ATTACK DEFENSE

by PentesterAcademy

Name	Bad Permission I
URL	https://attackdefense.com/challengedetails?cid=1623
Type	Android Pentesting : Basics

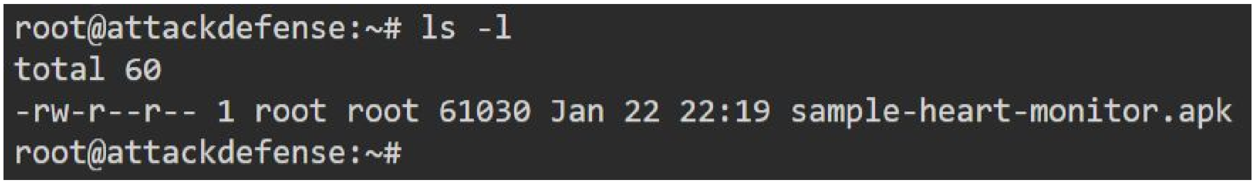
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Analyze the AndroidManifest.xml and identify the unnecessary/suspicious permission.

Solution:

Step 1: Start the lab and check the contents of the home directory.

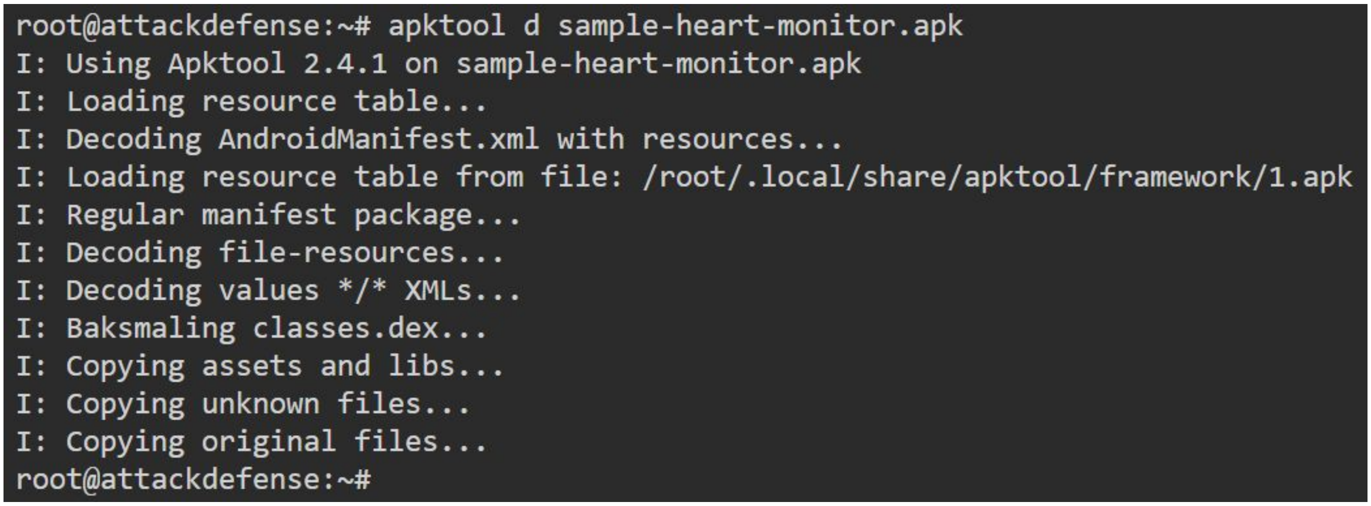
Command: ls -l



```
root@attackdefense:~# ls -l
total 60
-rw-r--r-- 1 root root 61030 Jan 22 22:19 sample-heart-monitor.apk
root@attackdefense:~#
```

Step 2: Open the APK using apktool

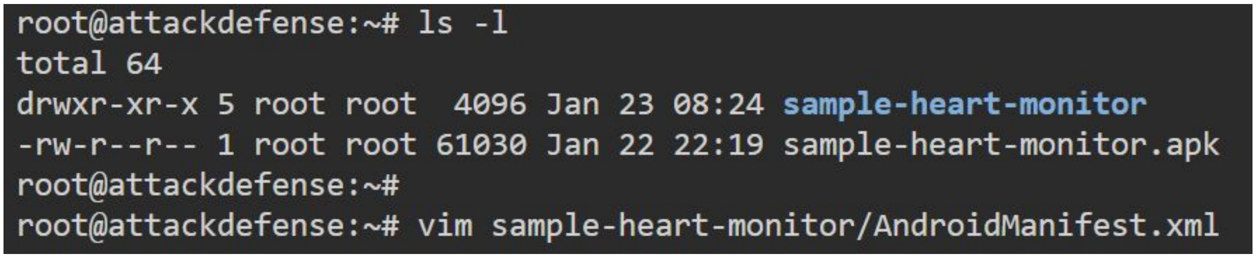
Command: apktool d sample-heart-monitor.apk



