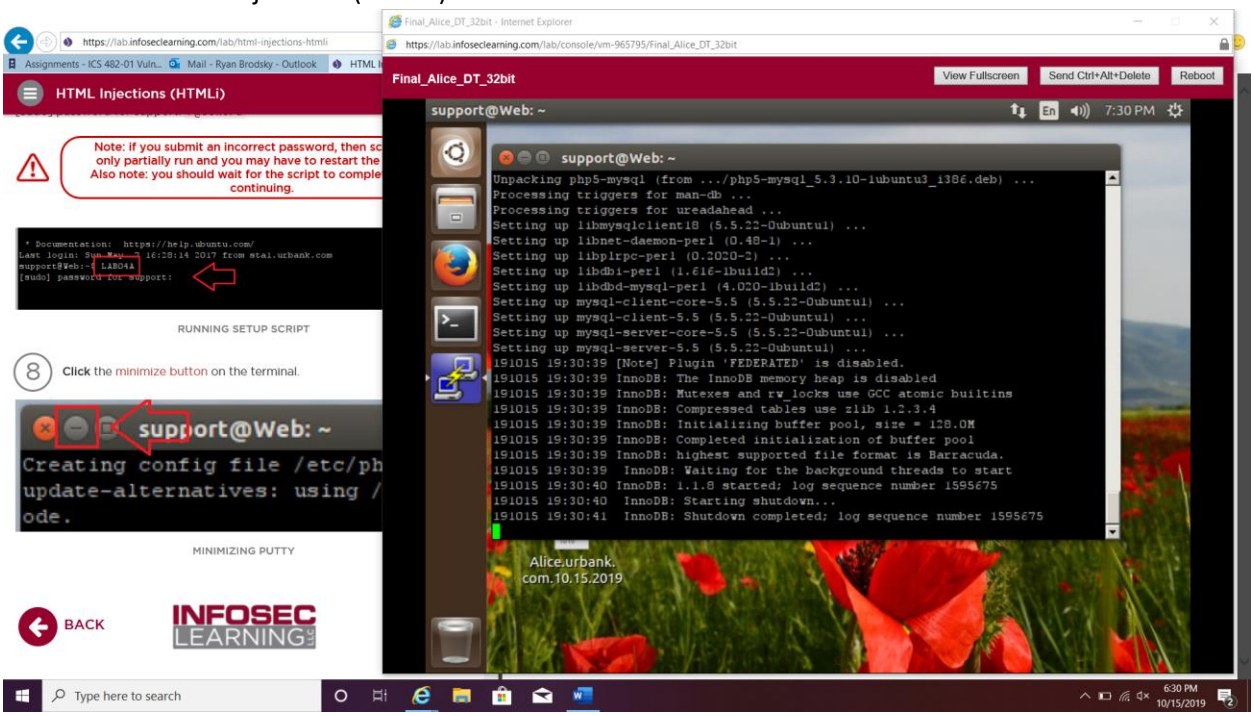
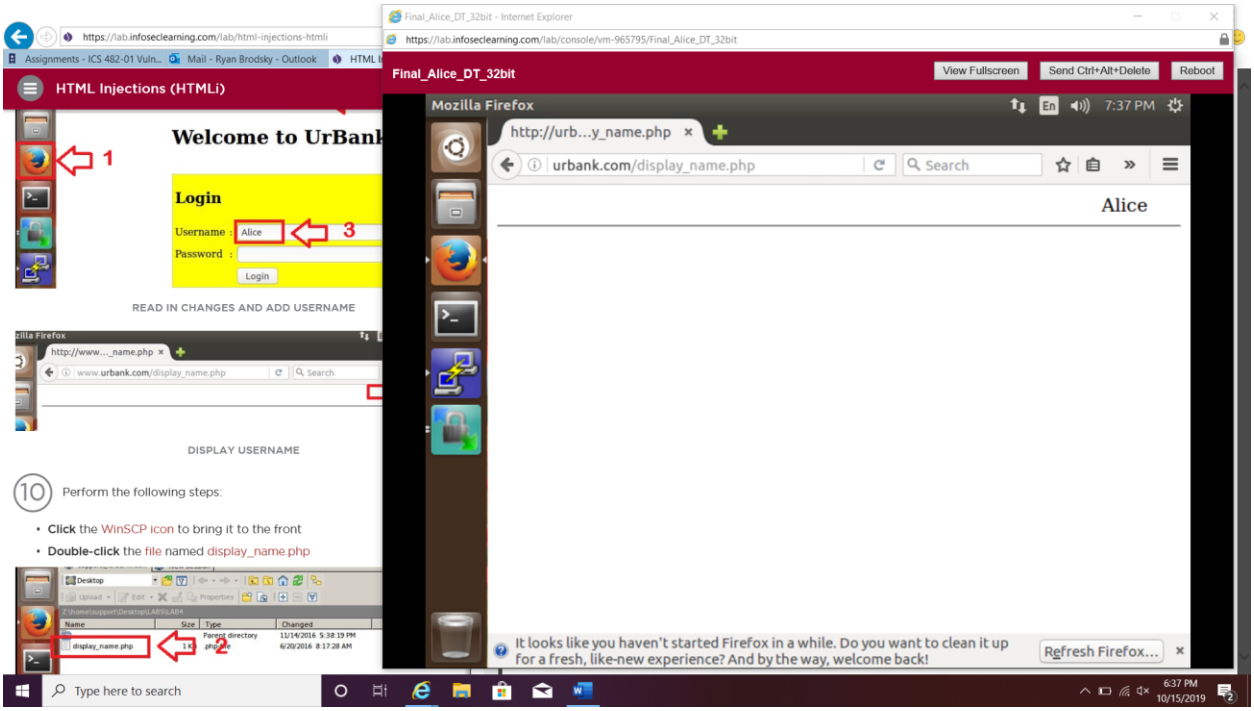
Ryan Brodsky

