网站搭建：

流程：购买域名和服务器(选择操作系统)、域名备案(国内服务器一般需要备案)和解析、利用集成化软件比如“宝塔”搭建网站

域名：例如[www.baidu.com](http://www.baidu.com)；国内一般需要备案，但比如中国香港就不需要备案

服务器：windows、linux；一般2核4G就行

DNS域名解析：将域名解析为IP地址

网站组成：

开发语言：asp、php、aspx、jsp、java、python、ruby、go、html、javascript等

程序源码：根据开发语言分类；应用类型分类；开源CMS分类(开源模板)；开发框架分类等

中间件容器：IIS、Apache、Nginx、Tomcat、Weblogic、Jboos、glasshfish等

数据库类型：Access、Mysql、Mssql、Oracle、db2、Sybase、Redis、MongoDB等

服务器操作系统：Windows系列、Linux系列、Mac系列等

第三方软件：phpmyadmin、vs-ftpd、VNC、ELK、Openssh等

现在有一些网站搭建集成化软件，比如“宝塔”

WEB应用安全漏洞分类：

SQL注入、文件安全、RCE执行、XSS跨站、CSRF/SSRF/CRLF、反序列化、逻辑越权、未授权访问、XXE/XML、弱口令安全等

大部分网站漏洞的根源：程序源码

数据包：

Accept：指浏览器或其他客户可以接爱的MIME文件格式;Servlet可以根据它判断并返回适当的文件格式

User-Agent：客户浏览器名称

Host：对应网址URL中的Web名称和端口号

Accept-Langeuage：指出浏览器可以接受的语言种类，如en或en-us，指英语

connection：用来告诉服务器是否可以维持固定的HTTP连接。http是无连接的，HTTP/1.1使用Keep-Alive为默认值，这样，当浏览器需要多个文件时(比如一个HTML文件和相关的图形文件)，不需要每次都建立连接

Cookie：浏览器用这个属性向服务器发送Cookie。Cookie是在浏览器中寄存的小型数据体，它可以记载和服务器相关的用户信息，也可以用来实现会话功能

Referer：表明产生请求的网页URL。如比从网页/icconcept/index.jsp中点击一个链接到网页/icwork/search，在向服务器发送的GET/icwork/search中的请求中，Referer是http://hostname:8080/icconcept/index.jsp。这个属性可以用来跟踪Web请求是从什么网站来的

Content-Type：用来表明request的内容类型。可以用HttpServletRequest的getContentType()方法取得

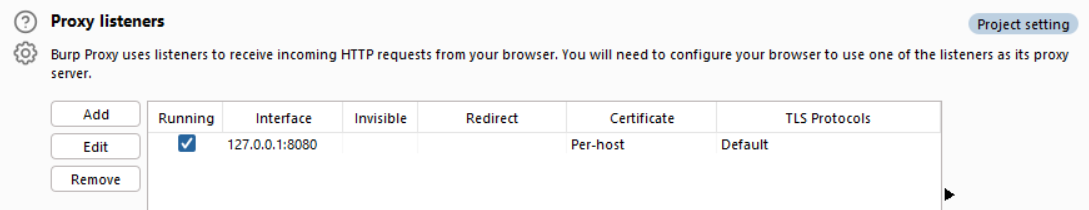
Accept-Charset：指出浏览器可以接受的字符编码。英文浏览器的默认值是ISO-8859-1.

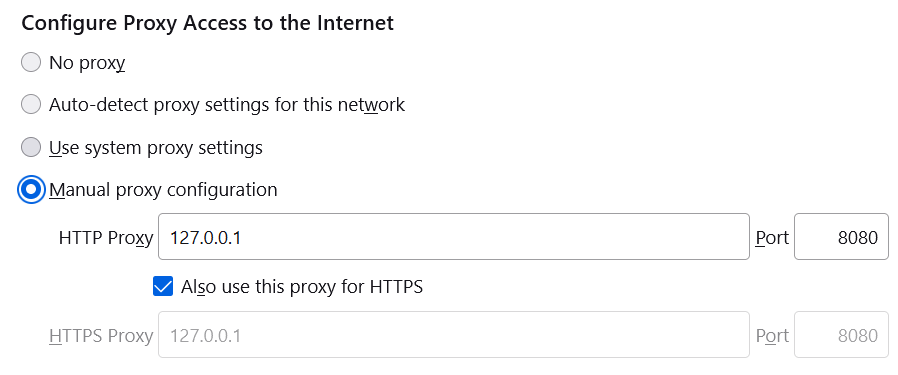
Accept-Encoding：指出浏览器可以接受的编码方式。编码方式不同于文件格式，它是为了压缩文件并加速文件传递速度。浏览器在接收到Web响应之后先解码，然后再检查文件格式

代理：

利用burpsuite抓包：某浪新闻点赞

设置代理：





设置代理，可以解决“禁IP”的问题

UA头：手机还是电脑



通过状态码判断：

文件夹：403存在 404不存在

文件：200存在 404不存在

常见的 HTTP 状态码：

200 - 请求成功

301 - 资源（网页等）被永久转移到其它URL

404 - 请求的资源（网页等）不存在

500 - 内部服务器错误