# Lab 4 Web Security

Donghang He

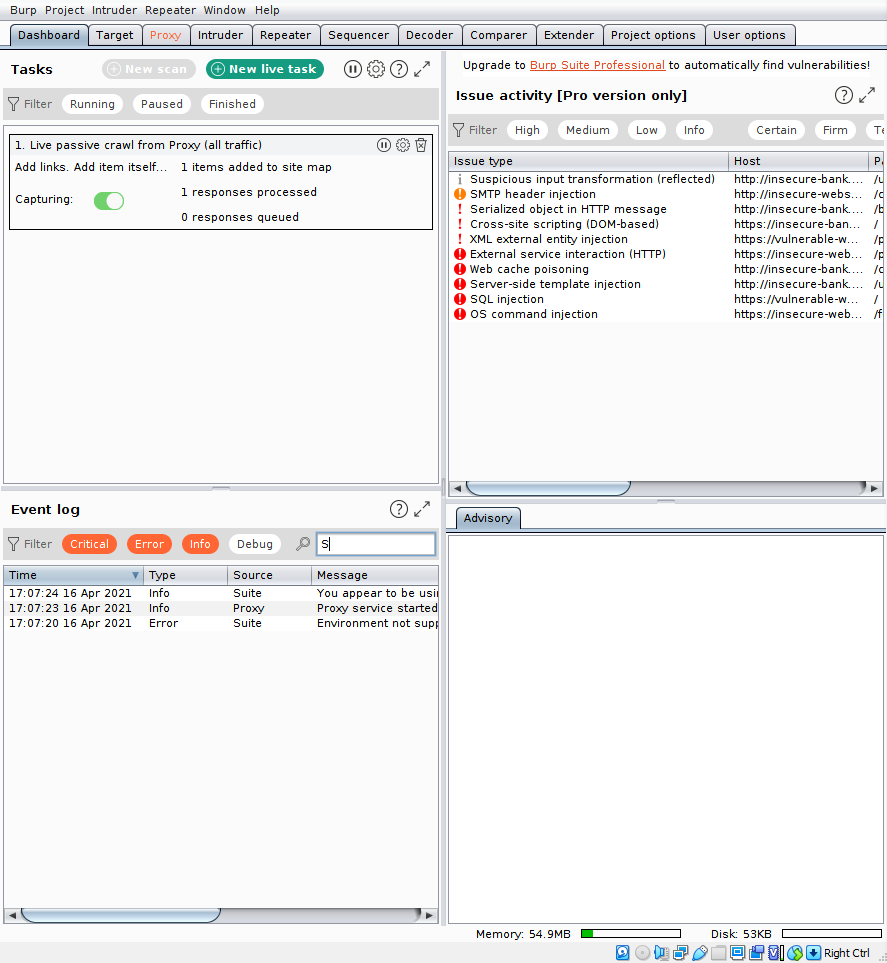
## Download and set up Burp suite

1. Download



1. Set up

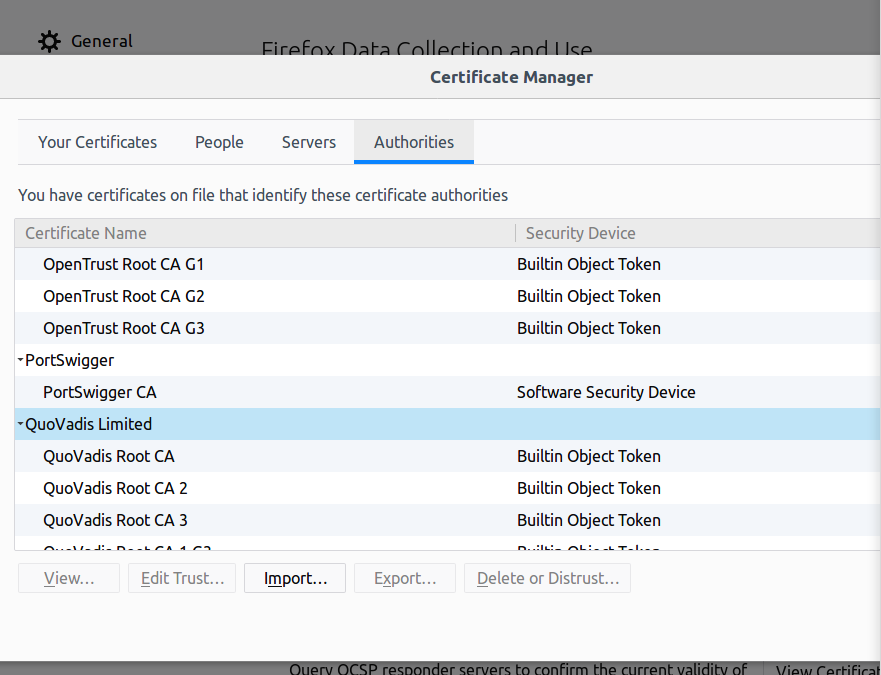
Start the burp suite.



Set the proxy configuration of the browser.



Add the certificate to the browser.



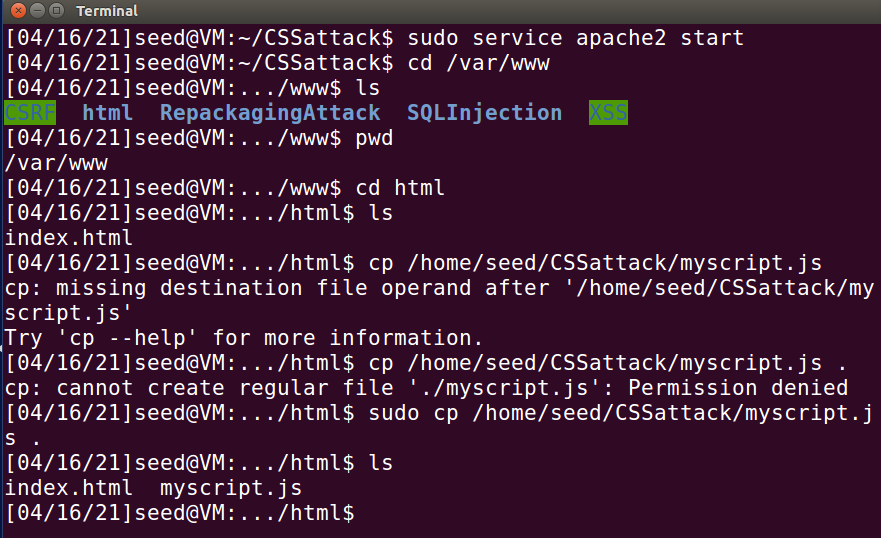
## Lab tasks

### Task 1: Posting a malicious message to display an alert window

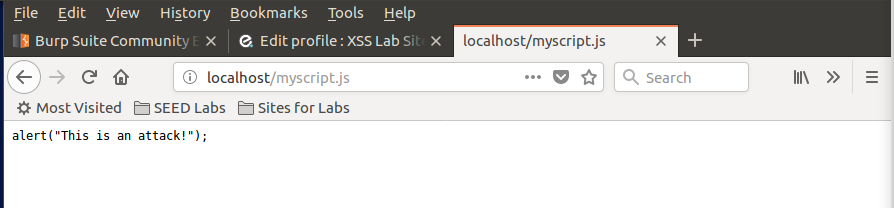
The code we need to add in the profile.



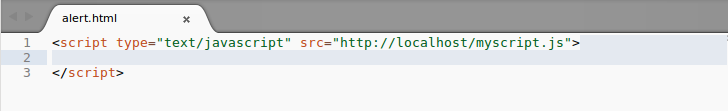
Move the file to the apache server folder.



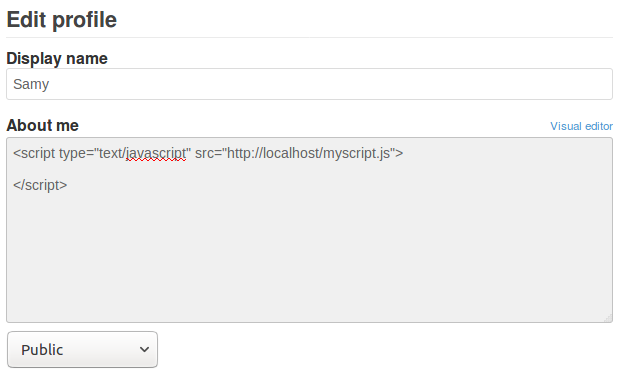
Check it in the browser.



