# 数据库备份拿webshell

实验靶机：liangjing-v7.0

说明：利用数据库备份功能，将我们上传的图片木马，备份改名成asp格式的文件，从而拿到webshell，现在大部分cms都已经写死了数据库备份的路径，但是一些老的站点还是会有这个漏洞，就比如良精通用企业v7.0的cms。

拿webshell演示：



进入后台，账号密码admin



在荣誉管理添加荣誉里可以上传图片文件



如果直接上传asp木马是会被过滤的



所以我们这里上传一个 asp图片格式的木马



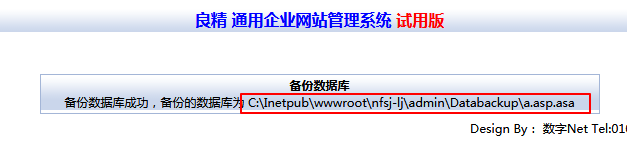
上传好后，复制图片的地址，访问数据库备份模块



这里的当前数据库路径可以被人为的修改，因此直接粘贴我们复制的图片地址改成asp文件



点击提交后，会显示备份后的地址



最后访问地址拿webshell http://192.168.10.12:8080/admin//Databackup/a.asp

