

“网络安全综合实验（I）”实验报告

**题目： 数据库安全基础实验**

院 系 网络空间学院

专业班级 信安1901班

姓 名 李欣宇

学 号 U201911658

日 期 2020 年 12 月

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 评分表 | 数据库安全基础实验报告评分  （50分） | | | | 完成  （50分） | 成绩 | |
| 评分 项目 | 过程 | 分析与小结 | 撰写 | 创新 | 完成任务 | 合计 | 教师 |
| 分值 | 20 | 20 | 5 | 5 | 50 | 100 | 签名 |
| 评分 |  |  |  |  |  |  |  |

报告要求及评分规则

1.请按照模板给出的格式，包括行距、字体、段落格式等，完成报告；

2.报告封面保持一致(如实填写基本信息及完成日期)；

3.实验报告内容应包括：封面、评分规则、实验过程记录、实验问题分析与总结、参考文献及资料列表；

4提交：电子材料应包括本实验电子版（doc）、实验参考文献资料的电子资源文件（pdf）。

5.主要考察能力： 实验动手能力、问题分析与归纳能力、文档规范撰写能力、创新能力；

6.其他要求：可按各指导老师要求的时间和提交方式提交；每次课实验报告可以单独提交；如果需要最终纸质报告的，可去掉模板中说明文字（斜体）之后，双面打印；

7.总评分=课程每次实验分数之和/课程实验次数。

其中：

每次实验分=实验完成分（50分）+实验报告分（50分）-扣分+加分；

计算方法：

实验完成分=（完成任务数量/总任务数量）\*50；

实验报告分=以下1-4项合计；

1）过程（要求：实验过程完整、清晰）(满分20)（优秀：18+ 良好：16+ 一般：14+）；

2）问题分析与小结（要求：有条理、细致）（满分20）（优秀：18+ 良好：16+ 一般14+）；

3）撰写（要求：语句通畅、格式规范）（满分5）（优秀：4+ 良好：3+ 一般：2+）；

4）创新（要求：见解独到、有创意）（满分5）（优秀：4+ 良好：3+ 一般：2+）；

扣分=报告迟交天数\*2分（满分10分）  （发现雷同抄袭的内容，该次实验不得分）；

加分=搜集整理与实验相关的学习资料作为附件，资料能帮助同学更好掌握相关知识的；获得同组人互评优秀的；提交最终报告时间为班级前3名。（满分5分）（项数\*1分）；

同组评价：

本实验中你的同组人姓名： 刘颖 学号： U201911663

你给同组人评价： 优 （优 良 中 及格）；

理由： 任务完成速度快，质量高，善于使用搜索引擎工具。

# 

# 数据库安全基础实验

## 实验环境及要求

### 实验平台及说明

虚拟机：Vmware 15或者VirtualBox；

操作系统：虚拟机内安装kali Linux；

已安装：kali Linux2020虚拟机；

服务启动：按第一次Linux及Window虚拟机种介绍的方法，启动mysql、apache2,ssh服务；

其他配置：实验中虚拟主机IP 192.168.153.140 ；

**实验分组**

本实验2人一组，同组成员： 李欣宇 、 刘颖 ；

### 实验场景设置

2021年秋天，你已经熟悉了“银河”公司的Linux服务器基本情况。因为受到公司裁员的影响，公司原来的数据管理员离开了公司，公司指派你和Bob，一起临时负责数据管理员的工作。在熟悉数据几种类型的操作的同时，注意从安全的角度，寻找，发现问题，并尽量利用mysql提供的功能解决这些问题。

根据场景，需要你完成以下操作，作为数据库安全基本操作实验通关考核。请和你的同组伙伴一起完成，遇到问题，可以进行讨论、查阅资料，解决问题。

## 过程记录/实验任务（共8个任务，20个小关卡）

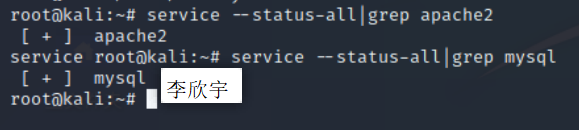
## 任务1 磨刀不误砍柴功

环境准备：为了使你们尽快熟悉业务数据，会将原来备份的一个数据库文件交给你，请你负责导入系统中；为了进行职责分工，将建立两个专门负责Galaxy数据库的账户，给你自己和你的伙伴Bob使用。

1）确认服务器上的数据库服务程序mysql已经开启；

2）确认服务器上的WWW服务程序apache2已经开启；

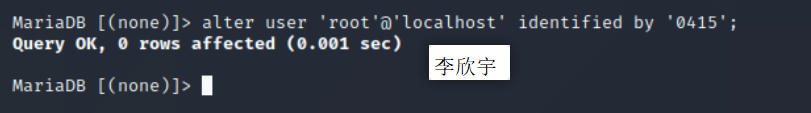
3）如果没有开启，请查阅资料，开启mysql服务及apache2服务；



确认mysql和apache2服务已经开启

4) 从虚拟机内部，通过命令行控制台，访问数据库服务；

*再通过mysql命令行，进入mysql，数据库root密码默认为空；进入后，可以给数据库root账户设置密码；*启动数据库控制台，创建一个数据库，取名字为*Galaxy;*

