防范被种ASP木马需要注意这10点Microsoft认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E9_98_B2_E8_8C_83_E8_A2_AB_E7_c100_644219.htm 由于ASP它本身是服务器提供的一贡服务功能，特别是最近由dvbbs的upfile文件出现漏洞以来，其高度的隐蔽性和难查杀性，对网站的安全造成了严重的威胁。因此针对ASP木马的防范和清除，为网管人员提出了更高的技术要求。 几个大的程序全部被发现存在上传漏洞，小程序更是不计其数，让asp木马一下占据了主流，得到广泛的使用，想必如果你是做服务器的话，一定为此头疼不止吧，特别是虚拟主机的用户都遇到过网页被篡改、数据被删除的经历，事后除了对这种行径深恶痛绝外，许多客户又苦于没有行之有效的防范措施。鉴于大部分网站入侵都是利用asp木马完成的，特写此文章以使普通虚拟主机用户能更好地了解、防范asp木马。也只有空间商和虚拟主机用户共同做好防范措施才可以有效防范asp木马！ 我们首先来说一下怎么样防范好了，说到防范我们自然要对asp木马的原理了，大道理我也不讲了，网上的文章有的是，简单的说asp木马其实就是用asp编写的网站程序，甚至有些asp木马就是由asp网站管理程序修改而来的。就比如说我们常见的asp站长助手，等等。 它和其他asp程序没有本质区别，只要是能运行asp的空间就能运行它，这种性质使得asp木马非常不易被发觉。它和其他asp程序的区别只在于asp木马是入侵者上传到目标空间，并帮助入侵者控制目标空间的asp程序。严重的从而获取服务器管理员的权限，要想禁止asp木马运行就等于禁止asp的运行，显然这是行不通的，这也是为什么asp木马猖獗的原因

！有人要问了，是不是就没有办法了呢，不，有办法的：第一：从源头入手，入侵者是怎么样上传asp木马的呢？一般哟几种方法，通过sql注射手段，获取管理员权限，通过备份数据库的功能将asp木马写入服务器。或者进入后台通过asp程序的上传功能的漏洞，上传木马等等，当然正常情况下，这些可以上传文件的asp程序都是有权限限制的，大多也限制了asp文件的上传。（比如：可以上传图片的新闻发布、图片管理程序，及可以上传更多类型文件的论坛程序等），如果我们直接上传asp木马的话，我们会发现，程序会有提示，是不能直接上传的，但由于存在人为的asp设置错误及asp程序本身的漏洞，给了入侵者可乘之机，实现上传asp木马。 因此，防范asp木马的重点就在于虚拟主机用户如何确保自己空间中asp上传程序的安全上，如果你是用别人的程序的话，尽量用出名一点的大型一点的程序，这样漏洞自然就少一些，而且尽量使用最新的版本，并且要经常去官方网站查看新版本或者是最新补丁，还有就是那些数据库默认路径呀，管理员密码默认呀，一定要改，形成习惯保证程序的安全性。 那么如果你是程序员的话，我还想说的一点就是我们在网站程序上也应该尽量从安全的角度上编写涉及用户名与口令的程序最好封装在服务器端，尽量少的在ASP文件里出现，涉及到与数据库连接地用户名与口令应给予最小的权限. 需要经过验证的ASP页面，可跟踪上一个页面的文件名，只有从上一页面转进来的会话才能读取这个页面。防止ASP主页.inc文件泄露问题. 防止UE等器生成some.asp.bak文件泄露问题等等特别是上传功能一定要特别注意 上面的只是对客户的一些要求，但是空间商由于无法预见虚拟主机用户会在自己站点中上传什

么样的程序，以及每个程序是否存在漏洞，因此无法防止入侵者利用站点中客户程序本身漏洞上传asp木马的行为。空间商只能防止入侵者利用已被入侵的站点再次入侵同一服务器上其他站点的行为。这也更加说明要防范asp木马，虚拟主机用户就要对自己的程序严格把关！为此我总结了ASP木马防范的十大原则供大家参考：1、建议用户通过ftp来上传、维护网页，尽量不安装asp的上传程序。2、对asp上传程序的调用一定要进行身份认证，并只允许信任的人使用上传程序。这其中包括各种新闻发布、商城及论坛程序，只要可以上传文件的asp都要进行身份认证！3、asp程序管理员的用户名和密码要有一定复杂性，不能过于简单，还要注意定期更换。4、到正规网站下载asp程序，下载后要对其数据库名称和存放路径进行修改，数据库文件名称也要有一定复杂性。建议我公司的客户使用.mdb的数据库文件扩展名，因为我公司服务器设置了.mdb文件防下载功能。5、要尽量保持程序是最新版本。6、不要在网页上加注后台管理程序登陆页面的链接。7、为防止程序有未知漏洞，可以在维护后删除后台管理程序的登陆页面，下次维护时再通过ftp上传即可。8、要时常备份数据库等重要文件。9、日常要多维护，并注意空间中是否有来历不明的asp文件。记住：一分汗水，换一分安全！10、一旦发现被入侵，除非自己能识别出所有木马文件，否则要删除所有文件。重新上传文件前，所有asp程序用户名和密码都要重置，并要重新修改程序数据库名称和存放路径以及后台管理程序的路径。做好以上防范措施，您的网站只能说是相对安全了，决不能因此疏忽大意，因为入侵与反入侵是一场永恒的战争！编辑特别推荐: WinXP不能访

问Windows7共享文件 诊断:电脑中毒后的一些表现 Windows7的新快速键 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com