In-class practice 2

Graded

Student

HARRY KIM

Total Points

100 / 100 pts

Question 1

Submit your answers as a PDF file

100 / 100 pts

- ✔ **+ 20 pts** Successfully set up the VM
- ✔ **+ 20 pts** Successfully set up the first attack scenario
- ✔ **+ 20 pts** Successfully set up the second attack scenario
- ✔ **+ 20 pts** Successfully complete the first attack scenario
  - **+ 15 pts** Sufficient efforts are demonstrated to tackle the first attack but no successful results are presented
  - **+ 10 pts** Some efforts are demonstrated to tackle the first attack, but the efforts only make partial sense
- ✔ **+ 20 pts** Successfully complete the second attack scenario
  - **+ 15 pts** Sufficient efforts are demonstrated to tackle the second attack but no successful results are presented
  - **+ 10 pts** Some efforts are demonstrated to tackle the second attack, but the efforts only make partial sense

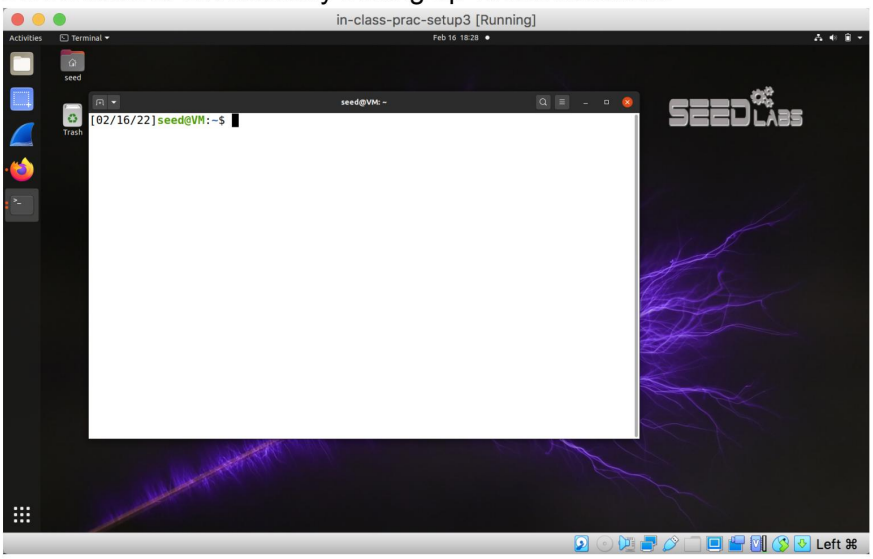
Question assigned to the following page: 1

Sevin Park
Harry Kim

Making it clear: **Sevin Park and Harry Kim worked together on this practice.**

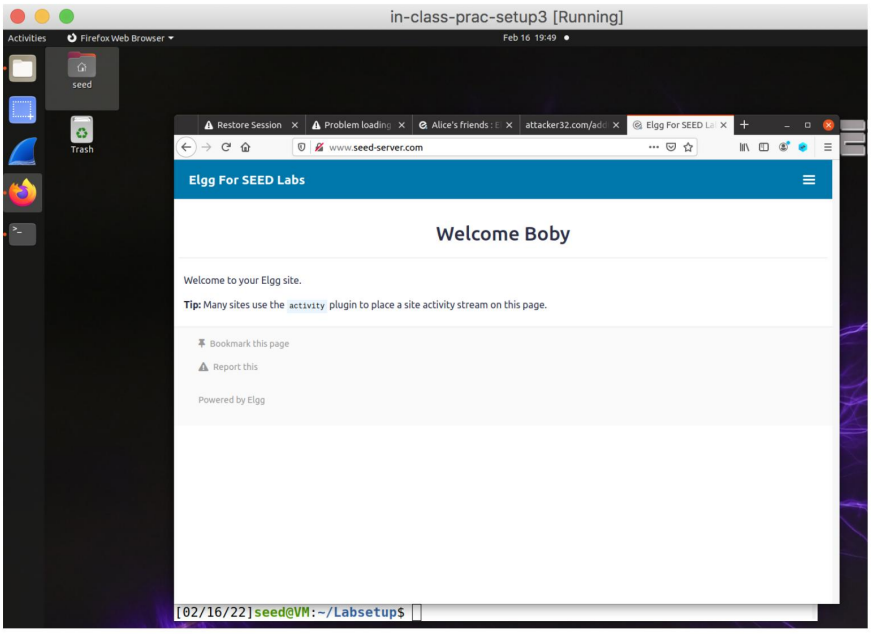
In-class practice 2

Screenshot of successfully setting up virtual machine:



<u>Discover XSS vulnerabilities</u>

Task 1: Display an Alert Window when visiting a user's profile

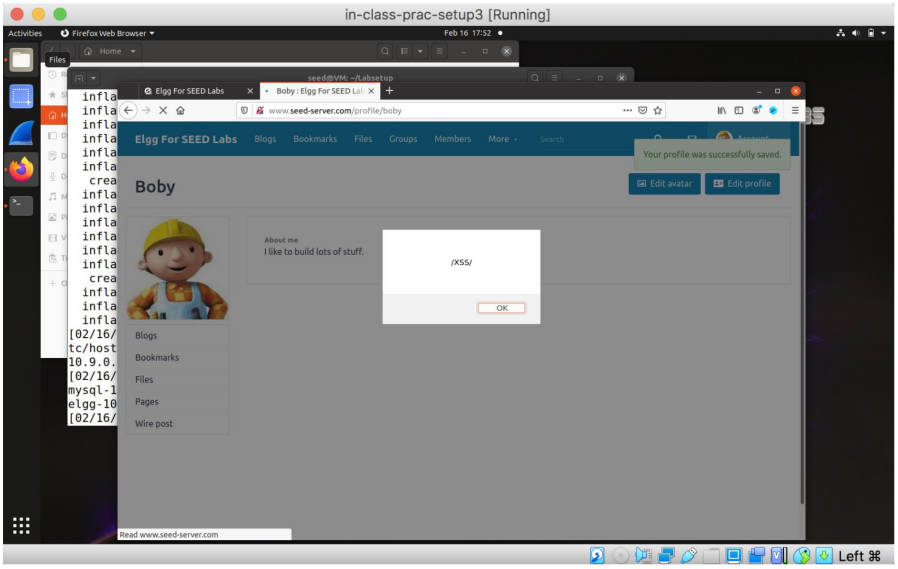


Question assigned to the following page: 1

Sevin Park
Harry Kim

Added the following to edit html of Bob's profile:

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



Question assigned to the following page: 1

Sevin Park
Harry Kim

Discover CSRF vulnerabilities

Task 1: CSRF Attack using GET Request

Successfully set up web security environment with commands:

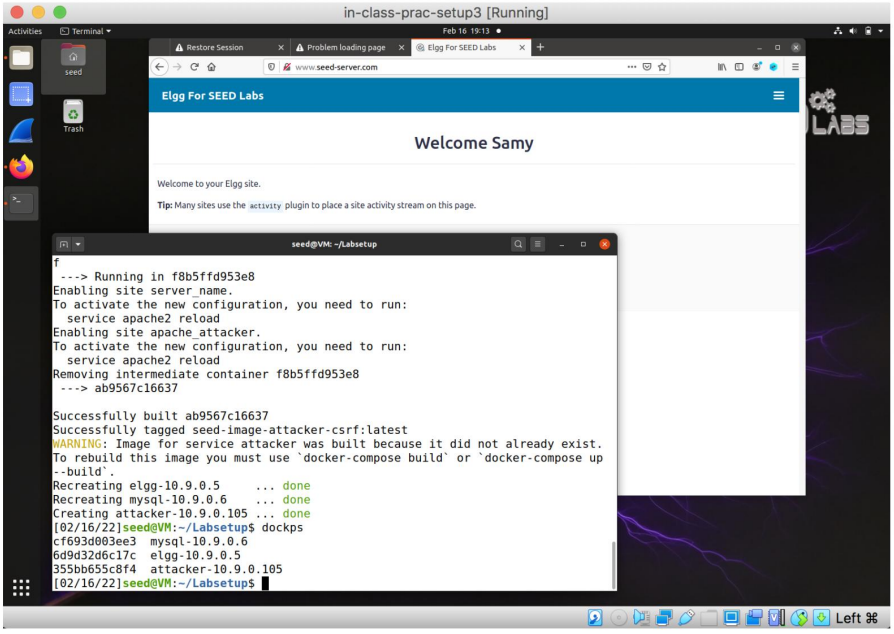
```
[02/16/22]seed@VM:~/Labsetup$ echo 10.9.0.5 www.seed-server.com | sudo tee -a /e
tc/hosts
10.9.0.5 www.seed-server.com
[02/16/22]seed@VM:~/Labsetup$ echo 10.9.0.105 www.attacker32.com | sudo tee -a /
etc/hosts
10.9.0.105 www.attacker32.com
[02/16/22]seed@VM:~/Labsetup$ docker-compose up -d
```

```
[02/16/22]seed@VM:~/Labsetup$ dockps
cf693d003ee3  mysql-10.9.0.6
6d9d32d6c17c  elgg-10.9.0.5
355bb655c8f4  attacker-10.9.0.105
[02/16/22]seed@VM:~/Labsetup$ sudo nano /etc/hosts
```

The command “sudo nano /etc/hosts” is for going into the file and checking if the IP address of the attacker website is correct. We verified that it’s 10.9.0.105.

