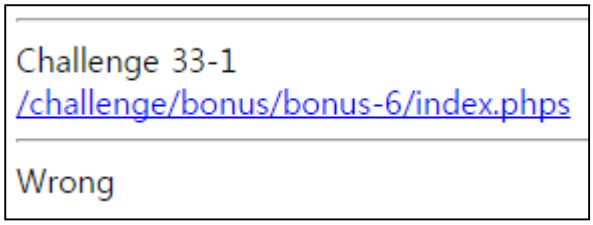
# webhacking.kr 33번문제

Xero
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)
2016-04-10
Email : wnsgurzxc@naver.com
Facebook : https://www.facebook.com/wnsgurzxc

다음과 같이 index.phps를 가르키고 Wrong을 출력한다.



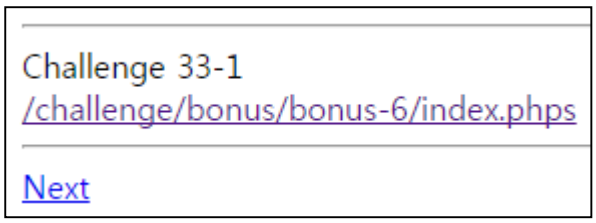

들어가보면 소스는 다음과 같다.

```php
<?
if($_GET[get]=="hehe")
{
echo("<a href=###>Next</a>");
}
else
{
echo("Wrong");
}
?>
```

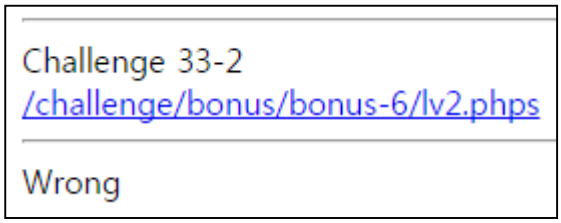
GET형식으로 get변수에 hehe값을 주면 된다.

?get=hehe

그러면 다음과 같이 Next버튼이 나온다.




Next를 누르면 다음 문제로 넘어간다.



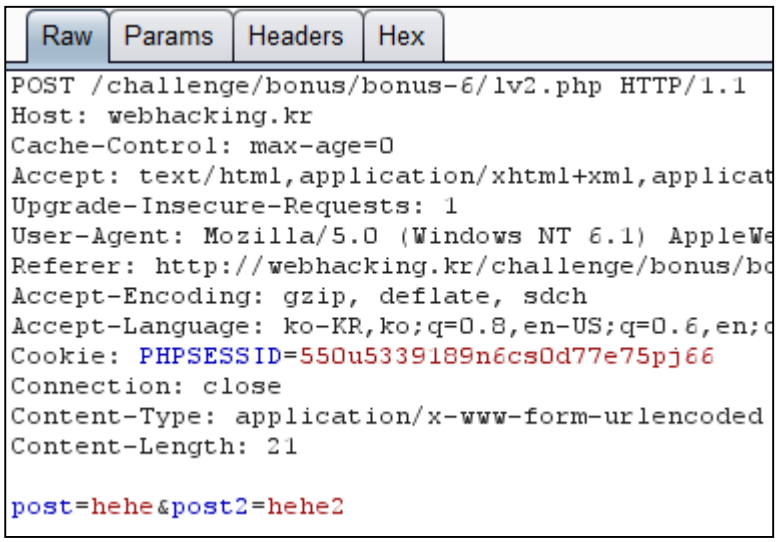
이번 소스는 다음과 같다.

```php
<?
if($_POST[post]=="hehe" && $_POST[post2]=="hehe2")
{
echo("<a href=##>Next</a>");
}
else
{
echo("Wrong");
}
?>
```

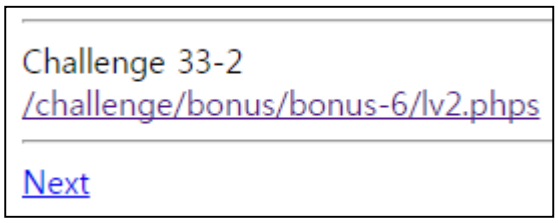
POST형식으로 post에 hehe, post2에 hehe2를 보내면 된다.

Burp Suite를 이용하여 다음과 같이 보냈다.

POST형식은 Content-Type: application/x-www-form-urlencoded 를 추가해야한다.




그러자 다음으로 넘어갈 수 있게 된다.



다음 문제이다.

