

# Window2003服务器安全配置方案

华安普特

HAPT

## 前言:

安全是相对的,安全防护不是追求一个永远也攻不破的安全技术,安全体系应能够保证在入侵发生,系统部分损失等较大风险产生时,关键任务不能中断,保持网络的生存能力。

安全防护是有时效性的,今天的安全明天就不一定很安全,因为网络的攻防是此消彼长,道高一尺,魔高一丈的事情,尤其是安全技术,它的敏感性、竞争性以及对抗性都是很强的,这就需要不断的检查、评估和调整相应的策略。

## 目录:

第一节 安装 Windows 2003 Server

第二节 安装和配置IIS

第三节 FTP服务器架设

第四节 win2003系统安全设置

第五节 IIS安全设置

第六节 设置安全的虚拟主机访问权限

## □□□ 安装 Windows 2003 Server

### 一、注意授权模式的选择(每服务器,每客户):

建议选择“每服务器”模式,用户可以将许可证模式从“每服务器”转换为“每客户”,但是不能从“每客户”转换为“每服务器”模式.,以后可以免费转换为“每客户”模式。

所谓许可证(CAL)就是为需要访问Windows Server 2003的用户所购买的授权。有两种授权模式:每服务器和每客户。

每服务器:该许可证是为每一台服务器购买的许可证,许可证的数量由“同时”连接到服务器的用户的最大数量来决定。每服务器的许可证模式适合用于网络中拥有很多客户端,但在同一时间“同时”访问服务器的客户端数量不多时采用。并且每服务器的许可证模式也适用于网络中服务器的数量不多时采用。

每客户:该许可证模式是为网络中每一个客户端购买一个许可证,这样网络中的客户端就可以合法地访问网络中的任何一台服务器,而不需要考虑“同时”有多少客户端访问服务器。该许可证模式适用于企业中有多台服务器,并且客户端“同时”访问服务器的情况较多时采用。

微软在许可数上只是给了你一个法律上的限制,而不是技术上的。

所以假如你希望服务器有更多的并发连接,只要把每服务器模式的数量改的大一些即可。这个数量会限制到windows中所有的网络应用,包括数据库。

### 二、安装时候使用NTFS分区格式,设定好NTFS磁盘权限。

C盘赋给administrators

和system用户组权限,删除其他用户组,其它盘也可以同样设置。注意网站最好不要放置在C盘。

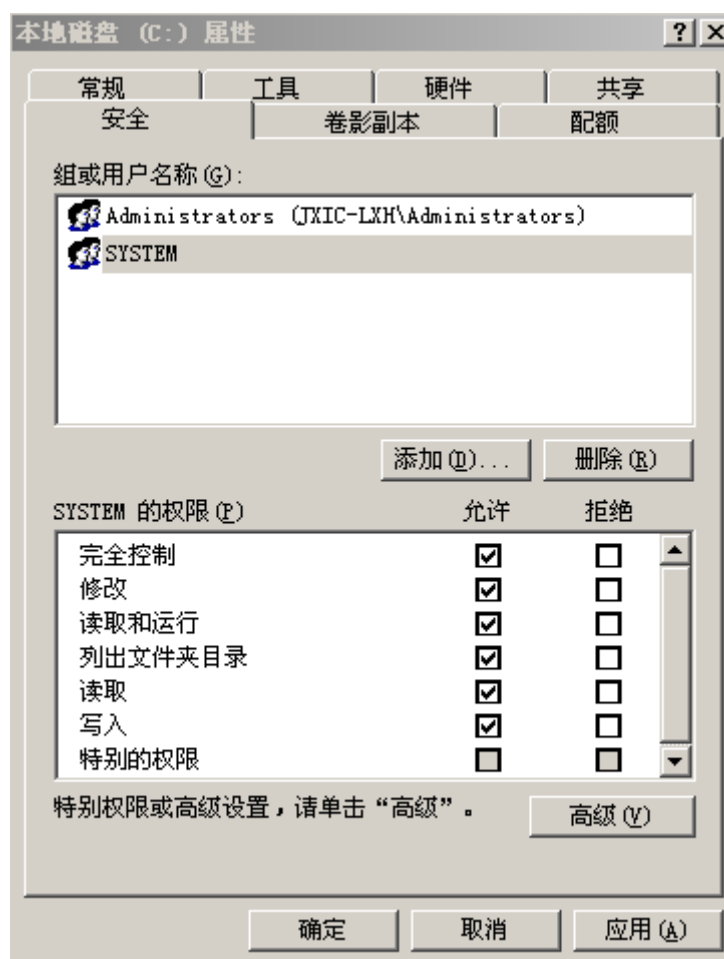
Windows目录要加上给users的默认权限,否则ASP和ASPX等应用程序就无法运行。另外,还将c:\windows\system32

目录下的一些DOS命令文件:net.exe, cmd.exe, tftp.exe, netstat.exe, regedit.exe, at.exe, attrib.exe, caccls.exe, 这些文件都设置只允许administrators访问。

另外在c:/Documents and

Settings/这里相当重要,后面的目录里的权限根本不会继承从前的设置,如果仅仅只是设置了C盘给administrators权限,而在All Users/Application Data目录默认everyone用户有权限,这样入侵这可以跳转到这个目录,写入脚本或只文件,再结合其他漏洞来提升权限;譬如利用serv-

u的本地溢出提升权限，或系统遗漏有补丁，数据库的弱点，甚至社会工程学等方法，在用做web/ftp服务器的系统里，建议是将这些目录都设置的限定好权限。



### 三、禁止不必要的服务和增强网络连接安全性

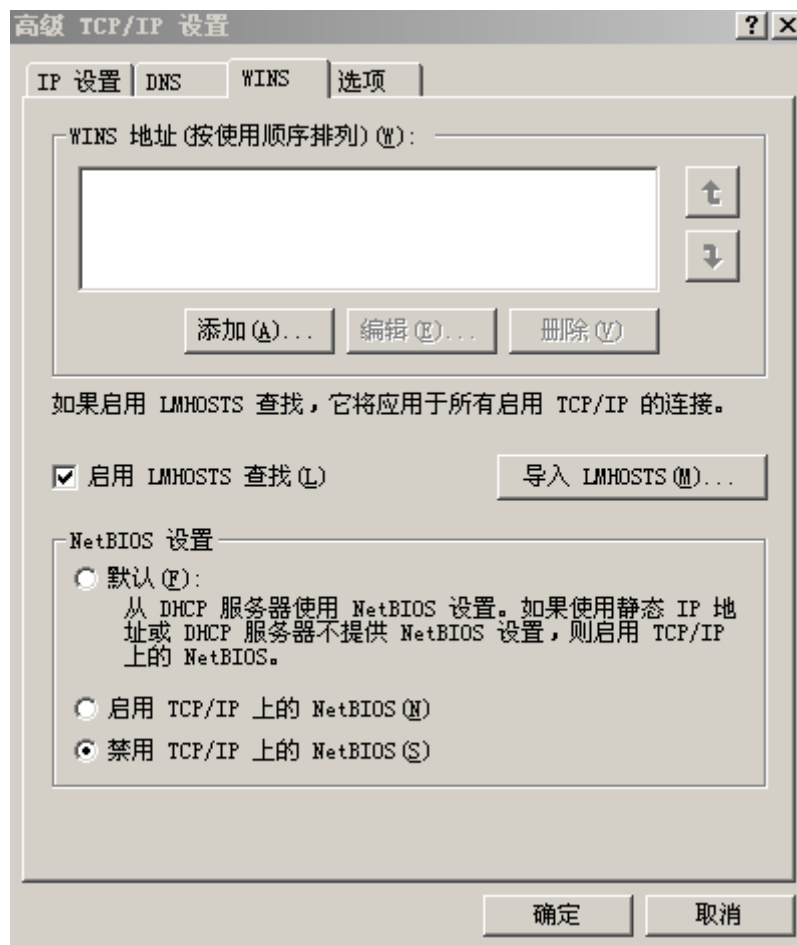
把不必要的服务都禁止掉，尽管这些不一定能被攻击者利用得上，但是按照安全规则 and 标准上来说，多余的东西就没必要开启，减少一份隐患。

在“网络连接”里，把不需要的协议和服务都删掉，这里只安装了基本的Internet协议(TCP/IP)，由于要控制带宽流量服务，额外安装了Qos数据包计划程序。

在高级tcp/ip设置里--

“NetBIOS”设置“禁用tcp/IP上的NetBIOS(S)”。在高级选项里，使用“Internet连接防火墙”，这是windows 2003

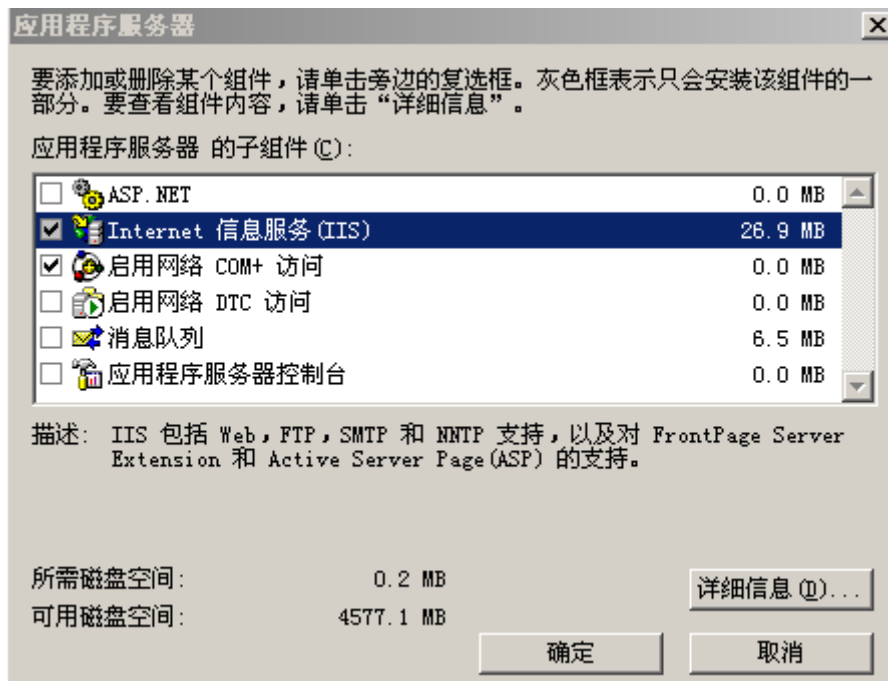
自带的防火墙，在2000系统里没有的功能，虽然没什么功能，但可以屏蔽端口，这样已经基本达到了一个IPSec的功能。



