

# Codeengn Challenges Advance RCE LEVEL5 풀이

## Reverse2 L05 Start

Author : Pass Corta

**Korea :**  
Serial 을 구하시오

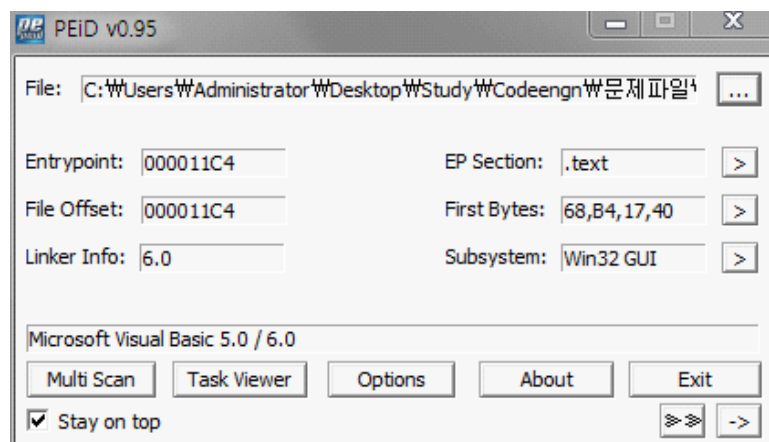
**English :**  
Find the Serial

[Down](#)

프로그램을 실행시켜 확인해보니, OK를 누르면 Mal Cracker!!라는 글자가 뜨면서 제작자의 닉네임이 메시지창에 뜬다.



PEID로 프로그램을 확인해보니



비주얼 베이직으로 만들어진 프로그램임을 확인 할 수 있다.

OLLY로 프로그램 분석을 시작해보았다.

먼저 올리에서 틀렸을때 나오는 문자열을 우클릭 -> Search for -> All reference text strings 기능을 이용해 찾았다.

```

004024F6 MOV DWORD PTR SS:[EBP-10C],Reverse2,00401FCC UNICODE "Jhonjhon_123"
0040259F MOV DWORD PTR SS:[EBP-10C],Reverse2,00401FCC UNICODE "Jhonjhon_123"
004025BD MOV DWORD PTR SS:[EBP-FC],Reverse2,00401FCC UNICODE "By Jhonjhon_123"
004026C2 PUSH Reverse2,00401FCC UNICODE "Mal Cracker!!!"
00402729 MOV DWORD PTR SS:[EBP-10C],Reverse2,00401FCC UNICODE "Jhonjhon_123"
00402747 MOV DWORD PTR SS:[EBP-FC],Reverse2,00401FCC UNICODE "By Jhonjhon_123"

```

그리고, 저 지점으로 가서 주변을 탐색해보니

VB의 문자열 비교 함수인 vbaStrCmp 함수를 찾을 수가 있었다.

```

00402474 50 PUSH EAX
00402475 51 PUSH ECX
00402476 FF15 44104000 CALL DWORD PTR DS:[<&MSVBVM60,___vbaStrCmp MSVBVM60,___vbaStrCmp

```

우선 저곳이 의심스러워 저곳에 BP를 걸고 시리얼에 123123을 넣고 프로그램을 실행시켜보았다.

그리고나서 함수 호출전 PUSH되는 EAX와 ECX의 값을 레지스터 상태창을 이용해 찾아보니

```

Registers (FPU)
EAX: 00208284 UNICODE "123123"
ECX: 002082F4 UNICODE "677345"

```

다음과 같이 내가 입력한 값과 이상한 값을 비교해주고있다.

저 이상한 값이 답인거 같아 인증을 했더니 답이었다 !:D