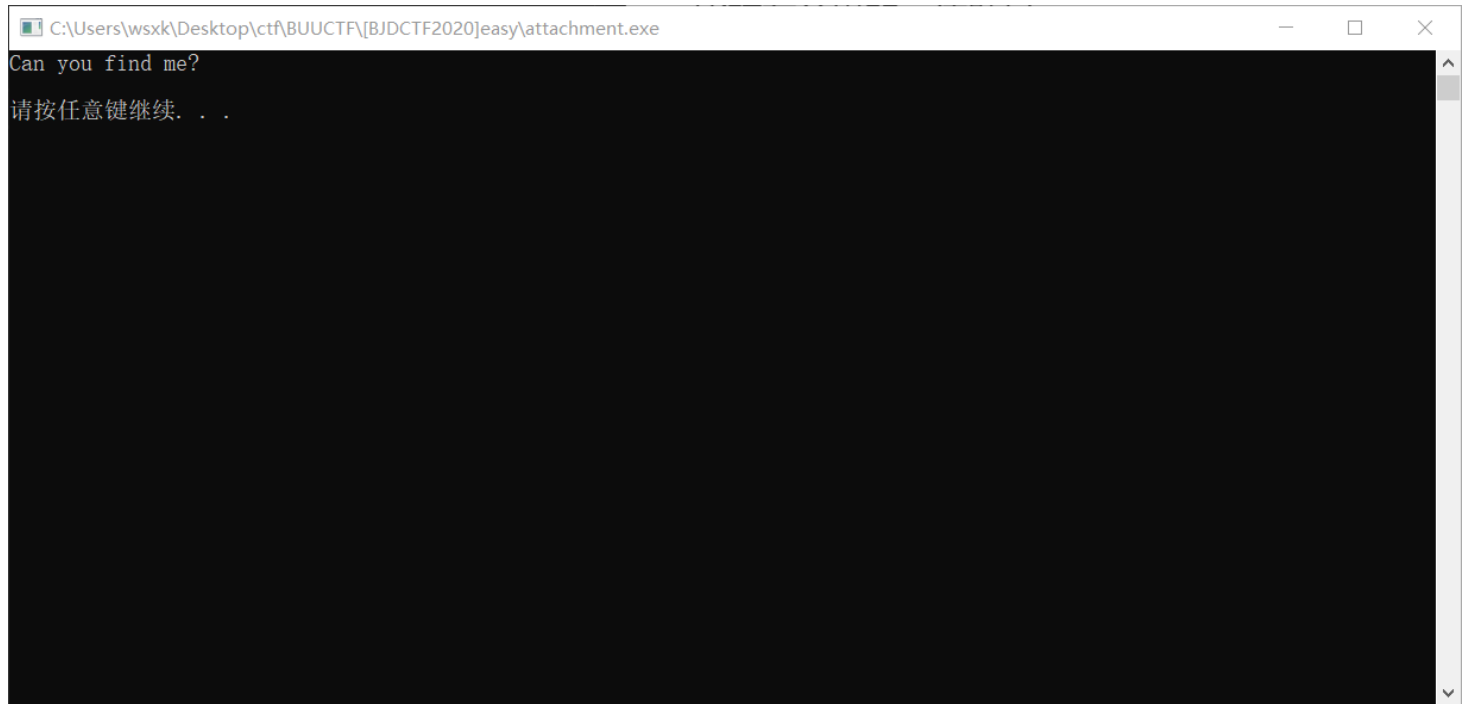


比较有意思的一道题目

开局啥都没



嗯，应该是把函数藏起来了

ida查看

```
1 int ques()
2 {
3     int v0; // edx
4     int result; // eax
5     int v2[50]; // [esp+20h] [ebp-128h] BYREF
6     int v3; // [esp+E8h] [ebp-60h]
7     int v4[10]; // [esp+EC] [ebp-5Ch]
8     int j; // [esp+114h] [ebp-34h]
9     __int64 v6; // [esp+118h] [ebp-30h]
10    int v7; // [esp+124h] [ebp-24h]
11    int v8; // [esp+128h] [ebp-20h]
12    int i; // [esp+12Ch] [ebp-1Ch]
13
14    v3 = '\x7F\xFA~1';
15    v4[0] = '\x02$\xFC';
16    v4[1] = '\x88JB9';
17    v4[2] = '\x02*\x84';
18    v4[3] = 139457077;
19    v4[4] = 262023;
20    v4[5] = -2008923597;
21    v4[6] = 143749;
22    v4[7] = 2118271985;
23    v4[8] = 143868;
24    for ( i = 0; i <= 4; ++i )
25    {
26        memset(v2, 0, sizeof(v2));
27        v8 = 0;
```

发现ques函数有点东西

可知出题人把该函数写入，但是不调用，让我们调用它
看到ques没有传参

视图(V) 调试(D) 跟踪(N) 插件(I) 收藏夹(I) 帮助(H) Dec 31 2020 (TitanEngine)

日志 断点 内存布局 调用堆栈 SEH链 脚本 符号 源代码 引用 线程 句柄 跟踪

004016E8 75 0C jne attachment.4016F6
004016EA C70424 20000000 mov dword ptr ss:[esp],20
004016F1 E8 41210000 call <JMP.&putchar>
004016F6 836D CC 01 sub dword ptr ss:[ebp-34],1
004016FA 837D CC 00 cmp dword ptr ss:[ebp-34],0
004016FE 79 85 jns attachment.401685
00401700 C70424 0A000000 mov dword ptr ss:[esp],A
00401707 E8 2C120000 call <JMP.&putchar>
0040170C 8345 E4 01 add dword ptr ss:[ebp-1C],1
00401710 837D E4 04 cmp dword ptr ss:[ebp-1C],4
00401714 0F8E 64FEFFFF jle attachment.40157E
0040171A 81C4 3C010000 add esp,13C
00401720 5B pop ebx
00401721 5E pop esi
00401722 5F pop edi
00401723 5D pop ebp
00401724 C3 ret
00401725 55 push ebp
00401726 89E5 mov ebp,esp
00401728 83E4 F0 and esp,FFFFFFF0
0040172B 81EC 00040000 sub esp,400
00401731 E8 6A0A0000 call attachment.4021A0
00401736 8D4424 10 lea eax,dword ptr ss:[esp+10]
0040173A 890424 mov dword ptr ss:[esp],eax
0040173D E8 FE110000 call <JMP.&time>
00401742 8D4424 10 lea eax,dword ptr ss:[esp+10]
00401746 890424 mov dword ptr ss:[esp],eax
00401749 E8 FA110000 call <JMP.&localtimes>

20:' '

A:'\n'

esi:&"C:\\Users\\wsxk\\Desktop\\ct

隐藏FPU

EAX	0000000A	
EBX	00000001	
ECX	76514620	msvcrt.
EDX	00000000	
EBP	0061FF70	
ESP	0061FEAC	
ESI	006E2270	&"C:\\U
EDI	00000041	'A'
EIP	00401724	attachme
EFLAGS	00000304	
ZF	0	
PF	1	
AF	0	

选择C:\Users\wsxk\Desktop\ctf\BUUCTF\BJDCTF2020\easy\attachment.exe

* * * *****
* * * * *

* * * * *
* * * *****
* * * * *

内存2 内存3 内存4 内存5 监视1 [v] 局部变量 结构体

十六进制 016 00 18 00 28 7C 91 77 14 00 16 00 78 74 91 77 ASCII (...)\w...xt.w