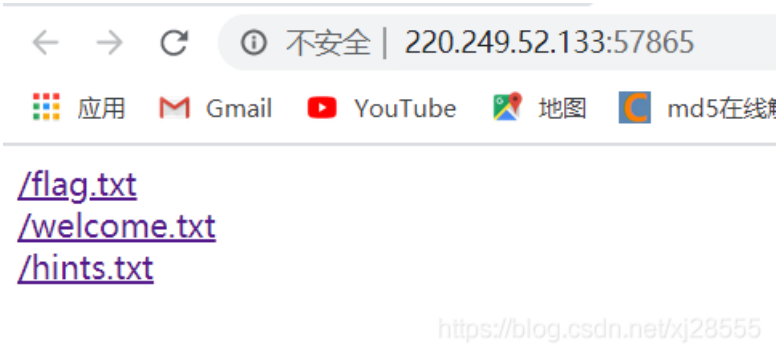
攻防世界 easytornado 解题思路

原创

「已注销」 于 2020-07-14 21:39:44 发布 1367 收藏 4
分类专栏： 攻防世界_web篇

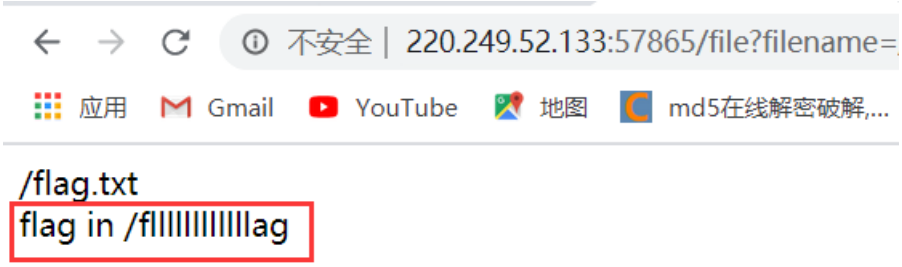
本文链接：https://blog.csdn.net/xj28555/article/details/107347562

