

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



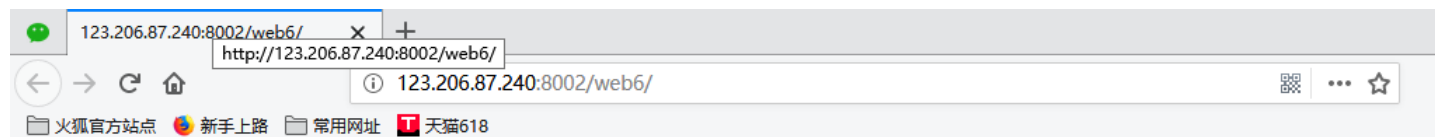
[BugKu 专栏收录该内容](#)

9 篇文章 0 订阅

订阅专栏

题目网址

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



我感觉你得快点!!!

https://blog.csdn.net/weixin_43826194

题解

方法

解密发现的重要信息, post过去

图解

```
1 </br>我感觉你得快点!!!<!-- OK ,now you have to post the margin what you find -->
2
```

查看源代码，看到了这条重要的信息，好像是要把发现的信息通过margin这个参数post过去

https://blog.csdn.net/weixin_43826194

我感觉你得快点!!!

打开开发人员工具响应头里看到了这个，显然是加密的

```

Cache-Control: no-store, no-cache, must-reval...te, post-check=0, pre-check=0
Connection: keep-alive
Content-Encoding: gzip
Content-Type: text/html;charset=utf-8
Date: Thu, 13 Jun 2019 14:33:47 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
flag: 6LeR55qE6L+YSLIN6ZSZ77yM57uZ5L2gZmxhZ+WQpzogTKRBMESEazE=
Keep-Alive: timeout=60
Pragma: no-cache
Server: nginx
Transfer-Encoding: chunked
    
```

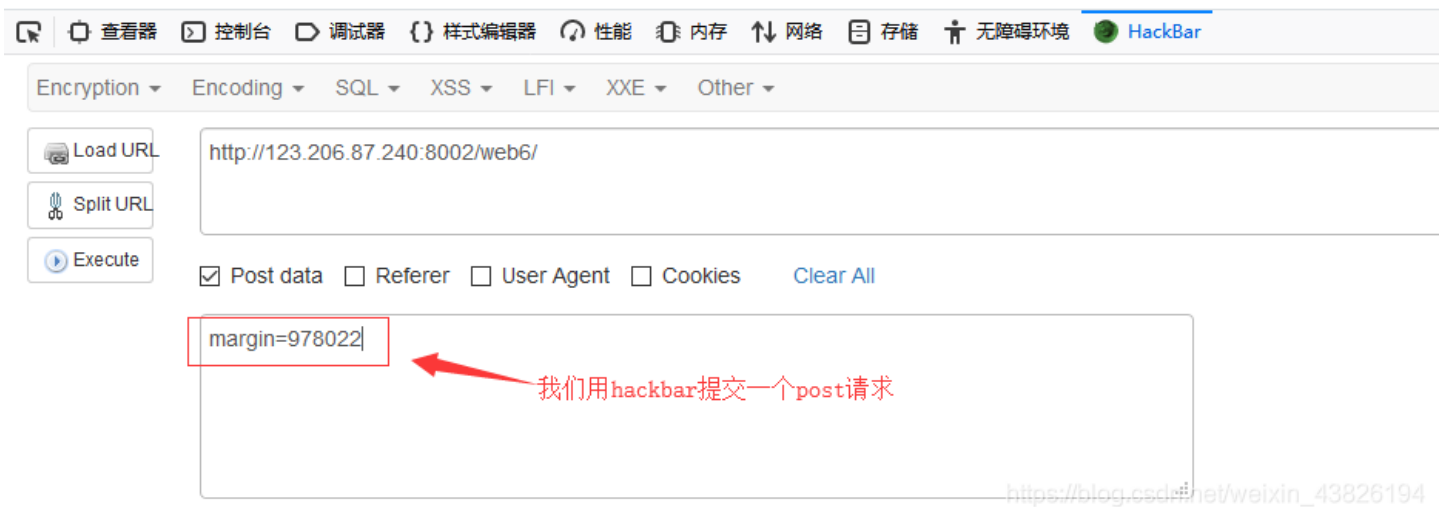
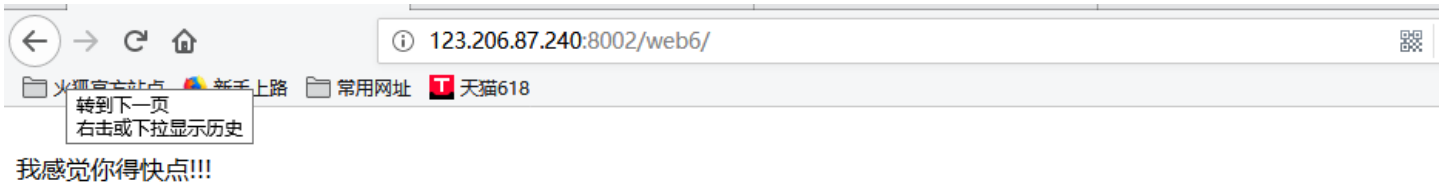
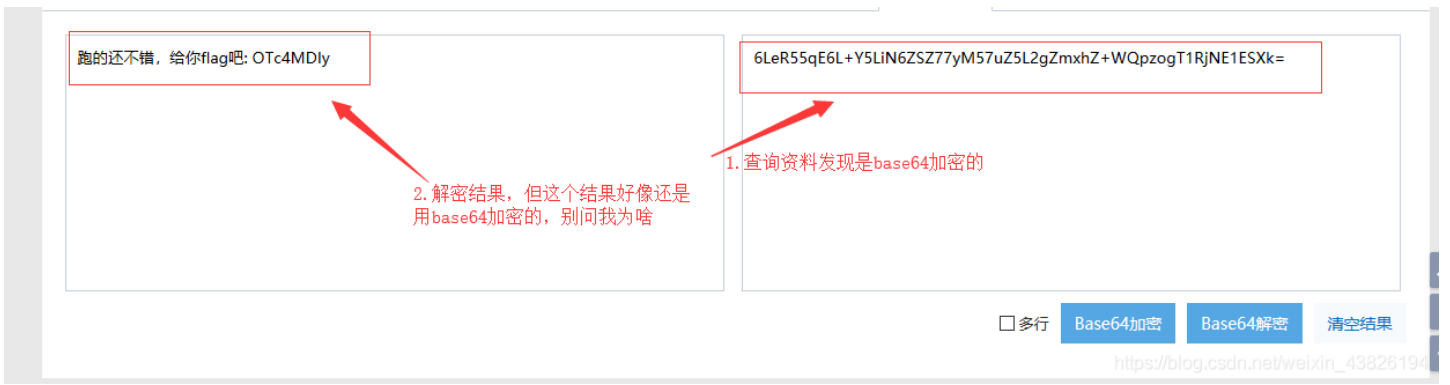
https://blog.csdn.net/weixin_43826194

