Web基础

Web：即万维网，由许多互相链接的超文本组成的系统，通过互联网访问

动态网页：能与后台数据库进行交互，数据传递，网页内容可能根据访问者身份不同而动态生成。

静态网页：纯粹HTML（标准通用标记语言下的一个应用）格式的网页通常被称为“静态网页”，静态网页是标准的HTML文件，它的文件扩展名是.htm、.html，可以包含文本、图像、声音、FLASH动画、客户端脚本和ActiveX控件及JAVA小程序等。

前端（html css JavaScript） 语言一定要去学

后端（php python java） 可以先只学一个PHP

数据库（sql） sql语言

学习语言网站推荐：<https://www.w3cschool.cn/> <https://www.runoob.com/>

C/S架构：客户端/服务器架构，指服务器负责数据的管理，客户机负责完成与用户的交互任务。

服务器：服务器是计算机的一种，它比普通计算机运行更快、负载更高、价格更贵。根据服务器所提供的服务，一般来说服务器都具备承担响应服务请求、承担服务、保障服务的能力。结构与普通的计算机内部结构相差不大

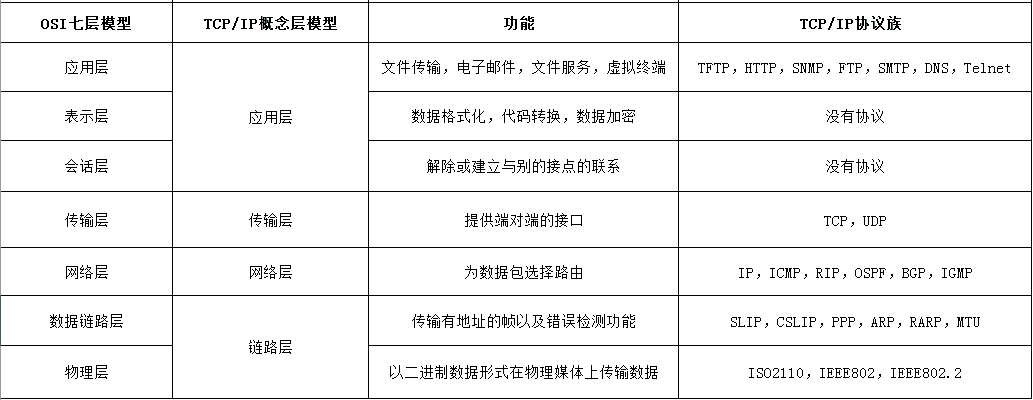
局域网（LAN）：局域网自然就是局部地区形成的一个区域网络，其特点就是分布地区范围有限，可大可小，如家庭局域网、公司局域网

广域网（WAN）：又称广域网、外网、公网。是连接不同地区局域网或城域网计算机通信的远程网。

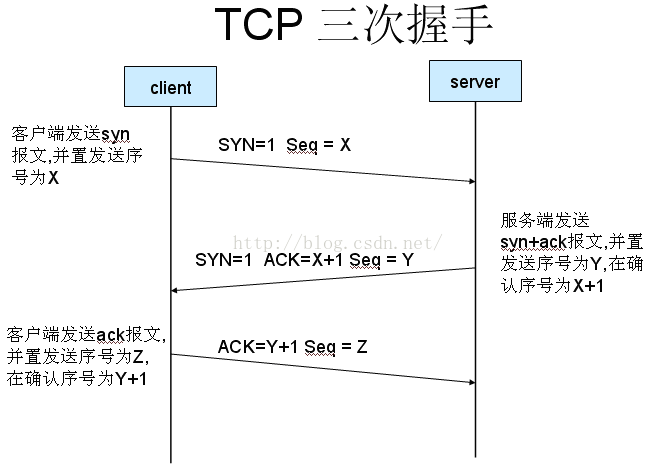
虚拟机：指通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统

网卡：网卡是一块被设计用来允许计算机在计算机网络上进行通讯的计算机硬件。拥有全球唯一的MAC地址。

MAC地址：直译为媒体存取控制位址，也称为局域网地址（LAN Address），MAC位址，以太网地址（Ethernet Address）或物理地址（Physical Address），它是一个用来确认网络设备位置的位址



