

burpsuite 之 Target

1、Target 功能

目标工具包含了 SiteMap，用你的目标应用程序的详细信息。它可以让你定义哪些对象在范围上为你目前的工作，也可以让你手动测试漏洞的过程，Target 分为 site map 和 scope 两个选项卡。

选项一、Site Map

SiteMap 会在目标中以树形和表形式显示，并且还可以查看完整的请求和响应。树视图包含内容的分层表示，随着细分为地址，目录，文件和参数化请求的 URL。您还可以扩大有趣的分支才能看到进一步的细节。如果您选择树的一个或多个部分，在所有子分支所选择的项目和项目都显示在表视图。

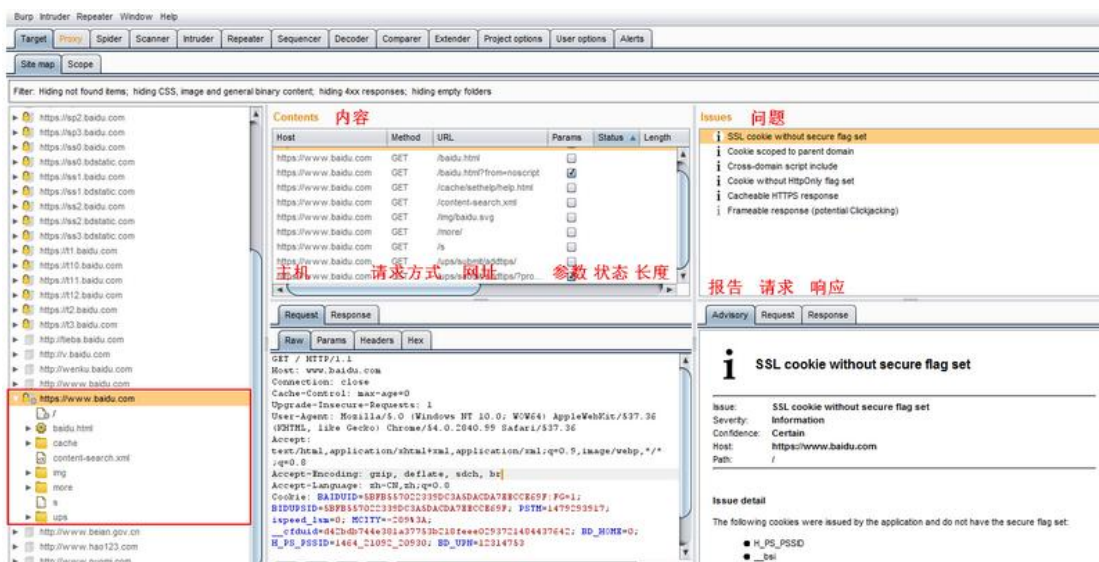
该表视图显示有关每个项目（URL，HTTP 状态代码，网页标题等）的关键细节。您可以根据任意列进行排序表（单击列标题来循环升序排序，降序排序，和未排序）。如果您在表中选择一个项目，请求和响应（如适用）该项目显示在请求/响应窗格。这包含了请求和响应的 HTTP 报文的编辑器，提供每封邮件的详细分析。

