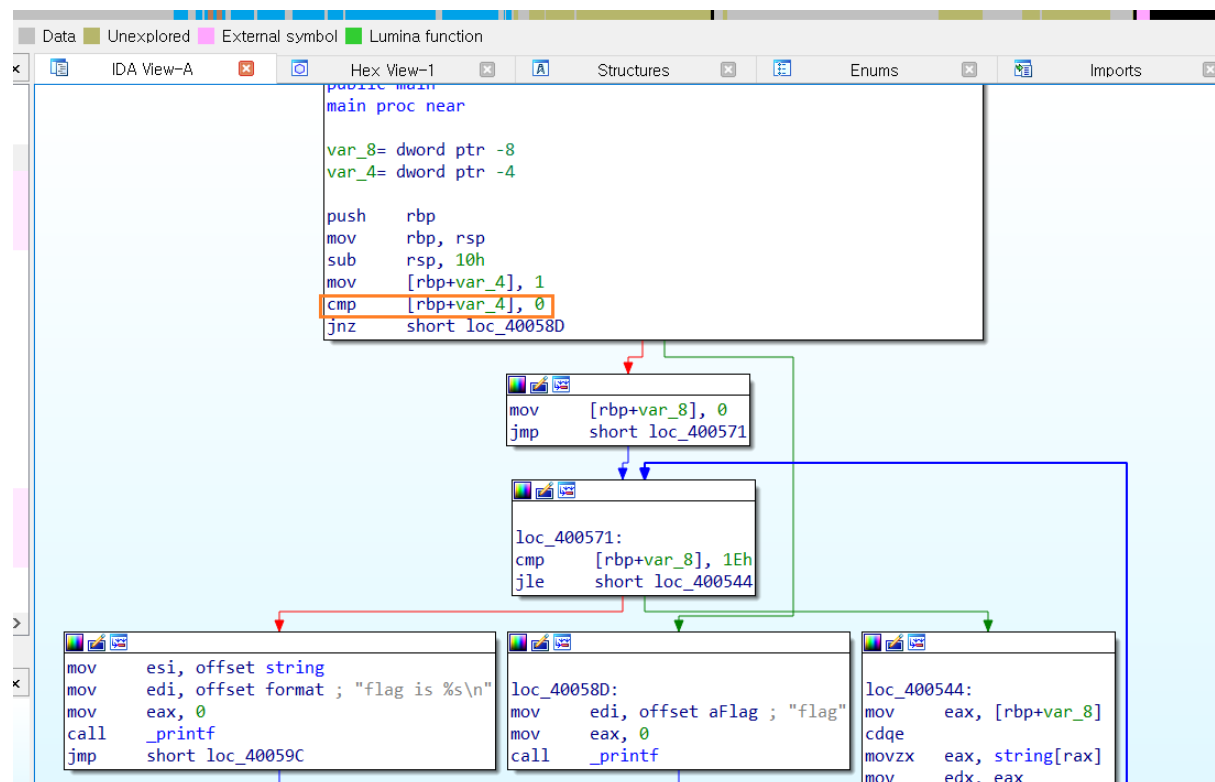


# Handray



음... 냐하하하하 라니! 뭔가 놀리는 것 같아서 열받는당! ㅎㅎ

일단 handray를 다운받아서 ida에 넣어보았다!



살펴보니 mov로 `[rbp+var_4]` 에 1을 넣어준 다음 0과 비교해서 같지 않으면 "flag를 뛰어넘었습니다"를 출력하는 곳으로 넘어간다. 따라서 우리는 저 `[rbp+var_4]` 에 0을 넣어주면 된다!

리눅스에서 `chmod` 로 실행권한 준 다음에 `gdb handray` 로 살펴보자!

```
gdb-peda$ disas main
Dump of assembler code for function main:
0x0000000000400526 <+0>:      push    rbp
0x0000000000400527 <+1>:      mov     rbp, rsp
0x000000000040052a <+4>:      sub     rsp, 0x10
0x000000000040052e <+8>:      mov     DWORD PTR [rbp-0x4], 0x1
0x0000000000400535 <+15>:     cmp     DWORD PTR [rbp-0x4], 0x0
0x0000000000400539 <+19>:     jne     0x40058d <main+103>
0x000000000040053b <+21>:     mov     DWORD PTR [rbp-0x8], 0x0
0x0000000000400542 <+28>:     jmp     0x400571 <main+75>
0x0000000000400544 <+30>:     mov     eax, DWORD PTR [rbp-0x8]
0x0000000000400547 <+33>:     cdq     
```

main+15에서 비교하니 `b *main+15` 를 한 다음 run을 해보자

```
Breakpoint 1, 0x0000000000400535 in main ()
gdb-peda$ x/wx $rbp-0x4
0x7fffffffef41c: 0x00000001
gdb-peda$ set *0x7fffffffef41c = 0
gdb-peda$ x/wx $rbp-0x4
0x7fffffffef41c: 0x00000000
```

[rbp-0x4]의 주소값을 알아내서 0으로넣어주고 확인한 다음 다시 시작해주자(c)

```
Breakpoint 1, 0x0000000000400535 in main ()
gdb-peda$ x/wx $rbp-0x4
0x7fffffffef41c: 0x00000001
gdb-peda$ set *0x7fffffffef41c = 0
gdb-peda$ x/wx $rbp-0x4
0x7fffffffef41c: 0x00000000
gdb-peda$ c
Continuing.
flag is HackCTF{.....}
[Inferior 1 (process 32982) exited normally]
```

그러면 flag 값을 알 수 있다!