codeengn-basic-L03 풀이

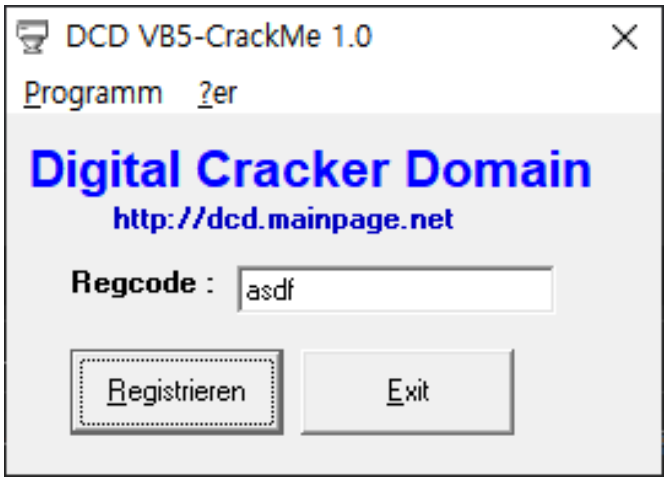
리버싱 문제풀이 / Wonlf / 2022. 3. 11. 10:21

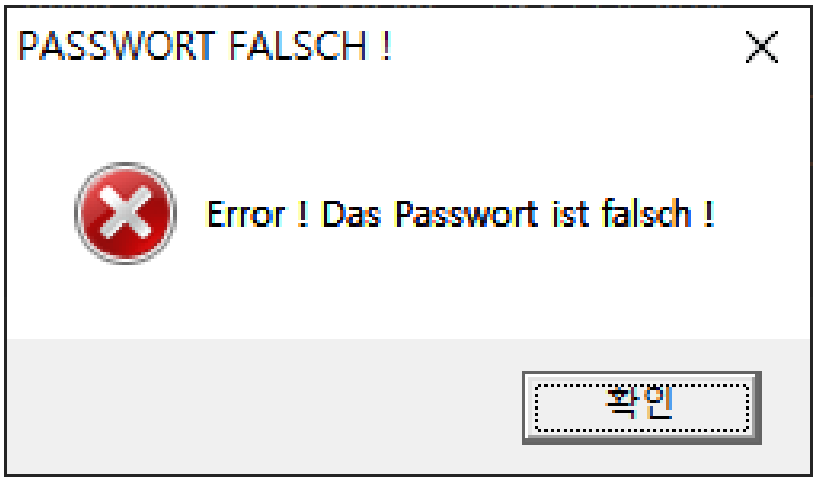
시작하기에 앞서 실행 했을 때 만약 "MSVBVM50.DLL"관련 오류가 뜬다면 단순히 DLL이 없어서 그러니 아래 링크에서 다운로드 받아서 32비트 64비트 맞는 경로에 넣어주시면 됩니다.

https://ko.dll-files.com/msvbvm50.dll.html

MSVBVM50.DLL은 Visual Basic 5.0으로 만든 응용 프로그램을 실행 하는데 필요한 파일이라고 하네요

실행시켜보면, 간단한 키젠 문제입니다.





틀린값 입력 했을 때 메시지 박스

까보면, Error메시지가 뜨는 곳으로 이동해보겠습니다.

```
00402A69  .  C785 7CFFFFFF 701E400( mov dword ptr ss:[ebp-84],03.401E70     401E70:L"Error ! Das Passwort ist falsch !"
00402A73  .  C785 74FFFFFF 0800000( mov dword ptr ss:[ebp-8C],8
00402A7D  .  E8 AAE6FFFF           call <JMP.&__vbaVarCopy>
00402A82  .  8D95 74FFFFFF         lea edx,dword ptr ss:[ebp-8C]
00402A88  .  8D4D DC               lea ecx,dword ptr ss:[ebp-24]
00402A8B  .  C785 7CFFFFFF 1000000( mov dword ptr ss:[ebp-84],10
00402A95  .  899D 74FFFFFF         mov dword ptr ss:[ebp-8C],ebx
00402A9B  .  E8 86E6FFFF           call <JMP.&__vbaVarMove>
00402AA0  .  8D95 74FFFFFF         lea edx,dword ptr ss:[ebp-8C]
00402AA6  .  8D4D CC               lea ecx,dword ptr ss:[ebp-34]
00402AA9  .  C785 7CFFFFFF B81E40( mov dword ptr ss:[ebp-84],03.401EB8     401EB8:L"PASSWORT FALSCH !"
```

CTRL + A를 눌러서 함수 전체로 볼 수 있게 만들어주고 함수를 뒤적거리다 보면,

```
004028BA  >  FF75 A8               push dword ptr ss:[ebp-58]
004028BD  .  68 DC1D4000           push 03.401DDC                           401DDC:L"2G83G35Hs2"
004028C2  .  E8 83E8FFFF           call <JMP.&__vbaStrCmp>
004028C7  .  8BF8                  mov edi,eax
004028C9  .  8D4D A8               lea ecx,dword ptr ss:[ebp-58]
004028CC  .  F7DF                  neg edi
004028CE  .  1BFF                  sbb edi,edi
004028D0  .  47                    inc edi
004028D1  .  F7DF                  neg edi
004028D3  .  E8 60E8FFFF           call <JMP.&__vbaFreeStr>
004028D8  .  8D4D A4               lea ecx,dword ptr ss:[ebp-5C]
004028DB  .  E8 52E8FFFF           call <JMP.&__vbaFreeObj>
004028E0  .  66:3BFE               cmp di,si
004028E3  .v 0F84 F3000000         je 03.4029DC
004028E9  .  6A 08                 push 8
004028EB  .  8D95 74FFFFFF         lea edx,dword ptr ss:[ebp-8C]
004028F1  .  5E                    pop esi
004028F2  .  8D4D AC               lea ecx,dword ptr ss:[ebp-54]
004028F5  .  C785 7CFFFFFF 081E40( mov dword ptr ss:[ebp-84],03.401E08     401E08:L"Danke, das Passwort ist richtig !"
```

KEY인 부분 같은게 나옵니다 CMP는 Compare의 약자이니 저게 비교함수로 추정 되네요.

어셈블리 해석을 조금 하자면

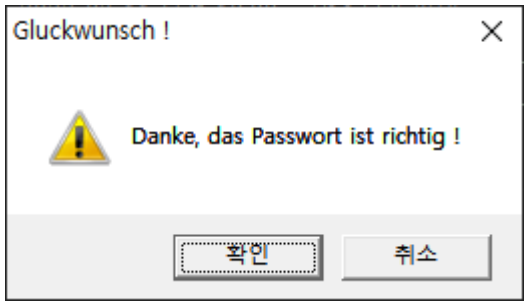
1. ebp-58 주소에 있는 값을 스택에 넣습니다.

2. 401DDC 주소에 있는 값을 스택에 넣습니다.

3. 함수 바로 위에 구문에서 값을 스택에 넣는다는건 함수의 인자값으로 사용하겠다는 겁니다.

4. 함수 호출

401DDC 주소에 있는 값을 넣어주니 다른 메시지박스가 뜨네요



문제는 함수의 이름만 원했으니 "vbaStrCmp"입력해줍시다.