Politechnika Białostocka	Prowadzący: dr inż. Maciej Brzozowski
Bezpieczeństwo Aplikacji Internetowych	
Temat: Generowanie haseł.	Ocena:
1. Dominik Adrian Kruk	
2. Mateusz Matocha	

1. Specyfikacja środowiska i technologii:

Język programowania: Java EE version 1.8.171

Baza danych: Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit

Production

Technologie: Spring 4.0; Thymeleaf 3.0.9; Hibernate 5.2; HTML 5;

System Operacyjny: Windows 10 Home Edition Wersja 10.0.17134 Kompilacja 17134

Program do zarządzania bazą danych: Oracle SQL Developer Version 17.3.0.271

Środowisko programistyczne(IDE): IntelliJ IDEA 2017.3.2 (Ultimate Edition)

Build #IU-173.4127.27, built on December 25, 2017

- 2. Wykonanie zadań:
 - Logowanie przy użyciu losowych wybranych fragmentów haseł przechowywanych po stronie serwera z wykorzystaniem funkcji hashujących i soli z następującymi kryteriami:
 - Długość od 8 do 16 znaków;
 - Maksymalnie zapytanie o fragment składający się z połowy hasła ale nie mniej niż pięć znaków;
 - Walidacja miejsca znaków;
 - Zmiana obecnego hasła po zalogowaniu z dodatkową weryfikacją:
 - Minimum 10 haseł cząstkowych;

Rozwiązania:

1) Select * from passwords:

	⊕ PASS_ID	⊕ USER_ID	∯ MASK	♦ PASSWORD_HASH
1	810	351	0110100110000000	\$2a\$11\$4rRqJ7UDm0b0cxSEGcZ9fuJe4abjLLDJfRHQ2IkkuKbrxNhSzY7uC
2	811	351	1101011000000000	\$2a\$11\$M64Uq8VPI0.OhyiAupuE7e18vlxHi2P2ZaFWKRMaVSNjibjIscUTC
3	812	351	1001101100000000	\$2a\$11\$6JIUqTF/kydxGh5u9zHDYu.xBU94GjVxeHKXIhhAO/MT2giAyTJxS
4	813	351	0011101010000000	\$2a\$11\$P4aCAjVx48VnIS30ITz1GuNlx1HCTBQpSZJ4TFIYN1Lo1XdyfaC7S
5	₩14	351	0111100100000000	\$2a\$11\$5x2kE5Wv5MV9CI4FJmMMvOTfiR6soHDrjmkg/W9HIIcmOOC1bTpT2
6	815	351	0011001110000000	\$2a\$11\$DePUlaz5GU2csBb0LmcC0eKK0ZrQOniNloZmVgs3d.0LxiTLJBL0q
7	816	351	1101110000000000	\$2a\$11\$pXAXzCTMrwGVW8jY25qgxOY48cQRicj4L4tmsRbiOfq0Z5GNmRSqm
8	817	351	1010011010000000	\$2a\$11\$nx0qTsX0.sQvAYWPGtFHEeG3/46A1qnFkkkWmp0pTpozW9J1n/KGy
9	818	351	0101110100000000	\$2a\$11\$h9CoC2D4yUhctkdurwoQ/u7RGfuop4xgckz/aDNRx5Xbg2nQx2iJ6
10	819	351	0101100110000000	\$2a\$11\$AmPg7gPZNCRrz7n/r5v4D.Nv1.nw12uN/JCeCd9N2/BeIhviExnRy
11	820	352	0110101010000000	\$2a\$11\$mXPi2qBL6XQGxWYAMDnbVOgpEfX0bjg1ByhInk.3Hu5Ymkc38Jvw2
12	821	352	1000111010000000	\$2a\$11\$00379q034yakmcfu3Kht3.ktDnocfKJ9THYdZPtN29DR76oFG77I.
13	822	352	1010001110000000	\$2a\$11\$utW1QCeYmypItLsgio2A50jex9TkCHkr2sezgJjHycJeDQSwqHusK
14	823	352	1010111000000000	\$2a\$11\$MZW0NjzQPRxbgeDkI/OibOsNLv.ZcllBiQavA4P1E9BCeUin6TM02
15	824	352	0111001010000000	\$2a\$11\$mae.0hdiiF4ppZ3Xd4m7aO6gG1rspohZPXR5H0E6DH0tWh7xVVeqS
16	825	352	1010011010000000	\$2a\$11\$6VMEfQneVNfRB3SFrP7y6ecimPTFCzFPHjE6TYkoY6BkMk/ZFVMdS
17	826	352	0110110010000000	\$2a\$11\$7ctlkSRCV102HB/jWINzvefrorS.QGQ/bS4mQ6wwfe0kOoA38hP22
18	827	352	1001011100000000	\$2a\$11\$Y6RsZftjXrc2tXvXbE/uP.zxTuHRbS0IR.eLyVLEbu24bF0y3p1E0
10	010	252	0100111100000000	COSCILICONSCRIBING CONCENEITION OF A CONTAINED TO A DESCRIPTION OF A DESCR

