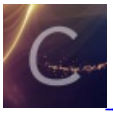
【WhaleCTF逆向题】第一期安卓加密writeup

原创

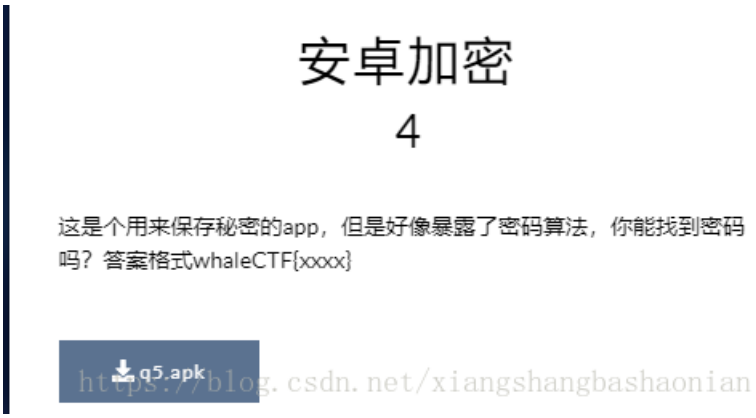
iqiqiya 于 2018-09-16 15:38:02 发布 886 收藏
分类专栏： 我的逆向之路 我的CTF之路 ------WhaleCTF 我的CTF进阶之路 文章标签： 【WhaleCTF逆向题】第一期安卓加密writeup 安卓加密writeup 【WhaleCTF逆向题】 writeup


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

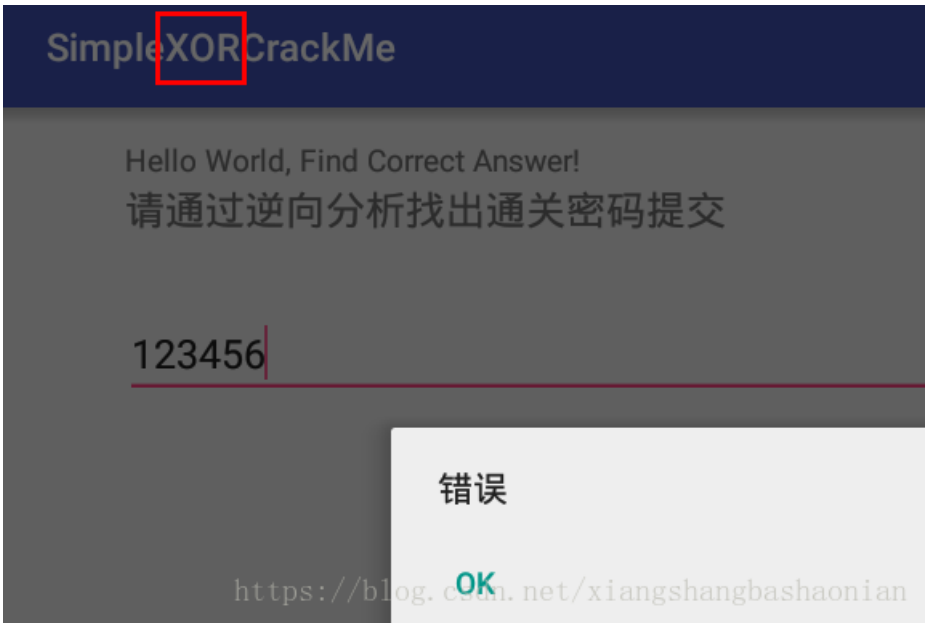

我的CTF之路
92 篇文章 5 订阅
订阅专栏


------WhaleCTF
8 篇文章 0 订阅
订阅专栏

题目信息如下：



安装到模拟器可以明显看出用的XOR运算



JEB载入　发现关键在check2　check1这个方法一点用也没有。。。

```
protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    this.setContentView(2130968601);
    this.editText = this.findViewById(2131492945);
    this.findViewById(2131492946).setOnClickListener(new View$OnClickListener() {
        public void onClick(View view) {
            DialogInterface$OnClickListener v1 = null;
            try {
                MainActivity.this.check2(MainActivity.this.editText.getText().toString());
                new AlertDialog$Builder(MainActivity.this).setMessage("正确").setNeutralButton("OK",
                        null).create().show();
            }
            catch(Exception v0) {
                new AlertDialog$Builder(MainActivity.this).setMessage("错误").setNeutralButton("OK",
                        v1).create().show();
            }
        }
    });
}
```


那我们就看看check2是怎样运算的

```
public void check2(String s) {
    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(s.length() != 16) {//我们的input长度必须等于16
        throw new RuntimeException();
    }

    try {
        v5 = this.getKey();//这里会调用getKey()这个方法 给v5赋值
    }
    catch(Exception v0) {
        v5 = this.getKey();
        System.arraycopy(v5, 0, s, v1, v1);
    }

    while(v4 < s.length()) {//v4相当于循环变量i  charAt()是获取对应位置字符 下面就是异或
        if((v7[v4] & 255) != ((s.charAt(v4) ^ v5.charAt(v4 % v5.length())) & 255)) {
            throw new RuntimeException();
        }

        ++v4;
    }
}
```

那我们来看看v5的值

```
public String getKey() {
    return "goodluck";//v5的值
}
```

python代码如下：

直接把v7这个数组从jeb抠出来比较省事

```
#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 = ''
#b= []
#a[i] & 255 == (s[i] ^ v5[i % len(v5)]) & 255
for i in range(0,len(v7)):
 flag += chr(v7[i] ^ ord(v5[i % len(v5)]))
 #b.append(chr(v7[i] ^ ord(s[i % len(s)])))
print flag
#print b
```

```
D64)] on win32
Type "copyright", "credits
>>>
=================== RESTAR
hello,worldpress
>>>
```