[BUGKU][CTF][Reverse][2020] Reverse writeup 1-7 暂时肝不动了

原创

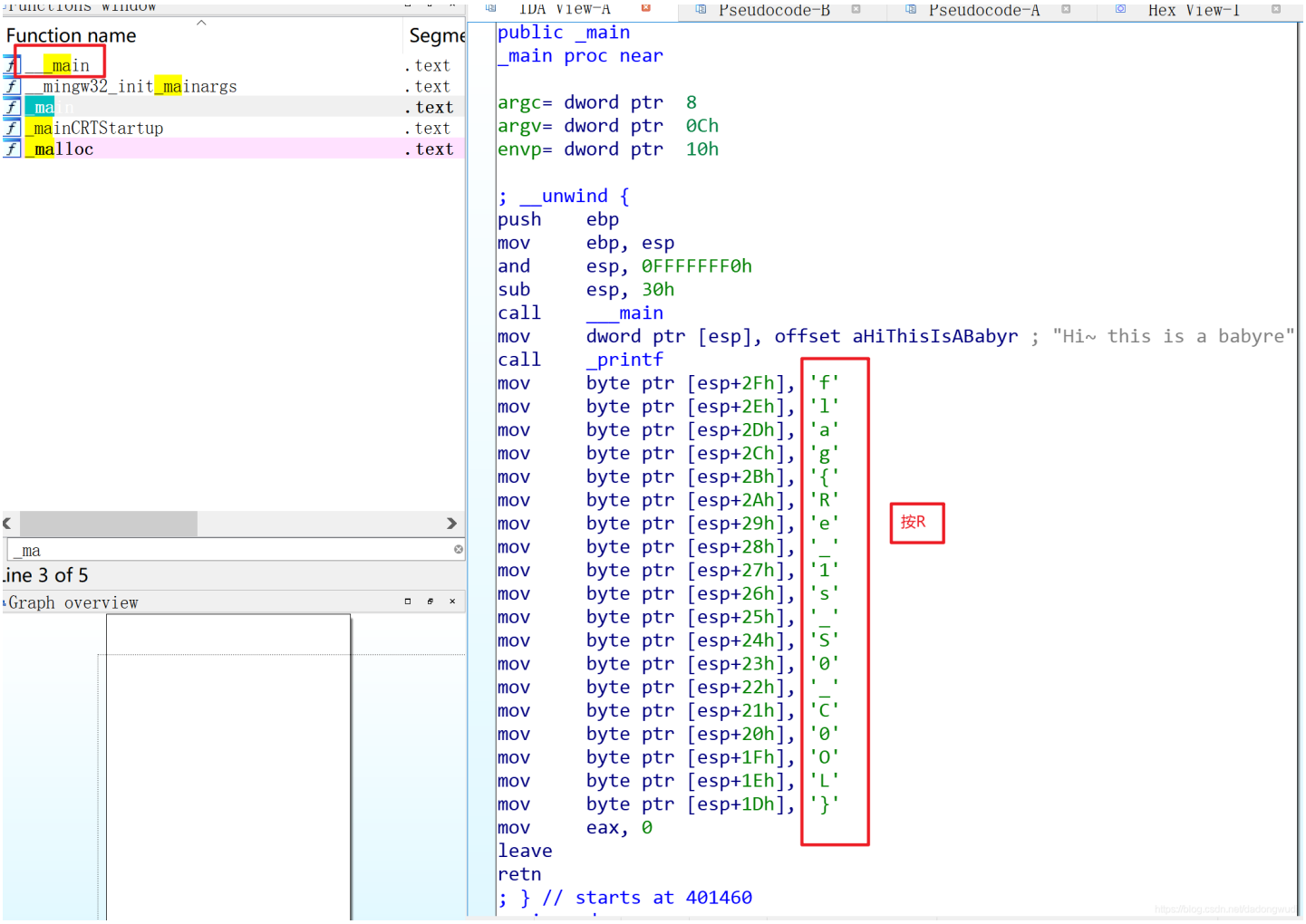
CryptWinter 于 2021-01-14 15:59:44 发布 256 收藏 1

