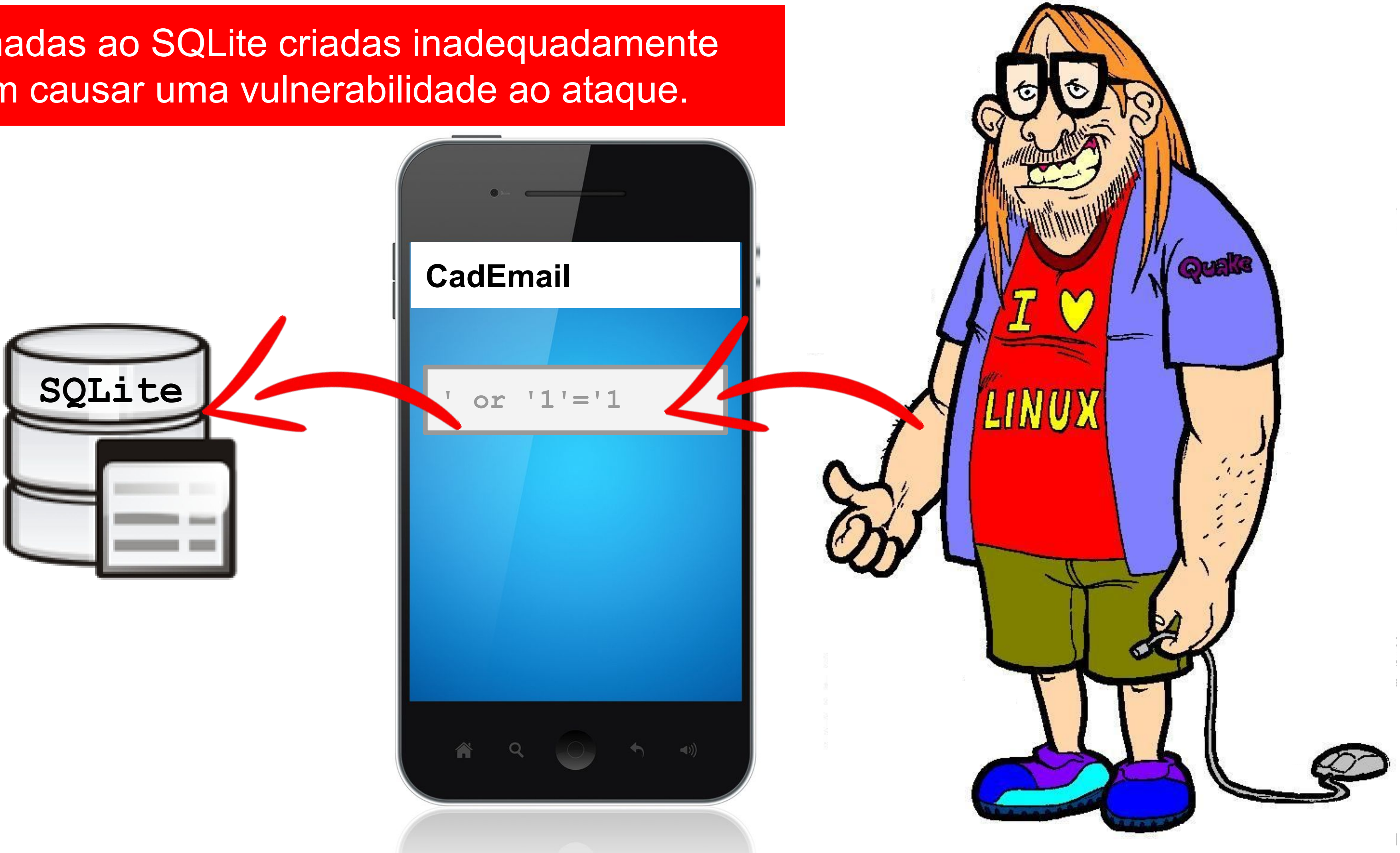
Desenvolvimento Mobile

SQL Injection (projeto ***CadEmail***)

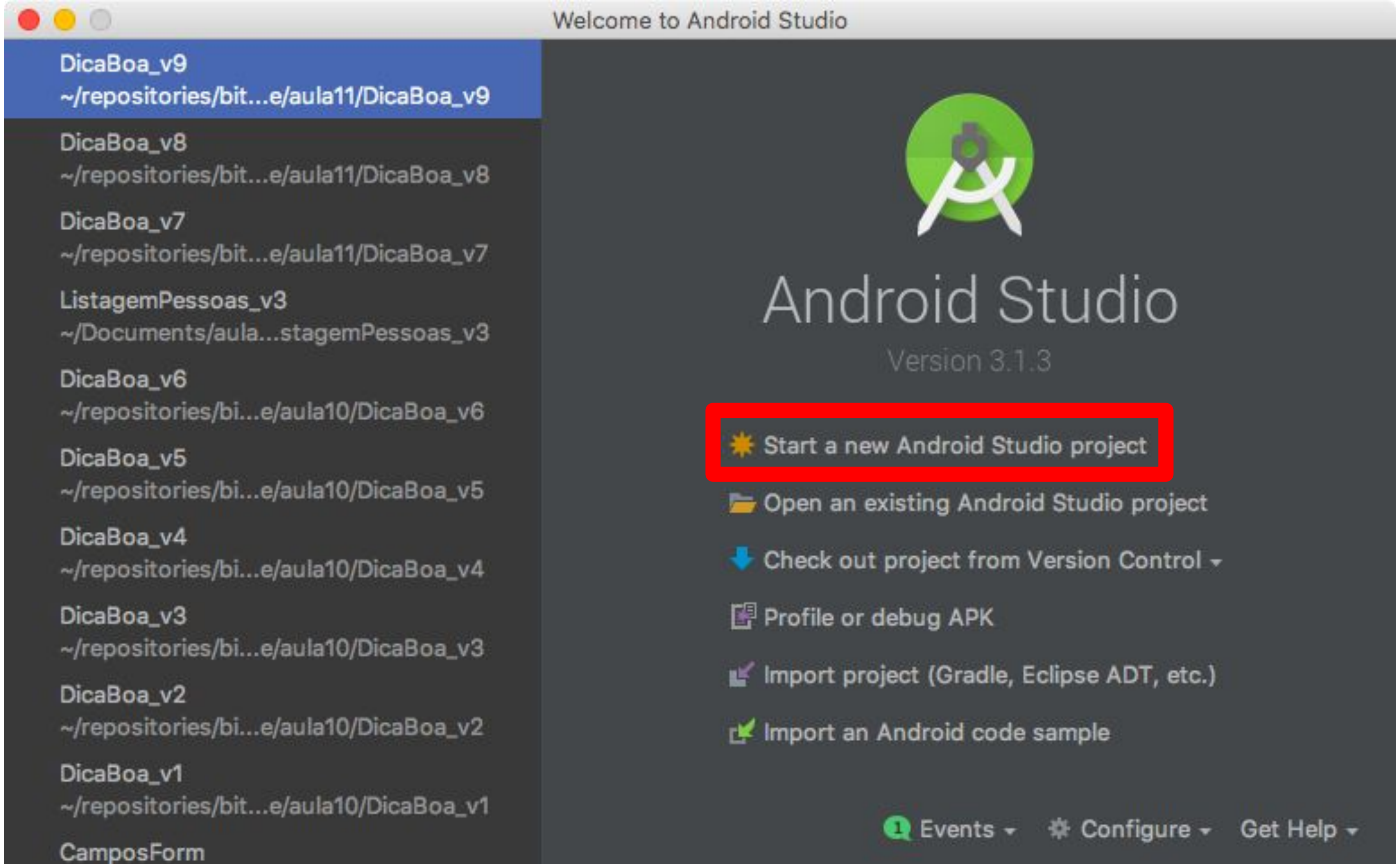
Exemplo de Ataque SQL Injection

OWASP: https://bit.ly/2jdWbXH

Chamadas ao SQLite criadas inadequadamente podem causar uma vulnerabilidade ao ataque.



