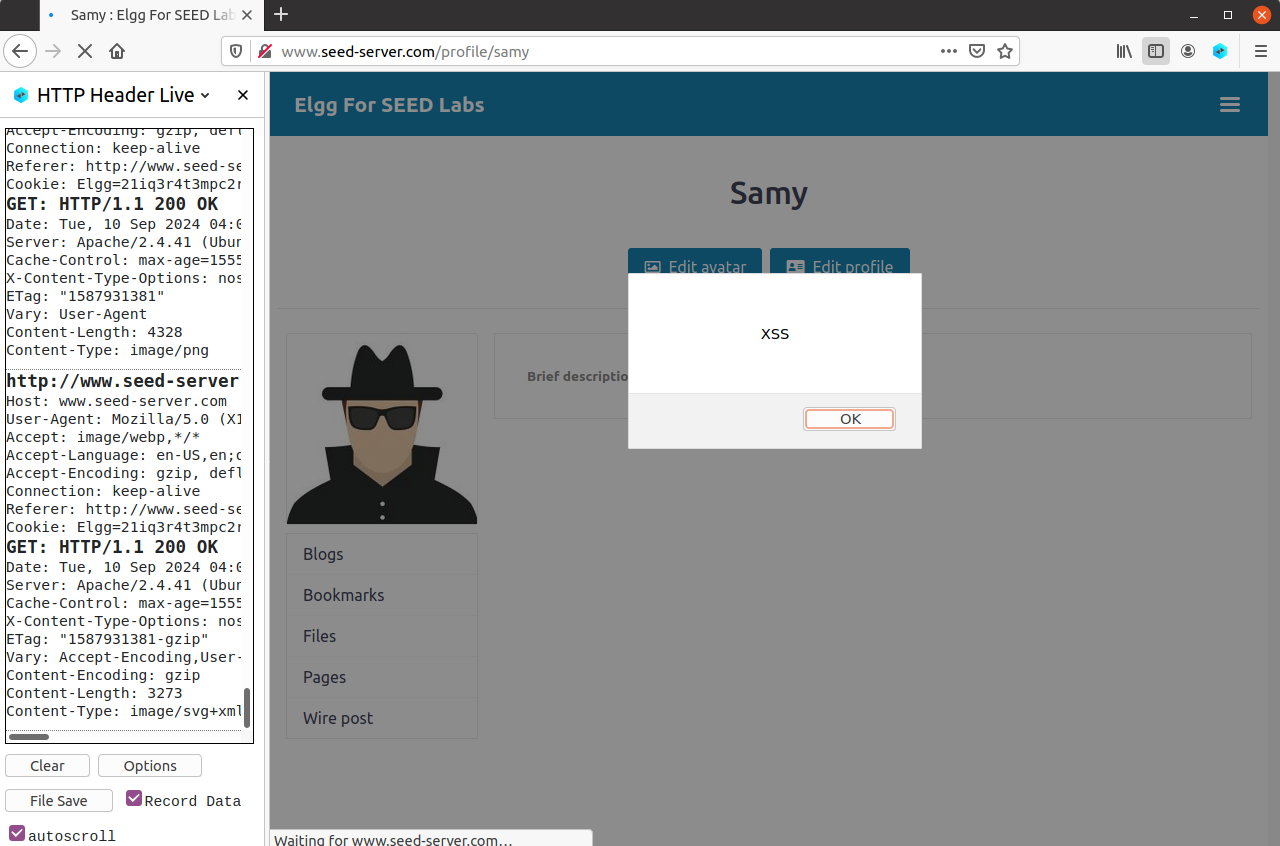
Name: Donghao Li

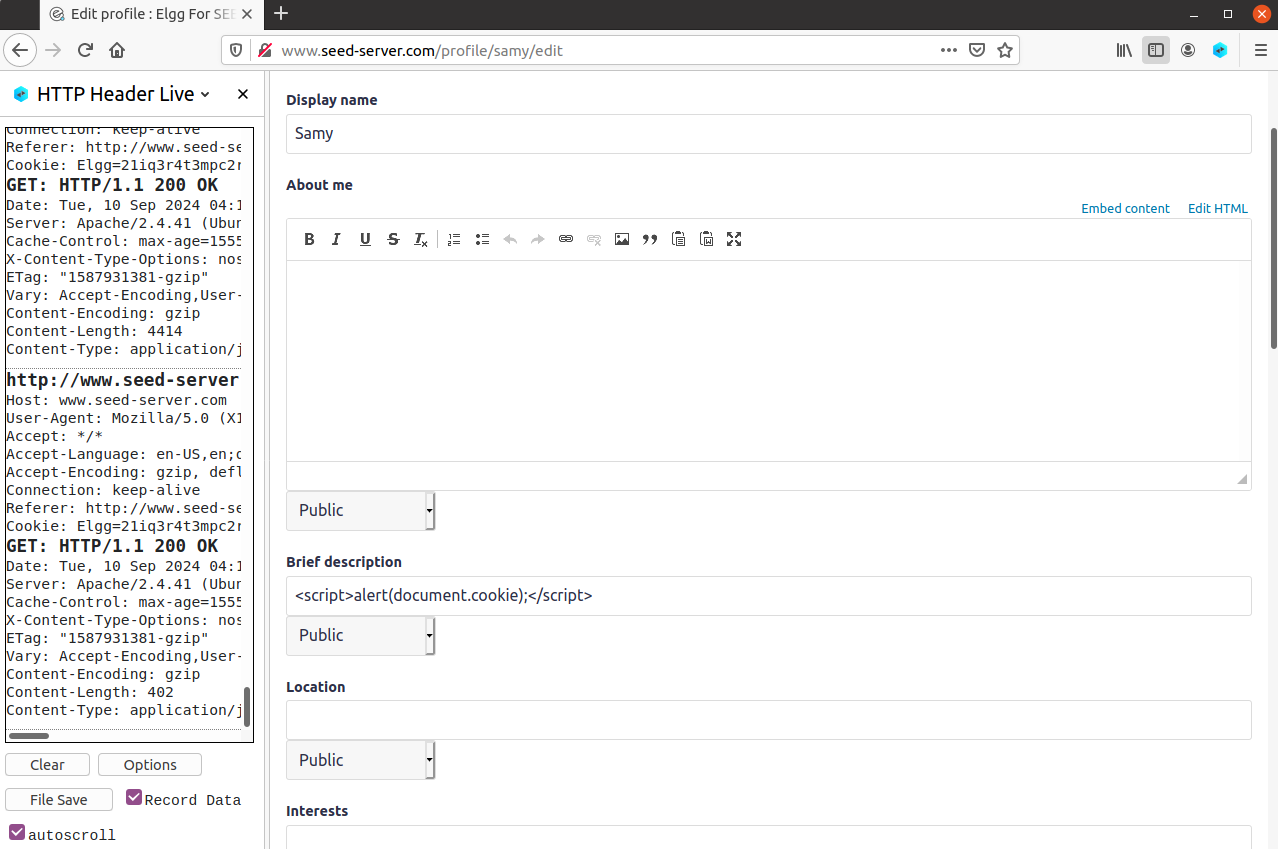
SUID: dli106

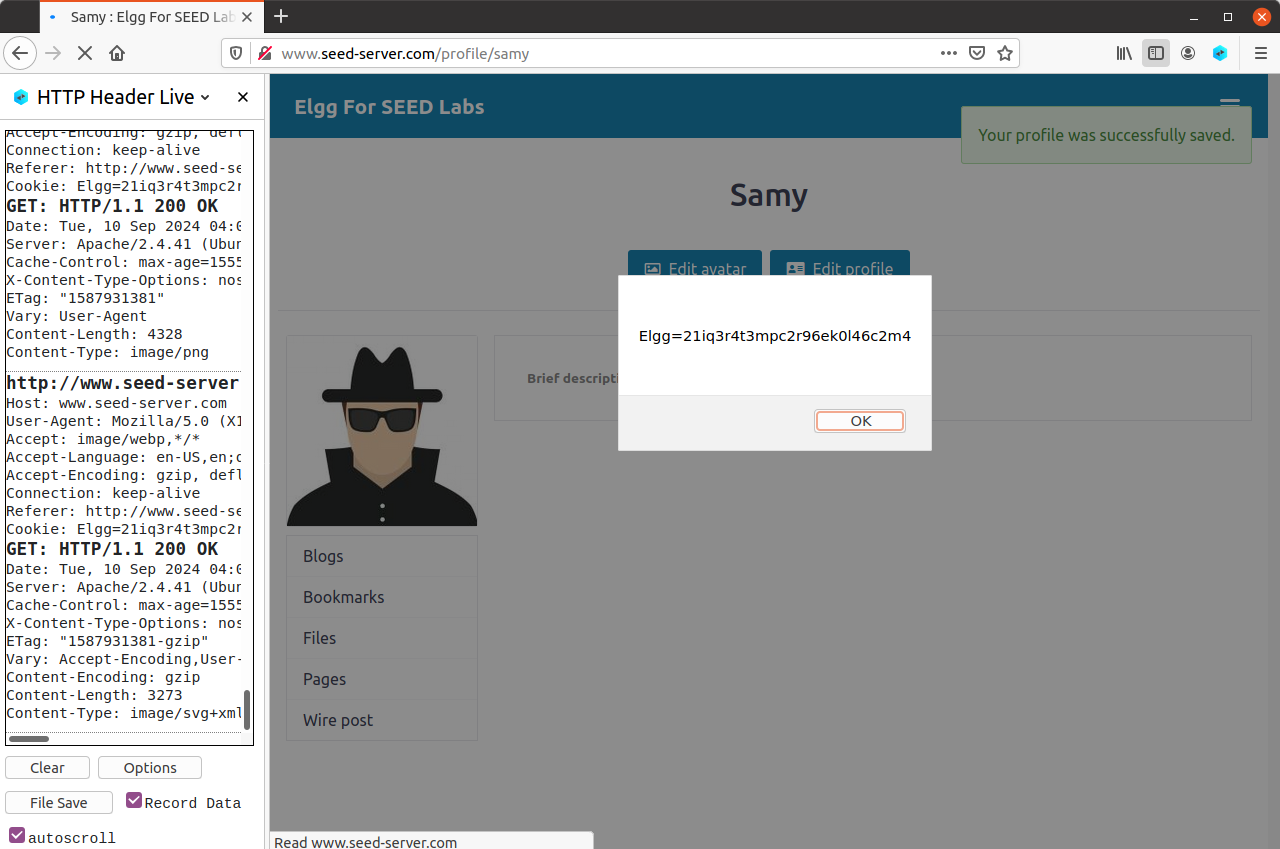
Task 1: Posting a Malicious Message to Display an Alert Window