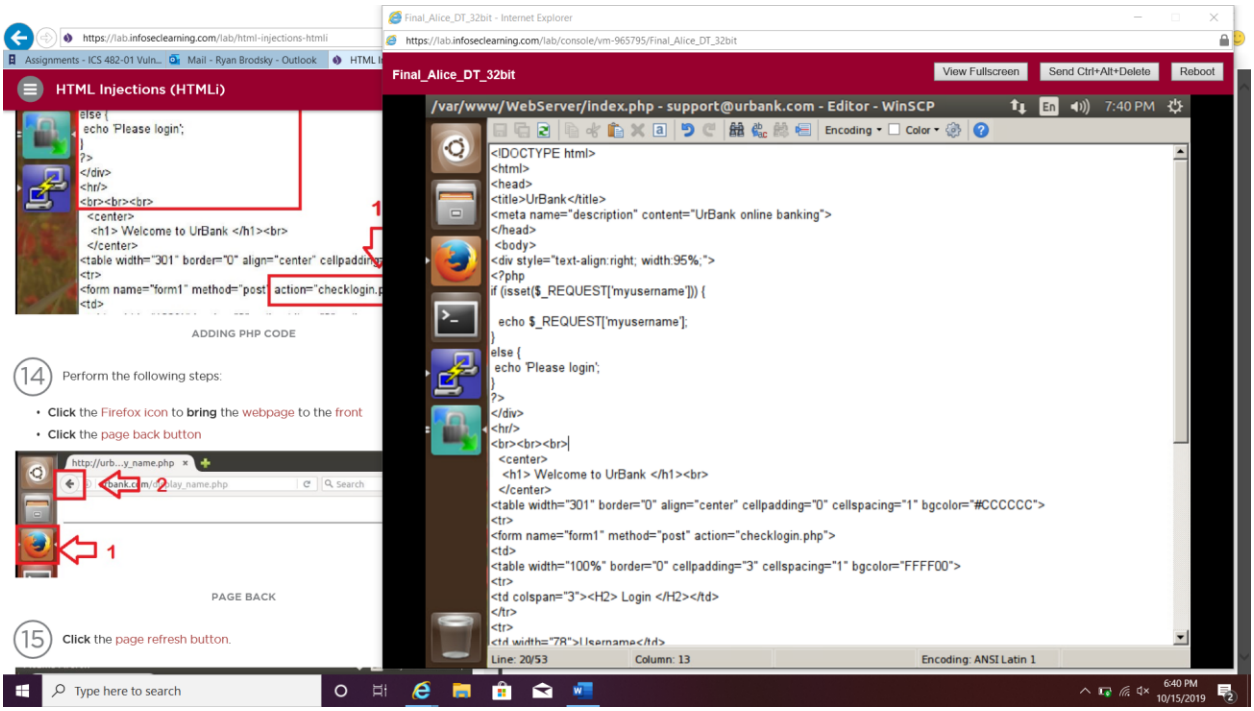
ICS 482

10/15/19

InfoSec Lab: HTML Injections (HTMLi)







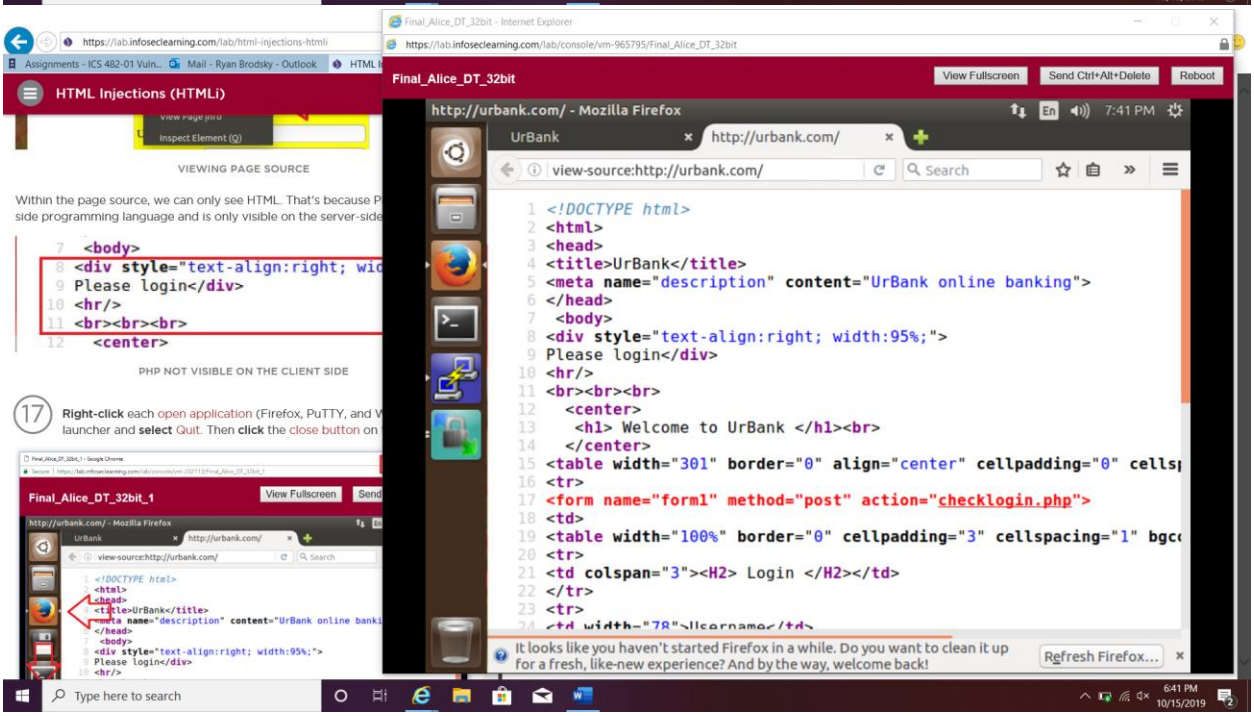
ADDING PHP CODE

14 Perform the following steps:

- **Click** the Firefox icon to **bring** the webpage to the front
- **Click** the page back button

PAGE BACK

15 **Click** the page refresh button.

