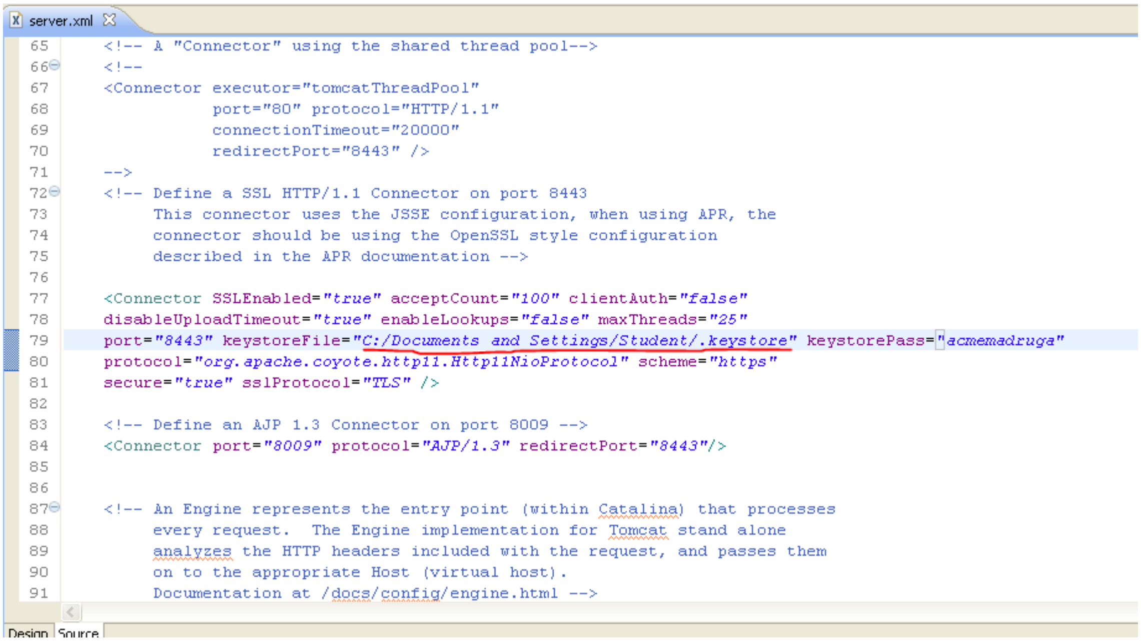
HTTPS CONFIGURATION GUIDE

Please follow the next steps to set up your secure connection for Acme-Madrgá:

Configure your server.xml file

1. Copy the “*.keystore”* file we provided and paste it in your personal profile folder, ex: “C:/Documents and Settings/Student/”.

