# Code Engn Basic

CodeEngn Basic 풀이 보고서 02~20

**제출일** 2018.12.25

**이름** 지현근



# Basic05

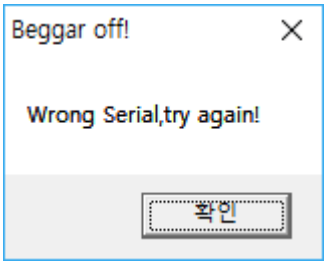
| 1. 문제 | 이 프로그램의 등록키는 무엇인가 |
|---|---|

## 2. 동적분석

### 1. 프로그램 실행

**① 분석하기**


프로그램을 실행하면 이름을 입력할 수 있는 부분과 코드를 입력할 수 있는 부분이 있는 것 같다. 그리고 Register now !를 보니 이 프로그램에 가입할 수 있는 등록키를 찾으면 되는 것 같다.


임의의 값을 입력하고 Register now !를 눌러보니 실패 문자열이 나온다.

**② 결과 정리**

| | |
|---|---|
| **파일이름** | 05.exe |
| **실행** | 가능 |
| **동적 분석을 통해 알아낸 정보** | 1. 실패 문자열은 Wrong Serial, try again!이다. |

3. 정적분석

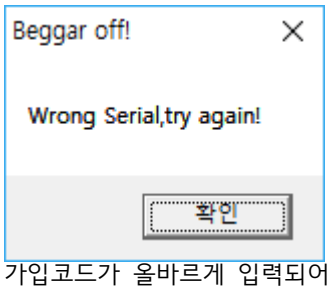
이 문제는 가입 코드를 찾아야 하므로 디버거를 열어준 후 바로 문자열을 검색했다. 문자열을 검색해보니 누가봐도 성공/실패 문자열인 문자들이 바로 눈에 보인다.

```
00440E9C  DD 05.00440CA8                    ASCII "4wB"
00440EA7  ASCII "Unitl"
00440EDC  MOV ECX,05.00440FC8               ASCII "No Name entered"
00440EE1  MOV EDX,05.00440FD8               ASCII "Enter a Name!"
00440F08  MOV ECX,05.00440FE8               ASCII "No Serial entered"
00440F0D  MOV EDX,05.00440FFC               ASCII "Enter a Serial!"
00440F2F  MOV EDX,05.00441014               ASCII "Registered User"
00440F4C  MOV EDX,05.0044102C               ASCII "GFX-754-IER-954"
00440F5A  MOV ECX,05.0044103C               ASCII "CrackMe cracked successfully"
00440F5F  MOV EDX,05.0044105C               ASCII "Congrats! You cracked this CrackMe!"
00440F74  MOV ECX,05.00441080               ASCII "Beggar off!"
00440F79  MOV EDX,05.0044108C               ASCII "Wrong Serial,try again!"
00440F8E  MOV ECX,05.00441080               ASCII "Beggar off!"
00440F93  MOV EDX,05.0044108C               ASCII "Wrong Serial,try again!"
```

여기서 누가봐도 가입코드인 "GFX-754-IER-954"로 이동하였다.

```
00440F44  .  E8 D7FEFDFF    CALL 05.00420E20
00440F49  .  8B45 FC        MOV EAX,DWORD PTR SS:[EBP-4]
00440F4C  .  BA 2C104400    MOV EDX,05.0044102C             ASCII "GFX-754-IER-954"
00440F51  .  E8 D62BFCFF    CALL 05.00403B2C
00440F56  .v 75 1A          JNZ SHORT 05.00440F72
00440F58  .  6A 00          PUSH 0
00440F5A  .  B9 3C104400    MOV ECX,05.0044103C             ASCII "CrackMe cracked successfully"
00440F5F  .  BA 5C104400    MOV EDX,05.0044105C             ASCII "Congrats! You cracked this CrackMe!"
00440F64  .  A1 442C4400    MOV EAX,DWORD PTR DS:[442C44]
00440F69  .  8B00           MOV EAX,DWORD PTR DS:[EAX]
00440F6B  .  E8 F8C0FFFF    CALL 05.0043D068
00440F70  .v EB 32          JMP SHORT 05.00440FA4
00440F72  >  6A 00          PUSH 0
00440F74  .  B9 80104400    MOV ECX,05.00441080             ASCII "Beggar off!"
00440F79  .  BA 8C104400    MOV EDX,05.0044108C             ASCII "Wrong Serial,try again!"
```

코드를 보면 입력한 가입코드가 "GFX-754-IER-954"과 같으면 JNZ를 타지 않고 성공 문자열을 출력한다. 하지만 가입코드를 올바르게 입력해도 오류문자가 계속 나오는걸 직접 실행해보면 알 수 있게 된다.




