|  |  |
| --- | --- |
| Bezpieczeństwo aplikacji Internetowych  Dr inż. Maciej Brzozowski | Studenci:  Bogumił Bierć  Łukasz Mosiej |
| Temat: Generowanie haseł |  |

# Środowisko:

- Java 8

- Hibernate 5

- MySql 5.5

- QueryDSL 3.7.2

- Spring Boot 1.3.3

- IntelliJ IDEA, MySQL Workbench, Mozilla Firefox

# Treść zadań

Udostępnij uzytkownikowi możliwość logowania przy użyciu losowo wybranych fragmentów ˙ haseł. Hasła powinny byc przechowywane po stronie serwera z wykorzystaniem funkcji hashujących oraz soli. Hasła powinny spełniac następujące kryteria:

• długość hasła od 8 do 16 znaków,

• co najmniej 5 znaków przy zapytaniu o fragment hasła,

• maksymalnie zapytanie o fragment składający się z połowy hasła jednak nie mniej niż z 5-ciu znaków,

• nalezy sprawdzać ustawienie podawanych znaków na właściwych pozycjach we fragmencie hasła,

• zmiana aktualnego hasła cząstkowego następuje po prawidłowym zalogowaniu - wymagana jest dodatkowa weryfikacja podczas próby zmiany hasła,

• co najmniej dziesięc haseł cząstkowych dla każdego użytkownika

• nalezy uwzględnić wszystkie ograniczenia związane z odstępami czasu logowania oraz uzytkownikami nienależącymi do systemu z poprzednich zajęć.

# Rozwiązania

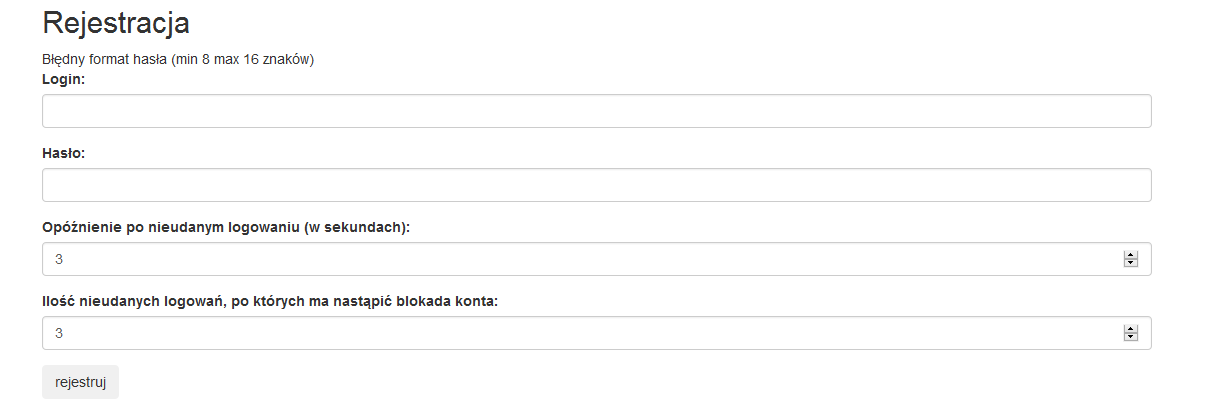
## Rejestracja



*Ekran rejestracji*

### Niepoprawna

[**http://localhost:8085/registerUser?login=bogumil&password=abc&delay=3&attempts=3**](http://localhost:8085/registerUser?login=bogumil&password=abc&delay=3&attempts=3)



### Poprawna

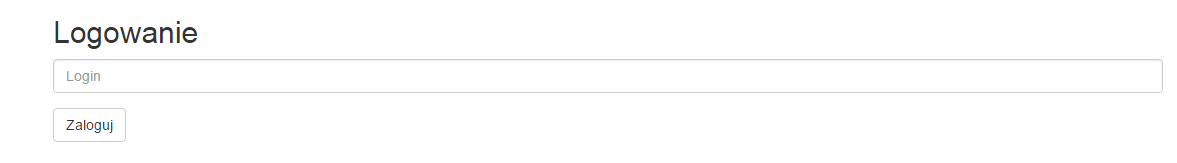
[**http://localhost:8085/registerUser?login=bogumil&password=bogumil123!&delay=3&attempts=3**](http://localhost:8085/registerUser?login=bogumil&password=bogumil123!&delay=3&attempts=3)



