



Web应用面临的IT安全风险与危机

孙政豪

目录

背景

威胁

防护

背景

- 1、Web的作用
- 2、Web安全的意义
- 3、Web安全的现状

Web的作用

Web丰富了我们的生活

淘宝网



网上购物



博客论坛



网银缴费



百度糯米

吃喝玩乐

Web安全的意义

电商

- 电商平台如果被不法分子攻破，平台的交易信息就会被不法分子利用，对平台自身和用户带来一定的影响

网金


- 互联网金融直接涉及到金钱，如果被不法分子攻陷，会直接导致金钱的损失。

网乐

- 吃喝玩乐平台是与我们的行为习惯强相关的，如果黑客拿到了我们的行为习惯，可以利用它来进一步获取更多的东西

Web安全对用户或者平台都是很有必要的

Web安全的现状

- ▶ 超过80%的攻击发生在应用层
 - ▶ 多样化的攻击越来越难以防御
 - ▶ Web系统开发商在安全领域投入少
- 

威胁

1、Web常用的攻击方式

2、OWASP Top 10

Web常用的攻击方式

Input Tampering

SQL Injection

LDAP, XPATH,
XQuery Injection

Cross Site Scripting
(XSS)

Exception Handling

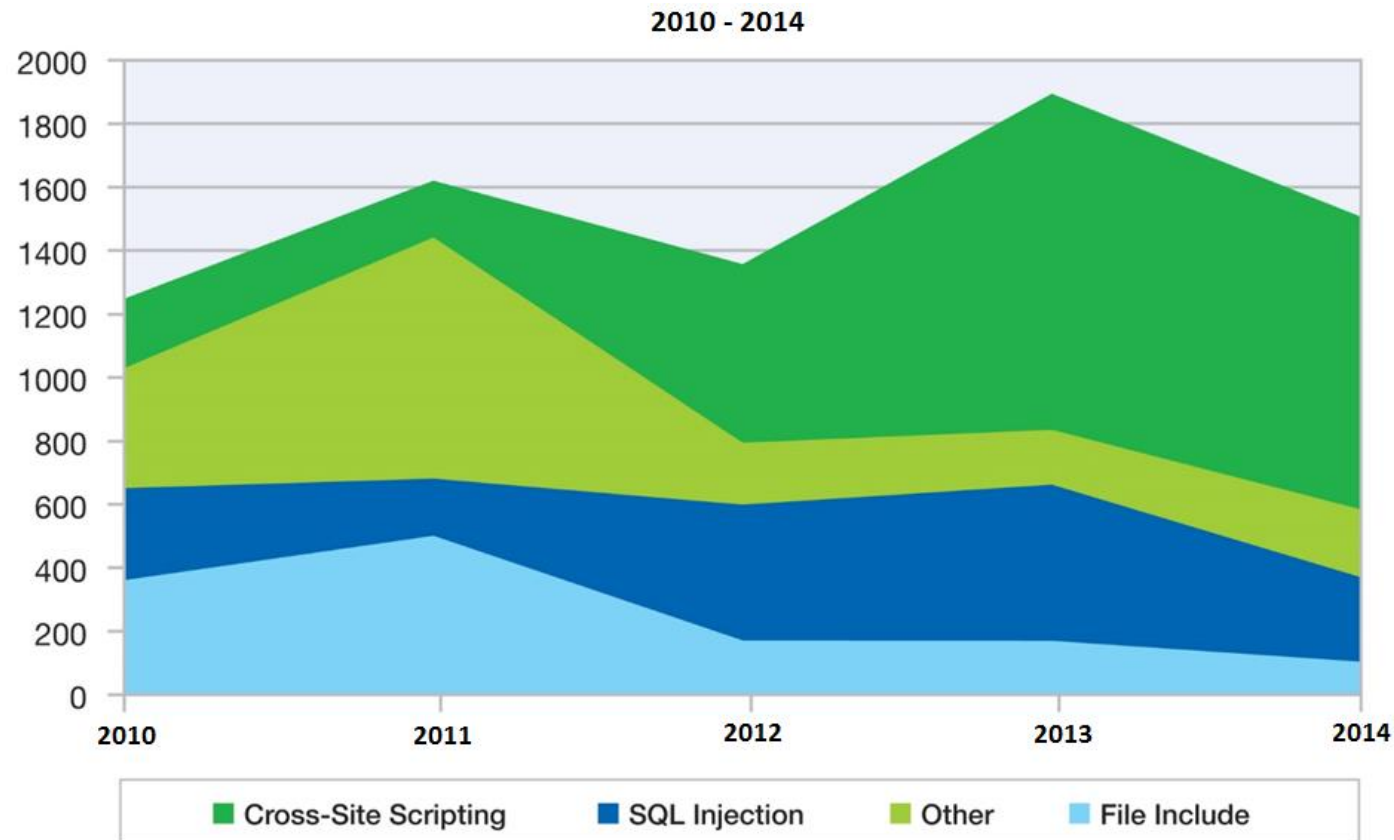
Session
Manipulation

Buffer Overflow

HTTP Parameter
Pollution (HPP)

...and many more

主流的Web攻击方法



资料来源：IBM X-Force®研究与发展

OWASP Top 10

OWASP Top 10 – 2010（旧版）	OWASP Top 10 – 2013（新版）
A1 – 注入	A1 – 注入
A3 – 失效的身份认证和会话管理	A2 – 失效的身份认证和会话管理
A2 – 跨站脚本（XSS）	A3 – 跨站脚本（XSS）
A4 – 不安全的直接对象引用	A4 – 不安全的直接对象引用
A6 – 安全配置错误	A5 – 安全配置错误
A7 – 不安全的加密存储 – 与A9合并成为➔	A6 – 敏感信息泄漏
A8 – 没有限制URL访问 – 扩展成为➔	A7 – 功能级访问控制缺失
A5 – 跨站请求伪造（CSRF）	A8 – 跨站请求伪造（CSRF）
<合并到A6 – 安全配置错误>	A9 – 使用含有已知漏洞的组件
A10 – 未验证的重定向和转发	A10 – 未验证的重定向和转发

