

Web 系统测试

4.10 渗透测试—Burp Target的使用

目 录

➤Burp Target 简介

➤Burp Target使用

- Burp Target 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

➤Burp Target的三个组成部分

- 目标域设置 Target Scope
- 站点地图 Site Map
- Target 工具的使用

➤ 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

- Target Scope 我们能方便地控制Burp 的拦截范围、操作对象，减少无效的请求
 - 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

Target Scope设置

Site map

Scope

?

Target Scope

↺

Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite. All fields take regex strings. The easiest way to exclude URL paths.

Include in scope

Add

Edit

Remove

Paste URL

Load ...

Enabled	Protocol	Host / IP range	Port	File
---------	----------	-----------------	------	------

包含规则

Exclude from scope

Add

Edit

Remove

Paste URL

Load ...

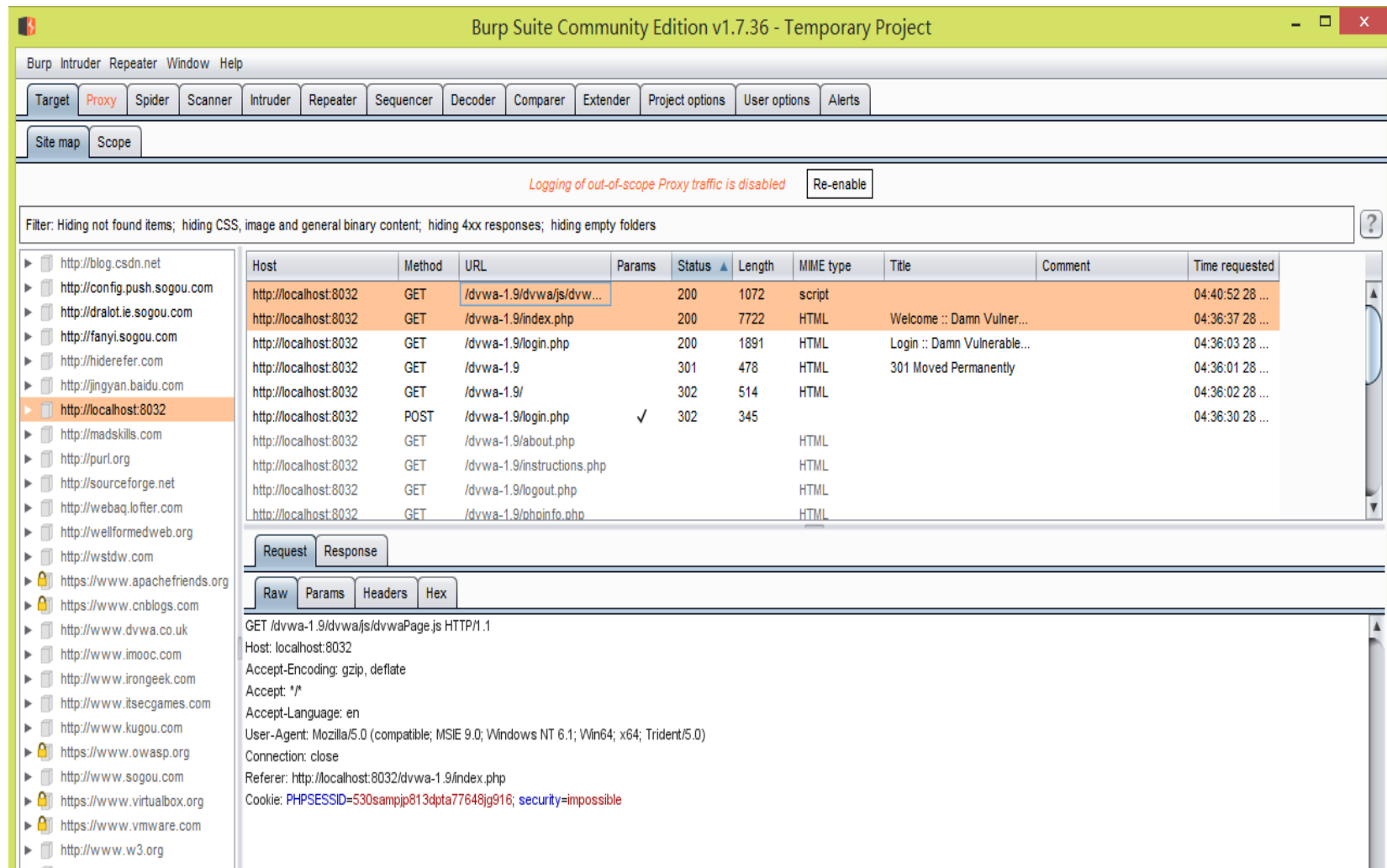
Enabled	Protocol	Host / IP range	Port	File
---------	----------	-----------------	------	------

去除规则

➤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

站点地图 Site Map

➤ 左边为访问的URL，
右边显示的是某一个
URL被访问的明细列
表，请求和应答内容
分别是什么



The screenshot shows the Burp Suite Community Edition v1.7.36 interface. The 'Site map' tab is selected, displaying a list of visited URLs on the left and a table of HTTP history on the right.

Site Map (Left Panel):

- http://blog.csdn.net
- http://config.push.sogou.com
- http://dralot.ie.sogou.com
- http://fanyi.sogou.com
- http://hiderefer.com
- http://jingyan.baidu.com
- http://localhost:8032**
- http://madskills.com
- http://purl.org
- http://sourceforge.net
- http://webqa.lofter.com
- http://wellformedweb.org
- http://wstdw.com
- https://www.apachefriends.org
- https://www.cnblogs.com
- http://www.dvwa.co.uk
- http://www.imooc.com
- http://www.irongeek.com
- http://www.itsecgames.com
- http://www.kugou.com
- https://www.owasp.org
- http://www.sogou.com
- https://www.virtualbox.org
- https://www.vmware.com
- http://www.w3.org

HTTP History Table (Right Panel):

