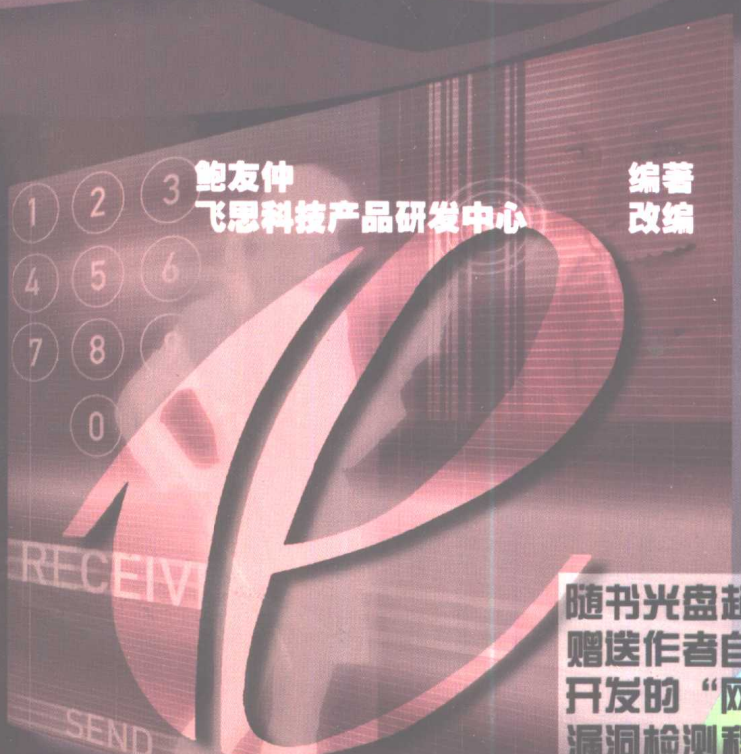
飞思教育
FECIT-Education
www.fecit.com.cn

技胜e筹

网络安全之防黑秘诀

精选台湾省最畅销精品计算机图书精心改编

鲍友仲 编著
飞思科技产品研发中心 改编



随书光盘超值赠送作者自行开发的“网络漏洞检测程序”

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn
PHEI

知城數位

网络安全之防黑秘诀

鲍友仲　编著

飞思科技产品研发中心　改编

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书精选台湾省最畅销精品计算机图书精心改编，书中针对黑客入侵 Web 网站的方法和防护措施进行了全面的介绍。

本书从最基本的黑客入侵网站的原理介绍起，循序渐进地介绍了一些较为简单的入侵网站的方法以及黑客直接利用 Windows NT/2000 系统中的漏洞进行入侵的方法及防护措施，并在最后介绍了 Windows NT/2000 系统中 Service Pack 的安装方法。

本书面向初、中级用户，可作为企业网管及家庭用户防范黑客入侵的参考书，是一本实用操作型的技术手册。

本书繁体字版名为《骇客解冻——Web 网站篇》，由知城数位科技股份有限公司出版，版权属鲍友仲所有。本书简体中文版由知城数位科技股份有限公司授权电子工业出版社独家出版。未经本书原版出版者和本书出版者书面许可，任何单位和个人均不得以任何形式或任何手段复制或传播本书的部分或全部内容。

图书在版编目（CIP）数据

网络安全之防黑秘诀/鲍友仲编著. —北京：电子工业出版社，2002.1
（技胜e筹）
ISBN 7-5053-7361-7

Ⅰ.网… Ⅱ.鲍… Ⅲ.计算机网络—安全技术，Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2001）第 093138 号

丛 书 名：技胜e筹
书　　名：**网络安全之防黑秘诀**
编　　著：鲍友仲
改　　编：飞思科技产品研发中心
责任编辑：卢国俊
排版制作：电子工业出版社计算机排版室监制
印 刷 者：北京大中印刷厂
出版发行：电子工业出版社　http://www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787×980　1/16　印张：17.25　字数：441.6 千字
版　　次：2002 年 1 月第 1 版　2002 年 1 月第 1 次印刷
书　　号：ISBN 7-5053-7361-7
　　TP・4242
印　　数：5 000 册　　定价：29.00 元（含光盘）
版权贸易合同登记号：01-2001-4019

