

# XCTF攻防世界 MISC jpg rctf-2015解题记录

原创

[UYU](#) 于 2021-09-10 20:29:21 发布 172 收藏

分类专栏: [CTF类笔记](#)

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/qq\\_35780686/article/details/120220092](https://blog.csdn.net/qq_35780686/article/details/120220092)

版权



[CTF类笔记](#) 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

## XCTF攻防世界 MISC jpg 解题记录

最近一直在闲暇之余做一些misc的题来充实一下生活, 解题的同时顺便做一下记录。

原题描述很简单 下载附件

jpg 建议

难度系数: ★★★★★★★★★★ 10

题目来源: RCTF-2015

题目描述: flag需要包含RCTF{}

题目场景: 暂无

题目附件: 附件1

CSDN @\_UYU\_

用foremost处理后得到两个文件



jpg



rar

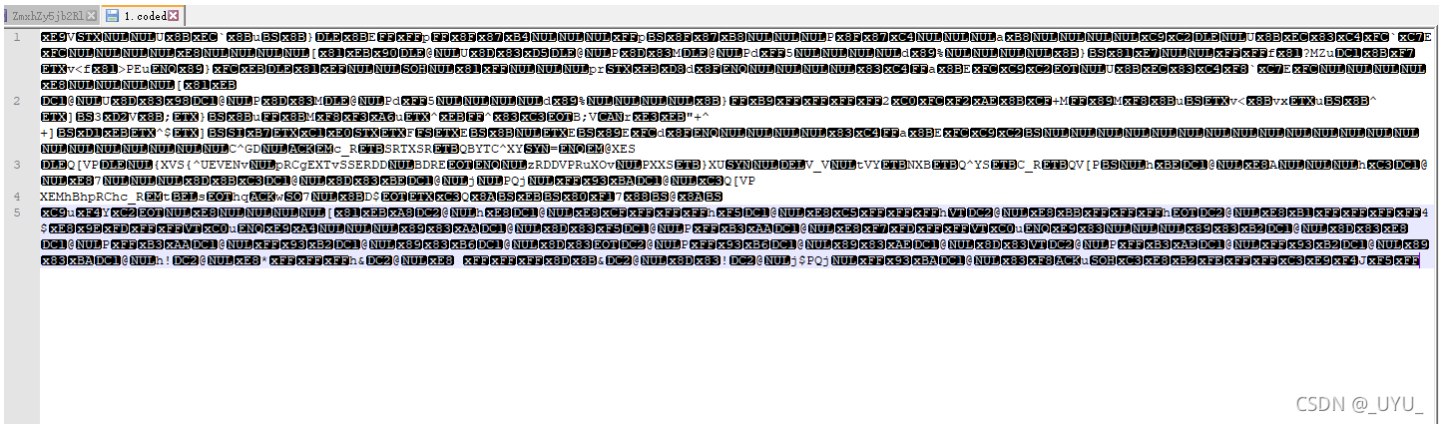


audit.txt

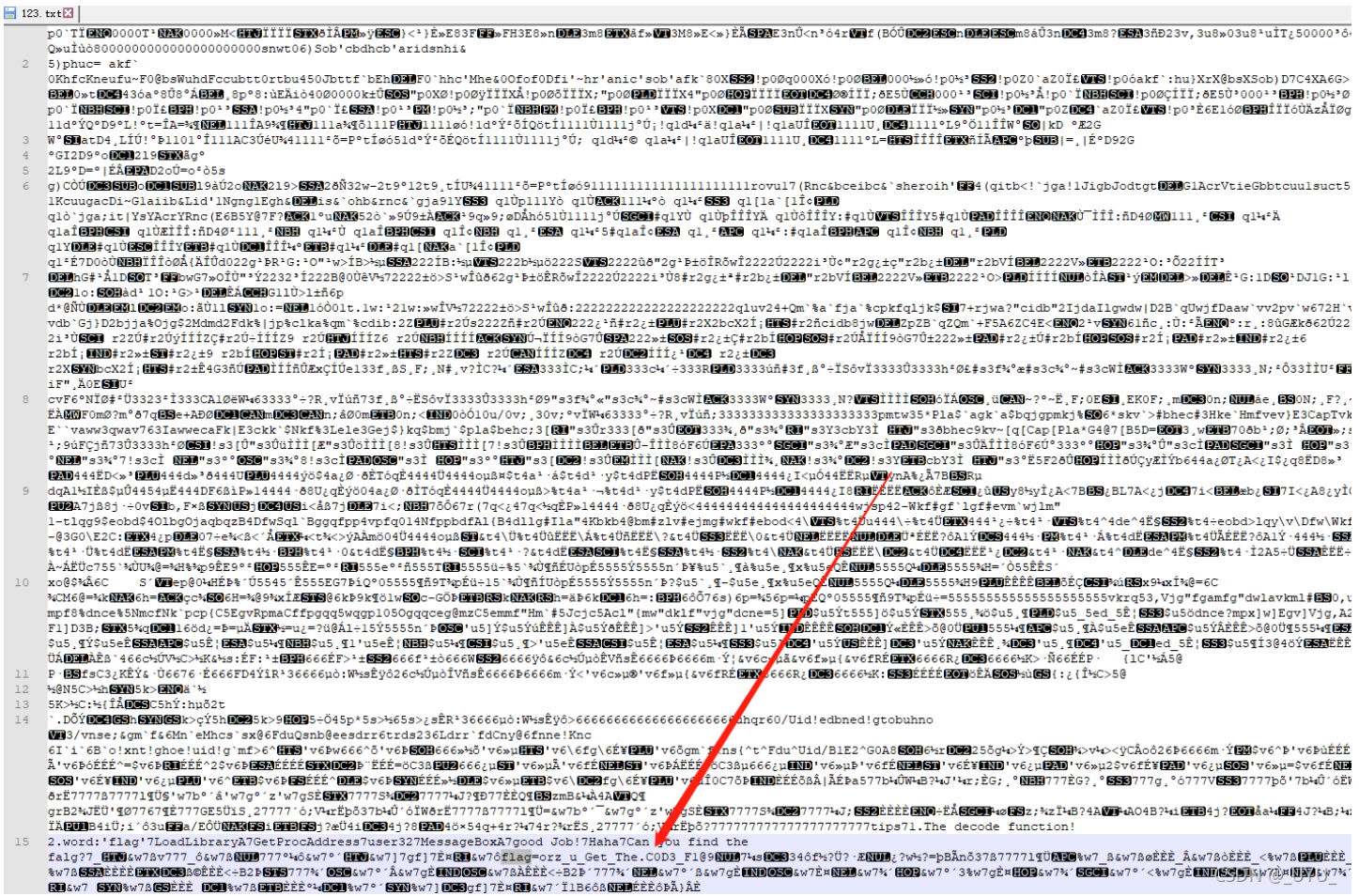
CSDN @\_UYU\_

rar暴力破解后得到口令123456



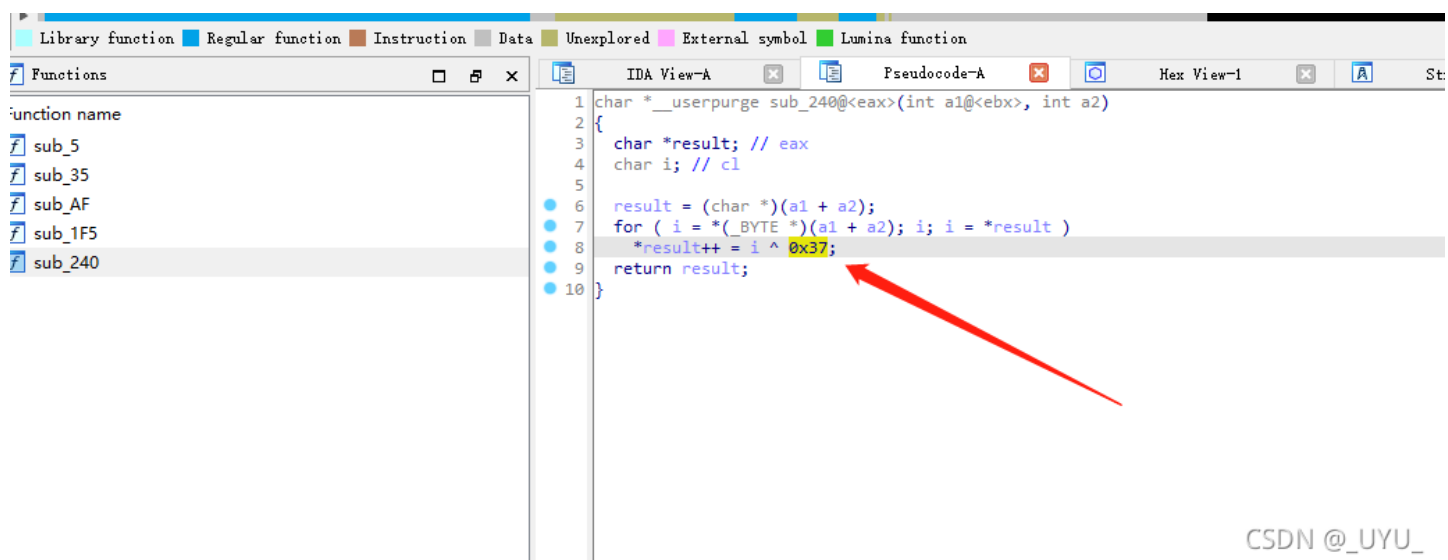


因为ZmxhZy5jb2Rl解码为flag.code,所以拖入ida 发现有变化(但奈何本人并不会逆向,所以此时与答案擦肩而过...)  
然后就是长达数小时的尝试,反码,补码,可见字符分析等等...终于在xor全部可见字符时找到了答案。



flag=orz\_u\_Get\_The.C0D3\_F1@9  
提交后通过  
虽然解出来了...但是基本上只是在猜...

顺便放上做逆向的大神后来给的关键截图...



The screenshot shows the IDA Pro interface with the following details:

- Functions List:** sub\_5, sub\_35, sub\_AF, sub\_1F5, sub\_240 (selected).
- Code View:**

```
1 char *__userpurge sub_240@<eax>(int a1@<ebx>, int a2)
2 {
3   char *result; // eax
4   char i; // cl
5
6   result = (char *) (a1 + a2);
7   for ( i = *(_BYTE *) (a1 + a2); i; i = *result )
8     *result++ = i ^ 0x37;
9   return result;
10 }
```
- Annotations:** Blue circular markers are present on lines 6, 7, 8, 9, and 10. The value `0x37` in line 8 is highlighted in yellow. A red arrow points from the right side of the image towards the `0x37` value.

CSDN @\_UYU\_