Bangladesh University of Engineering & Technology

Course No: CSE 406

Course Title:**Computer Security Sessional**

Offline-2:Cross-Site Scripting (XSS) Attack

Submitted By:

Name: Fatema Tuj Johora

Department: CSE

Section: A1

Roll: 1905022

Date of submission:02.15.2023

Title:Cross-Site Scripting (XSS) Attack

Introduction:

In this assignment, the network tab of the inspector tool serves as a vital resource for monitoring HTTP methods,(GET and POST). These methods play a crucial role in exchanging information on a website. By focusing on the network tab, we not only observe the HTTP methods in action but also analyze the request and response bodies. This allows us to gain a comprehensive understanding of how data is transferred, enhancing our ability to fulfill the requirements of the assignment effectively.We also have to use javascript , ajax to fulfill our goal.

Tasks:

- For the tasks, we need some variables like a timestamp and security token parameter. Also, the attacker's profile id is needed.
    - For timestamp parameter-> elgg.security.token.__elgg_ts
    - For token parameter-> elgg.security.token.__elgg_token
    - For attacker’s profile id-> elgg.page_owner.guid
    - For user’s profile id-> elgg.session.user.guid
- We also need a url and required contents for Ajax requests.
- To make sure that Samy won’t get affected by his own code, an extra condition should be checked.

Task 1:

Becoming the Victim’s Friend:

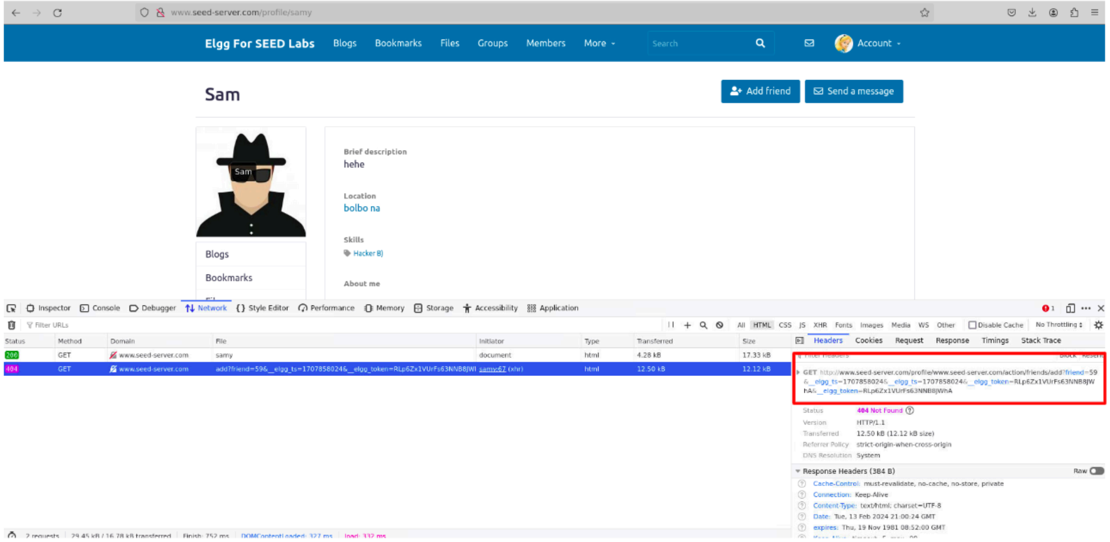
Steps:

- A url has to be formed to send friend request to the attacker, to do so :

  - urlHeader variable is declared, which contains the url.
  - urlHeader="http://www.seed-server.com/action/friends/add?friend="+elgg.page_owner.guid

Problems & Solutions:

- The requests and responses for the "add friend" feature were monitored in the Network tab of the Inspector. Then the sendurl variable was updated.However, a problem was encountered as the sendurl link was initially provided without "http://" resulting in errors.

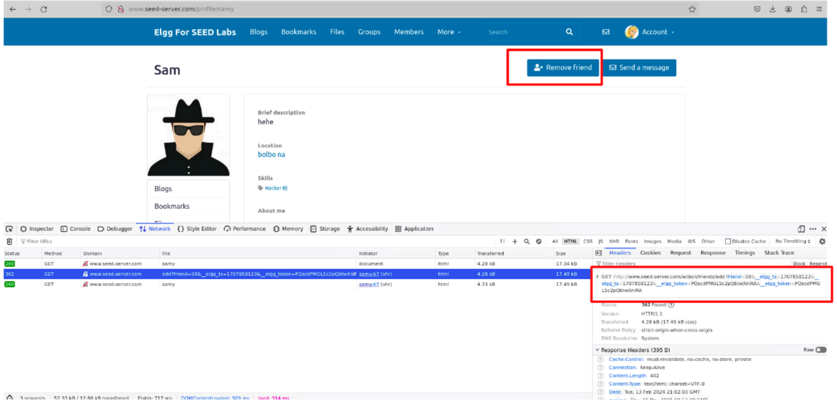


```
Status  Method  Domain               File                                                                    Initiator          Type  Transferred  Size
200     GET     www.seed-server.com  samy                                                                    document           html  4.28 kB      17.33 kB
404     GET     www.seed-server.com  add?friend=59&__elgg_ts=1707858024&__elgg_token=RLp6Zx1VUrFs63NNB8JWI  samy:67 (xhr)      html  12.50 kB     12.12 kB

GET http://www.seed-server.com/profile/www.seed-server.com/action/friends/add?friend=59&__elgg_ts=1707858024&__elgg_ts=1707858024&__elgg_token=RLp6Zx1VUrFs63NNB8JWhA&__elgg_token=RLp6Zx1VUrFs63NNB8JWhA
Status          404 Not Found
Version         HTTP/1.1
Transferred     12.50 kB (12.12 kB size)
Referrer Policy strict-origin-when-cross-origin
DNS Resolution  System
Response Headers (384 B)
Cache-Control: must-revalidate, no-cache, no-store, private
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Date: Tue, 13 Feb 2024 21:00:24 GMT
expires: Thu, 19 Nov 1981 08:52:00 GMT

2 requests | 29.45 kB / 16.78 kB transferred | Finish: 752 ms | DOMContentLoaded: 327 ms | load: 332 ms
```

