

“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 网络空间安全学院

专业班级

姓 名

学 号

日 期 2021 年 6 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： 学号：

你给同组人评价： 优 （优 良 中 及格）；

理由： 对SQL型数据库有基本的了解，能够进行一些基础操作并独立完成实验任务，达成了本次实验的学习目标。

# 

# 数据库安全基础实验

## 实验环境及要求

### 实验平台及说明

本实验同组成员： 、 ；

### 实验场景设置

2021年春天，你已经熟悉了“银河”公司的Linux服务器基本情况。公司指派你和Bob，负责数据管理员的工作。在了解几种类型数据操作的同时，寻找发现安全相关问题，并利用mysql的功能解决。

根据以上场景，完成以下操作，作为数据库安全基础实践通关考核。可组内讨论、查阅资料。

## 过程记录/实验任务（共8个关卡，20个小任务）

## 关卡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）确认数据服务mysql已经开启

2）确认web服务apache2已经开启:

3）如果没有开启，请查阅资料，开启mysql/mariadb服务及apache2服务。

4) 控制台访问数据库

启动数据库控制台，查看已有数据库列表；

创建数据库G*alaxy;*

5）安装phpmyadmin管理工具

*安装后查看phpmyadmin账户是否成功：*

*通过浏览器，因为自动配置，现在可以通过浏览器，访问数据库管理端了；但用户名只能用phpmyadmin；而用户root不能访问。为什么？*

**答：**允许root用户访问可能导致攻击者利用主机未修改的root用户密码直接进行攻击；

6）创建数据库用户Alice；*//用自己的名字;完成后，通过控制台，查看Alice账户；*

7）授权访问，允许Alice访问数据库Galaxy，并获得所有权限，可以转授。