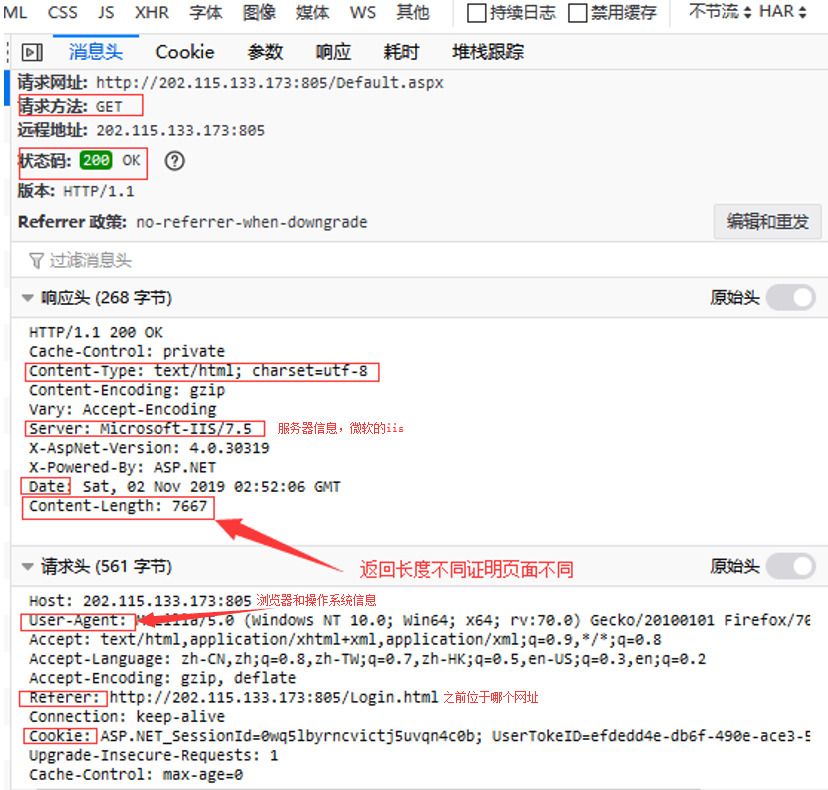
OSI七层模型：

查看IP： Windows下：ipconfig Linux下：ifconfig

HTTP协议（Hyper Text Transfer Protocol）：

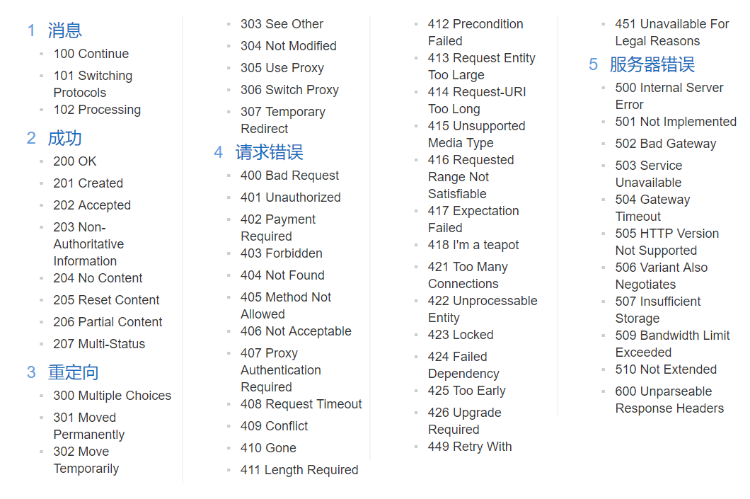
HTTP 协议构建于 TCP/IP 协议之上，是一个应用层协议，默认端口号是80

HTTP 是无连接无状态的

HTTP请求头、响应头

GET：从指定的资源请求数据。在url中传输，且长度有限制，因为url的长度最长是2048个字符

POST：向指定的资源提交要被处理的数据，长度没有限制，更安全，提交的参数不会显示在url中

状态码：表明网页服务器超文本传输协议响应状态的3位数字代码。

Referer：用来让服务器判断来源页面, 即用户是从哪个页面来的

X-Forwarded-For:是一个 HTTP 扩展头部，主要是为了让 Web 服务器获取访问用户的真实 IP 地址

Cookie：某些网站为了辨别用户身份，进行Session跟踪而储存在用户本地终端上的数据（通常经过加密），当用户再次访问时带上cookie进行请求，就不用再验证身份了

