

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 NetBeans6.1 na 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 podanych 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**

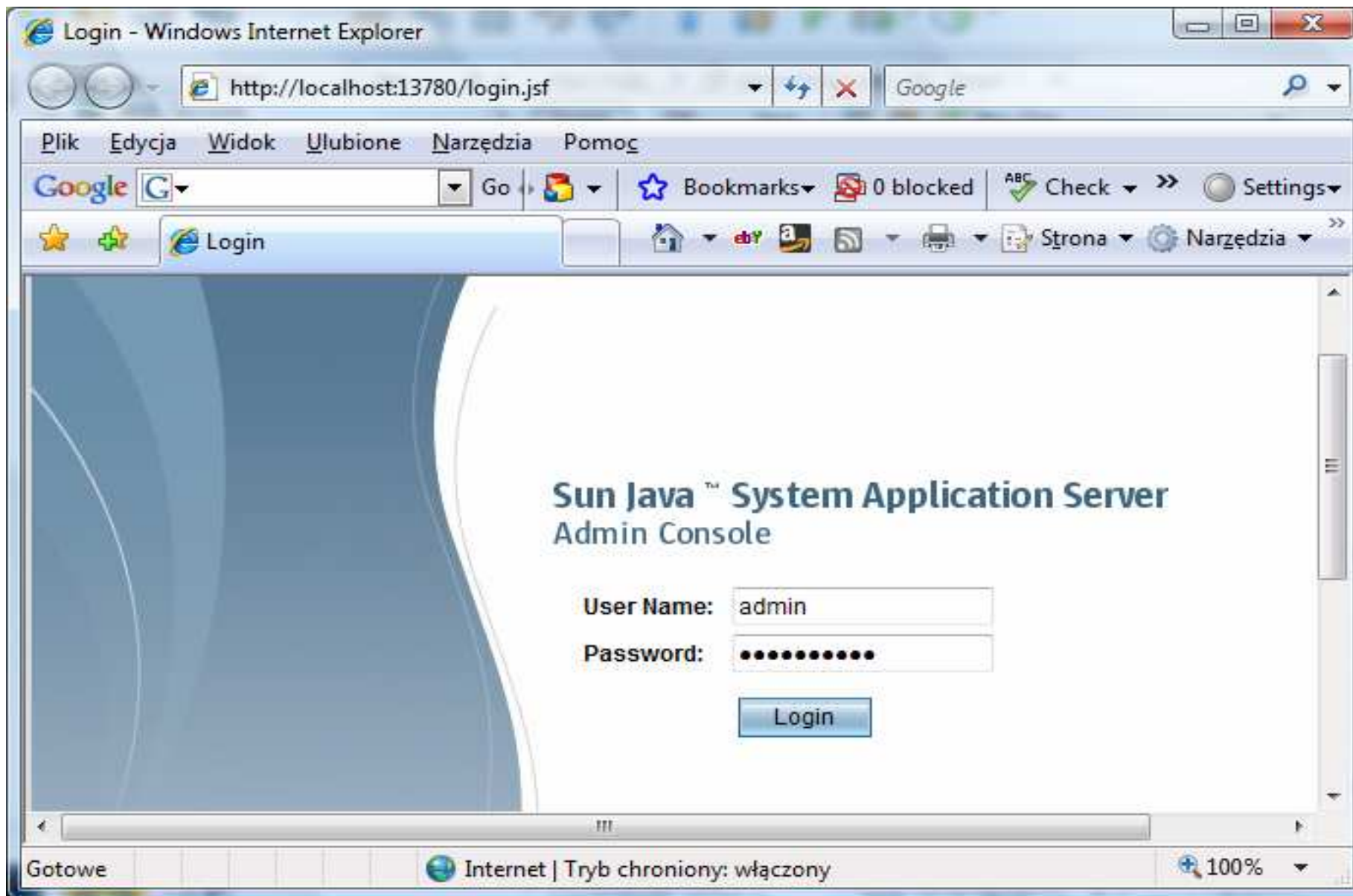
Ad 1, 2 file, admin-realm

- 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



Sun Java System Application Server 9.1_02 Admin Console - Windows Internet Explorer

http://localhost:13780/?rs-285265105=rs-1081433172

Plik Edycja Widok Ulubione Narzędzia Pomoc

Google G 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
- JBIC
 - Service Assemblies
 - Components
 - Shared Libraries
- Custom MBeans
- Resources
- Configuration

Update Center

Getting 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 offline

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

Go Bookmarks 0 blocked Check AutoLink Settings

Sun Java System Application Server 9.1_02 Admin...

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

- 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

Plik Edycja Widok Ulubione Narzędzia Pomoc

Google Go 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

Configuration > Security > Realms > file

Edit Realm

Edit an existing security realm

[Manage Users](#) [Save](#)

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

The screenshot shows the Sun Java System Application Server Admin Console interface. The browser window title is "Sun Java System Application Server 9.1_02 Admin...". The console header displays "User: admin | Domain: personalDomain | Server: localhost" and "Sun Java™ System Application Server Admin Console".

The left sidebar shows a tree view of the system configuration. The "Security" folder is expanded, and the "Realms" sub-folder is selected. The "file" realm is highlighted.

The main content area shows the breadcrumb "Configuration > Security > Realms > file" and the title "New File Realm User". Below the title, it says "Create new user accounts for the currently selected security realm." There are "OK" and "Cancel" buttons in the top right.

The form contains the following fields:

- User ID ***: A text box containing "klient". Below it, a note states: "Name of a user to be granted access to this realm; name can be up to 255 characters, must contain only alphanumeric, underscore, dash, or dot characters".
- Group List**: A text box containing "klienci". Below it, a note states: "Separate multiple groups with commas".
- New Password ***: A password field with six dots.
- Confirm New Password ***: A password field with six dots.

The status bar at the bottom shows "Gotowe", "Internet | Tryb chroniony: włączony", and "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 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

Configuration > Security > Realms > file

File Users

Manage user accounts for the currently selected security realm.

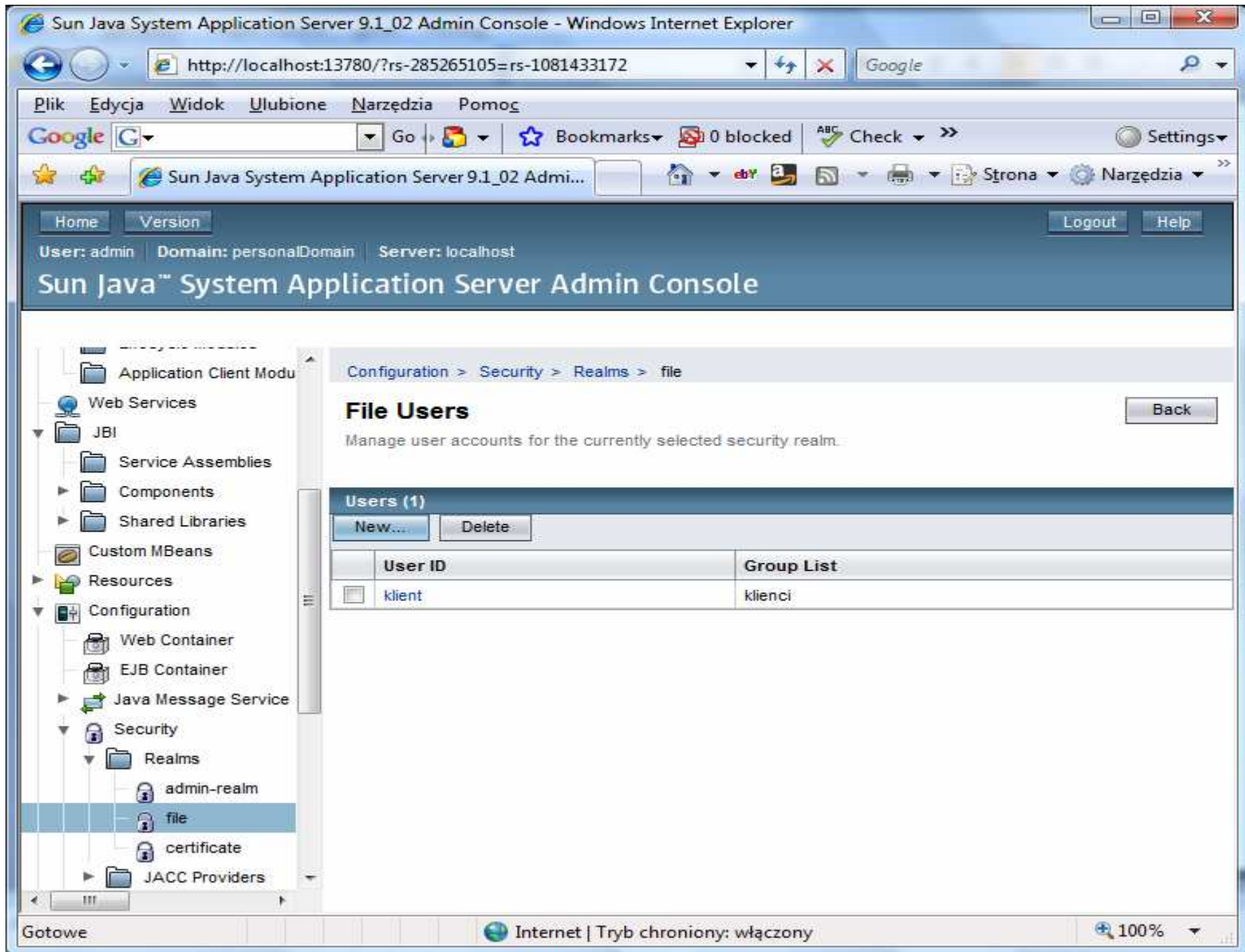
Back

Users (1)

New... Delete

	User ID	Group List
<input type="checkbox"/>	klient	klienci

Gotowe Internet | Tryb chroniony: włączony 100%

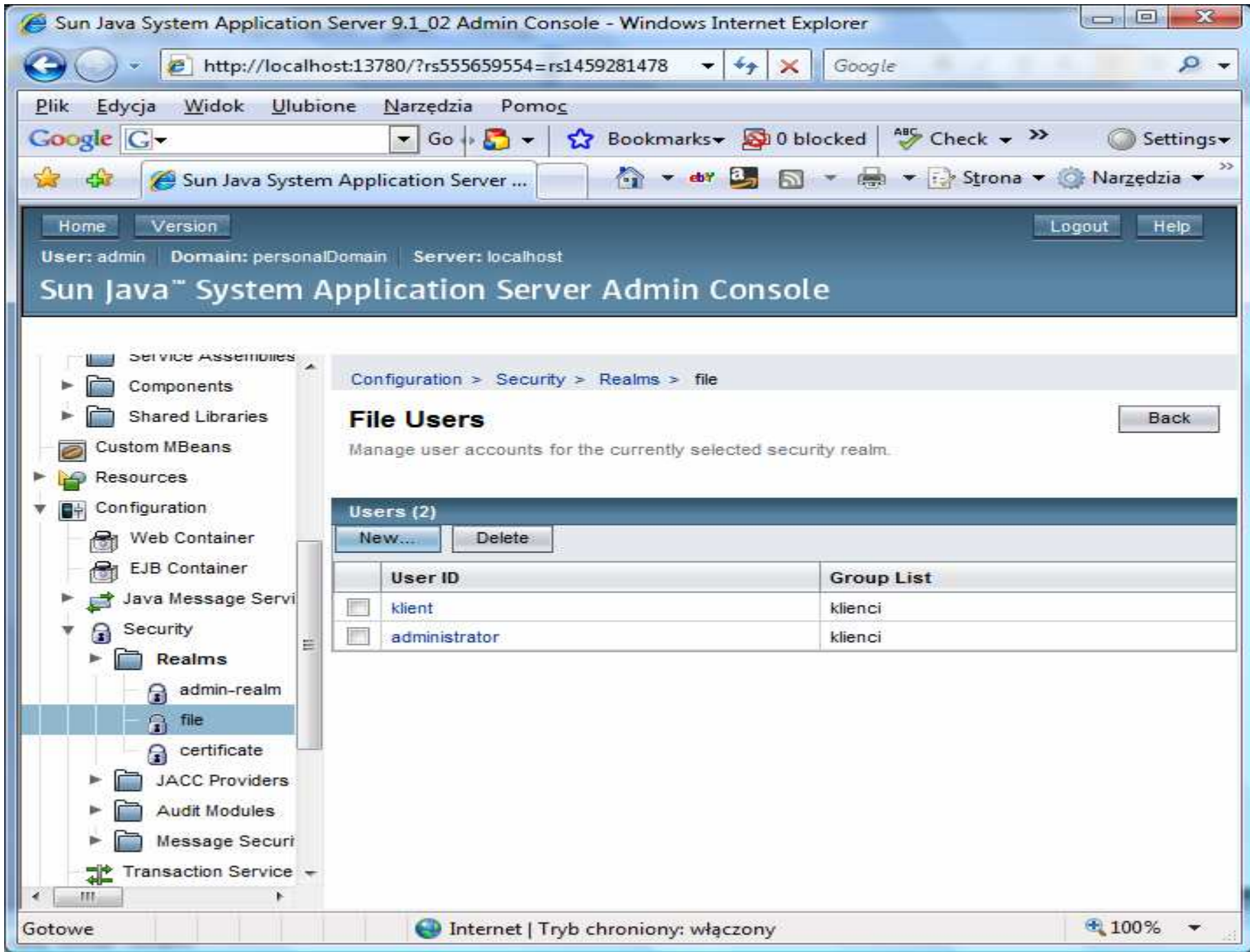


Wstawienie użytkownika z pełnymi uprawnieniami, które zostaną ustawione na poziomie aplikacji

The screenshot shows the Sun Java System Application Server Admin Console in a web browser. The browser's address bar displays "Sun Java System Application Server ...". The console interface includes a navigation menu on the left with categories like "Service Assemblies", "Resources", and "Configuration". The "Configuration" section is expanded to show "Security" > "Realms", with the "file" realm selected. The main content area displays the "New File Realm User" dialog box, which is used to create new user accounts for the selected security realm. The dialog box contains the following fields:

- User ID ***: administrator
- Group List**: klienci
- New Password ***: [masked with dots]
- Confirm New Password ***: [masked with dots]

The dialog box also includes "OK" and "Cancel" buttons. The browser's status bar at the bottom shows "Internet | Tryb chroniony: włączony" and a zoom level of "100%".



Home Version Logout Help
User: admin Domain: personalDomain Server: localhost
Sun Java™ System Application Server Admin Console

- Service Assemblies
 - 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

Manage user accounts for the currently selected security realm.

