

Write Up droids2

Kali ini saya mencoba untuk menyelesaikan sebuah challenge CTF yang bernama droids2.

droids2

400 points

Tags: **Category: Reverse Engineering**

AUTHOR: JASON

Description

Find the pass, get the flag. Check out this [file](#).

Hints ?

1 2 3


599 solves / 613 users attempted (98%)

92% Liked

picoCTF{FLAG}

Submit Flag

Di challenge ini diberikan sebuah file dengan extension .apk. .apk merupakan extension dari aplikasi-aplikasi yang digunakan pada operating system Android.

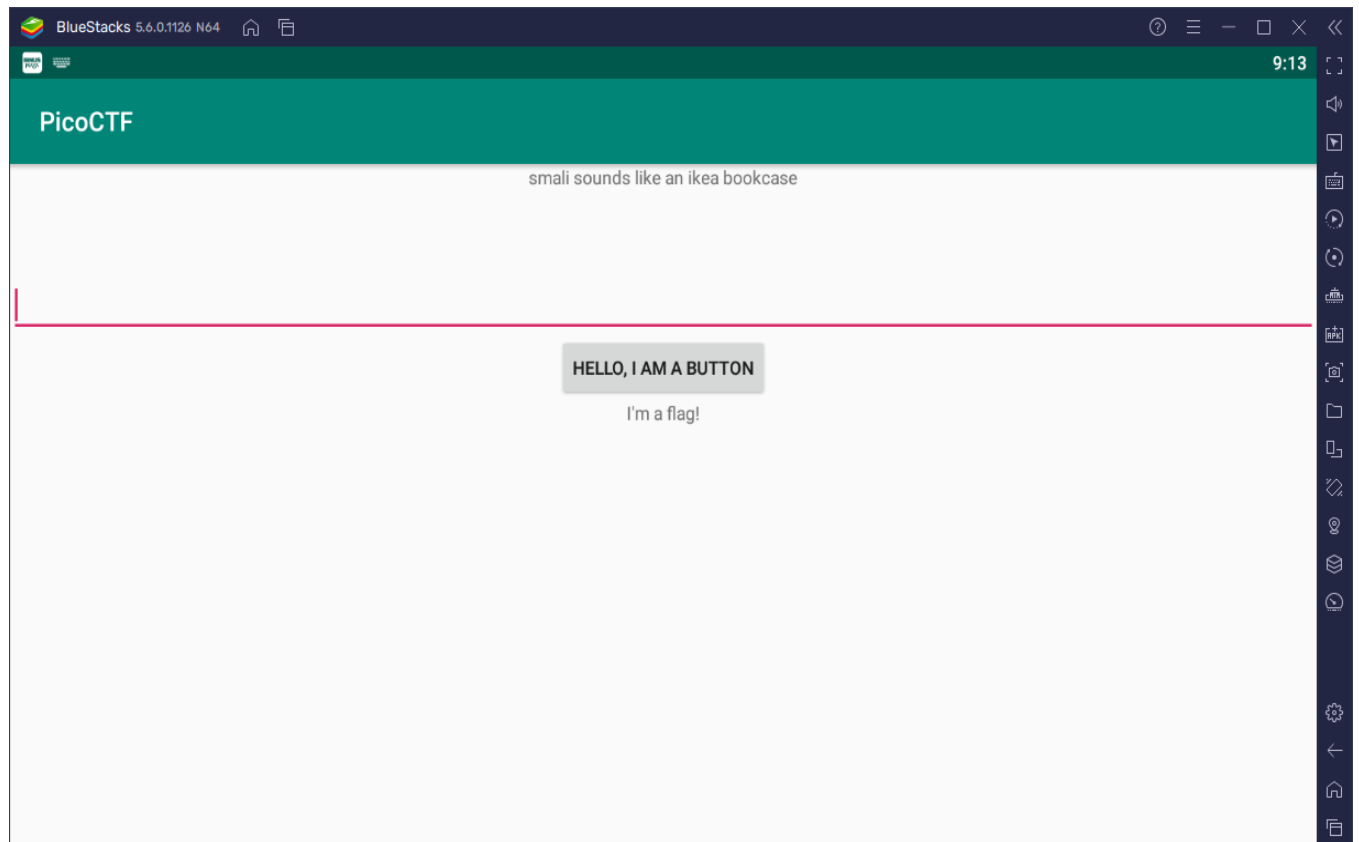
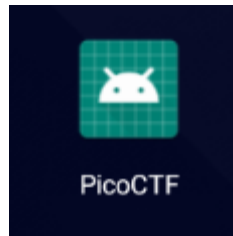
 two.apk

