# 电子商务与网络安全

DIANZISHANGWU YU WANGLUOANQUAN

主　编　宋梦华

对外经济贸易大学出版社
University of International Business and Economics Press

# 电子商务与网络安全

主编　宋梦华

对外经济贸易大学出版社
中国·北京

**图书在版编目（CIP）数据**

电子商务与网络安全 / 宋梦华主编. —北京：对外经济贸易大学出版社，2011
ISBN 978-7-81134-926-9

Ⅰ.①电… Ⅱ.①宋… Ⅲ.①电子商务－安全技术－专业学校－教材 Ⅳ.①F713.36

中国版本图书馆 CIP 数据核字（2010）第 256841 号



# 电子商务与网络安全

宋梦华　**主编**

**责任编辑**：刘　尧　高　卓

对外经济贸易大学出版社
北京市朝阳区惠新东街 10 号　　邮政编码：100029
邮购电话：010－64492338　　发行部电话：010－64492342
网址：http://www.uibep.com　　E-mail：uibep@126.com

山东省沂南县汇丰印刷有限公司印装　　新华书店北京发行所发行
成品尺寸：185mm×260mm　　13.75 印张　　318 千字
2011 年 7 月北京第 1 版　　2011 年 7 月第 1 次印刷

ISBN 978-7-81134-926-9
印数：0 001－3 000 册　　定价：21.00 元

# 前　言

电子商务的广泛应用，为中小企业提供了摆脱自身规模限制、最大限度利用信息技术和网络技术，从而在激烈的市场竞争中站稳脚跟的机会。作为一种崭新的商务运作模式，电子商务现已显现出巨大的现代商业价值。但是由于互联网的开放性、共享性和无序性，使得电子商务面临着多种风险和威胁，其中电子商务安全问题一直困扰着电子商务的发展。

电子商务安全是电子商务专业重要的专业基础课程。本书根据最新的职业教育教学改革精神，结合作者多年的教学与企业网络安全经验向学生系统地阐述电子商务面临的安全问题，并深入分析问题产生的根源，利用先进、适用的技术解决这些问题。

本书基于“项目导向、任务驱动、学做合一”的编写思路，设置有 6 大项目、17 个任务。内容包括认识电子商务网络安全重要性、了解电子商务网络结构与设备安全性、电子商务服务器安全性、电子商务系统安全性、电子商务系统数据安全性、电子商务网络系统管理与安全防范等。每个项目任务均按任务介绍、任务分析、任务实施、知识拓展及任务评价等目录结构组织编写。

本书可作为高职高专院校《电子商务与网络安全》课程的教材，也可作为应用型本科、成人教育、岗位培训班的教材，以及企业电子商务技术人员学习的参考书。

本书由天津海运职业学院的宋梦华老师负责全书的统稿、定稿工作。其中项目一和项目二由天津电子信息职业技术学院吴海龙老师编写；项目三和项目六由天津海运职业学院宋梦华老师编写；项目四、项目五由天津海运职业学院孟庆宝、天津职业大学赵学丽、王倩等老师联合编写。天津电子信息职业技术学院栾群老师也参加了编写工作，同时参编的还有微软（中国）有限公司的叶强先生等。本书的编写得到天津对外经济贸易职业学院魏秀敏教授的精心指导，在此表示感谢。

由于写作时间仓促和作者水平有限，书中不当之处在所难免，敬请广大读者批评指正。

编　者

2010 年 9 月

# 目　录

项目一

# 认识电子商务网络安全重要性

## 项目综述

电子商务是当前网络在经济全球化环境中尤为重要并极具生命力的商务模式。本项目的主要目的是让学生充分认识安全性在电子商务网站运行中的重要地位，从而培养其高度重视电子商务系统运行安全管理的意识，进而逐步学会对网络安全管理的基本能力。

## 任务1　了解网络攻击对网站运行的影响

### 任务介绍

随着 Internet 的广泛应用，公司形象网站、各大门户网站、电子商务网站等如雨后春笋般层出不穷，遍及全球的上网人数呈指数上涨。与此相伴的是，网络经济的利益驱动使黑客攻击越来越频繁，影响也越来越大。本任务主要是通过对国际知名网站遭遇盗窃篡改的典型案例分析强化学生对网站安全运行重要性的认识。

