**WEB**

# 简介

## 相关知识

Web即网页，提供给人们访问的。

**Web资源分为：**

静态web资源(如html页面): 指web页面中供人们浏览的数据始终是不变的

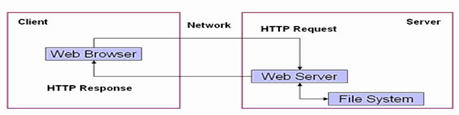
动态web资源： 指web页面中供人们浏览的数据是由程序产生的,不同的时间点访问web页面看到的内容各不相同。

## Web应用程序

Web应用程序指供浏览器访问的程序，通常也简称为web应用。例如有：a.html、b.html

Web应用开发好之后，若想提供外界访问，需要把web应用程序所在的目录交给web服务器管理，这个过程称之为虚拟目录的映射。

### 静态资源

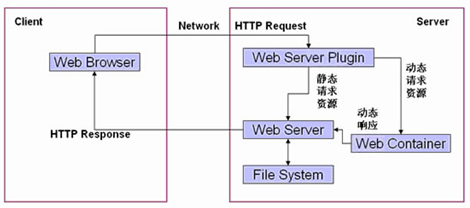


静态资源是用户通过浏览器请求web服务器，web服务器根据用户需求取出内容后返回给浏览器，浏览器经过渲染展现给用户

**缺点：**

* **Web页面内容无法更新**
* **静态页面无法访问数据库**

### 动态资源

****

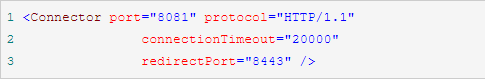
动态资源是指页面可以和用户进行交互，一般情况下用户请求页面，web服务器会根据用户的需求查询数据库的数据，将特定的数据返回给用户，结合JS实现动态的效果。

## Web服务器

Web服务器是一个计算机中的一个应用程序，用于用户发送的请求

# Tomcat服务器

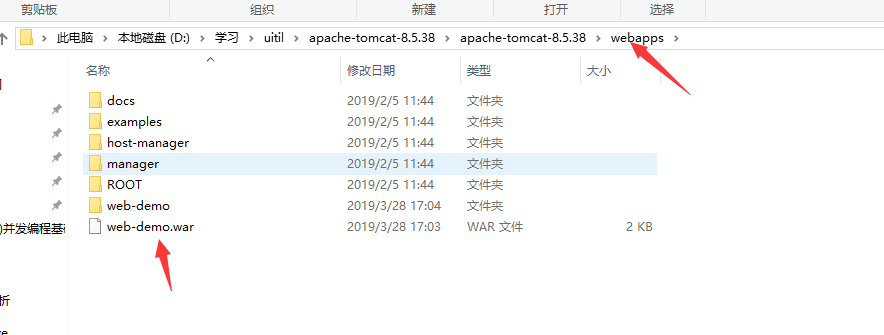
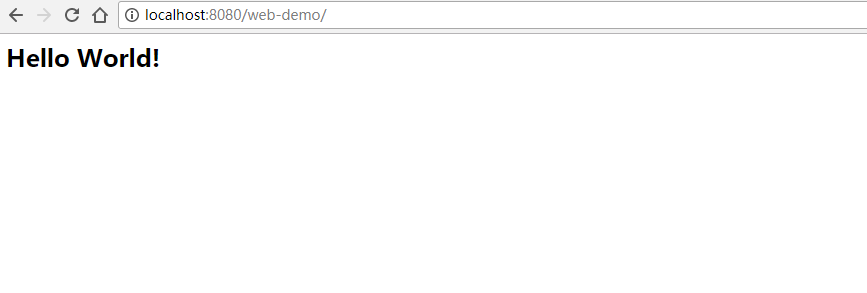
## 服务器端口配置

