華中科技大學

“网络安全综合实验（I）”实验指导

数据库安全基础实验

（V20210525）

1　数据库安全基础实验

1.1　实验环境及要求

1.1.1　实验平台及说明

虚拟机：Vmware 15 或 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；
实验分组
本实验 2 人一组，同组成员：_____ 、_____；

分组说明：与第一次分组类似，结合实践课程，便于实验同学间相互讨论、团队协作及相互支持，要求两位同学一组（Alice+Bob）。

参考资料：Linux 自带帮助 man、mariadb 官网资料、课程群共享文件、在线资料及文档、实验指导教材《网络安全综合实验（I）》。

提交时间及文件名说明：提交独立实验报告电子版一份，按指导老师要求的时间和方式提交；文件名按“姓名-数据库安全基础实验”。

报告格式说明：正文为宋体小 4 号，段首缩进 2 字符汉字，行间距 1 倍行距，字符间距为标准；截图保证内容清晰、图内字体大小合适；每页尽量不留大段空白。图片需要编号及命名；正文、图片、参考文献的格式，请参考华中科技大学毕业论文规范中关于排版的要求。

文档中包含的内容：1 封面首页信息及作者、完成时间； 2 完成任务的过程，可在任务书的基础上进行改写，补全主要截图及相应的过程说明文字；3 小结：总体感受、实验中遇到的最突出问题及收获、对实验环节的意见和建议；4 实验中为解决问题，查阅资料，请记录资料出处，包括资料名次、页码、网址，作为参考文献部分列表给出； 5 参考网络上资料的，请通过浏览器打印 pdf 功能保存；资料可归档为：参考资料.zip，与报告一并提交。

截图要求：实验过程中，请各自保留实验中虚拟机桌面截图，配上相应的说明文字；截图标注自己姓名水印；命令终端字体较小，请放大字体后再截图；

虚拟机用户名说明：

Kali 目前版本默认 username:kali; password:kali；增加本人用户及同组同学用户时，用同学的姓名拼音作为用户名；数据库默认用户 root，口令为空；

1.2　过程记录/实验任务（共 8 个关卡，20 个小任务）

1.2.1 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）确定虚拟机上的数据服务 mariadb/mysql 已经开启；

参考命令：sudo service --status-all|grep mariadb //进入 kali Linux 控制台，需要临时用超级用户权限执行

2）确认 web 服务 apache2 已经开启；

参考命令：sudo service -- status-all|grep apache2 // 进入 kali Linux 控制台后执行

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

参考命令：sudo service mysql start；service apache2 start；

4）控制台访问数据库；

*参考命令：mysql -u root -p //如果首次使用失败，可以用 su 命令，**切换到操作系统的 root 账号**，见 linux 基础实验 1.2.9；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；请一定记住该数据库用户名和对应密码，注意，这个用户和 kali 系统的 root 用户没有联系；*

启动数据库控制台，创建数据库 *Galaxy;*

参考命令：create database Galaxy;

参考命令：show databases;

5）安装 phpmyadmin 管理器；

参考命令： apt-get install phpmyadmin //如果提示找不到，可能因为未更新 kali 已安装的程序信息，则用下面方法解决；

参考命令：apt-get update

***注意：**安装 phpmyadmin 过程，要阅读一下英文提示信息！当提示要求对已安装的 web server 选择时，一定要选中选 apache2（kali 系统自带的 WWW 服务程序是 apache2），注意选项前有*号才表示选中了，用**空格键**进行选择，**默认是没有选中**的！选中后，安装程序才会搜索 kali 系统中 apache2 的目录，并对其配置文件进行修改，增加相应的 web 目录文件和数据库用户，进行自动配置；如果没有勾选，安装完成后，无法直接通过浏览器开启 phpmyadmin 管理 mysql 的功能，需要自己手动配置或者重新安装。*

