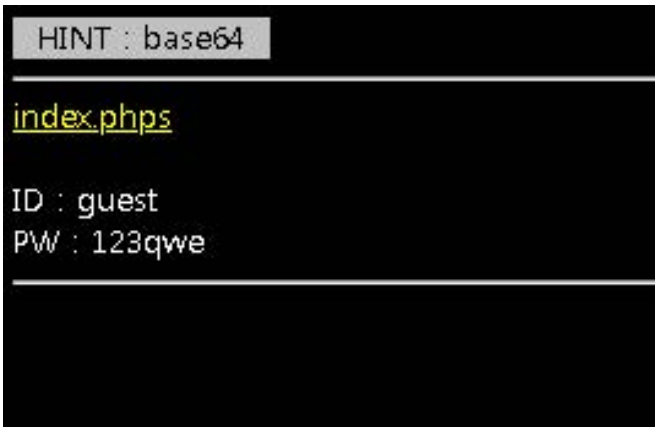
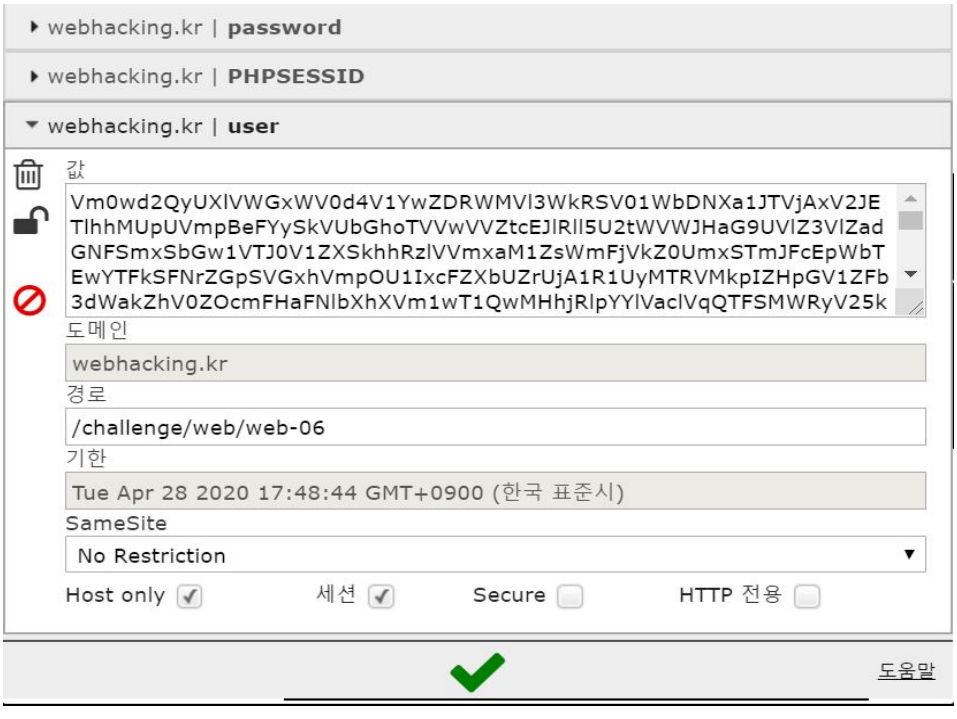


6번 문제를 보면, 처음에 index.php의 주소를 준다. 힌트로 base64를 준다.

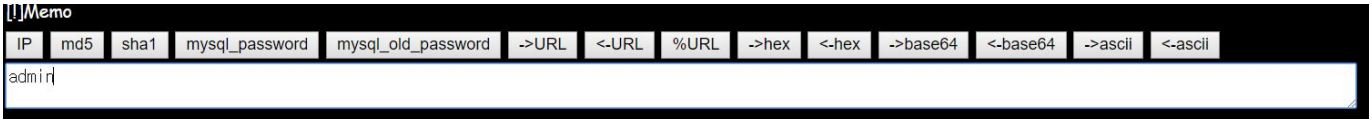
```
 Setcookie("user",$val_id);
 Setcookie("password",$val_pw);

for($i=0;$i<20;$i++)
{
    $decode_id=base64_decode($decode_id);
    $decode_pw=base64_decode($decode_pw);
}

echo("<font style=background:silver;color:black>  HINT : base64  </font><hr>
<a href=index.phps style=color:yellow;>index.phps</a><br><br>");
echo("ID : $decode_id<br>PW : $decode_pw<hr>");

if($decode_id=="admin" && $decode_pw=="admin")
{
    @solve(6,100);
}
```

