# INF3005 – Programmation web avancée

## Utilisation d'une base de données

Jacques Berger

# Objectifs

Introduire SQLite

Utiliser SQLite avec Python

Prévenir l'injection SQL

# Prérequis

Python

SQL

# Base de données

La majorité des applications web vont utiliser une certaine forme de base de données

Il existe plusieurs types de base de données

La plus courante est la base de données relationnelle

# SQL

Une base de données relationnelle sépare ses données dans des tables et chaque table contient des rangées et des colonnes

Les colonnes sont des champs; les rangées sont des enregistrements

# SQL

Les bases de données relationnelles utilisent le langage de requêtes SQL

Les applications envoient des requêtes SQL à la BD pour lire ou modifier ses données

# SQL

Le SQL est une notation standardisée mais certaines BD utilisent une version non standard du SQL

# SQLite

SQLite est une base de données sans installation et sans serveur

La BD est dans un fichier sur le disque, les données et le schéma sont dans le même fichier

# SQLite

Version courante : 3

SQL non standard

Légère et versatile, convient bien aux petites applications web

# SQLite

Pour une application avec un traffic élevé, un autre choix de BD serait plus adéquat

Exemple : mysql, postgres

# SQLite

Sur le site de SQLite, on peut télécharger 3 logiciels pour manipuler une BD SQLite

Le logiciel sqlite3 est une console de gestion permettant de lancer des requêtes sur un BD SQLite

# SQLite

En lançant SQLite avec un fichier de BD en paramètre, on peut s'y connecter

```
sqlite3 musique.db
```

# SQLite

Si la BD n'existe pas, on lance la commande en spécifiant le nom de fichier de la future BD

Dans la console, on peut créer la BD en exécutant le contenu d'un script SQL

```
.read musique.sql
```

# SQLite

Dans la console, on peut tester les requêtes SQL

# Python

Python supporte SQLite

Les fonctionnalités pour manipuler SQLite sont dans le module sqlite3

# Python

Voir les exemples

# Injection SQL

Patron d'attaque ciblant les bases de données

Si la requête SQL est mal construite, on peut mettre des données dans un champ d'une application qui vont endommager la BD

# Injection SQL

L'injection SQL est bien répandue sur le web

Il faut éviter de mettre des valeurs provenant de l'utilisateur directement dans une requête SQL

Voir un exemple vulnérable à l'injection SQL

# Injection SQL

On peut facilement se protéger contre l'injection SQL en utilisant des placeholders pour mettre les valeurs dans une requête SQL

Voir exemple

# Injection SQL

Vos applications web doivent être protégées contre l'injection SQL

Une révision du code utilisant la base de données peut aider à déceler les vulnérabilités

Les concaténations de chaînes de caractères dans une requête SQL sont toujours suspectes

# Plus loin...

SQLite
    https://sqlite.org/

Librairie sqlite3
    https://docs.python.org/2/library/sqlite3.html