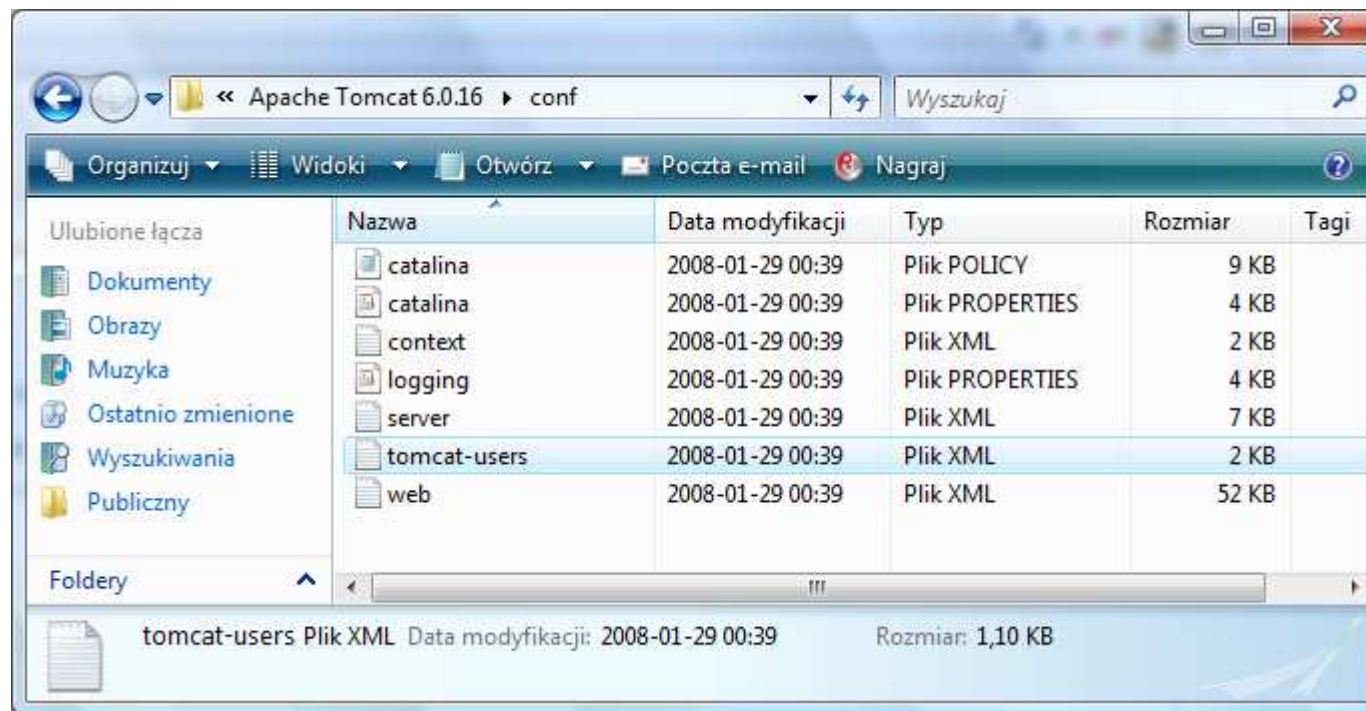
Back

Users (2)

New... Delete

	User ID	Group List
<input type="checkbox"/>	klient	klienci
<input type="checkbox"/>	administrator	klienci