**

**

5）在虚拟机内安装phpmyadmin管理器；

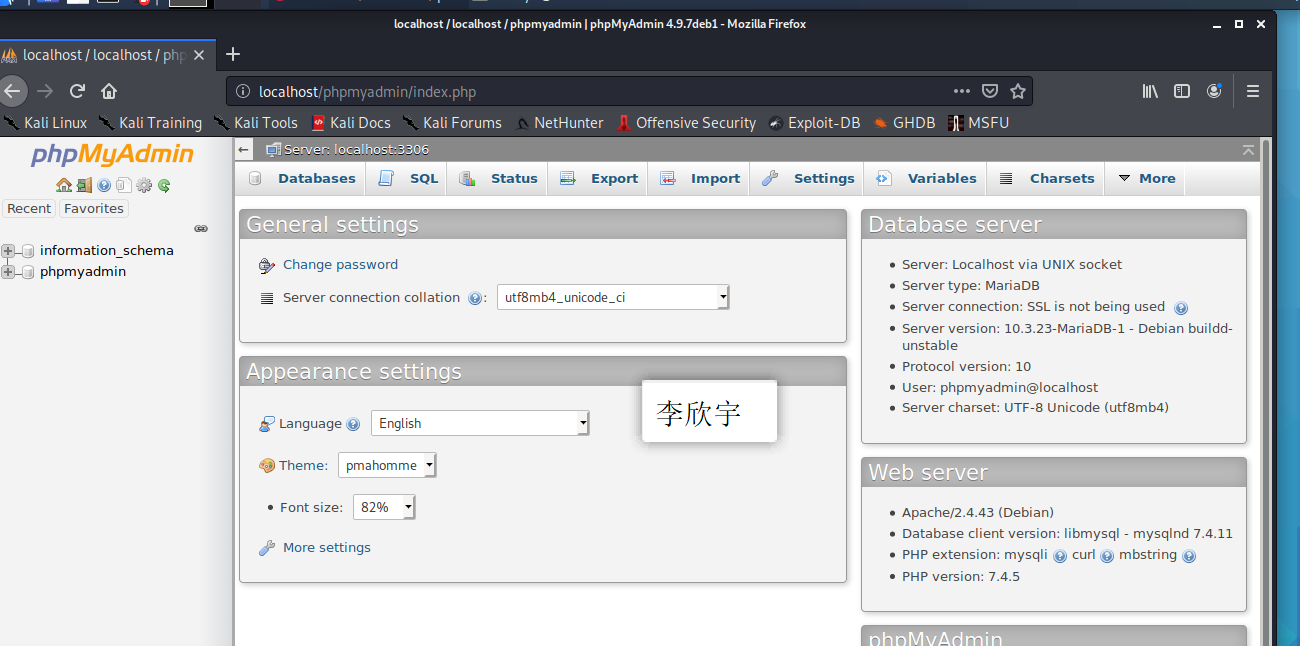
并通过phpmyadmin，自动配置一个可以访问mysql的账户，账户名phpmyadmin；配置phpmyadmin数据库密码;

通过命令行控制台，查看phpmyadmin账户是否成功；

通过浏览器，访问数据库管理端；

**

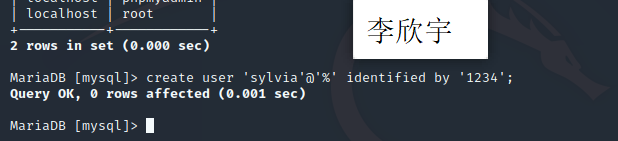
**

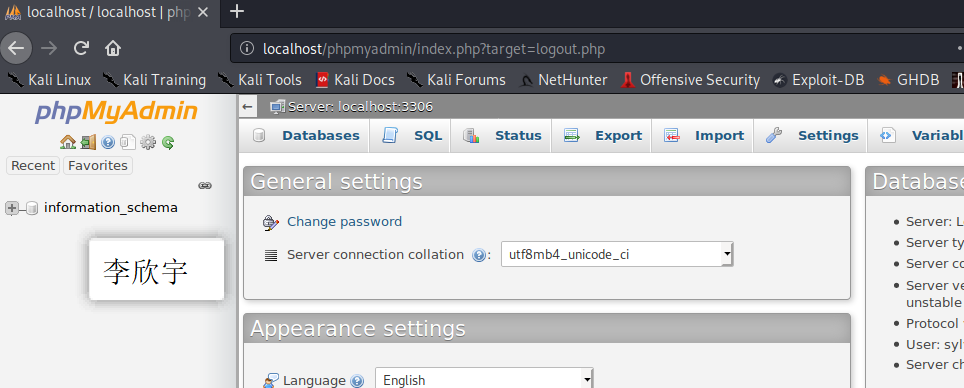
**

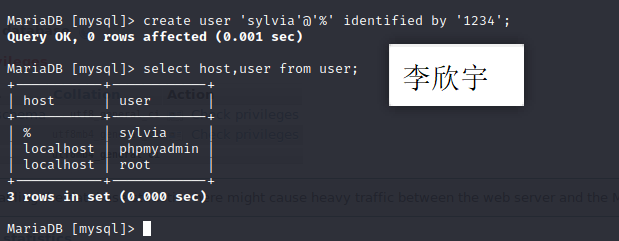
6）创建数据库用户sylvia；

通过浏览器及自己的用户，使用phpmyadmin图形界面访问数据库；查看你能访问哪些数据库实例；

通过命令行控制台，查看你的账户，查看权限；你能否看到Galaxy数据库？

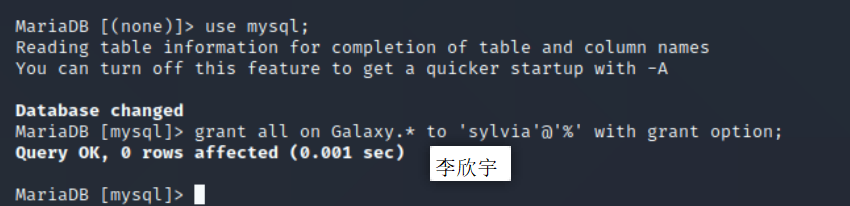








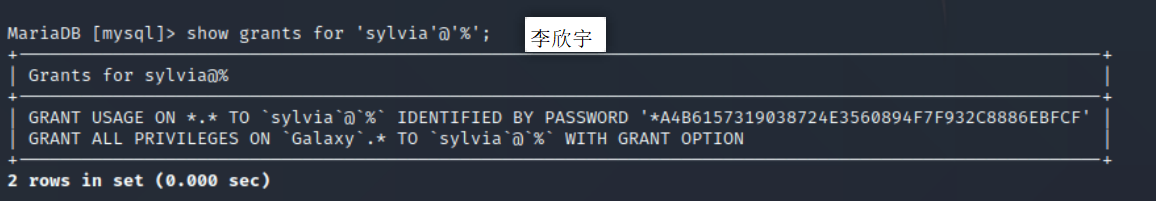
7）授权你自己（sylvia）访问数据库Galaxy、获得所有权限、允许你将权限转授；



8）验证7）的权限生效：虚拟机内，通过浏览器使用phpmyadmin连接数据库服务，使用你自己的用户名（sylvia）就可以通过phpmyadmin对Galaxy进行操作；