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requested
http://localhost:8032	GET	/dvwa-1.9/dvwa/js/dvwa...		200	1072	script			04:40:52 28 ...
http://localhost:8032	GET	/dvwa-1.9/index.php		200	7722	HTML	Welcome :: Damn Vulner...		04:36:37 28 ...
http://localhost:8032	GET	/dvwa-1.9/login.php		200	1891	HTML	Login :: Damn Vulnerable...		04:36:03 28 ...
http://localhost:8032	GET	/dvwa-1.9		301	478	HTML	301 Moved Permanently		04:36:01 28 ...
http://localhost:8032	GET	/dvwa-1.9/		302	514	HTML			04:36:02 28 ...
http://localhost:8032	POST	/dvwa-1.9/login.php	✓	302	345				04:36:30 28 ...
http://localhost:8032	GET	/dvwa-1.9/about.php				HTML			
http://localhost:8032	GET	/dvwa-1.9/instructions.php				HTML			
http://localhost:8032	GET	/dvwa-1.9/logout.php				HTML			
http://localhost:8032	GET	/dvwa-1.9/phpinfo.php				HTML			

Request/Response Details (Bottom Panel):

Request: GET /dvwa-1.9/dvwa/js/dvwaPage.js HTTP/1.1

Host: localhost:8032

Accept-Encoding: gzip, deflate

Accept: */*

Accept-Language: en

User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)

