

速度要快-writeup

打开题目

Challenge

1740 Solves

×

速度要快
100

速度要快!!!!!!

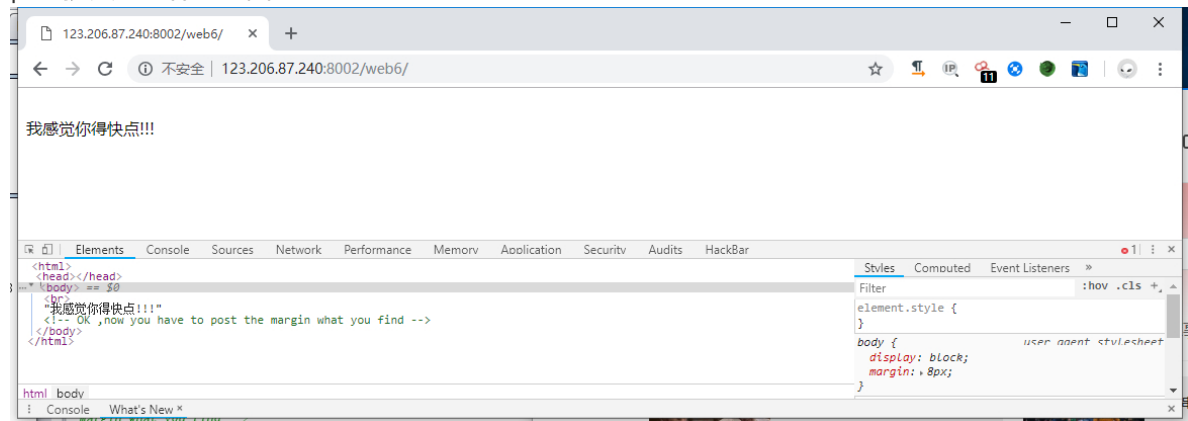
<http://123.206.87.240:8002/web6/>

格式KEY{xxxxxxxxxxxxxxxx}

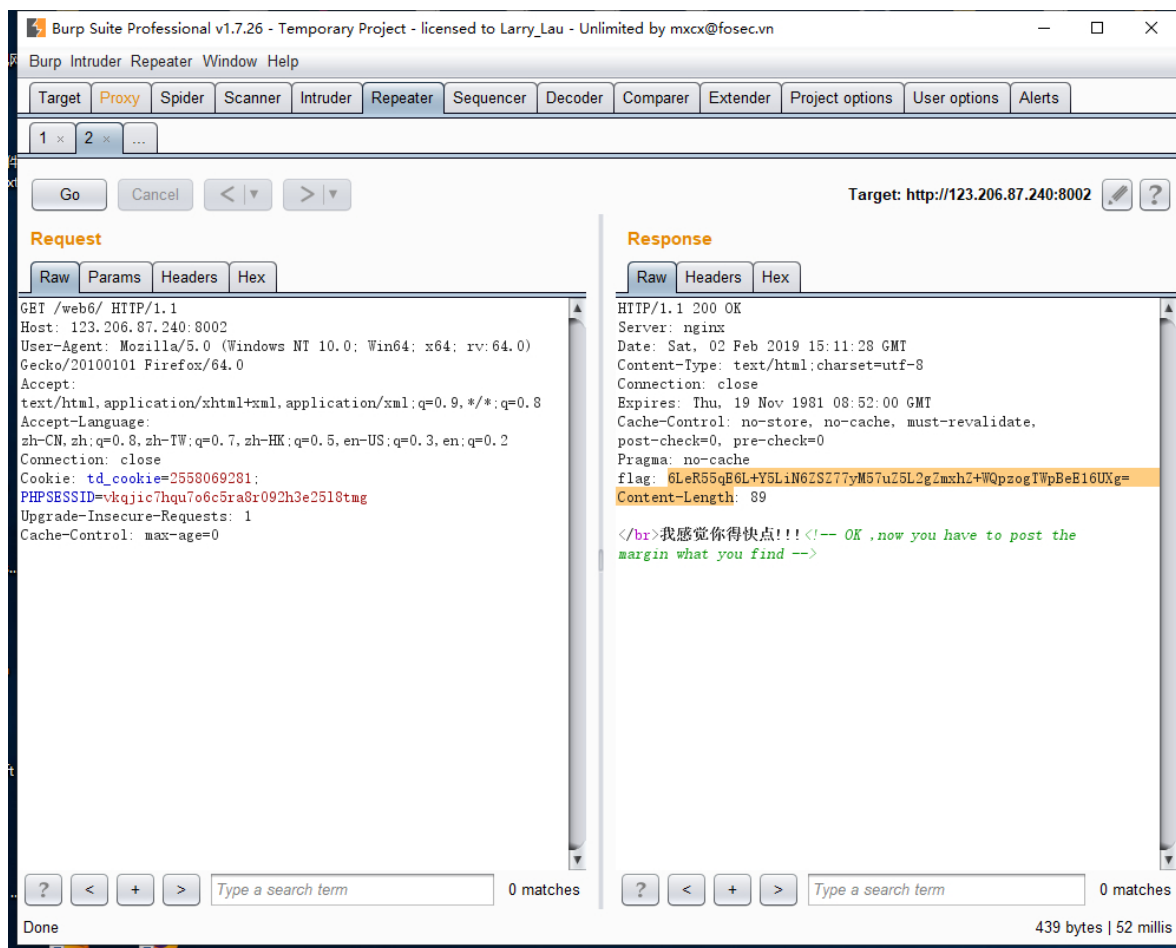
Flag

Submit

