

REPORT

Basic RCE Level 2

이름 : 신 민 구
제 출 일 : 2018.06.06

1. 문제 분석 및 실행

Challenges : Basic 02

Author : ArturDents

Korean :

패스워드로 인증하는 실행파일이 손상되어 실행이 안되는 문제가 생겼다. 패스워드가 무엇인지 분석하시오

English :

The program that verifies the password got messed up and ceases to execute. Find out what the password is.

[Download](#)

그림 1.1 Problem

Basic 02의 문제는 패스워드가 무엇인지 찾으라는 것이다. 한번 실행을 시켜보자.

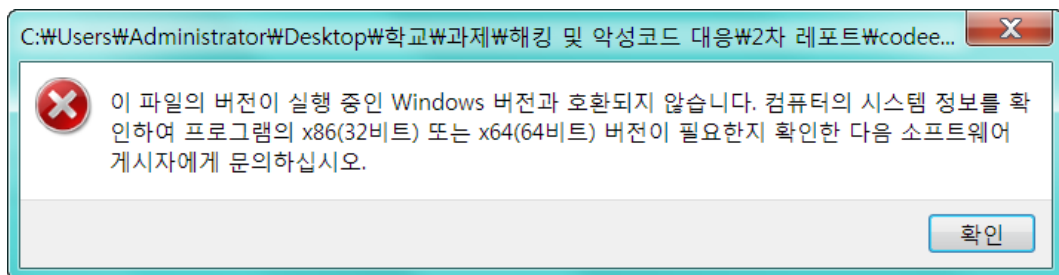


그림 1.2 실행 모습

파일이 손상이 되어서 위와 같은 메시지 박스가 나타났다. PEView를 통하여 파일이 어떻게 손상이 되었는지 살펴보자.

2. PEView

PEView라는 툴이 있는데 이는 파일의 구조를 볼 수 있다. PEView툴을 이용하여 열어보자.

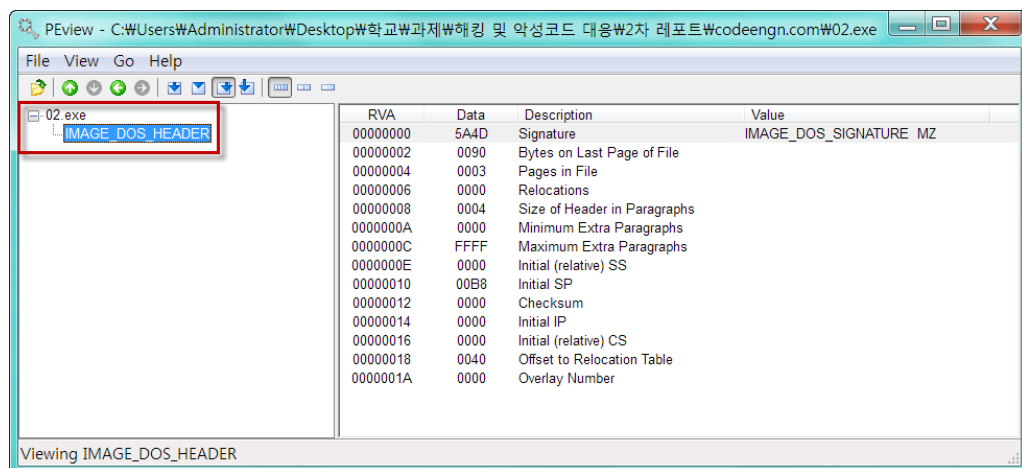


그림 2.1 PEView

구조를 보면 IMAGE_DOS_HEADER만 있다. 필수적으로 있어야 할 IMAGE_NT_HEADER, IMAGE_SECTION_HEADER 등 많은 것들이 없다. IMAGE_DOS_HEADER의 형태를 보면 많은 부분들이 잘못 되어 있는 것을 알 수 있다. 이것을 Hex Editor라는 프로그램으로 열어보자. Hex Editor은 binary 형식의 파일을 hex형식으로 보여주는 도구이다.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	Mz.....yy..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	,.....@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	0A	00	00	00	00	00	00	00	10	00	00	00	00	10	00
00000040	00	20	00	00	00	00	40	00	00	10	00	00	00	02	00	00@.....
00000050	04	00	00	00	00	00	00	04	00	00	00	00	00	00	00	00
00000060	00	50	00	00	00	04	00	00	00	00	00	00	00	02	00	00	..P.....
00000070	00	00	10	00	00	10	00	00	00	10	00	00	10	00	00	00
00000080	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00
00000090	2C	20	00	00	3C	00	00	00	40	00	00	18	03	00	00	00	...<...@.....
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000E0	00	00	00	00	00	00	00	00	20	00	00	2C	00	00	00	00
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000100	00	00	00	00	00	00	00	2E	74	65	78	74	00	00	00	00text...
00000110	52	01	00	00	00	10	00	00	00	02	00	00	00	04	00	00	R.....
00000120	00	00	00	00	00	00	00	00	00	00	00	20	00	00	60	00`
00000130	2E	72	64	61	74	61	00	00	38	01	00	00	00	20	00	00	..rdata..8....
00000140	00	02	00	00	00	06	00	00	00	00	00	00	00	00	00	00
00000150	00	00	00	00	40	00	00	40	2E	64	61	74	61	00	00	00@..@.data...
00000160	5C	02	00	00	00	30	00	00	00	02	00	00	00	08	00	00	\\....0.....@..Å
00000170	00	00	00	00	00	00	00	00	00	00	00	40	00	00	C0	00	..rsrc.....@..
00000180	2E	72	73	72	63	00	00	00	18	03	00	00	00	40	00	00@..
00000190	00	04	00	00	0A	00	00	00	00	00	00	00	00	00	00	00@..Å.....
000001A0	00	00	00	00	40	00	00	C0	00	00	00	00	00	00	00	00@..Å.....
000001B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

그림 2.12 Hex Editor

아무리 봐도 뭔가 상당히 잘못되어있는 것 같다. 그러나 이 HxD(Hex Editor) 에서도 함수나 여러 가지 정보를 보여준다. 그러니 밑으로 내려가서 살펴보도록 하자.

00000750	41 44 44 69 61 6C 6F 67 00 41 72 74 75 72 44 65	ADDIALOG.ArturDe
00000760	6E 74 73 20 43 72 61 63 6B 4D 65 23 31 00 00 00	nts CrackMe#1...
00000770	00 00 00 00 00 4E 6F 70 65 2C 20 74 72 79 20 61Nope, try a
00000780	67 61 69 6E 21 00 59 65 61 68 2C 20 79 6F 75 20	gain!.Yeah, you
00000790	64 69 64 20 69 74 21 00 43 72 61 63 6B 6D 65 20	did it!.Crackme
000007A0	23 31 00 4A 4B 33 46 4A 5A 68 00 00 00 00 00 00	#1.JK3FJZh.....

그림 2.13 Password

‘Yeah, you did it!’이라는 문자열이 있고 뒤에 Crack me#1과 ‘JK3FJZh’라는 문자열이 보인다. JK3FJZh가 뭔가를 나타내는 것 같은데 패스워드 인 것 같아 보인다. 이 값을 가지고 인증을 하면 인증이 되는 것을 보아 패스워드를 알 수 있다.