

【技术分享】BurpSuite 代理设置的小技巧 - 安全客，安全资讯平台



作者： 三思之旅

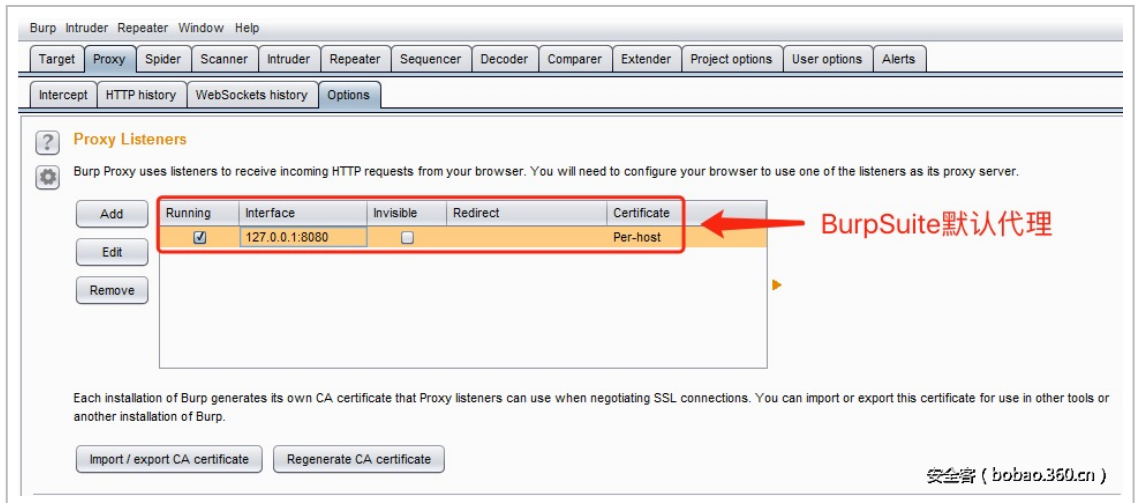
预估稿费：300RMB

投稿方式：发送邮件至 linwei#360.cn，或登陆网页版在线投稿

在 Web 渗透测试过程中，BurpSuite 是不可或缺的神器之一。BurpSuite 的核心是代理 Proxy，通常情况下使用 BurpSuite 的套路是：浏览器设置 BurpSuite 代理——> 访问 Web 应用程序——>BurpSuite 抓包分析。本人从事 Web 渗透测试尚不足一年，这期间在代理设置过程中踩到过一点『小坑』，现在将我踩过的『小坑』总结一下。本文主要面对新人朋友，老司机们请不吝赐教~

0x01 一般情形

最一般的情形是针对采用 HTTP 协议的 Web 应用程序的渗透测试。这种情况下，直接设置浏览器的代理服务器为 BurpSuite 即可，默认为 127.0.0.1:8080。



当然，直接更改浏览器的代理服务器设置比较繁琐，更好的办法是使用浏览器插件，预先设置好代理方案，然后根据实际情况一键切换。Chrome 推荐使用 Proxy SwitchyOmega 插件：



Firefox 推荐使用 FoxyProxy :



至于 IE 浏览器，说实在话用得很少，不建议用于渗透测试。一方面，IE 不支持扩展插件；另一方面，IE 的代理设置也就是系统全局代理，一旦更改了 IE 的代理，除了那些自带代理设置的程序外（如安装了 Proxy SwitchyOmega 扩展的 Chrome 浏览器），其他程序请求数据都要走代理，给我们的测试带来很大不便。但是，如果你非要用 IE 的话（比如针对某些不支持 Chrome 和 Firefox 的网银系统进行渗透测试），也有比较方便的解决办法，容我先卖个关子，后文会有说明。

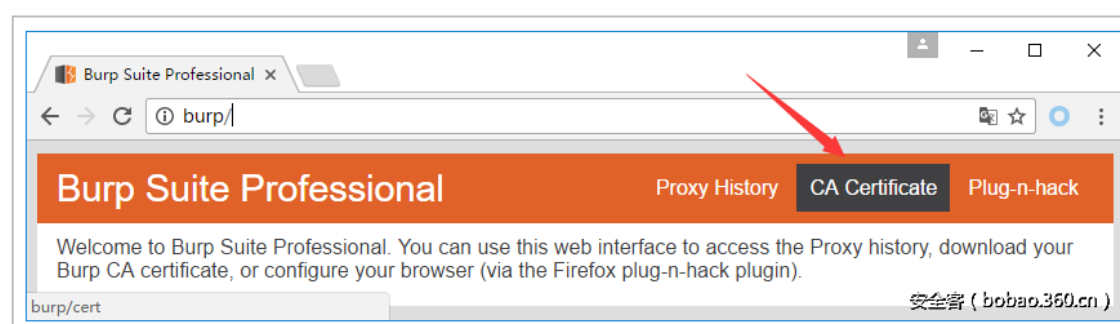
0x02 HTTPS 网站的情形

许多人在第一次使用 BurpSuite 抓取 HTTPS 网站报文时都会遇到『您的连接不是私密连接』（Chrome）、『此网站的安全证书存在问题』（IE）或者『您的连接不安全』（Firefox）的问题，这时候怎么办？

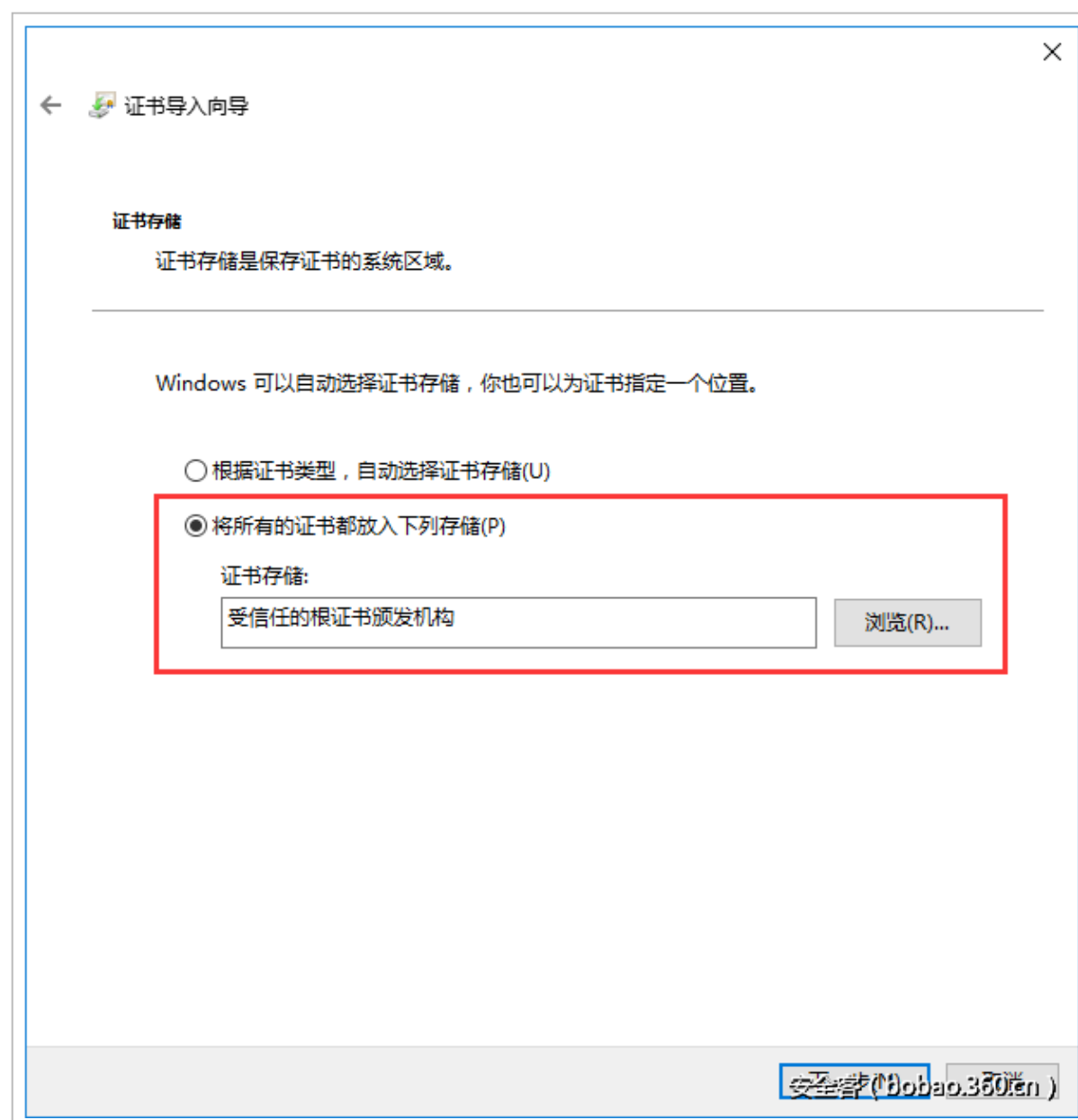


这个问题其实很简单，安装一个证书即可解决，想知道原因的可以自行 Google 一下 HTTPS 原理就能够得到答案。

首先，浏览器设置好 BurpSuite 代理服务器后，访问 <http://burp/>，然后点击右上角的 CA Certificate，这时会自动下载一个名为 cacert.der 的证书文件。