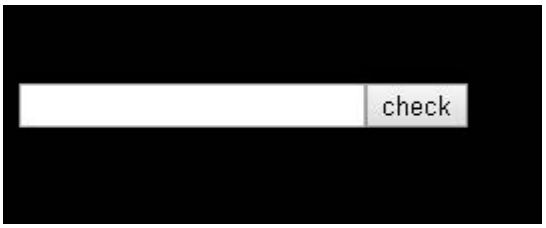
소스코드를 보면 cookie로 user와 password를 받는다는 것을 유추할 수 있다.
edit this cookie를 이용하여 본 쿠키값은 아래와 같다.



쿠키는 user값과 password를 가진다. user는 아마 guest일 것이고, password는 123qwe일 것이다. 이를 어드민으로 바꿔주자.

위의 소스코드에 의하면 base64 디코드를 20회 실행하므로, admin을 20번 인코딩한 값을 user와 password쿠키에 삽입하면 문제가 풀린다. 인코딩과 디코딩은 webhacking.kr내부에서도 지원한다.

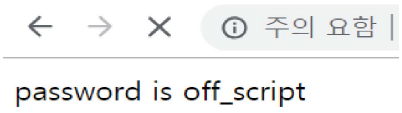




14번 문제는 처음 보면 text입력이 가능한 창과 check버튼이 있다. 소스를 보자.

```
<html>
<head>
<title>Challenge 14</title>
<style type="text/css">
body { background:black; color:white; font-size:10pt; }
</style>
</head>
<body>
<br><br>
<form name=pw><input type=text name=input_pwd><input type=button value="check" onclick=ck()></form>
<script>
function ck()
{
var ul=document.URL;
ul=ul.indexOf(".kr");
ul=ul*30;
if(ul==pw.input_pwd.value) { alert("Password is "+ul*pw.input_pwd.value); }
else { alert("Wrong"); }
}

</script>


</body>
</html>

```

url에서 .kr의 위치에 30을 곱한 값이 pw이면 성공이라고 한다.
kr의 위치는 http://webhacking.kr에서 17번째이므로 30*17 = 510답이다.



15번은...그냥 버프수트로 잡았더니 password가 나왔다

16번의 초기 형태는 이러하다. 키보드로 입력할경우 별이 하나씩 늘어난다. 소스를 보자.

```
function mv(cd)
{
kk(star.style.posLeft-50,star.style.posTop-50);
if(cd==100)
star.style.posLeft=star.style.posLeft+50;
if(cd==97) star.style.posLeft=star.style.posLeft-
50;
if(cd==119) star.style.posTop=star.style.posTop-
50;
if(cd==115)
star.style.posTop=star.style.posTop+50;
if(cd==124) location.href=String.fromCharCode(cd);
}
```

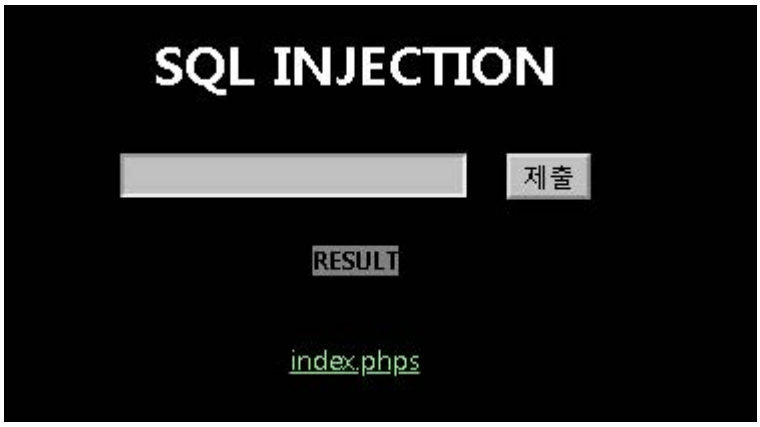
소스에는 키보드에 특정 버튼을 누를경우 별이 특정 행동을 한다하는것같다.
아스키 코드표에서 위의 숫자를 대조해보면 각각 W,A,S,D,|가 된다.
즉, 124에 해당하는 |를 누르면 정답으로 이동한다.

