

首先去github下载owasp zap: <https://github.com/zaproxy/zaproxy/wiki/Downloads> ,用迅雷会员下载比较快;
基础使用方法去freebuf看: <http://www.freebuf.com/sectool/5427.html>
首先要安装https证书、搞了好久找到了下载证书的地方 options->Dynamic SSL Certificates去保存证书,然后导入浏览器

safe mode #安全模式protected mode #保护模式standard mode #标准模式ATTACK mode #攻击模式

在owasp中需要添加断点拦截、同样也有拦截白名单和黑名单的设置,使用如下:

还有他的攻击模式做的比较好,输入网址攻击后会自动发送到spider模块,爬完后自动发送到主动扫描模块,也有扫描进度,可视化效果做的比burpsuite好,后面尝试下主

扫描完后自动转到警告模块可以查看扫描报告,也支持导出html、xml方式报告;
FUZZ模块配置使用貌似木有burpsuite强大、其他的还都是蛮好的,也有编码解码功能等等。
目测owasp-zap的主动扫描模块值得一用,还有下断点会把request和response都下断点返回,默认burpsuite的配置是不拦截response、而owasp-zap默认两个都拦截、

点击收藏 | 0 关注 | 0

[上一篇: 有木有通过社会工程学自动生产用户名...](#) [下一篇: 那些年我们一起学XSS](#)

1. 2 条回复



[ly55521](#) 2017-06-02 16:21:07

沙发。。。

0 回复Ta



[hades](#) 2017-06-02 16:44:38

地毯咯

0 回复Ta

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

[目录](#)

