教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导


360企业安全集团组织编写

网络空间安全重点规划丛书

顾问委员会主任：沈昌祥 编委会主任：封化民

# 漏洞扫描与防护

杨东晓 张锋 段晓光 马楠 编著

Cyberspace Security

根据教育部高等学校信息安全专业教学指导委员会编制的
《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社

教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

网络空间安全重点规划丛书

# 漏洞扫描与防护

杨东晓 张锋 段晓光 马楠 编著

清华大学出版社
北京

## 内 容 简 介

本书共分为9章。首先介绍漏洞的分类、特征和发展等基本知识，漏洞扫描的技术和流程；然后分析网络设备的常见漏洞及防范措施，操作系统的常见漏洞及防范措施，数据库的常见漏洞及防范措施，Web系统的常见漏洞及防范措施，用户名及口令猜解的类型与防范措施等方面的内容；最后描述软件配置检查的方法和标准，并结合详细案例对需求和解决方案进行详细分析解读，帮助读者更透彻地掌握漏洞扫描和防护。

本书每章后均附有思考题总结该章知识点，以便为读者的进一步阅读提供思路。

本书由360企业安全集团针对高校网络空间安全专业的教学规划组织编写，既可作为信息安全、网络空间安全专业及网络工程、计算机技术应用型人才培养与认证体系中的教材，也可作为负责网络安全运维的网络管理人员和对网络空间安全感兴趣的读者的基础读物。



**图书在版编目(CIP)数据**

漏洞扫描与防护/杨东晓等编著. —北京：清华大学出版社，2019
（网络空间安全重点规划丛书）
ISBN 978-7-302-51716-0

Ⅰ. ①漏… Ⅱ. ①杨… Ⅲ. ①计算机网络－网络安全－教材 Ⅳ. ①TN393.08

中国版本图书馆CIP数据核字(2018)第266960号

**责任编辑**：张　民　常建丽
**封面设计**：常雪影
**责任校对**：焦丽丽
**责任印制**：宋　林

**出版发行**：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
**印 刷 者**：北京富博印刷有限公司
**装 订 者**：北京市密云县京文制本装订厂
**经　　销**：全国新华书店
**开　　本**：185mm×260mm　　**印　　张**：9　　**字　　数**：205千字
**版　　次**：2019年1月第1版　　**印　　次**：2019年1月第1次印刷
**定　　价**：29.00元

产品编号：080631-01

网络空间安全重点规划丛书

# 编审委员会

# 出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。系列教材的作者都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

该系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到系列教材中，以进一步满足大家对外版书的需求。“高等院校信息安全专业系列教材”已于2006年年初正式列入普通高等教育“十一五”国家级教材规划。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会

暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展起到重要的指导和推动作用。2006 年教育部给武汉大学下达了“信息安全专业指导性专业规范研制”的教学科研项目。2007 年起该项目由教育部高等学校信息安全类专业教学指导委员会组织实施。在高教司和教指委的指导下，项目组团结一致，努力工作，克服困难，历时 5 年，制定出我国第一个信息安全专业指导性专业规范，于 2012 年年底通过经教育部高等教育司理工科教育处授权组织的专家组评审，并且已经得到武汉大学等许多高校的实际使用。2013 年，新一届“教育部高等学校信息安全专业教学指导委员会”成立。经组织审查和研究决定，2014 年以“教育部高等学校信息安全专业教学指导委员会”的名义正式发布《高等学校信息安全专业指导性专业规范》(由清华大学出版社正式出版)。

