

# Spring Security bcrypt Password Variants





# Spring Security Password Storage

- There are different algorithms/variants for bcrypt passwords:
  - Passwords starting with: **\$2a\$**, **\$2b\$**, **\$2y\$**, ...

Spring Security 5 only supports  
bcrypt passwords starting with \$2a\$

username	password	enabled
john	{bcrypt}\$2a\$04\$eFytJDGtjbThXa80FyOOBuFdK2lwjyWefYkMpiBEFlpBwDH.5PM0K	1
mary	{bcrypt}\$2a\$04\$eFytJDGtjbThXa80FyOOBuFdK2lwjyWefYkMpiBEFlpBwDH.5PM0K	1
susan	{bcrypt}\$2a\$04\$eFytJDGtjbThXa80FyOOBuFdK2lwjyWefYkMpiBEFlpBwDH.5PM0K	1



# Spring Security Password Storage

- Currently, Spring Security 5 only supports bcrypt passwords starting with **\$2a\$**
- If you use a different variant starting with **\$2b\$**, **\$2y\$**, ...
- The login will FAIL and you will get this dreaded error message in server logs

Be sure to use **\$2a\$**

**WARNING: Encoded password does not look like BCrypt**

Common pitfall



# BCrypt Variants

- FAQ: What are all of the bcrypt variants?
- Here is a good discussion of the BCrypt variants: **\$2a\$, \$2b\$, \$2y\$, ...**

[\*\*www.luv2code.com/bcrypt-variants\*\*](http://www.luv2code.com/bcrypt-variants)