M1 - Improper Platform Usage.

M1 - Improper Platform Usage

Penggunaan Platform yang Tidak Tepat terutama mencakup penyalahgunaan fitur platform atau gagal menggunakan kontrol keamanan platform yang disediakan dan didokumentasikan oleh platform dan komunitasnya. Pada aplikasi berbasis Android, file AndroidManifest.xml tentu saja merupakan informasi yang baik tentang konfigurasi platform dan bagaimana aplikasi seharusnya berperilaku. file ini memang harus diperiksa untuk konfigurasi kesalahan keamanan. Di sini, kita akan menggunakan proyek InsecureBankv2, aplikasi Android yang sengaja dibuat rentan untuk para penggemar keamanan dan pengembang untuk mempelajari tentang kerawanan Android dengan menguji aplikasi yang rentan.

AndroidManifest.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"/>
    <android:uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <android:uses-permission android:maxSdkVersion="18" android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <android: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="@andro
        <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="adju
        <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="com.android.insecurebankv2.ViewStatement"/>
        <provider android:authorities="com.android.insecurebankv2.TrackUserContentProvider" android:exported="true" android:name="com.android.insecurebankv2.Tr
        <receiver android:exported="true" android:name="com.android.insecurebankv2.MyBroadCastReceiver">
            <intent-filter>
                <action android:name="theBroadcast"/>
            </intent-filter>
        </receiver>
        <activity android:exported="true" android:label="@string/title_activity_change_password" android:name="com.android.insecurebankv2.ChangePassword"/>
        <activity android:configChanges="keyboard|keyboardHidden|orientation|screenLayout|screenSize|smallestScreenSize|uiMode" android:name="com.google.androi
        <activity android:name="com.google.android.gms.ads.purchase.InAppPurchaseActivity" android:theme="@style/Theme.IAPTheme"/>
        <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:exported="false" android:name="com.google.android.gms.wallet.EnableWalletOptimizationReceiver">
            <intent-filter>
                <action android:name="com.google.android.gms.wallet.ENABLE_WALLET_OPTIMIZATION"/>
            </intent-filter>
        </receiver>
    </application>
</manifest>
```

M1 - Improper Platform Usage

https://github.com/dineshshetty/Android-InsecureBankv2/blob/master/InsecureBankv2.apk

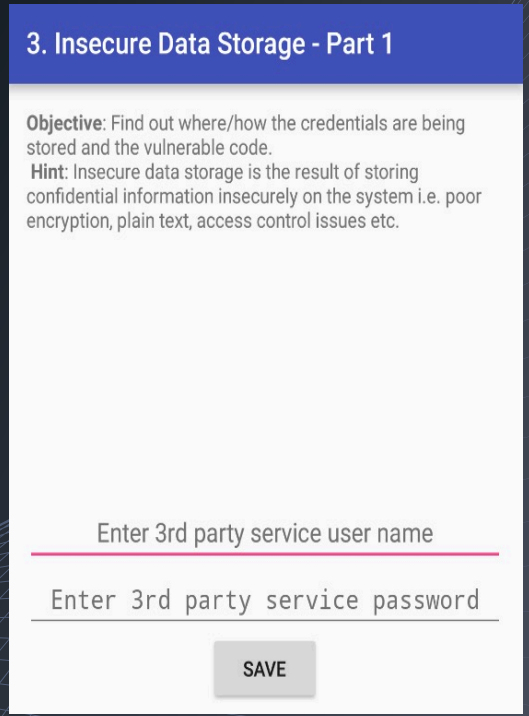
https://github.com/mwrlabs/drozer/releases/download/2.3.4/drozer-agent-2.3.4.apk

https://github.com/FSecureLABS/drozer/releases

M2 - Insecure Data Storage.

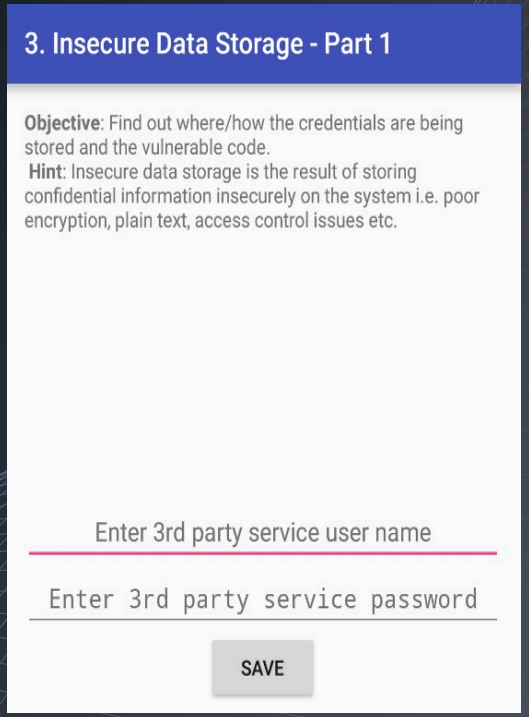
M2 - Insecure Data Storage

