HOW TO STORE A PASSWORD?

Storing passwords in plaintext is bad, to protect the passwords we hash them, that way even if a hacker sees the hashed passwords, he won't be able to use them immediately.

But hackers can use lookup tables to guess the original password from the hashed one! To combat that we add a salt to every password as we generate its hash, assuring that each hash is random, making the job of guessing the password even harder.

We can store the salt without encryption along with the hashed password, the hacker can't use the salt to guess the original password.

In other words, lookup tables are only effective when you are trying to break many passwords that were all hashed the same way, using the same hashing algorithm. Throwing in different salt for each password means that the passwords are not all hashed the same way.

Hasan Alsulaiman