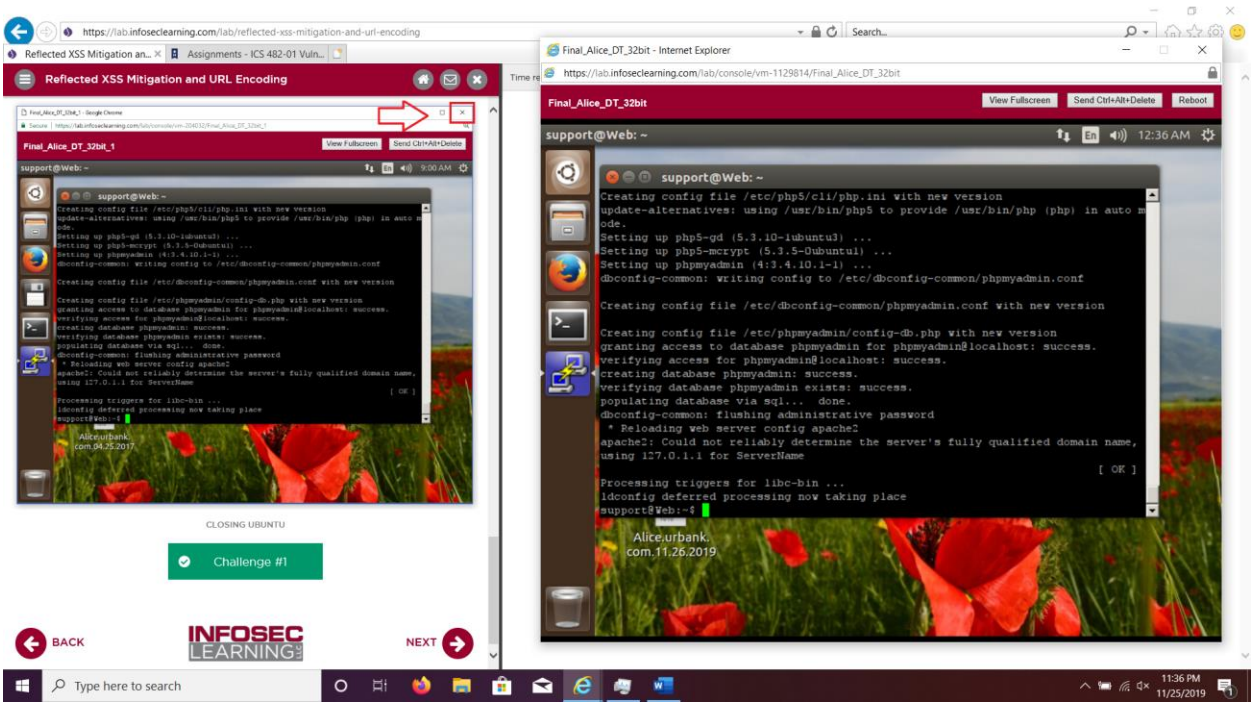
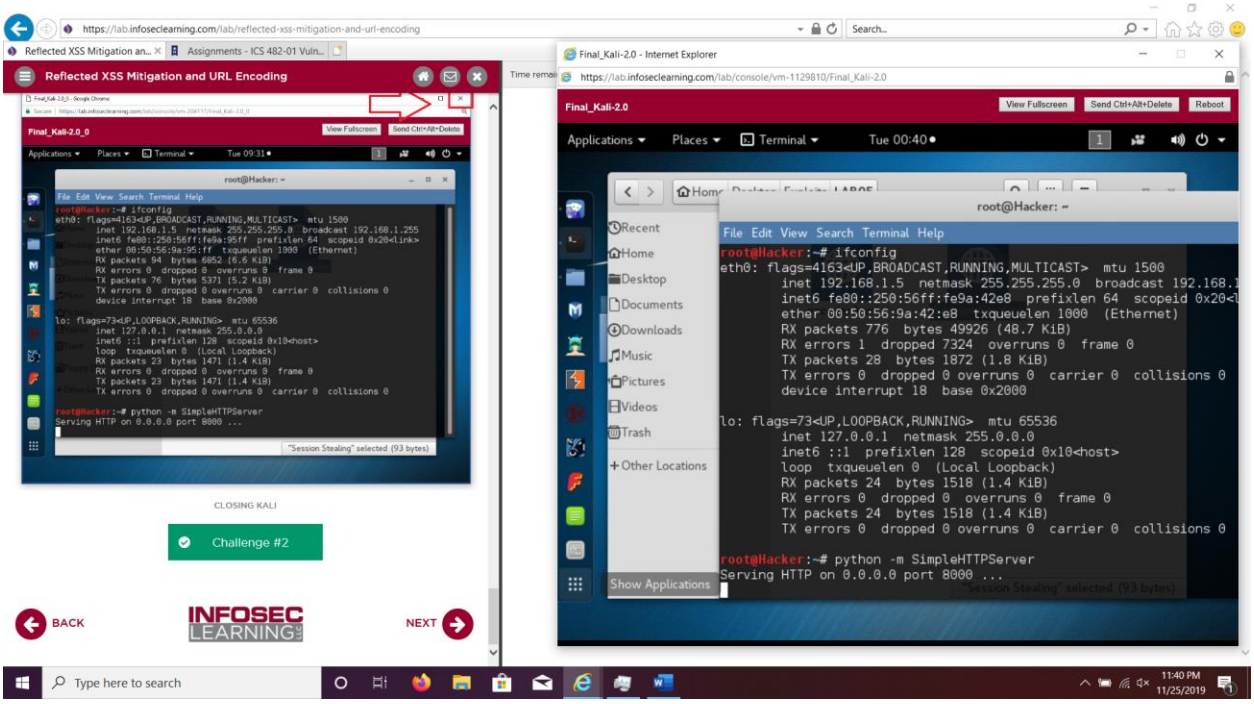
Ryan Brodsky

