Intro to Computer Security COMP 2300

Professor Sashank Narain

UMASS Lowell, Fall 2024

Class Project, Milestones 1-3

Authors: Patricia Antlitz, Andrew Jacobson, Paul Warwick, Flower Letourneau

The README.md of this project contains all instructions on how to properly run it.

GitHub Repository: https://github.com/andrewjacobson5/secureFTP

This project makes use of certificates to establish a mutual TLS connection which is used to secure the communication channel between the client and the server. This confirms both the client and server have certificates signed by the same Certificate Authority. Although the certificates are being properly generated, they are not fully integrated into the code quite yet. As of right now the main form of data security is password hashing and deletion, error handling and garbage collection. The certificates functionalities will be fully implemented on the part two of this project.

Given this information, to run this code, you must first generate the certificates:

You can run either `make generate-certificates` OR

`./generate_certificates.sh` if you have a **Unix or Linux** system.

You can run either `make generate-widows-cert` OR

`./generate_windows_cert.sh` if you have a **Windows** machine. Please note, the

windows certificate generation was not tested since none of us had a windows machine available at the moment to try it out.

This project also makes use of the **bcrypt** library. To run the code, you might need to use a virtual environment.

You can run the following commands on **Unix or Linux**: `python3 -m venv venv` and then: `source venv/bin/activate`

For **Windows**: `python3 -m venv venv`

and then: `.\venv\Scripts\activate`

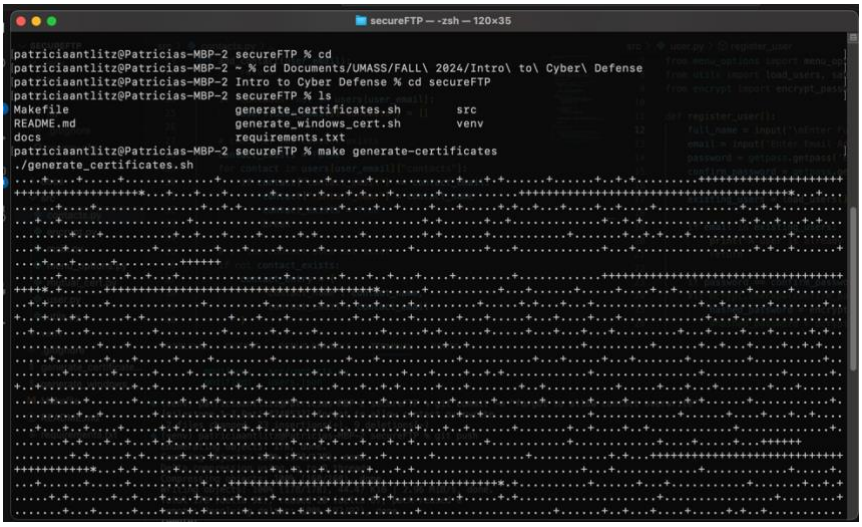
After activating your virtual environment, you can install **bcrypt:**

Run `make install` to automatically install the dependencies OR run `./requirements.txt`