Then I fixed it. So, with the correct url, task 1 was done successfully.



```
Status  Method  Domain               File                                                                    Initiator      Type  Transferred  Size
200     GET     www.seed-server.com  samy                                                                    document       html  4.28 kB      17.34 kB
302     GET     www.seed-server.com  add?friend=59&__elgg_ts=1707858123&__elgg_token=PQscdPMGL5c2pQblwXnlF  samy:67 (xhr)  html  4.28 kB      17.49 kB
200     GET     www.seed-server.com  samy                                                                    samy:67 (xhr)  html  4.33 kB      17.49 kB

GET http://www.seed-server.com/action/friends/add?friend=59&__elgg_ts=1707858123&__elgg_ts=1707858123&__elgg_token=PQscdPMGL5c2pQblwXnIRA&__elgg_token=PQscdPMGL5c2pQblwXnIRA
Status          302 Found
Version         HTTP/1.1
Transferred     4.28 kB (17.49 kB size)
Referrer Policy strict-origin-when-cross-origin
DNS Resolution  System
Response Headers (395 B)
Cache-Control: must-revalidate, no-cache, no-store, private
Connection: Keep-Alive
Content-Length: 402
Content-Type: text/html; charset=UTF-8
Date: Tue, 13 Feb 2024 21:02:03 GMT

3 requests | 52.33 kB / 12.88 kB transferred | Finish: 717 ms | DOMContentLoaded: 309 ms | load: 314 ms
```

Task 2:

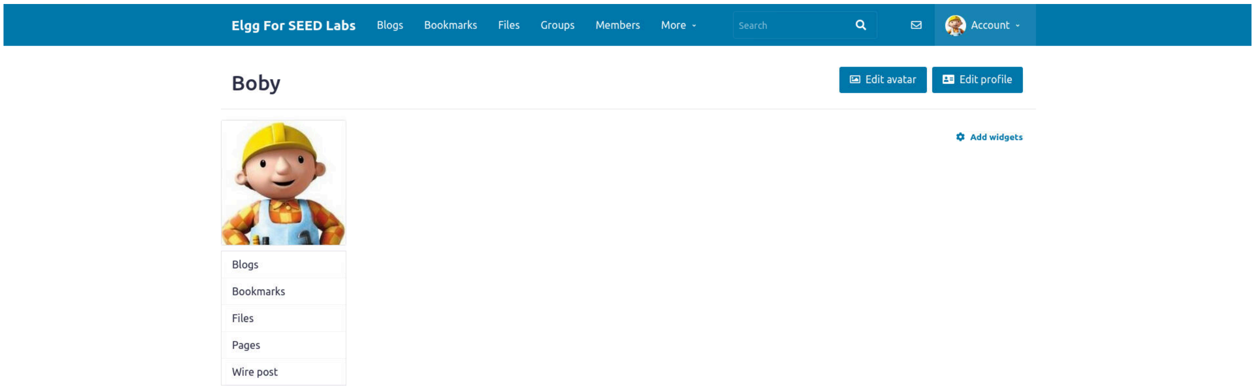
Modifying The Victim’s Profile:

Steps:

- A url has to be formed to edit the victim’s profile, to do so sendurl variable is declared
    - sendurl="http://www.seed-server.com/action/profile/edit"
- A variable named content is declared , which contains all the parameters of profile information and their values. This variable is sent with Ajax request.

