渗透测试神器-Burp精通学习（附下载）

原创

zkzq 于 2020-11-26 11:07:57 发布

> 版本说明：Burp Suite2.1
> 下载地址：链接：https://pan.baidu.com/s/1JPV8rRjzxCL-4ubj2HVsug 提取码：zkaq
> 使用环境：jre1.8以上
> 下载链接：https://pan.baidu.com/s/1wbS31_H0muBBCtOjkCm-Pg
> 提取码：zkaq
> 工具说明：Burp Suite 是用于攻击web 应用程序的集成平台

引言

在全球最受安全人员欢迎的工具榜单中，Burp Suite这个工具排名第一，并且排名第二的工具和它的功能和作用是一样的，并且还是免费的。

burp这个工具还是付费的，还能一直保持第一。可见burp这个工具在我们安全圈他的地位。

Burp Suite是一款信息安全从业人员必备的集成型的渗透测试工具，它采用自动测试和半自动测试的方式，包含了Proxy,Spider,Scanner,Intruder,Repeater,Sequencer,Decoder,Comparer等工具模块。

通过拦截HTTP/HTTPS的web数据包，充当浏览器和相关应用程序的中间人，进行拦截、修改、重放数据包进行测试。

所以本文会对burp的一些安装以及使用，进行一个系统的介绍。

burp的安装以及其配置

Burp Suite是由Java语言编写而成，而Java自身的跨平台性，使得软件的学习和使用更加方 便。

Burp Suite不像其他的自动化测试工具，它需要你手工的去配置一些参数，触发一些自动 化流程，然后它才会开始工作。

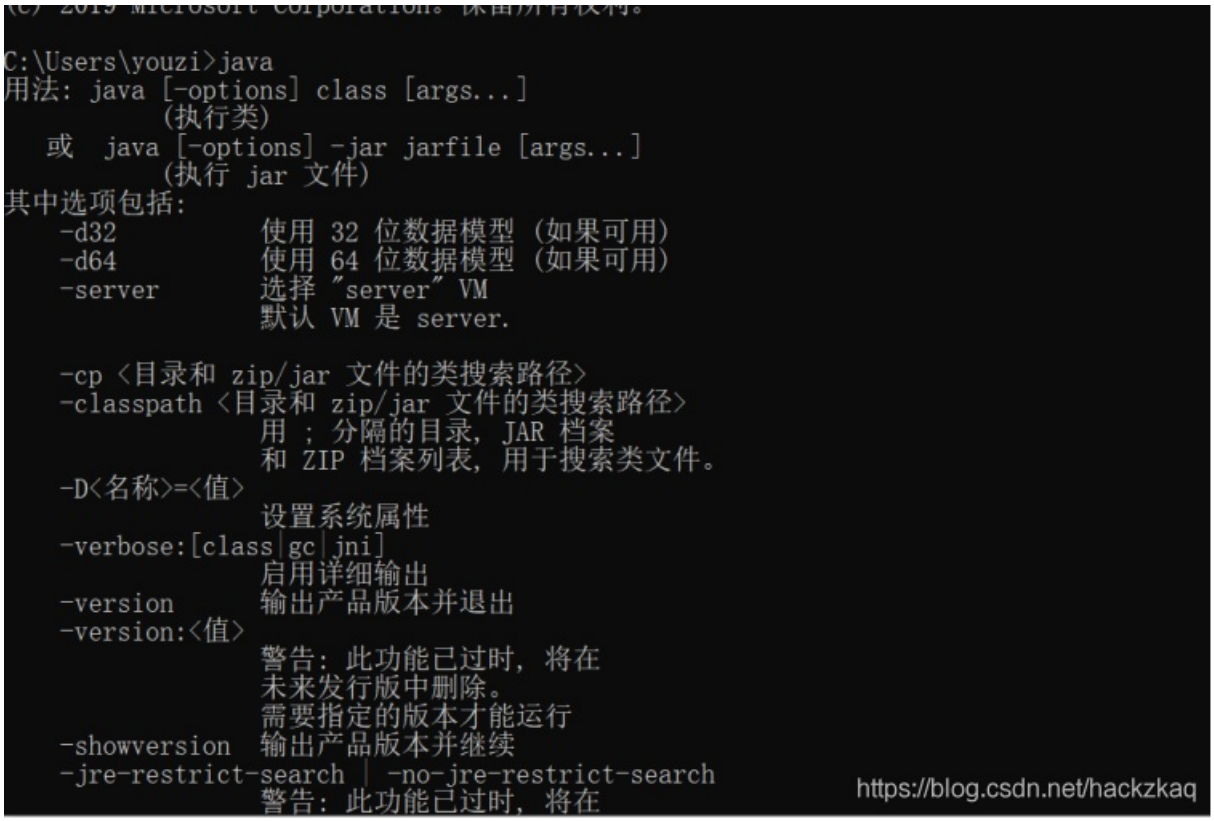
Burp Suite可执行程序是java文件类型的jar文件。

因为burp这个工具是付费的

所以有很多大佬弄了这个工具的破解版，基本功能都是具备的，知识许多高级工具会受限制，无法使用。

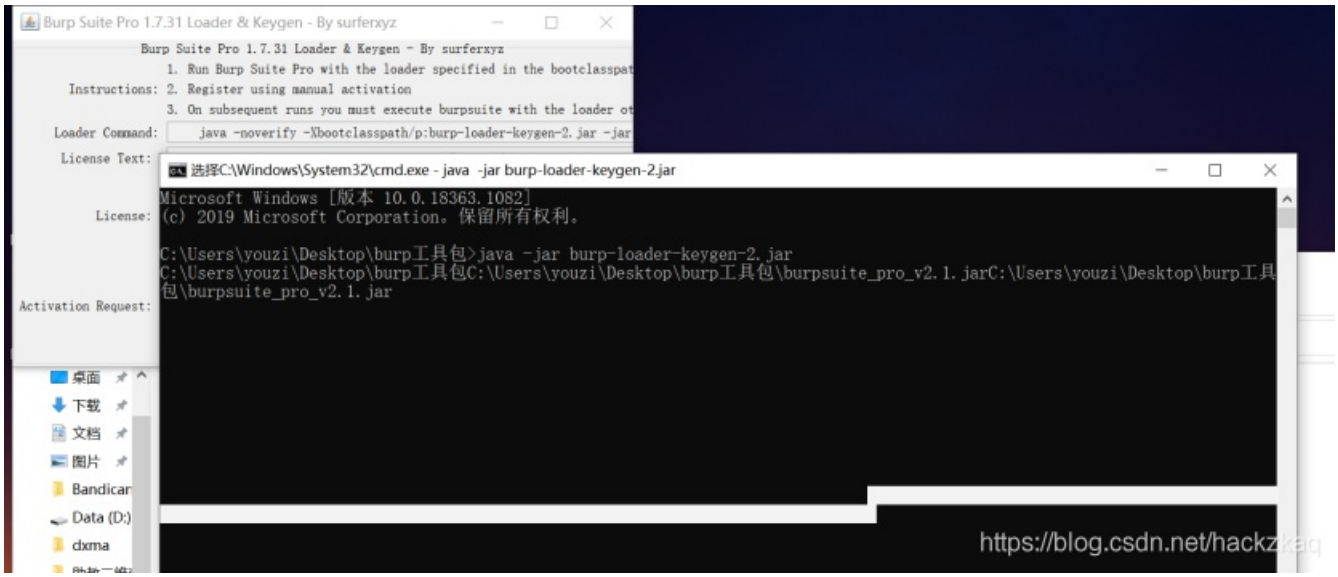
在burp工具下载安装之前，要确保自己的电脑本地安装了java环境。

网站上面有很多教程，我们直接按步骤安装就可以了。安装完java环境之后，打开cmd命令行，如果呈现出来下图所示的效果，就证明java环境已经安装好了。



Burp Suite是一个无需安装软件，下载完成后，直接从命令行启用即可。

这时，你只要在 cmd里执行java -jar /你burp工具的路径/burpSuite名字.jar即可启动Burp Suite,或者，
在工具所在路径下面打开cmd命令行，输入Java -jar burpSuite名字.jar



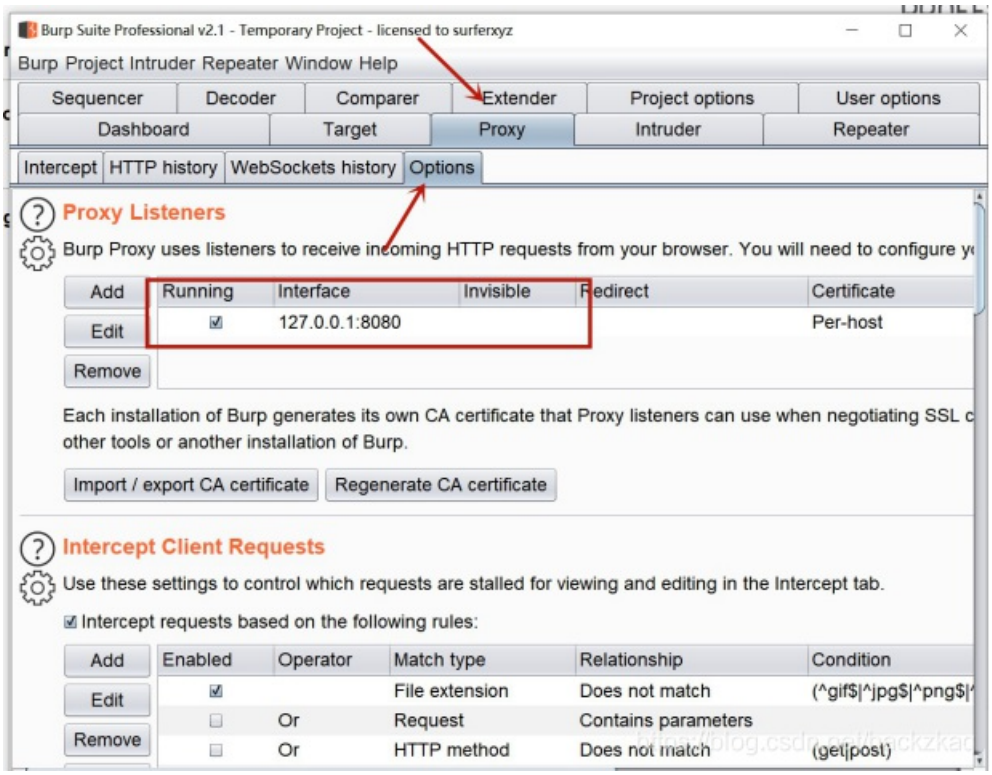
burp代理和浏览器设置

Burp Suite代理工具是以拦截代理的方式，拦截所有通过代理的网络流量，如客户端的请求数据、服务器端的返回信息等。

Burp Suite主要拦截http和https协议的流量，通过拦截，Burp Suite以中间人的方式，可以对客户端请求数据、服务端返回做各种处理，以达到安全评估测 试的目的。

在日常工作中，我们最常用的web客户端就是的web浏览器，我们可以通过代理的设置，做到 对web浏览器的流量拦截，并对经过Burp Suite代理的流量数据进行处理。

当Burp Suite 启动之后，默认拦截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。如图：


Burp Suite Professional v2.1 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Sequencer
Decoder
Comparer
Extender
Project options
User options
Dashboard
Target
Proxy
Intruder
Repeater
Intercept
HTTP history
WebSockets history
Options
Proxy Listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure y
Add
Edit
Remove
Running
Interface
Invisible
Redirect
Certificate
127.0.0.1:8080
Per-host
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL c
other tools or another installation of Burp.
Import / export CA certificate
Regenerate CA certificate
Intercept Client Requests
Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.
Intercept requests based on the following rules:
Add
Edit
Remove
Enabled
Operator
Match type
Relationship
Condition
File extension
Does not match
(^gif$|^jpg$|^png$|
Or
Request
Contains parameters
Or
HTTP method
Does not match
(get|post)

FireFox设置

系统代理

启动FireFox浏览器，点击右上角三条横线，点击【选项】。

2.在出现的搜索框里输入代理，点击【设置】。

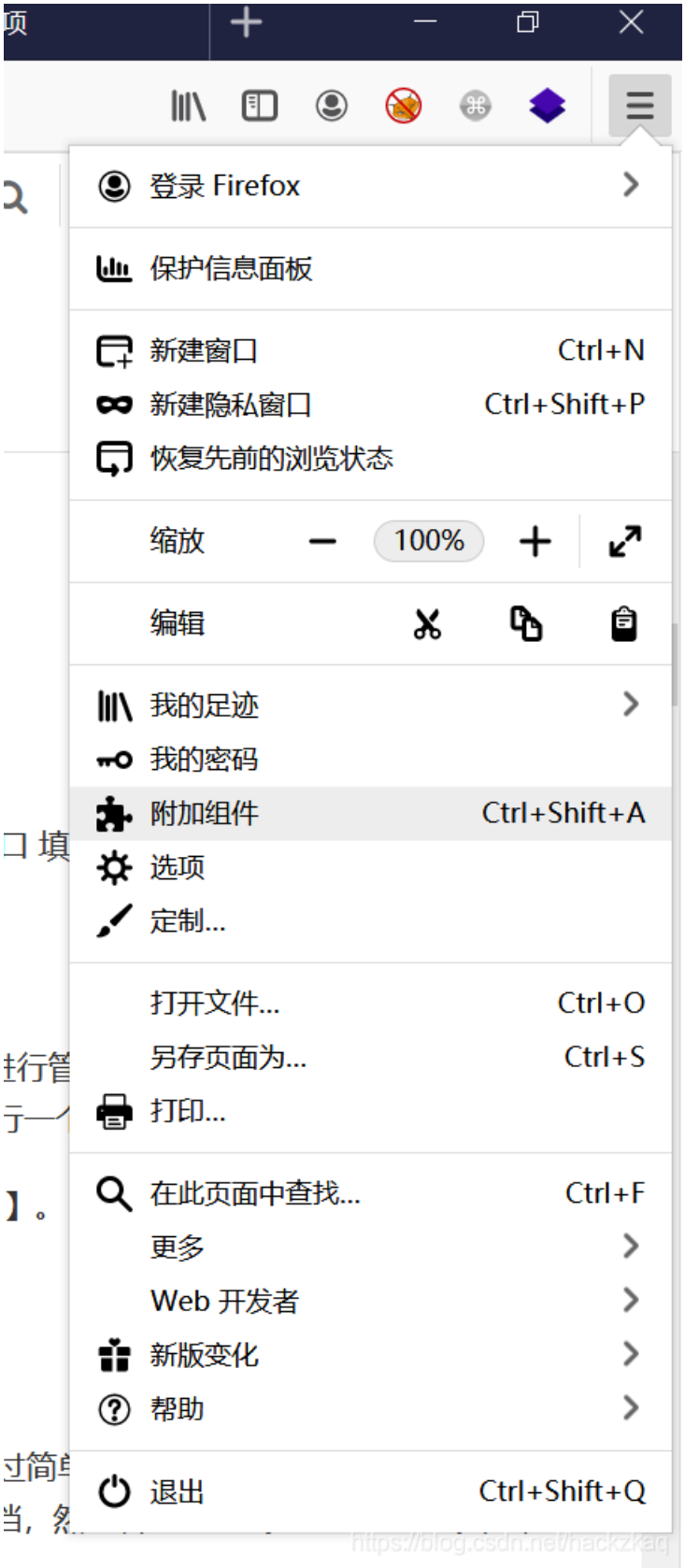
3.勾选手动代理配置，找到“http代理”，填写127.0.0.1，端口 填写8080，最后点击【确认】保存参数设置，完成FireFox的代理配置。

扩展插件

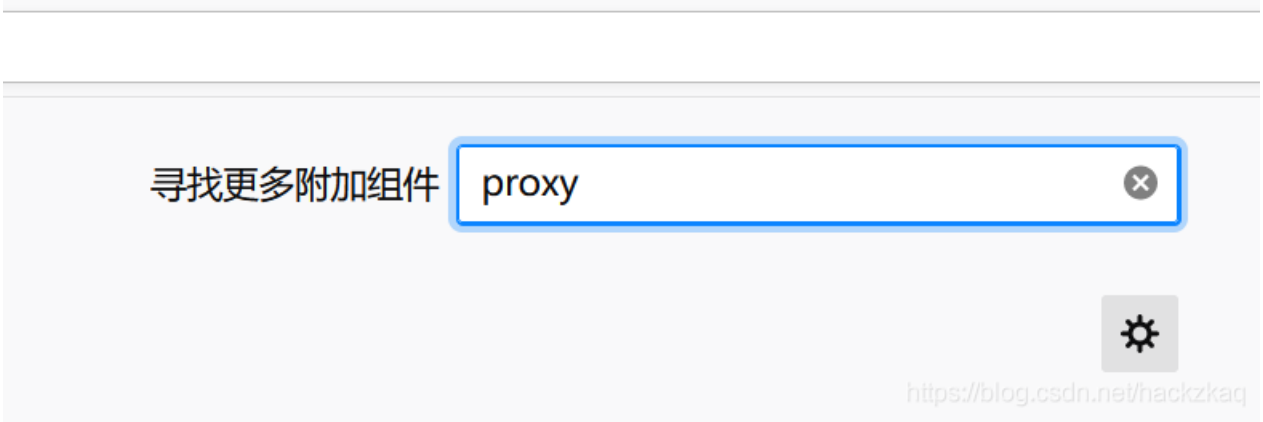
FireFox浏览器中，可以添加FireFox的扩展组件，对代理服务器进行管理。

