

# Vulnerability Assessment Report for diva app

Submitted by :- Sauda Momin

## 1. Minimum SDK Version is Too Low

## Description:

The application sets a very low minSdkVersion (15, Android 4.0.3), allowing the app to run on outdated Android versions with numerous security vulnerabilities.

The screenshot shows the AndroidManifest.xml file in an IDE. The manifest includes several permission declarations:

```
<uses-sdk android:minSdkVersion="15" android:targetSdkVersion="23"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.INTERNET"/>
```

It also lists numerous activities, each with its label and name:

```
<activity android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:name="com.jakhar.aseem.diva.MainActivity">
    <intent-filter>
        <action android:name="android.intent.action.MAIN"/>
        <category android:name="android.intent.category.LAUNCHER"/>
    </intent-filter>
</activity>
<activity android:label="@string/d1" android:name="jakhar.aseem.diva.LogActivity"/>
<activity android:label="@string/d2" android:name="jakhar.aseem.diva.HardcodeActivity"/>
<activity android:label="@string/d3" android:name="jakhar.aseem.diva.InsecureDataStorage1Activity"/>
<activity android:label="@string/d4" android:name="jakhar.aseem.diva.InsecureDataStorage2Activity"/>
<activity android:label="@string/d5" android:name="jakhar.aseem.diva.InsecureDataStorage3Activity"/>
<activity android:label="@string/d6" android:name="jakhar.aseem.diva.InsecureDataStorage4Activity"/>
<activity android:label="@string/d7" android:name="jakhar.aseem.diva.SQLInjectionActivity"/>
<activity android:label="@string/d8" android:name="jakhar.aseem.diva.InputValidation2URISchemeActivity"/>
<activity android:label="@string/d9" android:name="jakhar.aseem.diva.AccessControl1Activity"/>
<activity android:label="@string/apic_label" android:name="jakhar.aseem.diva.APIcredsActivity">
    <intent-filter>
        <action android:name="jakhar.aseem.diva.action.VIEW_CREDS"/>
        <category android:name="android.intent.category.DEFAULT"/>
    </intent-filter>

```

## **Root Cause:**

The android:minSdkVersion in the AndroidManifest.xml is set to an old API level, making the app compatible with legacy devices but exposing it to known security issues.

## **Impact:**

- Devices running old Android versions may lack modern security features and patches.
  - Increases risk of data leaks, privilege escalation, and exploitation of known OS vulnerabilities.