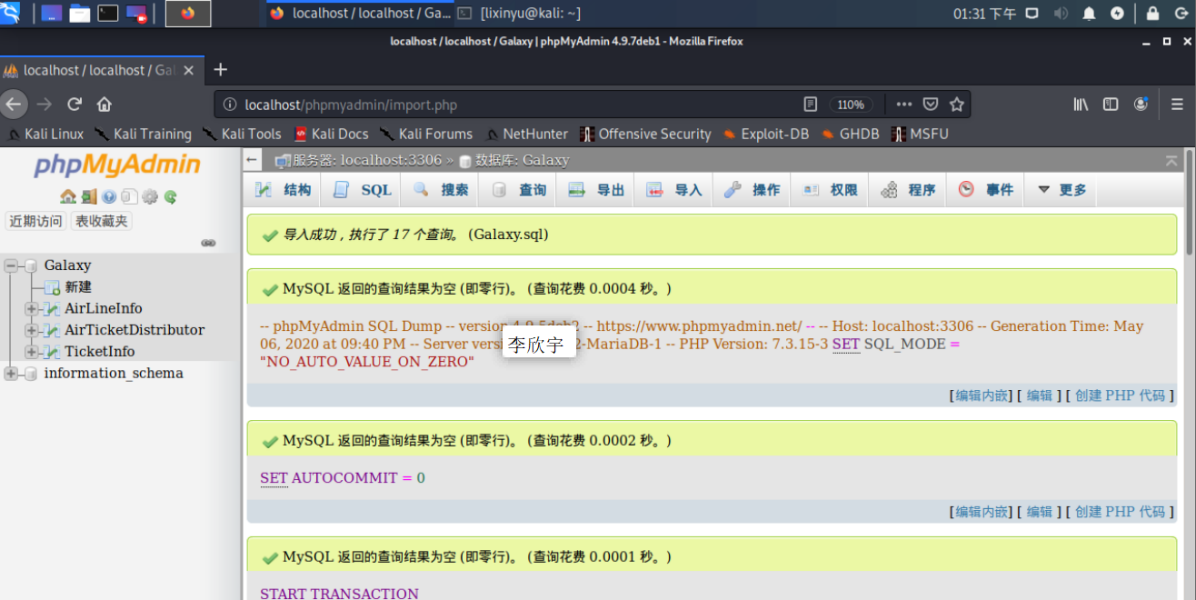
也可以通过命令行进行同样的验证；

![2N]@9K613P]()CMA2SC}2`B](data:image/png;base64,)



## 任务2 一个响指

9）数据恢复：从课程提供的某次数据库备份的文件中，恢复数据库Galaxy；

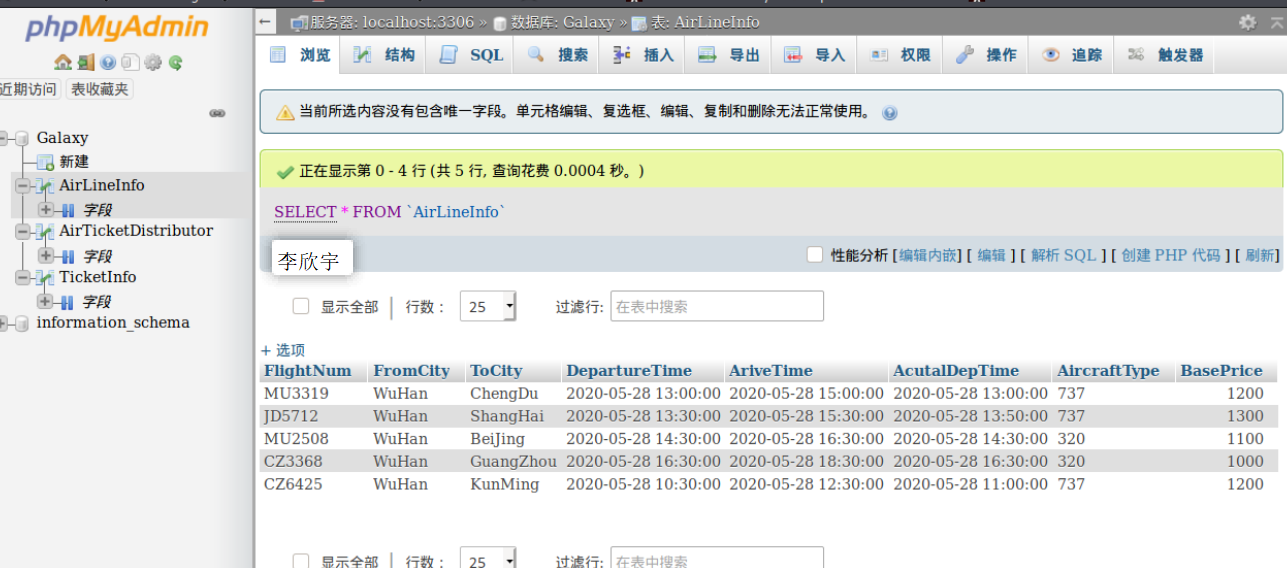


导入数据库Galaxy

10）查看恢复后的数据库：

导入成功后，通过浏览器查看数据内容。该数据库中目前有哪几个数据表：

有3个数据表 ；



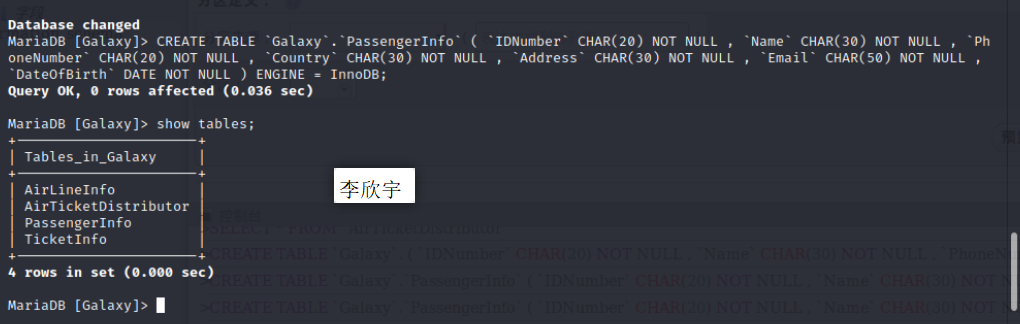
另外，查看各表内数据，看看其中有没有安全隐患？如果有，请列出来。

对于AirTicketDistributor表中，其内有相关商户的手机号码和邮箱等私人信息，更重要的是，还有明文口令。

## 任务3 24小时紧急任务

11）创建表

根据某个突发事件，公司进入应急响应状态，需要数据库能完成如下新需求：需要提供每位乘客的身份证号码和住址的查询，便于在第一时间，根据行程，联系到乘客，进行信息告知；作为数据库的管理人员，请你根据这一需求，查阅数据库相关的操作资料，能增加一张新表格。（提示：包括身份证号码，姓名，电话号码，国籍、住址、邮件地址、出生日期。身份证号码作为主关键字。另外，订票表格中，乘客姓名可以用身份证号码代替，或者额外加上身份证信息。）可以使用数据库图形管理工具。



