攻防世界web进阶区easytornado详解

原创

無名之涟 于 2020-07-21 00:30:03 发布

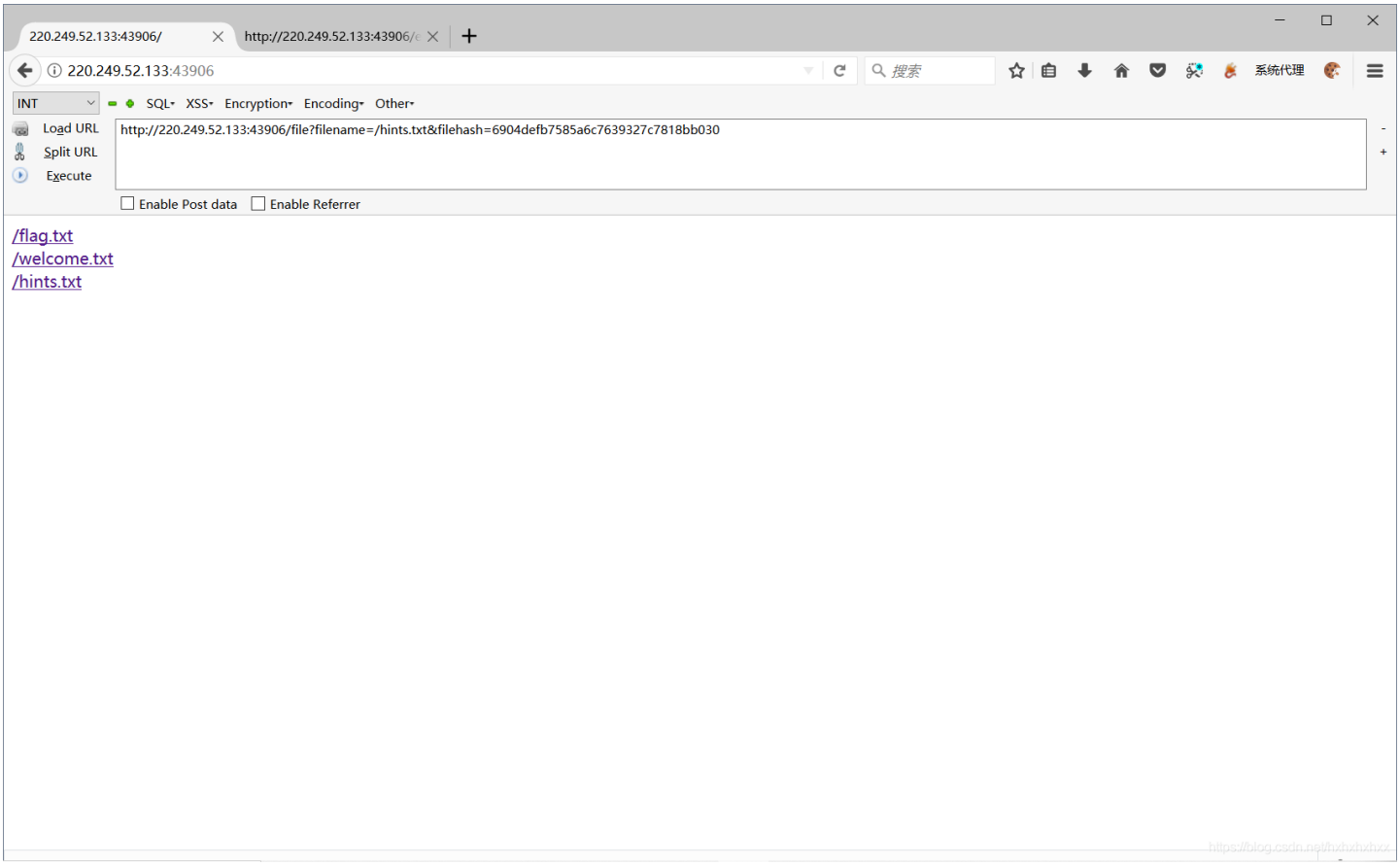
分类专栏： CTF