站点地图汇总所有的信息 BurpSuite 已经收集到的有关申请。这包括：所有这一切都通过代理服务器直接请求的资源。

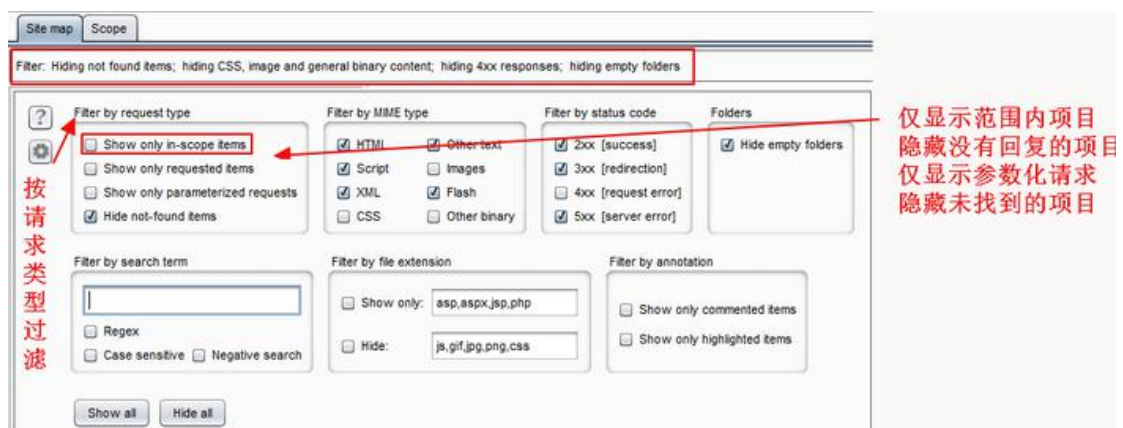
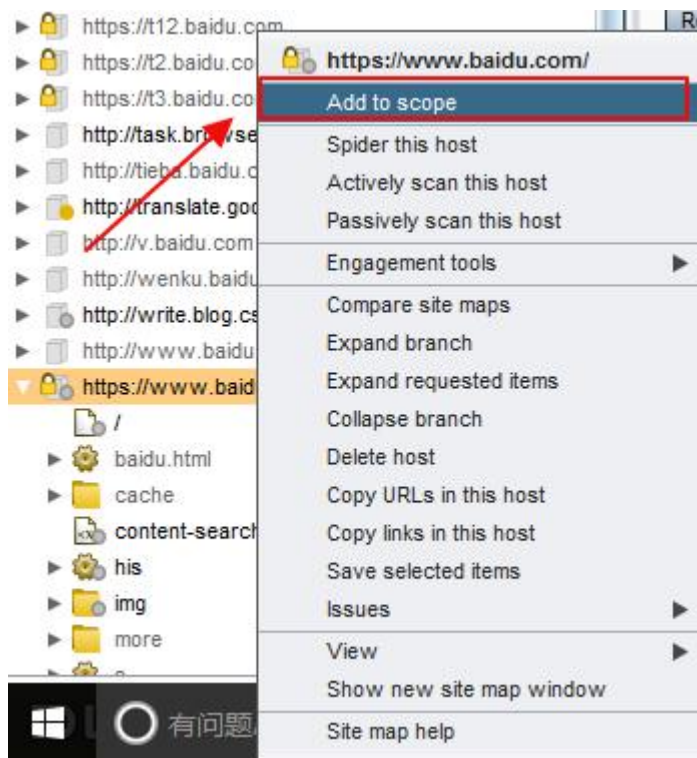
已推断出通过分析响应代理请求的任何物品（前提是你没有禁用被动 Spider）。

