山石网科智能 Web 防护技术白皮书

随着互联网和移动互联网的快速发展，网站的数量呈现爆发式的增长。根据中国互联网协会和国家互联网应急中心联合发布的数据，截止到 2017 年底，我国网站数量已经超过 526 万个。除了公开的网站，很多企业的业务系统也由传统的 C/S 模式转向更加开放的 B/S 模式。正是由于 Web 技术的开放性，网站和应用系统被不法分子攻击的概率也大大增加，SQL 注入攻击、跨站脚本（XSS）攻击、网站挂马、WebShell 等各种各样的攻击，都会对业务系统造成严重威胁。

Web 安全已经成为攻防对抗的前沿阵地。Verizon 2018 年发布的第 11 期《数据泄露调查报告》显示 (图 1），同 Web 应用程序相关的安全事件数量并不是最多的，但最终导致数据泄露的次数确是最多的。在 Web 应用防火墙已经成为企业级用户标准配置的情况下，针对 Web 应用程序的攻击仍然有着如此高的杀伤力，可见 Web 安全所面临的挑战是非常严峻的。

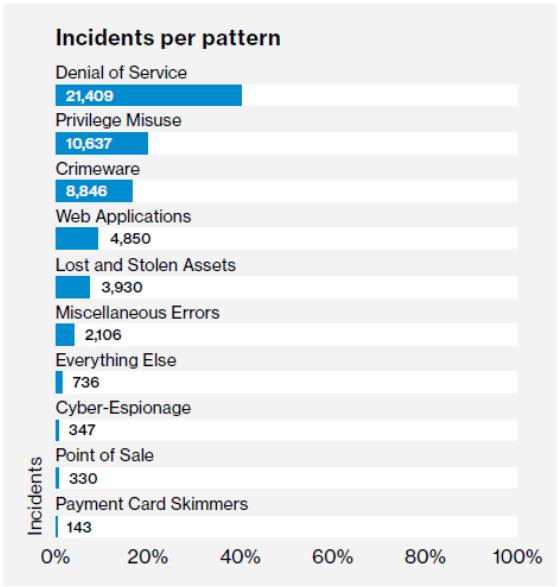

Figure 26. Percentage and count of incidents per pattern (n=53,308)

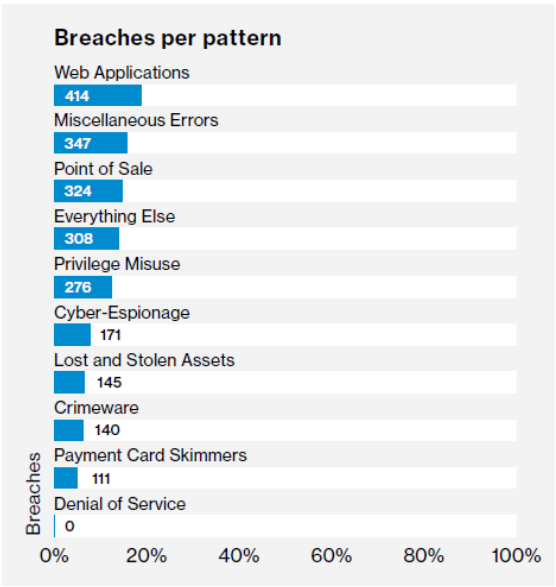

Figure 27. Percentage and count of breaches per pattern (n=2,216)

图 1：安全事件和数据泄露的发生方式对比

1、Web 安全防护面临的挑战

目前的 Web 安全防护措施通常更注重对外部攻击的防御，忽视对内部安全风险的发现和应对。但实际上，Web 安全防护的挑战一方面来自于外部安全形势的变化：对于不断出现的新的 Web 攻击方法，安全设备需要有自适应的应对策略；另一方面也需要不断提升内部的安全管理能力：随时掌握 Web 资产的变化，识别 Web 资产存在的漏洞和风险并及时应对。

