Wykład 3
Inżynieria oprogramowania

Przykład 1

Bezpieczeństwo(2)

wg „The Java EE 5 Tutorial

Autor: Zofia Kruczkiewicz

Struktura wykładu

1. **Utworzenie użytkowników i ról na serwerze aplikacji Sun Java System Application Server (GlassFish)**
2. **Definiowanie ról w serwerze *Tomcat Web Server***
3. **Konfigurowanie logowania**
4. **Wstawianie ról użytkowników do aplikacji**
5. **Tworzenie i konfiguracja ograniczeń bezpieczeństwa dla typu użytkownika administrator z największymi ograniczeniami**
6. **Tworzenie i konfiguracja ograniczeń bezpieczeństwa dla typu użytkownika z wybranymi ograniczeniami**
7. **Ustawienie czasu sesji**
8. **Zawartość deskryptora aplikacji *web.xml***
9. **Mapowanie mechanizmów bezpieczeństwa z aplikacji do serwera aplikacji - uruchomienie aplikacji w trybie uwierzytelniania *Form-Based Authentication*, zabezpieczenia przez role**
10. **Uruchomienie aplikacji w trybie uwierzytelniania *Basic-Based Authentication*, zabezpieczenia przez role**

1. Utworzenie użytkowników i ról na serwerze aplikacji Sun Java System Application Server (GlassFish)

1) Dodanie użytkowników do Serwera aplikacji JavaEE

- Uruchom **Serwer aplikacji** (np. klikając prawym klawiszem myszy w zakładce **Services** środowiska NetBeans6.1na opcję **GlassFish V2** i wybierając z menu pozycję **Start**)
- Uruchom **Admin Console** (np. klikając prawym klawiszem myszy w zakładce **Services** na opcję **GlassFish V2** i wybierając z menu pozycję **View Admin Console** lub po uruchomieniu przeglądarki podając adres url np. **http://localhost:13780/login.jsf**. Port serwera np. 13780 jest indywidualnie ustalany podczas instalacji serwera.)
- Należy zalogować się podając np.. Nazwę użytkownika **admin** oraz hasło **adminadmin** (można to zmienić albo podczas instalacji lub wg wskazówek poadnych w dalszej części)
- Należy wybrać opcję **Configuration** w drzewie Admin Console.
- Należy wybrać opcję **Security** w drzewie Admin Console.
- Należy wybrać opcję **Realms**:
  1. Należy wybrać opcję ***admin-realm*** do wstawienia użytkowników występujących w roli administratorów Serwera Aplikacji.
  2. Należy wybrać opcję ***file*** do wstawienia nowego użytkownika, który może być uwierzytelniany w aplikacjach JavaEE
  3. Do opcji **certificate** można wprowadzić jedynie certyfikaty ustalone np. za pomocą narzędzia ***keytool***

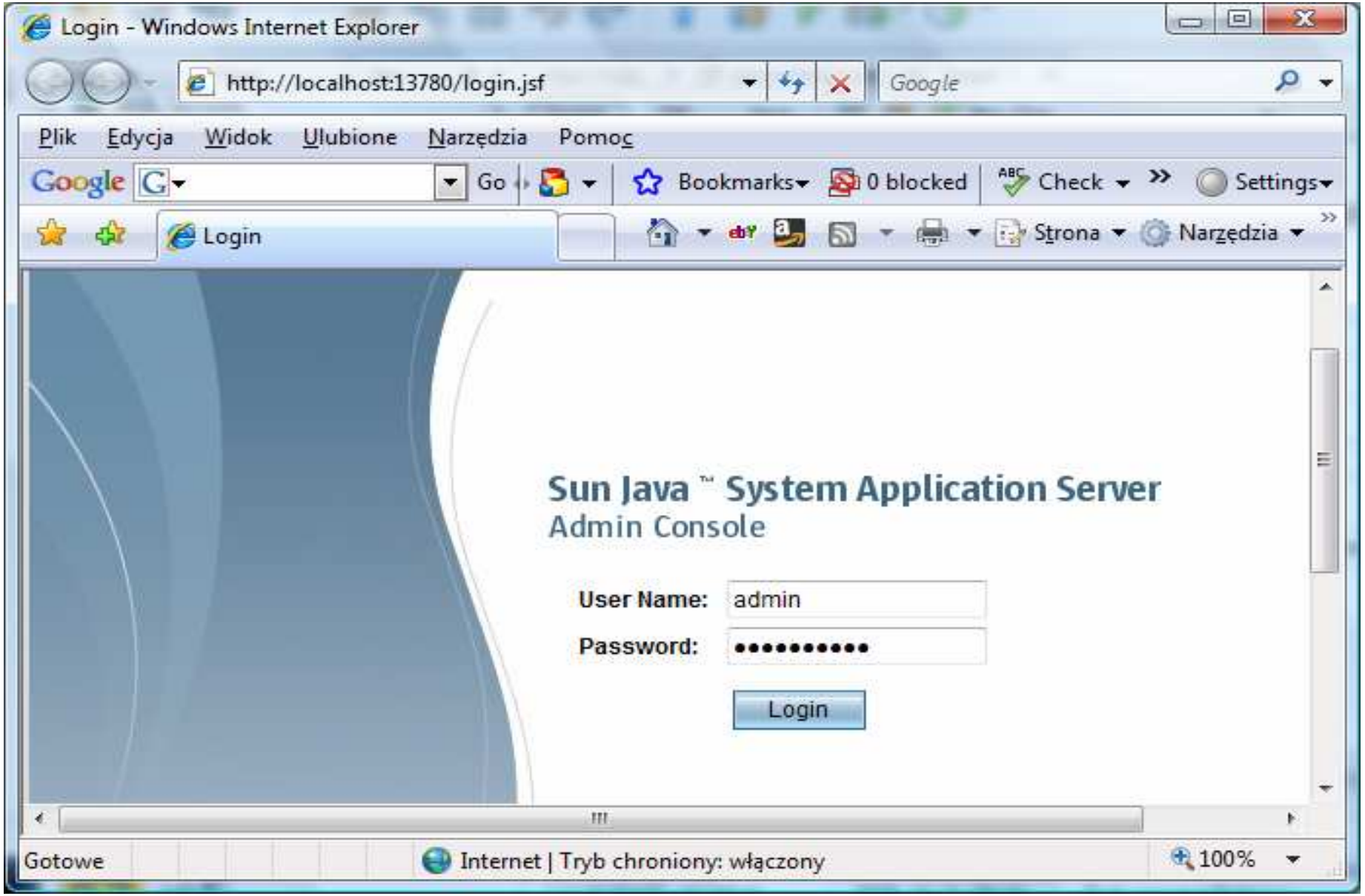
Ad 1, 2 *file, admin-realm*

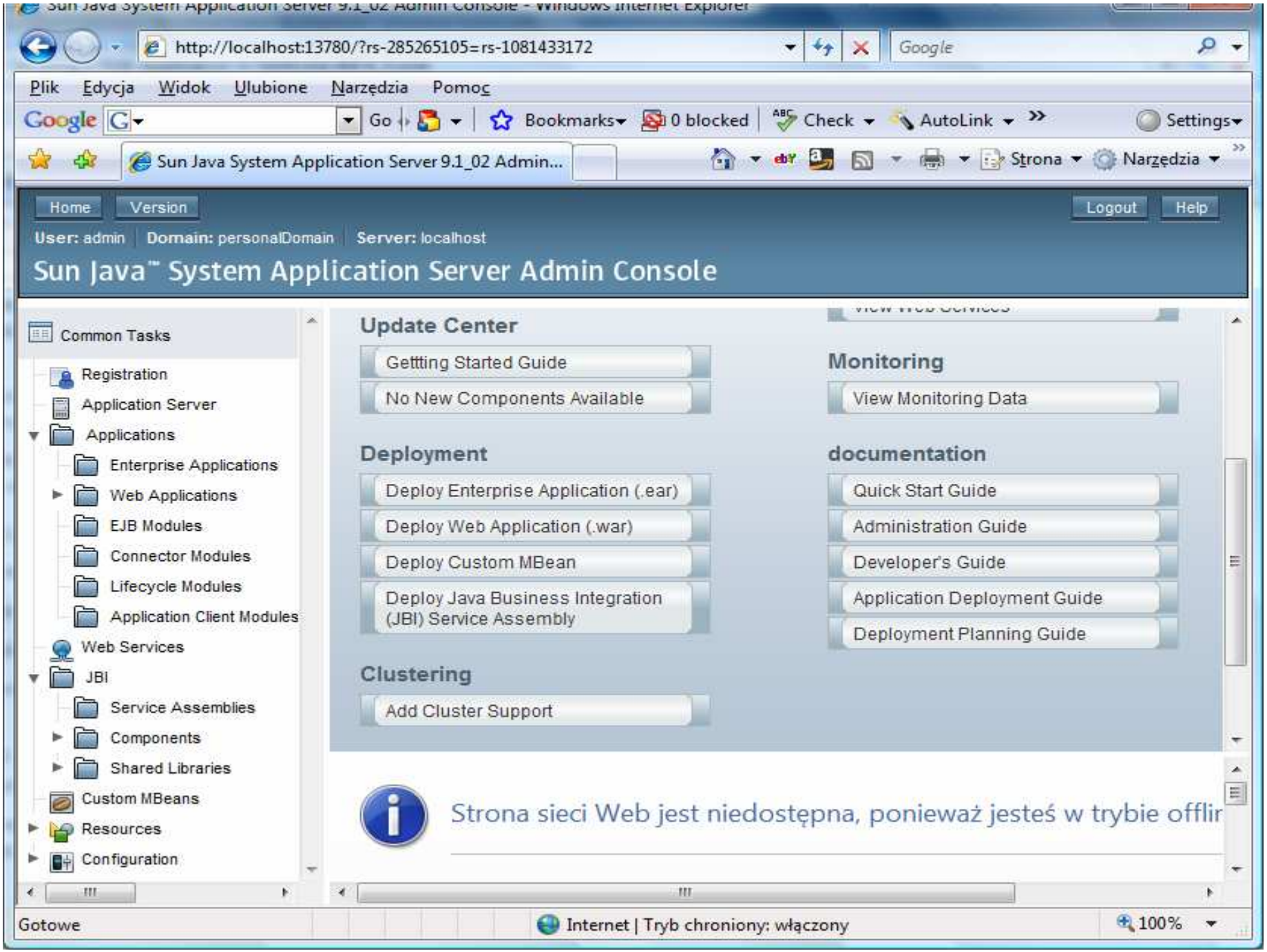
- Kliknij na przycisk **Manage Users**.
- Kliknij na przycisk **New** w celu dodania nowego użytkownika.
- Podaj poprawny dane do pól **User ID,** typu **Password** i **Group List**
  - Jeśli dodaje się użytkownika do file realm, wstawione dane służą do rozpoznania danych użytkowników aplikacji JavaEE wstawianych do formularza logowania podczas uruchamiania tej aplikacji.
  - Jeśli dodaje się użytkownika do admin-realm, wstawione poprawne dane do pól **User ID,** typu **Password** służą do rozpoznania danych serwera aplikacji JavaEE, natomiast należy wstawić **asadmin** w polu **Group List**
- Kliknij na przycisk **OK** w celu dodania nowego użytkownika.
- Kliknij na przycisk **Logout** w celu zakończenia zadania.

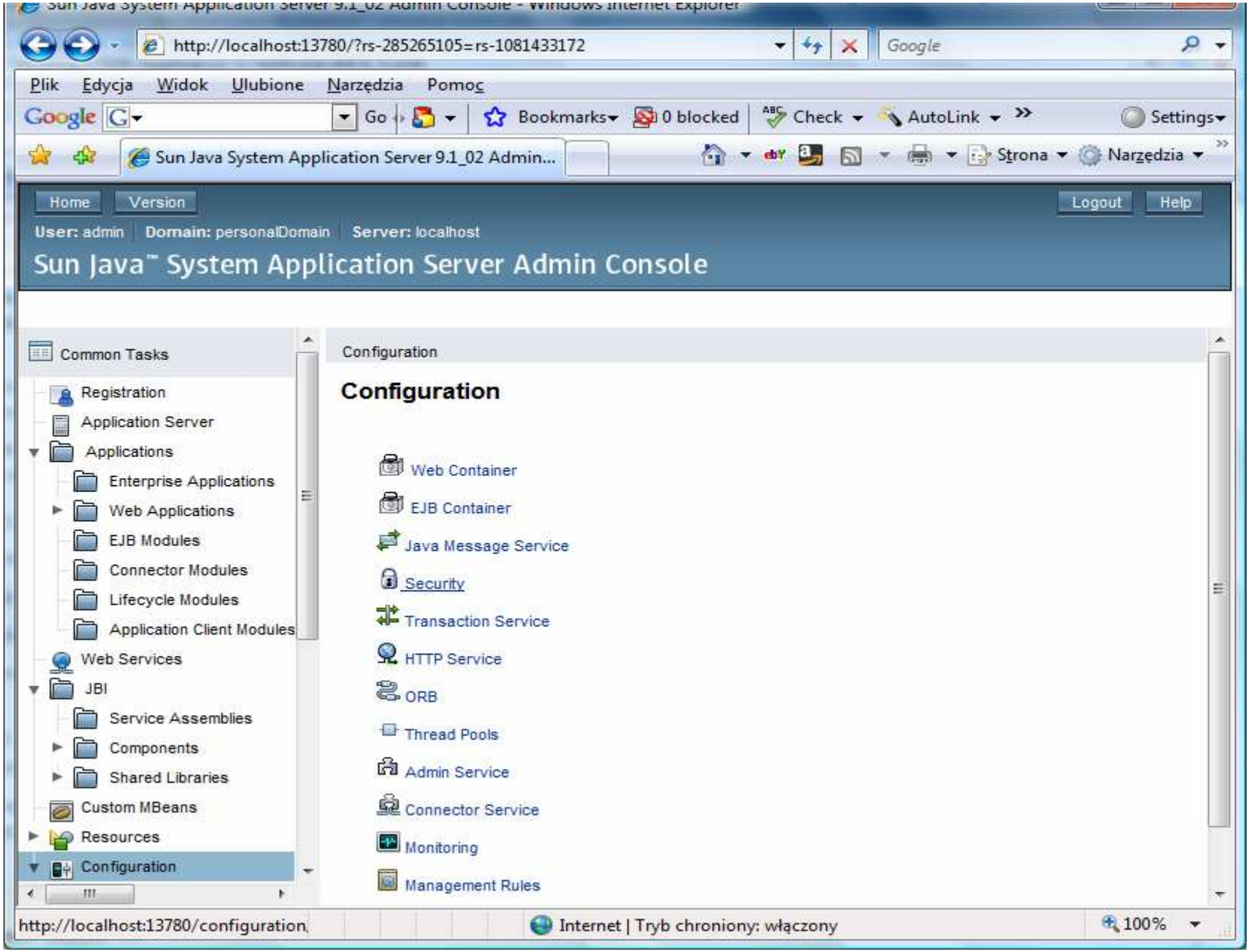
2) ***Dodawanie użytkowników do Certificate Realm

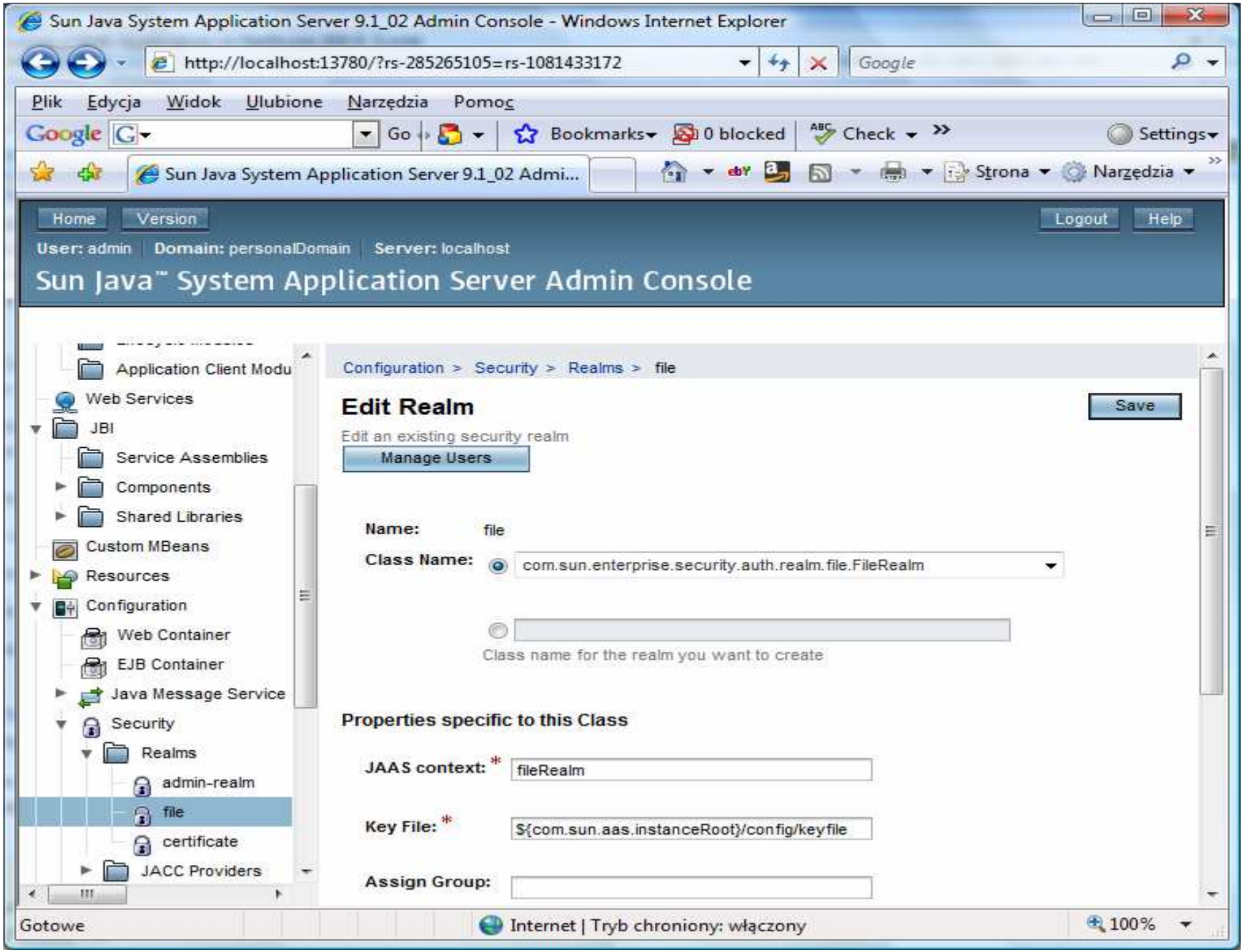
- W bazie **certificate realm**, dane identyfikujące użytkownika są używane do weryfikowania danych otrzymywanych z certyfikatów klientów

