webhacking.kr 42번문제

B1ackZer0
2011.05.05

다음과 같은 표가 있다.

| 번호 | 제목 | 첨부파일 |
|---|---|---|
| 2 | test | test.txt [download] |
| 1 | read me | test.zip [download] |

test.txt 의 링크를 눌렀을때의 글이다.

```
test~~~
```

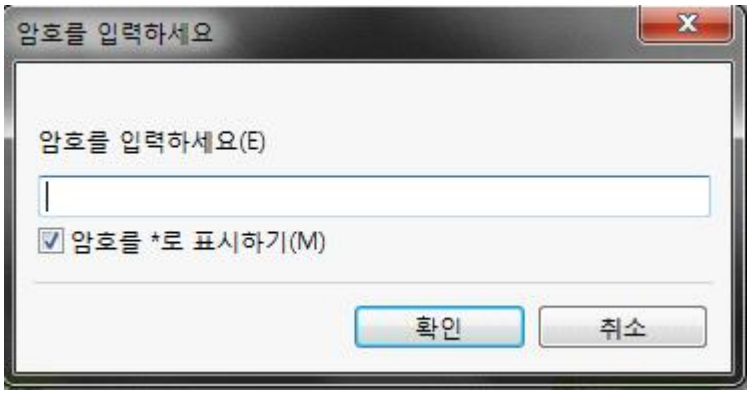
test.zip 의 링크를 눌렀을때는 그냥 alert로 경고창만 출력해서 소스를 보았다.

```
<html>
<head>
<title>Challenge 42</title>
</head>
<body>

<table border=1 align=center width=300>
<tr><td width=50>번호</td><td>제목</td><td>첨부파일</td></tr>
<tr><td>2</td><td>test</td><td>test.txt [<a href=?down=dGVzdC50eHQ=>download</a>]</tr>
<tr><td>1</td><td>read me</td><td>test.zip [<a href=javascript:alert("권한이%20없습니다")>download</a>]</td></tr>
</table>

<!-- 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.


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.

암호를 숫자로 설정하고 6자리로 하니 암호가 759852라는것을 알았다.


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

Password is

그냥 Password is만 나와있길래 소스 보기를 했다.
다음이 소스이다.
123456789null0987654321 를 인증했고, 인증에 성공했다.

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