Tests de Vulnérabilité

Introduction

La sécurité applicative est un enjeu majeur dans le développement logiciel, en particulier pour les applications manipulant des données sensibles. Afin d'évaluer la robustesse de notre application **MySurvey** face aux vulnérabilités potentielles, nous avons mis en place une analyse automatisée via **SonarQube**.
Ce test de vulnérabilité vise à :

- Identifier les failles de sécurité potentielles.
- Détecter les problèmes de maintenabilité pouvant impacter la qualité du code à long terme.
- S'assurer que les bonnes pratiques de développement sont respectées.

L'analyse a été intégrée dans notre pipeline, permettant un suivi en continu des problèmes de sécurité et de qualité à chaque mise à jour du code.

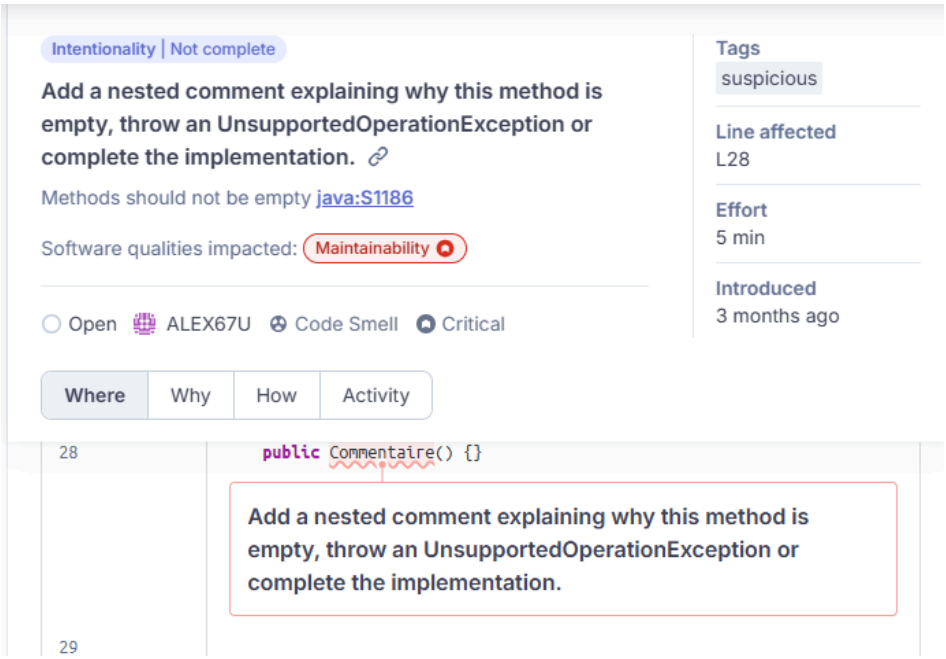
1. Intégration SonarQube

Processus d'Analyse :
À chaque push ou pull request sur la branche principale, notre pipeline CI/CD déclenche une analyse SonarQube. Cette analyse permet de générer un rapport détaillé qui identifie les vulnérabilités, les problèmes de maintenabilité et d'autres aspects de qualité du code.

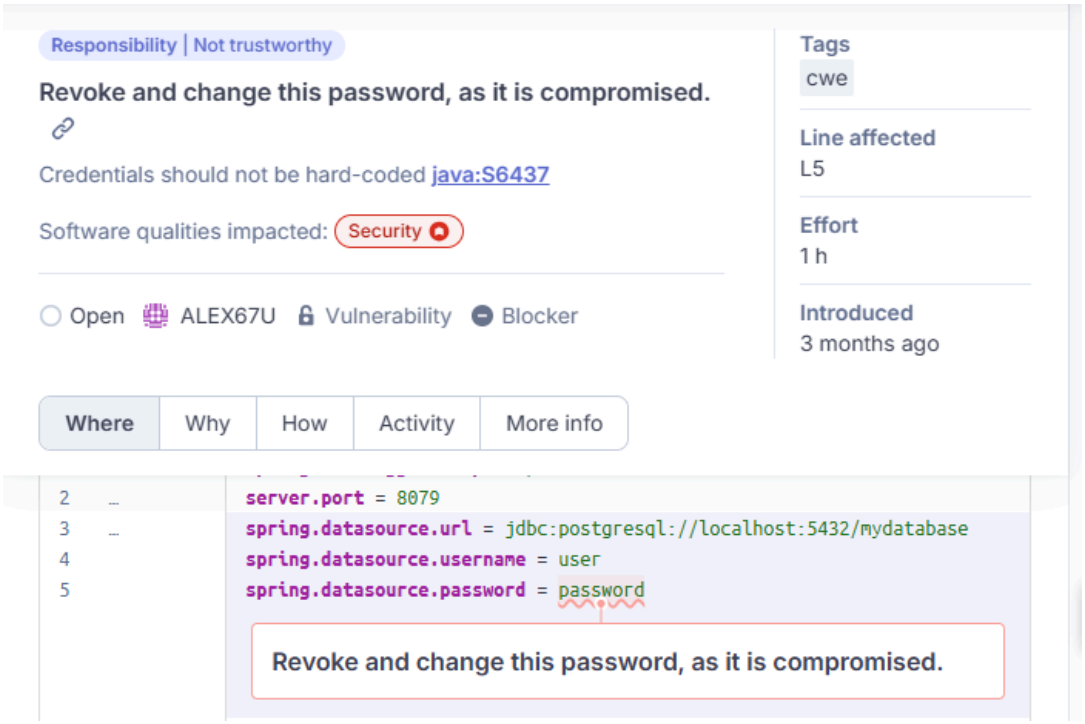
2. Issues Détectées

SonarQube a pu détecter quelques problèmes de maintenabilité et un problème de sécurité.

Problèmes de Maintenabilité :
Par exemple, la méthode constructeur vide suivante a été signalée par SonarQube :



Problème de Sécurité :
Un seul problème de sécurité a été relevé, concernant l'exposition de configurations sensibles :



3. Exécution des tests de sécurité (OWASP Dependency Check)

Pour compléter l'analyse de SonarQube, nous avons intégré un scan de sécurité **OWASP Dependency Check** afin de détecter les vulnérabilités présentes dans les dépendances du projet.

Intégration dans la pipeline CI/CD :

Dans le fichier **.github/workflows/ci-cd-pipeline.yml**, nous avons ajouté une étape pour exécuter OWASP Dependency Check.

Cette étape analyse les dépendances utilisées dans le projet et les compare aux bases de données des vulnérabilités connues (**NVD - National Vulnerability Database**).

Conclusion

L’intégration de SonarQube dans notre pipeline CI/CD nous permet de détecter rapidement des problèmes de qualité et de sécurité.

Les recommandations de SonarQube concernant la maintenabilité améliorent la lisibilité et facilitent la maintenance du code.

Ainsi, ces tests de vulnérabilité contribuent à assurer une qualité de code élevée et une sécurité renforcée tout au long du cycle de développement.