# SHA也难逃我手：巧用Cain破解MYSQL数据库密码

前言：MYSQL数据库用户密码跟其它数据库用户密码一样，在应用系统代码中都是以明文出现的，在获取文件读取权限后即可直接从数据库连接文件中读取，例如asp代码中的conn.asp数据库连接文件，在该文件中一般都包含有数据库类型，物理位置，用户名和密码等信息；而在MYSQL中即使获取了某一个用户的数据库用户（root用户除外）的密码，也仅仅只能操作某一个用户的数据库中的数据。

在实际攻防过程中，在获取Webshell的情况下，是可以直下载MYSQL数据库中保留用户的user.MYD文件，该文件中保存的是MYSQL数据库中所有用户对应的数据库密码，只要能够破解这些密码那么就可以正大光明的操作这些数据，虽然网上有很多修改MYSQL数据库用户密码的方法，却不可取，因为修改用户密码的事情很容易被人发现！

研究MYSQL数据库的加解密方式，在网络攻防过程中具有重要的意义；试想一旦获取了网站一定的权限后，如果能够获取MYSQL中保存用户数据，通过解密后，即可通过正常途径来访问数据库；一方面可以直接操作数据库中的数据，另一方面可以用来提升权限。通过在网络上查找资料，目前关于破解MYSQL方面的研究不多，本文算是抛砖引玉，虽然效果不是特别好，但也算是对破解MYSQL数据库用户密码的一种探讨和尝试。

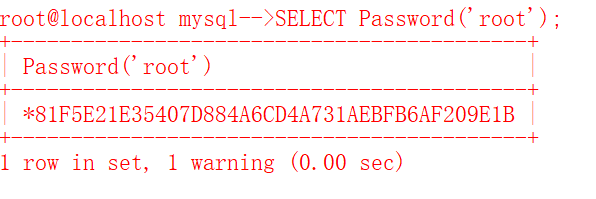
By:北冥

# 破解过程

# （第一）确定MYSQL加密方式

MYSQL数据库的认证密码有两种方式，MYSQL 4.1版本之前是MYSQL323加密，MYSQL 4.1和之后的版本都是MYSQLSHA1加密，MYSQL数据库中自带Old\_Password（str）和Password（str）函数,它们均可以在MYSQL数据库里进行查询，前者是MYSQL323加密，后者是MYSQLSHA1方式加密。Mysql5.7版本后采用的是**MYSQLSHA1方式加密**

