CSS337 Final Project

**Cross-site Scripting (XSS) and Web Hacking**

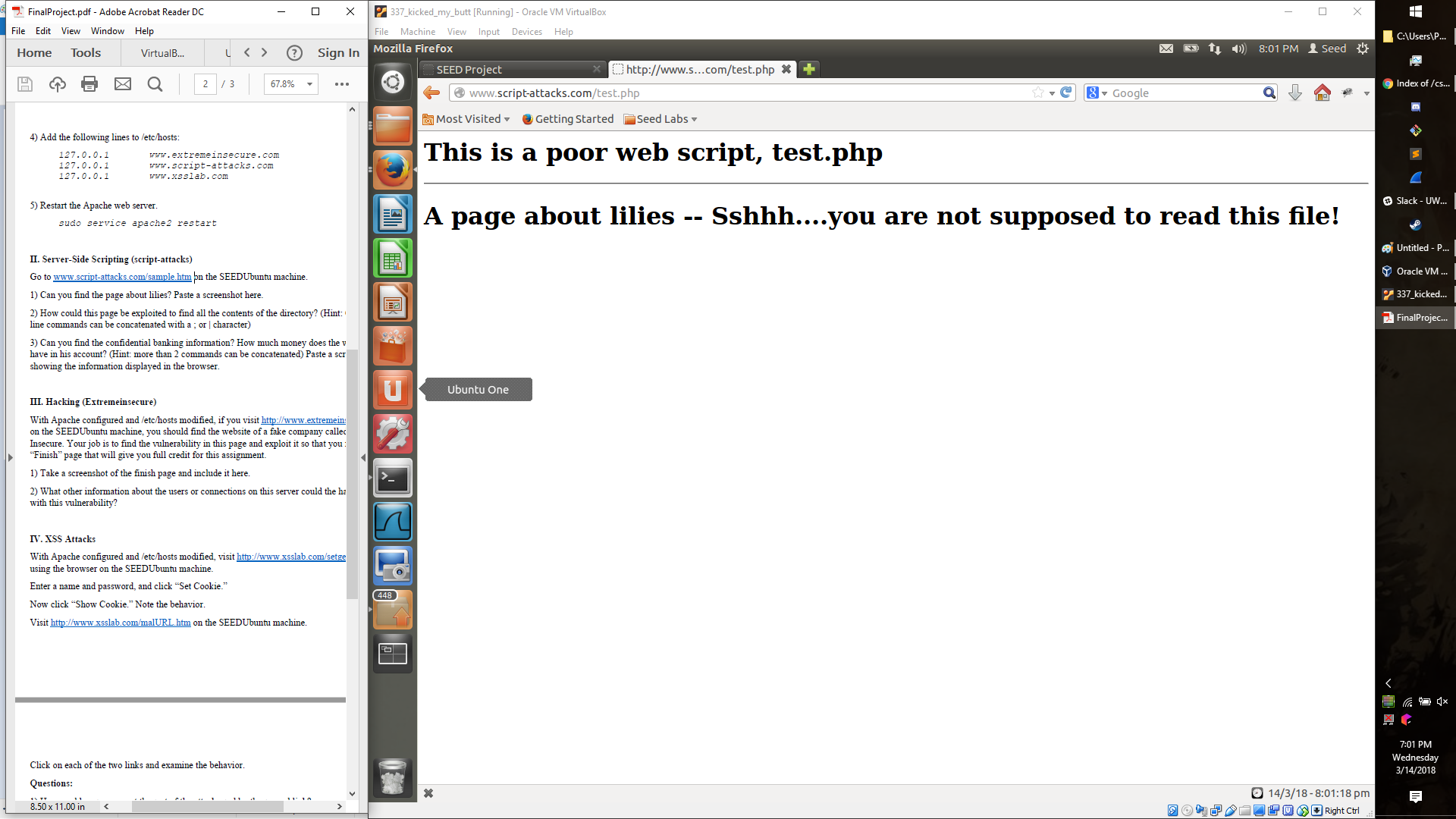
**I. SETUP:**

Yup, did it 😉

**II. Server-Side Scripting (script-attacks)**