**注意：不推荐使用TCP/IP筛选里的端口过滤功能。**譬如在使用FTP服务器的时候，如果仅仅只开放21端口，由于FTP协议的特殊性，在进行FTP传输的时候，由于FTP特有的Port模式和Passive模式，在进行数据传输的时候，需要动态的打开高端口，所以在使用TCP/IP过滤的情况下，经常会出现连接上后无法列出目录和数据传输的问题。所以在2003系统上增加的windows连接防火墙能很好的解决这个问题，所以都不推荐使用网卡的TCP/IP过滤功能。



一、仅安装必要的组件，选择Internet(信息服务IIS)即可。原则是网站需要组件功能才安装，比如ASP.NET或其它组件不需使用就不要安装。



## 二、修改上传文件的大小

Windows server 2003服务器, 当上传文件过大(超过200K)时, 提示错误号 2147467259。原因是IIS6.0默认配置把上传文件限制在200k, 超过即出错。解决方法如下:

- ☐ 首先, 停止以下服务:
- ☐ IIS admin service
- ☐ World Wide Web Publishing Service
- ☐ HTTP SSL
- ☐ 然后找到:

C:\Windows\system32\inet\metabase.xml \Windows\system32\inet\metabase.xml(不要用写字板, 要用记事本编辑, 否则容易出错。)

☐ 找到: ASPMaxRequestEntityAllowed 默认为 204800 (200k), 改成需要的! 保存。

☐ 最后, 启动上面被停止的服务, 就完成了!

☐ 注: 可能会碰到metabase.xml

文件不能被保存, 原因是你的服务未停干净, 建议重启以后再进行上面的操作。

## 第三节 FTP服务器架设

### 一、推荐使用Serv-U FTP Server Corporate v6.0.0.2

1. Serv-U最好不要使用默认安装路径, 设置Serv-U的目录权限, 只有管理员才能访问;

2. 启用Serv-U中的安全, serv-u的几点常规安全设置:

选中“Block “FTP bounce” attack and FXP”。什么是FXP呢? 通常, 当使用FTP协议进行文件传输时, 客户端首先向FTP服务器发出一个“PORT”命令, 该命令中包含此用户的IP地址和将被用来进行数据传输的端口号, 服务器收到后, 利用命令所提供的用户地址信息建立与用户的连

接。大多数情况下,上述过程不会出现任何问题,但当客户端是一名恶意用户时,可能会通过在PORT命令中加入特定的地址信息,使FTP服务器与其它非客户端的机器建立连接。虽然这名恶意用户可能本身无权直接访问某一特定机器,但是如果FTP服务器有权访问该机器的话,那么恶意用户就可以通过FTP服务器作为中介,仍然能够最终实现与目标服务器的连接。这就是FXP,也称跨服务器攻击。选中后就可以防止发生此种情况。

另外在“Block anti time-out schemes”也可以选中。其次,在“Advanced”选项卡中,检查“Enable security”是否被选中,如果没有,选择它们。



3. 可修改Serv-U的默认管理员名字和密码,默认端口也可以修改,详情见附录。

#### 第四节 win2003系统安全设置

- 1、将一些危险的服务禁止,特别是远程控制注册表服务及无用和可疑的服务。
- 2、关闭机器上开启的共享文件,设置一个批处理文件删除默认共享。
- 3、封锁端口

黑客大多通过端口进行入侵,所以你的服务器只能开放你需要的端口以下是常用端口:

80为Web网站服务;21为FTP服务;25 为E-mail SMTP服务;110为Email POP3服务。其他还有SQL Server的端口1433等,不用的端口一定要关闭!

关闭这些端口,我们可以通过Windows 2003的IP安全策略进行。

借助它的安全策略,完全可以阻止入侵者的攻击。你可以通过“管理工具→本地安全策略”进入,右击“IP安全策略”,选择“创建IP安全策略”,点[下一步]。输入安全策略的名称,点[下一步],一直到完成,你就创建了一个安全策略:

接着你要做的是右击“IP安全策略”,进入管理IP筛选器和筛选器操作,在管理IP筛选器列表中,你可以添加要封锁的端口,这里以关闭ICMP和139端口为例说明。

关闭了ICMP,黑客软件如果没有强制扫描功能就不能扫描到你的机器,也Ping不到你的机器。关闭ICMP的具体操作如下:点[添加],然后在名称中输入“关闭

ICMP”，点右边的[添加]，再点[下一步]。在源地址中选“任何IP地址”，点[下一步]。在目标地址中选择“我的IP地址”，点[下一步]。在协议中选择“ICMP”，点[下一步]。回到关闭ICMP属性窗口，即关闭了ICMP。

下面我们再设置关闭139，同样在管理IP筛选器列表中点“添加”，名称设置为“关闭139”，点右边的“添加”，点[下一步]。在源地址中选择“任何IP地址”，点[下一步]。在目标地址中选择“我的IP地址”，点[下一步]。在协议中选择“TCP”，点[下一步]。在设置IP协议端口中选择从任意端口到此端口，在此端口中输入139，点[下一步]。即完成关闭139端口，其他的端口也同样设置

然后进入设置管理筛选器操作，点“添加”，点[下一步]，在名称中输入“拒绝”，点[下一步]。选择“阻止”，点[下一步]。

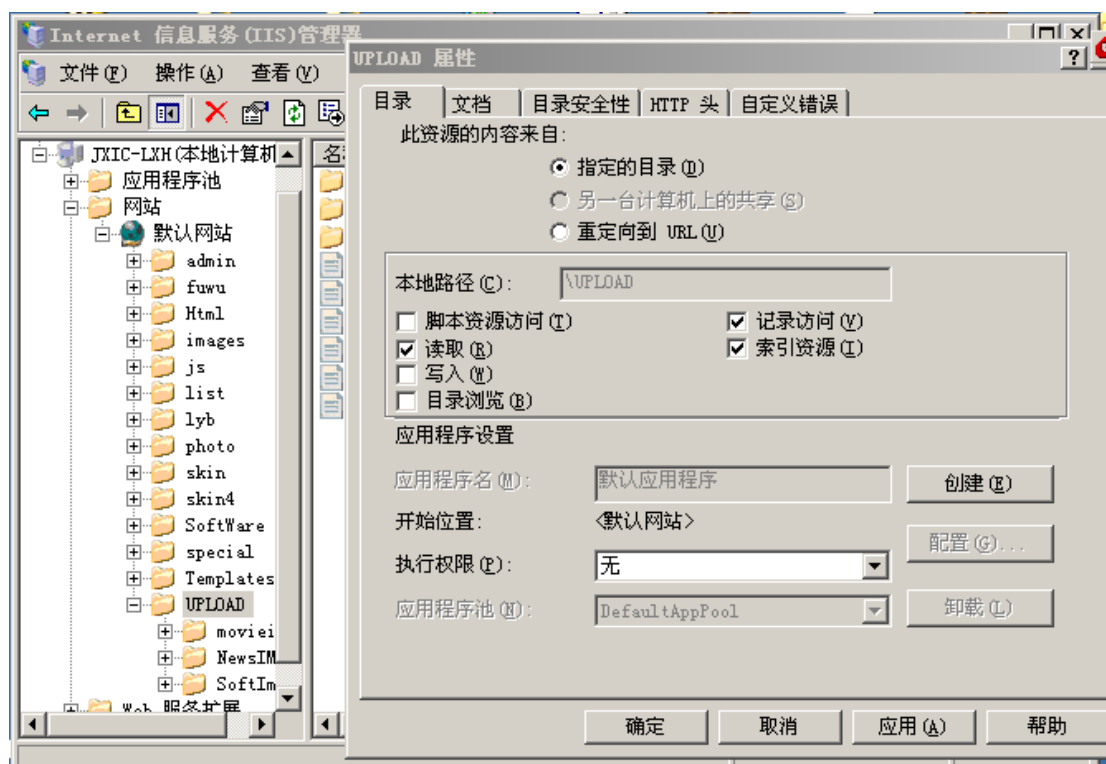
然后关闭该属性页，右击新建的IP安全策略“安全”，打开属性页。在规则中选择“添加”，点[下一步]。选择“此规则不指定隧道”，点[下一步]。在选择网络类型中选择“所有网络连接”，点[下一步]。在IP筛选器列表中选择“关闭ICMP”，点[下一步]。在筛选器操作中选择“拒绝”，点[下一步]。这样你就将“关闭ICMP”的筛选器加入到名为“安全”的IP安全策略中。同样的方法，你可以将“关闭139”等其他筛选器加入进来。

最后要做的是指派该策略，只有指派后，它才起作用。方法是右击“安全”，在菜单中选择“所有任务”，选择“指派”。IP安全设置到此结束，你可根据自己的情况，设置相应的策略。

