

# webhacking.kr 42번문제

Xero

박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)

2016-04-01

Email : wnsgurzxc@naver.com

Facebook : <https://www.facebook.com/wnsgurzxc>

파일 두 개가 있다.

no	subject	file
2	test	test.txt <a href="#">[download]</a>
1	read me	test.zip <a href="#">[download]</a>

소스를 보면 test.zip 비밀번호가 숫자로만 이루어져있다고 한다.

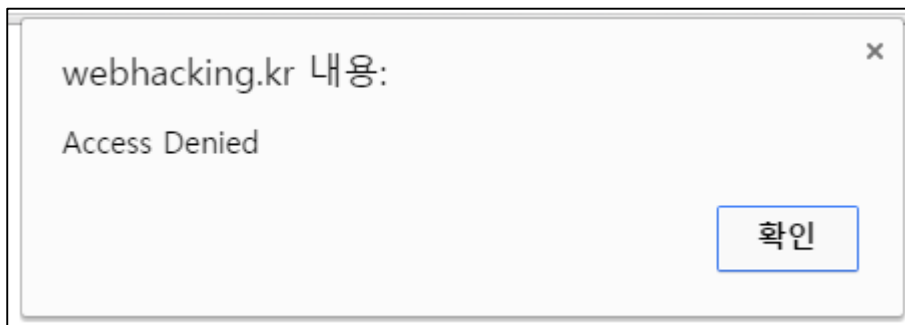
우선 test.txt를 download하면 다음의 주소로 들어가지고 test~~~ 값만 보인다.  
?down=dGVzdC50eHQ=

test~~~

위의 down값이 base64라고 생각하고 decode해보았다.  
그러자 test.txt가 떴다.

```
>>> import base64
>>> base64.b64decode(b'dGVzdC50eHQ=')
b'test.txt'
```

test.zip을 download하려고하면 Access Denied가 뜬다.



down값이 download하려는 파일이름을 base64인코딩해서 넣은 값이라고 생각하고 test.zip을 base64인코딩 해보았다.

```
>>> import base64
>>> base64.b64encode(b'test.zip')
b'dGVzdC56aXA='
```

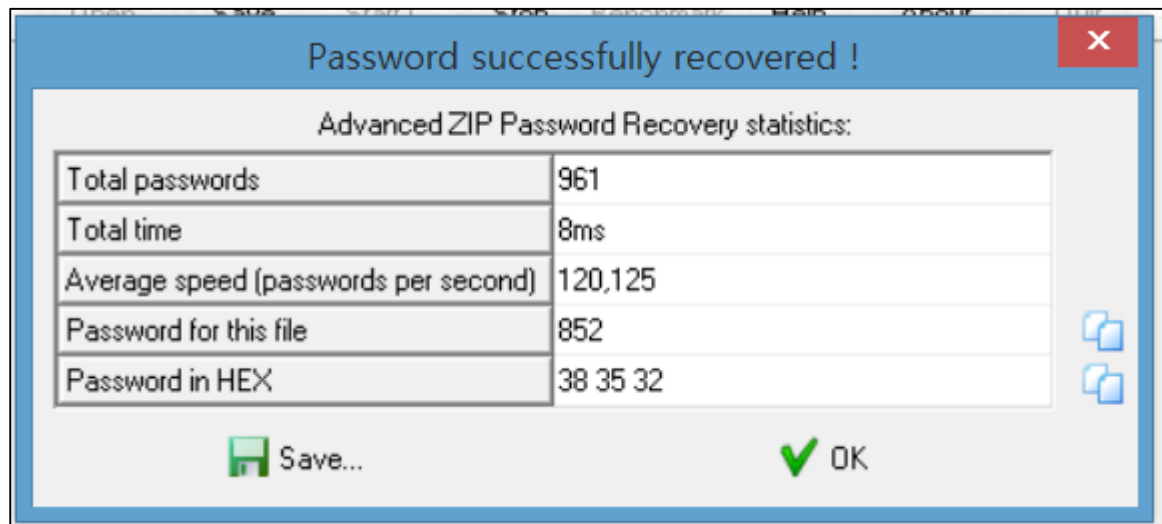
아래의 주소로 들어가면 test.zip을 다운받을 수 있다.  
?down=dGVzdC56aXA=

AZPR을 이용해서 풀기로 했다.

힌트로 숫자로만 되어있다고 했으므로 숫자로만 브루트포싱을 하면 된다.



비밀번호가 852인걸 알게 된다.



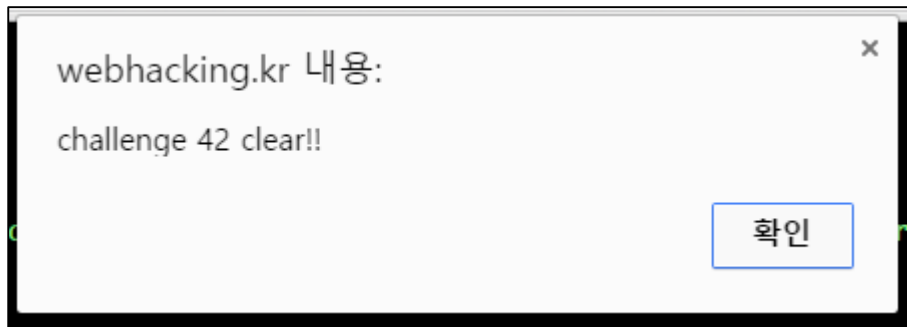
압축을 해제하면 readme.txt가 나오고 다음의 값이 있다.

<http://webhacking.kr/challenge/web/web-20/good.html>

위의 주소로 들어가면 password를 알려준다.

Password is 123456789null0987654321

Auth에 인증하면 클리어 된다.



KEY : 123456789null0987654321