八方网域
bafangwy.com

Burp Suite基本使用

无涯老师

课程大纲

八方网域
bafangwy.com

1、Burp 下载和激活
2、Burp Suite代理配置
3、Burp Suite拦截HTTPS
4、Burp Repeater抓包与改包
5、Burp Intruder爆破密码

01 Burp 下载和激活

下载内容

八方网域
bafangwy.com

1、Burp 程序——建议使用jar包，更方便激活
https://portswigger.net/burp/releases

2、JDK——推荐11版本/解压
https://repo.huaweicloud.com/java/jdk/

3、激活jar包、汉化jar包——github
https://github.com/h3110w0r1d-y/BurpLoaderKeygen/releases

参考教程

八方网域
bafangwy.com

《31-Win10配置JDK8，启动BP.pdf》
《32-Win10配置JDK11，启动BP.pdf》 （推荐）

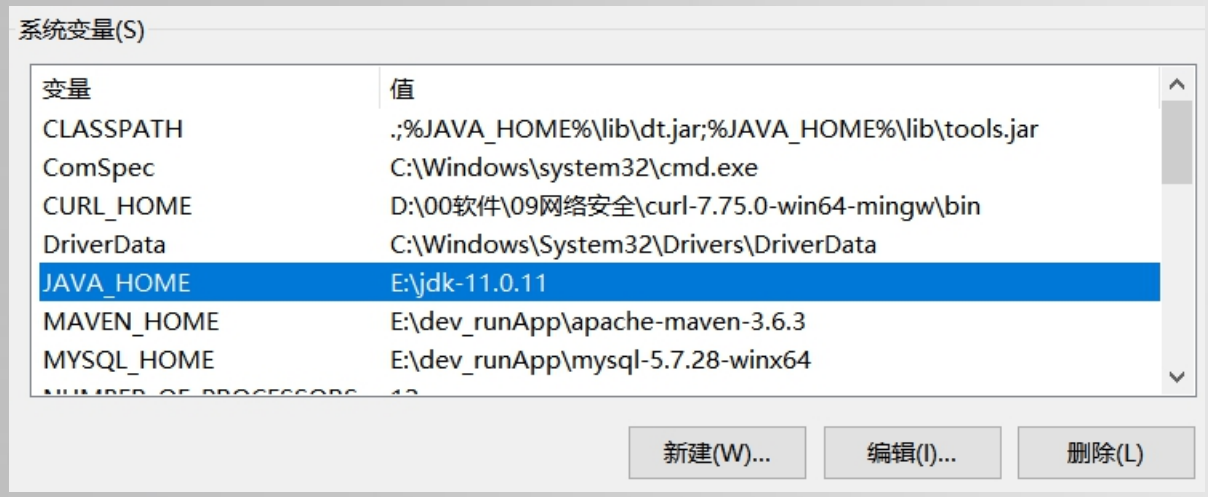
JDK8环境变量配置

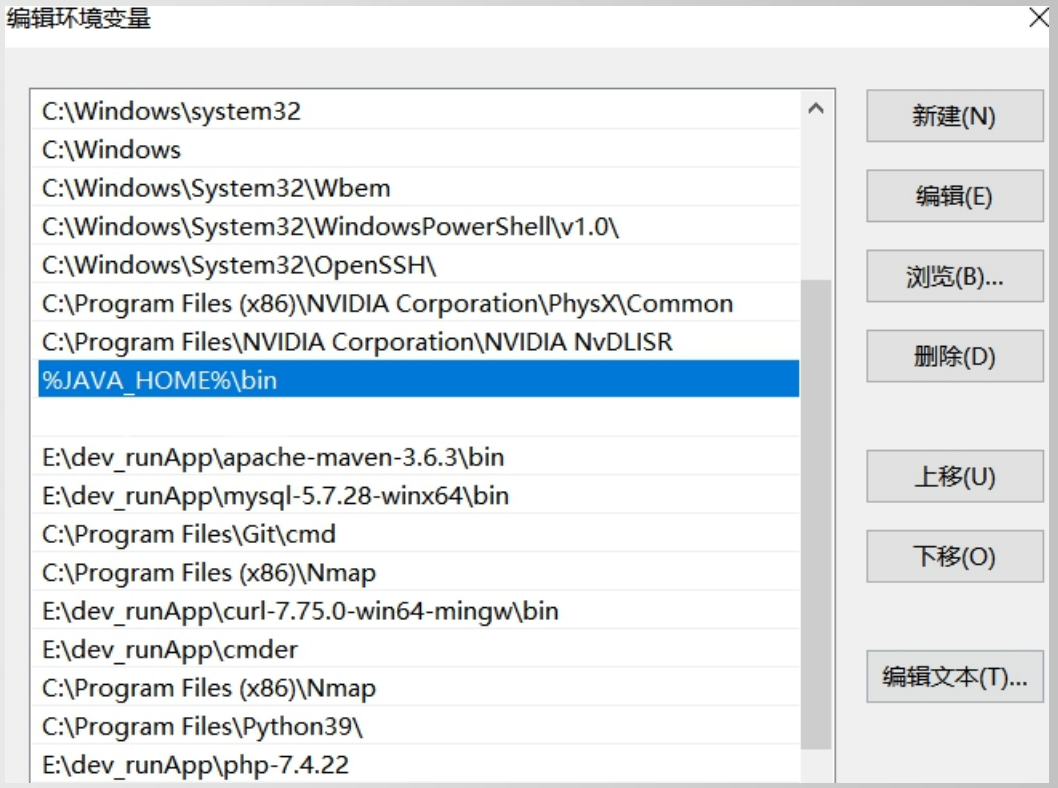
变量	值
JAVA_HOME	JDK解压的根路径，比如 E:\jdk-11.0.11
PATH	%JAVA_HOME%\jre\bin;%JAVA_HOME%\bin
classpath	%JAVA_HOME%\jre\bin%;JAVA_HOME%\bin

JDK11环境变量配置

八方网域
bafangwy.com

变量	值
JAVA_HOME	JDK解压的根路径，比如 E:\jdk-11.0.11
PATH	%JAVA_HOME%\bin





命令行方式启动

创建burp_start.bat，内容：

```
@echo off
cmd /k "java -jar BurpLoaderKeygen.jar"
```

激活

按步骤来，注意：
1、勾选Auto Run
2、勾选Ignore Update

VBS启动


```
set ws=WScript.CreateObject("WScript.Shell")
ws.Run "burp_start.bat",0
```