分类专栏： CTF 文章标签： BUGKU CTF 2020 Reverse writeup

本文链接：https://blog.csdn.net/dadongwudi/article/details/112599804

Reverse 入门逆向

步骤: ida main函数 按R



Reverse signin

关键字：

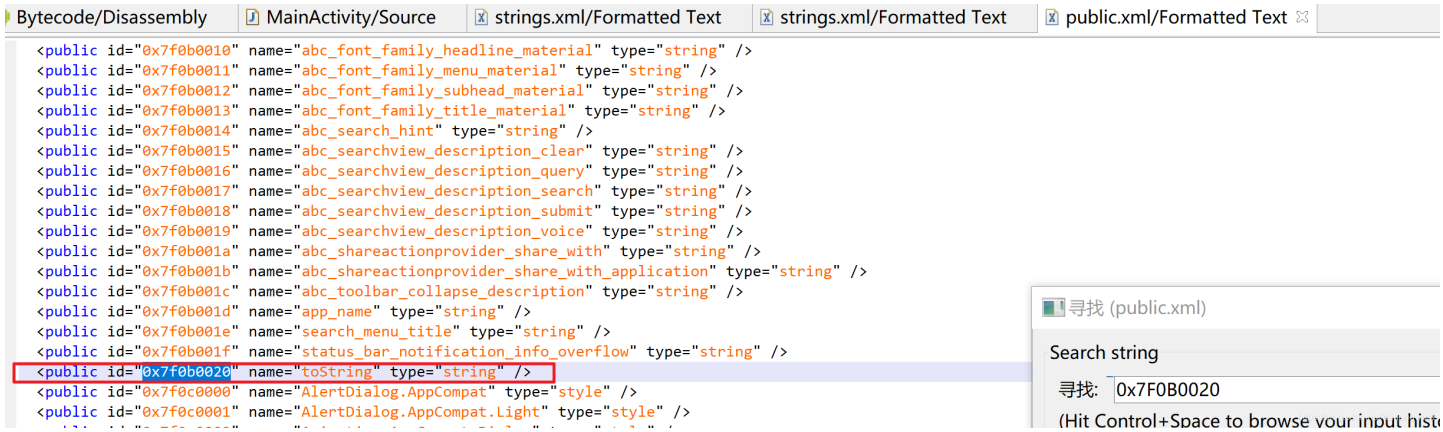
知识点：Android逆向分析。（常用工具：安卓模拟器、JEB、Cyberchef、Androidkiller）

步骤:

步骤：

1.用jeb打开，找到MainActivity，右键解析成java分析 ,需要反转后tostring()

2. 用jeb打开，找到MainActivity，右键解析成java分析



```
    <string>991YiZWOz81ZhFjZfJXdwk3X1k2XzIXZIt3ZhxmZ</string>
</resources>
```


3.在线或者使用脚本反转 ,base64解码

```
a ='991YiZWOz81ZhFjZfJXdwk3X1k2XzIXZIt3ZhxmZ'

b = ''

b = a[::-1]

print(b)
```

ZmxhZ3tIZXIzX2k1X3kwdXJfZjFhZ18zOWZiY199

编码 base64

flag{Her3_i5_y0ur_flag_39fbc_}

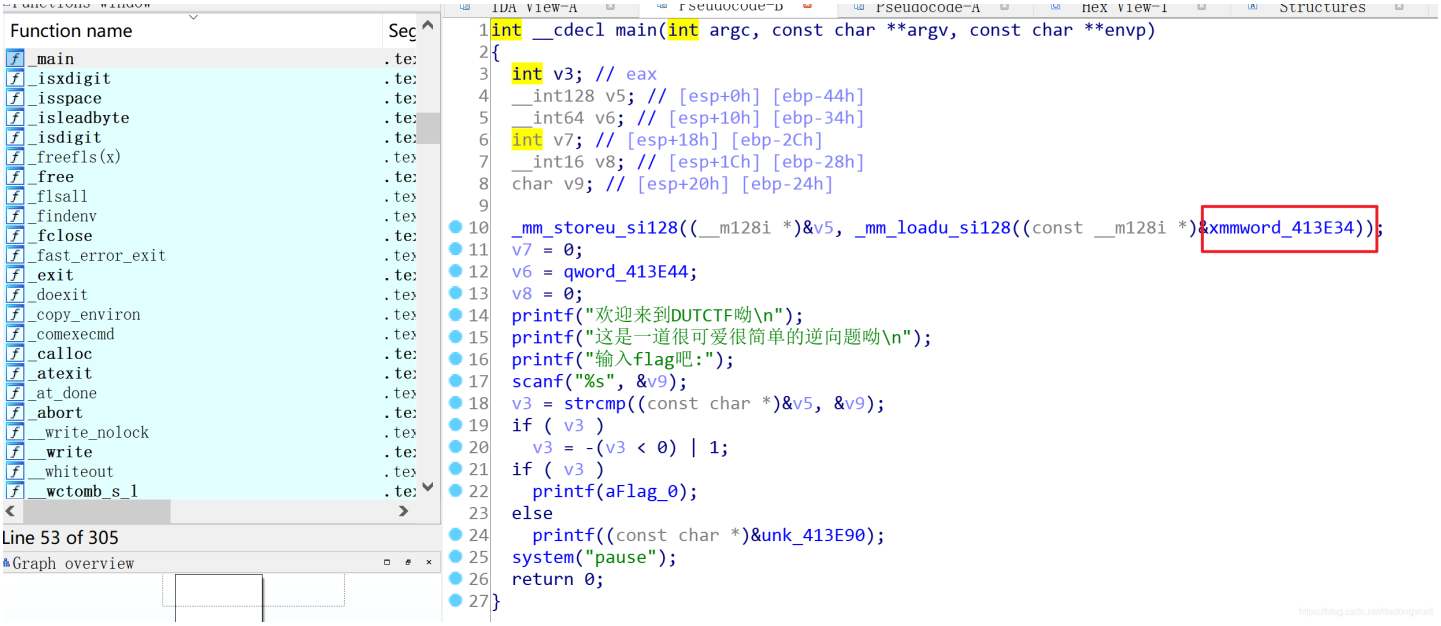
参考链接:https://www.cnblogs.com/myqzs/p/13724482.html