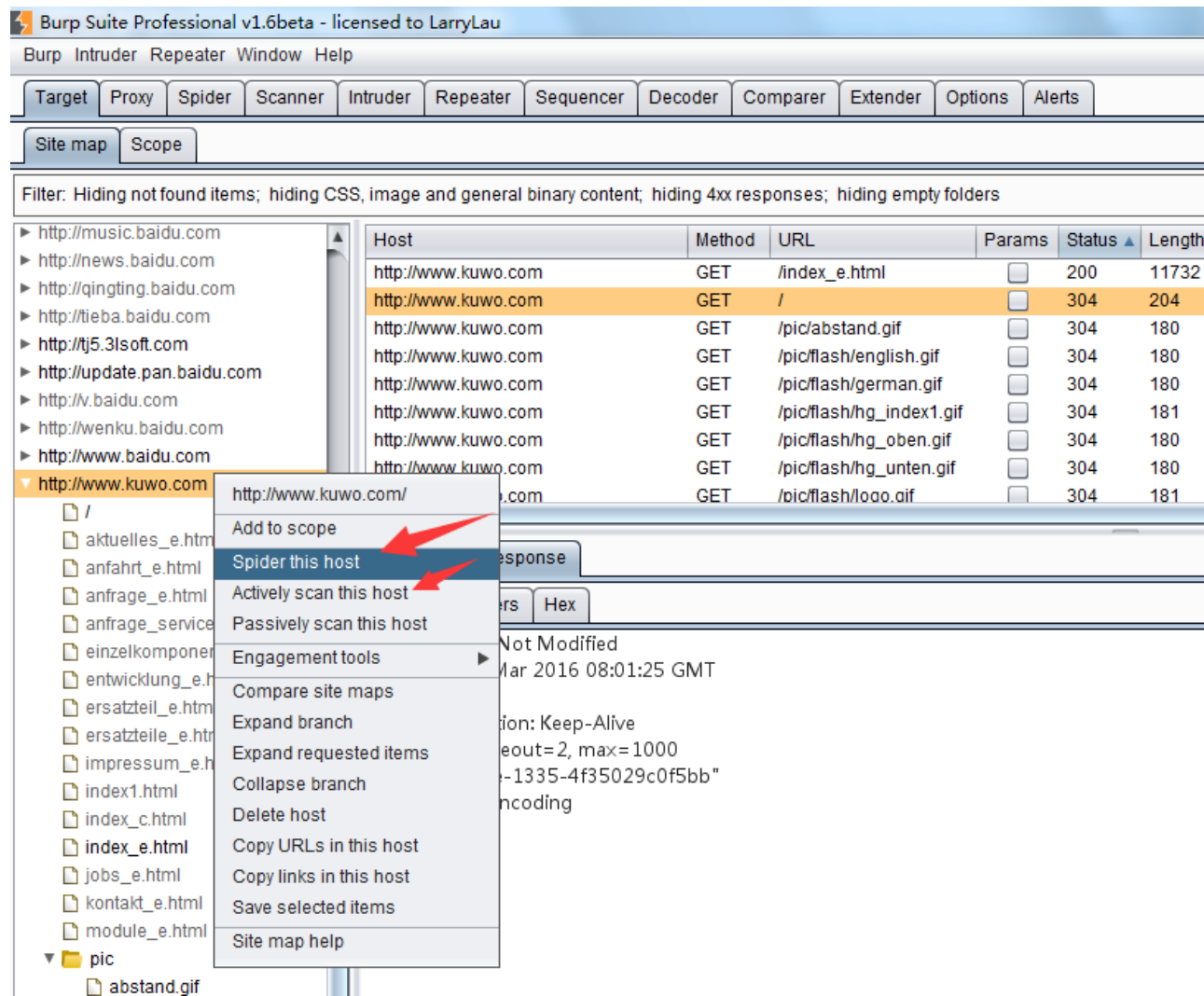
Connection: close

Referer: http://localhost:8032/dvwa-1.9/index.php

Cookie: PHPSESSID=530sompj813dpta77648jg916; security=impossible

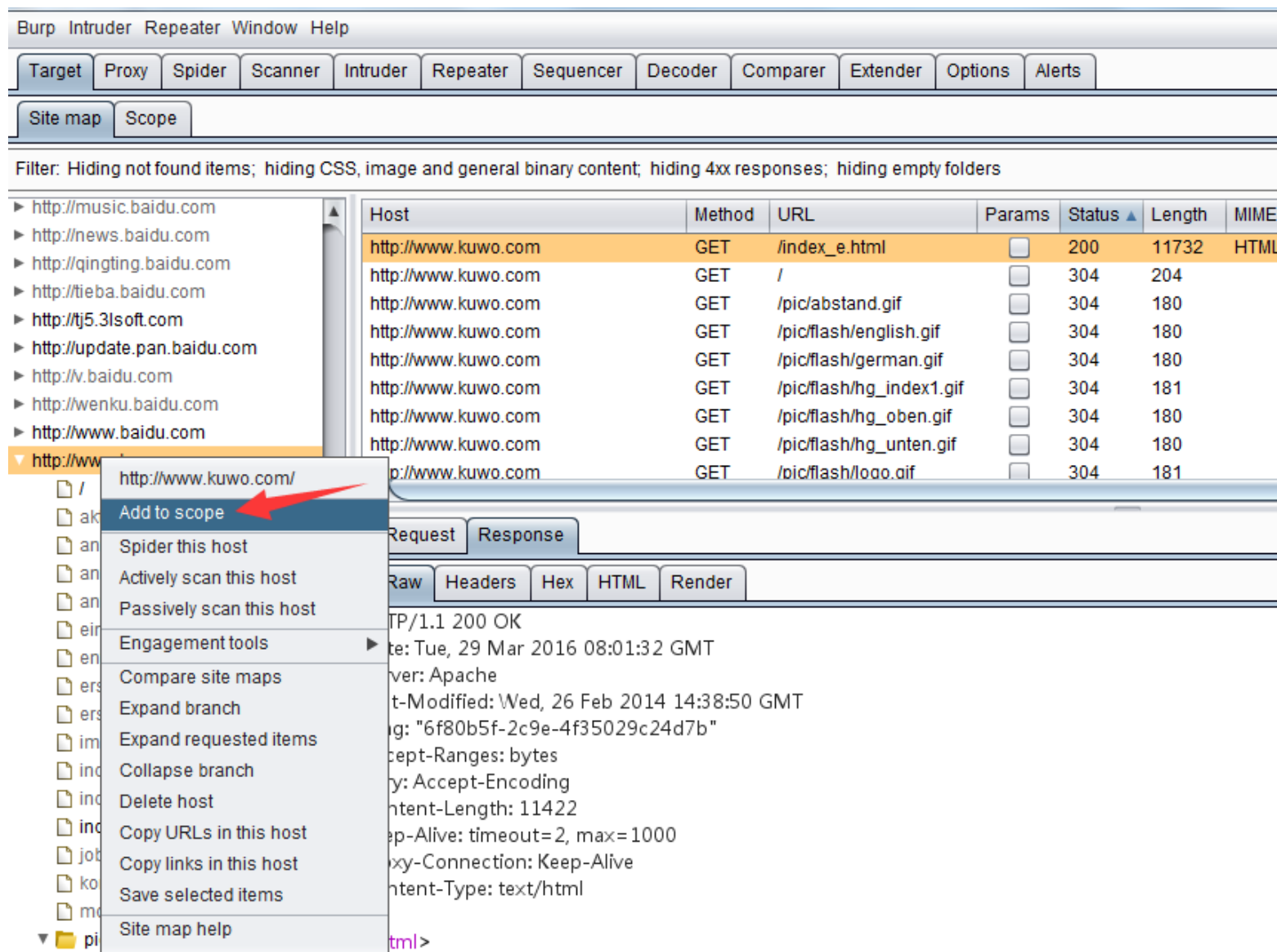
站点地图 Site Map

➤ 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



站点地图 Site Map

➤ 也可以将某个域
直接加入 Target
Scope 中



➤Target 工具的使用的使用主要包括以下部分：

- 手工获取站点地图
- 站点比较
- 攻击面分析

➤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，并使之能正常工作
- 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

