

1. Burpsuite的介绍

摘自百度百科对burpsuite的解释：

Burp Suite 是用于攻击web 应用程序的集成平台。它包含了许多工具，并为这些工具设计了许多接口，以促进加快攻击应用程序的过程。

也就是说，Burp Suite是web应用程序渗透测试集成平台。从应用程序攻击表面的最初映射和分析，到寻找和利用安全漏洞等过程，所有工具为支持整体测试程序而无缝地在一起工作。

平台中所有工具共享同一robust框架，以便统一处理HTTP请求、持久性、认证、上游代理、日志记录、报警和可扩展性。Burp Suite允许攻击者结合**手工和自动技术**去枚举、分析、攻击Web应用程序。

burpsuite具有以下功能：

- **Proxy** —— 是一个拦截HTTP/S的代理服务器，作为一个在浏览器和目标应用程序之间的中间人，允许你拦截，查看，修改在两个方向上的原始数据流。
- **Spider** —— 是一个应用智能感应的网络爬虫，它能完整的枚举应用程序的内容和功能。
- **Scanner** [仅限专业版] —— 是一个高级的工具，执行后，它能自动地发现web 应用程序的安全漏洞。
- **Intruder** —— 是一个定制的高度可配置的工具，对web应用程序进行自动化攻击，如：枚举标识符，收集有用的数据，以及使用fuzzing 技术探测常规漏洞。
- **Repeater** —— 是一个靠手动操作来补发单独的HTTP 请求，并分析应用程序响应的工具。
- **Sequencer** —— 是一个用来分析那些不可预知的应用程序会话令牌和重要数据项的随机性的工具。
- **Decoder** —— 是一个进行手动执行或对应用程序数据者智能解码编码的工具。
- **Comparer** —— 是一个实用的工具，通常是通过一些相关的请求和响应得到两项数据的一个可视化的“差异”。

2. Java环境的安装

- 默认下一步



- 路径不要修改



- jre也要安装，点击下一步



- 等待安装



- 安装完成



- 判断JAVA环境是否正常
- 打开cmd分别输入：

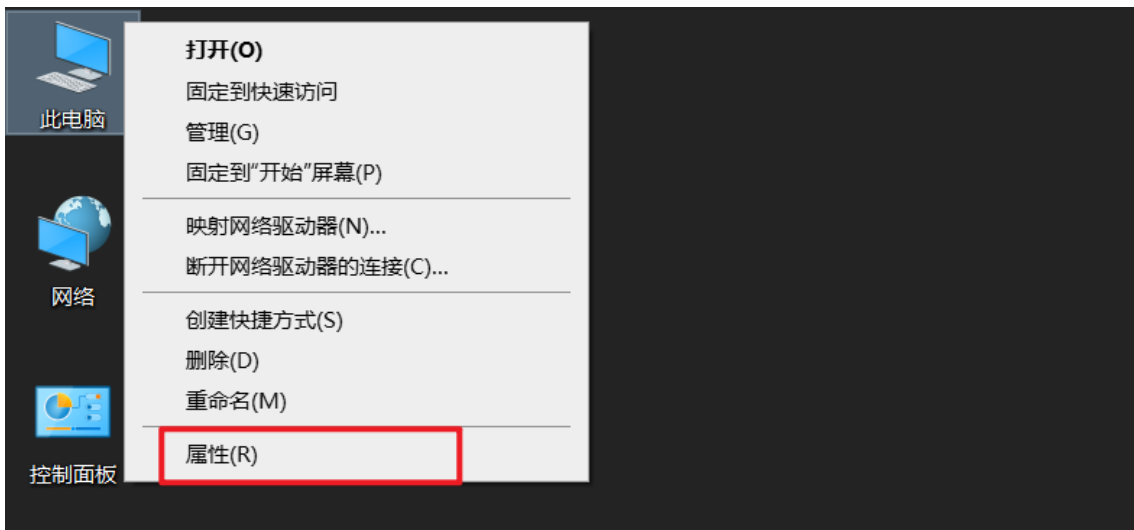
```
java
java -version
javac
```

- 如果出现类似以下情况，需要配置环境变量：

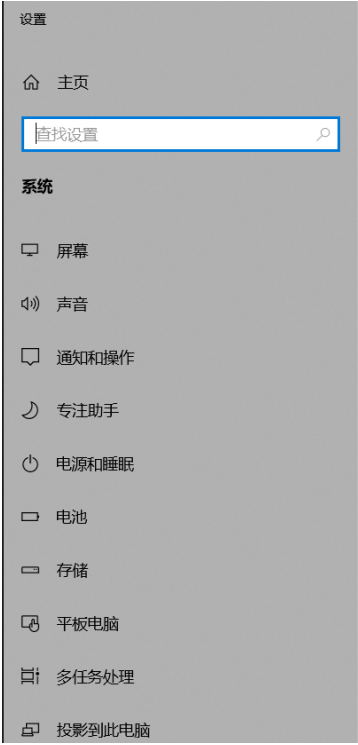
'javac' 不是内部或外部命令，也不是可运行的程序或批处理文件。

3. 环境变量配置

- 此电脑，右键属性



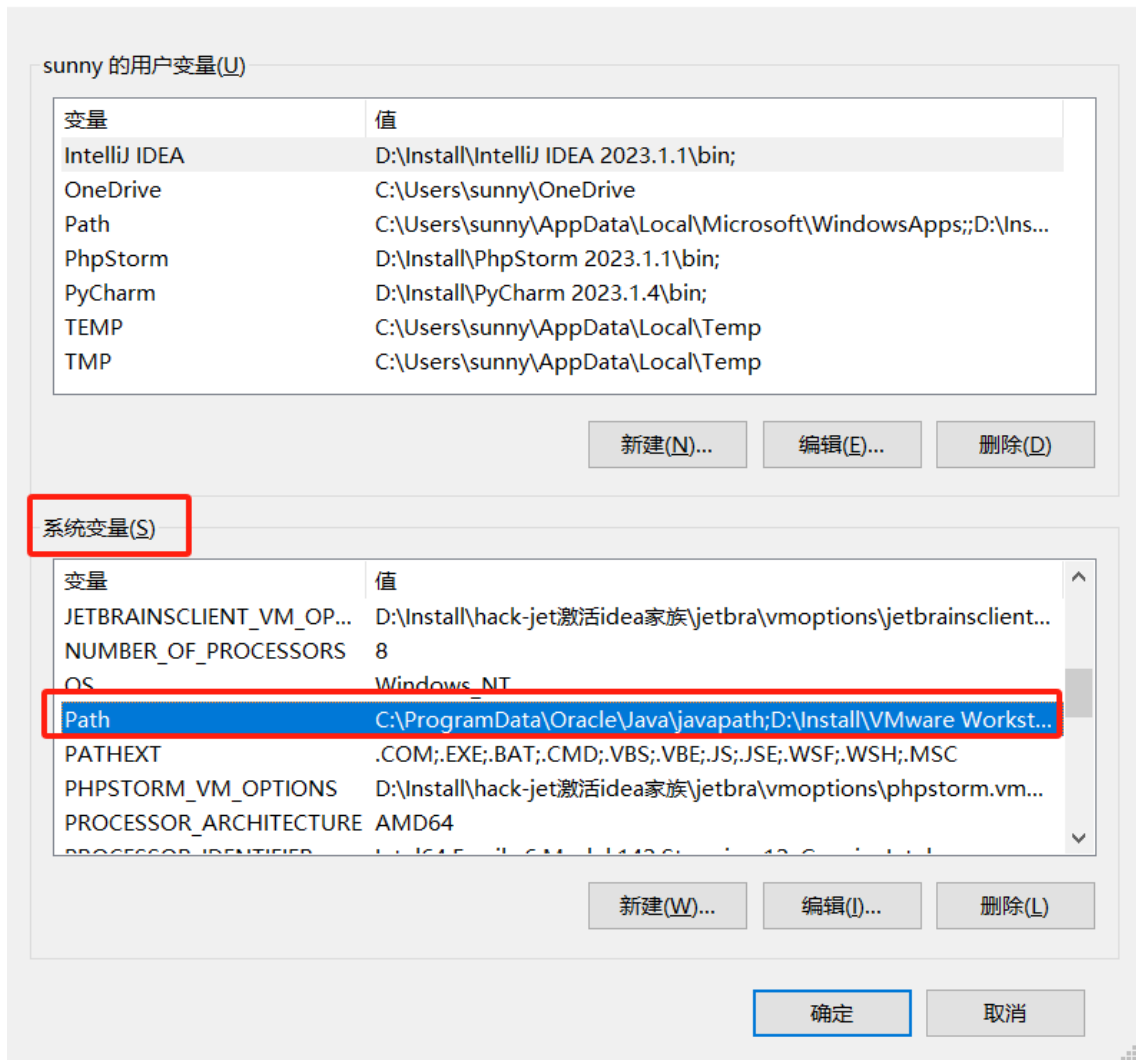
- 高级系统设置



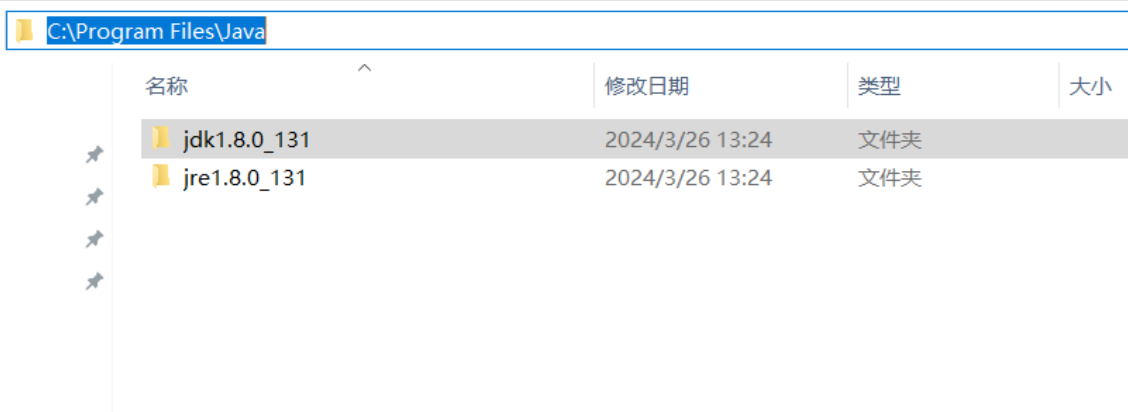
- 环境变量



- 编辑Path




- 复制java路径



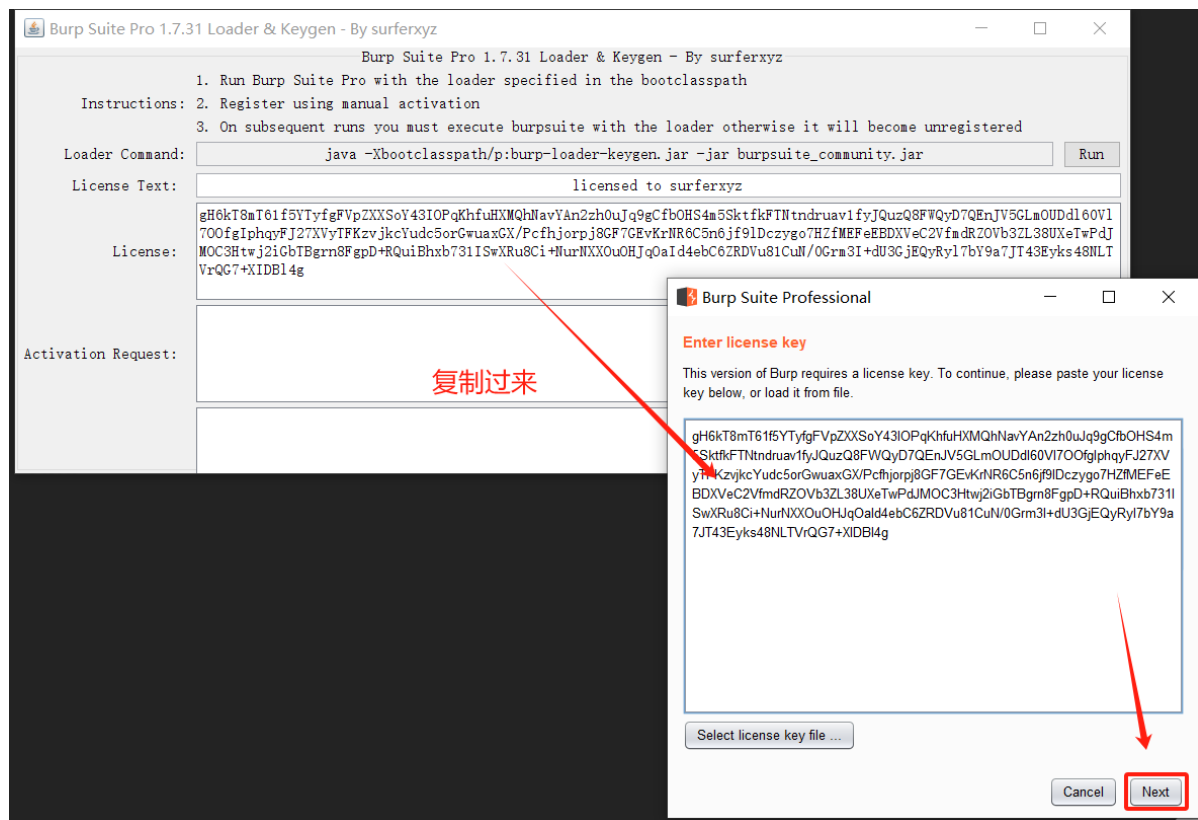
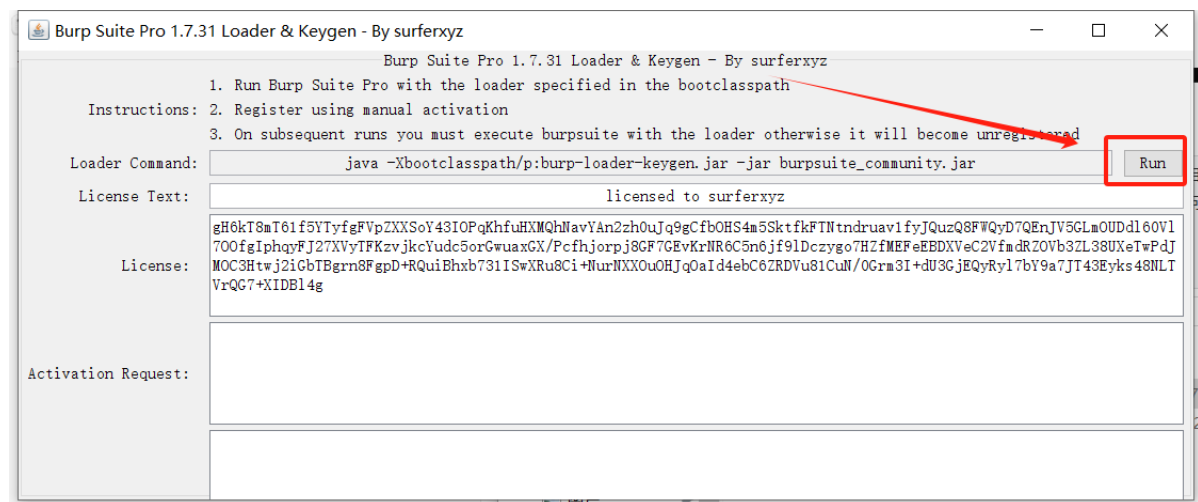
- 添加到环境变量中，一定要把所有的 确定 都点了才会生效

