i春秋-在线挑战-我很简单，请不要欺负我-过程记录

转载

weixin_33858336 于 2016-10-01 22:50:54 发布 189 收藏
文章标签： shell
原文链接：http://blog.51cto.com/12125295/1858328

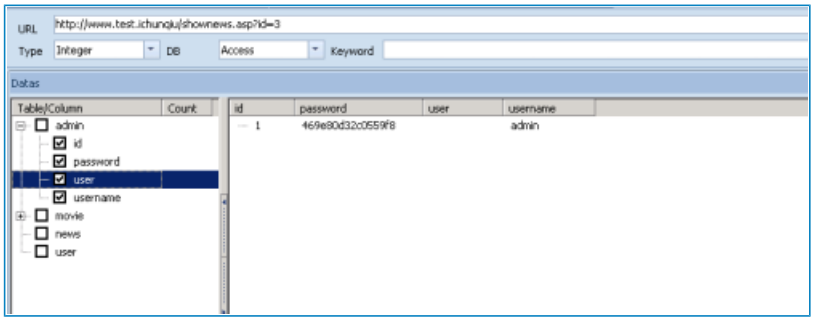
0x00 猜解目录

题目中实验工具已经给到了提示，要用御剑。所以直接直觉猜解到admin后台目录。

0x01 注入获取管理员密码

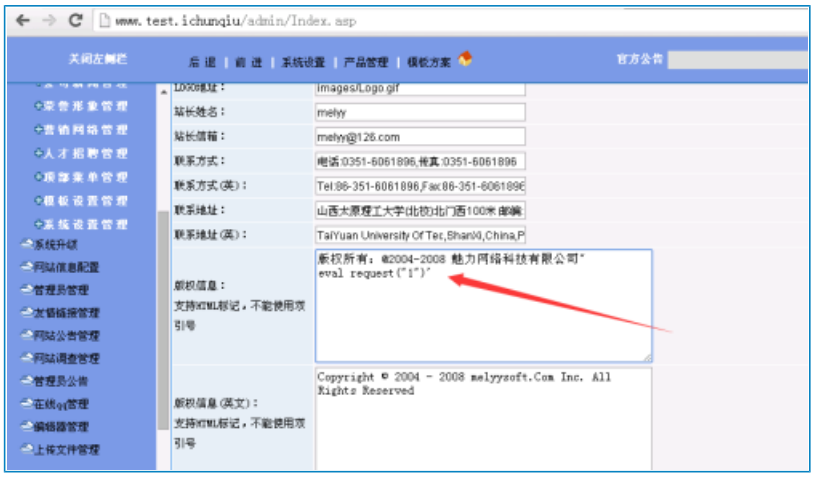
找到了后台，需要获取Shell一定是要在后台进行操作。所以用户名和密码基本可以肯定是注入得来。