Aplicação Exemplo



Welcome to Android Studio

DicaBoa_v9
~/repositories/bit...e/aula11/DicaBoa_v9

DicaBoa_v8
~/repositories/bit...e/aula11/DicaBoa_v8

DicaBoa_v7
~/repositories/bit...e/aula11/DicaBoa_v7

ListagemPessoas_v3
~/Documents/aula...stagemPessoas_v3

DicaBoa_v6
~/repositories/bi...e/aula10/DicaBoa_v6

DicaBoa_v5
~/repositories/bi...e/aula10/DicaBoa_v5

DicaBoa_v4
~/repositories/bi...e/aula10/DicaBoa_v4

DicaBoa_v3
~/repositories/bi...e/aula10/DicaBoa_v3

DicaBoa_v2
~/repositories/bi...e/aula10/DicaBoa_v2

DicaBoa_v1
~/repositories/bit...e/aula10/DicaBoa_v1

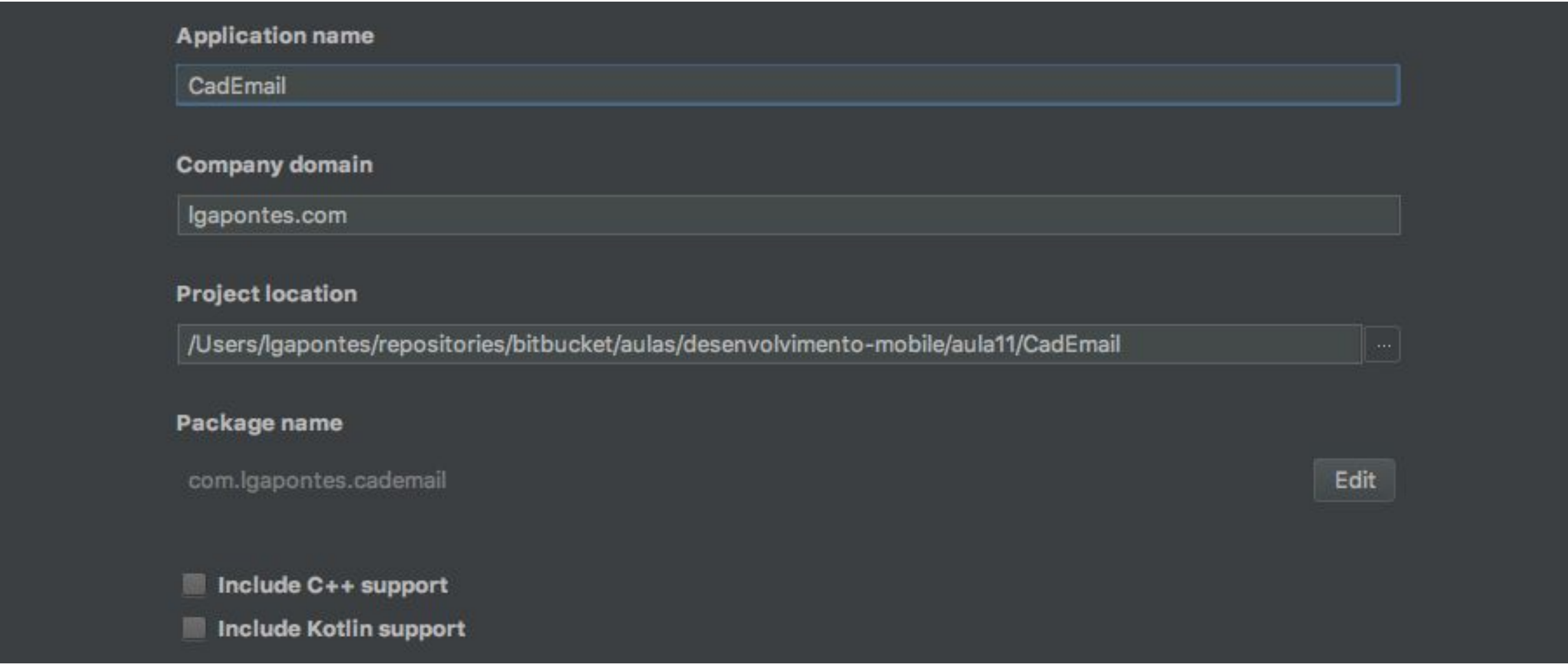
CamposForm

Android Studio

Version 3.1.3

Start a new Android Studio project
Open an existing Android Studio project
Check out project from Version Control ▾
Profile or debug APK
Import project (Gradle, Eclipse ADT, etc.)
Import an Android code sample
1 Events ▾
Configure ▾
Get Help ▾

Aplicação Exemplo



Application name

CadEmail

Company domain

lgapontes.com

Project location

/Users/lgapontes/repositories/bitbucket/aulas/desenvolvimento-mobile/aula11/CadEmail

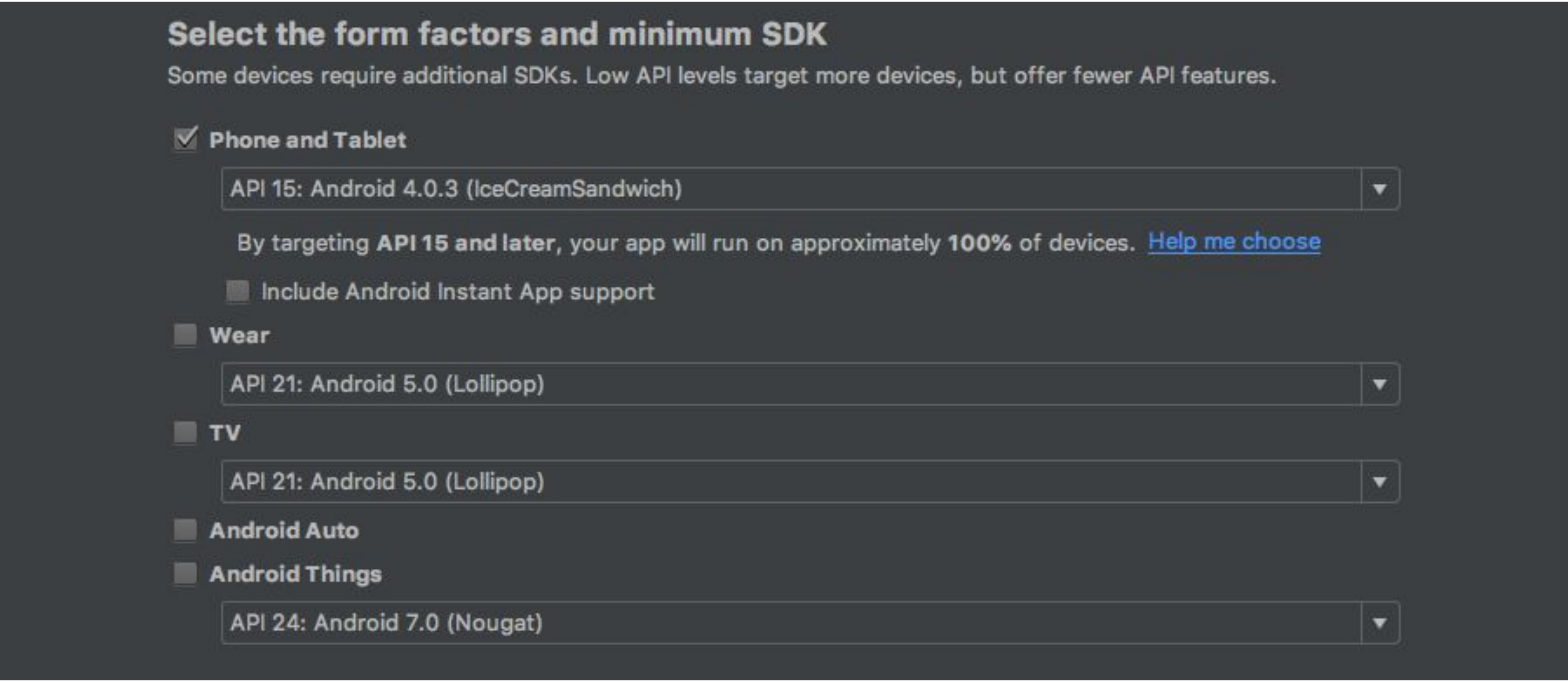
Package name

com.lgapontes.cademail

□ Include C++ support

□ Include Kotlin support

Aplicação Exemplo



Select the form factors and minimum SDK

Some devices require additional SDKs. Low API levels target more devices, but offer fewer API features.

☑ **Phone and Tablet**

API 15: Android 4.0.3 (IceCreamSandwich) ▼

By targeting **API 15 and later**, your app will run on approximately **100%** of devices. Help me choose