2. Definiowanie ról w serwerze *Tomcat Web Server*

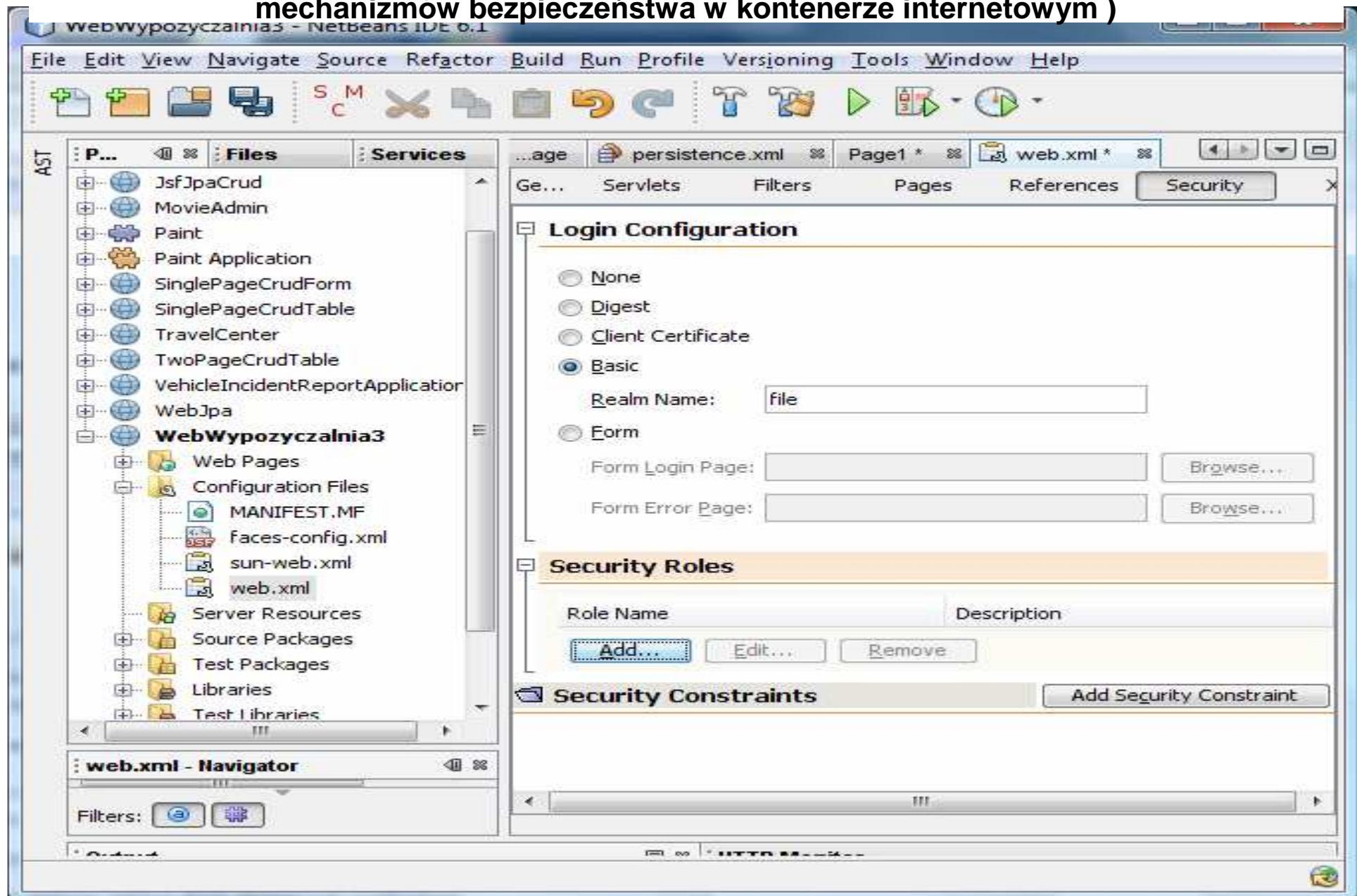



```
tomcat-users - Notatnik
Plik Edycja Format Widok Pomoc
<?xml version='1.0' encoding='utf-8'?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
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)

The screenshot shows the NetBeans IDE 6.1 interface with the 'Security' tab selected in the 'web.xml' file. The 'Login Configuration' section has 'Basic' selected. The 'Security Roles' section contains a table with two roles: 'klient1' and 'administrator1'. Two 'Add Security Role' dialog boxes are overlaid on the main window, one for 'klient1' and one for 'administrator1'.

Add Security Role Dialog (Top):

- Role Name: klient1
- Description: (empty)
- Buttons: OK, Cancel

Add Security Role Dialog (Bottom):

- Role Name: administrator1
- Description: (empty)
- Buttons: OK, Cancel

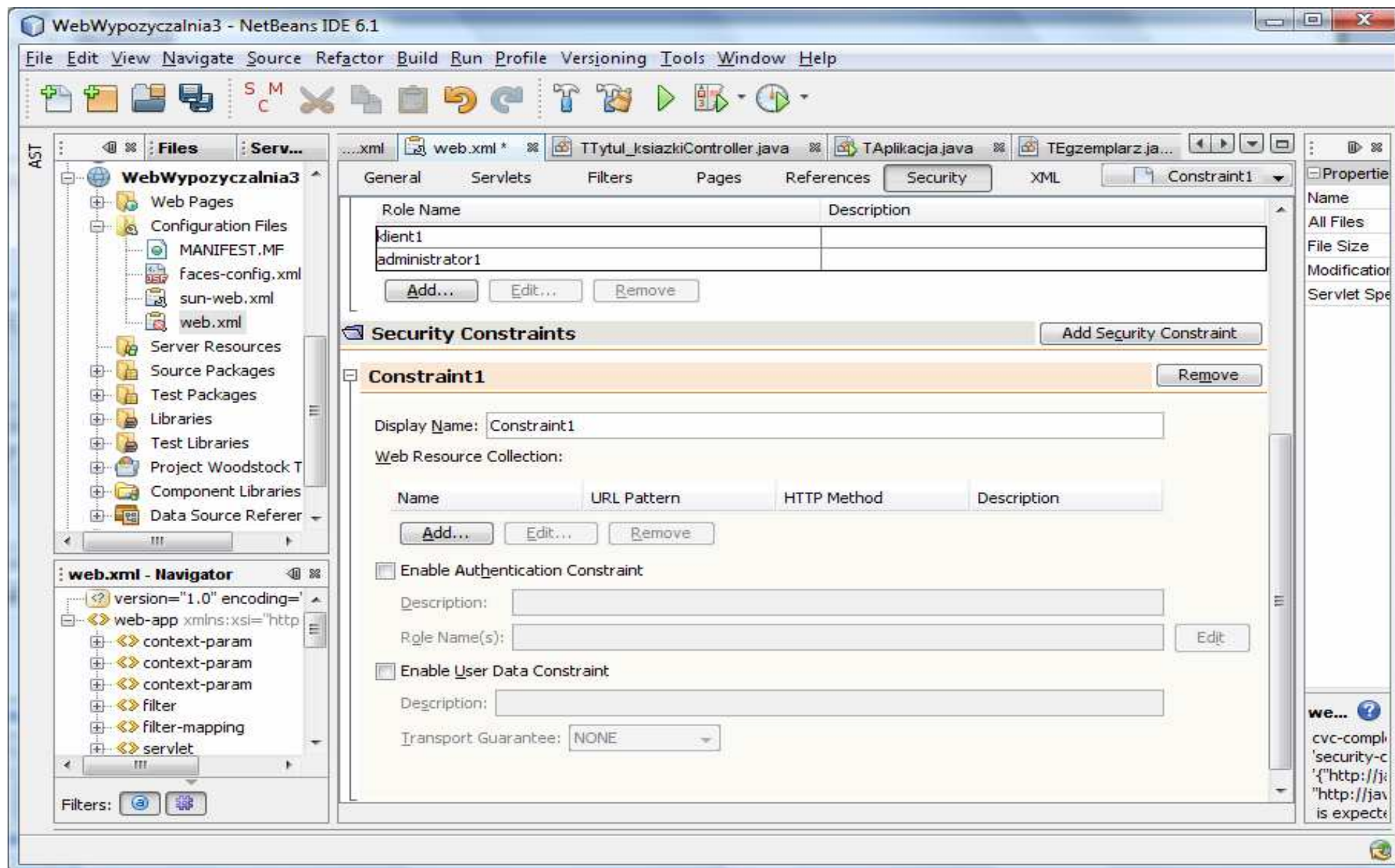
Main Window Security Configuration:

- Authentication: Basic
- Realm Name: file
- Form Login Page: /logon.jsp
- Form Error Page: /logonError.jsp

Security Roles Table:

Role Name	Description
klient1	
administrator1	

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*

The screenshot shows the NetBeans IDE 6.1 interface. The main window displays the 'Security' tab for the 'web.xml' file. The 'Security Constraints' section is expanded, showing a table with one entry, 'Constraint1'. The 'Display Name' field for this constraint is set to 'AdministratorConstraint'. Below the table, there are checkboxes for 'Enable Authentication Constraint' and 'Enable User Data Constraint', both of which are currently unchecked. The 'Transport Guarantee' is set to 'NONE'. The 'Web Resource Collection' table is empty. The 'Role Name' table at the top lists 'klient1' and 'administrator1'. The 'Files' pane on the left shows the project structure, and the 'web.xml - Navigator' pane shows the XML structure of the web application.

WebWypożyczalnia3 - NetBeans IDE 6.1

File Edit View Navigate Source Refactor Build Run Profile Versioning Tools Window Help

Files: WebWypożyczalnia3, Web Pages, Configuration Files, MANIFEST.MF, faces-config.xml, sun-web.xml, web.xml, Server Resources, Source Packages, Test Packages, Libraries, Test Libraries, Project Woodstock T, Component Libraries, Data Source Referer

web.xml - Navigator: version="1.0" encoding="UTF-8", web-app xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance", context-param, filter, filter-mapping, servlet

Security Constraints

Role Name	Description
klient1	
administrator1	

Constraint1

Display Name: AdministratorConstraint

Web Resource Collection:

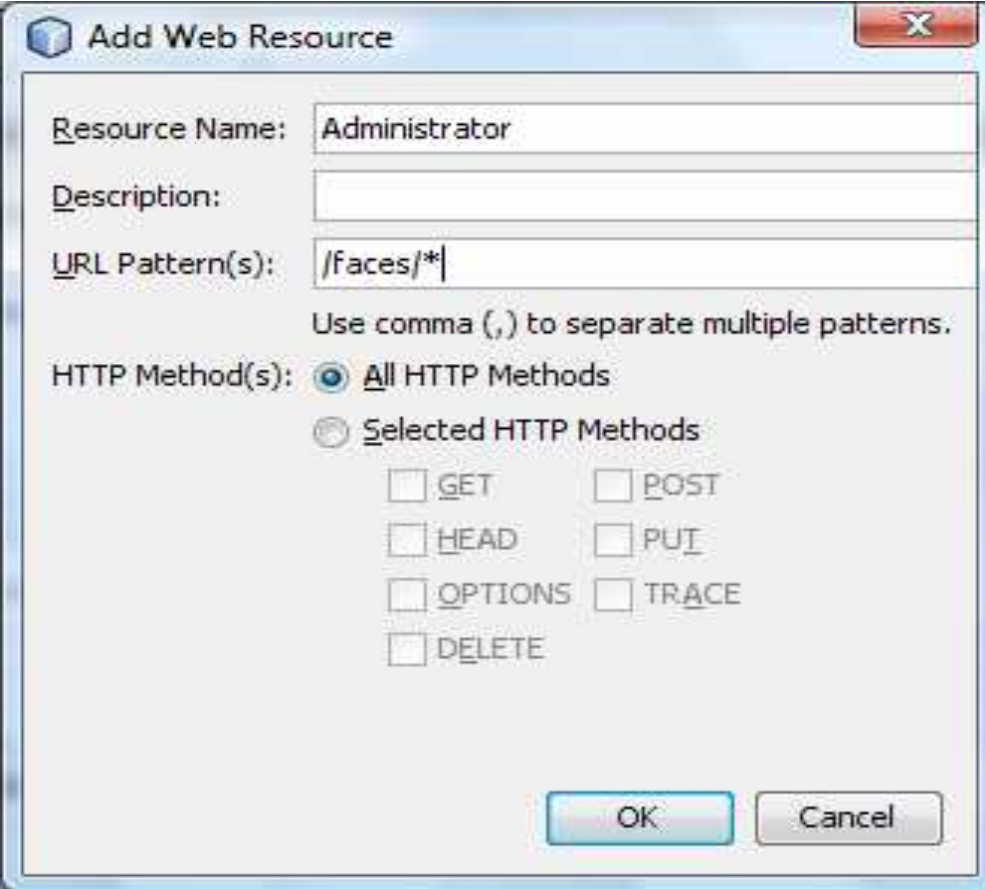
Name	URL Pattern	HTTP Method	Description
------	-------------	-------------	-------------

Enable Authentication Constraint

Enable User Data Constraint

Transport Guarantee: NONE

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

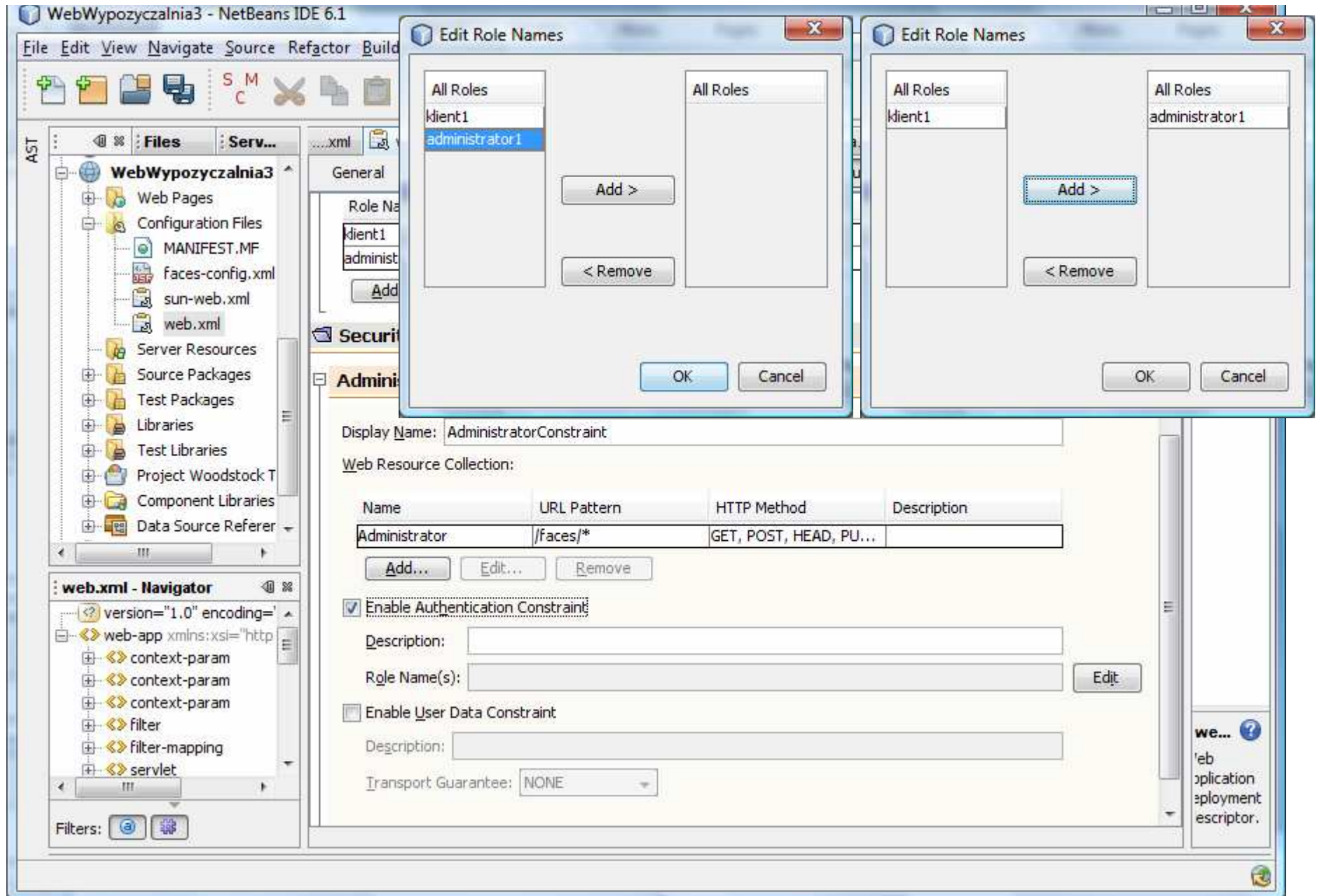


The screenshot shows a dialog box titled "Add Web Resource". It contains the following fields and options:

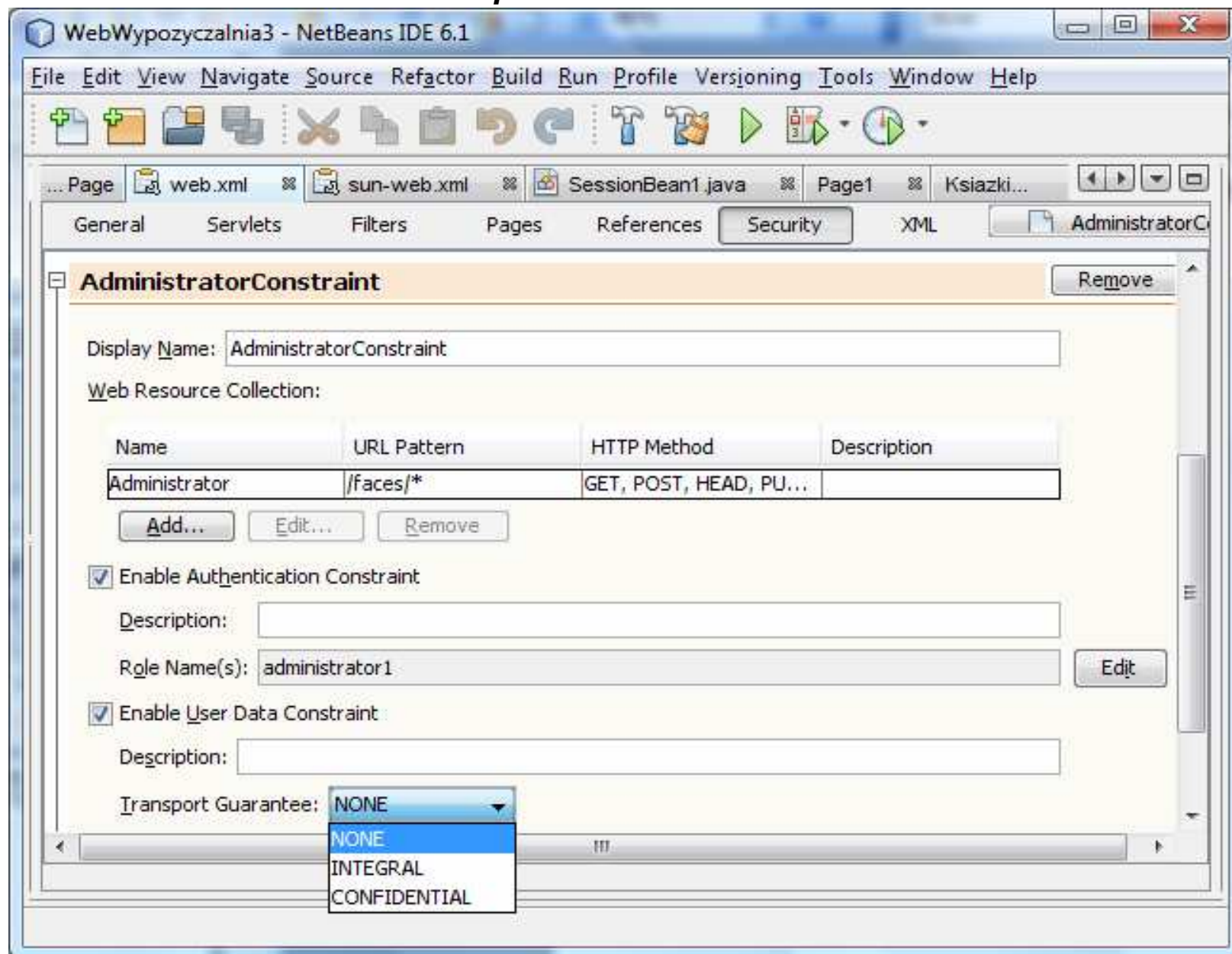
