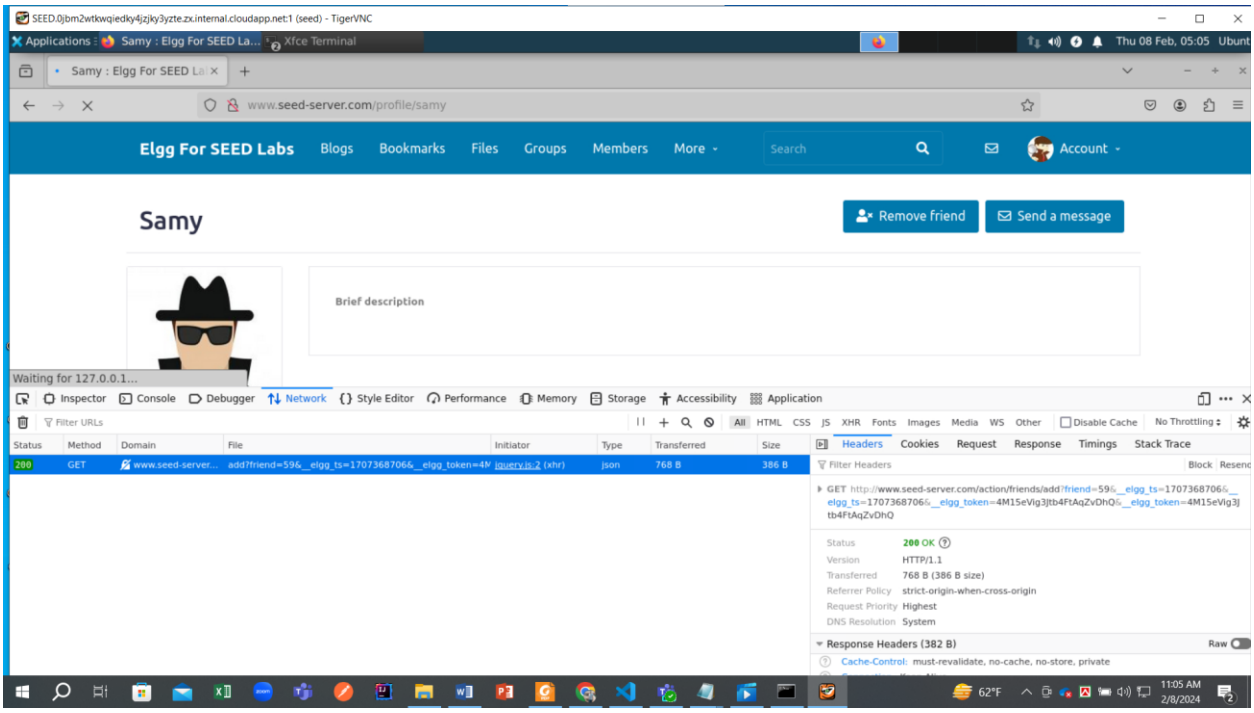
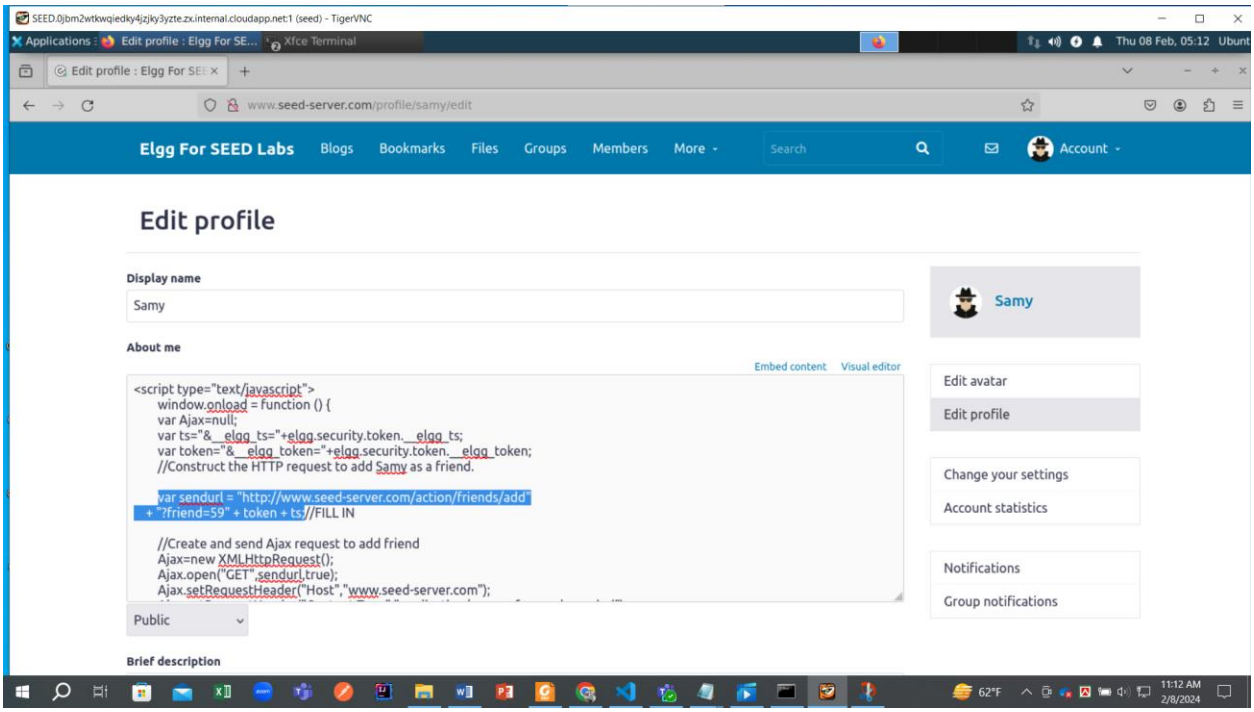
Task 1 :

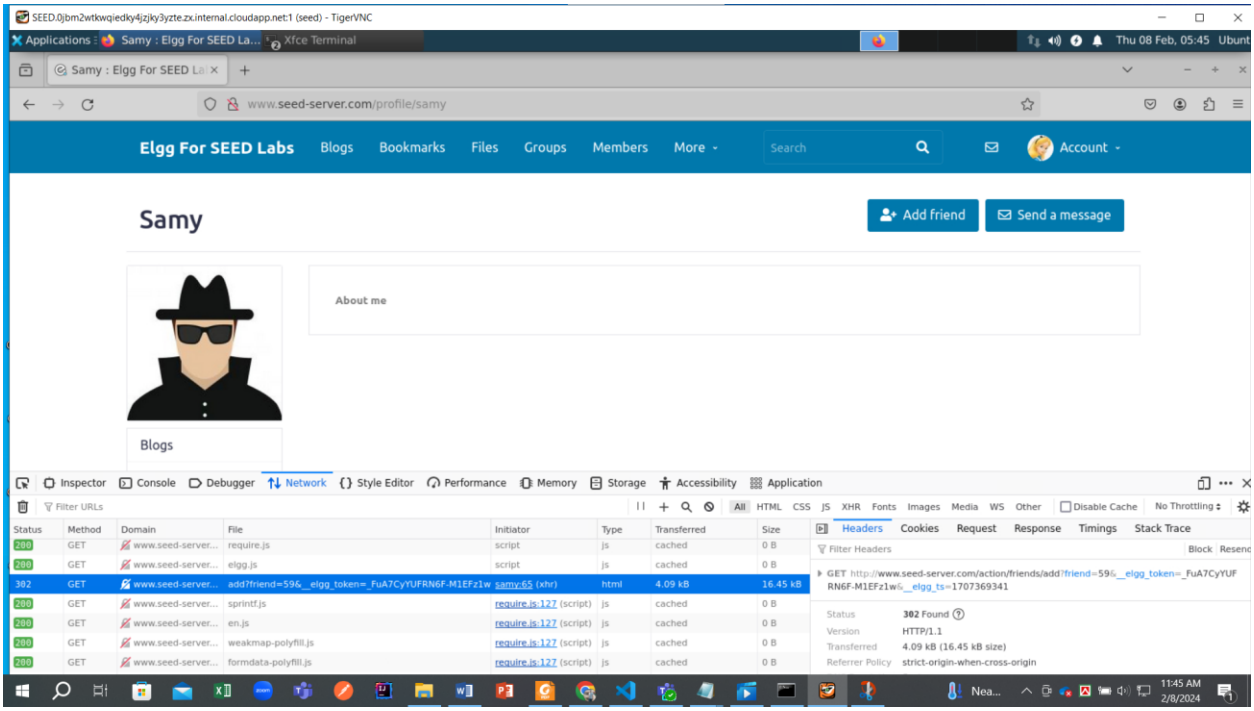
When add friend button is click by charlie , a html get ‘add friend’ request is send with samy’s id , time stamp and token parameter of charlie .



