이 게시물은 magune에 2010-04-23 오후 4:08:08에 게시되었습니다.

Reverse Eng(Reverse L03 Start)

범주 Reverse Eng ; [범주 선택 또는 새 범주 입력]

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?

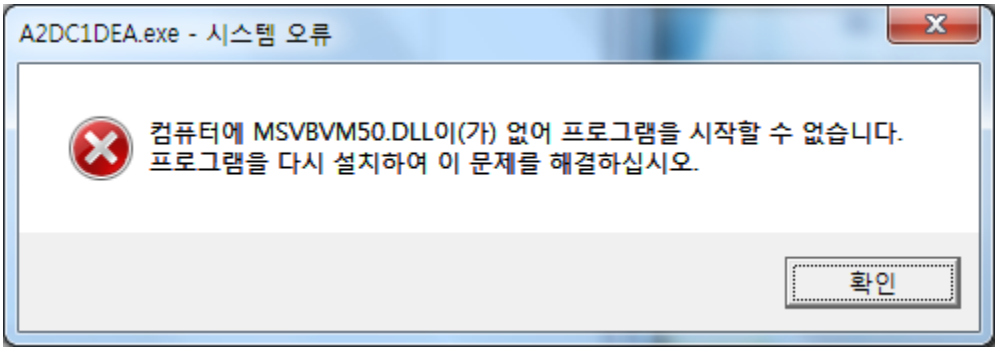
Down

총 86 분이 이 문제를 푸셨습니다. / 86 people solved this problem.

어느덧 3번 문제를 풀게 되었다.

이번엔 또 어떤 문제일까?? 비주얼베이직에서 스트링 비교함수 이름을 묻는 문제이다.

일단 다운받아서 어떤 프로그램인지 실행해 보자.



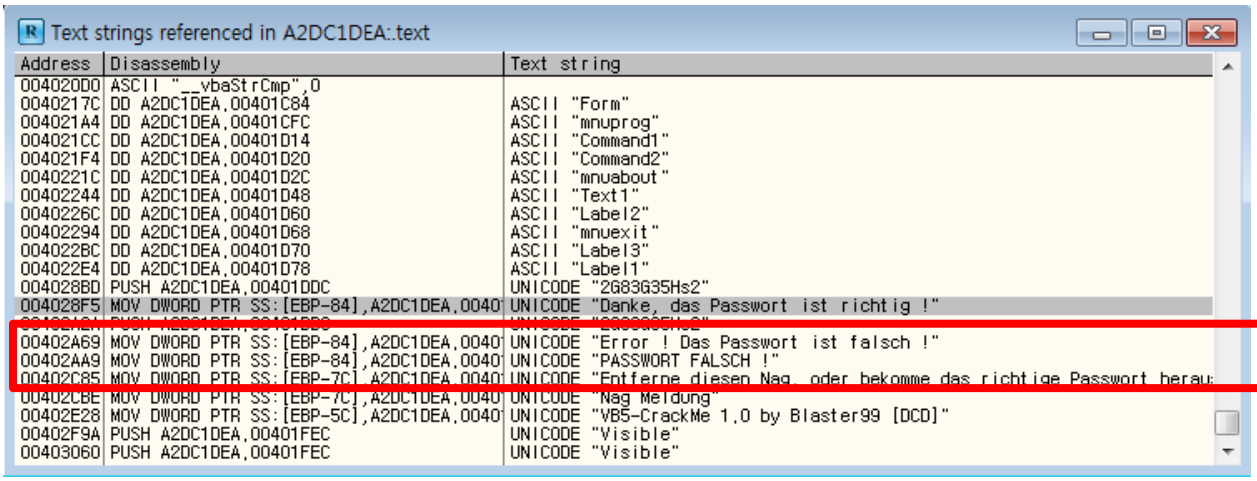
으잉?? 에러창이 뜬다. 비주얼베이직에서 사용하는 dll파일인거 같은데 실행이 안되는거 보니 파일이 있어야 문제를 풀 수 있을 것 같다. (dll파일은 첨부)

파일을 열어보니 메시지창이 뜨고 확인을 누르니 새로운 창이 떴다.

아무 패스워드를 넣고 Registrieren을 누르니 비밀번호가 틀렸다고 나온다.

자 이제 올리디버거를 넣고 돌려보자.

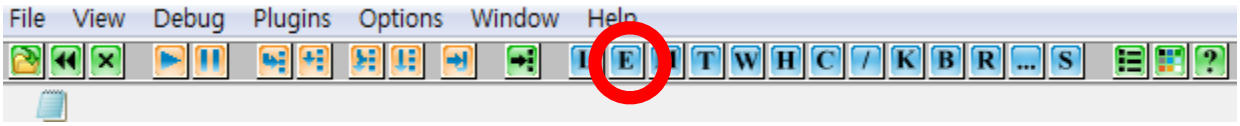
어떤식으로 진행이 되었는지는 알았으니 바로 속을 파보자. 마우스 오른쪽 클릭해서 search for -> All referenced text strings를 열어보자 또는 R아이콘을 클릭하면 된다.



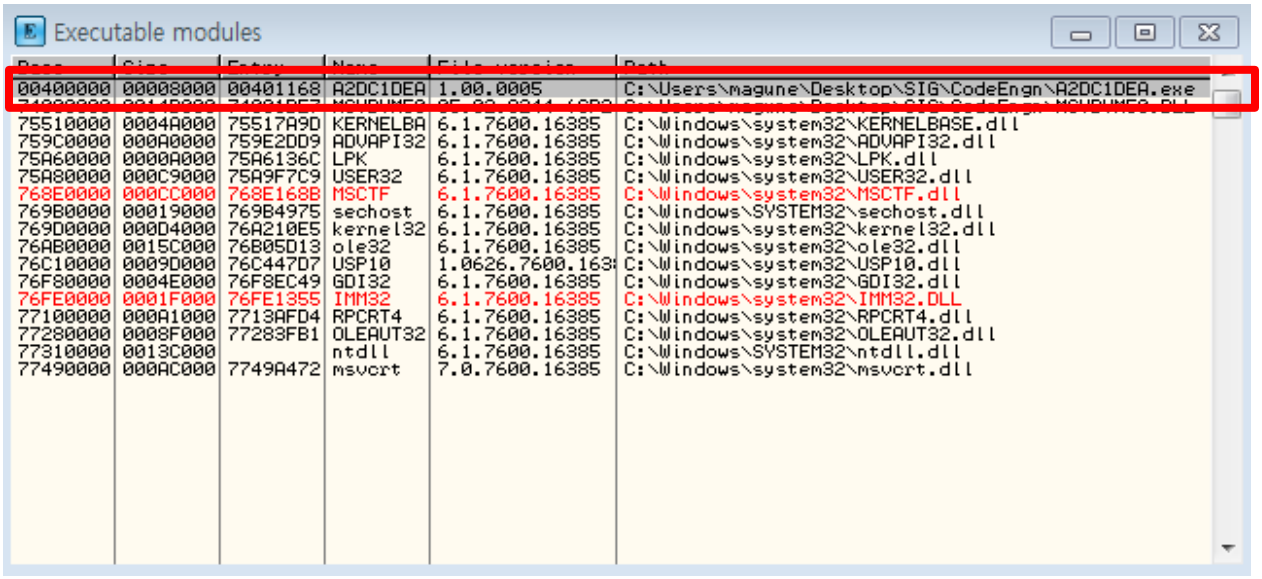
왼지 이상한 비밀번호와 함께 독일어로 패스워드가 맞다는 코드가 보인다. 더블클릭해보자. 패스워드가 맞다는 문구가 출력되기 위한 과정들을 위로 올려보며 보다 보니 왼지 아까 봤던 비밀번호같은것과 바로 아래 __vbaStrCmp라는 왼지 비주얼베이직 문자열(string) 비교(compare)이라는 느낌이 팍팍 풍기는 함수가 있다;;

그럼 확실히 문자열을 비교하는 함수인지 확인해 보자.

Window -> Executable modules를 누르거나 E아이콘을 클릭하면 된다.

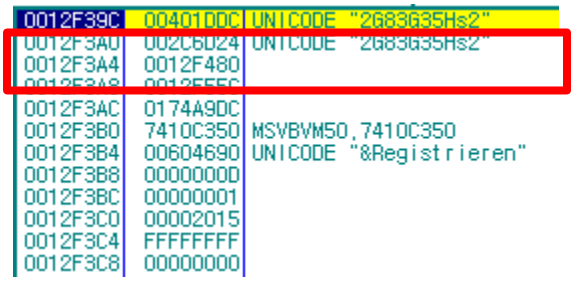


Executable modules는 실행 가능한 모든 모듈을 표시해 준다.

