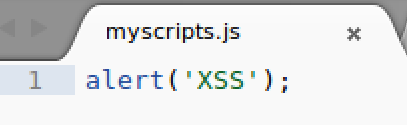
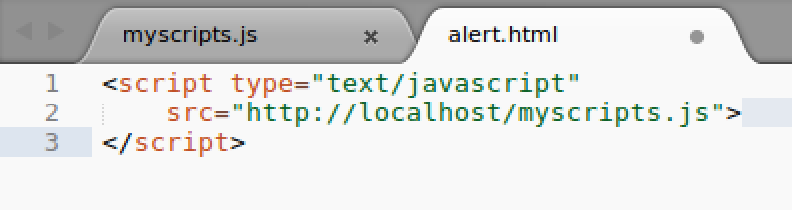
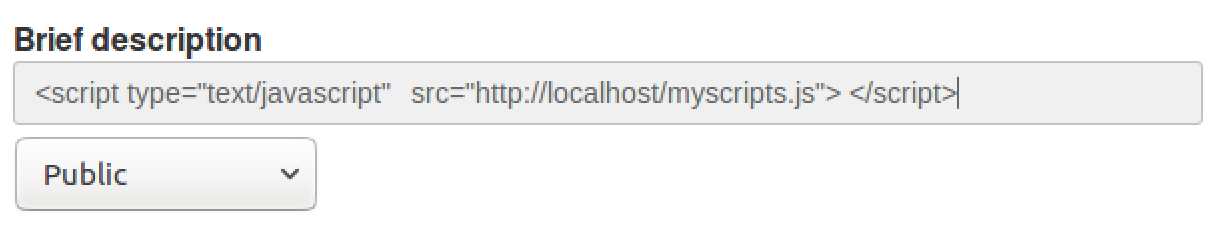
Lab 6

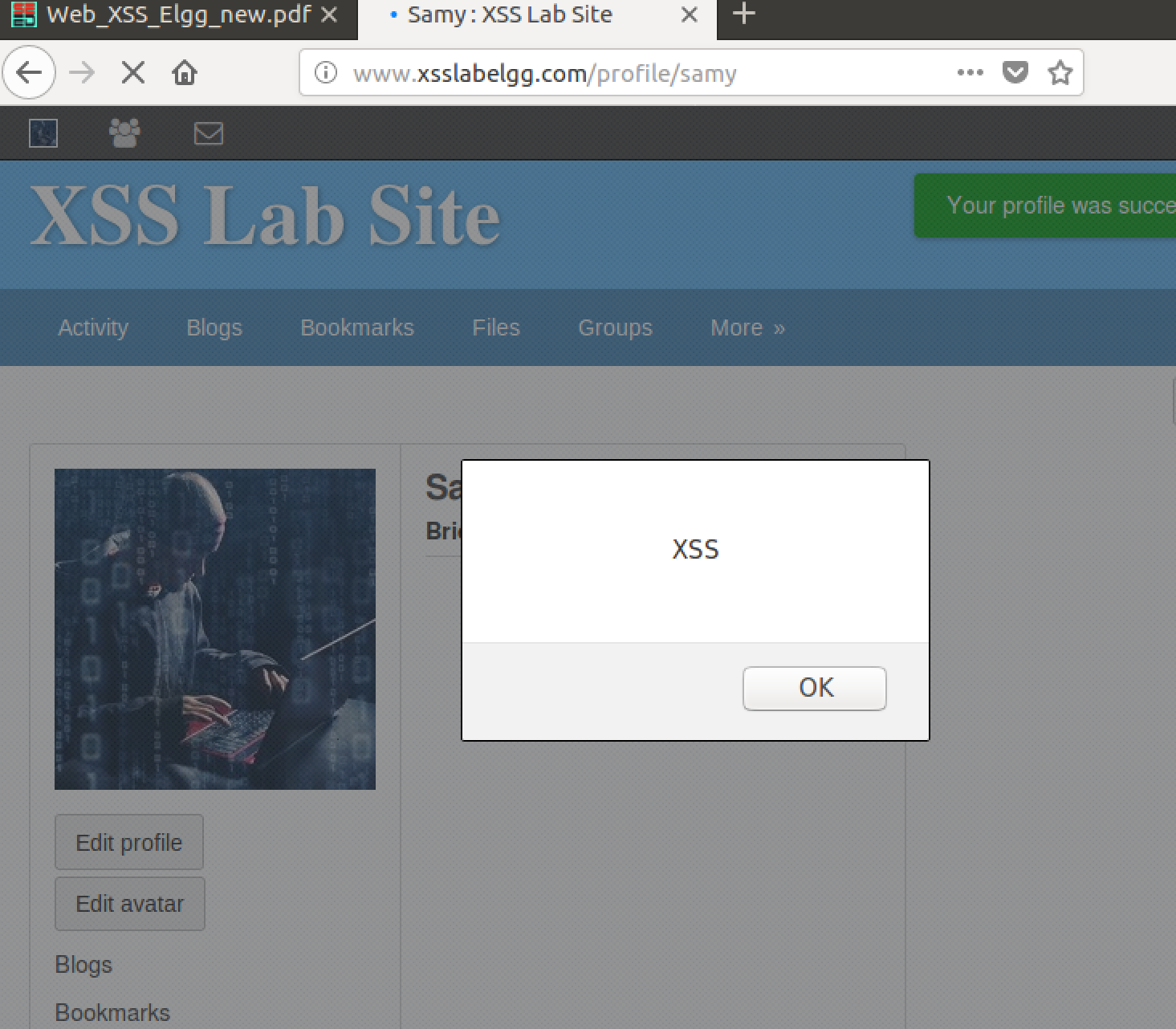
Task 1: Posting a Malicious Message to Display an Alert Window

Code Used:

Commands/Steps Used and Results:





Comments:

I created a myscripts.js file with the alert. I put it into the brief description and when I went back to the profile page of samy it showed me the alert. This is due to the fact that the script is set to run when the person is on his profile main page.

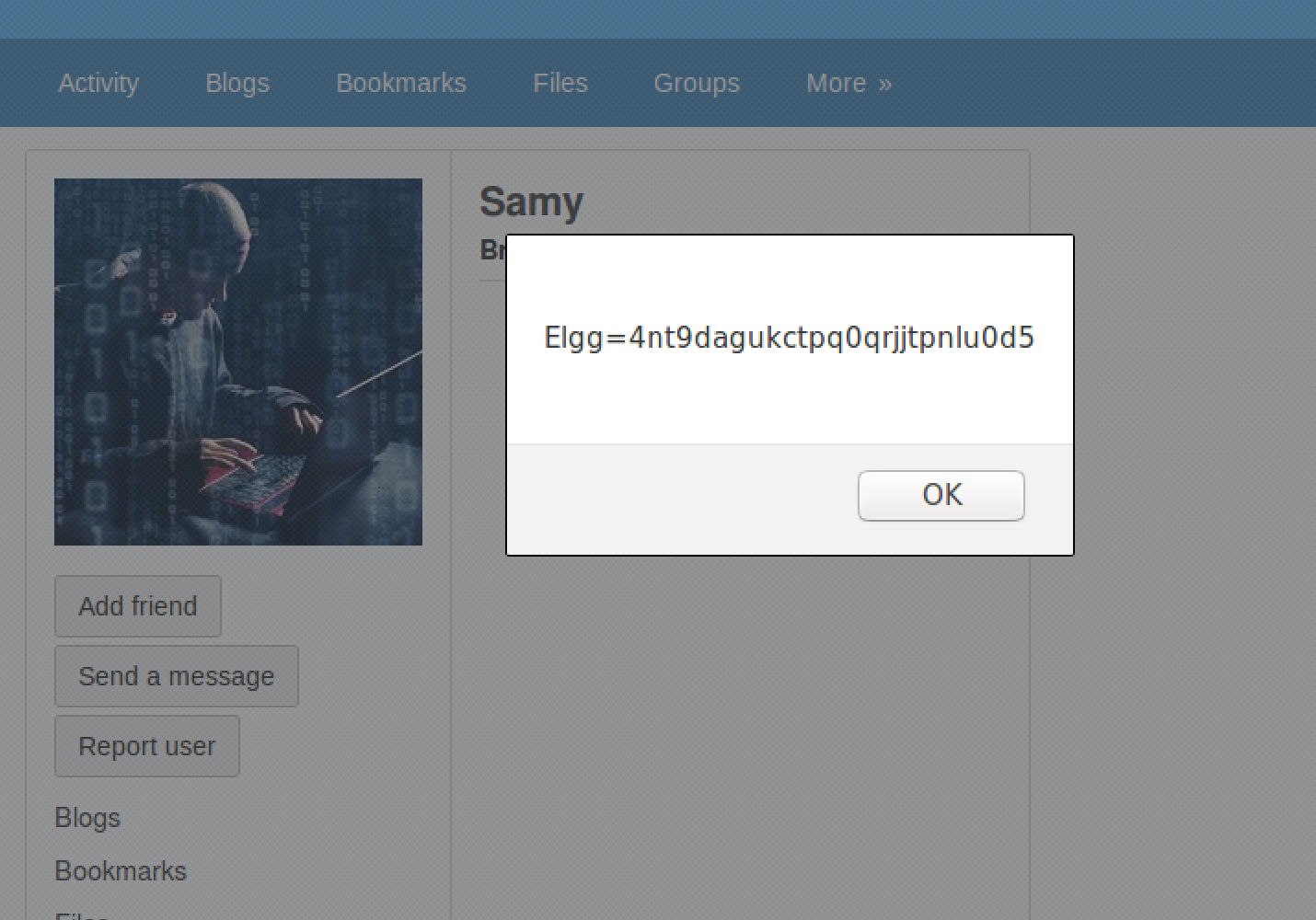
Task 2: Posting a Malicious Message to Display Cookies

Code Used:

**<script type=”text/javascript”> alert(document.cookie); </script>**

Commands/ Steps Used and Results:





Comments:

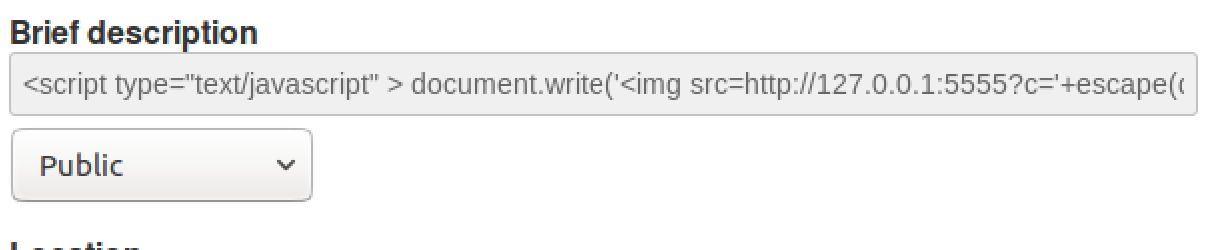
Just like before this does the same as the last task but it displays the cookies of the victim on the screen.

Task 3: Stealing Cookies from the Victim’s Machine

Code Used:

****

Commands/Steps Used and Results:



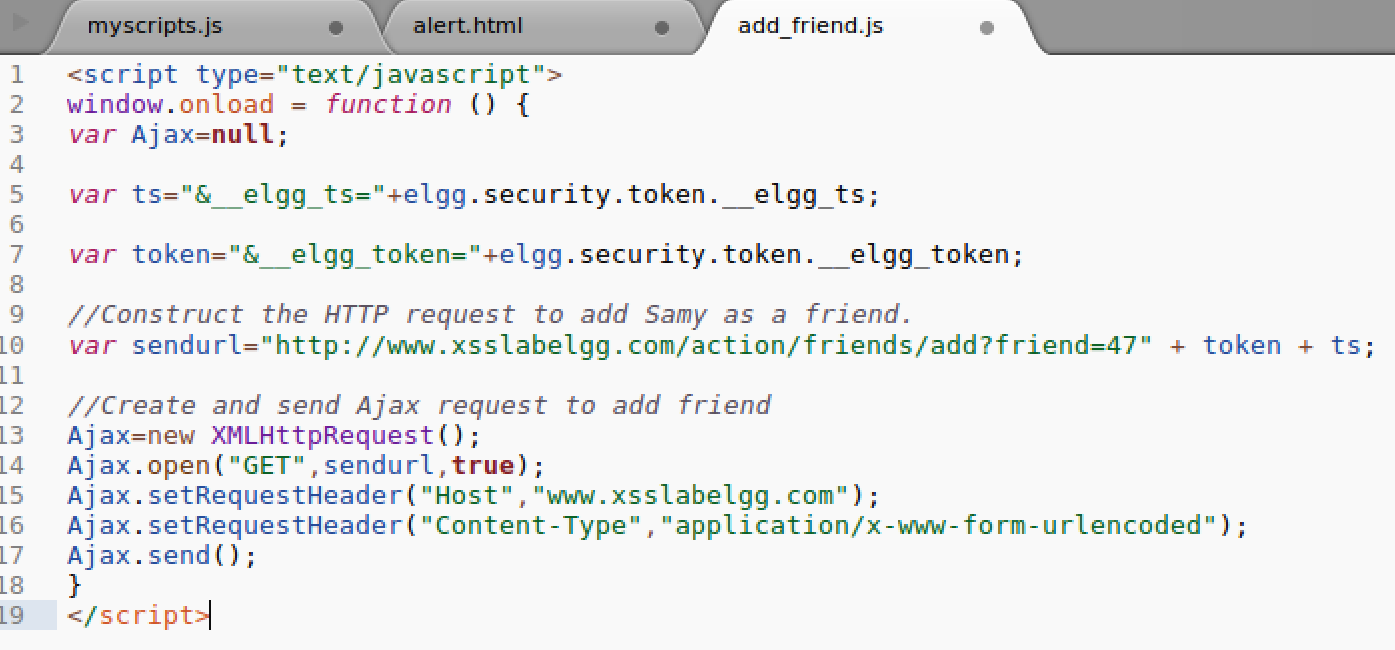


Comments:

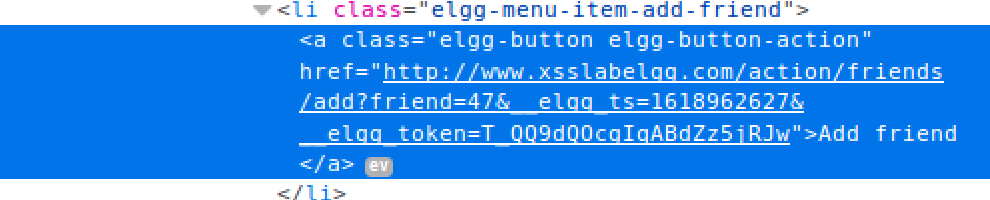
This code takes the cookies and sends them to the attacker who is awaiting a response from the port that will be called when a user is on the profile. This allows the attacker to steal the cookies of the victims.

