burpsuite 之 Spider

1、简介

Burp Spider 是一个映射 web 应用程序的工具。它使用多种智能技术对一个应用程序的内容和功能进行全面的清查。

Burp Spider 通过跟踪 HTML 和 JavaScript 以及提交的表单中的超链接来映射目标应用程序，它还使用了一些其他的线索，如目录列表，资源类型的注释，以及 robots.txt 文件。结果会在站点地图中以树和表的形式显示出来，提供了一个清楚并非常详细的目标应用程序视图。

Burp Spider 能使你清楚地了解到一个 web 应用程序是怎样工作的，让你避免进行大量的手动任务而浪费时间，在跟踪链接，提交表单，精简 HTNL 源代码。可以快速地确人应用程序的潜在的脆弱功能，还允许你指定特定的漏洞，如 SQL 注入，路径遍历。

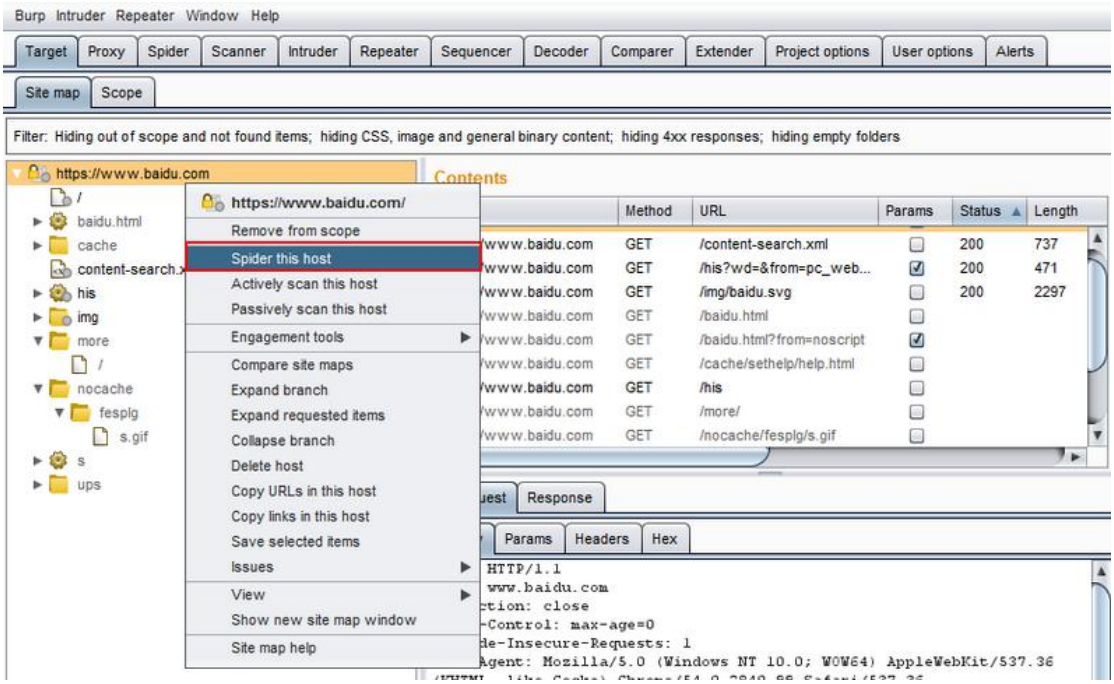
2、模块介绍

要对应用程序使用 Burp Spider 需要两个简单的步骤：

1.使用 Burp Proxy 配置为你浏览器的代理服务器，浏览目标应用程序(为了节省时间，你可以关闭代理拦截)。

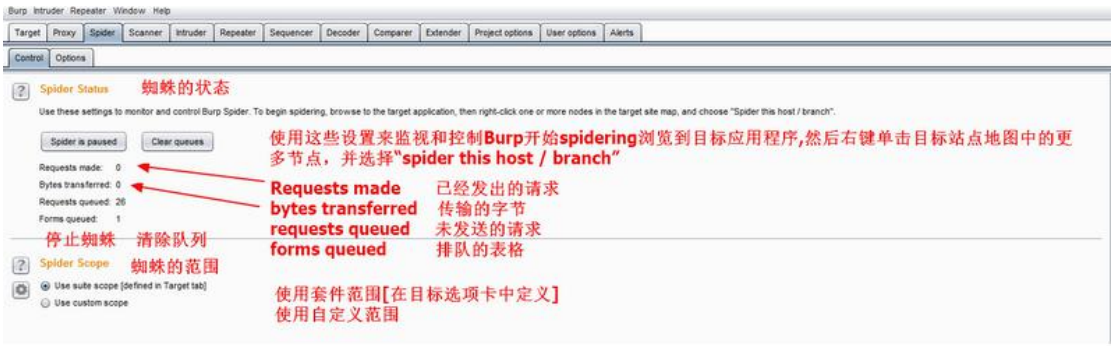
2.到站点地图的"arget"选项上，选中目标应用程序驻留的主机和目录。选择上下文菜单的"

spider this host/branc"选项。



选项一、Contro

用来开始和停止 Burp Spider，监视它的进度，以及定义 spidering 的范围。



选项二、Options

这个选项里包含了许多控制 Burp Spider 动作的选项。

1： Crawler Settings

- check robots.txt：检测 robot.txt 文件。选择后 Burp Spider 会要求和处理 robots.txt 文件，提取内容链接。

- Detect custom "not found" responese：检测自定义的'not found'响应。打开后 Burp Spider 会从每个域请求不存在的资源，编制指纹与诊断“not found”响应其它请求检测自定义“not found”的响应。

