MySQL 安全加固实验

一【实验目标】

- 了解 MySQL 数据库几种常见威胁
- 掌握几种常见的安全加固方式

二【实验环境】

- Windows 10

三【实验原理】

为了保证数据库的安全，一般需要对数据库进行安全加固操作。Mysql 数据库安全加固属主要涉及用户、权限、日志、远程等方面。常用的安全加固方法有以下几种。

第一种：删除空用户。某些版本的 MySQL 系统会默认创建一个无用户名无密码的匿名用户（Anonymous Account），也叫空用户。这使得数据库服务器存在无需密码便可以登录的风险。为消除此类安全隐患，应当删除空用户。

第二种：防止文件注入。mysql 对本地文件的存取主要通过 Load DATA LOCAL INFILE 等 SQL 语句实现，因此能够通过禁用该功能来防止黑客通过 SQL 注入的方式获取系统核心文件。

第三：日志输出。Mysql 默认有 error 日志文件输出，默认在 data 文件夹。若想获得更高的安全性，则可以增加查询日志、二进制日志、更新日志和慢查询日志文件输出。

四【实验步骤】

1、输入密码【Admin123456】，登录系统。如图 1 所示。

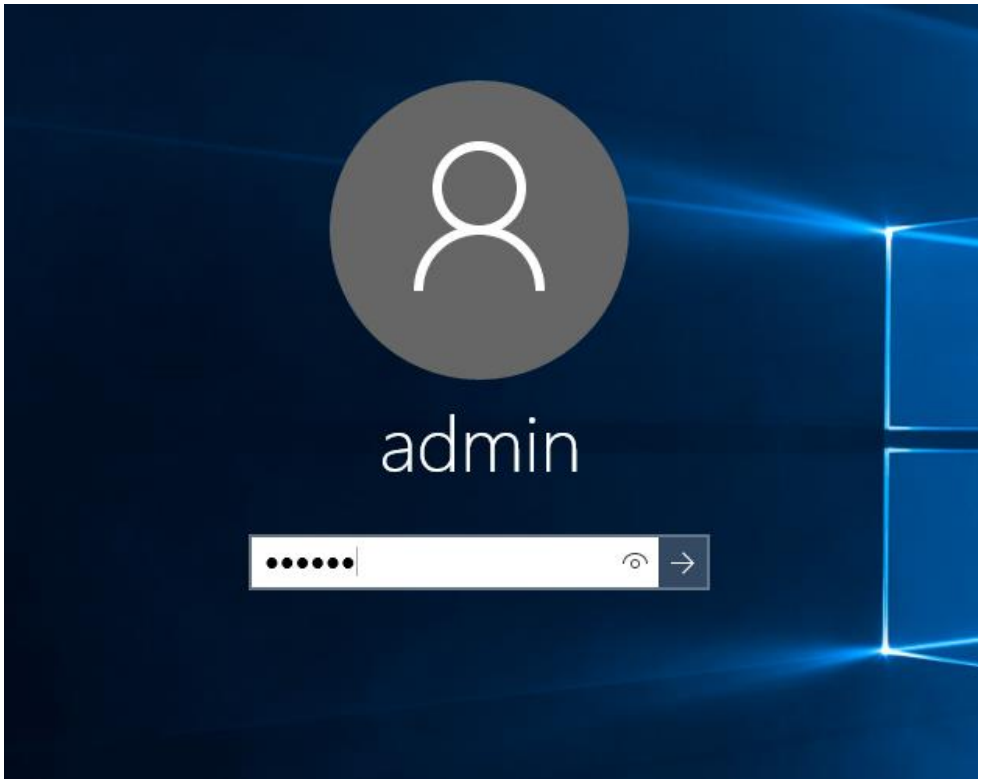


图 1

2、单击屏幕左下角的【开始】图标。如图 2 所示

图 2

3、在搜索框中搜索 cmd，选中 cmd，右键以管理员身份运行。如图 3 所示

图 3

4、成功打开命令行。如图 4 所示

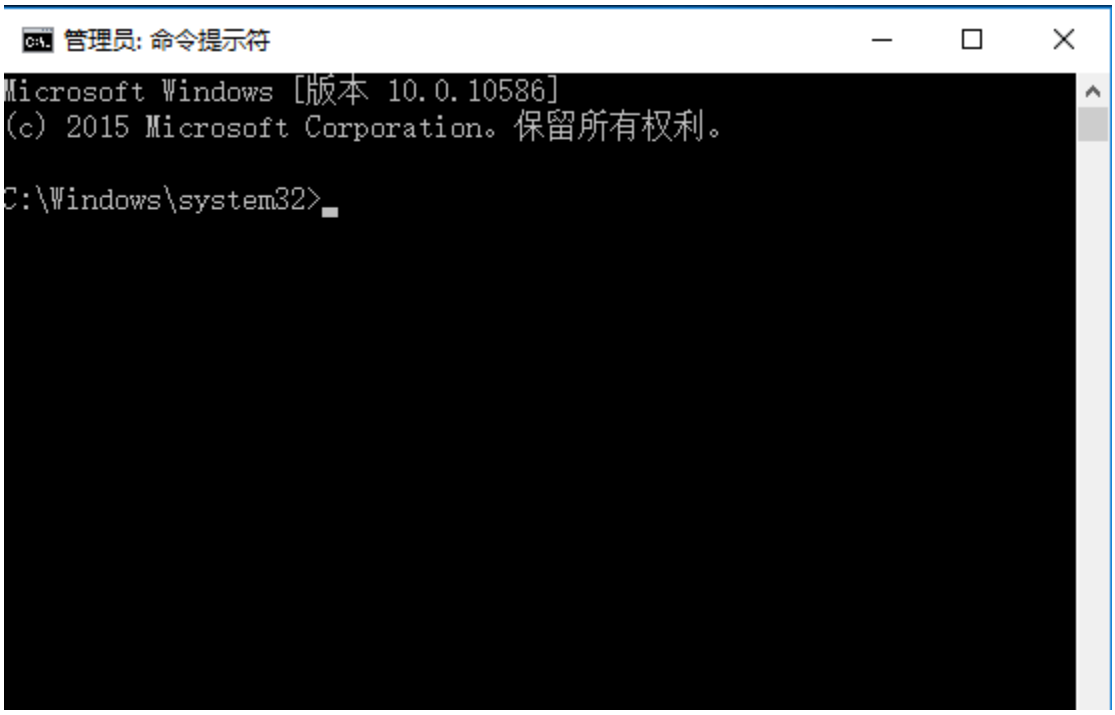


图 4

5、输入命令“net start mysql”开启 MySql 数据库服务，如图 5 所示

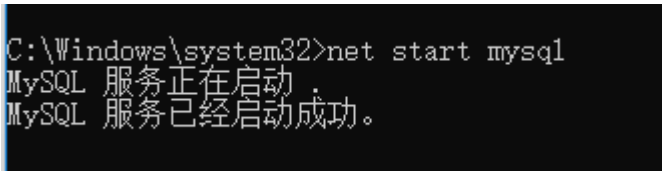


图 5

6、第一种常见的安全加固方式是删除空用户。在 MySql 数据库服务启动的情况下，可以直接使用输入命令 mysql -u root -p 并输入密码 111，使用 root 账号连接到数据库。连接成功界面如图 6 所示