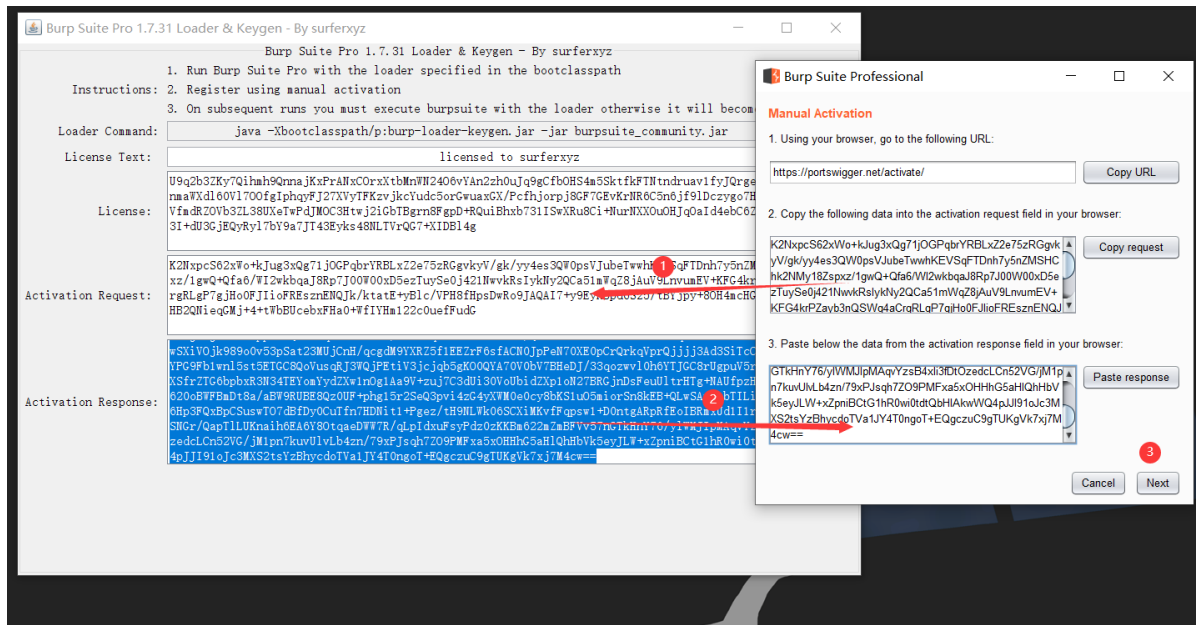
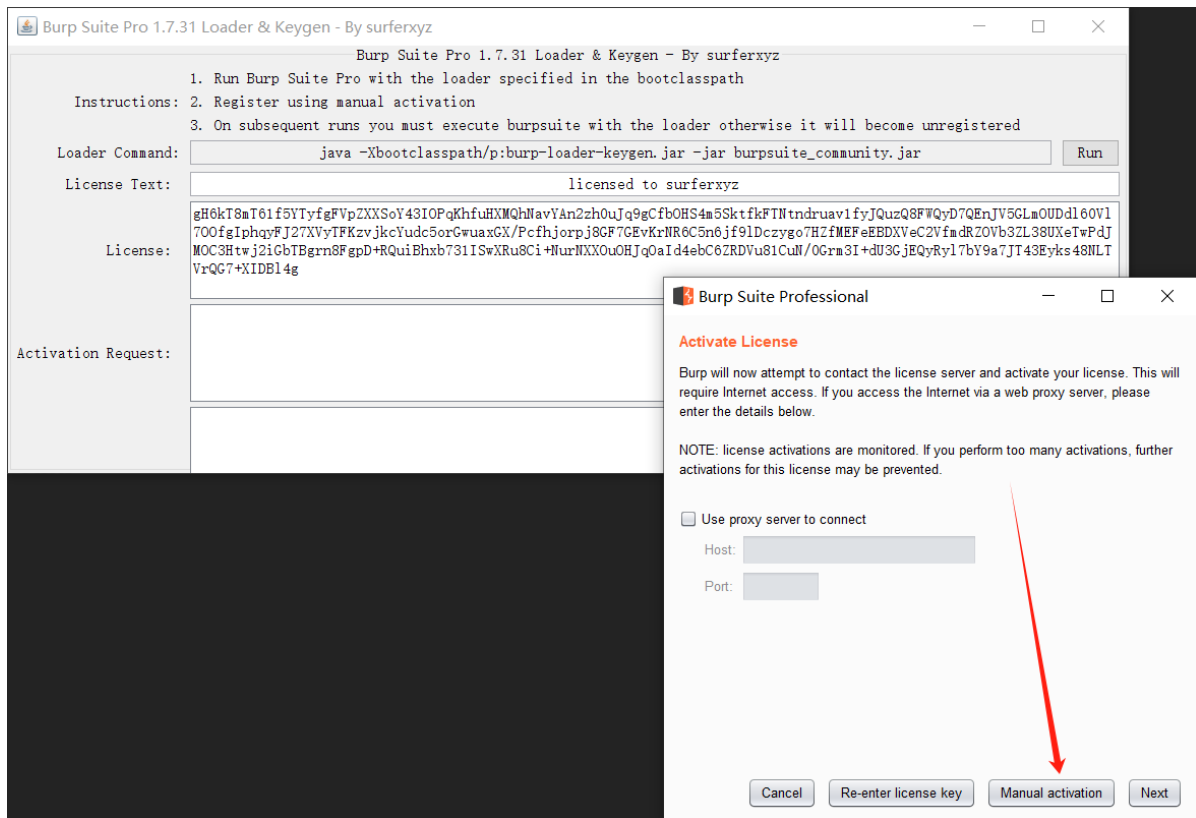
4. burp的破解

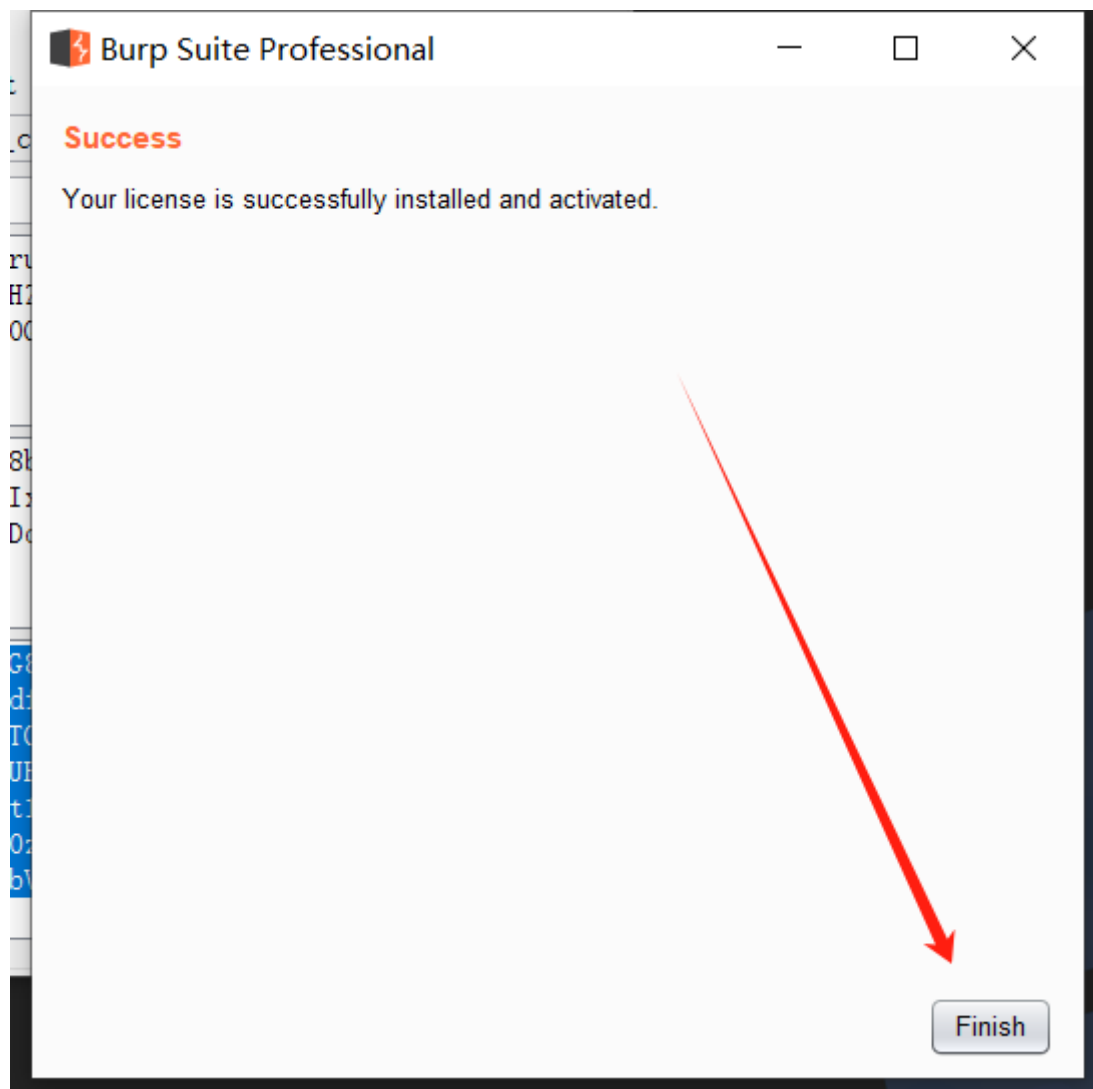
电脑 > 新加卷 (D:) > MyTools > Burpsuite Professional