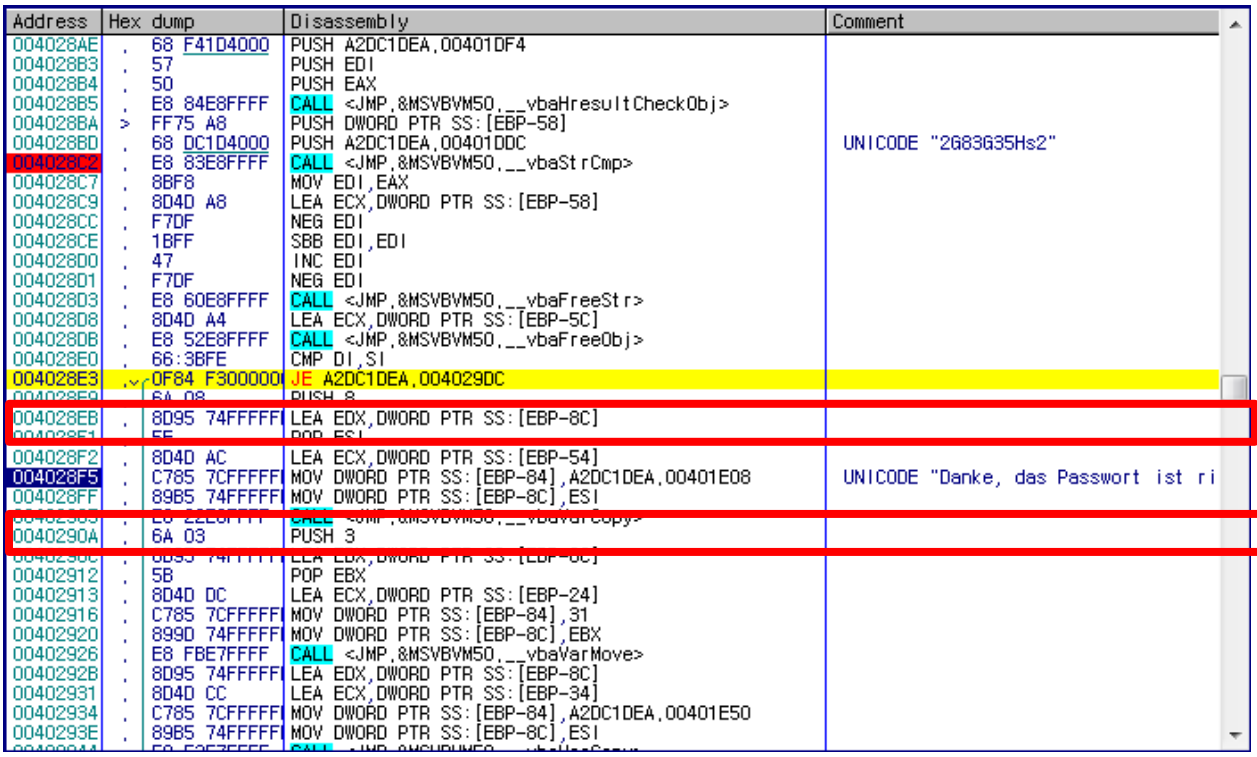


우리가 실행하고 있는 문제의 파일에 오른쪽 클릭을 하면 여러 세부 메뉴가 나오는데 View Names를 열어보자 그럼 아까 우리가 봤던 __vbaStrCmp라는 함수를 볼 수 있다. 마우스 오른쪽 클릭으로 Set breakpoint on every reference를 선택해서 참조가 된 모든 부분에 대해 브레이크 포인트를 걸어두자.

프로그램을 돌려보자. 이왕 돌리는 거 수상한 코드를 Regcode로 넣어보자. 브레이크 포인트에 도달하니 포즈상태가 되네?? 음 브레이크 포인트를 지정해 둔 vbaStrCmp를 호출하기 위해 스택에 두 개의 글자가 올라간 걸 볼 수 있다. 아 그럼 이거 가지고 비교를 하나 보다.



F8을 눌러가면서 좀 더 실행해 보자. 아래 그림을 보면 분기문이 보인다. 바로 패스워드가 맞다는 것과 틀리다를 결정하는 분기문인 것이다. (혹시 궁금 하면 화살표를 따라 추적해보자) 결국 이상한 코드는 비밀번호가 맞았고 패스워드가 맞다는 메시지 출력창을 나타낸다.



```
Address   Hex dump     Disassembly                                Comment
004028AE  .  68 F41D4000  PUSH A2DC1DEA,00401DF4
004028B3  .  57           PUSH EDI
004028B4  .  50           PUSH EAX
004028B5  .  E8 84E8FFFF  CALL <JMP,&MSVBVM50,__vbaHresultCheckObj>
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,00401E08  UNICODE "Danke, das Passwort ist ri
004028FF  .  89B5 74FFFFF MOV DWORD PTR SS:[EBP-8C],ESI
00402905  .  E8 22E8FFFF  CALL <JMP,&MSVBVM50,__vbaVarCopy>
0040290A  .  6A 03        PUSH 3
0040290C  .  8D95 74FFFFF LEA EDX,DWORD PTR SS:[EBP-8C]
00402912  .  5B           POP EBX
00402913  .  8D4D DC      LEA ECX,DWORD PTR SS:[EBP-24]
00402916  .  C785 7CFFFFF MOV DWORD PTR SS:[EBP-84],31
00402920  .  899D 74FFFFF MOV DWORD PTR SS:[EBP-8C],EBX
00402926  .  E8 FBE7FFFF  CALL <JMP,&MSVBVM50,__vbaVarMove>
0040292B  .  8D95 74FFFFF LEA EDX,DWORD PTR SS:[EBP-8C]
00402931  .  8D4D CC      LEA ECX,DWORD PTR SS:[EBP-34]
00402934  .  C785 7CFFFFF MOV DWORD PTR SS:[EBP-84],A2DC1DEA,00401E50
0040293E  .  89B5 74FFFFF MOV DWORD PTR SS:[EBP-8C],ESI
00402944  .  E8 F2E7FFFF  CALL <JMP,&MSVBVM50,__vbaVarCopy>
```