例如 FoxyProxy、FireX Proxy、Proxy Swither都是很好用的组件，这里对FoxyProxy进行一个讲解。

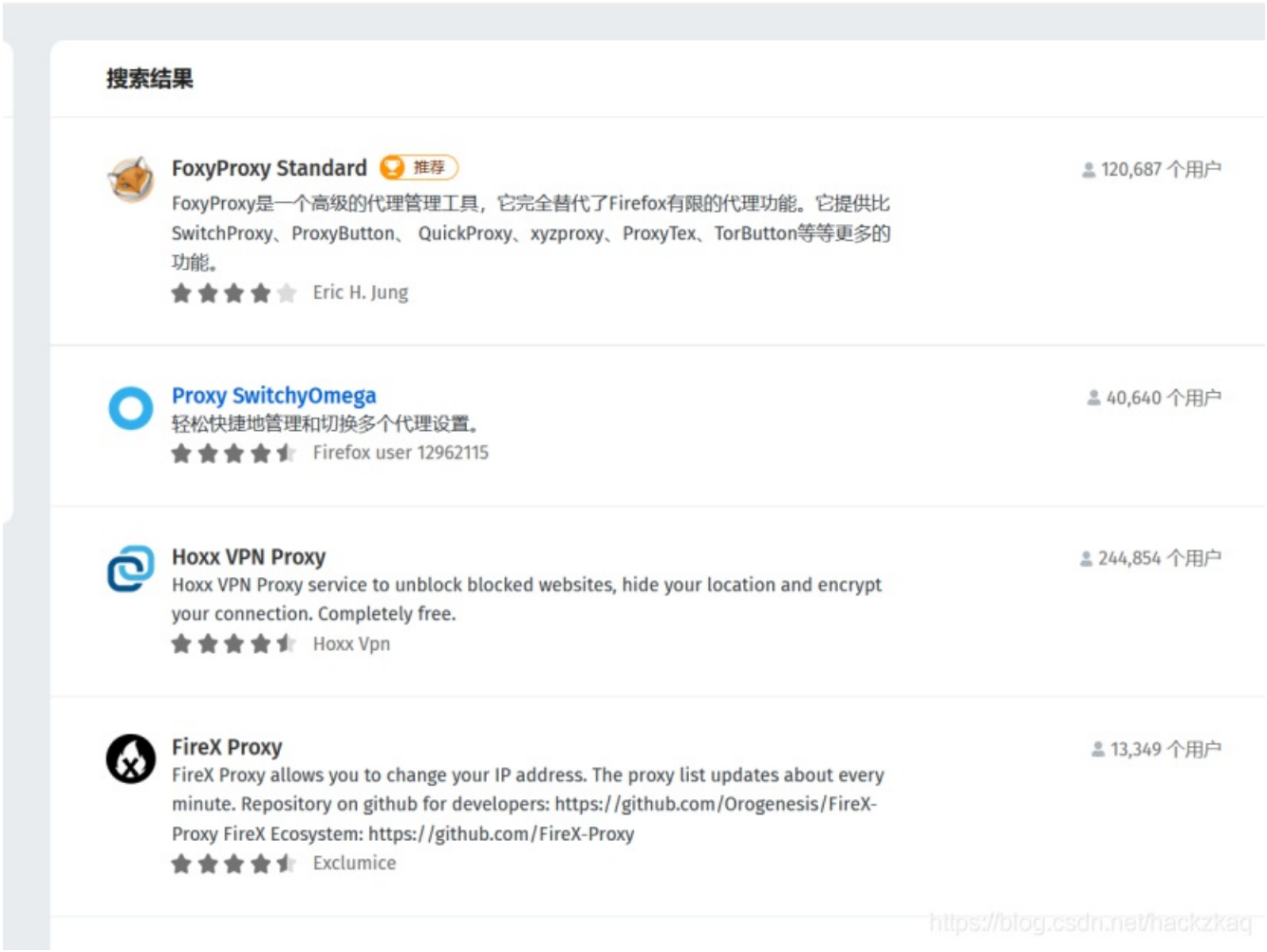
1.启动FireFox浏览器，点击右上角三条横线，点击【附加组件】。



2.在出现的搜索框里输入proxy。



呈现出的所有插件都是和代理相关的，选择你要安装的插件就可以了。



4.安装成功之后，会在浏览器右上角出现对应插件的标志。点击插件，点击【选项】。

5.对应把我们拦截的IP,拦截的端口添加上去。

6.使用哪一个代理的时候，就勾选对应的代理名称即可。

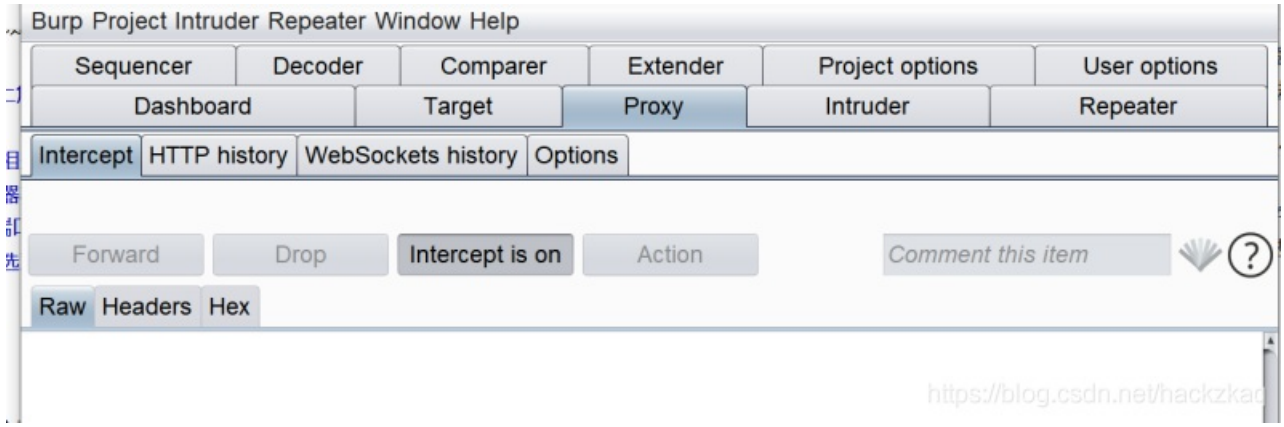
如何使用burp代理

Burp Proxy 是Burp Suite以用户驱动测试流程功能的核心，通过代理模式，可以让我们拦截、 查看、修改所有在客户端和服务端之间传输的数据包。

使用burp的流程如下：

首先，再确认burp工具安装成功，能正常运行之后，并且已经完成浏览器的代理 服务器配置。

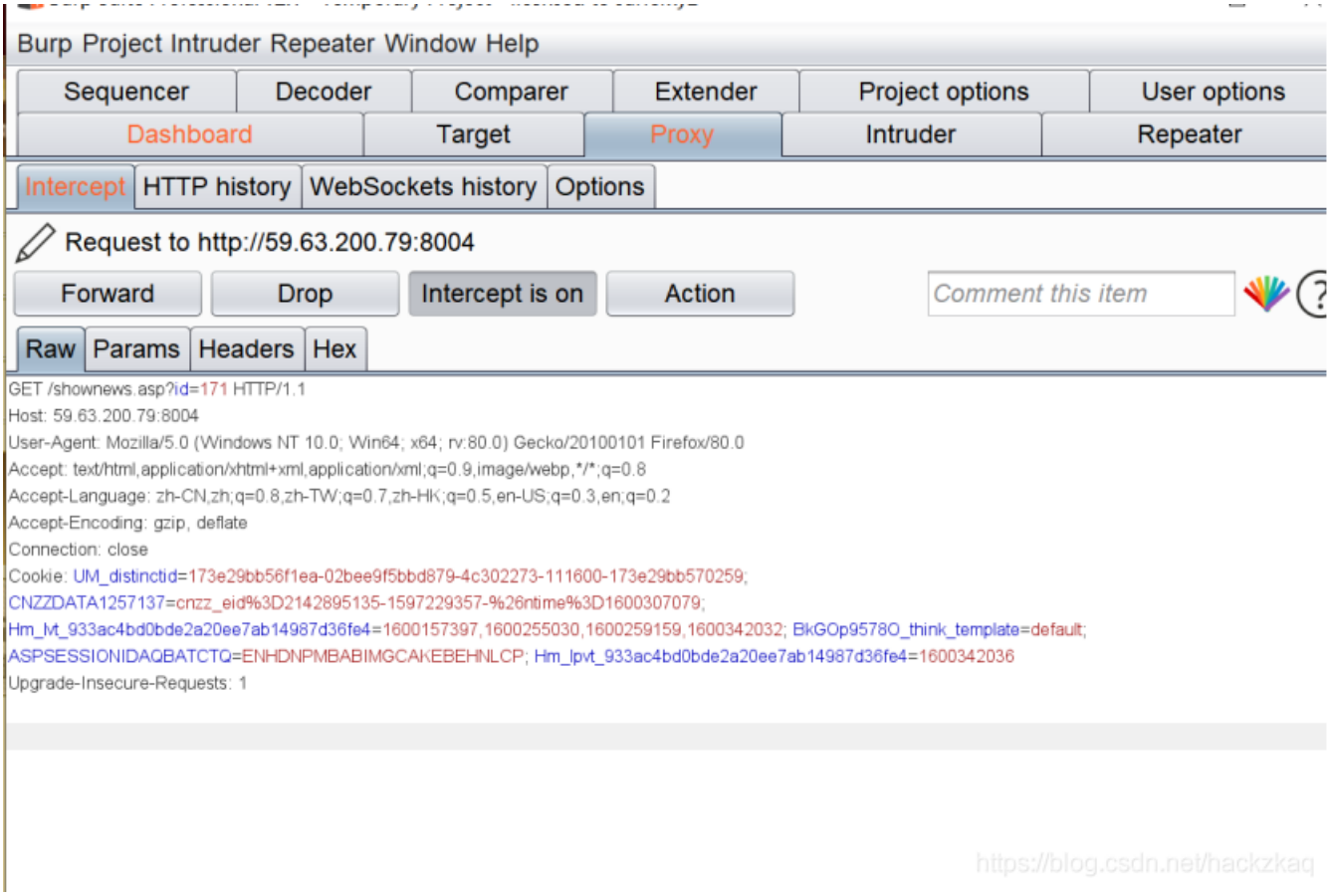
打开Proxy功能中的Intercept选项卡，确认拦截功能也就是能够抓数据包为“Interception is on”状态，如果显示 为“Intercept is off”则点击它，打开拦截功能。



3.打开浏览器，输入你需要访问的URL
（以靶场地址http://59.63.200.79:8004/shownews.asp?id=171 为例）并回车，这时你 将会看到数据流量经过Burp Proxy并暂停，直到你点击【Forward】，才会继续传输下去。

如果你点击了【Drop】，则这次通过的数据将会被丢失，不再继续处理。

4.当我们点击【Forward】之后，我们将看到这次请求返回的所有数据。



当Burp Suite拦截的客户端和服务器交互之后，我们可以在Burp Suite的消息分析选项卡中查看这次请求的实体内容、消息头、请求参数等信息。

消息分析选项视图主要包括以下四项：

Raw：web请求的raw格式，包含请求地址、http协议版本、主机头、浏 览器信息、Accept可接受的内容类型、字符集、编码方式、cookie等。我们可以手工去修改这些信息，对服务器端进行渗透测试。

params：客户端请求的参数信息、包括GET或者POST请求的参数、 Cookie参数。渗透人员可以通过修改这些请求参数来完成对服务器端的渗透测试。

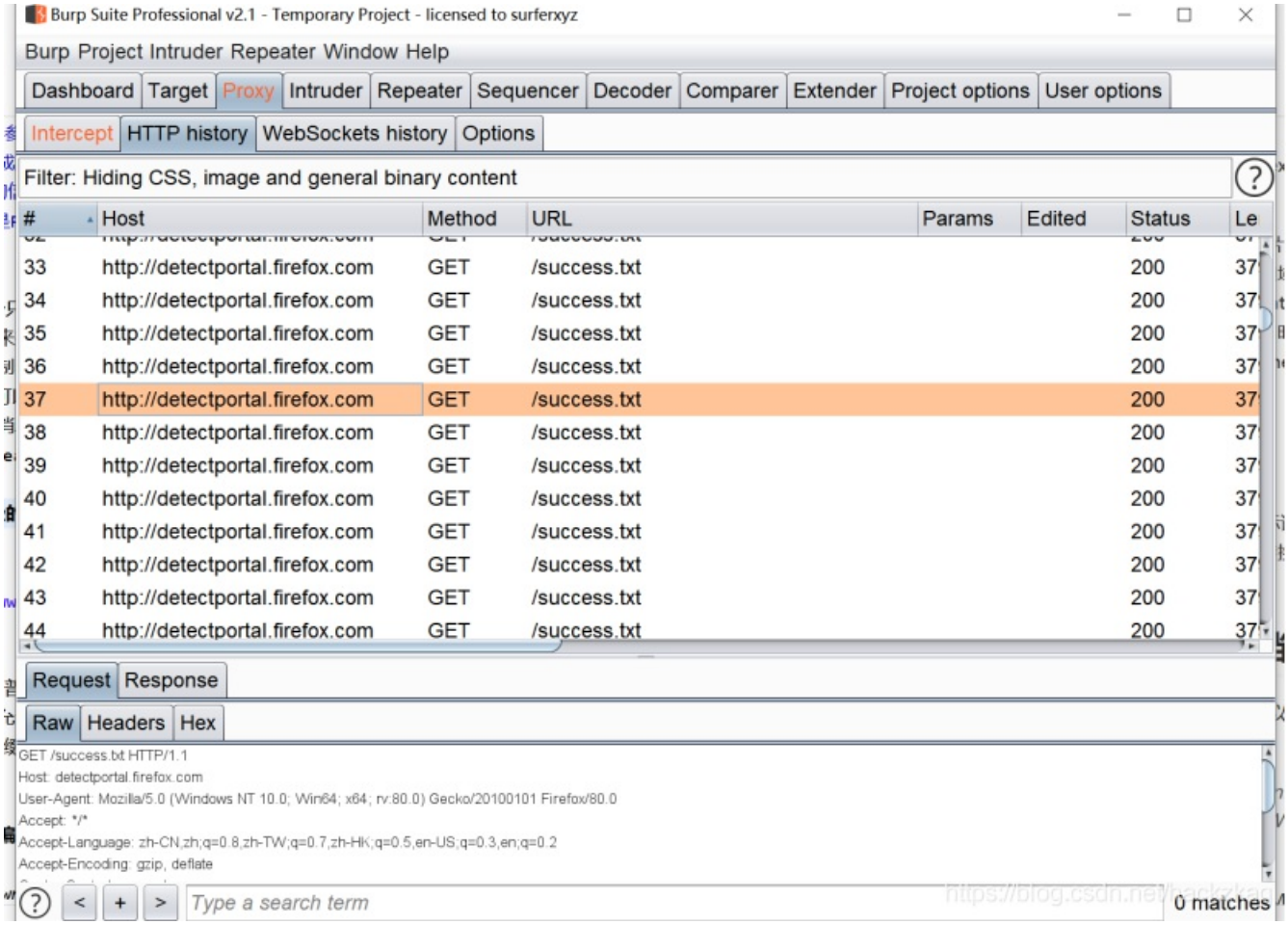
headers：与Raw显示的信息类似，只是在这里面展示得更直观。

Hex：这个视图显示的是Raw的二进制内容，渗透测试人员可以通过hex编辑器对请求的内容进行修改。

一般情况下，Burp Proxy只拦截请求的消息，普通文件请求如css、js、图片是不会被拦截 的，你可以修改默认的拦截选项来拦截这些静态文件，当然，你也可以通过修改拦截的作用域，参数或者服务器端返回的关键字来控制Burp Proxy的消息拦截。

所有流经Burp Proxy的消息，都会在http history记录下来，我们可以通过历史选项卡，查看传输的数据内容，对交互的数据进行测试和验证。

同时，对于拦截到的消息和历史消息，都可以通过右击弹出菜单，发送到Burp的其他组件，如Spider、Scanner、 Repeater、Intruder、Sequencer、Decoder、Comparer、Extender，进行进一步的测试。



