

# Codeengn Basic RCE Level3 풀이

## Reverse L03 Start

Author : Blaster99 [DCD]

**Korea :**

비주얼베이직에서 스트링 비교함수 이름은?

**English :**

What is the name of the Visual Basic function that compares two strings?

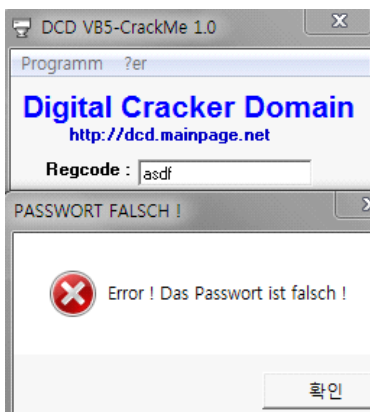
[Down](#)

무슨 프로그램인지 파일을 열어보았다.

MSVBVM50.dll 이 필요 하다 길래 dll을 설치해주고 프로그램을 실행해보았다.



Regcode를 입력하러해서 asdf를 넣어주고 Registrieren버튼을 눌렀다.



그러면 저런 에러가 뜬다.

아마 인증키와 똑같지 않다는것 같은데

프로그램을 분석하기위해 olly로 열어보았다.

Address	Hex dump	Disassembly	Comment
004028A5	3BC6	CMP EAX,ESI	
004028A7	7D 11	JGE SHORT A2DC1DEA,004028BA	
004028A9	68 A0000000	PUSH 0A0	
004028AE	68 F41D4000	PUSH A2DC1DEA,00401DF4	
004028B3	57	PUSH EDI	
004028B4	50	PUSH EAX	
004028B5	E8 84E8FFFF	CALL <JMP.&MSVBVM50,___vbaHresultCheckOb	
004028BA	FF75 A8	PUSH DWORD PTR SS:[EBP-58]	
004028BD	68 DC1D4000	PUSH A2DC1DEA,00401DDC	UNICODE "2683635Hs2"
004028C2	E8 83E8FFFF	CALL <JMP.&MSVBVM50,___vbaStrCmp>	
004028C7	8BF8	MOV EDI,EAX	
004028C9	8D4D A8	LEA ECX,DWORD PTR SS:[EBP-58]	
004028CC	F7DF	NEG EDI	
004028CE	1BFF	SBB EDI,EDI	
004028D0	47	INC EDI	
004028D1	F7DF	NEG EDI	
004028D3	E8 60E8FFFF	CALL <JMP.&MSVBVM50,___vbaFreeStr>	
004028D8	8D4D A4	LEA ECX,DWORD PTR SS:[EBP-5C]	
004028DB	E8 52E8FFFF	CALL <JMP.&MSVBVM50,___vbaFreeObj>	
004028E0	66 3BFE	CMP DI,SI	
004028E3	0F84 F3000000	JBE A2DC1DEA,004029DC	
004028E9	6A 08	PUSH 8	
004028EB	8D95 74FFFFFF	LEA EDX,DWORD PTR SS:[EBP-8C]	
004028F1	5E	POP ESI	
004028F2	8D4D AC	LEA ECX,DWORD PTR SS:[EBP-54]	
004028F5	C785 7CFFFFFF	MOV DWORD PTR SS:[EBP-84],A2DC1DEA,0040	UNICODE "Danke, das Passwort ist richtig !"
004028FF	89B5 74FFFFFF	MOV DWORD PTR SS:[EBP-8C],ESI	
00402905	E8 22E8FFFF	CALL <JMP.&MSVBVM50,___vbaVarCopy>	
0040290A	6A 03	PUSH 3	
0040290C	8D95 74FFFFFF	LEA EDX,DWORD PTR SS:[EBP-8C]	
00402912	5B	POP EBX	
00402913	8D4D DC	LEA ECX,DWORD PTR SS:[EBP-24]	
00402916	C785 7CFFFFFF	MOV DWORD PTR SS:[EBP-84],31	
00402920	8D9D 74FFFFFF	MOV DWORD PTR SS:[EBP-8C],EBX	
0040114A	<JMP.&MSVBVM50,___vbaStrCmp>		

Search for - > All intermodular calls 로 프로그램에 쓰인 전체적인 함수를 보고 그중에서 제일 문자열을 비교할만한 이름을 가진 vbaStrCmp 가 사용되는곳으로 이동해보았다.

함수호출전에 2G83G35Hs2 라는 문자열을 push해주고 vbaStrCmp라는 함수를 호출해준다.

아마 저 함수의 인자로 2G83G35Hs2 라는 문자열을 전달해준것 같다.

그리고 그 밑에 분기를 해주는데, 맞은 것, 안맞은 것을 메시지로 알려준다.

실제로 저 문자열을 프로그램의 문자열을 입력하는 박스에 넣고 인증을 해보면

인증키가 맞다고 나온다.

그러면 이제 codeengn이 원하는답이 뭔지 대충 짐작이 가지않는가?