17번 문제의 경우 입력창과 버튼 하나가 있다. 소스를 보자.

```
<script>

unlock=100*10*10+100/10-10+10+50-9*8+7-6+5-
4*3-2*1*10*100*10*10+100/10-10+10+50-9*8+7-
6+5-4*3-2*1*10*100*10*10+100/10-10+10+50-
9*8+7-6+5-4*3-2*1*10*100*10*10+100/10-
10+10+50-9*8+7-6+5-4*3-
2*1*10/100*10*10+100/10-10+10+50-9*8+7-6+5-
4*3-2*1*10*100*10*10+100/10-10+10+50-9*8+7-
6+5-4*3-2*1*10+100*10*10+100/10-10+10+50-
9*8+7-6+5-4*3-2*1*10-100*10*10+100/10-
10+10+50-9*8+7-6+5-4*3-
2*1*10/100*10*10+100/10-10+10+50-9*8+7-6+5-
4*3-2*1*10/100*10*10+100/10-10+10+50-9*8+7-
6+5-4*3-2*1*10/100*10*10+100/10-10+10+50-
9*8+7-6+5-4*3-2*1*10/100*10*10+100/10-
10+10+50-9*8+7-6+5-4*3-
2*1*10/100*10*10+100/10-10+10+50-9*8+7-6+5-
4*3-2*1*10/100*10*10+100/10-10+10+50-9*8+7-
6+5-4*3-2*1*10/100*10*10+100/10-10+10+50-
9*8+7-6+5-4*3-2*1*10/100*10*10+100/10-
10+10+50-9*8+7-6+5-4*3-
2*1*10/100*10*10+100/10-10+10+50-9*8+7-6+5-
4*3-2*1*10*100*10*10+100/10-10+10+50-9*8+7-
6+5-4*3-2*1*10*100*10*10+100/10-10+10+50-
9*8+7-6+5-4*3-2*1*10*100*10*10+100/10-
10+10+50-9*8+7-6+5-4*3-
2*1*10*100*10*10+100/10-10+10+50-9*8+7-6+5-
4*3-2*1*10*100*10*10+100/10-10+10+50-9*8+7-
6+5-4*3-2*1*10*100*10*10+100/10-10+10+50-
9*8+7-6+5-4*3-2*1*10*100*10*10+100/10-
10+10+50-9*8+7-6+5-4*3-2*1*10+9999999999;

function sub(){ if(login.pw.value==unlock){
alert("Password is "+unlock/10); }else {
alert("Wrong");  }}
```

```
> 100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10*100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10*100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10*100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10/100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10*100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10+100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10-100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10/100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10/100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10/100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10/100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10/100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10/100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10/100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10/100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10/100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10*100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10*100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10*100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10*100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10*100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10*100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10*100*10*10+100/10-10+10+50-9*8+7-6+5-4*3-
  2*1*10+9999999999
< 9997809307
```

소스에서는 위의 식의 결과값이 비밀번호라고 한다. 그냥 크롬 콘솔창에 그대로 입력하면 콘솔에서 계산해준다.



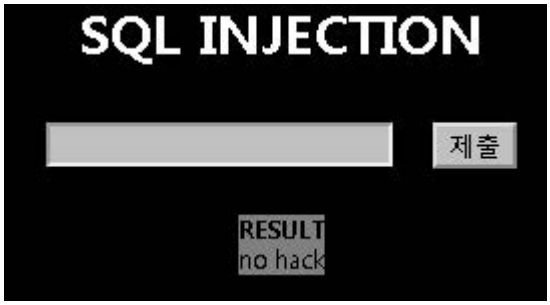
18번 문제는 대놓고 SQL INJECTION을 해달라고 한다. 우선 index.phps에 들어가보자.

```
<?
if($_GET[no])
{

if(eregi(" |/|₩(|₩)|₩t|₩||&|union|select|from|0x",$_GET[no])) exit("no hack");

$q=@mysql_fetch_array(mysql_query("select id from challenge18_table where id='guest' and no=$_GET[no]"));

if($q[0]=="guest") echo ("hi guest");
if($q[0]=="admin")
{
@solve();
echo ("hi admin!");
}

}
```

guest대신 admin을 들어가는 문제인데. 먼저 no로 guest와 admin 을 구별하는듯 보여 여러가지를 입력해본결과 1을 입력했을때 hi guest라는 문자가 뜨는것으로 확인되었다.
추측을 해보자면, admin은 0 또는 2일것이다.

