

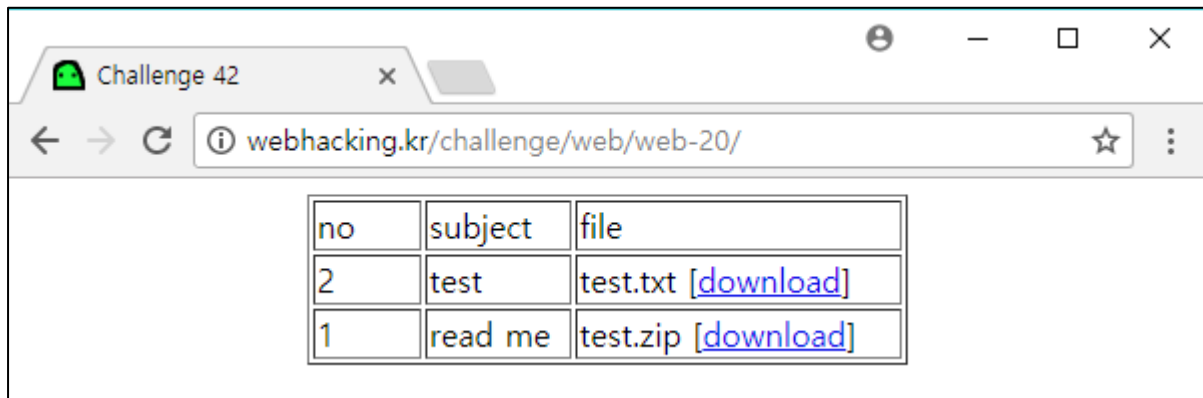
Level 42 문제 풀이



사이트	Webhacking.kr
작성일자	2017. 11. 10. 금
작성자	shamuxu

Level 42

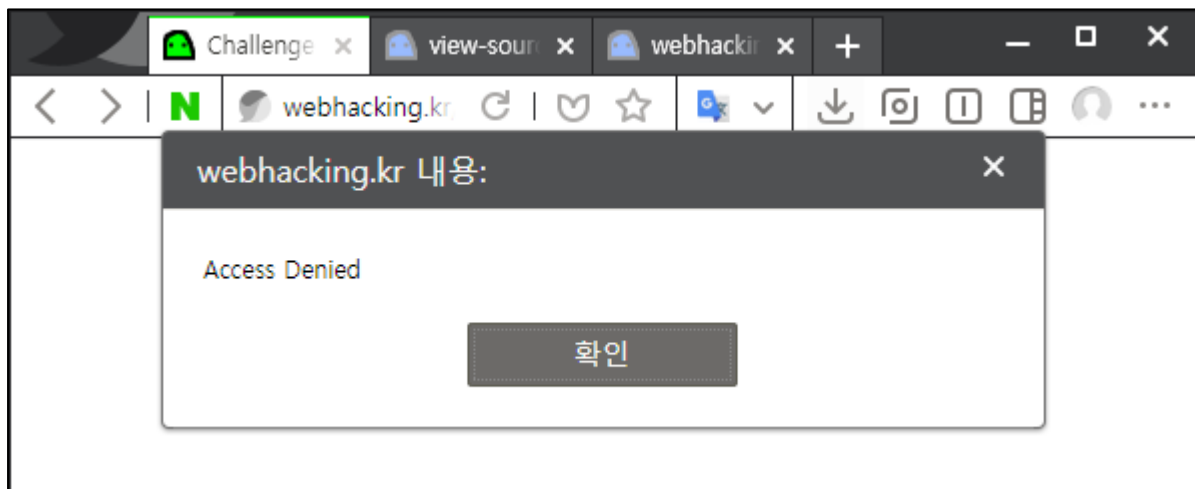
Level 42문제를 살펴보면 게시물 2개에 첨부된 파일이 각각 한 개씩 존재하는 페이지입니다.