Wynikiem zapytania są kolejne cząstkowe hasła użytkownika z dodatkiem soli i funkcji hashującej(bcrypt);

2) Walidacja długości hasła:

Rejestracja

username
•
Hasło powinno mieć od 8 do 16 znaków
•
Hasło powinno mieć od 8 do 16 znaków
Rejestruj

3) Logowanie przy użyciu fragmentów haseł:

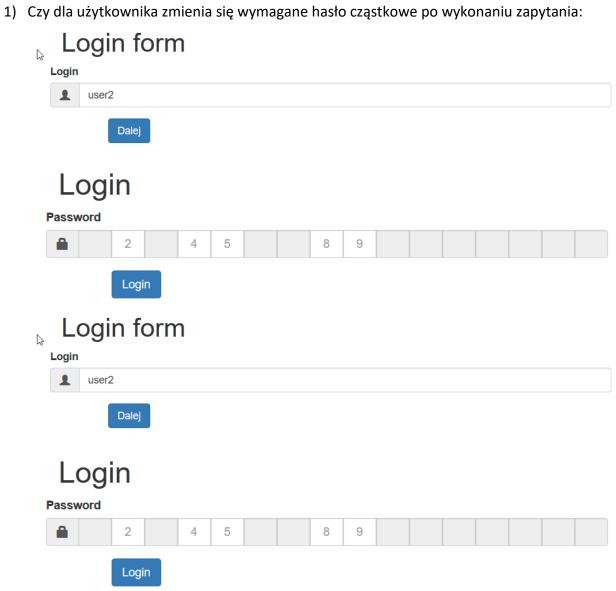
Login

Password 1 4 6 8 9 Login

Zmiana hasła:



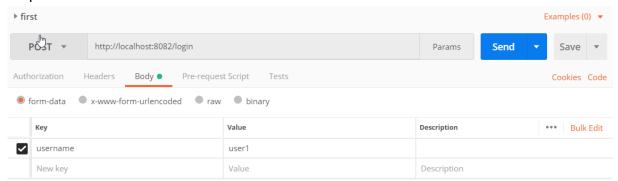
Testy:



3. Czy użytkownikowi zmienia się wymagane hasło po nieprawidłowym logowaniu:

pobranie maski:

Request:



Response:

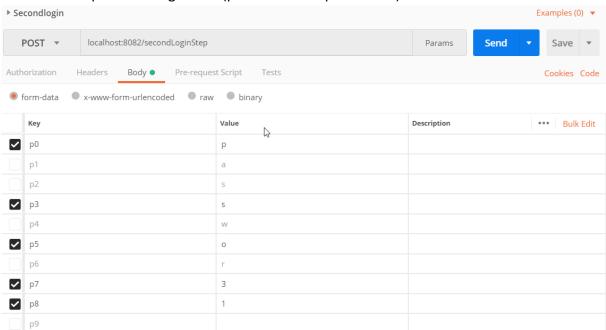
Napisz

-post

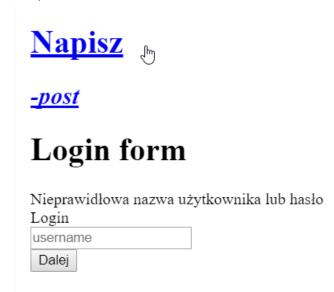
Login



Przesłanie nieprawidłowego hasła(prawidłowe to password1):



Response:

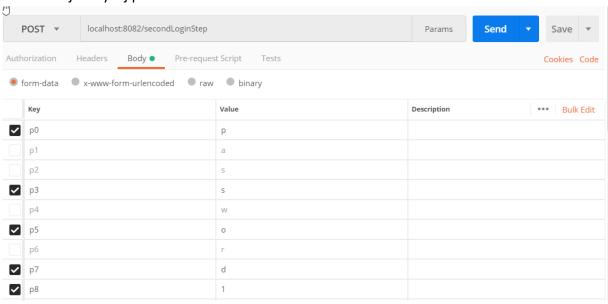


Ponowny Request po maskę:



czy użytkownikowi zmienia się maska po prawidłowym zalogowaniu:

Dla maski jak wyżej przesłanie hasła:



po poprawnym zalogowaniu, wylogowaniu i ponownym pobraniu maski:

