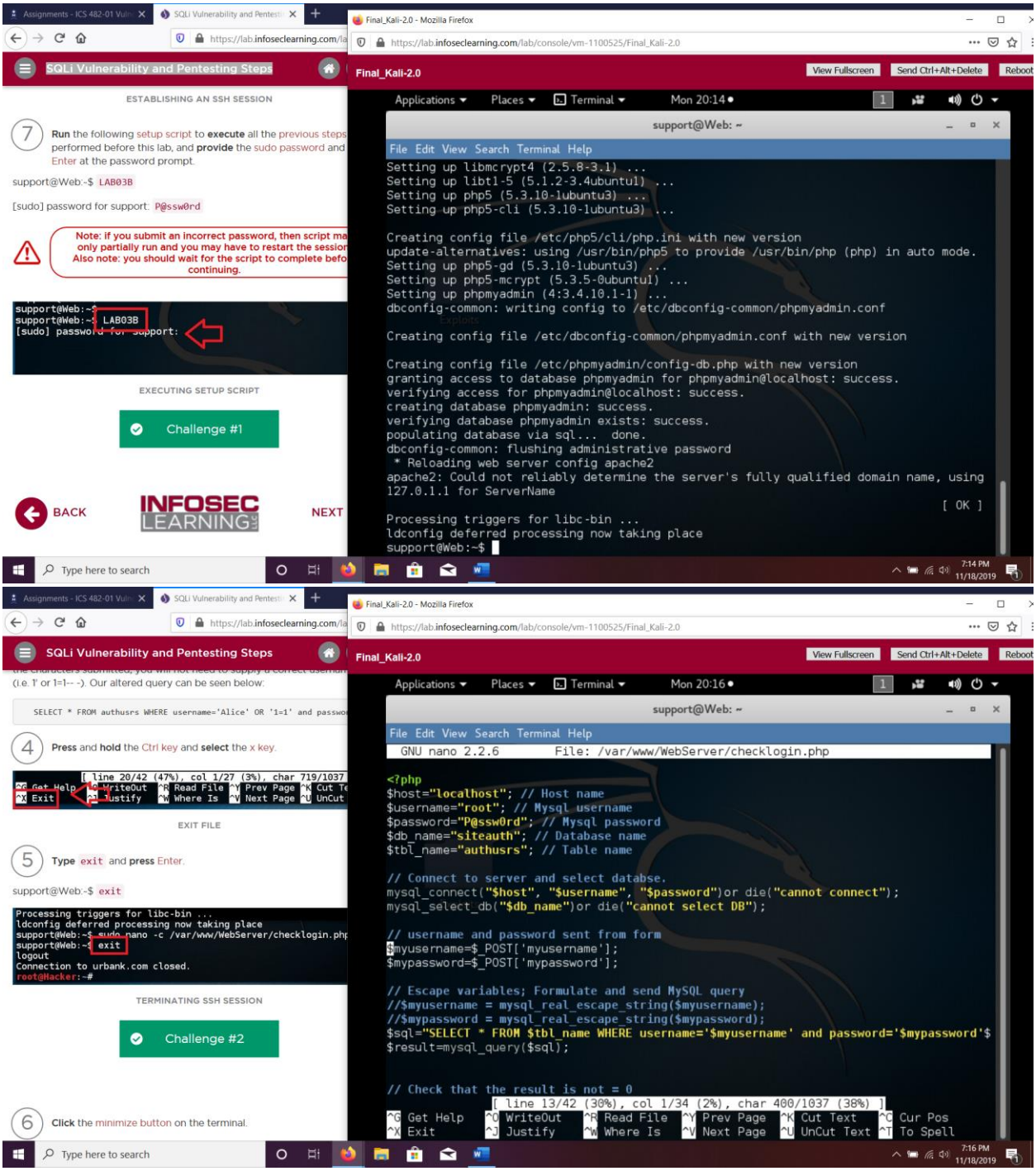
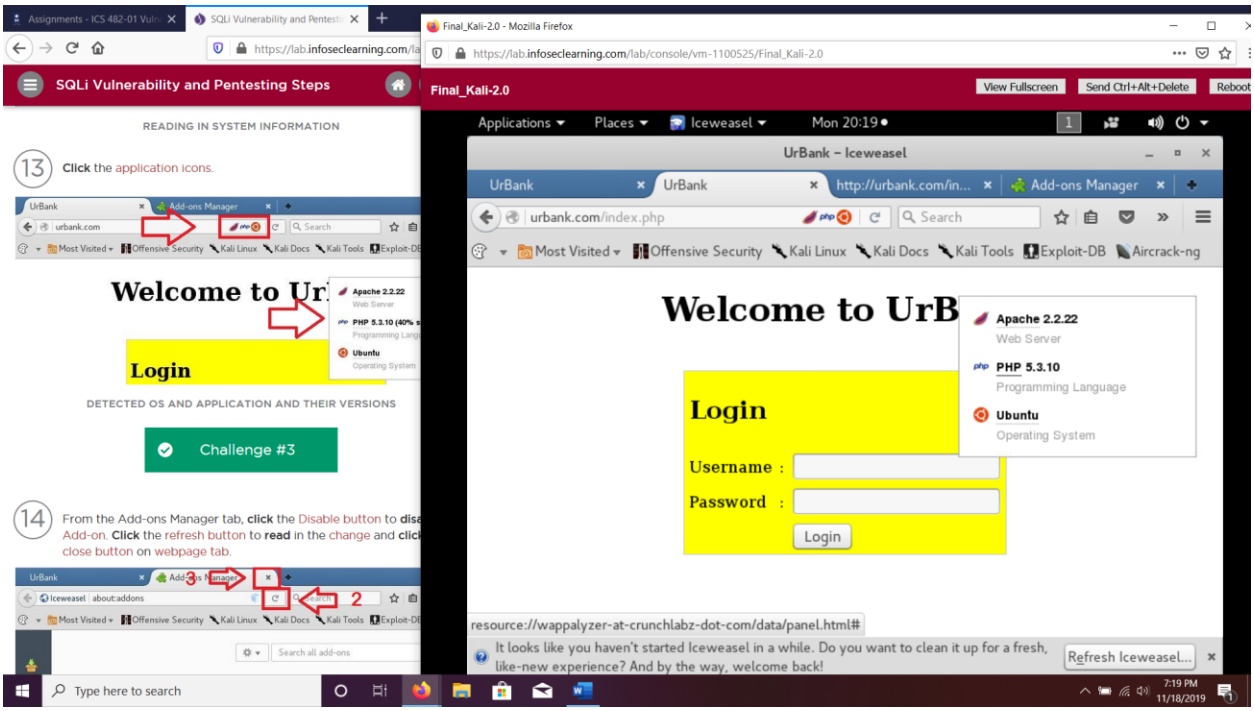
Ryan Brodsky