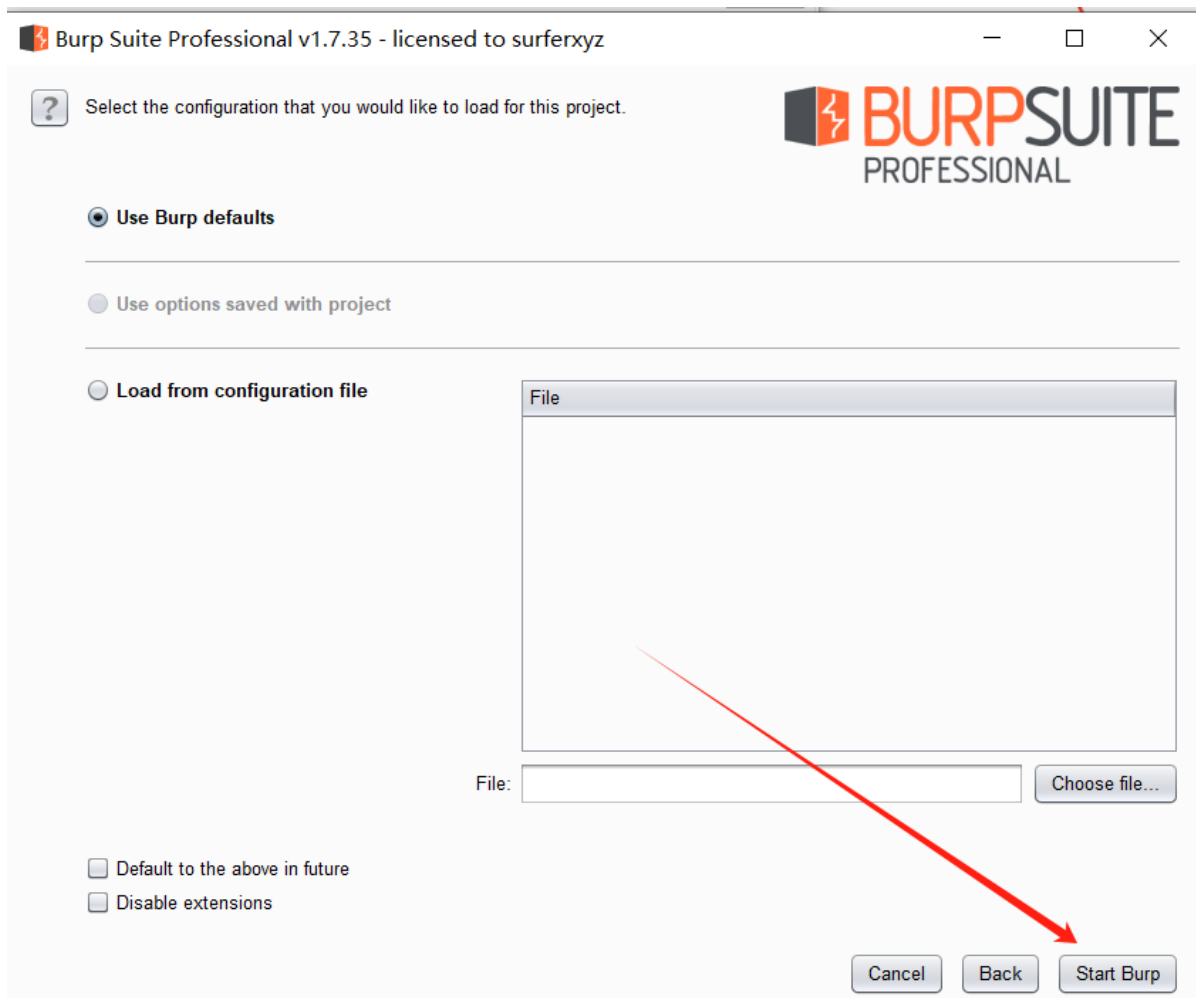
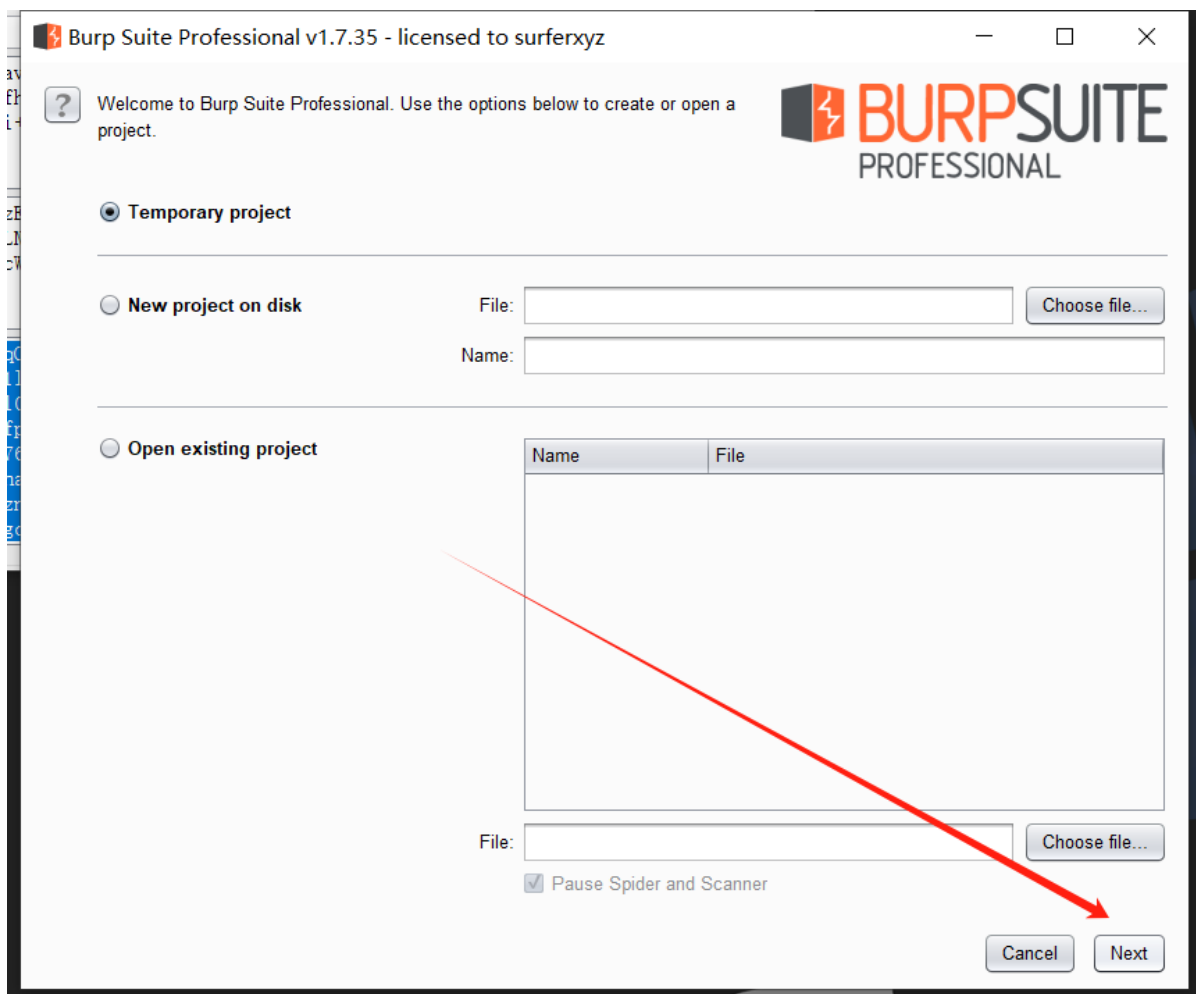
名称	修改日期	类型	大小
 burp-loader-keygen.jar	2018/1/25 17:01	Executable Jar File	64 KB
 burpsuite_community.jar	2018/7/2 16:24	Executable Jar File	27,487 KB