**将Tomcat服务器启动端口修改成8081端口**

## 服务器虚拟目录映射

**Web应用开发好后，若想供外界访问，需要把web应用所在的目录交给web服务器管理，这个过程称之为虚拟目录的映射。**

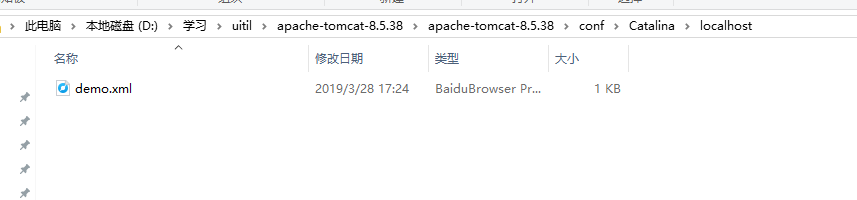
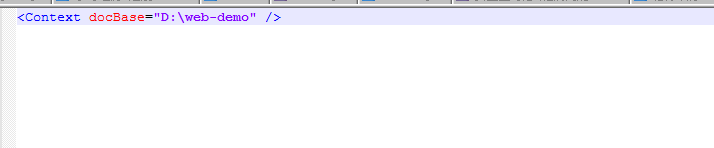
### tomcat服务器自动映射

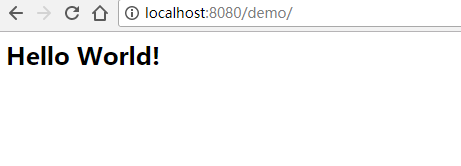
　tomcat服务器会自动管理webapps目录下的所有web应用，并把它映射成虚似目录。换句话说，tomcat服务器webapps目录中的web应用，外界可以直接访问。

### 方法二

在tomcat服务器的\conf\Catalina\localhost目录下添加一个以xml作为扩展名的文件，xml文件的名字可以任意取，比如下面的aa.xml，注意这一句话"**The context path and version will be derived from the base name of the file**"，这一句话的意思翻译过来就是"context元素的path属性源自于是这个xml文件的名字"，上面提到过，Context元素的path属性是用来配置虚似目录的名称的，所以虚似目录的名称就是这个xml文件的名称。

　　$CATALINA\_BASE指的就是tomcat服务器根目录，[enginename]指的是Tomcat服务器使用的引擎名称，Tomcat使用的引擎是Catalina

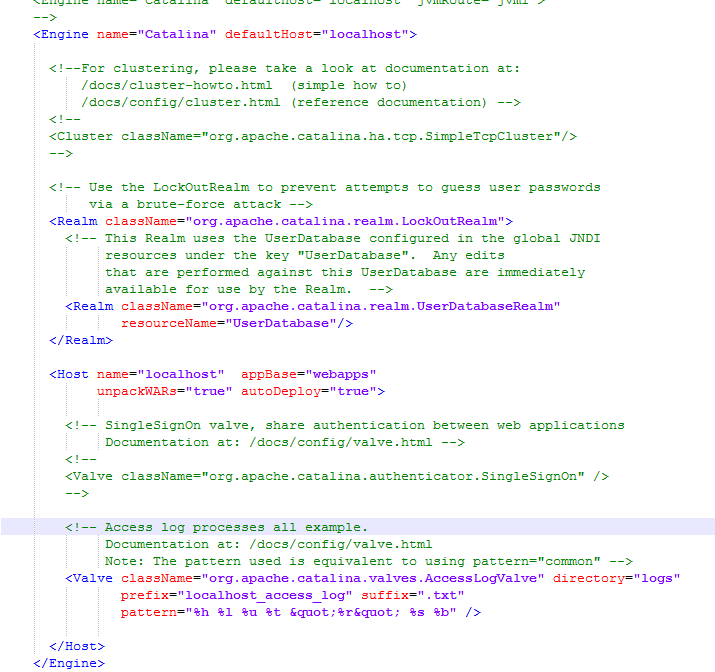


 Xml的文件名就是应用的虚拟目录。

## 配置虚拟主机

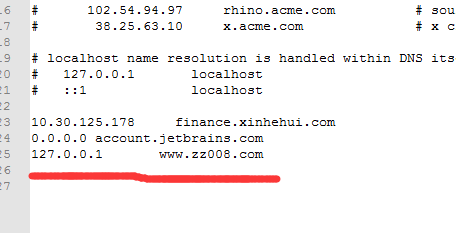
配置虚似主机就是配置一个网站。  
　　在Tomcat服务器配置一个虚拟主机(网站)，需要修改conf文件夹下的server.xml这个配置文件，使用Host元素进行配置，打开server.xml，可以看到Tomcat服务器自带的一个名称为localhost的虚拟主机(网站)

