电脑报 大众网络报 POPUNET WEEK

黑客首

漏洞攻击防范实例配套手册

漏洞终极攻防战

数百种最新漏洞利用方法 让你随心所欲……

著名全团体『中国鹰盟』创始人 万涛 主编

体验炸毁QQ快感　抢夺聊天管理权　IE把电脑变肉机

控制网站『走后门』　清除漏洞保权限　对DoS攻击说NO！

FTP主机转个遍　让Word『自动工作』

修改ROOT空密码　邮件服务信息防泄漏

山东电子音像出版社出版

nt "\nServer returned an ADO misconfiguration message\nAborting.\n";
b content_start{ # this will take in the server headers my (@in)=@_; my $c;for ($c=1;$c<500;$c++){ if($in[$c] =~/^\x0d\x0a/){if ($in[$c+1]
/^HTTP\/1.[01] [12]00/){ $c++; }else{ return $c+1; }}return -1;}# it should never get here actually
(@in)=@_; my $error=odbc_error(@in);if($error=~/ADO could not find the specified provider/){
my (@in)=@_; my $error=odbc_error(@in);

漏洞攻击防范实例配套手册

漏洞终极攻防战

山东电子音像出版社出版

my (@in)=@_; my $error=odbc
sub content_start{ # this will t
=~/^HTTP\/1.[01] [12]00/){ $c++
Da/){if ($in[$c+1]=~/^HTTP\/1.[01] [12]00/){ $c++; }else{ return $c+1; }}}return -1;}#
if($error=~/ADO could not find the specified provider/){
erver headers my (@in)=@_; my $c;for ($c=1;$c<500;$c++){ if($in[$c] =~/^\x0d\x0a/){if ($in[$c+1]
rn $c+1; }}}return -1;}# it should never get here actually

内容简介

计算机中存在大大小小，花样百出的漏洞。这些漏洞小则导致系统崩溃，大则导致非法用户以有机可乘，掌握计算机的控制权，从而给计算机的使用者带来不可估量的损失。那么漏洞究竟是什么？究竟有哪些漏洞？利用这些漏洞困难吗？如何才能封堵自己计算机上的漏洞？在书中我们将会给你明晰的答案。

注：本手册只从技术角度讨论漏洞，不得利用本手册所介绍内容进行不法活动。违者将受到法律制裁，于本社无关。

光盘运行环境

CPU 主频	PII 500 以上
分辨率	800×600 像素以上
内存	32M 以上
显存	8M 以上
光驱	8 倍速以上
操作系统	Win9x/2000/XP

光盘内容简介：中国安全教育网独家授权自创经典黑客歌曲。

扫描软件视频录像全辑——让你轻松学会扫描各种漏洞！

漏洞攻击防范实例 配套手册

策　　划：大众网络报社
制　　作：山东翔宇软件开发中心
责任编辑：刁　戈
特约编辑：乔康毅　王　洁
作　　者：候成岗
出版发行：山东电子音像出版社
装帧设计：敬　婕　朱　艳
光盘定价：19.8 元（本手册随盘赠送）

目录 contents

第一章 软件漏洞

第一节 聊天软件

第二节 上传下载软件漏洞

第三节 浏览器漏洞

目录
contents

目录 contents

第二节 RedHat 漏洞

第三节 HPUX 系统漏洞

第四节 FreeBSD 系统漏洞

第五节 Solaris 漏洞

目录
contents

第三章 服务器漏洞

第一节 WEB 服务器

第二节 FTP 服务器

目录 contents

第三节 邮件服务器漏洞

第四节 数据库服务器漏洞

第五节 流媒体服务漏洞

第六节 脚本漏洞

目录
contents

第一章 软件漏洞

/^\x0d\x0a/){if ($in[$c+1]=~/^HTTP\/1.[01] [12]00/){ $c++; }else{ return $c+1; }}}return -1;}#
b content_ in the server headers my (@in)=@_; my $c;for ($c=1;$c<500;$c++){ if($in[$c] =~/^\x0d\x0a/){if ($in[$c+1]=~/^HTTP\/1.[01] [12]00/){
++; }else{ return $c+1; }}}return -1;}# it should never get here actually
V (@in)=@_; my $error=odbc_error(@in);if($error=~/ADO could not find the specified provider/){