27/05/2022 18:03

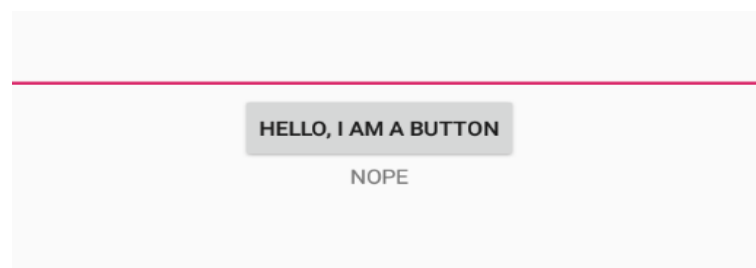
BlueStacks Androi...

1,747 KB

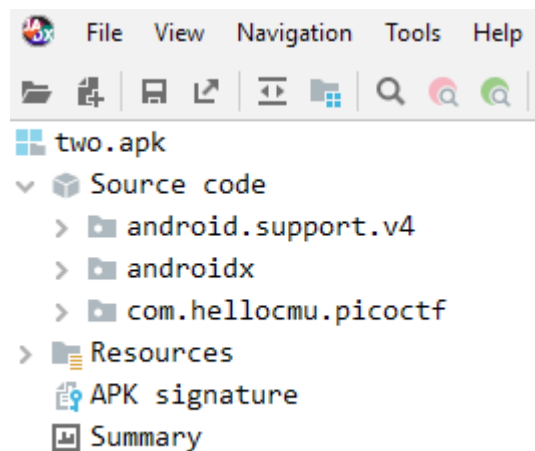
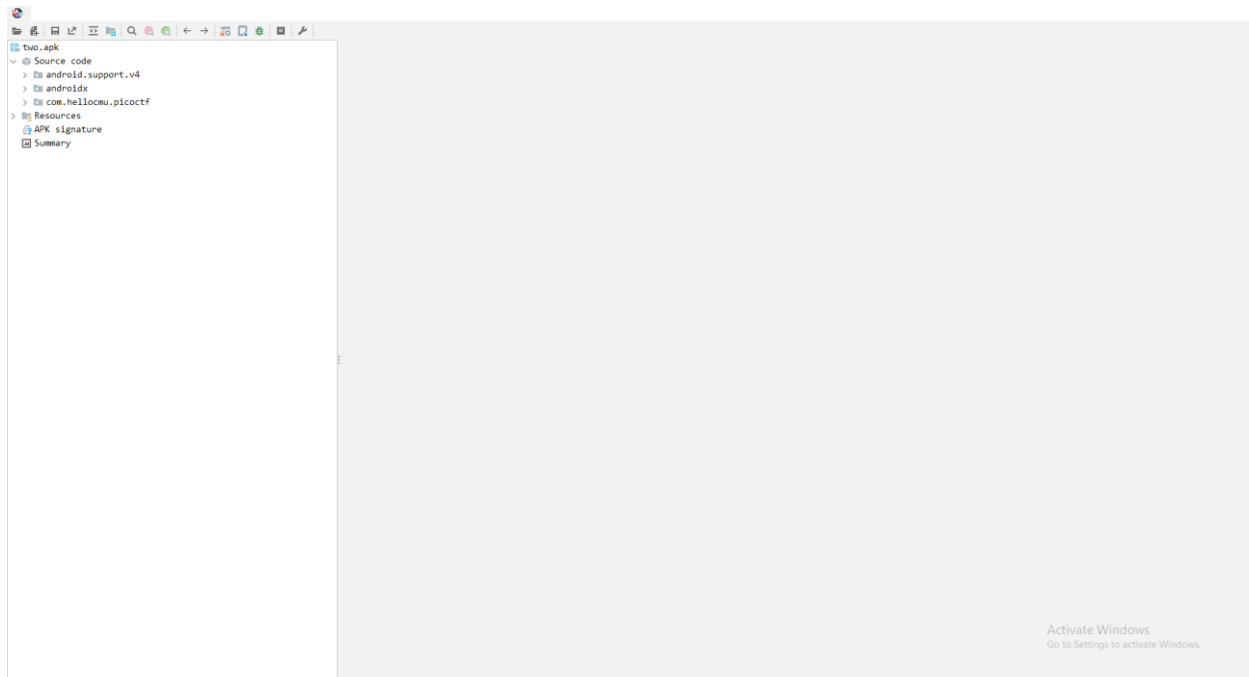
Karena kebetulan saya sudah menginstall BlueStacks(Emulator Android) maka saya bisa langsung menjalankan aplikasi tersebut.