URL（Uniform Resource Locator）统一资源定位符

协议://域名/目录/文件

因为我们不能随意对别人的网站发起攻击，所以就自己搭一个靶机：

Dvwa：（Damn Vulnerable Web Application）是一个用来进行安全脆弱性鉴定的PHP/MySQL Web应用，旨在为安全专业人员测试自己的专业技能和工具提供合法的环境

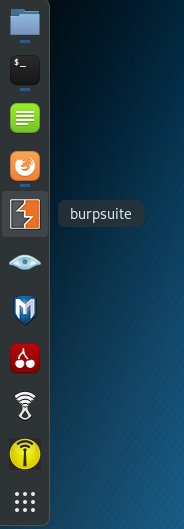
配置方法自行百度

Burpsuite：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

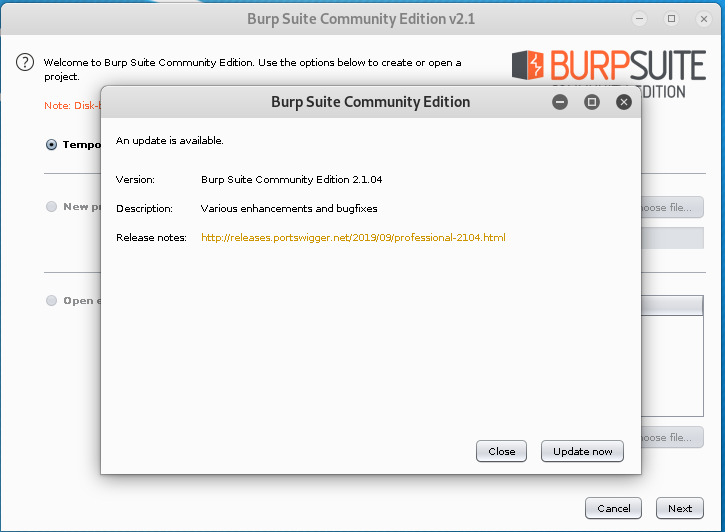
下载指南：<https://dwz.cn/d9p5tnfY> 百度一搜有很多的，找不到再QQ找我吧

使用指南：

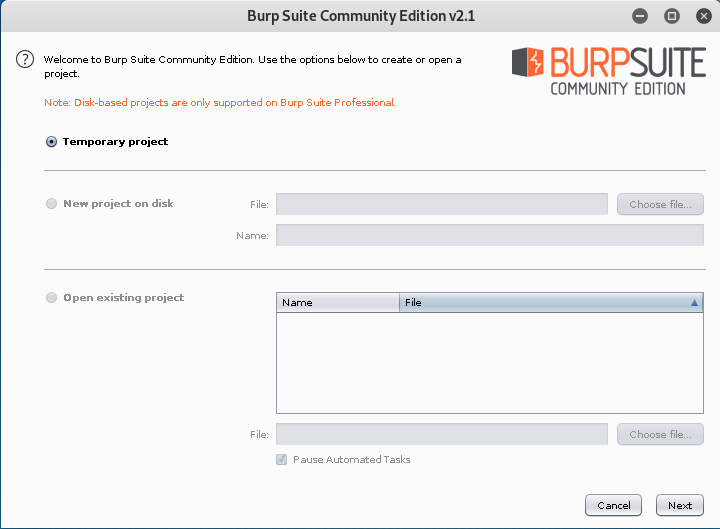
<https://t0data.gitbooks.io/burpsuite/content/chapter1.html>