### 第五节 IIS安全设置

- 1、删掉c:/inetpub目录，删除iis不必要的映射。
- 2、使用虚拟主机的每个web站点都应该新建单独的IIS来宾用户。
- 3、IIS为每个虚拟主机设置来宾帐号，这样即使一个网站由于后台漏洞被入侵也不会波及整台服务器，整个服务器管理权限不会沦陷。
- 4、IIS管理后台设置限定IP地址访问，仅仅开放需要进入后台的IP。
- 5、IIS管理器内一些文件夹内只有图片并没有程序(例如image、pic)，可将其运行权限设置为无(默认可运行脚本)。
- 6、将IIS日志默认保存位置修改至其它分区，防止黑客入侵后删除安全事件及web日志。
- 7、防止ASP木马程序入侵的三种办法：

1) 上传目录的权限选择无执行权限，即使上传木马也会因无执行权限而入侵失败。



访问时可执行文件的ASP显示：

网页无法显示

您要访问的网页中存在程序问题，因此无法显示网页。

请尝试下列操作：

- 打开 [www.eligun.com](http://www.eligun.com) 主页，然后寻找指向所需信息的链接。
- 单击 **刷新** 按钮，或者以后重试。

HTTP 403.1 禁止访问：禁止可执行访问  
Internet 信息服务

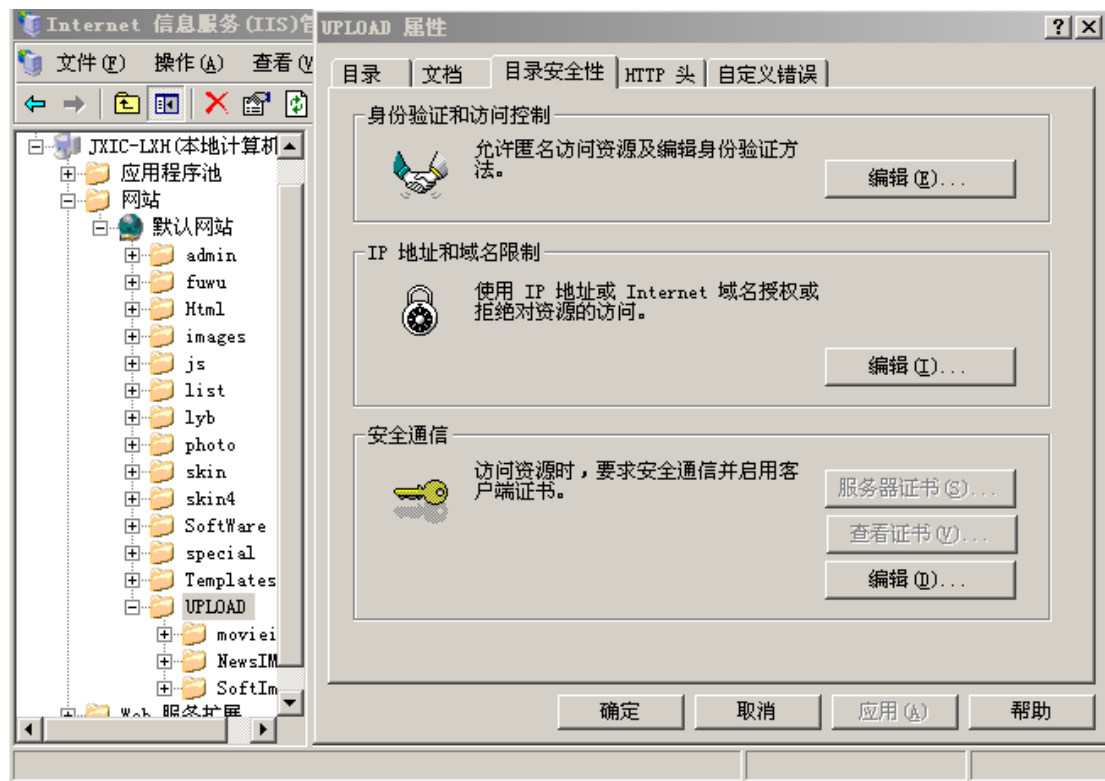
技术信息（支持个人）

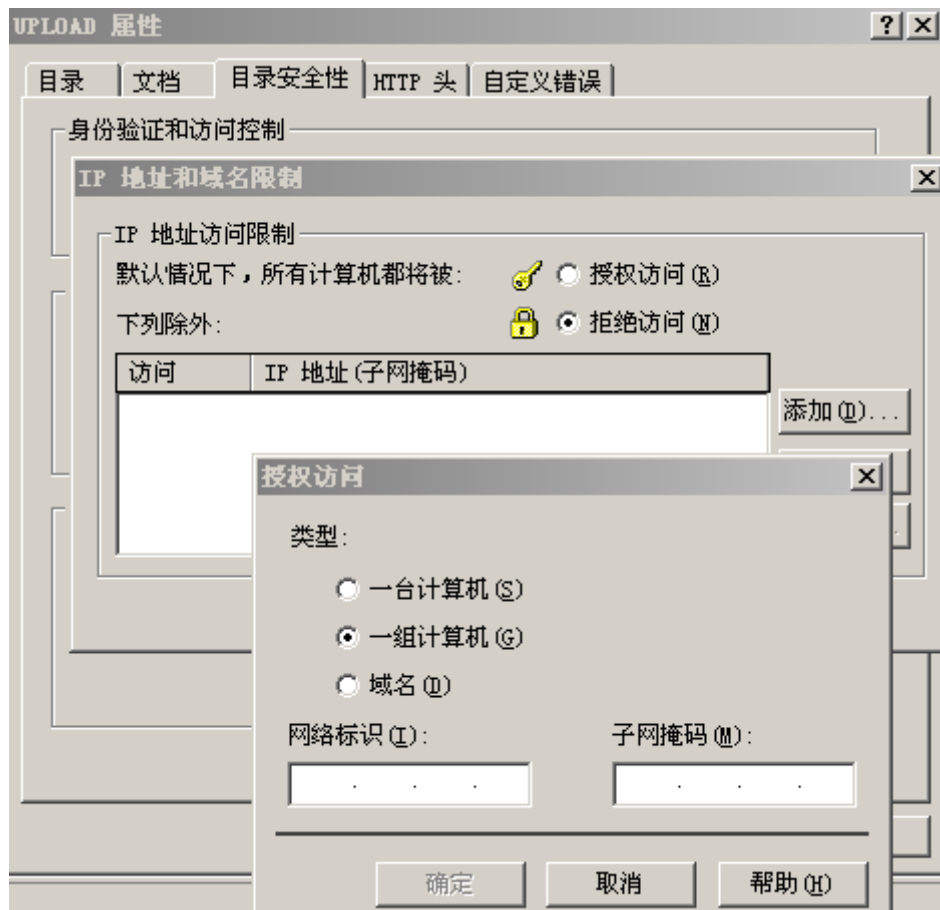
- 背景：  
您试图从目录中执行 CGI、ISAPI 或其他可执行程序，但该目录不允许执行程序。
- 详细信息：  
[Microsoft 支持](#)