Kategori penyimpanan data Insecure mencakup kerentanan atau risiko terkait. pertama jika ada informasi sensitif yang disimpan oleh aplikasi dan kedua bagaimana informasi ini diamankan. perhatikan bahwa dari sudut pandang keamanan. aplikasi harus dirancang untuk tidak menyimpan informasi sensitif di sisi klien di tempat pertama. Kategori ini juga mencakup segala jenis kebocoran data yang tidak dimaksudkan. ini termasuk masalah yang terkait dengan memiliki informasi sensitif dalam log aplikasi. dalam memori aplikasi atau kode yang diuraikan. kategori juga mencakup menyimpan informasi sensitif pada media seperti SDCard. file aplikasi atau database SQLite lokal.



M2 - Insecure Data Storage

Terkadang developer menggunakan Shared preferences ini untuk menyimpan credentials seperti username, password, token, dll. Walaupun Shared preferences dideklarasi pada Private Mode yang artinya hanya bisa diakses oleh aplikasi tersebut, tetapi jika device tersebut telah di-root, maka tetap saja file tersebut bisa diakses oleh aplikasi lainnya.

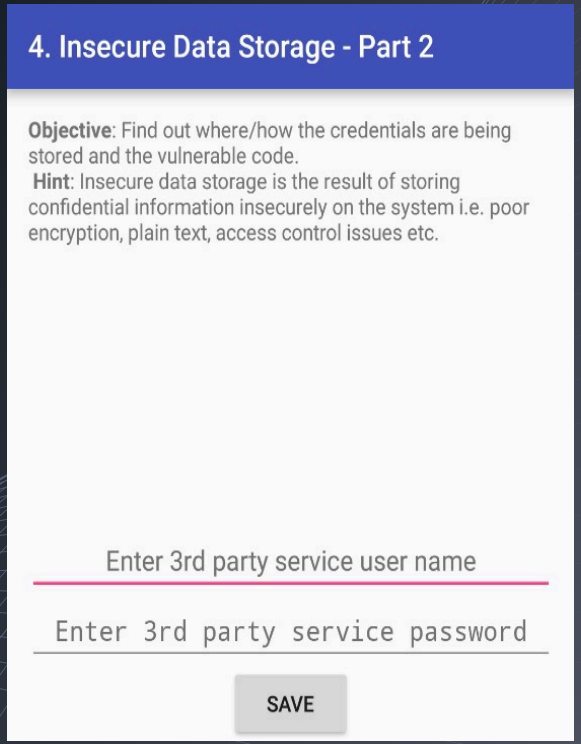


M2 - Insecure Data Storage

Aplikasi Android bisa menggunakan SQLite untuk menyimpan data secara lokal sebagai Relation Database Management System (RDBMS). Database tersebut biasanya berisi detail user, log transaksi, atau lainnya tergantung developer.

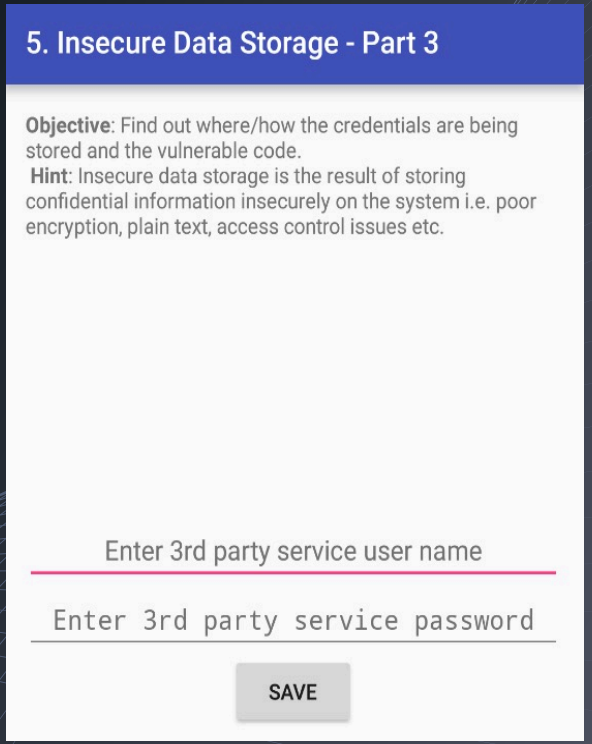
File database SQLite secara default disimpan di dalam direktori aplikasi sanbox, yaitu: /data/data/AppPackageName/databases/. Bisa jadi developer menyimpan file tersebut di luar direktori databases, tetapi masih di dalam direktori sanbox.

Untuk mengidentifikasi file SQLite Anda harus mencari beberapa ekstensi umum seperti .sqlite, .db, atau terkadang tanpa ekstensi. Untuk memastikannya kita bisa menggunakan perintah file pada shell.



M2 - Insecure Data Storage

Android menyediakan opsi untuk menyimpan file sementara (temporary file) secara lokal di dalam penyimpanan internal. Biasanya file ini digunakan untuk mencatat error, log, atau lainnya.
File temporary ini disimpan di dalam direktori aplikasi sandbox, yaitu /data/data/AppPackageName/.
Mungkin saja developer melakukan kesalahan dengan menyimpan data sensitif pada file tersebut.



M3 - Insecure Communication.

M3 - Insecure Communication

Mengamankan komunikasi antara klien dan server telah (dan akan) selalu menjadi yang terpenting dalam model ini untuk memberikan klien dengan implementasi yang aman yang menjamin keamanan data pribadi mereka. Metode yang digunakan untuk melindungi komunikasi. dikirim ke atau diterima dari server. sebagian besar didasarkan pada penggunaan implementasi infrastruktur kunci publik yang kuat yang. pada saat yang sama. menggunakan sertifikat untuk memastikan integritas dan kerahasiaan data dan komunikasi.

M3 - Insecure Communication

Mencegah lalu lintas
Mencegah lalu lintas untuk aplikasi seluler tidak mudah. ada beberapa kondisi penting yang harus dipenuhi agar berhasil melakukan serangan ini dan kompromi komunikasi antara aplikasi Android dan server backend yang terhubung. Kondisi-kondisi ini meliputi:

1. Kemampuan untuk menginstal sertifikat CA proksi pada perangkat.
2. Aplikasi mempercayai sertifikat yang dipasang pengguna.
3. Mengkonfigurasi workstation sebagai router.
4. Kemampuan untuk mengubah konfigurasi Wi-Fi perangkat.
5. Memotong pinning SSL (jika ada).

TERIMA KASIH