Reverse EASY re

关键字：ida

步骤:

1.main f5 F5翻译为伪C代码



2.strcmp()对面输入的值是否等于xmmword_413E34位置的值，双击xmmword_413E34 跟过去，发现了flag （按R显示字符串）

```
.rdata:00413E34 xmmword_413E34  xmmword '0tem0c1eW{FTCTUD'
.rdata:00413E34                                         ; DATA XREF: _main+10↑r
.rdata:00413E44 qword_413E44    dq '}FTCTUD'            ; DATA XREF: _main+27↑r
.rdata:00413E4C ; char aDutctf[]
.rdata:00413E4C aDutctf         db '欢迎来到DUTCTF呦',0Ah,0  ; DATA XREF: _main+1A↑o
.rdata:00413E5E                 align 10h
.rdata:00413E60 ; char asc_413E60[]
.rdata:00413E60 asc_413E60      db '这是一道很可爱很简单的逆向题呦',0Ah,0
.rdata:00413E60                                         ; DATA XREF: _main+3D↑o
.rdata:00413E80 ; char aFlag[]
.rdata:00413E80 aFlag           db '输入flag吧:',0          ; DATA XREF: _main+47↑o
.rdata:00413E8C ; char aS[]
.rdata:00413E8C aS              db '%s',0               ; DATA XREF: _main+55↑o
.rdata:00413E8F                 align 10h
.rdata:00413E90 unk_413E90      db  66h ; f             ; DATA XREF: _main+91↑o
.rdata:00413E91                 db  6Ch ; l
.rdata:00413E92                 db  61h ; a
```

3.字符串拼接后反转 ， 得到flag

DUTCTF{We1c0met0DUTCTF}

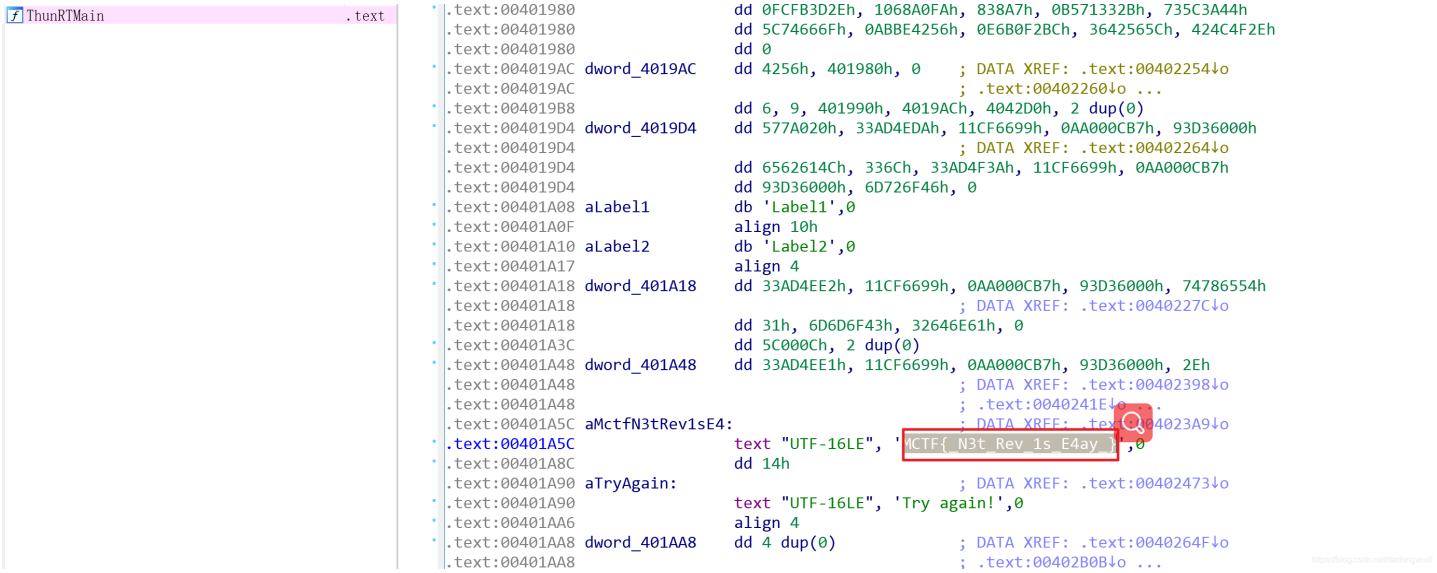
思路二：解压得到一个可执行文件，然后用Notepad++打开，直接搜索DUTCTF即可得到