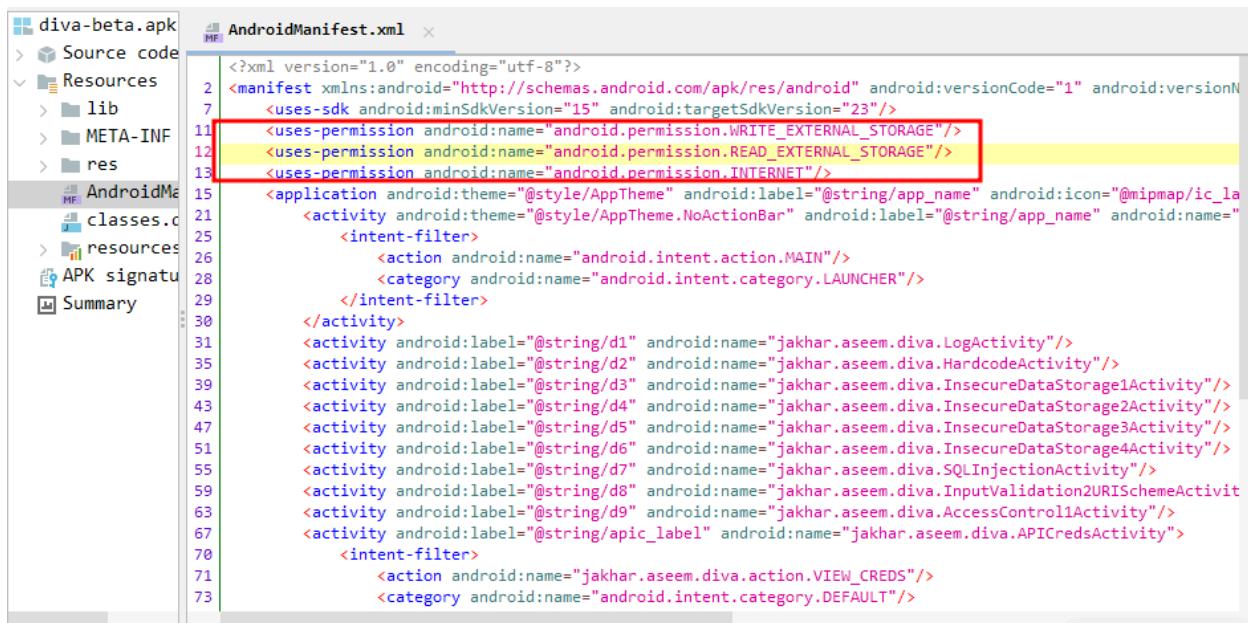
### **Mitigation:**

- Raise the minSdkVersion to 21 or higher (Android 5.0+) to ensure baseline security features.
  - Test the app for compatibility with the new minimum SDK to avoid runtime issues.

## 2. Sensitive Storage Permissions

### Description:

The application requests sensitive storage permissions (e.g., READ\_EXTERNAL\_STORAGE or WRITE\_EXTERNAL\_STORAGE) that provide full access to the device's storage.



The screenshot shows the AndroidManifest.xml file within an IDE. The manifest file contains several permission declarations, specifically lines 11, 12, and 13, which grant WRITE\_EXTERNAL\_STORAGE, READ\_EXTERNAL\_STORAGE, and INTERNET permissions respectively. These lines are highlighted with a red rectangular box. The manifest also defines an application with various activities and their corresponding labels and names.

```
<?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="jakhar.aseem.diva" android:minSdkVersion="15" android:targetSdkVersion="23">
    <uses-sdk android:minSdkVersion="15" android:targetSdkVersion="23"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <application android:theme="@style/AppTheme" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:allowBackup="true" android:label="Diva - Jakhar Aseem">
        <activity android:theme="@style/AppTheme.NoActionBar" android:label="@string/app_name" android:name="jakhar.aseem.diva.MainActivity" android:windowSoftInputMode="adjustPan">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/d1" android:name="jakhar.aseem.diva.LogActivity"/>
        <activity android:label="@string/d2" android:name="jakhar.aseem.diva.HardcodeActivity"/>
        <activity android:label="@string/d3" android:name="jakhar.aseem.diva.InsecureDataStorage1Activity"/>
        <activity android:label="@string/d4" android:name="jakhar.aseem.diva.InsecureDataStorage2Activity"/>
        <activity android:label="@string/d5" android:name="jakhar.aseem.diva.InsecureDataStorage3Activity"/>
        <activity android:label="@string/d6" android:name="jakhar.aseem.diva.InsecureDataStorage4Activity"/>
        <activity android:label="@string/d7" android:name="jakhar.aseem.diva.SQLInjectionActivity"/>
        <activity android:label="@string/d8" android:name="jakhar.aseem.diva.InputValidation2URISchemeActivity"/>
        <activity android:label="@string/d9" android:name="jakhar.aseem.diva.AccessControl1Activity"/>
        <activity android:label="@string/api_label" android:name="jakhar.aseem.diva.APIcredsActivity">
            <intent-filter>
                <action android:name="jakhar.aseem.diva.action.VIEW_CREDS"/>
                <category android:name="android.intent.category.DEFAULT"/>
            </intent-filter>
        </activity>
    </application>
</manifest>
```

### Root Cause:

The app declares storage permissions in the manifest, granting it access to all files on external storage, without restricting use to necessary files only.

### Impact:

- Any files stored on external storage, including user data or sensitive app files, could be exposed, modified, or deleted by other apps.
- Increases the risk of data leakage, tampering, and unauthorized access.

