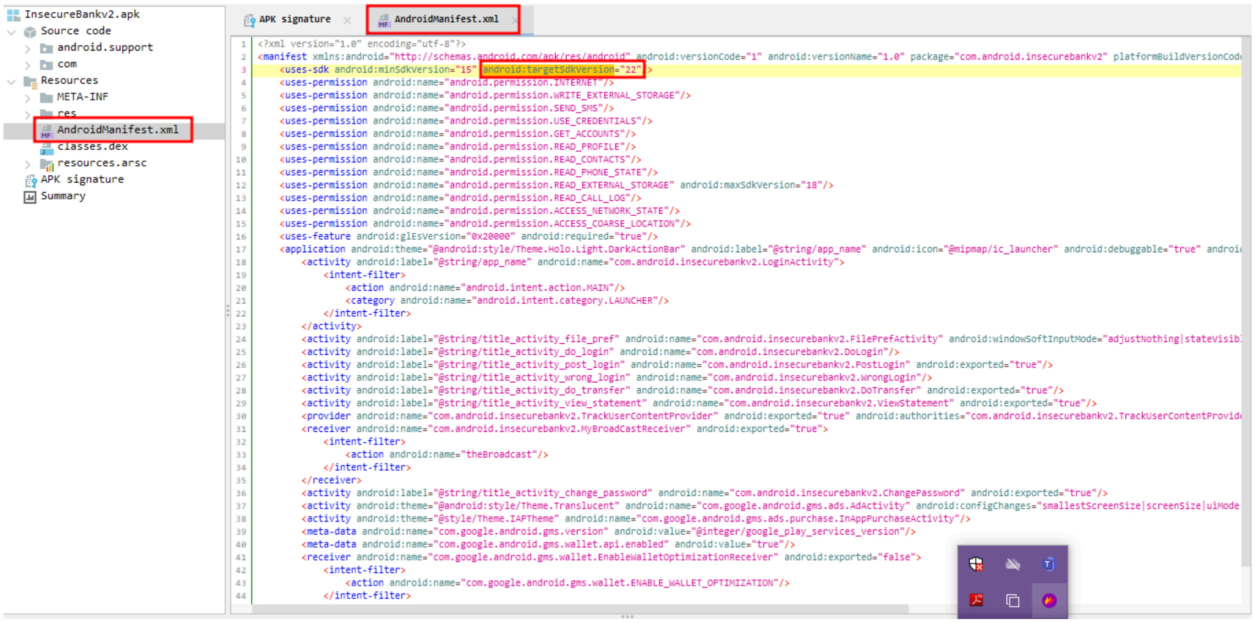
Vulnerability (static) Assessment Report for insecurebankv2

Submitted by :- Sauda Momin

1. Outdated Target SDK Version

Description:
The application is targeting an outdated SDK version (API Level 22). This means it is built for an older version of Android and does not align with the security and behavior changes introduced in later versions.



```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0" package="com.android.insecurebankv2" platformBuildVersionCod
    <uses-sdk android:minSdkVersion="15" android:targetSdkVersion="22"/>
    <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:name="android.permission.READ_EXTERNAL_STORAGE" android:maxSdkVersion="18"/>
    <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="0x20000" android:required="true"/>
    <application android:theme="@android:style/Theme.Holo.Light.DarkActionBar" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:debuggable="true" androi
        <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|stateVisib
        <activity android:label="@string/title_activity_do_login" android:name="com.android.insecurebankv2.DoLogin"/>
        <activity android:label="@string/title_activity_post_login" android:name="com.android.insecurebankv2.PostLogin" android:exported="true"/>
        <activity android:label="@string/title_activity_wrong_login" android:name="com.android.insecurebankv2.WrongLogin"/>
        <activity android:label="@string/title_activity_do_transfer" android:name="com.android.insecurebankv2.DoTransfer" android:exported="true"/>
        <activity android:label="@string/title_activity_view_statement" android:name="com.android.insecurebankv2.ViewStatement" android:exported="true"/>
        <provider android:name="com.android.insecurebankv2.TrackUserContentProvider" android:exported="true" android:authorities="com.android.insecurebankv2.TrackUserContentProvid
        <receiver android:name="com.android.insecurebankv2.MyBroadCastReceiver" android:exported="true">
            <intent-filter>
                <action android:name="theBroadcast"/>
            </intent-filter>
        </receiver>
        <activity android:label="@string/title_activity_change_password" android:name="com.android.insecurebankv2.ChangePassword" android:exported="true"/>
        <activity android:theme="@android:style/Theme.Translucent" android:name="com.google.android.gms.ads.AdActivity" android:configChanges="smallestScreenSize|screenSize|uiMode
        <activity android:theme="@style/Theme.IAPTheme" android:name="com.google.android.gms.ads.purchase.InAppPurchaseActivity"/>
        <meta-data android:name="com.google.android.gms.version" android:value="@integer/google_play_services_version"/>
        <meta-data android:name="com.google.android.gms.wallet.api.enabled" android:value="true"/>
        <receiver android:name="com.google.android.gms.wallet.EnableWalletOptimizationReceiver" android:exported="false">
            <intent-filter>
                <action android:name="com.google.android.gms.wallet.ENABLE_WALLET_OPTIMIZATION"/>
            </intent-filter>
```

Root Cause:
The targetSdkVersion in the app's build.gradle file has not been updated to the latest Android API level, causing the app to bypass modern security enforcement mechanisms.

