The FCCU banking application is vulnerable to SQL injection, by not properly sanitizing user input unauthorized commands are able to be run on the database.

To solve this, all queries that take user input should use a PHP function called prepared statements. This way the database knows what query it should expect, along with the data types of its input, so unauthorized queries can not be run.

The importance of this change can not be understated, while an attacker can not gain root access to our server, they can access all user data (including name and ssn) and make unauthorized transactions for up to as much money as they wish. In addition to making all queries prepared statements, alterations to users' balances need to be done in transactions. Through a carefully crafted sql injection, an attacker can send money to another account, and have the query that deducts that amount from their account fail, which essentially generates money from thin air. And since an attacker can log into any account, after generating as much money as they please into an account, they may transfer it to any bank they please, most likely under their control.