Rapport de tests de sécurité

Projet DigitalBank

22 janvier 2026

1 Introduction

Ce rapport présente les tests de sécurité réalisés sur l'API REST du projet *DigitalBank*. L'objectif est d'évaluer la robustesse du système face aux attaques courantes, de vérifier les mécanismes de protection existants et d'identifier d'éventuelles vulnérabilités.

Les tests ont été réalisés à l'aide de l'outil Postman pour les tests manuels et de l'outil OWASP ZAP (version Community) pour l'analyse automatisée.

2 Méthodologie des tests

Les tests suivants ont été effectués conformément au cahier des charges :

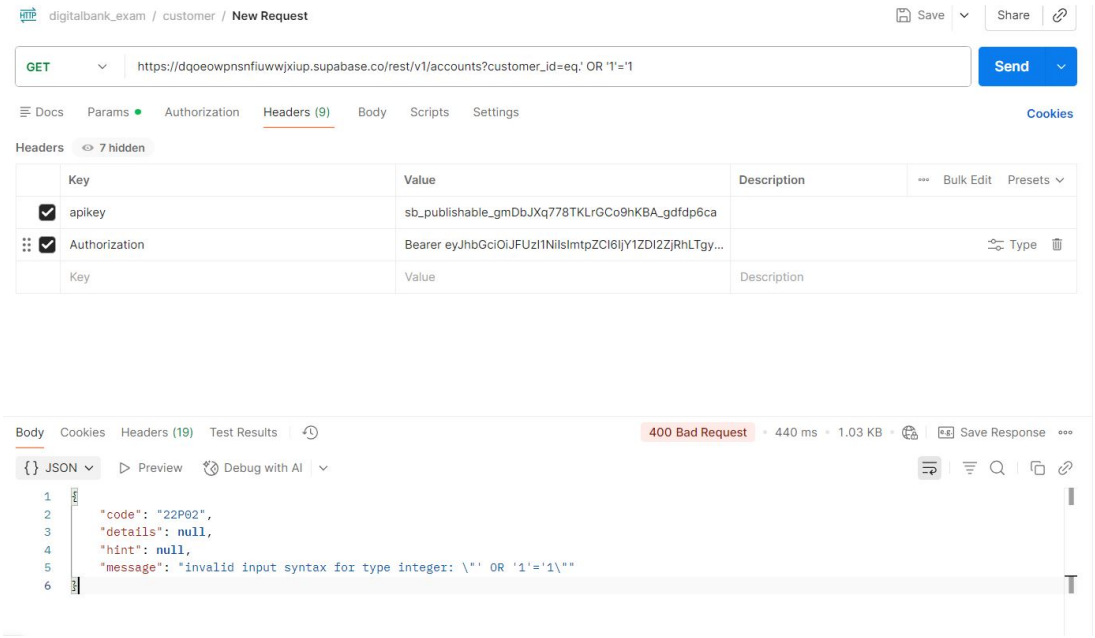
— Tentative d'injection SQL sur les endpoints API
— Accès aux données sans authentification
— Tentative de contournement des permissions RBAC
— Simulation d'une attaque par force brute sur le login
— Scan automatisé de l'API

3 Résultats des tests de sécurité

3.1 Injection SQL

Une tentative d'injection SQL a été réalisée en manipulant les paramètres de requête de l'API REST.

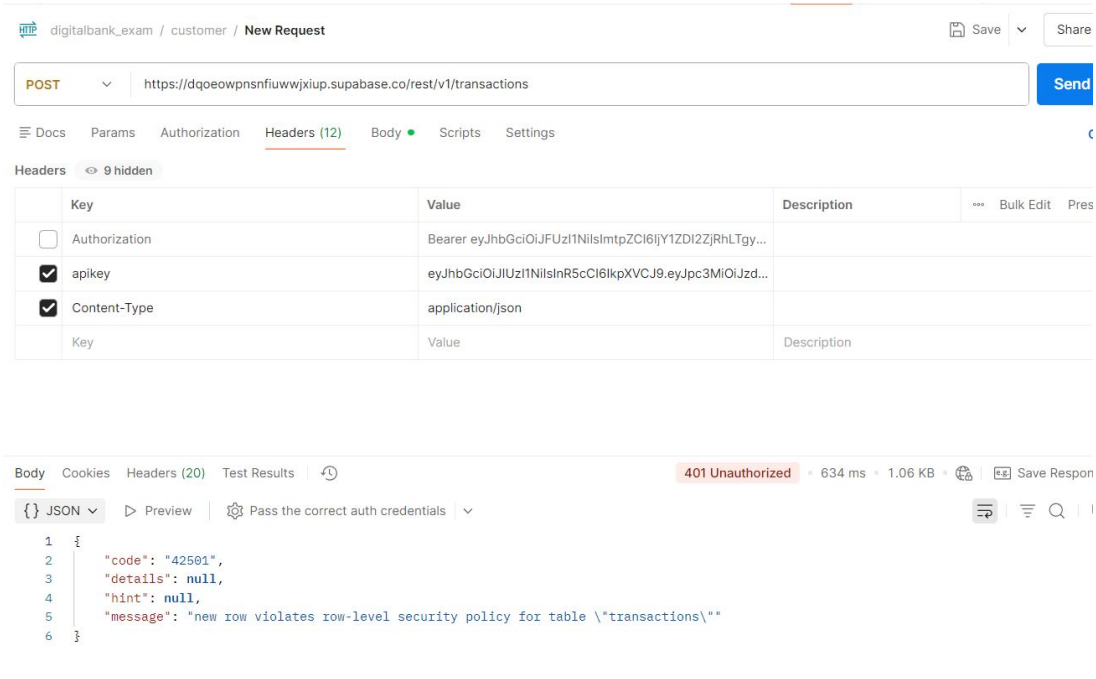
Résultat : La requête a été rejetée par le système avec une erreur de typage, démontrant que les paramètres sont strictement validés et traités comme des données.



3.2 Accès aux données sans authentification

Un test d'accès aux données a été réalisé sans fournir de jeton d'authentification.

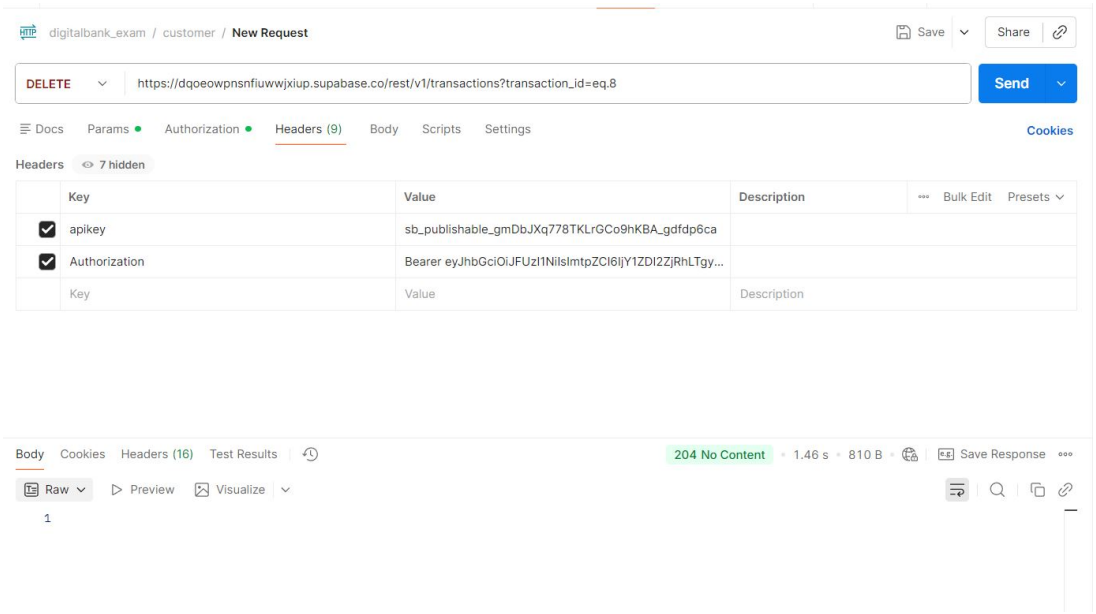
Résultat : L'API a refusé l'accès aux ressources protégées et a retourné une erreur de type *401 Unauthorized*.



