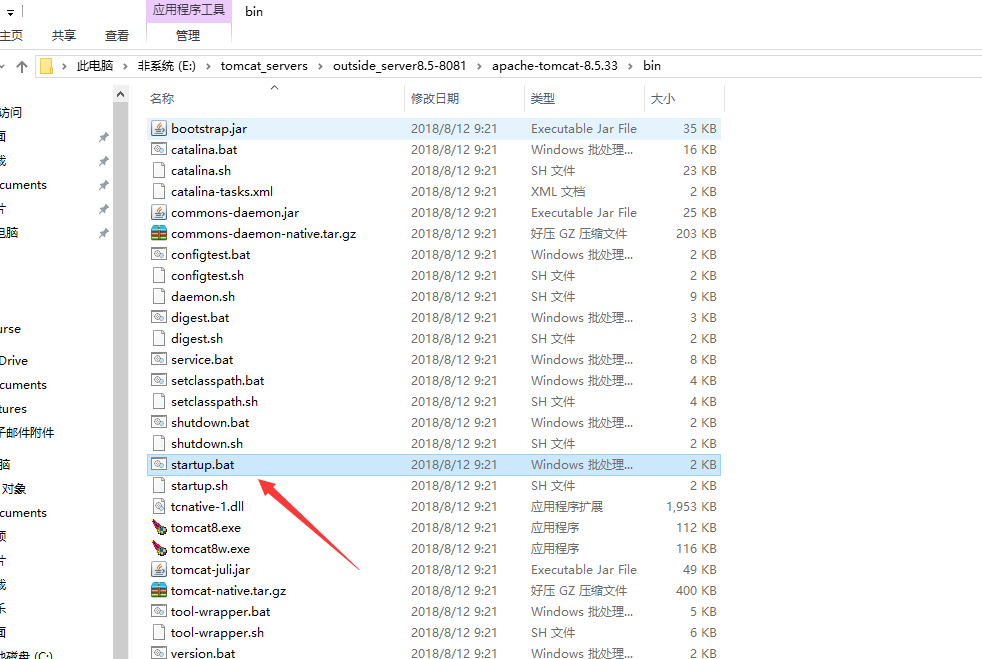
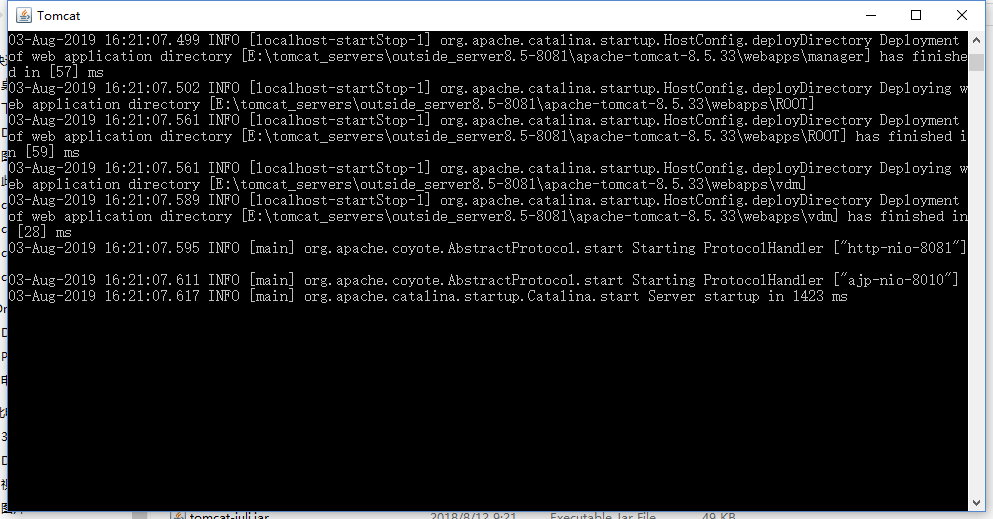
1. 前提。