1) Dodanie użytkowników do Serwera aplikacji JavaEE

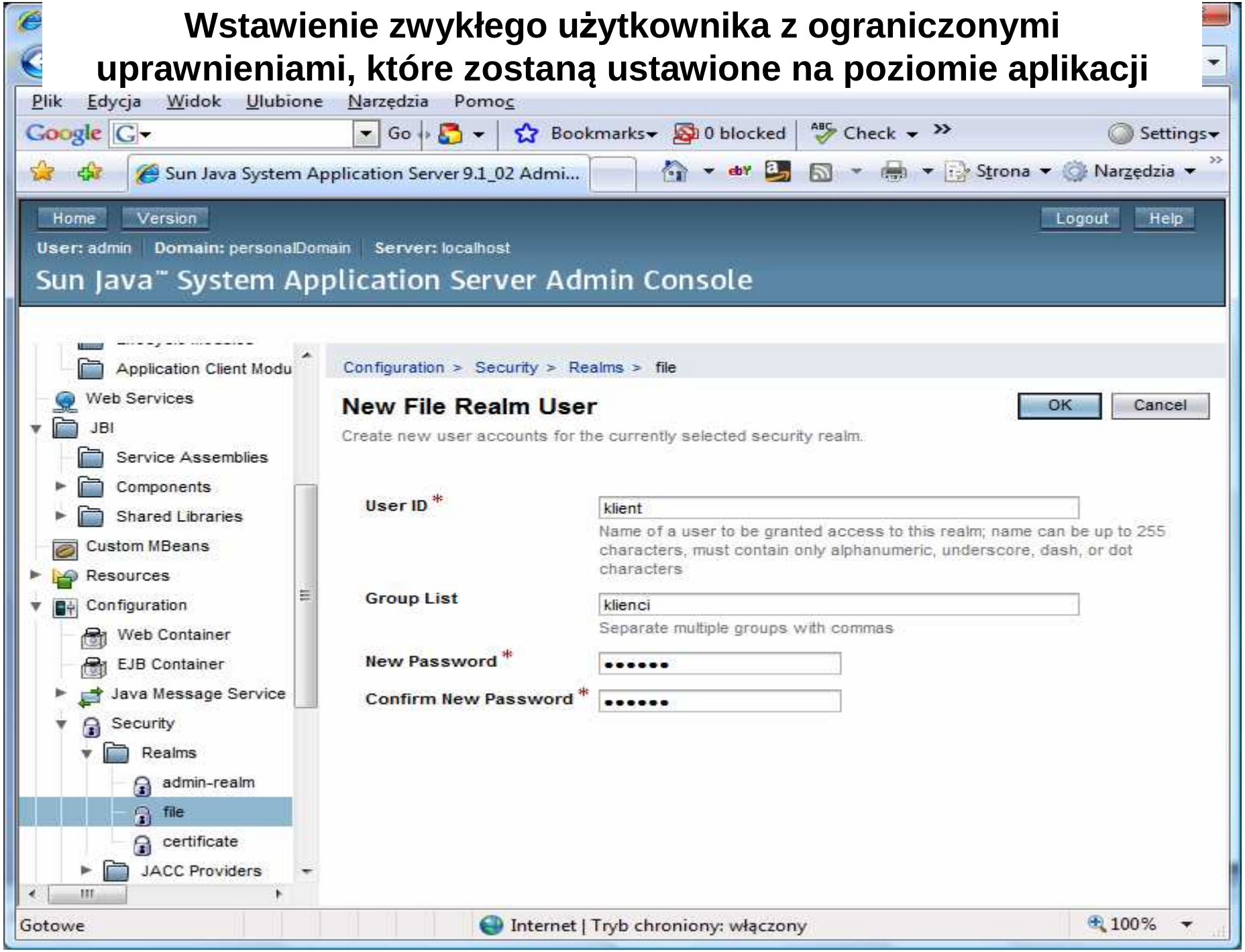


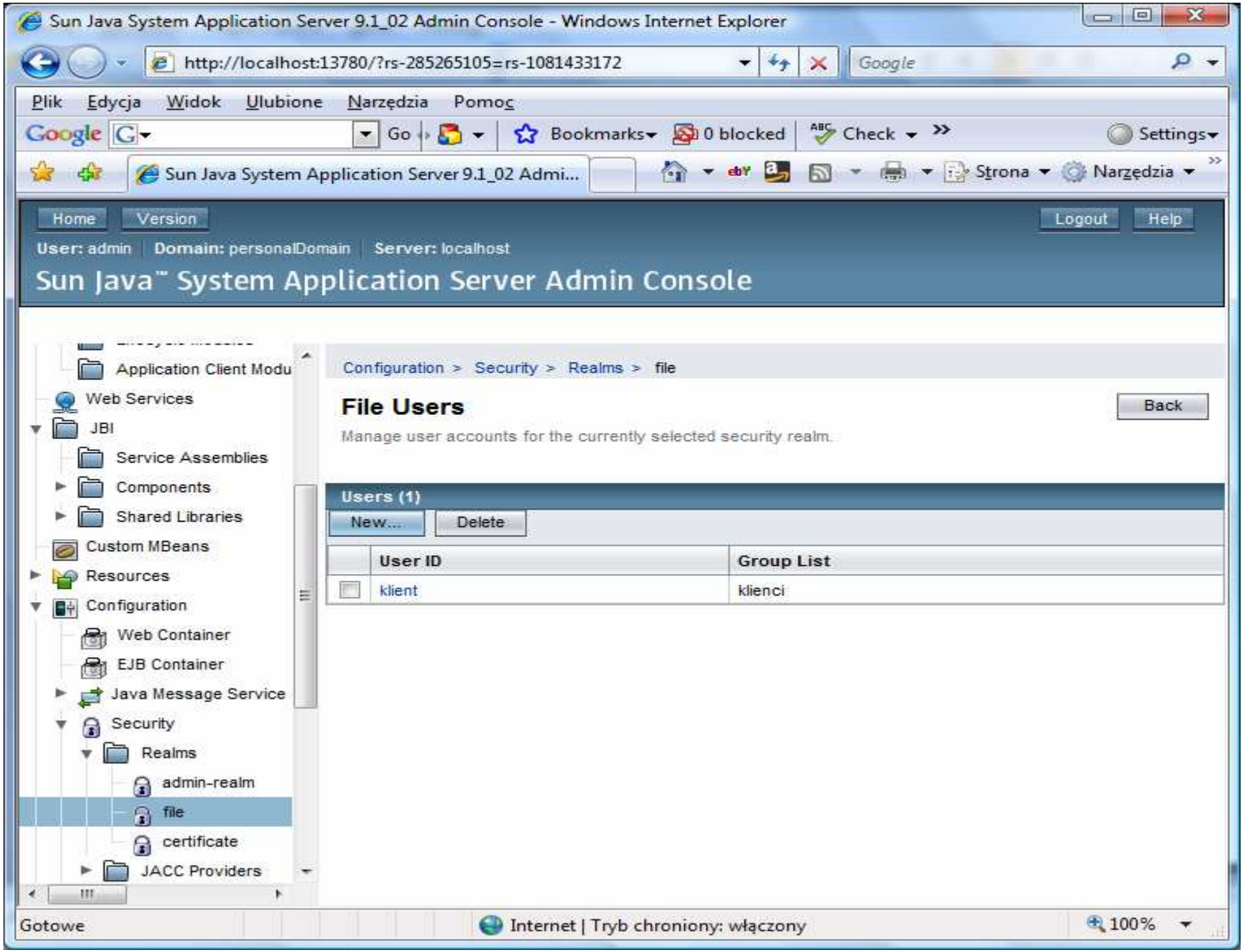

http://localhost:13780/?rs-285265105=rs-1081433172
Google
Plik Edycja Widok Ulubione Narzędzia Pomoc
Google Go Bookmarks 0 blocked Check AutoLink Settings
Sun Java System Application Server 9.1_02 Admin...
Strona Narzędzia
Home Version Logout Help
User: admin Domain: personalDomain Server: localhost
Sun Java™ System Application Server Admin Console
Common Tasks
Registration
Application Server
Applications
Enterprise Applications
Web Applications
EJB Modules
Connector Modules
Lifecycle Modules
Application Client Modules
Web Services
JBI
Service Assemblies
Components
Shared Libraries
Custom MBeans
Resources
Configuration
Update Center
Gettting Started Guide
No New Components Available
Deployment
Deploy Enterprise Application (.ear)
Deploy Web Application (.war)
Deploy Custom MBean
Deploy Java Business Integration (JBI) Service Assembly
Clustering
Add Cluster Support
Monitoring
View Monitoring Data
documentation
Quick Start Guide
Administration Guide
Developer's Guide
Application Deployment Guide
Deployment Planning Guide
Strona sieci Web jest niedostępna, ponieważ jesteś w trybie offlir
Gotowe
Internet | Tryb chroniony: włączony
100%


Sun Java System Application Server 9.1_02 Admin Console - Windows Internet Explorer
http://localhost:13780/?rs-285265105=rs-1081433172
Google
Plik Edycja Widok Ulubione Narzędzia Pomoc
Google Go Bookmarks 0 blocked Check AutoLink Settings
Sun Java System Application Server 9.1_02 Admin...
Strona Narzędzia
Home Version Logout Help
User: admin Domain: personalDomain Server: localhost
Sun Java™ System Application Server Admin Console
Common Tasks
Registration
Application Server
Applications
Enterprise Applications
Web Applications
EJB Modules
Connector Modules
Lifecycle Modules
Application Client Modules
Web Services
JBI
Service Assemblies
Components
Shared Libraries
Custom MBeans
Resources
Configuration
Configuration
Configuration
Web Container
EJB Container
Java Message Service
Security
Transaction Service
HTTP Service
ORB
Thread Pools
Admin Service
Connector Service
Monitoring
Management Rules
http://localhost:13780/configuration
Internet | Tryb chroniony: włączony
100%

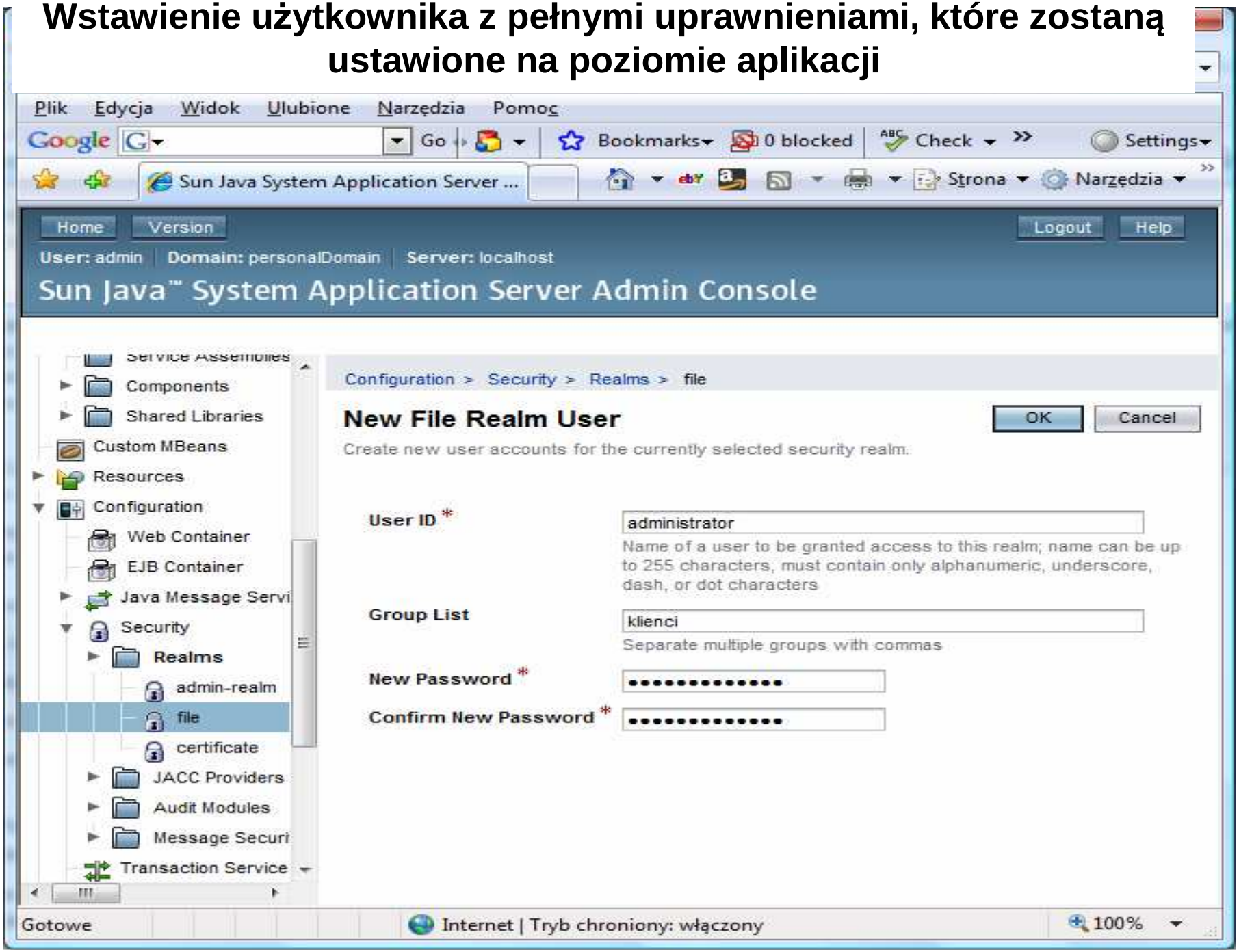

Sun Java System Application Server 9.1_02 Admin Console - Windows Internet Explorer
http://localhost:13780/?rs-285265105=rs-1081433172
Google
Plik Edycja Widok Ulubione Narzędzia Pomoc
Bookmarks 0 blocked Check Settings
Sun Java System Application Server 9.1_02 Admi...
Strona Narzędzia
Home Version Logout Help
User: admin | Domain: personalDomain | Server: localhost
Sun Java™ System Application Server Admin Console
Application Client Modu
Web Services
JBI
Service Assemblies
Components
Shared Libraries
Custom MBeans
Resources
Configuration
Web Container
EJB Container
Java Message Service
Security
Realms
admin-realm
file
certificate
JACC Providers
Configuration > Security > Realms > file
Edit Realm
Save
Edit an existing security realm
Manage Users
Name: file
Class Name: com.sun.enterprise.security.auth.realm.file.FileRealm
Class name for the realm you want to create
Properties specific to this Class
JAAS context: * fileRealm
Key File: * ${com.sun.aas.instanceRoot}/config/keyfile
Assign Group:
Gotowe
Internet | Tryb chroniony: włączony
100%

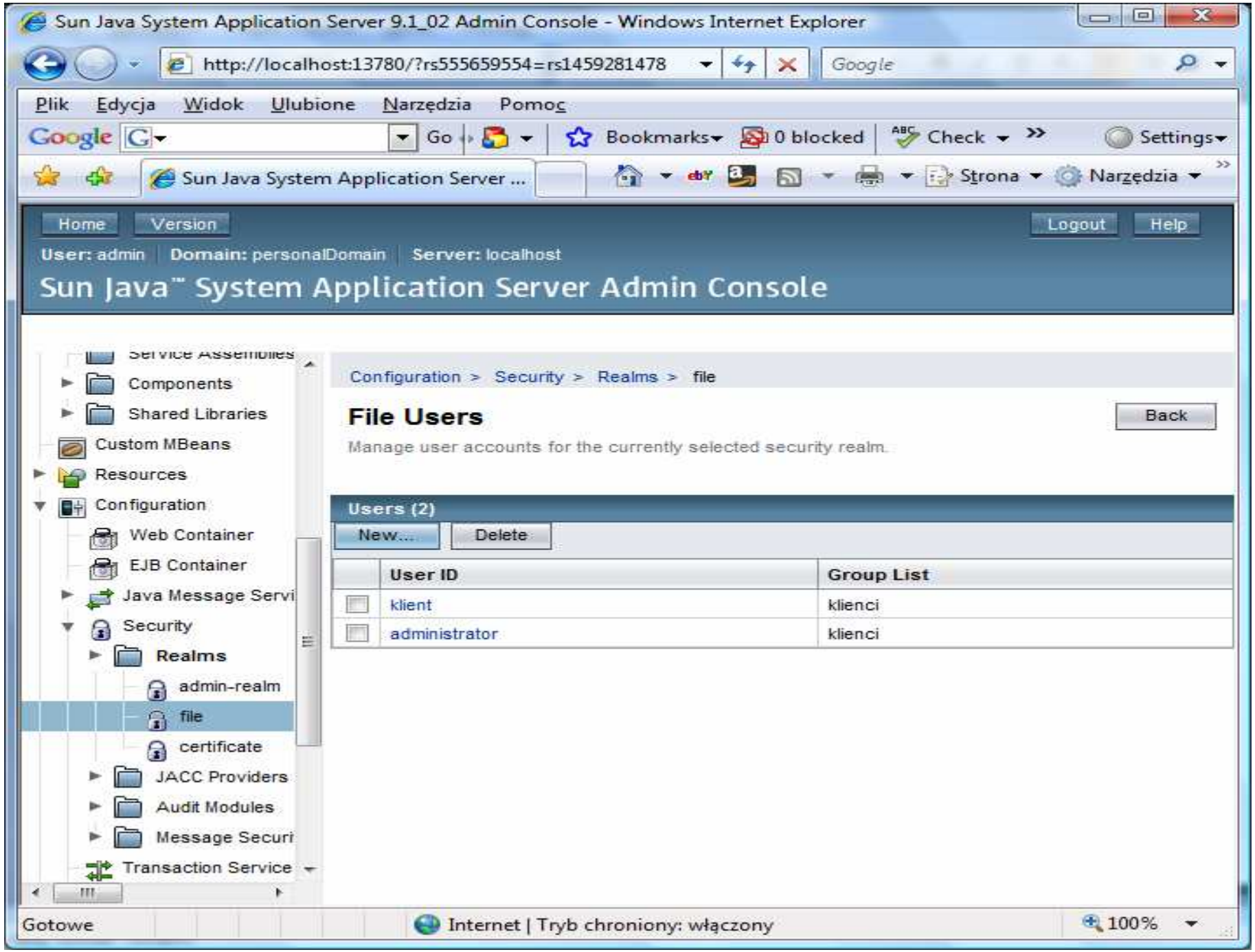
Wstawienie zwykłego użytkownika z ograniczonymi uprawnieniami, które zostaną ustawione na poziomie aplikacji



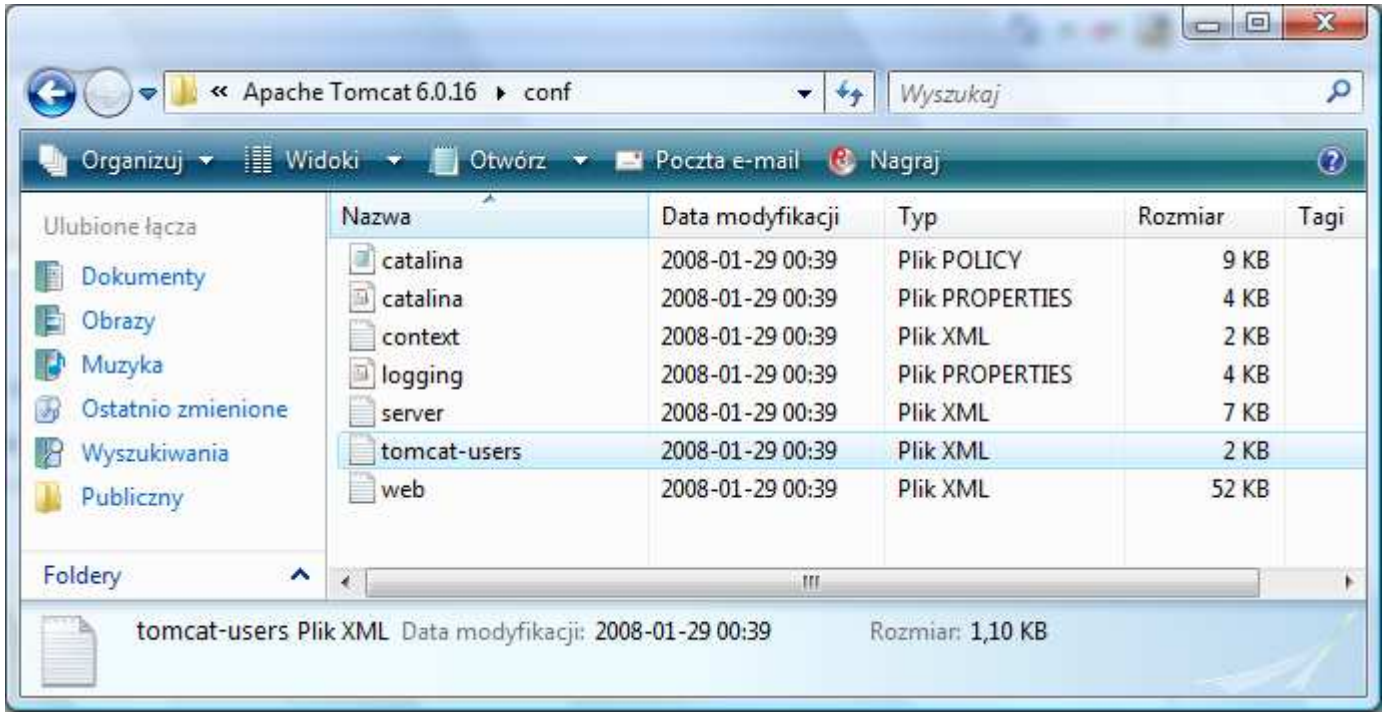

Sun Java System Application Server 9.1_02 Admin Console - Windows Internet Explorer
http://localhost:13780/?rs-285265105=rs-1081433172
Google
Plik Edycja Widok Ulubione Narzędzia Pomoc
Bookmarks 0 blocked Check Settings
Sun Java System Application Server 9.1_02 Admi...
Strona Narzędzia
Home Version Logout Help
User: admin Domain: personalDomain Server: localhost
Sun Java™ System Application Server Admin Console
Application Client Modu
Web Services
JBI
Service Assemblies
Components
Shared Libraries
Custom MBeans
Resources
Configuration
Web Container
EJB Container
Java Message Service
Security
Realms
admin-realm
file
certificate
JACC Providers
Configuration > Security > Realms > file
File Users
Back
Manage user accounts for the currently selected security realm.
Users (1)
New... Delete
User ID
Group List
klient
klienci
Gotowe
Internet | Tryb chroniony: włączony
100%

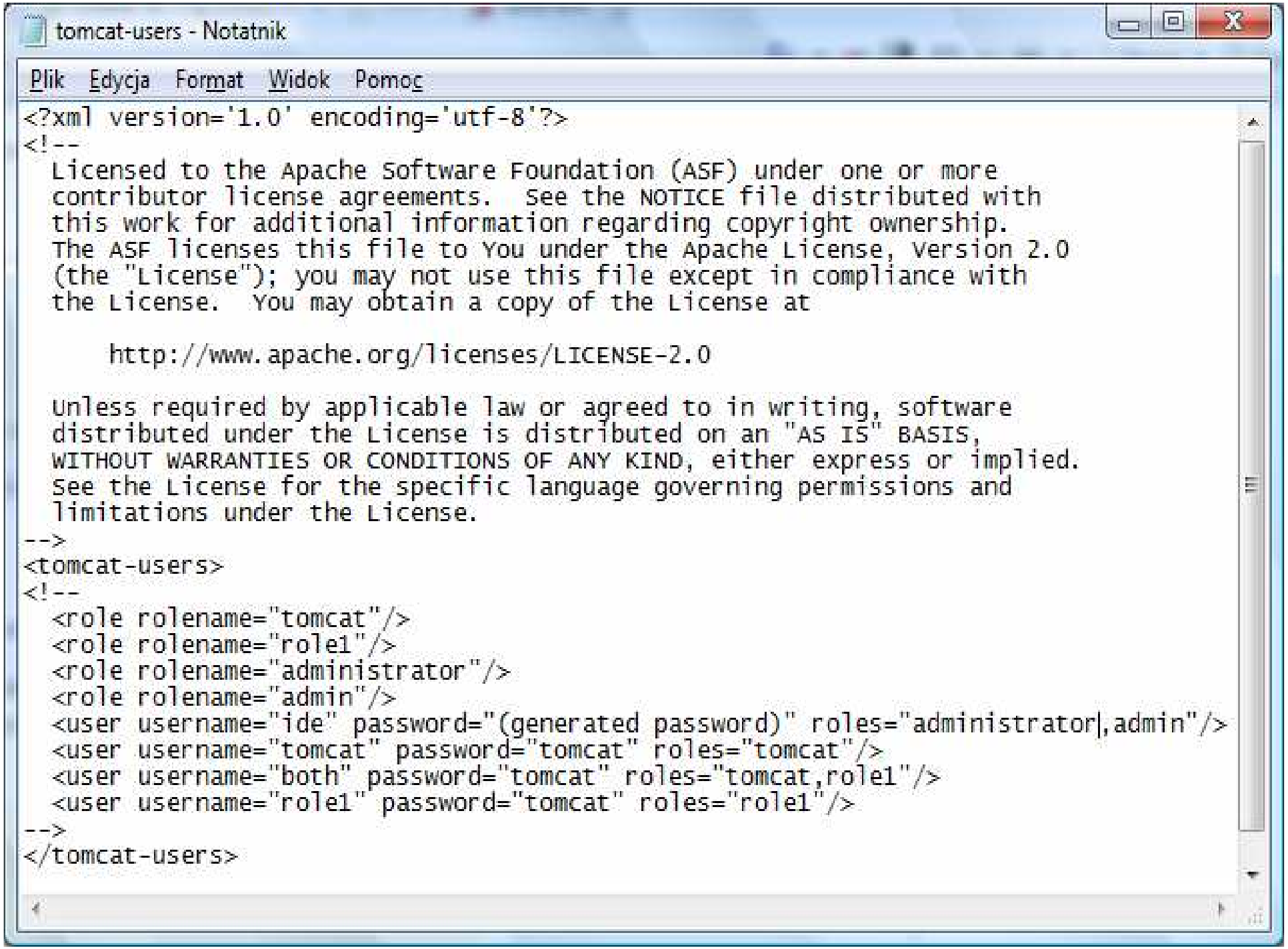
Wstawienie użytkownika z pełnymi uprawnieniami, które zostaną ustawione na poziomie aplikacji