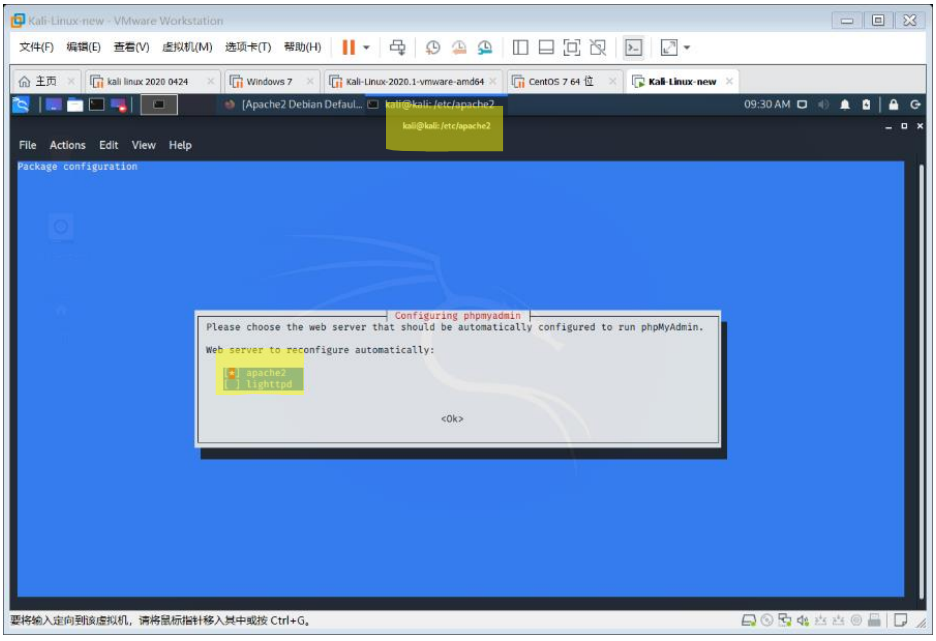

图 1-1 安装 phpmyadmin 时勾选 apache2

安装过程中，通过 phpmyadmin 管理入口，程序自动配置一个可以访问 mysql 的账户，账户名 phpmyadmin；密码通过下面界面输入；

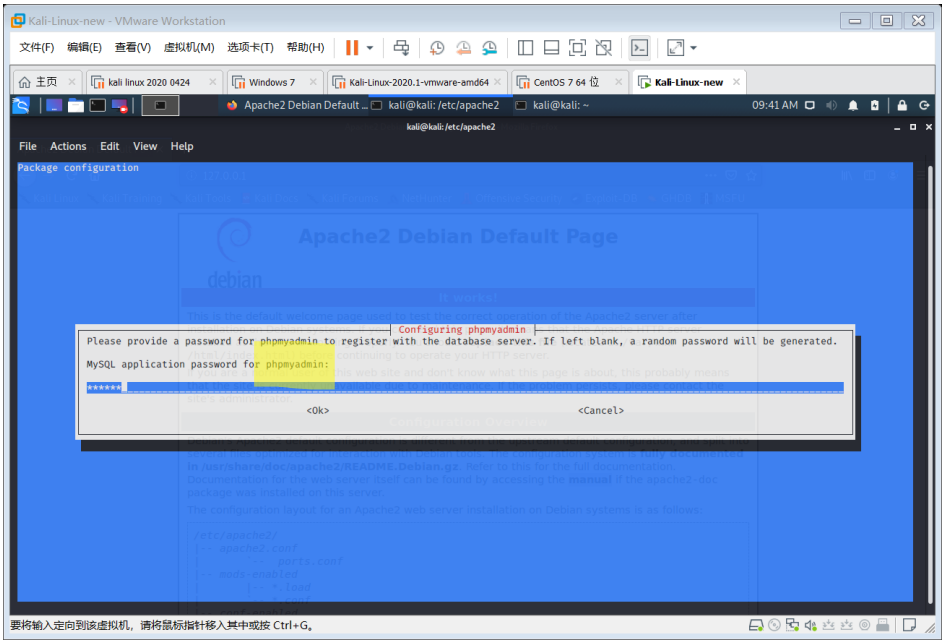

图 1-2 安装 phpmyadmin 时创建数据库用户密码

配置 phpmyadmin 数据库密码 123456;

// 此时，你可以通过 kali 控制台，用前面提到的命令，进入 mysql，参考命令：mysql -u root -p ；可以通过控制台查看 phpmyadmin 账户是否成功，参考命令：

```
show databases;    //列出数据库名
use mysql;         // 使用其中 mysql 数据库，其中存放了账户信息
select Host,User,Password from user; //从 user 表/视图中查看用户
```