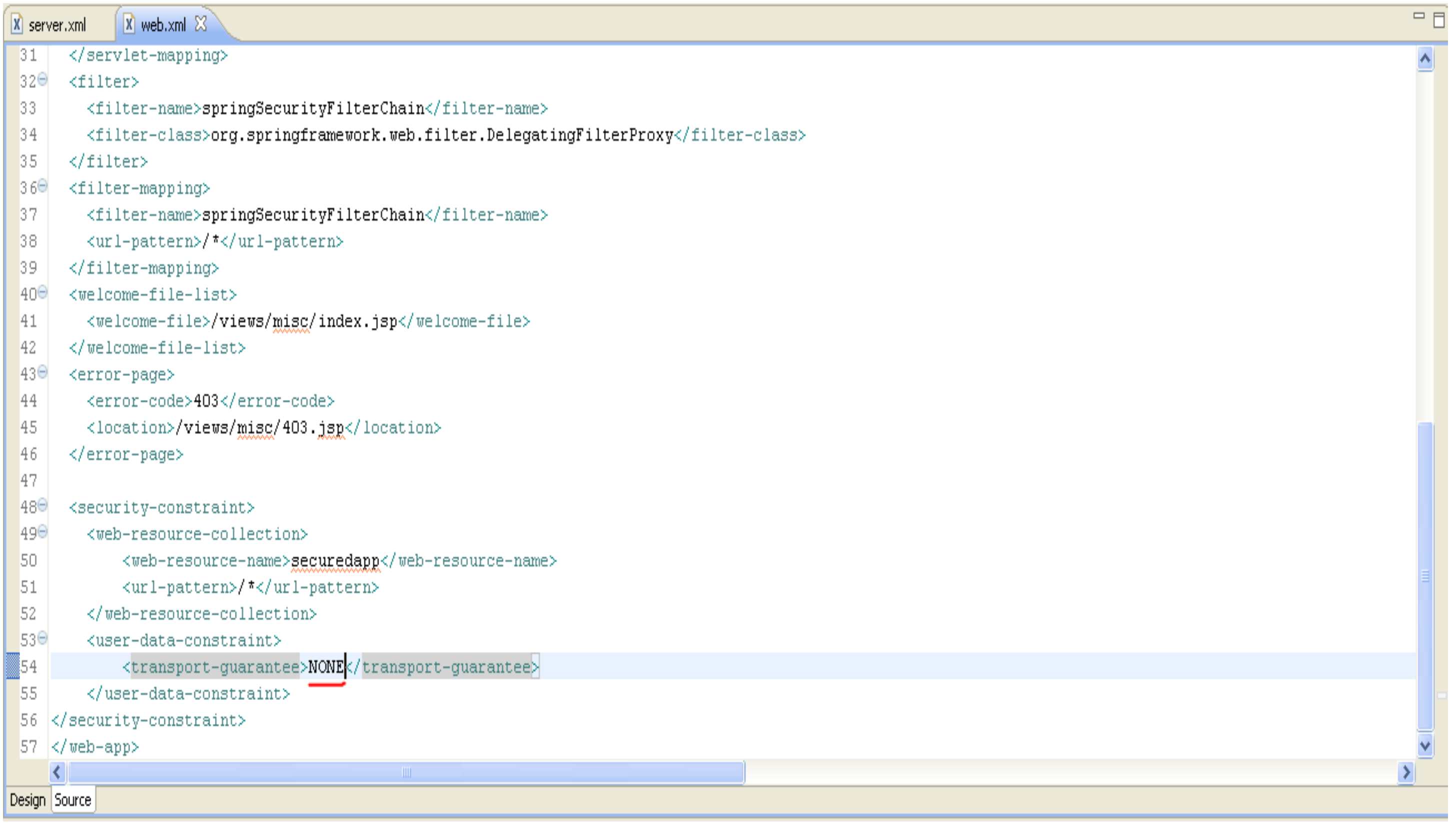
2. Edit your server.xml file at Servers > server.xml. Change the path specified in the keystoreFile attribute for 8443 port, using the path where you saved your “*.keystore”* file, ex: “C:/Documents and Settings/Student/.keystore”.



```
<!-- A "Connector" using the shared thread pool-->
<!--
<Connector executor="tomcatThreadPool"
           port="80" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
-->
<!-- Define a SSL HTTP/1.1 Connector on port 8443
     This connector uses the JSSE configuration, when using APR, the
     connector should be using the OpenSSL style configuration
     described in the APR documentation -->

<Connector SSLEnabled="true" acceptCount="100" clientAuth="false"
disableUploadTimeout="true" enableLookups="false" maxThreads="25"
port="8443" keystoreFile="C:/Documents and Settings/Student/.keystore" keystorePass="acmemadruga"
protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https"
secure="true" sslProtocol="TLS" />

<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"/>


<!-- An Engine represents the entry point (within Catalina) that processes
     every request.  The Engine implementation for Tomcat stand alone
     analyzes the HTTP headers included with the request, and passes them
     on to the appropriate Host (virtual host).
     Documentation at /docs/config/engine.html -->
```

