Codeengn Challenges Advance RCE LEVEL3 풀이

Reverse2 L03 Start

Author : Vallani

Korea :

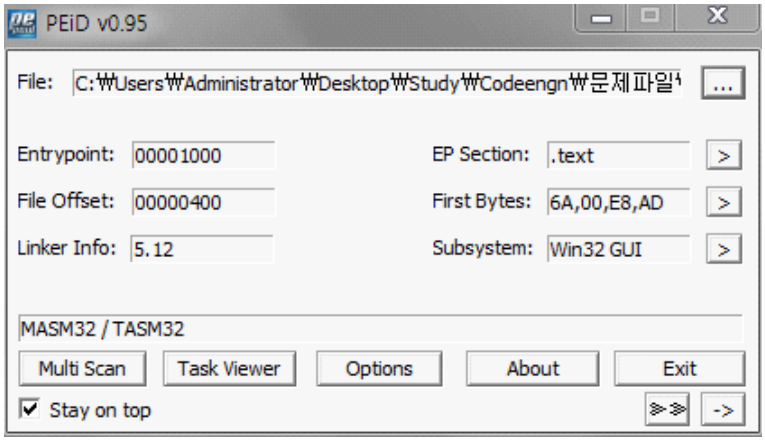
Name이 CodeEngn 일때 Serial은 무엇인가

English :

Find the Serial when the Name is CodeEngn

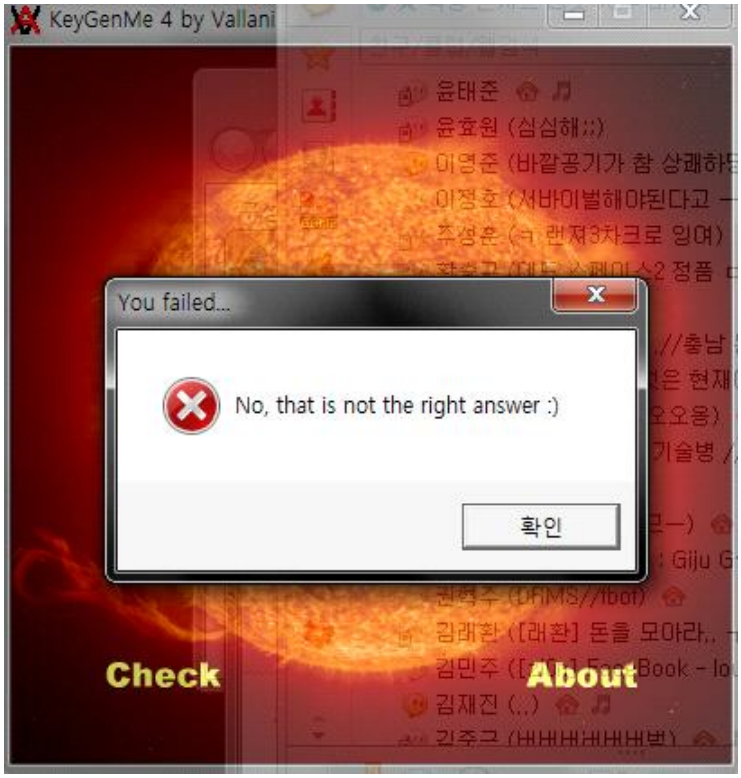
Down

프로그램을 실행시켜보니 이름을 입력하고 그에 맞는 시리얼을 입력 하는 프로그램이었다.
PEID로 프로그램에 대한 정보를 확인해보니,



어셈블리로 코딩된 프로그램이다.
어셈블리로 코딩된 프로그램들은 대게 리버싱에 불필요한게 많이 포함이 안되있어서 좋다 !

프로그램을 실행 시킨 후 NAME에 CodeEngn과 Serial에 123123을 넣은 후
Check 버튼을 눌렀는데,



다음과 같이 옳은 답이 아니라면서 버튼이벤트가 일어나야 프로그램이 활성화 되는 메세지창이 나왔다.

나는 이 문제를 풀기위해 OLLY DBG의 Back to User mode를 사용했다.