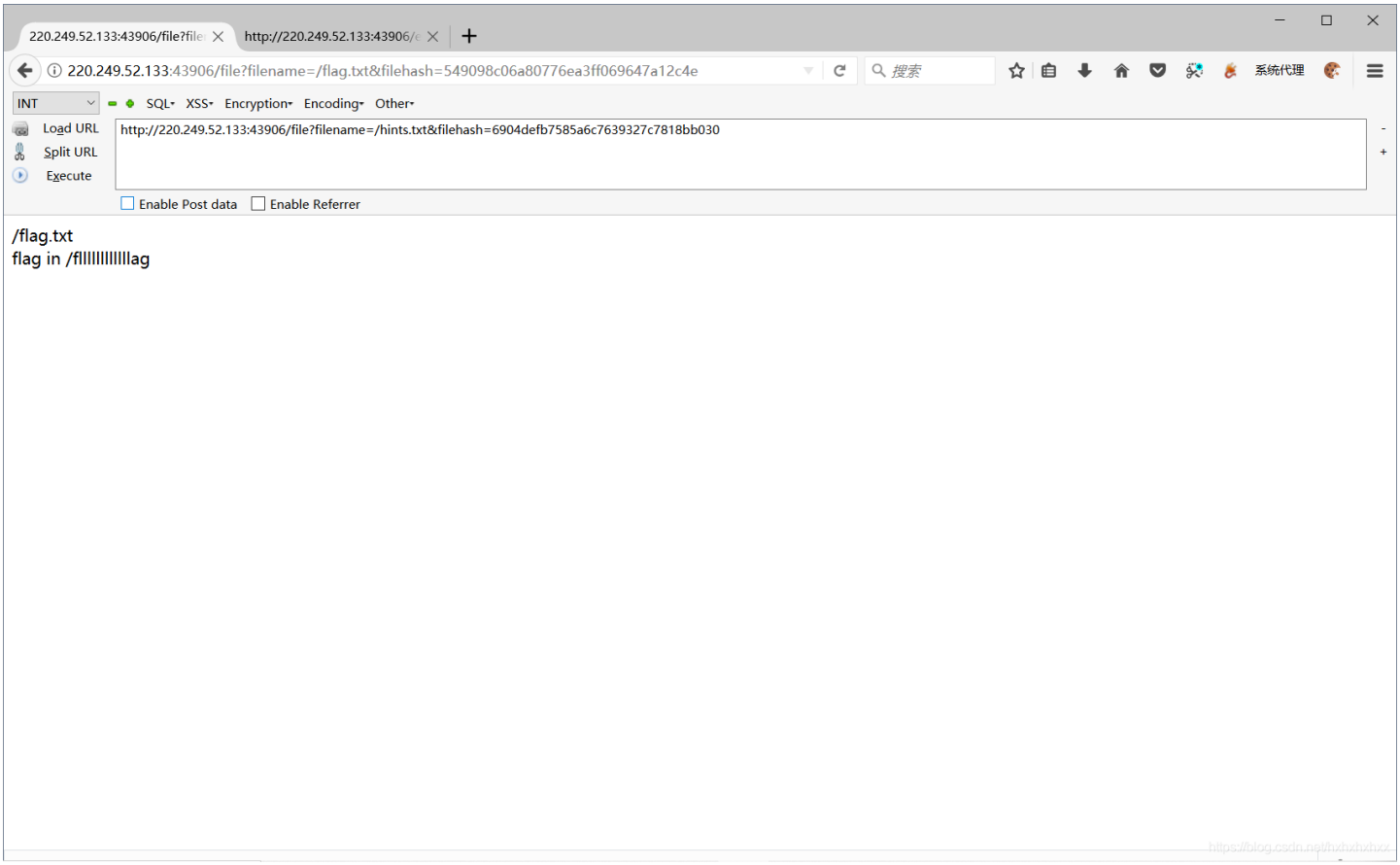
本文链接：https://blog.csdn.net/hxhxhxhxx/article/details/107475107

