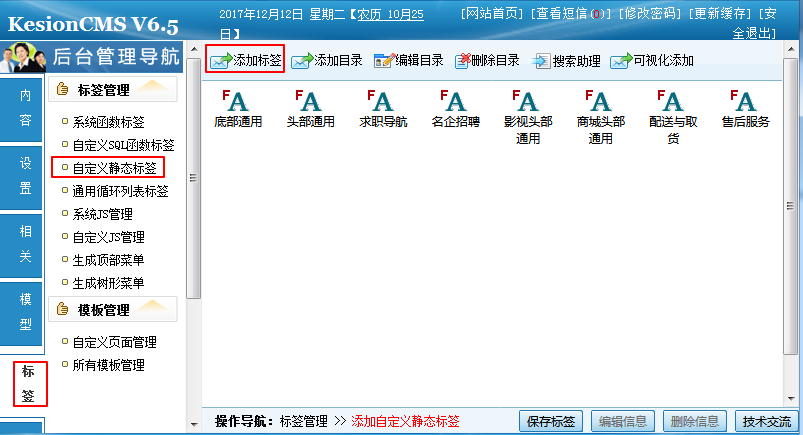
# 添加静态页面拿webshell

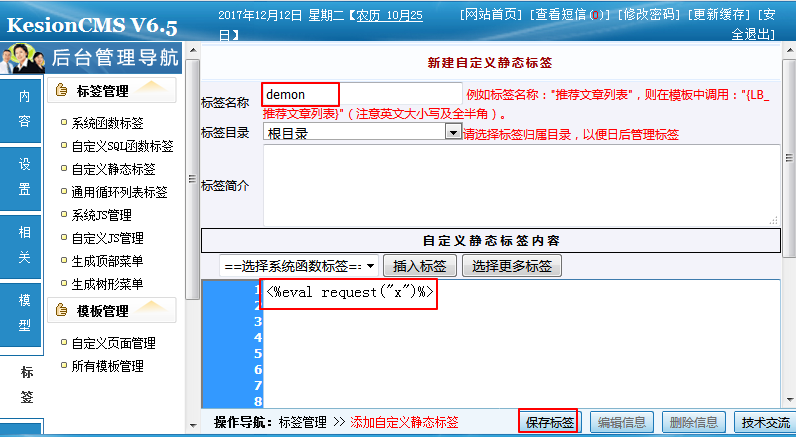
测试靶机： Kesion6.5-cms

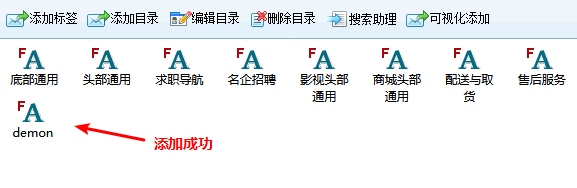
登录后台http://192.168.10.12/admin/login.asp admin admin888 8888