8）通过浏览器打开phpmyadmin，用Alice账户登录，对Galaxy进行操作；

*另外，Alice也可以通过类似mysql命令行，进入数据库管理。*

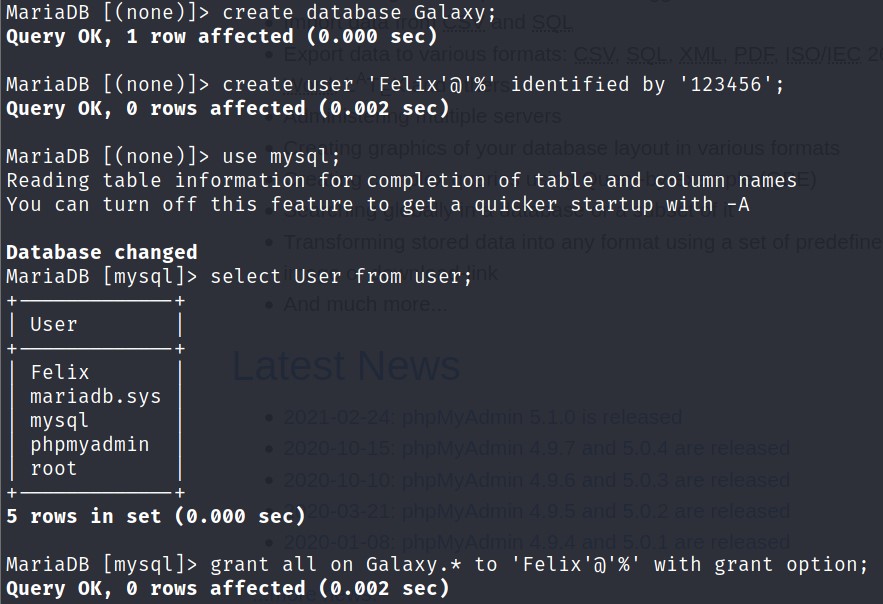


图1 创建数据库，新增用户，设定权限

## 关卡2 一个响指

9）数据恢复：从指导老师提供的文件中恢复数据库Galaxy

10）查看数据库

导入成功后，通过浏览器查看数据内容。该数据库中目前有数据表：

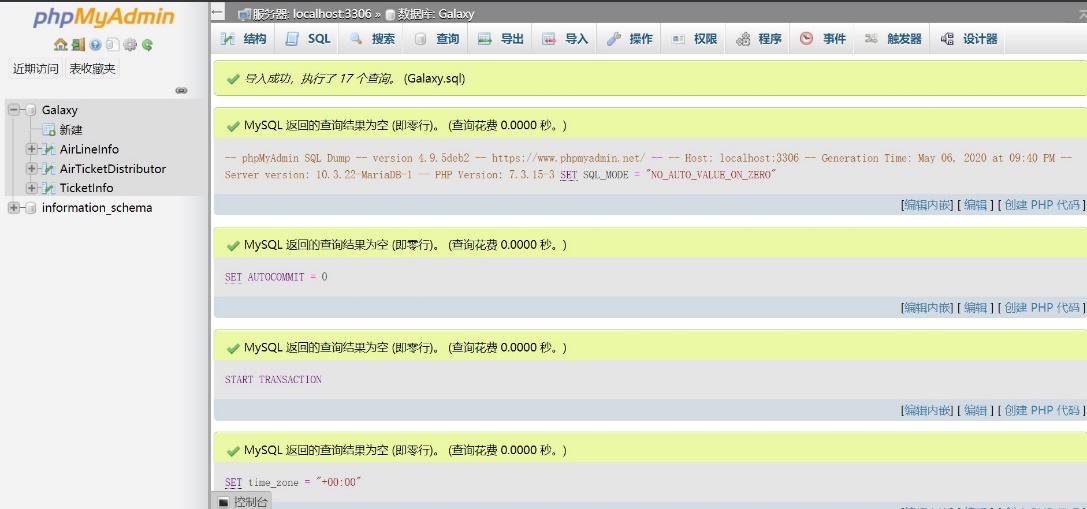
AirLineInfo AirTicket DistributerTicketInfo 三张表

另外，查看各表内数据，其中有没有安全隐患？请列出来。

有；AirDistributer表中的Pasword列均为123456，即密码均为123456

属于弱口令密码；

。



**图2 导入数据库**

## 关卡3 24小时紧急任务

11）创建表

根据应急状态下的新需求，需要知道每位乘客的身份证号码和住址，便于在第一时间，联系到乘客，进行信息告知；请你为此需求，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。）



**图3 创建了乘客信息表**

使用可视化工具建立了要求的乘客信息表如图3所示。

## 关卡4 仿真数据

12）增加表中数据(Insert)

为你的乘客信息表，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，以你的学号后四位作为开头，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。

## 关卡5 天气原因

13）修改数据(Update)

因为天气原因，2020年5月28日，飞往上海的航班JD5712推迟1小时，请按次信息，修改数据库中相应的航班信息；



图4 更新数据

使用Update命令和Date\_add函数对航班信息进行了更新。

## 关卡6 人多力量大

14）授权他人访问(Grant)