Impact:

- The app does not benefit from modern Android security features such as:
  - Runtime permission model (introduced in Android 6.0).
  - Broadcast receiver visibility restrictions.
  - Background execution and service limitations.

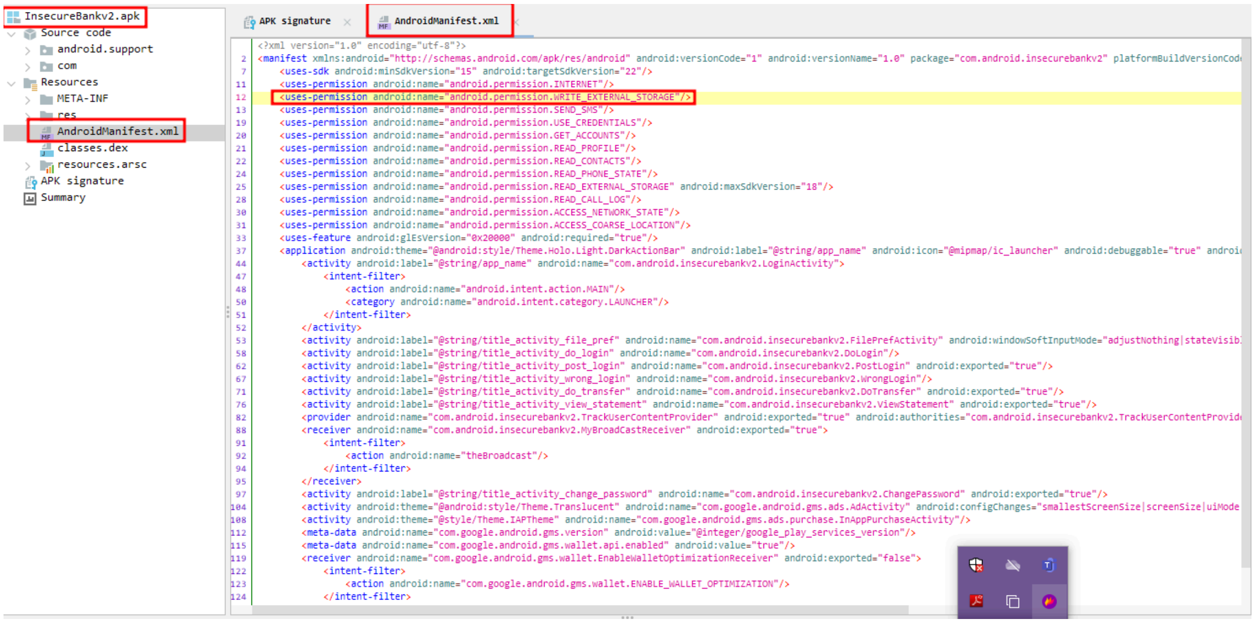
- Increased risk of privilege misuse, unintended data exposure, or unauthorized background activity.

Mitigation:
Update the targetSdkVersion to the latest stable release (API Level 33 or 34) in the build.gradle file, then review and modify the application code to ensure compatibility with new Android security and behavior policies.

2. Excessive External Storage Permission

Description:

The application requests permission to write data to external storage. This permission allows the app to read and write files in a location that is accessible to all other apps on the device.



```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0" package="com.android.insecurebankv2" platformBuildVersionCod
    <uses-sdk android:minSdkVersion="15" android:targetSdkVersion="22"/>
    <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:name="android.permission.READ_EXTERNAL_STORAGE" android:maxSdkVersion="18"/>
    <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="0x20000" android:required="true"/>
    <application android:theme="@android:style/Theme.Holo.Light.DarkActionBar" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:debuggable="true" androi
        <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|stateVisib
        <activity android:label="@string/title_activity_do_login" android:name="com.android.insecurebankv2.DoLogin"/>
        <activity android:label="@string/title_activity_post_login" android:name="com.android.insecurebankv2.PostLogin" android:exported="true"/>
        <activity android:label="@string/title_activity_wrong_login" android:name="com.android.insecurebankv2.WrongLogin"/>
        <activity android:label="@string/title_activity_do_transfer" android:name="com.android.insecurebankv2.DoTransfer" android:exported="true"/>
        <activity android:label="@string/title_activity_view_statement" android:name="com.android.insecurebankv2.ViewStatement" android:exported="true"/>
        <provider android:name="com.android.insecurebankv2.TrackUserContentProvider" android:exported="true" android:authorities="com.android.insecurebankv2.TrackUserContentProvid
        <receiver android:name="com.android.insecurebankv2.MyBroadCastReceiver" android:exported="true">
            <intent-filter>
                <action android:name="theBroadcast"/>
            </intent-filter>
        </receiver>
        <activity android:label="@string/title_activity_change_password" android:name="com.android.insecurebankv2.ChangePassword" android:exported="true"/>
        <activity android:theme="@android:style/Theme.Translucent" android:name="com.google.android.gms.ads.AdActivity" android:configChanges="smallestScreenSize|screenSize|uiMode
        <activity android:theme="@style/Theme.IAPTheme" android:name="com.google.android.gms.ads.purchase.InAppPurchaseActivity"/>
        <meta-data android:name="com.google.android.gms.version" android:value="@integer/google_play_services_version"/>
        <meta-data android:name="com.google.android.gms.wallet.api.enabled" android:value="true"/>
        <receiver android:name="com.google.android.gms.wallet.EnableWalletOptimizationReceiver" android:exported="false">
            <intent-filter>
                <action android:name="com.google.android.gms.wallet.ENABLE_WALLET_OPTIMIZATION"/>
            </intent-filter>
```