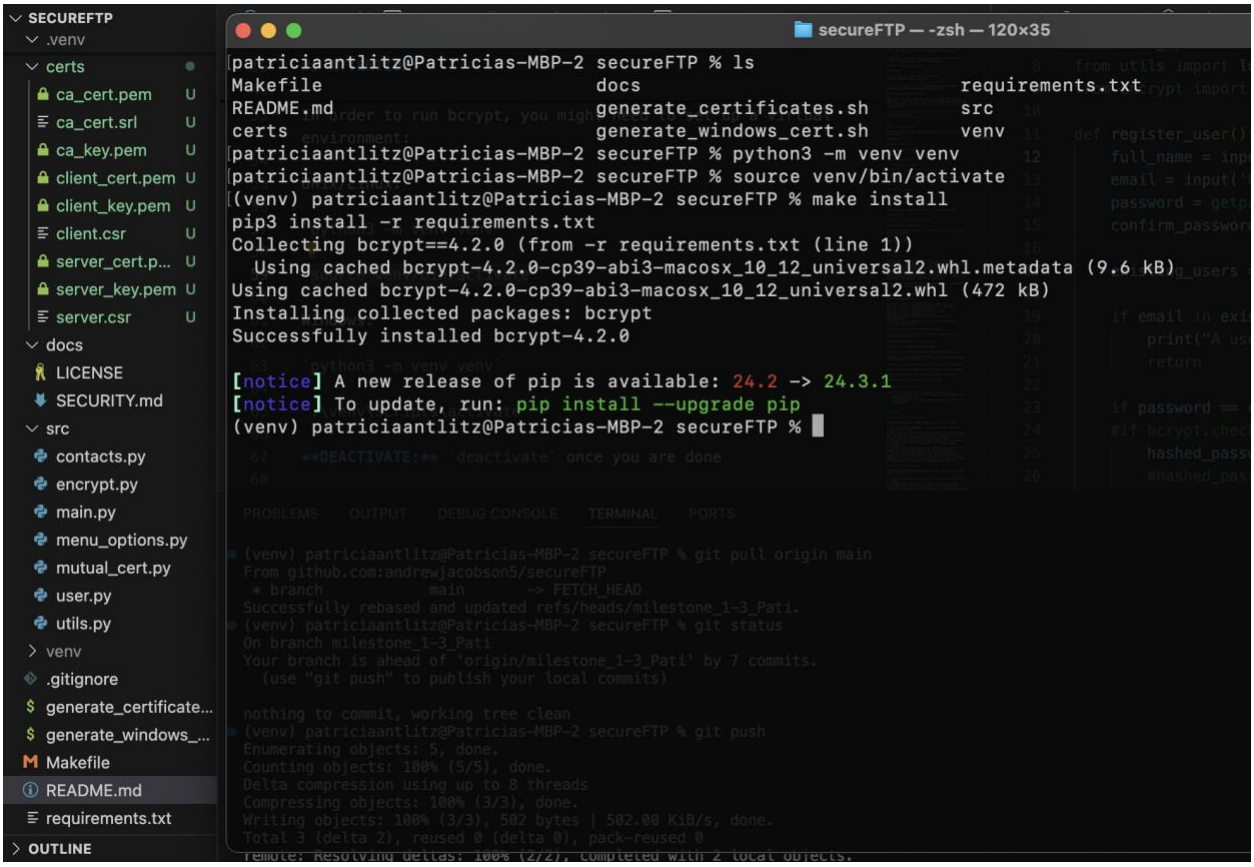
Now you are ready to run this program.

You can use `make run` to start or simply run the **main.py** file. Remember you can always use `make clean` to remove unnecessary files such as certificates once you finish running the program, and you can also run `deactivate` to deactivate the virtual environment.

