**Zadanie č.3**

Úvod do počítačovej bezpečnosti

Implementácia správy používateľských hesiel

2016/2017

**Autor: Michal Drahovský, Ján Dzvoník**

# Použite technológie

## Funkcie na generovanie a aplikovanie saltu

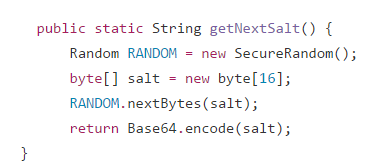
Salt je náhodne vygenerovány reťazec ktorý sa prikladá k nezahashovanému heslu aby sa zkomplikovali útoky zamerané na zlomenie hesla. Salt by mal byť pre každé nové heslo náhodný a unikátny. Vygenerovaný salt je následné potrebné si zapamätať aby si sním ďalej dalo overiť heslo.

Funkcie na generovanie saltu sme vytvorili v Classe Registration. Vygenerovaný salt sa následne aplikuje pri hashovaní hesla a zapíše sa do súboru hesla.txt do stĺpca za zahashované heslo. Pre každé heslo sa generuje unikátny a náhodný salt.

Na encodovanie saltu sme využili knižnicu com.sun.org.apache.xerces.internal.impl.dv.util.Base64;

Na generovanie saltu sme využili knižnicu java.security.SecureRandom, java.util.Random.

Ukážka zdrojového kódu funkcie, ktorá generuje salt.



Ukážka zdrojového kódu funkcie, ktorá aplikuje salt



Vygenerovaný salt može vyzerať napríklad: uEtD3IBQ4XWSk1t1UfFOkA==

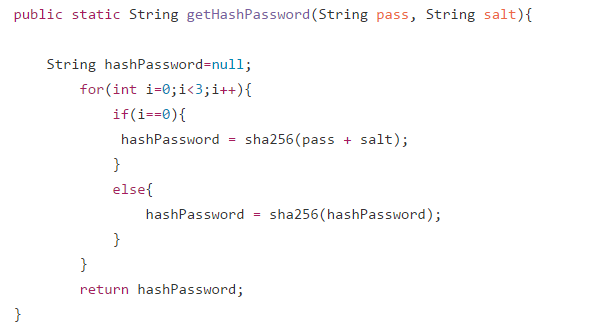
## Funkcie na zahashovanie saltového hesla

Z bezpečnostných dôvodov je potrebné jednotlivé heslá ukladať v nečitateľnej forme. Na tento problém sa používajú asymetrické hashovacie funkcie. To znamená, že sa nedajú spätne dešifrovať. V súčastnosti sa za bezpečnú hashovaciu funkciu považuje aj SHA-256. Túto funkciu sme si vybrali aj v našom zadaní.

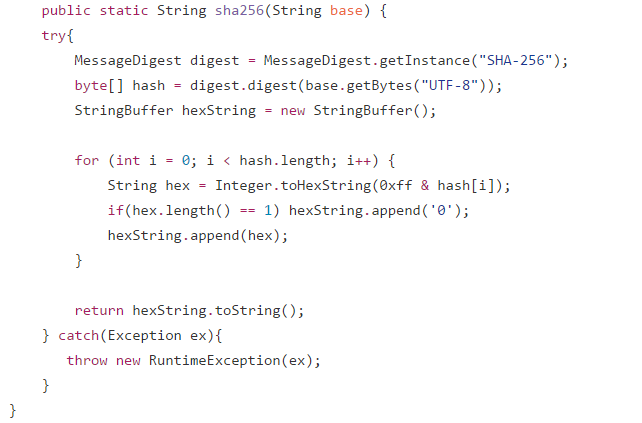
Funkcie na zahashovanie saltového hesla sme doprogramovali v Classe Registration pri registrácií a v Classe Login pri prihlasovaní. Táto funkcia zahashuje saltové heslo funkciou SHA256 a následne tento hash znova zahashuje ešte 2 krát taktiež funkciou SHA256.

Na hashovaciu funkciu SHA256 sme využili knižnicu java.security.MessageDigest;

Ukážka kódu generovania hesla



Ukážka kódu funkcie ktorá hashuje heslo funkciou SHA256



Zahashované heslo može byť v tvare: 105544b0cfa33a1910b32c7cf910f705b5b66b3778fe4fdf8bdef75c0860fda1

