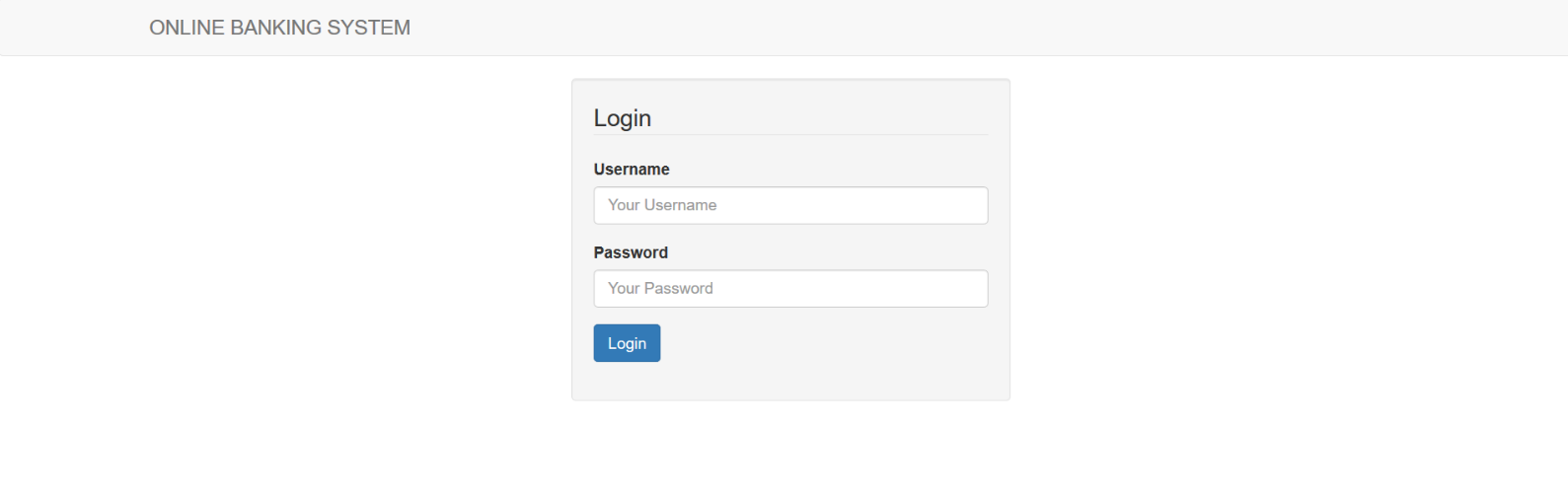
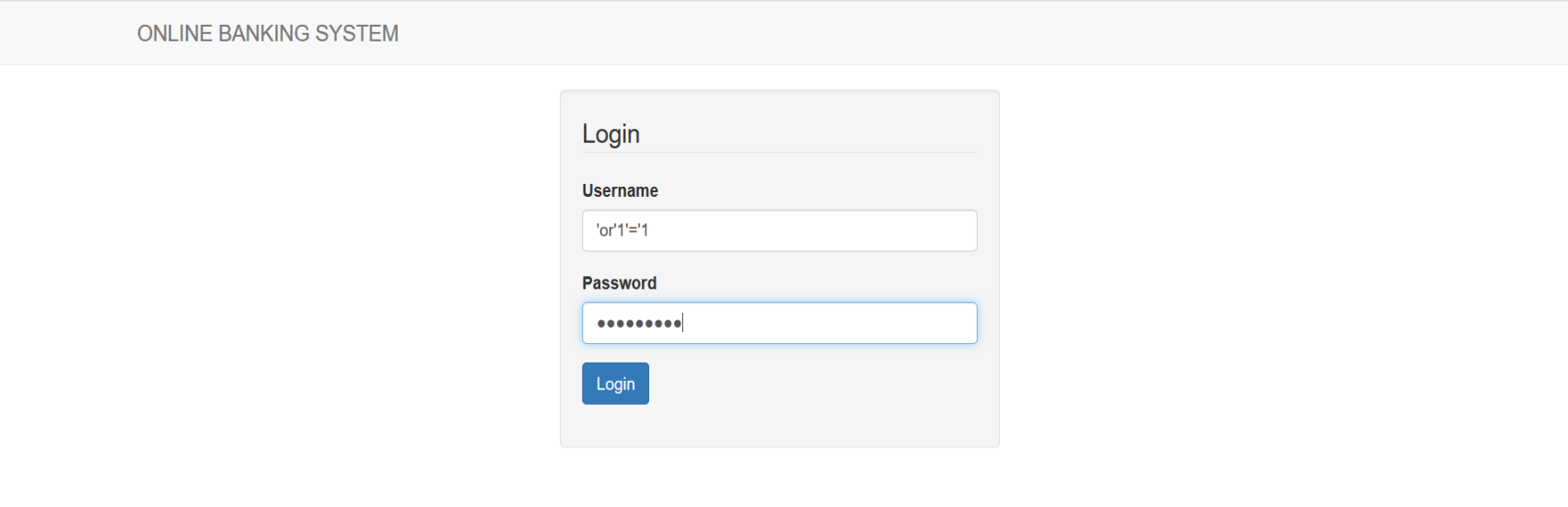
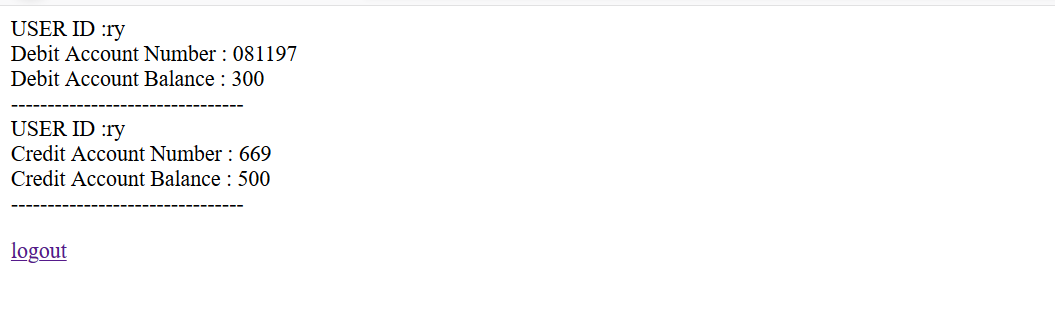
