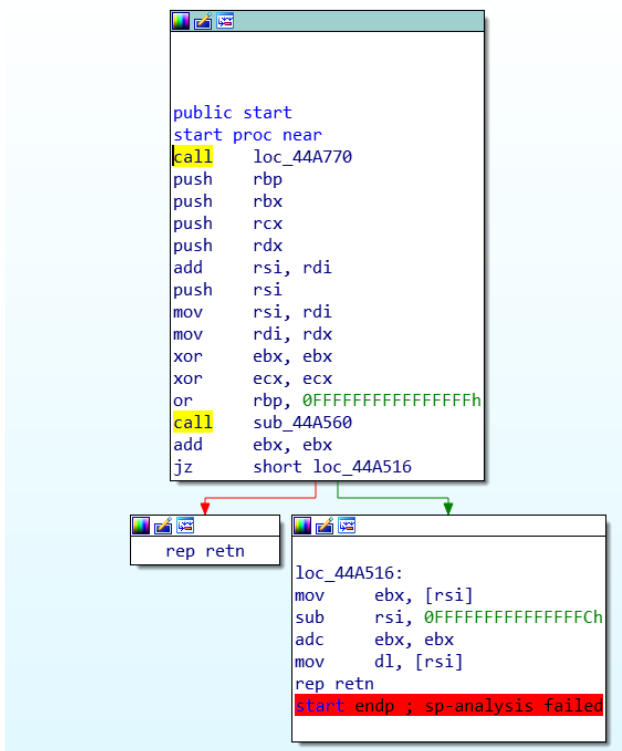


# [pwnable.kr] flag

문제 설명을 보면 리버싱 문제라고 나온다. 간단한 리버싱 문제인가 보다.

Gdb로 디스어셈블링 해보니 불가능하다고 한다. 그래서 아이다로 해봤는데 정체를 알 수 없는 내용만 나온다.

```
nicetauren@DESKTOP-6P5LMT7:/mnt/c/Users/82105/Downloads$ gdb-peda flag
Reading symbols from flag...
(No debugging symbols found in flag)
gdb-peda$ disas main
No symbol table is loaded. Use the "file" command.
```



분석에 실패했다고 한다.

왜인지 찾아보니 upx로 패킹 되어 있다고 이를 풀어줘야 풀 수 있다.

Upx는 여러 운영체제의 많은 파일 포맷을 지원하는 압축 프로그램이라고 한다.

구글링을 통해 upx.github.io에서 upx 언패킹 프로그램을 다운로드 후 언패킹 후 디스어셈블링하면 분석이 된다.

```

Dump of assembler code for function main:
0x0000000000401164 <+0>:    push    rbp
0x0000000000401165 <+1>:    mov     rbp, rsp
0x0000000000401168 <+4>:    sub     rsp, 0x10
0x000000000040116c <+8>:    mov     edi, 0x496658
0x0000000000401171 <+13>:   call    0x402080 <puts>
0x0000000000401176 <+18>:   mov     edi, 0x64
0x000000000040117b <+23>:   call    0x4099d0 <malloc>
0x0000000000401180 <+28>:   mov     QWORD PTR [rbp-0x8], rax
0x0000000000401184 <+32>:   mov     rdx, QWORD PTR [rip+0x2c0ee5]    # 0x6c2070 <flag>
0x000000000040118b <+39>:   mov     rax, QWORD PTR [rbp-0x8]
0x000000000040118f <+43>:   mov     rsi, rdx
0x0000000000401192 <+46>:   mov     rdi, rax
0x0000000000401195 <+49>:   call    0x400320
0x000000000040119a <+54>:   mov     eax, 0x0
0x000000000040119f <+59>:   leave
0x00000000004011a0 <+60>:   ret

```

여기서 누가봐도 flag가 있을 것 같은 주소를 가르키는 부분이 있다.

0x6c2070<flag> 이쪽을 조사해보면 될 듯 하다.

```

gdb-peda$ x 0x6c2070
0x6c2070 <flag>: 0x00496628

```

Flag의 바이너리 정보를 보니 가르키는 주소가 있다. 이 주소에 flag의 내용이 있을 것이다.

```

gdb-peda$ x/s 0x00496628
0x496628: "UPX...? sounds like a delivery service :)"

```

가르키는 주소에 있는 내용을 보니 flag가 나온다.