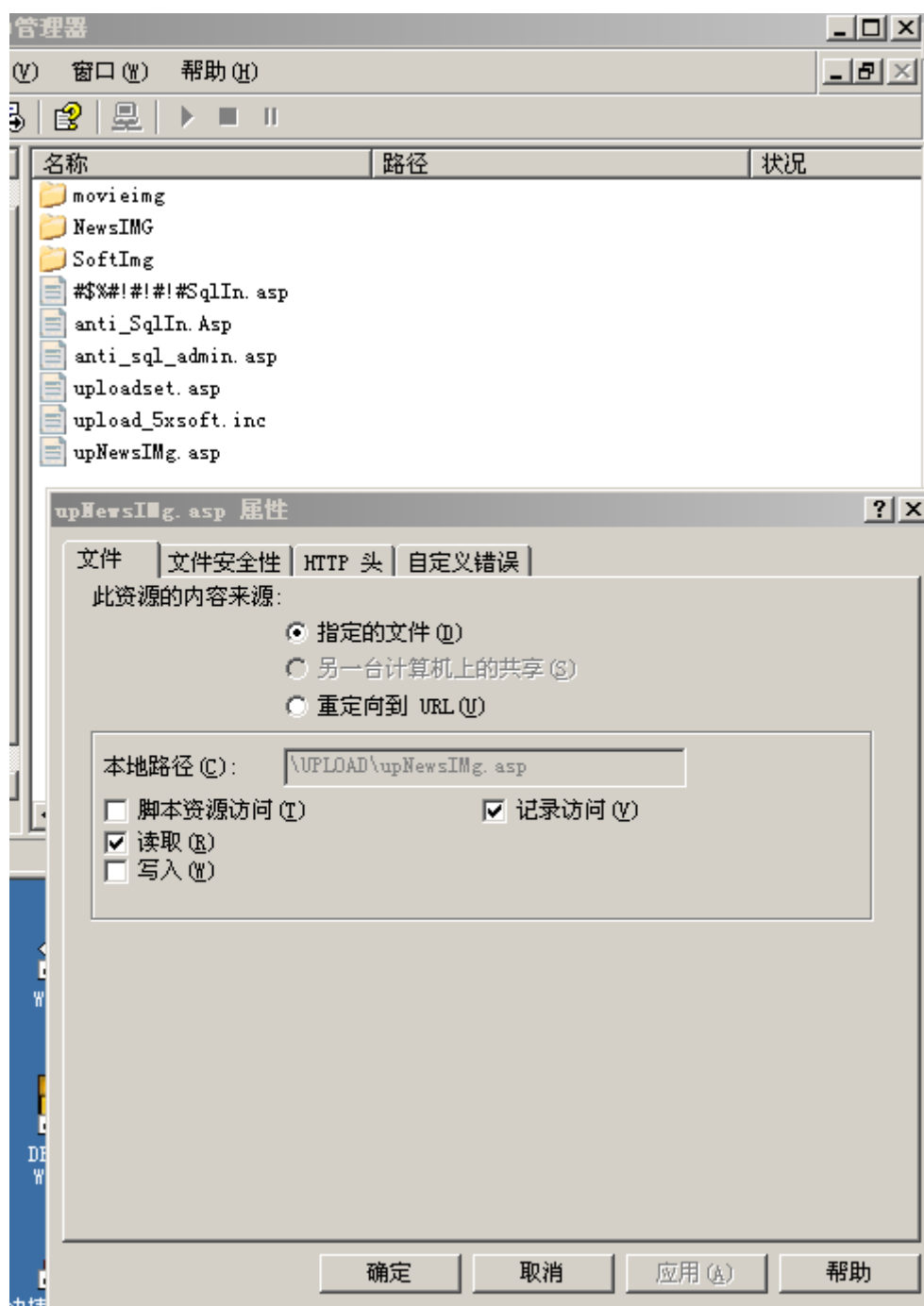
2) 上传的文件加上IP地址限制，只允许信息员机器IP地址访问。

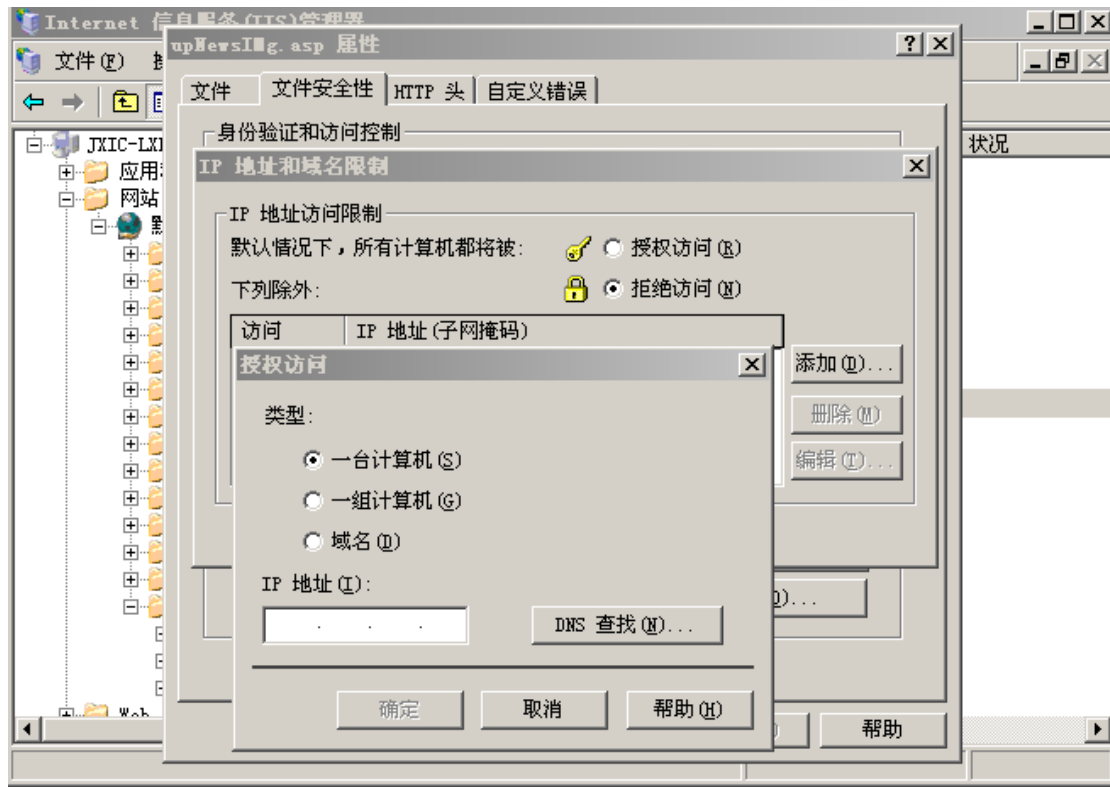
a. 目录限定：





b. 文件限定：





3□ 在上传文件中增加验证程序, 比如:

```
<!--#include FILE="../admin/check.asp"-->
```

这样打开页面即提示:

- 您没有进入本页面的权限, 本次操作已被记录!
- 本页面为[栏目管理员]等级以上用户专用, 请先[登陆](#)后进入.

4□ 加入防注入代码, 在上传文件入口处或关键程序中增加一行代码调用防注入

程序, 可以登陆后台对防注入程序进行管理, 查看入侵扫描信息。代码不要放在首页, 这样影响网站打开速度, 网站首页的ASP代码要尽可能少, 最好已经是HTML, 调用数据库内容太多会影响网站速度。

SQL通用防注入系统管理登陆

Password:

Login

系统更新记录:

更新记录:

2.0增强版 增加了自动封注入者Ip功能，使注入者不能再访问本站！  
3.0版 在2.0增强版的基础上，加入了后台管理功能：  
可以查看入侵者提交数据记录功能，解除对注入者ip封锁，以及删除注入记录功能！  
v3.1版 对核心代码做了优化，去除了一个没用的循环，使程序执行速度更快！  
使程序执行速度更快自定义警告信息，解决对post过滤而不能正常发帖问题，  
解决js和vbs通用问题,做到了真正意义上的asp通用防注入

SQL通用防注入系统 3.1 js&vbs通用版 (c)2005-6

登陆后台页面

SQL通用防注入系统

系统设置查看信息退出登陆

编号	操作 I P	是否锁定	操作	操作页面	操作时间	提交方式	提交参数	提交数据
<input type="checkbox"/> 1	66.249.66.201	已锁定	解锁IP	/interaction/show.asp	2006-5-11 2:51:08	Get	<%	MM_keepURL ((MM_keepURL!=
<input type="checkbox"/> 2	220.203.0.6	已锁定	解锁IP	/interaction/show.asp	2006-5-10 11:26:03	Get	<	MM_keepURL ((MM_keepURL!=
<input type="checkbox"/> 3	218.87.32.201	已锁定	解锁IP	/interaction/show.asp	2006-5-9 18:51:54	Get	ID	558 And 1=A
<input type="checkbox"/> 4	218.87.32.201	已锁定	解锁IP	/interaction/show.asp	2006-5-9 18:51:54	Get	ID	558 And 1=2
<input type="checkbox"/> 5	218.87.32.201	已锁定	解锁IP	/interaction/show.asp	2006-5-9 18:51:54	Get	ID	558 And 1=1
<input type="checkbox"/> 6	218.87.32.201	已锁定	解锁IP	/interaction/show.asp	2006-5-9 18:51:54	Get	ID	558%' And 1=2 And '%='
<input type="checkbox"/> 7	218.87.32.201	已锁定	解锁IP	/interaction/show.asp	2006-5-9 18:51:54	Get	ID	558%' And 1=1 And '%='
<input type="checkbox"/> 8	218.87.32.201	已锁定	解锁IP	/interaction/show.asp	2006-5-9 18:51:54	Get	ID	558' And 1=2 And '='
<input type="checkbox"/> 9	218.87.32.201	已锁定	解锁IP	/interaction/show.asp	2006-5-9 18:51:53	Get	ID	558' And 1=1 And '='
<input type="checkbox"/> 10	218.87.32.201	已锁定	解锁IP	/interaction/show.asp	2006-5-9 18:51:50	Get	ID	558 And 1=2
<input type="checkbox"/> 11	218.87.32.201	已锁定	解锁IP	/interaction/show.asp	2006-5-9 18:51:50	Get	ID	558 And 1=1
<input type="checkbox"/> 12	218.87.32.201	已锁定	解锁IP	/interaction/show.asp	2006-5-9 18:51:50	Get	ID	558%' and user+char(124)=0 and 'ακ'_'

入侵信息记录

### 系统设置

需要过滤的关键词:	' : and ( ) exec insert select delete update count 用" "分开
是否记录入侵者信息:	<input checked="" type="checkbox"/> 是
是否启用锁定IP:	<input checked="" type="checkbox"/> 是
是否启用安全表单:	<input type="checkbox"/> 否 慎用这个功能, 除非你对对表单很了解, 并确定对安全没影响!
您认为安全的表单:	password 123123 用" "分开
出错后的处理方式:	<input checked="" type="radio"/> 直接关闭网页
出错后跳转Url:	http://www.jxdpc.gov.cn 注意, 这里的都是半角符号, 就是英文的!
警告提示信息:	对你的注入行为警告! \n\n
阻止访问提示信息:	防注入系统提示你↓你的Ip已经被本系统自动锁定! \n\n如想访问本站请和管理员联系!
提交	

Sql通用防注入系统 v3.1β版 2005-12

在防注入系统后台系统设置中推荐采用“直接关闭网页”。锁定IP可以封扫描IP, 但不推荐使用, 以防误操作一个局域网段的internet出口地址全部被封。这个自己在使用中可以慢慢体会。

