EC04 – API sécurisée et documentée

Contexte général

Dans le cadre du projet **FoodSafe**, cette épreuve consiste à développer une **API publique** permettant aux utilisateurs d'interroger les fonctionnalités principales de l'application : recherche de produits, gestion du profil alimentaire et ajout aux favoris.

Cette API doit répondre aux standards actuels en matière de conception, de sécurité et de documentation. L'objectif est de proposer une API robuste, bien testée et facile à maintenir, tout en garantissant la protection des données sensibles (profils de santé, intolérances).

Les apprenants sont libres de choisir une architecture **REST** ou **GraphQL**, selon les besoins exprimés.

Livrables attendus

Livrable	Détail
Code source	Endpoints sécurisés, architecture claire
Documentation API	Fichier Swagger/OpenAPI ou équivalent
Tests unitaires	Couverture des endpoints critiques, rapports générés
README	Instructions de test, exemples de requêtes, gestion des tokens

Modalités d'évaluation

- **Type d'épreuve** : Mise en situation reconstituée sur ordinateur
- **Durée** : 4h
- **Nature** : Épreuve individuelle, sans oral
- **Critères évalués** :
  - C8.3 : Conception d'une API REST sécurisée (auth, JWT, middleware)
  - C8.4 : Documentation complète de l'API

- C8.5 : Tests unitaires sur les endpoints critiques

Recommandations

- Implémenter un **système d'authentification sécurisé** (JWT, tokens avec expiration)
- Organiser l'API autour de **ressources cohérentes** (ex : `/users`, `/products`, `/favorites`)
- Séparer clairement les responsabilités : contrôleurs, services, middlewares
- Fournir une **documentation Swagger/OpenAPI** claire et testable sans accompagnement
- Prévoir une **gestion des erreurs** standardisée (codes HTTP, messages explicites)
- Écrire des **tests unitaires automatisés** couvrant les cas critiques (auth, recherche produit, compatibilité)

Exemples d'éléments attendus

- Un endpoint `GET /products/compatible` qui retourne la liste des produits compatibles avec le profil utilisateur
- Un endpoint `POST /favorites` permettant d'ajouter un produit aux favoris, protégé par JWT
- Un endpoint `DELETE /favorites/:id` pour retirer un produit des favoris
- Des statuts HTTP clairs (`200`, `401`, `403`, `422`)
- Un fichier `openapi.yaml` ou équivalent documentant toutes les routes
- Des tests affichant un taux de couverture élevé sur les endpoints critiques

Nom de dossier attendu

- une archive ZIP nommée `EC04_NomPrenom.zip` contenant :
  - Le dossier `src` du projet (API)
  - Le fichier `README.md` avec exemples de requêtes et scripts de lancement
  - La documentation Swagger/OpenAPI
  - Les rapports de tests automatisés

Rappel pédagogique

Cette épreuve vise à valider la **capacité à exposer une API professionnelle** :

- Sécurisation des accès (authentification, autorisation)
- Structuration claire et maintenable du code
- Rédaction d'une **documentation technique complète et exploitable**
- Mise en œuvre de **tests automatisés** garantissant la fiabilité des endpoints

Elle prépare les apprenants à l'intégration d'une API dans une application front ou mobile, dans un contexte réaliste d'équipe, tout en respectant les contraintes liées aux données sensibles en santé.