SPRING SECURITY

HALIMA EL AMRI.

1. Introduction +

Dans ce rapport, nous examinerons en détail l'implémentation de la sécurité dans le projet LabXpert. La sécurité demeure une priorité cruciale pour assurer la confidentialité, l'intégrité et la disponibilité des données médicales au sein du système LabXpert.

Authentication

L'**authentification** dans le contexte de Spring Boot se réfère au processus de vérification de l'identité d'un utilisateur qui souhaite accéder à une application ou à des ressources protégées par l'application. Spring Boot offre un cadre robuste pour gérer l'authentification des utilisateurs de manière sécurisée.

Autorisation

L'**autorisation** dans le contexte des systèmes informatiques et des applications fait référence au processus de détermination des actions spécifiques qu'un utilisateur authentifié est autorisé à effectuer dans un système..

2 Technologies!

LabXpert repose sur une stack technique solide pour assurer la sécurité et la robustesse du système. Les principales technologies utilisées incluent :

- [ ] Langage de Programmation : Java
- [ ] Backend : Spring Boot API RESTful avec Spring Security et OAuth2
- [ ] Gestion de Dépendances : Apache Maven
- [ ] Base de Données : PostgreSQL
- [ ] Serveur d'Application : Apache Tomcat
- [ ] Testing : JUnit & Mockito
- [ ] Sécurité : Spring Security (Authentification, Autorisation, OAuth2, JWT)
- [ ] CICD : Jenkins
- [ ] Système de Gestion de Version : Git et Github
- [ ] Documentation de l'API : Swagger

- [ ] Logging : Log4j

3 Méthodologie

LabXpert utilise une approche robuste basée sur les technologies et les concepts suivants :

Authentification des Utilisateurs avec OAuth 2.0

OAuth 2.0 est utilisé comme protocole d'authentification ouvert et standard, assurant que seul un utilisateur autorisé a accès aux fonctionnalités du système.

Gestion des Utilisateurs, des Rôles et des Autorisations

Un système de gestion des utilisateurs avec différents rôles et autorisations est mis en place pour contrôler l'accès aux fonctionnalités du système de manière granulaire.

Token JWT (JSON Web Token)

LabXpert utilise des tokens JWT générés lors de l'authentification, renforçant la sécurité en évitant le stockage d'informations d'authentification côté serveur.

OAuth 2.0 pour la Sécurité au Niveau des Services

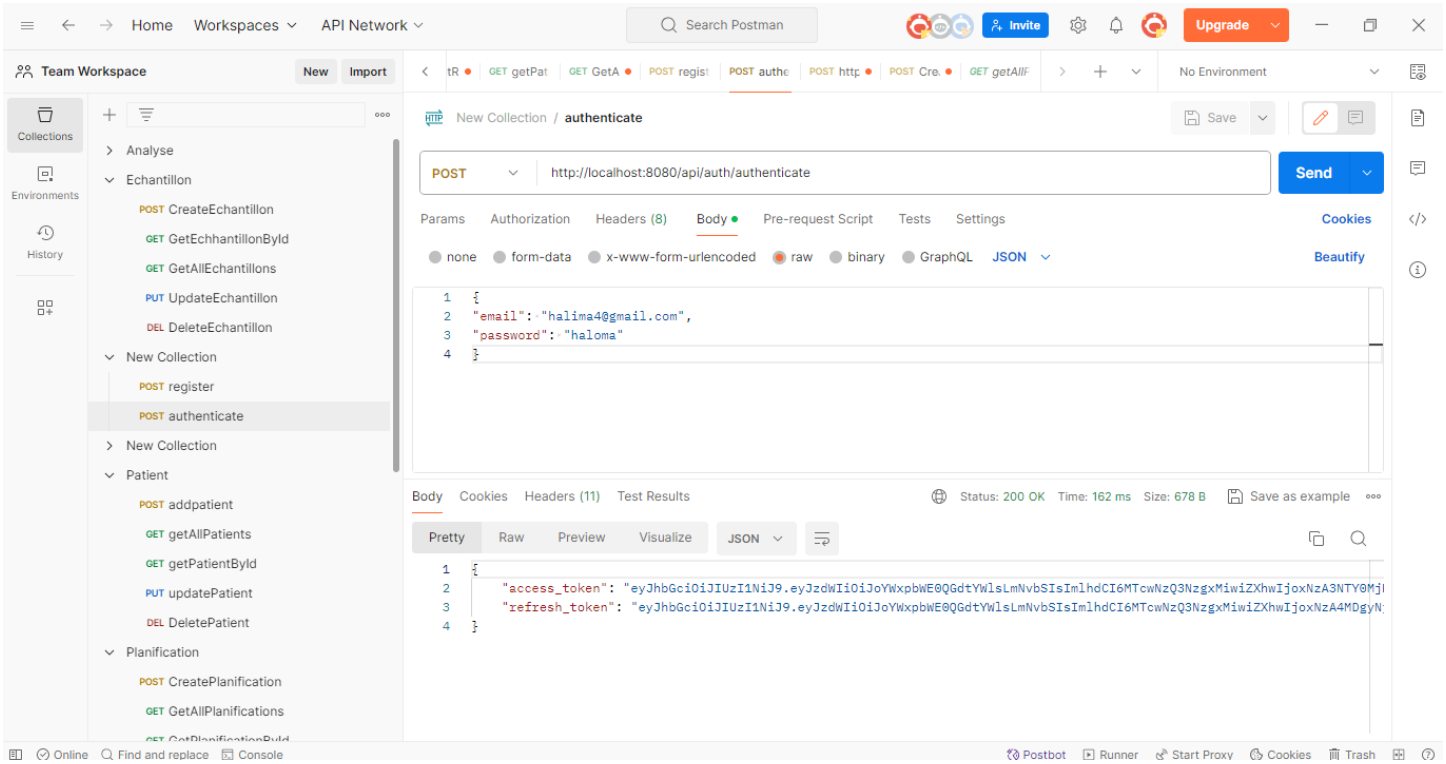
L'implémentation d'OAuth 2.0 au niveau des services garantit que seuls les utilisateurs autorisés peuvent effectuer des opérations spécifiques, renforçant ainsi la sécurité.

