



哈爾濱工業大學  
HARBIN INSTITUTE OF TECHNOLOGY

**2019 年秋季学期**  
**计算机学院大三**  
**计算机系统安全课程**

**Lab 4 实验报告**

姓名	冯帅
学号	1170301027
班号	1703201
电子邮件	1170301027@stu.hit.edu.cn
手机号码	15765513201

## 实验 4 完整性访问控制系统设计与实现

### 一、实验环境：

**Win10**

### 二、实验工具：

**IntelliJ IDEA, MySQL, Navicat**

### 三、编程语言：

**JAVA**

### 四、实验要求：

#### 一、系统设计说明：

设计完整性访问控制系统，实现系统，并满足某商业公司的完整性访问控制需求。

(1) 配合第 7 章，为商业公司设计系统，提出针对该公司业务需求的应用系统安全策略。安全策略中要明确指明对公司的要求与约束, 和对客户的要求与约束, 区分各自的责任。(当出现商业公司与客户间意见分歧或法律纠纷时，安全策略可作为仲裁依据)

(2) 配合第 9 章 为商业公司设计系统，应用系统满足完整性需求。需求中包含责任分离、功能分离、审计。

(3) 具体指明是哪类应用系统，应用背景范围不限，可以是银行、股票等，符合商业系统完整性需求即可。

(4) 4 学时，每人独立完成。

#### 二、系统要求：

(1) 给出应用系统的安全策略文档。

(2) 提供交互界面，能够完成录入、查询等功能。

(3) 满足责任分离、功能分离原则。

(4) 保存审计日志。

(5) 遵循 Clark-Wilson 模型，定义应用系统的完整性限制条件。

(6) 遵循 Clark-Wilson 模型的证明规则和实施规则，并在设计报告中有所体现。

## 五、实验报告：

### 1. 系统安全策略文档

用户身份有客户和管理员两种。管理员兼审计人员，可以审查日志，同时能够查看当前注册用户信息（只包含用户名），能够处理客户请求（如果有）。

客户需进行注册，每一个客户拥有一个唯一的注册用户名，服务器保存注册密码用于验证，但对他人不可见。

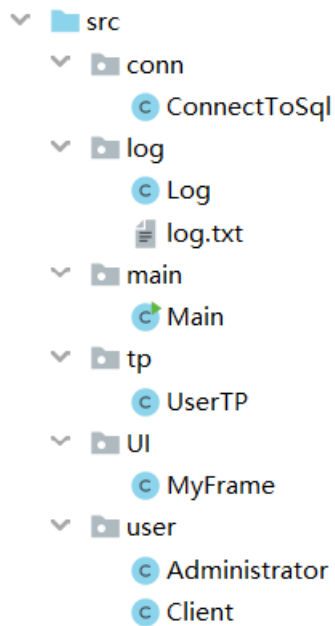
客户注册成功可以根据注册的用户名和密码进行验证登录，登录成功的客户能够进行余额查询，存储，取钱和转账功能。

显然在 Clark-Wilson 模型中，客户金额是 CDI，TP 是客户的转存取操作，系统验证保护完整性，保证有效 tp 执行之后满足收支相抵。

客户对余额的查询功能不涉及完整性，不需要经过管理员同意，但是客户进行转账以及存取功能时，需要在线管理员同意。客户提交申请之后，系统核实是否金额有误（为负或者超过存储余额）转至错误界面予以提醒，若操作无误，将申请提交至系统并检查在线管理员的是否存在，若管理员存在，则将申请提交至在线管理员的界面，管理员界面显示相关请求信息，决定是否予以受理。若无在线管理员，则申请正确提交之后跳出登录界面要求管理员登录，然后决定是否同意。

