

# burpsuite 之 Proxy

## 1、简介

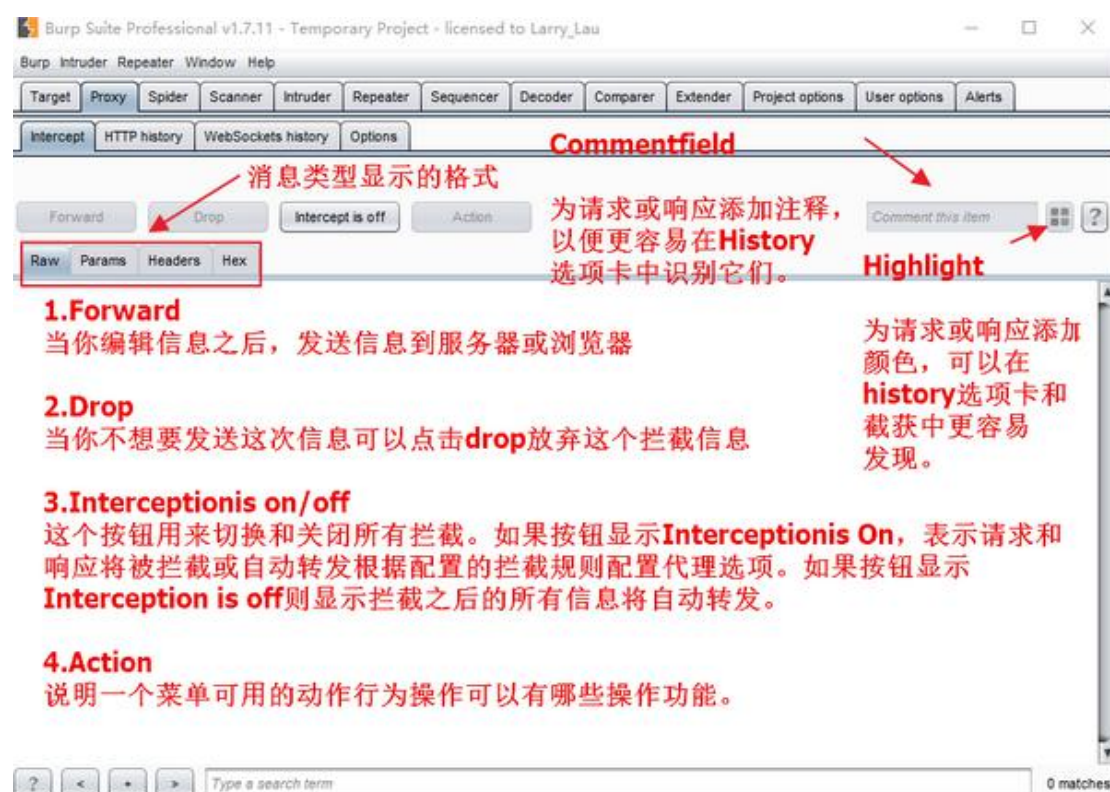
Proxy 代理模块作为 BurpSuite 的核心功能，拦截 HTTP/S 的代理服务器，作为一个在浏览器和目标应用程序之间的中间人，允许你拦截，查看，修改在两个方向上的原始数据流。

Burp 代理允许你通过监视和操纵应用程序传输的关键参数和其他数据来查找和探索应用程序的漏洞。通过以恶意的方式修改浏览器的请求，Burp 代理可以用来进行攻击，如：SQL 注入，cookie 欺骗，提升权限，会话劫持，目录遍历，缓冲区溢出。拦截的传输可以被修改成原始文本，也可以是包含参数或者消息头的表格，也可以十六进制形式，甚至可以操纵二进制形式的数据。在 Burp 代理可以呈现出包含 HTML 或者图像数据的响应消息。