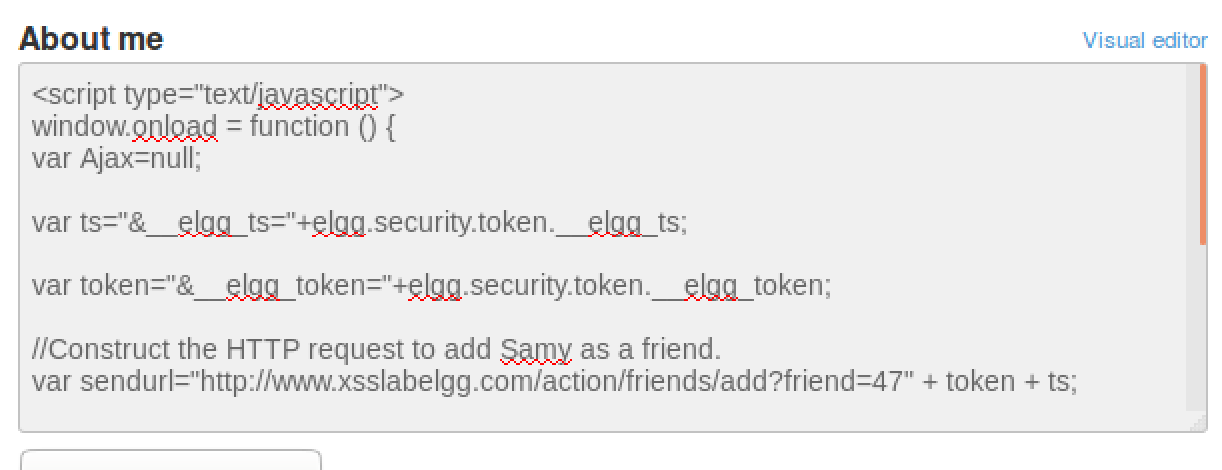
Task 4: Becoming the Victim’s Friend

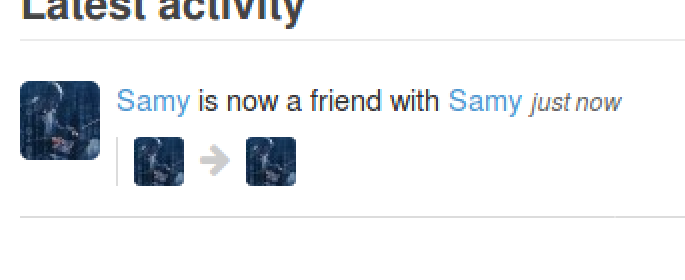
Code Used:

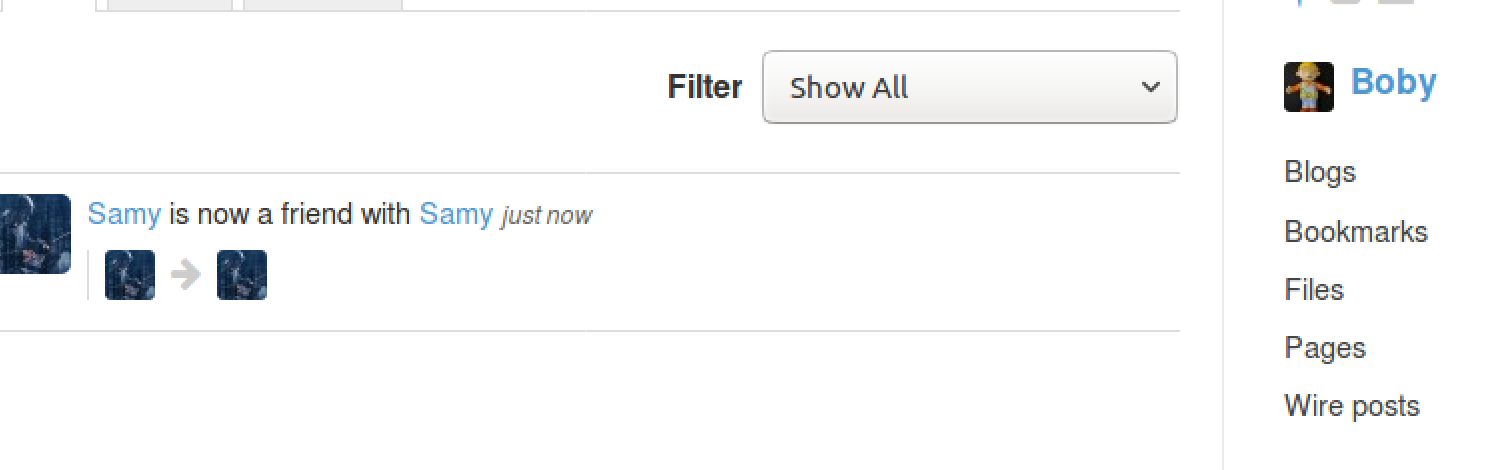


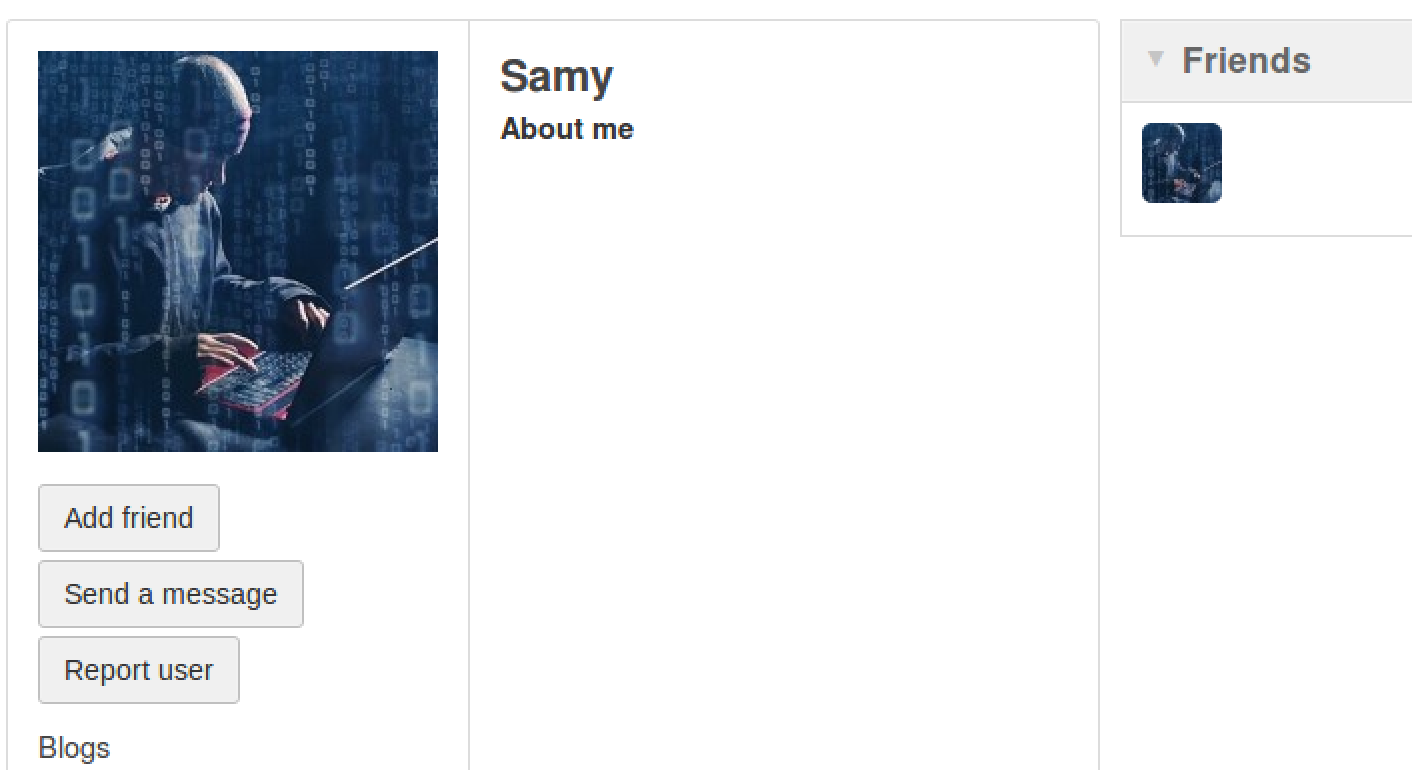
Commands/Steps Used and Results:

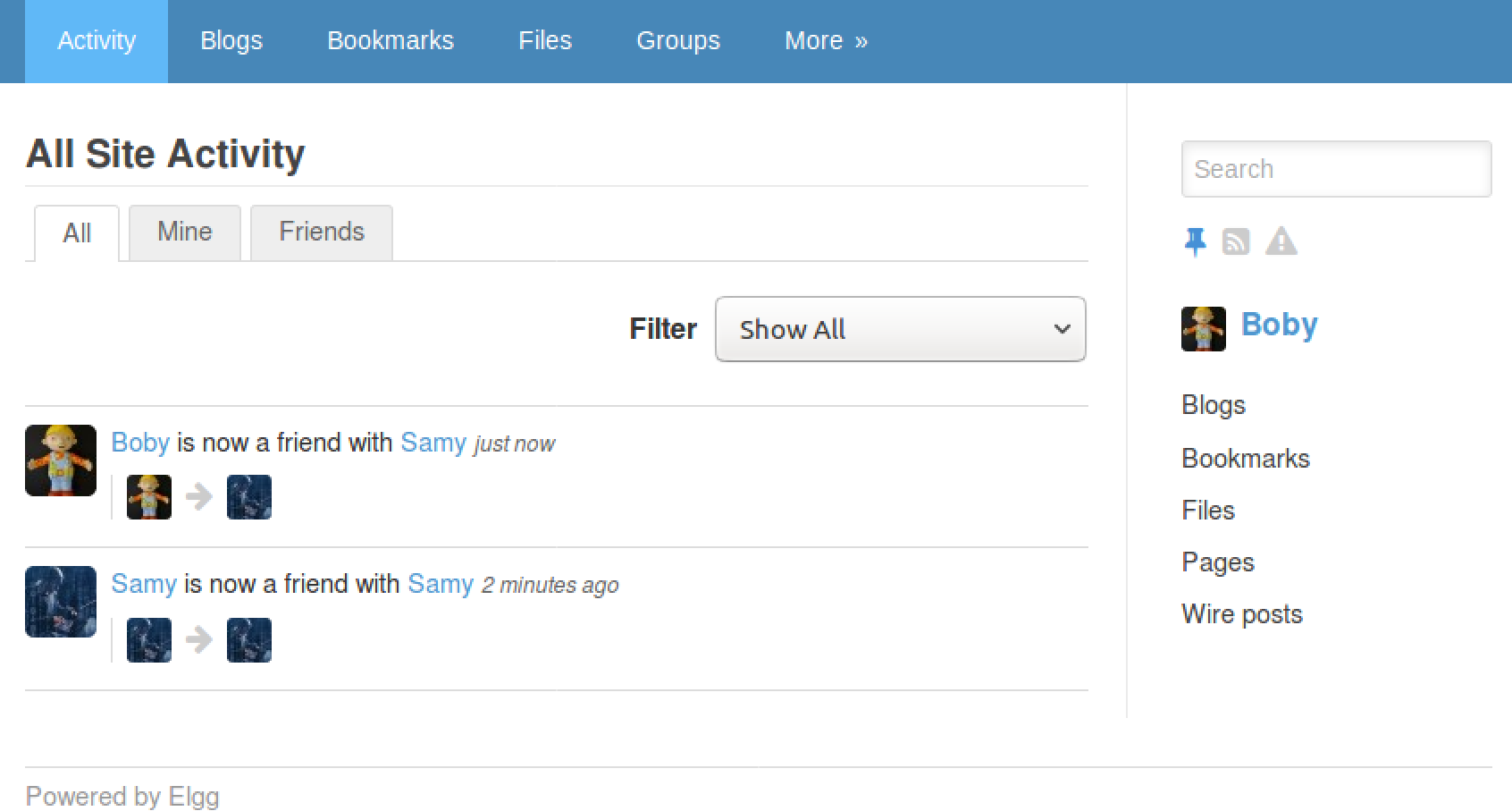












Question 1: They are used as a convergence against the attack

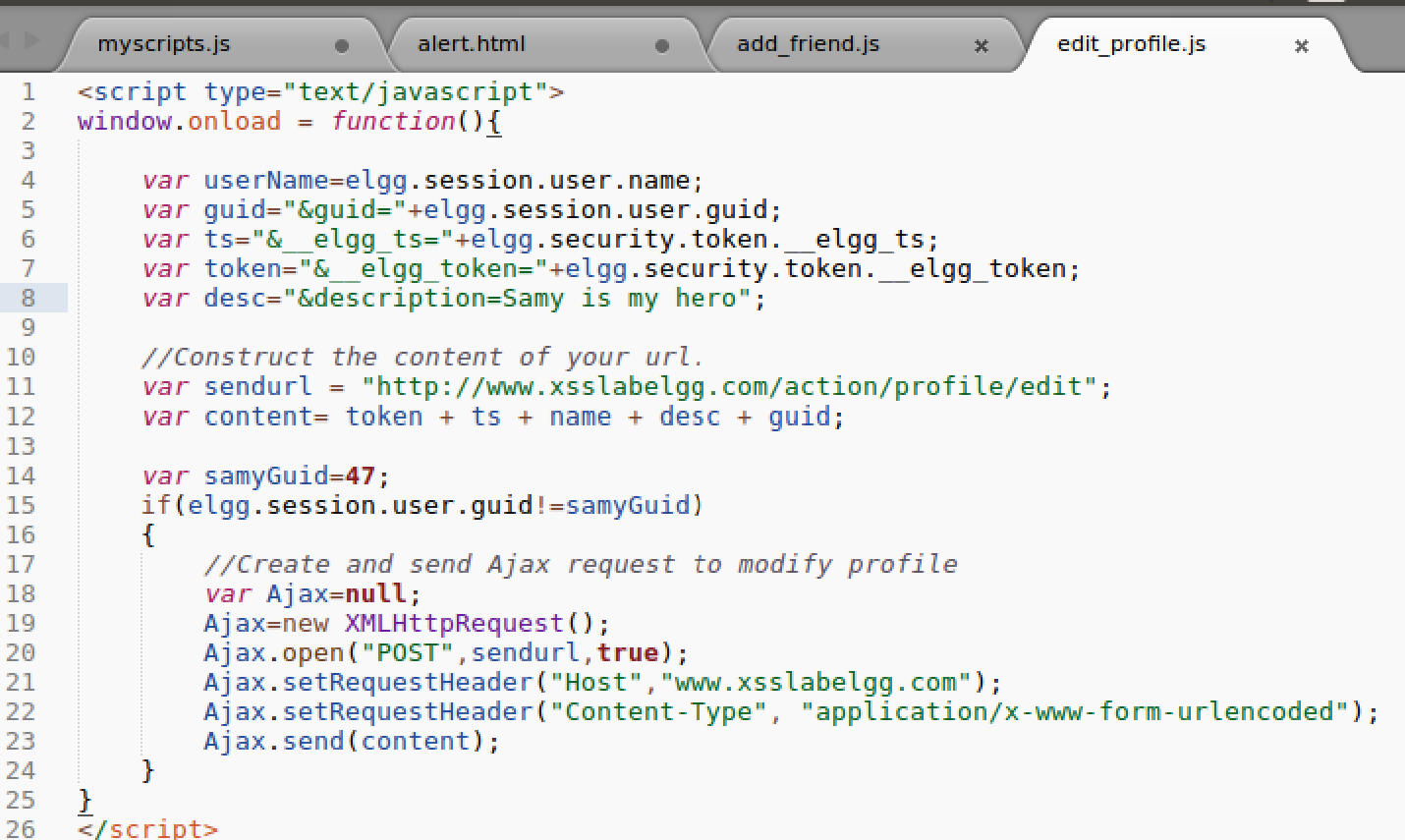
Question 2: No you cannot successfully launch the attack

Comments:

This code makes it so whoever looks/clicks on Samy’s profile, it will automatically add him as a friend. To find Samy’s id, I inspected the add friend button and found the url that it runs when someone click on it to add him as a friend. This code just makes it so they don’t even have to click on the button.

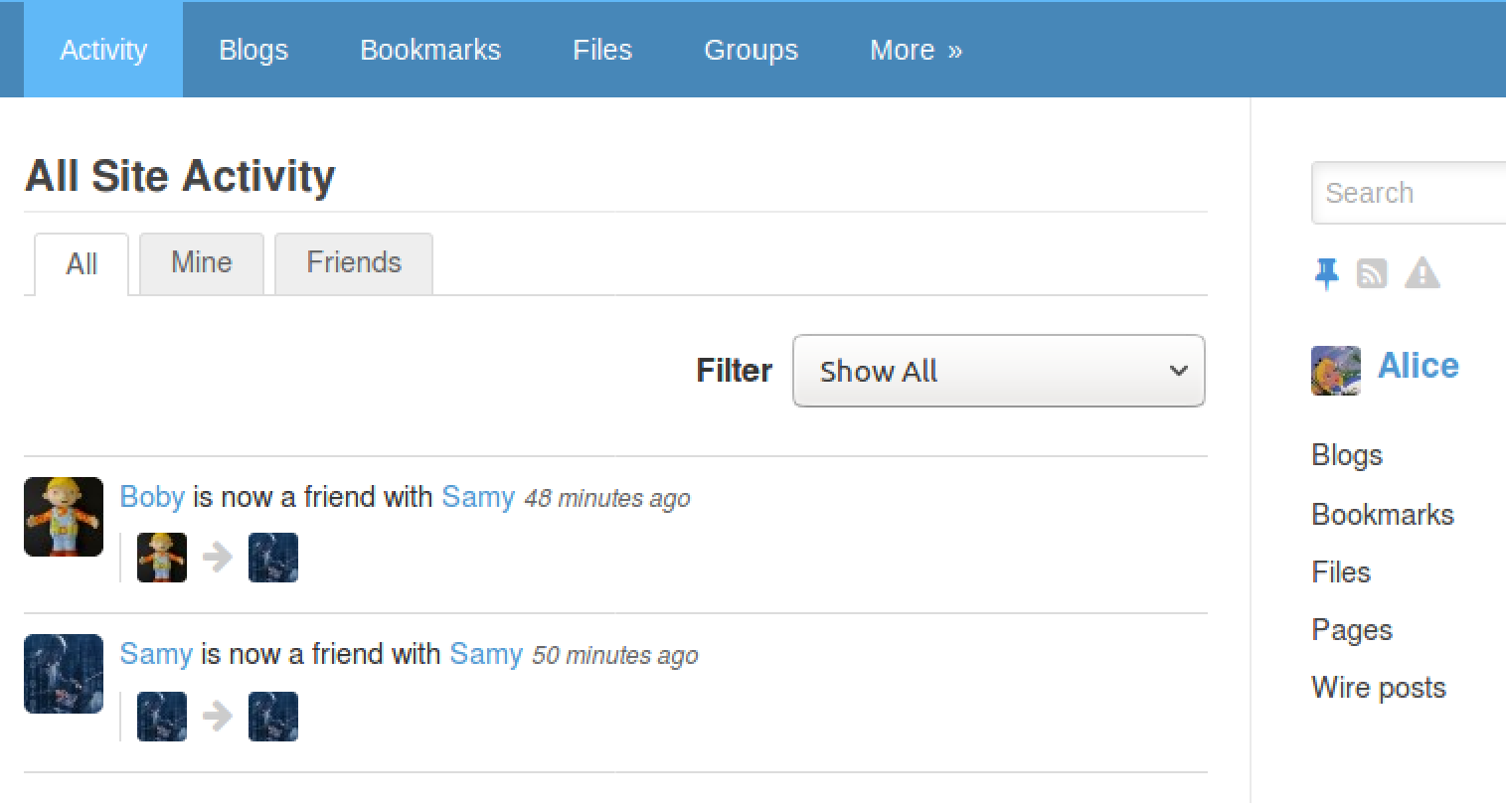
Task 5: Modifying the Victim’s Profile

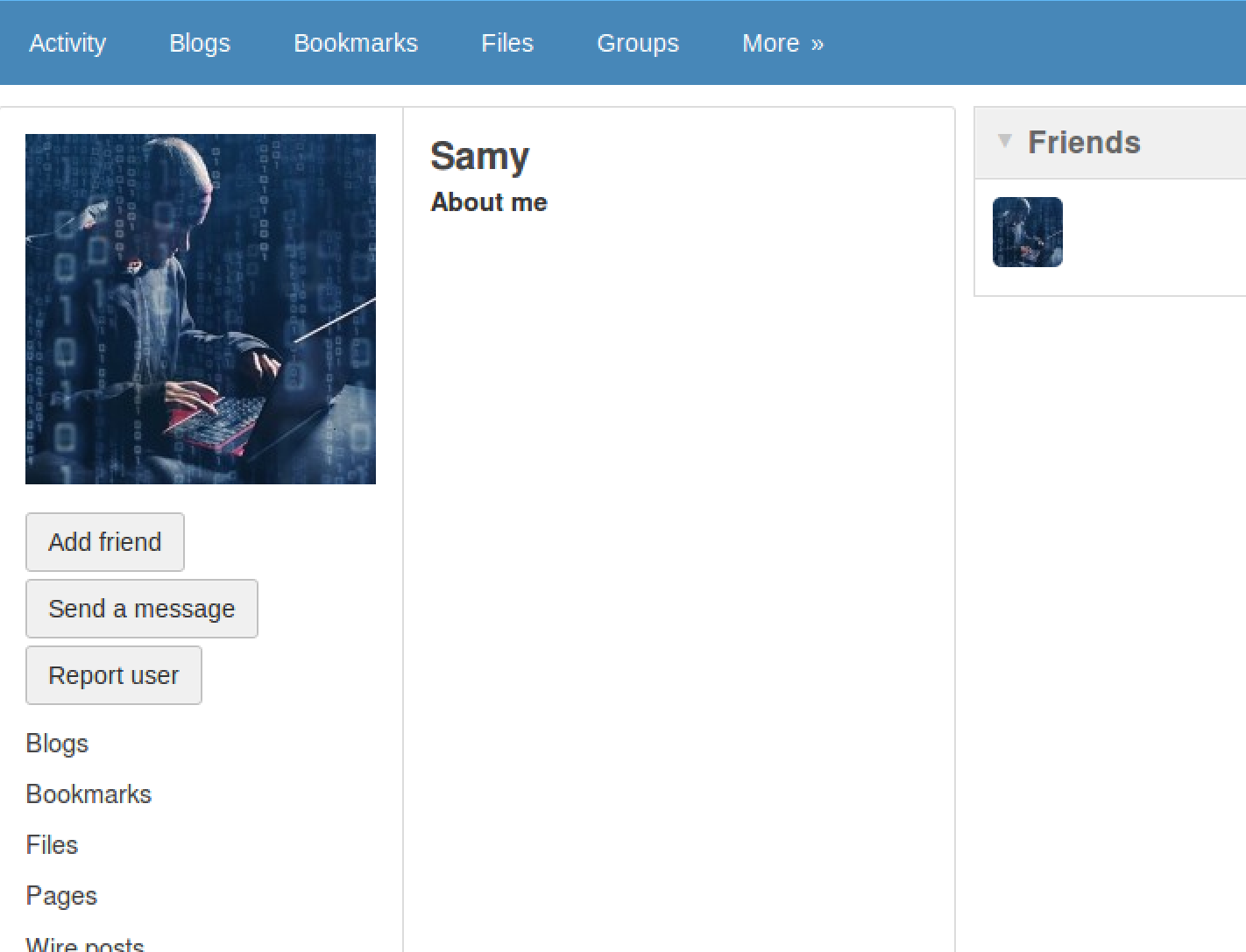
Code Used:

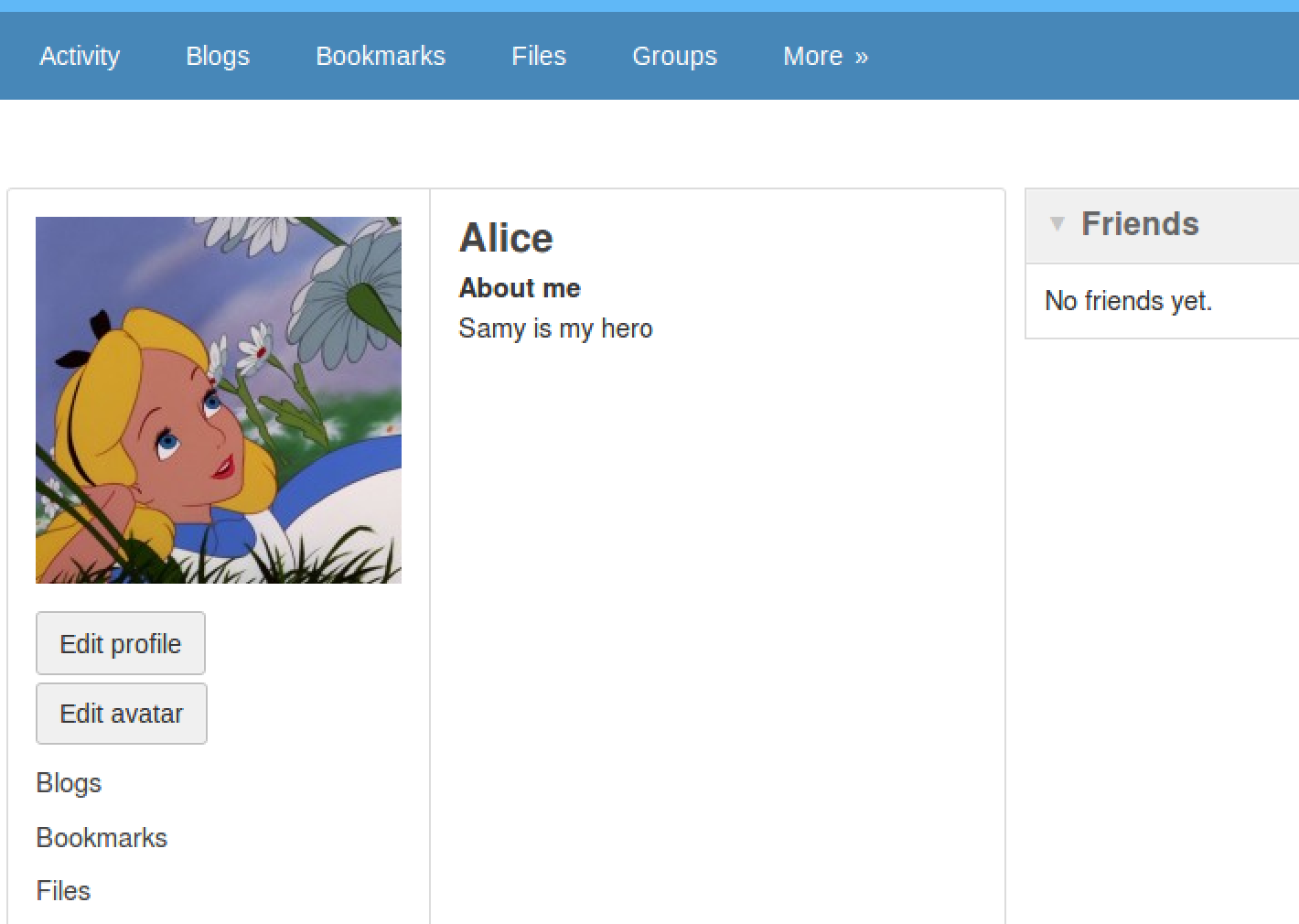


Commands/Steps Used and Results:









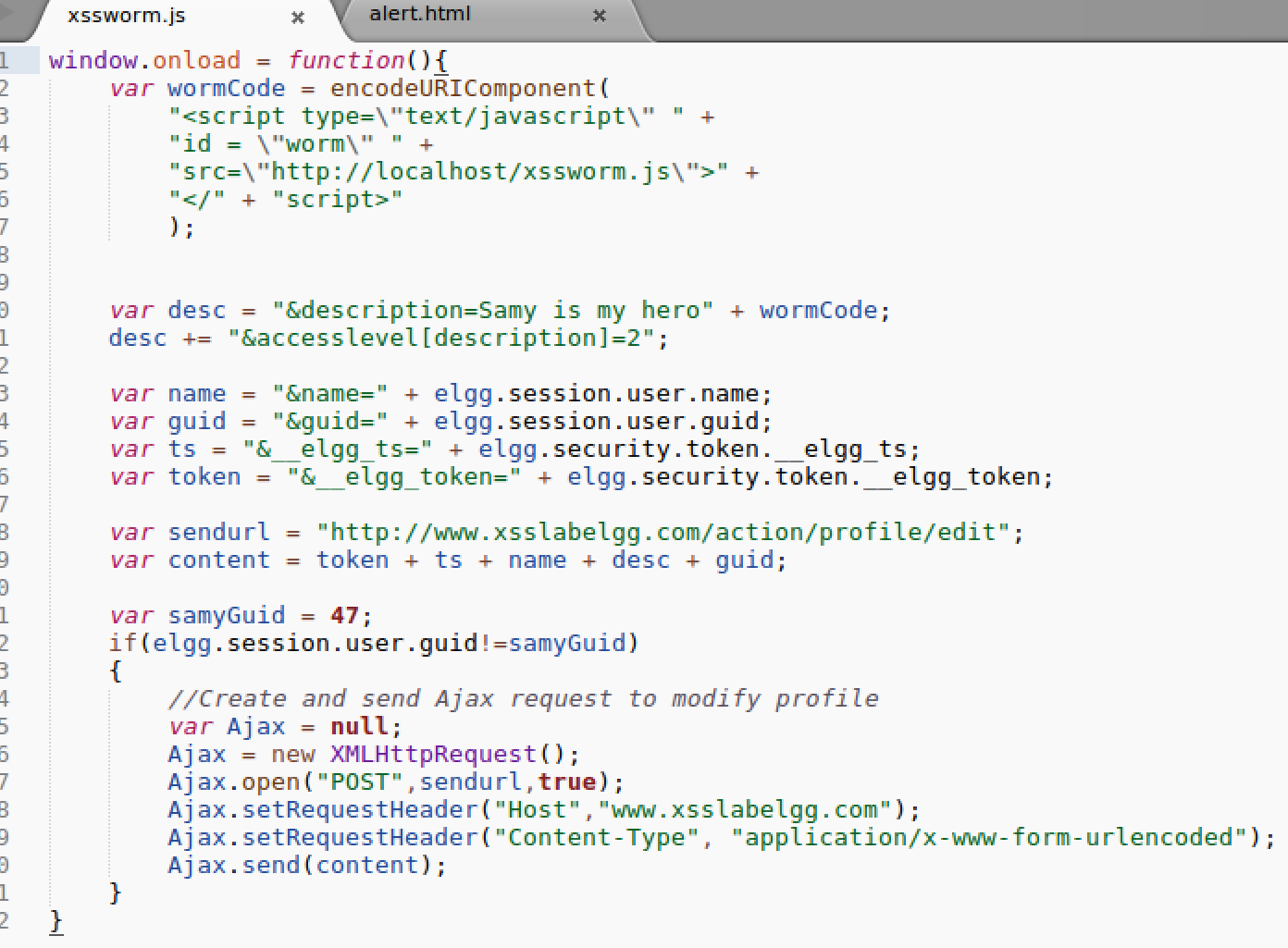
Question 3: The if statement makes it so Samy cannot attack himself. When I took it off and ran it again he was also attacked when I saved the changes and it returned me to his profile.

Comments:

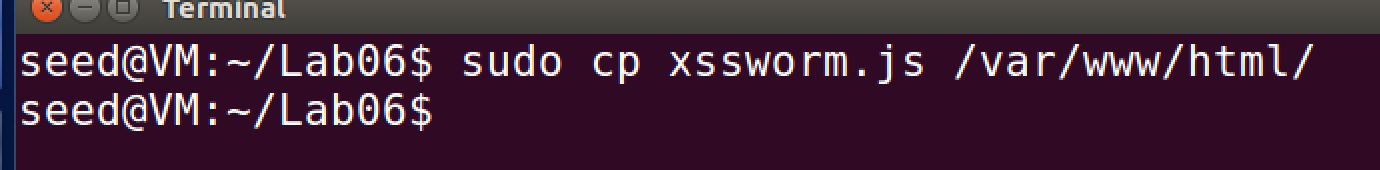
This code makes it so that everyone that looks at Samy’s profile will have their about me description change to “Samy is my hero”. Everyone but samy is affected because the code has it so it checks the id of the user and if it matches Samy’s user profile id, then it doesn’t modify his.

Task 6: Posting a Malicious Message to Display an Alert Window

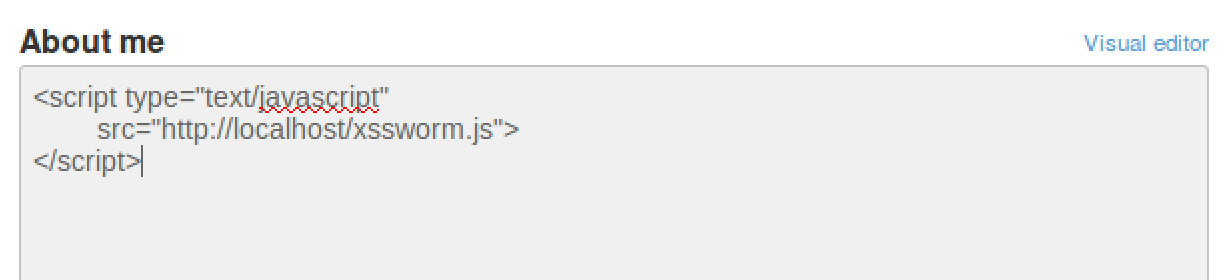
Code Used:

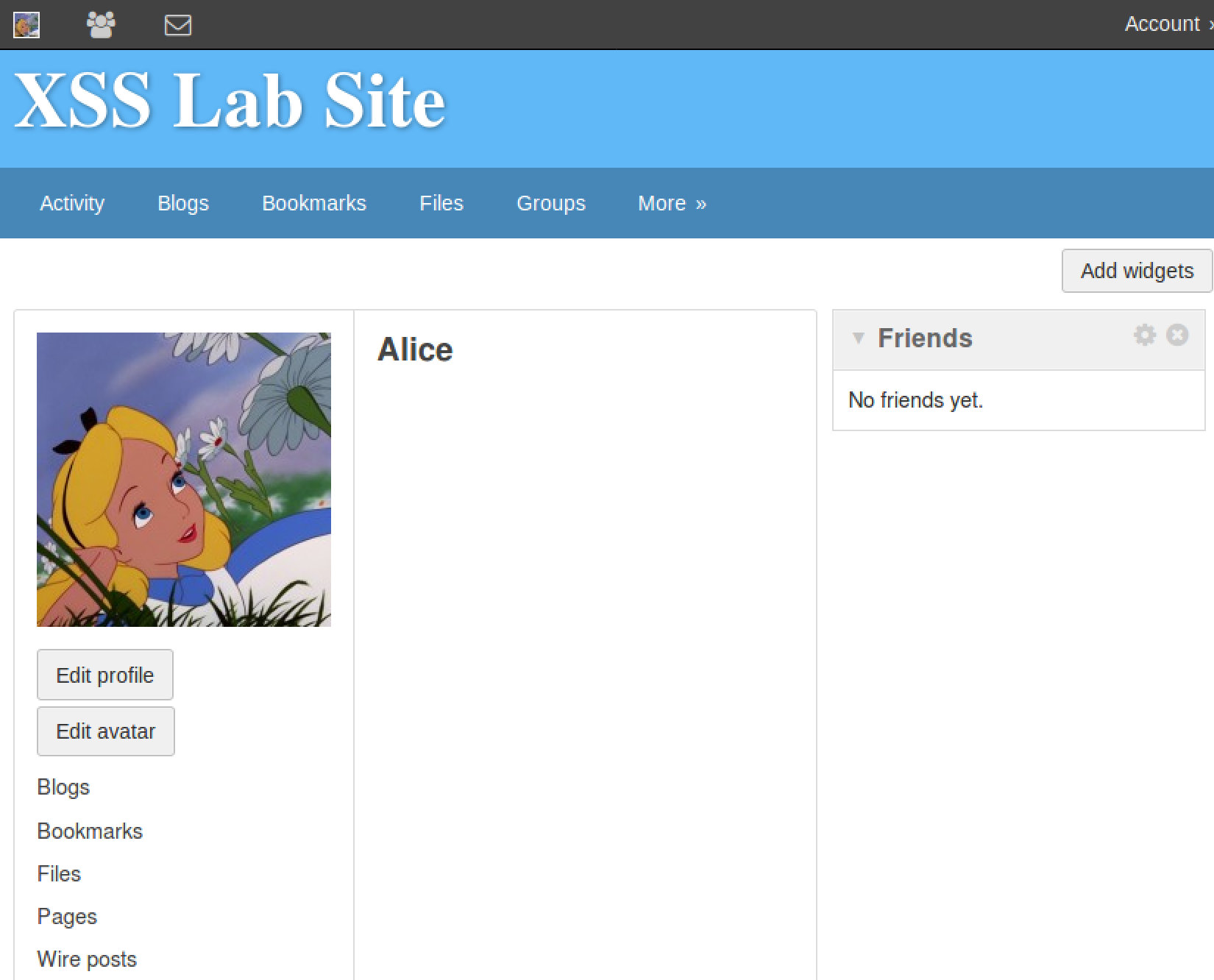


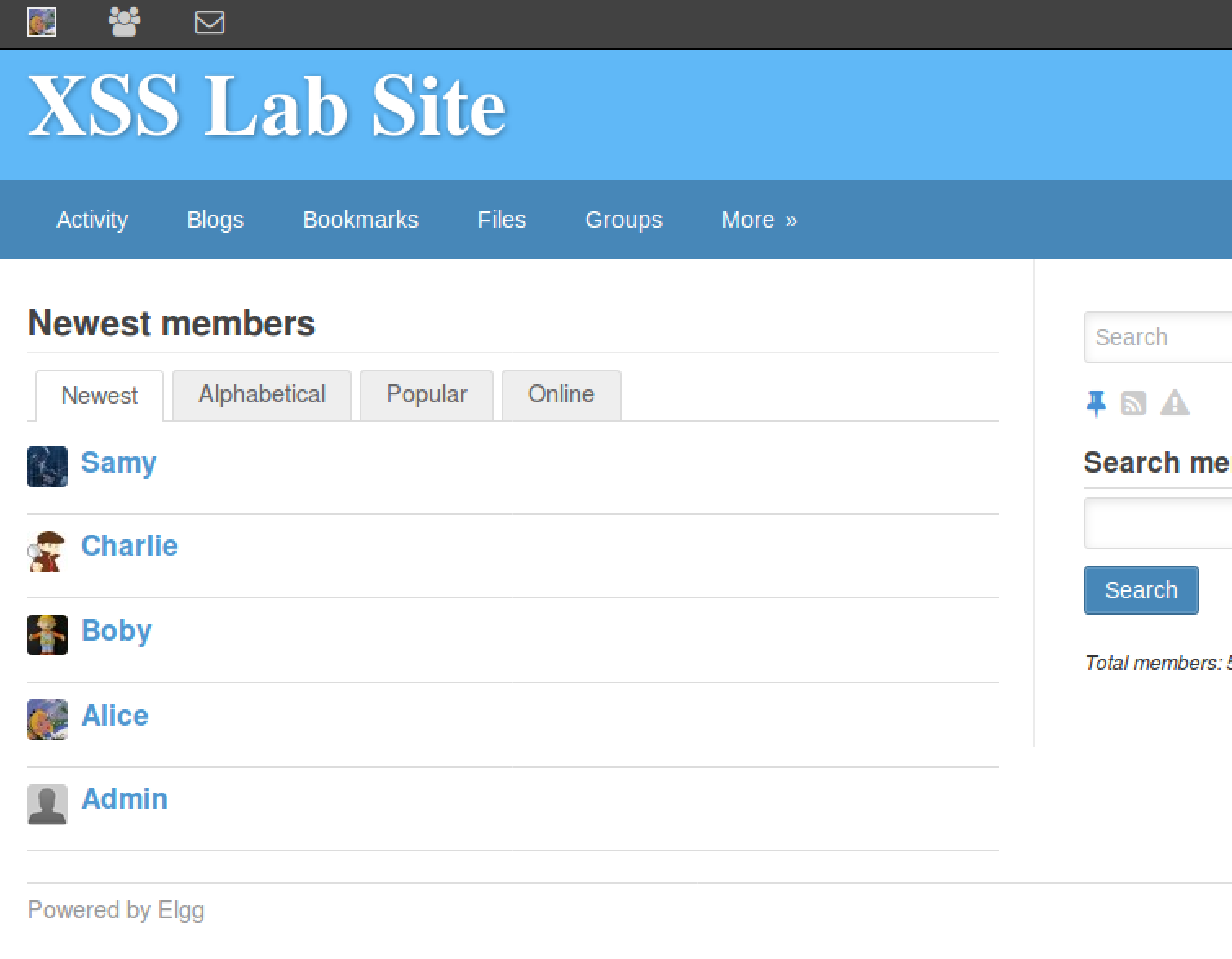
Commands/Steps Used and Results:

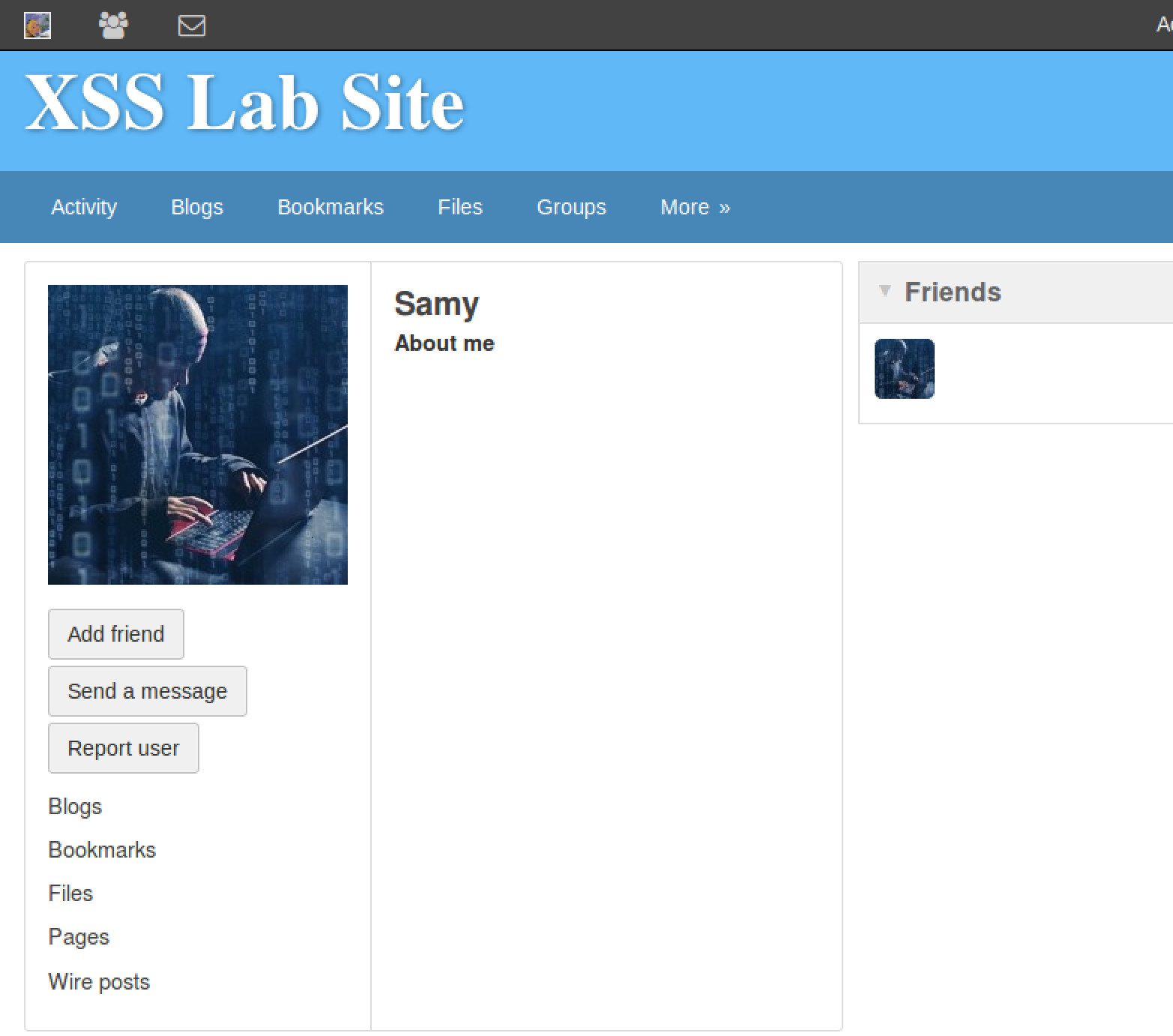


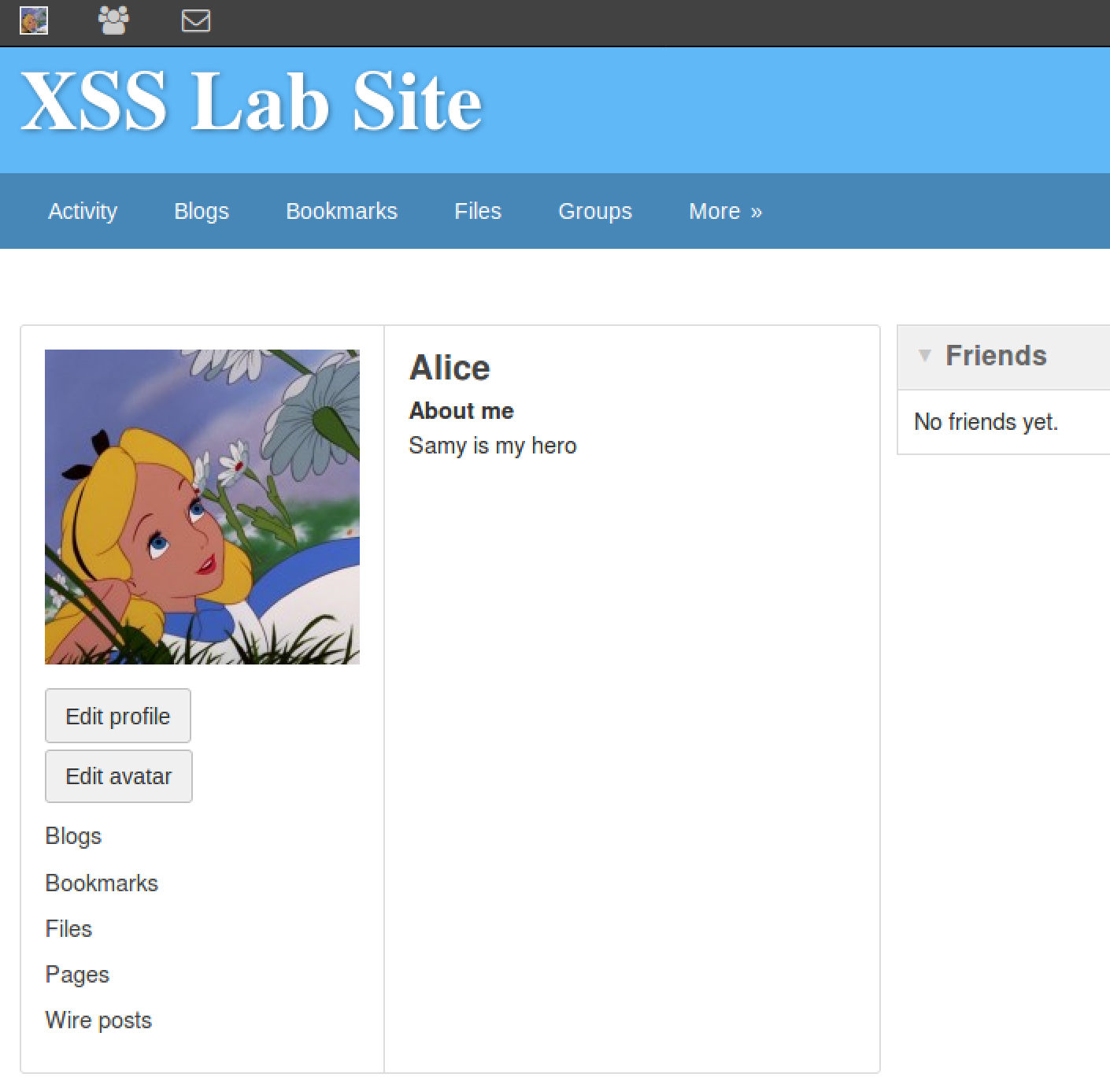
Link Approach:

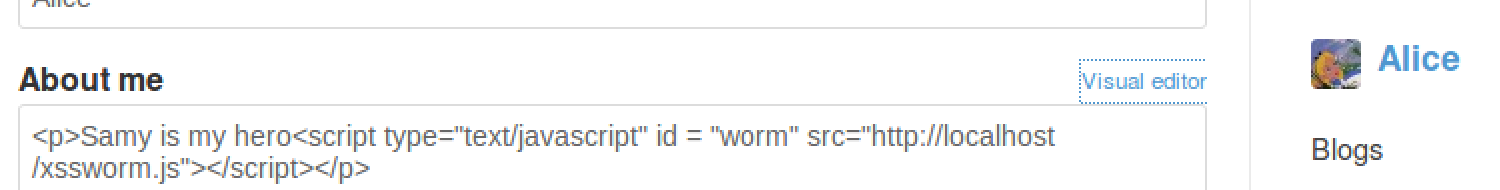


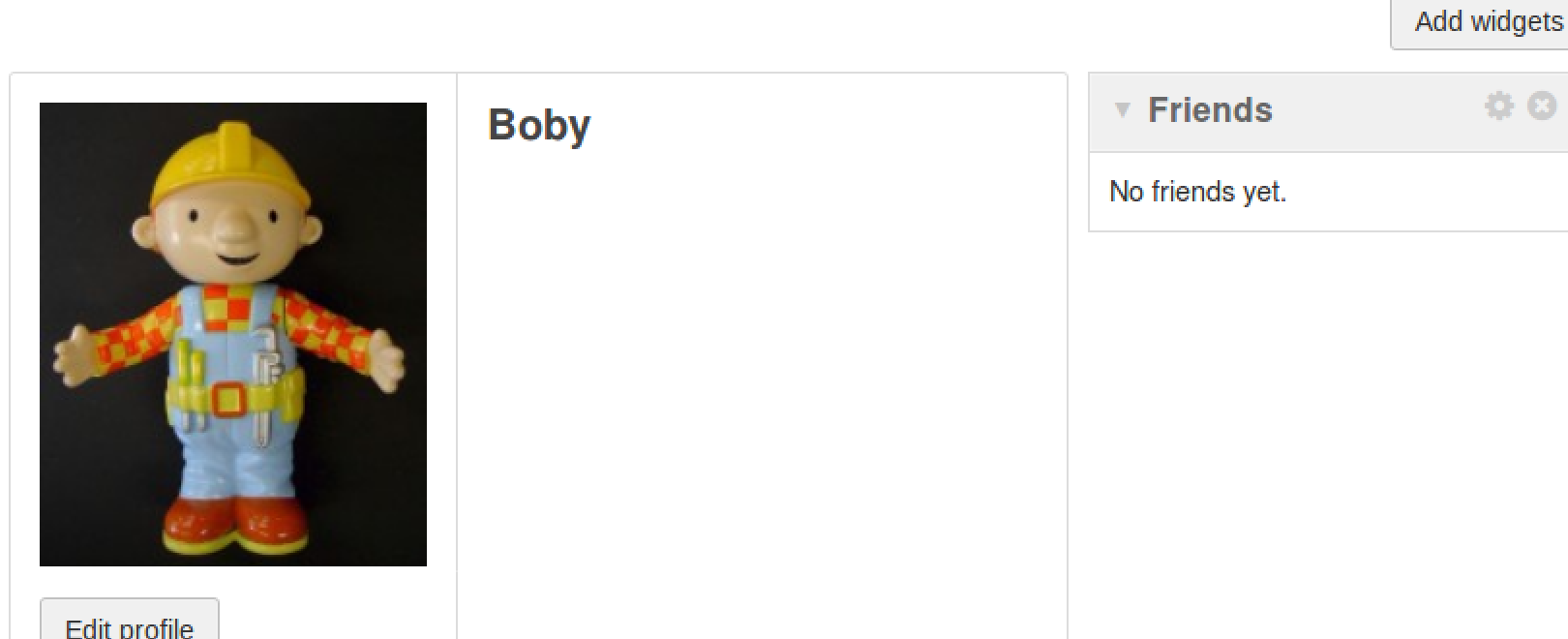


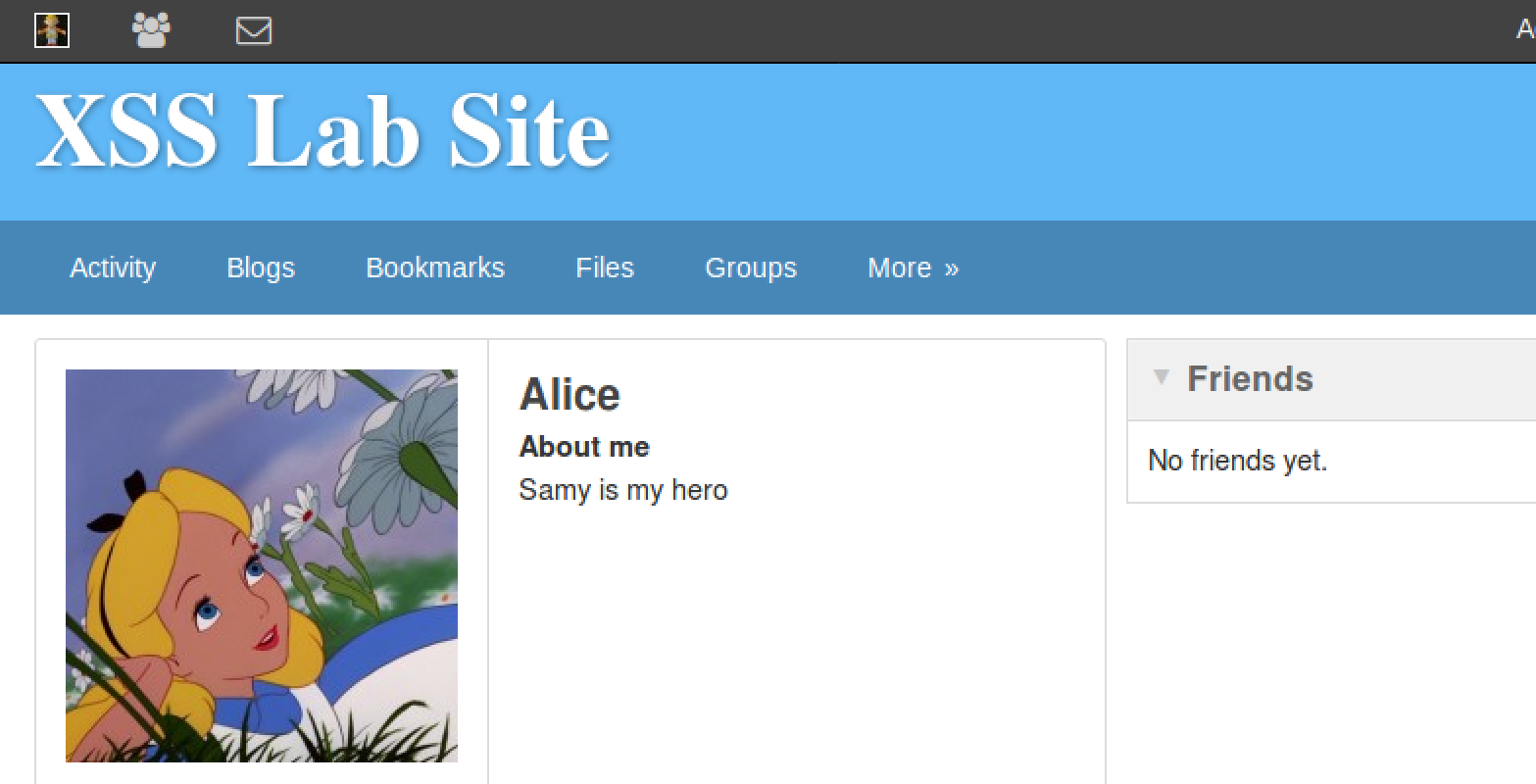


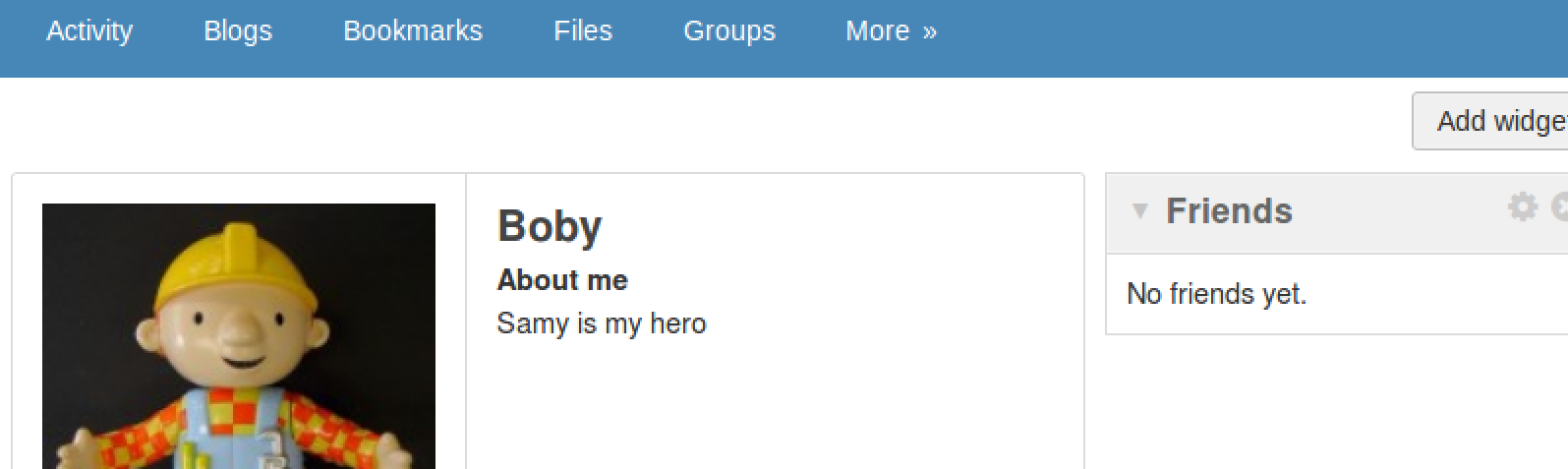


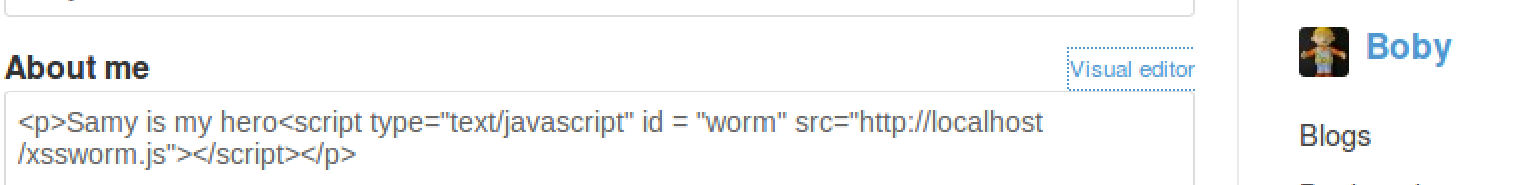




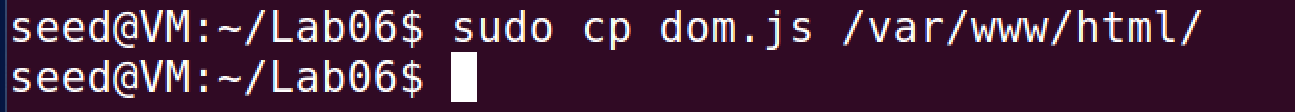


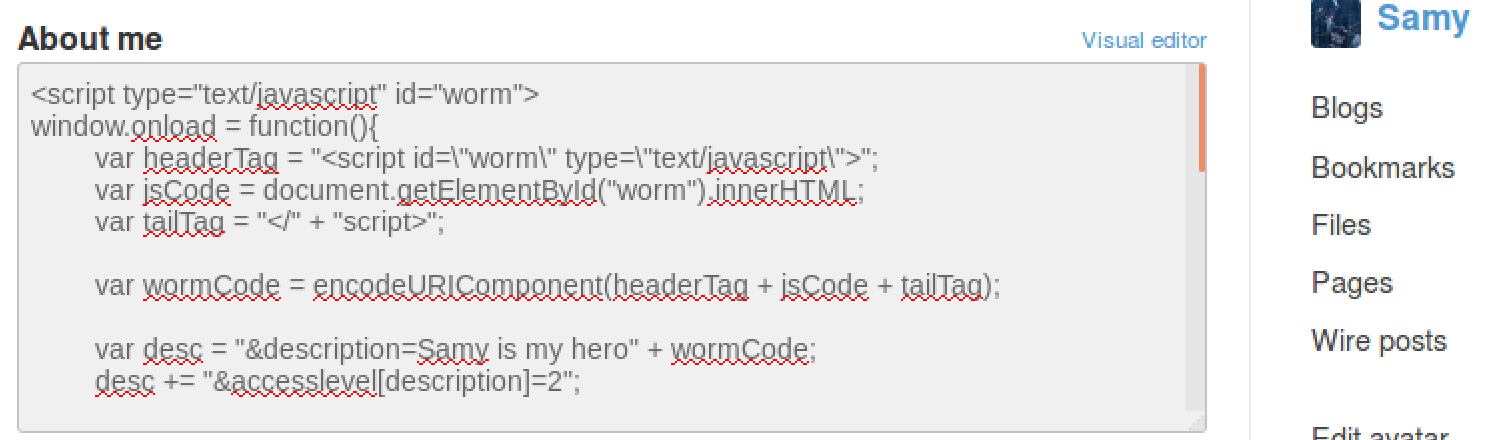


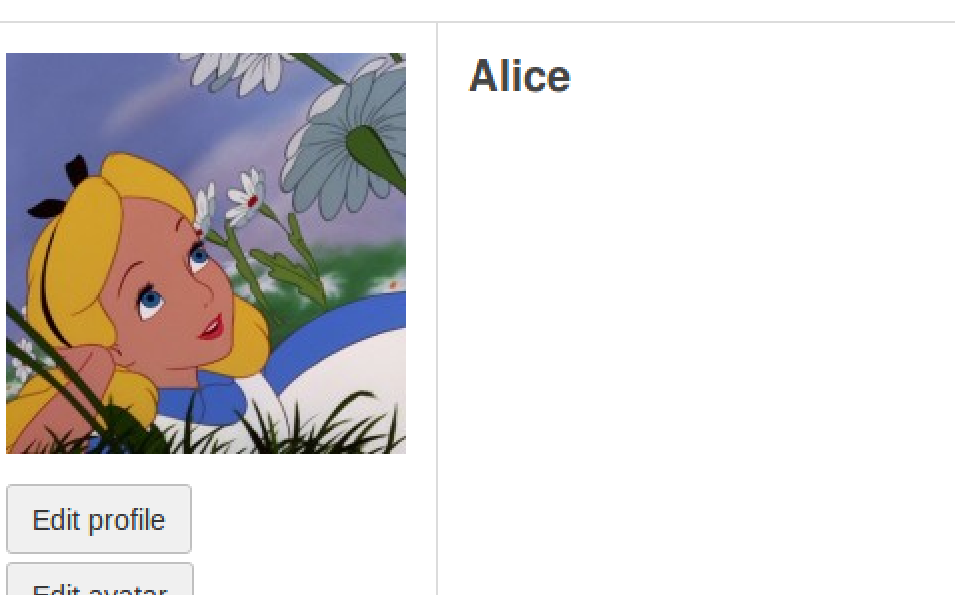


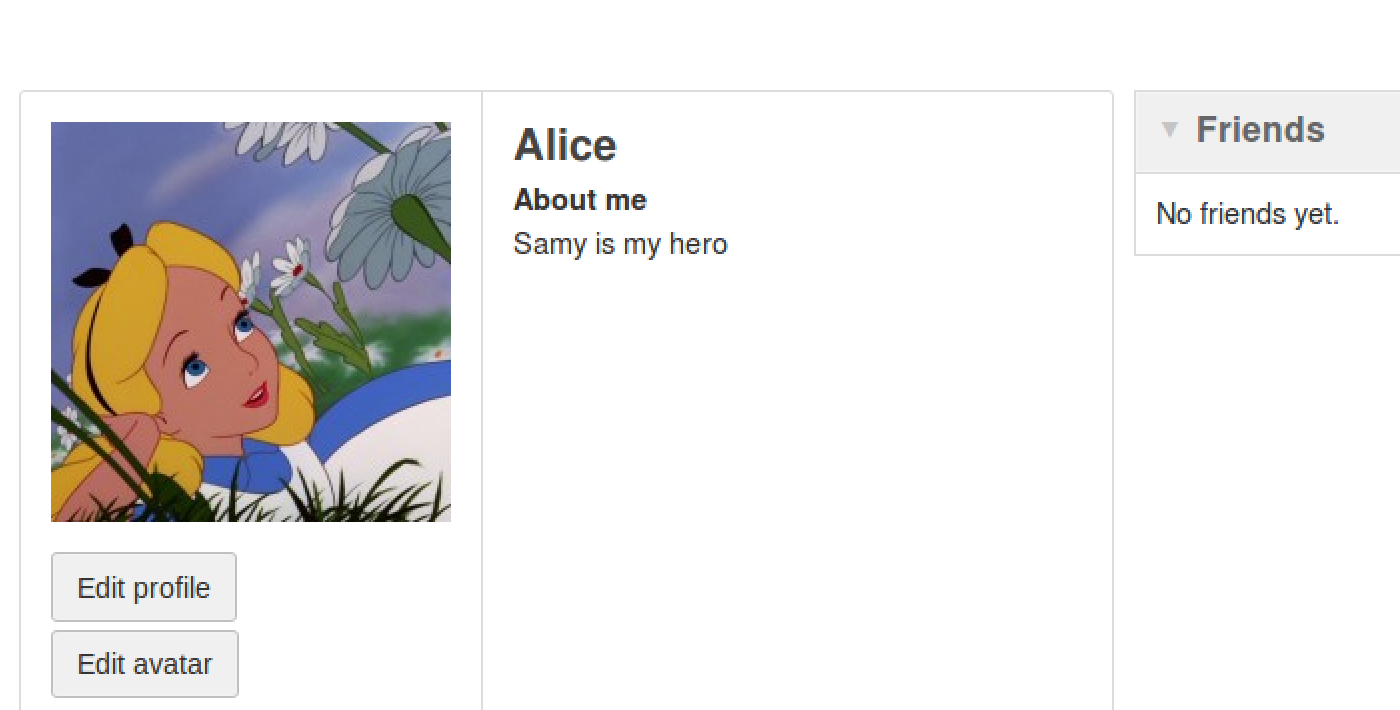


DOM Approach:



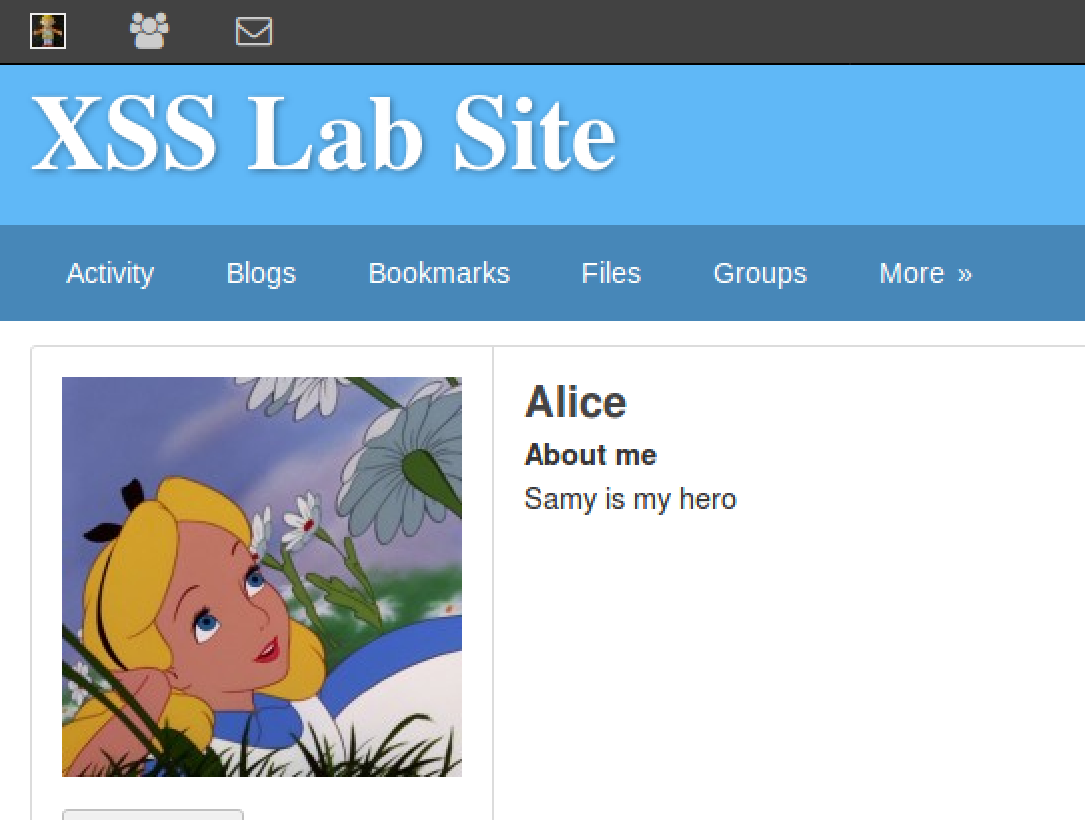














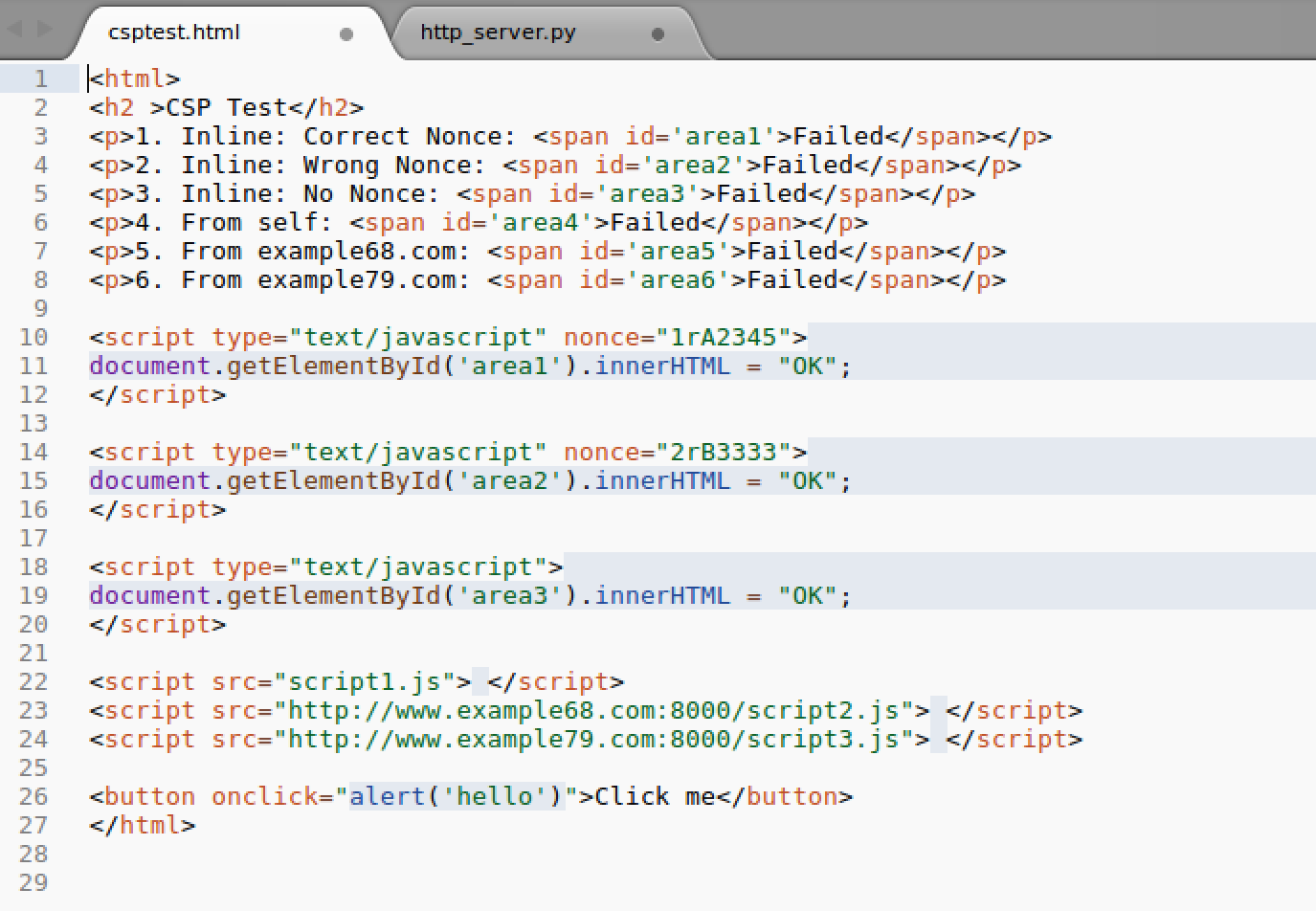
Comments:

For the Link approach means we copy the worm code to the server and then it that code is being called by the link that is in their About Me section. With the DOM approach it is basically just using the plain code instead of a link to infect the users. Both of these approaches infect the victims whenever they look at the profile of anyone who is infected with the code.

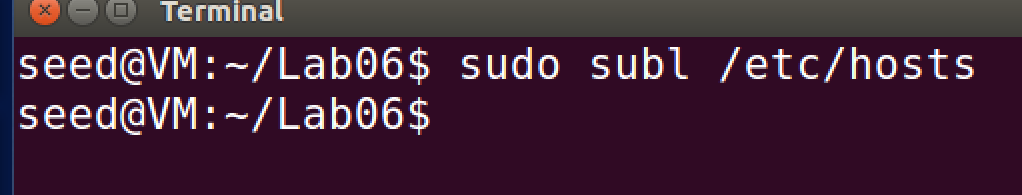
Task 7: Defeating XSS attacks using CSP

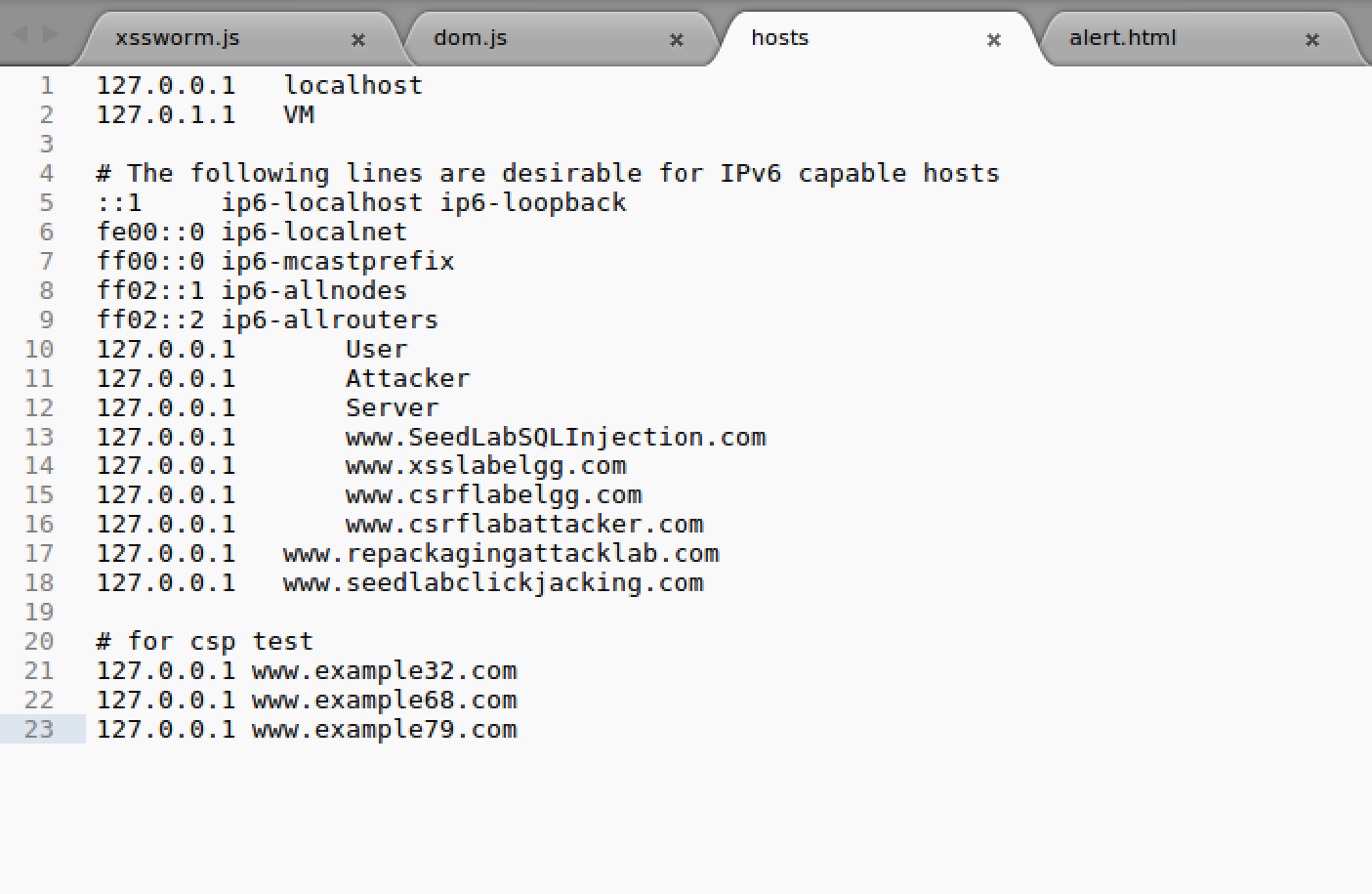
Code Used:

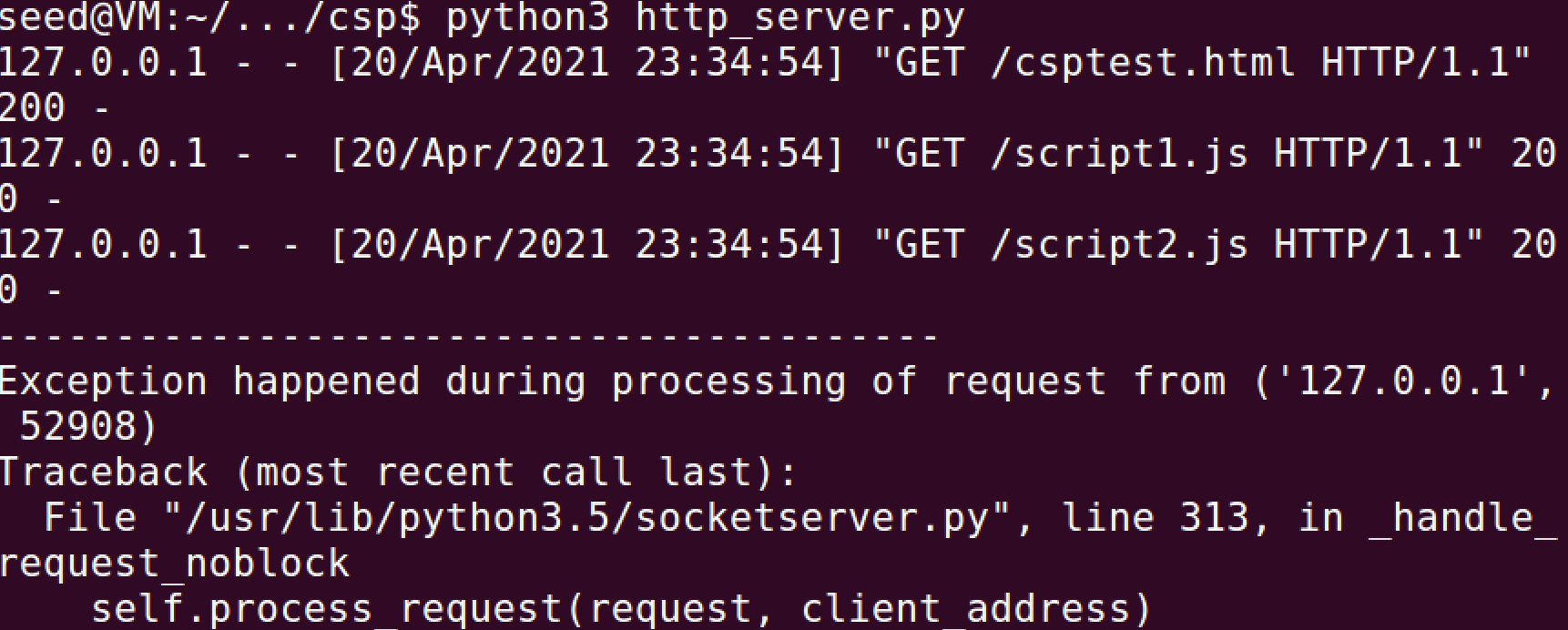


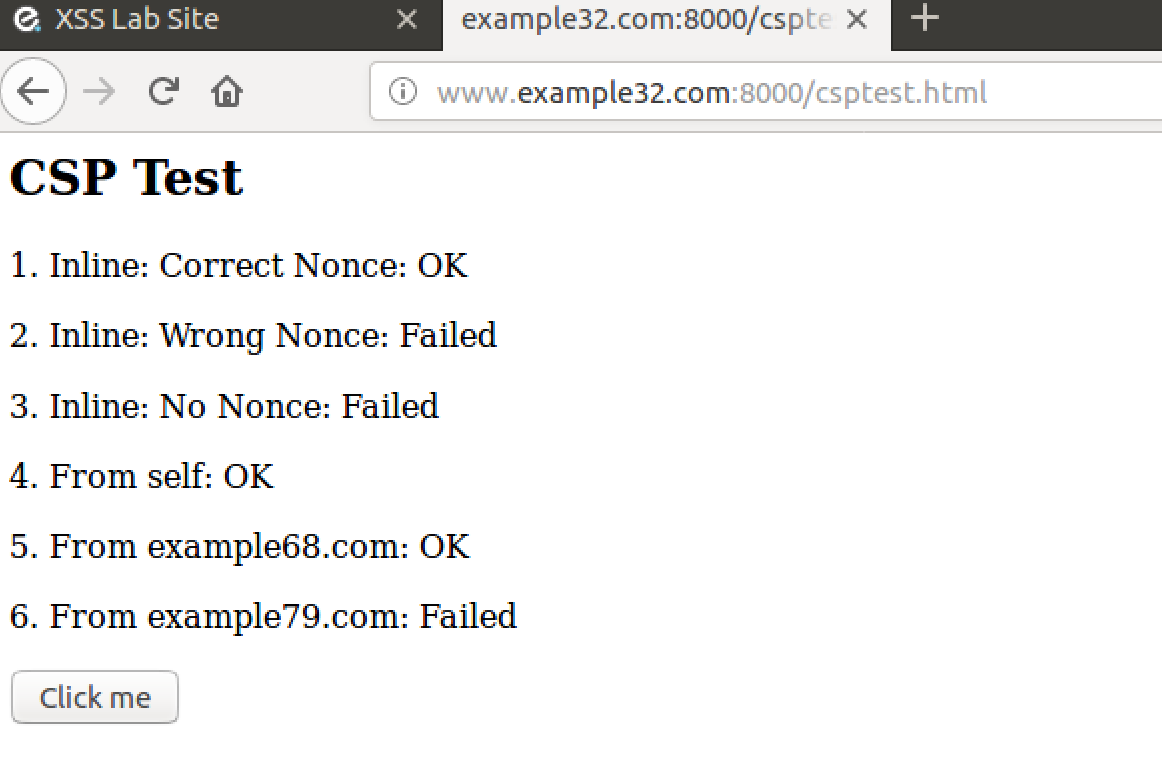


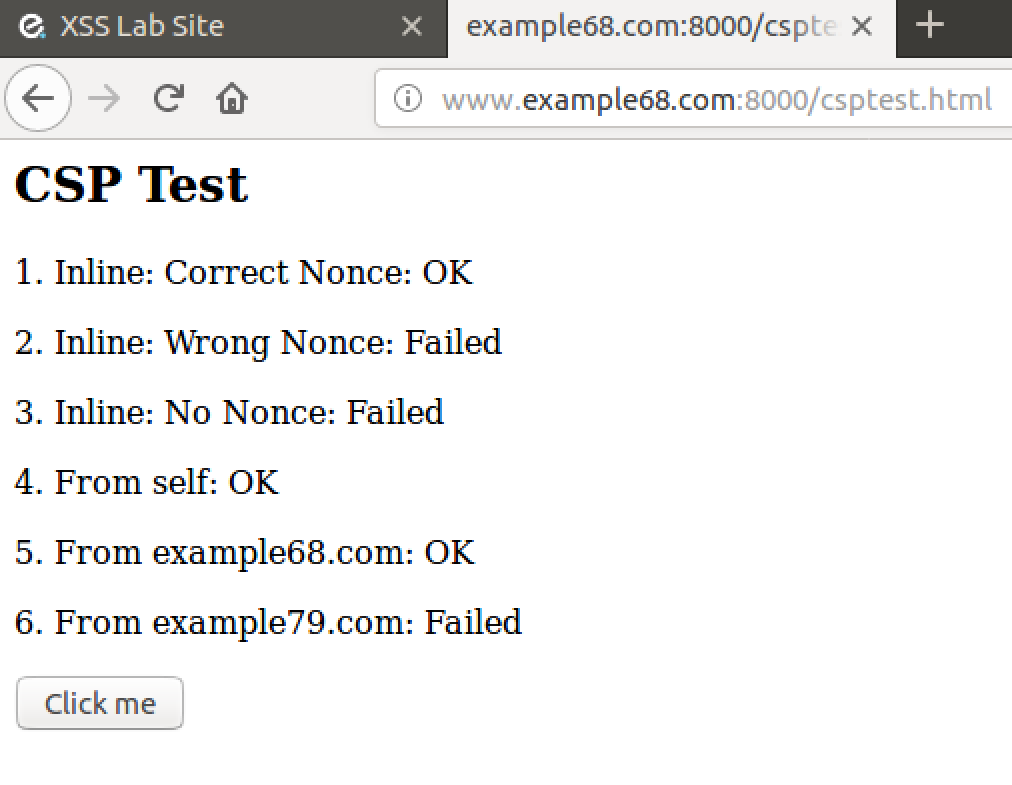
Commands/Steps Used and Results:





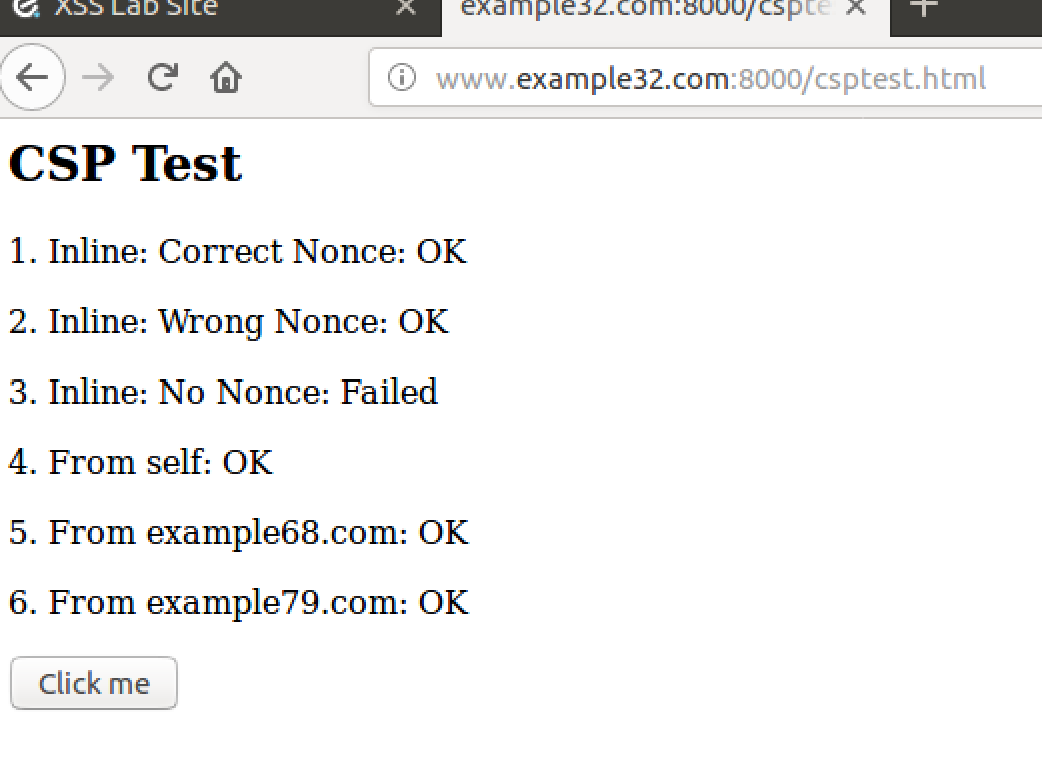




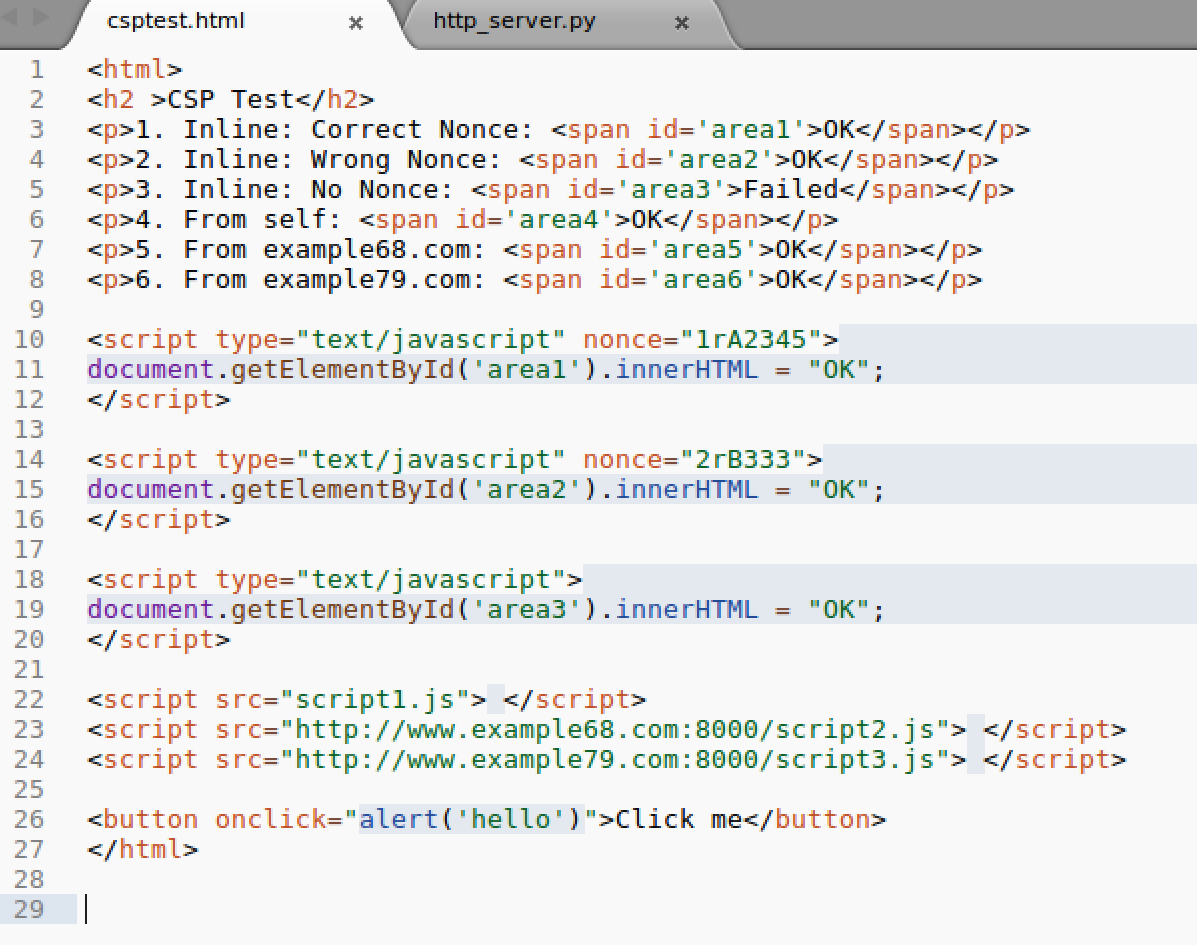




After Changing the Code



Code:



Comments:

The code CSP is set by the web server. To test it we have a csptest.html file that is initially set to failed for the codes of javascript running unless they succeed. I had to input the ip addresses and the individual urls into the hosts file in order for this to work and test it all. The first two URLs are both identical in the number of Oks and fails as well as the location of them. The third one has more Oks and less fails.