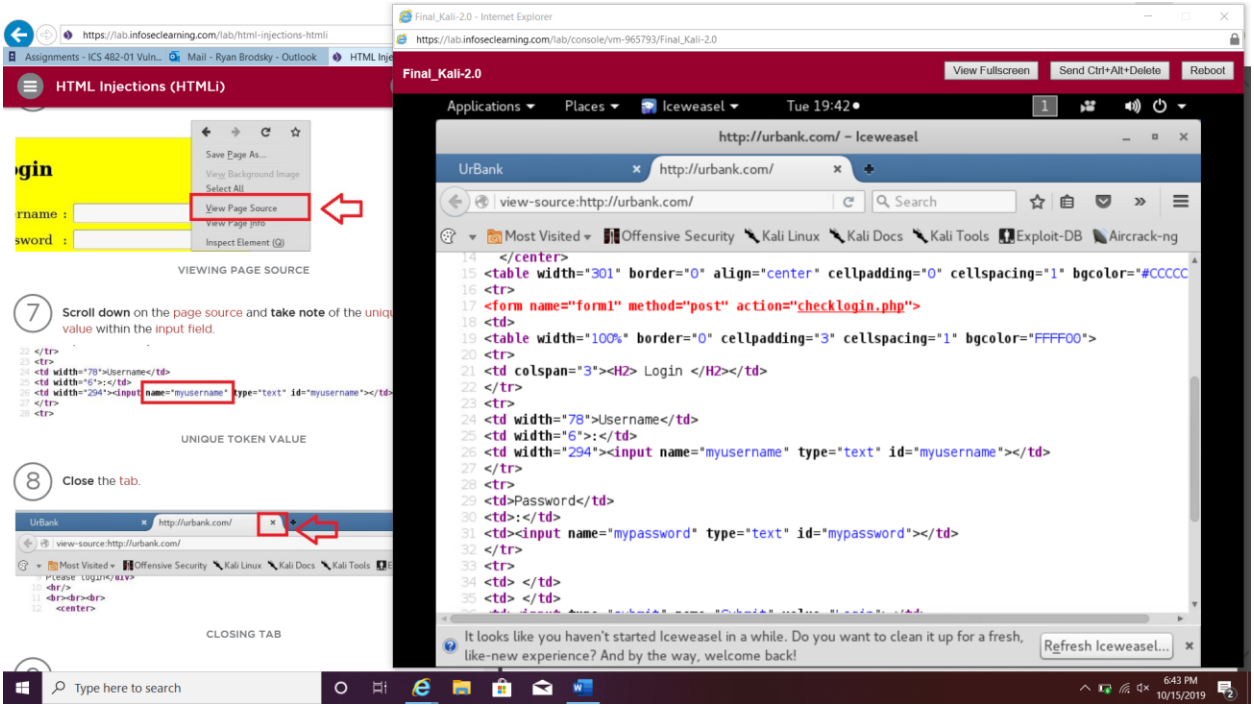


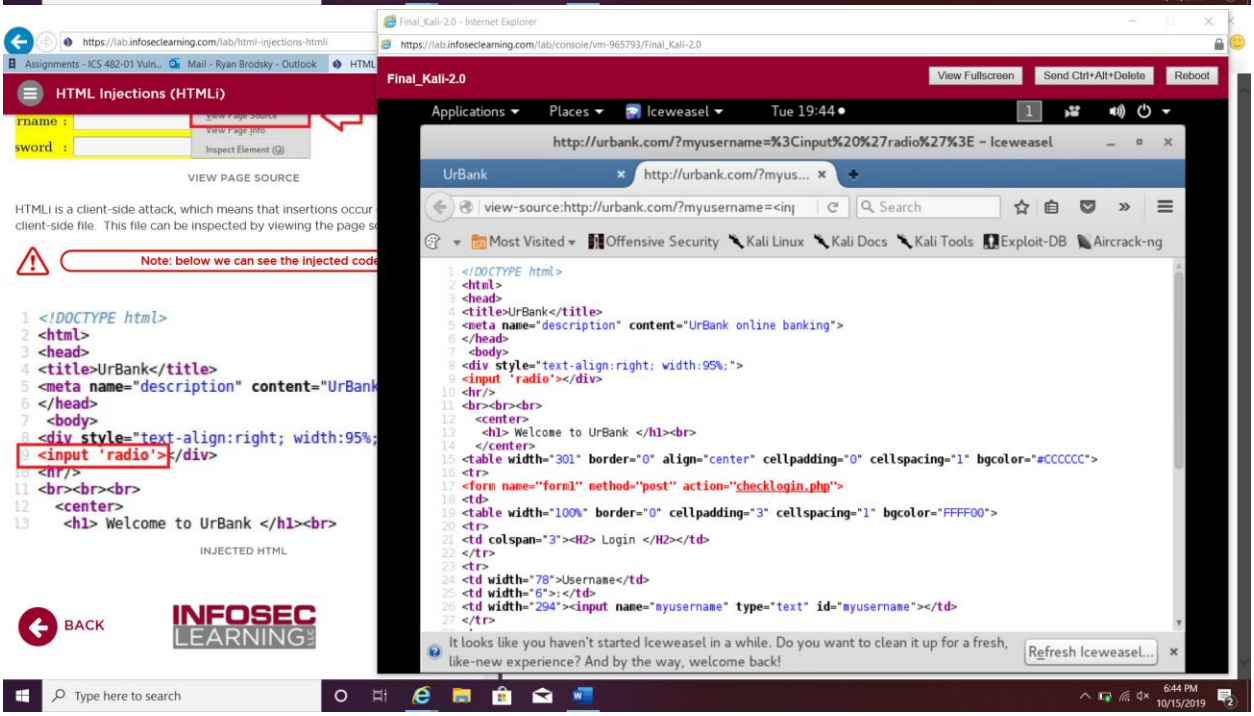
VIEWING PAGE SOURCE

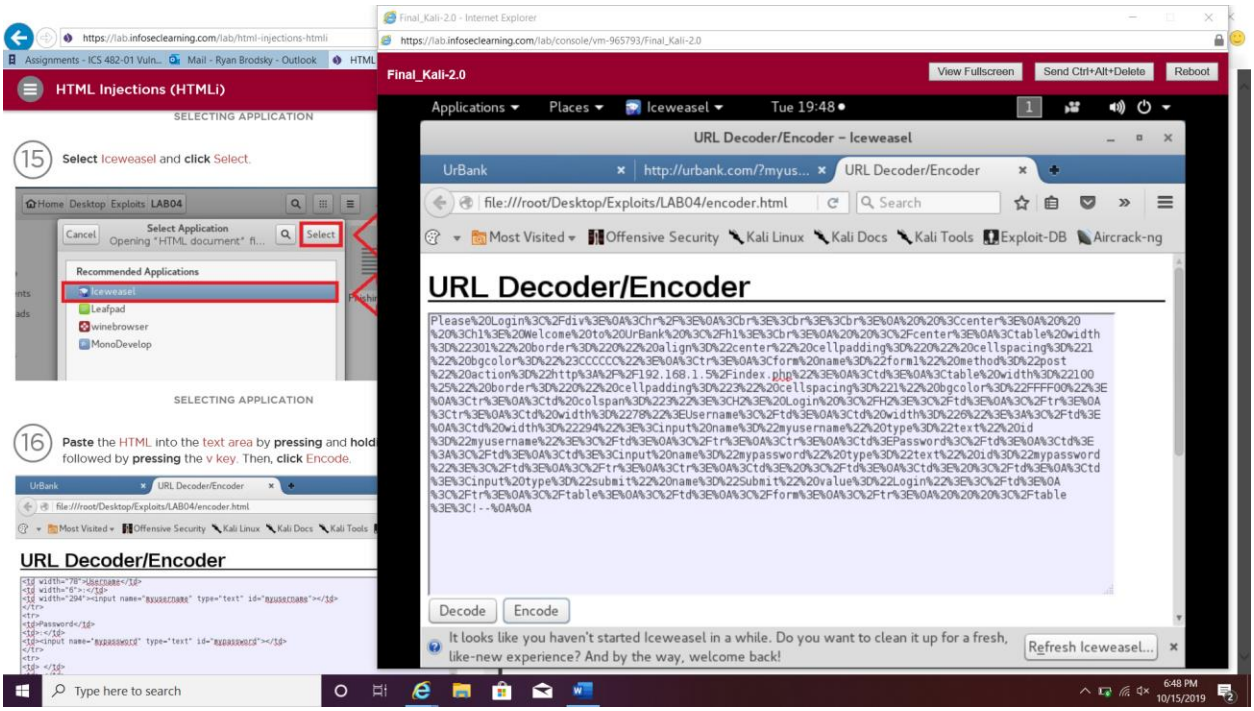
Within the page source, we can only see HTML. That's because P
side programming language and is only visible on the server-side