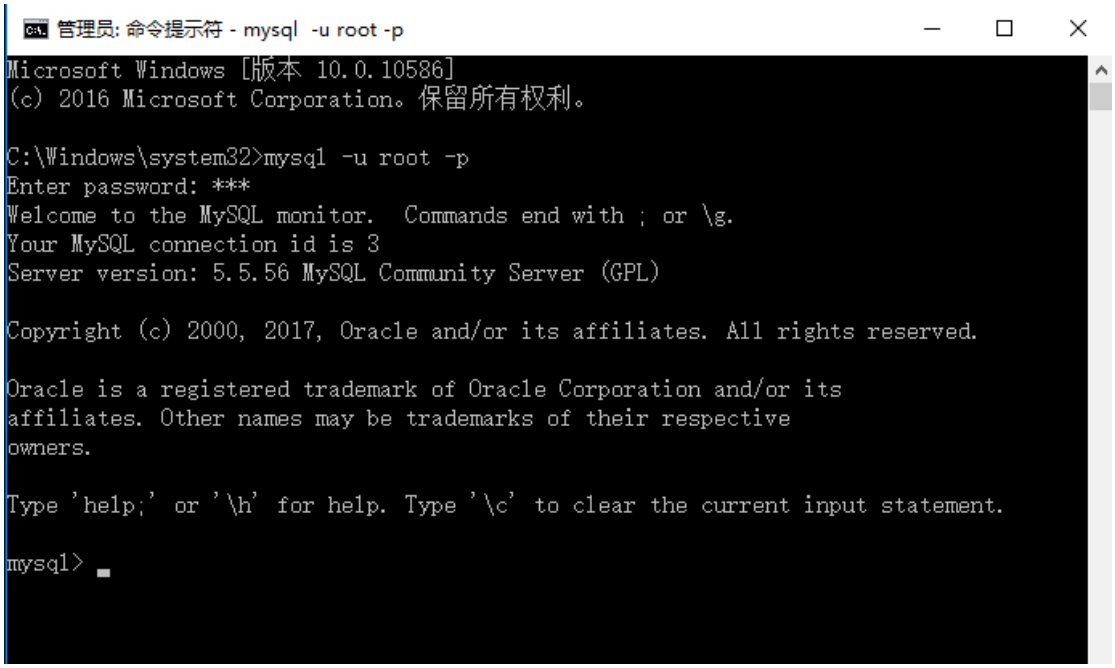


图 6

7、未删除空用户之前，输入命令“select user,host from mysql.user;”查看系统中是否有空用户，如图 7 所示.