创建一张表格

## 任务4 仿真数据

12）增加表中数据(Insert)

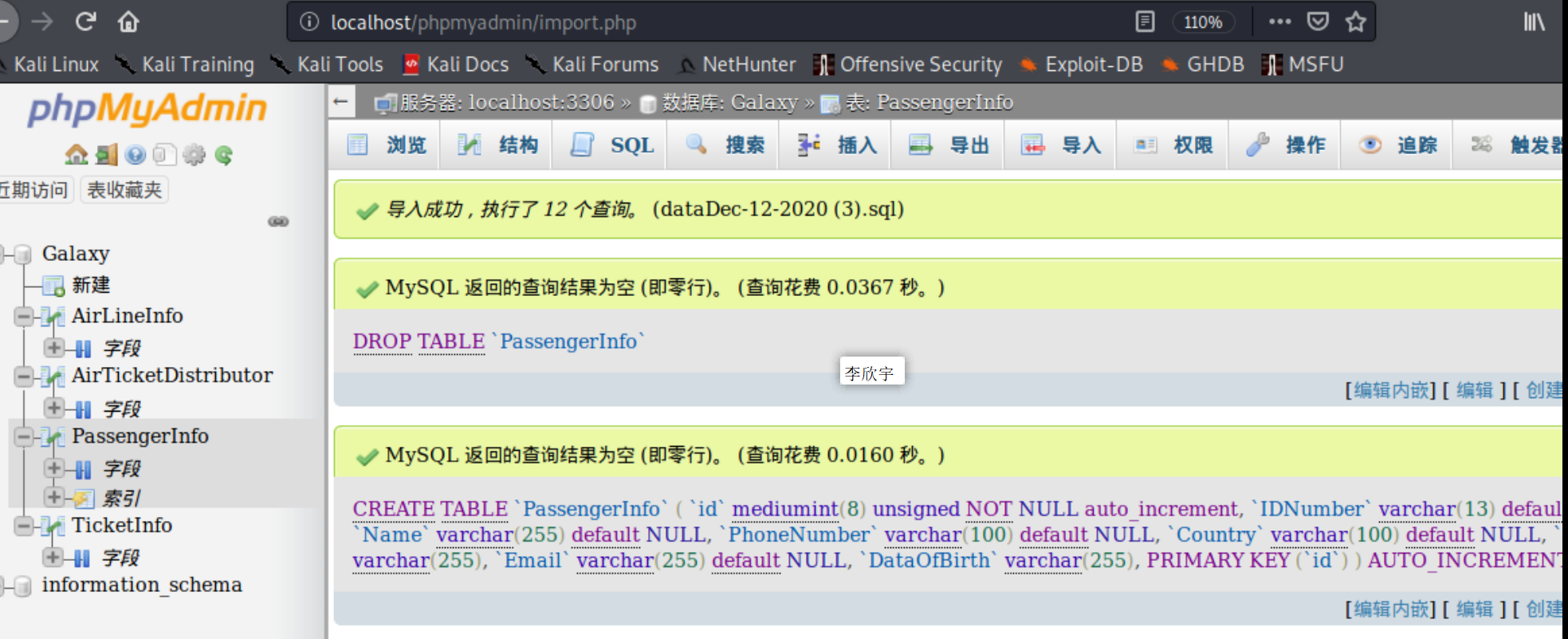
很多应用中，需要生成仿真数据，以测试系统性能、安全等问题；作为数据库管理员，请你为乘客信息表，增加模拟数据；模拟数据尽量保证随机性：身份证号码由数字组成；姓名用8位字母随机组成，邮件地址以15位以内的小写字母加数字组合为前缀，后面接@，在接标准域名；生日构成，年龄不超过200岁。

请先增加数据1条、5条、100条；

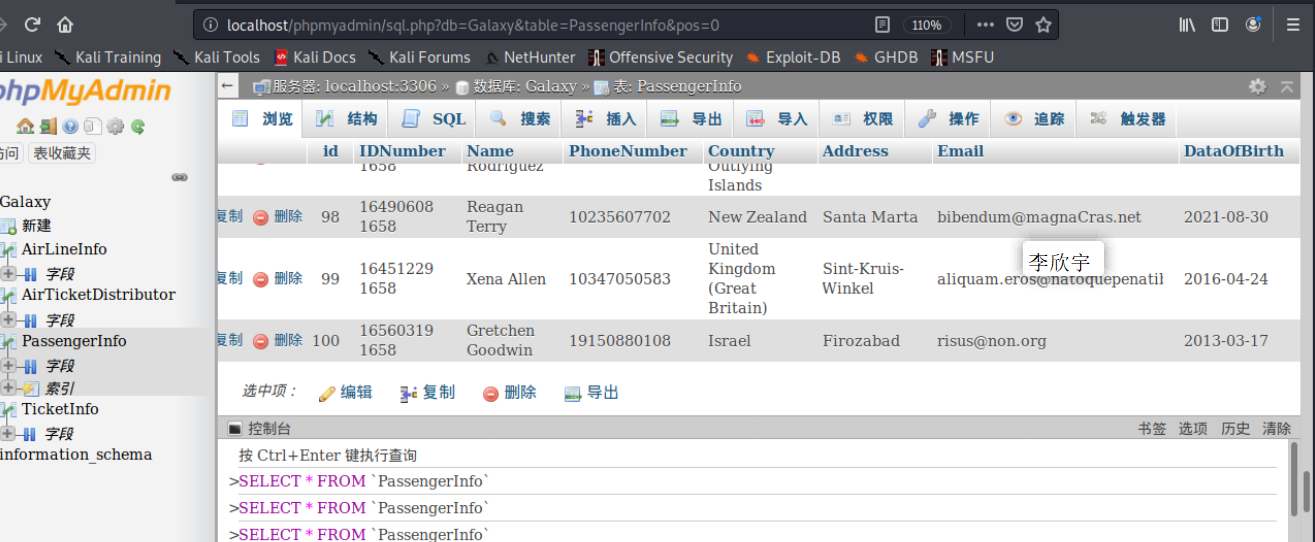
能力扩展：可以灵活运用课外查阅的其他工具，生成sql脚本完成仿真数据；



手动插入两条数据



将批量生成的100行数据导入表

查看导入的数据

## 任务5 天气原因

13）修改数据(Update)

