buuctf逆向刷题

原创

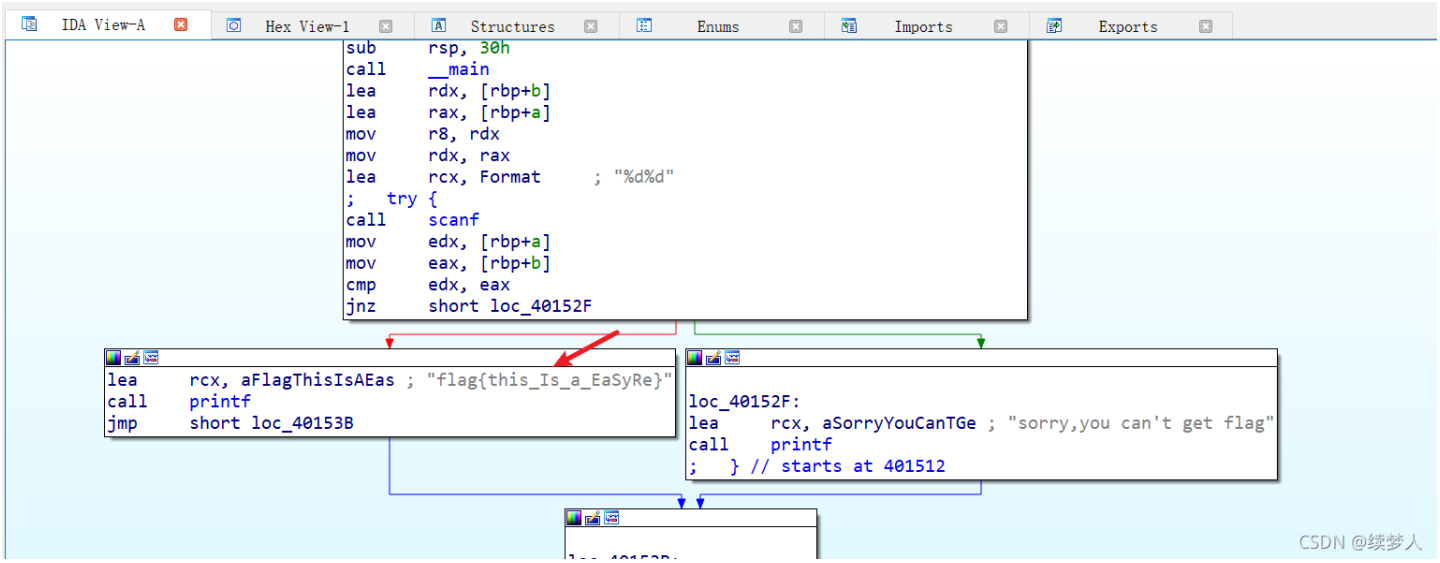
续梦人 于 2021-09-22 20:19:21 发布 36 收藏 1

分类专栏： re逆向 文章标签： 安全

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

easyre

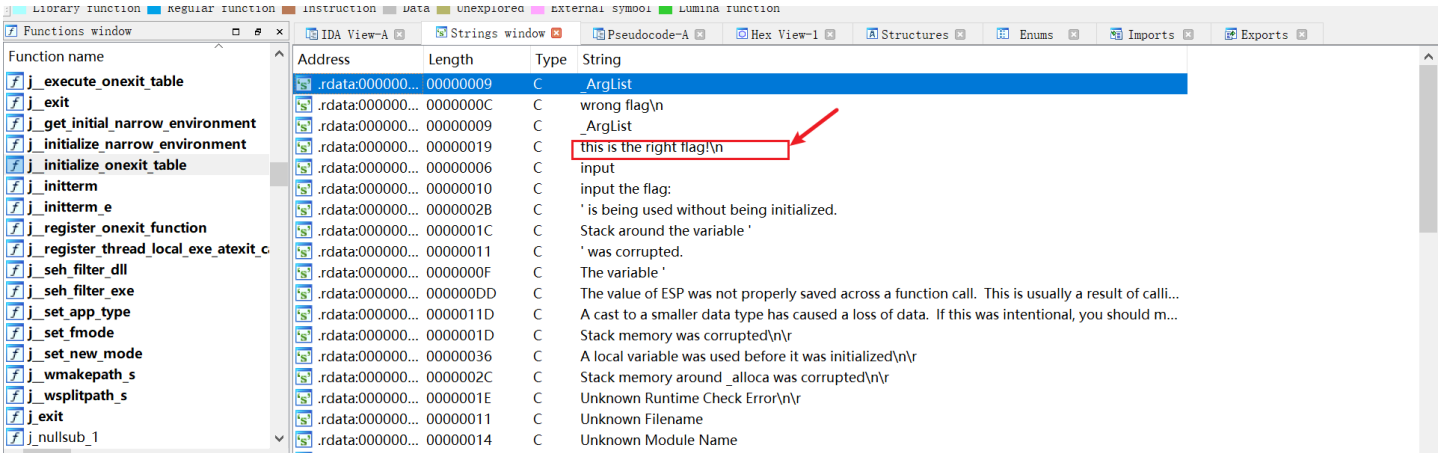
直接丢ida里面，就能看到flag

