i春秋 “百度杯”CTF比赛 十月场 Login

原创

「已注销」 于 2018-09-17 22:04:37 发布 473 收藏

分类专栏： i春秋

友链：https://cutt.ly/7777aaaa

本文链接：https://blog.csdn.net/include_heqile/article/details/82749864

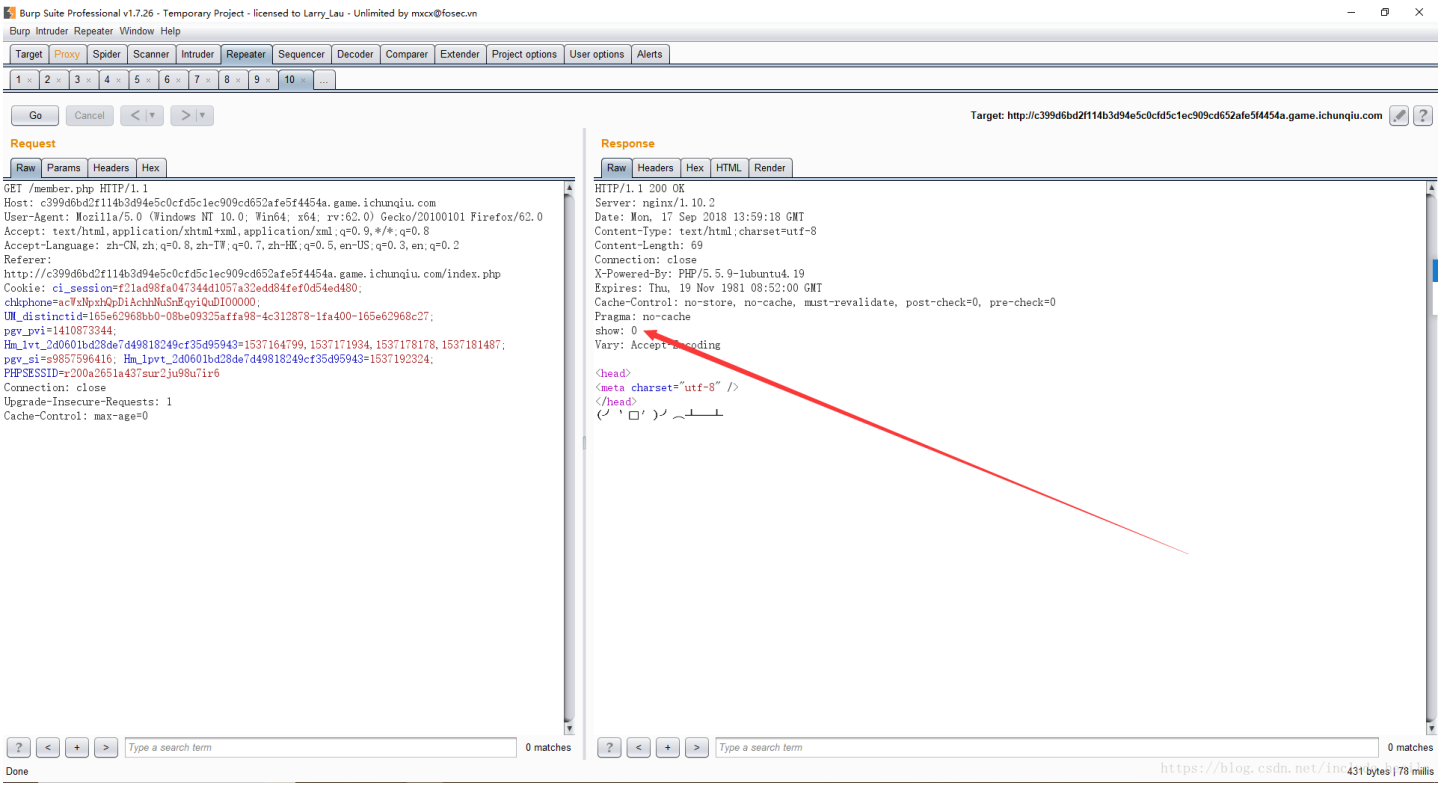
https://www.ichunqiu.com/battalion?t=1&r=0

