BugKu-web-速度要快 writeup

原创

MoonBack明月归 于 2019-06-15 15:49:37 发布 521 收藏 1

分类专栏： BugKu 文章标签： BugKu CTF web

本文链接：https://blog.csdn.net/weixin_43826194/article/details/91904535

题目网址

```
http://123.206.87.240:8002/web6/
```

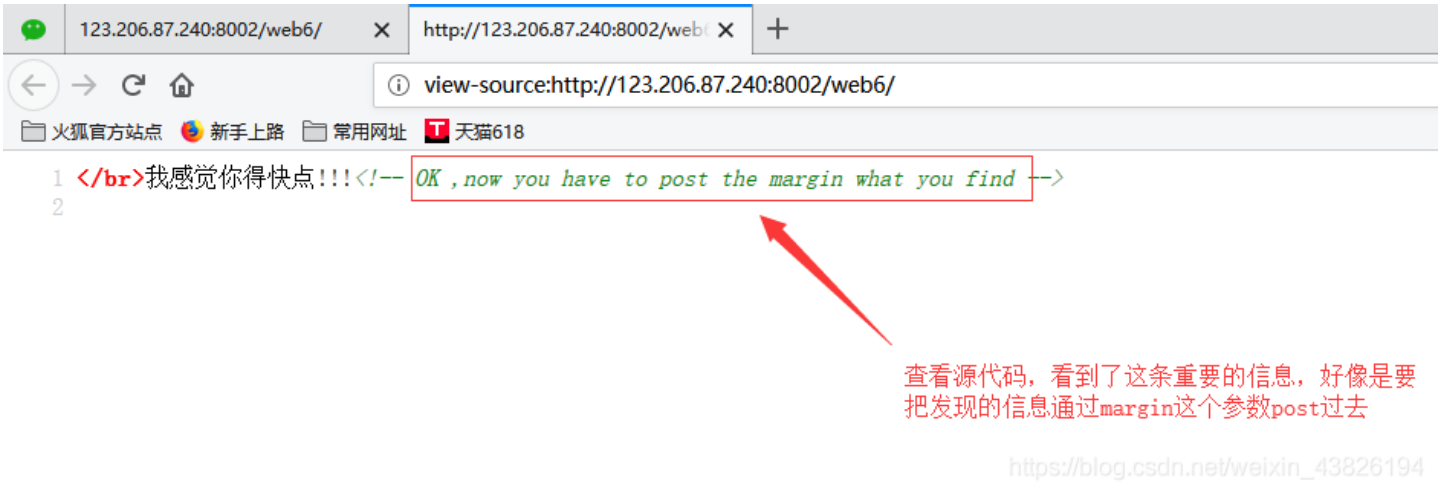
我感觉你得快点!!!

