

# i春秋象棋

转载

[weixin\\_30701575](#) 于 2019-09-04 23:07:00 发布 187 收藏

原文链接: <http://www.cnblogs.com/wosun/p/11462228.html>

版权

这是一道非常有意思的一道题，打开后就是一个pve的象棋游戏，我觉得下赢了就应该会出现flag，可惜多次尝试后失败了（果真有点厉害，我一时兴起就玩了好几把，有空试试拿更厉害的电脑跟他对下，如果赢了会怎么样）

不说象棋游戏了，我们来做这道题，首先是不可能通过下赢来获取flag的，他会自动挑战大师水平，尽管我选的新手。。。（我菜）



让另一个电脑大师级的和他对下，终于赢了（全程看不懂），但还是没flag。。。

查看源码发现js中有关键内容

```
<script src="js/common.js"></script>
<script src="js/play.js"></script>
<script src="js/AI.js"></script>
<script src="js/bill.js"></script>
<script src="js/[abcnlyx]{2}ctf[0-9]{3}.js"></script>
<script src="js/gam216.js"></script>
<div style="text-align:center;clear:both">
```

这里的文件都是js/巴拉巴拉的，所以很明显这是一个正则表达式，百度传送门：

<https://baike.baidu.com/item/%E6%AD%A3%E5%88%99%E8%A1%A8%E8%BE%BE%E5%BC%8F/1700215?fr=aladdin>

这里附上一个py脚本爆破正则表达式（源码链接：<https://www.ichunqiu.com/writeup/detail/781>）

```
#!/usr/bin/python
# coding=utf-8
# Author=haya
import urllib2
from multiprocessing.dummy import Pool as ThreadPool
urllist = []
re1 = 'myx'
re2 = '012346789'
url = 'http://ffffe6af593794c94834b881524ab1aa9f63ccb660b0648a2.changame.ichunqiu.com/js/'
pool = ThreadPool()
def url_list():
    for i in re1:
        for j in re1:
            for k in re2:
                for l in re2:
                    for m in re2:
                        urllist.append(url+i+j+'ctf'+k+l+m+'.js')
    return urllist

def url_open(url):
    try:
        result = urllib2.urlopen(url).read()
        if '404' not in result:
            print url+result
    except:
        pass

def main():
    urllist = url_list()
    pool.map(url_open, urllist)
    pool.close()
    pool.join()

if __name__ == '__main__':
    main()
```

运行就可以爆破出js文件也就是flag

```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 10.0.17134.950]
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\七星>cd desktop

C:\Users\七星\Desktop>python l.py
http://e4c7cecd0f524e1cb7deea781a85ebf547e3d4aff3124966.changame.ichunqiu.com/js/myctf801.jsflag{43f1c719-47d8-4a8d-9ba1-4f1a832eaf50}

C:\Users\七星\Desktop>python l.py
http://fff66af593794c94834b881524ab1aa9f63ccb660b0648a2.changame.ichunqiu.com/js/myctf801.jsflag{1a4a4de6-036d-4ec0-893b-856r2811e945}

C:\Users\七星\Desktop>
```

转载于:<https://www.cnblogs.com/wosun/p/11462228.html>