Ini adalah tampilan app tersebut ketika dibuka. Terdapat sebuah tombol yang bisa kita klik. Jika kita tidak menginput apapun atau inputnya random maka akan keluar sebuah kata NOPE.

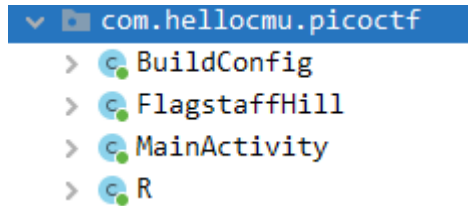


Karena sudah diketahui bahwa ini adalah sebuah app android maka saya menggunakan JADX, sebuah program untuk men decompile sebuah program ke Java.

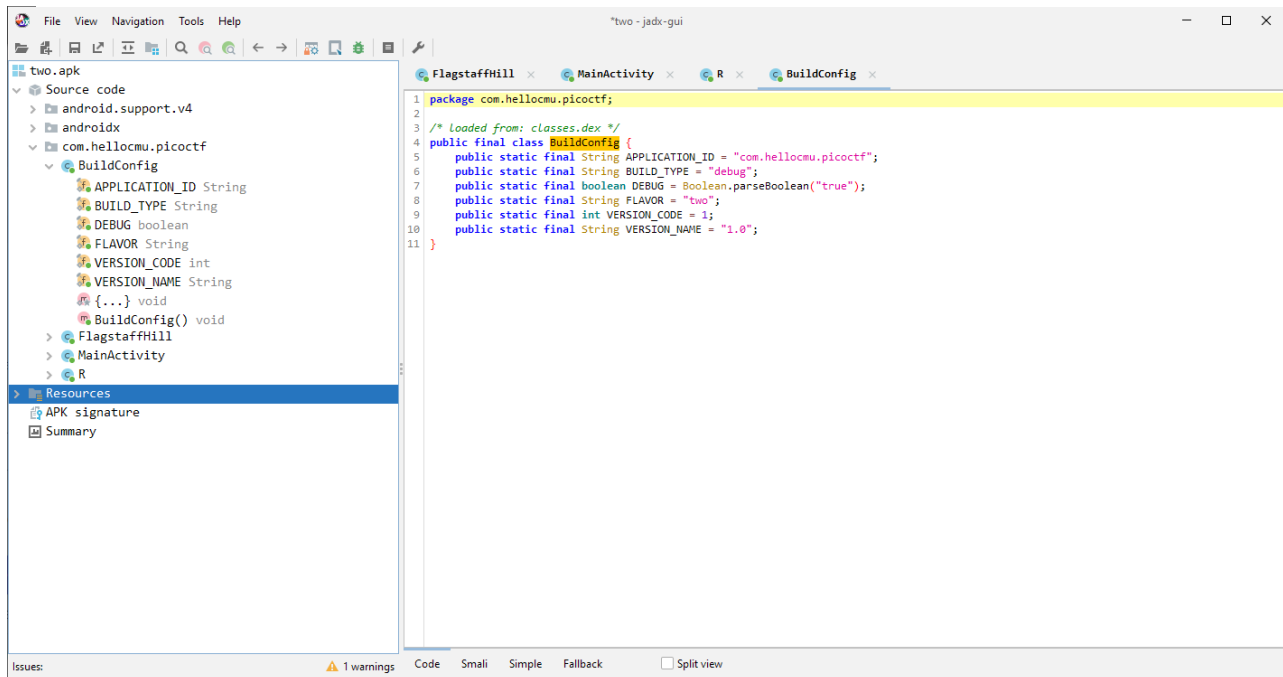


Pada menu Source code terdapat dropdown menu bernama com.hellocmu.picoctf.

Jika dibuka maka akan terlihat BuildConfig, FlagstaffHill, MainActivity, dan R.



BuildConfig berisi informasi tentang app tersebut.



FlagstaffHill berisikan sebuah function yang bernama getflag, yang dari namanya saja sudah memberikan sebuah clue.

```
package com.hellocmu.picoctf;

import android.content.Context;

/* Loaded from: classes.dex */
public class FlagstaffHill {
    public static native String sesame(String str);

    public static String getFlag(String input, Context ctx) {
        String[] witches = {"weatherwax", "ogg", "garlick", "nitt", "aching", "dissmass"};
        int second = 3 - 3;
        int third = (3 / 3) + second;
        int fourth = (third + third) - second;
        int fifth = 3 + fourth;
        int sixth = (fifth + second) - third;
        String password = "".concat(witches[fifth]).concat(".").concat(witches[third]).concat(".").concat(witches[second]).concat(".").concat(witches[sixth]).concat(".").concat(witches[3]).concat(".").concat(witches[fourth]);