5)使用从网上摘抄的源代码后台需要对其进行改动, 尤其是上传文件名, 比如upfile.asp改为jxic-upfile.asp。

## 第六节 设置安全的虚拟主机访问权限

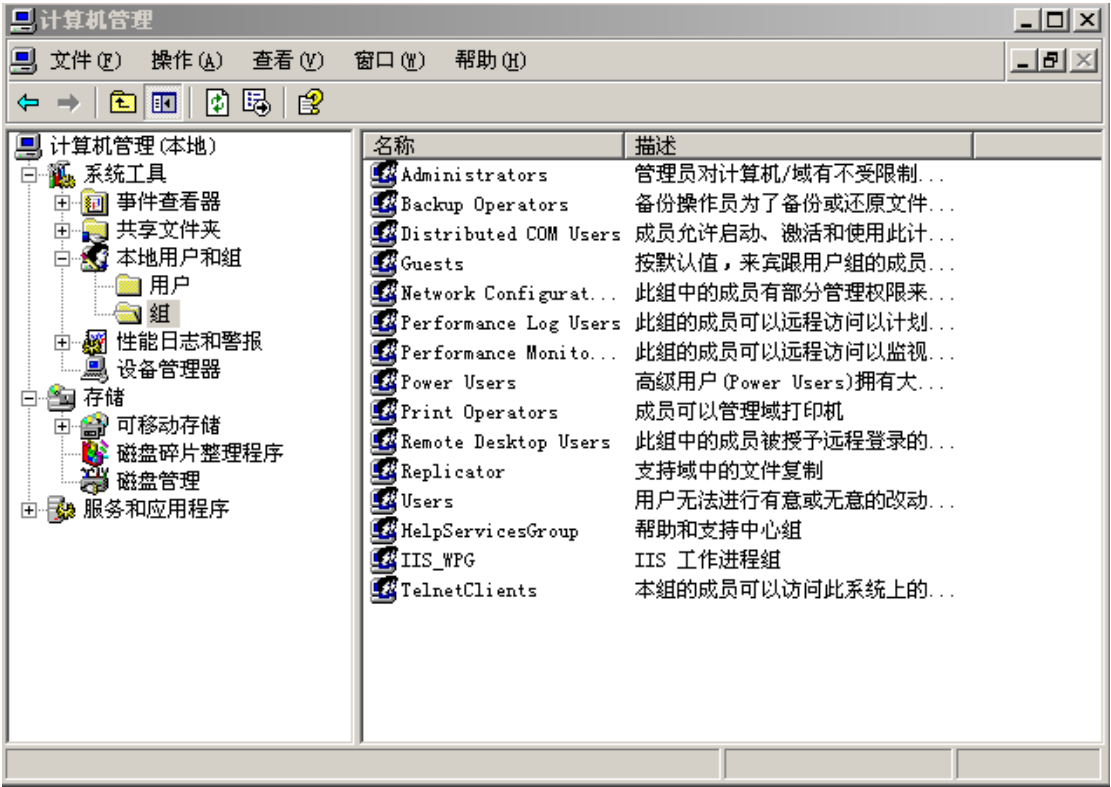
由于公网IP数量紧张, 多个站点在一台服务器已经很普遍, 对于拥有虚拟站点的主机, 我们要设置好用户的访问权, 同时对于有子网站的用户, 单列出一个主机头, 使用自己的虚拟目录, 这样在子网站存在漏洞被黑客入侵时也很难跨站入侵。

□□ 新建web网站访问用户组和用户。

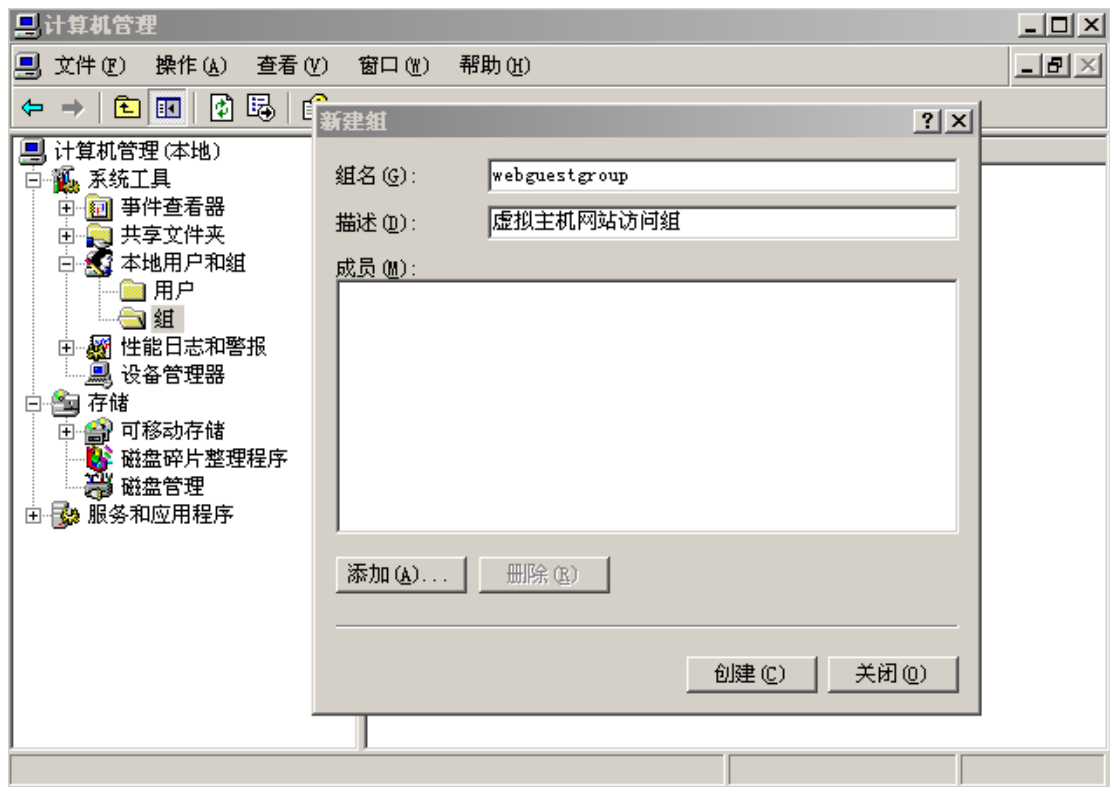
原理涉及到用户权限和组的权限, 我们的目的是新建一个组, 这个组的权限是由用户的权限来决定。只给予用户必要的权限即可。同时也为了避免网站访

