

CodeEngn Basic RCE L18

: Name이 CodeEngn일때 Serial은 무엇인가

16번 문제와 비슷하게 시리얼을 찾는 문제이다.

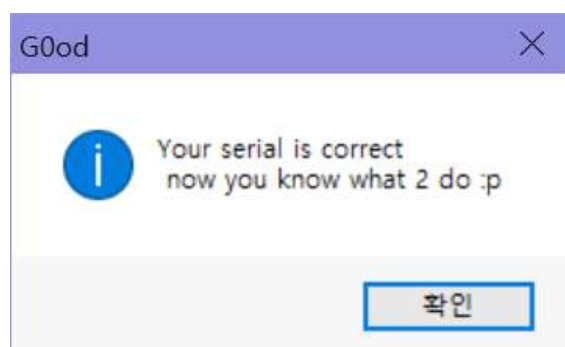
올리디버거에 올려 all text strings 찾아서 성공메세지/오류메세지 찾아 이동하였다.

004011E5	. 68 F0804000	PUSH 18.004080F0	String2 = "06162370056B6AC0"
004011E6	. 68 F07E4000	PUSH 18.00407EF0	String1 = "1111"
004011E7	. E8 DA000000	CALL <JMP.&kernel32.lstrcmpiA>	lstrcmpiA
004011E8	. 0BC0	OR EAX,EAX	
004011E9	. 74 16	JE SHORT 18.0040120E	
004011FA	. 6A 10	PUSH 10	Style = MB_OK MB_ICONHAND MB_APPLMODAL
004011FB	. 68 04664000	PUSH 18.00406604	Title = "Bad"
004011FC	. 68 E4654000	PUSH 18.004065E4	Text = "Your serial is Wrong, try again"
004011FD	. FF75 08	PUSH DWORD PTR SS:[EBP+8]	hOwner
004011FE	. E8 E6000000	CALL <JMP.&user32.MessageBoxA>	MessageBoxA
004011FF	. EB 5C	JMP SHORT 18.0040126A	
00401200	. 6A 40	PUSH 40	Style = MB_OK MB_ICONASTERISK MB_APPLMODAL
00401201	. 68 3C664000	PUSH 18.0040663C	Title = "Good"
00401202	. 68 08664000	PUSH 18.00406608	Text = "Your serial is correct! now you know what
00401203	. FF75 08	PUSH DWORD PTR SS:[EBP+8]	hOwner
00401204	. E8 D0000000	CALL <JMP.&user32.MessageBoxA>	MessageBoxA

오류메세지가 성공메세지보다 위쪽에 있는 걸로 보니 성공메세지로 점프하는 명령이 있을거라고 판단을 했고, 004011F6에 JE SHORT 0040120E로 이동하는 ( 성공메세지 ) 어셈블리어가 있다. 바로 위에 있는 함수를 보니 strcmp로, 문자열을 비교하는 함수이다.

004011D8	. 68 EC030000	PUSH 3EC	ControlID = 3EC (1004.)
004011D9	. FF75 08	PUSH DWORD PTR SS:[EBP+8]	hwnd
004011DA	. E8 01010000	CALL <JMP.&user32.GetDlgItemTextA>	GetDlgItemTextA
004011E5	. 68 F0804000	PUSH 18.004080F0	String2 = "06162370056B6AC0"
004011E6	. 68 F07E4000	PUSH 18.00407EF0	String1 = "1111"
004011E7	. E8 DA000000	CALL <JMP.&kernel32.lstrcmpiA>	lstrcmpiA
004011E8	. 0BC0	OR EAX,EAX	

인자값이 2개가 들어가는 것이 보이는데, 1111은 실행 시 내가 넣어준 임의의 값이고, string2에는 06162370056B6AC0 문자열이 들어가고 있다. 시리얼을 비교하는 것으로 보아 0616 ~~~ 이것이 이름이 CodeEngn일 때 시리얼 넘버라는 것을 추측할 수 있다.



성공 !!:)