

Password Storage


Background

Protecting stored passwords against potential database breaches is essential. If only plaintext passwords are stored, they will be exposed if the database is breached. Additionally, if no salt is used, hashed passwords are also vulnerable to rainbow table attacks.

Action items

- ✓ Add a salt attribute to the user table and generate a random salt for each password.
- ✓ Implement a hashing algorithm to hash `password + salt`.

Decisions

 Use the `bcrypt` hashing algorithm with a random salt for one-way encryption of passwords.

Demonstration

Attackers are not able to crack the encrypted passwords.

```
password : "$2b$10$GS8YXBRw5mhv7gPQxJ3L..fnURPLZESstAyN2L.EFHwpU0v7CyG8Ua"  
  roles : Array (1)  
    salt : "$2b$10$GS8YXBRw5mhv7gPQxJ3L.."  
  -
```