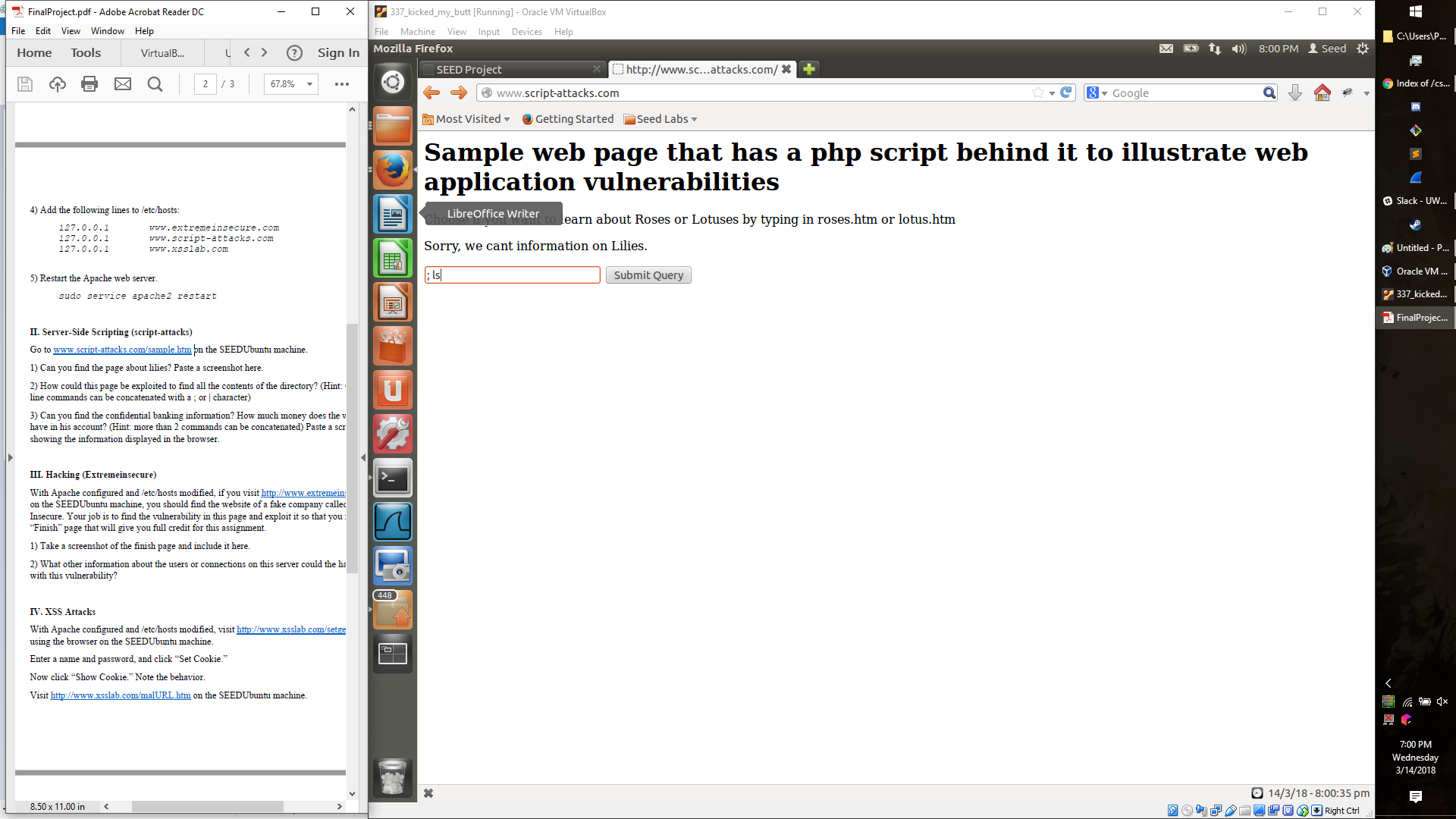
Go to www.script-attacks.com/sample.htm on the SEEDUbuntu machine.

1) Can you find the page about lilies? Paste a screenshot here.