对数据包的操作

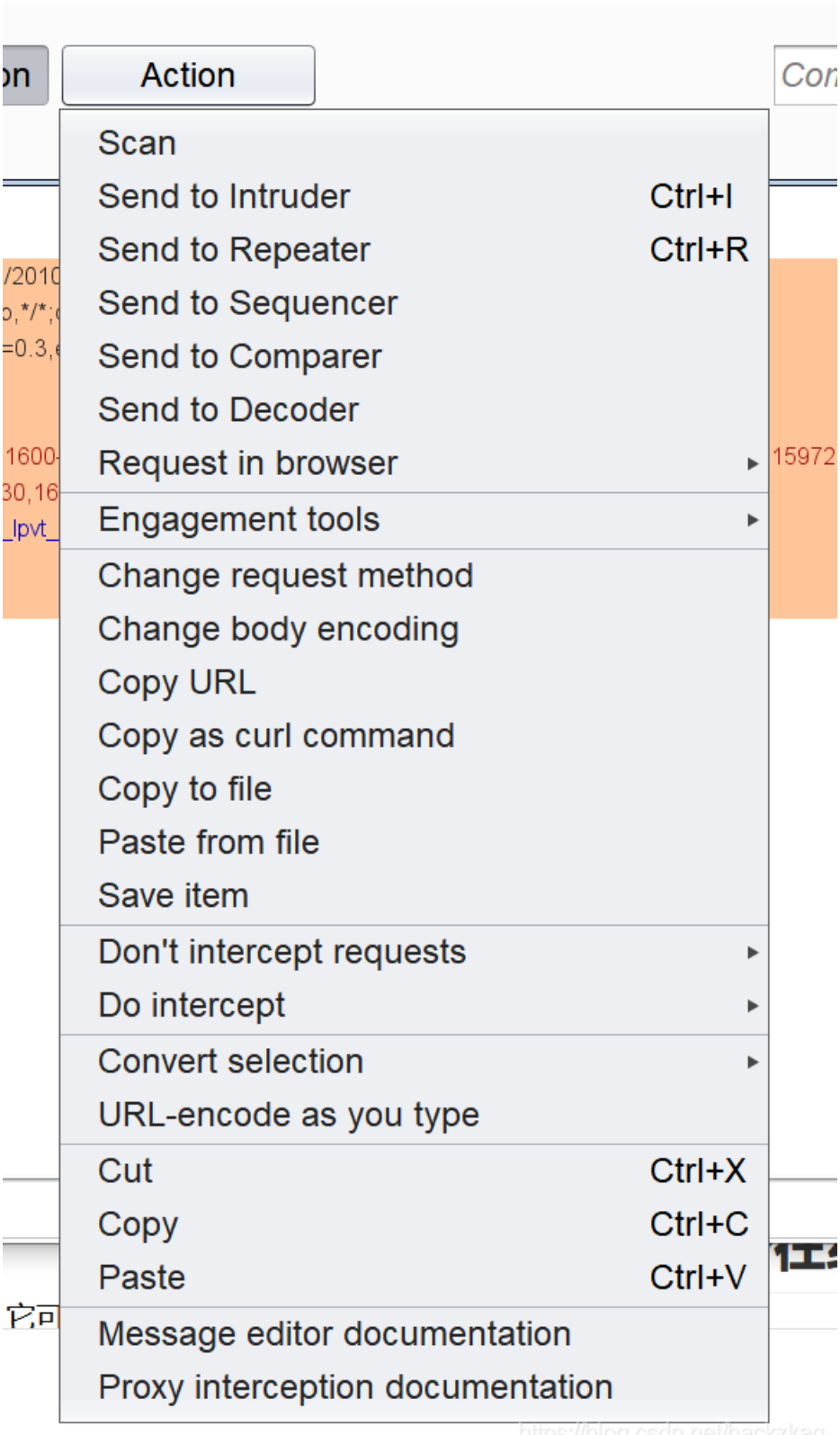
Burp Proxy的拦截功能主要由Intercept选项卡中的Forward、Drop、Interception is on/off、 Action、Comment 以及Highlight构成，它们的功能分别是：

Forward的功能：当你查看过消 息或者重新编辑过消息之后，点击此按钮，将发送消息至服务器端。
Drop的功能：你想丢失 当前拦截的消息，不再forward到服务器端。

Interception is on：表示拦截功能打开，拦截所有 通过Burp Proxy的请求据。

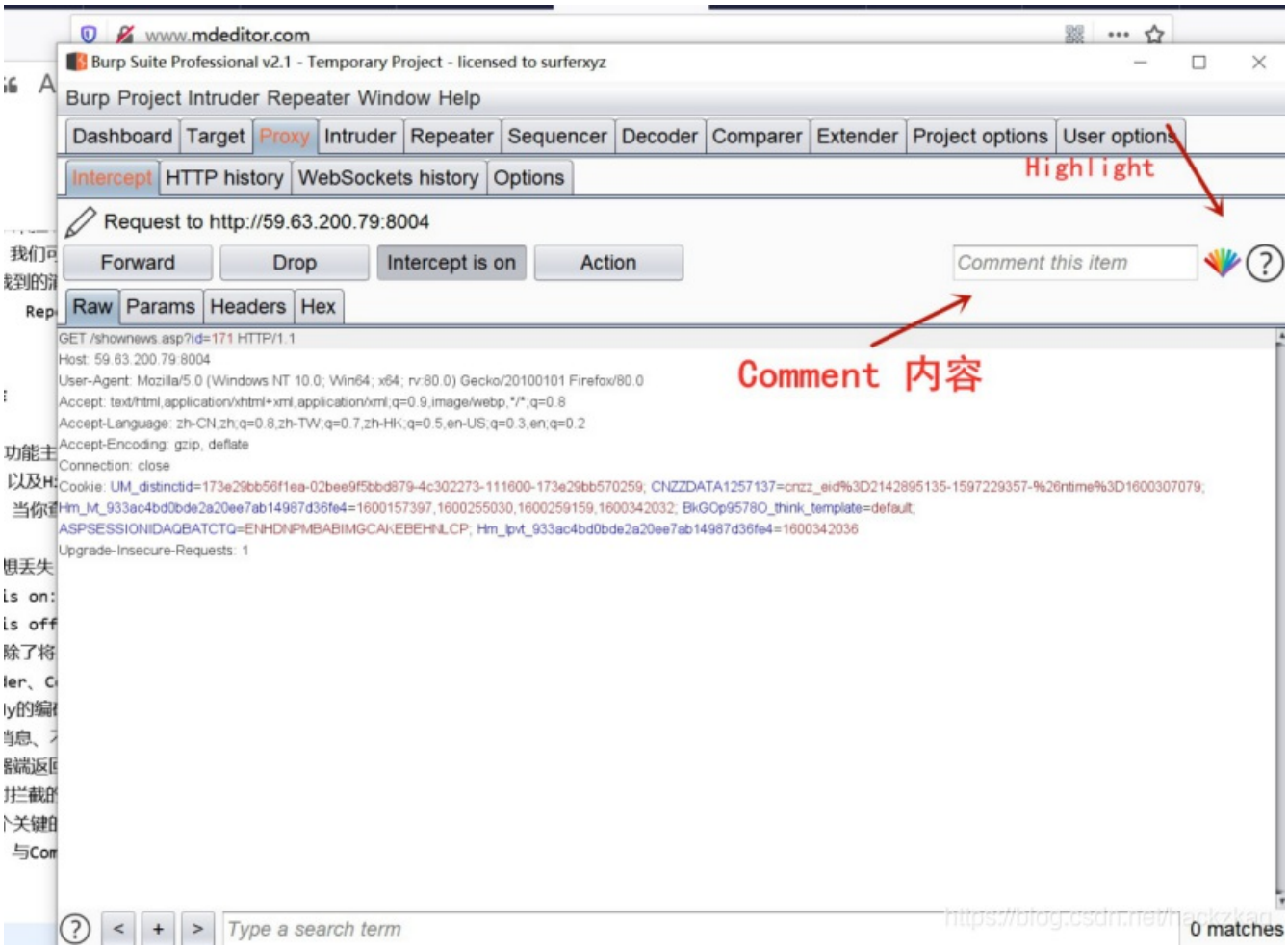
Interception is off表示拦截功能关闭，不再拦截通过Burp Proxy的所有请求数据。

Action的功能：除了将当前请求的消息传递到Spider、Scanner、 Repeater、Intruder、Sequencer、Decoder、Comparer组件外，还可以做一些请求消息的修改，如改变GET或者POST请求方式、改变请求body的编码，同时也可以改变请求消息的拦截设置，如不再拦截此主机的数据包、不再拦截此IP地址的消息、不再拦截此种文件类型的消息、不再拦截此目录的消息，也可以指定针对此消息拦截它的服务器端返回数据。



Comment的功能：对拦截的消息添加备注，在一次渗透测试中，你通常会遇到一连串的请求消息，为了便于区分，在某个关键的请求消息上，你可以添加备注信息。

Highlight的功能：与Comment功能有点类似，即对当前拦截的消息设置高亮，以便于其他的请求消息相区分。



SSL和Proxy高级选项

在前面一章的基础上，我们已经仅仅能够抓HTTP的数据包。

接下来我们继续学习如何抓https的包。

HTTPS协议是为了数据传输安全的需要，在HTTP原有的基础上，加入了安全套接字层SSL协议，通过CA证书来验证服务器的身份，并对通信消息进行加密。

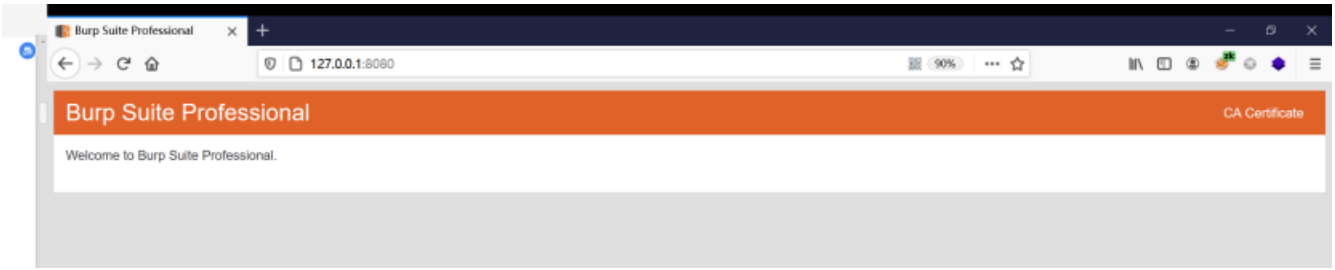
基于HTTPS协议这些特性， 我们在使用Burp Proxy代理时，需要增加更多的设置，才能拦截HTTPS的数据包。

CA证书的安装

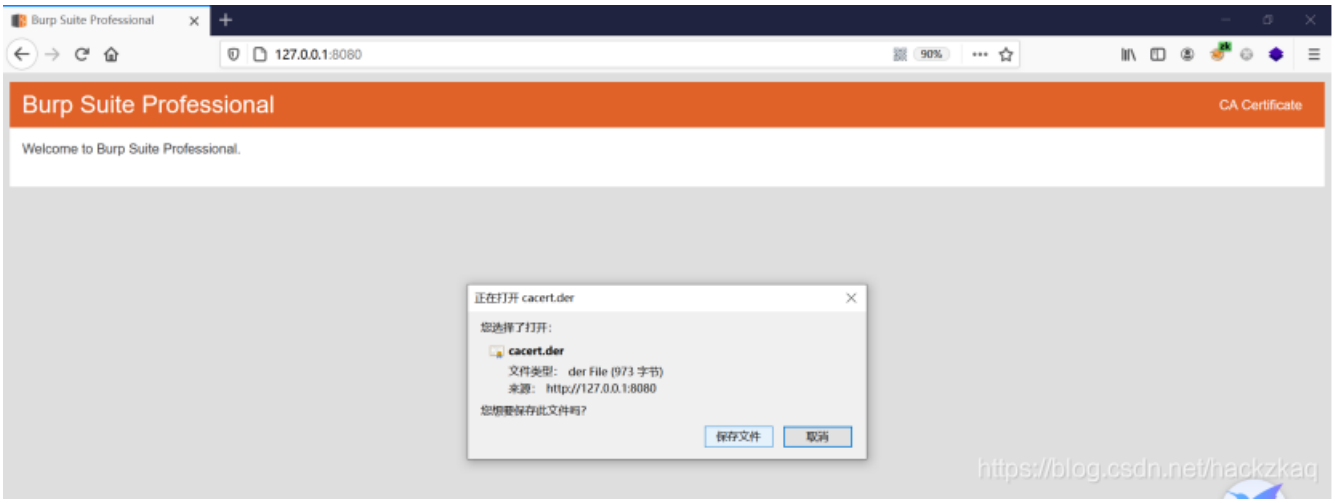
我们都知道，在HTTPS通信过程中，一个很重要的介质是CA证书。

一般来说，Burp Proxy代理过程中的CA主要分为如下几个步骤（以火狐浏览器为例子）

首先，根据前面学习的内容，我们已经已配置好Burp Proxy监听端口和浏览器代理服务器设置。
在burp打开的情况下，在浏览器URL栏的地方输入，你所拦截的IP和你所拦截的端口。127.0.0.1:8080。



3.点击CA证书，点击【保存文件】。



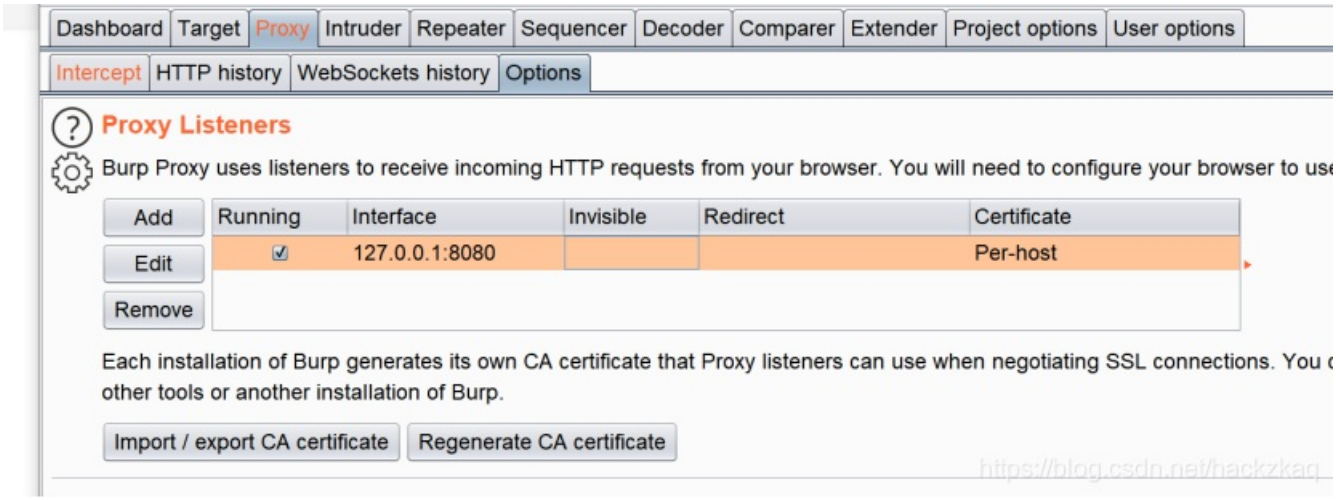
CA证书安装成功之后，就可以抓https的包了。

Proxy监听设置

当我们启动Burp Suite时，默认会监听本地回路地址的8080端口，除此之外，我们也可以在默 认监听的基础上，根据我们自己的需求，对监听端口和地址等参数进行自由设置。

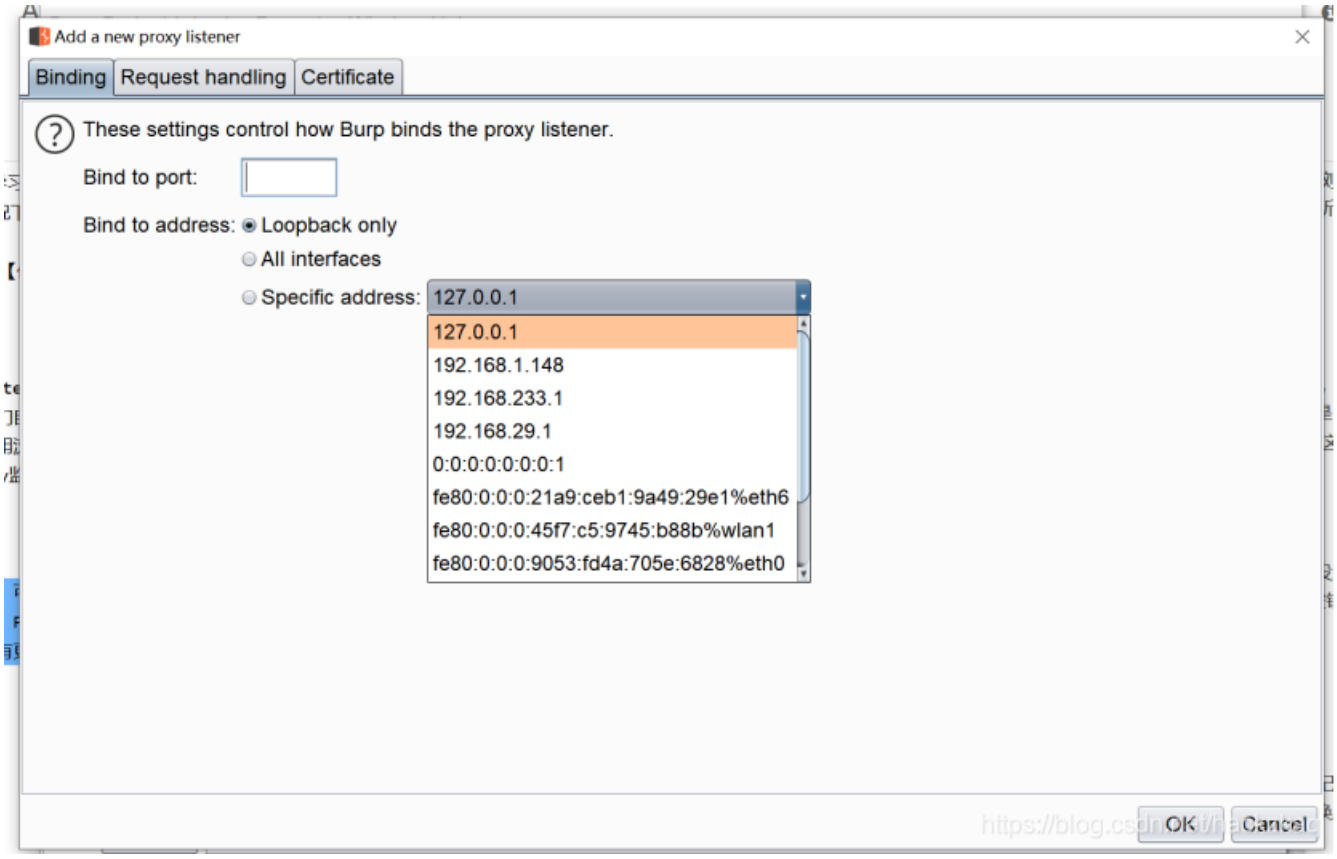
特别是当 我们测试非浏览器应用时，无法使用浏览器代理的方式去拦截客户端与服务器端通信的数据 流量，这种情况下，我们会使用自己的Proxy监听设置，而不会使用默认设置。