- ignore links to non-text content：忽略非文本内容的连接。这个选项被选中，Spider 不会请求非文本资源。使用这个选项，会减少 spidering 时间。

- request the root of all directories：请求所有的根目录。如果这个选项被选中，Burp Spider 会请求所有已确认的目标范围内的 web 目录，如果在这个目标站点存在目录遍历， 这选项将是非常的有用。

- make a non-parameterized request to each dynamic page：对每个动态页面进行非参数化的请求。如果这个选项被选中，Burp Spider 会对在范围内的所有

执行动作的 URL 进行无参数的 GET 请求。如果期待的参数没有被接收， 动态页面会有不同的响应，这个选项就能成功地探测出额外的站点内容和功能。

- Maximum link depth：这是 Burp Suite 在种子 URL 里的浏览”hops”的最大数。0 表示让 Burp Suite 只请求种子 URL。如果指定的数值非常大，将会对范围内的链接进行无限期的有效跟踪。将此选项设置为一个合理的数字可以帮助防止循环 Spider 在某些种类的动态生成的内容。

- Maximum parameterized requests per URL：请求该蜘蛛用不同的参数相同的基本 URL 的最大数目。将此选项设置为一个合理的数字可以帮助避免爬行“无限”的内容。

2： Passive Spidering

- Passively spider as you browse:如果这个选项被选中，Burp Suite 会被动地处理所有通过 Burp Proxy 的 HTTP 请求，来确认访问页面上的链接和表格。使用这个选项能让 Burp Spider 建立一个包含应用程序内容的详细画面，甚至此时你仅仅使用浏览器浏览了内容的一个子集，因为所有被访问内容链接到内容都会自动地添加到 Suite 的站点地图上。

- link depth to associate with proxy requests:这个选项控制着与通过 Burp Proxy 访问的 web 页面 有关的” link depth” 。为了防止 Burp Spider 跟踪

这个页面里的所有链接，要设置一个比上面 选项卡里的" maximum link depth" 值还高的一个值。

3： Form Submission

- individuate forms：个性化的形式。这个选项是配置个性化的标准(执行 URL，方法，区域，值)。当 Burp Spider 处理这些表格时，它会检查这些标准以确认表格是否是新的。旧的表格不会加入到提交序列。

- Don' t submit：开启后蜘蛛不会提交任何表单。

- prompt for guidance：提醒向导。如果被选中，在你提交每一个确认的表单前，Burp Suite 都会为你指示引导。这允许你根据需要在输入域中填写自定义的数据，以及选项提交到服务器的哪一个区域。

- automatically submit：自动提交。如果选中，Burp Spider 通过使用定义的规则来填写输入域的文本值来自动地提交范围内的表单。每一条规则让你指定一个简单的文本或者正则表达式来匹配表单字段名，并提交那些表单名匹配的字段值。

- set unmatched fields to：设置不匹配的字段。

4： application login

- don't submit login forms：不提交登录表单。开启后 burp 不会提交登录表单。
- prompt for guidance：提示向导。Burp 能交互地为你提示引导。默认设置项。
- handle as ordinary forms：以一般形式处理。Burp 通过你配置的信息和自动填充规则，用处理其他表单的方式来处理登陆表单。
- automatically submit these credentials：自动提交自定义的数据。开启后 burp 遇到登录表单会按照设定的值进行提交。

5： Spider Engine

- Number of threads - 设置请求线程。控制并发请求数。

- Number of retries on network failure - 如果出现连接错误或其他网络问题，Burp 会放弃和移动之前重试的请求指定的次数。测试时间歇性网络故障是常见的，所以最好是在发生故障时重试该请求了好几次。

- Pause before retry - 当重试失败的请求，Burp 会等待指定的时间（以毫秒为单位）以下，然后重试失败。如果服务器宕机，繁忙，或间歇性的问题发生，最好是等待很短的时间，然后重试。

- Throttle between requests：在每次请求之前等待一个指定的延迟（以毫秒为单位）。此选项很有用，以避免超载应用程序，或者是更隐蔽。

- Add random variations to throttle：添加随机的变化到请求中。增加隐蔽性。

6： Request Headers

您可以配置头蜘蛛在请求中使用的自定义列表。这可能是有用的，以满足各个应用程序的特定要求 - 例如，测试设计用于移动设备的应用程序时，以模拟预期的用户代理。

- Use HTTP version 1.1 ：在蜘蛛请求中使用 HTTP/1.1，不选中则使用 HTTP/1.0.
- Use Referer header：当从一个页面访问另一个页面是加入 Referer 头，这将更加相似与浏览器访问。