问出现500内部错误问题, 这个是由于IUSER帐号(默认的web访问用户)的三个系统文件内部时间不协调引起的。

1□ 首先右键点击“我的电脑”图标-“管理”-“本地用户和组”。

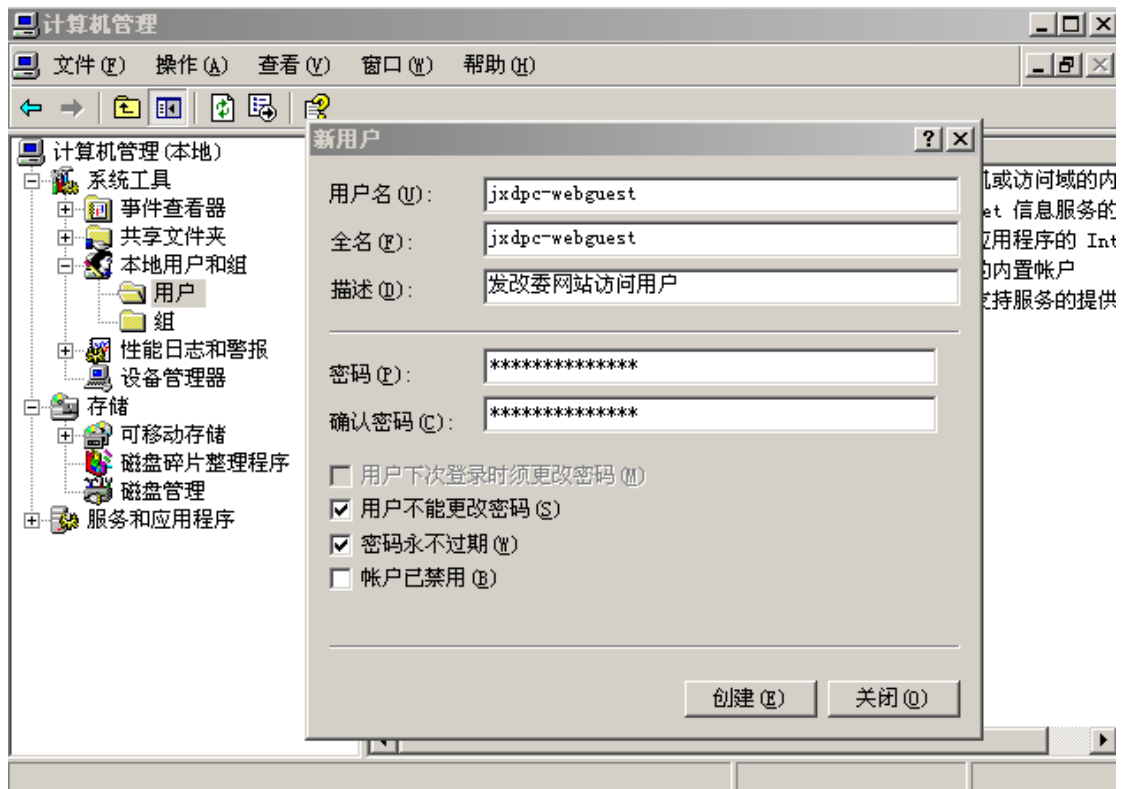


2□ 左边栏目中选择“组”, 点击右键, 选择“新建组”, 新建一个组名, 加上描述。



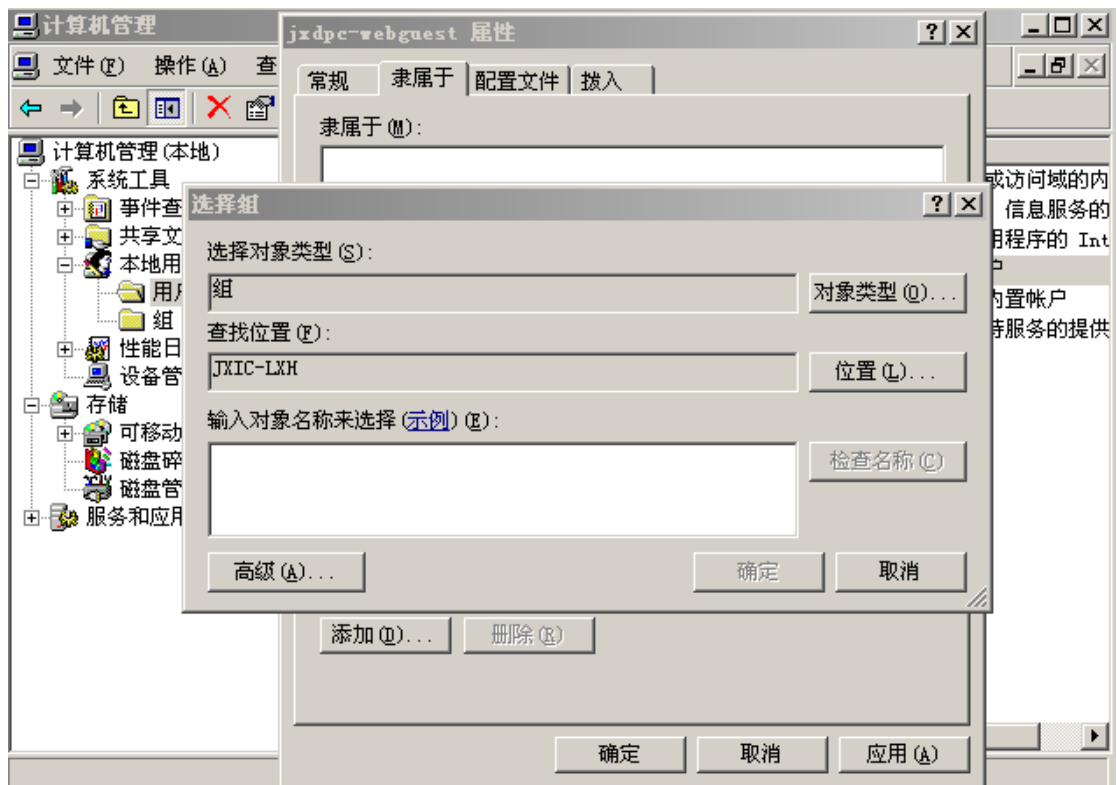
- 3□ 左边栏目中选择“用户”，点击右键，选择“新建用户”，新建一个用户名，加上描述，设置密码(后面IIS设置中需要此密码)，将用户下次登陆时需更改密码前的勾去除，同时勾选用户不能更改密码和密码永不过期。





