

S4- Sécurité IT et Confiance Numérique

**TP : Pentesting d’AndroGoat (Application Android Vulnérable)**

**Objectif** :

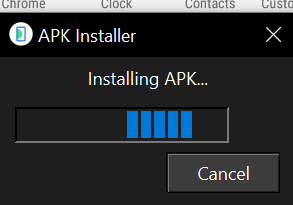
Identifier et exploiter des vulnérabilités dans AndroGoat en utilisant des outils courants de pentesting mobile.

**Prérequis :**

* Un appareil Android (émulateur ou physique, rooté/débuggable de préférence).
* ADB (Android Debug Bridge).
* Un décompilateur (Jadx-GUI recommandé).
* Un proxy d'interception (Burp Suite Community).
* Application cible : Choisir une application vulnérable (AndroGoat).

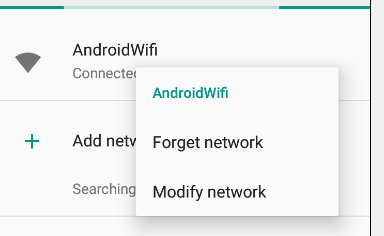
1. **Configuration du Lab** 
   * Étapes :
     + Téléchargez AndroGoat depuis GitHub.

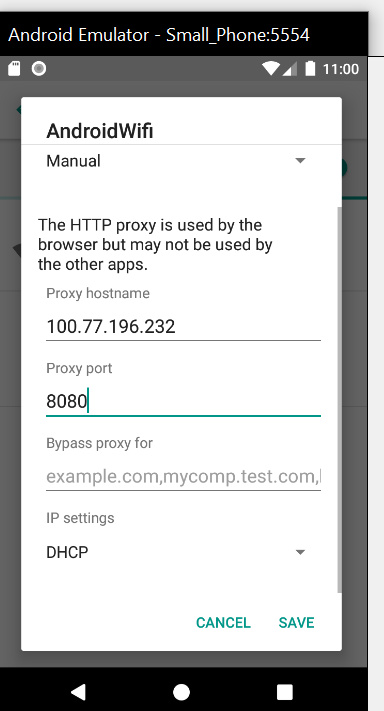
o Installez l’APK sur un émulateur (Android Studio).



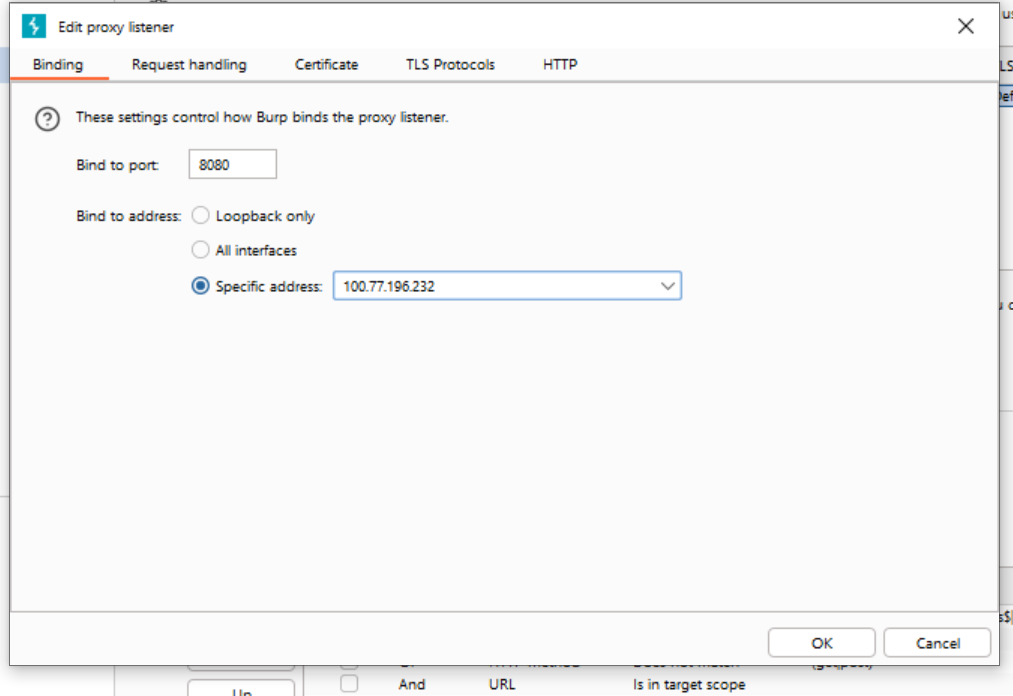
* + - Configurez ADB (Android Debug Bridge) pour interagir avec l’appareil :
      * adb devices # Vérifier la connexion
      * adb install AndroGoat.apk

