TP Base de données

1- Créer la base de données et les tables

Sur EduPython il y a un petit bouton à droite des outils “Démarrer SQLite DataBrowser”, c’est une interface graphique pour interagir avec la base de données.

Créer une base de données dans votre dossier de travail.

2- Ouvrez l’énoncé du bac que l’on a fait en cours pour le schéma des tables

Pour la table des clients ajoutez un champ email et mot de passe qui sont des chaines de caractère.

Créer ces tables avec l’outil graphique, vous voyez le SQL correspondant.

3 – Utilisez l’outil graphique pour entrer les références de meuble qui sont dans l’énoncé.

En Python maintenant

4 – Ouvrez la documentation de Python pour sqlite https://docs.python.org/3/library/sqlite3.html

Vous pouvez parcourir le début.

5- Suivez les instructions pour vos connecter à votre base de données que vous avez créée précédemment.

6- Ouvrez les deux fichiers csv contenant les informations à mettre dans les tables https://docs.python.org/3/library/csv.html (regardez notamment la notion de dialect et la classe Sniffer fournie par Python).

7- Encore en vous servant de la documentation sql, enregistrez le contenu des fichiers csv dans la base de données dans la table correspondante.

8 – Exécuter les requêtes demandées dans l’énoncé du bac mais en appelant directement le SQL dans Python.

Une injection SQL

1- Dans notre cas c’est un peu de la triche par ce qu’on a fait exprès de forger une chaine de caractère avant de l’envoyer
2- Demandez à l’utilisateur un email et un mot de passe et exécuter une requête qui retourne les informations qui correspondent au client en question. Ecrivez d’abord toute la chaine de caractère de la requête, une fois que la chaine est prête envoyez la directement.
3- En vous aidant de la section “guide how to” de la documentation Python sur sqlite, entre un input malicieux qui va retourner les données de tout le monde.
4- Faites pareil mais pour ajouter un nouvel utilisateur.
5- Utilisez la bonne méthode pour exécuter ces requêtes et protéger des injections SQL (de même, les solutions sont dans la documentation).