MAISON EN PLACE

PLAN DE SÉCURITÉ

1 - Risques et solutions identifiés

Risque	Contexte	Gravité (de 1 à 5)	Solutions / outils potentiels
Faible sécurité des mots de passe (MD5)	Les mots de passe sont actuellement stockés avec l'algorithme MD5, qui est vulnérable aux attaques par force brute ou par dictionnaire.	5	• Remplacer MD5 par **bcrypt** • Imposer des règles de complexité
Communication non sécurisée via HTTP	Certaines API utilisent le protocole HTTP, ce qui expose les données sensibles à des attaques de type "Man-in-the-Middle".	5	• Forcer l'utilisation du **HTTPS** • Implémenter des certificats SSL
Gestion de sessions non sécurisée	Absence de mécanisme de déconnexion automatique après une période d'inactivité, augmentant les risques d'usurpation de session (session hijacking).	4	• Déconnexion automatique • Utiliser **JWT** avec expiration
Attaque par déni de service (DDoS)	Une attaque DDoS pourrait saturer les serveurs de l'application, rendant le service indisponible pour les utilisateurs légitimes.	4	• Mettre en place un **WAF** (Web Application Firewall) • Utiliser un système de détection de trafic anormal
Vol de données via des injections SQL	Une mauvaise gestion des requêtes SQL pourrait permettre des injections SQL, compromettant ainsi les bases de données utilisateurs et produits.	4	• Utiliser des **requêtes préparées** et valider les entrées utilisateur
Mises à jour non sécurisées des dépendances	Utilisation de bibliothèques ou de frameworks non à jour contenant des vulnérabilités exploitées par des attaquants.	3	• Mettre en place un processus de **mise à jour régulière des dépendances**