# 28 WEB漏洞-XSS跨站之WAF绕过及安全修复



#常规WAF绕过思路

标签语法替换

特殊符号干扰

提交方式更改

垃圾数据溢出

加密解密算法

结合其他漏洞绕过

#自动化工具说明：https://github.com/s0md3v/XSStrike

XSStrike主要特点反射和 DOM XSS 扫描

多线程爬虫

Context分析

可配置的核心

检测和规避 WAF

老旧的 JS 库扫描

智能payload生成器

手工制作的 HTML & JavaScript 解析器

强大的fuzzing引擎

盲打 XSS 支持

高效的工作流

完整的 HTTP 支持

Bruteforce payloads支持

Payload编码

-h, --help //显示帮助信息

-u, --url //指定目标URL

--data //POST方式提交内容

-v, --verbose //详细输出

-f, --file //加载自定义paload字典

-t, --threads //定义线程数

-l, --level //爬行深度

-t, --encode //定义payload编码方式

--json //将POST数据视为JSON

--path //测试URL路径组件

--seeds //从文件中测试、抓取URL

--fuzzer //测试过滤器和Web应用程序防火墙。

--update //更新

--timeout //设置超时时间

--params //指定参数

--crawl //爬行

--proxy //使用代理

--blind //盲测试

--skip //跳过确认提示

--skip-dom //跳过DOM扫描

--headers //提供HTTP标头

-d, --delay //设置延迟

#安全修复方案

开启httponly,输入过滤，输出过滤等

PHP:http://www.zuimoge.com/212.html

JAVA:https://www.cnblogs.com/baixiansheng/p/9001522.html

#JAVA XSS平台练习

演示案例：

➢ 手工探针XSS绕过WAF规则

➢ 自动化XSS绕过WAF测试演示

➢ Fuzz下XSS绕过WAF测试演示

➢ 关于XSS跨站安全修复建议测试

涉及资源：

https://gitee.com/yhtmxl/imxss/

https://github.com/3xp10it/xwaf

https://xssfuzzer.com/fuzzer.html

https://github.com/s0md3v/XSStrike

https://bbs.pediy.com/thread-250852.htm

https://github.com/TheKingOfDuck/fuzzDicts