Sprawozdanie z projektu zaliczeniowego przedmiotów Projektowanie Systemów Informatycznych   
i Technologie Aplikacji Biznesowych.

**Członkowie zespołu:**

Krzysztof Śpionek 221506

Szymon Zawadzki 221515

**Cel:**

Stworzenie aplikacji webowej obsługującej rejestrację, umożliwi logowanie oraz zmianę hasła wykorzystującej bazę danych Oracle Database.

**Technologie i środowiska użyte w projekcie:**

- Oracle Database 12 z wykorzystaniem Oracle SQL Developer.

- Java EE z wykorzystaniem JSP i Serwletów (JDK + JRE w wersji 9.0.13).

- Eclipse JEE build z września 2018r.

- Apache Tomcat 9.0.13.

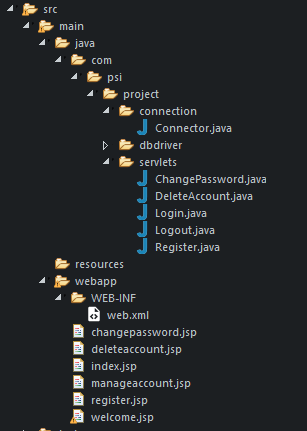
- Apache Maven 3.6.0.

- Sterownik JDBC Oracle – OJDBC8 (groupID Mavena: com.oracle.jdbc dla wersji 12.2.0.1).

**Opis aplikacji:**

Aplikacja została stworzona w środowisku Eclipse JEE. Wykorzystuje ona narzędzie Maven, które pozwala na uproszczenie i automatyzację budowy nowoczesnych aplikacji w języku Java. Wykonany projekt wykorzystuje archetyp maven-archetype-webapp, który pozwala na budowę dynamicznych aplikacji webowych. Projekt został stworzony w oparciu o technologię JSP z pośrednictwem Serwletów.

Aplikacja składa się z 6 stron JSP, 5 serwletów oraz z klasy Connector, która przechowuje wszystkie metody do łączenia się i wykonywania manipulacji na bazie danych Oracle.   
Struktura przedstawiona na rysunku 1.



Rysunek 1: struktura projektu.

Każdy z pięciu serwletów ma swoje określone zadanie, które by mógł je wykonać, wykorzystuje klasę Connector. Jest ona swoistym rdzeniem przechowującym między innymi logikę w jakim stanie jest konto, na które chcemy się zalogować. Zaimplementowane jest 6 scenariuszy z 5 różnymi komunikatami:

1. Po wpisaniu adresu mailowego, którego nie ma w bazie zwracany jest wynik 0, który wywołuje komunikat "Konto nie istnieje!".
2. Po wpisaniu poprawnego adresu mailowego, lecz niepoprawnego hasła zwracany jest  
   wynik 1, który wywołuje komunikat "Niepoprawne dane...".
3. Po trzeciej nieudanej próbie logowania zwracany jest wynik 4, który wywołuje komunikat  
   "Przekroczono limit błędnych prób logowania! Następuje zablokowanie konta.". Dodatkowo konto jest blokowane na okres 5 minut.
4. W trakcie trwania blokady przy próbie logowania zwracany jest wynik 3, który wywołuje komunikat "Konto jest zablokowane!".
5. Po upłynięciu czasu blokady i poprawnym wpisaniu danych (lub gdy po prostu wpiszemy poprawny adres email i hasło bez przekroczenia limitu dostępnych prób logowania) zwracany jest wynik 2, który pozwala nam na udane logowanie. Przechodzimy wtedy do strony welcome.jsp.
6. W przypadku, gdy użytkownik usunie konto, poprzez odpowiednie procedury użytkownik zostaje wylogowany. Konto zostanie oznaczone jako archiwalne, a przy próbie zalogowania się na nie sprawdzane jest dodatkowo, czy konto nie należy do listy kont archiwalnych. W przypadku, gdy należy, zwrócony zostanie wynik 0 (opisany w punkcie 1).

**Dodatkowe zaimplementowane elementy:**

1. Każde logowanie jest zapisywane w bazie danych z uwzględnieniem adresu IP, z którego użytkownik się chciał logować.
2. Hasła są szyfrowane przy pomocy funkcji hashującej SHA-256.
3. Każde użyte hasło jest zapamiętywane w bazie danych, sprawdzane one są przy próbie zmiany hasła do konta. W przypadku, gdy hasło było już kiedyś użyte w danym koncie, nie jest ono przyjmowane jako nowe, przez co nie możemy go użyć (zostajemy powiadomieni o zdarzeniu stosownym komunikatem).
4. Po poprawnym zalogowaniu się na konto jest tworzona sesja trwająca 5 minut odnawiana po dowolnej interakcji w obrębie zalogowanego konta. W przypadku braku interakcji, sesja wygasa, przez co wymagane jest ponowne zalogowanie się na konto.

**Baza danych:**

Baza danych została utworzona w środowisku SQL Developer Oracle. Składa się z 4 tabel:

- Logins – która jest tabelą główną przechowującą informacje dotyczące loginu użytkownika w tym wszelkie flagi.

- Logs – która przechowuje zapisy logowań użytkowników w systemie. Połączona kluczem obcym z tabelą Logins poprzez pole Id.

- Passwords – która przechowuje wszystkie użyte kiedykolwiek hasła dla konta użytkownika. Połączona kluczem obcym z tabelą Logins poprzez pole Id.

- Ips – która była przeznaczona na przechowywanie numerów IP przypisanych do użytkownika. Połączona kluczem obcym z tabelą Logins poprzez pole Id.

Dodatkowo na tabela zostały ustawione wyzwalacze:

Wyzwalacz NUMBEROFLOGS na tabeli Logs, zlicza niepoprawne logowania, ustawia blokadę w razie przekroczenia limitu liczby logowań oraz znosi blokady dla wszystkich kont jeżeli blokada trwa powyżej 5 minut.

Wyzwalacz ZERONUMBEROFLOGS na tabeli Logs zeruje licznik niepoprawnych logowań w momencie poprawnego zalogowania użytkownika.

Wyzwalacz PasswordInsert na tabeli Logins wprowadza hasła do tabeli historycznej Passwords.

Zastosowane zostały również procedury:

RemoveLogin – do ustawienia konta jako archiwalne.

UpdatePassword – do aktualizacji hasła użytkownika.

AddLogin – do dodania loginu w tabeli Logins

AddIp – do dodania Ip w tabeli Ips

UpdateBlockade – do zniesienia blokady kont spełniających warunek upływu 5 minut wykorzystująca funkcję timestamp\_difference do wyliczania różnicy czasu.