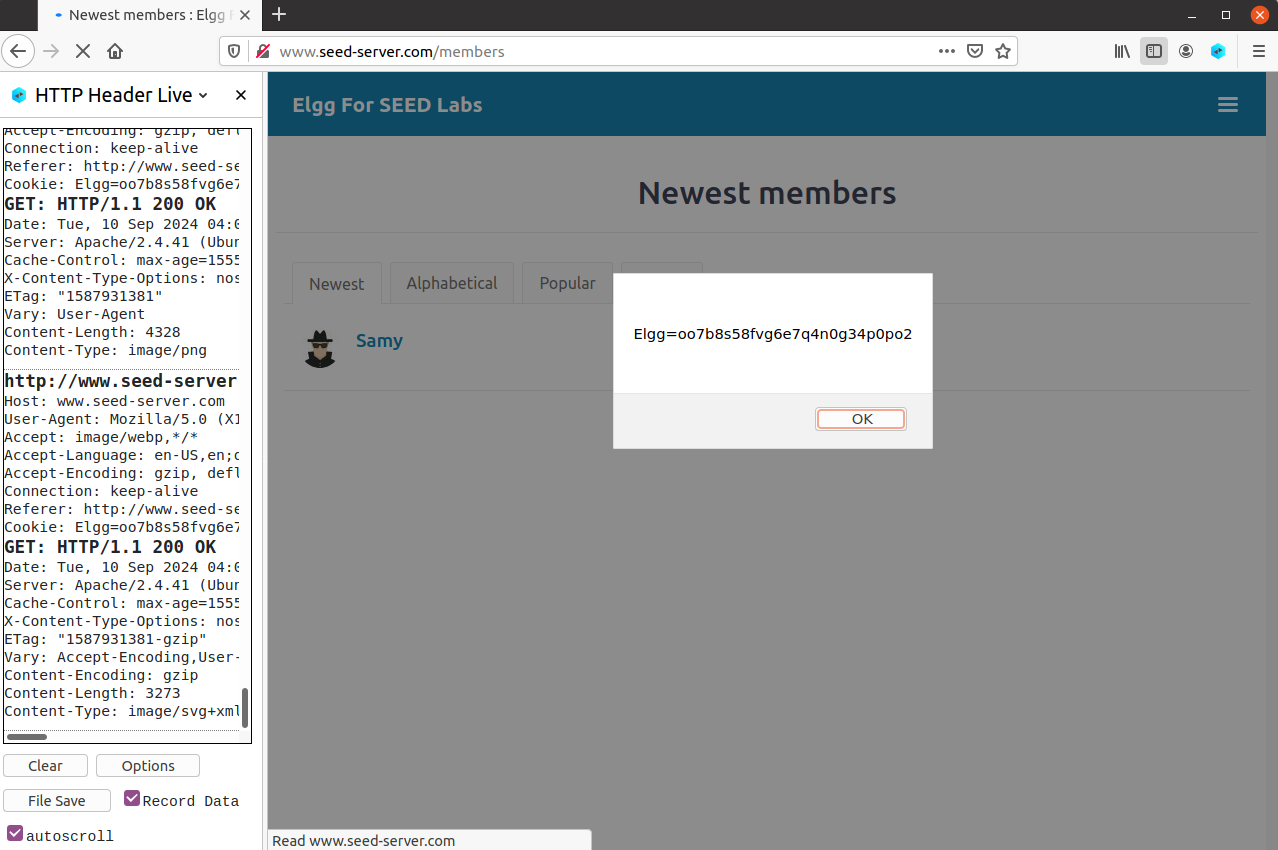
**Since the code is being added <script> the website will treat it as part of the website and run it, therefore everyone visits Samy’s profile page will see a XSS alert message.**

Task 2: Posting a Malicious Message to Display Cookies

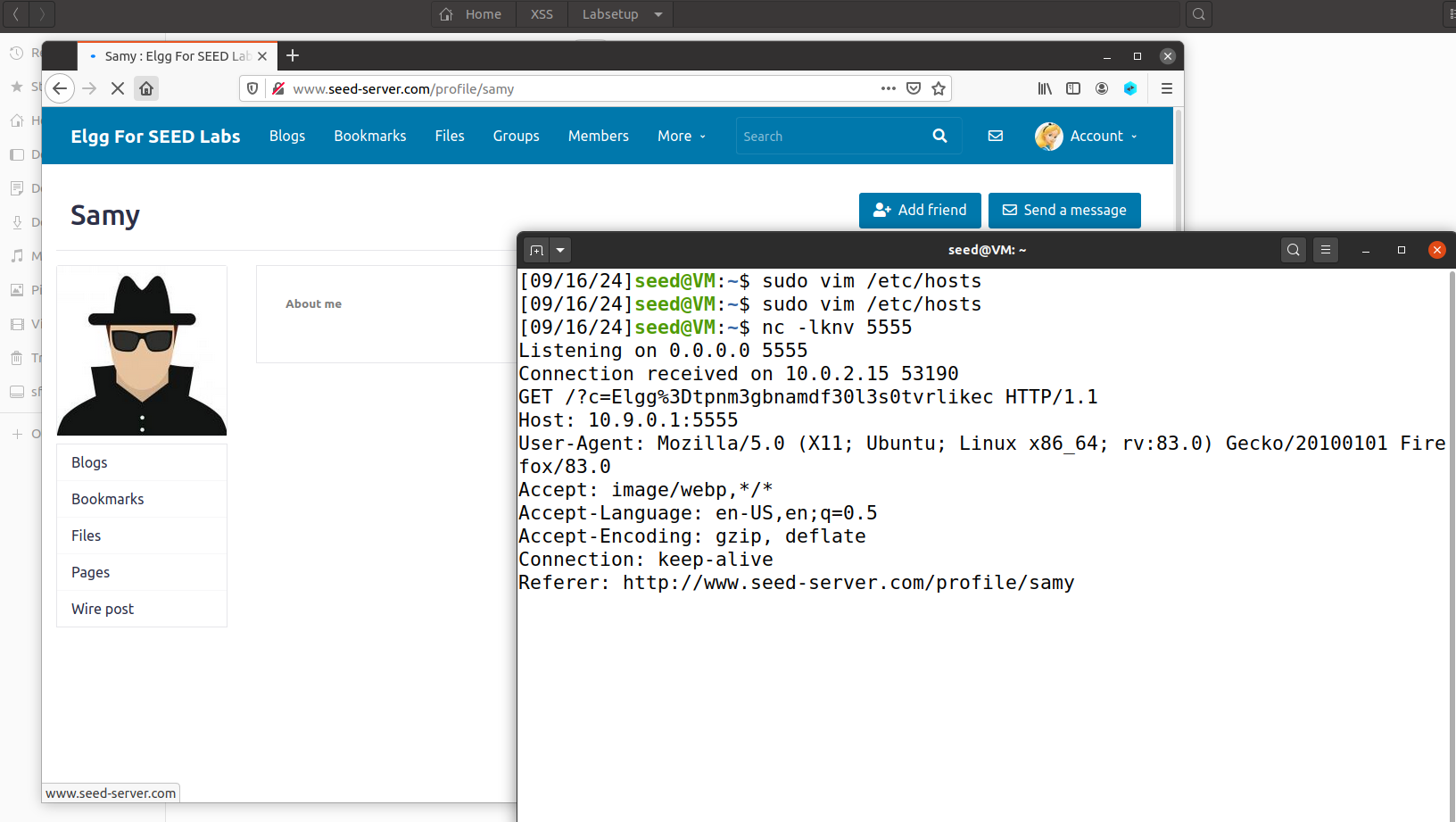
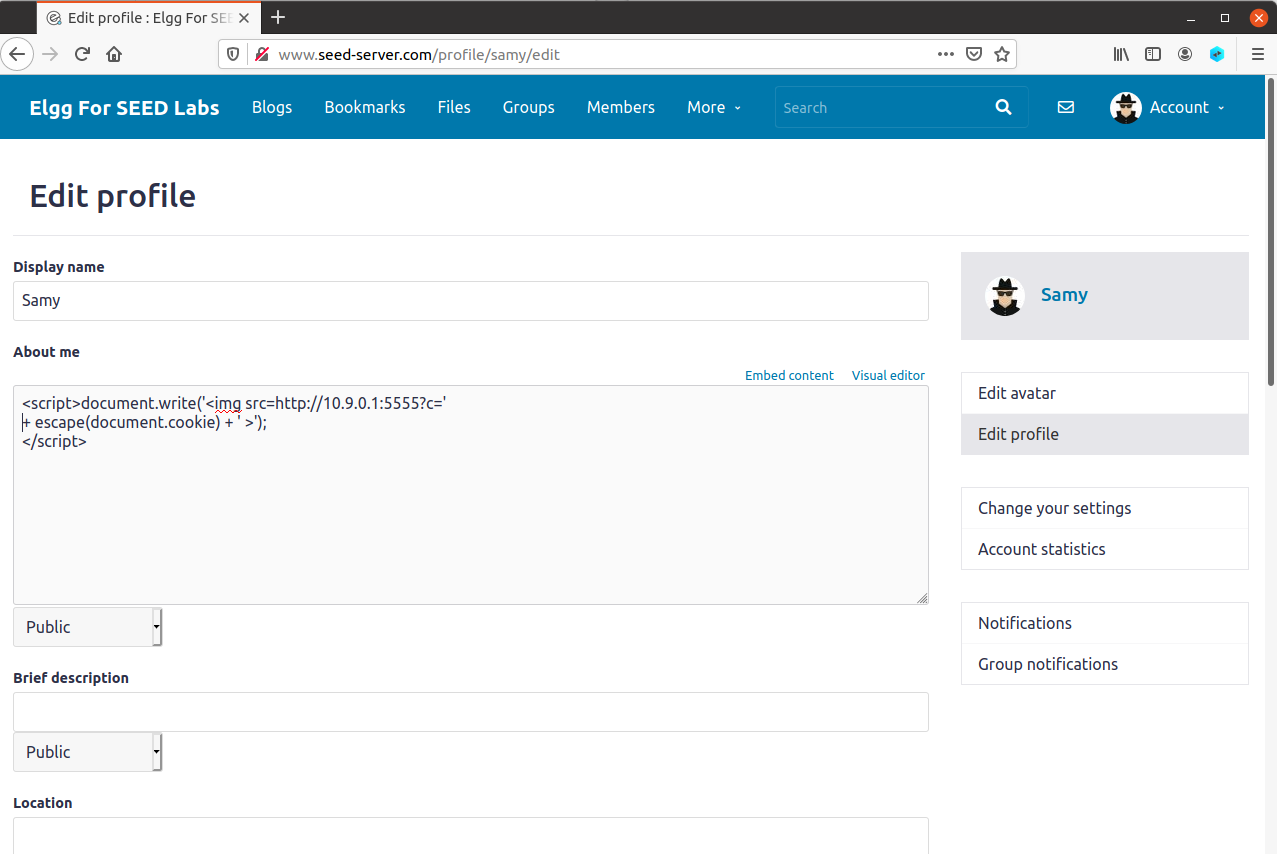
****

