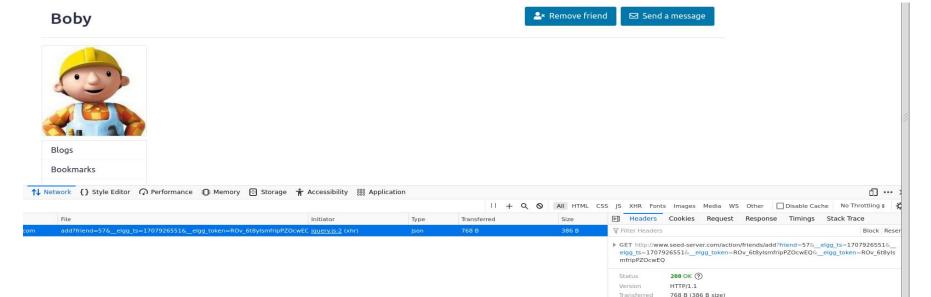
CSE 406 Assignment 2 Cross-Site Scripting (XSS) Attack

ID:1905040

TASK 1 Becoming the Victim's Friend

At first, I logged into Samy's account and sent a friend request to Boby. We have already opened inspect tab to check the status and link of our GET request.



TASK 1 Becoming the Victim's Friend

Then we checked the page source to find the guid of samy, which is 59. This is to prevent his friend request to himself.

These information are stored in elgg variable. We can also find the information needed for token and ts from here.

```
var elgg = {"config":{"lastcache":1587931381,"viewtype":"default","simplecache_enabled":1,"current_language":"en"},"security":{"token":{"_elgg_ts":1707927544,"__elgg_token":"W03Ng6SosJmyNglfZxUVwA"}},"session":{"user":{"guid":59,"type":"user","ow </script><script src="http://www.seed-server.com/cache/1587931381/default/jguery_ui_js"></script><script src="http://www.s
```

TASK 2 Modifying the Victim's Profile

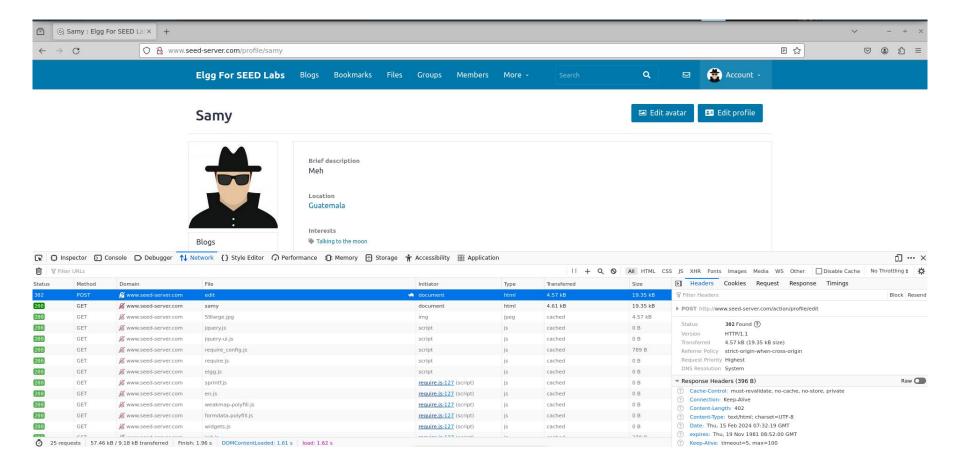
Again we will check how to edit profile using Samy's ID.

In inspect, we see 302 status in our POST request, in which if we check the header, we will find the link, which is www.seed-server.com/action/profile/edit

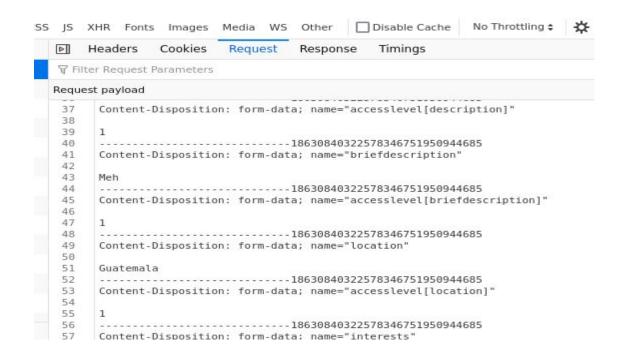
In Request tab, we can see the fields for which we have to change the values(e.g Logged in Users have a value 1)

The following images depict the above mentioned scenarios:

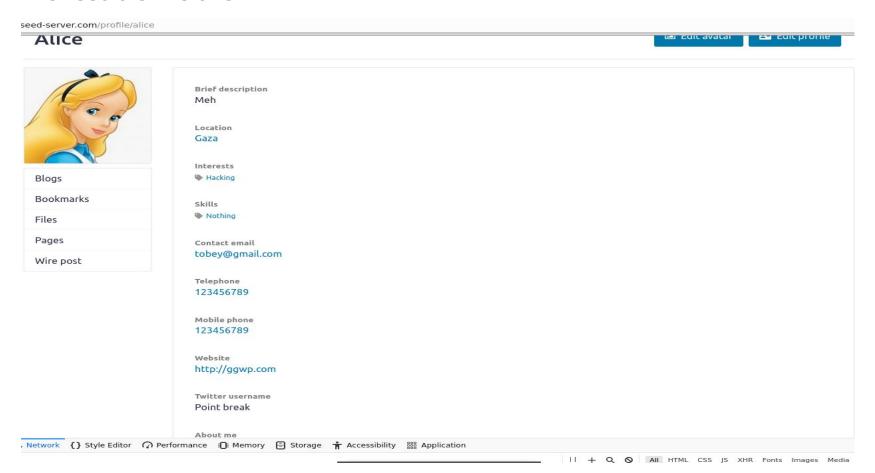
Changing Samy's ID values and checking the Headers' content for sending_url.



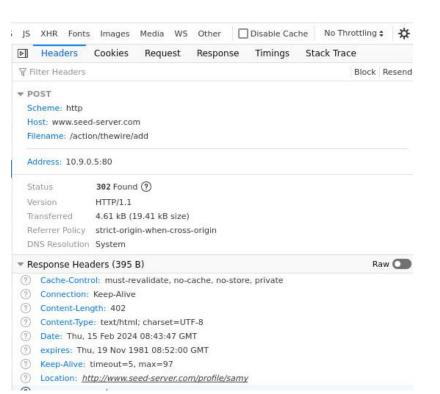
Field name, like "location", "accesslevel [location]" and their values found in Request Tab when we modified Samy's ID:

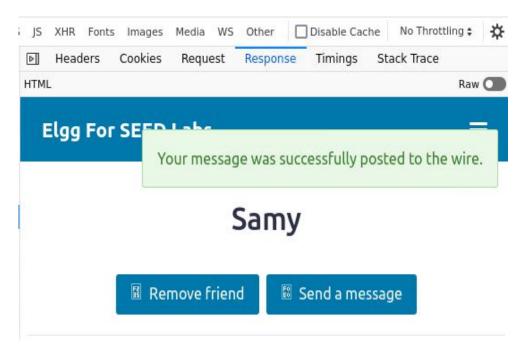


The result is like this:



TASK 3 Posting on the Wire on Behalf of the Victim





Explanation of last slides' photos

As this is a POST request ,just like task 2, our procedure is completely same. We find the field name and set its value accordingly.

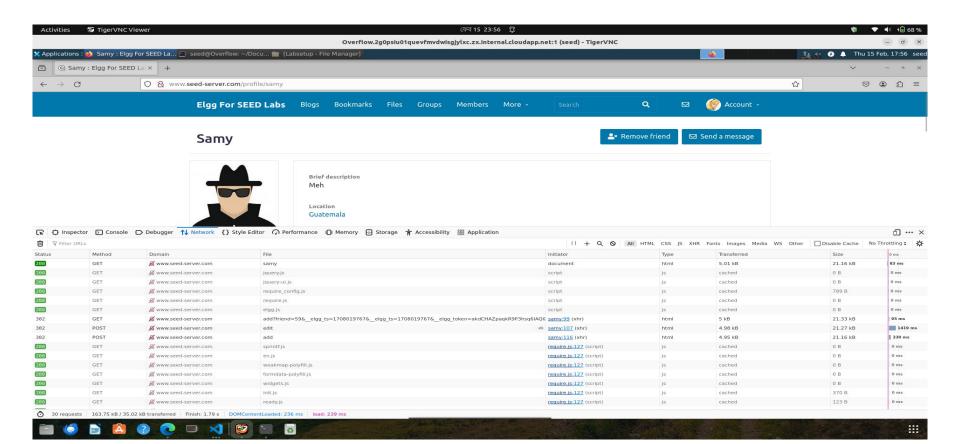
At first we will get the link from the Header as usual, and then modify the body field.

TASK 4 Design a Self-Propagating Worm

The work in this task comprises the tasks of other three files. So we are not adding the similar photos again.

The worm propagation code was provided in assignment resources, so we used that code snippet.

GET and POST requests being executed for the script.



Samy has been added to the friend List after visiting Alice's ID who has been formerly attacked visiting Samy's ID. We can see his posts in friends tab here.

Friends' wire posts



Wire-post addition after visiting Alice's account