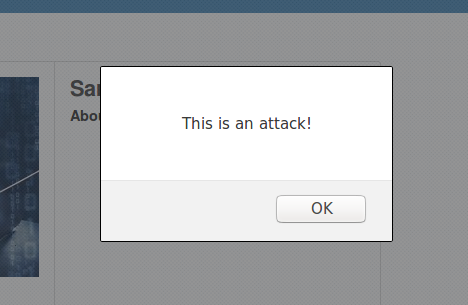
The HTML code.



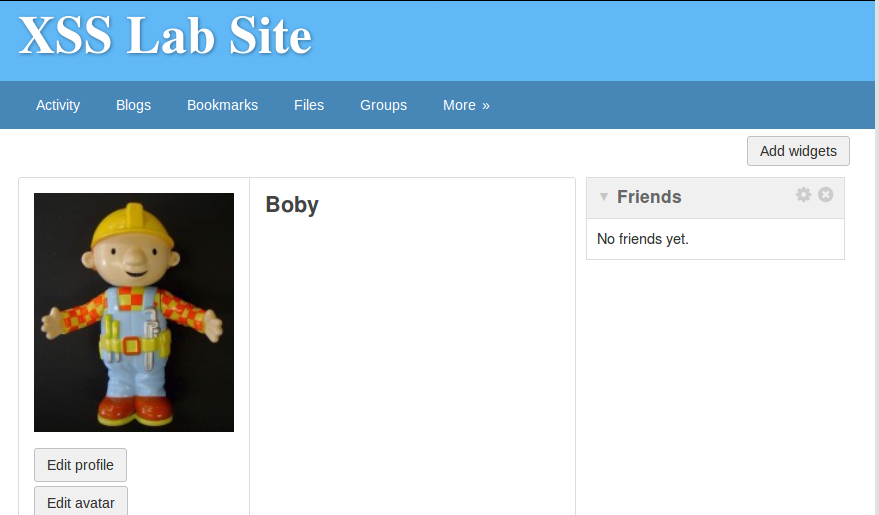
Put the code in the profile.



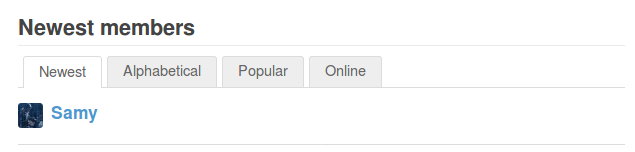
Click save and the alert shown on the page.



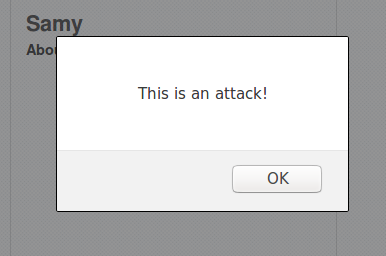
Login in to Boby’s account.



Check samy’s profile.

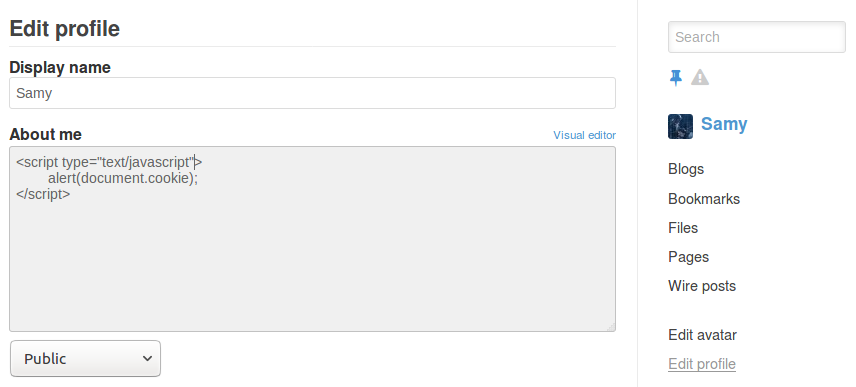


The alert shown on the page. Attack success.

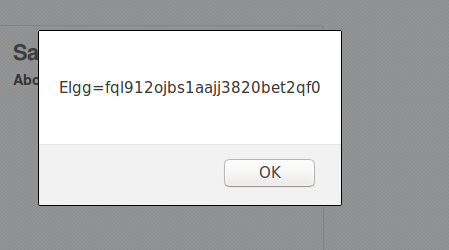


### Task 2: Posting a malicious message to display cookies

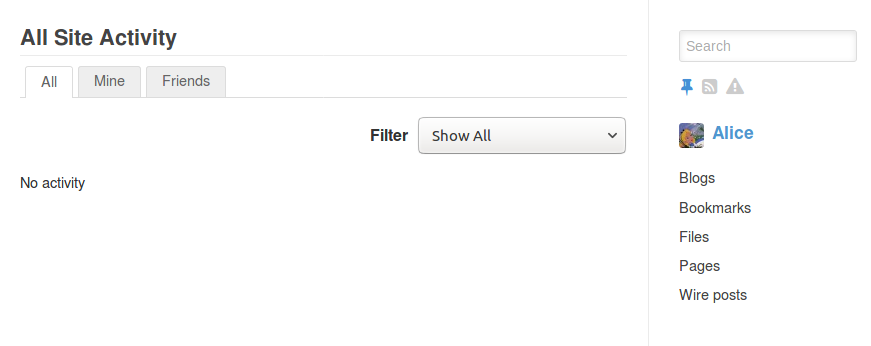
Put the code in samy’s profile.



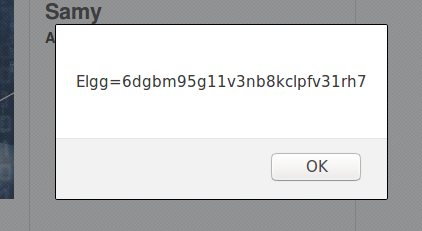
Click save and the alert shown with the cookie.



Login in to alice’s account.

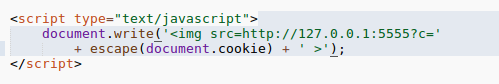


Check samy’s profile the alert shown on the page. Attack success.

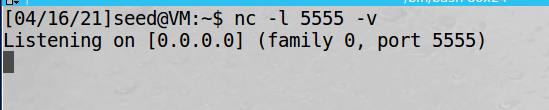


### Task 3: Stealing cookies from the victim’s machine

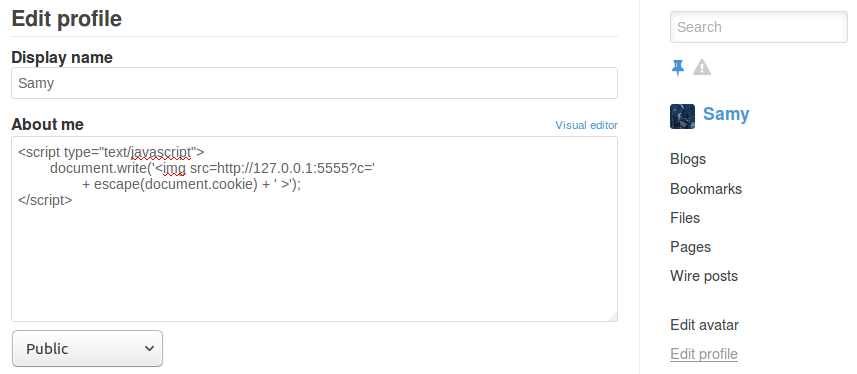
Stealing code.



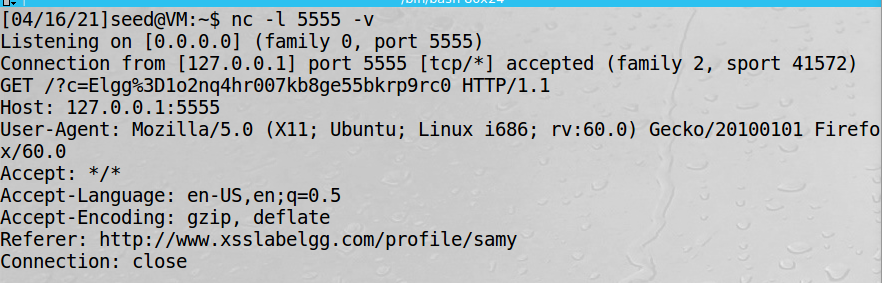
Launch the listener of the port 5555.