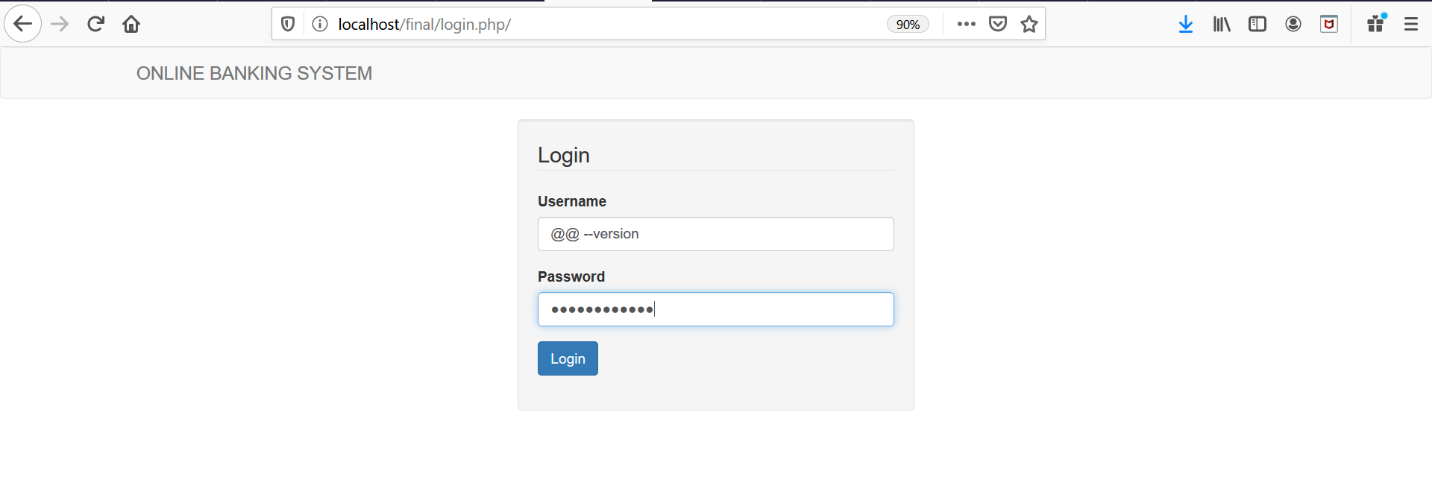
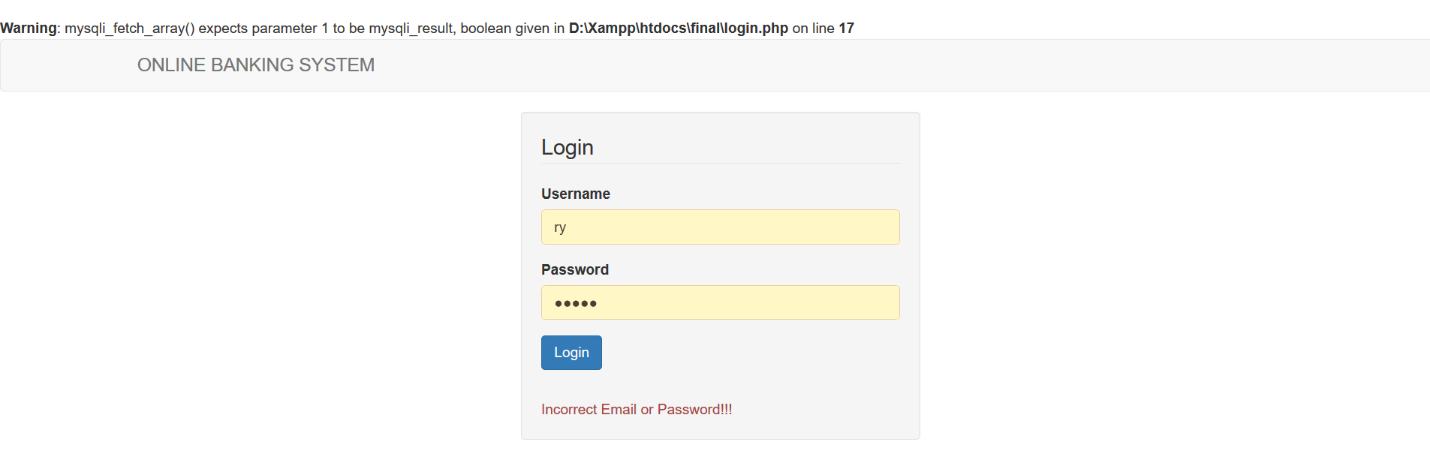
IDBMS Assignment