Configure your web.xml file

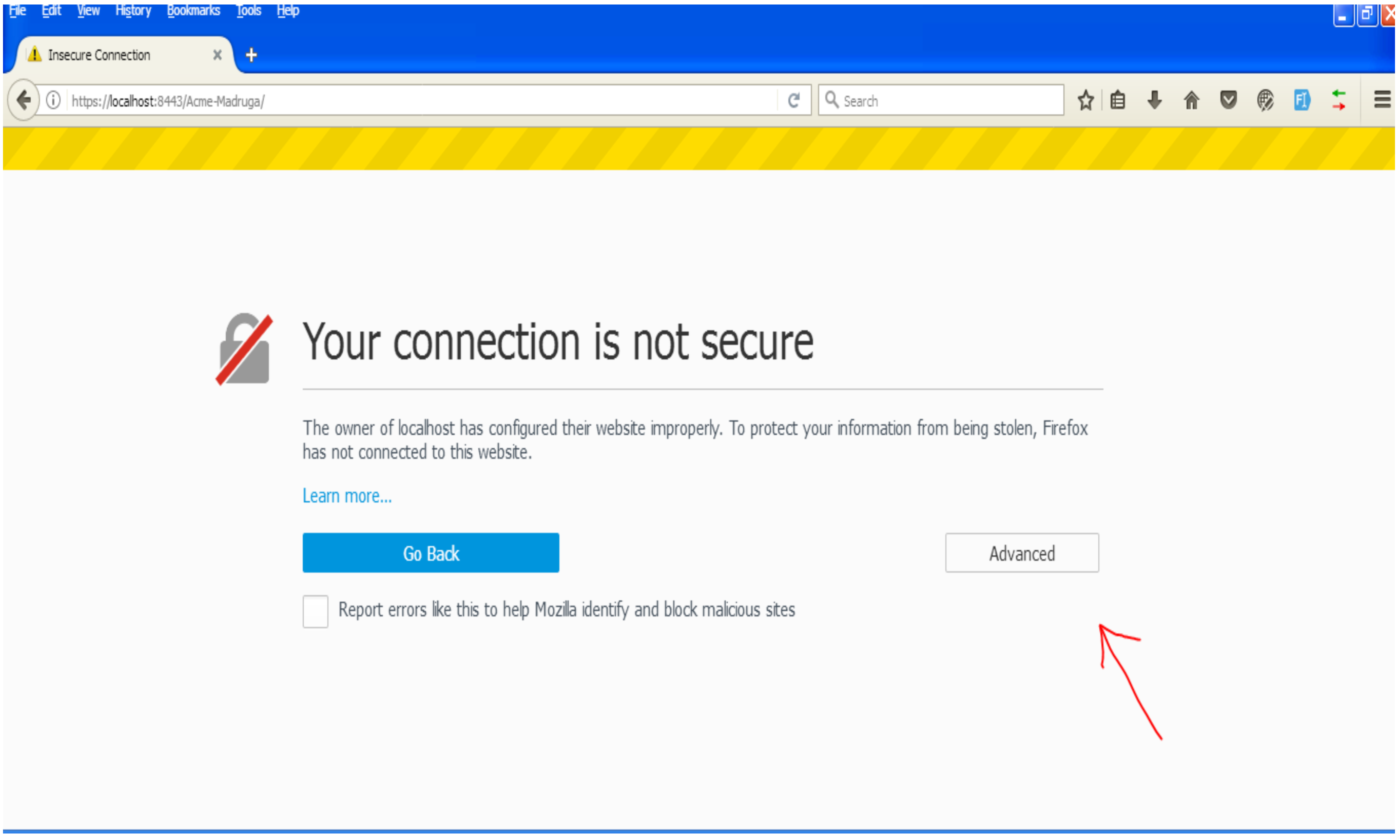
3. Edit your web.xml file at Acme-Madruga > src >main > webapp > WEB-INF > web.xml. Go to the end of the file and modify the transport-guarantee property from NONE to CONFIDENTIAL. This will force the application to use a secure connection (https), automatically redirecting to the right port (8443) when accessing http://localhost:8080/Acme-Madruga .



```
  </servlet-mapping>
  <filter>
    <filter-name>springSecurityFilterChain</filter-name>
    <filter-class>org.springframework.web.filter.DelegatingFilterProxy</filter-class>
  </filter>
  <filter-mapping>
    <filter-name>springSecurityFilterChain</filter-name>
    <url-pattern>/*</url-pattern>
  </filter-mapping>
  <welcome-file-list>
    <welcome-file>/views/misc/index.jsp</welcome-file>
  </welcome-file-list>
  <error-page>
    <error-code>403</error-code>
    <location>/views/misc/403.jsp</location>
  </error-page>

  <security-constraint>
    <web-resource-collection>
        <web-resource-name>securedapp</web-resource-name>
        <url-pattern>/*</url-pattern>
    </web-resource-collection>
    <user-data-constraint>
        <transport-guarantee>NONE</transport-guarantee>
    </user-data-constraint>
</security-constraint>
</web-app>
```

Calm your browser

4. Now let’s test it. Start your Tomcat server or restart if it already was. Open your browser and go to https://localhost:8443/Acme-Madruga . The browser will warn you because we are using a self-signed certificate, but don’t worry, we know we can trust it. Click on “Advance”, then on “Add Exception” and finally “Confirm Security Exception”.

