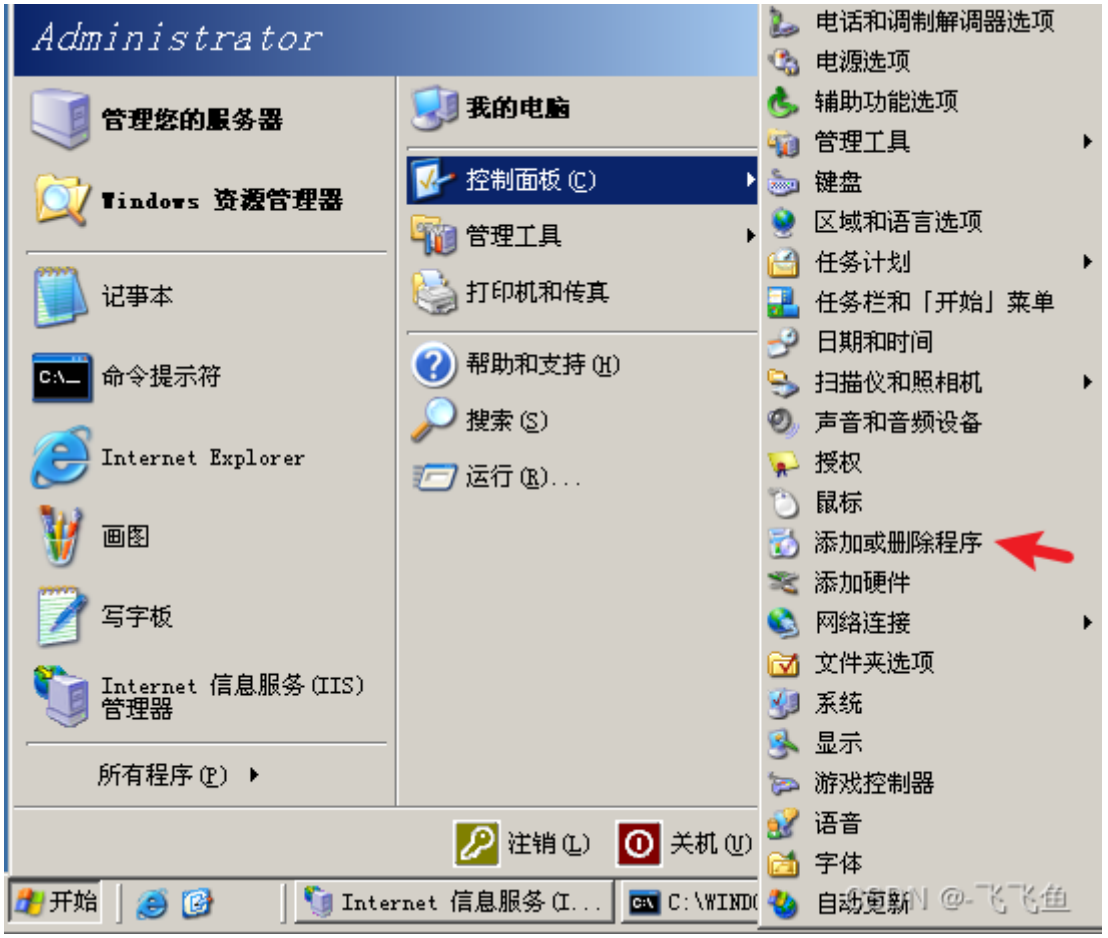
IIS6.0写权限漏洞复现获取WebShell

1.服务安装

IIS服务器属于Windows server平台，本次复现漏洞环境使用Windows server 2003 sp2系统，镜像文件在python配套教学工具中，里面包含了安装密钥文件。安装系统步骤略过，使用默认安装即可。