这道题还是比较狗的

首先进入题目链接，查看源代码，发现注释掉的提示`<!-- test1 test1 -->`

使用该账号和用户名登陆进去，发现一个掀桌的表情`(ノ ' □')ノ ﾍ┻┻`

查看源代码，没有任何提示，使用`burp suite`抓包，查看`http`报头中的字段，发现一个可疑字段`show`



现在我们在自己的请求包中加上该字段。并改变它的值，尝试改成`1`，结果有重大发现，我们得到了`member.php`的源代码，查看一下代码：

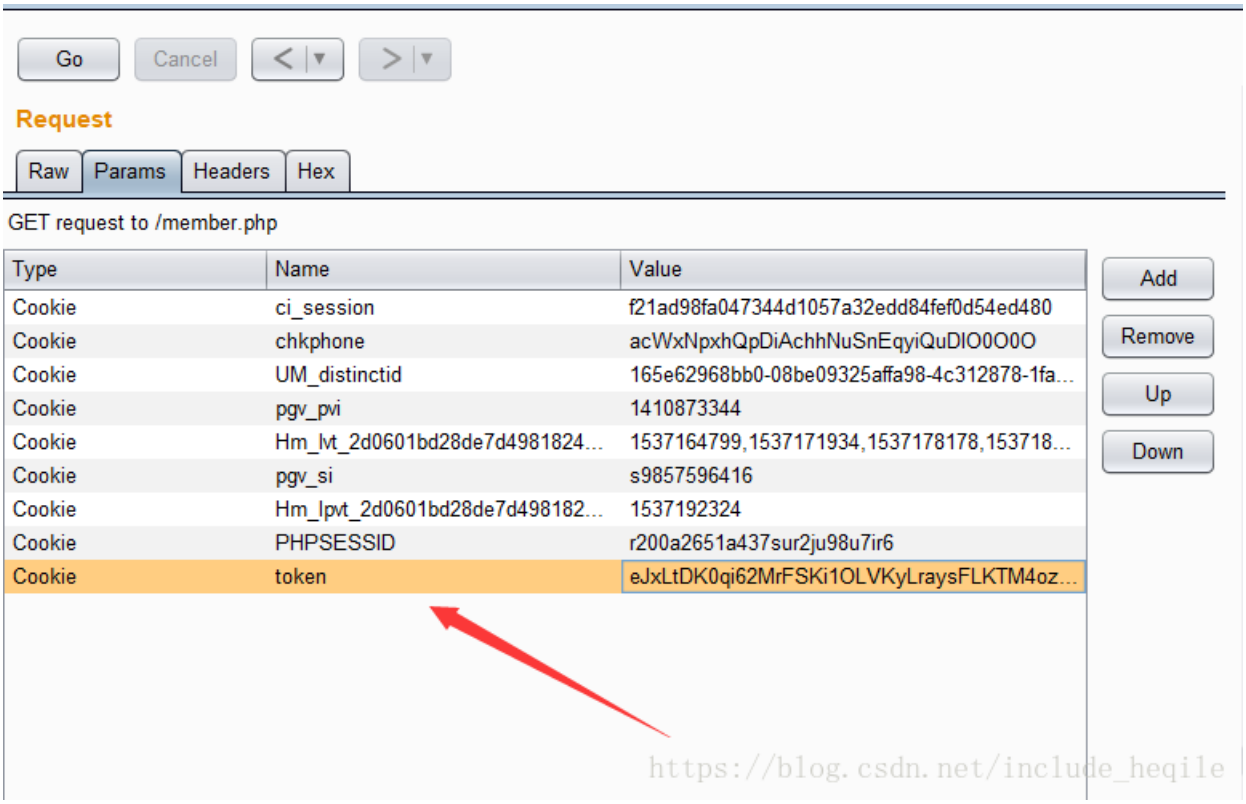
```php
<?php
 include 'common.php';
 $requset = array_merge($_GET, $_POST, $_SESSION, $_COOKIE);
 class db
 {
  public $where;
  function __wakeup()
  {
   if(!empty($this->where))
   {
    $this->select($this->where);
   }
  }

  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');
 }

?>
```

我们直接构造一个数组：

```php
$test = array("user" => "ichunqiu")
```

然后`base64_encode(gzcompress(serialize($test)))`

将得到的结果放入构造的请求中的`Cookie`的`token`字段中



这样就能得到`flag`了