凡购买电子工业出版社的图书，如有缺页、倒页、脱页、所附磁盘或光盘有问题者，请向购买书店调换。若书店售缺，请与本社发行部联系调换。电话　68279077

出版说明

天涯远不远？

不远！

咫尺有多近？

很远！

……

不经意间，我们从闲庭梦一般地漫步到了曾经还一度幻想着的 21 世纪。这是一个网络与电脑的时代，由于两者的普及与发展，空间被无限扩大，时间被大大节省，天涯与咫尺的距离变得从未有过的模糊，坐地日行八万里不再是浪漫主义的豪情，不出门便知天下事也成为了现实。从前我们一直在织梦，现在，梦就在我们眼前，活生生的，怎么，我们还要梦呓吗？

不要再呢喃了，当成一种生活去认真对待吧。

电脑、鼠标、网络，去追赶，还是徘徊？

徘徊不等于落伍，享受不等于成功，只有追赶才是硬道理。在这个日新月异的时代，每个人都能在感受到便捷的同时感受高速带来的生存压力……

电子工业出版社计算机图书研发部秉承其为读者服务的宗旨，隆重推出了《技胜e筹》系列丛书，希望能够以此向读者传达一份理念，告诉他们生活才刚刚开始；更希望为读者带来一个惊喜，使他们理解，其实时代并不会将每个人抛弃太远；当然，最重要的是为读者指明一条道路，当您在新时代中自由翱翔时，就会感觉到一份来自飞思的关怀和动力。

我们真的希望每个人的人生都能因此变得快乐而充实。

品牌标识：飞思教育 FECIT Education www.fecit.com.cn　飞思在线 FECIT Online www.fecit.com.cn

电子工业出版社计算机图书研发部

于北京

关 于 飞 思

新世纪之初的北京，一群满怀共同理想的年轻人聚集在飞思教育产品研发中心的旗帜下，他们将新的希望和活力注入了中国 IT 教育产品开发领域。飞思人在为把自己打造成为中国 IT 教育产品研发的精英团队而更加不懈努力。

21 世纪的今天，飞思人在多元化教育产品的开发和出版等方面已经迈出了坚实的第一步，开拓出属于自己的一片天空，初步赢来了涓涓细流。

如今，本着教育为科技服务的宗旨，飞思教育产品研发中心拓展为飞思科技产品研发中心，并以崭新的面貌等待您的支持与关注。

飞 思 人 理 念

我们经常感谢生活的慷慨，让我们这些原本并不同源的人得以同本，为了同一个梦想走到一起。

因为身处科技教育前沿，我们深感任重道远；因为伴随知识更新节奏，我们一刻不敢停歇。虽然我们年轻，但我们拥有

“严谨、高效、协作”的团队精神

全方位、立体化的服务意识

实力雄厚的作者群和开发队伍

当然，最重要的是我们拥有：

恒久不变的理想和永不枯竭的激情和灵感

正因如此，我们敢于宣称：

飞思教育＝丰富的内容+完美的形式

这也是你和我共同精心培育的品牌 

的承诺。

“问渠哪得清如许，为有源头活水来。”路再远，终需用脚去量；风景再美，均需自然抚育。

年轻的飞思人愿为清风细雨、阳光晨露，滋润您发芽，成长；更甘当坚实的铺路石，为您铺就成功之路。

此为试读，需要完整PDF请访问：www.ertongbook.com

前　言

关于本丛书

当今世界是e化的世界，因为电脑与 Internet 的普及和其特有的亲和性，无论是国家、大型企业还是个人用户，都能在几乎毫无限制的情况下，成为 WWW 中的一员。而由于电脑和网络的日益发达，整个世界正在逐渐变得越来越趋向融合。

作为这个日新月异的世界中的一员，您是否有过困惑，有过迷茫，不知自己该何去何从，不知该如何来适应这个社会，如何紧跟世界的潮流呢？抑或您苦于充电无门，想学习而又找不到好的资料呢？

《技胜e筹》系列丛书是电子工业出版社计算机图书研发部在充分考虑大陆地区读者需求的基础上，精选了一批由台湾地区资深专家编写的经典计算机图书，由飞思科技产品研发中心组织著名的专家、学者精心改编而成。本丛书在内容和版式上都有着其他同类图书不可比拟的优点：既符合读者的需求，又有一定的技术权威性，从内容上保证了图书的质量，是一套实用的指导性丛书。

《技胜e筹》系列丛书精彩的内容和完美的版式相得益彰，相信会给渴求完美的您带来一份惊喜，会让您在e化的世界中自由遨游，开拓属于自己的天空。

关于本书

网络安全是目前每一位网络管理员都关心的一个主要问题，人们几乎每天都能听到一些新闻，报道又有一家高级公司或政府的网站遭到攻击。在偶尔清净的几天里，人们也许又会听到一种专门攻击 WWW 服务器的网络病毒正在肆虐的蔓延。例如在 2001 年夏天出现的红色代码（Red Code）病毒，就是一种专门利用操作系统漏洞攻击 WWW 服务器的病毒。当时在数据中心的机房内，各个公司的网络管理员需要排队才能进入机房维护服务器。

