攻防世界re1

原创

starmultiple 于 2022-01-22 14:11:17 发布 232 收藏

分类专栏： 做题 文章标签： 开发语言

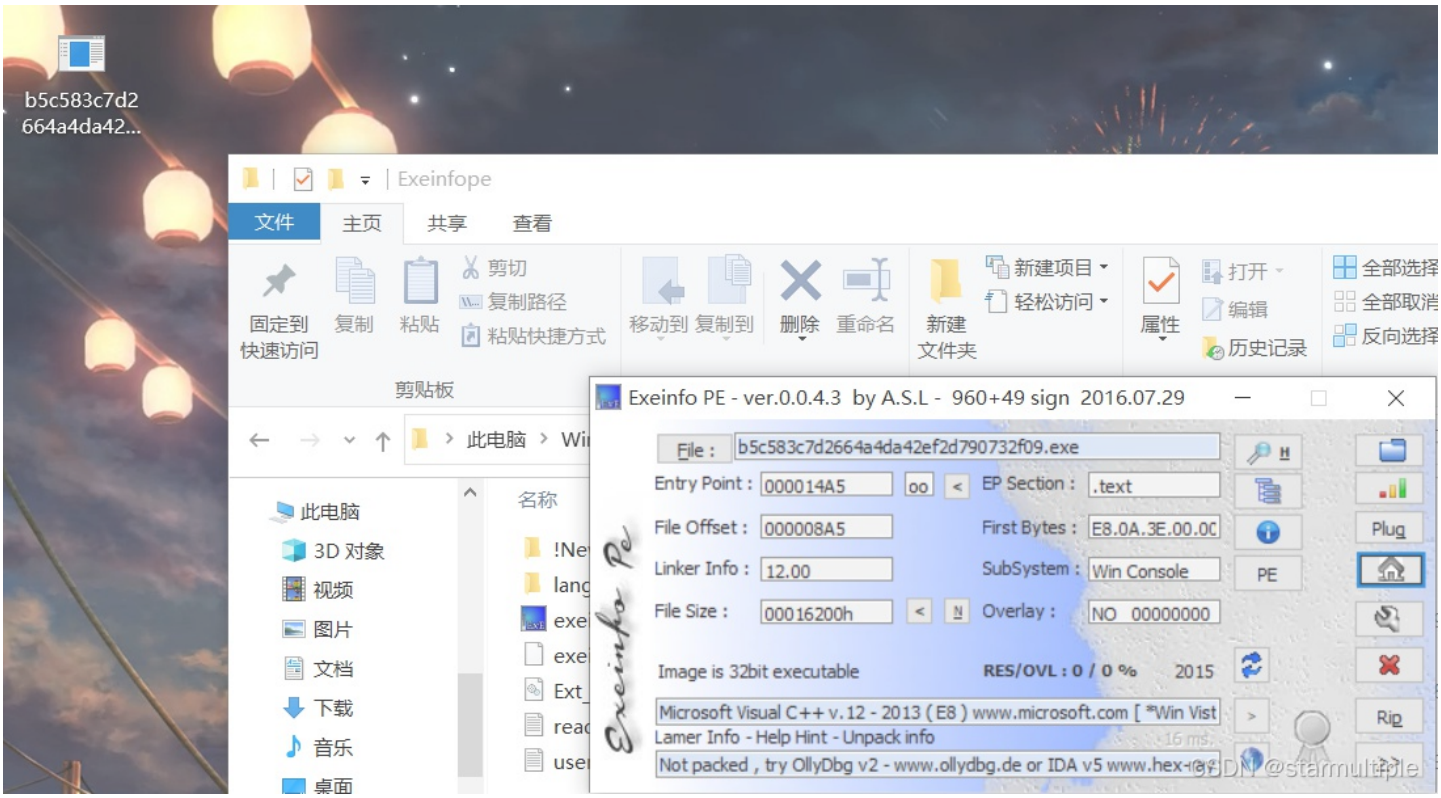
本文链接：https://blog.csdn.net/starmultiple/article/details/122636303