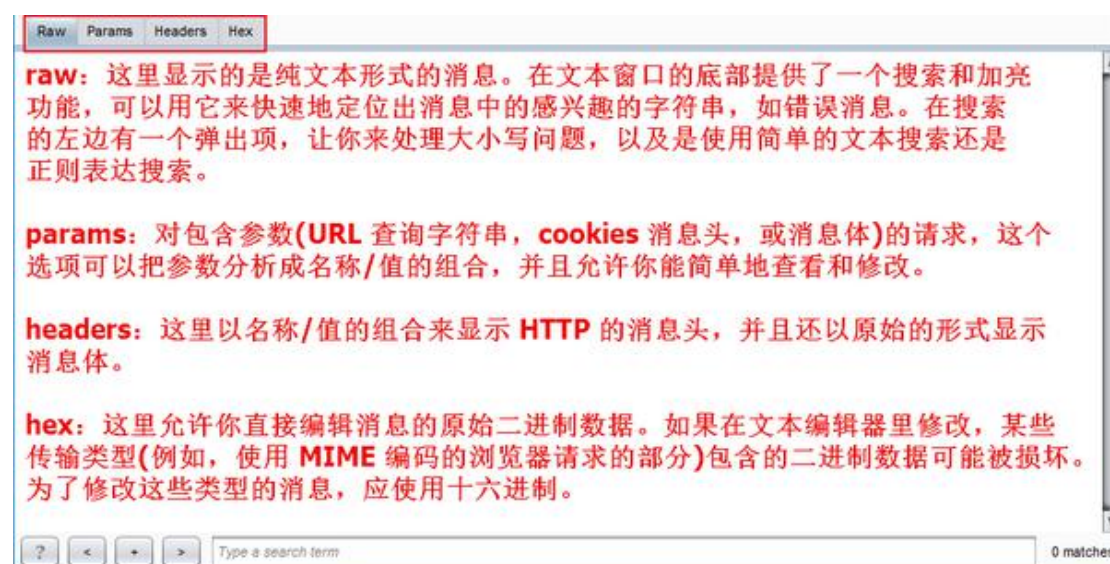
## 2、模块说明

### 2.1 Intercept

用于显示和修改 HTTP 请求和响应，通过你的浏览器和 Web 服务器之间。在 BurpProxy 的选项中，您可以配置拦截规则来确定请求是什么和响应被拦截（例如，范围内的项目，与特定文件扩展名，项目要求与参数，等）。该面板还包含以下控制：



## 消息类型显示的四种格式



### 1) Forward

当你编辑信息之后，发送信息到服务器或浏览器

### 2) Drop

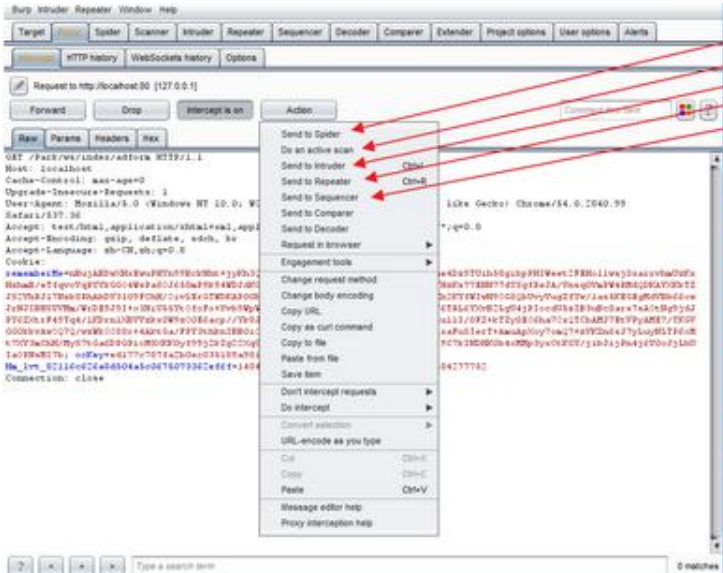
当你不想要发送这次信息可以点击 drop 放弃这个拦截信息

### 3) Interception is on/off

这个按钮用来切换和关闭所有拦截。如果按钮显示 Interception is On, 表示请求和响应将被拦截或自动转发根据配置的拦截规则配置代理选项。如果按钮显示 Interception is off 则显示拦截之后的所有信息将自动转发。