总结所有网站遭到黑客或病毒攻击的事件，您可以发现，无论是黑客还是病毒，他们大多数都是利用系统漏洞进行攻击。如果网络管理员能够站在黑客的角度，对系统漏洞进行检查并加以防范，那他的网站就可以抵御大多数的黑客攻击。当然有些黑客还会使用其他一些方法获得对服务器的控制权，例如使用三十六计中的“美人计”从网络管理员处窃取账户信息。当然这种问题的防范措施不在本书的讨论范围内。

本书将以 Microsoft 公司的 Windows NT/2000 作为服务器系统平台，介绍其漏洞的详细信息和防范方法。全书逻辑思路清晰，按照黑客通常使用的攻击手段，将主题分为“使用漏洞直接攻击”、“使用漏洞间接攻击”和“使用其他方法进行攻击”，并且书中针对每一种攻击方式，都对其防范的方法做出了详细的阐述。另外在本书的附录中还介绍了大量与网络安全相关的网站，这些网站时常会介绍一些最新的网络安全信息。

本书由电子工业出版社计算机图书研发部策划，飞思科技产品研发中心组织改编，主要由崔羽、郑东明、王永辉、张守凯、高鹏、许卫等人参与本书的改编工作，在此表示感谢。由于本书涉及的内容丰富，加之篇幅、时间所限，故书中不足之处，敬请读者批评指正。