2015 年 6 月，国务院学位委员会、教育部出台增设“网络空间安全”为一级学科的决定，将高校培养网络空间安全人才提到新的高度。2016 年 6 月，中央网络安全和信息化领导小组办公室(下文简称中央网信办)、国家发展和改革委员会、教育部、科学技术部、工业和信息化部及人力资源和社会保障部六大部门联合发布《关于加强网络安全学科建设和人才培养的意见》(中网办发文[2016]4 号)。为贯彻落实《关于加强网络安全学科建设和人才培养的意见》，进一步深化高等教育教学改革，促进网络安全学科专业建设和人才培养，促进网络空间安全相关核心课程和教材建设，在教育部高等学校信息安全专业教学指导委员会和中央网信办资助的网络空间安全教材建设课题组的指导下，启动了“网络空间安全重点规划丛书”的工作，由教育部高等学校信息安全专业教学指导委员会秘书长封化民校长担任编委会主任。本规划丛书基于“高等院校信息安全专业系列教材”坚实的工作基础和成果、阵容强大的编审委员会和优秀的作者队伍，目前已经有多本图书获得教育部和中央网信办等机构评选的“普通高等教育本科国家级规划教材”“普通高等教育精品教材”“中国大学出版社图书奖”和“国家网络安全优秀教材奖”等多个奖项。

“网络空间安全重点规划丛书”将根据《高等学校信息安全专业指导性专业规范》(及后续版本)和相关教材建设课题组的研究成果不断更新和扩展，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国网络空间安全学科的发展不断完善，力争为我国网络空间安全相关学科专业的本科和研究生教材建设、学术出版与人才培养做出更大的贡献。

我们的 E-mail 地址是：zhangm@tup.tsinghua.edu.cn，联系人：张民。

“网络空间安全重点规划丛书”编审委员会

# 前言

没有网络安全，就没有国家安全；没有网络安全人才，就没有网络安全。

为了更多、更快、更好地培养网络安全人才，如今，许多高校都在努力培养网络安全人才，都在加大投入，并聘请优秀老师，招收优秀学生，建设一流的网络空间安全专业。

网络空间安全专业建设需要体系化的培养方案、系统化的专业教材和专业化的师资队伍。优秀教材是培养网络空间安全专业人才的关键，但这是一项十分艰巨的任务。原因有二：其一，网络空间安全的涉及面非常广，包括密码学、数学、计算机、操作系统、通信工程、信息工程、数据库、硬件等多门学科，因此，其知识体系庞杂、难以梳理；其二，网络空间安全的实践性很强，技术发展更新非常快，对环境和师资要求也很高。

“漏洞扫描与防护”是高校网络空间安全和信息安全专业的基础课程，通过对漏洞各知识面的介绍帮助读者掌握漏洞扫描与防护。本书涉及的知识面宽，共分为 9 章。

第 1 章介绍漏洞基本知识，第 2 章介绍安全漏洞扫描系统，第 3 章介绍网络设备漏洞及其防范措施，第 4 章介绍操作系统漏洞及其防范措施，第 5 章介绍数据库系统漏洞及其防范措施，第 6 章介绍 Web 系统漏洞及其防范措施，第 7 章介绍用户名及口令猜解，第 8 章介绍软件配置检查，第 9 章介绍典型案例。

本书既适合作为高校网络空间安全、信息安全等相关专业课程的教材和参考资料，也适合网络安全研究人员作为网络空间安全的入门基础读物。

本书编写过程中得到 360 企业安全集团的王嘉、董少飞、任涛、裴智勇、翟胜军、北京邮电大学雷敏等专家学者的鼎力支持，在此对他们的工作表示衷心感谢！

由于作者水平有限，书中难免存在疏漏和不妥之处，欢迎读者批评指正。

作　者

2018 年 12 月

# 目录

# 第1章 漏洞的基本知识

2017年5月12日起，全球范围内爆发基于Windows网络共享协议进行攻击传播的蠕虫恶意代码，这是不法分子通过改造之前泄漏的NSA黑客武器库中“永恒之蓝”攻击程序发起的网络攻击事件。5个小时内，包括英国、俄罗斯等欧洲多国以及中国国内多所高校校内网、大型企业内网和政府机构专网中招，被勒索支付高额赎金后才能解密恢复文件，对重要数据造成严重损失。类似的软件漏洞事件层出不穷，这也间接表明，随着全球信息化的迅猛发展，软件在便利我们生活的同时，也给我们带来了很大的危害，其安全问题日益突出。软件漏洞是安全问题的根源之一。随着互联网和软件技术的不断发展，软件漏洞的数量日益增加，造成的危害也越来越大，由其引发的信息窃取、资源被控、系统崩溃等问题会对国民经济、社会稳定等产生重大威胁。因此，对软件漏洞的研究和防护日益受到重视。