攻防世界web进阶区easytornado详解

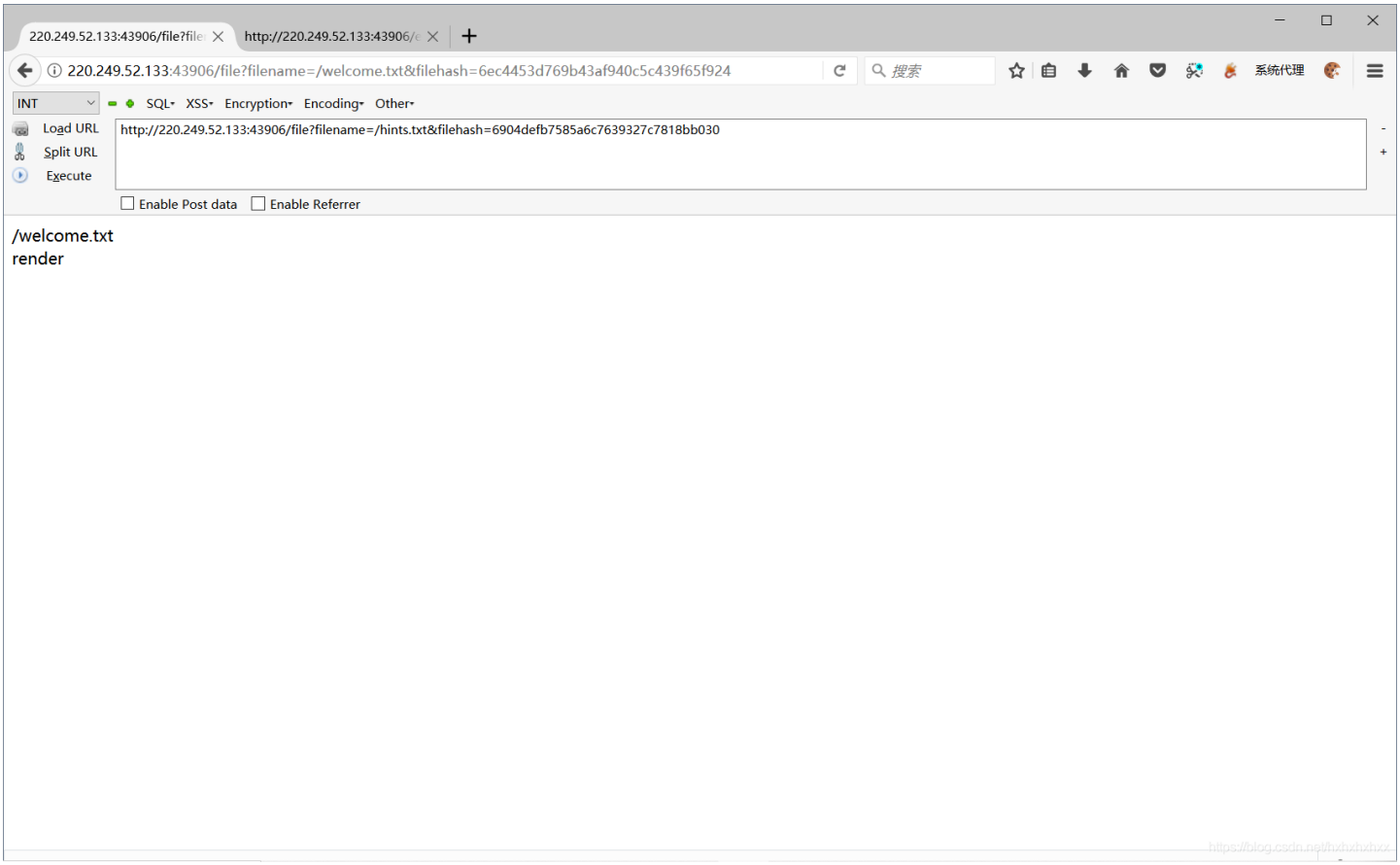
题目

