

Министерство науки и образования РФ  
Федеральное государственное автономное образовательное  
учреждение высшего профессионального образования  
«Санкт-Петербургский государственный электротехнический  
университет «ЛЭТИ» им. В. И. Ульянова (Ленина)»  
(СПбГЭТУ «ЛЭТИ»)

Факультет компьютерных технологий и информатики

Кафедра вычислительной техники

**Отчёт по лабораторной работе № 5  
на тему: “ Аутентификация и авторизация  
пользователей web-приложения”  
по дисциплине  
“Web-программирование”**

Выполнили студенты гр.9308:

Дементьев Д.П.

Проверил:

Павловский М.Г.

Санкт-Петербург, 2021 г.

## Оглавление

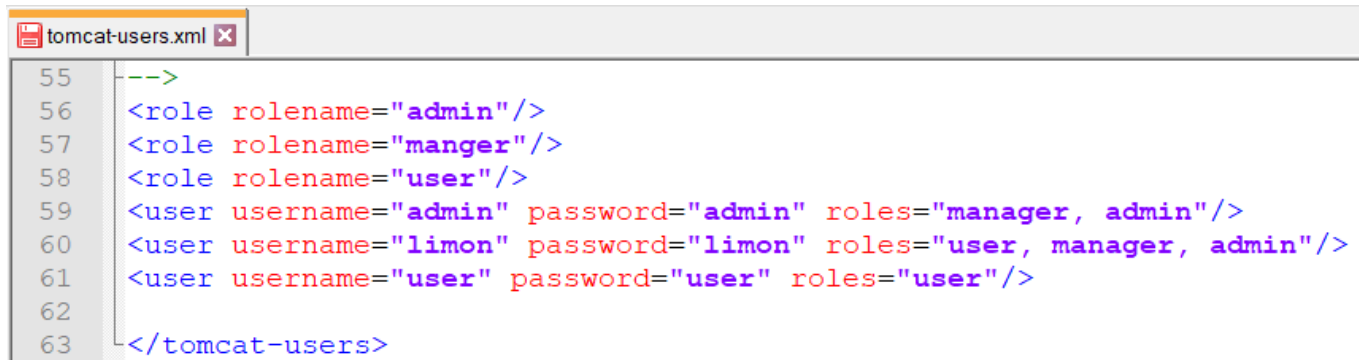
Введение .....	3
Настройка базовой аутентификации .....	3
SSL аутентификация .....	5
Вывод.....	7
Приложение 1. tomcat-users.xml.....	8
Приложение 2. server.xml .....	8
Приложение 3. web.xml .....	8

## Введение

Целью работы является знакомство со способами реализации аутентификации и авторизации пользователей Web-приложения.

### Настройка базовой аутентификации

Для начала необходимо добавить роли и пользователей в файл сервера Tomcat tomcat-users.xml:



```
55  <!-->
56  <role rolename="admin"/>
57  <role rolename="manager"/>
58  <role rolename="user"/>
59  <user username="admin" password="admin" roles="manager, admin"/>
60  <user username="limon" password="limon" roles="user, manager, admin"/>
61  <user username="user" password="user" roles="user"/>
62
63  </tomcat-users>
```