- Resource Name:** Administrator
- Description:** (empty field)
- URL Pattern(s):** /faces/*
- Use comma (,) to separate multiple patterns.**
- HTTP Method(s):**
 - All HTTP Methods
 - Selected HTTP Methods
 - GET
 - POST
 - HEAD
 - PUT
 - OPTIONS
 - TRACE
 - DELETE

At the bottom of the dialog are "OK" and "Cancel" buttons.

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

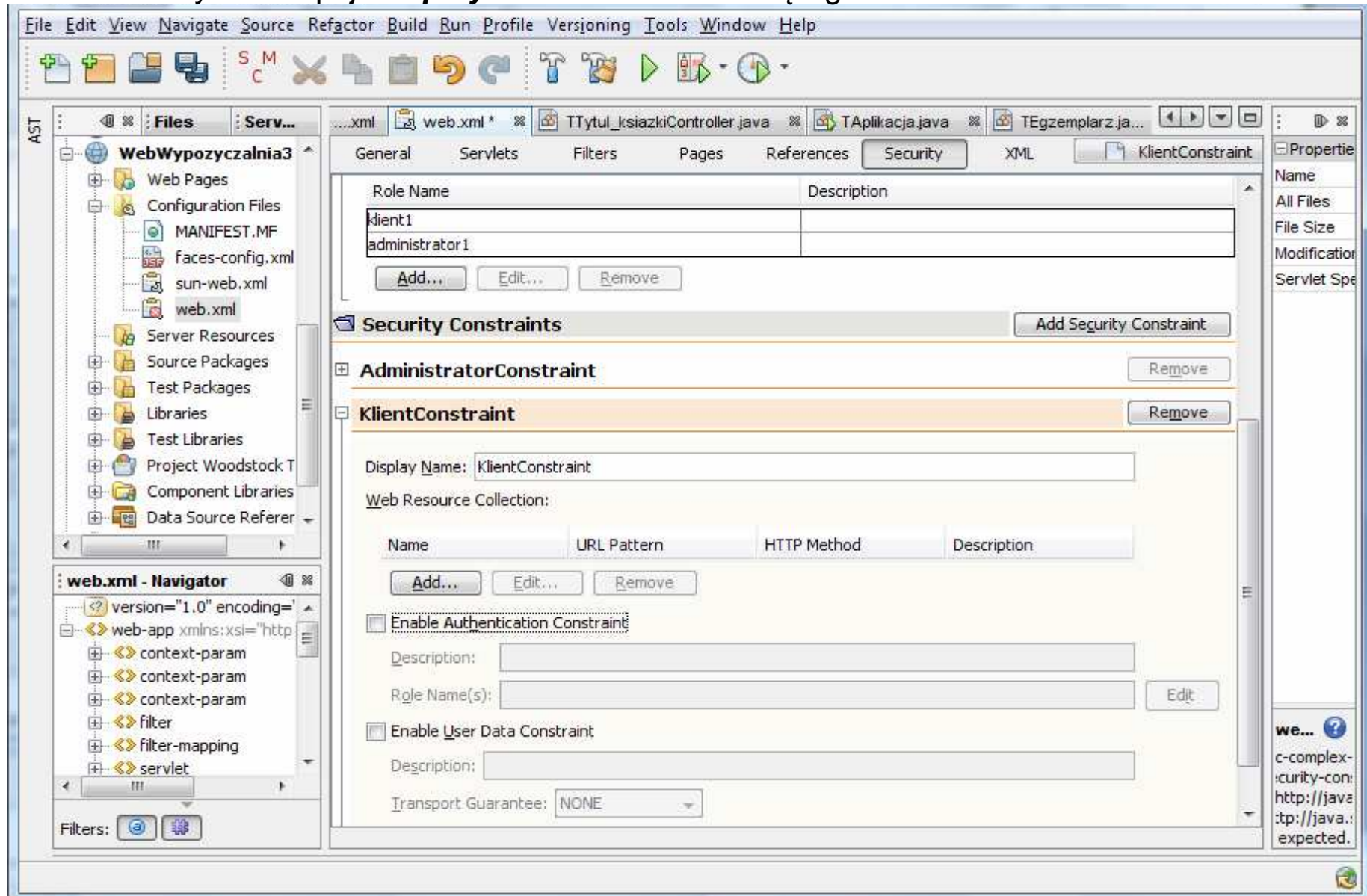


5.4. Przypisanie niezabezpieczonego protokołu transportu do ustawianych ograniczeń **AdministratorConstraint** za pomocą opcji **Enable User Data Constraint** i **Transport Guarantee = NONE**



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**

Edit Web Resource

Resource Name: Klient

Description:

URL Pattern(s): /faces/Page1.jsp, /faces/Tytuly.jsp, /faces/Ksiazki.jsp

Use comma (,) to separate multiple patterns.

HTTP Method(s): All HTTP Methods

Selectd HTTP Methods

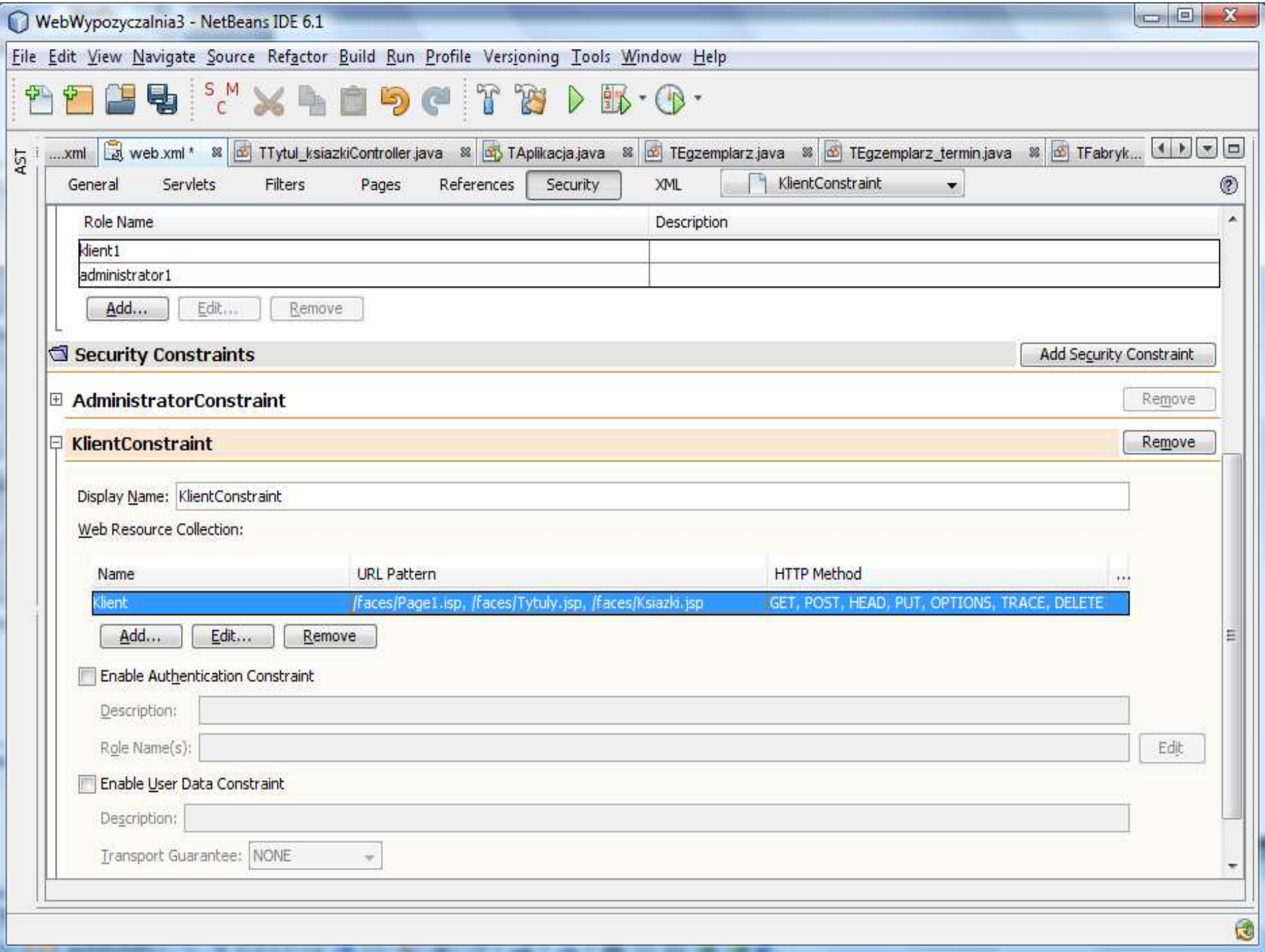
GET POST

HEAD PUT

OPTIONS TRACE

DELETE

OK Cancel



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

The screenshot illustrates the process of assigning the role 'klient1' to the 'KlientConstraint' security constraint. Two 'Edit Role Names' dialog boxes are shown, demonstrating the transfer of the role from the left pane to the right pane. The background IDE window shows the 'Security Constraints' configuration for 'KlientConstraint', where the 'Enable Authentication Constraint' checkbox is checked, and the 'Role Name(s)' field is set to 'klient1'.

Top Dialog: Edit Role Names

- Left pane: klient1, administrator1
- Right pane: All Roles
- Buttons: Add >, < Remove, OK, Cancel

Bottom Dialog: Edit Role Names

- Left pane: administrator1
- Right pane: klient1
- Buttons: Add >, < Remove, OK, Cancel

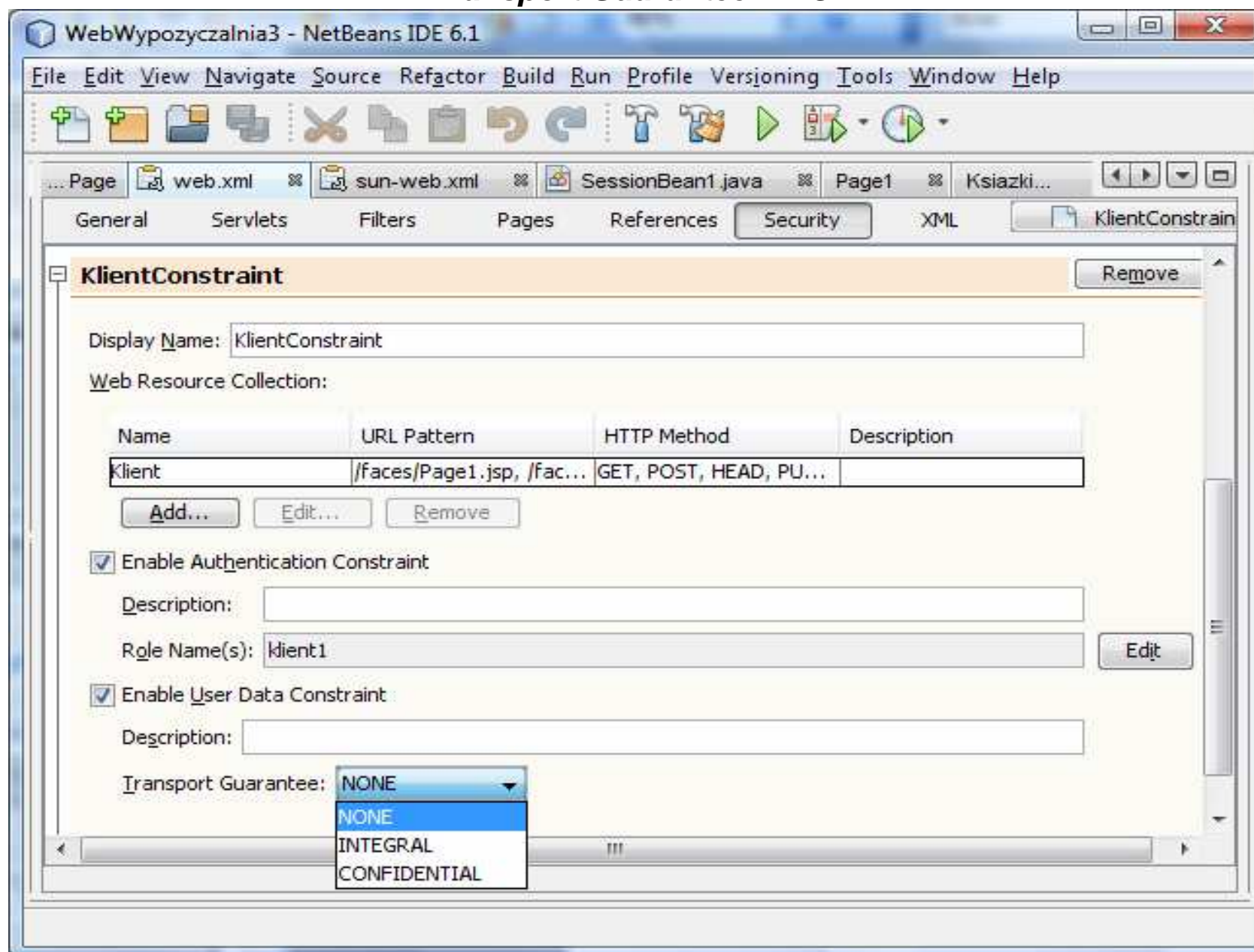
IDE Security Constraints Configuration

- Constraint: KlientConstraint
- Display Name: KlientConstraint
- Web Resource Collection:

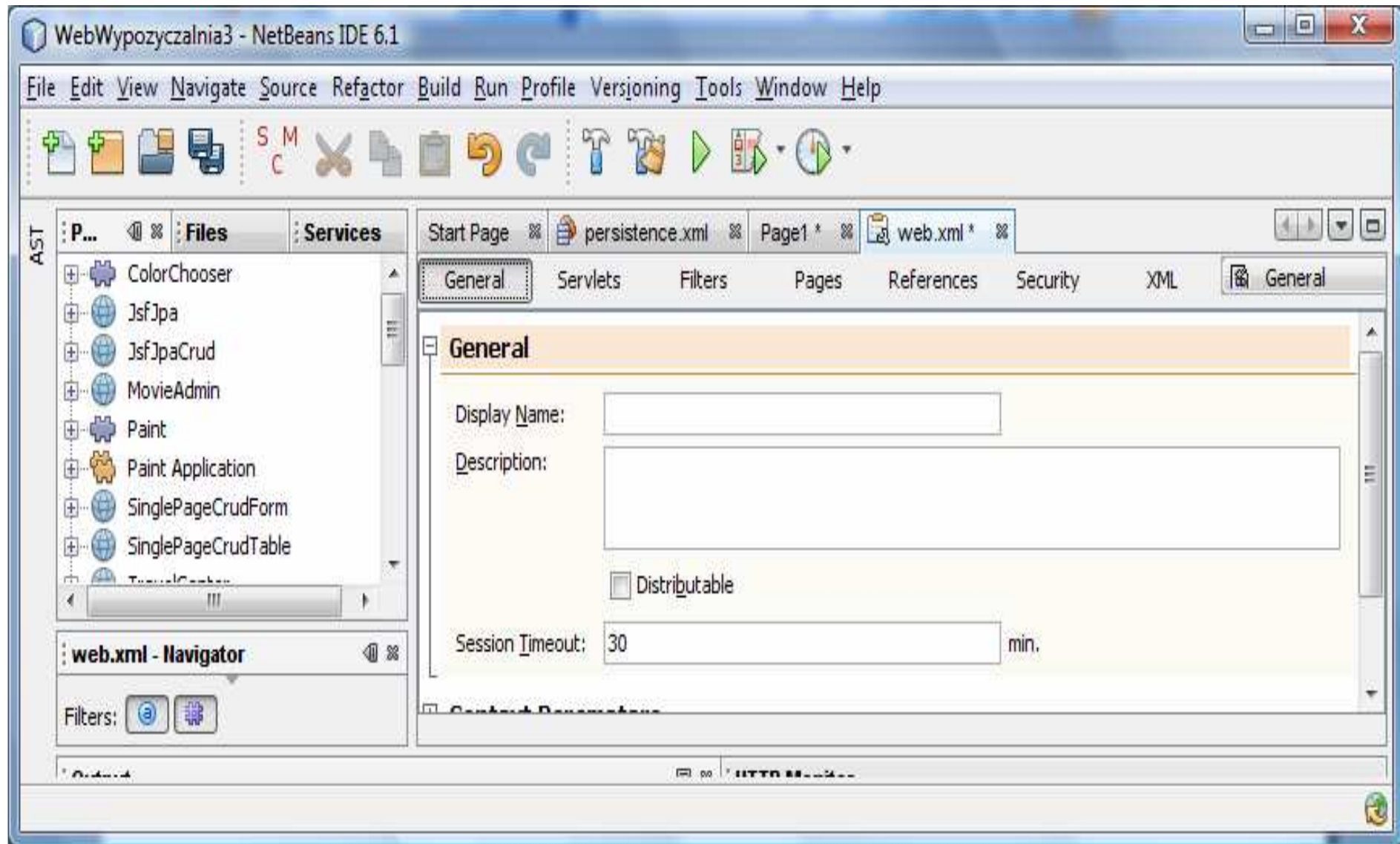
Name	URL Pattern	HTTP Method
klient	/faces/Page1.jsp, /fa...	GET, POST, HEAD, ...

- Enable Authentication Constraint
- Description:
- Role Name(s): klient1
- Enable User Data Constraint
- Description:
- Transport Guarantee: NONE

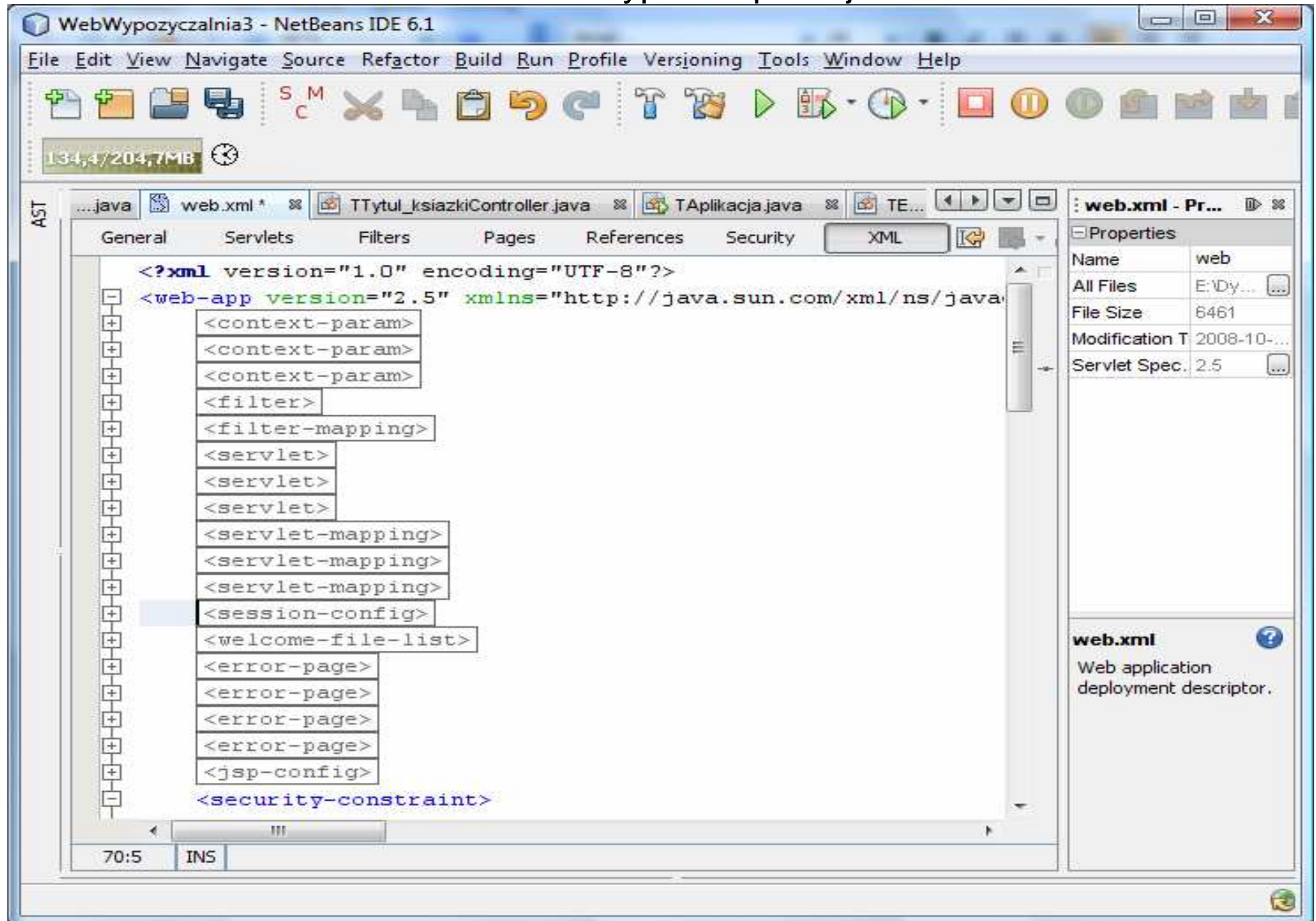
6.3. Przypisanie niezabezpieczonego protokołu transportu do ustawianych ograniczeń **KlientConstraint** za pomocą opcji **Enable User Data Constraint** i **Transport Guarantee = NONE**



7. Ustawienie czasu sesji



8. Zawartość deskryptora aplikacji *web.xml*



The screenshot shows the NetBeans IDE 6.1 interface. The main editor window displays the content of the `web.xml` file, which is a web application deployment descriptor. The code is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app version="2.5" xmlns="http://java.sun.com/xml/ns/java"
  <context-param>
  <context-param>
  <context-param>
  <filter>
  <filter-mapping>
  <servlet>
  <servlet>
  <servlet>
  <servlet-mapping>
  <servlet-mapping>
  <servlet-mapping>
  <session-config>
  <welcome-file-list>
  <error-page>
  <error-page>
  <error-page>
  <error-page>
  <jsp-config>
  <security-constraint>
```