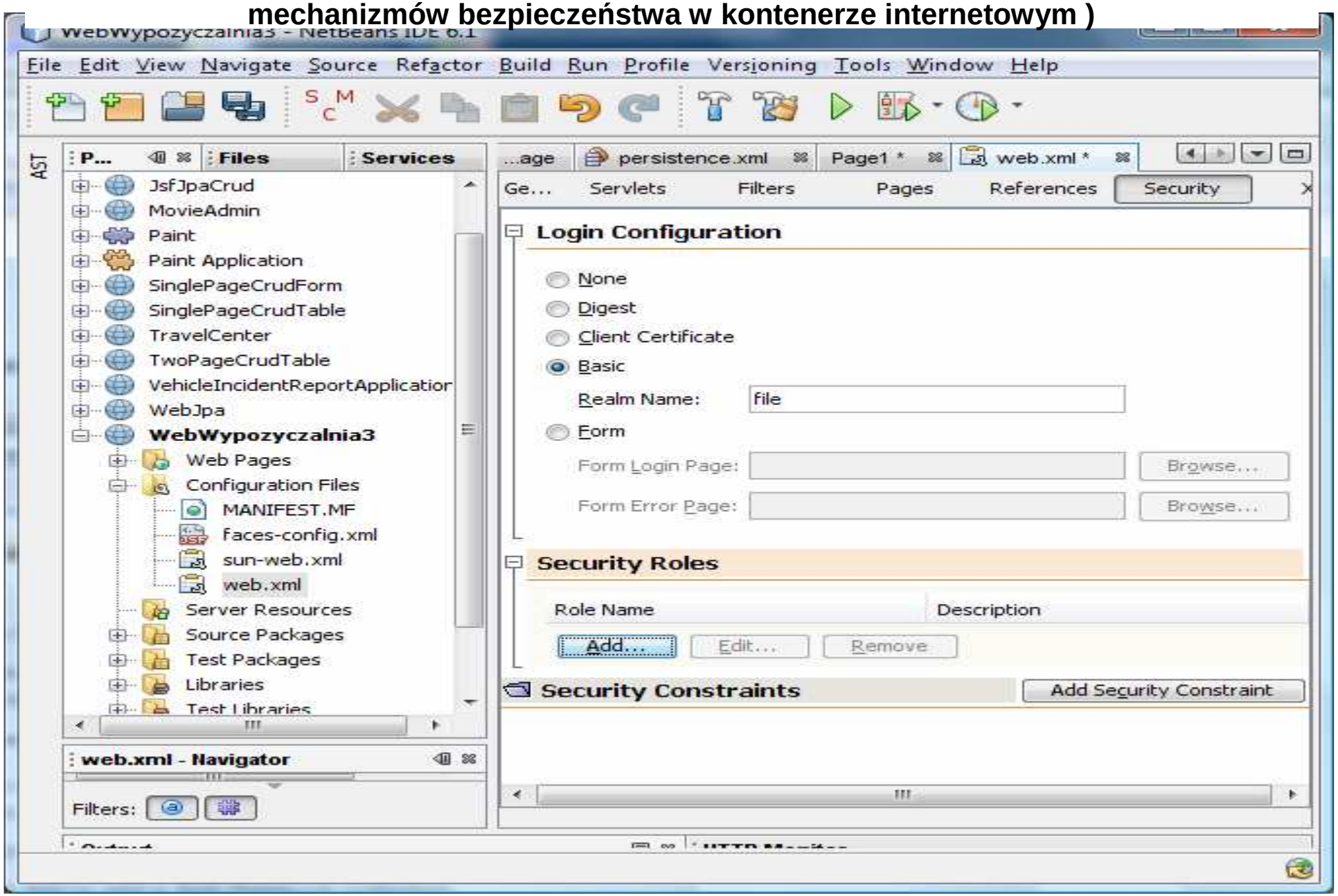

Sun Java System Application Server 9.1_02 Admin Console - Windows Internet Explorer
http://localhost:13780/?rs555659554=rs1459281478
Google
Plik Edycja Widok Ulubione Narzędzia Pomoc
Bookmarks 0 blocked Check Settings
Sun Java System Application Server ...
Strona Narzędzia
Home Version Logout Help
User: admin Domain: personalDomain Server: localhost
Sun Java™ System Application Server Admin Console
Components
Shared Libraries
Custom MBeans
Resources
Configuration
Web Container
EJB Container
Java Message Servi
Security
Realms
admin-realm
file
certificate
JACC Providers
Audit Modules
Message Securi
Transaction Service
Configuration > Security > Realms > file
File Users
Back
Manage user accounts for the currently selected security realm.
Users (2)
New... Delete
User ID
Group List
klient
klienci
administrator
klienci
Gotowe
Internet | Tryb chroniony: włączony
100%

2. Definiowanie ról w serwerze *Tomcat Web Server*

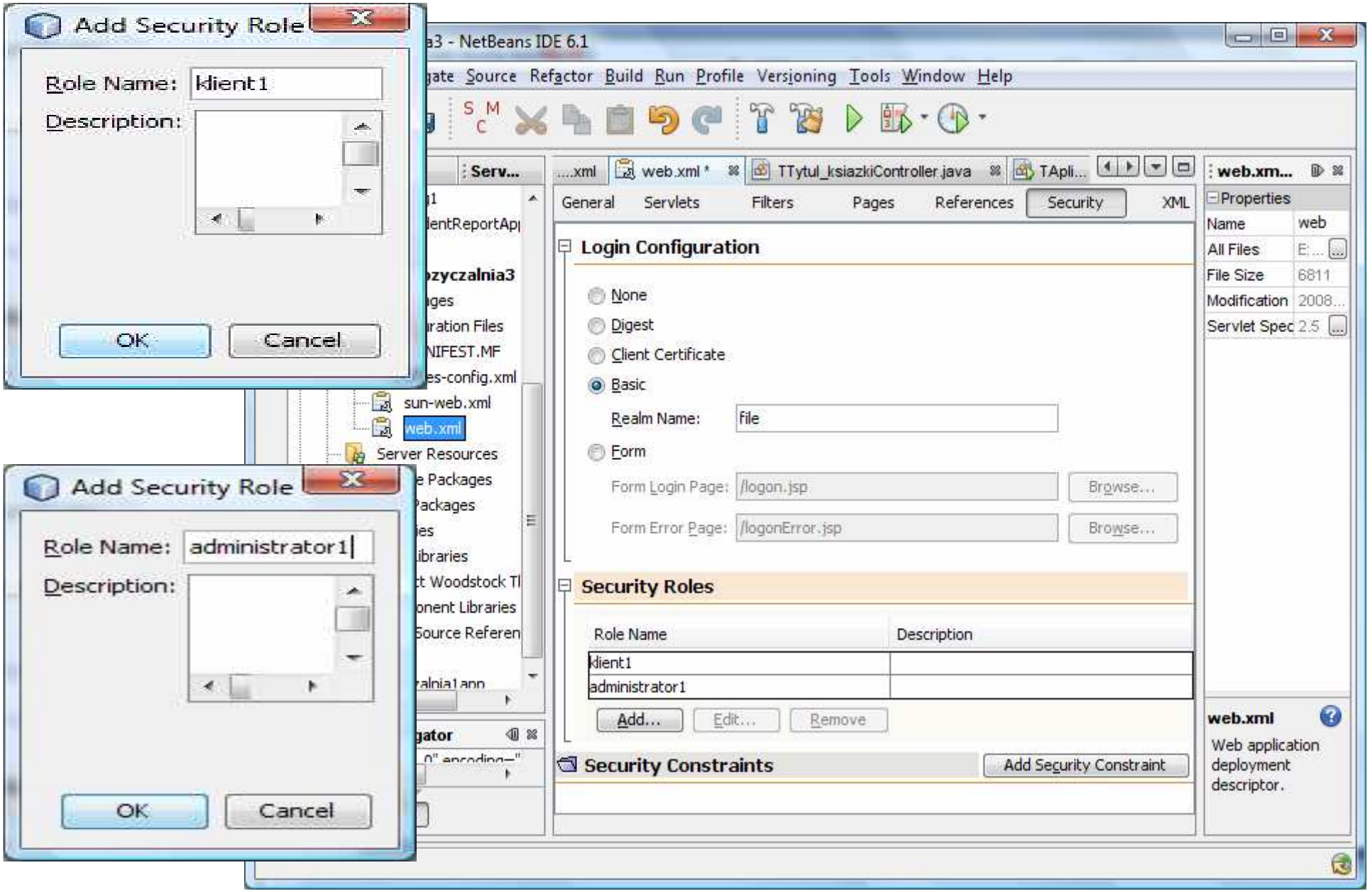



tomcat-users - Notatnik
Plik Edycja Format Widok Pomoc
<?xml version='1.0' encoding='utf-8'?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at
http://www.apache.org/licenses/LICENSE-2.0
Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->
<tomcat-users>
<!--
<role rolename="tomcat"/>
<role rolename="role1"/>
<role rolename="administrator"/>
<role rolename="admin"/>
<user username="ide" password="(generated password)" roles="administrator,admin"/>
<user username="tomcat" password="tomcat" roles="tomcat"/>
<user username="both" password="tomcat" roles="tomcat,role1"/>
<user username="role1" password="tomcat" roles="role1"/>
-->
</tomcat-users>

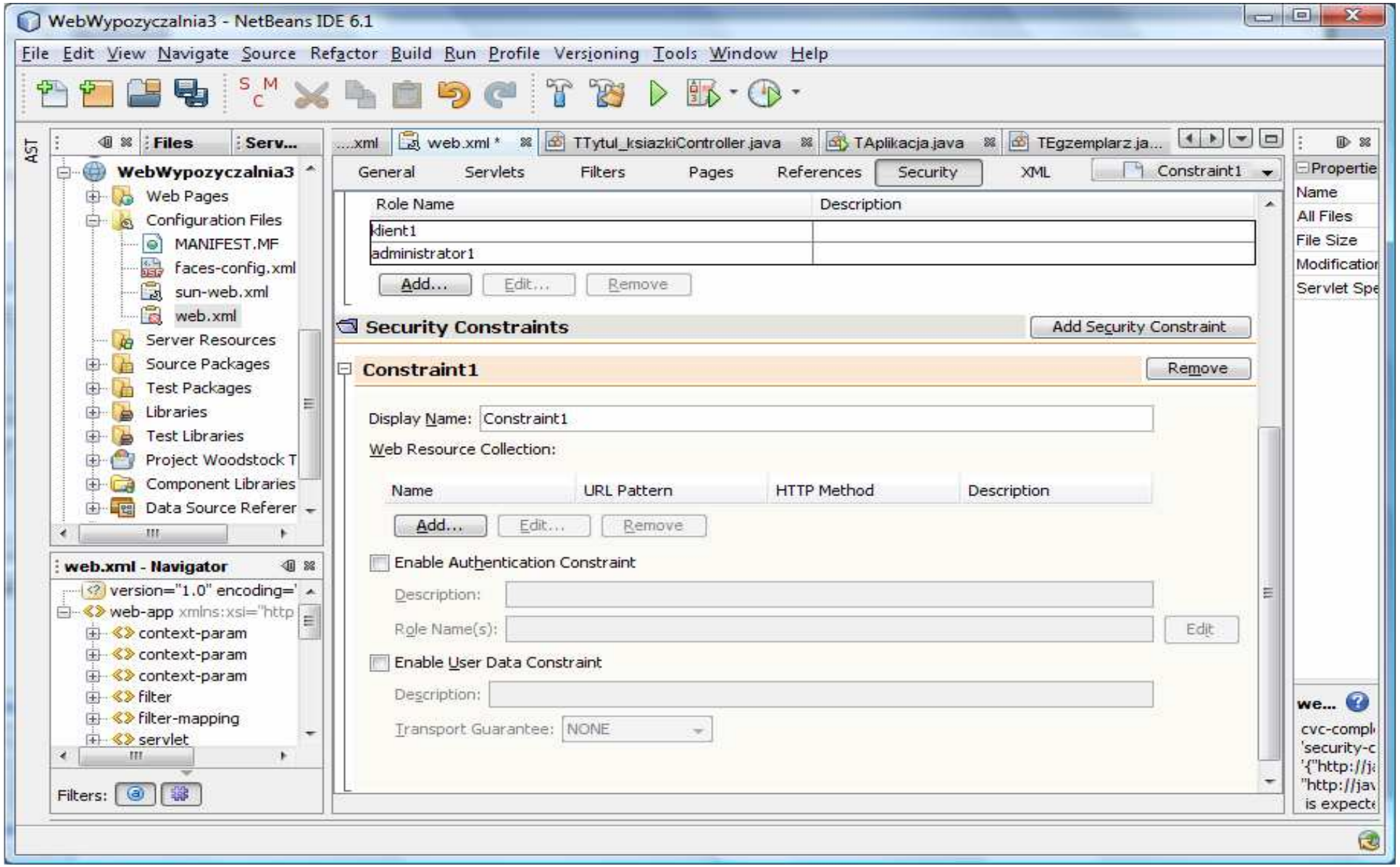
3. Konfigurowanie logowania – deskryptor aplikacji *web.xml* po wybraniu opcji *Security -> Login Configuration* (deklaratywne konfigurowanie mechanizmów bezpieczeństwa w kontenerze internetowym)



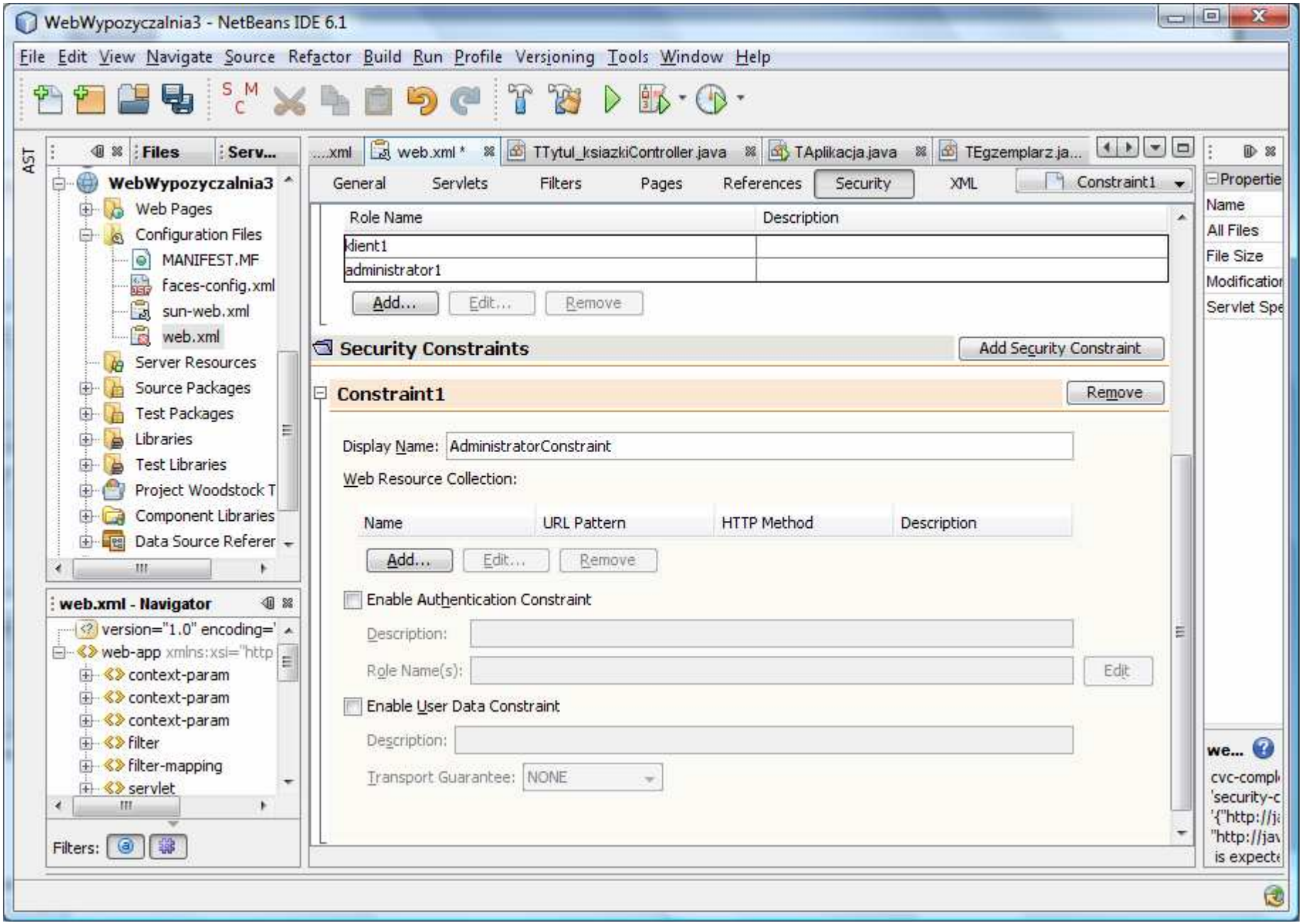
4. Wstawianie ról użytkowników do aplikacji – deskryptor aplikacji *web.xml* po wybraniu opcji *Security-> Security Roles* (deklaratywne konfigurowanie mechanizmów bezpieczeństwa w kontenerze internetowym)



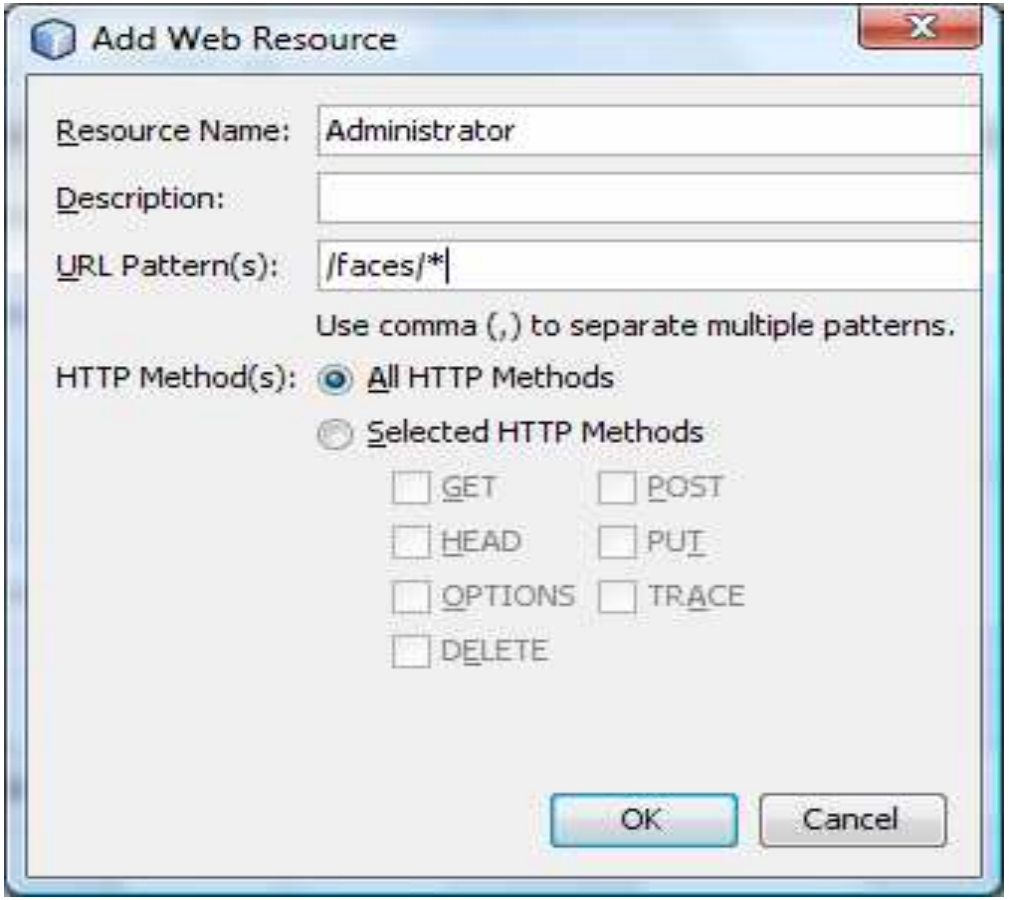
5. Tworzenie i konfiguracja ograniczeń bezpieczeństwa dla typu użytkownika administrator z największymi ograniczeniami – deskryptor aplikacji *web.xml* po wybraniu opcji *Security->Security Constraints* (deklaratywne konfigurowanie mechanizmów bezpieczeństwa w kontenerze internetowym)