가입코드가 올바르게 입력되어도 오류문자가 출력된다면 이름도 정해진 것이 아닐까 하는 의심을 가져야 한다. 바로 이름을 입력받는 코드로 가보자.

```
00440EB0  .  55             PUSH EBP
00440EB1  .  8BEC           MOV EBP,ESP
00440EB3  .  6A 00          PUSH 0
00440EB5  .  53             PUSH EBX
00440EB6  .  8BD8           MOV EBX,EAX
00440EB8  .  33C0           XOR EAX,EAX
00440EBA  .  55             PUSH EBP
00440EBB  .  68 BA0F4400    PUSH 05.00440FBA
00440EC0  .  64:FF30        PUSH DWORD PTR FS:[EAX]
00440EC3  .  64:8920        MOV DWORD PTR FS:[EAX],ESP
00440EC6  .  8D55 FC        LEA EDX,DWORD PTR SS:[EBP-4]
00440EC9  .  8B83 C4020000  MOV EAX,DWORD PTR DS:[EBX+2C4]
00440ECF  .  E8 4CFFFDFF    CALL 05.00420E20
00440ED4  .  837D FC 00     CMP DWORD PTR SS:[EBP-4],0
00440ED8  .v 75 18          JNZ SHORT 05.00440EF2
00440EDA  .  6A 00          PUSH 0
00440EDC  .  B9 C80F4400    MOV ECX,05.00440FC8             ASCII "No Name entered"
00440EE1  .  BA D80F4400    MOV EDX,05.00440FD8             ASCII "Enter a Name!"
00440EE6  .  A1 442C4400    MOV EAX,DWORD PTR DS:[442C44]
00440EEB  .  8B00           MOV EAX,DWORD PTR DS:[EAX]
00440EED  .  E8 76C1FFFF    CALL 05.0043D068
00440EF2  >  8D55 FC        LEA EDX,DWORD PTR SS:[EBP-4]
00440EF5  .  8B83 C8020000  MOV EAX,DWORD PTR DS:[EBX+2C8]
00440EFB  .  E8 20FFFDFF    CALL 05.00420E20
00440F00  .  837D FC 00     CMP DWORD PTR SS:[EBP-4],0
00440F04  .v 75 18          JNZ SHORT 05.00440F1E
```

이곳으로 추정된다. 별도로 주석이 처리된 부분이 없으니 BP를 걸어주고 실행해보며 찾아보자. 직접 F8을 통해 하나하나 분석해보면 아래 코드에서는 이름을 입력받고, 이 프로그램이 입력받았는지 확인한다.

```
00440EB0  .  55              PUSH EBP
00440EB1  .  8BEC            MOV EBP,ESP
00440EB3  .  6A 00           PUSH 0
00440EB5  .  53              PUSH EBX
00440EB6  .  8BD8            MOV EBX,EAX
00440EB8  .  33C0            XOR EAX,EAX
00440EBA  .  55              PUSH EBP
00440EBB  .  68 BA0F4400     PUSH 05.00440FBA
00440EC0  .  64:FF30         PUSH DWORD PTR FS:[EAX]
00440EC3  .  64:8920         MOV DWORD PTR FS:[EAX],ESP
00440EC6  .  8D55 FC         LEA EDX,DWORD PTR SS:[EBP-4]
00440EC9  .  8B83 C4020000   MOV EAX,DWORD PTR DS:[EBX+2C4]
00440ECF  .  E8 4CFFFDFF     CALL 05.00420E20
00440ED4  .  837D FC 00      CMP DWORD PTR SS:[EBP-4],0
00440ED8  .  75 18           JNZ SHORT 05.00440EF2
```

그리고 아래 코드까지 내려가면 EAX에 입력한 이름이 들어간걸 확인할 수 있다.

```
00440F2F  .  BA 14104400     MOV EDX,05.00441014          ASCII "Registered User"
```

```
EAX 024A7A38 ASCII "TEAMISAAC"
```

그리고 내려가다 보면 이름에 무슨 값을 입력해야하는지 주석처리가 떡하니 되어있는걸 확인할 수 있다.

```
00440F2F  .  BA 14104400     MOV EDX,05.00441014          ASCII "Registered User"
00440F34  .  E8 F32BFCFF     CALL 05.00403B2C
00440F39  .  75 51           JNZ SHORT 05.00440F8C
```

(처음에는 당연히 가입버튼 문자열인줄 알았다..)

EAX값에 "Registered User"라는 값이 들어있는지 확인하는 것 같다.

이쯤되면 정적분석이 끝났다. 이제 문제를 해결하면 된다.

## 4. 문제해결

위 정적분석에서 확인했듯이 이름칸에는 "Registered User",코드칸에는 "GFX-754-IER-954"를 입력해주면 성공 문자열이 출력된다. 그리고 문제에서는 가입코드를 찾으라고 했으니 정답은 "GFX-754-IER-954"이다.