

Secret Document


문제

473명 해결

×

Secret Document
150

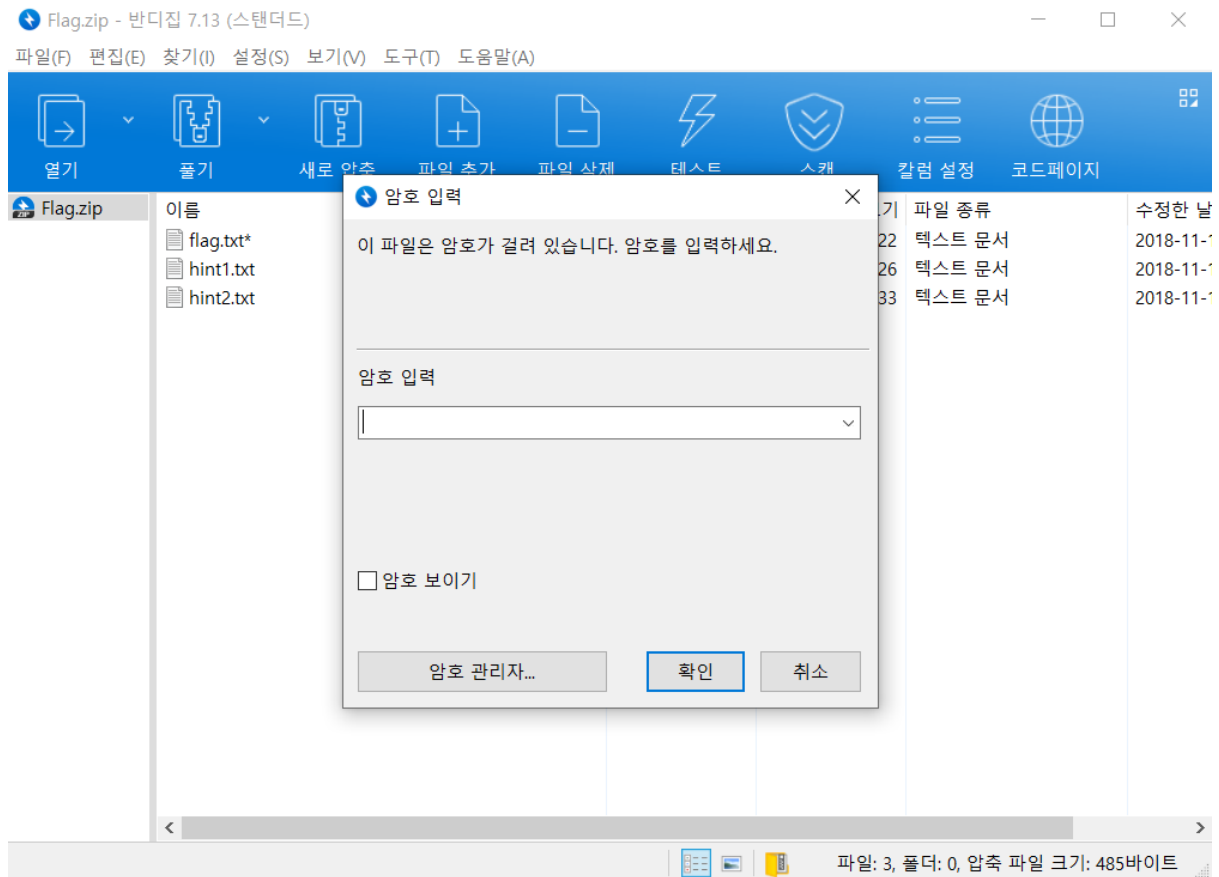
Author: Chu

 Flag.zip

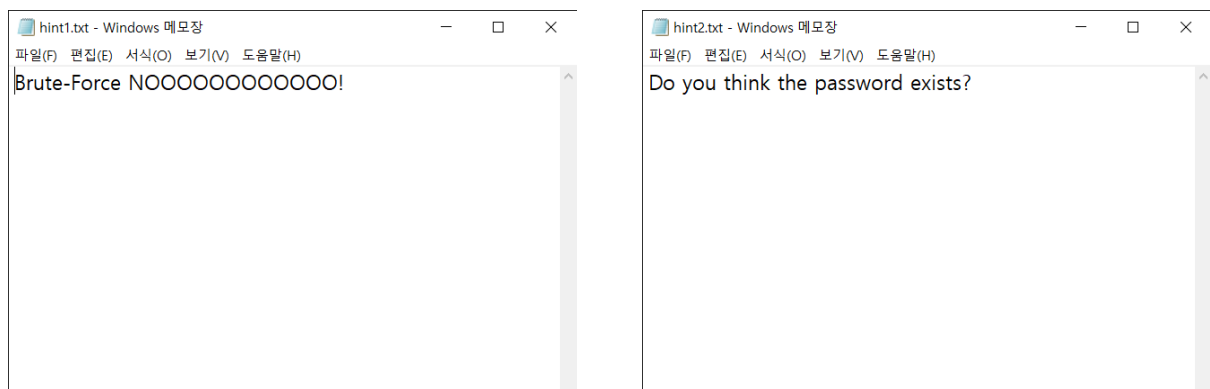
HackCTF{...}

제출

Flag.zip을 다운받아서 압축을 풀려고 하면 암호를 입력하라고 해서 풀 수가 없다ㅜㅜ



flag.txt* 파일은 열리지 않지만 hint1.txt 와 hint2.txt 파일은 열 수 있어서 열어보니까 다음과 같이 적혀 있다.



무차별 대입 공격은 ㄴㄴ하고 패스워드가 존재할거라고 생각하냐고? ㅋㅋㅋㅋ
그럼 당연히 존재 하지 않을 것 같다..

할게 뭐있나 싶어서 HxD로 hexa 값을 살펴보기로 했다!

들어가서 열어보니까 zip파일의 헤더시그니처(50 4B 03 04)가 총 3개나 존재했다.

문자열을 살펴봤을때 PK이라는 값이 여러번 보이길래 이상해서 찾아보니까

(50 4B 03 04) Local File Header

