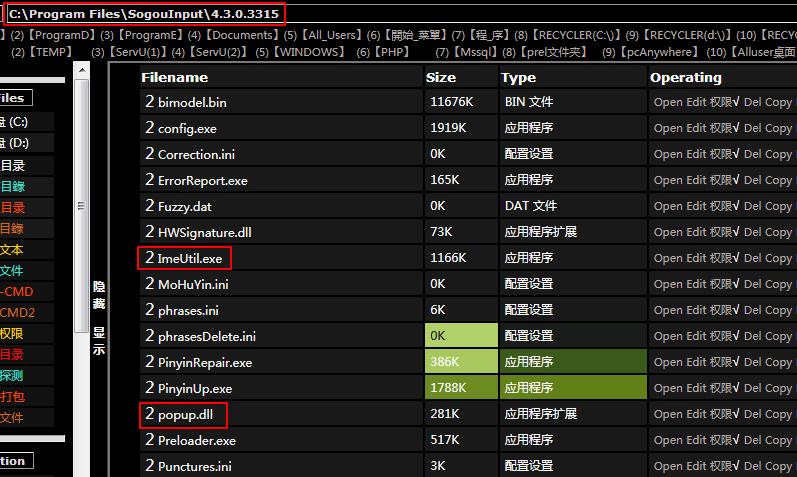
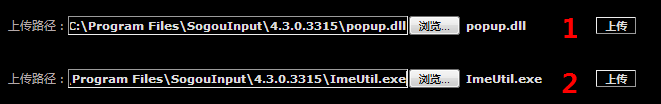
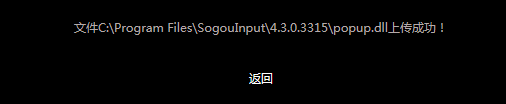
# sougou输入法提权

对于搜狗输入法4.3的版本可以利用imeutil.exe文件来提权，该文件是搜狗拼音被切换时会触发执行的一个可执行文件，替换该文件，新的文件可以创建超级管理员账号，只要管理员切换输入法就会触发执行。

首先利用大马上传imeutil.exe和popup.dll这两个文件

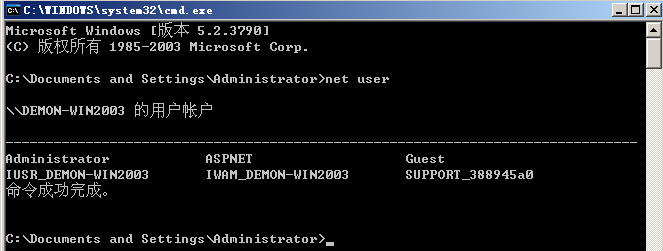






因为搜狗支持在线升级，所以软件所在的目录一般都是有写入文件的权限

上传成功后，下面模拟管理员切换拼音输入法时触发执行创建超级管理员账号



当管理员切换输入法，就会触发执行ImeUtil.exe 来创建sunwear用户