webhacking.kr/challenge/web/web-32/index.php?no=0

주소창을 보면, 주소창에 대놓고 no의 입력을 보여주는 것을 알 수 있다. 여기에 sql injection을 걸어보자.
http://webhacking.kr/challenge/web/web-32/index.php?no=0 or no = 2를 입력했더니



해킹하지 말랍니다.

소스코드를 보면 SQL을 막기위해 띄어쓰기 등을 막은것을 볼 수 있는데, 막지 않은 것으로 우회해보자. \n이 막혀있지않으므로 이것으로 뚫어보자.
url encoding을 해보면 \n은 %0a이므로 모든 띄어쓰기를 \n 으로 대체해보면
http://webhacking.kr/challenge/web/web-32/index.php?no=0%0aor%0ano2이다. 주소값에 입력하면 문제가 풀린다.

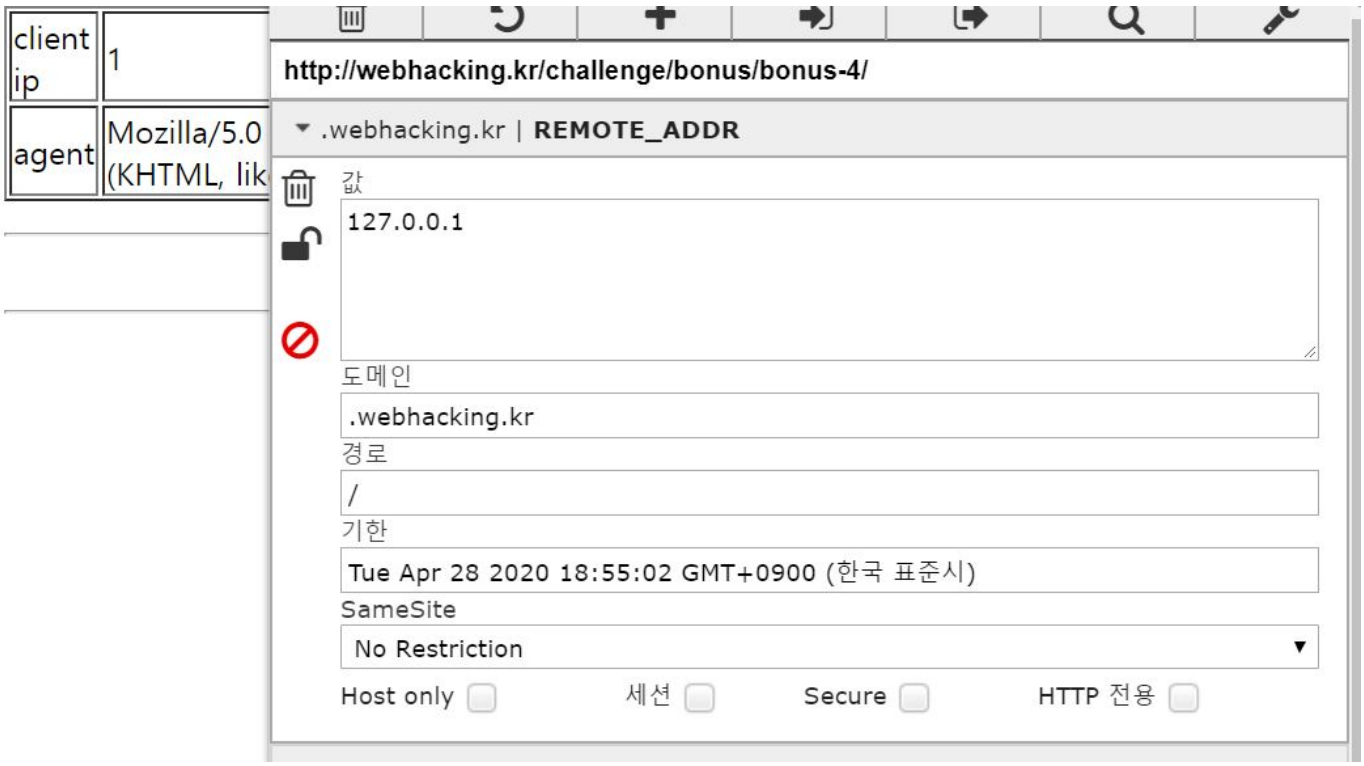
client ip	118.220.53.233
agent	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.108 Safari/537.36

Wrong IP!