访问链接，查看审查元素，提示<OK ,now you have to post the margin what you find>这里感觉需要post提交一些什么东西



利用burp suite进行抓包看看，在response中headers发现了一串base64



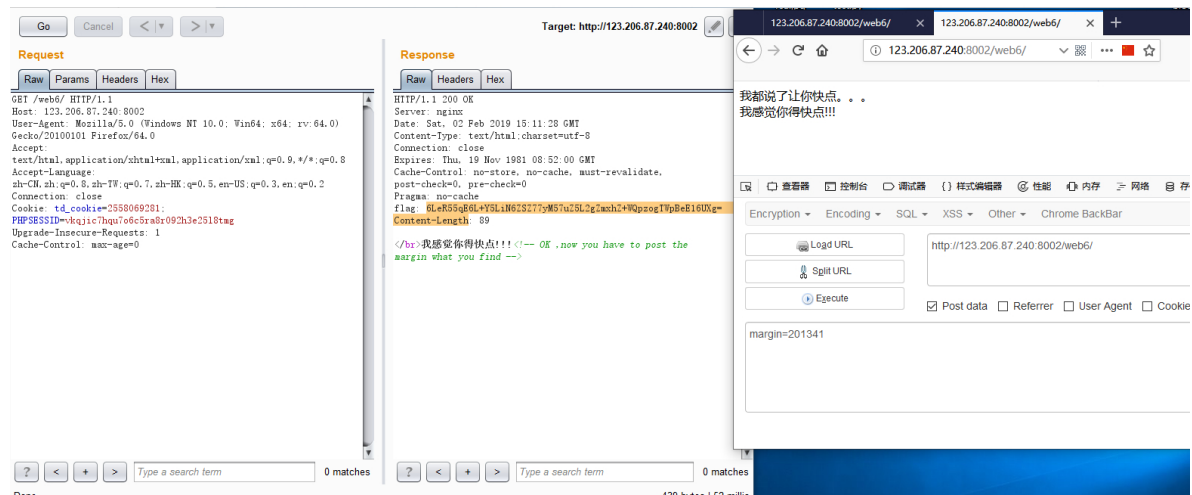
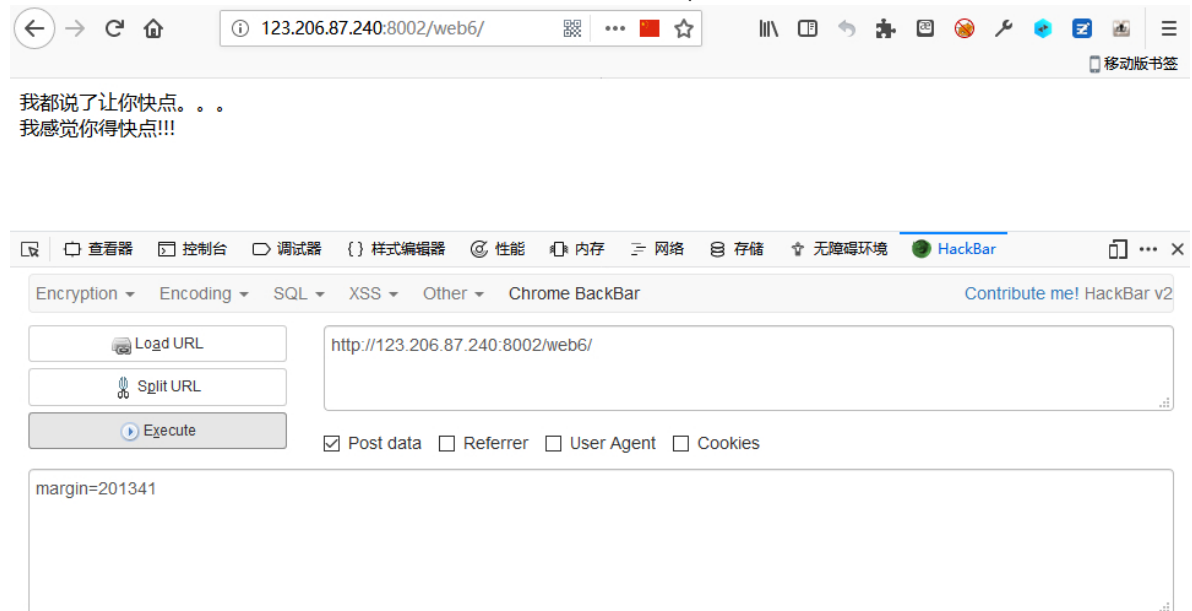
进行base64解密