1.首先应该保证http访问方式的tomcat服务器已经搭建完成，jdk使用的是1.8。

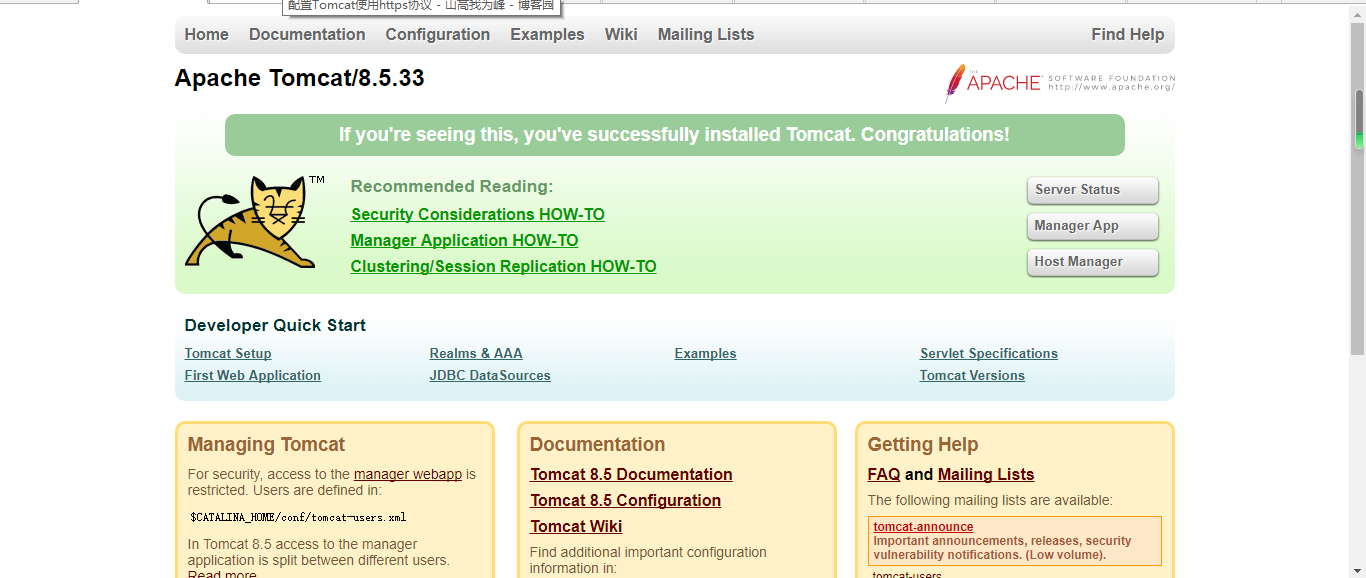
（1）http访问方式的tomcat搭建完成的查看：

a.进入到tomcat安装包bin目录下(比如：E:\tomcat\_servers\outside\_server8.5-8081\apache-tomcat-8.5.33\bin)双击startup.bat，并成功启动。



