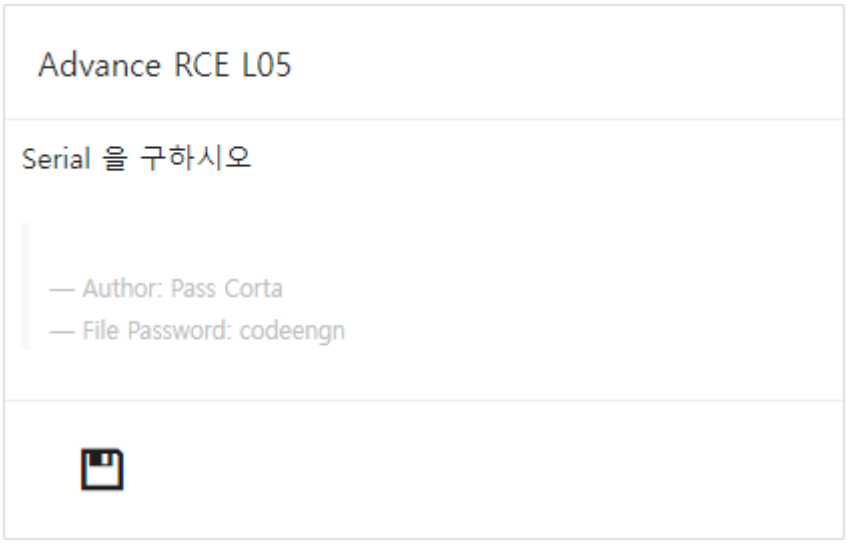
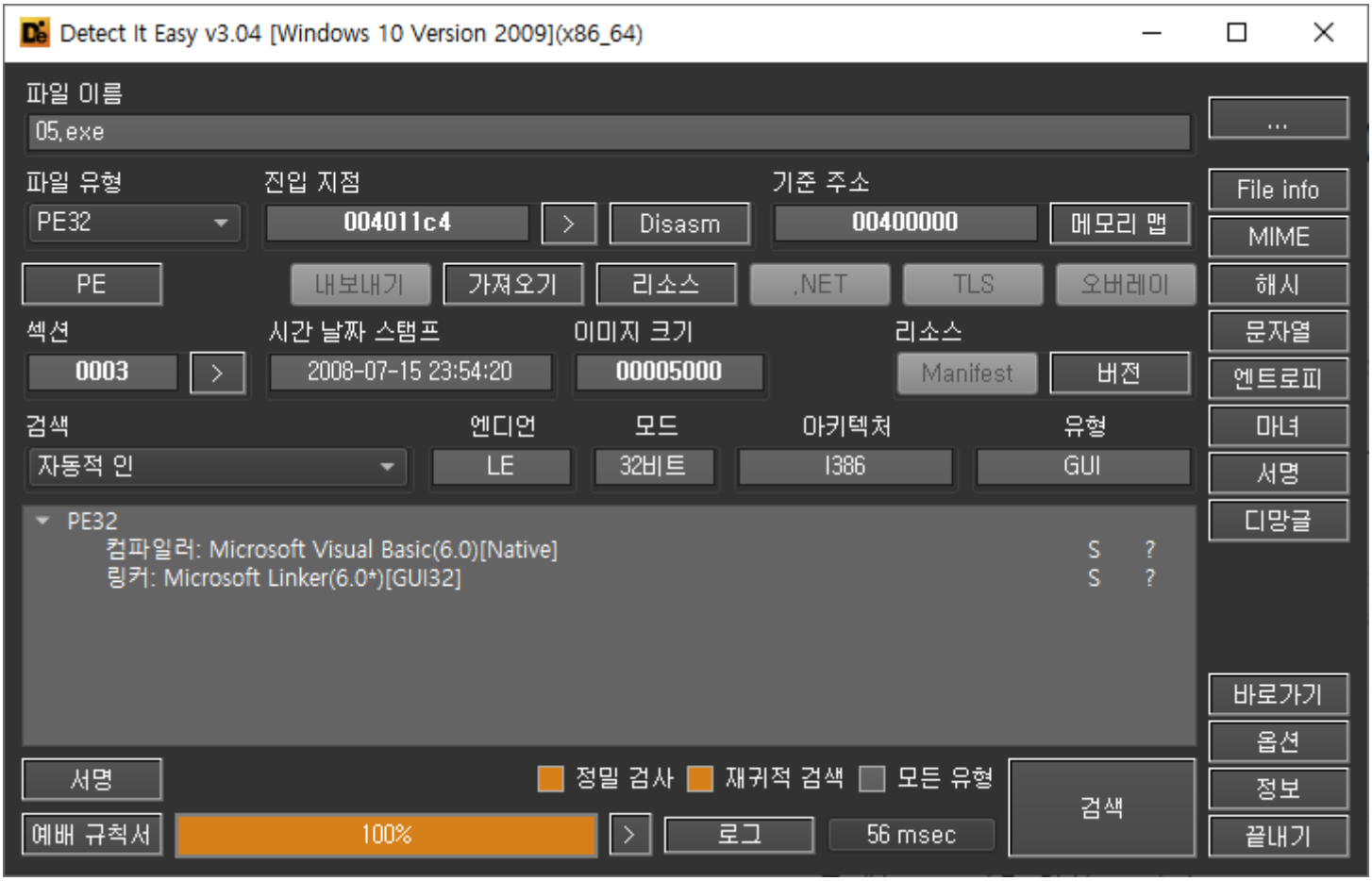
codeengn-advance-L05 풀이

