SMU®

CS 3339 Cyber Security Lab

LAB 8: PHP & SQL Injection

PART 1: SQL INJECTION TUTORIAL

Go through the SQL injection tutorial at
https://free.codebashing.com/free-content/php/sql_injection

Once you finish answer this question:
How can you best prevent SQL injection attacks? (Do some research)

PART 2: SETUP

1. Login to your Kali instance
2. Run the following commands from the terminal

```
apt update
apt install apache2
/etc/init.d/apache2 start
/etc/init.d/mysql start
apt -y install php7.3 libapache2-mod-php7.3
service apache2 restart
service mysql restart
```

3. Open MySQL in your terminal with the command: `mysql`
4. Run the commands:

```
CREATE DATABASE test;
quit;
```

5. Copy the contents of the **Lab 8/html** folder (from the .zip you downloaded for this assignment) into **/var/www/html**

You can also get the zip file from here: https://s2.smu.edu/~rtumac/cs3339/spring2020/Lab8/

6. Run the following command:

```
     mysql test < create_db.sql
```

7. Go back to the MySQL terminal. Run the following commands:
Create new user:

```
CREATE USER 'userhere'@'%' IDENTIFIED BY 'passwordhere';
```

Grant permissions to user:

```
GRANT ALL PRIVILEGES ON *.* TO 'userhere'@'%' WITH GRANT OPTION;
flush privileges;
```

8. Update new MySQL information in two files:
checklogin.php
searchResult.php

PART 3

Open a web browser and navigate to **localhost/login.html**

You can use the username: **john** and password: **1234** to login.
Your goal here is to NOT use that username or password to login to the website, instead use SQL injection.

Use what you learned from the tutorial in part 1 and what you can find online to help you login using SQL injection instead of the correct username and password.

What input did you use to complete this action? Specify your inputs on each field

PART 4

Now that you have logged in, navigate to localhost/search.html

This page has a basic search functionality to search for messages in a database. Some of these messages are public and others are private. This search bar only allows you to search for the public messages. Using SQL injection, get the search function to return all of the messages, both public and private.

What input did you use to complete this action? Specify your inputs on each field

PART 5

You have discovered that the name of the table that stores user information is members.

Go back to the localhost/login.html and use SQL injection to drop the table members from the database.

What input did you use to complete this action? Specify your inputs on each field

PART 6

Open up the file /var/www/html/checklogin.php in a text editor. This is the php file that is used to verify you have the correct username and password. As you have just seen, it does not work very well. Edit this file to help prevent SQL injection attempts.

This may take a bit of research. HINT: Google ‘mysqli prevent sql injection’

WHAT TO TURN IN

1. Document containing your answers to the questions highlighted in red
2. Edited checklogin.php and an explanation of how its security flaws were addressed