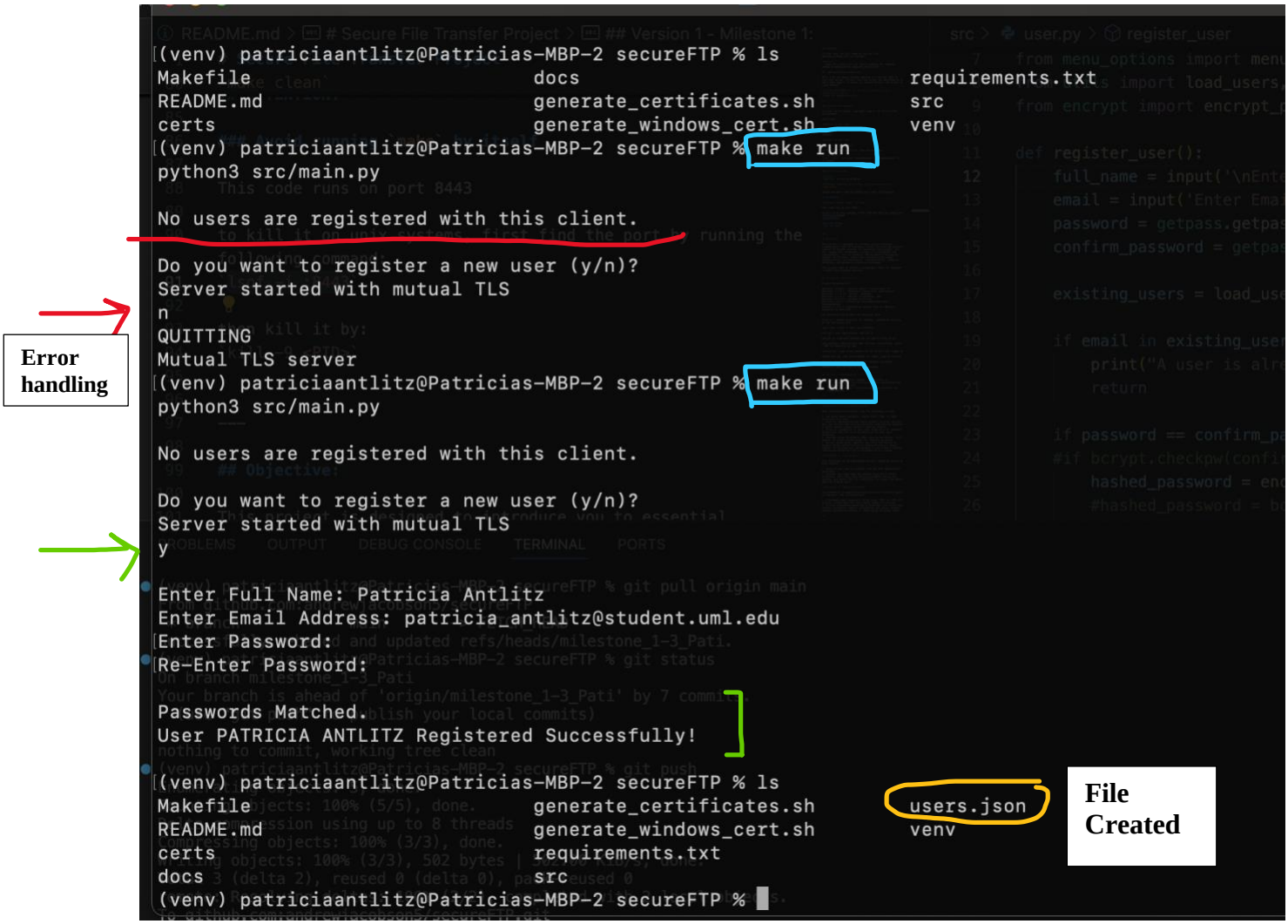
Certificate generation:



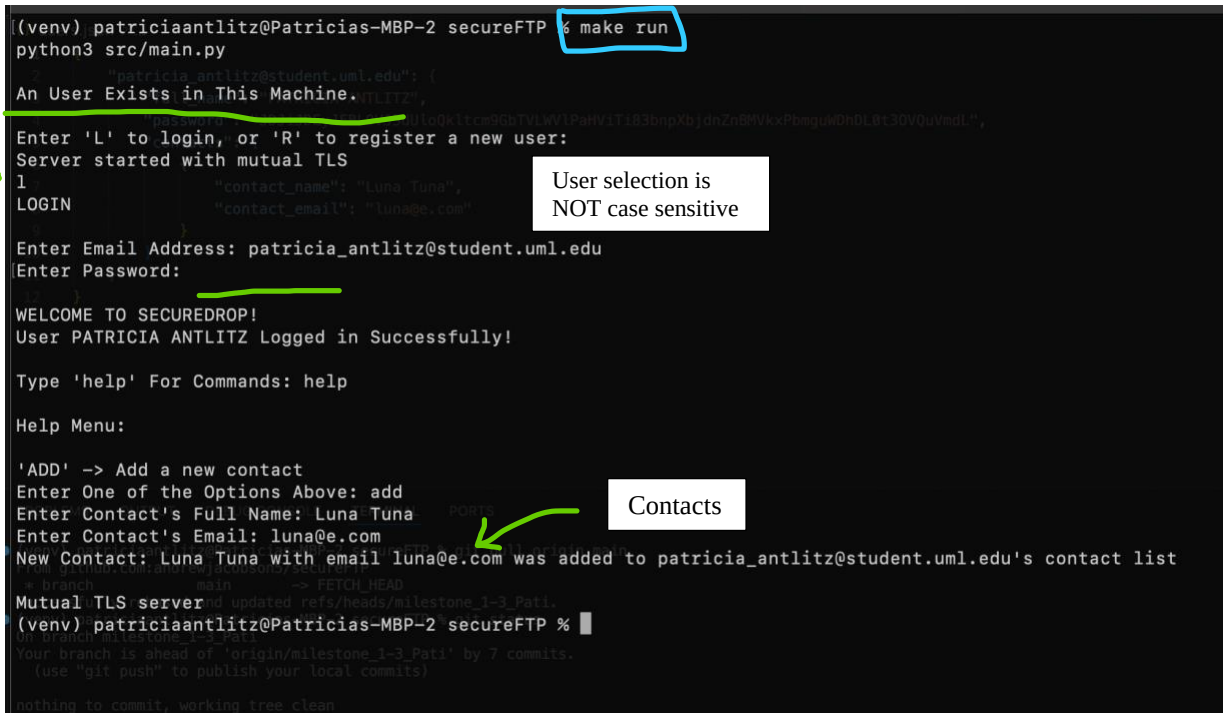
Create and activate an environment and install the required dependencies



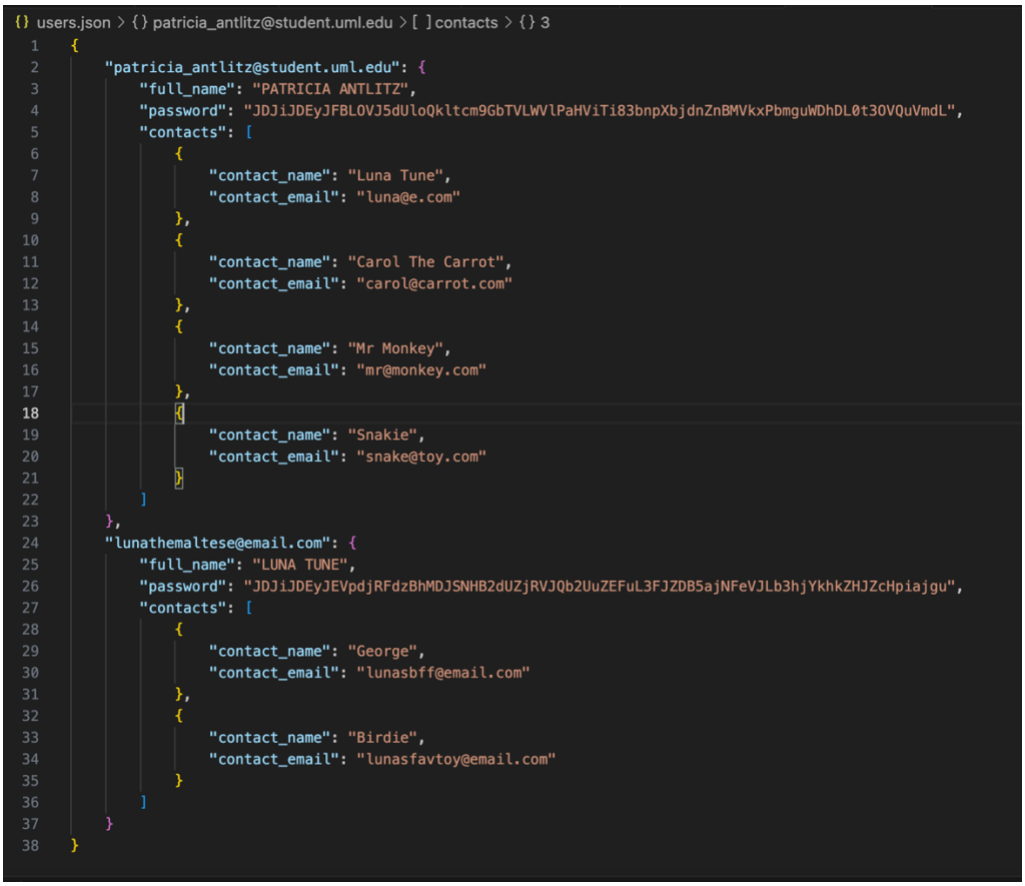
Run the program – the program will create an users.json file