Kali Linux自带（不过不是专业版）

安装好后：

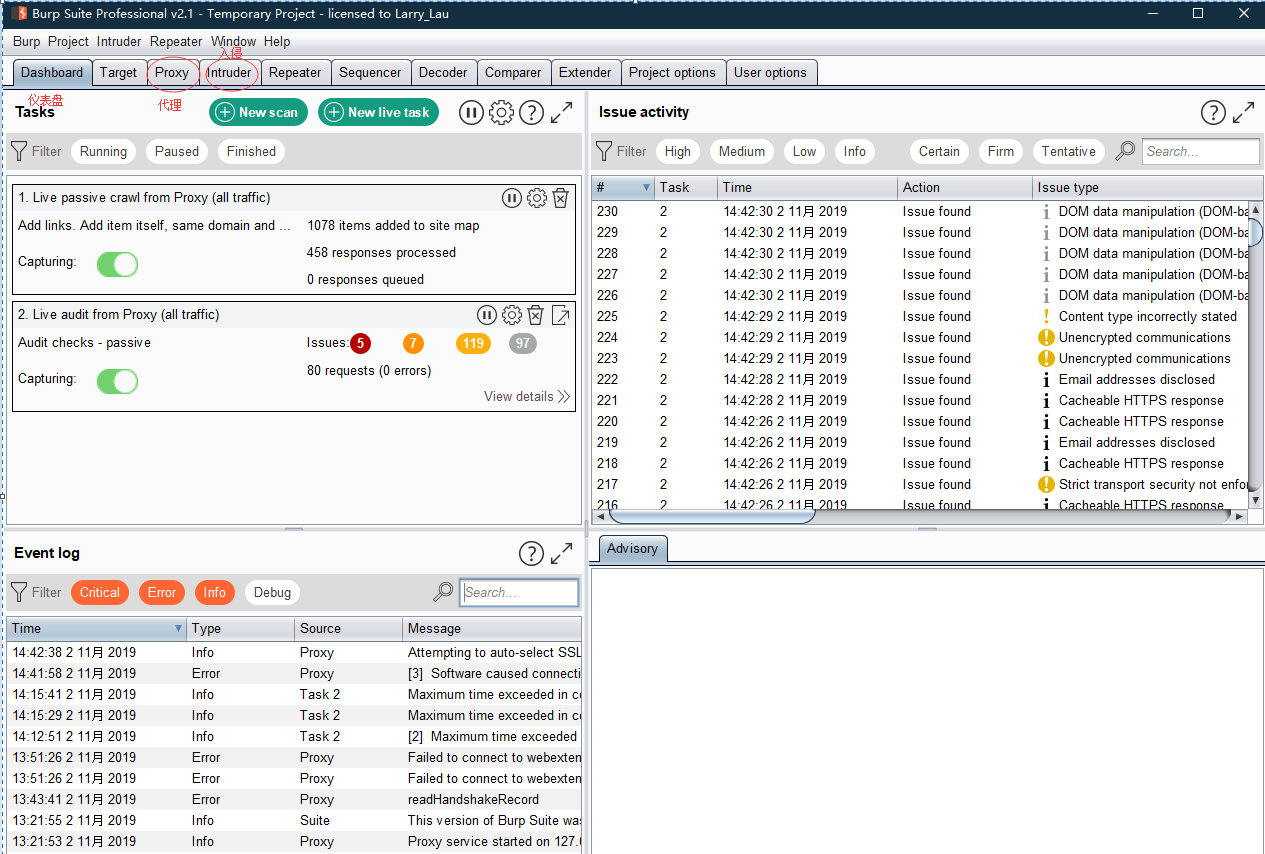
这里（可能会）提示有新版本，点击close关闭

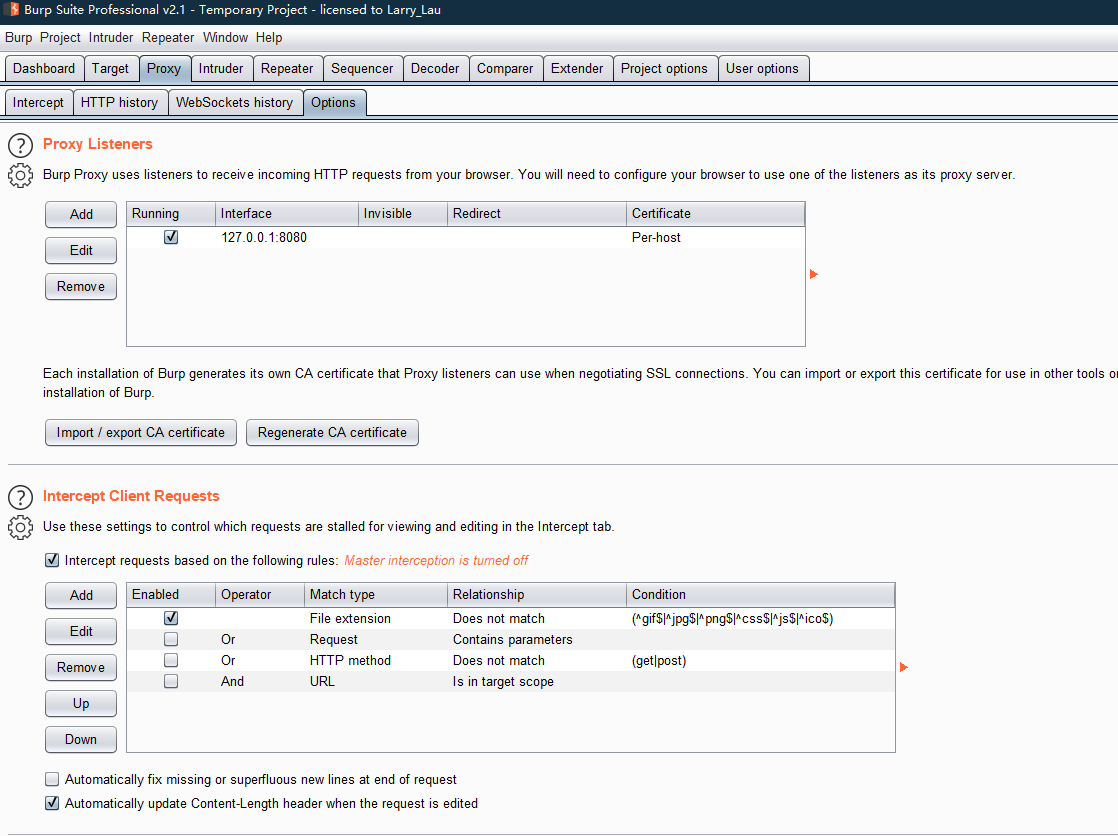


第一个选项，创建一个临时项目，然后点击next下一步

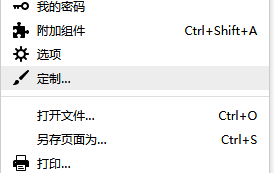
