计算机系统安全实验报告

实验名称：数据库用户的权限管理设计与实现

班级：1703101

学号：1170300520

姓名：郭子阳

计算机学院

1. 实验环境

- macOS 10.15.2
- Node.js 12.13.1
- Mysql Community 8.0.18
- Electron

2. 实验成果

本实验设计的是一个基于银行场景的管理程序，在数据库中建立对应的数据库和表，并为对应的普通用户和管理员建立数据库用户并分配相应的权限，以保证用户无法越权操作。

创建数据库表与用户和权限分配语句如下：

```
DROP DATABASE IF EXISTS lab3;
CREATE DATABASE `lab3` DEFAULT CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
USE lab3;

CREATE TABLE `bank`
(
    id int PRIMARY KEY AUTO_INCREMENT,
    username varchar(255) UNIQUE,
    currency int NOT NULL,
    valid tinyint(1) NOT NULL
);

INSERT INTO `bank` VALUES (1, 'ziyang', 100, true);
INSERT INTO `bank` VALUES (2, 'exp', 30, true);

DROP USER if EXISTS 'admin'@'localhost';
DROP USER if EXISTS 'ziyang'@'localhost';
DROP USER if EXISTS 'exp'@'localhost';

CREATE USER 'admin'@'localhost' IDENTIFIED WITH mysql_native_password BY 'admin';
CREATE USER 'ziyang'@'localhost' IDENTIFIED WITH mysql_native_password BY 'ziyang';
CREATE USER 'exp'@'localhost' IDENTIFIED WITH mysql_native_password BY 'exp';

GRANT select,insert,update ON lab3.bank to 'admin'@'localhost';
GRANT select ON mysql.columns_priv to 'admin'@'localhost';
GRANT Grant option ON lab3.bank to 'admin'@'localhost';
GRANT select(currency), select(username), select(valid) ON lab3.bank TO 'ziyang'@'localhost';
```

```
28 GRANT select(currency), select(username), select(valid) ON lab3.bank TO
   'exp'@'localhost';
29
30 FLUSH PRIVILEGES;
```

主要使用的表为lab3.bank，结构如下：

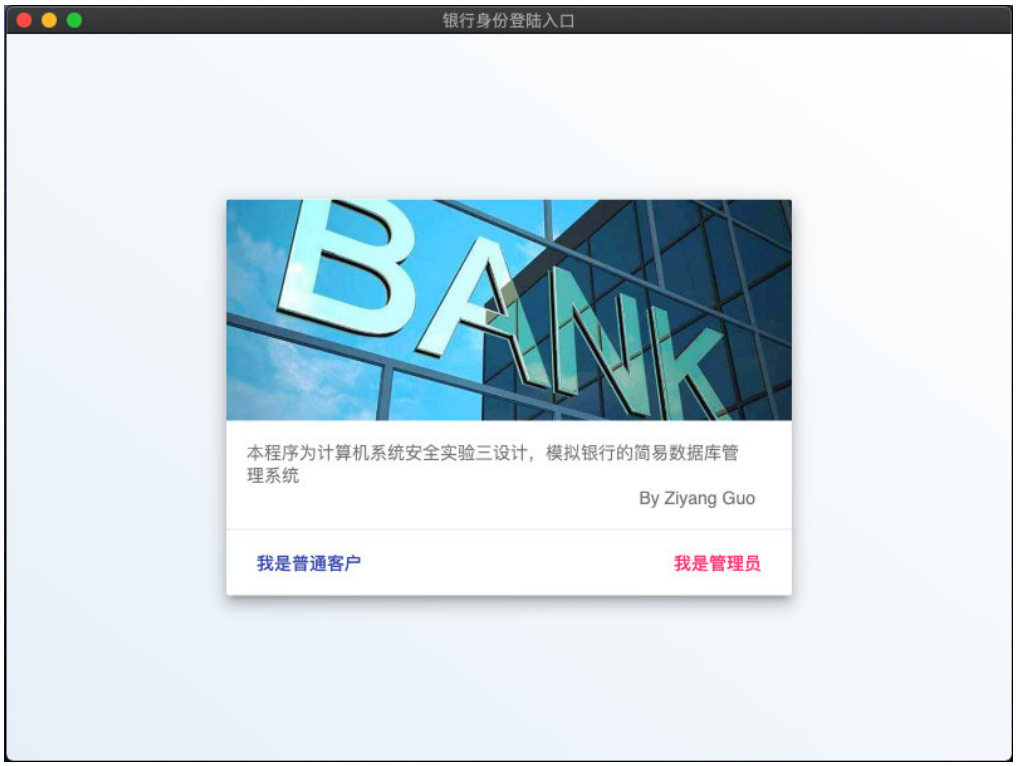
属性名称	属性类型	属性说明	主键
id	int	记录唯一ID	是
username	varchar(255)	用户名	
currency	int	用户账户余额	
valid	tinyint(1)	用户账户是否有效	

