코드엔진 Basic RCE L07

문제

> CodeEngn.com [코드엔진]
>
> 코드엔진은 국내 리버스엔지니어링 정보공유를 위해 2007년 부터 리버스엔지니어링 컨퍼런스 및 세미나, 워크숍을 현업 실무자들과 함께 운영하고 있는 비영리 커뮤니티입니다.
>
> https://ch.codeengn.com/

의 Basic RCE L07

해결 과정

- 실행파일을 ollyDbg에 올려 입력한 시리얼 값이 맞는 값인지 틀린값인지에 따라 다르게 출력되는 문자열들을 검색하여 찾음

```
00401103 PUSH    00402434                ASCII "Error!"
00401108 PUSH    0040243B                ASCII "The serial you entered is not correct!"
00401119 PUSH    00402406                ASCII "Well Done!"
0040111E PUSH    00402411                ASCII "Yep, you entered a correct serial!"
```

- 정답 문자열이 동적으로 만들어지는 방식으로 이루어져 있어 정답 문자열을 알아내기 위해 틀린 시리얼 값을 입력하면 출력되는 문자열을 정답 문자열로 바꿈

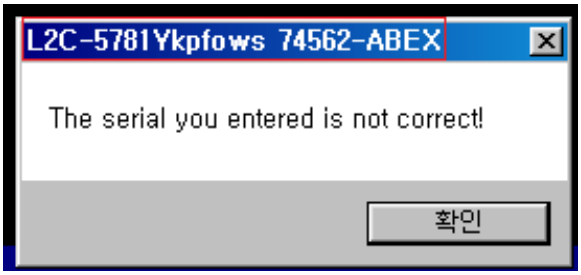
```
PUSH    0                       Style = MB_OK|MB_APPLMODAL
PUSH    00402434                Title = "Error!"
PUSH    0040243B                Text = "The serial you entered is not correct!"
PUSH    [ARG.1]                 hOwner = 7FFD6000
CALL    <JMP.&USER32.MessageBoxA>  MessageBoxA
```

변경 전(빨간 줄 박스안에 있는 코드를 변경할 예정)

```
PUSH    0                       Style = MB_OK|MB_APPLMODAL
PUSH    00402000
PUSH    0040243B                Text = "The serial you entered is not correct!"
PUSH    [ARG.1]                 hOwner = 7FFD6000
CALL    <JMP.&USER32.MessageBoxA>  MessageBoxA
```

변경 후(빨간 줄 박스안에 있는 코드에서 문자열의 주소값(PUSH옆 HEX값)을 변경)

- 그 후, 틀린 시리얼 값을 입력하여 출력된 문자열을 통해 정답 문자열을 파악



빨간 줄 박스안에 있는 문자열이 정답 문자열

- 정답 문자열에 포함되어있는 볼륨 이름을 보면 앞의 4개 문자가 제대로 출력되지 않고 +2해서 출력되는 것을 확인할 수 있음

정상적인 문자열

비 정상적인 문자열

- 위의 내용을 통해 컴퓨터 C드라이브의 이름이 ‘CodeEngn’일 경우 시리얼이 생성될 때 ‘CodeEngn’은 앞의 4개 문자에 +2를 해야함을 알 수 있으므로 이를 파악하여 해결

실행 흐름

- 사용자로부터 문자열을 받음
- GetVolumeInfomationA 함수를 사용하여 볼륨 이름 정보를 가져와 스택에 저장
- 두개의 이미 존재하는 문자열 사이에 볼륨 이름 정보를 끼워넣어서 문자열 완성
- 이때, 볼륨 이름 정보의 앞 4개 문자에 +2를 더해서 문자를 변경해야함
- 이렇게 완성된 문자열을 정답 문자열로 하고 이 문자열과 사용자가 입력한 문자열을 비교
- 비교하여 맞을경우 축하 문자열을 출력하고 틀릴경우 에러 문자열을 출력
- 모든 로직이 종료된 이후 프로그램 종료