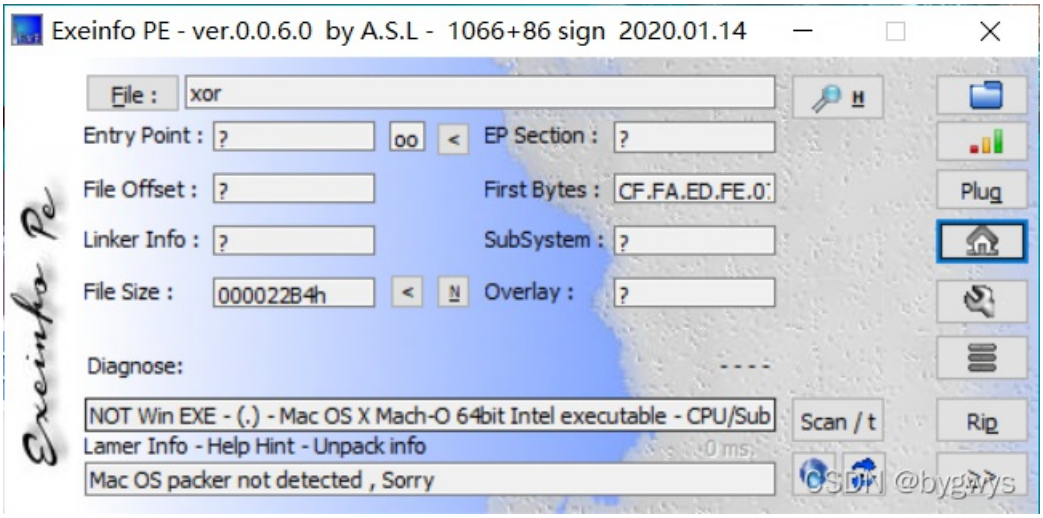
buuctf-xor

原创

bygwys 于 2022-01-18 16:04:41 发布 105 收藏
文章标签： p2p linq gnu

先查壳**64**位



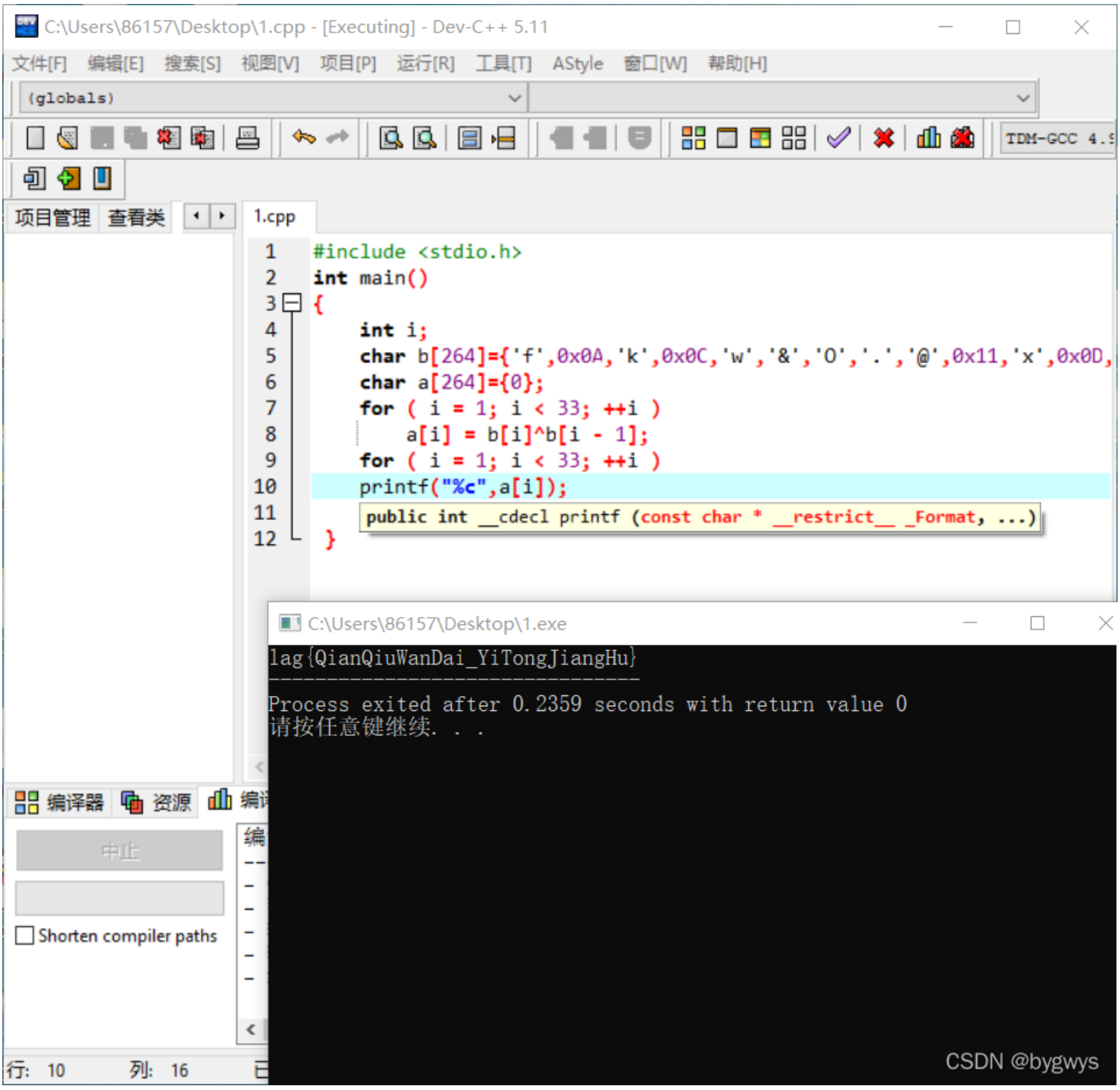
找到主函数

```
1  int __cdecl main(int argc, const char **argv, const char **envp)
2  {
3    int i; // [rsp+2Ch] [rbp-124h]
4    char __b[264]; // [rsp+40h] [rbp-110h] BYREF
5
6    memset(__b, 0, 0x100uLL);
7    printf("Input your flag:\n");
8    get_line(__b, 256LL);
9    if ( strlen(__b) != 33 )
10     goto LABEL_7;
11   for ( i = 1; i < 33; ++i )
12     __b[i] ^= __b[i - 1];
13   if ( !strncmp(__b, global, 0x21uLL) )
14     printf("Success");
15   else
16 LABEL_7:
17     printf("Failed");
18   return 0;
19 }
```

字符串显示

```
6E aFKWOXZUPFVMDGH db 'f',0Ah              ; DATA XREF: __data:_global↓o
6E                 db 'k',0Ch,'w&O.@',11h,'x',0Dh,'Z;U',11h,'p',19h,'F',1Fh,'v"M#D',0Eh,'g'
6E                 db 6,'h',0Fh,'G2O',0
90 aInputYourFlag  db 'Input your flag:',0Ah,0
90                                         ; DATA XREF: _main+B↑o
A2 ; const char aSuccess[]
A2 aSuccess        db 'Success',0          ; DATA XREF: _main+122↑o
AA ; const char aFailed[]
AA aFailed         db 'Failed',0           ; DATA XREF: _main:loc_100000EB0↑o
B1                 align 4
B1 __cstring       ends
B1
000FB4 ; ===========================================================================
```


写脚本



因为第一位不参与所以加个f

flag{QianQiuWanDai_YiTongJiangHu}