

看雪ctf晋级赛第一题wp

原创

rvOp111 于 2019-10-08 13:17:11 发布 125 收藏

分类专栏: [安全相关](#)

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/ZCMUCZX/article/details/102379215>

版权



[安全相关](#) 专栏收录该内容

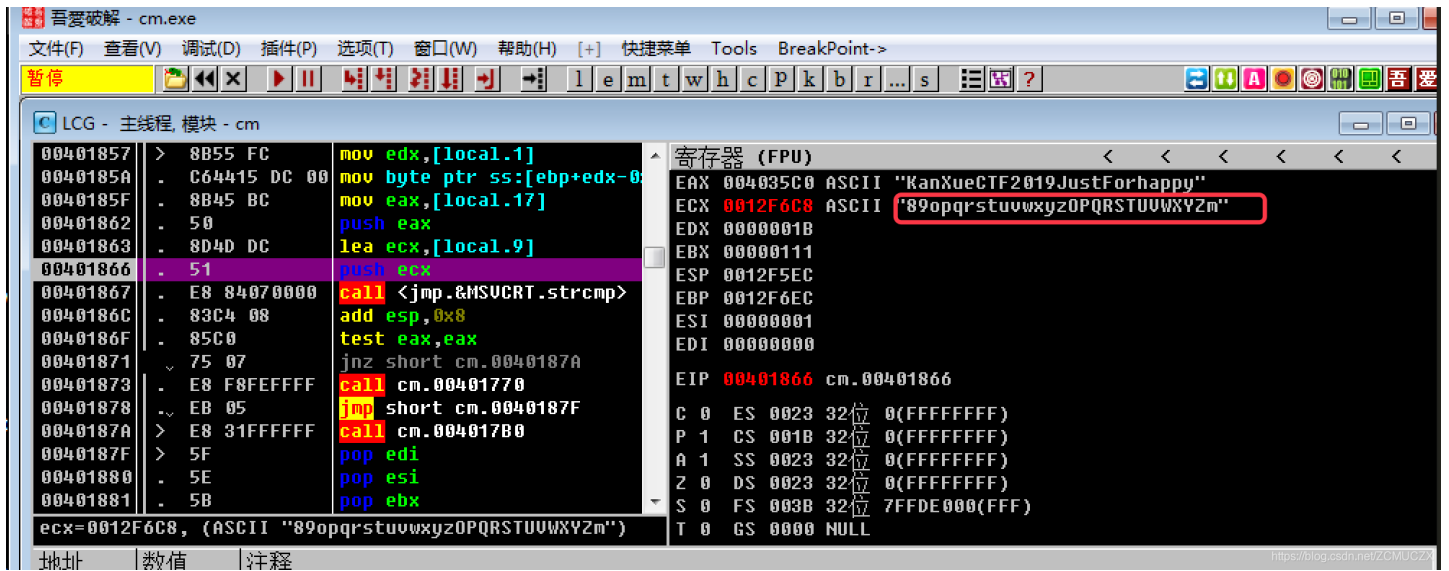
16 篇文章 0 订阅

订阅专栏

利用中文引擎搜索搜索到Kanxuectf这一串字符串的所在, 然后下断点

```
004017FB . 57 push edi
004017FC . C745 FC 0000 mov [local.1],0x0
00401803 . C745 F8 0000 mov [local.2],0x0
0040180A . C745 BC C035 mov [local.17],cm.004035C0 KanXueCTF2019JustForhappy
00401811 . C785 50FFFF mov [local.44],cm.00403580 abcdefghiABCDEFGHIJKLMNjklmn012345
00401818 > 8B45 FC mov eax,[local.1]
0040181E . 8B4D 08 mov ecx,[arg.1]
00401821 . 833C81 3E cmp dword ptr ds:[ecx+eax*4],0x3E
00401825 v 7D 30 jge short cm.00401857
00401827 . 8B55 FC mov edx,[local.1]
0040182A . 8B45 08 mov eax,[arg.1]
0040182D . 833C90 00 cmp dword ptr ds:[eax+edx*4],0x0
00401831 ~ 7C 24 jl short cm.00401857
00401833 . 8B4D FC mov ecx,[local.1]
00401836 . 8B55 08 mov edx,[arg.1]
00401839 . 8B048A mov eax,dword ptr ds:[edx+ecx*4]
```

之后就会发现它在和我们做比较, 然后我们输入的26个大写的英文字母变成了下面的内容



89opqrstuvwxyzOPQRSTUVWXYZm

然后我们就找到了下面的对应关系，然后我们需要从右边的字符串当中找到KanXueCTF2019JustForhappy，对应的左边的字符串

0 a

1 b

2 c

3 d

4 e

5 f

6 g

7 h

8 i

9 A

a B

b C

c D

d E

e F

f G

h I

i J

jK

kL

lM

mN

nj

ok

pl

qm

rn

s0

t1

u2

v3

w4

x5

y6

z7

A8

B9

Co

Dp

Eq

Fr

Gs

Ht

Iu

Jv

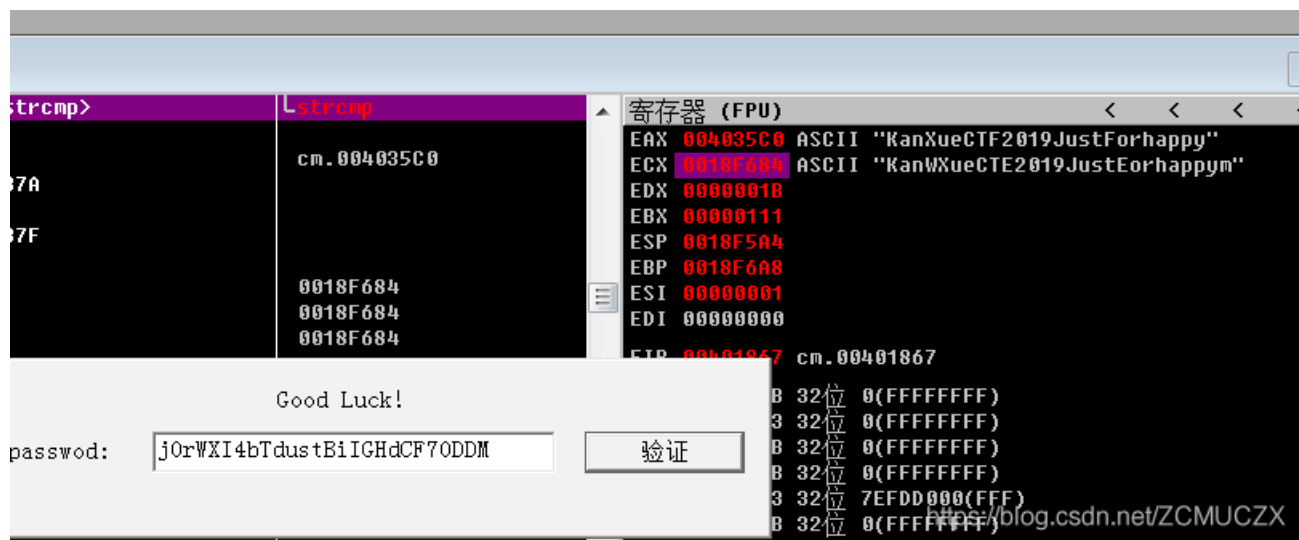
Kw

Lx

My

Nz

OO
PP
QQ
RR
SS
TT
UU
VV
WW
XX
YY
ZZ



j0rWXI4bTdustBiIGHdCF70DDM