Alice授权Bob对数据库galaxy的访问权限，便于Bob导入乘客信息数据。

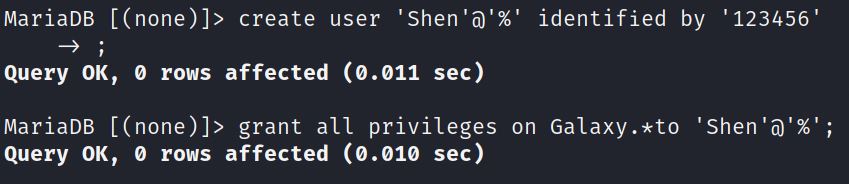


图5 创建用户Shen并授权

创建用户Shen，并给予其在任意ip访问和修改Galaxy数据库的权限。

## 关卡7 百密一疏

15）删除数据（Delete）

以Bob账户，登录数据库；导入了Bob负责产生的数据；但Bob使用中，查询数据后， Bob故意对分销商WangHu信息进行了删除！

*Select \* from AirTicketDistributor;*

*Delete from AirTicketDistributor where name=’WangHu’;*

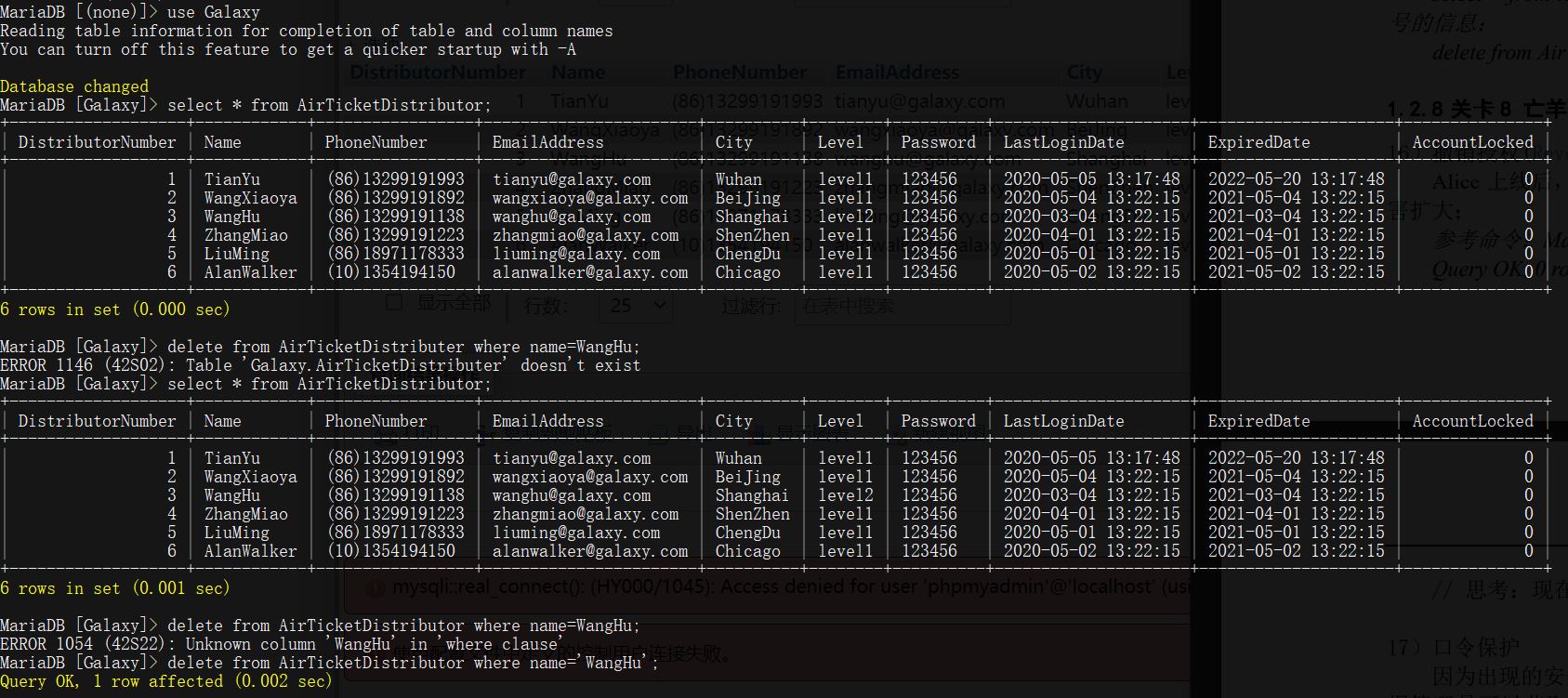


图6 在Shen用户下对分销商WangHu的信息进行了删除

删除前后AirTicketDistributor表的内容对比如图6所示。

## 关卡8 亡羊补牢

16）撤销授权(Revoke)

