Spring Security
Password Encryption

Password Storage

Password Storage

- So far, our user passwords are stored in plaintext … yikes!

username	password	enabled
john	{noop}test123	1
mary	{noop}test123	1
susan	{noop}test123	1

Password Storage

- So far, our user passwords are stored in plaintext … yikes!

username	password	enabled
john	{noop}test123	1
mary	{noop}test123	1
susan	{noop}test123	1

- Ok for getting started … but not for production / real-time project :-(

Password Storage - Best Practice

Password Storage - Best Practice

- The best practice is store passwords in an encrypted format

Password Storage - Best Practice

- The best practice is store passwords in an encrypted format

username	password	enabled
john	{bcrypt}$2a$04$eFytJDGtjbThXa80FyOOBuFdK2IwjyWefYkMpiBEFlpBwDH.5PM0K	1
mary	{bcrypt}$2a$04$eFytJDGtjbThXa80FyOOBuFdK2IwjyWefYkMpiBEFlpBwDH.5PM0K	1
susan	{bcrypt}$2a$04$eFytJDGtjbThXa80FyOOBuFdK2IwjyWefYkMpiBEFlpBwDH.5PM0K	1

Password Storage - Best Practice

Best Practice

- The best practice is store passwords in an encrypted format

username	password	enabled
john	{bcrypt}$2a$04$eFytJDGtjbThXa80FyOOBuFdK2IwjyWefYkMpiBEFlpBwDH.5PM0K	1
mary	{bcrypt}$2a$04$eFytJDGtjbThXa80FyOOBuFdK2IwjyWefYkMpiBEFlpBwDH.5PM0K	1
susan	{bcrypt}$2a$04$eFytJDGtjbThXa80FyOOBuFdK2IwjyWefYkMpiBEFlpBwDH.5PM0K	1

Encrypted version of password

Spring Security Team Recommendation

Spring Security Team Recommendation

- Spring Security recommends using the popular **bcrypt** algorithm

Spring Security Team Recommendation

- Spring Security recommends using the popular **bcrypt** algorithm

- bcrypt

Spring Security Team Recommendation

- Spring Security recommends using the popular **bcrypt** algorithm

- bcrypt
  - Performs one-way encrypted hashing

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

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

Bcrypt Additional Information

- Why you should use bcrypt to hash passwords

www.luv2code.com/why-bcrypt

Bcrypt Additional Information

- Why you should use bcrypt to hash passwords

  www.luv2code.com/why-bcrypt

- Detailed bcrypt algorithm analysis

  www.luv2code.com/bcrypt-wiki-page

Bcrypt Additional Information

- Why you should use bcrypt to hash passwords

  www.luv2code.com/why-bcrypt

- Detailed bcrypt algorithm analysis

  www.luv2code.com/bcrypt-wiki-page

- Password hashing - Best Practices

  www.luv2code.com/password-hashing-best-practices

How to Get a Bcrypt password

How to Get a Bcrypt password

You have a plaintext password and you want to encrypt using bcrypt

How to Get a Bcrypt password

You have a plaintext password and you want to encrypt using bcrypt

- Option 1: Use a website utility to perform the encryption

How to Get a Bcrypt password

You have a plaintext password and you want to encrypt using bcrypt

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

How to Get a Bcrypt password - Website

How to Get a Bcrypt password - Website

- Visit: **`www.luv2code.com/generate-bcrypt-password`**

How to Get a Bcrypt password - Website

- Visit: **`www.luv2code.com/generate-bcrypt-password`**

- Enter your plaintext password

How to Get a Bcrypt password - Website

- Visit: **`www.luv2code.com/generate-bcrypt-password`**
- Enter your plaintext password
- The website will generate a bcrypt password for you

DEMO