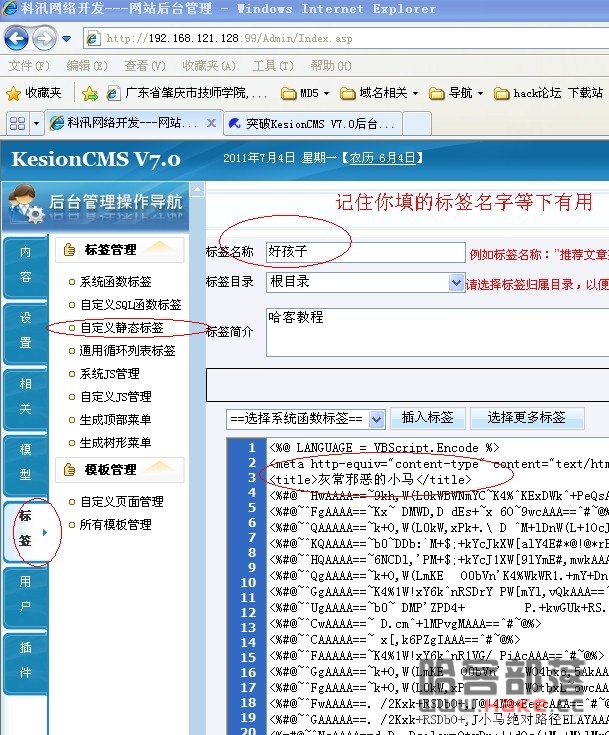
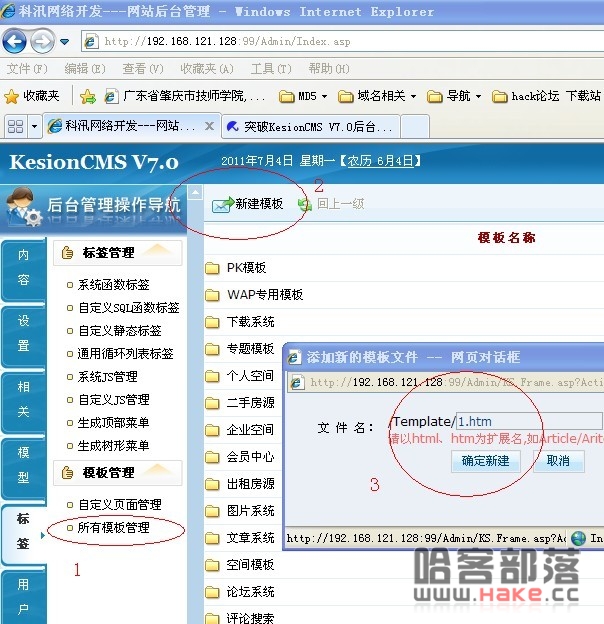
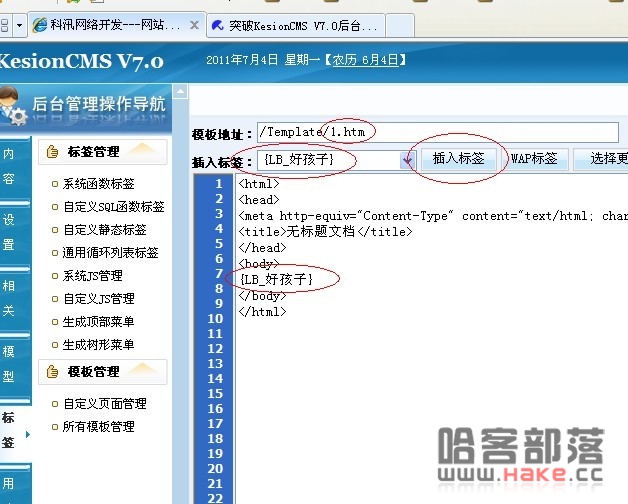
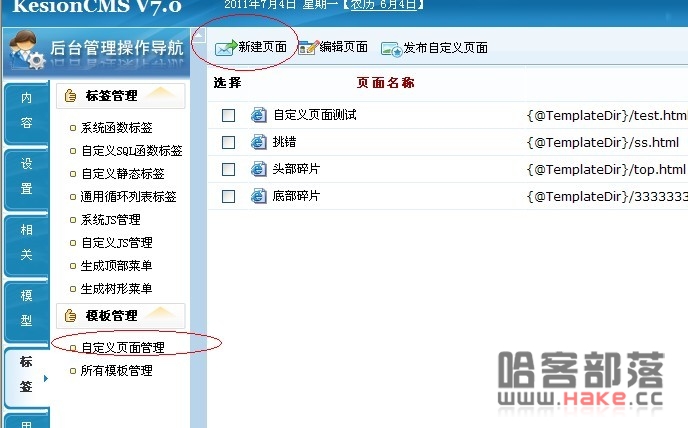
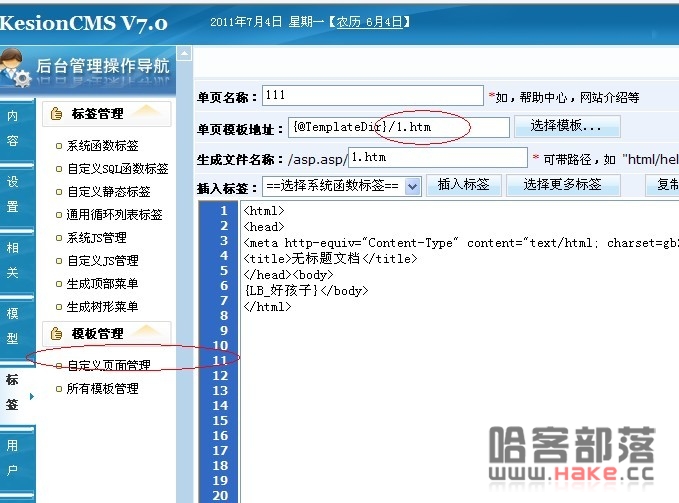
看到某位童鞋的《突破KesionCMS V7.0后台备份拿webshell》看了下感觉好像就是靠工具嘛！  
正好昨晚呢有位童鞋也给了我个KesionCMS V7.0的后台 当时啊！我那个蛋疼你是知道的！  
于是呼打开百度找0day吧  关键字：KesionCMS V7.0后台拿shell  没看到几个 不过还是看了一些思路  
不过不知道是我太笨看不懂呢还是怎么的 我传的小马都是乱码的我晕！！  
后来呢摸索了一下变动了一下 思路清晰了一点！ 好了不吹牛逼了！  
其它的不说 都知道什么上传啊捉包啊数据库备份啊改后缀啊都K了  
自己下载并搭建KesionCMS V7.0 系统测试 因为我是好孩子不会去入侵的。。  
一步一步来我会上图的，  
   
进后台后小鼠标点下下面那个基本信息设置\其它选项找到那个通用页面目录html/改为asp.asp/ 保存设置  
  
下一步自定义静态标签 就这样保存他   
  
  
下一步 点所有模版管理\新建模版\把名字改为1.htm（或其它.htm）  
   
  
新建后再找到新建的模版点击编辑把刚才的好孩子的标签插到<body> {LB\_好孩子} </body> 保存他   
再到自定义页面管理那里新建页面   
  
   
  
保存之后点击预览直接看到小马  
   
  
这只是一个思路。