### 任务分析

2010 年 8 月 2 日—2010 年 8 月 8 日，国家计算机网络应急技术处理协调中心发布网络安全信息与动态周报显示：

互联网网络安全态势整体评价为优。我国互联网基础设施运行整体平稳，全国范围或省级行政区域内未发生造成重大影响的基础设施运行安全事件。针对政府、企业以及广大互联网用户的主要安全威胁来自于软件高危漏洞、恶意代码传播以及网站攻击。依据 CNCERT 抽样监测结果和国家信息安全漏洞共享平台（CNVD）发布的数据，境内被木马控制的主机 IP 地址数目约为 6.4 万个，同种类木马感染量与前一周环比下降 16%（注 1）；境内被僵尸网络控制的主机 IP 地址数目为 6 478 个，环比下降 40%；境内被篡改政府网站数量为 72 个，环比下降 31%；新增信息安全漏洞 30 个，环比下降 49%，其中高危漏洞 3 个，比上周增加 2 个。

**注 1**：此周期调整了木马监测范围，总数变更为 64 种木马。为保证数据的可比性，仍取近两周相同种类木马的监测数据做环比分析。

根据 CNCERT 监测数据（注 2），本周境内被篡改政府网站数量为 72 个，较上周有所下降，

截至 8 月 9 日 12 时仍未恢复的被篡改政府部门网站如下表 1.1 所示。

**表 1.1　　网站被盗窃篡改情况统计**

| 被篡改页面 URL | 所属部门或地区 |
|---|---|
| http://aqzw.gov.cn/default.asp | 安徽省安庆市 |
| http://www.hzxf.gov.cn/r00t.htm | 广西壮族自治区贺州市 |
| http://www.zhq.gov.cn/zorro.htm | 河南省平顶山市 |
| http://dxzlly.gov.cn/index.htm | 黑龙江省大兴安岭地区 |
| http://www.sysld.gov.cn/index.htm | 黑龙江省双鸭山市 |
| http://www.sfhcgj.gov.cn/sbhack.txt | 黑龙江省绥芬河市 |
| http://szgtzy.gov.cn/index.htm | 湖北省随州市 |
| http://whlsj.gov.cn/newfile.asp | 湖北省武汉市 |
| http://old.xfjt.gov.cn/index.asp | 湖北省襄樊市 |
| http://yuanjiang.gov.cn/test.asp | 湖南省沅江市 |
| http://www.zzslj.gov.cn/l.htm | 湖南省株洲市 |
| http://www.zxst.gov.cn/zorro.htm | 湖南省资兴市 |
| http://www.alstax.gov.cn/index.htm | 内蒙古自治区阿拉善盟 |

**注 2**：CNCERT 监测的政府网站是指英文域名以“.gov.cn”结尾的网站，但不排除个别非政府部门也使用“.gov.cn”的情况。

中国反网络病毒联盟（ANVA）整理发布的活跃恶意代码如表 1.2 所示。其中，利用应用软件及操作系统漏洞进行传播的恶意代码仍占较高比例，与播放器相关的恶意代码活跃程度有所增强。ANVA 提醒互联网用户一方面要加强系统漏洞的修补加固，另一方面要加装安全防护软件。此外，不要轻易打开网络上来源不明的图片、音乐、视频等文件。

**表 1.2　　活跃恶意代码**

| 名　　称 | 特　　点 |
|---|---|
| Trojan.DL.Giframe.a | 这是一个下载者木马，利用浏览器 GIF 文件解析漏洞进行传播。黑客通过诱导用户浏览含有恶意代码的 GIF 文件的网页，来控制用户连接到特定的包含恶意程序的网页。不过，目前发现使用 Windows 图片查看器打开含有此恶意代码的 GIF 文件并不受影响 |

续表

| 名　　称 | 特　　点 |
| --- | --- |
| Trojan.DL.PicFrame.a | 这是一个下载者木马，利用浏览器查看图片文件解析漏洞进行传播。该病毒在 JPG 文件末尾附加了包含恶意网站链接的 <iframe></iframe>，由于 iframe 的 width 和 height 都很小，用户极易在未察觉的情况下访问恶意网址 |
| Trojan.DL.Script.VBS.Mnless.e | 这是一个经过加密地的 VBS 脚本病毒，病毒解密之后，将会从远程服务器下载文件并执行 |
| Hack.Exploit.Script.JS.Agent.ju | 该病毒采用加密脚本，利用 RealPlayer 播放器的溢出漏洞进行传播。病毒会将网页脚本加密成乱码字符，普通用户很难识别是病毒代码。病毒通过调用 RealPlayer 组件，用特定构造的 shellcode 进行溢出。成功之后，就会打开指定的下载地址，下载其他病毒 |

