Úvod do počítačovej bezpečnosti

Zadanie 5 - Implementácia správy používateľských hesiel

Cieľom zadanie bolo implementovať funkciu na kontrolu zložitosti hesla pri registrácii.

A. Špecifikácia

- Programovací jazyk: Java
- Knižnice: `java.security` (security framework)
  `javax.crypto` (kryptografické operácie)
  `org.passay` (slovníková kontrola)

B. Zložitosť hesla

Heslo je skupina písmen, číslic a špeciálnych znakov, ktorú si dokážeme zapamätať. Na ochranu účtu alebo systému je potrebné používať čo najsilnejšie heslo. Silné heslá sú ťažko uhádnuteľne a odolné voči útokom hrubou silou alebo slovníkovým útok.

Silné heslo by malo:

- byť dlhé, najmenej 10 znakov
- pozostávať z malých a veľkých písmen, číslic a aspoň jedného špeciálneho znaku

Silné heslo by nemalo:

- obsahovať (v akejkoľvek forme) nijaké údaje späté s vašou osobou (ako meno, dátum narodenie a podobne)
- byť slovníkovým slovom, frázou alebo často používaným slovom

Na zaručenie čo najväčšej bezpečnosti sa tiež odporúča nepoužívať rovnaké heslo na viacerých účtoch.

Ako prevencia pred prípadným útokmi môže slúžiť aj dvojfaktorová autentifikácia, ktorá tvorí ďalšiu bezpečnostnú vrstvu.

Jednoduchým riešením pre vytváranie silných hesiel je správca hesiel, ktorý generuje a uchováva hesla v zabezpečenom šifrovanom tvare.

C. Spustenie aplikácie

Aby bolo možné aplikáciu spustiť je potrebné mať na zariadení nainštalovanú JAVU. Aplikáciu je možné spusti dvojklikom na .jar súbor.

D. Používateľská príručka

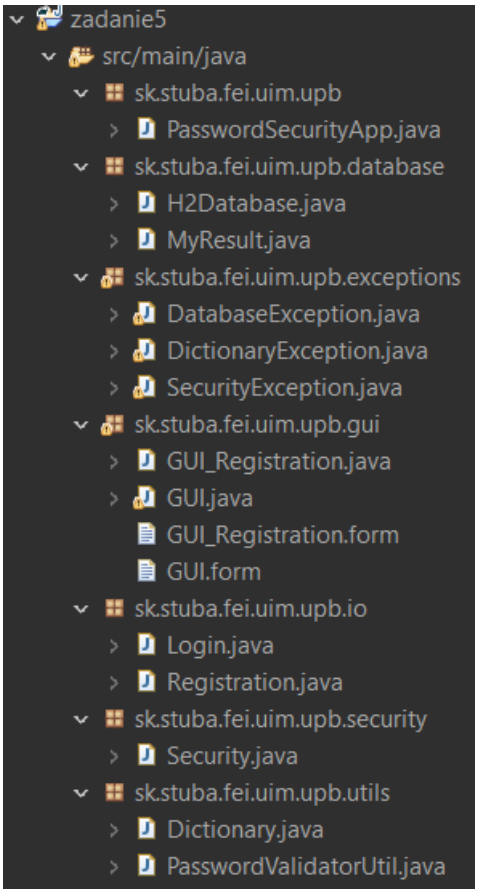
1. Návod na prepojenie databázy s aplikáciou

Aplikácia využíva embedded H2 databázu. Aplikácia hľadá predvolenú databázu v home adresári, preto je potrebné do neho (C:\Users\<meno>\database) nakopírovať priložený priečinok **`database`**. Tento priečinok obsahuje databázu **`myDB.mv.db`**, do ktorej sa ukladajú používateľské prihlasovacie údaje.

2. Návod na importovanie projektu do IDE

Aplikácia bola vyvíjaná v Eclipse IDE pričom bola vytvorená ako Gradle projekt, pre prípad, že by ste chceli otvárať kód aplikácie v IDE a nejako ho meniť, odporúčam aplikáciu importovať ako „existing gradle project“ aby náhodou nevznikali nejaké komplikácie.
V prípade, že by ste si chceli nanovo vygenerovať .jar stačí použiť gradle task „`jar`“, ktorý celý kód skompiluje, vybuilduje a zabalí do `zadanie5.jar`, takto vygenerovaný súbor je potom možné nájsť v `zadanie5\build\libs` adresári a spustiť ho.

3. Štruktúra projektu



4. Stručný popis hlavných tried:

Trieda	Funkcionalita
Registration	Riadenie registrácie nového používateľa
Login	Riadenie prihlasovania používateľov
Security	Generovanie a kontrola hashovaných hesiel
H2Database	Spojenie a vytváranie dotazov na DB
GUI	Grafické používateľské rozhranie aplikácie
GUI_Registration	Grafické používateľské rozhranie registrácie
Dictionary	Slovník
PasswordValidatorUtil	Kontrola zložitosti hesla

Registrácia nového užívateľa (Registration)

- Trieda vykonáva kontrolu duplicitnej registrácie používateľov s rovnakým používateľským menom a stará sa o registráciu nových používateľov

Prihlásenie nového užívateľa (Login)

- Trieda riadi prihlasovanie už existujúcich požívateľov a vykonáva kontrolu korektného zadania používateľského mena a hesla.

Generovanie hashovaných hesiel (Security)

- Trieda riadi generovanie saltu, hashovaných hesiel a tiež spätnú kontrolu hesiel pri prihlasovaní
- Na hashovanie je použitý **PBKDF2** algoritmus so saltom veľkosti 128 bitov
- Na to aby bol salt naozaj náhodný bola využitá trieda `java.security.SecureRandom`, ktorá poskytuje kryptograficky silný generátor náhodných čísel
- **PBKDF2** algoritmus obsahuje predvolenú funkcionalitu na oneskorenie
- Algoritmus aplikuje pseudo náhodnú funkciu opakovane na základe špecifikovaného počtu iteracií. Tato funkcionalita zaručuje spomalenie hashovacej funkcie a tiež sťažuje útočníkom uhádnutie hesla, pretože na to aby ho vedeli odhaliť je potrebné uhádnuť aj samotný počet iteracií, ktorý bol použitý pri jeho generovaní
- Metóda `PBEKeySpec(char[] password, byte[] salt, int iterationCount, int keyLength)` vytvorí kľuč, ktorý je následne použitý na vygenerovanie hashovaného hesla pomocou `SecretKeyFactory.getInstance("PBKDF2WithHmacSHA1")`

Aplikačná databáza (H2Database)

- Aplikácia využíva offline embedded H2 databázu uloženú v súbore **`myDB.mv.db`**
- Trieda riadi vytváranie spojenia s databázou ako aj jeho zatváranie
- V triede sa tiež nachádzajú metódy na vyberanie dát a ich pridávanie do databázy

Kontrola zložitosti hesla (PasswordValidatorUtil)

- Minimálna dĺžka hesla je 10 znakov
- Minimálny počet malých písmen je 1
- Minimálny počet veľkých písmen je 1
- Minimálny počet číslic je 1
- Heslo nesmie obsahovať medzery (whitespace characters)
- Heslo nesmie byť slovníkovým slovom (testovacie slovo - Digestor101)

Na testovanie zhody so slovníkovými slovami bola použitá databáza slov z aplikácie John the Ripper, ktorá slúži na prelamovanie hesiel spoločne s databáza slovenských slov.