Zadanie 4

Použité nástroje

- Java
- SQLite

Generovanie salt-u

- Vygeneroval som ho pomocou *SecureRandom* triedy. Využil som algorimus *SHA1PRNG*. Salt ukladáme do databázy ako tretiu položku po hash-i hesla.

Hash

- Využil som štandardné Java API, konkrétne triedu *MessageDigest* a algoritmus *SHA-512*.

Timeout

- Na sťaženie útoku som implementoval funckiu ktorá umelo pridá pol sekundové oneskerenie pri prihlásaní: *TimeUnit.MILLISECONDS.sleep(500);*

Validácia zložitosti hesla:

- Zložitosť zadaného heslo pri registrácia overujem pomocou regulárného výrazu. Konkrétne: *(?=.*[0-9])(?=.*[a-z])(?=\\S+$).{8,}*
- Heslo musí obsahovať:
    - Minimálne jedno veľké písmeno.
    - Minimálne jedno malé písmeno
    - Minimálne jedno číslo
    - Minimálna dĺžka je 8 znakov.

Spustenie aplikácie

- Aplikáciu je možné spustiť nasledujúcim príkazom
    - java -jar .\PasswordSecurity2-jar-with-dependencies.jar