攻防世界 Reverse高手进阶区 2分题 re-for-50-plz-50

原创

思源湖的鱼 于 2020-12-05 15:53:43 发布 104 收藏 1
分类专栏： ctf 文章标签： ctf 攻防世界 reverse MIPS

本文链接：https://blog.csdn.net/weixin_44604541/article/details/110691511

前言

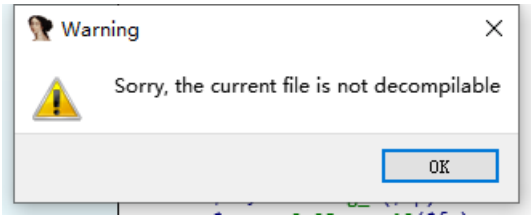
继续ctf的旅程
攻防世界Reverse高手进阶区的2分题
本篇是re-for-50-plz-50的writeup

发现攻防世界的题目分数是动态的
就仅以做题时的分数为准了

解题过程

PE查壳

扔进IDA



发现转不了伪代码

提示为MIPS
【十分钟教会你汇编】MIPS编程入门

```
loc_4013C8:
lui     $v0, 0x4A
addiu   $v1, $v0, (meow - 0x4A0000)  # "cbtcqLUBChERV[[Nh@_X^D]X_YPV[CJ"
lw      $v0, 0x28+var_10($fp)
addu    $v0, $v1, $v0
lb      $v1, 0($v0)
lw      $v0, 0x28+arg_4($fp)
addiu   $v0, 4
lw      $a0, 0($v0)
lw      $v0, 0x28+var_10($fp)
addu    $v0, $a0, $v0
lb      $v0, 0($v0)
xori    $v0, 0x37
sll     $v0, 24
sra     $v0, 24
beq     $v1, $v0, loc_401428
move    $at, $at
```


瞅着是把字符串取出和0x37进行异或

```
str="cbtcqLUBChERV[[Nh@_X^D]X_YPV[CJ"
flag=""
a=len(str)
for i in range(a):
    flag+=chr(0x37^ord(str[i]))
print (flag)
```

```
TUCTF{but_really_whoisjohngalt}
```

得到flag

结语

MIPS指令

网上有个Retdec插件
搞了好一会儿没装好
。。。