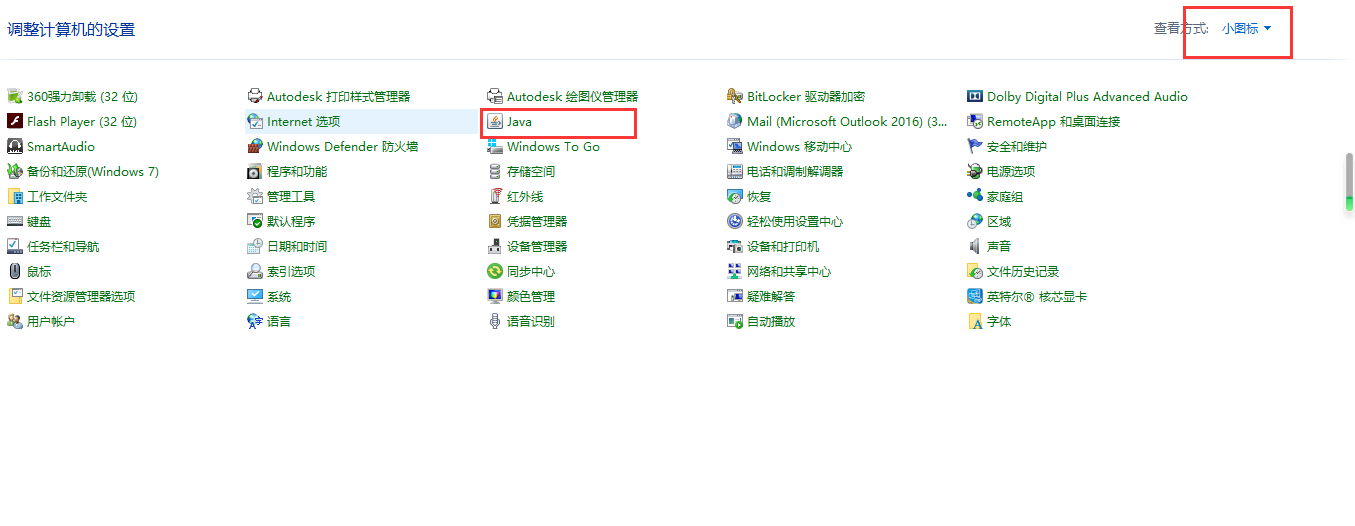


b.输入网址<http://localhost:8081/> 8081为当初设置的端口号。出现以下界面表示tomcat已经搭建。

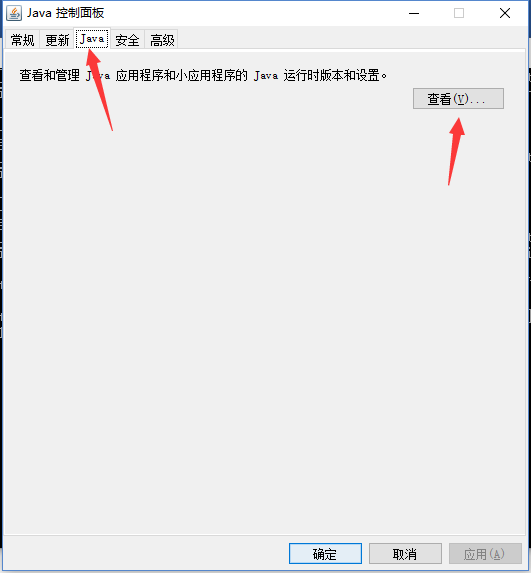


（2）.JDK的查看。

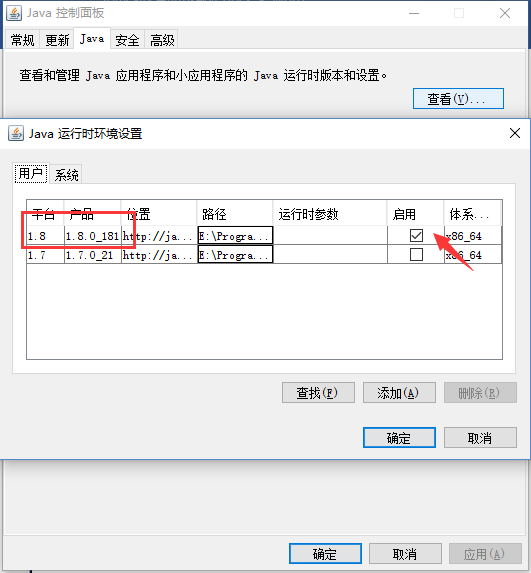
a.打开控制面板，找到java选项。



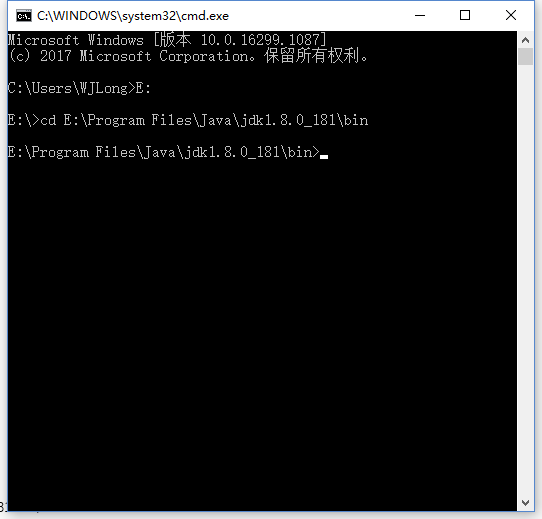
b.双击，在java选项下，点击查看



c.在JDK为1.8下面打勾。

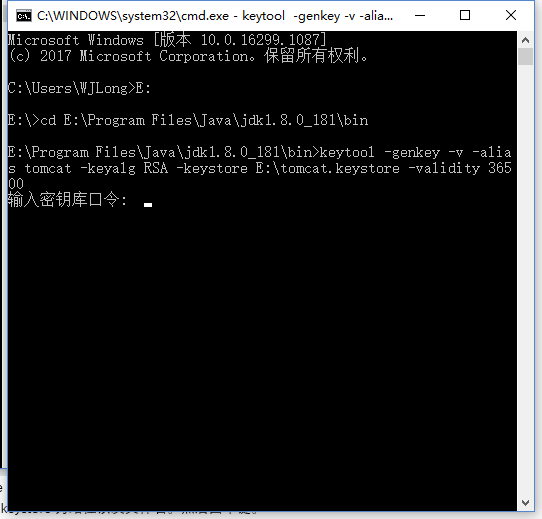


1. https的搭建。
2. 证书的生成。
3. 在CMD下打开1.8版本的JDK bin目录（比如E:\Program Files\Java\jdk1.8.0\_181\bin）

