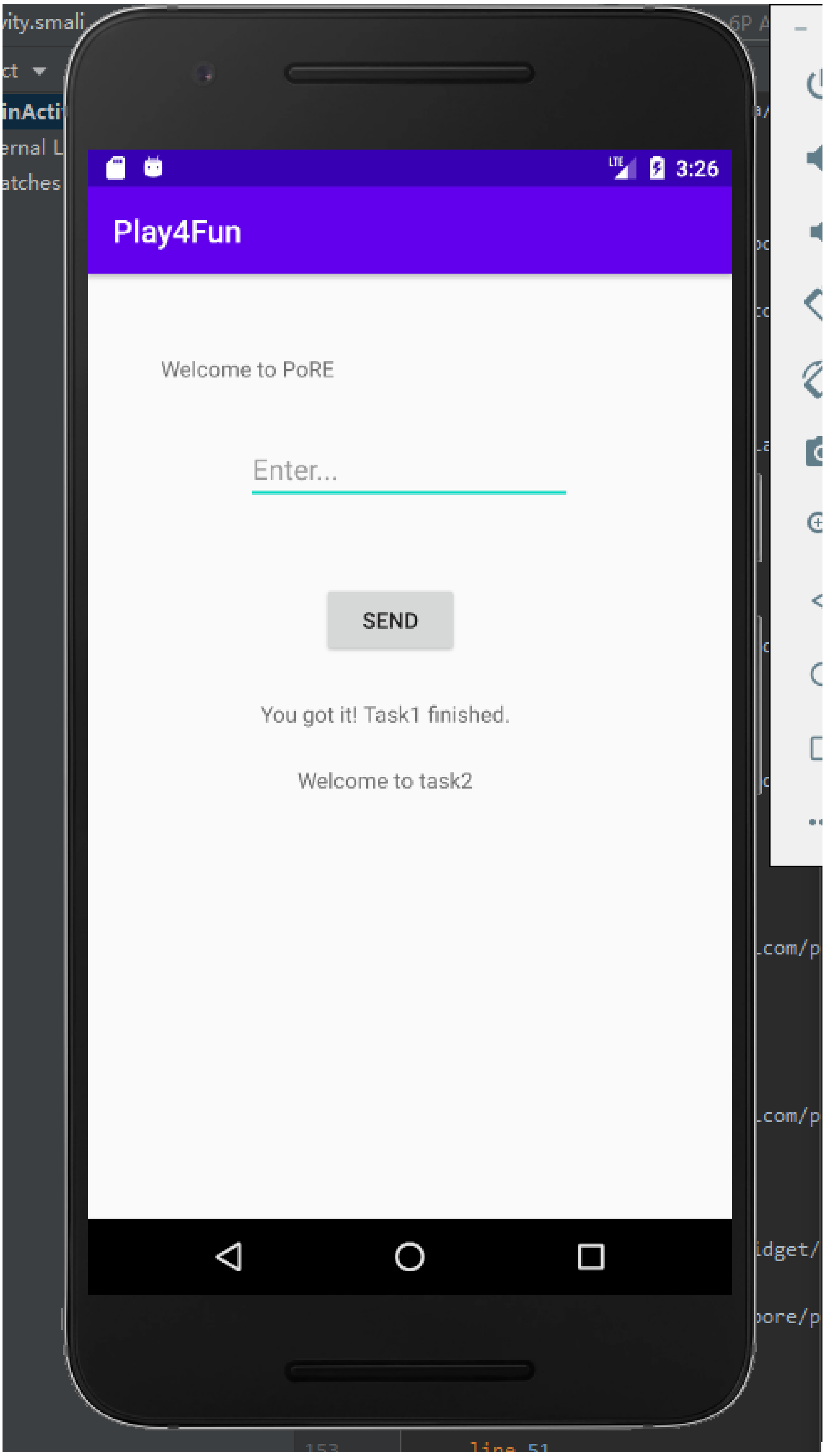
