whaleCTF-30days-逆向【第一期】-安卓加密-writeup

原创

sec小玖 于 2018-07-23 15:14:37 发布 739 收藏
分类专栏： CTF 逆向 文章标签： CTF 逆向 安卓

本文链接：https://blog.csdn.net/afuzong4267/article/details/81168116


CTF 同时被 2 个专栏收录
6 篇文章 0 订阅
订阅专栏


逆向
1 篇文章 0 订阅
订阅专栏

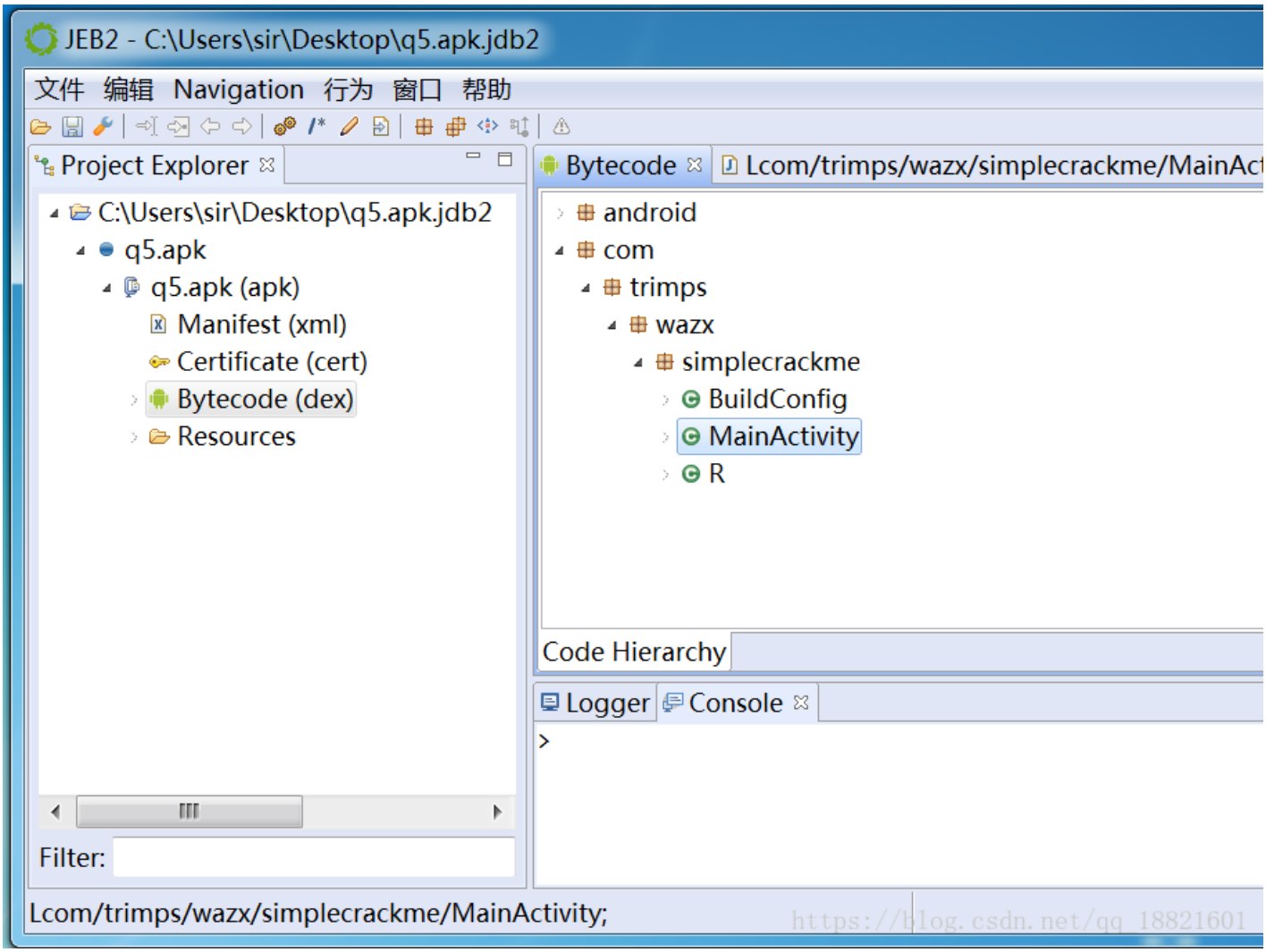
CTF小白，刚入坑，记录一下做题的方法，写的比较详细，大牛请轻喷。

题目：

> 这是个用来保存秘密的app，但是好像暴露了密码算法，你能找到密码吗？答案格式whaleCTF{xxxx}

下载文件后，首先在模拟器中打开运行一下，需要输入通关密码，随便输入一段提示“错误”

接下来使用jeb打开文件，进行反编译，查看MainActivity函数。



在代码中发现关键调用了check2函数，所以对check2函数进行分析：

```
MainActivity.this.check2(MainActivity.this.editText.getText().toString());
```

check2函数如下：

```
public void check2(String arg15) {
     String v5;
     int v4 = 0;
     int[] v7 = new int[16];
     int v3 = 16;
     int v1 = 5;
     v7[2] = 3;
     v7[7] = 4;
     v7[3] = 8;
     v7[1] = 10;
     v7[10] = 11;
     v7[0] = 15;
     v7[11] = 20;
     v7[6] = 20;
     v7[8] = 21;
     v7[15] = 24;
     v7[12] = 30;
     v7[13] = v3;
     v7[4] = 3;
     v7[14] = v3;
     v7[9] = 3;
     v7[5] = 89;
     if(arg15.length() != 16) {
         throw new RuntimeException();
     }

     try {
         v5 = this.getKey();
     }
     catch(Exception v0) {
         v5 = this.getKey();
         System.arraycopy(v5, 0, arg15, v1, v1);
     }

     while(v4 < arg15.length()) {
         if((v7[v4] & 255) != ((arg15.charAt(v4) ^ v5.charAt(v4 % v5.length())) & 255)) {
             throw new RuntimeException();
         }

         ++v4;
     }
 }
```

从 arg15.length() != 16 这里可以确定要求输入的字符串长度为16位。然后对v5进行了赋值，赋值为“foodluck”。

关键是while循环，对输入的字符串进行异或判断，于是使用python进行计算即可得到正确的字符串，payload如下：

```
# coding=utf-8
v4 = 0
v7 = [0]*16
v3 = 16
v1 = 5
v7[2] = 3
v7[7] = 4
v7[3] = 8
v7[1] = 10
v7[10] = 11
v7[0] = 15
v7[11] = 20
v7[6] = 20
v7[8] = 21
v7[15] = 24
v7[12] = 30
v7[13] = v3
v7[4] = 3
v7[14] = v3
v7[9] = 3
v7[5] = 89
v5 = 'goodluck'
flag = ''
while v4 < 16:
    flag += (chr(v7[v4] ^ ord(v5[v4 % len(v5)])))
    v4 += 1
print flag
```

运行即可得到flag：

hello,worldpress