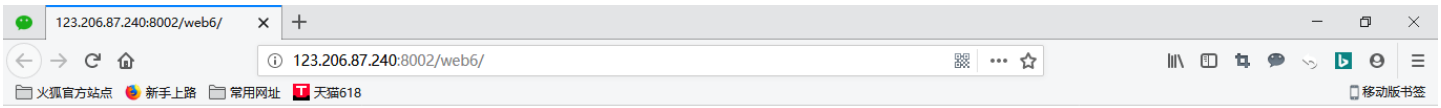
题解

方法

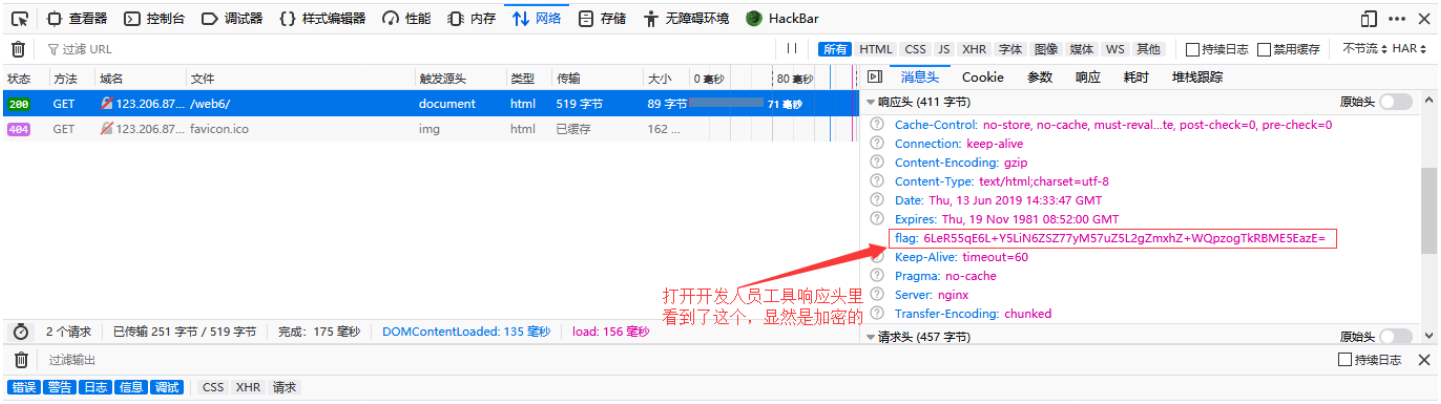
```
解密发现的重要信息，post过去
```

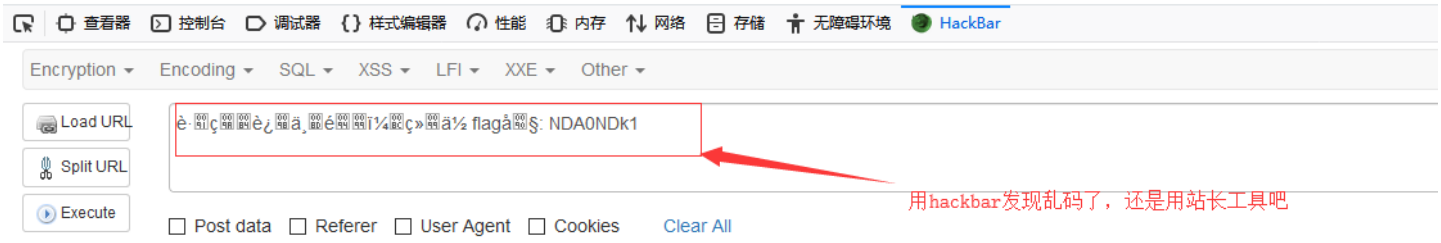
图解





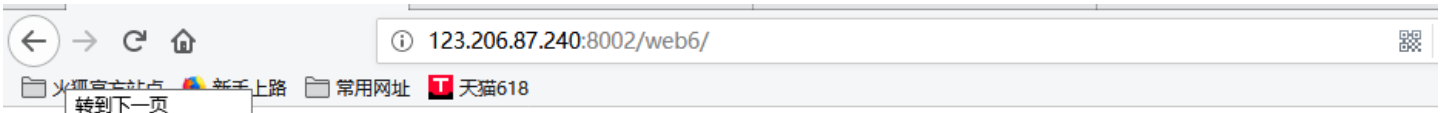
我感觉你得快点!!!