Рис.1. Файл tomcat-users.xml

Далее требуется изменить web.xml проекта. Попробуем ограничить доступ к главной странице: допустимыми ролями установим только «admin» и «manager». Фрагмент web.xml, отвечающий за настройку авторизации, приведён ниже:

```
<!-- Добавление авторизации пользователей -->
<security-role>
  <role-name>admin</role-name>
</security-role>

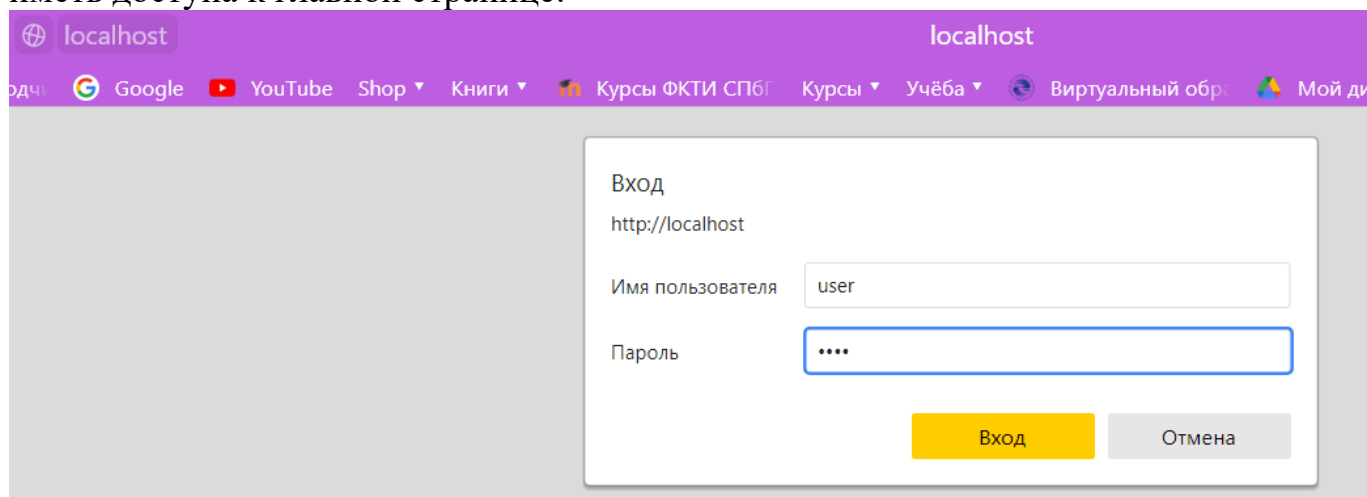
<security-role>
  <role-name>manager</role-name>
</security-role>

<security-role>
  <role-name>user</role-name>
</security-role>

<security-constraint>
  <web-resource-collection>
    <web-resource-name></web-resource-name>
    <url-pattern></url-pattern>
    <http-method>GET</http-method>
    <http-method>POST</http-method>
  </web-resource-collection>
  <auth-constraint>
    <role-name>admin</role-name>
    <role-name>manager</role-name>
  </auth-constraint>
</security-constraint>

<login-config>
  <auth-method>BASIC</auth-method>
  <realm-name>Write Post List</realm-name>
</login-config>
```

Теперь можем попробовать авторизоваться за пользователя user, который не должен иметь доступа к главной странице:



localhost

Вход

http://localhost

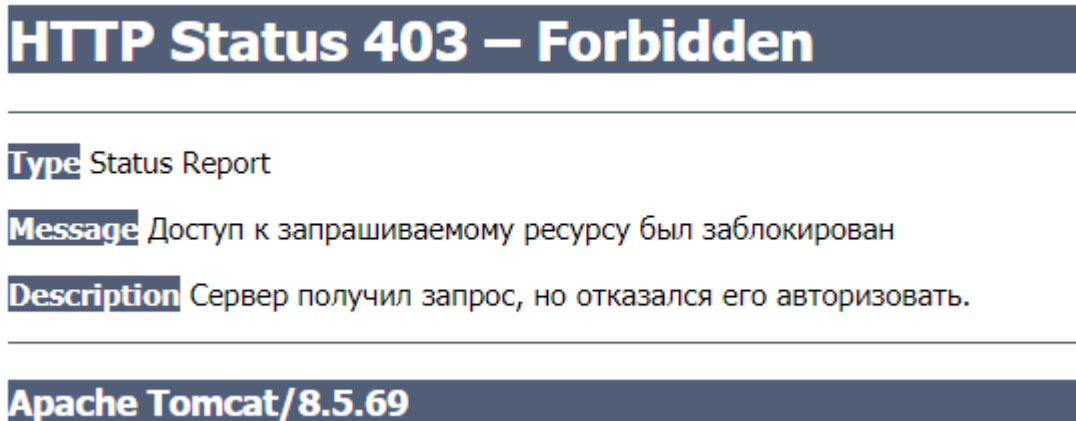
Имя пользователя user

Пароль .....