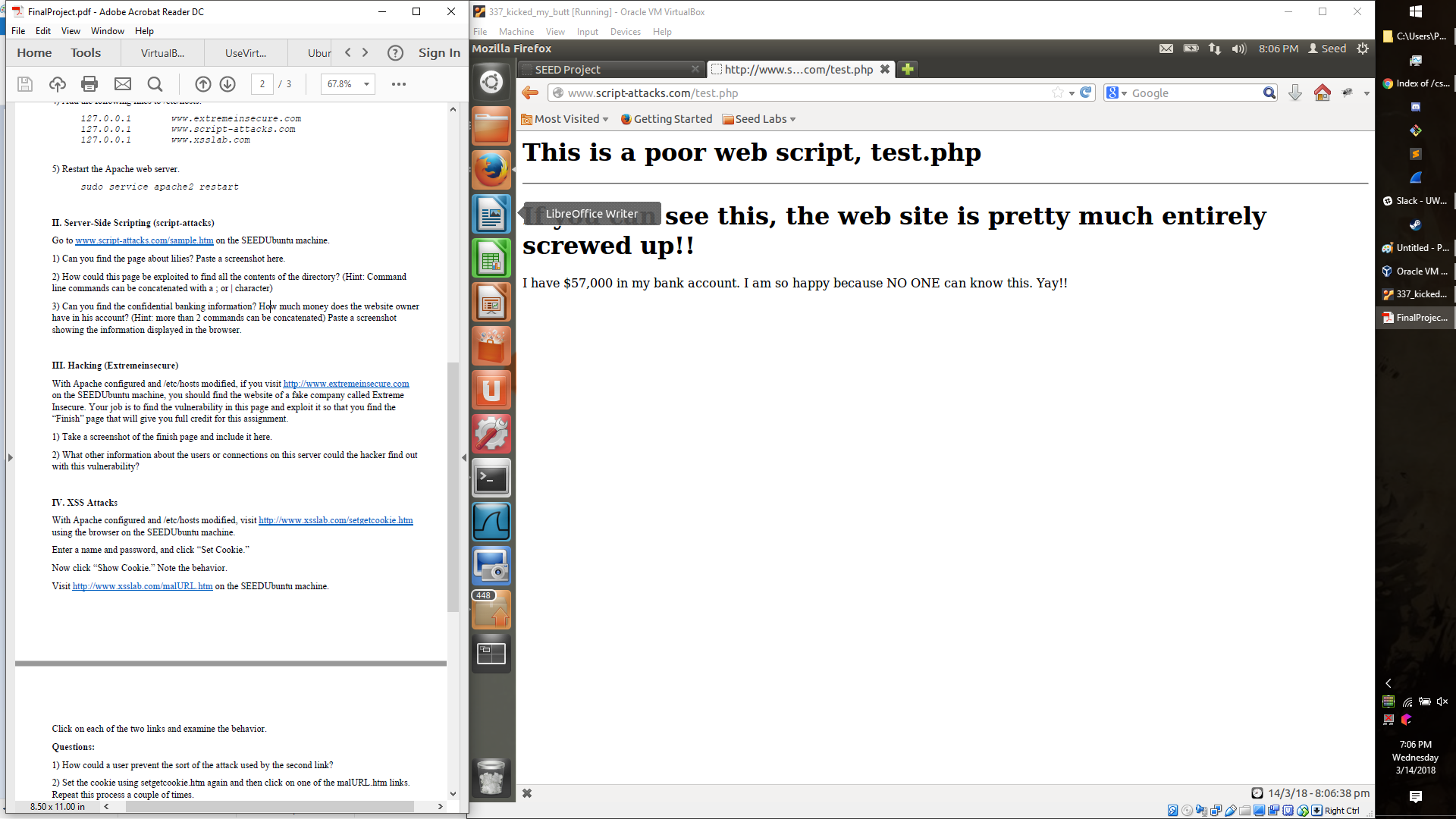


2) How could this page be exploited to find all the contents of the directory? (Hint: Command

line commands can be concatenated with a ; or | character)



3) Can you find the confidential banking information? How much money does the website owner have in his account? (Hint: more than 2 commands can be concatenated) Paste a screenshot showing the information displayed in the browser.