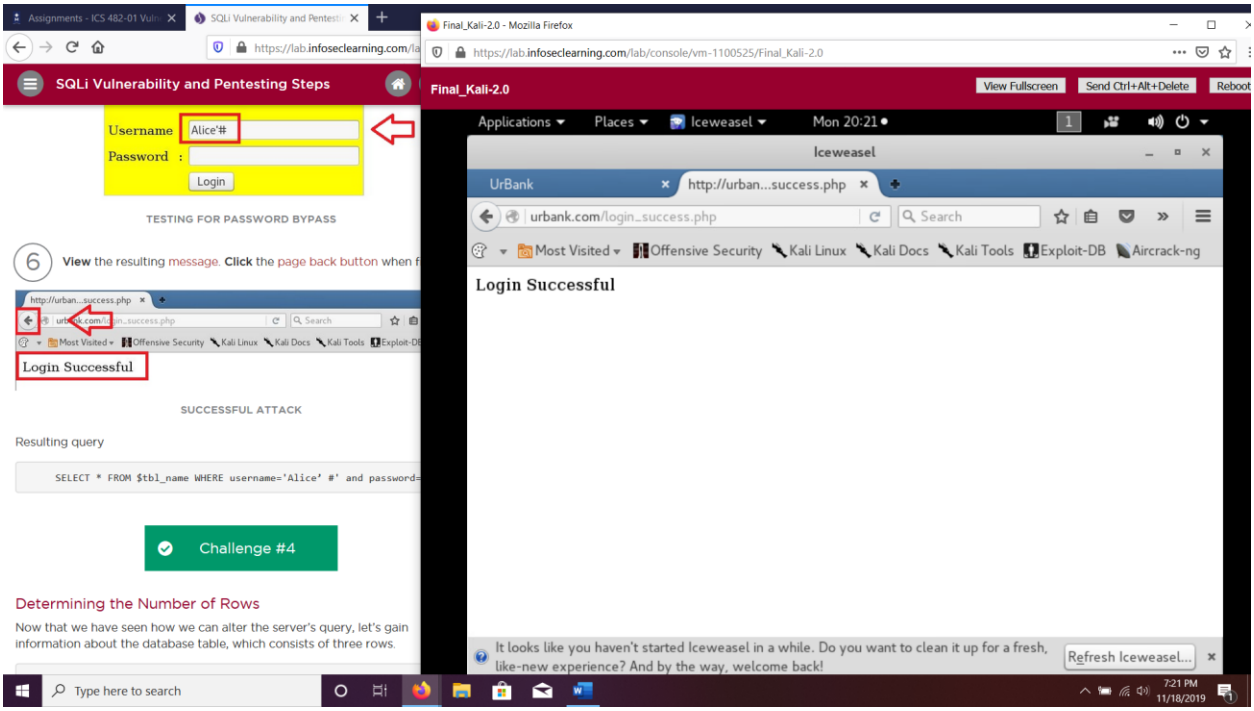
ICS482

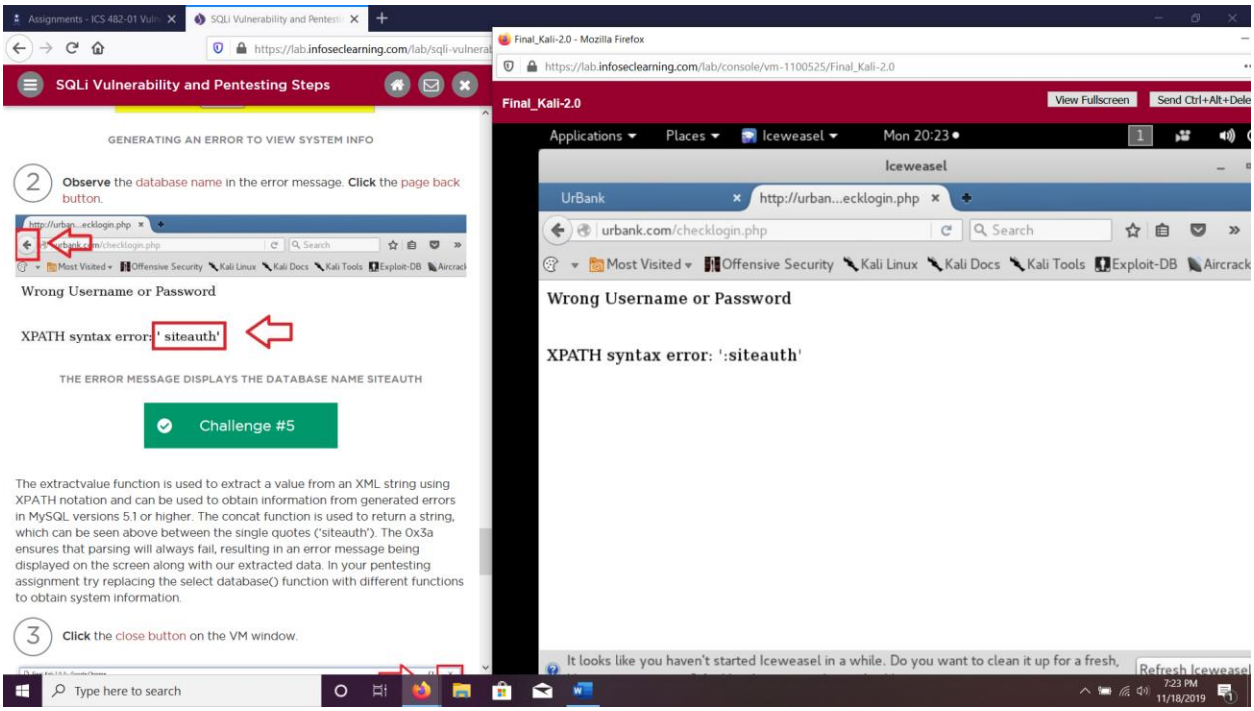
11/18/19

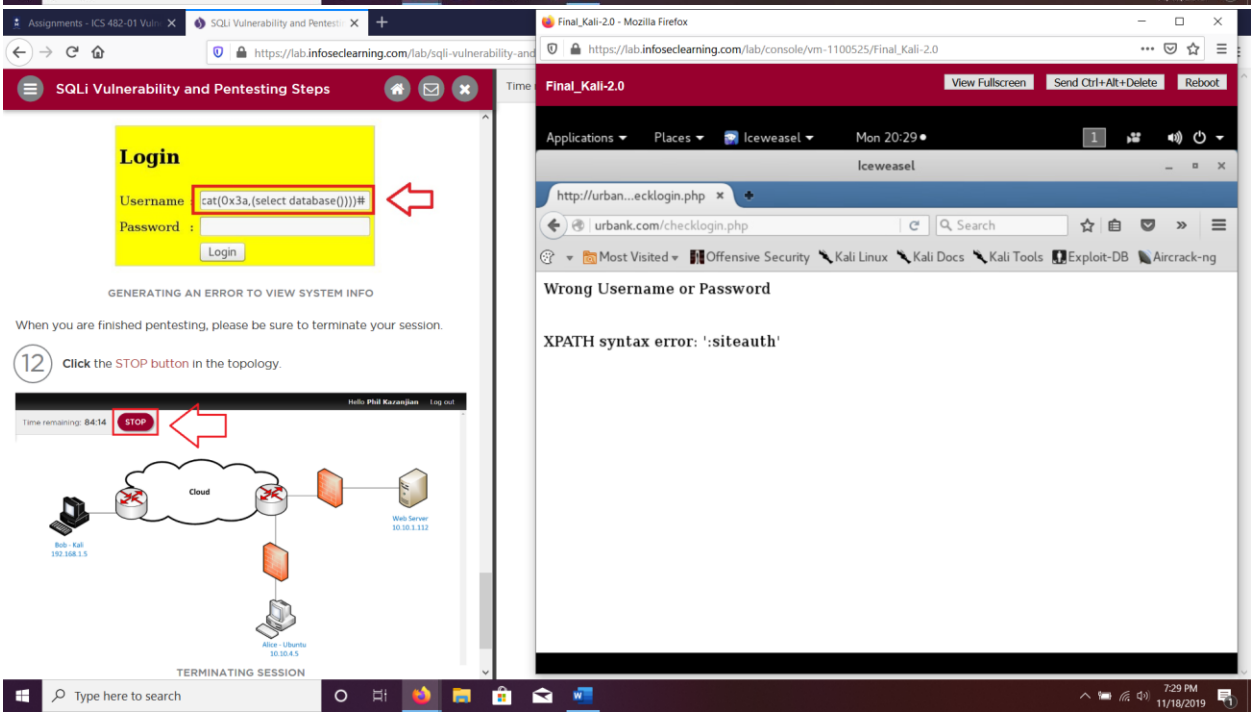
InfoSec Lab: SQLi Vulnerability and Pentesting Steps




SQLi Vulnerability and Pentesting Steps
READING IN SYSTEM INFORMATION
13 Click the application icons.
Welcome to Ur
Login
DETECTED OS AND APPLICATION AND THEIR VERSIONS
Challenge #3
14 From the Add-ons Manager tab, click the Disable button to dis
Add-on. Click the refresh button to read in the change and clic
close button on webpage tab.
Final_Kali-2.0 - Mozilla Firefox
https://lab.infoseclearning.com/lab/console/vm-1100525/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Applications
Places
Iceweasel
Mon 20:19
UrBank – Iceweasel
urbank.com/index.php
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Welcome to UrB
Apache 2.2.22
Web Server
PHP 5.3.10
Programming Language
Ubuntu
Operating System
Login
Username :
Password :
Login
resource://wappalyzer-at-crunchlabz-dot-com/data/panel.html#
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
7:19 PM
11/18/2019


SQLi Vulnerability and Pentesting Steps
Username Alice'#
Password :
Login
TESTING FOR PASSWORD BYPASS
