Android Application Vulnerability Assessment Report

(Hack2Hire)

1. Android Application Name :	**InsecureBankv2**
2. Application Package Name:	com.android.insecurebankv2
3. Application Server :	No Application Server Used (Only Local Analysis Performed)
4. Number of Activities :	10 Activities
5. Local Database :	Sqlite
6. Access Permission :	ALL
7. Auditor Name :	Manish Gupta

Detailed Report :

Name : Local Analysis (Static Code Analysis)	**Risk Rating :** *Medium (CVSS : 6-7)*

List of Security Issues :

A. These are the Security Vulnerabilities which is happen because of Misconfiguration In AndroidManifest.xml file.

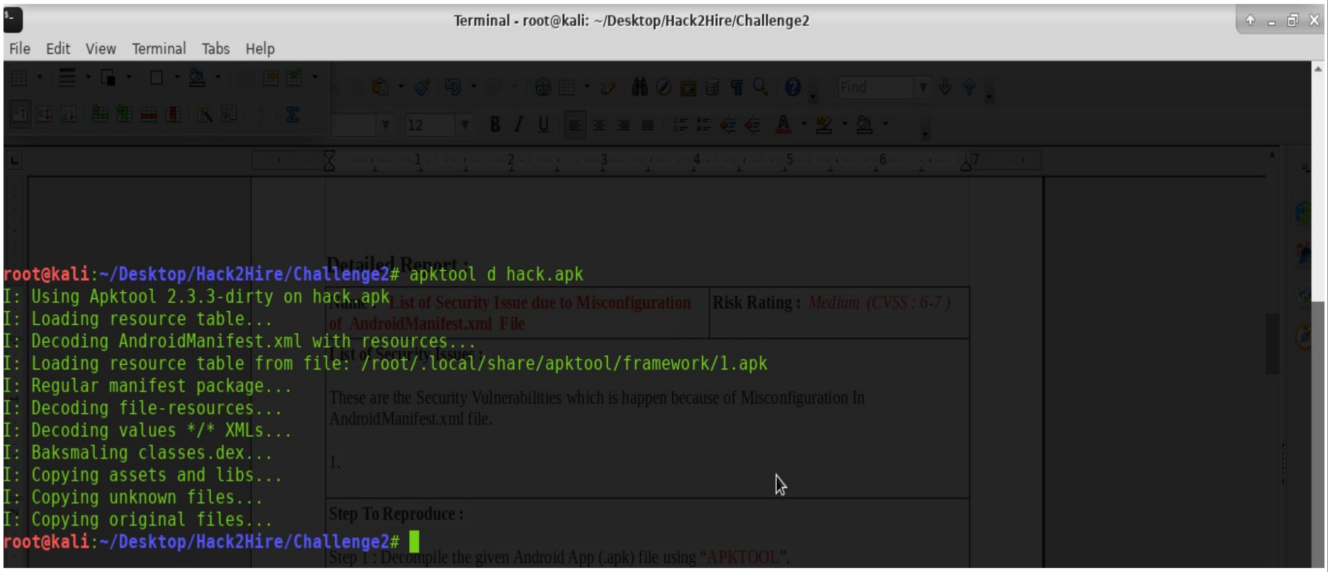
1. Insecure Content Provider access
2. Unnecessary Access Permission
3. Activities exported="true" .
4. Application Data Backup : allowBackup="true"
5. Application Debugging : debuggable="true"

