Documentation Sécurité

1. Utilisation de JWT (JSON Web Tokens)

L'application utilise un système de token JWT pour sécuriser l'accès à l'application et à la base de données (BDD). Les JWT sont des jetons cryptographiquement sécurisés qui permettent d'authentifier les utilisateurs de manière sécurisée. Chaque jeton contient des informations d'identification encodées qui sont vérifiées à chaque demande d'accès à l'application. Les JWT sont signés à l'aide d'une clé secrète, ce qui garantit leur intégrité et leur authentification.

2. Sécurisation des formulaires avec des expressions régulières (regex)

Tous les formulaires de l'application sont sécurisés à l'aide d'expressions régulières (regex) afin de prévenir les injections SQL et autres attaques potentielles. Les regex permettent de valider et de filtrer les entrées utilisateur, en s'assurant qu'elles correspondent à un format spécifique attendu. Cela réduit considérablement le risque d'injections de code malveillant via les formulaires de l'application.

3. Hashage des mots de passe

Les mots de passe des utilisateurs sont systématiquement hashés avant d'être stockés dans la base de données. Le hashage est un processus de transformation des données en une chaîne de caractères aléatoire et unique, rendant ainsi les mots de passe illisibles même en cas de compromission de la base de données. L'utilisation d'une fonction de hachage sécurisée garantit que les mots de passe ne peuvent pas être récupérés, même par les administrateurs système. Le password sera hashé en utilisant le système de hachage de symfony via le security.yaml ainsi que l'interface UserPasswordHasherInterface pour la vérification.

Bonnes Pratiques en Matière de Sécurité

En plus des mesures de sécurité mentionnées ci-dessus, l'application suit également les bonnes pratiques recommandées pour renforcer sa sécurité :

- ***Mises à jour régulières :*** *Les frameworks, bibliothèques et dépendances de l'application sont régulièrement mis à jour pour garantir qu'elle bénéficie des derniers correctifs de sécurité.*
- ***Principe du moindre privilège :*** *Les utilisateurs de l'application ne reçoivent que les autorisations nécessaires pour effectuer leurs tâches spécifiques, réduisant ainsi les risques liés à l'abus de privilèges.*