Week 11 Assignment Questions

1 Theoretical Exploration SQL Injection

1. Research Research and briefly explain what SQL injection is, how it can be exploited, it’s potential impact and potential mitigations.

SQL injection is a code injection technique that includes inserting SQL statements into an entry field for execution, altering the original SQL queries.

The injection is exploited by a security vulnerability of the software, like when a user’s input is invalidated and unsanitised, and the input itself is a series of SQL statements, that means the user can manipulate the query itself and gain access to the database, like forcing the query to return data that shouldn’t available to outsiders.

2 Practical

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

This code requires you to enter a name ‘Sam’

Then it will connect to the secretdata.db

And select the data whose name is ‘Sam’

And print it.

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

[('Correct operation of database',)]

1. Perform an SQLi Attack

The secret data is 'WW91Zm91bmR0aGVzZWNyZXQ='

I did this by input the name as” ' OR '1'='1 “

I decoded the secret data by base64 format decoder as ‘Youfoundthesecret’

It was encrypted

1. A Fix?

This is not a valid fix as the ‘one’ result that attacker see could still be the unwanted one, also, this will hinder the normal use of the database.

1. The Correct Fix

By sanitizing input, in my way, I would remove all quotations in the input.

import sqlite3

input = raw\_input(’Enter the name \’Sam\’: ’)

*input = input.replace("'","").replace('"',"")*

conn = sqlite3.connect("secretdata.db")

cursor = conn.cursor()

cursor.execute("SELECT data FROM secrets WHERE name = ’%s’;" % input)

data = cursor.fetchall()

print(data)