## 任务实施

通过案例分析，明显看出黑客攻击是网络安全的最大威胁。因为形形色色的网站都暴露在 Internet 这个公共网络平台上，网站安全随时受到遭遇黑客攻击的威胁。网站的安全因素包括设备的安全、数据库系统的安全、操作系统平台的安全、Web 应用程序的安全、网络传输过程的安全等。要想提高网站运行安全稳定，必须主动做好安全防范措施。网站的安全性问题主要表现在：接触安全问题之前，必须首先掌握必要的术语。

（1）脆弱性。脆弱性是系统的一个特征，它可能会使应用系统不完全按照预想方式运行，是系统运行状况欠佳的特征。

（2）威胁。威胁即指破坏系统安全的可能性。

（3）利用。利用即利用脆弱性的方法。

综合上述，为脆弱性导致了威胁，利用则实现了威胁，简而言之，就是攻击。

### 一、硬件设备安全的脆弱性

网络硬件主要包括网络互联设备，如：交换机、路由器、网关等。现在仅考虑针对硬件设备进行一些安全方面的配置，比如交换机的 VLAN，路由器的 ACL 配置等，却忽视了设备本身在工作中存在的脆弱性。

**（一）交换机脆弱性分析**

交换机在 OSI 数据链路层 MAC 子层工作，它可连接到单独的结点或整个网段的单个端口，在它们之间交换数据，并为每个端口到端口之间提供全部的局域网介质带宽。

（1）从设备自身看，首先是交换机在系统安装、启动和灾难恢复时一般处于不安全状态，有一定的脆弱性；其次，还存在物理威胁，一些外在因素的影响可能破坏交换机。

（2）从外在因素看，入侵者利用交换机软件或协议的脆弱性进行攻击，比如 IP 欺骗，TCP 连接功能被欺骗、截取、操纵，UDP 易受 IP 源路由和拒绝服务的攻击等，同时也

亦存在访问权滥用或后门等问题。

**（二）路由器脆弱性分析**

路由器工作在 OSI 模型的网络层，它可用来连接具有相同网络通信结构的网络，也可连接不同结构的网络。它为数据包提供最佳路径，并实现子网隔离和抑制广播风暴。

（1）从设备自身看，路由器相当于网络层的中继器。路由器不能真正实现即插即用，需要很多配置。配置文件一般包括路由器接口地址、登录密码、路由表接口状态、ARP 表、日志信息等。这些信息如果被攻击者获得，后果不堪设想。攻击者可将路由器作为平台，对其他站点扫描、侦察、攻击，甚至修改路由配置等。

（2）从外在因素看，路由器是在网络层实现多个网络互联的设备，如想得到路由器的访问控制权，任何人都可通过路由器对其他服务器发起拒绝服务攻击，而路由器不会自动生成警报通知用户所受到的攻击。且路由器的访问密码极不安全，可以通过 SNIFFER 探测，也可在专属公司网页上查寻。

**（三）网关脆弱性分析**

网关又叫做协议转换器，用来连接专用网络和公共网络的路由器。网关是将不同协议集的协议进行翻译、转换，是最复杂的网络互联设备，用于连接网络层之上执行不同高层协议的网络，构成异构的互联网，通常工作在 OSI 模型的第 4 层和更高层。

（1）从设备自身看，网关是软件和硬件结合的网络互联设备，是最复杂的网络互联设备，不同的网关用于不同的场合，其软件和硬件自身也存在脆弱性。

（2）从外在因素看，网关是针对特定的网络互联环境而设计的，不存在通用网关。有时制造商会留下可获得敏感信息的后门。

## 二、数据库管理系统安全的脆弱性

（1）数据库管理系统主要通过用户的登录验证、用户权限、数据使用权限以及审计功能提供安全性能。由于黑客常常通过探访工具强行登录和越权使用数据库的数据，给用户带来巨大的损失。对数据进行加密固然可以提高安全性，但加密又会与数据库管理系统的功能发生冲突或影响数据库的运行效率，故不常用。

（2）使用“服务器—浏览器”结构的网络应用程序因由应用程序直接对数据库进行操作，应用程序的某些缺陷有可能威胁到数据库的安全。因而，使用“数据库—服务器—浏览器”三层结构的应用程序通过标准工具对数据库进行操作，可加强其安全性。数据库的安全等级应与操作系统安全等级相适应，否则缺口会首先从最薄弱的环节打开。