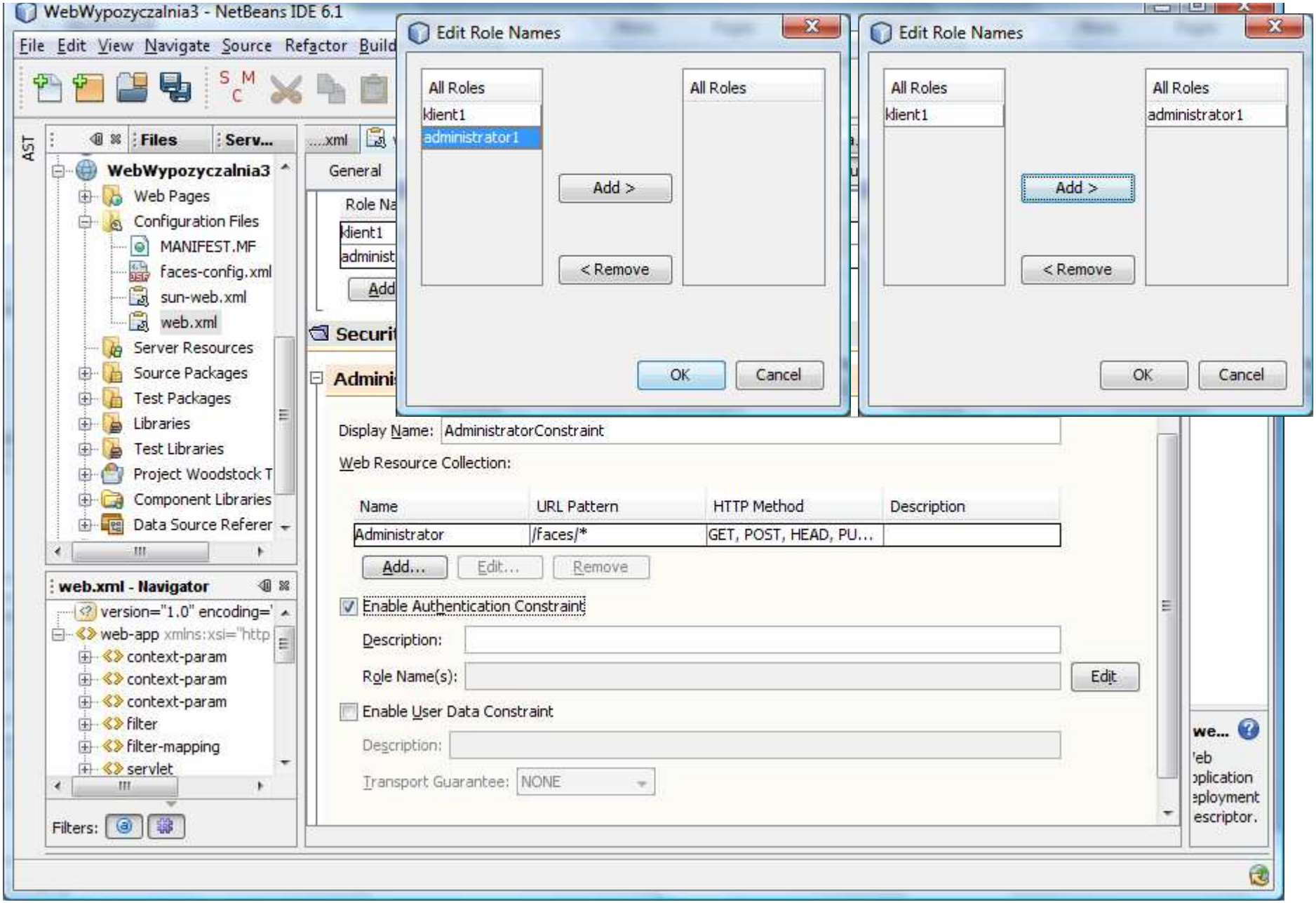
5.1. Podanie nazwy *AdministratorConstraint* ograniczeń w *Display name*



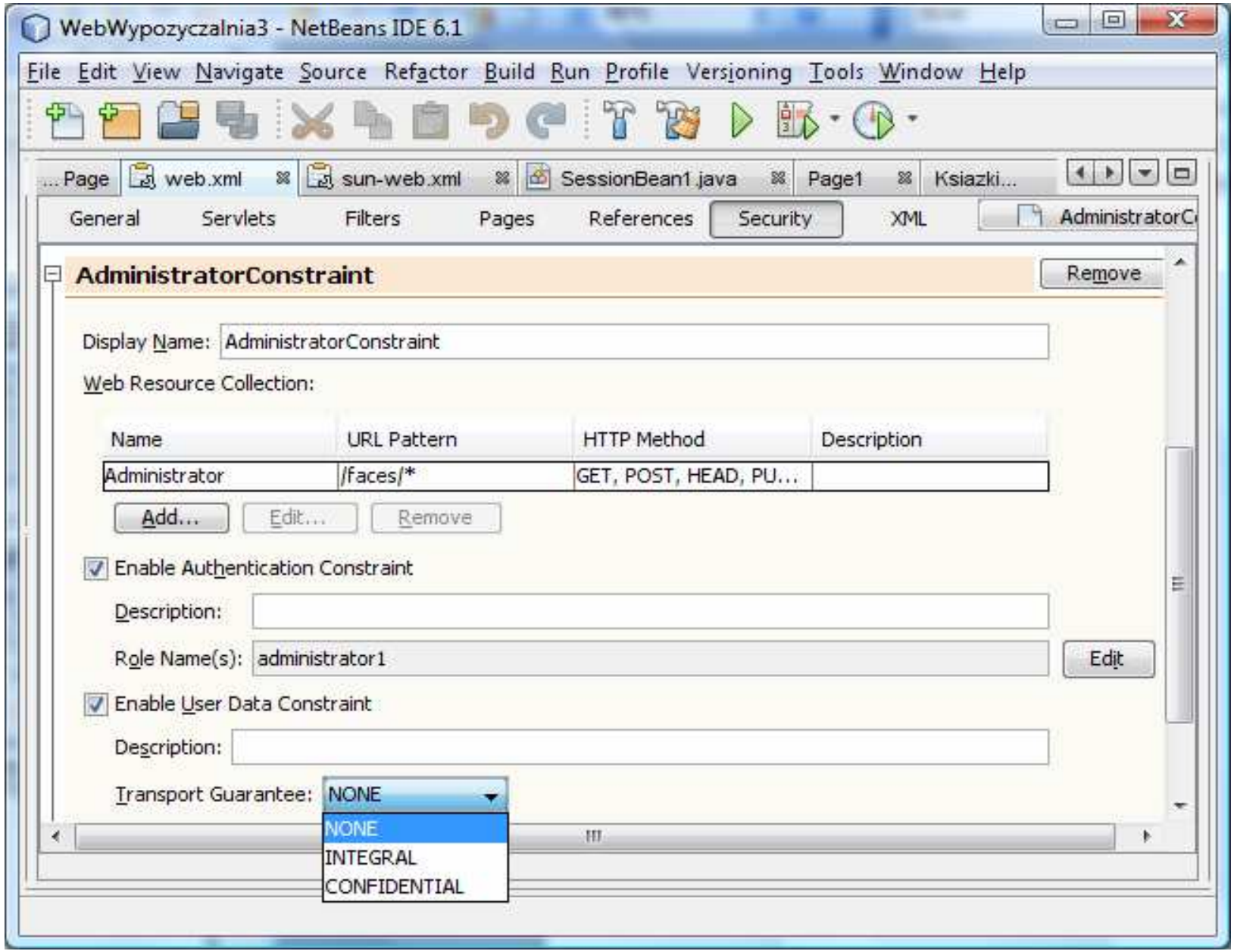
5.2. Dodanie kolekcji autoryzowanych adresów URL za pomocą opcji *Web Resources Collection -> Add* – ustawiono dostęp do wszystkich stron o wzorcu adresu *URL /faces/**



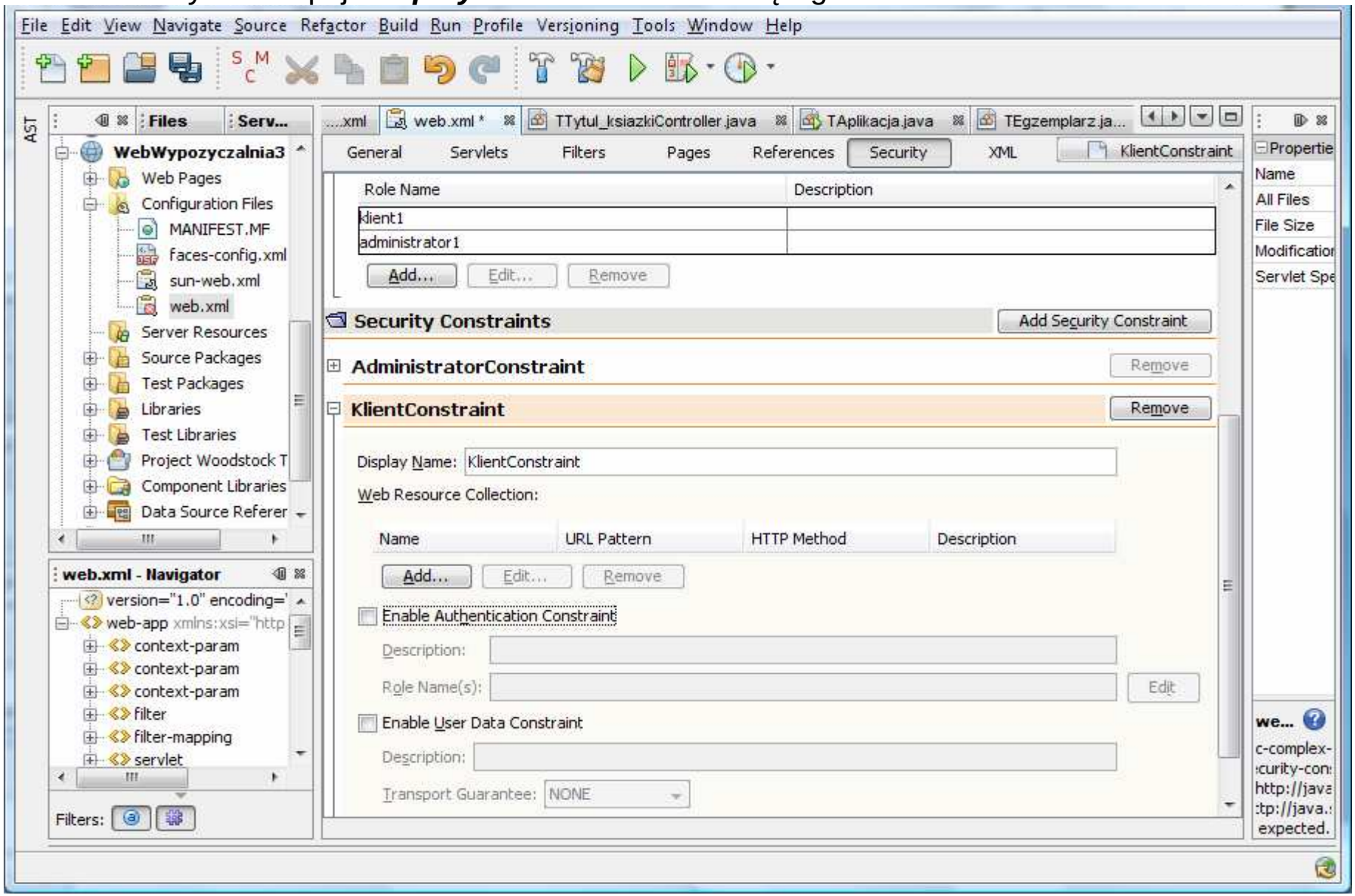
5.3. Przypisanie roli administrator1 do ustawianych ograniczeń *AdministratorConstraint* za pomocą opcji ***Enable Authentication Constraint*** i wyborze **Edit**



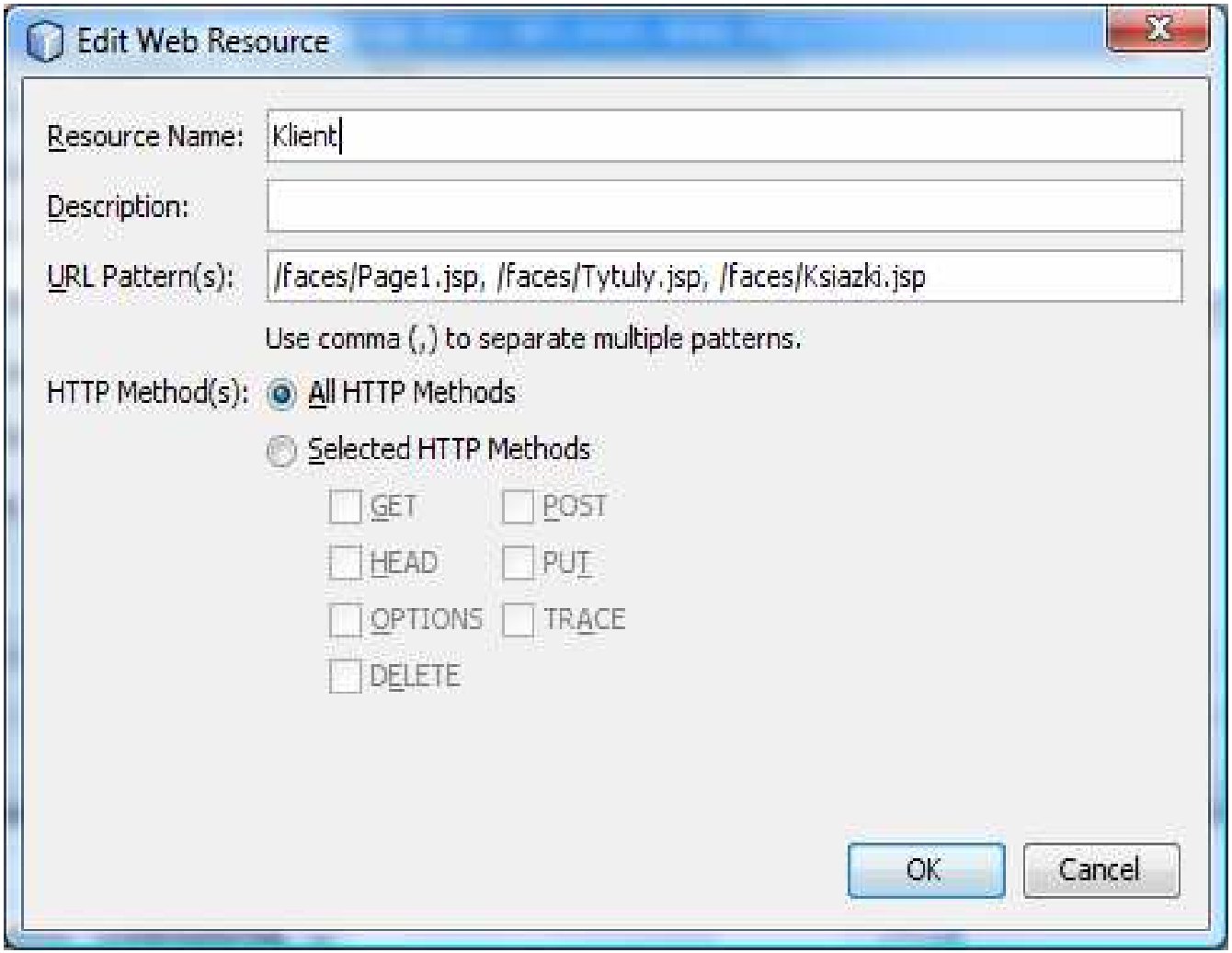
5.4. Przypisanie niezabezpieczonego protokołu transportu do ustawianych ograniczeń ***AdministratorConstraint*** za pomocą opcji ***Enable User Data Constrant*** **i** ***Transport Guarantee = NONE***

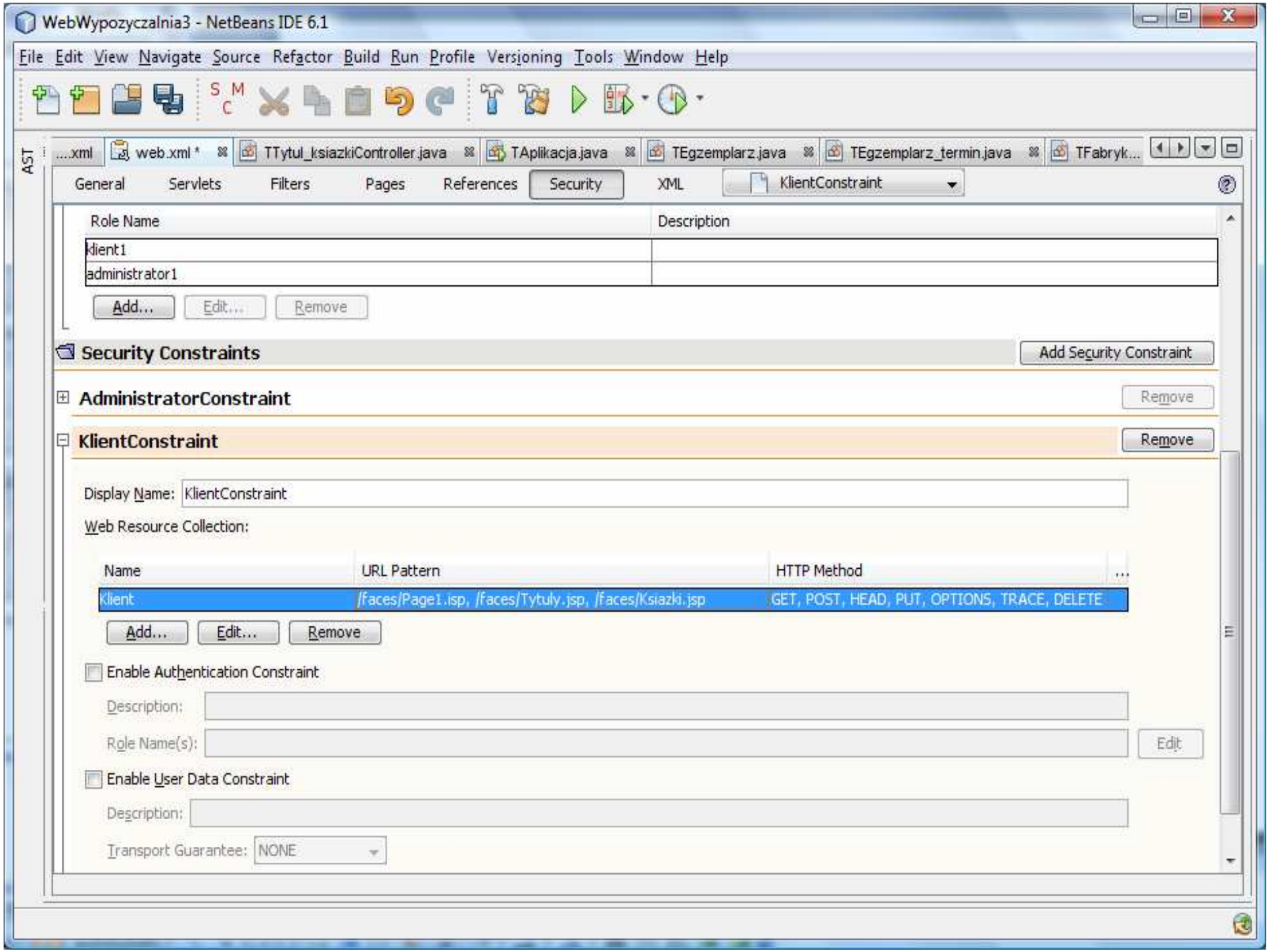


6. Tworzenie i konfiguracja ograniczeń bezpieczeństwa dla typu użytkownika z wybranymi ograniczeniami – deskryptor aplikacji ***web.xml*** po wybraniu opcji ***Security->Security Constraints*** (deklaratywne konfigurowanie mechanizmów bezpieczeństwa w kontenerze internetowym).
Po wyborze opcji ***Display Name*** nadano nazwę ograniczeniom ***KlientConstraint***