Вход Отмена

Рис.2. Авторизация под пользователем user

Закономерно получаем следующий результат:



**HTTP Status 403 – Forbidden**

---

**Type** Status Report

**Message** Доступ к запрашиваемому ресурсу был заблокирован

**Description** Сервер получил запрос, но отказался его авторизовать.

---

**Apache Tomcat/8.5.69**

Рис.3. Ошибка доступа к ресурсу

Теперь авторизуемся за пользователя admin с одноименным паролем. Без перезапуска сервера для повторной авторизации потребуется сбросить cookie-файлы браузера/зайти через другой браузер/зайти в режиме инкогнито, иначе доступ будет отказан повторно.

## Все записи сообщества

Пользователь	Комментарий	Дата
ДимонЛимон	всем привет в этом чатике	12-сентября-2021 00:59:11
Чппибарум	Жду обновлений приложения с нетерпением!	12-сентября-2021 00:59:11

[Новый пост](#)

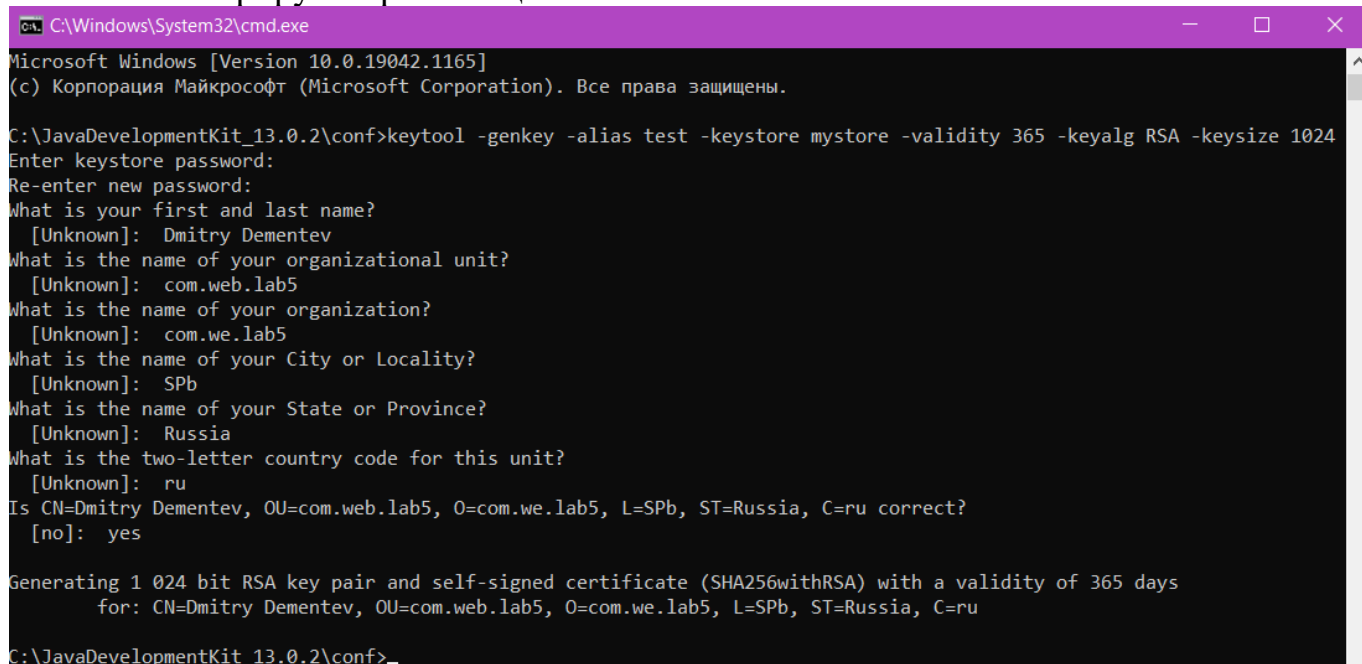
Доступные языки: [ru](#) [en](#) [de](#)

Рис.4. Успешная авторизация за роль admin

Важно заметить, что мы поставили авторизацию с корневой ссылки “/”, поэтому напрямую перейти по URL, например `http://localhost/new_post`, мы также не сможем без авторизации.