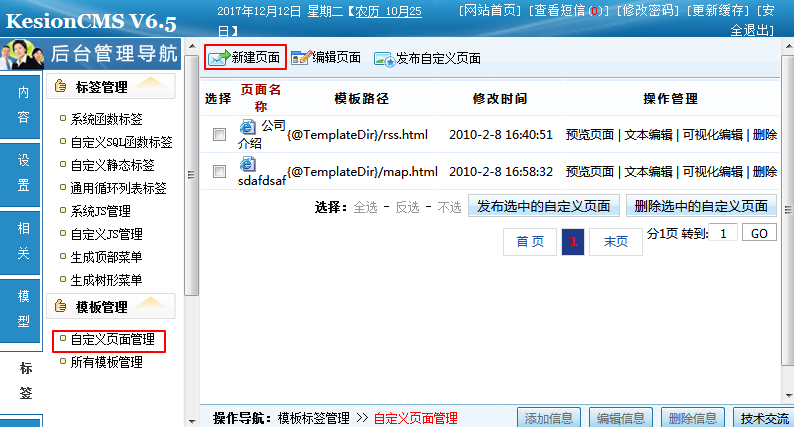




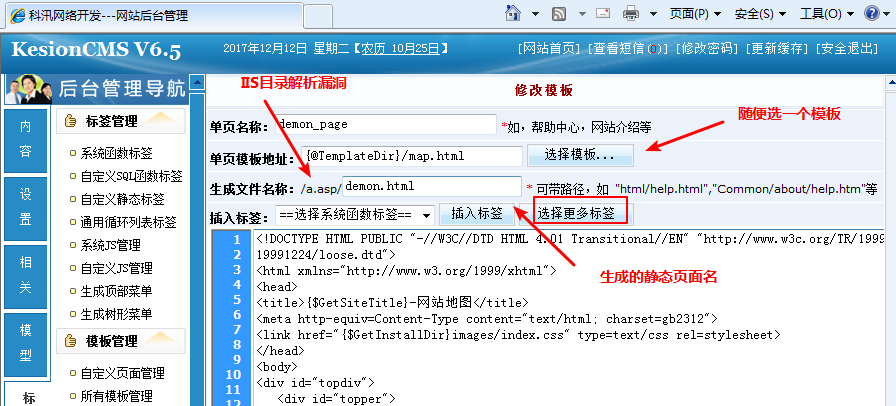




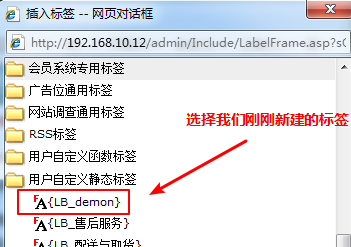




注意：点击新建页面时候可能没有反应，换IE浏览器就可以点出来了

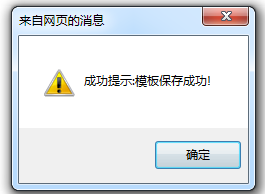


点出来后，选择模板和填写生成html的名字，然后点击选择更多标签

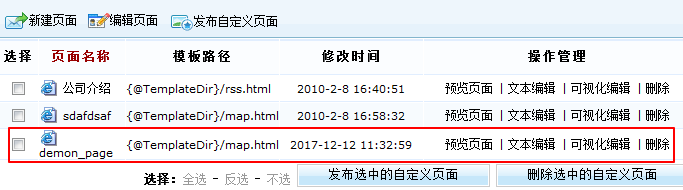


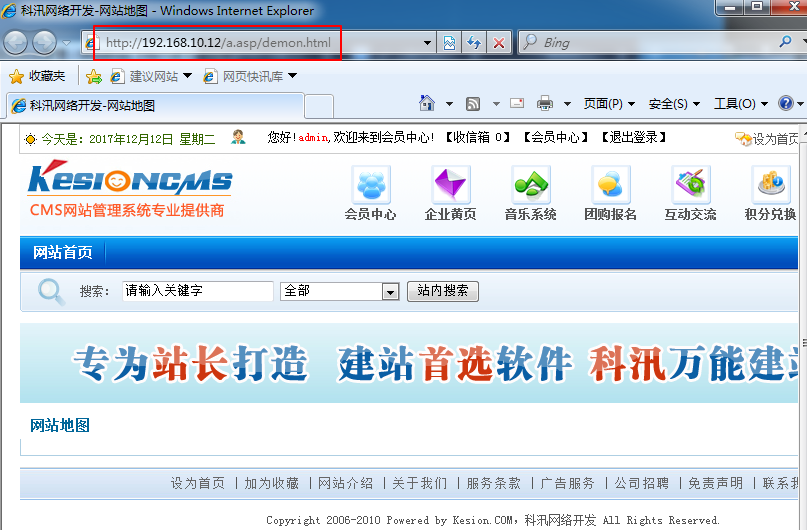
插入好后点击确定添加，就可以生成静态页面了。