- **Web 资产状态的掌握**

随着业务的扩展，网站的数量越来越多。以高校的应用为例，每个院系甚至不同的实验室都有独立维护的网站，此外还有校园 OA、一卡通、选课系统等诸多业务系统，而且这些业务系统通常归属不同的部门来管理。作为整体安全策略的制定和施行者，安全管理人员需要掌握 Web 资产的运营状态，避免防护遗漏而致其成为黑客攻击的靶机。

- **网站漏洞的发现和修复**

网站和业务系统之所以能够被攻击，最根本的原因还是因为其具有能够被利用的安全漏洞。这些漏洞可能是网站应用程序或 Web 框架自己的漏洞，比如近年来多次披露的 Struts2 框架漏洞；也可能是应用程序开发中对安全的重视不够而引入的，比如大部分的 SQL 注入漏洞、XSS 攻击漏洞等。不管是哪种漏洞，都需要及时发现并进行修复，避免成为黑客可以利用的攻击踏板。

- **针对未知 Web 攻击的防护**

多数的攻击行为可以通过特征签名和正则匹配的方式来发现，但对于无法明确攻击特征的未知威胁，也需要有相应的发现和处理手段。比如在网络边界的位置，通常利用网络流量分析（NTA）、沙箱（Sandbox）等安全技术来发现未知威胁。对于应用层威胁，由于访问行为和业务类型、网站结构，甚至不同网页的具体情况密切相关，需要有更深入的分析手段。

- **攻击的定位和误报的处理**

作为最常用的 Web 安全防护设备，Web 应用防火墙（WAF）在使用中很难实现 100% 准确的告警，我们需要有效的手段来对威胁日志进行分析，消除误报，否则管理员很容易淹没在海量告警中，而无法去发现真正有威胁的攻击。

2、山石网科智能 Web 防护技术

山石网科 Web 应用防火墙是新一代专业 的 Web 应用安全防护产品，可以帮助客户应对 OWASP TOP10 风

险，并针对 Webshell、网站挂马、暴力破解等各种 Web 攻击进行防御。针对目前 Web 安全防护所面临的挑战，山石网科 Web 应用防火墙在 Web 资产发现、漏洞评估、流量学习、威胁定位等方面全面应用智能分析和机器学习技术，帮助用户更轻松、更全面的部署 Web 安全防御策略，屏蔽 Web 漏洞和风险，确保网站的运营安全。

• 智能的资产发现

要有效的部署安全策略，首先要了解自己的系统和业务。传统的资产管理方式，需要安全管理员汇总各业务部门的网站信息，费时费力。山石网科 Web 应用防火墙提供智能资产发现功能，帮助用户主动发现并确认业务系统内的 B/S 网站信息，包括 IP 地址、业务端口、是否启用了 HTTPS 等，并将发现的网站一键添加为保护对象，确保不会遗漏任何一个网站的保护。