（3）系统管理员对系统和数据库的绝对控制权也是安全的一个突出问题。因为系统管理员有权查阅和删改任何敏感数据，系统对他的权力没有任何约束。故而，应实行系统管理员、安全员、审计员三权分立的互相制约机制。同时，该机制须得到操作系统和数据库管理系统的支持方能生效。

## 三、操作系统安全的脆弱性

（1）操作系统为了系统集成和系统扩张的需要，采用支持动态连接的系统结构。系统的服务和 I/O 操作都可用打补丁方式进行动态连接。由于黑客熟知打补丁方法，便形

成病毒滋生的营养缸。

（2）操作系统的进程可以创建，且这种进程可在远程网络节点上创建和激活，更为严重的是被创建的进程还继承了再创建进程的权力。这样，黑客在远程把间谍补丁打在一个合法用户特别是超级用户的身上，就能逃脱系统作业与进程监视程序的眼睛。

（3）操作系统为维护方便而预留的免口令入口和各种隐蔽通道，也便于黑客进出。

（4）操作系统提供的具有与系统核心层同等权力的 daemon 软件和远程过程调用 RPC 服务、网络文件系统 NFS 服务，以及 Debug、Wizard 等工具，也给黑客提供了翻云覆雨的机会。

## 四、Web 应用安全的脆弱性

对 Web 的攻击有很多种，其中一部分可使用 ASP.net 代码进行防范，但其他攻击方式仍可以产生破坏，如直接攻击服务器。攻击，即利用 Web 系统的脆弱性以实现一定的威胁。攻击的结果多样，如：

其一，未经授权的访问——用户获取了更多权限，从而将应用程序用于其他途径，如获取网站的管理员密码，散布政治言论等。

其二，代码执行——在目标系统上运行恶意代码，且导致其他威胁，如木马。

其三，拒绝服务——合法用户被禁止访问应用程序。

其四，信息失窃——机密的信息被盗取。

其五，破坏信息——信息遭到修改。如站点被涂改、发布攻击性消息和政治言论。

常见的脆弱性及其利用、威胁方式主要有缓冲压溢出、脚本注入和跨站脚本攻击。

### （一）缓冲区溢出

缓冲区溢出是迄今为止 Web 应用中最常被利用的脆弱性。

当应用程序的外部输入未经检查即被插入内存时，便存在缓冲区溢出的脆弱性。如插入长度超过内存为此分配的空间长度，输入就会溢出并占据内存的其他地方，甚至运行恶意代码。

对缓冲区溢出的利用，就是把附加的数据写到内存缓冲区的其他地方，导致程序崩溃。如果附加数据设计巧妙，甚至还可以重写函数的返回地址。如此，程序就会按照攻击者的意愿执行。

在 C++中，这个问题很常见，因为 C++可直接操作内存地址，进行很底层的操作。在.net 中也有这个问题，因为.net 基于托管代码之上，即.net 代码并非直接操作内存，而是在中间隔了一层 CLR。由于托管代码的执行要靠 CLR 作为边界检查，所以 CLR 中的任何脆弱性都将转变为应用程序的脆弱性。如有黑客知道 CLR 的问题，则托管代码也会产生问题。

### （二）脚本注入和跨站脚本攻击

无论何时，用户都要存有“用户都是恶意的”心理，即不能信任用户的随意输入，在用户输入时一定要检验。假如对用户的输入没有严格管理，就会在程序中引入脚本注入的脆弱性。该脆弱性允许用户将自己的脚本注入数据中，如在用户留言中，用户插入 <script>alert（‘error’）；</script>，那么留言的页面就会弹出提示。

跨站脚本的攻击一般表现为一个在 URL 参数中带有客户端的脚本，用来盗取用户的 cookie 信息等，具体为：

（1）SQL 注入。SQL 注入即通过把 SQL 命令插入到 Web 表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令，主要是恶意用户在程序的数据库中执行精心设计的 SQL 语句。其对网络安全威胁很大，甚至能获取服务器管理员的权限。

（2）分布式拒绝服务。分布式拒绝服务也称为 DDoS（Distribute Denial of Service）。DDoS 攻击是用大量的计算机攻击一个系统。很多计算机联合起来就可发送很多虚假请求，致使被攻击的系统超负荷，而丧失向其他用户提供服务的能力。

蓄意攻击者为发动 DDoS，就须获取足够多的机器。恶意用户设计在别人电脑上注入木马和病毒，获取机器控制权，“借”别人的电脑发送攻击。这种被控制的电脑就成为了“僵尸”。