汉化说明

burp_cn_start.bat

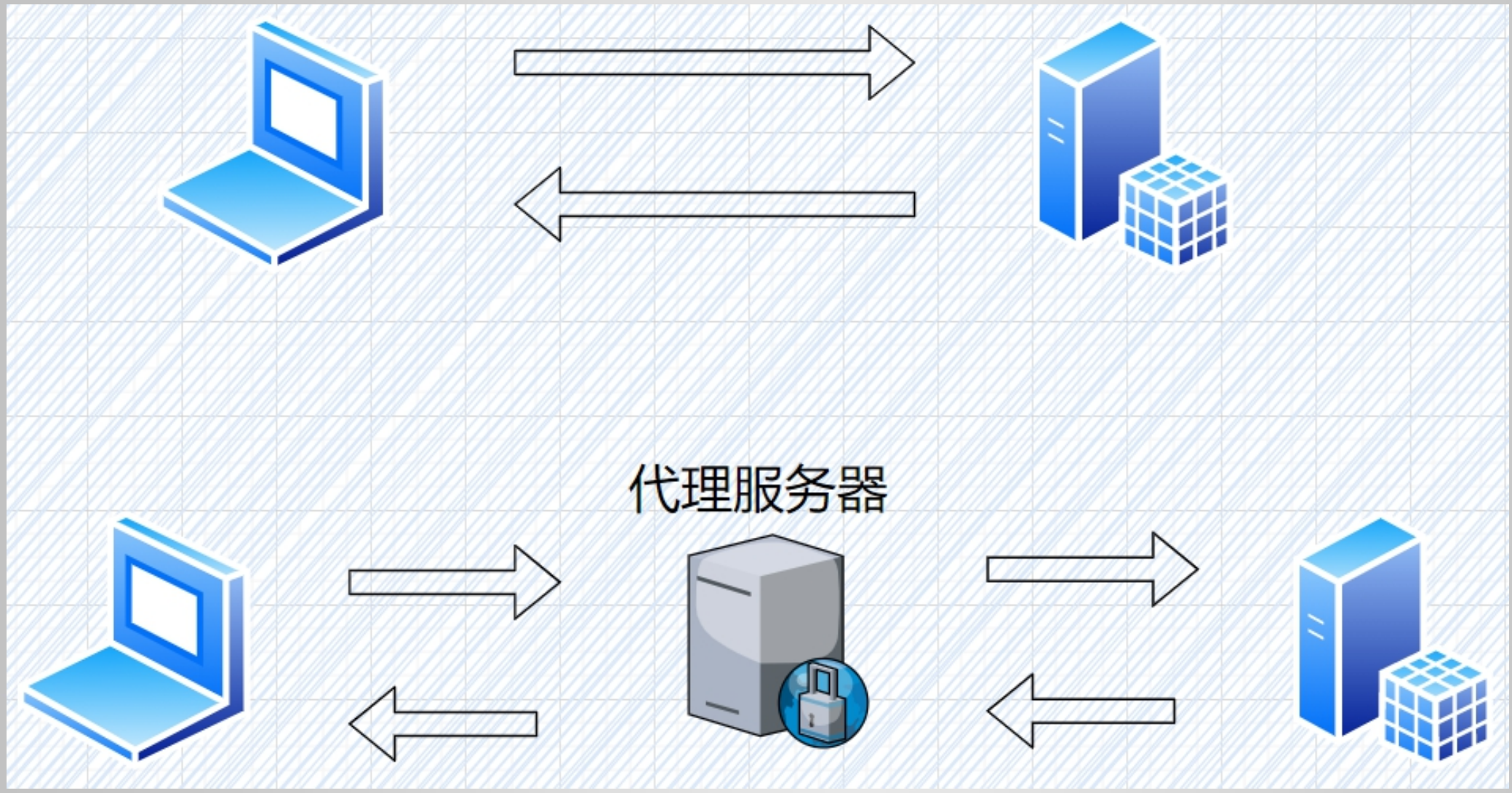
```
@echo off
cmd /k "java -jar BurpLoaderKeygenCn.jar"
```

