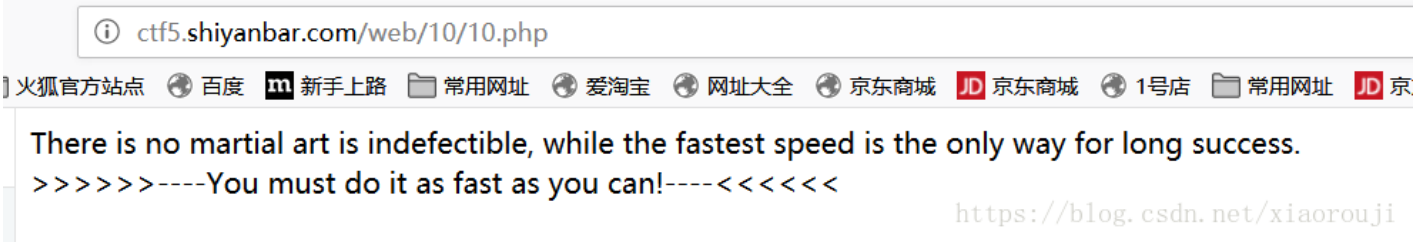
天下武功唯快不破-实验吧

原创

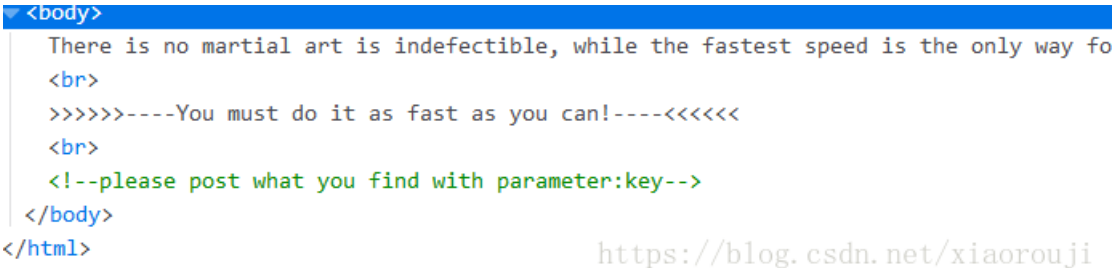
Xi4or0uji 于 2018-05-08 21:33:40 发布 4239 收藏
分类专栏： ctf

点开看见



然后题目暗示看看响应头，结果看到flag

感觉就是base64加密，然后解密，这个时候看下页面代码还有这句



所以题目就是想要我们去拿到header的flag，base64解密，然后再在url传key

同时还发现，传过来的flag是个随机值.....手动解密是不够时间的了，只能借助脚本的力量了

```
#coding:utf-8
import requests,base64
url="http://ctf5.shiyanbar.com/web/10/10.php"
t = requests.get(url)
flag = t.headers['FLAG'] #拿到响应头的flag
flag = base64.b64decode(flag) #base64解密
flag = flag.decode() #这里还有个decode是因为要把它从bytes型转成string型
flag = flag.split(':')[1] #取后面flag的部分
data = {'key':flag} #构造key
re = requests.post(url,data=data).content #制造请求报文，发送请求
print(re)
```

然后就能拿到flag了