**III. Hacking (Extremeinsecure)**

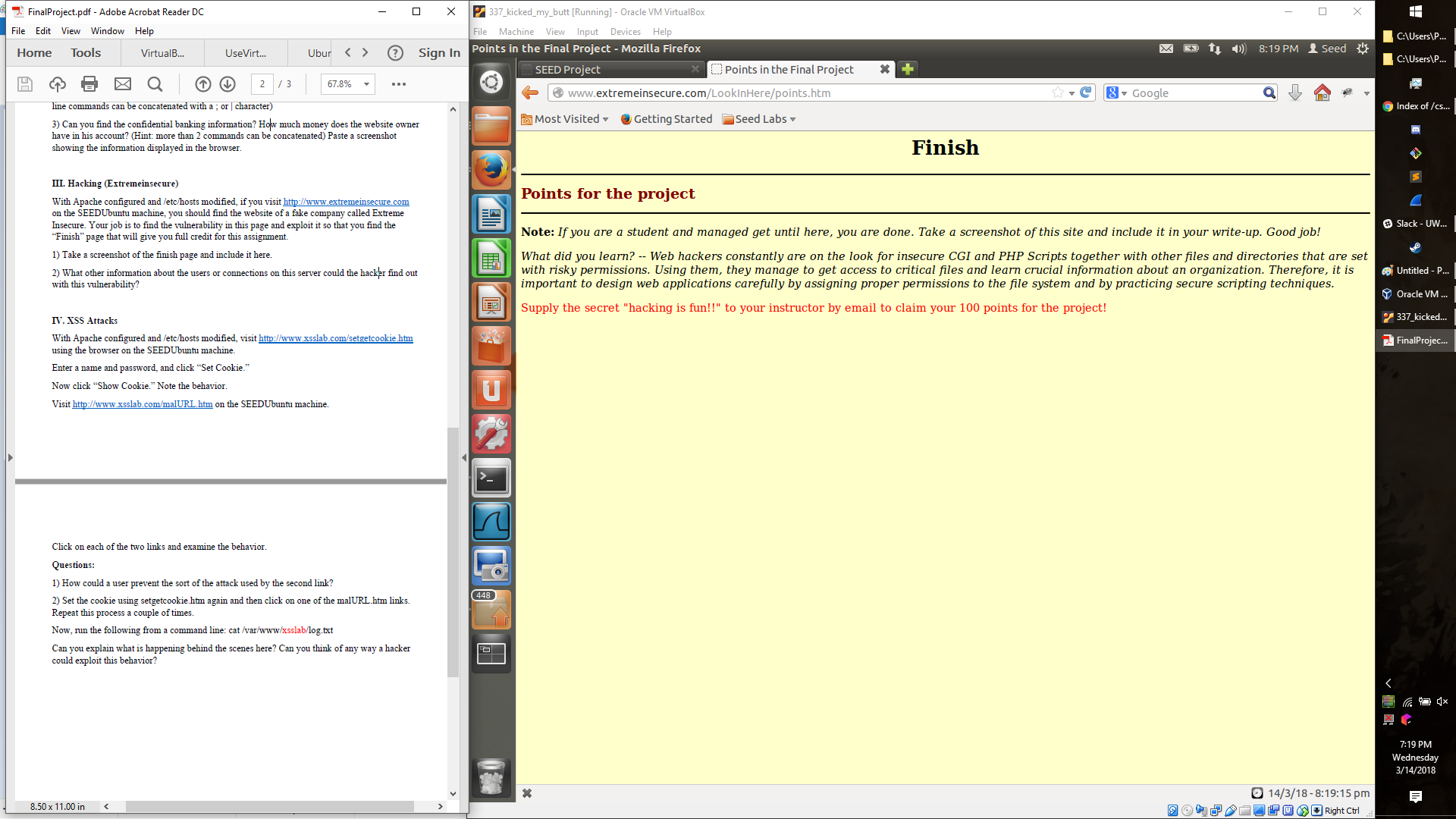
With Apache configured and /etc/hosts modified, if you visit http://www.extremeinsecure.com

on the SEEDUbuntu machine, you should find the website of a fake company called Extreme

Insecure. Your job is to find the vulnerability in this page and exploit it so that you find the

“Finish” page that will give you full credit for this assignment.

1) Take a screenshot of the finish page and include it here.



2) What other information about the users or connections on this server could the hacker find out

with this vulnerability?

Anything that the user or workstation that is running the webserver has or can see.

**IV. XSS Attacks**

With Apache configured and /etc/hosts modified, visit http://www.xsslab.com/setgetcookie.htm

using the browser on the SEEDUbuntu machine.

Enter a name and password, and click “Set Cookie.”

Now click “Show Cookie.” Note the behavior.

Visit http://www.xsslab.com/malURL.htm on the SEEDUbuntu machine.

Click on each of the two links and examine the behavior.

