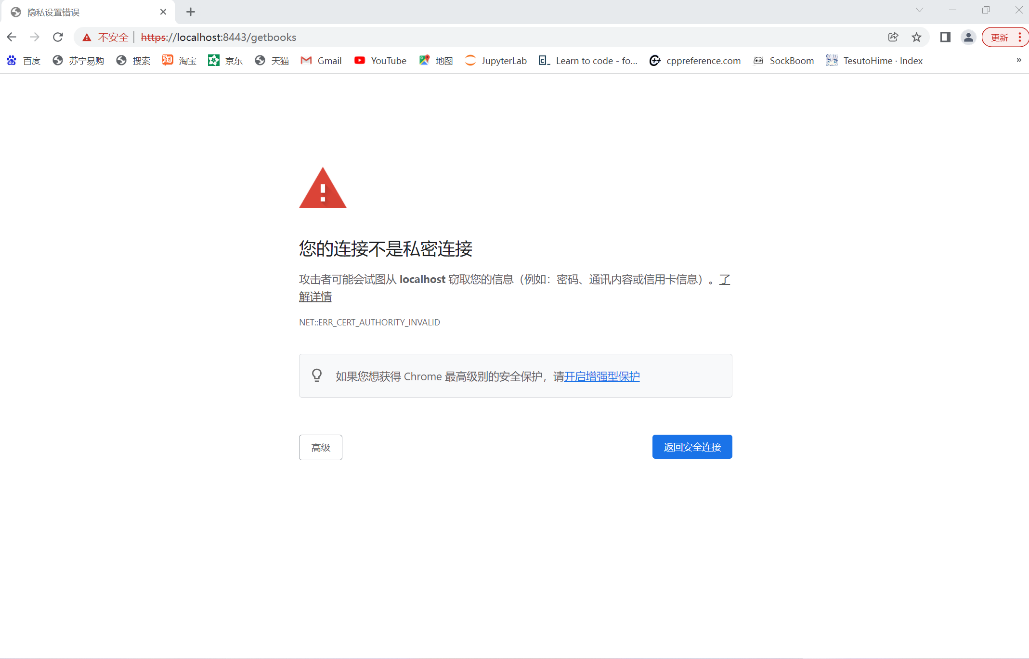
（1）在chrome浏览器网址中输入localhost:8080/getbooks后，会自动重定向到8443端口，此时由于自制证书不被浏览器信任，呈现出连接不安全的提示。