Rahul Reddy Yerva

16231559

Part -1:

* I have designed a web application on Online banking system using MySql and PHP.
* Where a user can know about his account and debit details.
* Below is the screen shot of login page
* First SQL-Injection , when I have given
* We are able to login to the page dashboard.php
* Second SQL Injection



* The second SQL – Injection is about Error based injection where the hacker gets to know the type of database technology the application is using. Here, we get to know that the application is using MySQL in the backend.

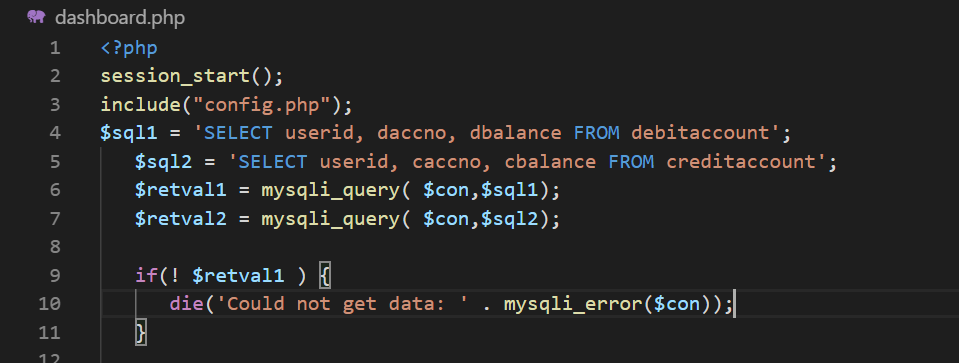
**Code Zip for Part1:**

**Config.php:** To connect to the database

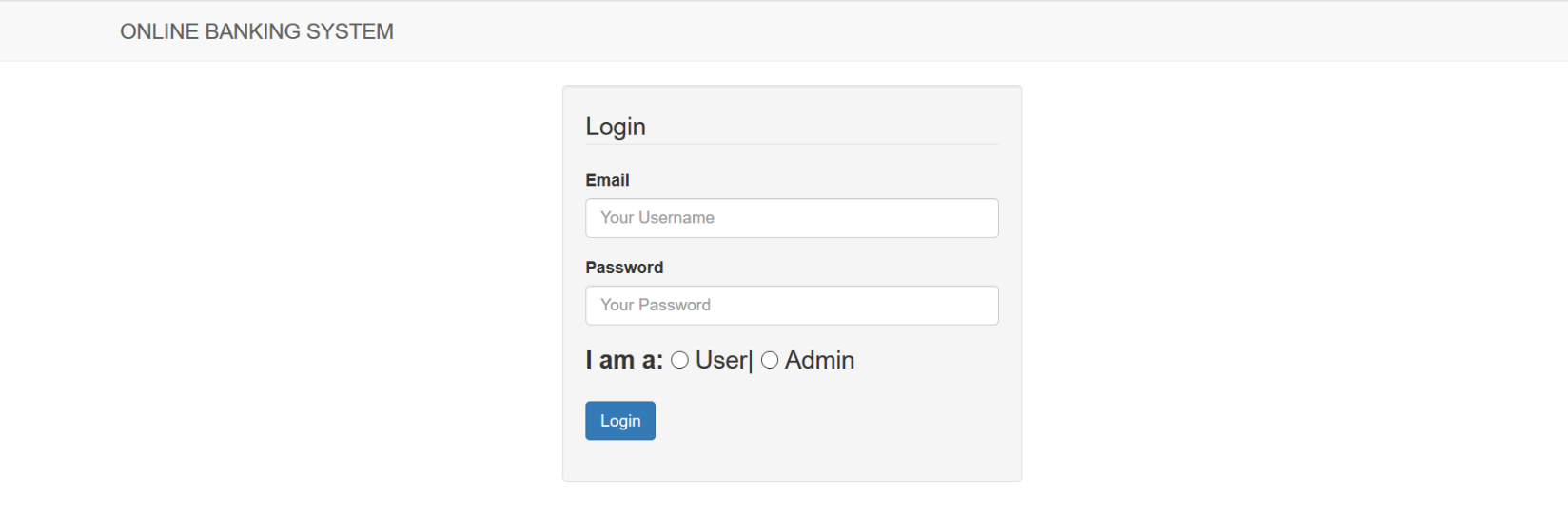
**Login.php:** Below is the screen shot for Login query.

