

【jarvisoj刷题之旅】逆向题目[61dctf]androideeasy的writeup

原创

iqiqiya 于 2018-09-09 15:38:40 发布 收藏 1
分类专栏: 我的CTF之路 我的逆向之路 我的CTF进阶之路 文章标签: jarvisoj的逆向题目androideeasy的writeup jarvisoj androideeasy reverse

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/82558864>

版权



我的CTF之路 同时被 3 个专栏收录

92 篇文章 5 订阅

订阅专栏



我的逆向之路

108 篇文章 10 订阅

订阅专栏

我的CTF进阶之路

108 篇文章 18 订阅

订阅专栏

题目名字androideeasy 那么猜测就是一个apk

winhex打开后果然是

改下后缀 载入Androidkiller

The screenshot shows the Androidkiller tool interface. The top menu bar includes '文件' (File), '打开' (Open), '隐藏面板' (Hide Panel), '视图' (View), '配置' (Configure), and '关于' (About). The main window has tabs for '开始' (Start) and 'androideeasy'. The left sidebar displays project information: '名称: AndroidTest', '包名: com.a.sample.androidtest', and '入口: com.a.sample.androidtest.MainActivity'. It also lists 'Activity' (com.a.sample.androidtest.MainActivity), 'Receiver', 'Service', and 'Uses-Permission' (android.permission.RECEIVE_BOOT_C). The right pane shows the decompiled code of MainActivity.smali:

```
.class public Lcom/a/sample/androidtest/MainActivity;
.super Landroid/support/v7/app/AppCompatActivity;
.source "MainActivity.java"

# instance fields
.field private editText:Landroid/widget/EditText;

.field private s:[B

# direct methods
.method public constructor <init>()V
.locals 1
.prologue
.line 10
.invoke-direct {<b0>} Landroid/support/v7/app/AppCompatActivity:-><init>()V
```

At the bottom of the code pane, it says '行: 42 列: 25 插入' and 'https://blog.csdn.net/xiangshangashaonian...'.

直接看java源码

```
protected void onCreate(Bundle savedInstanceState)
{
    super.onCreate(savedInstanceState);
    setContentView(2130968603);
    this.editText = ((EditText)findViewById(2131427415));
    findViewById(2131427416).setOnClickListener(new View.OnClickListener()
    {
        public void onClick(View paramAnonymousView)
        {
            if (MainActivity.this.check())
                Toast.makeText(jdField_this, "You got the flag!", 1).show();
            for (;;)
            {
                return;
                Toast.makeText(jdField_this, "Sorry your flag is wrong", 1).show();
            }
        }
    });
}
```

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

明显可以看出关键就在check()方法

```
private EditText editText;
private byte[] s = { 113, 123, 118, 112, 108, 94, 99, 72, 38, 68, 72, 87, 89, 72, 36, 118, 100, 78, 72, 87, 121, 83, 101, 39, 62, 94, 62, 38, 107, 115, 106 };

public boolean check()
{
    boolean bool1 = false;
    byte[] arrayOfByte = this.editText.getText().toString().getBytes();
    boolean bool2;
    if (arrayOfByte.length != this.s.length)
        bool2 = bool1;
    for (;;)
    {
        return bool2;
        for (int i = 0;; i++)
        {
            if ((i >= this.s.length) || (i >= arrayOfByte.length))
                break label75;
            bool2 = bool1;
            if (this.s[i] != (arrayOfByte[i] ^ 0x17))
                break;
        }
        label75:
        bool2 = true;
    }
}
```

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

很明显就是一个简单的异或运算

那么我们只要将byte[] s的每一个字符与0x17异或即可得到flag

Py代码:

```
a = [113, 123, 118, 112, 108, 94, 99, 72, 38, 68, 72, 87, 89, 72, 36, 118, 100, 78, 72, 87, 121, 83, 101, 39, 62, 94, 62, 38, 107, 115, 106]
flag = ''
for i in range(0,31):
    flag += chr(a[i] ^ 0x17)
    #print(ord(c[i]))
print(flag)
```

最后提交，正确

[61dctf]androideeasy

156 SOLVERS

50

REVERSE

androideeasy.apk.17e528e9498d4ae25dc82ad43730a03d

SUBMIT

Correct Answer!!Congratulations!

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