Intégration d'OAuth 2.0 avec JWT

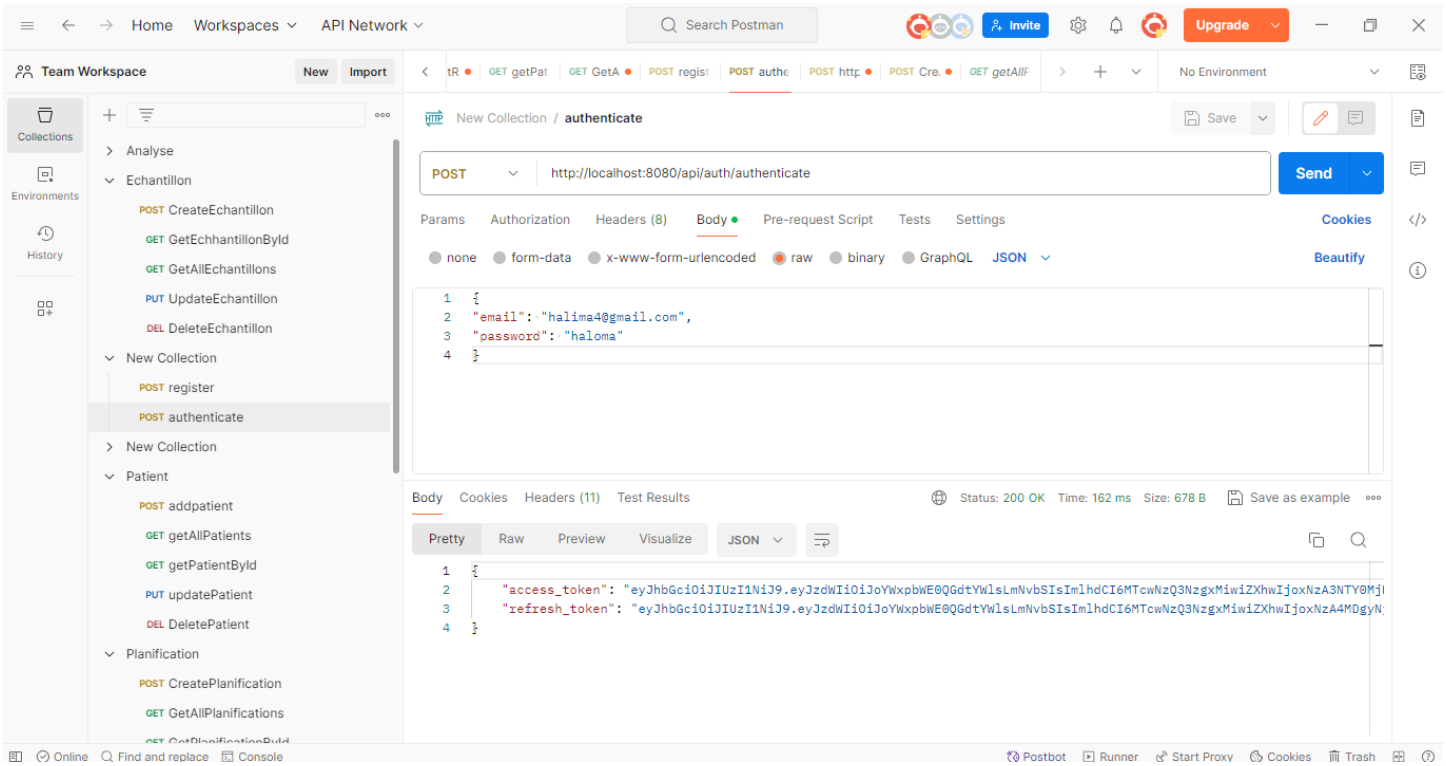
La combinaison d'OAuth 2.0 avec JWT offre une double couche de sécurité, assurant une authentification solide et la délégation sécurisée des autorisations