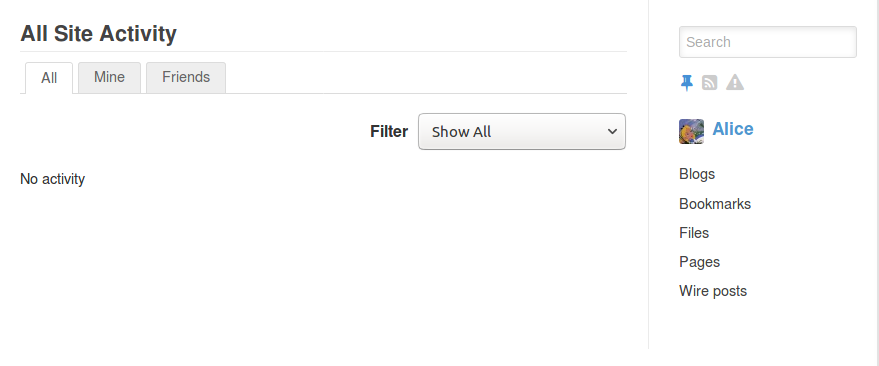
Put the code in samy’s profile.



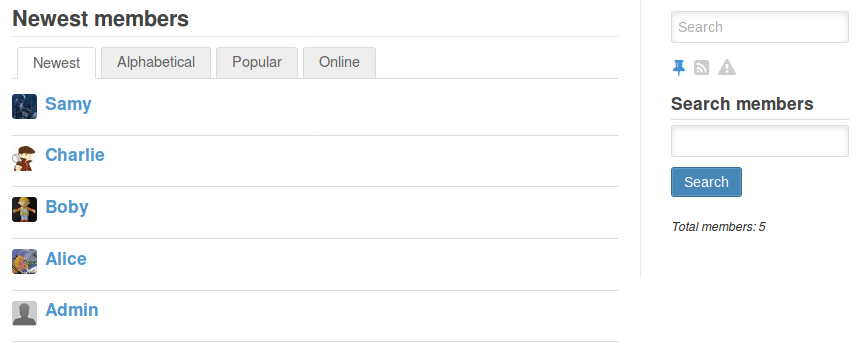
Save and check the listener. Shown the token in the terminal.



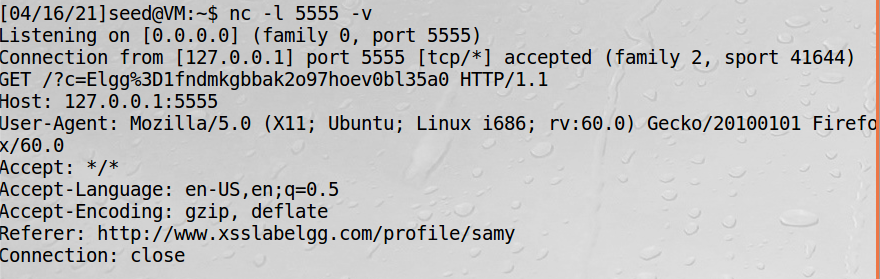
Login to alice’s account



Check samy’s profile.



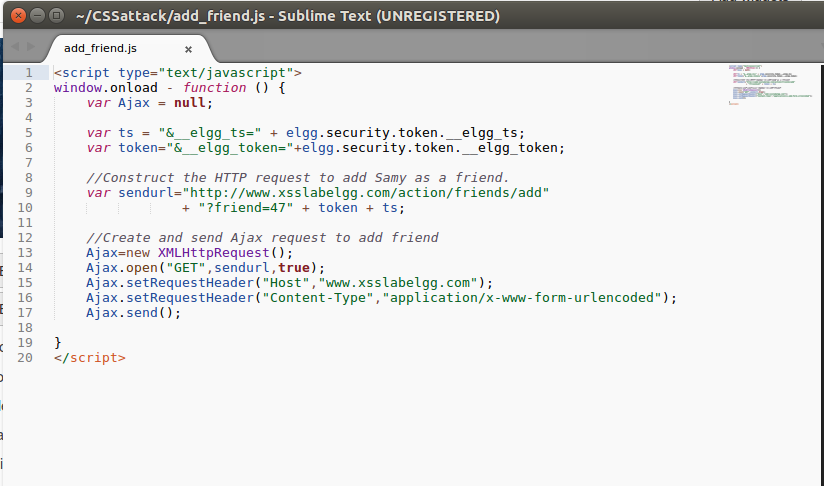
Get the token of Alice. Attack success



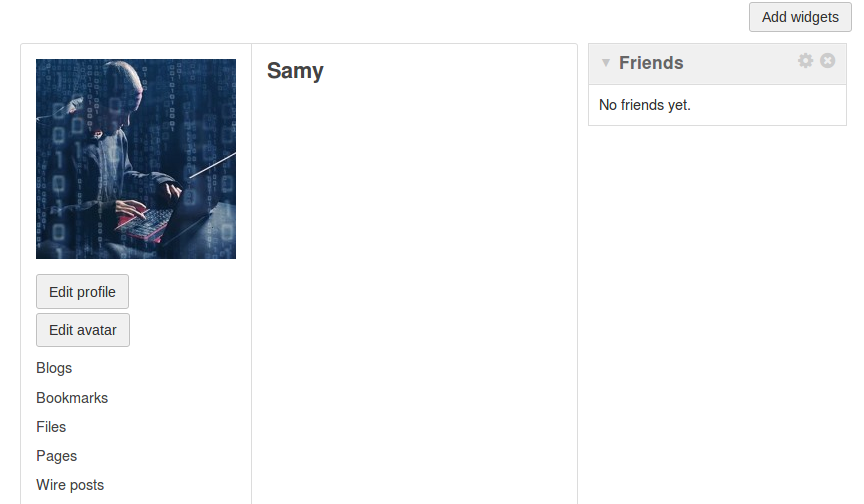
### Task 4: Becoming the victim’s friend

Code for add friend. And the URL could get from the Burp suite by adding friend in the website.

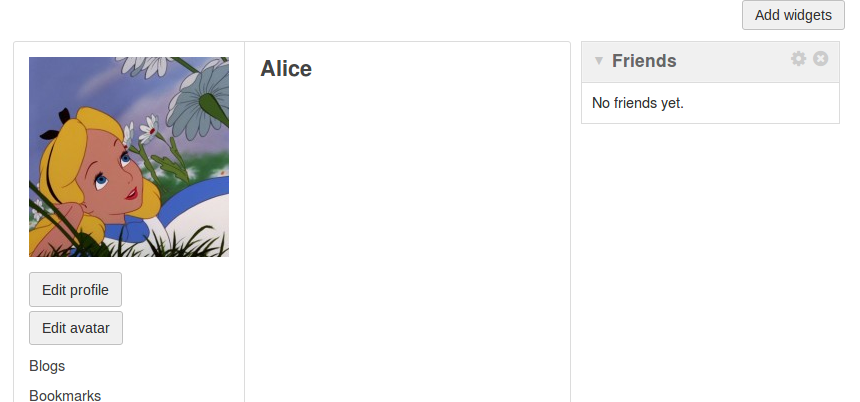




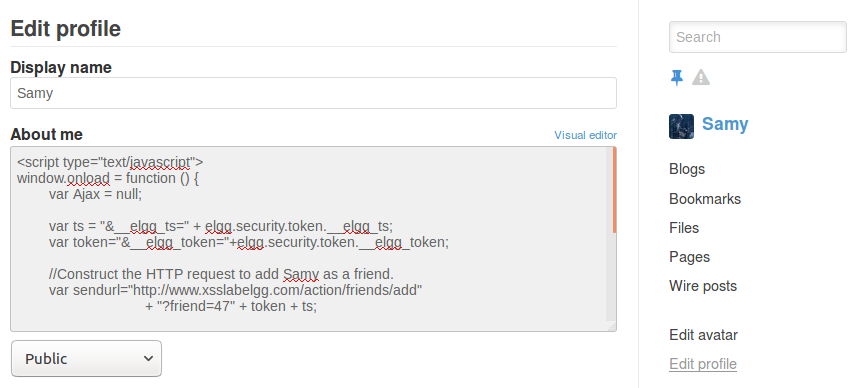
Samy hasn’t any friends.



