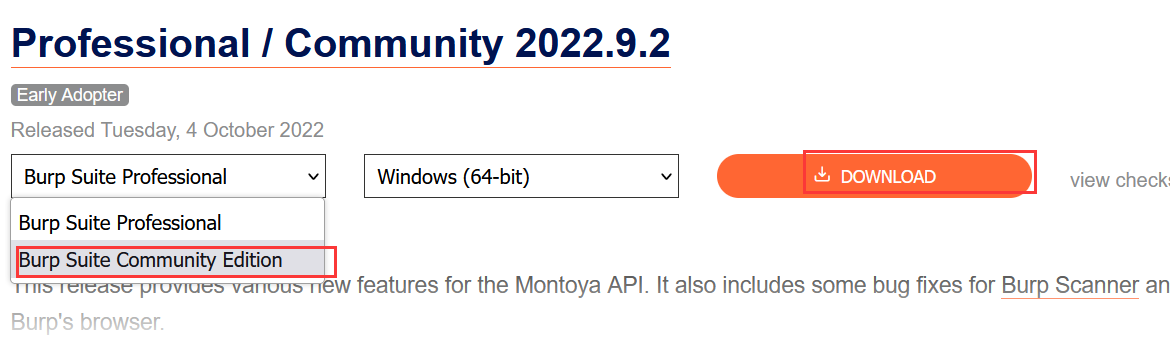
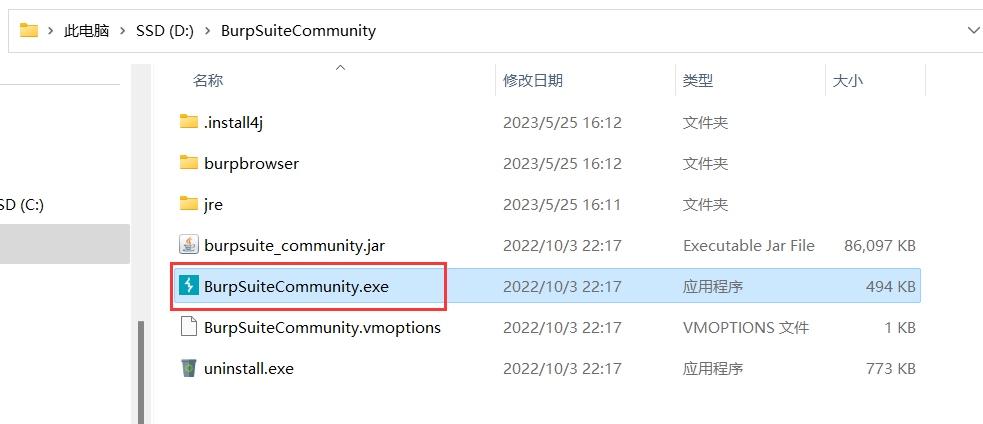
Burp Suite 是用于攻击web 应用程序的集成平台，包含了许多工具。Burp Suite为这些工具设计了许多接口，以加快攻击应用程序的过程。所有工具都共享一个请求，并能处理对应的HTTP 消息、持久性、认证、代理、日志、警报。

