i春秋 WEB 象棋

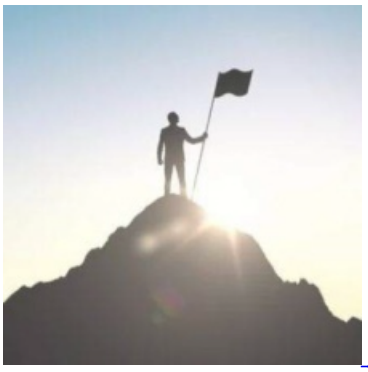
原创

A_dmins 于 2019-06-17 21:13:16 发布 789 收藏 1

分类专栏： CTF题 一天一道CTF i春秋CTF

本文链接：https://blog.csdn.net/qq_42967398/article/details/92712105

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 象棋

一天一道CTF题目，能多不能少

打开页面，一副象棋映入眼帘，玩了一会，，，太菜了，打不过人机，，，：

打开网页源代码，仔细查看一番，发现有一处CTF的字样~~：

```
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<link href="css/index.css" rel="stylesheet" type="text/css" />
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
<title>HTML5实现中国象棋游戏</title>
<link href="css/zzsc.css" type="text/css" rel="stylesheet" />
</head>
<body>

<div class="box" id="box">
    <div class="chess_left">
        <canvas id="chess">对不起，您的浏览器不支持HTML5，请升级浏览器至IE9、firefox或者谷歌浏览器! </canvas>
        <audio src="audio/click.wav" id="clickAudio" preload="auto"></audio>
        <!--<audio src="audio/check.wav" id="checkAudio" preload="auto"></audio>-->
        <audio src="audio/select.wav" id="selectAudio" preload="auto"></audio>
        <div>
            <div class="bn_box" id="bnBox">
                <input type="button" name="offensivePlay" id="tyroPlay" value="新手水平" />
                <input type="button" name="offensivePlay" id="superPlay" value="中级水平" />
                <input type="button" name="button" id="" value="大师水平" disabled />
                <!--
            <input type="button" name="offensivePlay" id="offensivePlay" value="先手开始" />
            <input type="button" name="defensivePlay" id="defensivePlay" value="后手开始" />
            -->
                <input type="button" name="regret" id="regretBn" value="悔棋" />
                <input type="button" name="bill1Bn" id="bill1Bn" value="棋谱" class="bn_box" />
                <input type="button" name="stypeBn" id="stypeBn" value="换肤" />
            </div>
        </div>
    </div>
    <div class="chess_right" id="chessRight">
        <select name="bill1List" id="bill1List">
        </select>
        <ol id="bill1Box" class="bill1_box">
        </ol>
    </div>
    <div id="moveInfo" class="move_info"> </div>
</div>
<script src="js/common.js"></script>
<script src="js/play.js"></script>
<script src="js/AI.js"></script>
<script src="js/bill1.js"></script>
<script src="js/[abcmlyx]{2}ctf[0-9]{3}.js"></script>
<script src="js/gambit.js"></script>
<div style="text-align:center;clear:both">
<p>适用浏览器：360、FireFox、Chrome、Safari、Opera、傲游、搜狗、世界之窗. 不支持IE8及以下浏览器。<br /><span style="color:red">细节决定成败</span></p>
</div>
</body>
</html>
```

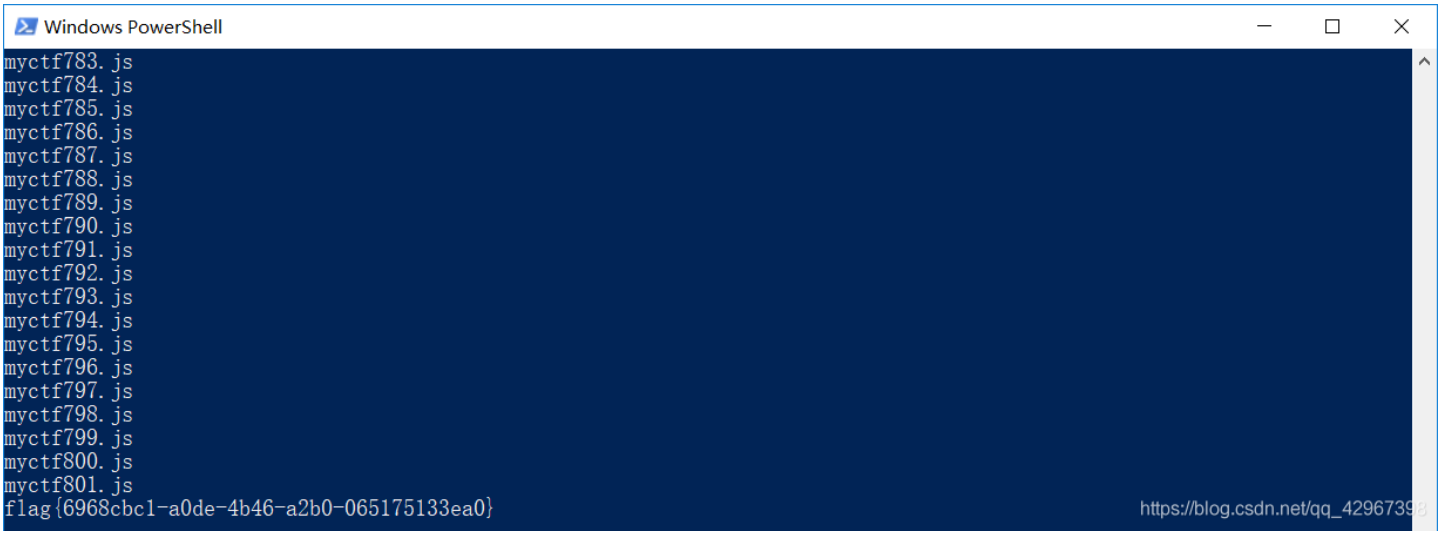

这个正则表达式嘛，第一反应是爆破这个文件叫什么名字，因为实在找不到还有啥地方不对了

（直接访问肯定是么得的，不信的可以去试试）

上脚本：

```
import requests
import base64
import sys
import hashlib

url = "http://5fe2d6ae625c466b9629c09d06e51bf8f78579f0682b43ed.changame.ichunqiu.com/js/"
key1= "abcmlyx"
key2 = "0123456789"

#这里是生成字典，，，
dic = []
for i in key1:
 for j in key1:
  for k in key2:
   for l in key2:
    for m in key2:
     key3 = i+j+"ctf"+str(k)+str(l)+str(m)+".js"
     dic.append(key3)
#print(dic)

#稍微算了一下，这样爆破真的耗时。。。。。。要是会多线程就好了，菜不能昧啊~~~

for i in range(0,len(dic)):
 res=requests.get(url+dic[i])
 print(dic[i])
 if "flag" in res.text:
  print(res.text)
  break;
```

是真的菜，这个跑了好久，建议各位兄弟还是不要使用我这个脚本了，真的慢
菜不能昧
最后跑出来的结果是/js/myctf801.js:



输入到网址，get flag：`flag{6968cbc1-a0de-4b46-a2b0-065175133ea0}`