LU08d - Security

Spring Boot enthält praktischerweise auch einfachere Arten, um mit Passwörtern umzugehen.

BCryptPasswordEncoder

Beim Aufruf der Methode `encode` wird jedes Mal ein neuer zufälliger Salt generiert und verwendet. Dieser Salt wird zusammen mit dem eigentlichen Hash ausgegeben im Format: $2a$10$[22-Zeichen-Salt][31-Zeichen-Hash]

```
import org.springframework.security.crypto.bcrypt.BCryptPasswordEncoder;

...
BCryptPasswordEncoder encoder = new BCryptPasswordEncoder();
String passwordHash = encoder.encode(password);
```

Wird zu einem späteren Zeitpunkt der Hash überprüft, wird entsprechend der korrekte Salt gelesen und verwendet.

```
encoder.matches(plainPassword, passwordHash)
```

Dies hat den vorteilhaften Nebeneffekt, das der Salt nicht mehr separat abgespeichert werden muss.

From:
https://wiki.bzz.ch/ - **BZZ - Modulwiki**

Permanent link:
https://wiki.bzz.ch/de/modul/ffit/3-jahr/java/learningunits/lu08/d?rev=1761615189

Last update: **2025/10/28 02:33**