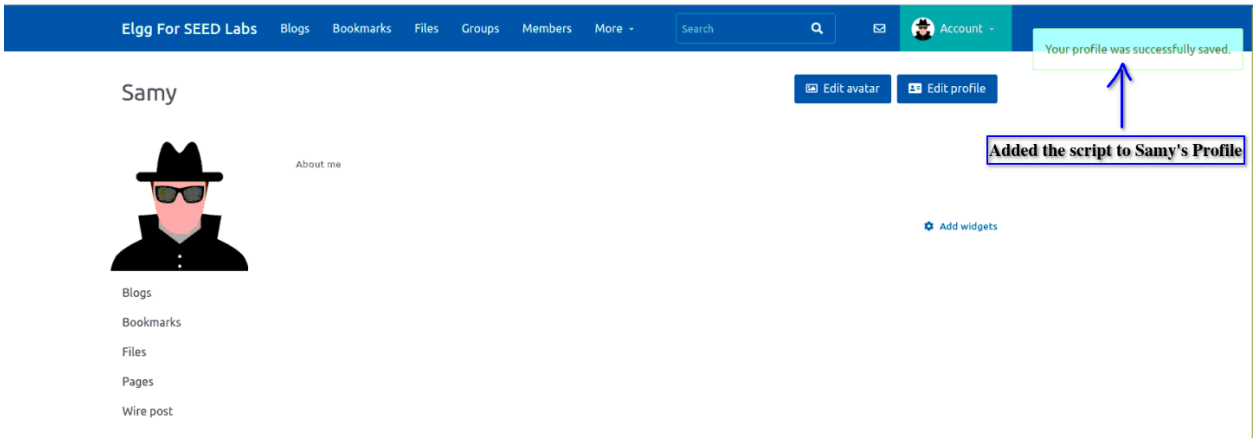
```
Content-Disposition: form-data; name="location"

0n16hb
-----------------------------313949188223129143493944273 86
Content-Disposition: form-data; name="accesslevel[location]"

1
```

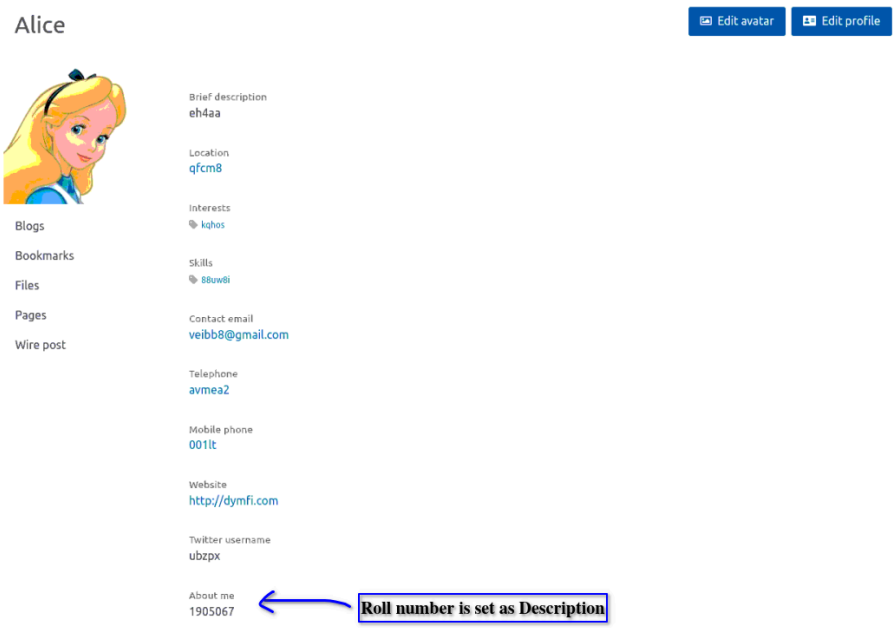
As for content , the modified values are set with respect to the corresponding field. Since , each field access must be set only for the logged in users , the access level is set to 1 for each field . Here we can see that each of the fields have some random string (maintaining the constraint of

proper format for webpage and gmail) . And in our About section , it shows my roll number. So , I set the access level for each field to 1 and created a random string function for the parameters. Following the type of content in the body , the solution can also be achieved by using formdata. In that solution , we have to append for each information type along with their access level.



