守护者也会有漏洞防火墙不是万能的 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/267/2021_2022__E5_AE_88_E6_8A_A4_E8_80_85_E4_c101_267025.htm 凭防火墙再也不足以保护网上资产。如今，黑客及其攻击策略是越来越精明、越来越危险。当前的一大威胁就是应用层攻击，这类攻击可以偷偷潜入防火墙、直至潜入Web应用。没错，这类攻击有不少喜欢把宝贵的客户数据作为下手目标。 那么，为什么普通防火墙阻止不了这类攻击呢？因为这类攻击伪装成正常流量，没有特别大的数据包，地址和内容也没有可疑的不相配，所以不会触发警报。最让人害怕的一个例子就是SQL指令植入式攻击（SQL injection）。在这种攻击中，黑客利用你自己的其中一张HTML表单，未经授权就查询数据库。另一种威胁就是命令执行。只要Web应用把命令发送到外壳程序，狡猾的黑客就可以在服务器上随意执行命令。 另一些攻击比较简单。譬如说，HTML注释里面往往含有敏感信息，包括不谨慎的编程人员留下的登录信息。于是，针对应用层的攻击手段，从篡改coOKIes到更改HTML表单里面的隐藏字段，完全取决于黑客的想象力。不过好消息是，大多数这类攻击是完全可以阻止的。 如果结合使用，两种互为补充的方案可以提供稳固防线。首先，使用应用扫描器彻底扫描你的Web应用，查找漏洞。然后，使用Web应用防火墙阻止不法分子闯入。 应用扫描器基本上可以对你的服务器发动一系列模拟攻击，然后汇报结果。KaVaDo ScanDo、Sanctum AppScan Audit和SPI Dynamics在详细列出缺陷、建议补救方法方面的功能都相当全面。AppScan Audit尤其值得关注，因为这款产

品具有事后检查功能，可以帮助编程人员在编制代码时就查出漏洞。不过，这些工具包没有一款比得上安全专业人士的全面审查。 一旦你设法堵住了漏洞，接下来就是部署Web应用防火墙。这类防火墙的工作方式很有意思：弄清楚进出应用的正常流量的样子，然后查出不正常流量。为此，Web应用防火墙必须比普通防火墙更深层地检查数据包。Check Point在这方面最出名，不过KaVaDo、NetContinuum、Sanctum和Teros等其它厂商的名气相对要小。这类防火墙有的采用软件，有的采用硬件，还有一些则兼而有之。不过别误以为这类防火墙是即插即用的，即便采用硬件的也不能。与入侵检测系统一样，你也要认真调整Web应用防火墙，以减少误报，又不让攻击潜入进来。 由于垃圾邮件以及越来越狡猾的攻击，如果您以为安装防火墙就万事大吉，高枕无忧的话，您就应该好好想想上面所说您该如何应对。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com