

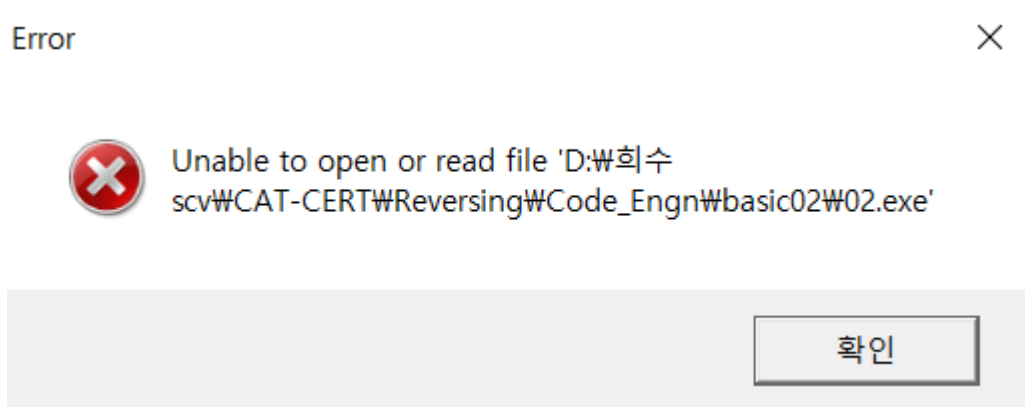
Challenges : Basic 02

Author : ArturDents

Korean :

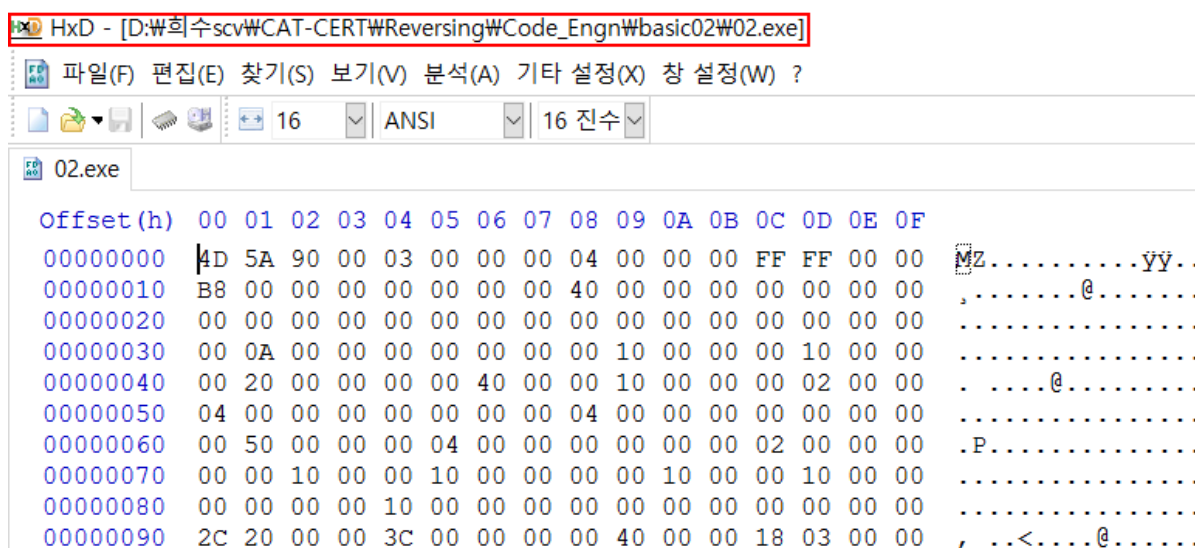
패스워드로 인증하는 실행파일이 손상되어 실행이 안되는 문제가 생겼다. **패스워드**가 무엇인지 분석하시오

▶ 디버깅하여 패스워드를 알아내면 될 것 같다.



▶ 하지만 **ollydbg**로 디버깅하려고 하면 에러를 띄운다.

▶ 마찬가지로 **IDA**에서도 정상적인 디버깅을 할 수 없다.



▶ 이진 파일을 16진수값으로 보여주고 수정도 할 수 있는 헥스 에디터인 **HxD**로 열어 보았다.

▶ 왼쪽의 **offset**, 중앙의 **hex코드**, 오른쪽의 **text(hex코드를 아스키로 출력)**가 있다.

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

▶ 패스워드가 숨겨져 있을 것으로 예상하고 **text**부분을 관찰해보자.

▶ 밑으로 내리다 보면 **text**부분에 위와 같은 문자열을 발견할 수 있다.

▶ ‘Nope, try again!’은 실패 메시지의 문자열 내용인 것 같고 ‘Yeah, you did it!’은 성공 메시지의 문자열 내용인 것 같다.

▶ 이후 ‘JK3FJZh’라는 문자열을 볼 수 있는데 문제에서 요구하는 **password**값 인 것 같다.