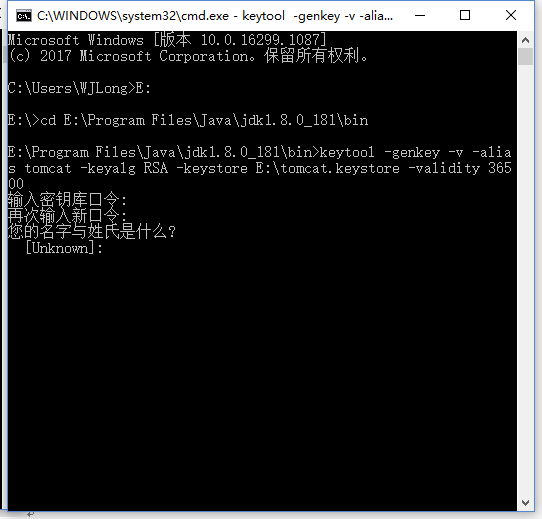


1. 输入：keytool -genkey -v -alias tomcat -keyalg RSA -keystore E:\tomcat.keystore -validity 36500

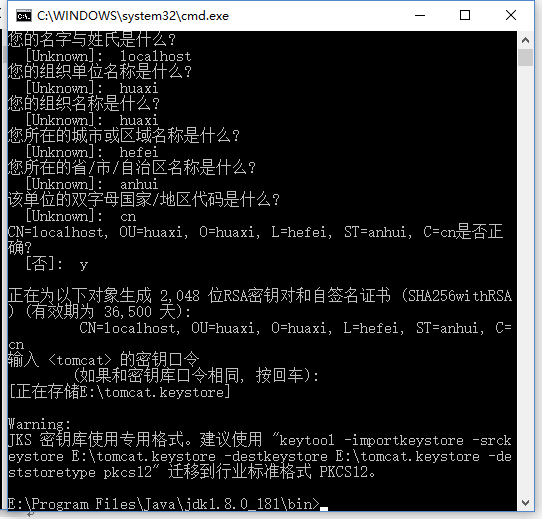
其中的tomcat是秘钥库的别名，36500是秘钥库的有效时间，单位为天，E:\tomcat.keystore为路径以及文件名。然后回车键。