Reverse Easy_vb

关键字：ida

步骤:

ida 打开 往下翻 MCTF 替换 flag



Reverse Timer(阿里CTF)

关键字：

知识点：

步骤:

1.下载文件发现是apk，先安装运行下发现有一个倒计时，只是时间为200000秒。猜测是让时间走完获取flag。

2.JEB查看

```
package net.bluelotus.tomorrow.easyandroid;

import android.os.Bundle;
import android.os.Handler;
import android.support.v7.app.AppCompatActivity;
import android.view.Menu;
import android.view.MenuItem;
import android.widget.TextView;

public class MainActivity extends AppCompatActivity {
    int beg = (((int) (System.currentTimeMillis() / 1000)) + 200000);
    int k = 0;
    int now;
    long t = 0;

    public native String stringFromJNI2(int i);

    public static boolean is2(int n) {
        if (n <= 3) {
            if (n > 1) {
                return true;
            }
            return false;
        } else if (n % 2 == 0 || n % 3 == 0) {
            return false;
        } else {
            int i = 5;
```

```
            while (i * i <= n) {
                if (n % i == 0 || n % (i + 2) == 0) {
                    return false;
                }
                i += 6;
            }
            return true;
        }
    }

    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView((int) R.layout.activity_main);
        final TextView tv1 = (TextView) findViewById(R.id.textView2);
        final TextView tv2 = (TextView) findViewById(R.id.textView3);
        final Handler handler = new Handler();
        handler.postDelayed(new Runnable() {
            public void run() {
                MainActivity.this.t = System.currentTimeMillis();
                MainActivity.this.now = (int) (MainActivity.this.t / 1000);
                MainActivity.this.t = 1500 - (MainActivity.this.t % 1000);
                tv2.setText("AliCTF");
                if (MainActivity.this.beg - MainActivity.this.now <= 0) {
                    tv1.setText("The flag is:");
                    tv2.setText("alictf{" + MainActivity.this.stringFromJNI2(MainActivity.this.k) + "}");
                }
                MainActivity mainActivity;
                if (MainActivity.is2(MainActivity.this.beg - MainActivity.this.now)) {
                    mainActivity = MainActivity.this;
                    mainActivity.k += 100;
                } else {
                    mainActivity = MainActivity.this;
                    mainActivity.k--;
                }
                tv1.setText("Time Remaining(s):" + (MainActivity.this.beg - MainActivity.this.now));
                handler.postDelayed(this, MainActivity.this.t);
            }
        }, 0);
    }

    public boolean onCreateOptionsMenu(Menu menu) {
        getMenuInflater().inflate(R.menu.menu_main, menu);
        return true;
    }

    public boolean onOptionsItemSelected(MenuItem item) {
        if (item.getItemId() == R.id.action_settings) {
            return true;
        }
        return super.onOptionsItemSelected(item);
    }

    static {
        System.loadLibrary("lhm");
    }
}
```

首先初始化了beg为当前时间加上200000。`(System.currentTimeMillis() / 1000)`是获得系统的时间，单位为毫秒,转换为秒。

看`onCreate`方法，找到关键处

```
if (MainActivity.this.beg - MainActivity.this.now <= 0) {
                    tv1.setText("The flag is:");
                    tv2.setText("alictf{" +
MainActivity.this.stringFromJNI2(MainActivity.this.k) + "}");
                }
```

所以`MainActivity.this.beg - MainActivity.this.now <= 0`就是过了得时间。如果过了200000秒则出现flag。flag是使用native层来打印。

思路：能不能直接跳过200000秒直接出现flag呢?