其他配置

字体大小
汉字乱码

02 Burp Suite代理配置

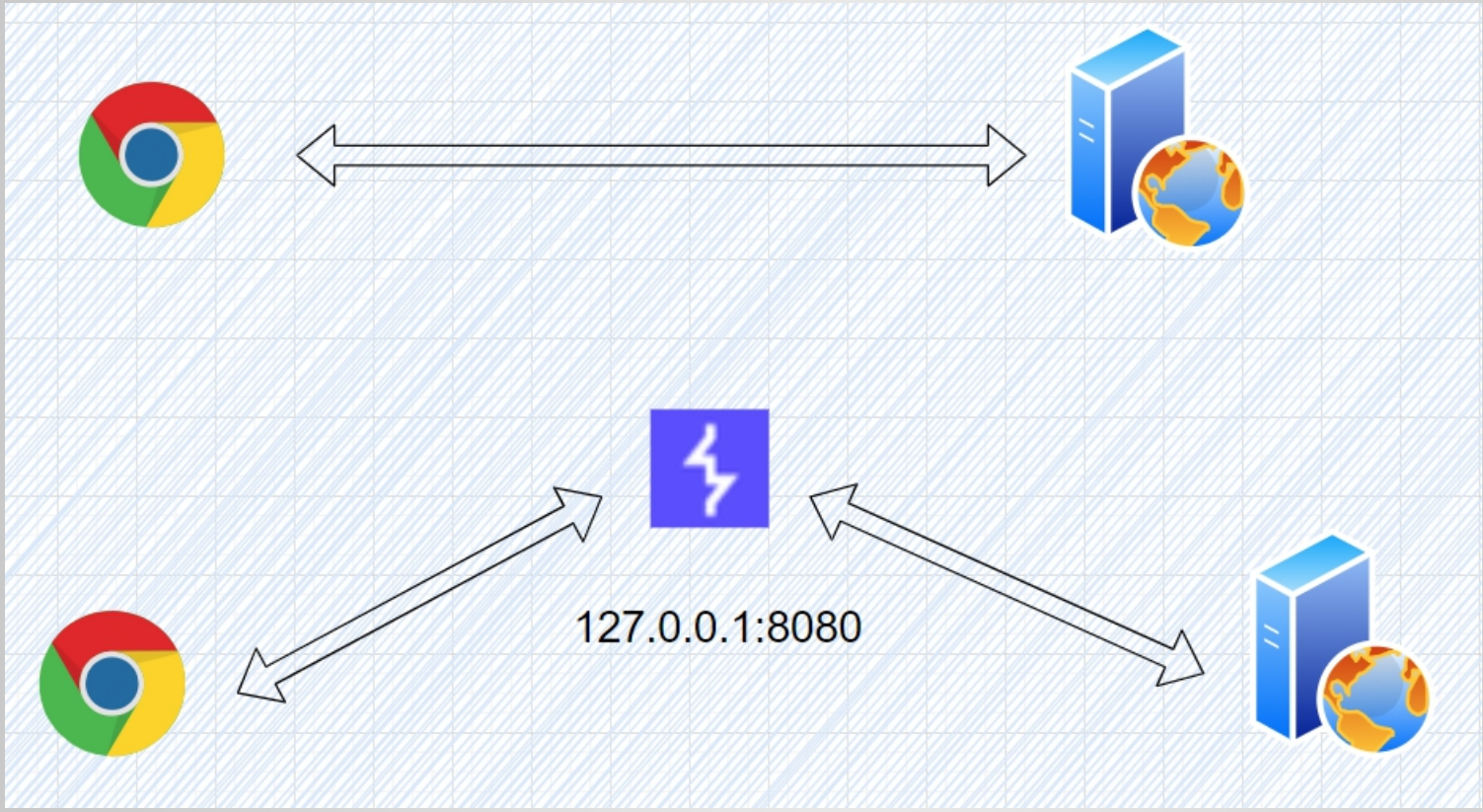
网络代理



网络代理的作用

- 突破IP限制
- 隐藏IP
- 加速访问
- ……

浏览器代理设置

