

软件安全入门

第一课 软件安全基本知识

目录

CONTENTS

01 软件安全问题的背景

02 软件安全分析技术方法



赛博梦工厂
Cyber Works

01

软件安全问题的背景



赛博梦工厂
Cyber Works

1.1 软件安全问题的背景

目前软件应用越来越广泛，软件安全问题也越来越突出：

一方面是由于技术和应用的快速发展，致使软件自身越来越复杂，规模也越来越庞大，开发过程中不可避免地会出现一些错误从而引入各种程序漏洞。

另一方面是由于当软件承载了越来越多的利益时，一些组织开始利用软件的安全问题来获取利益。



1.2 典型的安全问题

恶意软件

主要指病毒、木马、蠕虫、僵尸网络、间谍软件等。
其共同特点是在用户不知情的情况下实施一系列的破坏功能，如窃取信息、远程控制等。



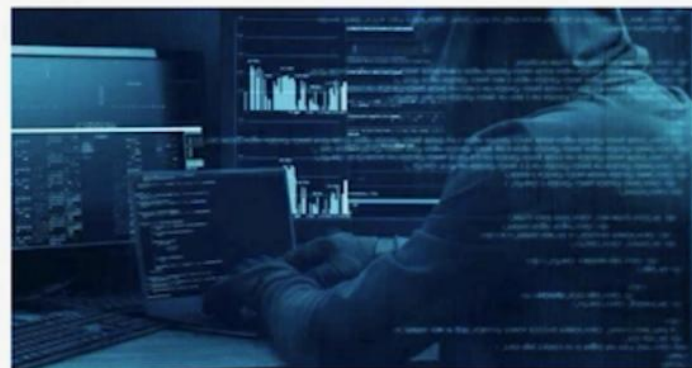
软件后门

是指软件开发人员有意设计，刻意对用户隐瞒的一些功能。
其特点是难发现、易利用、难取证，是软件产品中重要的安全威胁之一。



软件漏洞

是指由于程序设计实现错误造成的软件问题。
攻击者利用软件漏洞可以造成程序崩溃，获取敏感数据或执行任意代码。



1.3 软件安全分析的目标



存在问题

首要问题是分析目标软件中是否存在恶意功能、漏洞或者后门。



机理问题

确定问题存在之后，进一步分析其具体是如何实现的或是什么原因造成的。



对策问题

根据相关机理分析结果，提出相应的防御对策。



赛博梦工厂
Cyber Works

02

软件安全分析技术方法



赛博梦工厂
Cyber Works

2.1 软件安全技术分类

静态分析

对软件的可执行代码进行分析。

优点：可以对软件代码进行较为全面的整体性分析。

缺点：无法分析大规模、复杂的软件代码；无法应对软件加壳等手段。

动态分析

直接运行软件，然后监测软件运行过程，实施分析。

优点：分析过程的复杂度低，准确性高。

缺点：一次只能执行一条路径，分析的全面性较差。



赛博梦工厂

Cyber Works

2.2 软件安全分析典型技术



•1.软件安全问题的背景

·主要内容包括:软件安全问题出现的原因、典型的安全问题 (恶意软件、软件漏洞、软件后门)、软件安全性分析的目标。

•2.软件安全分析技术方法

主要内容包括: 软件逆向分析技术的分类 (静态分析和动态分析)、典型技术的简要介绍 (反汇编与反编译、程序调试、程序切片、污点传播分析、符号执行、模糊测试)。





谢谢观赏