20200812信息安全实训

笔记本:	我的第一个笔记本		
创建时间:	2020/8/12 18:19	**更新时间:**	2020/8/12 19:19
作者:	820410740@qq.com		
URL:	https://blog.csdn.net/wyj_1216/article/details/83043627		

攻防世界
easytornado 进入网站后看到有flag.txt 看到显示 /flllllllllag,考虑filename=/flllllllllllag 显示Error签名错误 考虑服务端模板注入（ssti攻击）尝试输入/error?msg={{1}}，发现存在模板注入 msg={{7*7}} 发现不存在运算 经过尝试发现存在附属文件handler.settings 输入msg={{handler.settings}} 发现'cookie_secret'
进行md5加密（通过打开第二个文件发现需要md5加密）
最后输入 /file?filename=/flllllllllllag&filehash=39995d0191d02ad3f89393a6701f6e73
得到flag

shrine 整理代码发现为flask框架，猜测有ssti注入 仔细看代码发现有两个路径 作为测试代码是发现存在模板注入 flag被放在config文件中
```
{{get_flashed_messages.__globals__['current_app'].config['FLAG']}}
```
注意是在/shrine下的

lottery .git源码泄露 访问robots.txt可以看到.git api.php bp抓包 发现numbers没有检查数据类型 构造几次数据就可以买flag了
由于网站无法注册，无法通关