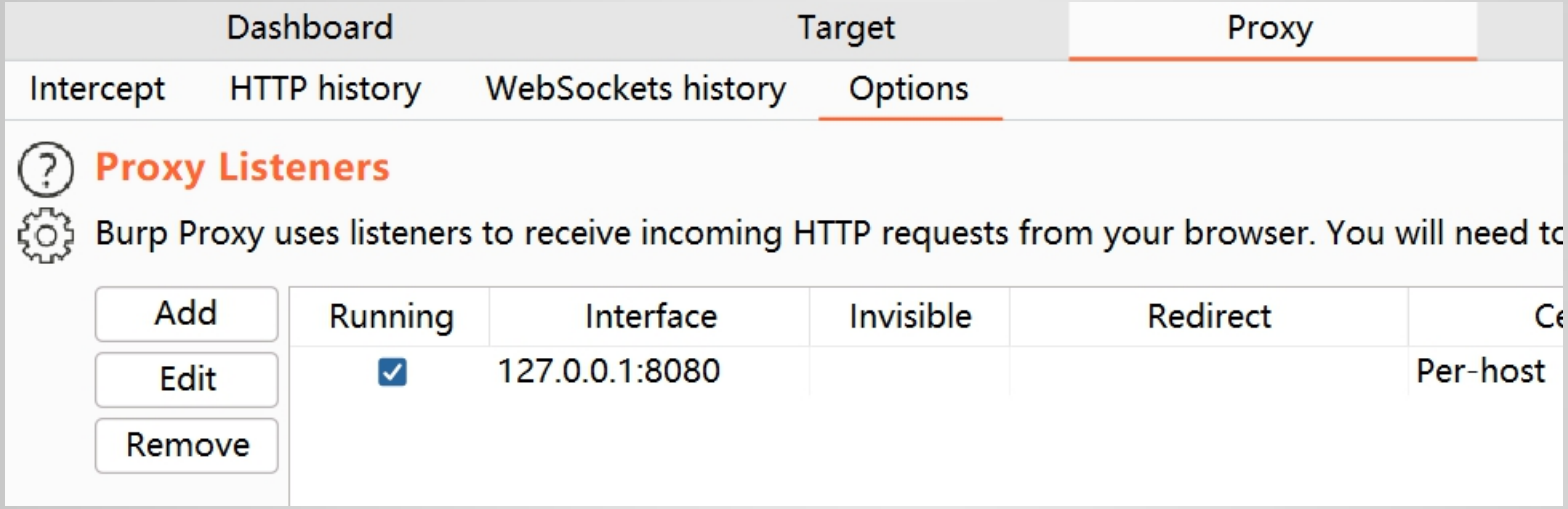


Burp代理的作用

拦截HTTP(S)请求，并对请求和响应进行处理和利用

浏览器代理设置（火狐）

BP代理设置



Intercept

