JUMING 聚铭

聚铭 Web 应用防护系统
产品白皮书

聚铭网络科技有限公司

目 录

声明

在本文中如无特别说明，聚铭网络均指南京聚铭网络科技有限公司和北京聚铭信安科技有限公司。

JUMING 聚铭图标为聚铭网络的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系聚铭网络技术服务部。

联系信息

南京总部：南京市雨花台区软件大道180号南京大数据产业基地7栋4层

电话：025-52205520/52205570

传真：025-52205565

全国服务热线：400-1158-400

网址：www.juminfo.com

产品支持：support@juminfo.com

一、 前言

Web 应用平台的应用范围有哪些？

随着计算及业务逐渐向数据中心高度集中发展，Web业务平台已经在各类政府、企业机构的核心业务区域，如电子政务、电子商务、运营商的增值业务等中得到广泛应用，很多企业都将应用架设在Web平台上，Web成为一种普适平台。

Web 应用带来的威胁有什么？

Web业务的迅速发展也引起了黑客们的强烈关注，他们将注意力从以往对传统网络服务器的攻击逐步转移到了对Web业务的攻击上。黑客利用网站操作系统的漏洞和Web程序的SQL注入漏洞等得到Web服务器的控制权限，轻则篡改网页内容，重则窃取重要内部数据，更为严重的则是在网页中植入恶意代码，使得网站访问者受到侵害。

当前网络上75%的攻击是针对Web应用的。这些攻击可能导致网站遭受声誉损失、经济损失甚至政治影响。各类网站客户已逐渐意识到Web安全问题的重要性，但传统安全设备（防火墙/IPS）解决Web应用安全问题存在局限性，而整改网站代码需要付出较高代价从而变得较难实现。同时，很多关系国计民生的重要网站，面临监管机构安全合规的要求。

如何解决 Web 应用安全问题？

面对来势汹汹的Web安全威胁，政府、教育、企业为了保护好自身的Web服务器绞尽脑汁。Web服务器在交互性增强的同时，也带来了更高的网络危险性、混乱性和复杂性。

- 如何防止 Web 服务器、数据库服务器被窃取信息？
- 如何验证用户提交数据的安全性？
- 如何防止黑客上传木马、控制服务器？

Web应用防护系统的出现，使Web应用安全的问题迎刃而解。

二、 来自 Web 的安全威胁

目前中国互联网发展迅猛，Web应用越来越为丰富的同时，Web服务器以其强大的计算能力、处理性能及蕴含的较高价值逐渐成为主要攻击目标，层出不穷的网络安全问题仍然难以避免。利用分网页篡改获得经济利益现象普遍；个人信息泄露引发的精准网络诈骗和勒索事件增多；移动互联网恶意程序的传播渠道转移到网盘或广告平台等网站。SQL注入、网页篡改、网页挂

马等安全 事件，频繁发生。针对Web的攻击事件也在不断增多，常见来自Web的安全威胁有几下几种：

1. SQL 注入
2. 木马上传
3. 远程溢出
4. XSS 跨站脚本
5. 本地、远程包含漏洞利用
6. 重要信息窃取
7. 验证、认证绕过
8. Cookie、Session 劫持
9. 网站挂马
10. 数据库信息泄露
11. 应用层 DOS 攻击

三、 新一代的 Web 应用防护技术

从安全角度考虑，针对目前泛滥的SQL注入、跨站脚本、应用层DDoS等Web应用攻击，提供有效检测、防护，降低攻击的影响，最为理想情况，解决根本问题是对Web应用代码进行整改，严格遵循安全编码，确保网站安全。但通常，我们会发现为此付出的代价过大，对正常业务开展有很大影响。

Web应用防护系统以解决诸如防火墙一类传统设备束手无策的Web应用安全问题。与传统防火墙不同，WAF工作在应用层，因此对Web应用防护具有先天的技术优势。基于对Web应用业务和逻辑的深刻理解，WAF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，从而对各类网站站点进行有效防护。

四、 安全防护机制

1. 基于规则库的防护

WAF提供了灵活和丰富的内置规则库，以满足各种用户的需要。一个WAF安全策略由一系列的规则集组成，每一个规则集定义了对一个具体的攻击采用什么样的响应动作。Web管理界面提供了按照攻击的严重级别、攻击的分类、规则的使能状态、响应动作进行规则配置处理的手段，大大简化了用户的操作