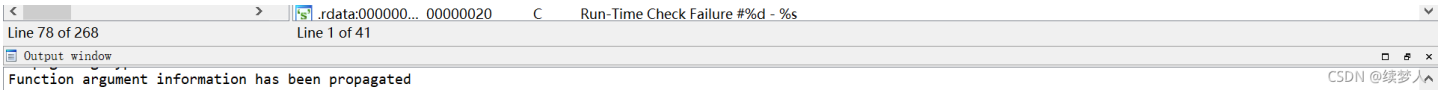


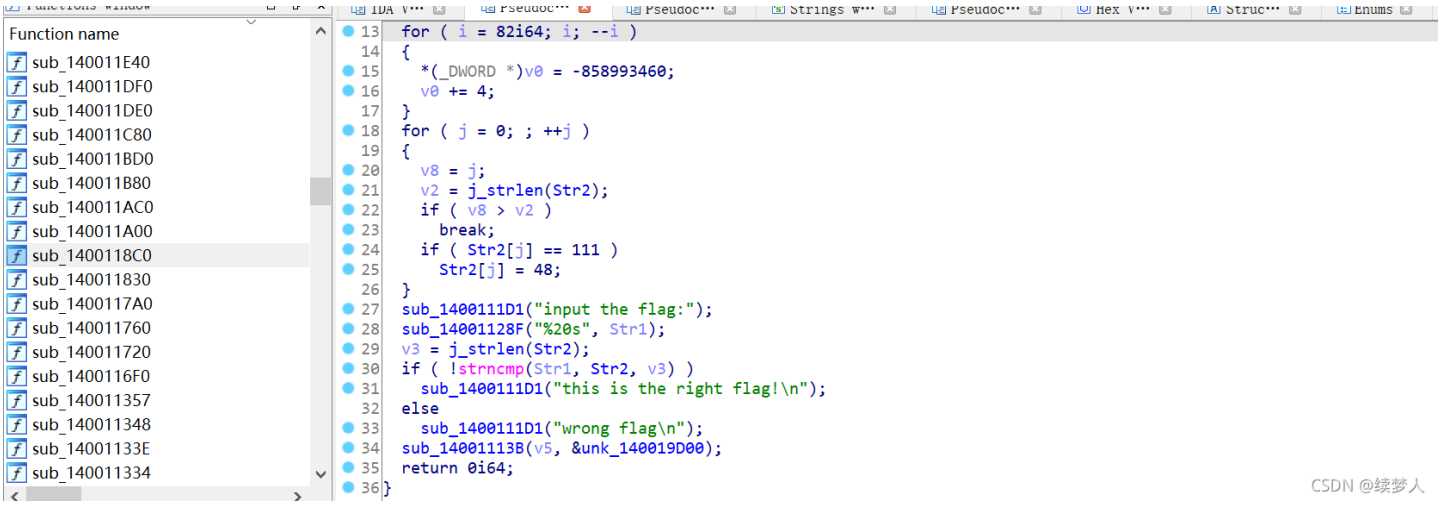
reverse1

F5反编译，查看函数

有点多，shift + F12查找字符串



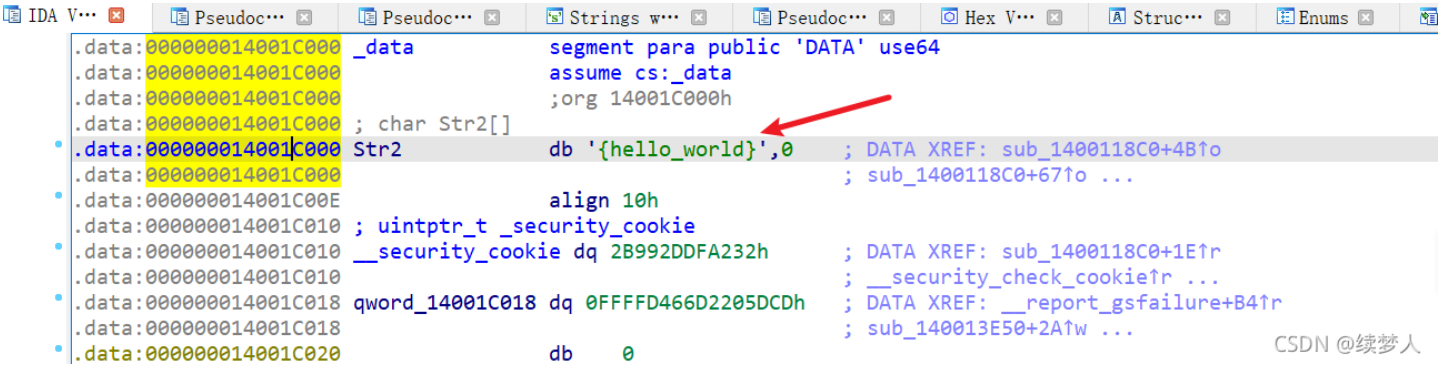




strncmp函数比较Str1和Str2是否xiangt
同时当字符的值是111时，要换成48

