【攻防世界】十六 --- easytornado

原创

通地塔 于 2020-12-28 18:30:06 发布 100 收藏 1

分类专栏： 攻防世界 文章标签： ctf 网络安全

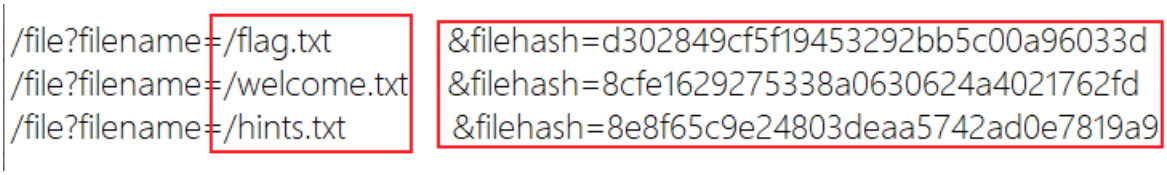
本文链接：https://blog.csdn.net/qq_43168364/article/details/111871465

题目 — easytornado

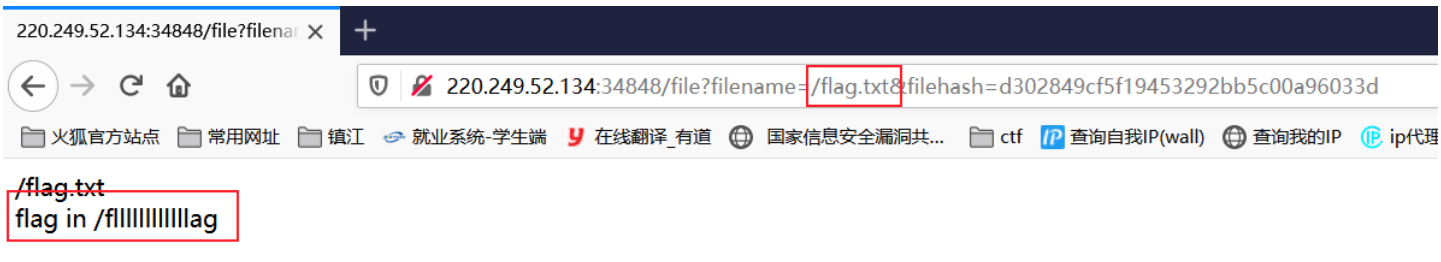
一、writeup

主页有三个文件

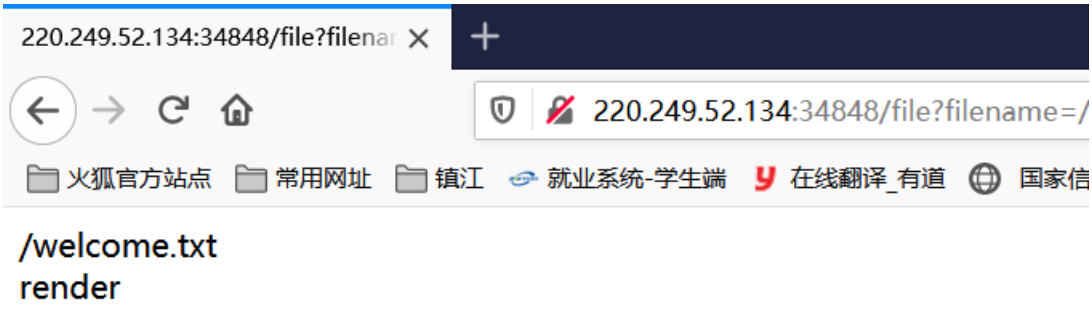
分别访问以下可以看到他们的URL格式如下图所示



都是文件名带一个filehash的格式，那就可以猜测访问flag文件的url格式应该就是：`/file?filename=/flag的文件名&filehash=xxx`。接下来依次看这几个文件的内容。`/flag.txt` 文件



