Bugku web19 writeup

原创

5mack 于 2021-04-25 20:50:55 发布 29 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/Code_Aape/article/details/116137891

Bugku web19 writeup

题目描述

速度要快！

打开网页只有一句话：我感觉你得快点!!!

分析

和上一道秋名山一样，又是GKD的题，是不是又要用脚本做啊

尝试1

国际惯例先按F12，html代码注释里面有一句（OK ,now you have to post the margin what you find）。margin，难道是CSS的margin吗

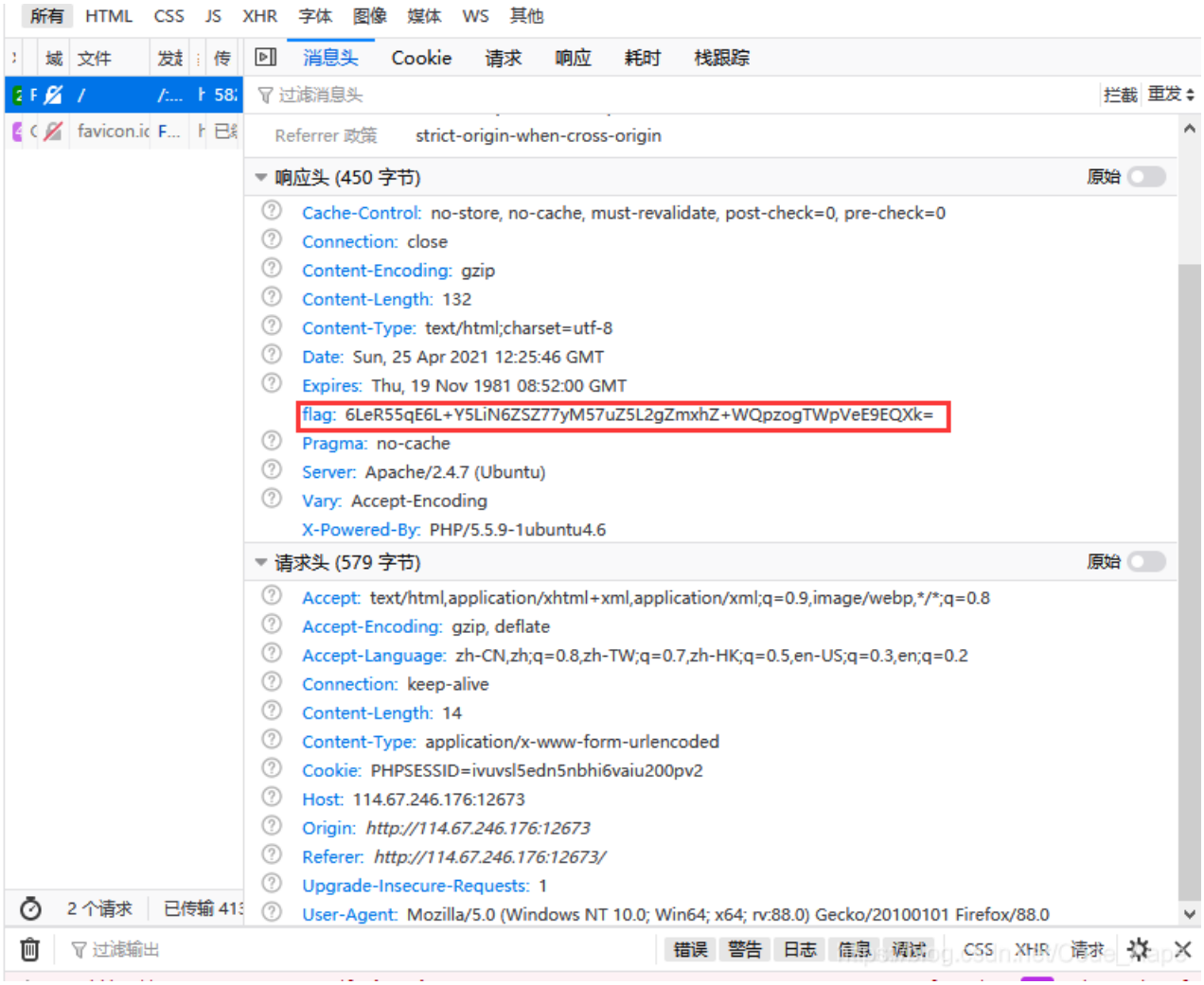
果然没那么简单，用hackbar试着post `margin=8`：

页面：我都说了让你快点。。。我感觉你得快点!!!

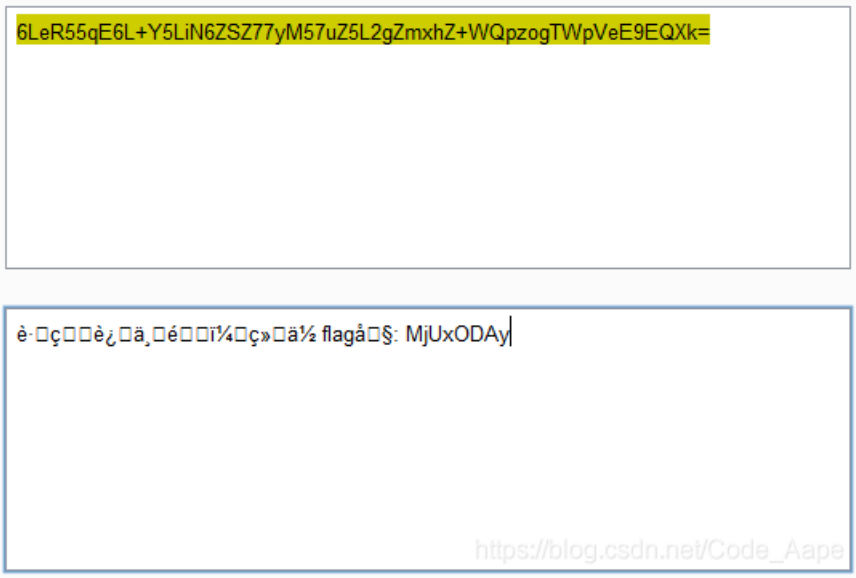
试着post其他margin值，效果一样，果然没有8这个值什么事

尝试2

看看消息头呢：



响应头里面有个flag字段，看起来是base64，解码一下：



看起来冒号后面有串非乱码的字符串，也是base64，再解码：251802

> margin：[名词]页边空白;白边;(获胜者在时间或票数上领先的)幅度，差额，差数;余地;备用的时间。
> 看意思，margin肯定是数字

这个应该就是需要的margin值，post一下。果不其然，还是让我搞快点

刷新页面，header的flag后面的值一直在变，那就脚本呗

```
import requests
import base64

sessions = requests.session()
url = 'http://114.67.246.176:12673/'
flagheader = sessions.post(url).headers['flag']
flag_first_decode = base64.b64decode(flagheader).decode()
margin = base64.b64decode(flag_first_decode.split(":")[1].strip()).decode()
flag = sessions.post(url, data={'margin': margin}).text
print(flag)
```

得到flag