|  |
| --- |
| 作者:人生  [www.hake.cc](http://www.hake.cc/)  好久没出文章了，最近有点小忙。。  遇到一个站，  一开始，直接上传FCK得到SHELL觉得直接能提  wps_clip_image-3734.png  拿到SHELL后，  wps_clip_image-22111.png  坑爹的事情来了。禁止了目录。然后我翻到根目录的时候  wps_clip_image-4117.png  然后对应图片访问  wps_clip_image-28595.png  居然提示无该地址。。。。这搞的飞机让我头大的要命。。。  发现有其他旁站，干脆翻到其他旁站。过了半个小时终于有个网站目录是对的。拿到了SHELL  wps_clip_image-10947.png  辛苦了半个小时终于拿到SHELL了，但后面坑爹的事情来了。  上传了NET大马一个访问不到  wps_clip_image-11081.png  然后看了ASP大马的权限，更悲剧。。。  wps_clip_image-5706.png  wps_clip_image-19072.png  不管什么目录都没权限，搞得我快发毛了。而且还有SU，，可没一个能提得上  想了想，貌似ASPX一句话可以执行。然后丢个ASPX一句话上菜刀  连接果断成功，不截拦。人品啊。  执行EXE 成功，  然后接下来一路就比较风顺了  wps_clip_image-21982.png   System权限。  wps_clip_image-19891.png  收工  wps_clip_image-3630.png |

[wps\_clip\_image-3738.png](http://wwww.hake.cc/forum.php?mod=attachment&aid=MzYxNHw4OTgwNTk4MHwxMzE5NTYzNDc4fDgxNTI%3D&nothumb=yes) (18.67 KB, 下载次数: 9)



[wps\_clip\_image-21261.png](http://wwww.hake.cc/forum.php?mod=attachment&aid=MzYyMXwzMzNjMDM3NnwxMzE5NTYzNDc4fDgxNTI%3D&nothumb=yes) (10.41 KB, 下载次数: 0)