(venv) patriciaantlitz@Patricias-MBP-2 secureFTP % ls
Makefile
README.md
certs
docs
generate_certificates.sh
generate_windows_cert.sh
requirements.txt
src
venv
(venv) patriciaantlitz@Patricias-MBP-2 secureFTP % make run
python3 src/main.py
No users are registered with this client.
Do you want to register a new user (y/n)?
Server started with mutual TLS
n
QUITTING
Mutual TLS server
(venv) patriciaantlitz@Patricias-MBP-2 secureFTP % make run
python3 src/main.py
No users are registered with this client.
Do you want to register a new user (y/n)?
Server started with mutual TLS
y
Enter Full Name: Patricia Antlitz
Enter Email Address: patricia_antlitz@student.uml.edu
Enter Password:
Re-Enter Password:
Passwords Matched.
User PATRICIA ANTLITZ Registered Successfully!
(venv) patriciaantlitz@Patricias-MBP-2 secureFTP % ls
Makefile
README.md
certs
docs
generate_certificates.sh
generate_windows_cert.sh
requirements.txt
src
users.json
venv
Error handling
File Created

LOGIN



After adding different users and more contacts:



Contact Overwrite:

```
(venv) patriciaantlitz@Patricias-MBP-2 secureFTP % make run
python3 src/main.py

An User Exists in This Machine.

Enter 'L' to login, or 'R' to register a new user:
Server started with mutual TLS
l
LOGIN

Enter Email Address: lunathemaltese@email.com
Enter Password:

WELCOME TO SECUREDROP!
User LUNA TUNE Logged in Successfully!

Type 'help' For Commands: help

Help Menu:

'ADD' -> Add a new contact
Enter One of the Options Above: add
Enter Contact's Full Name: Squeaky
Enter Contact's Email: lunasfavtoy@email.com
Existing Contact UPDATED to Squeaky for email address: lunasfavtoy@email.com

Mutual TLS server
(venv) patriciaantlitz@Patricias-MBP-2 secureFTP %
```