## Logowanie hasłem cząstkowym

### Wprowadzanie loginu

**http://localhost:8085/loginWithFragmentLoginCheck?login=bolek**



*Ekran wprowadzania loginu*

### Wprowadzanie hasła

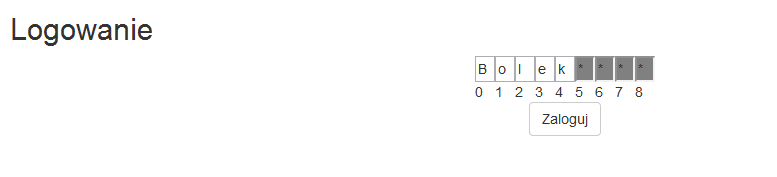
**http://localhost:8085/loginWithFragmentPasswordCheck?login=bolek&password[0]=B&password[1]=o&password[2]=l&password[3]=e&password[4]=k&password[5]=\*&password[6]=\*&password[7]=\*&password[8]=\***



*Ekran wprowadzania hasła cząstkowego*



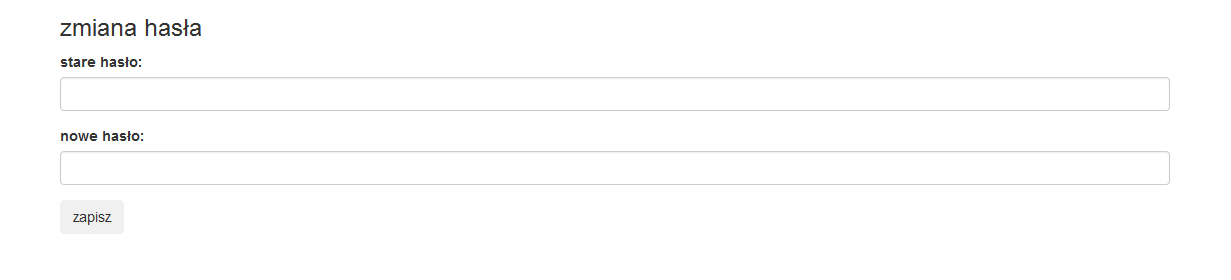
*Zostało wpisane błędne hasło – fragment się nie zmienia*



*Po poprawnym zalogowaniu zmienił sie fragment*

## Zmiana hasła

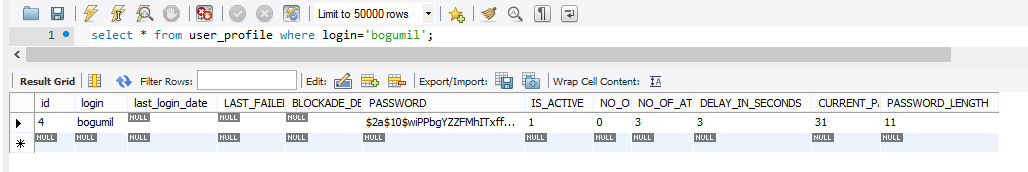
**http://localhost:8085/changePassword?oldPassword=bogumil123!&password=bogumil1234!2**