****

**Since the website treats the script message as code and run it, we can use document.cookie as a variable to display the visitor’s cookie. The second figure shows Samy’s cookie while it visits his own profile. Whereas Alcie vist Samy’s profile, the cookie displayed was completely different.**

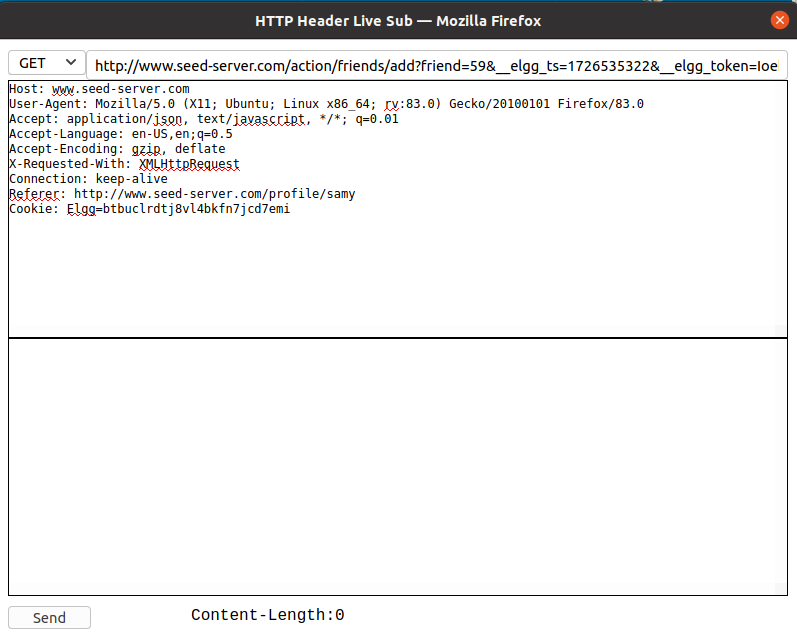
****

Task 3: Stealing Cookies from the Victim’s Machine

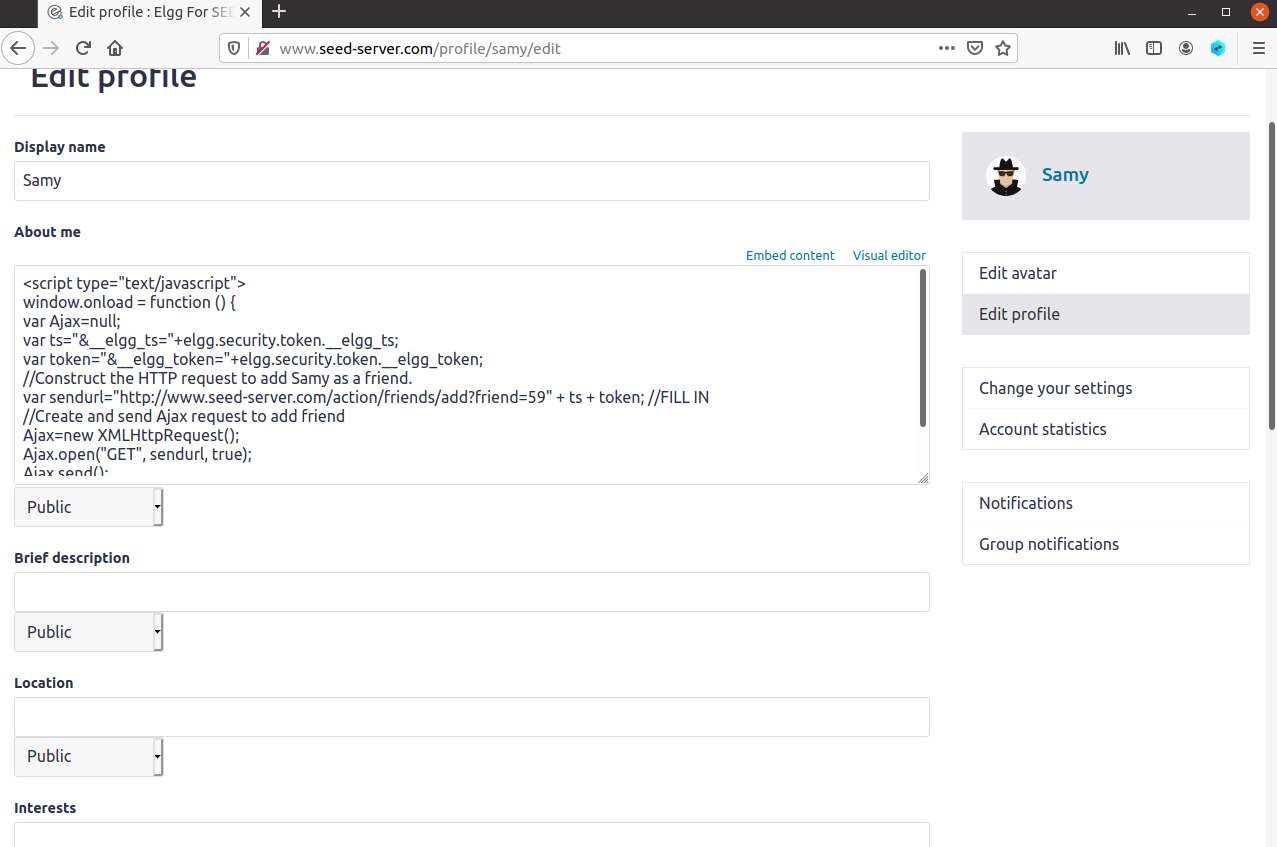
****

**For this task, instead of showing a message to the victim, the code is being used to store and show some visitor information to the attacker. As in Figure two when Alice visits Samy’s profile and the about me code gets run, the malicious code attached will save the cookie, and follow important information in the remote server 5555. Then the attacker can check anytime through the command nc -lknv 5555 to get those information.**