本章主要介绍漏洞的基础知识。通过本章的学习，可以理解漏洞的定义和成因、漏洞的特征及危害、常见的漏洞类型以及漏洞的现状和未来发展趋势。

## 1.1 漏洞概述

### 1.1.1 漏洞的定义

漏洞(vulnerability)是指计算机系统的硬件、软件、协议在系统设计、具体实现、系统配置或安全策略上存在的缺陷和不足。漏洞本身并不会导致系统损坏，但它能够被攻击者利用，从而获得计算机系统的额外权限，使攻击者能够在未授权的情况下访问或破坏系统，影响计算机系统的正常运行，甚至造成安全损害。

微软安全响应中心对漏洞的定义为：即使在使用者合理配置了产品的条件下，由于产品自身存在的缺陷，产品的运行可能被改变，产生设计者未预料到的后果，并可能最终导致安全性被破坏的问题，其主要包括使用者系统被非法侵占、数据被非法访问并泄漏，系统拒绝服务等。

漏洞的概念早在1947年冯·诺依曼建立计算机系统结构理论时就有所提及。他认为计算机的发展和自然生命有相似性，一个计算机系统也有天生的类似基因的缺陷，也可能在使用和发展的过程中产生意想不到的问题。每个平台无论是硬件，还是软件，都可能存在漏洞，漏洞的影响范围可能包括硬件和软件，如系统本身及其支撑软件、网络客户和服务器软件、网络路由器和安全防火墙等。

### 1.1.2 漏洞的成因

产生漏洞的原因有很多，大体上可分为技术角度、经济角度和应用环境角度三大类成因。

#### 1. 技术角度

从技术角度来说，计算机系统漏洞又被分为两种：第一种是应用系统自身存在的“先天性漏洞”；第二种是在应用系统的开发过程中由于开发人员的疏忽而造成的“后天性漏洞”。从客观上来说，用户使用的应用系统种类多样，开发迅速，所以应用软件系统自身就存在一些固有的安全隐患，这种由于硬件而先天就存在的漏洞体现了应用系统的脆弱性。从主观上来说，当前的应用系统大都依托人工进行研发，而部分开发人员在设计应用软件时可能缺乏一定的安全知识和经验。即使是专门的安全研究人员，也有可能在开发过程中存在考虑不周、不够完备的情况，这些主观的人为因素使得应用系统不可避免地存在安全漏洞。

#### 2. 经济角度

计算机系统的安全性不是显性价值，厂商要实现安全性，就要额外付出巨大的代价。厂商更加重视计算机系统的功能、性能、易用性，而不愿意在安全质量上做更大的投入，甚至某些情况下，为了提高计算机系统效率而降低其安全性，结果导致计算机系统安全问题越来越严重，这种现象可以进一步归结为经济学上的外在性。

#### 3. 应用环境角度

互联网已经逐渐融入人类社会的方方面面，伴随互联网技术与信息技术的不断融合与发展，导致计算机系统的运行环境发生改变，从传统的封闭、静态和可控变为开放、动态和难控，攻易守难的矛盾进一步增强。

同时，随着移动互联网和物联网的不断发展，它们与互联网共同构成了更加复杂的异构网络。在这个比互联网网络环境还要复杂的应用环境下，漏洞类型和数量急剧增加，漏洞产生的危害和影响远远超过在非网络或同构网络环境下漏洞的危害和影响程度。

## 1.2 漏洞的特征与危害

### 1.2.1 漏洞的特征

漏洞是一个抽象的概念，具有如下特征。

#### 1. 漏洞是一种状态或条件，表现为不足或者缺陷

漏洞的存在并不会直接对系统造成损害，但是它可以被攻击者利用，从而造成对系统安全的威胁、破坏，影响计算机系统的正常运行，甚至造成损坏。计算机系统漏洞也不同于一般的计算机故障，漏洞的恶意利用能够影响人们的工作和生活，甚至会带来灾难性的

