

Actividad 5

Pablo Sanchez Galdamez (21001135)

Contenidos

Vulnerabilidad	1
Solución	1
Justificación	2

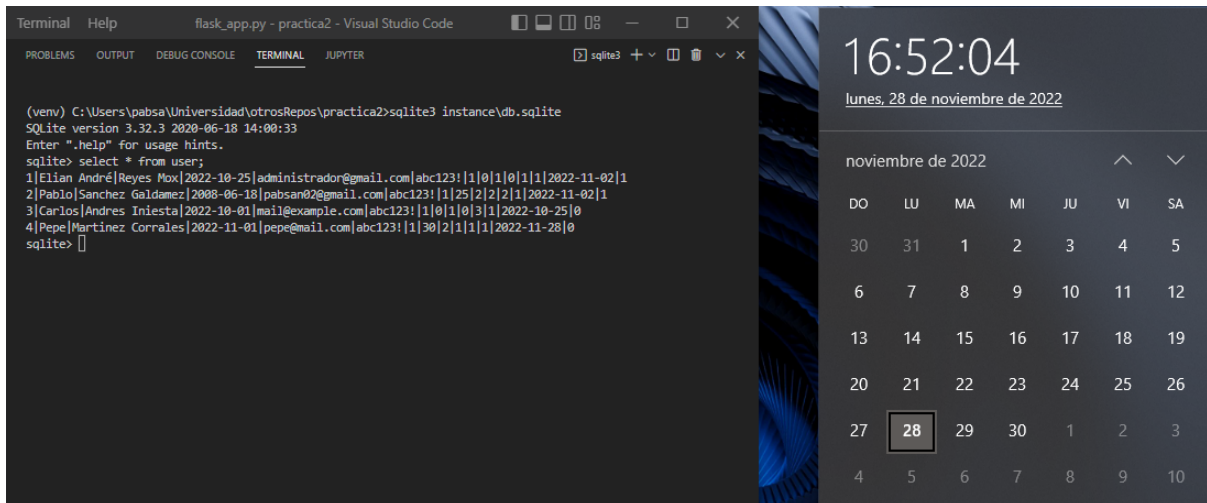
Tomaré la aplicación que desarrollamos en el curso “Práctica del Desarrollo de software II”.
Puede ver la aplicación original en este repositorio:

<https://github.com/Polo123456789/Practica-del-desarrollo-de-software-II>

La buena práctica que se aplicará es “Cifrado de datos sensibles”.

Vulnerabilidad

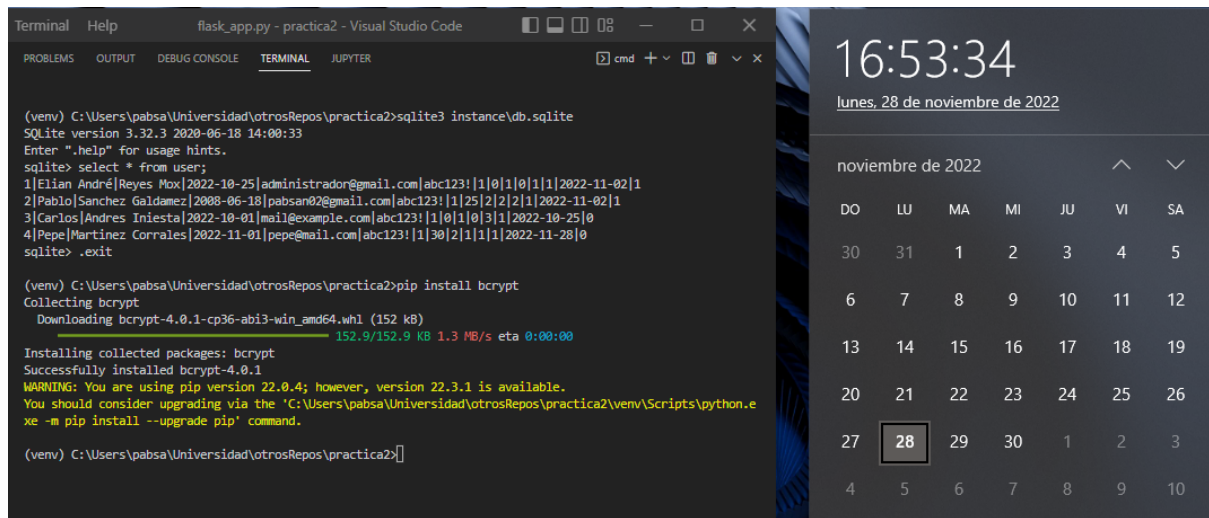
Actualmente las contraseñas de los usuarios se guardan en texto plano:



Solución

Utilizaremos el paquete de python **bcrypt** para encriptar las contraseñas antes de guardarlas.