第一章要讲到的是漏洞篇中最常见的软件漏洞。众所周知，软件是我们平时上网用得最多的东西，像聊天用的软件：QQ、MSN 等，浏览网页要用浏览器软件：Internet Explorer、Netscape 等，上传网页要用到上传软件：Cutfp、Leapftp 等。它们虽然给我们带来了很大的方便，但是都有漏洞存在，大多数漏洞可以导致入侵者直接进入我们的电脑，破坏我们的数据。那么我们经常使用的这些软件到底漏洞在哪里呢？在这一章中，就为大家依次分析一些危险大、传播广的软件漏洞，好让大家在懂得其危害的同时，采取措施防范漏洞。

第一节　聊天软件

说到聊天，我估计在坐的每一个朋友都经历过吧！先不说早期网络上流行至今的 IRC，就拿目前国内的一些娱乐站点的聊天室，飞速发展的即时通讯软件（例如：QQ，MSN 等）来说，就可以看出聊天在我们网络生活中占有多大的份量。

这些聊天软件在方便我们与朋友交流、与家人联系、与同事工作的同时，难道真的就是那么尽如人意吗？其实不然，相当一部分聊天软件都存在漏洞。这些漏洞轻则导致系统不能正常使用，重则导致机密文件泄露或是系统崩溃。到底这些聊天软件的漏洞危害在哪里？我们大家又如何防范？在这一节，大家将会全面接触到。

一、QQ 大字体导致程序崩溃

漏洞概述：大家知道，理论上在 QQ 中最大只能发送 22 号大的文字给对方，但实际上可以突破这种限制发送任意大的字给对方，这时候 QQ 会调用 Riched20.dll 文件，而该文件存在一个缓冲区溢出漏洞。就是这个漏洞可导致使用此 DLL 模块相应功能的应用程序崩溃。经分析得出结论，当字体大小数字串长度超过 32 字节时，就会引发缓冲区溢出，当超过 34 字节以后就有可能导致应用程序崩溃。

适用环境：QQ2000c、QQ2003、QQ2003II 和 QQ2003III 测试版

攻击原理：相信大家知道，在 QQ 中最大只能发送 22 号的字体给对方，有没有别的办法让我们突破这种限制发送任意大的字号或图形给对方呢？答案是有！这就是本文所要讲的一个关于“大字体导致缓冲区溢出漏洞”。下面告诉大家该怎样做。首先，要求接收方使用最新版的 QQ，发送方可以使用任意版本的 QQ，在 QQ 好友名单中选定一个好友的头像，选择“收发消息”，在出现的“发送消息”窗口，输入如下字串：

{\urtf\deflang2052{\fonttbl{\f0\fprq2\a comic sans ms;}{\f1\a 宋体}}

{\colortbl ;\red250\green50\blue199;\red20\green230\blue100;\red250\green180\blue0;\red100

图 1-1

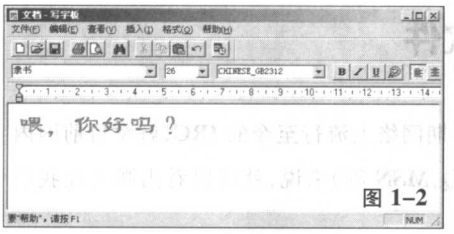

图 1-2

图 1-3

图 1-4

green200\blue250;}\pard\cf1\f0\fs100 Hap\cf2\fs80 Py n\cf3\fs50 eW y\cf4\fs120 eaR\cf0\f1\fs18 \par }

点击“送讯息”按钮，对方就会收到特大的一行文字：**Happy new year**(如图 **1-1**)，不但字母大小不一，而且每一个字的颜色都不一样！你的 **QQ** 好友一定会惊喜不已，因为在正常的情况下对方是不会收到这么大的文字的！