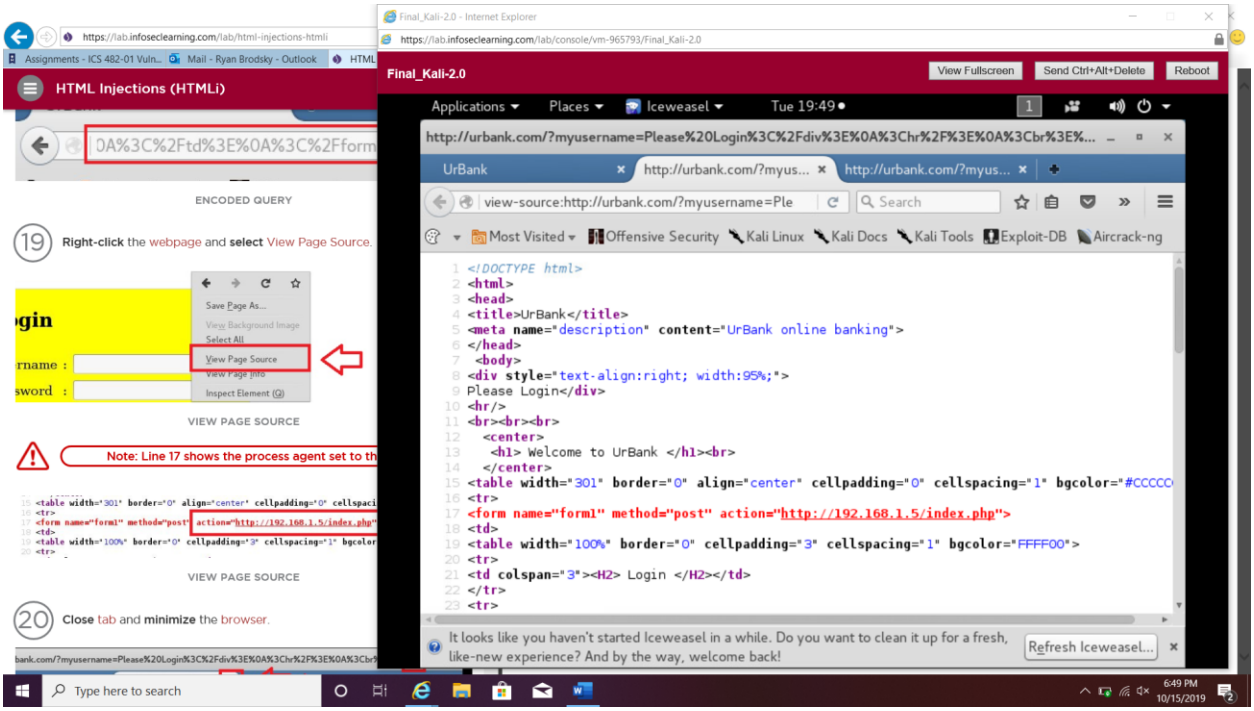
PHP NOT VISIBLE ON THE CLIENT SIDE

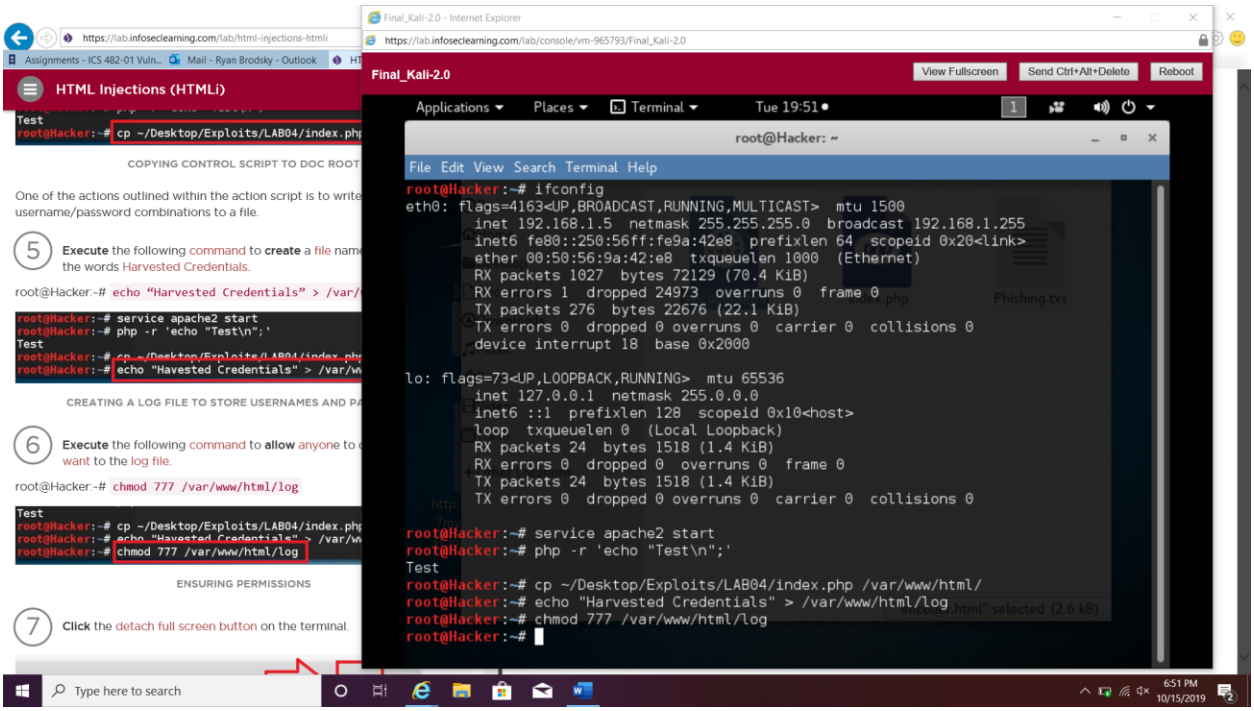
17 **Right-click** each open application (Firefox, PuTTY, and V
launcher and **select** Quit. Then **click** the close button on

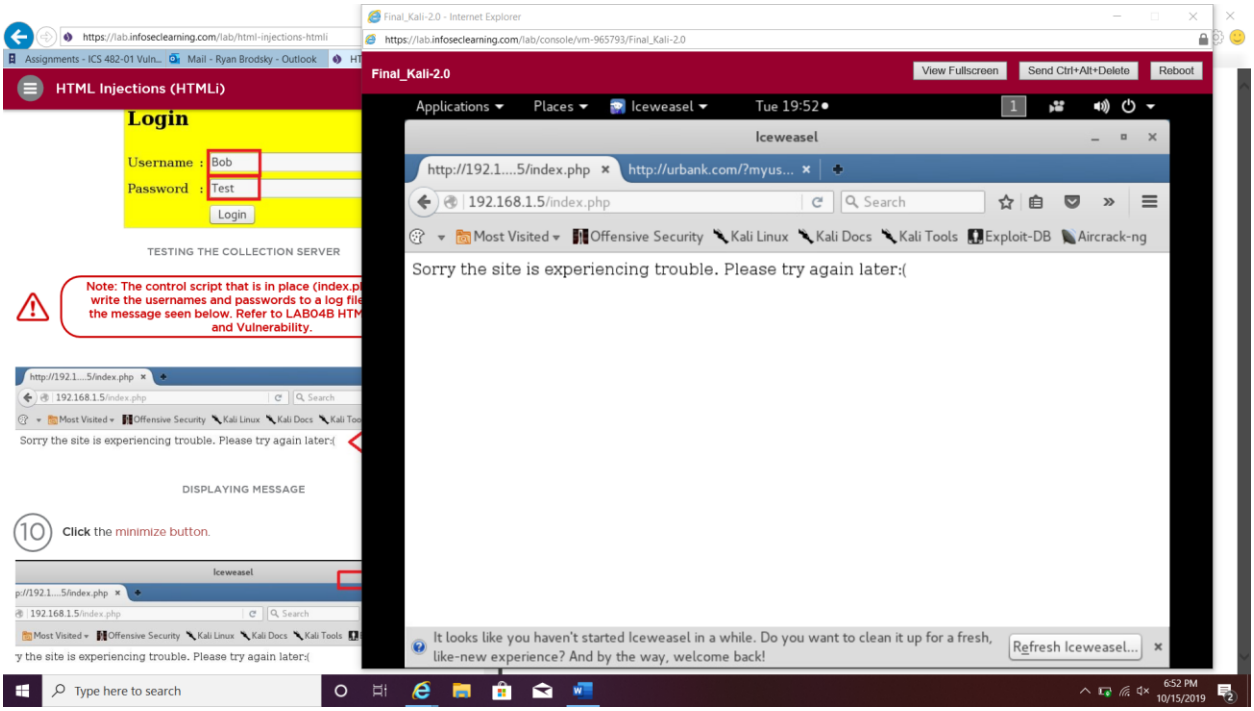

HTML Injections (HTMLi)
VIEWING PAGE SOURCE
Scroll down on the page source and take note of the unique value within the input field.
UNIQUE TOKEN VALUE
Close the tab.
CLOSING TAB
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
http://urbank.com/ - Iceweasel
view-source:http://urbank.com/
It 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...

