Python: usare bcrypt

bcrypt è una libreria di hashing di password ampiamente utilizzata in Python per garantire la sicurezza delle password degli utenti. Questa libreria utilizza un algoritmo di hash robusto e a prova di futuro, noto come Blowfish, che è resistente ai tentativi di decifrare le password tramite attacchi di forza bruta.

L'uso di bcrypt in Python è abbastanza semplice. Per prima cosa, è necessario installare la libreria bcrypt utilizzando il gestore dei pacchetti di Python, come pip. Una volta installata, è possibile importare il modulo bcrypt nel proprio script Python.

Per eseguire l'hashing di una password, è necessario generare un valore di salt unico per ciascuna password. Il salt è una stringa casuale che viene aggiunta alla password prima dell'hashing per rendere più difficile l'attacco con l'uso di tabelle rainbow (rainbow table attack). Successivamente, si può utilizzare la funzione `bcrypt.hashpw()` per eseguire l'hashing effettivo.

```
import bcrypt

password = "password".encode('utf-8') # Conversione
della password in byte
salt = bcrypt.gensalt() # Generazione del valore di
salt

hashed_password = bcrypt.hashpw(password, salt) #
Esecuzione dell'hashing della password

print(hashed_password) # Stampa della password
hashata
```

Per verificare una password in fase di autenticazione, si può utilizzare la funzione `bcrypt.checkpw()`. Questa funzione confronta la password in chiaro con la password hashata memorizzata nel database e restituisce `True` se corrispondono, altrimenti `False`.

```
import bcrypt

stored_password =
"$2b$12$Yy1ajxM7Fex7RHm/rEqc5OpqoEjY8wEsGQ.z91hJXn8tN
ofhXyc0S" # Password hashata salvata nel database
password = "password".encode('utf-8') # Conversione
della password in byte

if bcrypt.checkpw(password, stored_password):
    print("Password corretta!")
else:
    print("Password errata!")
```

In conclusione, bcrypt è una libreria affidabile per l'hashing delle password in Python, che offre un'adeguata protezione contro gli attacchi di forza bruta. Utilizzando bcrypt, è possibile garantire la sicurezza delle password degli utenti e proteggere i dati sensibili nel sistema.