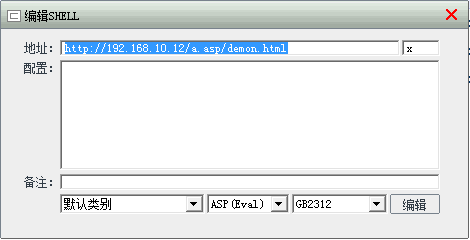


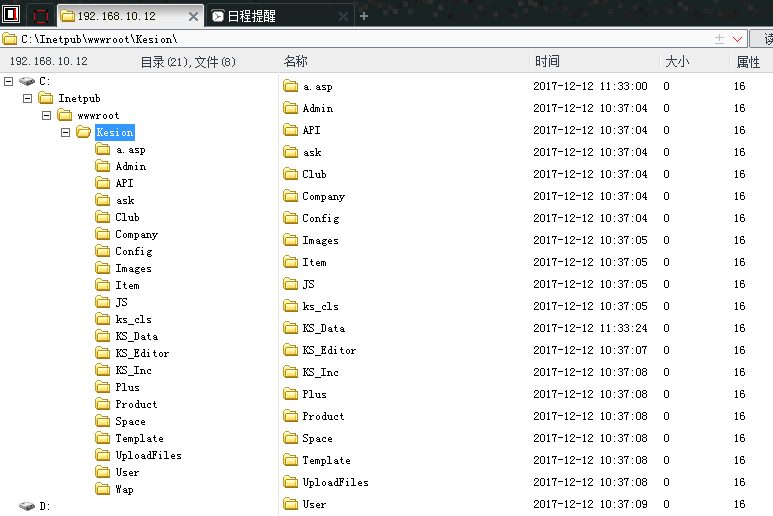
然后点预览页面



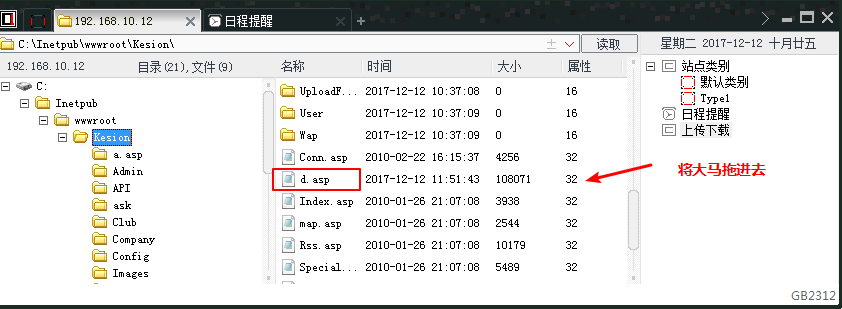


复制URL，用菜刀连接一下

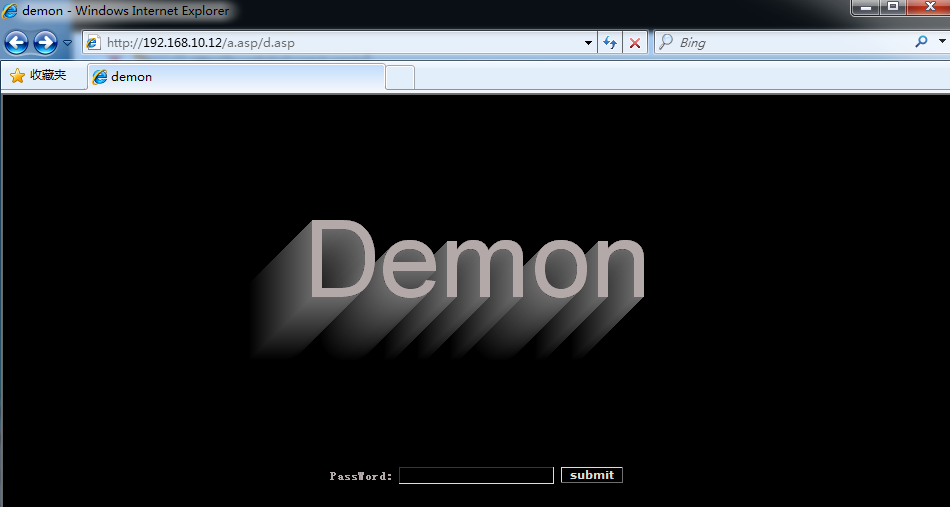


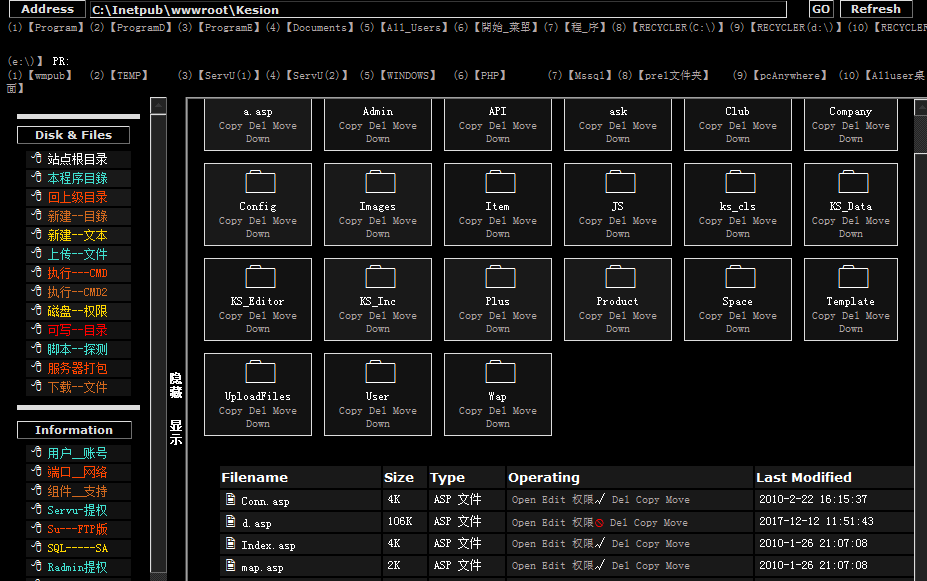


成功Getsehll，进入a.asp目录下直接上传asp大马



然后浏览器连接一下大马





注意：直接将大马上传到a.asp/目录下，登录密码后会爆503错误，最好上传到其他目录