

buuctf逆向刷题

原创

续梦人 于 2021-09-22 20:19:21 发布 36 收藏 1

分类专栏: [re逆向](#) 文章标签: [安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/CHAWUCIREN1/article/details/120420292>

版权



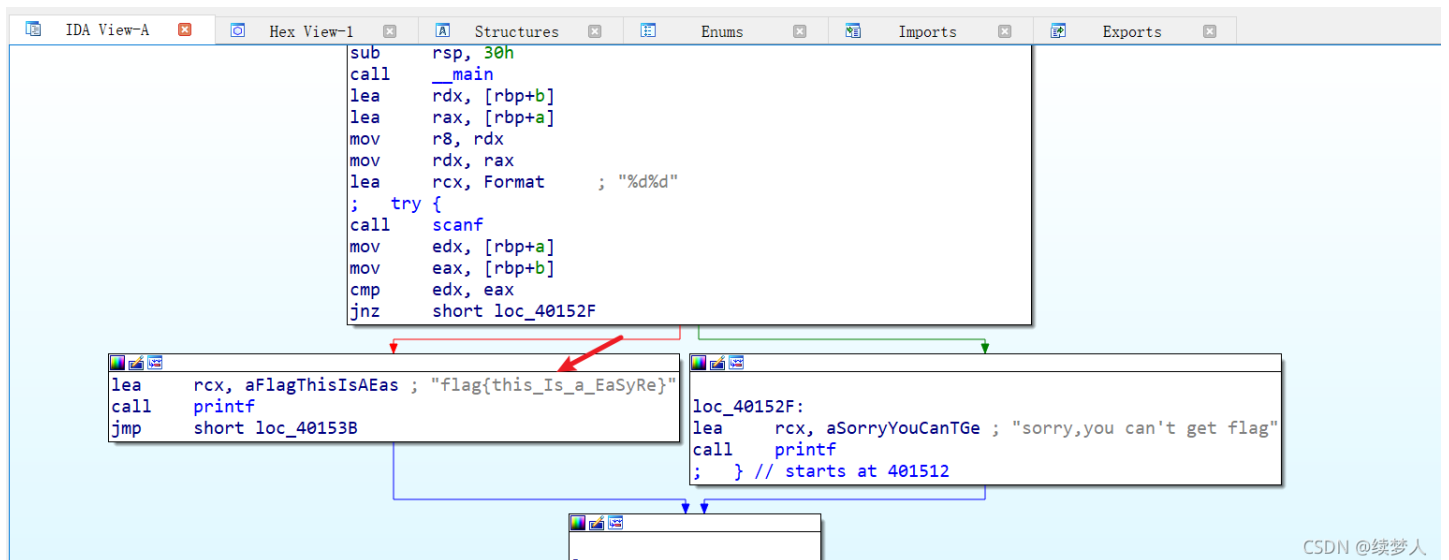
[re逆向](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

easyre

直接丢ida里面, 就能看到flag

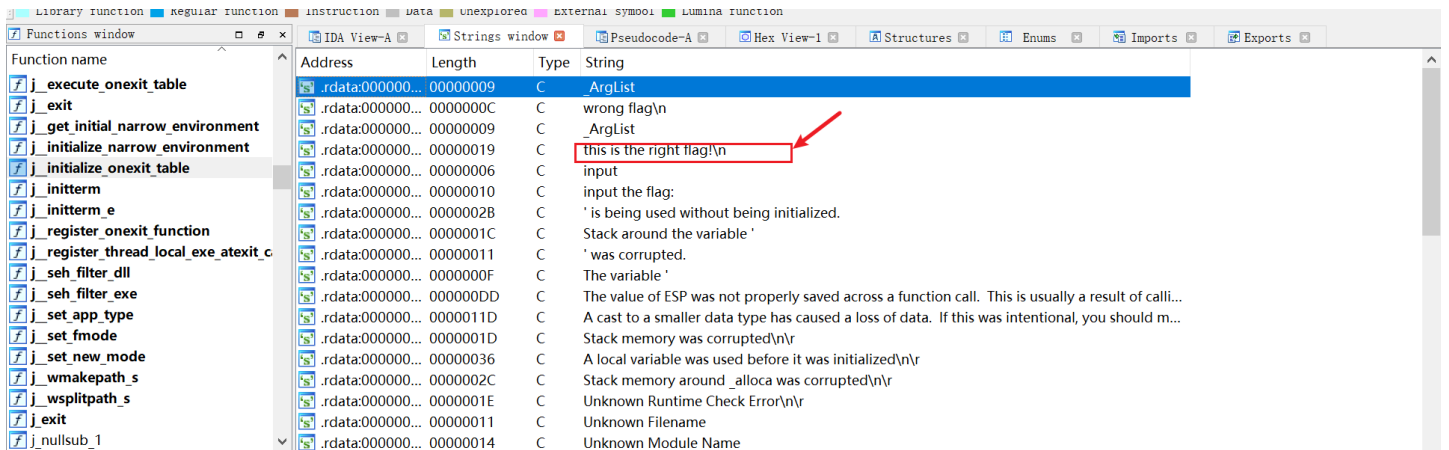


CSDN @续梦人

reverse1

F5反编译, 查看函数

有点多, shift + F12查找字符串



```

Line 78 of 268      Line 1 of 41
Output window
Function argument information has been propagated
CSDN @续梦人