因为气象部门提供的天气预报预警，航空公司将2020年5月28日，飞往上海的航班JD5712推迟1小时，作为航班数据的管理者，请你按提供的信息，修改航班信息数据；



命令行修改数据

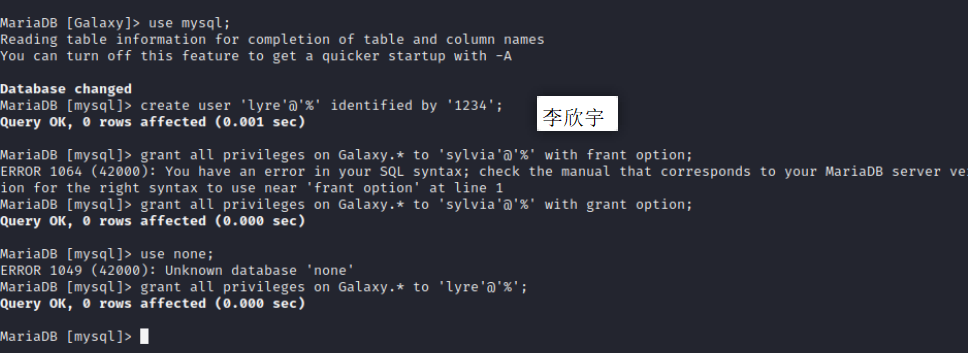


图形界面查看数据

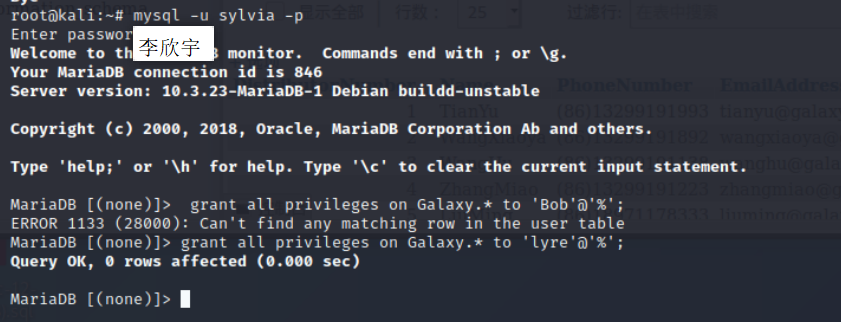
## 任务6 人多力量大Many Hands Make Light Work

14）授权他人访问(Grant)

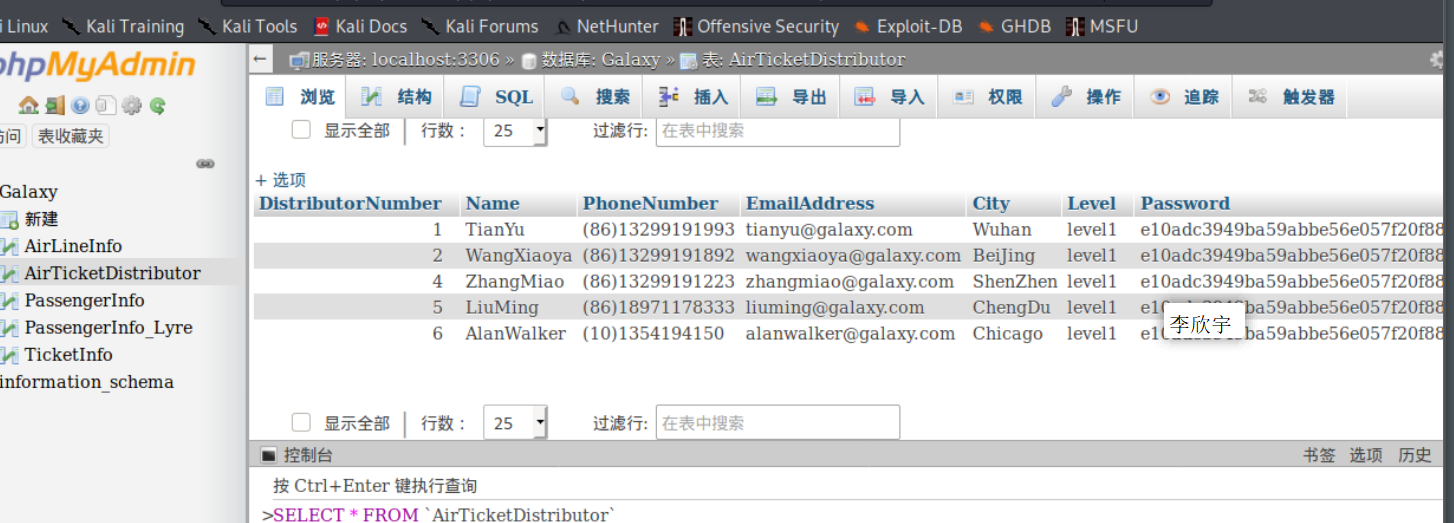
你（Alice）授权授权你的同组人（Bob）对数据库galaxy访问、可由Bob访问你虚拟机中的数据库并导入他生成的100条乘客信息数据，这样你们都有200条数据了！