有一个关键变量`k`，往下看，看看k有没有什么运算。

```
if (MainActivity.is2(MainActivity.this.beg - MainActivity.this.now)) {
                    mainActivity = MainActivity.this;
                    mainActivity.k += 100;
                } else {
                    mainActivity = MainActivity.this;
                    mainActivity.k--;
                }
```

将差值用is2函数判断，如果true，就k+100 ,如果false,就k-1。那就要看下is2函数

```
public static boolean is2(int n) {
        if (n <= 3) {
            if (n > 1) {
                return true;
            }
            return false;
        } else if (n % 2 == 0 || n % 3 == 0) {
            return false;
        } else {
            int i = 5;
            while (i * i <= n) {
                if (n % i == 0 || n % (i + 2) == 0) {
                    return false;
                }
                i += 6;
            }
            return true;
        }
    }
```


直接照着写一个即可，然后可以算出关键变量k

解密脚本，算出k = 1616384

```
def is2(n):
    if(n <= 3):
        if(n > 1):
            return True
        return False
    elif(n % 2 == 0 or n % 3 == 0):
        return False
    else:
        i = 5
        while(i * i <= n):
            if (n % i == 0 or n % (i + 2) == 0):
                return False
            i += 6
    return True

k=0

for i in  range(200000,0,-1):
    k = k + 100 if is2(i) else k - 1
print(k)
```

```
(base) PS D:\CTF\script> python .\ali.py
1616384
```

3. 实现

的话，用Androidkiller打开项目，因为跳转后输出了The flag is,所以搜索该字符串,双击跟过去

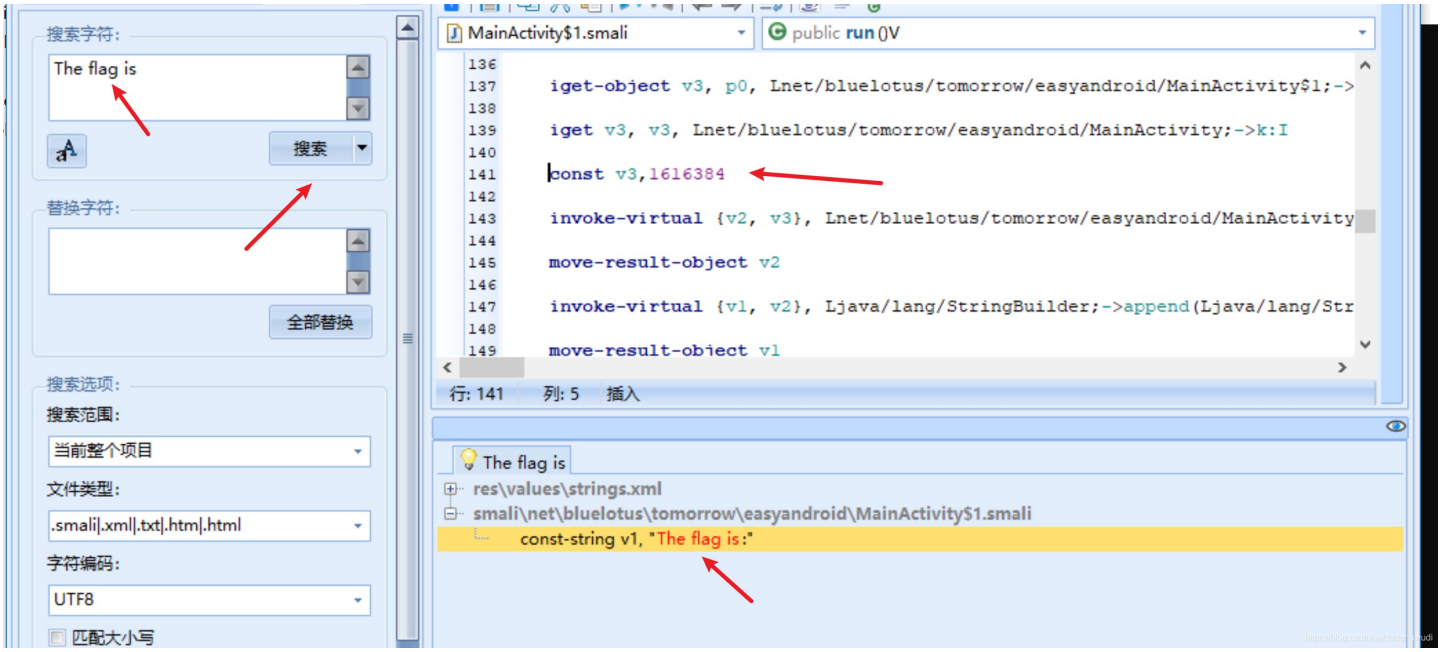
3.1 第113行的if-gtz v0, :cond_0。 if-ltz是如果大于0跳转 ，那改成如果小于0跳转就跳过了200000秒等待了。对应的语句为if-ltz v0, :cond_0。

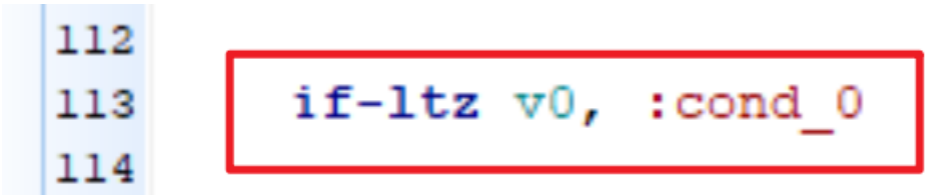
3.2 然后要找到赋值k的位置，看第129行-149行，因为k的值是在alictf{和}之间传入的。

