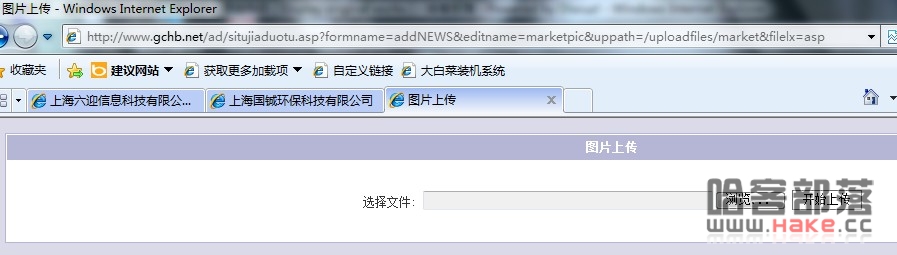
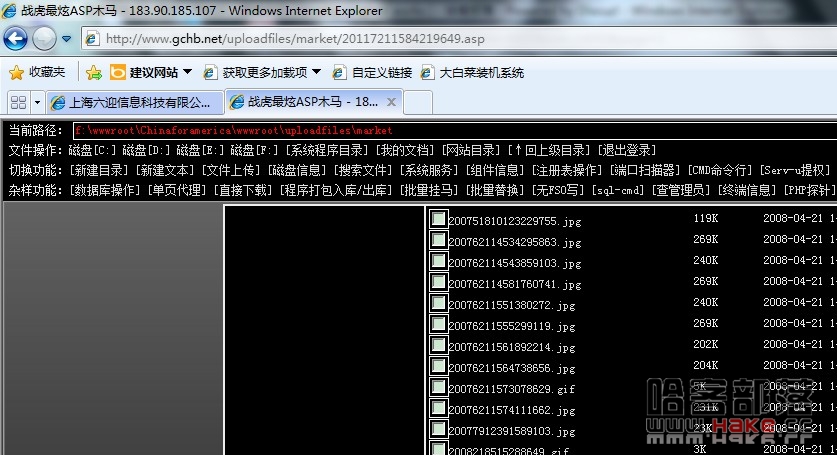
大家好 我是战虎：  
     先来看我们的目标站！  
[http://www.gchb.net](http://www.gchb.net/)  
    先随便  点个连接  加个单引号！、  
  
报错了  ！   好接着来and 1=1  
返回正常  
   
那我们来看下and 1=2    
   
有注射漏洞！     这里我们直接丢啊D    其实也可以手工 我们为了节约时间就用工具  
扫 因为这不是我们的重点  
  
我们先来找找后台   admin   admin/admin\_login.asp        login.asp     manage     
  都不行       算了 丢工具扫下！  用pker  扫下。  
   
看见什么了  ？  ad  很熟悉对吧  那我们试试  
   直接找到后台了  
   
帐号密码都出来了  
    帐号是 admin   密码是  hezh  我们先登陆进去看下      有数据库备份 但是没有  权限郁闷了    
   
  我们还是先找上传 ！  
   
点击上传图片 ！  现在重点来了    ！  
   
  你们看见出什么了吗？        
我们看URL  的最后  里面 是个filelx=jpg    意思是 它这里  
  上传的类型是JPG的   那我们把 JPG  改成ASP的呢  
然后点刷新一下  看   后面变成了ASP了  
   
  那我们现在上传ASP看下呢    
  呵呵ASP的直接上传成功了！   
看下我们的地址！    
  呵呵直接就是ASP的  那我们直接来访问下 马儿的地址   
[http://www.gchb.net//uploadfiles/market/20117211584219649.asp](http://www.gchb.net/uploadfiles/market/20117211584219649.asp)  
  
呵呵 进去       
呵呵这样我们就成功的拿到了webshell了  
   重点是  我们要把那个上传地址的JPG  改成ASP    
  直接可以成功突破限制  上传ASP的   这样会省去我们很多的时间  
   其实我们在渗透的时候 多观察下    
      有时候我们会发现很多地方可以利用  省去我们走很多弯路！！！  
   好了 教程 就到这了 ！  希望审核能够通过！