6 View the resulting message. Click the page back button when f
Login Successful
SUCCESSFUL ATTACK
Resulting query
SELECT * FROM $tbl_name WHERE username='Alice' #' and password=
Challenge #4
Determining the Number of Rows
Now that we have seen how we can alter the server's query, let's gain information about the database table, which consists of three rows.
Final_Kali-2.0 - Mozilla Firefox
https://lab.infoseclearning.com/lab/console/vm-1100525/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Applications
Places
Iceweasel
Mon 20:21
Iceweasel
http://urban...success.php
urbank.com/login_success.php
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Login Successful
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
7:21 PM
11/18/2019


SQLi Vulnerability and Pentesting Steps
GENERATING AN ERROR TO VIEW SYSTEM INFO
2 Observe the database name in the error message. Click the page back button.
Wrong Username or Password
XPATH syntax error: ' siteauth'
THE ERROR MESSAGE DISPLAYS THE DATABASE NAME SITEAUTH
Challenge #5
The extractvalue function is used to extract a value from an XML string using XPATH notation and can be used to obtain information from generated errors in MySQL versions 5.1 or higher. The concat function is used to return a string, which can be seen above between the single quotes ('siteauth'). The 0x3a ensures that parsing will always fail, resulting in an error message being displayed on the screen along with our extracted data. In your pentesting assignment try replacing the select database() function with different functions to obtain system information.
3 Click the close button on the VM window.
Final_Kali-2.0 - Mozilla Firefox
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Dele
Iceweasel
UrBank
http://urban...ecklogin.php
urbank.com/checklogin.php
Wrong Username or Password
XPATH syntax error: ':siteauth'
Type here to search


SQLi Vulnerability and Pentesting Steps
Login
Username cat(0x3a,(select database()))#
Password :
Login
GENERATING AN ERROR TO VIEW SYSTEM INFO
When you are finished pentesting, please be sure to terminate your session.
12 Click the STOP button in the topology.
STOP
Cloud
TERMINATING SESSION
Final_Kali-2.0 - Mozilla Firefox
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Iceweasel
http://urban...ecklogin.php
urbank.com/checklogin.php
Wrong Username or Password
XPATH syntax error: ':siteauth'
Type here to search