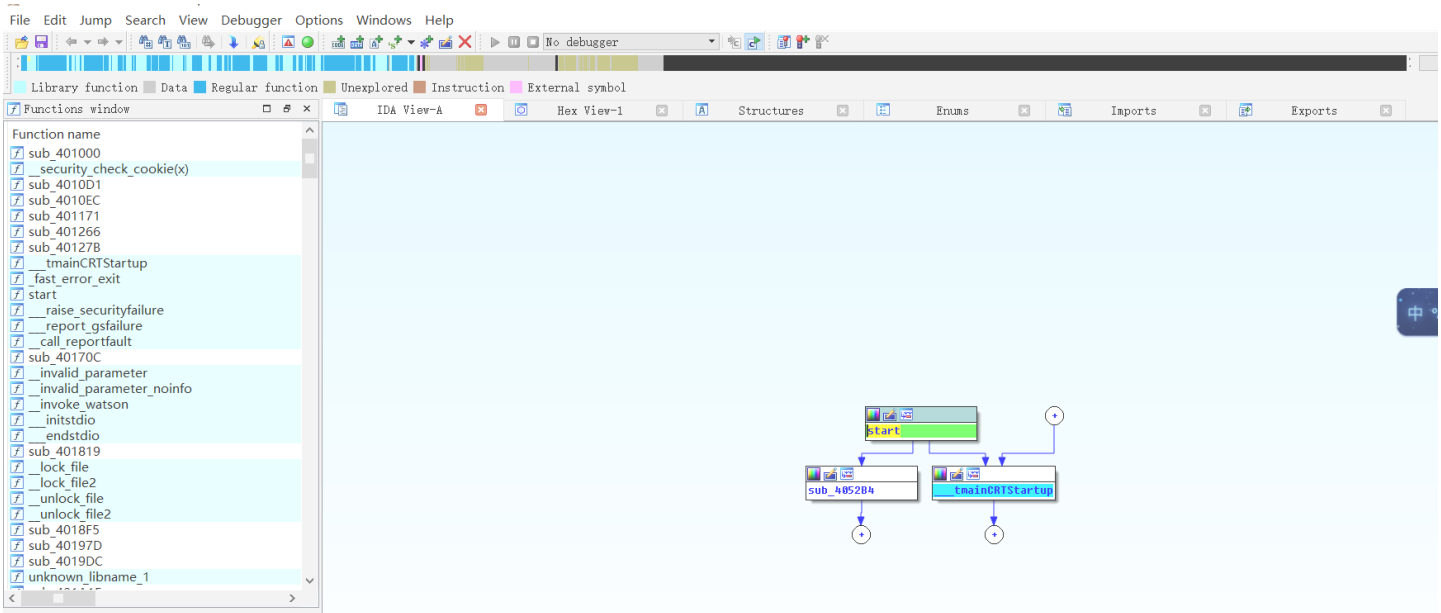
版权

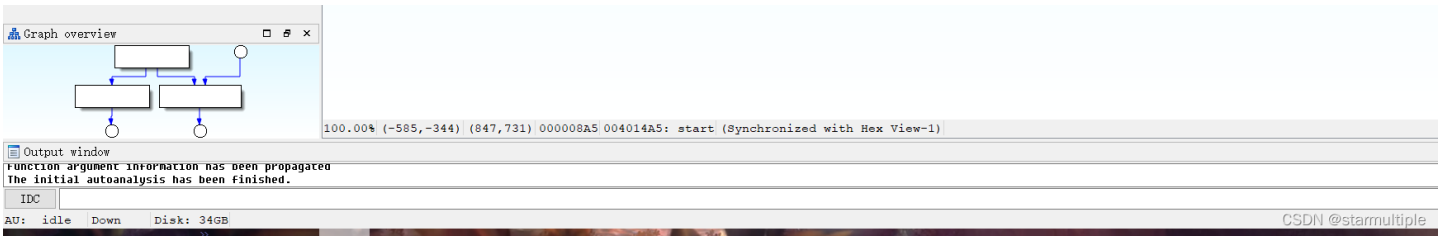
做题 专栏收录该内容

11 篇文章 0 订阅

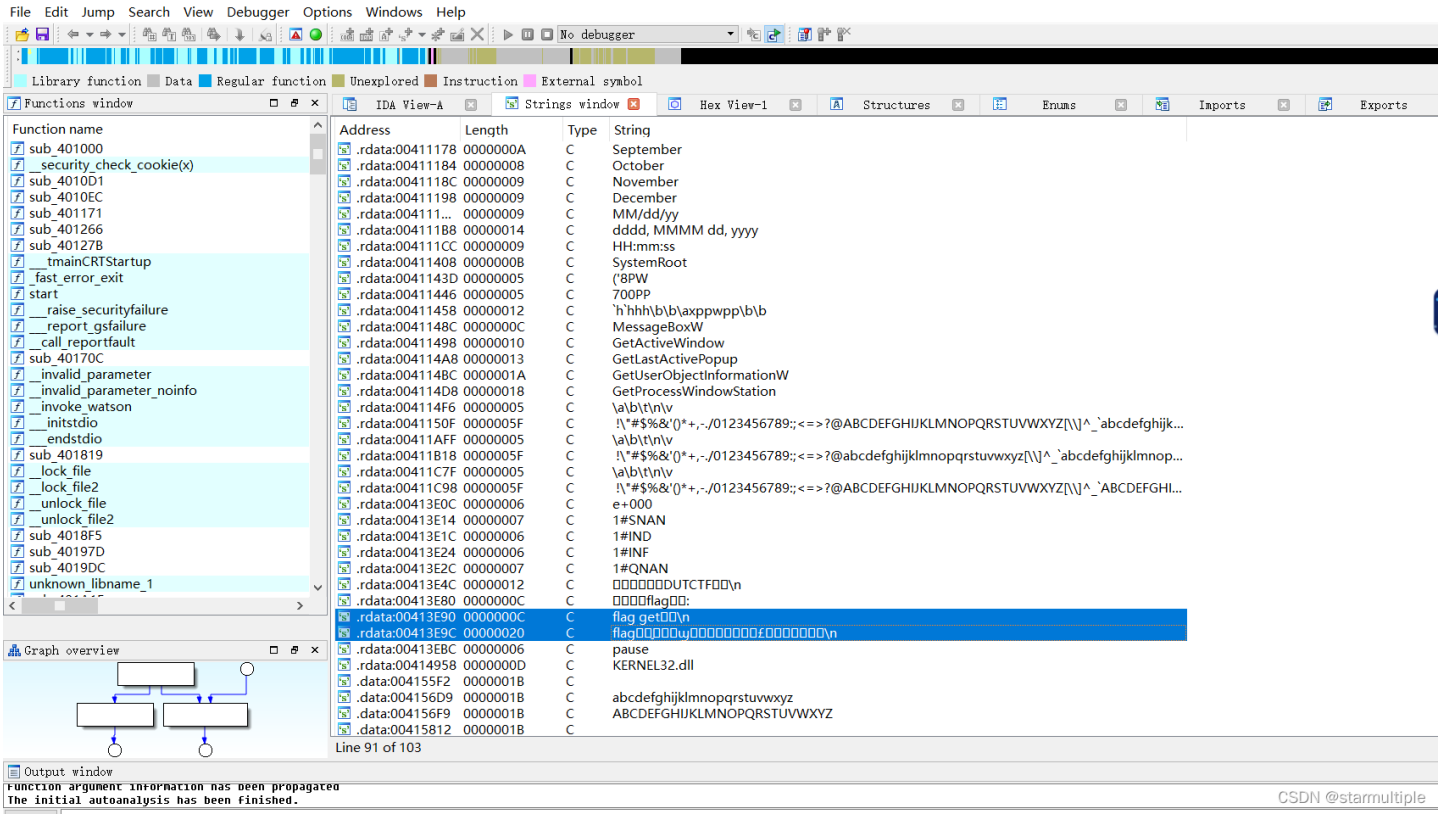
订阅专栏



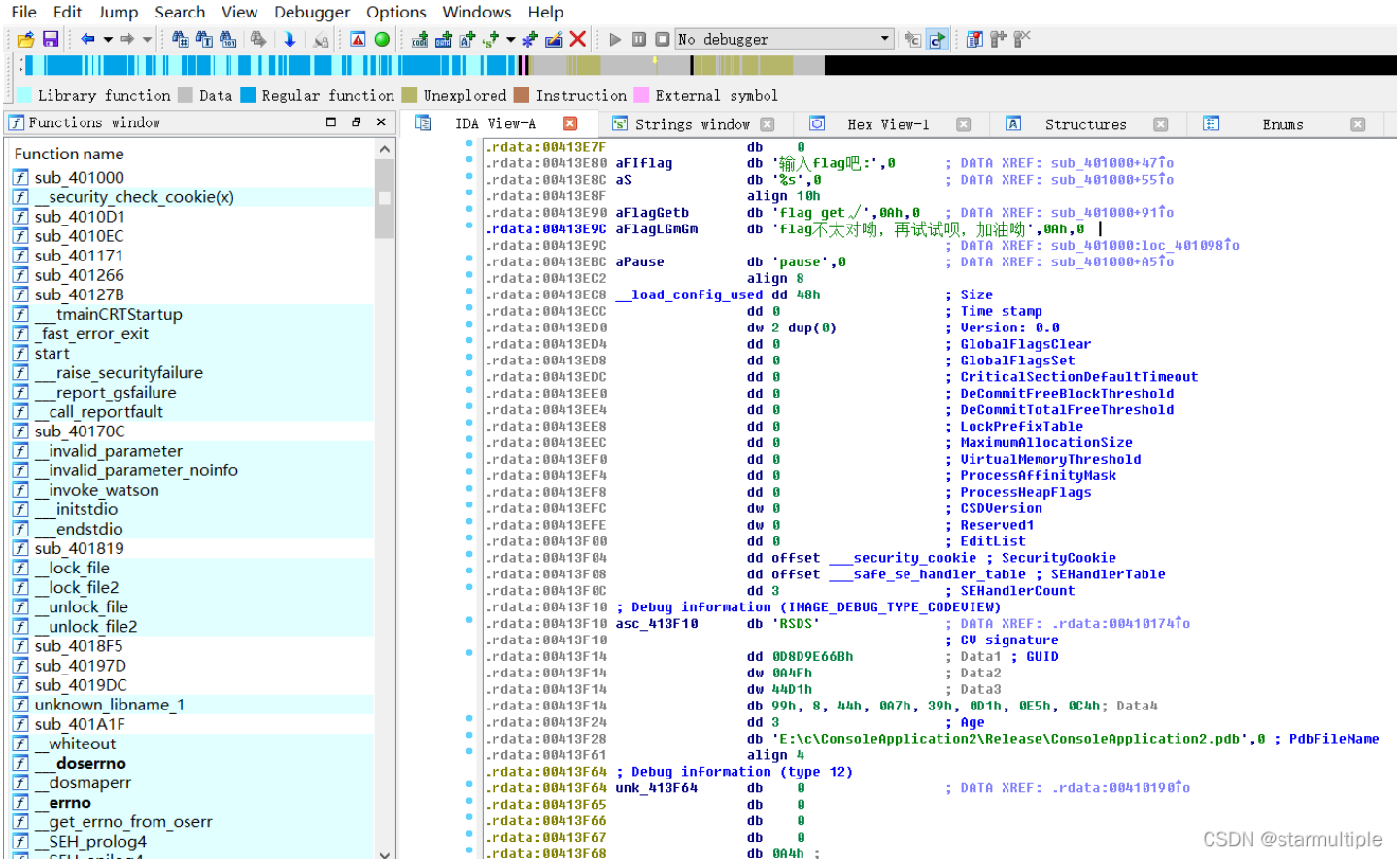




shift F12后找到flag

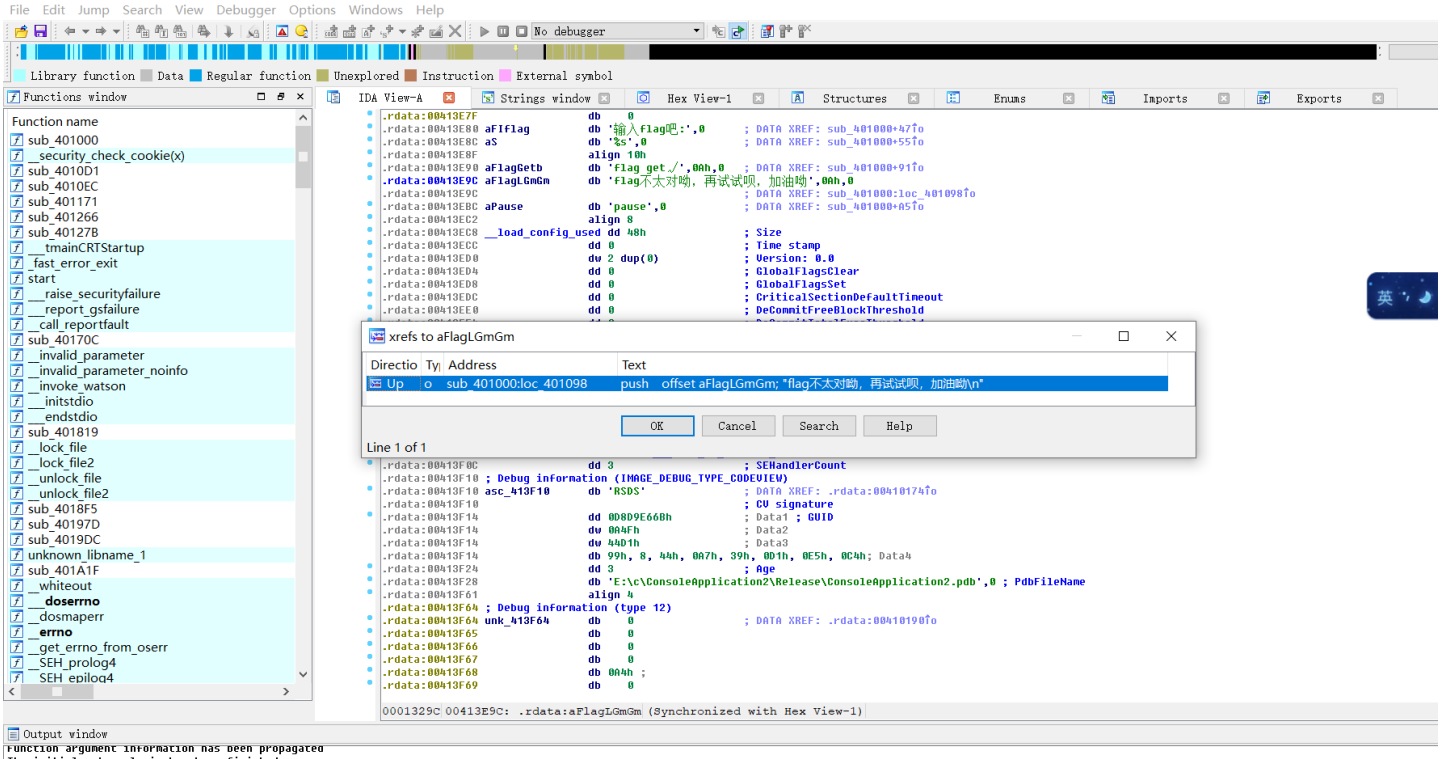


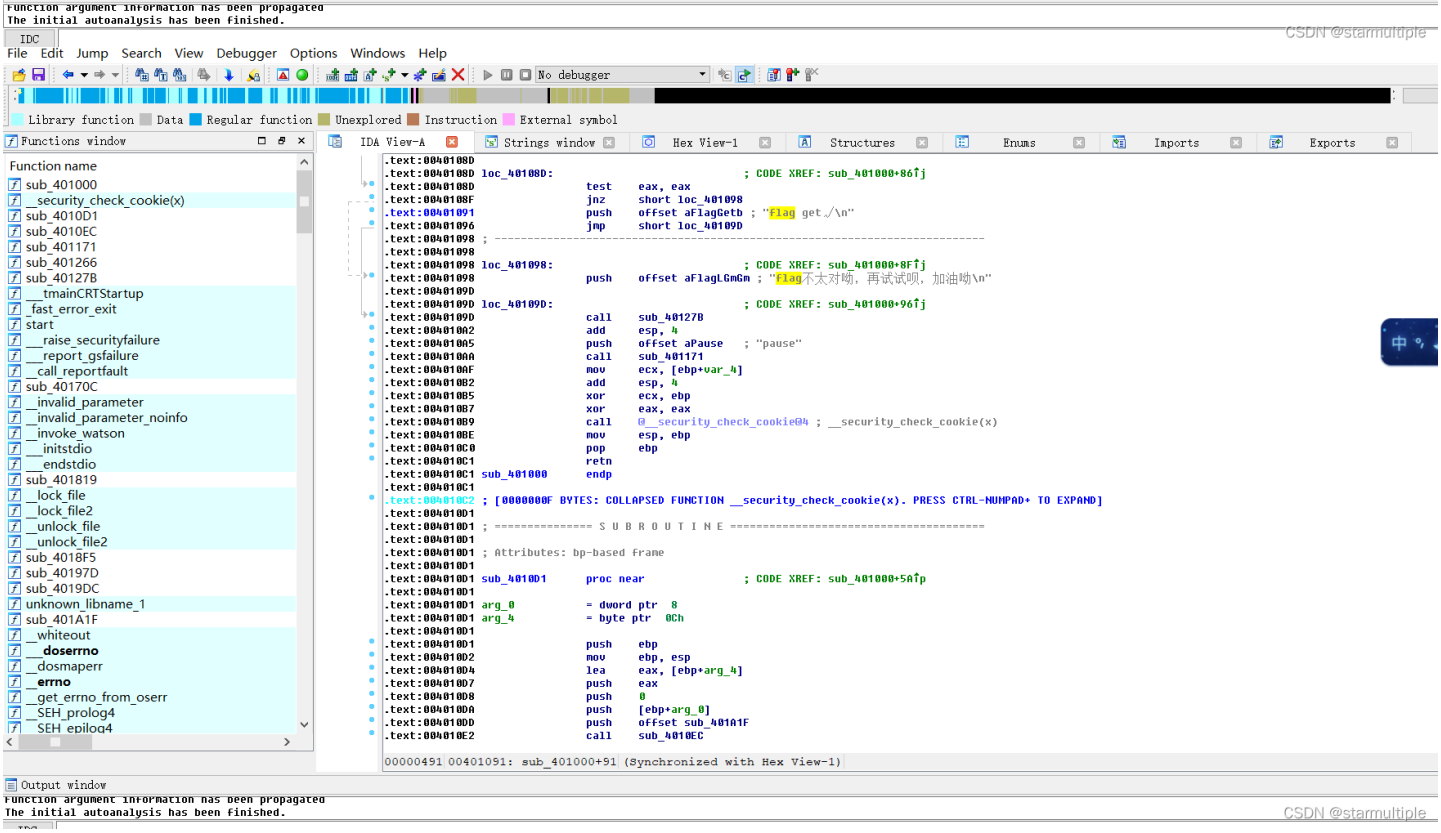
双击



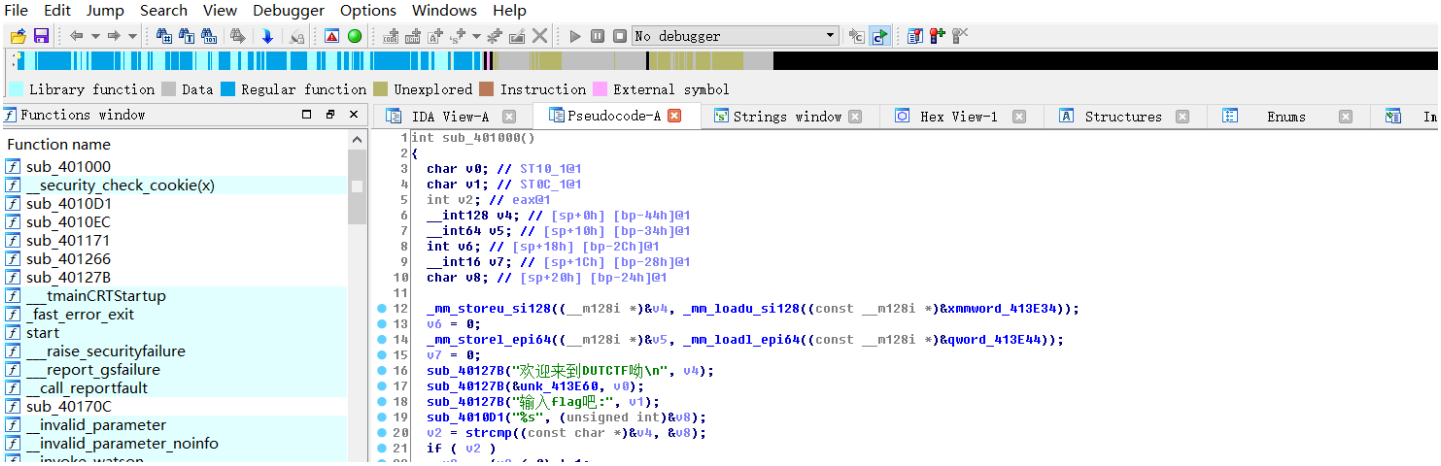
ctr x 获取当前代码地址，点击,出现以下，

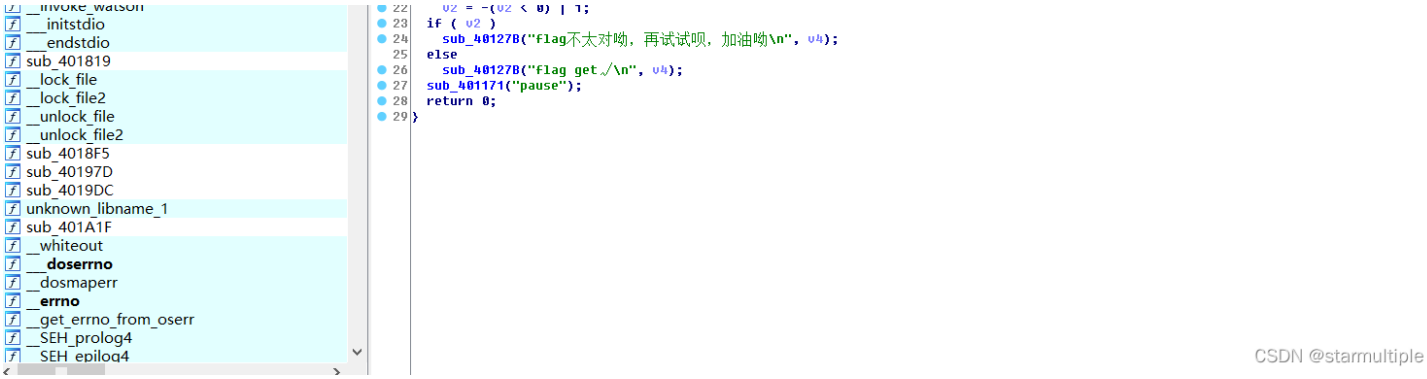
点击查看


File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
