科普：Web应用程序防火墙（WAF）是个啥？是如何防护网站的？

产品名称	科普：Web应用程序防火墙（WAF）是个啥？是如何防护网站的？
公司名称	广州微码互联科技有限公司
价格	.00/件
规格参数	
公司地址	天河区中山大道中379号
联系电话	13480273125 13480273125

产品详情

Web应用程序防火墙（有时也简称为WAF）可以通过监视和过滤Internet与网站之间的HTTP通信来保护网站。

一个WAF可以防止网站受跨站请求伪造的喜欢（被攻击CSRF），本地文件包含（LFI），SQL注入，跨站点脚本（XSS），等等。

70%—80%的应用程序中有待利用的严重漏洞，消除这些漏洞至关重要。

企业必须使用一系列专门针对OSI的每个级别的工具（第3层网络级别的过滤和第7层应用程序级别的过滤）来针对多种不同的攻击媒介提供整体防御。

应用程序和密码设置永远不会完全完美，因此确保保护数据免受分布式拒绝服务（DDoS）攻击，不良僵尸程序和垃圾邮件的侵害很重要，最重要的在应用程序中建立针对业务逻辑漏洞的防御机制。

攻击or防护是如何进行的？

一个Web应用防火墙位于客户机和他们想连接到互联网服务之间，由WAF检查这些连接，因为它们首先被路由到它。

跨站点脚本是最常见的流行应用程序攻击媒介之一，它涉及攻击者向客户端的浏览器中注入恶意代码，修改用户设置，盗取/污染cookie，窃取机密数据，甚至更改内容显示虚假信息。

WEB应用防火墙还具有多面性的特点。比如从网络入侵检测的角度来看可以把WAF看成运行在HTTP层上的IDS设备;从防火墙角度来看，WAF是一种防火墙的功能模块;还有人把WAF看作“ 深度检测防火墙 ”的增强。

WAF可以防御的另一种威胁是服务器配置错误。来宾帐户和默认密码之类的不安全设置通常容易成为攻击者的目标，因为管理员没有遵循zuijia安全性做法，因此创建了这些漏洞。

输入验证效果不佳的网站可能容易受到代码注入漏洞的攻击，这使攻击者试图让SQL语句潜行以访问未经授权的数据库。WAF可以检测并阻止这些尝试。

过时的库和软件也是易受攻击的领域，但Web应用程序防火墙可以用作临时解决方案，并阻止这些漏洞，并对其进行修补。

监视和日志记录不足也可能导致恶意活动的早期迹象被忽略，但是WAF可以充当集中式日志记录点，并通知管理员任何正在进行的威胁。并且在达到极限值时进行处理。这对暴力攻击的识别和响应是十分有利的。

攻击者还可能试图通过扫描网站的结构后利用不安全的框架获取敏感信息的访问。Web应用程序防火墙可以锁定网站的某些区域，以便只有受信任方才能访问它们。

WAF还会通过单一入口点实施地理，IP和基于身份的验证政策。增强输入验证，可以有效防止网页篡改、信息泄露、木马植入等恶意网络入侵行为。从而减小Web服务器被攻击的可能性。

现实情况是，一周中的每一天都在对网站进行黑客攻击，一项研究表明，网站遭受攻击的平均频率是每39秒一次。当然，攻击不一定等同于成功的黑客攻击，Web应用程序防火墙的工作就是确保不会成功。

最常见的应用程序攻击类型包括SQL注入，分布式拒绝服务（DDoS），污损，恶意软件和帐户劫持。SQ注入占所有Web攻击的三分之二。

Web应用的CC攻击，是网络安全领域的难题之一，如何做到智能高效地防护CC，是行业内的重点关注话题。