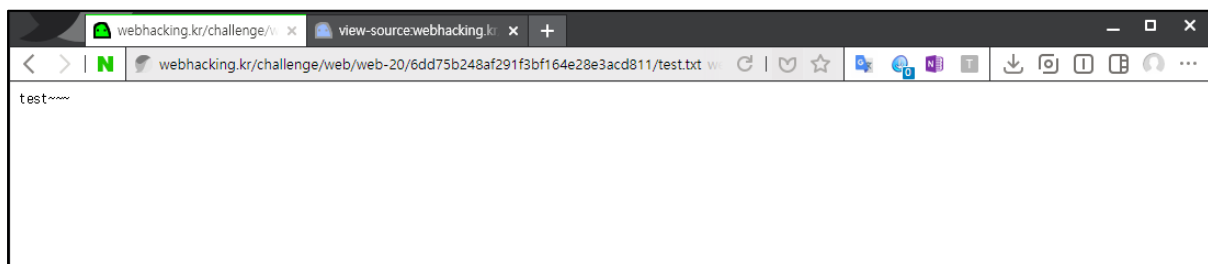
[그림 1] Level 42 문제 페이지

각각 두 파일을 다운로드 시도해보면 test.zip 파일은 접근불가.

test.txt 파일은 단순히 test~~~ 메시지만 출력됩니다.



[그림 2] test.zip 다운로드

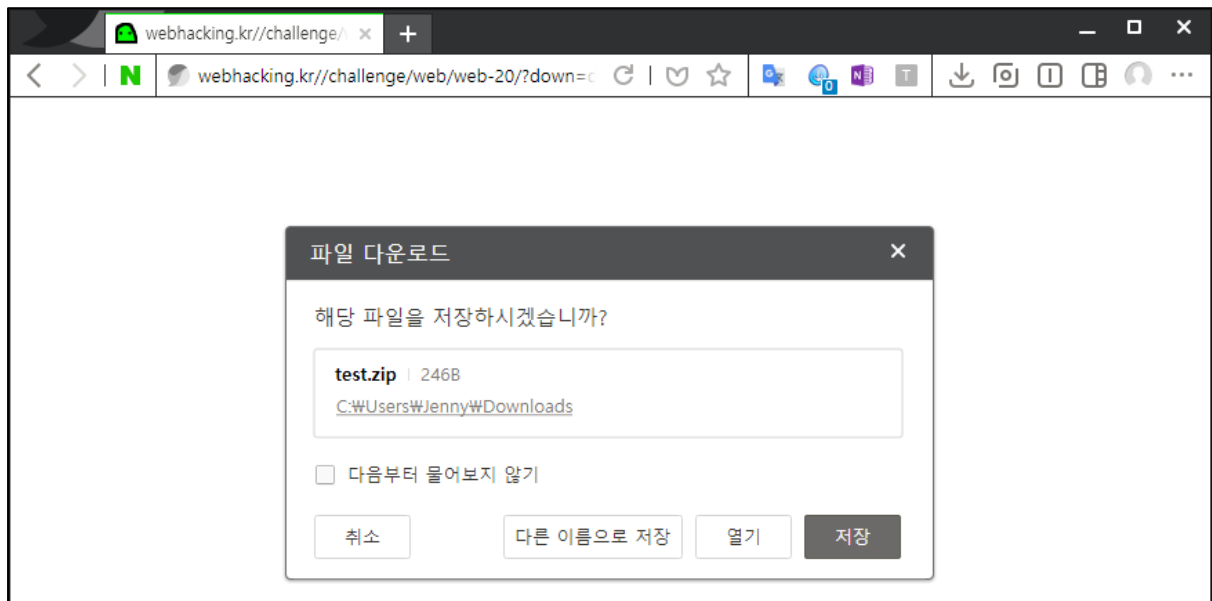


[그림 3] test.txt 다운로드

url을 살펴보면 down 파라미터에 다운받을 파일을 base64로 인코딩하여 전달합니다.