后果。

### 2. 漏洞并不都能进行自动检测

漏洞自动检测技术能够低成本、高效率地发现信息系统的安全漏洞，但并不是所有漏洞都能够进行自动检测，事件型漏洞就只能依靠人工挖掘，而且潜在的事件型漏洞的数量可能还要多于通用型漏洞。另外，为了避免对目标服务器产生负面影响，安全检测程序常常会选择性忽略某些漏洞，如文件上传和下载等。所以，以安全检测为目的的漏洞扫描会存在一定的漏报和误报。

### 3. 漏洞与时间紧密相关

一个系统从发布时起，随着用户的深入使用，系统中存在的漏洞便会不断地被发现。早期被发现的漏洞也会不断被系统供应商发布的补丁修补，或在以后发布的新版本中得到纠正。在新版系统纠正旧版中漏洞的同时，也会引入一些新的漏洞和错误。因而，随着时间的推移，旧的漏洞不断消失，新的漏洞不断出现。漏洞问题是长期存在的，变化的只是漏洞的内容。

### 4. 漏洞通常由不正确的系统设计或错误逻辑造成

在所有的漏洞类型中，逻辑错误所占的比例最高。绝大多数的漏洞是由于疏忽造成的。数据处理(如对变量赋值)比数值计算更容易出现逻辑错误，过小和过大的程序模块都比中等程序模块更容易出现错误。

### 5. 漏洞会影响大范围的软硬件设备

漏洞的影响范围非常广。也就是说，在操作系统、网络客户和服务器软件、网络路由器和安全防火墙等不同的软硬件设备中都可能存在着不同的安全漏洞问题。具体而言，在不同种类的软、硬件设备，同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在各自不同的安全漏洞问题。

## 1.2.2　漏洞的危害

漏洞的存在虽然不会主动威胁系统的正常运行，但由于别有用心的人的存在，使得漏洞直接威胁着系统安全。漏洞的存在，使得病毒得以传播，网络攻击得以进行。通常从以下 5 个方面评估漏洞对系统安全特性造成的危害。

### 1. 系统的完整性(integrity)

攻击者可以利用漏洞入侵系统，能够在未经授权的情况下对存储或传输过程中的信息进行删除、修改、伪造、乱序、重放、插入等破坏操作，从而破坏计算机系统的完整性。

### 2. 系统的可用性(availability)

攻击者利用漏洞破坏系统或者阻止网络正常运行，导致信息或网络服务不可用，即合法用户的正常服务要求得不到满足，从而破坏了系统的可用性。

### 3. 系统的机密性(confidentiality)

攻击者利用漏洞给非授权的个人和实体泄漏受保护的信息。需要注意的是，在很多

场景下，系统的机密性和完整性是交叠的。

#### 4. 系统的可控性(controllability)

攻击者利用漏洞，使得系统对于合法用户而言处在“失控”状态，从而破坏系统对信息的控制能力。

#### 5. 系统的可靠性(reliability)

攻击者利用漏洞对用户认可的质量特性(信息传递的迅速性、准确性以及连续地转移等)造成危害，也就是指系统无法在规定的条件和时间完成规定的功能。

## 1.3 漏洞的分类方式

漏洞的分类方法有很多。从漏洞作用方式看，可以分为本地提权漏洞、远程代码执行漏洞、拒绝服务漏洞等；从漏洞的普遍性看，又可以分为通用型漏洞、事件型漏洞和 0day 漏洞。

### 1.3.1 漏洞的作用方式

#### 1. 本地提权漏洞

本地提权漏洞是指可以实现非法提升程序或用户的系统权限，从而实现越权操作的安全漏洞。生活中常见的苹果手机越狱，安卓手机 Root，实际上都是利用本地提权漏洞实现的，目的是让使用者可以获得 iOS 系统或安卓系统禁止用户拥有的系统权限。利用此类漏洞，恶意程序可以非法访问某些系统资源，进而实现盗窃信息或系统破坏。