创建lyre用户



授权lyre

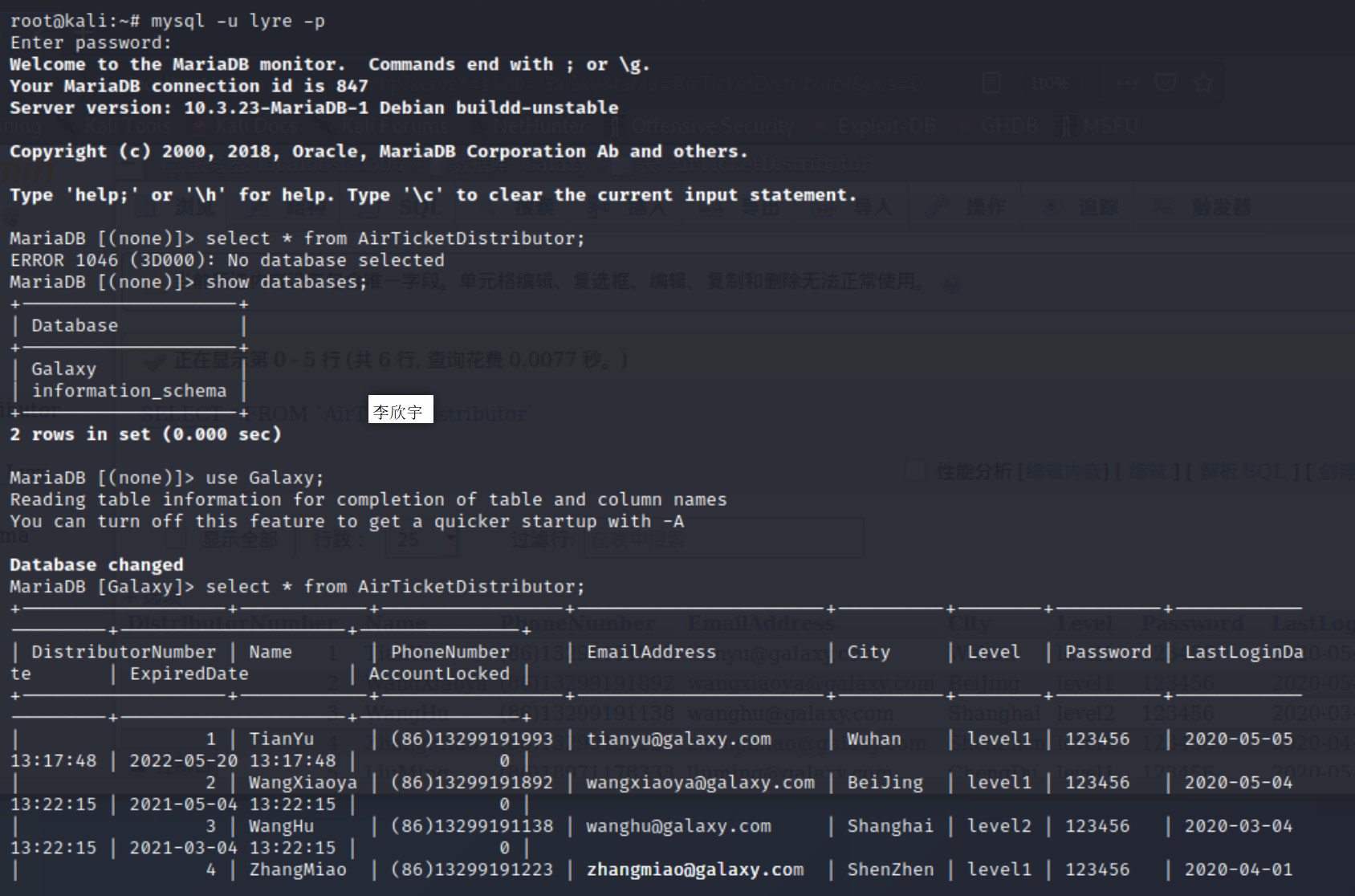


使用lyre登录并导入数据

## 任务7 百密一疏OOps

15）删除数据（Delete）

你的同组人Bob，登录数据库；导入了Bob负责录入产生的另外100条数据； Bob通过查询，发现了其中一个分销商是自己以前的雇主，由于私人原因，Bob恶意对该分销商信息进行了删除！



登录lyre，查看商户信息



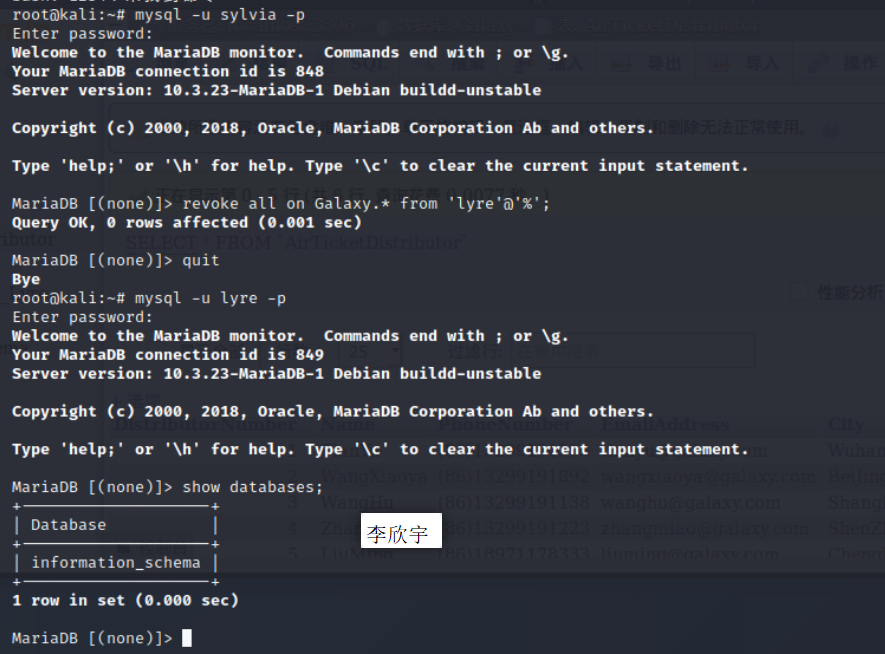
删除商户信息

## 任务8 亡羊补牢

16）撤销授权(Revoke)

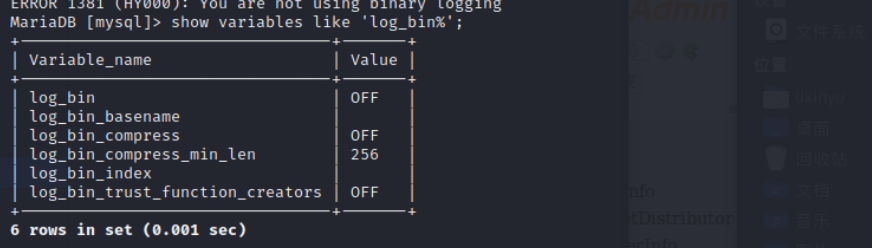
你（Alice）上线后，发现分销商信息缺失！首先，收回了对Bob的授权，防止损害扩大；思考：现在请测试Bob还能访问Galaxy数据库吗？