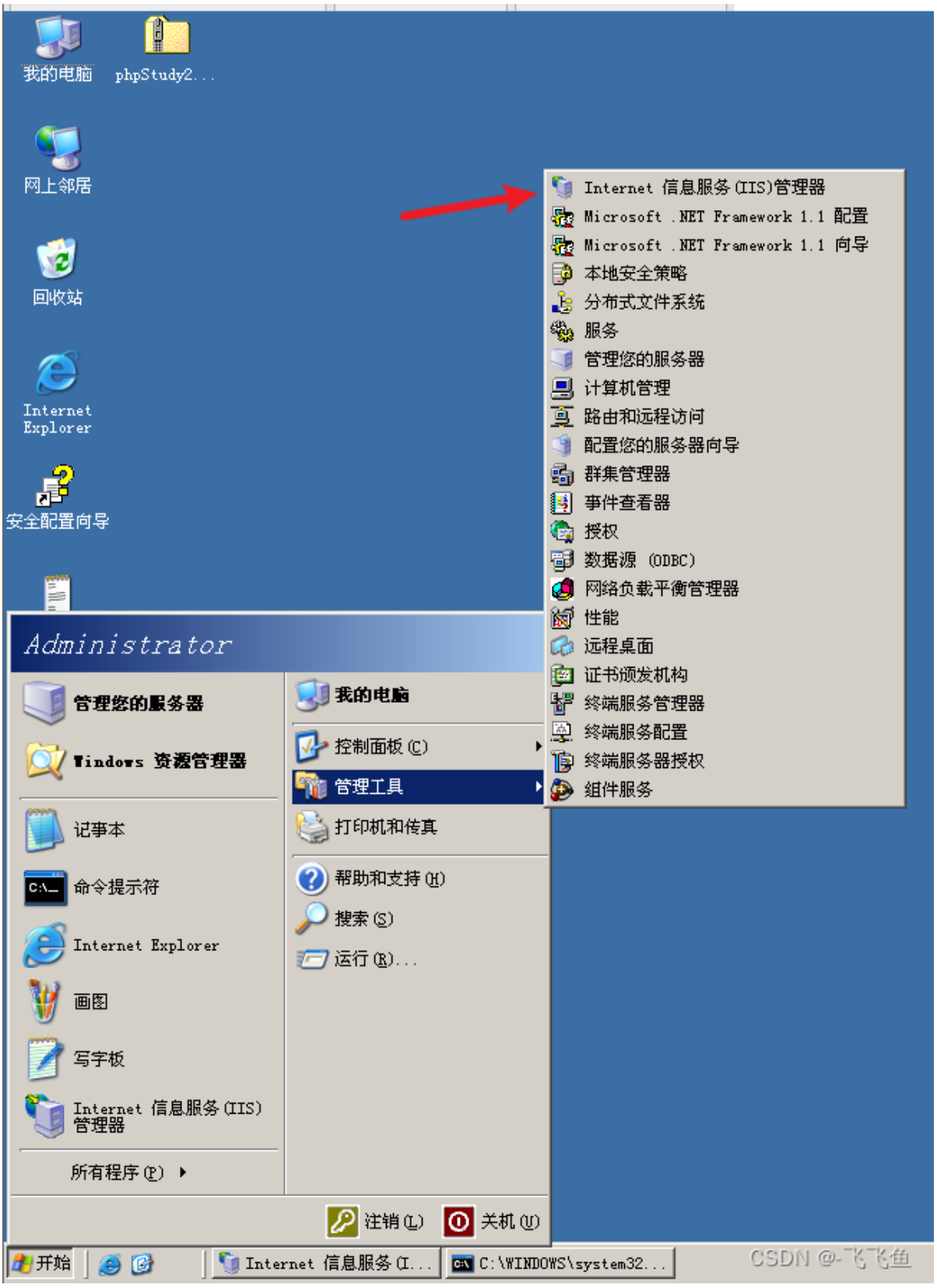
系统启动后，在系统启动菜单中运行IIS，如果没有该选项，说明IIS没有进行默认安装，可以通过`控制面板-->添加或删除程序`手动进行安装。