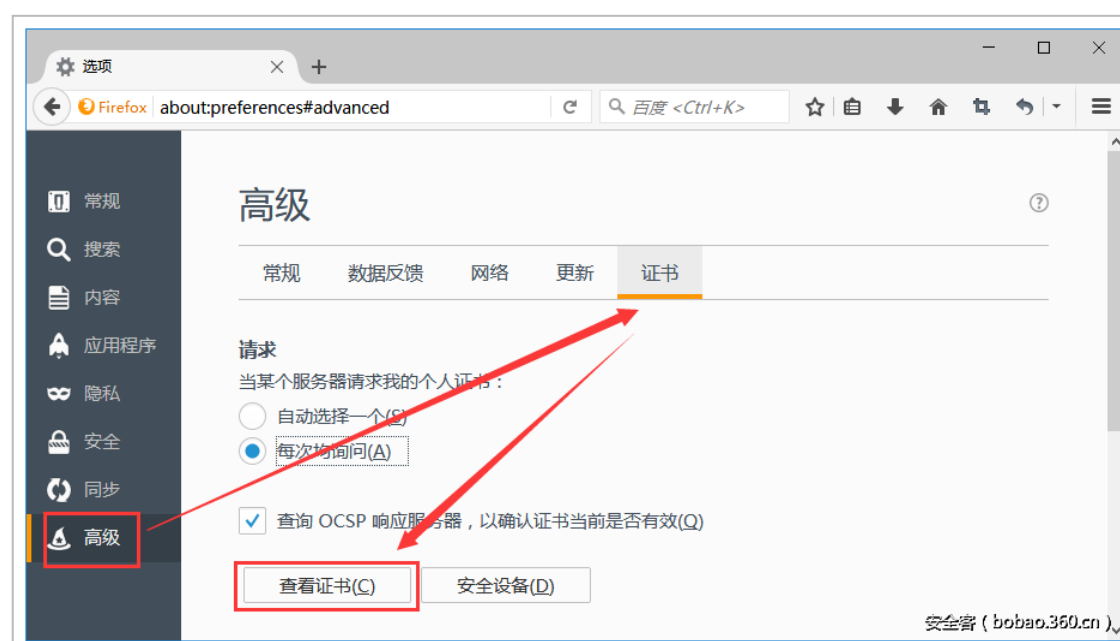


打开这个证书文件，根据提示安装这个证书，基本上是一路『下一步』，唯一需要注意的是，在『证书存储』这一步选择将证书存储在『受信任的根证书颁发机构』。

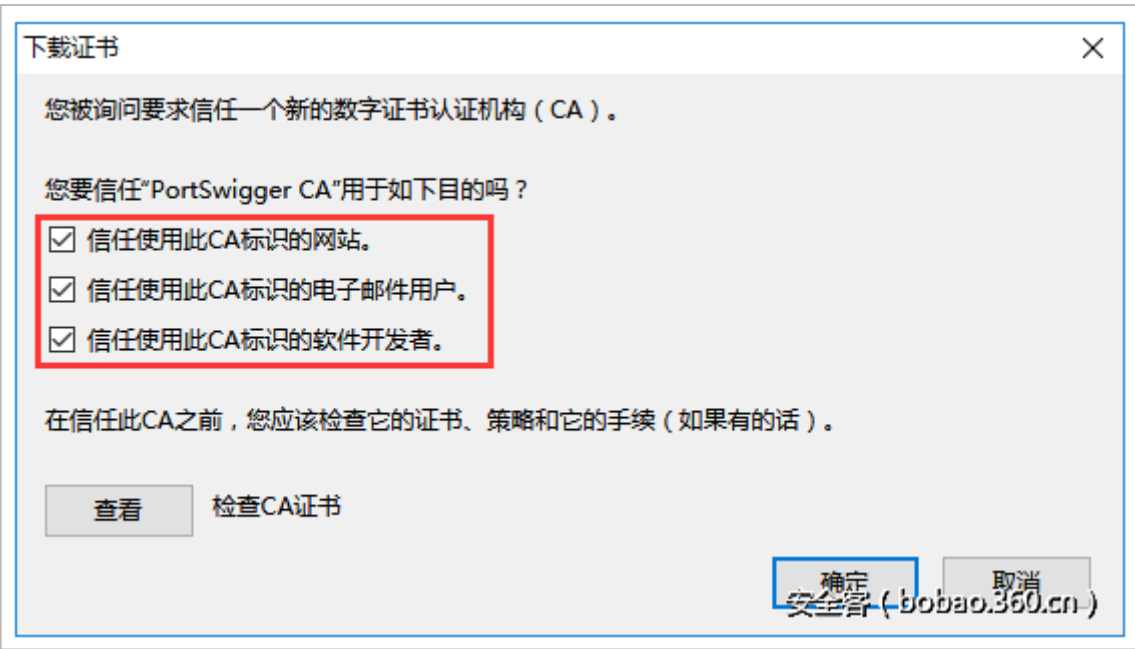


证书安装好之后，Chrome 和 IE 就能够正常访问 HTTPS 网站了（由于 Google 一直在推全网 HTTPS，Chrome 对证书要求很严格，我们安装的证书不是权威机构颁发的，因此地址栏会一直提示『不安全』，但是不影响使用）。

不过，如果你使用 Firefox 浏览器的话，还需要增加一步，即将证书导入到 Firefox 中。打开 Firefox 的『选项——高级——证书』，然后点击『查看证书』按钮打开『证书管理器』。



在『证书管理器』中，点击下方的『导入』按钮，导入之前下载的 cacert.der 证书文件，并且在弹出的『下载证书』对话框中，勾选 3 个『信任使用此 CA 标识的.....』复选框，最后点击『确定』即可。



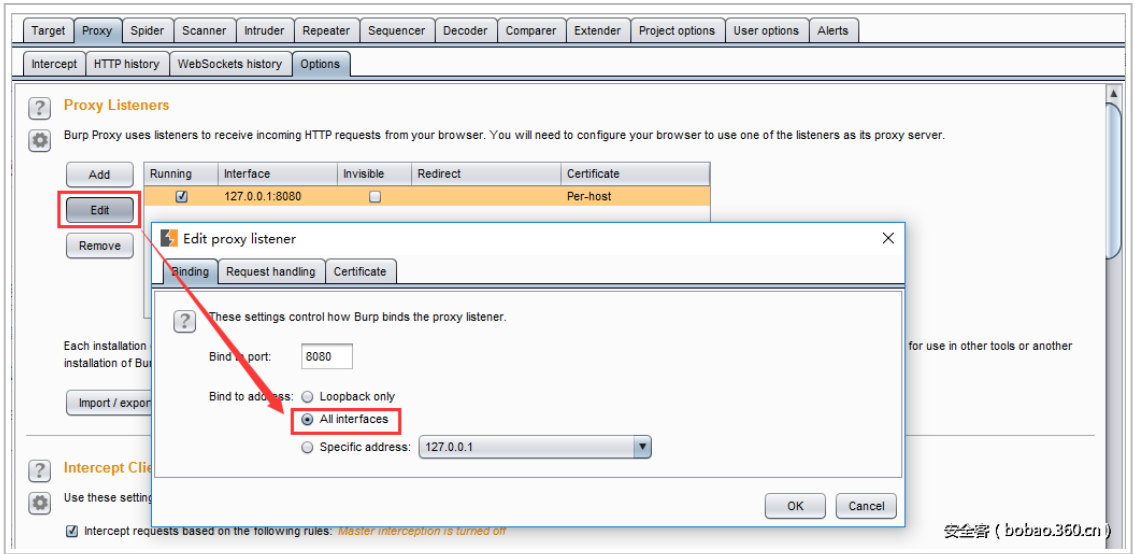
这时候，Firefox 也可以正常使用了。

0x03 移动端流量抓取

有时候，我们还需要对移动 APP 进行抓包分析，这时候该怎么办？

其实很简单，两步即可解决。

第一步，在 BurpSuite 的 Proxy Listeners 中，选中当前在用的代理，点击左侧的 Edit 按钮，在弹出的对话框中，将 Bind to address 选项设置为 All interfaces。



第二步，手机和 PC 连接同一 Wifi，打开手机 Wifi 设置，设置 HTTP 代理服务器为 BurpSuite 所在的 PC 的 IP 地址，端口为 BurpSuite 的代理端口。以 iPhone 为例，其设置如下图所示。



