**Instruction for the SQL Injection Attack**

Both the containers are present in the folder named as SQLInjection along with the DML file.

There is another folder named scripts in which I have written three scripts with different functionalities such as-

1. **Script\_get\_admin.py:** By using this script we are inject a sql querry through the form on the login page using the username field to get the access as an admin and then the response is getting saved as an html file.
2. **Script\_bobby\_get1.py:** In this script we are editing the salary of the employee boby as 1$ by passing a different querry in the edit profile and then the response is getting saved as an html file.
3. **Script\_all\_get\_raise\_exceptBobby.py:** In this querry, salary of everyone else is getting raised except bobby. And then the response is getting saved as an html file.
4. **All\_at\_once.py :** This script is to do all these functions on a single hit. Basically it is a merger of all the other three scripts.