### 2. 交互界面

## 系统架构解析：



**ConnectToSql:** 唯一管理服务器数据库

**Log:** 记录审计日志

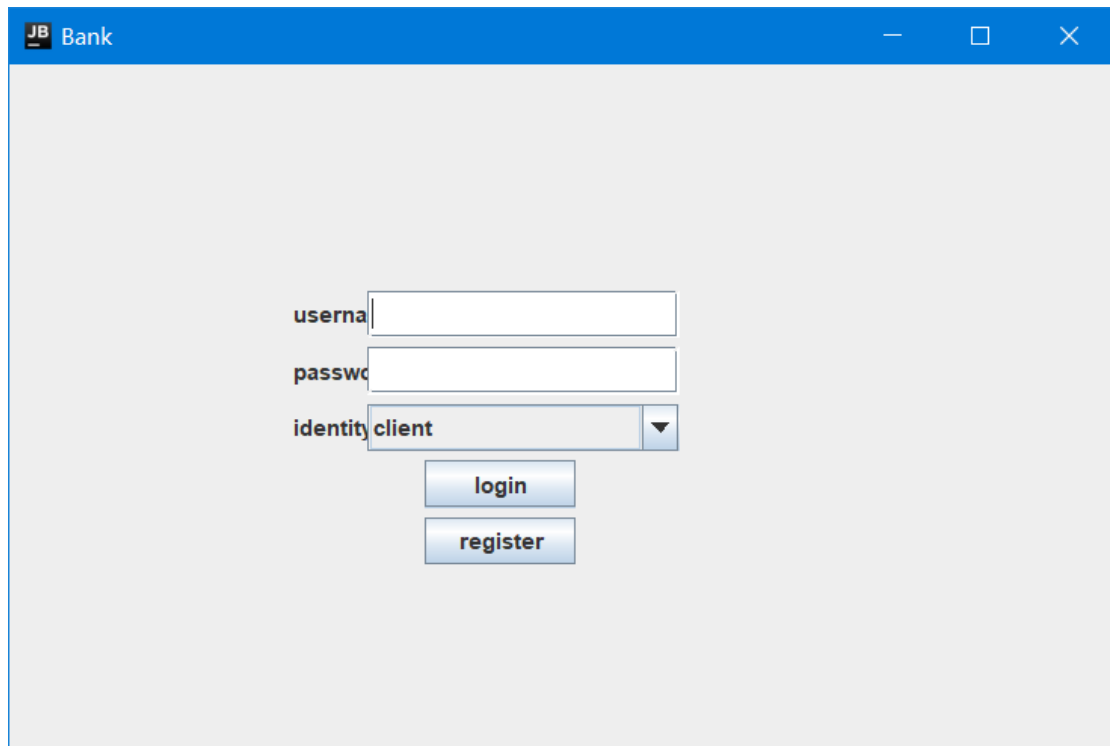
**Main:** 程序入口

**UserTP:** 唯一指定用户（包括管理员和客户）各种操作

**MyFrame:** UI 实现，包括用户登录，注册，各种操作的界面

**user:** 两种身份

## 登录界面



The image shows a web browser window titled "JB Bank". The page has a light gray background. In the center, there are three input fields: "username", "password", and "identity client". The "identity client" field is a dropdown menu with a downward arrow. Below these fields are two buttons: "login" and "register".