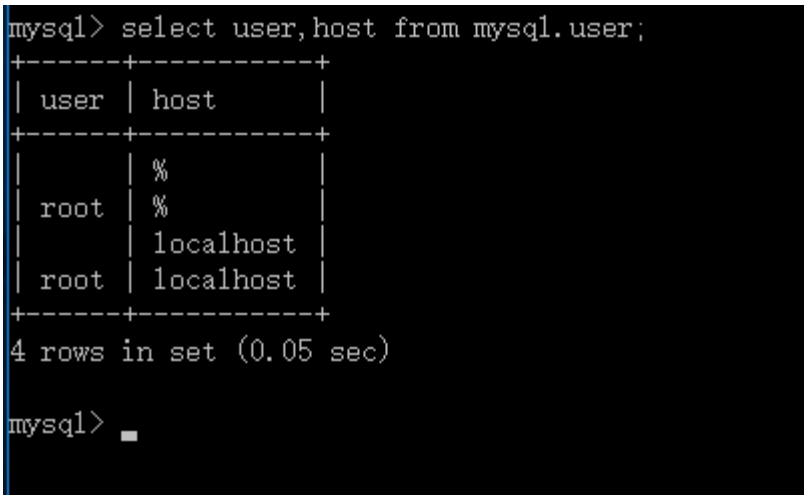


图 7

8、执行下图所示命令，删除空用户。如图 8 所示

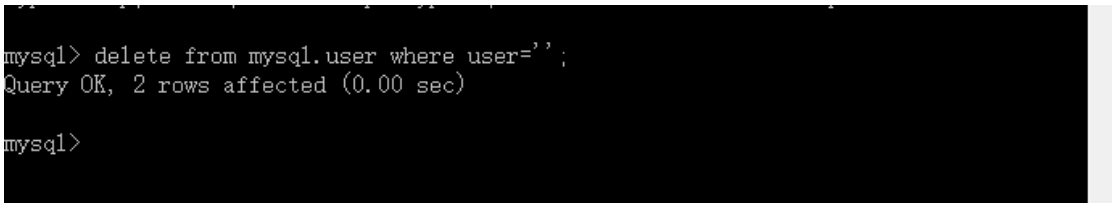


图 8

9、第二种常见的安全防固方式是防止文件注入。MySQL 默认允许文件注入。打开待注入文件 C:/code/test.txt。如图 9 所示。

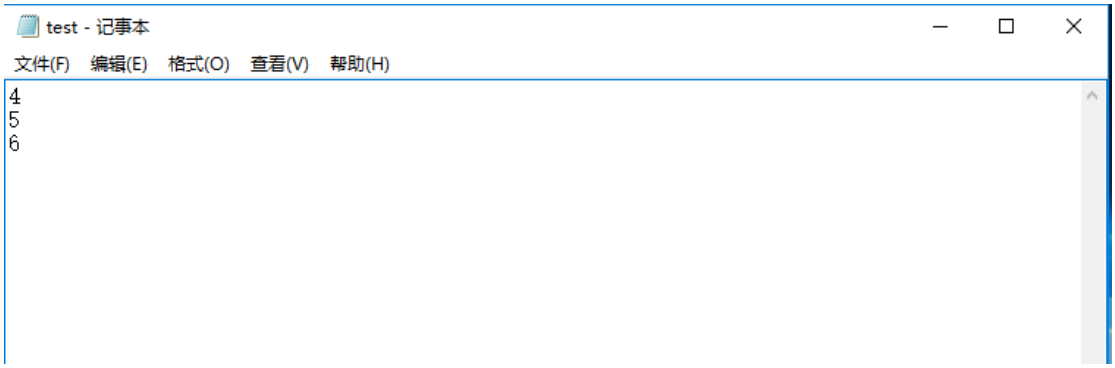
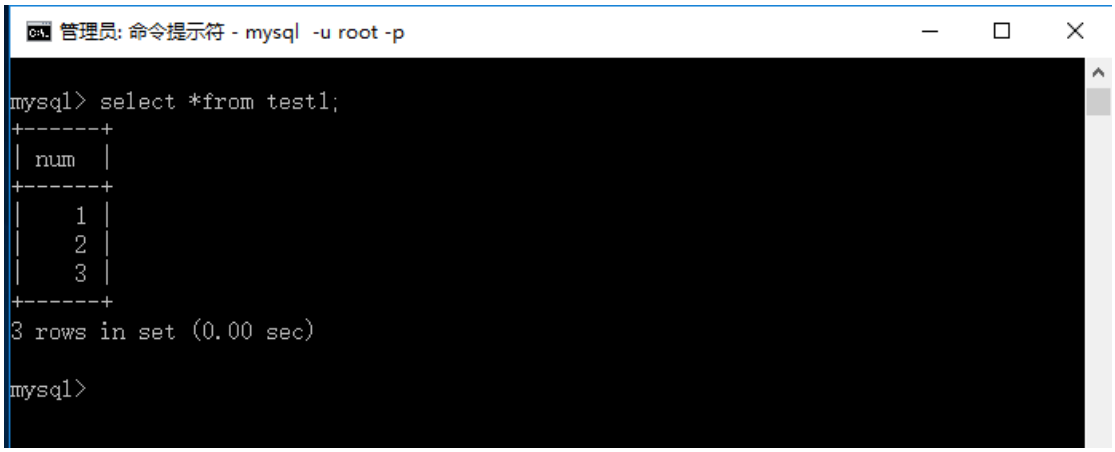


图 9

10、将文件注入到数据库 test 的 test1 表中。注入前 test1 表的内容，如图 10 所示。



图,10

11、输入命令 LOAD DATA LOCAL INFILE 'C:/code/test.txt' INTO TABLE test1;。将文件内容注入到表 test1 中。如图 11 所示。

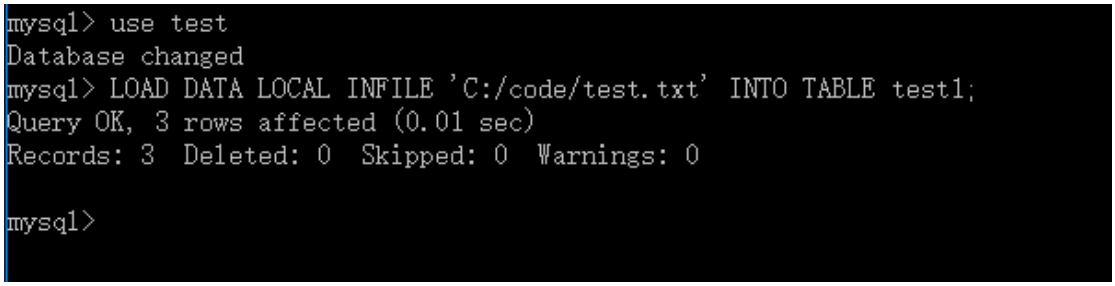


图 11

12、再次查看表 test1 中的内容，发现注入成功。如图 12 所示。

```
mysql> select *from test1;
+------+
| num  |
+------+
|    1 |
|    2 |
|    3 |
|    4 |
|    5 |
|    6 |
+------+
6 rows in set (0.00 sec)

mysql>
```