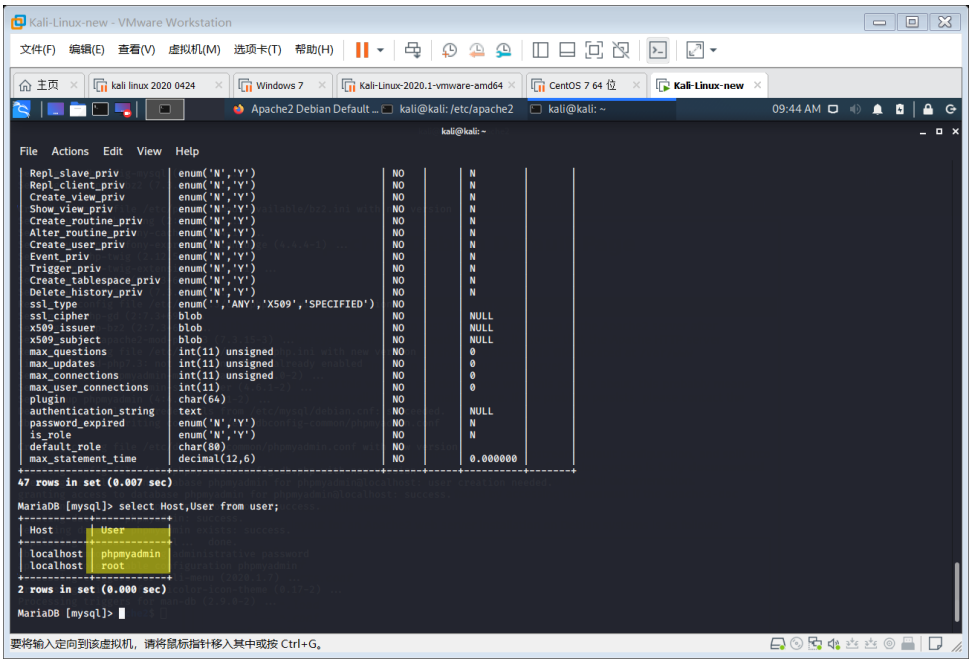

图 1-3 控制台查询表 user

如果配置成功，会从控制台命令模式，查找到 mysql 系统的 User 里增加了用户 phpmyadmin。同步继续完成安装配置 phpmyadmin，默认进行，直到结束。