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；

请测试Bob是否还能继续访问Galaxy数据库。

17）口令保护（Update）

因为出现的安全问题，引起了你的注意，发现分销商密码是明文存放的，数据管理员可以获取分销商的明文口令。为此，你对该口令进行了简单保护，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。

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，简单加密表项

19）备份数据库(Backup)

完成这些记录后，请你对系统进行备份；

20）密文查询

在命令行模式下，查询口令是‘123456’的所有分销商，因为该口令过于简单，准备通知他们修改口令。

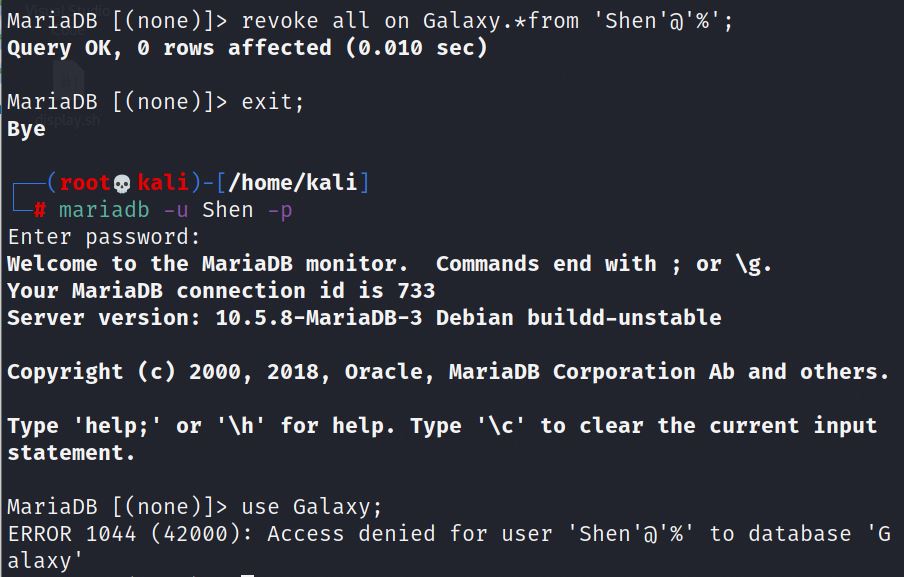


图7 移除了Shen用户对Galaxy的权限

移除了Shen用户对Galaxy的所有权限，经测试Shen用户已不能使用Galaxy。



图8 使用md5加密Password

使用update对Password进行md5加密后的结果如图8所示。



图9 对电话号码进行AES加密

使用update对分销商的电话号码进行AES加密。



图10 使用phpmyadmin对数据库进行导出

使用导出功能进行备份。

执行查询后，发现分销商密码均为123456，属于弱口令，建议予以更改。

## 课外阅读与扩展关卡

1）了解kali下mariadb服务是MySQL吗？查找mariadb、Mysql、Oracle相关资料了解MySQL的背景；我们国家有自己的数据库系统吗？

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，重点查阅与安全有关的操作，比如Grant/Revoke；MD5；AES\_Encrypt/AES\_Decrypt的段落；

3）\*创新扩展实验：请你建一个仿真数据库，用来记录某城市的注射新冠疫苗的相关信息，假设有100000人；//要记录哪些信息（比如注射疫苗的时间、地点、型号、人的姓名、证件号、联系方式）？谁可以访问这些信息？如何保证信息真实有效？

**解答：**

Mariadb是mysql的一个分支，完全兼容mysql，使用了不同的存储引擎；我国有OceanBase，达梦，TiDB等数据库；

## 实验问题分析与总结

本次实验学习MySQL型数据库的基本操作；主要遇到的问题是：基础知识不足，比如基础SQL语句和函数；创建模拟数据的任务可能需要MySQL编程的知识，具有一定的学习成本。

## 参考文献及资料列表

1. PG/MySQL/SqlServer数据库中批量制造测试模拟数据——CSDN，https://blog.csdn.net/inrgihc/article/details/105393922