Audit de Sécurité – WorkNest

Stack technique auditée

Frontend : React + Tailwind CSS
Backend : Node.js + Express
Base de données : PostgreSQL
ORM : Prisma / Sequelize
Authentification : JWT + bcrypt
Validation : express-validator
Documentation : Swagger
Infrastructure : Docker

Vulnérabilités identifiées

- Rate limiting global perfectible pour les routes sensibles (authentification)
- Absence de révocation des tokens JWT
- Logs applicatifs pouvant contenir des données sensibles
- Politique RGPD partiellement implémentée

Mesures de sécurité en place

- Hashage des mots de passe avec bcrypt (12 rounds)
- JWT avec expiration
- Validation et sanitation des entrées utilisateur
- Protection HTTP via Helmet, CORS et rate limiting
- Requêtes SQL sécurisées via ORM

Recommandations

- Rate limiting spécifique sur /auth/login
- Refresh tokens + blacklist
- Logs d’audit
- Chiffrement des données sensibles
- 2FA pour les comptes administrateurs

Conclusion

La plateforme respecte les standards de sécurité d’une application SaaS moderne. Des améliorations sont recommandées avant une mise en production à grande échelle.

Tests & Recettage – WorkNest

Objectif

Valider la fiabilité, la sécurité et la conformité fonctionnelle de la plateforme WorkNest.

Tests de sécurité réalisés

- Refus d’accès aux routes protégées sans JWT
- Validation des données côté backend
- Gestion des erreurs sans fuite d’informations
- Protection contre injections SQL

Tests fonctionnels critiques

- Inscription et authentification
- Réservation et paiement
- Gestion des espaces (admin)
- Accès tableau de bord utilisateur

Anomalies et améliorations

- Messages d’erreur perfectibles
- Validation client à renforcer
- Logs d’audit à implémenter

Conclusion

Les tests confirment la stabilité et la sécurité globale du système. La plateforme est conforme aux exigences du projet Bloc 4.