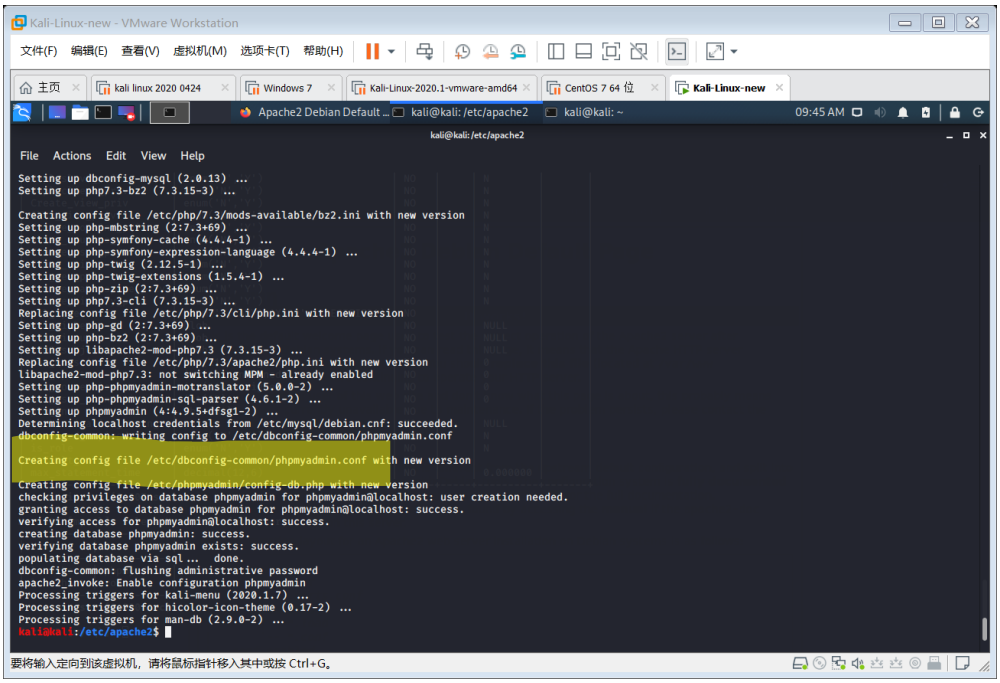

图 1-4 安装 phpmyadmin 完成时提示信息

phpmyadmin 安装完成后显示信息如上图所示。

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？

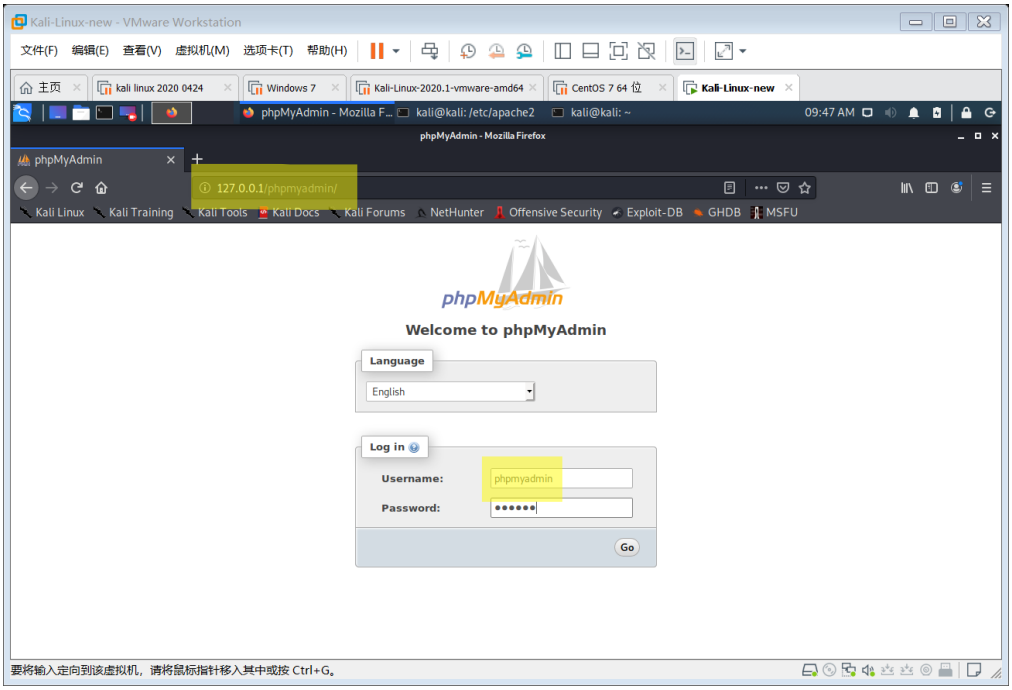

图 1-5 安装 phpmyadmin 后访问本地数据库服务

6）创建数据库用户 Alice；*//Alice 用自己的名字代替，命令中用英文单引号*

```
MariaDB [mysql]> create user 'Alice'@'%' identified by '1234';
Query OK, 0 rows affected (0.001 sec)
```

//创建时，用的%表示访问 mysql 时的 ip 范围，这样，用 Alice 也可以访问 phpmyadmin 图形界面了，如下图。看一下，Alice 能访问哪些数据库呢？

