

Sécurité Applicative Mobile et Tests - Projet KeepNote

Introduction

Ce module complémentaire au projet KeepNote se concentre sur les aspects de sécurité et de tests de l'application mobile. Vous devrez mettre en œuvre des pratiques de sécurité modernes dans votre application React Native/Expo et développer une suite de tests pour valider son bon fonctionnement.

Date de rendu : 29 avril 2025

Objectifs pédagogiques

- Comprendre et appliquer les principes fondamentaux de la sécurité mobile
- Maîtriser les outils de sécurité spécifiques à l'écosystème React Native et Expo
- Identifier et corriger les vulnérabilités courantes dans les applications mobiles
- Mettre en place une stratégie de test efficace pour valider les fonctionnalités et la sécurité
- Appliquer les recommandations de l'OWASP Mobile Top 10

Exigences de sécurité

Stockage sécurisé des données sensibles

- Utilisation obligatoire d'Expo SecureStore pour stocker toutes les informations sensibles (jetons d'authentification, etc.)
- Aucune donnée sensible ne doit être stockée dans AsyncStorage non chiffré
- Mise en œuvre d'une stratégie de chiffrement pour les données locales avec expo-crypto

Communications sécurisées

- Utilisation correcte des appels API fournis
- Validation appropriée des réponses
- Gestion structurée des erreurs sans exposition d'informations sensibles

Protection contre les attaques courantes

- Validation de toutes les entrées utilisateur pour prévenir les injections
- Protection contre les attaques XSS
- Implémentation de mécanismes de défense contre les attaques CSRF (le cas échéant)
- Vérification de l'absence de données sensibles dans les logs et les variables d'environnement

Authentification sécurisée

- Stockage sécurisé des jetons d'authentification (via SecureStore)
- Gestion appropriée des sessions et de leur expiration
- Mécanisme de déconnexion complet (suppression des jetons stockés)
- Protection contre les tentatives de connexion multiples

Exigences de test

Tests unitaires avec Jest

- Implémentation d'au moins 3 tests unitaires avec Jest couvrant :
 1. Un test pour le système d'authentification
 2. Un test pour les fonctionnalités de gestion des notes ou des tâches
 3. Un test pour les mécanismes de sécurité (SecureStore, validation des entrées, etc.)

Chaque test devra inclure des commentaires clairs expliquant son objectif. Tous les tests doivent obligatoirement être réalisés avec Jest.

Audit de sécurité

Pendant l'évaluation, nous examinerons les aspects suivants de votre application :

1. Identification des mécanismes de protection des données sensibles
2. Vérification de l'absence de vulnérabilités évidentes
3. Évaluation des mesures de sécurité implémentées

Ressources recommandées

- Documentation officielle d'Expo SecureStore
- Documentation expo-crypto
- OWASP Mobile Security Testing Guide
- Guide de sécurité React Native
- Documentation Jest pour React Native

Barème d'évaluation (20 points)

Sécurité (14 points)

Stockage sécurisé (5 points)

- Utilisation correcte d'Expo SecureStore (2 points)
- Absence de données sensibles dans le stockage non sécurisé (1,5 points)
- Implémentation de chiffrement avec expo-crypto (1,5 points)

Communications sécurisées (3 points)

- Utilisation correcte des appels API (1 point)
- Gestion appropriée des réponses API (1 point)
- Gestion correcte des erreurs (1 point)

Protection contre les attaques (3 points)

- Validation des entrées utilisateur (1 point)
- Protection XSS (1 point)
- Absence de fuite d'informations sensibles (1 point)

Authentification sécurisée (3 points)

- Stockage sécurisé des jetons (1 point)
- Gestion des sessions (1 point)
- Mécanisme de déconnexion complet (1 point)

Tests (6 points)

- Implémentation des 3 tests unitaires requis (4,5 points - 1,5 point par test)
- Commentaires explicatifs dans le code des tests (1,5 points)

Remise du projet

Votre projet devra inclure :

- Un répertoire `__tests__` contenant vos 3 tests Jest
- Le code source intégrant toutes les mesures de sécurité requises

Bonne chance pour ce projet de sécurité et de tests applicatifs !