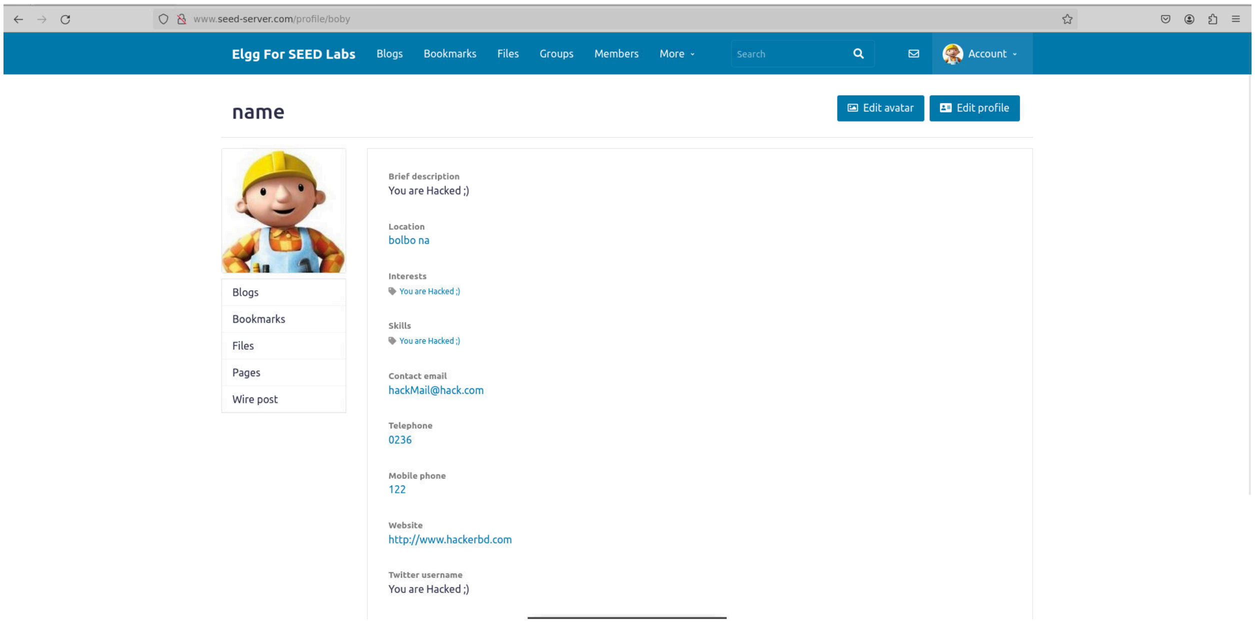
Problems & Solutions:

- During this step, several problems were encountered.
    - Initially, after editing the profile, the changes were not reflected in the profile display,but were changed in the "edit profile" page. Upon inspecting the response for the request, it was identified that errors were occurring due to specific fields accepting only certain types of values. To resolve this issue, adjustments were made to the field values:
        - Website: Only accepts proper URL values.
        - Phone/Mobile: Only accepts numeric values.
        - Email: Only accepts strings with "@"
    - Despite these corrections, the issue persisted. Further investigation revealed that an incorrect GUID was provided for the "guid" field. Instead of using "elgg.session.user.guid", "elgg.page_owner.guid" was mistakenly used
    - After fixing it, task 2 was done successfully
- This is the screenshot of victim’s profile before visiting the attacker’s profile:



Boby

- This is the screenshot of victim’s profile after visiting the attacker’s profile:



name

Brief description
You are Hacked ;)

Location
bolbo na

Interests
You are Hacked ;)

Skills
You are Hacked ;)

Contact email
hackMail@hack.com

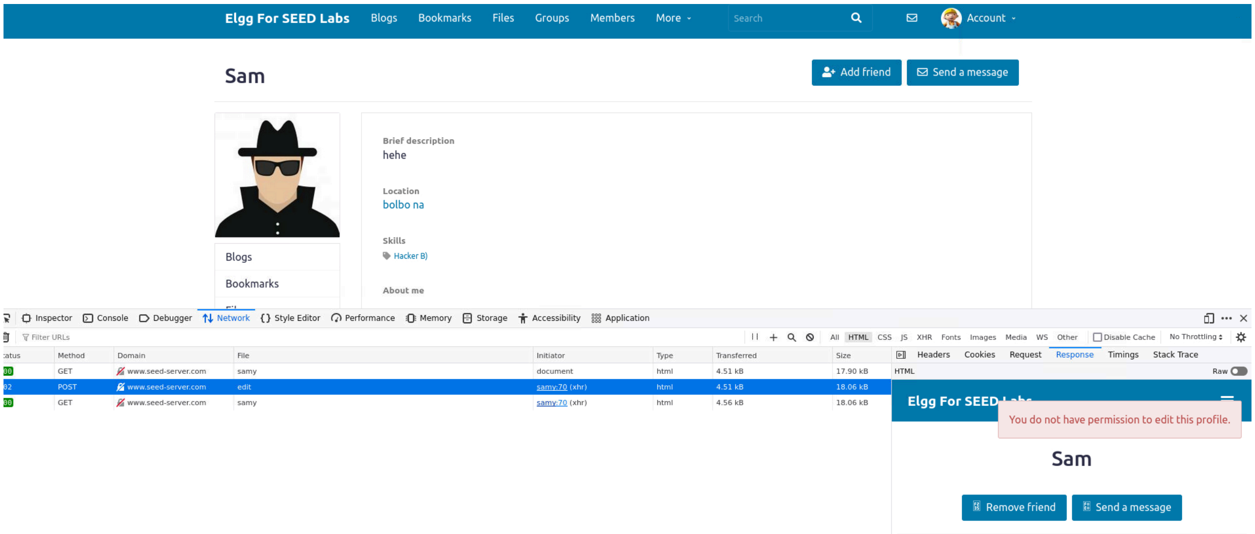
Telephone
0236

Mobile phone
122

Website
http://www.hackerbd.com

Twitter username
You are Hacked ;)