双击

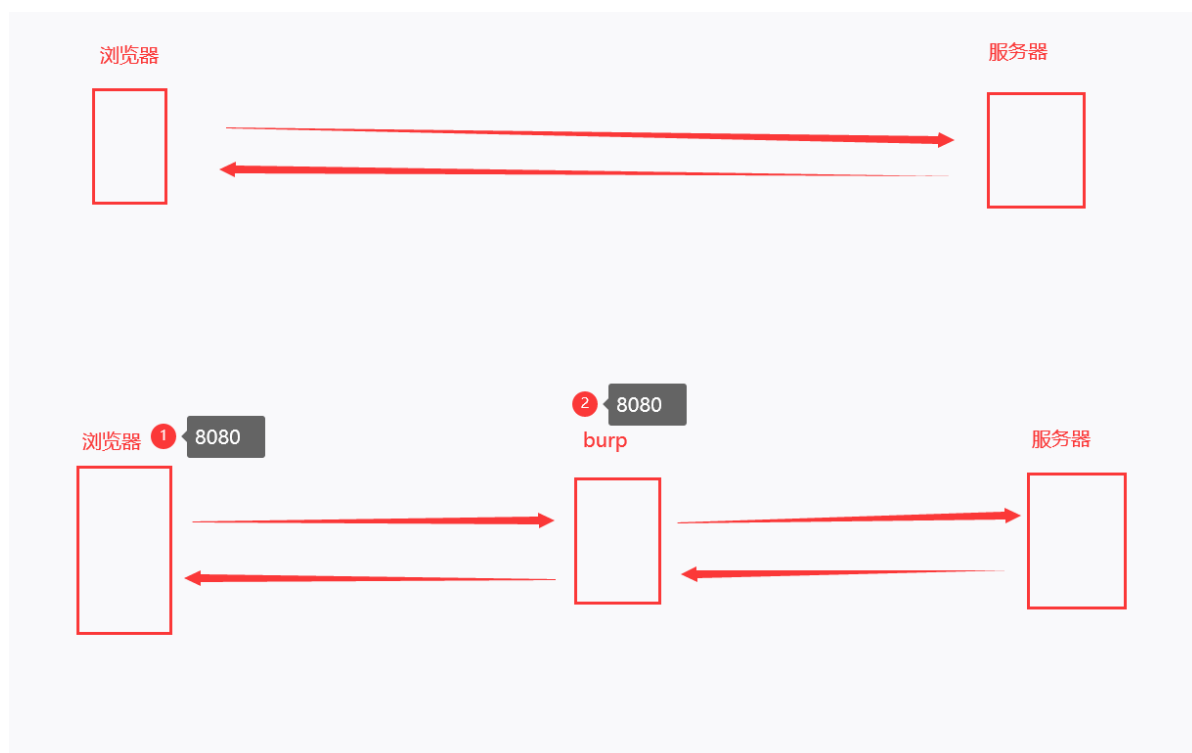








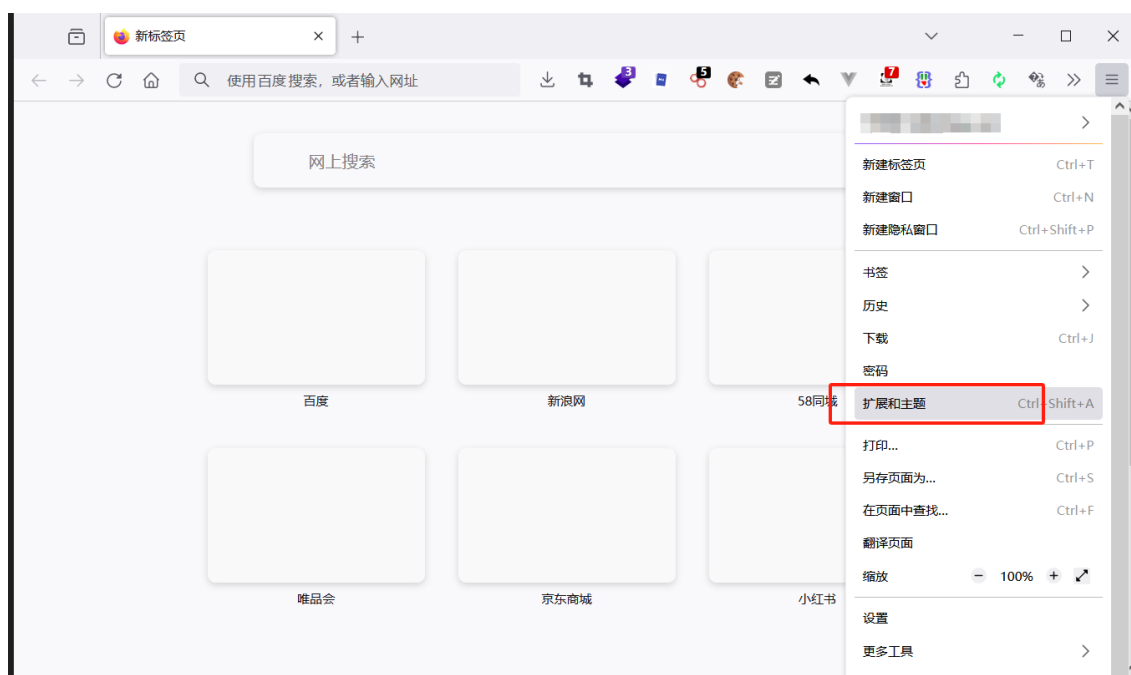
5. burp代理配置



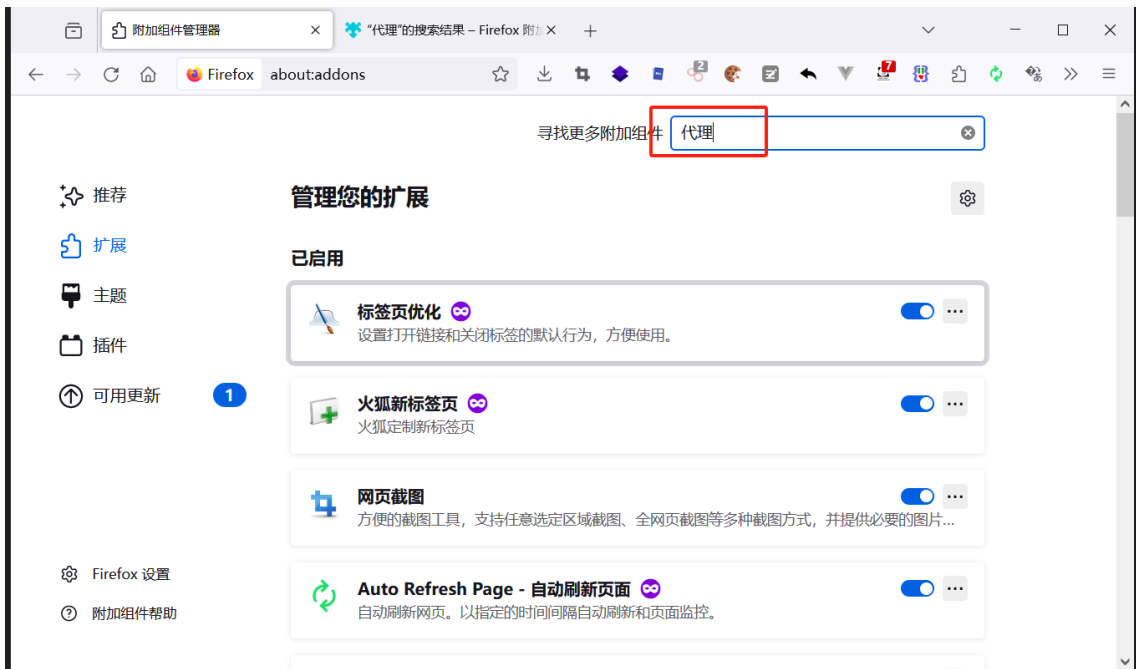
5.1 firefox代理配置

(1) 安装代理插件

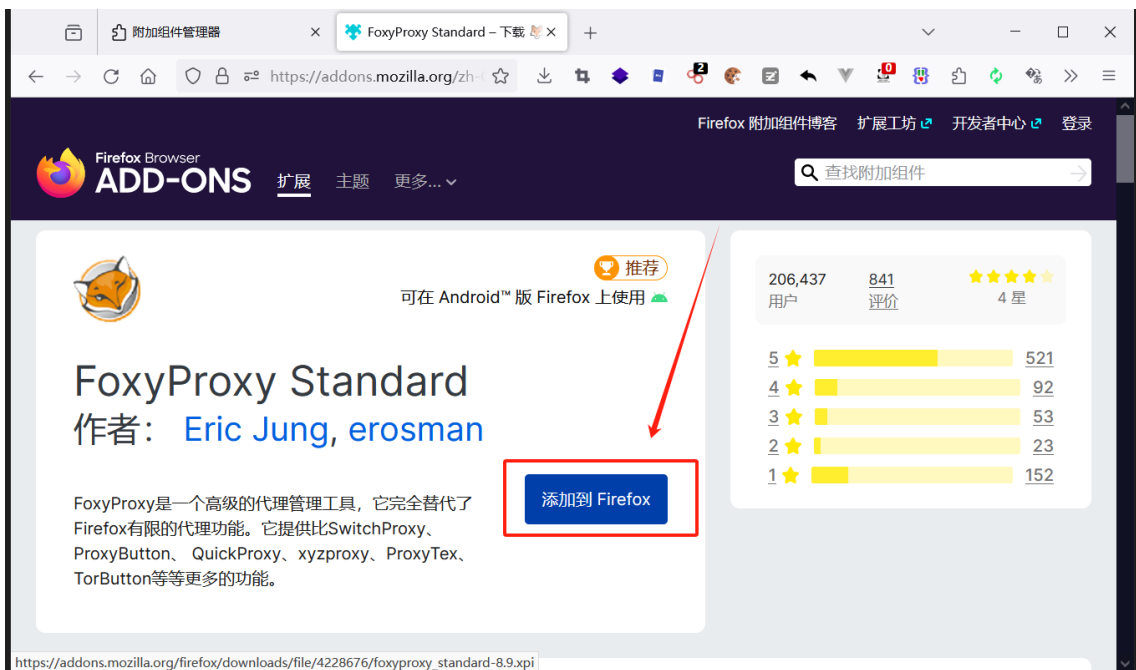
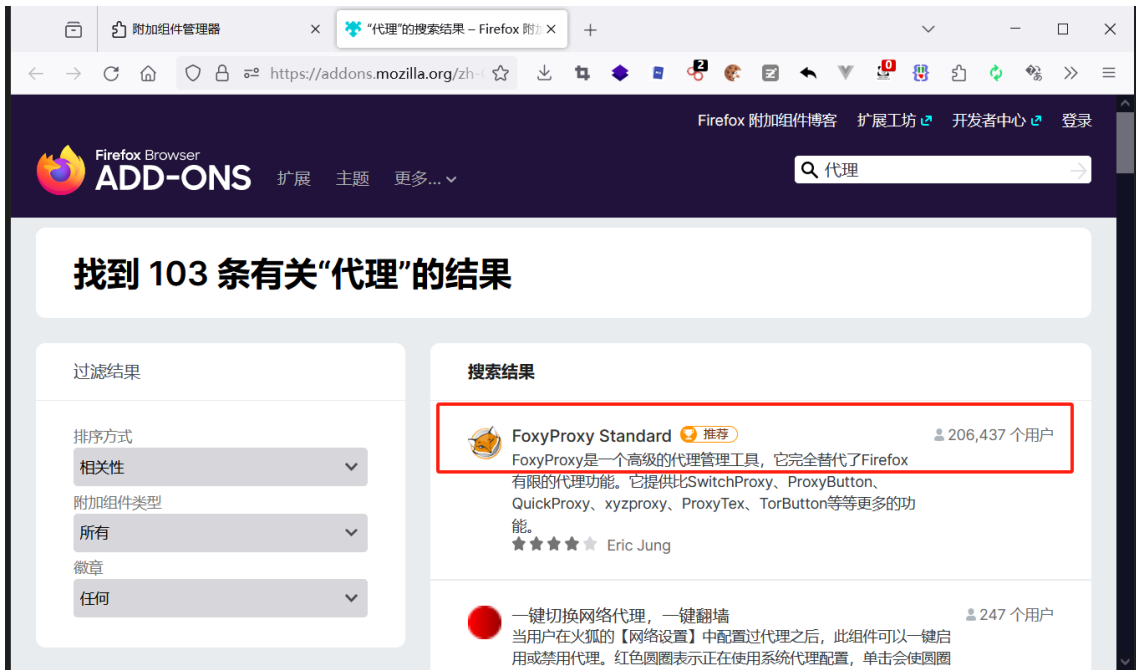
- 扩展和主题



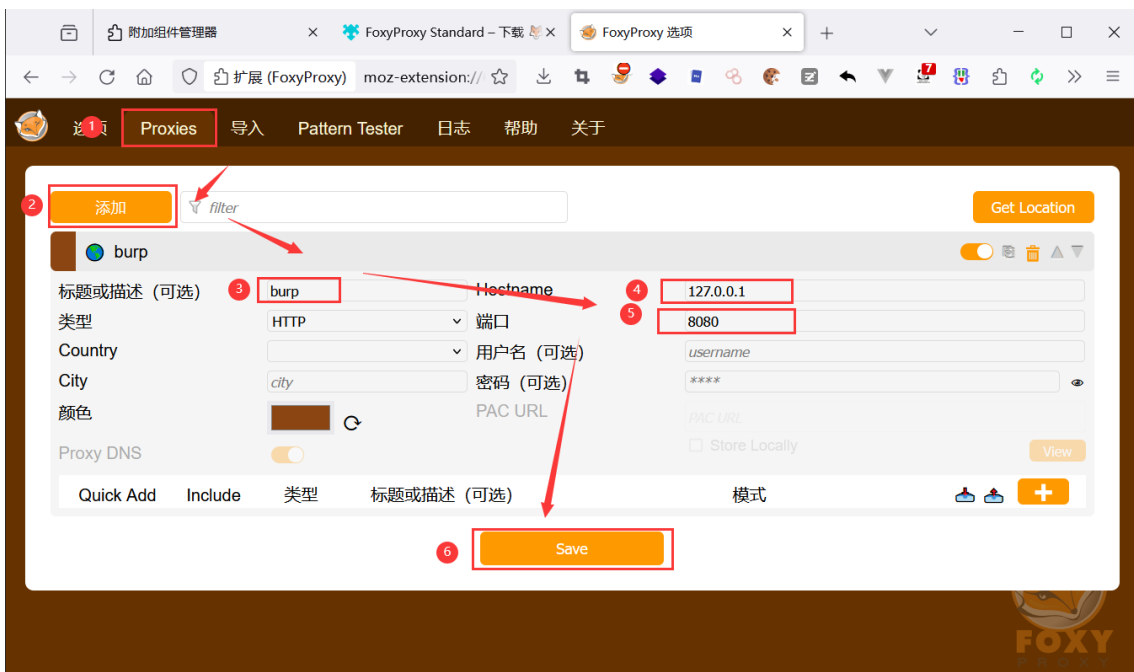
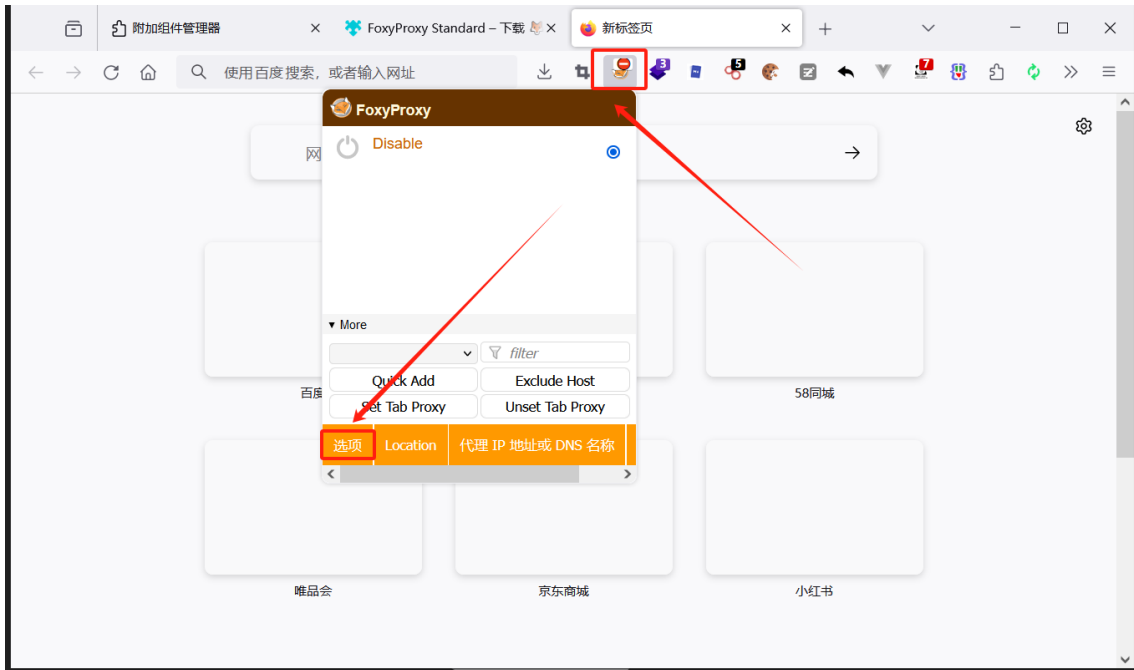
- 搜索代理



