攻防世界 Reverse高手进阶区 2分题 666

原创

思源湖的鱼 于 2020-12-24 14:00:57 发布 139 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/111625382

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

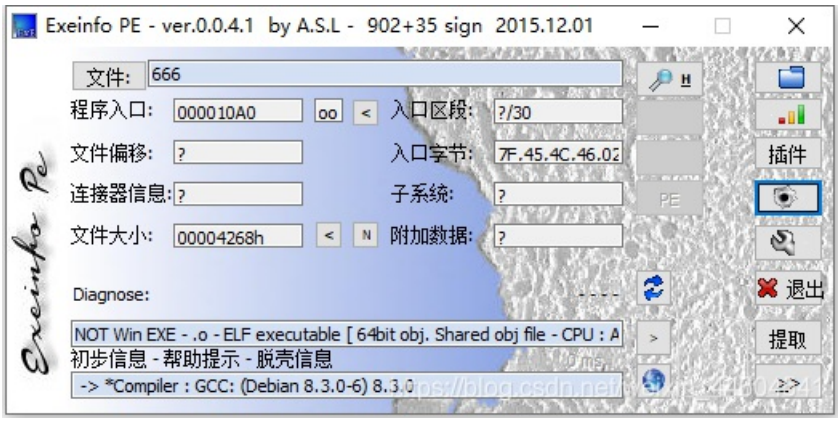
本篇是666的writeup

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

```c
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char s; // [rsp+0h] [rbp-1E0h]
  char v5; // [rsp+F0h] [rbp-F0h]

  memset(&s, 0, 0x1EuLL);
  printf("Please Input Key: ", 0LL);
  __isoc99_scanf("%s", &v5);
  encode(&v5, &s);
  if ( strlen(&v5) == key )
  {
    if ( !strcmp(&s, enflag) )
      puts("You are Right");
    else
      puts("flag{This_1s_f4cker_flag}");
  }
  return 0;
}
```



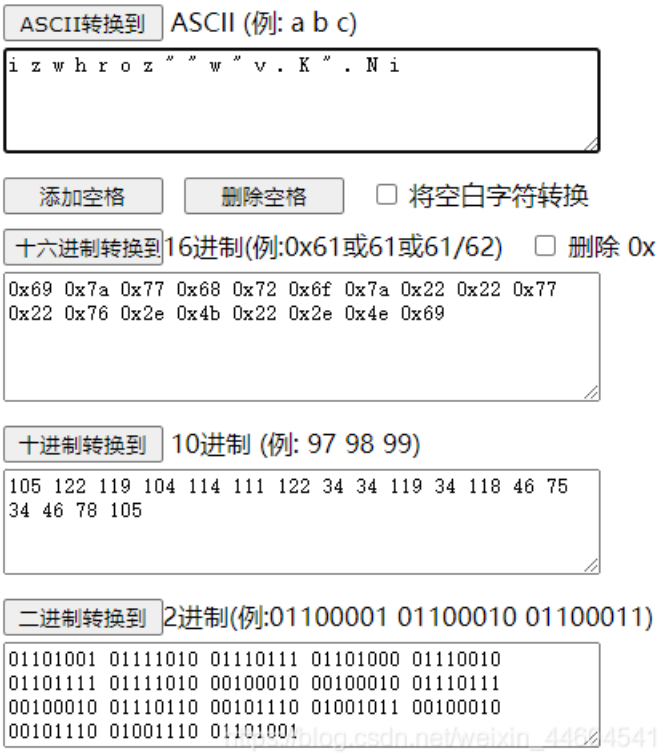
```c
int __fastcall encode(const char *a1, __int64 a2)
{
  char v3[32]; // [rsp+10h] [rbp-70h]
  char v4[32]; // [rsp+30h] [rbp-50h]
  char v5[40]; // [rsp+50h] [rbp-30h]
  int v6; // [rsp+78h] [rbp-8h]
  int i; // [rsp+7Ch] [rbp-4h]

  i = 0;
  v6 = 0;
  if ( strlen(a1) != key )
    return puts("Your Length is Wrong");
  for ( i = 0; i < key; i += 3 )
  {
    v5[i] = key ^ (a1[i] + 6);
    v4[i + 1] = (a1[i + 1] - 6) ^ key;
    v3[i + 2] = a1[i + 2] ^ 6 ^ key;
    *(_BYTE *)(a2 + i) = v5[i];
    *(_BYTE *)(a2 + i + 1LL) = v4[i + 1];
    *(_BYTE *)(a2 + i + 2LL) = v3[i + 2];
  }
  return a2;
}
```



```
.data:0000000000004060 enflag          db 'izwhroz""w"v.K".Ni',0
.data:0000000000004060                                         ; DATA XREF: main+8F↑o
.data:0000000000004073                 align 20h
.data:0000000000004080                 public key
.data:0000000000004080 key             dd 12h                  ; DATA XREF: encode+2D↑r
.data:0000000000004080                                         ; encode+5F↑r ...
```

转换下enflag



根据逻辑

写脚本

```
enflag=[105, 122, 119, 104, 114, 111, 122, 34, 34, 119, 34, 118, 46, 75, 34, 46, 78, 105, 0]
flag=''
for i in range(0,18,3):
    flag+=chr((18^enflag[i])-6)
    flag+=chr((18^enflag[i+1])+6)
    flag+=chr(18^enflag[i+2]^6)
print(flag)
```

得到flag：`unctf{b66_6b6_66b}`

结语

简单题