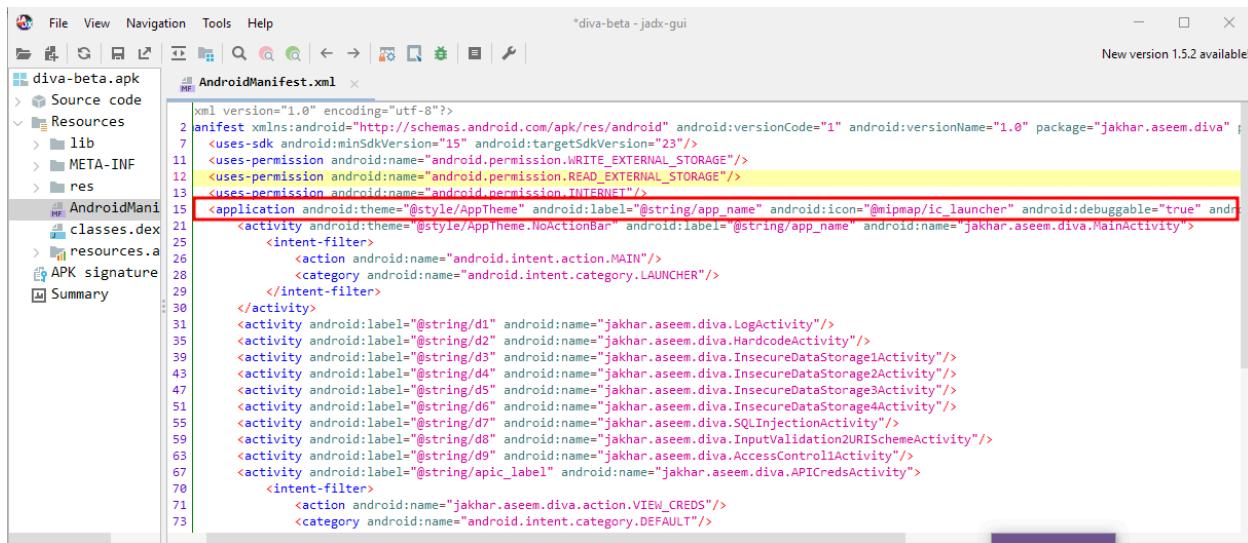
### Mitigation:

- Remove sensitive storage permissions if they are not required
- Use internal app storage or scoped storage APIs (Android 10/API 29+) for sensitive files.
- Restrict file access to app-private directories and avoid storing sensitive data in shared locations.

### 3. Debuggable App Enabled

#### Description:

The application is built with debugging enabled (`android:debuggable="true"`), allowing external tools to attach a debugger to the app.



The screenshot shows the JADX GUI interface with the file "AndroidManifest.xml" open. The code editor displays the XML manifest. A specific line of code, `<application android:theme="@style/AppTheme" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:debuggable="true" android:allowBackup="true" android:label="jakhar.aseem.diva>MainActivity">`, is highlighted with a red rectangle. The code editor has syntax highlighting for XML tags and strings. The top bar shows the title "diva-beta - jadx-gui" and a message "New version 1.5.2 available!".

```
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="jakhar.aseem.diva" android:allowBackup="true">
    <uses-sdk android:minSdkVersion="15" android:targetSdkVersion="23"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <application android:theme="@style/AppTheme" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:debuggable="true" android:allowBackup="true" android:label="jakhar.aseem.diva>MainActivity">
        <activity android:theme="@style/AppTheme.NoActionBar" android:label="@string/app_name" android:name="jakhar.aseem.diva.MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/d1" android:name="jakhar.aseem.diva.LogActivity"/>
        <activity android:label="@string/d2" android:name="jakhar.aseem.diva.HardcodeActivity"/>
        <activity android:label="@string/d3" android:name="jakhar.aseem.diva.InsecureDataStorage1Activity"/>
        <activity android:label="@string/d4" android:name="jakhar.aseem.diva.InsecureDataStorage2Activity"/>
        <activity android:label="@string/d5" android:name="jakhar.aseem.diva.InsecureDataStorage3Activity"/>
        <activity android:label="@string/d6" android:name="jakhar.aseem.diva.InsecureDataStorage4Activity"/>
        <activity android:label="@string/d7" android:name="jakhar.aseem.diva.SQLInjectionActivity"/>
        <activity android:label="@string/d8" android:name="jakhar.aseem.diva.InputValidation2URISchemeActivity"/>
        <activity android:label="@string/d9" android:name="jakhar.aseem.diva.AccessControl1Activity"/>
        <activity android:label="@string/apic_label" android:name="jakhar.aseem.diva.APICredsActivity">
            <intent-filter>
                <action android:name="jakhar.aseem.diva.action.VIEW_CREDS"/>
                <category android:name="android.intent.category.DEFAULT"/>
            </intent-filter>
        </activity>
    </application>

```

#### Root Cause:

The `android:debuggable` attribute in the `AndroidManifest.xml` is set to true, either manually or due to a debug build configuration, exposing the app in production.

