

# Android Security & Exploitation



**Aditya Gupta (@adi1391)**

**Founder, Attify (<http://attify.com>)**

**[adi@attify.com](mailto:adi@attify.com)**

Certifications : <http://securitytube-training.com>

Pentester Academy : <http://PentesterAcademy.com>

# Dropbox vulnerability

- Vulnerability in the content provider
- Not exported, but a big mistake by the developer
- Use dropbox.apk and try to find out the vulnerability
- Discovered by the Intrepidus Group

```
<?xml version="1.0" encoding="utf-8"?>
<manifest android:versionCode="1130" android:versionName="1.1.3" android:installLocation="auto" package="
com.dropbox.android"
  xmlns:android="http://schemas.android.com/apk/res/android">
  <uses-sdk android:minSdkVersion="3" android:targetSdkVersion="9" />
  <supports-screens android:anyDensity="true" android:smallScreens="true" android:normalScreens="true"
android:largeScreens="true" android:resizeable="true" android:xlargeScreens="true" />
  <application android:label="@string/app_name" android:icon="@drawable/icon" android:name=".
DropboxApplication" android:hardwareAccelerated="true">
    <meta-data android:name="android.app.default_searchable" android:value=".FileListActivity" />
    <provider android:name=".provider.DropboxProvider" android:authorities="com.dropbox.android.
Dropbox">
      <grant-uri-permission android:pathPrefix="/" />
    </provider>
    <service android:label="Dropbox Service" android:icon="@drawable/icon" android:name=".service.
DropboxService" android:enabled="true" android:exported="true" />
    <receiver android:label="Dropbox Network Status Receiver" android:icon="@drawable/icon" android:
name=".service.DropboxNetworkReceiver" android:enabled="false" android:exported="true">
      <intent-filter>
        <action android:name="android.net.conn.CONNECTIVITY_CHANGE" />
      </intent-filter>
    </receiver>
  </application>
</manifest>
```