BasicRCE_L02

[문제] 패스워드로 인증하는 실행파일이 손상되어 실행이 안돼는 문제가 생겼다. 패스워드가 무엇인지 분석하시오.

다운받아 실행하면 정말로 실행이 되지 않았습니다. 제가 생각할 수 있는 것 중 가장 단순한 정보수집을 위해 HexEditor를 사용하여 바이너리 코드를 조금 확인하기로 했습니다.

해당 프로그램에서 사용되었을 함수의 이름이 보입니다.

```
05C0: 00 00 00 00  C0 20 00 00  B2 20 00 00  F0 20 00 00  ..... ... ... ..
05D0: A6 20 00 00  D2 20 00 00  94 20 00 00  E0 20 00 00  . ... ... ... ..
05E0: 00 00 00 00  92 00 44 69  61 6C 6F 67  42 6F 78 50  ......DialogBoxP
05F0: 61 72 61 6D  41 00 B8 00  45 6E 64 44  69 61 6C 6F  aramA...EndDialo
0600: 67 00 00 01  47 65 74 44  6C 67 49 74  65 6D 00 00  g...GetDlgItem..
0610: 02 01 47 65  74 44 6C 67  49 74 65 6D  54 65 78 74  ..GetDlgItemText
0620: 41 00 BB 01  4D 65 73 73  61 67 65 42  6F 78 41 00  A...MessageBoxA.
0630: 10 02 53 65  6E 64 4D 65  73 73 61 67  65 41 00 00  ..SendMessageA..
0640: 2B 02 53 65  74 46 6F 63  75 73 00 00  55 53 45 52  +.SetFocus..USER
0650: 33 32 2E 64  6C 6C 00 00  75 00 45 78  69 74 50 72  32.dll..u.ExitPr
0660: 6F 63 65 73  73 00 11 01  47 65 74 4D  6F 64 75 6C  ocess...GetModul
0670: 65 48 61 6E  64 6C 65 41  00 00 4B 45  52 4E 45 4C  eHandleA..KERNEL
0680: 33 32 2E 64  6C 6C 00 00  00 00 00 00  00 00 00 00  32.dll..........
0690: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
06A0: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
06B0: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
```

그리고 조금 더 많은 정보를 위해 휠을 아래로 내리면 다음과 같은 메시지도 확인할 수 있습니다.

```
0740: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0750: 41 44 44 69  61 6C 6F 67  00 41 72 74  75 72 44 65  ADDialog.ArturDe
0760: 6E 74 73 20  43 72 61 63  6B 4D 65 23  31 00 00 00  nts CrackMe#1...
0770: 00 00 00 00  00 4E 6F 70  65 2C 20 74  72 79 20 61  .....Nope, try a
0780: 67 61 69 6E  21 00 59 65  61 68 2C 20  79 6F 75 20  gain!.Yeah, you
0790: 64 69 64 20  69 74 21 00  43 72 61 63  6B 6D 65 20  did it!.Crackme
07A0: 23 31 00                              00 00 00 00  #1.       ......
07B0: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
```

Nope, try again!
Yeah, you did it!

마치 무슨 조건이 일치하였을 시에 메시지 창으로 띄우지 않을가 생각할 수 있으며, 다음으로 나오는 Crackme#1. JK3FJZh...

다음 문제를 위한 인증키 값을 띄워주지 않나 생각해봅니다. 인증 페이지에서 확인해보겠습니다.