Introduction

LabXpert est un système de gestion de laboratoire mettant l'accent sur la confidentialité, l'intégrité, et la disponibilité des données médicales. La sécurité demeure une priorité essentielle dans ce système, visant à assurer que seuls les utilisateurs autorisés bénéficient d'un accès aux fonctionnalités appropriées. Cette documentation offre un aperçu détaillé des fonctionnalités de sécurité intégrées dans LabXpert.

Fonctionnalités de Sécurité

Authentification des Utilisateurs via OAuth 2.0

LabXpert utilise le protocole d'authentification ouvert et standard OAuth 2.0, permettant aux utilisateurs de s'authentifier de manière sécurisée. Cette approche garantit que seuls les utilisateurs autorisés ont accès aux fonctionnalités du système.

Gestion des Utilisateurs, des Rôles, et des Autorisations

LabXpert dispose d'un système de gestion des utilisateurs avec divers rôles (techniciens, responsables de laboratoire, administrateurs, etc.), chacun se voyant attribuer des autorisations spécifiques. L'interface d'administration simplifie la gestion de ces rôles et autorisations.

Token JWT (JSON Web Token)

LabXpert génère des tokens JWT lors de l'authentification. Ces tokens, basés sur OAuth 2.0, sont inclus dans chaque requête ultérieure, 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. Cette approche granulaire renforce la sécurité, empêchant tout accès non autorisé même au sein des rôles définis.

Intégration d'OAuth 2.0 avec JWT

La combinaison d'OAuth 2.0 avec JWT offre une double couche de sécurité, assurant une authentification robuste et une délégation sécurisée des autorisations. Cela améliore la sécurité du système, crucial dans le contexte des données médicales.

Configuration de Sécurité

Configuration des Clés RSA

Les clés RSA sont configurées pour la génération et la vérification des tokens JWT. Elles sont utilisées pour signer et vérifier l'authenticité des tokens.

Implémentation de UserDetailsService

La classe CustomUserDetailsService implémente l'interface UserDetailsService pour charger les détails de l'utilisateur depuis la base de données. Elle récupère les informations de l'utilisateur, y compris son nom d'utilisateur, son mot de passe et ses rôles, pour l'authentification.

Configuration de Spring Security

La classe SpringSecurityConfig configure la sécurité de l'application Spring. Elle définit les règles d'autorisation, les filtres de sécurité, et les gestionnaires d'authentification pour protéger les ressources de l'application.

API REST Sécurisée

LabXpert expose une API REST sécurisée pour accéder aux fonctionnalités du système. Les contrôleurs REST sont protégés par des annotations @PreAuthorize qui vérifient les autorisations des utilisateurs avant l'exécution des méthodes.

Exemples d'Annotations @PreAuthorize

@PreAuthorize("hasAnyAuthority('SCOPE_ROLE_ADMIN', 'SCOPE_ROLE_LABORATORY_MANAGER')") : Cette annotation vérifie si l'utilisateur possède les autorisations nécessaires pour accéder à la ressource. Dans cet exemple, seuls les utilisateurs avec les rôles d'administrateur ou de responsable de laboratoire sont autorisés.

Conclusion

LabXpert s'engage à fournir une plateforme sécurisée et conforme aux normes pour le traitement des analyses médicales. En intégrant des normes de sécurité telles que OAuth 2.0 et JWT, LabXpert garantit la protection des données sensibles, suivant les meilleures pratiques en matière de sécurité.