

CodeEngn Reverse Challenge

Basic RCE #3

Reverse L03 Start

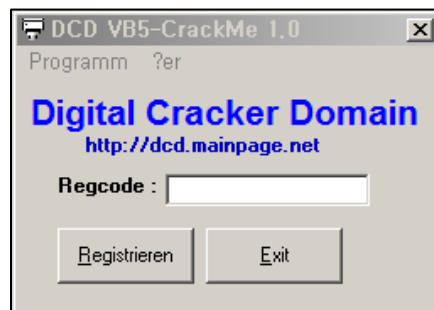
Author : Blaster99 [DCD]

Korea :
비주얼베이직에서 스트링 비교함수 이름은?

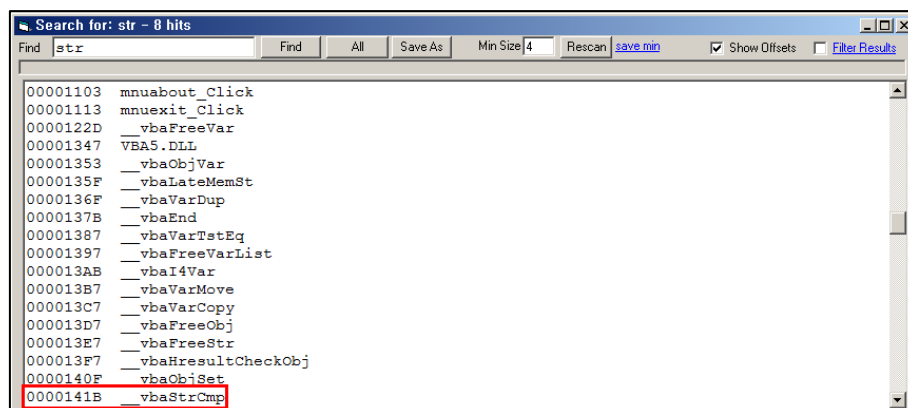
English :
What is the name of the Visual Basic function that compares two strings?

[Down](#)

문제는 문자열 비교함수의 이름을 묻고 있습니다. 문제 파일을 실행했을 때 보이는 다음 화면에서 사용자가 입력한 등록코드가 유효한지 검사하는 과정에서 해당 함수를 찾을 수 있을 것으로 생각했습니다.



이전 문제와 같이 문제 파일 안에서 유효 문자열을 검색했더니 의심되는 문자열을 발견할 수 있었습니다.



100%의 가까운 심증이 있지만 물증을 확보하기 위해서 올리디버거의 갖가지 유용한 기능을 찾아 공부해 보았고 현재 실행중인 모듈 안에서 심볼들을 검색하는 Ctrl+N 기능으로 쉽게 해당 함수를 찾고 브레이크 포인트도 설정 할 수 있었습니다.

Names in A2DC1DEA			
Address	Section	Type	Name
00405134	.idata	Import	MSVBVM50.EVENT_SINK_Release
00401168	.text	Export	<ModuleEntryPoint>
0040511C	.idata	Import	MSVBVM50.__vbaChkstk
004050F0	.idata	Import	MSVBVM50.__vbaEnd
00405140	.idata	Import	MSVBVM50.__vbaExceptionHandler
0040514C	.idata	Import	MSVBVM50.__vbaFPException
00405188	.idata	Import	MSVBVM50.__vbaFreeObj
00405184	.idata	Import	MSVBVM50.__vbaFreeStr
004050E8	.idata	Import	MSVBVM50.__vbaFreeVar
004050EC	.idata	Import	MSVBVM50.__vbaFreeVarList
004050FC	.idata	Import	MSVBVM50.__vbaHresultCheckObj
00405168	.idata	Import	MSVBVM50.__vbaI4Var
00405104	.idata	Import	MSVBVM50.__vbaLateMemSt
00405108	.idata	Import	MSVBVM50.__vbaObjSet
0040512C	.idata	Import	MSVBVM50.__vbaObjVar
00405124	.idata	Import	MSVBVM50.__vbaStrCmp
00405170	.idata	Import	MSVBVM50.__vbaVarCopy
0040516C	.idata	Import	MSVBVM50.__vbaVarDup
004050E4	.idata	Import	MSVBVM50.__vbaVarMove
00405128	.idata	Import	MSVBVM50.__vbaVarTstEq

References in A2DC1DEA: .text to MSVBVM50.__vbaStrCmp		
Address	Disassembly	Comment
0040114A	JMP DWORD PTR DS: [<MSVBVM50.__vbaStrCmp>]	MSVBVM50.__vbaStrCmp
004028C2	CALL <JMP.<MSVBVM50.__vbaStrCmp>>	
00402A2F	CALL <JMP.<MSVBVM50.__vbaStrCmp>>	

등록코드를 입력하고 등록 버튼을 누르면 미리 설치한 브레이크 포인트에서 실행이 멈춰지는 것을 봤을 때 예상이 맞은 것을 알 수 있었습니다.

004028B4	. 50	PUSH EAX	
004028B5	. EB 84E8FFFF	CALL <JMP.<MSVBVM50.__vbaHresultCheckObj>>	
004028BA	> FF75 A8	PUSH DWORD PTR SS: [EBP-58]	
004028BD	. 68 DC1D4000	PUSH A2DC1DEA.00401DDC	UNICODE "2G83G35Hs2"
004028C2	. EB 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	. 19FF	SBB EDI, EDI	
004028D0	. 47	INC EDI	
004028D1	. F7DF	NEG EDI	
004028D3	. EB 60E8FFFF	CALL <JMP.<MSVBVM50.__vbaFreeStr>>	
004028D8	. 8D4D A4	LEA ECX, DWORD PTR SS: [EBP-5C]	
004028DB	. EB 52E8FFFF	CALL <JMP.<MSVBVM50.__vbaFreeObj>>	
004028E0	. 66:3BFE	CMP DI, SI	
004028E3	. 0FB4 F3000000	JGE 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	. C7B5 7CFFFFFF	MOV DWORD PTR SS: [EBP-84], A2DC1DEA.004028FF	UNICODE "Danke, das Passwort ist richtig !"
004028FF	. 8B85 74FFFFFF	MOV DWORD PTR SS: [EBP-8C], ESI	
00402905	. EB 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	. C7B5 7CFFFFFF	MOV DWORD PTR SS: [EBP-84], 31	
00402920	. 8B85 74FFFFFF	MOV DWORD PTR SS: [EBP-8C], EBX	

vbaStrCmp 함수 첫 번째 인자로 전달되는 문자열 "2G83G35Hs2"을 확인해 보니 유효한 등록코드라는 것도 알 수 있었습니다.



문제의 정답은 "vbaStrCmp" 입니다.
감사합니다.

Team B10S letmeln