Root Cause:

The app declares the WRITE_EXTERNAL_STORAGE permission in the Android manifest without a valid necessity, enabling access to publicly readable and modifiable storage areas.

Impact:

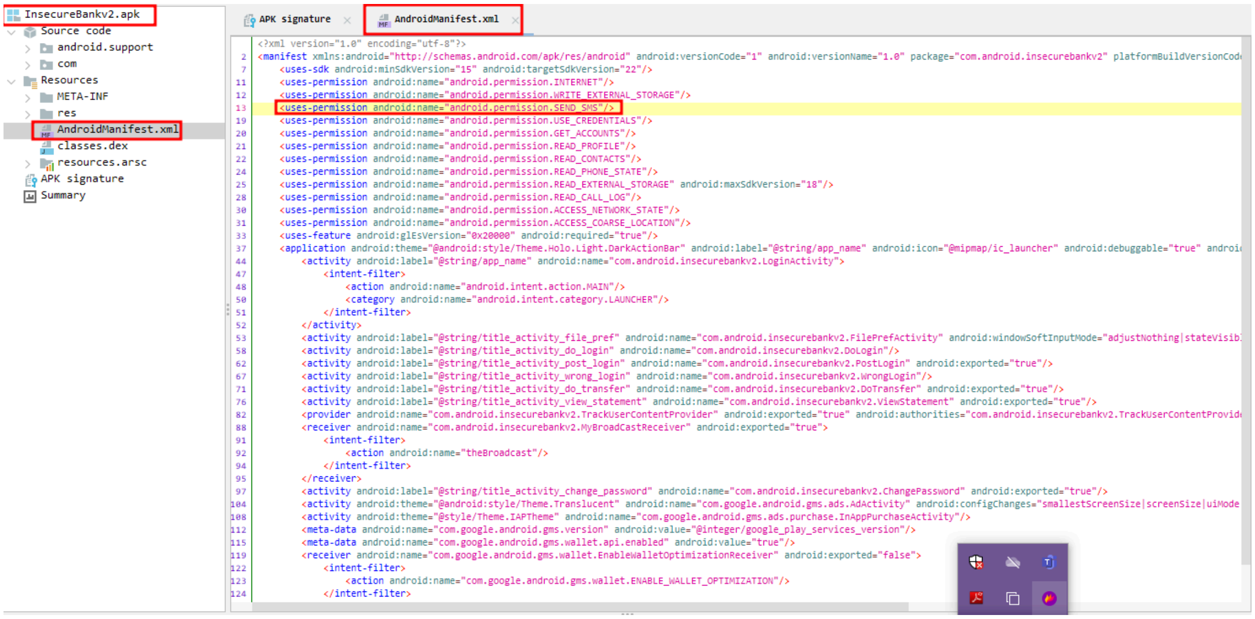
- Sensitive data saved in external storage can be accessed, modified, or deleted by other apps.
- This increases the risk of data leakage, unauthorized manipulation, and potential exploitation by malicious apps.

Mitigation:

- Store sensitive data in internal storage or use scoped storage APIs introduced in Android 10 (API level 29).
- Remove the WRITE_EXTERNAL_STORAGE permission if not required for app functionality.
- Restrict file access using private app directories or content providers.

