

秋名山老司机-writeup

打开题目，秋名山老司机来飙车吗？

Challenge

1710 Solves

×

秋名山老司机

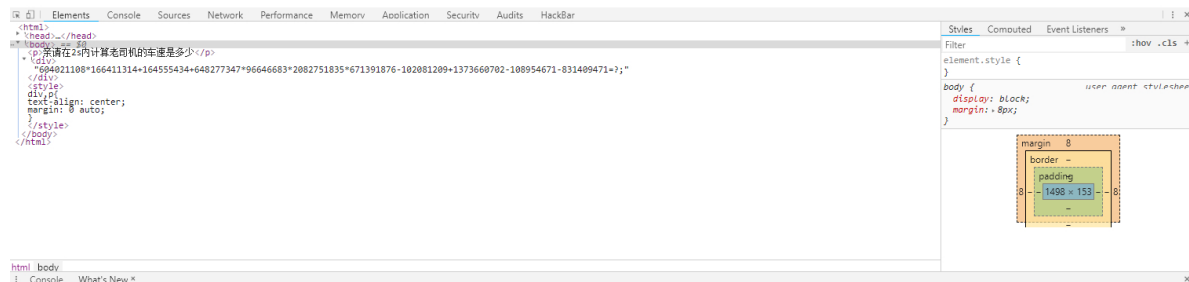
100

<http://123.206.87.240:8002/qiumingshan/>
是不是老司机试试就知道。

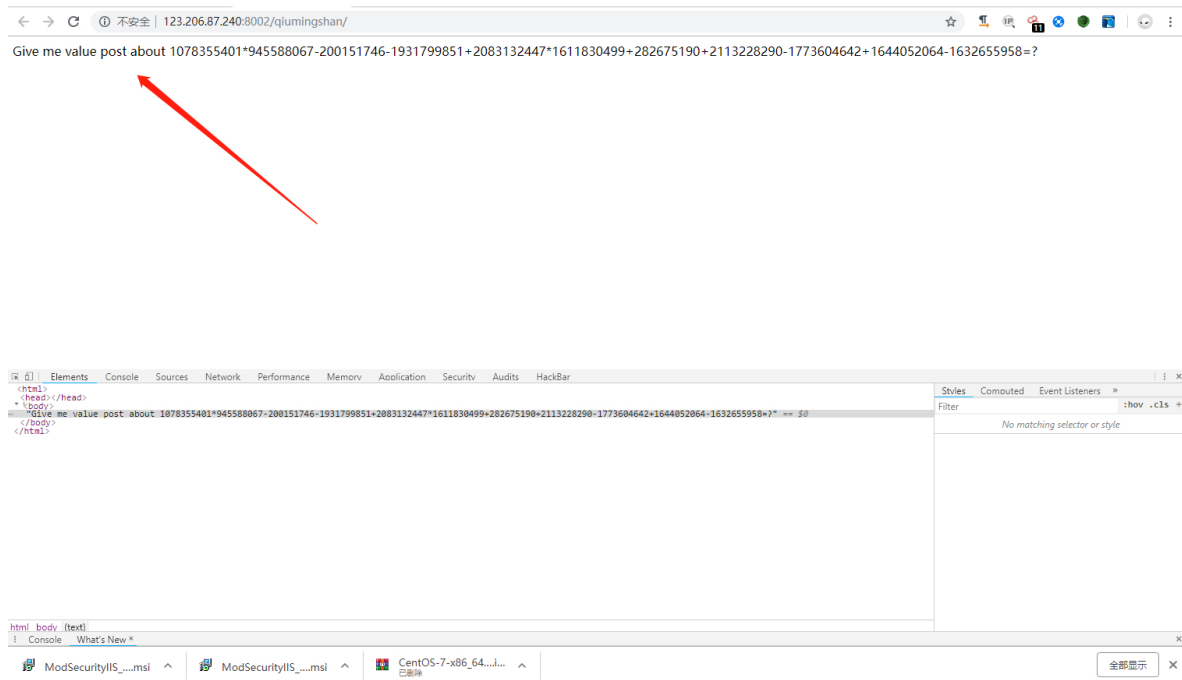
Flag

Submit

访问链接，发现是一道计算题，算了下，2s?这道题明显要求计算响应内容中的表达式并POST请求正确的信息返回结果，还是快速反弹POST请求



这里会纳闷传值传给谁，刷新了几下发现提示Give me value post about



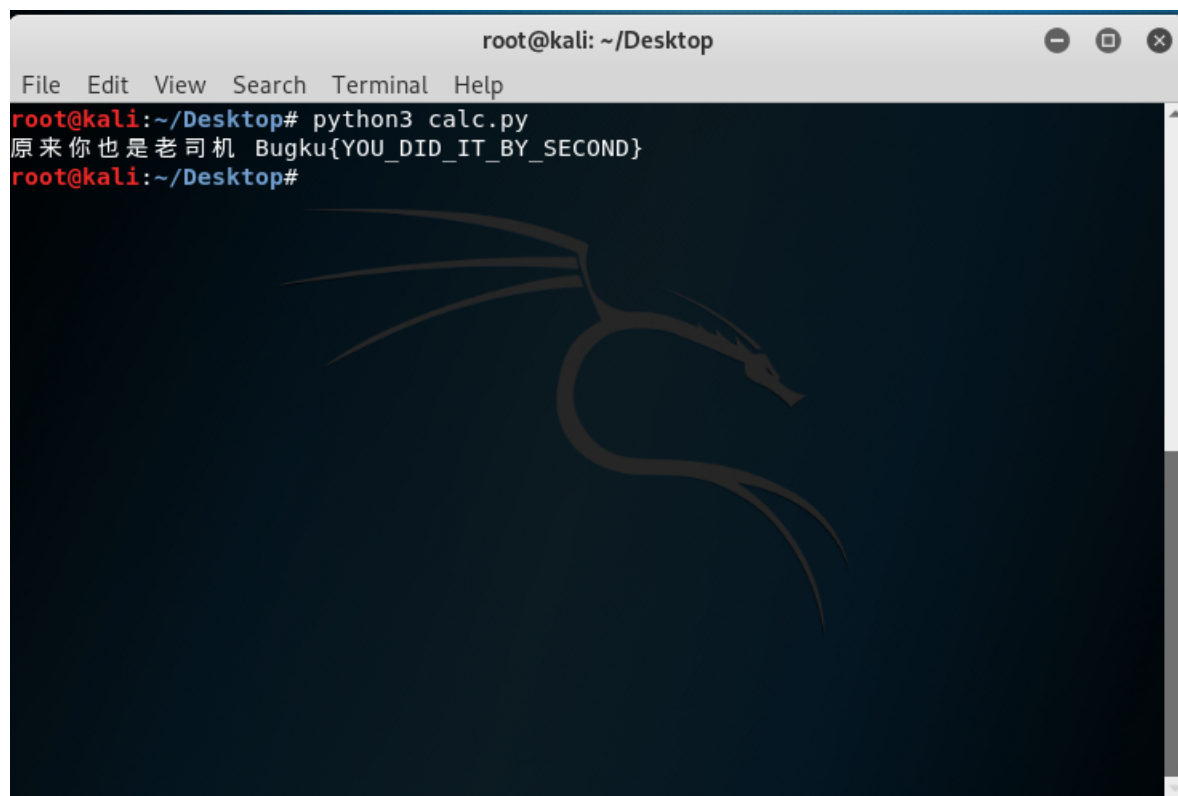
直接写python

```
# coding: utf-8

# 导入模块
import requests
import re

url = 'http://123.206.87.240:8002/qiumingshan/' # 链接
convert = requests.Session() # 创建session对象, session对象可以使我们跨请求保持某些
# 参数, 也可以在同一个session实例发出的所有请求之间保持cookies
html = convert.get(url).text # get请求
reg = re.compile(r'(?<=<div>).*?(?=\=)').findall(html) # 匹配表达式如
['2024653276+1430867578+1152697161*392577551-
1429779315*779503901+1352271449+1584130862+557093247+1523782933+1160059856']
payload = {'value': eval(reg[0])} # eval计算式子(匹配出来的是列表)并构造post请求的
# data部分
flag = convert.post(url, data=payload) # post带参数提交
flag.encoding = 'utf-8' # 'utf-8'格式
print(flag.text)
```

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# python3 calc.py
原来你也是老司机 Bugku{YOU_DID_IT_BY_SECOND}
root@kali:~/Desktop#
```



这个因为是2s的原因，要结合环境（程序自身的运行时间、网速等因素）也有可能python的计算与服务端的计算有误差，导致出现了要一定的概率才会出现flag，（触及到我的知识盲区-_-!）多尝试几次。可以加个while True 循环，亦或者加个多线程并发。