

# MOCTF Web writeup（持续更新）

原创

Um0 于 2019-03-15 20:19:08 发布 449 收藏

分类专栏: [MOCTF](#) 文章标签: [ctf](#) [mocft](#) [web](#) [网络安全](#)

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\\_41358038/article/details/88582962](https://blog.csdn.net/qq_41358038/article/details/88582962)

版权



[MOCTF 专栏收录该内容](#)

3 篇文章 0 订阅

订阅专栏

## MOCTF Web writeup（持续更新）

### 1.一道水题

查看源代码, flag在最下面

### 2.还是水题

按F12打开开发者工具控制台, 选中这个文本框

请输入mocft:  提交

Wrong Answer!

```
<html>
<head>...</head>
<body>
  <form action="/.index.php" method="post">
    "
    请输入mocft:
    ...
    <input type="password" value disabled="disabled" name="password" maxlength=
    == 50
    ...
    <input type="submit" value="提交">
  </form>
  "
  Wrong Answer!
  "
</body>
</html>
```

将划横线部分删去, 将4改为5, 输入mocft, 提交一下即得flag

### 3.访问限制

打开后显示

只允许使用NAME浏览器访问!

用BP抓包，send to repeater

Target: http://119.23.73.3:5001

**Request**

```
Raw Headers Hex
GET /web3/ HTTP/1.1
Host: 119.23.73.3:5001
User-Agent: Mozilla/5.0 (Windows NT 10.0; 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
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

**Response**

```
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Date: Fri, 15 Mar 2019 12:04:36 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.14
Vary: Accept-Encoding
Content-Length: 195
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE html>
<html lang="zh-CN">
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
</head>
<body>
<center>□□□□□NAIVE□□□□□</center></body>
```

[https://blog.csdn.net/qq\\_41358038](https://blog.csdn.net/qq_41358038)

将Firefox改为NAIVE，GO一下即可

**Request**

```
Raw Headers Hex
GET /web3/ HTTP/1.1
Host: 119.23.73.3:5001
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 NAIVE/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
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

**Response**

```
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Date: Fri, 15 Mar 2019 12:06:31 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.14
Vary: Accept-Encoding
Content-Length: 206
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE html>
<html lang="zh-CN">
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
</head>
<body>
<center>Flag:
moctf{[redacted]}</center><!--By:daoyuan--></body>
```

[https://blog.csdn.net/qq\\_41358038](https://blog.csdn.net/qq_41358038)

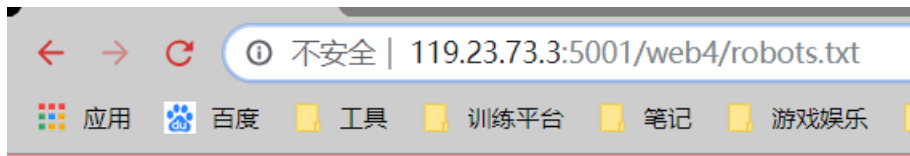
## 4. 机器蛇

打开之后是一个很无聊的小游戏，直接查看源代码，在最下面发现了一个

```
2979
2980
2981
2982
2983
```

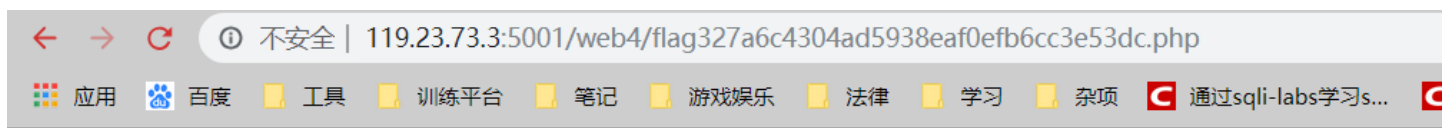
```
2984
2985 <!--robots.txt-->
2986
```

那就直接访问一下这个文件



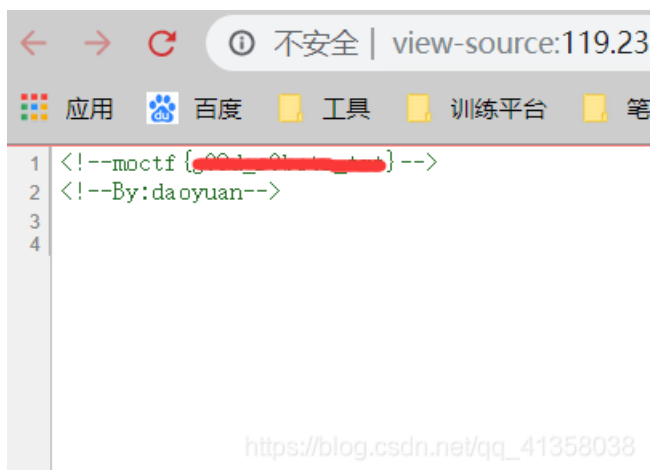
```
user-agent:
Disallow: /flag327a6c4304ad5938eaf0efb6cc3e53dc.php
Disallow: /index.html
```

再访问一下这个php文件



[https://blog.csdn.net/qq\\_41358038](https://blog.csdn.net/qq_41358038)

打开后竟是一片空白



[https://blog.csdn.net/qq\\_41358038](https://blog.csdn.net/qq_41358038)

查看一下源代码

得到flag!