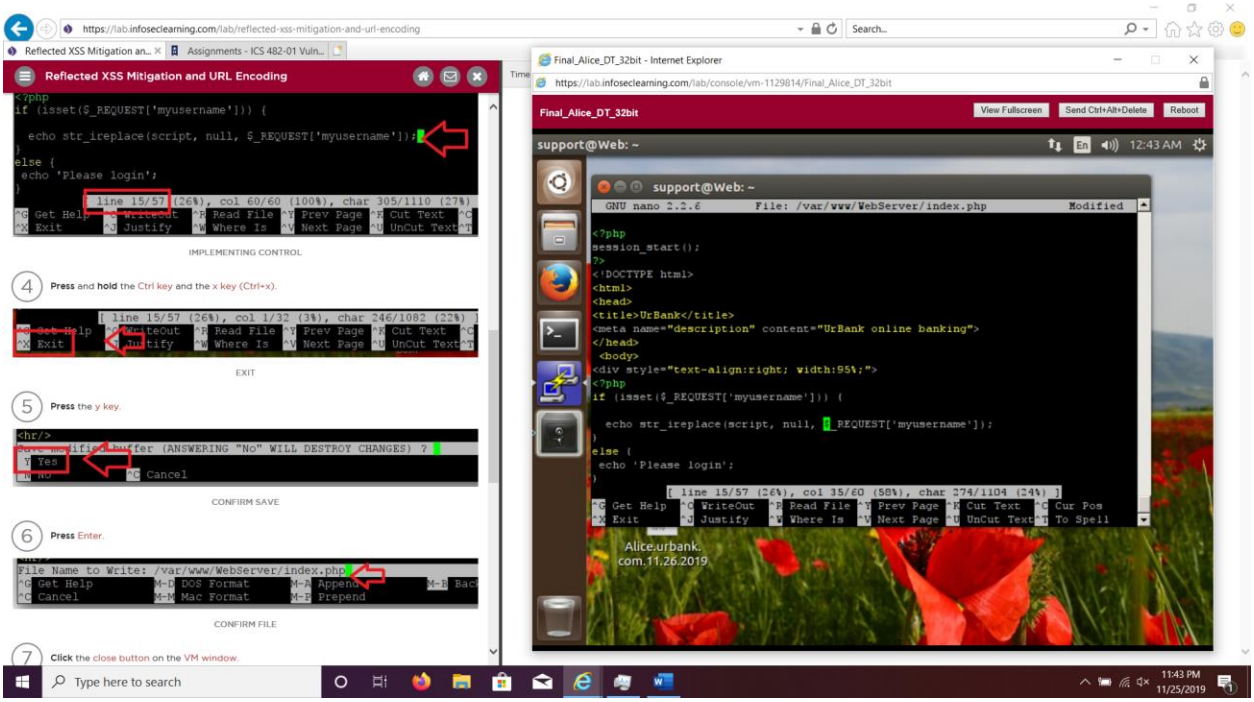
ICS 482

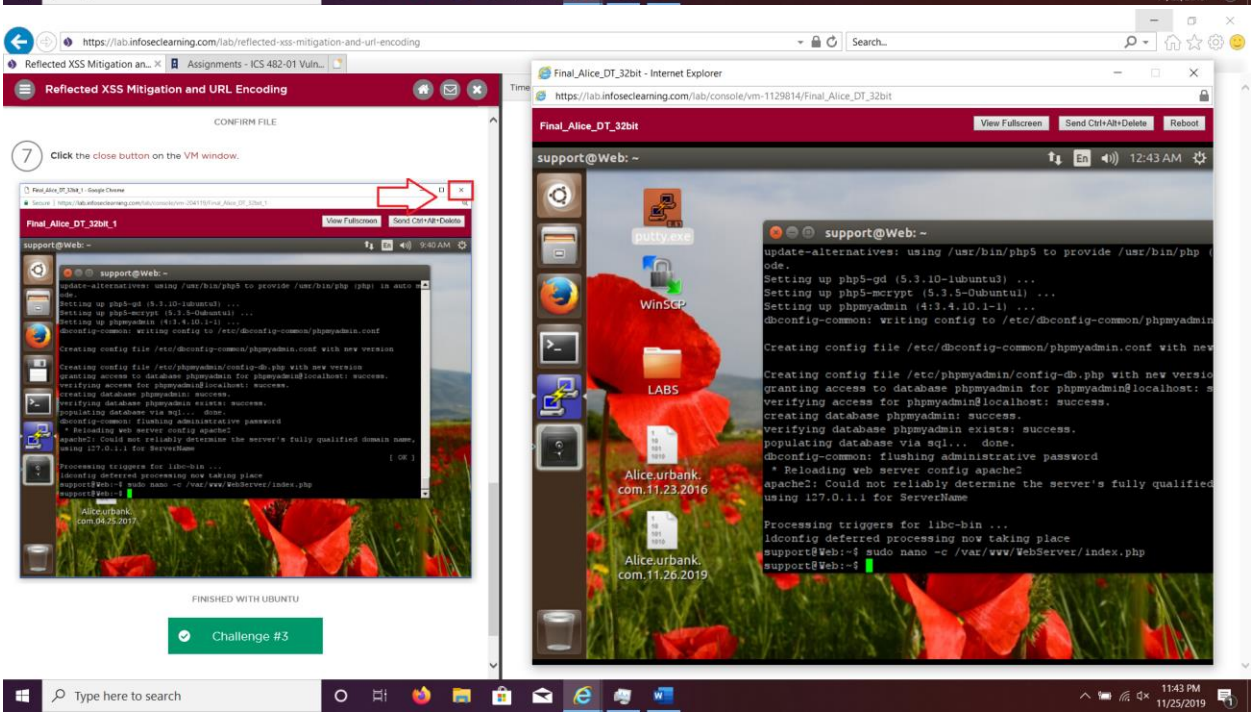
11/25/2019

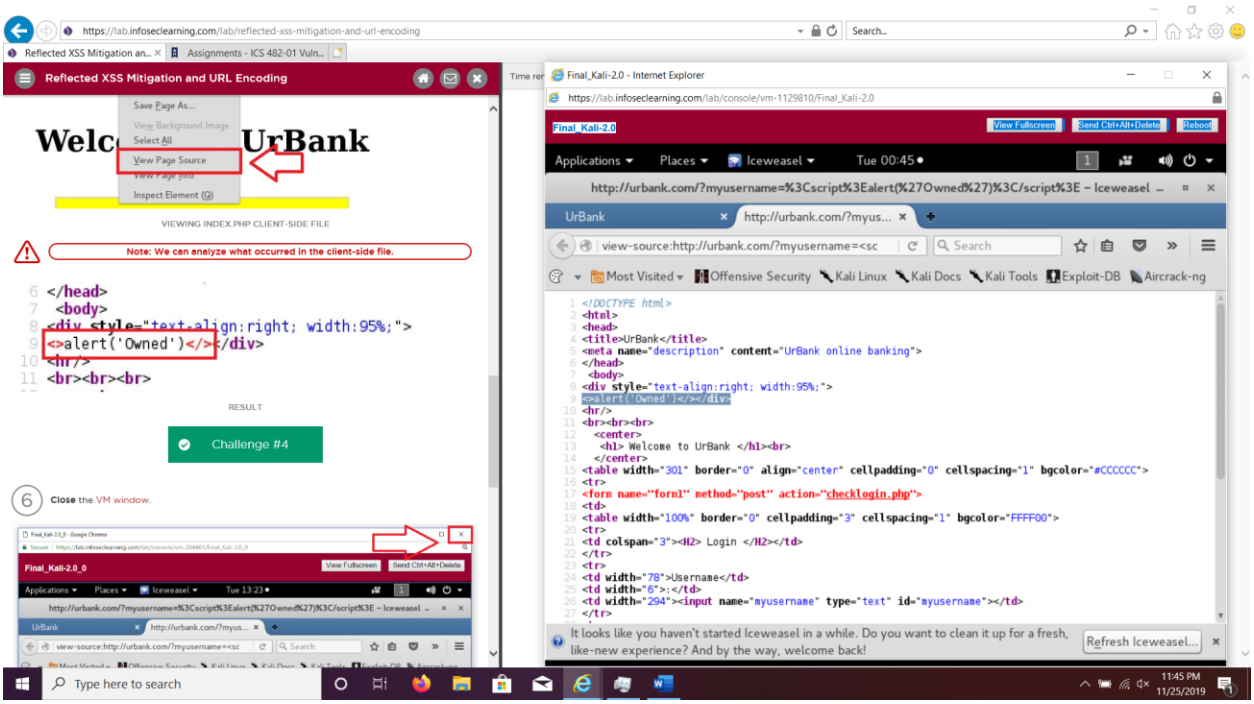
InfoSec Lab: Reflected XSS Mitigation and URL Encoding






Reflected XSS Mitigation and URL Encoding
IMPLEMENTING CONTROL
4 Press and hold the Ctrl key and the x key (Ctrl+x).
EXIT
5 Press the y key.
CONFIRM SAVE
6 Press Enter.
CONFIRM FILE
7 Click the close button on the VM window.
Final_Alice_DT_32bit - Internet Explorer
Final_Alice_DT_32bit
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
support@Web: ~
12:43 AM
Alice.urbank.
com.11.26.2019
Type here to search
11:43 PM
11/25/2019


Reflected XSS Mitigation and URL Encoding
CONFIRM FILE
7 Click the close button on the VM window.
FINISHED WITH UBUNTU
Challenge #3
Final_Alice_DT_32bit - Internet Explorer
Final_Alice_DT_32bit
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
support@Web: ~
12:43 AM
putty.exe
WinSCP
LABS
Alice.urbank.
com.11.23.2016
Alice.urbank.
com.11.26.2019
Type here to search
11:43 PM
11/25/2019


Reflected XSS Mitigation and URL Encoding
Save Page As...
View Background Image
Select All
View Page Source
Inspect Element (Q)
VIEWING INDEX.PHP CLIENT-SIDE FILE
Note: We can analyze what occurred in the client-side file.
</head>
<body>

