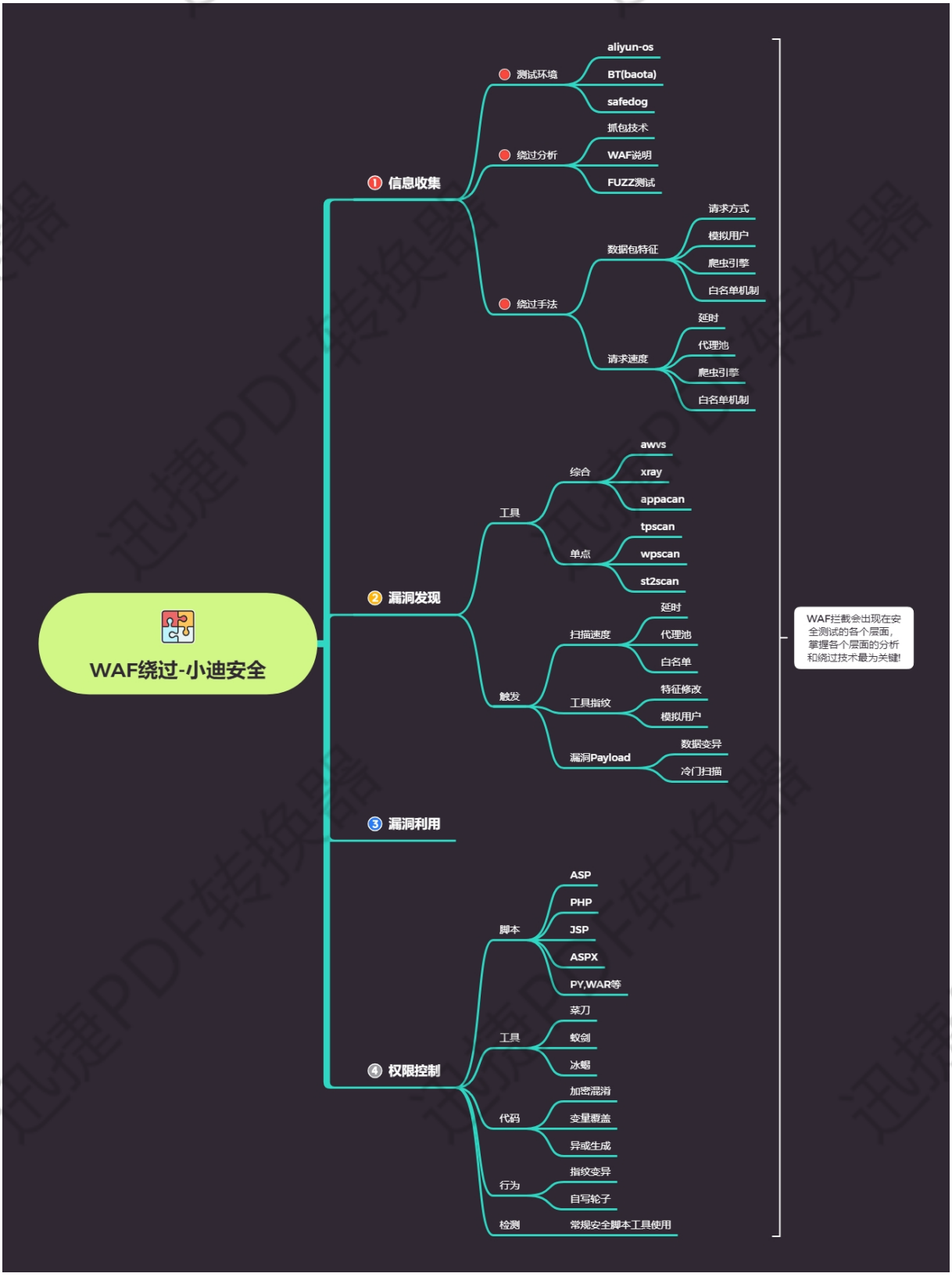
WAF 绕过-权限控制之代码混淆及行为造轮子



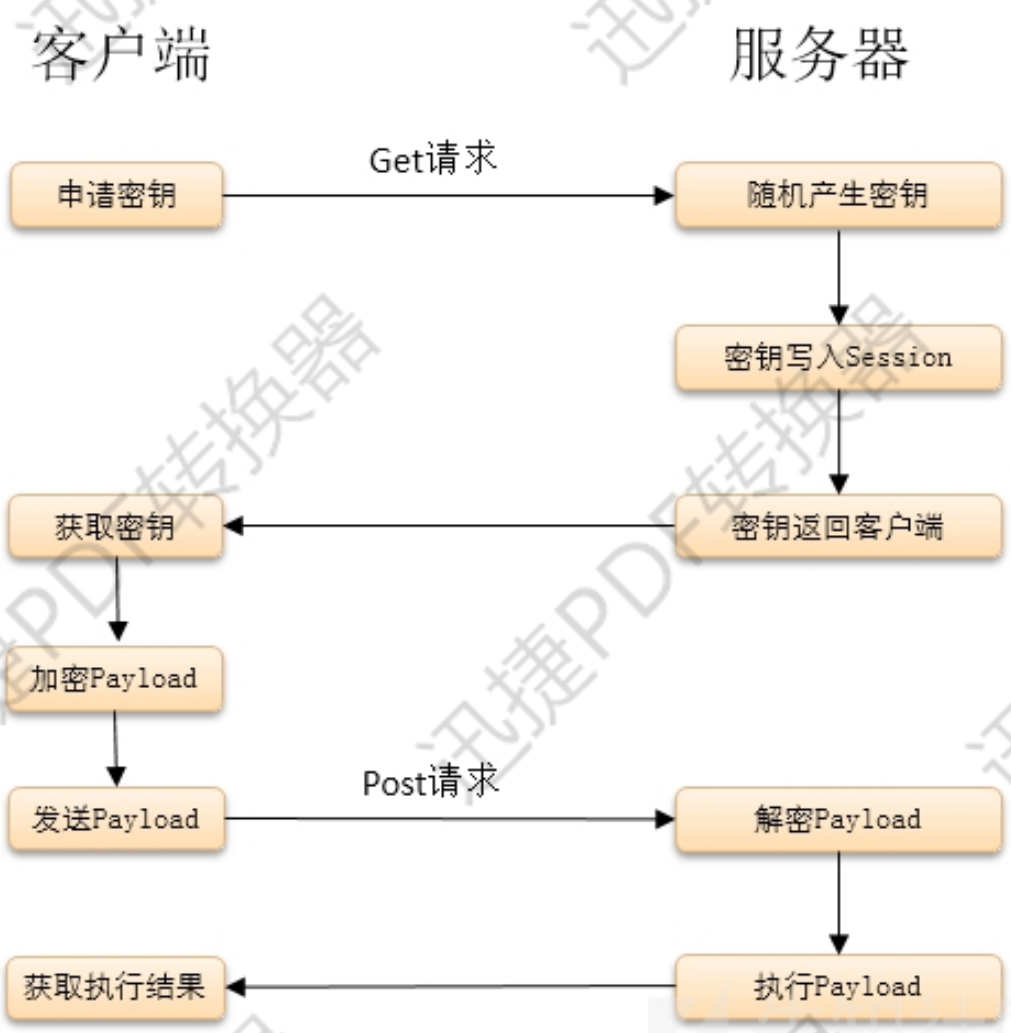
#Safedog 代码层手写及脚本绕过
变量覆盖，加密混淆，异或生成
#BT Aliyun 代码层手写及脚本绕过
编码解码(变量覆盖，加密混淆，异或生成)

ASP,PHP,ASPX,JSP,PY 等后门免杀同理

http://test.xiaodi8.com/x.php?id=x
mr6=cGhwaW5mbygpOw==

http://test.xiaodi8.com/xx.php?x=b&y=assert
z=cGhwaW5mbygpOw== 执行代码
z=ZmlsZV9wdXRfY29udGVudHMoInRlc3QudHh0IiwiMSIpOw== 写入文件
z=dmFyX2R1bXAoc2NhbmRpcigiLiIpKTs= 读取文件

菜刀，蚁剑，冰蝎优缺点
菜刀：未更新状态，无插件，单向加密传输
蚁剑：更新状态，有插件，拓展性强，单向加密传输
冰蝎：更新状态，未知插件，双向加密传输



演示案例：

- Safedog-手写覆盖变异简易代码绕过-代码层
- Safedog-基于接口类加密混淆代码绕过-代码层
- BT,Aliyun-基于覆盖加密变异下编码解码绕过-代码层
- Safedog-基于工具功能数据包指纹修改变异绕过-行为层
- Safedog,BT,Aliyun-基于冰蝎新型控制器绕过全面测试-行为层
- Safedog,BT,Aliyun-基于手写新型控制器绕过全面测试-行为层

涉及资源：

https://github.com/djunny/enphp

https://www.phpjiami.com/phpjiami.html

https://github.com/rebeyond/Behinder/releases/

https://github.com/AntSwordProject/antSword/releases

https://pan.baidu.com/s/1msqO2kps139NNP9ZEIAVHw 提取码：xiao
