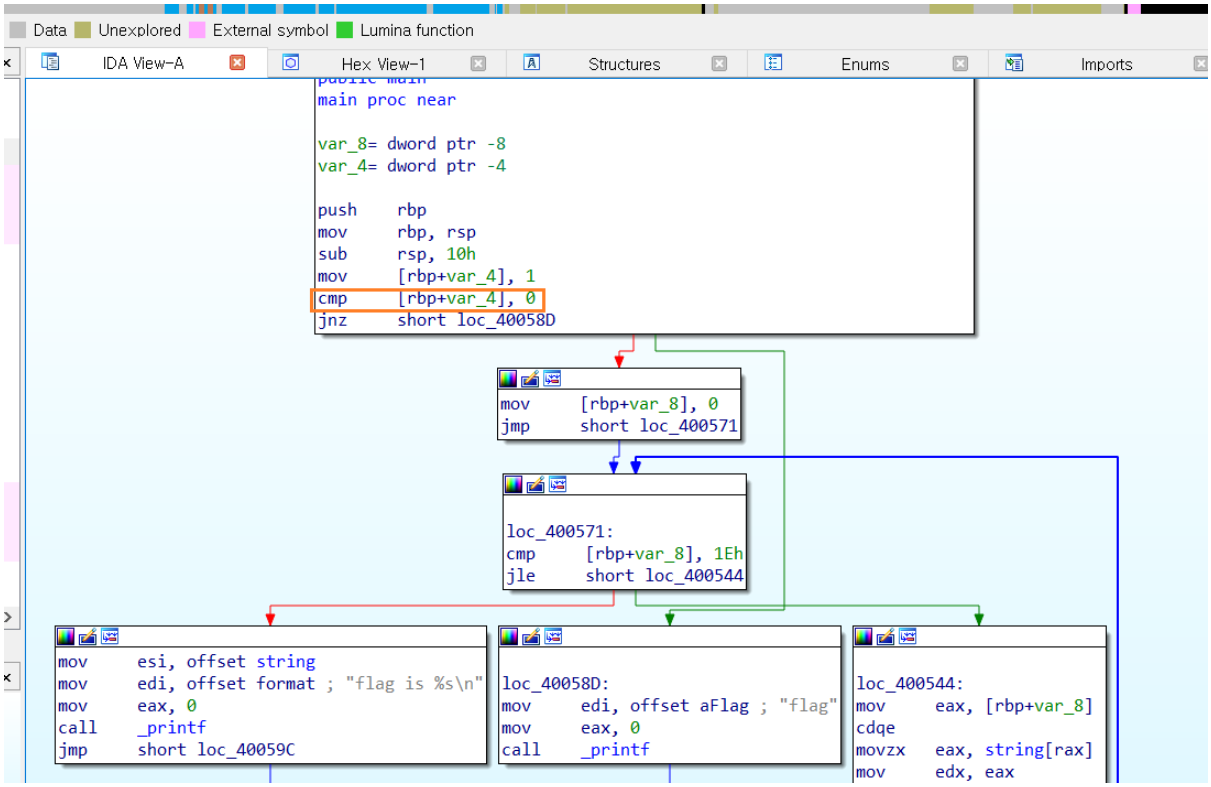
Handray

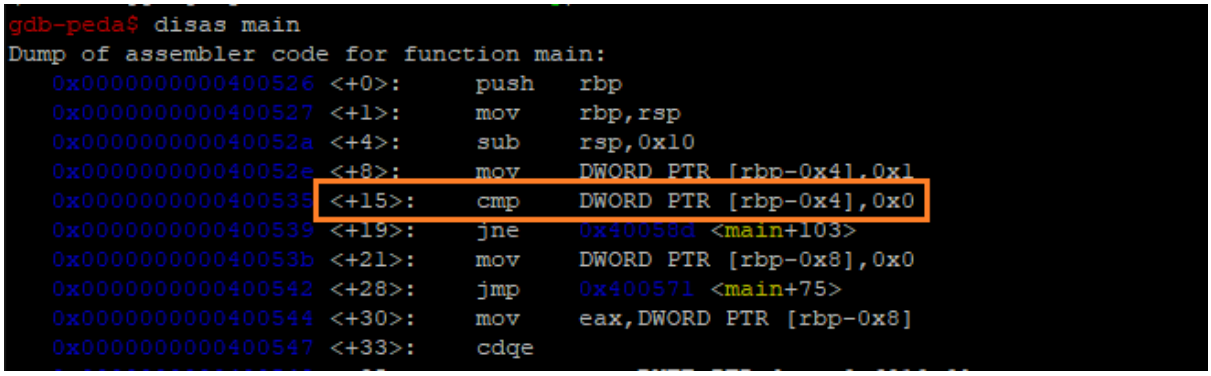
음... 냐하하하하 라니! 뭔가 놀리는 것 같아서 열받는당! ㅎㅎ

일단 handray를 다운받아서 ida에 넣어보았다!

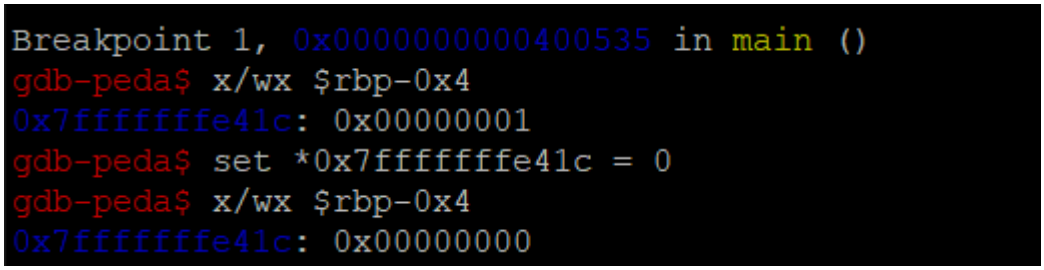


살펴보니 mov로 `[rbp+var_4]`에 1을 넣어준 다음 0과 비교해서 같지 않으면 "flag를 뛰어넘었습니다"를 출력하는 곳으로 넘어간다. 