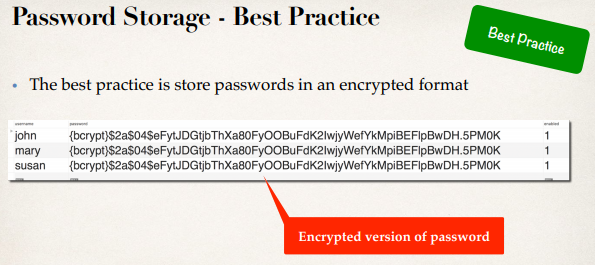
**55.1. Spring Security - Password Encryption – Bcrypt**

**Password Storage in Database**:

For real-life project, store password as plain text in the database is never a good practice. The best practice is store passwords in an encrypted format.



**Spring Security Team Recommendation**:

* Spring Security recommends using the popular **bcrypt** algorithm
* **bcrypt**
  + Performs one-way encrypted hashing
  + Adds a random salt to the password for additional protection
  + Includes support to defeat brute force attacks

**Bcrypt Additional Information**:

* Why you should use **bcrypt** to hash passwords
  + <https://medium.com/@danboterhoven/why-you-should-use-bcrypt-to-hash-passwords-af330100b861>
* Detailed **bcrypt** algorithm analysis
  + <https://en.wikipedia.org/wiki/Bcrypt>
* Password hashing - Best Practices
  + <https://crackstation.net/hashing-security.htm>

**How to Get a Bcrypt password**:

We have a plaintext password and we want to encrypt using **bcrypt**

* Option 1: Use a website utility to perform the encryption
* Option 2: Write Java code to perform the encryption

**Get a Bcrypt password – Website**:

* Visit the link: <https://www.devglan.com/online-tools/bcrypt-hash-generator>
* Enter our plaintext password
* The website will generate a bcrypt password for us
* We can use these encrypted passwords and add them to user accounts in our database.

**Note**:

Multiple runs will generate a different password due to random password salting.

**Development Process (Step-by-Step)**:

1. Run SQL Script that contains encrypted passwords
   1. Modify DDL for password field, length should be 68
2. Modify database properties file to point to new database schema

**That's it … no need to change Java source code**

**Spring Security Password Storage**:

In Spring Security 5, passwords are stored using a specific format.

Password column should be at last 68 characters wide because for "Bcrypt" in curly braces, that eight characters and then the encoded password is 60 characters. When use bcrypt our encoded password should always 60 characters in length.



**Modify DDL for Password Field**:

Now we have to modify the DDL for the password field.

DROP TABLE IF EXISTS `users`;

CREATE TABLE `users` (

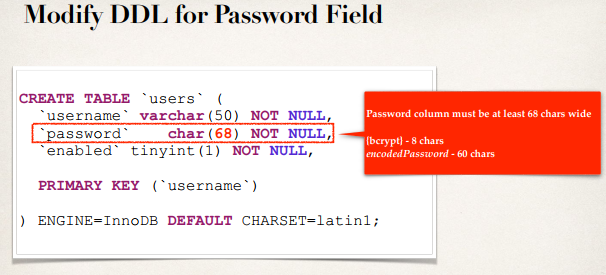
`username` varchar(50) NOT NULL,

`password` char(68) NOT NULL,

`enabled` tinyint(1) NOT NULL,

PRIMARY KEY (`username`)

) ENGINE=InnoDB DEFAULT CHARSET=latin1;



**Step-1: Run SQL Script that contains encrypted passwords**:

DROP DATABASE IF EXISTS `spring\_security\_demo\_bcrypt`;

CREATE DATABASE IF NOT EXISTS `spring\_security\_demo\_bcrypt`;

USE `spring\_security\_demo\_bcrypt`;

DROP TABLE IF EXISTS `users`;

CREATE TABLE `users` (

`username` varchar(50) NOT NULL,

`password` char(68) NOT NULL,

`enabled` tinyint(1) NOT NULL,

PRIMARY KEY (`username`)

) ENGINE=InnoDB DEFAULT CHARSET=latin1;

INSERT INTO `users`

VALUES

('john','{bcrypt}$2a$04$eFytJDGtjbThXa80FyOOBuFdK2IwjyWefYkMpiBEFlpBwDH.5PM0K',1),

('mary','{bcrypt}$2a$04$eFytJDGtjbThXa80FyOOBuFdK2IwjyWefYkMpiBEFlpBwDH.5PM0K',1),

('susan','{bcrypt}$2a$04$eFytJDGtjbThXa80FyOOBuFdK2IwjyWefYkMpiBEFlpBwDH.5PM0K',1);

DROP TABLE IF EXISTS `authorities`;

CREATE TABLE `authorities` (

`username` varchar(50) NOT NULL,

`authority` varchar(50) NOT NULL,

UNIQUE KEY `authorities\_idx\_1` (`username`,`authority`),

CONSTRAINT `authorities\_ibfk\_1` FOREIGN KEY (`username`) REFERENCES `users` (`username`)

) ENGINE=InnoDB DEFAULT CHARSET=latin1;

INSERT INTO `authorities`

VALUES

('john','ROLE\_EMPLOYEE'),

('mary','ROLE\_EMPLOYEE'),

('mary','ROLE\_MANAGER'),

('susan','ROLE\_EMPLOYEE'),

('susan','ROLE\_ADMIN');

**Step 2: Point to New Database Schema**:

# JDBC connection properties

jdbc.driver=com.mysql.jdbc.Driver

jdbc.url=jdbc:mysql://localhost:3306/**spring\_security\_demo\_bcrypt**?useSSL=false

jdbc.user=springstudent

jdbc.password=springstudent

# Connection pool properties

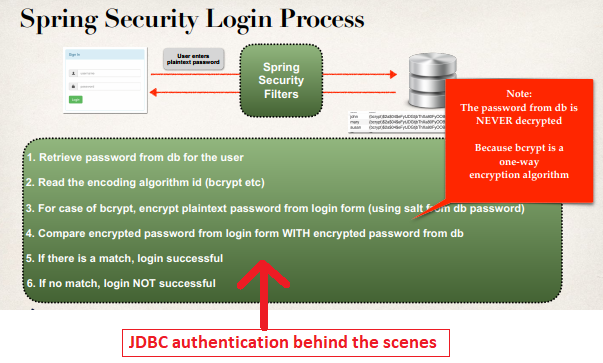
connection.pool.initialPoolSize=5

connection.pool.minPoolSize=5

connection.pool.maxPoolSize=20

connection.pool.maxIdleTime=3000

**Spring Security Login Process**:



55.1. Spring Security - Password Encryption - Bcrypt