Groupe 4 - Clément Miesse, Ambroise Mostin et Cyril Wastchenko
→ Lead Clément

Semaine 10 : 4 - 8 Mai

Sécurité

Quels sont les biens à protéger?

- Le serveur
- La base de données
- Le code

Quelles sont les vulnérabilités et les menaces de ces biens?

Serveur → Accès non autorisé, données vulnérables
Base de données → Injection SQL, copie non autorisée de données sensibles, abus/élévation de privilège
Code → Cross-Site Scripting (XSS), Buffer Overflow et Broken Authentication

Pour chaque menace, quels sont les risques associés?

Risques :

1. Accès non autorisé au serveur / accès aux données sur le serveur
2. Copie de données de la base de données
3. Accès aux données de la BDD suite à un abus/une élévation de privilèges
4. Injection SQL dans la BDD
5. Cross-Site Scripting
6. Buffer Overflow
7. Broken Authentication

Contre-mesures (cfr ci-dessous) :

1. Authentification par clés RSA, désactivation de la connexion via ROOT
2. Connexion à la DB via un seul utilisateur, par mot de passe
3. /
4. /
5. /
6. Testing → détection d'anomalies dans le code
7. Mots de passe Hashés

Documenter les risques résiduels

- Accès à la base de données via Root par mot de passe - **à améliorer**
- Abus / élévation de droits dans la BDD → **Non géré**
- Injection SQL → **Non géré**
- Cross-site scripting → **Non géré**

Assurer la maintenance (plan de suivi, monitoring, stratégies de réaction/mitigation

Utilisation de PM2 → **TODO**

Contres-mesures

Authentification par clés RSA

- Désactivation de la connexion sur l'utilisateur root
- Création et utilisation de clés RSA pour se connecter
- Désactivation de la connexion par mot de passe pour tous les utilisateurs

Mots de passe (hash)

- Hash des mots de passe de la table users (connexion à la partie Admin du projet)

HTTPS

- Création d'une certification HTTPS (SSL grâce à Lets Encrypt) pour le nom de domaine probio.host

Reverse proxy (Nginx)

- Nginx renvoie toute requête HTTP et HTTPS sur le port 443
- Les requêtes à l'API sont redirigées vers '/api'
- Les requêtes vers le front-end sont redirigées vers '/'

Firewall

- Utilisation du firewall UFW limitant les ports ouverts sur le serveur
- Ports autorisés : 22, 80, 443, 8080, 5000, ...

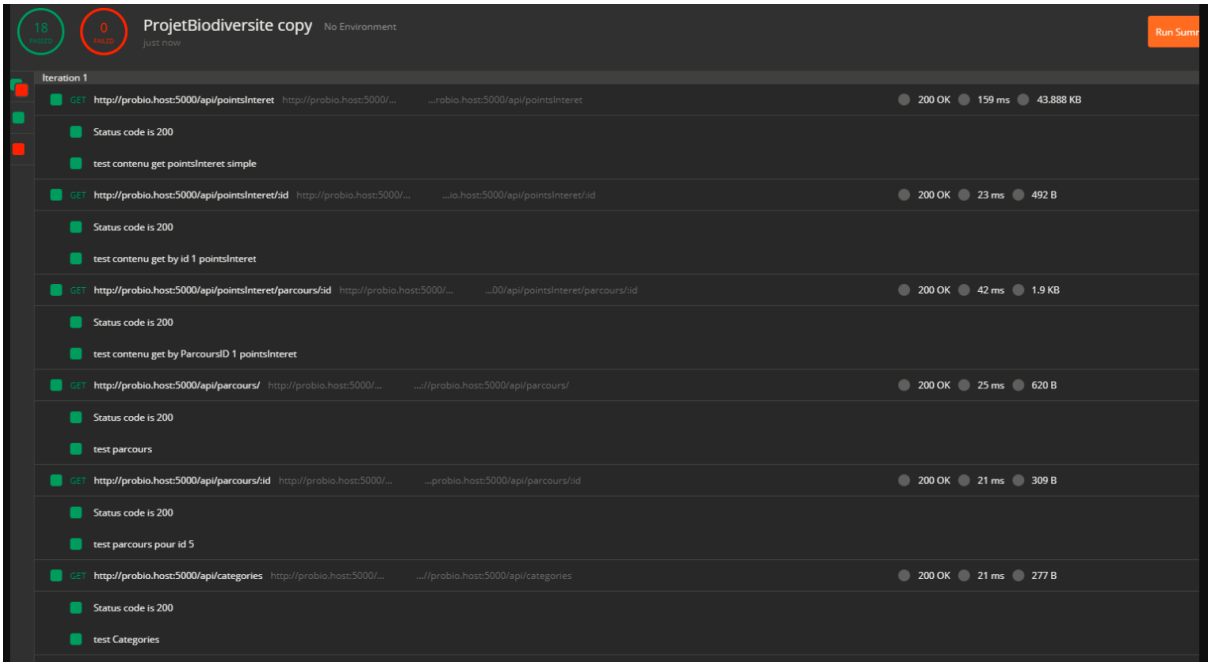
Testing

Tests unitaires

- Fichier Common.test.js (fichier de tests unitaires utilisant Jest pour tester Common.js)
- Les méthodes getUser(), getToken(), removeUserSession(), setUserSession(token, user) sont testées
- Les autres méthodes de l'api sont de simple appels à l'API et enregistre les données dans des State ou sont intestables même en hardcodant
- Suite à cela, le code coverage est très faible, 5.85% des statements, 3.51% des branches, 3.64% des fonctions et 5.39% des lignes sont testées. Seuls les méthodes de Utils/Common.js sont correctement testées

Tests d'API

Vérification sur le statut → Retour 200
Vérification sur les données → Données ponctuelles pour chaque fonction



Code coverage