那么如何得到以上代码呢？这是用写字板和 **16** 进制文件编辑器 **UltraEdit-32** 得到的。首先，在 **Windows** 自带的写字板中输入你想发送的内容并编辑这些内容，比方说你可以在写字板中选择字体为隶书，然后给每一个要发送的字选择不同的颜色，要发送的内容的大小也可以在写字板中选择，在文号下拉列表框中填入你想发送的字符的大小即可（如图 **1-2**）。

然后在写字板的“文件”菜单中选择“另存为”，在“保存类型”下拉列表框中找到“**Rich Text** 格式 **(RTF)**”，将其保存为 **RTF** 文件即可(如图 **1-3**)。

现在，运行 **UltraEdit-32**，用它打开这个编辑好的 **RTF** 文件，你会看到这个 **RTF** 文件的内容就是我们上面输入的那些代码！

在通常情况下，最上面的一行代码“**{\rtf1\ansi\ansicpg936\deff0 {\fonttbl {\f0\fnil\fprq2 comic sans ms;}{\f1\fnil\fcharset134 \'cb\'ce\'cc\'e5;}}**”不能起到作用，把它改成以下代码“**{\urtf\deflang2052{\fonttbl{\f0\fprq2\a comic sans ms;}{\f1\a** 宋体**}}**”，这样，所有版本的 **QQ** 就都能接收到你发的超大型文字了。包括 **QQ2003III** 系列的最新版本。

把所有的代码写到 **QQ** 中，然后发给你的朋友，对方就会看到你精心准备的这些内容！如果你想临时改变发送文字的大小，可以在 **QQ** 中将上面那些代码“**\pard\cf1\f0\fs100 Hap\cf2\fs80 Py n\cf3\fs50 eW y\cf4\fs120 eaR\cf0\f1\fs18 \par }**”中任何一个“**fs**”后面的数值改成你所要的大小即可。如果想再简单一点，可以直接在 **QQ** 的信息栏中在上面这一行代码中修改你想要发的文字。按照这个原理和方法，不仅能发送文字，还可以发送特殊字符，效果非常好(如图 **1-4**)。

另外，如果你将“**fs**”后面的代码改得非常大，比方将它改为 **30** 个 **9** 然后发送给对方，猜猜看会怎样？在屏幕上将出现一个对话框，显示非法操作，然后 **QQ** 将自动关闭（如图 **1–5**）！

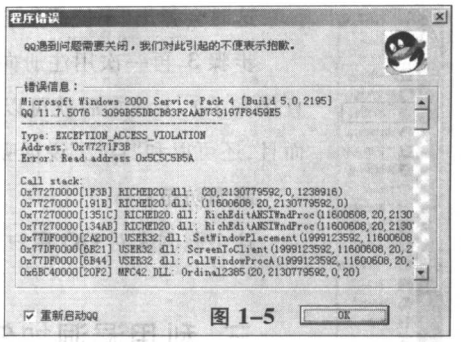

图 1–5

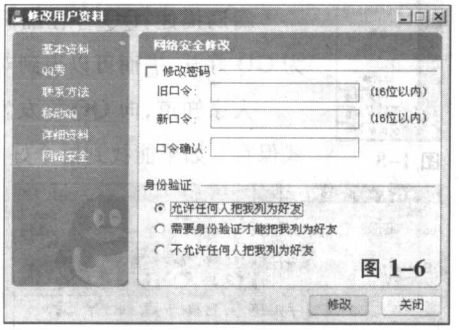

图 1–6

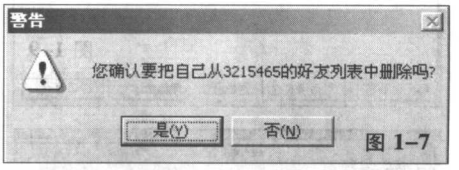

图 1–7

攻击原理：

漏洞描述：这一招可以让自己的头像出现在本身的列表上，这不仅显得很酷，而且有很实用的功能哦！其实最早期的 **QQ** 版本中是可以直接把自己加为好友的，现在的版本却行不通了。但是只要我们肯动手，没有什么能难倒我们的。