JB Bank

username

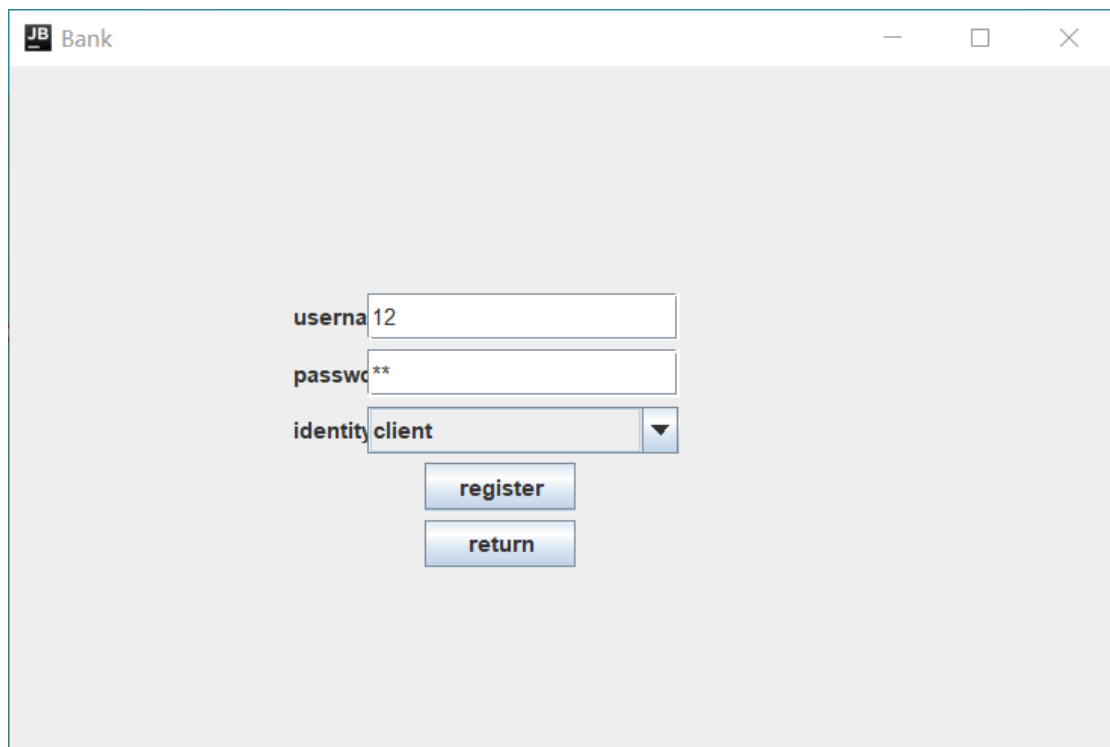
password

identity client

login

register

注册界面



The image shows a web browser window titled "JB Bank". The page has a light gray background. In the center, there are three input fields: "username", "password", and "identity client". The "username" field contains the text "12". The "password" field contains two asterisks "\*\*". The "identity client" field is a dropdown menu with a downward arrow. Below these fields are two buttons: "register" and "return".

