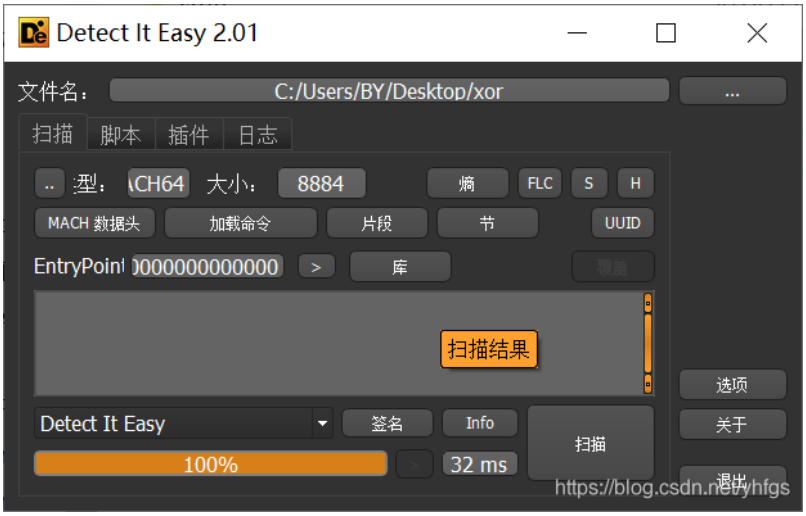
buuctf——xor

原创

re3sry 于 2021-05-27 17:03:55 发布 241 收藏

1.主要文件为xor，查壳，丢到DIE中。

无壳，64位文件。



2.丢到IDA中，找到main，F5.

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int i; // [rsp+2Ch] [rbp-124h]
  char __b[264]; // [rsp+40h] [rbp-110h] BYREF

  memset(__b, 0, 0x100uLL);
  printf("Input your flag:\n");
  get_line(__b, 0x100u);
  if ( strlen(__b) != 33 )
    goto LABEL_7;
  for ( i = 1; i < 33; ++i )
    __b[i] ^= __b[i - 1];
  if ( !strncmp(__b, global, 041uLL) )
    printf("Success");
  else
LABEL_7:
    printf("Failed");
  return 0;
```


3.分析代码，

由第一个if可知flag长度为33.

for循环是对flag进行异或运算第一个数不变。

下一个if是比较flag和global（即flag异或运算后是global），查看global。

```
H db 'f',0Ah                    ; DATA XREF: __data:_global↓o
  db 'k',0Ch,'w&O.@',11h,'x',0Dh,'Z;U',11h,'p',19h,'F',1Fh,'v"M#D',0Eh,'g'
  db 6,'h',0Fh,'G2O',0
  db 'Input your flag:',0Ah,0
```

4.写脚本。

File Edit Format Run Options Window Help

```
s=['f',0x0A, 'k',0x0C,'w&O.@',0x11,'x',0x0D,'Z;U',0x11,'p',0x19,'F',0x1F,'v"M#D',0x0E,'g',0x6,'h',0x0F,'G2O',0]
for i in range(len(s)):
    if type(s[i])==int:
        s[i]=chr(s[i])
s="".join(s)
flag='f'
for i in range(1,len(s)):
    flag += chr(ord(s[i])^ord(s[i-1]))
print(flag)
```


4.get flag

```
C:\Users\BY>python C:\Users\BY\Desktop\xor（未解）\xor.py
flag{QianQiuWanDai_YiTongJiangHu}0
```