作业四: SSL

第一部分 代码部分

将8080的Http转发到8443的端口代码:通过connector实现如下!

```
1
 2
    @SpringBootApplication
    public class EBookBackendApplication {
 3
 4
 5
        @Bean
        public TomcatServletWebServerFactory tomcatServletWebServerFactory(Connector
 6
    connector) {
 7
            TomcatServletWebServerFactory tomcat=new TomcatServletWebServerFactory(){
 8
                @Override
 9
                protected void postProcessContext(Context context) {
                     SecurityConstraint securityConstraint=new SecurityConstraint();
10
                     securityConstraint.setUserConstraint("CONFIDENTIAL");
11
                     SecurityCollection collection=new SecurityCollection();
12
                     collection.addPattern("/*");
13
14
                     securityConstraint.addCollection(collection);
15
                     context.addConstraint(securityConstraint);
16
17
                }
18
19
            };
20
            tomcat.addAdditionalTomcatConnectors(connector);
21
            return tomcat;
22
        }
23
        @Bean
2.4
        public Connector connector(){
25
            Connector connector=new
    Connector("org.apache.coyote.http11.Http11NioProtocol");
            connector.setScheme("http");
2.6
            connector.setPort(8080);
27
            //Set the secure connection flag that will be assigned to requests
28
    received through this connector.
29
            //@param secure The new secure connection flag
            //if connector.setSecure(true), the http use the http and https use the
30
    https;
31
            // else if connector.setSecure(false),the http redirect to https;
            connector.setSecure(false);
32
            connector.setRedirectPort(8443);
3.3
34
            connector.setAllowTrace(true);
35
36
            return connector;
37
        }
38
```

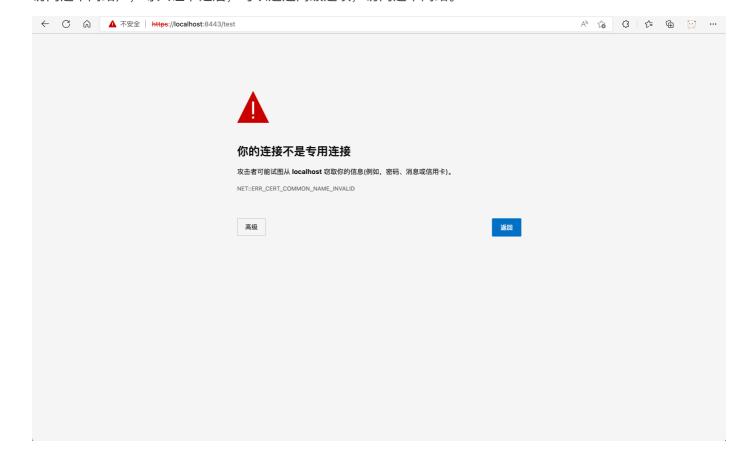
第二部分 问题回答

HTTPS 通信方式与HTTP 通信方式的差异:

- HTTP是明文传输内容的,可能会被截获,不安全。HTTPs的传输内容经过了公钥的加密,所以更安全。
- 默认的端口不一样,HTTP默认端口80,HTTPS默认443,对应后端的分别是8080和8443端口
- 使用 HTTPS 协议需要到 CA(Certificate Authority,数字证书认证机构) 申请证书,一般免费证书较少,因而需要一定费用。证书颁发机构如:Symantec、Comodo、GoDaddy 和 GlobalSign 等。
- HTTPS 其实就是建构在 SSL/TLS 之上的 HTTP 协议,所以,要比较 HTTPS 比 HTTP 要更耗费服务器资源。

解释为什么会出现和之前只使用HTTP 时的差异,为什么需要导入证书才能正常访问,并且将你生成证书和导入证书的过程,用Shell 命令和截图进行说明。

之前只使用HTTP的时候,浏览器的标识处写的是不安全,现在用了自己签名的证书后,Edge提示的是红色的不安全,Safari没有不安全提示(证书已经导入到了系统中)。Safari是系统自带的浏览器可以读取相关的证书目录发现是用户自己的证书所以信任,Edge在未导入证书之前的情况是完全不能访问的(也就是没有任何按钮可以强制访问这个网站),导入证书之后,可以通过高级选项,访问这个网站。



自签名证书容易受到SSL中间人攻击,所以自签名证书是不会被浏览器所信任的证书,用户在访问自签证书时,浏览器会警告用户此证书不受信任,需要人工确认是否信任此证书。所有使用自签证书的网站都明确地告诉用户出现这种情况,用户必须点信任才可以继续浏览。