- These are the screenshots after visiting the attacker’s profile (when guid was wrong):
  - Screenshot of response:



Sam

Brief description
hehe

Location
bolbo na

Skills
Hacker B)

About me

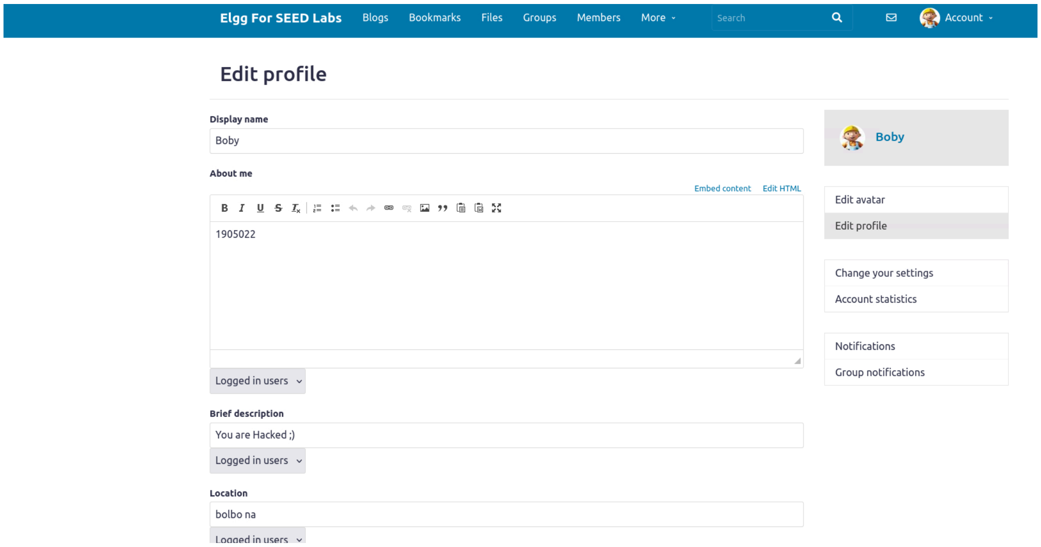
:atus	Method	Domain	File	Initiator	Type	Transferred	Size
00	GET	www.seed-server.com	samy	document	html	4.51 kB	17.90 kB
02	POST	www.seed-server.com	edit	samy:70 (xhr)	html	4.51 kB	18.06 kB
00	GET	www.seed-server.com	samy	samy:70 (xhr)	html	4.56 kB	18.06 kB

Elgg For SEED Labs

You do not have permission to edit this profile.

Sam

- Screenshot of victims “edit-profile”:



Edit profile

Display name
Boby

About me
1905022

Logged in users

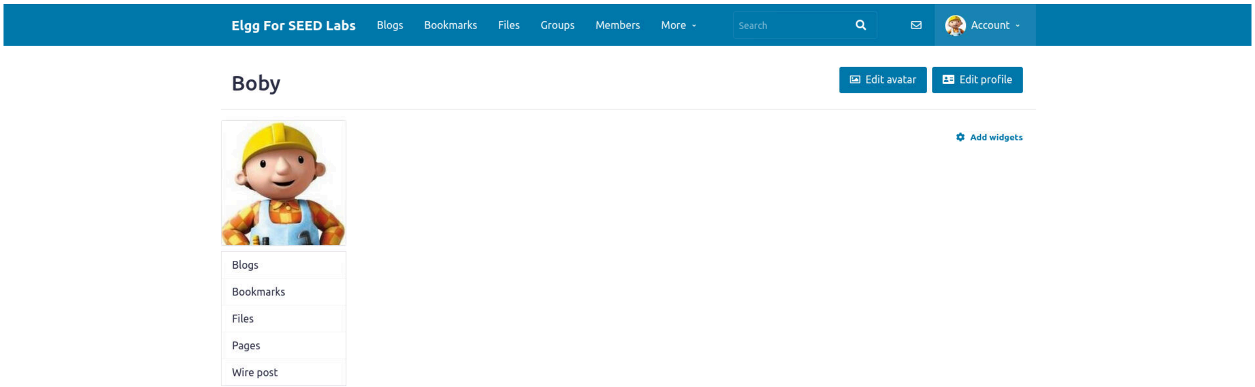
Brief description
You are Hacked ;)

Logged in users

Location
bolbo na

Logged in users

- Screenshot of victim’s profile:(nothing changed)



Boby

Task 3:

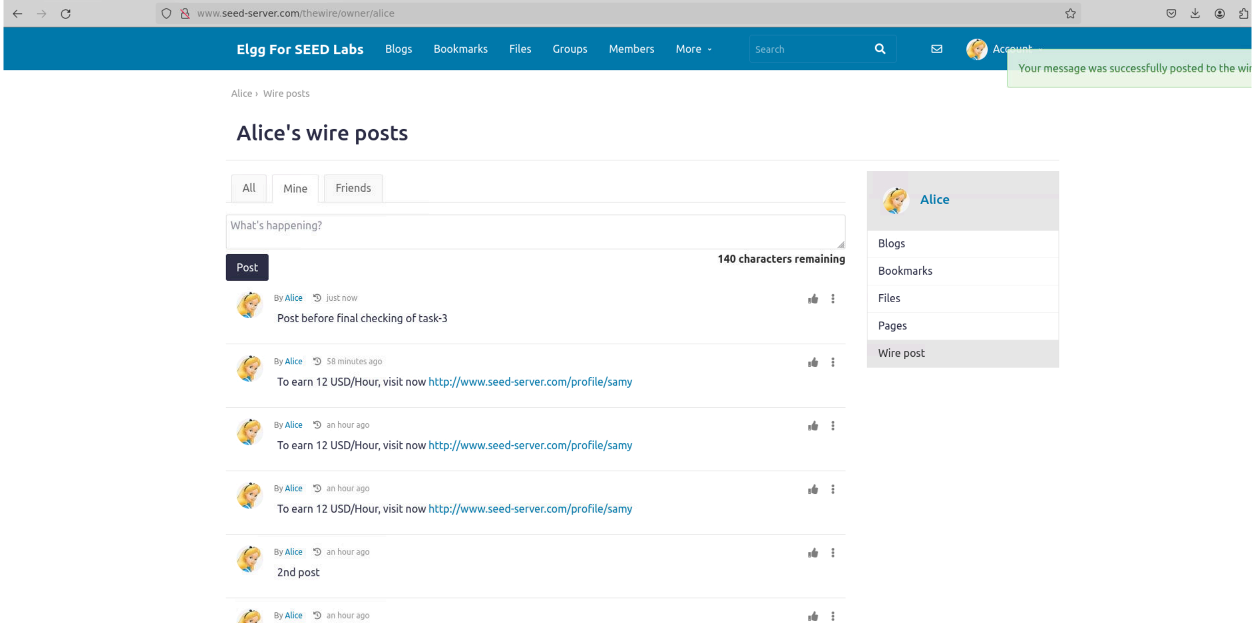
Posting on the Wire on Behalf of the Victim :

Steps:

- A url has to be formed to wire a post on t the victim's profile, to do so sendurl variable is declared
  - sendurl="http://www.seed-server.com/action/thewire/add"
- A variable named content is declared , which contains the body of the post which is sent with Ajax request. But, to post attacker's profile link, we need Samy's profile link, which can be got by http://www.seed-server.com/profile/samy"

Problems & Solutions:

- Same as Task 2 , so it was done successfully without any error
- Screenshot of victim's "wire post" page before visiting attacker's profile:



Your message was successfully posted to the wi

Alice's wire posts

What's happening?

Post

140 characters remaining

By Alice just now
Post before final checking of task-3

By Alice 58 minutes ago
To earn 12 USD/Hour, visit now http://www.seed-server.com/profile/samy

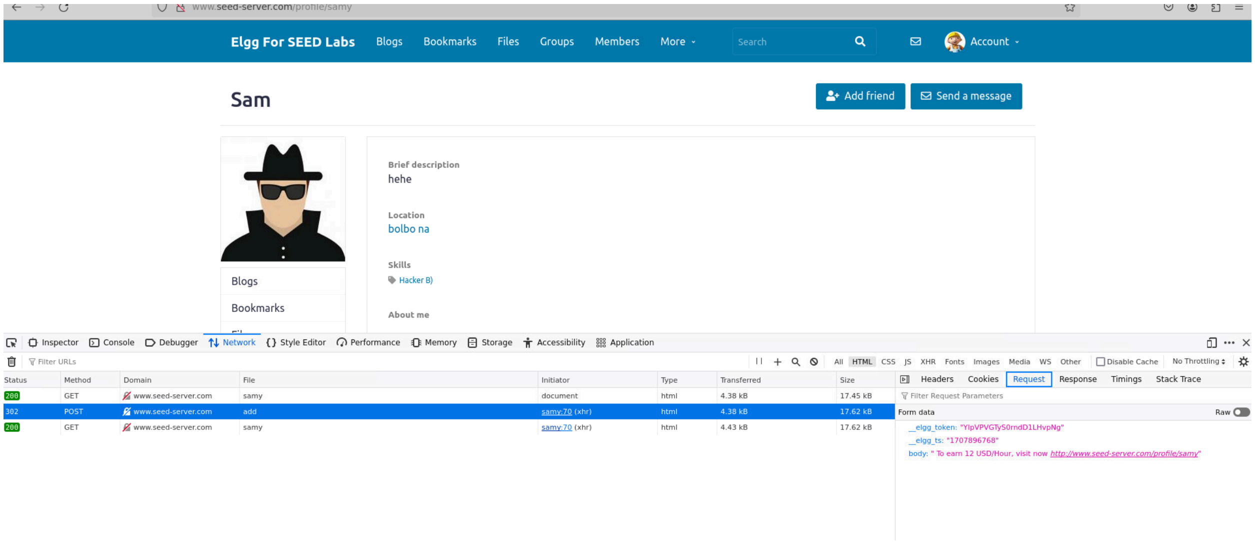
By Alice an hour ago
To earn 12 USD/Hour, visit now http://www.seed-server.com/profile/samy