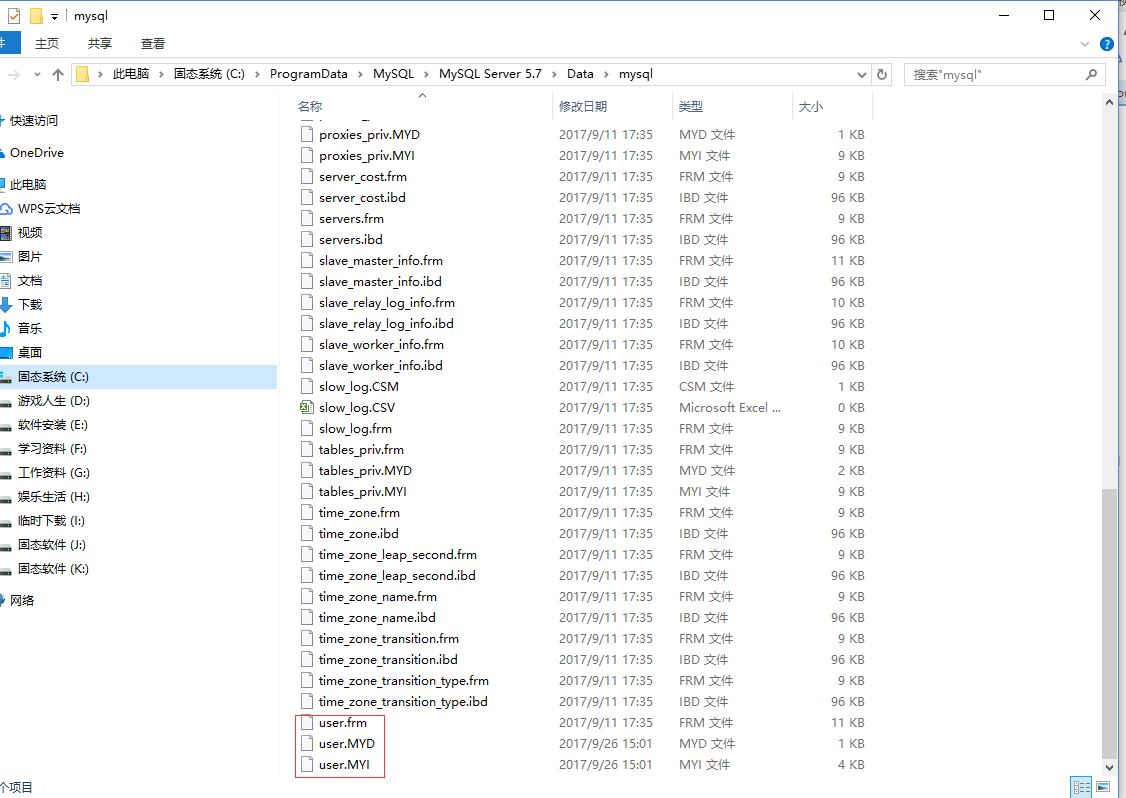
**以MYSQLSHA1方式加密**



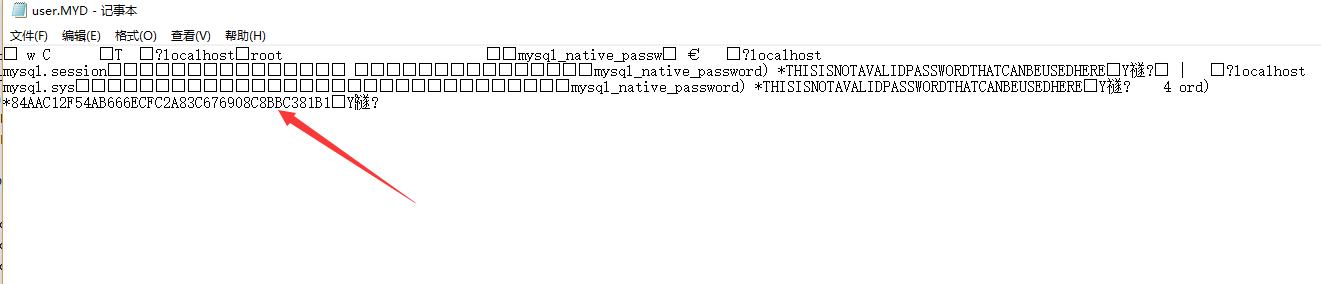
查询结果MYSQLSHA1 = \*81F5E21E35407D884A6CD4A731AEBFB6AF209E1B    执行结果如图所示，MYSQLSHA1中生存的是41位字符串，其中\*是不加入实际的密码运算中，通过观察在很多用户中都携带了“\*”，在实际破解过程中去掉“\*”，也就是说MYSQLSHA1加密的密码的实际位数是40位。

# （第二）寻找MYSQL数据库用户密码文件

在新版本的MYSQL5.7数据库中所有设置默认都保存在“C:\ProgramData\MySQL\MySQL Server 5.7\Data”中，data目录下有个叫mysql的文件夹，如图所示，有关用户一共有三个文件即user.frm、user.MYD和user.MYI，MYSQL数据库用户密码都保存在user.MYD文件中，包括root用户和其他用户的密码。