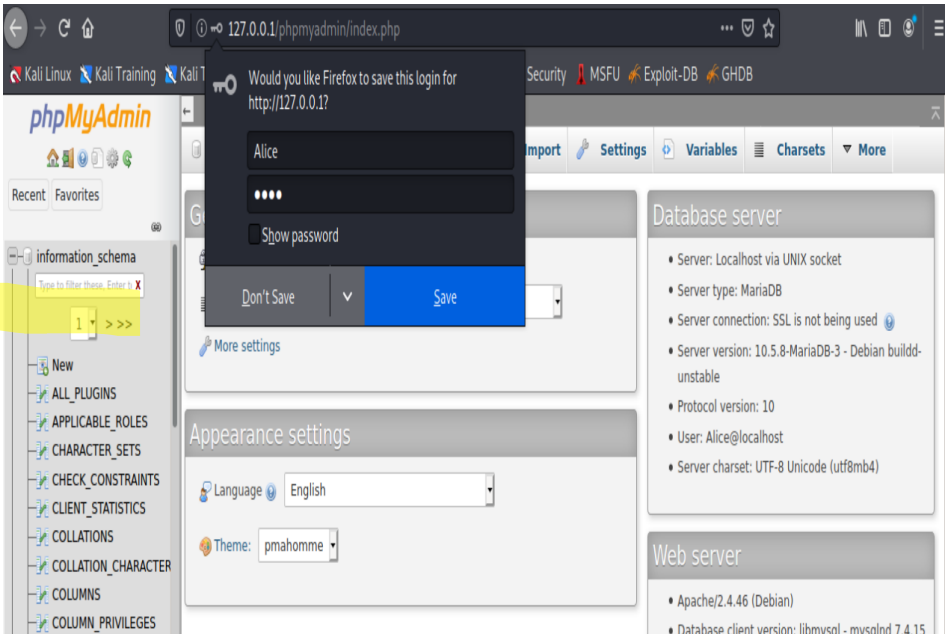

图 1-6 通过 phpmyadmin 工具查看用户 Alice 能访问的数据库

通过控制台，可查看 user 表中 Alice 账户；

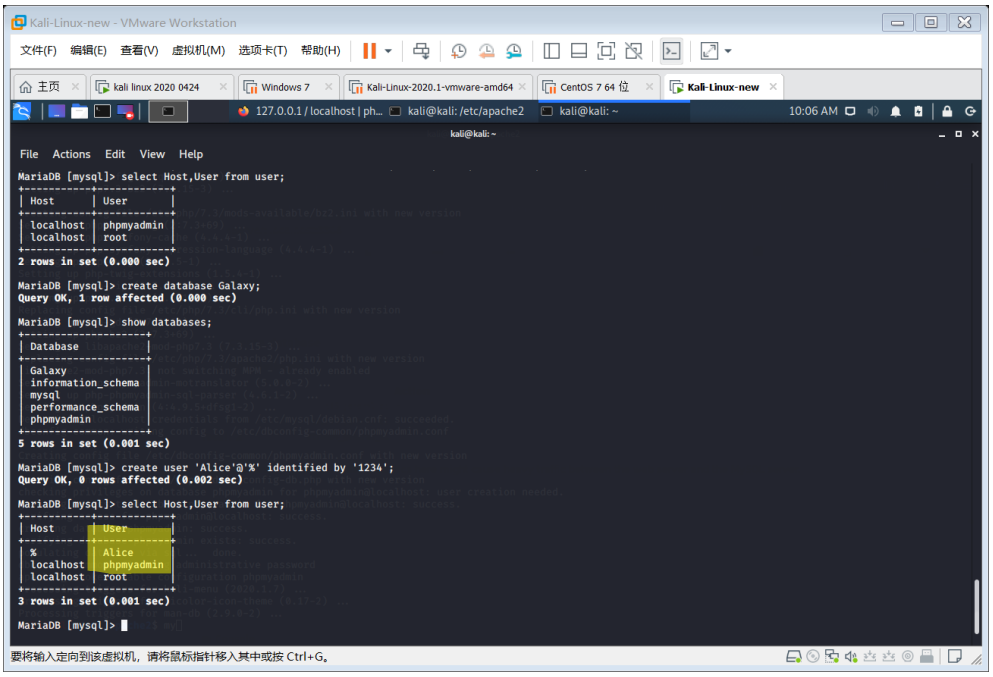

图 1-7 通过控制台测试数据库用户 Alice 能访问的 mysql 系统内数据库

//设置 Alice 口令 1234， %表示可以从任意 ip 地址进行访问

*// 查看权限：select * from information_schema.user_privileges； 当前 Alice 有什么权限*

```
MariaDB [mysql]> select * from information_schema.user_privileges;
+-------------------+---------------+-----------------+--------------+
| GRANTEE           | TABLE_CATALOG | PRIVILEGE_TYPE  | IS_GRANTABLE |
+-------------------+---------------+-----------------+--------------+
| 'Alice'@'%'       | def           | USAGE           | NO           |
| 'LiuMing'@'%'     | def           | SELECT          | YES          |
| 'LiuMing'@'%'     | def           | INSERT          | YES          |
| 'LiuMing'@'%'     | def           | UPDATE          | YES          |
| 'LiuMing'@'%'     | def           | DELETE          | YES          |
| 'LiuMing'@'%'     | def           | CREATE          | YES          |
```

7）授权访问，允许 Alice 访问数据库 Galaxy，并获得所有权限，可以转授他人。因版本会升级产生变化，可参考官网 https://mariadb.com/kb/en/grant/

参考命令：grant all on Galaxy. to 'Alice'@'%' with grant option;*

```
MariaDB [mysql]> grant all on Galaxy.* to Alice@'%' with grant option;
Query OK, 0 rows affected (0.002 sec)
```

