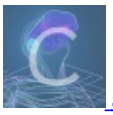
攻防世界 app1 wp

原创

__ys 于 2021-02-08 14:50:42 发布 69 收藏

分类专栏： apk

本文链接：https://blog.csdn.net/qq_39214793/article/details/113756775



app1（第一份安卓题）

1. 丢进模拟器查看

2. 用JEB解析查看

```java
import android.view.View;
import android.widget.Button;
import android.widget.EditText;
import android.widget.Toast;

public class MainActivity extends AppCompatActivity {
    Button btn;
    public final String pName;
    EditText text;

    public MainActivity() {
        super();
        this.pName = "com.example.yaphetshan.tencentgreat";
    }

    protected void onCreate(Bundle arg3) {
        super.onCreate(arg3);
        this.setContentView(0x7F04001B);
        this.btn = this.findViewById(0x7F0B0058);
        this.text = this.findViewById(0x7F0B0057);
        this.btn.setOnClickListener(new View$OnClickListener() {
            public void onClick(View arg10) {
                try {
                    String v1 = MainActivity.this.text.getText().toString();
                    PackageInfo v2 = MainActivity.this.getPackageManager().getPackageInfo("com.example.yaphetshan.tencentgreat", 0x4000);
                    String v3 = v2.versionName;
                    int v4 = v2.versionCode;
                    int v0 = 0;
                    while(v0 < v1.length()) {
                        if(v0 >= v3.length()) {
                            break;
                        }

                        if(v1.charAt(v0) != (v3.charAt(v0) ^ v4)) {
                            Toast.makeText(MainActivity.this, "再接再厉，加油~", 1).show();
                            return;
                        }
                        else {
                            ++v0;
                            continue;
                        }
                    }

                    if(v1.length() != v3.length()) {
                        goto label_39;
                    }

                    Toast.makeText(MainActivity.this, "恭喜开启闯关之门！", 1).show();
                    return;
                }
                catch(PackageManager$NameNotFoundException v5) {
                }

            label_39:
                Toast.makeText(MainActivity.this, "年轻人不要耍小聪明噢", 1).show();
            }
        });
    }
}
```


分析可知是将输入flag与versionName和versionCode的异或值相比较

在BuildConfig可以查看versionName与versionCode的值

```
.field public static final APPLICATION_ID:String = "com.example.yaphetshan.tencentgreat"

.field public static final BUILD_TYPE:String = "debug"

.field public static final DEBUG:Z = false

.field public static final FLAVOR:String = ""

.field public static final VERSION_CODE:I = 0xF

.field public static final VERSION_NAME:String = "X<cP[?PHNB<P?aj"
```

写脚本获得flag即可

```cpp
#include<bits/stdc++.h>
using namespace std;
string flag="X<cP[?PHNB<P?aj";
int main()
{
 for(int i=0;i<flag.length();i++)
  flag[i]^=0xF;
 cout<<flag;
 return 0;
}
```