

# CodeEngn Basic RCE L03 Writeup



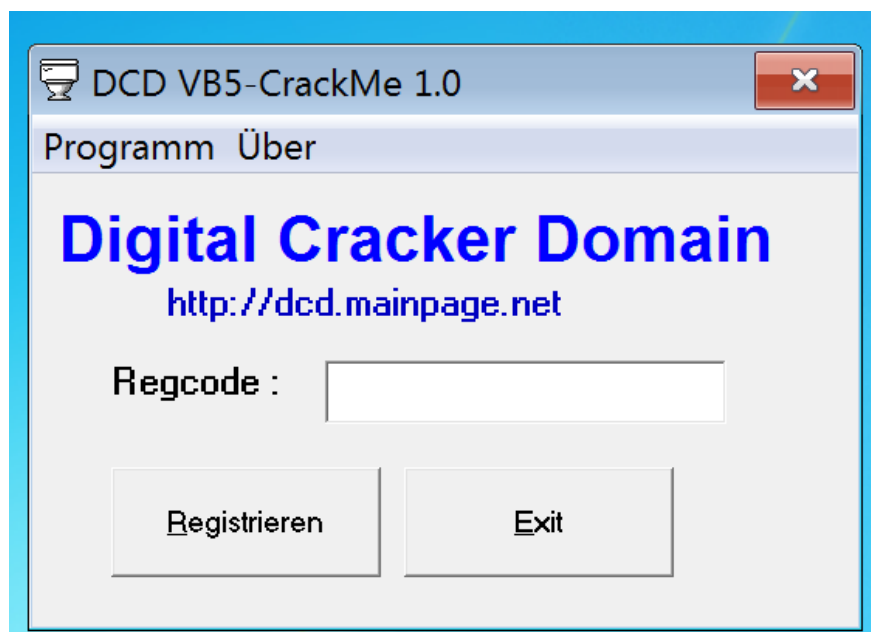
Daniel Smith

Feb 18 · 2 min read

Let's start RCE

Filename: 03.exe  
Description: 비주얼베이직에서 스트링 비교함수 이름은?  
Author: Blaster99 [DCD]

프로그램을 실행 시켜보자



실행 시

아무래도 패스워드 크랙 문제인 것 같다

Description 에서 string 비교 함수의 이름을 찾으라는 힌트를 주었으므로 All intermodular calls 로 현재 코드 영역에서 호출하려는 API 들을 살펴보자

```

0040116D CALL <JMP.&MSVBVM50.#100> MSVBVM50.ThunRTMain
00402891 CALL <JMP.&MSVBVM50.__vbaObjSet> MSVBVM50.__vbaObjSet
004028B5 CALL <JMP.&MSVBVM50.__vbaHresultCheckObj> MSVBVM50.__vbaHresultCheckObj
004028C2 CALL <JMP.&MSVBVM50.__vbaStrCmp> MSVBVM50.__vbaStrCmp
004028D3 CALL <JMP.&MSVBVM50.__vbaFreeStr> MSVBVM50.__vbaFreeStr
004028DB CALL <JMP.&MSVBVM50.__vbaFreeObj> MSVBVM50.__vbaFreeObj
00402905 CALL <JMP.&MSVBVM50.__vbaVarCopy> MSVBVM50.__vbaVarCopy
00402926 CALL <JMP.&MSVBVM50.__vbaVarMove> MSVBVM50.__vbaVarMove

```

vb 는 잘 모르지만 살펴보다 보면 친숙한 이름을 가진 vbaStrCmp 함수가 있다

```

004028B5 . E8 84E8FFF CALL <JMP.&MSVBVM50.__vbaHresultCheckObj>
004028BA > FF75 A8 PUSH DWORD PTR SS:[EBP-58]
004028BD . 68 DC1D400 PUSH 03.00401DDC UNICODE "2G83G35Hs2"
004028C2 . E8 83E8FFF CALL <JMP.&MSVBVM50.__vbaStrCmp>
004028C7 . 8BF8 MOV EDI,EAX
004028C9 . 8D4D A8 LEA ECX,DWORD PTR SS:[EBP-58]
004028CC . F7DF NEG EDI

```

들어가보면 이런 코드들이 보이는데 아마 오른쪽에 있는것이 패스워드인듯 하다

```

004028A5 . 3BC6 CMP EAX,ESI
004028A7 . 7D 11 JGE SHORT 03.004028BA
004028A9 . 68 A000000 PUSH 0A0
004028AE . 68 F41D400 PUSH 03.00401DF4
004028B3 . 57 PUSH EDI
004028B4 . 50 PUSH EAX
004028B5 . E8 84E8FFF CALL <JMP.&MSVBVM50.__vbaHresultCheckObj>
004028BA > FF75 A8 PUSH DWORD PTR SS:[EBP-58]
004028BD . 68 DC1D400 PUSH 03.00401DDC UNICODE "2G83G35Hs2"
004028C2 . E8 83E8FFF CALL <JMP.&MSVBVM50.__vbaStrCmp>
004028C7 . DCD VB5-CrackMe 1.0
004028C9 . 77 11 JGE SHORT 03.004028BA
004028CC . 77 11 JGE SHORT 03.004028BA
004028CE . 77 11 JGE SHORT 03.004028BA
004028D0 . 77 11 JGE SHORT 03.004028BA
004028D1 . 77 11 JGE SHORT 03.004028BA
004028D3 . 77 11 JGE SHORT 03.004028BA
004028D8 . 77 11 JGE SHORT 03.004028BA
004028DB . 77 11 JGE SHORT 03.004028BA
004028E0 . 77 11 JGE SHORT 03.004028BA
004028E3 . 77 11 JGE SHORT 03.004028BA

```

vbaStrCmp 에 BP 를 건뒤 “abcd” 문자열을 입력하여 stack을 살펴보자

```

0012F398 004028A5 77 11 JGE SHORT 03.004028BA
0012F39C 00401DDC Ü@. UNICODE "2G83G35Hs2"
0012F3A0 001720CC Ì|. UNICODE "abcd"
0012F3A4 0012F480 66↑

```

실행 후의 stack 모습

두 문자열을 비교하는 것 같다

2G83G35Hs2를 입력하면 성공

