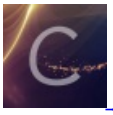
【jarvisoj刷题之旅】逆向题目爬楼梯的writeup

原创

iqiqiya 于 2018-09-11 16:09:42 发布 834 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


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

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

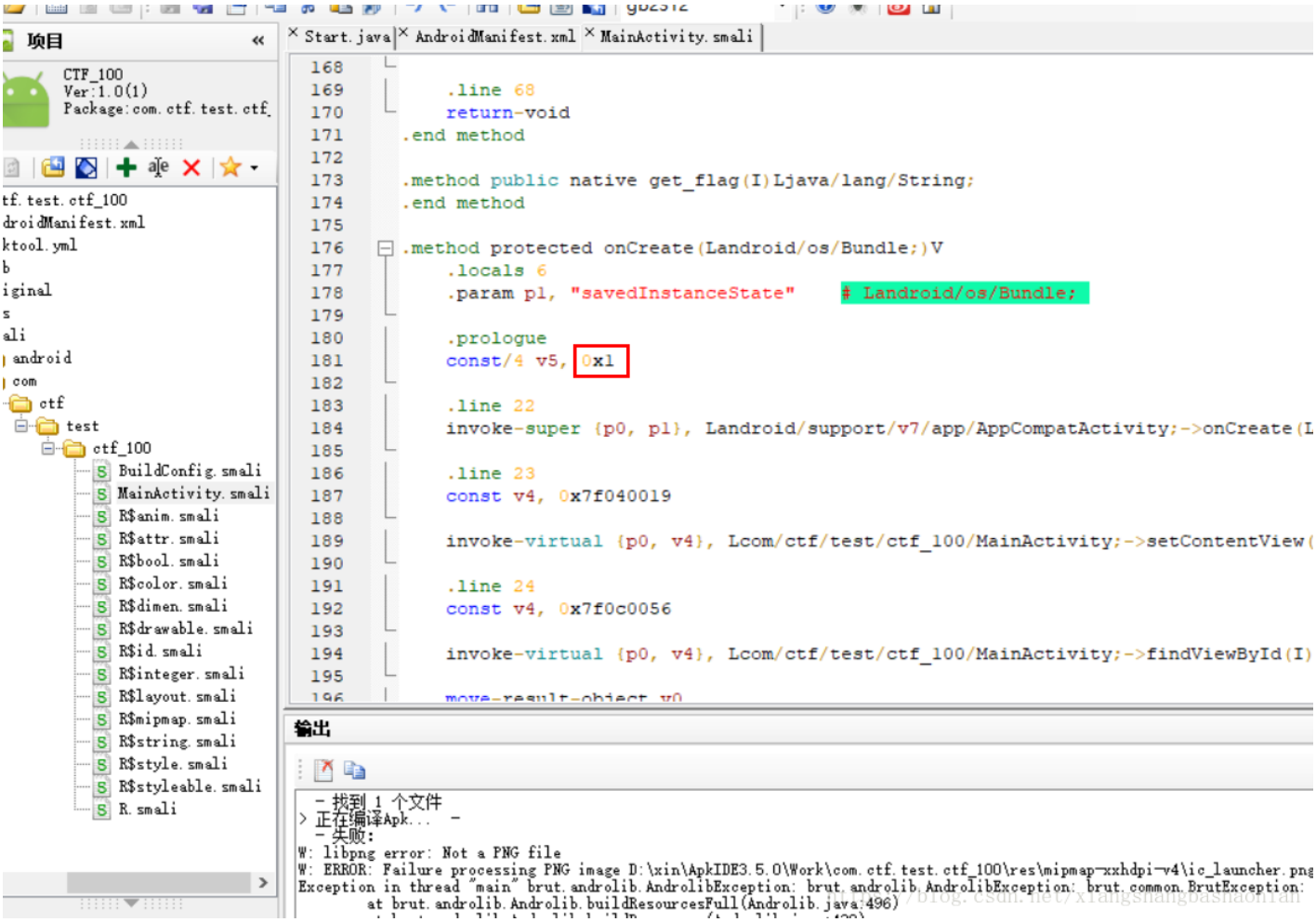
```
import android.widget.Button;
import android.widget.TextView;
import java.util.Random;

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;
      }
    }
  }
}
```


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



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

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