扩展能力：能恢复被删除的数据吗？



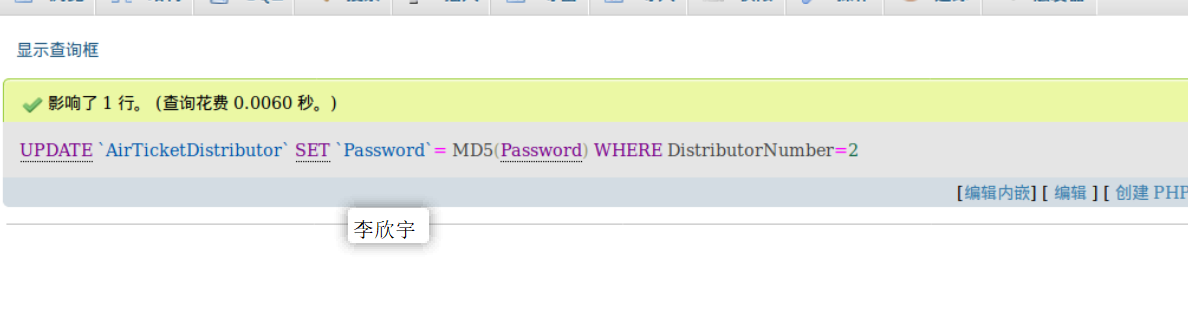
撤销给lyre的授权后查看lyre的权限

恢复被删数据：可以通过数据库binlog日志恢复，前提是binlog日志是开启，遗憾的是，我的binlog日志是关闭的，也就不能恢复。

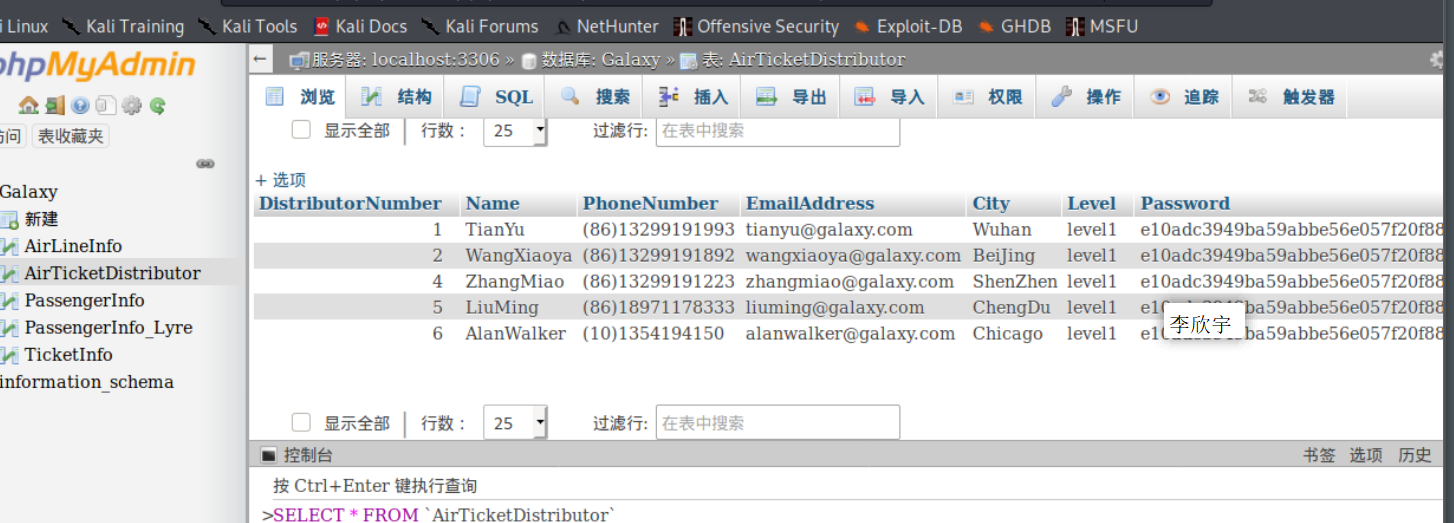


17）口令和信息保护

数据库某个使用者能看到数据库表中敏感信息，包括电话号码、密码，你觉得安全吗？因为这次出现的安全问题，引起了你的注意，发现分销商的姓名、密码是明文存放的，数据管理员可以获取分销商的信息及明文口令。为此，需要你对这些信息进行简单保护：用hash函数处理密码，将口令的hash值存入数据库的口令字段，代替原来的明文密码。



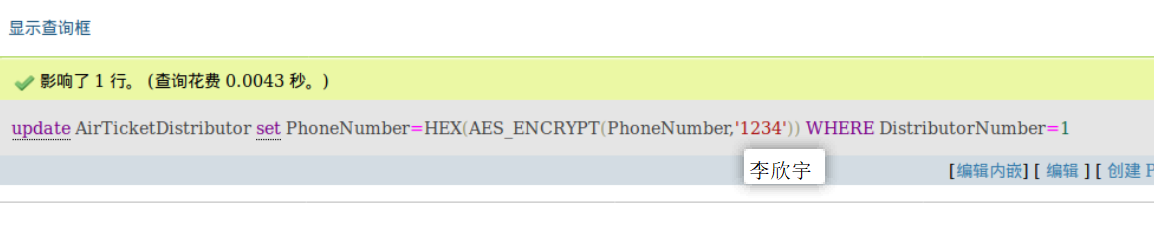
加密明文口令



查看加密后的商户信息

18）加密数据(Encrypt)