解出来感觉还是怪怪的，感觉还是base64，进行再次解密



将解密出来的进行提交, 提交失败, 想到源代码中的注释, post提交看一下



提示我 (都说了让你快点。。。)

然后几次尝试发现每次headers中的base64在变化,发现PHPSESSID字段应该是要post提交保持同一个会话

写python进行post提交

```
# coding: utf-8

# 导入模块
import requests
import base64

url = 'http://123.206.87.240:8002/web6/' # 链接
convert = requests.session() # 创建会话对象 (保持cookie)
html = convert.get(url) # get请求
head = html.headers['flag'] # 获取头部flag信息

decode_1 = base64.b64decode(head) # 进行base64解密
code = decode_1.decode('utf-8') # bytes转string
separate = code.split(':') # 将base64解密后的字符串进行以':'进行分隔, 获取flag后面的值
decode_2 = base64.b64decode(separate[1]) # 返回分隔后的字符串列表, 将解密后的进行二次base64解密

flag = convert.post(url, data={'margin': decode_2}) # 构造margin参数post提交
```

```
print(flag.text)
```

```
1  # coding: utf-8
2
3  # 导入模块
4  import requests
5  import base64
6
7  url = 'http://123.206.87.240:8002/web6/' # 链接
8  convert = requests.session() # 创建会话对象(保持cookie)
9  html = convert.get(url) # get请求
10 head = html.headers['flag'] # 获取头部flag信息
11
12 decode_1 = base64.b64decode(head) # 进行base64解密
13 code = decode_1.decode('utf-8') # bytes转string
14 separate = code.split(':') # 将base64解密后的字符串进行以 ':' 进行分隔, 返回分隔后的字符串列表
15 decode_2 = base64.b64decode(separate[1]) # 将解密后的进行二次base64解密
16
17 flag = convert.post(url, data={'margin': decode_2}) # 构造margin参数post提交
18 print(flag.text)
19
```

Run: endoce x

"D:\Python Project\web2\venv\Scripts\python3.exe" "D:/Python Project/web2/endoce.py"
KEY {111dd62fcd377076be18a}

Process finished with exit code 0