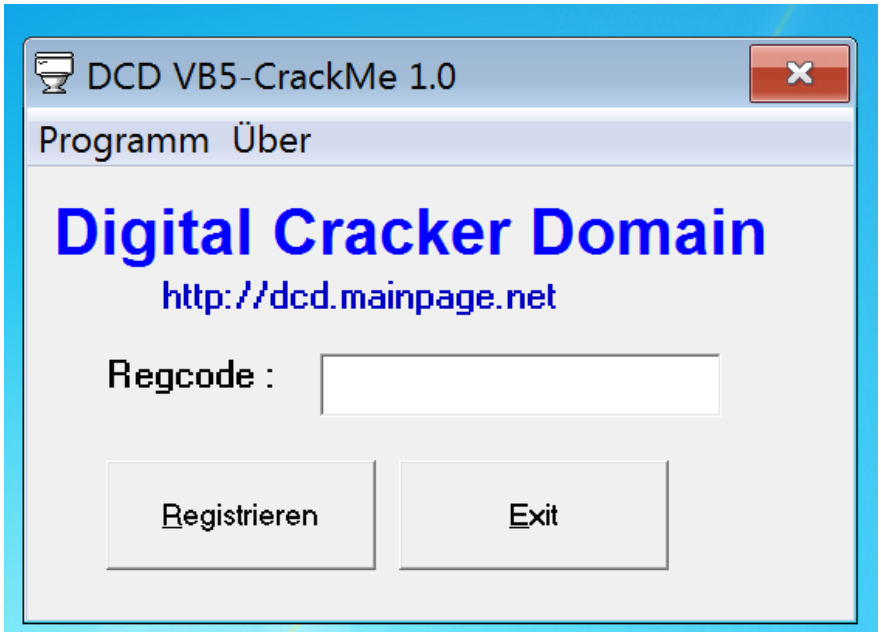
CodeEngn Basic RCE L03 Writeup

Daniel Smith
Feb 18 · 2 min read

Let's start RCE

```
Filename: 03.exe
Description: 비주얼베이직에서 스트링 비교함수 이름은?
Author: Blaster99 [DCD]
```

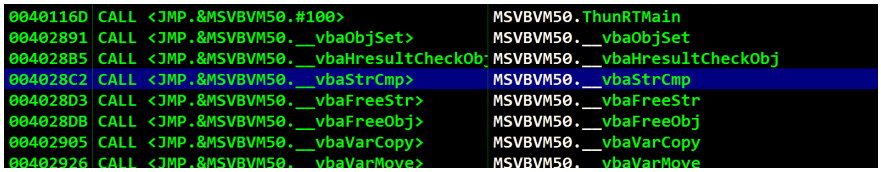
프로그램을 실행 시켜보자



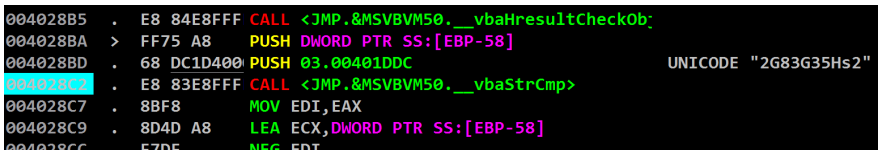
실행 시

아무래도 패스워드 크랙 문제인 것 같다

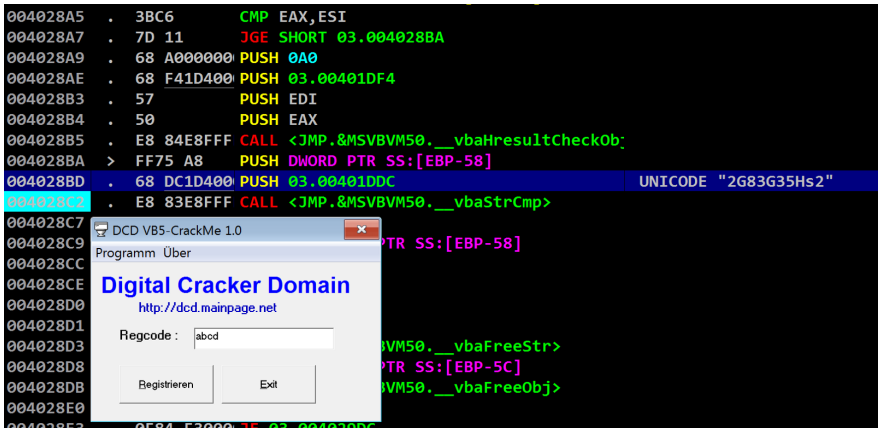
Description 에서 string 비교 함수의 이름을 찾으라는 힌트를 주었으므로 All intermodular calls 로 현재 코드 영역에서 호출하려는 API 들을 살펴보자



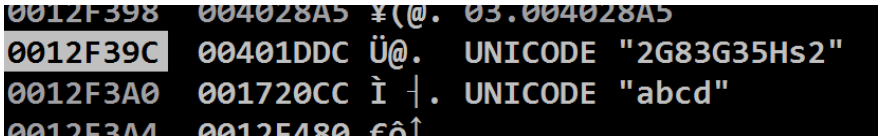
vb 는 잘 모르지만 살펴보다 보면 친숙한 이름을 가진 vbaStrCmp 함수가 있다



들어가보면 이런 코드들이 보이는데 아마 오른쪽에 있는것이 패스워드인듯 하다



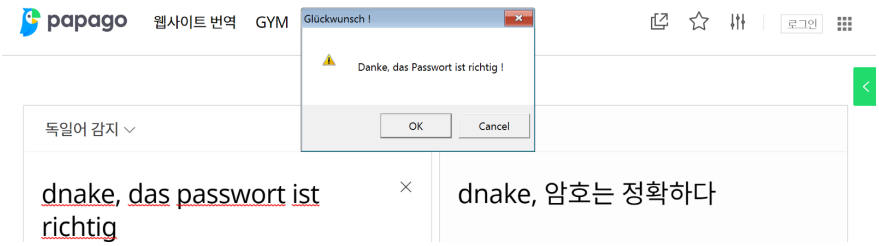
vbaStrCmp 에 BP 를 건뒤 “abcd” 문자열을 입력하여 stack을 살펴보자



실행 후의 stack 모습

두 문자열을 비교하는 것 같다

2G83G35Hs2를 입력하면 성공


papago
웹사이트 번역
GYM
Glückwunsch !
Danke, das Passwort ist richtig !
OK
Cancel
로그인
독일어 감지
dnake, das passwort ist richtig
dnake, 암호는 정확하다