我们的联系方式：

电话：（010）68131648　　（010）68134545

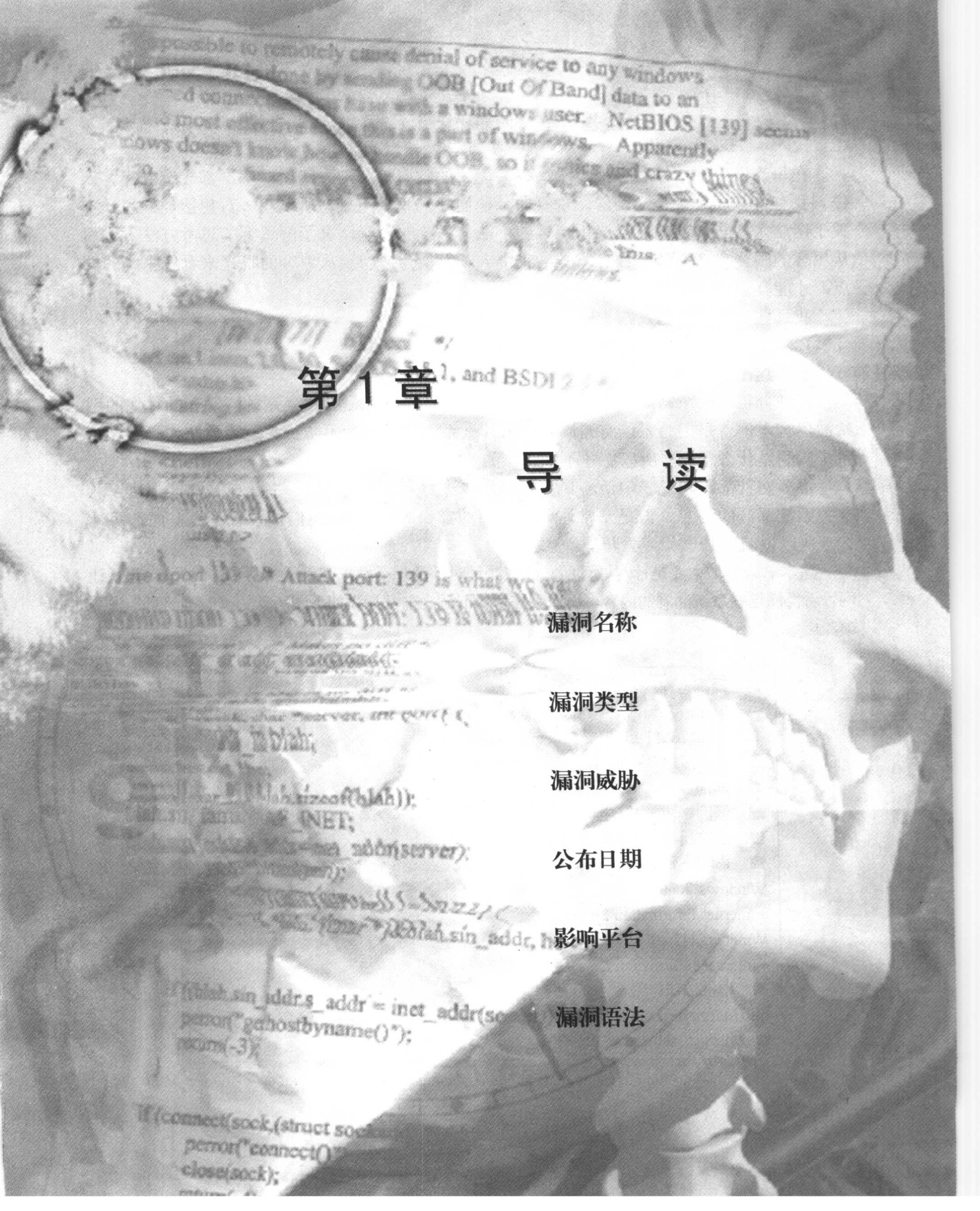
E-mail：support@fecit.com.cn

网址：http://www.fecit.com.cn　　http://www.fecit.net

电子工业出版社计算机图书研发部

目　录

此为试读,需要完整PDF请访问: www.ertongbook.com



第1章

导　　读

漏洞名称

漏洞类型

漏洞威胁

公布日期

影响平台

漏洞语法

在每次发生的“黑客大战”中，许多无辜的政府机关与民间企业网站都会遭到黑客入侵。我有许多朋友都是当网管，说真的，他们其实是很无辜，所以我一直想帮他们写一本关于网站入侵防护的书，以分析黑客的手法、系统的漏洞，来了解黑客的思考方法，进而从黑客的眼光来看系统要如何防护。我个人一直认为，您要从黑客的眼光来看您系统的弱点，才能真正知道防护的重点在哪里。

我那些当网管的朋友常常问我以下两个问题：

1. **“为什么我的网站被黑客入侵？”**
2. **“这个系统漏洞是什么？究竟要如何防护？”**

仔细分析这两个问题，其实您会发现他们问的内容都是有关“系统漏洞”的。您的网站被黑客入侵就是因为系统有漏洞，但为什么系统有漏洞却不防护呢？因为您不知道这个系统漏洞是什么意思，所以您才不知道该如何防护。

很多网管都跟我说一句话，其实他们非常努力，常常从网络、书籍或是其他渠道注意有关系统漏洞的消息，但是常常这些消息写的都很“精简”，他们根本看不懂里面在写什么，所以也就不知该如何去防护。

这本书既然最主要是针对网管所写（或是针对那些想了解黑客入侵网站手法的人），为了让网管看得懂这些系统漏洞的内容，所以我在每个漏洞之前都加上如下图所示的“漏洞信息”说明项。

■ 漏洞名称：
一. 微软命名为“Absent Directory Browser Argument”漏洞（MS00-044）
二. “IIS ISM.DLL 泄露文件部分内容的漏洞”
三. 黑客俗称“+.htr”泄露文件信息的漏洞
■ 漏洞类型：信息泄露型
■ 漏洞威协：低~中
■ 公布日期：200 年 7 月 17 日
■ 影响平台：
Windows 2000
+Internet Information Server 5.0
Windows NT 4.0
+Internet Information Server 4.0
■ 漏洞语法：
http://target/test.pl+.htr
http://target/global.asa+.htr

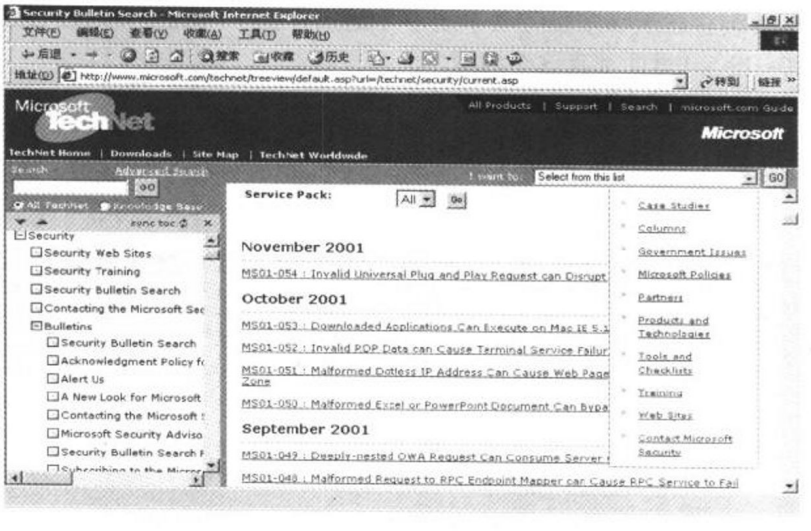
这些说明项的作用是让网管能够很快就了解这个漏洞的基本情况。下面简单地解释一下各个说明项中内容的意义。