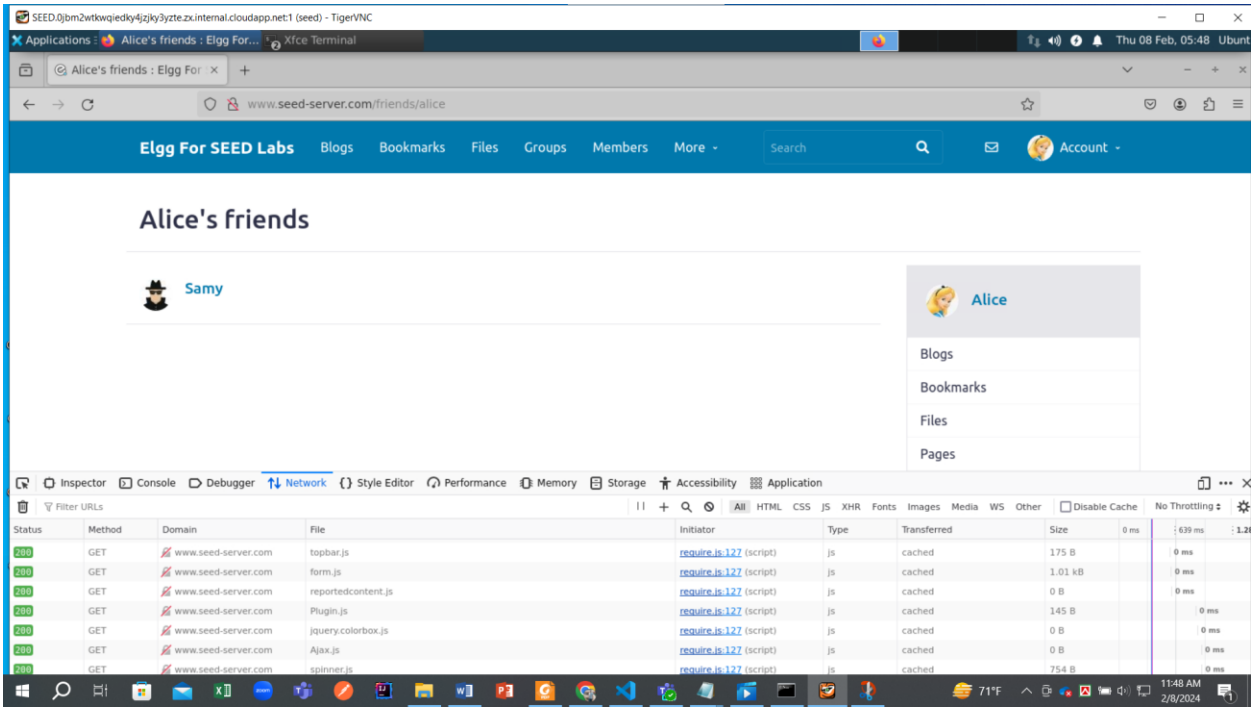
To do XSS attack , Samy put a java script in his ‘about me’ text field .



When Alice view samy's profile , the script is executed , a http get 'add friend' request with samy's id , time stamp and token of "Alice" is sent .

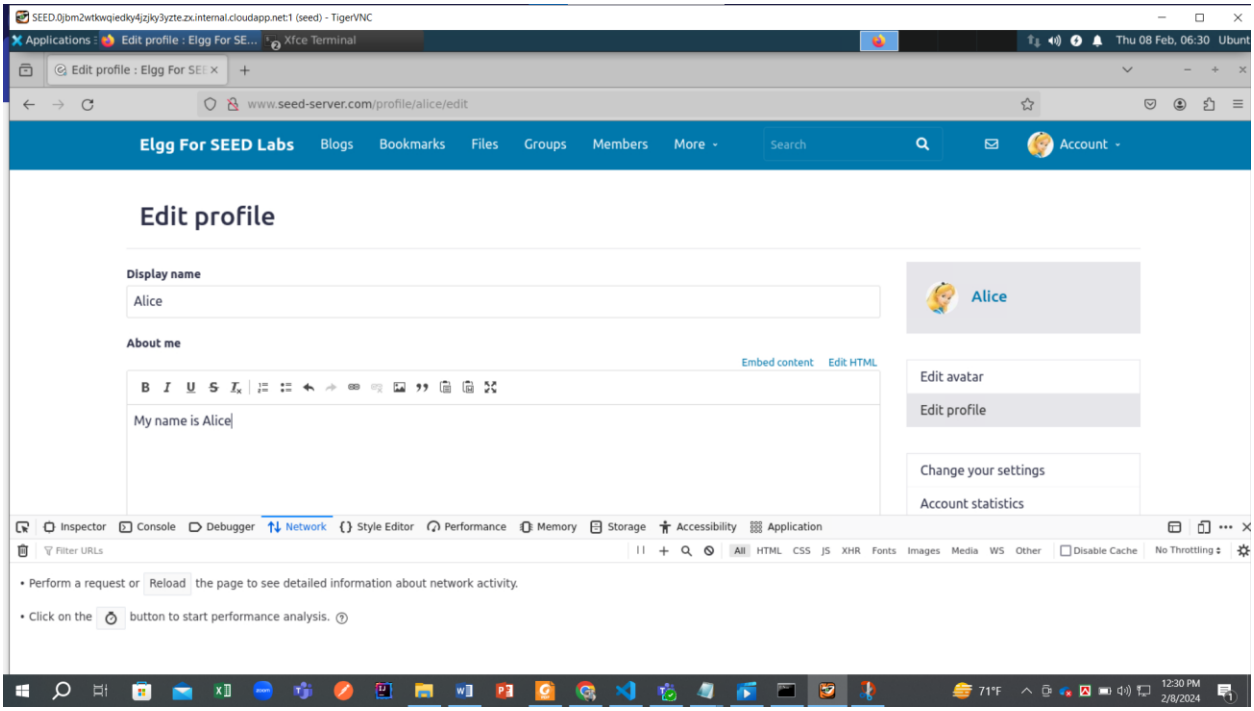


After that , samy becomes the user's friend , though the user doesn't click the add friend button .

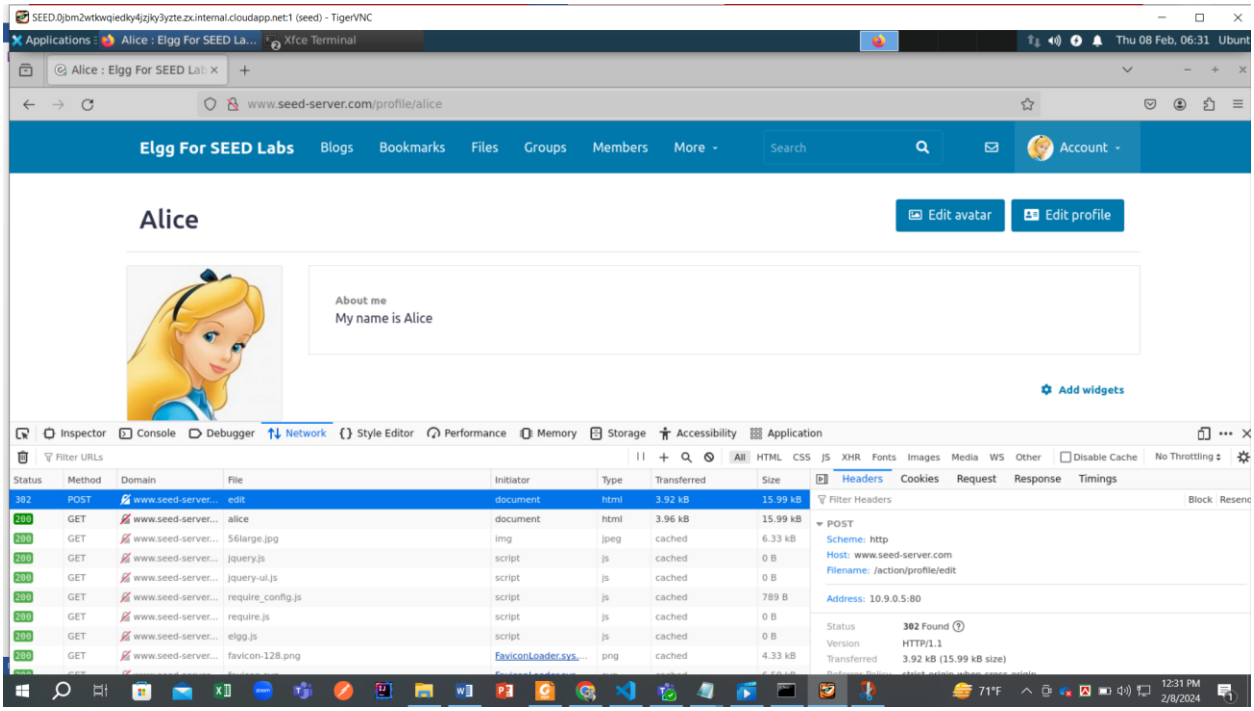


Task 2 :

