

codeengn-advance-L03 풀이


리버싱 문제풀이 / Wonlf / 2022. 5. 4. 13:27

Advance RCE L03

Name이 CodeEngn 일때 Serial은 무엇인가

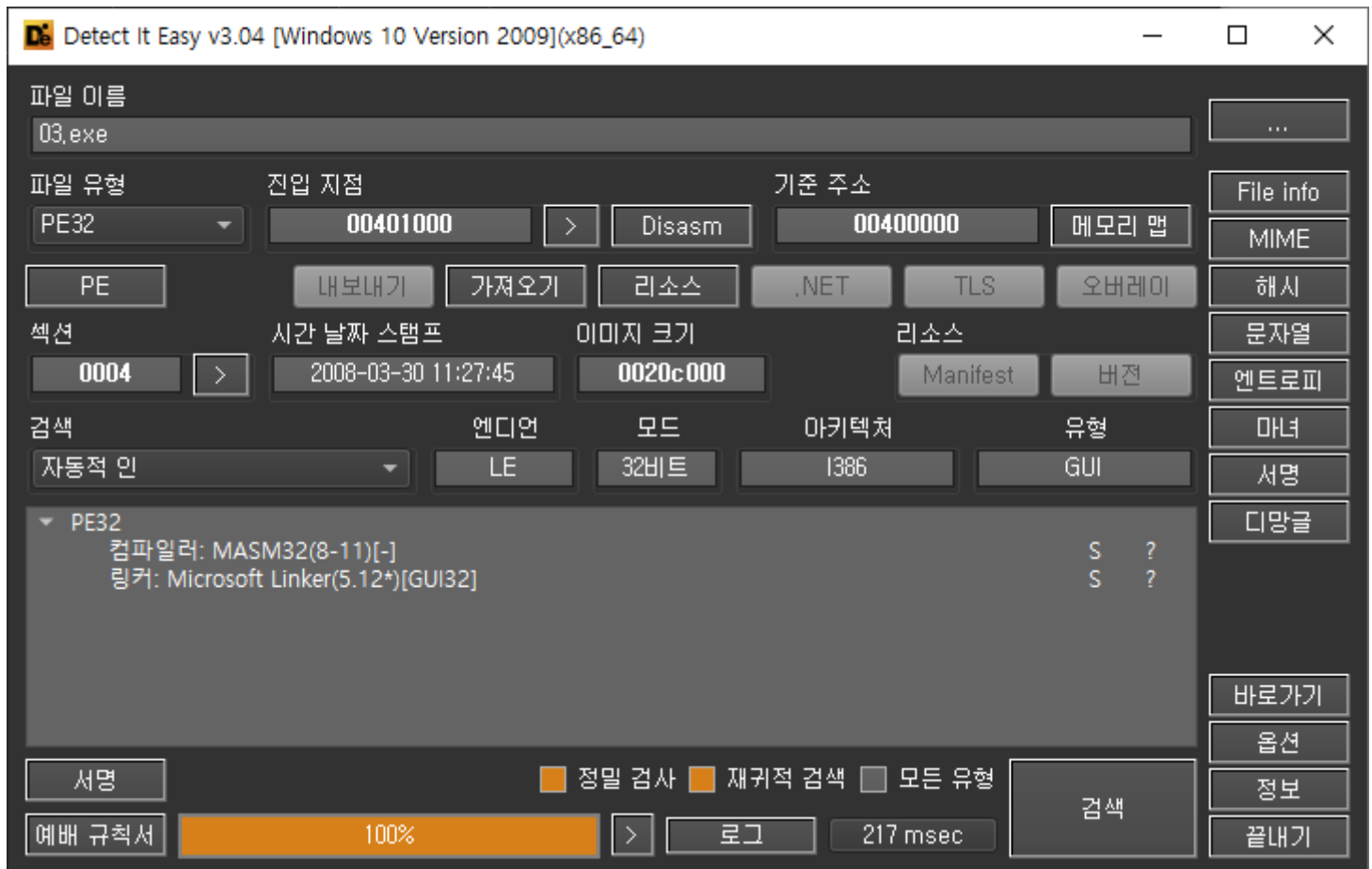
— Author: Vallani

— File Password: codeengn



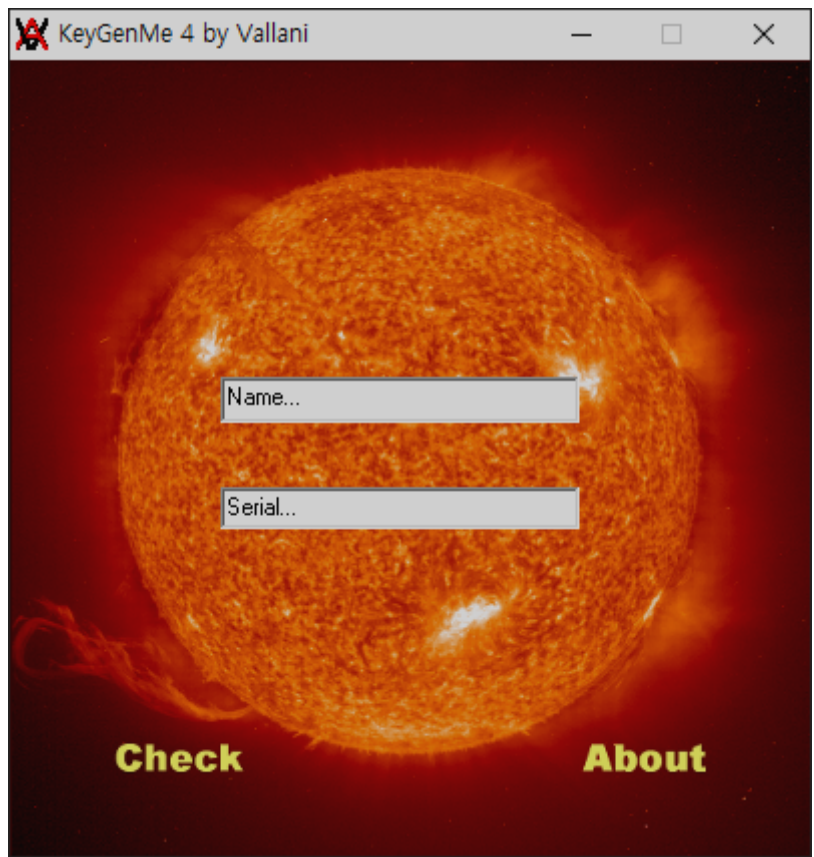
문제는 Name이 CodeEngn 일 때 Serial을 원하고 있다.