Burp Suite是由Java语言编写而成，使用之前需要先安装JAVA环境。教程略。

Burp Suite下载：<https://portswigger.net/burp/releases> 选择版本

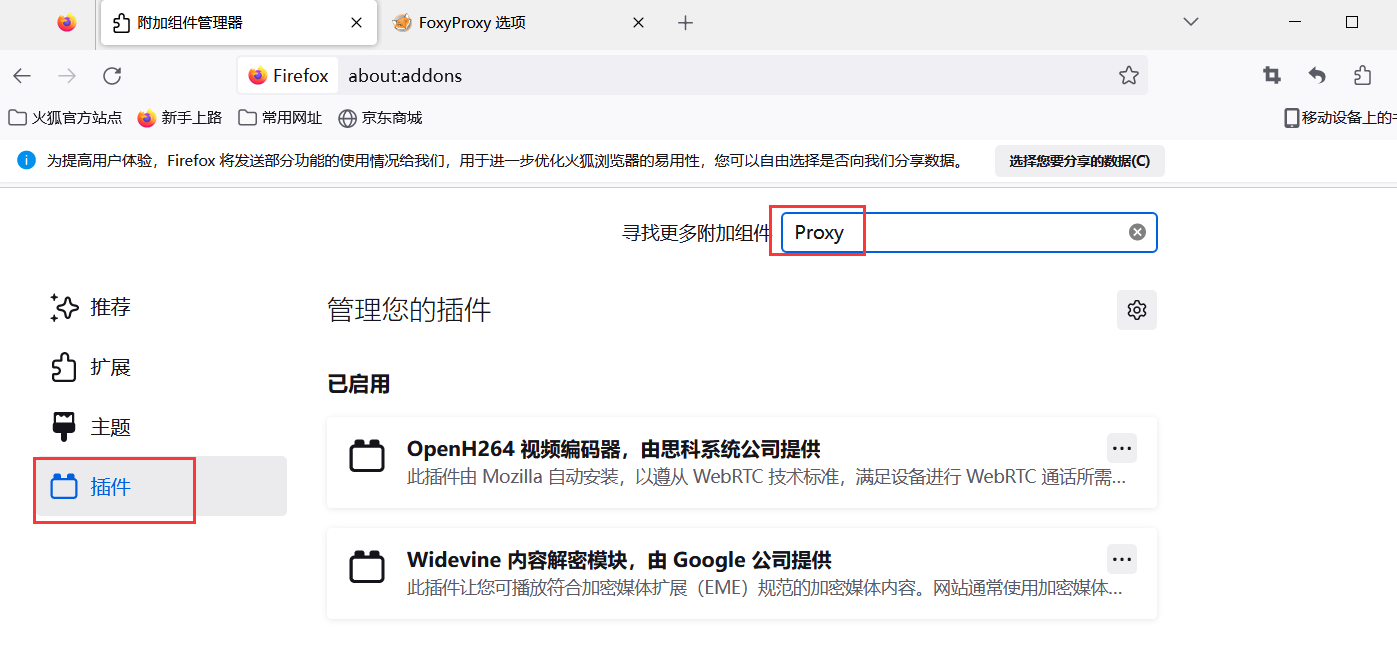


下载后安装(图片显示的是**社区版**，**专业破解版**安装：<https://ccalt.cn/2023/04/04/BurpSuite%E5%85%A8%E5%B9%B3%E5%8F%B0%E7%A0%B4%E8%A7%A3%E9%80%9A%E7%94%A8-%E8%87%B3%E4%BB%8A%E5%8F%AF%E7%94%A8/>)



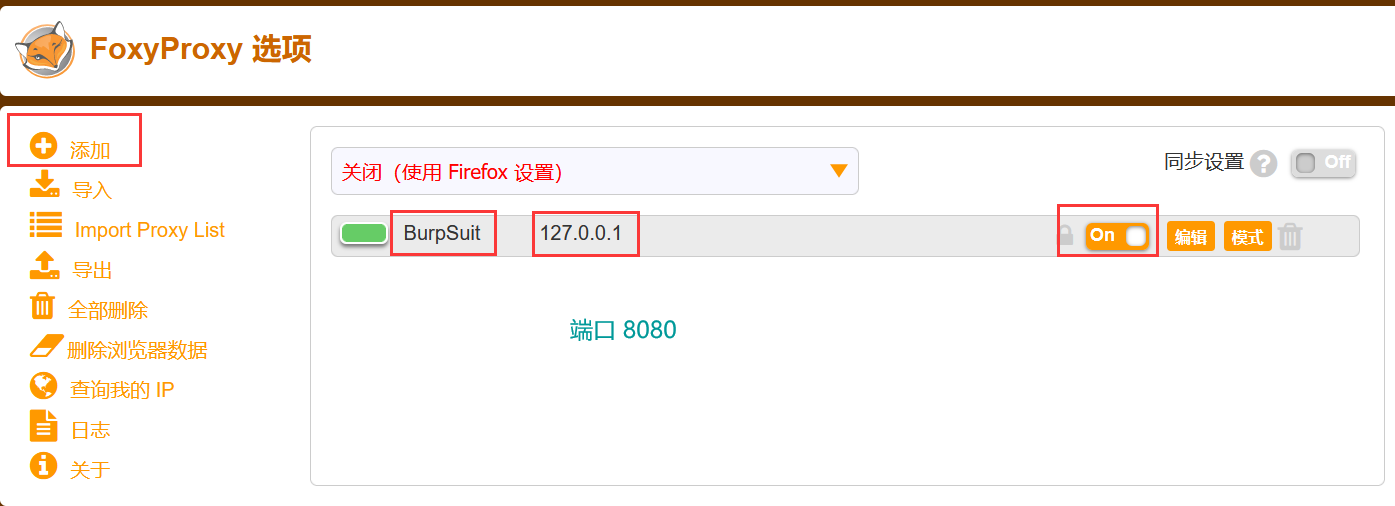
安装浏览器代理插件，以火狐浏览器为例：可参考<https://blog.csdn.net/elmoyan/article/details/126852647>