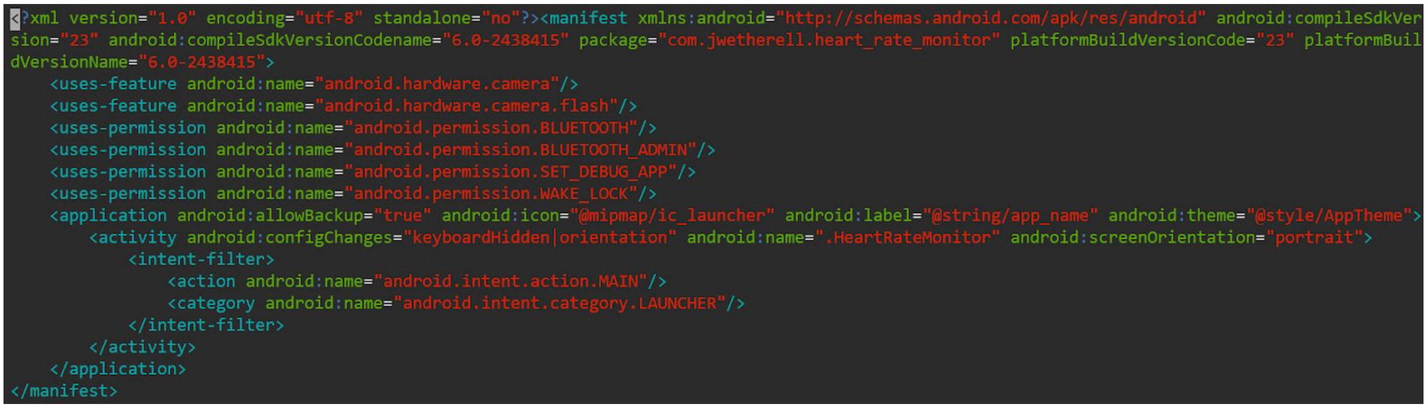
```
root@attackdefense:~# apktool d sample-heart-monitor.apk
I: Using Apktool 2.4.1 on sample-heart-monitor.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
root@attackdefense:~#
```

Step 3: Apktool will extract all files in a new directory. Open the AndroidManifest.xml file and read it thoroughly.

Command: vim sample-heart-monitor/AndroidManifest.xml

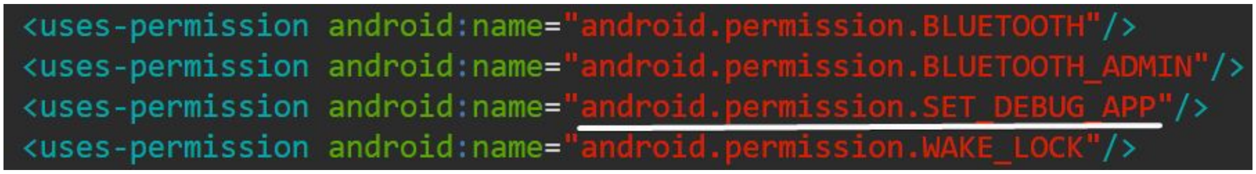


```
root@attackdefense:~# ls -l
total 64
drwxr-xr-x 5 root root  4096 Jan 23 08:24 sample-heart-monitor
-rw-r--r-- 1 root root 61030 Jan 22 22:19 sample-heart-monitor.apk
root@attackdefense:~#
root@attackdefense:~# vim sample-heart-monitor/AndroidManifest.xml
```