Die로 열어본다.



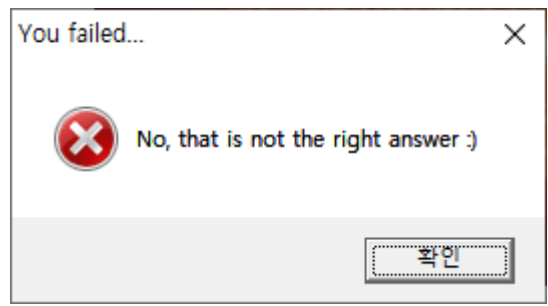
특이사항은 보이지 않는다.

파일을 실행시켜본다.



배경이 흐릿한 창이 뜨게 되고

Serial에서는 저 input을 말하는 것 같다.



특정 값을 입력 했을 때, 통과가 될지 안될지를 구분하는 것 같다.

디버거로 열어본다.

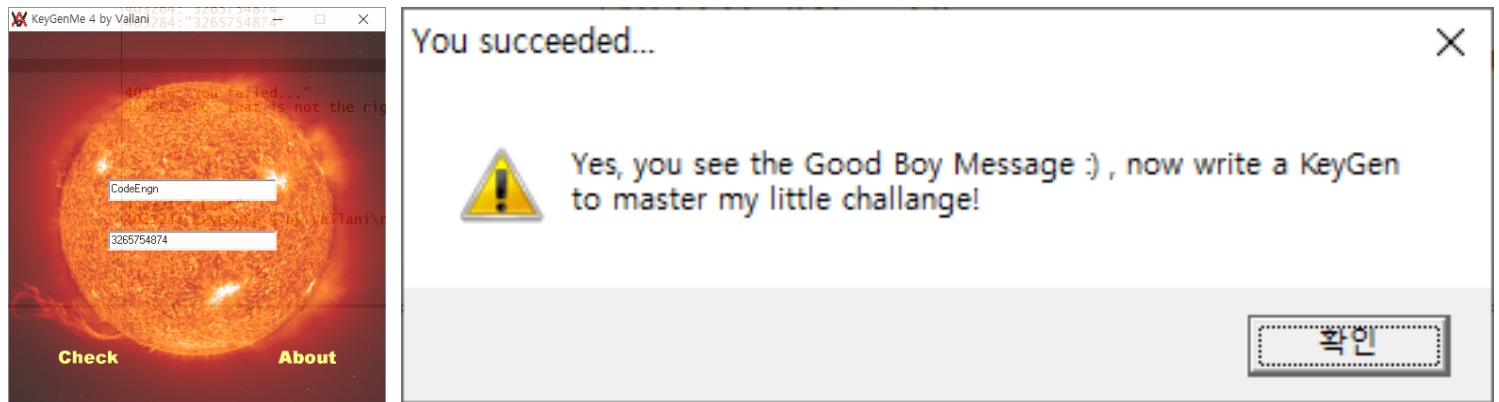
00401181	A3 00304000	mov dword ptr ds:[403000],eax	403264:"Serial..."
00401186	892D 5C324000	mov dword ptr ds:[40325C],ebp	403284:"2806763129"
0040118C	68 64324000	push 03.403264	
00401191	68 84324000	push 03.403284	
00401196	E8 25020000	call <JMP.&1strcmpA>	
0040119B	99	cdq	
0040119C	F7F8	idiv eax	
0040119E	6A 10	push 10	
004011A0	68 16314000	push 03.403116	403116:"You failed..."
004011A5	68 F1304000	push 03.4030F1	4030F1:"No, that is not the right answer :)"
004011AA	6A 00	push 0	
004011AC	E8 3F020000	call <JMP.&MessageBoxA>	
004011B1	EB 1E	jmp 03.4011D1	

input에 입력된 값을 그대로 하고 check를 눌렀을 때 나오는 문자열로 해당 구문이 있는 곳에 접근하였다.
시리얼 칸에 입력되어 있는 Serial... 과 특정 값인 2806763129 을 비교 하고 있다.

name에 CodeEngn을 입력하고 다시 구문에 들어가본다.

0040118C	68 64324000	push 03.403264	403264:"Serial..."
00401191	68 84324000	push 03.403284	403284:"3265754874"
00401196	E8 25020000	call <JMP.&1strcmpA>	
0040119B	99	cdq	
0040119C	F7F8	idiv eax	
0040119E	6A 10	push 10	
004011A0	68 16314000	push 03.403116	403116:"You failed..."
004011A5	68 F1304000	push 03.4030F1	4030F1:"No, that is not the right answer :)"

Name에 "Name..." 이라고 입력했을 때와 "CodeEngn" 을 입력 했을 때 비교하는 값이 "3265754874" 로 달라졌다.
이것을 Serial에 입력해본다.



통과가 되었다.
Serial을 홈페이지에 인증해주면 Success가 되었다.