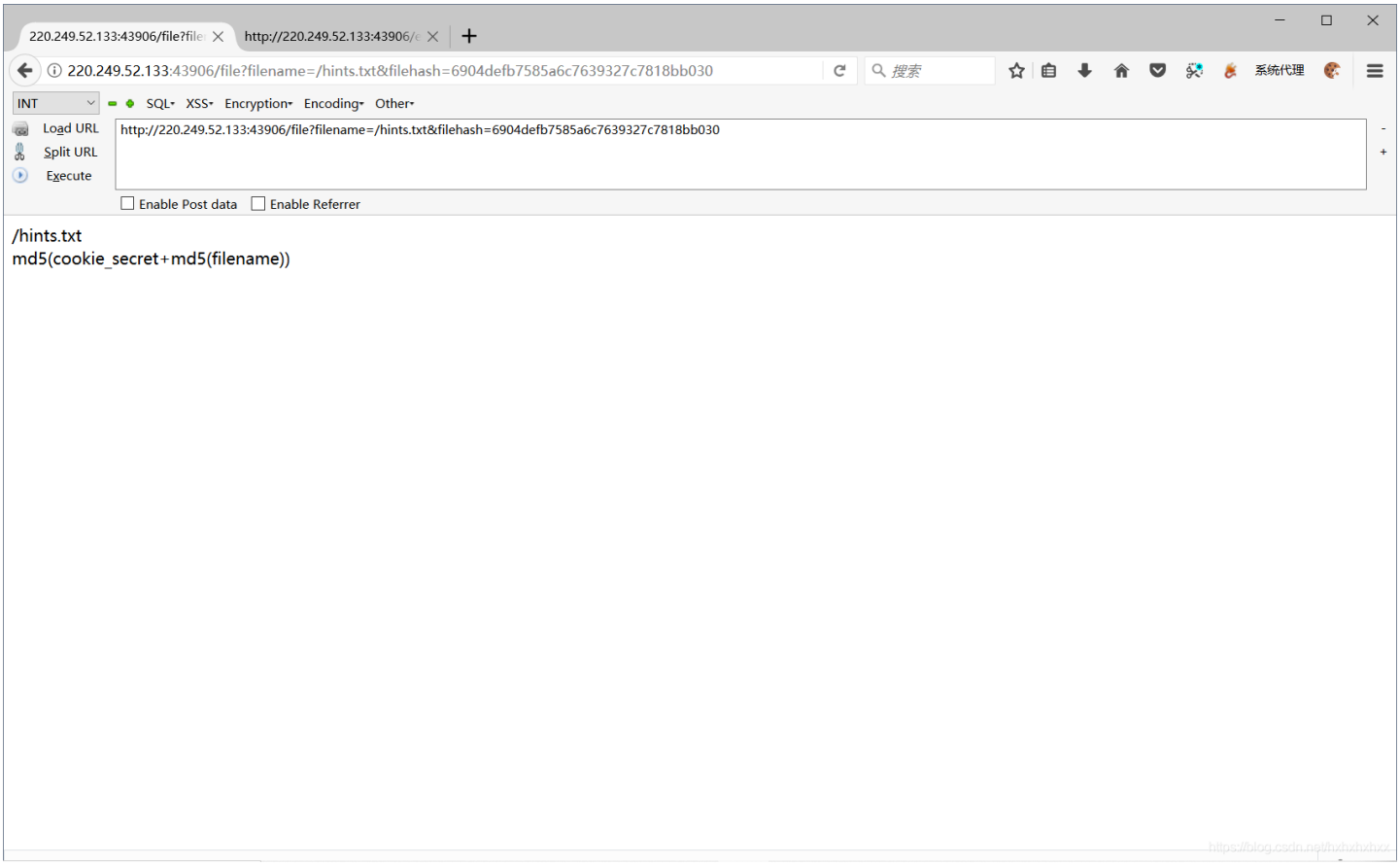
提示：tornado框架