然，如果 APP 走的是 HTTPS 通道，仍然需要安装证书才能正常访问，方法同前，不再赘述。

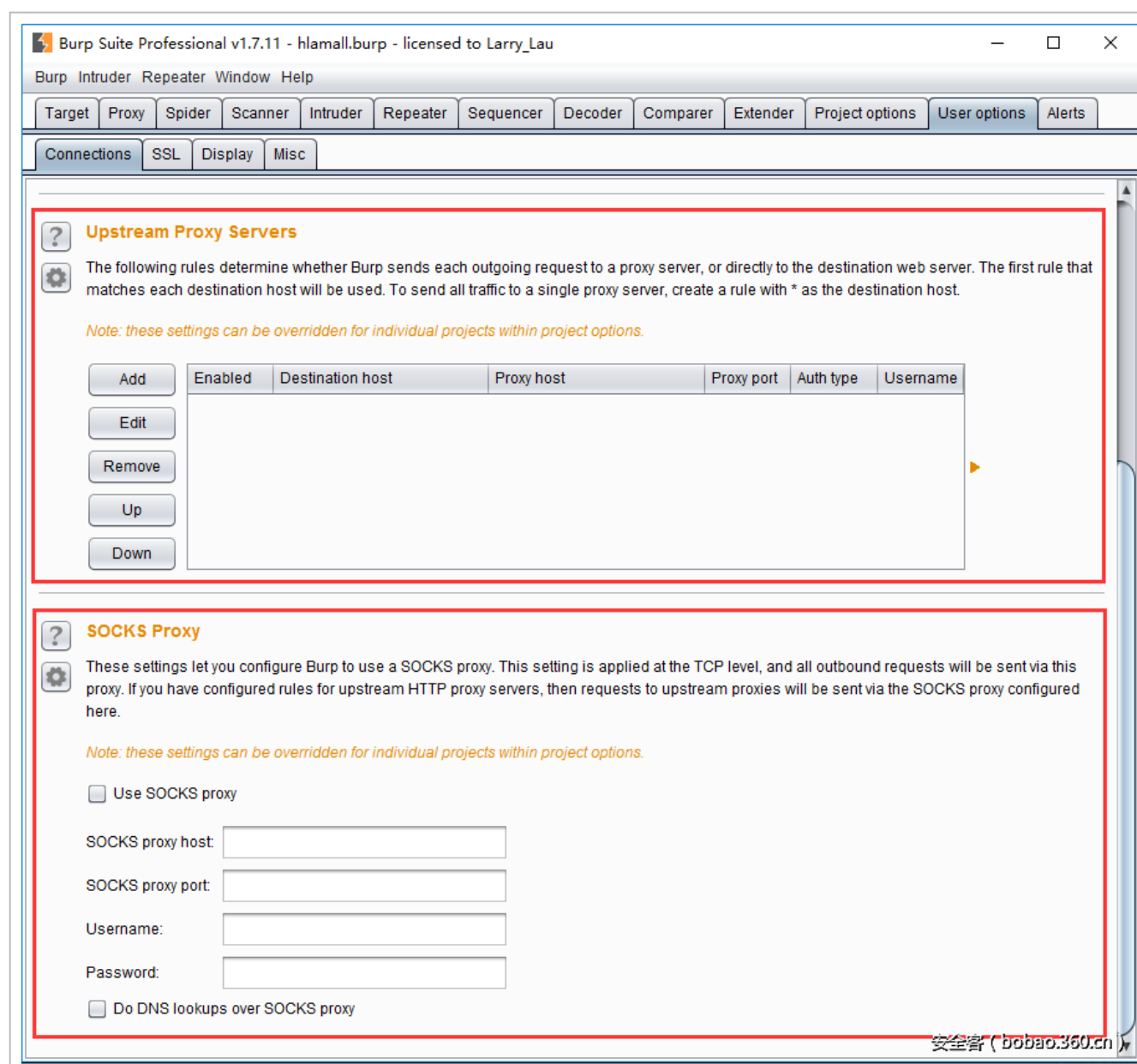
0x04 多重代理的情形

在某些网络环境中，访问目标网站需要走代理。比如说，为了访问 google.com，我已经给浏览器设置了 SS 代理（默认 127.0.0.1:1080），现在我想对 google.com 进行渗透测试，那么该怎么设置浏览器代理？这时候不能简单的把浏览器代理设置为 BurpSuite，这样虽然可以进行抓包，但是没有了 SS 的帮助，我们是无法访问 google.com 的，抓包也就没有意义了。这时候该怎么办？

在这种情况下，我们必须借助代理链了。

顾名思义，代理链就一系列的代理形成的链条。像刚才那种情形，我们首先设置浏览器的代理为 BurpSuite 以便能够抓包；然后为 BurpSuite 再设置一个上游代理即 SS。这样访问 google.com 时，请求数据先经过 BurpSuite，于是可以进行抓包了；然后再流向 SS，最后经过 SS 服务器到达 google.com。服务器端返回的响应则刚好相反。通过这个 BurpSuite——SS 的代理链，我们就解决了本节开头所描述的问题。

作为一个神器，BurpSuite 是具备这个功能的。在 BurpSuite 的 User options 下的 Connections 页面中，有『Upstream Proxy Servers』和『SOCKS Proxy』这两个配置项，都是跟代理链相关的。接下来逐一进行说明。



1. Upstream Proxy Servers

在该设置项中，可以设置多个上游代理服务器规则，满足规则的请求将被发送至相应的代理服务器。只说概念过于无聊，还是以 google.com 为例进行说明。

为了对 google.com 进行抓包分析，我们首先要设置浏览器的代理为 BurpSuite，这一点是毫无疑问的。为了能正常访问 google.com，还需要设置 BurpSuite 的上流代理为 SS（127.0.0.1:1080）。点击 Upstream Proxy Servers 列表框左侧的 Add 按钮，打开『Edit upstream proxy rule』对话框。这里一共有 8 个设置项，一般情况下只需关注前 4 个：

Destination host: 这里填入目标网站域名或者 IP，支持通配符（* 表示 0 个或者任意个字符，? 表示除点号之外的任意一个字符）。在本例中，我们可以填入 *.google.com。

