Bcrypt Encoding For User Registration

➢ **When we implement Bcrypt in an existing application, we face a challenge:**

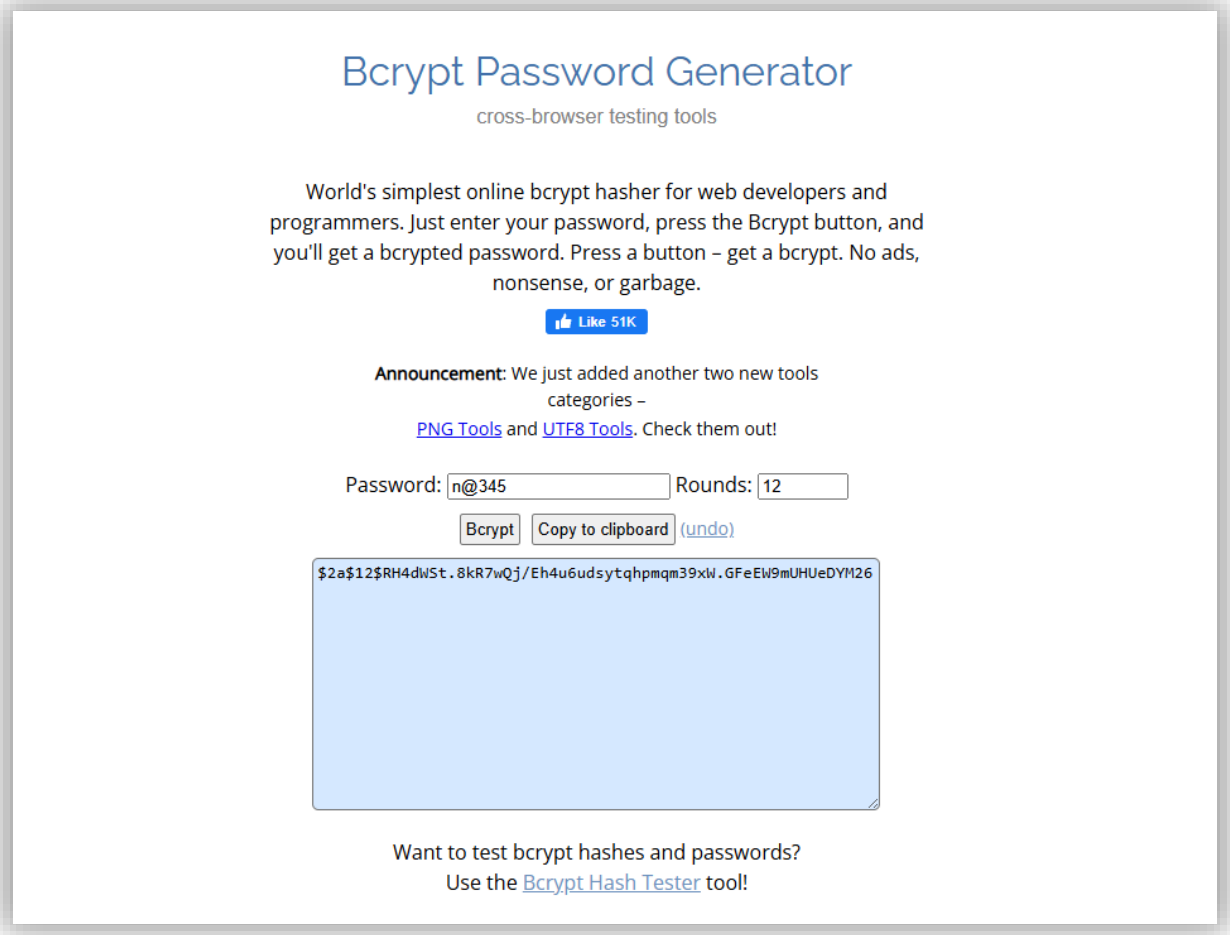
- Existing users already have plain text passwords in the database
- Our authentication system expects plain text passwords
- Once Bcrypt is implemented, the system will try to compare Bcrypt hashes with plain text