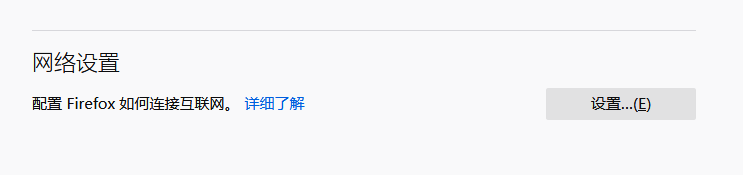


勾选默认配置，开始

抓包、攻击常用代理和入侵两个功能模块



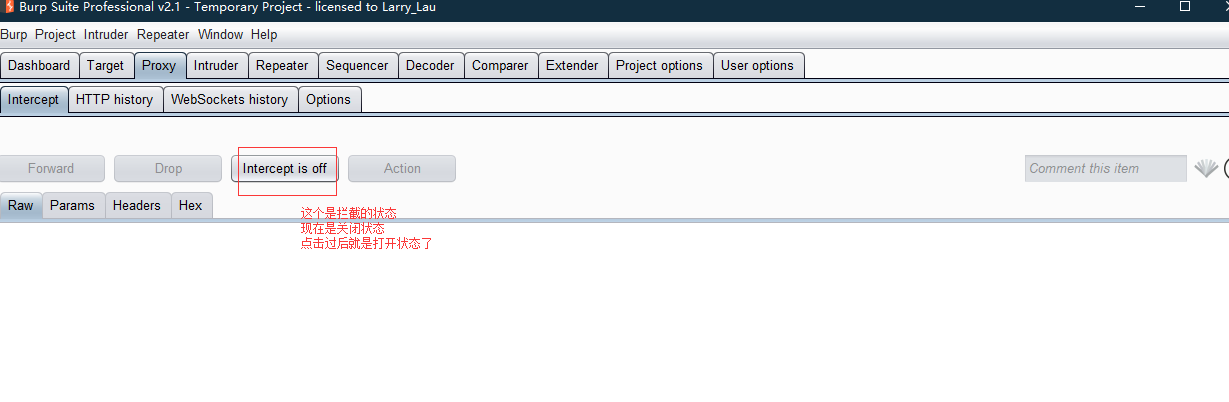
默认分配的代理地址和端口是127.0.0.1 ：8080,我们可以从Burp Suite的proxy选项卡的options上查看

