**0x1 windows 8.3命名规则**

8.3是一中对档案名称命名的方法，这在DOS和Microsoft Windows的Windows 95及Windows NT3.5以的前版本中，在FAT档案系统中的常用方法。详见百度百科[8.3命名规则](http://baike.baidu.com/view/3307200.htm)。对于8.3命名规则知道下面四条就行了：

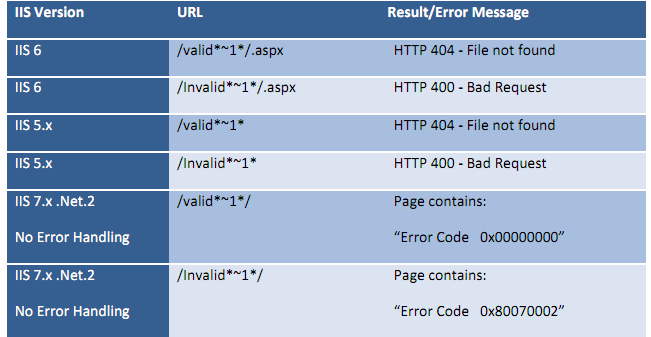
1. 文件名中最多只可以含有8个字符
2. 文件后缀最多3个字符
3. 目录名文件名都要是大写字
4. 当在windows下创建一个新文件时，系统同时会创建一个与ms-dos兼容的8.3命名的短文件名
5. 在cmd下可以用dir /x命令来查看对应的

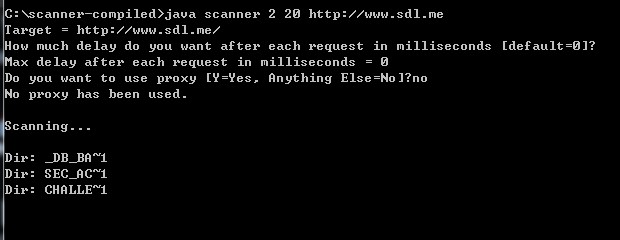
下图是虚拟机中某个目录用命令dir /x查看的情况：



**0x2在windows+iis下的安全性**

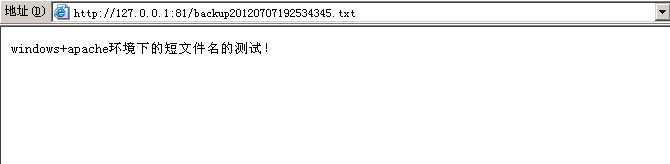
当在windows下搭建的是iis时，web文件和目录同样会像上面那样有好多的以8.3格式命名短文件名和目录名。那么就可以通过访问这些短文件名，根据服务器返回的信息来判断文件是否存在。下面是访问文件和对应的返回信息。



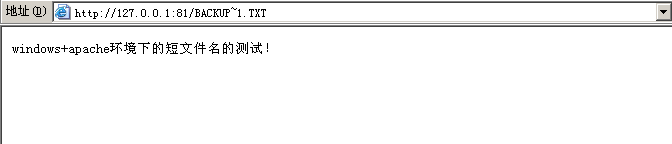
假设文件mypassword.txt这个文件名很长，不好猜测，同时它对应的短文件名是：MYPASS~1.TXT，那么直接猜测MYPASS~1.TXT会比上面猜测容易的多，然后通过这个文件名可以再进行猜测。具体细节可以看exploit-db上面的文档[Microsoft IIS tilde character “~” Vulnerability/Feature – Short File/Folder Name Disclosure](http://www.exploit-db.com/wp-content/themes/exploit/docs/19527.pdf)。同时作者有一个利用工具[iis-shortname-scanner](http://code.google.com/p/iis-shortname-scanner-poc/)

**0x3在windows+apache下的安全性**

在iis的环境下只是用来猜测和暴力破解文件名和目录是否存在，我们却不能利用浏览器通过短文件名来访问，因为iis做了限制，但是在apache就不一样，我们可以在浏览器里直接输入文件的短文件名来进行远程访问。例如，有一个文件长文件名是backup20120707192534345.txt



当我们如下访问时：



至于这个能做什么就看想象了：）

0x4参考文档

[Microsoft IIS tilde character “~” Vulnerability/Feature – Short File/Folder Name Disclosure](http://www.exploit-db.com/wp-content/themes/exploit/docs/19527.pdf)

[Windows Short (8.3) Filenames – A Security Nightmare?](http://www.acunetix.com/blog/web-security-zone/articles/windows-short-8-3-filenames-web-security-problem/)

<http://zone.wooyun.org/content/487>

**By qingshen**

**Blog** <http://hi.baidu.com/new/qingsh4n>