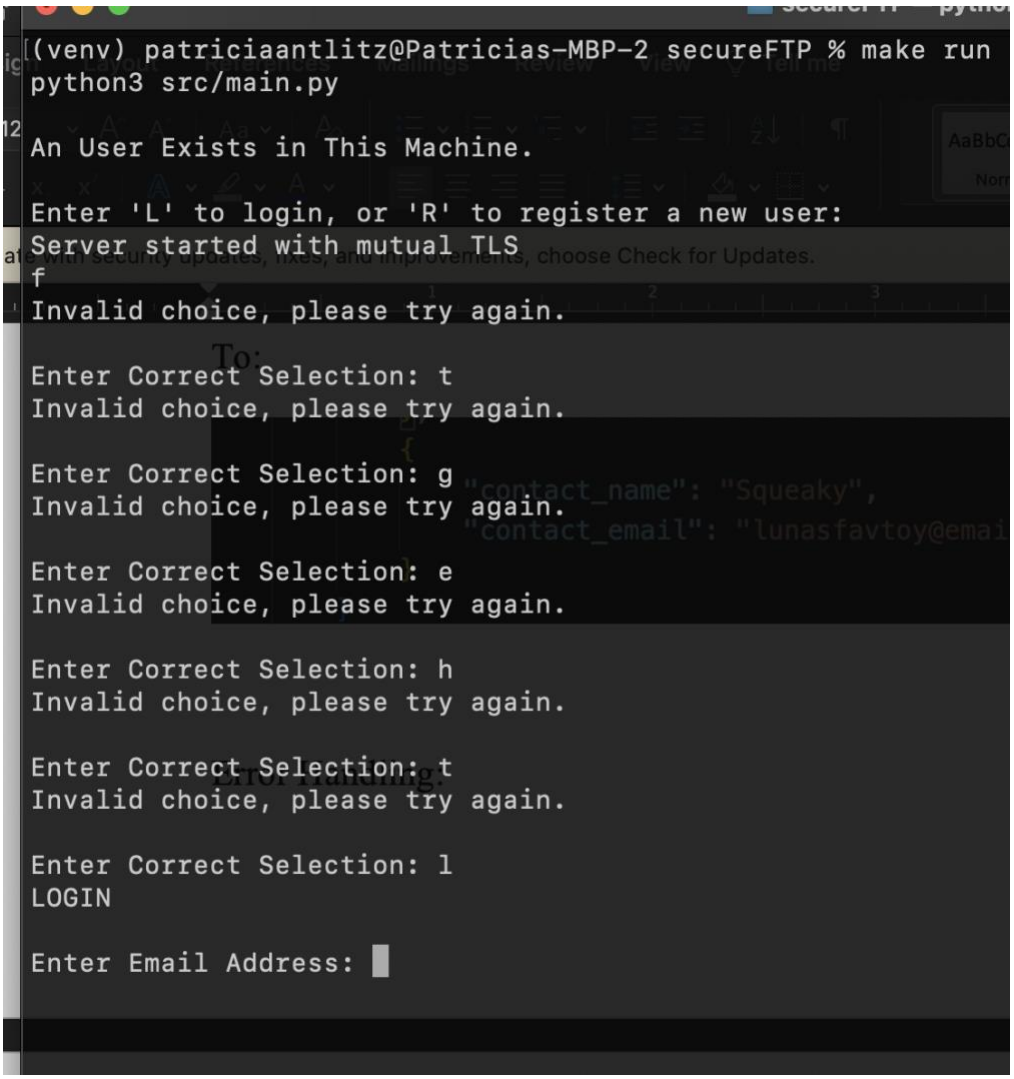
From:

```
        {
            "contact_name": "Birdie",
            "contact_email": "lunasfavtoy@email.com"
        }
    ]
```