Function name
sub_401000
__security_check_cookie(x)
sub_4010D1
sub_4010EC
sub_401171
sub_401266
sub_40127B
__tmainCRTStartup
_fast_error_exit
start
__raise_securityfailure
__report_gsfailure
__call_reportfault
sub_40170C
__invalid_parameter
__invalid_parameter_noinfo
__invoke_watson
__initstdio
__endstdio
sub_401819
__lock_file
__lock_file2
__unlock_file
__unlock_file2
sub_4018F5
sub_40197D
sub_4019DC
unknown_libname_1
sub_401A1F
__whiteout
__doserrno
__dosmaperr
__errno
__get_errno_from_oserr
__SEH_prolog4
__SEH_epilog4
IDA View-A
Strings window
Hex View-1
Structures
Enums
Imports
Exports
.rdata:00413E7F db 0
.rdata:00413E80 aFlflag db '输入flag吧:',0 ; DATA XREF: sub_401000+47↑o
.rdata:00413E8C aS db '%s',0 ; DATA XREF: sub_401000+55↑o
.rdata:00413E8F align 10h
.rdata:00413E90 aFlagGetb db 'flag_get./',0Ah,0 ; DATA XREF: sub_401000+91↑o
.rdata:00413E9C aFlagLGmGm db 'flag不太对呦，再试试呗，加油呦',0Ah,0
.rdata:00413E9C ; DATA XREF: sub_401000:loc_401098↑o
