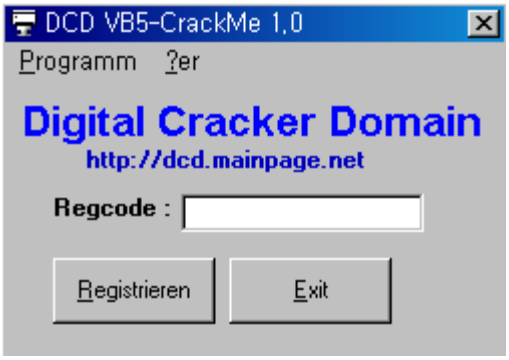
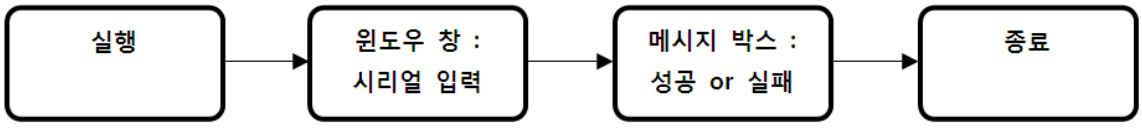
Basic RCE 03

작성자	koromoon (koromoon@naver.com)
작성일	2011-08
문제	비주얼베이직에서 스트링 비교함수 이름은?
정답	vbaStrCmp

(1) 설명

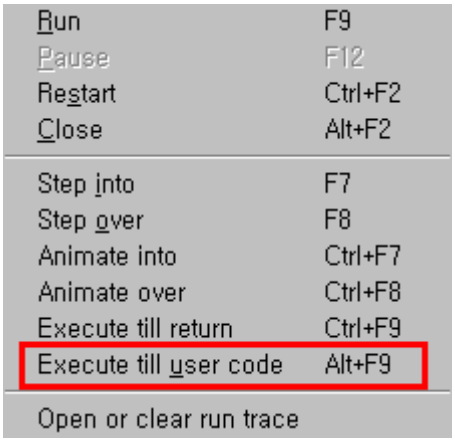


시리얼을 찾는 프로그램으로써 비밀번호를 입력하면 성공 메시지를 출력하고 그렇지 않으면 에러 메시지를 출력함. 또한 비주얼베이직으로 되어 있다는 걸 확인할 수 있음.



로직이 위와 같으며 스트링 검색을 해서 이벤트 시점을 찾아도 되지만 더 빠른 방법 중의 하나인 Back to user mode 방법을 이용함.

(2) Back to user mode



Back to user mode : 특정 이벤트를 일어나기 전에 설정해두고 Call 명령이 일어난 바로 다음 위치를 잡을 수 있는 방법

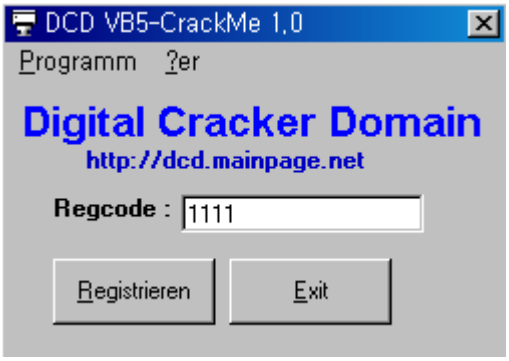
사용 순서 :

① 프로세스 attach (open)
② Run (F9)
③ 프로그램을 메시지 창과 같은 정지된 상태로 만듬.
④ paused (F12)
⑤ back to user mode (Alt+F9) 설정
⑥ 프로그램에서 이벤트 발생 (메시지 창에서는 확인 버튼 클릭)
⑦ OllyDbg에서 해당 부분에 커서가 설정됨.

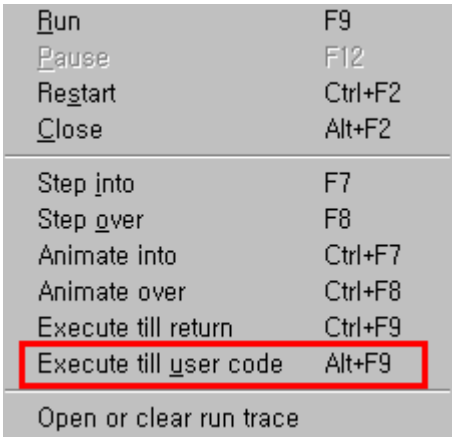
(주의할 점 : back to user mode 기능은 브라우저나 내부 스레드가 작동하는 프로그램의 경우에는 내부 이벤트가 수시로 일어나서 해당 모드가 풀려버리니 사용하려면 **메시지 박스와 같이 프로세스가 멈추는 상태에서 사용해야 함.**)

(3) 크랙 방법

OllyDbg에서 F9(Run)를 눌러서 프로그램을 실행함.