JB Bank

username

password

identity client

register

return

管理员界面

JB Bank

username

root

password

\*\*\*\*\*

identity

administrator

login

register

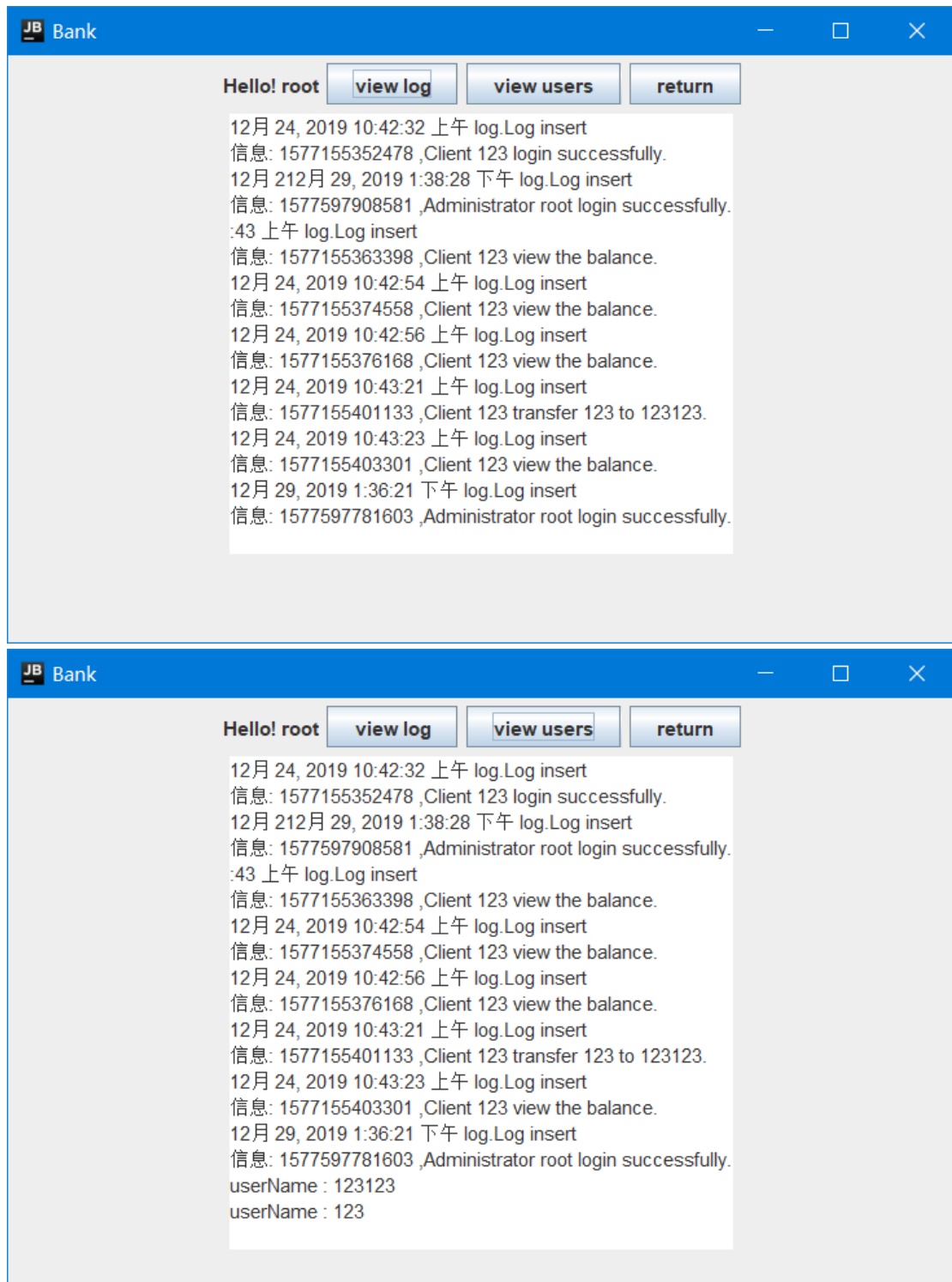
JB Bank

Hello! root

view log

view users

return



客户界面

JB Bank

—

□

×

username

123

password

\*\*\*

identity

client

▼

login

register

JB Bank

—

□

×

Balance Inquiry

Deposit

Withdraw

Transfer

Return



JB Bank

balance: 279

return

申请界面

JB Bank

opposit

123123

money:

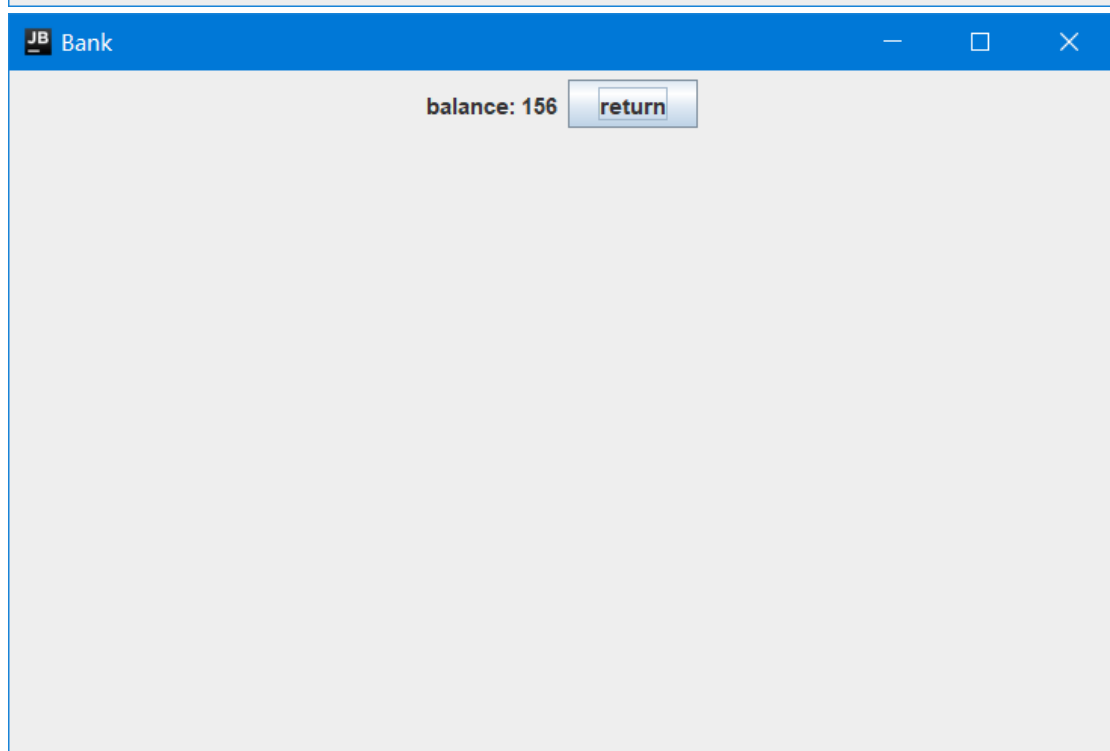
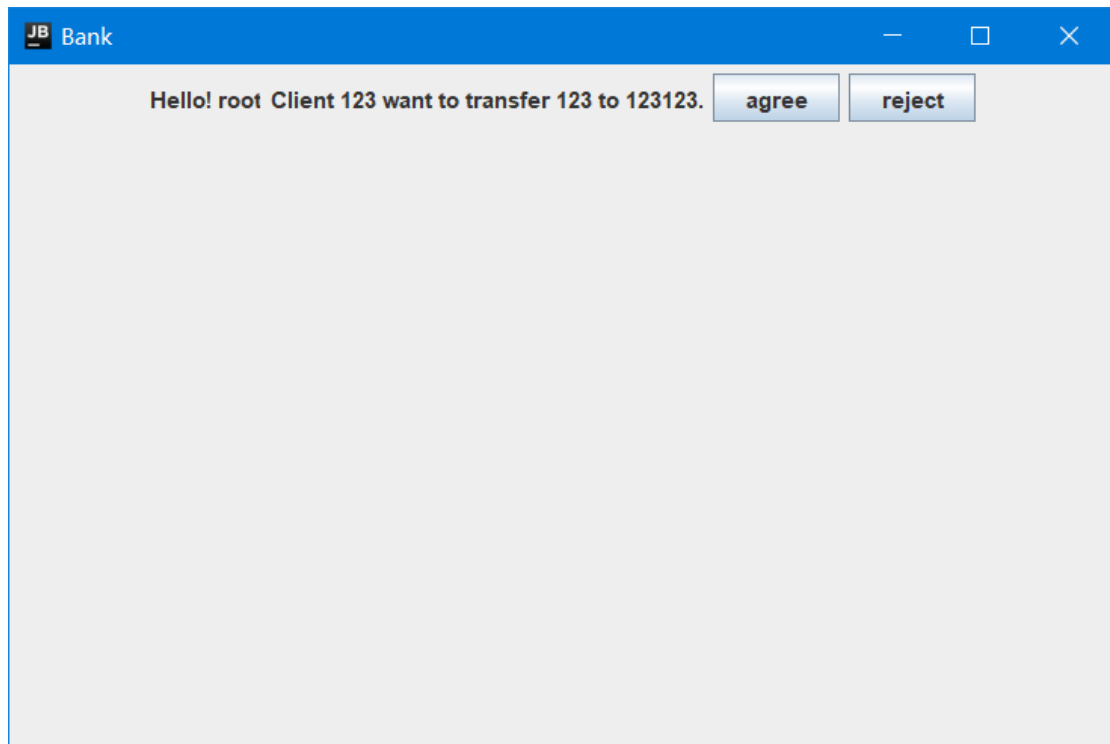
123