Proxy host: 填入 SS 代理服务器的 IP 地址，即 127.0.0.1。如果为空表示直接连接。

Proxy port: 填入 SS 的代理地址，即和 1080。

Authentication type: 这里选择认证类型，由于 SS 本地代理无需认证，这是选择 None。

如果 Authentication type 为 None，则接下来的 4 项内容无需理会，否则需要根据实际情况设置以下 4 项内容。

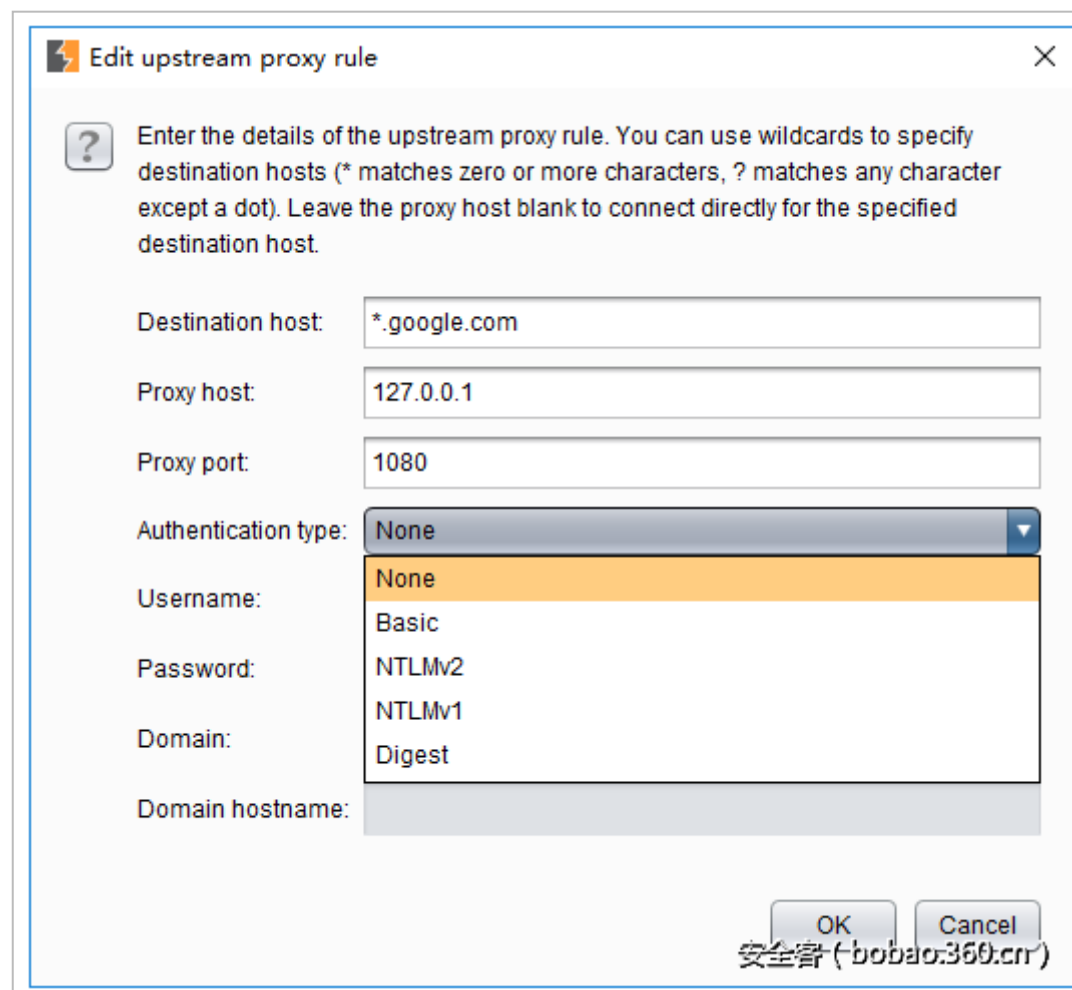
Username: 用户名。

Password: 密码。

Domain: 域。仅用于 NTLM 认证类型。

Domain hostname: 域主机名。仅用于 NTLM 认证类型。

设置内容如下图所示，最后点击 OK 即可。

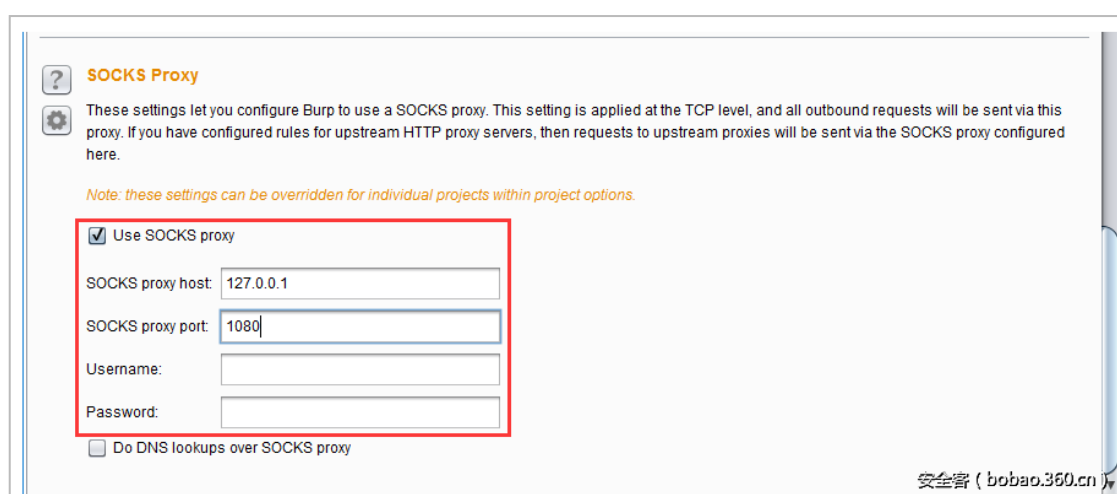


这时候你会发现 google.com 已经能够访问了，并且 BurpSuite 中也成功地抓取到了相应的请求报文。

你可以同时设置多个 Upstream Proxy Servers，在使用过程中，BurpSuite 会按顺序将请求的主机与 Destination host 中设置的内容进行比较，并将请求内容发送至第一个相匹配的 Proxy server。因此，Proxy Server 的顺序很重要，讲究个先来后到！

2. SOCKS Proxy

与 Upstream Proxy Servers 的作用类似，SOCKS Proxy 的功能也是将请求内容发送至相应的代理服务器。不同之处在于，SOCKS Proxy 作用于 TCP 协议层，因此如果设置了该项，那么所有的请求数据都会被发送至 SOCKS 代理服务器。所以，SOCKS Proxy 的设置更简单。同样以 google.com 为例，先在下方的输入框中依次填入 SOCKS 代理服务器的 IP、端口（如果 SOCKS 代理服务器需要认证，还需要填写用户名和密码），然后勾选 Use SOCKS proxy 即可。



需要注意的一点是，如果同时设置了 Upstream Proxy Servers 和 SOCKS Proxy，则根据规则应该发送至上游代理的请求将会通过 SOCKS Proxy 发送。

0x05 被测客户端不支持代理设置的情形

有时候，我们想对电脑上的某客户端进行抓包分析，然而这个客户端并没有代理设置的功能，怎么办？如果直接设置系统代理当然也是可以的，但是这样一来所有程序的流量都要经过 BurpSuite，一方面有可能影响非测试软件的使用；另一方面，BurpSuite 中非测试软件请求记录过多也影响我们的分析测试。有没有更好的解决方案？

答案是肯定的，这时候就需要 Proxifier 登场了。Proxifier 是什么？且看官网的说明：

Proxifier allows network applications that **do not** support working **through** proxy servers to operate **through** a SOCKS or HTTPS proxy **and** chains.

简单的说，使用 Proxifier 能够为那些本身不能设置代理的软件设置 SOCKS 或者 HTTPS 代理（链）。Proxifier 的体积虽小，但功能却十分强大，除了有 Windows 版之外，还有 Mac 版的。因此，非常值得关注。

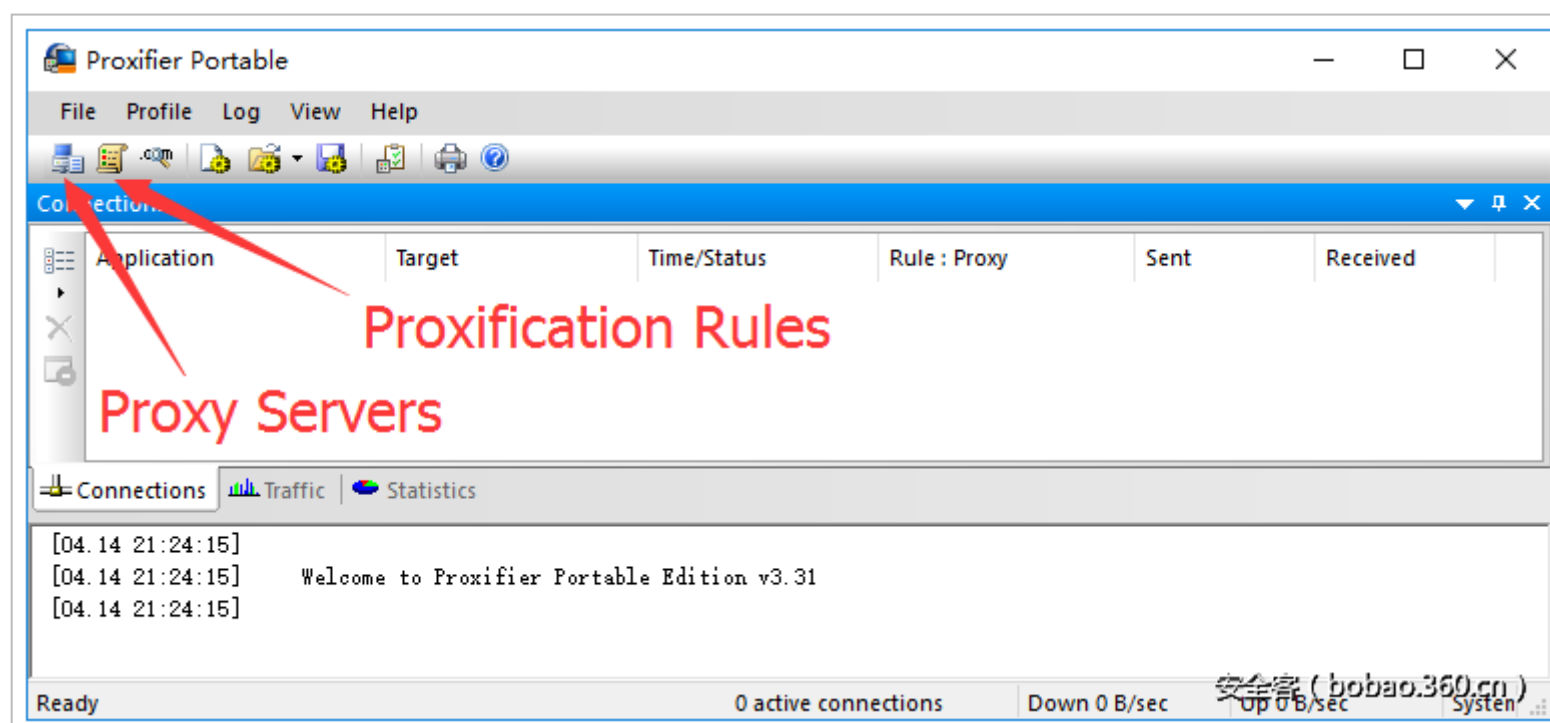
还是通过实例进行说明。有一次，需要对某微信公众号进行渗透测试，有些微信公众号的链接复制到浏览器中可以直接打开，但是这个公众号做了限制，只能在微信中打开，即使改了 UA 也不行。