适用系统：所有 **QQ** 版本

这是由于 **QQ** 会调用 **Riched20.dll** 文件，而该文件存在一个缓冲区溢出漏洞，该漏洞可使用此 **DLL** 模块使相应功能的应用程序崩溃。经高手分析得出，当字体大小数字串长度超过 **32** 字节时，就会引发缓冲区溢出。当超过 **34** 字节以后就有可能导致应用程序崩溃。目前很多软件包括国内最流行的既时通讯软件 **QQ(QQ2000c 0825** 版本以后)和网易泡泡都受此漏洞影响，对方可以给你发送一个包含利用漏洞的攻击消息，那你的 **QQ** 在查看对方的消息时会立即崩溃。

在 **QQ** 出现非法操作下线后，仍然可以重新登录 **QQ** 上线，而且可以查看到对方发来的源代码，所以建议大家不要用这个办法搞破坏，因为别人完全可以“以彼之道还施彼身”。

防范方法：使用 **QQ2003III** 系列的新版本 **QQ** 不会受此漏洞影响，你可以把给你发送这种恶意代码的人加入到“黑名单”中，这样他就没法骚扰你了。或者在“好友个人设定”标签中，找到“不接收该好友发来的任何消息”，在前面打上“√”，也可以防范对方发送这样的代码给你，或者可以在 **http://hacker.popunet.com/download/ms-qool.RAR** 下载相应的补丁。

二、利用 QQ 漏洞将自己添加为好友

步骤 1 首先建议 **QQ** 的个人设定里设置身份验证方式为“允许任何人把我列为好友”（如图 **1–6**），然后切换到“黑名单”组，在里面空白处点击右键并选“添加坏人名单”，输入自己的 **QQ** 号码，**QQ** 会自动提示，是否删除这个号码（如图 **1–7**），别管它，尽管删除即可。

步骤 2 接下来再把这个“坏人”（即自己的 **QQ** 号）拖到“我的好友”组中去，这时候会出现系统消息，**XXXX** 请求身份验证，通过身份验证。

图 1-8

这时会弹出“不能添加自己”的提示，不理会它，直接退出 QQ。

步骤 3 再一次用注册向导登录时(注意这里一定要用注册向导方式进行登录，而不要直接登录)，上线之后就可以看见自己的头像已经在自己的好友 QQ 列表中了(如图 1-8)，而且，还可以和“自己”说话呢！

漏洞防范：

这个漏洞未对 QQ 用户造成任何攻击和危害，带来的只是好玩和新奇，所以不用防范。

三、利用漏洞加任意号码到 QQ 好友中

漏洞描述：QQ 存在漏洞，可以使攻击者在未曾通过用户身份验证的时候，直接加对方为 QQ 好友，进而可以得到对方的 IP 地址等危险信息。

大家知道，向 QQ 好友发送消息时，他的 QQ 号码会出现在内存地址中，并以明文的方式保存。如果能找到这个好友的 QQ 号码在内存中的地址，并将这个内存地址中的数据，即该 QQ 号码换为想加入的那个人的 QQ 号，并锁定该数据，这样只要不关机，无论怎么开、关 QQ，内存地址中“记住”的永远都是这个新 QQ 号。点击这个 QQ 好友准备发送消息，更新资料，会发现他的号码变为你想加入的那个人的 QQ 号码了！利用这个特性，可以尝试将任何号码加入到 QQ 号码中。

