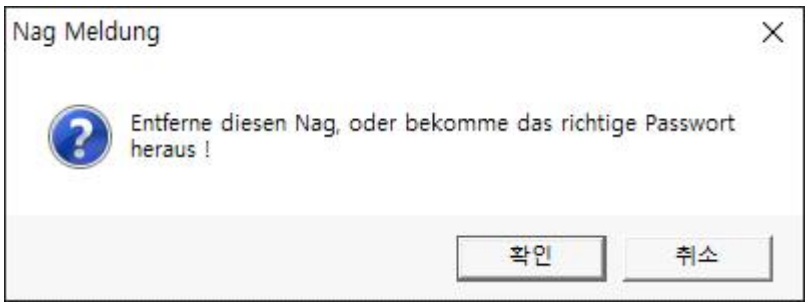
REPORT:

코드엔진 Basic

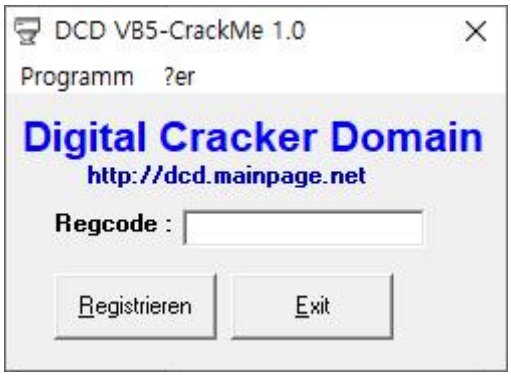
RCE 03 Writeup

COLONY
1824275 정상지

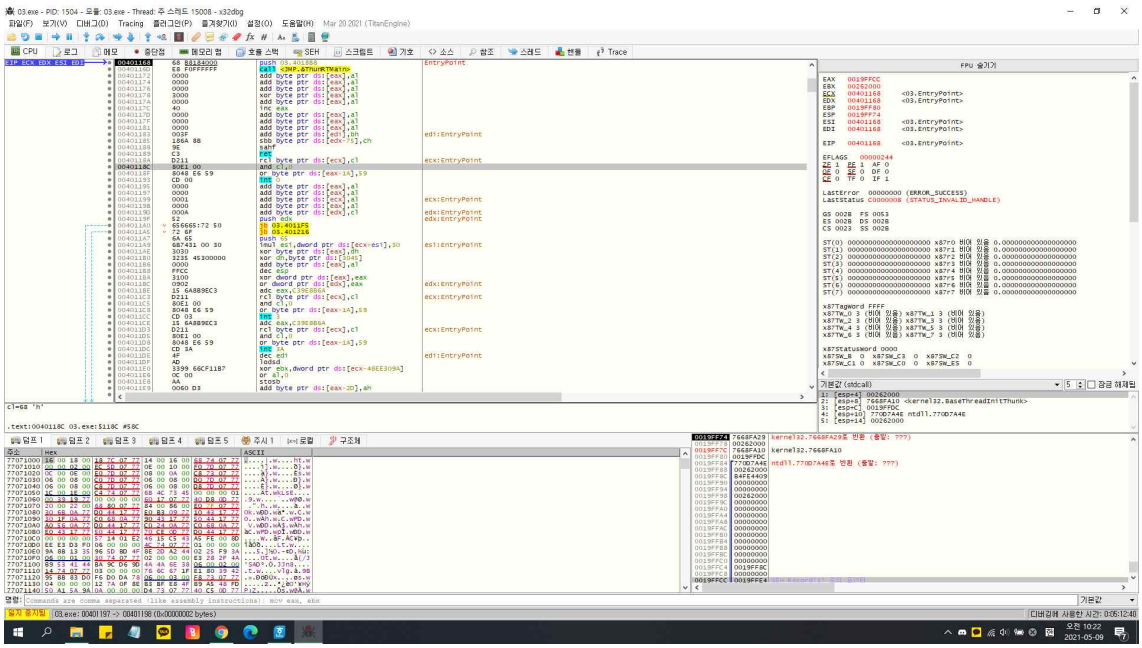
2021.05.09



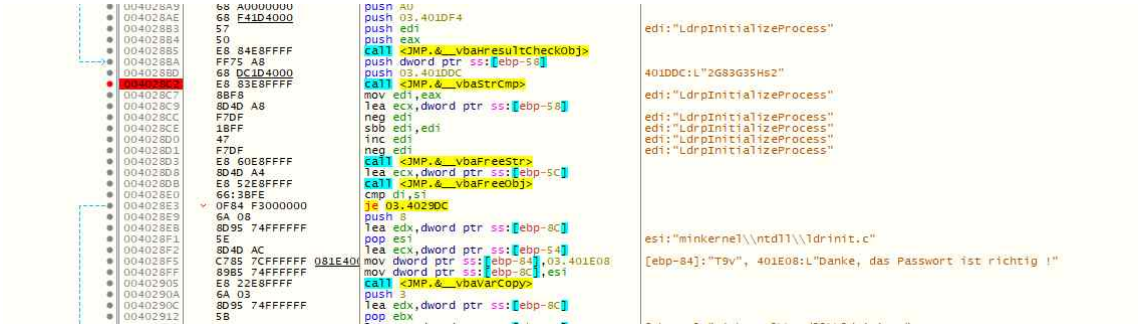
03문제의 프로그램 실행 시 출력되는 메시지 박스
해당 화면에서 [확인]을 누르면



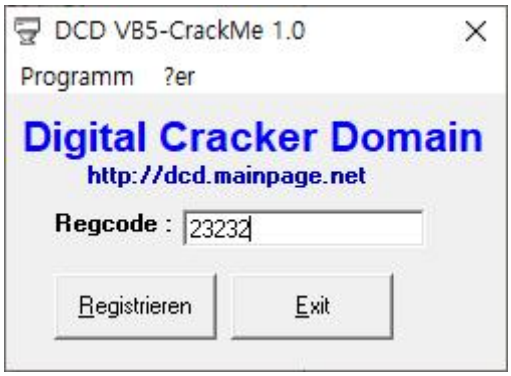
이와 같은 창이 출력된다



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



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



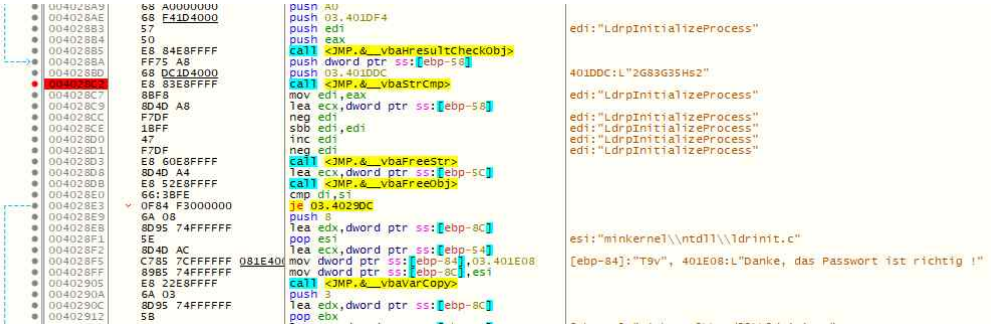
무작위 문자(숫자)를 입력하고 해당 프로그램의 동작을 확인한다
[Registrieren]을 누르면 eax 레지스터의 값이 FFFFFFFF로 리턴된다

```
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
```

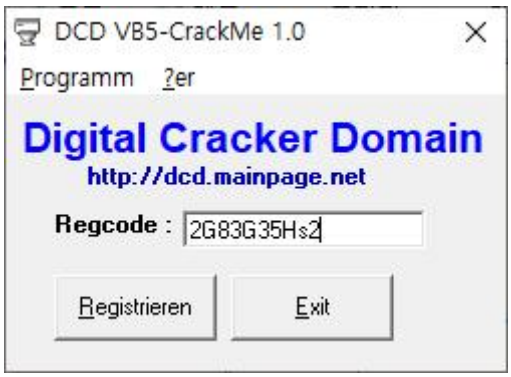
이후 분기문 전 까지의 구문을 실행하게 되면 eax의 값을 edi에 복사하고 해당 값을 증감시키다가 esi와 비교하여 분기문을 실행시킨다

```
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



<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

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

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