

# [Code\_Engn] Basic RCE L03

🕒 생성일	@2022년 12월 1일 오후 12:20
☰ 태그	Rev

## Basic RCE L03

비주얼베이직에서 스트링 비교함수 이름은?

— Author: Blaster99 [DCD]  
— File Password: codeengn



## 실행화면



문자열 비교함수 이름을 찾기 위해서 xdbg를 사용하여 디버깅을 해보았습니다.

주소	디스어셈블리	String Address	문자열
00401061	and eax,<03.&_vbaChkstk>	0040511C	&"GWP="
004012C0	sbb eax,50040	00050040	L"ms-win-core-pkeyhelper-11-1-0"
004018B0	push 03.401DDC	00401DDC	L"2G83G35Hs2"
004018F5	mov dword ptr ss:[ebp-84],03.401E08	00401E08	L"Danke, das Passwort ist richtig !"
00401A5A	push 03.401DDC	00401DDC	L"2G83G35Hs2"
00401A69	mov dword ptr ss:[ebp-84],03.401E70	00401E70	L"Error ! Das Passwort ist falsch !"
00401A69	mov dword ptr ss:[ebp-84],03.401E88	00401E88	L"PASSWORT FALSCH !"
00401C85	mov dword ptr ss:[ebp-7C],03.401EF0	00401EF0	L"Entferne diesen Nag, oder bekomme das richtige Passwort heraus !"
00401C8E	mov dword ptr ss:[ebp-7C],03.401F78	00401F78	L"Nag Meldung"
00401E28	mov dword ptr ss:[ebp-5C],03.401F94	00401F94	L"VBS-crackme 1.0 by elasters99 [DCO]"
00401F9A	push 03.401FEC	00401FEC	L"visible"
00403060	push 03.401FEC	00401FEC	L"visible"
740C1C00	push msvbvm50.740C1DE4	740C1DE4	L"kernel32.dll"
740C1CEC	push msvbvm50.740C1DDC	740C1DDC	L"IsTNT"
740C1D40	mov dword ptr ds:[741D3B68],eax	741D3B68	&"C:\Users\usung\Documents\코드엔진\Basic RCE L03\03.exe\""
740C1D57	cmp dword ptr ds:[741D3B68],0	741D3B68	&"C:\Users\usung\Documents\코드엔진\Basic RCE L03\03.exe\""
740C31F5	push msvbvm50.741CFD04	741CFD04	L"\r\n"
740C40D5	mov dword ptr ds:[ebx+4],50000	00050000	L"nsmanger-11-1-0"
740C50C4	mov ecx,msvbvm50.741D0860	741D0860	L"자"
740C5126	mov esi,msvbvm50.741D2860	741D2860	&"C:\Users\usung\Documents\코드엔진\Basic RCE L03\03.exe"
740C5134	mov eax,dword ptr ds:[741D3B68]	741D3B68	&"C:\Users\usung\Documents\코드엔진\Basic RCE L03\03.exe\""
740C5139	mov dword ptr ds:[741D08AC],esi	741D08AC	&"C:\Users\usung\Documents\코드엔진\Basic RCE L03\03.exe\""
740C5144	mov esi,dword ptr ds:[741D3B68]	741D3B68	&"C:\Users\usung\Documents\코드엔진\Basic RCE L03\03.exe\""
740C5491	push msvbvm50.740C552C	740C552C	L"kernel32"
740C54A6	push msvbvm50.740C5514	740C5514	L"GetProcAddressMask"
740C54C0	push msvbvm50.740C5500	740C5500	L"GetCurrentProcess"

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	
mov dword ptr ss:[ebp-B8],eax	
call <JMP.&_vbaFreeStr>	
lea ecx,dword ptr ss:[ebp-5C]	ecx:EntryPoint
call <JMP.&_vbaFreeObj>	
cmp word ptr ss:[ebp-B8],0	
je 03.402847	
lea edx,dword ptr ss:[ebp-8C]	edx:EntryPoint
lea ecx,dword ptr ss:[ebp-54]	ecx:EntryPoint
mov dword ptr ss:[ebp-84],03.401E70	401E70:L"Error ! Das Passwort ist falsch !"
mov dword ptr ss:[ebp-8C],8	
call <JMP.&_vbaVarCopy>	
lea edx,dword ptr ss:[ebp-8C]	edx:EntryPoint
lea ecx,dword ptr ss:[ebp-24]	ecx:EntryPoint
mov dword ptr ss:[ebp-84],10	
mov dword ptr ss:[ebp-8C],ebx	
call <JMP.&_vbaVarMove>	
lea edx,dword ptr ss:[ebp-8C]	edx:EntryPoint
lea ecx,dword ptr ss:[ebp-34]	ecx:EntryPoint
mov dword ptr ss:[ebp-84],03.401E88	401E88:L"PASSWORT FALSCH !"
mov dword ptr ss:[ebp-8C],8	
call <JMP.&_vbaVarCopy>	

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