• 添加代理

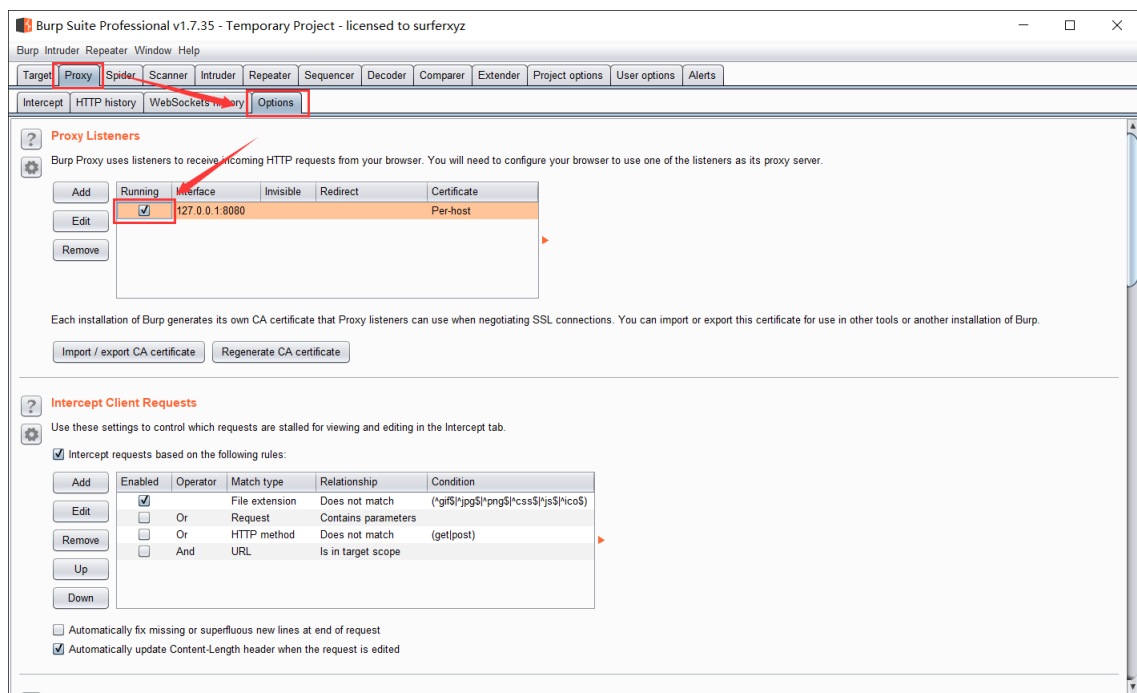


- 插件配置

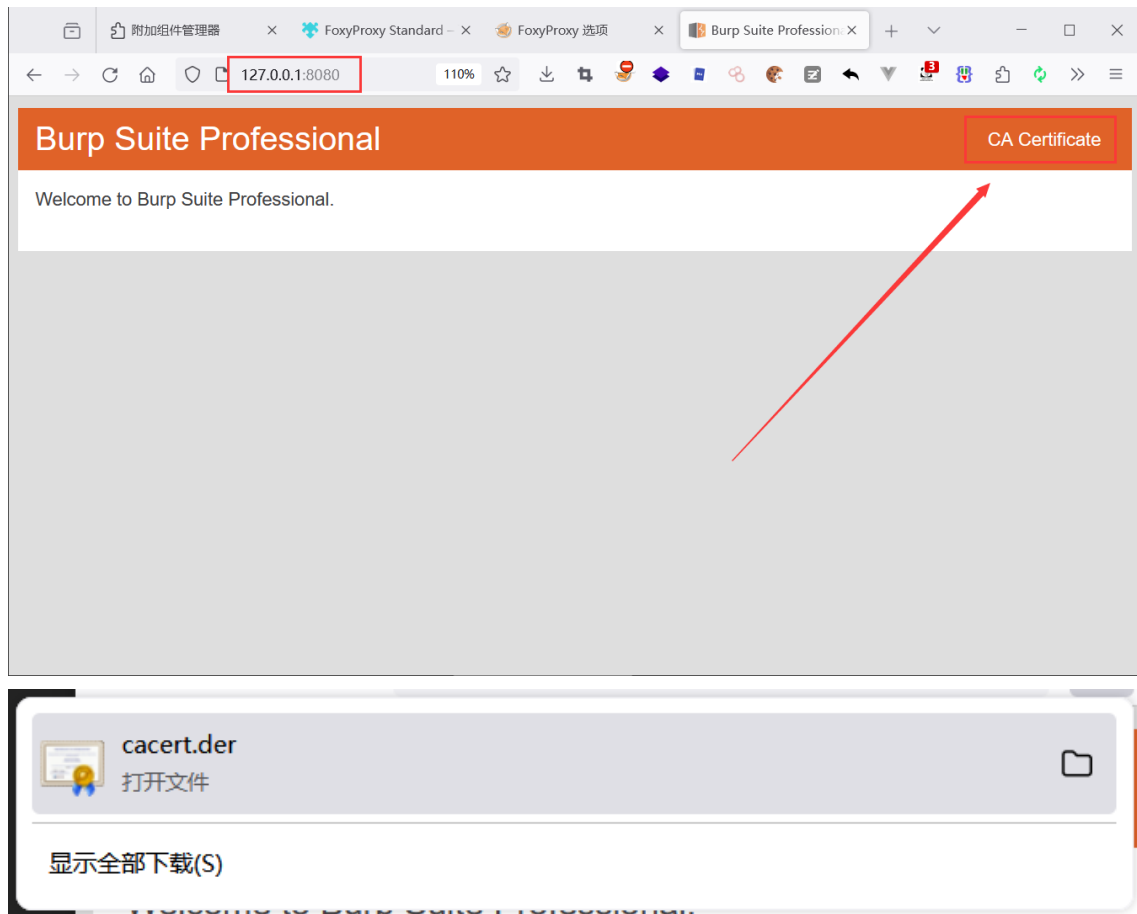


(2) firefox导入证书

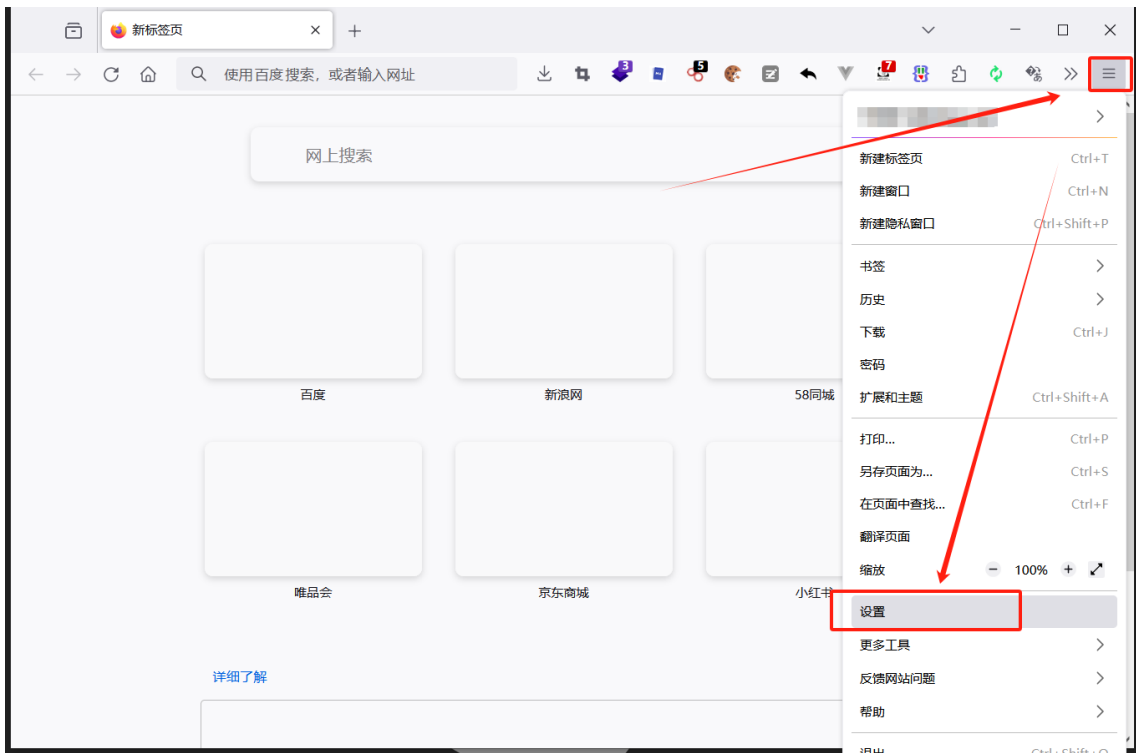
- 开启burpsuite的8080端口



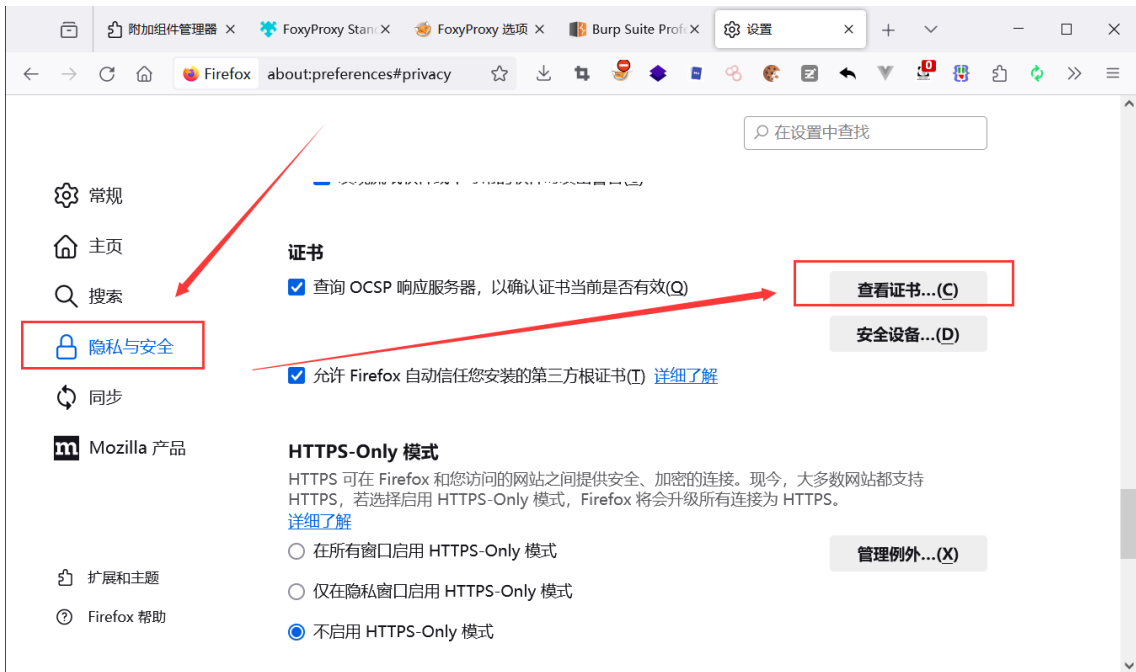
- 访问 <http://127.0.0.1:8080> 或者 <http://burp>, 下载证书



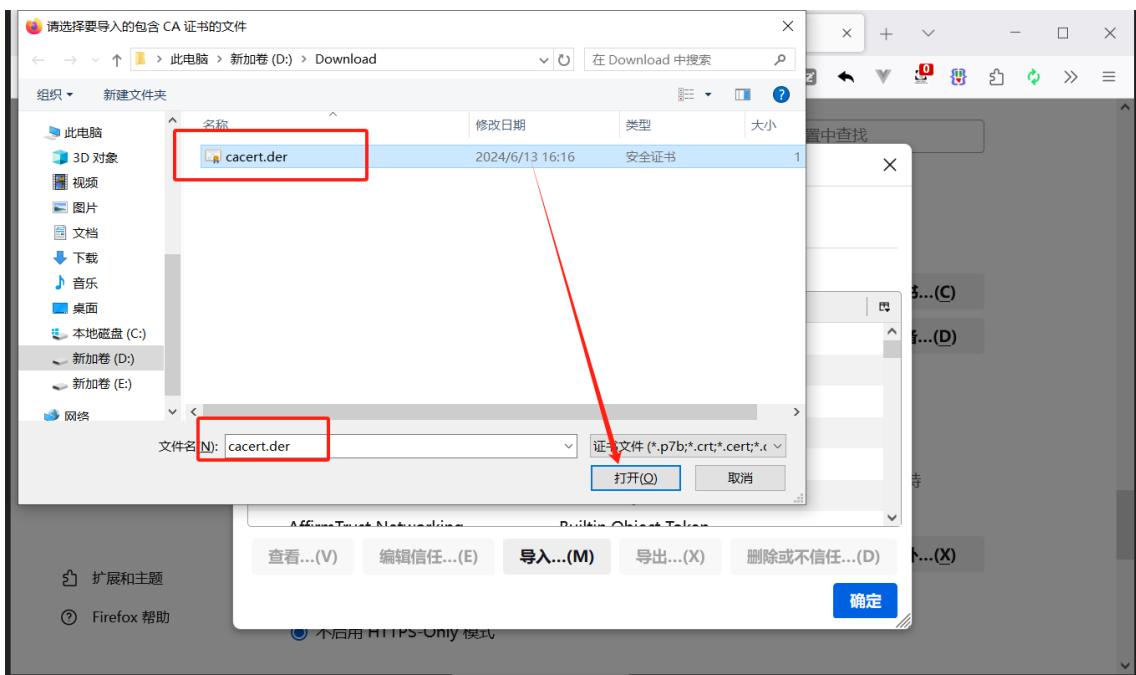
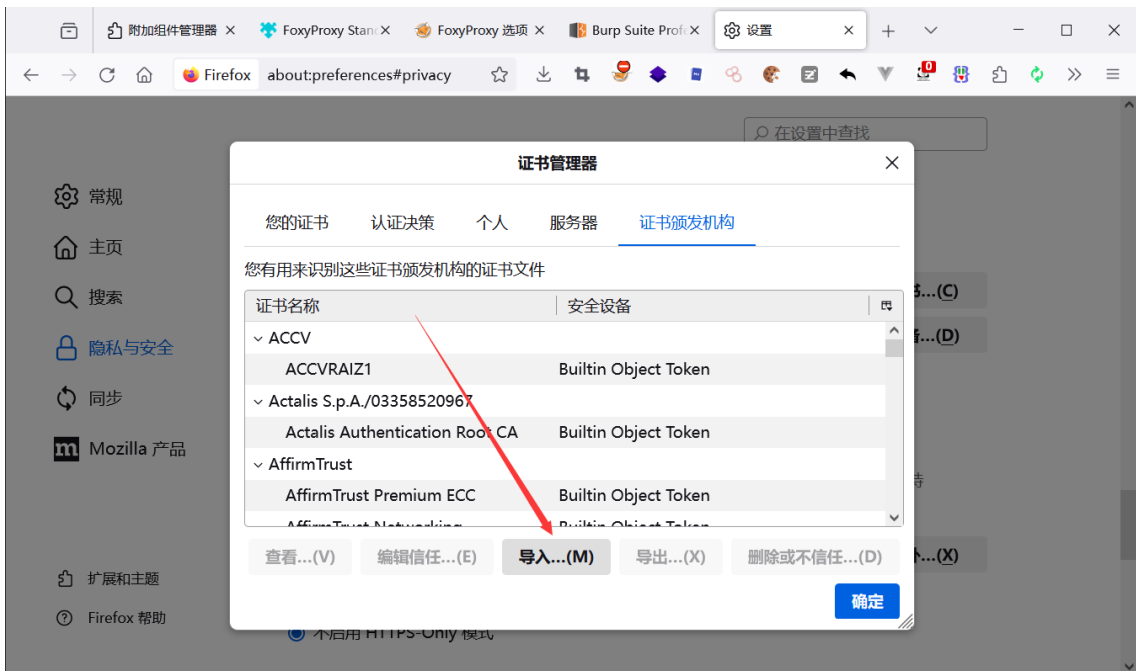
- 把证书导入浏览器, 进入设置



