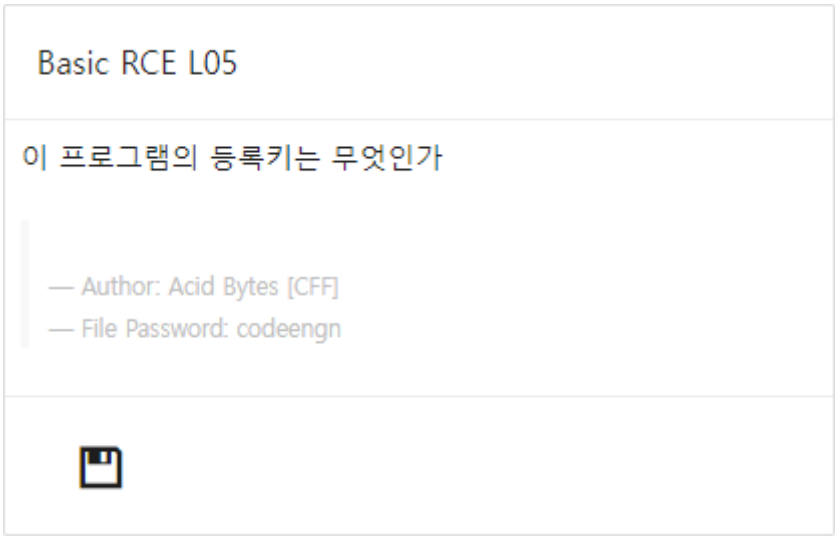
codeengn-basic-L05 풀이 UPX패킹 풀기

리버싱 문제풀이 / Wonlf / 2022. 3. 11. 12:15



한참을 삽질하다가 풀이를 보고 패킹이 되어 있다는 사실을 알았다. 이제부터 DIE로 정적분석을 먼저 해보고 동적분석을 진행 해야겠다.

UPX로 패킹이 되어 있습니다. 언패킹을 해보겠습니다.

```
PS C:\Users\a02\Downloads\upx-3.96-win64> .\upx.exe -d C:\Users\a02\Downloads\05.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    315392 <-    132608   42.05%    win32/pe     05.exe
upx: C:\Users\a02\Downloads\05.exe: IOException: C:\Users\a02\Downloads\05.exe: Permission denied

Unpacked 1 file: 0 ok, 1 error.
```

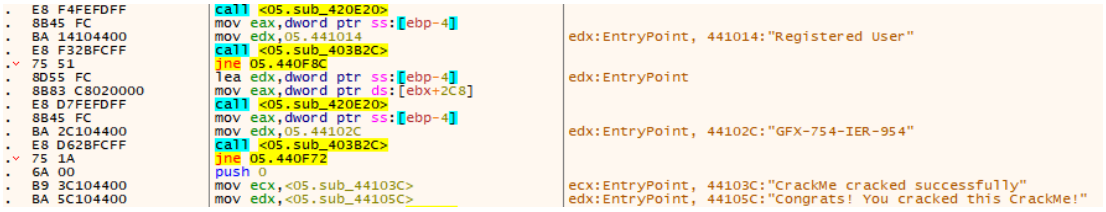
권한 오류로 언패킹이 되지 않아 찾아보니 파일이 디버거로 열려있으면 안된다고 합니다. 꺼주고 언패킹 하니

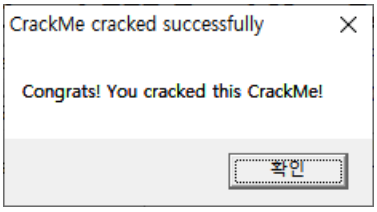
```
PS C:\Users\a02\Downloads\upx-3.96-win64> .\upx.exe -d C:\Users\a02\Downloads\05.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    315392 <-    132608   42.05%    win32/pe     05.exe

Unpacked 1 file.
```

성공 이제 파일을 뜯어보겠습니다.





딱 보니 저 두개가 ID와 PW같네요 입력하니 성공입니다.

막상 까보니 쉽네요

이 번문제는 UPX패킹과 문제 풀기 전에 정적분석을 먼저 해야겠다는 가르침을 얻었습니다