Rapport d’analyse de menaces
Threat Analyzer

Date : 18/01/2026 18:49

Résumé exécutif

Niveau global : Élevé
Score de risque : 70 / 100
Niveau de risque : Élevé

Menaces identifiées

Injection SQL (Gravité : Élevée)

L'application est vulnérable aux injections SQL, permettant à un attaquant d'exécuter des requêtes malveillantes sur la base de données et d'accéder à des données sensibles.

Recommandations :

- Utiliser des paramètres liés (prepared statements) pour toutes les requêtes SQL
- Valider et nettoyer toutes les entrées utilisateur avant utilisation
- Implémenter des mesures de sécurité supplémentaires comme la limitation des privilèges et le suivi des activités

Faille d'authentification (Gravité : Élevée)

Des failles dans le système d'authentification pourraient permettre à des utilisateurs non autorisés d'accéder à l'application et aux données sensibles.

Recommandations :

- Implémenter une authentification robuste avec des mécanismes tels que l'authentification à deux facteurs
- Mettre en place des politiques de mot de passe solides et forcer leur changement régulier
- Surveiller les tentatives de connexion et bloquer les comptes en cas d'activité suspecte

Fuite de données (Gravité : Critique)

L'application pourrait être vulnérable à des fuites de données sensibles (informations personnelles, données financières, etc.) en raison de problèmes de sécurité dans le traitement et le stockage des données.

Recommandations :

- Chiffrer les données sensibles, tant en transit qu'au repos
- Limiter l'accès aux données en fonction des rôles et des privilèges des utilisateurs
- Mettre en place des contrôles et des journaux d'audit pour détecter et investiguer les fuites de données

Déni de service (Gravité : Moyenne)

L'application pourrait être vulnérable à des attaques par déni de service, ce qui pourrait la rendre indisponible pour les utilisateurs légitimes.

Recommandations :

- Mettre en place des mécanismes de protection contre les attaques par déni de service (limitation de connexions, quotas, etc.)
- Surveiller et analyser les journaux d'événements pour détecter les activités suspectes
- Dimensionner l'infrastructure de manière adéquate pour faire face à des charges de trafic élevées

Vulnérabilités dans les bibliothèques tierces (Gravité : Moyenne)

L'application utilise des bibliothèques tierces qui peuvent contenir des vulnérabilités connues, exposant l'application à des risques de sécurité.

Recommandations :

- Maintenir à jour toutes les bibliothèques tierces utilisées dans l'application
- Surveiller les annonces de sécurité et appliquer rapidement les correctifs nécessaires
- Envisager l'utilisation d'outils d'analyse des dépendances pour détecter les vulnérabilités