在前台页面里找一个有参数的，放在pangolin里面操作一下，用户名和密码来了。MD5把密码解密：admin888



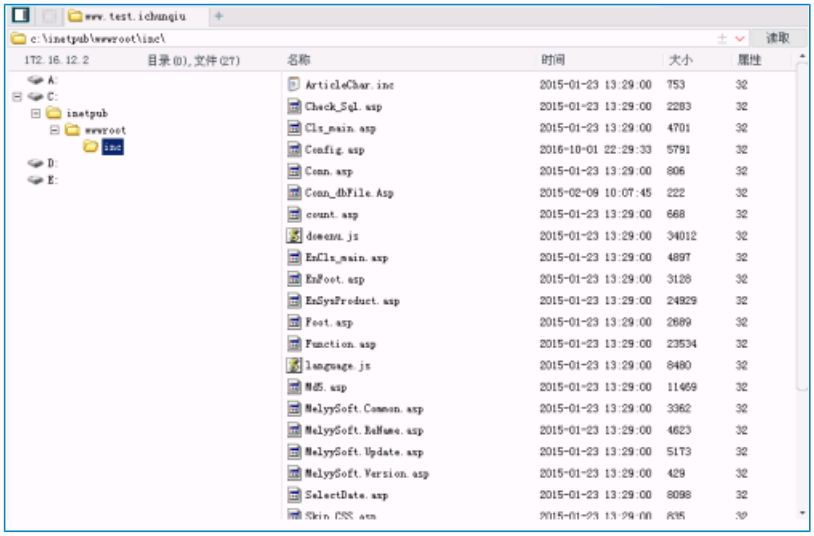
0x02 写配置文件GetShell

后台功能丰富，有数据库备份、有上传点、有上传文件类型限制设置。后台备份直接是不生效的，上传也是不成功的。经过提示得知，shell并不是直接上传的，而是在系统设置里面写配置文件得来的。



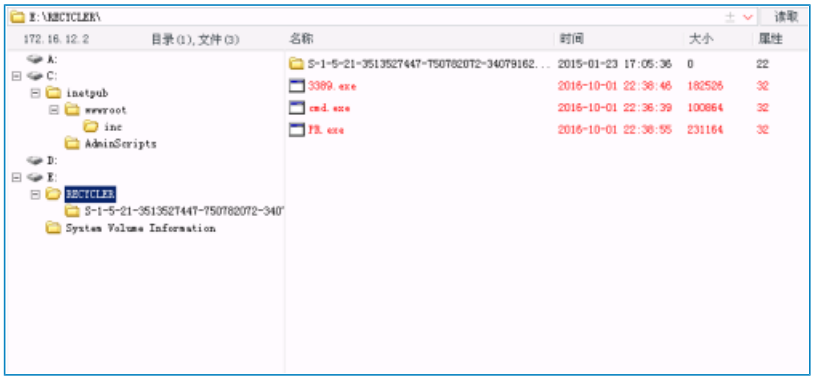
保存系统设置中的信息后，一句话***被写入到了inc/config.asp文件中。

使用菜刀即可进行连接。



0x03 上传提权文件

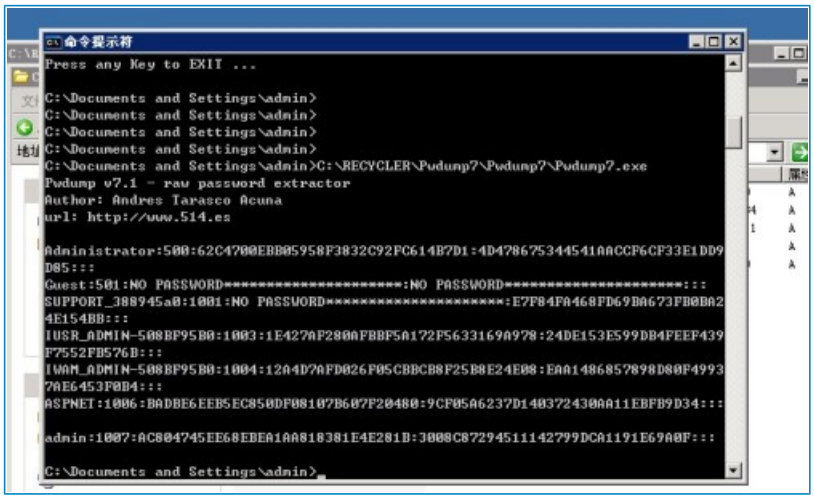
普通的目录下，没有写入的权限。找一个RECYCLER把提权用的文件上传。根据提示，把CMD、PR和3389上传上去。



完成上传后，查看一下基本信息。开始使用PR提权并运行3389来才打开远程端口并创建用于远程的管理员。

0x04 登录并上传破解程序

有很多工具可以上传，直接上传了pwdump7，运行获取LM。



0x05 破解得到管理员密码

转载于:https://blog.51cto.com/12125295/1858328