

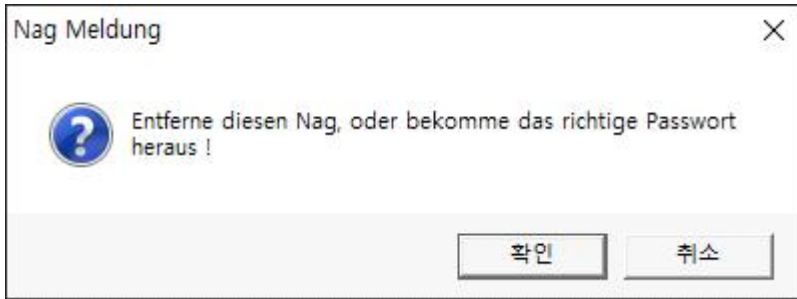
REPORT:

코드엔진 Basic

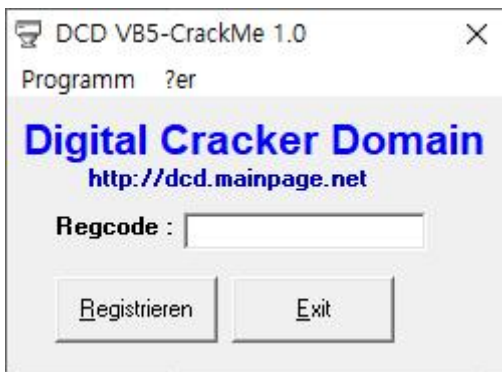
RCE 03 Writeup

COLONY
1824275 정상지

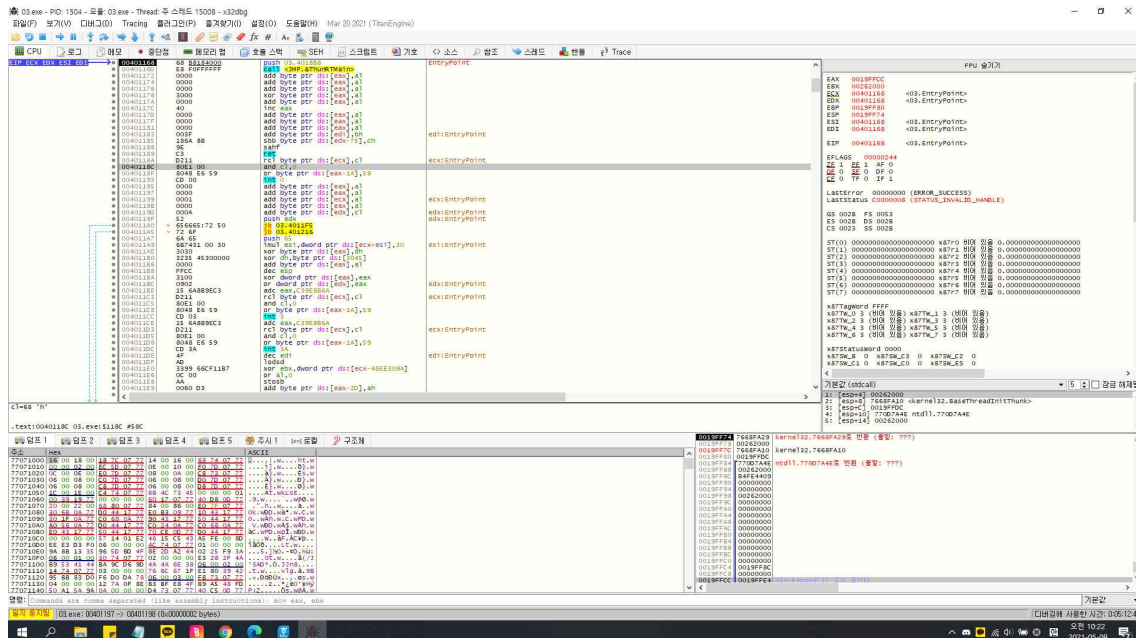
2021.05.09



03문제의 프로그램 실행 시 출력되는 메시지 박스
해당 화면에서 [확인]을 누르면



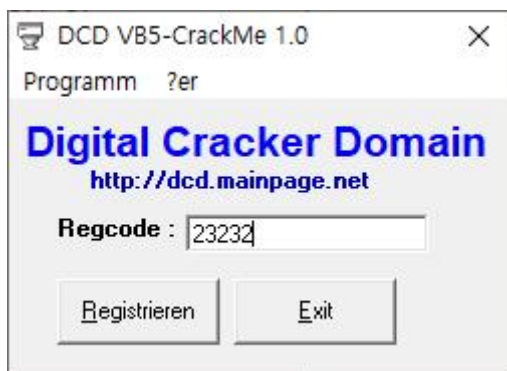
이와 같은 창이 출력된다



x32dbg를 이용하여 프로그램을 열고 문자열 참조를 통해 처음 봤던 메시지 박스의 문자열이 있는 곳으로 이동한다

<pre> 004028A9 68 00000000 004028AE 57 004028B3 50 004028B4 E8 84E8FFFF 004028B5 F775 A8 004028BA 68 0C1D4000 004028BD E8 83E8FFFF 004028C7 8BF8 004028C9 804D A8 004028CC F7DF 004028CE 1BFF 004028D0 47 004028D1 F7DF 004028D3 E8 60E8FFFF 004028D8 804D A4 004028DB E8 52E8FFFF 004028E0 6613BF 004028E3 0F84 F3000000 004028E9 6A 08 004028EB 8095 74FFFFFF 004028F1 5E 004028F2 804D AC 004028F5 C785 7CFFFFFF 004028FF 8985 74FFFFFF 00402905 E8 22E8FFFF 0040290A 6A 03 0040290C 8095 74FFFFFF 00402912 5B </pre>	<pre> push .40 push 03.401DF4 push edi push eax call <JMP.<_vbaHresultCheckObj> push dword ptr ss:[ebp-58] push 03.401DDC call <JMP.<_vbaStrCmp> mov edi,eax lea ecx,dword ptr ss:[ebp-58] neg edi sbb edi,edi inc edi neg edi call <JMP.<_vbaFreeStr> lea ecx,dword ptr ss:[ebp-5C] call <JMP.