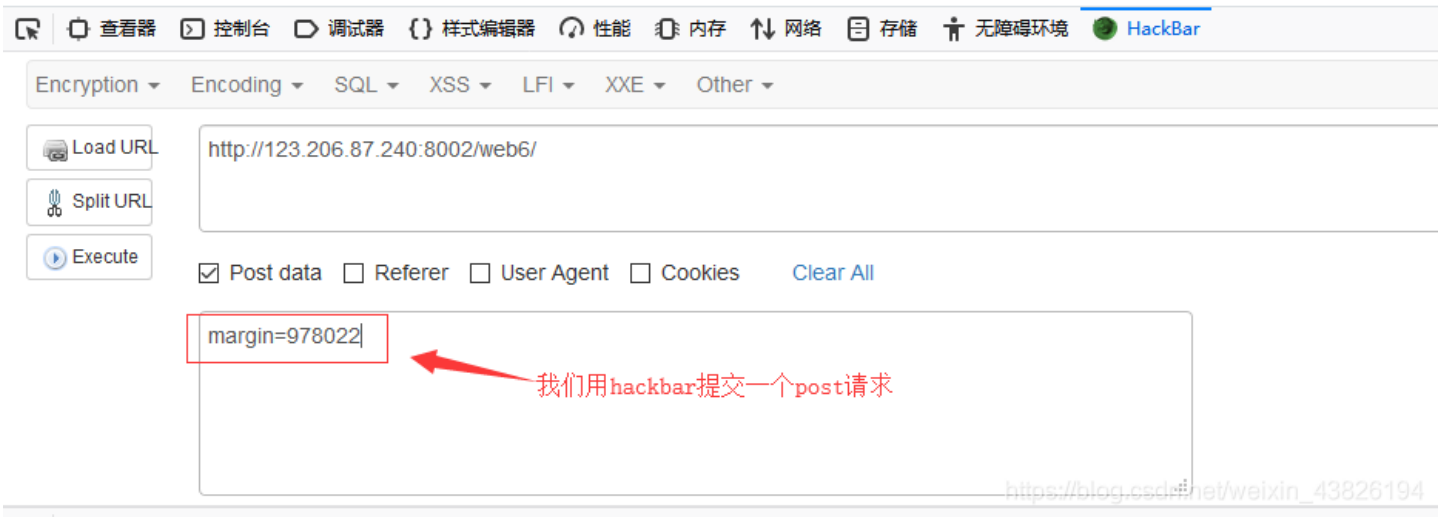



跑的还不错，给你flag吧: OTc4MDIy
6LeR55qE6L+Y5LiN6ZSZ77yM57uZ5L2gZmxhZ+WQpzogT1RjNE1ESXk=
1. 查询资料发现是base64加密的
2. 解密结果，但这个结果好像还是用base64加密的，别问我为啥
多行
Base64加密
Base64解密
清空结果


文字加密解密
MD5加密/解密
URL加密
JS加/解密
JS混淆加密压缩
ESCAPE加/解密
BASE64
散列/哈希
迅雷，快车，旋风URL加解密
978022
OTc4MDIy
再解密，发现这一串数字，显然没有加密信息了
多行
Base64加密
Base64解密
清空结果


123.206.87.240:8002/web6/
常用网址
天猫618
转到下一页
右击或下拉显示历史

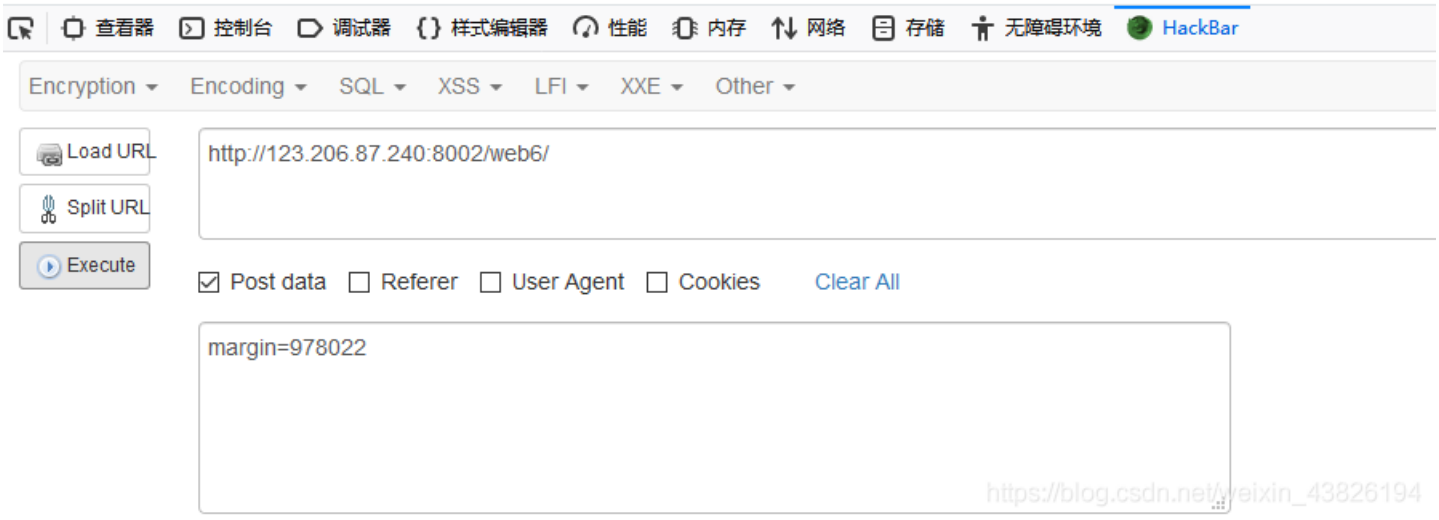
我感觉你得快点!!!

