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

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

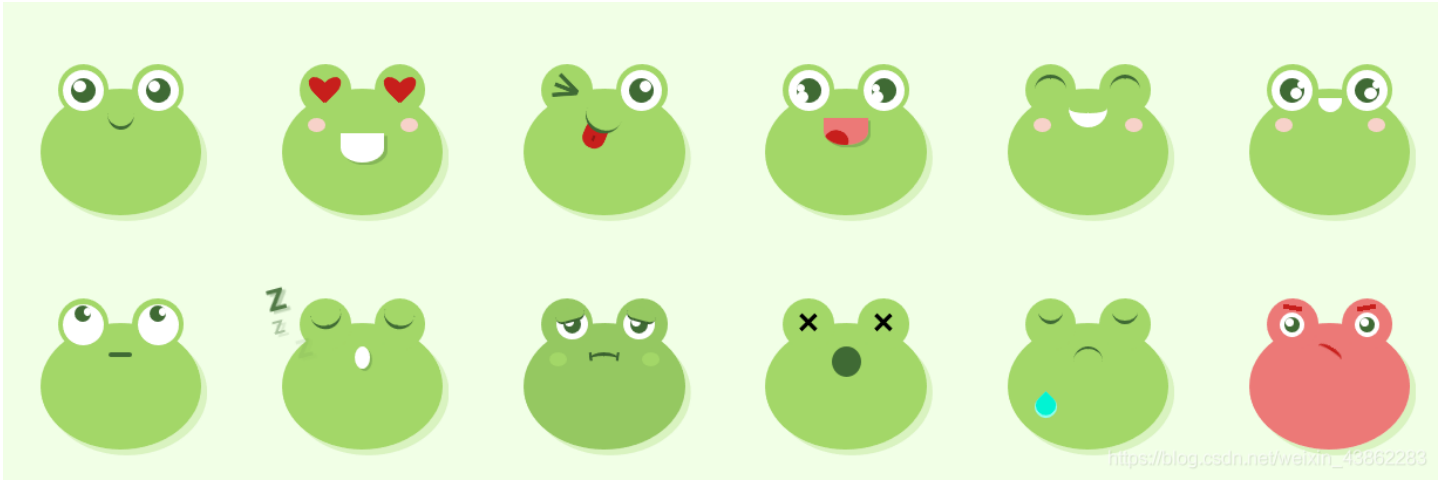
规则：

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

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

然后在给输入框输入moctf就可以得到flag了

访问限制

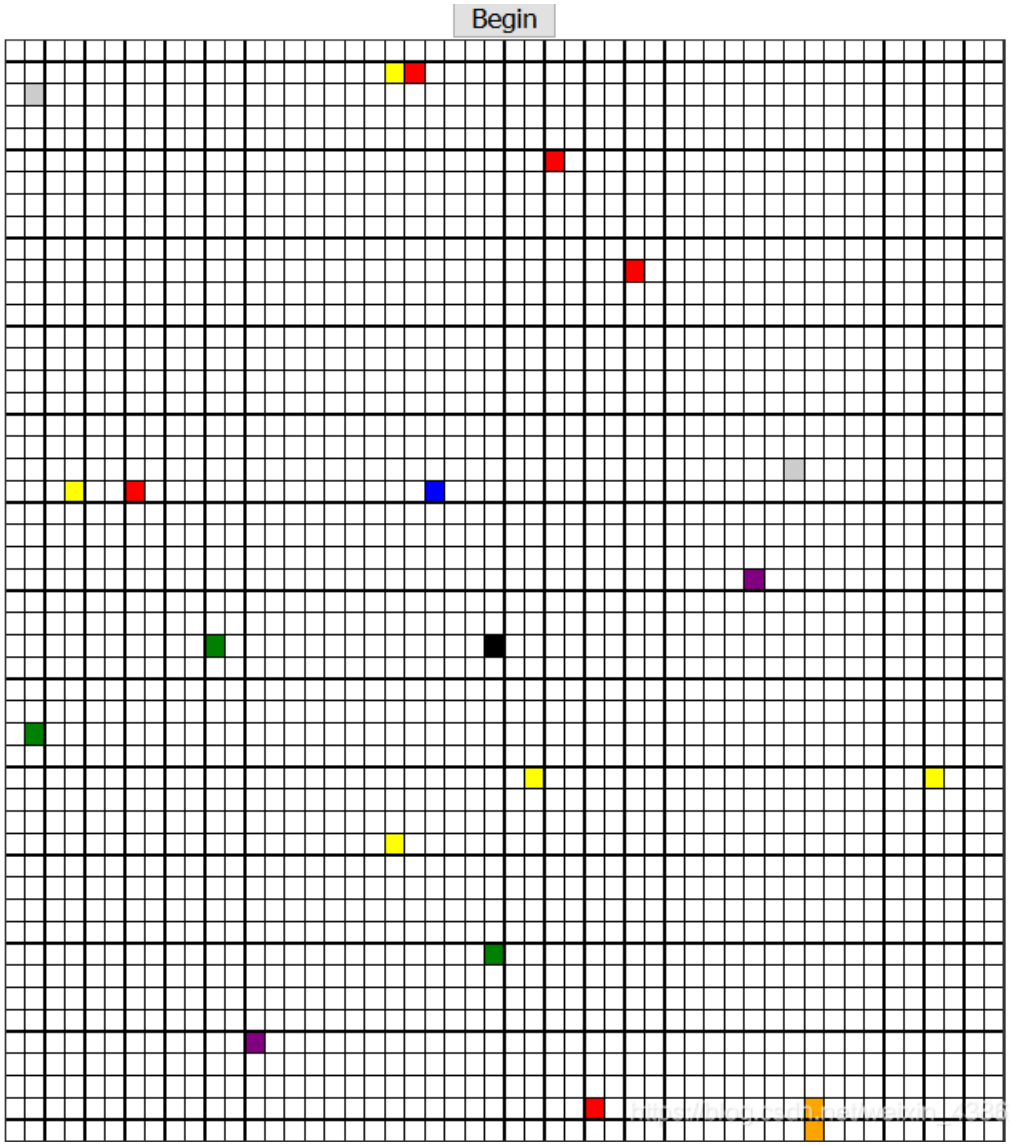
只允许使用NAIVE浏览器访问！

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.moctf.com/challenges
Cookie: PHPSESSID=67t2icj1v9v8htmn05j16281k6
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```


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moctf