# 4、WAF拟解决的问题

1、网站程序隐患。由于网站研发人员对WEB安全的认知能力有限以及绝大多数网站运维管理人员的安全意识相对薄弱，导致WEB服务程序往往存在SQL注入、跨站脚本、源码泄露、弱密码、第三方插件漏洞等问题，黑客利用这些漏洞可以获取WEB服务器的控制权限,轻则篡改网页的内容,重则窃取重要的敏感数据。

2、0day漏洞频发。从底层操作系统到WEB容器、数据库、第三方程序或者插件每年都会爆出致命0day漏洞，如Nginx目录遍历漏洞、Struts2漏洞、CMS漏洞、JAVA反序列等0day漏洞。黑客能够利用这些致命的0day漏洞入侵WEB服务器，获取有价值的信息，破坏一些重要的数据，导致系统瘫痪。

3、DDoS攻击猖獗。DDoS攻击自出现之日起就对服务器造成了极大威胁。近年来，DDoS攻击愈演愈烈,尤其以CC攻击为主，对服务器的稳定产生了极大影响。