Rapport d'analyse statique - [app-debug.apk]

A) Informations générales

- **Date d'analyse :** 27/02/2026
- **Analyste :** Belrhazi Ahmed
- **APK analysé :** app-debug.apk
- **Provenance :** test
- **Outils utilisés :** jadx-gui-1.5.5-with-jre-win , dex-tools-v2.4 , jd-gui-windows-1.6.6

B) Résumé exécutif

L'analyse statique de l'application de test app-debug.apk a révélé **2 vulnérabilités de configuration** majeures situées dans le Manifeste.
Le code source a également été audité à la recherche de secrets (tokens, http), mais les résultats se sont révélés être des faux positifs provenant des bibliothèques standards Android.

Le niveau de risque global est évalué comme **Moyen/Élevé** (principalement dû au mode débogage actif).

Actions prioritaires recommandées :

1. Désactiver le mode débogage (debuggable="false") pour la version de production.
2. Désactiver la sauvegarde automatique des données (allowBackup="false").

C) Constats détaillés

Constat #1 : Application Débogable (Critique)

- **Sévérité :** Élevée
- **Description :** L'application est configurée pour autoriser le débogage. Cela permet à n'importe qui ayant un accès physique au téléphone de se connecter à l'application via ADB/JDB, de voir les variables en mémoire et d'injecter du code.
- **Localisation :** `AndroidManifest.xml`, ligne 20 : `android:debuggable="true"`
- **Remédiation :** Passer cet attribut à `false`. Généralement, cela est géré automatiquement par Gradle (`buildTypes { release { ... } }`), mais il faut s'assurer de ne pas publier l'APK "debug".
- **Remédiation recommandée :** Ne jamais stocker de secrets dans le code. Utiliser des variables d'environnement au moment de la compilation ou un système de gestion de clés sécurisé (Android Keystore).

Constat #2 : Sauvegarde ADB autorisée

- **Sévérité : Moyenne**
- **Description :** L'attribut allowBackup est activé. Cela signifie que les données privées de l'application (bases de données, préférences) peuvent être extraites via la commande adb backup si le téléphone est déverrouillé.
- **Localisation** : AndroidManifest.xml, ligne 21 : android:allowBackup="true"
- **Remédiation :** Définir explicitement android:allowBackup="false" si la sauvegarde cloud n'est pas nécessaire, ou chiffrer les données sensibles.
- **Remédiation recommandée :** Forcer l'utilisation de HTTPS partout.

D) Annexes

Composants Exportés

- **Activity :** `com.example.formulaire.MainActivity` est exportée (`android:exported="true"`). C'est normal pour l'écran de lancement (Launcher), mais c'est un point d'entrée public.

Permissions

- L'application ne demande pas de permissions système sensibles standards (comme INTERNET ou CAMERA) dans les captures visibles, à part une permission de signature interne pour le `DYNAMIC_RECEIVER`.