1. **Gestion des secrets** : ADMIN_TOKEN en clair dans le code
   solution : passer par un .env
2. **Manipulation de la base de données** via le body.id dans api/delete-user
3. **Contrôle d'accès** si ADMIN_TOKEN en clair, header facile a trouver
4. **Affichage dynamique** : http://localhost:3000/api/welcome?name=<input>, injection de code via url
   solution : ajouter un regex `if (!/^[a-zA-Z0-9_-]{3,20}$/.test(req.query.name)) {`

5. **Fuite d'informations** : injection dans la requete SQL /api/user

http://localhost:3000/api/user?username=user1' UNION SELECT id, username, password FROM users WHERE username='admin