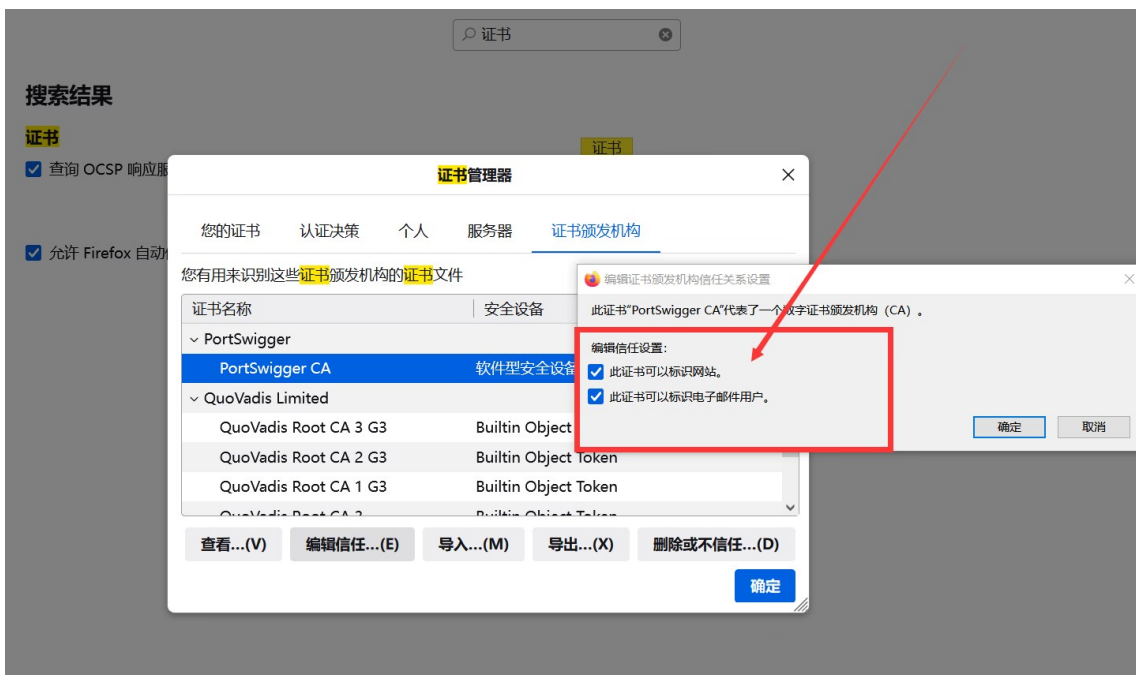
- 隐私与安全—查看证书



- 导入证书



- 全部勾选信任

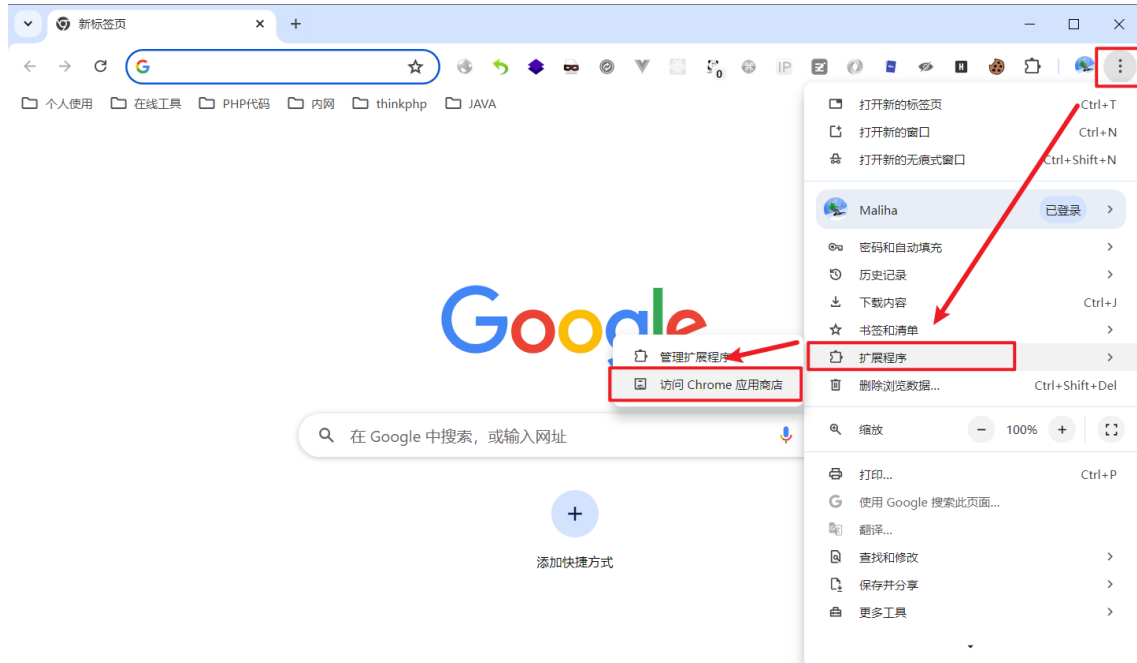


- 重启浏览器

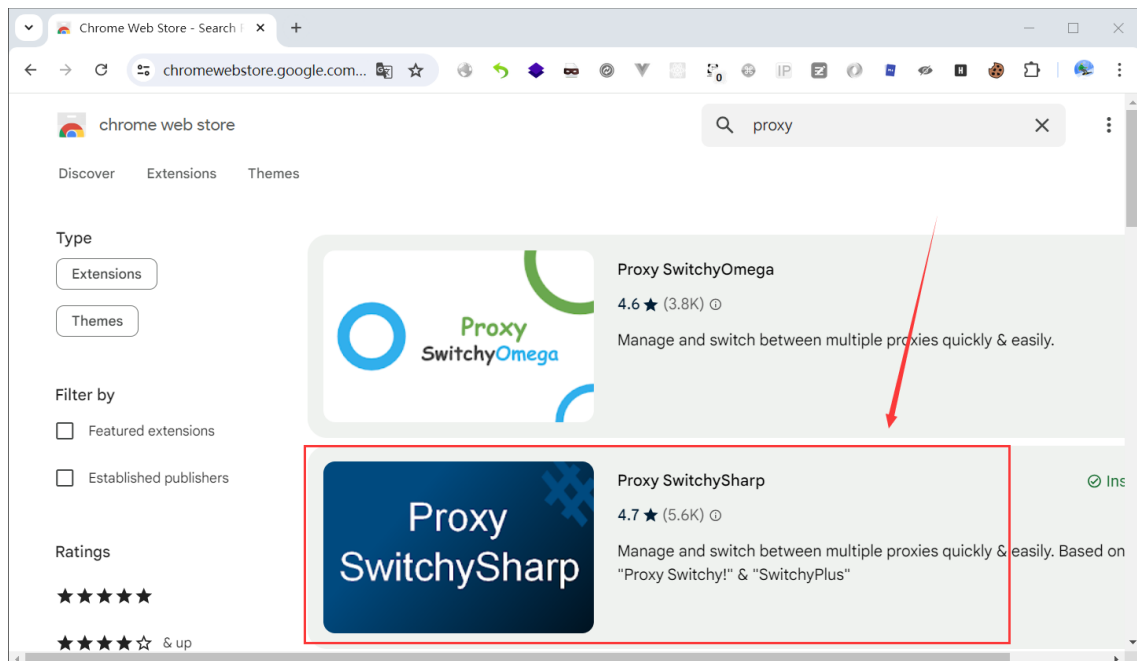
5.2 chrome代理配置

(1) 安装代理插件

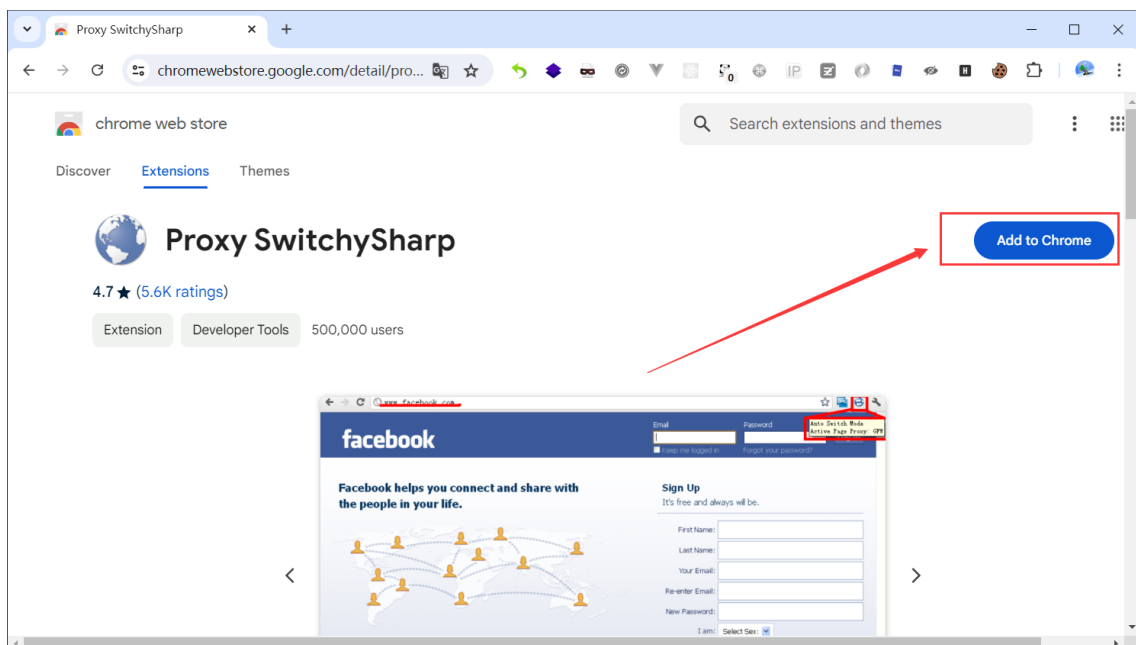
- 扩展程序—访问chrome应用商店



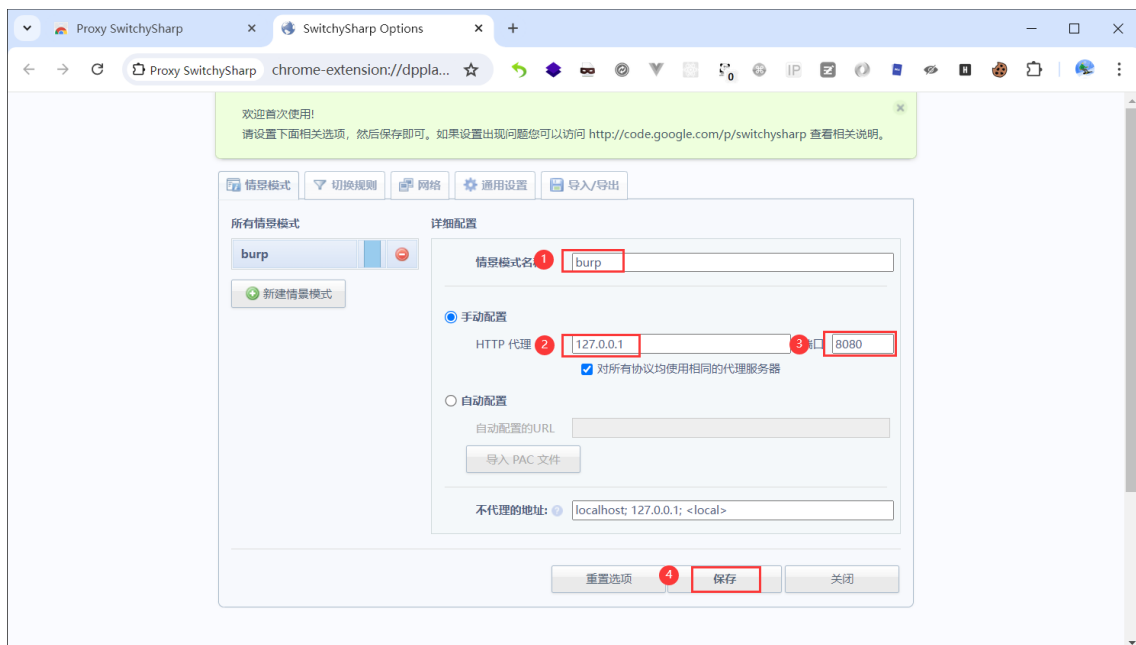