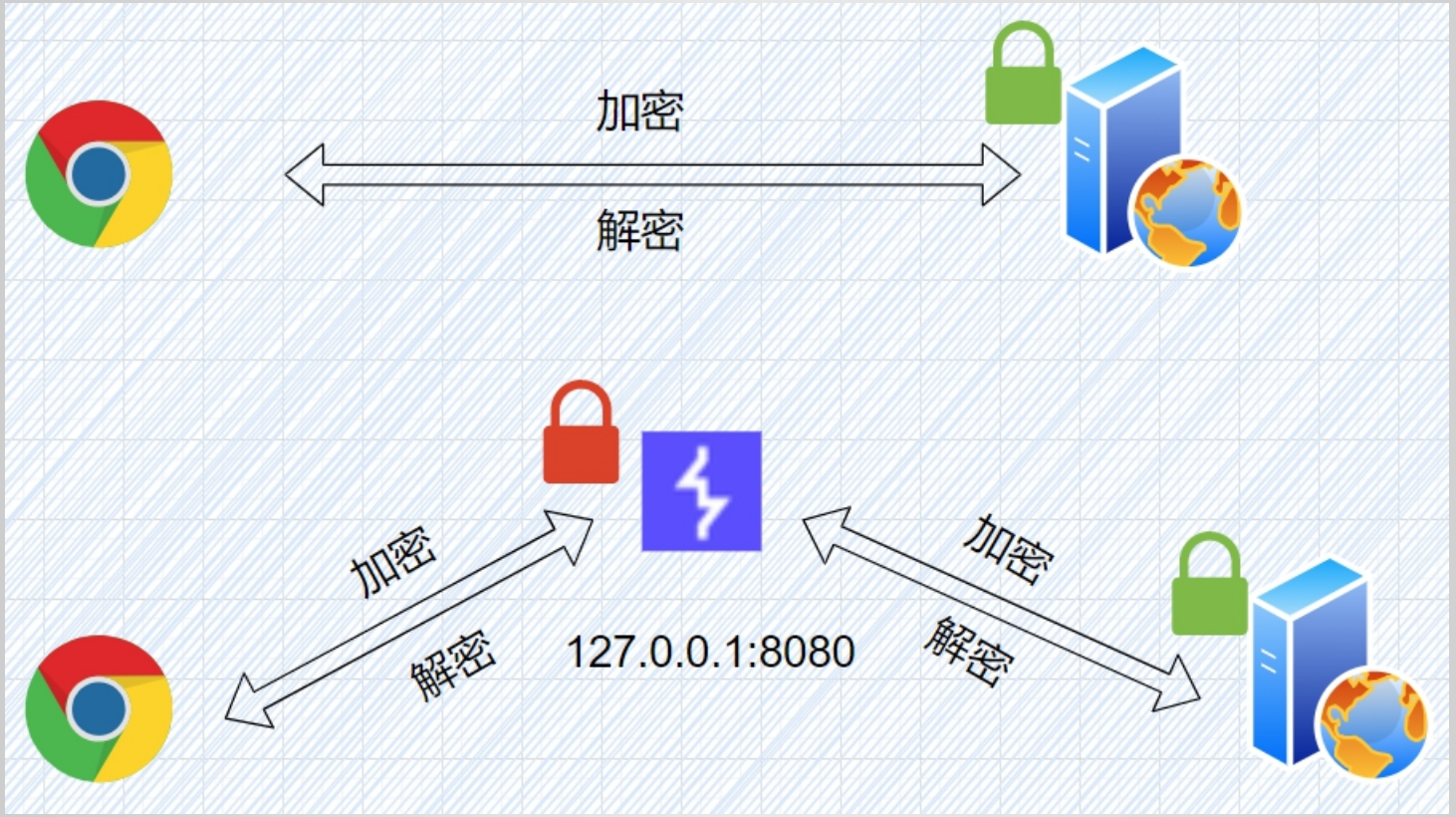
操作	描述
Forward	放行本次拦截的包，发送到服务器
Drop	丢弃本次拦截的包
on/off	拦截开关
Action	对数据的操作
Open in Browser	打开内置浏览器