Challenge 33-3
/challenge/bonus/bonus-6/33.phps

Wrong

소스를 보면 GET형식 myip에 내 ip주소를 넣으면 된다.

```php
<?
if($_GET[myip]==$_SERVER[REMOTE_ADDR])
{
echo("<a href=##.php>Next</a>");
}
else
{
echo("Wrong");
}
?>
```

ipip.kr에서 내 ip를 알아냈다.

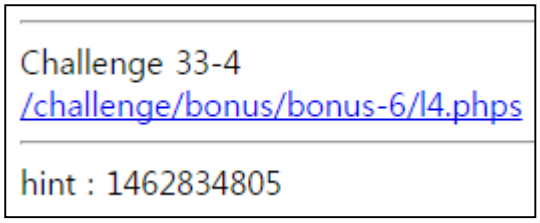

다음과 같이 보내니 통과하였다.

?myip=112.187.212.247

Challenge 33-3
/challenge/bonus/bonus-6/33.phps

Next

이번엔 hint가 있다.




소스를 보면 GET형식 password 값이 현재 시간을 타임스탬프 한 값을 md5한 것과 같으면 통과이다.

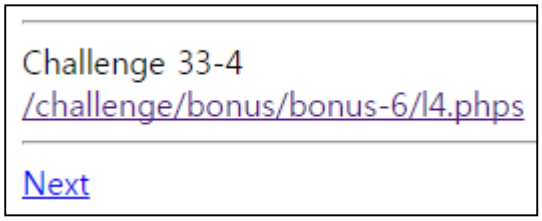
```php
<?
if($_GET[password]==md5(time()))
{
echo("<a href=###>Next</a>");
}
else
{
echo("hint : ".time());
}
?>
```

hint로 현재 타임스탬프 값을 주니 조금 뒤의 값을 미리 md5하여 password로 보내보기로 했다.

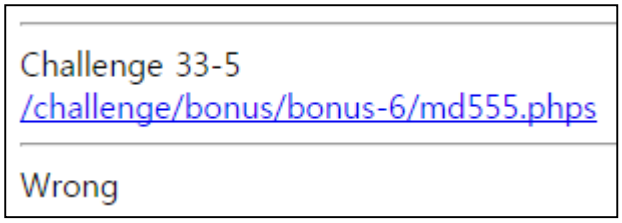
```
>>> import hashlib
>>> hashlib.md5(b'1462835100').hexdigest()
'20876d8ad16a5f39f3b29437d517bbd1'
```

다음의 값을 시간에 맞게 넣으면 통과이다.

?password=20876d8ad16a5f39f3b29437d517bbd1



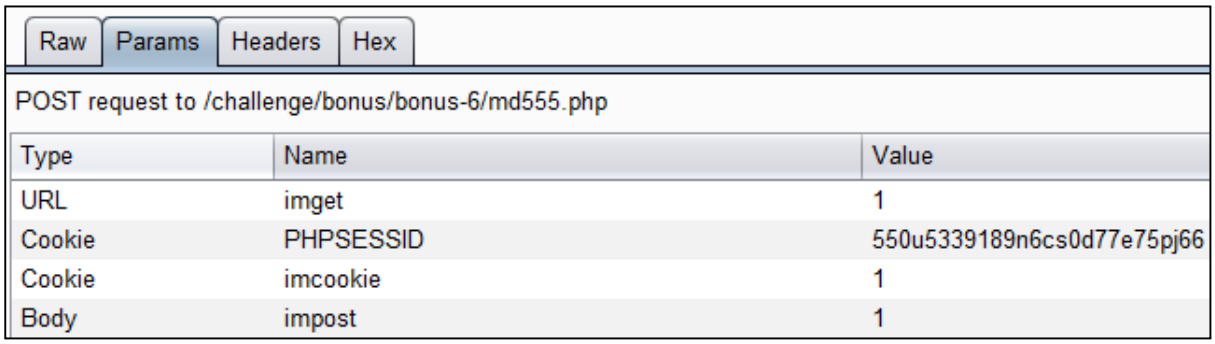
또 소스페이지를 가리킨다.



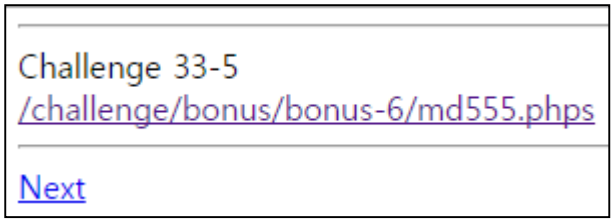

GET형식의 imget값과 POST형식의 impost값과 COOKIE로 imcookie값이 존재하면 통과이다.

```php
<?
if($_GET[imget] && $_POST[impost] && $_COOKIE[imcookie])
{
echo("<a href=###>Next</a>");
}
else
{
echo("Wrong");
}
?>
```

Burp Suite로 다음과 같이 보냈다.