### 4) Action

说明一个菜单可用的动作行为操作可以有哪些操作功能。

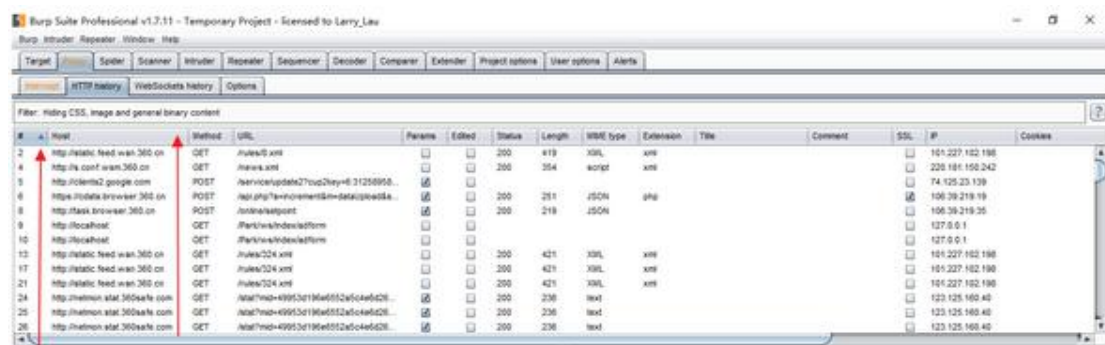


The screenshot shows the Burp Suite interface with the 'Action' menu open. Red arrows point from various menu items to their corresponding Chinese descriptions on the right:

- Send to Spider 发送给蜘蛛
- Do an active scan 执行主动扫描
- Send to Intruder 发送到入侵者
- Send to Repeater 发送到中继器
- Send to Sequencer 发送到序列发生器
- Send to Comparer 发送到比较器
- Send to Decoder 发送到解码器
- Request in browser 在浏览器的请求
- Engagement tools 参与工具
- Change request method 变更请求的方法
- Change body encoding 改变body的编码
- Copy URL 复制网址
- Cope as curl command 作为curl命令
- Cope to file 处理文件
- Pase form file Pase表单文件
- Save item 保存项目
- Don't intercept requests 不拦截请求
- Do intercept 做拦截
- Convert seiection 转换选择
- URL-encode as you type 你需要URL编码的
- Cut 剪切
- Copy 复制
- Paste 粘贴
- Message edit help 消息编辑帮助
- Proxy interception help 代理拦截帮助

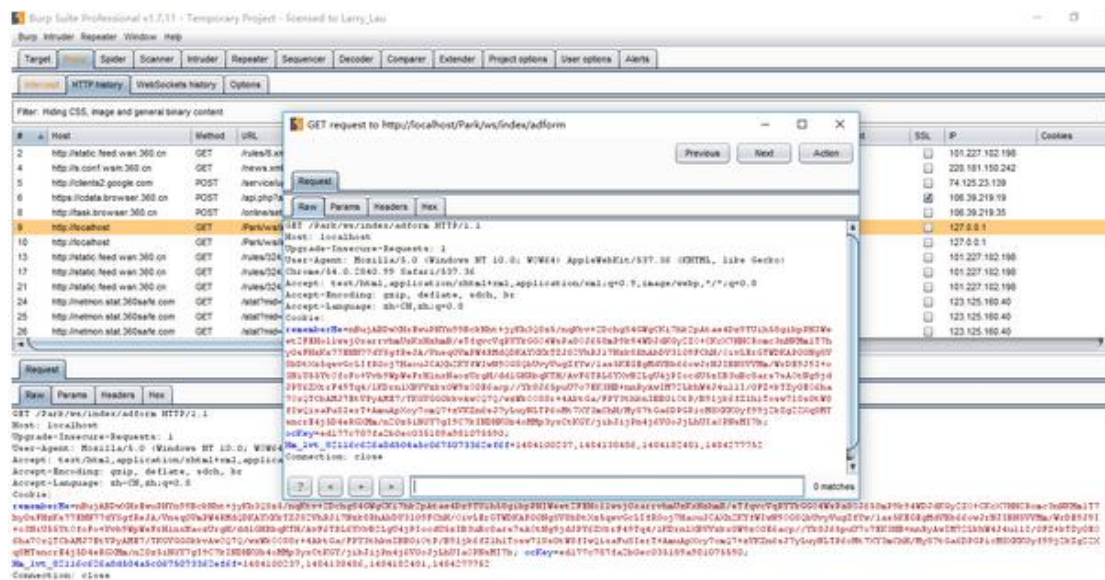
## 2.2 HTTP History

这个选项是用来显示所有请求产生的细节, 显示的有目标服务器和端口, HTTP 方法, URL, 以及请求中是否包含参数或被人工修改, HTTP 的响应状态码, 响应字节大小, 响应的 MIME 类型, 请求资源的文件类型, HTML 页面的标题, 是否使用 SSL, 远程 IP 地址, 服务器设置的 cookies, 请求的时间。