Proxy监听设置

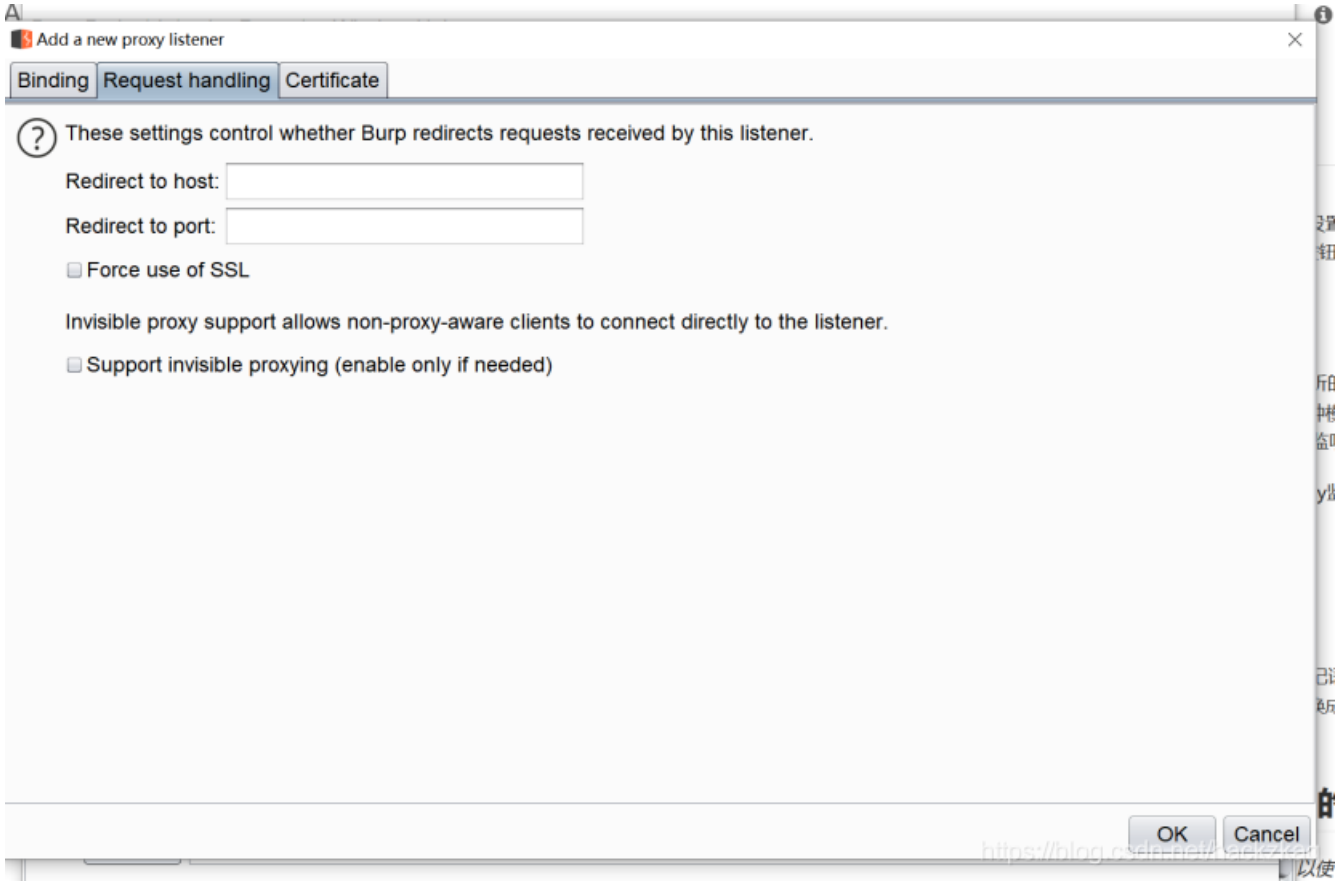


当我们在实际使用中，可能需要同时测试不同的应用程序时，我们可以通过设置不同的代理 端口，来区分不同的应用程序，Proxy监听即提供这样的功能设置。

点击图中的【Add】按钮，会弹出Proxy监听设置对话框，里面有更丰富的设置，满足我们不同的测试需求。



请求处理Request Handling 请求处理主要是用来控制接受到Burp Proxy监听端口的请求 后，如果对请求进行处理的。



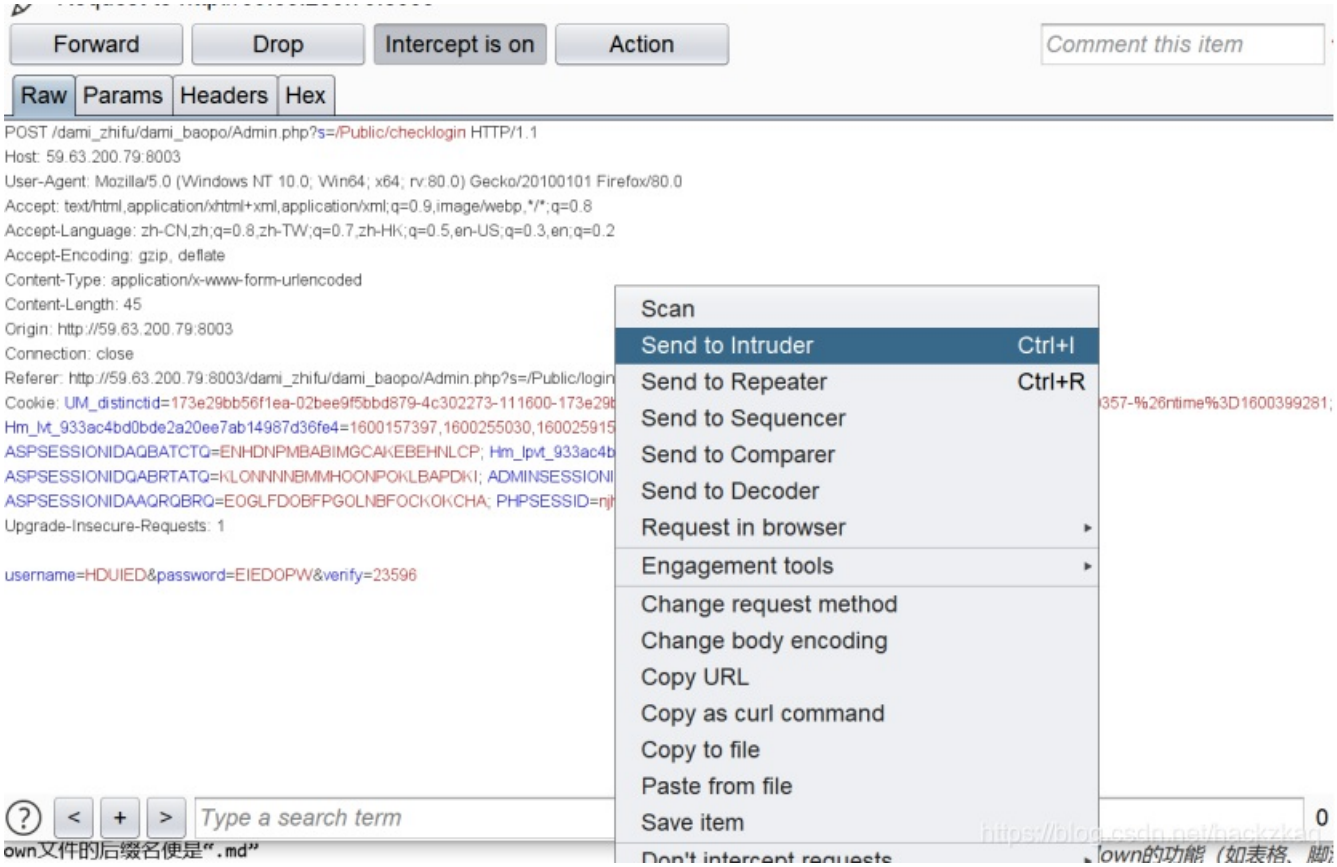
Burp工具之Intruder模块

Burp Intruder作为Burp Suite中一款功能极其强大的自动化测试工具，通常被系统安全渗透测试人员被使用在各种任务测试的场景中。

Intruder使用场景和操作步骤

在渗透测试过程中，我们经常使用Burp Intruder，它的工作原理是：Intruder在原始请求数据的基础上，通过修改各种请求参数，以获取不同的请求应答。

每一次请求中，Intruder通常会携带一个或多个Payload,在不同的位置进行攻击重放，通过应答数据的比对分析来获得需要的特征数据。Burp Intruder通常被使用在以下场景：



