有史以来最好的虚拟主机安全配置 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/460/2021_2022__E6_9C_89_E5_8F_B2_E4_BB_A5_E6_c100_460846.htm 注入漏洞、上传漏洞、弱口令漏洞等问题随处可见。跨站攻击，远程控制等等是再老套不过了的话题。有些虚拟主机管理员不知是为了方便还是不熟悉配置，干脆就将所有的网站都放在同一个目录中，然后将上级目录设置为站点根目录。有些呢，则将所有的站点的目录都设置为可执行、可写入、可修改。有些则为了方便，在服务器上挂起了QQ，也装上了BT.更有甚者，竟然把Internet来宾帐号加入到Administrators组中！汗……！普通的用户将自己的密码设置为生日之类的6位纯数字，这种情况还可以原谅，毕竟他们大部分都不是专门搞网络研究的，中国国民的安全意识提高还需要一段时间嘛，但如果是网络管理员也这样，那就怎么也有点让人想不通了。网络安全问题日益突出，最近不又有人声称“ 万网：我进来玩过两次了！ ”一句话，目前很大部分的网站安全状况让人担忧！ 这里就我个人过去的经历和大家一同来探讨有关安全虚拟主机配置的问题。以下以建立一个站点cert.ecjtu.jx.cn为例，跟大家共同探讨虚拟主机配置问题。 一、建立Windows用户 为每个网站单独设置windows用户帐号cert，删除帐号的User组，将cert加入Guest用户组。将用户不能更改密码，密码永不过期两个选项选上。 二、设置文件夹权限 1、设置非站点相关目录权限 Windows安装好后，很多目录和文件默认是everyone可以浏览、查看、运行甚至是可以修改 的。这给服务器安全带来极大的隐患。这里就我个人的一些经验提一些在入侵中

较常用的目录。 C：\.D：\.…… C:\perl C:\temp\ C:\Mysql\ c:\php\ C:\autorun.inf C:\Documents and setting\ C:\Documents and Settings\All Users\「开始」菜单\程序\ C:\Documents and Settings\All Users\「开始」菜单\程序\启动 C:\Documents and Settings\All Users\Documents\ C:\Documents and Settings\All Users\Application Data\Symantec\ C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere C:\WINNT\system32\config\ C:\winnt\system32\inetsrv\data\ C:\WINDOWS\system32\inetsrv\data\ C:\Program Files\ C:\Program Files\Serv-U\ c:\Program Files\KV2004\ c:\Program Files\Rising\RAV C:\Program Files\RealServer\ C:\Program Files\Microsoft SQL server\ C:\Program Files\Java Web Start\ 以上这些目录或文件的权限应该作适当的限制。如取消Guests用户的查看、修改和执行等权限。由于篇幅关系，这里仅简单提及。 2、设置站点相关目录权限： A、设置站点根目录权限：将刚刚建立的用户cert给对应站点文件夹，假设为D：\cert设置相应的权限：Adiministrators组为完全控制；cert有读取及运行、列出文件夹目录、读取，取消其它所有权限。 B、设置可更新文件权限：经过第1步站点根目录文件夹权限的设置后，Guest用户已经没有修改站点文件夹中任何内容的权限了。这显然对于一个有更新的站点是不够的。这时就需要对单独的需更新的文件进行权限设置。当然这个可能对虚拟主机提供商来说有些不方便。客户的站点的需更新的文件内容之类的可能都不一样。这时，可以规定某个文件夹可写、可改。如有些虚拟主机提供商就规定，站点根目录中uploads为web可上传文件夹，data或者 database为数据库文件夹。这样虚拟主

机服务商就可以为客户定制这两个文件夹的权限。当然也可以像有些做的比较好的虚拟主机提供商一样，给客户做一个程序，让客户自己设定。可能要做到这样，服务商又得花不小的钱财和人力哦。 基本的配置应该大家都会，这里就提几个特殊之处或需要注意的地方。 1、主目录权限设置：这里可以设置读取就行了。写入、目录浏览等都可以不要，最关键的就是目录浏览了。除非特殊情况，否则应该关闭，不然将会暴露很多重要的信息。这将为黑客入侵带来方便。其余保留默认就可以了。 2、应用程序配置：在站点属性中，主目录这一项中还有一个配置选项，点击进入。在应用程序映射选项中可以看到，默认有许多应用程序映射。将需要的保留，不需要的全部都删除。在入侵过程中，很多程序可能限制了asp，php等文件上传，但并不对cer，asa等文件进行限制，如果未将对应的应用程序映射删除，则可以将asp的后缀名改为cer或者asa后进行上传，木马将可以正常被解析。这也往往被管理员忽视。另外添加一个应用程序扩展名映射，可执行文件可以任意选择，后缀名为。mdb.这是为了防止后缀名为mdb的用户数据库被下载。 3、目录安全性设置：在站点属性中选择目录安全性，点击匿名访问和验证控制，选择允许匿名访问，点击编辑。如下图所示。删除默认用户，浏览选择对应于前面为cert网站设定的用户，并输入密码。可以选中允许IIS控制密码。这样设定的目的是为了防止一些像站长助手、海洋等木马的跨目录跨站点浏览，可以有效阻止这类的跨目录跨站入侵。 4、可写目录执行权限设置：关闭所有可写目录的执行权限。由于程序方面的漏洞，目前非常流行上传一些网页木马，绝大部分都是用web进行上传的。由于不可

写的目录木马不能进行上传，如果关闭了可写目录的执行权限，那么上传的木马将不能正常运行。可以有效防止这类形式web入侵。 5、处理运行错误：这里有两种方法，一是关闭错误回显。IIS属性——主目录——配置——应用程序调试——脚本错误消息，选择发送文本错误信息给客户。二是定制错误页面。在IIS属性——自定义错误信息，在http错误信息中双击需要定制的错误页面，将弹出错误映射属性设置框。消息类型有默认值、URL和文件三种，可以根据情况自行定制。这样一方面可以隐藏一些错误信息，另外一方面也可以使错误显示更加友好。 