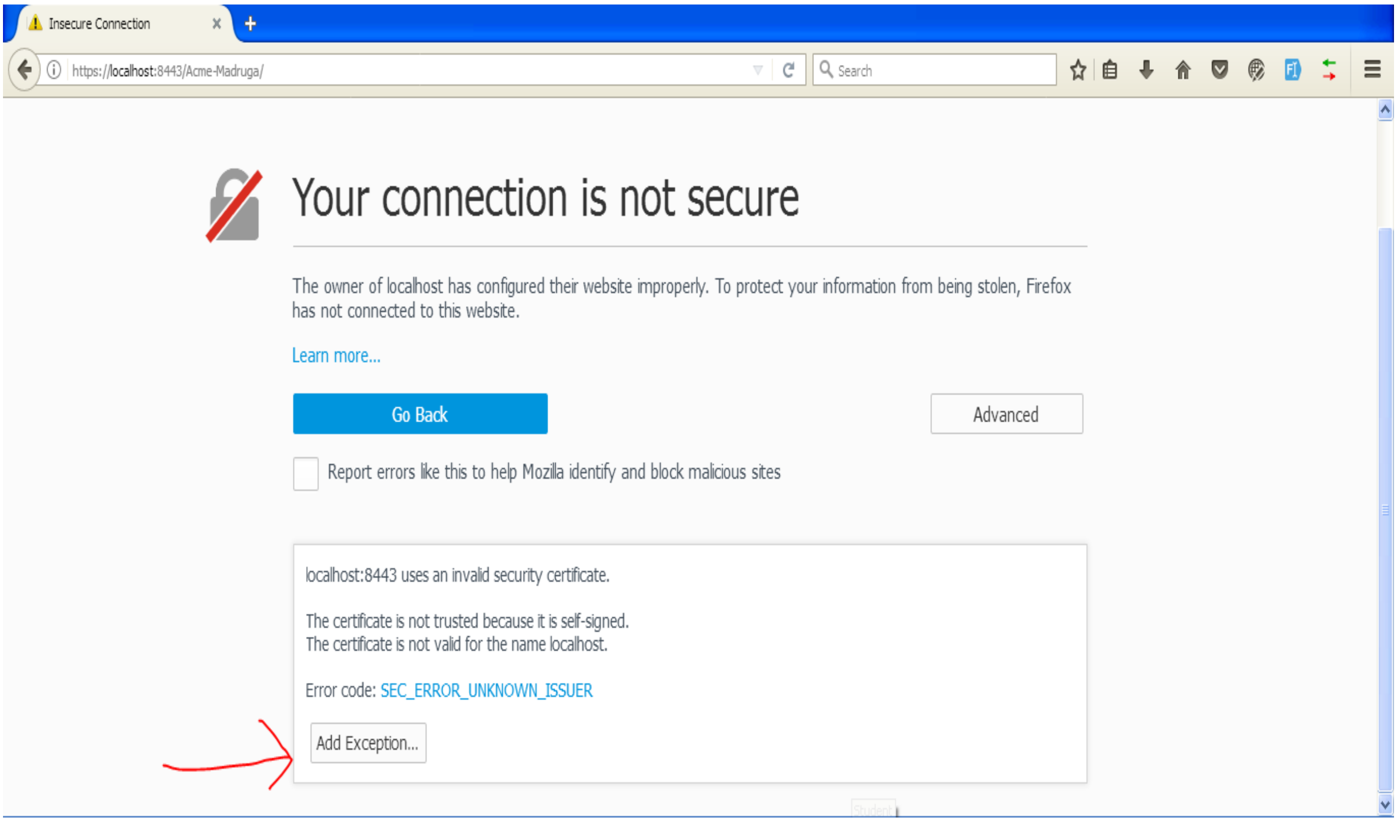

File Edit View History Bookmarks Tools Help
Insecure Connection
https://localhost:8443/Acme-Madruga/
Search

Your connection is not secure

The owner of localhost has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more...

