Exercice : Création d'une API de gestion d'utilisateurs avec authentification JWT

Objectif :

Créer une API qui permet l'inscription, la connexion et l'accès à des ressources protégées via JSON Web Tokens (JWT).

Instructions :

1. Initialisez un nouveau projet Node.js et installez les dépendances nécessaires (Express, Bcrypt, JSON Web Token).
2. Créez les fichiers et répertoires nécessaires pour votre application (routes/, controllers/, models/, etc.).
3. Implémentez les routes /signup, /login et /profile dans les fichiers de routes.
    - POST /signup : Permet l'inscription d'un nouvel utilisateur avec un nom d'utilisateur et un mot de passe. Stockez les informations de l'utilisateur dans une base de données MySQL ou MongoDB après avoir haché le mot de passe avec Bcrypt.
    - POST /login : Permet à un utilisateur existant de se connecter en vérifiant les informations d'identification. Si les informations sont correctes, générez un JWT contenant l'ID de l'utilisateur.
    - GET /profile : Route protégée qui nécessite une authentification JWT. Utilisez un middleware pour vérifier la validité du JWT et renvoyer les informations du profil de l'utilisateur.
4. Testez votre API en utilisant des outils comme Postman ou cURL pour vous assurer que l'inscription, la connexion et l'accès aux ressources fonctionnent correctement.