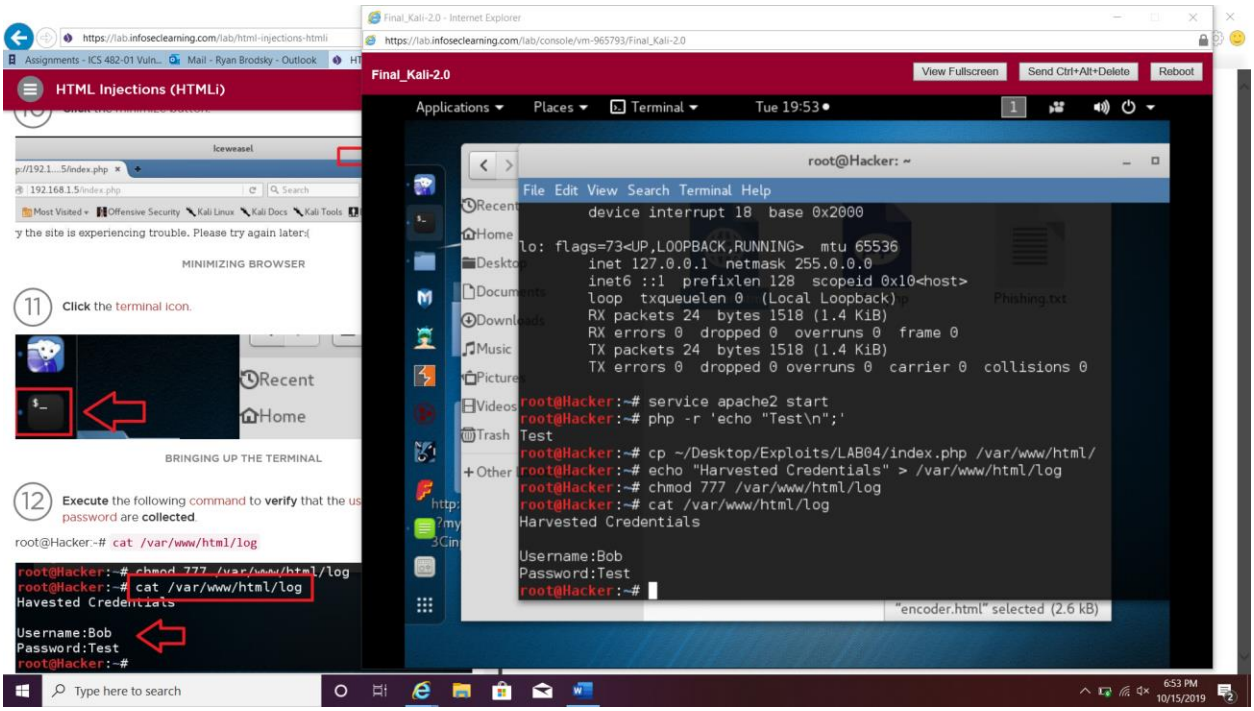

HTML Injections (HTMLi)
VIEW PAGE SOURCE
HTMLi is a client-side attack, which means that insertions occur
client-side file. This file can be inspected by viewing the page s
Note: below we can see the injected code
INJECTED HTML
BACK
INFOSEC LEARNING
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
http://urbank.com/?myusername=%3Cinput%20%27radio%27%3E - Iceweasel
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...