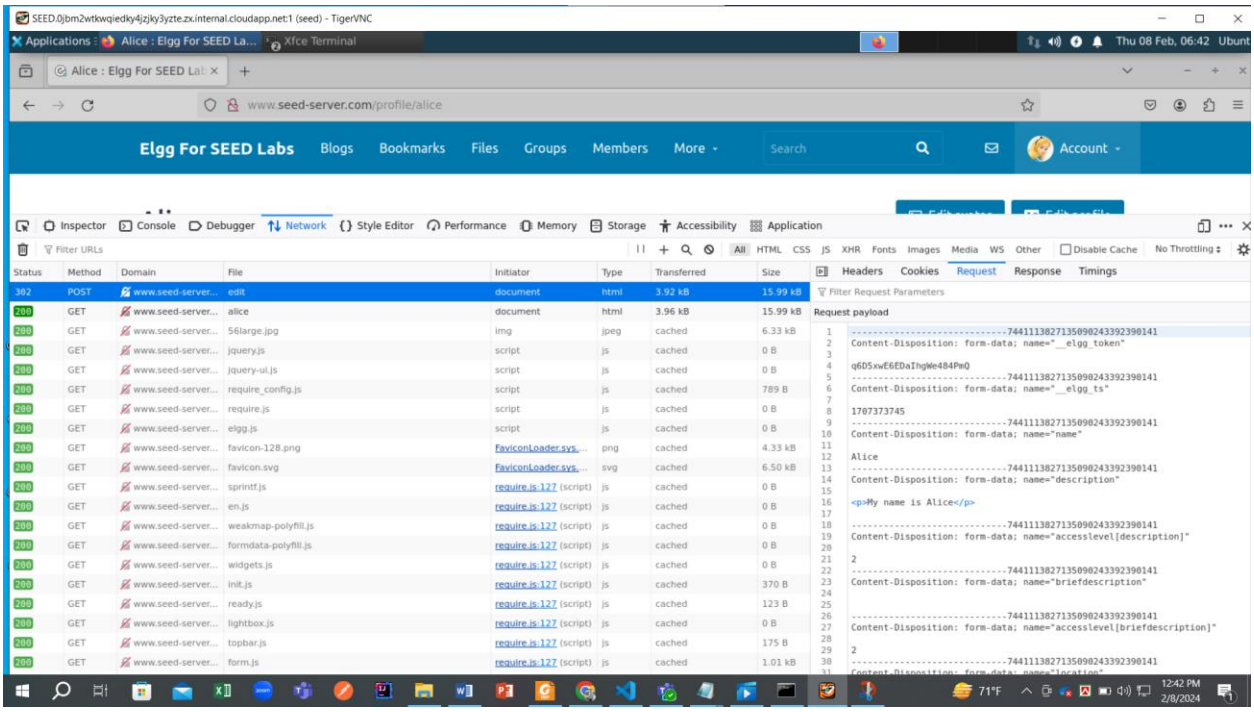
In Edit profile , Alice write something .



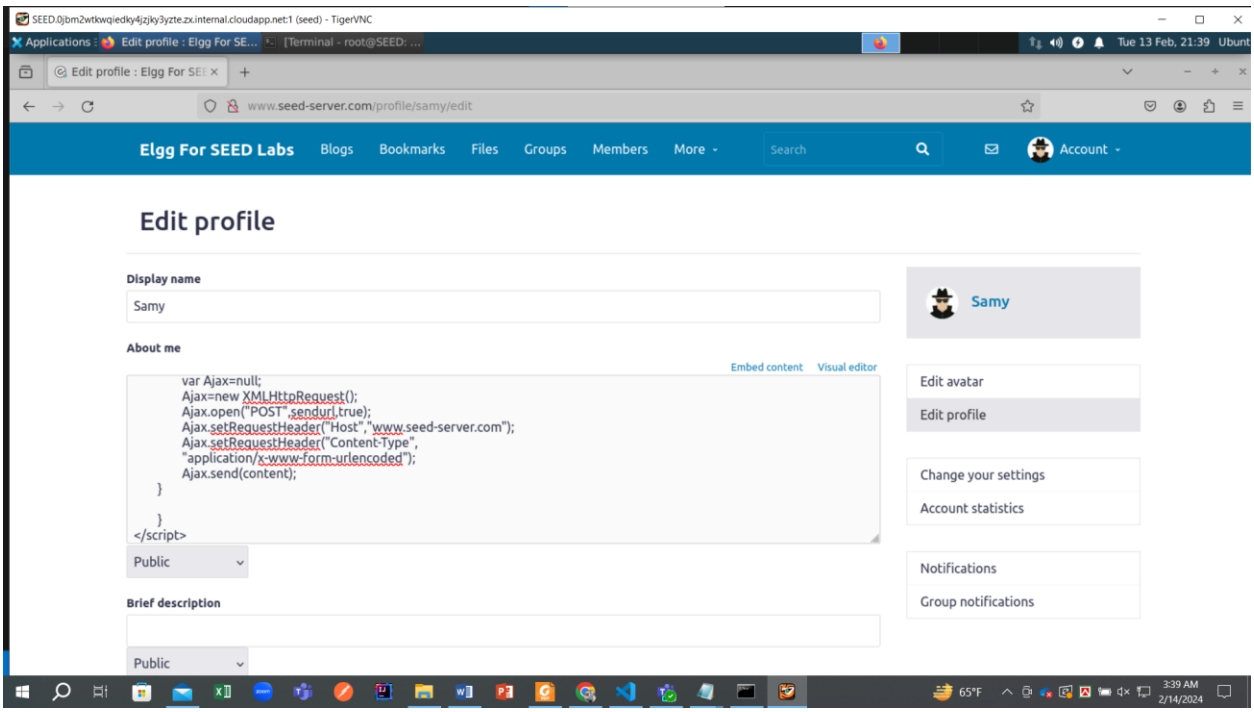
when Alice click save button , a post request is send.



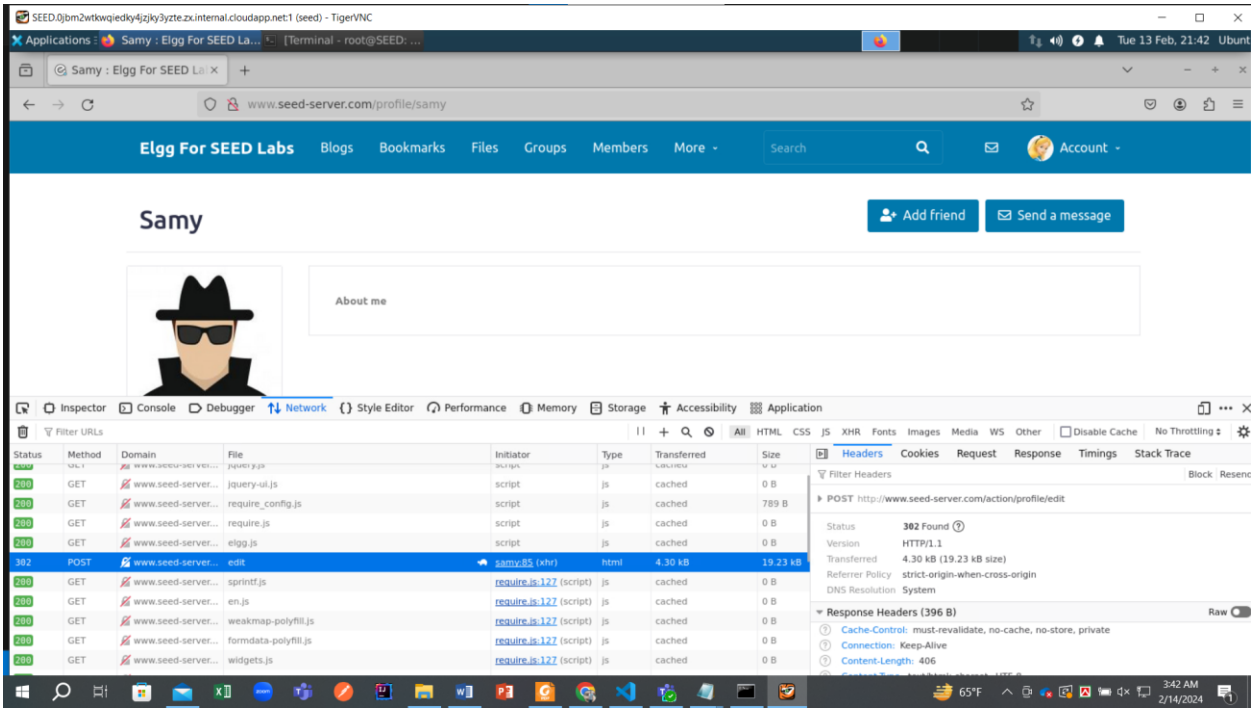
Here is request payload of “Post” request. All the field’s access levels are 2 for **public**



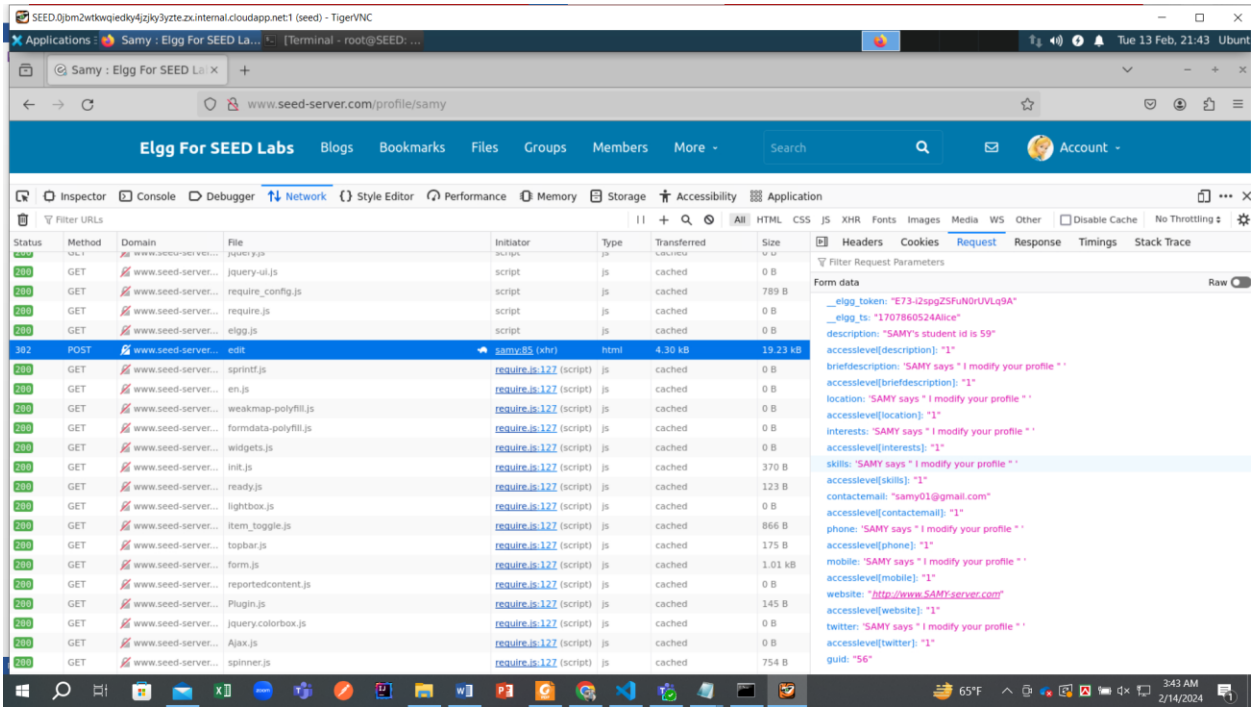
To do XSS attack , Samy put a java script in his ‘about me’ text field .