图 12

13、文件注入会给数据库带来较大威胁，为此在非必要时应当关闭文件注入功能。首先点击桌面左下角的【文件夹】图标。如图 13 所示

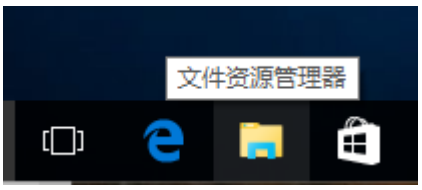


图 13

14、在弹出的窗口中点击【本地磁盘（C:）】选项，在界面右侧左键双击“Tools”文件夹（以实际设备 MySQL 安装位置为准）。如图 14 所示。

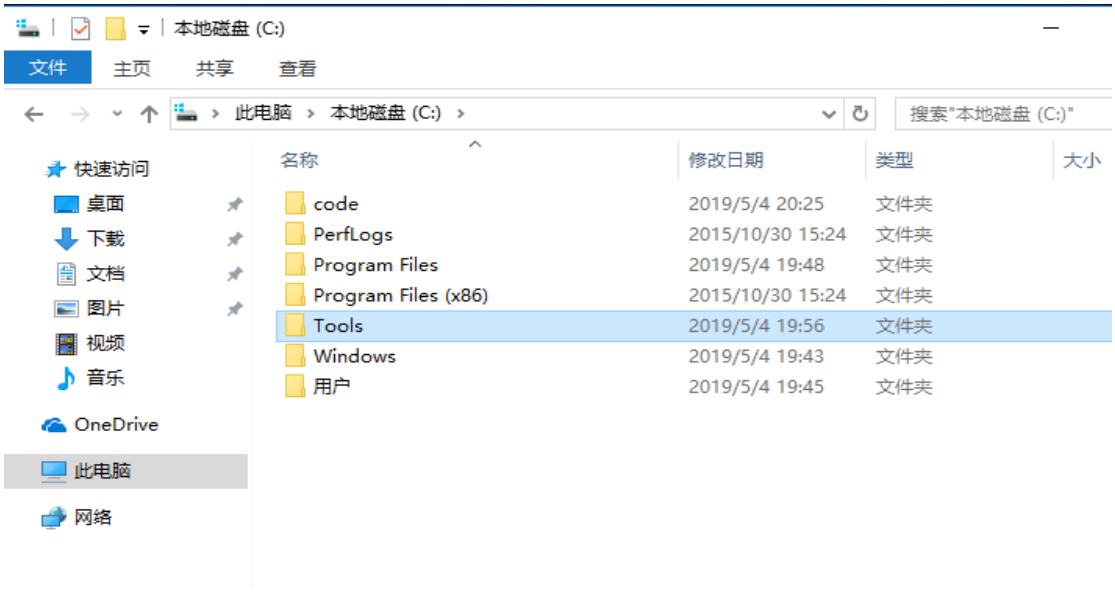


图 14

15、进入 Tools 文件夹后，双击 MySQL 文件夹，再双击 MySQL Server 5.5 文件夹，进入 MySQL 目录。如图 15 所示。

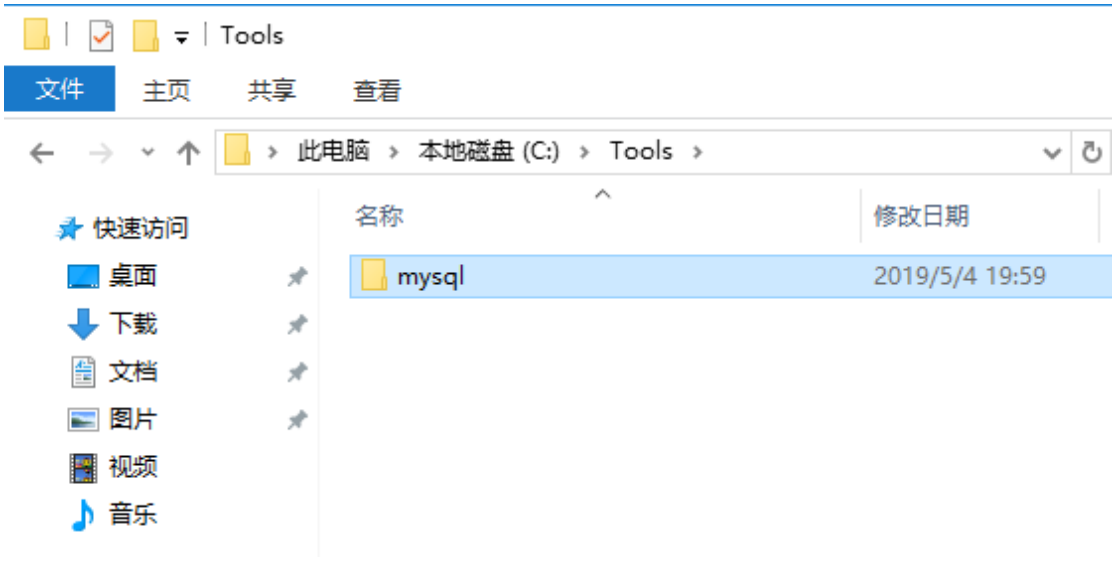