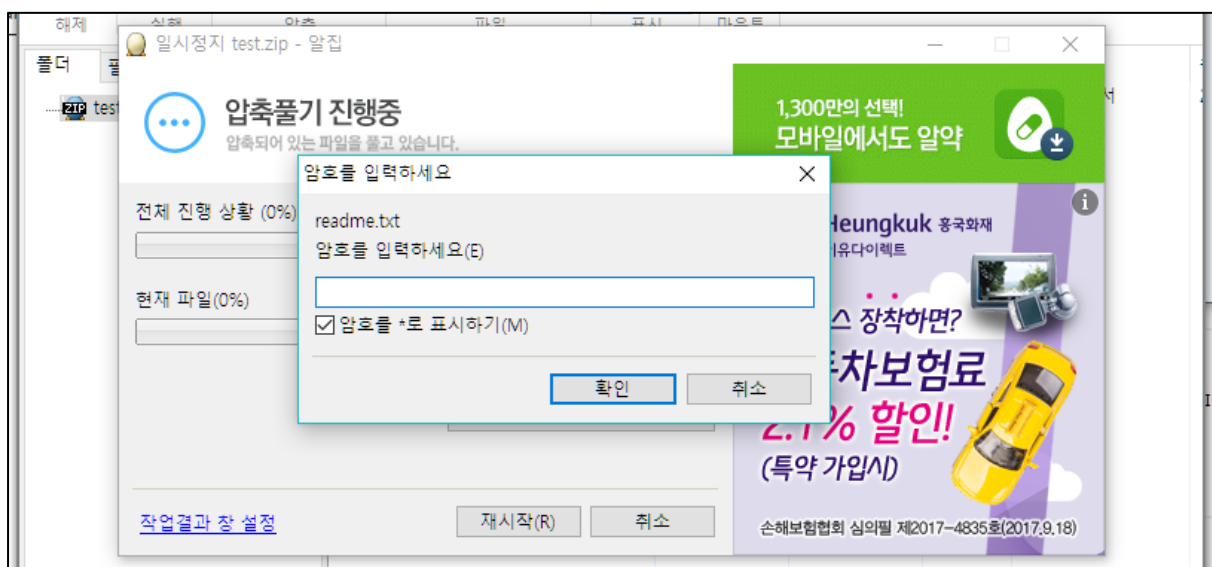
http://webhacking.kr//challenge/web/web-20/?down=dGVzdC50eHQ= -> test.txt

이를 이용하여 down 파라미터에 test.zip base64 인코딩(dGVzdC56aXA=) 값을 전달하면 test.zip 파일을 다운받을 수 있습니다.



