HASHING AND SALTING OF PASSWORDS

DONE BY,

AKEPATI JYOSHNA REDDY(21PW02)

JENISA MERLIN D(21PW08)

These days' cybercrimes are increasing and there is a threat to privacy of people. So to reduce these kind of issues and to save passwords we are using Hashing mechanism.

Here there will be a function called hash function which will convert our password into hashed password which looks completely different form through a mathematical algorithm. The hashed password cannot be reverted.

A salt is added to the hashing process to improve the uniqueness and complexity of the password without additional user requirements. This minimizes passwords attacks.

The main terms what we are going to use here are:

- MySQL or PostgreSQL database
- Salting
- Hashing
- Password storing
- Encryption

The general workflow:

1. The user creates an account
2. The password is hashed and stores in database. At no point is the plain text (unencrypted) password ever return to the hard drive.
3. When the user attempts to the login the hash of the password they entered is checked against the hash of the real password (retrieved from the database).
4. If the hashes match the user is granted access if not the user is informed that the user is entered an invalid login credentials. We always say invalid ID or password but not either one this prevents the attackers from enumerating the valid username without knowing their passwords.
5. Step 3 and 4 will repeat whenever someone tries to login their account.