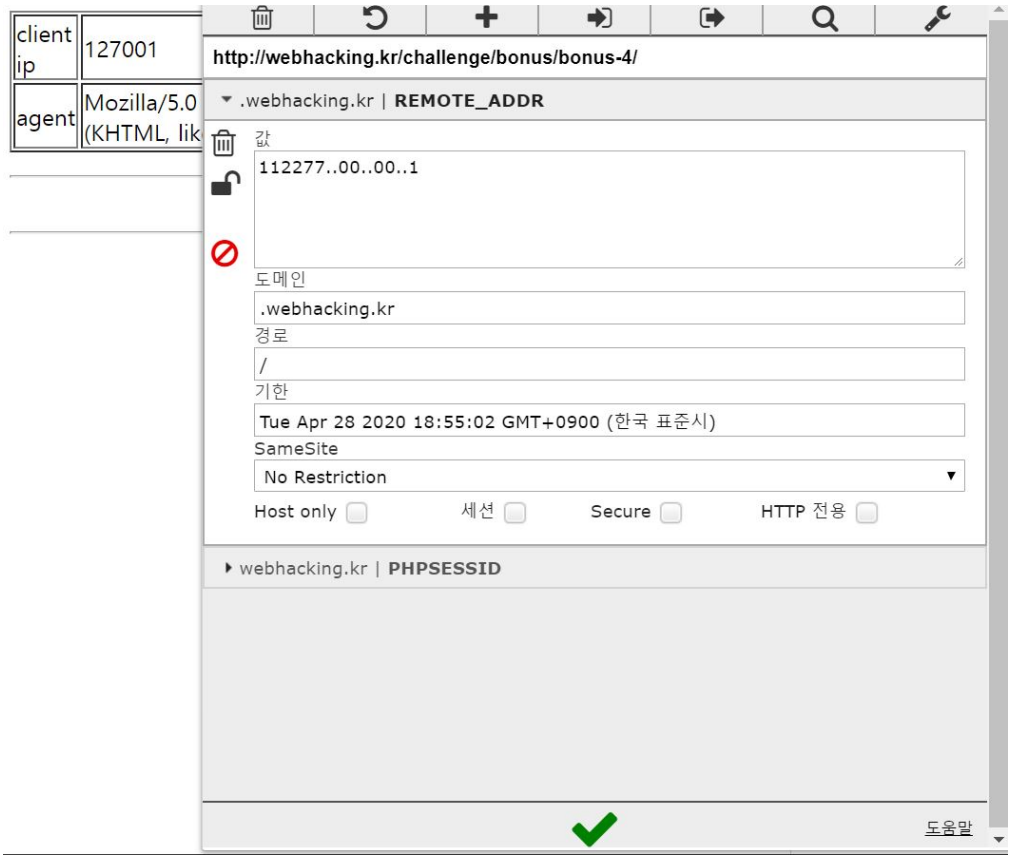
24번 문제를 처음 들어가보면 ip가 틀렸다고 한다. 소스에 index에 대한 힌트가 있어 index에 접근해보았다.

```
<?

extract($_SERVER);
extract($_COOKIE);

if(!$REMOTE_ADDR) $REMOTE_ADDR=$_SERVER[REMOTE_ADDR];

$ip=$REMOTE_ADDR;
$agent=$HTTP_USER_AGENT;


if($_COOKIE[REMOTE_ADDR])
{
$ip=str_replace("12","",$ip);
$ip=str_replace("7.","",$ip);
$ip=str_replace("0.","",$ip);
}

echo("<table border=1><tr><td>client ip</td><td>$ip</

if($ip=="127.0.0.1")
{
@solve();
}

else
{
echo("<p><hr><center>Wrong IP!</center><hr>");
}
?>
```

ip가 127.0.0.1이면 성공이라한다. 또한 ip는 cookie에서 REMOTE_ADDR로 수정이 가능하며, 쿠키값내의 12,7.,0.은 ""으로 대체된다고한다.