.rdata:00413EBC aPause db 'pause',0 ; DATA XREF: sub_401000+A5↑o
.rdata:00413EC2 align 8
.rdata:00413EC8 __load_config_used dd 48h ; Size
.rdata:00413ECC dd 0 ; Time stamp
.rdata:00413ED0 dw 2 dup(0) ; Version: 0.0
.rdata:00413ED4 dd 0 ; GlobalFlagsClear
.rdata:00413ED8 dd 0 ; GlobalFlagsSet
.rdata:00413EDC dd 0 ; CriticalSectionDefaultTimeout
.rdata:00413EE0 dd 0 ; DeCommitFreeBlockThreshold
xrefs to aFlagLGmGm
Directio Ty Address Text
Up o sub_401000:loc_401098 push offset aFlagLGmGm; "flag不太对呦，再试试呗，加油呦\n"
OK Cancel Search Help
Line 1 of 1
.rdata:00413F0C dd 3 ; SEHandlerCount
.rdata:00413F10 ; Debug information (IMAGE_DEBUG_TYPE_CODEVIEW)
.rdata:00413F10 asc_413F10 db 'RSDS' ; DATA XREF: .rdata:00410174↑o
.rdata:00413F10 ; CV signature
.rdata:00413F14 dd 0D8D9E66Bh ; Data1 ; GUID
.rdata:00413F14 dw 0A4Fh ; Data2
.rdata:00413F14 dw 44D1h ; Data3
.rdata:00413F14 db 99h, 8, 44h, 0A7h, 39h, 0D1h, 0E5h, 0C4h; Data4
.rdata:00413F24 dd 3 ; Age
.rdata:00413F28 db 'E:\c\ConsoleApplication2\Release\ConsoleApplication2.pdb',0 ; PdbFileName
.rdata:00413F61 align 4
.rdata:00413F64 ; Debug information (type 12)
.rdata:00413F64 unk_413F64 db 0 ; DATA XREF: .rdata:00410190↑o
.rdata:00413F65 db 0
.rdata:00413F66 db 0
.rdata:00413F67 db 0
.rdata:00413F68 db 0A4h ;
.rdata:00413F69 db 0
0001329C 00413E9C: .rdata:aFlagLGmGm (Synchronized with Hex View-1)
Output window
Function argument information has been propagated
The initial autoanalysis has been finished.
IDC
CSDN @starmultiple