以文本方式查看user.MYD文件可以找到加密过的密文



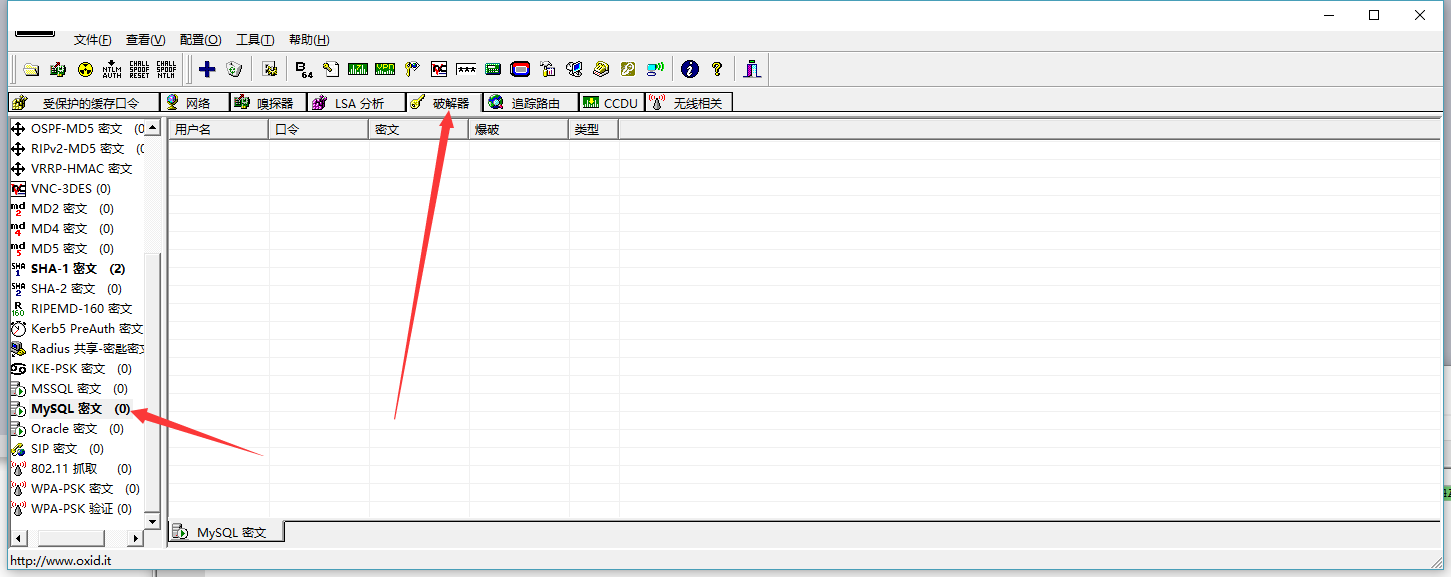
可以得到密文：84AAC12F54AB666ECFC2A83C676908C8BBC381B1