## SSL аутентификация

Сначала сгенерируем хранилище ключей и сам ключ:



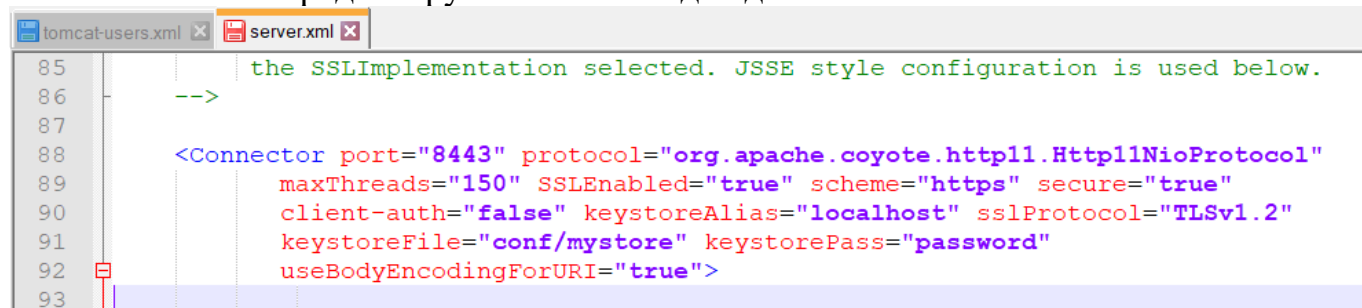
```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19042.1165]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\JavaDevelopmentKit_13.0.2\conf>keytool -genkey -alias test -keystore mystore -validity 365 -keyalg RSA -keysize 1024
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: Dmitry Dementev
What is the name of your organizational unit?
[Unknown]: com.web.lab5
What is the name of your organization?
[Unknown]: com.we.lab5
What is the name of your City or Locality?
[Unknown]: SPb
What is the name of your State or Province?
[Unknown]: Russia
What is the two-letter country code for this unit?
[Unknown]: ru
Is CN=Dmitry Dementev, OU=com.web.lab5, O=com.we.lab5, L=SPb, ST=Russia, C=ru correct?
[no]: yes

Generating 1 024 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 365 days
for: CN=Dmitry Dementev, OU=com.web.lab5, O=com.we.lab5, L=SPb, ST=Russia, C=ru
C:\JavaDevelopmentKit_13.0.2\conf>
```

Рис.5. Создание хранилища и SSL ключа

Созданный ключ поместим в папку /conf в корневой директории сервера Apache Tomcat и также отредактируем `server.xml` для добавления SSL ключа:



```
tomcat-users.xml x server.xml x
85 the SSLImplementation selected. JSSE style configuration is used below.
86 -->
87
88 <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
89     maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
90     client-auth="false" keystoreAlias="localhost" sslProtocol="TLSv1.2"
91     keystoreFile="conf/mystore" keystorePass="password"
92     useBodyEncodingForURI="true">
93
```

Рис.6. Добавление SSL ключа в `server.xml`

Для Java версии 8+ необходимо обязательно выставить значение `sslProtocol="TLSv1.2"`.