flag in /fllllllllllag

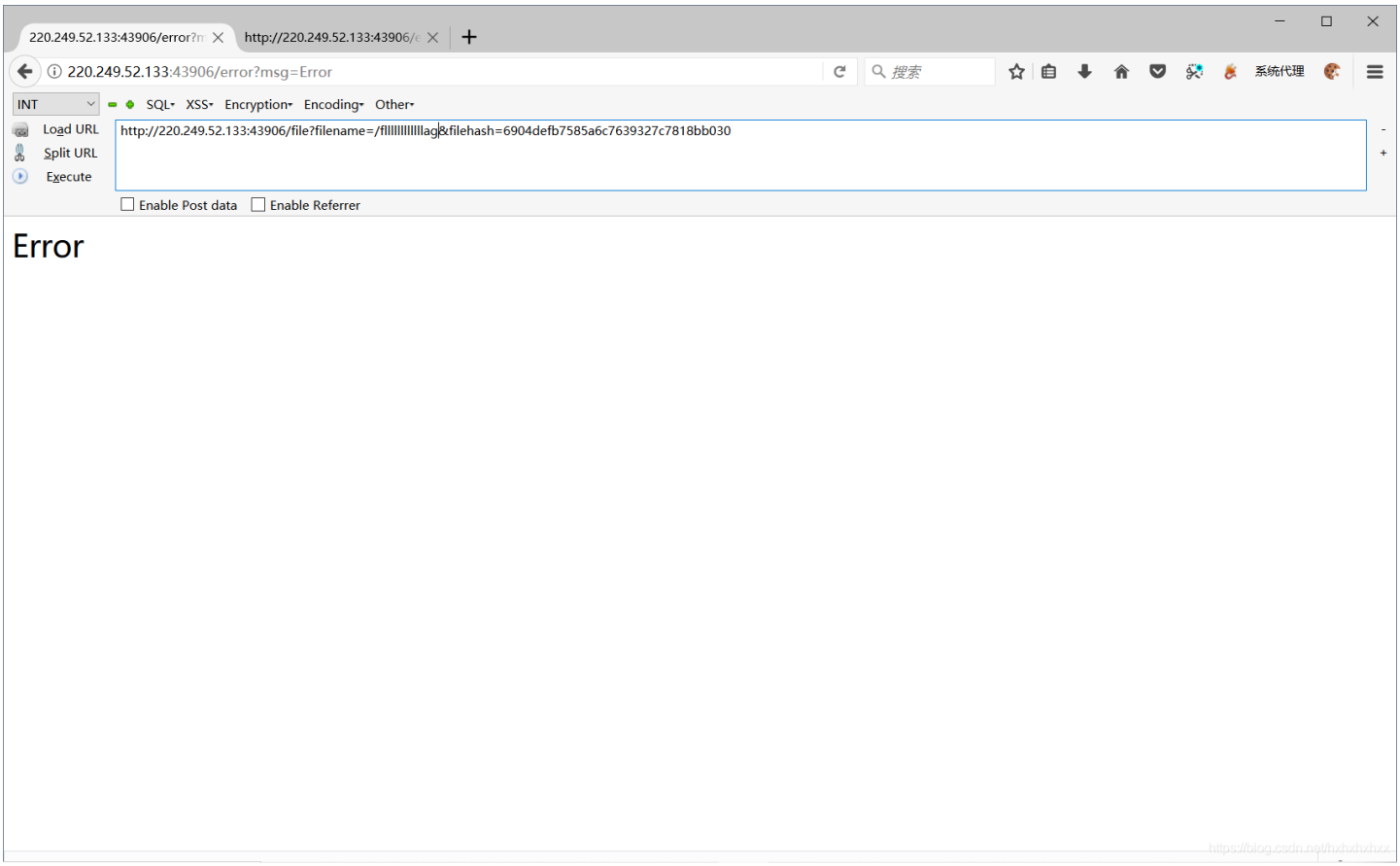