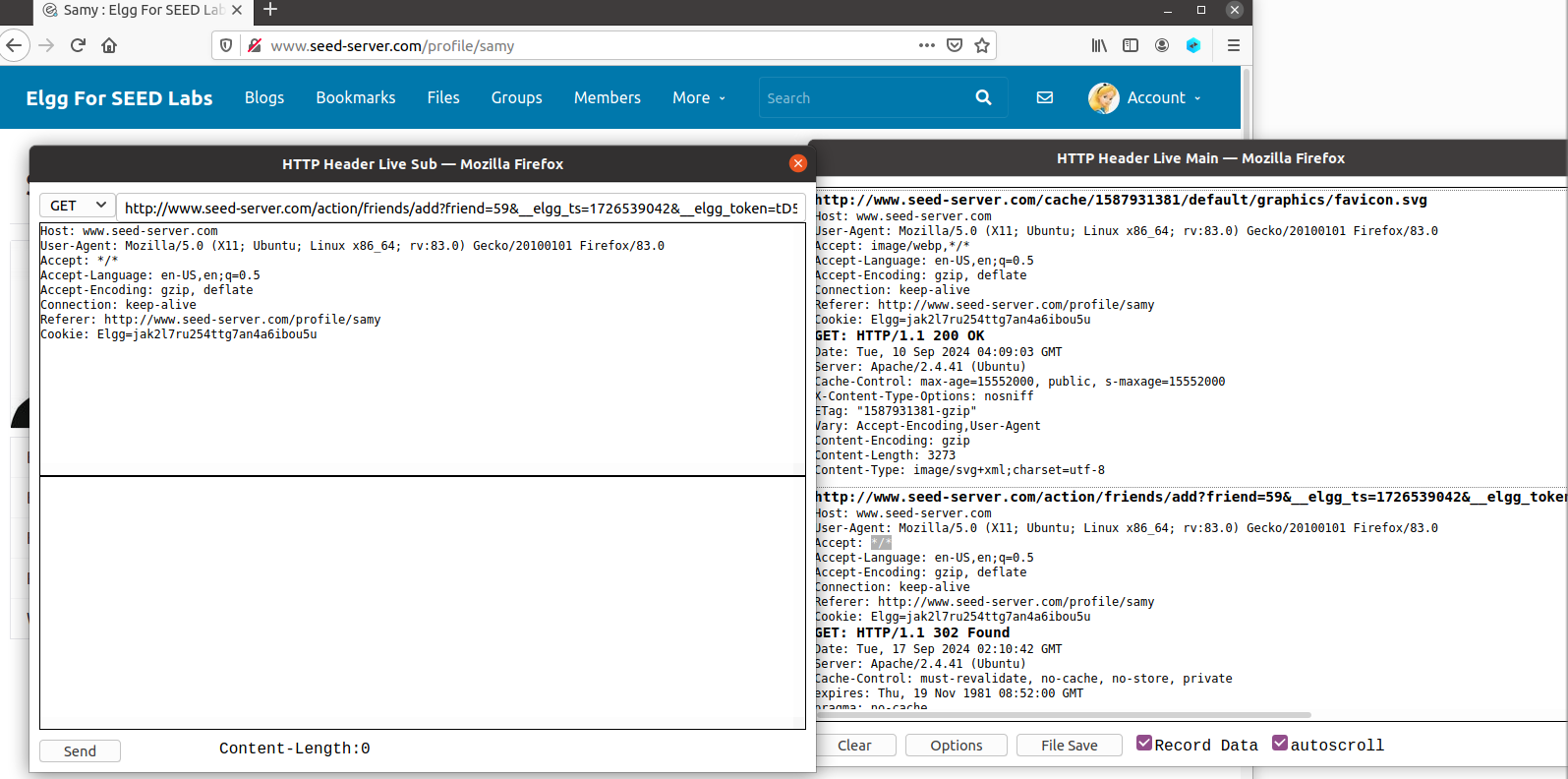
Task 4: Becoming the Victim’s Friend



<http://www.seed-server.com/action/friends/add?friend=59&__elgg_ts=1726535322&__elgg_token=Ioek0bLP475O43GAvfCUgw&__elgg_ts=1726535322&__elgg_token=Ioek0bLP475O43GAvfCUgw>



**from the add friend get request we can notice how the URL should looks like. Then we can edit it in the sendurl var in of out XSS malicious code in figure 2. Therefore when ever a victim visit Samy’s profile, the web page will run the script and the victim will add Samy as friend.**

****

**As shown in the figure above, the addfriend request is being run.**

Question 1: Explain the purpose of Lines ➀ and ➁, why are they are needed? •

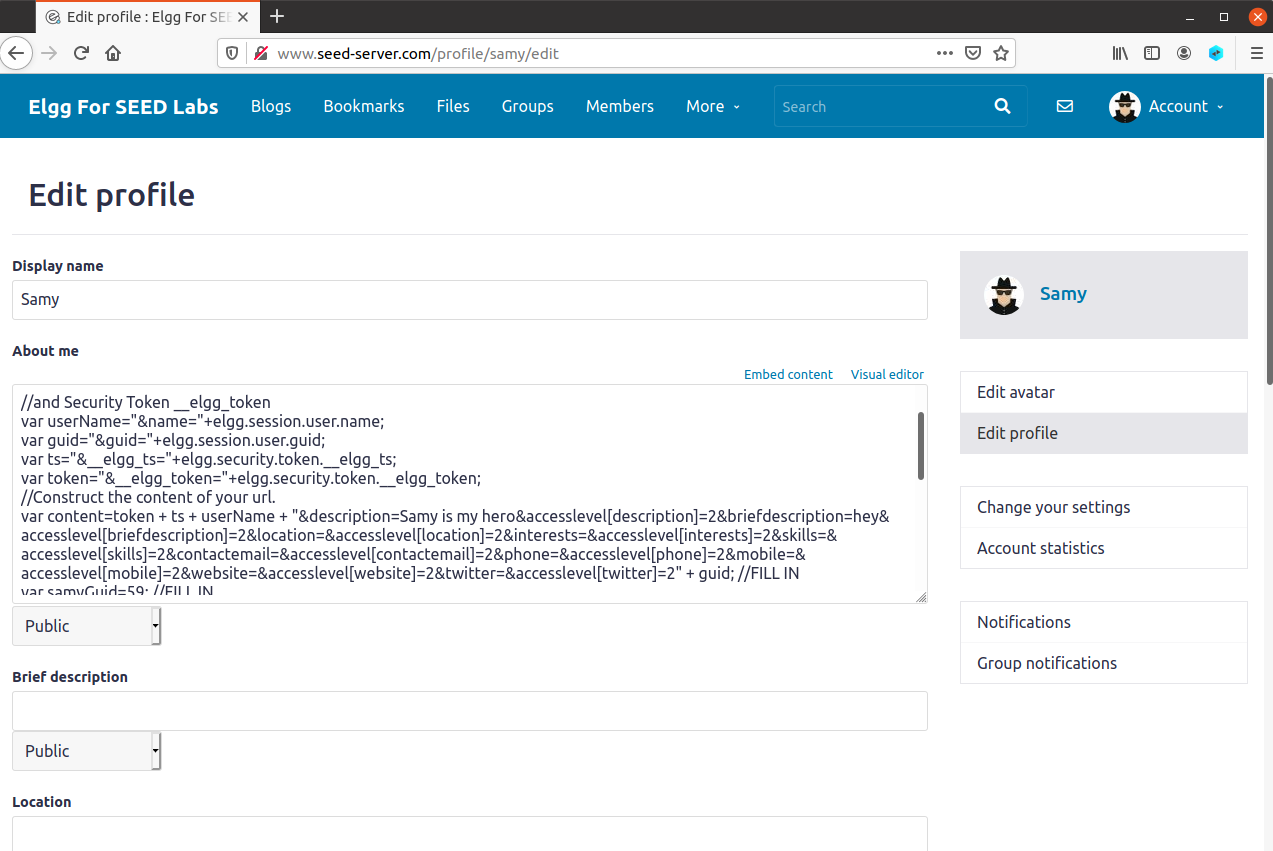
**Answer: the purpose of 1 and 2 is to get the ts and token of the victim who visited Sammy’s page. They are needed because the website will need the ts and token for verification when it launches the sent addfriend URL, if ts and token are missing, the website wont add Samy as a friend of the victim**

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?

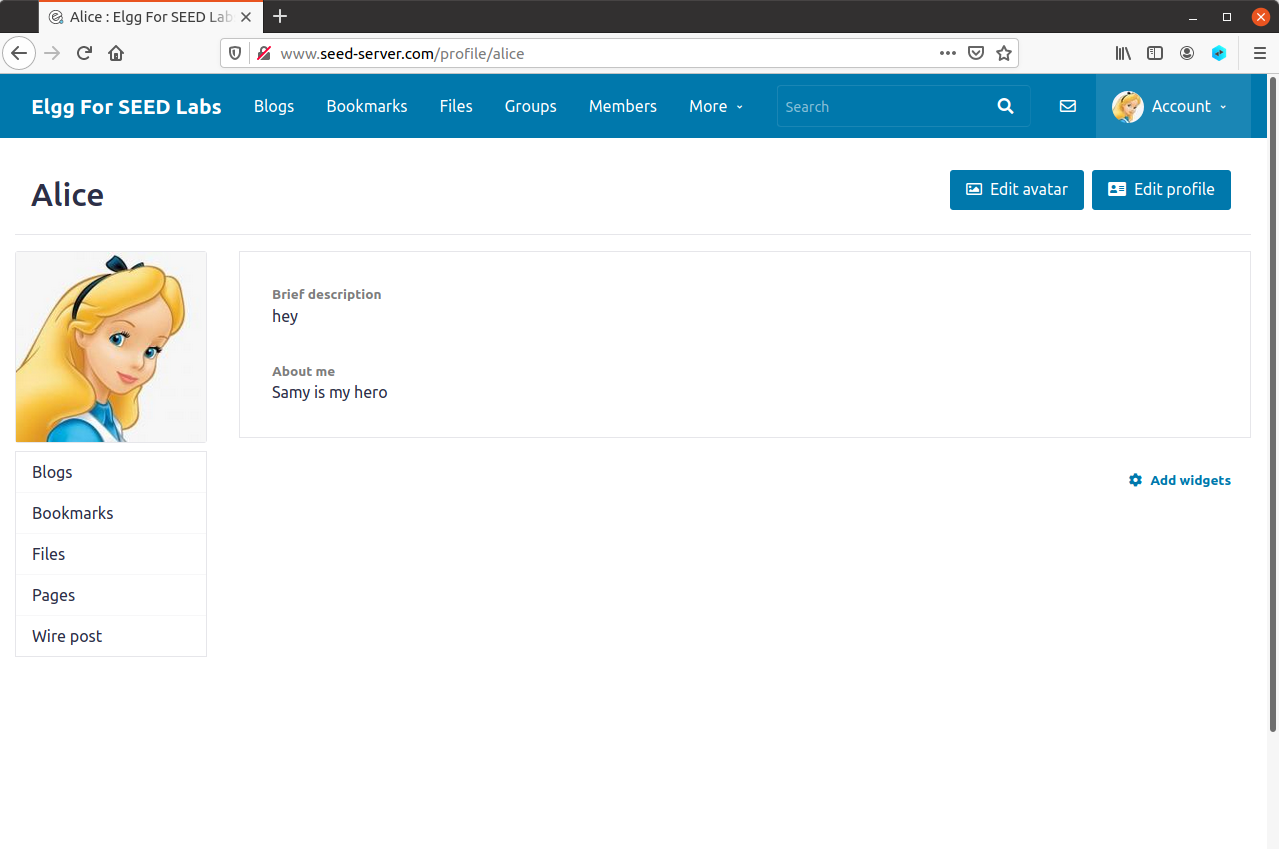
**Answer: The launch will fail with a high probability. because the editor mode will automatically add <p> at the beginning and end of the text attributed, therefore, the malicious code will be treated as a text instead of a script code.**

