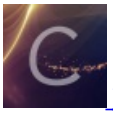
南京邮电大学网络攻防平台逆向writeup之[maze]

原创

巫师54 于 2017-07-31 17:29:56 发布
分类专栏： WriteUP



#1

用IDA打开很容易找到入口位置发现，密码长度必须是24位，格式是nctf{**********}，然后给s1截断了前5个字符，在字符串判断循环的时候长度减了1，if (++v3 >= strlen(&s1) - 1)，也就是说，取{*****}之间的内容。

```
puts("Input flag:");
scanf("%s", &s1, 0LL);
if ( strlen(&s1) != 24 || strncmp(&s1, "nctf{", 5uLL) || *(&byte_6010BF + 24) != 125 )
```

#2 关键判断函数

有个字符串：' ******* * **** * **** * *** *# *** *** ***   *********' , 长度为64，里面只有三种字符，空格、*和# ASCII 值为 32,42,35

关键判断函数1：

```
if ( !(unsigned __int8)sub_400690((__int64)asc_601060, SHIDWORD(youbiao), youbiao) )
```

这个SHIDWORD让我迷惹了很久，学艺不精啊，把SHIDWORD(youbiao)和youbiao看成两个不同的变量就行了。

```
__int64 __fastcall sub_400690(__int64 a1, int a2, int a3)
{
  __int64 result; // rax@1

  result = *(_BYTE *)(a1 + a2 + 8LL * a3);
  LOBYTE(result) = (_DWORD)result == 32 || (_DWORD)result == 35;
  return result;
}
```

关键判断函数2：最后一次字符串游标算下来的ASCII必须是35

```
if ( *(&asc_601060[8 * (signed int)youbiao] + SHIDWORD(youbiao)) != 35 )
    goto LABEL_20;
  v7 = "Congratulations!";
```

先遍历一张表出来，看哪些a2,a3符合条件，还好35只有一个，如何一步步往下走也能分析出来了

a2 0 a3 0 ascii 32 0
a2 1 a3 0 ascii 32 1
a2 1 a3 1 ascii 32 2
a2 1 a3 4 ascii 32
a2 2 a3 1 ascii 32 3
a2 2 a3 3 ascii 32 7
a2 2 a3 4 ascii 32 8
a2 2 a3 5 ascii 32 9
a2 2 a3 6 ascii 32 10
a2 3 a3 1 ascii 32 4
a2 3 a3 2 ascii 32 5
a2 3 a3 3 ascii 32 6
a2 3 a3 6 ascii 32 11
a2 4 a3 4 ascii 35 18
a2 4 a3 6 ascii 32 12
a2 5 a3 1 ascii 32
a2 5 a3 2 ascii 32
a2 5 a3 3 ascii 32
a2 5 a3 4 ascii 32 17
a2 5 a3 6 ascii 32 13
a2 6 a3 1 ascii 32
a2 6 a3 4 ascii 32 16
a2 6 a3 5 ascii 32 15
a2 6 a3 6 ascii 32 14

参数a1表示的是这个字符串的位置，a2+8*a3表示位移，最终必须是位移到空格或者#的地方，才算过关。

#3 计算过程

接上一条，chr(111) a2++; chr(79)a2--;chr(48)a3++;chr(49)a3--;每一位都进行判断

```
dic=chr(79)+chr(111)+chr(46)+chr(48)
key="oOoOOoOOOOOOOOOOOO"
password="nctf{"+key+"}"
cmpstr="  *******   *  **** * ****  * ***  *#  *** *** ***     *********"
'O.  0 1 3 4 6'
print "cmpstr",len(cmpstr)
print "password",len(password)
print "key",len(key)
print "dic",dic

for i in range(8):
 for j in range(8):
  if ord(cmpstr[i+8*j])==32 or ord(cmpstr[i+8*j])==35:
```

```
  if ord(cmpstr[i+8*j])==32 or ord(cmpstr[i+8*j])==35:
   print "i",i,'j',j,ord(cmpstr[i+8*j])

def check2(v9,k):
 print 'a2 is ',v9 ,"a3 is ",k
 if cmpstr[8*k+v9]==chr(32) or cmpstr[8*k+v9]==chr(35):
  return True
 else:
  return False

c=0

def check(str):
 j=0
 k=0
 global c
 #c=0
 for i in str:
  print 'checking : ',i,ord(i),c,j
  c+=1
  if i == chr(79):
   #j+=1
   j-=1
   if j>0:
    if check2(j,k):
     continue
    else:
     return False
   else:
    return False
  if i == chr(111):
   #j+=1
   j+=1
   if j<8:
    if check2(j,k):
     continue
    else:
     return False
   else:
    return False
  if i ==chr(46):
   k-=1

   if k>0:
    if check2(j,k):
     continue
    else:
     return False
   else:
    return False
  if i ==chr(48):
   k+=1

   if k<8:
    if check2(j,k):
     continue
    else:
     return False
   else:
    return False
```

```
 print 'J is ',j ,"k is ",k
 return check2(j,k)

#print "count",c

key="o0oo00O000oooo..OO"

print "checking......"

f=check(key)
print 'the finall check is',f

password="nctf{"+key+"}"
#print "check2",check2(4)

print password,len(password)
exit()
```

nctf{o0oo00O000oooo..OO}

提交正确