Software Security
Assignment 1

Follow the steps shown below to create a database and test SQL Injection

Step 1 -> Database creation
- Start your console
- Change the path to the directory of the python files
- Run the following command in your console: python3 Database.py
- Check if the file Lesson2.db is created in your working directory
- Check if the values inside the table match with the values of the query

Step 2 -> Logic Implementation
- Open the file Program.py in an editor of your choice (for example VS Code)
- Check the implementation of the function is_admin()

Step 3 -> Test Logic
- Uncomment/comment the functions is_admin() on line 17, 18 and 19 in Program.py
    - is_admin('ran')
    - is_admin('haki')
    - is_admin('foo')
- Save the changes after each change
- Run Program.py
- Check the output value

Step 4 -> Inject malicious SQL and get access to the application
- Uncomment is_admin("' Or 1=1; --") and rerun the application
- Save the changes
- Run Program.py
- Check if the returned value gives you admin permission

Step 5 -> Inject malicious SQL and elevate access rights
- Comment line 5 in Program.py
- Uncomment line 6 in Program.py
- Uncomment line 23 in Program.py and run the code is_admin("'; update users set admin = '1' where username = 'haki'; select True; --")
- Save the changes
- Check in Lesson2.db if the user "haki" has now admin permission

Deliverable:

Write a report and explain what happened in each step. If anything went wrong, explain the reason and what you did to fix it.