confirm

return

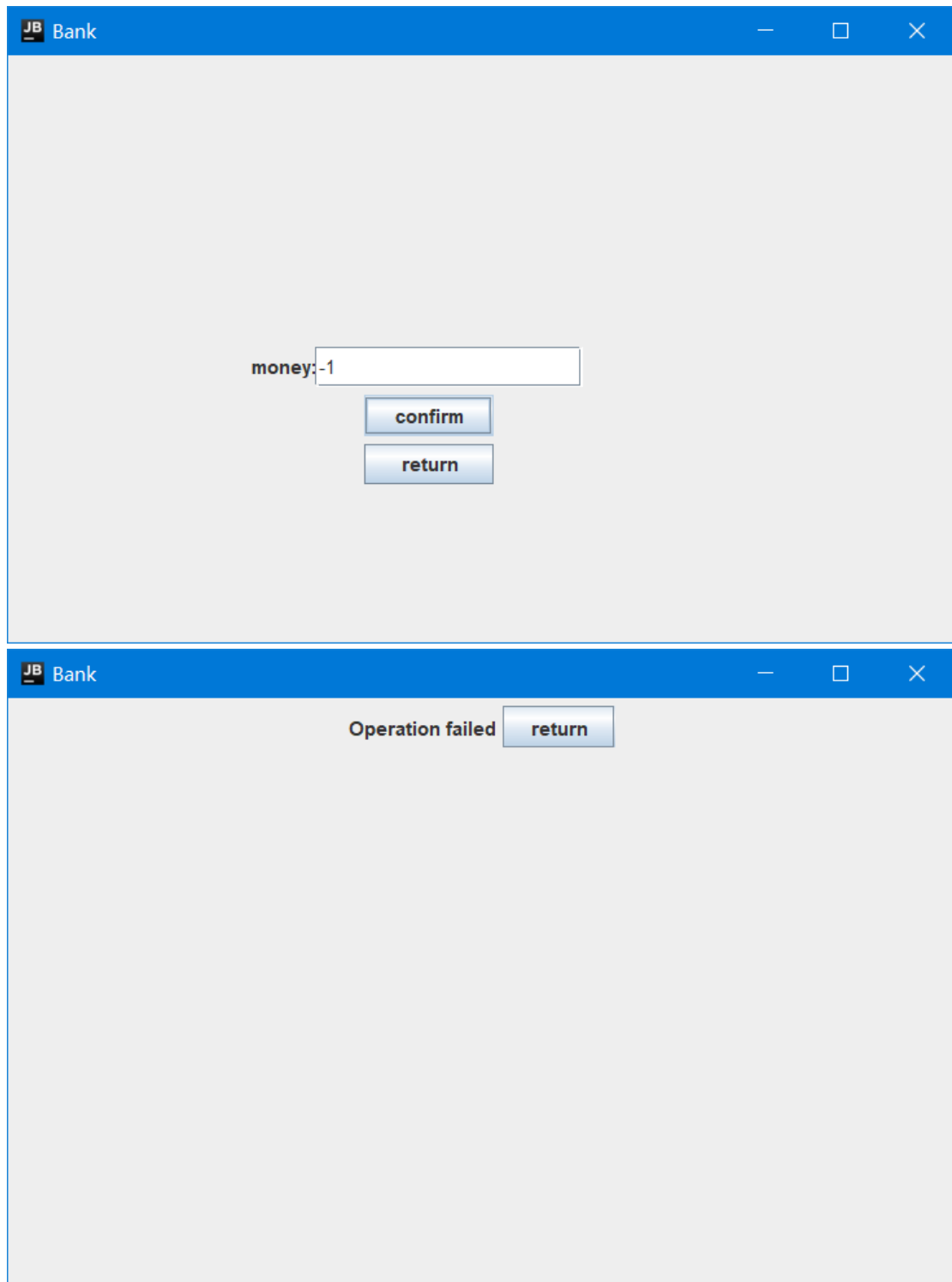
userName	password	balance
123123	123123	915
123	123	279