为火狐浏览器设置代理

找到选项

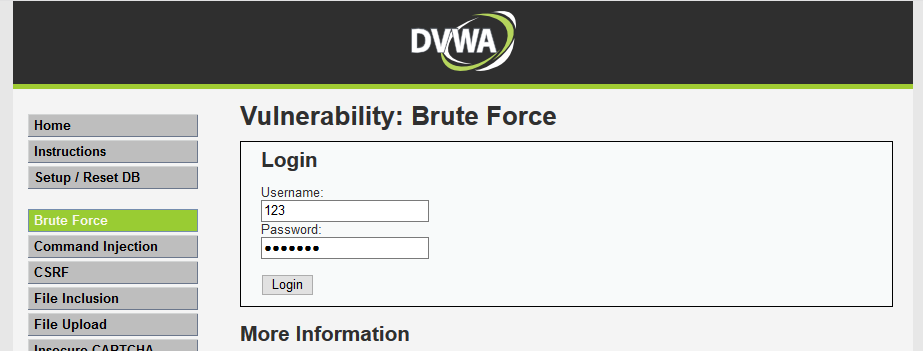
选项进去滑到最底，点击设置

按照图示配置，抓包结束后再将选项选回不使用代理服务器

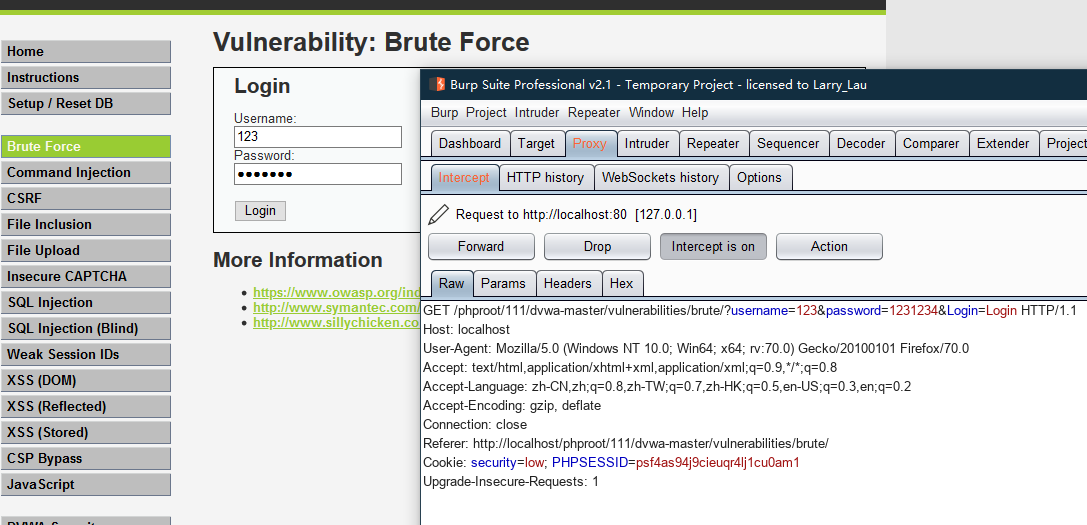
设置完毕就可以开始抓包啦

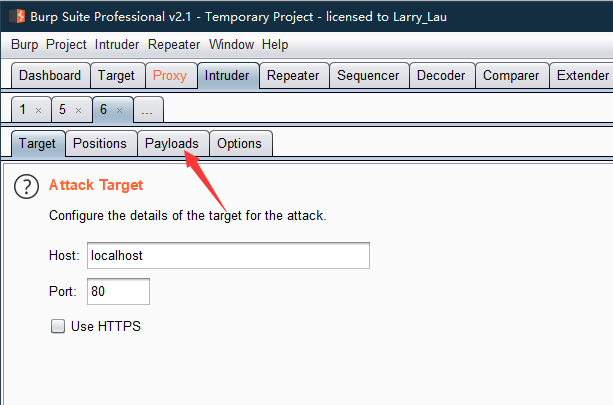
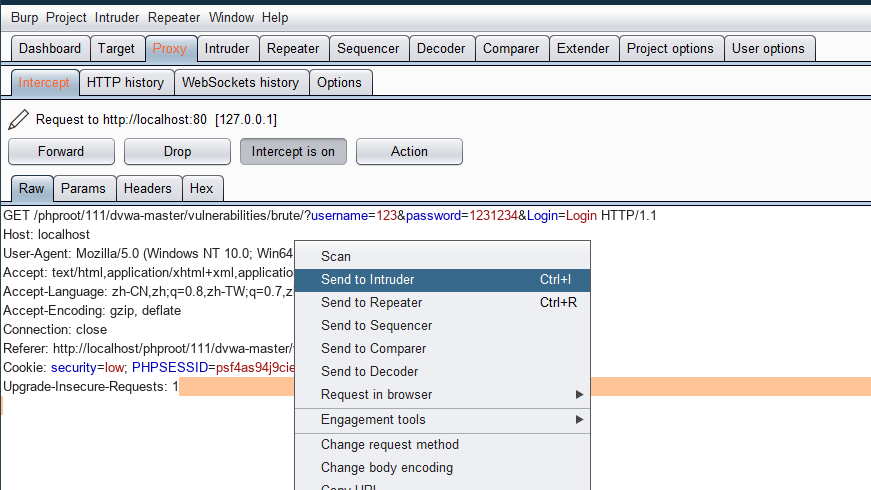
打开之后，浏览器每次点击都会一直转圈，因为请求被burpsuite拦截了

中文对照图



选择brute force 右侧登录框随便填，然后到burpsuite 开始抓包，点击后再回到dvwa点击login登录，此时burpsuite已经拦截了浏览器的请求数据了

这里的内容就是请求头

右键单击，选择send to intruder，此时工具栏Intruder字体变色，然后点击它

点击payloads 设置字典（出问题了后面的内容都删了）

前面这个配置字典过程有点问题，没有说到要选择攻击方式，这里有四种攻击方式：

第一种：

Sniper标签 这个是我们最常用的，Sniper是狙击手的意思。这个模式会使用单一的payload【就是导入字典的payload】组。它会针对每个position中$$位置设置payload。这种攻击类型适合对常见漏洞中的请求参数单独地进行测试。攻击中的请求总数应该是position数量和payload数量的乘积。

第二种：

Battering ram – 这一模式是使用单一的payload组。它会重复payload并且一次把所有相同的payload放入指定的位置中。这种攻击适合那种需要在请求中把相同的输入放到多个位置的情况。请求的总数是payload组中payload的总数。简单说就是一个playload字典同时应用到多个position中