(请求索引号)、Host(主机)、Method(请求方式)、URL(请求地址)、Params(参数)、Edited(编辑)、Status(状态)、Length(响应字节长度)、MIME type(响应的MLME类型)、Extension(地址文件扩展名)、Title(页面标题)、Comment(注释)、SSL、IP(目标IP地址)、Cookies

双击某个请求即可打开详情,通过 Previous/next 可以快速切换请求, 并且 Action 也可以将请求发送至其他模块。

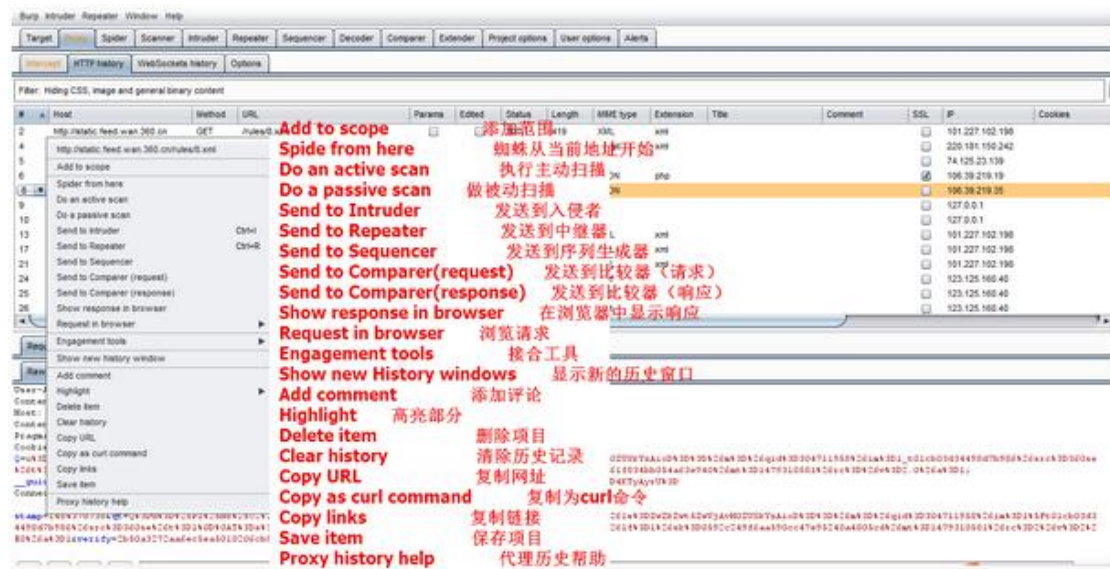


可以通过最左边的列里的下拉菜单来加亮单个选项



#	Host	Method	URL	Params
2	http://static.feed.wan.360.cn	GET	/rules/8.xml	<input type="checkbox"/>
4	http://s.conf.wsm.360.cn	GET	/news.xml	<input type="checkbox"/>
5	http://clients2.google.com	POST	/service/update2?cup2key=6:31258958...	<input checked="" type="checkbox"/>
6	https://cdata.browser.360.cn	POST	/api.php?a=increment&m=dataUpload&s...	<input checked="" type="checkbox"/>
8	http://task.browser.360.cn	POST	/online/setpoint	<input checked="" type="checkbox"/>
8	http://localhost	GET	/Park/ws/index/adform	<input type="checkbox"/>
8	http://localhost	GET	/Park/ws/index/adform	<input type="checkbox"/>
8	http://static.feed.wan.360.cn	GET	/rules/324.xml	<input type="checkbox"/>
8	http://static.feed.wan.360.cn	GET	/rules/324.xml	<input type="checkbox"/>
8	http://static.feed.wan.360.cn	GET	/rules/324.xml	<input type="checkbox"/>
8	http://netmon.stat.360safe.com	GET	/stat?mid=49953d196e6552a5c4e6d26...	<input checked="" type="checkbox"/>
8	http://netmon.stat.360safe.com	GET	/stat?mid=49953d196e6552a5c4e6d26...	<input checked="" type="checkbox"/>
8	http://netmon.stat.360safe.com	GET	/stat?mid=49953d196e6552a5c4e6d26...	<input checked="" type="checkbox"/>
8				
8				
8				
8				