By Alice an hour ago
To earn 12 USD/Hour, visit now http://www.seed-server.com/profile/samy

By Alice an hour ago
2nd post

By Alice an hour ago

- Screenshot of request-response while visiting attacker’s profile:
  - Request:



Sam

Brief description
hehe

Location
bolbo na

Skills
Hacker B)

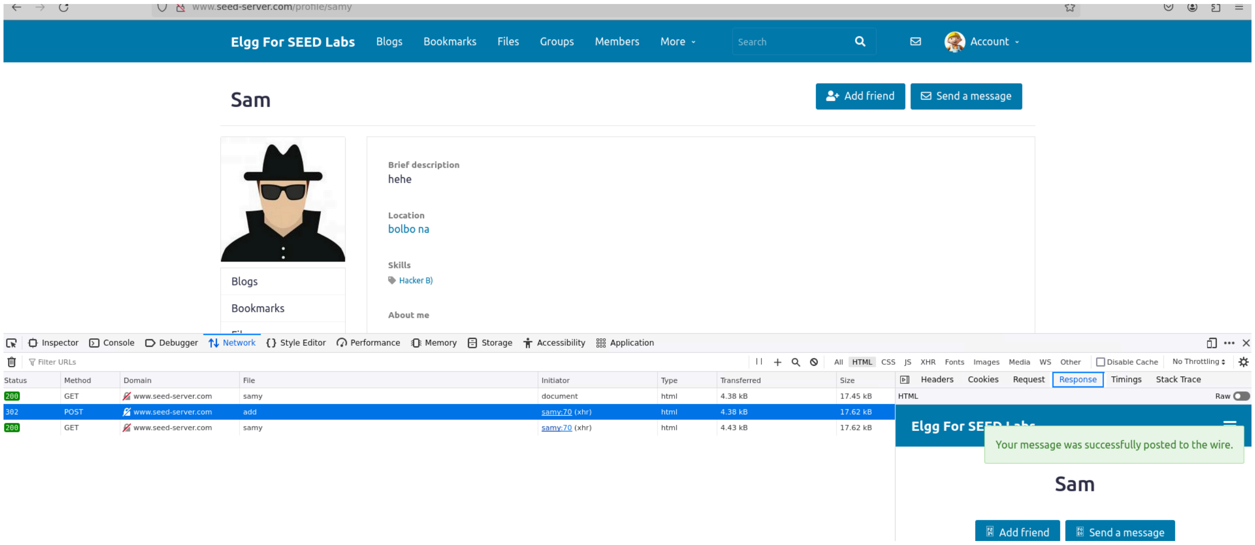
About me

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.seed-server.com	samy	document	html	4.38 kB	17.45 kB
302	POST	www.seed-server.com	add	samy:70 (xhr)	html	4.38 kB	17.62 kB
200	GET	www.seed-server.com	samy	samy:70 (xhr)	html	4.43 kB	17.62 kB

Form data

```
__elgg_token: "YIpVPVGTyS0rndD1LHvpNg"
__elgg_ts: "1707896768"
body: " To earn 12 USD/Hour, visit now http://www.seed-server.com/profile/samy"
```

- Response:



Sam

Brief description
hehe

Location
bolbo na

Skills
Hacker B)