4 Implémentation

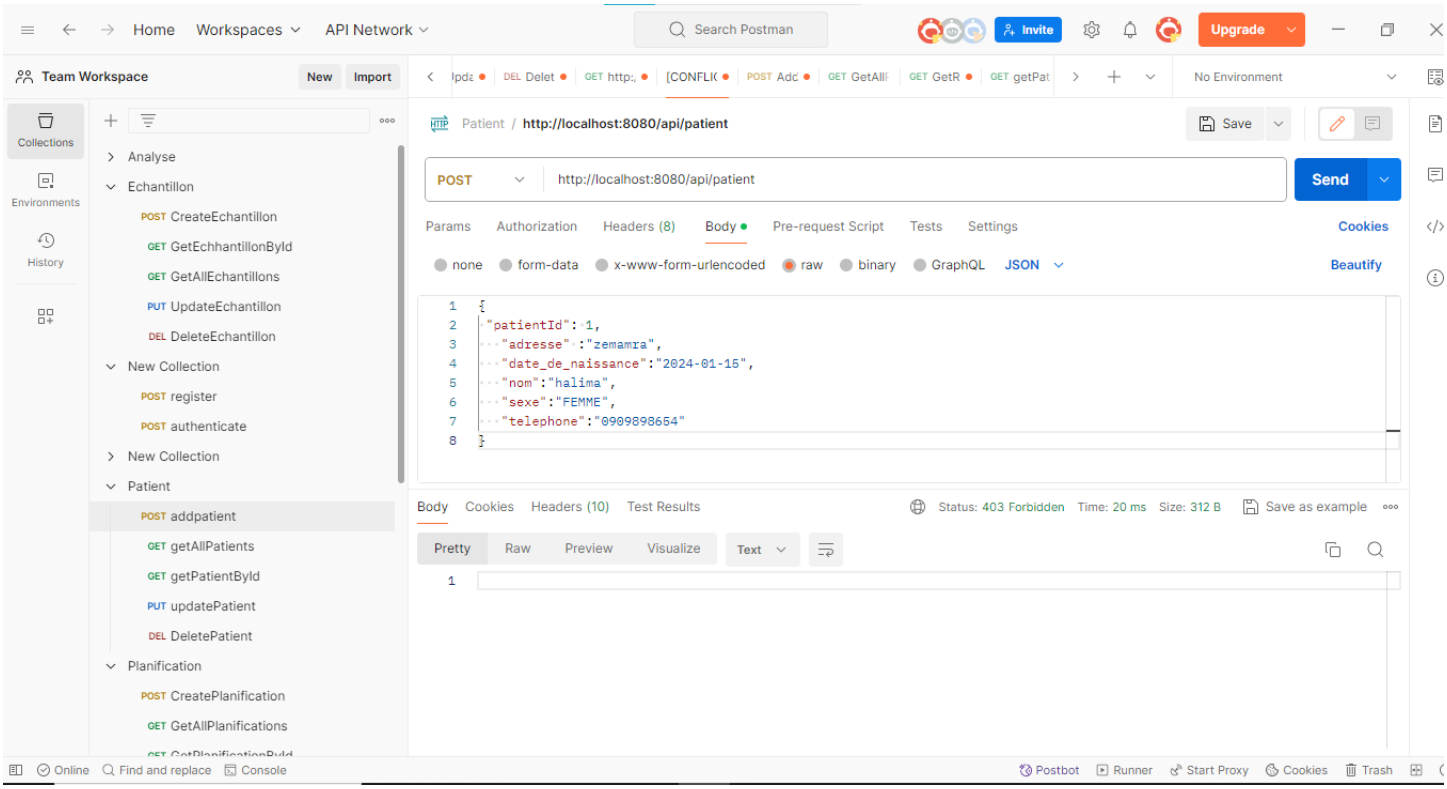
- **Registre(Admin)**



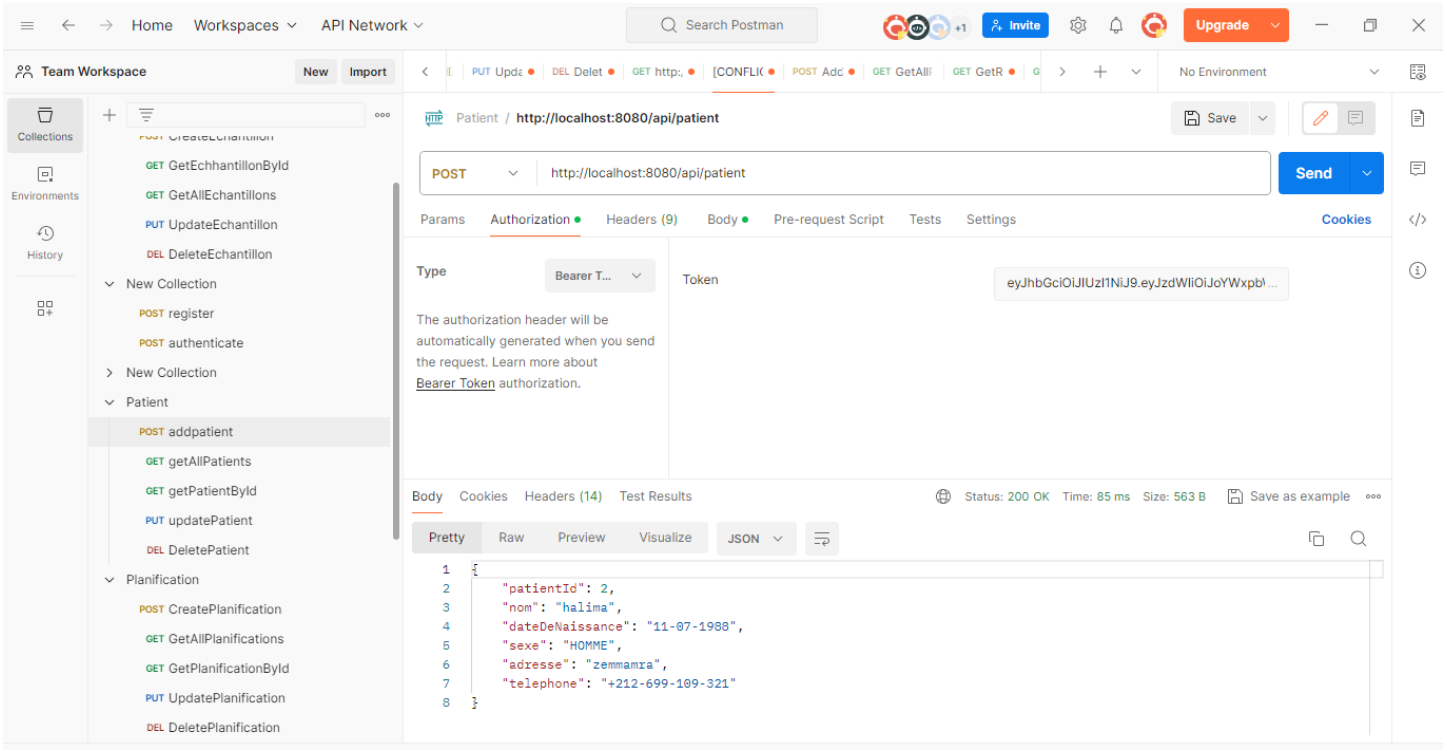
- **Authentification**



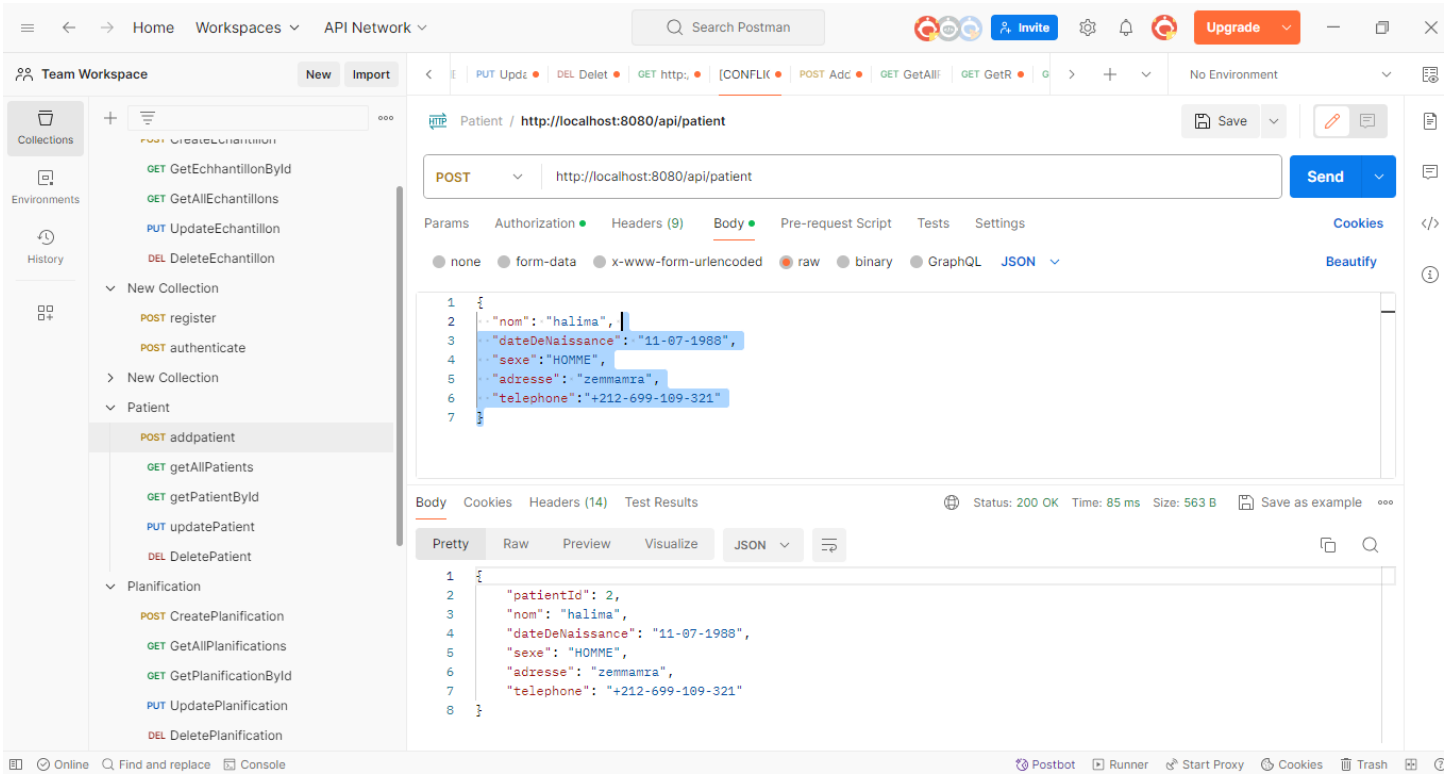
- **Création échouée**



- **Ajout de Autorisation**

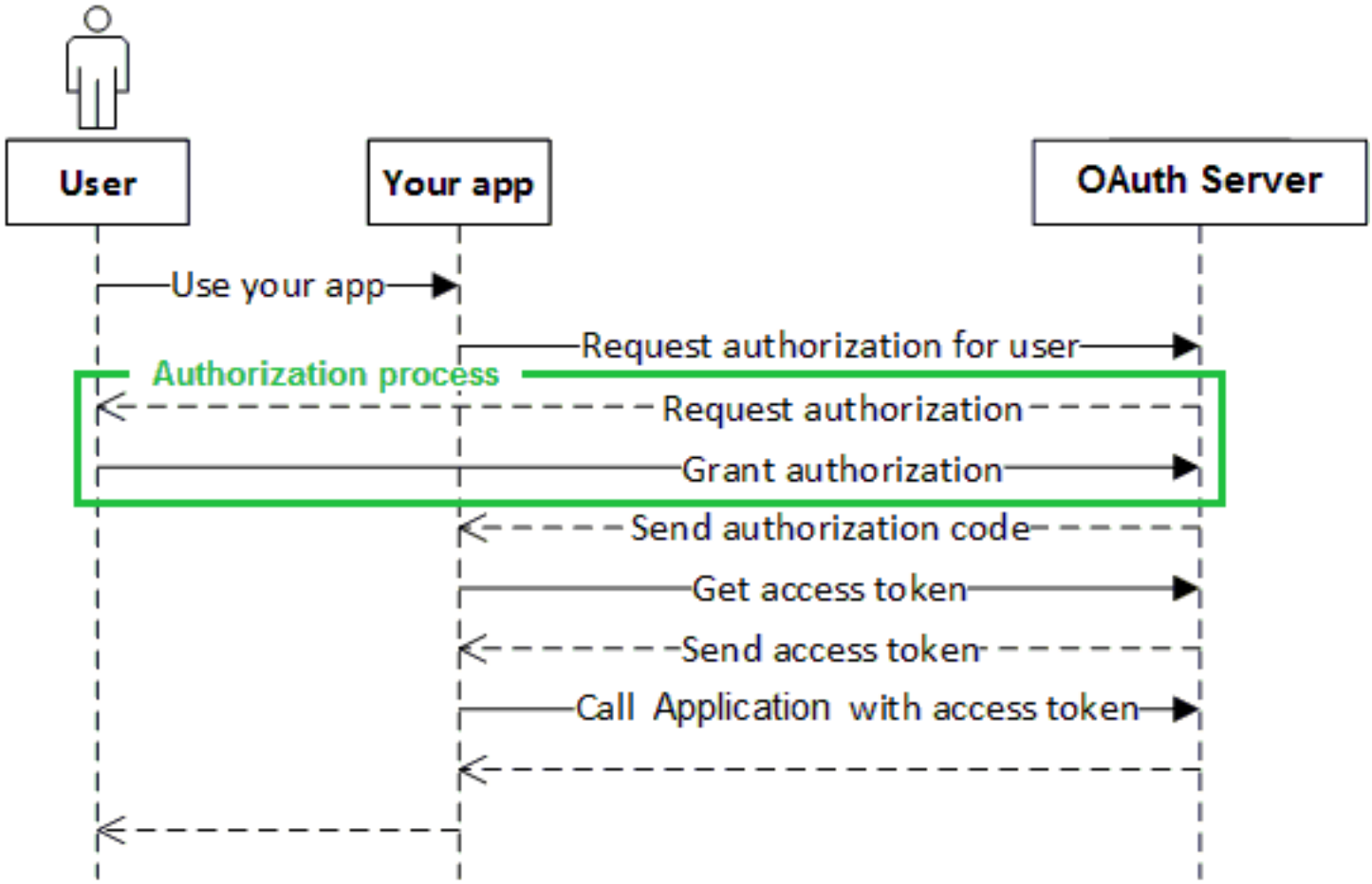


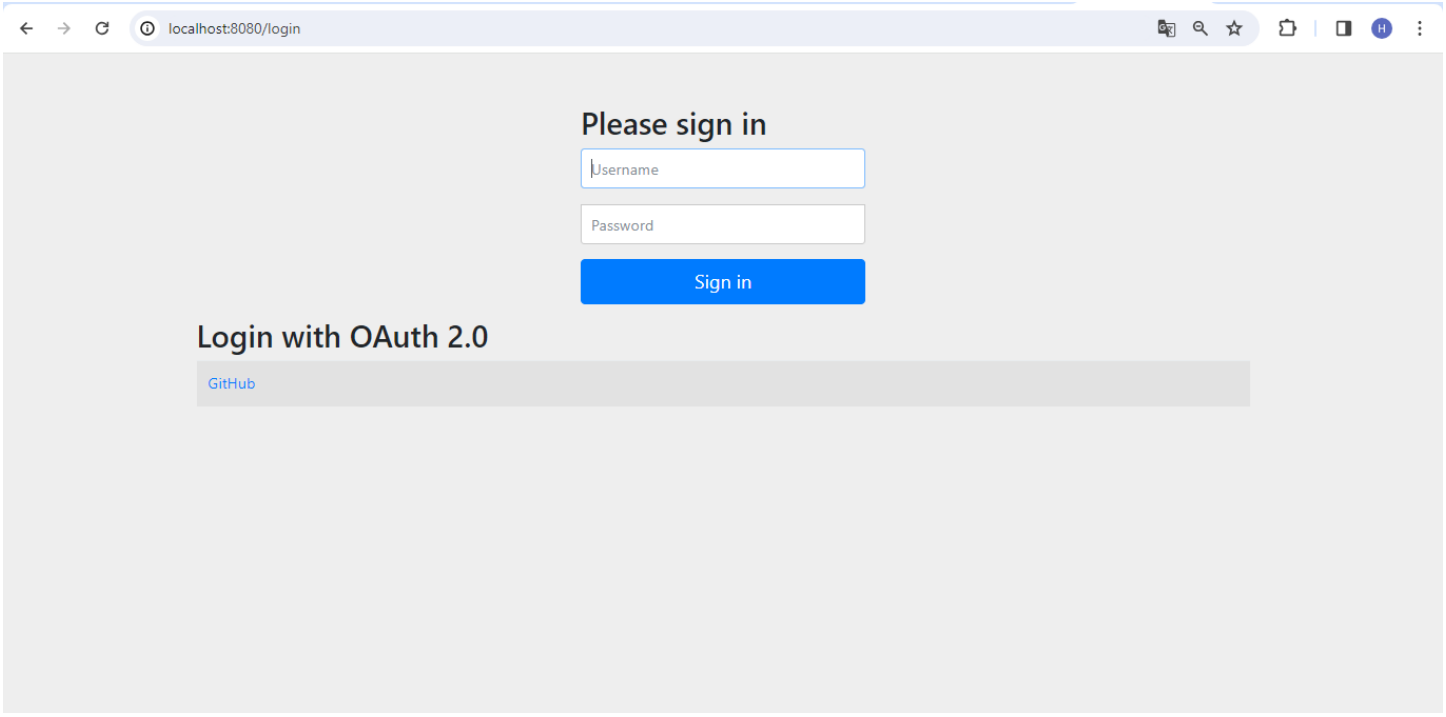
- **Création avec succès**

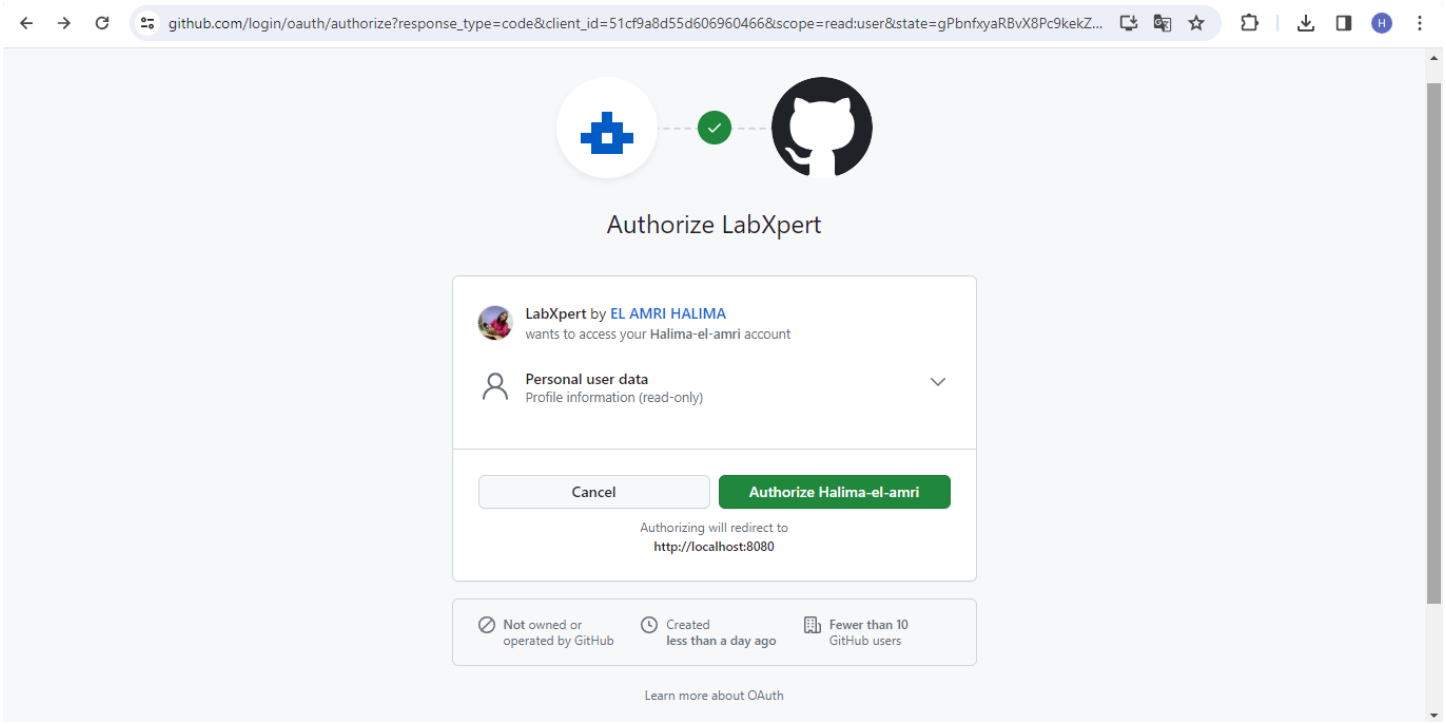


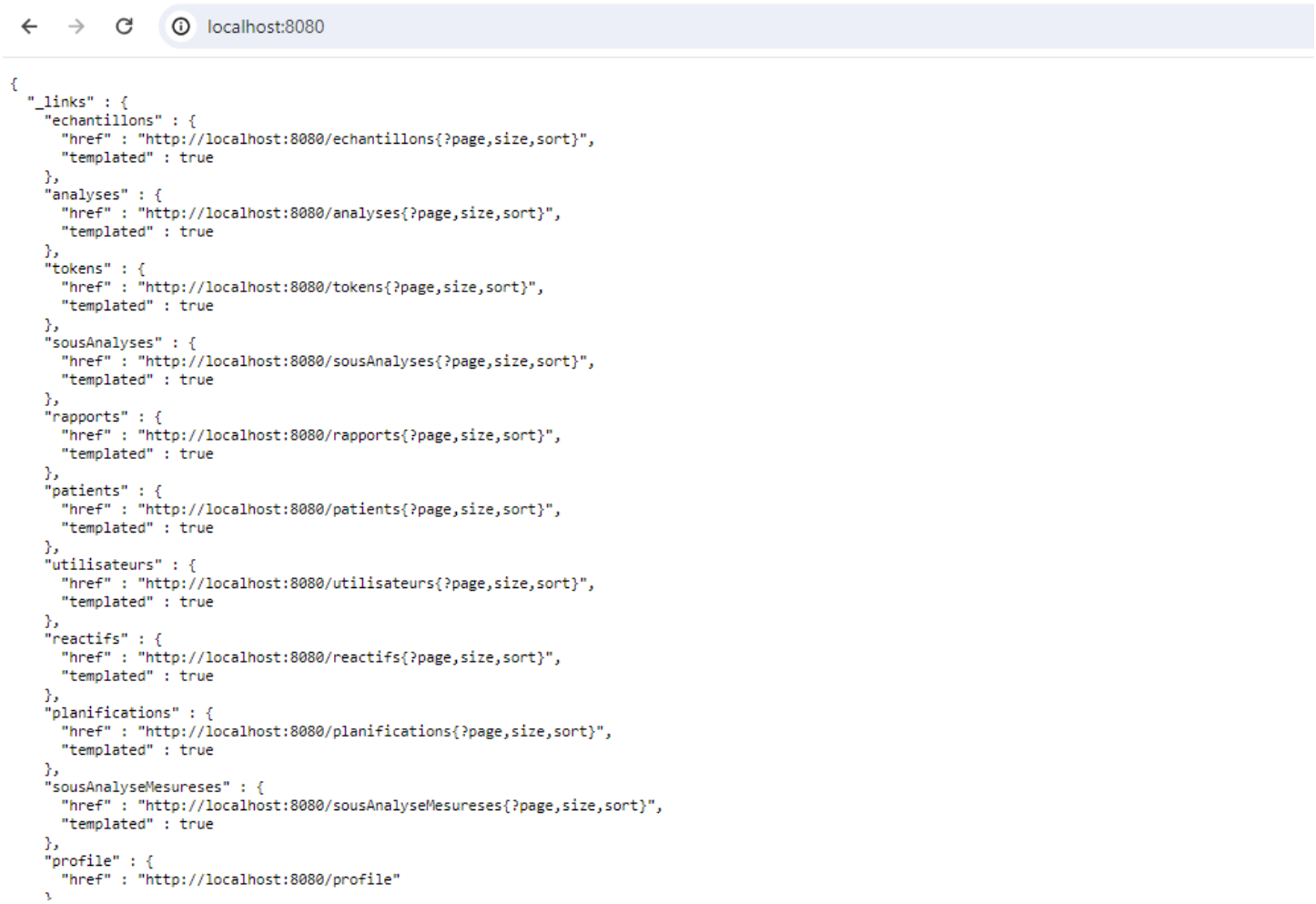
- **OAuth 2 dans notre application**