图 1-8 通过控制台为用户 Alice 授权

8）通过 phpmyadmin 工具管理：网络浏览器，Alice 就可以通过 phpmyadmin 对 Galaxy 进行操作；

访问 phpmyadmin 页面，用 Alice 用户进入系统；另外，Alice 也可以通过命令行进入数据库；

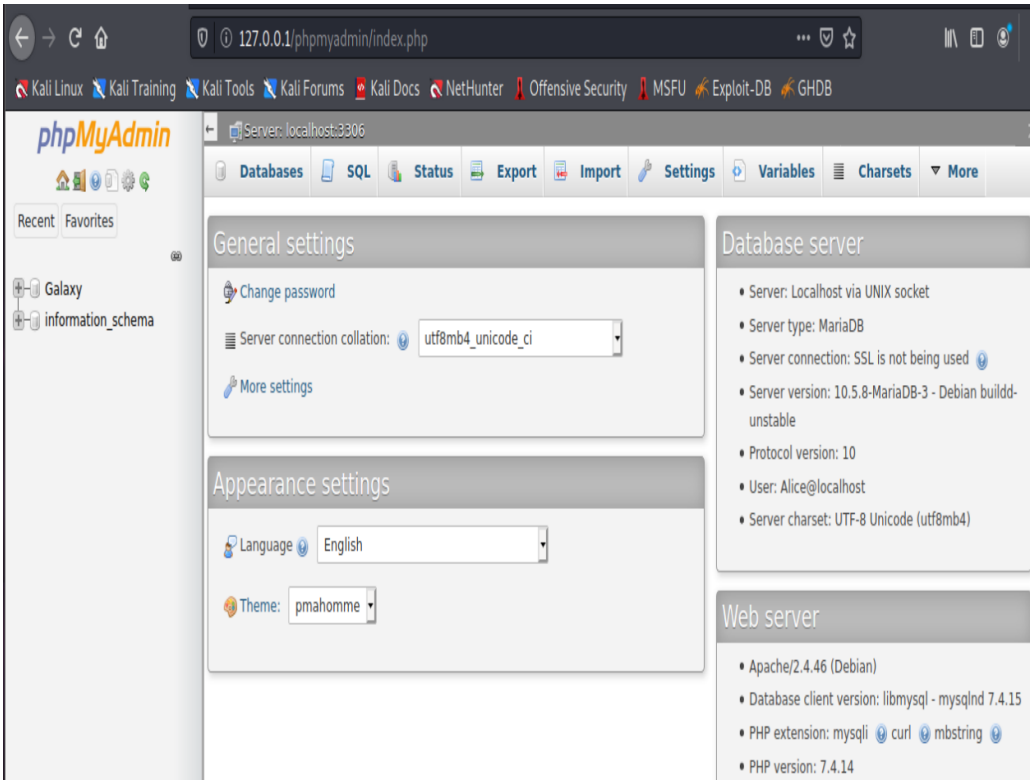

图 1-9 通过 phpmyadmin 用户 Alice 访问新增的数据库 Galaxy

1.2.2 关卡 2 一个响指

9）数据恢复：从备份的文件中恢复数据库 Galaxy

选择左侧 Galaxy 数据库，从右边功能中，选择“导入”，选择备份的数据 Galaxy.sql 文件完成导入。

图 1-10 通过 phpmyadmin 工具进行数据库导入

参考过程：如图 1-10 所示。

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：

_____；

另外，查看各表内数据，其中有没有安全隐患？如果有，请列出来。

_____

_____。

1.2.3 关卡 3 24 小时紧急任务

11）创建表

根据目前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。

参考语句：create table； //可以利用图形接口，结合语句预览，了解创建表格的命令行格式CREATE TABLE `AliceDB`.`PassengerInfo` (`IDNumber` CHAR(20) NOT NULL , `Name` CHAR(30) NOT NULL , `PhoneNumber` CHAR(20) NOT NULL , `Country` CHAR(30) NOT NULL , `Address` CHAR(30) NOT NULL , `Email` CHAR(50) NULL , `DateOfBirth` DATE NOT NULL , PRIMARY KEY (`IDNumber`(20))) ENGINE = InnoDB;