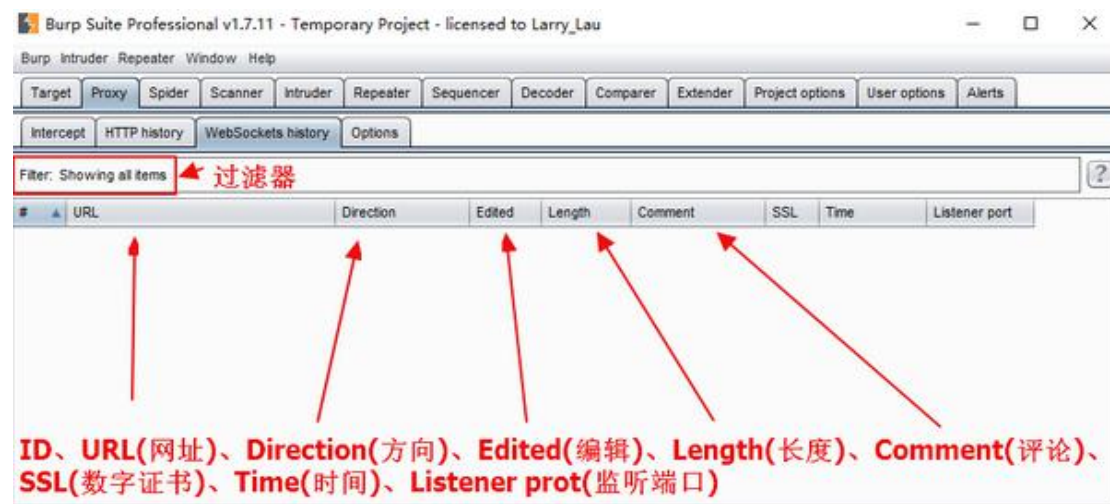
在历史记录表里，右击一个或多个选项，就会显示一个上下文菜单让你执行一些操作，包括修改目标范围，把这些选项发送到其他 Burp 工具，或者删除这些项：



还可以通过配置过滤器来确定哪些顶层的数据项显示在表格里。有效应用程序包含了大量的内容，如图像，CSS 等，这些有利于从视图上隐藏的。AJAX 应用程序产生大量相似的异步请求，你可能会想把他们从视图上过滤出来来查看一

些感兴趣的项。在这个历史记录表的顶部有一个过滤栏。单击会有一个弹出窗口，让你来精准地配置显示哪些内容在表格里：

## 2.3 WebSockets history



该选项主要用于设置代理监听、请求和响应，拦截反应，匹配和替换，ssl等,其中有八大选项:Proxy Listeners、Intercept Client Requests、Intercept Server Responses、Intercept WebSockets Messages、Response Modification、Match and replace、SSL Pass Through、Miscellaneous

