

Sécurité (résumé bac+2)

Authentification

- Mot de passe hashé avec **bcrypt**
- Authentification par **JWT**
- Rôles : USER / EMPLOYE / ADMIN

Bonnes pratiques

- Vérification des champs côté serveur
- Tokens expirables (reset mot de passe)
- Réponses génériques pour l'oubli de mot de passe
- Accès protégé par middleware (`requireAuth` , `requireRole`)

Emails (dev)

En environnement de développement, l'envoi d'email est simulé :

- journalisé en base (`email_log`)
- affiché en console