第三种：

Pitchfork – 这一模式是使用多个payload组。对于定义的位置可以使用不同的payload组。攻击会同步迭代所有的payload组，把payload放入每个定义的位置中。比如：position中A处有a字典，B处有b字典，则a【1】将会对应b【1】进行attack处理，这种攻击类型非常适合那种不同位置中需要插入不同但相关的输入的情况。请求的数量应该是最小的payload组中的payload数量

第四种：

Cluster bomb – 这种模式会使用多个payload组。每个定义的位置中有不同的payload组。攻击会迭代每个payload组，每种payload组合都会被测试一遍。比如：position中A处有a字典，B处有b字典，则两个字典将会循环搭配组合进行attack处理这种攻击适用于那种位置中需要不同且不相关或者未知的输入的攻击。攻击请求的总数是各payload组中payload数量的乘积。

这里我们应该选择第四种攻击方式，第四种方式需要设置两个字典

找到个视频，从第八分钟开始看就可以了（其他的漏洞类型也可以跟着这个视频做一做）

<https://www.bilibili.com/video/av66653656/?p=3>



这里就是两个字典了（电脑上双击图标可以打开）然后可以自己创建txt文档保存下来

课后作业： 注册攻防世界：<https://adworld.xctf.org.cn/>

答题里面web新手练习区

View\_socrce (查看网页源码)

get\_post （get post两种请求方式）

cookie（查看cookie）

xff\_referer（修改xff、referer绕过检测）

weak\_auth (弱口令，可猜可爆破)

webshell（百度中国菜刀用法）