The University of Sydney
School of Information Technologies

THE UNIVERSITY OF SYDNEY

INFO2222—Usability and Security S1 2018
Week 11 Assignment Questions

The assignment this week address a common flaw that exists in the world of software development - SQL Injection.

1 Theoretical Exploration SQL Injection

a) Research
Research and briefly explain what SQL injection is, how it can be exploited, it's potential impact and potential mitigations.

2 Practical Let's Get Coding...

In this section, you will be given a database file called *secretdata.db* and a python script called *sqli.py* that interacts with the SQLite3 database. You may need to install sqlite3 - on any debian based Linux this is achieved by 'sudo apt-get install sqlite3' and if you are running non-debian based Linux you will probably know how to Google ;)

To solve these exercises you are not permitted to modify the code to make solving it trivial - nor simply accessing the database without the code provided - that will not class as a valid solution to recieve marks.

a) Read The Code
Before running code, read it and understand what it does. Never trust code you receive blindly. Briefly explain what it does.

```
import sqlite3

input = raw_input('Enter the name \'Sam\': ')
conn = sqlite3.connect("secretdata.db")
cursor = conn.cursor()
cursor.execute("SELECT data FROM secrets WHERE name = '%s';" % input)
data = cursor.fetchall()

print(data)
```

b) Run The Code
Run the code and state what the normal output is for the program.

c) Perform an SQLi Attack
Perform an SQLi attack on this program. What is the secret data that would not be accessed when

following the programs instructions? How did you do this? Did you decode the secret data? Was it encrypted?

d) A Fix?
A friend states that the fix is easy, just use **cursor.fetchone()** instead of **cursor.fetchall()**. This way, only one result is returned and the attacker won't be able to see the result. Is this a valid fix?

e) The Correct Fix
Write the correct fix for this code and test it. How did you do it? Please present the code.