B. These are the Security Vulnerabilities which is happen because of Source code Related issue.

1. Hardcoded secrets (Open the converted JAR file using JD-GUI)

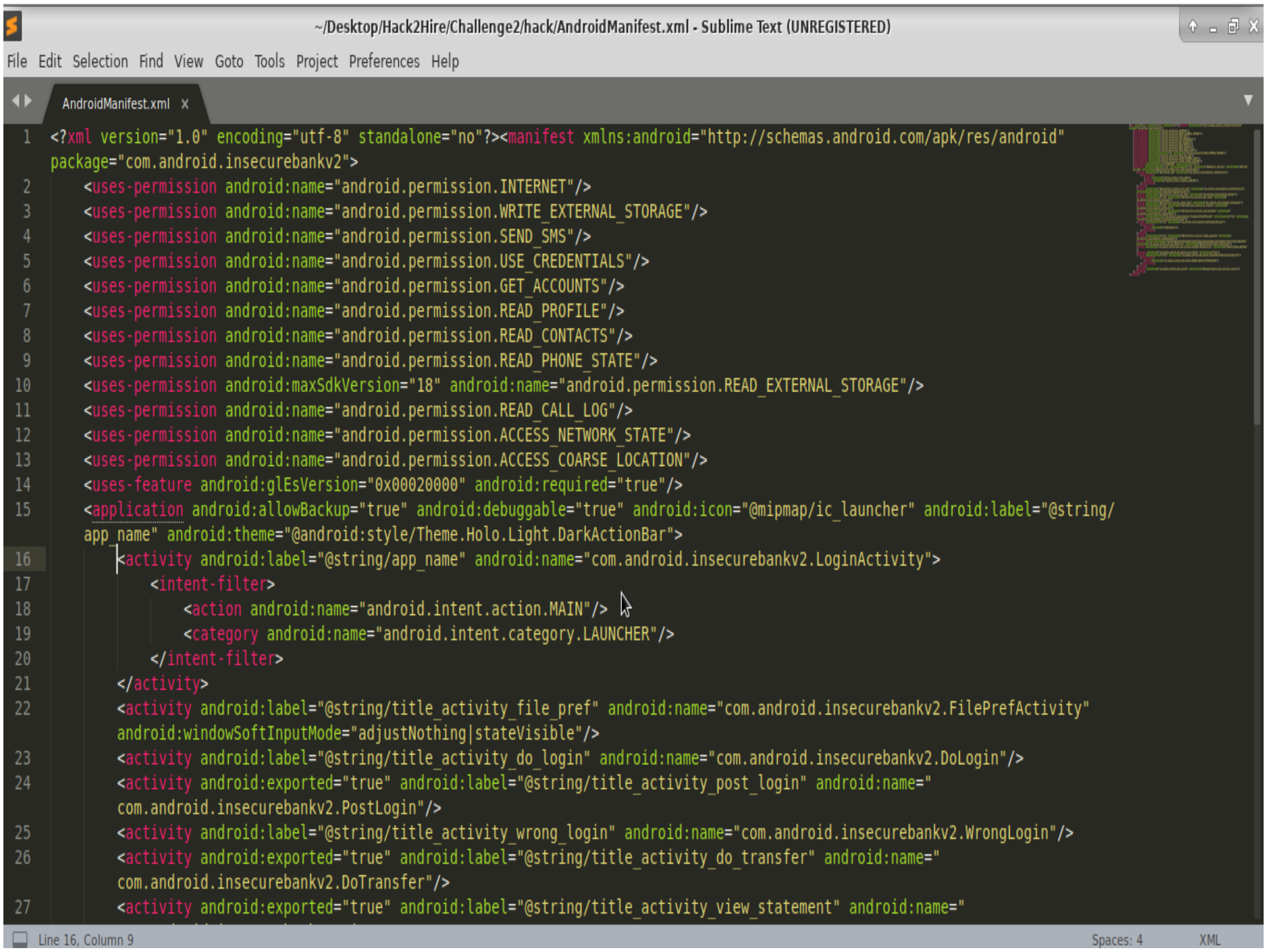
Step To Reproduce :

Step 1 : Decompile the given Android App (.apk) file using “APKTOOL”.



```
root@kali:~/Desktop/Hack2Hire/Challenge2# apktool d hack.apk
I: Using Apktool 2.3.3-dirty on hack.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@kali:~/Desktop/Hack2Hire/Challenge2#
```

Step 2: Now open the “**AndroidManifest.xml**” File using any text editor. Which Present is in Decompile Directory of APK.


~/Desktop/Hack2Hire/Challenge2/hack/AndroidManifest.xml - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
AndroidManifest.xml
Line 16, Column 9
Spaces: 4
XML

```xml
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android"
package="com.android.insecurebankv2">
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.SEND_SMS"/>
    <uses-permission android:name="android.permission.USE_CREDENTIALS"/>
    <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
    <uses-permission android:name="android.permission.READ_PROFILE"/>
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:maxSdkVersion="18" android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_CALL_LOG"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-feature android:glEsVersion="0x00020000" android:required="true"/>
    <application android:allowBackup="true" android:debuggable="true" android:icon="@mipmap/ic_launcher" android:label="@string/
    app_name" android:theme="@android:style/Theme.Holo.Light.DarkActionBar">
        <activity android:label="@string/app_name" android:name="com.android.insecurebankv2.LoginActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/title_activity_file_pref" android:name="com.android.insecurebankv2.FilePrefActivity"
        android:windowSoftInputMode="adjustNothing|stateVisible"/>
        <activity android:label="@string/title_activity_do_login" android:name="com.android.insecurebankv2.DoLogin"/>
        <activity android:exported="true" android:label="@string/title_activity_post_login" android:name="
        com.android.insecurebankv2.PostLogin"/>
        <activity android:label="@string/title_activity_wrong_login" android:name="com.android.insecurebankv2.WrongLogin"/>
        <activity android:exported="true" android:label="@string/title_activity_do_transfer" android:name="
        com.android.insecurebankv2.DoTransfer"/>
        <activity android:exported="true" android:label="@string/title_activity_view_statement" android:name="
```

Note: One Can see that because of Improper Configuration in AndroidManifest.xml file, A lot of Security Issues are present.

