Rapport technique Backend Secureprofile

Spring Boot

Holali David GAVI

Objectif du projet

Ce projet a pour objectif la mise en place d'une API REST sécurisée en Java avec Spring Boot. Il couvre les aspects suivants :

- Authentification et autorisation JWT
- Chiffrement des données sensibles
- Séparation des rôles (USER / ADMIN)
- Stockage et vérification des tokens d'actualisation
- Sécurité des endpoints

Stack technique

- Java 17
- Spring Boot 3.4.5
- Spring Security
- Spring Data JPA
- PostgreSQL (via Render)
- JWT (jjwt)
- BCryptPasswordEncoder
- AES pour chiffrement
- spring-dotenv (lecture du fichier .env)

Sécurité Implémentée

- JWT : access + refresh tokens
- Données chiffrées (AES) : email, username
- Passwords hachés avec BCrypt
- Rôles : USER / ADMIN avec @PreAuthorize
- JWT obligatoire pour tous les endpoints sensibles
- Contrôle d'accès par rôle (USER, ADMIN)
- Logout = suppression du refresh token
- Journalisation des actions sensibles

Objectifs CI/CD

- Automatiser le build Maven
- Analyser le code avec SonarCloud
- Dockeriser l’application backend
- Pousser l’image sur Docker Hub
- Versionner les builds

Étapes réalisées

- Intégration Maven + SonarCloud
- Gestion sécurisée des variables via GitHub Secrets
- Dockerfile propre avec ARG & ENV
- Workflow GitHub avec version hash
- Push automatique sur DockerHub