初始，admin用户作为管理员，对lab3.bank表拥有全部增查改的权限，和mysql.column_priv表的查询权限（用于确认其他用户的权限），且可以将自己的权限赋予其他用户和收回，admin对于其他表没有任何权限。并建立两个初始普通用户：exp和ziyang，都只对lab3.bank拥有查询权限。所有用户的密码和用户名相同。

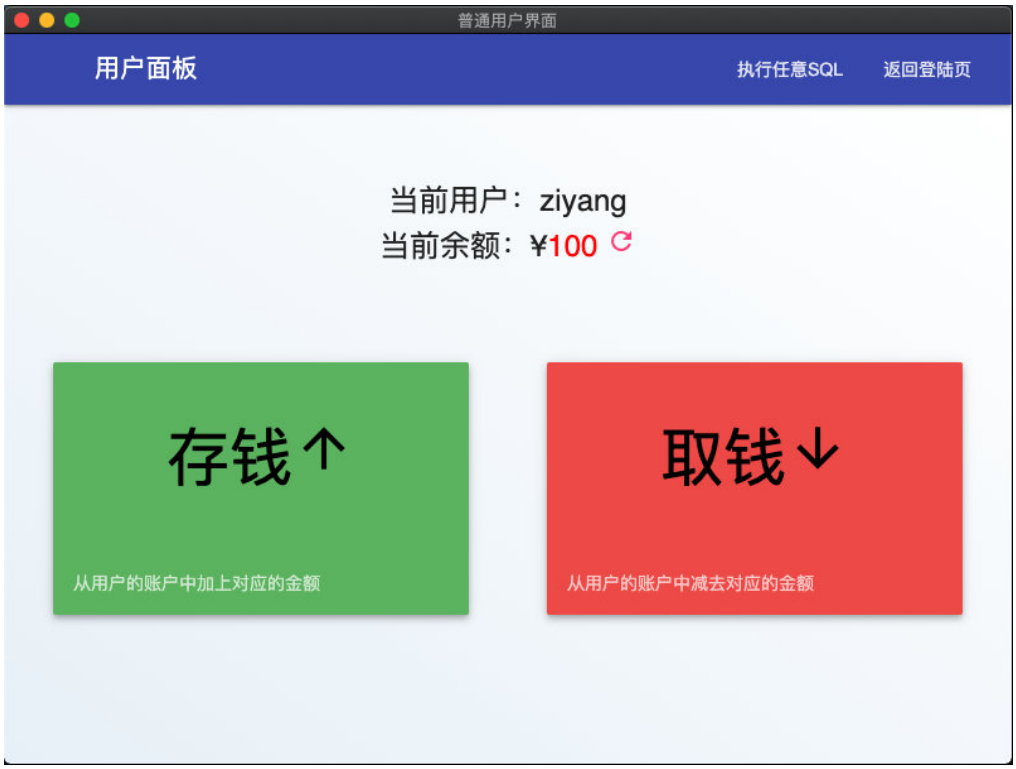
图形化操作界面使用的是Electron + 前端技术构建，可以保证跨平台一致。

界面如下：

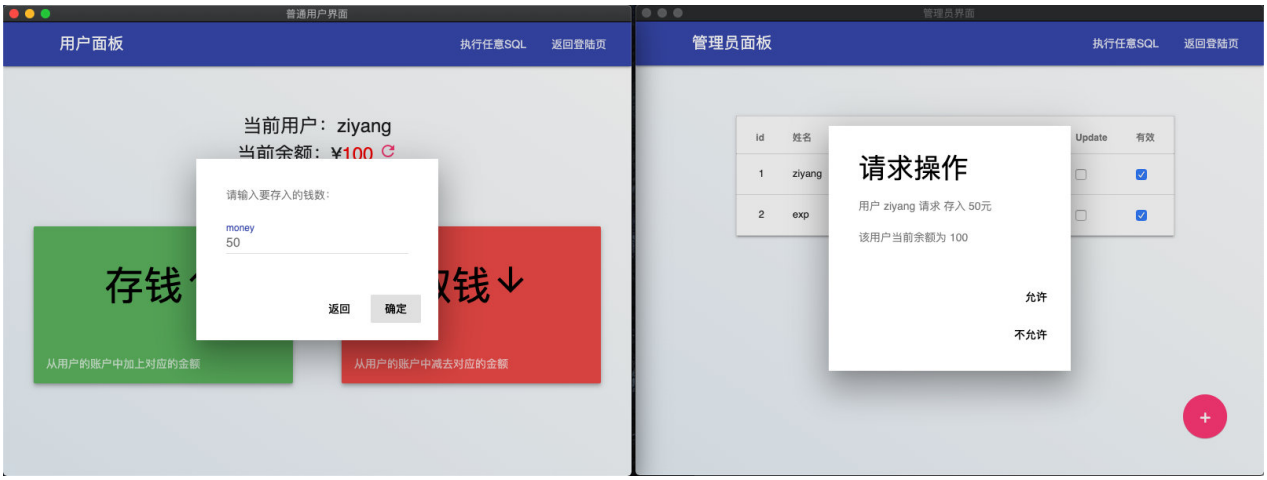