리버싱 문제풀이 / Wonlf / 2022. 5. 6. 16:32



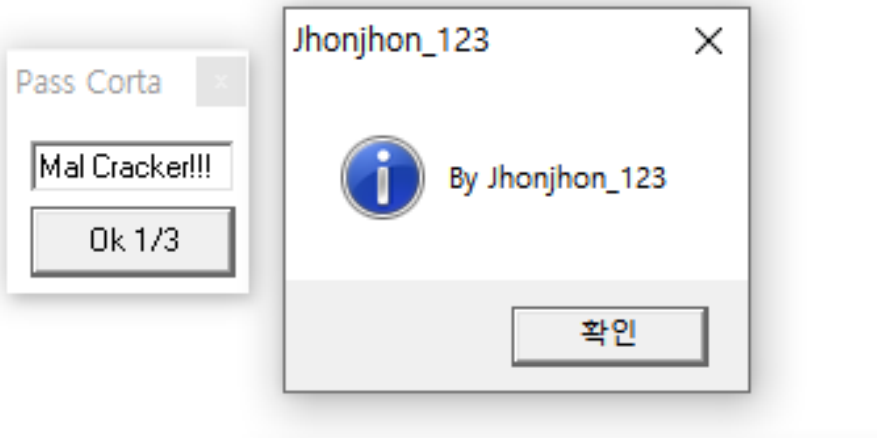
문제는 Serial을 원하고 있다.

Die에 넣어본다.



Visual Basic으로 구현되어 있다.

프로그램을 실행시켜본다.



빈 input에 아무 값을 입력하고 나니, Mal Cracker!!라는 문구로 대체되고 메시지 박스가 뜬다.

문제에서 말하는 이 input을 원하는 것 같다.

디버거로 열어본다.

주소	디스어셈블리	문자열
004010C1	and eax,<05.&__vbaChkstk>	&"QWP="
004024F6	mov dword ptr ss:[ebp-10C],05.401F80	L"Jhonjhon_123"
00402514	mov dword ptr ss:[ebp-FC],05.401F60	L"¡¡¡Bien!!!"
0040259F	mov dword ptr ss:[ebp-10C],05.401F80	L"Jhonjhon_123"
004025BD	mov dword ptr ss:[ebp-FC],05.401FA0	L"By Jhonjhon_123"
0040269B	mov ebx,dword ptr ds:[<&__vbaFreeObj>]	"#沐`"
004026C2	push 05.401FCC	L"Mal Cracker!!!"
00402729	mov dword ptr ss:[ebp-10C],05.401F80	L"Jhonjhon_123"
00402747	mov dword ptr ss:[ebp-FC],05.401FA0	L"By Jhonjhon_123"

문자열 찾기로 실패와 성공에 해당하는 주소를 찾았다.

성공 문자열을 사용하는 곳으로 가본다.

