iis权限设置:IIS安全权限设置

疯狂代码 http://CrazyCoder.cn/ ĵ:http:/CrazyCoder.cn/WebSecurity/Article74444.html

系统用户情况为:

administrators 超级管理员(组)

system 系统用户(内置安全主体)

guests 来宾帐号(组)

iusr_服务器名 匿名访问web用户

iwam_服务器名 启动iis进程用户

www_cnnsc_org 自己添加用户、添加后删除Users(组)、删除后添加到guests来宾帐号(组)

为加强系统安全、(guest)用户及(iusr_服务器名)用户均被禁用

将访问web目录全部账户设为guests组、去除其他组

■盘符 安全访问权限

▵C:\盘 administrators(组) 完全控制权限、system(内置安全主体) 完全控制权限

▵D:\盘 (如果用户网站WebSite内容放置在这个分区中)、administrators(组) 完全控制权限

▵E:\盘 administrators(组) 完全控制权限、system(内置安全主体) 完全控制权限

▵f:\盘 administrators(组) 完全控制权限、system(内置安全主体) 完全控制权限

▵如有其他盘符类推下去.

■目录安全访问权限

▲c:\windows\

▵administrators(组) 完全控制权限、system(内置安全主体) 完全控制权限

▲c:\windows\system32\

▵administrators(组) 完全控制权限、system(内置安全主体) 完全控制权限、iwam_服务器名(用户) 读取+运行权限

▲c:\windows\temp\

▵administrators(组) 完全控制权限、system(内置安全主体) 完全控制权限、guests(组) 完全控制权限

▲C:\WINDOWS\system32\config\

▵administrators(组) 完全控制权限、system(内置安全主体) 完全控制权限

▲c:\Program Files\

▵administrators(组) 完全控制权限、system(内置安全主体) 完全控制权限

▲C:\Program Files\Common Files\

▵administrators(组) 完全控制权限、system(内置安全主体) 完全控制权限、guests(组) 读取+运行权限

▲c:\Documents and Settings\

▵administrators(组) 完全控制权限、system(内置安全主体) 完全控制权限

▲C:\Documents and Settings\All Users\

▵administrators(组) 完全控制权限、system(内置安全主体) 完全控制权限

▲C:\Documents and Settings\All Users\Application Data\

▵administrators(组) 完全控制权限、system(内置安全主体) 完全控制权限
▲C:\Documents and Settings\All Users\Application Data\Microsoft\
▵administrators(组) 完全控制权限、system(内置安全主体) 完全控制权限
▲C:\Documents and Settings\All Users\Application Data\Microsoft\HTML Help\
▵administrators(组) 完全控制权限、system(内置安全主体) 完全控制权限

■禁止系统盘下EXE文件:
net.exe、cmd.exe、tftp.exe、netstat.exe、regedit.exe、regedt32.exe、at.exe、attrib.exe、cacls.exe
▵些文件都设置成 administrators 完全控制权限

■新建WWW(网站WebSite)根目录【administrators(组) 完全控制权限、system(内置安全主体) 完全控制权限】
▲根目录里新建wwwroot目录
▲网站WebSite根目录、网页请上传到这个目录
▵administrators(组) 完全控制权限
▵www_cnnsc_org(用户)完全控制权限
▲根目录里新建logfiles目录
▲网站WebSite访问日志文件、本目录不占用您空间
▵administrators(组) 完全控制权限
▲根目录里新建database目录
▲数据库目录、用来存放ACCESS数据库
▵administrators(组) 完全控制权限
▲根目录里新建others目录
▲用于存放您其它文件、该类文件不会出现在网站WebSite上
▵administrators(组) 完全控制权限
▵www_cnnsc_org(用户)完全控制权限
▲在FTP(登陆消息文件里填)IIS日志介绍说明:
〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓
欢迎您使用本虚拟主机.
请使用CUTEFTP或者LEAFTP等软件Software上传您网页.
注意、如果上传不了、请把FTP软件SoftwarePASV模式关掉再试.
您登陆进去根目录为FTP根目录
\--wwwroot网站WebSite根目录、网页请上传到这个目录.
\--logfiles 网站WebSite访问日志文件、本目录不占用您空间.
\--database 数据库目录、用来存放ACCESS数据库.