参考过程工具：phpmyadmin；

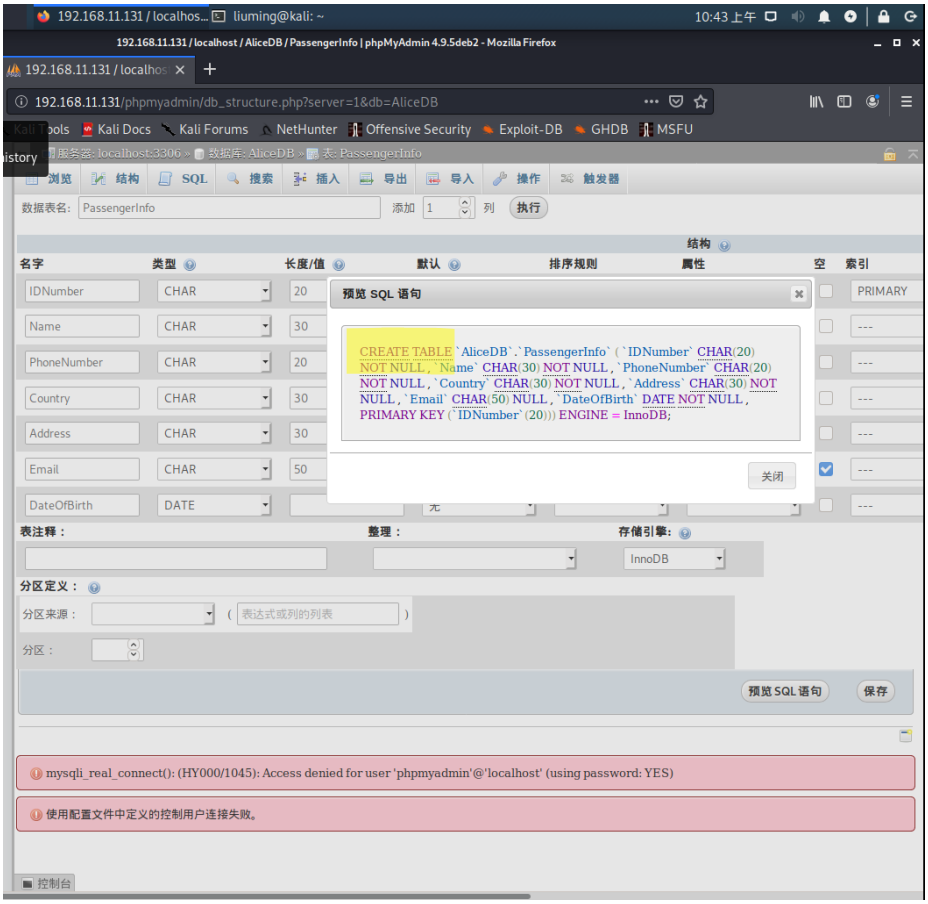

图 1-11 通过 phpmyadmin 工具增加数据库实例中的数据表

1.2.4 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。

增加数据 1 条、5 条、100 条，可以灵活运用其他工具生成 sql 脚本。*//思考：数据生成，有哪些办法？*

参考工具：phpmyadmin；//通过图形工具获得 sql 语句的模板，后续可以找编辑器，生成批量

参考命令：

INSERT INTO `PassengerInfo` (`IDNumber`, `Name`, `PhoneNumber`, `Country`, `Address`, `Email`, `DateOfBirth`) VALUES ('111138728716727172', 'LiLiang', '(86)15217845478', 'CN', 'RM 1-10, THRD, HY District, WH', 'LiLiang@wuhan.com', '1999-11-04')

1.2.5 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，修改航班信息；

参考命令：Update AirLineInfo set DepartureTime=Date_add(DepartureTime,INTERVAL 1 HOUR) where FlightNum ='JD5712'and DepartureTime LIKE "2020-05-28%"

1.2.6 关卡 6 人多力量大 Many Hands Make Light Work

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 帮导入另外 100 条乘客信息数据，这样你们都有 200 条数据了！

参考命令：

1. root 用户先授权 Alice，在数据库 Galaxy 上所有表的所有权限，并同意 Alice 将权限授予他人：

mysql -u root -p //root 进入 mysql；

创建 Alice 和 Bob 账号；

create user 'Alice'@'%' identified by '1234'; //如果 Alice 账号存在，则跳过

create user 'Bob'@'%' identified by '1234'; //如果 Bob 账号存在，则跳过

GRANT ALL PRIVILEGES ON Galaxy. TO 'Alice'@'%' WITH GRANT OPTION;*

// 对 Alice 授权，并退出系统；后续由 Alice 管理 Galaxy 数据库，并向其他用户授权。

2. Alice 进入系统，对 Bob 授权；

参考命令：

MariaDB [(none)]> grant all privileges on Galaxy. to 'Bob'@'%';*

Query OK, 0 rows affected (0.000 sec)

