|  |  |
| --- | --- |
| Politechnika Białostocka  Bezpieczeństwo Aplikacji Internetowych | Prowadzący: dr inż. Maciej Brzozowski |
| Temat: PS-5 SQL Injection   1. Dominik Adrian Kruk 2. Mateusz Matocha | Ocena: |

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

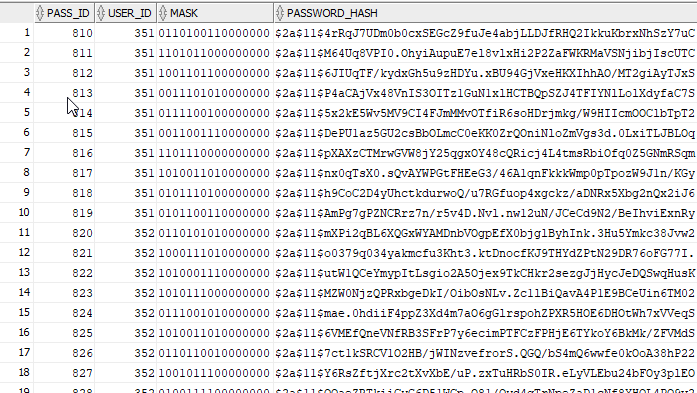
Technologie: Spring 4.0; Thymeleaf 3.0.9; Hibernate 5.2; HTML 5;   
System Operacyjny: Windows 10 Home Edition Wersja 10.0.17134 Kompilacja 17134  
Program do zarządzania bazą danych: Oracle SQL Developer Version 17.3.0.271  
Środowisko programistyczne(IDE): IntelliJ IDEA 2017.3.2 (Ultimate Edition)

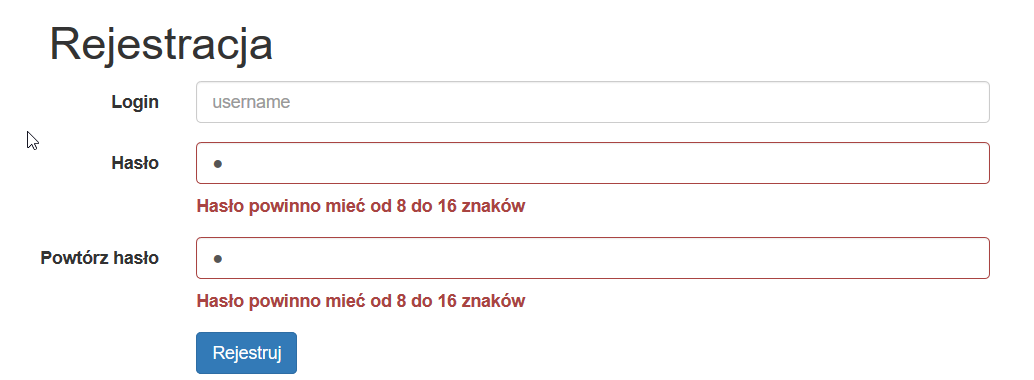
Build #IU-173.4127.27, built on December 25, 2017

1. Wykonanie zadań:
2. 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;

Rozwiązanie:

1. Select \* from passwords:  
     
   Wynikiem zapytania są kolejne cząstkowe hasła użytkownika z dodatkiem soli i funkcji hashującej;
2. Walidacja długości hasła:



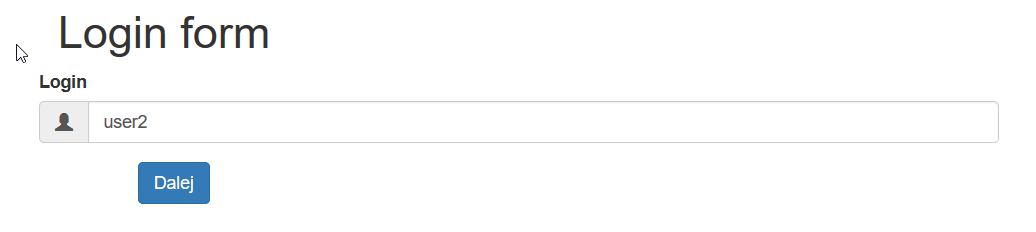
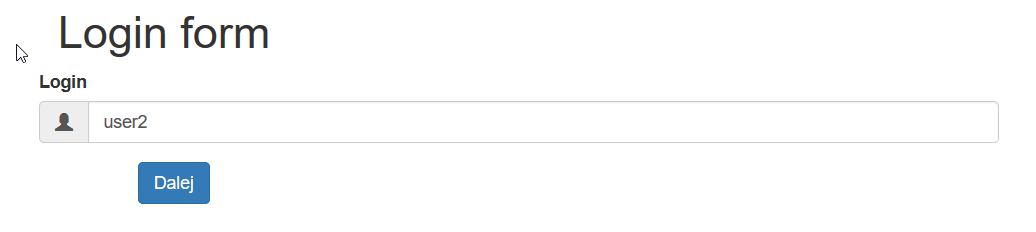
1. Logowanie przy użyciu fragmentów haseł:

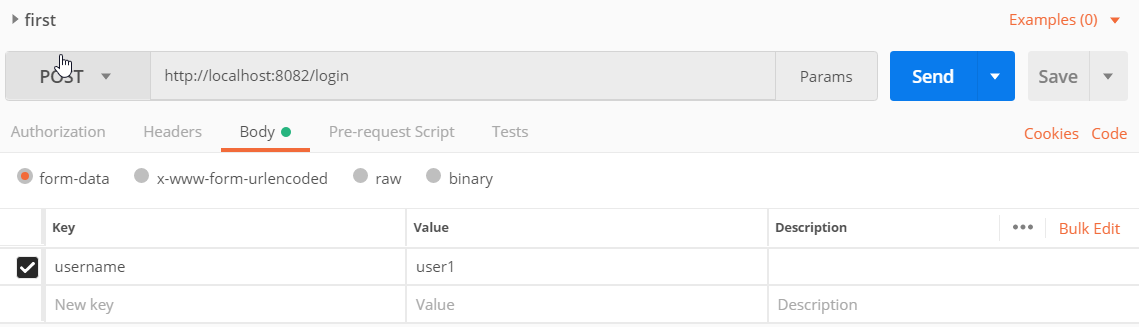


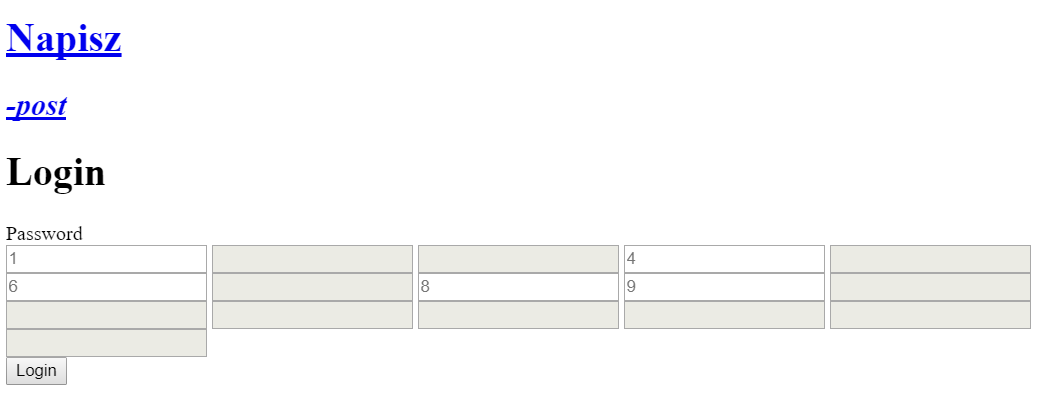
1. Zmiana hasła:

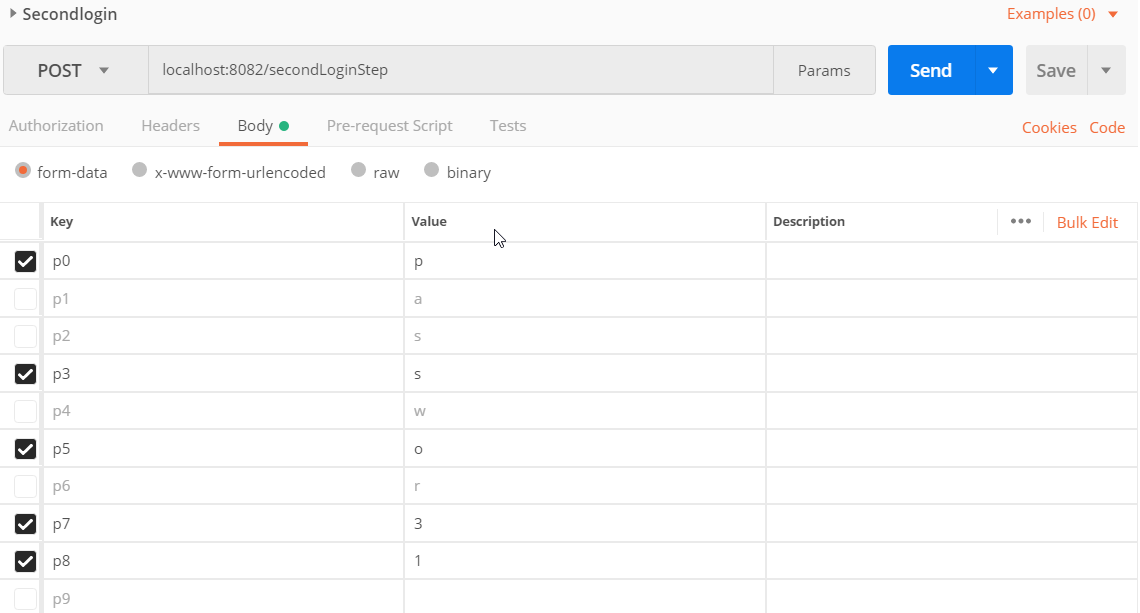
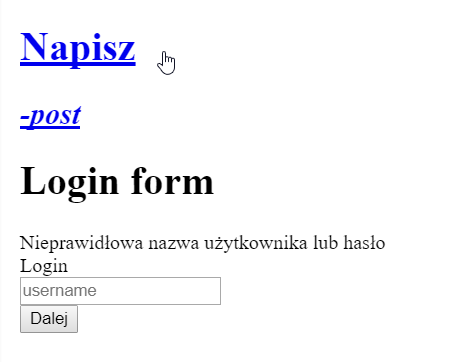