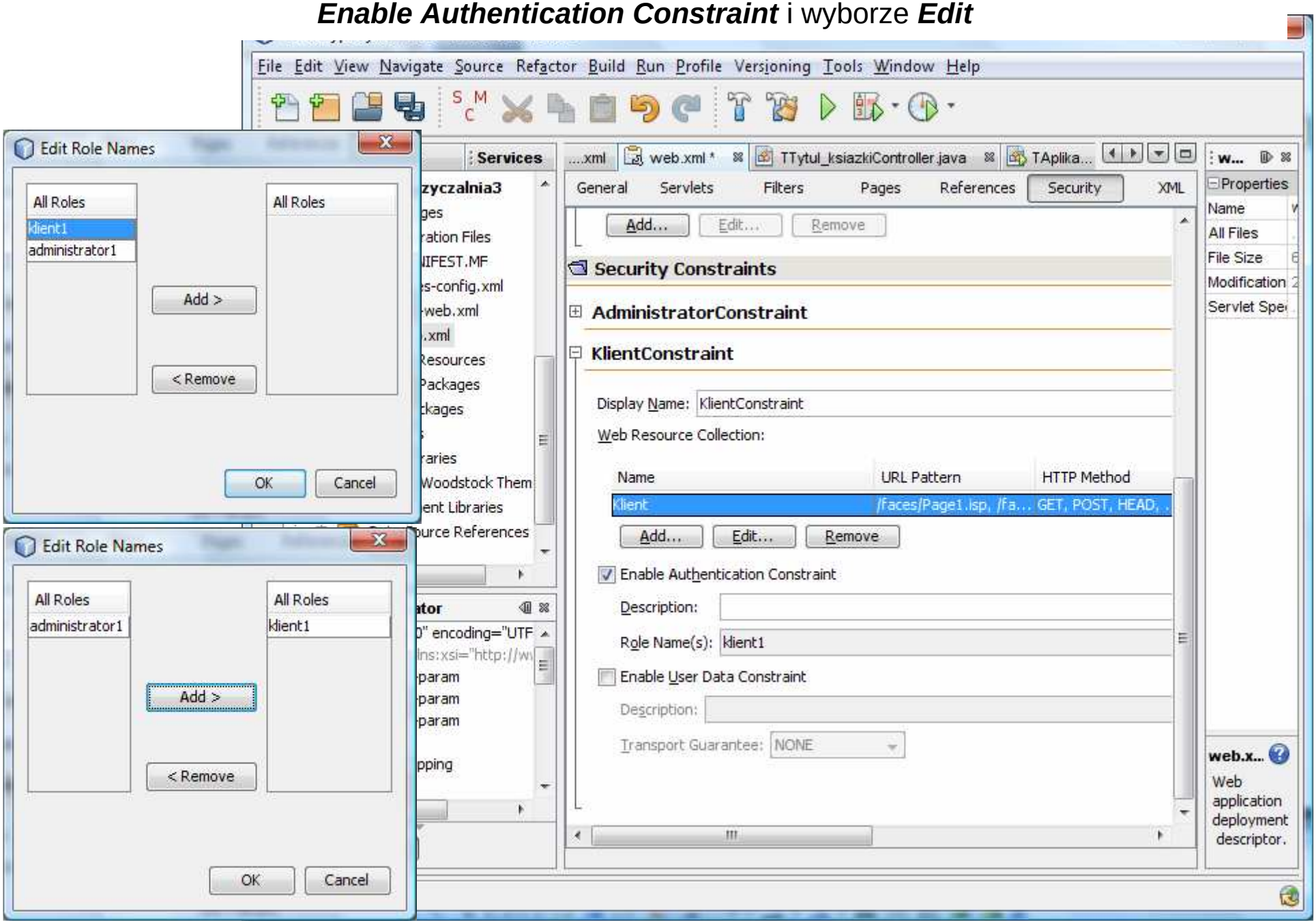


6.1. Dodanie kolekcji autoryzowanych wybranych wzorców adresów URL za pomocą opcji ***Web Resources Collection -> Add***

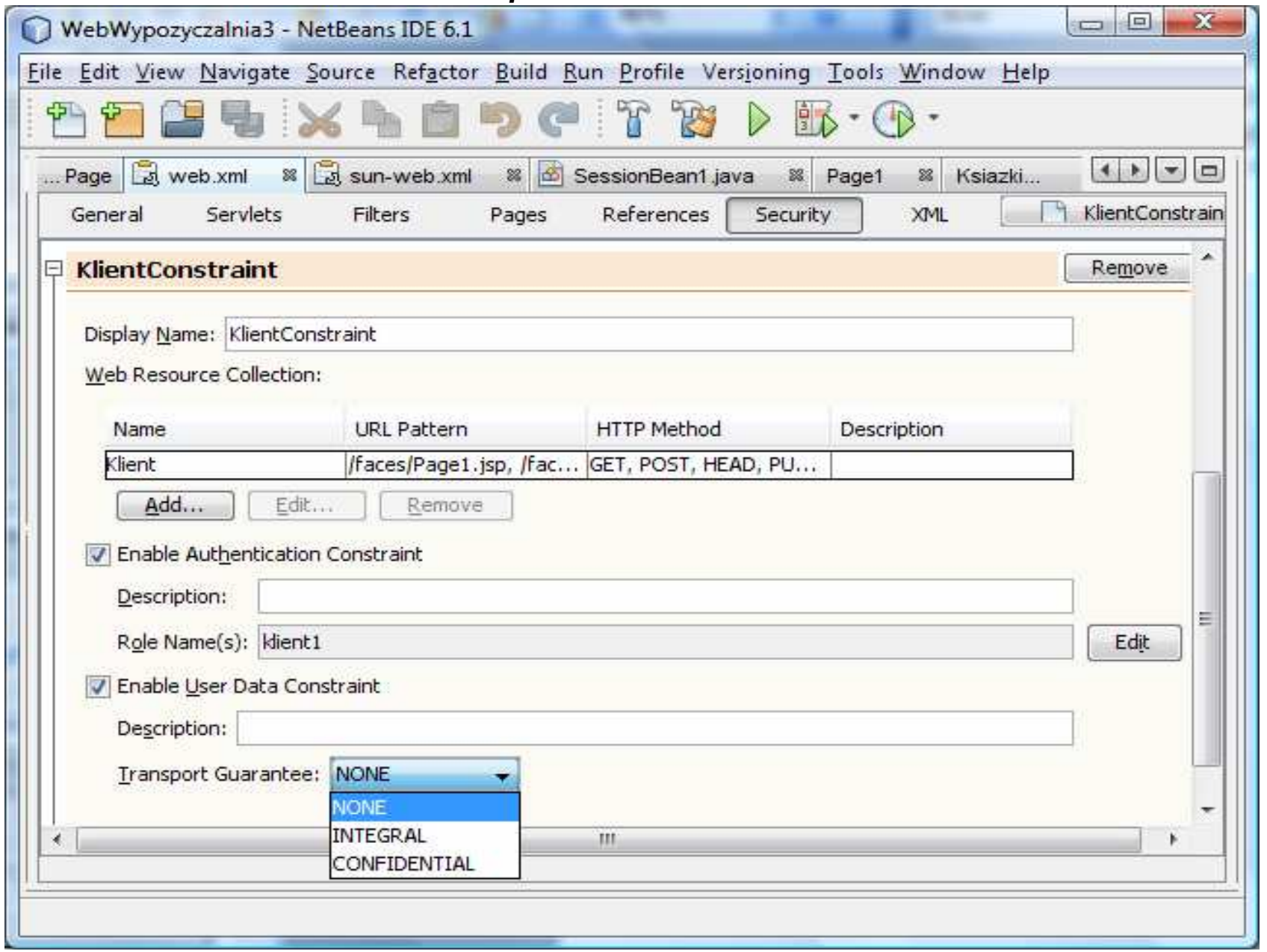



WebWypozyczalnia3 - NetBeans IDE 6.1
File Edit View Navigate Source Refactor Build Run Profile Versioning Tools Window Help
AST
....xml
web.xml *
TTytul_ksiazkiController.java
TAplikacja.java
TEgzemplarz.java
TEgzemplarz_termin.java
TFabryk...
General
Servlets
Filters
Pages
References
Security
XML
KlientConstraint
Role Name
Description
klient1
administrator1
Add...
Edit...
Remove
Security Constraints
Add Security Constraint
AdministratorConstraint
Remove
KlientConstraint
Remove
Display Name: KlientConstraint
Web Resource Collection:
Name
URL Pattern
HTTP Method
Klient
/faces/Page1.jsp, /faces/Tytuly.jsp, /faces/Ksiazki.jsp
GET, POST, HEAD, PUT, OPTIONS, TRACE, DELETE
Add...
Edit...
Remove
Enable Authentication Constraint
Description:
Role Name(s):
Edit
Enable User Data Constraint
Description:
Transport Guarantee: NONE

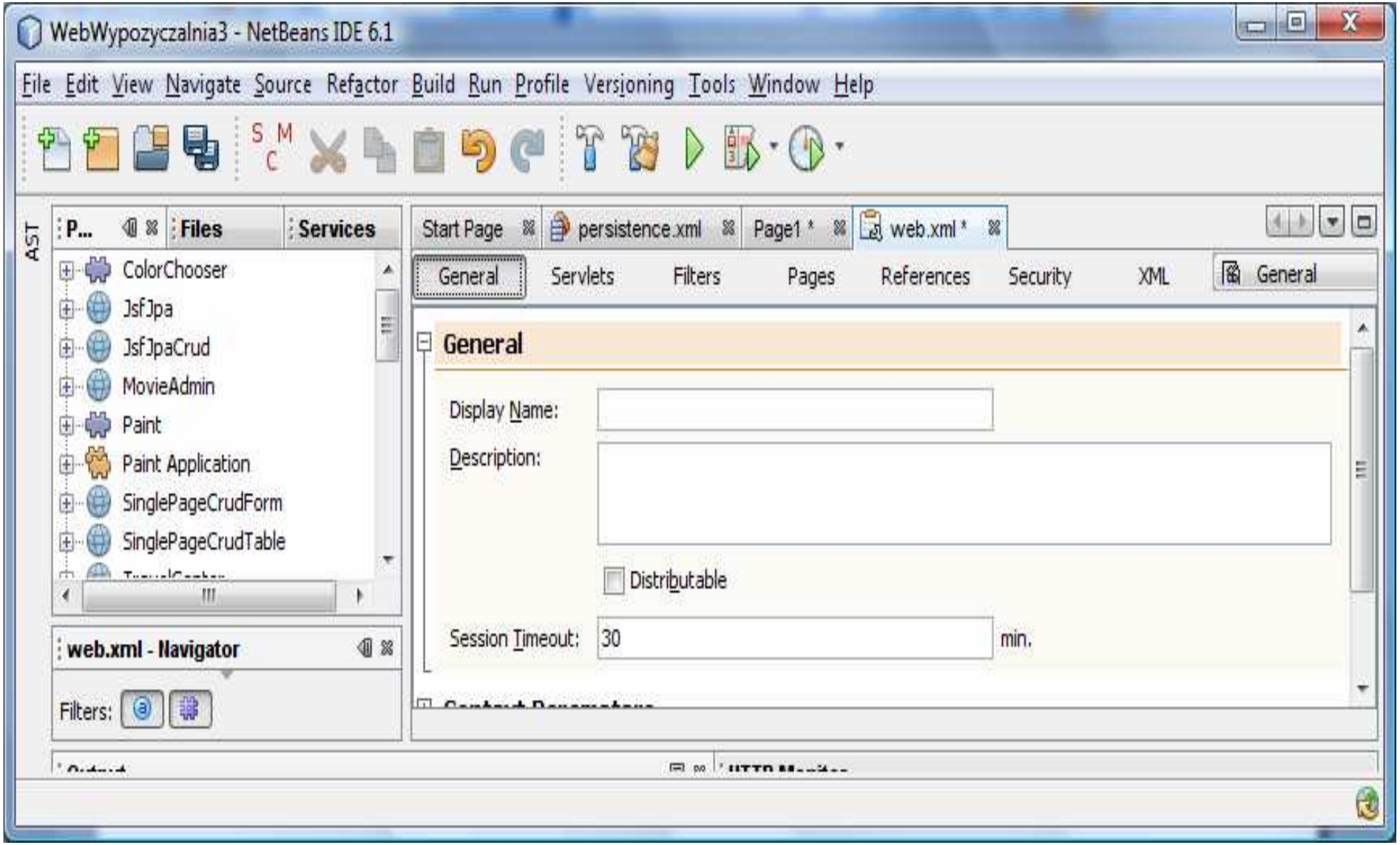
6.2. Przypisanie roli klient1 do ustawianych ograniczeń ***KlientConstraint*** za pomocą opcji ***Enable Authentication Constraint*** i wyborze ***Edit***



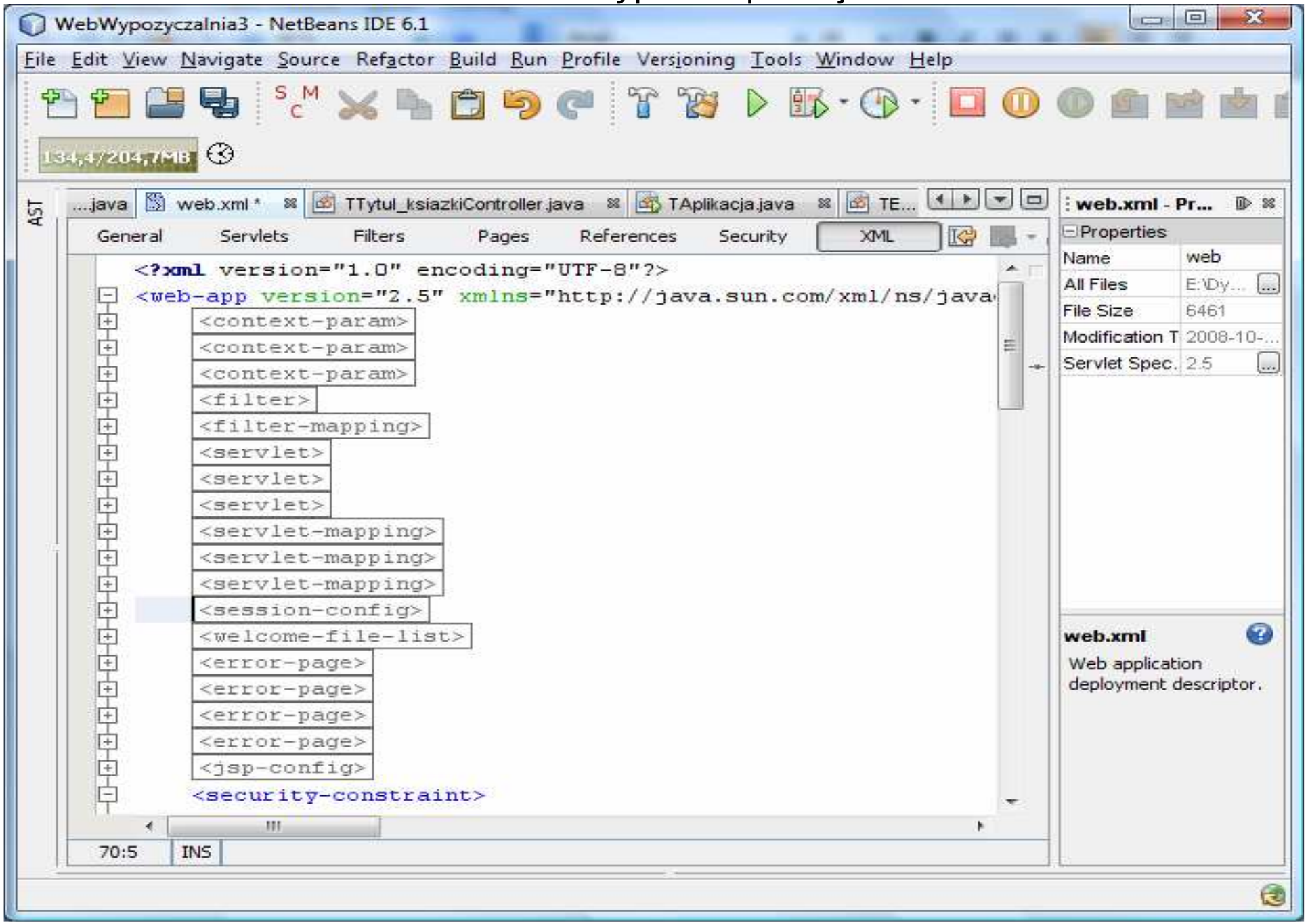
6.3. Przypisanie niezabezpieczonego protokołu transportu do ustawianych ograniczeń ***KlientConstraint*** za pomocą opcji ***Enable User Data Constrant*** **i** ***Transport Guarantee = NONE***