□ Include Android Instant App support

□ **Wear**

API 21: Android 5.0 (Lollipop) ▼

□ **TV**

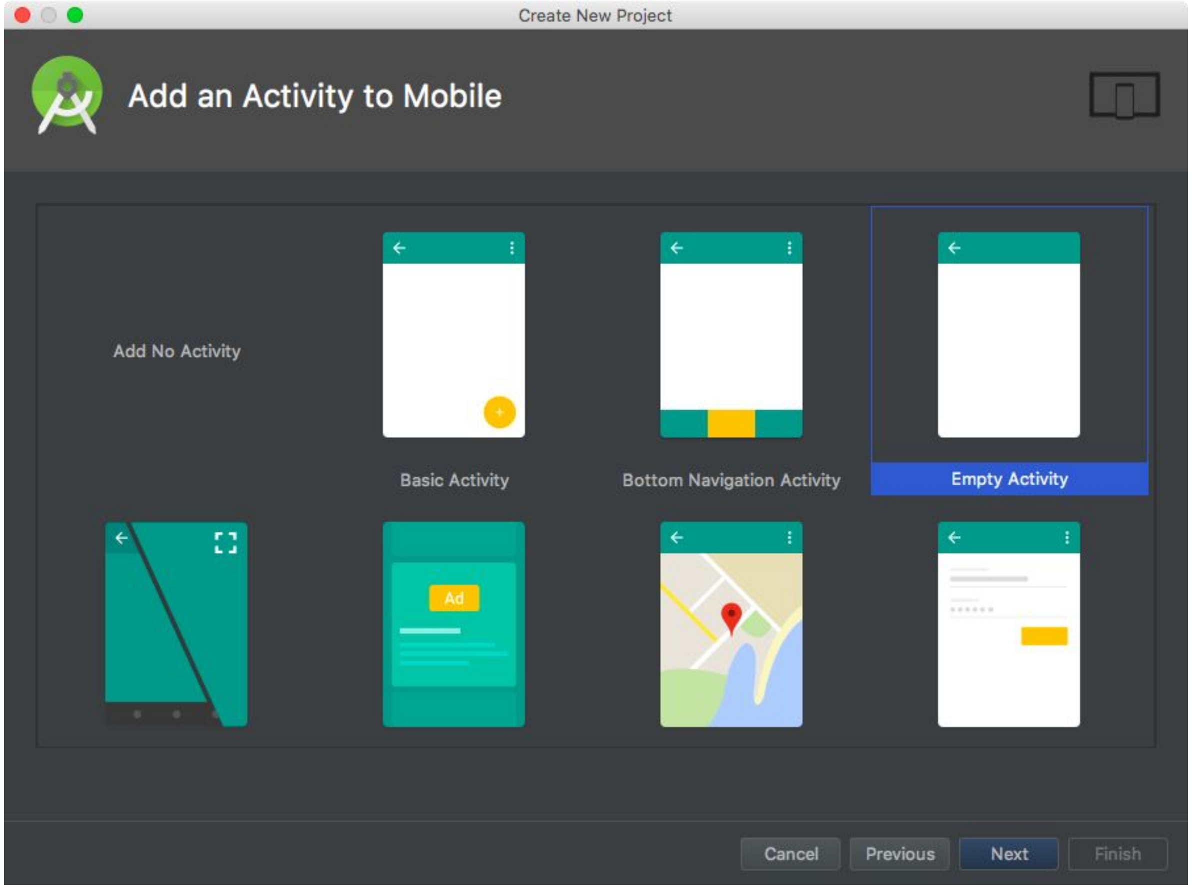
API 21: Android 5.0 (Lollipop) ▼

□ **Android Auto**

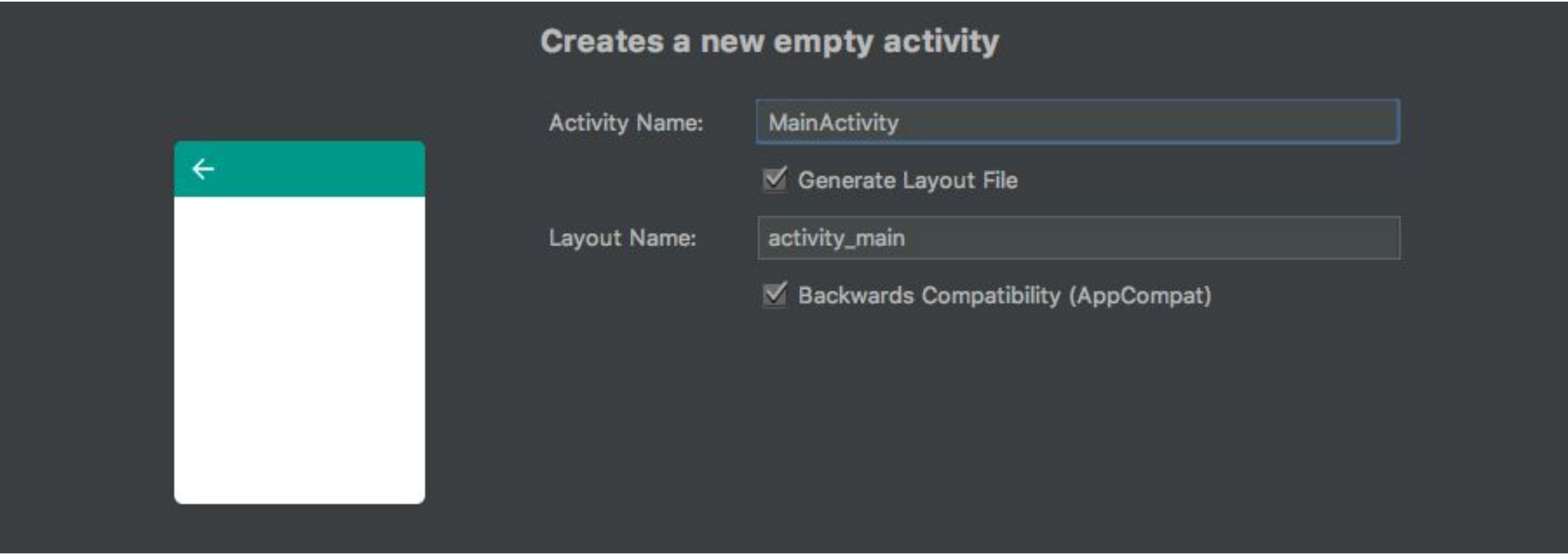
□ **Android Things**

API 24: Android 7.0 (Nougat) ▼

Aplicação Exemplo



Aplicação Exemplo



Creates a new empty activity

Activity Name: MainActivity

☑ Generate Layout File

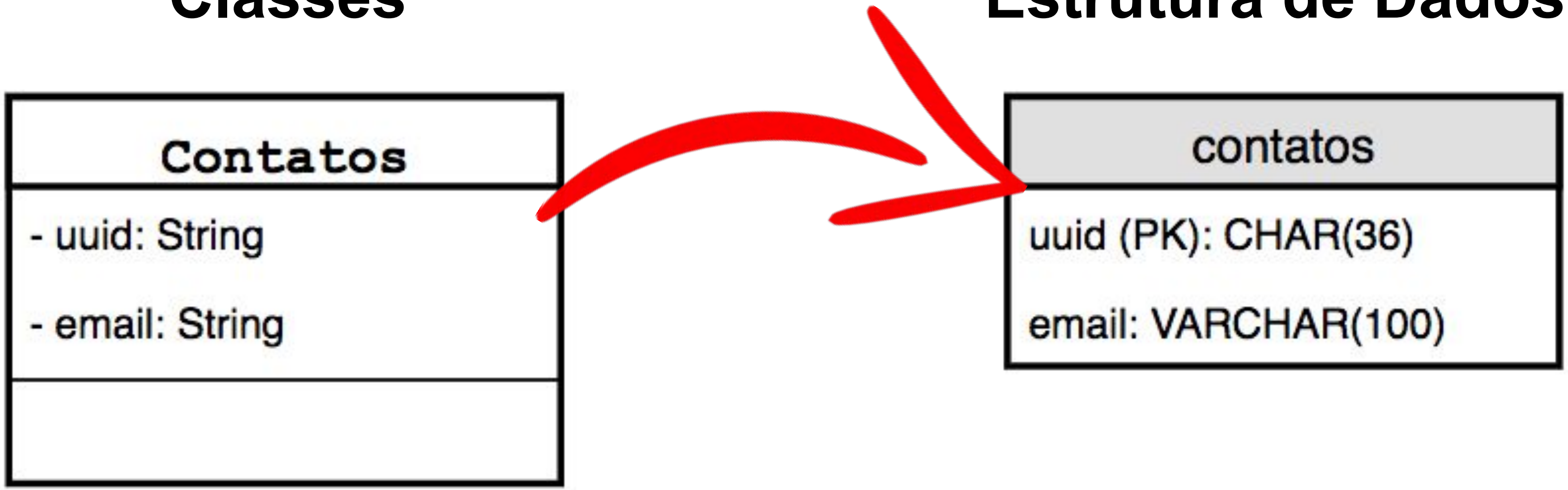
Layout Name: activity_main

☑ Backwards Compatibility (AppCompat)

Aplicação Exemplo

Diagrama de Classes

Diagrama de Estrutura de Dados



Contatos

- uuid: String

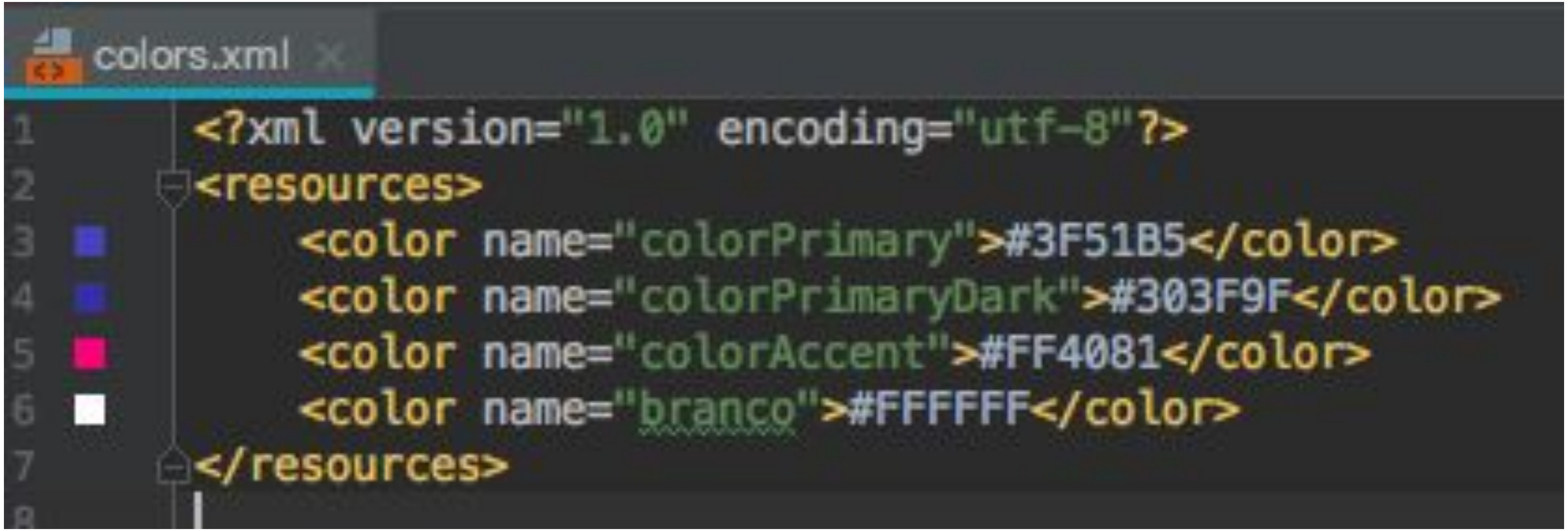
- email: String

contatos

uuid (PK): CHAR(36)

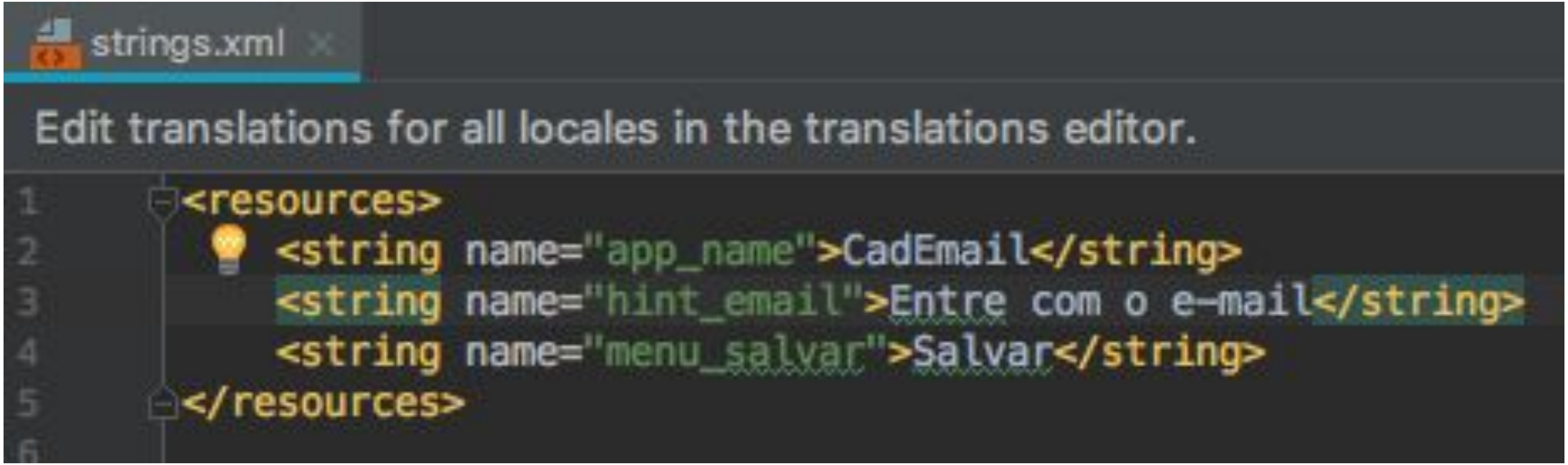
email: VARCHAR(100)

Aplicação Exemplo



```xml
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <color name="colorPrimary">#3F51B5</color>
    <color name="colorPrimaryDark">#303F9F</color>
    <color name="colorAccent">#FF4081</color>
    <color name="branco">#FFFFFF</color>
</resources>
```