<_vbaFreeObj> cmp di,s1 je 03.40290C push 3 lea edx,dword ptr ss:[ebp-8C] pop esi lea ecx,dword ptr ss:[ebp-54] mov dword ptr ss:[ebp-84],03.401E08 mov dword ptr ss:[ebp-8C],esi call <JMP.<_vbaVarCopy> push 3 lea edx,dword ptr ss:[ebp-8C] pop ebx </pre>	<pre> edi:"LdrpInitializeProcess" 401DDC:L"2G89G35H62" edi:"LdrpInitializeProcess" edi:"LdrpInitializeProcess" edi:"LdrpInitializeProcess" edi:"LdrpInitializeProcess" esi:"minkernel\\ntdll\\ldrinit.c" [ebp-84]:"T9v", 401E08:L"Danke, das Passwort ist richtig !" </pre>
--	---	---

<vbaStrCmp>에서 해당 프로그램의 입력값을 비교하는 연산을 수행하는 지 알아보기 위해 중단 점을 설정한다



무작위 문자(숫자)를 입력하고 해당 프로그램의 동작을 확인한다
[Registrieren]을 누르면 eax 레지스터의 값이 FFFFFFFF로 리턴된다

```

EAX  FFFFFFFF
EBX  0077E598
ECX  00000003
EDX  02600000
EBP  0019F2A4
ESP  0019F1D4
ESI  00000000
EDI  0260A93C

EIP  004028C7  03.004028C7

EFLAGS  00000284
ZF 0 PF 1 AF 0
OF 0 SF 1 DF 0
CF 0 TF 0 IF 1

```

이후 분기문 전 까지의 구문을 실행하게 되면 eax의 값을 edi에 복사하고 해당 값을 증감시키다가 esi와 비교하여 분기문을 실행시킨다

```

EAX 00000000
EBX 0048E598
ECX 0019F248
EDX 00000020
EBP 0019F2A4
ESP 0019F1D4
ESI 00000000
EDI 00000000

EIP 004028E0 03.004028E0

EFLAGS 00000200
ZF 0 PF 0 AF 0
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1