따라서 우리는 저 `[rbp+var_4]`에 0을 넣어주면 된다!

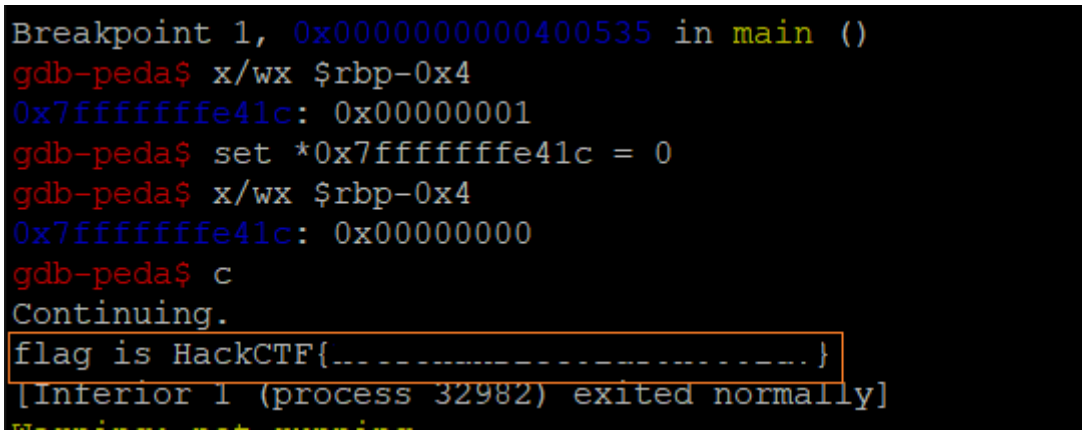
리눅스에서 `chmod`로 실행권한 준 다음에 `gdb handray`로 살펴보자!



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



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



그러면 flag 값을 알 수 있다!