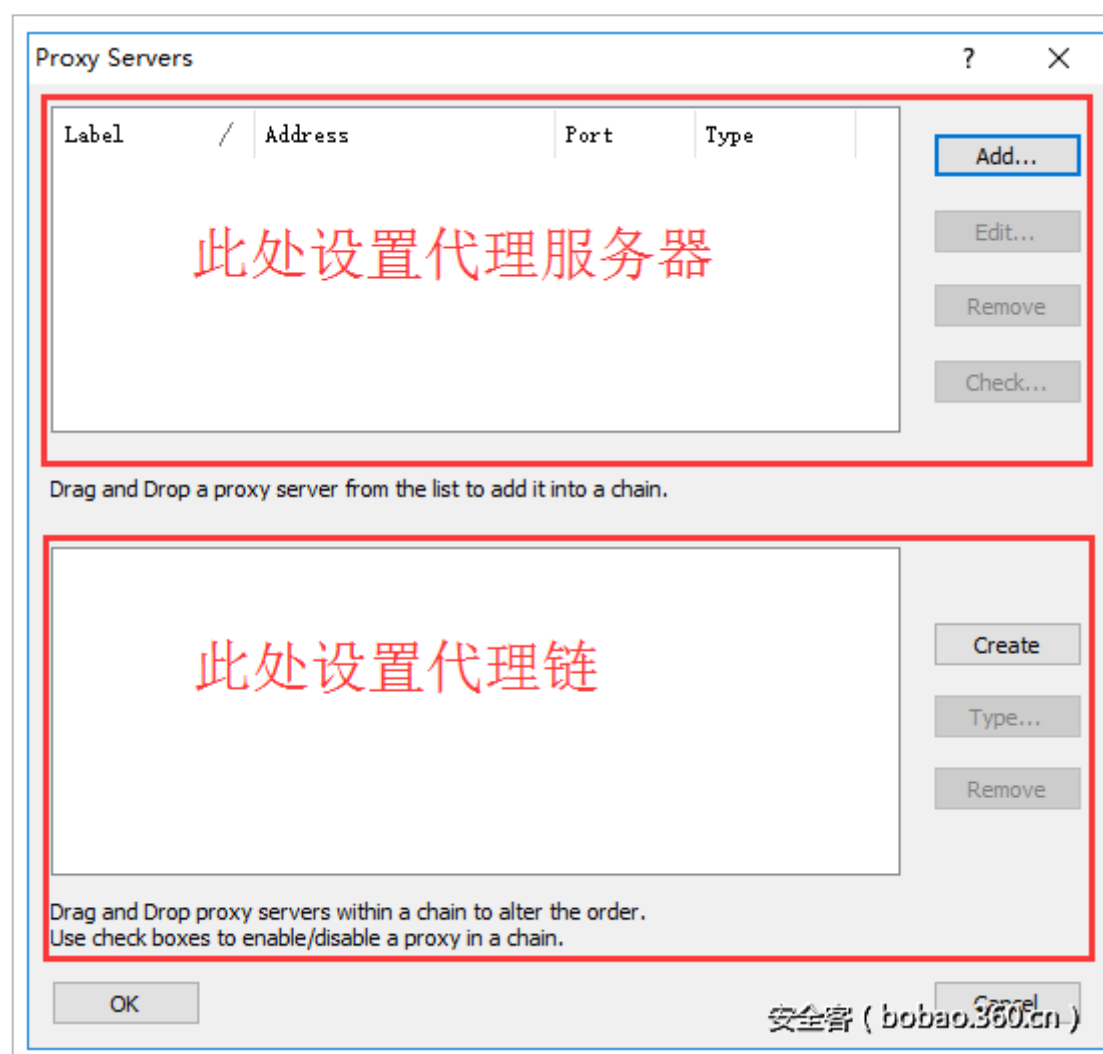
微信网页版中只能看到公众号发的文章，而不能进行交互。设置手机代理倒是可以进行测试，但是一边在手机上操作、一边在 PC 上抓包很不方便，而且容易给领导一种一直在玩手机的错觉..... 微信 PC 版功能倒是挺全，然而却不能设置代理！

怎么办？貌似山穷水尽了。最后寄希望于 Google，经过一番搜索，直到 Proxifier 的出现，总算柳暗花明！言归正传，接下来看看 Proxifier 怎么玩。

Proxifier 的界面很简洁，我们重点关注其中的两个功能，即 Proxy Servers 和 Profication Rules。工具栏中最左侧的两个图标分别对应这两个功能。

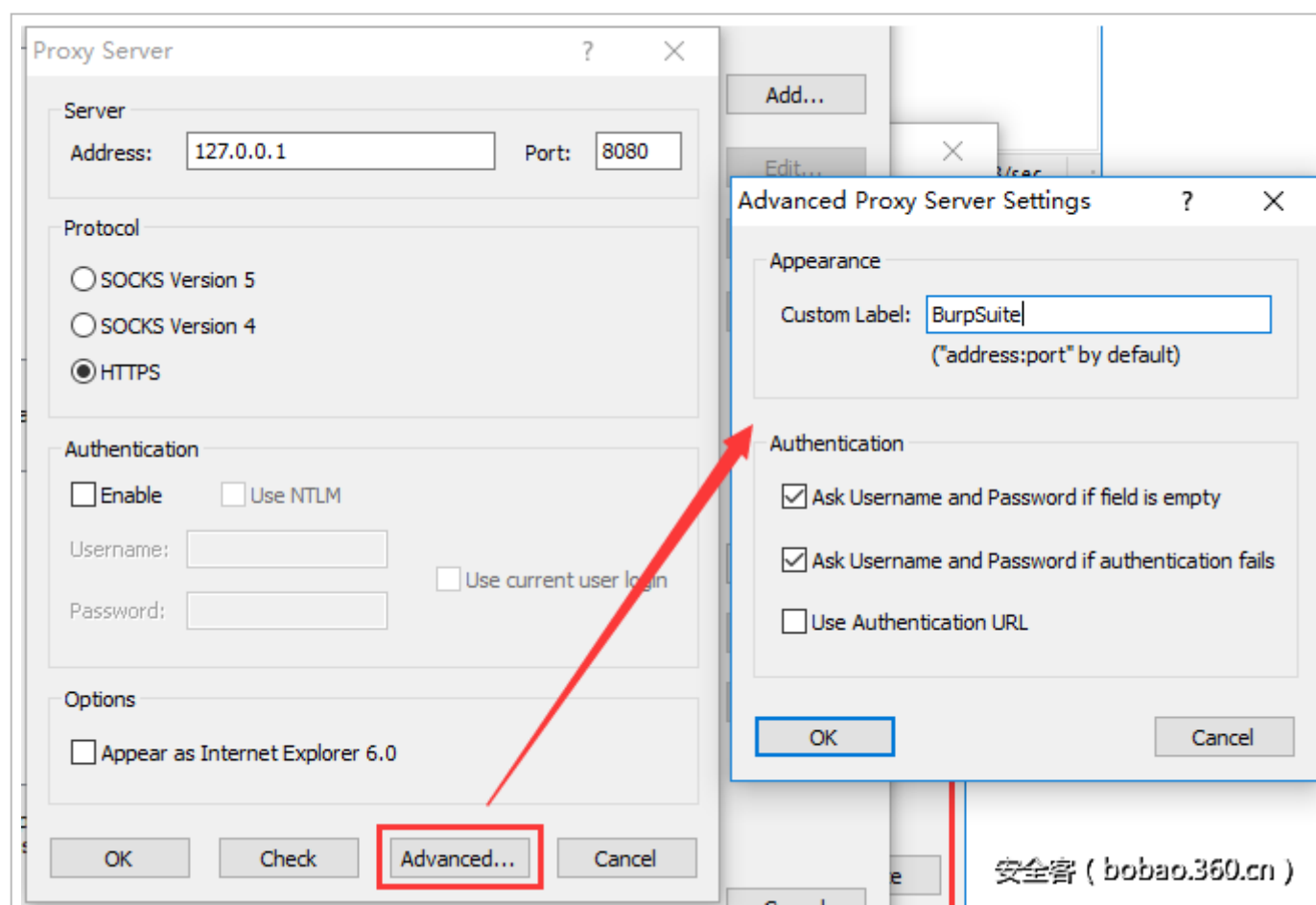


首先点击工具栏第一个图标，打开 Proxy Servers 对话框。Proxy Servers 对话框分为上下两部分，上半部分用于设置代理服务器，下半部分用于设置代理链。