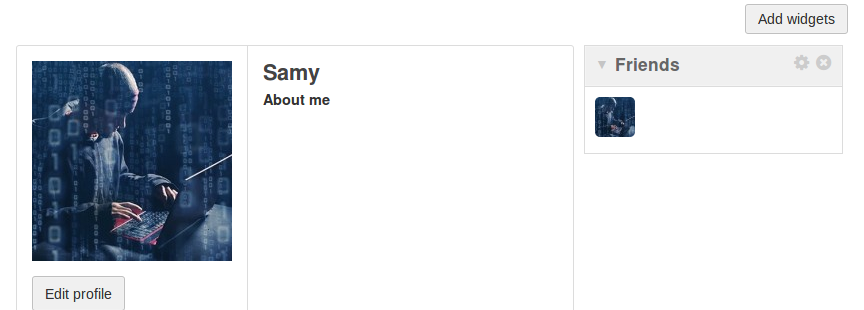
Alice hasn’t any friends.



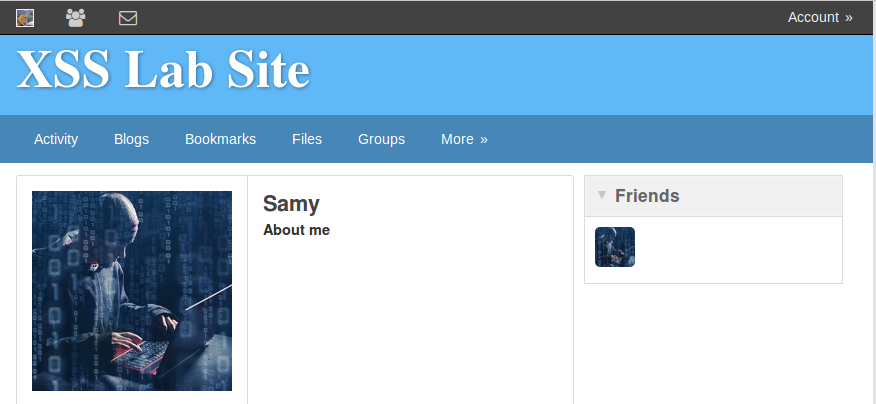
Put the code in samy’s profile.



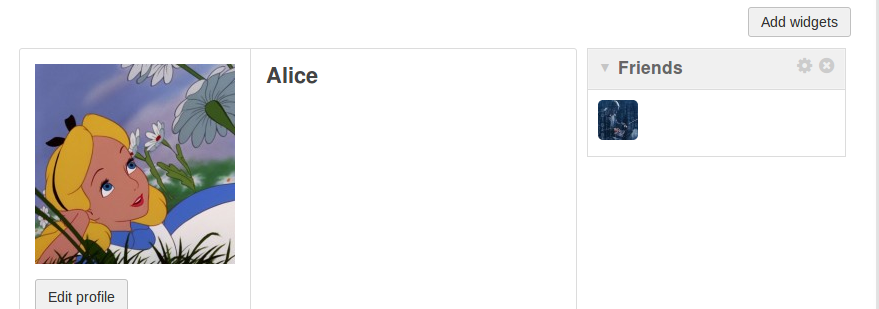
Save and refresh the page, you can see Samy and himself as a friend. Attack success for himself.



Login to Alice’s account and visit Samy’profile.

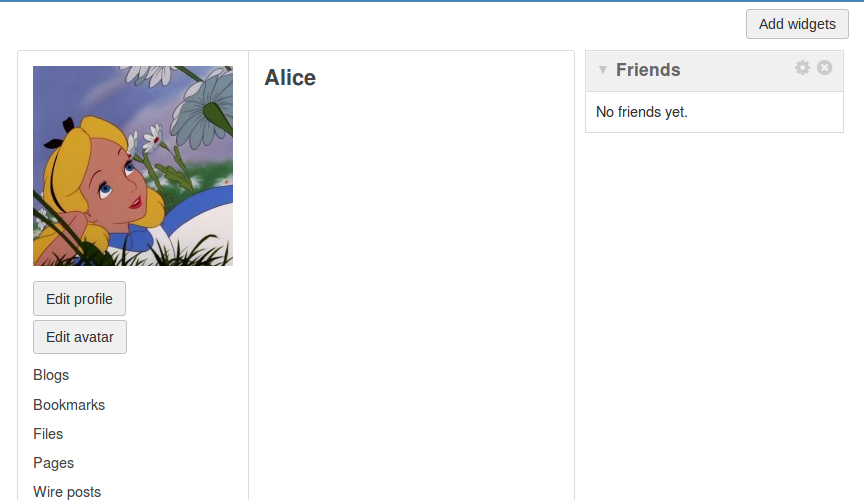


Back to Alice’s profile you can see Samy becomes to Alice’s friend. Attack success.



Question 1: line 1 and 2 are using for getting the timestamp and token to attack the website.

Question 2: of cause the attack will failed. If the code copy to the text mode. It will become to the normal text not the JS code.

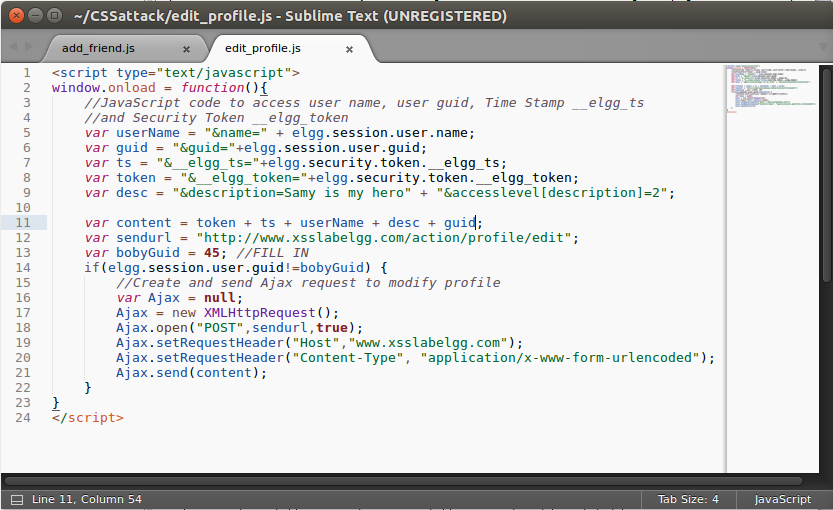


### Task 5: Modifying the victim’s profile

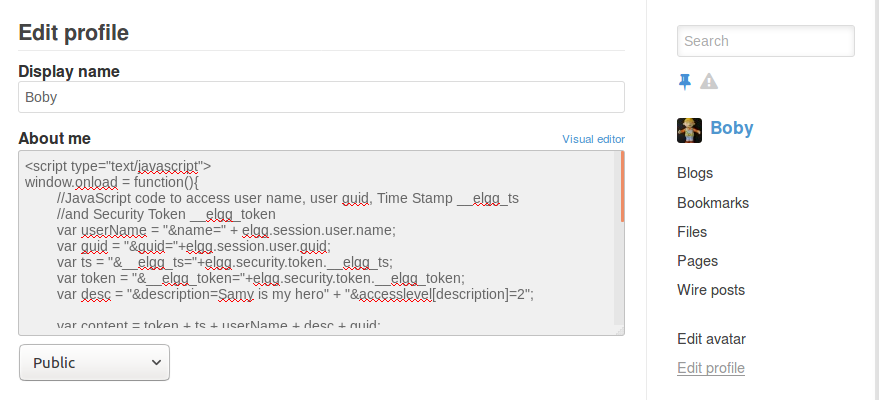
Use Boby as the attacker. We need to check his guid. You could find it in the source code of him profile page.

Also we can find what paramaters we need to edit the profile in the Burp Suite. And make it together become the content. Also the URL could find in the Burp Suite.

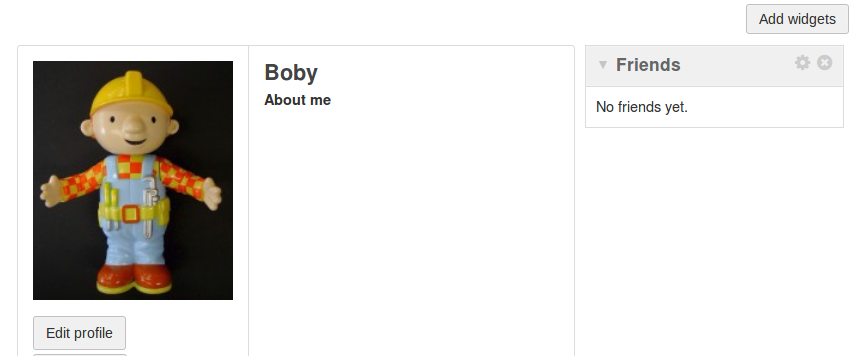
Code for edit the profile.