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

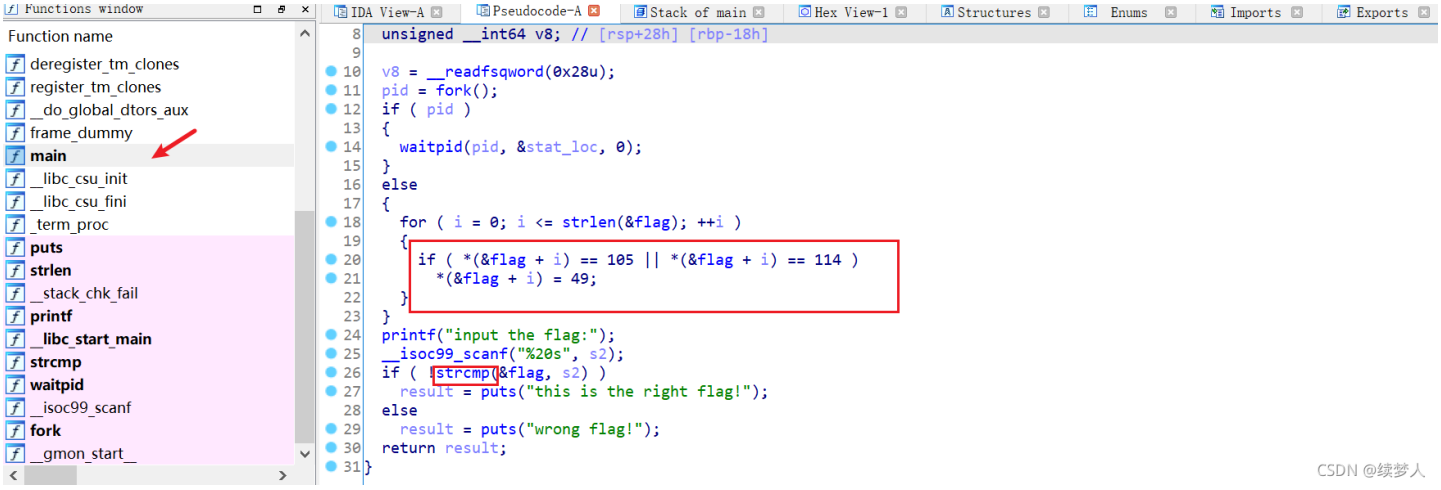
双击Str2



为了锻炼编程思想，写个脚本吧

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

reverse2



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;
}
}
```

