YOUR LOGO

Web传输安全及SSL安全

2024

主讲人：郑冬贤

时间：2024

- 目录 -

01 Web传输安全基础

02 SSL/TLS协议详解

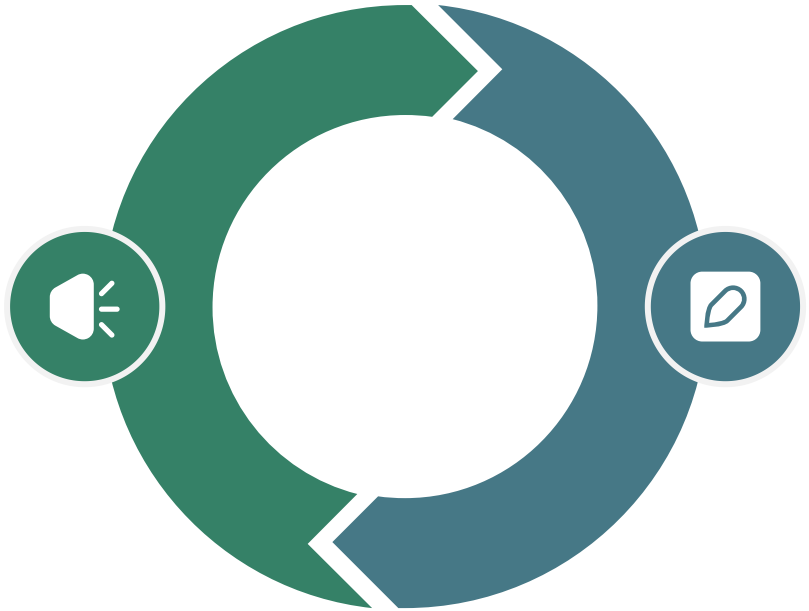
03 Web传输安全实践

YOUR LOGO

Part 01

Web传输安全基础

HTTPS与加密传输



HTTPS定义与作用

HTTPS通过SSL/TLS协议对数据进行加密，保护数据传输过程中的隐私和完整性。使用HTTPS可以防止中间人攻击，确保数据在客户端和服务器之间安全传输。

端口与协议

HTTPS默认使用443端口，而HTTP使用80端口；HTTPS在传输层提供加密保护。

SSL/TLS协议的作用

数据加密与安全

SSL/TLS协议通过加密技术确保数据传输的安全性，防止数据被窃取或篡改。

SSL/TLS协议支持多种加密算法，可以根据安全需求选择适合的加密套件。

身份验证与信任

SSL/TLS通过数字证书验证服务器身份，确保用户连接到正确的服务器。

数字证书由可信的证书颁发机构（CA）签发，增强用户对网站的信任。

YOUR LOGO

Part 02

SSL/TLS协议详解

SSL/TLS握手过程

密钥交换机制

SSL/TLS握手过程中，客户端和服务器交换密钥，为会话创建一个安全的加密通道。

使用非对称加密技术交换密钥，确保即使在公开的网络中也能安全传输。

会话密钥的生成与使用

会话密钥用于加密和解密会话中的数据，提高数据传输的效率和安全性。

会话密钥的生成基于客户端和服务器协商的加密算法和密钥长度。

SSL/TLS版本与安全性

TLS版本演进

TLS协议经历了多个版本的演进，每个新版本都旨在提高安全性和修复已知漏洞。

TLS 1.3是目前最新的版本，提供了更安全的加密和更高效的握手过程。

安全性比较

旧版本的SSL/TLS存在已知的安全漏洞，如SSL 3.0的POODLE攻击。

推荐使用TLS 1.2或更高版本，以确保数据传输的最高安全标准。

YOUR LOGO

Part 03

Web传输安全实践

实施HTTPS

证书申请与安装

网站管理员需要从CA申请SSL/TLS证书，并在服务器上安装配置。

正确配置证书和私钥是实现HTTPS的关键步骤。

HTTPS部署检查

使用在线工具检查HTTPS部署是否正确，确保没有混合内容或证书错误。

定期检查证书有效期，确保证书更新不会影响网站的可用性。

安全审计与漏洞扫描

01

定期安全审计

定期进行Web应用安全审计，检查潜在的安全漏洞和配置问题。

安全审计帮助及时发现并修复安全问题，减少攻击风险。

漏洞扫描工具使用

使用自动化工具如Nessus、Acunetix进行漏洞扫描，发现Web应用的安全弱点。

根据扫描结果采取相应的安全措施，如代码修复或配置更新。

YOUR LOGO

谢谢大家

2024

主讲人：郑冬贤

时间：2024