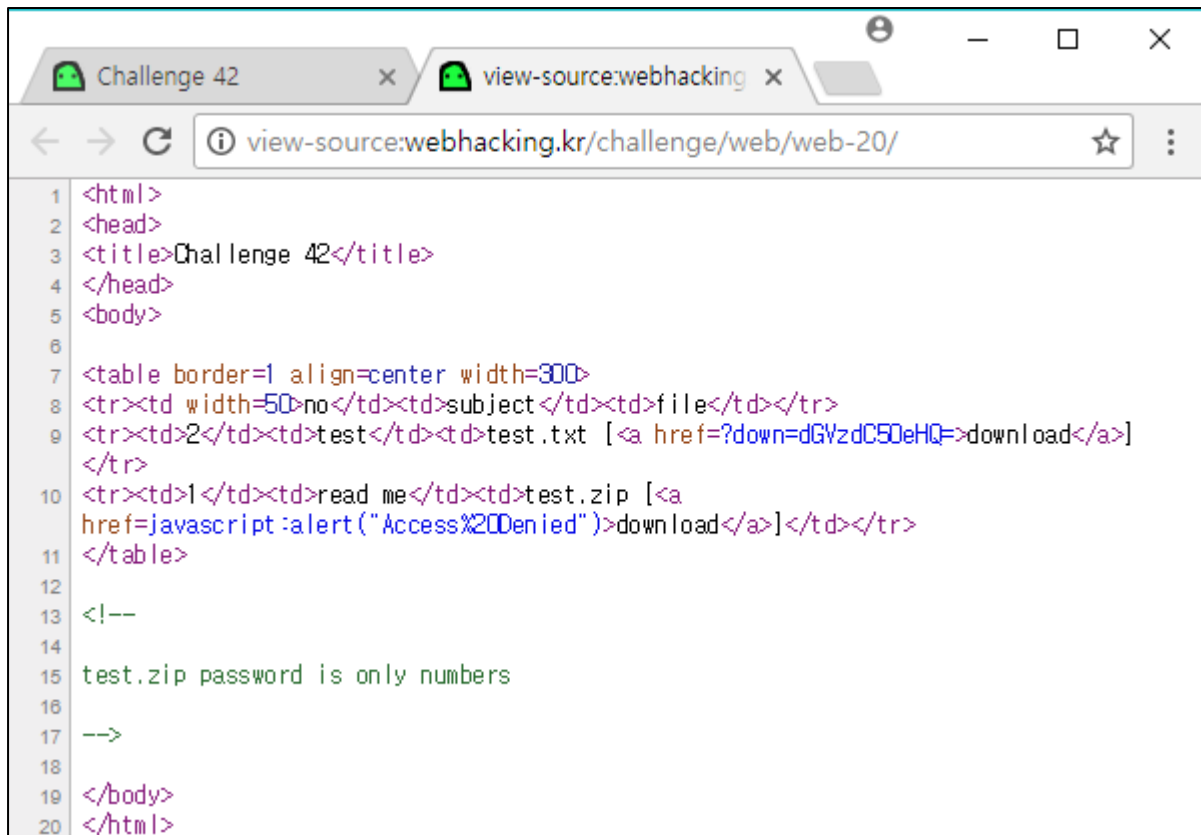
[그림 4] test.zip 파일 다운로드

다운로드 받은 알집 파일을 열어보면 패스워드가 걸려있는 것을 확인할 수 있습니다.



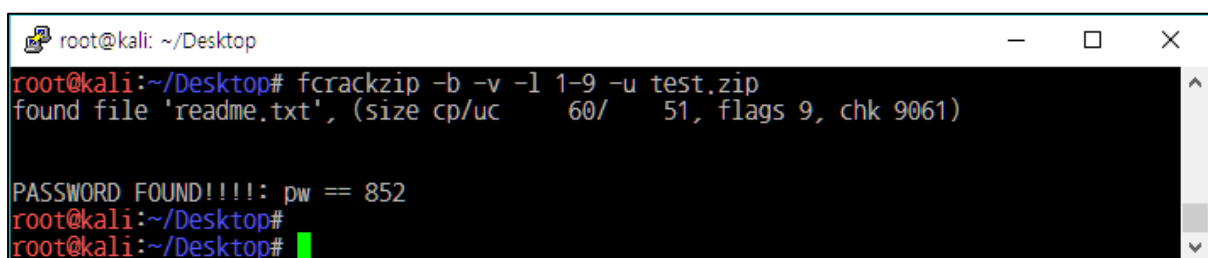
[그림 5] 알집 패스워드 설정 확인

[그림 1]의 페이지 소스보기를 통해 패스워드의 힌트를 확인할 수 있습니다.



[그림 6] 패스워드 힌트

다음은 Kali Linux 에는 zip 파일 패스워드 크래킹 툴을 사용하여 패스워드를 알아낸 화면입니다.



