

# MOCTF web writeup

原创

[NineMeet\\_111](#) 于 2019-04-27 16:49:58 发布 85 收藏

分类专栏: [信息安全](#) 文章标签: [MOCTF](#) [信息安全](#)

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/weixin\\_43862283/article/details/89555271](https://blog.csdn.net/weixin_43862283/article/details/89555271)

版权



[信息安全](#) 专栏收录该内容

14 篇文章 0 订阅

订阅专栏

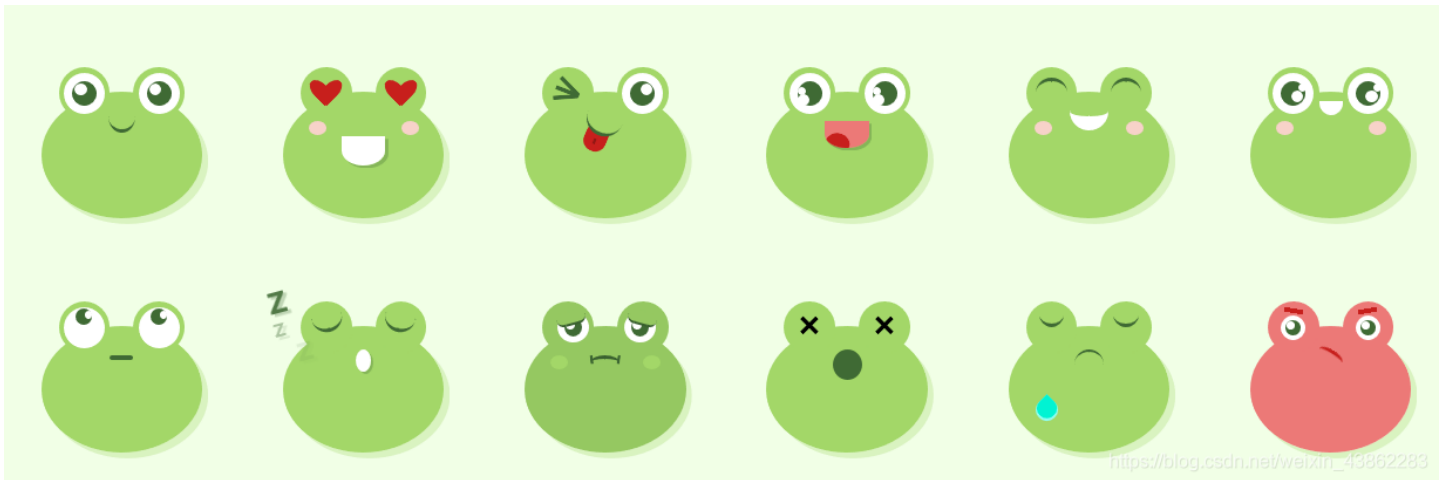
前言

今天发现一个不错的平台, 就试了试水, 写一波web题的wp  
规则:

- 1.不允许攻击比赛平台, 违者直接封IP封号处理
- 2.Flag形式为moctf{\*\*\*\*\*},如果有特殊的会在题目中说明

一道水题

打开一堆青蛙



打开源码, 搜索moctf就找到了flag了

还是水题

请输入moctf :

Wrong Answer!

发现输入框不能填写，原因是网的js代码限制了，使用开发者工具修改网页js代码



```
<head>...</head>
<body>
  <form action="./index.php" method="post">
    请输入moctf:
    <input value="" name="password" maxlength="5"
      type="password">
    <input value="提交" type="submit">
  </form>
  Wrong Answer!
  https://blog.csdn.net/weixin_43862283
```