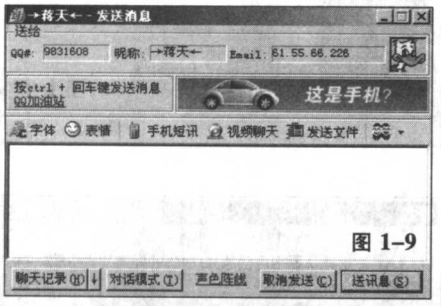

图 1-9

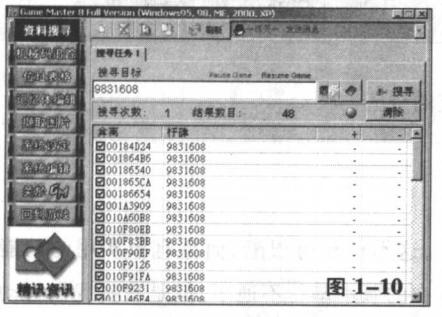

图 1-10

图 1-11

适用版本：任何 QQ 版本

攻击原理：当攻击者想加某人到自己的 QQ 好友中，进而获取其 IP 地址等危险信息的时候，如果对方拒绝，那该怎么办？攻击者使用一个方法可以随意加任何人到你的 QQ 好友名单中！首先攻击者得准备一款游戏修改软件，如 FPE2001 或 Game Master8.0 都行。以 Game Master8.0 为例。

步骤 1 假设攻击者要加的 QQ 号码是 821661，前提条件是必须要有身份验证号，但不要直接发消息请求加入。先找一个自己本身的 QQ 好友，假设是 9831608，然后打开发送信息框(如图 1-9)。

步骤 2 启动 Game Master 8.0，点左侧的“资料搜寻”，点右上方的下拉菜单，在其中找到“发送信息”一项，然后向修改游戏一样，在搜索目标中填入 9831608 这个号码，点右侧“搜寻”，一般情况下你会找到好多这样的地址(如 1-10)。

将它们全都选中，然后点右键，在弹出菜单中选择“把所有记号都加入”，在数值项中填入我们要加的 QQ 号并在“自

动锁定”前面打上钩(如图 **1–11**)。

步骤 **3** 重新运行一下 **QQ**,在好友里就会出现 **821661** 这个号码了(如图 **1–12**),但是对他发的消息只能出现在对方的“陌生人”名单里。**OK**,已经成功地将这个号加为好友了。此漏洞暂时没有解决办法,就连“拒绝任何人加为好友”也不管用了。

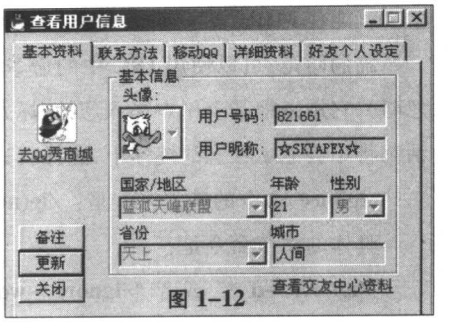

图 1–12

漏洞防范:惟一要做的就是当这种人出现你的陌生中,立即把他拖进黑名单即可。

四、MIRC DCC SEND 缓冲器溢出让 MIRC 受到影响

漏洞描述:英国 **MIRC** 公司出品的 **IRC** 类客户端软件,目前风靡于全世界。界面优美,彩色文本行,具有全 **dcc**、**xdcc** 文件发送和接收能力,**aliases**, 能远程命令和事件操作与位置相关的下拉菜单、**www** 和声音支持。世界相当多国家的人都在使用 **mIRC** 进行交流! **MIRC DCC SEND** 缓冲器溢出漏洞可能允许远程攻击者导致 **mIRC** 客户系统崩溃。来自“**DCC SEND**”的一个请求能够引起致命的错误,导致受影响的 **mIRC** 客户系统崩溃。攻击者可以利用这个漏洞使 **mIRC** 遭受影响。

适用系统:

Khaled Mardam-Bey mIRC 6.1

Khaled Mardam-Bey mIRC 6.11

不受影响系统:

Khaled Mardam-Bey mIRC 6.12

攻击原理:

攻击者只需要在使用 **mICR** 聊天的过程中(如图 **1–13**),输入以下请求(如图 **1–14**):

