I-UPB Zadanie 5

Pri riešení tohto zadania som použil programovací jazyk **Java 11**. V predošlom zadaní som implementoval nasledujúce metódy (Súbor: Security.java) a implementoval som komunikáciu s **MySQL Databázou** (Súbor: Database.java , Dump databázy tiež nájdete v zipku), ktorú môže definovať používateľ pri spúšťaní programu. **PBKDF2WithHmacSHA512**[1] som si vybral z toho dôvodu, že v sebe už zahŕňa časový odstup a ochranu proti brute force útokom.

```java
protected static String hash(String password, byte[] salt) throws InvalidKeySpecException {
    try {
        int iterations = 1000;
        char[] chars = password.toCharArray();

        PBEKeySpec spec = new PBEKeySpec(chars, salt, iterations, keyLength: 64 * 8);
        SecretKeyFactory skf = SecretKeyFactory.getInstance("PBKDF2WithHmacSHA512");
        byte[] hashByteArray = skf.generateSecret(spec).getEncoded();

        // Convert Byte Array to String and return it
        return new String(hashByteArray, StandardCharsets.UTF_8);
    } catch (NoSuchAlgorithmException e) {
        e.printStackTrace();
    }

    return "";
}
```

```java
protected static byte[] getSalt() throws NoSuchAlgorithmException {
    // We always need to use a SecureRandom to create good salts, and in Java,
    // the SecureRandom class supports the “SHA1PRNG” pseudo random number generator algorithm
    SecureRandom sr = SecureRandom.getInstance("SHA1PRNG");

    //Create array for salt
    byte[] salt = new byte[16];

    //Get a random salt
    sr.nextBytes(salt);

    return salt;
}
```

[1] https://stackoverflow.com/questions/19348501/pbkdf2withhmacsha512-vs-pbkdf2withhmacsha1

V tomto zadaní som pridal validáciu pre používateľské heslá. Kód vidíte na nižšie uvedenom obrázku. Na validáciu som použil podľa odporúčania **Passay**[2]. Jednotlivé pravidlá sú okomentované. Nastavil som dĺžku hesla na 10-99 znakov. Nepodporuje whitespace znaky. Vyžadujem od používateľa zadať heslo s 3-3 veľkými a malými písmenami, podobne 3 číslami. Na slovníkovú časť tejto úlohy som si vybral Rock You, ktorý sme použili v 0. Zadaní, keď sme chceli cracknuť heslo slovníkovým útokom. Ak používateľ nespĺňa niektoré podmienky, program mu označí všetky nedostatky.

```java
protected static MyResult isValid(String user_password) throws IOException {
    List<Rule> rules = new ArrayList<>();
    //Rule 1: Password length should be in between 10 and 99 characters
    rules.add(new LengthRule(10, 99));

    //Rule 2: No whitespace allowed
    rules.add(new WhitespaceRule());

    //Rule 3: At least three Upper-case characters
    rules.add(new CharacterRule(EnglishCharacterData.UpperCase,  num: 3));

    //Rule 4: At least three Lower-case characters
    rules.add(new CharacterRule(EnglishCharacterData.LowerCase,  num: 3));

    //Rule 5: At least three digits
    rules.add(new CharacterRule(EnglishCharacterData.Digit,  num: 3));

    //Rule 6: The password should not be in the rockyou.txt file
    Dictionary wordListDictionary = new DictionaryBuilder().addFile("passwordsecurity2/rockyou.txt").build();
    rules.add(new DictionaryRule(wordListDictionary));

    //Display error messages from file if password does not obey all the rules
    Properties props = new Properties();
    props.load(new FileInputStream( name: "passwordsecurity2/passay.properties"));
    MessageResolver resolver = new PropertiesMessageResolver(props);

    PasswordValidator validator = new PasswordValidator(resolver, rules);
    PasswordData password = new PasswordData(user_password);
    RuleResult result = validator.validate(password);

    if (result.isValid()) {
        return new MyResult(true, "Valid Password");
    } else {
        return new MyResult(false, String.join( delimiter: "\n", validator.getMessages(result)));
    }
}
```

Spúšťanie programu:

Najprv si musíme skompilovať program:

```
javac -cp .:mysql-connector-java-8.0.25.jar:passay-1.6.1.jar
passwordsecurity2/PasswordSecurity2.java
```

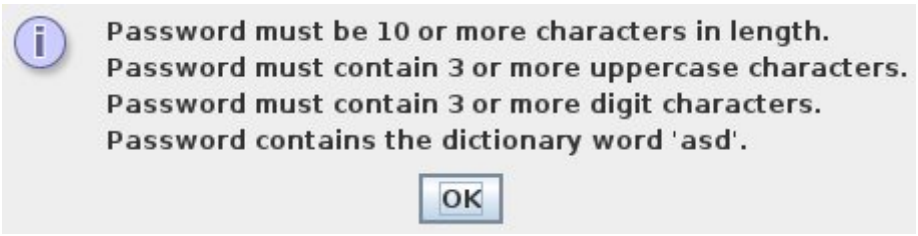
[2] https://www.passay.org/

Po kompilácii si môžeme spustiť program nasledujúcim príkazom:

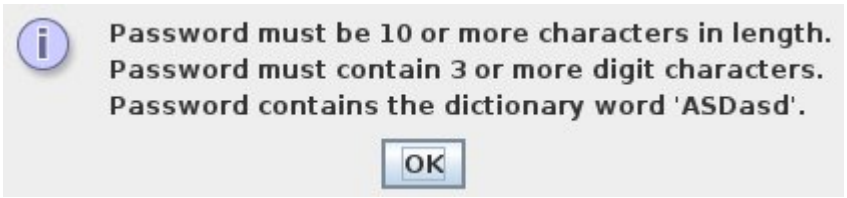
```
java -cp ".:mysql-connector-java-8.0.25.jar:passay-1.6.1.jar"
passwordsecurity2.PasswordSecurity2 < Database Connection URL -
jdbc:mysql://localhost:3306/upb > < Database Table > < Database User > <
Database Password >
```

Dôkaz o fungovaní tohto projektu:

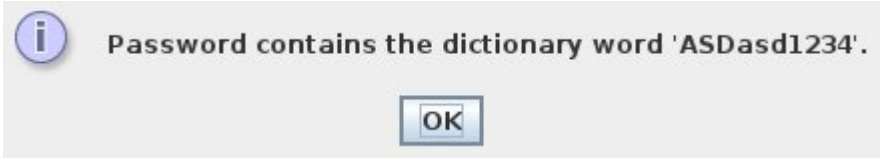
Heslo „asd“ :



Heslo „ASDasd“:



Heslo „ASDasd1234“:



Heslo „sNCNoJzDkn8bzKE978iHFeYXJFaQ“:

Uložený používateľ v DB:

#	user_name	password	salt
1	joe_mama	77+9bgEFV2ocPO+/vVluPu+/vSfw71QyaNlW1Dw71SXgRaGu+/ve+/ve+/vUrw71PPu+/ve+/vTzw73w73w704Ae+/ve+/vS/w703KtGYCe+/ve+/vVsEV++/vSjw73w73w71LMe+/vQ==	vWCgArwjlpRJXYTyhMVH6w==