        return input.equals(password) ? sesame(input) : "NOPE";
    }
}
```

Di dalam function tersebut ada sebuah array bernama witches yang berisi enam string. Kemudian ada beberapa variable integer dan sebuah string bernama password.

Dalam string password terdapat concat yang berfungsi untuk menambahkan atau menggabungkan dua buah string menjadi satu. Kita bisa lihat juga concat dilakukan berkali-kali untuk menggabungkan string dalam array witches.

```
String password=
"".concat(witches[fifth]).concat(".").concat(witches[third]).concat(".").concat(witches[second]).concat(".").concat(witches[sixth]).concat(".").concat(witches[3]).concat(".").concat(witches[fourth]);
```

Index dari array tersebut adalah variable-variable integer yang diberikan di atasnya, jadi jika kita ingin mengetahui password kita harus menyelesaikan teka-teki integer terlebih dahulu.

Int second = 3 - 3 = 0

$\text{Int third} = (3/3) + \text{second} = 1 + 0 = 1$

$\text{Int fourth} = (\text{third} + \text{third}) - \text{second} = (1 + 1) - 0 = 2$

$\text{Int fifth} = 3 + \text{fourth} = 3 + 2 = 5$

$\text{Int sixth} = (\text{fifth} + \text{second}) - \text{third} = (5 + 0) - 1 = 4$

Jangan lupa ada concat(".") yang menambahkan . (titik) diantara setiap string.

String password akan menjadi :