(50 4B 01 02) Central File Header

이렇게 두 종류의 zip파일 시그니처가 있었다.

Local Header	Central directory file header
4Byte: Local file header signature	4Byte: Local file header signature
2Byte: Version needed to extract	2Byte: Version made by
2Byte: General purpose bit flag	2Byte: Version needed to extract
	2Byte: General purpose bit flag

둘다 General purpose bit flag라고 하여 암호화를 나타내는 flag가 있는데 위치가 조금 다르다.

만약 General purpose bit flag에 "09 08" 이라고 들어 있으면

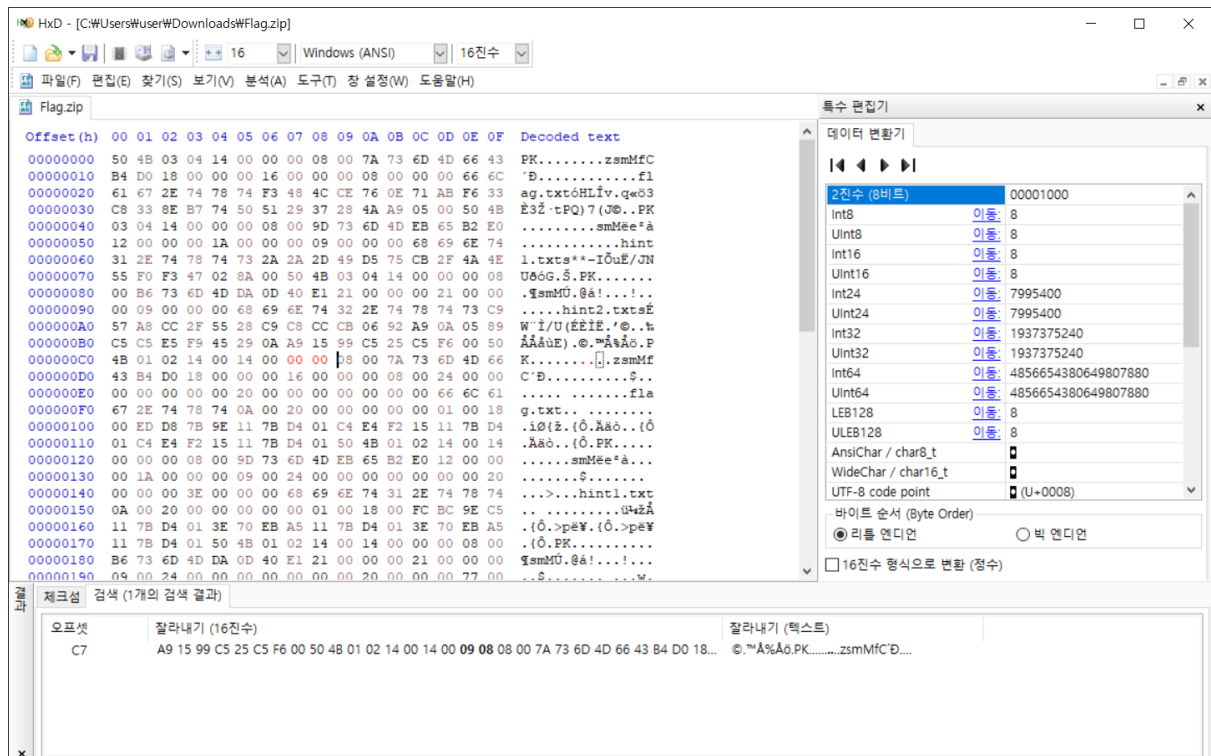
리틀엔디안 방식을 쓰기 때문에 bit 값을 확일할때는 08 09 → 1000 1001로 알아야한다.

