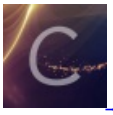
【WhaleCTF逆向题】第二期包剪锤【初级】writeup

原创

iqiqiya 于 2018-09-27 17:21:56 发布 610 收藏

分类专栏： 我的逆向之路 我的CTF之路 ------WhaleCTF 我的CTF进阶之路 文章标签： 【WhaleCTF逆向题】第二期包剪锤【初级】writeup 包剪锤【初级】writeup writeup reverse


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

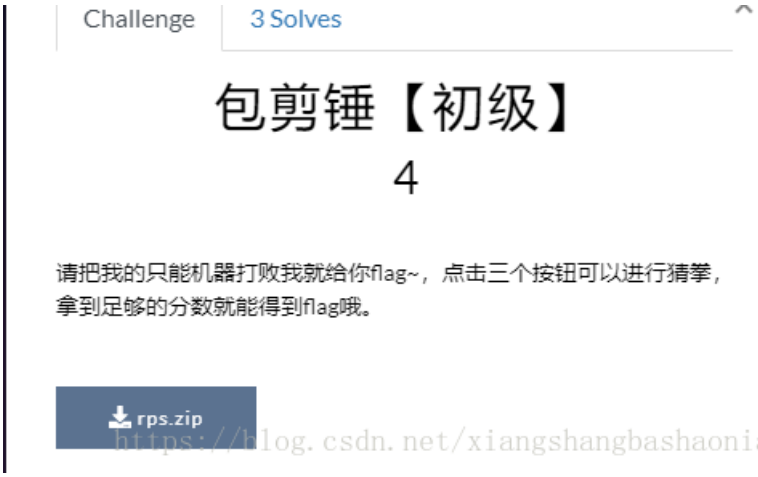

我的CTF之路

92 篇文章 5 订阅
订阅专栏


------WhaleCTF

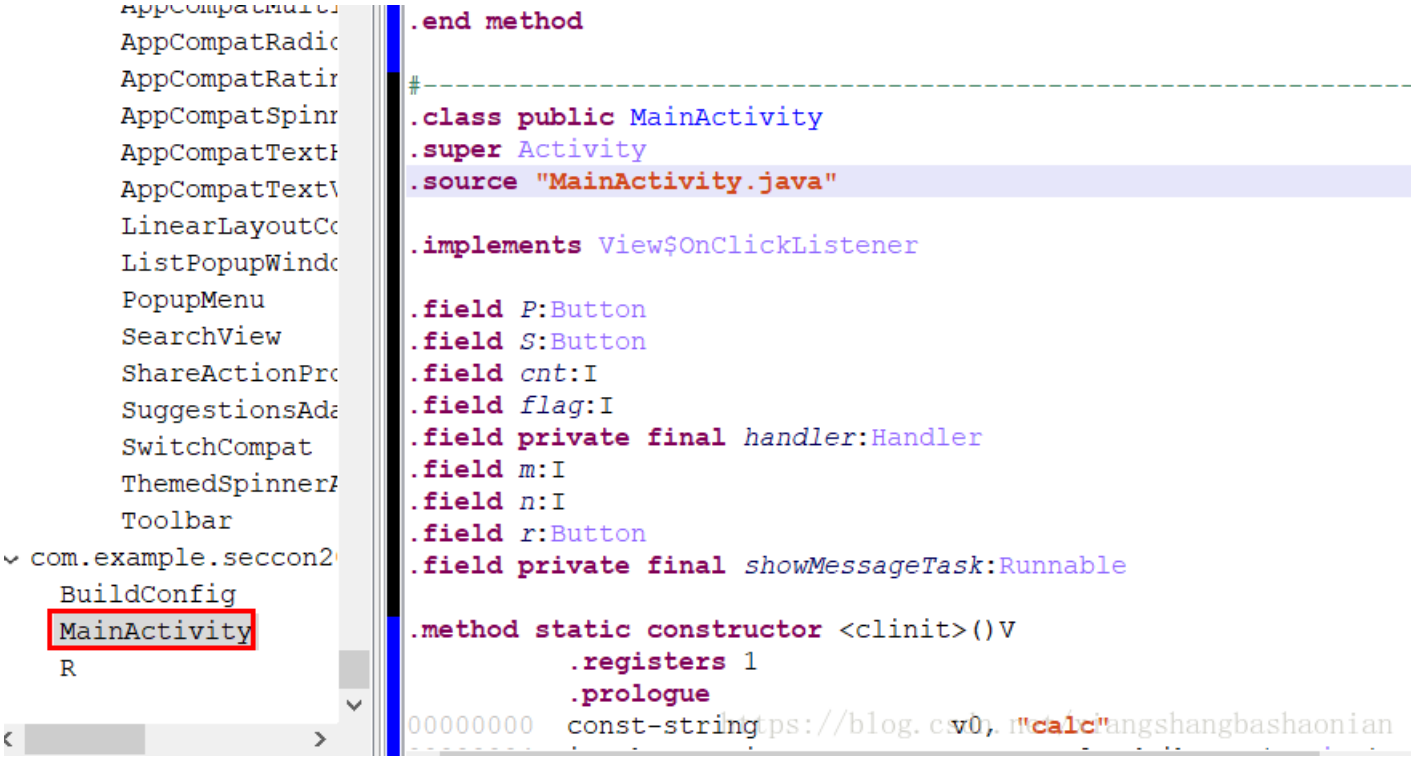
8 篇文章 0 订阅
订阅专栏

题目信息：



拿到apk 载入jeb

双击MainActivity 然后tab键可以反汇编成java代码



大体可以看出 通过Random()每次生成一个随机数v9

通过这个v9再构造一个字符串数组 v1[]

下面对数组元素进行赋值

所以n对应的就是CPU的取值　m就是我们的选择

```
    public void onClick(View v) {
        int v9 = 3;
        int v8 = 2;
        if(this.flag != 1) {
            this.flag = 1;
            this.findViewById(2131492946).setText("");
            View v2 = this.findViewById(2131492944);
            View v3 = this.findViewById(2131492945);
            this.m = 0;
            this.n = new Random().nextInt(v9);
            String[] v1 = new String[v9];
            v1[0] = "CPU: Paper";
            v1[1] = "CPU: Rock";
            v1[v8] = "CPU: Scissors";
            ((TextView)v3).setText(v1[this.n]);
            if(v == this.P) {
                ((TextView)v2).setText("YOU: Paper");  // 布
                this.m = 0;
            }

            if(v == this.r) {
                ((TextView)v2).setText("YOU: Rock");  // 石头
                this.m = 1;
            }

            if(v == this.S) {
                ((TextView)v2).setText("YOU: Scissors");  // 剪刀
                this.m = v8;
            }
```