DDoS 攻击主要攻击服务器，且攻击方式防不胜防。因为很多防护软件和防火墙不能区分请求的正确与虚假。

（3）人的问题。很多情况下被利用的脆弱性并非技术上的脆弱性，而是人的脆弱性。假如用户没有安全意识，便极易受骗为攻击者打开系统。欺骗方式多种多样，常见的是用 E-mail 诱使用户执行某些程序，另外还有蠕虫。

（4）蛮力攻击。如不采取一定的措施防止用户无休止的尝试连接应用程序，就容易受到不计其数的猜测密码口令的攻击，即蛮力攻击。

攻击的方式是设计一个程序，用它向目标应用发送很多请求以测试不同的密码口令。

需要注意的是，在考虑安全问题时，人们常常把程序比作一个城堡，在城堡周围建造城墙且严格盘查各个通道。但即使如此，对那些已进入城堡的用户也无计可施。

## 五、计算机网络安全的脆弱性

互联网的体系结构和 TCP/IP 协议在创建之时并未充分考虑安全需要，故存在许多安全漏洞和根本性缺陷，给攻击者留下可乘之机。计算机网络安全的脆弱性主要表现在：

（1）易遭窃听和欺骗。数据包在互联网传输时，要经过很多节点的重发，而局域网内通常采用的以太网或令牌网技术都是广播类型的。这样，窃听者便可轻易得到用户的数据包。如用户数据包没有强有力的加密措施，就等于把信息拱手送给窃听者。比较陈旧的 DNS 服务软件易受虚假的 IP 地址信息欺骗。另一种 IP 地址欺骗方式是在阻塞受害的某台主机后再用受害者的 IP 地址在网络上行骗。

（2）脆弱的 TCP/IP 服务。基于 TCP/IP 协议的服务很多，最常用的有 WWW、FTP、E-mail，此外还有 TFTP、NFS、Finger 等，都存在各种各样的安全问题。WWW 服务所使用的 CGI 程序、Java Applet 小程序和 SSI 都有可能成为黑客得力工具。FTP 的匿名服务造成系统资源的极大浪费。TFTP 则完全没有安全性，常被用来窃取口令文件。E-mail 的安全漏洞曾导致蠕虫在互联网蔓延。E-mail 的电子炸弹和附件经常携带病毒，严重威

胁互联网安全。至于 X Windows 服务、基于 RPC 的 NFS 服务、BSD UNIX 的“r”族服务如 rlogin、rsh、rexec 等，如在配置防火墙时忘记关闭它们在互联网的使用，则用户的内部网络就会裸露在黑客面前。

（3）配置的错误和疏忽。网络系统本身的复杂性导致防火墙的配置相当复杂。在更好的辅助工具出现之前，缺乏训练的网络管理员很有可能发生配置错误，给黑客造成可乘之机。系统配置的过于宽容，或因对服务的安全性缺乏了解而未限制、禁止这些不安全服务，或对某些节点的访问要求给予太多权力，都会给计算机网络安全带来危害。

## 知识拓展

### 一、网络概念简述

#### （一）OSI 模型

网络发展中一个重要里程碑是 ISO（Internet Standard Organization，国际标准组织）对 OSI（Open System Interconnect，开放系统互联）七层网络模型的定义。它不但成为以前与后续的各种网络技术评判、分析的依据，也成为网络协议设计和统一的参考模型。

OSI 七层模型称为开放式系统互联参考模型(如图 1.1 所示)，是一种框架性设计方法，OSI 七层模型通过七个层次化的结构模型使不同系统、不同网络之间实现可靠的通信，帮助不同类型的主机实现数据传输。

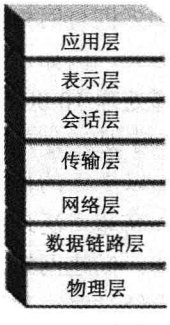

图 1.1　OSI 参考模型

网络七层的划分使网络不同功能模块（不同层次）分担起不同职责，带来如下好处：

（1）减轻问题复杂程度，一旦网络发生故障，可迅速定位故障所处层次，便于查找纠错。

（2）在各层分别定义标准接口，使具备相同对等层的不同网络设备实现互操作，各层之间则相对独立，一种高层协议可放在多种低层协议上运行。

（3）能有效刺激网络技术革新。因为每次更新都可在小范围内进行，不需对整个网络动大手术。

（4）便于研究和教学。

#### （二）SNIFFER 嗅探器

Sniffer Pro 是一款一流的便携式网管和应用故障诊断分析软件，不管在有线网络还是在无线网络中，都能给予网络管理人员实时网络监视、数据包捕获及故障诊断分析能力。基于便携式软件的解决方案具备最高的性价比，且能让用户获得强大的网管和应用故障诊断功能。其主要应用环境为：网络流量分析、网络故障诊断；应用流量分析及故障诊断（已上线或将要上线的应用）；网络病毒流量、异常流量检测；无线网络分析、非法接入设备检查；网络安全检查、网络行为审计。

