Zadanie 4
I-UPB: Úvod do počítačovej bezpečnosti

October 25, 2021

1 Úvod

Podstatou zadania je doplnenie funkcie hashovania hesiel do databázy spolu so saltovaním hesiel.

2 Databáza

Pre jednoduchosť bola použitá databáza H2. Pre pripojenie, komunikáciu a dopytovanie bola použitá knižnica Hibernate.

3 Implementácia

Aplikácia umožňuje registráciu nového používateľa a prihlásenie. Pre bezpečné uloženie a overenie hesla je postup pri registrácií následovný:

1. Používateľ sa registruje menom a heslom
2. pred uložením hashu hesla sa vygeneruje salt
3. salt sa uloží do databázy
4. zasaltované heslo sa zahashuje
5. hash zasaltovaného hesla sa uloží do databázy.

Pre generovanie saltu sa používa javovská classa SecureRandom pri ktorom generujeme pole bytov o veľkosti 16B. Pre hashovanie bol využitý algoritmus PBKDF2.
Postup pri prihlasovaní je následovný:

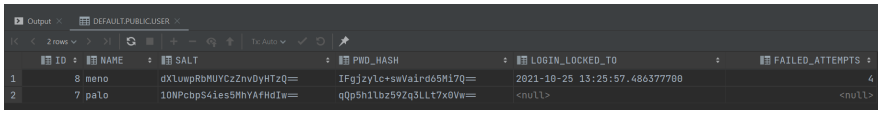
1. Používateľ zadá svoje meno a heslo

2. aplikácia overí či používateľ zo zadaným menom existuje
3. ak neexistuje tak vyhodí chybovú hlášku
4. pre existujúceho používateľa sa vyberie z databázy jeho salt
5. zadané heslo sa zasaltuje a vypočíta sa hash
6. ak sa hash zhoduje z hashom v databáze, tak používateľ je úspešne prihlásený
7. pokiaľ sa hash nezhoduje z hashom v databáze tak aplikácia vyhodí hlášku o neúspešnom prihlásení.

Pokiaľ sa používateľ pokúsil prihlásiť 5x neúspešne prihlasovanie mu bude znemožnené ďalšie 3 minúty.

Niekedy je potrebne kliknúť na tlačítko Login viac krát aby sa event zaregistroval. (Takto to bolo keď som prvý krat spustil skopírovaný poskytnutý projekt)

Obsah DB ktorá je priložená v projekte:



DB create script:

```
    CREATE TABLE USER
(
    ID               INT     NOT NULL AUTO_INCREMENT,
    NAME             VARCHAR NOT NULL,
    PWD_HASH         VARCHAR not null,
    SALT             VARCHAR NOT NULL,
    LOGIN_LOCKED_TO DATETIME,
    FAILED_ATTEMPTS int,
    PRIMARY KEY (ID)
);
```

4 Spustenie

Odovzdaný bol IDEA projekt kde je konfigurácia spustenia no pri problémoch je alternatíva spustiť príkazy:

- mvn clean install
- mvn h2:spawn
- mvn exec:java