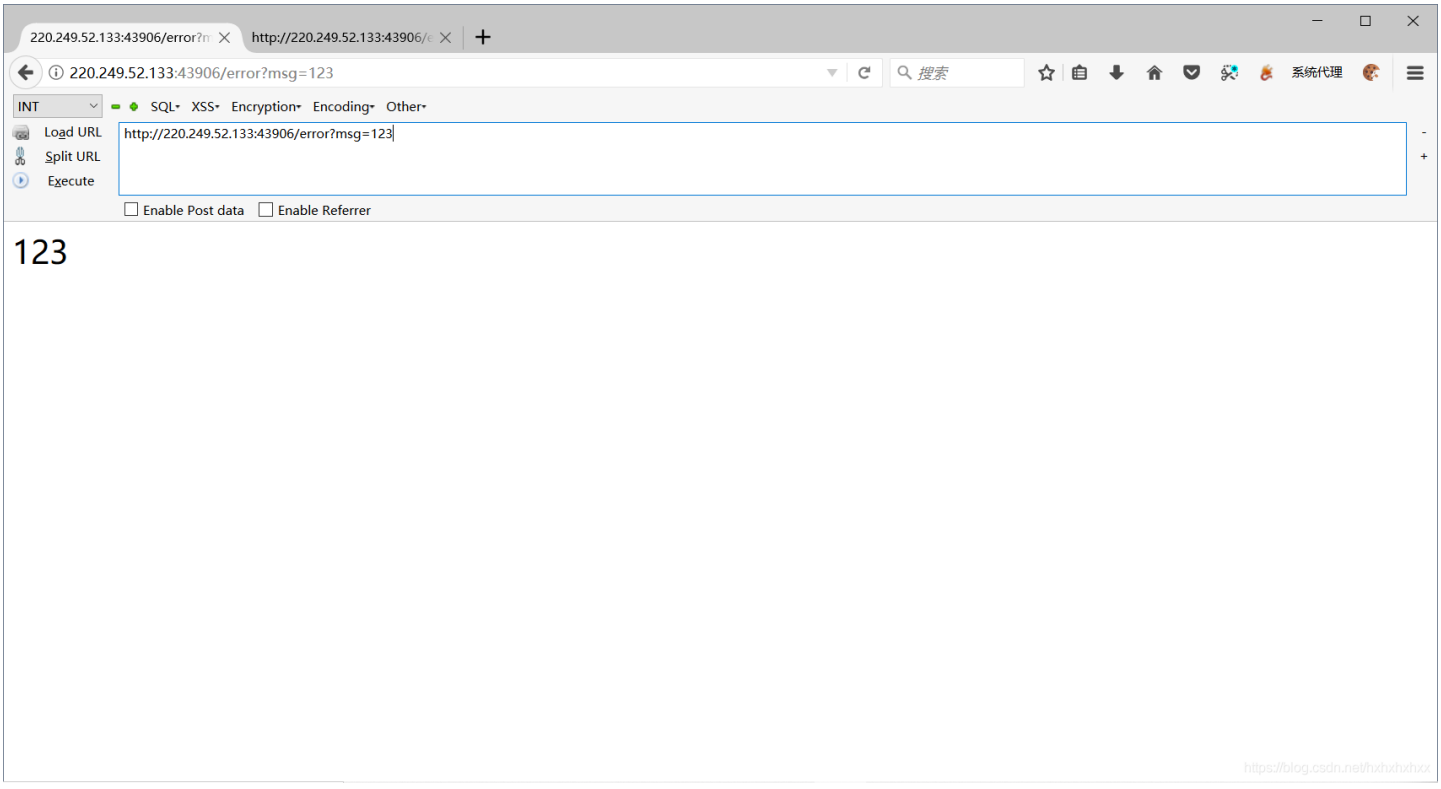
md5(cookie_secret+md5(filename))