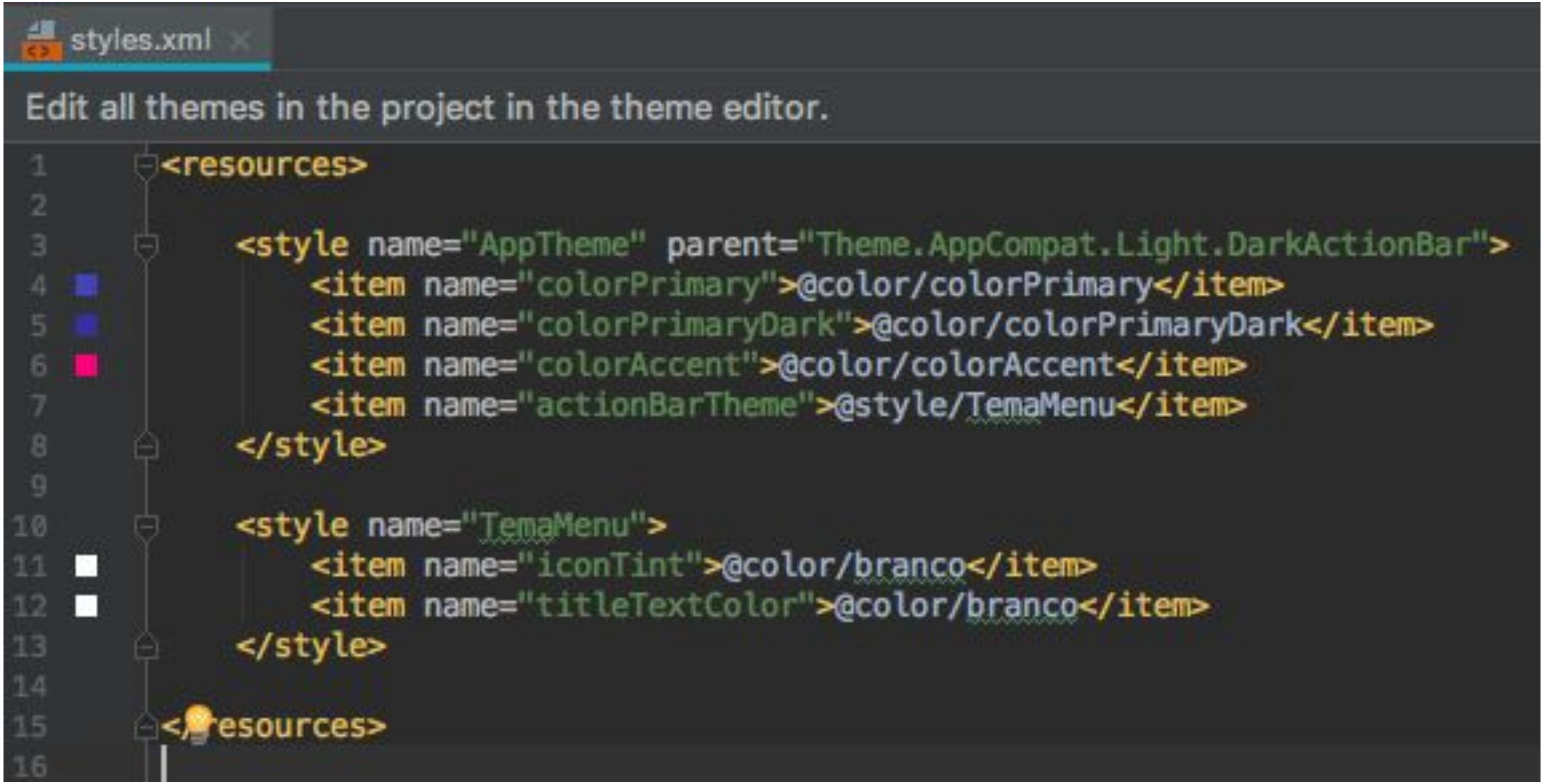
Aplicação Exemplo



Edit translations for all locales in the translations editor.

```
<resources>
    <string name="app_name">CadEmail</string>
    <string name="hint_email">Entre com o e-mail</string>
    <string name="menu_salvar">Salvar</string>
</resources>
```

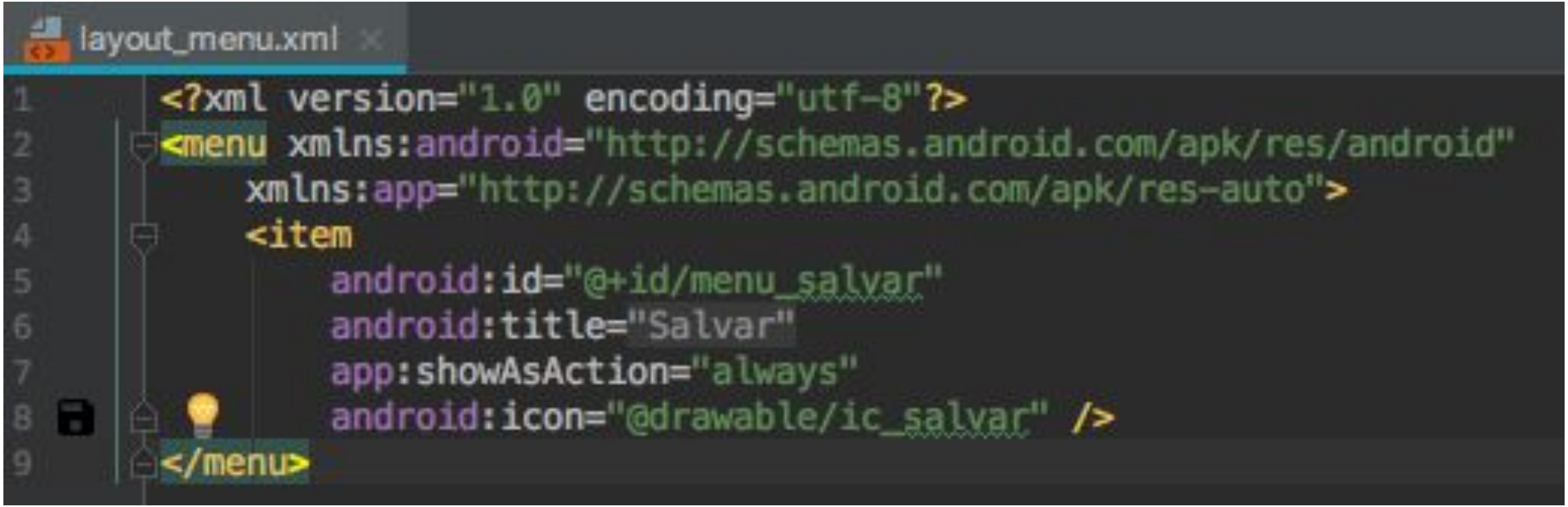
Aplicação Exemplo



Edit all themes in the project in the theme editor.

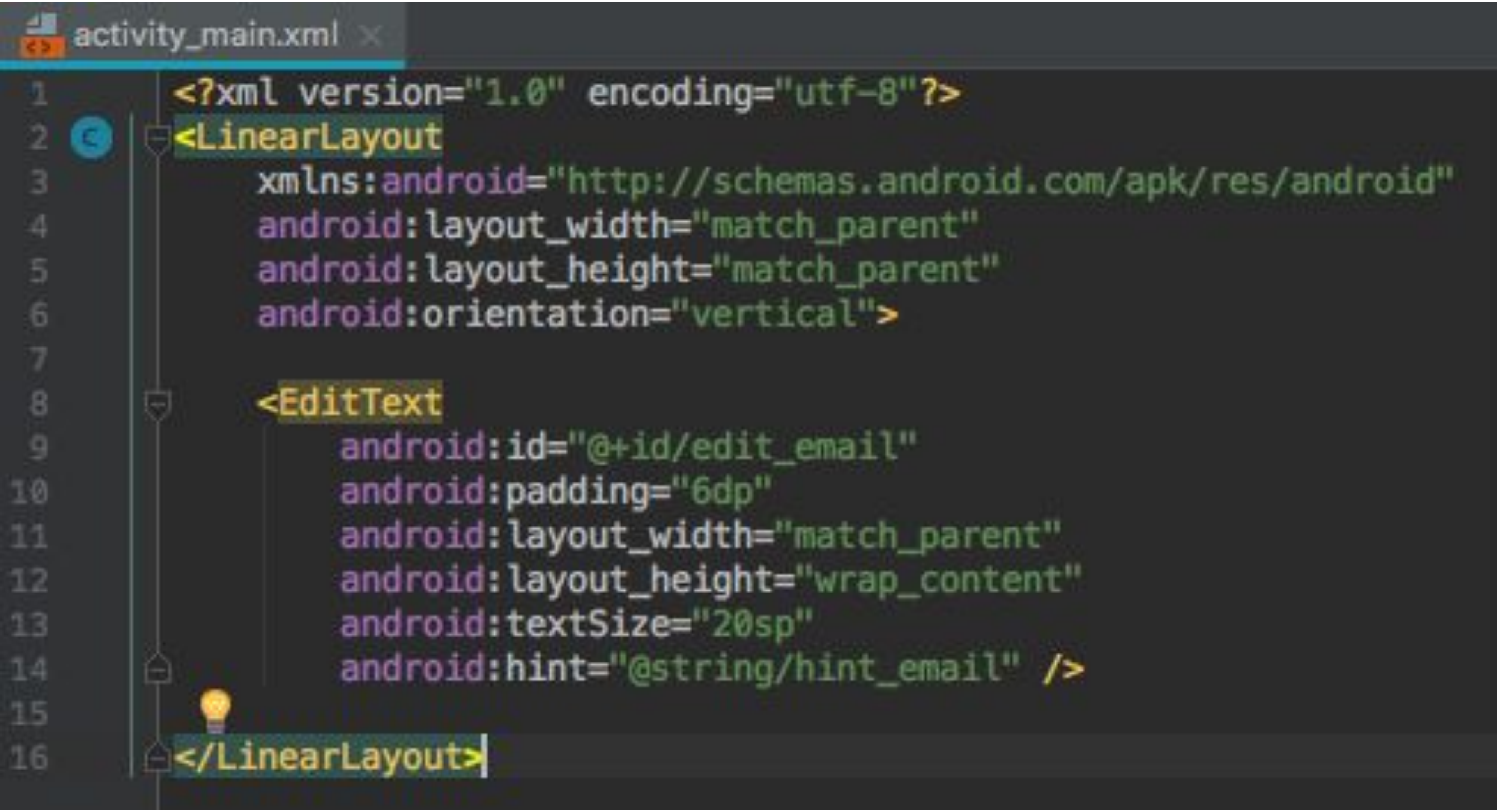
```xml
<resources>

    <style name="AppTheme" parent="Theme.AppCompat.Light.DarkActionBar">
        <item name="colorPrimary">@color/colorPrimary</item>
        <item name="colorPrimaryDark">@color/colorPrimaryDark</item>
        <item name="colorAccent">@color/colorAccent</item>
        <item name="actionBarTheme">@style/TemaMenu</item>
    </style>

    <style name="TemaMenu">
        <item name="iconTint">@color/branco</item>
        <item name="titleTextColor">@color/branco</item>
    </style>

</resources>
```