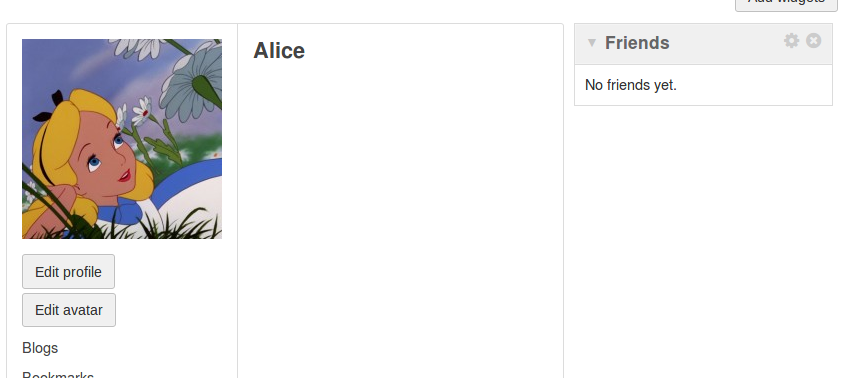
Save the code to ‘about me’.



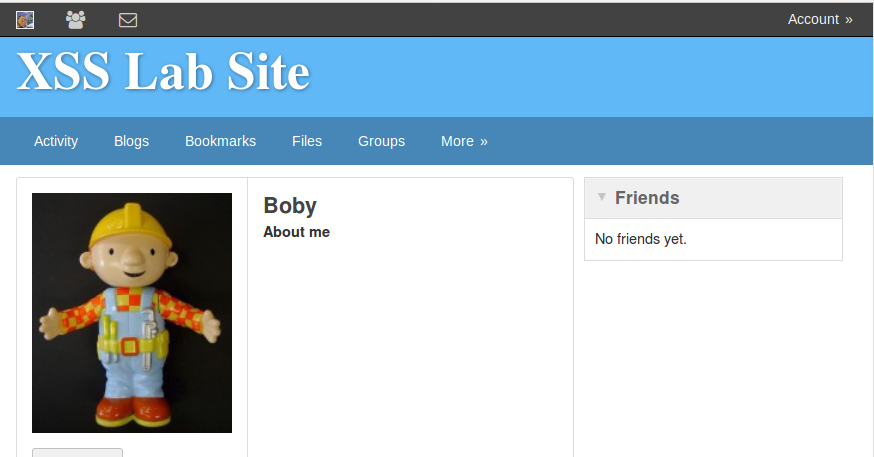
Check Boby’s profile found not attack himself.



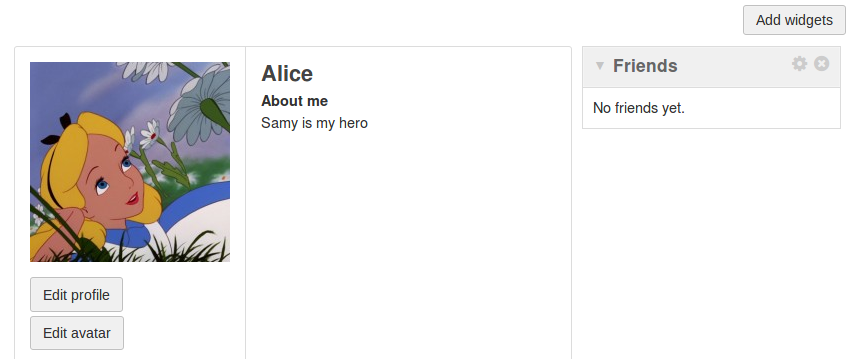
Login in to Alice’s account.



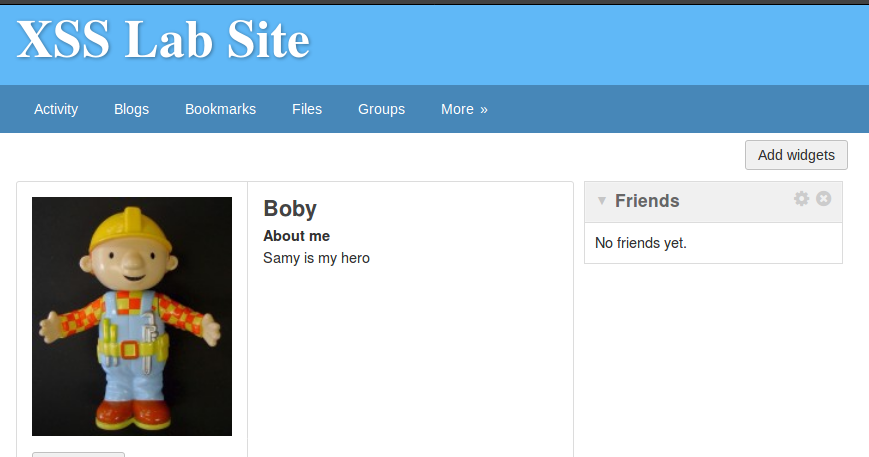
Visit Boby’s profile.



Back to Alice’s profile found the ‘about me’ has been changed. Attack success.

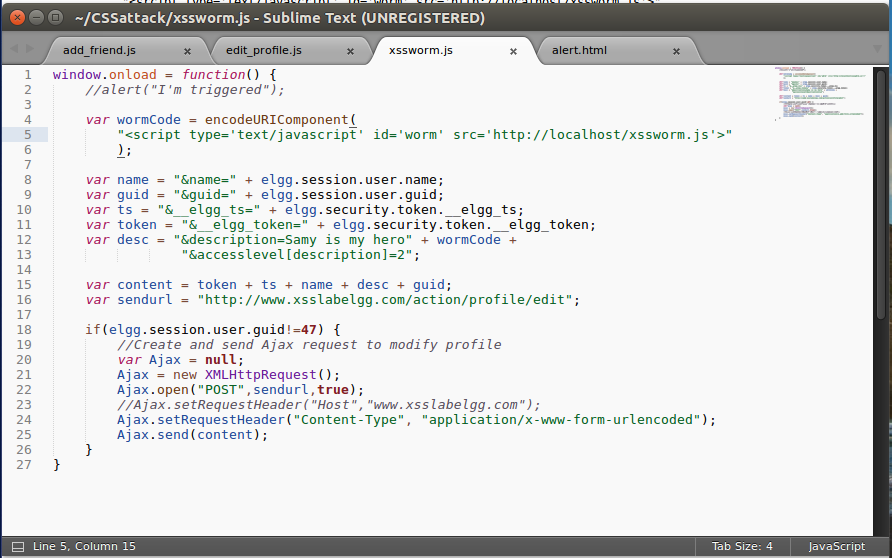


Question 3: this line is for not attack himself. Answer of remove this line. Boby himself will be attack. Also everyone visit him profile will be attacked.

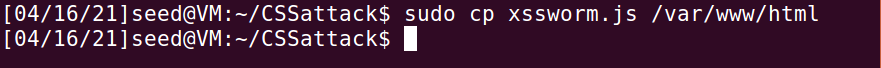


### Task 6: Writing a self-propagating XSS worm

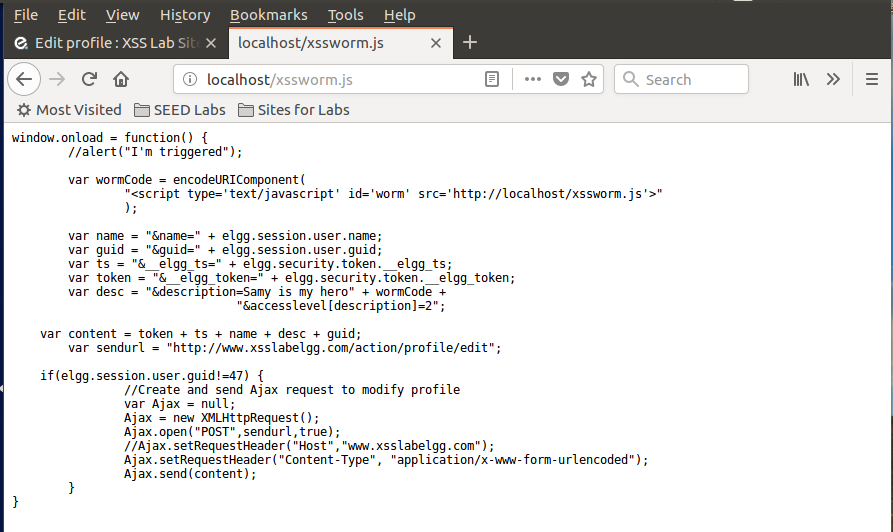
This is the worm I used in this task to modify the profile and copy the worm to it.