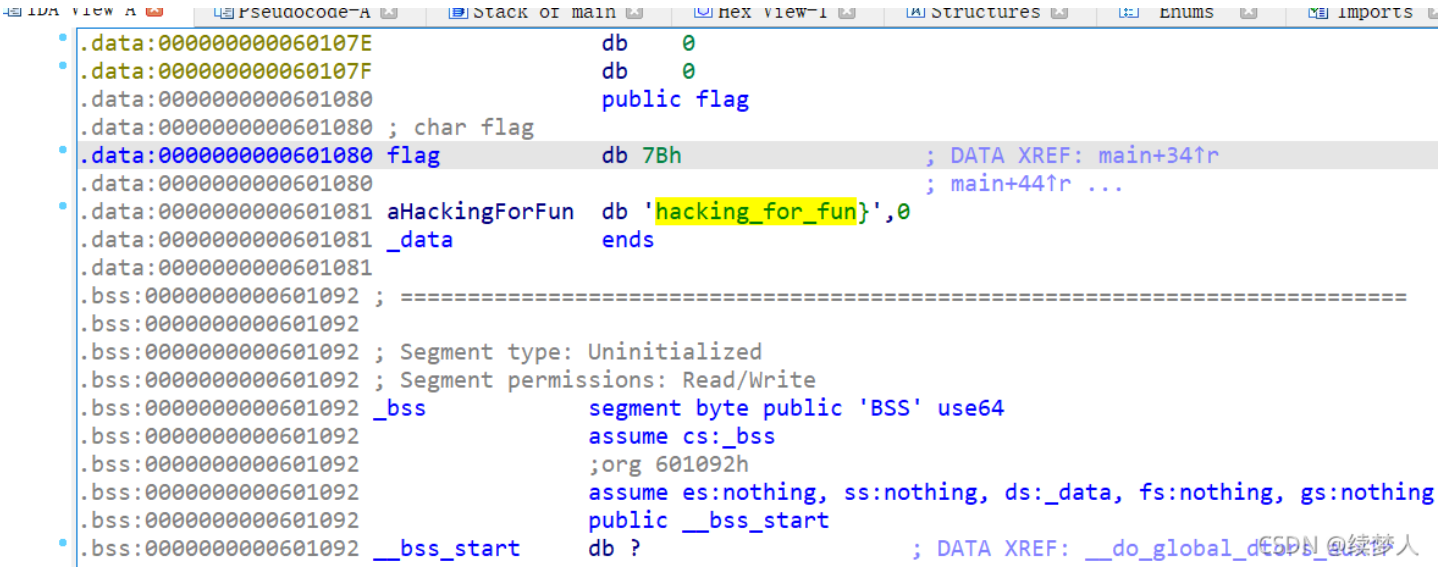
```
>>> chr(105)
'i'
>>> chr(114)
'r'
>>> chr(49)
'1'
>>>
```

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;
}
0000083A main:26 (40083A)
```

双击flag



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)
```