平时我们将开发好的JavaWeb应用放到webapps文件夹下，然后就可以使用"**http://localhost:端口号/demo**"的方式去访问了，其实访问的就是name是"localhost"的那台虚拟主机(Host)，这台虚拟主机管理webapps文件夹下的所有web应用。

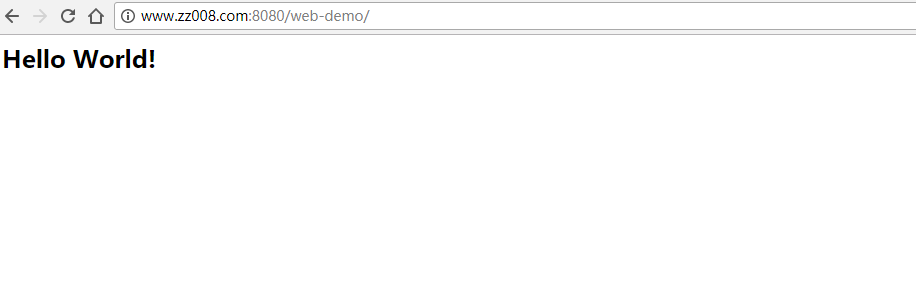
新建一个虚拟主机：

　　 这里我们新配置一个虚拟主机，虚拟主机的name是"www.zz008.com"，虚拟主机" www.zz008.com "现在管理着webapps文件夹下的所有web应用，平时我们在互联网上使用域名"www.baidu.com"访问百度的网站时，其实就是在访问一个名称是"www.baidu.com"的虚拟主机，所以当我们要访问name是" www.zz008.com "的这个虚拟主机时，就可以使用"域名(www.zz008.com)"去访问，注意一下appBase="D:\learn\webapps"，这里的webapps文件夹代表的不是一个项目的根目录，而是一个存放了一个或者多个JavaWeb应用的文件夹

不过要想访问[www.zz008.com这个域名还得修改host](http://www.zz008.com这个域名还得修改host)文件:

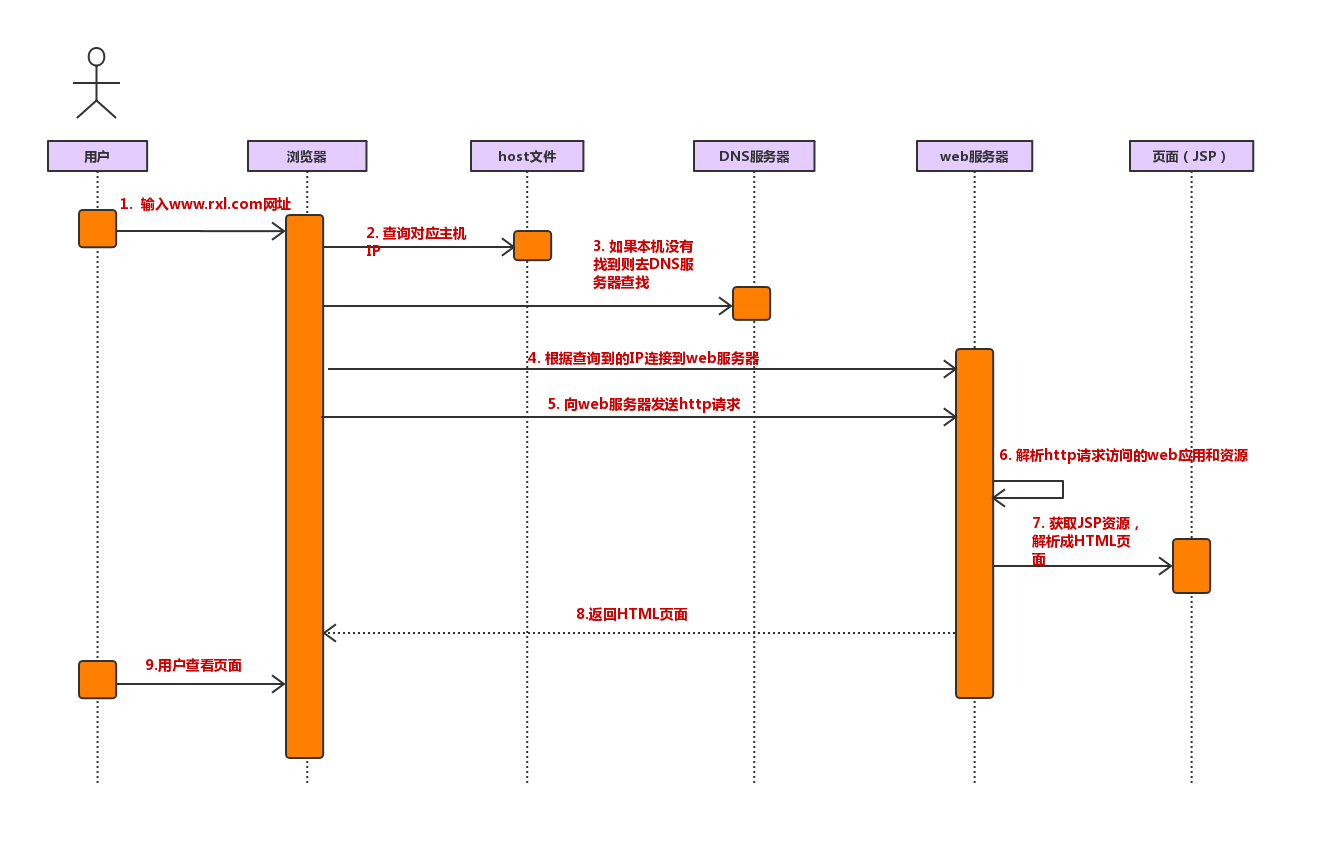


最后就可以访问了:

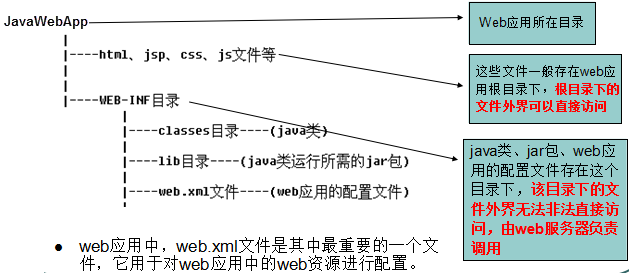


## 浏览器与服务器交互过程

**如图：**



## JavaWeb应用的组成结构



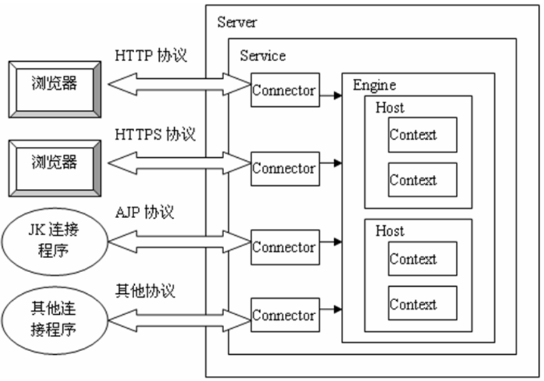
WebRoot →Web应用所在目录，一般情况下虚拟目录要配置到此文件夹当中。

　　　　┝WEB-INF：**此文件夹必须位于WebRoot文件夹里面，而且必须以这样的形式去命名，字母都要大写。**

　　　　　　┝web.xml：**配置文件，有格式要求，此文件必须以这样的形式去命名，并且必须放置到WEB-INF文件夹中。**

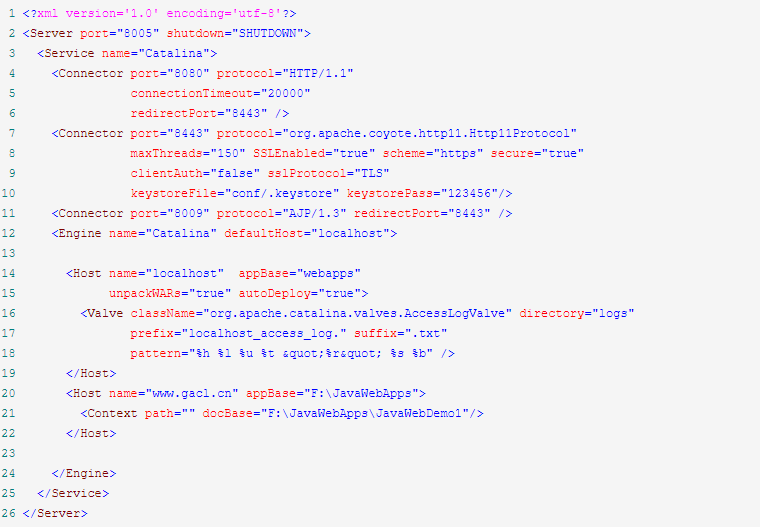
　　web.xml的格式可以直接从Tomcat中参考得到：找到Tomcat目录下的webapps\ROOT\WEB-INF这个目录下的web.xml文件，把这个文件拷贝到我们新建的WEB-INF文件夹中，并修改这个web.xml文件，把里面的注释删除掉，只留下如下所示的代码即可：