图 15

16、找到文件名为“my.ini”的配置文件，双击打开。如图 16 所示。

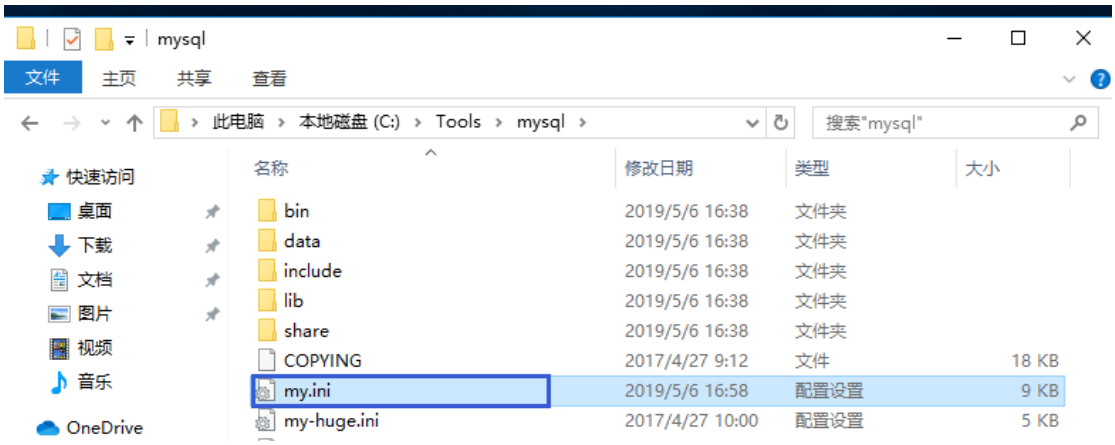


图 16

17、在配置文件末尾加上 local_infile=0 表示不允许文件注入，保存。如图 17 所示。

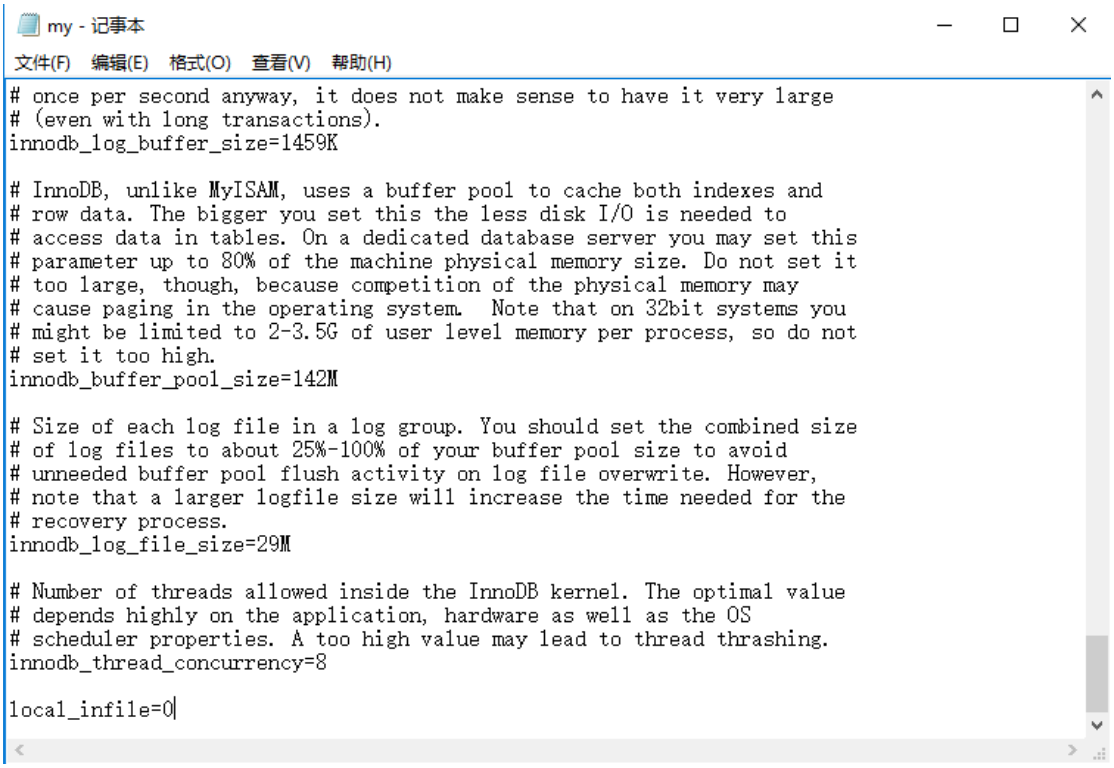


图 17

18、重启 MySQL 服务，如图 18 所示

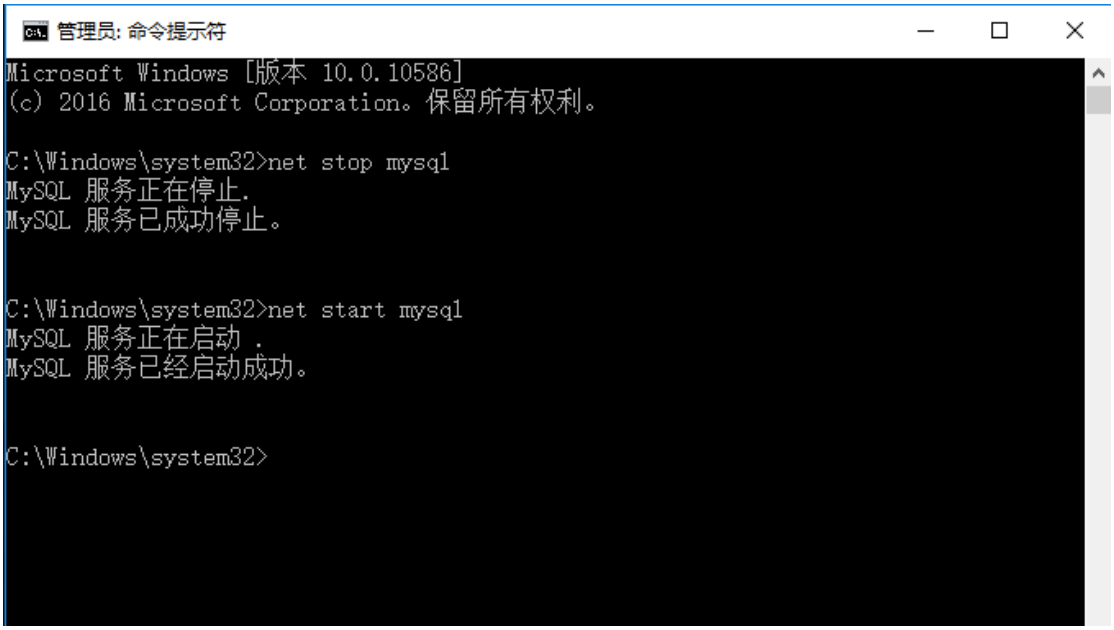


图 18

19、若使用命令行重启 MySql 失败，使用“Windows+R”组合键，在弹出框中输入“services.msc”命令，如图 19 所示。