#### Impact:

- Attackers can reverse engineer, inspect memory, or manipulate app behavior.
- Sensitive data such as credentials or encryption keys can be extracted.
- Increases the risk of security bypasses and unauthorized actions.

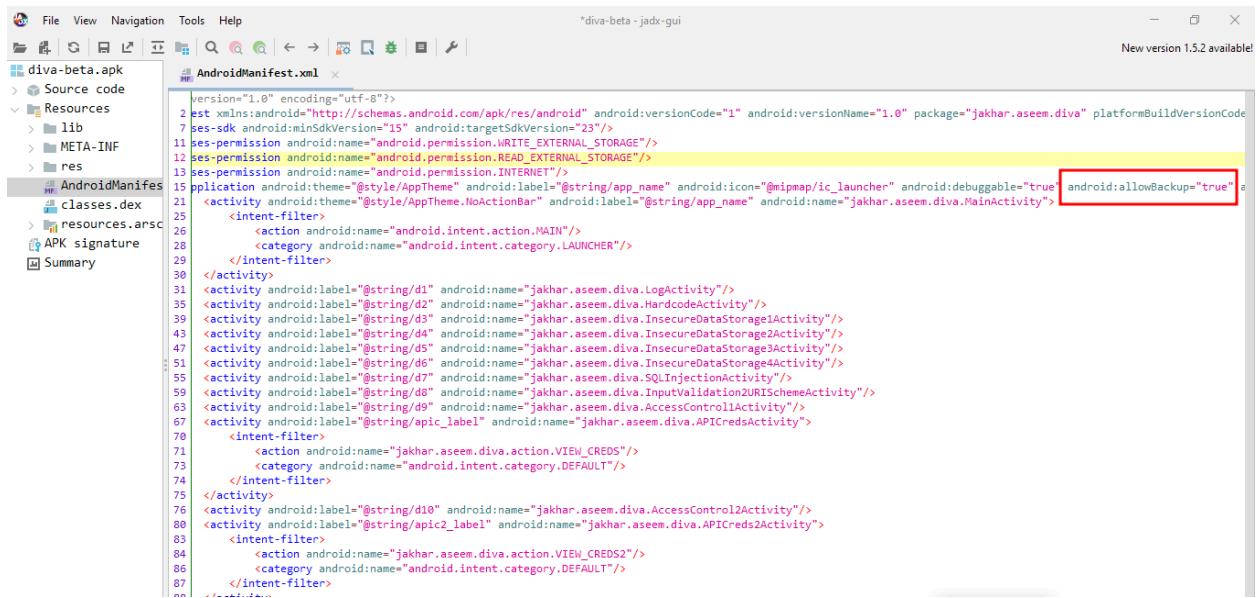
#### Mitigation:

- Set `android:debuggable="false"` for all release builds.
- Maintain separate debug and release build variants.
- Verify release APKs using `aapt dump badging <app.apk>` to confirm `debuggable` is disabled.

## 4. App Backup Allowed

### Description:

The application allows backup of its data (`android:allowBackup="true"`), enabling Android's backup mechanisms to store and restore app data.



```
File View Navigation Tools Help *diva-beta - jadx-gui
diva-beta.apk
Source code
Resources
lib
META-INF
res
AndroidManifest.xml
AndroidManifest.xml
version="1.0" encoding="utf-8"?>
<uses-sdk android:minSdkVersion="15" android:targetSdkVersion="23"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<application android:theme="@style/AppTheme" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:debuggable="true" android:allowBackup="true">
    <activity android:theme="@style/AppTheme.NoActionBar" android:label="@string/app_name" android:name="jakhar.aseem.diva.MainActivity">
        <intent-filter>
            <action android:name="android.intent.action.MAIN"/>
            <category android:name="android.intent.category.LAUNCHER"/>
        </intent-filter>
    </activity>
    <activity android:label="@string/d1" android:name="jakhar.aseem.diva.LogActivity"/>
    <activity android:label="@string/d2" android:name="jakhar.aseem.diva.HardcodeActivity"/>
    <activity android:label="@string/d3" android:name="jakhar.aseem.diva.InsecureDataStorage1Activity"/>
    <activity android:label="@string/d4" android:name="jakhar.aseem.diva.InsecureDataStorage2Activity"/>
    <activity android:label="@string/d5" android:name="jakhar.aseem.diva.InsecureDataStorage3Activity"/>
    <activity android:label="@string/d6" android:name="jakhar.aseem.diva.InsecureDataStorage4Activity"/>
    <activity android:label="@string/d7" android:name="jakhar.aseem.diva.SQLInjectionActivity"/>
    <activity android:label="@string/d8" android:name="jakhar.aseem.diva.InputValidationURISchemeActivity"/>
    <activity android:label="@string/d9" android:name="jakhar.aseem.diva.AccessControl1Activity"/>
    <activity android:label="@string/apic_label" android:name="jakhar.aseem.diva.APICredsActivity">
        <intent-filter>
            <action android:name="jakhar.aseem.diva.action.VIEW_CREDS"/>
            <category android:name="android.intent.category.DEFAULT"/>
        </intent-filter>
    </activity>
    <activity android:label="@string/d10" android:name="jakhar.aseem.diva.AccessControl2Activity"/>
    <activity android:label="@string/apic2_label" android:name="jakhar.aseem.diva.APICreds2Activity">
        <intent-filter>
            <action android:name="jakhar.aseem.diva.action.VIEW_CREDS2"/>
            <category android:name="android.intent.category.DEFAULT"/>
        </intent-filter>
    </activity>