□ Report errors like this to help Mozilla identify and block malicious sites



Your connection is not secure

The owner of localhost has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

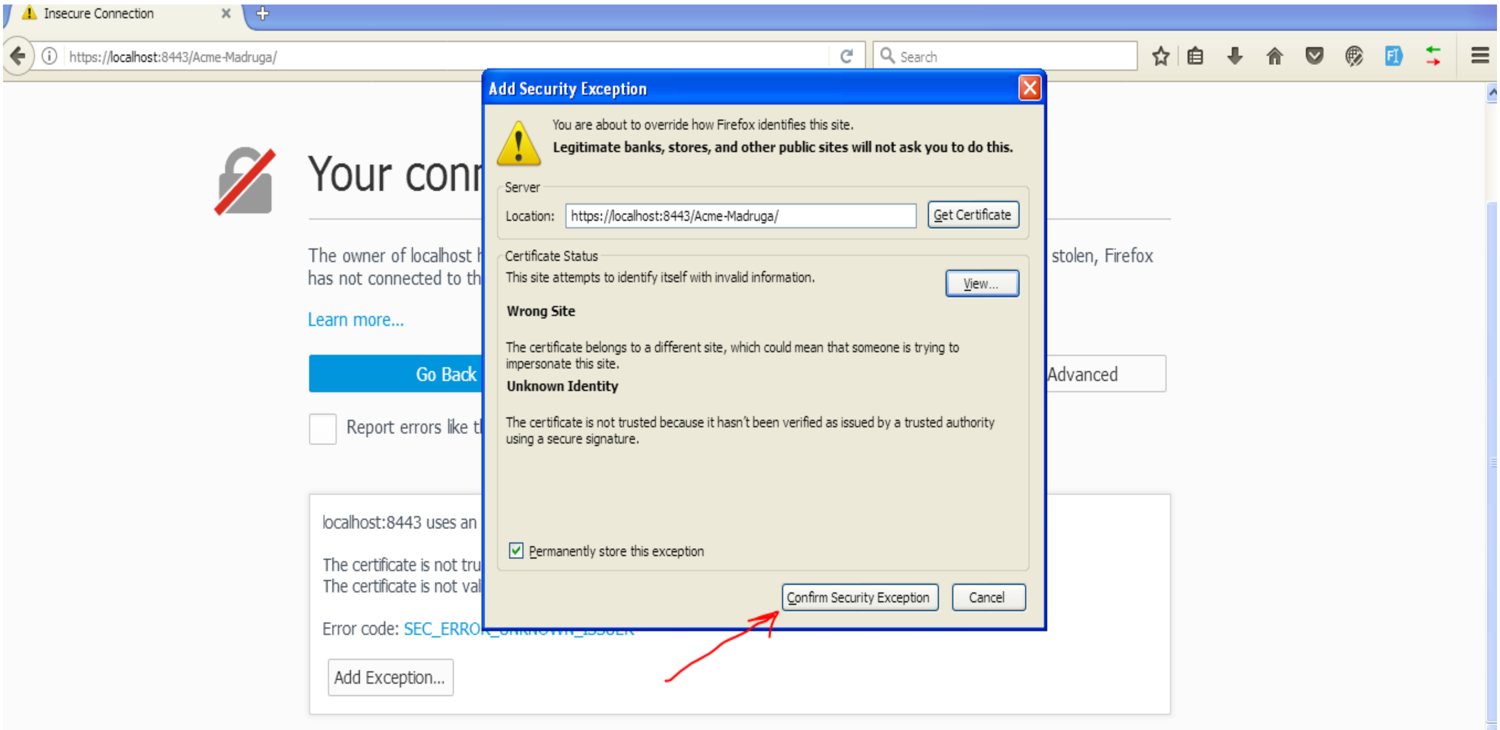
Learn more...

□ Report errors like this to help Mozilla identify and block malicious sites

localhost:8443 uses an invalid security certificate.

The certificate is not trusted because it is self-signed.
The certificate is not valid for the name localhost.