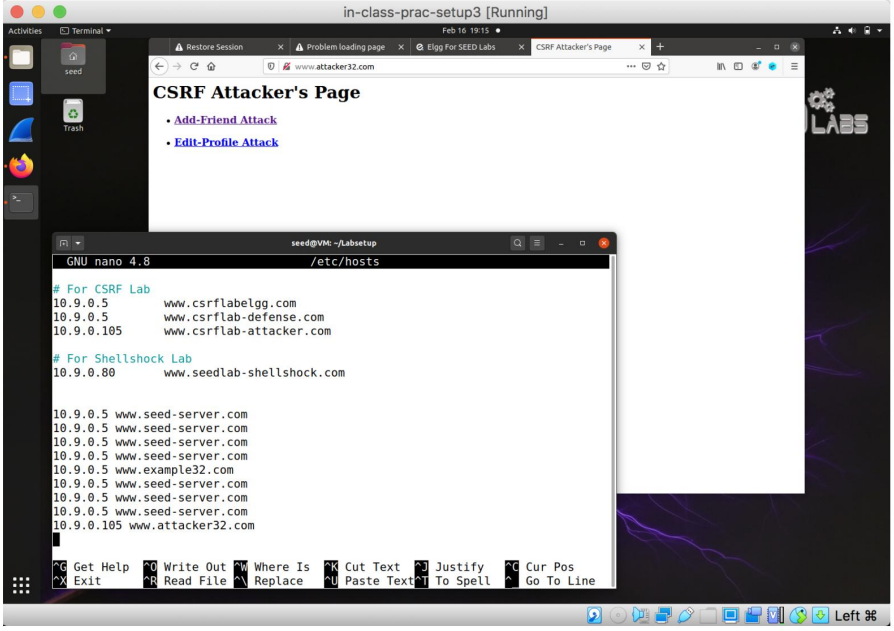
Then these next commands were used to edit the addfriend.html file so that once Alice clicks on the link, Samy is immediately added as Alice’s friend.

```
[02/16/22]seed@VM:~/Labsetup$ docksh 355bb655c8f4
root@355bb655c8f4:/# cd /var/www/attacker/
root@355bb655c8f4:/var/www/attacker# nano addfriend.html
```