1. 运行代理监听器

2. 设置接口为 127.0.0.1:8080

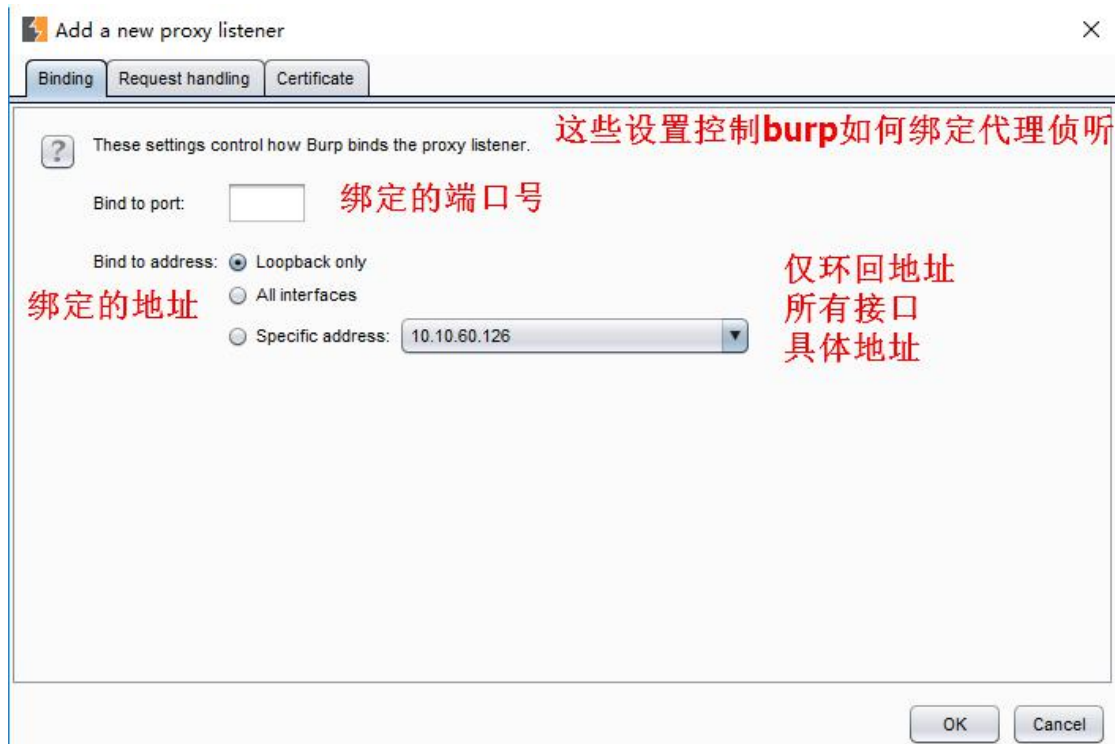
3. 启用代理监听器

4. 设置重定向为全部

5. 设置证书为每个主机

add: 添加一个新的代理地址。

1) binding: 新建一个代理, bind to port-绑定端口号 , bind to address -绑定 ip 地址

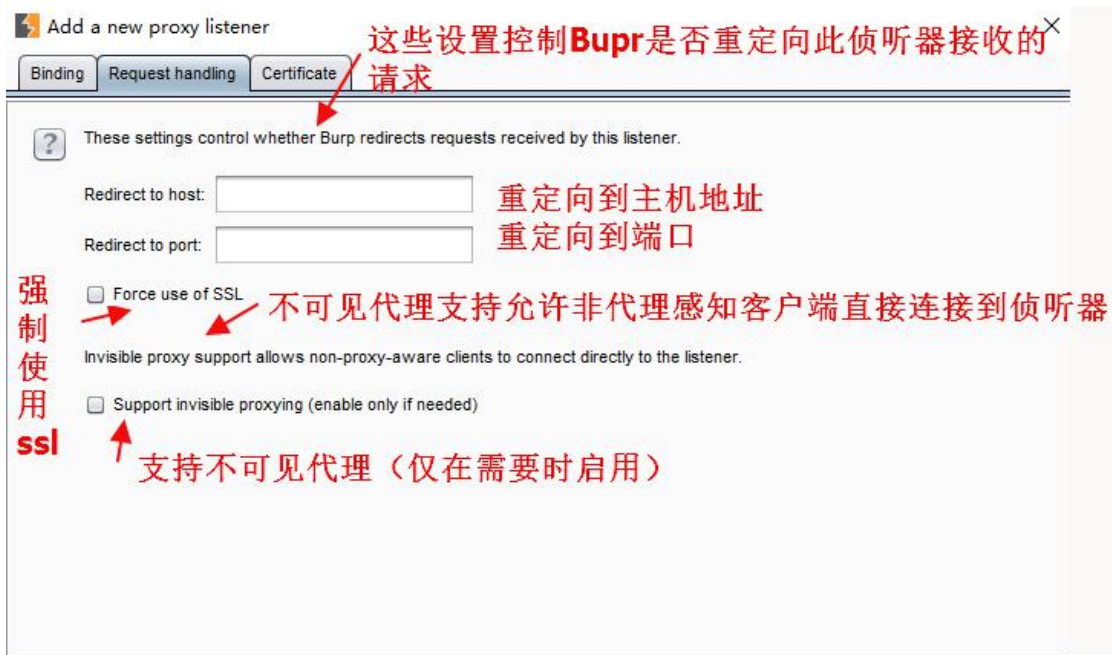


2)request hadning:这些设置包括选项来控制是否 BurpSuite 重定向通过此侦听器接收到的请求:

Redirect to host - 如果配置了这个选项, Burp 会在每次请求转发到指定的主机, 而不必受限于浏览器所请求的目标。需要注意的是, 如果你正使用该选项, 则可能需要配置匹配/替换规则重写的主机中的请求, 如果服务器中, 您重定向请求预期, 不同于由浏览器发送一个主机头。2.2.Redirect to port - 如果配置了这个选项, Burp 会在每次请求转发到指定的端口, 而不必受限于浏览