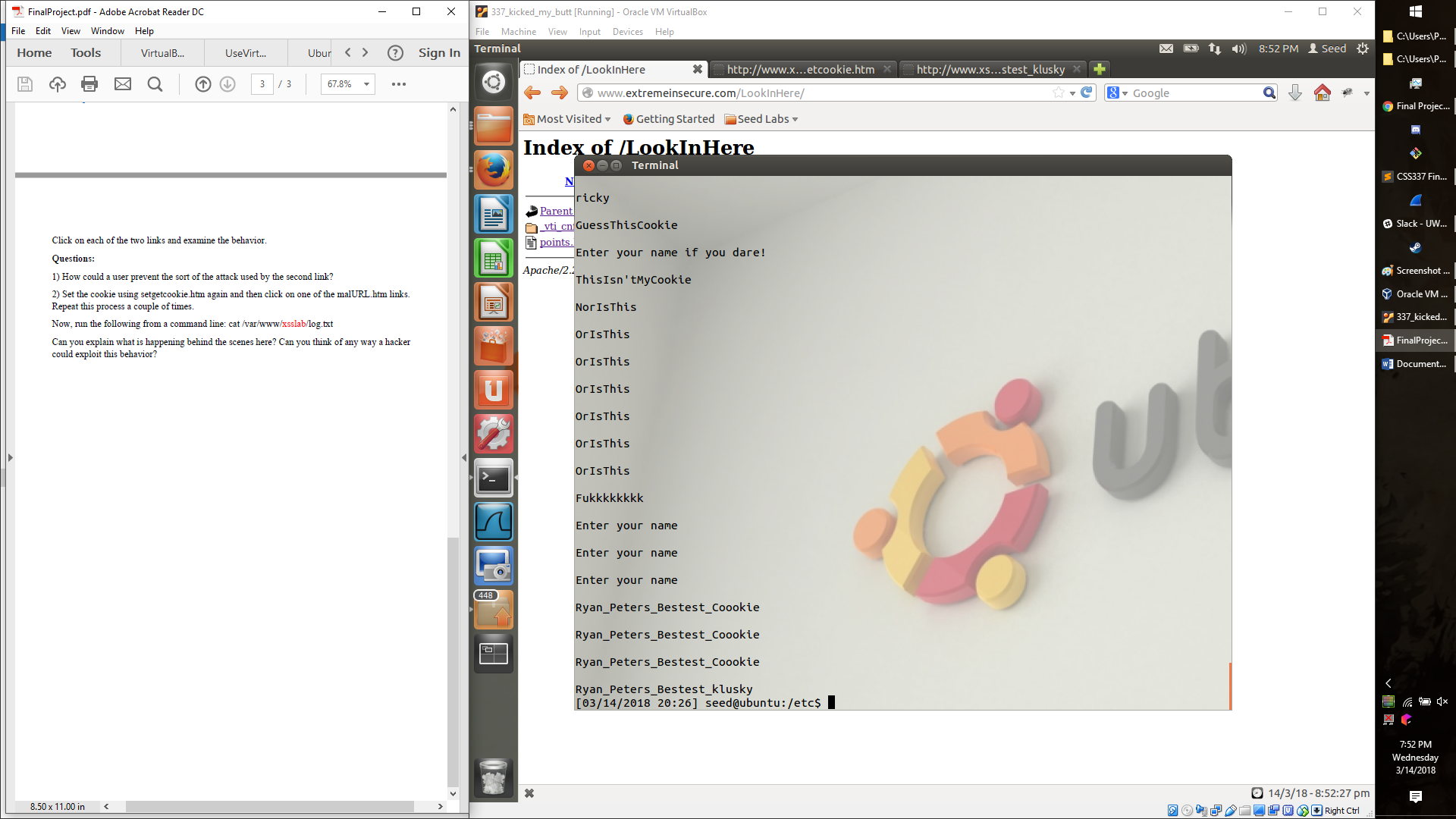
**Questions:**

1) How could a user prevent the sort of the attack used by the second link?

One way is to copy/pasta the link directly into the address bar, definitely don’t click on it.

2) Set the cookie using setgetcookie.htm again and then click on one of the malURL.htm links.

Repeat this process a couple of times.



Now, run the following from a command line: cat /var/www/xsslab/log.txt

Can you explain what is happening behind the scenes here? Can you think of any way a hacker

could exploit this behavior?

They are logging all the Kookies into a kooky log, where they can later extract other peoples account and/or session information, also they take their damn cookies… which is crime enough!