内容使用 Spider 或内容发现功能查找。

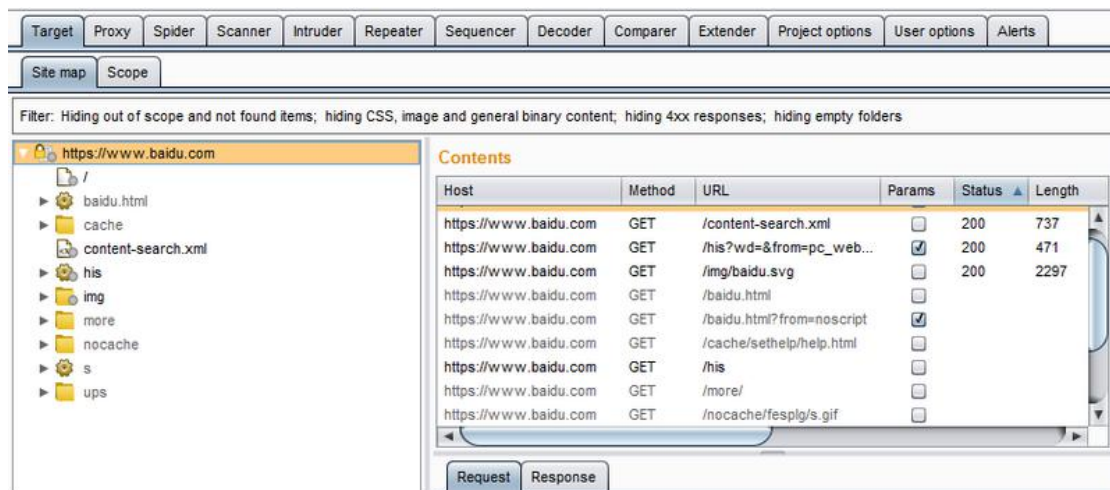
由用户手动添加的任何项目，从其它工具的输出。



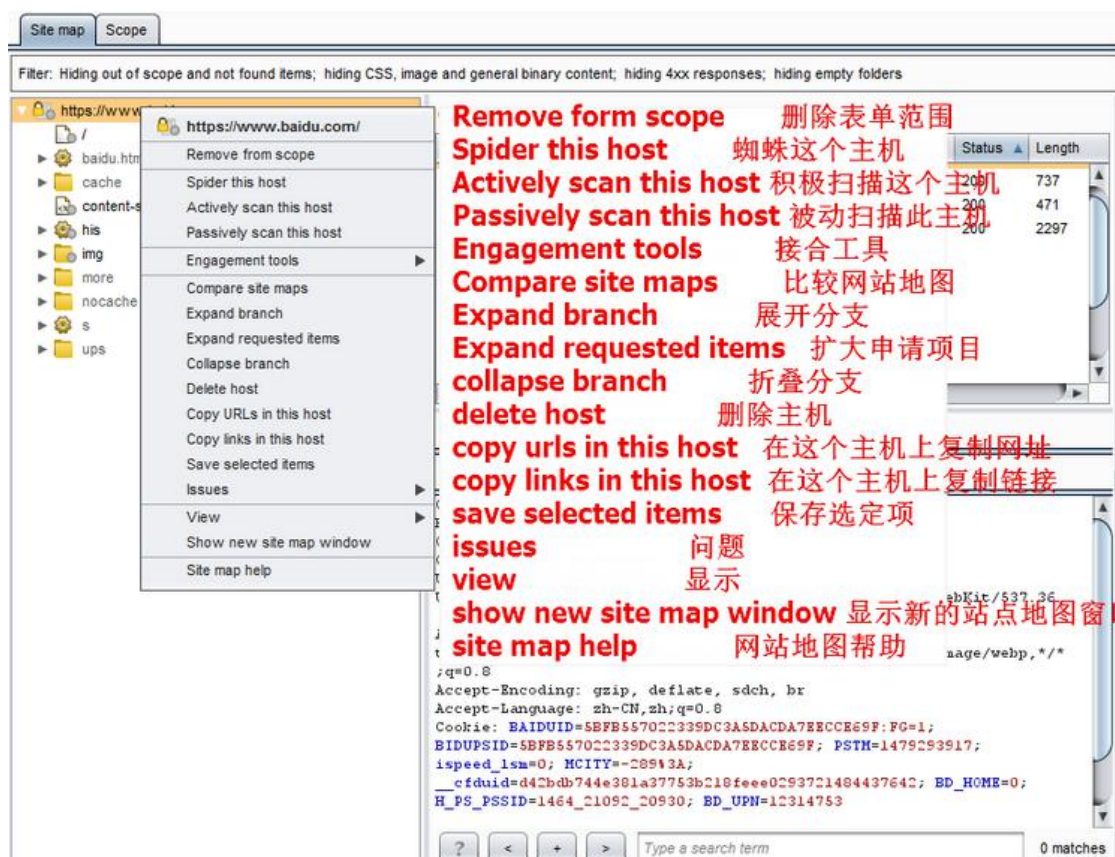
这样看起来 site map 是不是很乱, 则可以右击 add to scope, 然后点击 Filter 勾选 Show only in-scope items, 此时你再回头看 Site map 就只有百度一个地址了, 这里 filter 可以过滤一些参数, show all 显示全部, hide 隐藏所有, 如果勾选了表示不过滤



选择之后就只剩下一个网址了

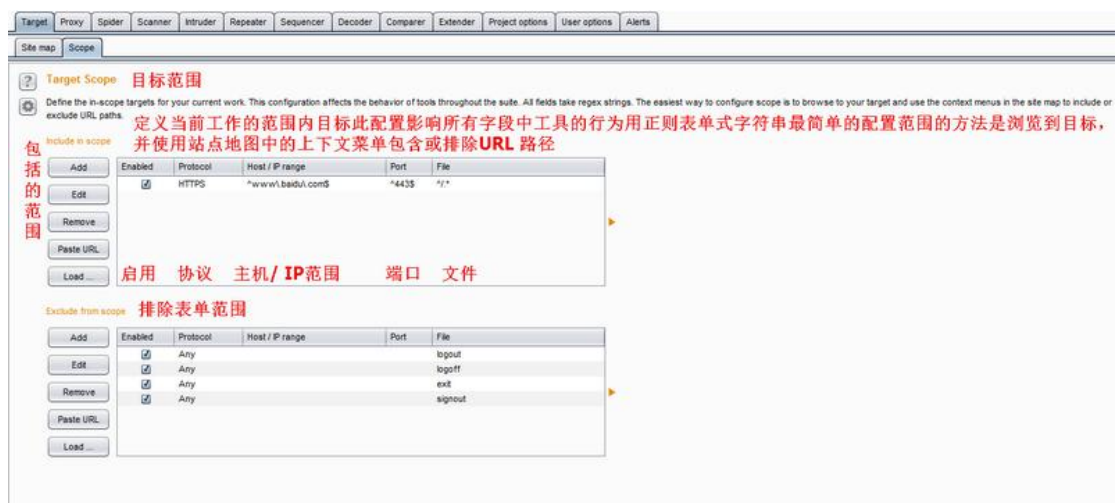


针对地址右击显示当前可以做的一些动作操作等功能。



选项二、Scope

这个主要是配合 Site map 做一些过滤的功能



已请求在 SiteMap 中的项目会显示为黑色。尚未被请求的项目显示为灰色