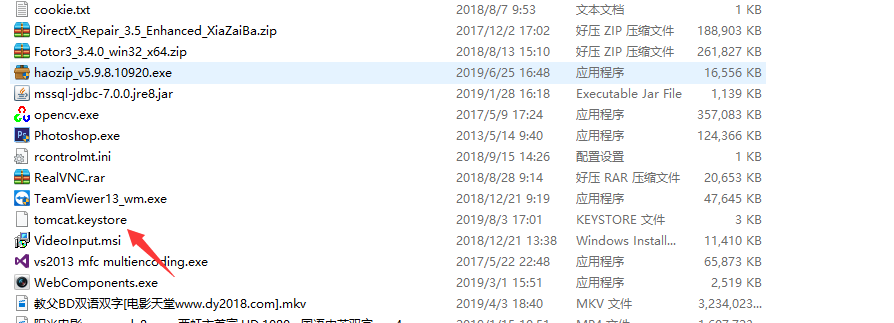


1. 输入口令，输入的数字两次是看不到的，但是必须一样。

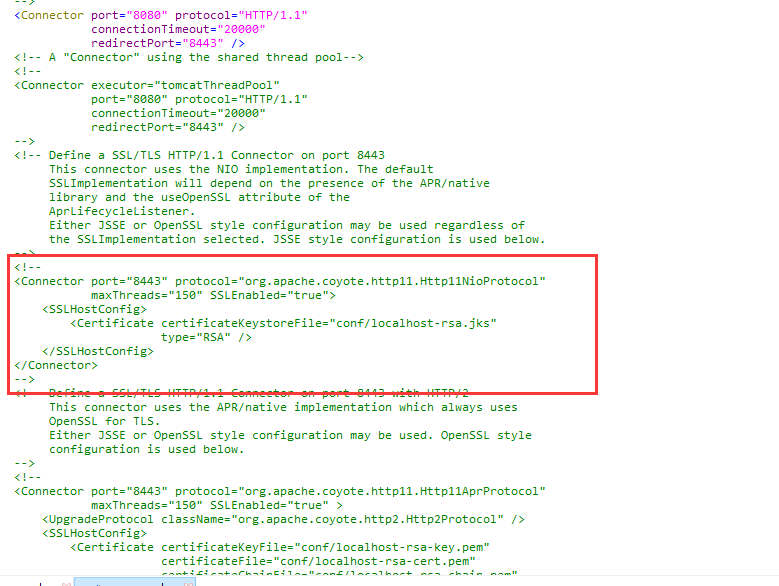


1. 填写相关性息，姓氏最好为localhost,否填为y如果密钥与口令相同，回车，也可以自己设置，证书生成成功





1. https方式的搭建。
2. 在tomcat的conf文件夹下，找到server.xml（比如E:\tomcat\_servers\apache-tomcat-8.5.33-windows-x64\apache-tomcat-8.5.33\conf），编辑,找到以下代码段：



1. 取消掉注释，然后改为：

<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"

maxThreads="150" SSLEnabled="true" scheme="https" secure="true"

clientAuth="false" sslProtocol="TLS"

keystoreFile="E:/tomcat.keystore" keystorePass="123888">

<!-- <SSLHostConfig>

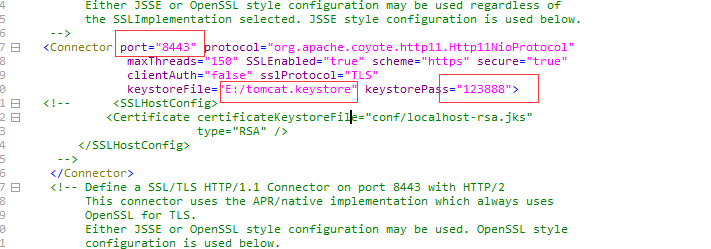
<Certificate certificateKeystoreFile="conf/localhost-rsa.jks"