Aplicação Exemplo



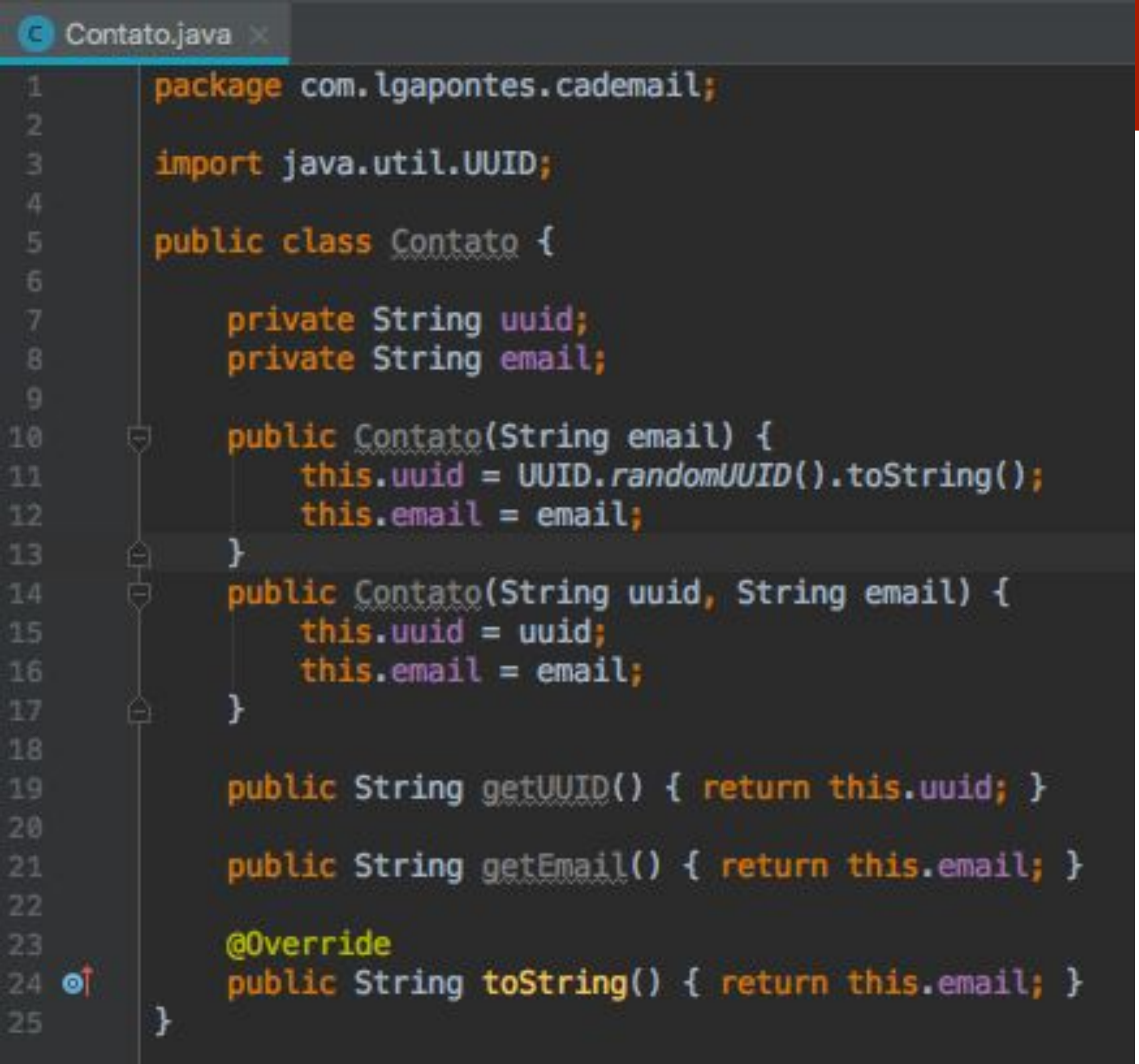
layout_menu.xml

```
<?xml version="1.0" encoding="utf-8"?>
<menu xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:app="http://schemas.android.com/apk/res-auto">
    <item
        android:id="@+id/menu_salvar"
        android:title="Salvar"
        app:showAsAction="always"
        android:icon="@drawable/ic_salvar" />
</menu>
```



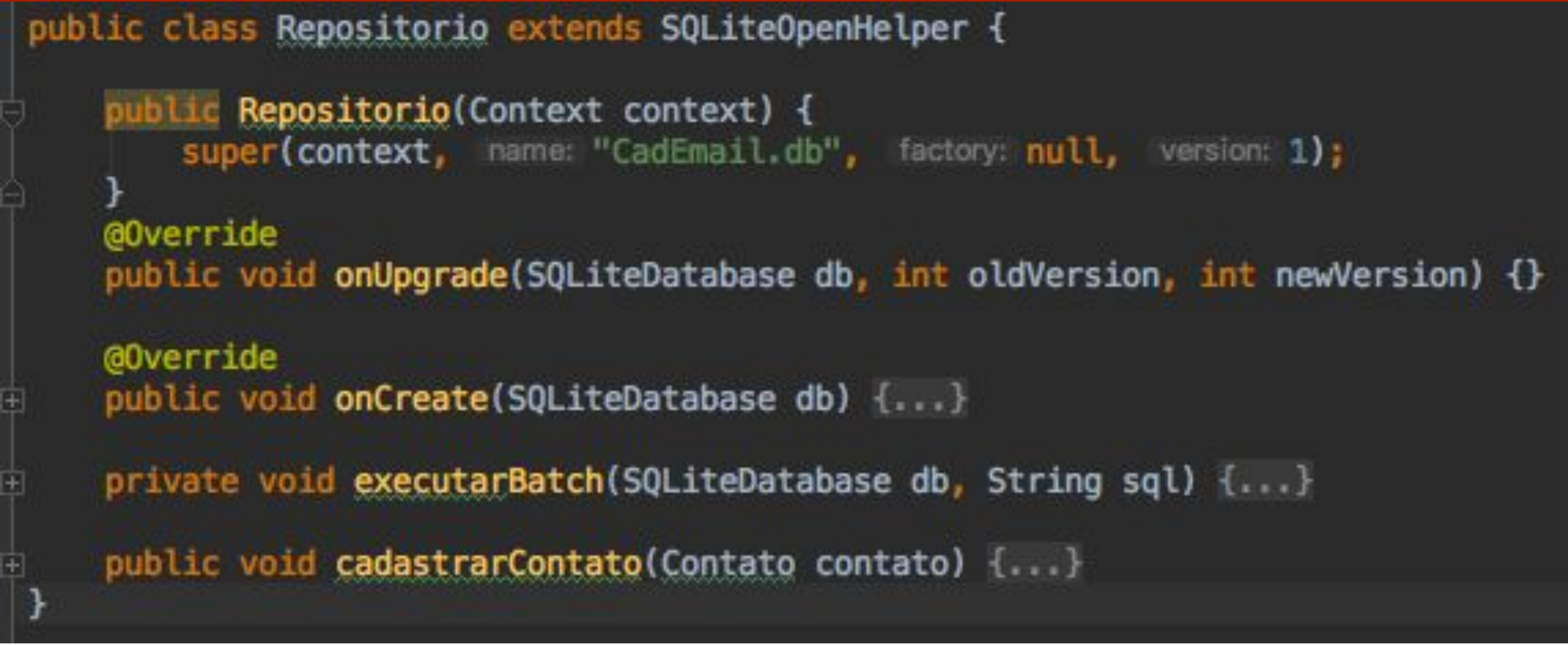
```xml
<?xml version="1.0" encoding="utf-8"?>
<LinearLayout
    xmlns:android="http://schemas.android.com/apk/res/android"
    android:layout_width="match_parent"
    android:layout_height="match_parent"
    android:orientation="vertical">

    <EditText
        android:id="@+id/edit_email"
        android:padding="6dp"
        android:layout_width="match_parent"
        android:layout_height="wrap_content"
        android:textSize="20sp"
        android:hint="@string/hint_email" />

</LinearLayout>
```

Aplicação Exemplo



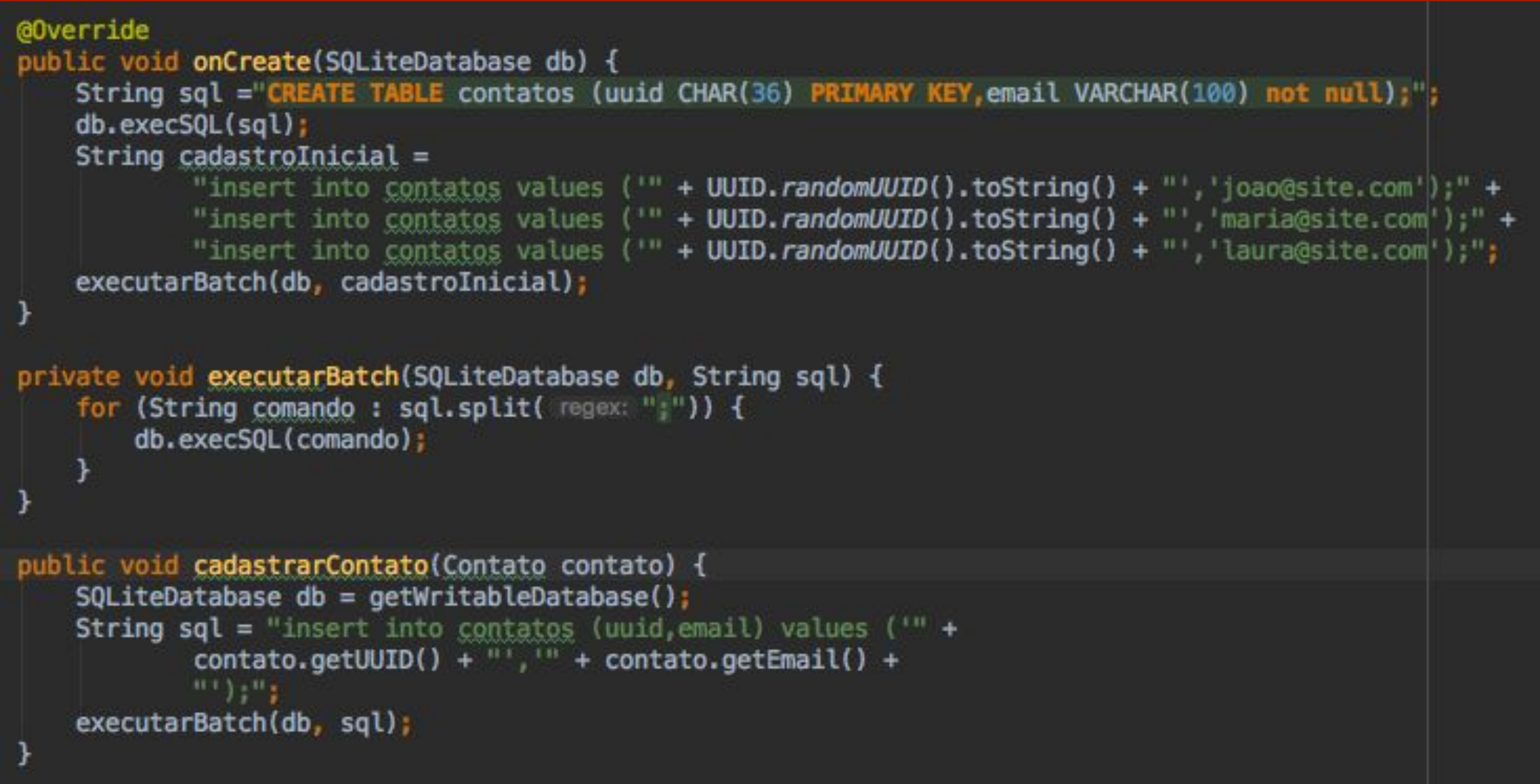
```java
package com.lgapontes.cademail;

import java.util.UUID;

public class Contato {

    private String uuid;
    private String email;

    public Contato(String email) {
        this.uuid = UUID.randomUUID().toString();
        this.email = email;
    }
    public Contato(String uuid, String email) {
        this.uuid = uuid;
        this.email = email;
    }

    public String getUUID() { return this.uuid; }

    public String getEmail() { return this.email; }

    @Override
    public String toString() { return this.email; }
}
```