拦截功能

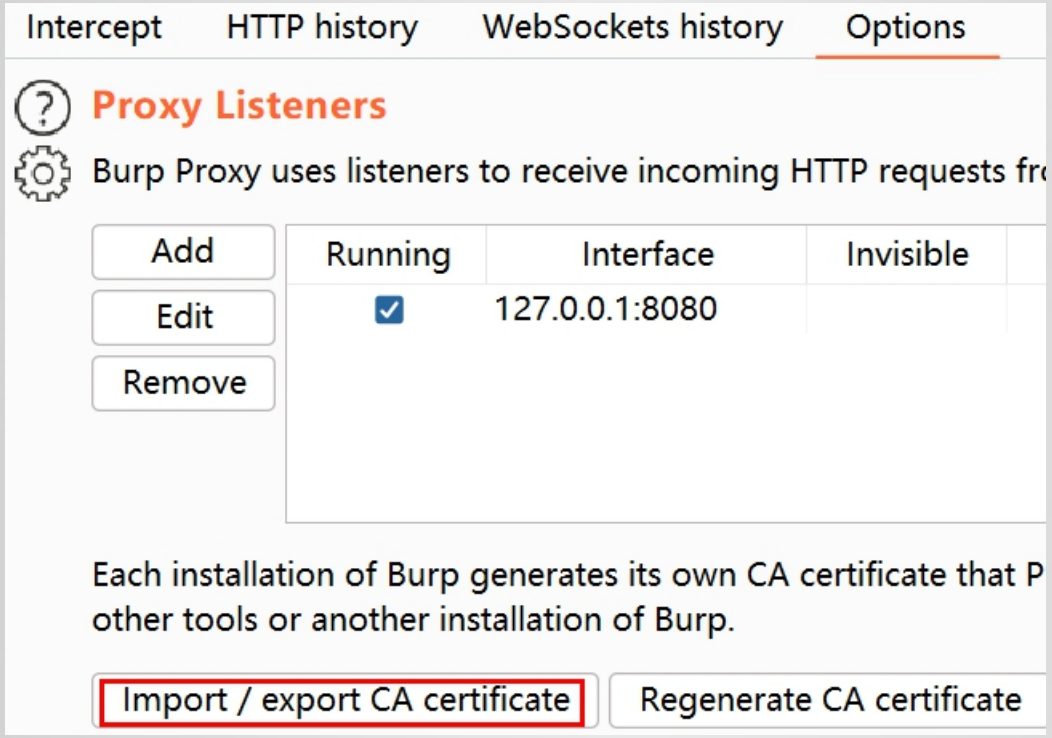
注意：
1、BP内置浏览器不需要配置代理，自动拦截所有的请求。
2、默认不拦截响应，需要右键设置

