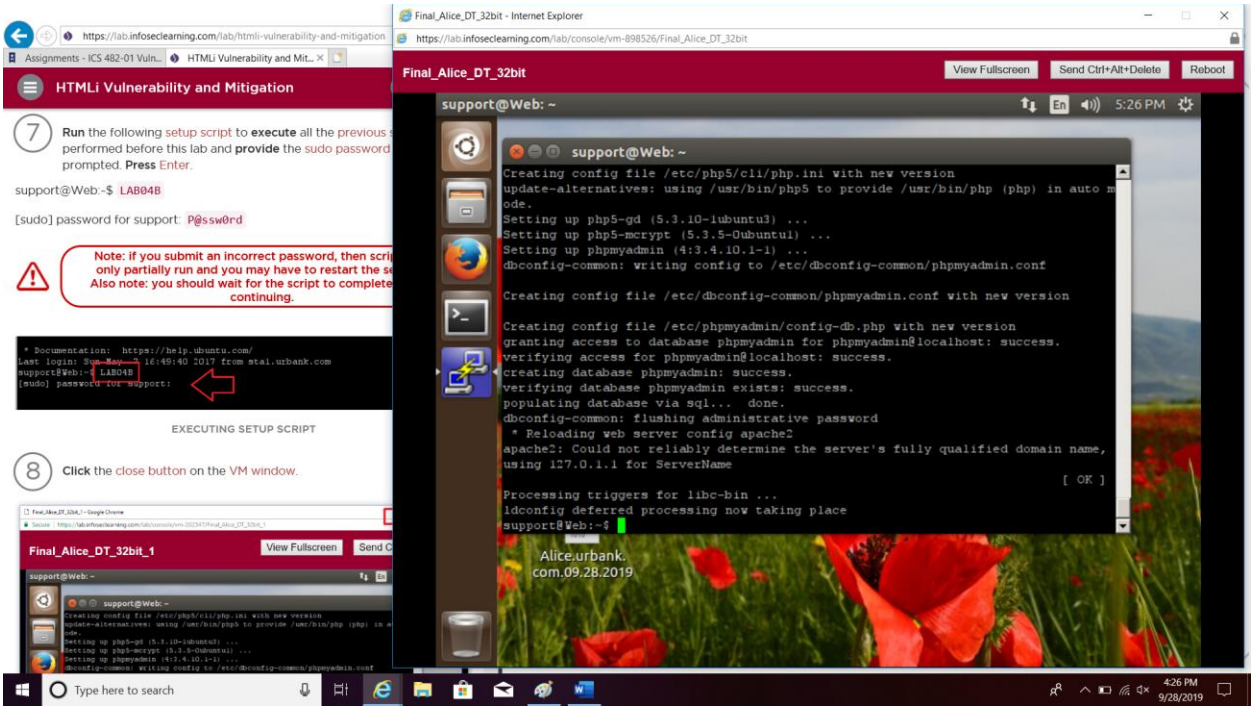
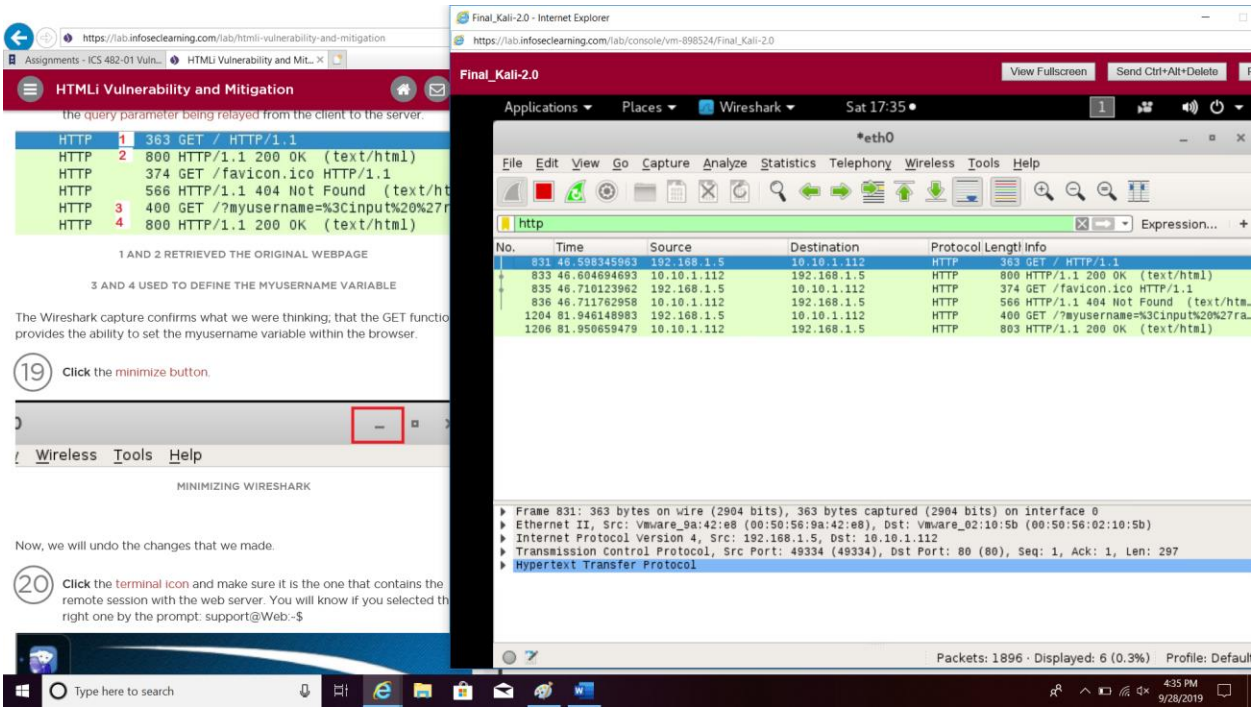
Ryan Brodsky

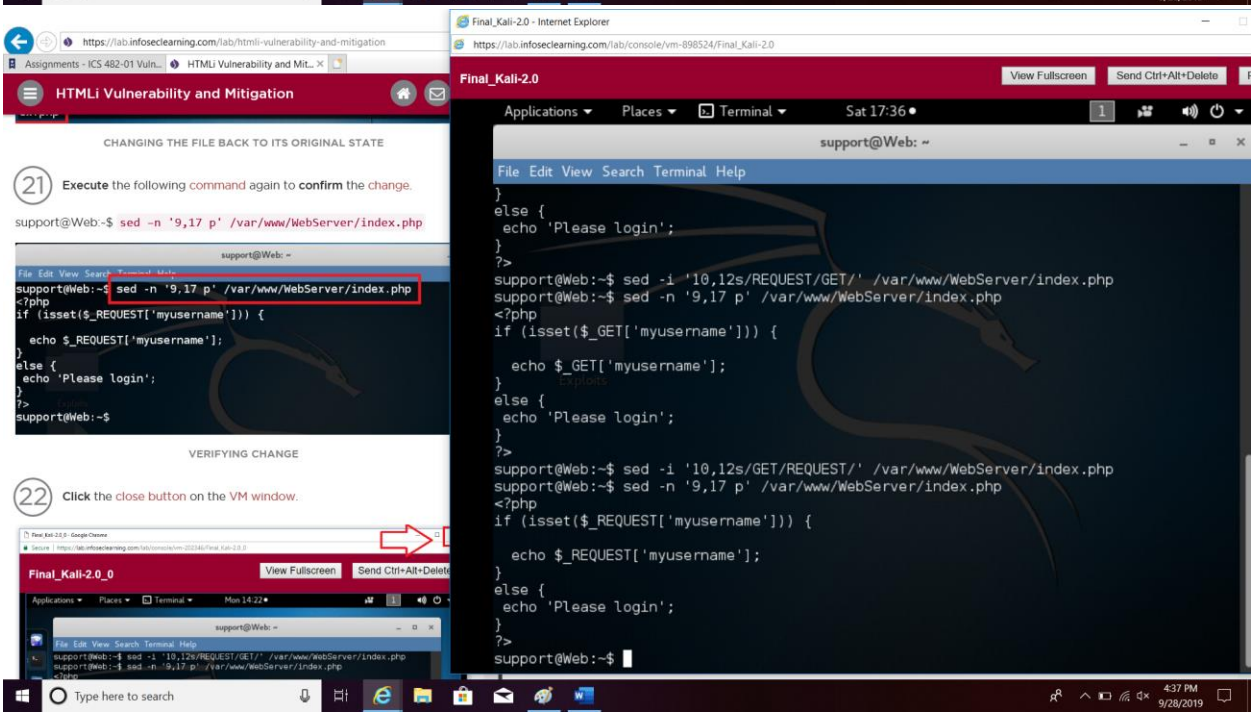
ICS 482

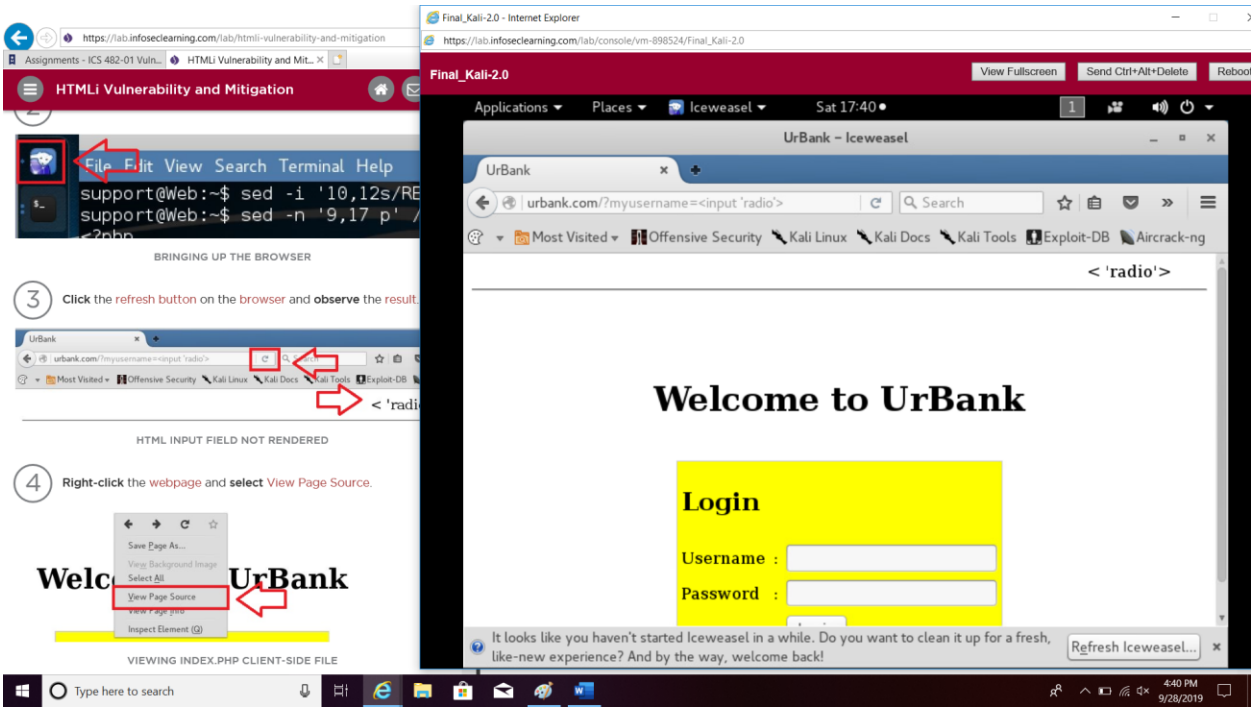
9/28/2019

InfoSec Lab: HTMLi Vulnerability and Mitigation




HTMLi Vulnerability and Mitigation
the query parameter being relayed from the client to the server.
HTTP 1 363 GET / HTTP/1.1
HTTP 2 800 HTTP/1.1 200 OK (text/html)
HTTP 374 GET /favicon.ico HTTP/1.1
HTTP 566 HTTP/1.1 404 Not Found (text/ht
HTTP 3 400 GET /?myusername=%3Cinput%20%27r
HTTP 4 800 HTTP/1.1 200 OK (text/html)
1 AND 2 RETRIEVED THE ORIGINAL WEBPAGE
3 AND 4 USED TO DEFINE THE MYUSERNAME VARIABLE
The Wireshark capture confirms what we were thinking, that the GET functio
provides the ability to set the myusername variable within the browser.
