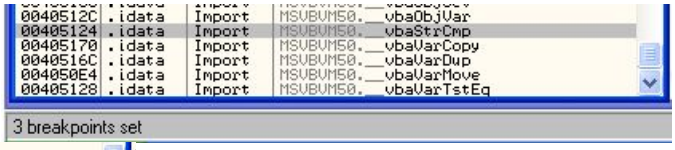
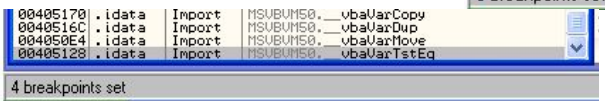
REPORT CODE ENGN level3

이번 문제는 간단하게 비주얼 베이직에서 스트링 비교함수를 묻는 문제였다.
우선 비주얼 베이직에서 사용되어지는 비교할 때 자주 사용되는 함수들을 모아봤다.

__vbaVarTstEq
__vbaVarTstNe
__vbaVarCmpEq
__vbaStrCmp
__vbaStrComp
__vbaStrCompVar

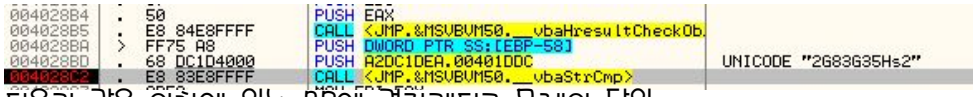
이렇게 6개가 자주사용되는 비교함수이다.





그리고 위에서 말한 함수 중 2가지가 사용되었고 모든 위치에 BP를 걸었다.

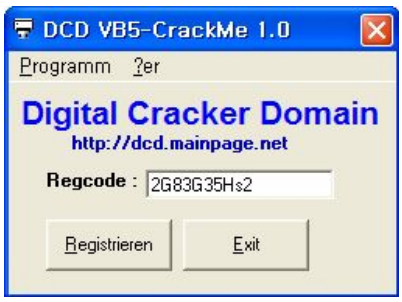
그리고 아무런 값을 입력후 Registerieren을 했을 때,



다음과 같은 위치에 있는 BP에 걸리게되고 문제의 답인,
사용된 문자열비교함수는 vbaStrCmp 인 것을 확인할수 있다.
그리고

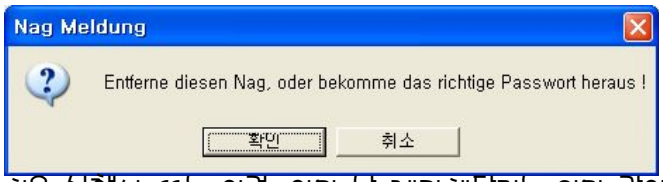
스택을 확인해보면 내가 입력한 qwe 와 2G83G35Hs2 와 비교되는 것을 볼수 있는데 저것이 Regcode인 것을 알수 있다.

아무런 조작하지 않고 그냥 BP를 제거하고 계속 실행시키면 다음과 같은 MessageBox를 확인할수 있다.
그리고 이것을 외에서 확인한 Regcode를 입력해봤다.

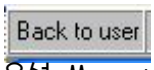


그럼 다른 MessageBox가 뜨며 인증이 성공된 것을 확인할 수 있다.
아마 Good Luck! Thank, this password mathed 이런 뜻인것같다.

그리고



처음 실행시 뜨는 이것, 아마 날 제거해달라는 의미 같아서 제거를 시도해봤다.



우선 MessageBox가 떴을 때, Back to user mode 상태로 변경후에,

```
00402CF4  .  E8 21E4FFFF     CALL <JMP.&MSVBVM50.__vbaI4Var>
00402CF9  .  50              PUSH EAX
00402CFA  .  8D45 AC         LEA EAX,DWORD PTR SS:[EBP-54]
00402CFD  .  50              PUSH EAX
00402CFE  .  E8 1DE4FFFF     CALL <JMP.&MSVBVM50.#595>
00402D03  .  8D95 5CFFFFFF   LEA EDX,DWORD PTR SS:[EBP-A4]
00402D09  .  8D4D BC         LEA ECX,DWORD PTR SS:[EBP-44]
00402D0C  .  8985 64FFFFFF   MOV DWORD PTR SS:[EBP-9C],EAX
```

확인후 진행했을때의 위치이다, 위의 call에서 메시지 박스를 부르는거같다.

그래서 제거를 했다.

```
00402CF9     B8 01000000     MOV EAX,1
00402CFE     90              NOP
00402CFF     90              NOP
00402D00     90              NOP
00402D01     90              NOP
00402D02     90              NOP
```

eax 에 1을 넣어주는 이유는 MB_OK에서 확인버튼을 눌러야지 계속진행되기 때문이다, 만약 취소를 누르게 되면 프로그램은 종료하기 때문이다.
call 명령만 제거해준 것이 아니라 위에서부터 제거해준이유는 __stdcall 형식이기 때문에 call부분만 지워버리게되면 스택이 정리되지않아 프로그램이 비정상 종료하기 때문이다.