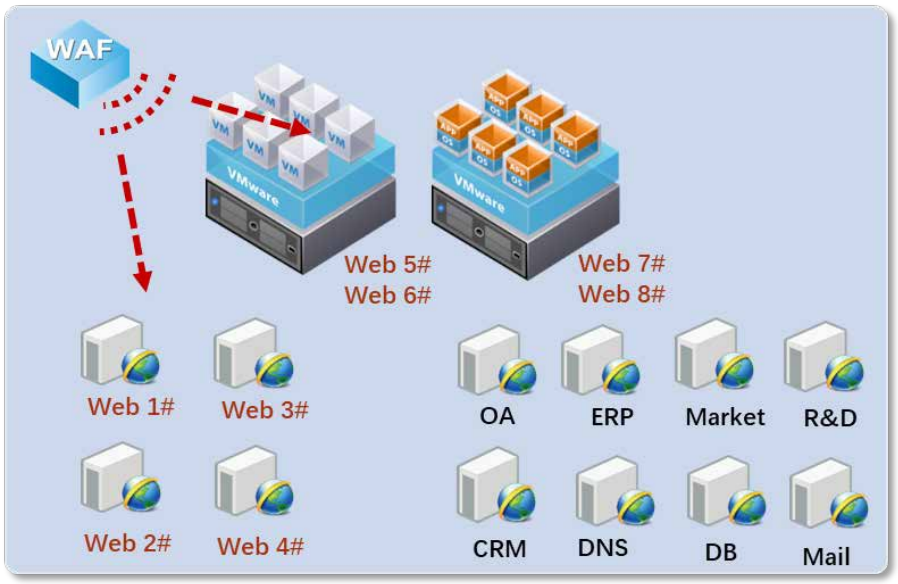

图 2、利用站点自发现定义需要保护的 Web 主机

• 智能的虚拟补丁

安全漏洞的存在是网站被攻击的最重要原因。根据 Trustwave 的统计，高达 99.7% 的 Web 应用系统都会存在安全漏洞，而平均每个 Web 应用系统的漏洞数量高达 11 个。因此，掌控 Web 资产的漏洞状态，做到知己知彼，是制定网站安全策略的重要前提。山石网科 Web 应用防火墙集成了 Web 应用漏洞扫描功能，可以定期对网站和应用系统进行扫描，发现漏洞并提醒用户进行修复。山石网科 Web 应用防火墙同时还支持智能虚拟补丁功能，对存在漏洞的 URL 页面进行针对性防护，将针对漏洞的利用行为拦截。虚拟补丁对于一些老旧应用系统来说特别适用，这些应用可能采用了比较老的操作系统、Web 应用程序，存在的漏洞比较多。针对服务器的修复时间较长会影响业务，采用虚拟补丁则可快速提供保护。

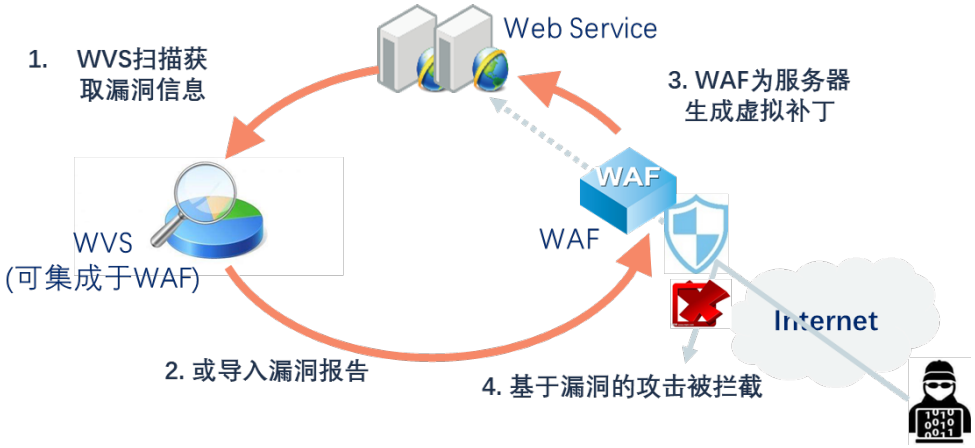

图 3、通过漏扫和虚拟补丁为 Web 漏洞提供快速保护

• 智能的流量自学习

对于 SQL 注入、跨站脚本攻击等主流的应用层攻击，一般是通过特征签名和正则匹配来进行检测，即基于黑名单的检测方式。但基于黑名单的检测方式无法发现特征不明确的攻击行为，而且容易出现误报。另一种检测思路是采用白名单的检测机制，即对网站的流量进行学习并建立流量模型，后续发现同正常访问行为违背的流量则认为是异常流量。山石网科 Web 应用防火墙同时采用了这两种检测机制，可以对网站的动态 URL、URL 参数、COOKIE、IP 分布等内容进行智能的机器学习，学习完之后管理员还可以对学习结果进行优化和校正，最终生成网站的动态 URL 树，并为这棵的每一条动态 URL 建立安全基线，提供个性化保护。