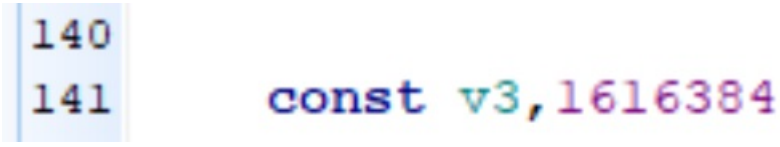
看到了139行的的iget v3, v3, Lnet/bluelotus/tomorrow/easyandroid/MainActivity;->k:I，知道v3是k的值。

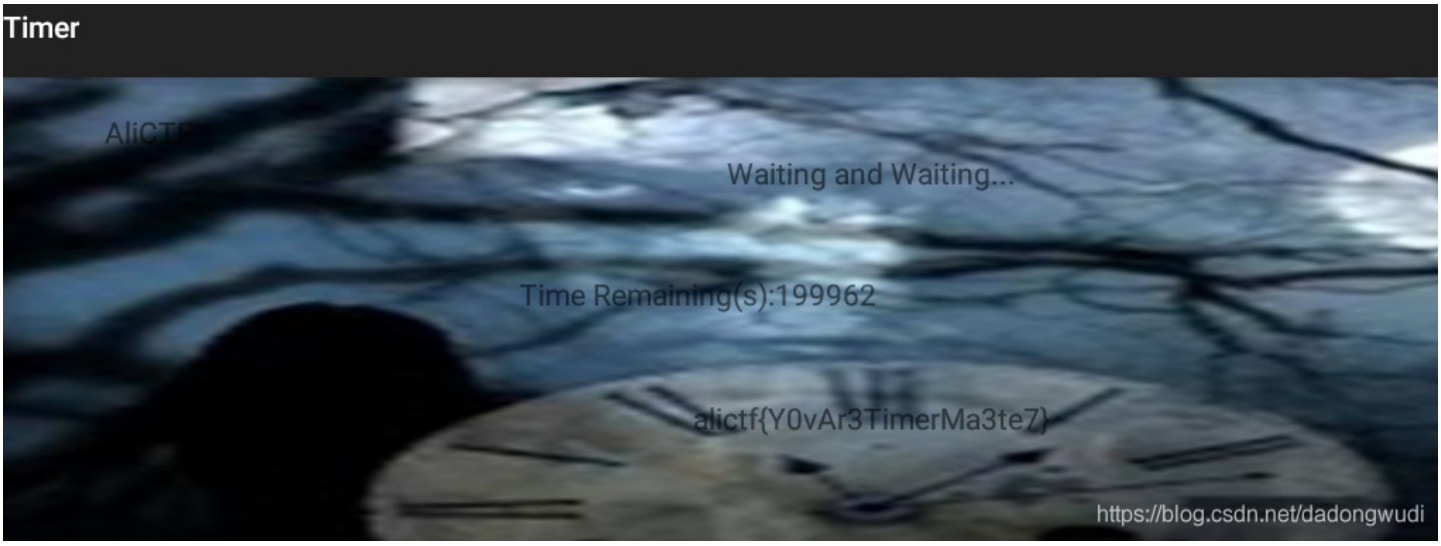
于是在下面赋值const v3,1616384

然后保存，编译，安装运行就出现flag。（jdk=1.8 apktool>=2.3）







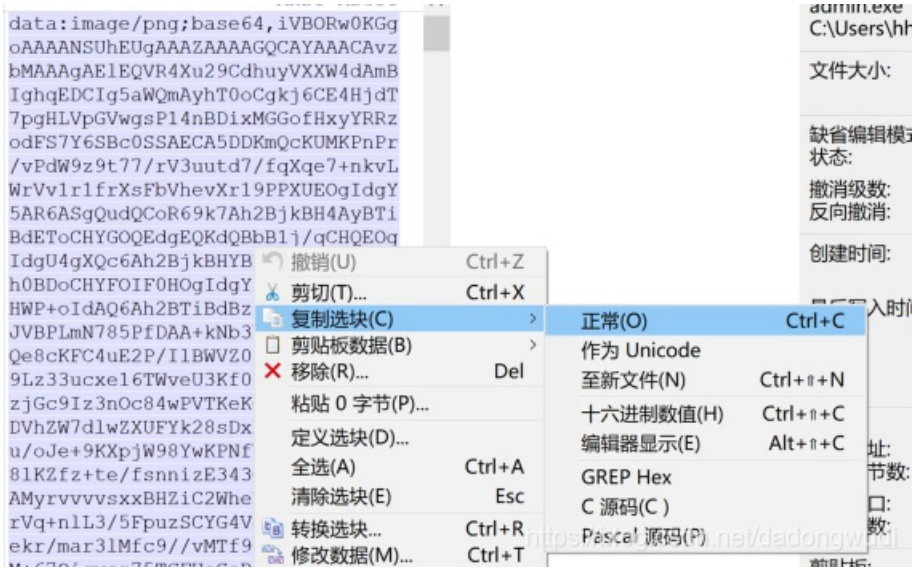


Reverse 逆向入门

关键字：winhex

步骤:

1.winhex 打开 复制黏贴到浏览器



2.QR扫描出结果


自动扩张
尺寸(M)
4
图片像素
148 × 148
编码(C)
DoCoMo
电话簿信息
电子邮件
网页书签
文本信息
bugku{inde_9882ihsd8-0}

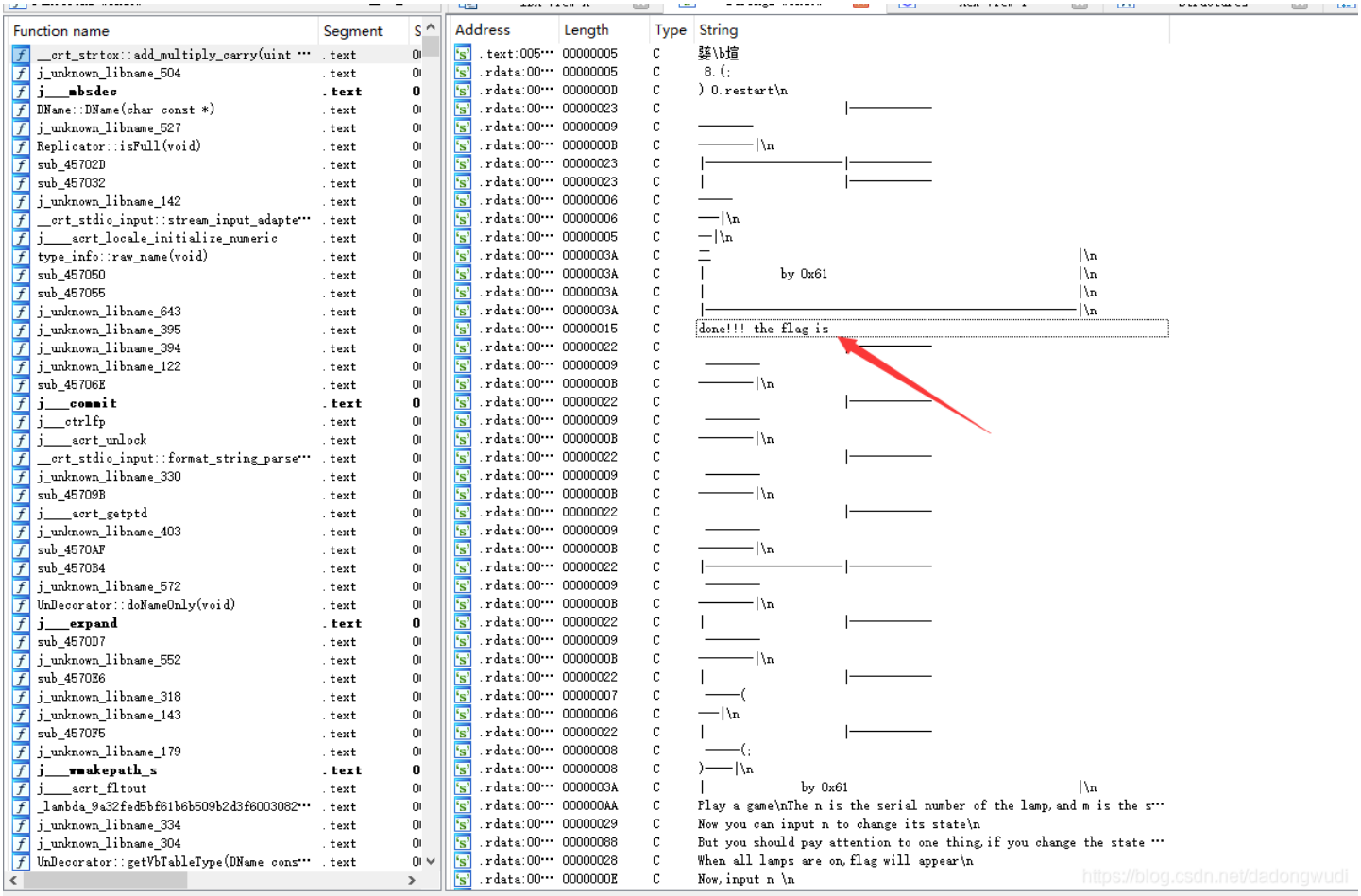
Reverse 游戏过关

关键字：ida

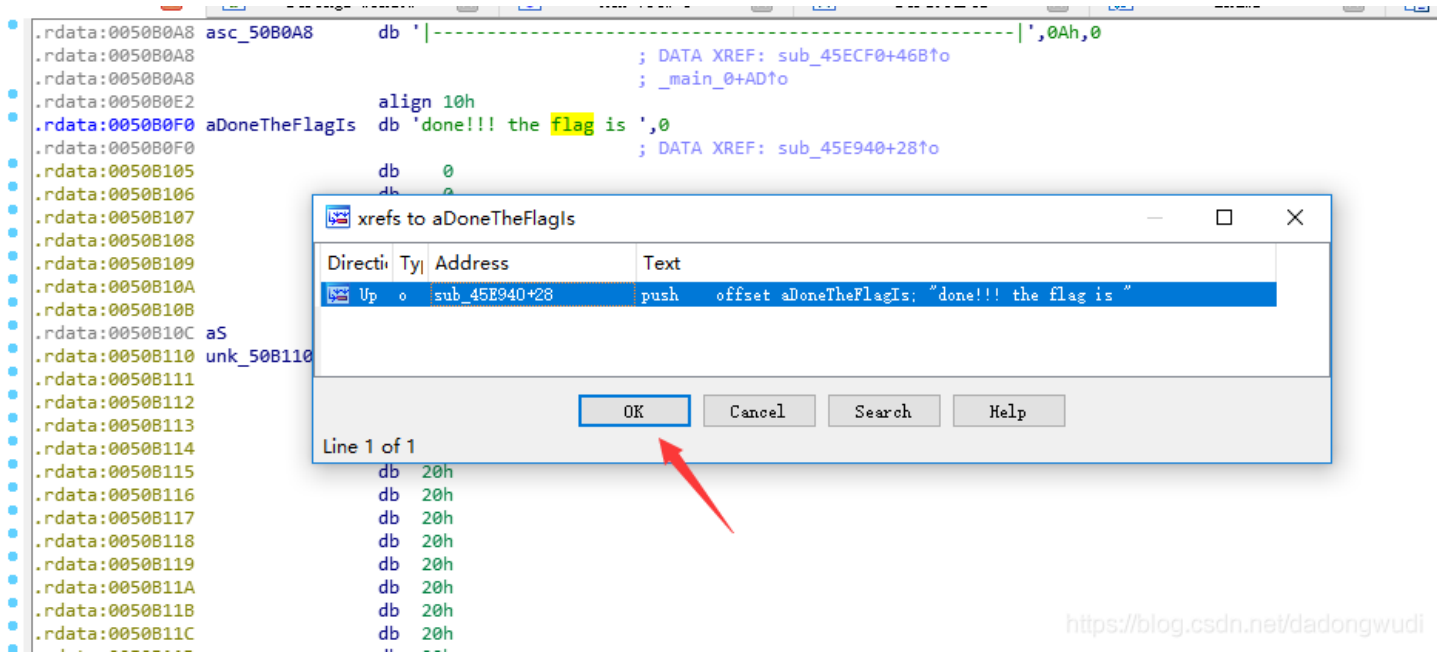
步骤:

1.首先就是看运行遍程序，了解下程序流程以及关键字符串。然后打开ida

Shift+F12查看下字符串，然后双击过去



2.按Cirt+X交叉引用显示调用位置



3.F5看下伪代码，两个数组按位异或再和0x13异或生成flag

```
array1 = [18,64,98,5,2,4,6,3,6,48,49,65,32,12,48,65,31,78,62,32,49,32,1,57,96,3,21,9,4,62,3,5,4,1,2,3,44,65,78,3
2,16,97,54,16,44,52,32,64,89,45,32,65,15,34,18,16,0]
array2 = [123,32,18,98,119,108,65,41,124,80,125,38,124,111,74,49,83,108,94,108,84,6,96,83,44,121,104,110,32,95,1
17,101,99,123,127,119,96,48,107,71,92,29,81,107,90,85,64,12,43,76,86,13,114,1,117,126,0]

flag = ''
for i in range(len(array1)):
    flag+= chr(array1[i] ^ array2[i] ^ 0x13 )
print(flag)
```

Reverse
关键字：
知识点：
步骤:

Reverse
关键字：
知识点：
步骤:

Reverse
关键字：
知识点：
步骤:

Reverse
关键字：
知识点：
步骤:

Reverse
关键字：
知识点：
步骤:

Reverse
关键字：
知识点：
步骤:

参考链接：
https://www.codeqq.com/log/7Zjb2O7Z.html

https://blog.csdn.net/ahilll/article/details/84787700