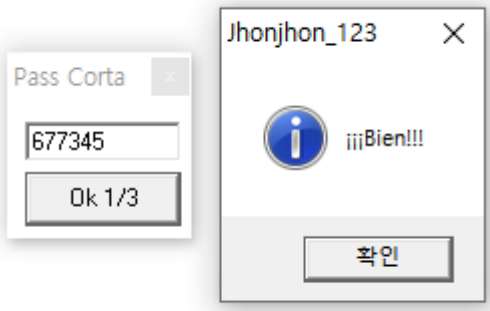
```
00402476   FF15 44104000          call dword ptr ds:[<&__vbaStrCmp>]
0040247C   8BD8                   mov ebx,eax
0040247E   8D95 68FFFFFF          lea edx,dword ptr ss:[ebp-98]          edx:EntryPoint
00402484   F7DB                   neg ebx
00402486   1BDB                   sbb ebx,ebx
00402488   8D85 64FFFFFF          lea eax,dword ptr ss:[ebp-9C]
0040248E   52                     push edx                               edx:EntryPoint
0040248F   43                     inc ebx
00402490   50                     push eax
00402491   6A 02                  push 2
00402493   F7DB                   neg ebx
00402495   FF15 7C104000          call dword ptr ds:[<&__vbaFreeStrList>]
0040249B   8D8D 5CFFFFFF          lea ecx,dword ptr ss:[ebp-A4]          ecx:EntryPoint
004024A1   8D95 60FFFFFF          lea edx,dword ptr ss:[ebp-A0]          edx:EntryPoint
004024A7   51                     push ecx                               ecx:EntryPoint
004024A8   52                     push edx                               edx:EntryPoint
004024A9   6A 02                  push 2
004024AB   FF15 18104000          call dword ptr ds:[<&__vbaFreeObjList>]
004024B1   83C4 18                add esp,18
004024B4   66:3BDF                cmp bx,di
004024B7   0F84 57010000          je 05.402614
004024BD   8B35 8C104000          mov esi,dword ptr ds:[<&__vbaVarDup>]  esi:EntryPoint
004024C3   B9 0A000000            mov ecx,A                              ecx:EntryPoint, A:'\n'
004024C8   B8 04000280            mov eax,80020004
004024CD   898D 1CFFFFFF          mov dword ptr ss:[ebp-E4],ecx          ecx:EntryPoint
004024D3   898D 2CFFFFFF          mov dword ptr ss:[ebp-D4],ecx          ecx:EntryPoint
004024D9   BB 08000000            mov ebx,8
004024DE   8D95 ECFEFFFF          lea edx,dword ptr ss:[ebp-114]         edx:EntryPoint
004024E4   8D8D 3CFFFFFF          lea ecx,dword ptr ss:[ebp-C4]          ecx:EntryPoint
004024EA   8985 24FFFFFF          mov dword ptr ss:[ebp-DC],eax
004024F0   8985 34FFFFFF          mov dword ptr ss:[ebp-CC],eax
004024F6   C785 F4FEFFFF 801F400( mov dword ptr ss:[ebp-10C],05.401F80   401F80:L"Jhonjhon_123"
00402500   899D ECFEFFFF          mov dword ptr ss:[ebp-114],ebx
00402506   FFD6                   call esi                               esi:EntryPoint
00402508   8D95 FCFEFFFF          lea edx,dword ptr ss:[ebp-104]         edx:EntryPoint
0040250E   8D8D 4CFFFFFF          lea ecx,dword ptr ss:[ebp-B4]          ecx:EntryPoint
00402514   C785 04FFFFFF 601F400( mov dword ptr ss:[ebp-FC],05.401F60   401F60:L"¡¡¡Bien!!!"
```

위로 올려보니 문자열을 비교하는 함수를 찾았다. 함수에 브레이크 포인트를 걸고 키를 입력해본다.

```
00402474   50                     push eax                               eax:L"12345"
00402475   51                     push ecx                               ecx:L"677345"
00402476   FF15 44104000          call dword ptr ds:[<&__vbaStrCmp>]
```

함수의 인자값으로 내가 입력한 12345와 특정 값을 비교하는 것을 볼 수 있다.

이것을 실제 프로그램에 넣어본다.



실제 프로그램에서 인증을 성공 하였다. 그대로 페이지에 인증 해주면 된다.

성공!