아무런 키값을 입력하고 확인을 눌르면 에러 메시지창이 나옴.



그때 F12(Pause)를 눌러서 정지하고 Alt+F9(Execute till user code)를 눌러서 Back to user mode로 들어가보자!

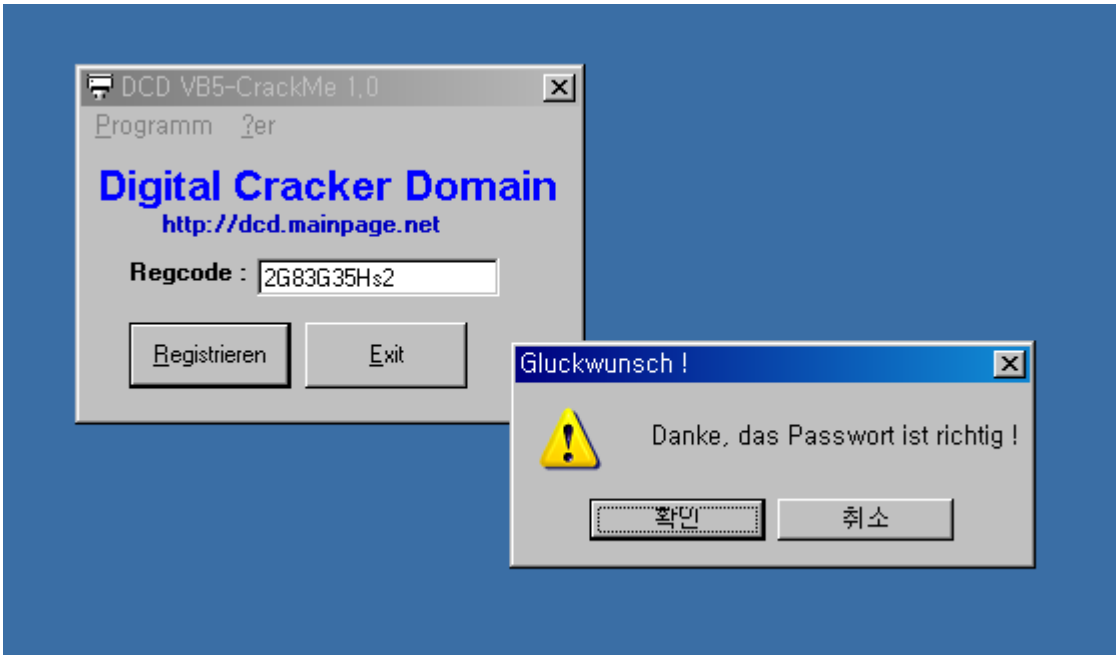
```
00402A52  .  66:83BD 48FF CMP WORD PTR SS:[EBP-B8],0
00402A5A  .v 0F84 E700000 JE A2DC1DEA.00402B47
00402A60  .  8D95 74FFFFF LEA EDX,DWORD PTR SS:[EBP-8C]
00402A66  .  8D4D AC      LEA ECX,DWORD PTR SS:[EBP-54]
00402A69  .  C785 7CFFFFF MOV DWORD PTR SS:[EBP-84],A2DC1DEA.0040  UNICODE "Error ! Das Passwort ist falsch !"
00402A73  .  C785 74FFFFF MOV DWORD PTR SS:[EBP-8C],8
00402A7D  .  E8 AAE6FFFF  CALL <JMP.&MSVBVM50.__vbaVarCopy>
00402A82  .  8D95 74FFFFF LEA EDX,DWORD PTR SS:[EBP-8C]
00402A88  .  8D4D DC      LEA ECX,DWORD PTR SS:[EBP-24]
00402A8B  .  C785 7CFFFFF MOV DWORD PTR SS:[EBP-84],10
00402A95  .  899D 74FFFFF MOV DWORD PTR SS:[EBP-8C],EBX
00402A9B  .  E8 86E6FFFF  CALL <JMP.&MSVBVM50.__vbaVarMove>
00402AA0  .  8D95 74FFFFF LEA EDX,DWORD PTR SS:[EBP-8C]
00402AA6  .  8D4D CC      LEA ECX,DWORD PTR SS:[EBP-34]
00402AA9  .  C785 7CFFFFF MOV DWORD PTR SS:[EBP-84],A2DC1DEA.0040  UNICODE "PASSWORT FALSCH !"
00402AB3  .  C785 74FFFFF MOV DWORD PTR SS:[EBP-8C],8
00402ABD  .  E8 6AE6FFFF  CALL <JMP.&MSVBVM50.__vbaVarCopy>
00402AC2  .  8D45 84      LEA EAX,DWORD PTR SS:[EBP-7C]
00402AC5  .  897D 8C      MOV DWORD PTR SS:[EBP-74],EDI
00402AC8  .  50           PUSH EAX
00402AC9  .  8D45 94      LEA EAX,DWORD PTR SS:[EBP-6C]
00402ACC  .  50           PUSH EAX
00402ACD  .  8D45 CC      LEA EAX,DWORD PTR SS:[EBP-34]
00402AD0  .  50           PUSH EAX
00402AD1  .  8D45 DC      LEA EAX,DWORD PTR SS:[EBP-24]
00402AD4  .  50           PUSH EAX
00402AD5  .  8975 84      MOV DWORD PTR SS:[EBP-7C],ESI
00402AD8  .  897D 9C      MOV DWORD PTR SS:[EBP-64],EDI
00402ADB  .  8975 94      MOV DWORD PTR SS:[EBP-6C],ESI
00402ADE  .  E8 37E6FFFF  CALL <JMP.&MSVBVM50.__vbaI4Var>
00402AE3  .  50           PUSH EAX
00402AE4  .  8D45 AC      LEA EAX,DWORD PTR SS:[EBP-54]
00402AE7  .  50           PUSH EAX
00402AE8  .  E8 33E6FFFF  CALL <JMP.&MSVBVM50.#595>
00402AED  .  8D95 54FFFFF LEA EDX,DWORD PTR SS:[EBP-AC]
00402AF3  .  8D4D BC      LEA ECX,DWORD PTR SS:[EBP-44]
00402AF6  .  8985 5CFFFFF MOV DWORD PTR SS:[EBP-A4],EAX
Stack address=0012F434
EDX=008F0608
```