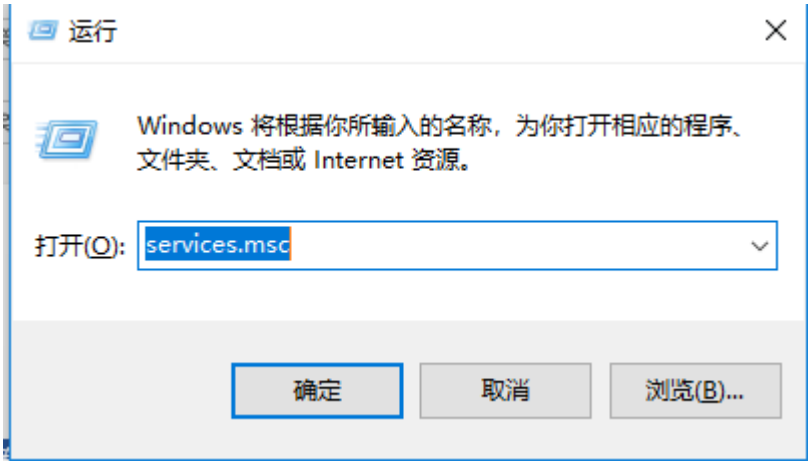


图 19

20、回车后，在弹出的服务窗口选中 MySQL 服务，鼠标右键，选择“重新启动”该服务，如图 20 所示。

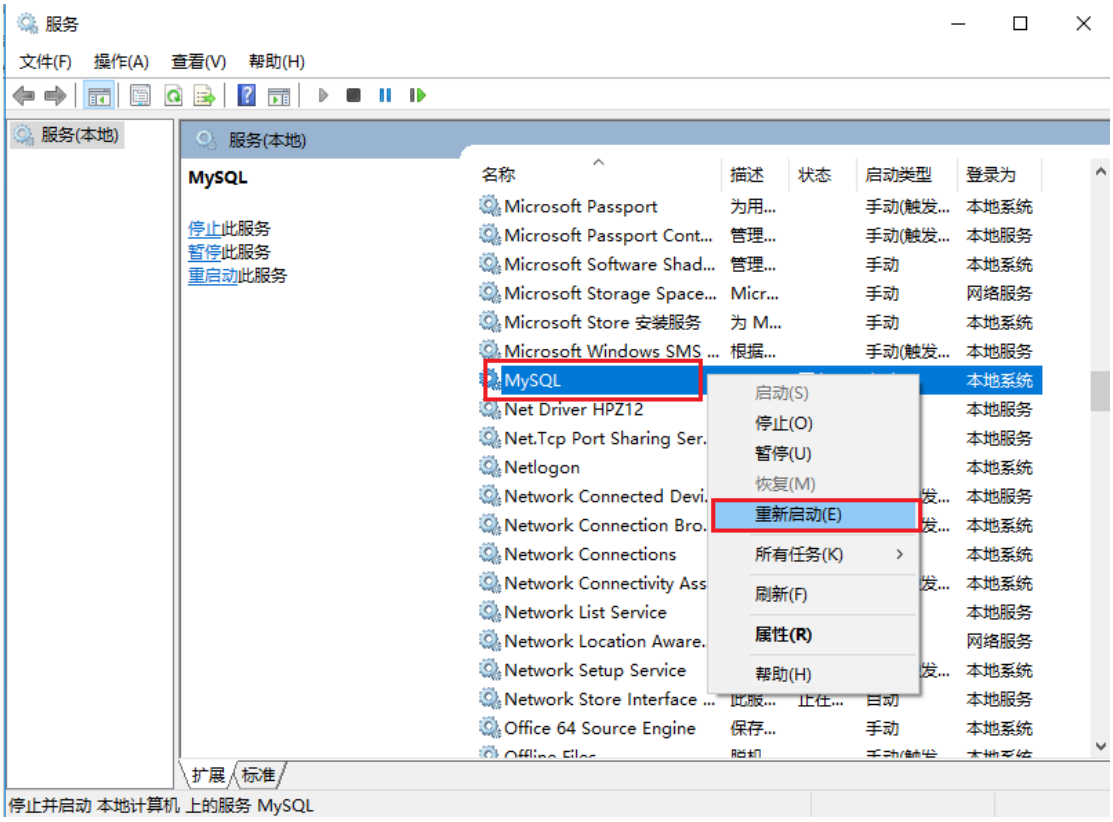


图 20

21、再次执行文件注入操作，执行失败，成功禁止了文件注入操作。如图 21 所示。

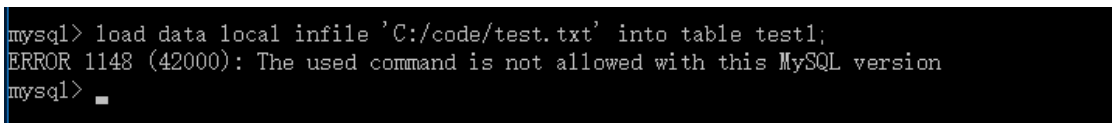


图 21

22、第三种常见的安全防固方式是日志输出。在第 MySQL 安装目录下，找到 data 文件夹，双击打开，本实验中安装目录为“C:\Tools\mysql”。如图 22 所示。

