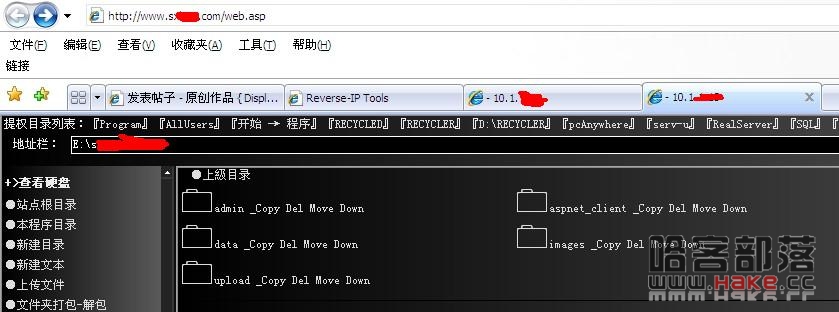
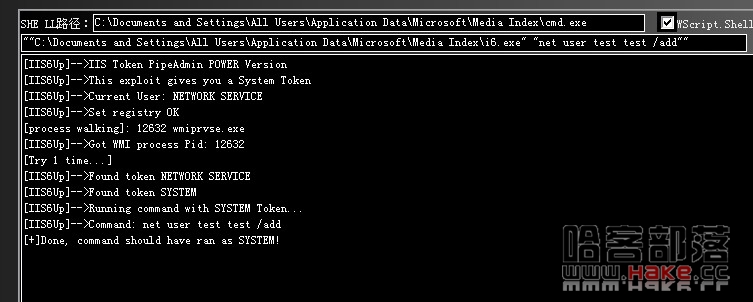
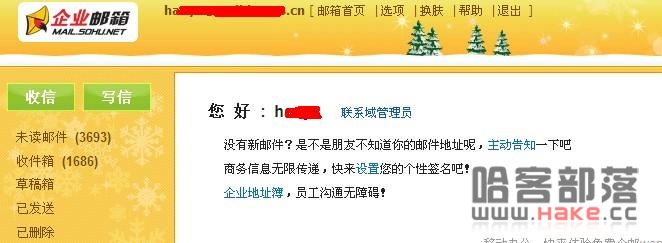
图/文  
作者：过河的卒  
闲来无事，随便找了一个站点，这是一个导航站，大家看看。一般遇到这样的站点，我都是找同F其他站点拿下。  


2011-7-24 15:01 上传

[**下载附件** (101.85 KB)](http://wwww.hake.cc/forum.php?mod=attachment&aid=MzE1M3wyZjcwYmU5ZXwxMzE5NjQxNDUyfDgxNTI%3D&nothumb=yes)

找了下同F站点，只有1个，是一个教研之类的网站，通过一些常规的方法没有拿下，怎么办呢，我看到了下面的技术支持。也是这个做站的。  
   
他上面一般都会有成功案例之类的东西，就继续在案例里面找，找了一个注入点，用啊D检测下，出现问题。  
   
大家看到了吧，只有用户名，没有密码，可能大家会想，你既然已经找到后台，可以看看表段然后添加上啊，是常规应该这样，但是后台的表段就是username和password，大家仔细看看，我涂红的部分，第一个用户是他网站的域名，第二个是技术支持的域名，第三个是字母加数字。那么我们现在就应该试试用户名是那个字母加数字，而密码就是这串数字了，当然结局是美好的，顺利拿到一个shell。  
   
如你看到的一样，这个目录很熟悉吧，如果支持aspx提权有希望，这个全部不支持，只支持asp，（提权我尝试了，没有提起，不过后来我看到他总共有3台服务器，我们可以抓取hash来社工试试，当然这是后话了）我们回到正题，聪明的你应该能想到了吧。当然了，下载他的数据库，然后破解那个技术支持域名的md5，就可以通杀他做的所有网站。教研站通过wvs顺利扫到后台  
拿下shell。  
   
大家看，这个图上有2台他的服务器，都是内网一个是10.1.1.11 一个是10.1.1.13 其中10.1.1.12也是他的 上面挂了些类似门户的站点我们的目标是10.1.1.13提权开始。支持ws，看到这里，你是否又该偷笑了，拿站不到最后一步，先不要笑。  
   
C D盘符无浏览权限，E盘出现垃圾箱，说的很不专业啊。。。 应该是回收站。上cmd，出现下面让人纠结的一幕。  
   
现在怎么办呢，当然是换位置了，我们继续找啊找，你也可以用啊D写的读写目录检测来尝试，我现在习惯找星外爆出来的那个media index 我们继续上cmd尝试，结果让人欣慰。为了让文章篇幅短点，我就直接简略了。上了i6 以及n多神奇，执行net命令是无效的，exe名称换了也是无用功，怎么办，我们上我们的远控马，利用i6来执行。  
   
记得在无回显的时候加上双引号，论坛已经有人发过此类教程，在此感谢。马顺利上线，抓出了hash尝试了其他2个服务器，都失败。为了力求真实性，我还是放一张服务器截图。  
   
另外一个10.1.1.11暂时没有拿到 10.1.1.12这台上面倒是有不少站，而且一个用的是讯时 也进去了 但是管理所有漏洞全部补好了，他那个编辑器还有个历遍目录，也是鸡肋，这里不说，利用那个技术支持的账号，顺利登陆他的邮箱，以及淘宝支付宝之类的，这里放出一张邮箱截图。淘宝支付宝就不展示了，毕竟我们不要给人家带来麻烦。  
   
最后说下，只是技术交流，请勿给别人自造麻烦，感谢isosky给我破解的hash，以及md5，刚看他写了个公告，就决定用此文支持他一下，也是小菜文章，大牛莫笑。88~。