## Tomcat体系结构



Tomcat服务器的启动是**基于一个server.xml**文件的，Tomcat启动的时候**首先会启动一个Server**，Server里面就会启动Service，Service里面就会启动多个"Connector(连接器)"，每一个连接器都在等待客户机的连接，当有用户使用浏览器去访问服务器上面的web资源时，首先是连接到Connector(连接器)，Connector(连接器)是不处理用户的请求的，而是将用户的请求交给一个Engine(引擎)去处理，Engine(引擎)接收到请求后就会解析用户想要访问的Host，然后将请求交给相应的Host，Host收到请求后就会解析出用户想要访问这个Host下面的哪一个Web应用,一个web应用对应一个Context。

## 互联网上的加密原理

Tomcat服务器启动时候会启动多个Connector(连接器)，而Tomcat服务器的连接器又分为加密连接器和非加密连机器，比如：

### 1. 对称加密

采用单钥密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密，这种加密方法称为对称加密，也称为单密钥加密。

　　需要对加密和解密使用相同密钥的加密算法。由于其速度快，对称性加密通常在消息发送方需要加密大量数据时使用。对称性加密也称为密钥加密。

　　所谓对称，就是采用这种加密方法的双方使用方式用同样的密钥进行加密和解密。密钥是控制加密及解密过程的指令。算法是一组规则，规定如何进行加密和解密。

　　加密的安全性不仅取决于加密算法本身，密钥管理的安全性更是重要。**因为加密和解密都使用同一个密钥，如何把密钥安全地传递到解密者手上就成了必须要解决的问题**。

　　常用的对称加密有：DES、IDEA、RC2、RC4、SKIPJACK、RC5、AES算法等

### 2. 非对称加密

非对称加密算法需要两个密钥：**公开密钥（publickey）**和**私有密钥（privatekey）**。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。 非对称加密算法实现机密信息交换的基本过程是：甲方生成一对密钥并将其中的一把作为公用密钥向其它方公开；得到该公用密钥的乙方使用该密钥对机密信息进行加密后再发送给甲方；甲方再用自己保存的另一把专用密钥对加密后的信息进行解密。另一方面，甲方可以使用乙方的公钥对机密信息进行签名后再发送给乙方；乙方再用自己的私匙对数据进行验签。

#### 非对称加密工作原理

　　1.A要向B发送信息，A和B都要产生一对用于加密和解密的公钥和私钥。

　　2.A的私钥保密，A的公钥告诉B；B的私钥保密，B的公钥告诉A。

　　3.A要给B发送信息时，A用B的公钥加密信息，因为A知道B的公钥。

　　4.A将这个消息发给B（已经用B的公钥加密消息）。

　　5.B收到这个消息后，B用自己的私钥解密A的消息。其他所有收到这个报文的人都无法解密，因为只有B才有B的私钥

　　发送方使用接收方的公钥对数据加密，而接收方则使用自己的私钥解密，这样，信息就可以安全无误地到达目的地了，即使被第三方截获，由于没有相应的私钥，也无法进行解密。通过数字的手段保证加密过程是一个不可逆过程，即只有用私有密钥才能解密。