Classe de Repositorio.java



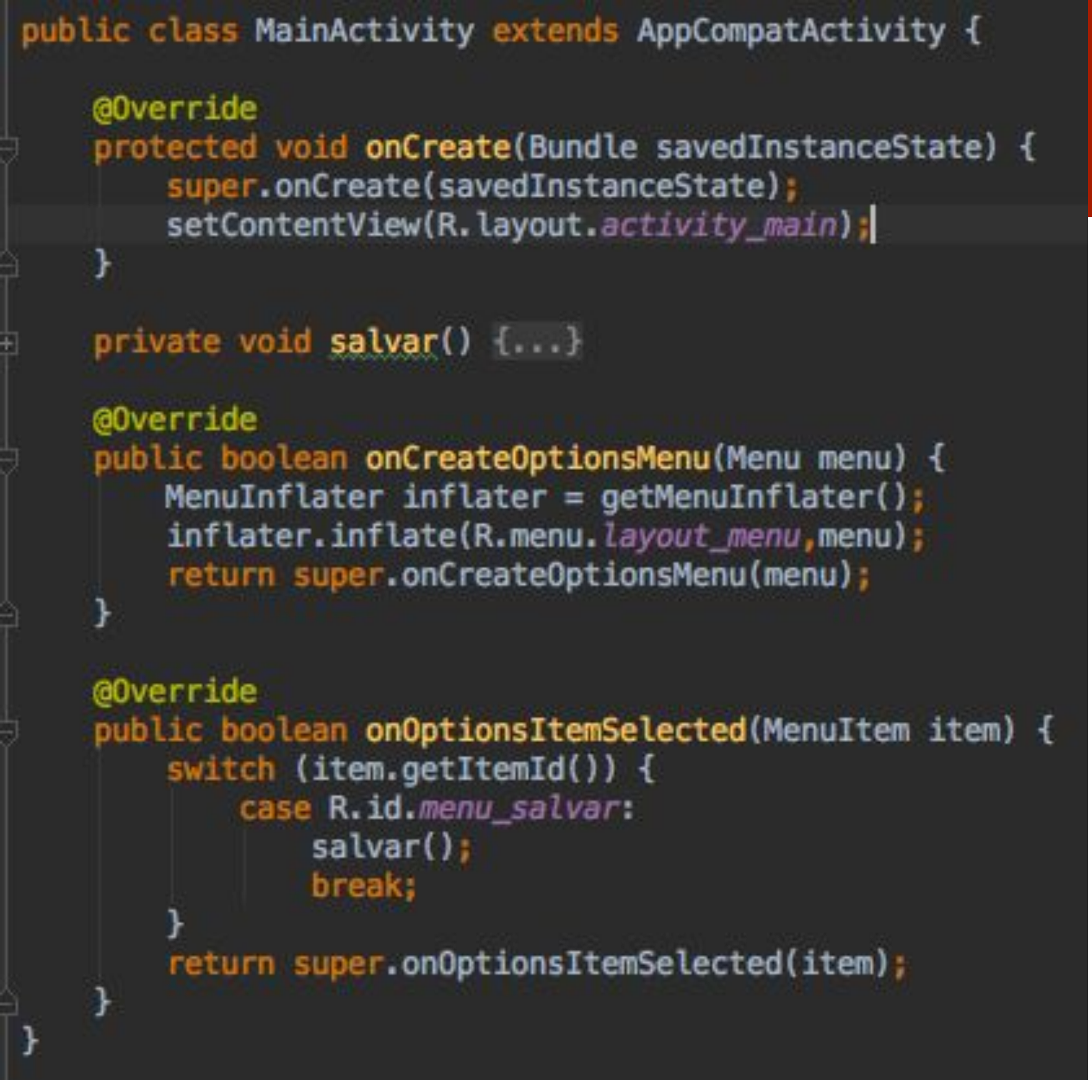
```
public class Repositorio extends SQLiteOpenHelper {

    public Repositorio(Context context) {
        super(context, name: "CadEmail.db", factory: null, version: 1);
    }
    @Override
    public void onUpgrade(SQLiteDatabase db, int oldVersion, int newVersion) {}

    @Override
    public void onCreate(SQLiteDatabase db) {...}

    private void executarBatch(SQLiteDatabase db, String sql) {...}

    public void cadastrarContato(Contato contato) {...}
}
```

Classe de Repositorio.java



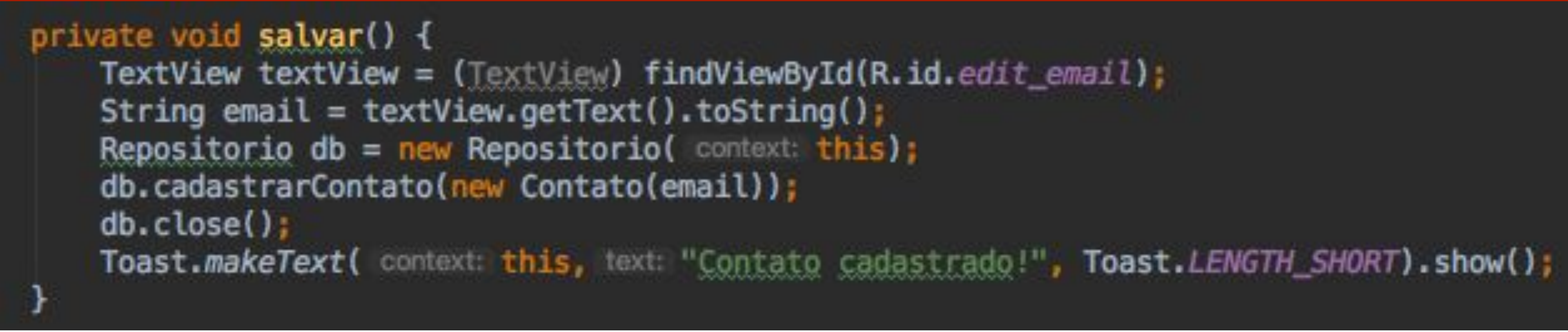
```
@Override
public void onCreate(SQLiteDatabase db) {
    String sql ="CREATE TABLE contatos (uuid CHAR(36) PRIMARY KEY,email VARCHAR(100) not null);";
    db.execSQL(sql);
    String cadastroInicial =
            "insert into contatos values ('" + UUID.randomUUID().toString() + "','joao@site.com');" +
            "insert into contatos values ('" + UUID.randomUUID().toString() + "','maria@site.com');" +
            "insert into contatos values ('" + UUID.randomUUID().toString() + "','laura@site.com');";
    executarBatch(db, cadastroInicial);
}

private void executarBatch(SQLiteDatabase db, String sql) {
    for (String comando : sql.split( regex: ";")) {
        db.execSQL(comando);
    }
}

public void cadastrarContato(Contato contato) {
    SQLiteDatabase db = getWritableDatabase();
    String sql = "insert into contatos (uuid,email) values ('" +
            contato.getUUID() + "','" + contato.getEmail() +
            "');";
    executarBatch(db, sql);
}
```

