**功能测试与抓包工具**

抓包就是将**网络传输发送与接收的数据包进行截取**，重发，编辑，转存等操作，也用来检查网络安全。抓包经常被用来进行数据截取等。

常用的抓包工具：fiddler,Charles,F12

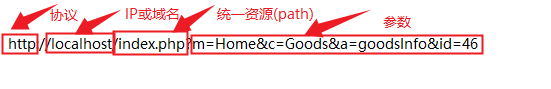
**HTML与HTTP协议**

URL：统一资源定位符

HTML：超文本标记语言

HTTP：超文本传输协议

**URL格式：**



协议：客户端和服务端通讯的标准，HTTP、HTTPS

IP或域名:

端口号：协议默认的端口号是可以省略的

资源路径(path)：资源存放的位置，资源可以是各种超文本信息，如音频，视频等

**参数**：

1. 用?与URL的主体部分分开

2）参数的格式 参数名=参数值，有多个参数时用&拼接即可

**HTTP请求与响应**

基本概念：

客户端：用于发送请求，如浏览器，APP等

 服务端：处理客户端请求并返回数据，如

请求：客户端向服务器索要数据

响应：服务器处理完成后，返回数据与信息给客户端

**Fiddler原理**

原理：

1. 请求先发送给fiddler，fiddler接收请求后转发给服务器

2、服务器处理请求后将响应数据返回给fiddler，fiddler在转发给客户端（浏览器）

**HTTP请求**

请求内容

**请求行：**

1）位置是在第一行

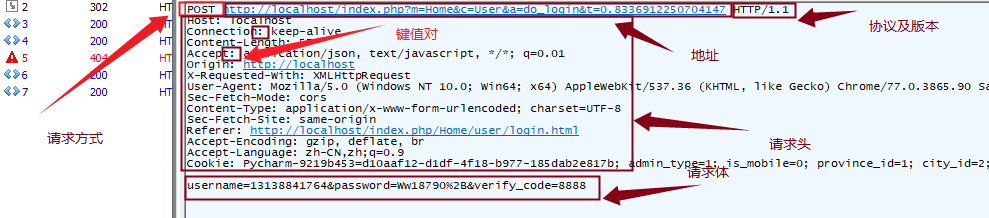
**2）请求方式，请求地址，协议及版本**

**请求头：**

1）位置是在第一行之后，到空行之前

2）用来描述客户端信息的相关参数，一般以**键值对**的形式存在，如描述浏览器类型等

**请求体：**位置在空行之后

**HTTP响应(报文)**

响应内容

**响应行**

1）位置是在第一行

2）协议及版本，响应状态码，状态消息

**响应头**

1)位置是在第一行之后，空行之前

2)告诉客户端服务器相关信息，如web服务器类型

**响应体**

位置在空行之后，如登录成功

**HTTP响应内容**

在状态码用数字表示的响应状态，最常见的有：

200：表示成功

3xx：表示数据路径发生改变-->重定向302,304

4xxx：表示客户端问题

1. ->表示页面没有找
2. ->表示访问的数据被禁止

5xx:表示服务器错误

1. 响应数据的长度，通常返回的数据内容越多，用户等待时间越长
2. 响应数据的类型，除了可以返回网页数据外还可以返回：图片、文字、音乐...

**响应状态码**

由3位数组成，第一位数字代表响应消息的级别

2xx：成功，如200

3xx:重定向，如302

4xx:客户端存在问题，如404

5xx：服务器端存在问题，如501

**面试题：get和post的区别**

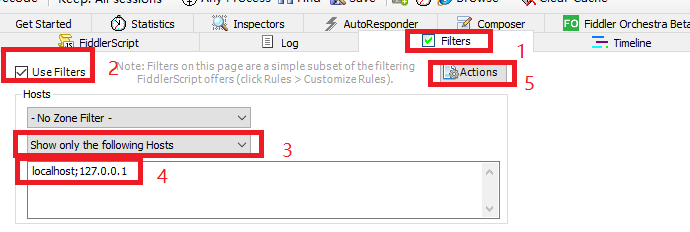
1. **最直观的区别就是get把参数包含在URL中，post通过请求体传递参数**
2. **get比post更不安全，因为参数直接暴露在URL上，所以不能用来传递敏感信息**
3. get在浏览器回退时是无害的，而post会再次提交请求
4. get请求只能进行URL编码，而post支持多种编码方式
5. get请求参数会被完整保留在浏览器历史记录里，而post中的参数不会被保留
6. **get请求在URL中传递的参数是有长度限制（浏览器导致）的，而post没有**
7. 对参数的数据类型,get只接受ASCII字符，而post没有限制
8. get参数通过URL传递，post放在请求体中

**Fiddler为什么能抓到数据？**

代理的作用

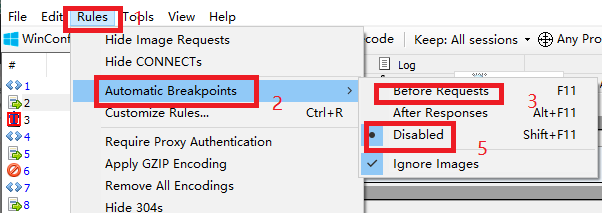
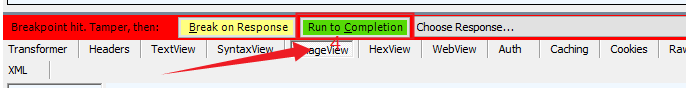
**设置过滤**

1. 点击Filters页签，勾选”Use Filters”
2. Host下方的第二个下拉框，选择”show only the following Hosts”
3. 在下方输入框中输入要抓包的主机地址（多个地址用英文分号隔开，如:localhost;127.0.0.1）
4. 点击右上角的“Actions”选择“Run Filterset Now”
5. 如果取消过滤，去掉”Use Filters”的勾选



**设置断点**

在服务端修改手机号码为6位



**修改响应**