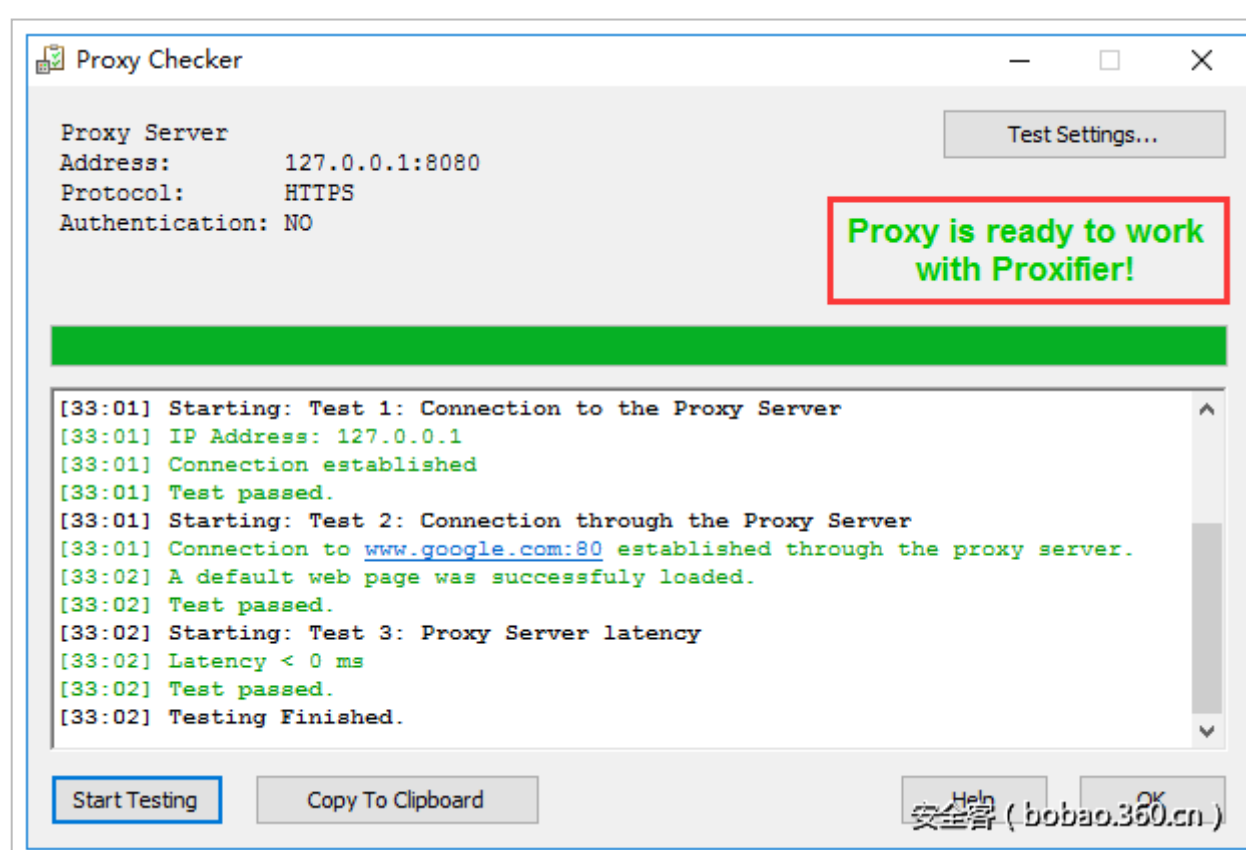


1. 代理服务器设置

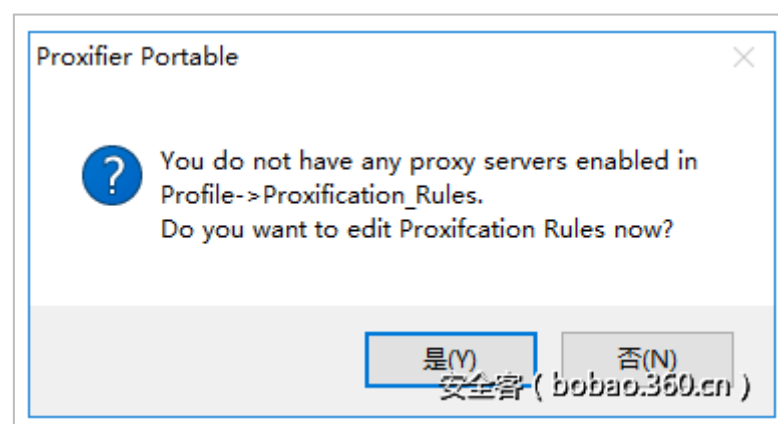
我们先讲讲代理服务器设置。点击 Add 按钮，增加一个代理服务器，填入相应的代理服务器地址和端口，这里填入 BurpSuite 的代理 127.0.0.1:8080；Protocol 中选择 HTTPS；点击 Advanced 按钮，设置一个 Custom Label 以方便区分。



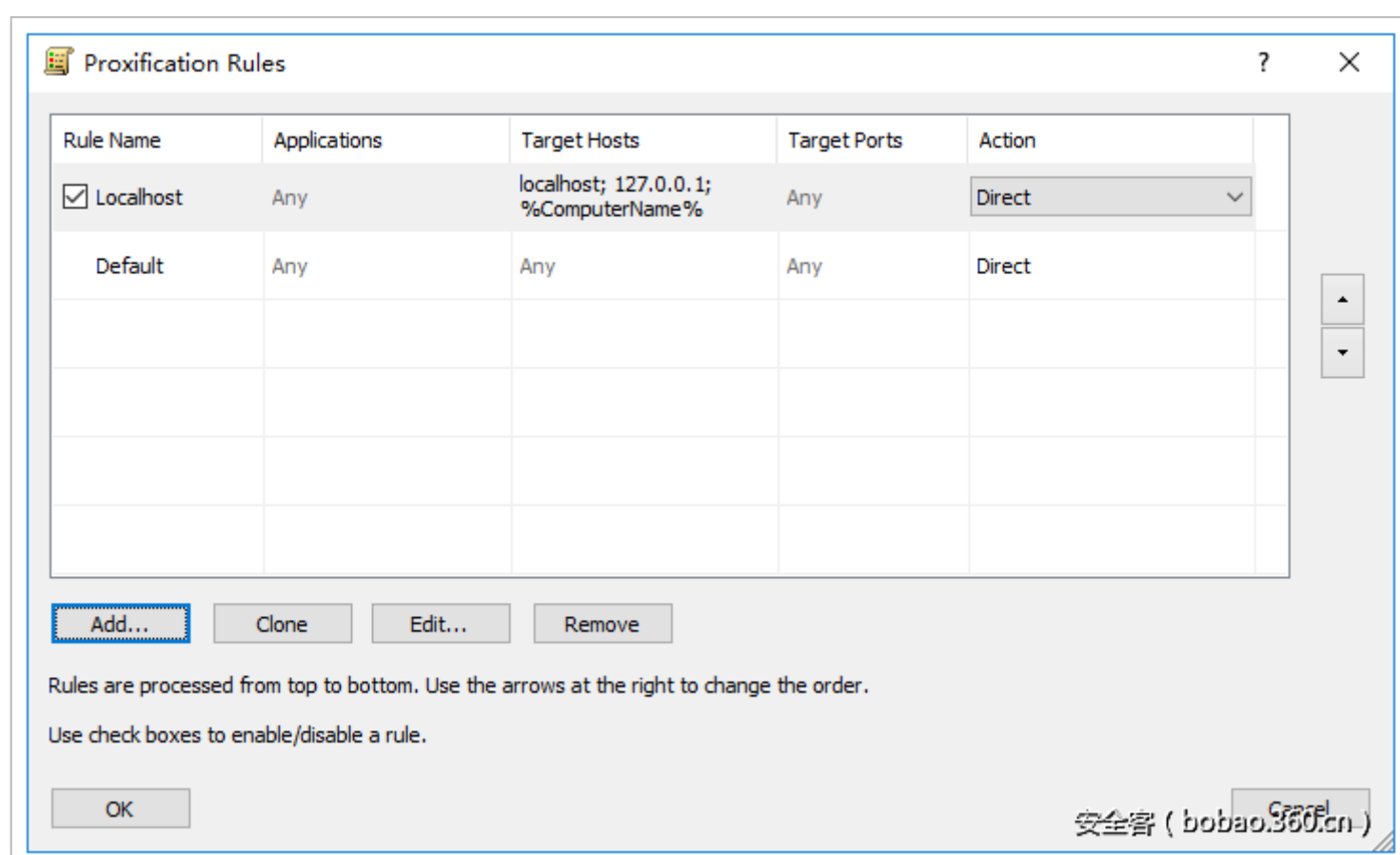
设置完成之后，可以点击下方的 Check 按钮测试一下代理是否设置成功。如果出现下图所示的 Proxy is ready to work with Proxifier! 说明代理设置成功。不过默认的用于测试的目标网站是 www.google.com，很有可能出现误判，建议点击右上角的 Test Settings 按钮将 Target host 更改为不挂代理也可正常访问的网站。



Proxy Server 设置完成之后会提示你尚未设置当前启用的代理服务器，是否要进入规则设置，点击『是』即可进行代理规则设置。也可以点击工具栏第二个图标进入『Proxification Rules』对话框。



