|  |
| --- |
| 目标 ：[http://wadcszc.com](http://wadcszc.com/) 这是群里一个大牛发的，接单大牛不解释！！！ 群里关于求助入侵的通通列为接单黑阔，唉！！！何必呢 （不知从何时我也被人这样称呼了，我解释下没接过单http://wwww.hake.cc/static/image/smiley/coolmonkey/12.gif） 那朋友求助后台地址， 最近迷恋Pker，废话不说开扫！！发现robots.txt   未命名.jpg  chongsheng147258369     当时就怀疑这个是后台目录了，打开显示403 继续扫啊，为什么你就停下了呢？ 开扫<http://wadcszc.com/chongsheng147258369/>        未命名.jpg   <http://wadcszc.com/chongsheng147258369/ewebeditor.asp?id=x&style=standard>  明显ewebeditor编辑器，但是打开后果断蹦到后台，指向的后台并不是编辑器的而是站点后台  <http://wadcszc.com/chongsheng147258369/logon.asp>         有inc   果断后面conn.asp    爆出数据库路径（其实注入中转也能拿到管理用户密码） Microsoft JET Database Engine 错误 '80004005''e:\webuser\zc0001\wwwroot\chongsheng147258369\data\#@!$%%%00dddd1fksf\_#%gggg$^#$$yiller111111.asp'不是一个有效的路径。 确定路径名称拼写是否正确，以及是否连接到文件存放的服务器未命名.jpg 。/chongsheng147258369/Inc/conn.asp，行 4   数据库我试了 可以下载的URL编码 你们懂的  未命名.jpg   进了后台后，上传无用，无备份等XXX               果断利用一句话  未命名.jpg  成功拿到webshell    细心+耐心+思路+方法=技术（俺没有）  大牛勿笑http://wwww.hake.cc/static/image/smiley/coolmonkey/01.gif |

[未命名.jpg](http://wwww.hake.cc/forum.php?mod=attachment&aid=MzEzOHxlOGZmODdjMHwxMzE5NjM1MDMzfDgxNTI%3D&nothumb=yes) (28.71 KB, 下载次数: 0)

