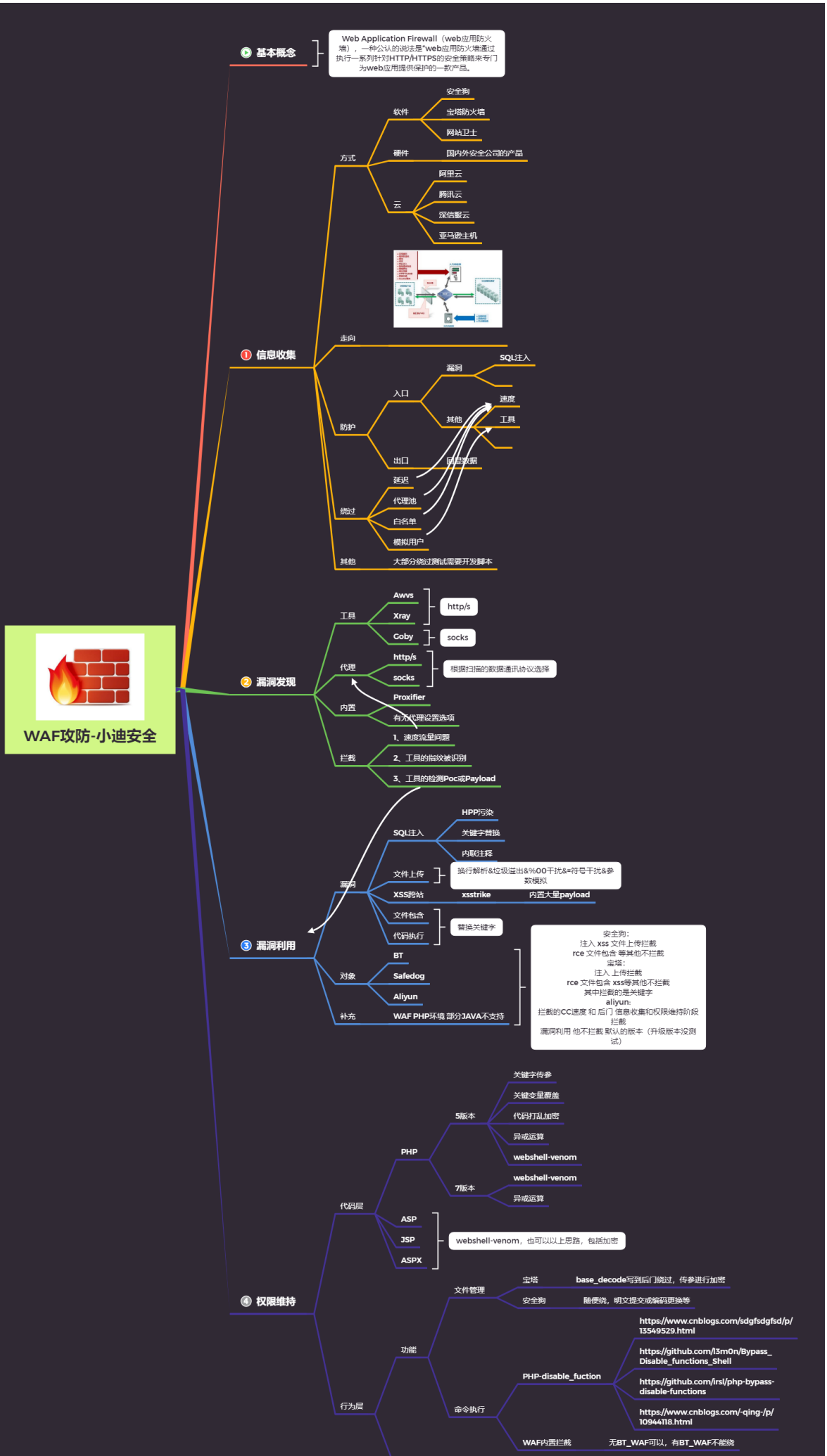
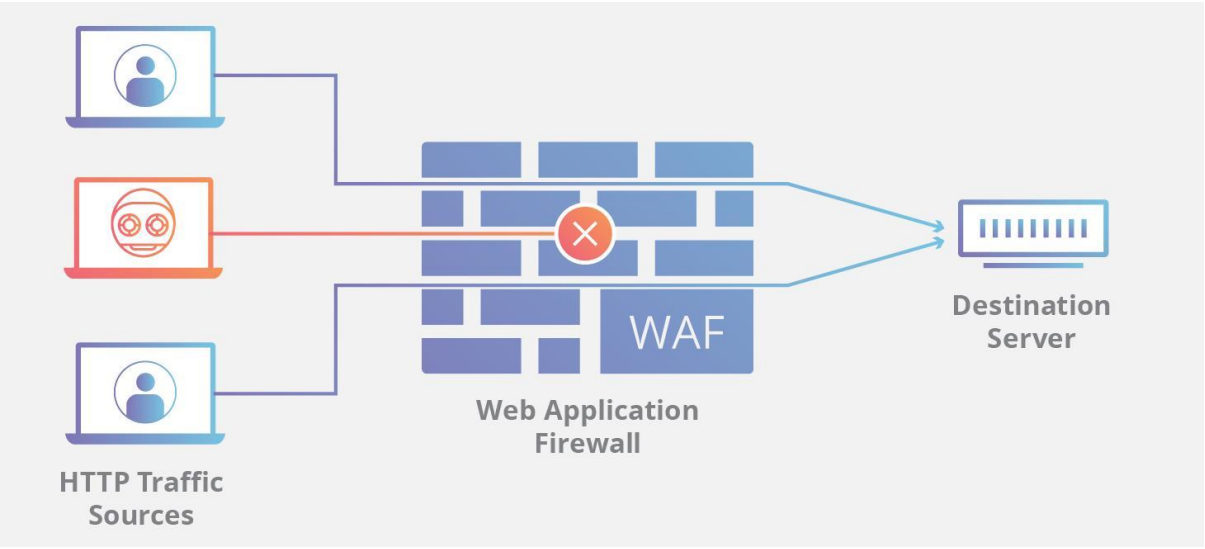