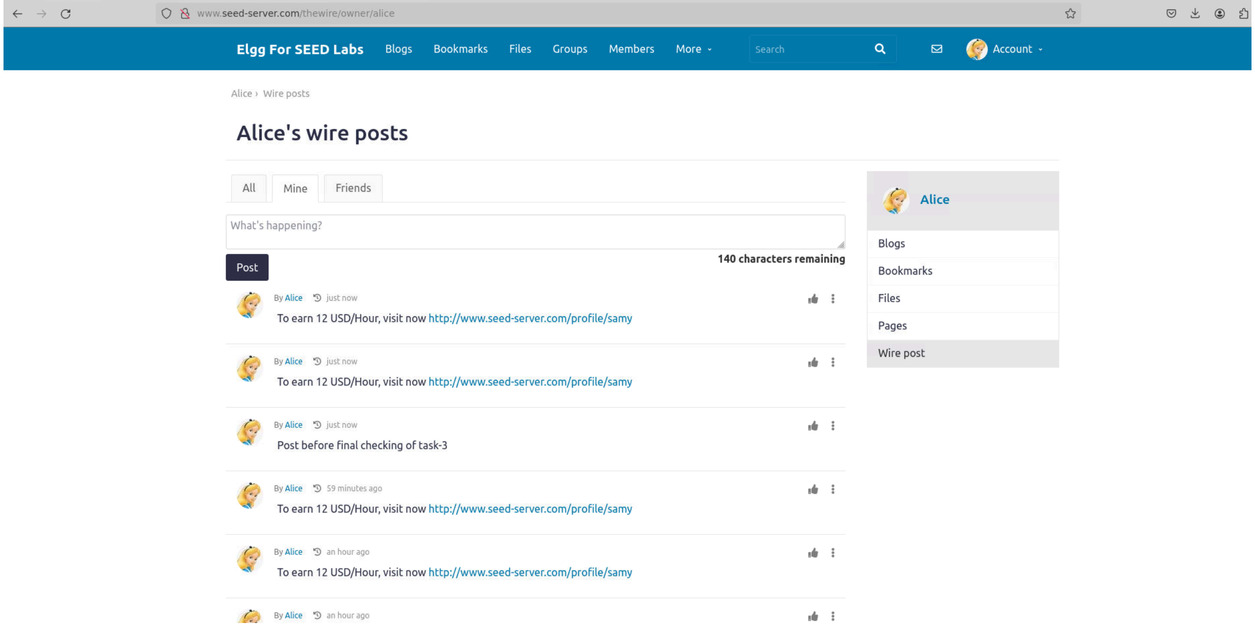
About me

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.seed-server.com	samy	document	html	4.38 kB	17.45 kB
302	POST	www.seed-server.com	add	samy:70 (xhr)	html	4.38 kB	17.62 kB
200	GET	www.seed-server.com	samy	samy:70 (xhr)	html	4.43 kB	17.62 kB

Your message was successfully posted to the wire.

Sam

- Screenshot of victim’s “wire post” page after visiting attacker’s profile:



Alice's wire posts

140 characters remaining

By Alice just now
To earn 12 USD/Hour, visit now http://www.seed-server.com/profile/samy

By Alice just now
To earn 12 USD/Hour, visit now http://www.seed-server.com/profile/samy

By Alice just now
Post before final checking of task-3

By Alice 59 minutes ago
To earn 12 USD/Hour, visit now http://www.seed-server.com/profile/samy

By Alice an hour ago
To earn 12 USD/Hour, visit now http://www.seed-server.com/profile/samy

By Alice an hour ago

Task 4:

Design a Self-Propagating Worm:

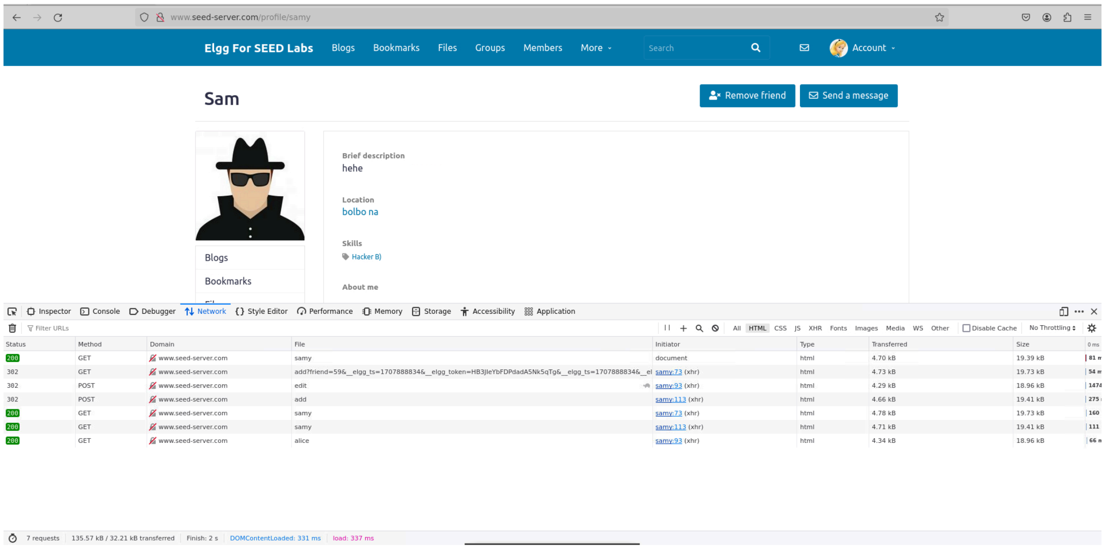
Steps:

- To design a self- propagating worm which will:
  - Add attacker as a friend
  - Modify victim's profile, where description contains same worm code
  - Post own profile link on the wire

  all previous task's codes are merged with worm code.

Problems & Solutions:

- Screenshot of http methods while visiting attacker's profile:
  - One Get method for sending friend request to attacker
  - Two Post methods for editing victim's profile and for posting profile link