标识符枚举Web应用程序经常使用标识符来引用用户、账户、资产等数据信息。例如:用户名，文件ID和密码等。

提取更加精准，有用的数据 在某些场景下，而不是简单地识别有效标识符，你需要通过简单标识符提取一些其他的数据。

比如说，你想通过用户的个人空间id，获取所有用户在个人空间标准的昵称和年龄。

模糊测试，如SQL注入，跨站点脚本和文件路径遍历可以通过请求参数提交各种测试字符串，并分析错误消息和其他异常情况，来对应用程序进行检测。

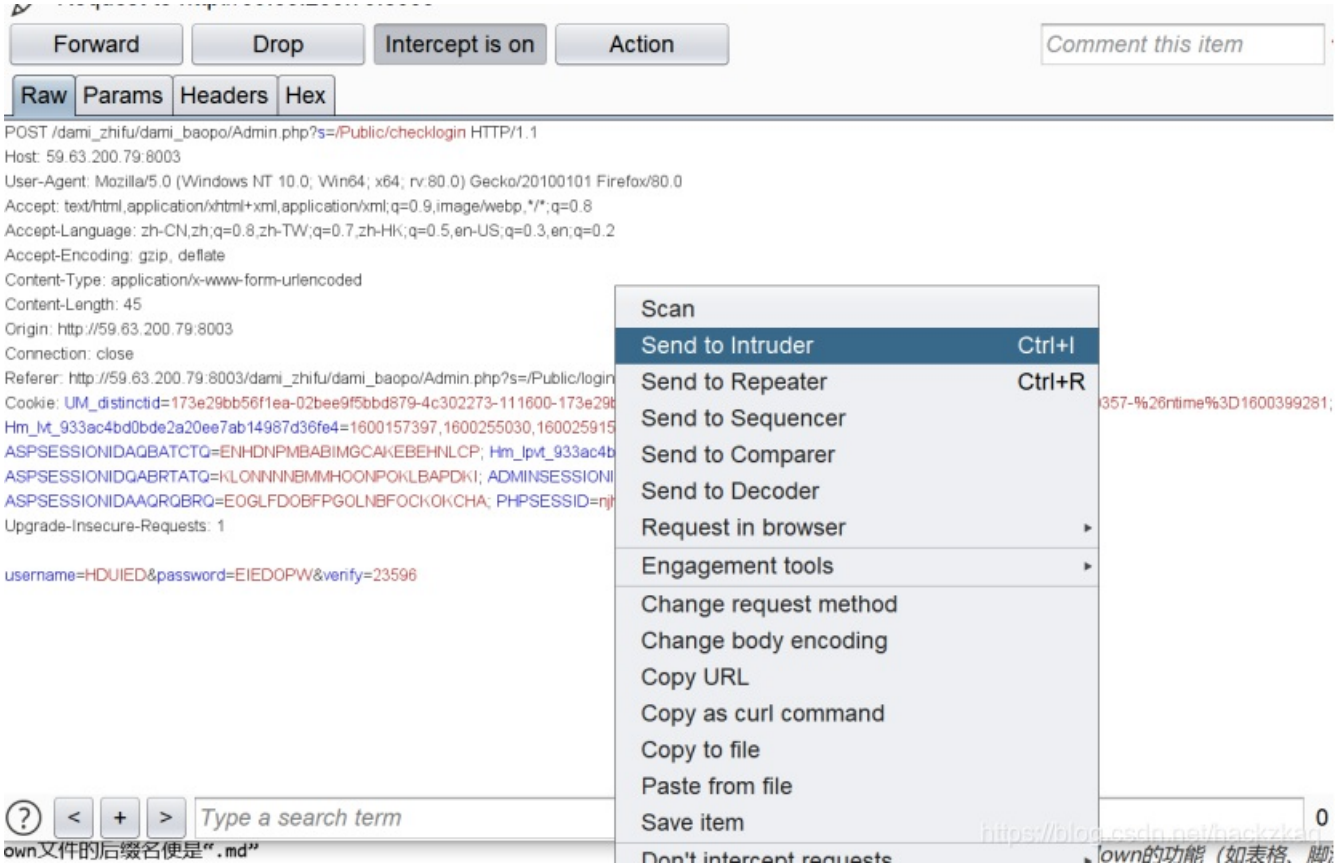
由 于的应用程序的大小和复杂性，手动执行这个测试是一个耗时且繁琐的过程。

这样的场景，您可以设置Payload，通过Burp Intruder自动化地对Web应用程序进行模糊测试。

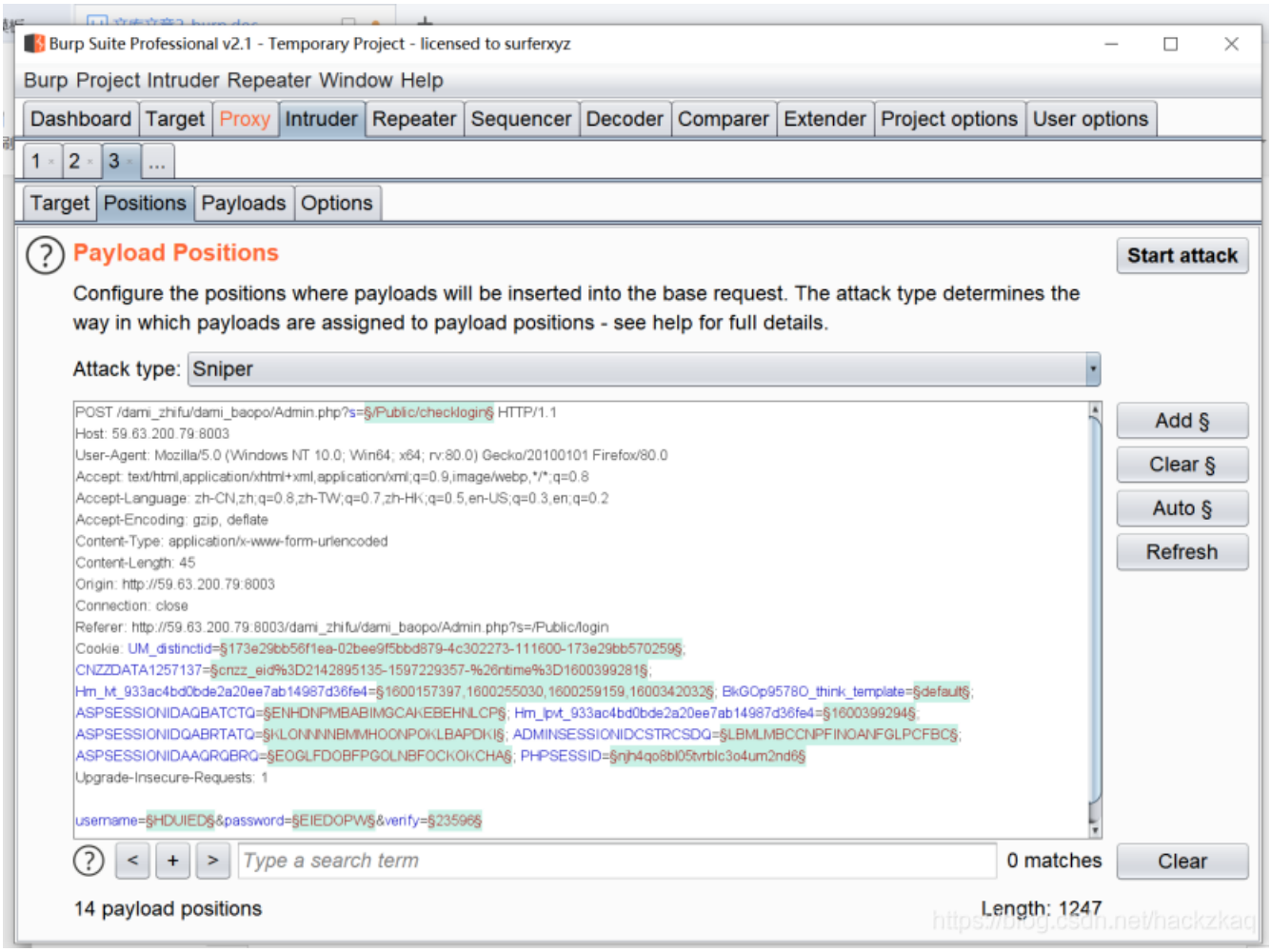
使用Burp Intruder进行测试时，步骤为：

确认Burp Suite安装正确并正常启动，且完成了浏览器的代理设置。

进入Burp Proxy选项卡，并通过右击菜单，发送到Intruder。



3.进行Intruder 选项卡，打开Target和Positions子选项卡。这时，你会看到上一步发送过来 的请求消息。

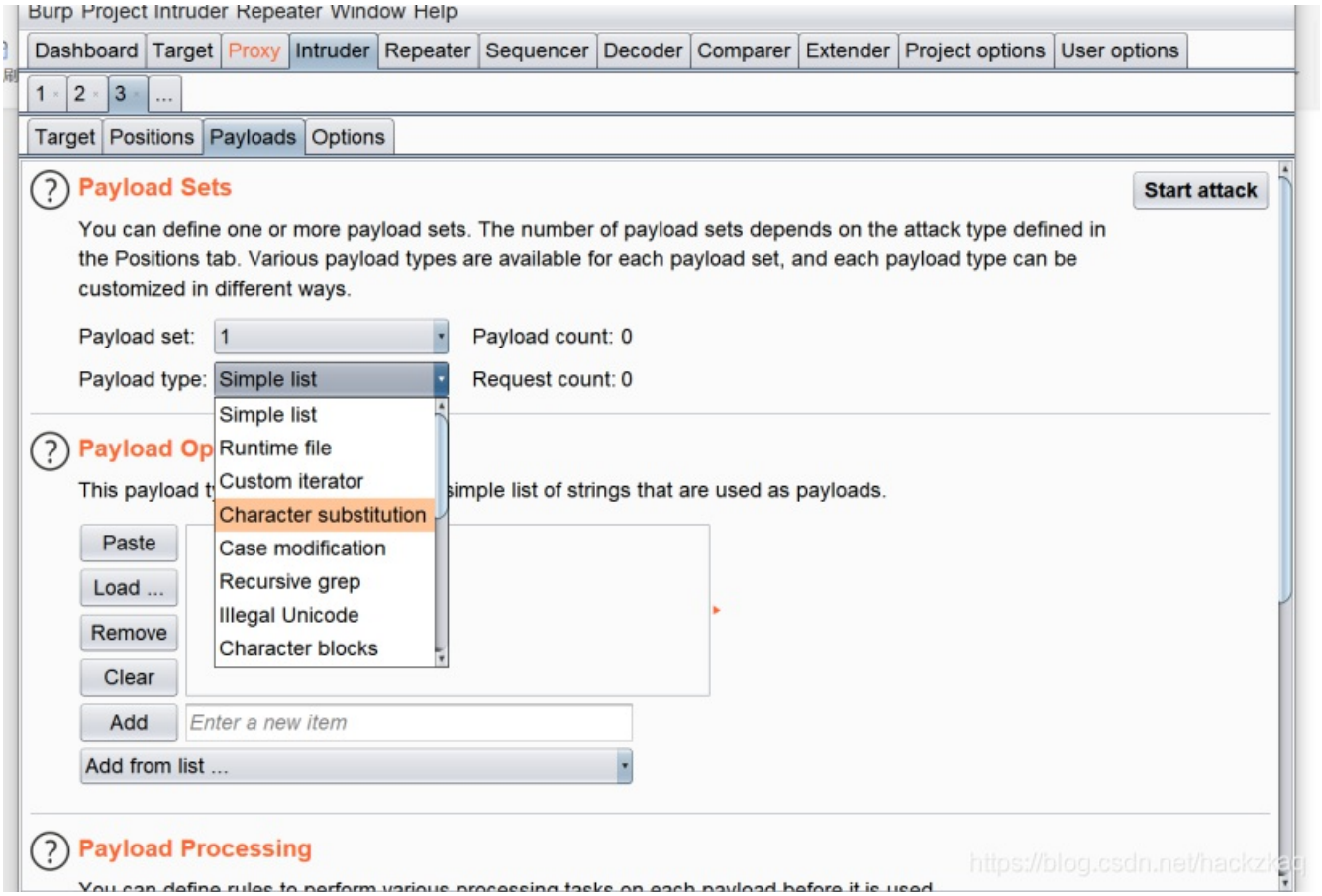


4.因为我们了解到Burp Intruder攻击的基础是围绕刚刚发送过来的原始请求信息，在原始信息指定的位置上设置一定数量的攻击Payload，通过Payload来发送请求获取应答消息。

默认情况下，Burp Intruder会对请求参数和Cookie参数设置成Payload position，前缀添加 标识符合，当发送请求时，会将的参数替换为 Payload。

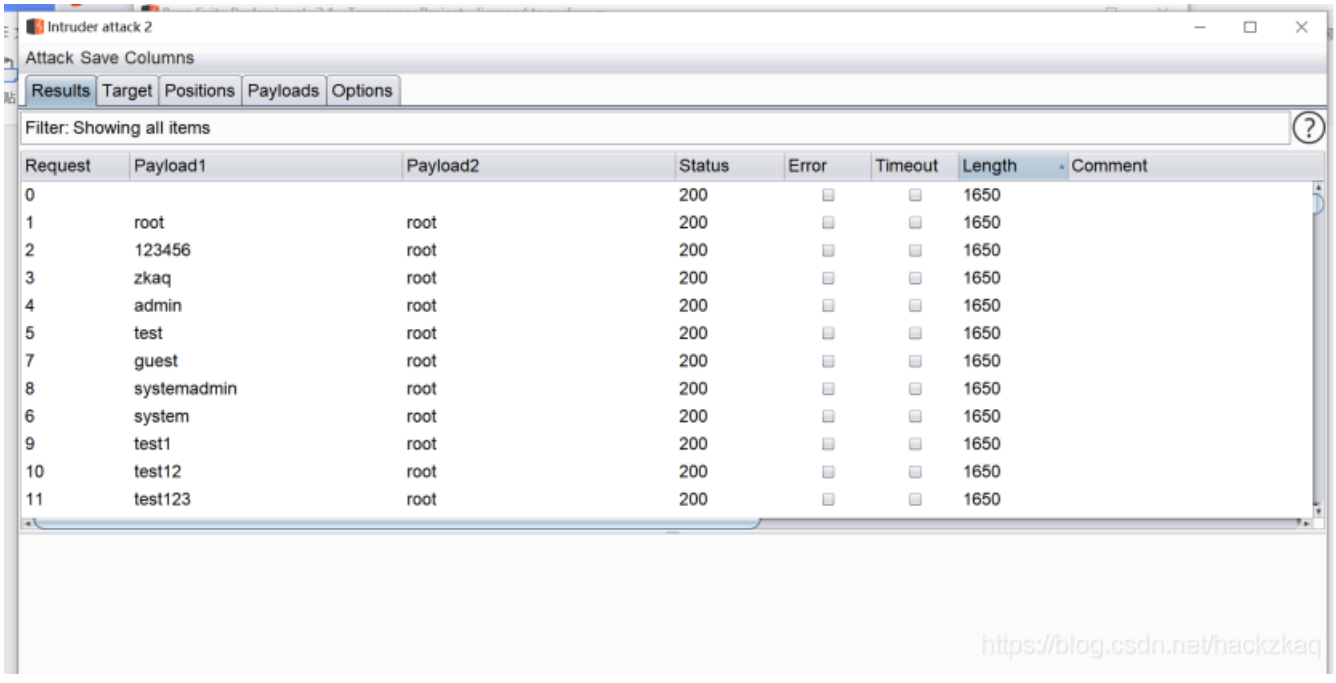
5.在Position界面的右边，有【Add $】、【Clear $】、【Auto $】、【Refersh $】四个按 钮，是用来控制请求消息中的参数在发送过程中是否被Payload替换，如果不想被替换，则选择此参数，点击【Clear 】，即将参数前缀 去掉。

6.当我们打开Payload 子选项卡，选择Payload的生成或者选择策略，默认情况下选 择“Simple list”,当然你也可以通过下拉选择其他Payload类型或者手工添加。

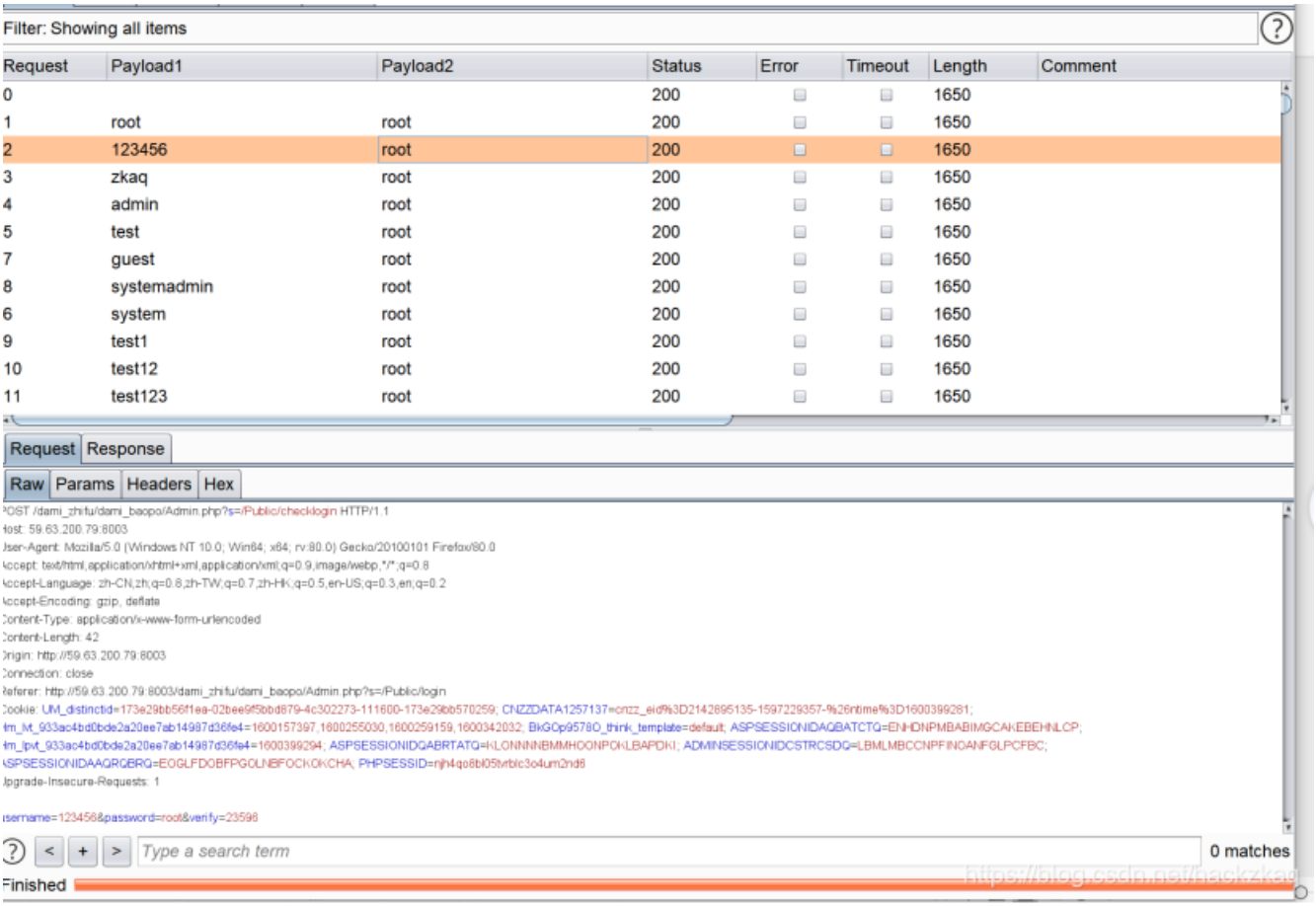


7.此时在界面的右上角，点击【Start attack】，发起攻击。

8.此时，Burp会自动打开一个新的界面，包含攻击执行的情况、Http状态码、长度等结果信息。



9.我们可以选择其中的某一次通信信息，查看请求消息和应答消息的详细。



观察那些长度异常的结果。

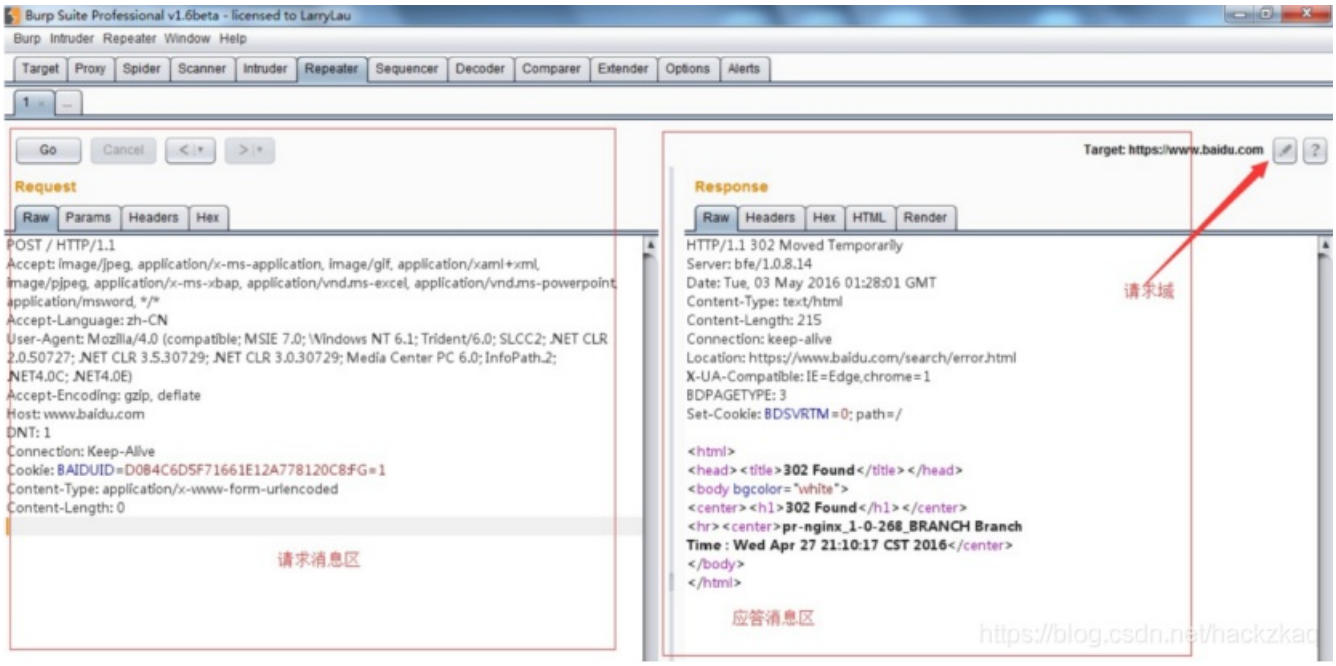
Burp工具之Repeater模块

Burp Repeater作为Burp Suite中一款手工验证HTTP消息的测试工具，通常用于多次重放请求 响应和手工修改请求消息的修改后对服务器端响应的消息分析。

Repeater的使用

在渗透测试过程中，我们经常使用Repeater来进行请求与响应的消息验证分析，比如修改请 求参数，验证输入的漏洞；修改请求参数，验证逻辑越权；从拦截历史记录中，捕获特征性 的请求消息进行请求重放。

Burp Repeater的操作界面如下图所示：



请求消息区为客户端发送的请求消息的详细信息，Burp Repeater为每一个请求都做了请求编 号，当我们在请求编码的数字上双击之后，可以修改请求的名字，这是为了方便多个请求消 息时，做备注或区分用的。

在编号的下方，有一个【GO】按钮，当我们对请求的消息编辑完之后，点击此按钮即发送请求给服务器端。

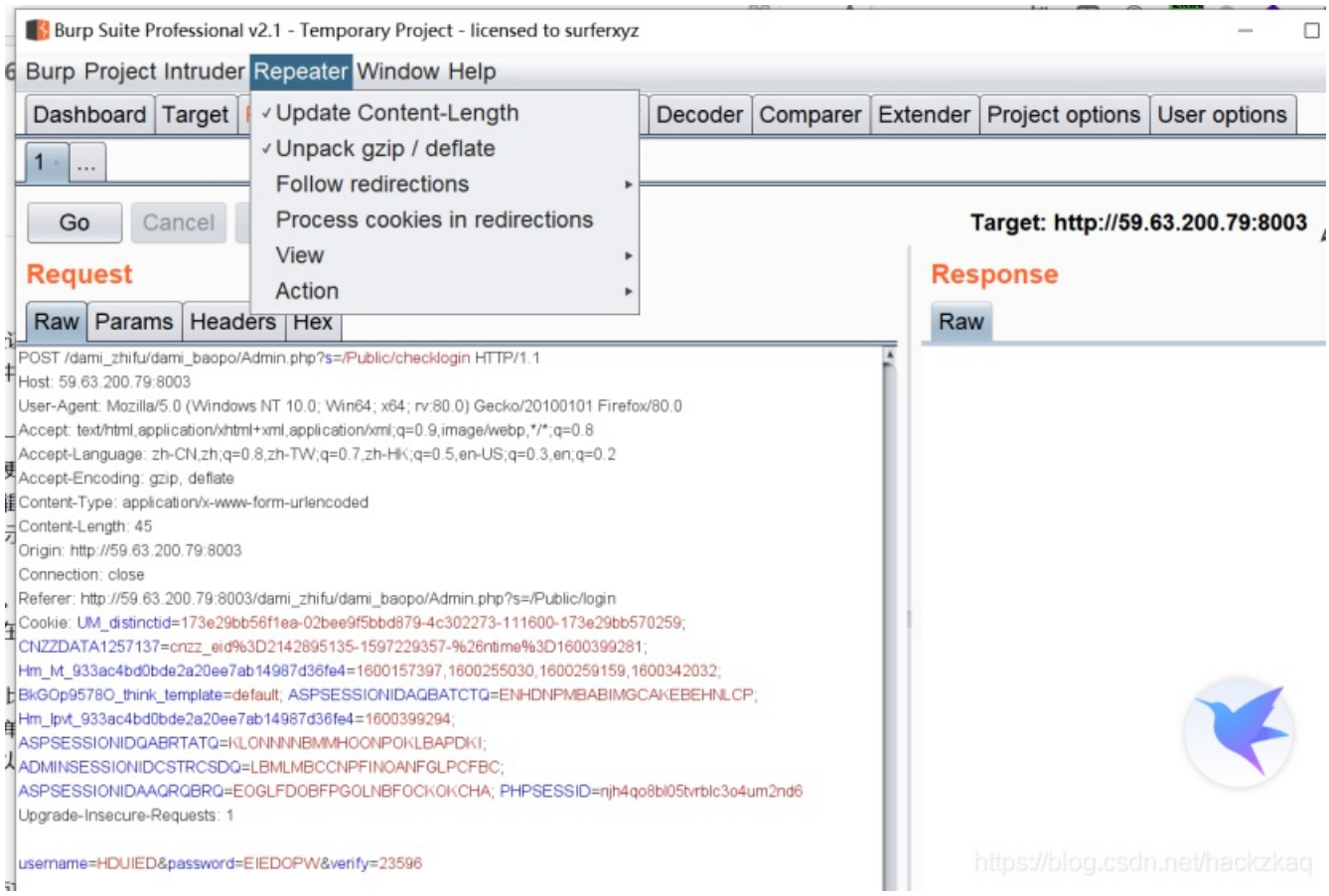
服务器的请求域可以在target处进行修改，如上图所示。

应答消息区为对应的请求消息点击【GO】按钮后，服务器端的反馈消息。通过修改请求消息的参数来比对分析每次应答消息之间的差异，能更好的帮助我们分析系统可能存在的漏洞。