然后在给输入框输入moctf就可以得到flag了

## 只允许使用NAIVE浏览器访问！

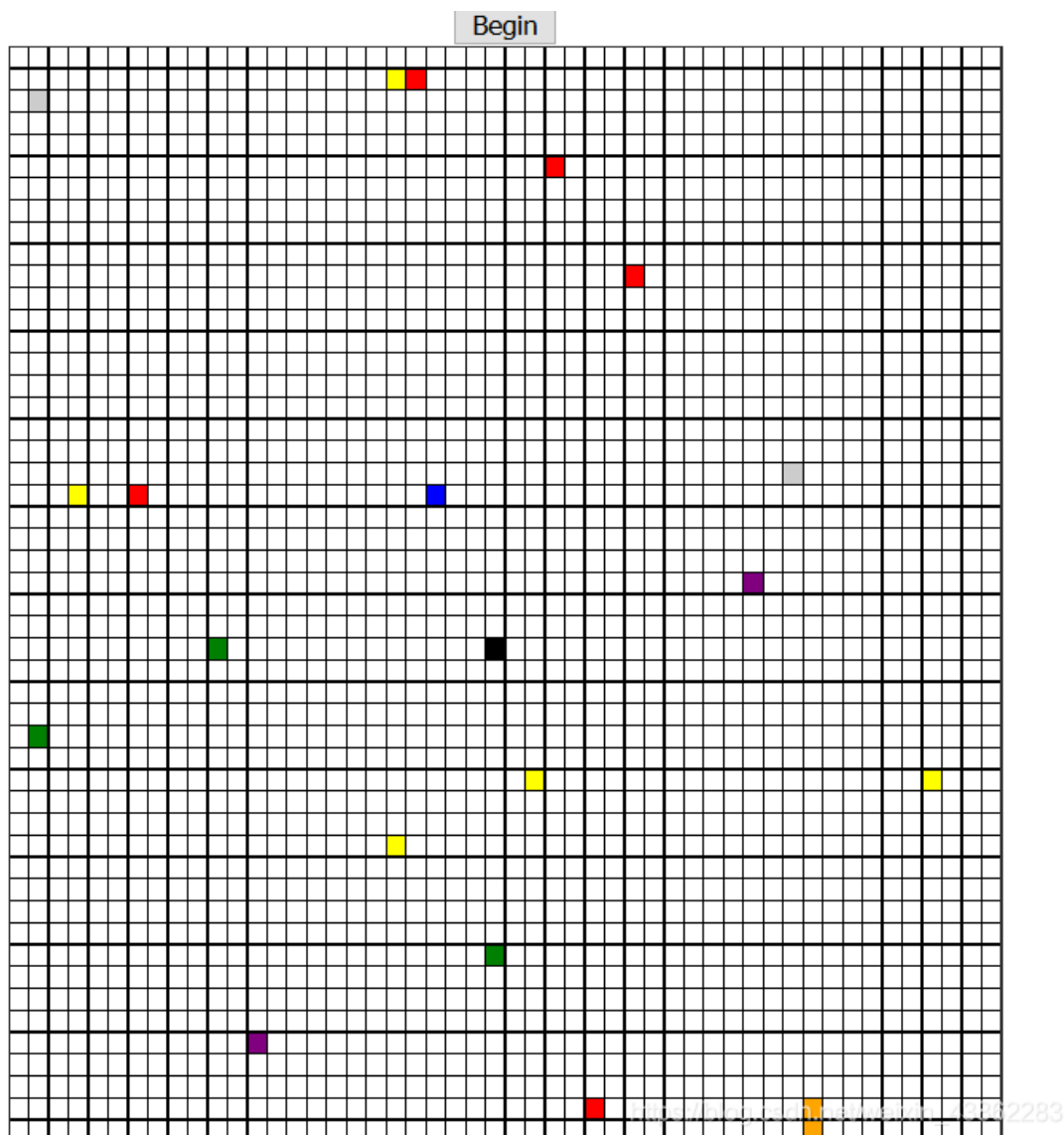
访问页面页面回显

使用BP，修改抓取到的内容

```
GET /web3/ HTTP/1.1
Host: 119.23.73.3:5001
User-Agent: NAIVE
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-HK,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.mocmf.com/challenges
Cookie: PHPSESSID=67t2icj1v9v6htmn05j16281k6
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

[https://blog.csdn.net/weixin\\_43862283](https://blog.csdn.net/weixin_43862283)

### 机器蛇



上下左右还不能用，算了，查看源码，发现有个robots.txt，访问robots.txt发现mocmf