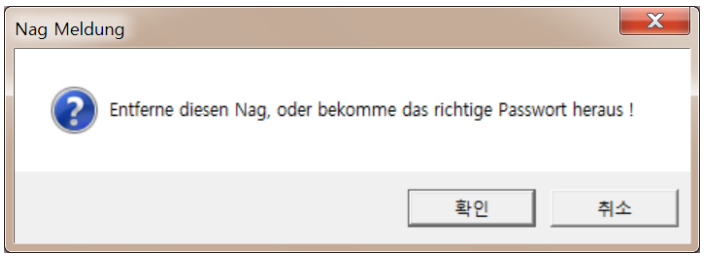
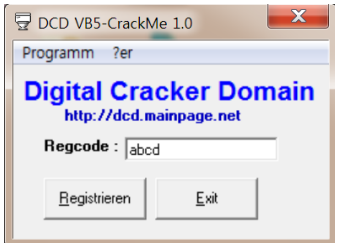
코드 엔진 Challenges: Basic 03

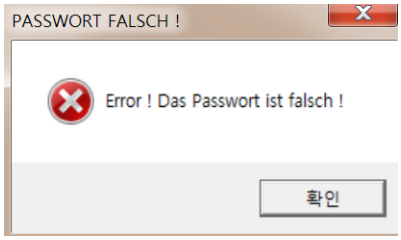
Author: Blaster99[DCD]
Korean: 비주얼베이직에서 스트링 비교 함수 이름은?

문제를 확인했으니 파일을 다운로드 받아서 실행해보자.



위와 패스워드를 찾으라는 것 같은 내용의 메시지 박스가 나타난다.





확인 버튼을 누르면 위와 같이 Regcode를 입력하는 창이 나오는데 여기에 아무 문자나 누르고 Registration을 눌렀을시 위와 같이 Error 박스가 나온다.

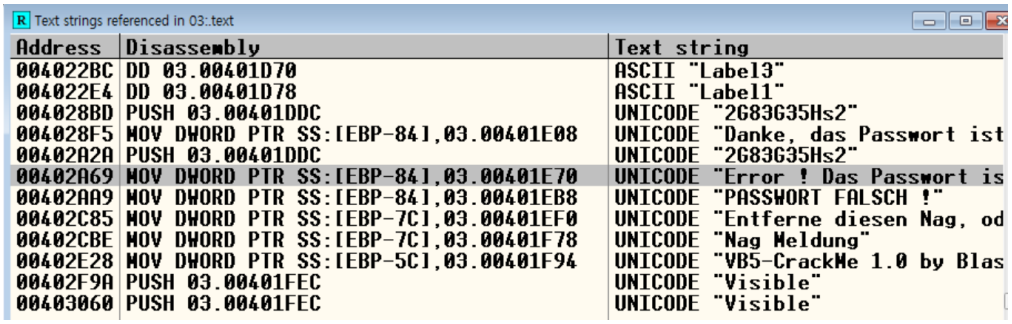
이 프로그램과 문제에서 비교함수를 찾으라는 점에서 이 프로그램이 패스워드와 사용자 입력값을 비교함수를 통해서 참과 거짓을 판단할 것 같다는 생각이든다.