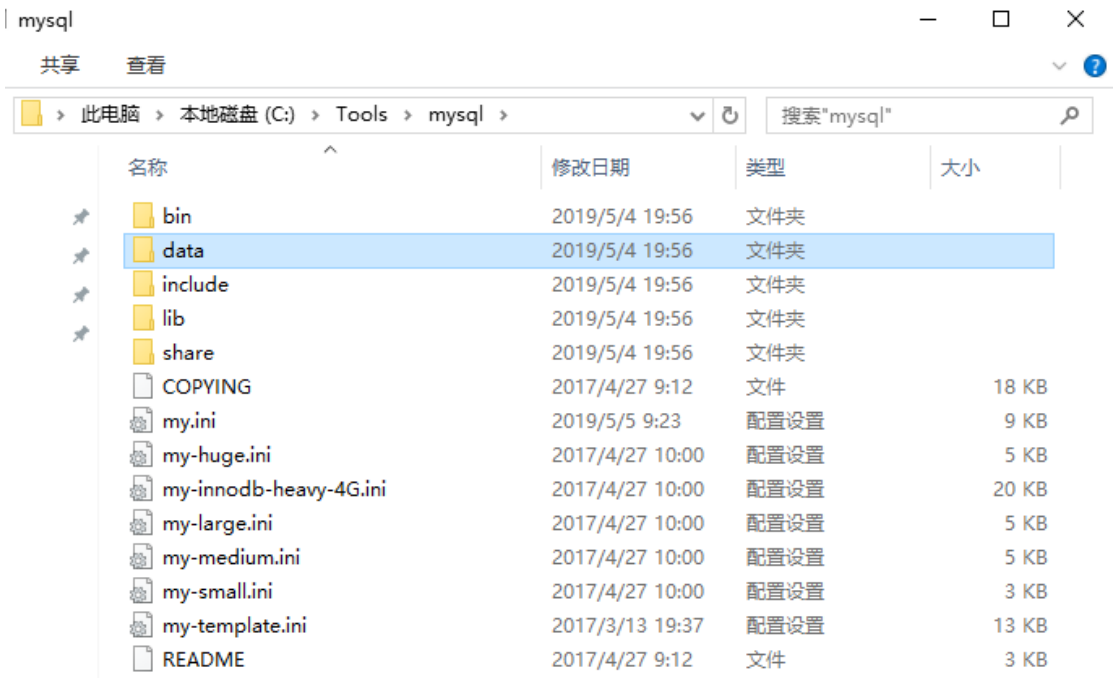


图 22

23、打开 data 文件后，单击地址栏。如图 23 所示。

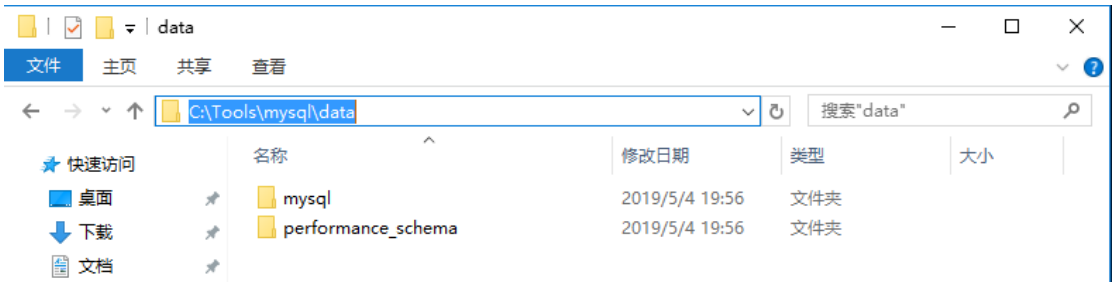


图 23

24、右击鼠标，选择复制，将 data 的位置进行复制。如图 24 所示。

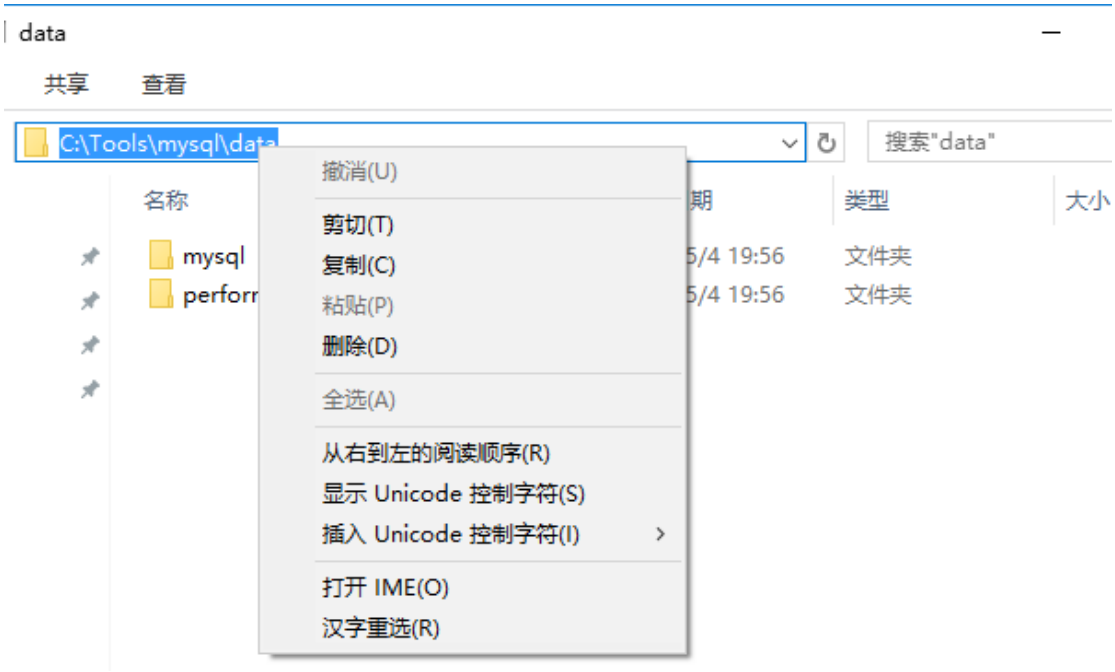


图 24

25、单击左箭头按钮，返回上一级目录。如图 25 所示。

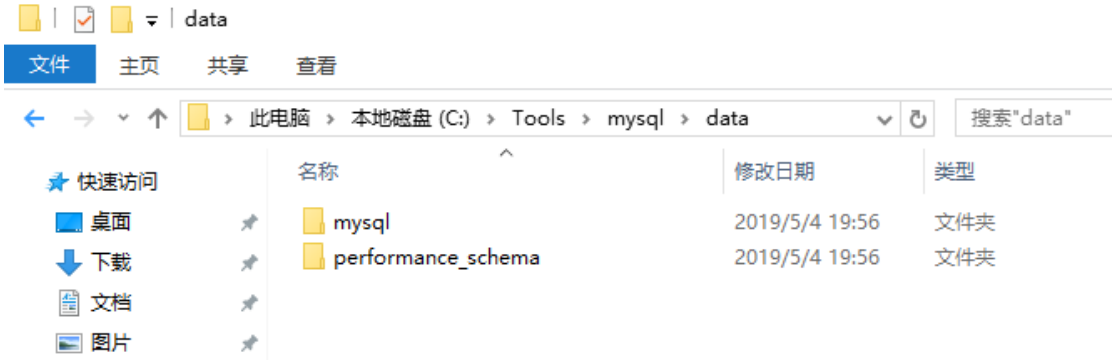


图 25

26、找到文件名为“my.ini”的配置文件，双击打开。如图 26 所示。

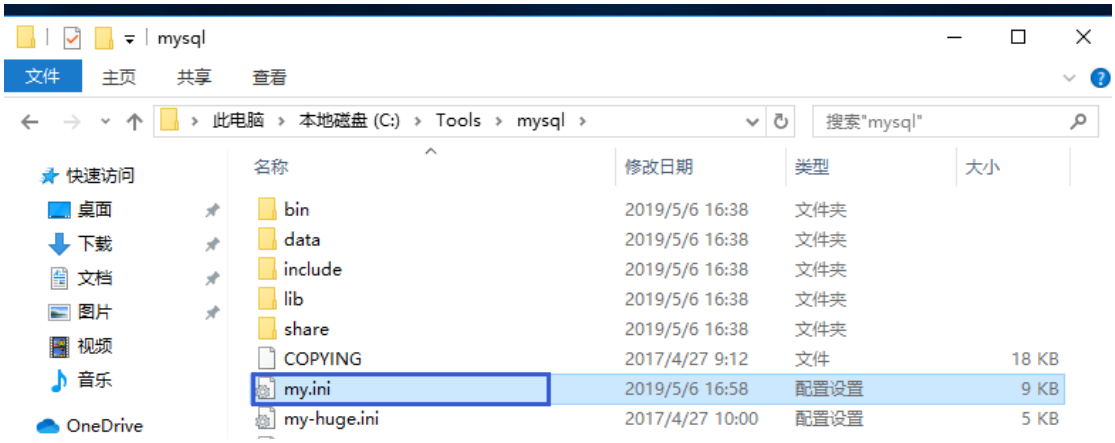


图 26

27、在文件底部添上如下内容，使 MySQL 新增了日志输出。（目录地址即为复制的 data 目录地址，注意：输入地址时请使用“/”隔开每一级目录）。log:查询日志;log-error：错误日志,log-bin:二进制日志;log-slow-queries：慢查询日志。如图 27 所示。