在我们使用Burp Repeater时，通常会结合Burp的其他工具一起使用，比如Proxy的历史记录，Scanner的扫描记录、Target的站点地图等，通过其他工具上的右击菜单，执行【Send to Repeater】，跳转到Repeater选项卡中，然后才是对请求消息的修改以及请求重放、数据分析与漏洞验证。

可选项设置（Options）

与Burp其他工具的设置不同，Repeater的可选项设置菜单位于整个界面顶部的菜单栏中，如图所示：



可选项设置（Options）

与Burp其他工具的设置不同，Repeater的可选项设置菜单位于整个界面顶部的菜单栏中，如 图所示：
其设置主要包括以下内容：

更新Content-Length，这个选项是用于控制Burp是否自动更新请求消息头中的Content-Length。
解压和压缩（Unpack gzip / deflate ）这个选项主要用于控制Burp是否自动解压或压缩服务器端响应的内容。

跳转控制（Follow redirections） 这个选项主要用于控制Burp是否自动跟随服务器端作请 求跳转，比如服务端返回状态码为302，是否跟着应答跳转到302指向的url地址。

它有4个选项，分别是永不跳转（Never），站内跳转（On-site only ）、目标域内跳转（In- scope only）、始终跳转（Always），其中永不跳转、始终跳转比较好理解，站内跳转 是指当前的同一站点内跳转；目标域跳转是指target scope中配置的域可以跳转。

跳转中处理Cookie（Process cookies in redirections ） 这个选项如果选中，则在跳转过 程中设置的Cookie信息，将会被带到跳转指向的URL页面，可以进行提交。

视图控制（View） 这个选项是用来控制Repeater的视图布局。

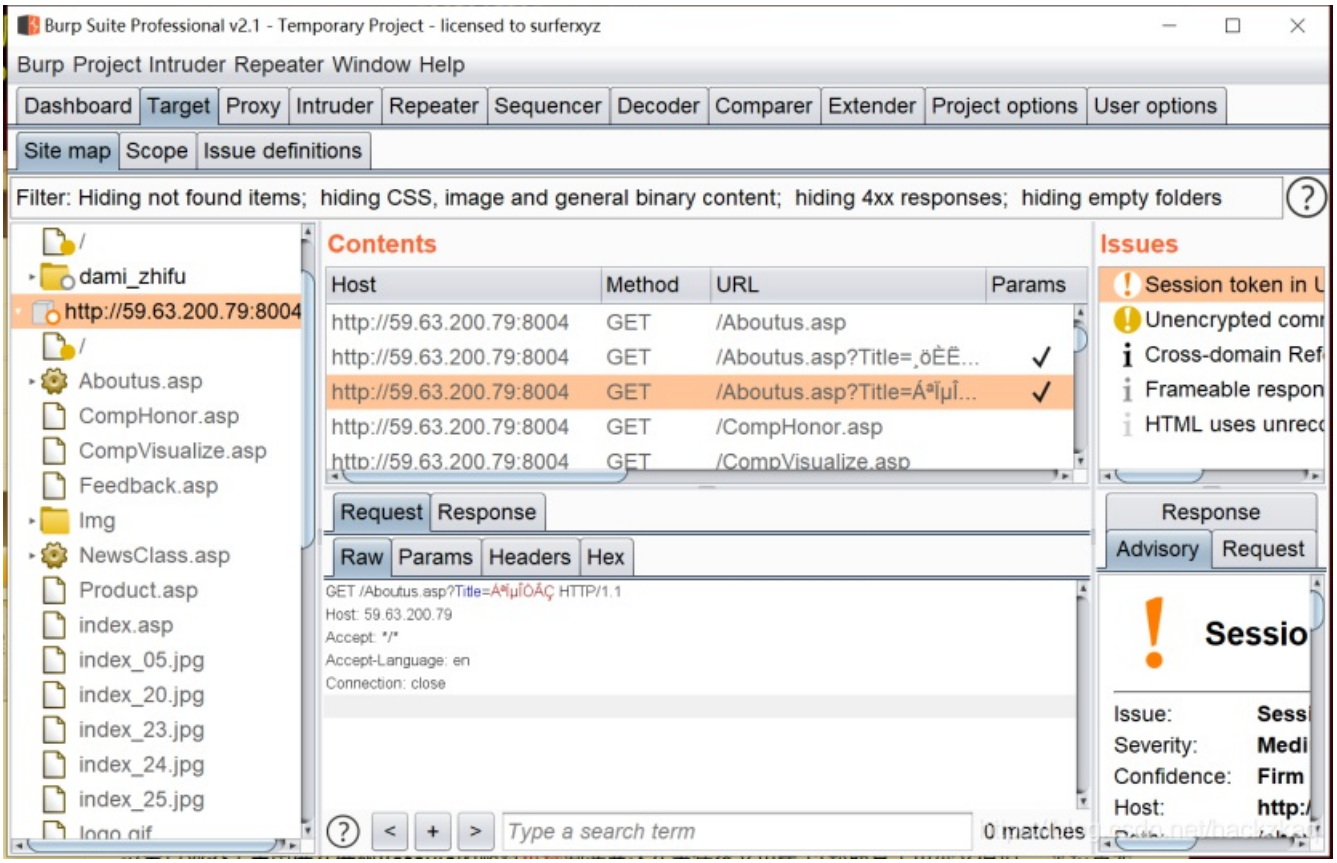
其他操作（Action） 通过子菜单方式，指向Burp的其他工具组件中。

Burp工具之Target模块

Burp Target 组件主要包含站点地图、目标域、Target工具三部分组成，他们帮助渗透测试人员更好地了解目标应用的整体状况、当前的工作涉及哪些目标域、分析可能存在的攻击面等信息。

站点地图Site Map

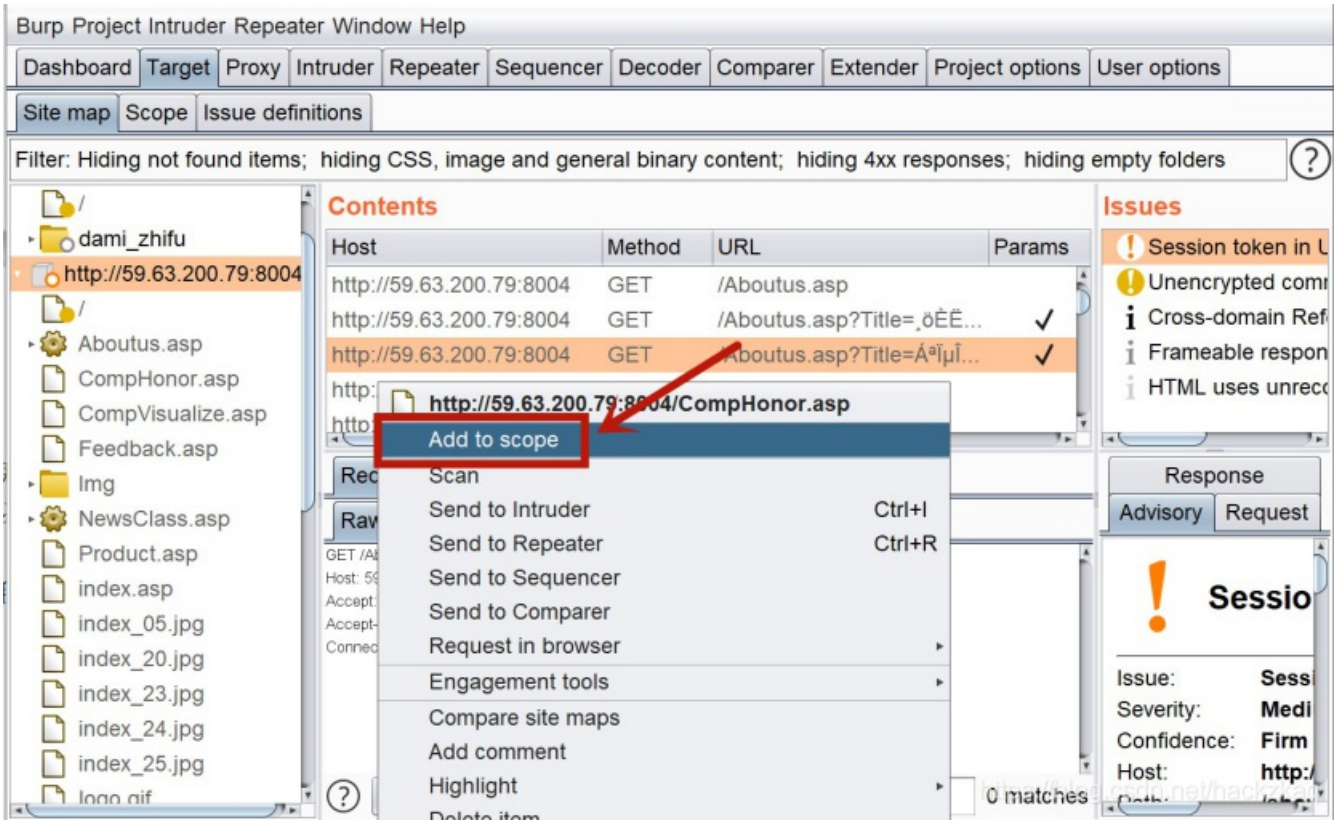
对封神台靶场进行抓包，进行渗透测试，通过浏览器浏览的历史记录在站点地图中的展现结果。



从图中我们可以看出，Site Map的左边为访问的URL，按照网站的层级和深度，树形展示整个应用系统的结构和关联其他域的url情况；

右边显示的是某一个url被访问的明细列表，共访问哪些url，请求和应答内容分别是什么，都有着详实的记录。 基于左边的树形结构，我们可以选择某个分支，对指定的路径进行扫描和抓取。

同时，我们也可以将某个域直接加入Target Scope中。



除了加入Target Scope外，从上图中我们也可以看到，对于站点地图的分层，可以通过折叠和展开操作，更好的分析站点结构。

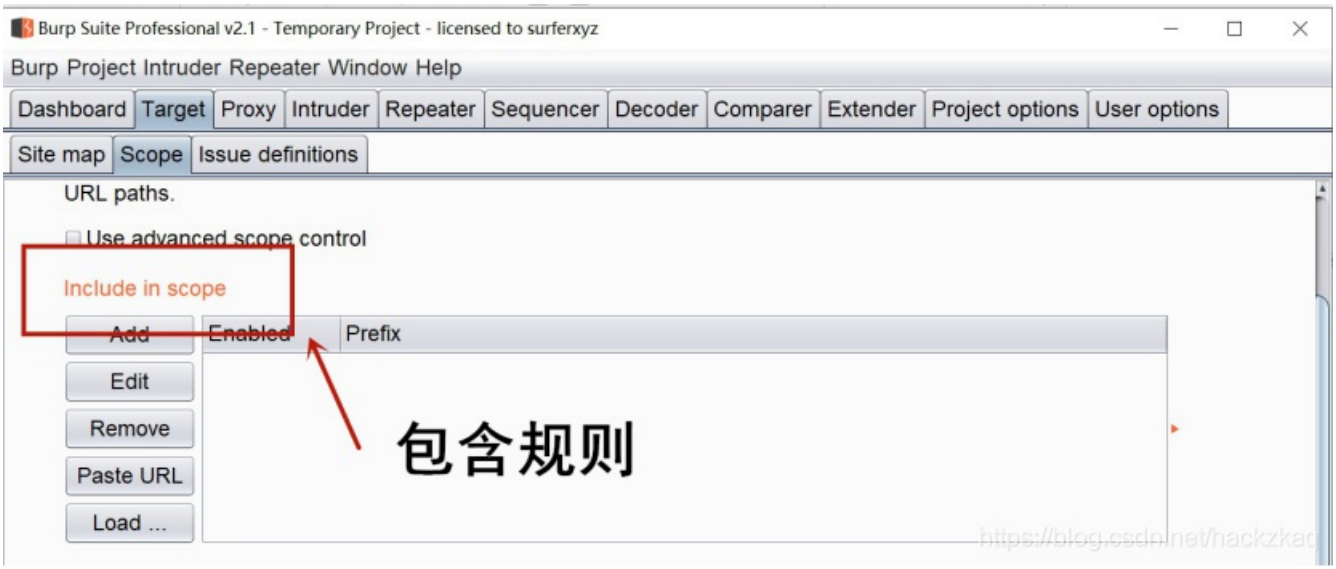
目标域设置 Target Scope

Target Scope中作用域的定义比较宽泛，通常来说，当我们对某个产品进行渗透测试时，可以通过域名或者主机名去限制拦截内容，这里域名或主机名就是我们说的作用域；

如果我们想 限制得更为细粒度化，比如，你只想拦截login目录下的所有请求，这时我们也可以在此设 置，此时，作用域就是目录。

总体来说，Target Scope主要使用于下面几种场景中：

限制站点地图和Proxy历史中的显示结果
告诉Burp Proxy 拦截哪些请求
Burp Spider抓取哪些内容
Burp Scanner自动扫描哪些作用域的安全漏洞
在Burp Intruder和Burp Repeater 中指定URL
通过Target Scope 我们能方便地控制Burp的拦截范围、操作对象，减少无效的噪音。在 Target Scope的设置中，主要包含两部分功能：允许规则和去除规则。



其中允许规则很容易理解，即包含在此规则列表中的操作允许、有效。

如果此规则用于拦截，则请求消息匹配包含规则列表中的将会被拦截；否则，请求消息匹配去除列表中的将不会被拦截。

规则主要由协议、域名或IP地址、端口、文件名4个部分组成， 这就意味着我们可以从协议、域名或IP地址、端口、文件名4个维度去控制哪些消息出现在允 许或去除在规则列表中。

当我们设置了Target Scope （默认全部为允许），使用Burp Proxy进行代理拦截，在渗透测 试中通过浏览器代理浏览应用时，Burp会自动将浏览信息记录下来，包含每一个请求和应答的详细信息，保存在Target站点地图中。