//Alice 退出 mysql 后，用 Bob 登录系统，查看数据库及表

1.2.7 关卡 7 百密一疏 OOps

15）删除数据（Delete）

以 Bob 账户，登录数据库；导入了 Bob 负责录入产生的另外 100 条数据；但 Bob 通过查询，发现了其中一名分销商的信息，因为私人原因，Bob 故意对该分销商信息进行了删除！

参考命令：

*select * from AirTicketDistributor; //Bob 查看分销商信息，发现 WangHu 账号的信息；*

delete from AirTicketDistributer where name='WangHu';

1.2.8 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；

参考命令：MariaDB [(none)]> revoke all on Galaxy. from 'Bob'@'%';*

Query OK, 0 rows affected (0.000 sec)Alice

// 思考：现在请测试 Bob 还能访问 Galaxy 数据库吗？

17）口令保护

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。

参考方法：利用 phpmyadmin，找到表格后，用语句 update 进行修改：

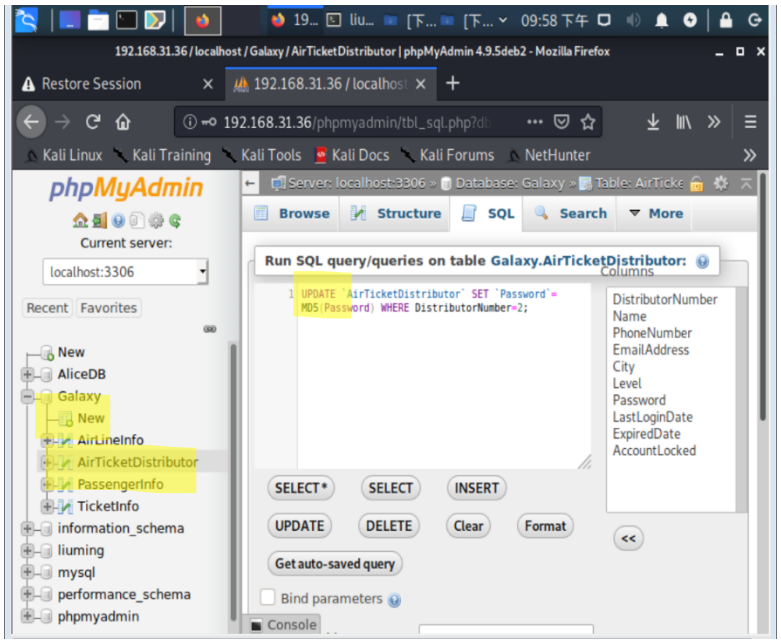

图 1-12 通过 phpmyadmin 工具修改数据表中数据

UPDATE `AirTicketDistributor` SET `Password`= MD5(Password) WHERE DistributorNumber=1;

图 1-13 通过 phpmyadmin 工具修改数据表中数据结果

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

参考命令：

update AirTicketDistributor set
PhoneNumber=HEX(AES_ENCRYPT(PhoneNumber,'1234'))
WHERE DistributorNumber=1;

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。

参考命令：

*SELECT * FROM `AirTicketDistributor` WHERE PASSWORD=MD5('123456') or Password='123456';*

// 将加密后的数据表导出，准备后面实验中继续使用其中的数据

e10adc3949ba59abbe56e057f20f883e

1.2.9 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？

1.3 实验问题分析与总结

（说明：每个实验任务，按照实验过程记录在 1.2 节中，实验中遇到的典型问题、对产生该问题的原因、解决要点的分析过程、本部分实验值得归纳的总结内容、实验的意见和建议，记录在 1.3 节中）

××

××

××

1.4 参考文献及资料列表

（说明：请将你完成实验过程中，为了完成任务或者解决问题，查阅的资料及时整理出来，列表记录到 1.4 节中，供其他阅读者学习和参考之用；给出的网址类型，将对应网址的资料，用浏览器打印功能，转成 pdf 文件；其他类型的，以 pdf 格式文件方式保存；参考资料打包提交；）