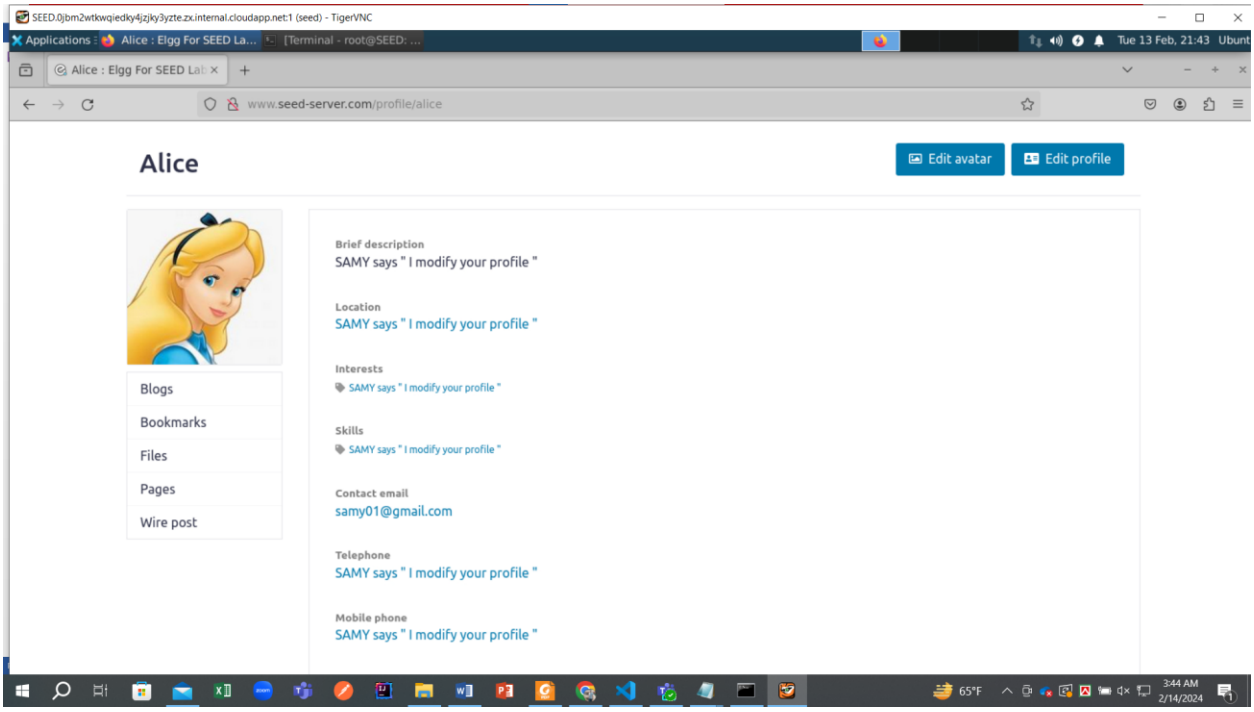
When Alice view samy’s profile , the script is executed , a http post request is sent to edit Alice profile , though Alice doesn’t visit her edit profile page and click the ‘save’ button.



In request body of 'post' request , all the field's access levels are set to "Logged in Users" , Samy set his ID in description and all other fields are set to "Samy says "i modify you" ".

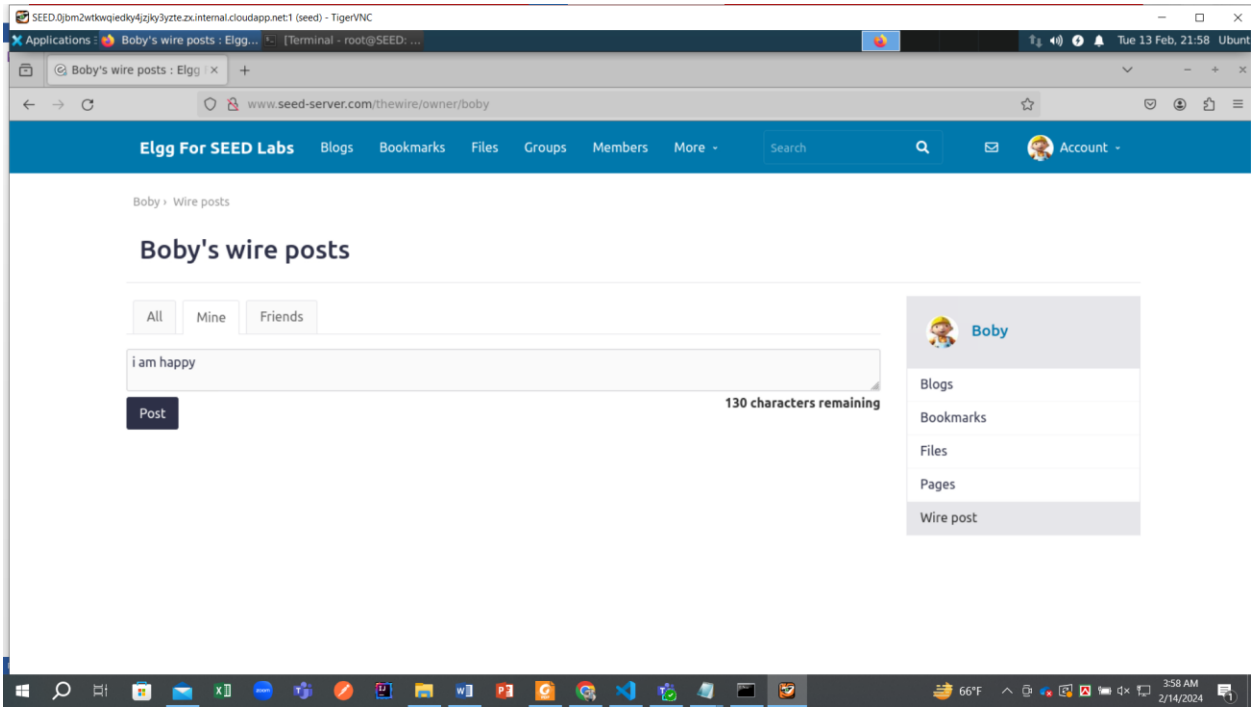


When Alice visit her profile, she see the modification though she doesn't edit her profile.

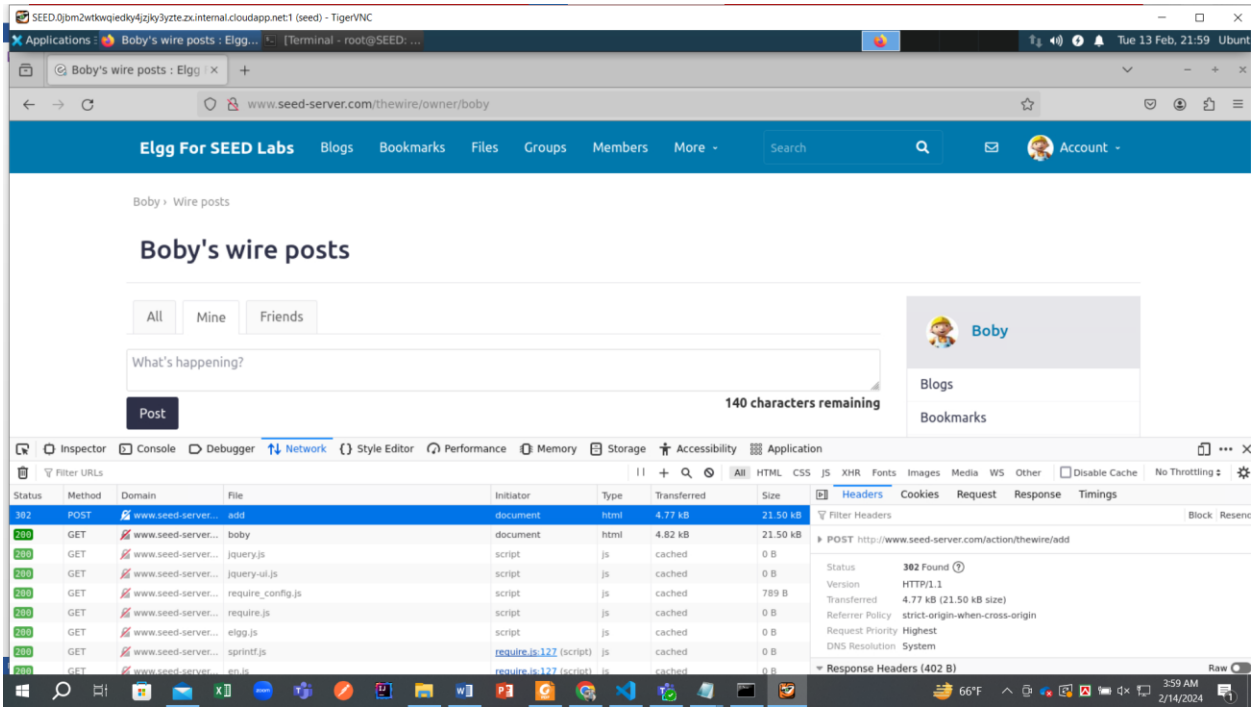


Task 3:

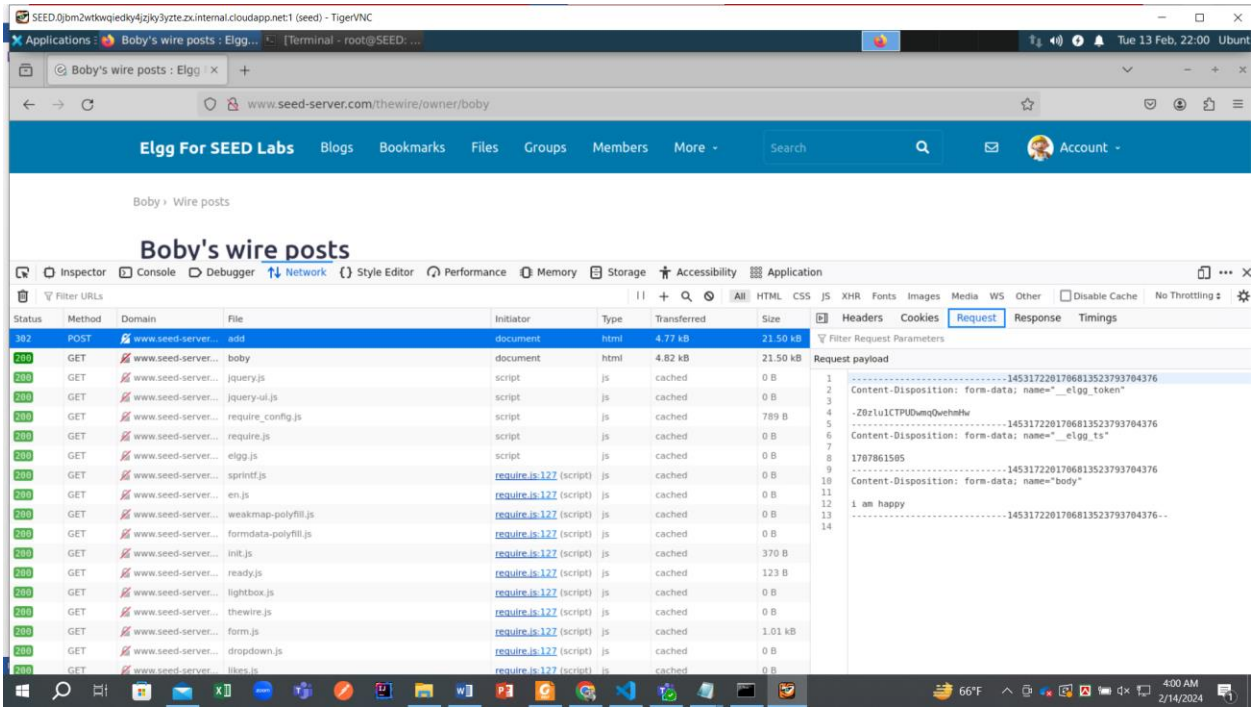
In Boby's wire posts , Boby writes something.



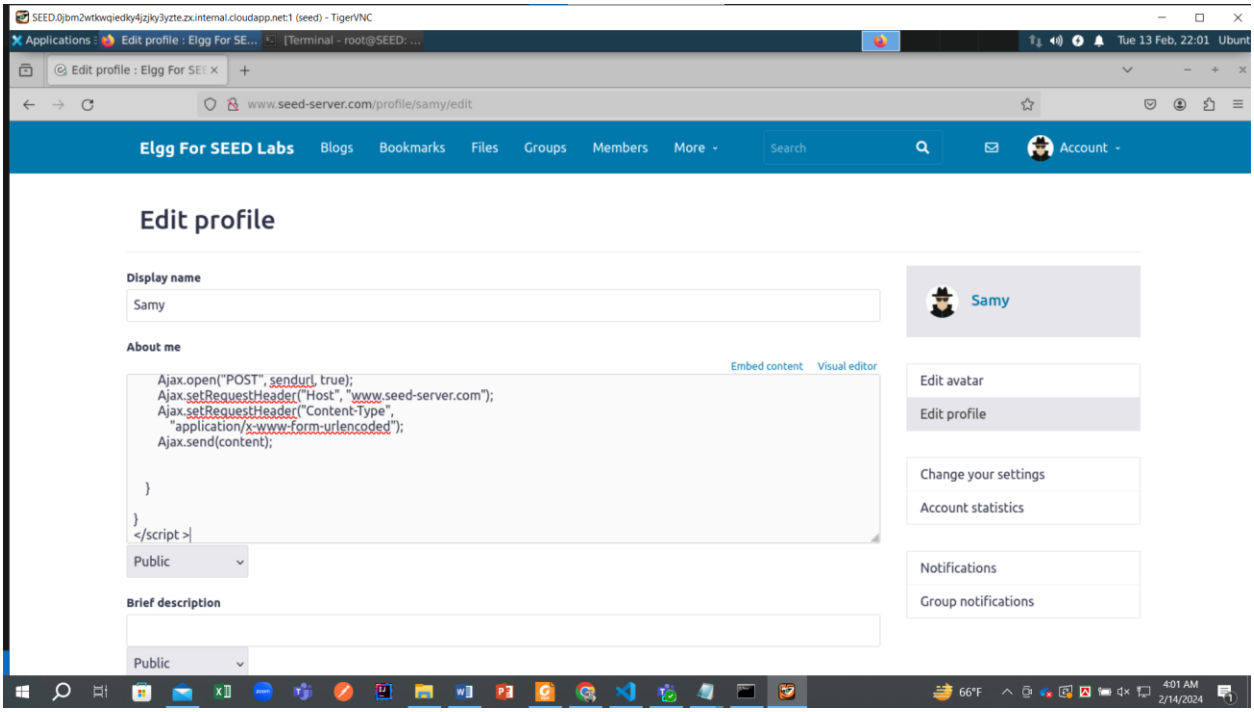
When ‘post’ button is clicked , a http post request is sent .



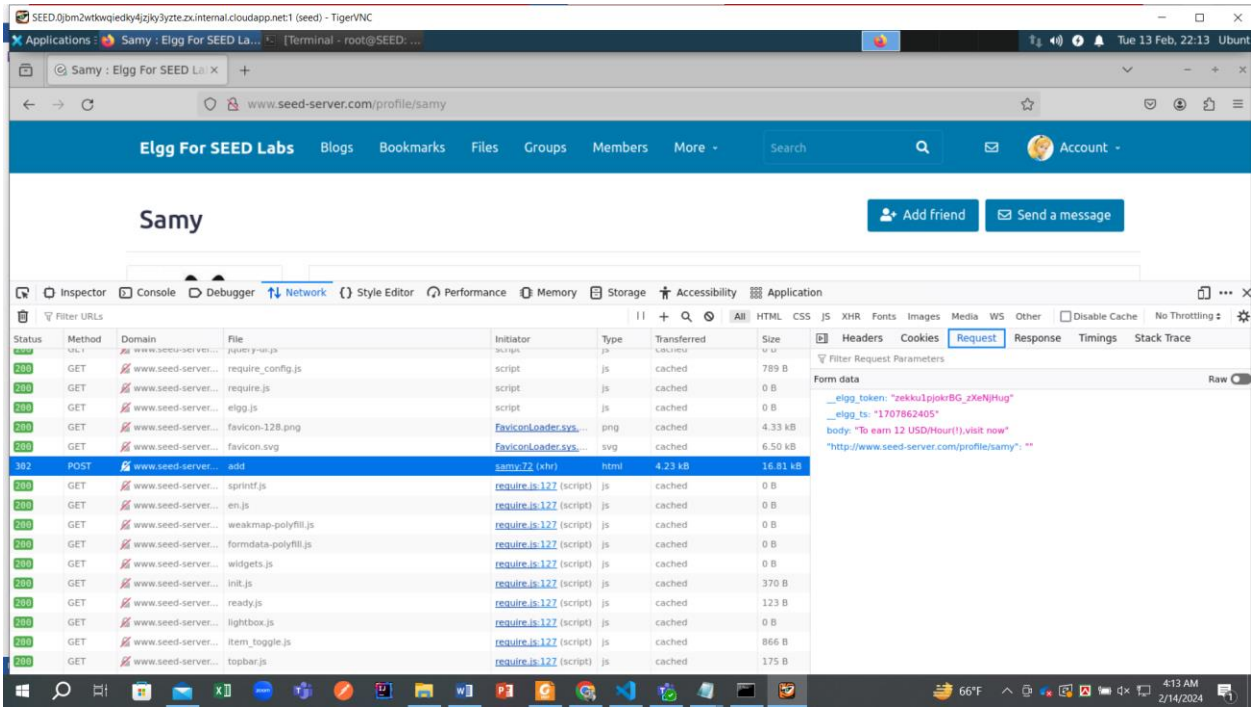
In request body of post request , we see this.



