深聊waf那些事儿（二）——安全小课堂第二十六期

2016-09-09 京东安全应急响应中心

安全小课堂第二十六期

waf是web应用防火墙（Web Application Firewall）的简称，对来自Web应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，为web应用提供防护，也称作应用防火墙，是网络安全纵深防御体系里重要的一环。本期我们继续来聊一聊waf那些事儿。

本期邀请到
携程安全专家张亮
唯品会安全专家yy
阿里安全专家破见
大家欢迎~

1

豌豆妹

本期咱们继续来聊waf~请问优秀的开源waf引擎都有哪些呢？

小丸子

在软waf方面，首推当然是modsecurity，其次是基于ngx_lua的lua-resty-waf、ngx_lua_waf，还有就是Naxsi、WAFNinja、raptor_waf，一般基于apache、nginx的waf模块其实都可以，两种都有优缺点，适合业务场景的才是最优秀的。

2

豌豆妹

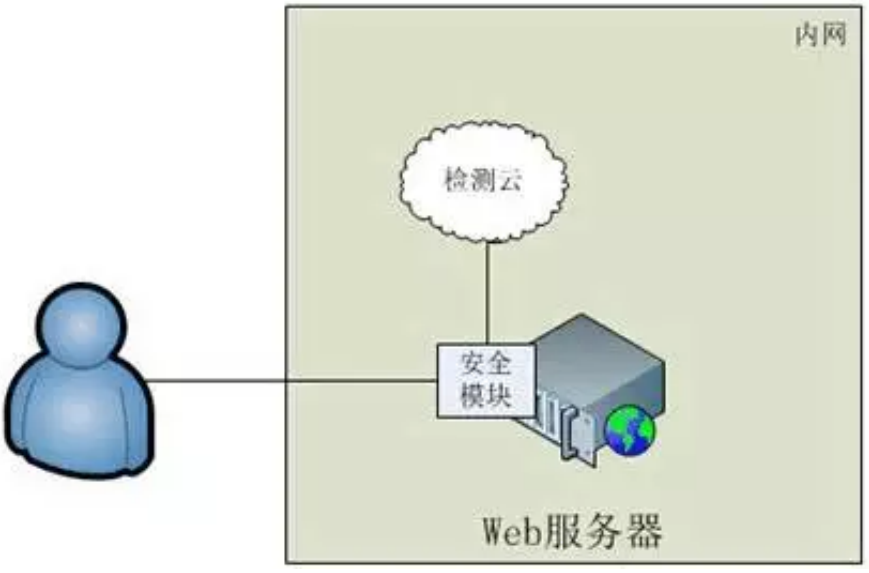
大流量高并发场景下应该选择哪种waf方案？

柴可夫斯基

根据我们自己的经验，基于nginx的waf模块是比较普遍且能够经得起考验的。最好能根据流量情况进行完整架构设计，才能以最小的试错成本达到最大的收益。

哆啦A梦

上面开源的waf都不太适合高并发场景，它们和Web Server 耦合太严重。如下图所示，这样的方式比较适合，把WAF检测引擎和web server分开，这样Web server能力不受waf限制，waf也不受Web server限制。



3

豌豆妹

怎么测试waf的防御能力？

小新 

可根据请求方法、请求方式、请求大小、编码、边界等各种维度去测试，判断响应与所期望的结果是否相同。覆盖面、准确率、覆盖类型、性能、异常也都是很重要的测试点。

葫芦娃 

我是这么做的，核心是第三点：

1、搭建带带漏洞的站点；

2、使用扫描器扫描，覆盖基本盘；

3、waf场景绕过技术的总结，变为标准测试，人工测试绕过。

4

豌豆妹

怎么从waf日志中分析出未知攻击威胁？

小丸子 

waf日志里的通常都是已知的攻击威胁了，如果想要知道未知的攻击威胁，可能需要waf支持粗粒度的特征，然后进行关联分析聚合出还未拦截的攻击威胁。

豌豆妹

怎么从全量日志中分析出未知威胁(0day 、 APT等)来完善waf规则？

哆啦A梦

以攻击特征为策略的waf，不可能做到发现未知攻击。
这个需求不应该属于waf，不符合WAF的定位。根据这个需求，完全可以产生一个新的安全产品，威胁感知、态势感知。

柴可夫斯基

WAF是安全防御的一个环节，不能解决所有问题。做WAF产品，一定要弄清楚定位，发现未知攻击，0day不适合放在WAF上。

豌豆妹

你以为上面的就是本次话题的全部内容？哈哈~太天真，更多干货还在JSRC核心白帽子群呢~想加入JSRC核心白帽子群，拥有和大牛交流沟通的宝贵机会吗？那就快多刷京东漏洞，成为JSRC核心白帽子吧！

安全小课堂往期回顾：

1、论安全响应中心的初衷；
2、安全应急响应中心之威胁情报探索；
3、论安全漏洞响应机制扩展；
4、企业级未授权访问漏洞防御实践；
5、浅谈企业SQL注入漏洞的危害与防御；
6、信息泄露之配置不当；
7、XSS之攻击与防御；
8、电商和O2O行业诈骗那些事儿（上）；
9、电商和O2O行业诈骗那些事儿（下）；
10、CSRF的攻击与防御；
11、账户体系安全管理探讨；
12、远程代码执行漏洞的探讨；
13、服务器安全管控的探讨；
14、畅谈端口安全配置；
15、谈一谈github泄露；
16、撞库攻击是场持久战；
17、url重定向攻击的探讨；
18、聊聊弱口令的危害（一）；
19、聊聊弱口令的危害（二）；
20、聊聊XML注入攻击；
21、聊聊暴力破解；
22、谈谈上传漏洞；
23、浅谈内网渗透；
24、聊聊短信验证码安全；
25、深聊waf那些事儿（一）。

京东安全应急响应中心