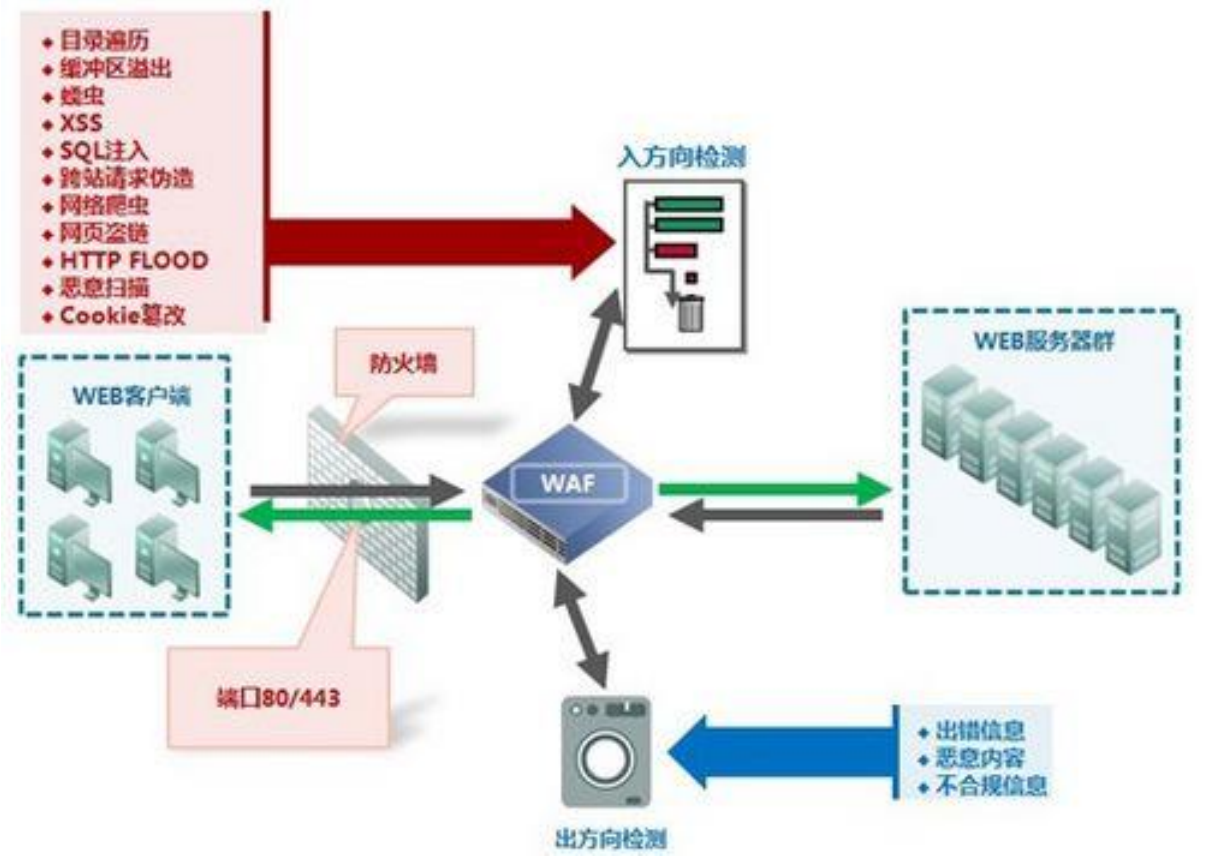
WAF 攻防-信息收集&识别&被动探针&代理池&仿指纹&白名单