4□ 在右边栏目中选中刚创建的用户“jxdpc-webguest”，右键选择“属性”-

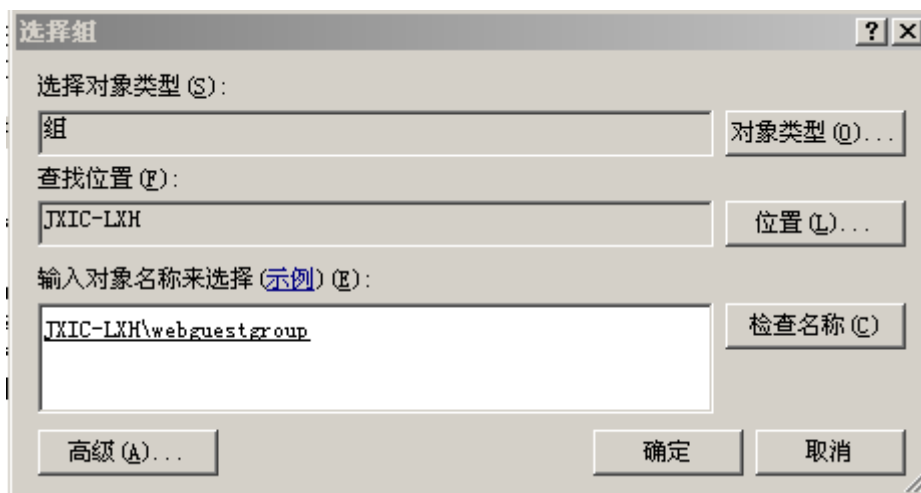
“隶属于”，选择 “Users”组后点击“删除”，在点击“添加”。



5□ 点击“高级”，再点击“立即查找”。

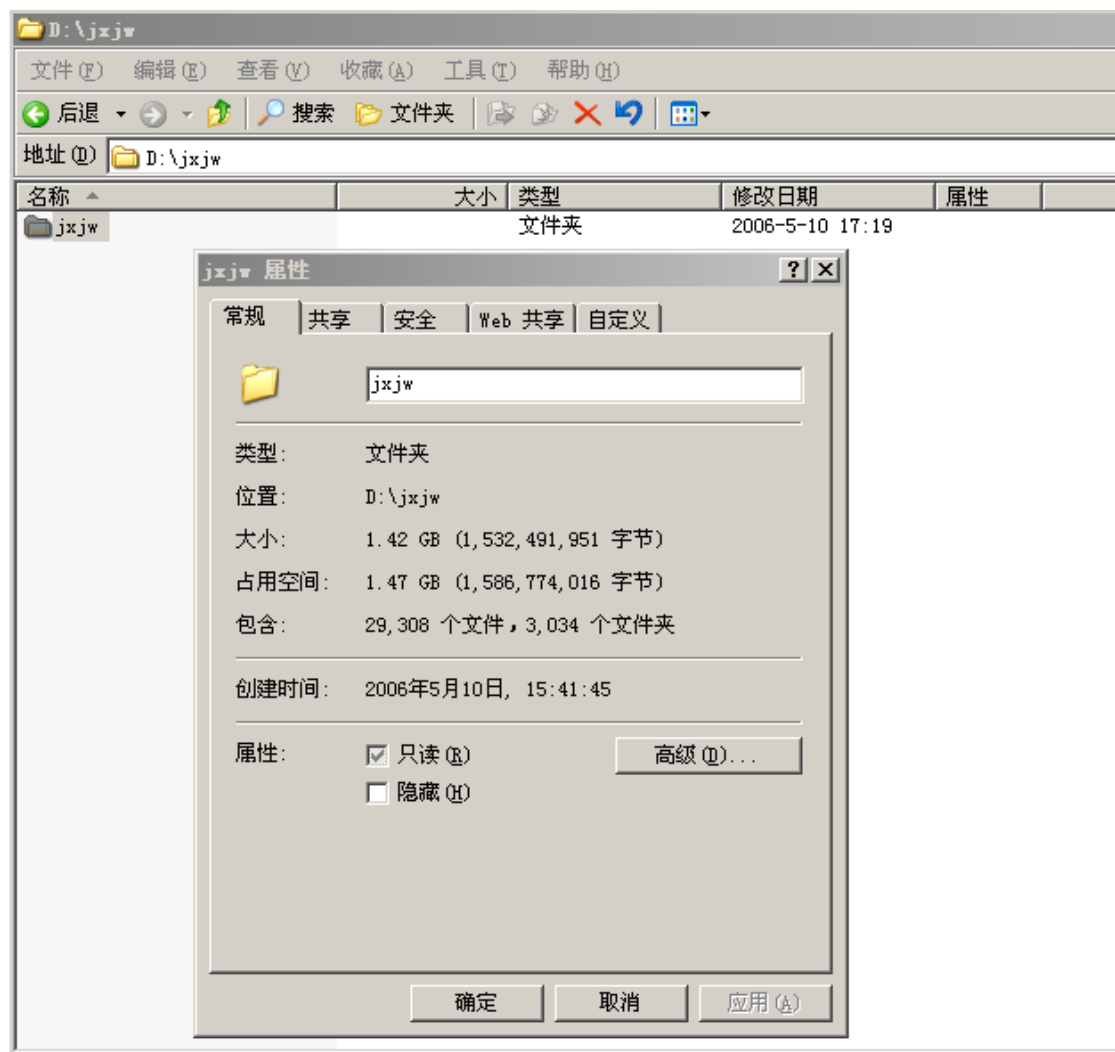


6、双击新建的组“webguestgroup”，添加到下图所示方框后-点击确定完成。



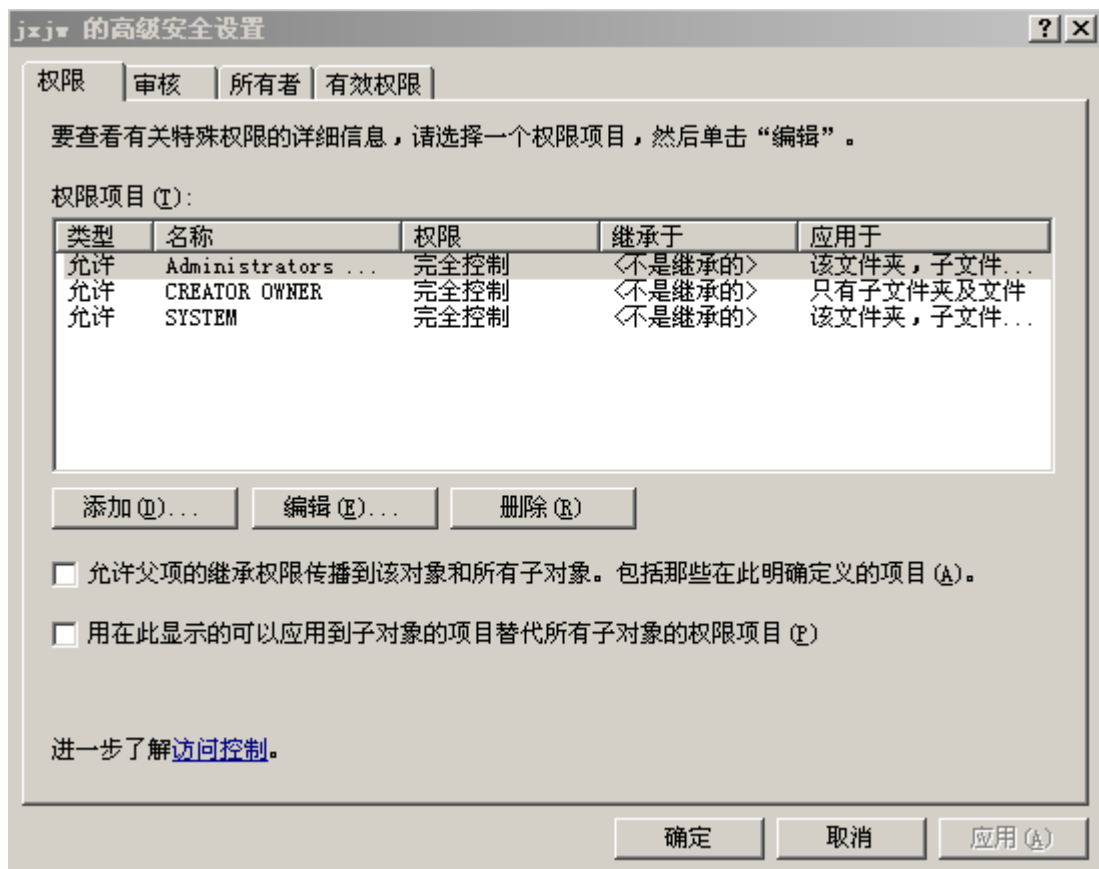
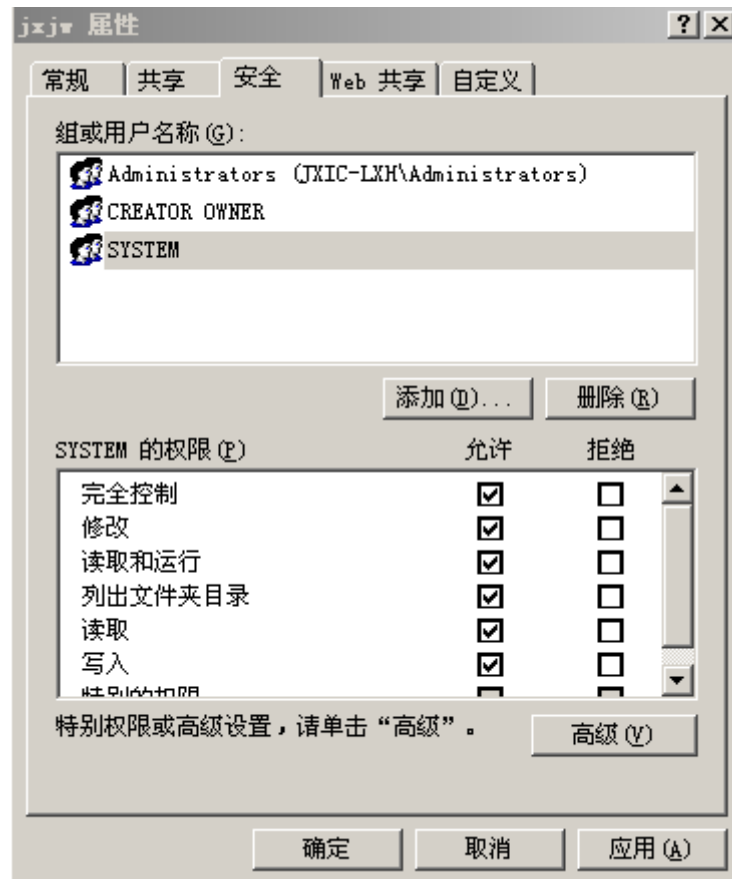
二、设置目录的权限，我们把web网站放在D盘jxjw文件夹(基于安全考虑)。

1、进入网站所在目录，点右键选择“属性”。



## 2、选择“安全”，将除Administrators, CREATOR

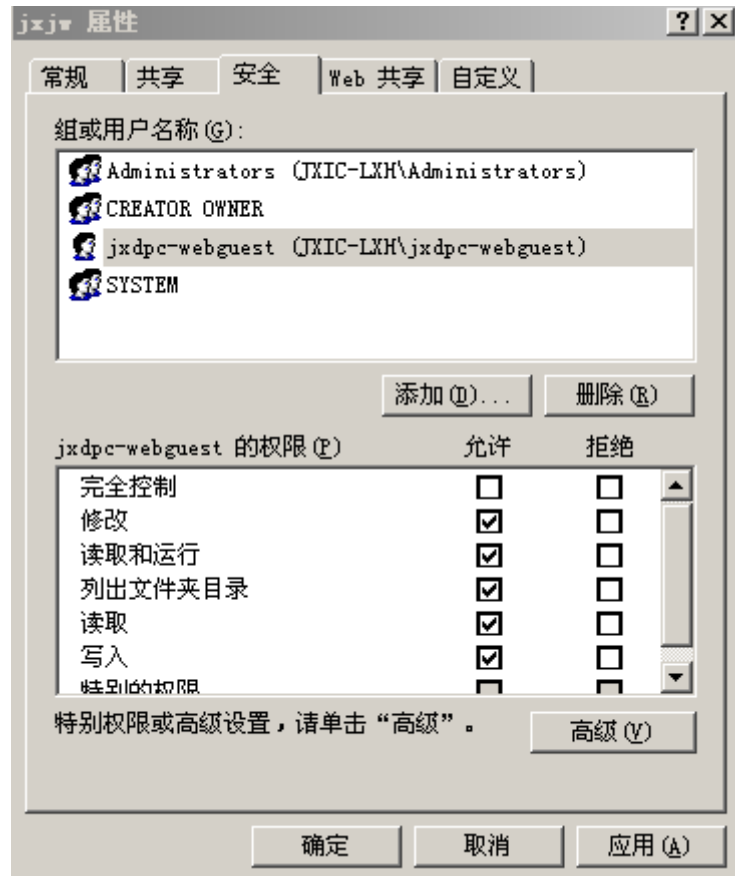
OWNER, SYSTEMS的用户组删除。有些组提示不能删除，是因为继承权限的原因，可以点击上图中的“高级”，将“允许父项的继承项传播到该对象和所有子对象”勾去除-选择“应用”。