关于为什么需要导入证书才能正常访问,浏览器在访问网站的时候详细的过程如下:

- 首先浏览器通过URL网址去请求服务端,服务端接收到请求后,就会给浏览器发送一个自己的证书
- 浏览器接收到证书以后,就要开始进行验证工作了。首先从证书中得知证书的颁发机构,然后从浏览器系统中去寻找此颁发机构的根证书。CA机构的根证书都是预先嵌入到浏览器中的,如果在浏览器系中没有找到对应的根证书,就代表此机构不是受信任的,那么就会警告无法确认证书的真假。
- 如果是在系统中找到了相关的证书,但是考虑到这个证书是自签名的,所以会提示用户是否信任网站
- 否则找不到的话,就可能会强制阻止访问网站。

所以综上所述,需要导入证书才能正常访问。

第三部分 步骤解释

第一步: 产生keystore文件

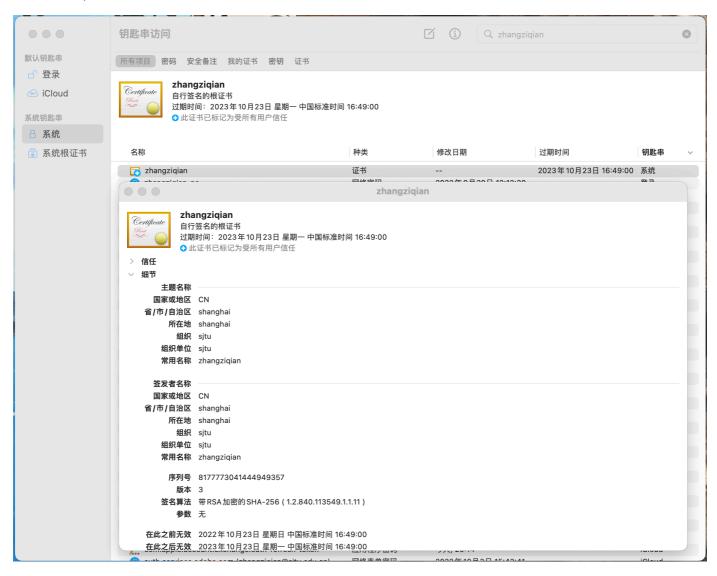
```
zhangzigian@zhangzigiandeMac-Studio /bin % keytool -genkey -v -keystore
   zzq.keystore -alias zhangziqian -keyalg RSA -validity 365 -keystore
   /Users/zhangziqian/Desktop/zzq.keystore
2
   输入密钥库口令:
   再次输入新口令:
3
4
   Warning:
   多次指定了 -keystore 选项。除最后一个之外, 其余的将全部忽略。
5
   您的名字与姓氏是什么?
 6
7
     [Unknown]: zhangzigian
   您的组织单位名称是什么?
8
9
     [Unknown]: situ
   您的组织名称是什么?
10
     [Unknown]: sjtu
11
   您所在的城市或区域名称是什么?
12
     [Unknown]: shanghai
13
   您所在的省/市/自治区名称是什么?
14
     [Unknown]: shanghai
15
16
   该单位的双字母国家/地区代码是什么?
17
     [Unknown]: CN
18
   CN=zhangziqian, OU=sjtu, O=sjtu, L=shanghai, ST=shanghai, C=CN是否正确?
     [否]: 是
19
2.0
21
   正在为以下对象生成 2,048 位RSA密钥对和自签名证书 (SHA256withRSA) (有效期为 365 天):
2.2
      CN=zhangziqian, OU=sjtu, O=sjtu, L=shanghai, ST=shanghai, C=CN
   [正在存储/Users/zhangziqian/Desktop/zzq.keystore]
2.3
```

第二步: 导出cer后缀的证书

- zhangziqian@zhangziqiandeMac-Studio key % keytool -export -alias zhangziqian keystore ./zzq.keystore -rfc -file ./zzq.cer
- 2 输入密钥库口令:
- 3 存储在文件 <./zzg.cer> 中的证书

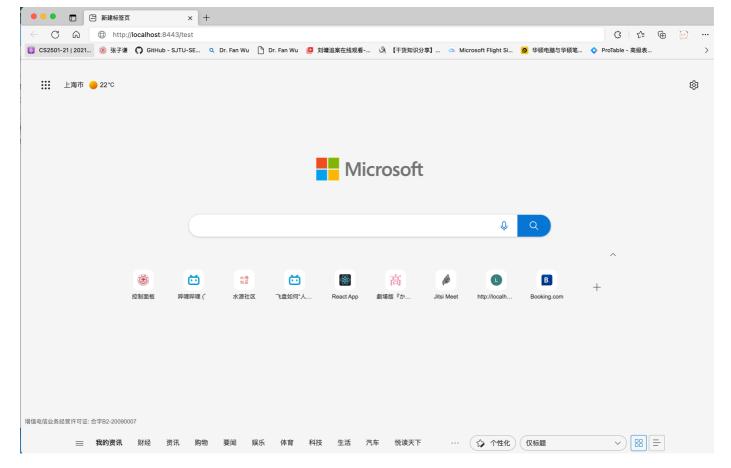
第三步: 导入系统

如下图所示,导入后的结果可以在钥匙串中看到!