# （第三）用****Cain软件****对密文进行解密

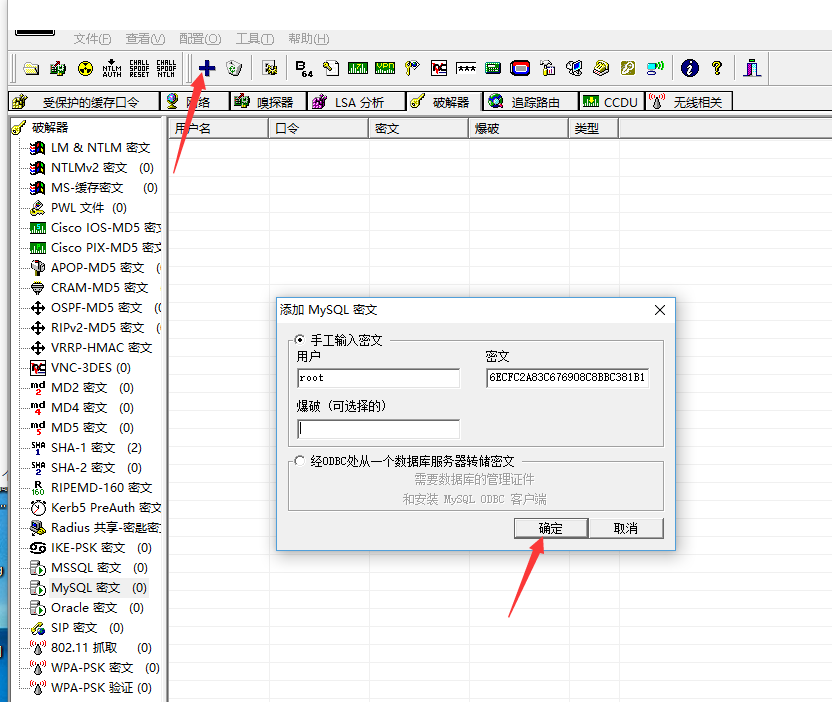
软件下载地址：http://15563.url.tudown.com/xiaz/cain@134\_21400.exe

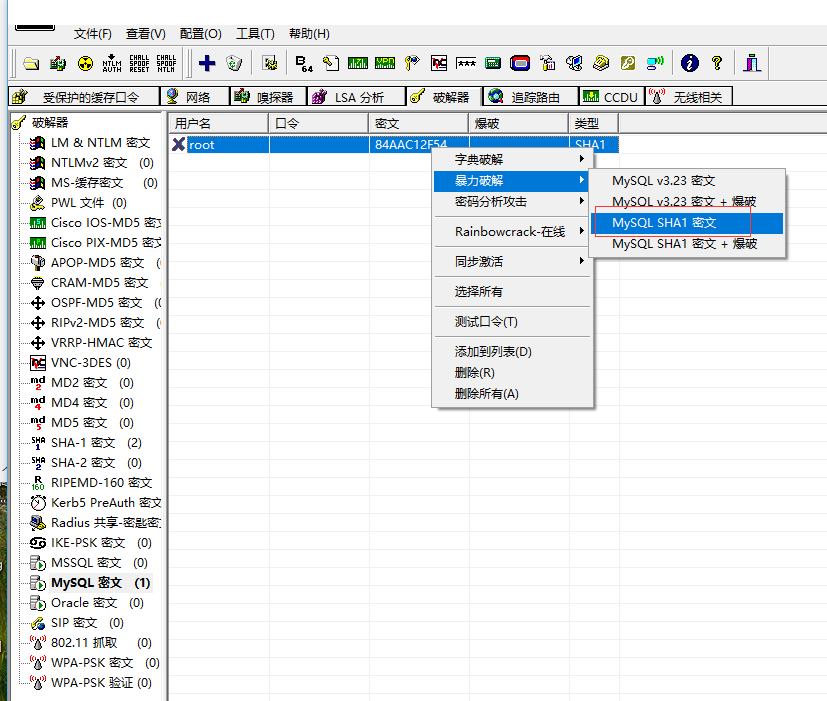
复制第二步得到的密文：84AAC12F54AB666ECFC2A83C676908C8BBC381B1

