**SQL Injection**

For this activity you will be creating a StudentInfo table containing student information and complete an SQL Injection. Please see the below instructions.

***Login into MySQL server***

1. Use the following command.

$ sudo mysql -u root -p

1. Enter your password and Press **Enter**.

***Create the StudentInfo table***

1. Use the following commands to create the StudentInfo table and fill the table with data.

> USE studentDB;

> CREATE TABLE StudentInfo (StudentID int,FirstName varchar(255), LastName varchar(255);

> INSERT INTO StudentInfo (StudentID, FirstName, LastName)

 -> VALUES (11123, “Julie”, “Johnson”);

> INSERT INTO StudentInfo (StudentID, FirstName, LastName)

 -> VALUES (44456, “Leroy”, “Jenkins”);

1. Display the StudentInfo table.

> SELECT \* FROM StudentInfo;

***Create stu2 table***

1. Use the following commands to create the Schedule2 table and fill the table with data.

> CREATE TABLE Schedule2 (StudentID int, SectID int, CourseName varchar(225), ClassTime varchar(255));

> INSERT INTO Schedule2 (StudentID, SectID, CourseName, ClassTime)

 -> VALUES (44456, 98765, “Intro to Java”, “9:30 a.m. – 10:45 a.m.”);

> INSERT INTO Schedule2 (StudentID, SectID, CourseName, ClassTime)

 -> VALUES (44456, 87654, “Chemistry 101”, “12:00 a.m.- 12:50 p.m.”);

INSERT INTO Schedule2 (StudentID, SectID, CourseName, ClassTime)

 -> VALUES (44456, 76543, “Calculus II”, “1:00 p.m. – 1:50 p.m.”);

Create a new table containing information about the classes of all students.

1. Create new table ClassRegistration.

> CREATE TABLE ClassRegistration (CourseName, ClassTime, SectionID);

> INSERT INTO ClassRegistration SELECT CourseName, ClassTime, SectionID FROM Schedule1 UNION ALL SELECT CourseName, SectID FROM Schedule2;

1. Display the Class Registration table.

> SELECT \* FROM ClassRegistration;

1. Use the following commands to complete an SQL Injection Based on a Batched SQL Statement.

> SELECT CourseName

 -> FROM Schedule1

 -> WHERE CourseName = “BIOL 101”;

 -> DROP TABLE Schedule1;

1. Check to see if Schedule1 table still exists.

> SELECT \* FROM Schedule1;

*You should get and error saying:*

ERROR 1146 (42S0R): Table ‘studentDB.Schedule1’ does not exist

1. Exit the MySQL Server.

>exit;

You have successfully completed an SQL Injection!