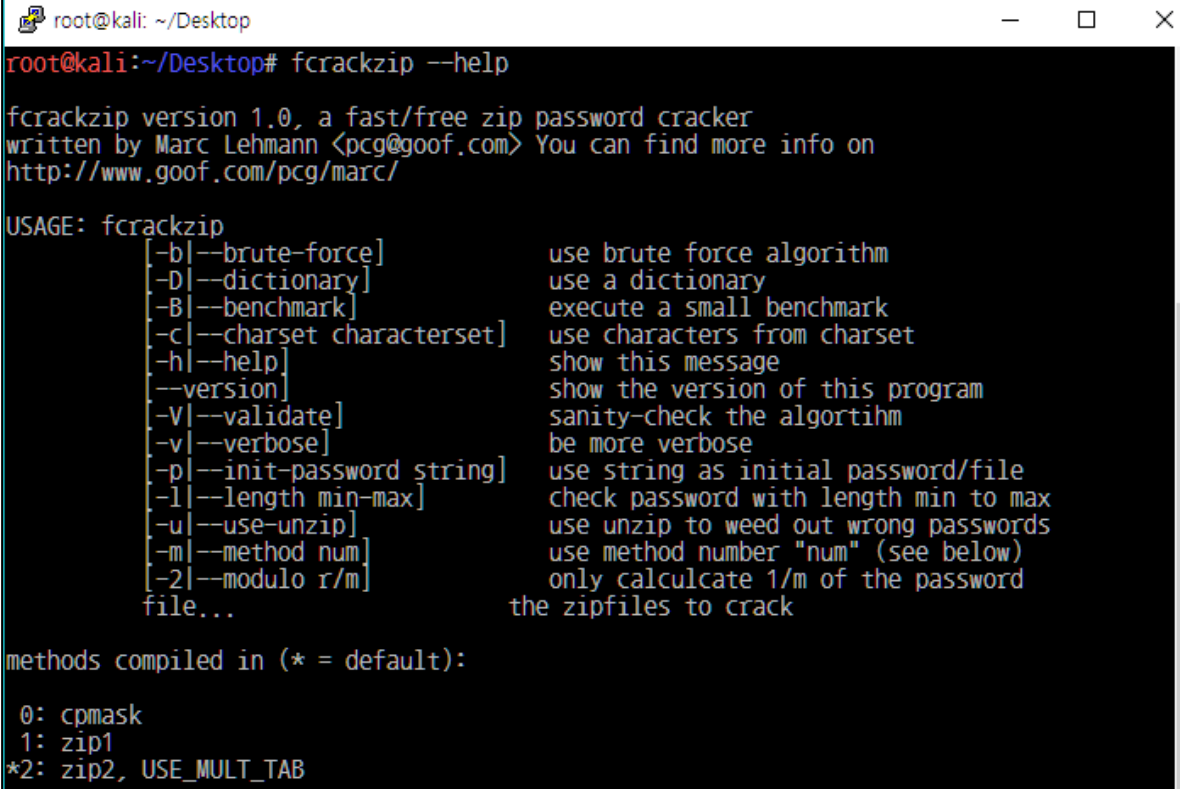
[그림 7] 패스워드 확인

fcrackzip 사용법

- b: Brute force Mode
- v: 자세한 정보 출력
- l: 글자 수 min-max
- u: 틀린 패스워드 출력 제외

-c: 문자 설정(오직 숫자라고 했으니 '1' 입력, 영어문자도 포함할 경우 'aA', 특수문자 '!' 적으면 됨)

--help 을 통해 다른 옵션들을 확인할 수 있다.



```
root@kali: ~/Desktop
root@kali:~/Desktop# fcrackzip --help

fcrackzip version 1.0, a fast/free zip password cracker
written by Marc Lehmann <pcg@goof.com> You can find more info on
http://www.goof.com/pcg/marc/

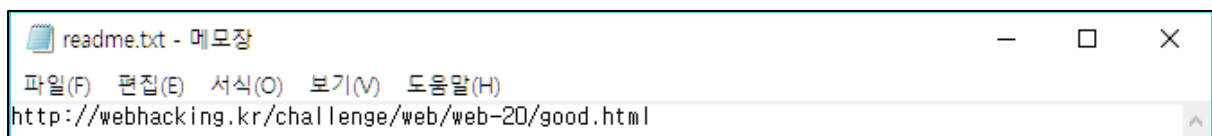
USAGE: fcrackzip
    [-b|--brute-force]      use brute force algorithm
    [-D|--dictionary]      use a dictionary
    [-B|--benchmark]       execute a small benchmark
    [-c|--charset charset] use characters from charset
    [-h|--help]            show this message
    [--version]            show the version of this program
    [-V|--validate]        sanity-check the algorithm
    [-v|--verbose]         be more verbose
    [-p|--init-password string] use string as initial password/file
    [-l|--length min-max]  check password with length min to max
    [-u|--use-unzip]        use unzip to weed out wrong passwords
    [-m|--method num]       use method number "num" (see below)
    [-2|--modulo r/m]       only calculate 1/m of the password
    file...                the zipfiles to crack

methods compiled in (* = default):
  0: cpmask
  1: zip1
 *2: zip2, USE_MULT_TAB
```

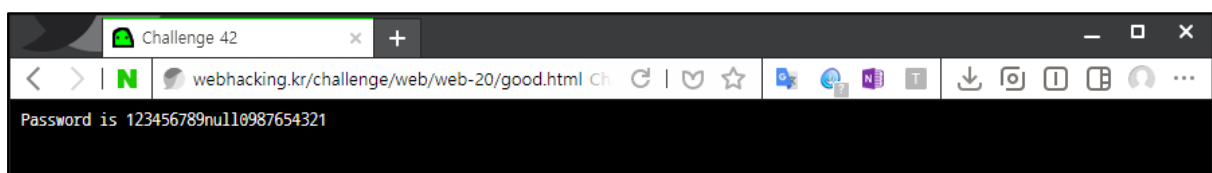
[그림 8] fcrackzip 사용법

패스워드 852를 입력하면 압축파일 안에 readme.txt 파일을 확인할 수 있습니다.

해당 주소에는 42번 문제의 인증 값이 적혀 있습니다.



[그림 9] readme.txt



[그림 10] level 42 인증값