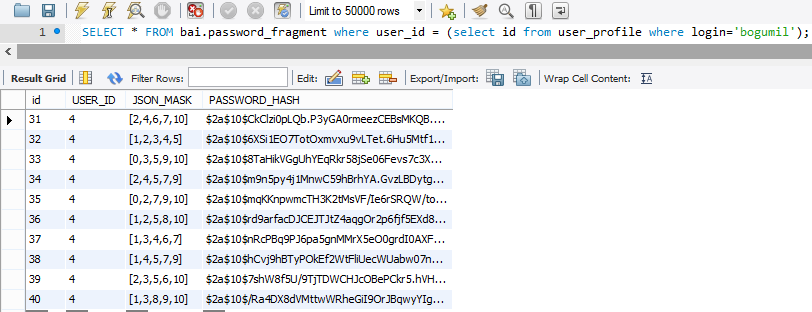


*Wymagana weryfikacja – podanie starego hasła*

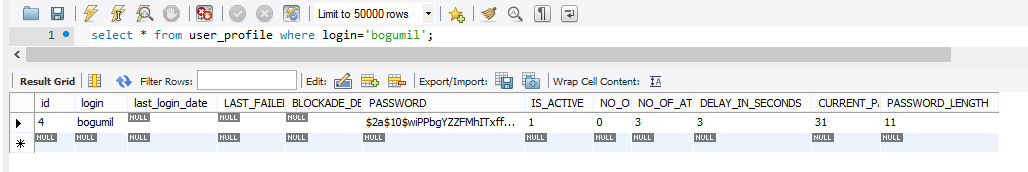
## Dane w bazie

### Po zarejestowaniu





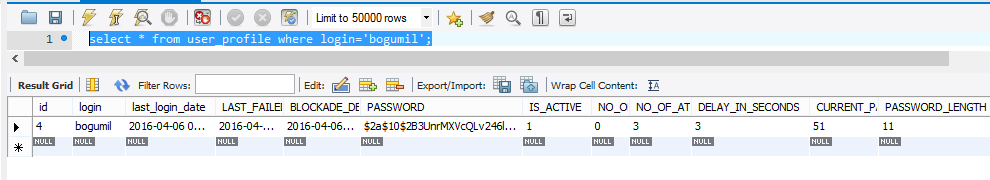
### Po niepoprawnym logowaniu

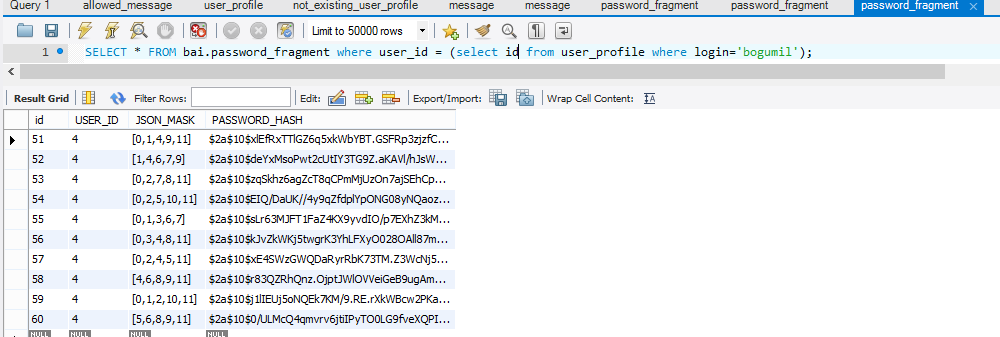


### Po poprawnym logowaniu

Jak widać po niepoprawny logowaniu nie zmienia sie aktualny fragment hasła, po poprawnym logowaniu zmienia się.

### Po zmianie hasła





Na nowo wygenerowane zostały fragmenty haseł oraz ustawiony id aktualnego fragmentu.

## Skrypt tworzący bazę:

**CREATE SCHEMA** `bai`  
 **DEFAULT CHARACTER SET** *utf8*;  
  
**USE** bai;  
  
*-- ----------------------------------------------------------------------  
-- ------- TABLES--------------------------------------------------------  
-- ----------------------------------------------------------------------***CREATE TABLE** USER\_PROFILE (  
 **id INTEGER NOT NULL AUTO\_INCREMENT**,  
 **login VARCHAR**(255) **UNIQUE**,  
 **last\_login\_date DATETIME**,  
 **LAST\_FAILED\_LOGIN\_DATE DATETIME**,  
 **BLOCKADE\_DEADLINE DATETIME**,  
 **PASSWORD VARCHAR**(255),  
 **IS\_ACTIVE BOOLEAN**,  
 **NO\_OF\_FAILED\_LOGINS\_SINCE\_LAST INTEGER**,  
 **NO\_OF\_ATTEMPTS\_BEFORE\_BLOCKADE INTEGER**,  
 **DELAY\_IN\_SECONDS INTEGER**,  
 **CURRENT\_PASSWORD\_FRAGMENT\_ID INTEGER**,  
 **PASSWORD\_LENGTH INTEGER**,  
 **PRIMARY KEY** (**id**)  
);  
  