1. **Interception du Trafic Réseau** 
   * Configuration d'un Proxy



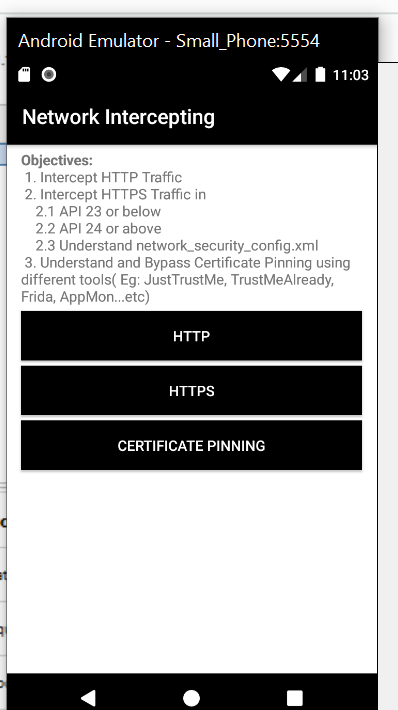


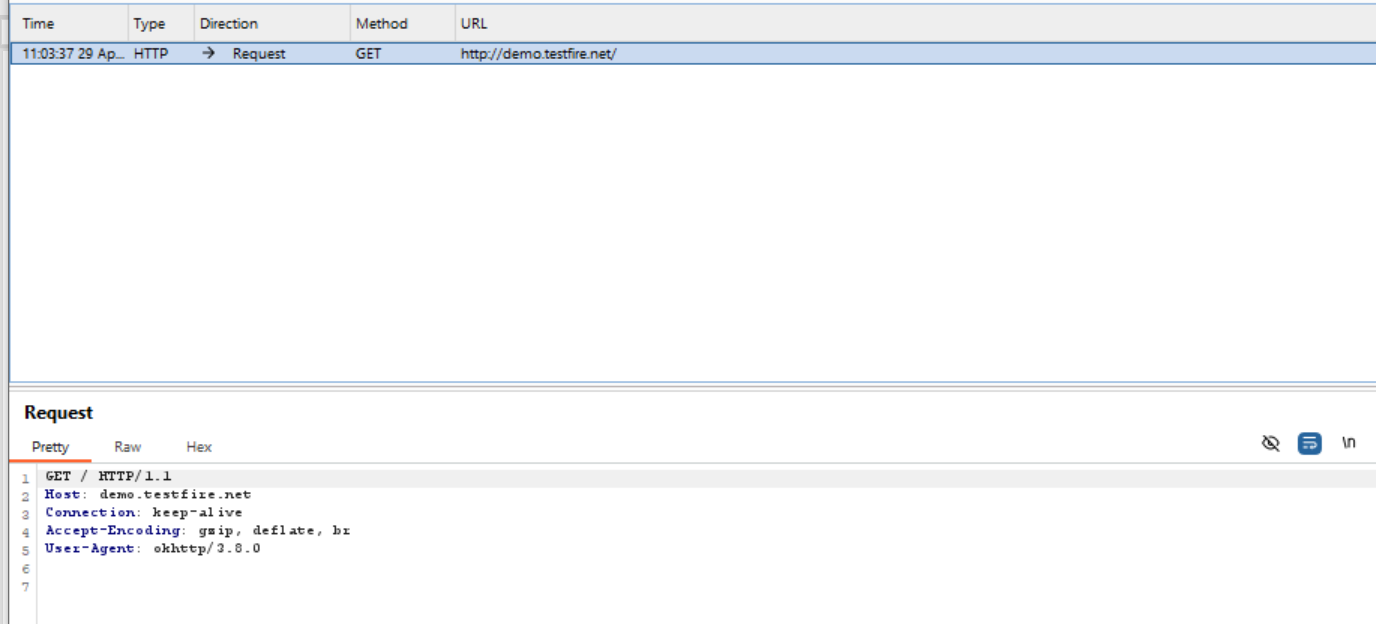
* + - Définir l'adresse IP de votre machine comme proxy (ex: 192.168.18.231:8080).