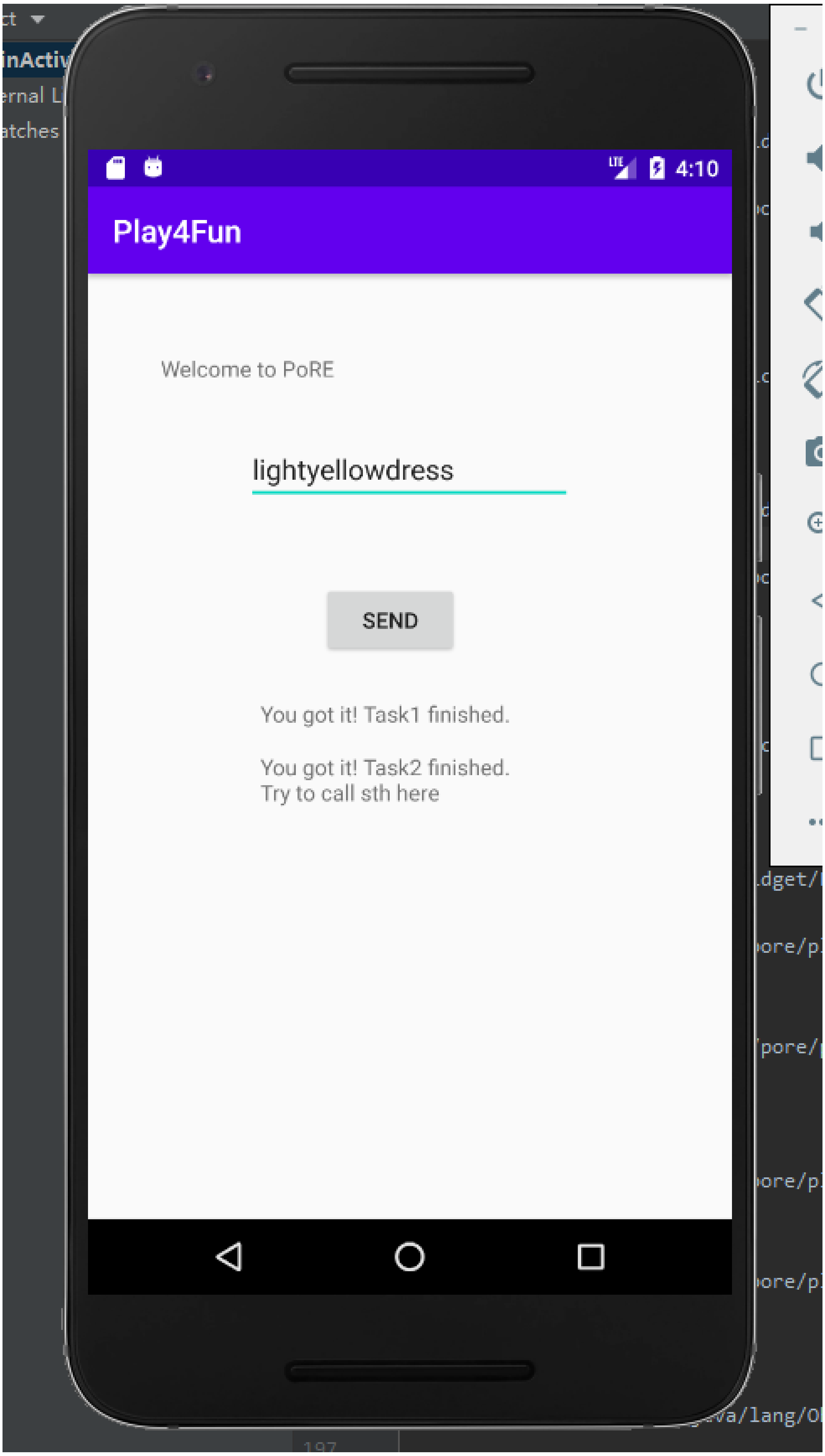