第四步: 打开浏览器访问测试接口

Edge的截图如下:



回车访问,发现被重定向到了8443



[{"belonguser":"user7","chileItem":[{"belonguser":"user7","bookID":2,"bookinfo":{"ID":2,"ISBN":"978-7-000-00001-1","author":"这就是物理编者","bookname":"这就是物理。","departure":"武汉","description":"这套书叫做《这就是物理》,一共有10本、涵盖了物质、磁性、光、电、能量、引力、热、声音、力与运动等十大物理主题,几乎震括了学校学过的全部物理知识点、\r\n\r\n书中通过权人化的情景。趣味性的语言,深入浅出地把物理概念解释得清楚到位,最重要的是,卡通人物的手绘,漫画风格的板式,孩子们都爱看。\r\n\r\n物理是我们认识世界的基础。如果你的家里也有一个好奇宝宝,每天都要问一堆的为什么,比如,为什么温度计能测量温度,为什么脱毛农时会有"解谢"的声音,为什么下雨天总是先看到内电后听到雷声,你能解释清楚吗?\r\n\r\n在这套书中,孩子们在生活中的"十万个为什么"都能找到答案,","displaytitle": "【热钥】这就是物理,小学科普物理读物 知识百科全书","imgtitle":"https://myebookpicture.oss-cn-hangzhou.aliyuncs.com/image/2.jpg","inventory":259,"price":1825,"publisher":"科学出版

予。, "Indiction: inttps://myebookpicture.oss-com-nanganou.aliyuncs.com/image/2.jpg , inventory :227, pinter :225, puntions: - 「「アンロの (**) punum:27 (**) pun

育", "imgtitle": "https://myebookpicture.oss-cn-hangzhou.aliyuncs.com/image/15.jpg", "inventory":93, "price":5221, "publisher": "科学出版

**, "seln.umbher":20), "buyunum":5, "comment": "", "create_itemtime":
{"date":8, "day":5, "hours":0, "minutes":57, "month":6, "nanos":0, "seconds":34, "time":1657213054000, "timezoneOffset":-480, "year":122}, "itemID":50, "orderID":18, "payprice":26105, "status":2, "bo oktitle": "大级交流真题试卷考试单词测: "Hours":0, "booking": "https://myebookpicture.oss-cn-hangzhou.aliyuncs.com/image/15.jpg"}], "contactphone": "11111113333", "create_time":
{"date":8, "day":5, "hours":0, "minutes":57, "month":6, "nanos":0, "seconds":34, "time":1657213054000, "timezoneOffset":-480, "year":122), "destination": "tom3的住
ff", "orderID":18, "postalcode": "400000", "receivername": "TomN", "totalprice":26105), ("belonguser": "user7", "chileItem":{{"belonguser": "user7", "booklinfo":{"ID":15, "booklinfo":{"ID":15,

育","imgtitle":"https://myebookpicture.oss-cn-hangzhou.aliyuncs.com/image/15.jpg", inventory":93, "price":5221, "publisher":"科学出版