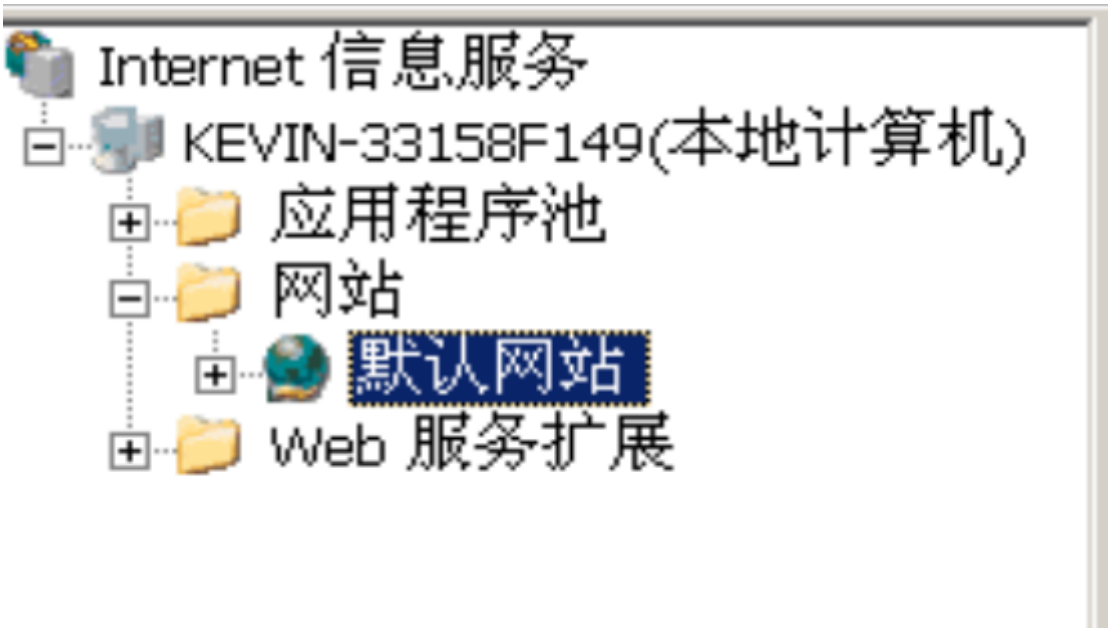
依次选择`添加/删除组件-->应用程序服务器`

2.属性配置

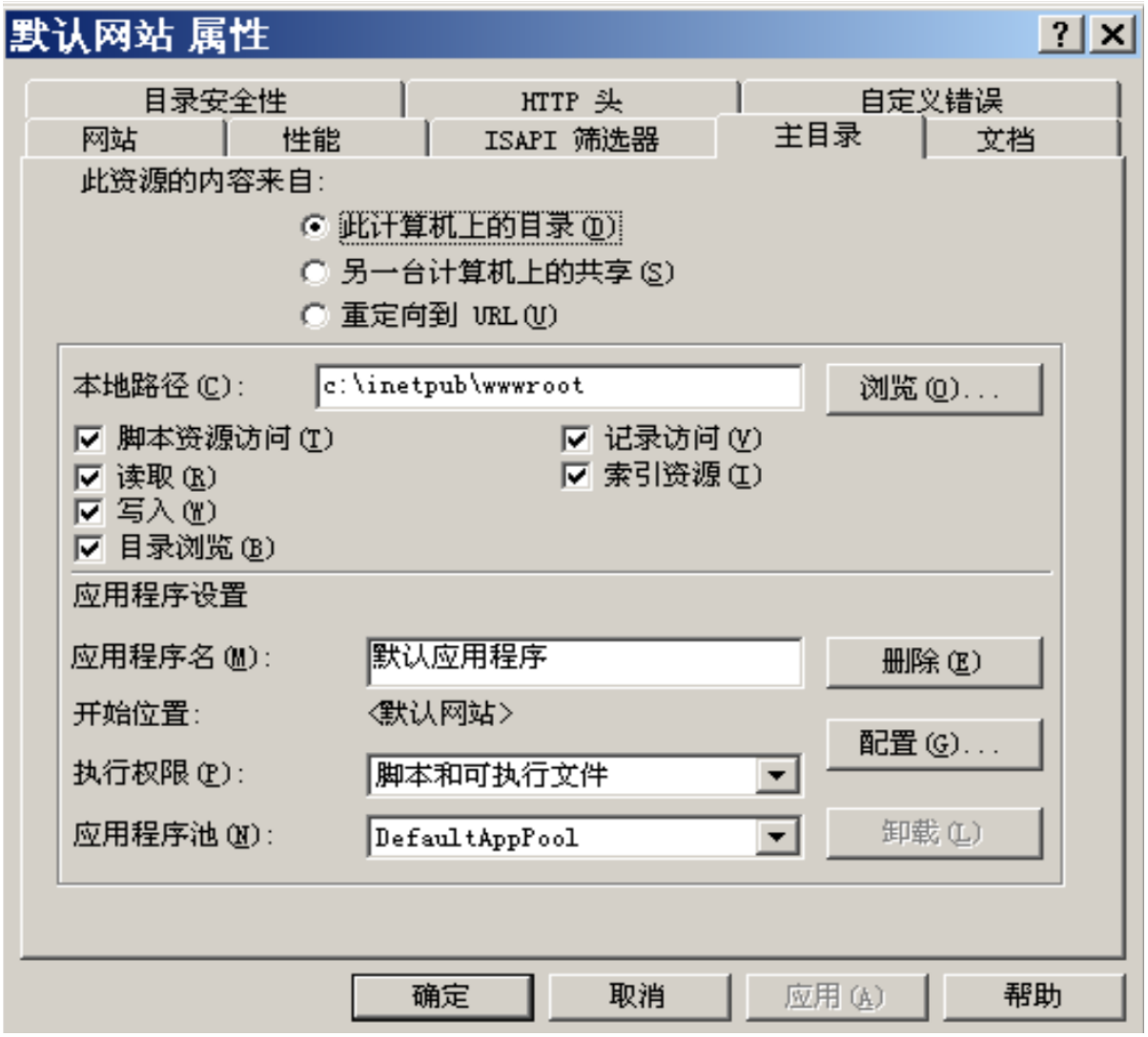
环境搭好后，需要进行一些默认配置，在管理工具中，找到internet信息服务管理器



