LAB EXERCISE

9

COMP3134

Introduction to Cyber Security

Week: 14

Objective(s):
Attacking the database server and applying mitigation techniques

Learning Outcome(s):
Classify levels of database insecurities
Compare and differentiate SQL injections
Critique and execute mitigation techniques

Table of Contents

Contents

Summary 3

A. Clone GitHub Repo 3

B. Connect to Droplet Server 3

C. Log Into Droplet Database 3

D. Database Structure Set-Up 4

E. Database Data Dump 4

F. Create PHP Page to Interact with Database 4

G. Testing and Exploiting SQL Vulnerabilities 5

H. Mitigate SQL Injections 6

I. Export the Table Structure & Data 6

J. Commit and Upload Changes to GitHub repo 6

Summary

Goal: Attacking the database server and applying mitigation techniques

In Effort To: Compare, classify and differentiate levels of database insecurities with the goal of critiquing and executing mitigation techniques to prevent SQL injections

A. Clone GitHub Repo

Clone course GitHub repo to any location on your local machine
Navigate to the location above and create a folder named **wk13**
Use this local folder created above to create all the files necessary for this Lab Exercise

B. Connect to Droplet Server

Using GitBash (on Windows) or the Terminal (on Mac), connect to your droplet server by executing the following command

```
ssh droplet_username@droplet_ip_address
```

When prompted, user your droplet password

C. Log Into Droplet Database

Open the file that stores your mysql default password & copy the sql password

```
nano /root/.digitalocean_password
```

Log into your Droplet Database by authenticated

```
mysql -u root -p
```

When prompted for the password, paste the default password

D. Database Structure Set-Up

In the database interface, create a new schema
Create the following table in the newly created schema

Table named users
- id-PK
- username
- email
- firstname
- lastname
- active

E. Database Data Dump

Add 5 unique rows to the users table
Add 1 additional rows to the users table with the following info
- firstname = Ben
- active = 0
- Any other values for the other columns

F. Create PHP Page to Interact with Database

Create a PHP page named **getusers_1.php**
Create a form where a user can query database.
The form will have
- 1 input field
- 1 submit button
- The form method will be GET

The page will also have an HTML table below the form that will display the column values for all the results of the matched rows of the query.

When user submits form, it the page will query the database to find all matching rows where the first name equals the value of the query and the active column equals to 1

Do not sanitize input

G. Testing and Exploiting SQL Vulnerabilities

Create a text file name **sql_vulnerabilities_summary.txt**, write your observations for the following scenarios

1) Using the page **getusers_1.php**, type the following value into the form

Ben

Write your observations. Are they as expected? Explain in your own words what occurred.

2) Using the page **getusers_1.php**, type the following value into the form

Ben'--

*
Please note that the string above is 7 characters long:
Ben, a single quote, two dashes and a single space
*
Write your observations. Are they as expected? Explain in your own words what occurred.

3) Using the page **getusers_1.php**, type the following value into the form

Ben' or 1=1

Write your observations. Are they as expected? Explain in your own words what occurred.

H. Mitigate SQL Injections

To mitigate SQL injections, apply prepared statements in your programing language.
Create a file named **getusers_2.php**. Copy the contents of **getusers_1.php** as your starting point.
Apply prepared statements and re-run the 3 scenarios from Step G

I. Export the Table Structure & Data

Export the table structure and data from the schema created in this exercise.
Name the file **dump.sql**

J. Commit and Upload Changes to GitHub repo

Commit the changes to your repo by:

1. Opening a GitBash window and ensure that it is connected to your local machine
2. Navigate to local repository directory location
3. Add all the files completed in this Lab Exercise
4. Commit the changes
5. Push the changes to your GitHub course repo

Please refer to the instructions in the last section of Lab Exercise 1