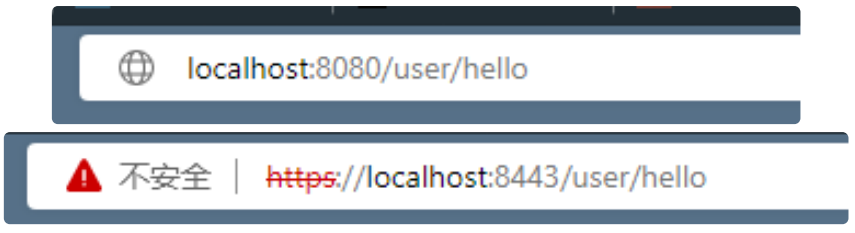
hw4

http 请求重定向

```
: id_test: partitions assigned: [topic1-0]
: id_test: partitions assigned: [topic2-0]
: Tomcat started on port(s): 8443 (https) 8080 (http) with context path ''
: Started BackendApplication in 4.061 seconds (JVM running for 5.138)
```

通过更改 SpringBoot 内置的 tomcat 的配置，为其增加一个监听 8080 端口 http 请求且转发给 https 请求的 8443 端口的 connector。

通过这个配置，所有访问 8080 端口的 http 请求都会被重定向到了 8443 端口，如下图所示：



由于本地没有导入服务器的证书，因此浏览器认为该网站是不安全的。

为何出现了与 http 的差异

使用了 `https` 通信后，当用户通过 `https` 请求服务器资源时，若用户没有该服务器提供的证书，则会认为该网站可能是不安全的，用户可以通过第三方机构提供的公钥对网站的证书进行解密，若能解开，则说明该网站的证书是经过该机构认证过的，是相对安全的，此时用户可以将该证书导入，浏览器便会认为该网站是安全的。

为何需要导入证书

为了提供对网站服务器的身份认证，保护交换数据的隐私与完整性，https 请求需要保证网站内容是真实而未被第三方修改过的，为了证明自己的身份，服务器端将自己的公钥交给第三方进行加密并颁发数字证书给用户，用户拿到服务器的数字证书后，通过第三方机构颁发的公开密钥进行解开就能验证证书的有效性以及公开密钥的真实性。

也就是说用户之所以需要导入证书是为了验证访问的服务器的身份。

证书制作流程

- 制作客户端密钥库

```
C:\Users\Feng>keytool -genkey -v -alias mykey -keyalg RSA -storetype PKCS12 -keystore D:\mykey.p12
输入密钥库口令:
再次输入新口令:
您的名字与姓氏是什么?
  [Unknown]:  Feng
您的组织单位名称是什么?
  [Unknown]:  SJTU
您的组织名称是什么?
  [Unknown]:  SJTU
您所在的城市或区域名称是什么?
  [Unknown]:  Shanghai
您所在的省/市/自治区名称是什么?
  [Unknown]:  Shanghai
该单位的双字母国家/地区代码是什么?
  [Unknown]:  CN
CN=Feng, OU=SJTU, O=SJTU, L=Shanghai, ST=Shanghai, C=CN是否正确?
  [否]:  y

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 90 天):
        CN=Feng, OU=SJTU, O=SJTU, L=Shanghai, ST=Shanghai, C=CN
[正在存储D:\mykey.p12]
```

- 制作服务端密钥库

```
C:\Users\Feng>keytool -genkey -v -alias tomcat -keyalg RSA -keystore D:\tomcat.keystore -validity 36500 -ext
SAN=dns:localhost,ip:127.0.0.1
输入密钥库口令:
再次输入新口令:
您的名字与姓氏是什么?
  [Unknown]:  Feng
您的组织单位名称是什么?
  [Unknown]:  SJTU
您的组织名称是什么?
  [Unknown]:  SJTU
您所在的城市或区域名称是什么?
  [Unknown]:  Shanghai
您所在的省/市/自治区名称是什么?
  [Unknown]:  Shanghai
该单位的双字母国家/地区代码是什么?
  [Unknown]:  CN
CN=Feng, OU=SJTU, O=SJTU, L=Shanghai, ST=Shanghai, C=CN是否正确?
  [否]:  y
```

- 客户端证书导入服务端密钥库：需要先从客户端密钥库导出证书，再将导出的证书导入服务端密钥库

```
C:\Users\Feng>keytool -import -v -file D:\mykey.cer -keystore D:\tomcat.keystore
输入密钥库口令:
所有者: CN=Feng, OU=SJTU, O=SJTU, L=Shanghai, ST=Shanghai, C=CN
发布者: CN=Feng, OU=SJTU, O=SJTU, L=Shanghai, ST=Shanghai, C=CN
序列号: 4b606b6
生效时间: Fri Oct 28 14:13:17 CST 2022, 失效时间: Thu Jan 26 14:13:17 CST 2023
证书指纹:
         SHA1: 3D:F7:8E:59:B8:72:0A:FF:4A:A7:1B:CC:38:F2:EF:77:86:EA:9E:BA
         SHA256: 76:B3:CF:CB:7C:1A:32:28:99:81:1F:67:63:8B:20:B5:EF:78:7C:4B:D5:79:B4:2E:1D:23:06:9A:BA:19:EB:AC
签名算法名称: SHA256withRSA
主体公共密钥算法: 2048 位 RSA 密钥
版本: 3

扩展:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 04 A9 22 31 74 2E 94 A6   8D 6A 03 A5 F0 4E 11 3E  ..."1t....j...N.>
0010: 0A BA F4 4F                                        ...O
]
]

是否信任此证书? [否]:  y
证书已添加到密钥库中
[正在存储D:\tomcat.keystore]
```

- 导出服务器端密钥库证书

```
C:\Users\Feng>keytool -keystore D:\tomcat.keystore -export -alias tomcat -file D:\tomcat.cer
输入密钥库口令:
存储在文件 <D:\tomcat.cer> 中的证书
```

证书导入

在本机安装客户端密钥库 `mykey.p12` 以及服务端证书 `tomcat.cer`，并将证书安装到“受信任的根证书颁发机构”。

- 以上操作完成后，发现已经可以“安全”地访问服务器资源