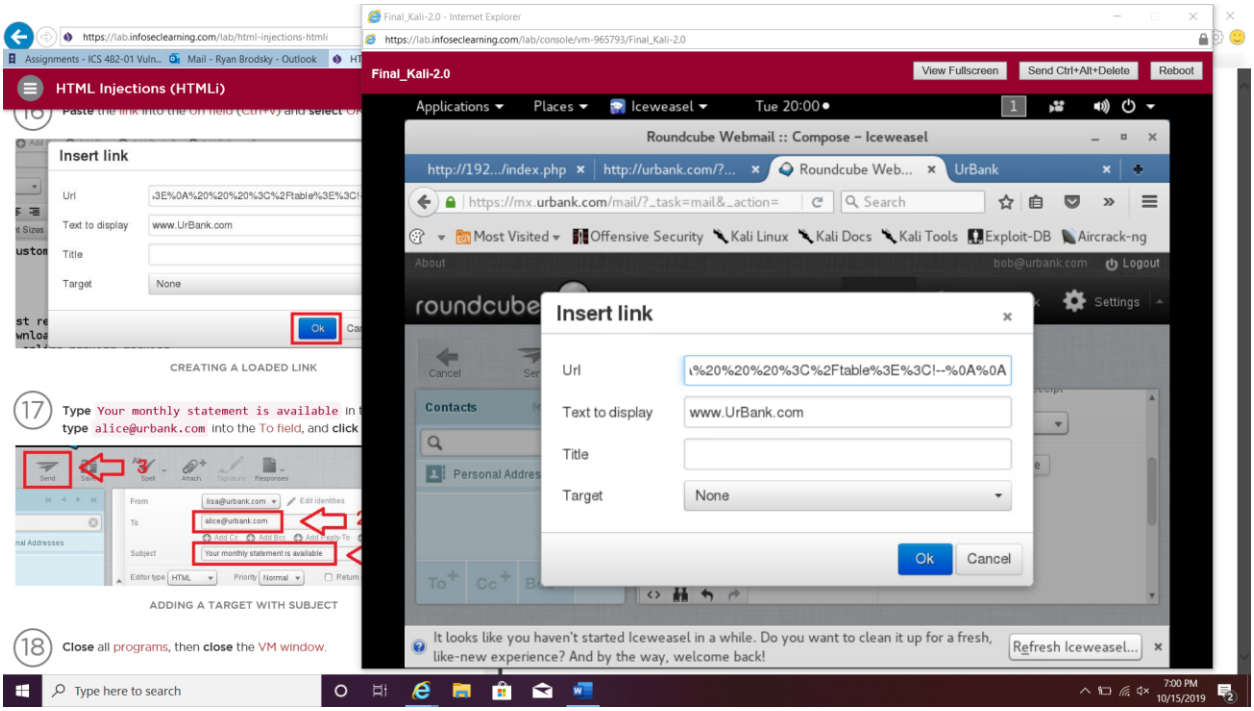

HTML Injections (HTMLi)
SELECTING APPLICATION
15 Select Iceweasel and click Select.
Select Application
Recommended Applications
Iceweasel
Leafpad
winebrowser
MonoDevelop
SELECTING APPLICATION
16 Paste the HTML into the text area by pressing and hold
followed by pressing the v key. Then, click Encode.
URL Decoder/Encoder
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
URL Decoder/Encoder – Iceweasel
URL Decoder/Encoder
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...
Type here to search
6:48 PM
10/15/2019

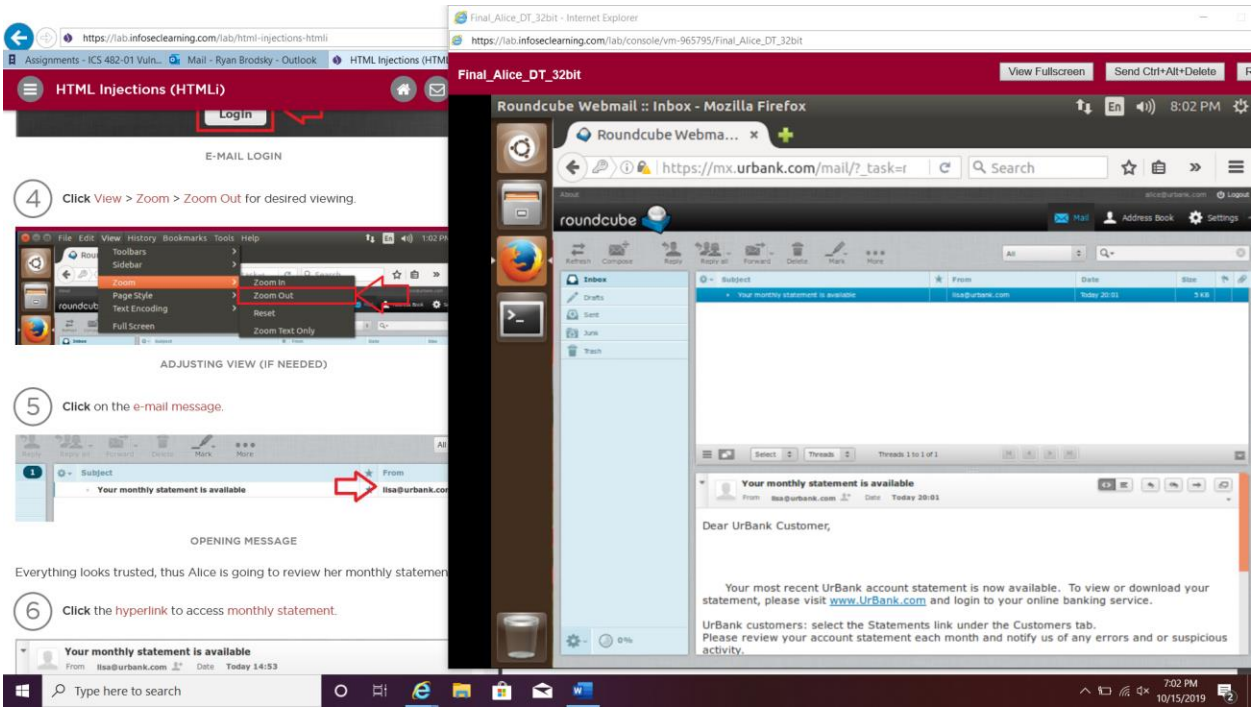

HTML Injections (HTMLi)
ENCODED QUERY
19 Right-click the webpage and select View Page Source.
Save Page As...
Select All
View Page Source
Inspect Element (Q)
VIEW PAGE SOURCE
Note: Line 17 shows the process agent set to th
VIEW PAGE SOURCE
20 Close tab and minimize the browser.
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
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...
Type here to search
6:49 PM
10/15/2019