Error code: SEC_ERROR_UNKNOWN_ISSUER



Insecure Connection

https://localhost:8443/Acme-Madruga/

Your conn

The owner of localhost h
has not connected to th

stolen, Firefox

Learn more...

Go Back

Advanced

□ Report errors like t

localhost:8443 uses an

The certificate is not tru
The certificate is not val

Error code: SEC_ERROR

Add Exception...

Add Security Exception

You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://localhost:8443/Acme-Madruga/

Get Certificate

Certificate Status

This site attempts to identify itself with invalid information.

View...

Wrong Site

The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.

Unknown Identity

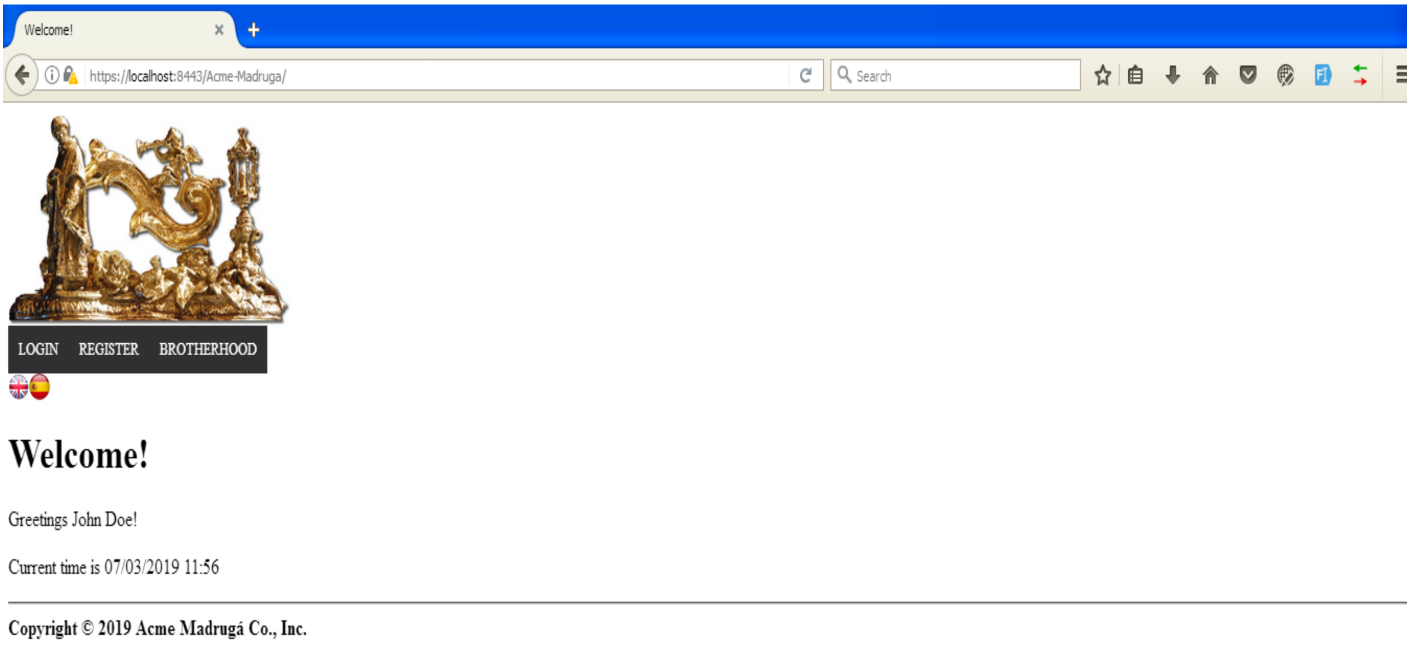
The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

☑ Permanently store this exception

Confirm Security Exception

Cancel

5. Voilà! Your Acme-Madruga application is ready to go at https://localhost:8443/Acme-Madruga as well as http://localhost:8080/Acme-Madruga (this will redirect you to the previous one).



Welcome!

https://localhost:8443/Acme-Madruga/

LOGIN REGISTER BROTHERHOOD

Welcome!

Greetings John Doe!

Current time is 07/03/2019 11:56

Copyright © 2019 Acme Madrugá Co., Inc.

Hope this guide helped you get your secure connection running, if you have any questions, feel free to contact me at jsaferrete@gmail.com .