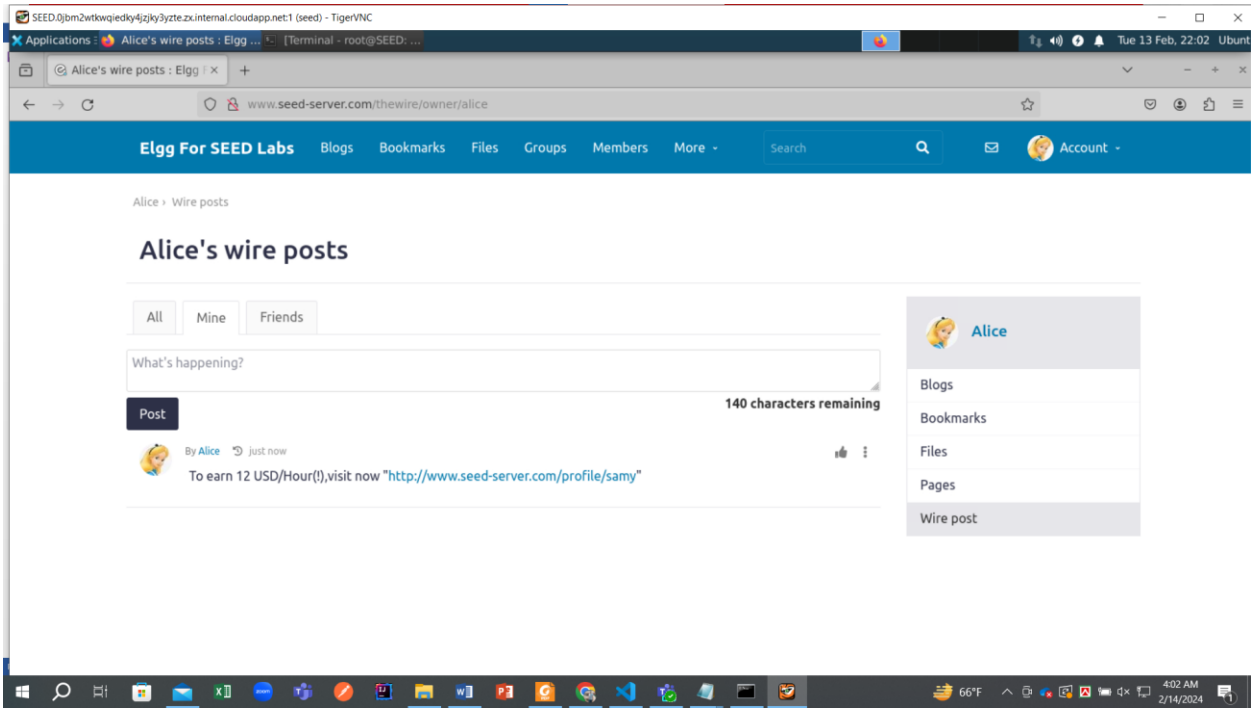
To do XSS attack , Samy put a java script in his ‘about me’ text field .



When Alice view samy’s profile , the script is executed , a http post request is sent to post by Alice , though Alice doesn’t click the ‘post’ button.

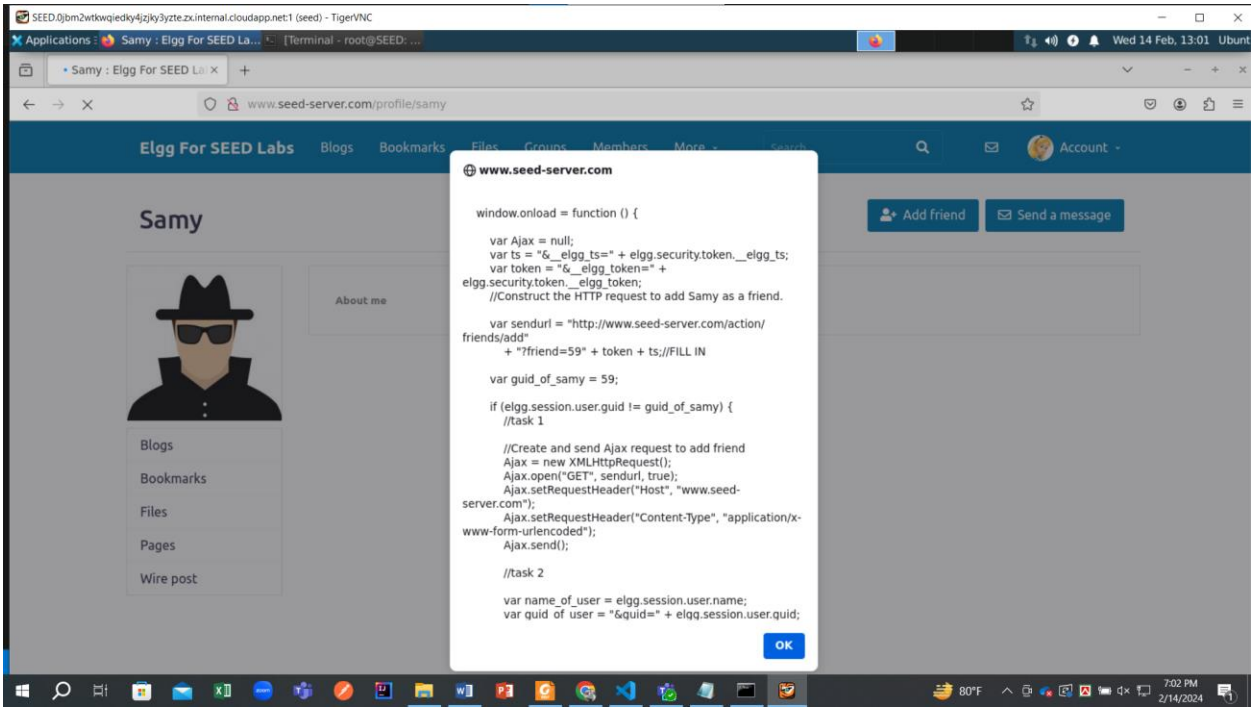


When Alice visits Alice’s wire posts , she see a post is published by herself , though she doesn’t .

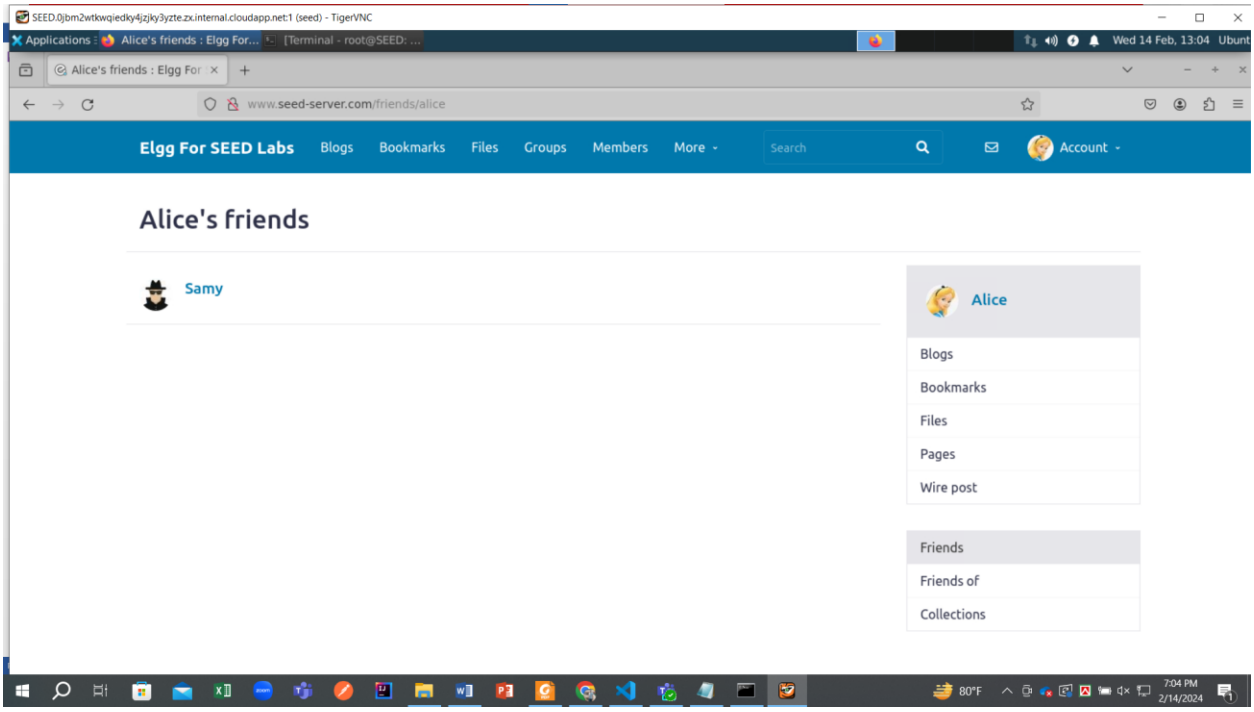


Task 4 :