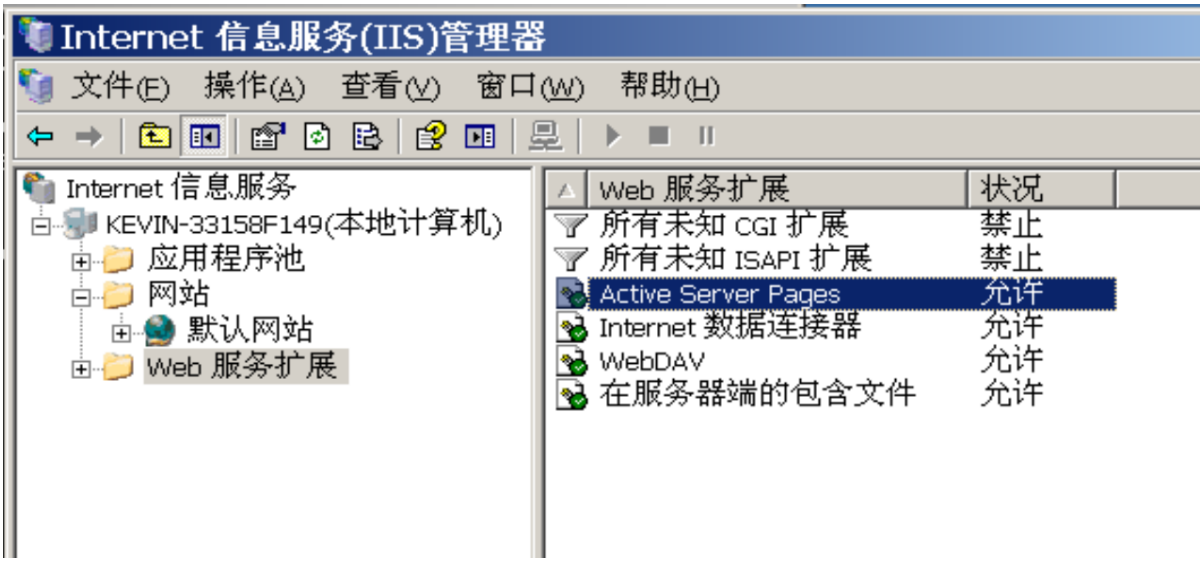
进入后找到默认网站，右键点击选择属性



在弹出的窗口`打开主目录`，并勾选所有复选框。WebDAV作用是上传下载文件，所以权限要给足够。

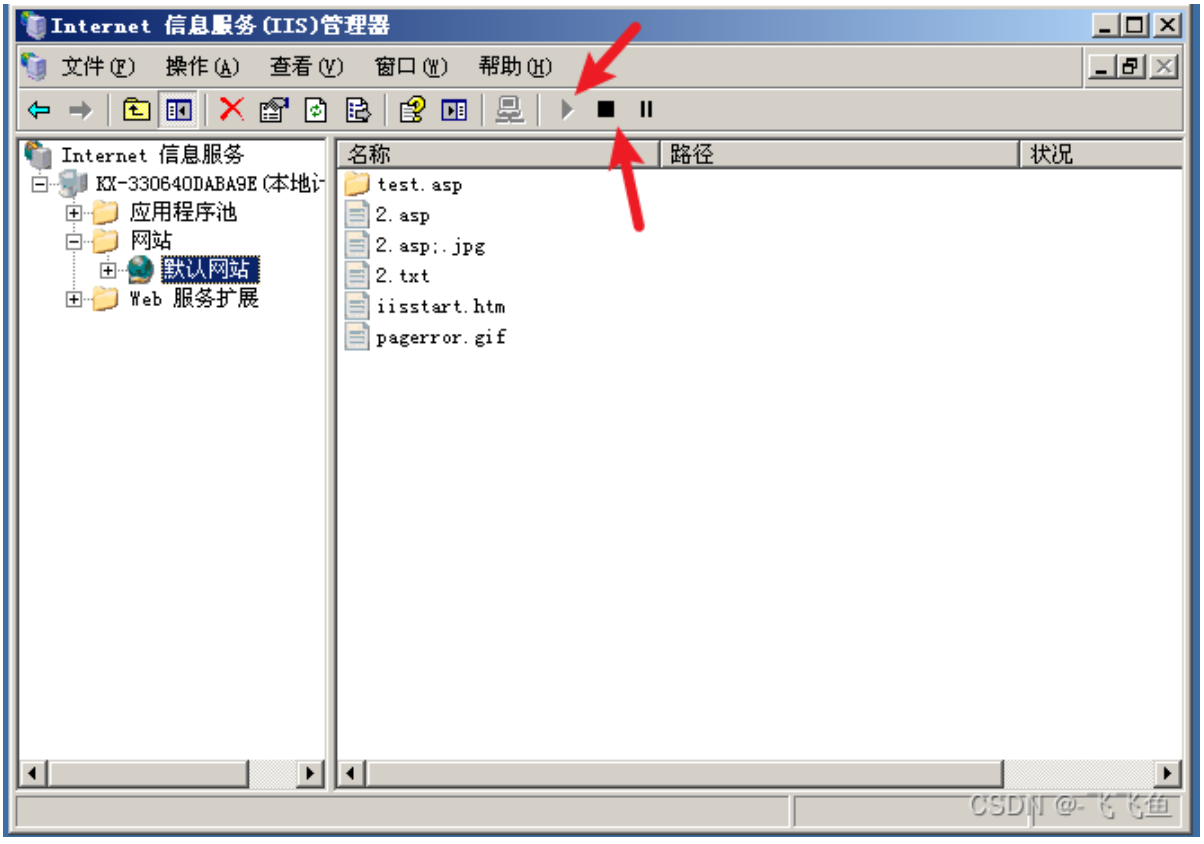


在`web服务扩展`中，将`Active Server Pages`和`WebDAV`两个选项设置为允许。



其中，`Active ServerPages`为ASP的全称，对于一般的ASP服务来说，该选项是必须要启用的，否则网站仅支持HTML，JPG等静态资源。而`WebDAV`是漏洞成因之一，必须手动开启。