The right sidebar shows the Properties window for the `web.xml` file. The Properties window displays the following information:

Properties	
Name	web
All Files	E:\Dy...
File Size	6461
Modification T	2008-10-...
Servlet Spec.	2.5

Below the Properties window, there is a description of the file:

web.xml
Web application deployment descriptor.



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



Start Page web.xml * sun-web.xml

General

Servlets

Filters

Pages

References

Security

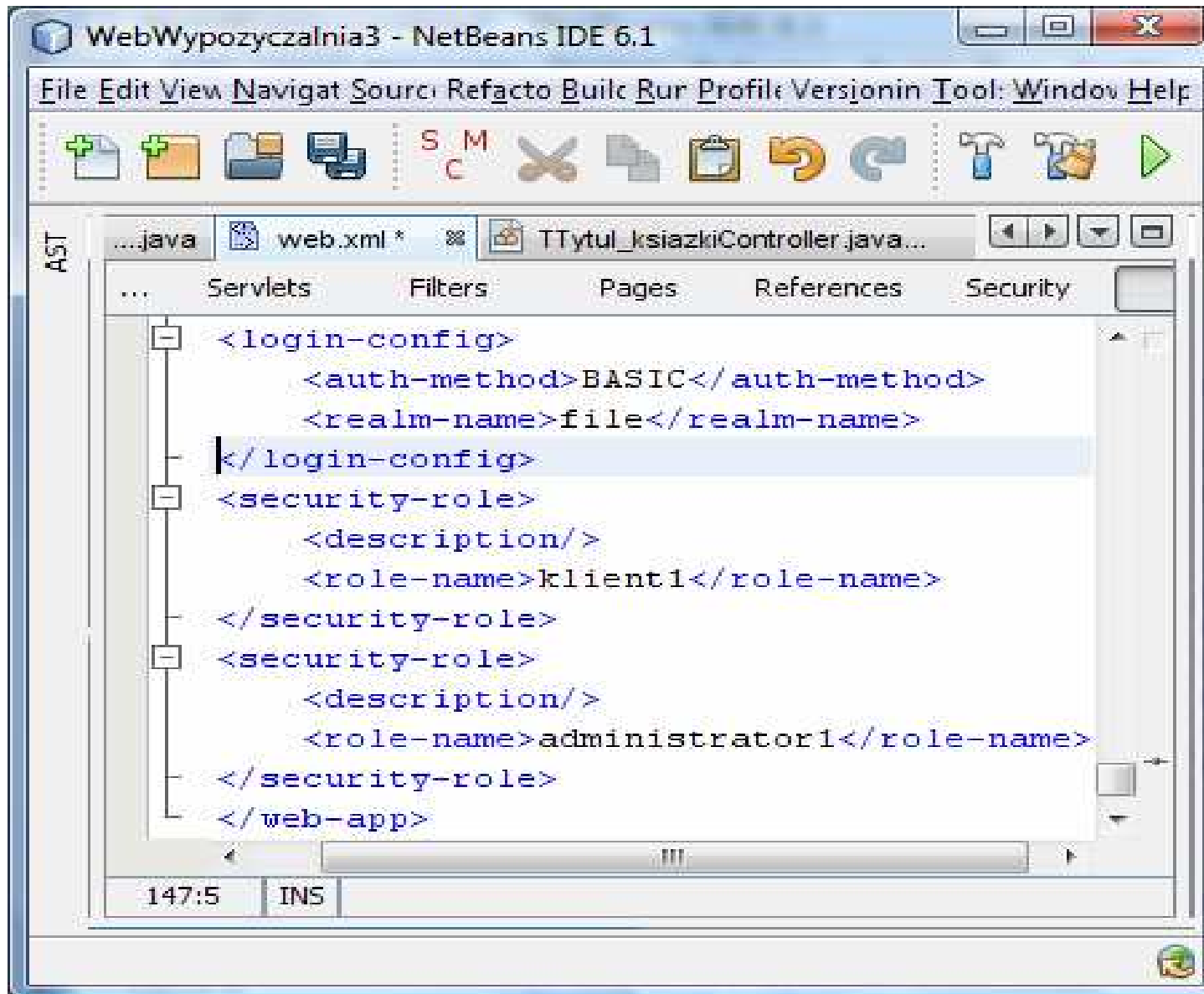
XML

```
<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

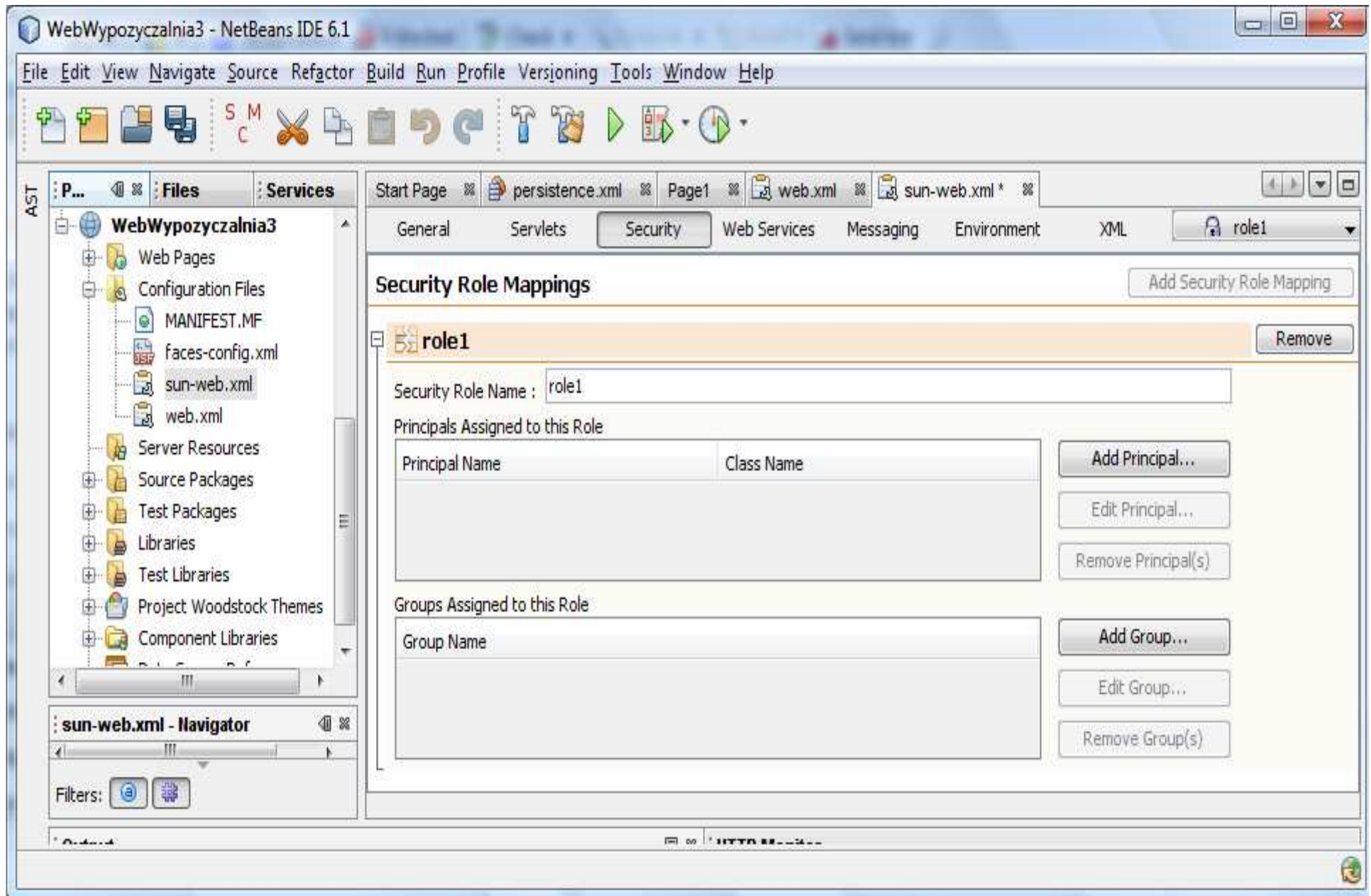


The screenshot shows the NetBeans IDE 6.1 interface. The main window displays the AST (Abstract Syntax Tree) view of a web.xml file. The code defines a login configuration and two security roles:

```
<login-config>
  <auth-method>BASIC</auth-method>
  <realm-name>file</realm-name>
</login-config>
<security-role>
  <description/>
  <role-name>klient1</role-name>
</security-role>
<security-role>
  <description/>
  <role-name>administrator1</role-name>
</security-role>
</web-app>
```

The status bar at the bottom indicates the cursor is at line 147, column 5, with the text "INS" displayed.

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**

The screenshot displays an IDE interface with the 'Security Role Mappings' configuration for the 'administrator1' role. The 'Add Principal' dialog box is open, showing the 'Principal Name' field set to 'administrator' and the 'Class Name' field empty. The 'Security Role Mappings' panel shows the 'administrator1' role with a table of principals assigned to it:

Principal Name	Class Name
administrator	

The 'Add Principal...' button is highlighted. The 'Groups Assigned to this Role' section is empty. The 'Run Main Project (F6)' tooltip is visible over the IDE's toolbar.

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

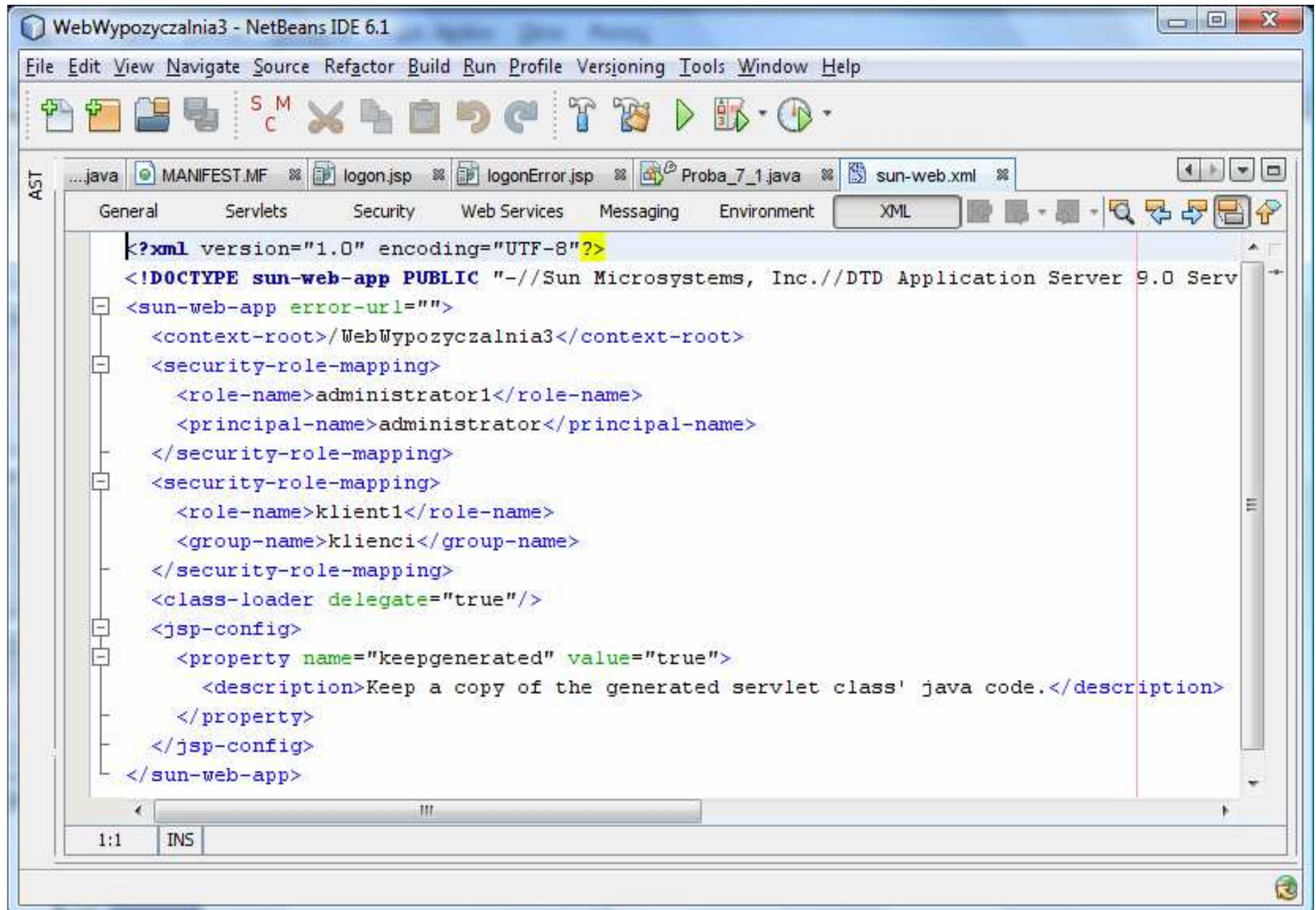
The screenshot shows the NetBeans IDE 6.1 interface. The main window is titled "WebWypożyczalnia3 - NetBeans IDE 6.1". The menu bar includes "File", "Edit", "View", "Navigate", "Source", "Refactor", "Build", "Run", "Profile", "Version", "Tools", "Window", and "Help". The toolbar contains various icons for file operations and development actions. The main editor area shows several tabs: "...xml", "sun-web.xml", and "faces-config.xml...". The "Security" tab is selected, displaying the "Security Role Mappings" configuration.

The "Security Role Mappings" panel shows two roles: "administrator1" and "klient1". The "klient1" role is selected. Below the role list, the "Security Role Name" is set to "klient1". The "Principals Assigned to this Role" section contains a table with columns "Principal Name" and "Class Name", and buttons for "Add Principal...", "Edit Principal...", and "Remove Principal(s)". The "Groups Assigned to this Role" section contains a table with a column "Group Name", where "kienci" is selected. Buttons for "Add Group...", "Edit Group...", and "Remove Group(s)" are visible.

The "Add Group" dialog is open in the foreground. It prompts the user to "Enter the new group name here :". The "Group Name" field contains "kienci". Below this, it says "Or select a previously entered group name from the table below :". A table with a "Group Name" column is shown, but it is empty. At the bottom of the dialog are "OK", "Cancel", and "Help" buttons.

At the bottom of the IDE window, a status bar displays "Save All finished." and a small icon.

9.3. Zawartość deskryptora serwera aplikacji




The screenshot displays the NetBeans IDE 6.1 interface. The title bar reads "WebWypożyczalnia3 - NetBeans IDE 6.1". The menu bar includes "File", "Edit", "View", "Navigate", "Source", "Refactor", "Build", "Run", "Profile", "Versioning", "Tools", "Window", and "Help". The toolbar contains various icons for file operations and development. The main editor window shows the "sun-web.xml" file with the following XML content:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE sun-web-app PUBLIC "-//Sun Microsystems, Inc.//DTD Application Server 9.0 Serv
<sun-web-app error-url="">
  <context-root>/WebWypożyczalnia3</context-root>
  <security-role-mapping>
    <role-name>administrator1</role-name>
    <principal-name>administrator</principal-name>
  </security-role-mapping>
  <security-role-mapping>
    <role-name>klient1</role-name>
    <group-name>klienci</group-name>
  </security-role-mapping>
  <class-loader delegate="true"/>
  <jsp-config>
    <property name="keepgenerated" value="true">
      <description>Keep a copy of the generated servlet class' java code.</description>
    </property>
  </jsp-config>
</sun-web-app>
```