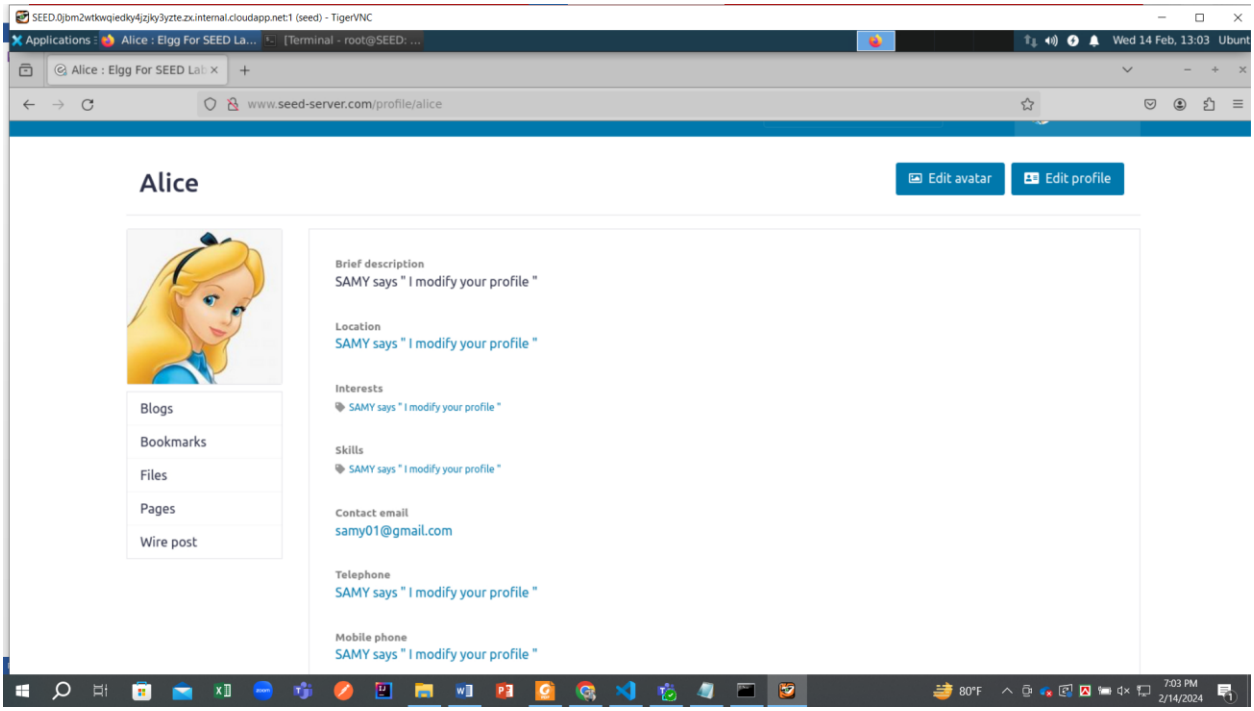
I write a malicious JavaScript program by merging task 1 , task 2 ,task 3 and given example of using DOM APIs . **To do XSS attack , Samy put a java script in his 'about me' text field . When Alice view samy's profile , the script is executed , an alert message is shown.**

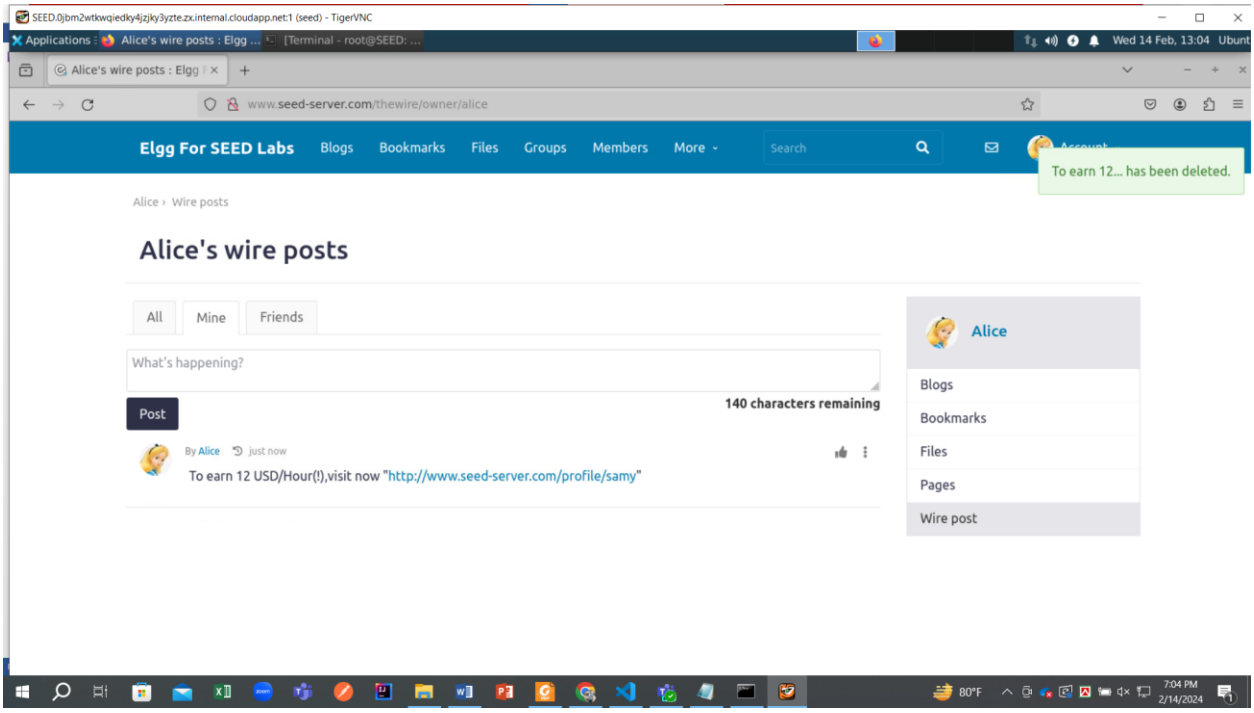


The worm sends a friend request to Samy without Alice clicking the add friend button.

