YOUR LOGO

Web服务器软件安全防护策略

2024

主讲人：郑冬贤

时间：2024

目录 Contents

YOUR LOGO

Part 01

系统与软件更新

定期检查并应用安全补丁

PART 01

操作系统和服务器软件的更新通常包含已知漏洞的修复，防止攻击者利用这些漏洞入侵系统。

PART 02

定期更新有助于保护Web服务器不受新发现安全威胁的影响。

保持软件最新状态

01

确保所有安装在服务器上的软件，包括Web服务器软件、数据库管理系统和应用程序框架等，都保持最新版本。

02

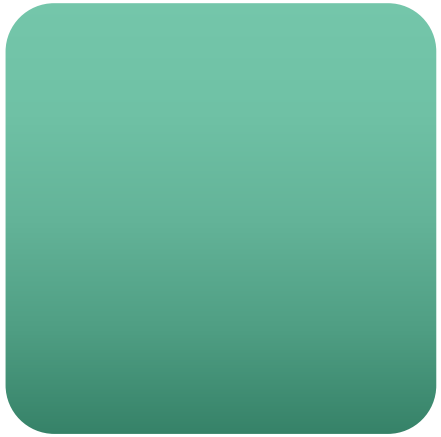
及时更新可以减少系统漏洞，提高整体安全性。

YOUR LOGO

Part 02

最小权限原则

限制用户和服务权限



01

实施最小权限原则，确保系统中的每个用户和服务只能访问其完成任务所必需的资源。

02

例如，Web服务器进程应只拥有读取文件的权限，而不应具备修改或执行脚本的权限。

减少潜在损害

01

限制权限可以减少被攻击后的潜在损害，防止攻击者在系统内横向移动。

YOUR LOGO

Part 03

强化密码策略

使用强密码并定期更换

01

使用强密码策略，并定期更换密码，避免使用默认密码，对于管理账户尤其重要。

02

强密码应包含大小写字母、数字和特殊字符，长度不少于12个字符。

多因素认证

考虑使用多因素认证，为登录过程增加一层额外的安全保护，提高账户安全性。

YOUR LOGO

Part 04

网络隔离与监控

配置网络防火墙和入侵检测系统

01

通过配置网络防火墙和入侵检测系统，限制不必要的网络访问，仅允许必要的端口和服务暴露于外网。

02

监控网络流量，以便及时发现异常模式，如频繁的登录尝试或不寻常的大量流量，这些可能是黑客攻击的迹象。

YOUR LOGO

Part 05

数据加密

使用SSL/TLS协议

01

对敏感数据进行加密处理，包括在传输过程中使用SSL/TLS协议加密数据，以及在存储时对敏感信息进行加密。

02

确保使用足够强度的加密算法和密钥长度，避免使用已被破解的旧算法。

YOUR LOGO

Part 06

备份与恢复计划

定期备份服务器数据和配置

定期备份服务器数据和配置，并确保备份的完整性和可用性。

建立恢复计划，以便在数据丢失或系统受损时能够迅速恢复服务。

离线存储备份

备份应存储在安全的位置，最好是离线存储，以防止勒索软件等威胁。

YOUR LOGO

Part 07

Web应用安全

部署Web应用防火墙和安全插件

部署Web应用防火墙和安全插件，帮助过滤恶意输入，防止跨站脚本攻击和SQL注入等攻击。

对Web应用进行定期的安全审计和漏洞扫描，可以发现并修复潜在的安全隐患。

YOUR LOGO

谢谢大家

2024

主讲人：郑冬贤

时间：2024