19 Click the minimize button.
Wireless Tools Help
MINIMIZING WIRESHARK
Now, we will undo the changes that we made.
20 Click the terminal icon and make sure it is the one that contains the
remote session with the web server. You will know if you selected th
right one by the prompt: support@Web:~$
Final_Kali-2.0 - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-898524/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Applications Places Wireshark Sat 17:35
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
No. Time Source Destination Protocol Lengtl Info
831 46.598345983 192.168.1.5 10.10.1.112 HTTP 363 GET / HTTP/1.1
833 46.604694693 10.10.1.112 192.168.1.5 HTTP 800 HTTP/1.1 200 OK (text/html)
835 46.710123962 192.168.1.5 10.10.1.112 HTTP 374 GET /favicon.ico HTTP/1.1
836 46.711762958 10.10.1.112 192.168.1.5 HTTP 566 HTTP/1.1 404 Not Found (text/htm
1204 81.946148983 192.168.1.5 10.10.1.112 HTTP 400 GET /?myusername=%3Cinput%20%27ra
1206 81.950659479 10.10.1.112 192.168.1.5 HTTP 803 HTTP/1.1 200 OK (text/html)
Frame 831: 363 bytes on wire (2904 bits), 363 bytes captured (2904 bits) on interface 0
Ethernet II, Src: Vmware_9a:42:e8 (00:50:56:9a:42:e8), Dst: Vmware_02:10:5b (00:50:56:02:10:5b)
Internet Protocol Version 4, Src: 192.168.1.5, Dst: 10.10.1.112
Transmission Control Protocol, Src Port: 49334 (49334), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 297
Hypertext Transfer Protocol
Packets: 1896 · Displayed: 6 (0.3%) Profile: Default
Type here to search
4:35 PM
9/28/2019


HTMLi Vulnerability and Mitigation
CHANGING THE FILE BACK TO ITS ORIGINAL STATE
21 Execute the following command again to confirm the change.
support@Web:~$ sed -n '9,17 p' /var/www/WebServer/index.php
support@Web: ~
support@Web:~$ sed -n '9,17 p' /var/www/WebServer/index.php
<?php
if (isset($_REQUEST['myusername'])) {
echo $_REQUEST['myusername'];
}
else {
echo 'Please login';
}
?>
support@Web:~$
VERIFYING CHANGE
22 Click the close button on the VM window.
Final_Kali-2.0_0
View Fullscreen
Send Ctrl+Alt+Delete
Final_Kali-2.0 - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-898524/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Applications Places Terminal Sat 17:36
support@Web: ~
File Edit View Search Terminal Help
support@Web:~$ sed -i '10,12s/REQUEST/GET/' /var/www/WebServer/index.php
support@Web:~$ sed -n '9,17 p' /var/www/WebServer/index.php
support@Web:~$ sed -i '10,12s/GET/REQUEST/' /var/www/WebServer/index.php
support@Web:~$ sed -n '9,17 p' /var/www/WebServer/index.php
support@Web:~$
Type here to search
4:37 PM
9/28/2019


HTMLi Vulnerability and Mitigation
File Edit View Search Terminal Help
support@Web:~$ sed -i '10,12s/RE
support@Web:~$ sed -n '9,17 p' /
BRINGING UP THE BROWSER
3 Click the refresh button on the browser and observe the result.
< 'radi
HTML INPUT FIELD NOT RENDERED
4 Right-click the webpage and select View Page Source.
Save Page As...
View Background Image
Select All
View Page Source
Inspect Element (Q)
Welc UrBank
VIEWING INDEX.PHP CLIENT-SIDE FILE
Final_Kali-2.0 - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-898524/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Applications
Places
Iceweasel
Sat 17:40
UrBank – Iceweasel
UrBank
urbank.com/?myusername=<input 'radio'>
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
< 'radio'>
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
4:40 PM
9/28/2019