위와같이 입력할경우 12,7.,0.이 모두 제거되어 1만 남게된다.그럼 제거되었을때 127.0.0.1이 남을수 있도록 112277..00..00..1을 입력하면 성공적으로 ip값이 127.0.0.1로 출력된다.

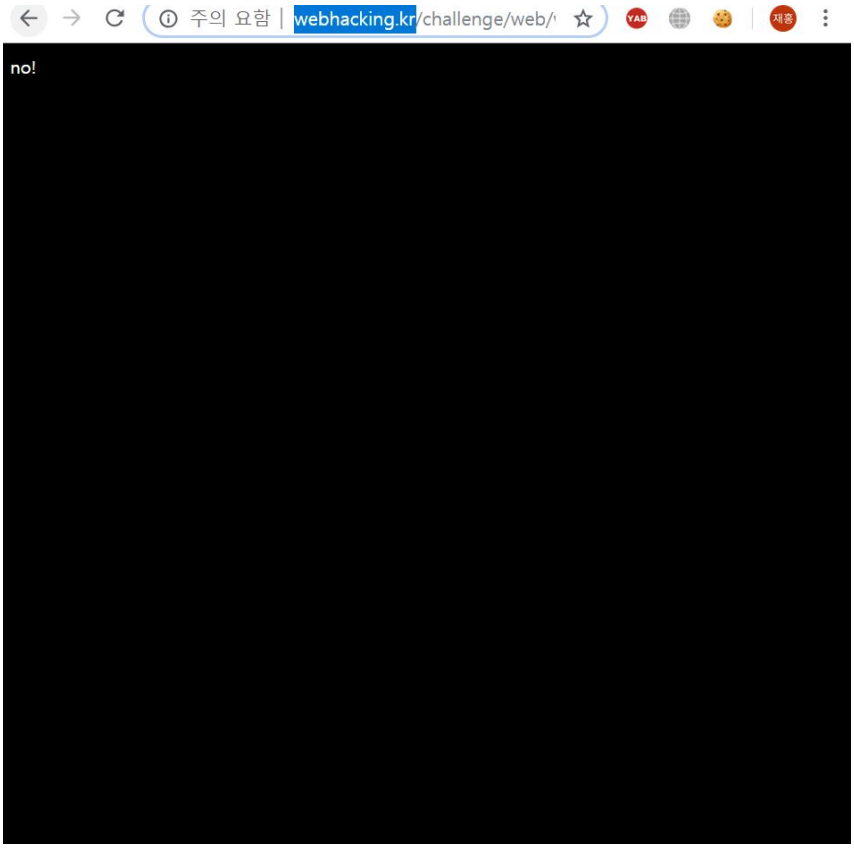


index.phps

26번은 index만 달랑 있다. 들어가보면,

```
<?

if(eregi("admin",$_GET[id])) { echo("<p>no!"); exit(); }

$_GET[id]=urldecode($_GET[id]);

if($_GET[id]=="admin")
{
@solve(26,100);
}

?>
```

다음과 같은 소스를 볼수 있다. get방식을 사용하고 있으므로, url 값을 수정하여 답을 볼수 있을 것으로 판단했다. admin이 직접 있을경우 no를 출력한다하여 url encode를 하여서 주소창에 넣었더니..



여전히 안된다고한다.
원인으로는 admin글자 체크 전에 내용을 미리 decode해버리는게 문제인것으로 판단하여, 2회 decode 한 값을 주소창에 넣었다.

LOG INJECTION

Login Admin

38번 문제는 log injection 이라고 한다.

> log
> 118.220.53.233:123

123을 친뒤 admin을 눌러보면 123이 로그에 남은것을 확인할 수 있다. 소스에 있는 힌트에 따라 admin으로 로그인해보니

LOG INJECTION

you are not admin

어드민이 아니라고한다. 로그를 보면 내가 친 문장앞에 내 ip가 입력되는것을 확인했다. 혹시나 해서 내 주소 뒤쪽에 admin을 붙여서 입력했더니 문제가 풀렸다.