Name : Local Analysis (Dynamic (Run Time) Analysis)	Risk Rating : *Medium (CVSS : 6-7)*

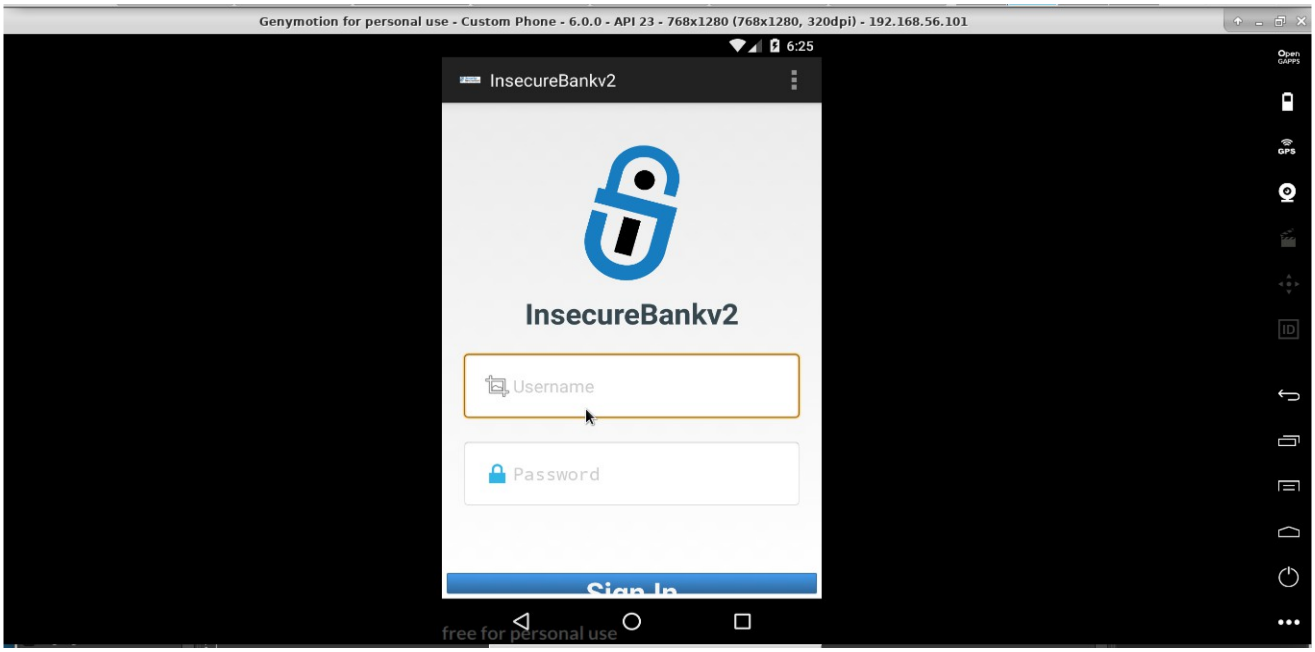
List of Security Issues :

These are the Security Vulnerabilities which is happen because of Insecure Coding Practices and Weak Cryptography Encryption .

1. Local Encryption issues
2. Root Detection and Bypass
3. Insecure Webview implementation
4. Sensitive Information in Memory
5. Insecure Logging mechanism
6. Insecure SDCard storage
7. Application Debuggable

Step To Reproduce :

Step 1 : Install the Application in “Android Emulator” and Perform Security Analysis Using “ADB” Handler.


Genymotion for personal use - Custom Phone - 6.0.0 - API 23 - 768x1280 (768x1280, 320dpi) - 192.168.56.101
6:25
InsecureBankv2
InsecureBankv2
Username
Password
Sign In
free for personal use

Step 2: Perform Security Analysis using these ADB command .

1. adb connect (For Connect to Android Emulator)
2. adb logcat (For log analysis)
3. adb shell (For Access File System)
4. adb shell am (For Activity Manager)
5. Sqlitebrowser for Reading database information (Local Database).

Thank You