Also copy to apache folder.



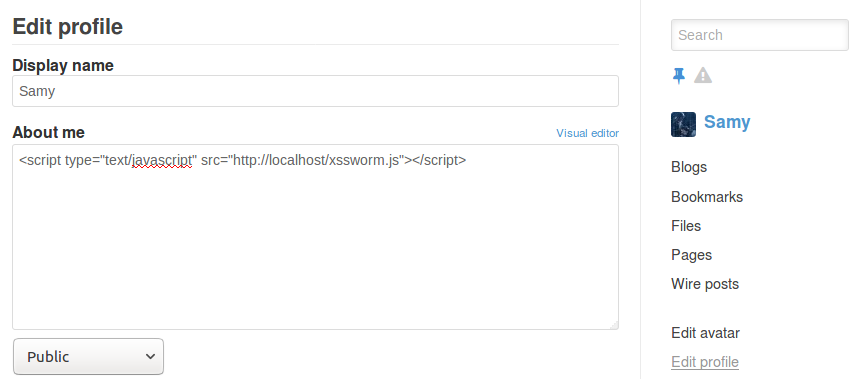
Run it in browser.



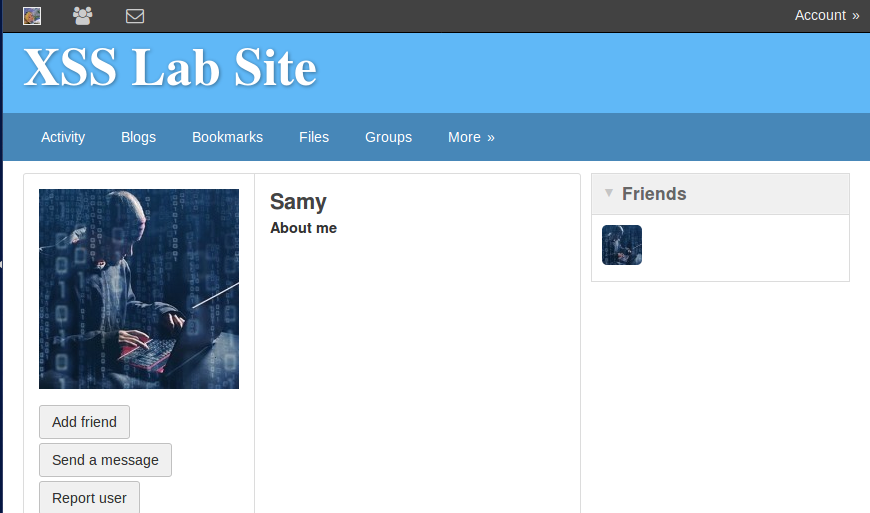
The code set in profile



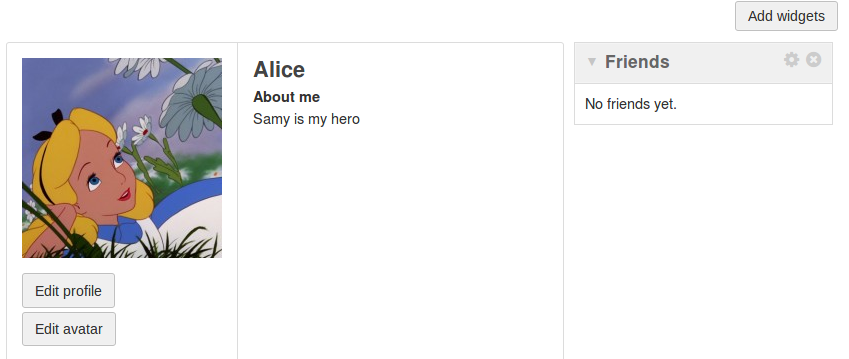
Save it in profile.



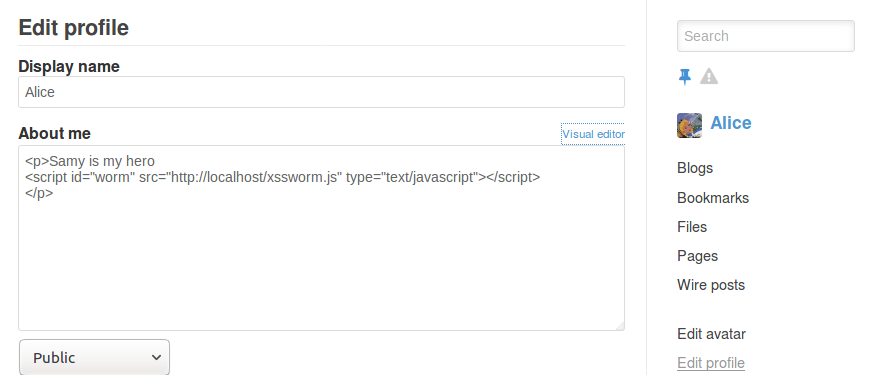
Login to Alice’s account and visit Samy’s profile.

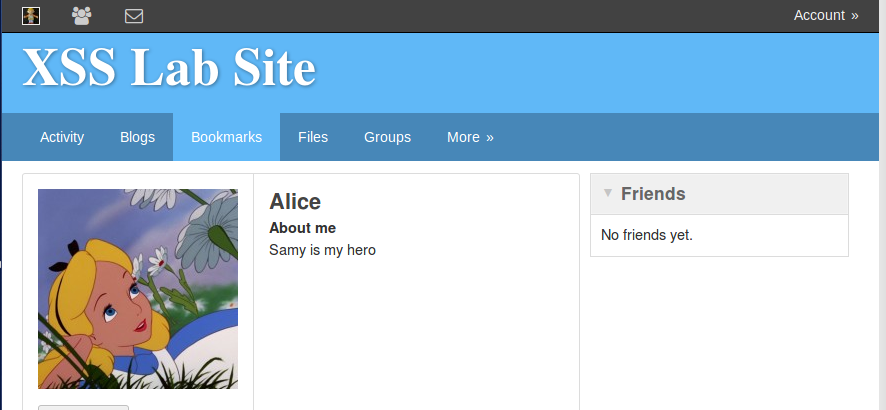


Alice’s profile has been modified. Attack success.

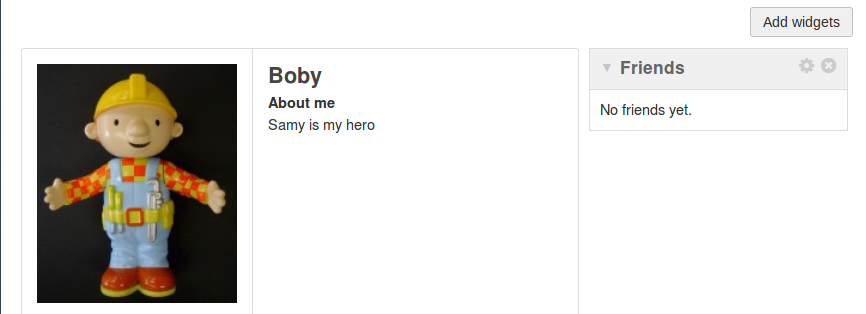


Also the worm has been copied to Alice’s profile.

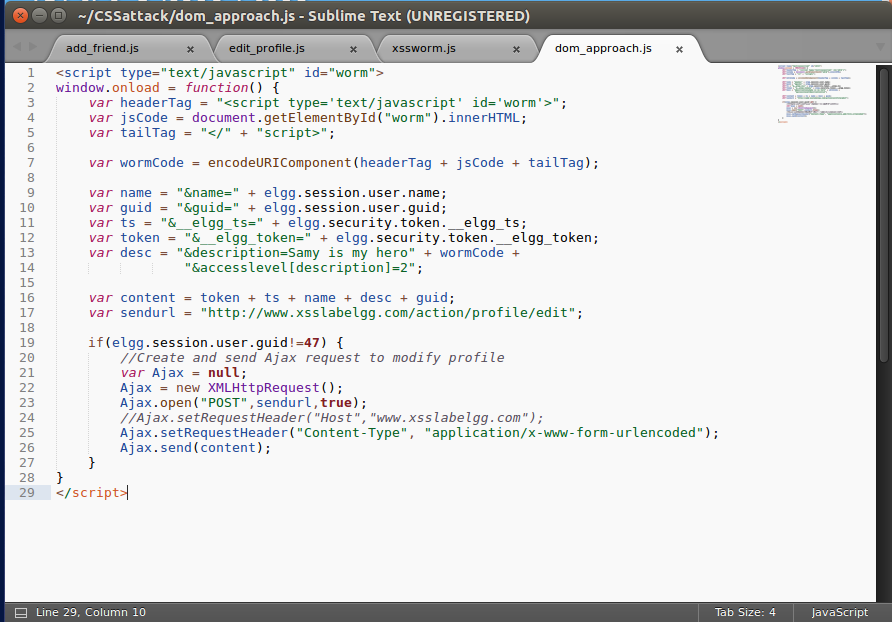


Login in to Boby’s account and visit Alice’s profile.  


