문제 : 비주얼베이직에서 스트링 비교함수 이름은?

사용된 모든 함수 보기

Ollydbg 우클릭 -> Search for -> All intermodular calls 클릭

```
00401168 PUSH 4018B8                (Initial CPU selection)
0040116D CALL 00401162              MSVBVM50.ThunRTMain
00402891 CALL 00401144              MSVBVM50.__vbaObjSet
004028B5 CALL 0040113E              MSVBVM50.__vbaHresultCheckObj
004028C2 CALL 0040114A              MSVBVM50.__vbaStrCmp
004028D3 CALL 00401138              MSVBVM50.__vbaFreeStr
004028DB CALL 00401132              MSVBVM50.__vbaFreeObj
00402905 CALL 0040112C              MSVBVM50.__vbaVarCopy
00402926 CALL 00401126              MSVBVM50.__vbaVarMove
```

수상한 함수명

우클릭 -> 해당 함수 사용으로 들어감

```
004028B3 . 57           PUSH EDI
004028B4 . 50           PUSH EAX
004028B5 . E8 84E8FFFF  CALL 0040113E                   <JMP.&MSVBVM50.__vbaHresultCheckObj>
004028BA > FF75 A8      PUSH DWORD PTR SS:[EBP-58]
004028BD . 68 DC1D4000  PUSH 401DDC                     UNICODE "2G83G35Hs2"
004028C2 . E8 83E8FFFF  CALL 0040114A                   <JMP.&MSVBVM50.__vbaStrCmp>
004028C7 . 8BF8         MOV EDI, EAX
004028C9 . 8D4D A8      LEA ECX, DWORD PTR SS:[EBP-58]
```

저기 회색줄이 저 함수가 실행되는 부분.

그니까 그 전에 Cmp(compare)하기 위해 비교할 스트링(str)을 받아야 함.

일단 하나 보이네? 2G83G35Hs2

이건 정답인 것 같고. 그 위를 보면 빈 칸 한줄 있고, CALL 하나가 더 있다

-> 다른 함수 사용

그럼 그 전에 입력 받아야 함.

004028BA에 BP(F2) 걸고 Run(F9) 하자.

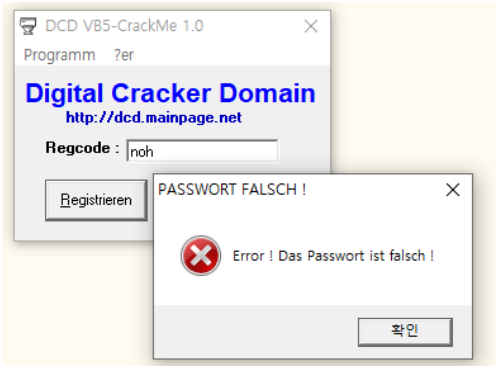
```
0019F240 00000000
0019F244 00000000
0019F248 00000000
0019F24C 00000038
0019F250 0274A90C
0019F254 00689C14 UNICODE "noh"
0019F258 00000000
0019F25C 0019F29C
0019F260 74DC31FC RETURN to win32u.74DC31FC
0019F264 76A8A209 RETURN to gdi32ful.76A8A209 from win32u.NtGdiPolyPatBlt
0019F268 00000000
```

pw로 noh 입력한 상태 -> 스택에 들어감.

여기서 F7 눌러서 다음줄 가자.

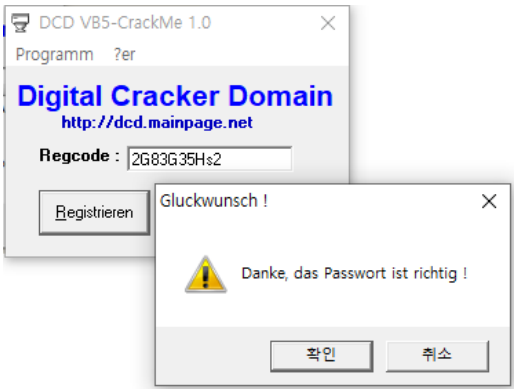
```
0019F1CC 0019F254
0019F1D0 004028A5 03.004028A5
0019F1D4 00401DDC UNICODE "2G83G35Hs2"
0019F1D8 00689C14 UNICODE "noh"
0019F1DC 0019F2B8
```

2G83G35Hs2 도 들어옴. 이제 이 두 개를 비교할 것 같다.



당연히 실패라고 뜸.

그럼 그냥 재시작해서 2G83G35Hs2 써보자. 이게 맞으면 vbaStrCmp가 문자열 비교함수 맞음.



맞다.

정답은 vbaStrCmp