Task 5: Modifying the Victim’s Profile

\_\_elgg\_token=XzSvrN4dAnaQyjhpl0x7kw&\_\_elgg\_ts=1726539561&name=Samy&description=&accesslevel[description]=2&briefdescription=hey&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&interests=&accesslevel[interests]=2&skills=&accesslevel[skills]=2&contactemail=&accesslevel[contactemail]=2&phone=&accesslevel[phone]=2&mobile=&accesslevel[mobile]=2&website=&accesslevel[website]=2&twitter=&accesslevel[twitter]=2&guid=59



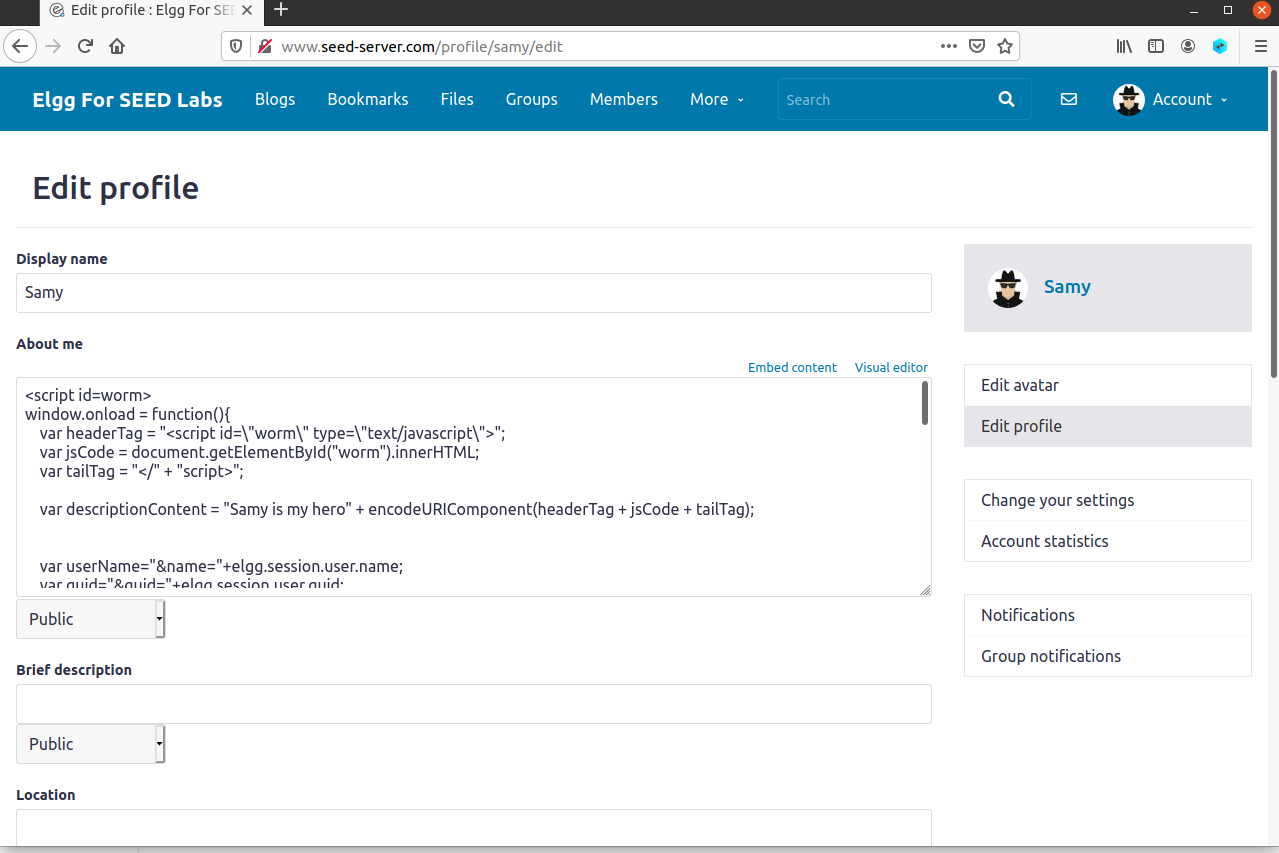
**As the string shown above says the post request content for edit profile look like this. By this we know the content are in form of token + ts + userName + description content + guid. After fill in the XSS code in Samy’s about me part, when a victim visit Samy’s profile, the victim’s about me page will change.**

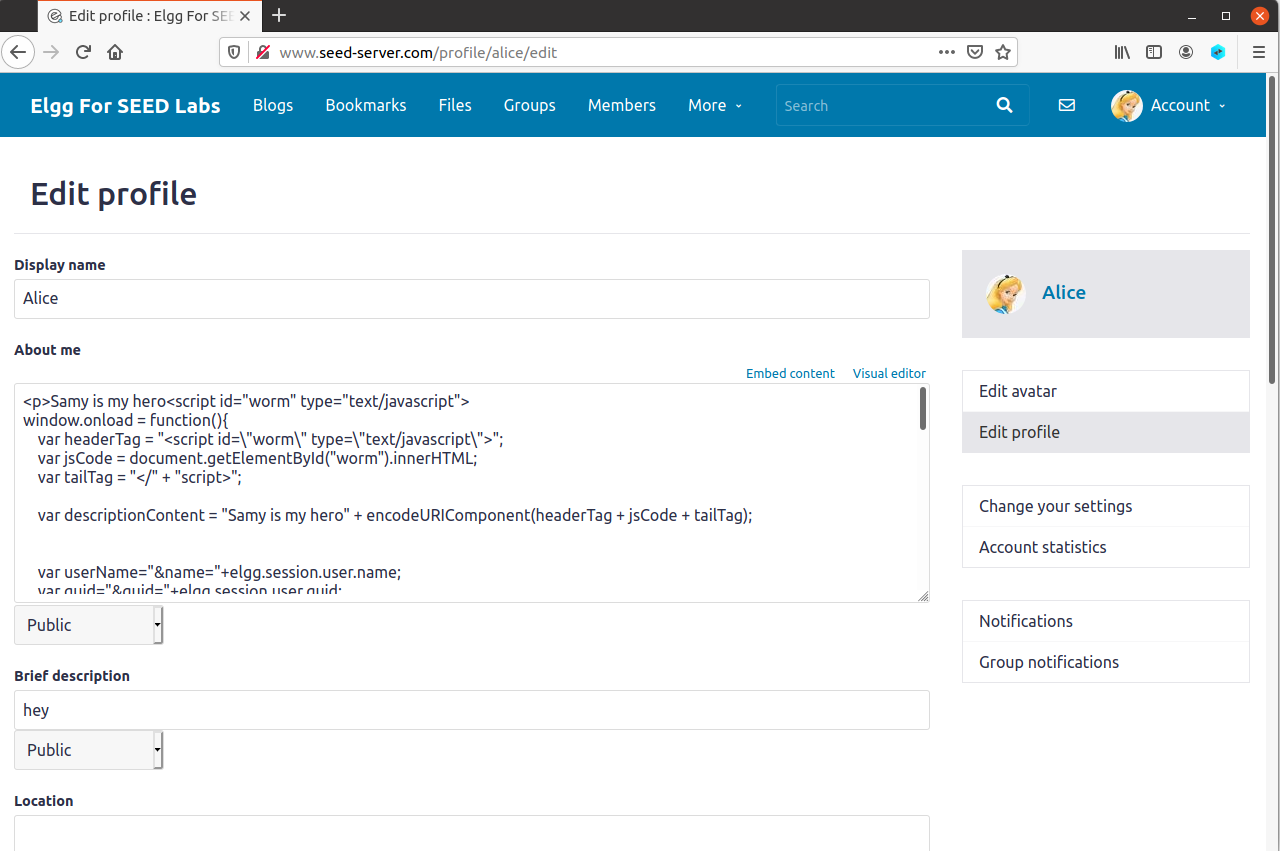
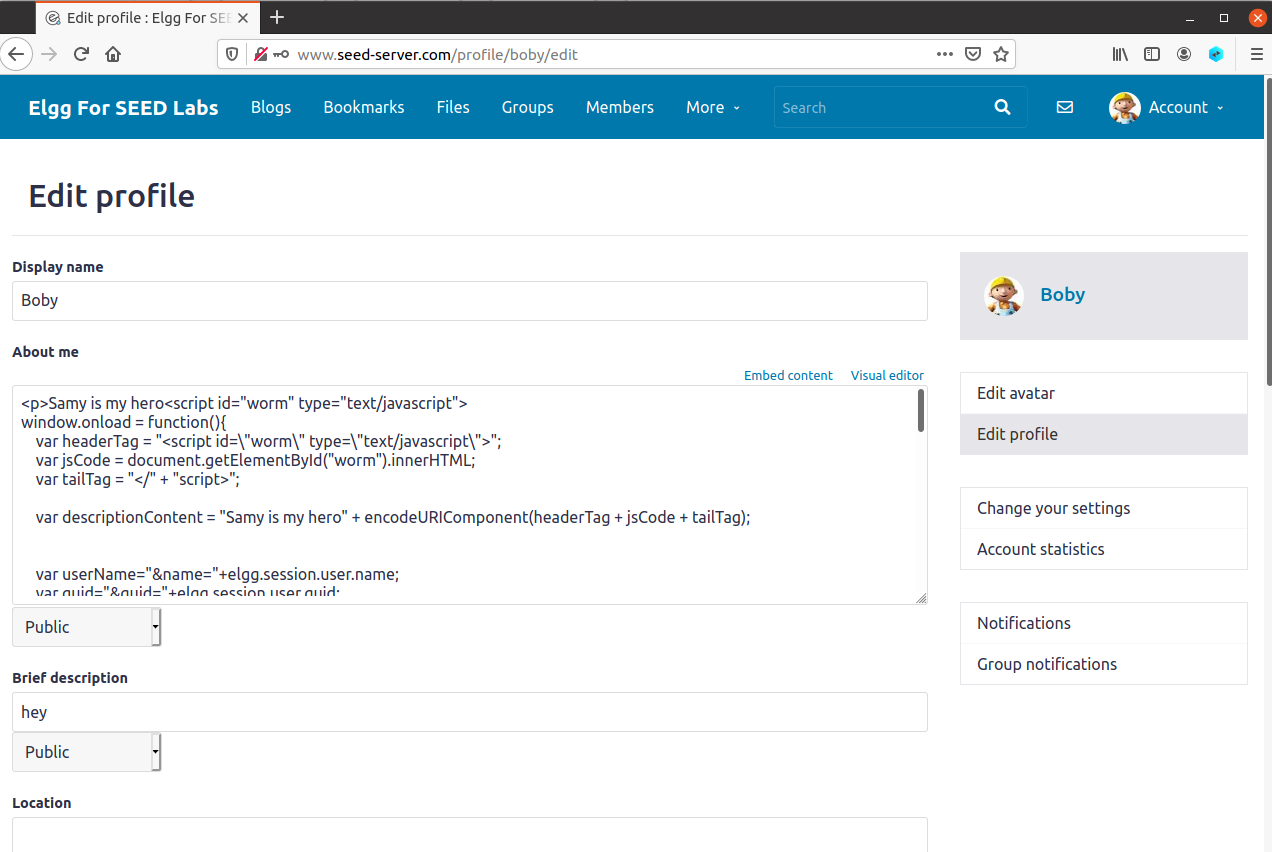


Question 3: Why do we need Line ➀? Remove this line, and repeat your attack. Report and explain your observation.

