Password manager

-User is asked to give Master password at account creation

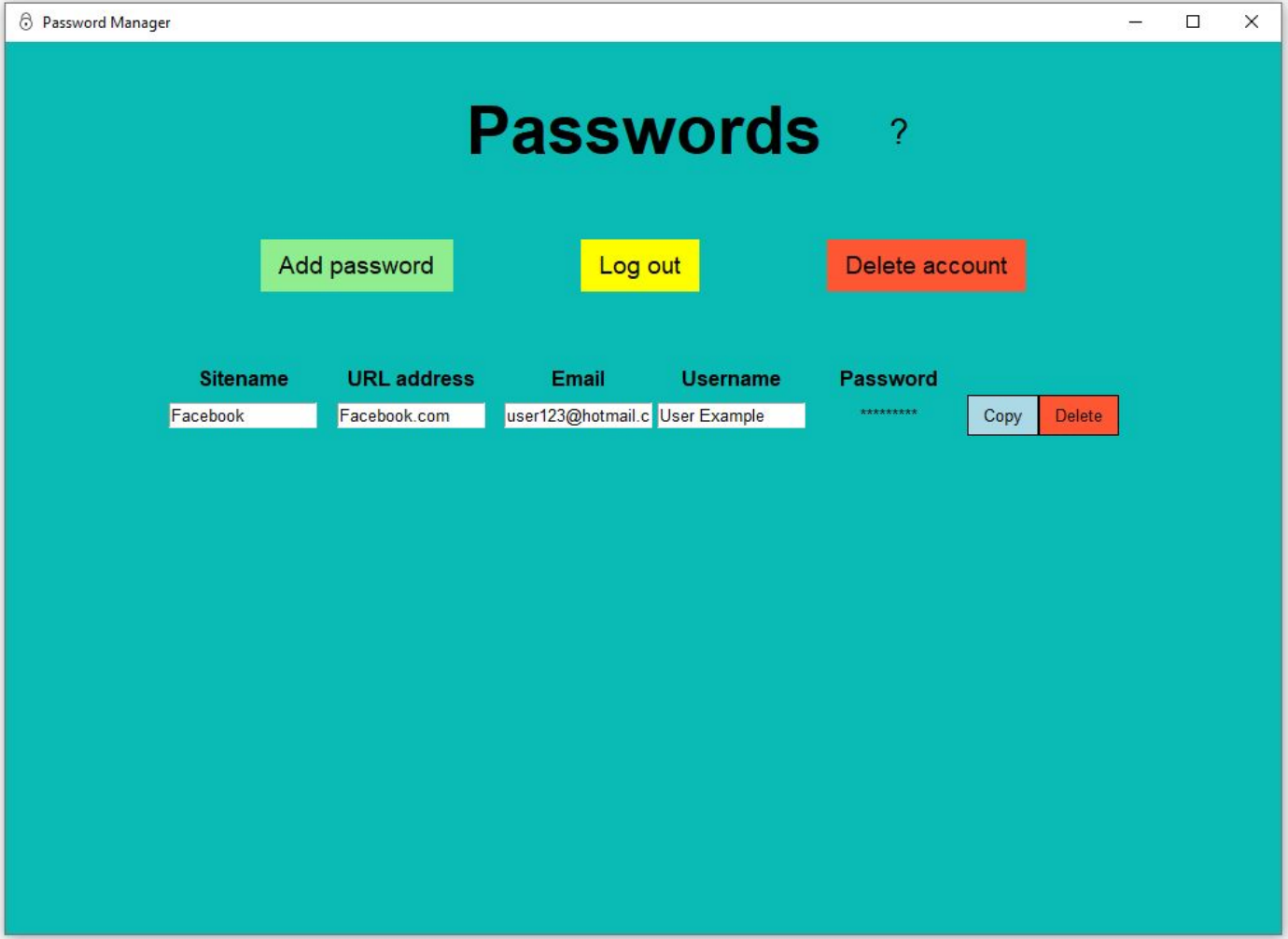
-Master password is used to log in

-Inside the program user can add passwords, delete them and copy them to clipboard

-Also there is possibility to delete passwords or the account

-Password manager database can contain one user at a time.