Classe de `MainActivity.java`

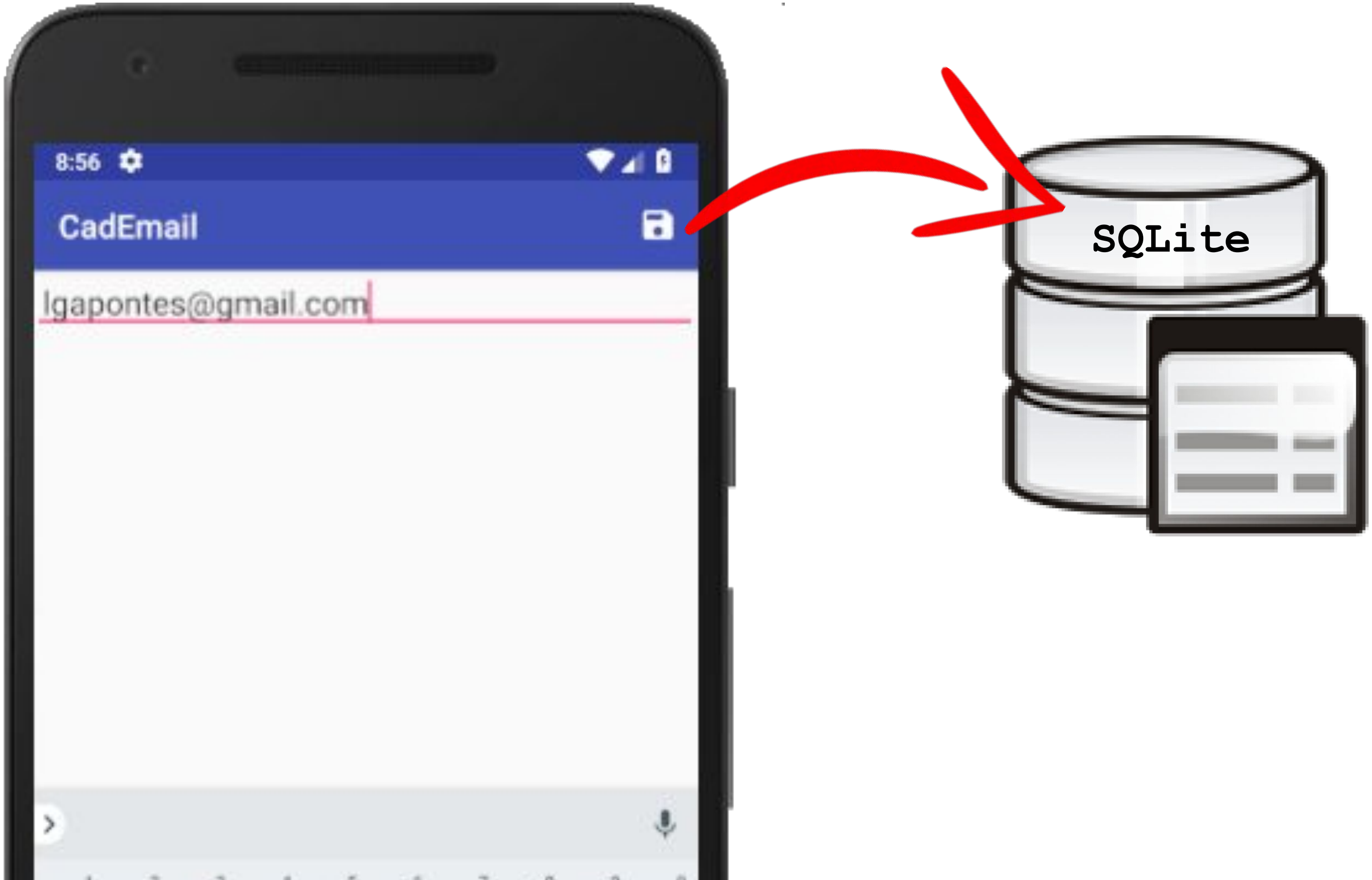


```java
public class MainActivity extends AppCompatActivity {

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
    }

    private void salvar() {...}

    @Override
    public boolean onCreateOptionsMenu(Menu menu) {
        MenuInflater inflater = getMenuInflater();
        inflater.inflate(R.menu.layout_menu,menu);
        return super.onCreateOptionsMenu(menu);
    }

    @Override
    public boolean onOptionsItemSelected(MenuItem item) {
        switch (item.getItemId()) {
            case R.id.menu_salvar:
                salvar();
                break;
        }
        return super.onOptionsItemSelected(item);
    }
}
```

Classe de `MainActivity.java`

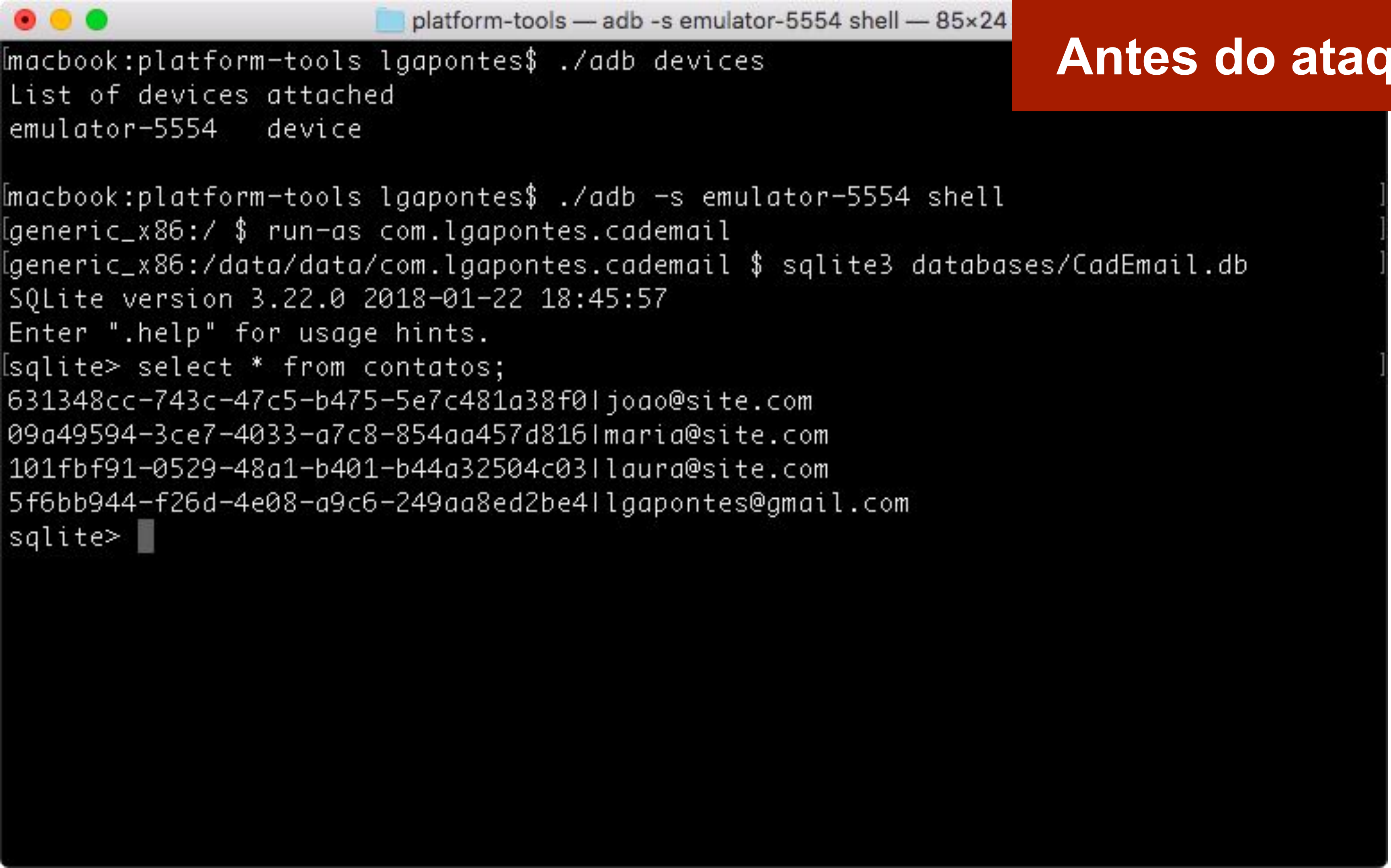


```java
private void salvar() {
    TextView textView = (TextView) findViewById(R.id.edit_email);
    String email = textView.getText().toString();
    Repositorio db = new Repositorio( context: this);
    db.cadastrarContato(new Contato(email));
    db.close();
    Toast.makeText( context: this, text: "Contato cadastrado!", Toast.LENGTH_SHORT).show();
}
```

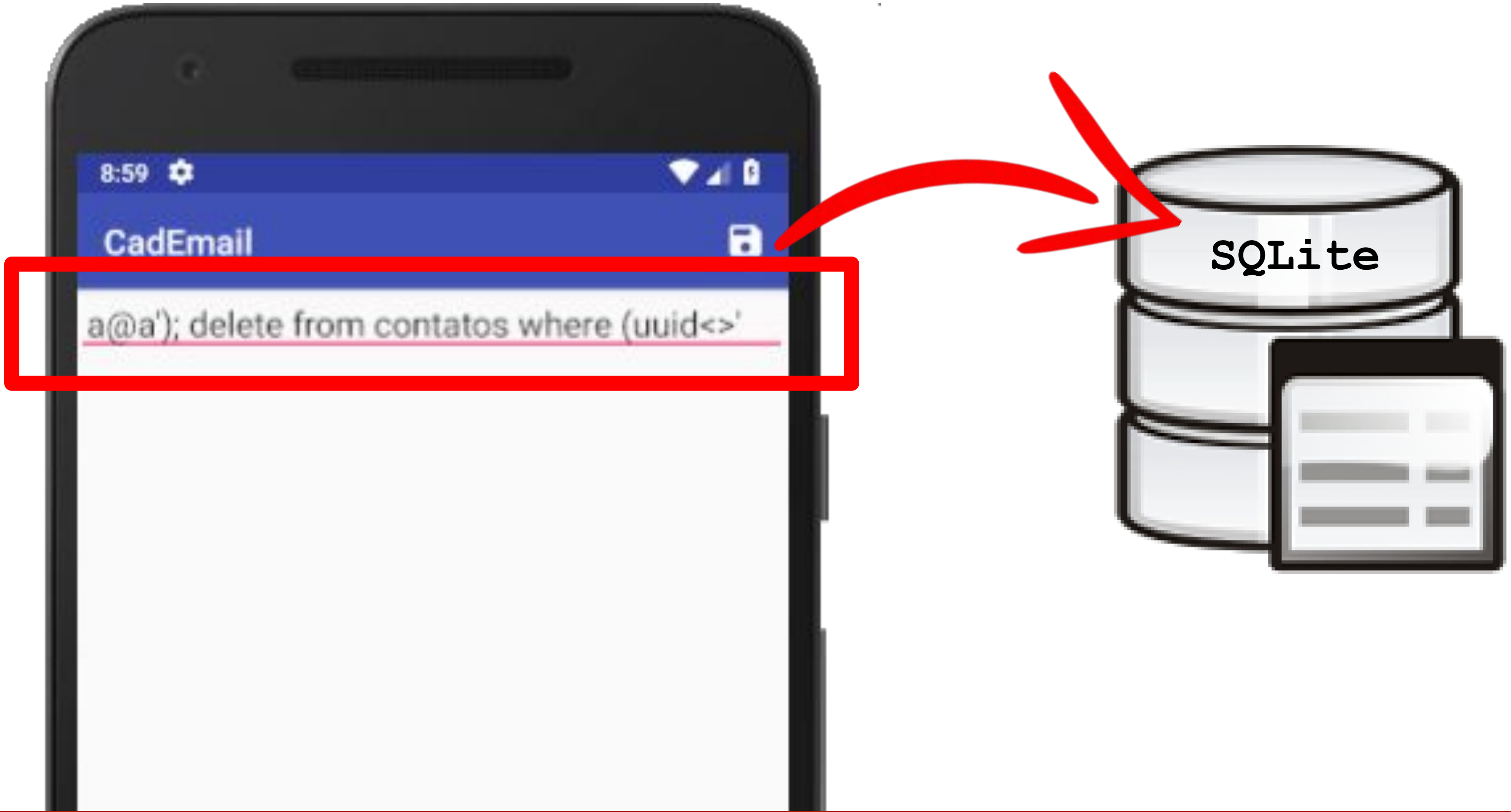


lgapontes@gmail.com

Antes do ataque...