#### （三）SQL 注入

这是通过把 SQL 命令插入到 Web 表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令。比如，前期很多影视网站泄露 VIP 会员密码

大多是通过 Web 表单递交查询字符而暴出，因这类表单极易遭受 SQL 注入式攻击。

当应用程序使用输入内容构造动态 SQL 语句以访问数据库时，会发生 SQL 注入攻击。如果代码使用存储过程，而这些存储过程作为包含未筛选的用户输入字符串传递，也会发生 SQL 注入，导致攻击者使用应用程序登录到数据库执行命令。如果应用程序使用特权过高的账户连接到数据库，此问题会更加严重。在某些表单中，用户输入的内容直接用来构造（或影响）动态 SQL 命令，或作为存储过程的输入参数，这些表单极易受到 SQL 注入的攻击。这是由于许多网站程序在编写时没有对用户输入的合法性进行判断，或程序本身的变量处理不当埋下了安全隐患。此种情况下，用户只要提交一段数据库查询代码，再根据程序返回即会获得一些敏感信息或控制整个服务器——SQL 注入。

**（四）DDoS 服务攻击**

全名是 Distribution Denial of Service（分布式拒绝服务攻击），很多 DoS 攻击源同时攻击某台服务器即为 DDoS 攻击。其攻击方式有多种，最基本的攻击是利用合理服务请求占用过多服务资源，使服务器无法处理合法用户的指令。

DDoS 攻击手段是在传统 DoS 攻击基础上产生的一类攻击方式。单一 DoS 攻击通常采用一对一方式，当被攻击目标 CPU 速度低、内存小或网带不宽时，攻击效果明显。随着计算机与网络技术发展、计算机处理能力迅速增长、内存大大增加，致使 DoS 攻击难度加大。例如，攻击软件每秒钟可发送 3 000 个攻击包，但用户的主机与网络带宽每秒钟可处理 10 000 个攻击包，则 DoS 攻击未达目的。

于是，分布式的拒绝服务攻击手段（DDoS）应运而生，就是用更多的傀儡机发起进攻，以更大的规模进攻受害者。

高速广泛连接的网络给社会带来巨大方便的同时也为 DDoS 攻击创造了极为有利的条件。低速网络时代黑客占领攻击用的傀儡机时，优先考虑离目标网络距离近的机器，因为经过路由器的跳数少、效果好。而现在电信骨干节点间的连接均以 G 为级别，大城市间更可达到 2.5G 连接，这使攻击可从更远的地方或其他城市发起，攻击者的傀儡机可以分布在更大范围，选择更为灵活。遭受 DDoS 攻击会发生以下现象：

（1）被攻击的主机上有大量等待的 TCP 连接。

（2）网络中充斥大量无用的数据包，源地址为假。

（3）制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通信。

（4）利用受害主机提供的服务或传输协议上的缺陷，反复高速发出特定的服务请求，使受害主机无法及时处理所有正常请求。

（5）严重时会造成系统死机。

**（五）TCP/IP 协议**

TCP/IP 协议即传输控制协议/网际协议（Transmission Control Protocol / Internet Protocol），供已连接因特网的计算机进行通信的通信协议。该协议定义了电子设备（比如计算机）如何连入因特网，以及数据如何在它们之间传输的标准，也是互联网中基本通信语言或协议。在私网中被用作通信协议。当直接网络连接时，计算机应提供一个 TCP/IP 程序副本，此时接收所发送信息的计算机也应有一个 TCP/IP 程序的副本。