The status bar at the bottom shows "1:1" and "INS".


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

Łączenie z localhost



Serwer localhost w lokalizacji file wymaga nazwy użytkownika i hasła.

Ostrzeżenie: ten serwer żąda wysłania Twojej nazwy użytkownika i hasła w niezabezpieczony sposób (podstawowe uwierzytelnienie bez bezpiecznego połączenia).


Nazwa użytkownika:  administrator

Hasło:

Zapamiętaj moje hasło


OK Anuluj

Łączenie z localhost



Serwer localhost w lokalizacji file wymaga nazwy użytkownika i hasła.

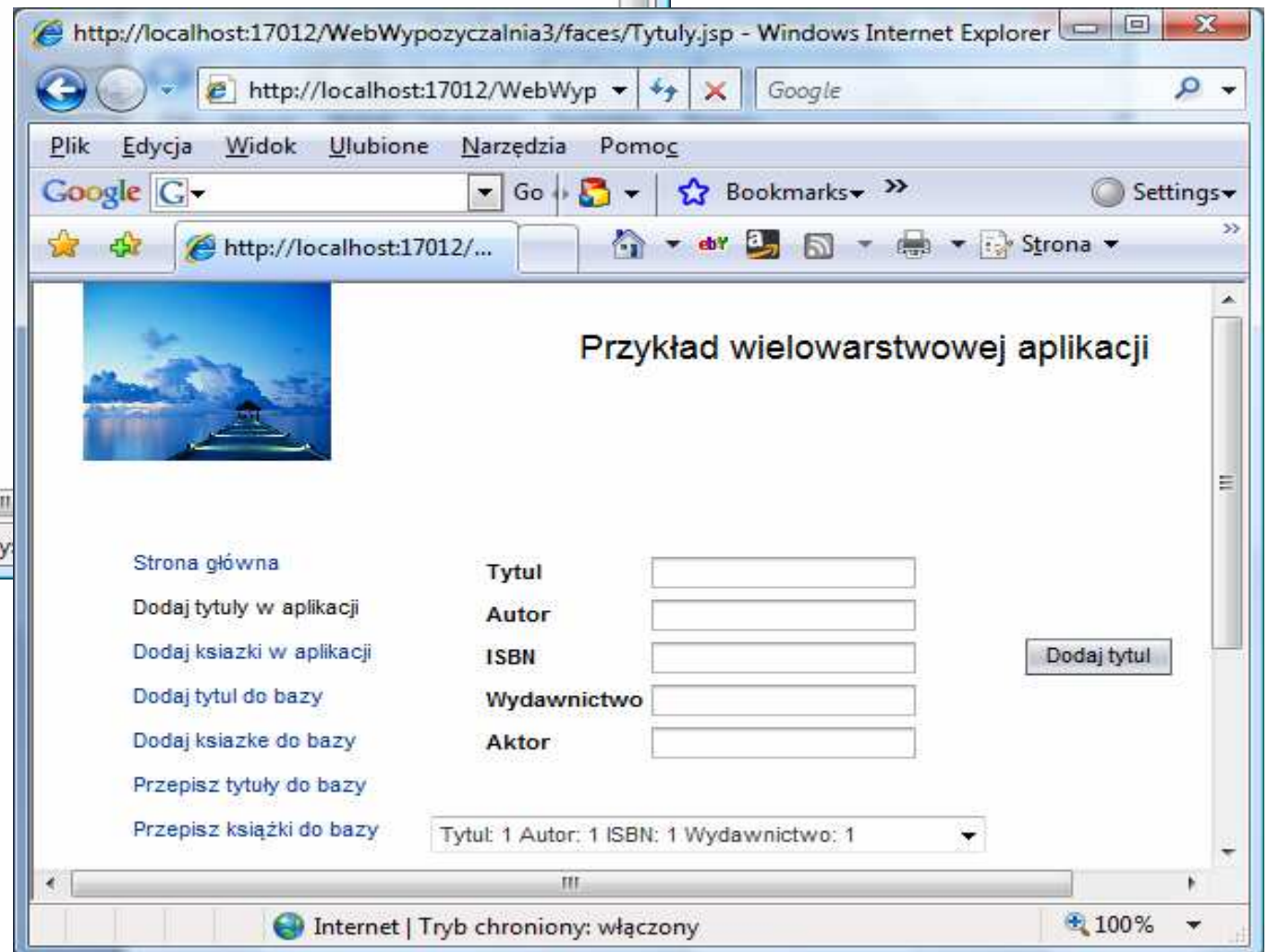
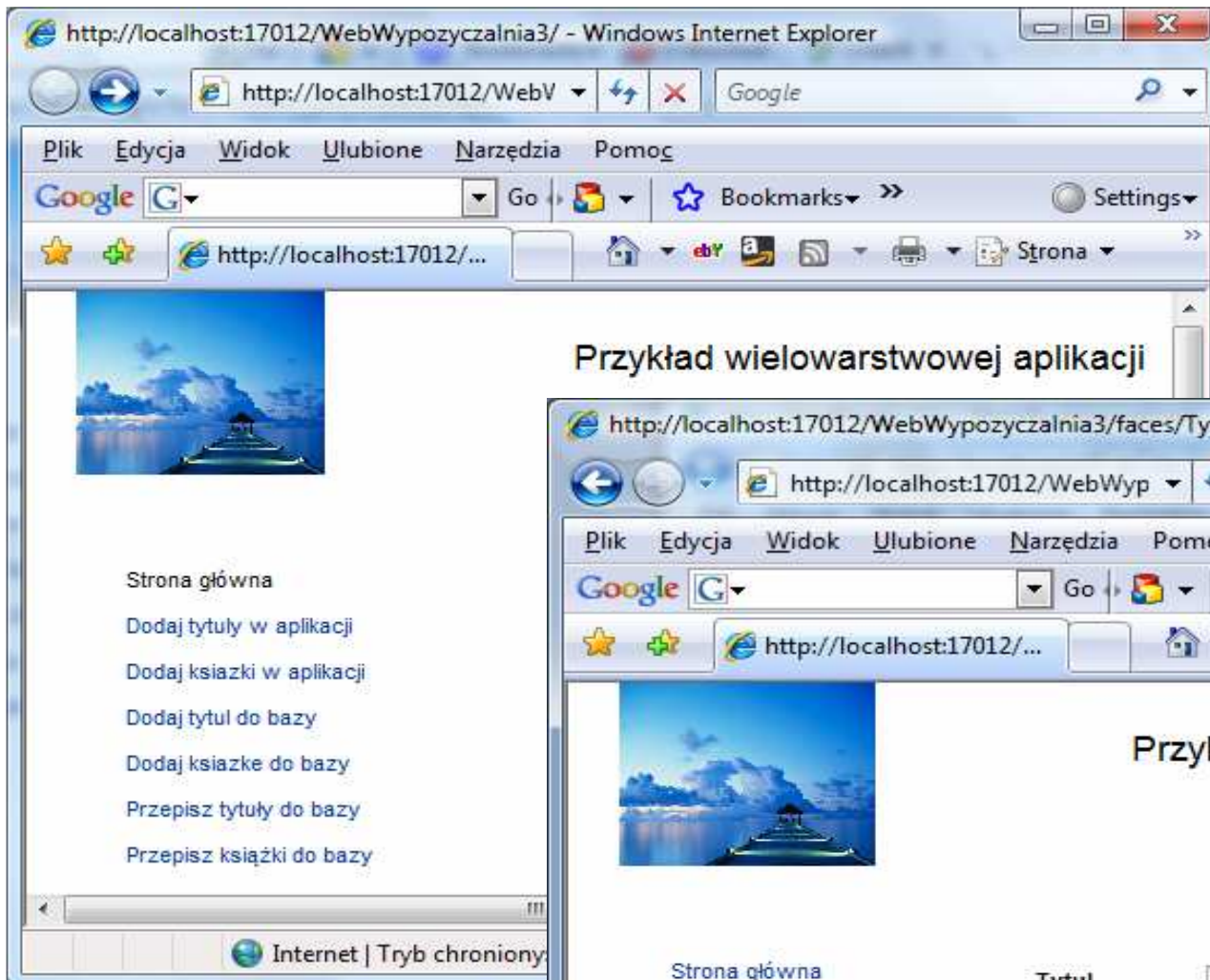
Ostrzeżenie: ten serwer żąda wysłania Twojej nazwy użytkownika i hasła w niezabezpieczony sposób (podstawowe uwierzytelnienie bez bezpiecznego połączenia).

Nazwa użytkownika:  klient

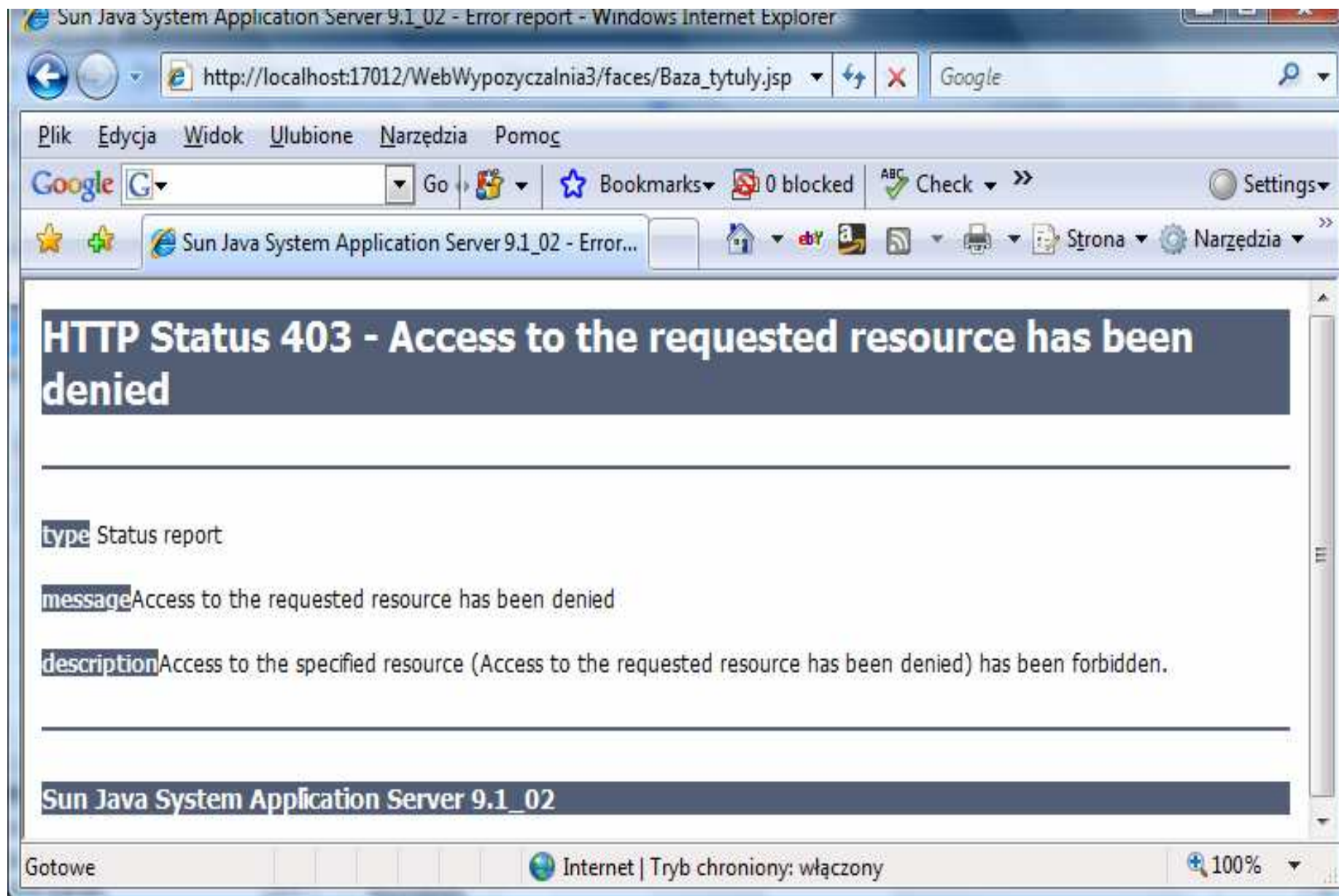
Hasło:

Zapamiętaj moje hasło

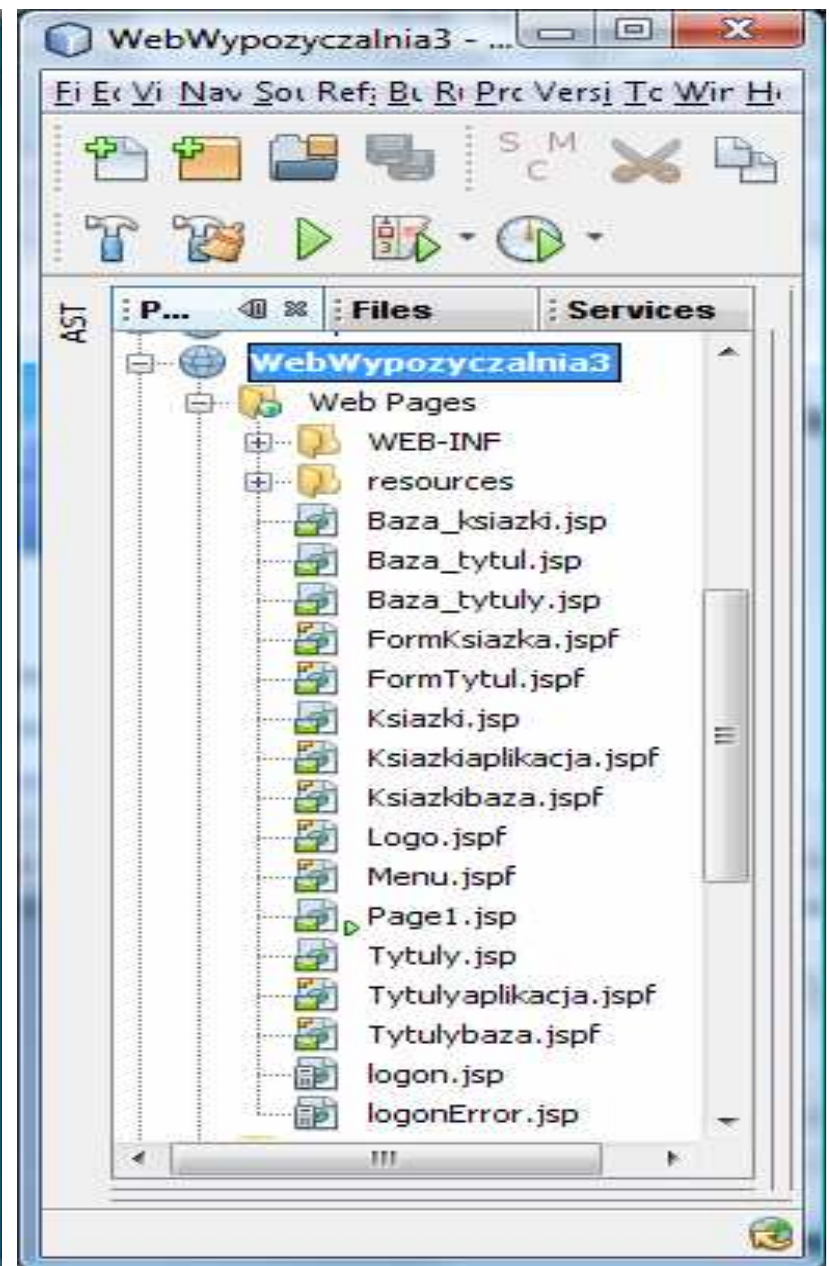
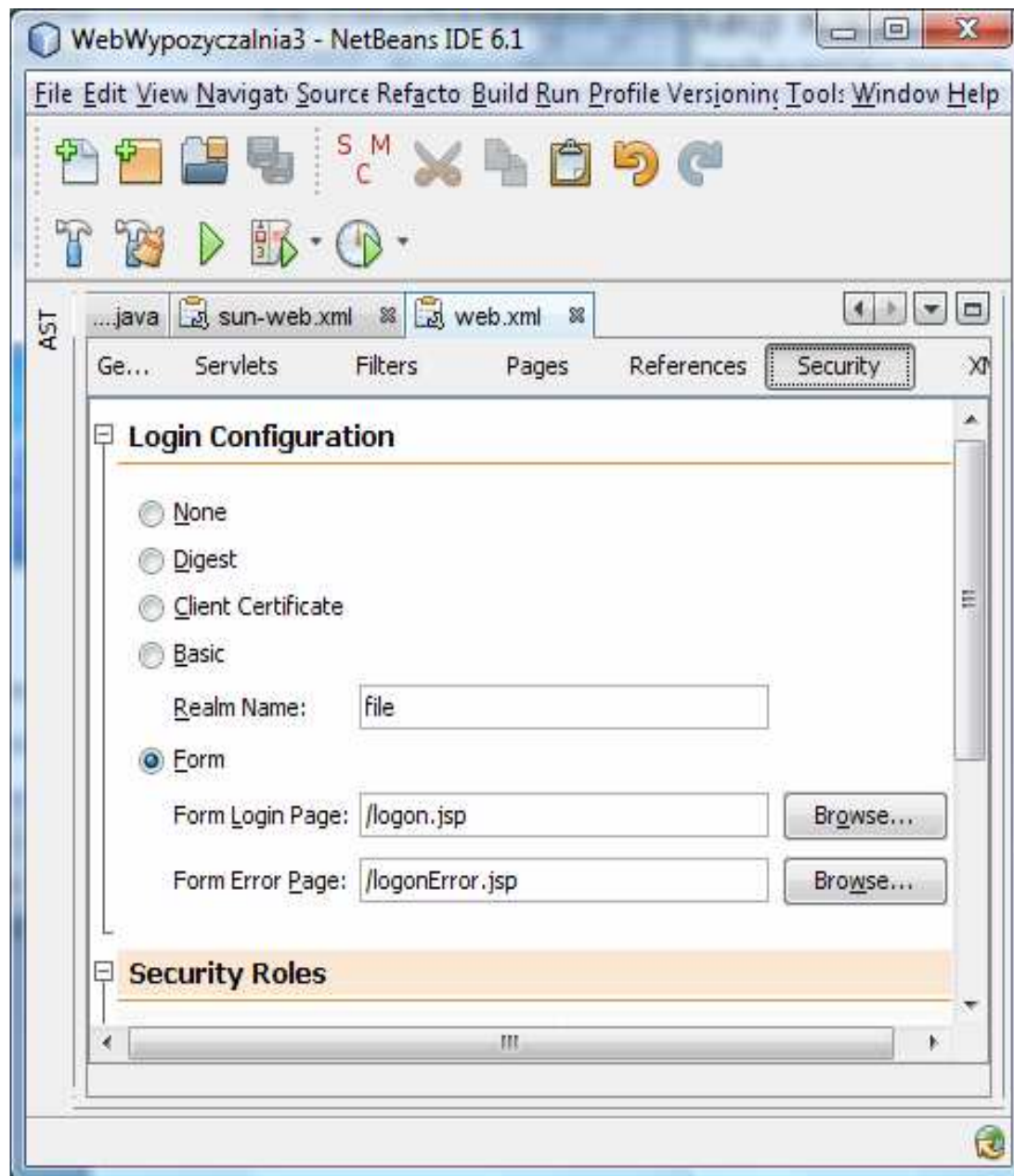
OK Anuluj



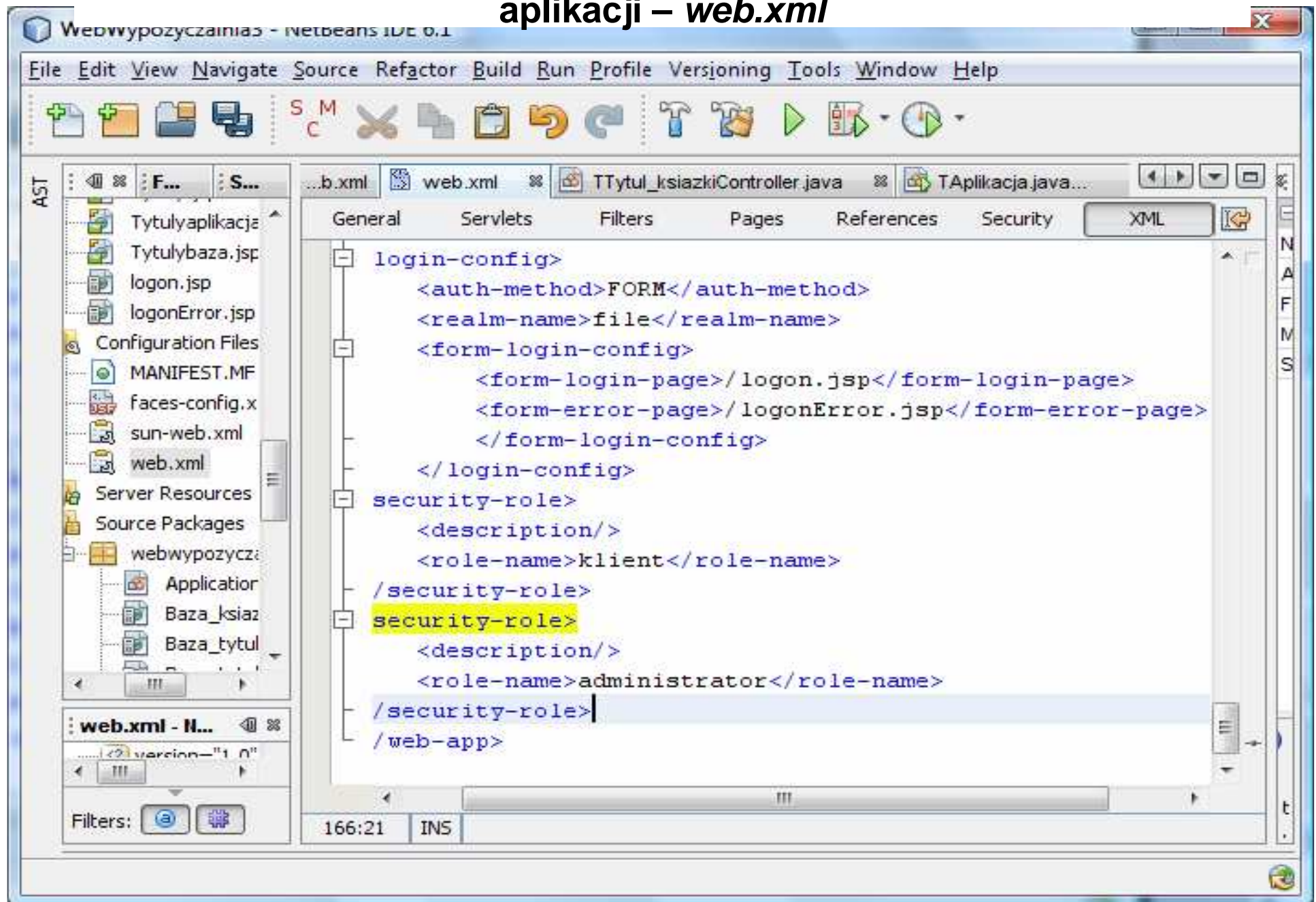
Niedostępne strony dla użytkownika „klient” występującego w roli „klient1”
(objęte ograniczeniem **Web Resource Collection**)



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



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



The screenshot shows the NetBeans IDE interface with the `web.xml` file open in XML view. The file is part of a web application project named "Webwypożyczalnia". The XML content is as follows:

```
<?xml version="1.0" encoding="UTF-8" ?>
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
    http://xmlns.jcp.org/xml/ns/javaee/web-app_3_0.xsd"
  version="3.0">
  <login-config>
    <auth-method>FORM</auth-method>
    <realm-name>file</realm-name>
    <form-login-config>
      <form-login-page>/logon.jsp</form-login-page>
      <form-error-page>/logonError.jsp</form-error-page>
    </form-login-config>
  </login-config>
  <security-role>
    <description/>
    <role-name>klient</role-name>
  </security-role>
  <security-role>
    <description/>
    <role-name>administrator</role-name>
  </security-role>
</web-app>
```

The IDE interface includes a menu bar (File, Edit, View, Navigate, Source, Refactor, Build, Run, Profile, Versioning, Tools, Window, Help), a toolbar with various icons, and a project explorer on the left showing the file structure. The XML view is currently selected, and the status bar at the bottom indicates the cursor is at line 166, column 21 in insert mode.

10.2. Zawartość formularza logowania

The screenshot shows an IDE window with the following components:

- File Explorer:** Shows a project structure with files like `logon.jsp`, `logonError.jsp`, `Configuration Files`, `MANIFEST.MF`, `faces-config.xml`, and `sun-web.xml`.
- logon.jsp - Navigator:** A tree view showing the DOM structure of the page, including `html`, `head`, `title`, `h2`, `br`, `form`, `p`, `strong`, and `input` elements.
- Main Editor:** Displays the source code of `logon.jsp`. The code includes a copyright notice in French and an HTML form for user login.

```
*
* Cette distribution peut comprendre des composants developpes par de
* tierces parties. Sun, Sun Microsystems, le logo Sun, Java et J2EE
* sont des marques de fabrique ou des marques deposees de Sun
* Microsystems, Inc. aux Etats-Unis et dans d'autres pays.
*!
-->
<%@ taglib uri="http://java.sun.com/jsp/jstl/core" prefix="c" %>
<%@ taglib uri="http://java.sun.com/jsp/jstl/functions" prefix="fn" %>
<html>
<head><title>Login Page</title></head>

<h2>Logowanie do systemu:</h2>
<br><br><form action="j_security_check" method=post>
<p><strong>Nazwa uzytkownika: </strong>
<input type="text" name="j_username" size="25">
<p><p><strong>Haslo: </strong>
<input type="password" size="15" name="j_password">
<p><p>
<input type="submit" value="Submit">
<input type="reset" value="Reset">
</form>
</html>
```

33:8 INS

Save All finished.