Question assigned to the following page: 1

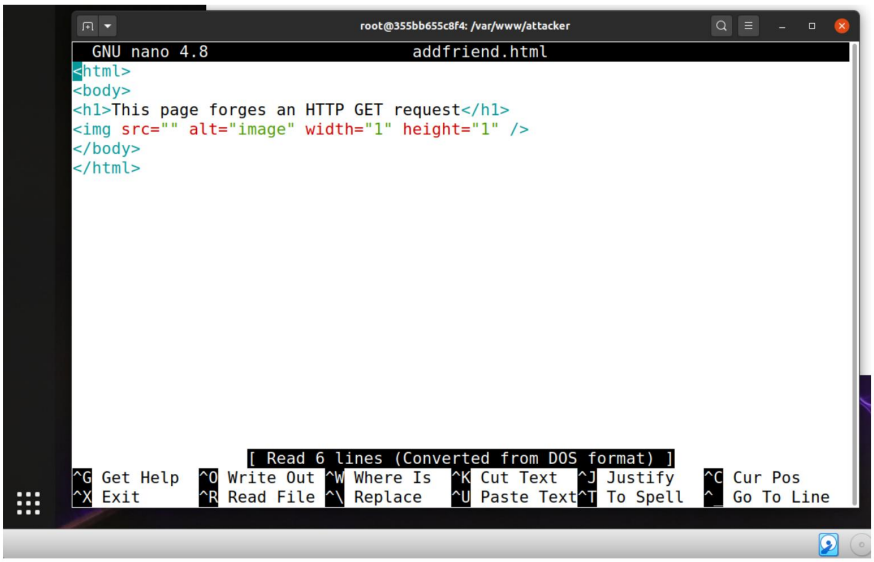
Sevin Park
Harry Kim



Question assigned to the following page: 1

Sevin Park
Harry Kim

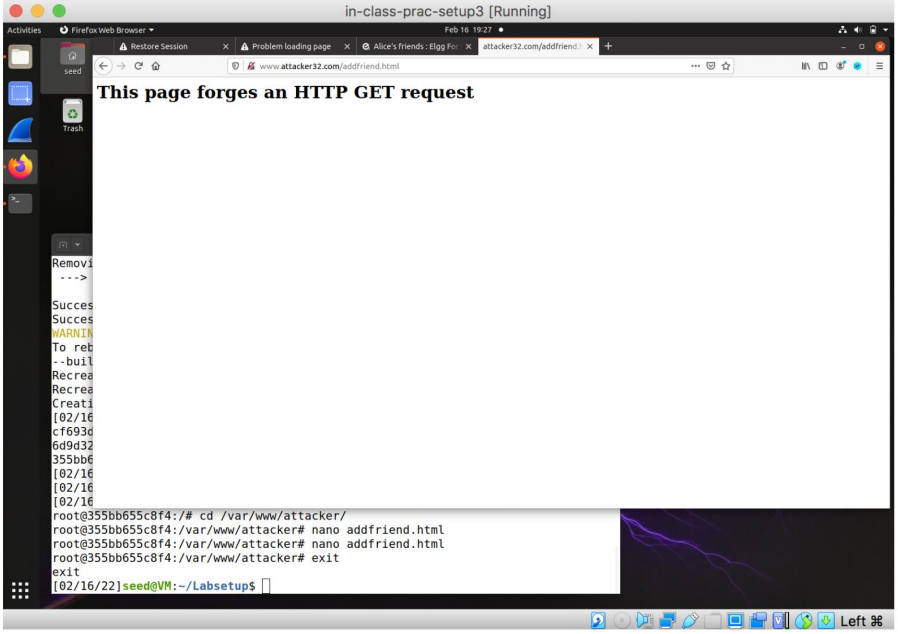
Before:

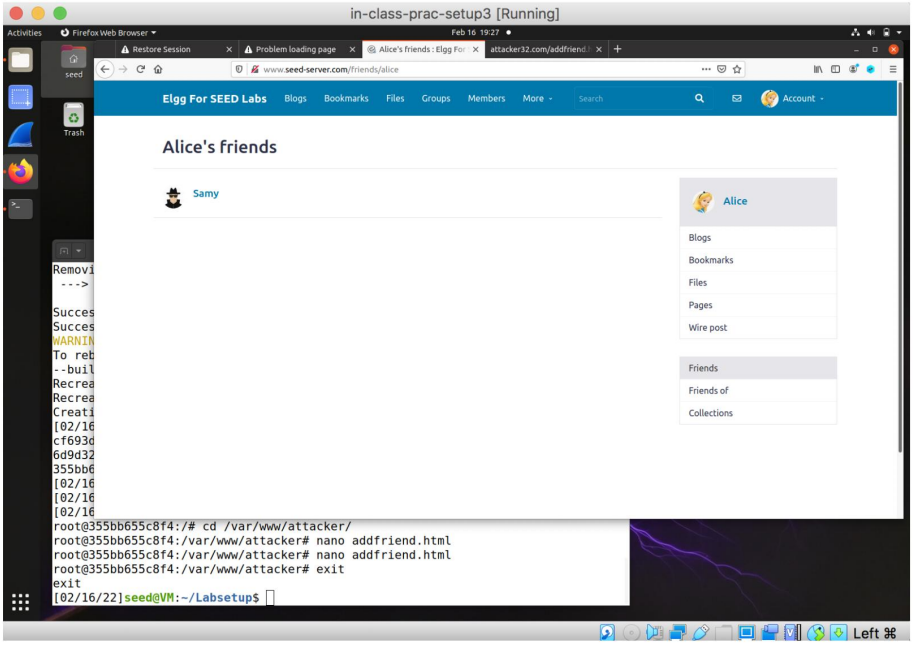


After:

Question assigned to the following page: 1

Sevin Park
Harry Kim





Question assigned to the following page: 1

Sevin Park
Harry Kim

The vulnerabilities we found and how we exploited those vulnerabilities:

For XSS task 1:

The vulnerability was how we were able to edit html code when we choose to edit the profile.

We exploited it by using javascript code to make an alert pop up.

For CSRF task 1:

Inside Alice's account, we inspected the element that allowed Alice to add friends. There was a link that enabled Alice to add a friend, so that link was the vulnerability.

To exploit that vulnerability, we copied that link and pasted it into our addfriend.html file so that once Alice clicks on our link, Samy is immediately added as Alice's friend.