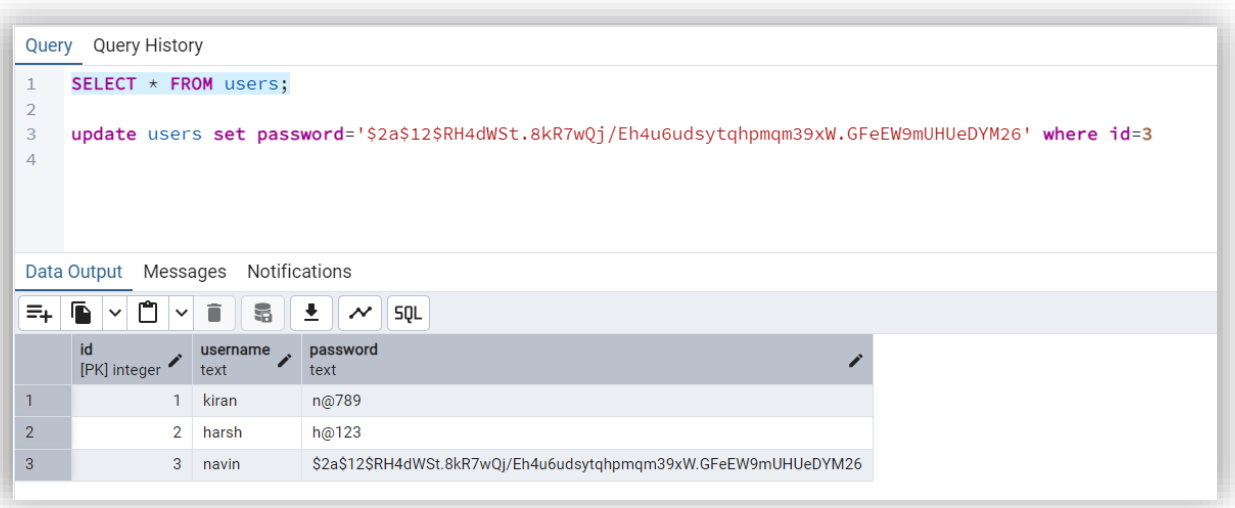
➢ **Update Existing Password Data**

Before implementing Bcrypt, we need to:

- Update existing passwords in the database
- Convert plain text passwords to Bcrypt-encoded versions
- This can be done using an update query after generating encoded passwords

You can generate encoded passwords using an online tool like https://www.browsrling.com:





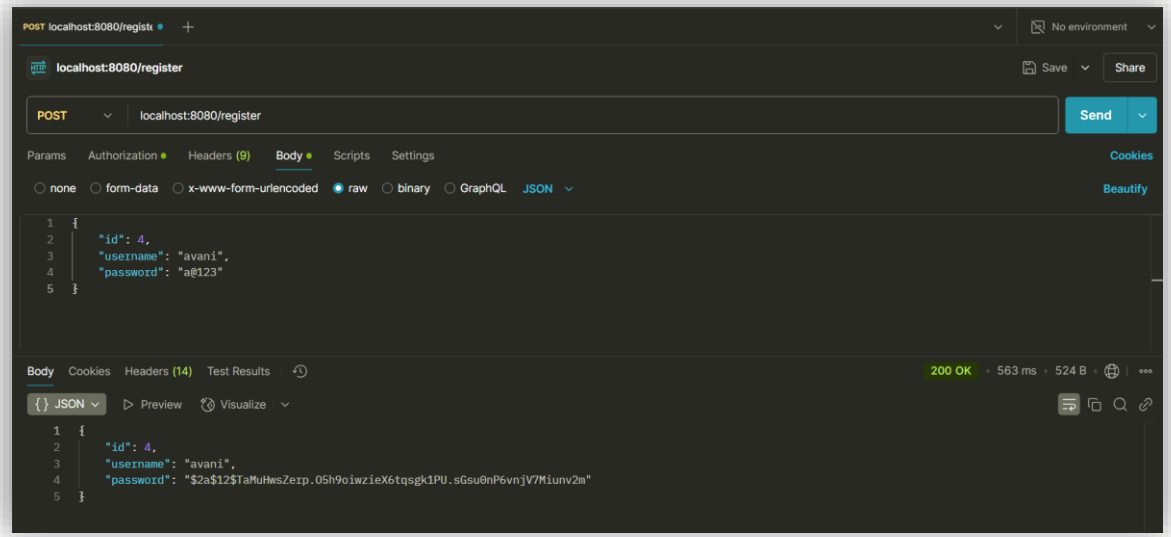
➢ **Implementing Bcrypt in the Service Layer**