\--others 用于存放您其它文件该类文件不会出现在网站WebSite上.
为了保证服务器高速稳定运行、请勿上传江湖游戏、广告交换、
博彩类网站WebSite、大型论坛、软件Software下载等耗费系统资源.
IIS日志介绍说明
\--Date 动作发生时日期
\--Time 动作发生时时间
\--s-sitename 客户所访问Internet服务于以及例子号
\--s-computername 产生日志条目服务器名字
\--s-ip 产生日志条目服务器IP地址
\--cs-method客户端企图执行动作(例如GET思路方法)
\--cs-uri-stem被访问资源、例如Default.asp
\--cs-uri-query 客户所执行查询
\--s-port 客户端连接端口号
\--cs-username通过身份验证访问服务器用户名、不包括匿名用户
\--c-ip 访问服务器客户端IP地址
\--cs(User-Agent) 客户所用浏览器
\--sc-status用HTTP或者FTP术语所描述动作状态
\--sc-win32-status用Microsoft Windows术语所描述动作状态
〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓〓

■禁止下载Access数据库
▵Internet 信息服务(IIS)管理器→网站WebSite→属性→主目录→配置→添加
▵可执行文件:C:\WINDOWS\twain_32.dll
▵扩展名:.mdb
▲如果你还想禁止下载其它东东
▵Internet 信息服务(IIS)管理器→网站WebSite→属性→主目录→配置→添加
▵可执行文件:C:\WINDOWS\twain_32.dll
▵扩展名:.(改成你要禁止文件名)
▲然后删除扩展名:shtml stm shtm cdx idc cer

■防止列出用户组和系统进程:
▵开始→→管理工具→服务
▵找到 Workstation 停止它、禁用它

■卸载最不安全组件:
▵开始→运行→cmd→回车键

▲cmd里输入:
▵regsvr32/u C:\WINDOWS\system32\wshom.ocx
▵del C:\WINDOWS\system32\wshom.ocx
▵regsvr32/u C:\WINDOWS\system32\shell32.dll
▵del C:\WINDOWS\system32\shell32.dll
▵也可以设置为禁止guests用户组访问

■解除FSO上传小于200k限制:
▵在服务里关闭IIS admin service服务
▵打开 C:\WINDOWS\system32\inetsrv\MetaBase.xml
▵找到ASPMaxRequestEntityAllowed
▵将其修改为需要值、默认为204800、即200K、把它修改为51200000(50M)、然后重启IIS admin service服务

■禁用IPC连接
▵开始→运行→regedit
▵找到如下组建(HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa)中(restrictanonymous)子键
▵将其值改为1即

■清空远程可访问注册表路径:
▵开始→运行→gpedit.msc
▵依次展开“计算机配置→Windows 设置→安全设置→本地策略→安全选项”
▵在右侧窗口中找到“网络访问:可远程访问注册表路径”
▵然后在打开窗口中、将可远程访问注册表路径和子路径内容全部设置为空即

■关闭不必要服务
▵开始→→管理工具→服务
▵Telnet、TCP\IP NetBIOS Helper

■解决终端服务许可证过期办法
▵如果你服务器上已经开着终端服务、那就在添加删除里删除终端服务和终端授权服务
▵我电脑--右键属性--远程---远程桌面、打勾、应用
▵重启服务器、OK了、再也不会提示过期了

■取消关机原因提示
▵开始→运行→gpedit.msc
▵打开组策略编辑器、依次展开
▵计算机配置→管理模板→系统
▵双击右侧窗口出现(显示“关闭事件跟踪”)
▵将(未配置)改为(已禁用)即可

2009-9-24 0:36:08
疯狂代码 http://CrazyCoder.cn/