Rapport Technique

Développement d'une API sécurisée pour Strateg.in

Présenté par :

TRAORE OGBAN MOUSSA

Table des matières

TABLE DES FIGURES

INTRODUCTION

Ce rapport détaille le cycle de développement d'une API sécurisée, élaborée en réponse aux besoins spécifiques de Strateg.in. Ce projet se concentre sur la conception et la réalisation d'une application permettant aux utilisateurs de réaliser des opérations d'inscription, de connexion, ainsi que d'accéder à une liste exhaustive des utilisateurs déjà enregistrés sur la plateforme. L'objectif central de cette initiative est de fournir une solution robuste et sécurisée, intégrant des fonctionnalités d'authentification avancées pour garantir une expérience utilisateur fiable et protégée.

I- Objectif du Projet

L'objectif principal du projet était de créer une API sécurisée en utilisant Node.js comme langage de programmation, respectant les normes et dépendances telles que ES6, les fonctions fléchées, Express, et Mongoose pour interagir avec une base de données MongoDB.

II- Architecture de l'application

L'application est structurée en trois parties principales : l'API (Application Programming Interface), l'Extranet, et l'App. L'API est responsable de gérer les routes d'inscription, de connexion, et d'accès aux utilisateurs. L'Extranet représente l'interface utilisateur permettant l'inscription et la connexion des utilisateurs. Enfin, l'App utilise le token généré lors de la connexion pour accéder à la liste des utilisateurs via l'API.

NB: ce projet a été developpé avec Vs code et pour tester l'application il faut installer postman

III- Mise en oeuvre

1. Routes d'Inscription et de Connexion

La route /register permet à un utilisateur de créer un compte en fournissant une adresse e-mail et un mot de passe. La route /login est utilisée pour récupérer un token après la création du compte. Les mots de passe sont sécurisés grâce à l'utilisation de la bibliothèque Bcrypt pour le hachage.