3. Dangerous Permission Granted by Default

Description:
The application uses a dangerous permission (e.g., SEND_SMS) that is automatically granted at installation time because the app targets an old Android SDK version.



```xml
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0" package="com.android.insecurebankv2" platformBuildVersionCod
    <uses-sdk android:minSdkVersion="15" android:targetSdkVersion="22"/>
    <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:name="android.permission.READ_EXTERNAL_STORAGE" android:maxSdkVersion="18"/>
    <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="0x20000" android:required="true"/>
    <application android:theme="@android:style/Theme.Holo.Light.DarkActionBar" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:debuggable="true" androi
        <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|stateVisib
        <activity android:label="@string/title_activity_do_login" android:name="com.android.insecurebankv2.DoLogin"/>
        <activity android:label="@string/title_activity_post_login" android:name="com.android.insecurebankv2.PostLogin" android:exported="true"/>
        <activity android:label="@string/title_activity_wrong_login" android:name="com.android.insecurebankv2.WrongLogin"/>
        <activity android:label="@string/title_activity_do_transfer" android:name="com.android.insecurebankv2.DoTransfer" android:exported="true"/>
        <activity android:label="@string/title_activity_view_statement" android:name="com.android.insecurebankv2.ViewStatement" android:exported="true"/>
        <provider android:name="com.android.insecurebankv2.TrackUserContentProvider" android:exported="true" android:authorities="com.android.insecurebankv2.TrackUserContentProvid
        <receiver android:name="com.android.insecurebankv2.MyBroadCastReceiver" android:exported="true">
            <intent-filter>
                <action android:name="theBroadcast"/>
            </intent-filter>
        </receiver>
        <activity android:label="@string/title_activity_change_password" android:name="com.android.insecurebankv2.ChangePassword" android:exported="true"/>
        <activity android:theme="@android:style/Theme.Translucent" android:name="com.google.android.gms.ads.AdActivity" android:configChanges="smallestScreenSize|screenSize|uiMode
        <activity android:theme="@style/Theme.IAPTheme" android:name="com.google.android.gms.ads.purchase.InAppPurchaseActivity"/>
        <meta-data android:name="com.google.android.gms.version" android:value="@integer/google_play_services_version"/>
        <meta-data android:name="com.google.android.gms.wallet.api.enabled" android:value="true"/>
        <receiver android:name="com.google.android.gms.wallet.EnableWalletOptimizationReceiver" android:exported="false">
            <intent-filter>
                <action android:name="com.google.android.gms.wallet.ENABLE_WALLET_OPTIMIZATION"/>
            </intent-filter>
```

Root Cause:
The app targets a pre-Marshmallow (API < 23) SDK, which does not enforce the runtime permission model, causing dangerous permissions to be granted automatically upon installation.

Impact:

- Malicious apps or attackers could exploit this permission to perform sensitive operations (e.g., sending SMS to premium-rate numbers) without user awareness or consent.
- Leads to privacy violations, financial loss, or unauthorized actions on the device.

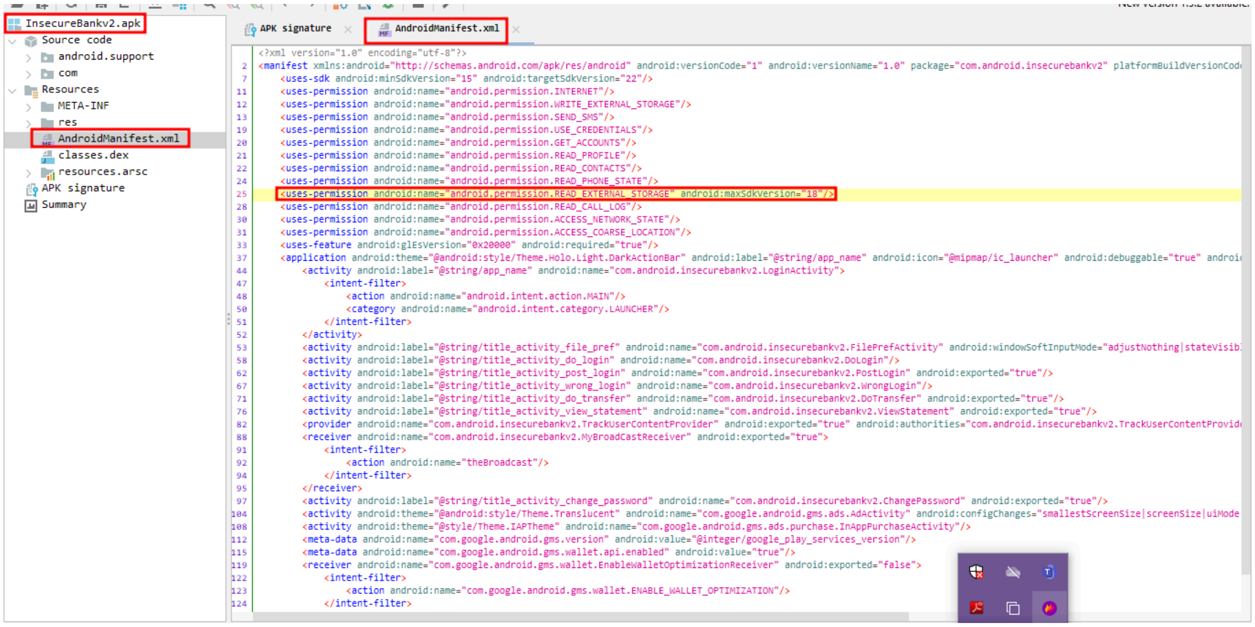
Mitigation:

- Update the app to target the latest SDK version (API 33/34) to enforce the runtime permission model.
- Request dangerous permissions dynamically at runtime with clear user justification.
- Remove unused dangerous permissions from the manifest.