```

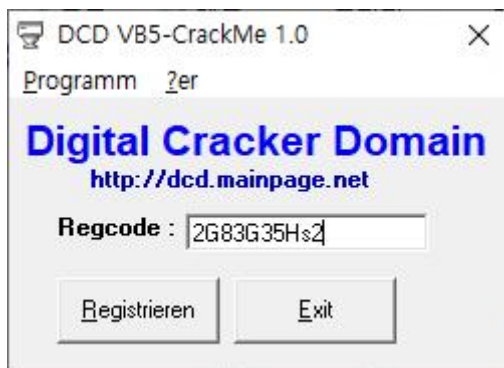
분기문 실행 바로 전의 모습

```

004028A9 68 00000000 push 0
004028AC 68 F4D40000 push 03.40D4F4
004028B3 57          push edi
004028B4 50          push eax
004028B5 E8 84E8FFFF call <JMP.<vbaHresultCheckObj>
004028B8 FF75 A8     push dword ptr esi:[ebp-58]
004028BD 68 DC4D4000 push 03.40D4DC
004028C2 E8 83E8FFFF call <JMP.<vbaStrCmp>
004028C7 8BF8       mov edi,eax
004028C8 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 50E8FFFF call <JMP.<vbaFreeStr>
004028D8 8D4D A4     lea ecx,dword ptr ss:[ebp-5C]
004028DB E8 52E8FFFF call <JMP.<vbaFreeObj>
004028E0 6613BF     cmp di,s1
004028E3 0F84 F3000000 je 03.40290C
004028E9 6A 08      push 8
004028EB 8D95 74FFFFF lea edx,dword ptr ss:[ebp-8C]
004028F1 5E         pop esi
004028F2 8D4D AC     lea ecx,dword ptr ss:[ebp-54]
004028F5 C785 7CFFFFFF mov dword ptr ss:[ebp-84],03.401E08
004028FF 8B85 74FFFFF mov dword ptr esi:[ebp-8C],esi
00402905 E8 22E8FFFF call <JMP.<vbaVarCopy>
0040290A 6A 03      push 3
0040290C 8D95 74FFFFF lea edx,dword ptr ss:[ebp-8C]
00402912 5B         pop ebx
00402912 5B         pop ebx
edi:"LdrpInitializeProcess"
401DDC:L"2G83G35Hs2"
edi:"LdrpInitializeProcess"
edi:"LdrpInitializeProcess"
edi:"LdrpInitializeProcess"
edi:"LdrpInitializeProcess"
esi:"minkernel\\ntdll\\ldrinit.c"
[ebp-84]:"T9v", 401E08:L"Danke, das Passwort ist richtig !"

```

<vbaStrCmp>호출 전에 주석에서 보이다시피 2G83G35Hs2라는 문자열이 있다



이번에는 무작위가 아닌 해당 문자열을 입력한다

```

EAX 00000000
EBX 0068E598
ECX 00000000
EDX 023F0000 "8征5]?"
EBP 0019F2A4
ESP 0019F1D4
ESI 00000000
EDI 023FA93C

EIP 004028C7 03.004028C7

EFLAGS 00000244
ZF 1 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1

```

해당 함수 호출 리턴 시 이번엔 eax의 값이 00000000으로 리턴되었다

EAX	00000000	
EBX	0068E598	
ECX	0019F248	
EDX	00000020	
EBP	0019F2A4	
ESP	0019F1D4	
ESI	00000000	
EDI	FFFFFFFF	
EIP	004028E0	03.004028E0
EFLAGS	00000200	
ZF	0	PF 0 AF 0
OF	0	SF 0 DF 0
CF	0	TF 0 IF 1

esi와 edi를 비교하는 분기문 바로 전의 모습으로 이번엔 esi와 edi의 값이 서로 달라서 ZF가 0의 값이 입력되었다

004028D8	80 4D A4	lea ecx, dword ptr ss:[ebp-5C]	
004028DB	E8 52E8FFFF	call <JMP.&_vbaFreeObj>	
004028DE	66 3BFE	cmp di, si	
004028E0	0F84 F3000000	jle 03.40290C	
004028E3	6A 08	push 8	
004028E6	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 !"
004028FF	89B5 74FFFFFF	mov dword ptr ss:[ebp-8C], esi	

해당 분기문 밑의 “Danke, das Passwort ist richtig!”이라는 메시지를 받고 이후 해당 메시지를 출력한다

비주얼베이직에서 String 비교함수는 <vbaStrCmp>이고 해당 프로그램의 Password는 2G83G35Hs2이다