

**МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И.УЛЬЯНОВА (ЛЕНИНА)**

Кафедра ВТ

**ОТЧЕТ
по лабораторной работе №6
по дисциплине «Java программирование
интернет-приложений»
Тема: Аутентификация и авторизация пользователей
WEB-приложения**

Преподаватель

Репин С.А.

Павловский М.Г.

Санкт-Петербург
2022

СОДЕРЖАНИЕ

1. Цель работы	3
2. Выполнение работы	3
3. Вывод	4
Исходный код tomcat-users.xml	4
Исходный код server.xml	5
Исходный код web.xml	6

1. ЦЕЛЬ РАБОТЫ

Знакомство со способами реализации аутентификации и авторизации пользователей Web-приложения.

2. ВЫПОЛНЕНИЕ РАБОТЫ

В проект, созданный лабораторной работе № 5, была добавлена аутентификация и авторизация. Для этого в tomcat по средствам редактирования файла tomcat-users.xml были добавлены роли admin и manager, а также пользователь admin/admin. Затем информация о существовании такого пользователя была добавлена в файл web.xml. В том же файле указаны страница, к которой надо применить правила аутентификации, и метод аутентификации.

Кроме того, сервер был настроен для работы через HTTPS (по порту 8443). Для этого был сгенерирован соответствующий сертификат, который затем был прописан в специальном Connector в файле server.xml.

```
> sudo keytool -genkey -alias test -keystore /usr/share/tomcat.keystore -validity 365 -keyalg RSA -keysize 1024
[sudo] password for root:
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]: Stepan Repin
What is the name of your organizational unit?
  [Unknown]: ETU
What is the name of your organization?
  [Unknown]: ETU
What is the name of your City or Locality?
  [Unknown]:
What is the name of your State or Province?
  [Unknown]:
What is the two-letter country code for this unit?
  [Unknown]: RU
Is CN=Stepan Repin, OU=ETU, O=ETU, L=Unknown, ST=Unknown, 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=Stepan Repin, OU=ETU, O=ETU, L=Unknown, ST=Unknown, C=RU

Warning:
The generated certificate uses a 1024-bit RSA key which is considered a security risk. This key size will be disabled in a future update.
```

Рис. 2.1 Процесс генерации сертификата



Рис. 2.2 Подключение по HTTP с окном авторизации

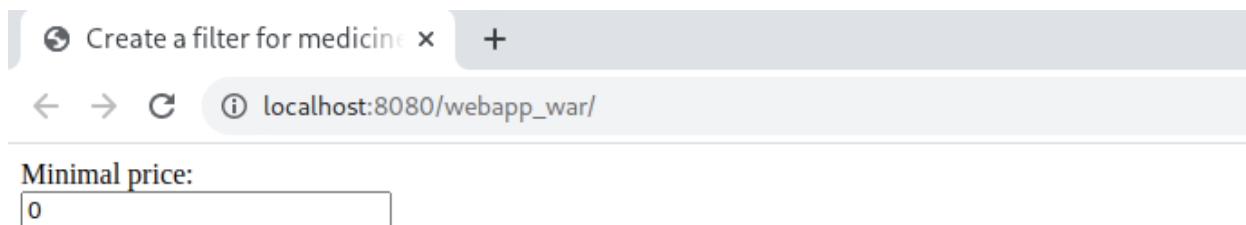


Рис. 2.3 Результат успешной авторизации – переход к странице MedicineFilter.jsp



Рис. 2.4 Загрузка страницы по HTTPS

3. ВЫВОД

В ходе выполнения лабораторной работы были получены практические навыки разработки WEB-приложений с поддержкой аутентификации и авторизации. Кроме того, были получены знания о генерации сертификатов и подключении HTTPS.

ИСХОДНЫЙ КОД TOMCAT-USERS.XML

```
<?xml version="1.0" encoding="UTF-8"?>
<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">
  <role rolename="manager" />
```

```

    <role rolename="admin" />
    <user username="admin" password="admin" roles="manager, admin" />
</tomcat-users>

```

ИСХОДНЫЙ КОД SERVER.XML

```

<?xml version="1.0" encoding="UTF-8"?>
<Server port="8005" shutdown="SHUTDOWN">
  <Listener
    className="org.apache.catalina.startup.VersionLoggerListener" />
  <Listener
    className="org.apache.catalina.core.AprLifecycleListener"
    SSLEngine="on" />
  <Listener
    className="org.apache.catalina.core.JreMemoryLeakPreventionListener" />
  <Listener
    className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener" />
  <Listener
    className="org.apache.catalina.core.ThreadLocalLeakPreventionListener" />

  <GlobalNamingResources>
    <Resource name="UserDatabase" auth="Container"
      type="org.apache.catalina.UserDatabase"
      description="User database that can be updated and saved"
      factory="org.apache.catalina.users.MemoryUserDatabaseFactory"
      pathname="conf/tomcat-users.xml" />
  </GlobalNamingResources>

  <Service name="Catalina">

    <Connector port="8080" protocol="HTTP/1.1"
      connectionTimeout="20000"
      useBodyEncodingForURI="true"/>
    <Connector port="8443"
      protocol="org.apache.coyote.http11.Http11NioProtocol"
      SSLEnabled="true"
      maxThreads="150" scheme="https" secure="true"
      clientAuth="false" sslProtocol="TLS"
      useBodyEncodingForURI="true">
      <SSLHostConfig>
        <Certificate
          certificateKeystoreFile="/usr/share/tomcat.keystore"
          certificateKeystorePassword="111111"
          type="RSA"/>
        </SSLHostConfig>
      </Connector>

```

```

<Engine name="Catalina" defaultHost="localhost">

  <Realm className="org.apache.catalina.realm.LockOutRealm">
    <Realm className="org.apache.catalina.realm.UserDatabaseRealm"
      resourceName="UserDatabase"/>
  </Realm>

  <Host name="localhost" appBase="webapps"
    unpackWARs="true" autoDeploy="true">

    <Valve className="org.apache.catalina.valves.AccessLogValve"
      directory="logs"
      prefix="localhost_access_log" suffix=".txt"
      pattern="%h %l %u %t &quot;%r&quot; %s %b" />

  </Host>
</Engine>
</Service>
</Server>

```

ИСХОДНЫЙ КОД WEB.XML

```

<!DOCTYPE web-app PUBLIC
"-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
"http://java.sun.com/dtd/web-app_2_3.dtd" >

<web-app>
  <display-name>Web Application</display-name>
  <welcome-file-list>
    <welcome-file>/MedicineFilter.jsp</welcome-file>
  </welcome-file-list>

  <security-role>
    <role-name>admin</role-name>
  </security-role>

  <security-constraint>
    <web-resource-collection>
      <web-resource-name>
        Medicine List Filter
      </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>
    </auth-constraint>

```

```
</security-constraint>

<login-config>
  <auth-method>BASIC</auth-method>
  <realm-name>Filter Medicine List</realm-name>
</login-config>
</web-app>
```