默认有两条直连的规则。点击左下方的 Add 按钮，进入具体的规则设置页面。



设置内容并不复杂，一共五个设置项：

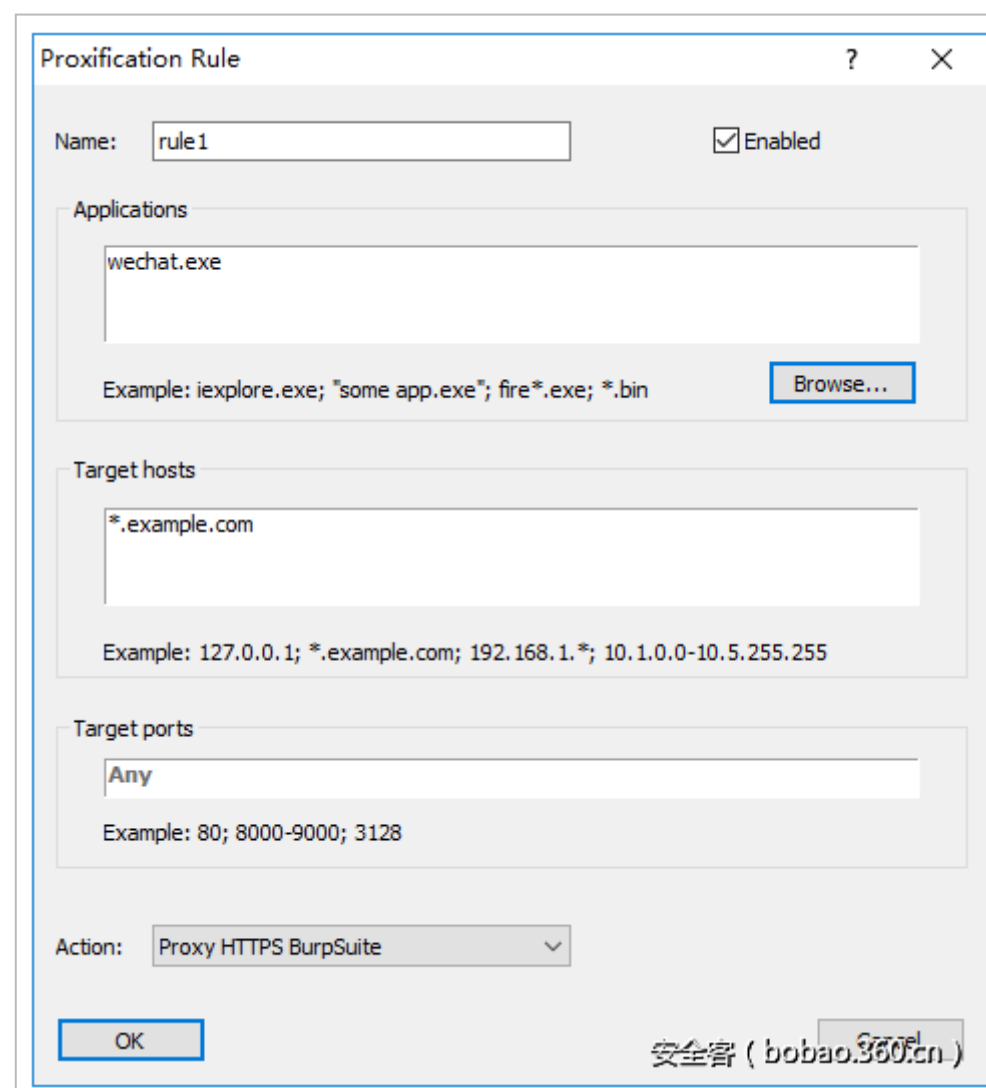
Name：可任意设置，建议设置有意义的名称以方便使用。

Applications：设置代理的应用，此处设置的是微信的主程序 wechat.exe。

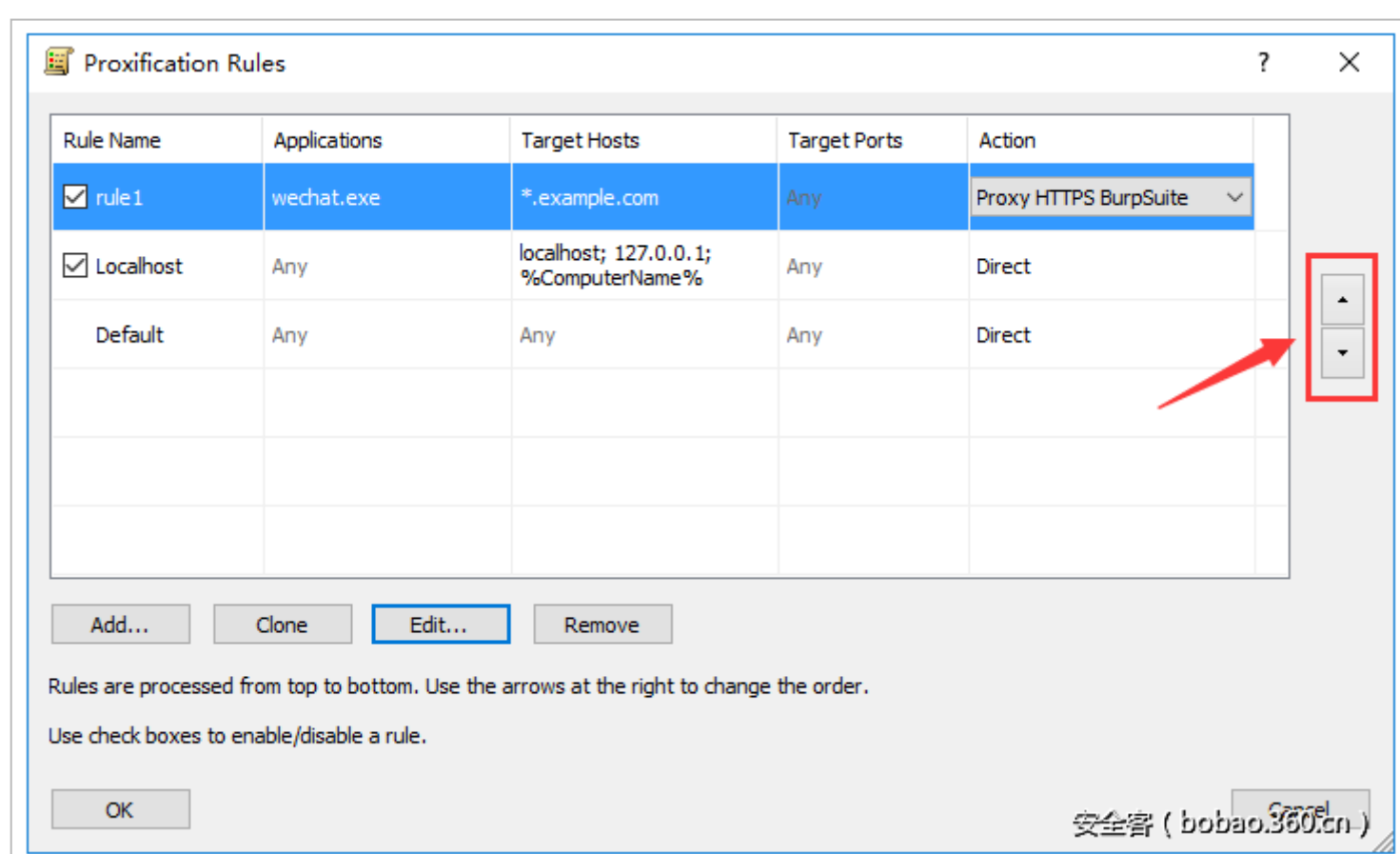
Target hosts：设置访问哪些网站走代理，根据实际情况填写。

Target ports：设置访问目标网站的哪些端口才走代理，根据实际情况填写即可。

Action：这里选择上一步设置的代理服务器即可。除了自定义的代理服务器外，这里还有 Direct 和 Block 的选项，分别是直连和阻止连接，说明 Proxifier 还可以有选择的屏蔽某些站点，在某些情况下还是很有用的。

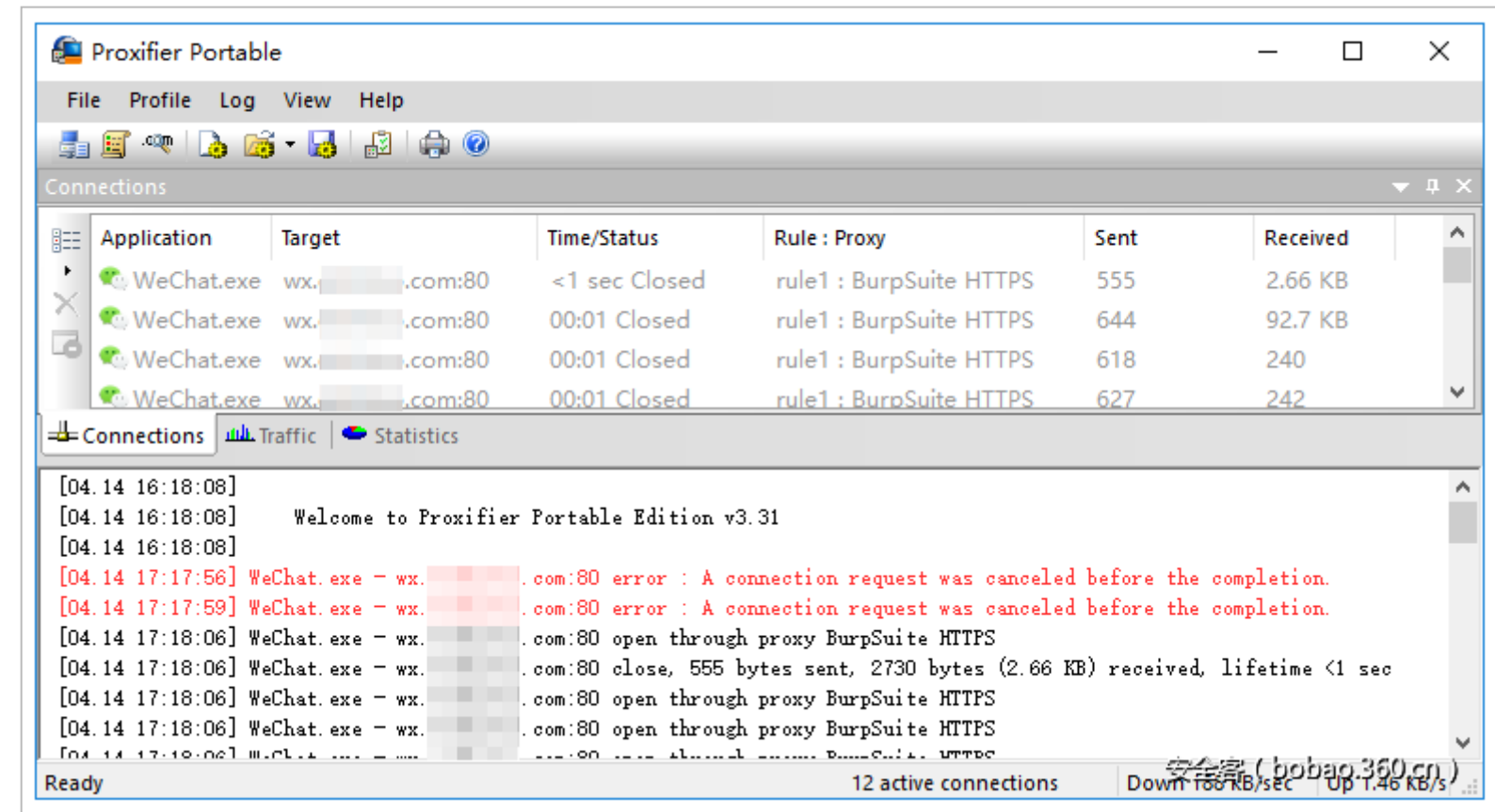


规则设置好之后，可点击规则列表框右侧的方向按钮，更改规则的顺序。和 BurpSuite 的 Upstream Proxy Servers 一样，这里也讲究个先来后到，所以当前在用的规则越靠前越好。如果你设置好代理及规则之后不起作用，可以到这里看看顺序是不是没有调整好。



