攻防世界 Reverse高手进阶区 2分题 Reversing-x64Elf-100

原创

思源湖的鱼 于 2020-12-18 14:03:05 发布 115 收藏

分类专栏： ctf 文章标签： ctf 攻防世界 reverse

本文链接：https://blog.csdn.net/weixin_44604541/article/details/111358087

ctf 专栏收录该内容

200 篇文章 23 订阅

订阅专栏

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Reversing-x64Elf-100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

```
signed __int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  signed __int64 result; // rax
  char s; // [rsp+0h] [rbp-110h]
  unsigned __int64 v5; // [rsp+108h] [rbp-8h]

  v5 = __readfsqword(0x28u);
  printf("Enter the password: ", a2, a3);
  if ( !fgets(&s, 255, stdin) )
    return 0LL;
  if ( (unsigned int)sub_4006FD(&s, 255LL) )
  {
    puts("Incorrect password!");
    result = 1LL;
  }
  else
  {
    puts("Nice!");
    result = 0LL;
  }
  return result;
}
```



```
signed __int64 __fastcall sub_4006FD(__int64 a1)
{
  signed int i; // [rsp+14h] [rbp-24h]
  const char *v3; // [rsp+18h] [rbp-20h]
  const char *v4; // [rsp+20h] [rbp-18h]
  const char *v5; // [rsp+28h] [rbp-10h]

  v3 = "Dufhbmf";
  v4 = "pG`imos";
  v5 = "ewUglpt";
  for ( i = 0; i <= 11; ++i )
  {
    if ( (&v3)[i % 3][2 * (i / 3)] - *(char *)(i + a1) != 1 )
      return 1LL;
  }
  return 0LL;
}
```


简单的逻辑

```
s = ["Dufhbmf", "pG`imos", "ewUglpt"]
flag = ""
for i in range(12):
    flag += chr(ord(s[i%3][2*int(i/3)])-1)
print(flag)
```

得到flag：`Code_Talkers`

结语

简单题