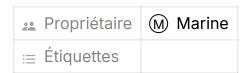
Exercice: Création d'une API d'authentification sécurisée avec Node.js et Express



Objectif

Vous allez développer une API REST permettant l'inscription, l'authentification et la gestion des sessions utilisateur en utilisant **Express**, **Argon2** pour le hash des mots de passe, et **JWT** pour l'authentification par token.

Instructions

Étape 1: Initialisation du projet

- 1. Créez un nouveau projet Node.js
- 2. **Créez un fichier** server.js et configurez un serveur Express avec JSON et CORS

Étape 2 : Gestion des utilisateurs

- 1. Ajoutez un tableau users pour simuler une base de données.
- 2. Créez une route POST /register pour inscrire un utilisateur :
 - Vérifiez si l'utilisateur existe déjà.
 - Hash le mot de passe avec Argon2.
 - Stockez l'utilisateur dans la base simulée.

Étape 3: Authentification des utilisateurs

1. Ajoutez une route POST /login qui :

- Vérifie si le nom d'utilisateur existe.
- Vérifie le mot de passe avec Argon2.
- Génère un token JWT.
- Définit un cookie sécurisé contenant le token.

Étape 4 : Protéger une route avec JWT

- 1. Créez un middleware authenticateToken pour vérifier le token dans les cookies.
- 2. Ajoutez une route GET /profile protégée par ce middleware.

Étape 5 : Déconnexion

1. **Ajoutez une route POST** /logout qui supprime le token en le remplaçant par un cookie expiré