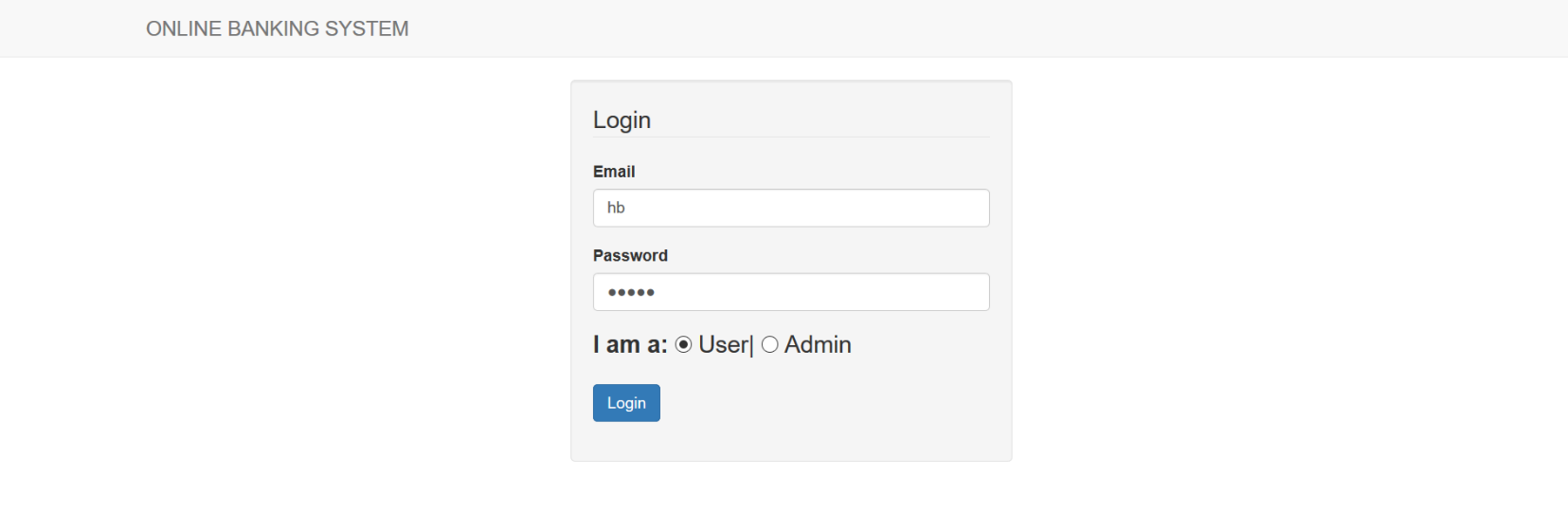


**Dashboard.php:** Below is the code zip for accessing the data



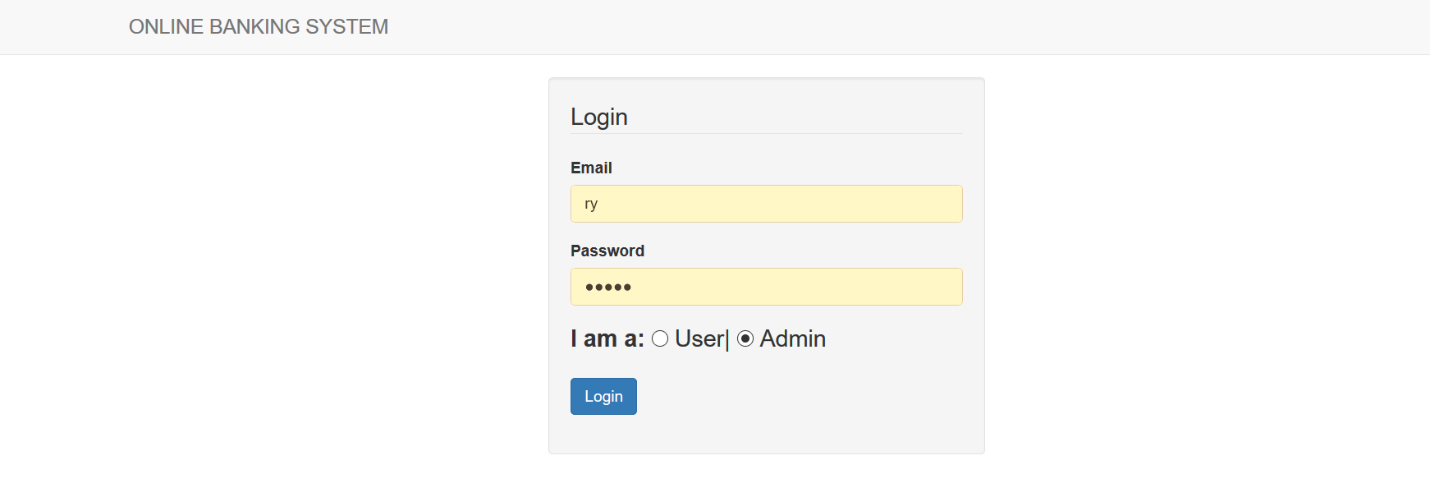
**Part-2:**

* In part-2, I have introduced two users and in the database I have introduced a new column in the data