

MOCTF——Web

原创

team39 于 2019-04-20 15:56:06 发布 150 收藏

分类专栏: [Web \(网页\)](#)

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/team39/article/details/89418731>

版权



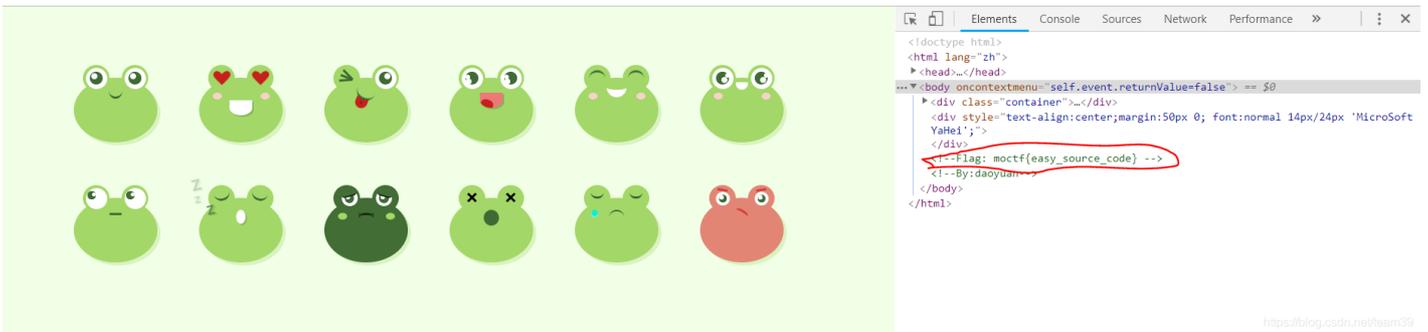
[Web \(网页\)](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

第一题: 一道水题

直接审查元素



第二题: 还是水题

观察页面, 题目要求在对话框输入moctf, 但是发现输入框不能输入, 审查元素, 发现——



disabled元素——禁用 input。被禁用的 input 元素既不可用, 也不可点击。可以设置 disabled 属性, 直到满足某些其他的条件为止 (比如选择了一个复选框等等)。

maxlength元素——限制最大输入长度为4。

所以: 把这两个属性都删除掉, 然后输入moctf, 即可。

请输入moctf: 提交

Flag: moctf{break_the_html}

```
Elements Console Sources Network >> 1 X
<html>
  <head>...</head>
  <body>
    <form action="/index.php" method="post">
      请输入moctf:
      <input type="password" value name="password">
      <input type="submit" value="提交">
    </form>
    ...
    Flag: moctf{break_the_html} == $0
    <!--By:daoyuan-->
  </body>
</html>
```

第三题：访问限制

web3/

只允许使用NAIVE浏览器访问!

<https://blog.csdn.net/team39>

用BurpSuite抓包

```
GET /web3/ HTTP/1.1
Host: 119.23.73.3:5001
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://www.moctf.com/challenges
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

<https://blog.csdn.net/team39>

因为他只能是NAIVE浏览器访问，所以就把他的User-Agent的值改成NAIVE，然后forward。

又发现

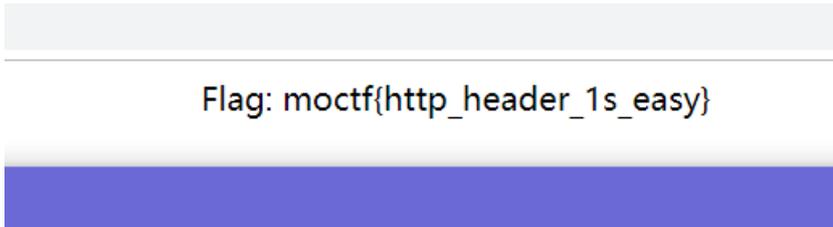
只允许香港记者访问!

再把Accept-Language的值改成zh-HK，然后forward

```
GET /solves HTTP/1.1
Host: www.moctf.com
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: NAIVE
Referer: http://www.moctf.com/challenges
Accept-Encoding: gzip, deflate
Accept-Language: zh-HK
Cookie:
session=.eJwVj8tqwzAQAH-I7NkHx49DDT0UFEQKk6EIS2hvbuwmsrwnC1tFPLvdQ9znWfUmlwcv-jeh-UyFRBH6NpmV8D6sR4n6G7w8AYdaG92Ye4r9KEh_8loHJpEKZV3lzD_Jy
wXropIhK2IkNm-RmBi9Sii3tnQL8b5RNlXpV6iPNTk97Wq_ruUyKZG9MT3Av4vkyf68DbAHxNA9ePcP8DT_dLhg.D5xZEw.URgxUMbt669PgFHsYaoINVEf2oM
Connection: close
```

https://blog.csdn.net/team39

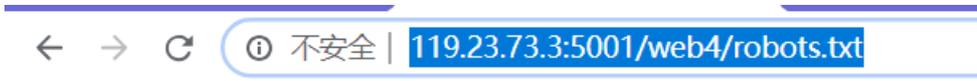
然后



第四题：机器蛇

审查元素，发现有robots.txt，于是访问119.23.73.3:5001/web4/robots.txt

https://blog.csdn.net/team39



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

发现flag327a6c4304ad5938eaf0efb6cc3e53dc.php

进去F12 找到flag

```
Elements Console Sources Network >>
<!--m0ctf{g00d_r0bots_txt}-->
<!--By:daoyuan-->
<html>
  <head></head>
  ... <body></body> == $0
</html>
```

<https://blog.csdn.net/team39>

第五题：PHP黑魔法