이때 첫번째 bit가 1이면 해당파일은 암호화 되었다고 나타나기 때문에 0으로 바꿔줘야한다.

The screenshot shows the HxD hex editor interface. The main window displays the hex data of a zip file. The 'General purpose bit flag' field (offset 0000004B) contains the value 09 08. The 'Data descriptor' field (offset 000000F0) contains the value 00 00. The 'Data descriptor' field is highlighted in the 'Data descriptor' tab. The 'Data descriptor' tab shows the following data:

Offset	Hex	Text
00000000	50 4B 03 04 14 00 00 00 08 00 7A 73 6D 4D 66 43	PK.....zsmMfC
00000001	B4 D0 18 00 00 00 16 00 00 00 08 00 00 00 66 6C	'D.....fl
00000002	61 67 2E 74 78 74 F3 48 4C CE 76 0E 71 AB F6 33	ag.txtôHLIv.qeô3
00000003	C8 33 8E B7 74 50 51 29 37 28 4A A9 05 00 50 4B	E3Z-tPQ)7(J0..PK
00000004	03 04 14 00 00 00 08 00 9D 73 6D 4D EB 65 B2 E0smMée*à
00000005	12 00 00 00 1A 00 00 00 09 00 00 00 68 69 6E 74hint
00000006	31 2E 74 78 74 73 2A 2A 2D 49 D5 75 CB 2F 4A 4E	l.txts**~IôuE/JN
00000007	55 F0 F3 47 02 8A 00 50 4B 03 04 14 00 00 00 08	UôôG.Š.PK.....
00000008	00 B6 73 6D 4D DA 0D 40 E1 21 00 00 00 21 00 00	..smMÜ.ôâ!...!...
00000009	00 09 00 00 00 68 69 6E 74 32 2E 74 78 74 73 C9hint2.txtsE
0000000A	57 A8 CC 2F 55 28 C9 C8 CB 06 92 A9 0A 05 89	W'i/U(EEIE.'@..h
0000000B	C5 C5 E5 F9 45 29 0A A9 15 99 C5 25 C5 F6 00 50	ÅÅÅôE).@..Å%Åô.Š
0000000C	4B 01 02 14 00 14 00 09 08 08 00 7A 73 6D 4D 66zsmMf
0000000D	43 B4 D0 18 00 00 00 16 00 00 00 08 00 24 00 00	C'D.....Š..
0000000E	00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C 61fla
0000000F	67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00 18	g.txt..
00000010	00 ED D8 7B 9E 11 7B D4 01 C4 E4 F2 15 11 7B D4	.iô(z.(ô.Åaô..(ô
00000011	01 C4 E4 F2 15 11 7B D4 01 50 4B 01 02 14 00 14	Åaô..(ô.PK.....
00000012	00 00 00 08 00 9D 73 6D 4D EB 65 B2 E0 12 00 00smMée*à...
00000013	00 1A 00 00 00 09 00 24 00 00 00 00 00 00 00 20Š.....
00000014	00 00 00 3E 00 00 00 68 69 6E 74 31 2E 74 78 74hint1.txt
00000015	0A 00 20 00 00 00 00 00 01 00 18 00 FC BC 9E C5ô%ÅÅ
00000016	11 7B D4 01 3E 70 EB A5 11 7B D4 01 3E 70 EB A5	.(ô.>pë¥.(ô.>pë¥
00000017	11 7B D4 01 50 4B 01 02 14 00 14 00 00 00 08 00	.(ô.PK.....
00000018	B6 73 6D 4D DA 0D 40 E1 21 00 00 00 21 00 00 00	šsmMÜ.ôâ!...!...
00000019	09 00 24 00 00 00 00 00 00 20 00 00 00 77 00Š.....

여기서 보면 저 Central File Header 종류의 General purpose bit flag 이 암호화 됐다고 표시하고 있으니 저 09 08 부분을 00 00 으로 바꿔준다



이제 다시 파일을 열어보면 암호없이 압축해제가 된다!