详解

首先我们知道了，flag在==/fllllllllllllag==里面
那么我们尝试直接输入



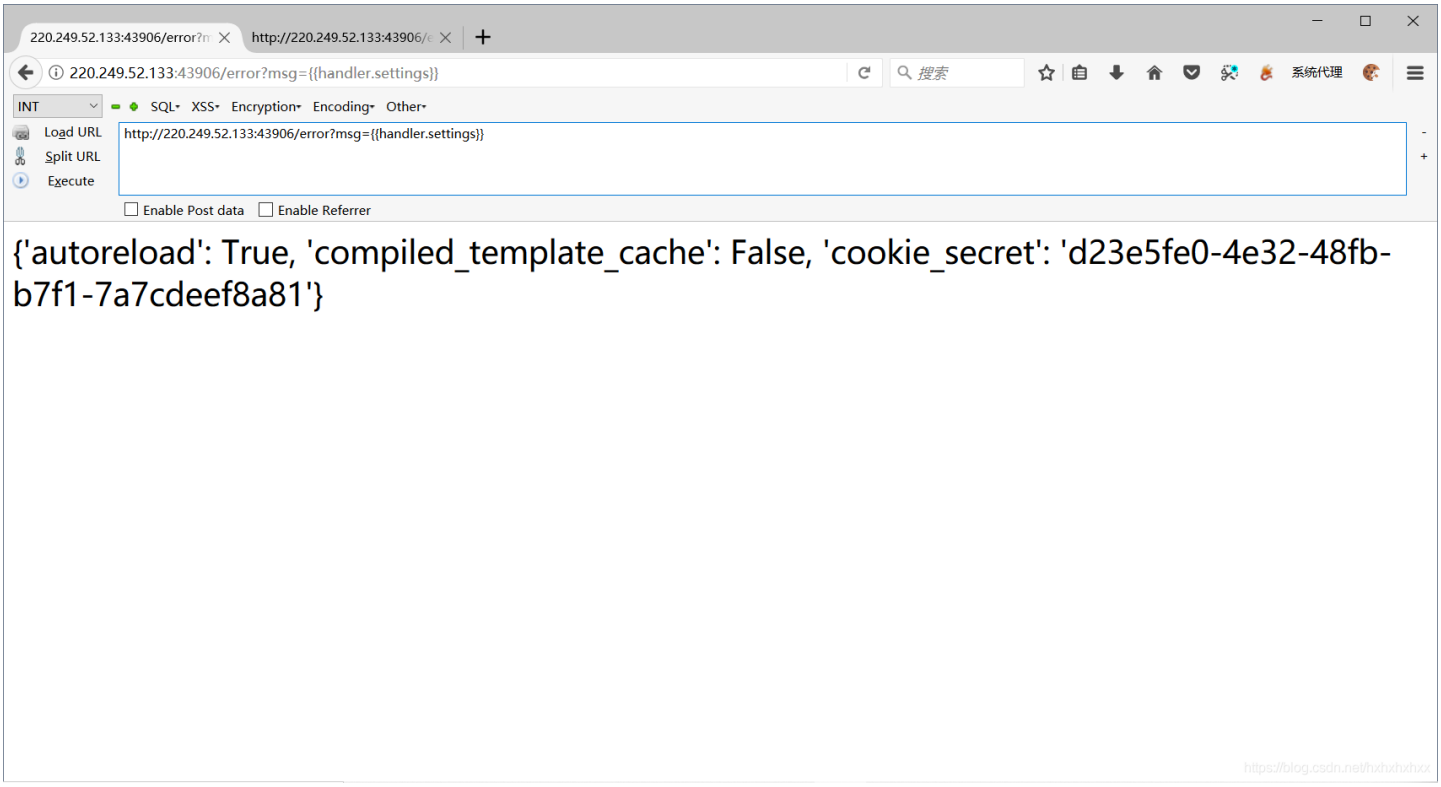
访问出现error



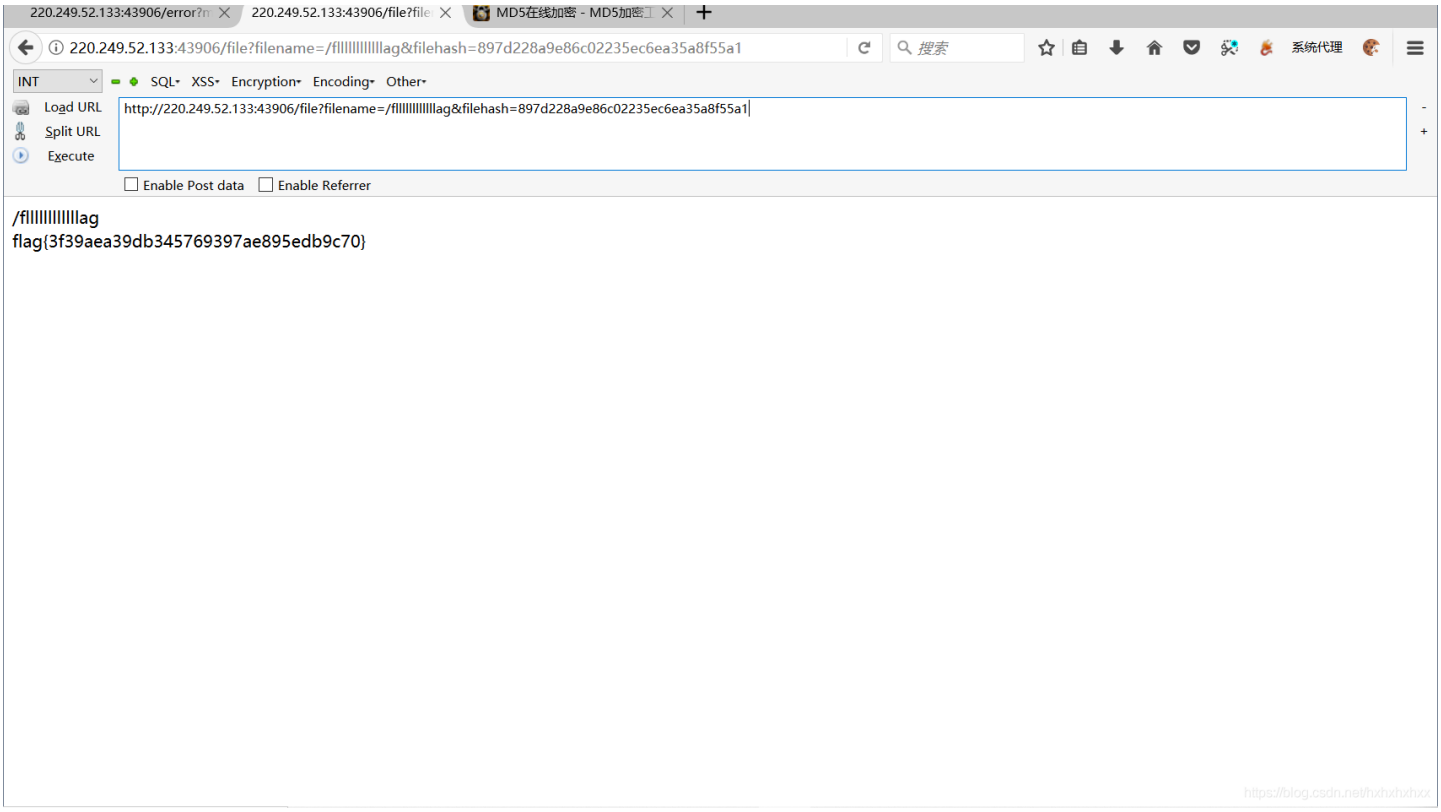
我们发现msg是可以进行更改的
那么我们进行ttsi模板注入检测，并没有发现可以使用的
（使用tplmap）


```
/error?msg={{handler.settings}}
```

在Tornado里，应用的设置可以通过handler.settings访问。
我们拿到cookie



这时候我们想到了他的hint
使用md5来做hash的值
md5(cookie_secret+md5(filename))



然后加上文件名字

flag{3f39aea39db345769397ae895edb9c70}

创作打卡挑战赛