**CREATE TABLE** NOT\_EXISTING\_USER\_PROFILE (  
 **id INTEGER NOT NULL AUTO\_INCREMENT**,  
 **login VARCHAR**(255) **UNIQUE**,  
 **LAST\_FAILED\_LOGIN\_DATE DATETIME**,  
 **BLOCKADE\_DEADLINE DATETIME**,  
 **IS\_ACTIVE BOOLEAN**,  
 **NO\_OF\_FAILED\_LOGINS\_SINCE\_LAST INTEGER**,  
 **NO\_OF\_ATTEMPTS\_BEFORE\_BLOCKADE INTEGER**,  
 **DELAY\_IN\_SECONDS INTEGER**,  
 **PRIMARY KEY** (**id**)  
);  
  
**CREATE TABLE** MESSAGE (  
 **id INTEGER NOT NULL AUTO\_INCREMENT**,  
 **CONTENT VARCHAR**(555),  
 **OWNER\_ID INTEGER**,  
 **PRIMARY KEY** (**id**)  
);  
  
**ALTER TABLE** MESSAGE **ADD CONSTRAINT** messageOwnerId **FOREIGN KEY** (**OWNER\_ID**) **REFERENCES** USER\_PROFILE (**id**);  
  
**CREATE TABLE** ALLOWED\_MESSAGE (  
 **id INTEGER NOT NULL AUTO\_INCREMENT**,  
 **USER\_ID INTEGER**,  
 **MESSAGE\_ID INTEGER**,  
 **PRIMARY KEY** (**id**)  
);  
  
**CREATE TABLE** PASSWORD\_FRAGMENT (  
 **id INTEGER NOT NULL AUTO\_INCREMENT**,  
 **USER\_ID INTEGER**,  
 **JSON\_MASK VARCHAR**(255),  
 **PASSWORD\_HASH VARCHAR**(255),  
 **PRIMARY KEY** (**id**)  
);  
  
*-- ----------------------------------------------------------------------  
-- ------- DATA ---------------------------------------------------------  
-- ----------------------------------------------------------------------  
  
-- USER\_PROFILE***INSERT INTO** `user\_profile` (**`id`**, **`login`**, **`last\_login\_date`**, **`LAST\_FAILED\_LOGIN\_DATE`**, **`BLOCKADE\_DEADLINE`**, **`PASSWORD`**, **`IS\_ACTIVE`**, **`NO\_OF\_FAILED\_LOGINS\_SINCE\_LAST`**, **`NO\_OF\_ATTEMPTS\_BEFORE\_BLOCKADE`**, **`DELAY\_IN\_SECONDS`**, **`CURRENT\_PASSWORD\_FRAGMENT\_ID`**, **`PASSWORD\_LENGTH`**)  
**VALUES** (1, **'antek'**, **NULL**, **NULL**, **NULL**, **'$2a$10$TBygVhH4SadL8QV.z1UGKOSyxira3rfcSn4nAGvB0v3b4nyi5LByq'**, 1, 0, 3, 3, 1,  
 9); *-- Antek123!***INSERT INTO** `user\_profile` (**`id`**, **`login`**, **`last\_login\_date`**, **`LAST\_FAILED\_LOGIN\_DATE`**, **`BLOCKADE\_DEADLINE`**, **`PASSWORD`**, **`IS\_ACTIVE`**, **`NO\_OF\_FAILED\_LOGINS\_SINCE\_LAST`**, **`NO\_OF\_ATTEMPTS\_BEFORE\_BLOCKADE`**, **`DELAY\_IN\_SECONDS`**, **`CURRENT\_PASSWORD\_FRAGMENT\_ID`**, **`PASSWORD\_LENGTH`**)  
**VALUES** (2, **'bolek'**, **NULL**, **NULL**, **NULL**, **'$2a$10$zeYubYCCCjjCwkEnH.Djd.O1HabXrZ4SgW5EIdNdSsgHt55pVyFnu'**, 1, 0, 3, 3, 11,  
 9); *-- Bolek123!***INSERT INTO** `user\_profile` (**`id`**, **`login`**, **`last\_login\_date`**, **`LAST\_FAILED\_LOGIN\_DATE`**, **`BLOCKADE\_DEADLINE`**, **`PASSWORD`**, **`IS\_ACTIVE`**, **`NO\_OF\_FAILED\_LOGINS\_SINCE\_LAST`**, **`NO\_OF\_ATTEMPTS\_BEFORE\_BLOCKADE`**, **`DELAY\_IN\_SECONDS`**, **`CURRENT\_PASSWORD\_FRAGMENT\_ID`**, **`PASSWORD\_LENGTH`**)  
**VALUES** (3, **'lolek'**, **NULL**, **NULL**, **NULL**, **'$2a$10$kxmsLKFF0RlC6tUv1/JthuRVp6j79tl.nLvkas14KYdxy9M36VYpy'**, 1, 0, 3, 3, 21,  
 9); *-- Lolek123!  
  
