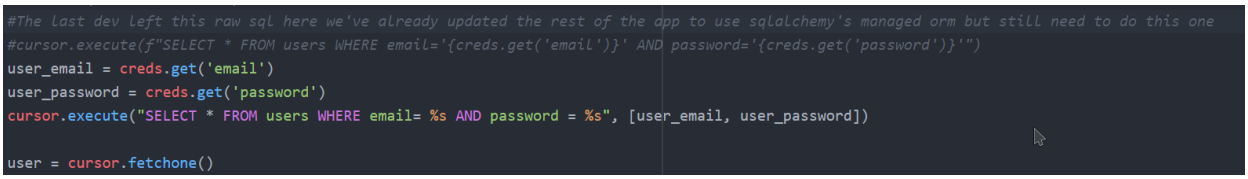
The previous SELECT statement grabbed input from the user during the statement, which allowed it to be modified by what the user entered. To fix this, a prepared statement was implemented using a parameterized query. The user input was gathered first, and used as the parameters outside of the sql SELECT statement.



```
#The last dev left this raw sql here we've already updated the rest of the app to use sqlalchemy's managed orm but still need to do this one
#cursor.execute(f"SELECT * FROM users WHERE email='{creds.get('email')}' AND password='{creds.get('password')}'")
user_email = creds.get('email')
user_password = creds.get('password')
cursor.execute("SELECT * FROM users WHERE email= %s AND password = %s", [user_email, user_password])

user = cursor.fetchone()
```