type="RSA" />

</SSLHostConfig>

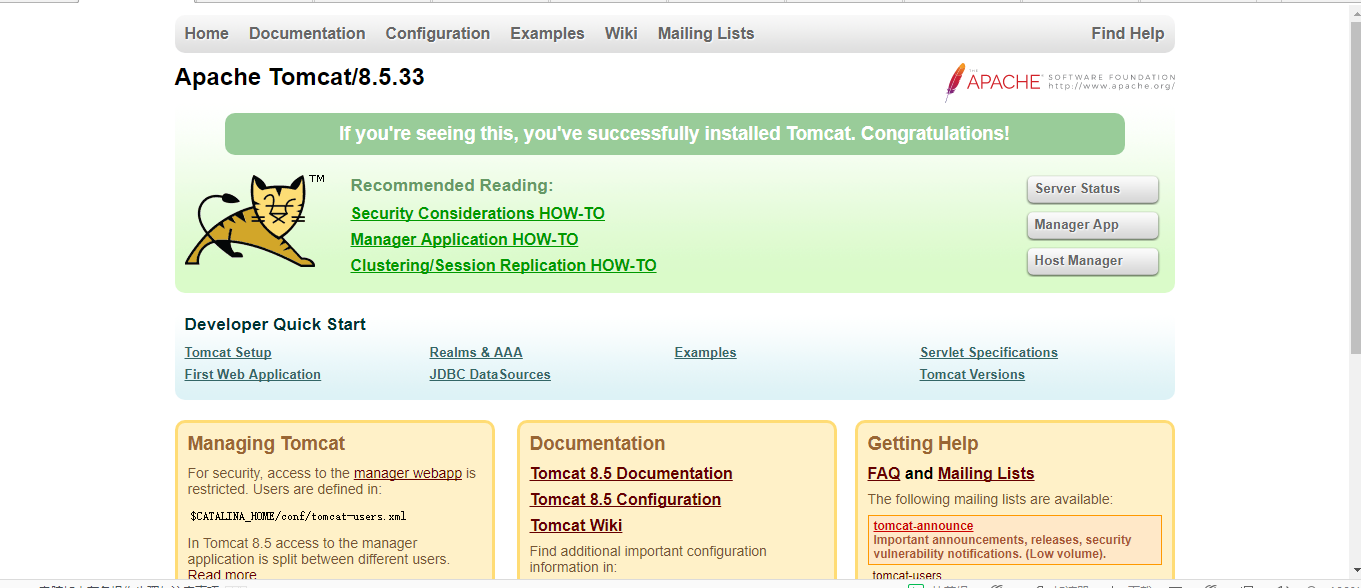
-->

</Connector>

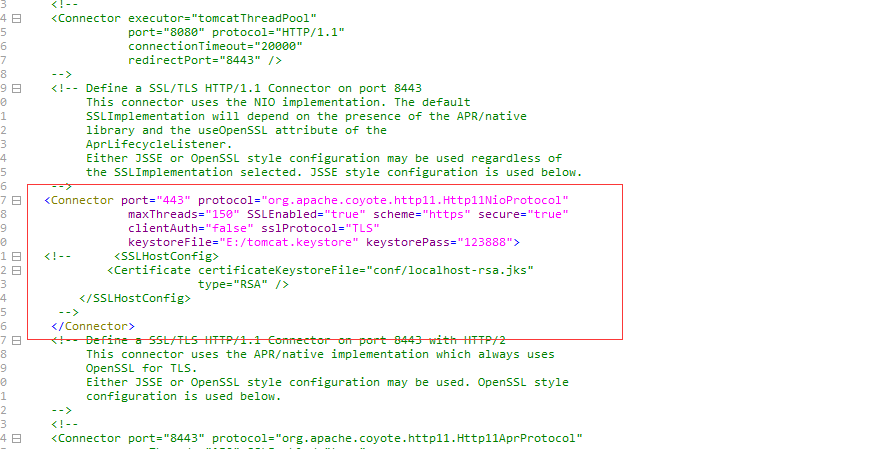


8443为你之后的访问端口，keystoreFile为证书的路径名，keystorePass为之前的密码。

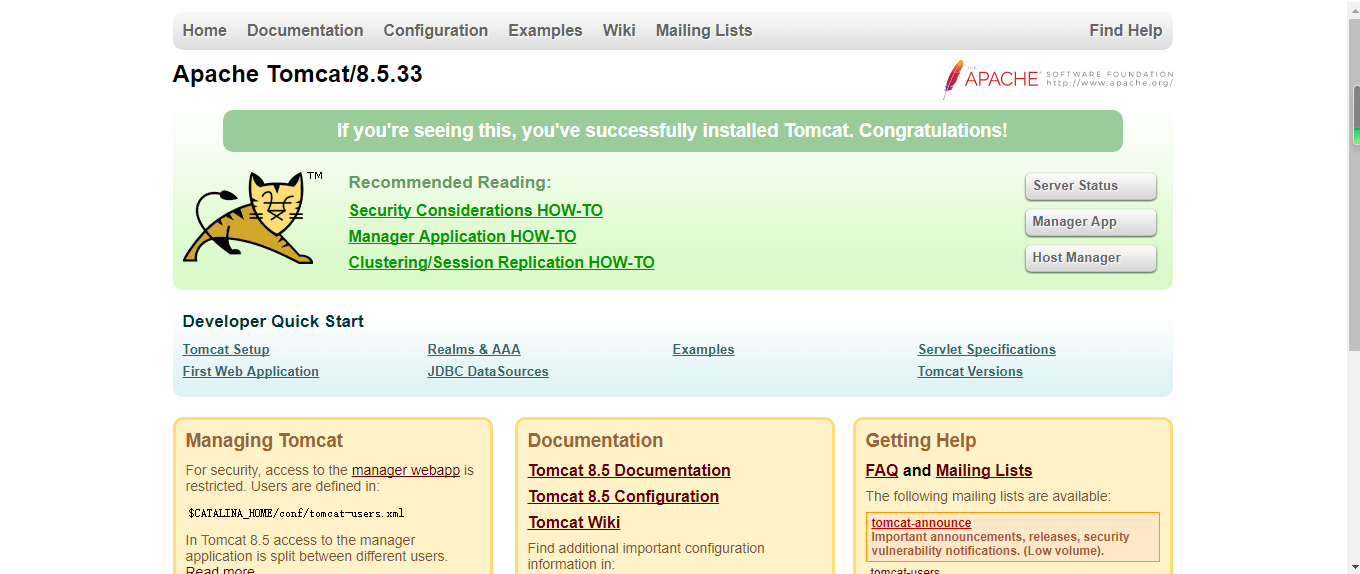
1. 访问路径<https://localhost:8443/> 出现以下页面，说明配置成功。



1. 忽略端口的访问方式, 在互联网上, http协议的默认端口是80, https的默认端口是443, 这里将端口改为了443,重启tomcat即可忽略端口进行访问。



E,输入<https://localhost/> 如果出现以下页面表示访问成功。



f.至此配置成功，关于访问路径不安全，参阅了大量资料之后，必须要花钱去认证证书，网上的很多办法都行不通。