base with the name usertype, where there are two types of users admin and user.
* Below is the screenshot for login page

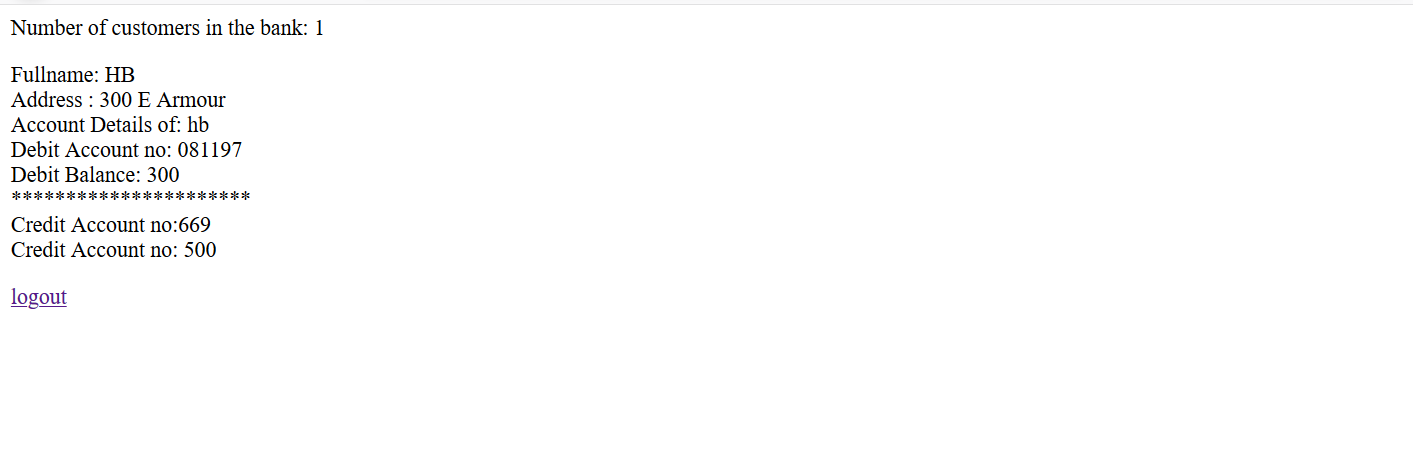


When the user with user privilage with username ‘hb’ logs in she gets to know the account details.