OAuth 2.0 est un protocole d'autorisation ouvert qui permet à des applications tierces d'obtenir un accès limité à des ressources protégées d'un serveur HTTP, telles que des profils utilisateur ou des données, sans avoir besoin de partager les identifiants d'authentification (comme des noms d'utilisateur et des mots de passe).


User
Your app
OAuth Server
Use your app
Request authorization for user
Authorization process
Request authorization
Grant authorization
Send authorization code
Get access token
Send access token
Call Application with access token


localhost:8080/login
Please sign in
Username
Password
Sign in
Login with OAuth 2.0
GitHub


github.com/login/oauth/authorize?response_type=code&client_id=51cf9a8d55d606960466&scope=read:user&state=gPbnfxyaRBvX8Pc9kekZ...
Authorize LabXpert
LabXpert by EL AMRI HALIMA
wants to access your Halima-el-amri account
Personal user data
Profile information (read-only)
Cancel
Authorize Halima-el-amri
Authorizing will redirect to
http://localhost:8080
Not owned or operated by GitHub
Created less than a day ago
Fewer than 10 GitHub users
Learn more about OAuth


localhost:8080
{
"_links" : {
"echantillons" : {
"href" : "http://localhost:8080/echantillons{?page,size,sort}",
"templated" : true
},
"analyses" : {
"href" : "http://localhost:8080/analyses{?page,size,sort}",
"templated" : true
},
"tokens" : {
"href" : "http://localhost:8080/tokens{?page,size,sort}",
"templated" : true
},
"sousAnalyses" : {
"href" : "http://localhost:8080/sousAnalyses{?page,size,sort}",
"templated" : true
},
"rapports" : {
"href" : "http://localhost:8080/rapports{?page,size,sort}",
"templated" : true
},
"patients" : {
"href" : "http://localhost:8080/patients{?page,size,sort}",
"templated" : true
},
"utilisateurs" : {
"href" : "http://localhost:8080/utilisateurs{?page,size,sort}",
"templated" : true
},
"reactifs" : {
"href" : "http://localhost:8080/reactifs{?page,size,sort}",
"templated" : true
},
"planifications" : {
"href" : "http://localhost:8080/planifications{?page,size,sort}",
"templated" : true
},
"sousAnalyseMesureses" : {
"href" : "http://localhost:8080/sousAnalyseMesureses{?page,size,sort}",
"templated" : true
},
"profile" : {
"href" : "http://localhost:8080/profile"

Conclusion

En intégrant des technologies de pointe telles que OAuth 2.0, JWT, et Spring Security, LabXpert offre une plateforme sécurisée et conforme aux normes pour le traitement des analyses médicales. La sécurité demeure une priorité absolue dans le développement et le déploiement continu de LabXpert, assurant ainsi la confidentialité et l'intégrité des données médicales.