

Ryan Brodsky

ICS482

11/18/19

InfoSec Lab: SQLi Vulnerability and Pentesting Steps

The screenshot displays the 'SQLi Vulnerability and Pentesting Steps' lab interface. The left sidebar contains instructions for establishing an SSH session and executing a setup script. The right terminal window shows the execution of the setup script, which configures the environment for a web server and database. The terminal output includes the following steps:

- Setting up libmcp4 (2.5.8-3.1) ...
- Setting up libt1-5 (5.1.2-3.4ubuntu1) ...
- Setting up php5 (5.3.10-1ubuntu3) ...
- Setting up php5-cli (5.3.10-1ubuntu3) ...
- Creating config file /etc/php5/cli/php.ini with new version
- update-alternatives: using /usr/bin/php5 to provide /usr/bin/php (php) in auto mode.
- Setting up php5-gd (5.3.10-1ubuntu3) ...
- Setting up php5-mcrypt (5.3.5-8ubuntu1) ...
- Setting up phpmyadmin (4:3.4.10.1-1) ...
- dbconfig-common: writing config to /etc/dbconfig-common/phpmyadmin.conf
- Creating config file /etc/dbconfig-common/phpmyadmin.conf with new version
- Creating config file /etc/phpmyadmin/config-db.php with new version
- granting access to database phpmyadmin for phpmyadmin@localhost: success.
- verifying access for phpmyadmin@localhost: success.
- creating database phpmyadmin: success.
- verifying database phpmyadmin exists: success.
- populating database via sql... done.
- dbconfig-common: flushing administrative password
- * Reloading web server config apache2
- apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
- Processing triggers for libc-bin ...
- ldconfig deferred processing now taking place

The terminal window also shows the execution of a PHP file, which is a simple web application for testing SQLi vulnerabilities. The PHP code includes the following lines:

```
<?php
$host="localhost"; // Host name
$username="root"; // Mysql username
$password="P@ssw0rd"; // Mysql password
$db_name="siteauth"; // Database name
$table_name="authurs"; // Table name

// Connect to server and select database.
mysql_connect("$host", "$username", "$password")or die("cannot connect");
mysql_select_db("$db_name")or die("cannot select DB");

// username and password sent from form
$myusername=$_POST['myusername'];
$mypassword=$_POST['mypassword'];

// Escape variables; Formulate and send MySQL query
// $myusername = mysql_real_escape_string($myusername);
// $mypassword = mysql_real_escape_string($mypassword);
$sql="SELECT * FROM $table_name WHERE username='$myusername' and password='$mypassword'";
$result=mysql_query($sql);

// Check that the result is not = 0
```

Assignments - ICS 482-01 Vul... SQLi Vulnerability and Pentest... Final_Kali-2.0 - Mozilla Firefox

https://lab.infoseclearning.com/la... https://lab.infoseclearning.com/lab/console/vm-1100525/Final_Kali-2.0

SQLi Vulnerability and Pentesting Steps

READING IN SYSTEM INFORMATION

13 Click the application icons.

Welcome to UrB

Login

DETECTED OS AND APPLICATION AND THEIR VERSIONS

Challenge #3

14 From the Add-ons Manager tab, click the Disable button to disable the Add-on. Click the refresh button to read in the change and click the close button on webpage tab.

UrBank - Iceweasel

UrBank

http://urbank.com/in...

Add-ons Manager

urbank.com/index.php

Most Visited

Offensive Security

Kali Linux

Kali Docs

Kali Tools

Exploit-DB

Aircrack-ng

Welcome to UrB

Login

Username :

Password :

Login

Apache 2.2.22
Web Server

PHP 5.3.10 (40%
Programming Lang)

Ubuntu
Operating System

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...

7:19 PM
11/18/2019

Assignments - ICS 482-01 Vul... SQLi Vulnerability and Pentest... Final_Kali-2.0 - Mozilla Firefox

https://lab.infoseclearning.com/la... https://lab.infoseclearning.com/lab/console/vm-1100525/Final_Kali-2.0

SQLi Vulnerability and Pentesting Steps

TESTING FOR PASSWORD BYPASS

6 View the resulting message. Click the page back button when finished.

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

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.

UrBank - Iceweasel

UrBank

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...

7:21 PM
11/18/2019

Assignments - ICS 482-01 Vuln... SQLi Vulnerability and Pentest... Final_Kali-2.0 - Mozilla Firefox

https://lab.infoseclearning.com/lab/console/vm-1100525/Final_Kali-2.0

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.

http://urban...ecklogin.php

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.

It looks like you haven't started Iceweasel in a while. Do you want to clean it up for a fresh, Refresh Iceweasel

7:23 PM 11/18/2019

Assignments - ICS 482-01 Vuln... SQLi Vulnerability and Pentest... Final_Kali-2.0 - Mozilla Firefox

https://lab.infoseclearning.com/lab/console/vm-1100525/Final_Kali-2.0

SQLi Vulnerability and Pentesting Steps

12 Click the STOP button in the topology.

Time remaining: 8:434

Cloud

Web Server 10.10.1.112

Bob - Kali 10.10.1.5

Alice - Ubuntu 10.10.4.5

TERMINATING SESSION

7:29 PM 11/18/2019

Final_Kali-2.0

Applications Places Iceweasel Mon 20:23

http://urban...ecklogin.php

urbank.com/checklogin.php

Wrong Username or Password

XPATH syntax error: 'siteauth'

Final_Kali-2.0

Applications Places Iceweasel Mon 20:29

http://urban...ecklogin.php

urbank.com/checklogin.php

Wrong Username or Password

XPATH syntax error: 'siteauth'

Reboot