03 Burp Suite拦截HTTPS

安全警告



导出证书

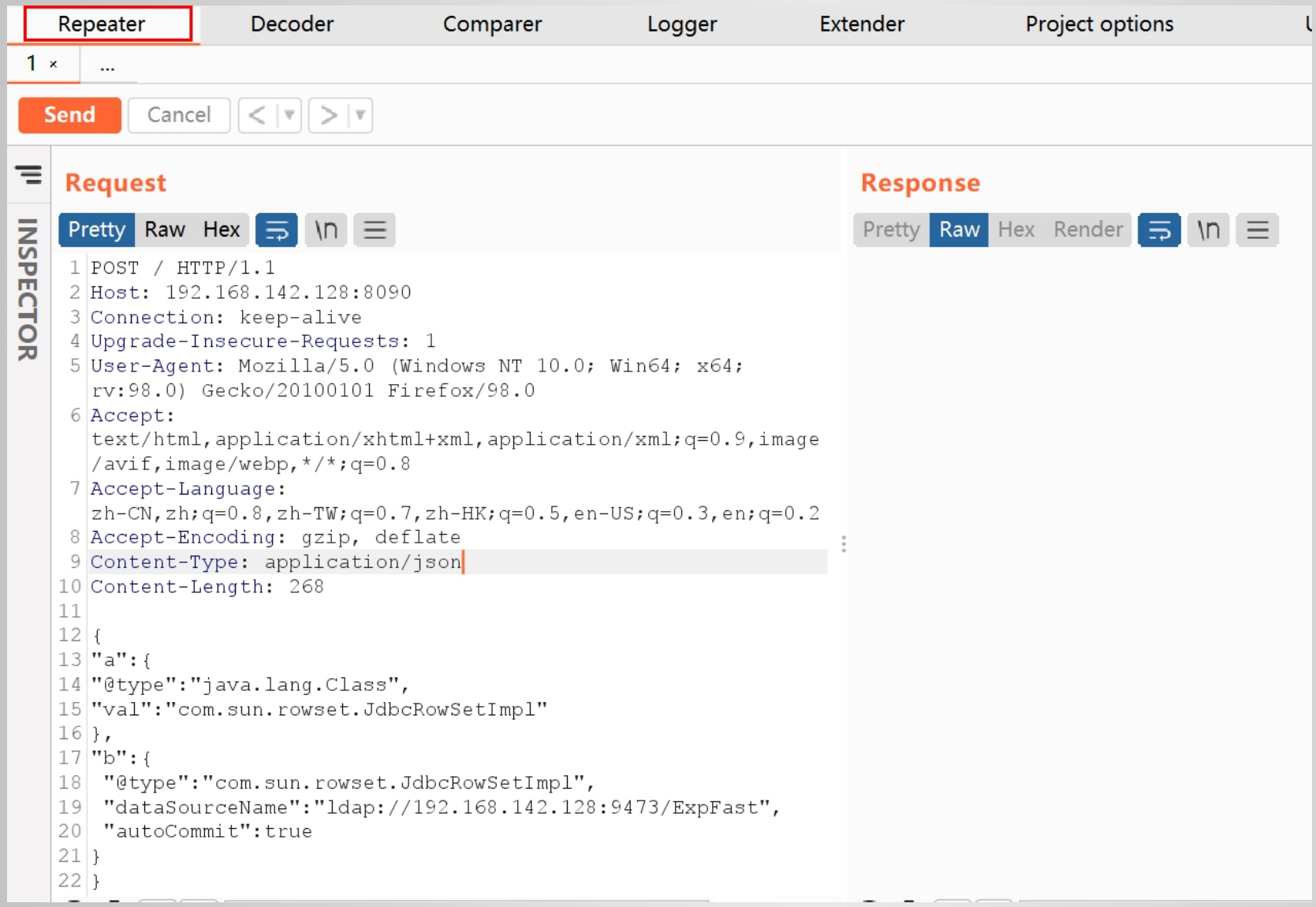


1、导出.der
2、或者开启代理的情况下，http://burp获得证书

浏览器导入证书（火狐）

