B1ackZer0 2011.05.05

## 다음과 같은 표가 있다.

변호	제목	첨부파일
2	test	test.txt [ <u>download</u> ]
1	read me	test.zip [ <u>download</u> ]

test.txt 의 링크를 눌렀을때의 글이다.

test~~~

test.zip 의 링크를 눌렀을때는 그냥 alert로 경고창만 출력해서 소스를 보았다.

<html>

<head>

<title>Challenge 42</title>

</head>

<body>

번호제목첨부파일

2testtest.txt

[<a

href=?down=dGVzdC50eHQ=>download</a>]

<!-- test.zip 파일의 패스워드는 숫자로만 이루어져 있습니다. -->

</body>

</html>

test.txt 의 링크를 눌렀을때 ?down=dGVzdC50eHQ= 로 이동된다.

저것을 base64로 디코드 해보니 test.txt가 나왔다.

그렇다면 ?down=test.zip을 base64인코드 한 값을 넣으면 될 것 같다.

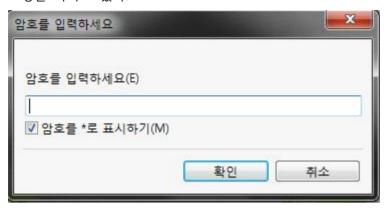
## 다음과 같은 주소로 들어갔다.

### http://webhacking.kr/challenge/web/web-20/?down=dGVzdC56aXA=

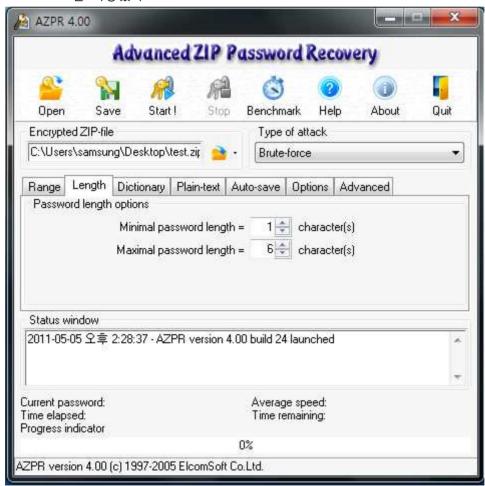
역시나 예상대로 test.zip을 얻었다.

하지만 암호가 걸려있다.

주석의 힌트대로 숫자로 구성되어있는것은 알았지만 무엇인지를 모르니 툴을 이용해 브루트 포싱을 하기로 했다.



## AZPR 4.00을 이용했다.



AZPR 4.00 - 75% Advanced ZIP Password Recovery Password successfully recovered! Advanced ZIP Password Recovery statistics: 870,961 Total passwords Total time 41ms Average speed (passwords per second) 21,242,951 Password for this file 759852 Password in HEX 37 35 39 38 35 32 **V**OK Save... Status window \samsung\Desktop\ 2011-05-05 오후 2:28:54 - Starting brute-force attack... 2011-05-05 오후 2:28:54 - Password successfully recovered !

암호를 숫자로 설정하고 6자리로 하니 암호가 759852라는것을 알았다.

위의 암호로 압축을 풀어서 나온 파일을 txt로 열었더니 <a href="http://webhacking.kr/challenge/web/web-20/good.html">http://webhacking.kr/challenge/web/web-20/good.html</a> 라는 주소가 나왔다. 위의 주소로 들어가니 다음과 같은 글이 있었다.

## Password is

Current password: 759852

Time elapsed:

그냥 Password is만 나와있길래 소스 보기를 했다. 다음이 소스이다.

123456789null0987654321 를 인증했고, 인증에 성공했다.

2011-05-05 오후 2:28:54 - '759852' is a valid password for this file

Password length = 6, total: 1,000,000, processed: 759,851

AZPR version 4.00 (c) 1997-2005 ElcomSoft Co.Ltd.

<html><head><title>Challenge 42</title></head><body bgcolor=black><font size=2 color=white>Password is <!-- 123456789null0987654321 --></body></html>

Average speed:

Time remaining:

22,332,333 p/s