前提是主机支持shtm,shtml

当网站不允许上传asp cer cdx htr等文件时

上传一个shtml文件, 内容为:  
<!--#include file="conn.asp"-->  
直接请求这个shtml文件, conn.asp就一览无遗, 数据库路径也就到手啦!  
并且又看了那篇shtml的介绍后，恍然大悟，终于明白了！  
原来就是如上所说的，  
<!--#include file="conn.asp"-->  
就是一条SSI指令，其作用是将"info.htm"的内容拷贝到当前的页面中，当访问者来浏览时，会看到其它HTML文档一样显示info.htm其中的内容。  
我在本地试验成功！在我的iis目录下建了一个test.stm文件，内容为：  
<!--#include file="ok.asp"-->  
又在同一目录下放了一个我的一个文件ok.asp  
在浏览器中请求test.shtm，没有什么反映，一片空白。  
但是一查看源代码，狂晕，原来就是我的asp文件的内容！  
这样我们就可以利用这个来获取要目标机的web的conn文件来获得数据库路径，  
但是一个前提是服务器的对shtm或者shtml的扩展没有删除。  
====================================================  
现在很多网站的都不能上传asp，asa，cer等文件

经典的上传漏洞也没有了，但是很多网站还是可以上传其他的，比如shtm或者shtml文件，我发现了一个方法，你可以在本地建立的个shtml文件，然后输入

<!--#include file="conn.asp"-->

conn.asp就是你想读取的asp文件，当然是连接数据库的文件

呵呵，然后上传上去，最后用你的浏览器请求下这个shtml文件,怎么是空白哪？

哈.查看下这个网页的援代码，就是conn.asp的代码。

不用我告诉你都应该怎么作了吧。