-- PASSWORD\_FRAGMENT***INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (1, 1, **'[2,3,4,6,8]'**, **'$2a$10$Aze/mY3WtBIWdbuPoRwZoeOl2gFVkXMohwSQo15d5ci0Tm39ZyO8i'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (2, 1, **'[0,1,3,5,8]'**, **'$2a$10$vJSCTH5y.ZVR5/Zq2RrhxOq0829mTECKbIyOAjS9F1wISHlzoR5yK'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (3, 1, **'[0,1,4,7,8]'**, **'$2a$10$DWsaMKiiFE79IKM3ExE9qOIazP7a98jFgUr64mkglDoeHQ1JMYFW2'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, `PASSWORD\_HASH`)  
**VALUES** (4, 1, **'[1,2,3,7,8]'**, **'$2a$10$Tdkylvhw1Sjodi35jrBlgudXtnu139KGOWGLxKmPFH3p5q0moaoPG'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (5, 1, **'[0,1,3,5,7]'**, **'$2a$10$NVOynX0aOA4NWFgBj48FbeuGJAh60MMgODbLA6DIUtQBZp3KZ6Uci'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (6, 1, **'[0,1,2,3,7]'**, **'$2a$10$kZ8I/AJuNHcAJy21XfuVheG2QBAm63mEBzp5aGZq2zuD2eO09A0lO'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (7, 1, **'[0,2,3,4,7]'**, **'$2a$10$n.K/wdXi1udrrf12db4sreZtaaozZ5Y/a1B4WEh0gl11vLRoQzsQC'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (8, 1, **'[1,2,3,5,8]'**, **'$2a$10$DtDItRp9d4OmG.5iyrZWC.X7gNJv.QV1cYQmG17NVyIJGJfpdYnj6'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (9, 1, **'[1,2,6,7,8]'**, **'$2a$10$ifMAcgSFvK/D9i5LLq/QVOR7XDZDWqoEp4EBvUrXcytaxChO1QlvK'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (10, 1, **'[2,4,5,7,8]'**, **'$2a$10$9r4yeWECu2cWI4geWkwX0e96NzB0iFEagurL5RH5P7MLfaAzu5YNe'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (11, 2, **'[0,1,5,6,8]'**, **'$2a$10$ozjcbxCwu/kz7J3IQ8wROulnhL2A7rwvCJyz6q161Tmnk49PAAcYm'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (12, 2, **'[0,4,5,6,8]'**, **'$2a$10$.VMQQF72gfMTWzZDFbadfuZc7xCHC9Axh9LZ7Fyi23TerLk.bpRQ6'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (13, 2, **'[0,2,3,7,8]'**, **'$2a$10$sIxxSn0IVAn6pVPRhaTGbO/9q52bLsLRkVRv.51iz3k/Ilq0Tm4S2'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (14, 2, **'[1,3,4,5,8]'**, **'$2a$10$eMBO..f1x6dSf8aRwCuU3.cV6WPO/nEcOf5JHFkHsSTNwSLqCsKya'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (15, 2, **'[0,1,2,3,4]'**, **'$2a$10$W5tFAqHCpOkcHK9MYzVW..uUVTlts0Hv46CulmsLwzwkPWGFTNcTe'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (16, 2, **'[0,3,4,5,6]'**, **'$2a$10$H5QdiFz8mdddunq5sIS.d.5xiNZKJRDWZfwch3CyhH9QR4ZIEOdgq'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (17, 2, **'[0,1,4,6,8]'**, **'$2a$10$xjgAOvLzzYChESIeFw8flO3T7Z7eH82rWDhbxz7g/OdxyB4uK.jpa'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (18, 2, **'[0,2,3,4,7]'**, **'$2a$10$7Uvo0f9yiW2yP3J3s/hEieeXBWfg2t1XQdbZS1uMhsUstkwlkwpne'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (19, 2, **'[0,3,4,6,8]'**, **'$2a$10$9XsAuV4A7Ka.oUtDPfDchOB6ycK7yg1xpxpdwYmLLZryTxy7Xz0jy'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (20, 2, **'[1,3,4,5,6]'**, **'$2a$10$GEr6og/oyKW..xznIIBt0uvnU6YngoBn5NDPhJRqMV2IV3S/tVp6S'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (21, 3, **'[0,2,3,5,6]'**, **'$2a$10$h8ZBOHVsKyyDEf3o3P2Nx.pob5eapLafIjI1LjGmMz3urTTCrkX6W'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (22, 3, **'[0,1,3,7,8]'**, **'$2a$10$1hxHceTM4cTOJChRHEl1Pu0sooaVZUiEH8sa.bHv/EIW2R7wQwy8K'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (23, 3, **'[2,4,5,6,7]'**, **'$2a$10$3lvKNsBg4G6P1qxpMoxtKevx0jkgzyQNgHTtQZe62A4e667NTFE0e'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (24, 3, **'[0,1,2,3,7]'**, **'$2a$10$C2Enmb6Yl/zcJkw3WfhsU.7mZZpddn8xuTNCRKlyCHRomKa3C8CSm'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (25, 3, **'[0,1,2,4,8]'**, **'$2a$10$ZxW2L4nhliU/Gy.Sk31ad.iNdeuYslaUQt72NyQSj/SG9rE5BHH9K'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (26, 3, **'[1,2,5,7,8]'**, **'$2a$10$tAJjLBsU4KhC1b3cABy7m.vgtkRmXb6NCgIg/3pzI2qrP1741LduS'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (27, 3, **'[0,3,4,5,8]'**, **'$2a$10$lUyZiNBh/u9S3ACwGOwwbeRD66nRfMObBVqO1952FJcjropC3eZV6'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (28, 3, **'[1,2,3,4,5]'**, **'$2a$10$B871/H5yiiCwPAboFNPiIeV2/E8sy71esffYiLST9BcLmlvAn1f/C'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (29, 3, **'[0,2,3,4,8]'**, **'$2a$10$w2X9bnzuzYrpuR3G5Yxb.OIiALExA3zWwWpCcf0VWwC2QjebeuhKi'**);  
**INSERT INTO** `password\_fragment` (**`id`**, **`USER\_ID`**, **`JSON\_MASK`**, **`PASSWORD\_HASH`**)  
**VALUES** (30, 3, **'[0,1,5,6,8]'**, **'$2a$10$8/DgbobXXj/KF2Tt7sZcTuyJszKgHXb.gANP59c0KadpoYzYuWq1.'**);  
  
