Korean :

비주얼베이직에서 스트링 비교함수 이름은?

English :

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

문자열 비교하는 함수..는 c언어에서는 strcmp였던걸로 기억하는데...일단 실행시켜보려고 하니까 이번에는 MSVBVM50.dll오류가 났다. MSVBVM50.dll을 받아서 설치했더니 실행되었다.

MSVBVM을 쓴걸로 봐서 이 프로그램은 비쥬얼베이직으로 만들어져 있음을 알 수 있다. (사실 문제에서 비쥬얼 베이직에서의 문자열 비교함수를 찾으라 했으니 주는 프로그램도 비쥬얼베이직으로 만들어진 것이겠다만)

실행해보니까 전에 실습했던 내용이었다. nag를 없애고 password를 찾아라!라는 그 프로그램이었다. 다만 조금 다른건 언어가 영어가 아니라는 점? password가 아니라 passwort라 쓰여있다. 그래도 돌아가는 방식은 비슷하겠거니 생각해서 search for-all referenced strings를 사용해서 문자열을 찾았다.

```
          ASCII "Label3"
          ASCII "Label1"
          UNICODE "2G83G35Hs2"
31E08     UNICODE "Danke, das Passwort ist richtig !"
          UNICODE "2G83G35Hs2"
31E70     UNICODE "Error ! Das Passwort ist falsch !"
31EB8     UNICODE "PASSWORT FALSCH !"
31EF0     UNICODE "Entferne diesen Nag, oder bekomme das richtige Passwort heraus !"
31F78     UNICODE "Nag Meldung"
31F94     UNICODE "VB5-CrackMe 1.0 by Blaster99 [DCD]"
          UNICODE "Visible"
```

이렇게 만든이가 써둔듯한 글귀들이 보인다. 근데 왠 반복되서 나오는 2G83G35Hs2라는 글자가 보인다. 그걸 더블클릭하여 해당 코드로 가봤더니

```
4028BA  >  FF75 A8      PUSH DWORD PTR SS:[EBP-58]
4028BD  .  68 DC1D4000  PUSH 00401DDC                 UNICODE "2G83G35Hs2"
4028C2  .  E8 83E8FFFF  CALL <JMP.&MSVBVM50.__vbaStrCmp>  Jump to MSVBVM50.__vbaStrCmp
4028C7  .  8BF8         MOV EDI,EAX
```

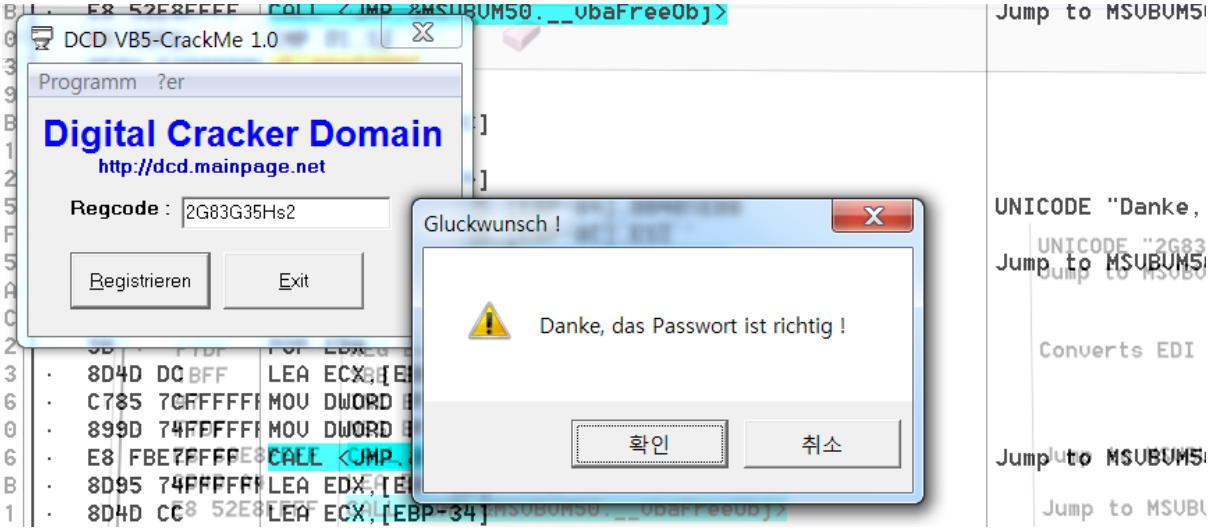
이렇게 비교함수가 나온다. 비쥬얼베이직에서 string을 비교cmp하는 함수 발견!

이때 함수주소를 직접 콜하는게 아니라 vbaStrCmp의 주소로 점프하라는 명령이 있는 주소로 간다.

그리고 정답을 쓰고 실행하다 보면

```
·   68 DC1D4000     PUSH 00401DDC                          UNICODE "2G83G35Hs2"
·   E8 83E8FFFF     CALL <JMP.&MSVBVM50.__vbaStrCmp>       Jump to MSVBVM50.__vbaStrCmp
·   8BF8            MOV EDI,EAX
·   8D4D A8         LEA ECX,[EBP-58]
·   F7DF            NEG EDI                                Converts EDI to boolean
·   1BFF            SBB EDI,EDI
·   47              INC EDI
·   F7DF            NEG EDI
·   E8 60E8FFFF     CALL <JMP.&MSVBVM50.__vbaFreeStr>      Jump to MSVBVM50.__vbaFreeStr
·   8D4D A4         LEA ECX,[EBP-5C]
·   E8 52E8FFFF     CALL <JMP.&MSVBVM50.__vbaFreeObj>      Jump to MSVBVM50.__vbaFreeObj
·   66:3BFE         CMP DI,SI
·   0F84 F3000000   JE 004029DC
·   6A 08           PUSH 8
·   8D95 74FFFFFF   LEA EDX,[EBP-8C]
·   5E              POP ESI
·   8D4D AC         LEA ECX,[EBP-54]
·   C785 7CFFFFFF   MOV DWORD PTR SS:[EBP-84],00401E08     UNICODE "Danke, das Passwort ist
·   89B5 74FFFFFF   MOV DWORD PTR SS:[EBP-8C],ESI
·   E8 22E8FFFF     CALL <JMP.&MSVBVM50.__vbaVarCopy>      Jump to MSVBVM50.__vbaVarCopy
```

이렇게 원하는 답 Danke, ~를 얻어낼 수 있다.



성공. Q3의 답은 __vbaStrCmp이고 이 프로그램의 등록코드는 2G83G35Hs2이다.