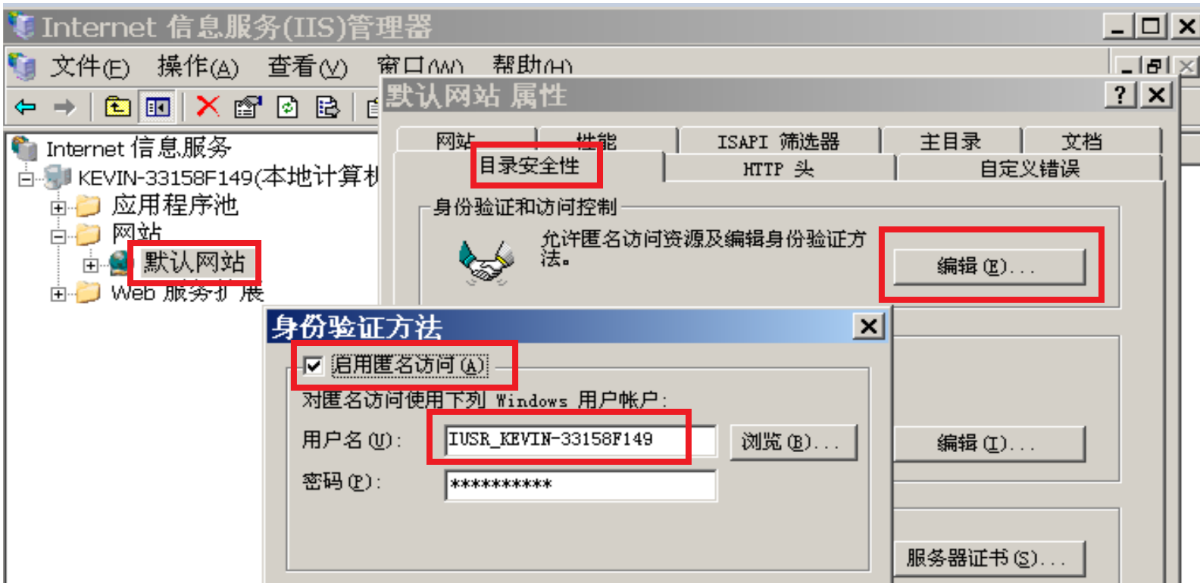
修改完配置后，需要重启IIS服务，选择默认网站，点击上方停止按钮，再点击启动按钮。



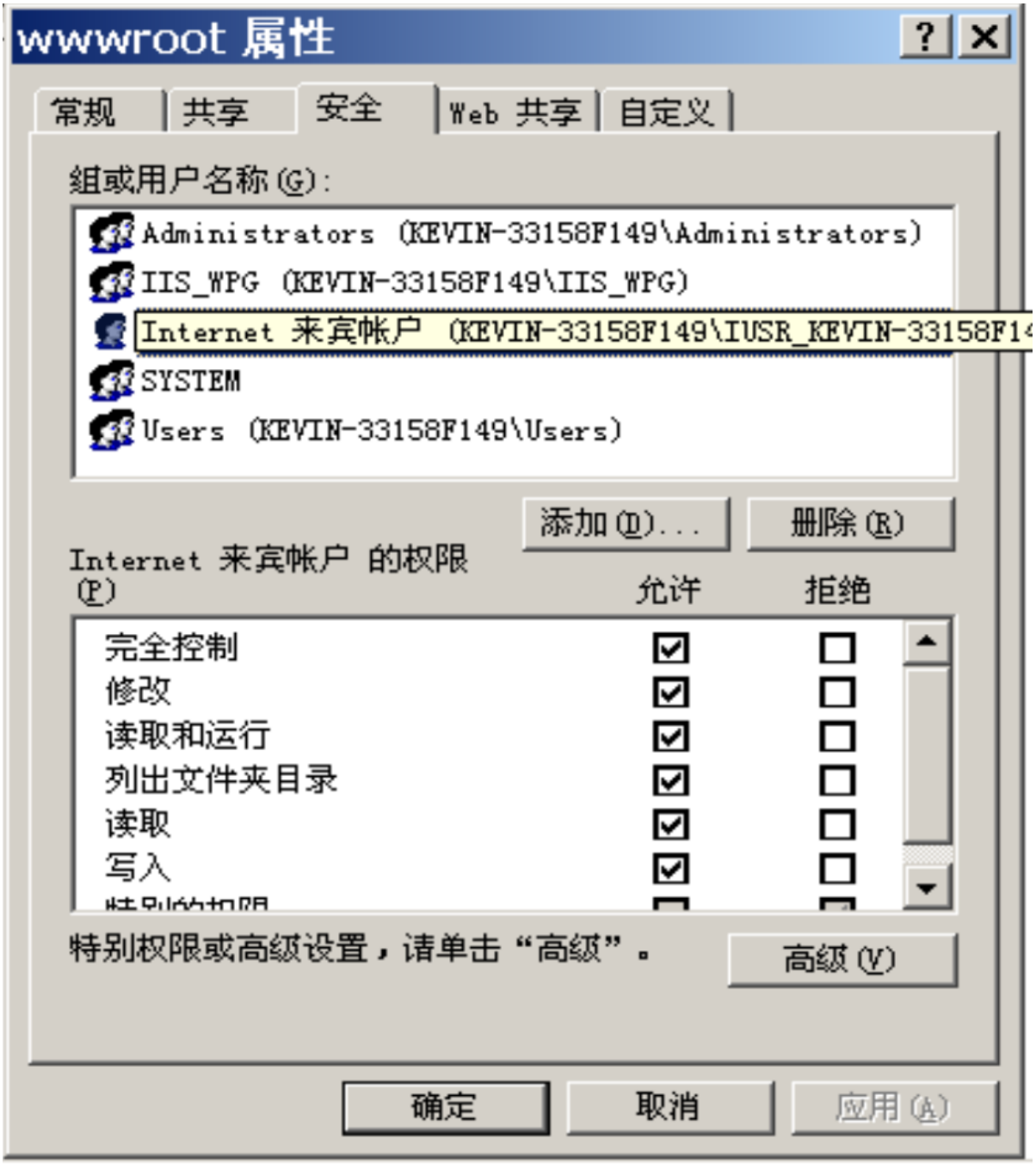
3.网站目录权限配置

上面配置完网站主目录的读取和写入后，还需要配置网站目录匿名用户的访问权限。

右键点击`默认网站`，选择`属性`。在`默认网站属性`中，选择`目录安全性`标签，在`身份验证和访问控制`中选择`编辑`。在`身份验证方法`对话框中，将`启用匿名访问`打勾，并记录用户名。