4. Legacy External Storage Read Permission

Description:

The application requests permission to read from external storage, which provides access to files stored in shared public directories on the device.



```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0" package="com.android.insecurebankv2" platformBuildVersionCod
    <uses-sdk android:minSdkVersion="15" android:targetSdkVersion="22"/>
    <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:name="android.permission.READ_EXTERNAL_STORAGE" android:maxSdkVersion="18"/>
    <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="0x20000" android:required="true"/>
    <application android:theme="@android:style/Theme.Holo.Light.DarkActionBar" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:debuggable="true" androi
        <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|stateVisib
        <activity android:label="@string/title_activity_do_login" android:name="com.android.insecurebankv2.DoLogin"/>
        <activity android:label="@string/title_activity_post_login" android:name="com.android.insecurebankv2.PostLogin" android:exported="true"/>
        <activity android:label="@string/title_activity_wrong_login" android:name="com.android.insecurebankv2.WrongLogin"/>
        <activity android:label="@string/title_activity_do_transfer" android:name="com.android.insecurebankv2.DoTransfer" android:exported="true"/>
        <activity android:label="@string/title_activity_view_statement" android:name="com.android.insecurebankv2.ViewStatement" android:exported="true"/>
        <provider android:name="com.android.insecurebankv2.TrackUserContentProvider" android:exported="true" android:authorities="com.android.insecurebankv2.TrackUserContentProvid
        <receiver android:name="com.android.insecurebankv2.MyBroadCastReceiver" android:exported="true">
            <intent-filter>
                <action android:name="theBroadcast"/>
            </intent-filter>
        </receiver>
        <activity android:label="@string/title_activity_change_password" android:name="com.android.insecurebankv2.ChangePassword" android:exported="true"/>
        <activity android:theme="@android:style/Theme.Translucent" android:name="com.google.android.gms.ads.AdActivity" android:configChanges="smallestScreenSize|screenSize|uiMode
        <activity android:theme="@style/Theme.IAPTheme" android:name="com.google.android.gms.ads.purchase.InAppPurchaseActivity"/>
        <meta-data android:name="com.google.android.gms.version" android:value="@integer/google_play_services_version"/>
        <meta-data android:name="com.google.android.gms.wallet.api.enabled" android:value="true"/>
        <receiver android:name="com.google.android.gms.wallet.EnableWalletOptimizationReceiver" android:exported="false">
            <intent-filter>
                <action android:name="com.google.android.gms.wallet.ENABLE_WALLET_OPTIMIZATION"/>
            </intent-filter>
```

Root Cause:

The app declares the READ_EXTERNAL_STORAGE permission in the manifest, maintaining compatibility with older Android versions where storage access was less restricted.

Impact:

- Sensitive files stored on external storage can be accessed by other apps.
- This increases the risk of data leakage, information disclosure, and unauthorized access to user data.

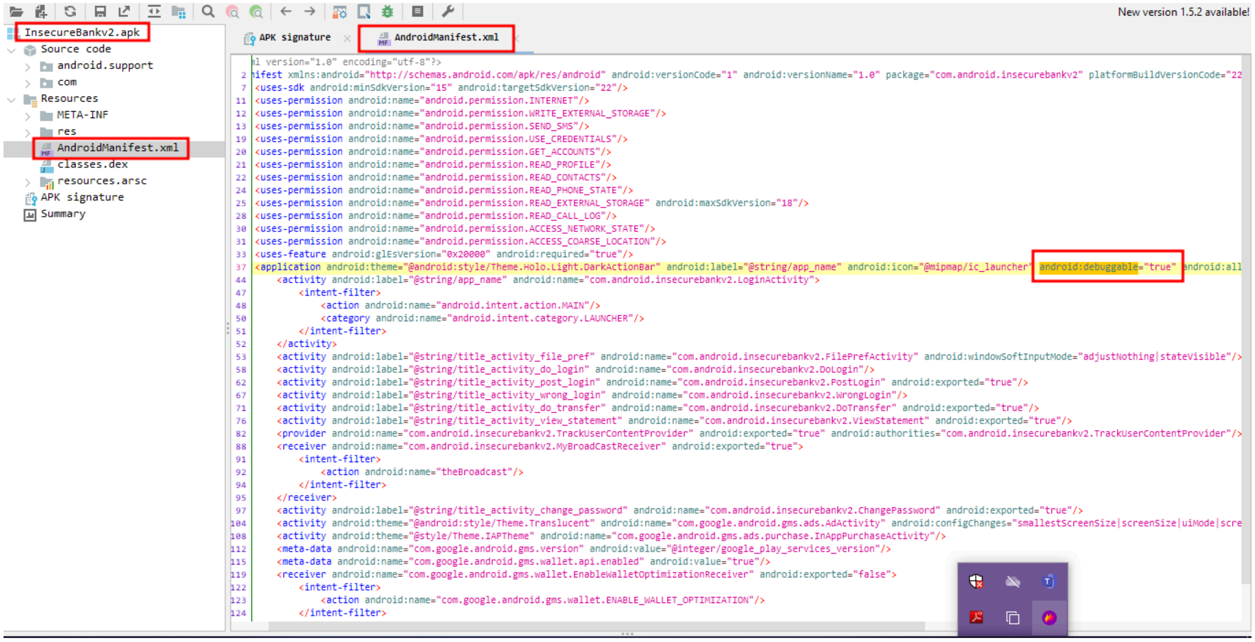
Mitigation:

- Avoid storing or accessing sensitive data in external storage.
- Use internal app-specific storage or scoped storage APIs (introduced in Android 10, API 29).
- Remove the READ_EXTERNAL_STORAGE permission if it is not required by app functionality.