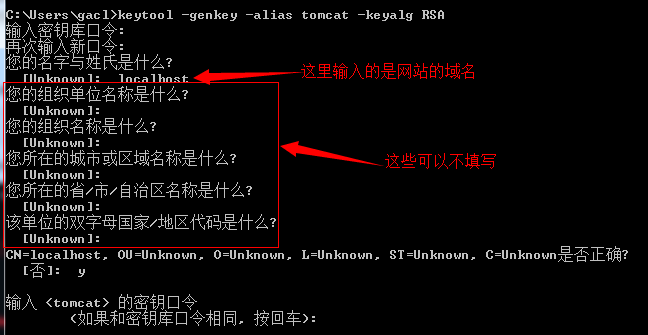
　　非对称性加密依然没有解决数据传输的安全性问题，比如A想向B发数据，B首先生成一对密钥(公钥和私钥)，然后将公钥发给A，A拿到B发给他的公钥有就可以使用公钥加密数据后发给B，然而在B公钥发送给A的这个过程中，很有可能会被第三方C截获，C截获到B的公钥后，也使用B的公钥加密数据，然后发给B，B接收到数据后就晕了，因为搞不清楚接收到的数据到底是A发的还是C发的，这是其中一个问题，另一个问题就是，C截获到B发的公钥后，C可以自己生成一对密钥(公钥和私钥)，然后发给A，A拿到公钥后就以为是B发给他的，然后就使用公钥加密数据发给B，发送给B的过程中被C截获下来，由于A是用C发给他的公钥加密数据的，而C有私钥，因此就可以解密A加密过后的内容了，而B接收到A发给他的数据后反而解不开了，因为数据是用C的公钥加密的，B没有C的私钥，所以就无法解密。所以，**非对称性加密存在一个问题：A想向B发数据，A如何确定拿到的公钥一定是B发的呢？那么如何解决这个问题呢？只能靠一个第三方机构(CA机构，即证书授权中心(Certificate Authority )，或称证书授权机构)来担保。A想向B发数据，B首先将公钥发给CA机构，CA机构拿到B的公钥后跑到B的家里问：这是你发的公钥吗？B确认过后说是：没错，是我发的！那么此时CA机构就会为B的公钥做担保，生成一份数字证书给B，数字证书包含了CA的担保认证签名和B的公钥，B拿到CA的这份数字证书后，就发给A，A拿到数字证书后，看到上面有CA的签名，就可以确定当前拿到的公钥是B发的，那么就可以放心大胆地使用公钥加密数据，然后发给B了。**

## https连接器

### 生成Tomcat服务器的数字证书

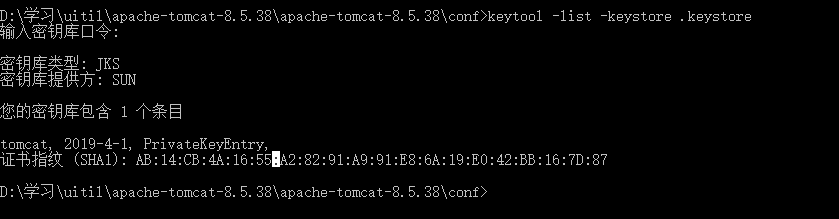
　　SUN公司提供了制作证书的工具keytool， 在JDK 1.4以后的版本中都包含了这一工具，它的位置为<JAVA\_HOME>\bin\keytool.exe

