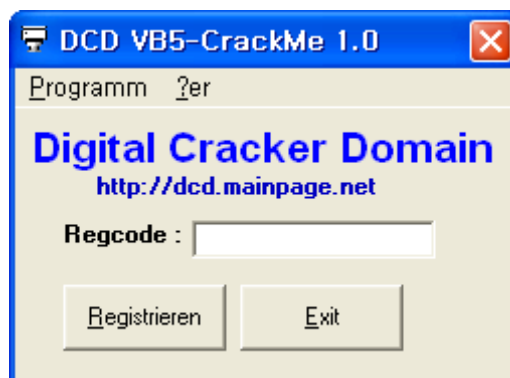
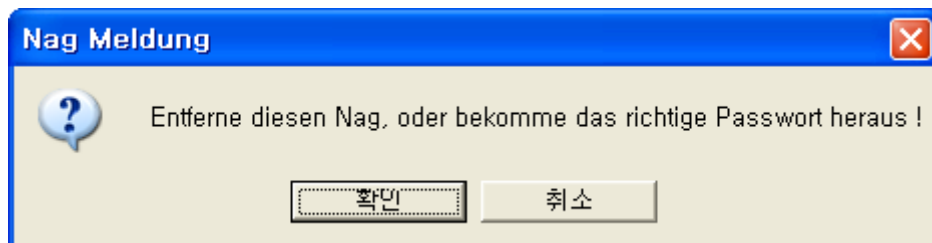


Basic 03 풀이

힌트 : 비주얼베이직에서 스트링 비교함수 이름은?

1. 프로그램 실행하여 기능 확인

무슨 말인지는 모르겠지만.. 패스워드를 맞추라는 내용 같다.



임의의 패스워드를 입력하면 아래와 같은 오류창이 나온다.



오류창 문자열을 통해 패스워드 확인 분기점을 찾을 수 있을 것 같다.

2. OllyDbg를 사용하여 코드 분석

OllyDbg의 [All referenced text strings] 기능을 통해 아래와 같이 오류창에서 사용된 문자열을 확인하였다.

```

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

```

해당 문자열로 이동후 앞뒤 코드를 확인해 보니 특정 유니코드 값을 확인하고 CMP 연산을 통해 비교하는 분기문을 확인 할 수 있었다.

00402A27	> FF75 A8	PUSH DWORD PTR SS:[EBP-58]	
00402A28	68 DC1D4000	PUSH 03.00401DDC	UNICODE "2G83G35Hs2"
00402A2F	E8 16E7FFFF	CALL <JMP.&MSUBUM50. __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.&MSUBUM50. __vbaFreeStr>	
00402A4A	8D4D A4	LEA ECX,DWORD PTR SS:[EBP-5C]	
00402A4D	E8 E0E6FFFF	CALL <JMP.&MSUBUM50. __vbaFreeObj>	
00402A52	66:83BD 48FF	CMP WORD PTR SS:[EBP-B8],0	
00402A5A	0F84 E7000000	JE 03.00402B47	
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],03.00401E70	UNICODE "Error ! Das Passwort ist falsch !"
00402A73	C785 74FFFFFF	MOV DWORD PTR SS:[EBP-8C],8	

CMP 비교값에 사용된 2G83G35Hs2 값이 패스워드 임을 확인하였다. 하지만 해당 문제는 비주얼베이직에서 사용하는 스트링 비교함수의 이름이다. 따라서 답은 vbaStrCmp가 이번 문제의 정답이다.

- End -