10.3. Zawartość okna obsługi błędu logowania

The screenshot displays the NetBeans IDE 6.1 interface. The title bar reads "WebWypożyczalnia3 - NetBeans IDE 6.1". The menu bar includes "File", "Edit", "View", "Navigate", "Source", "Refactor", "Build", "Run", "Profile", "Versioning", "Tools", "Window", and "Help". The toolbar contains various icons for file operations and development tools. The status bar at the top shows "183,8/204,7MB".

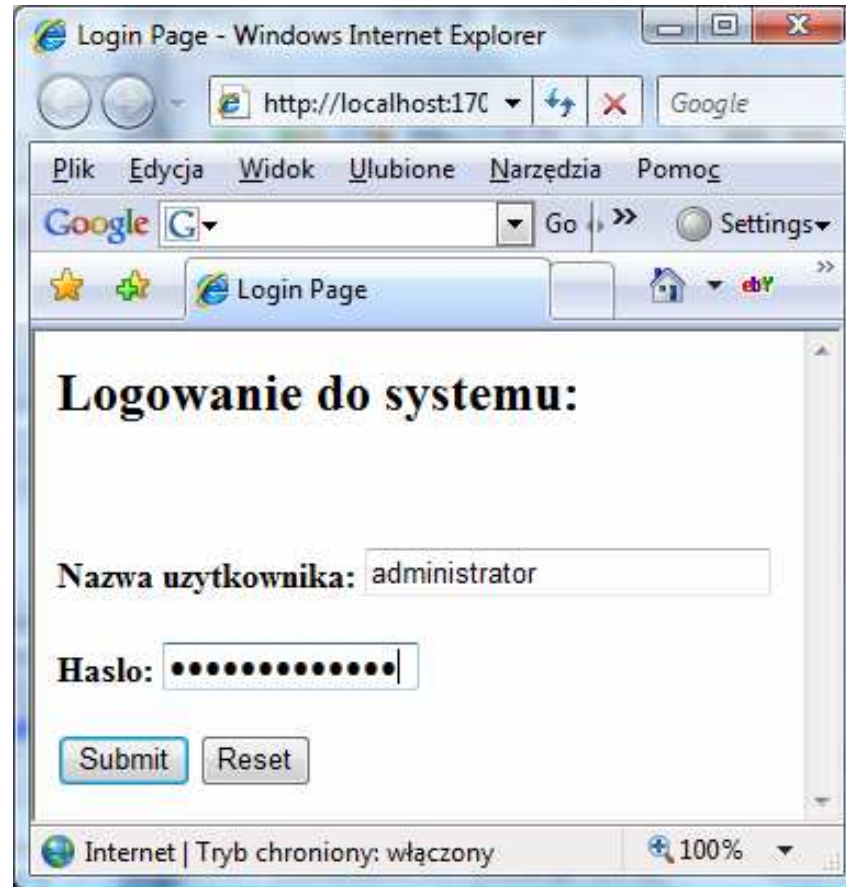
The left sidebar shows the "Files" view with a project tree containing files like Logo.jspf, Menu.jspf, Page1.jsp, Tytuly.jsp, Tytulyaplikacja.jspf, Tytulybaza.jspf, logon.jsp, and logonError.jsp. The "logonError.jsp" file is selected. Below it, the "logonError.jsp - Navigator" view shows a tree structure of the document: html > head > title > body > h2 > p > code > em > code > h2 > a.

The main editor window shows the source code of logonError.jsp. The code is as follows:

```
<%@ taglib uri="http://java.sun.com/jsp/jstl/core" prefix="c" %>
<html>
<head>
<title>
    Login Error
</title>
</head>
<body>
<c:url var="url" value="/index.jsp"/>
<h2>Invalid user name or password.</h2>
<p>Please enter a user name or password that
is authorized to access this application.
For this application, this means a user has been
created in the <code>file</code> realm and
has been assigned to the <em>group</em> of <code>user</code>.
Click here to</p>
<h2><a href="{url}">Try Again</a></h2>
</body>
</html>
```

The status bar at the bottom indicates the cursor is at line 35, column 8, in the "INS" (Insert) mode.

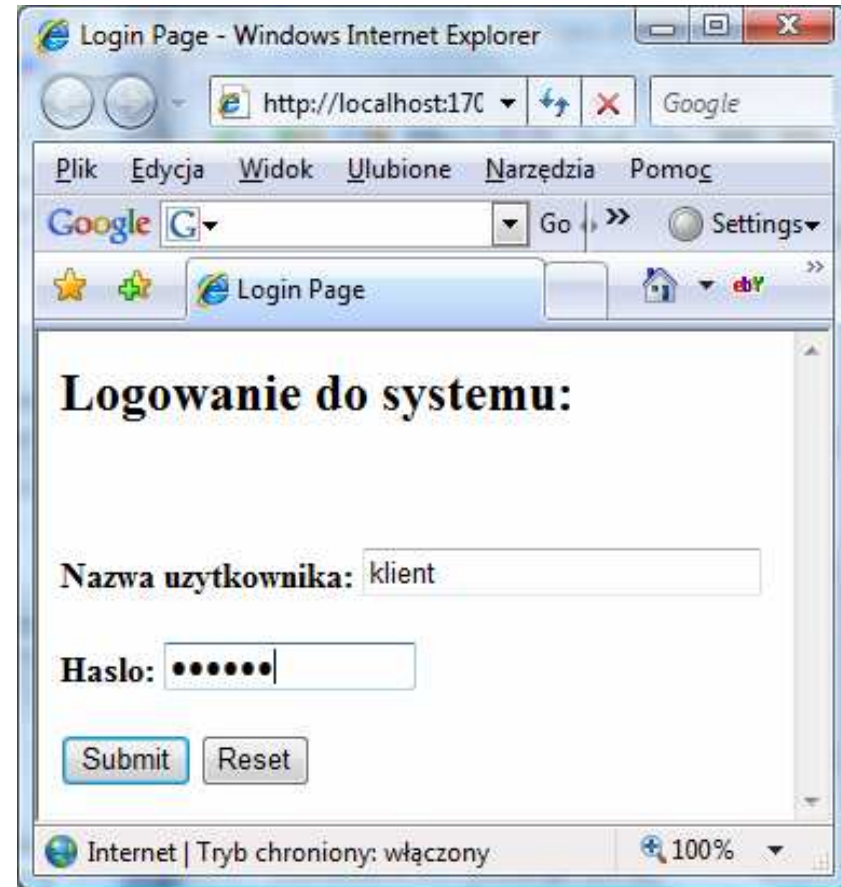
10.4. Uruchomienie aplikacji w trybie uwierzytelniania **Form**, zabezpieczenia przez role



Windows Internet Explorer window titled "Login Page". The address bar shows "http://localhost:170". The page content includes the heading "Logowanie do systemu:" and a form with the following fields and buttons:

- Nazwa użytkownika: administrator
- Haslo: [masked]
- Submit
- Reset

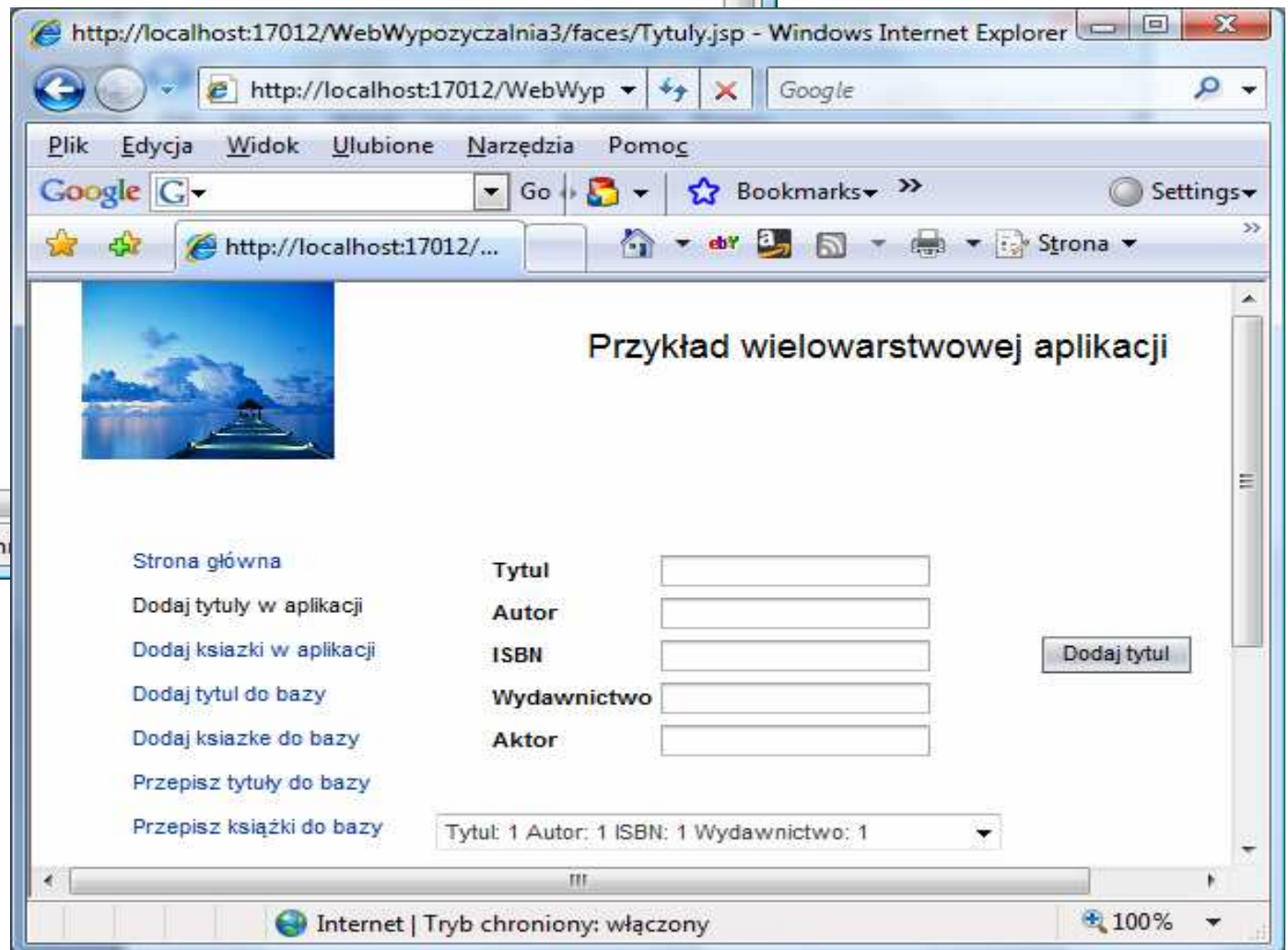
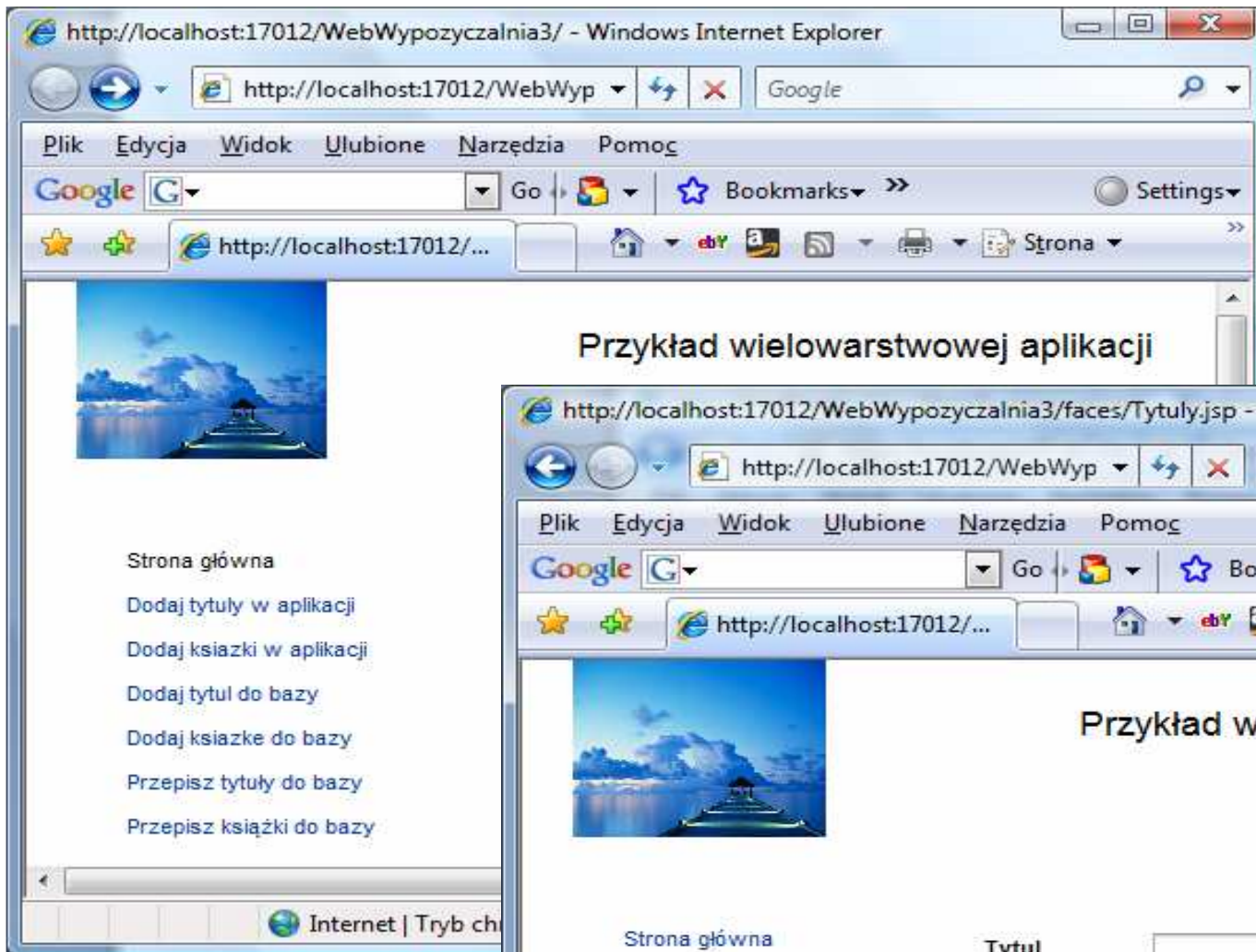
The status bar at the bottom indicates "Internet | Tryb chroniony: włączony" and "100%".



Windows Internet Explorer window titled "Login Page". The address bar shows "http://localhost:170". The page content includes the heading "Logowanie do systemu:" and a form with the following fields and buttons:

- Nazwa użytkownika: klient
- Haslo: [masked]
- Submit
- Reset

The status bar at the bottom indicates "Internet | Tryb chroniony: włączony" and "100%".



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