通过规则库匹配，WAF能够对攻击行为的防护：

- SQL 注入攻击（包括 URL、POST、Cookie 等方式的注入）
- XSS 攻击、CSRF 攻击
- Web 常规攻击（包括远程包含、数据截断、远程数据写入等）
- 命令执行（执行 Windows、Linux、Unix 关键系统命令）
- 危险存储过程执行
- 缓冲区溢出攻击
- 数据库信息窃取、泄露
- 网站挂马
- 扫描器探测
- 恶意代码
- “零日”攻击

2. Webshell 的识别

传统的Webshell上传防护是通过特征库匹配方式来辨别木马、后门，但是特征库是有限的，如果特征库中没有该特征，或者对Webshell木马稍加改动，即可绕过防护设备。

Web应用防护系统的Webshell防护拦截，并不是基于传统特征库匹配方式，而是通过动态检测监控代码中的敏感函数情况，提取内容特征和统计特征的方式，对webshell连接工具的通信流量进行识别的检测方案，自动对系统Webshell木马，进行实时探测并拦截，从而大大降低被绕过的风险。

3. 错误信息的防护

很多情况下，服务器的报错信息会暴露网站的绝对或相对路径、网站部分源码、SQL语句信息等，自动对返回的错误信息进行过滤，禁止外界可以看到服务器报错信息，有效对数据库内部信息进行防护。

4. 自定义规则的防护

针对有能力的高级用户，还提供了自定义和编写规则内容的功能。用户可以编写自己的规则，支持字符串快速匹配与正则匹配。

五、 主要技术优势

1. 高并发处理技术

Web应用防护系统，基于协议优化的检测引擎，对网络协议底层的深层次的优化，可以达到百万级别的并发连接。

2. 快速特征库匹配技术

特征库主要用于检测各类已知攻击，对网络中传输的数据包进行高速匹配，确保能够准确、快速地检测到此类攻击。规则库进行支持与匹配，提供高品质的攻击特征介绍和分析，基于高速、智能模式匹配方法，能够精确识别各种已知应用攻击，保证第一时间检测到攻击行为。

3. SQL 语句识别技术

Web应用防护系统可以通过识别注入攻击中使用的SQL语句，识别SQL语法结构，而不是通过简单的select/insert/update等简单的SQL关键词的字符串匹配。在对攻击的识别和准确率上可以大大提高。

4. 多种编码还原技术

Web应用防护系统可以有效防止黑客利用大小写变换、ASCII编码、UNICODE编码、注释、混淆等方式绕过检测引擎。解码模块可以将复杂编码后的数据还原为最基本的数据格式进行匹配。

5. 识别扫描行为特征

Web应用防护系统能够设置扫描防护规则，识别扫描行为和扫描器特征，阻止攻击者或扫描器对网站的大规模扫描行为，帮助Web业务降低被入侵的风险并减少扫描带来的垃圾流量。将短时间内访问当前防护对象下大量无效目录，自动拉入黑名单，在一段时间内对该攻击源的所有请求执行拦截。

6. CC 安全防护技术

CC安全防护是为了防御CC攻击，CC主要是用来消耗服务器资源的，攻击者控制某些主机不停地发大量数据包给对方服务器造成服务器资源耗尽，一直到宕机崩溃。Web应用防护系统可以设置CC防护规则，拦截针对网站页面请求的CC攻击，并返回拦截提示页面，避免恶意入侵长

时间占用消耗服务器的核心资源，造成服务器性能异常问题。确保网络数据中心稳定运行，解决因恶意请求导致网站业务响应缓慢或无法正常提供服务。

7. API 业务防护技术

随着Web应用通过广泛使用应用编程接口(API)从互连扩展到协作，让已经存在的安全问题变得更加复杂，API防护可以保护应用免受通常可逃过传统防火墙检测的API攻击。

Web应用防护系统借助可通过速率限制、行为分析和防自动化来保护 XML、JSON的独特防御机制，可自动检测应用程序接口威胁，为API接口提供严格的策略规则，并阻止各类攻击和特殊内容类型，从而将应用威胁拒之门外。