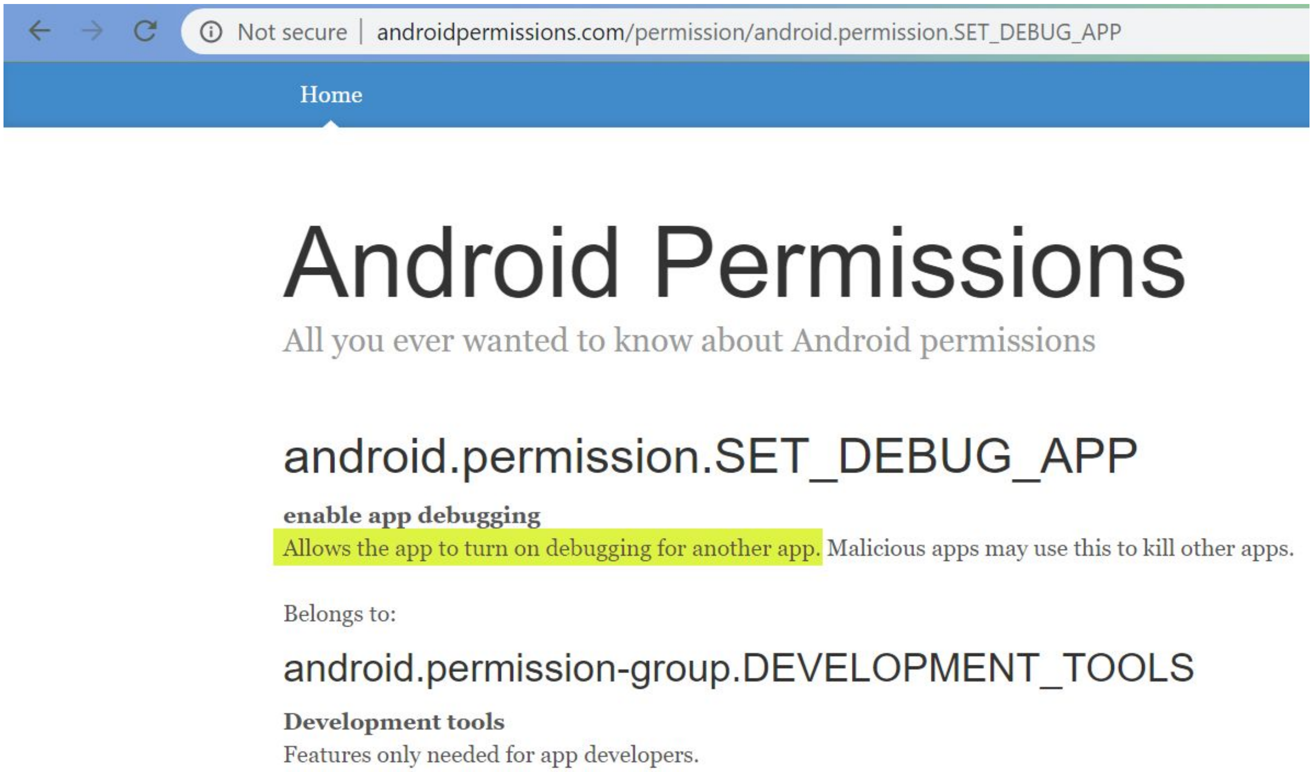
```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" android:compileSdkVer
sion="23" android:compileSdkVersionCodename="6.0-2438415" package="com.jwetherell.heart_rate_monitor" platformBuildVersionCode="23" platformBuil
dVersionName="6.0-2438415">
    <uses-feature android:name="android.hardware.camera"/>
    <uses-feature android:name="android.hardware.camera.flash"/>
    <uses-permission android:name="android.permission.BLUETOOTH"/>
    <uses-permission android:name="android.permission.BLUETOOTH_ADMIN"/>
    <uses-permission android:name="android.permission.SET_DEBUG_APP"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <application android:allowBackup="true" android:icon="@mipmap/ic_launcher" android:label="@string/app_name" android:theme="@style/AppTheme">
        <activity android:configChanges="keyboardHidden|orientation" android:name=".HeartRateMonitor" android:screenOrientation="portrait">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
    </application>
</manifest>
```

Step 4: Check the permission elements



```
<uses-permission android:name="android.permission.BLUETOOTH"/>
<uses-permission android:name="android.permission.BLUETOOTH_ADMIN"/>
<uses-permission android:name="android.permission.SET_DEBUG_APP"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
```

Step 5: The android.permission.SET_DEBUG_APP allows the application to turn on debugging for another application.


Not secure | androidpermissions.com/permission/android.permission.SET_DEBUG_APP
Home

Android Permissions

All you ever wanted to know about Android permissions

android.permission.SET_DEBUG_APP

enable app debugging

Allows the app to turn on debugging for another app. Malicious apps may use this to kill other apps.

Belongs to:

android.permission-group.DEVELOPMENT_TOOLS

Development tools

Features only needed for app developers.

There is no reason for a heart rate monitor application to have this permission. So, this is the answer.

References:

1. AndroidManifest.xml (https://developer.android.com/guide/topics/manifest/manifest-intro)
2. Information on permissions: http://androidpermissions.com/
3. SET_DEBUG_APP (http://androidpermissions.com/permission/android.permission.SET_DEBUG_APP)
4. Base AndroidManifest.xml is taken from here: https://github.com/phishman3579/android-heart-rate-monitor