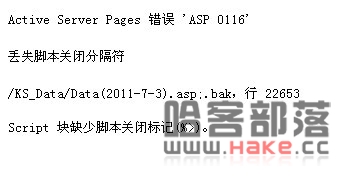
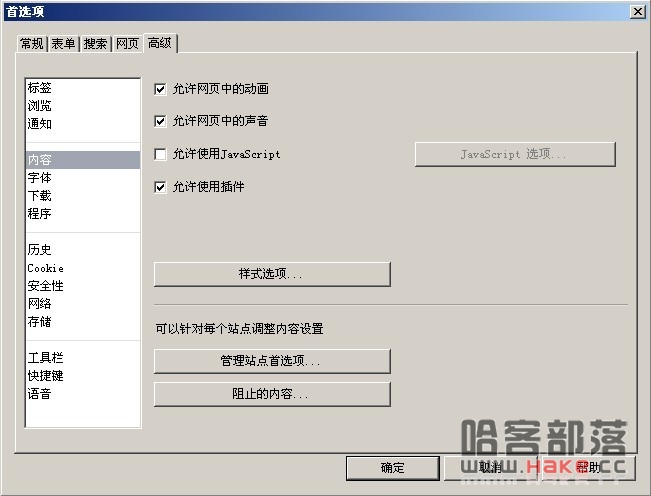
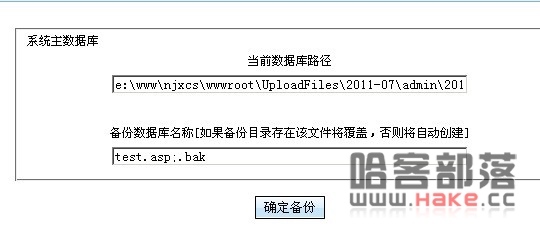
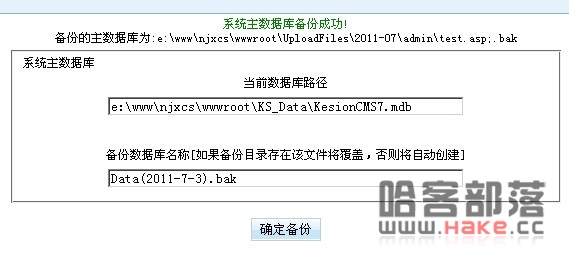
可能有些童鞋看到这个题目的时候,会感到许些的蛋疼。不就一个备份嘛，突然个啥子捏？的确是个备份，但这个备份呢，是有限制的。有些童鞋入侵KesionCMS的时候，可能会遇见过这么一个备份，然而在网上，似乎木有人分享过这么一个思路。我在这里就分享下，喜欢的我表示感谢，不喜欢的可以任意拍砖。  
  此刻已凌晨6:01。刚才，检测一个网站，然后旁站呢，遇到了一个KesionCMS V7.0，后台很容易就进去了，因为默认的帐号密码之类的尚未更改。后台功能看上去十分的强大，让我感到了许多的欣慰。我好象知道，胜利就在眼前了。当然，网上也爆过许多KesionCMS后台可以得到webshell的方法。也有讲到备份那块的，思路是:数据库插马-把NOTDOWN里面的数据UPDATA成一句话备份。而我现在讲的就是另一种思路，好象灌水成分过多了，不好意思，我们继续。  
                                                         
  
  当前数据库路径是不可以修改的，就是因为这样，我们备份出来的马才木有闭合。                  
  那么我是如何突破的呢？我这里就用到了opera浏览器。(个人感觉还是挺不错的，好吧，我承认，我在打广告。)竟然数据库被做了手脚了，我们像以往一样备份图片不就行了？导致备份的数据库路径无法修改的罪魁祸首就是那几个代码了，我们现在就来去掉它。目前我们还未能查看到备份数据库文件的代码，一般打开新框架就可以了，但是这里右键已无效，我想一定是javascript作怪，那就先把javascript停止使用。  
                                                               
  
  果然，这下右键恢复了，右键打开框架，就弹出了新框架，地址是<http://www.xxoo.com/admin/KS.Database.asp?Action=BackUp> 一看，竟然是空白页面，查看源代码，发现了这么一段玩意。<script>alert('请不要，非法提交！');history.back();</script>看来也是做了手脚的了，它已经阻止不了我了。  
  这里我的解决方法是-通过查看后台源代码找出导航地址-通过导航访问，因为通过导航访问不会提示非法了。这个过程就不一一解释了，相信难不倒各位的，我们继续回到主题吧。访问导航地址Index.asp?Action=Left，然后通过导航点击数据库维护，这样就可以了。最后，查看源代码，找到罪魁祸首，去掉后当前数据库路径自然就可以修改了。往下看:      
  
  这么一个活生生的readonly (只读)，就出现在我们眼前了，好的，我们现在就结束它的生命吧。去掉之后，点击opera左上角的应用保存，返回后，你会发现数据库路径可以修改了。这里顺便说一下上传伪装图片木马，一般的文件头欺骗是无法通过的，我这里用到了edjpgcom工具合并了一张一句话图片木马，或者使用copy命令，效果也是相同的。上传伪装图片一句话木马后，查看源代码，得到地址：/UploadFiles/2011-07/admin/2011070305523639373.jpg，现在我们就开始来备份。  
   
      
  
  用菜刀连接<http://www.xxoo.com/UploadFiles/2011-07/admin/xxoo.asp;.bak>，成功。  
    