一切设置就绪，别忘了点击 OK 按钮保存。这时候，在 PC 版的微信中对目标公众号进行相应的操作与访问，BurpSuite 就能够抓取到 HTTP 报文了。同时，在 Proxifier 中能够

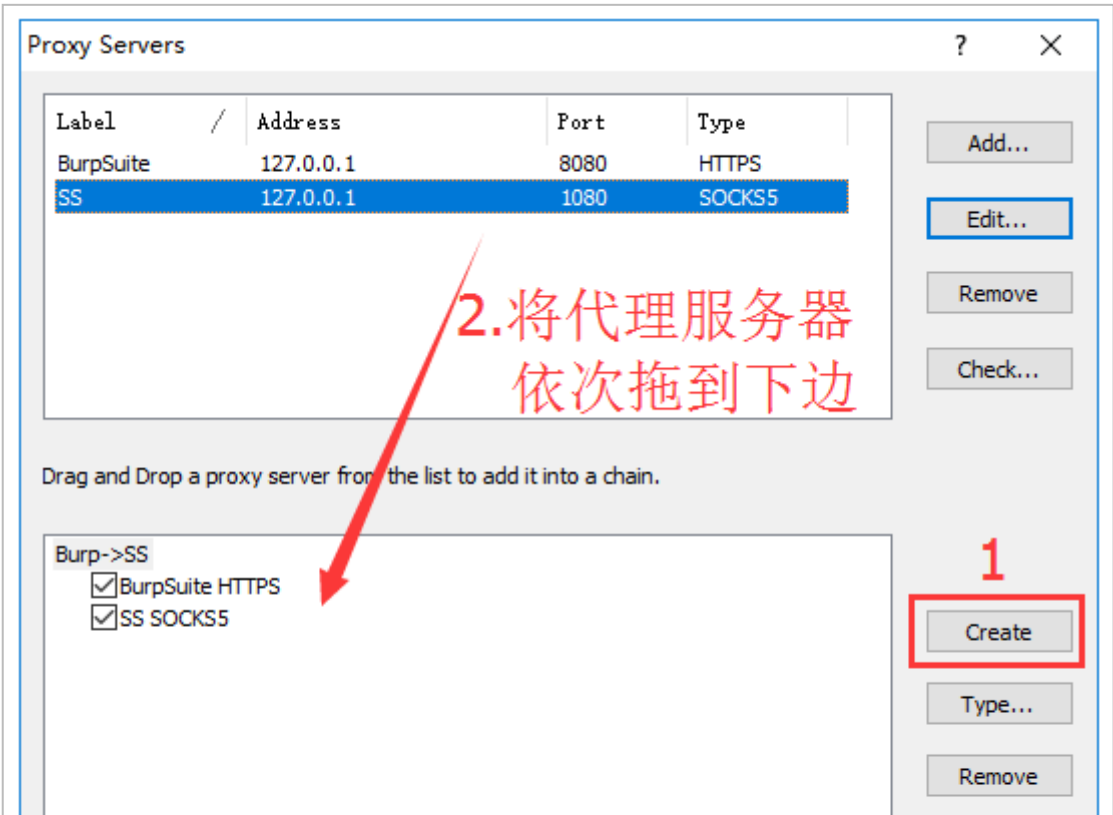
看到连接状态与日志。（PS：我发现每次使用 Proxifier 一开始总会出错，过几秒钟就正常了，不知道啥原因？）

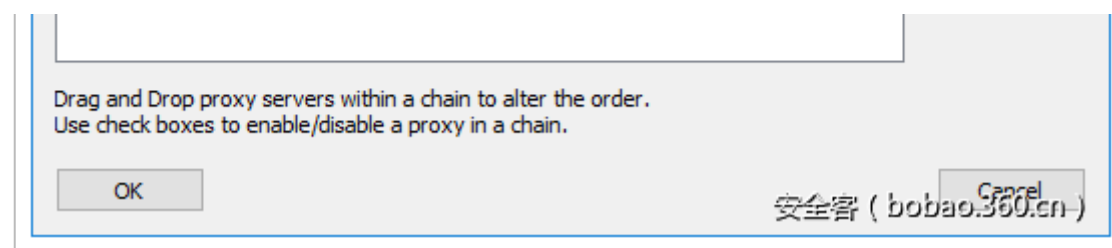


回到本节开头的那个问题，对于那些无法设置代理的客户端程序，可以使用 Proxifier 为其设置代理，进而使用 BurpSuite 等工具抓包分析。此外，如果将 Proxification Rule 中的 Application 设置为 IE 浏览器，即可选择性地将目标站点的 HTTP 请求发送至 BurpSuite，这就解决了使用 IE 进行渗透测试时代理设置不方便的问题。

2. 代理链设置

接下来说一说 Proxifier 的代理链功能。为了实现代理链，首先需要设置多个代理（在 Proxifier 中，仅有一个代理服务器的代理链也是允许的，但那没什么意义）。还拿 google.com 的例子进行说明，我们需要两个代理：BurpSuite (127.0.0.1:8080) 和 SS (127.0.0.1:1080)。先在 Proxy Servers 中增加一个 SS (127.0.0.1:1080) 的 SOCKS5 代理服务器。然后点击下方右侧的 Create 按钮，新建一个代理链，名称随意，比如 BurpSuite->SS。最后用鼠标依次将上方的 BurpSuite 和 SS 代理服务器拖到下方即可。注意，这里的顺序也很重要。



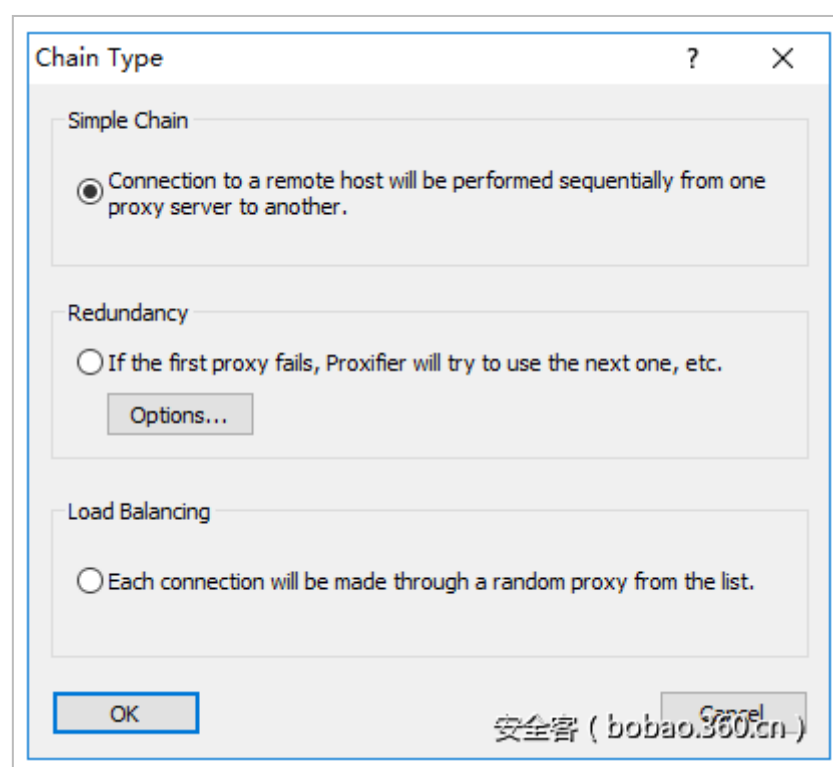


点击 Create 按钮下方的 Type 按钮可以设置代理链的类型，一共有 3 种类型的代理链：

Simple Chain：简单类型，请求数据从上到下依次经过各代理服务器，这个是默认选项。

Redundancy：冗余类型，如果第一个代理服务器无法连接，则尝第二个，以此类推。

Load Balancing：负载均衡类型，请求数据会随机地发送到列表中的各个代理服务器。



按照我们的需求，需要选择默认的 Simple Chain。有了代理链，接下来仍然需要设置代理规则，设置方法同前，只不过在 Action 中选择刚才设置的代理链即可。

BurpSuite 自带的 Upstream Proxy Servers 和 SOCKS Proxy 完全可以解决 google.com 的问题，这里仅仅是以此为例进行说明。Proxifier 的代理链功能十分强大，至于怎么用就看大家的脑洞了~

0x05 结束语

本文总结了我在使用 BurpSuite 过程中所学会一点关于代理设置的小技巧。个人感觉平时在使用 BurpSuite 的过程中，仅仅用到了一小部分功能。今后应该抽空多研究一下自带的帮助文档，也希望大家多分享相关的技巧，大家共同进步！