File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
Function name
sub_401000
__security_check_cookie(x)
sub_4010D1
sub_4010EC
sub_401171
sub_401266
sub_40127B
__tmainCRTStartup
_fast_error_exit
start
__raise_securityfailure
__report_gsfailure
__call_reportfault
sub_40170C
__invalid_parameter
__invalid_parameter_noinfo
__invoke_watson
__initstdio
__endstdio
sub_401819
__lock_file
__lock_file2
__unlock_file
__unlock_file2
sub_4018F5
sub_40197D
sub_4019DC
unknown_libname_1
sub_401A1F
__whiteout
__doserrno
__dosmaperr
__errno
__get_errno_from_oserr
__SEH_prolog4
__SEH_epilog4
IDA View-A
Strings window
Hex View-1
Structures
Enums
Imports
Exports
.text:0040108D
.text:0040108D loc_40108D: ; CODE XREF: sub_401000+86↑j
.text:0040108D test eax, eax
.text:0040108F jnz short loc_401098
.text:00401091 push offset aFlagGetb ; "flag get./\n"
.text:00401096 jmp short loc_40109D
.text:00401098 ; ---
.text:00401098
.text:00401098 loc_401098: ; CODE XREF: sub_401000+8F↑j
.text:00401098 push offset aFlagLGmGm ; "flag不太对呦，再试试呗，加油呦\n"
.text:0040109D
.text:0040109D loc_40109D: ; CODE XREF: sub_401000+96↑j
.text:0040109D call sub_40127B
.text:004010A2 add esp, 4
.text:004010A5 push offset aPause ; "pause"
.text:004010AA call sub_401171
.text:004010AF mov ecx, [ebp+var_4]
.text:004010B2 add esp, 4
.text:004010B5 xor ecx, ebp
.text:004010B7 xor eax, eax
.text:004010B9 call @__security_check_cookie@4 ; __security_check_cookie(x)
.text:004010BE mov esp, ebp
.text:004010C0 pop ebp
.text:004010C1 retn
.text:004010C1 sub_401000 endp
.text:004010C1
.text:004010C2 ; [0000000F BYTES: COLLAPSED FUNCTION __security_check_cookie(x). PRESS CTRL-NUMPAD+ TO EXPAND]
.text:004010D1
.text:004010D1 ; =============== S U B R O U T I N E =======================================
.text:004010D1
.text:004010D1 ; Attributes: bp-based frame
.text:004010D1
.text:004010D1 sub_4010D1 proc near ; CODE XREF: sub_401000+5A↑p
.text:004010D1
.text:004010D1 arg_0 = dword ptr 8
.text:004010D1 arg_4 = byte ptr 0Ch
.text:004010D1
.text:004010D1 push ebp
.text:004010D2 mov ebp, esp
.text:004010D4 lea eax, [ebp+arg_4]
.text:004010D7 push eax
.text:004010D8 push 0
.text:004010DA push [ebp+arg_0]
.text:004010DD push offset sub_401A1F
.text:004010E2 call sub_4010EC
00000491 00401091: sub_401000+91 (Synchronized with Hex View-1)
Output window
Function argument information has been propagated
The initial autoanalysis has been finished.
CSDN @starmultiple

F5查看伪代码


File Edit Jump Search View Debugger Options Windows Help
No debugger
Library function Data Regular function Unexplored Instruction External symbol
Functions window
Function name
sub_401000
__security_check_cookie(x)
sub_4010D1
sub_4010EC
sub_401171
sub_401266
sub_40127B
__tmainCRTStartup
_fast_error_exit
start
__raise_securityfailure
__report_gsfailure
__call_reportfault
sub_40170C
__invalid_parameter
__invalid_parameter_noinfo
IDA View-A
Pseudocode-A
Strings window
Hex View-1
Structures
Enums
int sub_401000()
{
char v0; // ST10_1@1
char v1; // ST0C_1@1
int v2; // eax@1
__int128 v4; // [sp+0h] [bp-44h]@1
__int64 v5; // [sp+10h] [bp-34h]@1
int v6; // [sp+18h] [bp-2Ch]@1
__int16 v7; // [sp+1Ch] [bp-28h]@1
char v8; // [sp+20h] [bp-24h]@1
_mm_storeu_si128((__m128i *)&v4, _mm_loadu_si128((const __m128i *)&xmmword_413E34));
v6 = 0;
_mm_storel_epi64((__m128i *)&v5, _mm_loadl_epi64((const __m128i *)&qword_413E44));
v7 = 0;
sub_40127B("欢迎来到DUTCTF呦\n", v4);
sub_40127B(&unk_413E60, v0);
sub_40127B("输入flag吧:", v1);
sub_4010D1("%s", (unsigned int)&v8);
v2 = strcmp((const char *)&v4, &v8);
if (v2)



可以发现v4与flag有关

查看xmword_413E34

R转换16进制数

A合并后出现

```
413E2C                  align 4
413E2C ; char a1Qnan[]
413E2C a1Qnan           db '1#QNAN',0           ; DATA XREF: sub_40F02C:loc_4
413E33                  align 4
413E34 aDutctfWe1c0met  db 'DUTCTF{We1c0met0DUTCTF}',0 ; DATA XREF: sub_40106
413E4C aNDutctf         db '欢迎来到DUTCTF呦',0Ah,0 ; DATA XREF: sub_401000+1
413E5E                  align 10h
413E60 unk_413E60       db 0D5h ;               ; DATA XREF: sub_401000+3D↑o
413E61                  db 0E2h ;
```