同时，因为分销商的电话信息也是明文的，一旦系统被越权访问，可以直接获得分销商清单，因此需要对该项进行安全防护，简单加密表中数据。



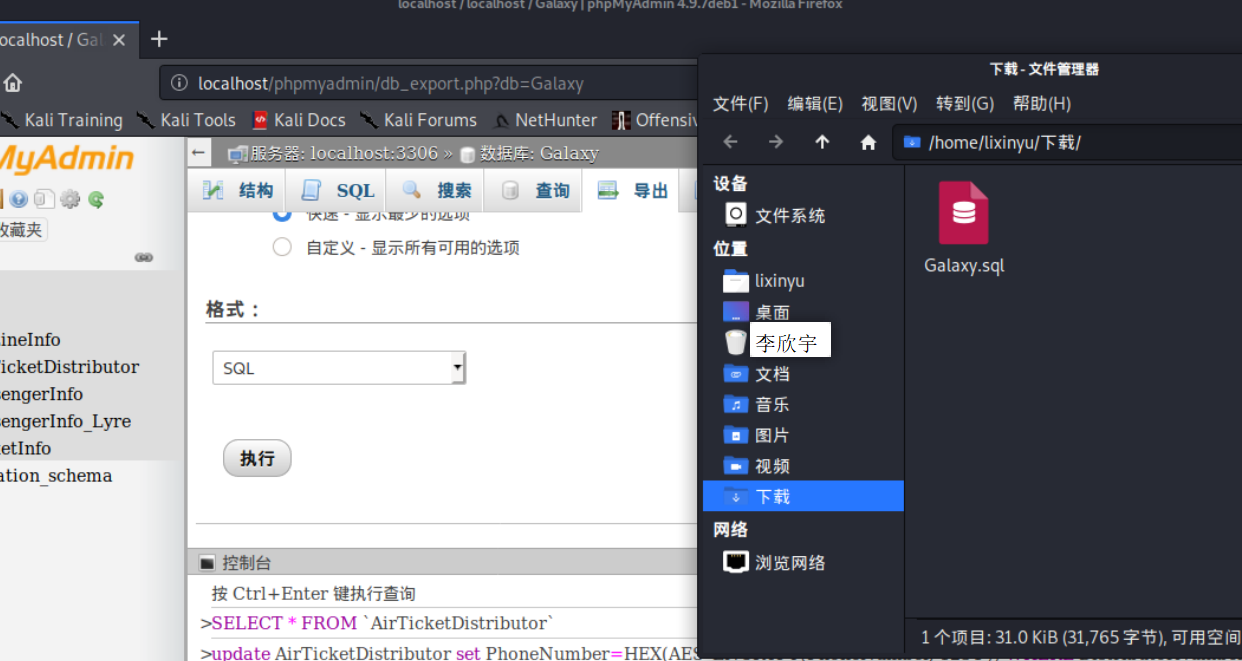
加密电话信息



查看加密后的商户信息

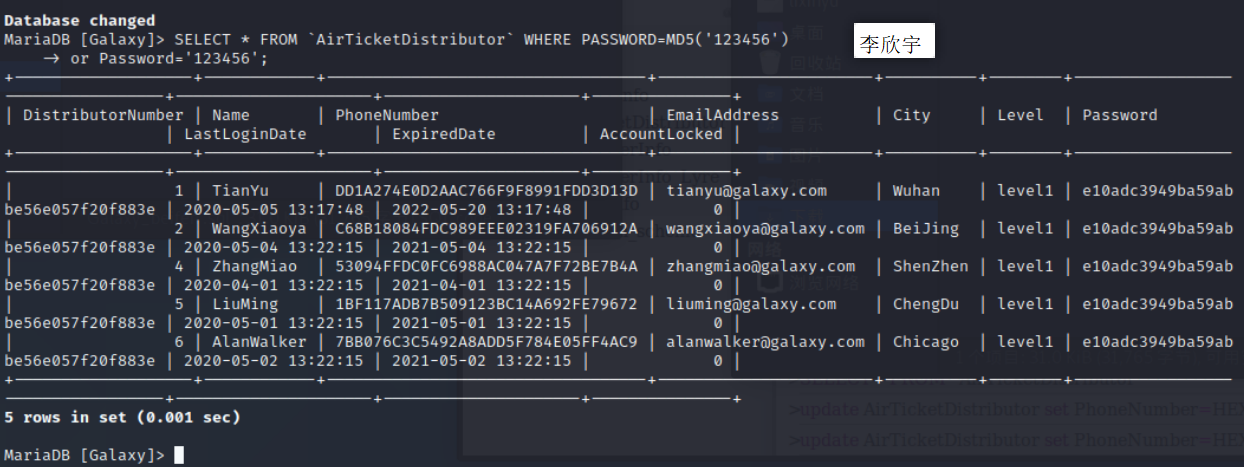
19）备份数据库(Backup)

完成这些记录后，请你对系统进行备份；



在图形化界面直接将当前数据库导出进行备份

20）密文查询

虽然数据被加密了，但为了完成公司正常业务，需要进行查询。加密了的数据如何查询呢？有些用户习惯使用容易记忆的弱口令，比如‘123456’，请你在命令行模式下，查询所有使用该弱口令的分销商名字，准备邮件通知他们修改口令。

查看使用弱口令的用户

## 扩展阅读

1）了解kali下mysql服务是MySQL吗？查找Mysql、Oracle相关资料了解MySQL的发展背景；

2）[阅读MySQL手册英文版](file:///C:\\Users\\liumi\\AppData\\Roaming\\Microsoft\\Word\\3%20Mysql\\refman-8.0-en.a4.pdf)中，关于Grant/Revoke；MD5；AES\_Encrypt/AES\_Decrypt的相关说明；

3）\*创新扩展实验I：将乘客信息表中导入大量仿真数据，形成不同量级的原始数据（1k、10k、100k条）；对其中姓名、电话、住址信息加密；对比明文和密文的查询时间差异；

4）\*创新扩展实验II：建一个仿真数据库，用来处理应对本次疫情环境下，1000000人规模从居住地到工作地、购物点的最新14天的路径记录；尽量保证隐私数据，而在授权后，可以恢复出14天内的生活路径信息；

5）关于mysql的root账户通过phpmyadmin进行管理，出于安全考虑，默认root账户是不能访问的，解决方法：alter user 'root'@'localhost' identified by '123456'修改root本地密码为123456；

## 实验问题分析与总结

遇到的主要问题是phpmyadmin的安装，本人使用的是kali2019.3版本，采用了两种安装方式均失败。

①apt-get install 安装，使用自动安装的方式会出现白屏的状况.通过查阅博客，是缺少了php-mbstring 和php-gettext两个包，但是安装后并没有解决。查找其他相关博客，均没有解决白屏问题的，待解决。

②使用安装包手动安装，出现2006错误，使用搜索引擎查找相关解决方法，只找到一篇相关博客，但是与之相关的四个问题都不存在，未解决。

最终无奈之下，重装了kali2020.3版本，使用apt-get install 顺利安装，但以上两个问题的原因仍未知。

总结：这次实验还是很崩心态的，尤其是第一步就卡了几天，但还是很感谢老师和同学的帮助。我也是第一次接触数据库这个概念，确实在后面几个任务中学习到了很多数据库的知识，尤其是恢复数据这一任务，让我觉得这是最有用也是最cool的。

## 参考文献及资料列表

[1]详解：如何恢复MySQL数据库下误删的数据-aiLiNux-51CTO博 客,https://blog.51cto.com/alinu/1911417

[2]数据生成generatedata,http://www.generatedata.com/

[3]恢复mysql数据库数据,https://www.cnblogs.com/nikeodong/p/10615058.html

[4]Ubuntu 安装 PhpMyAdmin 管理 MySQL 数据 库,https://www.cnblogs.com/xpwi/p/9821371.html

[5] 安装phpMyAdmin图文教程-学 习,https://blog.csdn.net/qq\_37608398/article/details/80716458