LOG INJECTION

118.220.53.233:admin
Login Admin

log
118.220.53.233:123admin

jaehong13 : already solved this challenge. (38 , 100 - 2019-04-28 19:27:08)

제출

39번 문제도 소스에 index에 대한 힌트가 있어 힌트를 따라 index에 접근했다.

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

<?

$pw="????";

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();

}

?>

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

good을 입력해야하는데,위의 query문의 작은따옴표가 닫치지 않아 코드가 깨지고 있으나, 작은따옴표를 넣으려고 보니 작은따옴표를 입력하면 작은따옴표 2개로 바꿔버린다고 한다.
그러나, 인풋을 받을때 maxlength가 15이므로, good이후에 모두 공백으로 채우고 마지막에만 작은따옴표를 입력하면 추가적으로 생긴 작은따옴표는 입력 최대값을 넘어가게 되므로 작은따옴표가 한개만 입력되게 된다.

You have cleared the 39 problems.

Score + 100

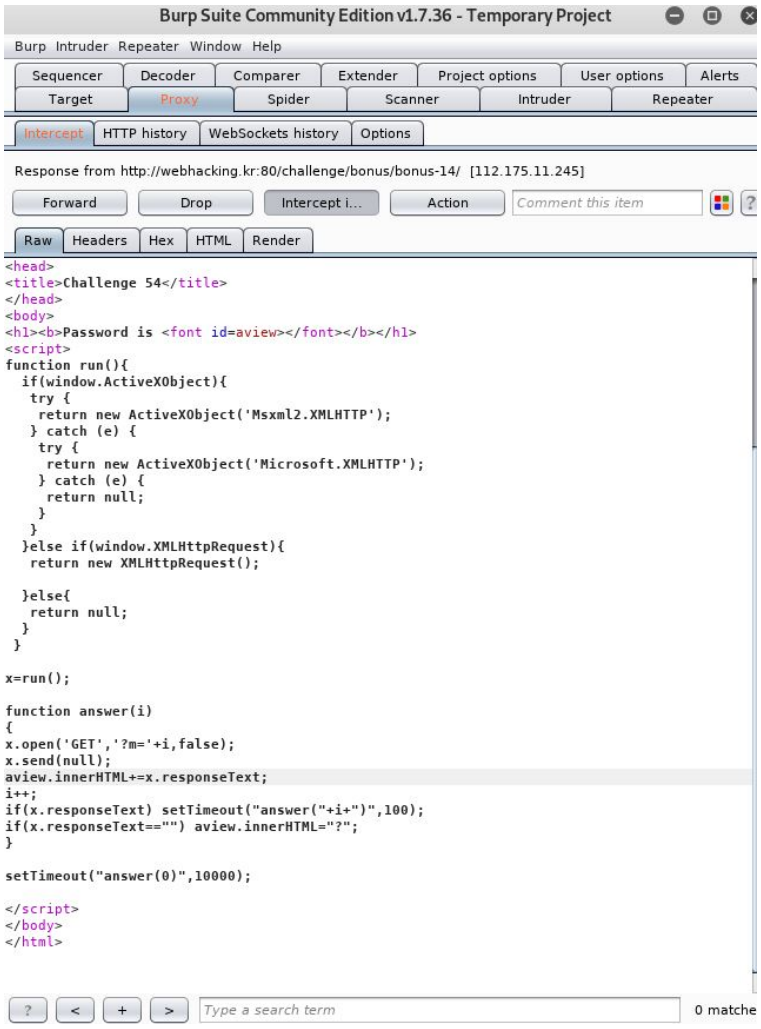
---

good 제출

Password is 3

Password is d

54번은 password is 이후 password를 한글자씩 보여준다. 눈빠지게 봐도 풀리기는 하겠다만 그러고 싶진 않으므로 버프수트를 이용하여 소스를 수정하도록 하자.



소스를 잡아서 보면 answer함수에서 한글자를 계속 바꿔가는것을 알수있다.
aview.innerhtml=x.responseText;를
aview.innerhtml+=x.responseText;로 바꾸면

Password is c3cfea

위와같이 입력되는 값이 사라지지않고 계속 추가되는것을 알수있다. 느긋하게 기다리면 답이 전부 출력된뒤 ?가 출력된다.