Welcome to PoRE

You got it! Task1 finished.

Welcome to task2

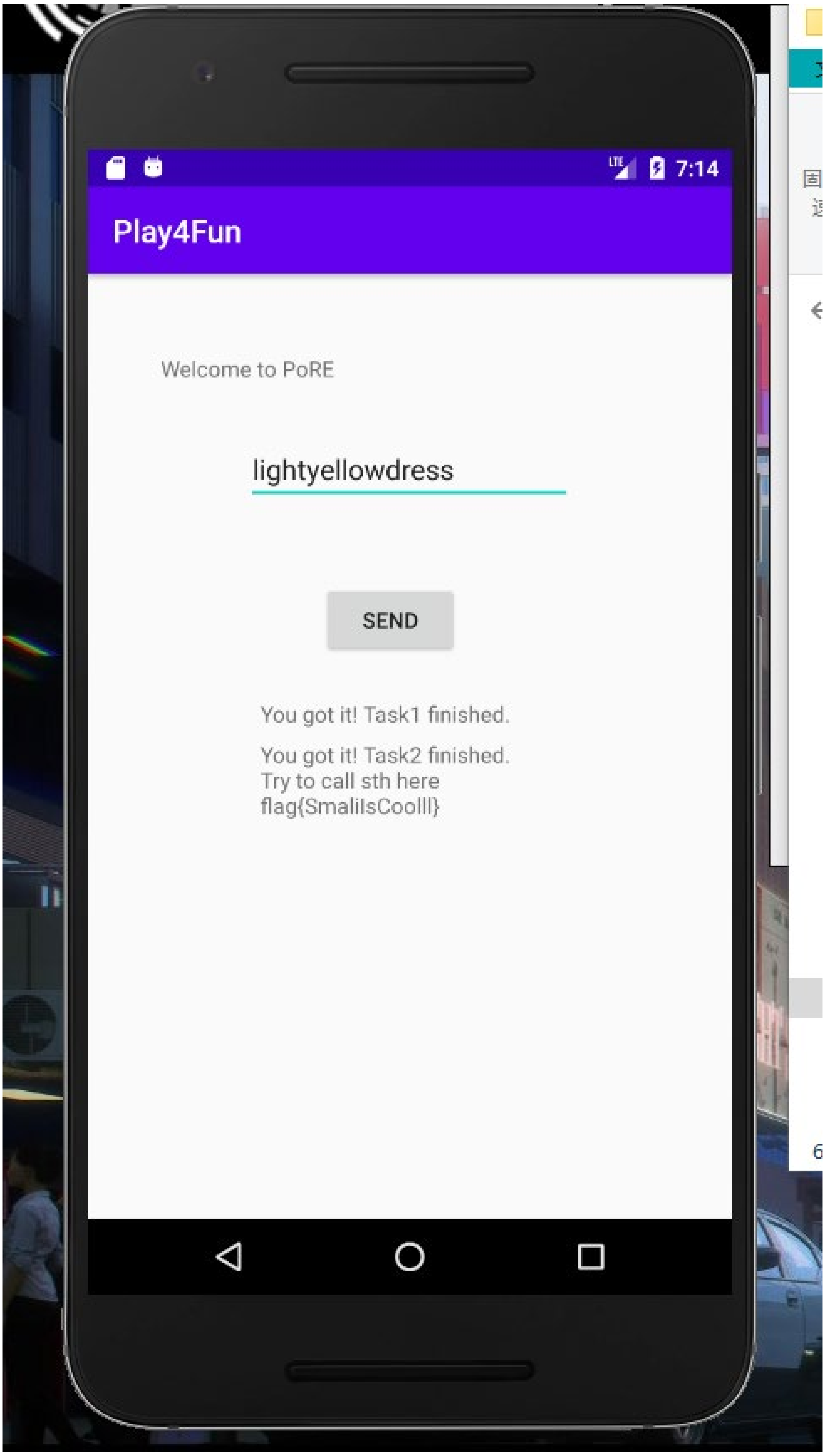


Welcome to PoRE

lightyellowdress

You got it! Task1 finished.