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。
① 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
回显数据
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
② 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
有为代理设置选项
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
③ 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）
④ 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


HTTP Traffic
Sources
WAF
Web Application
Firewall
Destination
Server


目录遍历
缓冲区溢出
蠕虫
XSS
SQL注入
跨站请求伪造
网络爬虫
网页盗链
HTTP FLOOD
恶意扫描
Cookie篡改
入方向检测
WEB客户端
防火墙
WAF
WEB服务器群
端口80/443
出错信息
恶意内容
不合规信息
出方向检测

#知识点：

0、WAF 介绍&模式&识别&防护等

1、信息收集-被动扫描&第三方接口

2、信息收集-基于爬虫&文件目录探针

3、信息收集-基于用户&代理池&白名单

#章节点：

WAF 绕过主要集中在信息收集，漏洞发现，漏洞利用，权限控制四个阶段。

#补充点：

1、什么是 WAF?

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。

基本可以分为以下 4 种

软件型 WAF

以软件的形式安装在服务器上面，可以接触到服务器上的文件，因此就可以检测服务器上是否有 webshell，是否有文件被创建等。

硬件型 WAF

以硬件形式部署在链路中，支持多种部署方式。当串联到链路上时可以拦截恶意流量，在旁路监听模式时只记录攻击但是不进行拦截。

云 WAF

一般以反向代理的形式工作，通过配置后，使对网站的请求数据优先经过 WAF 主机，在 WAF 主机对数据进行过滤后再传给服务器

网站内置的 WAF

就是来自网站内部的过滤，直接出现在网站代码中，比如说对输入的参数强制类转换啊，对输入的参数进行敏感词检测啊什么的

2、如何判断 WAF?

Wafw00f，看图识别，其他项目脚本平台

https://mp.weixin.qq.com/s/3uUZKryCufQ_HcuMc8ZgQQ

3、常见 WAF 拓扑&防护?

见上图流量走向&常见漏洞

4、目前有哪些常见 WAF 产品?

演示案例:

- 信息收集-被动扫描-黑暗引擎&三方接口
- 信息收集-目录扫描-Python 代理加载脚本
- 信息收集-爬虫扫描-Awvs&Xray&Goby 内置

#信息收集常见检测：

1、脚本或工具速度流量快

2、脚本或工具的指纹被识别

3、脚本或工具的检测 Payload

#信息收集常见方法：

1、延迟：解决请求过快封 IP 的情况

2、代理池：在确保速度的情况下解决请求过快封 IP 的拦截

3、白名单：模拟白名单模拟 WAF 授权测试，解决速度及测试拦截

4、模拟用户：模拟真实用户数据包请求探针，解决 WAF 指纹识别

#信息收集-被动扫描-黑暗引擎&三方接口

黑暗引擎：Fofa Quake Shodan zoomeye 0.zone 等

其他接口：https://forum.ywhack.com/bountytips.php?getinfo

#信息收集-目录扫描-Python 代理加载脚本

```
import requests
import time

headers={
    'Connection': 'keep-alive',
    'Cache-Control': 'max-age=0',
    'Upgrade-Insecure-Requests': '1',
    'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114
Safari/537.36',
    'Sec-Fetch-Dest': 'document',
    'Accept':
'text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9',
    'Sec-Fetch-Site': 'none',
    'Sec-Fetch-Mode': 'navigate',
    'Sec-Fetch-User': '?1',
    'Accept-Encoding': 'gzip, deflate, br',
    'Accept-Language': 'zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7',
   'Cookie': 'bdshare_firstime=1581597934650;
PHPSESSID=ncsajdvh39qse0qlsgqokshuc4;
yx_auth=dc4fq8FAEkyiAUZ54b5zl9GGStCxXoRb1TFaAaozygMiSc5uZYHjR3gCQ
m%2BtKNz3bcjbTi8BRgcd%2F7LvR0lHN1j319CI6x29Z2QDI38',
}
```

涉及资源:

补充：涉及录像课件资源软件包资料等下载地址