打开网站主目录，默认都在`c:\inetpub\wwwroot`，选择`wwwroot`目录，右键点击`属性`，在`安全`标签页找到刚刚记录的匿名用户名，在下方权限中，将允许列的复选框都打勾。然后`应用-->确定`。



到此，基础环境和漏洞复现都配置完毕。

Apache的安装与运行

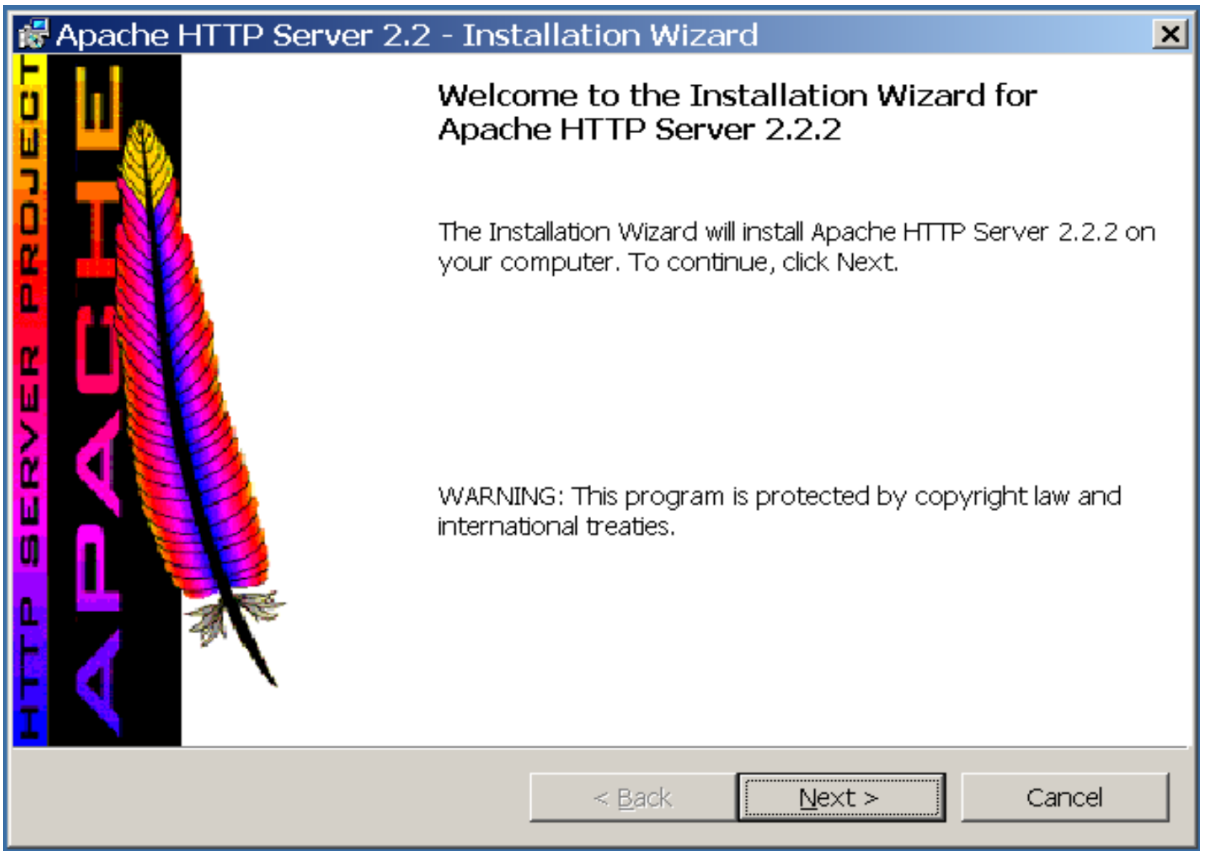
1.下载Apache 2.4

https://archive.apache.org/dist/httpd/binaries/win32/apache_2.2.2-win32-x86-no_ssl.msi

