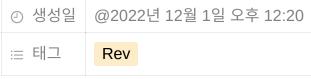
[Code_Engn] Basic RCE L03



Basic RCE L03 비주얼베이직에서 스트링 비교함수 이름은? — Author: Blaster99 [DCD] — File Password: codeengn

실행화면



문자열 비교함수 이름을 찾기 위해서 xdbg를 사용하여 디버깅을 해보았습니다.

문자열 참조로 모든 문자열을 보았을때 Error ! Das Passwort ist falsch !" 라는 부분위 쪽에 스트링 비교함수가 있을꺼 같아서 위치로 가보았습니다.

```
push eax
   call <JMP.&__vbaHresultCheckObj>
push dword ptr ss:[ebp-58]
   push 03.401DDC
                                                                          401DDC:L"2G83G35Hs2"
   call <JMP.&__vbaStrCmp>
   neg eax
   sbb eax,eax
   lea ecx,dword ptr ss:[ebp-58]
                                                                         ecx:EntryPoint
   neg eax
   neg eax
   mov dword ptr ss:[ebp-B8],eax
call <JMP.&_vbaFreeStr>
lea ecx,dword ptr ss:[ebp-50]
                                                                         ecx:EntryPoint
   call <JMP.&__vbaFreeObj>
cmp word ptr ss:[ebp-B8],0
    ie 03.402B47
lea edx,dword ptr ss:[ebp-8C]
lea ecx,dword ptr ss:[ebp-54]
mov dword ptr ss:[ebp-8C],8
                                                                         edx:EntryPoint
                                                                         ecx:EntryPoint
401E70:L"Error ! Das Passwort ist falsch !"
call <JMP.&_vbaVarCopy>
lea edx,dword ptr ss:[ebp-8C]
lea ecx,dword ptr ss:[ebp-24]
mov dword ptr ss:[ebp-84],10
mov dword ptr ss:[ebp-8C],ebx
                                                                         edx:EntryPoint
                                                                         ecx:EntryPoint
call <JMP. & vbaVarMove>
lea edx,dword ptr ss: [ebp-8C]
lea ecx,dword ptr ss: [ebp-84],03.401EB8
mov dword ptr ss: [ebp-84],8
                                                                         edx:EntryPoint
                                                                         ecx:EntryPoint
401EB8:L"PASSWORT FALSCH !"
   call <JMP.&__vbaVarCopy>
```

위치로 이동했을때 위에는 비밀번호처럼 보이는 문자열이 있고 그 아래에 vbaStrCmp라는 함수가 호출됩니다. StrCmp가 있는걸로 보아 이것이 비주얼베이직에서 스트링 비교함수 이름이라고 생각했습니다.