相对于 OSI（七层协议）参考模型，TCP/IP 协议的功能实现如表 1.3 所示。

表 1.3　　TCP/IP 与 OSI 模型各层实现功能的对照表

| OSI 中的层 | 功　　能 | TCP/IP 协议族 |
| --- | --- | --- |
| 应用层 | 文件传输、电子邮件、文件服务、虚拟终端 | TFTP、HTTP、SNMP、FTP，SMTP、DNS、Telnet |
| 表示层 | 数据格式化、代码转换、数据加密 | 没有协议 |
| 会话层 | 解除或建立与其他接点联系 | 没有协议 |
| 传输层 | 提供端对端的接口 | TCP、UDP |
| 网络层 | 为数据包选择路由 | IP、ICMP、RIP，OSPF、BGP、IGMP |
| 数据链路层 | 传输有地址的帧及错误检测功能 | SLIP、CSLIP、PPP、ARP，RARP、MTU |
| 物理层 | 以二进制数据形式在物理媒体传输数据 | ISO2110、IEEE802、IEEE802.2 |

数据链路层包括硬件接口和协议。ARP，RARP 两个协议主要用来建立送到物理层的信息和接收从物理层传来的信息。

网络层中的协议主要有 IP，ICMP，IGMP 等，它包含了 IP 协议模块，是所有基于 TCP/IP 协议网络的核心。在网络层中，IP 模块完成大部分功能。ICMP 和 IGMP 及其他支持 IP 的协议帮助 IP 完成特定的任务，如传输差错控制信息以及主机/路由器之间的控制电文等。网络层掌管着网络中主机间的信息传输。

传输层上的主要协议是 TCP 和 UDP。正如网络层控制着主机之间的数据传递，传输层控制那些将要进入网络层的数据。两个协议就是它管理这些数据的两种方式：TCP 是一个基于连接的协议；UDP 则是面向无连接服务的管理方式的协议。

应用层位于协议栈的顶端，主要任务是应用。常用的协议功能如下：

Telnet，提供远程登录（终端仿真）服务。

FTP，提供应用级的文件传输服务，即远程文件访问等服务。

SMTP，电子邮件协议。

TFTP，提供小而简单的文件传输服务，从某个角度说是对 FTP 的一种替换（在文件特别小并且仅有传输需求的时候）。

SNMP，简单网络管理协议。

DNS，域名解析服务，即如何将域名映射成 IP 地址的协议。

HTTP，超文本传输协议，依靠这个协议可在网上看到图片、动画、音频等。

## 二、网站的安全防范技术

由于电子商务网站完全开放的 Internet 网络运行，当客户在计算机系统存放、传输和处理大量支付信息、订货信息、谈判信息、商业机密文件的同时，网络黑客、入侵者、计算机病毒也遍布于网上窃取、篡改和破坏商务信息。为确保电子商务活动的健康发展和正常进行，除应加大对黑客和计算机犯罪的打击力度，还应加强电子商务网站的自身安全防护。

企业在架设电子商务网站时，应对安全措施给予高度重视。

**（一）电子商务网站的安全要求**

从网站内部看，网站计算机硬件、通信设备的可靠性，操作系统、网络协议、数据库系统等自身的安全漏洞，都会影响网站安全运行。从网站外部看，网络黑客、入侵者、计算机病毒也是危害电子商务网站安全的重要因素。电子商务网站的安全包括三方面要求：

（1）网站硬件的安全要求网站的计算机硬件、附属通信设备及网站传输线路稳定可靠，只有经过授权的用户才能使用和访问。

（2）网站软件的安全是指网站软件不被非法篡改、不受计算机病毒的侵害，网站数据信息不被非法复制、破坏和丢失。

（3）网站传输信息的安全是指能确定客户真实身份，确保信息在传输过程中不被他人窃取、篡改或偷看。

**（二）电子商务网站的安全措施**

（1）防火墙技术。这是一个由硬件设备或软件、或软硬件组合而成，在内部网与外部网之间构造的保护屏障。所有内部网和外部网之间的连接都必须经过此保护层，并由它进行检查和连接。只有被授权的通信才能通过防火墙，使内部网络与外部网络在一定意义下隔离，防止非法入侵、非法使用系统资源、执行安全管制措施。

防火墙分为两类：一是包过滤防火墙，它对数据包进行分析、选择，依据系统内事先设定的过滤逻辑确定是否允许该数据包通过；二是代理防火墙，它能将网络通信链路分为两段，使内部网与 Internet 不直接通信，而用代理服务器作为数据中转站，只有可信赖的数据才方可通过。

两种防火墙利弊互见：包过滤器只能结合源地址、目标地址和端口号发挥作用，若攻击者攻破包过滤防火墙，整个网络就会公开；代理防火墙比包过滤器慢，当网站访问量增大时会影响上网速度；代理防火墙在设立和维护规则时比较复杂，有时会导致错误配置和安全漏洞。