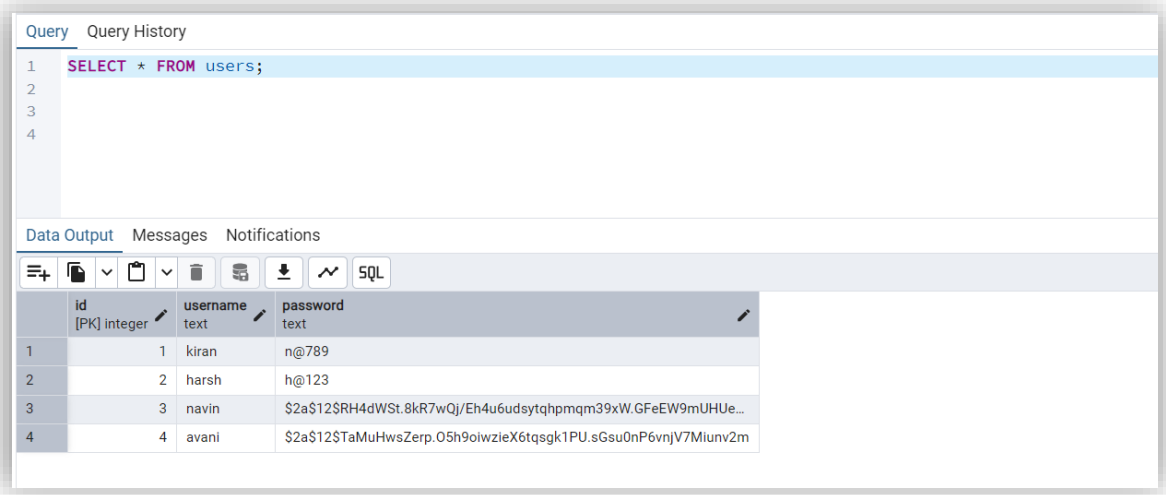
- In the UserService class, create a BCryptPasswordEncoder object
- Set the strength parameter (rounds) to 12 for good security
- Before saving the user, encode the password using the encoder
- Save the user with the encoded password to the database

Example:

```
package com.telusko.springsecdemo.service;
import org.springframework.beans.factory.annotation.Autowired;
import org.springframework.security.crypto.bcrypt.BCryptPasswordEncoder;
import org.springframework.stereotype.Service;
import com.telusko.springsecdemo.dao.UserRepo;
import com.telusko.springsecdemo.model.User;

@Service
public class UserService {

    @Autowired
    private UserRepo repo;
    private BCryptPasswordEncoder encoder = new BCryptPasswordEncoder(12);

    public User saveUser(User user) {
        user.setPassword(encoder.encode(user.getPassword()));
        System.out.println(user.getPassword());
        return repo.save(user);
    }
}
```

Output:





👉 Remember

- BCryptPasswordEncoder is part of Spring Security framework
- The parameter 12 represents the work factor (2^12 = 4,096 rounds)
- Higher work factor means better security but slower performance
- encode() method transforms the plain text password into a Bcrypt hash
- We're printing the encoded password to console for demonstration (not recommended in production)
- After this implementation, all new users will have encoded passwords
- The authentication system must also be updated to verify with Bcrypt (covered in next section)