Manifest Analysis

**High**

* **Debug Enable For App [android:debuggable=true]**

*Opção de Debugging está ativado, deixando vulnerável para tentativas de engenharia reversa, e um atacante conseguir informações sensíveis do aplicativo.*

* **Content Provider (jakhar.aseem.diva.NotesProvider) is not Protected [android:exported=true]**

*A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device*.

**Warning**

* **Application Data can be Backed up [android:allowBackup=true]**

*This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.*

* **Activity (jakhar.aseem.diva.APICredsActivity) is not Protected, An intent-filter exists.**

*An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.*

* **Activity (jakhar.aseem.diva.APICreds2Activity) is not Protected. An intent-filter exists.**

*An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.*

Code Analysis

**Warning**

**CWE:** CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

**OWASP Top 10:** M7: Client Code Quality

App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.

**Files**

jakhar/aseem/diva/InsecureDataStorage2Activity.java

jakhar/aseem/diva/NotesProvider.java

jakhar/aseem/diva/SQLInjectionActivity.java

**CWE:** CWE-276: Incorrect Default Permissions

**OWASP Top 10:** M2: Insecure Data Storage

**OWASP MASVS:** MSTG-STORAGE-2

App creates temp file. Sensitive information should never be written into a temp file.

**Files**

jakhar/aseem/diva/InsecureDataStorage3Activity.java

**CWE:** CWE-276: Incorrect Default Permissions

**OWASP Top 10:** M2: Insecure Data Storage

**OWASP MASVS:** MSTG-STORAGE-2

App can read/write to External Storage. Any App can read data written to External Storage.

**Files**

jakhar/aseem/diva/InsecureDataStorage4Activity.java

**Info**

**CWE:** CWE-532: Insertion of Sensitive Information into Log File

**OWASP MASVS:** MSTG-STORAGE-3

The App logs information. Sensitive information should never be logged.

**Files**

jakhar/aseem/diva/InsecureDataStorage2Activity.java

jakhar/aseem/diva/LogActivity.java

jakhar/aseem/diva/AccessControl1Activity.java

jakhar/aseem/diva/AccessControl2Activity.java

jakhar/aseem/diva/SQLInjectionActivity.java

jakhar/aseem/diva/InsecureDataStorage3Activity.java

jakhar/aseem/diva/InsecureDataStorage4Activity.java

Binary Analysis

lib/x86\_64/libdivajni.so

**High: 2**

**Warning: 1**

**Info:4**

**lib/armeabi-v7a/libdivajni.so**

**High: 2**

**Warning: 1**

**Info:4**

**lib/mips/libdivajni.so**

**High: 3**

**Warning: 1**

**Info: 3**

**lib/arm64-v8a/libdivajni.so**

**High: 3**

**Warning: 1**

**Info: 3**

**lib/x86/libdivajni.so**

**High: 1**

**Warning: 1**

**Info: 5**

**lib/mips64/libdivajni.so**

**High: 2**

**Warning: 1**

**Info: 3**

**lib/mips64/libdivajni.so**

**High: 3**

**Warning: 1**

**Info: 3**

Hardcoded Secrets

"pkey" : "notespin"