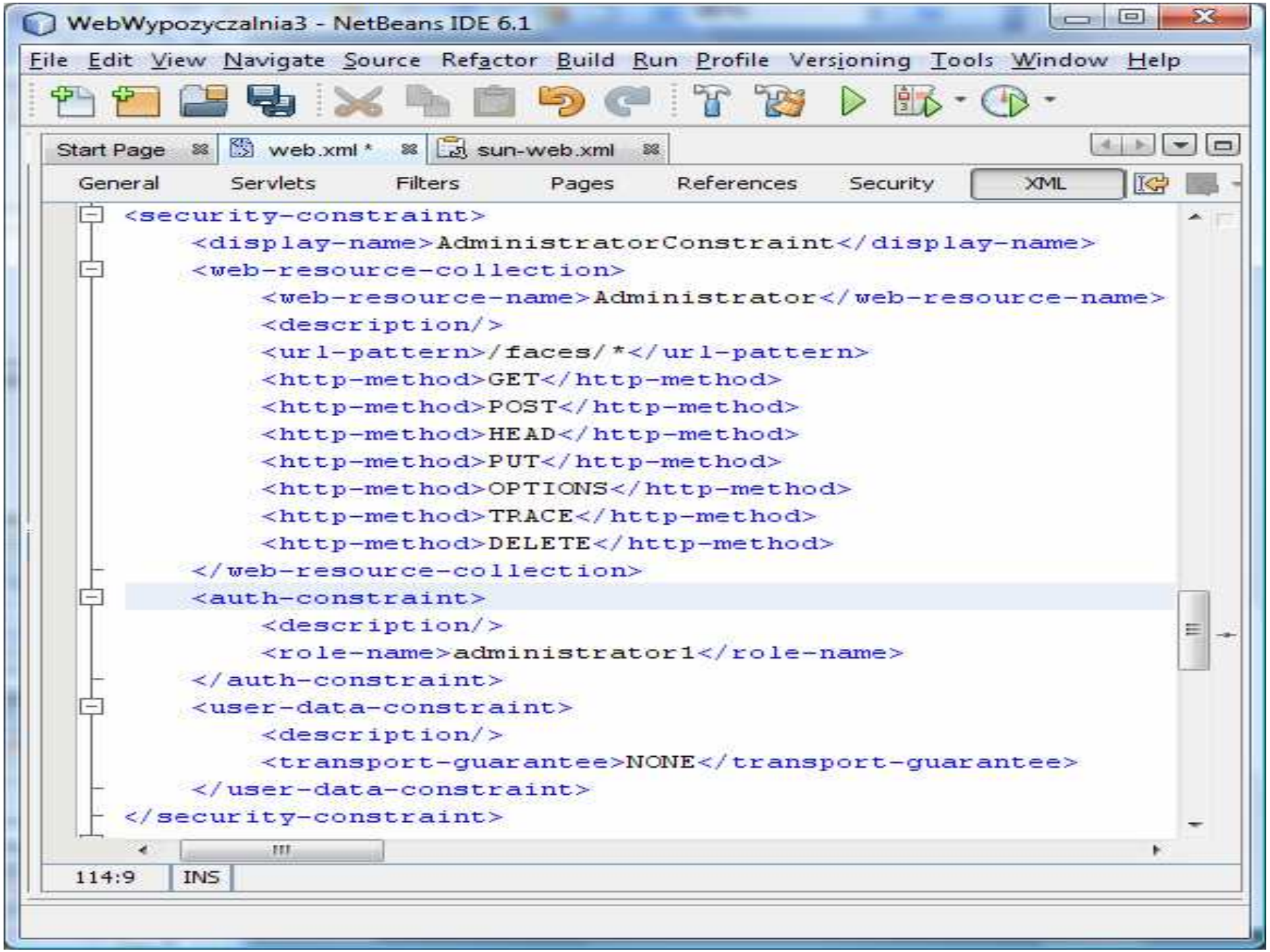


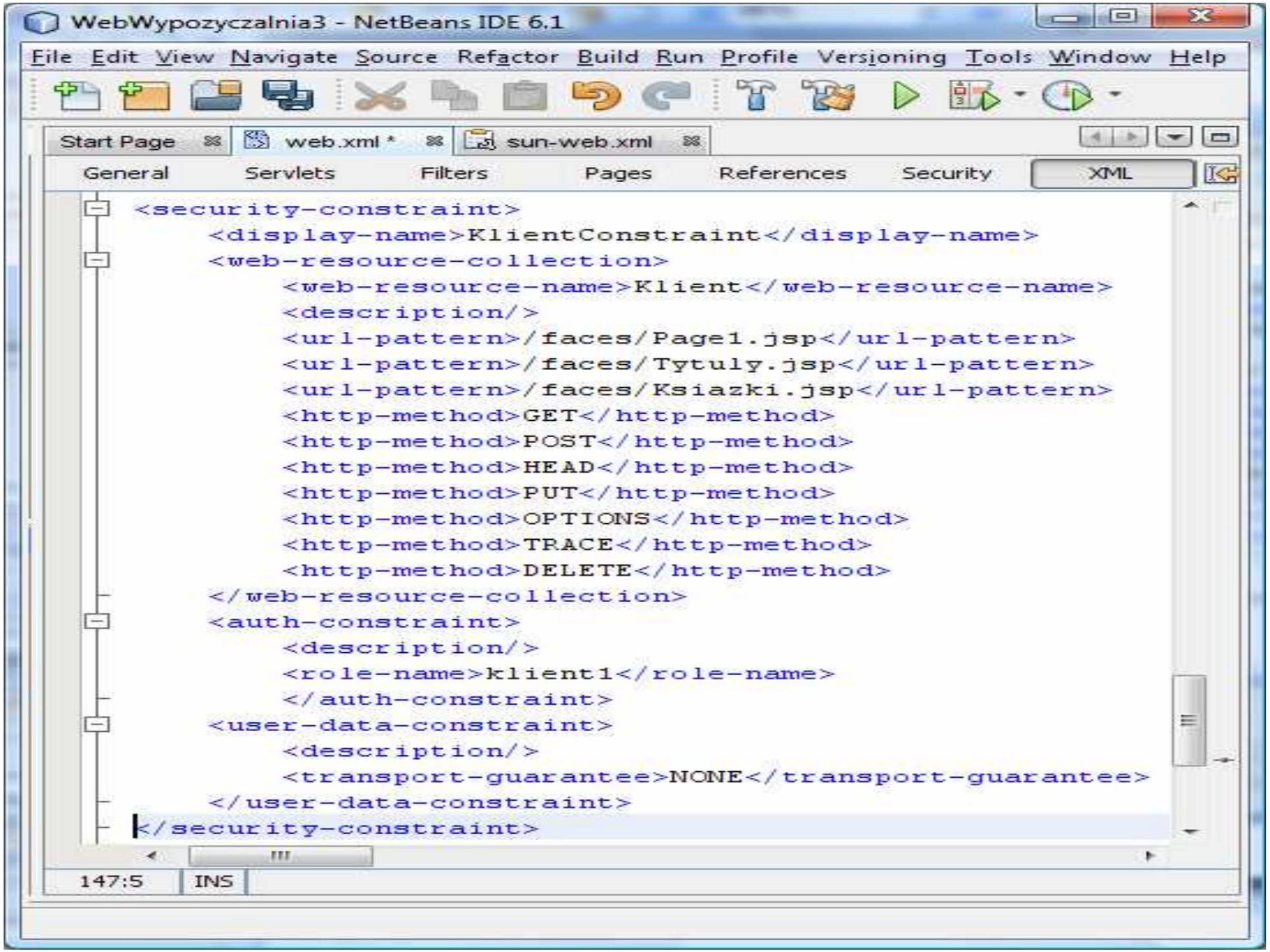
7. Ustawienie czasu sesji



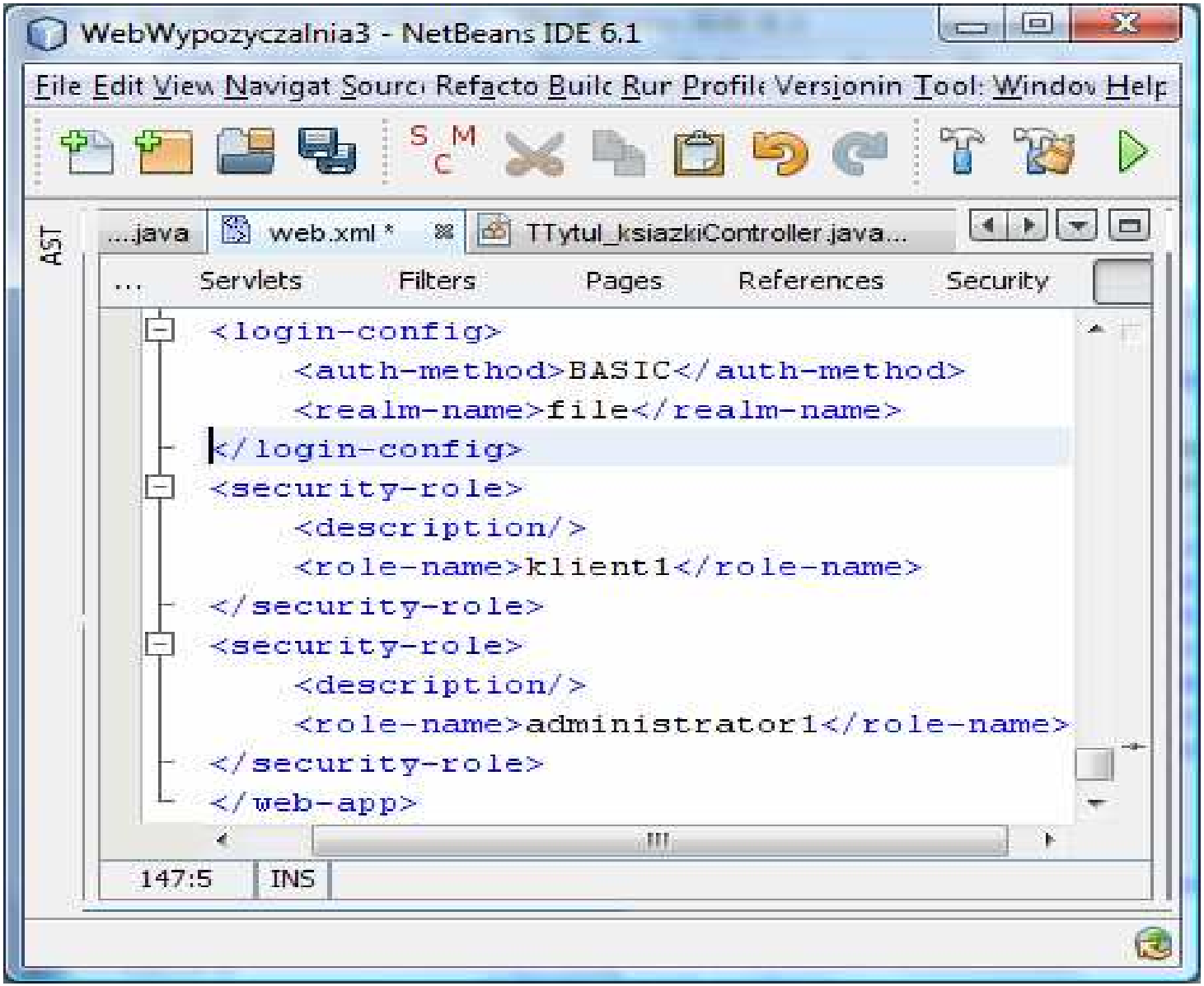
8. Zawartość deskryptora aplikacji ***web.xml***



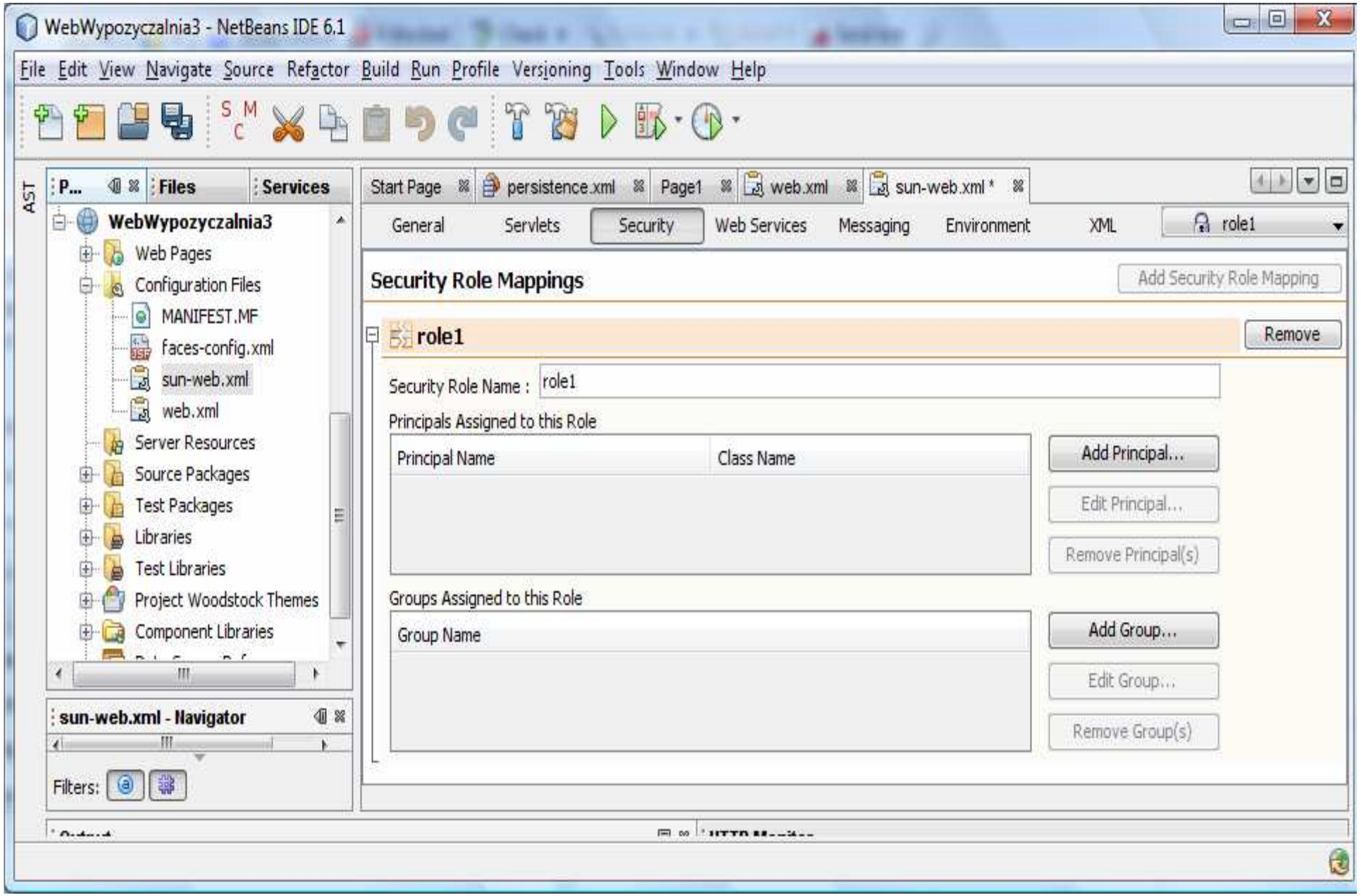

WebWypozyczalnia3 - NetBeans IDE 6.1
File Edit View Navigate Source Refactor Build Run Profile Versioning Tools Window Help
Start Page
web.xml *
sun-web.xml
General
Servlets
Filters
Pages
References
Security
XML
<security-constraint>
<display-name>AdministratorConstraint</display-name>
<web-resource-collection>
<web-resource-name>Administrator</web-resource-name>
<description/>
<url-pattern>/faces/*</url-pattern>
<http-method>GET</http-method>
<http-method>POST</http-method>
<http-method>HEAD</http-method>
<http-method>PUT</http-method>
<http-method>OPTIONS</http-method>
<http-method>TRACE</http-method>
<http-method>DELETE</http-method>
</web-resource-collection>
<auth-constraint>
<description/>
<role-name>administrator1</role-name>
</auth-constraint>
<user-data-constraint>
<description/>
<transport-guarantee>NONE</transport-guarantee>
</user-data-constraint>
</security-constraint>
114:9
INS


WebWypozyczalnia3 - NetBeans IDE 6.1
File Edit View Navigate Source Refactor Build Run Profile Versioning Tools Window Help
Start Page
web.xml *
sun-web.xml
General
Servlets
Filters
Pages
References
Security
XML
<security-constraint>
<display-name>KlientConstraint</display-name>
<web-resource-collection>
<web-resource-name>Klient</web-resource-name>
<description/>
<url-pattern>/faces/Page1.jsp</url-pattern>
<url-pattern>/faces/Tytuly.jsp</url-pattern>
<url-pattern>/faces/Ksiazki.jsp</url-pattern>
<http-method>GET</http-method>
<http-method>POST</http-method>
<http-method>HEAD</http-method>
<http-method>PUT</http-method>
<http-method>OPTIONS</http-method>
<http-method>TRACE</http-method>
<http-method>DELETE</http-method>
</web-resource-collection>
<auth-constraint>
<description/>
<role-name>klient1</role-name>
</auth-constraint>
<user-data-constraint>
<description/>
<transport-guarantee>NONE</transport-guarantee>
</user-data-constraint>
</security-constraint>
147:5
INS

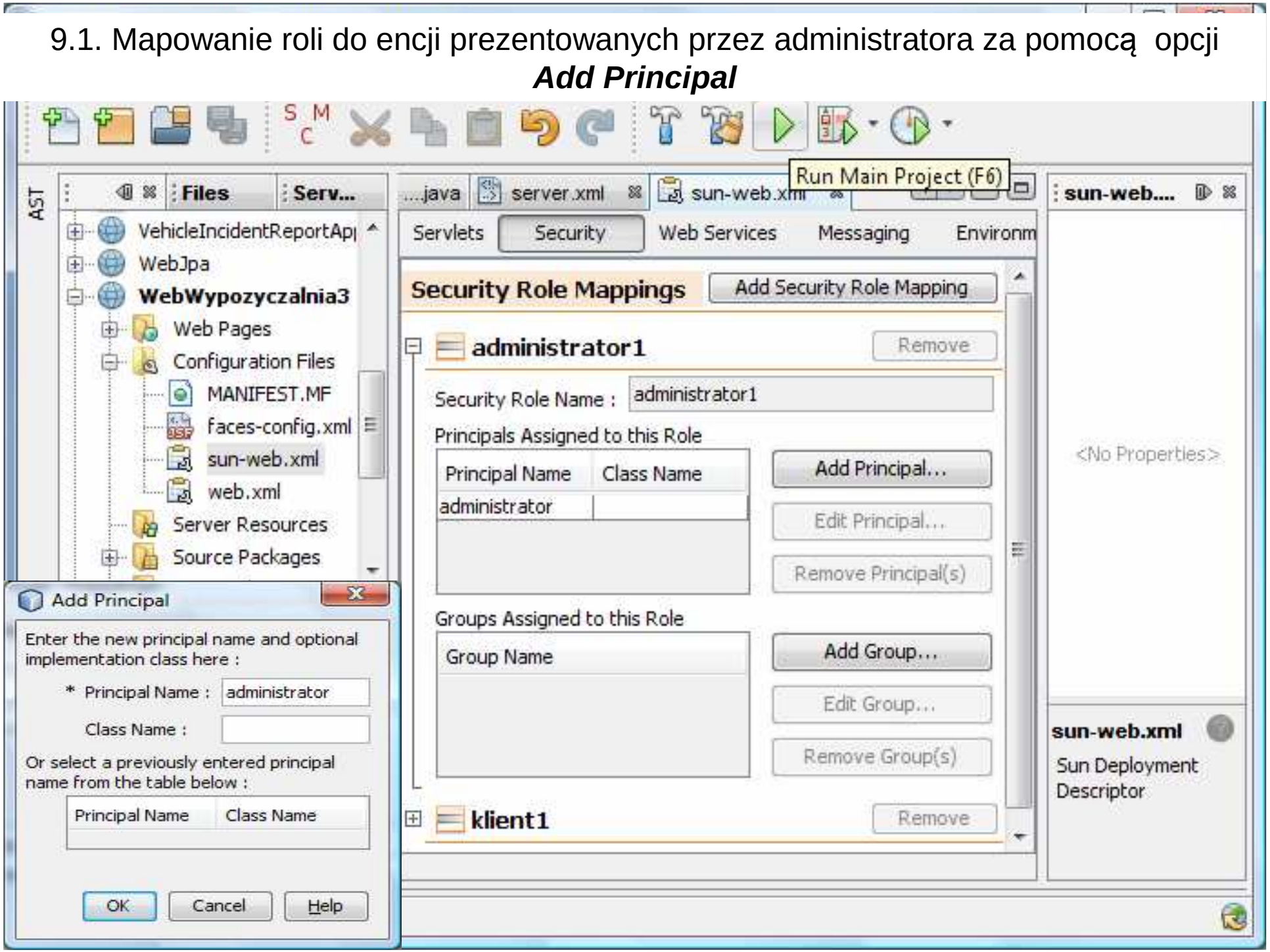
Definicja ról i systemowy formularz logowania



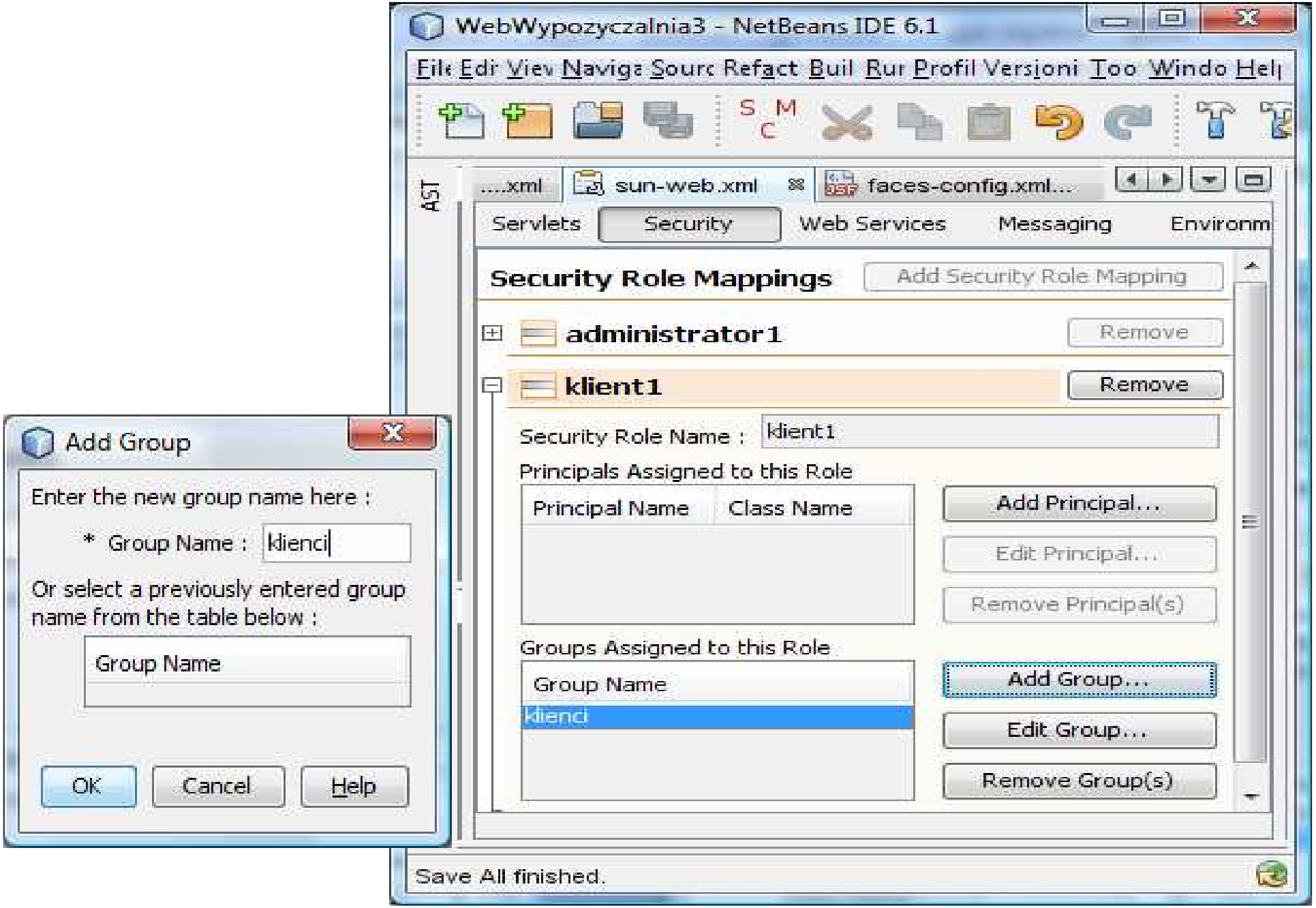
9. Mapowanie mechanizmów bezpieczeństwa z aplikacji do serwera aplikacji za pomocą mapowania ról bezpieczeństwa z ***pliku web.xml*** do deskryptora serwera aplikacji ***sun-web.xml***



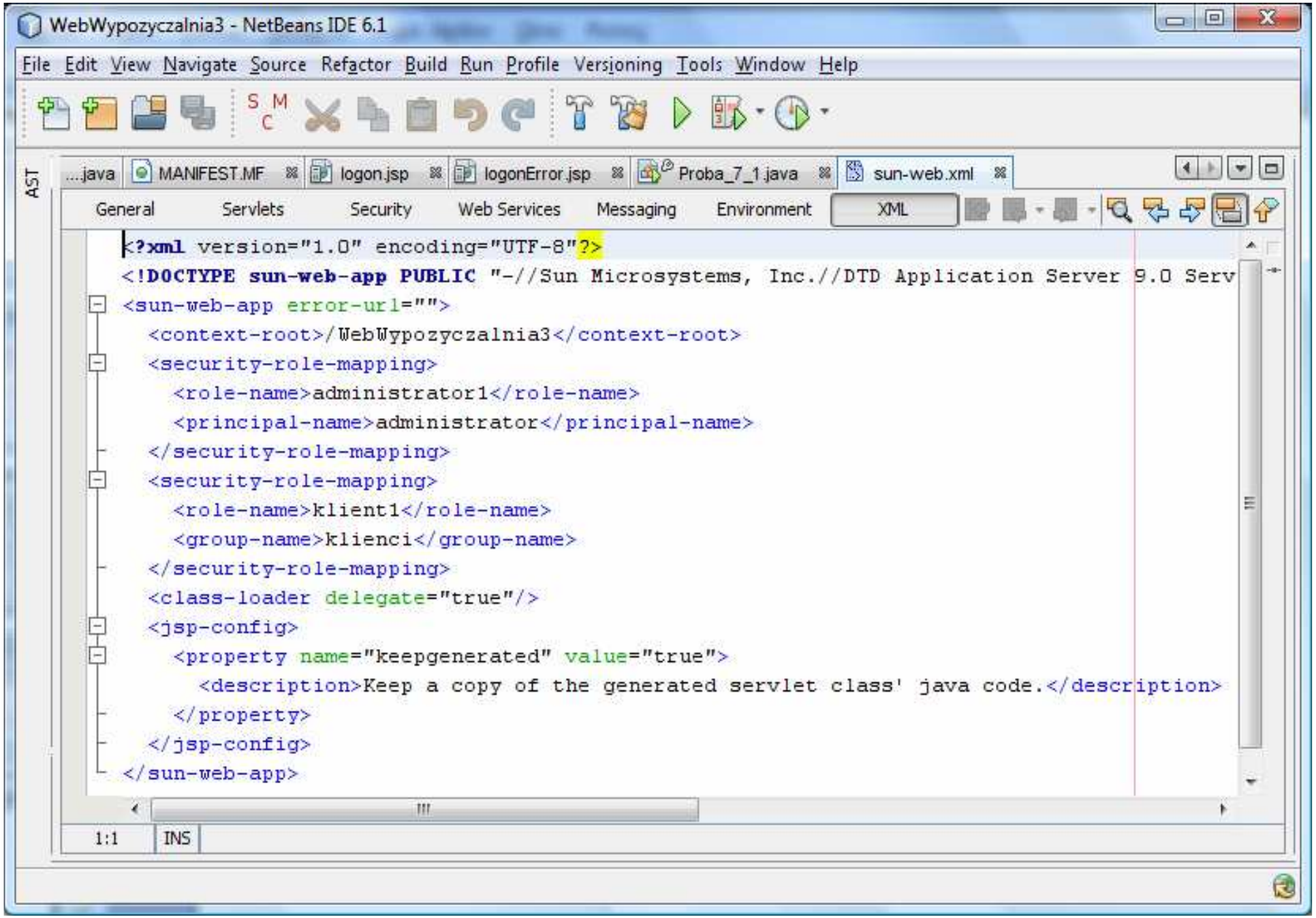
9.1. Mapowanie roli do encji prezentowanych przez administratora za pomocą opcji ***Add Principal***