Instalación del paquete:

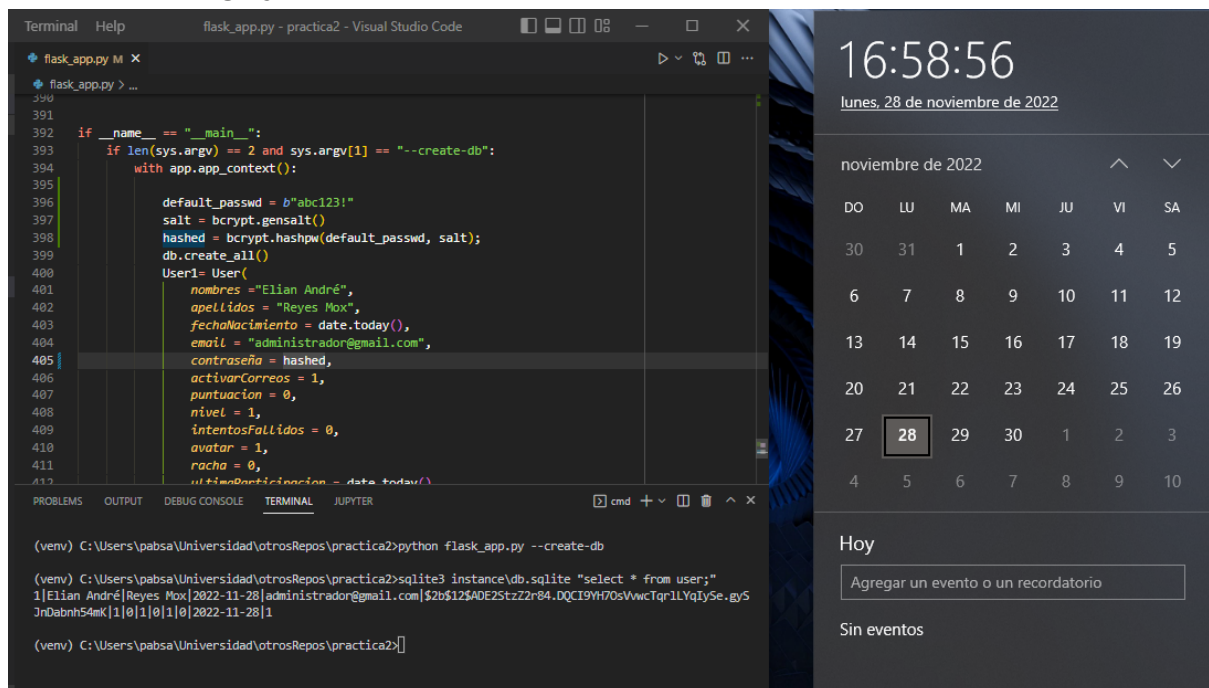


```
(venv) C:\Users\pabsa\Universidad\otrosRepos\practica2>sqlite3 instance\db.sqlite
SQLite version 3.32.3 2020-06-18 14:00:33
Enter ".help" for usage hints.
sqlite> select * from user;
1|Elián André|Reyes Mox|2022-10-25|administrador@gmail.com|abc123!|1|0|1|0|1|2022-11-02|1
2|Pablo|Sanchez Galdamez|2008-06-18|pabsan02@gmail.com|abc123!|1|25|2|2|1|2022-11-02|1
3|Carlos|Andrés Iniesta|2022-10-01|mail@example.com|abc123!|1|0|1|0|3|1|2022-10-25|0
4|Pepe|Martínez Corrales|2022-11-01|pepe@mail.com|abc123!|1|30|2|1|1|1|2022-11-28|0
sqlite> .exit

(venv) C:\Users\pabsa\Universidad\otrosRepos\practica2>pip install bcrypt
Collecting bcrypt
  Downloading bcrypt-4.0.1-cp36-abi3-win_amd64.whl (152 kB)
    152.9/152.9 KB 1.3 MB/s eta 0:00:00
Installing collected packages: bcrypt
Successfully installed bcrypt-4.0.1
WARNING: You are using pip version 22.0.4; however, version 22.3.1 is available.
You should consider upgrading via the 'C:\Users\pabsa\Universidad\otrosRepos\practica2\venv\Scripts\python.exe -m pip install --upgrade pip' command.

(venv) C:\Users\pabsa\Universidad\otrosRepos\practica2>
```

Hash en el código y contraseña encriptada:



```
flask_app.py M X
flask_app.py > ...
391
392 if __name__ == "__main__":
393     if len(sys.argv) == 2 and sys.argv[1] == "--create-db":
394         with app.app_context():
395
396             default_passwd = b"abc123!"
397             salt = bcrypt.gensalt()
398             hashed = bcrypt.hashpw(default_passwd, salt);
399             db.create_all()
400             User1= User(
401                 nombres = "Elián André",
402                 apellidos = "Reyes Mox",
403                 fechaNacimiento = date.today(),
404                 email = "administrador@gmail.com",
405                 contraseña = hashed,
406                 activarCorreos = 1,
407                 puntuacion = 0,
408                 nivel = 1,
409                 intentosFallidos = 0,
410                 avatar = 1,
411                 racha = 0,
412                 ultimaParticipacion = date.today()
413             )

(venv) C:\Users\pabsa\Universidad\otrosRepos\practica2>python flask_app.py --create-db

(venv) C:\Users\pabsa\Universidad\otrosRepos\practica2>sqlite3 instance\db.sqlite "select * from users;"
1|Elián André|Reyes Mox|2022-11-28|administrador@gmail.com|$2b$12$ADEZ5tZzR84.DQC19YH70sVvncTqr1LYqLYSe.gv5JnDabnh54mk|1|0|1|0|1|0|2022-11-28|1

(venv) C:\Users\pabsa\Universidad\otrosRepos\practica2>
```

Justificación

Decidí solucionar este problema de seguridad ya que si se llega a filtrar la base de datos por algún motivo estaría colocando en un riesgo alto a todos los usuarios del sitio.

Decidí utilizar bcrypt porque luego de investigar un poco tengo entendido que es el estándar a día de hoy para cifrar contraseñas.