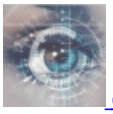
攻防世界 easytornado

原创

听门外雪花飞 于 2022-02-23 11:13:26 发布 1837 收藏

分类专栏： ctf刷题纪 文章标签： 安全

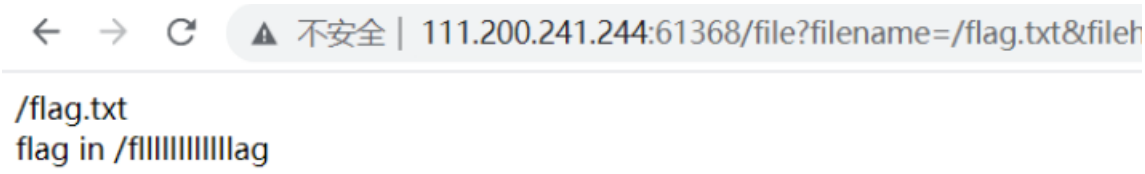
本文链接：https://blog.csdn.net/weixin_52268949/article/details/123085687



easytornado

进入环境就这样子

我们逐一访问看看

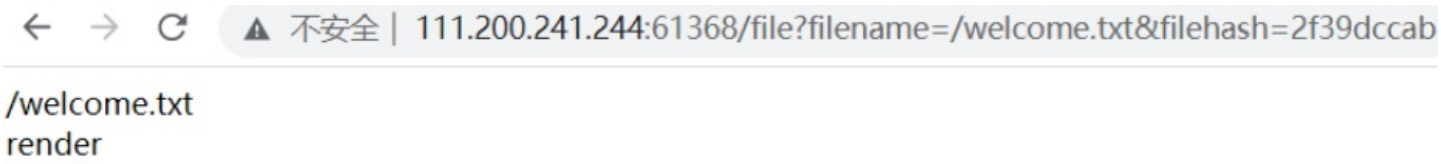


进入flag.txt提示flag in /fllllllllllllag我们访问fllllllllllllag看看

报了一个error，且在浏览器有回显，莫非是模板注入，我们试一试，把error换成456看看浏览器回显

确定有模板注入了但是这里没有更多信息我们只能先放一放了

然后我们去访问welcome.txt看看



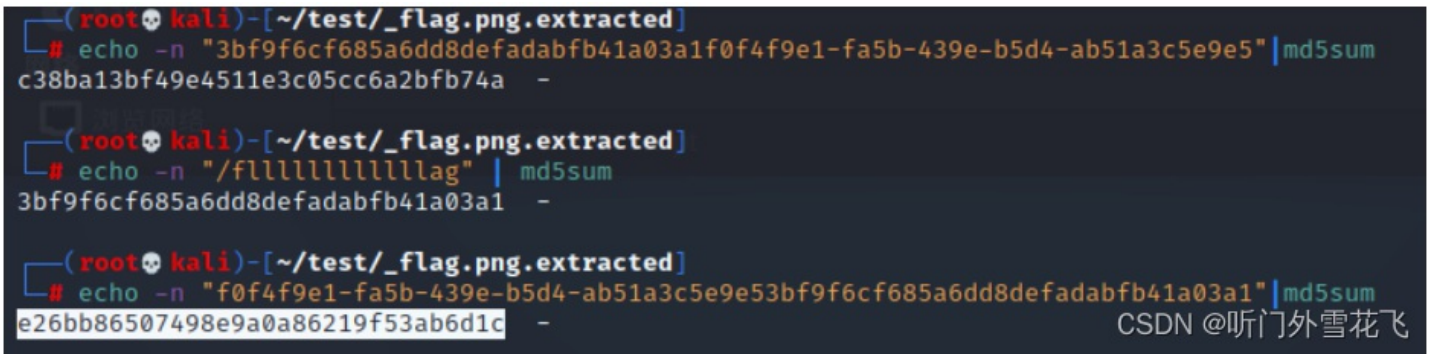
第二个是一个render，render是一个Tomado框架的一个渲染函数，即可以通过传递不同的参数形成不同的页面。

还有个hints.txt我们访问

这个式子的意思先把filename给md5加密一遍，然后加上cookie_secret总体再md5加密一遍，filename我们知道是/fllllllllllag,那我们嘚想办法获得cookie_secret值，这时我们想到我们第二个目录的render函数，那我们可以去Tormado官网看看cookie_secret是在哪个函数里面，通过查阅文档可以构造payload

```
http://111.200.241.244:61368/error?msg={{handler.settings}}
```

{'autoreload': True, 'compiled_template_cache': False, 'cookie_secret': 'f0f4f9e1-fa5b-439e-b5d4-ab51a3c5e9e5'}



然后我们只需要把filename给md5加密然后再加上cookie_secret再MD5加密一次最后构造payload即可拿到flag

```
http://111.200.241.244:61368/file?filename=/flllllllllllag&filehash=e26bb86507498e9a0a86219f53ab6d1c
```