如果代理设置出问题，建议将浏览器**恢复默认后**重新开始。



火狐浏览器代理配置：目的是让火狐浏览器的请求先传往BurpSuite，在BurpSuite上进行流量数据的处理。

这里代理插件可以任选一个。

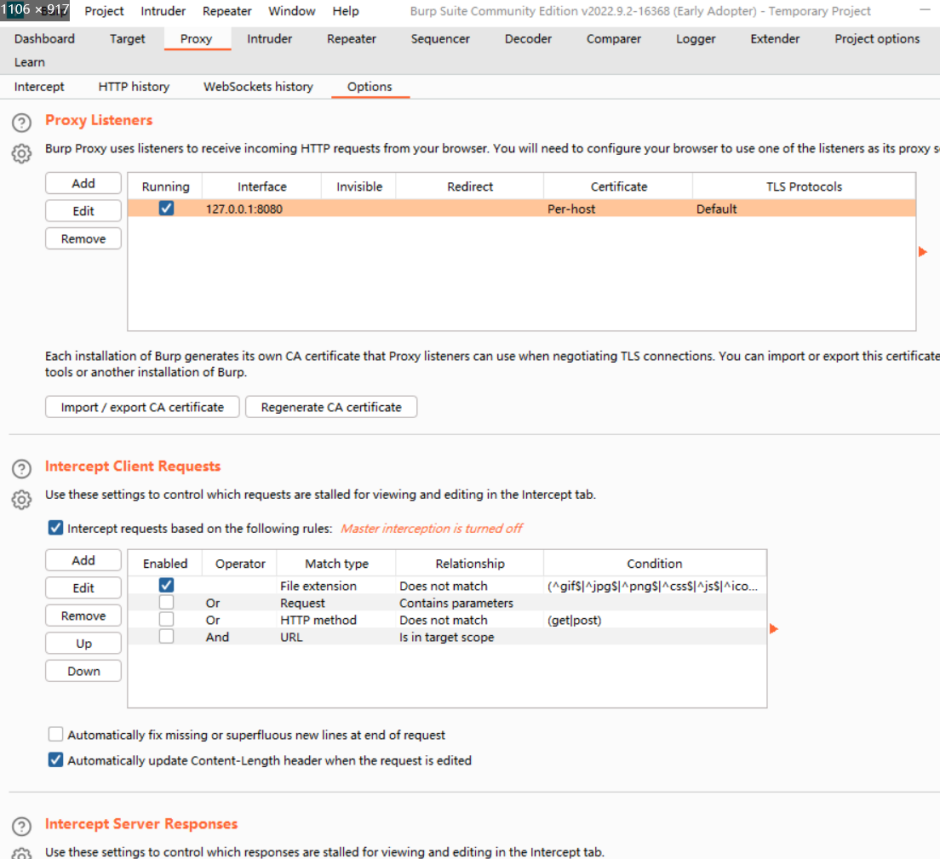




进入：<http://burp> 下载证书并打开，存储



证书安装完后，再访问HTTPS链接就不会报安全问题了（需注意重启浏览器才能生效）

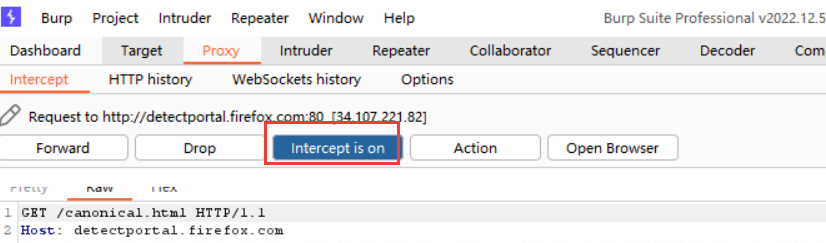
打开burp，设置burpsuite监听的ip和端口。

抓包测试：

burp抓包之前要先打开前面配置的浏览器代理。

学习BurpSuit-Proxy使用：<https://blog.csdn.net/elmoyan/article/details/127224990>

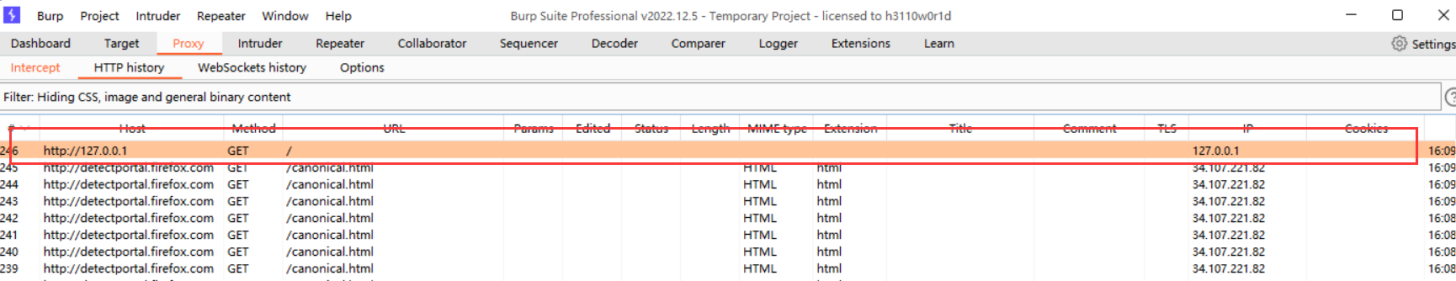
打开burp，打开拦截：



在浏览器输入靶场地址：



会发现burp中拦截到这个请求：



此时，浏览器的状态是等待的，因为这个请求被burp拦截还未被**放行**（**forward**）。

抓包的时候：**Interception is off（后面SQL注入实验中，多数情况下是抓包状态）**

拦截请求时**：Interception is on**