Samy's profile won't be affected if he visits himself, which is maintained by the condition check that `elgg.session.user.guid!=SamyGUID.`

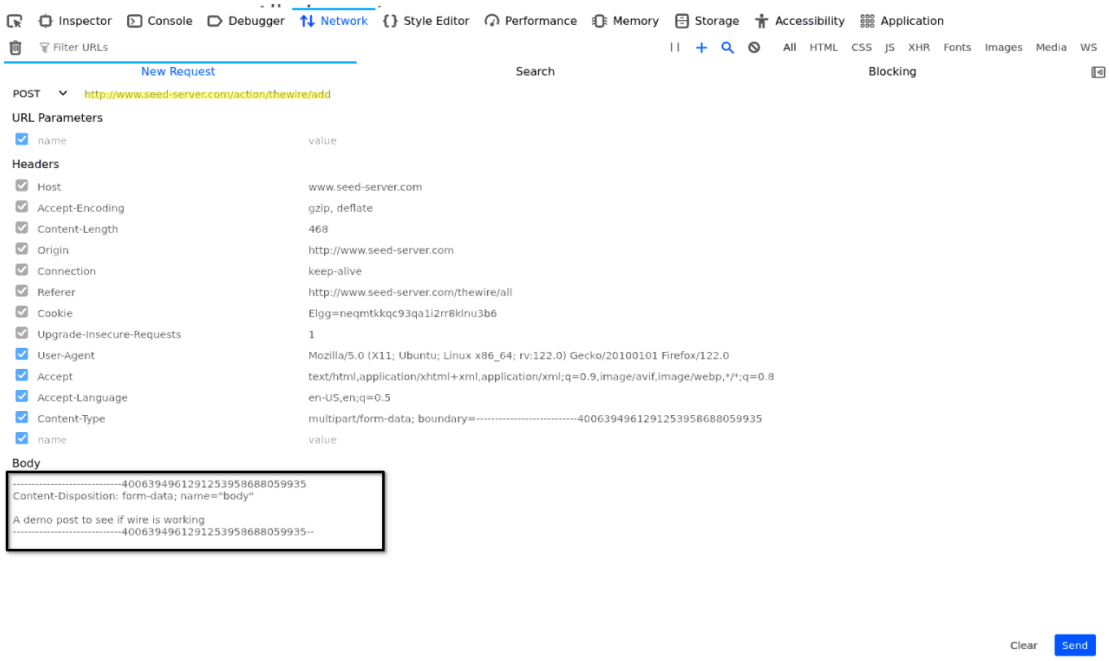
If we revisit Samy's profile now , we will not see any change here. But if we try the same from Alice's profile , we will see the changes below:



Task 3:

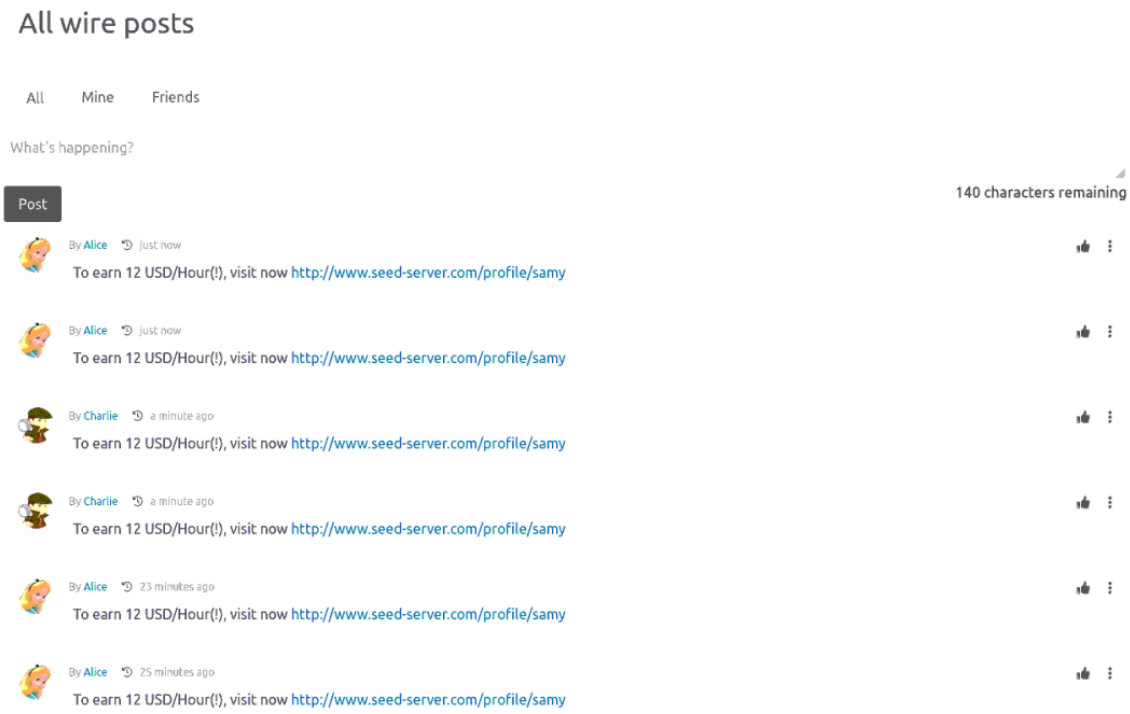
Following the process of task 2, visiting the attackers profile, there will be a post made from the account of the victim. On the wire , the text will have the link of the attacker (in our case , samy).