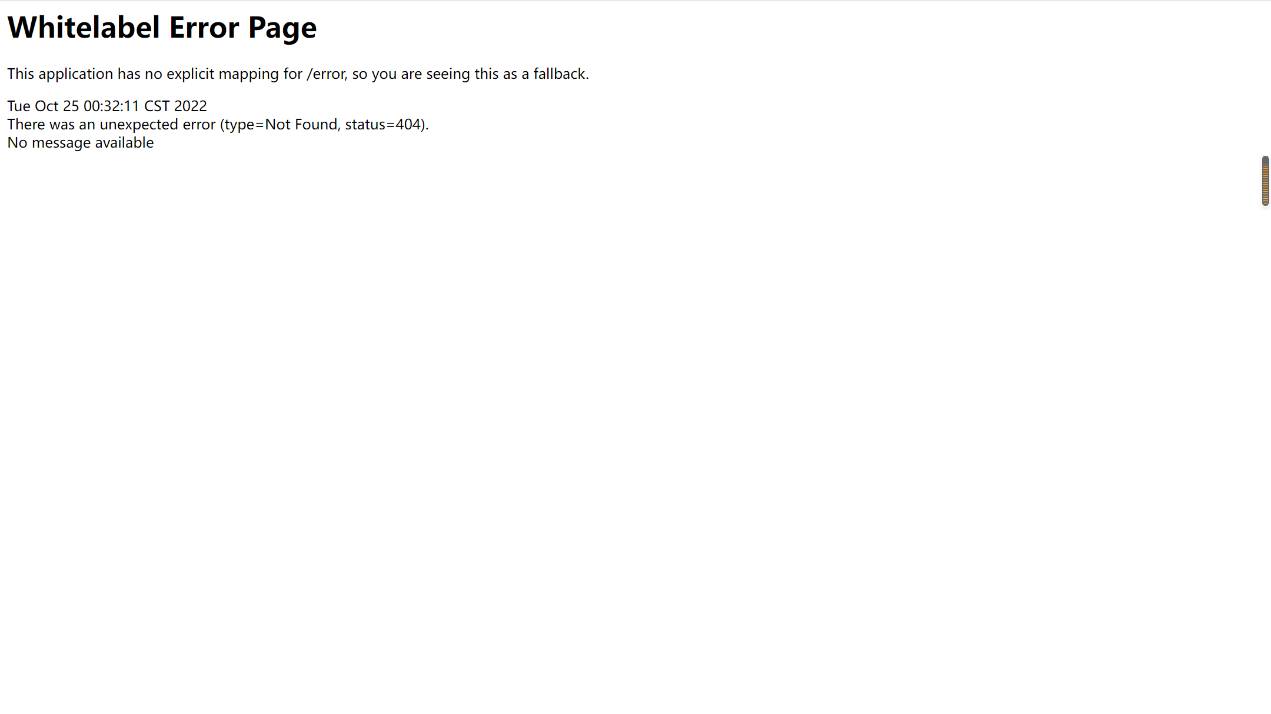




在经过网上搜索之后，我找到了两种方法：

法一：在chrome浏览器的设置中找到管理证书，选择正确的证书文件，将不受信任证书导入，由于自制的证书无法解析，遂放弃。

法二：点击页面空白处后直接输入“thisisunsafe”即可，法二成功运行后如图

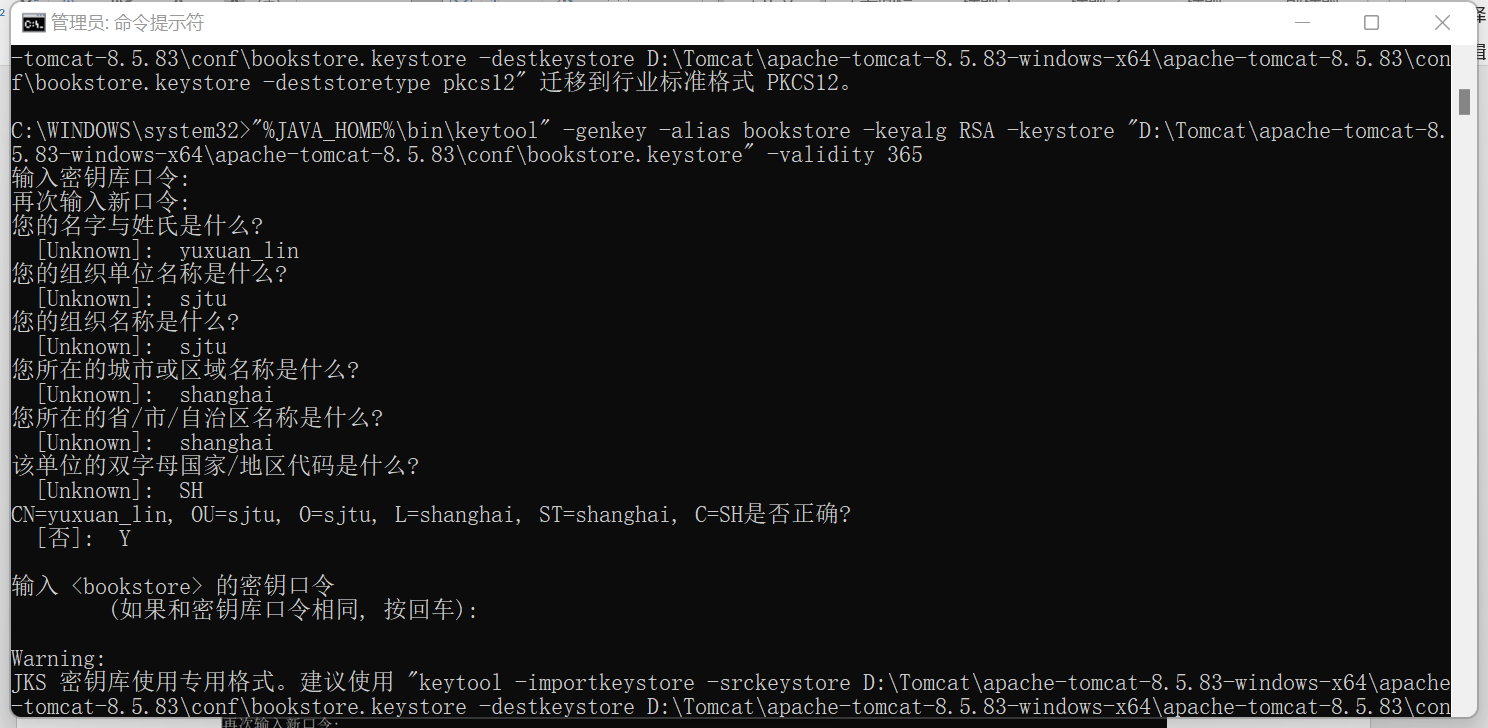


出现这种报错的原因是该访问网址仅向后端发起请求，并没有经过前端的修饰，无法被浏览器所解析。有尝试过访问localhost:8081（即前端运行端口）通过查看前端是否能顺利向后端发送申请来查看，但结果顺利，似乎仍然使用的是http协议

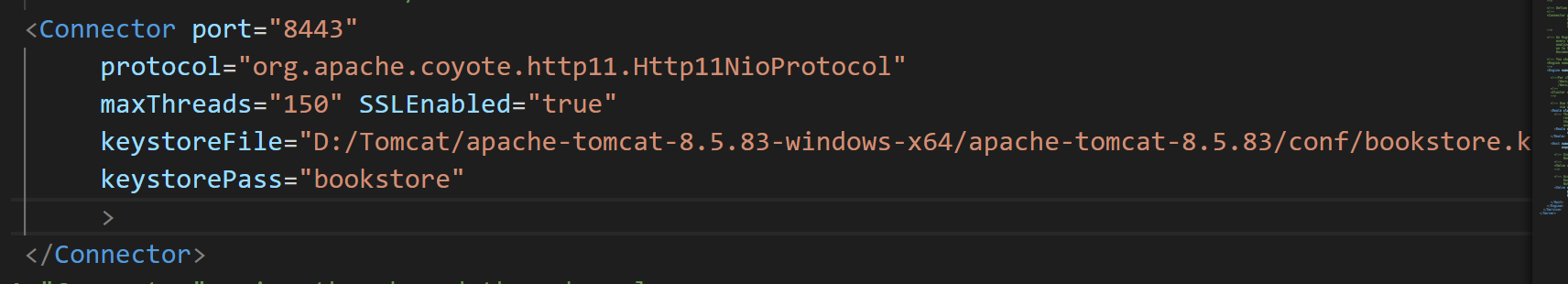
（2）https通信时在原先http明文传输的基础上通过ssl进行加密，加强了数据传输过程中的安全性，同时通过ssl证书，在每个发送到浏览器的数据都有数字签名用于验证数据是否真实有效。

（3）证书主要用于验证得到信息的真实有效性。网站的SSL证书包含一个公共密钥，Web浏览器可以使用该公共密钥来确认服务器发送的文档已经由拥有相应私有密钥的人进行了数字签名。如果服务器的证书已由公共信任的证书颁发机构的签名，则浏览器将接受证书中包含的所有标识信息均已由可信的第三方验证。

生成证书的过程：在命令行输入以下命令，指定密钥库的名字和位置。



在server.xml中修改如下代码将证书导入tomcat



在application.properties中写入如下代码，把证书导入项目中

