Web 任务 wp

1. 给的第一题是 newbugku 的，但是最近好多 web 题都挂了，这个我也没进去，不过之前好像做了，也忘记是啥了
2. http://123.206.87.240:9004/1ndex.php?id=5

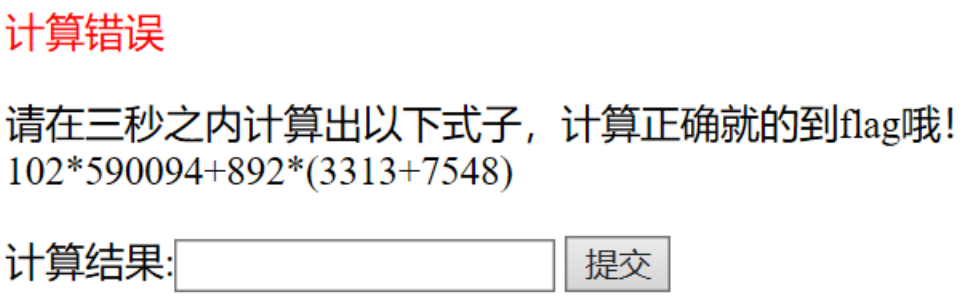
   这道题目好像有点印象，但是忘记当时怎么做的，重新复现一遍

   待会回来补上

3.网址链接坏了

4.网址链接坏了

5. http://123.206.31.85:10002/



   这道题目算是老题目了，直接写脚本 post 就行了，关键点还是得建立一个 session，否则会 post 失败

```
url= 'http://123.206.31.85:10002/'

import requests

s = requests.session()

a = s.get(url=url)

print(a.text)

import re

quary = re.findall(re.compile(r'(.*)</p>'),a.text)

print(quary)

print(eval(quary[0]))

form_data={'result':eval(quary[0])}

print(s.post(url=url,data=form_data).text)
```

获得 flag： flag{b37d6bdd7bb132c7c7f6072cd318697c}

6. http://47.95.208.167:10005/index.php?mod=home

Bugku _留言本

主页 | 新建留言

Delete

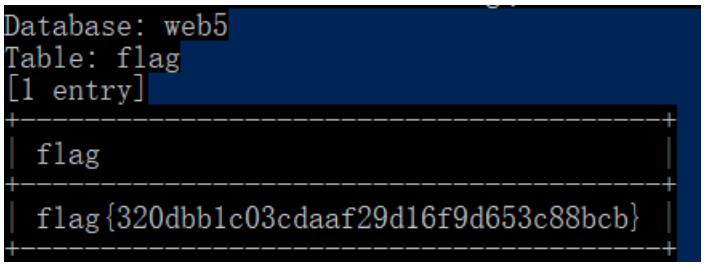
Post -- 1

1

at 2018-11-30 15:35:33

这道题目怎么说呢看到留言 1 进去，url 链接上有 id=2，直接上 sqlmap

python sqlmap.py -u 47.95.208.167:10005/?mod=read"&"id=2 –dump



第七题和第八题也挂了，好像 bugku_论剑的这个服务器关了服务 123.206.31.85