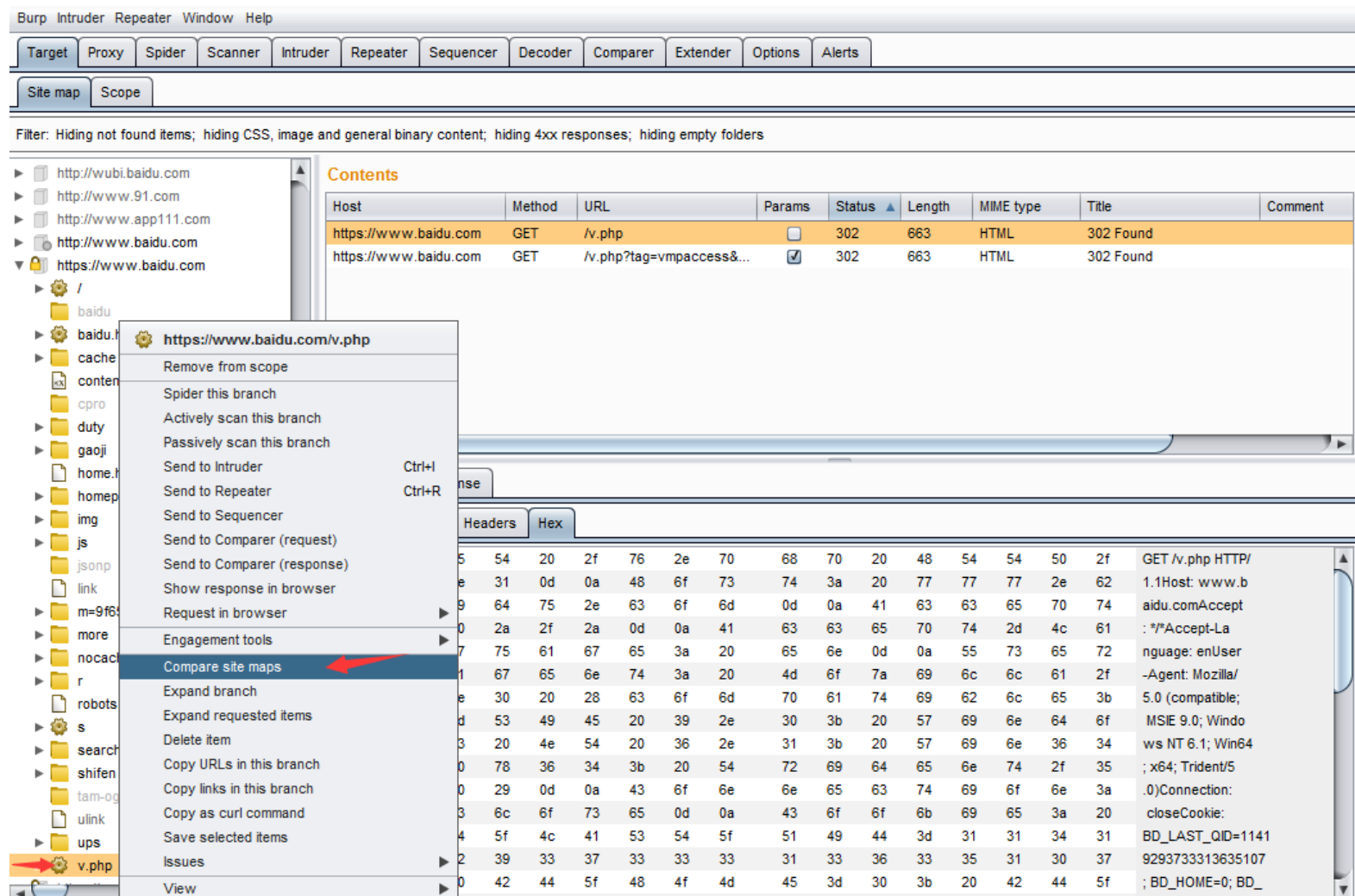
➤手工获取站点地图的方式的好处：

- 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
- 与自动抓取相比，则需要更长的时间，如果需要渗透测试的产品系统是大型的系统，则对于系统的功能点依次操作一遍所需要的精力和时间对渗透测试人员来说付出都是很大的

- 站点比较是一个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。当我们登录应用系统，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
- 一般来说，主要有以下3种场景：
 1. 同一个帐号，具有不同的权限，比较两次请求结果的差异
 2. 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
 3. 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