그러자 통과했다.



이번문제도 hint를 준다.

Challenge 33-6
/challenge/bonus/bonus-6/gpcc.phps

hint : Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.94 Safari/537.36

COOKIE에 test값이 ip주소를 md5한 값와 같고, POST형식의 kk값이 user agent값을 md5한 값과 같다면 통과이다.

```
<?
if($_COOKIE[test]==md5("$_SERVER[REMOTE_ADDR]") &&
$_POST[kk]==md5("$_SERVER[HTTP_USER_AGENT]"))
{
echo("<a href=###>Next</a>");
}
else
{
echo("hint : $_SERVER[HTTP_USER_AGENT]");
}
?>
```

파이썬으로 코딩하였다.

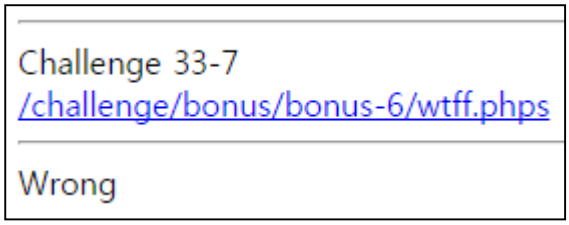
```
>>> import hashlib
>>> hashlib.md5(b'112.187.212.247').hexdigest()
'5bf2d570661eafc61e0fea9acf452385'
>>> hashlib.md5(b'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/50.0.2661.94 Safari/537.36').hexdigest()
'ba15455fccb9905222bc9a1407aad9eb'
```

각 값을 COOKIE로 test변수를 만들어서 넣고, POST로 kk변수에 보내면 된다.
그러자 통과되었다.

Challenge 33-6
/challenge/bonus/bonus-6/gpcc.phps

Next

또 소스 페이지를 보여준다.

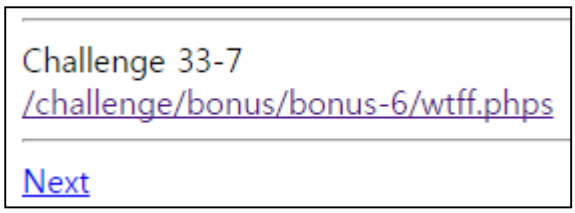



내 ip에서 .을 뺀 값을 변수이름과 값으로 보내주면 된다.

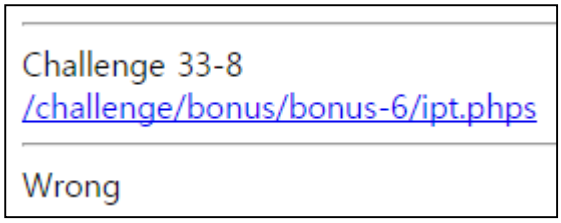
```php
<?
$_SERVER[REMOTE_ADDR]=str_replace(".","",$_SERVER[REMOTE_ADDR]);
if($_GET[$_SERVER[REMOTE_ADDR]]==$_SERVER[REMOTE_ADDR])
{
echo("<a href=###>Next</a>");
}
else
{
echo("Wrong<br>".$_GET[$_SERVER[REMOTE_ADDR]]);
}
?>
```

다음의 값을 보내면 된다.

?112187212247=112187212247



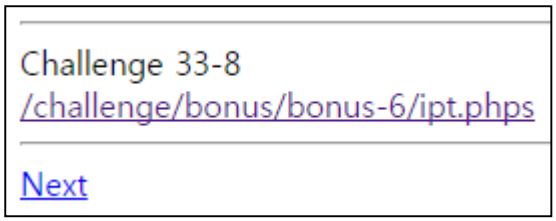
8번째 문제이다.