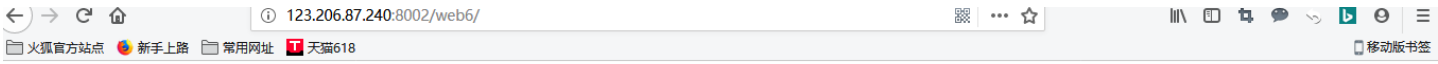

查看器
控制台
调试器
样式编辑器
性能
内存
网络
存储
无障碍环境
HackBar
Encryption
Encoding
SQL
XSS
LFI
XXE
Other
Load URL
Split URL
Execute
http://123.206.87.240:8002/web6/
Post data
Referer
User Agent
Cookies
Clear All
margin=978022
我们用hackbar提交一个post请求


123.206.87.240:8002/web6/
火狐官方站点
新手上路
常用网址
天猫618

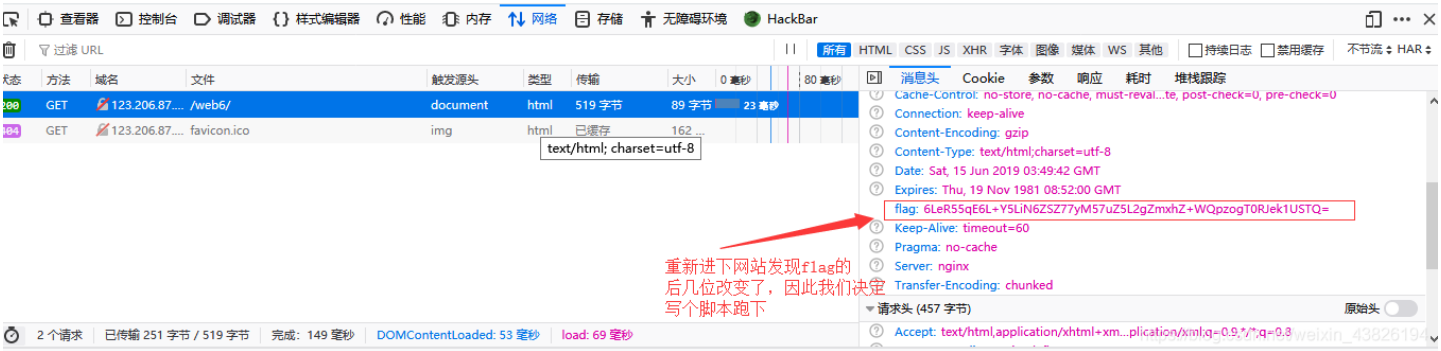
我都说了让你快点。。。
我感觉你得快点!!!

多出来这个提示信息，是哪里出现问题了那？





我感觉你得快点!!!



重新进下网站发现flag的后几位改变了，因此我们决定写个脚本跑下

```python
import requests
import base64
s=requests.session()
#requests库的session会话对象可以跨请求保持某些参数
r=s.get("http://123.206.87.240:8002/web6/")
# print(r.headers)
#flag在header里
aaa=r.headers['flag']
flag=base64.b64decode(r.headers['flag']).decode().split(": ")[-1]
#base64解密
# print(flag)
flag1=base64.b64decode(flag).decode()
#base64再解密
# print(flag1)
dic={"margin":flag1}
tr=s.post("http://123.206.87.240:8002/web6/",data=dic)
#post参数
print(tr.text)
```

```
D:\Python\python.exe D:/Py/Pycharm/bugku/webspeed.py
KEY{111dd62fcd377076be18a}

进程已结束，退出代码 0
```

成功解题