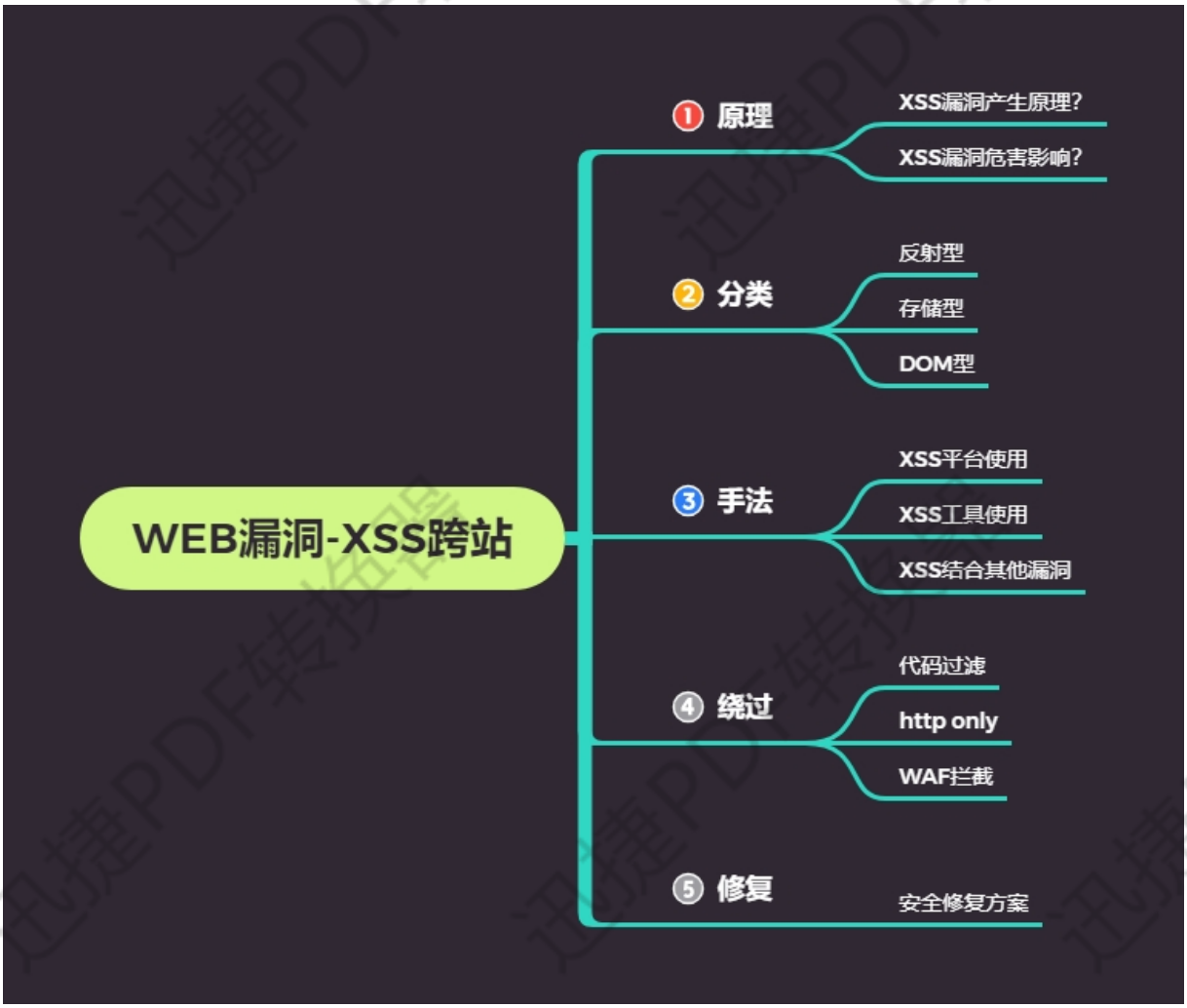
WEB 漏洞-XSS 跨站之 WAF 绕过及安全修复



#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
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