Force use of SSL - 如果配置了这个选项, Burp 会使用 HTTPS 在所有向外的连接, 即使传入的请求中使用普通的 HTTP。您可以使用此选项, 在与 SSL 相关的响应修改选项结合, 开展 sslstrip 般的攻击使用 Burp, 其中, 强制执行 HTTPS 的应用程序可以降级为普通的 HTTP 的受害用户的流量在不知不觉中通过 BurpProxy 代理。





3)Certificate:这些设置控制呈现给客户端的 SSL 服务器的 SSL 证书。

Generate CA-signed per-host certificate-这是默认选项。安装后，BurpSuite 创造了一个独特的自签名的证书颁发机构（CA）证书，并将此计算机上使用，每次 BurpSuite 运行。当你的浏览器发出 SSL 连接到指定的主机，Burp 产生该主机，通过 CA 证书签名的 SSL 证书。您可以安装 BurpSuite 的 CA 证书作为在浏览器中受信任的根，从而使每个主机的证书被接受，没有任何警报。您还可以导出其他工具或 Burp 的其他实例使用 CA 证书。

Generate a CA-signed certificate with a specific hostname---||这类似于前面的选项;然而，Burp 会产生一个单一的主机证书与每一个 SSL 连接使用，使用您指定的主机名。在进行无形的代理时，此选项有时是必要的，因为客户端没有发送连接请求，因此 Burp 不能确定 SSL 协议所需的主机名。你也可以安装 BurpSuite 的 CA 证书作为受信任的根。

Use a custom certificate---||-此选项使您可以加载一个特定的证书(在 PKCS # 12 格式) 呈现给你的浏览器。如果应用程序使用它需要特定的服务器证书 (例如一个给定序列号或证书链) 的客户端应该使用这个选项。



edit: 编辑选中的代理地址。

remove: 删除选中代理地址。

## 选项 2: Intercept Client Requests

配置拦截规则, 设置拦截的匹配规则。 当 Intercept request based on the following rules 为选中状态时, burpsuite 会配置列表中的规则进行拦截或转发。