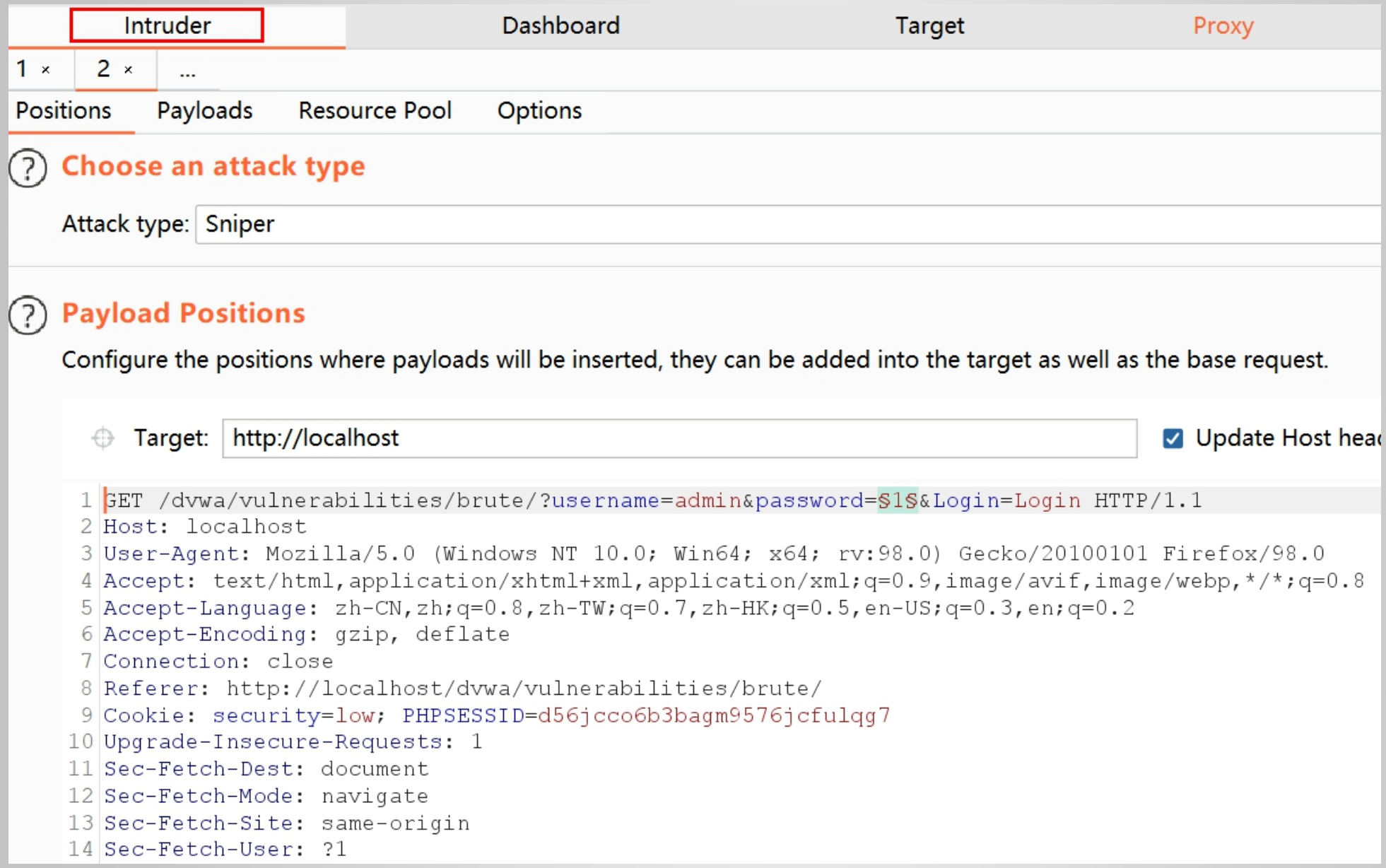
04 Burp Repeater抓包与改包

Repeater



05 Burp Intruder爆破密码

Intruder



Thank you for watching