Теперь проверим работу защищённого протокола, перейдя по ссылке <https://localhost:8443/> :

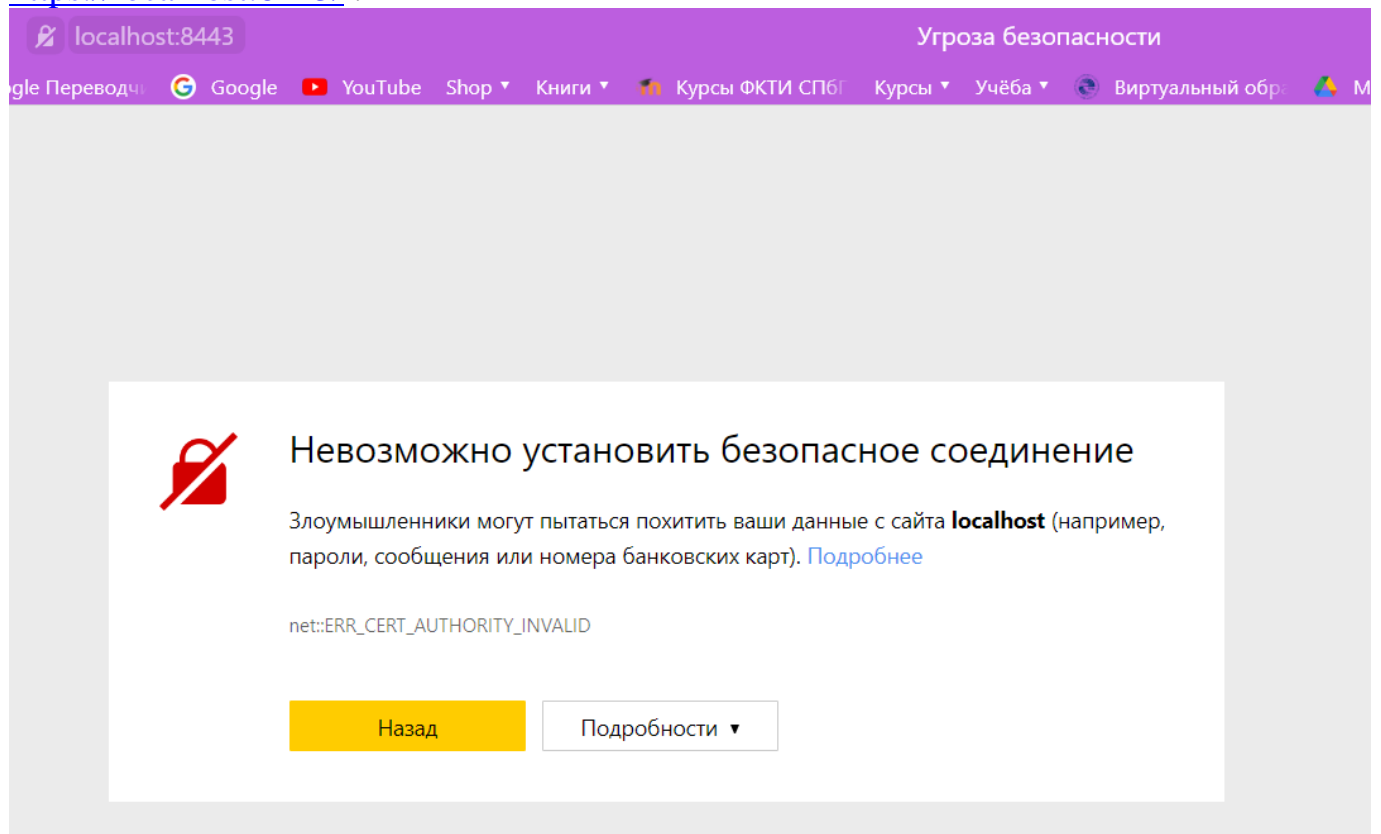


Рис.7. Предупреждение при переходе

Подтверждаем переход, авторизуемся как пользователь admin:

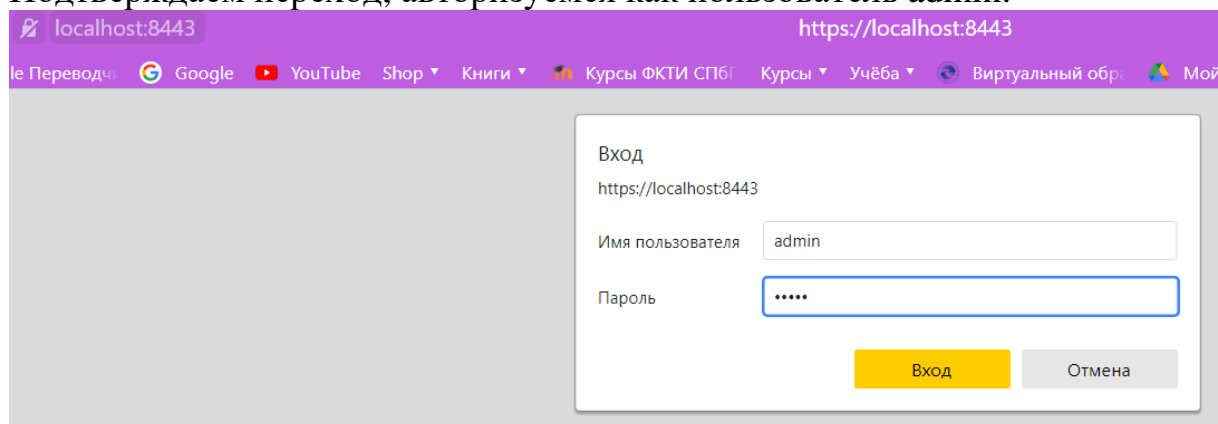


Рис.8. Авторизация по защищенному протоколу

Успешно переходим на главную страницу:



## Все записи сообщества

Пользователь	Комментарий	Дата
Димон.Лимон	всем привет в этом чатике	12-сентября-2021 02:21:35
Чппибарум	Жду обновлений приложения с нетерпением!	12-сентября-2021 02:21:35

[Новый пост](#)

Доступные языки: [ru](#) [en](#) [de](#)

Рис.9. Главная страница по адресу <https://localhost:8443/>

## **Вывод**

В ходе выполнения лабораторной работы были изучены технологии аутентификации: базовая, а также при помощи протокола SSL. Было создано хранилище ключей, а также разобран способ защиты содержимого сервера при помощи ролей и прав доступа.

## Приложение 1. tomcat-users.xml

```
<tomcat-users xmlns="http://tomcat.apache.org/xml"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
  version="1.0">
```

## Приложение 2. server.xml

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
  maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
  client-auth="false" keystoreAlias="localhost" sslProtocol="TLSv1.2"
  keystoreFile="conf/mystore" keystorePass="mystore"
  useBodyEncodingForURI="true"/>
```

## Приложение 3. web.xml

```
<?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_4_0.xsd"
  version="4.0">

  <welcome-file-list>
    <welcome-file>PostsTitle.jsp</welcome-file>
  </welcome-file-list>

  <!--Изменение ссылки URL с "/PostsTitle.jsp" на "/posts" -->
  <servlet>
    <servlet-name>PostsTitle</servlet-name>
    <jsp-file>/PostsTitle.jsp</jsp-file>
  </servlet>
  <servlet-mapping>
    <servlet-name>PostsTitle</servlet-name>
    <url-pattern>/posts</url-pattern>
  </servlet-mapping>

  <servlet>
    <servlet-name>PostForm</servlet-name>
    <jsp-file>/post_form.jsp</jsp-file>
  </servlet>
  <servlet-mapping>
    <servlet-name>PostForm</servlet-name>
    <url-pattern>/new_post</url-pattern>
  </servlet-mapping>

  <!-- Добавление авторизации пользователей -->
  <security-role>
    <role-name>admin</role-name>
  </security-role>

  <security-role>
    <role-name>manager</role-name>
  </security-role>

  <security-role>
    <role-name>user</role-name>
  </security-role>

  <security-constraint>
    <web-resource-collection>
```



```
        <web-resource-name>/</web-resource-name>
        <url-pattern>/</url-pattern>
        <http-method>GET</http-method>
        <http-method>POST</http-method>
    </web-resource-collection>
    <auth-constraint>
        <role-name>admin</role-name>
        <role-name>manager</role-name>
    </auth-constraint>
</security-constraint>

<login-config>
    <auth-method>BASIC</auth-method>
    <realm-name>Write Post List</realm-name>
</login-config>

</web-app>
```