webhacking.kr 37번문제

Xero
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)
2016-04-15
Email : wnsgurzxc@naver.com
Facebook : https://www.facebook.com/wnsgurzxc

다음과 같이 파일제출이 있다.

소스를 보면 index.phps를 가르킨다.

Index.phps로 들어가보면 다음과 같은 소스를 볼 수 있다.

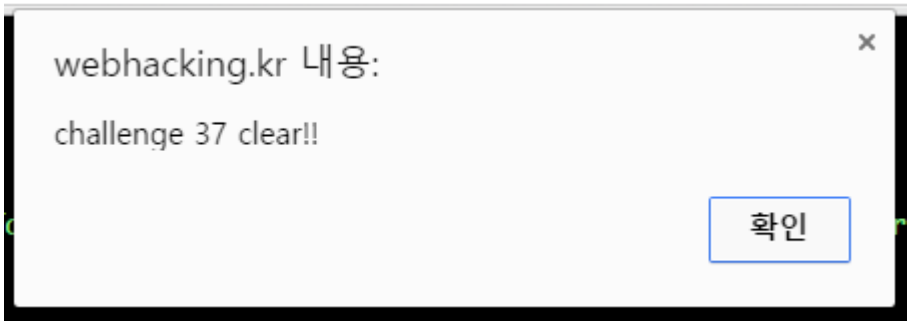
```php
<?
$pw="???";
$time=time();
$f=fopen("tmp/tmp-$time","w");
fwrite($f,"127.0.0.1");
fclose($f);
$fck=@file("tmp/.number");
if($fck) $fck=$fck[0];
if(!$fck) $fck=0;
$fck++;
$f2=fopen("tmp/.number","w");
fwrite($f2,$fck);
fclose($f2);
$file_nm=$HTTP_POST_FILES[upfile][name];
$file_nm=str_replace("<","",$file_nm);
$file_nm=str_replace(">","",$file_nm);
$file_nm=str_replace(".","",$file_nm);
$file_nm=str_replace(" ","",$file_nm);
if($file_nm)
{
$f=@fopen("tmp/$file_nm","w");
@fwrite($f,$_SERVER[REMOTE_ADDR]);
@fclose($f);
}
echo("<pre>");
$kk=scandir("tmp");
for($i=0;$i<=count($kk);$i++)
{
echo("$kk[$i]\n");
}
echo("</pre>");
$ck=file("tmp/tmp-$time");
$ck=$ck[0];
$request="GET /$pw HTTP/1.0\r\n";
$request.="Host: $ck\r\n";
$request.="\r\n";
$socket=@fsockopen($ck,7777,$errstr,$errno,1);
@fputs($socket,$request);
@fclose($socket);
```

```php
echo("$ck:7777<br>");
if($fck>=30)
{
$kk=scandir("tmp");
for($i=0;$i<=count($kk);$i++)
{
@unlink("tmp/$kk[$i]");
}
}
?>
```

정리하자면 time함수로 타임스탬프 값이름의 tmp파일을 계속 생성하고, 업로드한 파일엔 내 ip를 적는다.
그리고 현재 timestamp값 이름의 파일을 읽어서 그 ip 7777포트로 답을 보낸다.
netcat으로 7777포트를 열고 타이밍을 맞춰서 파일을 올리면 답을 받는다.

```
C:₩Users₩Xero₩Downloads₩netcat-win32-1.12>nc.exe -l -p 7777
GET /d3eef9a21866f7383fd0b7857668123e HTTP/1.0
Host: 122.36.59.10
```

Auth에 인증하면 클리어된다.



KEY : d3eef9a21866f7383fd0b7857668123e