提示flag在：/flllllllllllag中，我们的URL格式又进一步确定了：`/file?filename=/flllllllllllag&filehash=xxx`，现在只要确定了`filehash`如何计算就可以得到`flag`。再看`/welcome.txt`文件

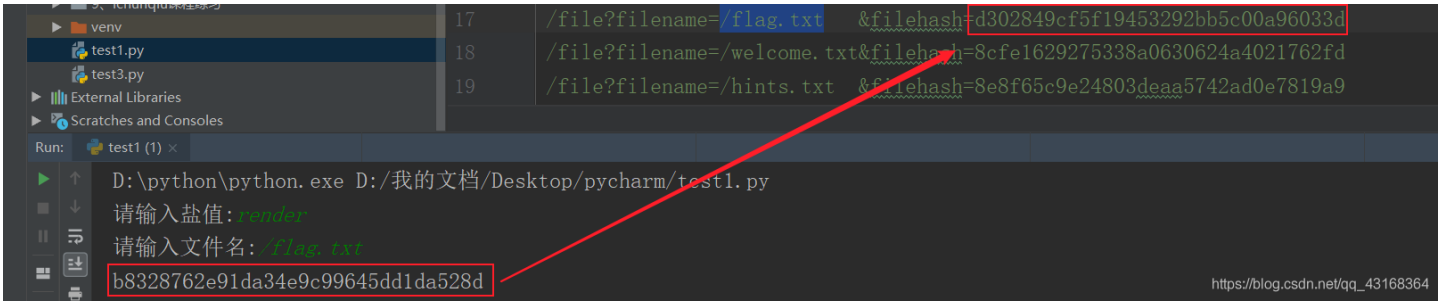


这里显示了一个`render`，不知道是什么，先放着，再看`/hints.txt`文件中的内容

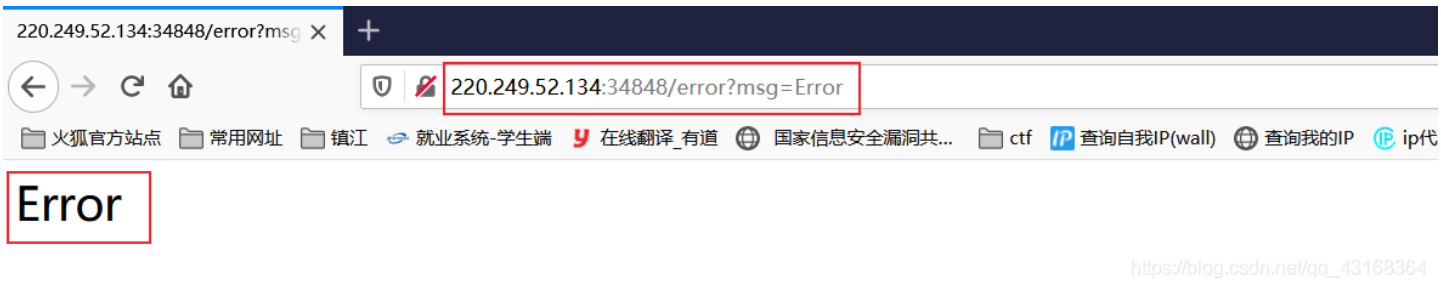
这里告诉了我们`filehash`的计算方法：`md5(cookie_secret + md5(filename))`，接下来只要确定了cookie_secret的值是什么，我们就可以得到flag了。起初我以为cookie_secret 就是 render，于是编写了如下所示的代码去计算 `filehash`

```
import hashlib
def md5(message):
    md5 = hashlib.md5()
    md5.update(message.encode('utf-8'))
    return md5.hexdigest()

def main(salt, name):
    print(md5(salt + md5(name)))


if __name__ == "__main__":
    cookie_secret = input("请输入盐值:")
    filename = input("请输入文件名:")
    main(cookie_secret, filename)
```