```

```

Function name
sub_140011E40
sub_140011DF0
sub_140011DE0
sub_140011C80
sub_140011BD0
sub_140011B80
sub_140011AC0
sub_140011A00
sub_1400118C0
sub_140011830
sub_1400117A0
sub_140011760
sub_140011720
sub_1400116F0
sub_140011357
sub_140011348
sub_14001133E
sub_140011334

13 for ( i = 82i64; i; --i )
14 {
15     *(_DWORD *)v0 = -858993460;
16     v0 += 4;
17 }
18 for ( j = 0; ; ++j )
19 {
20     v8 = j;
21     v2 = j_strlen(Str2);
22     if ( v8 > v2 )
23         break;
24     if ( Str2[j] == 111 )
25         Str2[j] = 48;
26 }
27 sub_1400111D1("input the flag:");
28 sub_14001128F("%20s", Str1);
29 v3 = j_strlen(Str2);
30 if ( !strcmp(Str1, Str2, v3) )
31     sub_1400111D1("this is the right flag!\n");
32 else
33     sub_1400111D1("wrong flag\n");
34 sub_14001113B(v5, &unk_140019D00);
35 return 0i64;
36 }
CSDN @续梦人

```

strcmp函数比较Str1和Str2是否相等
同时当字符的值是111时，要换成48

```

>>> chr(111)
'o'
>>> chr(48)
'0'
>>>

```

双击Str2

```

IDA V... Pseudoc... Pseudoc... Strings w... Pseudoc... Hex V... Struc... Enums
.data:00000014001C000 _data segment para public 'DATA' use64
.data:00000014001C000 assume cs:_data
.data:00000014001C000 ;org 14001C00h
.data:00000014001C000 ; char Str2[]
.data:00000014001C000 Str2 db '{hello_world}',0 ; DATA XREF: sub_1400118C0+4B↑o
.data:00000014001C000 ; sub_1400118C0+67↑o ...
.data:00000014001C00E align 10h
.data:00000014001C010 ; uintptr_t __security_cookie
.data:00000014001C010 __security_cookie dq 2B992DDFA232h ; DATA XREF: sub_1400118C0+1E↑r
.data:00000014001C010 ; __security_check_cookie↑r ...
.data:00000014001C018 qword_14001C018 dq 0FFFD466D2205DCDh ; DATA XREF: __report_gsfailure+B4↑r
.data:00000014001C018 ; sub_140013E50+2A↑w ...
.data:00000014001C020 db 0
CSDN @续梦人

```

为了锻炼编程思想，写个脚本吧

```

key = "{hello_world}"
flag = ''
for i in key:
    if i == "o":
        flag = flag + "0"
    else:
        flag = flag + i
print("flag"+flag)

```

reverse2

```

8  unsigned __int64 v8; // [rsp+28h] [rbp-18h]
9
10 v8 = __readfsqword(0x28u);
11 pid = fork();
12 if ( pid )
13 {
14     waitpid(pid, &stat_loc, 0);
15 }
16 else
17 {
18     for ( i = 0; i <= strlen(&flag); ++i )
19     {
20         if ( *(&flag + i) == 105 || *(&flag + i) == 114 )
21             *(&flag + i) = 49;
22     }
23 }
24 printf("input the flag:");
25 __isoc99_scanf("%20s", s2);
26 if ( !strcmp(&flag, s2) )
27     result = puts("this is the right flag!");
28 else
29     result = puts("wrong flag!");
30 return result;
31 }

```

CSDN @续梦人

strcmp(&flag, s2)比较flag和s2的值

```

for ( i = 0; i <= strlen(&flag); ++i )
{
    if ( *(&flag + i) == 105 || *(&flag + i) == 114 )
        *(&flag + i) = 49;
}

```

```

>>> chr(105)
'i'
>>> chr(114)
'r'
>>> chr(49)
'1'
>>> |

```

也就是说当flag里面的字符有i或者r时，变为1

```

unsigned __int64 v8; // [rsp+28h] [rbp-18h]

v8 = __readfsqword(0x28u);
pid = fork();
if ( pid )
{
    waitpid(pid, &stat_loc, 0);
}
else
{
    for ( i = 0; i <= strlen(&flag); ++i )
    {
        if ( *(&flag + i) == 105 || *(&flag + i) == 114 )
            *(&flag + i) = 49;
    }
}
printf("input the flag:");
__isoc99_scanf("%20s", s2);
if ( !strcmp(&flag, s2) )
    result = puts("this is the right flag!");
else
    result = puts("wrong flag!");
return result;
}

```

CSDN @续梦人

双击flag

```
IDA view A | Pseudocode-A | Stack of main | Hex view-1 | Structures | Enums | Imports
.data:000000000060107E db 0
.data:000000000060107F db 0
.data:0000000000601080 public flag
.data:0000000000601080 ; char flag
.data:0000000000601080 flag db 7Bh ; DATA XREF: main+34↑r
.data:0000000000601080 ; main+44↑r ...
.data:0000000000601081 aHackingForFun db 'hacking_for_fun',0
.data:0000000000601081 _data ends
.data:0000000000601081
.bss:0000000000601092 ; =====
.bss:0000000000601092
.bss:0000000000601092 ; Segment type: Uninitialized
.bss:0000000000601092 ; Segment permissions: Read/Write
.bss:0000000000601092 _bss segment byte public 'BSS' use64
.bss:0000000000601092 assume cs:_bss
.bss:0000000000601092 ;org 601092h
.bss:0000000000601092 assume es:nothing, ss:nothing, ds:_data, fs:nothing, gs:nothing
.bss:0000000000601092 public __bss_start
.bss:0000000000601092 __bss_start db ? ; DATA XREF: __do_global_ctors_start@.ctors
```

编写一个小脚本

```
key = "{hacking_for_fun}"
flag = ''
for i in key:
    if i == "i" or i == "r" :
        flag = flag + "1"
    else:
        flag = flag + i
print("flag"+flag)
```