- 搜索proxy



- Add to Chrome

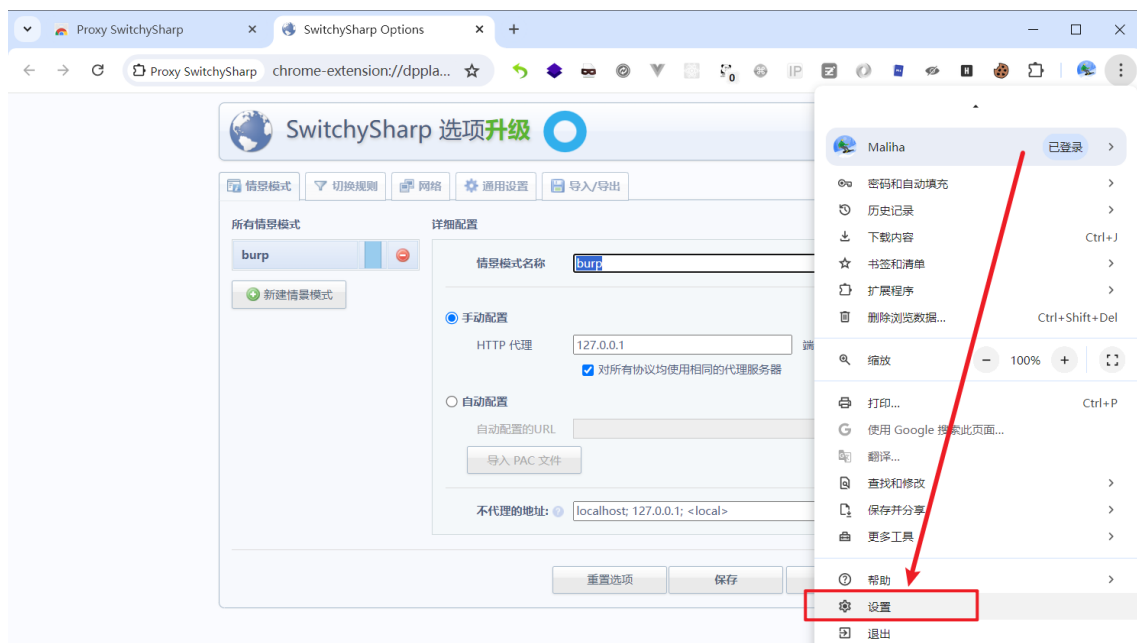


- 配置插件

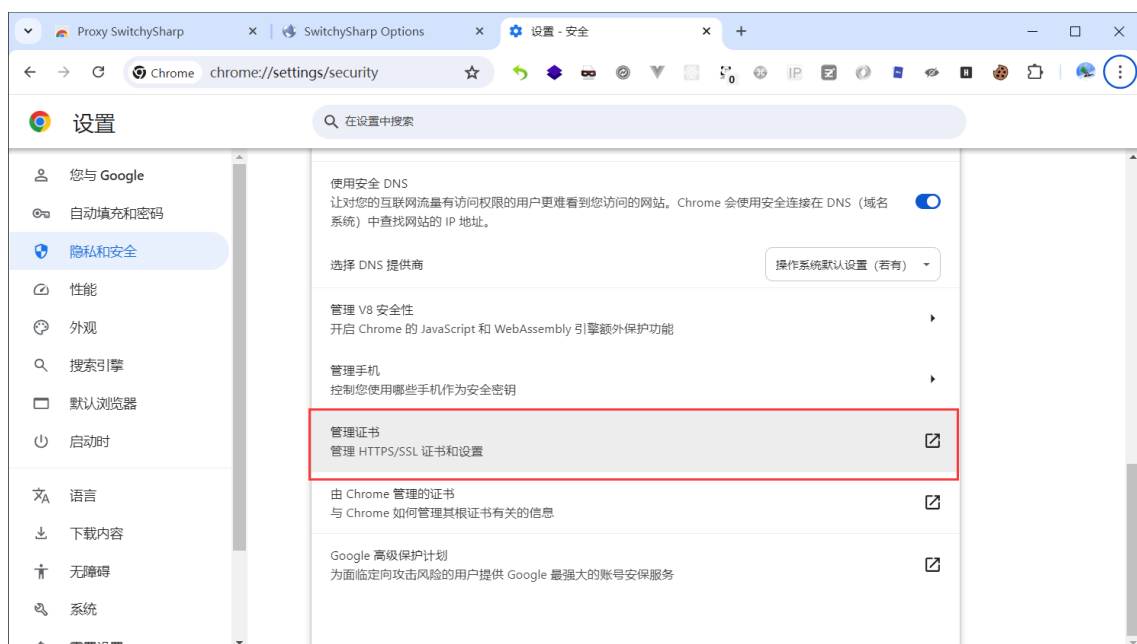
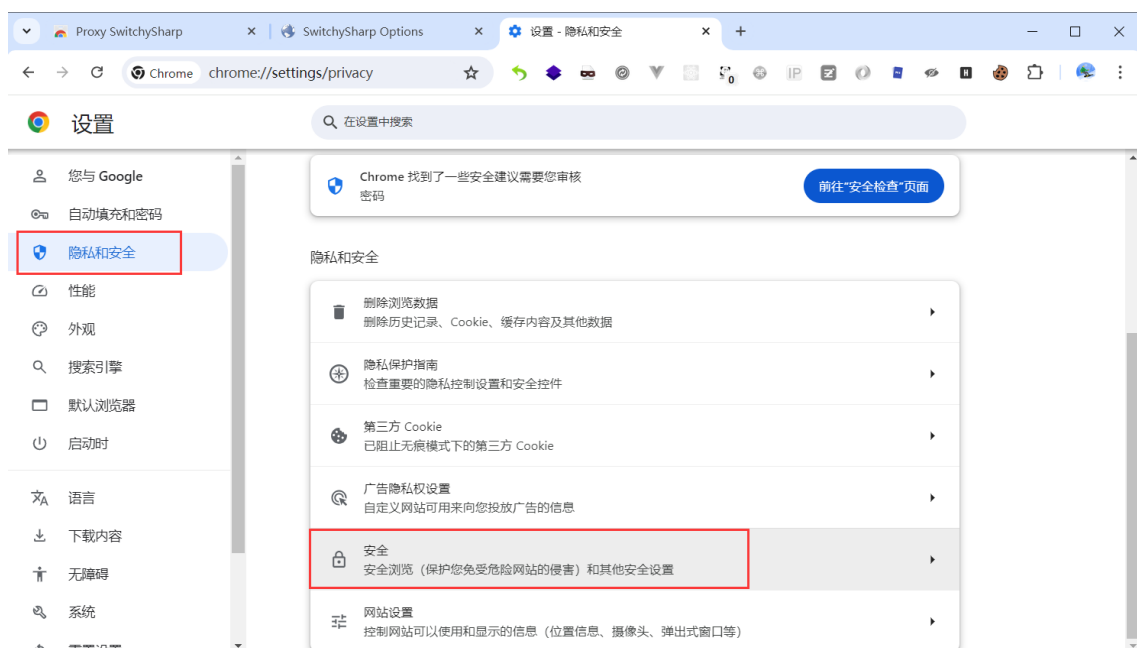


(2) chrome导入证书

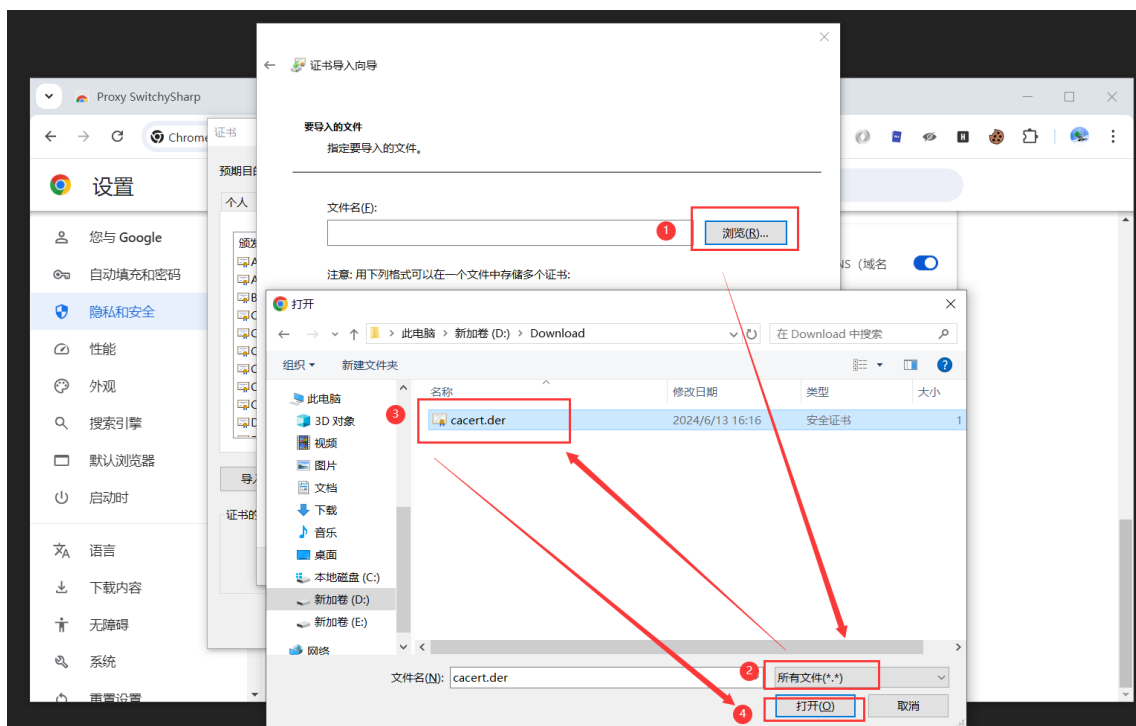
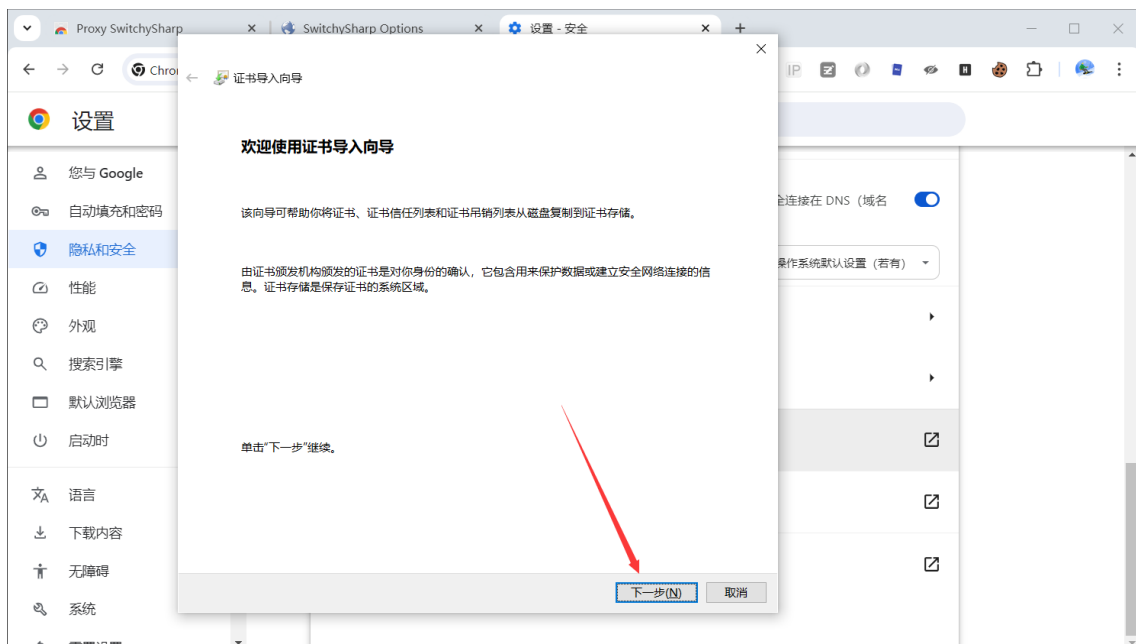
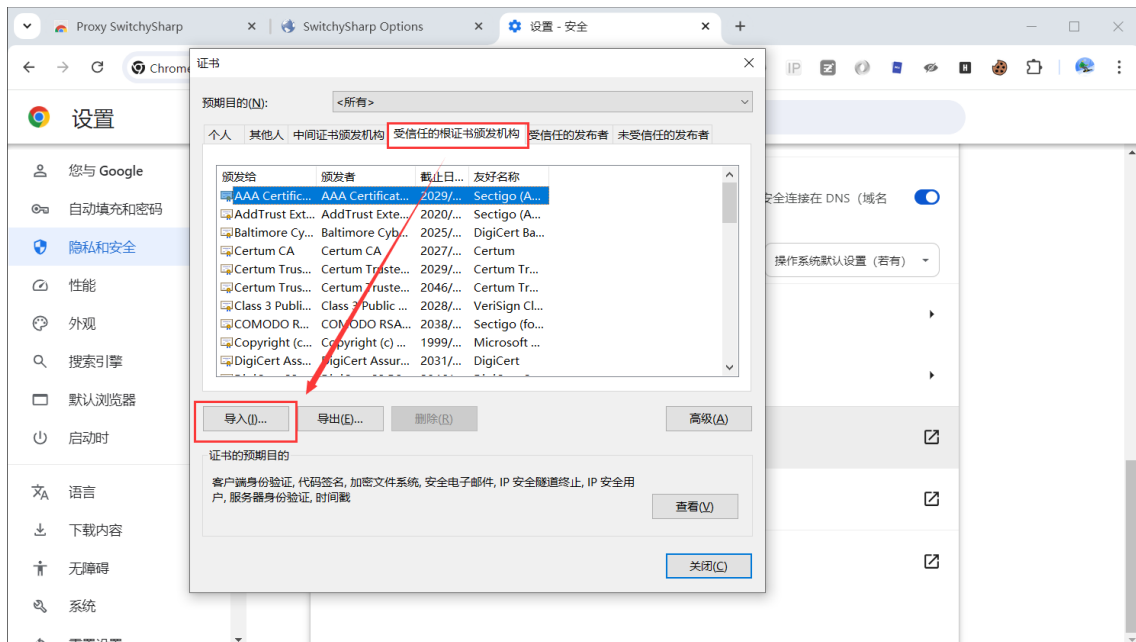
- 选择设置