5. Debuggable App in Production

Description:

The application is built with debugging enabled, allowing it to run in debug mode even in the production environment.



```
l version="1.0" encoding="utf-8"?>
ifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0" package="com.android.insecurebankv2" platformBuildVersionCode="22
<uses-sdk android:minSdkVersion="15" android:targetSdkVersion="22"/>
<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:name="android.permission.READ_EXTERNAL_STORAGE" android:maxSdkVersion="18"/>
<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="0x20000" android:required="true"/>
<application android:theme="@android:style/Theme.Holo.Light.DarkActionBar" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:debuggable="true" android:all
    <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:label="@string/title_activity_post_login" android:name="com.android.insecurebankv2.PostLogin" android:exported="true"/>
    <activity android:label="@string/title_activity_wrong_login" android:name="com.android.insecurebankv2.WrongLogin"/>
    <activity android:label="@string/title_activity_do_transfer" android:name="com.android.insecurebankv2.DoTransfer" android:exported="true"/>
    <activity android:label="@string/title_activity_view_statement" android:name="com.android.insecurebankv2.ViewStatement" android:exported="true"/>
    <provider android:name="com.android.insecurebankv2.TrackUserContentProvider" android:exported="true" android:authorities="com.android.insecurebankv2.TrackUserContentProvider"/>
    <receiver android:name="com.android.insecurebankv2.MyBroadCastReceiver" android:exported="true">
        <intent-filter>
            <action android:name="theBroadcast"/>
        </intent-filter>
    </receiver>
    <activity android:label="@string/title_activity_change_password" android:name="com.android.insecurebankv2.ChangePassword" android:exported="true"/>
    <activity android:theme="@android:style/Theme.Translucent" android:name="com.google.android.gms.ads.AdActivity" android:configChanges="smallestScreenSize|screenSize|uiMode|scre
    <activity android:theme="@style/Theme.IAPTheme" android:name="com.google.android.gms.ads.purchase.InAppPurchaseActivity"/>
    <meta-data android:name="com.google.android.gms.version" android:value="@integer/google_play_services_version"/>
    <meta-data android:name="com.google.android.gms.wallet.api.enabled" android:value="true"/>
    <receiver android:name="com.google.android.gms.wallet.EnableWalletOptimizationReceiver" android:exported="false">
        <intent-filter>
            <action android:name="com.google.android.gms.wallet.ENABLE_WALLET_OPTIMIZATION"/>
        </intent-filter>
```

Root Cause:

The android:debuggable attribute in the AndroidManifest.xml file is set to "true" (or automatically enabled by a debug build configuration), exposing the app to debugging tools.

Impact:

- Attackers can attach a debugger to the app to inspect memory, modify runtime variables, and bypass security checks.
- Enables extraction of sensitive data, such as credentials or encryption keys, from the app's memory or backup files.

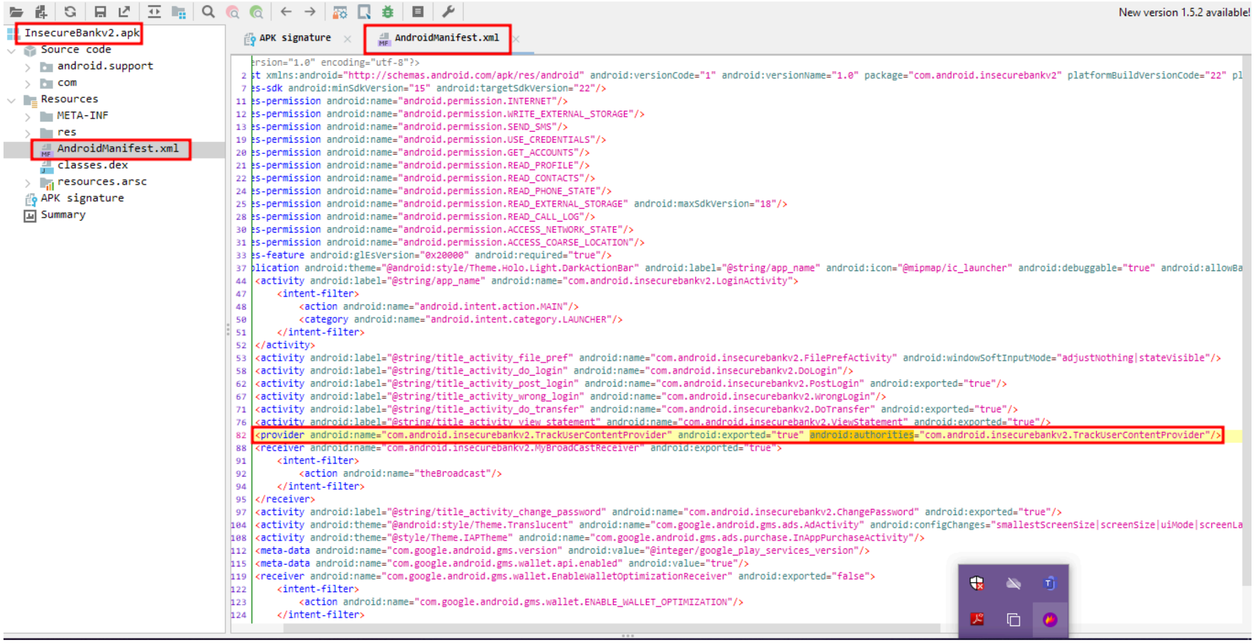
Mitigation:

- Ensure android:debuggable="false" in the release build configuration.
- Verify release APKs using aapt dump badging <app.apk> to confirm the debuggable flag is disabled.
- Maintain separate debug and release build variants to prevent accidental exposure.