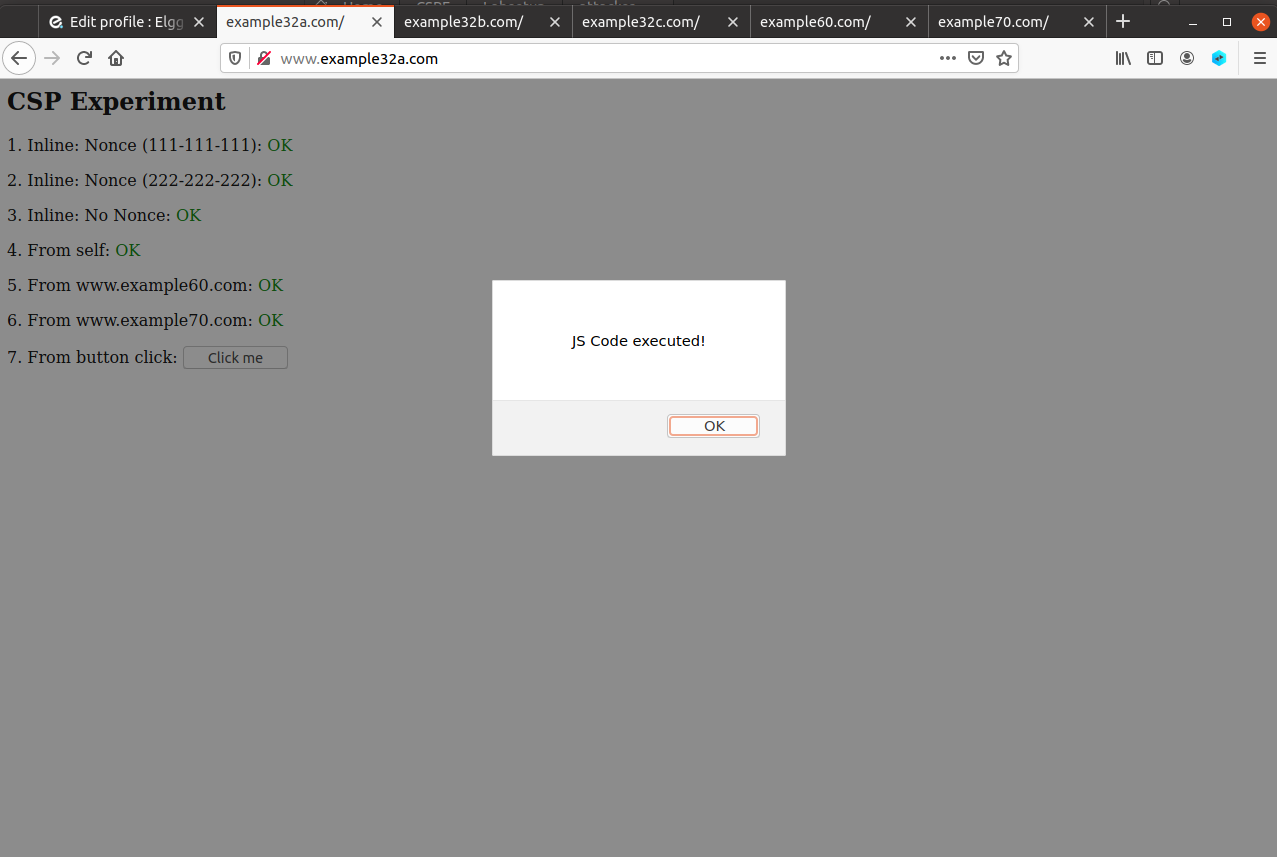
**since the XSS worm is not self propagating, without this line of code when samy himself access his profile page, his about me page will being edited, the XSS attack will not work anymore.**

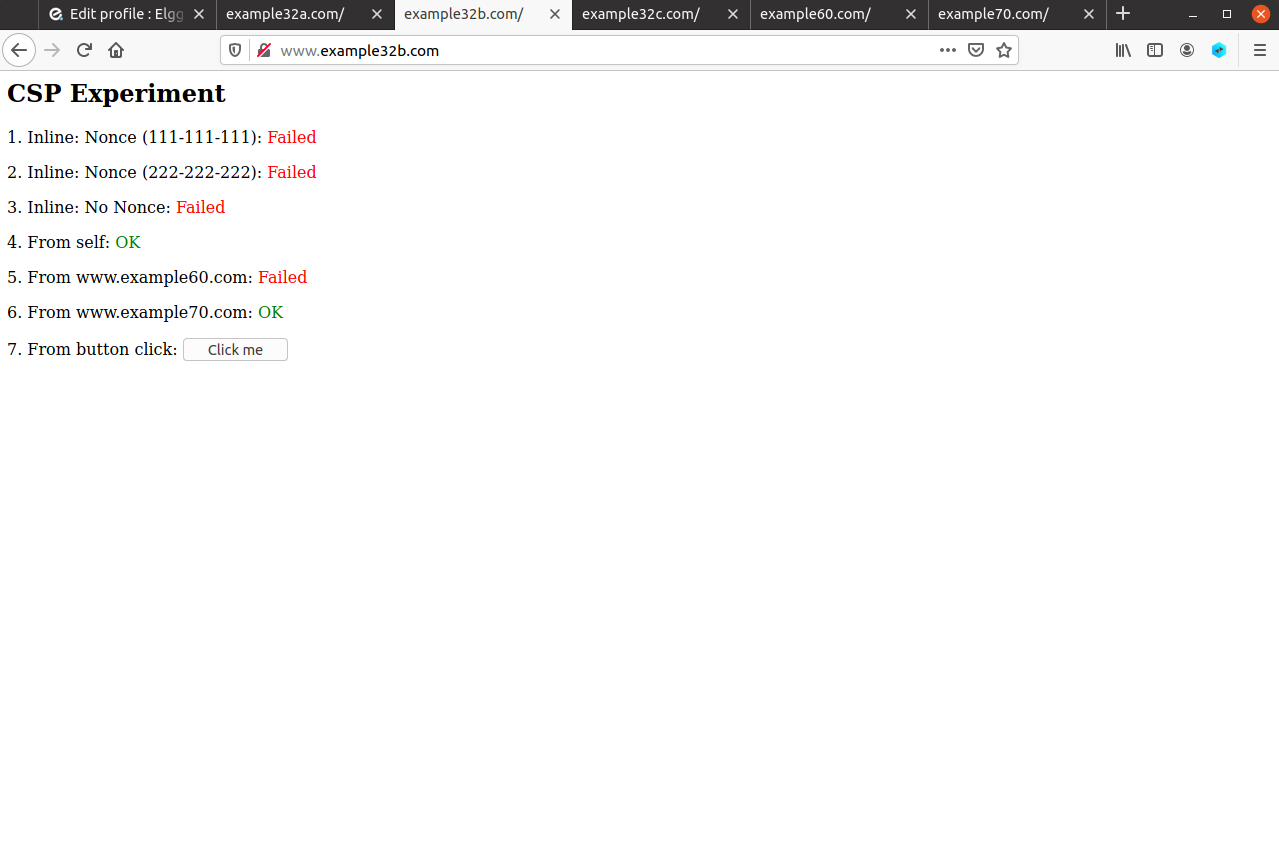
Task 6: Writing a Self-Propagating XSS Worm