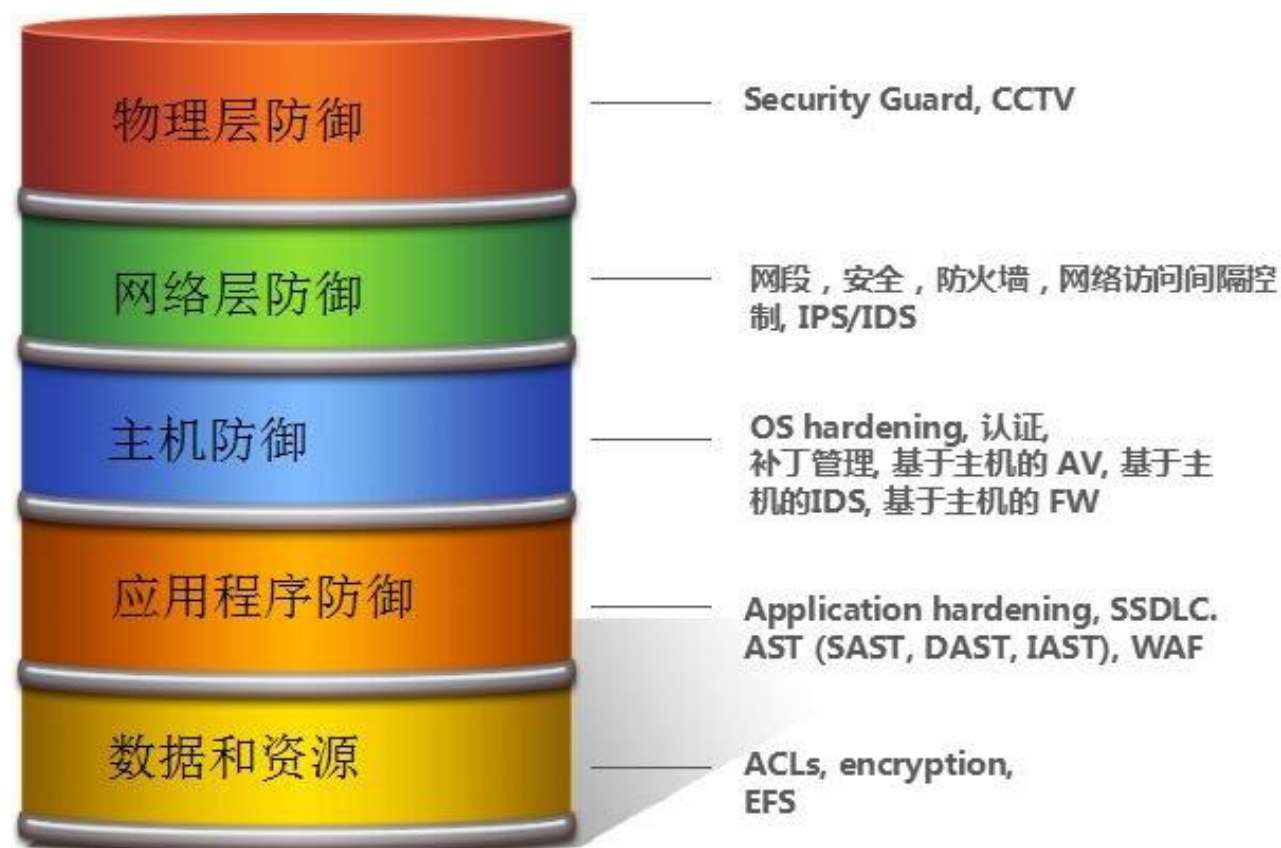
防护

- 1、常见的防护方法
- 2、Web应用防火墙
- 3、运行时应用自我防护

常见的防护方法

- 分层次防御

- 提高攻击者被检测到的概率
- 降低攻击者成功得手的几率

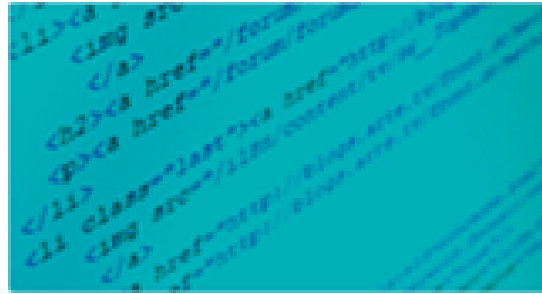


安全软件的开发生命周期-SSDLC





安全领域的指导
人才少见



缺乏安全且有效的流程
指导文档



研发团队往往很少
考虑安全因素

Web应用防火墙

- ▶ Web应用防火墙（WAF）是部署在Web服务器的入口，检测所有进入服务器的报文通过正则表达式的方式匹配报文的特征字段，来判断是否为攻击。

WAF, Web Application FireWall

国际上公认的一种说法：Web应用防火墙是通过执行一系列针对HTTP/HTTPS的安全策略来专门为Web应用提供保护的一项技术。

降低数据泄露风险



用精炼的规则对攻击实施过滤，加上HTTP协议合规检查、状态码过滤等机制，降低数据泄露风险。

支持Web服务可用性



集成DDoS防护功能，与SQL注入防护等功能一起使用，提供多层次攻击过滤，支撑Web服务可用性。

控制恶意访问



支持多种Web访问控制，包括HTTP访问控制、自动化攻击工具识别、控制非法文件上传和下载、阻止盗链和爬虫等。

保护Web客户端



提供CSRF防护、XSS防护、Cookie签名和加密等安全策略，保护Web客户端。

RASP, 运行时应用自我防护

Gartner.

G00269825

Maverick* Research: Stop Protecting Your Apps; It's Time for Apps to Protect Themselves

Published: 25 September 2014

Analyst(s): Joseph Feiman

Modern security fails to test and protect all apps. Therefore, apps must be capable of security self-testing, self-diagnostics and self-protection. It should be a CISO top priority. (Maverick research deliberately exposes unconventional thinking and may not agree with Gartner's official positions.)

实时应用自我保护技术（Runtime Application Self - Protection）也称RASP技术，是2014年9月Gartner的调研员Feiman提出的一种全新概念。他指出，网络的边界逐渐在消失，同时诸如WAF这类的“边界保护”技术也无法深入应用内部，对应用的逻辑数据流理解不全面，由此带来的误杀率高的现象时有发生。