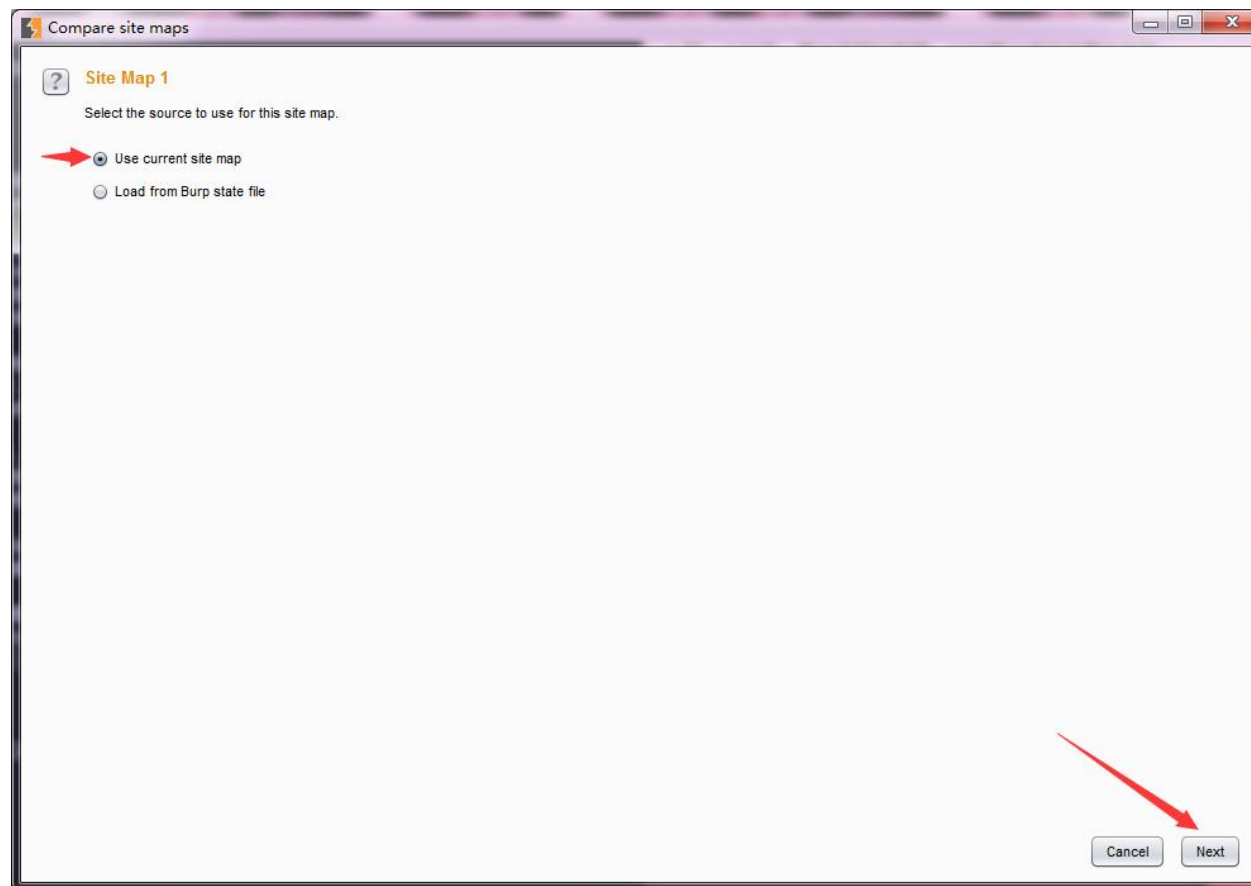
Target 工具的使用——站点比较

➤ 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



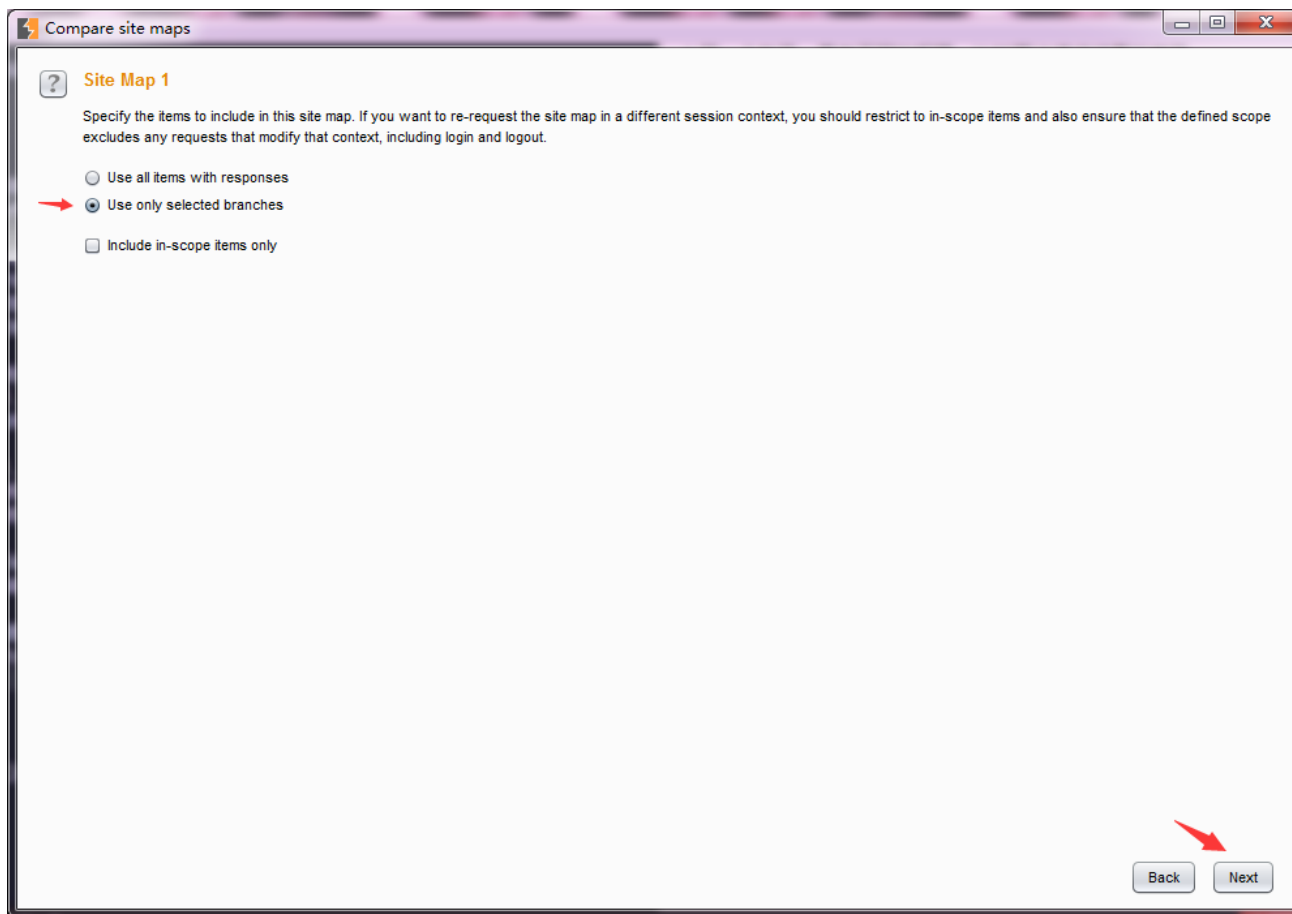
Target 工具的使用—站点比较

- 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

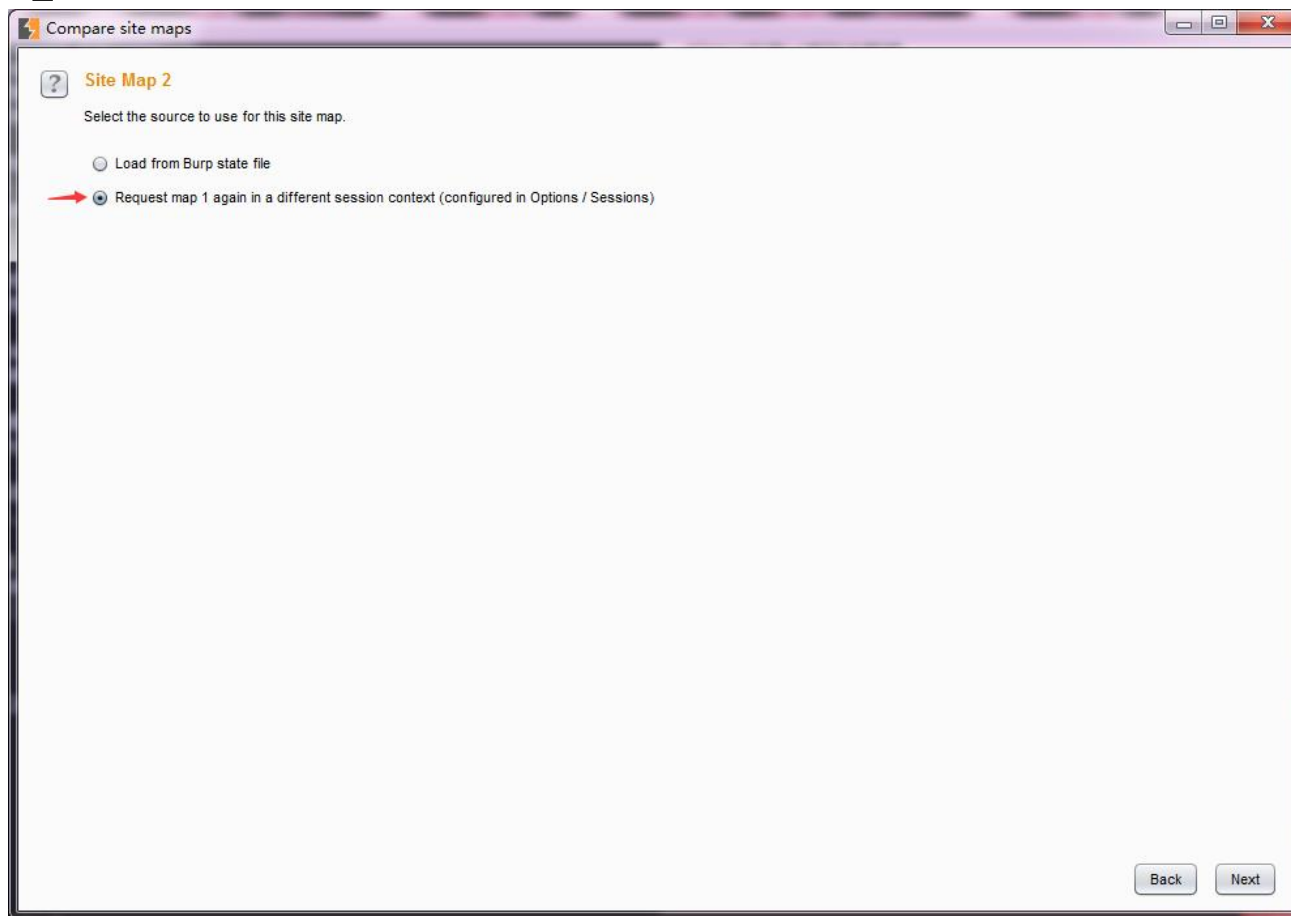


Target 工具的使用—站点比较

➤ 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

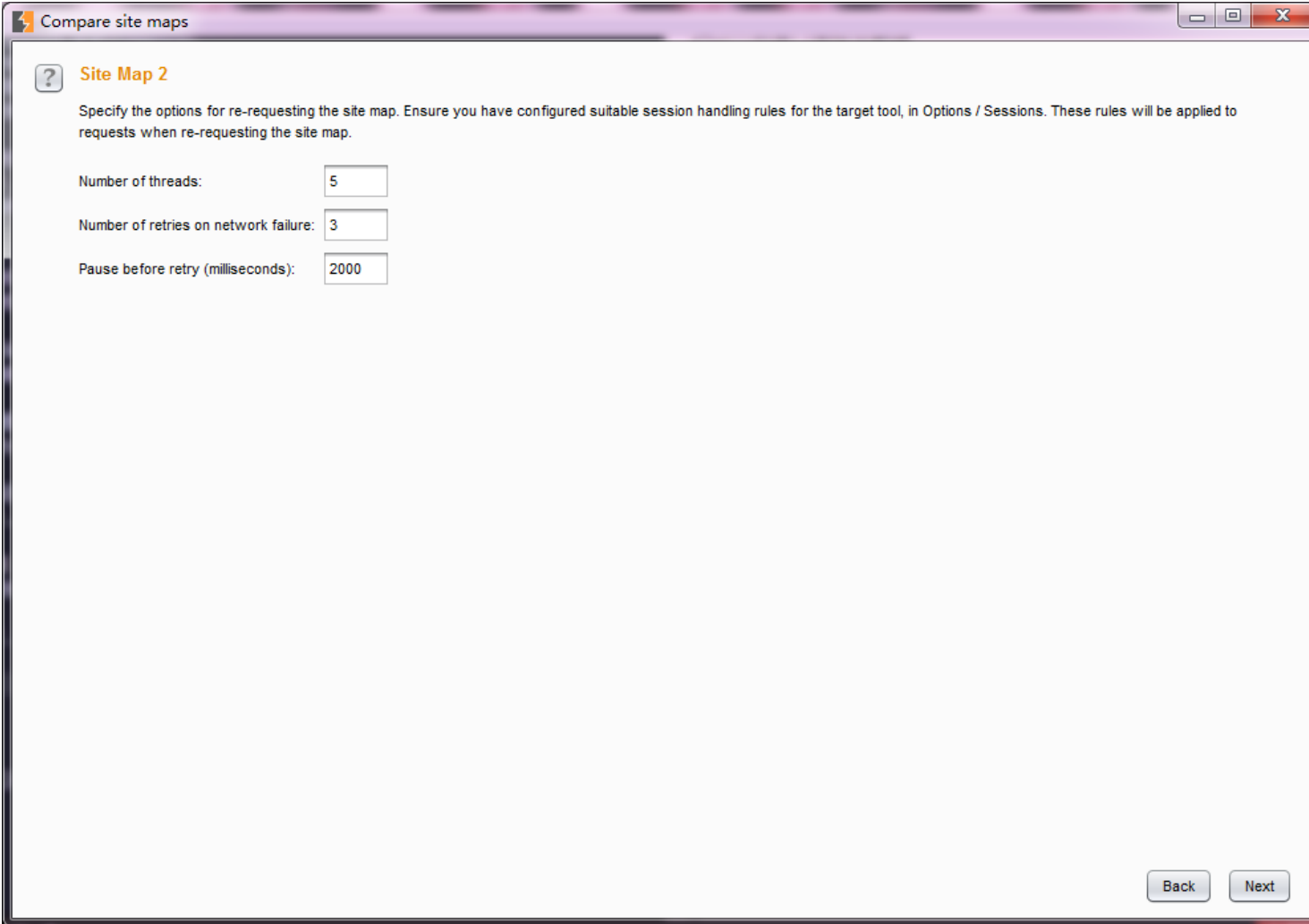


- 对于Site Map 2我们同样有两种方式，第一种是之前我们已经保存下来的Burp Suite 站点记录，第二种是重新发生一次请求作为Site Map2



Target 工具的使用—站点比较

➤ 指定通信的并发线程数、失败重试次数、暂停的间隙时间



Compare site maps

? Site Map 2

Specify the options for re-requesting the site map. Ensure you have configured suitable session handling rules for the target tool, in Options / Sessions. These rules will be applied to requests when re-requesting the site map.

Number of threads:

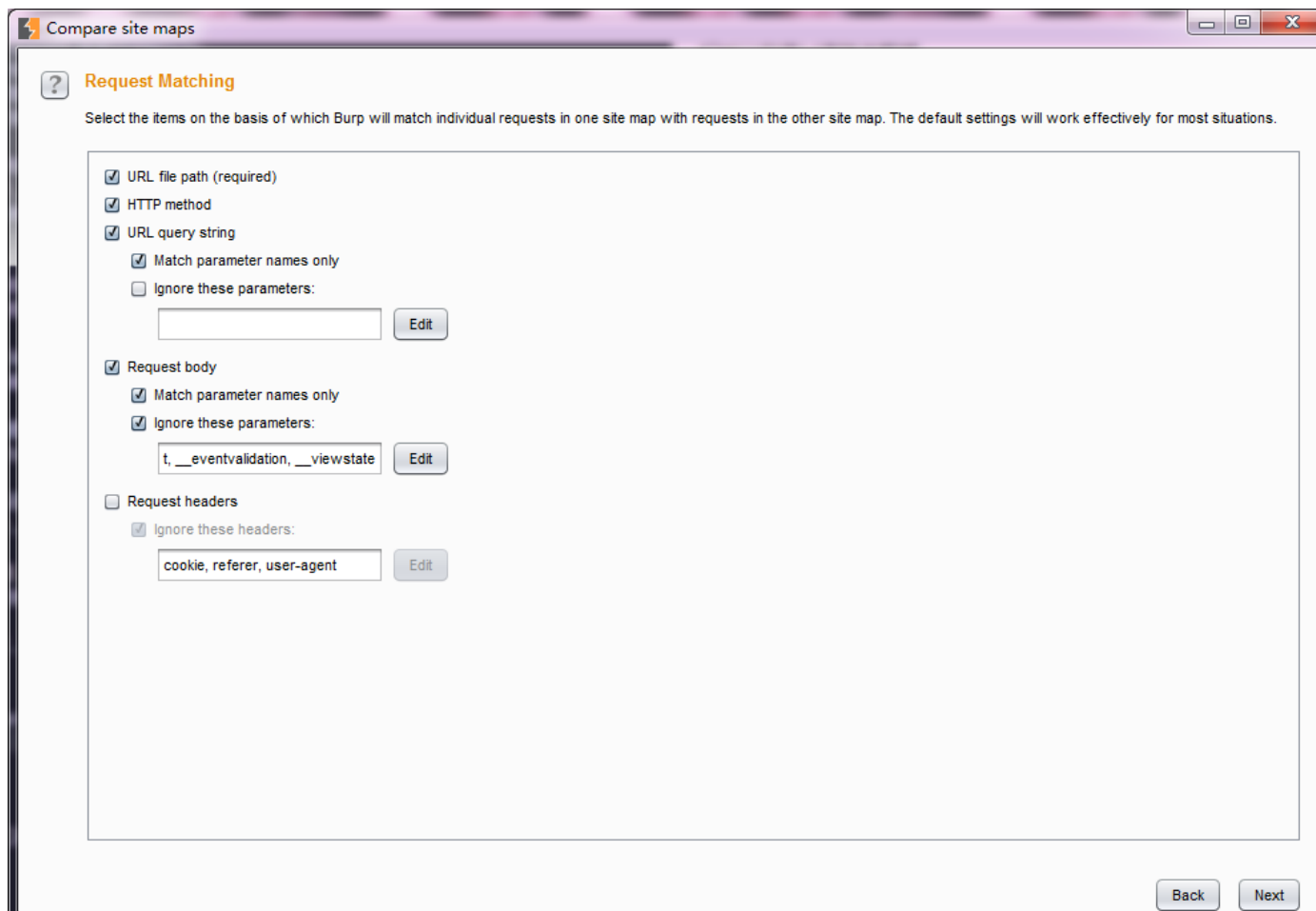
Number of retries on network failure:

Pause before retry (milliseconds):

Back Next

Target 工具的使用——站点比较

➤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



- 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

Target 工具的使用—站点比较



Compare site maps

? **Response Comparison**

Configure the options below to determine how Burp handles certain features of responses when performing comparisons.

Response headers

☒ Include headers

☒ Except for:

☐ Exclude headers

☐ Except for:

Form field values

☒ Include form field values

☒ Except for:

☐ Exclude form field values

☐ Except for:

Whitespace

☒ Ignore whitespace-only variations

MIME type

☒ Don't compare non-text content

- 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

Target 工具的使用—站点比较



Compare site maps

Filter: Showing all items

Key: Modified Deleted Added ☒ Sync selection

Map 1

https://www.baidu.com

Host	Method	URL
https://www.baidu.com	GET	/v.php
https://www.baidu.com	GET	/v.php?tag=vmpaccess&...

Request Response

Raw Headers Hex HTML Render

2_0301_C011_N_I_I_0; expires=Thu, 31-Mar-16 12:24:20 GMT; domain=www.baidu.com; path=/

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">

<html><head>

<title>302 Found</title>

</head><body>

<h1>Found</h1>

5 highlights

Map 2

https://www.baidu.com

Host	Method	URL
https://www.baidu.com	GET	/v.php
https://www.baidu.com	GET	/v.php?tag=vmpaccess&...

Request Response

Raw Headers Hex HTML Render

31-Mar-16 13:27:02 GMT; domain=www.baidu.com; path=/

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">

<html><head>

<title>302 Found</title>

</head><body>

<h1>Found</h1>

5 highlights

Change options Close

Target 工具的使用—攻击面分析

➤ 通过站点地图，打开Analyze Target

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Contents

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment
https://www.baidu.com	GET	/		200	101814	HTML	...	
https://www.baidu.com	GET	/?tn=79081068_1_oem_dg		200	101641	HTML	...	
https://www.baidu.com	GET	/baidu.html		200	22087	HTML	...	
https://www.baidu.com	GET	/baidu.html?from=noscript		200	22088	HTML	...	
https://www.baidu.com	GET	/cache/		200	7868	HTML	...	
https://www.baidu.com	GET	/cache/sethelp/		200	40997	HTML	...	
https://www.baidu.com	GET	/cache/sethelp/help.html		200	41931	HTML	...	
https://www.baidu.com	GET	/cache/sethelp/xml/baidu...		200	1165	XML	...	
https://www.baidu.com	GET	/cache/sethelp/xml/baidui...		200	1013	XML	...	

