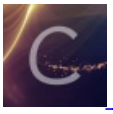
【jarvisoj刷题之旅】逆向题目[61dctf]androideasy的writeup

原创

iqiqiya 于 2018-09-09 15:38:40 发布 520 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androideasy的write androideasy的writeup jarvisoj androideasy reverse


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

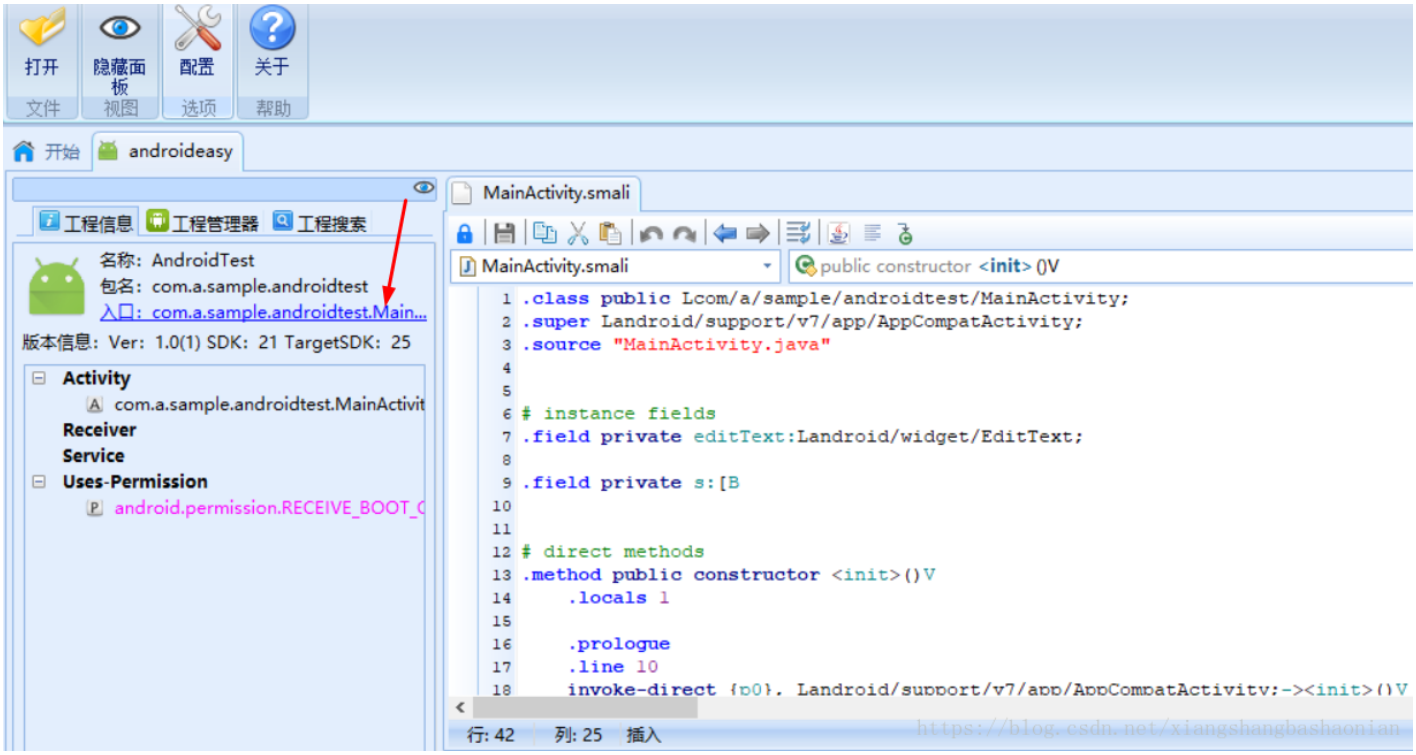

我的逆向之路
108 篇文章 10 订阅
订阅专栏

我的CTF进阶之路
108 篇文章 18 订阅
订阅专栏

题目名字androideasy　那么猜测就是一个apk

winhex打开后果然是

改下后缀　载入Androidkiller



直接看java源码

```
protected void onCreate(Bundle paramBundle)
{
  super.onCreate(paramBundle);
  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();
      }
    }
  });
```


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 label175;
      }
      bool2 = bool1;
      if (this.s[i] != (arrayOfByte[i] ^ 0x17)) {
        break;
      }
    }
    label175:
    bool2 = true;
  }
```


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, 3
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]androideasy 156 SOLVERS 50 REVERSE

androideasy.apk.17e528e9498d4ae25dc82ad43730a03d

flag{It_1S_@N_3asY_@nDr0)l)1|d} SUBMIT

Correct Answer!!Congratulations!