如何使用Target 工具

手工获取站点地图

当我们手工获取站点地图时，需要遵循以下操作步骤：

1.设置浏览器代理和Burp Proxy代理。
2.关闭Burp Proxy的拦截功能。
3.手工浏览网页，这时，Target会自动记录站点地图信息。

这种方式的好处在于我们可以根据自己的需 要和分析，自主地控制访问内容，记录的信息比较准确。

但缺点就是比自动抓取相比需要更长的时间进行渗透测试，对渗透人员付出的时间和精力是很大的。

站点比较

这是一个Burp提供给渗透测试人员对站点进行动态分析的利器，我们在比较帐号权限 时经常使用到它。

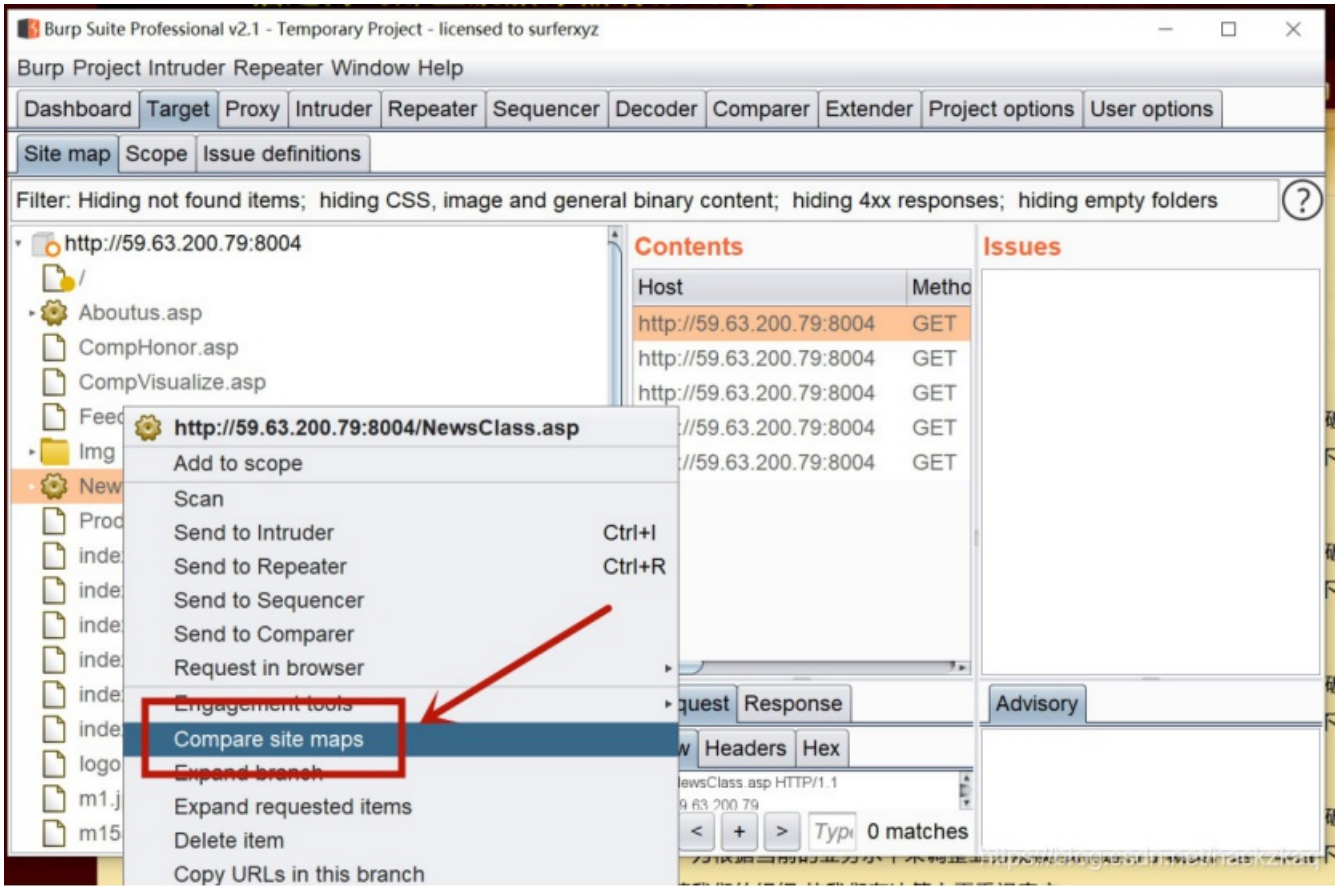
当我们登陆应用系统，使用不同的帐号，帐号本身在应用系统中被赋予了 不同的权限，那么帐号所能访问的功能模块、内容、参数等都是不尽相同的，此时使用站点比较，能很好的帮助渗透测试人员区分出来。

一般有三种场景：

同一个帐号，具有不同的权限，比较两次请求结果的差异;.
两个不同的帐号，具有不同的权限，比较两次请求结果的差异；
两个不同的帐号，具有相同的权限，比较两次请求结果的差异。

如何对站点进行比较：

1.首先我们在需要进行比较的功能链接上右击， 找到站点比较的菜单，点击菜单进入下一步。



2.由于站点比较是在两个站点地图之间进行的，所以我们在配置过程中需要分别指定Site Map 1和Site Map2。

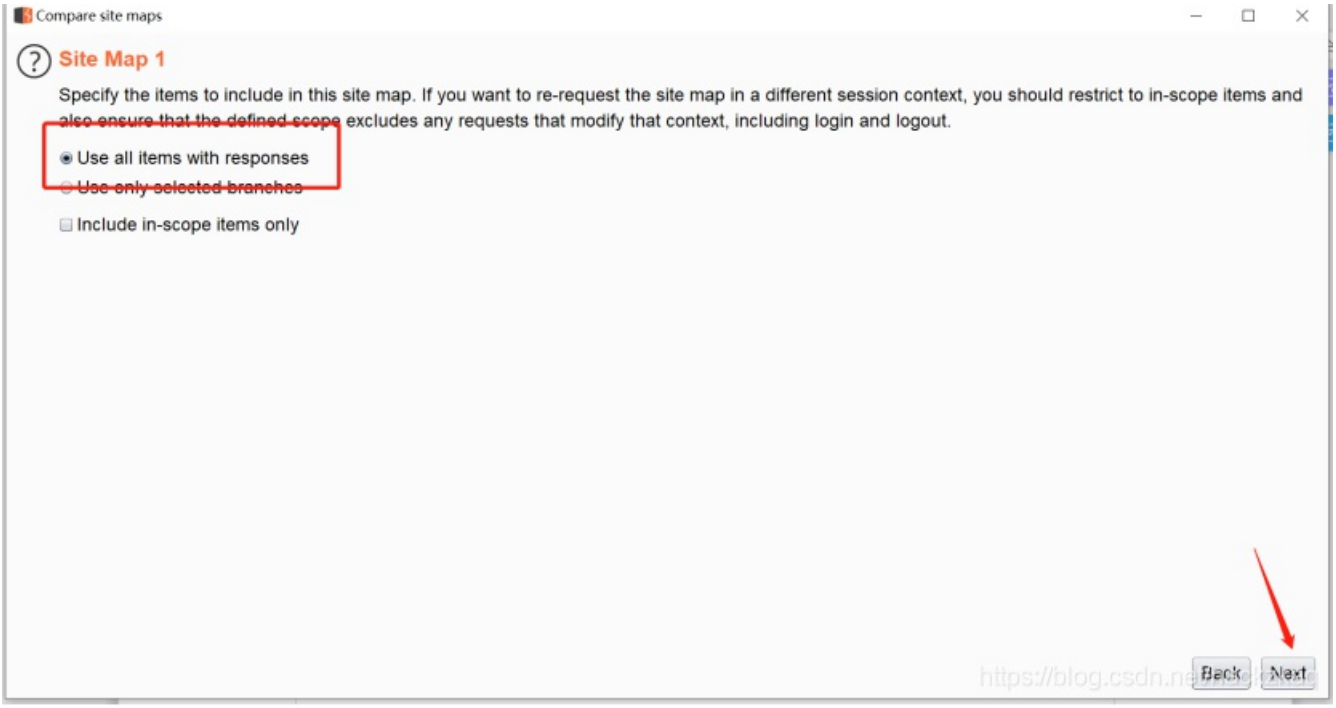
通常情况下，Site Map 1 我们默认为当前会话。

如图所示，点击【Next】。

3.这时我们会进入Site Map 1 设置页面，如果是全站点比较我们选择第一项，如果仅仅比较我们选中的功能，则选择第二项。

如下图，点击【Next】。

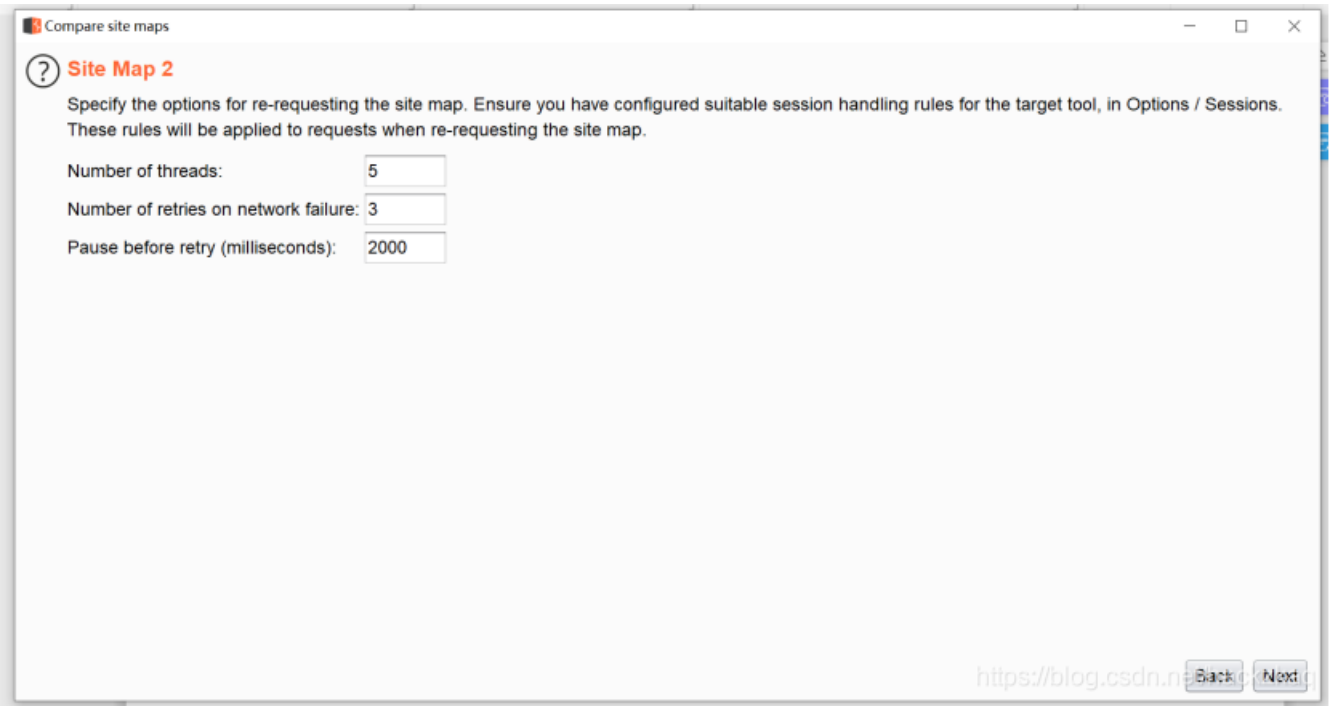
如果全站点比较，且不想加载其他域时，我们可以勾选只选择当前域。



4.接下来就是Site Map 2 的配置，对于Site Map 2我们同样有两种方式，第一种是之前我们已经保存下来的Burp Suite 站点记录，第二种是重新发生一次请求作为Site Map2.这里，我们选择第二种方式。

5.如果上一步选择了第二种方式，则进入请求消息设置界面。

在这个界面，我们需要指定通信 的并发线程数、失败重试次数、暂停的间隙时间。



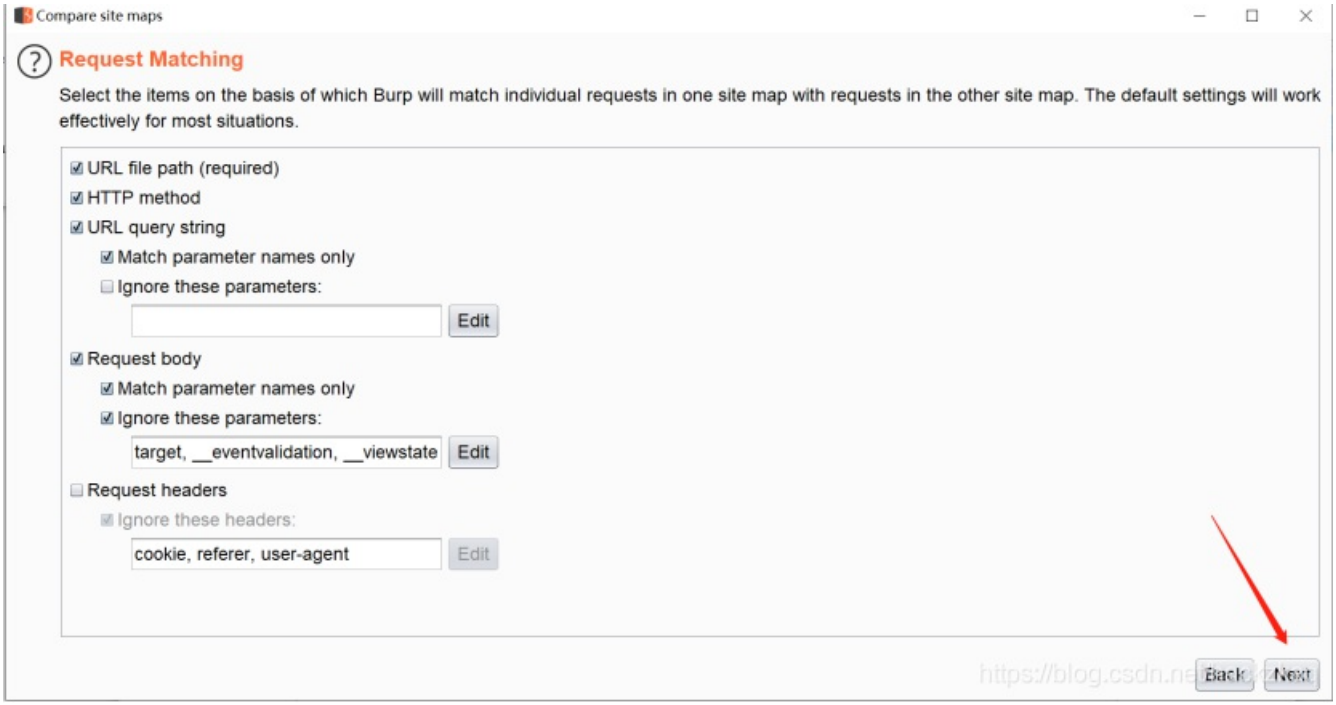
6.设置完Site Map 1 和Site Map 2之后，将进入请求消息匹配设置。

在这个界面，我们可以通过URL文件路径、Http请求方式、请求参数、请求头、请求Body来对匹配条件进行过滤。

7.设置请求匹配条件，接着进入应答比较设置界面。

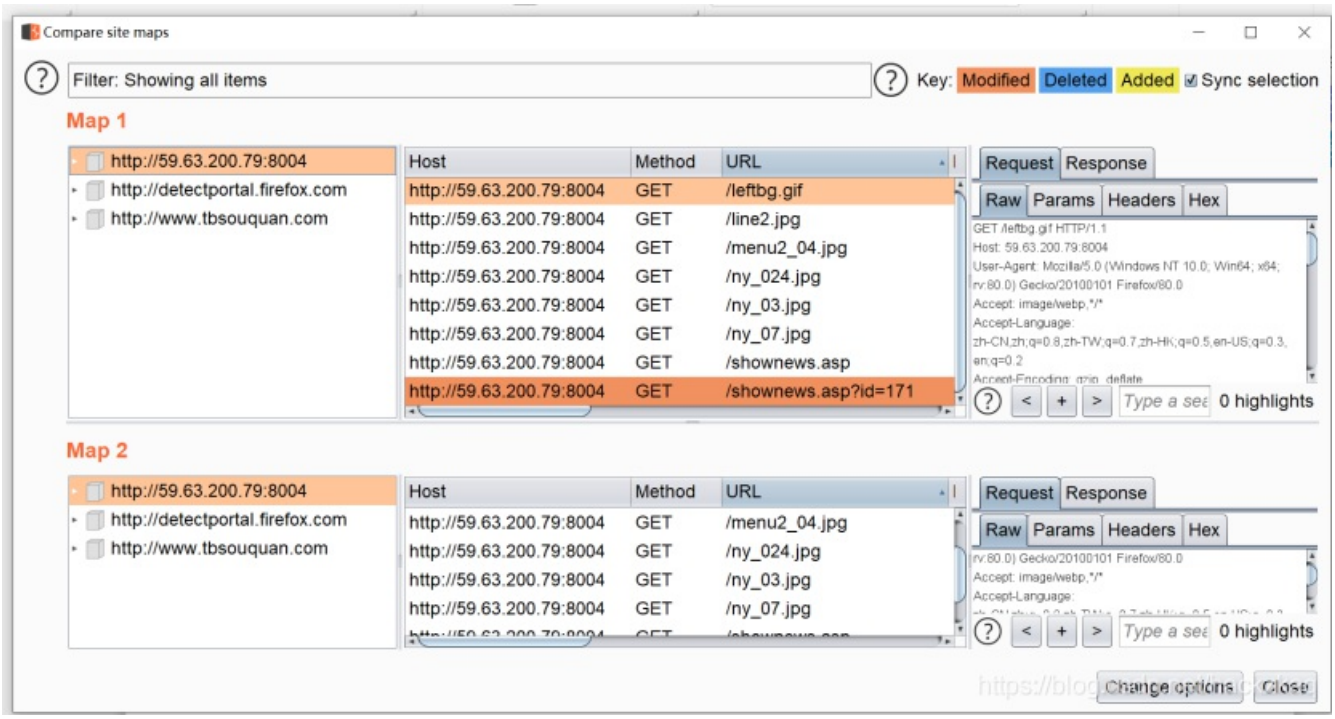
在这个界面上，我们可以设置哪些内容我们指定需要进行比较的。

从下图我们可以看出，主要有响应头、form表单域、空格、MIME 类型。点击【Next】。



8.如果我们之前是针对全站进行比较，且是选择重新发生一次作为Site Map2的方式，则界面加载过程中会不停提示你数据加载的进度，如果涉及功能请求的链接较少，则很快进入比较界面。