dis~~mass~~.ogg.weatherwax.aching.nitt.garlick

Pada MainActivity ada function bernama buttonClick yang menerima sebuah input berupa string lalu menjalankan fungsi getflag dari FlagstaffHill setelah tombol diklik.

```
package com.hellocmu.picoctf;

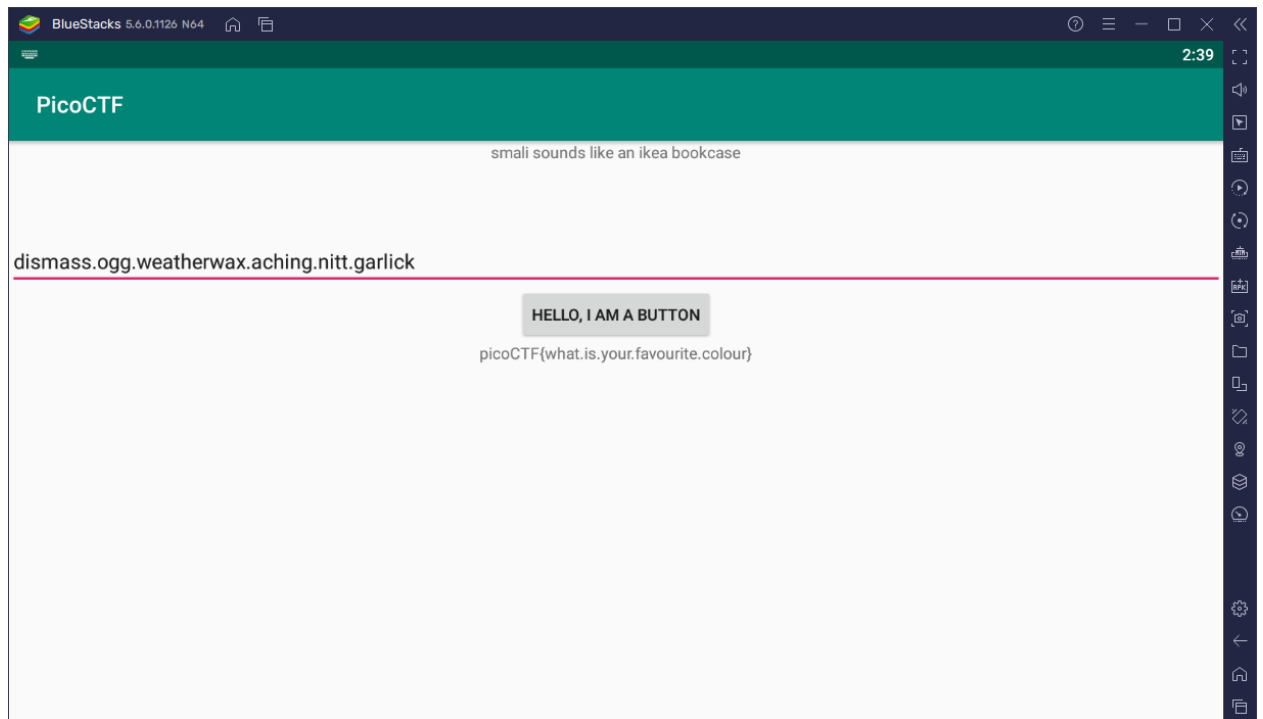
import android.content.Context;
import android.os.Bundle;
import android.view.View;
import android.widget.Button;
import android.widget.EditText;
import android.widget.TextView;
import androidx.appcompat.app.AppCompatActivity;

/* Loaded from: classes.dex */
public class MainActivity extends AppCompatActivity {
    Button button;
    Context ctx;
    TextView text_bottom;
    EditText text_input;
    TextView text_top;

    /* JADX INFO: Access modifiers changed from: protected */
    @Override // androidx.appcompat.app.AppCompatActivity, androidx.fragment.app.FragmentActivity, androidx.core.app.C
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
        this.text_top = findViewById(R.id.text_top);
        this.text_bot = com.hellocmu.picoctf.R.id.text_bottom;
        this.text_inp = findViewById(R.id.text_input);
        this.ctx = getApplicationContext();
        System.loadLibrary("hellojni");
        this.text_top.setText(R.string.hint);
    }

    public void buttonClick(View view) {
        String content = this.text_input.getText().toString();
        this.text_bottom.setText(FlagstaffHill.getFlag(content, this.ctx));
    }
}
```

Setelah itu saya coba menginput password yang sudah didapatkan lalu mengklik tombol.



Dengan seketika app tersebut mengeluarkan flagnya yaitu :

picoCTF{what.is.your.favourite.colour}