Testy:

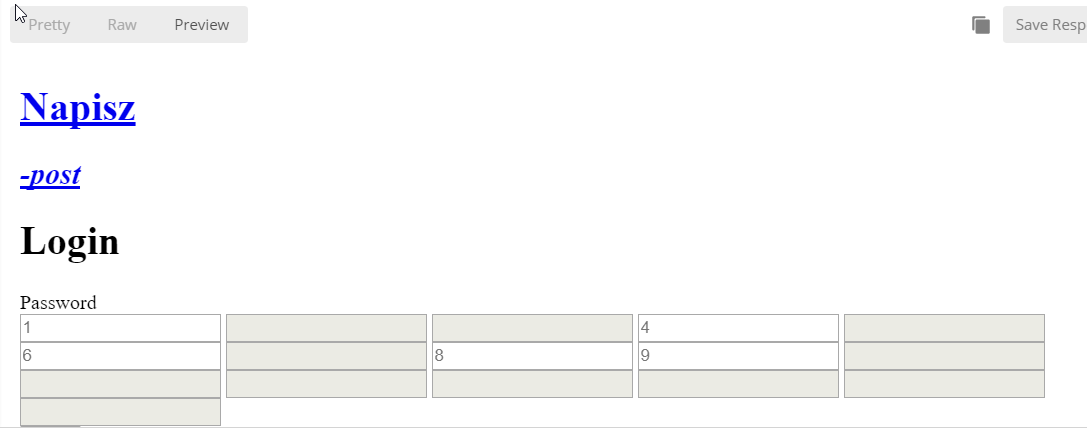
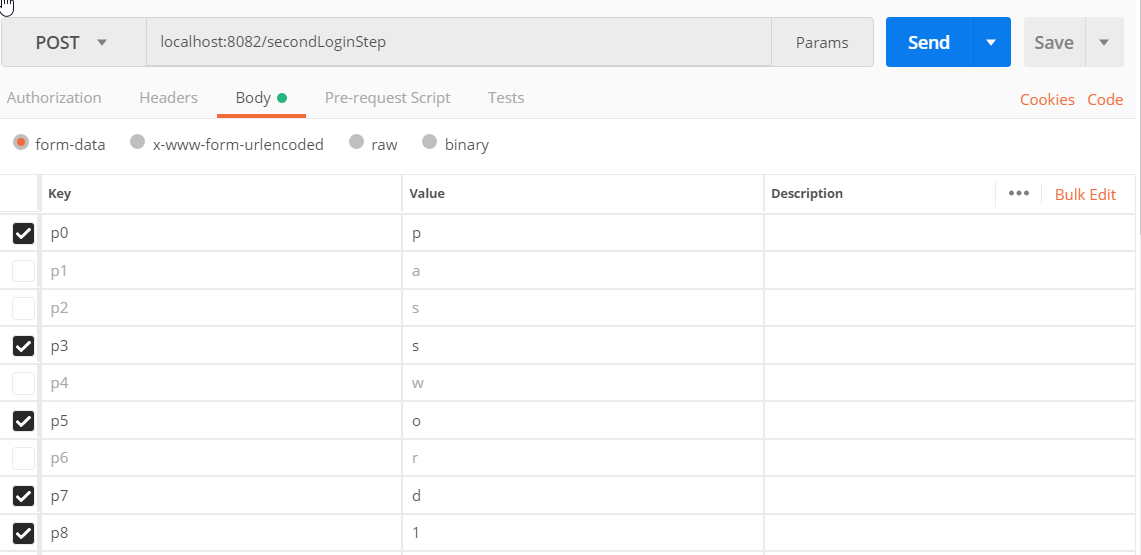
1. Czy dla użytkownika zmienia się wymagane hasło cząstkowe po wykonaniu zapytania:  
     
   
2. Czy użytkownikowi zmienia się wymagane hasło po nieprawidłowym logowaniu:

pobranie maski:  
Request:  


Response:  


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:  