You got it! Task2 finished.
Try to call sth here

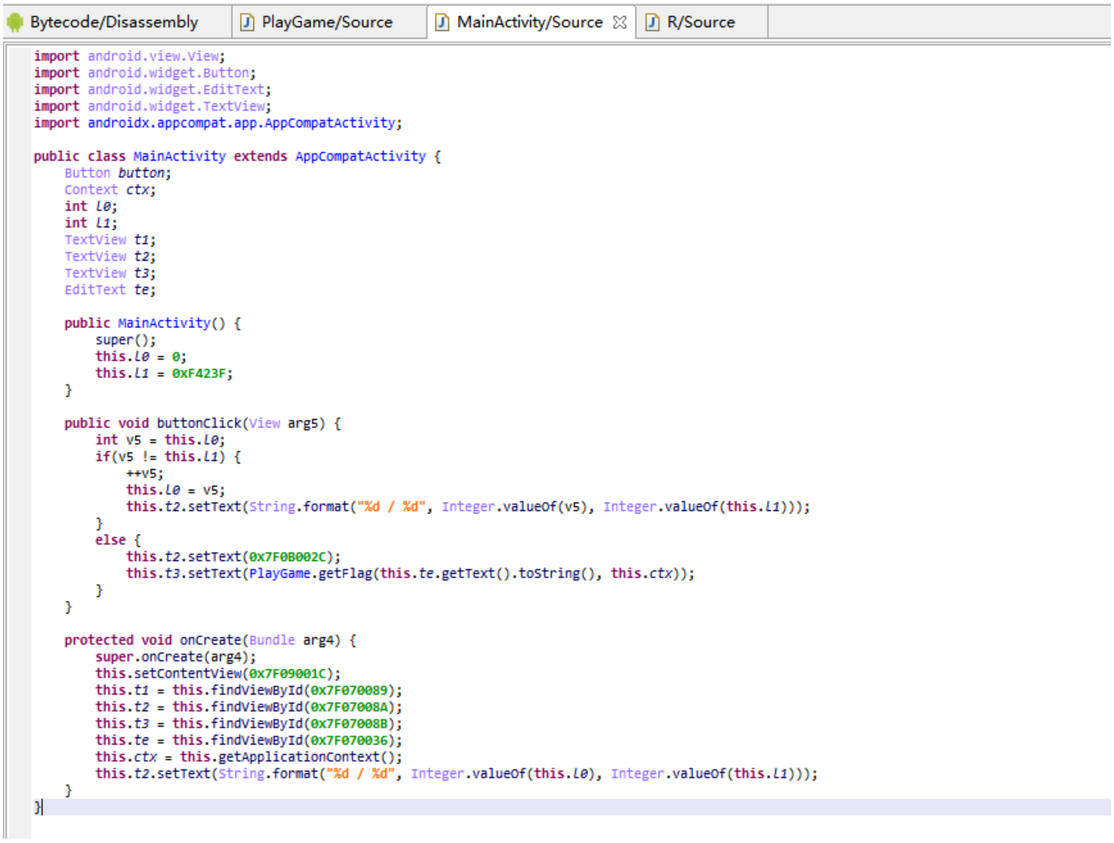


Welcome to PoRE

lightyellowdress

You got it! Task1 finished.

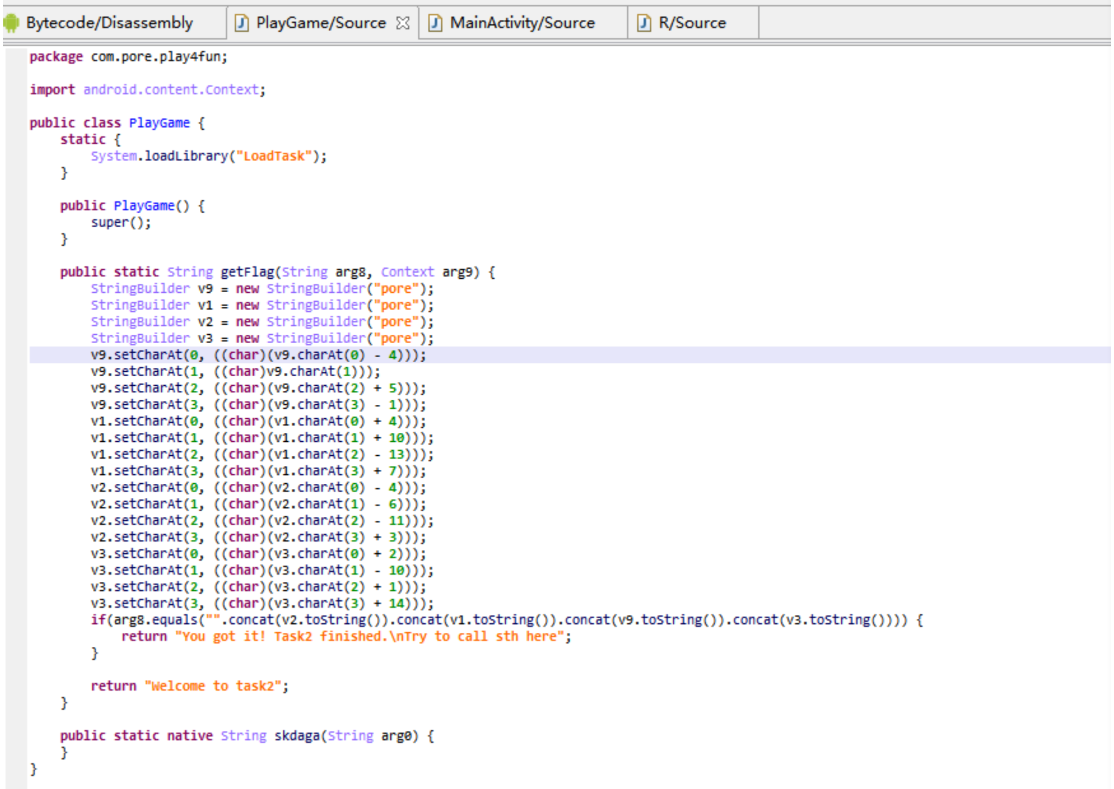
You got it! Task2 finished.
Try to call sth here
flag{SmaliIsCoolll}



```java
import android.view.View;
import android.widget.Button;
import android.widget.EditText;
import android.widget.TextView;
import androidx.appcompat.app.AppCompatActivity;

public class MainActivity extends AppCompatActivity {
    Button button;
    Context ctx;
    int l0;
    int l1;
    TextView t1;
    TextView t2;
    TextView t3;
    EditText te;

    public MainActivity() {
        super();
        this.l0 = 0;
        this.l1 = 0xF423F;
    }

    public void buttonClick(View arg5) {
        int v5 = this.l0;
        if(v5 != this.l1) {
            ++v5;
            this.l0 = v5;
            this.t2.setText(String.format("%d / %d", Integer.valueOf(v5), Integer.valueOf(this.l1)));
        }
        else {
            this.t2.setText(0x7F0B002C);
            this.t3.setText(PlayGame.getFlag(this.te.getText().toString(), this.ctx));
        }
    }

    protected void onCreate(Bundle arg4) {
        super.onCreate(arg4);
        this.setContentView(0x7F09001C);
        this.t1 = this.findViewById(0x7F070089);
        this.t2 = this.findViewById(0x7F07008A);
        this.t3 = this.findViewById(0x7F07008B);
        this.te = this.findViewById(0x7F070036);
        this.ctx = this.getApplicationContext();
        this.t2.setText(String.format("%d / %d", Integer.valueOf(this.l0), Integer.valueOf(this.l1)));
    }
}
```

Task1：

There’s a condition loop here. It requires you click the button until the 0 increases to 999999. I just replace the “if-ge” in smali by “goto”, unconditional jump to where we want.



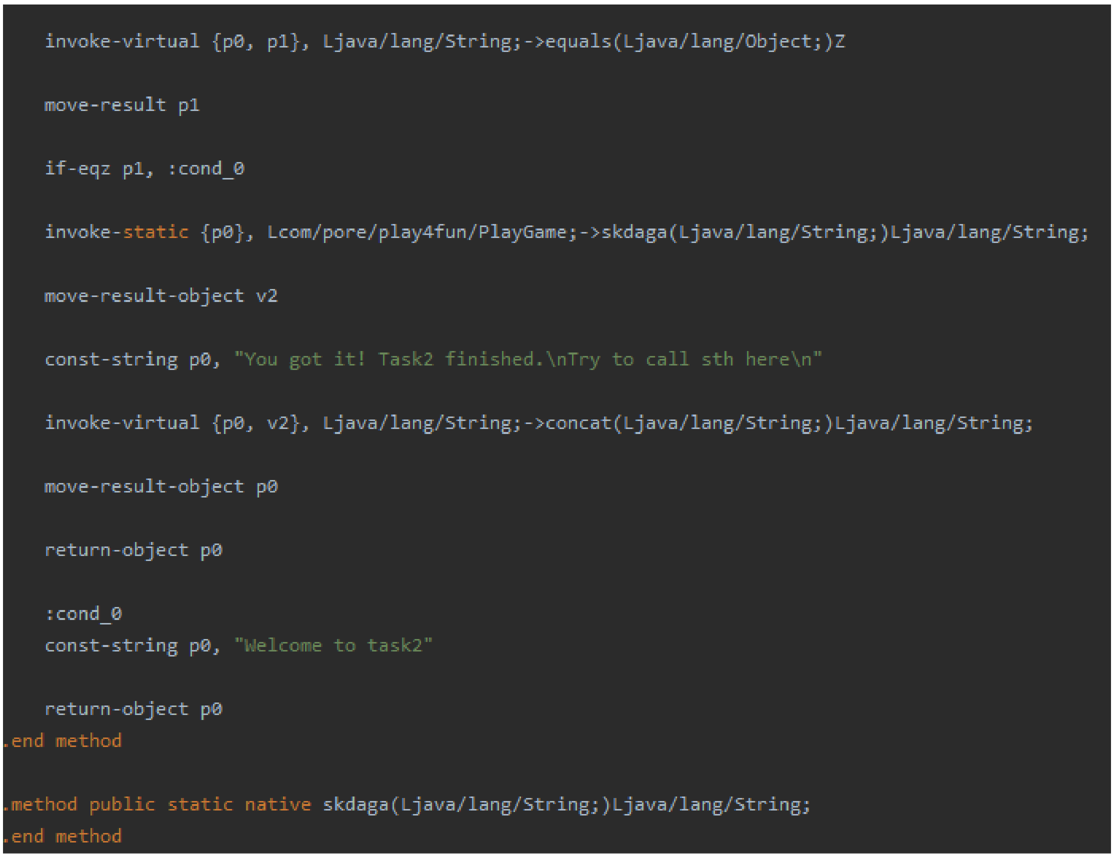
```
package com.pore.play4fun;

import android.content.Context;

public class PlayGame {
    static {
        System.loadLibrary("LoadTask");
    }

    public PlayGame() {
        super();
    }

    public static String getFlag(String arg8, Context arg9) {
        StringBuilder v9 = new StringBuilder("pore");
        StringBuilder v1 = new StringBuilder("pore");
        StringBuilder v2 = new StringBuilder("pore");
        StringBuilder v3 = new StringBuilder("pore");
        v9.setCharAt(0, ((char)(v9.charAt(0) - 4)));
        v9.setCharAt(1, ((char)v9.charAt(1)));
        v9.setCharAt(2, ((char)(v9.charAt(2) + 5)));
        v9.setCharAt(3, ((char)(v9.charAt(3) - 1)));
        v1.setCharAt(0, ((char)(v1.charAt(0) + 4)));
        v1.setCharAt(1, ((char)(v1.charAt(1) + 10)));
        v1.setCharAt(2, ((char)(v1.charAt(2) - 13)));
        v1.setCharAt(3, ((char)(v1.charAt(3) + 7)));
        v2.setCharAt(0, ((char)(v2.charAt(0) - 4)));
        v2.setCharAt(1, ((char)(v2.charAt(1) - 6)));
        v2.setCharAt(2, ((char)(v2.charAt(2) - 11)));
        v2.setCharAt(3, ((char)(v2.charAt(3) + 3)));
        v3.setCharAt(0, ((char)(v3.charAt(0) + 2)));
        v3.setCharAt(1, ((char)(v3.charAt(1) - 10)));
        v3.setCharAt(2, ((char)(v3.charAt(2) + 1)));
        v3.setCharAt(3, ((char)(v3.charAt(3) + 14)));
        if(arg8.equals("".concat(v2.toString()).concat(v1.toString()).concat(v9.toString()).concat(v3.toString()))) {
            return "You got it! Task2 finished.\nTry to call sth here";
        }

        return "Welcome to task2";
    }

    public static native String skdaga(String arg0) {
    }
}
```

Task2:

It’s about the token.

By reading the reverse Java code of smali, I found that the token is calculated by ascii from “poreporeporepore” to “lightyellowdress”.

So I just input the “lightyellowdress” and find it true.



```
    invoke-virtual {p0, p1}, Ljava/lang/String;->equals(Ljava/lang/Object;)Z

    move-result p1

    if-eqz p1, :cond_0

    invoke-static {p0}, Lcom/pore/play4fun/PlayGame;->skdaga(Ljava/lang/String;)Ljava/lang/String;

    move-result-object v2

    const-string p0, "You got it! Task2 finished.\nTry to call sth here\n"

    invoke-virtual {p0, v2}, Ljava/lang/String;->concat(Ljava/lang/String;)Ljava/lang/String;

    move-result-object p0

    return-object p0

    :cond_0
    const-string p0, "Welcome to task2"

    return-object p0
.end method

.method public static native skdaga(Ljava/lang/String;)Ljava/lang/String;
.end method
```

Task3:

I found a weird method called skdaga in smali, and it's a native method. I guess it will give me the secret answer. I reverse the .so in library and found it a C method which turn the inputted string to another string. So I change the flow and input the token into the method, and got the secret answer "flag{SmaliIsCoolll}.