For a legitimate Wire post , we will find the URL sent , which looks like :



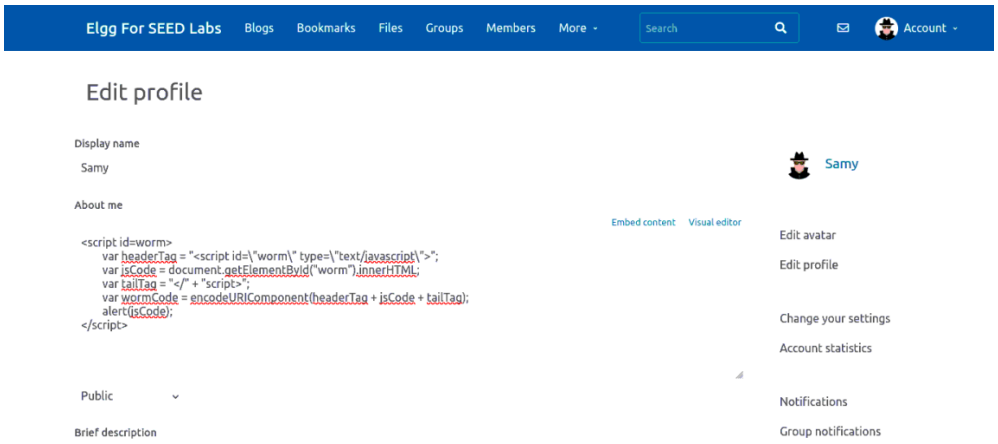
So, this will create a wire post that looks like :

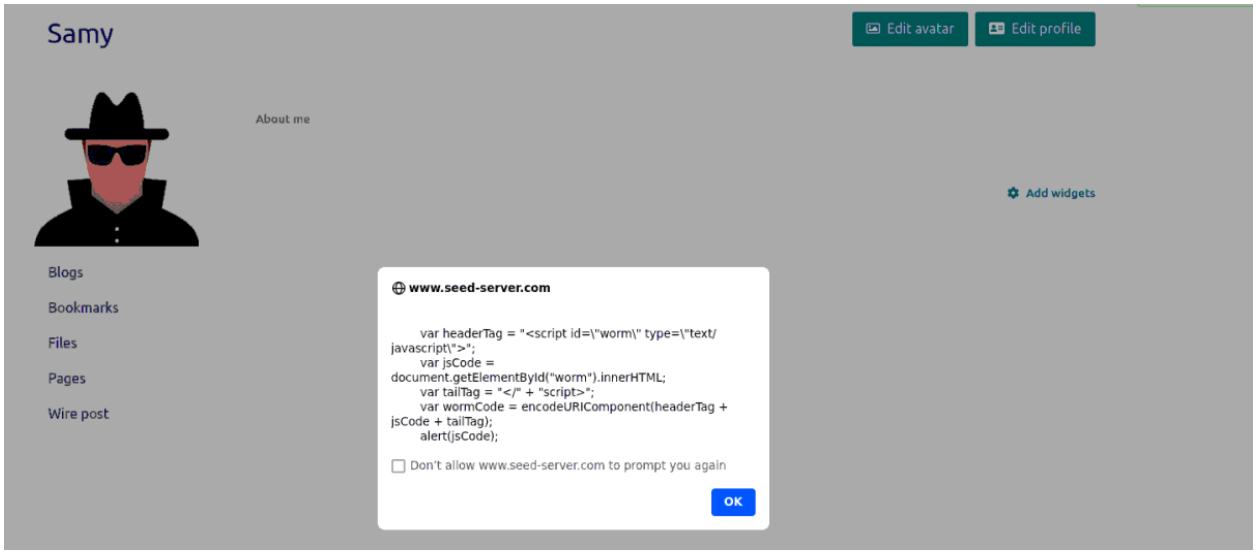
To implement our required task3 , I modified the send url to the post method adding posts to the wire. The Ajax will send the necessary contents which are our desired texts , with the urlencoded link to samy's profile. This problem , same as problem 2 , can also be solved by appending information to the formdata or modifying it as content. In our solution, we showed both approaches.



Task 4:

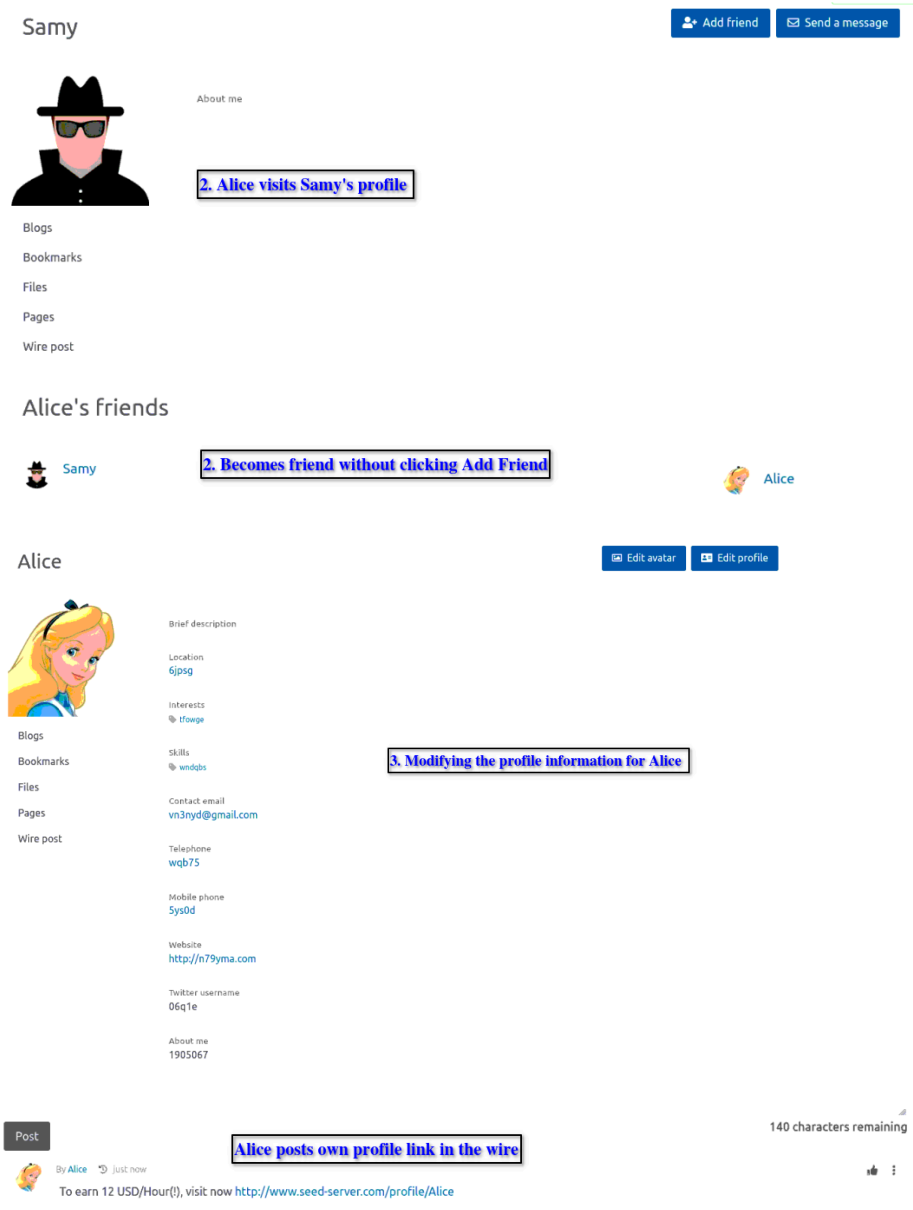
In task 4 , the ideas from previous tasks are assembled. Here, we are given a script with the id “worm”. By the usage of innerHTML, alert (wormcode) shows the complete script written already. For example, if we add the given script in anyone's description, the output would look like this :