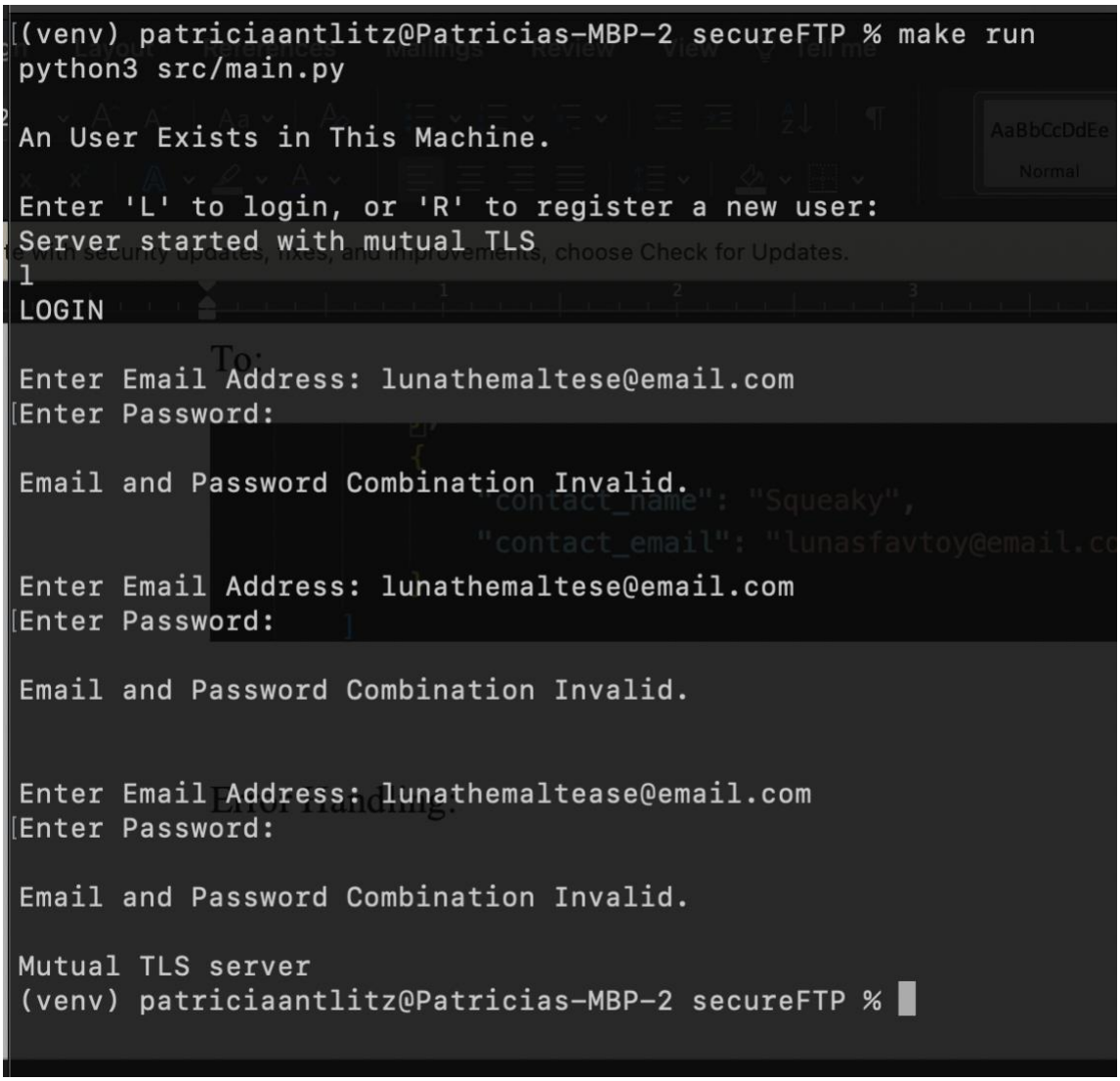
To:

```
        {
            "contact_name": "Squeaky",
            "contact_email": "lunasfavtoy@email.com"
        }
    ]
```

Error Handling:



3 attempts on credentials:


(venv) patriciaantlitz@Patricias-MBP-2 secureFTP % make run
python3 src/main.py
An User Exists in This Machine.
Enter 'L' to login, or 'R' to register a new user:
Server started with mutual TLS
l
LOGIN
Enter Email Address: lunathemaltese@email.com
Enter Password:
Email and Password Combination Invalid.
Enter Email Address: lunathemaltese@email.com
Enter Password:
Email and Password Combination Invalid.
Enter Email Address: lunathemaltease@email.com
Enter Password:
Email and Password Combination Invalid.
Mutual TLS server
(venv) patriciaantlitz@Patricias-MBP-2 secureFTP %