```

### Root Cause:

The `android:allowBackup` attribute in the `AndroidManifest.xml` is set to true, allowing any user or attacker with device or backup access to copy app data.

### Impact:

- Sensitive data stored by the app can be extracted from backups.
- Increases risk of data leakage, privacy violations, and unauthorized access to user information.

### Mitigation:

- Set `android:allowBackup="false"` for release builds.
- Review sensitive data stored in the app and ensure it is protected even if backups are enabled.
- Use **encryption** for any critical stored data if backups are necessary.

## 5. Exported Content Provider

### Description:

The application's ContentProvider is exported (`android:exported="true"`), allowing other apps on the device to access or modify its data.



The screenshot shows the AndroidManifest.xml file within the AIDE IDE. The manifest contains multiple activity definitions and a provider definition. The provider is highlighted with a red rectangle, specifically the line where `android:exported="true"` is set. The provider is named `jakhar.aseem.diva.NotesProvider`.

```
15 <application android:theme="@style/AppTheme" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:debuggable="true" android:
16     <activity android:theme="@style/AppTheme.NoActionBar" android:label="@string/app_name" android:name="jakhar.aseem.diva.MainActivity">
17         <intent-filter>
18             <action android:name="android.intent.action.MAIN"/>
19             <category android:name="android.intent.category.LAUNCHER"/>
20         </intent-filter>
21     </activity>
22     <activity android:label="@string/d1" android:name="jakhar.aseem.diva.LogActivity"/>
23     <activity android:label="@string/d2" android:name="jakhar.aseem.diva.HardcodeActivity"/>
24     <activity android:label="@string/d3" android:name="jakhar.aseem.diva.InsecureDataStorage1Activity"/>
25     <activity android:label="@string/d4" android:name="jakhar.aseem.diva.InsecureDataStorage2Activity"/>
26     <activity android:label="@string/d5" android:name="jakhar.aseem.diva.InsecureDataStorage3Activity"/>
27     <activity android:label="@string/d6" android:name="jakhar.aseem.diva.InsecureDataStorage4Activity"/>
28     <activity android:label="@string/d7" android:name="jakhar.aseem.diva.SQLInjectionActivity"/>
29     <activity android:label="@string/d8" android:name="jakhar.aseem.diva.InputValidation2URISchemeActivity"/>
30     <activity android:label="@string/d9" android:name="jakhar.aseem.diva.AccessControl1Activity"/>
31     <activity android:label="@string/apic_label" android:name="jakhar.aseem.diva.APIcredsActivity">
32         <intent-filter>
33             <action android:name="jakhar.aseem.diva.action.VIEW_CREDS"/>
34             <category android:name="android.intent.category.DEFAULT"/>
35         </intent-filter>
36     </activity>
37     <activity android:label="@string/d10" android:name="jakhar.aseem.diva.AccessControl2Activity"/>
38     <activity android:label="@string/apic2_label" android:name="jakhar.aseem.diva.APIcreds2Activity">
39         <intent-filter>
40             <action android:name="jakhar.aseem.diva.action.VIEW_CREDS2"/>
41             <category android:name="android.intent.category.DEFAULT"/>
42         </intent-filter>
43     </activity>
44     <provider android:name="jakhar.aseem.diva.NotesProvider" android:enabled="true" android:exported="true" android:authorities="jakhar.aseem.diva.
45     <activity android:label="@string/d11" android:name="jakhar.aseem.diva.AccessControl3Activity"/>
46     <activity android:label="@string/d12" android:name="jakhar.aseem.diva.Hardcode2Activity"/>
47     <activity android:label="@string/phones" android:name="jakhar.aseem.diva.AccessControl3NotesActivity"/>
48     <activity android:label="@string/d13" android:name="jakhar.aseem.diva.InputValidation3Activity"/>
49 </application>
50 <test>
```