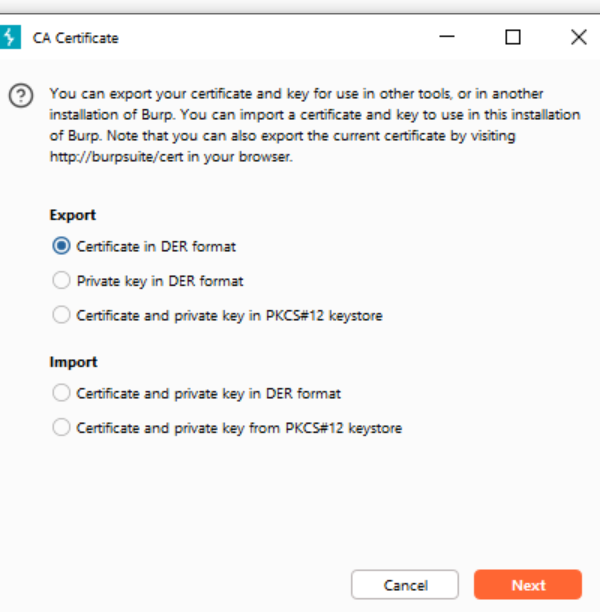
o Dans Burp Suite, configurez un **Proxy Listener** correspondant.

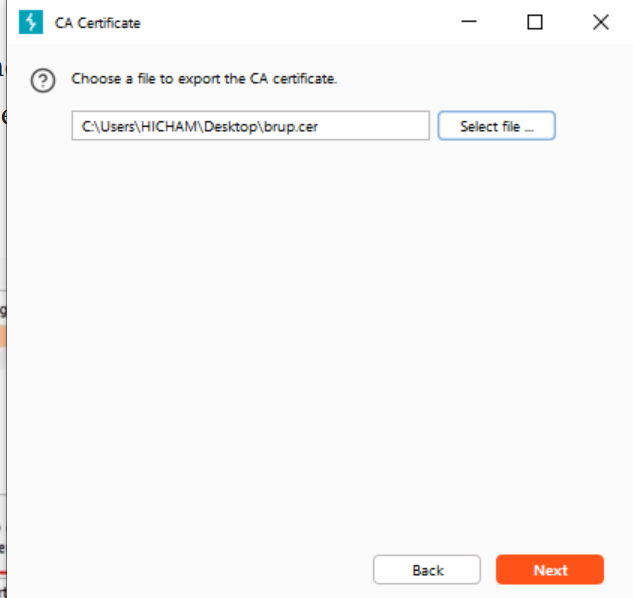
* + - * Ouvrez AndroGoat et cliquez sur "HTTP" : le trafic sera intercepté dans Burp Suite.

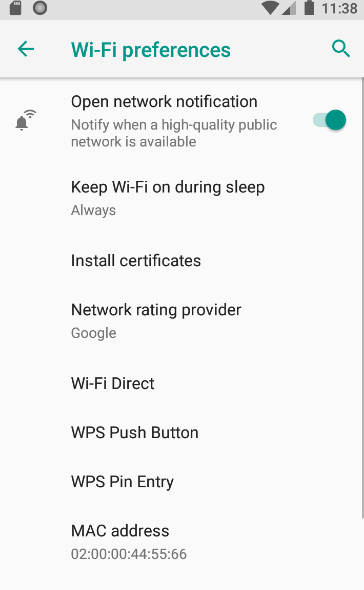




* + - Pour HTTPS, exportez le certificat Burp (format .cer) et installez-le sur le mobile
      * Accédez aux paramètres Wi-Fi > Certificats > Installez le fichier.
      * Interceptez du trafic HTTPS.

