ID：T1190

战术：初始访问

平台：Linux、Windows、MacOS

数据源：数据包捕获、Web 日志、Web 应用程序防火墙日志、应用程序日志

利用面向公众的应用程序

使用软件、数据或命令来利用面向因特网的计算机系统或程序中的弱点，以引起意外或不可预料的行为。系统中的弱点可能是缺陷、故障或设计漏洞。这些应用程序通常是网站，但可以包括数据库（如 SQL）[1]、标准服务（如 SMB[2]或 SSH）和任何其他具有 Internet 可访问开放套接字的应用程序，如 Web 服务器和相关服务。[3]根据所利用的缺陷这可能包括利用 “防御逃逸 “。
对于网站和数据库，OWASP top 10 给出了前 10 名最常见的基于 Web 的漏洞。

缓解

应用程序隔离和最小特权原则有助于减少漏洞的影响。应用程序隔离将限制被利用目标可以访问的其他进程和系统功能，服务帐户的最低权限将限制被利用进程对系统其余部分获得的权限。Web 应用程序防火墙可用于限制应用程序的对外暴露。
使用 DMZ 或独立的托管基础设施将面向外部的服务器和服务与内网的其余部分进行分段。
在设计用于部署到外部可访问系统的自定义软件时，请使用安全编码最佳实践准则。避免 OWASP、CWE 和其他软件缺陷识别工作记录的问题。
定期扫描外部可访问系统的漏洞，并建立流程，以便在通过扫描和公开披露发现关键漏洞时快速修补系统。

检测

监视应用程序日志中是否存在可能表明尝试或成功利用的异常行为。使用深度包检查来查找常见的漏洞攻击流量的组件，如 SQL 注入。Web 应用程序防火墙可能检测到试图利用漏洞的不正确输入。