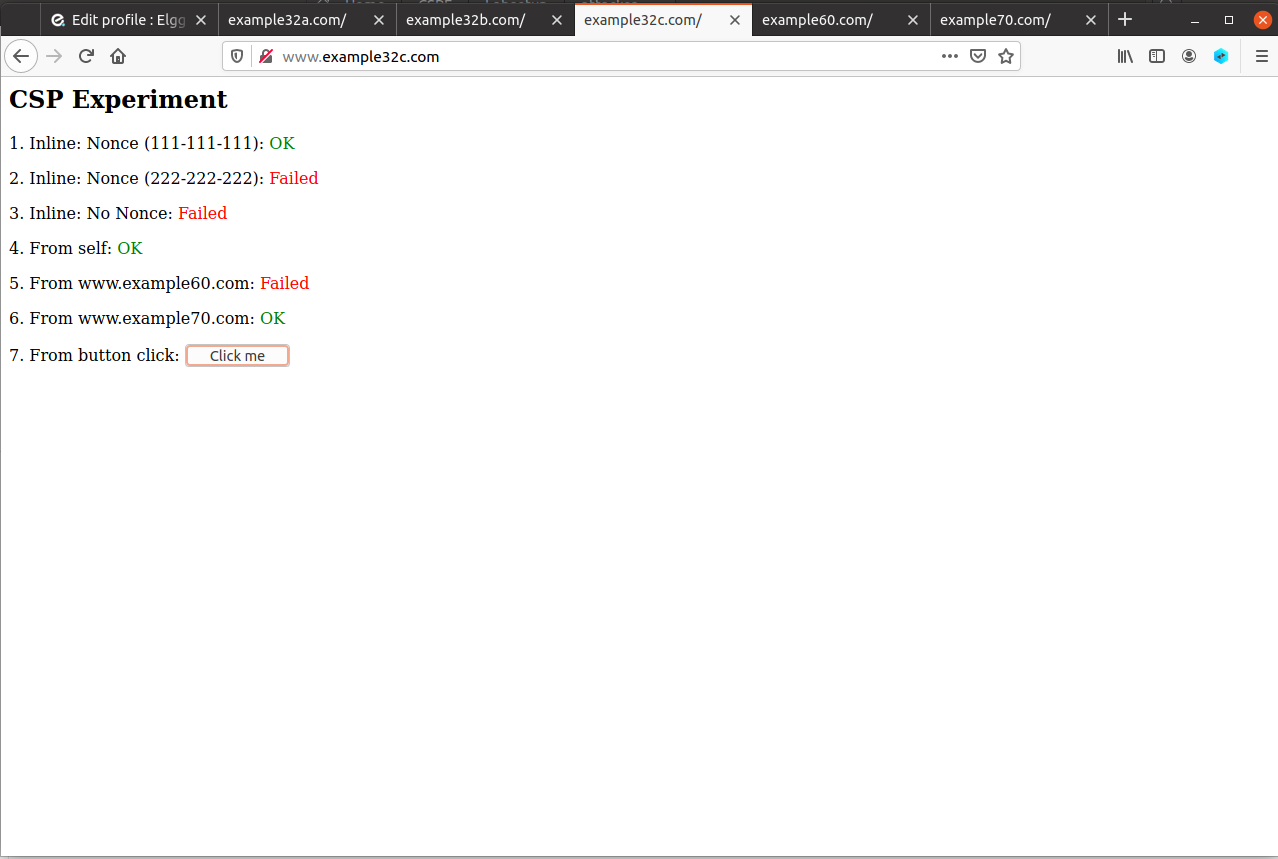


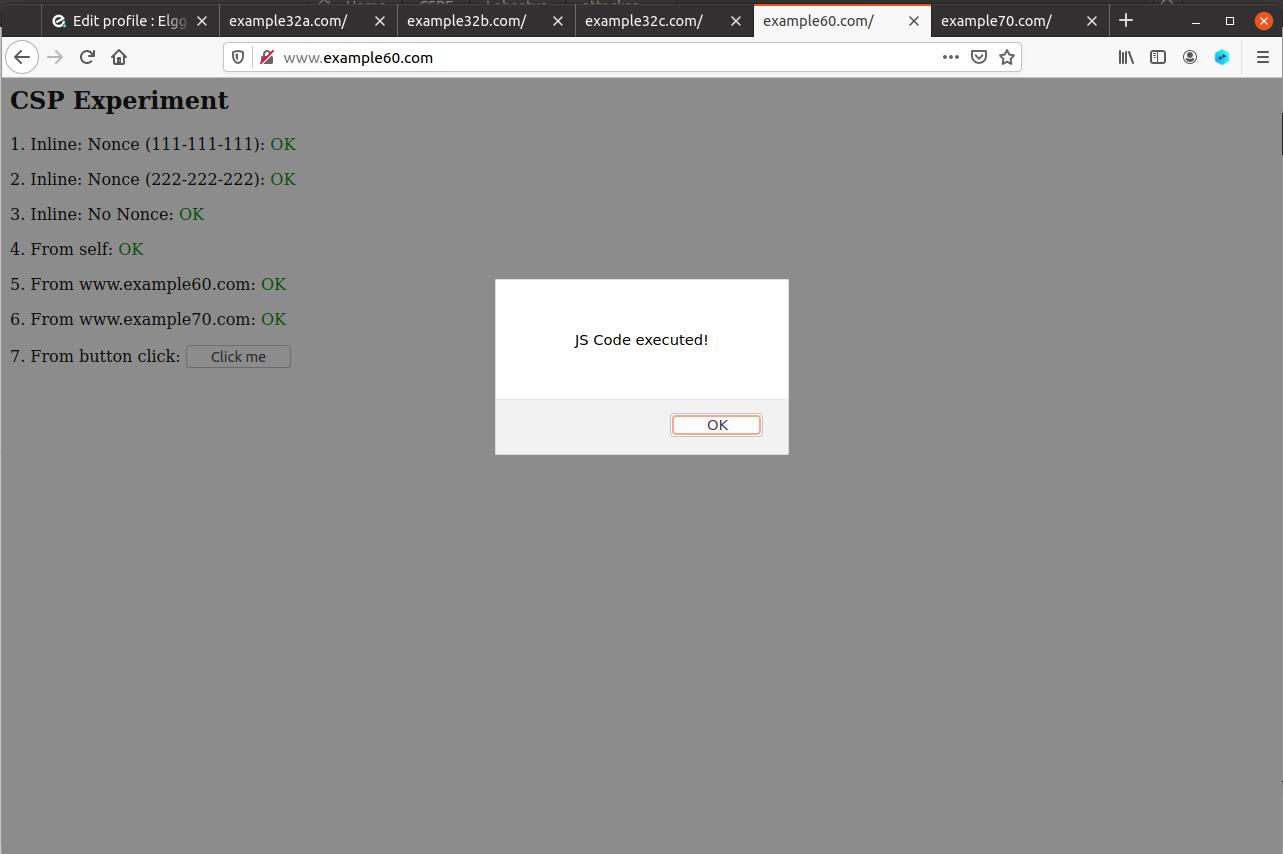
**As shown in the figure, i wrote a self propagating XSS Worm using DOM, by this i simple use header tag and tailtag to write the edit profile XSS Worm, as you can see after visiting Samy’s profile, Alice’s profile being edited, and then when boby visit Alice’s profile, his profile got edited as well.**  

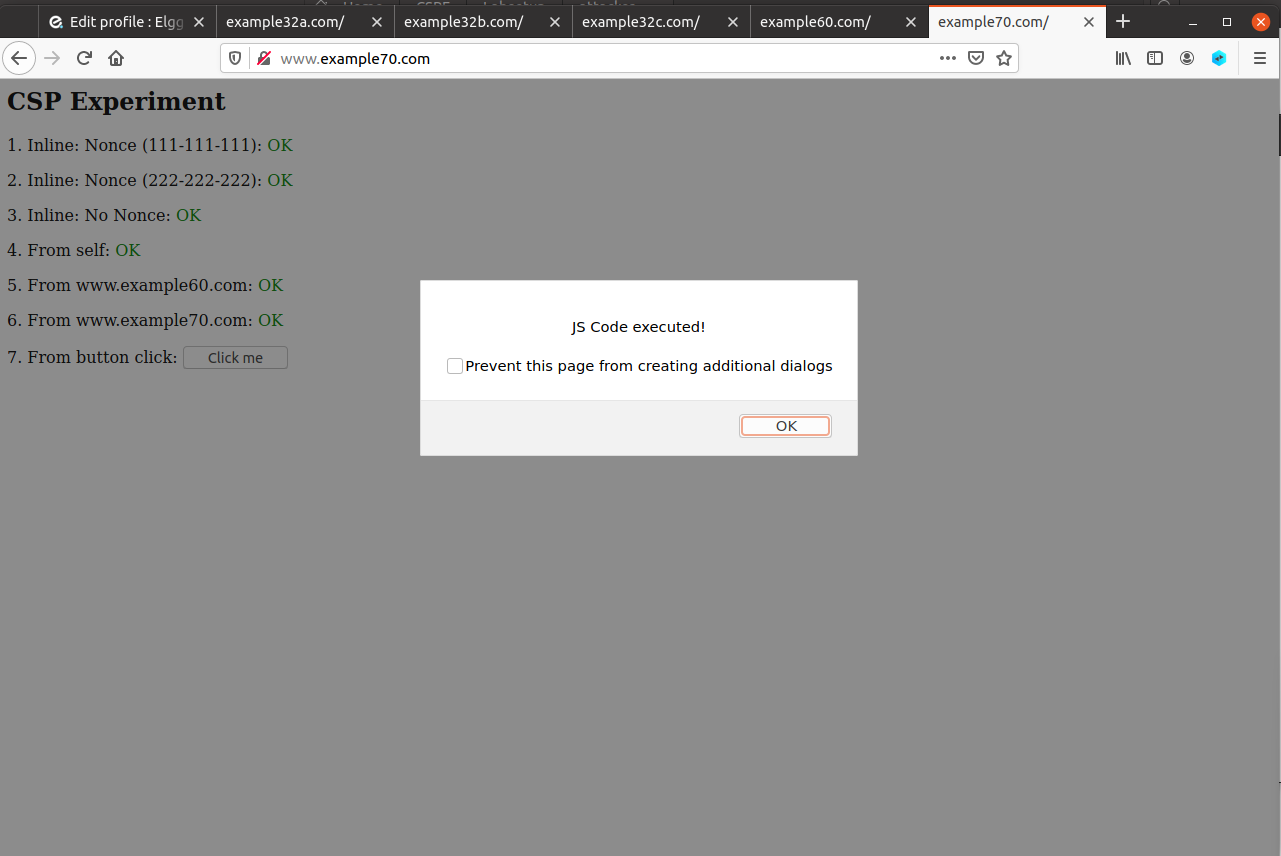
Task 7: Defeating XSS Attacks Using CSP











1. Describe and explain your observations when you visit these websites.

**Different websites display the content based on their only CSP policies. This is because their own CSP policies prevent certain form of text or information from certain website being displayed**

1. 2. Click the button in the web pages from all the three websites, describe and explain your observations.