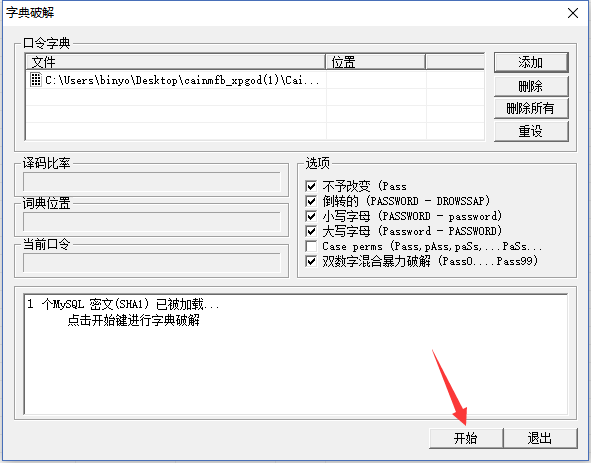
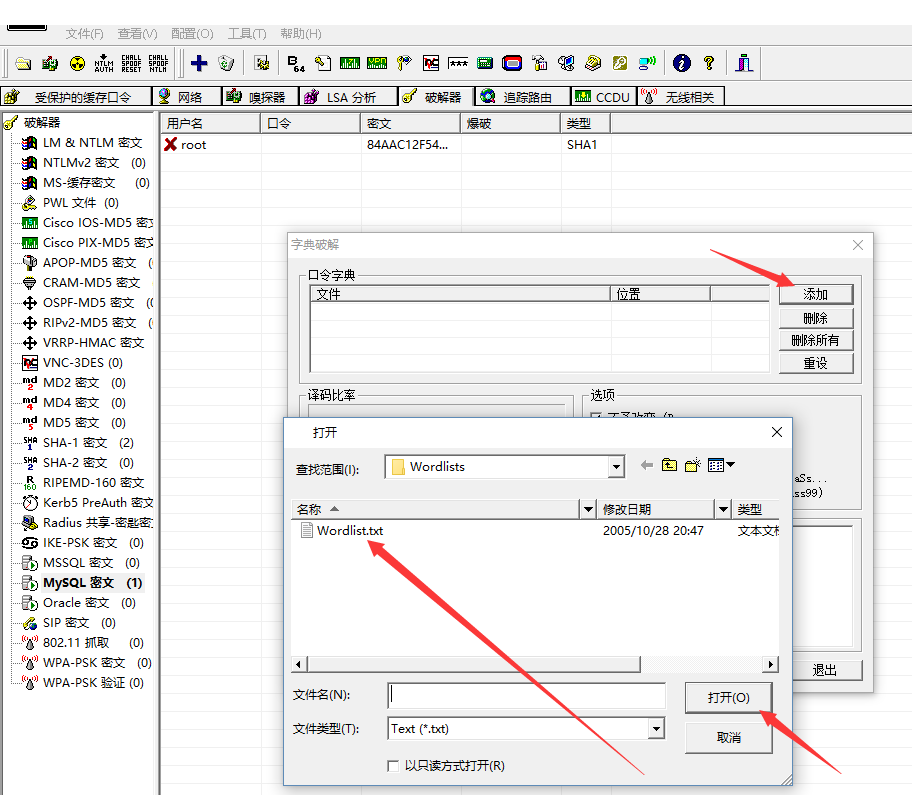
然后打开软件切换到破解器界面，右边功能框选择mysql密文如图所示

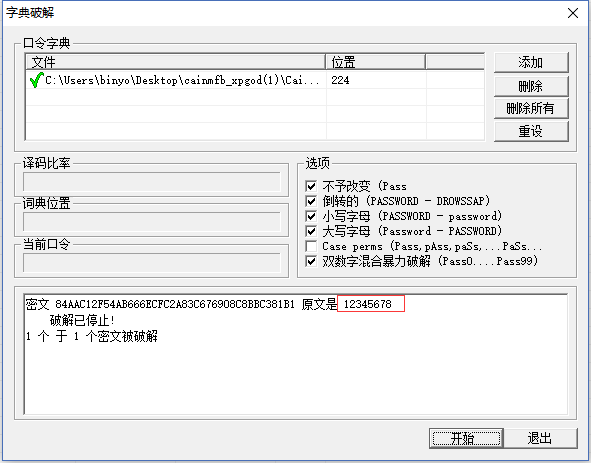
打开软件

添加密文









总结：

通过使用cain来破解MYSQL密码，算是一种较好的尝试，只要使用字典工具生成一些具有一定强度的字典，对于设计不太复杂的MYSQL密码，破解还是较为容易的。