#### 2. 远程代码执行漏洞

现代计算机系统大多可以远程登录或访问，但必须在设备开启了远程访问功能，并且访问者的登录账号拥有远程访问权限的情况下才行。而远程代码执行漏洞，就是指无须验证账号的合法性，就可以实现远程登录访问的安全漏洞。

远程代码执行漏洞也是最危险的一类安全漏洞，如冲击波、熊猫烧香、永恒之蓝勒索蠕虫(WannaCry)等超级病毒能够实现快速大规模传播，主要就是因为这些病毒利用了未打补丁的计算机系统中的远程代码执行漏洞，发动对联网计算机的自动攻击。对于存在此类漏洞的计算机和设备，只要连接在互联网上，就是危险的，因为攻击者的攻击完全不需要使用者的配合，不需要使用者有任何不当的联网操作，如打开不明文件，浏览恶意网址等。

#### 3. 拒绝服务漏洞

拒绝服务漏洞，是指可以导致目标应用或系统暂时或永远性失去响应正常服务的能力，影响系统的可用性。这种漏洞的主要作用是使程序系统崩溃，无法正常工作。拒绝服务漏洞又可细分为远程拒绝服务漏洞和本地拒绝服务漏洞。前者大多被攻击者用于向服务器发动攻击，后者则大多被用于计算机病毒对本地系统和程序的攻击。

### 1.3.2　漏洞的普遍性

#### 1. 通用型漏洞

由于现今绝大多数的软件、网站或信息系统开发都不是从零起步，而是使用某些现成的开发平台或开源代码开发出来的，因此，使用同一系统平台或同一开源代码开发出的软件、网站或信息系统就往往有可能存在同样的或相似的安全漏洞。这种普遍存在的相同或相似的漏洞就是通用型漏洞。

#### 2. 事件型漏洞

事件型漏洞主要是指软件、网站或信息系统中的某一个具体的、独特的漏洞，这个漏洞的出现有很大的偶然性，只与相关软件、网站或信息系统自身的开发过程、运维过程有关，在其他地方不会复现。例如，常见的弱密码问题、业务逻辑漏洞、系统设置不当等，一般都属于事件型漏洞。

从历史经验看，90％以上的软件、网站或信息系统都存在事件型安全漏洞。当系统开发平台被曝出存在安全漏洞时，几乎所有使用该平台开发出的软件、网站或信息系统都会同时存在安全漏洞。

#### 3. 0day 漏洞

0day 漏洞也称为零日漏洞，它是指已经有人知道，但厂商尚未修复的安全漏洞。攻击者利用 0day 漏洞发动攻击，理论上来说几乎是不可能防御的。但由于 0day 漏洞的发现非常困难，一旦被安全机构掌握，0day 漏洞也就立即失效了。所以，网络攻击者如果持有 0day 漏洞，一般不会使用到普通人身上，而是会用来攻击高价值的目标。此外，如果是厂商已经提供了补丁，但由于各种原因，相关软件、系统或设备还没有打上这些补丁的漏洞，因而可以被有效地攻击和利用，这种漏洞称为 Nday 漏洞。

## 1.4　常见的漏洞类型

### 1.4.1　操作系统漏洞

操作系统漏洞是指操作系统或操作系统自带应用软件在逻辑设计上出现的缺陷或编写时产生的错误，这些缺陷或错误可以被不法者利用，通过网络植入木马、病毒等方式攻击或控制整个计算机，窃取计算机中的重要资料和信息，甚至破坏计算机系统。

#### 1. Windows 系统漏洞

Windows 操作系统是迄今为止使用最广泛的个人计算机操作系统，从最早的 DOS 系统发展到 Windows 7、Windows 8 和 Windows 10 系统，其系统的安全性逐渐提高，但是却避免不了漏洞的存在。因此，用户需要认识这些漏洞，并掌握修复漏洞的常用方法。

由于 Windows 操作系统在桌面操作系统的垄断地位，大量的攻击者开始研究该系统的漏洞。Windows 操作系统与 Linux 等开放源码的操作系统不一样，普通用户无法获取