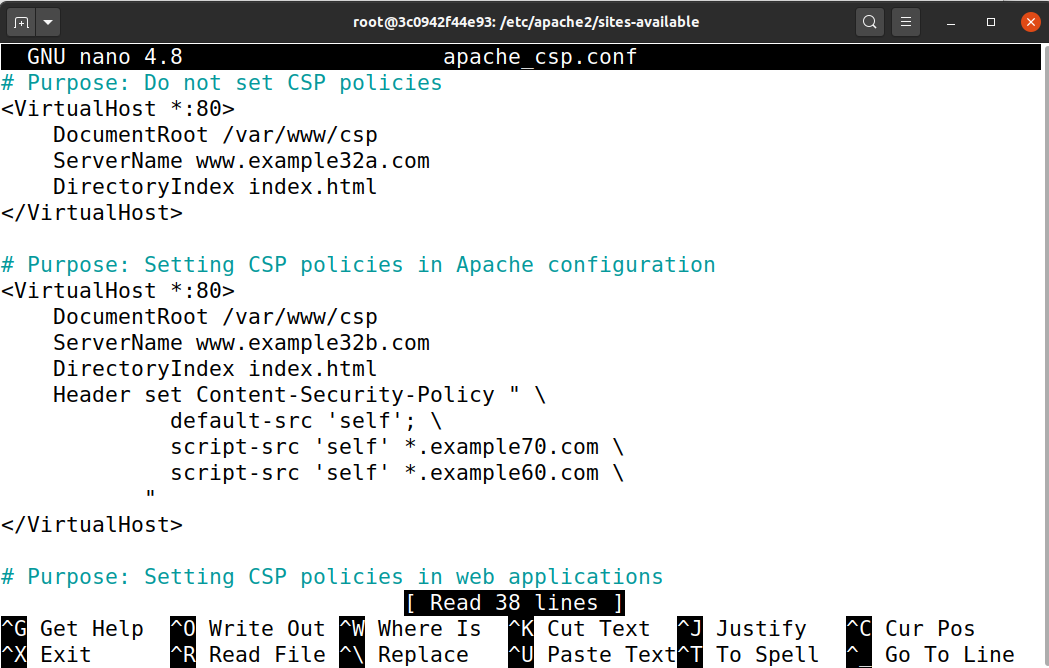
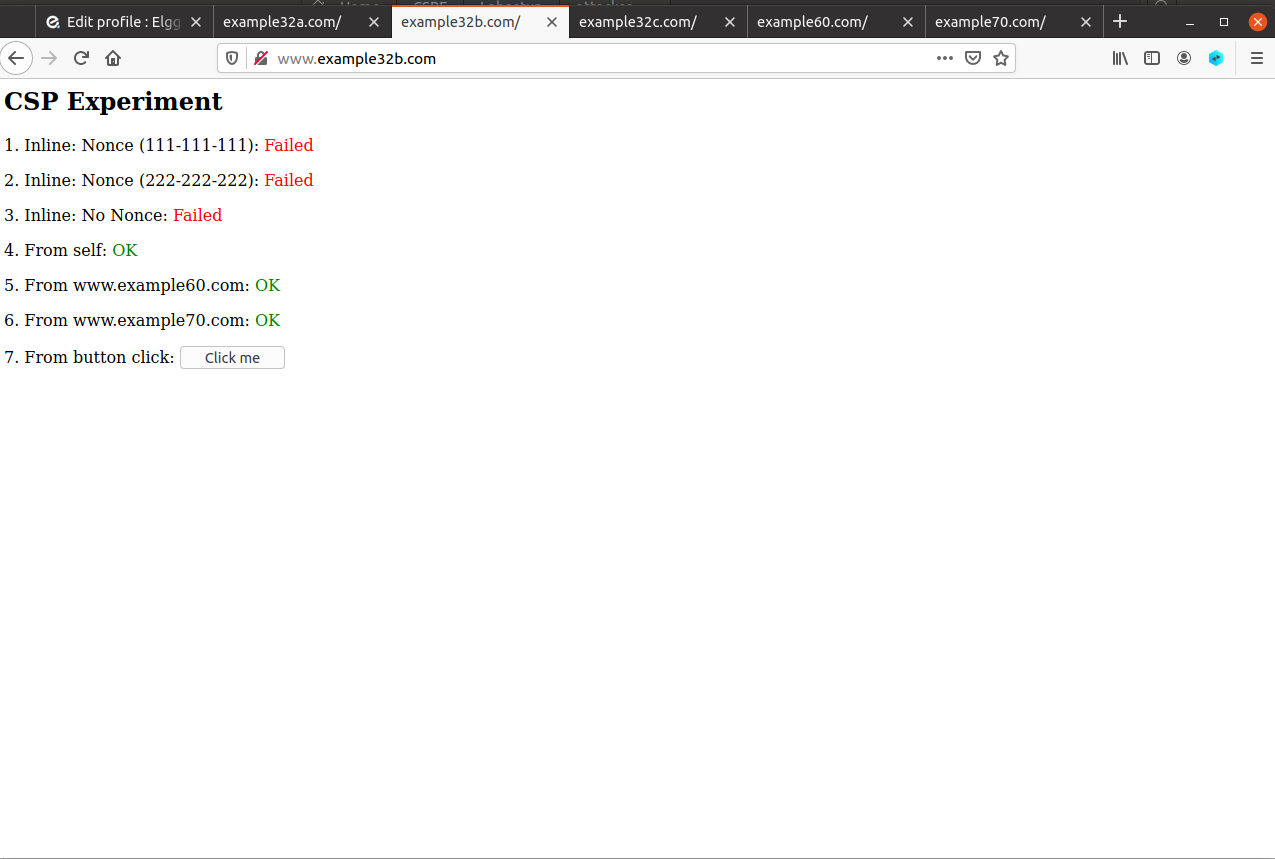
**Only Example32b and example32c can not pop out click button. In phpindex.php**

**For example 32a, it follows the index.html policy and shows the thing clearified in the html**

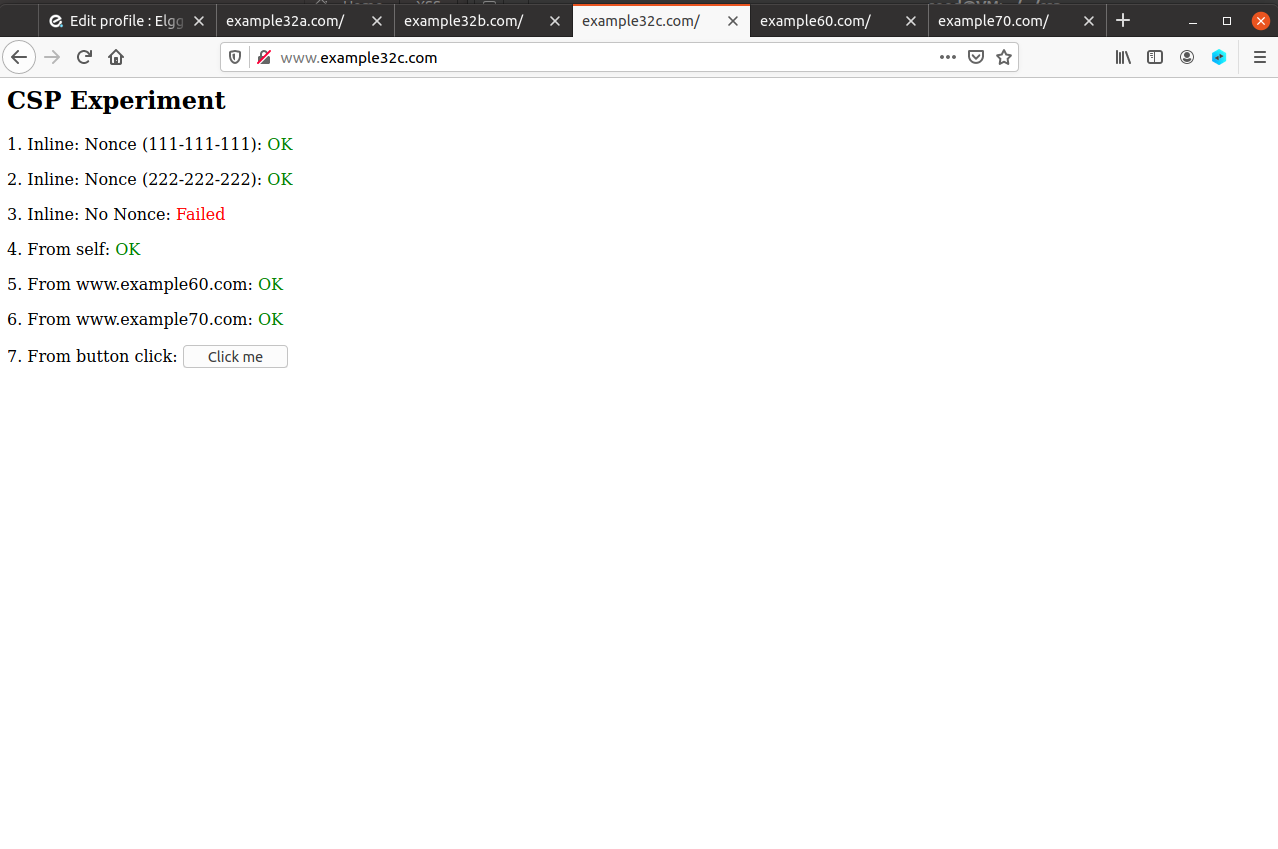
**For example32b, although it follows the index.html at first but it then clarify a header set content security policy which repla the index that include a button click policy. So it do not contain a button. For example32c it do not contain a button click policy at the beginning, so there is no reaction when click the cutton.**

**For example60 and example 70, since there is no policy clearified, the button will then display what in has been designed to show.**

1. Change the server configuration on example32b (modify the Apache configuration), so Areas 5 and 6 display OK. Please include your modified configuration in the lab report.



1. Change the server configuration on example32c (modify the PHP code), so Areas 1, 2, 4, 5, and 6 all display OK. Please include your modified configuration in the lab report.





1. Please explain why CSP can help prevent Cross-Site Scripting attacks.

CSP helps website operators prevent certain malicious headers or even malicious websites. This will effectively prevent XSS attacks. Because operators are in a relatively initiative position prevent possible risks.