

# 【jarvisoj刷题之旅】逆向题目爬楼梯的writeup

原创

iqiqiya 于 2018-09-11 16:09:42 发布 收藏  
分类专栏: 我的逆向之路 我的CTF之路 我的CTF进阶之路 文章标签: [【jarvisoj刷题之旅】逆向题目爬楼梯的writeup](#) 爬楼梯 writeup

版权声明: 本文为博主原创文章, 遵循[CC 4.0 BY-SA](#)版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/xiangshangashaonian/article/details/82627540>

版权



[我的逆向之路 同时被 3 个专栏收录](#)

108 篇文章 10 订阅

订阅专栏



[我的CTF之路](#)

92 篇文章 5 订阅

订阅专栏

[我的CTF进阶之路](#)

108 篇文章 18 订阅

订阅专栏

先放到模拟器中运行一波

CTF\_100

爬楼梯啊,爬楼梯.....

要爬的楼层: 376832

已爬的楼层: 27

爬一层楼

爬到了,看FLAG

<https://blog.csdn.net/xiangshangashaonian>

难道是得一直点吗 作为懒人的我可不答应

于是APKIDE反编译 用jd\_jui直接看java源码

```
>MainActivity.class
```

```
import android.widget.Button;
import android.widget.TextView;
import java.util.Random;

public class MainActivity
    extends AppCompatActivity
{
    public int has_gone_int;
    public int to_reach_int;

    static
    {
        if (!Debug.isDebuggerConnected())
            System.loadLibrary("ctf");
    }
}

public void Btn_up_onclick(View paramView)
{
    this.has_gone_int += 1;
    paramView = "" + this.has_gone_int;
    ((TextView)findViewById(2131492948)).setText(paramView);
    if (this.to_reach_int <= this.has_gone_int)
        ((Button)findViewById(2131492950)).setClickable(true);
}

public void btn2_onclick(View paramView)
{
    ((TextView)findViewById(2131492951)).setText("{Flag:" + get_flag(this.to_reach_int) + "}");
}

public native String get_flag(int paramInt);

protected void onCreate(Bundle paramBundle)
{
    super.onCreate(paramBundle);
    setContentView(2130968601);
    ((Button)findViewById(2131492950)).setClickable(false);
    this.has_gone_int = 0;
    paramBundle = new Random();
    for (this.to_reach_int = paramBundle.nextInt(); this.to_reach_int = paramBundle.nextInt()
    {
        if (this.to_reach_int < 0)
            this.to_reach_int *= -1;
        if (5 < this.to_reach_int)
        {
            this.to_reach_int %= 32;
            this.to_reach_int *= 16384;
            ((TextView)findViewById(2131492947)).setText("" + this.to_reach_int);
            ((TextView)findViewById(2131492951)).setText("");
            return;
        }
    }
}
```

<https://blog.csdn.net/xiangshangbashaonian>

由java代码可知 我们只要直接让“爬到了，看FLAG“这个按钮可点击即可

那么让他可被点击 只需要改这里就好

```
protected void onCreate(Bundle paramBundle)
{
    super.onCreate(paramBundle);
    setContentView(2130968601);
    ((Button)findViewById(2131492950)).setClickable(false);
    this.has_gone_int = 0;
    paramBundle = new Random();
    for (this.to_reach_int = paramBundle.nextInt(); this.to_reach_int = paramBundle.nextInt()
```

分析可知 后面的传值 是与v5相关的 那么只要将他赋值1即可

The screenshot shows the APKIDE IDE interface. On the left, the project tree displays a project named 'CTF\_100' with version '1.0(1)' and package 'com.ctf.test.ctf'. It includes files like 'AndroidManifest.xml', 'MainActivity.smali', and various resource files in smali format. On the right, the main window shows the decompiled Java code in smali format. A specific line of code, 'const/4 v5, 0x1', is highlighted with a red box. Below the code editor is an 'Output' panel showing build logs. The logs indicate that 1 file was found, the apk is being built, and there is a failure due to a libpng error: 'libpng error: Not a PNG file' and an 'ERROR: Failure processing PNG image' message.

```
168     .line 68
169     return-void
170     .end method
171
172     .method public native get_flag(I)Ljava/lang/String;
173     .end method
174
175     .method protected onCreate(Landroid/os/Bundle;)V
176         .locals 6
177         .param p1, "savedInstanceState" # Landroid/os/Bundle;
178
179         .prologue
180         const/4 v5, 0x1
181
182         .line 22
183         invoke-super (p0, p1), Landroid/support/v7/app/AppCompatActivity;->onCreate(L
184
185         .line 23
186         const v4, 0x7f040019
187
188         invoke-virtual (p0, v4), Lcom/ctf/test/ctf_100/MainActivity;->setContentView(
189
190         .line 24
191         const v4, 0x7f0c0056
192
193         invoke-virtual (p0, v4), Lcom/ctf/test/ctf_100/MainActivity;->findViewById(I)
194
195         move-result-object v0
196
输出
- 找到 1 个文件
> 正在编译Apk...
- 失败:
W: libpng error: Not a PNG file
W: ERROR: Failure processing PNG image D:\xin\ApkIDE3.5.0\Work\com.ctf.test.ctf_100\res\mipmap-xxhdpi-v4\ic_launcher.png
Exception in thread "main" brut.androlib.AndrolibException: brut.androlib.AndrolibException: brut.common.BrutException:
at brut.androlib.Androlib.buildResourcesFull(Androlib.java:496)
at blog.CSDN.net/Xiangshangbashaonian
```

改过之后 发现APKIDE与Androidkiller都没办法编译成功（不知道是哪里的原因 如果有大神知道 还请不吝赐教）

【2018.9.14更新】已经找到原因 可以看这篇文章详细解释<https://blog.csdn.net/xiangshangbashaonian/article/details/82708572>

我用了bin神的mt管理器成功

下午3:42

4G 4G

## CTF\_100

爬楼梯啊,爬楼梯.....

要爬的楼层: 507904

已爬的楼层: 0

爬一层楼

爬到了,看FLAG

{Flag:268796A5E68A25A1}

<https://blog.csdn.net/xiangshangbashaonian>

但是这个题目有意思的是

在我第三次次启动他的时候 他居然给的随机数是0

呃呃。。。

所以有时候运气也很关键

还有就是一定要看清格式再提交。。。

## 爬楼梯

85 SOLVERS

100

REVERSE

对压缩包中的程序进行分析并获取flag。flag形式为16位大写md5。

题目来源：CFF2016

CFF\_100.rar.dbeee1536c0a5ef5844f42c93602aae5

You have solved this Challenge!

SUBMIT

<https://blog.csdn.net/xiangshangbashaonian>