**keytool -genkey -alias tomcat -keyalg RSA**

使用keytool生成一个名字为tomcat的证书,存放在.keystore这个密钥库中

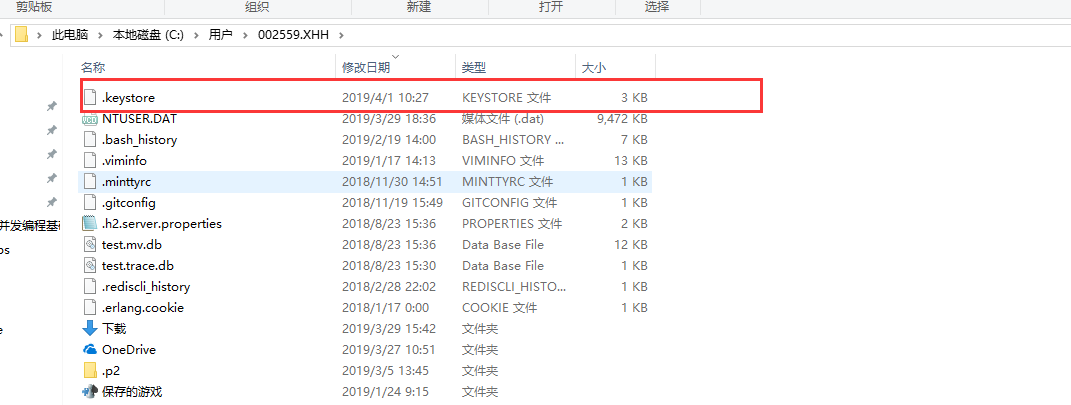
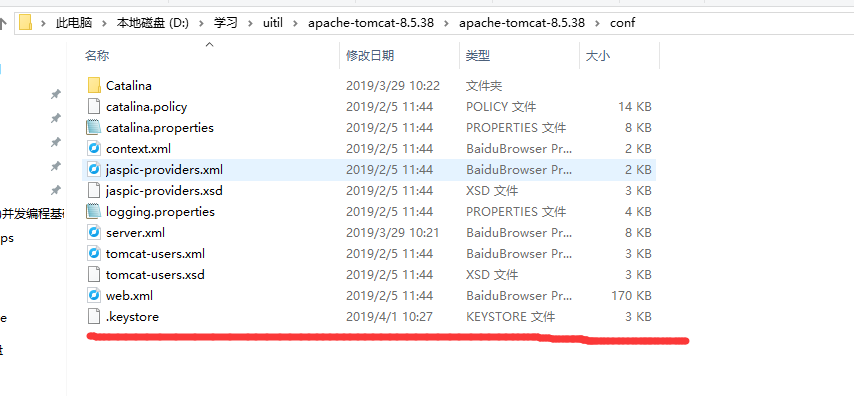
命令执行完之后，操作系统的用户文件夹下面就会生成一个.keystore文件：

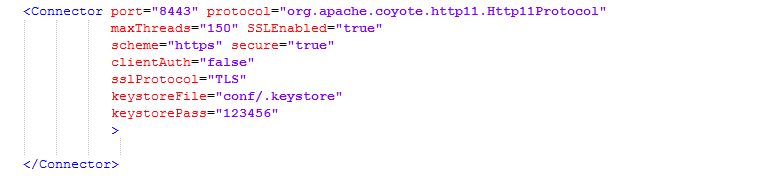
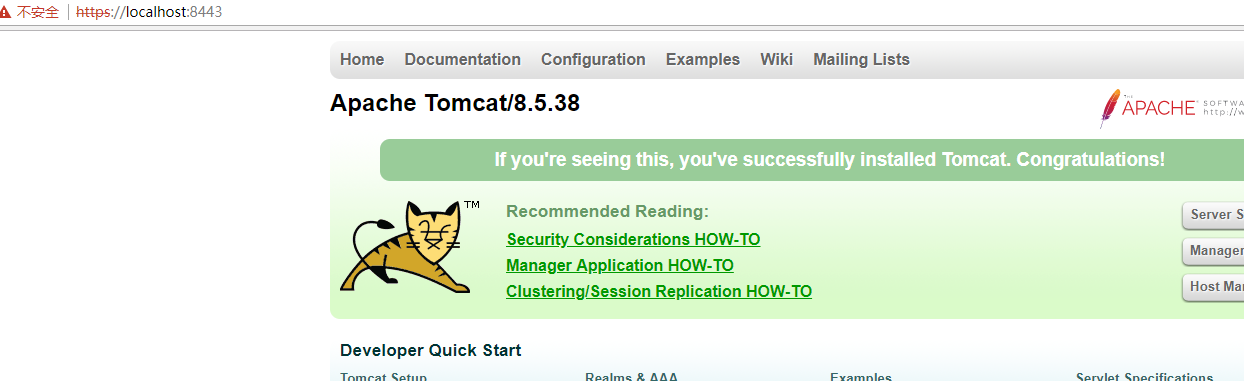
使用命令：**keytool -list -keystore .keystore**

查看.keystore密钥库里面的所有证书

### 配置https连接器

1. **将生成的.keystore密钥库文件拷贝到Tomcat服务器的conf目录下：**



1. **修改server.xml文件，配置https连接器：**
2. **在server.xml文件中配置了一个端口是8443的加密连接器，浏览器访问8443端口的连接器时，将会以加密的方式来访问web服务器，这个连接器收到浏览器的请求后，将会向浏览器出示一份数字证书，浏览器再用数字证书里面的公钥来加密数据，keystoreFile="conf/.keystore" 用来指明密钥库文件的所在路径，服务器从密钥库中提取证书时需要密码，keystorePass="123456"指明密钥库的访问密码。**
3. **使用"https://localhost:8443/"访问8443的加密连接器**

