图/文  
转载注明 [哈客部落](http://www.hake.cc/)  
[www.hake.cc](http://www.hake.cc/)  
我们滴目标站是：[http://www.cyczw.com](http://www.cyczw.com/)  
传说中的冥客。。现在真是啥客都有。。。过几天是死客  
好了 我们开始我们的演讲大会！我文笔不好。。  
咳咳。。开始。。  
第一步:偶是旁滴！！!看到个公司站。。什么公司就不透露了。。  
找到了编辑器目录cmsedit，结果MD5密码解不出，也懒的跑了。。  
我就去看了下他的新闻，注入不了。。哥就cookie注入。。成功了。。但是那密码卡的弄不出啊。。我组合了好几次- -  
进后台。。发现备份数据库不行，本地提交不行。。我就上传去老。下载文件。上传个JPG，抓包，上穿ASP，成功，结果目录没有。失败  
继续添加新闻。。一样抓包，这次上传成功鸟！把我激动的呀。。直接传个大马。。看了下C:\RECYCLER 可写 可读。。  
传个CMD 传个ASPX大马 测试下。。  
set命令 成功。。其他命令全OVER 包括那什么突破PR的方法。。结果我把马给了miss..他突然来了句可以跨目录- -。。  
我怀着激动的心情去拿ASP跨目录结果失败。。。但是换ASPX居然可以跨。。偶激动呀。。  
他不是以域名名称做FTP帐号，文件夹肯定也不是了。一个一个找吧。找PHP滴站。。找了N久啊。终于找到了。。  
后面大家都知道了。。挂了个TXT就闪了。。无破坏。。分享下。。  
花了偶半小时去入侵这个破站。。。  
<http://www.cyczw.com/shaolong.txt>  