用hackbar发现乱码了，还是用站长工具吧

```

Encryption Encoding SQL XSS LFI XXE Other
Load URL Split URL Execute
Post data Referrer User Agent Cookies Clear All
    
```

https://blog.csdn.net/weixin_43826194



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？

The screenshot shows a web proxy tool interface. At the top, there are navigation icons for '查看器' (Viewer), '控制台' (Console), '调试器' (Debugger), '样式编辑器' (Style Editor), '性能' (Performance), '内存' (Memory), '网络' (Network), '存储' (Storage), '无障碍环境' (Accessibility), and 'HackBar'. Below this is a menu with 'Encryption', 'Encoding', 'SQL', 'XSS', 'LFI', 'XXE', and 'Other'. The main area has a 'Load URL' button and a text input field containing 'http://123.206.87.240:8002/web6/'. Below the URL field are 'Split URL' and 'Execute' buttons. A section for request headers has checkboxes for 'Post data' (checked), 'Referer', 'User Agent', and 'Cookies', along with a 'Clear All' button. A large text area contains the request body 'margin=978022'. At the bottom right of this area, there is a URL 'https://blog.csdn.net/weixin_43826194'. The browser's address bar at the bottom shows '123.206.87.240:8002/web6/' and several bookmarks.

我感觉你得快点!!!

The screenshot shows a browser's network developer tool. The 'Network' tab is active, showing a list of requests. The first request is a GET to '123.206.87.240:8002/web6/' with a status of 200. The response headers are expanded, showing various metadata. A red box highlights the 'flag' header: 'flag: 6LeR55qE6L+Y5LiN6Z5Z77yM57uZ5L2gZmxhZ+WQpzogTORJek1USTQ='. A red arrow points to this header with the text: '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' (Re-entered the website and found that the last few digits of the flag have changed, so we decided to write a script to run it). Other headers include 'Cache-Control: no-store, no-cache, must-reval...te, post-check=0, pre-check=0', 'Connection: keep-alive', 'Content-Encoding: gzip', 'Content-Type: text/html; charset=utf-8', 'Date: Sat, 15 Jun 2019 03:49:42 GMT', 'Expires: Thu, 19 Nov 1981 08:52:00 GMT', 'Keep-Alive: timeout=60', 'Pragma: no-cache', 'Server: nginx', and 'Transfer-Encoding: chunked'. The status bar at the bottom shows '2个请求 | 已传输 251 字节 / 519 字节 | 完成: 149 毫秒 | DOMContentLoaded: 53 毫秒 | load: 69 毫秒'.

```
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)
```

```
websp...
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