*-- MESSAGE***INSERT INTO** MESSAGE (**ID**, **CONTENT**, **OWNER\_ID**) **VALUES** (1, **'Wsiada baba do windy a tam schody'**, 1);  
**INSERT INTO** MESSAGE (**ID**, **CONTENT**, **OWNER\_ID**) **VALUES** (2, **'Wchodzi popek do salonu Ery i prosi telefon na firme'**, 1);  
**INSERT INTO** MESSAGE (**ID**, **CONTENT**, **OWNER\_ID**) **VALUES** (3, **'Dlaczego murzyn nie może być żydem? Bo bez przesady.'**, 2);  
**INSERT INTO** MESSAGE (**ID**, **CONTENT**, **OWNER\_ID**) **VALUES** (4, **'0.7 zgłoś się'**, 2);  
**INSERT INTO** MESSAGE (**ID**, **CONTENT**, **OWNER\_ID**) **VALUES** (5, **'pehap pehap pehap pfffffff'**, 2);  
  
*-- ALLOWED\_MESSAGE***INSERT INTO** ALLOWED\_MESSAGE (**USER\_ID**, **MESSAGE\_ID**) **VALUES** (1, 3);  
**INSERT INTO** ALLOWED\_MESSAGE (**USER\_ID**, **MESSAGE\_ID**) **VALUES** (3, 1);  
**INSERT INTO** ALLOWED\_MESSAGE (**USER\_ID**, **MESSAGE\_ID**) **VALUES** (3, 2);  
**INSERT INTO** ALLOWED\_MESSAGE (**USER\_ID**, **MESSAGE\_ID**) **VALUES** (3, 5);