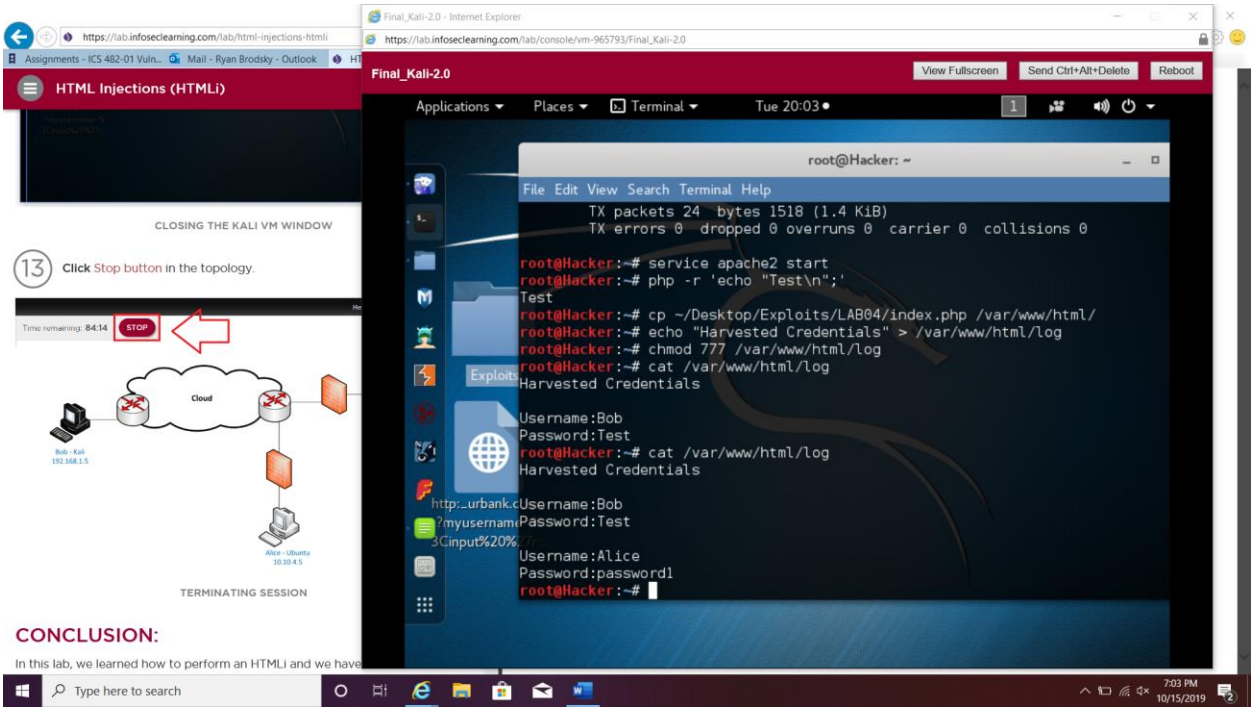

HTML Injections (HTMLi)
cp ~/Desktop/Exploits/LAB04/index.php
COPYING CONTROL SCRIPT TO DOC ROOT
One of the actions outlined within the action script is to write
username/password combinations to a file.
5 Execute the following command to create a file nam
the words Harvested Credentials.
root@Hacker:~# echo "Harvested Credentials" > /var/
service apache2 start
php -r 'echo "Test\n";'
echo "Havested Credentials" > /var/w
CREATING A LOG FILE TO STORE USERNAMES AND PA
6 Execute the following command to allow anyone to
want to the log file.
root@Hacker:~# chmod 777 /var/www/html/log
chmod 777 /var/www/html/log
ENSURING PERMISSIONS
7 Click the detach full screen button on the terminal.
Final_Kali-2.0 - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-965793/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Terminal
Tue 19:51
root@Hacker: ~
File Edit View Search Terminal Help
root@Hacker:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.5 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::250:56ff:fe9a:42e8 prefixlen 64 scopeid 0x20<link>
ether 00:50:56:9a:42:e8 txqueuelen 1000 (Ethernet)
RX packets 1027 bytes 72129 (70.4 KiB)
RX errors 1 dropped 24973 overruns 0 frame 0
TX packets 276 bytes 22676 (22.1 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 18 base 0x2000
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 0 (Local Loopback)
RX packets 24 bytes 1518 (1.4 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 24 bytes 1518 (1.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@Hacker:~# service apache2 start
root@Hacker:~# php -r 'echo "Test\n";'
Test
root@Hacker:~# cp ~/Desktop/Exploits/LAB04/index.php /var/www/html/
root@Hacker:~# echo "Harvested Credentials" > /var/www/html/log
root@Hacker:~# chmod 777 /var/www/html/log
root@Hacker:~#
Type here to search
6:51 PM
10/15/2019


HTML Injections (HTMLi)
Login
Username : Bob
Password : Test
Login
TESTING THE COLLECTION SERVER
Note: The control script that is in place (index.p
write the usernames and passwords to a log file
the message seen below. Refer to LAB04B HTM
and Vulnerability.
Sorry the site is experiencing trouble. Please try again later:(
DISPLAYING MESSAGE
10 Click the minimize button.
Final_Kali-2.0 - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-965793/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Iceweasel
Tue 19:52
Iceweasel
http://192.1....5/index.php
http://urbank.com/?myus...
192.168.1.5/index.php
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Sorry the site is experiencing trouble. Please try again later:(
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...
Type here to search
6:52 PM
10/15/2019


HTML Injections (HTMLi)
MINIMIZING BROWSER
11 Click the terminal icon.
BRINGING UP THE TERMINAL
12 Execute the following command to verify that the us
password are collected.
root@Hacker:~# cat /var/www/html/log
root@Hacker:~# cat /var/www/html/log
Havested Credentials
Username:Bob
Password:Test
root@Hacker:~#
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Terminal
Tue 19:53
root@Hacker: ~
File Edit View Search Terminal Help
device interrupt 18 base 0x2000
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 0 (Local Loopback)
RX packets 24 bytes 1518 (1.4 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 24 bytes 1518 (1.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@Hacker:~# service apache2 start
root@Hacker:~# php -r 'echo "Test\n";'
Test
root@Hacker:~# cp ~/Desktop/Exploits/LAB04/index.php /var/www/html/
root@Hacker:~# echo "Harvested Credentials" > /var/www/html/log
root@Hacker:~# chmod 777 /var/www/html/log
root@Hacker:~# cat /var/www/html/log
Harvested Credentials
Username:Bob
Password:Test
root@Hacker:~#
"encoder.html" selected (2.6 kB)
Type here to search
6:53 PM
10/15/2019


HTML Injections (HTMLi)
CREATING A LOADED LINK
Insert link
Url
Text to display
www.UrBank.com
Title
Target
None
Ok
17 Type Your monthly statement is available in t
type alice@urbank.com into the To field, and click
ADDING A TARGET WITH SUBJECT
18 Close all programs, then close the VM window.
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Iceweasel
Tue 20:00
Roundcube Webmail :: Compose – Iceweasel
Insert link
Url
%20%20%20%3C%2Ftable%3E%3C!--%0A%0A
Text to display
www.UrBank.com
Title
Target
None
Ok
Cancel
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...
Type here to search
7:00 PM
10/15/2019





CONCLUSION:

In this lab, we learned how to perform an HTMLi and we have