# Funkcie na kontrolu zložitosti hesla

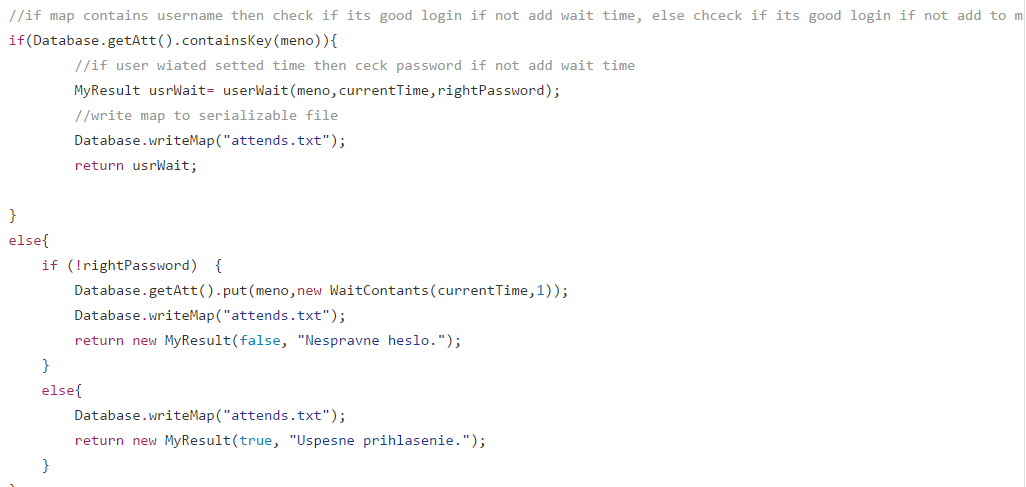
# Funkcie na vytvorenie časového odstupu medzi pokusmi o prihlásenie

Vytvorenie časového odstupu medzi jednotlivými nesprávnymi pokusmi sa používa aby sa predišlo prelomeniu hesla technikou brute force. Jednotlivé pokusy sa zaznamenávajú v programe a následne sa obmedzí prístup k aplikácií pre zadaného používateľa. Ak sa používateľ prihlasuje veľa krát so zlým heslom jeho čas dokedy sa nemožu prihlásiť sa zväčšuje o niekohlo sekúnd až minút. Pre užívateľa niekoľko sekúnd nepredstavuje veľké množstov času ale pri počítači riadenom útoku sa predĺži útok o podstatne viacej času.

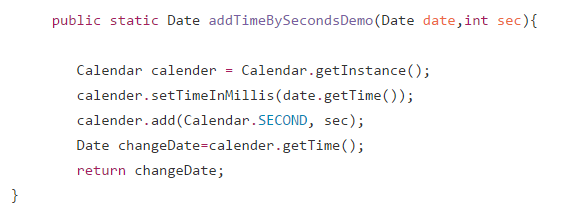
Funkcie, ktoré kontrolujú správnosť údajov a vytvárajú časový odstup medzi prihláseniami sme vytvorili v Class Login a funkcie, ktoré následne ukladajú informácie o jednotlivých uživateľoch a ich pokusoch o prihlásenie v Class Database. Ďalej sme si vytvorili pomocnú class WaitContants. Táto class iba uchováva čas vo formáte Date a počet sekúnd o ktoré sa navyšuje suspendovanie uživateľského konta.

Ak sa používateľ prihlási so zlým heslom, je pridaný do mapy kde ako kľúč je login a hodnota je inštancia class WaitConstant so dátumom a časom dokedy musí čakať a počet sekúd koľko má čakať. Ak používateľ znová zadá zlé heslo aplikácia sa pozrie do mapy či sa tam používateľ nachádza. Ak áno tak okontroluje či jeho čas, dokedy sa nemože prihlásiť je menši ako súčasný čas. Ak sa nenachádza v mape tak sa používateľa pokúsy prihlásiť. Ak použivateľova suspendácia vypršala tak sa ho pokúsi prihlásiť. Ak sa znova zle prihlási tak jeho čas sespendovania sa navýši o počet sekúnd, ktoré mu prislúchajú. Počet sekúnd koľko má čakať a čas suspendovania sa vždy navyšuje pri každom zlom pokuse o prihlásenie alebo pri pokuse o prihlásenie pred vypršaním suspendácie. Mapa s používateľmi je vždy aktualizovaná a zapisovná do databázy(súboru), pri každom pokuse o prihlásenie aby sa predišlo tomu, že ak používateľ vypne aplikáciu jeho suspendácia by sa stratila. Preto pri spustení aplikácie si načíta dáta zo súboru (attends.txt) a aktualizuje mapu.

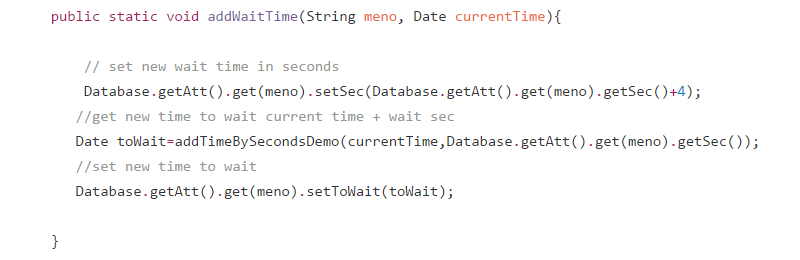
Ukážka kódu overovania prihlásenia



Ukážka kódu funkcie, ktorá pridá k súčasnému dátumu počet sekúnd ktoré ma užívateľ čakať



Ukážka kódu funkcie, ktorá aktualizuje čas suspendácie používateľa



Ukážka kódu funkcie, ktorá overí či používateľ čakal zadaný suspendačný čas