3、添加新建的用户“jxdpc-webguest”。

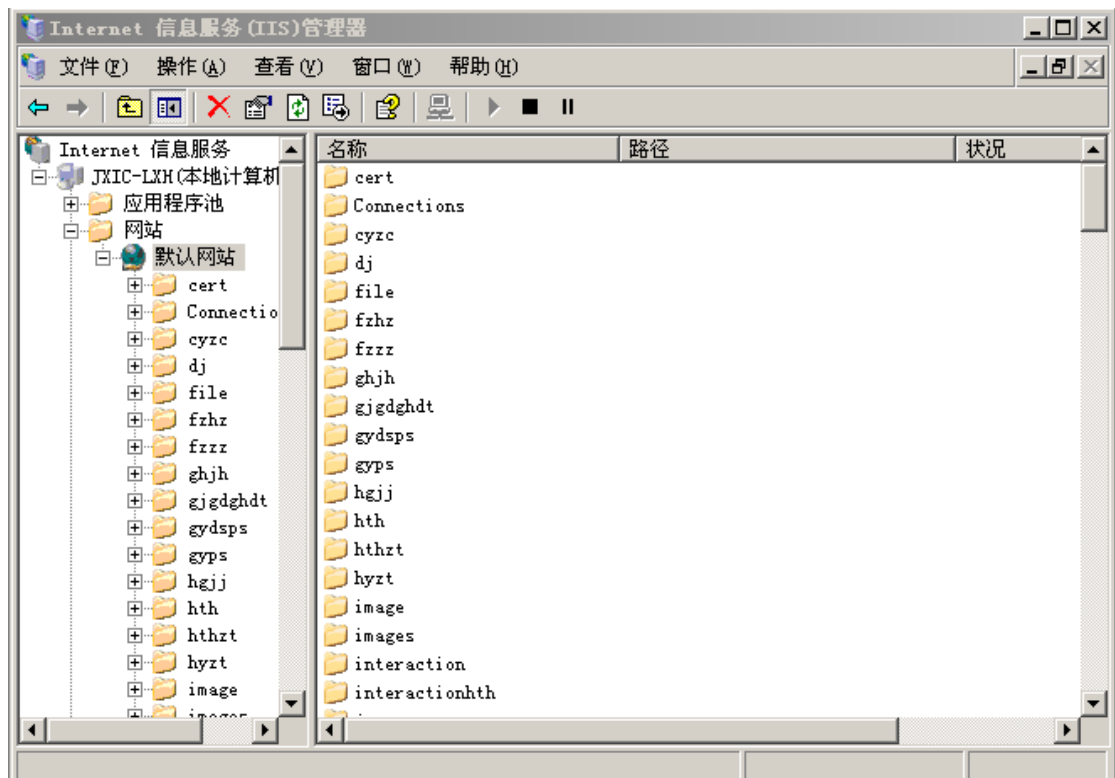


4、给予“用户修改、读取和运行、列出文件夹目录、读取、写入”这些权限，  
 去除“完全控制”权限。

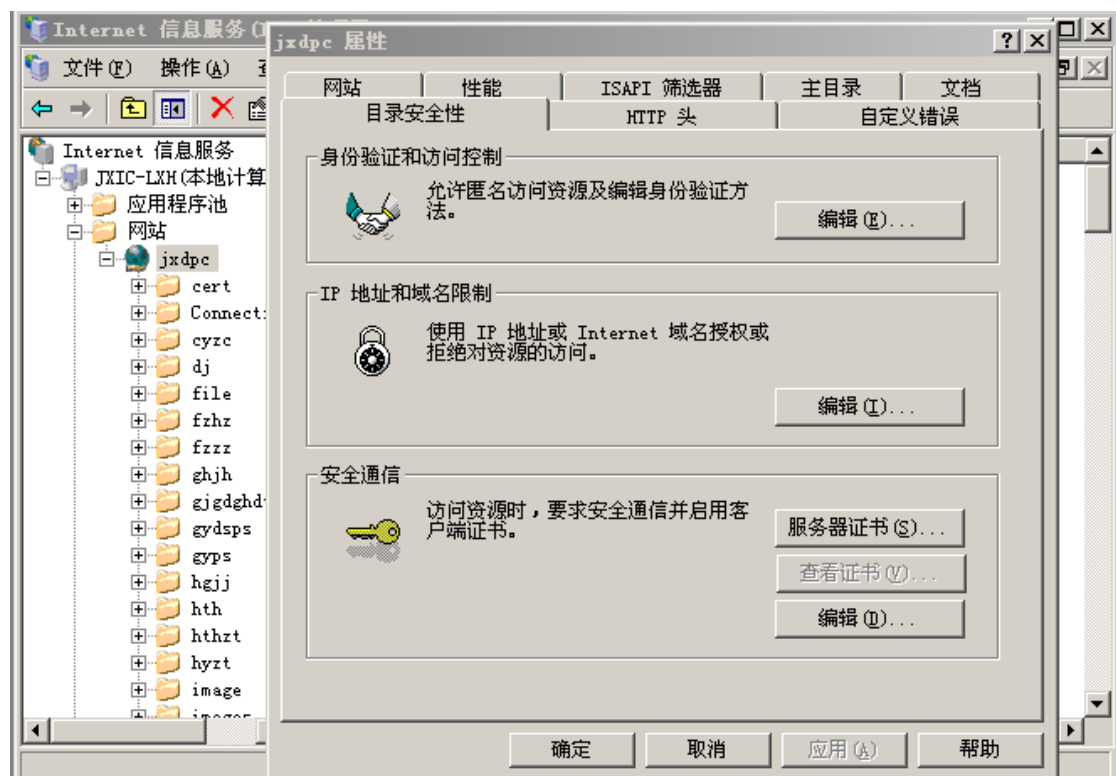


### 三、IIS设置。

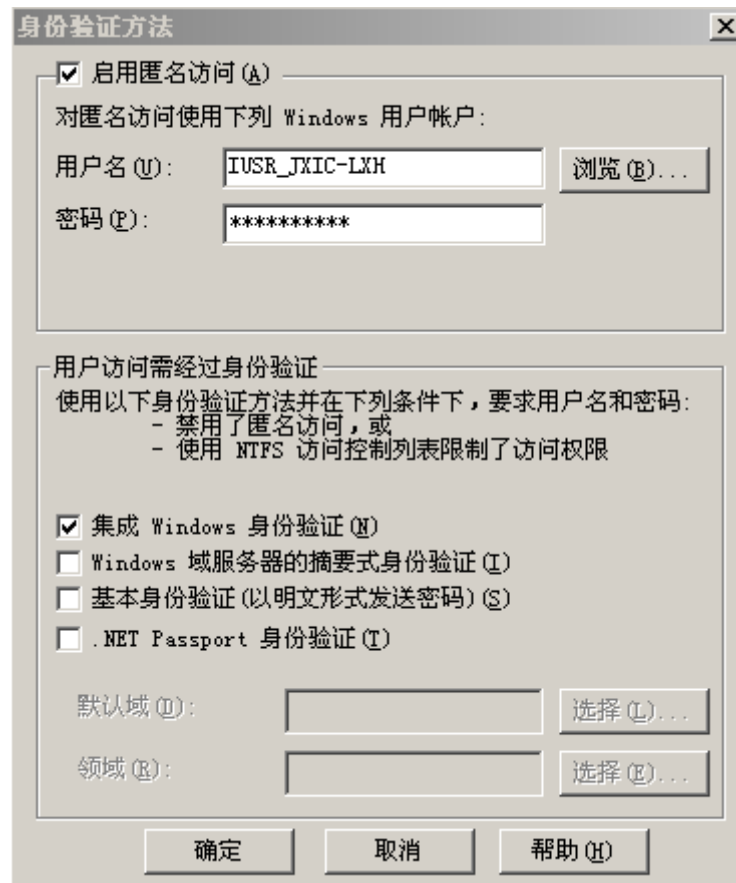
- 1、依次打开“开始”-“设置”-“控制面板”-“管理工具-Internet 信息服务 (IIS) 管理器”。



2、左边栏目中选择网站，点右键选择“属性”-“目录安全性”。



3、身份验证和访问机制中选择“编辑”。



4、选择“浏览”-“选择用户”-“高级”-“立即查找”-选择“jxdpc-webguest”用户。



**选择用户** [?] [X]

选择此对象类型 (S):  
 对象类型 (O)...

查找位置 (L):  
 位置 (L)...

**一般性查询**

名称 (A):

描述 (D):

☐ 禁用的帐户 (B)

☐ 不过期密码 (X)

自上次登录后的天数 (T):

列 (C)...


立即查找 (F)

停止 (T)



搜索结果 (U):

确定 取消

名称 (RDN)	在文件夹中
 Guest	JXIC-LXH
 IUSR_JXIC-LXH	JXIC-LXH
 IWAM_JXIC-LXH	JXIC-LXH
 jxdpc-webguest	JXIC-LXH
 jxic-yeskyli	JXIC-LXH
 SUPPORT_388945a0	JXIC-LXH

5、输入网站访问用户密码，需要输入两次，选择“确定”。

身份验证方法

☒ 启用匿名访问 (A)

对匿名访问使用下列 Windows 用户帐户:

用户名 (U): JXIC-LXH\jxdpc-webguest 浏览 (B)...

密码 (P): \*\*\*\*\*

用户访问需经过身份验证

使用以下身份验证方法并在下列条件下, 要求用户名和密码:

- 禁用了匿名访问, 或
- 使用 NTFS 访问控制列表限制了访问权限

☒ 集成 Windows 身份验证 (W)

☐ Windows 域服务器的摘要式身份验证 (I)

☐ 基本身份验证 (以明文形式发送密码) (S)

☐ .NET Passport 身份验证 (T)

默认域 (D): 选择 (L)...

领域 (R): 选择 (R)...

确定 取消 帮助 (H)

身份验证方法

☒ 启用匿名访问 (A)

对匿名访问使用下列 Windows 用户帐户:

用户名 (U): JXIC-LXH\jxdpc-webguest 浏览 (B)...

密码 (P): \*\*\*\*\*

确认密码

重新输入密码进行确认:

\*\*\*\*\*

确定 取消

☐ 基本身份验证 (以明文形式发送密码) (S)

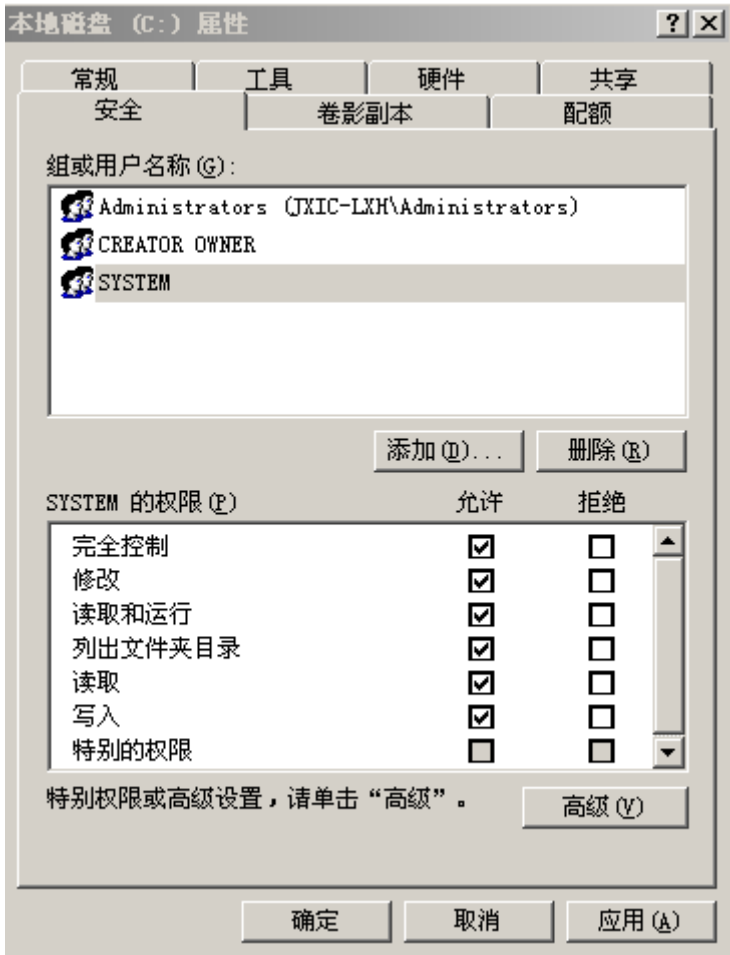
☐ .NET Passport 身份验证 (T)

默认域 (D): 选择 (L)...

领域 (R): 选择 (R)...

确定 取消 帮助 (H)

四、修改所有盘符的权限，将除Administrators, SYSTEM的用户组删除，尤其是删除Users组、Everyone组。删除了EVERYONE用户组，含义是使普通用户不能越权，而且ASP还可以正常使用。



总结:就这样非常轻松的解决用户设置权限的问题。以上我们又做了非常健全的越权限制，有效防止了跨站攻击，就算黑客得到了此用户，也只是网站访问来宾用户，丝毫危机不到服务器其它网站，IIS虚拟站点的安全问题，相信足以排除提升权限的忧患了。

疑问一、有些人认为只需要建立新用户，将新用户放在guest组下即可，我自己认为建立一个单独的组很有必要，这个组的权限是由用户的权限的集合，guest组仍然具有一定的权限。

疑问二、完全控权限与下面所有的权限勾上是否相等, 完全控制权限包括下面所有权限, 我们只需要给予必要的权限, 因此网站访问来宾用户不需要勾上完全控制权限。

大家有疑问可以去网络上查询权限的相关资料, 这个是大家学习Windows系统中一个重要的课程内容。

2015年10月8日