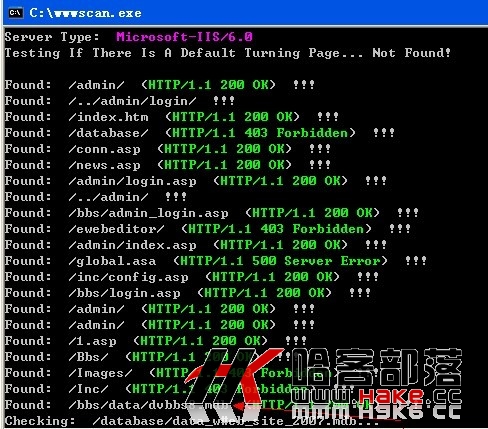
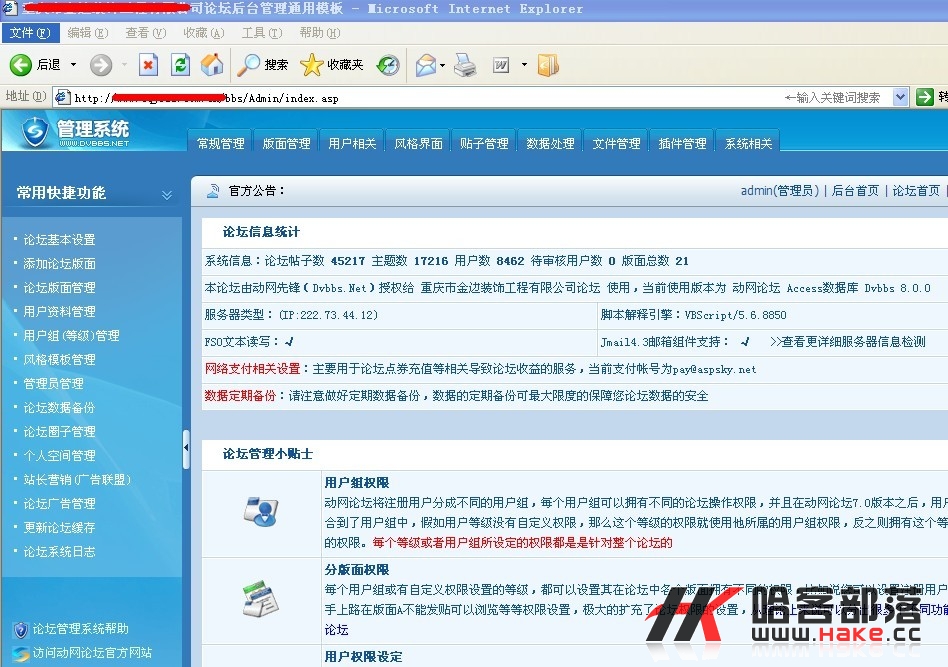
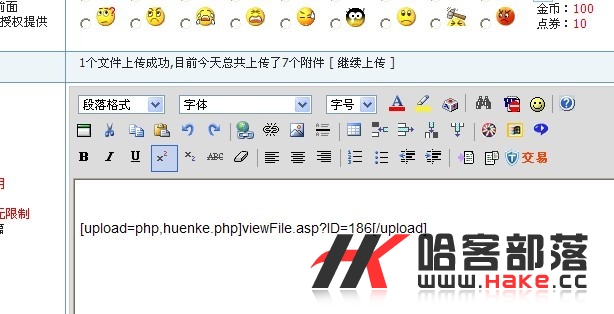
大家好,欢迎各位来哈客部落学习,这里是一个很不错的学习地方.  
  
论坛地址 [www.hake.cc](http://www.hake.cc)  
  
作者：张三疯  
  
小弟今天来哈客，见到哈客很多大牛，哎。小弟也写个菜鸟文章吧。希望大牛别骂。小菜学习。大牛就路过吧。  
  
开始。<http://www.xxxxxxx.com.cn/> 重庆金边装饰工程有限公司 这个是我们今天的目标。  
  
打开访问下，是asp的，呵呵，我一般日站都喜欢丢进工具让他扫。  
  
真郁闷，工具扫不出注入点，手工看看。[http://www.xxxxx.com.cn/artshow.asp?tid=438'](http://www.xxxxx.com.cn/artshow.asp?tid=438)  结果出现这样 请不要在参数中包含非法字符尝试注入！ 哎 防止注入了,我们换思路,中转看看. 结果一样不行,哎没办法了.丢进啊D扫下看能扫出什么东西出来不.  
<http://www.xxxxx.com.cn/admin/login.asp> 默认后台 不过扫的结果 扫到了一个<http://www.xxxxxx.com.cn/bbs/>  论坛.  
  
呵呵 论坛 看看能不能从论坛下手了.丢进wwwscan让他扫  哈哈 扫得过程中 有惊喜了 看图  
  
呵呵 扫除数据库地址了. 不废话,直接下载数据库.  
这时候知道了账号密码,我们就登陆论坛 账号密码 admin admin888 呵呵 登陆成功。看图  
  
好，我们就点击论坛的管理 账号密码都是 admin admin888 登陆后台成功  
  
这时候我们怎么拿shell呢？ 然后被我看到了论坛数据库备份。  
  
不过，是有数据库备份，但是怎么都是找不到上传文件的页面。放弃。换个思路。  
接下来，我在里面观察了很久。点版面管理-然后高级设置-往下拉    看到上传文件类型  
  
  
我在里面添加了 php和asp   
我们在后台找不到上传的页面，我们就从论坛上传看看。随便找个地方上传，就发表文章吧。  
OK，上传PHP马成功。图  
  
我们点击用户控制版面。  
  
这个是我们刚上传上去的。  
  
马的路径 <http://www.xxxxxx.com.cn/bbs/UploadFile/2011-5/201159224759583.php>  
OK,成功拿下shell  
  
  
呵呵，第一次写，有点紧张，写得不好的不要骂我。谢谢