由于两种防火墙各有优缺点，故应组合使用。目前最新的防火墙产品集成了代理和包过滤技术，提供了管理数据段和实现高吞吐速度的解决方案。这些混合型设备在安全要求比吞吐速度有更高要求时，能实行代理验证服务；在需要高速时，能灵活采用包过滤规则作为保护方法。

（2）入侵检测系统。防火墙是一种隔离控制技术，一旦入侵者进入了系统，便不受任何阻挡。它不能主动检测和分析网络内外的危险行为，捕捉侵入罪证。而入侵检测系统能监视和跟踪系统、事件、安全记录和系统日志，以及网络的数据包，识别任何无益活动，更能预先检测入侵者攻击，利用报警与防护系统报警、阻断攻击。入侵检测系统采用的技术有特征检测和异常检测两种。

特征检测。假设入侵者活动用一种模式表示，特征检测的目标是检测主体活动是否符合这些模式。它能检查出原有的入侵方法，但对新的入侵方法尚无能为力。其难点是，设计出的模式既能表现“入侵”现象又不影响正常活动的问题没有解决。

异常检测。假设入侵者活动异于正常主体活动。根据该理念建立主体正常活动的“活

动简档”，将当前主体活动状况与“活动简档”相比较，当违反其统计规律时，即判断该活动属“入侵”行为。异常检测的难题在于如何建立“活动简档”及如何设计统计算法，不把正常操作作为“入侵”或忽略真正“入侵”行为。

（3）网络漏洞扫描器。这是一个漏洞和风险评估工具，用于发现、发掘和报告安全隐患和可能被黑客利用的网络安全漏洞，分为内部扫描和外部扫描。

内部扫描。漏洞扫描器以 root 身份登录目标主机，记录系统配置的各项主要参数，将之与安全配置标准库进行比较和匹配，凡不满足者即视为漏洞。

外部扫描。通过远程检测目标主机 TCP/IP 不同端口的服务，记录目标给予的回答，搜集到很多目标主机信息，例如：是否能用匿名登录、是否有可写的 FTP 目录、是否能用 TELNET 等。然后与漏洞扫描系统提供的漏洞库进行匹配，满足匹配条件则视为漏洞；也可通过模拟黑客进攻手法，对目标主机系统进行攻击性的安全漏洞扫描。如果模拟攻击成功，则视为漏洞存在。

（4）防病毒系统。由于病毒在网络中存储、传播、感染的途径多、速度快、方式各异，对网站危害大，应采用全方位防病毒产品，实施“层层设防、集中控制、以防为主、防杀结合”的防病毒策略，构建全面的防病毒体系。常用防病毒技术有：

反病毒扫描。通过分析病毒代码找出能成为病毒结构线索的惟一特征。病毒扫描软件可搜索这些特征或其他能表示有某种病毒存在的代码段。

完整性检查。通过识别文件与系统的改变发现病毒。但完整性检查程序只有当病毒正发作时才起作用，而网站可能在完整性检查程序开始前已感染病毒，从而避开检查。

行为封锁。行为封锁可防止病毒破坏。这种技术可在病毒发作时阻止它。一旦反常情况发生，行为封锁软件即会检测出并警告用户。

（5）启用安全认证系统。企业电子商务网站除须保持网站本身硬件与软件安全，还包括保持传输信息安全，使这些重要信息在传输过程中免遭他人窃取、偷看或修改。安全认证系统的作用是，对重要信息采用密码技术加密，接收方收到密文后再行解密、还原。目前电子商务中普遍采用 SSL 安全协议。该协议主要提供以下服务：

其一，认证用户和服务器，使它们能确信数据将被发送到正确的客户机和服务器上。

其二，加密数据以隐藏被传送数据。

其三，维护数据完整性，确保数据在传输过程中不被改变。

企业电子商务网站的设计人员需在认真进行安全分析、风险评估、商业需求分析和网站运行效率分析的基础上，制定整体安全解决方案。主要把握：为保证整体安全解决方案的效率，各安全产品间应实现联动机制。当漏洞扫描器发觉安全问题，即通知系统管理员，及时采取补漏措施；当入侵检测系统检测到攻击行为时，即利用防火墙实时阻断；当防病毒系统发现新病毒时，亦能及时更新入侵检测系统的病毒攻击库，提高入侵检测系统检测效率。由于安全产品和服务器、安全产品与安全产品之间都需进行必要的数据通信，为保证通信的保密性和完整性，可采用安全认证手段。只有各种安全产品实现联动，网络安全才有保障。