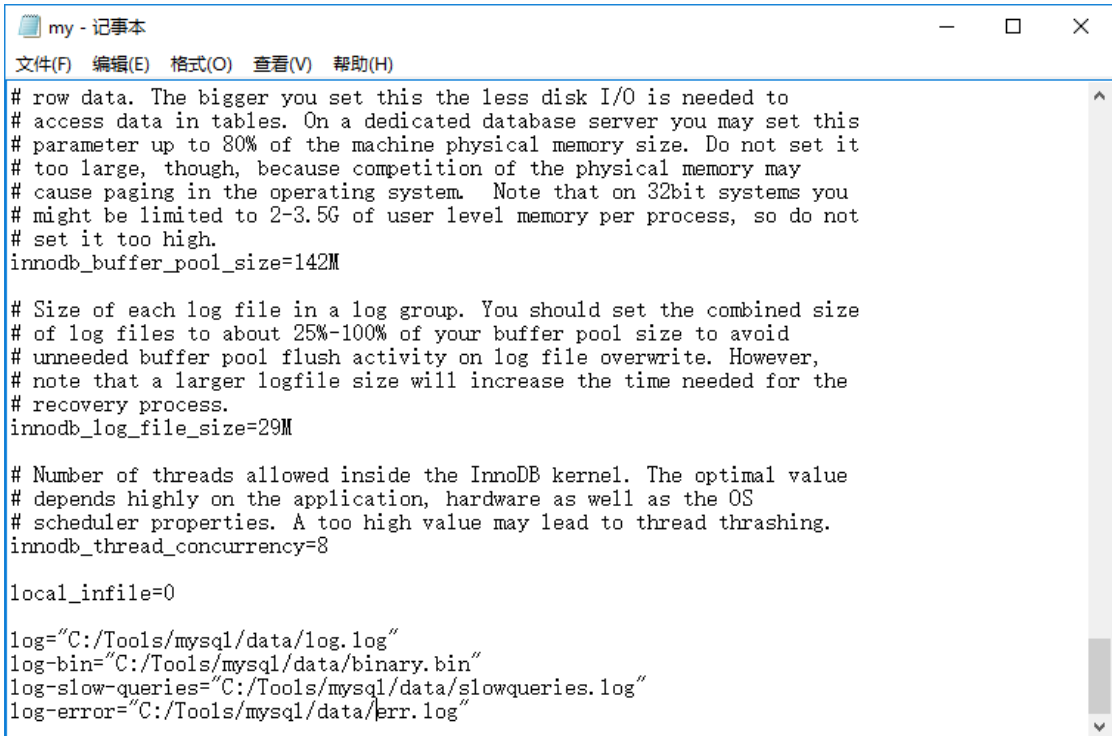


图 27

28、修改配置文件后需要重启 MySQL 服务。先关闭 MySQL。如图 28 所示。

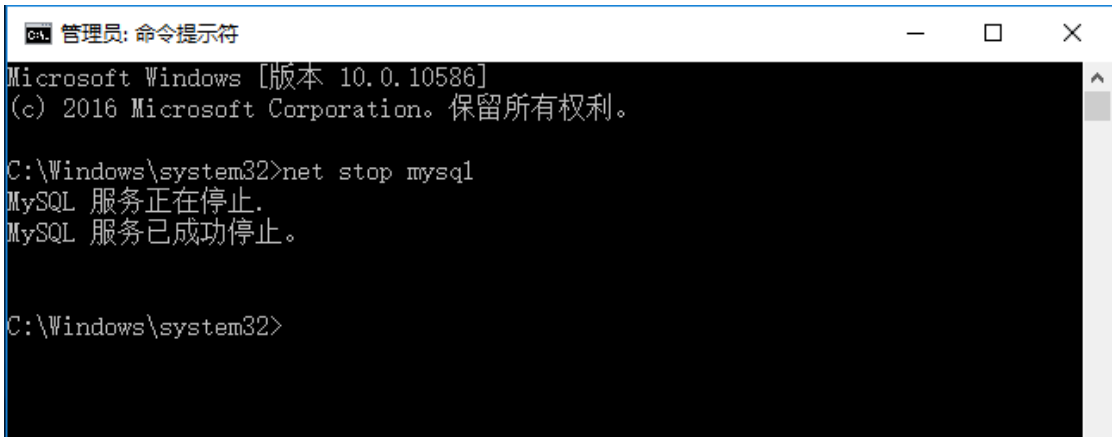


图 28

29、再开启 MySQL 服务。如图 29 所示。

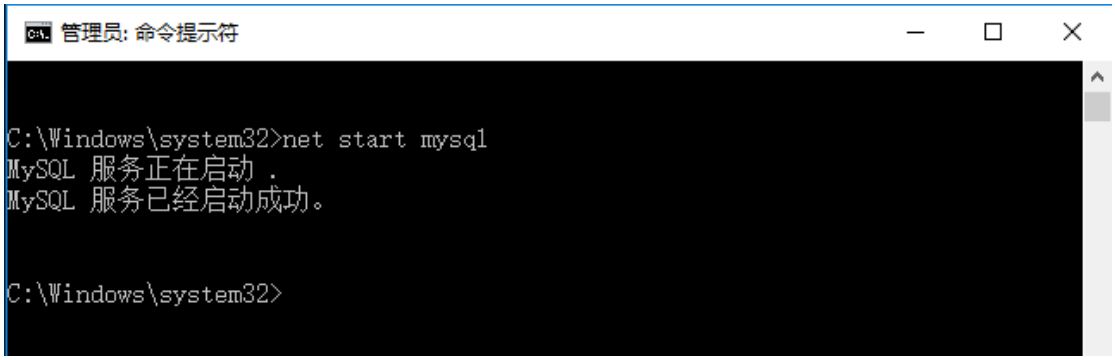


图 29

30、重新启动 MySQL 后打开第 17 步中的 data 文件夹，发现多了四个文件，这四个文件就是之前设置的日志文件。如图 30 所示。

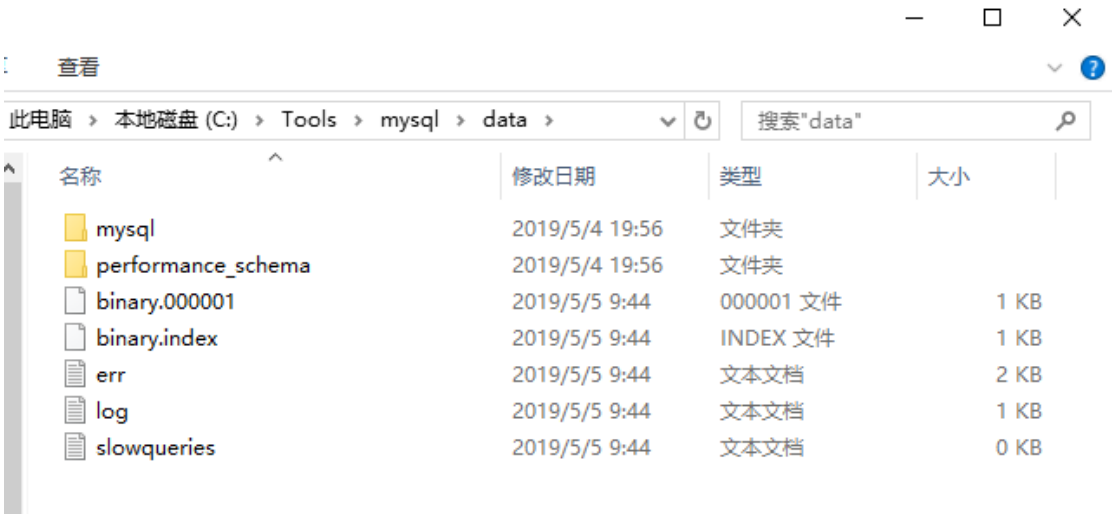


图 30

五【实验思考】

- 如何通过禁止远程访问的方式实现安全加固？