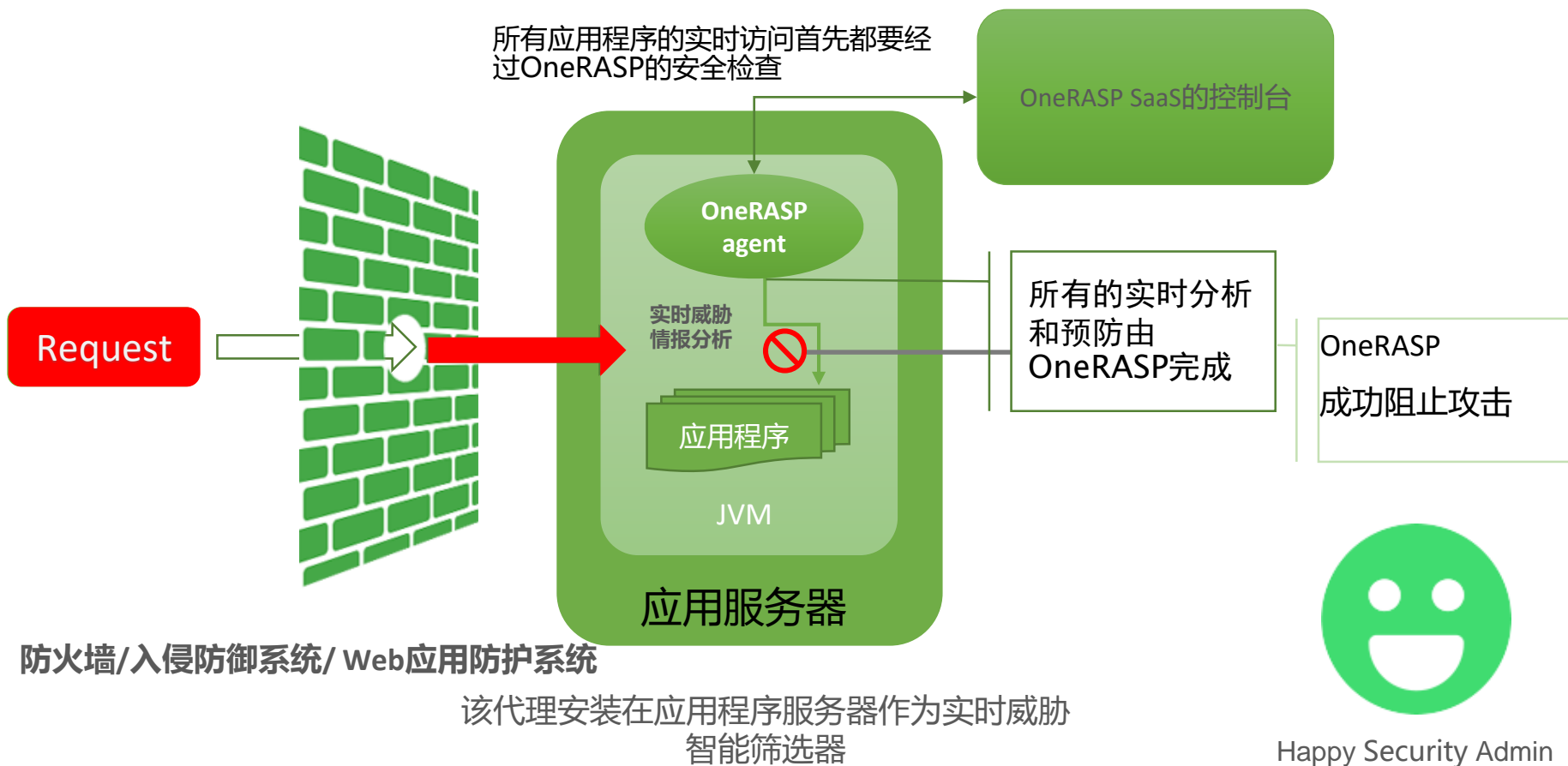
为什么需要 RASP 技术

- 程序完成的太久远，找不到源代码
- 漏洞数量太多
- 缺少安全专家去推动SSDLC
- 开发团队缺乏安全经验
- 第三方供应商的漏洞修复周期长
- 系统中存在未知的漏洞



所以，你需要使用RASP产品打**虚拟补丁**，来保护你的应用程序

RASP 请求示例图



- RASP技术不同与传统的WAF，它像一剂疫苗注入到应用中，与应用一起运行，对外提供服务。
- 结合应用的逻辑和数据流，在运行时对访问应用的代码进行检测，当某种请求与预设置的规则集相匹配时，即可实现攻击的实时阻断，对于已知漏洞来讲，相当于为其打了虚拟补丁，起到补偿控制（没有真正的修复漏洞，却起到了修复漏洞后的效果）的作用，这样研发人员也可以根据自己的时间和精力对漏洞进行修补。
- 但是由于RASP技术是一项全新的概念，且对技术的要求很高，目前国内外真正做这个方面的公司极少。

谢谢！