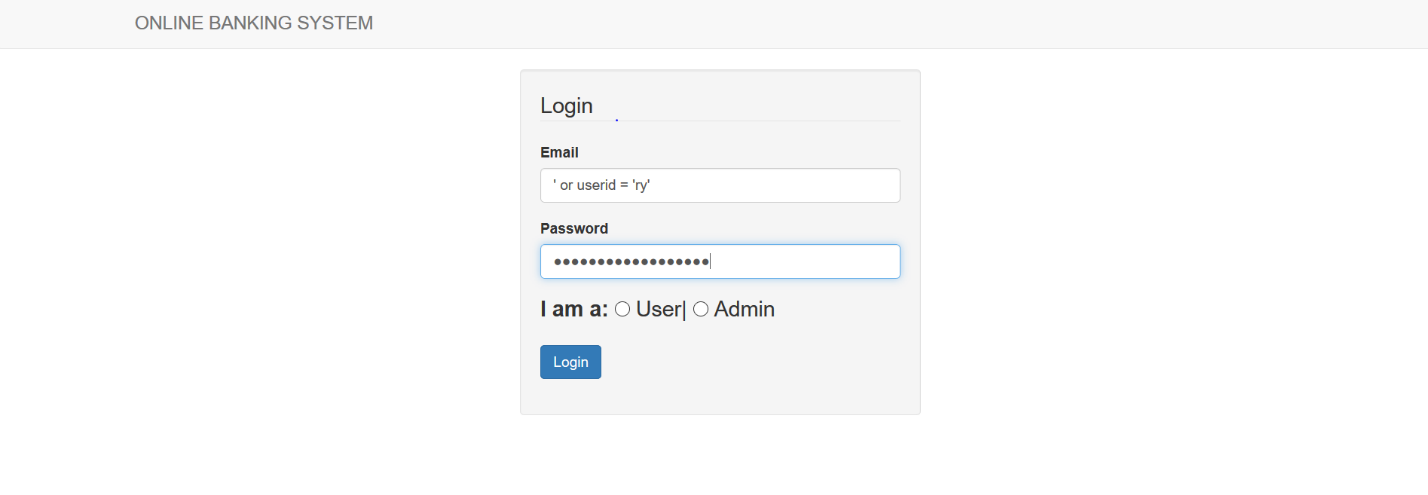
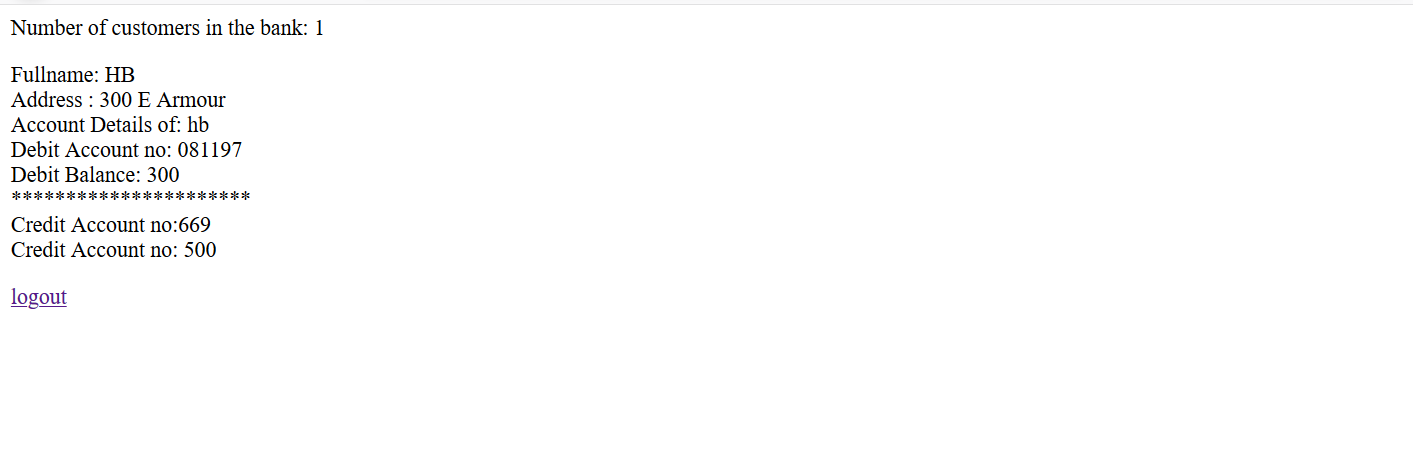
When the user with admin privilege with admin name ‘ry’ logs in he gets to know the customer details, he is able to see much more information about the customers.



