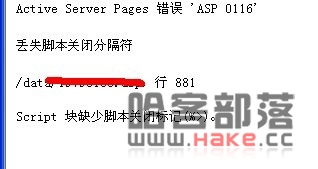
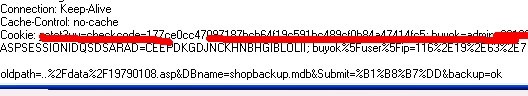
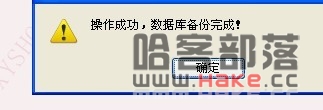
本帖最后由 geary 于 2011-6-26 21:15 编辑  
  
昨晚看到一asp站。  
没注入，看后台。  
   
发现还要填写后台目录。  
猜不到。  
所以拿起工具开扫。  
   
看到123.rar这个文件  
好奇之下下载下来。  
发现是整站。  
找到数据库，拿到帐号密码，找到后台目录。  
果断进之。  
   
上传没办法利用，想到数据库是asp的。  
想插入一句话。访问出现。  
  
   
  
看到有数据库管理。  
   
想到以前，有些站可从这突破，所以抱着尝试的心态。抓包。  
   
数据库和备份路径都在这，那就可以突破了。  
试下，打开火狐live http headers这个插件。  
   
其中..%2Fdata%2F19790108.asp为数据库路径  
shopbackup.mdb为备份。  
传一张图片马儿上去，路径为..%2Fpic%2F201111.jpg  
备份成12.asp  
   
修改后的Content-Length数值要一样。  
修改好提交。  
   
把路径和数据库改了，提交。  
备份成功。  
拿到了这个站的权限。  