社","sellnumber":20),"buynum":2,"comment":"","create_Itemtime":
{"date':7,'day":4,"hours":0,"minutes':3,"month":6,"nanos":0,"seconds':40,"time":1657123420000,"timezoneOffset":-480,"year":122),"itemID":42,"orderID":23,"payprice":5221,"status":2,"book
title":"六级英语真题试卷考试单词词汇书历年模拟题卷子练习题大学6级听力阅读专项训练火星标学教育","bookurl":"https://myebookpicture.oss-cn-hangzhou.aliyuncs.com/image/15.jpg"),
{"belonguser":"user?","booktD":2,"bookinfo":("ID":2,"ISBN":"978-7-000-00001-1","author":"这就是物理","bookurl":"bookmen":"这就是物理","departure":"近次","departure":"近次","description":这套书叫做《这就是物理》,一共
有10本、海笔7物质、磁性、光、电、能量、引力、热、声音、力与运动等十大物理主题。几乎看括了学验白金物地理知识点,L<\n\n\n+中通过以从CM的情景,越味性的语言。深入进出地地物理理会解释得清楚的(最重要的是,卡遇人物的手 会,漫画风格的版式,孩子们都爱看。\r\n\r\n物理是我们认识世界的基础。如果你的家里也有一个好奇宝宝,每天都要问一堆的为什么,比如,为什么温度计能测量温度,为什么脱毛农时会有"噼啪"的声音,为什么下雨天总是先看到闪电后听到雷 声,你能解释清楚吗?\r\n\r\n在这套书中,孩子们在生活中的"十万个为什么"都能找到答案。"displaytitle":" [热铜]这就是物理 小学有器物理读物 知识百科全书","imgtitle":"https://myebookpicture.oss-cn-hangshou.aliyuncs.com/image/2.jpg","inventory":259,"price":1825,"publisher":"科学出版社","sellnumber":20),"buynum":1,"comenter!"","""oreate_Itemtime":
{"date":7,"day":4,"hours":0,"minutes":3,"month":6,"nanos":0,"seconds":43,"time":1657123423000,"timezoneOffset":-480,"year":122),"itemID":43,"orderID":23,"payprice":1220,"status":2,"book
title":"[选辑]这就是物理 小学科普物理读物 知识百科全书","hours":0,"minutes":3,"month":6,"nanos":0,"seconds":43,"time":1657123423000,"timezoneOffset":-480,"year":122),"itemID":43,"orderID":23,"payprice":1220,"status":2,"book
title":"[选辑]这就是物理 小学科普物理读物 知识百科全书","bookurl":"https://myebookpicture.oss-cn-hangzhou.aliyuncs.com/image/2.jpg",("belonguser":"user7","bookDD":8,"bookhanfo':
{"ID":8,"ESSN*:"978-00-000007-7","author":"May 5,"bookhanfo':
{"ID":8,"ESSN*:"988-2-000-00007-7","author":"May 5,"bookhanfo':
{"ID":8,"ESSN*:"988-2-000-00007-7","author":"May 5,"bookhanfo':
{"ID":8,"ESSN*:"988-2-000-00007-7","author":"May 5,"bookhang*:"May 5,"bookhang*:"May 5,"bookhang*:"May

交大、哈工大等等,都对这门课给予了非常高的地位。其他学校不太了解,但是给工大16级课改,直接用这门课取代了计算机组成原理,便知道唐奶奶的计组书有多出名)而且高达5个学分,可见这门课的重要性。","displaytitle":"2022全新 深入期解计算机系统·计算机机器 打包销售","加度计记论":"加度订记》:"批估工作,此时,是一个"批估工业出版社出版","sellnumber":22),"buynum":2,"comment":""",create_Itemtime":
{"date":5, "day ":3, "hours":22, "minutes":6, "month":9, "nanos":0, "seconds":10, "time":1664978770000, "timezoneOffset":-480, "year":122), "itemID":60, "orderID":23, "payprice":3222, "status":2, "boo ktitle":"2022全新 深入理解计算机系统 计算机模型 "即记销售","bookburl":"https://myebookpicture.oss-cn-hangzhou.aliyuncs.com/image/8.jpg"), "contactphone":"11111113333", "create_time":
{"date":6, "day":4, "hours":0, "minutes":9, "month":9, "manos":0, "seconds":13, "time":1664986153000, "timezoneOffset":-480, "year":122}, "destination": "tom3的性 所","orderID":23, "postalcode":"dolongous":"rookiD":4, "bookinfo":("ID":4, "ISBN":"978-7-000-00003-3", "author":"人民日报出版社编写组", "booknme":"人民日报教你写文章,"departure":"北京", "description":"《人民日报教你写文章 技法与指导》,共分为5个大章节:立意、结构、选材、技法、语言,正好对应解决孩子写作 的5大规点、每个章节又分四个关键步骤:思维导弧、另外这次课,变战演练,让孩子学得居尼清晰。无论是《技法与指导》,还是《热点与素材》,都是在让孩子们学会官媒级别的写作技巧,并告诉孩子们,《人民日报》上的好文章,就是这

Safari可以识别系统的用户证书:

[{"belonguser":"user7","chileItem":[{"belonguser"