먼저 PEView를 이용해서 IMAGE_OPTIONAL_HEADER를 통해 알아본 Entry Point는 00401168이며

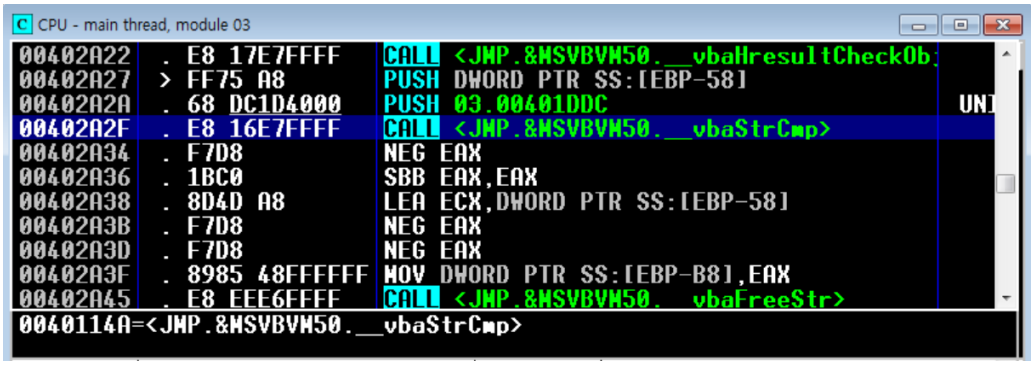
RVA	Data	Description	Value
000050E8	0F0FD0D2	Virtual Address	0000 __vbaFreeVar
000050EC	0F10182B	Virtual Address	0000 __vbaFreeVarList
000050F0	0F03873E	Virtual Address	0000 __vbaEnd
000050F4	0F0E7855	Virtual Address	0000 _adj_fdiv_m64
000050F8	0F0E7EDC	Virtual Address	0000 _adj_fprem1
000050FC	0F02B4EB	Virtual Address	0000 __vbaHresultCheckObj
00005100	0F0E7809	Virtual Address	0000 _adj_fdiv_m32
00005104	0F10322E	Virtual Address	0000 __vbaLateMemSt
00005108	0F01E2F2	Virtual Address	0000 __vbaObjSet
0000510C	0F0D405A	Virtual Address	0253
00005110	0F0E78A1	Virtual Address	0000 _adj_fdiv_m16i
00005114	0F0E79A1	Virtual Address	0000 _adj_fdivr_m16i
00005118	0F0399B2	Virtual Address	0000 _CIsin
0000511C	0F01F90B	Virtual Address	0000 __vbaChkstk
00005120	0F02299D	Virtual Address	0000 EVENT_SINK_AddRef
00005124	0F01F8F6	Virtual Address	0000 __vbaStrCmp
00005128	0F10B99E	Virtual Address	0000 __vbaVarTstEq
0000512C	0F03361F	Virtual Address	0000 __vbaObjVar
00005130	0F0E7F91	Virtual Address	0000 _adj_fpatan
00005134	0F037FD1	Virtual Address	0000 EVENT_SINK_Release
00005138	0F0342BF	Virtual Address	0000 _CIsqrt
0000513C	0F03634A	Virtual Address	0000 EVENT_SINK_QueryInterface

[Import Address Table]
IAT를 통해 본 결과 참조하는 함수가 매우 많으며 IAT의 RVA값과 Image Base(00400000) 결합한 000405124 주소가 실제 가리키고있는 _vbaStrCmp 함수가 스트링 비교 함수 일 것 같다. 이를 확인해보기위해서 올리디버거를 실행해 파일을 분석해보록하자.

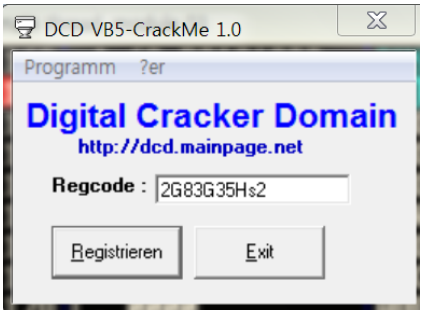
비교함수를 통한 방법이 맞다면 올리디버거의 검색기능으로 에러메시지 내용을 검색한 뒤 , 역으로 추적하면 비교함수를 찾을 수 있을 것이다. 그럼 먼저 올리디버거를 통해서 파일을 연 뒤 에러 메시지창의 메시지 내용을 검색해보자 .

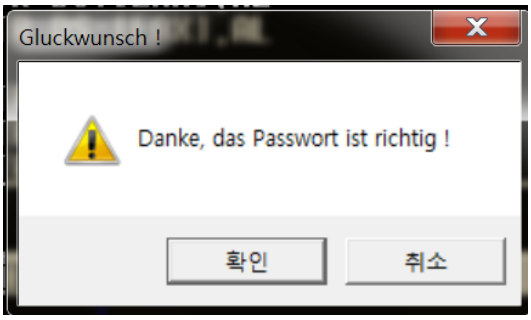


문자열 찾기 기능을 통해 에러 메시지를 더블 클릭해서 해당 메시지에 대한 코드영역으로 이동해보면



에러메시지를 찾고 그 주위의 코드를 둘러본 결과 다른 조건분기점들과 다르게 2가지 코드를 푸쉬하고 분기를 하며 그 중 위에서 수상하게 여긴 문자열과 (2G83G35Hs2) 다른 코드를 푸쉬하고 vbaStrCmp 함수를 호출하는 것을 보니 비교함수 일것이라는 것을 알 수 있다.
확인을 위해 RegCode칸에 2G83G35Hs2를 입력하자 암호가 맞다는 메시지를 출력하게된다.





더 정확한 확인을 위해 004028C2에 BP를 설정하고 실행시키면 우리가 입력한 Regcode는 004028BA에 저장되는 것을 볼 수 있다.

문제에 대한 정답은 vbaStrCmp 함수이다.