YOUR LOGO

缓冲区溢出攻击与防护

2024

主讲人：郑冬贤

时间：2024

CONTENTS

目录

YOUR LOGO

Part 01

缓冲区溢出概念

缓冲区溢出定义

01

缓冲区溢出是指程序在向缓冲区写入数据时超出其边界，导致相邻内存区域被覆盖。

02

这种溢出可能破坏程序的正常运行，甚至允许攻击者执行任意代码。

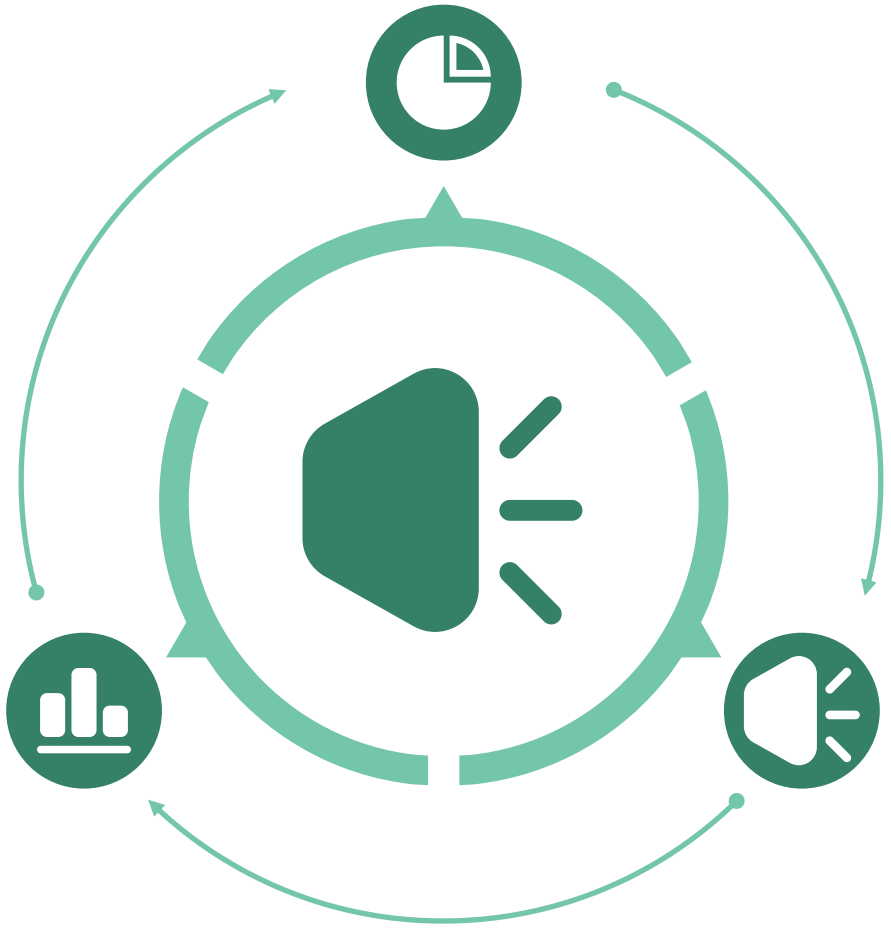
缓冲区溢出原理

攻击者通过精心构造的输入数据，使得程序执行流程被改变，达到攻击目的。

缓冲区溢出漏洞广泛存在于各种操作系统和应用软件中。

缓冲区溢出危害

缓冲区溢出攻击可能导致系统崩溃、数据泄露、权限提升等严重后果。



攻击者可利用缓冲区溢出漏洞进行远程代码执行，控制目标系统。

YOUR LOGO

Part 02

缓冲区溢出攻击类型

堆溢出

堆溢出发生在程序动态分配的内存区域，攻击者可能破坏堆数据结构。

01

堆溢出攻击可能导致程序崩溃或执行攻击者的代码。

02

栈溢出

01

栈溢出发生在程序的栈内存区域，攻击者可能破坏返回地址等关键信息。

02

栈溢出攻击是最常见的缓冲区溢出攻击类型。

全局数组溢出

01

全局数组溢出发生在程序的全局或静态分配的内存区域。

02

攻击者通过溢出修改全局变量，可能导致程序逻辑错误或代码执行。

YOUR LOGO

Part 03

缓冲区溢出防护措施

输入验证

01. / 对所有用户输入进行严格的验证和过滤，防止恶意数据进入程序。

02. / 使用白名单机制，只允许预定义的安全输入通过。

代码审计与静态分析

定期进行代码审计和静态分析，发现并修复潜在的缓冲区溢出漏洞。

使用自动化工具辅助检测，提高审计效率和准确性。

安全编程实践

采用安全的编程实践，如使用安全的函数库，避免使用不安全的函数。

对缓冲区操作进行显式的长度检查，防止溢出。

YOUR LOGO

Part 04

运行时防护技术

地址空间布局随机化（ASLR）

通过地址空间布局随机化技术，增加攻击者预测内存地址的难度。

ASLR能够降低缓冲区溢出攻击的成功率。

数据执行保护（DEP）

01

开启数据执行保护，防止攻击者在数据段执行代码。

02

DEP能够阻止恶意代码的执行，提高系统的安全性。

堆栈保护机制

01

使用堆栈保护机制，如Canary和StackGuard，检测并阻止栈溢出攻击。

02

这些机制通过在栈上设置哨兵值来检测缓冲区溢出。

YOUR LOGO

Part 05

应急响应与恢复

建立应急响应机制

01

建立快速响应机制，一旦发现缓冲区溢出攻击，立即采取措施。

02

包括隔离受影响系统、分析攻击源和修复漏洞等。

数据备份与恢复

01

定期备份关键数据和系统配置，确保在遭受攻击后能够快速恢复。

02

制定详细的数据恢复计划，减少攻击造成的损失。

YOUR LOGO

谢谢大家

2024

申请人：郑冬贤

时间：2024