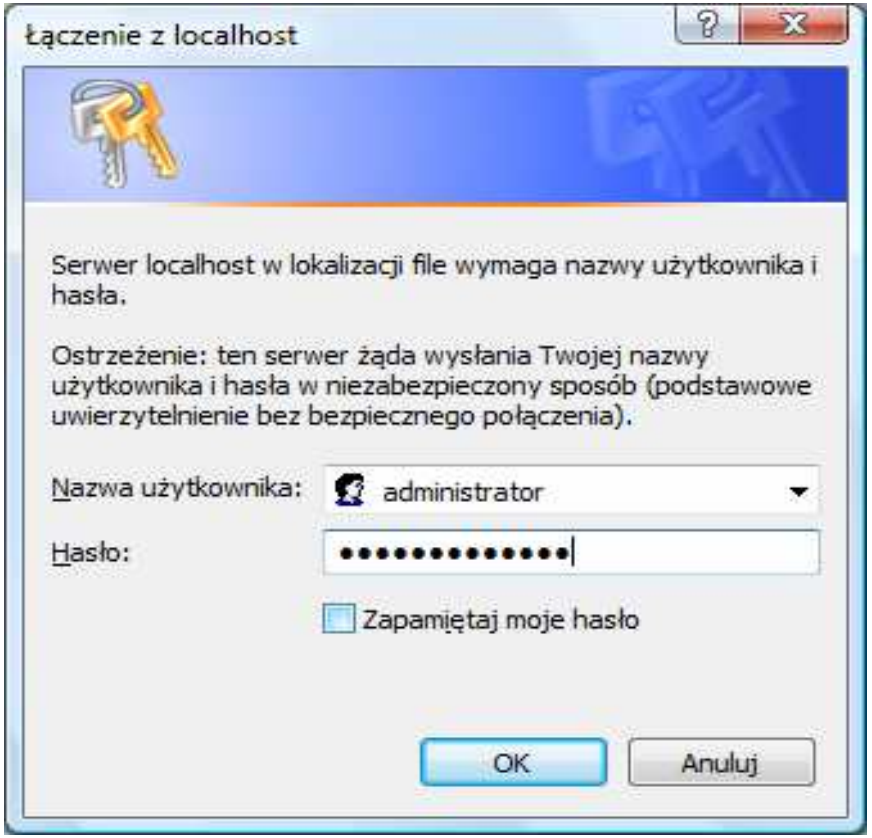
9.2. Mapowanie roli do encji prezentowanych przez klienta za pomocą opcji ***Add Group***

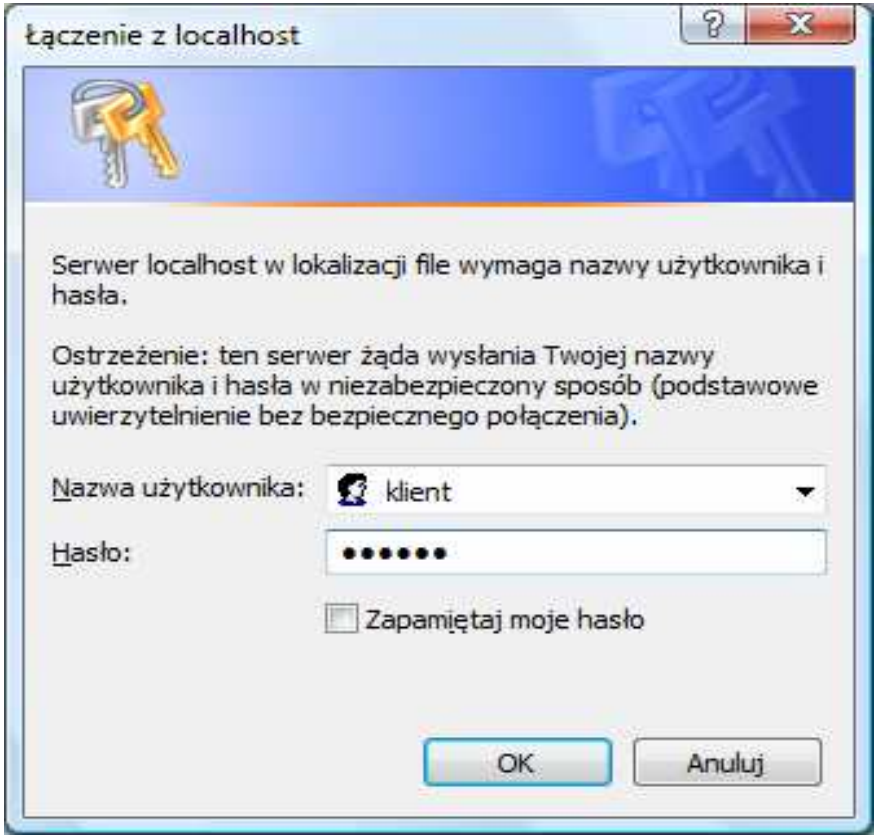


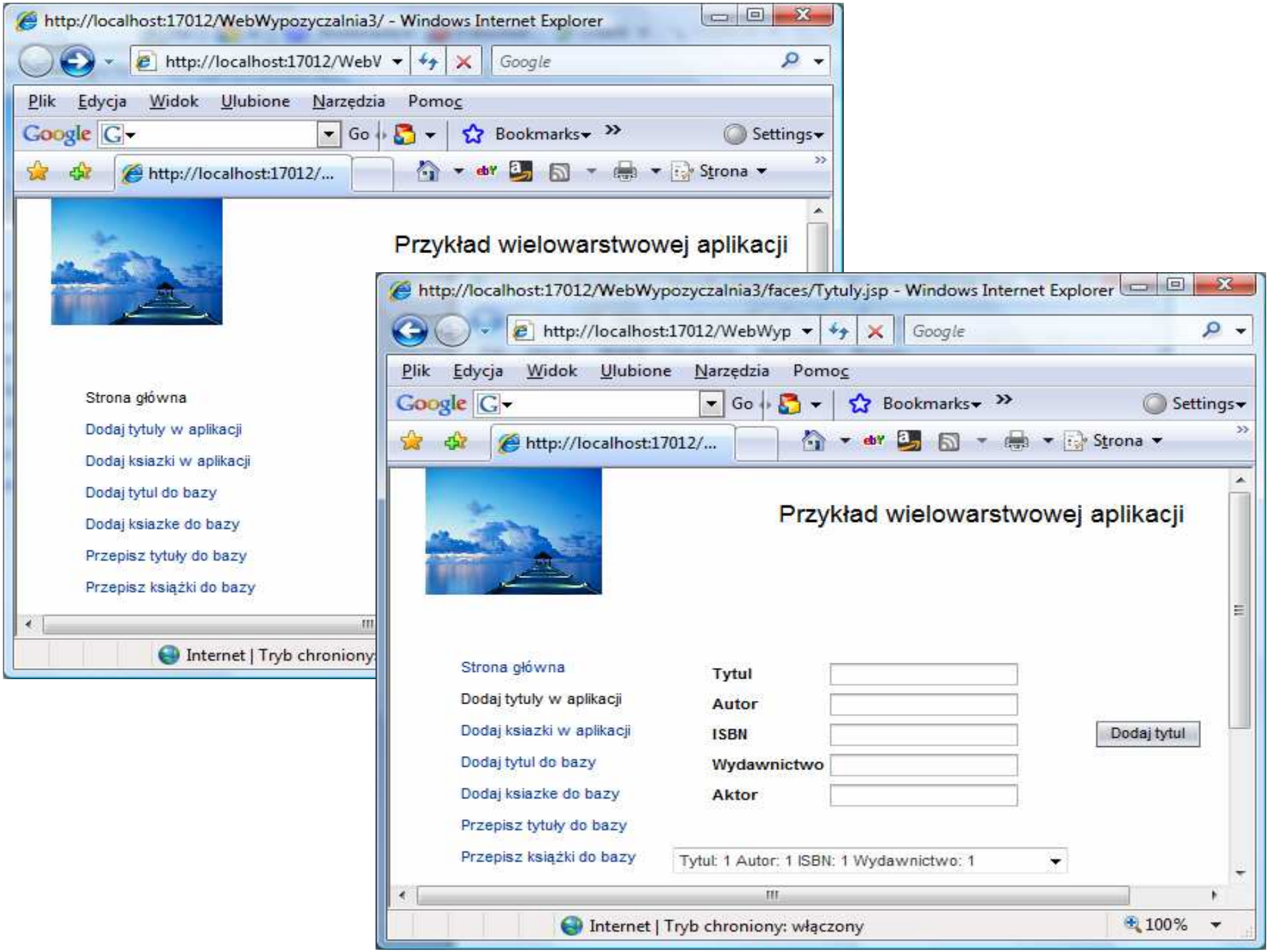
9.3. Zawartość deskryptora serwera aplikacji



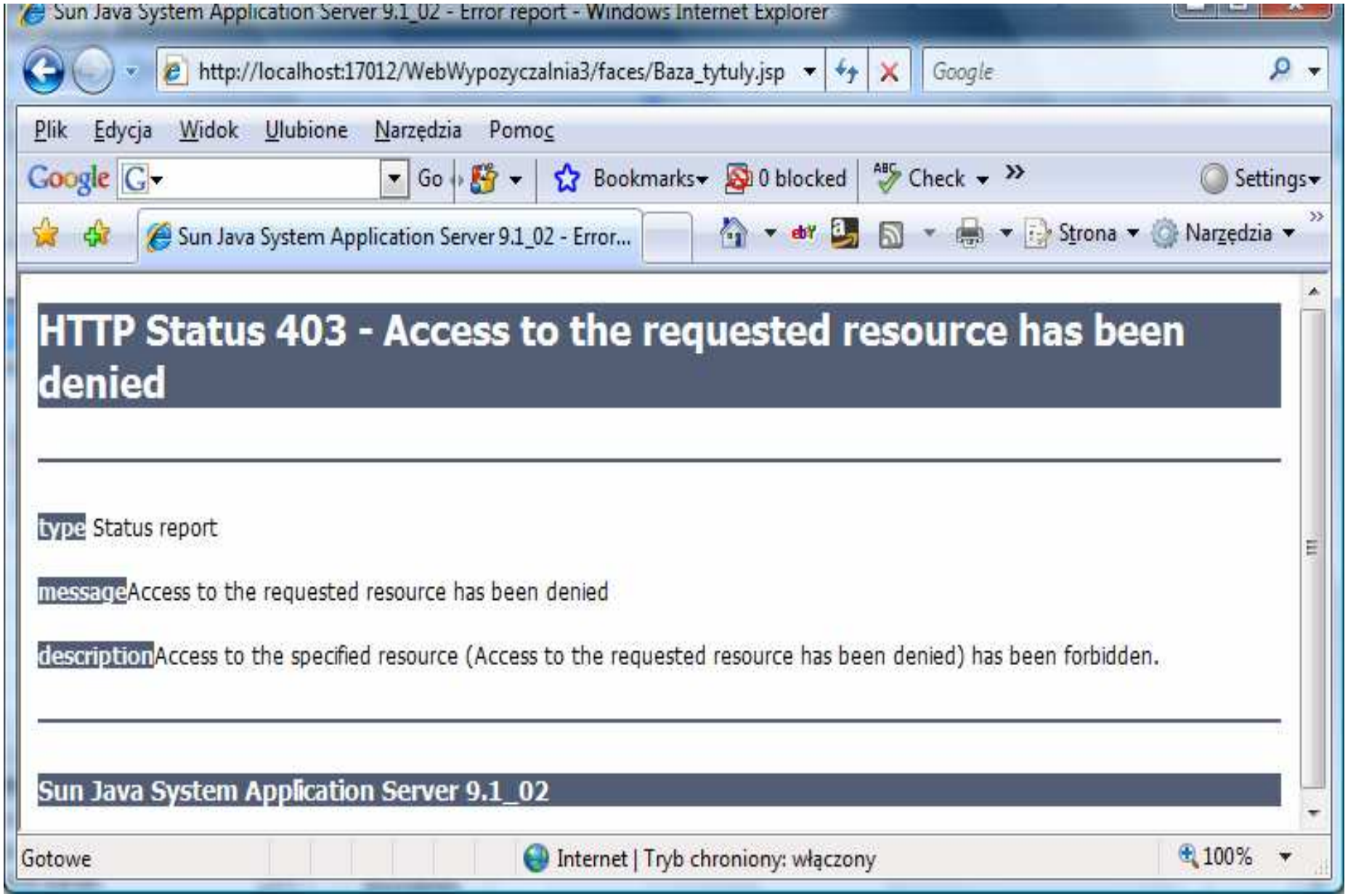
9.4. Uruchomienie aplikacji w trybie uwierzytelniania **Basic-*Based Authentication*** HTTP, zabezpieczenia przez role



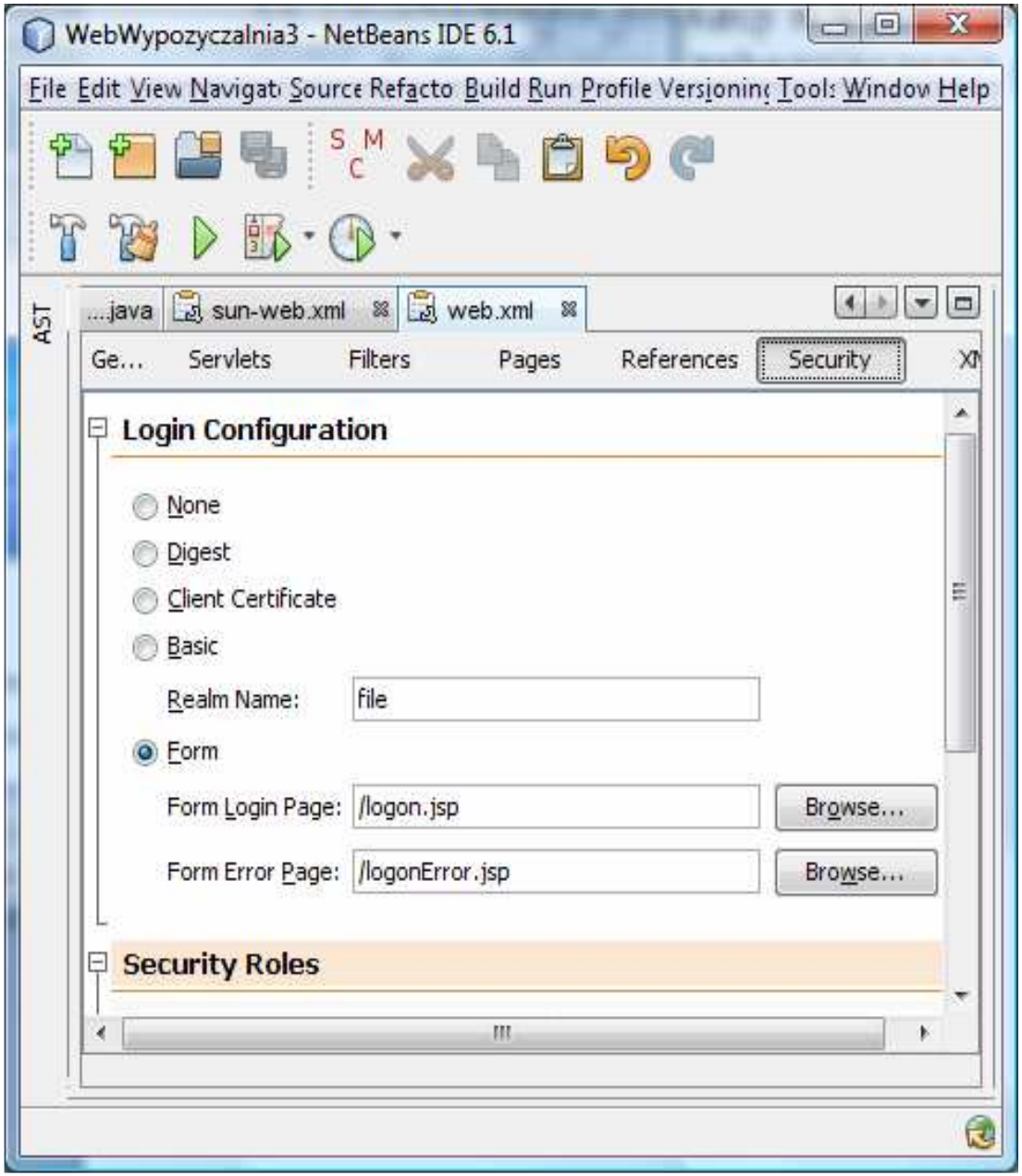


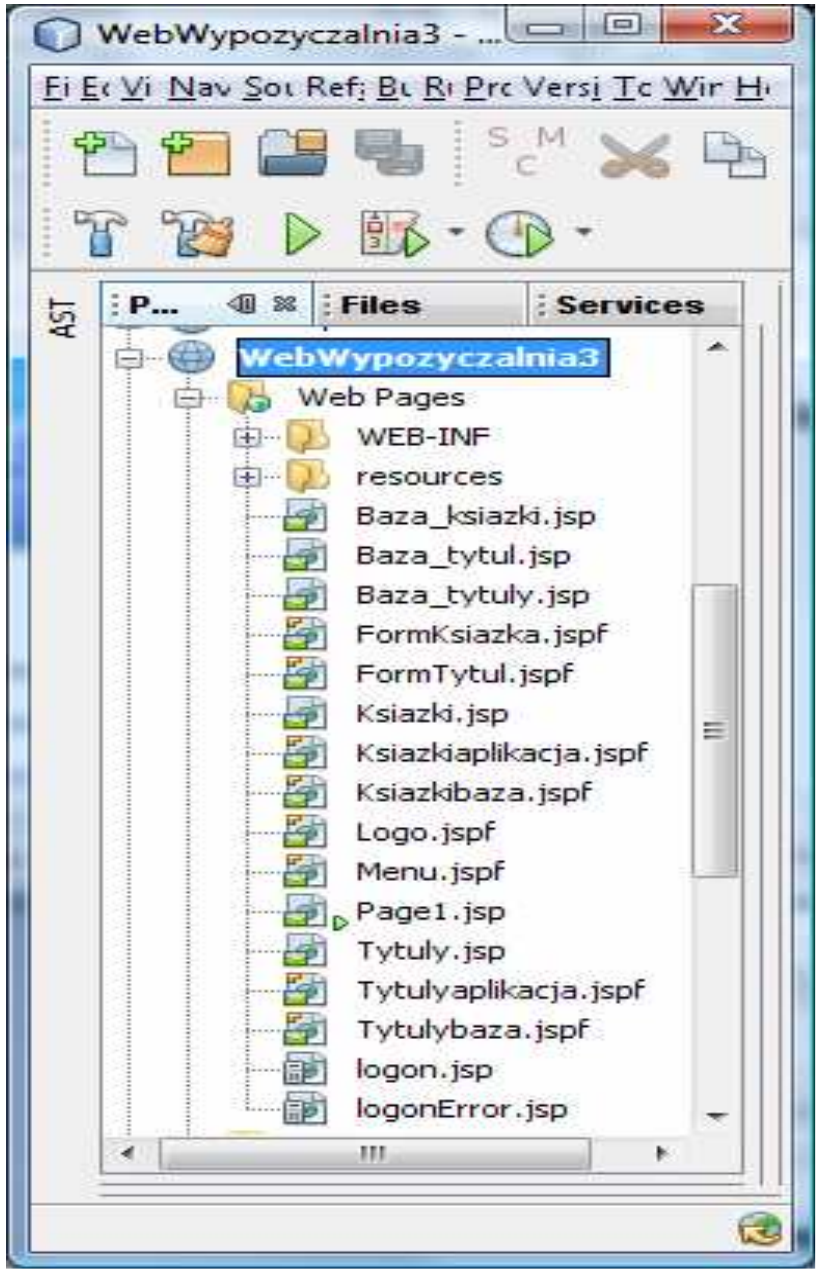

http://localhost:17012/WebWypozyczalnia3/ - Windows Internet Explorer
Plik Edycja Widok Ulubione Narzędzia Pomoc
Przykład wielowarstwowej aplikacji
Strona główna
Dodaj tytuly w aplikacji
Dodaj ksiazki w aplikacji
Dodaj tytul do bazy
Dodaj ksiazke do bazy
Przepisz tytuły do bazy
Przepisz książki do bazy
http://localhost:17012/WebWypozyczalnia3/faces/Tytuly.jsp - Windows Internet Explorer
Przykład wielowarstwowej aplikacji
Tytul
Autor
ISBN
Wydawnictwo
Aktor
Dodaj tytul
Tytul: 1 Autor: 1 ISBN: 1 Wydawnictwo: 1
Internet | Tryb chroniony: włączony
100%

Niedostępne strony dla użytkownika „klient” występującego w roli „klient1”
(objęte ograniczeniem ***Web Resource Collection***)