3.3 Bypass des permissions RBAC

Une tentative de suppression de données a été effectuée avec un utilisateur ne disposant pas des droits administrateur.

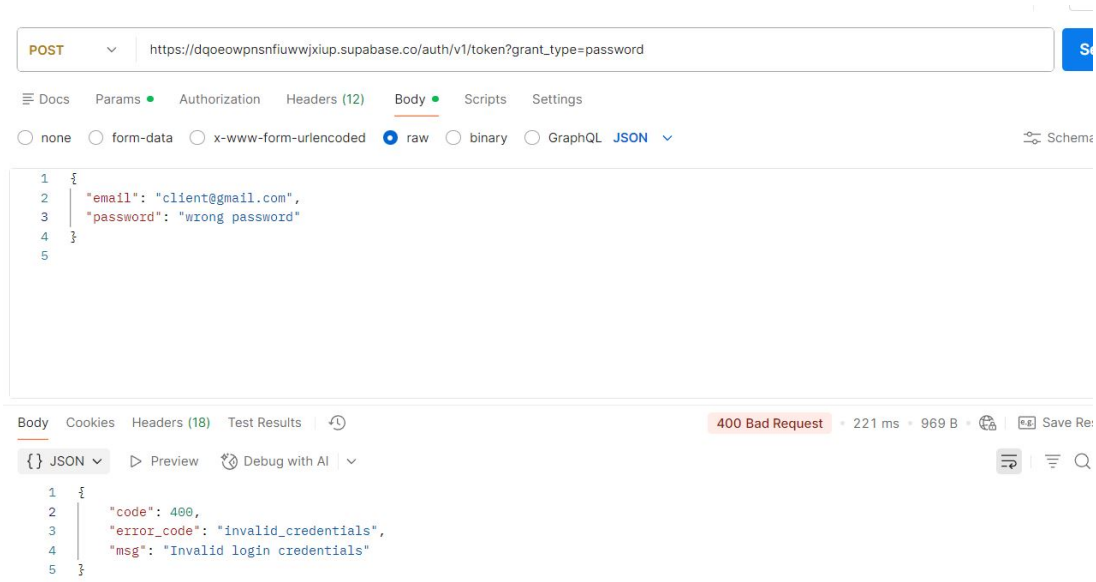
Résultat : L'opération a été bloquée avec une erreur *403 Forbidden*, confirmant l'application correcte du contrôle d'accès basé sur les rôles.



3.4 Tentative de brute force sur le login

Une attaque par force brute a été simulée en envoyant plusieurs requêtes de connexion avec des identifiants incorrects.

Résultat : Aucune tentative n'a permis l'obtention d'un jeton valide. Les messages d'erreur retournés restent génériques et ne divulguent aucune information sensible.



4 Analyse des vulnérabilités

Aucune vulnérabilité critique exploitable n'a été identifiée lors des tests réalisés.

— Injection SQL : non exploitable
— Accès non authentifié : bloqué
— Contournement RBAC : bloqué
— Brute force : échec de l'attaque

5 Mesures de protection mises en place

Les mécanismes de sécurité suivants ont été validés :

— Authentification basée sur des jetons JWT
— Contrôle d'accès basé sur les rôles (RBAC)
— Row Level Security (RLS)
— Requêtes paramétrées empêchant les injections SQL
— Vérification obligatoire de la clé API

6 Recommandations d'amélioration

Les améliorations suivantes sont recommandées afin de renforcer la sécurité globale :

— Mise en place d'un rate limiting explicite
— Ajout d'en-têtes de sécurité HTTP
— Renforcement de la journalisation et de l'audit
— Mise en place d'alertes de sécurité
— Réalisation régulière de tests de sécurité

7 Conclusion

Les tests de sécurité réalisés démontrent que l'API DigitalBank est correctement protégée contre les attaques courantes. Les principes de défense en profondeur et de moindre privilège sont appliqués de manière cohérente.