i春秋题库之真的很简单

原创

qq_38060946 于 2020-08-19 09:57:46 发布 989 收藏

分类专栏： i春秋题库 入门题 文章标签： 信息安全

i春秋题库 同时被 2 个专栏收录

1 篇文章 0 订阅

订阅专栏

入门题

1 篇文章 0 订阅

订阅专栏

题目：真的很简单

第一次模拟渗透测试记录

参考目录：[1]https://blog.csdn.net/qq_35582562/article/details/80956338
[2]https://blog.csdn.net/qq_19980431/article/details/101035672;
[3]https://blog.csdn.net/wangyi_lin/article/details/9286937
[4]https://bbs.ichunqiu.com/thread-35338-1-1.html
这是我第一次进行模拟渗透测试，尝试把理论知识转换为实践经验。并在此过程中进行更加深入的学习。

第一题：获取网站管理员的密码

我在进行实验的时候，实验提示已经挂掉了，在网上找来了其他前辈的经验作参考。
根据左侧的提示第一步可以使用dedeCMS工具来进行网站管理员密码的爆破。
从网站的底部标签可以看到，这个网站应该是用的织梦的CMS来搭建的。

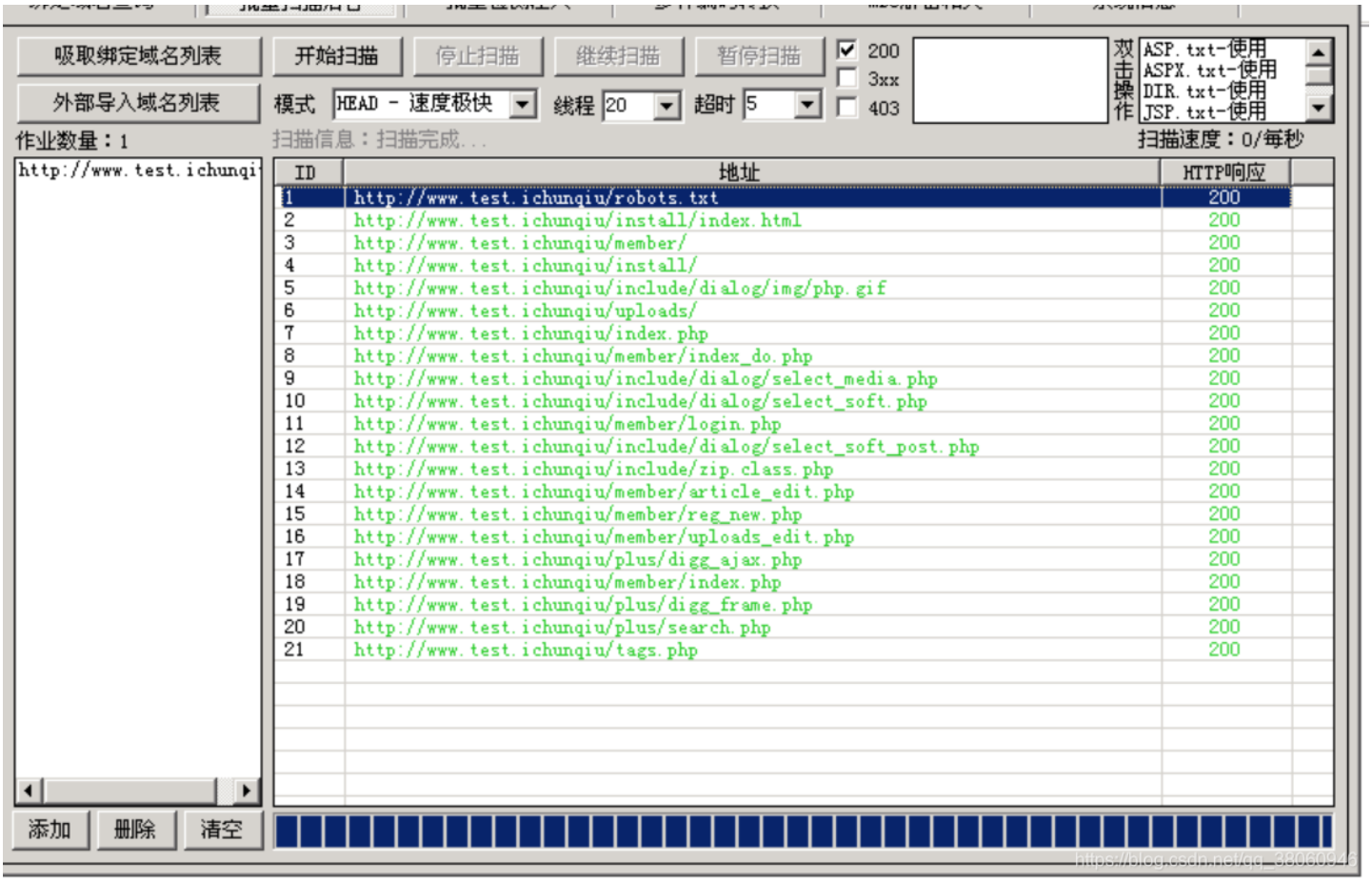
下载dedeCMS的地址是'**file.ichunqiu.com/49ba59ab**'
下载之后直接输入目标网站的域名就可以进行爆破了。

如上图，可以得到网站的管理员用户名为ichunqiu，密码为'**adab29e084ff095ce3eb**'从格式来看应该是加密后的密文。
在另一篇博客里看到，织梦的密码加解密的格式为：加密的时候DEDECMS的密码是32位MD5减去头5位，减去尾七位，得到20 MD5密码；
解密的时候需要前位减3后位减1，得到16位MD5。然后再去解密。这里推荐一个免费的MD5解密网站：https://www.somd5.com/

解密后得到管理员密码为：**only_system**

第二题：获取网站后台目录名

要获得后台目录名，我首先想到的是用御剑进行扫描



如上图，御剑扫描的都是字典中保存的常见的后台目录，并没有题目中网站的根目录。
在这里可以试一下去找网站所用CMS的已知漏洞中有没有可以获取到后台目录名的。
找到MySQL报错信息中可能含有后台地址
data/mysqli_error_trace.inc
可以尝试访问该文件，在返回的信息中可以看到网站的后台目录。

如上图返回来的报错信息中有目录名lichunqiul可以试一下能不能用来登录后台

测试之后出现了后台登录的页面那这应该就是后台页面了，用第一题处获取的用户名和密码来进行登录

第三题：获取管理员桌面flag信息

在登录之后，想获得管理员桌面的flag信息，首先要可以看到管理员的系统目录，在网上找的方法中，大家普遍用植入后台的方法，用一句话代码上传到服务器然后用菜刀之类的三十远程连接。
要想上传代码需要谢盖系统的上传限制，可以在登录后的系统中修改
在系统-基本参数-附件设置中，修改允许上传的文件类型添加php类型
然后打开ichunqiu的工具找到中国菜刀，打开文件夹中的一句话，创建一个txt文件，把php代码写入其中保存，然后上传（记得修改文件后缀名为php）
然后在附件管理中找到上传的文件，复制它的地址，打开菜刀右键空白处添加，地址就是文件地址，密码是一句话代码中的中括号内的部分。
添加后双击，出现以下页面则成功了

之后找到桌面文件夹的flag文件，但是打开之后是空的

之后找到桌面文件夹的flag文件，但是打开之后是空的

据前辈的经验来看，是需要进行提权，在菜刀打开终端页面进入到桌面文件夹，更改系统用户对flag文件的权限（用cacls命令），修改后得到flag。