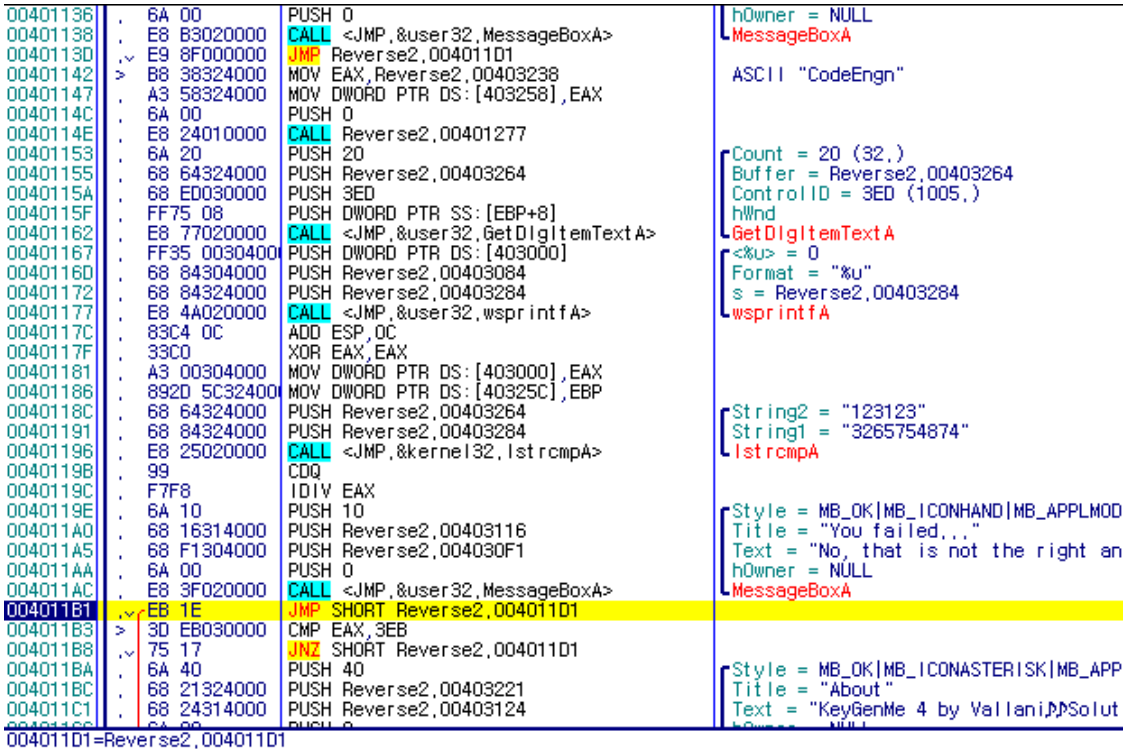
Back to User 기능은 프로세스가 뭐쳤을때 (입력을 받거나 , 버튼 입력을 받을때 등) 이용하면 좋은 기능이다, 특정 이벤트가 일어나기전에(버튼 이벤트같은)Back to User 모드를 설정해주고 이벤트를 수행하면, CALL 명령이 일어난 직후의 위치로 이동 하는 기능이다.

사용 방법은 다음과 같다,

1 . 프로그램을 OLLY로 실행이나 attach후 실행을 시킨 뒤
2 . 프로그램을 정지된 상태로 만든다.
3 . OLLY에서 일시 정지 버튼을 누른 후(F12)
4 . Back to user mode(ALT + F9)를 설정해준다
5 . 그리고 프로그램에서 이벤트를 발생시킨다. (예를 들어 예, 아니오 버튼 클릭 등)

이렇게 하면 OLLY가 표시하는 주소의 위치가 CALL명령이 일어난 직후로 이동이 된다.

실제로 프로그램에 NAME에 CodeEngn을 넣고 Serial에 123123을 넣은 후 확인 창에서 일어나는 버튼 이벤트를 이용해서 Back to User 기능을 쓰면



다음과 같은 화면이 나온다.

나는 여기서 문자열을 비교해주는 함수에서 답을 얻었다.