Sam

Brief description
hehe

Location
bolbo na

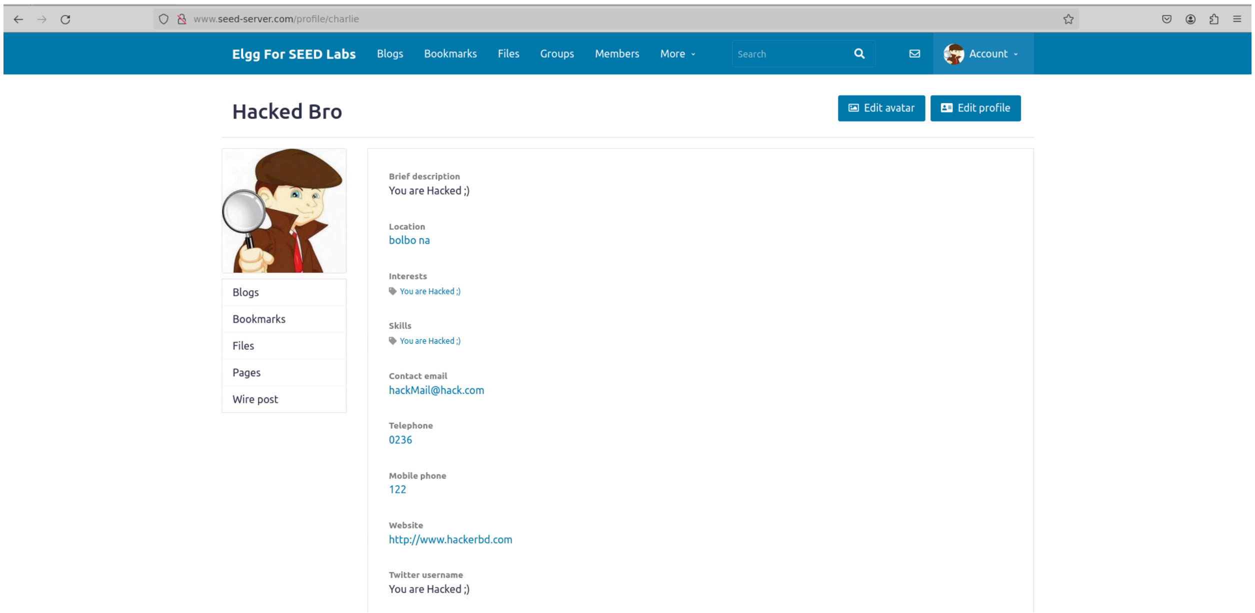
Skills
Hacker B)

About me

Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms
200	GET	www.seed-server.com	samy	document	html	4.70 kB	19.39 kB	81 m
302	GET	www.seed-server.com	add?friend=59&__elgg_ts=1707888834&__elgg_token=HB3JleYbFDPdadA5Nk5qTg&__elgg_ts=1707888834&__el	samy:73 (xhr)	html	4.73 kB	19.73 kB	54 m
302	POST	www.seed-server.com	edit	samy:93 (xhr)	html	4.29 kB	18.96 kB	1474
302	POST	www.seed-server.com	add	samy:113 (xhr)	html	4.66 kB	19.41 kB	275
200	GET	www.seed-server.com	samy	samy:73 (xhr)	html	4.78 kB	19.73 kB	160
200	GET	www.seed-server.com	samy	samy:113 (xhr)	html	4.71 kB	19.41 kB	111
200	GET	www.seed-server.com	alice	samy:93 (xhr)	html	4.34 kB	18.96 kB	66 m

7 requests | 135.57 kB / 32.21 kB transferred | Finish: 2 s | DOMContentLoaded: 331 ms | load: 337 ms

- Screenshot of Victim's Profile:



Hacked Bro

Brief description
You are Hacked ;)

Location
bolbo na

Interests
You are Hacked ;)

Skills
You are Hacked ;)

Contact email
hackMail@hack.com

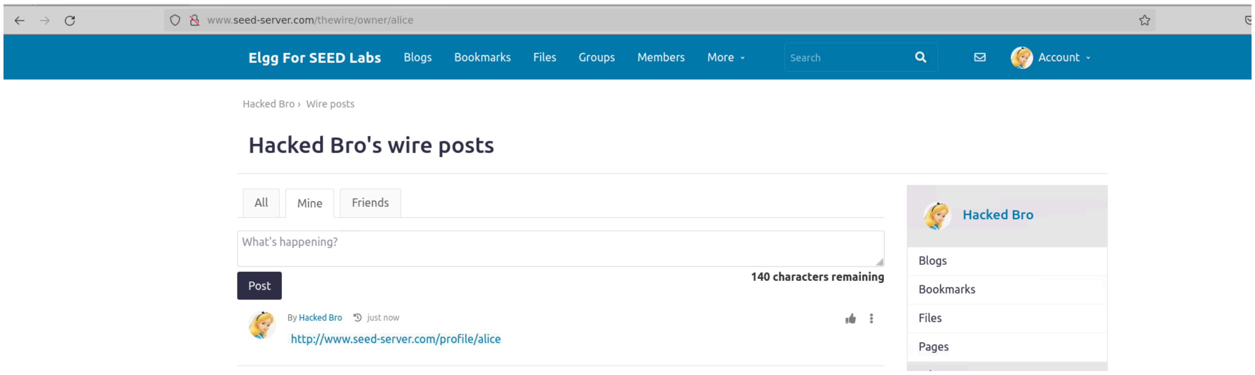
Telephone
0236

Mobile phone
122

Website
http://www.hackerbd.com

Twitter username
You are Hacked ;)

- Screenshot of Wired-Post :



Hacked Bro's wire posts

By Hacked Bro just now
http://www.seed-server.com/profile/alice

Conclusion:

In the presented context, the execution of malicious JavaScript code has been employed to manipulate the behavior of a social networking

application. Specifically, the code focuses on the creation of forged HTTP requests, aiming to send friend requests ,modify profile information,wire posts or propagate a worm . These actions are carried out through the careful construction of URLs and AJAX requests, exploiting potential vulnerabilities.
Using javascript, Ajax our objectives are fulfilled.