攻防世界web进阶区easytornado

原创

gongjingege 于 2020-07-28 16:47:08 发布 344 收藏

分类专栏： ctf

本文链接：https://blog.csdn.net/gongjingege/article/details/107634464

题目有描述提示，**tornado框架**

打开链接

/flag.txt
/welcome.txt
/hints.txt

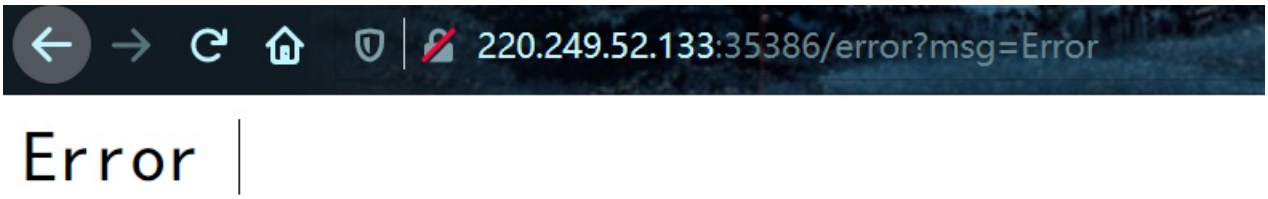
发现3个文件

/flag.txt
flag in /fllllllllllllag

/welcome.txt
render

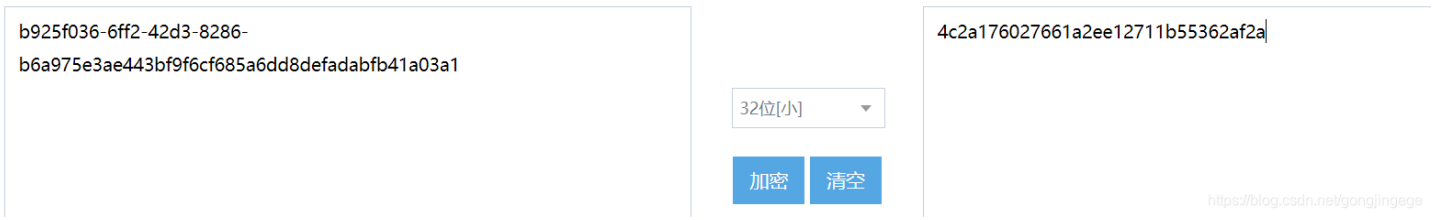
/hints.txt
md5(cookie_secret+md5(filename))

1，flag in /fllllllllllag
2，render，可能会是SSTI模板注入
3，md5(cookie_secret+md5(filename))
url中输入/fllllllllllag，直接error



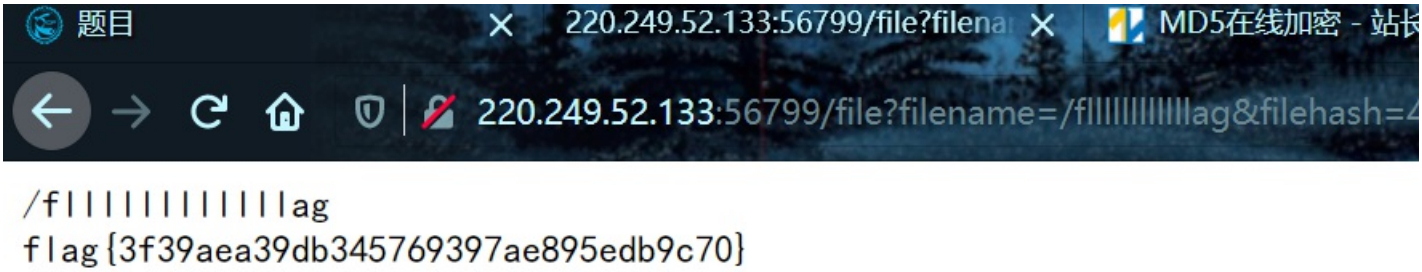
用handler.settings对象拿到cookie
url输入/error?msg={{handler.settings}}

根据hint，filehash值由md5加密
先filename即/fllllllllllag加密，再和cookie拼接，一块md5加密



url加上/file?filename=/fllllllllllag&filehash=4c2a176027661a2ee12711b55362af2a

得到flag



知识点：tornado框架，用handler.settings对象拿到cookie，md5加密

2020.7.28 公瑾