-No need for more because this is stand-alone program



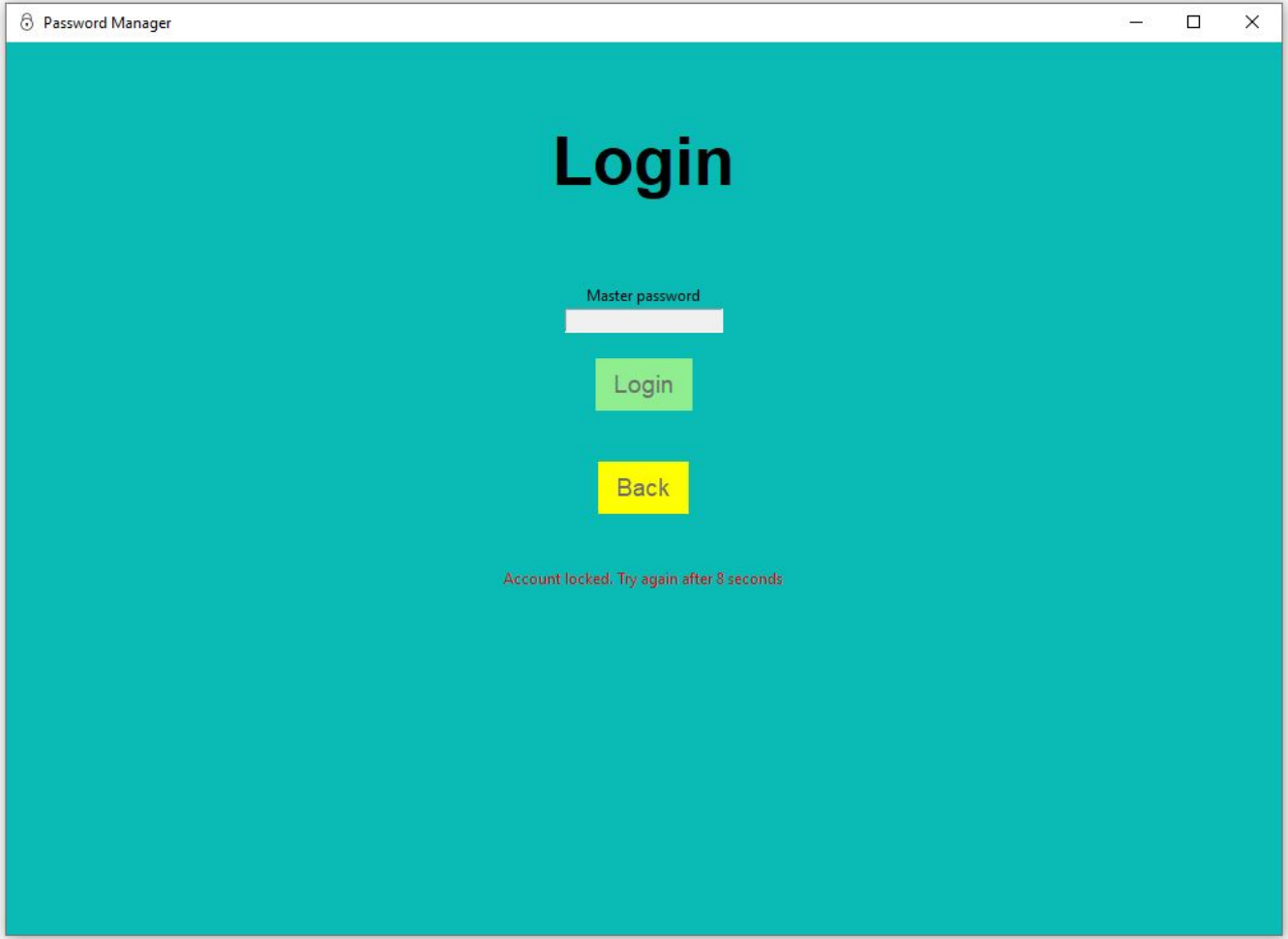
There are many input validations, error handlings and preventions of wrongdoing:

-Brute force prevention. Timer doubles after every third try.

-SQL injections are prevented with parameterized queries

-Master password has to meet strict criteria

-Length of inserted data is restricted. URL and email formats are checked



Coding was done with PyCharm using Python 3.0

GUI was created with Tkinter

PyCryptodome was used in hashing and PBKDF2

SQLite is used to all store data

How does it work?