에러 메시지창의 확인을 누르면 Call 명령이 일어난 바로 다음 위치로 이동하는 걸 확인하실 수 있음.

```
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 "2G83G35Hs2"
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  .v 0F84 F300000 JE A2DC1DEA.004029DC
004028E9  .  6A 08        PUSH 8
004028EB  .  8D95 74FFFFF LEA EDX,DWORD PTR SS:[EBP-8C]
004028F1  .  5E           POP ESI
004028F2  .  8D4D AC      LEA ECX,DWORD PTR SS:[EBP-54]
004028F5  .  C785 7CFFFFF MOV DWORD PTR SS:[EBP-84],A2DC1DEA.0040  UNICODE "Danke, das Passwort ist richtig !"
004028FF  .  89B5 74FFFFF MOV DWORD PTR SS:[EBP-8C],ESI
00402905  .  E8 22E8FFFF  CALL <JMP.&MSVBVM50.__vbaVarCopy>
```

```
00402A21  .  50            PUSH EAX
00402A22  .  E8 17E7FFFF   CALL <JMP.&MSVBVM50.__vbaHresultCheckOb
00402A27  >  FF75 A8       PUSH DWORD PTR SS:[EBP-58]
00402A2A  .  68 DC1D4000   PUSH A2DC1DEA.00401DDC                  UNICODE "2G83G35Hs2"
00402A2F  .  E8 16E7FFFF   CALL <JMP.&MSVBVM50.__vbaStrCmp>
00402A34  .  F7D8          NEG EAX
00402A36  .  1BC0          SBB EAX,EAX
00402A38  .  8D4D A8       LEA ECX,DWORD PTR SS:[EBP-58]
00402A3B  .  F7D8          NEG EAX
00402A3D  .  F7D8          NEG EAX
00402A3F  .  8985 48FFFFFF MOV DWORD PTR SS:[EBP-B8],EAX
00402A45  .  E8 EEE6FFFF   CALL <JMP.&MSVBVM50.__vbaFreeStr>
00402A4A  .  8D4D A4       LEA ECX,DWORD PTR SS:[EBP-5C]
00402A4D  .  E8 E0E6FFFF   CALL <JMP.&MSVBVM50.__vbaFreeObj>
00402A52  .  66:83BD 48FF  CMP WORD PTR SS:[EBP-B8],0
00402A5A  .v 0F84 E700000  JE A2DC1DEA.00402B47
00402A60  .  8D95 74FFFFFF LEA EDX,DWORD PTR SS:[EBP-8C]
00402A66  .  8D4D AC       LEA ECX,DWORD PTR SS:[EBP-54]
00402A69  .  C785 7CFFFFFF MOV DWORD PTR SS:[EBP-84],A2DC1DEA.0040  UNICODE "Error ! Das Passwort ist falsch !"
00402A73  .  C785 74FFFFFF MOV DWORD PTR SS:[EBP-8C],8
00402A7D  .  E8 AAE6FFFF   CALL <JMP.&MSVBVM50.__vbaVarCopy>
```

위로 좀 올라가 보면 성공 메시지와 에러 메시지 부분에서 공통적인 단어인 "2G83G35Hs2"가 시리얼 키값이며 그 밑에 vbaStrCmp 함수가 스트링 비교함수임.



시리얼 2G83G35Hs2 을 입력하면 성공 메시지가 뜸.