6. Unprotected ContentProvider Exposure

Description:

The application’s ContentProvider component is publicly exposed without any access restrictions, allowing other apps to query or modify its data through content URIs.



```
ersion="1.0" encoding="utf-8"?>
st xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0" package="com.android.insecurebankv2" platformBuildVersionCode="22" pl
es-sdk android:minSdkVersion="15" android:targetSdkVersion="22"/>
es-permission android:name="android.permission.INTERNET"/>
es-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
es-permission android:name="android.permission.SEND_SMS"/>
es-permission android:name="android.permission.USE_CREDENTIALS"/>
es-permission android:name="android.permission.GET_ACCOUNTS"/>
es-permission android:name="android.permission.READ_PROFILE"/>
es-permission android:name="android.permission.READ_CONTACTS"/>
es-permission android:name="android.permission.READ_PHONE_STATE"/>
es-permission android:name="android.permission.READ_EXTERNAL_STORAGE" android:maxSdkVersion="18"/>
es-permission android:name="android.permission.READ_CALL_LOG"/>
es-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
es-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
es-feature android:glEsVersion="0x20000" android:required="true"/>
plication android:theme="@android:style/Theme.Holo.Light.DarkActionBar" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:debuggable="true" android:allowBa
<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:label="@string/title_activity_post_login" android:name="com.android.insecurebankv2.PostLogin" android:exported="true"/>
<activity android:label="@string/title_activity_wrong_login" android:name="com.android.insecurebankv2.WrongLogin"/>
<activity android:label="@string/title_activity_do_transfer" android:name="com.android.insecurebankv2.DoTransfer" android:exported="true"/>
<activity android:label="@string/title_activity_view_statement" android:name="com.android.insecurebankv2.ViewStatement" android:exported="true"/>
<provider android:name="com.android.insecurebankv2.TrackUserContentProvider" android:exported="true" android:authorities="com.android.insecurebankv2.TrackUserContentProvider"/>
<receiver android:name="com.android.insecurebankv2.MyBroadCastReceiver" android:exported="true">
    <intent-filter>
        <action android:name="theBroadcast"/>
    </intent-filter>
</receiver>
<activity android:label="@string/title_activity_change_password" android:name="com.android.insecurebankv2.ChangePassword" android:exported="true"/>
<activity android:theme="@android:style/Theme.Translucent" android:name="com.google.android.gms.ads.AdActivity" android:configChanges="smallestScreenSize|screenSize|uiMode|screenLa
<activity android:theme="@style/Theme.IAPTheme" android:name="com.google.android.gms.ads.purchase.InAppPurchaseActivity"/>
<meta-data android:name="com.google.android.gms.version" android:value="@integer/google_play_services_version"/>
<meta-data android:name="com.google.android.gms.wallet.api.enabled" android:value="true"/>
<receiver android:name="com.google.android.gms.wallet.EnableWalletOptimizationReceiver" android:exported="false">
    <intent-filter>
        <action android:name="com.google.android.gms.wallet.ENABLE_WALLET_OPTIMIZATION"/>
    </intent-filter>
```

Root Cause:

The android:exported attribute in the AndroidManifest.xml is set to true (or not explicitly defined), and no readPermission or writePermission is enforced for the ContentProvider.

Impact:

- Malicious apps can read, modify, or inject data into the exposed ContentProvider.
- This can lead to data theft, data corruption, or privilege escalation through unauthorized access to the app’s internal data.

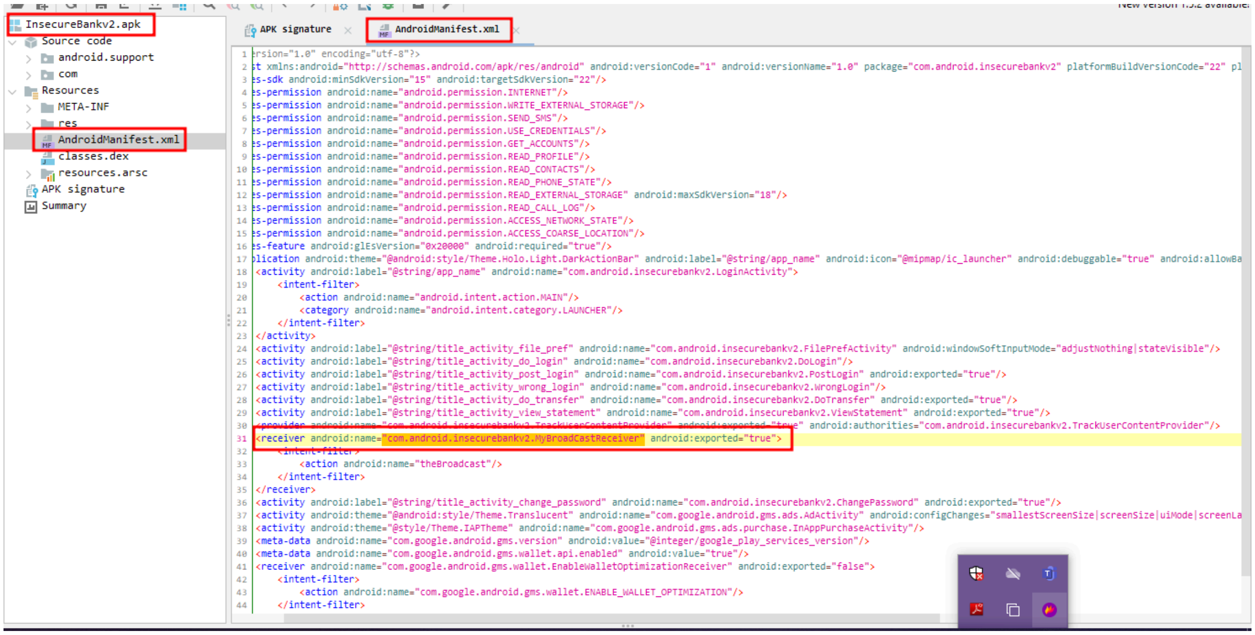
Mitigation:

- Set android:exported="false" for ContentProvider components that are not intended for external access.
- If external access is required, enforce proper permissions using android:readPermission and android:writePermission.
- Validate and sanitize all inputs received through content URIs.

7. Unprotected Exported BroadcastReceiver

Description:

The application exposes a BroadcastReceiver publicly without enforcing any permissions, allowing external apps to send intents to it.



```
rsion="1.0" encoding="utf-8"?>
t xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0" package="com.android.insecurebankv2" platformBuildVersionCode="22" pl
s-sdk android:minSdkVersion="15" android:targetSdkVersion="22"/>
s-permission android:name="android.permission.INTERNET"/>
s-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
s-permission android:name="android.permission.SEND_SMS"/>
s-permission android:name="android.permission.USE_CREDENTIALS"/>
s-permission android:name="android.permission.GET_ACCOUNTS"/>
s-permission android:name="android.permission.READ_PROFILE"/>
s-permission android:name="android.permission.READ_CONTACTS"/>
s-permission android:name="android.permission.READ_PHONE_STATE"/>
s-permission android:name="android.permission.READ_EXTERNAL_STORAGE" android:maxSdkVersion="18"/>
s-permission android:name="android.permission.READ_CALL_LOG"/>
s-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
s-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
s-feature android:glEsVersion="0x20000" android:required="true"/>
lication android:theme="@android:style/Theme.Holo.Light.DarkActionBar" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:debuggable="true" android:allowBa
<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:label="@string/title_activity_post_login" android:name="com.android.insecurebankv2.PostLogin" android:exported="true"/>
<activity android:label="@string/title_activity_wrong_login" android:name="com.android.insecurebankv2.WrongLogin"/>
<activity android:label="@string/title_activity_do_transfer" android:name="com.android.insecurebankv2.DoTransfer" android:exported="true"/>
<activity android:label="@string/title_activity_view_statement" android:name="com.android.insecurebankv2.ViewStatement" android:exported="true"/>
<provider android:name="com.android.insecurebankv2.TrackUserContentProvider" android:exported="true" android:authorities="com.android.insecurebankv2.TrackUserContentProvider"/>
<receiver android:name="com.android.insecurebankv2.MyBroadCastReceiver" android:exported="true">
    <intent-filter>
        <action android:name="theBroadcast"/>
    </intent-filter>
</receiver>
<activity android:label="@string/title_activity_change_password" android:name="com.android.insecurebankv2.ChangePassword" android:exported="true"/>
<activity android:theme="@android:style/Theme.Translucent" android:name="com.google.android.gms.ads.AdActivity" android:configChanges="smallestScreenSize|screenSize|uiMode|screenLa
<activity android:theme="@style/Theme.IAPTheme" android:name="com.google.android.gms.ads.purchase.InAppPurchaseActivity"/>
<meta-data android:name="com.google.android.gms.version" android:value="@integer/google_play_services_version"/>
<meta-data android:name="com.google.android.gms.wallet.api.enabled" android:value="true"/>
<receiver android:name="com.google.android.gms.wallet.EnableWalletOptimizationReceiver" android:exported="false">
    <intent-filter>
        <action android:name="com.google.android.gms.wallet.ENABLE_WALLET_OPTIMIZATION"/>
    </intent-filter>
```

Root Cause:

The android:exported attribute in the AndroidManifest.xml is set to true (or not defined for receivers with intent-filters), and no permissions are required to interact with the receiver.

Impact:

- Attackers can send **spoofed broadcasts** to the app.
- May result in **unauthorized actions**, **manipulation of app behavior**, or **execution of unintended code**.
- Could lead to **data corruption**, **denial of service**, or **privilege abuse**.

Mitigation:

- Set android:exported="false" for receivers intended for internal use only.
- If external broadcasts are required, enforce a signature-level permission using android:permission.
- Validate all incoming broadcast intents before processing.