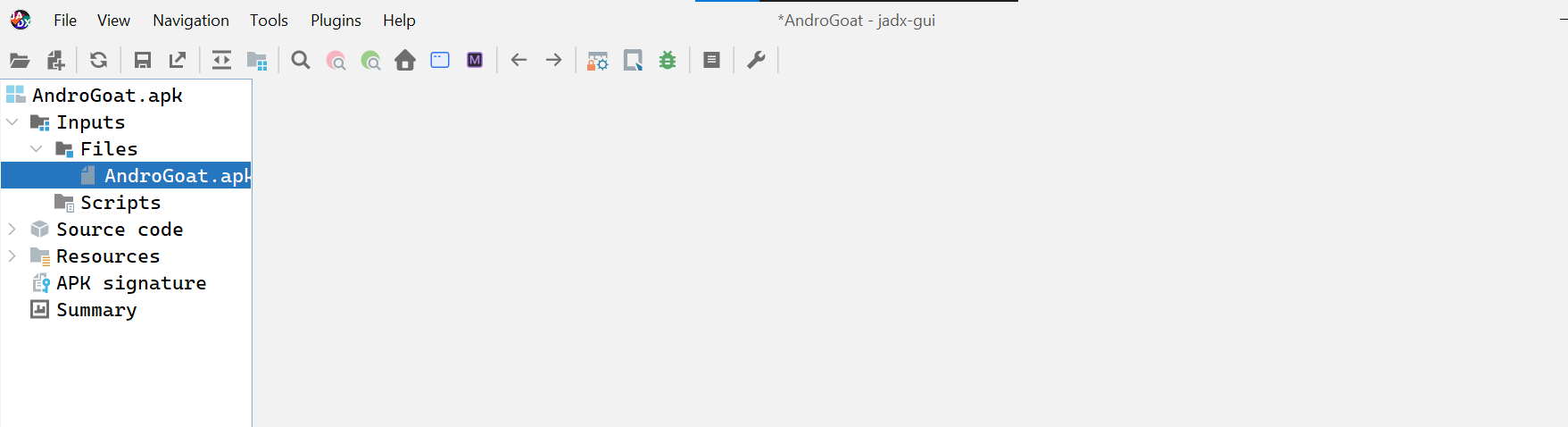




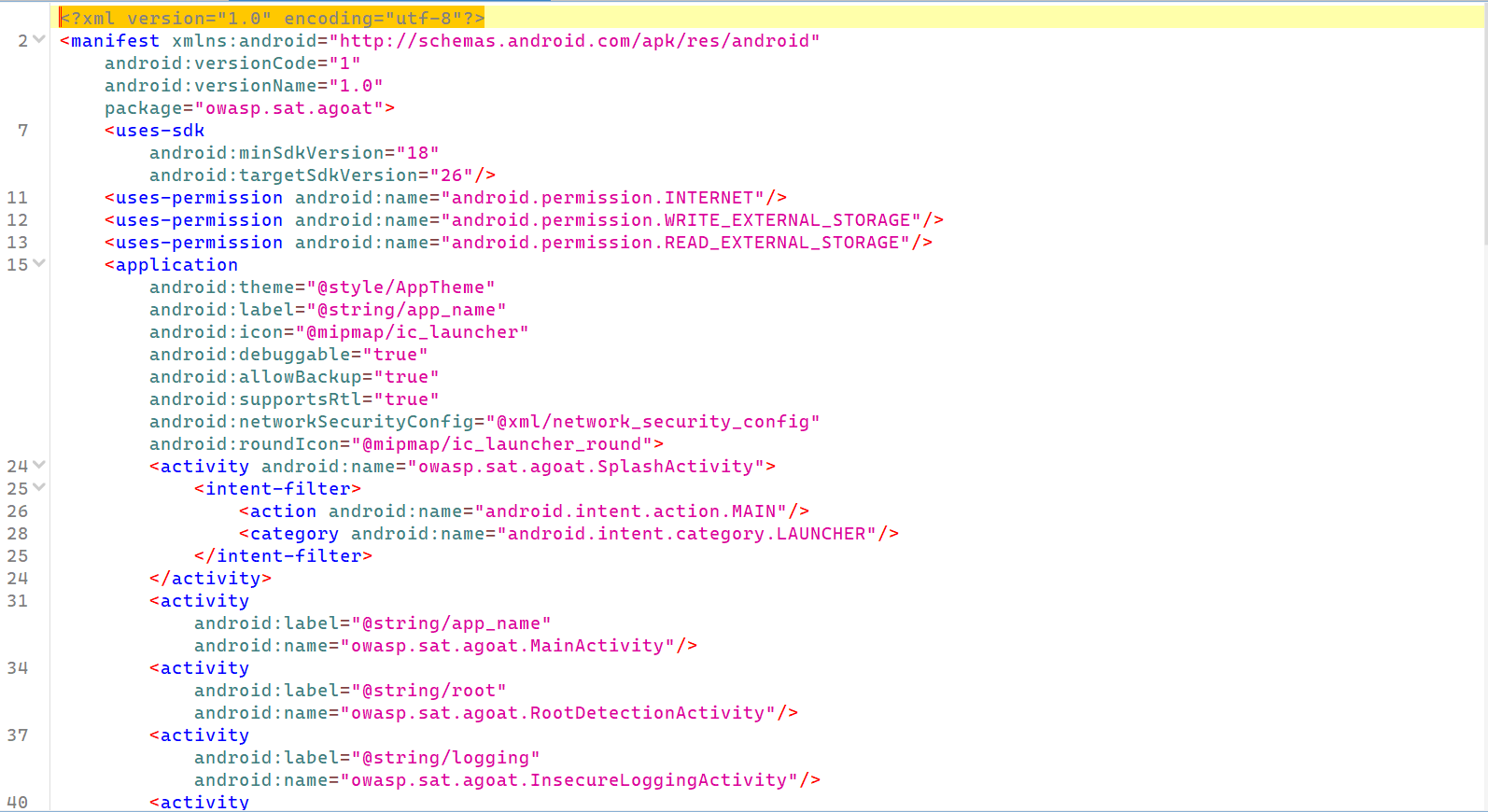




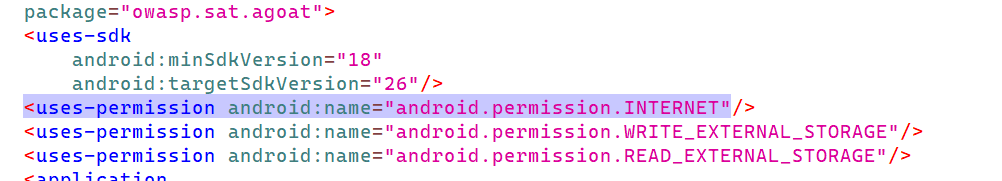
1. **Analyse Statique** 
   * Objectif : Comprendre la structure de l'application et identifier des points d'intérêt sans l'exécuter.
   * Outil : JADX-GUI.  Comment faire :
     + Ouvrez l'APK d'AndroGoat avec JADX-GUI.



* + - Examinez le fichier AndroidManifest.xml pour comprendre les permissions demandées, les activités exportées, les services, les broadcast receivers et les content providers. Portez une attention particulière aux intent-filters pour les deeplinks.



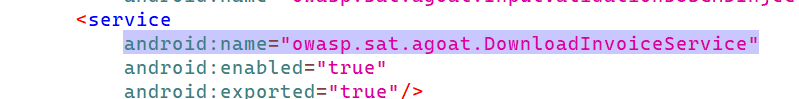
**comprendre les permissions demandées**