### 安装数字证书

# Http协议

## 什么是HTTP协议

HTTP是hypertext transfer protocol（超文本传输协议）的简写，它是TCP/IP协议的一个应用层协议，用于定义WEB浏览器与WEB服务器之间交换数据的过程。客户端连上web服务器后，若想获得web服务器中的某个web资源，需遵守一定的通讯格式，**HTTP协议用于定义客户端与web服务器通迅的格式。**

## HTTP协议的版本

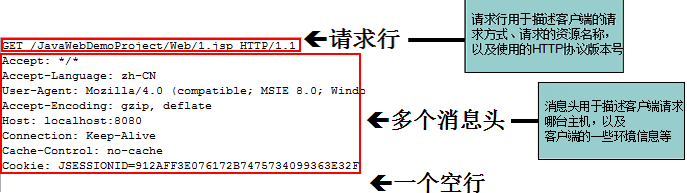
**HTTP/1.0 :** 客户端与web服务器建立连接后，只能获得一个web资源

**HTTP/1.1：**允许客户端与web服务器建立连接后，在一个连接上获取多个web资源。

## HTTP请求

**客户端连上服务器后，向服务器请求某个web资源，称之为客户端向服务器发送了一个HTTP请求**。

一个完整的HTTP请求包括如下内容：**一个请求行、若干消息头、以及实体内容**



### 请求行

请求行中的GET称之为请求方式，请求方式有： POST、GET、HEAD、OPTIONS、DELETE、TRACE、PUT，常用的有： GET、 POST  
　　用户如果没有设置，默认情况下浏览器向服务器发送的都是get请求，例如在浏览器直接输地址访问，点超链接访问等都是get，用户如想把请求方式改为post，可通过更改表单的提交方式实现。  
　　不管POST或GET，都用于向服务器请求某个WEB资源，这两种方式的区别主要表现在数据传递上：如果请求方式为GET方式，则可以在请求的URL地址后以?的形式带上交给服务器的数据，多个数据之间以&进行分隔，例如：GET /mail/1.html?name=abc&password=xyz HTTP/1.1  
　　GET方式的特点：在URL地址后附带的参数是有限制的，**其数据容量通常不能超过1K。**  
　　如果请求方式为POST方式，则可以在请求的实体内容中向服务器发送数据，Post方式的特点**：传送的数据量无限制。**

### 消息头

HTTP请求中的常用消息头:

**Accept:** 浏览器通过这个头告诉服务器，它所支持的数据类型。

**Accept-Charset：**浏览器告诉服务器，它支持哪种字符集

**Accept-Encoding:** 浏览器告诉服务器，它的语言环境

**Host:** 告诉服务器，想访问哪台主机

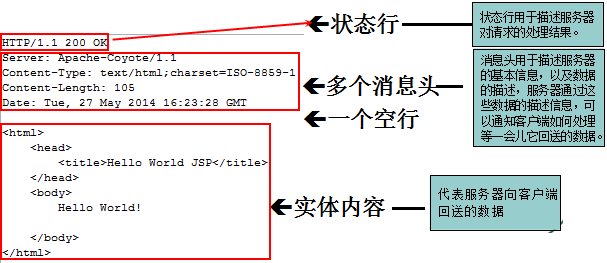
**If-Modified-Since：**浏览器告诉服务器，缓存数据的时间

**Referer:** 告诉服务器，客户机是哪个页面来的，防盗链

**Connection**: 告诉服务器,请求完后是断开链接还是保持链接

## HTTP响应

**一个HTTP响应代表服务器向客户端回送的数据**，它包括： 一个状态行、若干消息头、以及实体内容 。



### 状态行

**状态行格式：** **HTTP版本号　状态码　原因叙述<CRLF>**

 举例：HTTP/1.1 200 OK

状态码用于表示服务器对请求的处理结果，它是一个三位的十进制数。响应状态码分为5类，