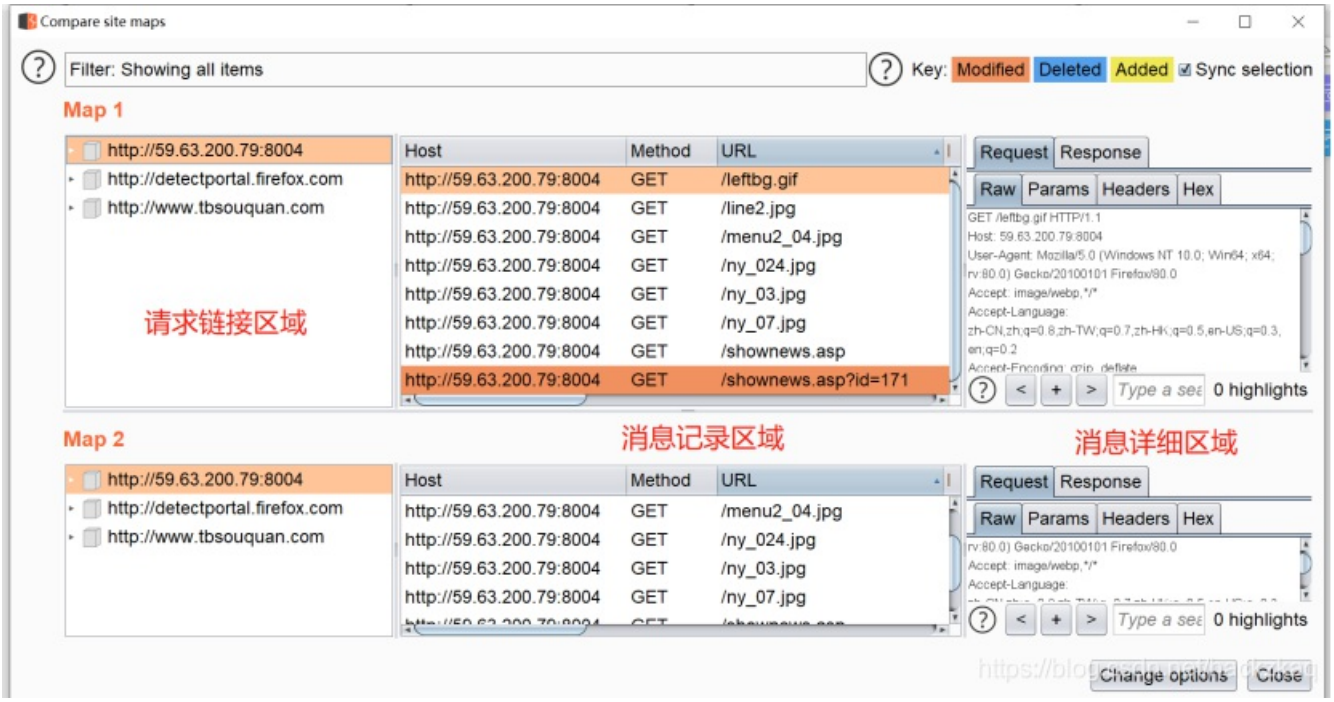
如下图。



9.从上图我们可以看到，站点比较的界面上部为筛选过滤器，下部由左、中、右三块构成。

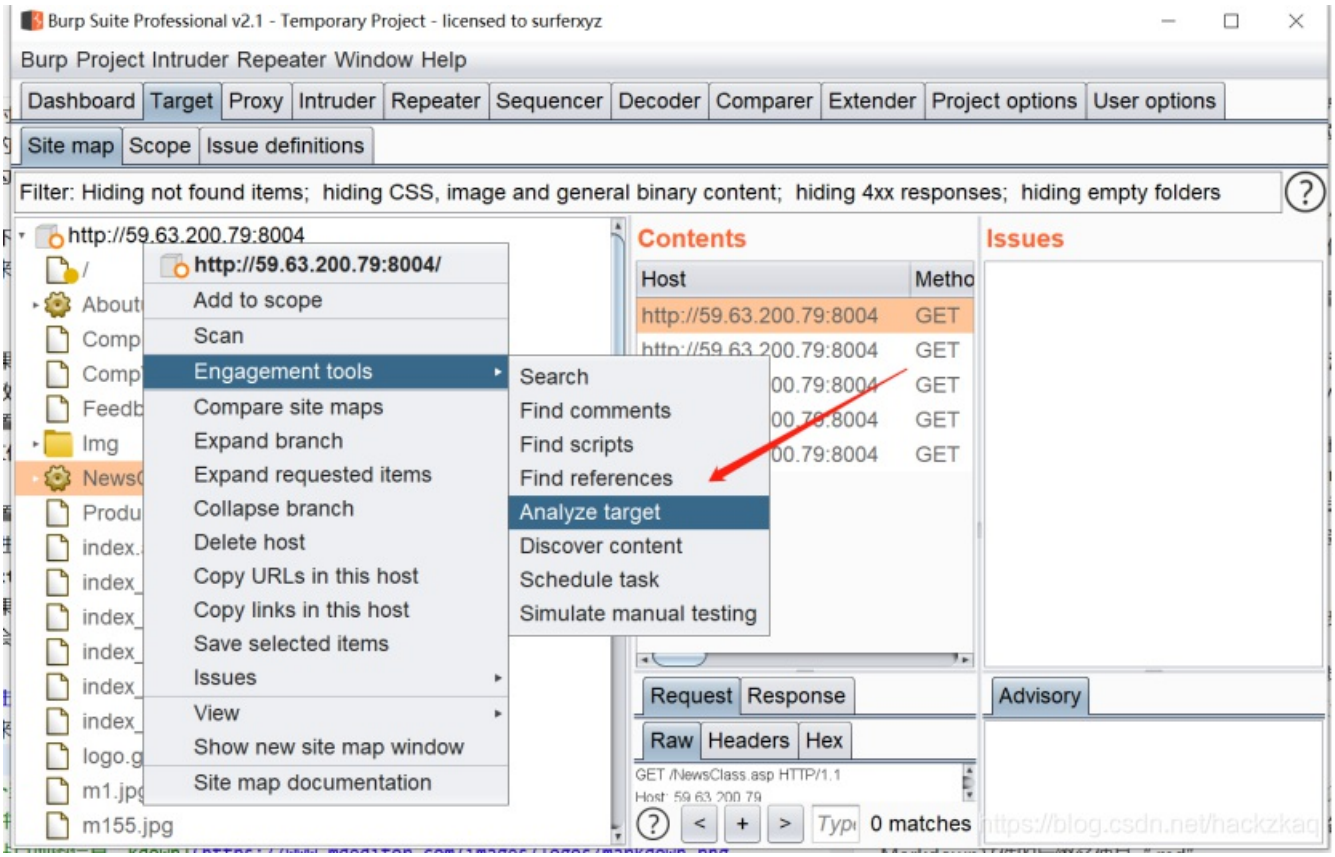
左边为请求的链接列表，中间为Site Map 1 和Site Map 2的消息记录，右边为消息详细信息。

当我们选择Site Map 1某条消息记录时，默认会自动选择Site Map 2与之对应的记录，这是有右上角的【同步选择】勾选框控制的，同时，在右边的消息详细区域，会自动展示Site Map 1与Site Map 2通信消息的差异，包含请求消息和应答消息，存在差异的地方用底色标注出来。

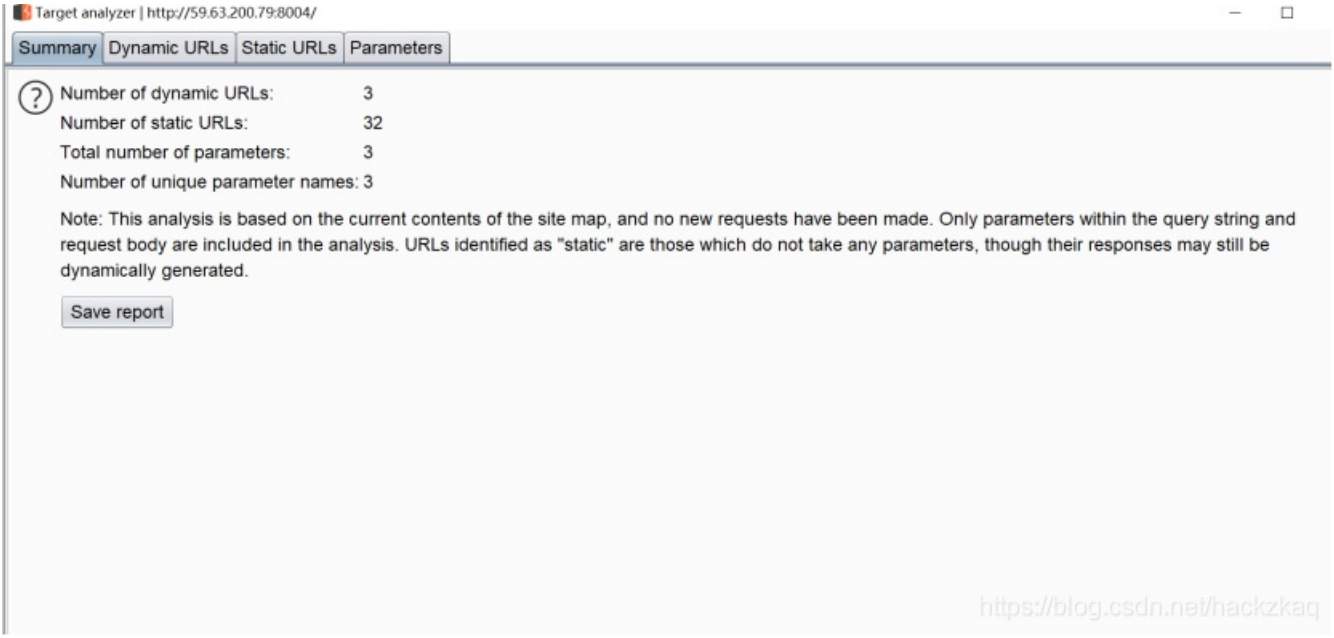


攻击面分析

我们来看一下Analyze Target的使用：1.首先，我们通过站点地图，打开 Analyze Target。

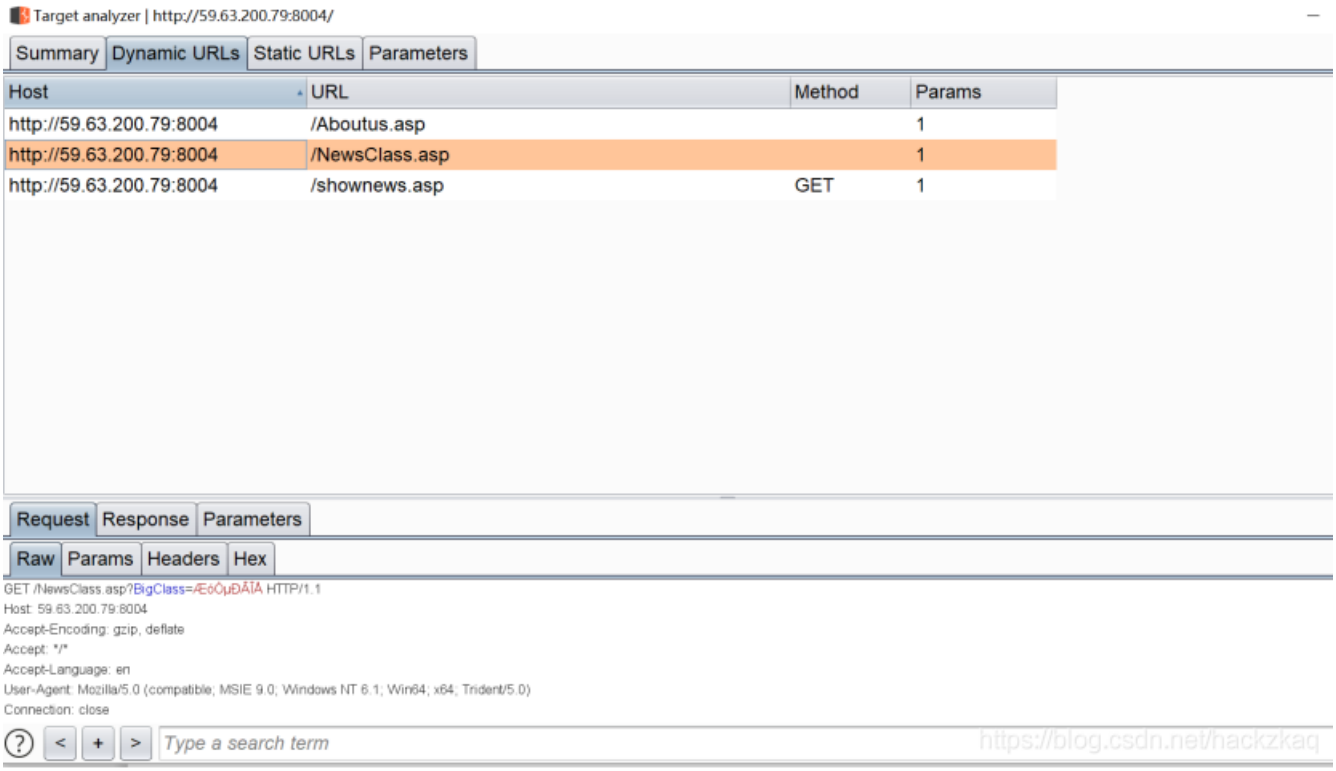


2.在弹出的分析界面中，我们能看到概况、动态URL、静态URL、参数4个视图。



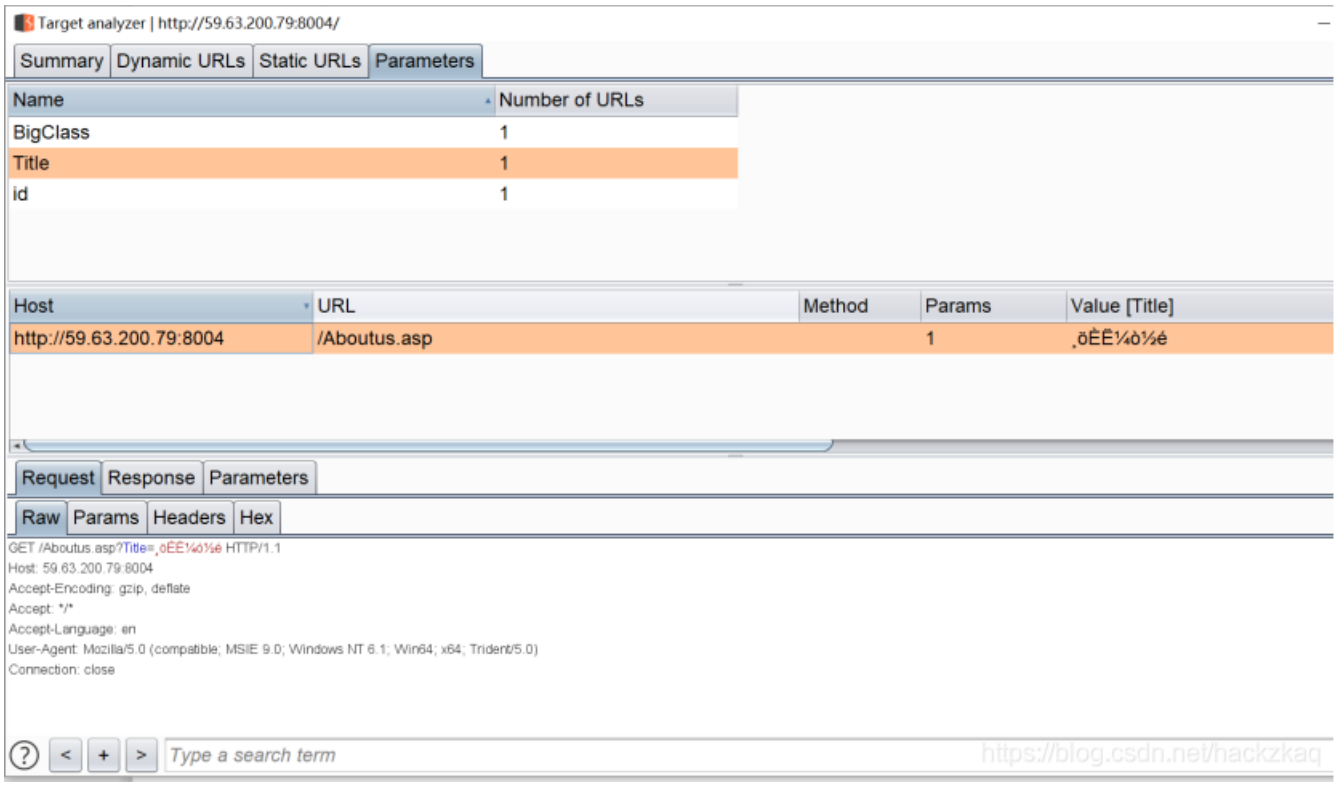
3.概况视图主要展示当前站点动态URL数量、静态URL数量、参数的总数、唯一的参数名数目，通过这些信息，我们对当前站点的总体状况有粗线条的了解。

4.动态URL视图展示所有动态的URL请求和应答消息，跟其他的工具类似，当你选中某一条消息时，下方会显示此消息的详细信息。



5.静态和动态的URL视图是类似的。

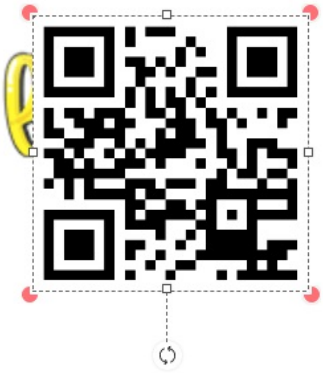
6.参数视图有上中下三部分组成，上部为参数和参数计数统计区，你可以通过参数使用的次数进行排序，对使用频繁的参数进行分析；中部为参数对于的使用情况列表，记录对于的参数每一次的使用记录；下部为某一次使用过程中，请求消息和应答消息的详细信息。



在使用攻击面分析功能时，需要注意，此功能主要是针对站点地图中的请求URL进行分析，如果某些URL没有记录，则不会被分析到。同时，在实际使用中，存在很点站点使用伪静态，如果请求的URL中不带有参数，则分析时无法区别，只能当做静态URL来分析。

黑客教程视频.工具.靶场.进群

限时扫码领取。



黑客