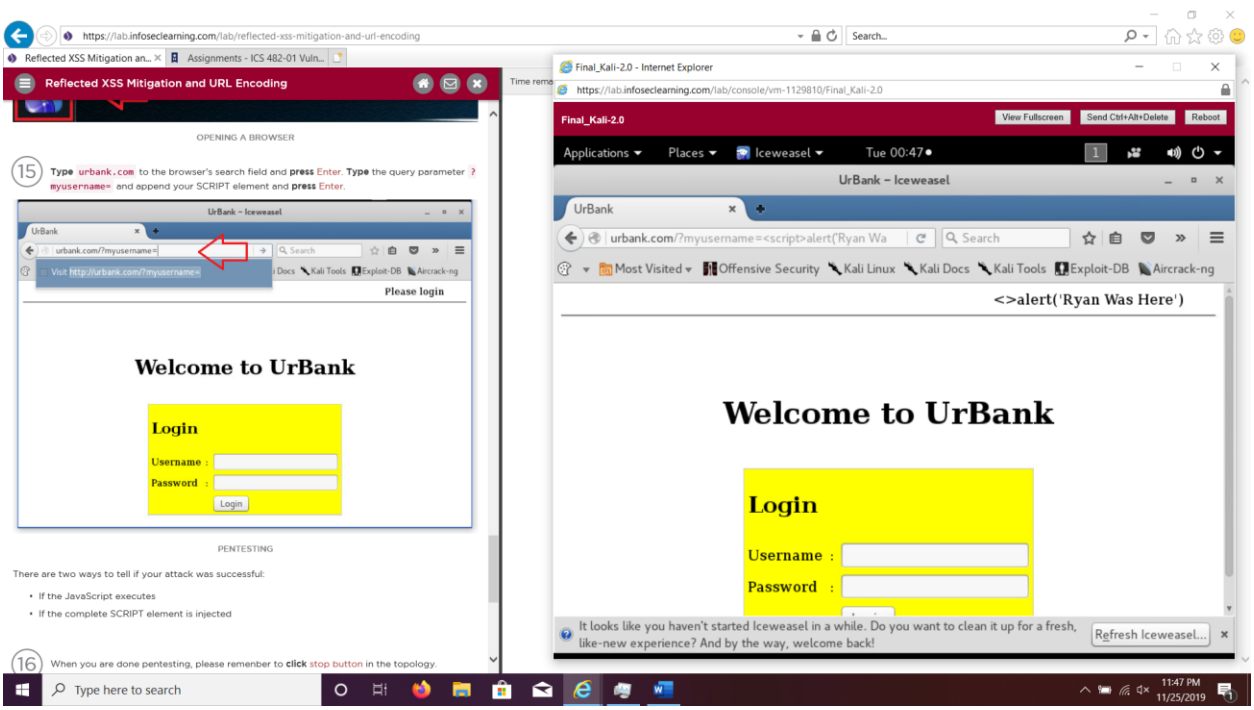
<>alert('Owned')</>
<hr/>

RESULT
Challenge #4
6 Close the VM window.
Final_Kali-2.0 - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-1129810/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Iceweasel
Tue 00:45
http://urbank.com/?myusername=%3Cscript%3Ealert(%27Owned%27)%3C/script%3E - Iceweasel
UrBank
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>

<>alert('Owned')</>
<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
11:45 PM
11/25/2019


Reflected XSS Mitigation and URL Encoding
OPENING A BROWSER
15 Type urbank.com to the browser's search field and press Enter. Type the query parameter ?myusername= and append your SCRIPT element and press Enter.
UrBank - Iceweasel
Please login
Welcome to UrBank
Login
Username :
Password :
Login
PENTESTING
There are two ways to tell if your attack was successful:
If the JavaScript executes
If the complete SCRIPT element is injected
16 When you are done pentesting, please remember to click stop button in the topology.
Final_Kali-2.0 - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-1129810/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Iceweasel
Tue 00:47
UrBank - Iceweasel
UrBank
urbank.com/?myusername=<script>alert('Ryan Wa
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
<>alert('Ryan Was Here')
Welcome to UrBank
Login
Username :
Password :
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
11:47 PM
11/25/2019