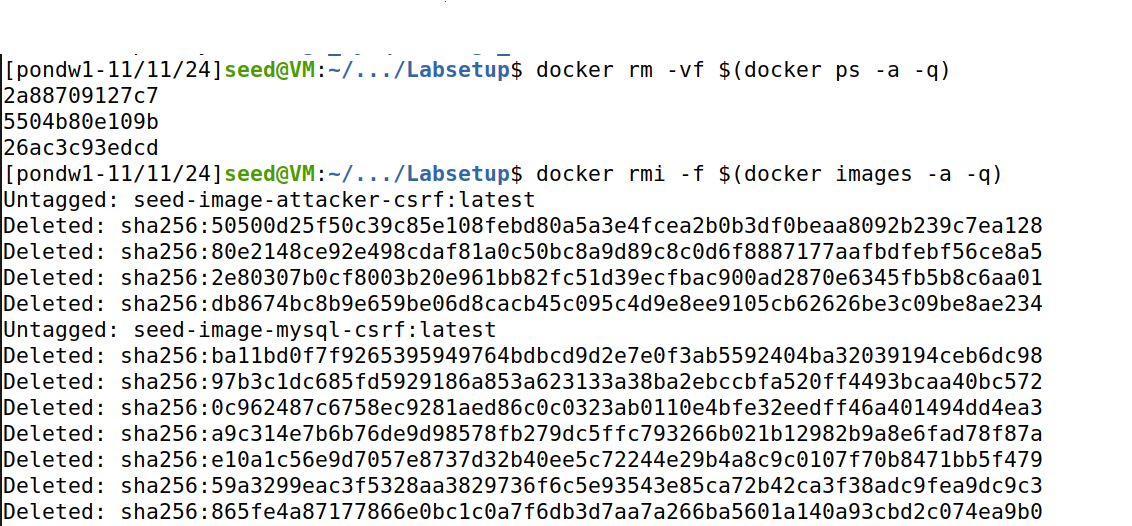
Will Pond

Removing all contains from previous lab



Building up the container

A screenshot of a computer screen

Description automatically generated

Running dcup

A screenshot of a computer

Description automatically generated

Editing the /etc/hosts file and putting in the 10.9.0.5 www.seed-server.com

A screenshot of a computer

Description automatically generated

Checking the docker to see everything is running

A screenshot of a computer

Description automatically generated

Getting the root ID for elgg website

A screenshot of a computer code

Description automatically generated

**TASK1**

Adding the javascript code in the brief description after login as Samy and clicking save.

A screenshot of a computer

Description automatically generated

After clicking save I got alert message saying that “Attack with XSS”

A screenshot of a computer

Description automatically generated

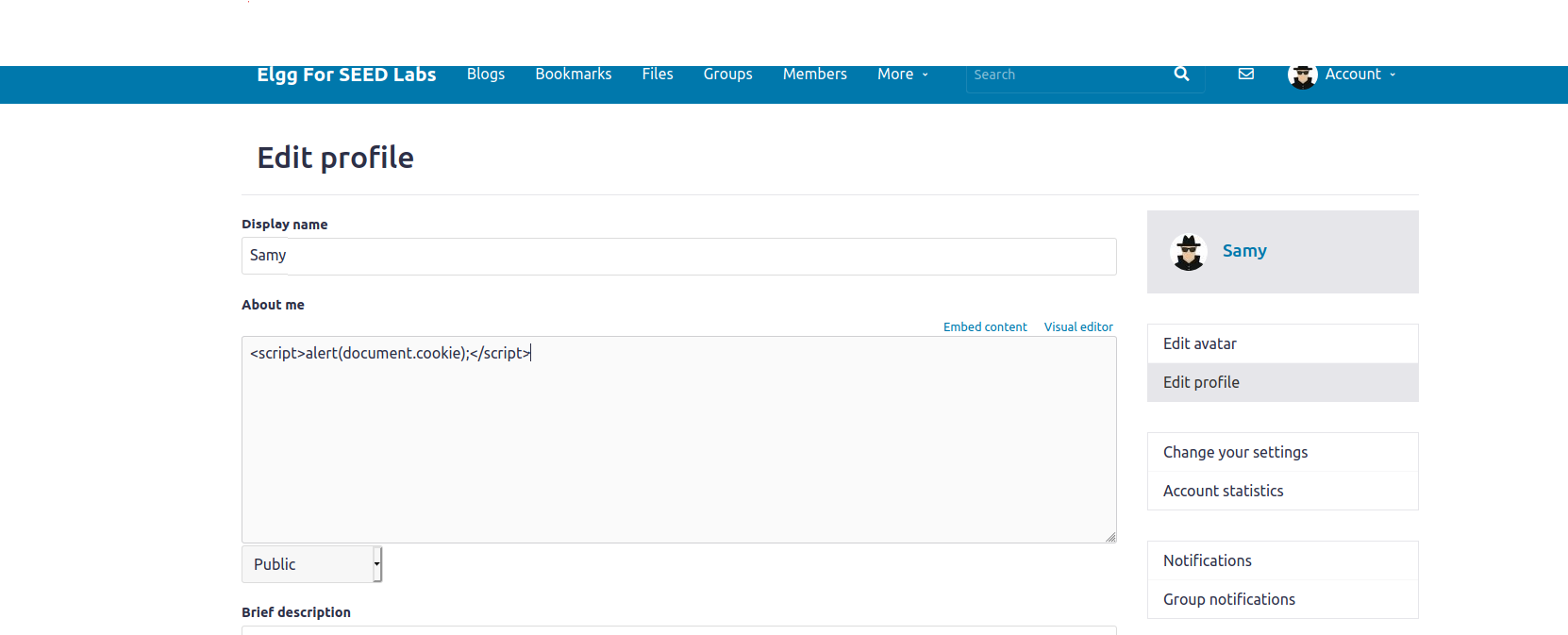
Login in as Alice and view Samy profile I got alert message saying the exact same thing

A screenshot of a computer

Description automatically generated

**TASK 2**

Login as Samy and putting the JavaScript code into the about me section after clicking edit html and then save it.