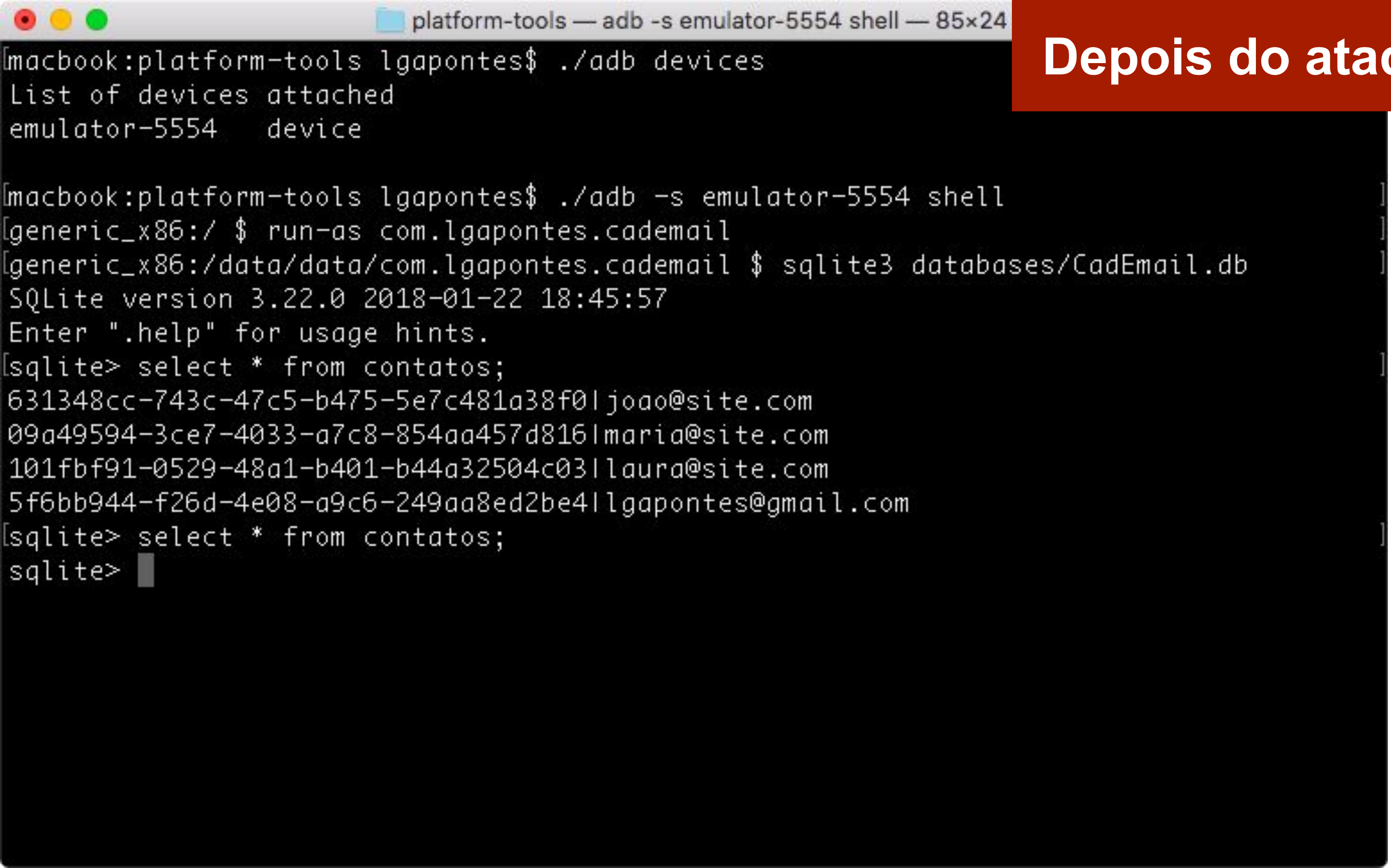
```
macbook:platform-tools lgapontes$ ./adb devices
List of devices attached
emulator-5554   device

macbook:platform-tools lgapontes$ ./adb -s emulator-5554 shell
generic_x86:/ $ run-as com.lgapontes.cademail
generic_x86:/data/data/com.lgapontes.cademail $ sqlite3 databases/CadEmail.db
SQLite version 3.22.0 2018-01-22 18:45:57
Enter ".help" for usage hints.
sqlite> select * from contatos;
631348cc-743c-47c5-b475-5e7c481a38f0|joao@site.com
09a49594-3ce7-4033-a7c8-854aa457d816|maria@site.com
101fbf91-0529-48a1-b401-b44a32504c03|laura@site.com
5f6bb944-f26d-4e08-a9c6-249aa8ed2be4|lgapontes@gmail.com
sqlite> 
```



a@a'); delete from contatos where (uuid<>'

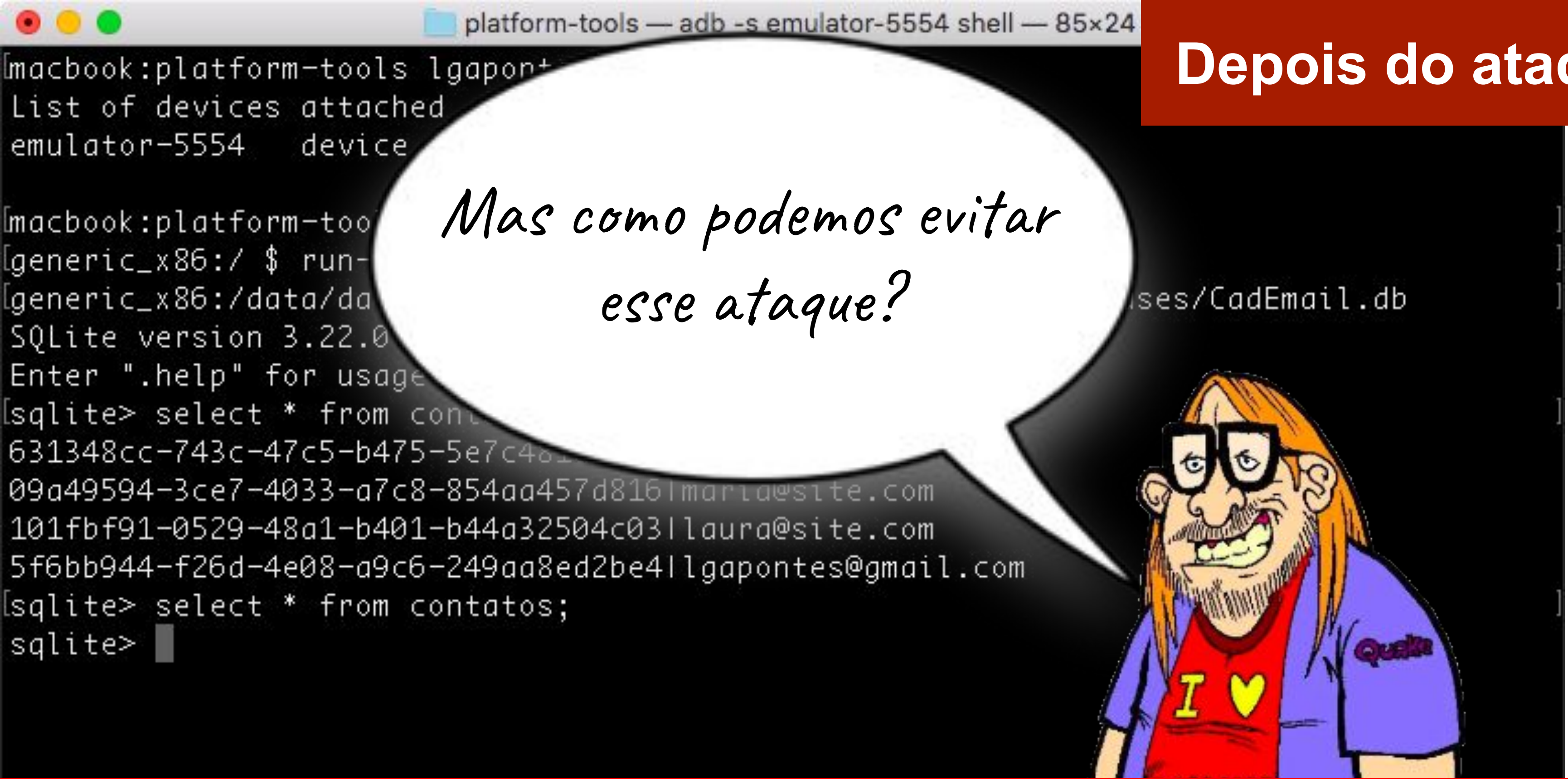
a@a'); delete from contatos where (uuid<>'

Depois do ataque...



```
macbook:platform-tools lgapontes$ ./adb devices
List of devices attached
emulator-5554   device

macbook:platform-tools lgapontes$ ./adb -s emulator-5554 shell
generic_x86:/ $ run-as com.lgapontes.cademail
generic_x86:/data/data/com.lgapontes.cademail $ sqlite3 databases/CadEmail.db
SQLite version 3.22.0 2018-01-22 18:45:57
Enter ".help" for usage hints.
sqlite> select * from contatos;
631348cc-743c-47c5-b475-5e7c481a38f0|joao@site.com
09a49594-3ce7-4033-a7c8-854aa457d816|maria@site.com
101fbf91-0529-48a1-b401-b44a32504c03|laura@site.com
5f6bb944-f26d-4e08-a9c6-249aa8ed2be4|lgapontes@gmail.com
sqlite> select * from contatos;
sqlite> 
```

Depois do ataque...



platform-tools — adb -s emulator-5554 shell — 85×24

```
macbook:platform-tools lgapont
List of devices attached
emulator-5554    device

macbook:platform-too
generic_x86:/ $ run-
generic_x86:/data/da                                            ses/CadEmail.db
SQLite version 3.22.0
Enter ".help" for usage
sqlite> select * from con
631348cc-743c-47c5-b475-5e7c48
09a49594-3ce7-4033-a7c8-854aa457d816|maria@site.com
101fbf91-0529-48a1-b401-b44a32504c03|laura@site.com
5f6bb944-f26d-4e08-a9c6-249aa8ed2be4|lgapontes@gmail.com
sqlite> select * from contatos;
sqlite>
```

Utilizando o `ContentValues` conforme apresentado no slide da aula 11.

Obrigado!