WIN2000SERVER安全配置技巧58条（三） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/140/2021_2022_WIN2000SER_c100_140037.htm 21.安装最新的MDAC（http://www.microsoft.com/data/download.htm） 说明：MDAC为数据访问部件，通常程序对数据库的访问都通过它，但它也是黑客攻击的目标，为防止以前版本的漏洞可能会被带入升级后的版本，建议卸载后安装最新的版本。注意：在安装最新版本前最好先做一下测试，因为有的数据访问方式或许在新版本中不再被支持，这种情况下可以通过修改注册表来档漏洞，祥见漏洞测试文档。 22.设置IP拒绝访问列表 说明：对于WWW服务，可以拒绝一些对站点有攻击嫌疑的地址；尤其对于FTP服务，如果只是自己公司上传文件，就可以只允许本公司的IP访问改FTP服务，这样，安全性大为提高。 23.禁止对FTP服务的匿名访问 说明：如果允许对FTP服务做匿名访问，该匿名帐户就有可能被利用来获取包多的信息，以致对系统造成危害。 24.建议使用W3C扩充日志文件格式，每天记录客户IP地址，用户名，服务器端口，方法，URI字根，HTTP状态，用户代理，而且每天均要审查日志。（最好不要使用缺省的目录，建议更换一个记日志的路径，同时设置日志的访问权限，只允许管理员和system为Full Control） 说明：作为一个重要措施，既可以发现攻击的迹象，采取预防措施，也可以作为受攻击的一个证据。 25.慎重设置WEB站点目录的访问权限，一般情况下，不要给予目录以写入和允许目录浏览权限。只给予.ASP文件目录以脚本的权限，而不要给与执行权限。 说明：目录访问权限必须慎重设

置，否则会被黑客利用。 26.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。 说明：用户名与口令，往往是黑客们最感兴趣的东西，如果被通过某种方式看到源代码，后果是严重的。因此要尽量减少它们在ASP文件中的出现次数。出现次数多得用户名与口令可以写在一个位置比较隐蔽的包含文件中。如果涉及到与数据库连接，理想状态下只给它以执行存储过程的权限，千万不要直接给予该用户以修改、插入、删除记录的权限。 27.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。 说明：现在的需要经过验证的ASP程序多是在页面头部加一个判断语句，但这还不够，有可能被黑客绕过验证直接进入，因此有必要跟踪上一个页面。具体漏洞见所附漏洞文档。 28.防止ASP主页.inc文件泄露问题 当存在asp 的主页正在制作并没有进行最后调试完成以前，可以被某些搜索引擎机动追加为搜索对象，如果这时候有人利用搜索引擎对这些网页进行查找，会得到有关文件的定位，并能在浏览器中察看到数据库地点和结构的细节揭示完整的源代码。 解决方案：应该在网页发布前对其进行彻底的调试；安全专家需要褂讪asp 包含文件以便外部的用户不能看他们。 首先对 .inc 文件内容进行加密，其次也可以使用 .asp 文件代替 .inc 文件使用户无法从浏览器直接观看文件的源代码。.inc 文件的文件名不用使用系统默认的或者有特殊含义容易被用户猜测到的，尽量使用无规则的英文字母。 