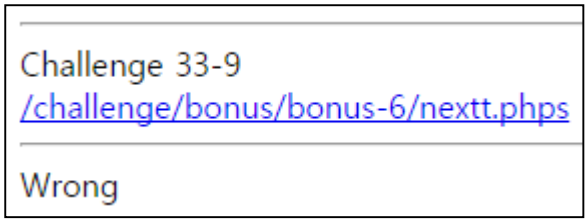

GET형식의 addr변수가 없다면 내 ip를 넣어준다.
그리고 addr변수 값이 127.0.0.1이면 통과시킨다.
addr으로 127.0.0.1을 넣어주면 될 것이다.

```php
<?
extract($_GET);
if(!$_GET[addr]) $addr=$_SERVER[REMOTE_ADDR];
if($addr=="127.0.0.1")
{
echo("<a href=###>Next</a>");
}
else
{
echo("Wrong");
}
?>
```

다음과 같이 값을 보내면 된다.
?addr=127.0.0.1



9번이다.




소스를 해석하면 a부터 z까지 answer에 더하는데 i가 2씩 증가하므로 2칸씩 건너뛰며 더하면 된다.
그 값을 GET형식으로 ans에 보내면 된다.

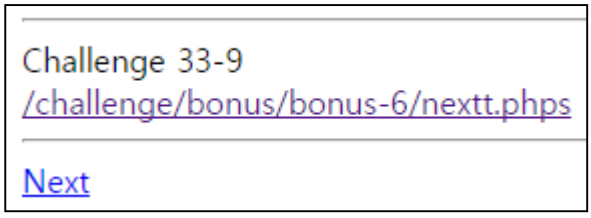
```
<?
for($i=97;$i<=122;$i=$i+2)
{
$ch=chr($i);
$answer.=$ch;
}
if($_GET[ans]==$answer)
{
echo("<a href=###>Next</a>");
}
else
{
echo("Wrong");
}
?>
```

파이썬으로 코딩하여 다음과 같은 값을 얻었다.

```
>>> sAnswer=''
>>> for i in range(97,123,2):
        sAnswer+=chr(i)

>>> sAnswer
'acegikmoqsuwy'
```

다음의 값을 보내자 통과했다.

?ans=acegikmoqsuwy



드디어 10번이다.

Challenge 33-10
/challenge/bonus/bonus-6/forfor.phps

소스는 다음과 같다.

```php
<?
$ip=$_SERVER[REMOTE_ADDR];
for($i=0;$i<=strlen($ip);$i++)
{
$ip=str_replace($i,ord($i),$ip);
}
$ip=str_replace(".","",$ip);
$ip=substr($ip,0,10);
@mkdir("answerip/$ip");
$answer=$ip*2;
$answer=$ip/2;
$answer=str_replace(".","",$answer);
$pw="###";
$f=fopen("answerip/$ip/$answer.$ip","w");
fwrite($f,"Password is $pw\n\nclear ip : $_SERVER[REMOTE_ADDR]");
fclose($f);
?>
```

다음처럼 http://phpcodepad.com/ 를 이용하였다.

<?php

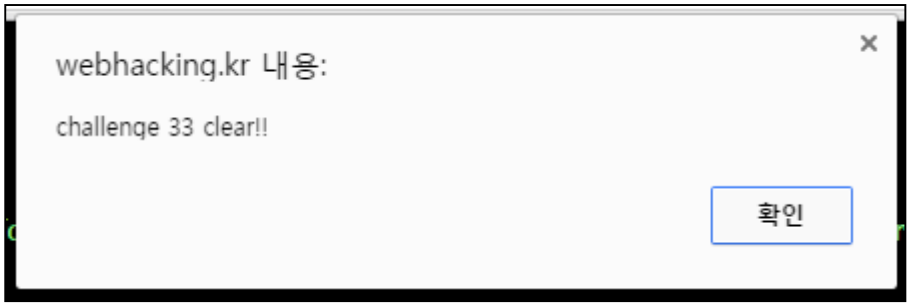
# do not start with php open tag.

```php
$ip='112.187.212.247';

for($i=0;$i<=strlen($ip);$i++)
{
$ip=str_replace($i,ord($i),$ip);
}

$ip=str_replace(".","",$ip);

$ip=substr($ip,0,10);

echo $ip.' ';

$answer=$ip*2;
$answer=$ip/2;
$answer=str_replace(".","",$answer);

echo $answer;
```

그러자 ip는 5510755107, answer는 27553775535 값이 나왔다.
소스에서 answerip/$ip/$answer.$ip 에 Password를 쓰므로 거기로 들어가면 된다.
다음의 주소로 가니 Password를 출력했다.
/answerip/5510755107/27553775535.5510755107

```
Password is ed0e7d33fde8290a3007e0526ef77a6c

clear ip : 112.187.212.247
```

Auth에 인증하면 클리어된다.




KEY : ed0e7d33fde8290a3007e0526ef77a6c