### Root Cause:

The `android:exported` attribute in the `AndroidManifest.xml` is set to true, and no permissions are enforced, making the provider publicly accessible.

### Impact:

- Other apps can read, modify, or delete data in the content provider.
- May lead to data leakage, unauthorized modifications, or app logic manipulation.

### Mitigation:

- Set `android:exported="false"` if the provider is not intended for external access.
- If external access is required, enforce **read/write permissions** using `android:readPermission` and `android:writePermission`.
- Validate all data received via content URIs before processing.

## 6. Unprotected Activity with Intent Filter

### Description:

The application exposes an activity via an intent filter without any protection, allowing other apps to send intents to it.

The screenshot shows the AndroidManifest.xml file in an IDE. The manifest contains several activities, each with an intent filter. Two specific intent filters are highlighted with a red rectangle. The first intent filter is associated with the activity labeled "jakhar.aseem.diva.APIcredsActivity". The second intent filter is associated with the activity labeled "jakhar.aseem.diva.APIcreds2Activity". Both intent filters contain an action with the name "jakhar.aseem.diva.action.VIEW\_CREDS" and a category "android.intent.category.DEFAULT".

```
<?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="jakhar.aseem.diva">
    <uses-sdk android:minSdkVersion="15" android:targetSdkVersion="23"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <application android:theme="@style/AppTheme" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:debuggable="true">
        <activity android:theme="@style/AppTheme.NoActionBar" android:label="@string/app_name" android:name="jakhar.aseem.diva.MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/d1" android:name="jakhar.aseem.diva.LogActivity"/>
        <activity android:label="@string/d2" android:name="jakhar.aseem.diva.HardcodeActivity"/>
        <activity android:label="@string/d3" android:name="jakhar.aseem.diva.InsecureDataStorage1Activity"/>
        <activity android:label="@string/d4" android:name="jakhar.aseem.diva.InsecureDataStorage2Activity"/>
        <activity android:label="@string/d5" android:name="jakhar.aseem.diva.InsecureDataStorage3Activity"/>
        <activity android:label="@string/d6" android:name="jakhar.aseem.diva.InsecureDataStorage4Activity"/>
        <activity android:label="@string/d7" android:name="jakhar.aseem.diva.SQLInjectionActivity"/>
        <activity android:label="@string/d8" android:name="jakhar.aseem.diva.InputValidation2URISchemeActivity"/>
        <activity android:label="@string/d9" android:name="jakhar.aseem.diva.AccessControl1Activity"/>
        <activity android:label="@string/apic_label" android:name="jakhar.aseem.diva.APIcredsActivity">
            <intent-filter>
                <action android:name="jakhar.aseem.diva.action.VIEW_CREDS"/>
                <category android:name="android.intent.category.DEFAULT"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/d10" android:name="jakhar.aseem.diva.AccessControl2Activity"/>
        <activity android:label="@string/apic2_label" android:name="jakhar.aseem.diva.APIcreds2Activity">
            <intent-filter>
                <action android:name="jakhar.aseem.diva.action.VIEW_CREDS2"/>
            </intent-filter>
        </activity>
    </application>
</manifest>
```

### Root Cause:

The activity is declared in the AndroidManifest.xml with an intent-filter but without any permission restrictions, making it publicly accessible.

### Impact:

- Malicious apps can launch the activity and potentially access sensitive data like API keys or user information.
- Increases the risk of data theft or unauthorized app behavior manipulation.

### Mitigation:

- Protect the activity by adding a custom permission in the manifest:  
    `android:permission="your.app.PERMISSION"`
- Only allow trusted apps or components to invoke the activity.
- Validate all inputs received via intents before processing.