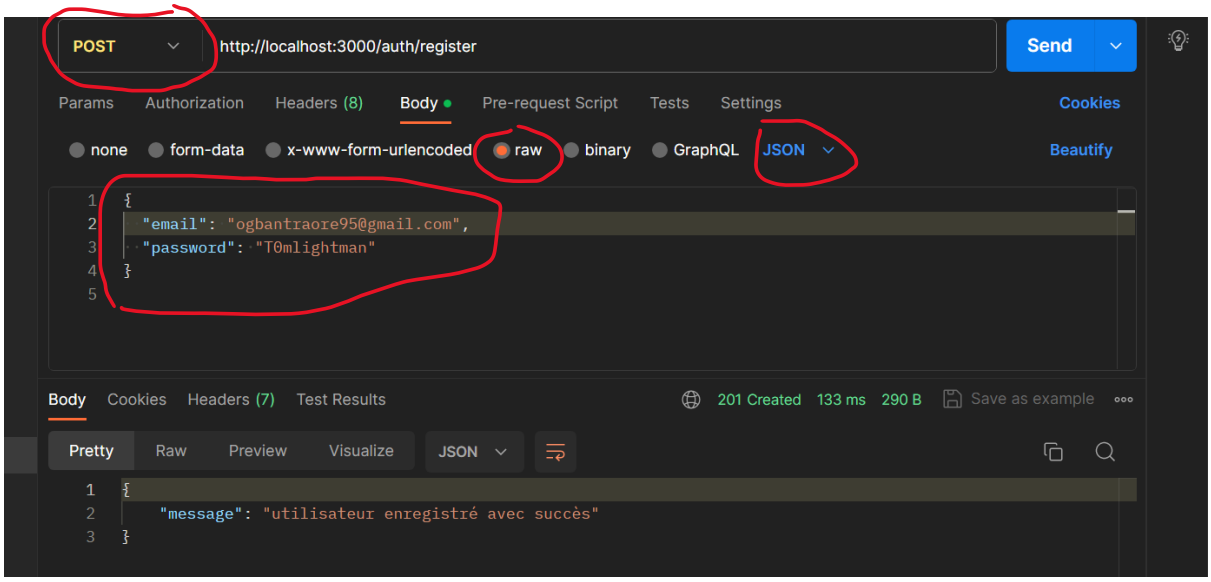

Figure 1 : Enregistrement d'un nouvel utilisateur

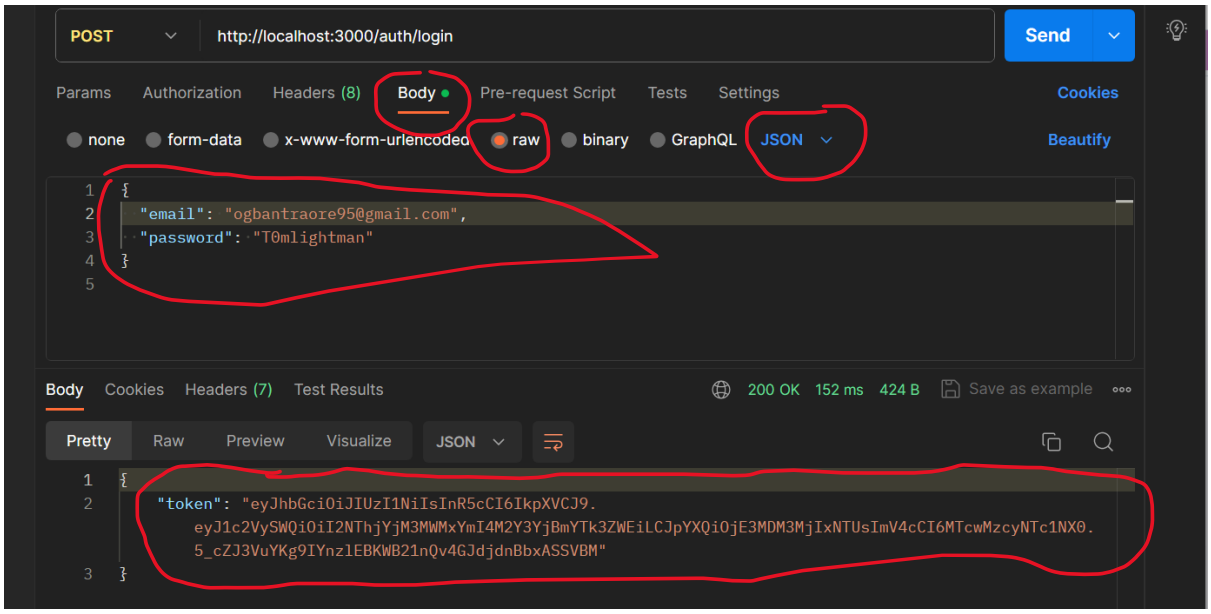

Figure 2 : Recuperation d'un token

2. Sécurité et Authentication

La sécurité est garantie par l'utilisation de tokens JWT (Json Web Tokens) pour gérer l'authentification des utilisateurs. Les mots de passe sont stockés de manière sécurisée dans la base de données grâce à Bcrypt.

3. Accès à la Liste des Utilisateurs

Une fois connecté, un utilisateur peut accéder à la liste des utilisateurs via la route /users. Cette route est protégée par un middleware d'authentification, garantissant que seuls les utilisateurs authentifiés peuvent accéder à cette ressource.