主界面：



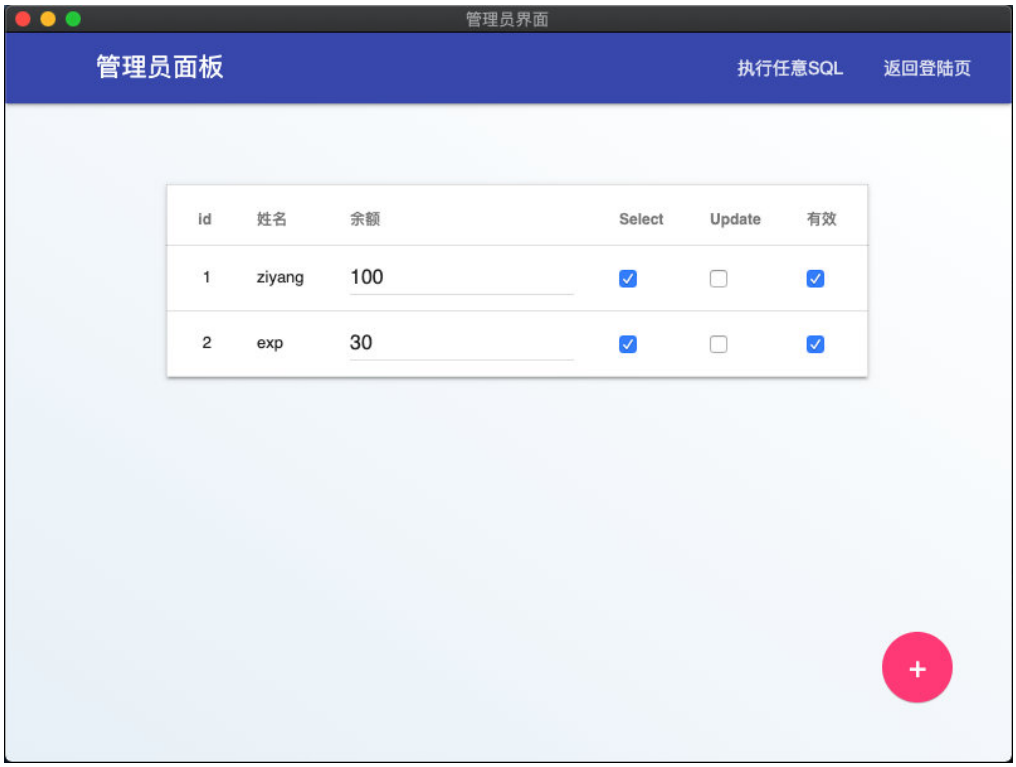
普通用户操作界面：



由于用户对表没有UPDATE权限，所以当用户请求存钱或者取钱时，是通过Socket通信想管理员端发送请求，管理员可以同意或者不同意操作，如果同意，则会对表中用户的记录进行update：



管理员可以在管理员界面对用户的权限进行操作，包括直接设置用户的余额、查询的权限、更新的权限以及用户是否有效：



有效字段的设置是为了删除用户使用，当用户字段的有效位被设置为0时，该用户相当于不存在，则无法登陆：