注意: 如果该复选框未选中, 那么即使 Intercept is on 也无法截取数据包。

规则可以通过 Enabled 列中的复选框选择开启或关闭。

规则可以是域名, IP 地址, 协议, HTTP 方法, URL, 文件扩展名, 参数, cookie ,

头/主体内容，状态代码， MIME 类型， HTML 页面标题等。

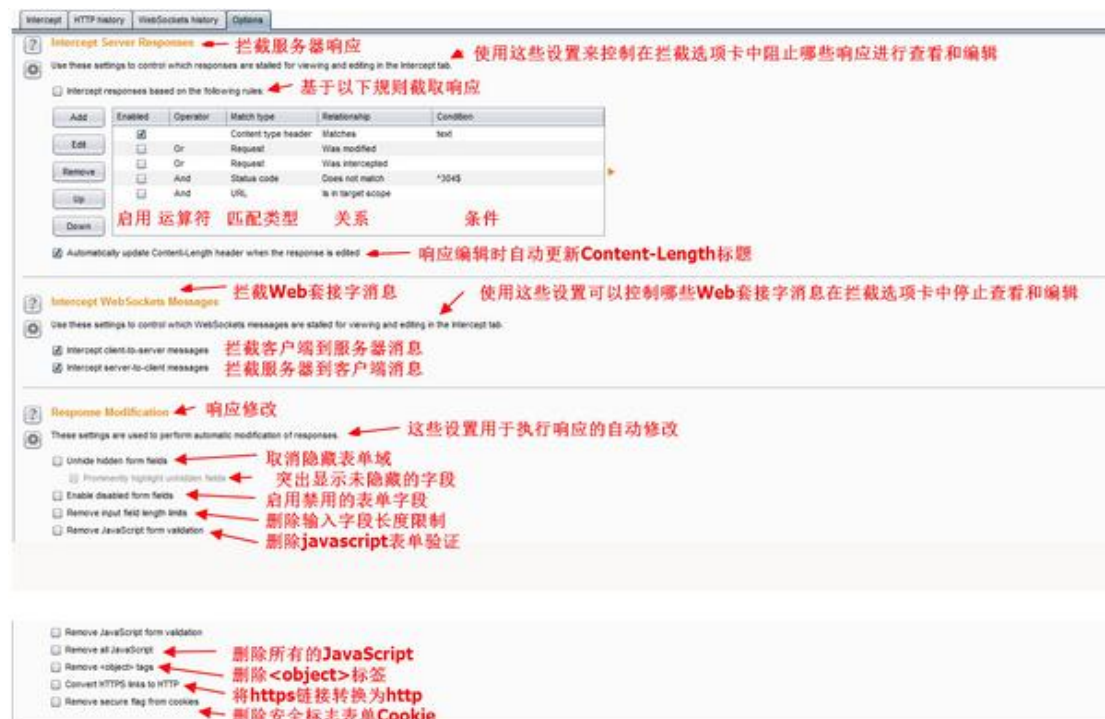
规则按顺序处理，并且使用布尔运算符 AND 和 OR 组合。

### 选项 3: Intercept Server Responses

配置拦截规则，设置拦截的匹配规则，不过这个选项是基于服务端拦截，当选小的 Intercept request based on the following rules 为选中状态时，burpsuite 会匹配响应包。

### 选项 4: Intercept WebSockets Messages

### 选项 5: Response Modification



### 选项 6: Match and replace

用于自动替换请求和响应通过代理的部分。对于每一个 HTTP 消息，已启用的匹配和替换规则依次执行，选择适用的规则进行匹配执行。

规则可以分别被定义为请求和响应，对于消息头和身体，并且还特别为只请求的第一行。每个规则可以指定一个文字字符串或正则表达式来匹配，和一个字符串来替换它。对于邮件头，如果匹配条件，整个头和替换字符串匹配留空，然后头被删除。如果指定一个空的匹配表达式，然后替换字符串将被添加为一个新的头。有可协助常见任务的各种缺省规则 - 这些都是默认为禁用。匹配多行区域。您可以使用标准的正则表达式语法来匹配邮件正文的多行区域。

## 选项 7: SSL Pass Through

**匹配和替换**

这些设置用于自动替换通过代理的部分请求和响应

Enabled	Item	Match	Replace	Type	Comment
<input type="checkbox"/>	Request header	*None-Match*\$		Regex	Require non-cached responses
<input type="checkbox"/>	Request header	*Referer*\$		Regex	Hide Referer header
<input type="checkbox"/>	Request header	*Accept-Encoding*\$		Regex	Require non-compressed responses
<input type="checkbox"/>	Response header	*Set-Cookie*\$		Regex	Ignore cookies
<input type="checkbox"/>	Request header	*Host: foo.example.org\$	Host: bar.example.org	Regex	Rewrite Host header
<input type="checkbox"/>	Request header	Origin: foo.example.org		Regex	Add spoofed CORS origin
<input type="checkbox"/>	Response header	*Strict-Transport-Security*\$		Regex	Remove HSTS headers

开启 选项 匹配 替换 类型 注释

**SSL 通过**

这些设置用于指定目标 Web 服务器，Burp 将直接通过 SSL 连接没有关于请求的详细信息或通过这些协议做出的响应将可用在代理拦截视图或历史

Enabled	Host / IP range	Port
<input type="checkbox"/>		

启用 主机 / IP 范围 端口

☐ Automatically add entries on client SSL negotiation failure 在客户端 SSL 协商失败时自动添加条目

## 选项 8: Miscellaneous

**其他**

这些设置控制 burp 代理的行为的一些具体细节，你可以在这里更改默认设置来处理特殊问题或情况

- ☐ Use HTTP/1.0 in requests to server 在对服务器的请求中使用 HTTP / 1.0
- ☐ Use HTTP/1.0 in responses to client 在对客户端的响应中使用 HTTP / 1.0
- ☐ Set response header "Connection: close" 设置响应头"连接: 关闭"
- ☒ Set "Connection: close" on incoming requests 设置"连接关闭"传入请求
- ☒ Strip Proxy-\* headers in incoming requests 启用代理-\* headers 传入请求
- ☒ Unpack gzip / deflate in requests 在请求中解压缩 gzip / deflate
- ☒ Unpack gzip / deflate in responses 在响应中解压缩 gzip / deflate
- ☐ Disable web interface at http://burp 禁用 HTTP Web 接口: http://burp
- ☐ Allow requests to web interface using fully-qualified dns hostnames 允许使用完全限定 dns hostnames 对 Web 界面
- ☐ Suppress Burp error messages in browser 抑制 Burp 在 browser 错误消息
- ☐ Disable logging to history and site map 禁用日志记录到历史记录和站点地图