进入题目

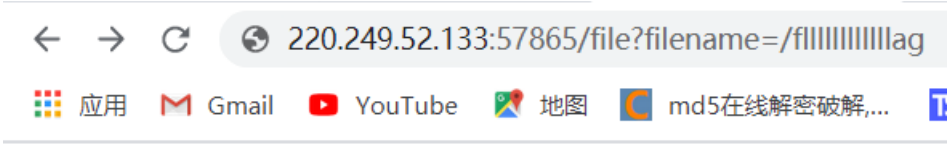


有三个txt目录，我们分别点击。

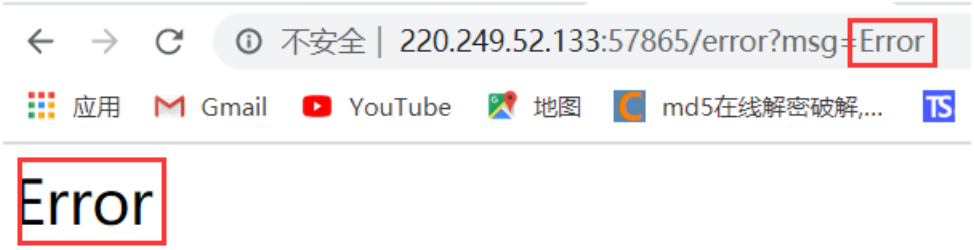
第一个/flag.txt



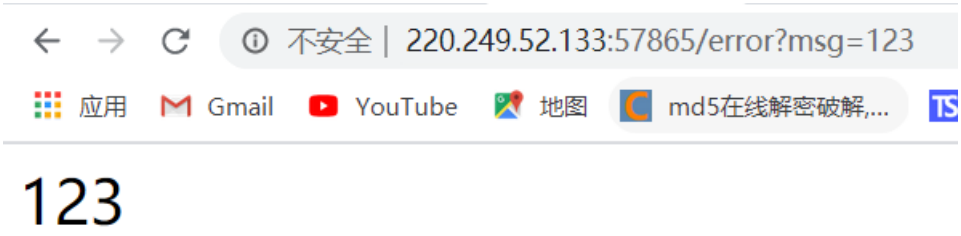
他说flag 在/fllllllllllllag里面，那我们访问一下看看



回车后发现

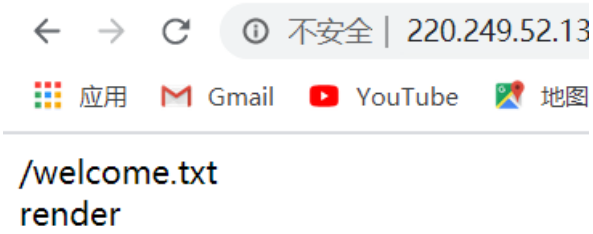


报了一个error，且在浏览器上有回显，那判断这里是否存在模板注入呢，我们可以试一试，把error换成123看浏览器是否还存在回显。



还是有回显，初步证明这里是存在模板注入的。但是知道有模板注入没有更多的信息了，所以我们只好先放这里了。继续看其他目录。

第二个/welcome.txt

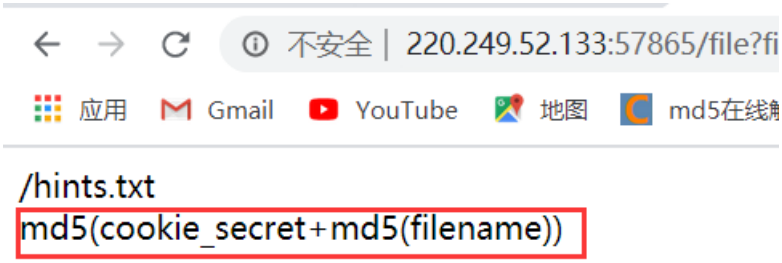


第二个是一个render，这个render是什么呢，不知道，所以我特意去Tomado的官网看了看render的作用官网链接给大家放这里了

https://www.tornadoweb.org/en/stable/

发现render是一个Tomado框架的一个渲染函数，即可以通过传递不同的参数形成不同的页面。

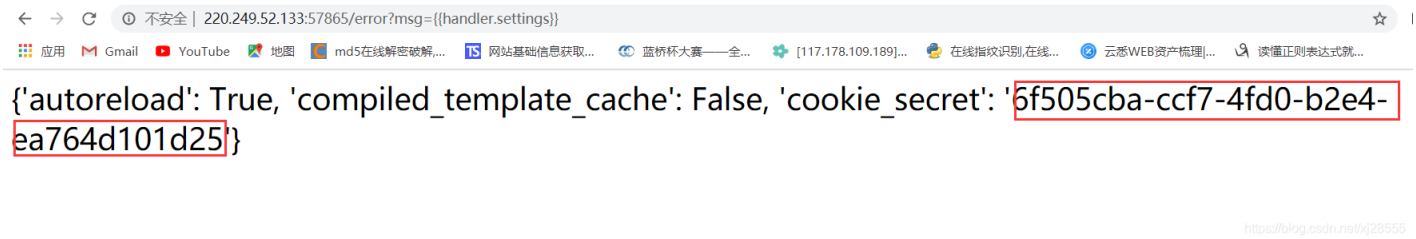
第三个/hints.txt



看到一个式子，先把filename给MD5加密一遍，然后加上cookie_secret然后总体在MD5加密一遍，filename我们知道是/fllllllllllllag现在只有cookie_secret不知道，那么我们现在就是想办法获取cookie_secret值，这个时候我们又想起我们第二个目录时的render渲染函数，那我们可以去Tomado官网看看cookie_secret是在那个函数里面，通过查阅文档可以构造payload

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

来过去到cookie_secret如图。



现在把filename给MD5加密然后再加上cookie_secret再MD5加密一次然后构造payload即可拿到flag！