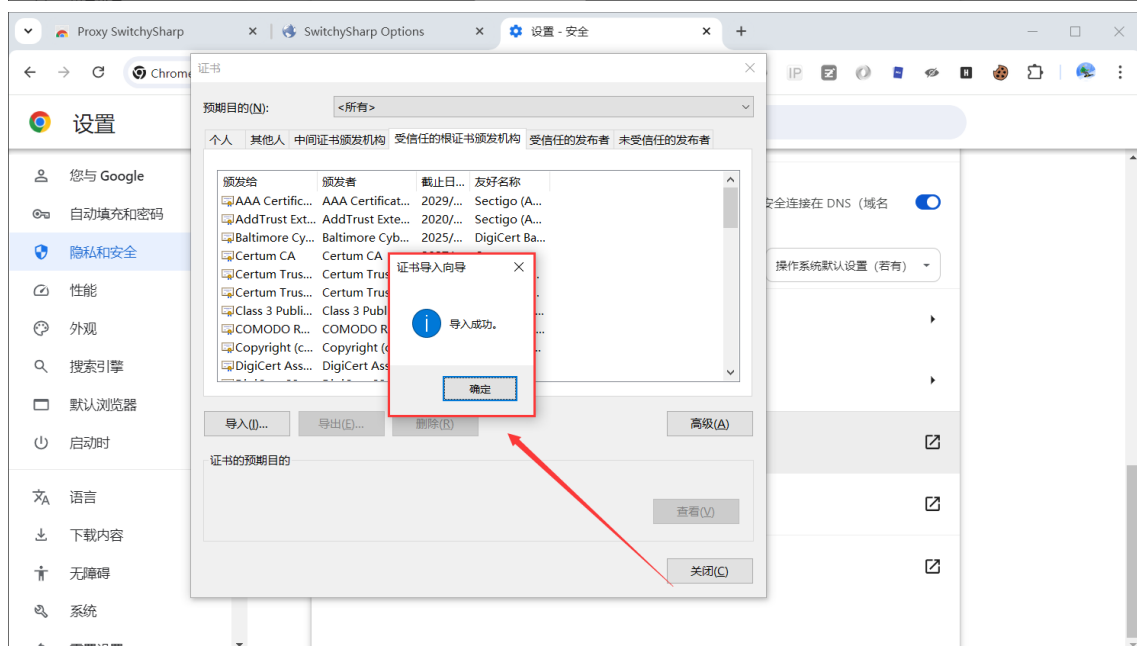
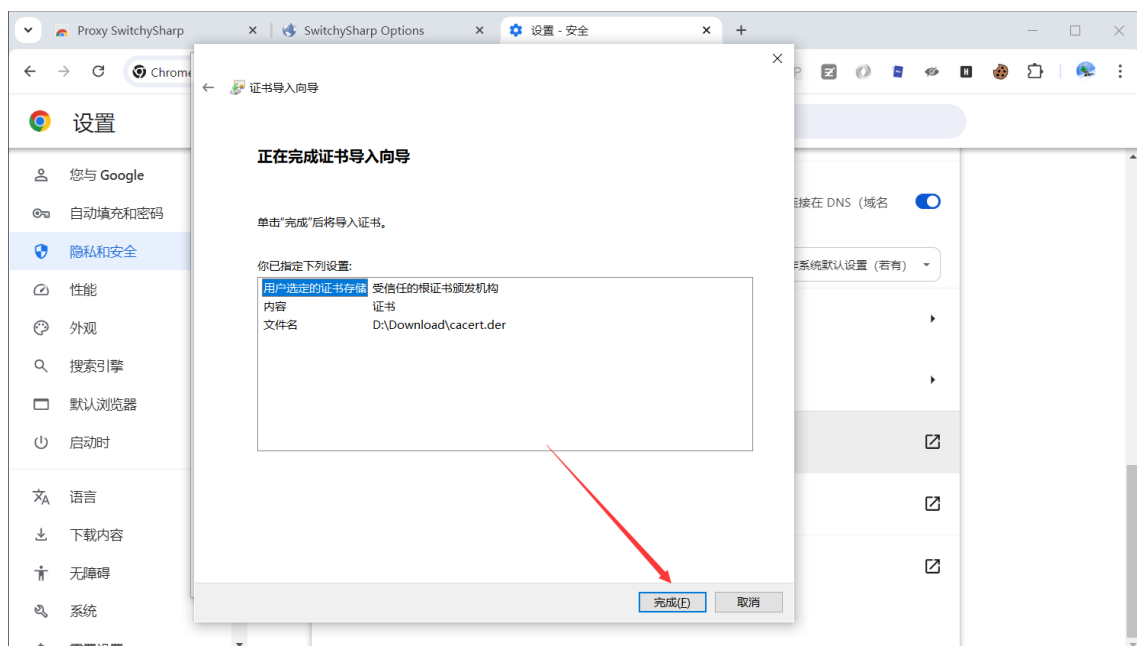
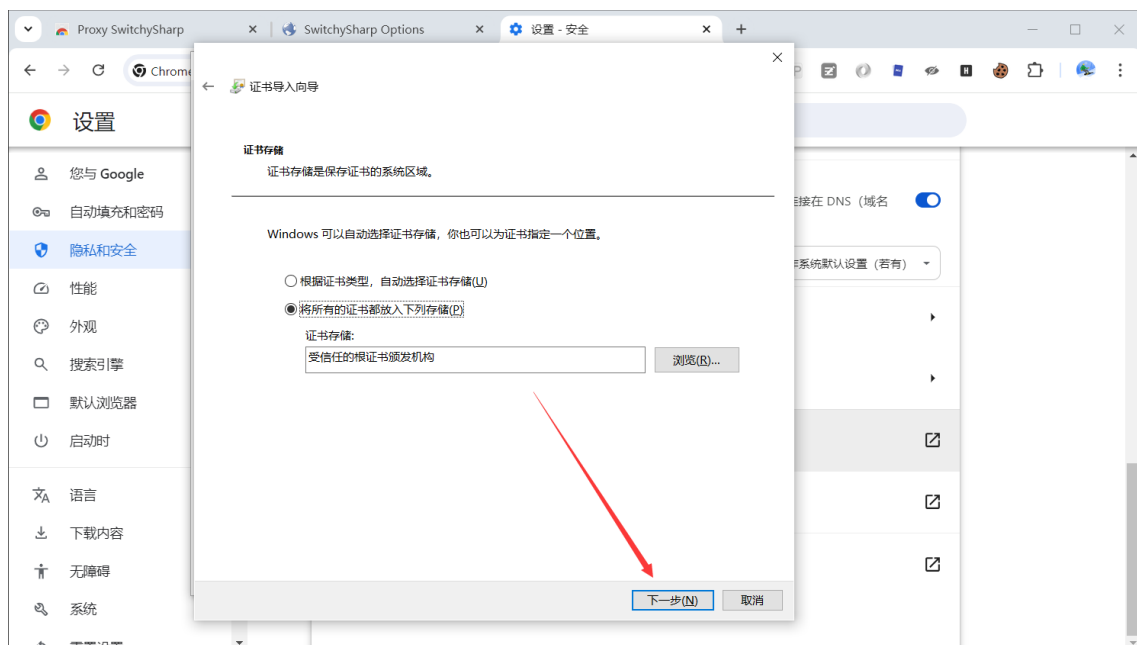


- 隐私和安全—安全—管理证书



- 导入证书

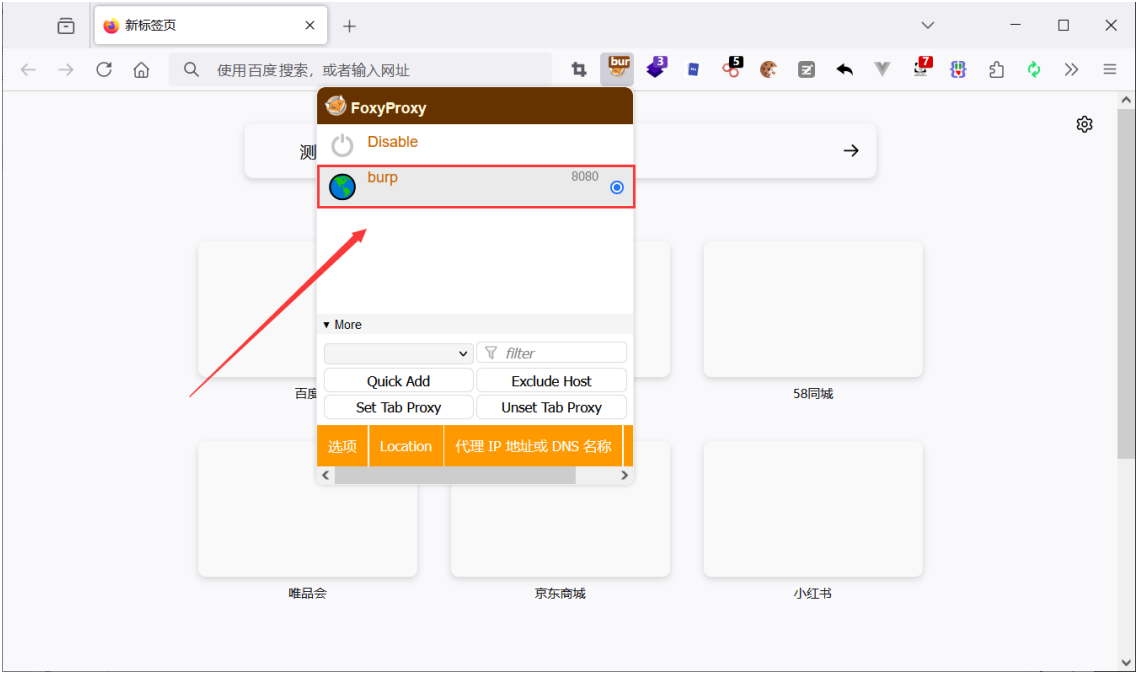




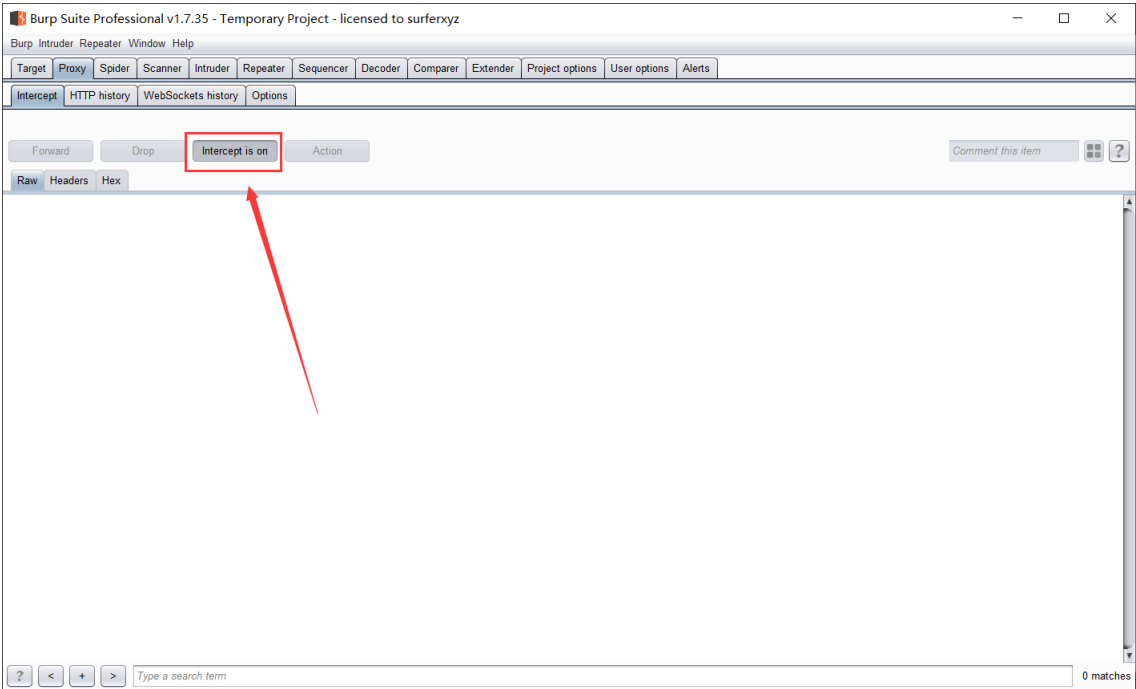
- 重启浏览器

6. 开启代理插件尝试抓包

- 开启代理选项



- 开启burp抓包



- 随便访问一个网站，测试是否能抓到包，这边访问百度，成功抓到

