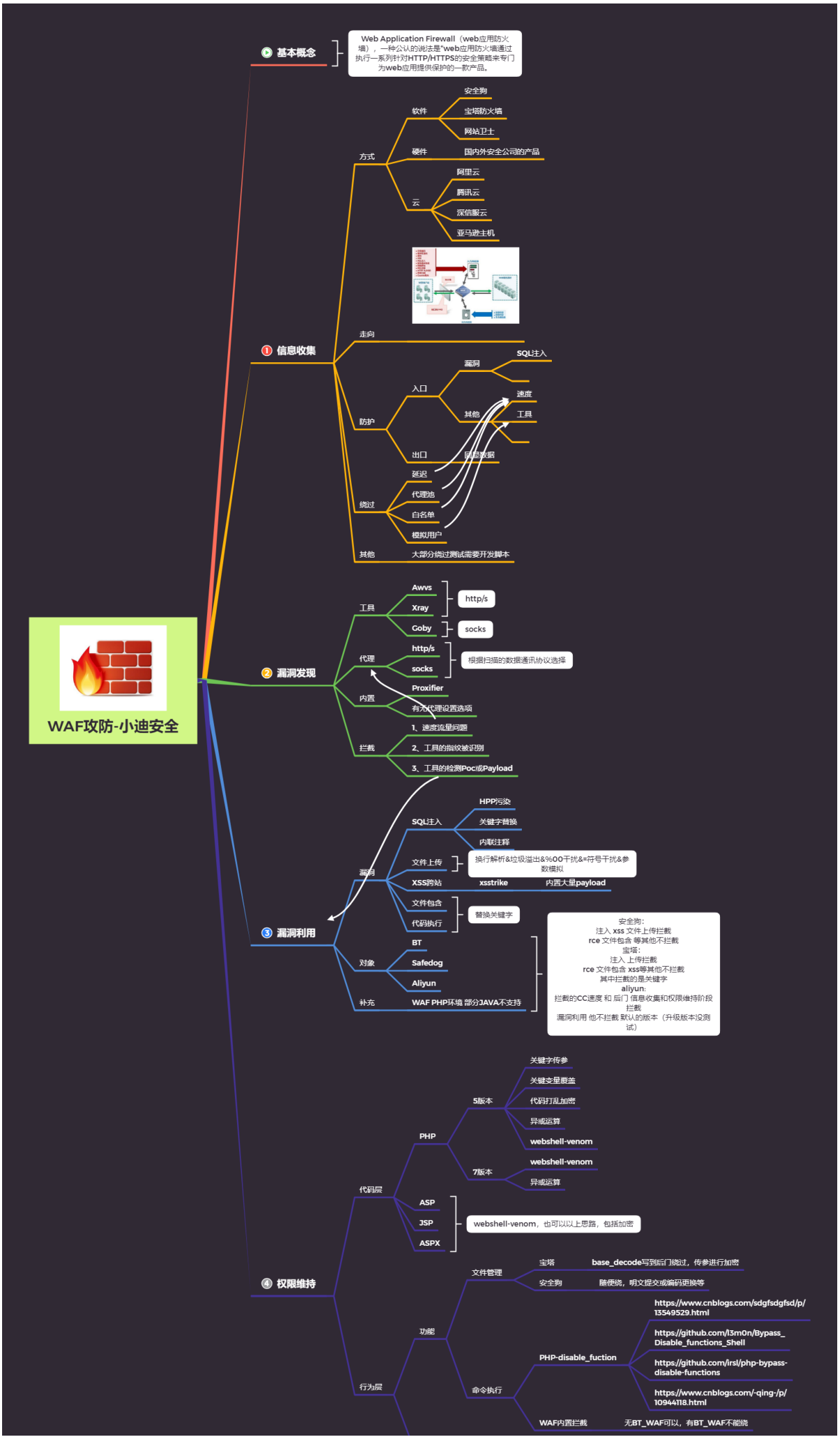
Day79　WAF 攻防-漏洞发现&协议&代理池&Goby&Awvs&Xray


WAF攻防-小迪安全
基本概念
Web Application Firewall（web应用防火墙），一种公认的说法是"web应用防火墙通过执行一系列针对HTTP/HTTPS的安全策略来专门为web应用提供保护的一款产品。
信息收集
方式
软件
安全狗
宝塔防火墙
网站卫士
硬件
国内外安全公司的产品
云
阿里云
腾讯云
深信服云
亚马逊主机
走向
防护
入口
漏洞
SQL注入
其他
速度
工具
出口
同步数据
绕过
延迟
代理池
白名单
模拟用户
其他
大部分绕过测试需要开发脚本
漏洞发现
工具
Awvs
Xray
http/s
Goby
socks
代理
http/s
socks
根据扫描的数据通讯协议选择
内置
Proxifier
有无代理设置选项
拦截
1、速度流量问题
2、工具的指纹被识别
3、工具的检测Poc或Payload
漏洞利用
漏洞
SQL注入
HPP污染
关键字替换
内联注释
文件上传
换行解析&垃圾溢出&%00干扰&=符号干扰&参数模拟
XSS跨站
xsstrike
内置大量payload
文件包含
代码执行
替换关键字
对象
BT
Safedog
Aliyun
补充
WAF PHP环境 部分JAVA不支持
安全狗：
注入 xss 文件上传拦截
rce 文件包含 等其他不拦截
宝塔：
注入 上传拦截
rce 文件包含 xss等其他不拦截
其中拦截的是关键字
aliyun：
拦截的CC速度 和 后门 信息收集和权限维持阶段拦截
漏洞利用 他不拦截 默认的版本（升级版本没测试）
权限维持
代码层
PHP
5版本
关键字传参
关键变量覆盖
代码打乱加密
异或运算
webshell-venom
7版本
webshell-venom
异或运算
ASP
JSP
ASPX
webshell-venom，也可以以上思路，包括加密
行为层
功能
文件管理
宝塔
base_decode写到后门绕过，传参进行加密
安全狗
随便绕，明文提交或编码更换等
命令执行
PHP-disable_fuction
https://www.cnblogs.com/sdgfsdgfsd/p/13549529.html
https://github.com/l3m0n/Bypass_Disable_functions_Shell
https://github.com/irsl/php-bypass-disable-functions
https://www.cnblogs.com/-qing-/p/10944118.html
WAF内置拦截
无BT_WAF可以，有BT_WAF不能绕

1.知识点

- 1、Http/s&Sock5协议
- 2、Awvs&Xray&Goby代理
- 3、Proxifier进程代理使用
- 4、Safedog&BT&Aliyun防护

```
在漏洞发现中，WAF会对三个方向进行过滤拦截：
1、速度流量问题
2、工具的指纹被识别
3、工具的检测 Poc或 Payload
```

2.演示案例

2.1 Awvs漏扫-Safedog-白名单-内置

```
加入白名单扫描，防 Safedog拉黑 IP
```

2.2 Awvs漏扫-BT&Aliyun-代理池-内置

```
加入代理池扫描，防 BT或 Aliyun拉黑 IP
```

2.3 Xray漏扫-BT&Aliyun-Proxifier-进程

```
加入代理池扫描，防 BT或 Aliyun拉黑 IP
```

2.4 Goby漏扫-BT&Aliyun-Socket5-内置

```
加入代理池扫描，防 BT或 Aliyun拉黑 IP
```