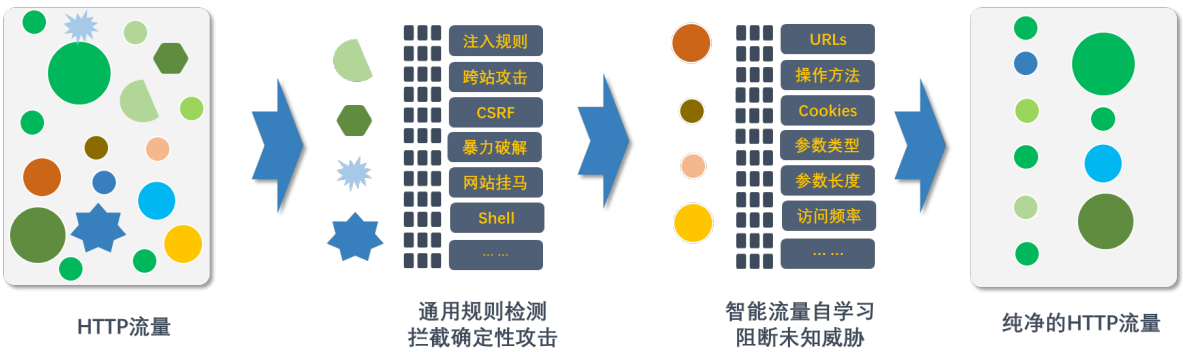

图 4、通过流量自学习发现未知威胁

• 智能的日志聚合

Web 应用防火墙在实际部署中，需要根据具体的业务流量和上下文对告警日志进行分析，并相应调整防护规则，取得更高的检测效果。对于某个攻击特征，在 A 业务场景下是攻击，在 B 业务场景下可能是误报。另一方面，单一的威胁事件可能是误报，但结合上下文进行分析则可能是攻击行为，比如：通常采用 GET

操作来访问的 URL，检测到了某个用户的 POST 操作，这个异常操作本身并不意味着攻击行为，但我们继续分析这个用户 IP，发现它还上传了一个可执行文件，同时对内网的某个网段进行了扫描，那么就可以断定这个 IP 是在进行攻击尝试。要从海量日志中发现真正有威胁的攻击，就要求 Web 应用防火墙具备丰富的日志展现和关联分析手段。山石网科 Web 应用防火墙的日志可以提供各个维度的分析信息，并提供了强大的智能聚合能力，可以按照攻击特征、攻击源等角度对日志进行聚合。按照攻击特征的聚合，能够从攻击频次、攻击者分布角度入手，屏蔽掉客户端普遍发生的误报率高的告警，避免对安全管理员产生干扰；按照攻击源角度的聚合，可以根据时间轴对同一 IP 触发的不同告警进行详细分析，结合攻击者的 Payload 信息，发现真正有威胁的攻击并将攻击者添加到黑名单。

图 5、通过智能的日志聚合定位真正的攻击

3、总结

Web 应用防火墙的部署和防御效果对于确保应用层安全有着至关重要的作用。但由于 Web 应用系统的规模日趋庞大，以及 Web 应用防火墙本身的专业性，要全面发挥它的防护作用也是需要很多的技巧。山石网科 Web 应用防火墙通过智能分析和机器学习等技术的应用，让防护策略和威胁分析变得更加简单，帮助用户更轻松得应对应用层风险和未知攻击，保护业务系统的稳健运营。

Copyright © 2018，Hillstone Networks版权所有，保留所有权利。
Hillstone、Hillstone Networks标识、山石网科、StoneOS、StoneManager、Hillstone PnPVPN、UTM Plus均为Hillstone Networks所属商标。所有其他商标和注册商标均为其各自公司的财产。
本文所包含信息可能会有所修改，恕不另行通知，如需最新信息请浏览Hillstone Networks网站(www.hillstonenet.com.cn)。