Will Pond

Lab set up

Running dcbuild to create the docker images

A screenshot of a computer

Description automatically generated

Running dcup to start the container

A computer screen shot of a computer

Description automatically generated

After Opening up a new terminal tab I ran dockps to get the process status

A screenshot of a computer

Description automatically generated

Opening the etc/hosts file and making configurations to the DNS

A screenshot of a computer

Description automatically generated

**TASK1**

Logging into the seed-sever.com as Alice

A screenshot of a computer

Description automatically generated

Opening up the get request through HTTP Header live Main –Mozilla Firefox also getting the password for Alice

A screenshot of a computer

Description automatically generated

Getting the post request with the other added values

A screenshot of a computer

Description automatically generated

**TASK2**

Logging in as Samy

**A screenshot of a computer

Description automatically generated**

Adding Alice to Samy friends and getting the request which contains her GUID which is 56

**A screenshot of a computer

Description automatically generated**

Look at Samy profile source code to get the GUID which is 59

A black screen with white text

Description automatically generated

Editing the addfriend.html and putting in the link from the GET request of Alice from the previous step.

A screen shot of a computer

Description automatically generated

Find the addfriend.html in the root of @5504b80e109b which was found in dockps command for the attacker

A screenshot of a computer

Description automatically generated

Copying the addfriend.html to the docker

A black screen with text on it

Description automatically generated

Making sure it was copy to the docker

A screen shot of a computer

Description automatically generated

Sending Alice a message to visit the webpage to add Samy as a friend

A screenshot of a computer

Description automatically generated

After Alice clicked on the link and accessed the webpage Samy was added as a friend.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Task3**

Logging back in as Samy and adding “Samy is my hero. Description of his profile

A screenshot of a computer

Description automatically generated

Getting the POST when I made changes to his profile and clicking save.

A screenshot of a computer

Description automatically generated

Making changes to the editprofile.html and putting in the need values from the previous steps

A screenshot of a computer

Description automatically generated

Copying it to the docker

A black screen with text

Description automatically generated

Check the docker and make sure it was copy over right

A screenshot of a computer

Description automatically generated

Sending Alice a message to click on the link so I can add Samy is my hero to her profile

A screenshot of a computer

Description automatically generated

After clicking on the link in the message the profile got update to say “Samy is my hero.”

A screenshot of a computer

Description automatically generated

**Question 1**

Bob can check the GET request captured by HTTP Header Live to get the information to do the attack

**Question 2**

Bob can still launch the CSRF attack to modify the victim’s Elgg profile if the security tokens are predictable to guess and if they make the request easily to be authorized the profile modifications by doing brute force attack. Otherwise he cannot.

**TASK4**

Using the docksh to get elgg and find the Csrf.php file

A screen shot of a computer

Description automatically generated

Enabling the validation of the Secret token by commenting out the return for request

A screen shot of a computer

Description automatically generated

Clearing the description of Samy and removing him from friends

A screenshot of a computer

Description automatically generated

Trying to add Samy as a friend when clicking on the link, but is missing a token

A screenshot of a computer

Description automatically generated

Trying to add “Samy is my hero.” To her profile when clicking the link but it is going into a loop of missing token.

A screenshot of a computer

Description automatically generated

**TASK5**

**A screenshot of a computer

Description automatically generated**

Link A

**A screenshot of a computer

Description automatically generated**

GET A

**A screenshot of a computer

Description automatically generated**

Post A

**A screenshot of a computer

Description automatically generated**

**Link B**

**A screenshot of a computer

Description automatically generated**

Get B

**A screenshot of a computer

Description automatically generated**

Post B

**A screenshot of a computer error

Description automatically generated**

**Question1**

The reason why some cookies are not sent in certain scenarios is because all the Experiment A cookies are showing both requests which are coming from the same site

Experiment B GET Request has both normal and lax, but POST only was cookies because it is a cross-site.

**Question 2**

Same Site Cookies can help servers detect whether a request is a cross site or a same-site request by using defense to a CSRF to check the cookies to see if the cookie is accepted or not.

**Question 3**

How I would use Same Site cookie mechanism is to identify how first party cookies can be sent if quarry is the same as URL address if not, they don’t get sent.

**Lab Reflection**

In this Lab I was able to do a Cross-Site Request Forgery attack. It involves using a victim user, a trusted site and a malicious site to do the attack. To perform the attack, I had injected the malicious site to HTTP request for the use to click on to cause damage. The pen open-source social network application to do the attack on Elgg. To set up the Lab I had to use the docker to in the zip file to build and run to do the attack.

In Task1 I was able to observe the HTTP Request through HTTP Header Live. Then in Task2 I was able to add Samy to Alice friends without her permission. To do I use HTTP Header live to get the GUID when she login and put this request information in the image tag of the malicious webpage. Next sending a message to Alice to click on its website to automatic add Samy to friends.

Task3 adding “Samy is my hero.” in the profile description by the POST Request. To do this I had to use the HTTP Request POST when I was saving the edit profile description. Then put that information into the editprofile.html and send it to Alice to click on it to change her profile description. Finally, Task4 was turning on the defense by enabling the secret token validation by commenting on the return of Request function of Csrf.php causing all the attacks to fail. Also, in Task5 I was observing on how Experimenting with Same Site cookie are implemented