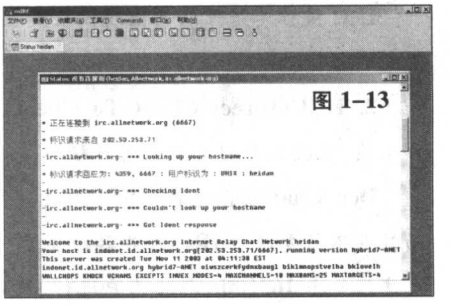
图 1–13

/quote PRIVMSG #mirc :^ADCC SEND ″a a a a a a a a a a a a a a a a a a a a

a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a

a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a

a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a

a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a

a a″ 1363975063 3500 4^A

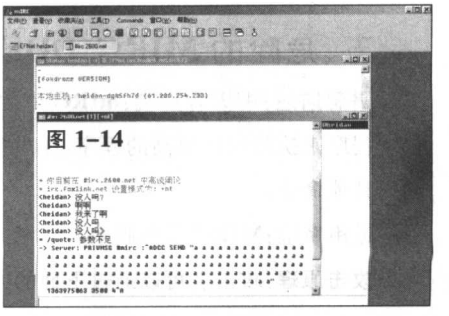
图 1–14

就能使 MIRC 客户系统崩溃，严重影响客户的正常使用！

漏洞防范：可以使用 IRC 中的命令来禁止有 DCC Chat 有关的连接，这个命令是：**/ignore** 命令（即忽略），它用来把某个用户加入您的“坏人黑名单”。一旦某个用户进入了你的 IRC 的黑名单，他说的任何话都将不会显示在您的终端上，这样就达到了防范的目的！

/ignore 命令的基本格式是：**/ig(nore)** 用户昵称

具体的防范命令是：

"/ignore -d *" 或者 **"/ignore -wd *"**（如图 **1-15**）。

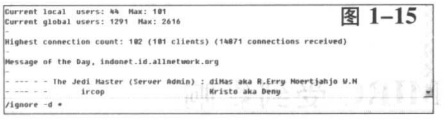

图 1-15

当然也可以升级 MIRC 的程序版本来防止这个漏洞，前面说过不受影响系统是：**Khaled Mardam-Bey MIRC 6.12**，可以去 MICR 的官方主页下载：**http://www.mirc.com/get.html**。

注意：IRC 的聊天方式经常以命令开头代表某种方式，例如：**/exit**，断开服务器的连接，并关闭 mIRC；**/help** ，弹出 mIRC 的 help 窗口；**/Join** 命令加入一个指定的频道，例如：**/Join #China** 等。

上面提到的**/quote** 命令也是 IRC 常用命令之一。

小知识：

1. IRC(Internet Relay Chat，国际互联网中继交谈）。简单来说就是来自世界各地的 IRC 用户登录上 IRC 服务器，由 IRC 服务器把他们彼此的交谈信息中继给彼此，但是 RFC1459 协议赋予了 IRC 更强大的功能。目前世界上较大的国际性 IRC 服务网络有美国的 **Undernet, DalNet, EFNet**，中国大陆的 IRC 网络有 **SunNet**，**263** 首都在线，**PCHome**。

IRC 被称为是互联网出现以来最激动人心的服务，它和目前风行的 ICQ 具有本质的不同。IRC 具有真正的社区性。

2. DCC(Direct Client To Client)是一个 IRC 中的 CTCP 协议下面的子协议，通常直接客户对客户交谈、直接客户对客户文件传输即是通过这个协议实现的。

Dcc Chat 跟普通的私聊不同之处在于，两个人的聊天信息不需要服务器中继，这样不但更加安全，而且也不必受限于 IRC 服务器的速度，但是必须双方都能够互相联接上对方。比如上海 **8888VIP** 用户就无法跟一个 **163ChinaNet** 用户进行 **DCC Chat**，因为他们彼此无法联接上对方。

五、危险的 MIRC DDE 安全权限漏洞

漏洞描述：聊天客户端：mIRC 中的 **DDE (Dynamic Data Exchange)** 存在一个漏洞可以导致一般权利程序来执行权限更高的程序。如当管理员在执行 DDE 服务时，一般用户可以利用漏洞以管理员身份运行其他命令。

适用系统：MIRC 所有版本。

攻击原理：攻击者可以通过下面的方法来达到利用 mIRC 中的 DDE 存在漏洞的目的。