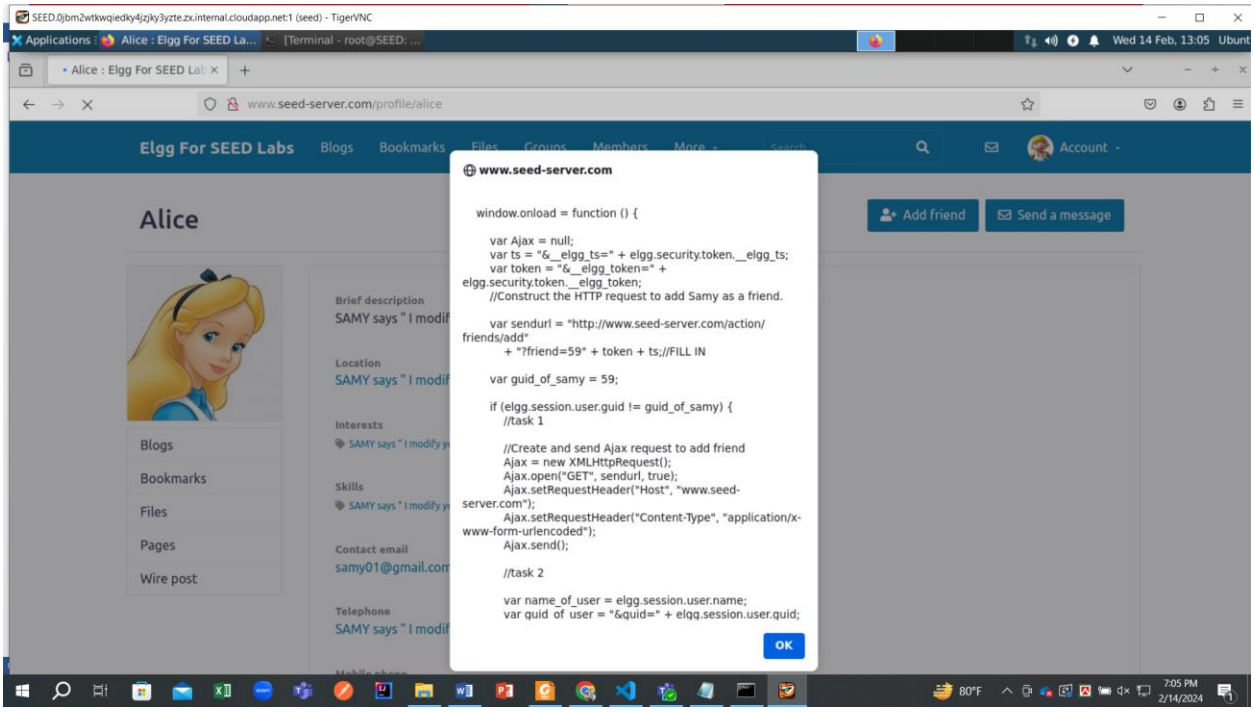


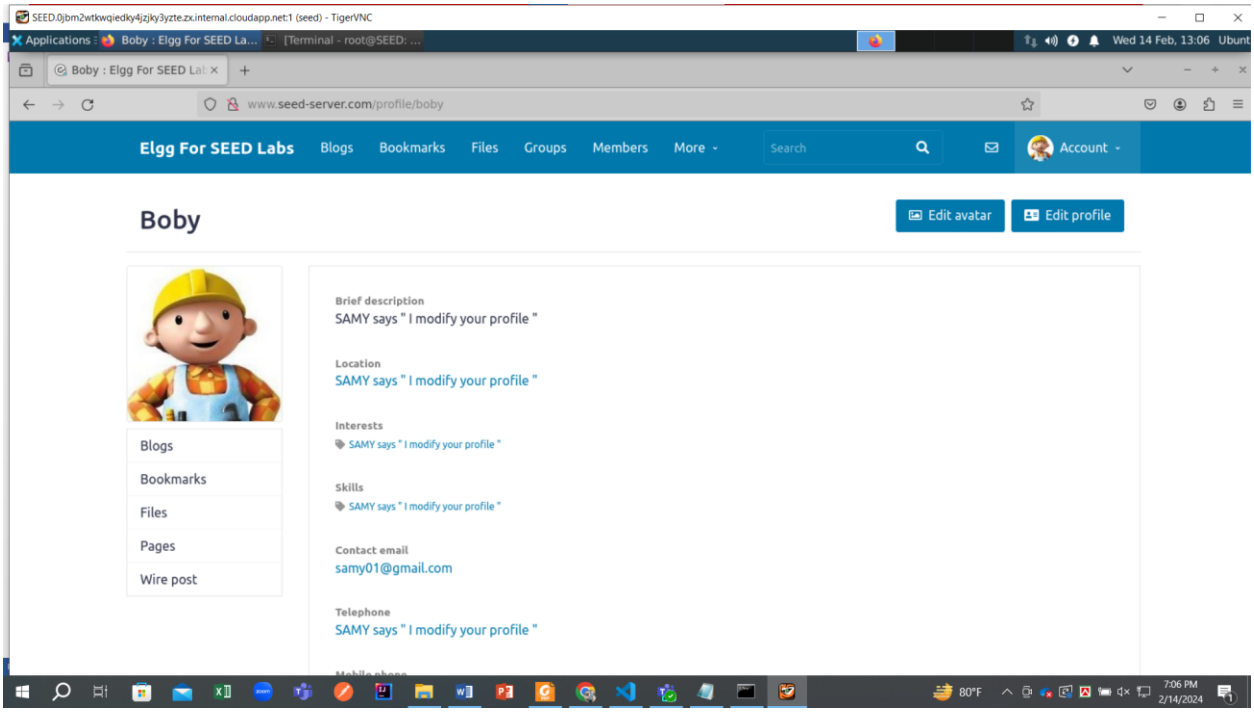
The worm replicates itself by modifying Alice's profile and posting Alice's profile link on the wire.

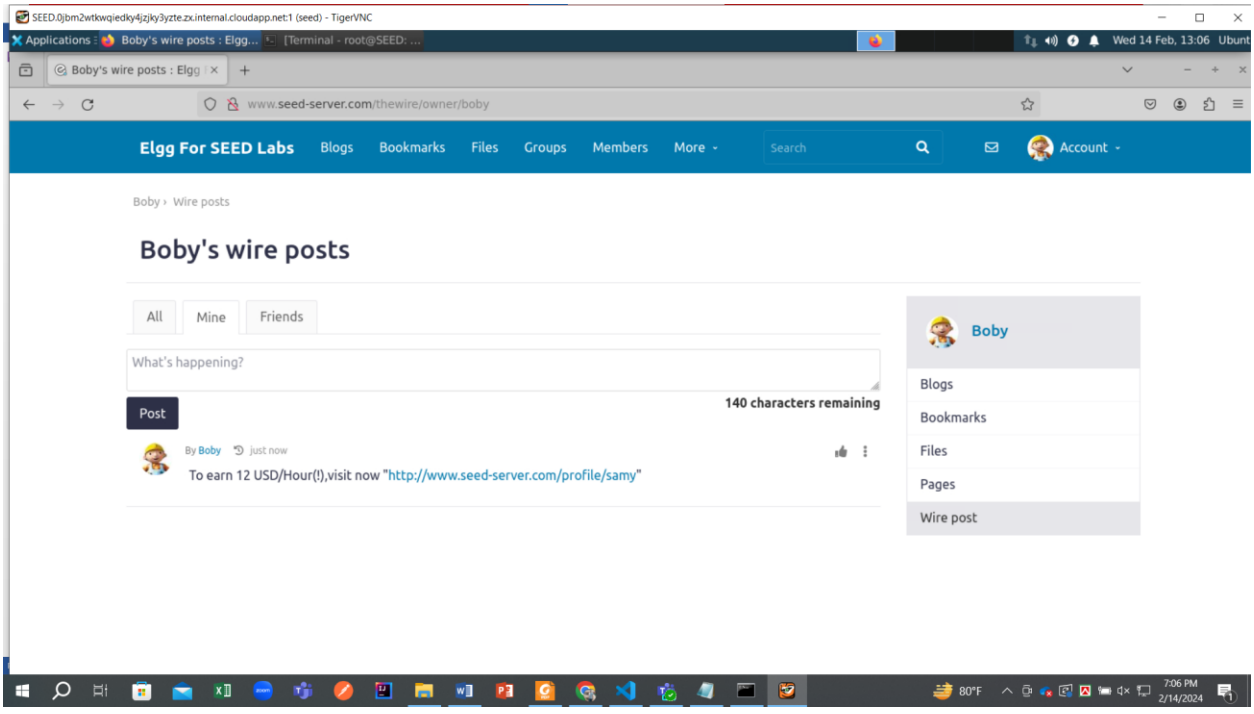


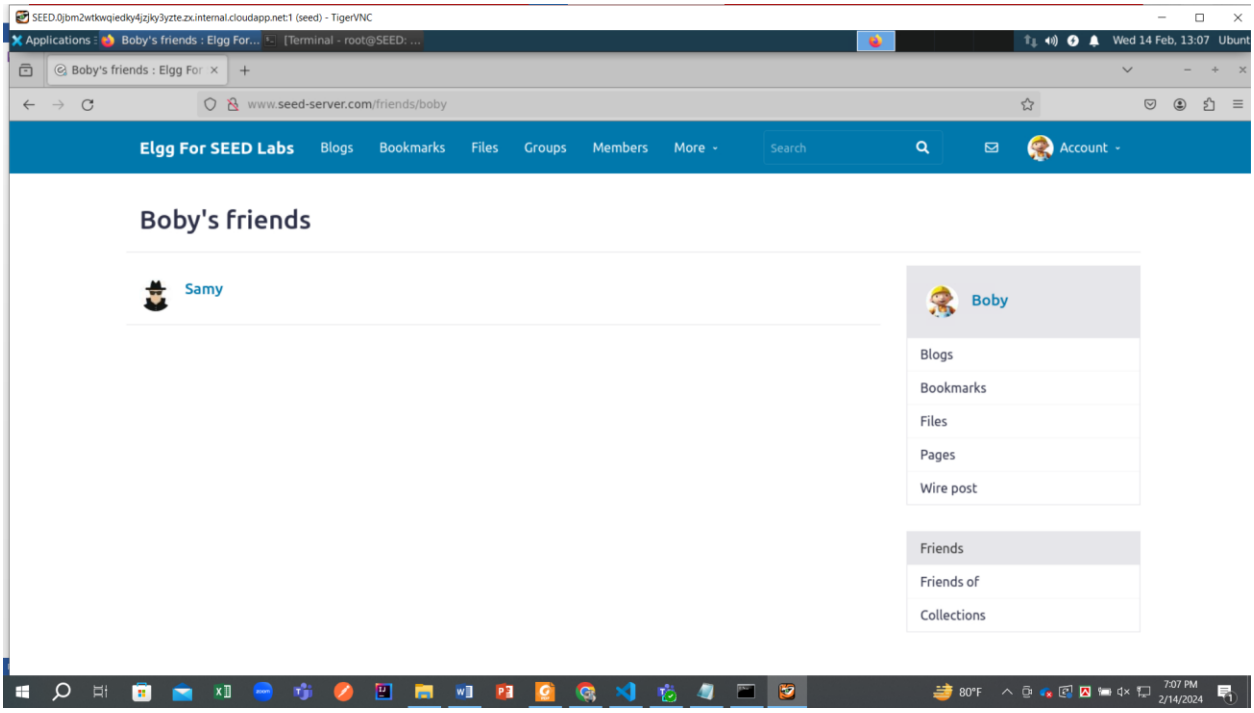


When Boby visits Alice's profile, he also adds Samy as a friend, and the Worm replicates itself to Boby's profile and posts his profile link on the wire. An alert message is shown.




SEED.0jbm2wtkwqiedky4jzjky3yzte.zx.internal.cloudapp.net:1 (seed) - TigerVNC
Applications
Boby : Elgg For SEED La...
[Terminal - root@SEED: ...
Wed 14 Feb, 13:06
Ubunt
Boby : Elgg For SEED La
www.seed-server.com/profile/boby
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Boby
Edit avatar
Edit profile
Blogs
Bookmarks
Files
Pages
Wire post
Brief description
SAMY says " I modify your profile "
Location
SAMY says " I modify your profile "
Interests
SAMY says " I modify your profile "
Skills
SAMY says " I modify your profile "
Contact email
samy01@gmail.com
Telephone
SAMY says " I modify your profile "
80°F
7:06 PM
2/14/2024


SEED.0jbm2wtkwqiedky4jzjky3yzte.zx.internal.cloudapp.net:1 (seed) - TigerVNC
Applications
Boby's wire posts : Elgg...
[Terminal - root@SEED: ...
Wed 14 Feb, 13:06
Ubunt
Boby's wire posts : Elgg
www.seed-server.com/thewire/owner/boby
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Boby › Wire posts
Boby's wire posts
All
Mine
Friends
What's happening?
Post
140 characters remaining
By Boby just now
To earn 12 USD/Hour(!),visit now "http://www.seed-server.com/profile/samy"
Boby
Blogs
Bookmarks
Files
Pages
Wire post
80°F
7:06 PM
2/14/2024


SEED.0jbm2wtkwqiedky4jzjky3yzte.zx.internal.cloudapp.net:1 (seed) - TigerVNC
Applications
Boby's friends : Elgg For...
[Terminal - root@SEED: ...
Wed 14 Feb, 13:07
Ubunt
Boby's friends : Elgg For
www.seed-server.com/friends/boby
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Boby's friends
Samy
Boby
Blogs
Bookmarks
Files
Pages
Wire post
Friends
Friends of
Collections
80°F
7:07 PM
2/14/2024