,"departure":"武汉","description":"这套书叫做《这就 \r\n\r\n书中通过拟人化的情景,趣味性的语言,深入浅出地把物 好奇宝宝,每天都要问一堆的为什么,比如,为什么温度计能测量流 为什么"都能找到答案。","displaytitle":"【热销】这就是物 hangzhou.aliyuncs.com/image/2.jpg","inventory":25 {"date":18, "day":6, "hours":20, "minutes":5, "month" e":2440, "status":2, "booktitle":" [热销] 这就是物理 /J {"belonguser":"user7","bookID":5,"bookinfo":{"ID" 践", "departure": "上海", "description": "", "displayti hangzhou.aliyuncs.com/image/5.jpg","inventory":23 {"date":18, "day":6, "hours":20, "minutes":5, "month" e":8919,"status":2,"booktitle":"密码编码学与网络安全 hangzhou.alivuncs.com/image/5.jpg"}], "contactphor {"date":18, "day":6, "hours":20, "minutes":5, "month" 所", "orderID":12, "postalcode": "400000", "receiverna {"ID":15,"ISBN":"978-7-000-00014-4","author":"本书 拟题卷子练习题大学6级听力阅读专项训练火星标学教育","imgti hangzhou.aliyuncs.com/image/15.jpg","inventory":9
{"date":8,"day":5,"hours":0,"minutes":57,"month": ::26105, "status":2, "booktitle": "六级英语真题试卷考试! hangzhou.aliyuncs.com/image/15.jpg"}], "contactpho {"date":8,"day":5,"hours":0,"minutes":57,"month": 所","orderID":18,"postalcode":"400000","receiverna {"ID":15,"ISBN":"978-7-000-00014-4","author":"本书 拟题卷子练习题大学6级听力阅读专项训练火星标学教育","imgti hangzhou.aliyuncs.com/image/15.jpg","inventory":9{"date":7,"day":4,"hours":0,"minutes":3,"month":6 :5221, "status": 2, "booktitle": "六级英语真题试卷考试单设 hangzhou.aliyuncs.com/image/15.jpg"},{"belonguser ',"departure":"武汉","description":"这套书叫做《这就 \r\n\r\n书中通过拟人化的情景,趣味性的语言,深入浅出地把物 好奇宝宝,每天都要问一堆的为什么,比如,为什么温度计能测量流 为什么"都能找到答案。","displaytitle":"【热销】这就是物 hangzhou.aliyuncs.com/image/2.jpg", "inventory":25 {"date":7,"day":4,"hours":0,"minutes":3,"month":6 Safari 浏览器正在使用 localhost 的加密连接。



使用数字证书进行加密后,在将信息发送到https网站localhost或从该网站发出信息时,信

zhangziqian zhangzigian 自行签名的根证书 过期时间: 2023年10月23日 星期一 中国标准时间 16:49:00 此证书已标记为受所有用户信任 信任 使用此证书时: 使用系统默认 ? 加密套接字协议层(SSL) 未指定值 X.509基本策略 未指定值 主题名称 国家或地区 CN 省/市/自治区 shangha 所在地 shanghai 组织 situ 组织单位 sjtu 常用名称 zhangziqian 签发者名称 国家或地区 CN 省/市/自治区 shangha 所在地 shanghai 组织 situ 组织单位 sjtu 常用名称 zhangziqian

"author":"这就是物理编者" 等十大物理主题, 几乎囊括了学村 \r\n\r\n物理是我们认识世 能解释清楚吗?\r\n\r\n在这套

"comment":"","create_It 480, "year": 122}, "itemID" -hangzhou.aliyuncs.com/i cname": "密码编码学与网络安全 tps://myebookpicture.oss :1, "comment": "", "create 480, "year": 122}, "itemID"

480, "year": 122}, "destina [{"belonguser":"user7" ,"displaytitle":"六级英语

,"comment":"","create_It
30,"year":122},"itemID": "https://myebookpicture

30, "year":122}, "destinat [{"belonguser":"user7" "displaytitle": "六级英语

,"comment":"","create_It
0,"year":122},"itemID":4 https://myebookpicture.c ,"author":"这就是物理编者 等十大物理主题, 几乎囊括了学村 \r\n\r\n物理是我们认识世界 能解释清楚吗? \r\n\r\n在这套 ss-cn-

"comment": "". "create It 0, "year":122}, "itemID":4

好

:1220,"status":2,"booktitle":"[热销]这就是物理 小学科普物理读物 知识百科全书","bookurl":"https://myebookpicture.oss-cn-hangzhou.aliyuncs.com/ima {"belonguser":"user7"."bookID":8."bookinfo":{"ID":8."ISBN":"978-7-000-00007-7"."author":"翻译者: XXX 编写者: ABC"."bookname":"深入理解计算机系统

隐藏证书