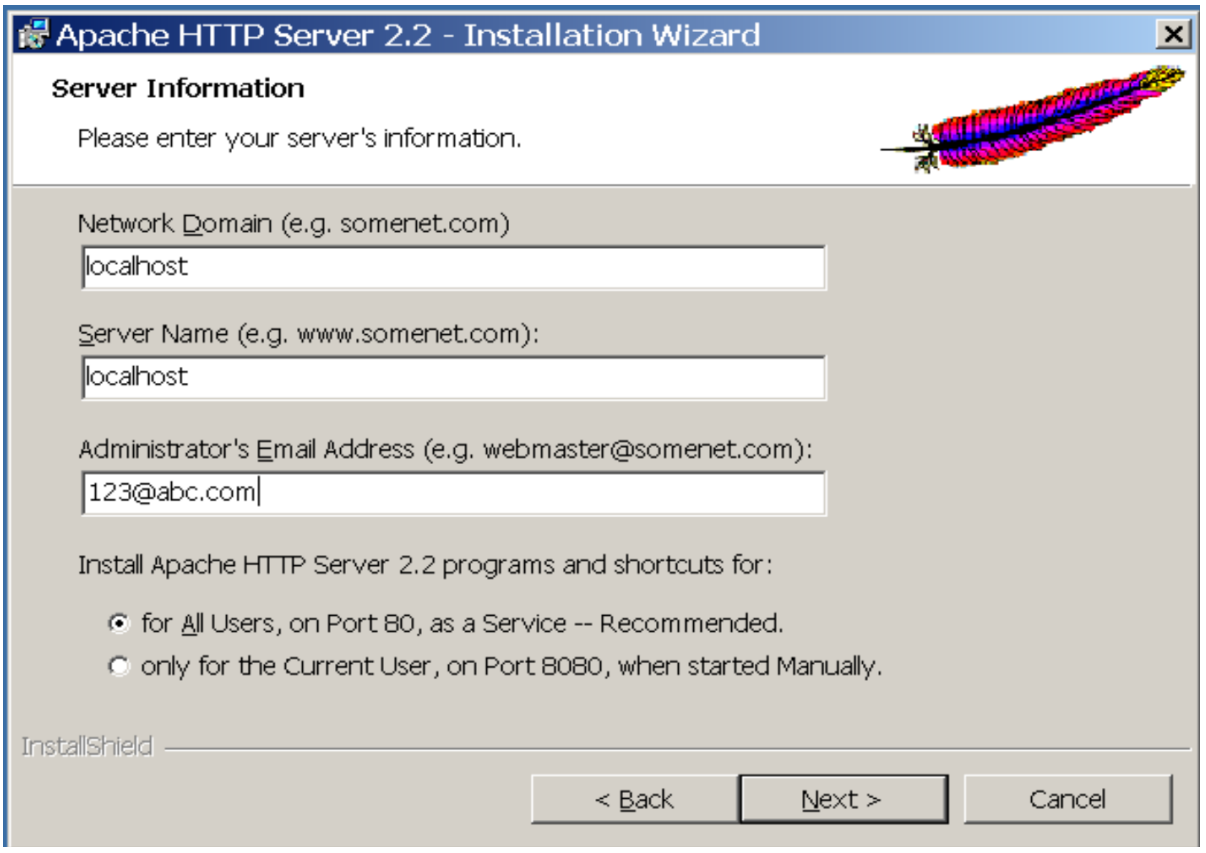
2.安装Apache

注意：如果与IIS安装在同一台服务器，需要关闭IIS，再进行安装Apache，否则会端口冲突！

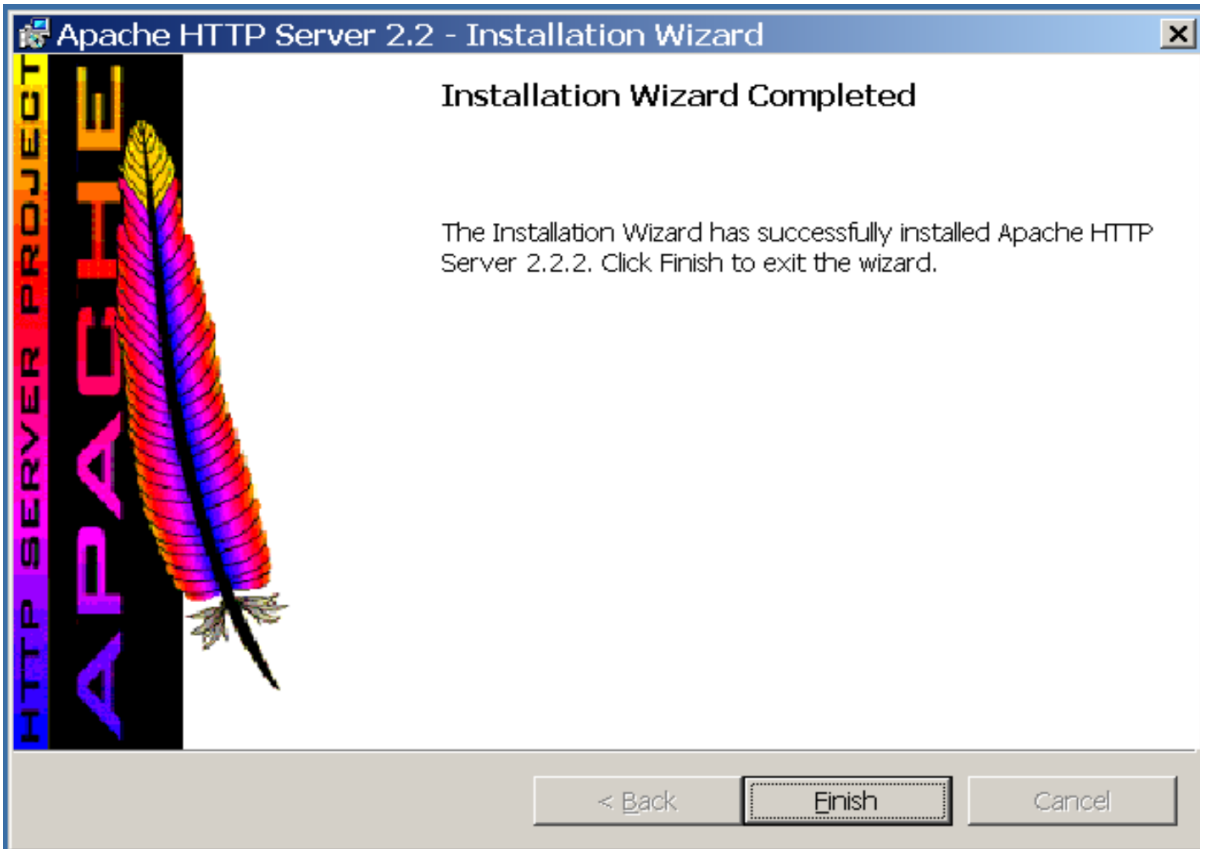
1.双击打开.msi文件



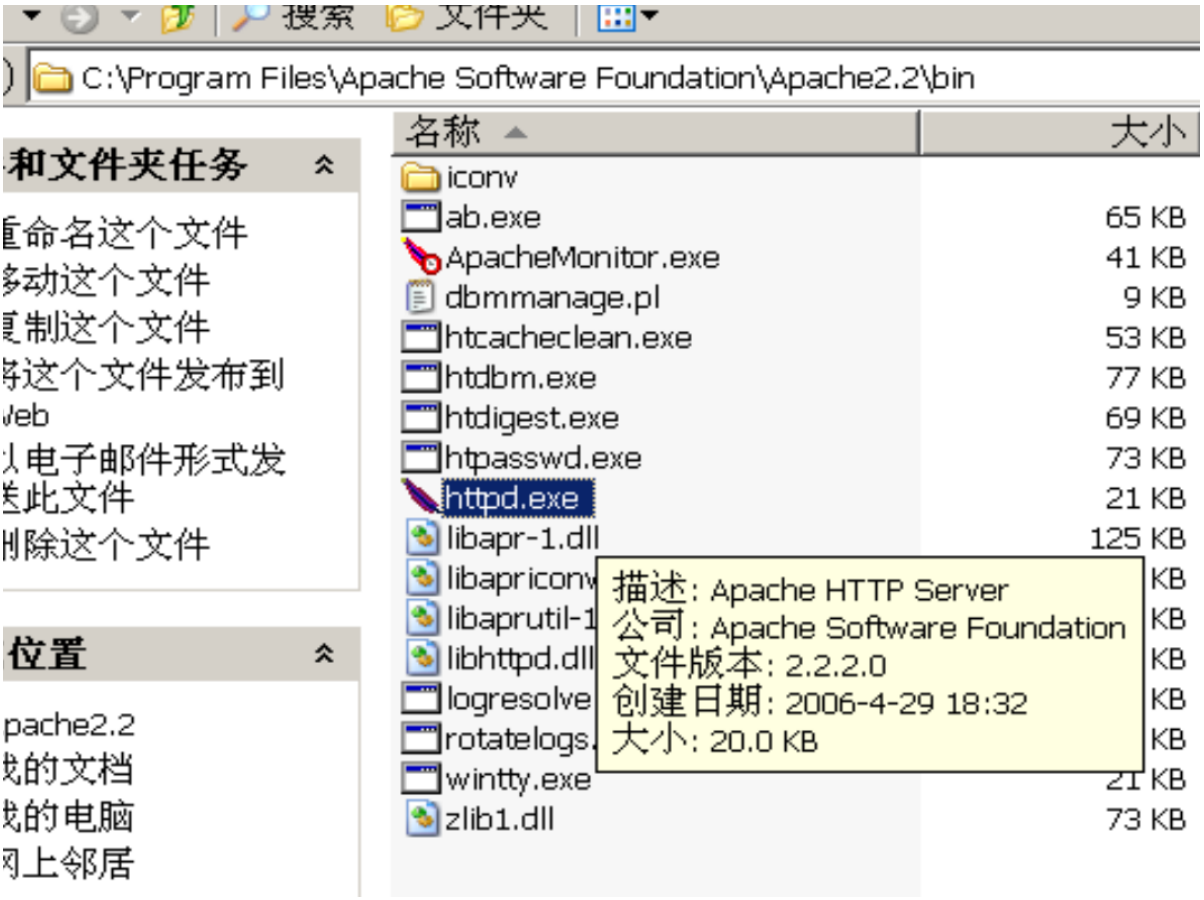
2.默认都是下一步，直到server infomation这一步，填写如下信息：



3.之后继续默认下一步，直到完成安装



4.进入安装目录，双击运行httpd服务


搜索
文件夹
C:\Program Files\Apache Software Foundation\Apache2.2\bin
和文件夹任务
重命名这个文件
移动这个文件
复制这个文件
将这个文件发布到
Web
以电子邮件形式发送此文件
删除这个文件
位置
pache2.2
我的文档
我的电脑
网上邻居
名称
大小
iconv
ab.exe 65 KB
ApacheMonitor.exe 41 KB
dbmmanage.pl 9 KB
htcacheclean.exe 53 KB
htdbm.exe 77 KB
htdigest.exe 69 KB
htpasswd.exe 73 KB
httpd.exe 21 KB
libapr-1.dll 125 KB
libapriconv KB
libaprutil-1 KB
libhttpd.dll KB
logresolve KB
rotatelogs KB
wintty.exe 21 KB
zlib1.dll 73 KB
描述: Apache HTTP Server
公司: Apache Software Foundation
文件版本: 2.2.2.0
创建日期: 2006-4-29 18:32
大小: 20.0 KB