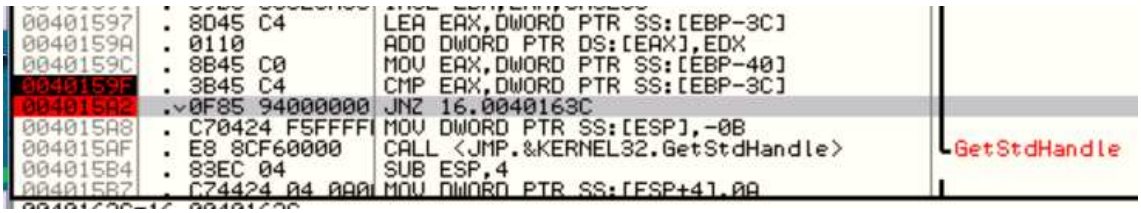
CodeEngn Basic RCE L16
: Name이 CodeEngn일때 Serial을 구하시오

15번 문제와 요구하는 것은 똑같은데,

16.exe를 실행시키면 위와 같은 콘솔 창이 나온다.

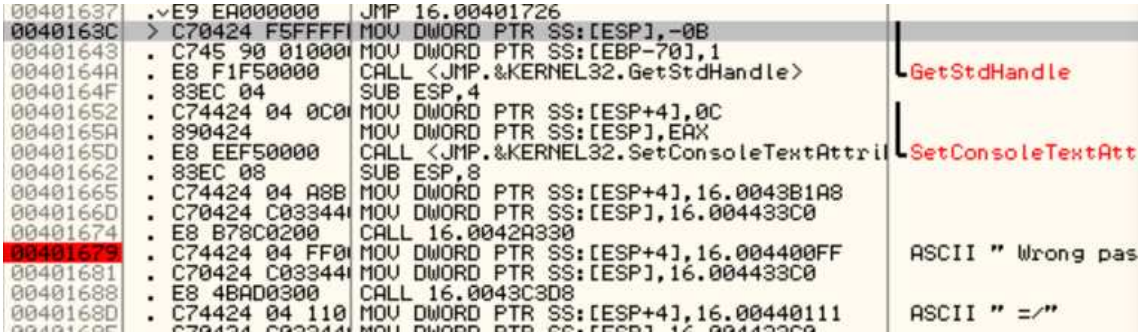


올리디버거에 올렸더니 에러메세지와 성공메세지 위에 CMP가 딱 하나 존재한다.

CMP EAX, DWORD PTR SS:[EBP-3C]
JNZ 0040163C

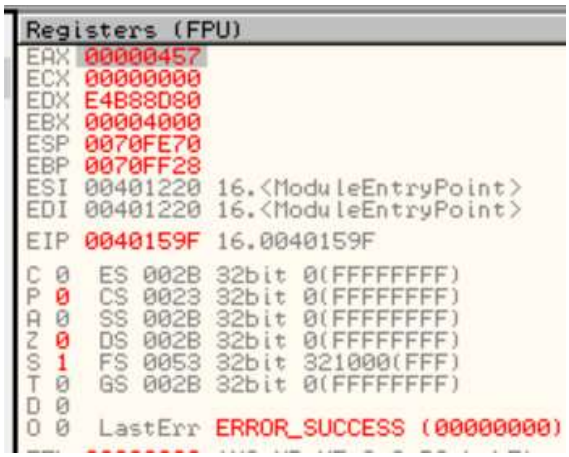
EAX와 스택영역의 EBP-3C의 4바이트 공간 값을 비교하고, 이 값이 같아야 성공메세지로 가게 된다.

반대로 0040163C 는

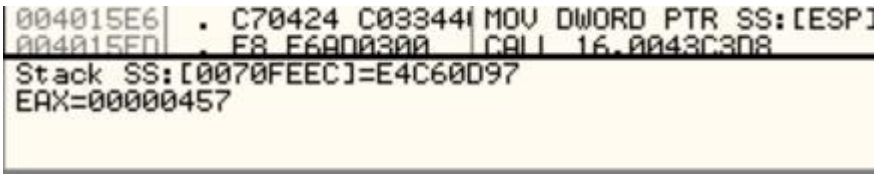


에러메세지 바로 위에 존재한다는 것을 알 수 있다.

CMP와 JNZ에 각각 BP를 걸고 실행했고, 이름과 패스워드를 입력하였다.



EAX값이 1111의 16진수 값 457 이므로, 1111을 입력한다는 것을 알 수 있다.
즉 NAME이 CodeEngn일 때의 패스워드 값은 "스택영역의 EBP-3C주소의 4바이트 값"이라는 것을 알 수 있다.



EBP-3C 는 0070FEEC이고, 이 값이 E4C60D97이라는 것을 올리디버거에서 알려주고 있다. E4C60D97은 4바이트 값도 맞기 때문에, 이게 답이라는 것을 알 수 있다! 이 외에도 밑에 HEX가 나와있는 곳에서 CTRL+G를 눌러 0070FEEC를 집어넣으면 확인이 가능하다.

굿잽 ! 이라는 성공 메세지가 나온다.