管理员确认界面



	userName	password	balance
▶	123123	123123	1038
	123	123	156

错误界面



### 3. 满足责任分离，功能分离原则

责任分离：用户存取转账等对敏感数据的操作需要在线管理员同意，并且强制要求管理确认才能执行。

功能分离：只有系统程序拥有对数据库的修改权限，对外只是提

供接口，有且只有登录客户拥有对自己数据有修改的权限（只转账存取等操作）。

#### 4. 保存审计日志

审计日志：管理员兼审计人员，用户的每一次操作都被记录到审计日志中，详见上图管理员界面中的 view log

#### 5. 遵循 Clark-Wilson 模型，定义应用系统的完整性限制条件。

Clark-Wilson 模型需要满足下面几点：

- 1) 主体必须被识别和认证
- 2) 客体只能通过规定的程序进行操作
- 3) 主体只能执行规定的程序
- 4) 必须维护正确的审计日志
- 5) 系统必须被证明能够正确工作

所有系统用户（管理员和客户）为主体，主体需要进行身份认证，用注册时的密码。客户只能执行指定的操作，系统维护审计日志，管理员根据日志确保系统正确的执行指定的程序，维护一致性和完整性

#### 6. 遵循 Clark-Wilson 模型的证明规则和实施规则，并在设计报告中有所体现。

证明规则 1：

当任意 IVP 运行时，它必须保证所有的 CDI 处于有效状态

当用户登录后，只能查看当前余额，没有如要进行对数据库中的数据进行操作。只能提交申请，待管理员同意后，才能更改数据库。

证明规则 2:

对相关联的 CDI, 一个 TP 必须将这些 CDI 从一个有效状态转到另一个有效状态

在管理员同意后, 会进行存取钱操作操作, 同时记录这一操作, 操作后进行比较, 保证其处于完整性的状态

证明规则 3:

系统执行操作时, 符合责任分离原则。

模型需要保证用户身份和执行代码身份一致。所以需要验证身份。用户进行存取钱操作时只有经过管理员同意才能操作数据库

实施规则 1:

系统要维护关联关系, 保证经过验证的 TP 操作相应的 CDI

在用户提出申请后, 管理员同意, 就代表该操作已经被验证。被验证的这个账单可以对数据库中, 相应的存款金额进行更改。

实施规则 2:

TP 操作 CDI 时, 保证操作用户有权对相应 CDI 做操作, TP 所代表的用户是 CDI 的真实用户

经过确认的申请, 即管理员同意后, 可以对数据库中的 CDI (即客户的存款金额) 进行更改。

实施规则 3:

系统执行操作时, 需要用户和管理员共同执行, 符合责任分离原则

模型需要保证用户身份和执行代码身份一致

满足责任分离原则, 客户和管理员都不能单独对存款金额进行更改, 只有用户申请, 管理员同意后系统进行操作并记录日志。

实施规则 4:

只有可以授予 TP 访问规则的主体才能修改列表中相应的表项，授权主体不能执行 TP 操作

只有用户提出申请，管理员确认才能进行 TP 操作。单独授权的管理员，没有执行 TP 操作的能力。

## **六、心得体会：**

为商业公司设计一个管理系统需要考虑方方面面，时间有限考虑的不够全面，只做了表面的功能，基本实现了银行必须实现的功能，还有诸多考虑不周的地方。

## **七、附录（源代码）：**

详见报告外的工程文件