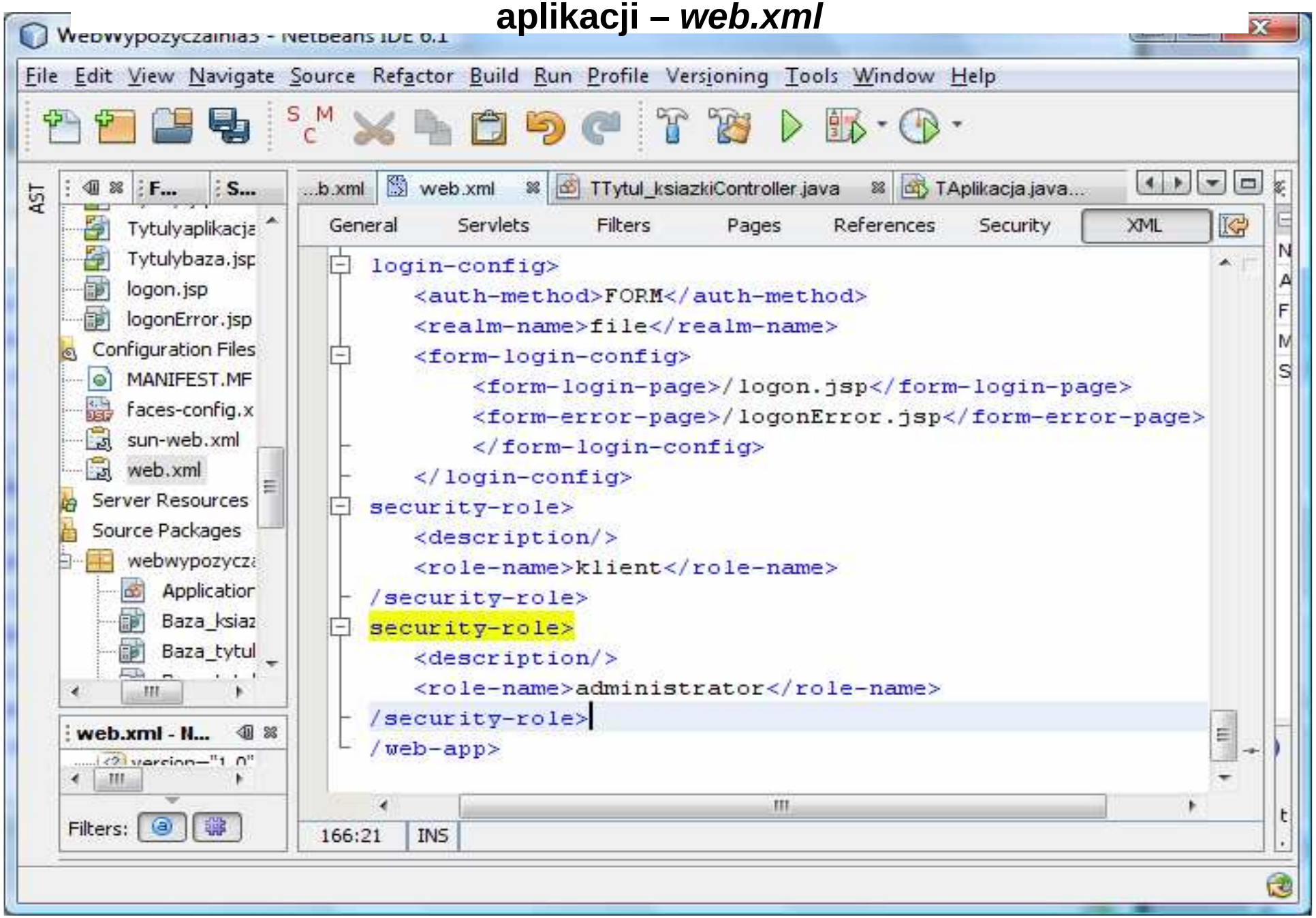


10. Uruchomienie aplikacji w trybie uwierzytelniania ***Form-Based Authentication***, zabezpieczenia przez role

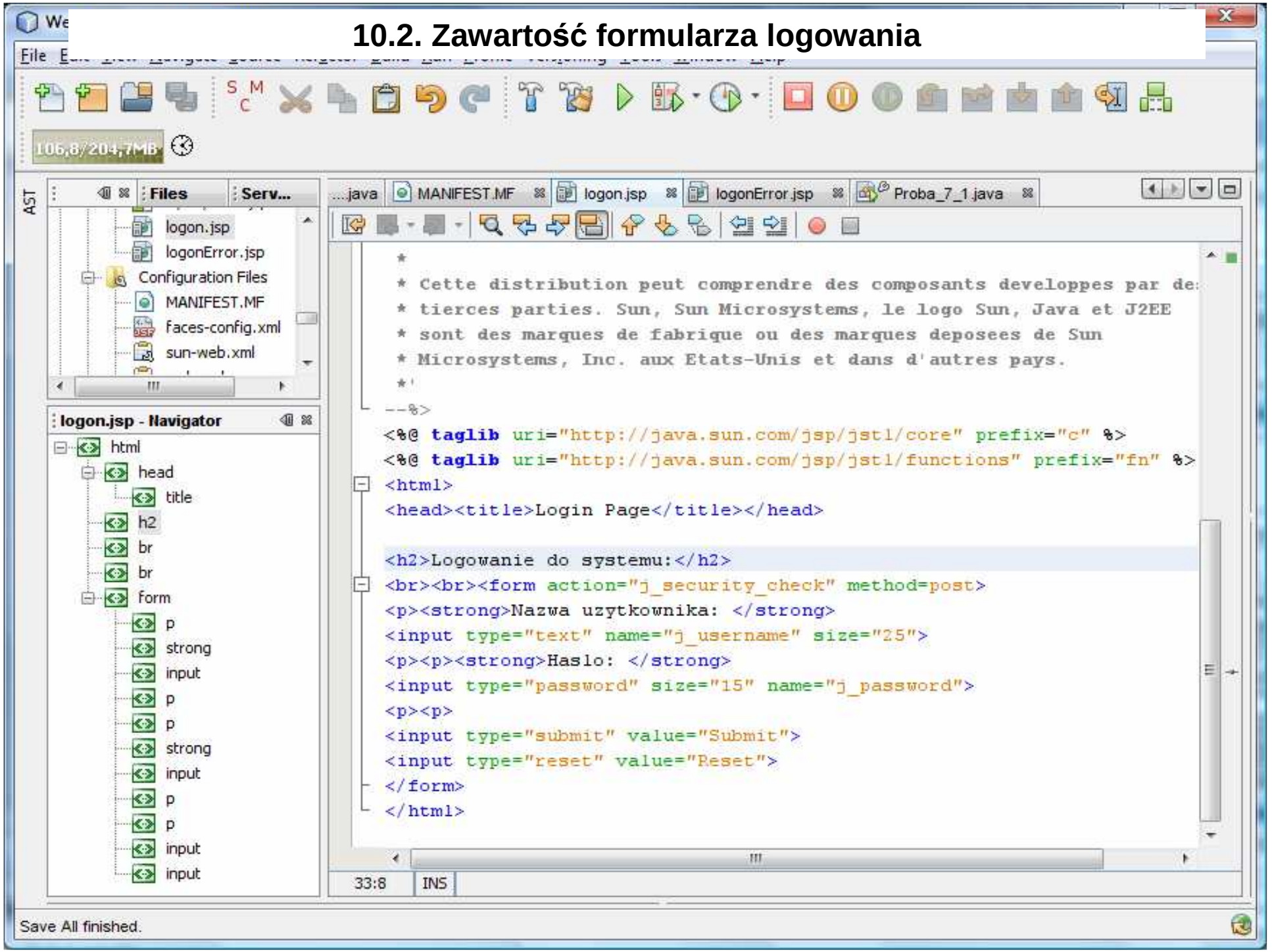




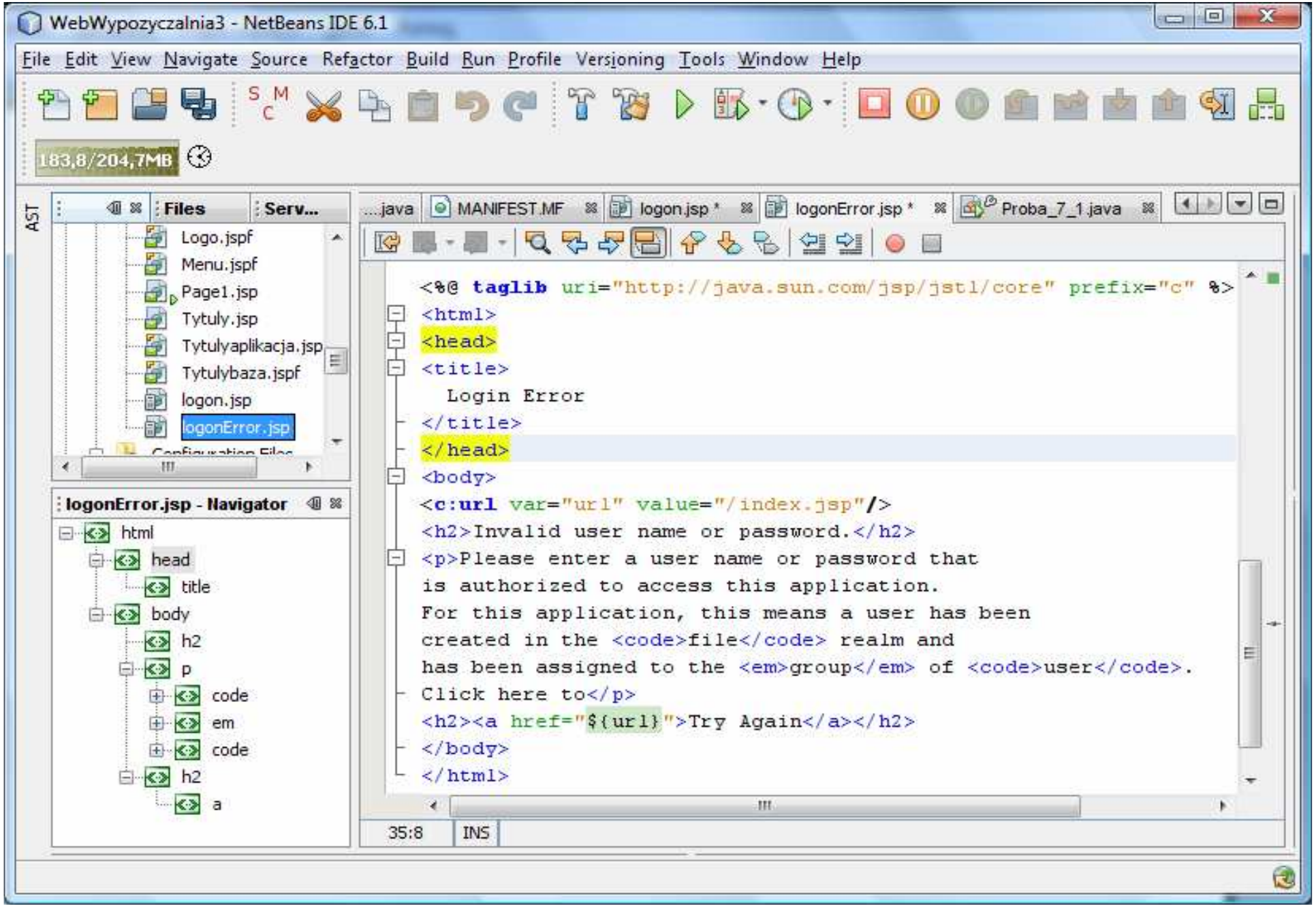
10.1. Deklaracja formularza okna logowania w pliku deskryptora aplikacji – *web.xml*



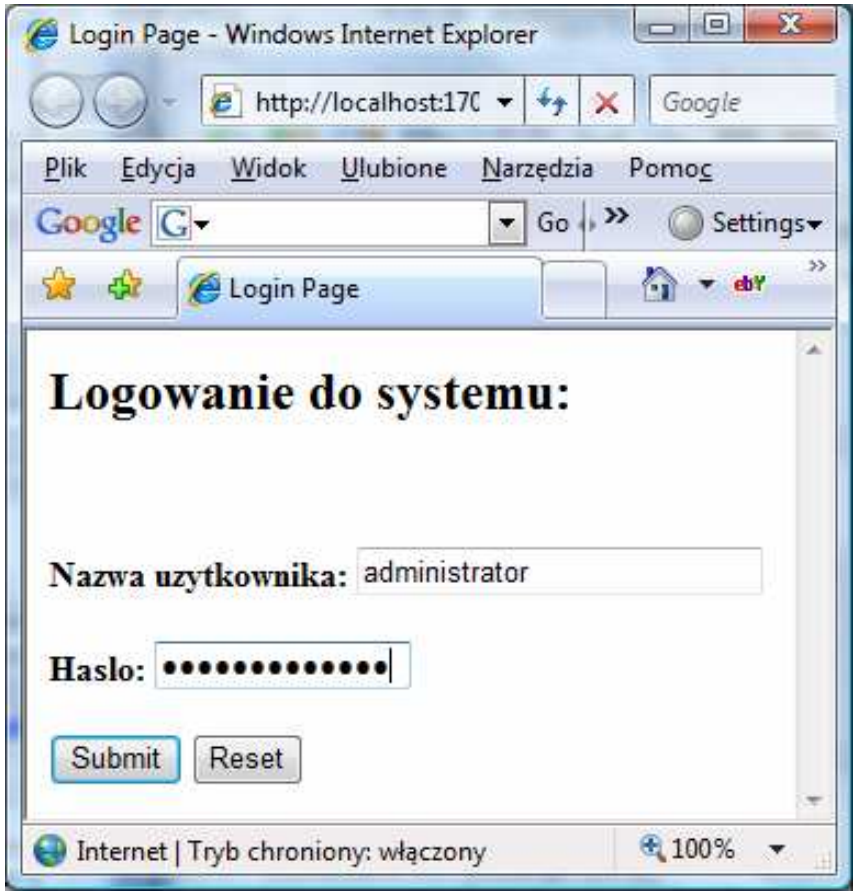
10.2. Zawartość formularza logowania

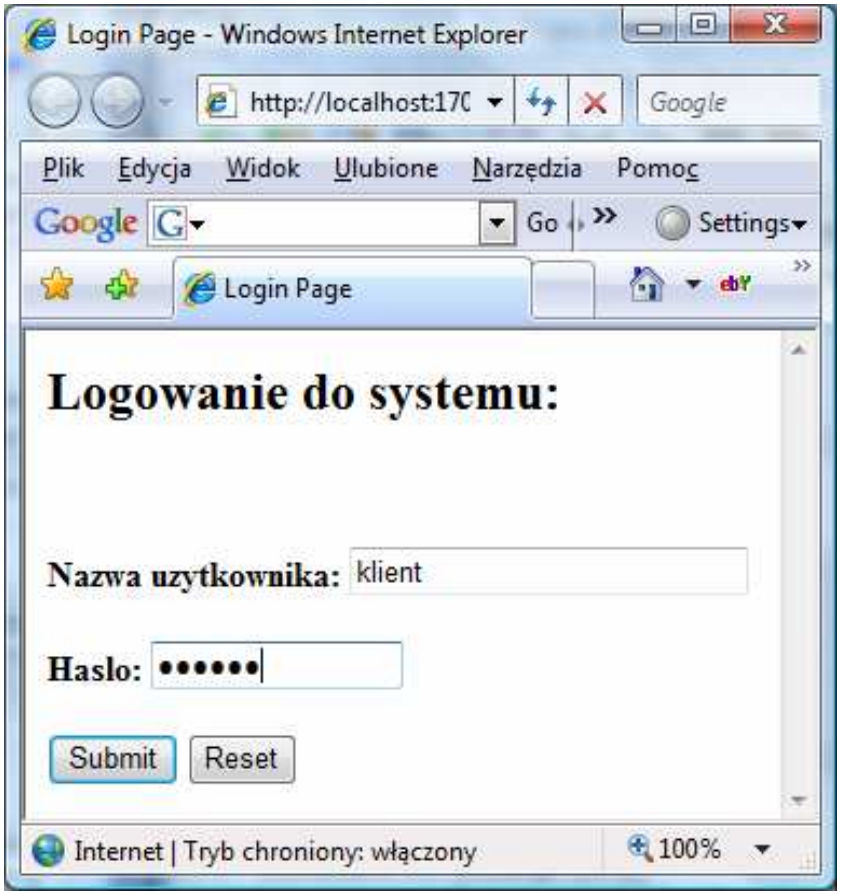


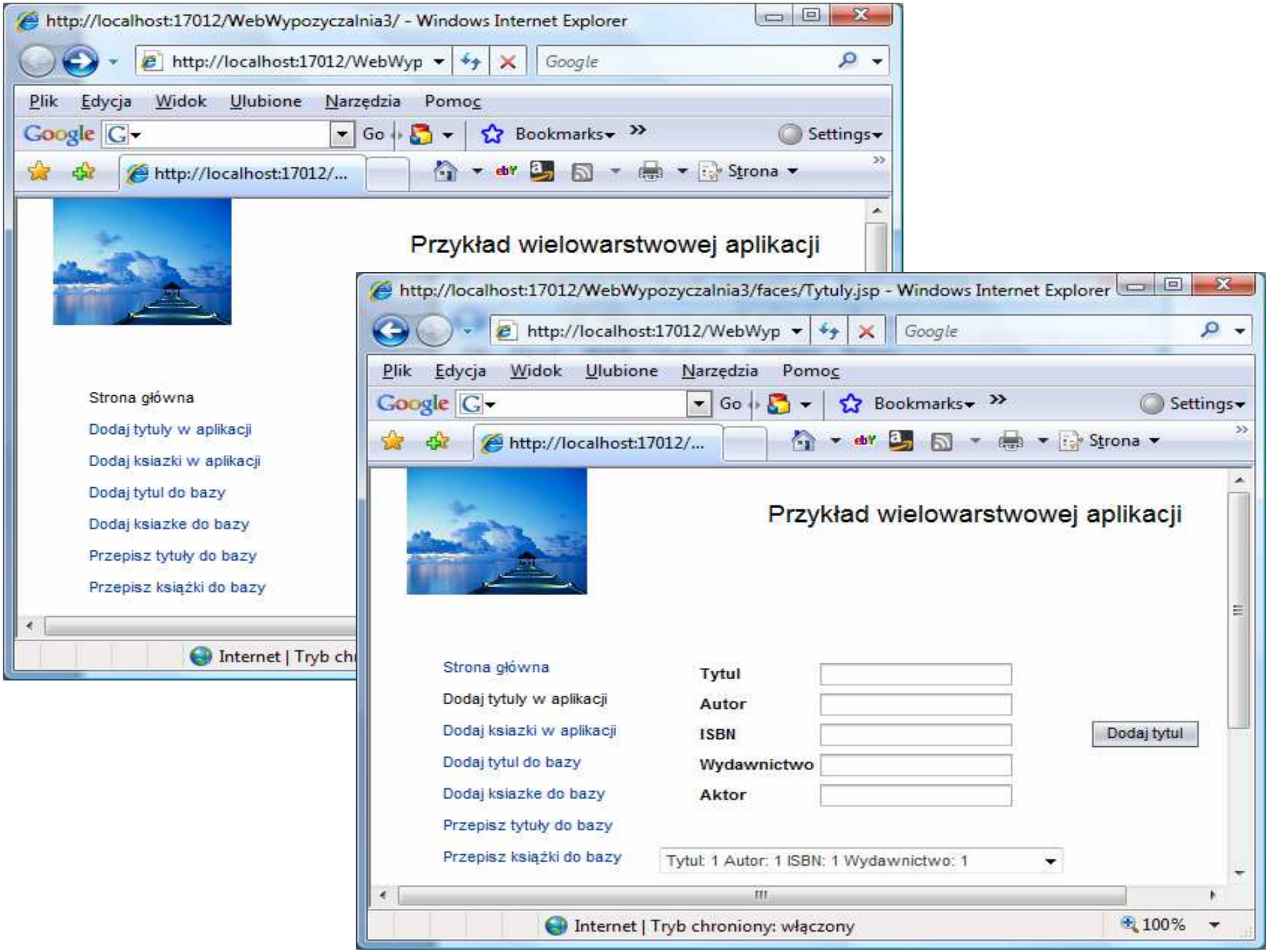
10.3. Zawartość okna obsługi błędu logowania



10.4.Uruchomienie aplikacji w trybie uwierzytelniania ***Form***, zabezpieczenia przez role






http://localhost:17012/WebWypozyczalnia3/ - Windows Internet Explorer
http://localhost:17012/WebWyp
Google
Plik Edycja Widok Ulubione Narzędzia Pomoc
Go
Bookmarks
Settings
http://localhost:17012/...
Strona
Przykład wielowarstwowej aplikacji
Strona główna
Dodaj tytuly w aplikacji
Dodaj ksiazki w aplikacji
Dodaj tytul do bazy
Dodaj ksiazke do bazy
Przepisz tytuły do bazy
Przepisz książki do bazy
Internet | Tryb ch
http://localhost:17012/WebWypozyczalnia3/faces/Tytuly.jsp - Windows Internet Explorer
http://localhost:17012/WebWyp
Google
Plik Edycja Widok Ulubione Narzędzia Pomoc
Go
Bookmarks
Settings
http://localhost:17012/...
Strona
Przykład wielowarstwowej aplikacji
Strona główna
Dodaj tytuly w aplikacji
Dodaj ksiazki w aplikacji
Dodaj tytul do bazy
Dodaj ksiazke do bazy
Przepisz tytuły do bazy
Przepisz książki do bazy
Tytul
Autor
ISBN
Wydawnictwo
Aktor
Dodaj tytul
Tytul: 1 Autor: 1 ISBN: 1 Wydawnictwo: 1
Internet | Tryb chroniony: włączony
100%

Niedostępne strony dla użytkownika występującego w roli ***„klient1***” (objęte ograniczeniem ***Web Resource Collection***)