Below is the admin view

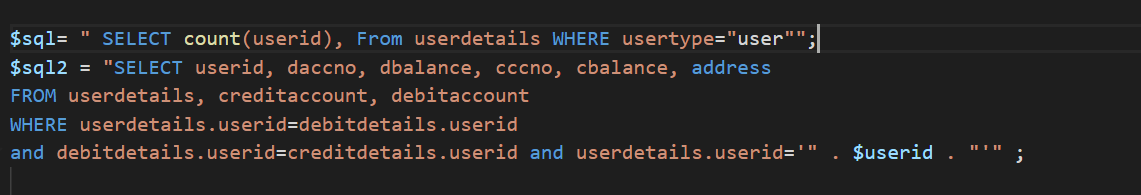


Even after this below is the sql injection screen shot

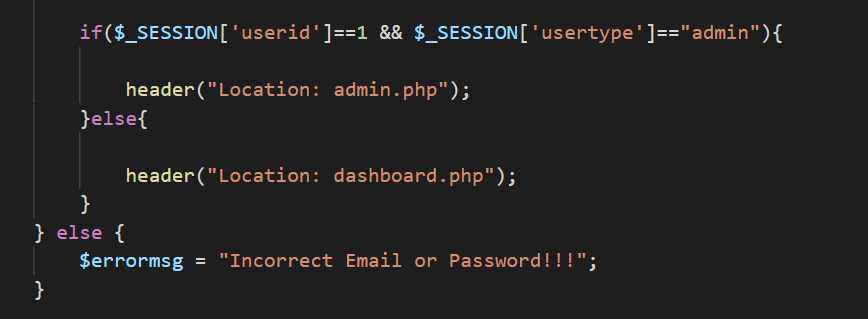


**Code Zip of Part-2:**

**Admindashboard.php**

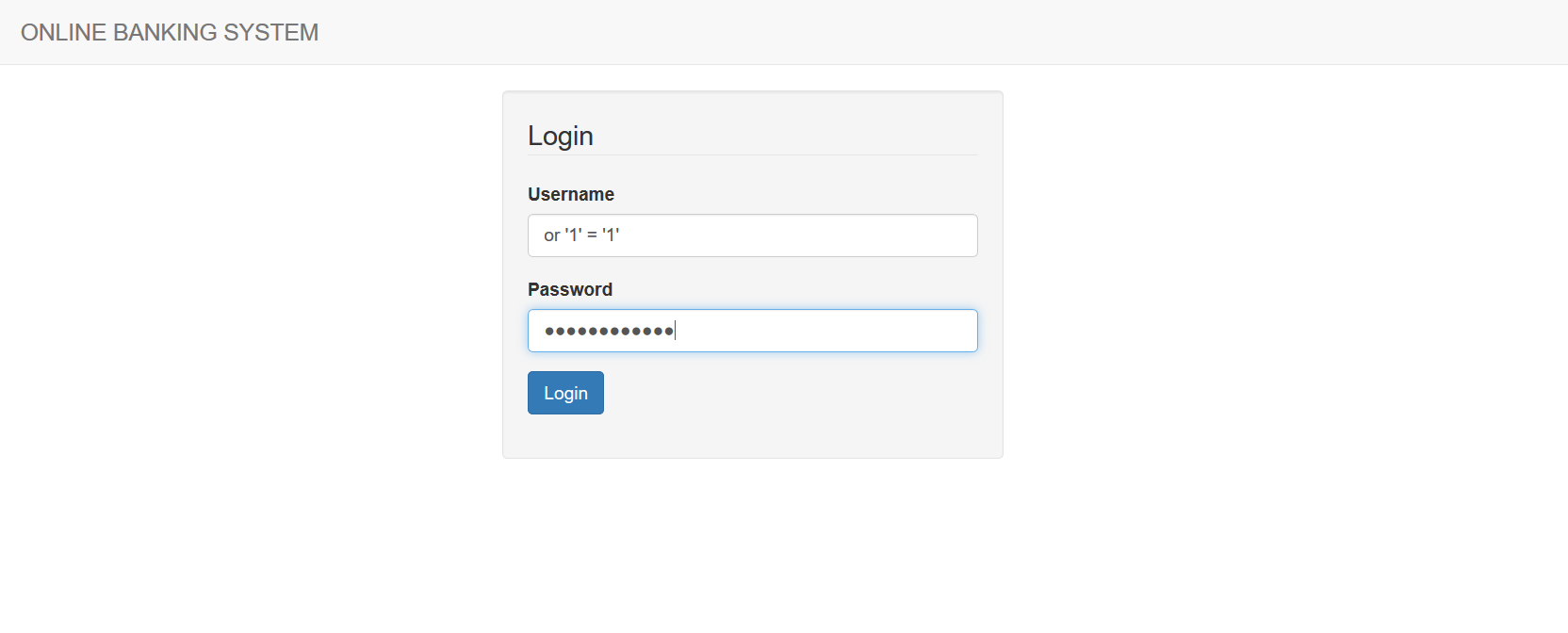


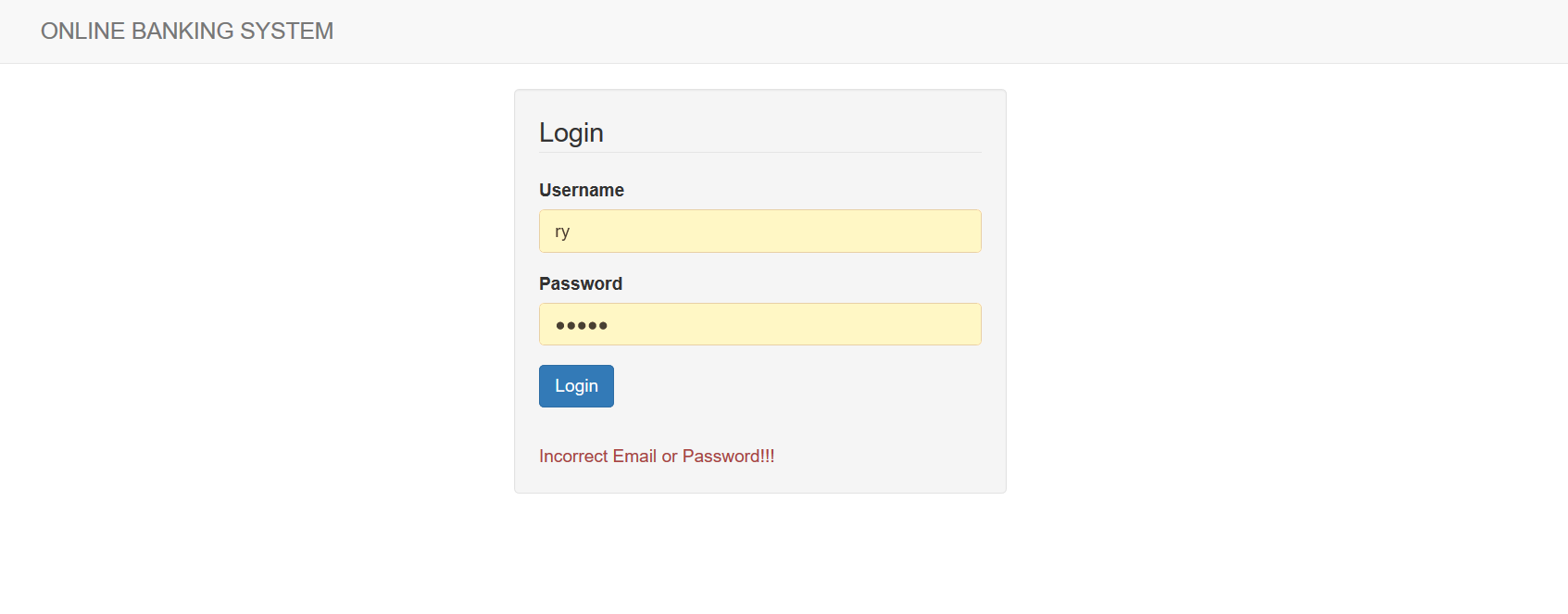
**Login.php**



**Part3:**

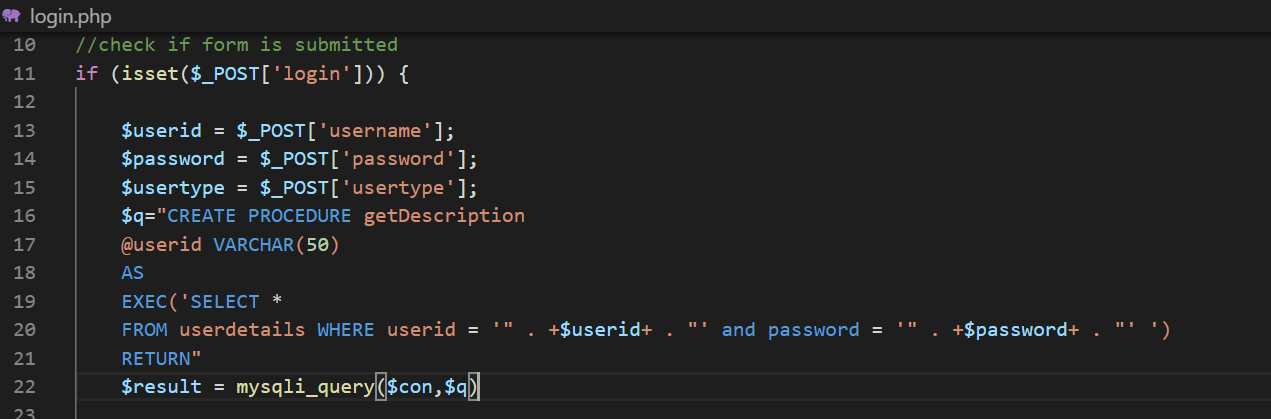
* I have used stored procedures in the code and then tried , I could see that it is able to prevent sql injection and logging in correctly





**Code Zip for Part-4**

**Login.php**



**Part-4:**

* I have saved the username and password of the database connection inside the variables $user and $password in config.php file as below.



* It is not safe for the passwords and usernames to save in php files, as sometimes hackers may have a view at it, so it is recommended to store these usernames and passwords in a configuration file outside webroot and we need to make sure that it is not public accessible.
* We can also prevent it by encrypting the username and passwords by using different software available today
* References:

<https://security.stackexchange.com/questions/13353/is-it-safe-to-store-the-database-password-in-a-php-file>

<https://www.codementor.io/ccornutt/keeping-credentials-secure-in-php-kvcbrk55z>

**Part-5:**

* Data Breaches has gained much attention as businesses now a days are depending on digital data stored inside a databases
* There are 4 types of data breaches

Ransomware

Malware

Phishing

Denial of service

* Proper architecture and proper malware protection of the applications will have been able to save the business from data breaches.
* Now a days data insurance is becoming popular, where we will be able to get the data insured.
* <https://digitalguardian.com/blog/history-data-breaches>
* <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>