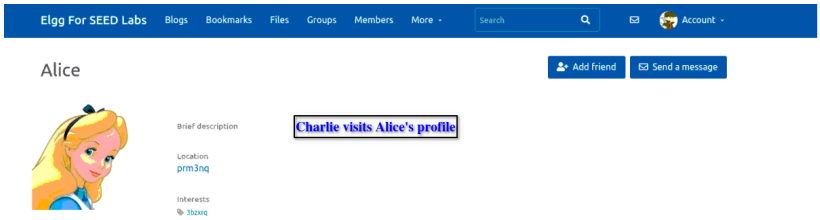




I used this idea to propagate the script to anyone's profile starting from the initial visit to samy's profile. Within the js code, I assembled the previous three tasks. Here I needed three URLs, and two content bodies for posting in the wire and changing profile information . And finally added this to samy's description.

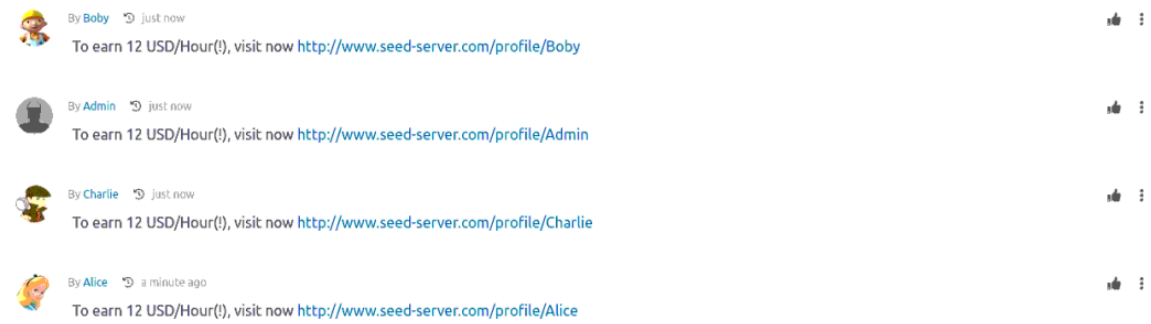
The difference from previous tasks is that now instead of sending to Samy's profile in the wire , I will use `elgg.session.user.name`. Also to make sure , the worm is propagated, the worm code is added to the description of the victim, so that if someone else visits the victim's profile, he/she becomes the victim too. `var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);` , is added to the description field , in this way , if anyone visits the victim's profile, the wormcode will be added to their own profile and hence propagate. Finally if the current user is not Samy , I send three Ajax requests. The output is shown following the steps in spec:


Samy
Add friend
Send a message
About me
2. Alice visits Samy's profile
Blogs
Bookmarks
Files
Pages
Wire post
Alice's friends
Samy
2. Becomes friend without clicking Add Friend
Alice
Alice
Edit avatar
Edit profile
Brief description
Location
6jpsg
Interests
tfowge
Skills
wndqbs
Contact email
vn3nyd@gmail.com
Telephone
wqb75
Mobile phone
5ys0d
Website
http://n79yma.com
Twitter username
06q1e
About me
1905067
Blogs
Bookmarks
Files
Pages
Wire post
3. Modifying the profile information for Alice
Post
140 characters remaining
Alice posts own profile link in the wire
By Alice
just now
To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/Alice


Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Alice
Add friend
Send a message
Brief description
Location
prm3nq
Interests
3tzxrq
Charlie visits Alice's profile


Charlie's friends
Samy
Adds Samy as friend
Charlie
Blogs
Bookmarks
Files
Pages


By Boby just now
To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/Boby
By Alice a minute ago
To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/Alice
Boby posts his own profile link by visiting Alice


By Boby just now
To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/Boby
By Admin just now
To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/Admin
By Charlie just now
To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/Charlie
By Alice a minute ago
To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/Alice