漏洞名称

通常很多网管找不到漏洞相关的资料，原因是他们不知道这个漏洞的名称是什么、黑客一般如何称呼它，或软件厂商官方如何称呼它。所以在“漏洞名称”说明项里，会列出黑客一般称呼它的名称及微软官方称呼它的名称，在微软名称后面的“MS00-044”编号，是这个漏洞在微软网站安全布告栏里面的编号，通过此编号您可以连到微软安全公告网站，网址为：

http://www.microsoft.com/technet/security/current.asp

如下图所示 ，通过编号的名称您可以迅速找到有关这个漏洞的微软官方信息，对于帮助您防护漏洞，这个编号是很重要的。



漏洞类型

通常情况，漏洞的类型可以分为三种类型：

“攻击入侵型”——黑客可以通过这个漏洞入侵到服务器里，并可以更换您网站的网页。

“攻击死机型”——黑客可以通过这个漏洞攻击服务器，可以使服务器停止服务，结果是使您网站崩溃。

“信息泄露型”——黑客可以通过这个漏洞取得服务器内的机密信息，如“ASP 程序

源代码”、“客户账户资料”和“服务器系统文件”等机密文件。

漏洞威胁

我们可以将一个漏洞对于您服务器的危害程度分为“低”、“中”、“高”三大等级。通常列入在“高”等级以上的系统漏洞，表示可以让黑客直接攻击造成服务器危害。

公布日期

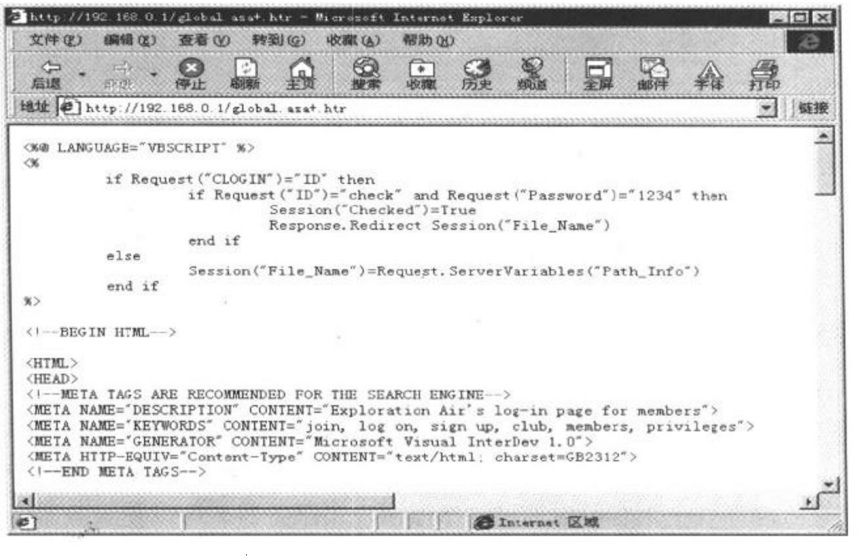
说明漏洞第一次在全球发表的日期，或是后续更新信息的时间。“公布日期”能够帮助您很快了解这个漏洞是新发现还是旧漏洞，对于网管来说，如果您的服务器存有一堆旧系统漏洞的话，那您真的要检讨一下，自己是不是对于系统安全太不重视，为什么旧漏洞到现在还没防护。

影响平台

说明表示漏洞存在于哪些服务器系统中。是只存在于 Windows NT+IIS 4.0，还是连 Windows 2000+IIS 5.0 里面都有这个漏洞。

漏洞语法

“漏洞语法”表示漏洞直接通过 IE 浏览器就可以入侵/测试的语法。如使用漏洞语法“http://server/global.asa+.htr”，在 IE 浏览器中执行的结果如下图所示。



除了对上面这些漏洞信息说明项的阐述之外，我还把漏洞分成两大类：

“黑客直接入侵攻击”——黑客可以借助这个漏洞直接执行攻击或入侵。

“黑客间接入侵攻击”——黑客可以利用从这个漏洞搜集到的信息，间接执行攻击或入侵。

通常直接入侵攻击的漏洞威胁性都较高，所以各位网管一定要防护系统漏洞。

此为试读，需要完整PDF请访问：www.ertongbook.com