**SQL Injection Application**

Introduction

* This Java application was created to teach about SQL injection vulnerabilities and exploits, but we will also use it this semester as a target for vulnerability analysis and testing.

Installation instructions

* Download SQLInjection.jar into any chosen directory or folder on an on-campus system (Windows or Linux) where you can run Java from the command line.
* Java should be installed on most lab and personal systems, but if it isn't, it should be easy to install Java yourself. Java is available at <http://www.oracle.com/technetwork/java/javase/downloads/index.html> – all you need is the current Java runtime environment (JRE) to run this progam, but if you want to develop in Java you'll need the full Software Development Kit (SDK).

Execution instructions

* At the command line, you can run the application with:
  + java –jar SQLInjection.jar

Assignment, Part A: SQL Injection vulnerability testing instructions

* Using the SQL injection techniques we discussed in class, find as many different username and password string combinations as possible that demonstrate SQL injection techniques on this application.
* By “different”, I mean conceptually different, not just different in value for the same construct; e.g. some string that involves 1 = 1 is not different than 2 = 2, 3 = 3, etc. Different data types (e.g. characters and strings) will be considered different. Different logical ideas (e.g. using the last single quote to end off password content vs. using the SQL comment character to comment out the last single quote from the application) will be considered different attack ideas. The use of different meta-characters signifies different attacks as well.

Assignment, Part B: Other vulnerability testing instructions

* Using any other techniques (including those discussed in class or elsewhere), find any other vulnerabilities that can be exploited on this application.
* HINT: the Oracle connection username and password are within this application; see if you can find them
* REMINDER: if you discover the username/password application, do NOT alter the underlying database account, the username or password, or any tables found under this Oracle account – that is improper conduct under the general security ethics we've discussed and under the policies of this course.