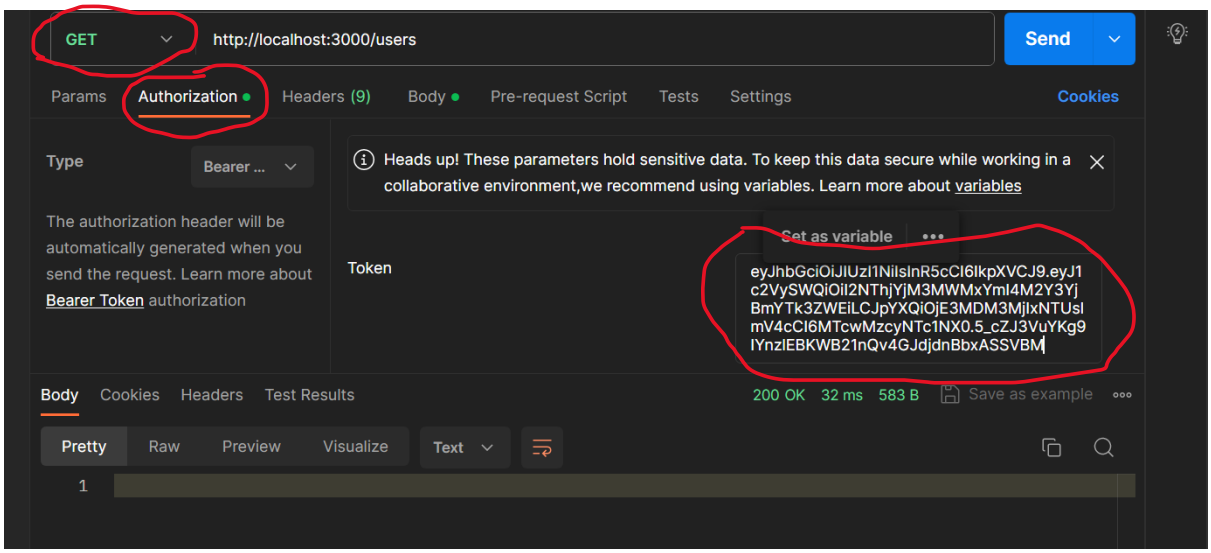

Figure 3 : Ajout du token

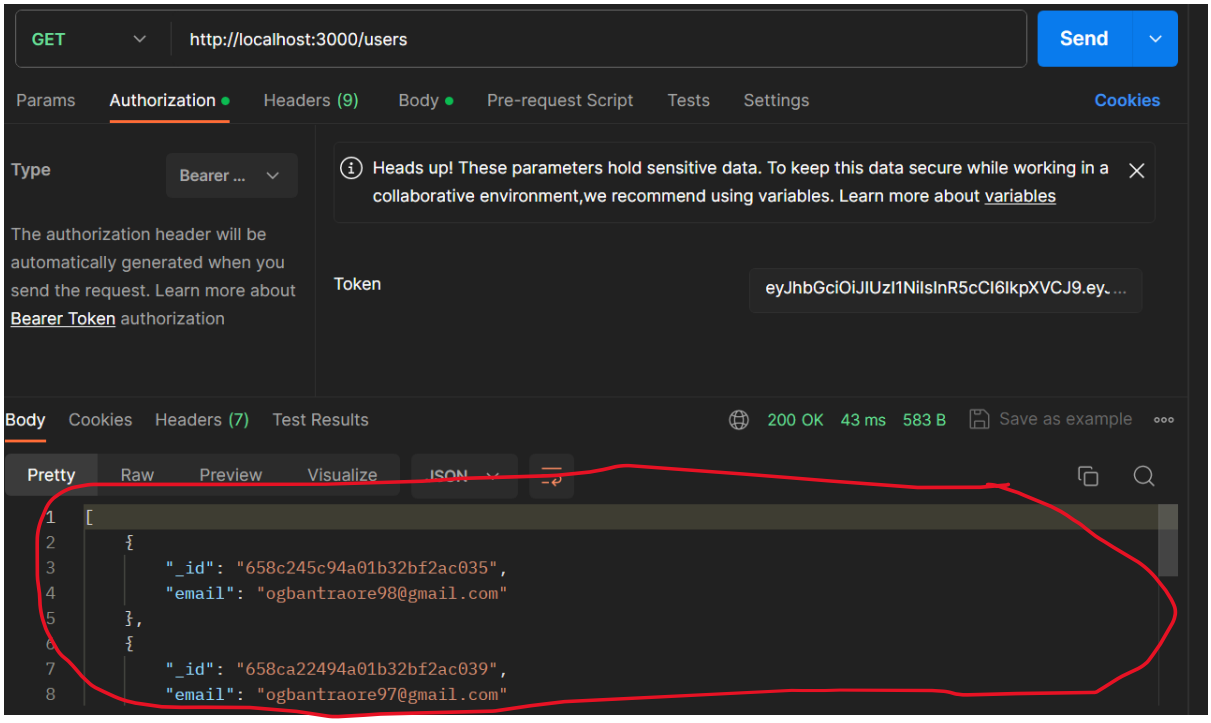

Figure 4 :Accéder à la liste des utilisateurs

IV. Base de données MongoDB

La base de données MongoDB est hébergée sur Atlas, offrant une solution robuste et évolutive. La connexion à la base de données est établie grâce à Mongoose, facilitant l'interaction avec les données.

CONCLUSION

Le projet a été un succès en fournissant une API sécurisée répondant aux exigences du test technique de Strateg.in. L'utilisation de technologies modernes telles que Node.js, Express, Mongoose, et MongoDB a permis de créer une application robuste et évolutive. L'implémentation de l'authentification par tokens JWT assure un niveau élevé de sécurité pour les utilisateurs.