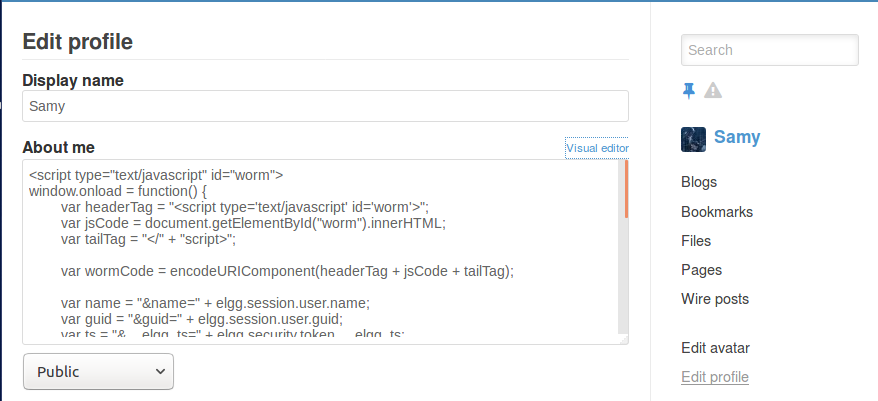
Boby’s profile has been change. Attack success.



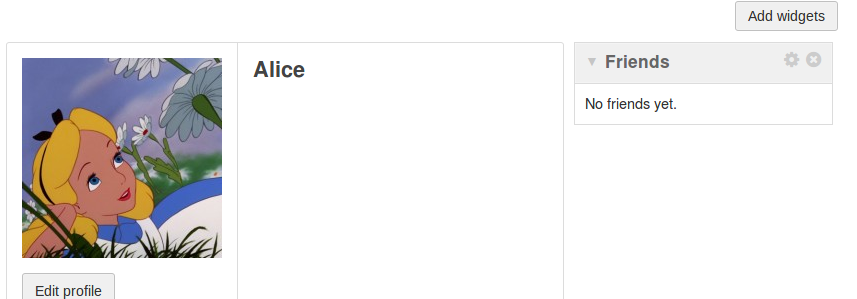
DOM approach code.



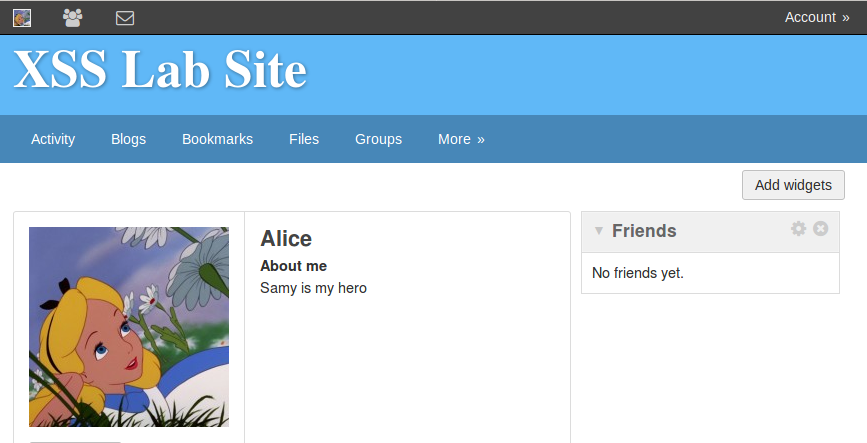
Save the code to Samy’s profile.



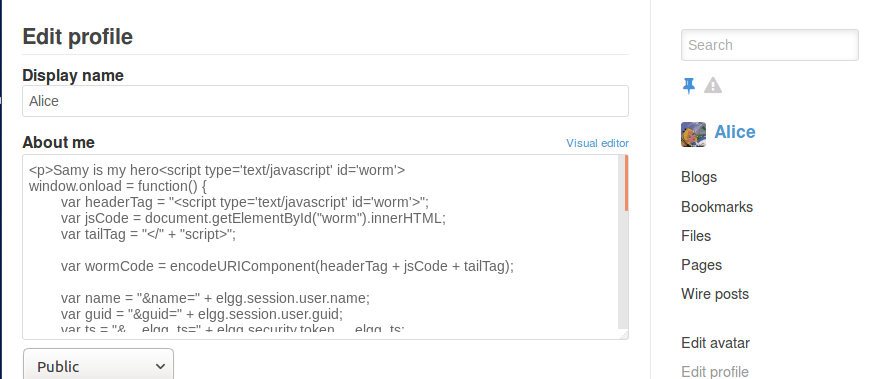
Check Alice’s profile its empty.



After visit Samy’s profile it changed. Attack success.



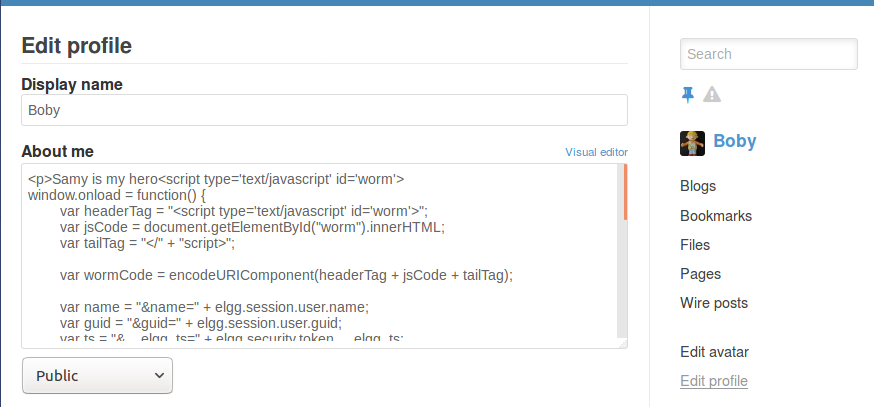
Also the DOM worm has been copied to Alice’s profile.



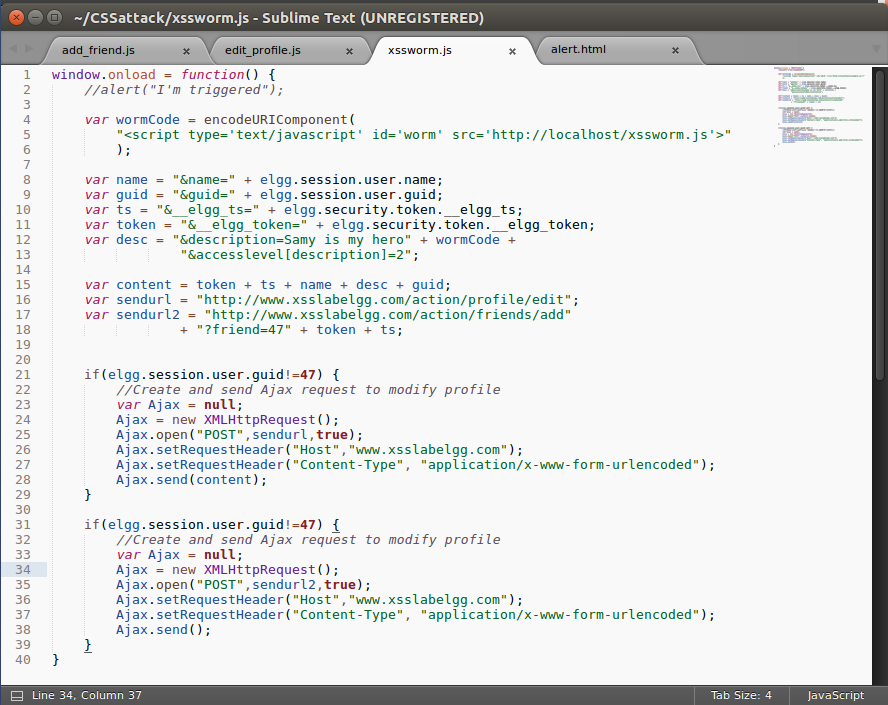
Login to Boby’s account and the profile is empty.