为方便查看下面我截了关键部分 run()方法就是关键

可以看到只有两种情况才可以win! cnt++

那么cnt很显然就是记录我们win的次数

而再看最后一个if语句 可以知道当cnt = 1000时 我们就可以拿到flag

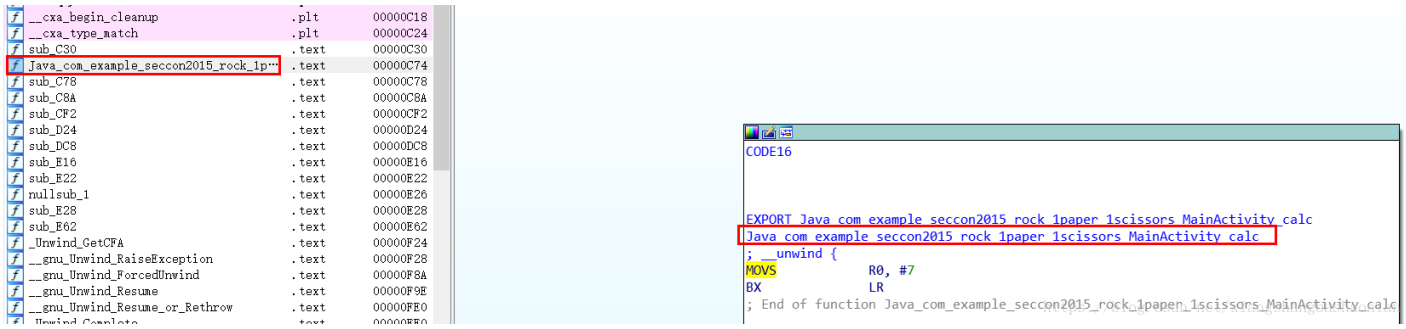
取值就是SECCON{(cnt + calc) * 107}

那么cnt当然就是1000 那么就差calc的值了

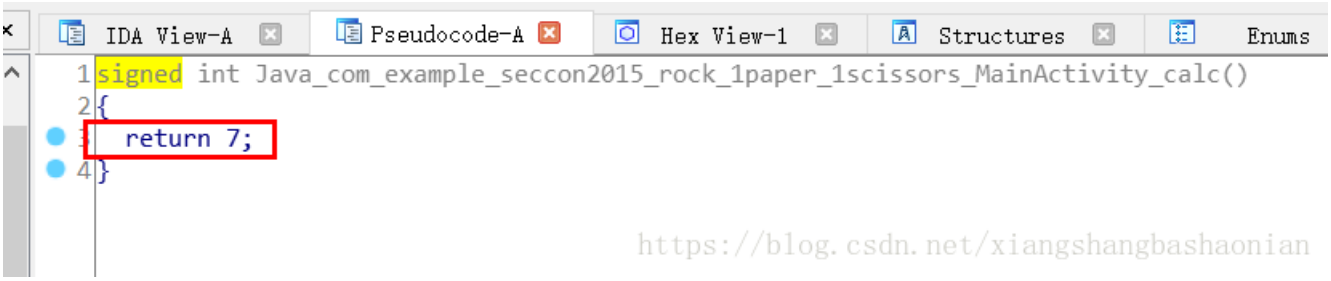
```
public MainActivity() {
    super();
    this.cnt = 0;
    this.handler = new Handler();
    this.showMessageTask = new Runnable() {
        public void run() {
            View v0 = MainActivity.this.findViewById(2131492946);
            if(MainActivity.this.n - MainActivity.this.m == 1) {
                ++MainActivity.this.cnt;
                ((TextView)v0).setText("WIN! +" + String.valueOf(MainActivity.this.cnt));
            }
            else if(MainActivity.this.m - MainActivity.this.n == 1) {
                MainActivity.this.cnt = 0;
                ((TextView)v0).setText("LOSE +0");
            }
            else if(MainActivity.this.m == MainActivity.this.n) {
                ((TextView)v0).setText("DRAW +" + String.valueOf(MainActivity.this.cnt));
            }
            else if(MainActivity.this.m < MainActivity.this.n) {
                MainActivity.this.cnt = 0;
                ((TextView)v0).setText("LOSE +0");
            }
            else {
                ++MainActivity.this.cnt;
                ((TextView)v0).setText("WIN! +" + String.valueOf(MainActivity.this.cnt));
            }

            if(1000 == MainActivity.this.cnt) {
                ((TextView)v0).setText("SECCON{" + String.valueOf((MainActivity.this.cnt + MainActivity
                        .this.calc()) * 107) + "}");
            }

            MainActivity.this.flag = 0;
        }
    };
```


将rps.apk解压 找到libcalc.so

IDA载入



如果看不明白 就F5



那就很清楚咯 calc就是7

那么flag就是SECCON{(1000+7)* 107} -->SECCON{107749}

提交正确