1. Device secret (salt) is created randomly when creating account
2. Master password is hashed with SHA256
3. Master password and device secret are passed into PBKDF2 to create valid key for AES-256. This key is called Master key
4. Master key is used to encrypt inserted passwords with AES-256, which are then stored to the database.
5. Master key is used again to decrypt passwords when retrieving them from database

```python
def generateDeviceSecret(length=10):
    return ''.join(random.choices(string.ascii_uppercase + string.digits, k = length))
```

```python
# Hash the MASTER PASSWORD
hashed_mp = hashlib.sha256(password.encode()).hexdigest()
```

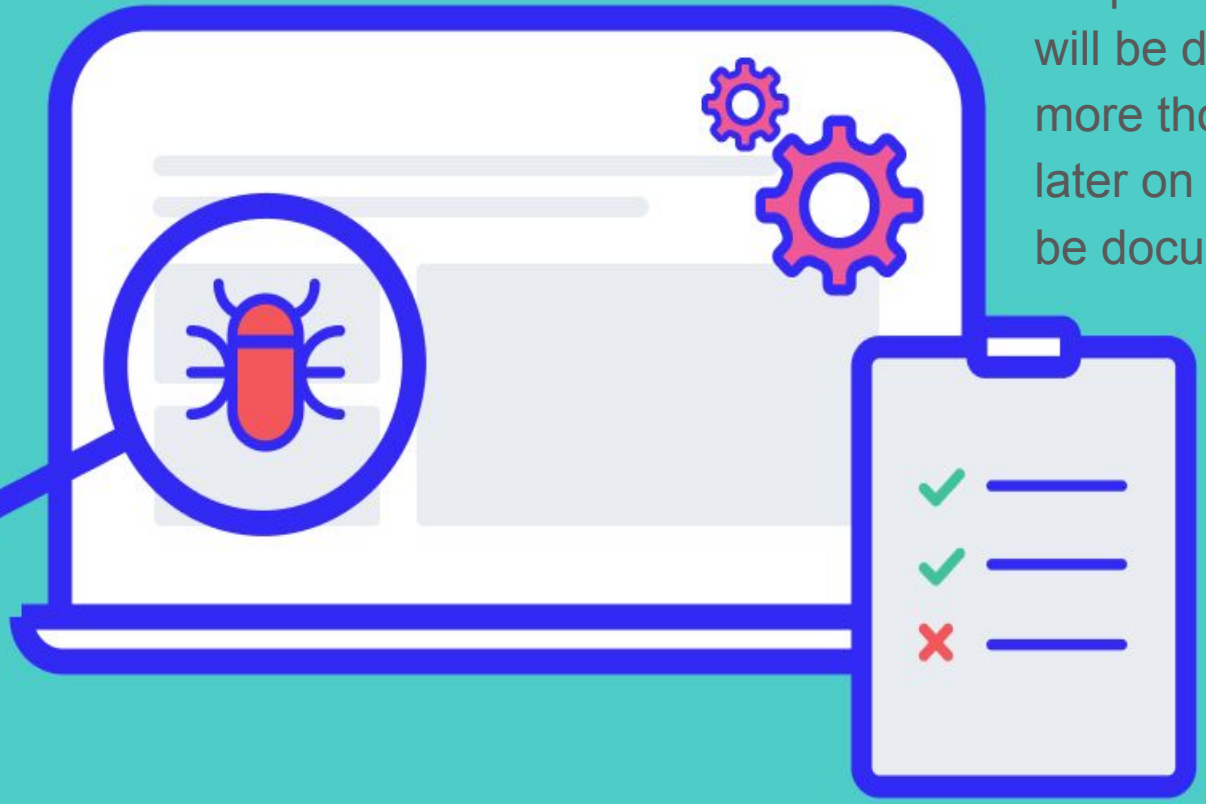
```python
def computeMasterKey(mp,ds):
    password = mp.encode()
    salt = ds.encode()
    key = PBKDF2(password, salt, 32, count=1000000, hmac_hash_module=SHA512)
    return key
```

```python
#encrypt password
encrypted = aesutil.encrypt(key=mk, source=password, keyType="bytes")
```

```python
# decrypt password
decrypted = aesutil.decrypt(key=mk, source=password, keyType="bytes")
```

Testing

Proper testing has not yet done. Every method was tested right after implementation by using GUI to on ensure the proper functioning.



Proper testing will be done more thoroughly later on and it will be documented.

usersnap blog

Demonstration

if time allows…