After visit Alice’s profile the profile changed. Attack success.

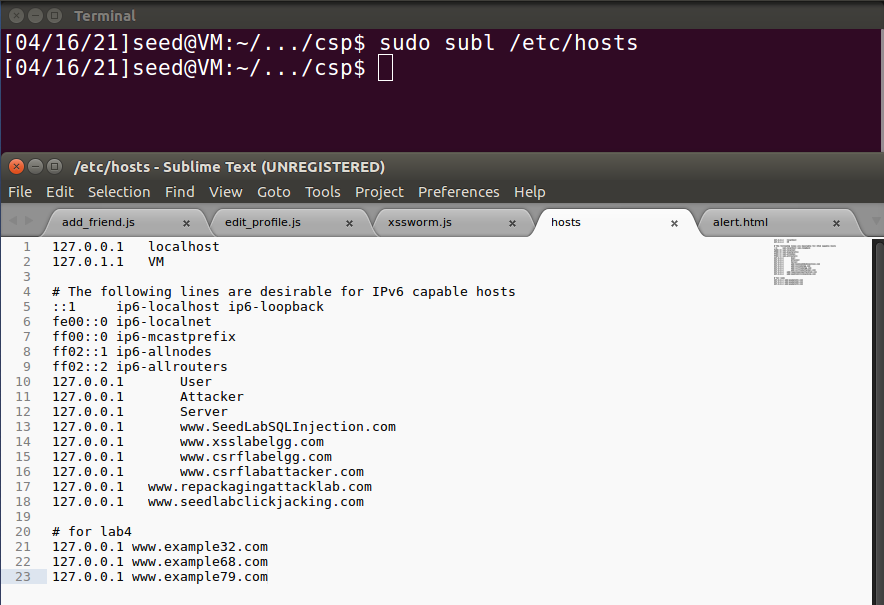


I forgot to add Samy to the visitor’s friend. So, I change the code of the worm. Others are same so I didn’t do the screen shot again.

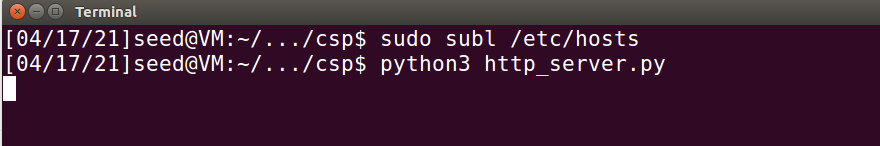


### Task 7: Defeating XSS attacks using CSP

Set up the DNS entry.



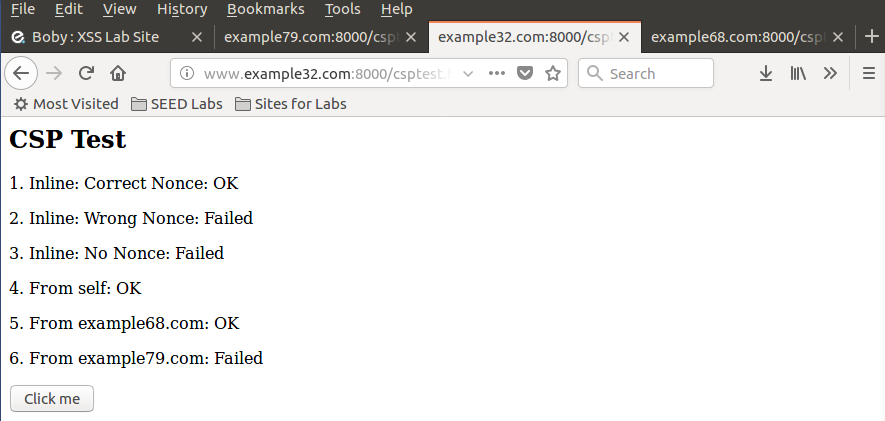
Run a web server.

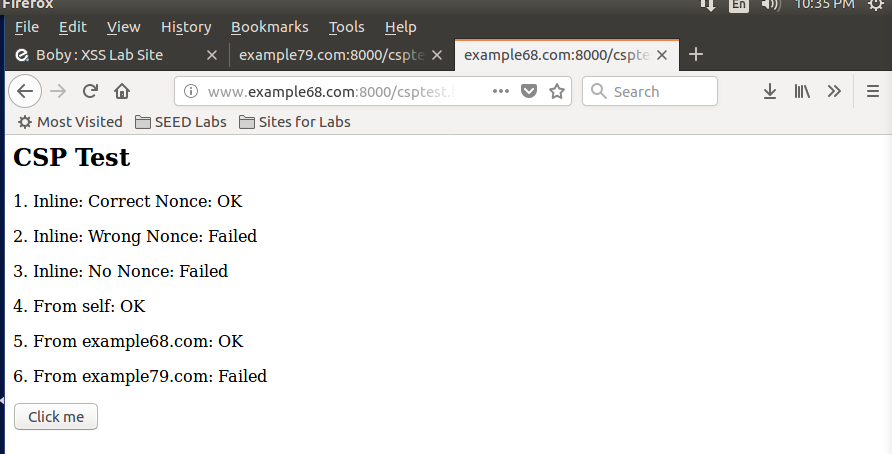


Visit URLs

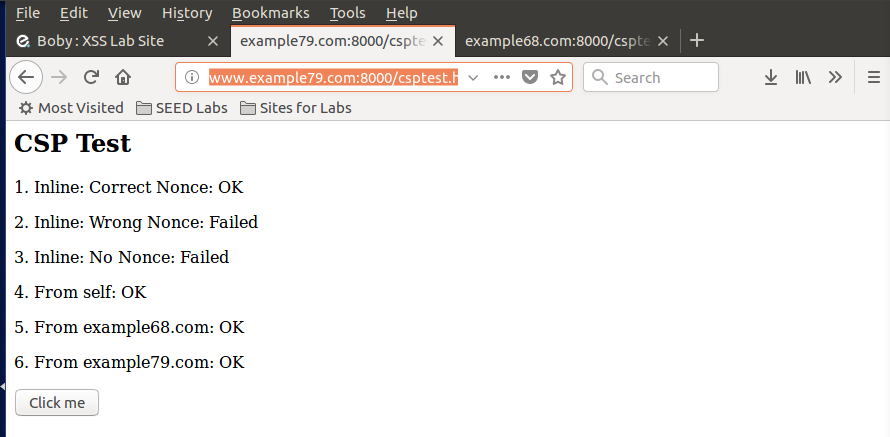
For the 1-6:

1. In the python code the CSP ‘script-src’ set nonce=1rA2345.
2. In the python code the CSP ‘script-src’ didn’t set nonce=2rB3333.
3. There is nonce set in the CSP ‘script-src’ so it’s Failed.
4. Script from itself is OK
5. Example68.com:8000 also set in the CSP ‘script-src’ so it’s OK
6. Example79.com:8000 not set in the CSP so it’s Failed.

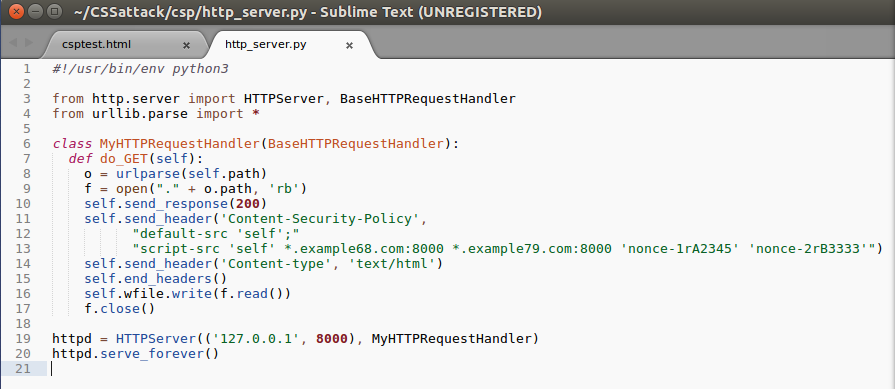




In this URL the No. 6 is OK because the URL is example79.com.



So, if you want to make Fields 1, 2, 4, 5 and 6 all display OK. The code is



## Summary

The purpose of the lab is to learn the XSS attack. And I learn how to implement this attack and achieve all tasks in this lab. The lab is ok not too hard and its clear. There isn’t any problem if you use windows OS.