**INTERNET**

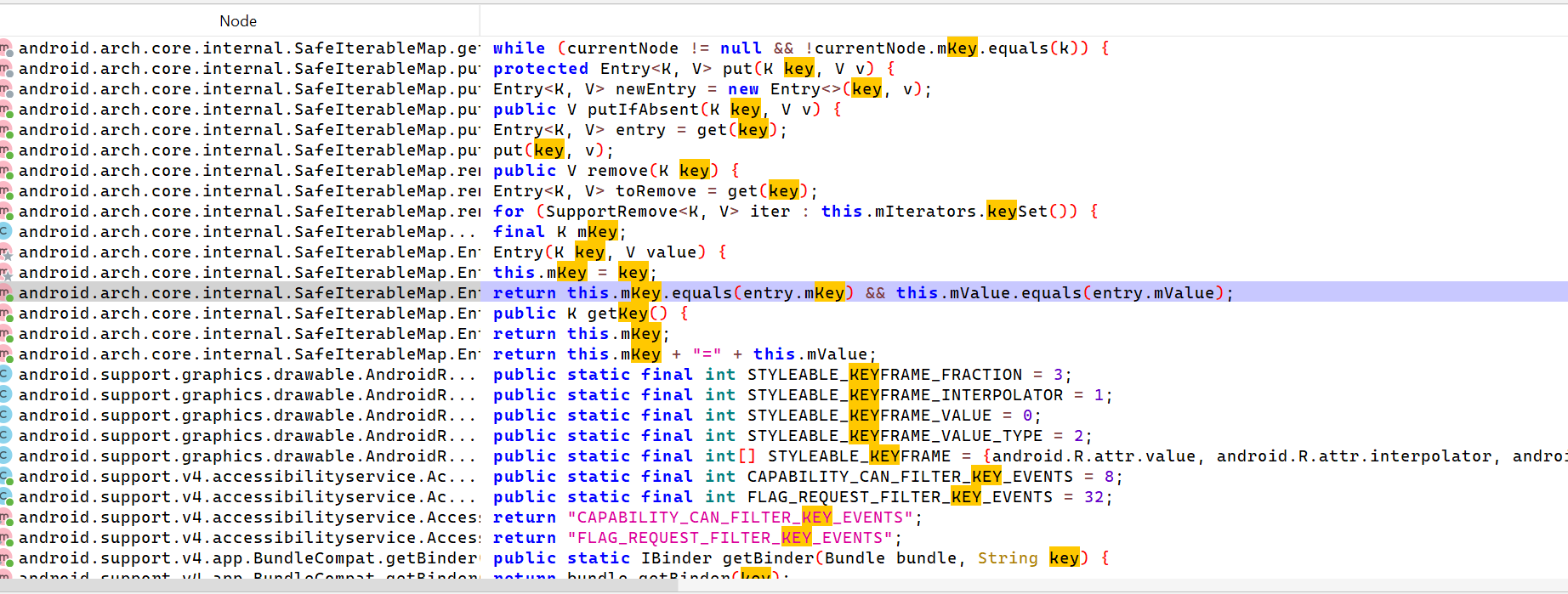
**WRITE/READ\_EXTERNAL\_STORAGE**

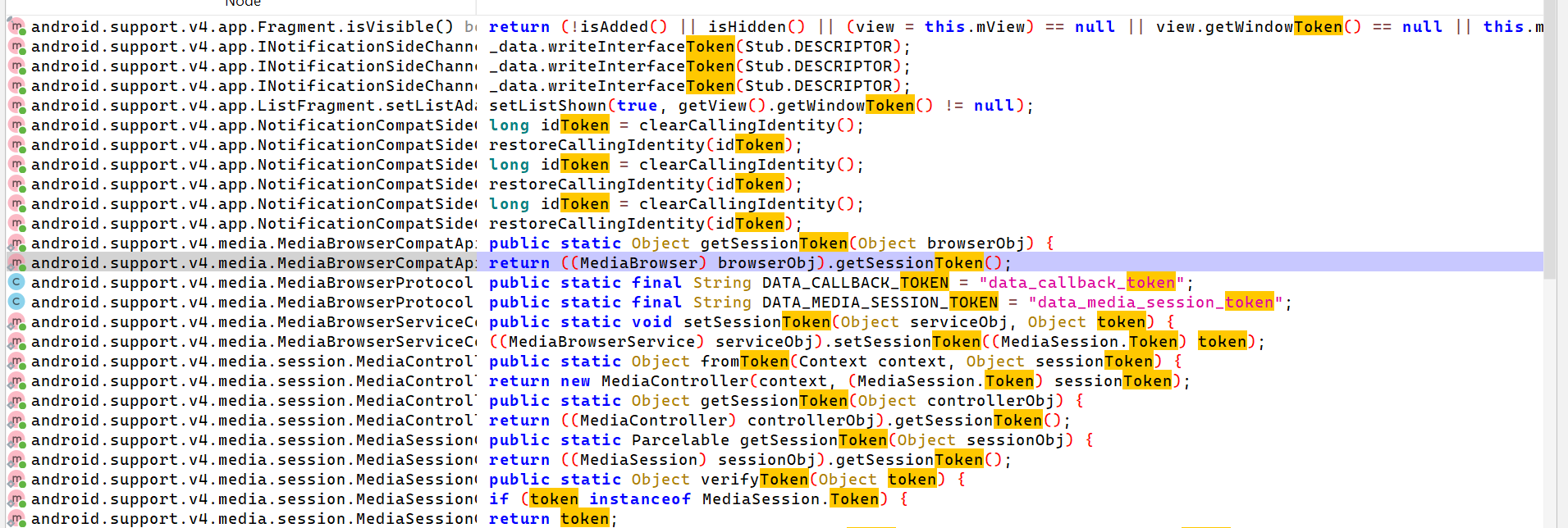
**Services**

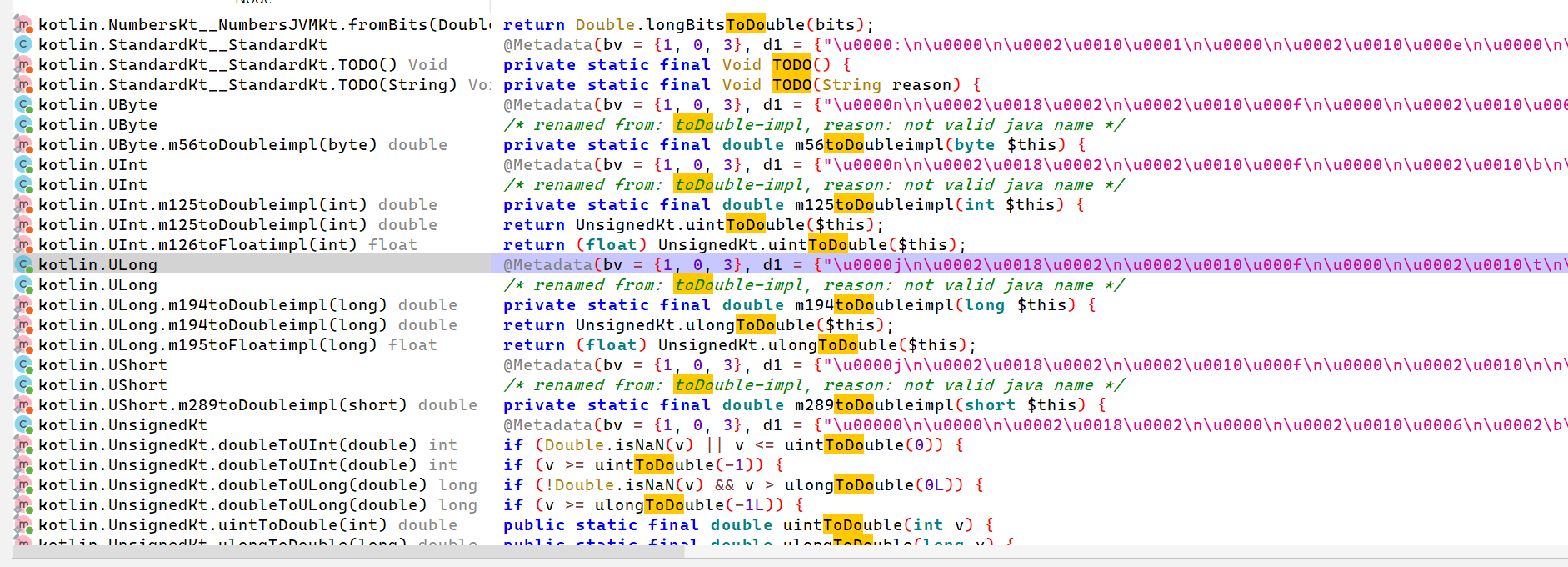


* + - Naviguez dans le code source décompilé (Java). Recherchez des mots-clés suspects (password, key, token, secret, TODO, etc.).









**Tutoriel à suivre** : Pentesting Mobile : Guide pas à pas de l'évaluation AndroGoat

**Liens** : https://infosecwriteups.com/mobile-pentesting-androgoat-assessment-walkthrough-

1a63a7edc677