Lab: Database Security

# Setup

In Kali, enter the following command to enter the MySQL terminal.

mysql -uroot -ppassword

In the MySQL terminal, execute the following two commands to create the application’s database account.

CREATE USER 'itsc315'@'localhost' IDENTIFIED BY 'password';

GRANT ALL PRIVILEGES ON \* . \* TO 'itsc315'@'localhost';

Download the application ITSC315Lab7 and open in NetBeans.

Run the SQL script located in sait.database to create the database.

# Problem 1: Examining SQL Injection attacks against a Database

For this part, you are going to pretend you are “Abe”. Your credentials are abe/password. Log in as Abe to understand how the application works.

Your goal is to use blind SQL injection on the login form to determine the password for admin.

It is possible to do this without looking at the code and guessing what the structure of the database is. Hints will be provided during the scheduled lab time.

Optional: Use sqlmap to hack the application.

Optional: Dump the admin’s password or even whole users table into <h3>Hi ${currentUser.firstName}</h3>

# Problem 2: Secure the Application

Secure the application using the following techniques.

Required for this lab:

1. Implement PreparedStatements for all database queries. You need to change the repository (broker) layer only.

Optional:

1. Limit the privileges of the itsc315 database account to use the itsc315 account and only the SELECT, INSERT, DELETE, UPDATE operations.

<http://www.liquidweb.com/kb/grant-permissions-to-a-mysql-user-on-linux-via-command-line/>

1. Move the database credentials from DBUtil to web.xml using environment variables