Getting Samy cook after clicking the save button

A screenshot of a computer

Description automatically generated

Login in as Alice and viewing Samy profile and getting her cookie from an alert message.

A screenshot of a computer

Description automatically generated

**Task3**

Running the nc -l 5555 command to listen for incoming connections

**A close-up of a computer screen

Description automatically generated**

Putting the JavaScript code in the about me section and saving it

A screenshot of a computer

Description automatically generated

Getting the cookie of and Samy in the first ncl – 5555 command and then getting Alice cookie when viewing Samy profie and running the ncl -555 command

A screenshot of a computer

Description automatically generated

**Task4**

Getting Samy GUID through his profile source code which is 59 or HTTP Header live to get format of the request

A black and white screen with text

Description automatically generated

A screenshot of a computer

Description automatically generated

Create a JavaScript file to put the code in as a place holder when I copy the code into the description section of Samy profile and save it.

A screenshot of a computer

Description automatically generated

Putting the code in the about me section

A screenshot of a computer

Description automatically generated

Login as Alice and view Samy profile and look back at Alice friends and Samy was added as friend

A screenshot of a computer

Description automatically generated

**Question 1**

**Explain the purpose of Lines ➀ and ➁, why are they needed?**

Lines 1 and 2 are needed because they are getting the values of \_\_elgg\_ts and \_\_\_elgg\_token as these values are uniquely generated so they are serving as security clearance to avert CRSF attacks

**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?**

The answer to that question is no because extra HTML code would be added to the previous code and adding unnecessary symbols characters to it will prevent the code to executing appropriately. Therefore, Text Mode is needed.

**TASK 5**

The post Request from HTTP Header live when update the profile so it can used in the JavaScript program

**A screenshot of a computer

Description automatically generated**

Create a JavaScript file to put the code in as a place holder when I copy the code into the description section of Samy profile and save it. After understanding the post request of edit profile from the HTTP inspection tool edit the code again construct the URL from the post request

A screenshot of a computer program

Description automatically generated

Placing the code in the about me section

A screenshot of a computer

Description automatically generated

Login in as Alice and viewing Samy profile and going back to Alice profile there was a modification in the about me section. The add text said that “Samy is my hero”.

A screenshot of a computer

Description automatically generated

**Question 3**

**Why do we need Line ➀? Remove this line and repeat your attack. Report and explain  
your observation.**

Removing the Line 1 code of if(elgg.session.user.guid!=samyGuid)

**A screenshot of a computer

Description automatically generated**

After click save and view Samy profile he attacks himself and he too as the “Samy is my hero” in the about me section

**A screenshot of a computer

Description automatically generated**

So, the purpose of that line of code is to check if GUID is Samy if so, don’t execute that block of code because you would attack yourself by that point. Therefore, that line of code is a precaution for him.

**TASK6**

**Using DOM Approach**

Create a JavaScript file to put the code in as a place holder when I copy the code into the description section of Samy profile and save it. This is a copy of the edit profile code with add modification of the DOM API.

**A screenshot of a computer

Description automatically generated**

Placing the code in the about section in Samy profile and then click save.

**A screen shot of a computer

Description automatically generated**

Login as Alice to viewed Samy profile and then look back at her profile she was been infected by the worm. About her says “The Worm is Spreading”.

A screenshot of a computer

Description automatically generated

Login as Boby to viewed Alice profile and then look back at his profile he was been infected by the worm. About him says “The Worm is Spreading”.

A screenshot of a computer

Description automatically generated

The HTTP Header live request Post

A screenshot of a computer

Description automatically generated

**Lab 6 Reflection**

In this lab I was able to do Cross-site scripting by injecting malicious code like JavaScript into the victim web browser. I Used the Elgg open-source web application for social network to launch my attacks. In Task1 was able to write a JavaScript program inside the description field so that when other users view Samy profile they would get alert message saying “XXS attack”. In Task2 I was able write a JavaScript program to display cookies in an alert message by using the doucument.cookie when the code is placed in the about me section and when other users view Samy profile they will see their cookies in alert message.

In Task 3 I was able to steal cookies from people when they visited Samy profile by using using img tag to get the HTTP GET request then using escape(document.cookie to document the cookie when writing the JavaScript program running the nc -l 5555 command to listen for the connection when people view Samy profile to steal their cookie. Task 4 involved becoming the victim’s friend by writing a JavaScript program. To do this I had to figure out the GET request of adding a friend and then Getting GUID of Samy to be placed inside code. After that place the code inside about me section of the profile and have people view Samy profile to be automatically add Samy as a friend.

In Task5 I was able to modify the Victims Profile by writing a JavaScript program like in Task4, but I must get the POST request when updating the profile. Then place the code in about section and the Text mode should be enabled to launch the attack. So, when people view the profile, their profile also get updated with added text in Samy profile. Finally, in Task6 I was to create Self-Propagating XSS Worm using the DOM approach by writing a JavaScript program to get the API DOM and then using code of the for edit profile to complete the attack. So when people view Samy people they will be inflected and when other people view their they will also be inflected.