但是发现计算得到的结果和url中的内容并不相同



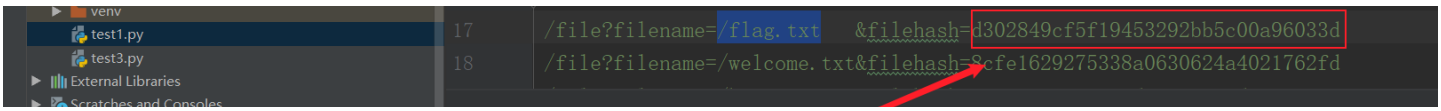
so，cookie_secret 肯定就不是render了。需要继续找cookie_secret。发现当输入错误的 filehash值 ， 会回显出如下所示的内容

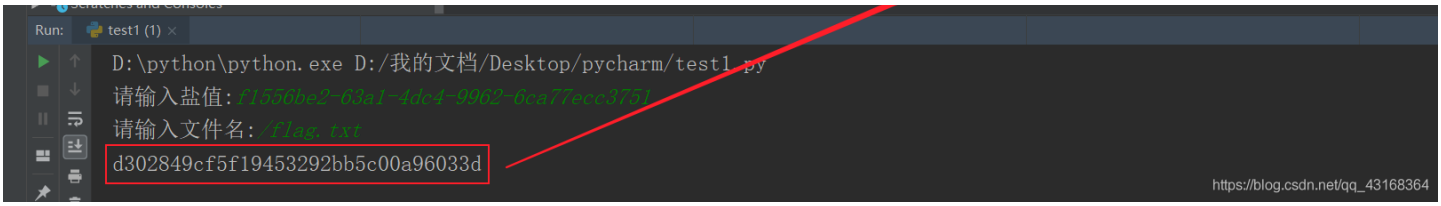


这里试了以下SSTI貌似不存在

到这里就没有思路了。查阅资料得知，可以访问：`?msg={{handler.settings}}`，得到应用的设置（这里其实是有SSTI的），这里面有`cookie_secret`。（另：在Tornado的前端页面模板中，Tornado提供了一些对象别名来快速访问对象，Handler对象指向的处理当前这个页面的RequestHandler对象。执行?msg={{datetime}} 还可以访问到datetime模块）

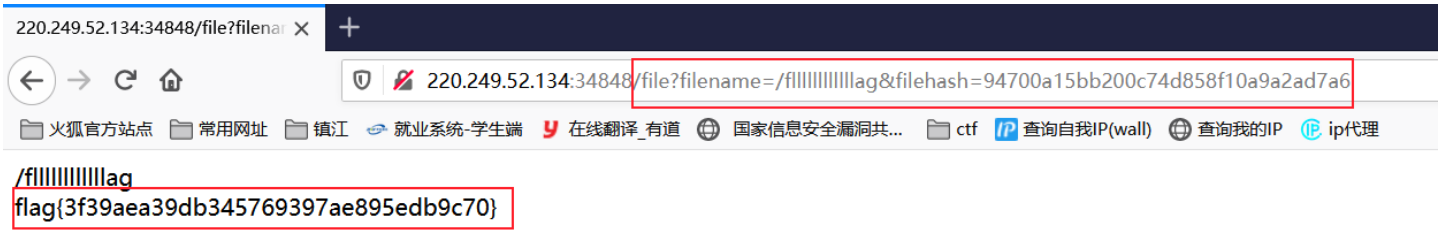
将得到的cookie_secret带到代码中





可以看到得到的`filehash`和`url`中的相同，找到了`cookie_secret: f1556be2-63a1-4dc4-9962-6ca77ecc3751`，运行程序得到访问`/fllllllllllllag`文件的filehash

构造url：`/file?filename=/fllllllllllllag&filehash=94700a15bb200c74d858f10a9a2ad7a6`，得到flag



二、知识点

- **Tornado** — py的一个**web开发框架**
- 在 **Tornado** 里，应用的设置可以通过**{{handler.settings}}**访问。（如果有SSTI的话）
- 观察URL的格式访问文件
- **/error?msg={{datetime}}** — 在Tornado的前端页面模板中，datetime是指向python中datetime这个模块，Tornado提供了一些对象别名来快速访问对象