Issues

Advisory

Site map

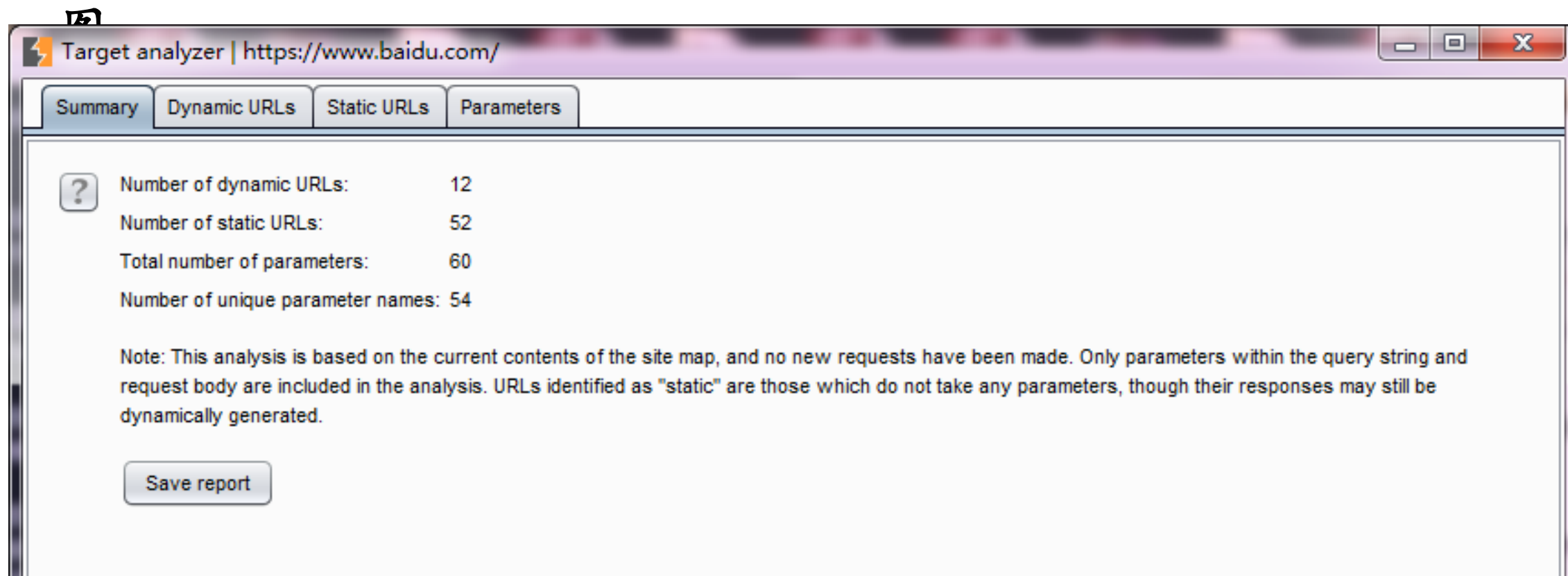
Scope

Engagement tools

- Search
- Find comments
- Find scripts
- Find references
- Analyze target
- Discover content
- Schedule task
- Simulate manual testing

Target 工具的使用—攻击面分析

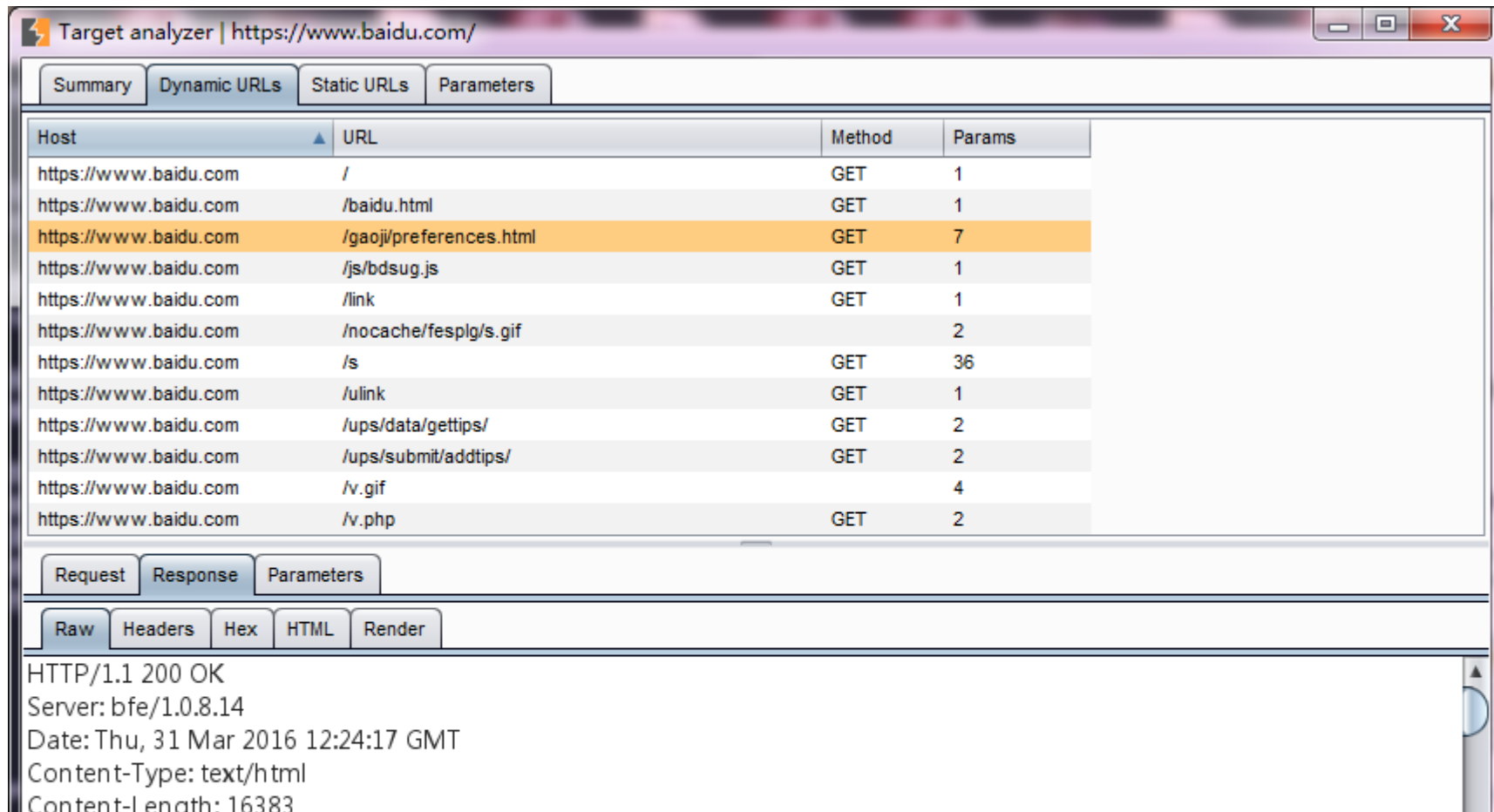
➤分析界面中，可以看到概况、动态URL、静态URL、参数4个视



- 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大致的了解

Target 工具的使用—攻击面分析

➤ 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



The screenshot shows the Target analyzer interface for the URL <https://www.baidu.com/>. The 'Dynamic URLs' tab is selected, displaying a table of requests. The third row is highlighted, showing a GET request to <https://www.baidu.com/gaoji/preferences.html> with 7 parameters. Below the table, the 'Request' tab is selected, showing the raw HTTP request details.

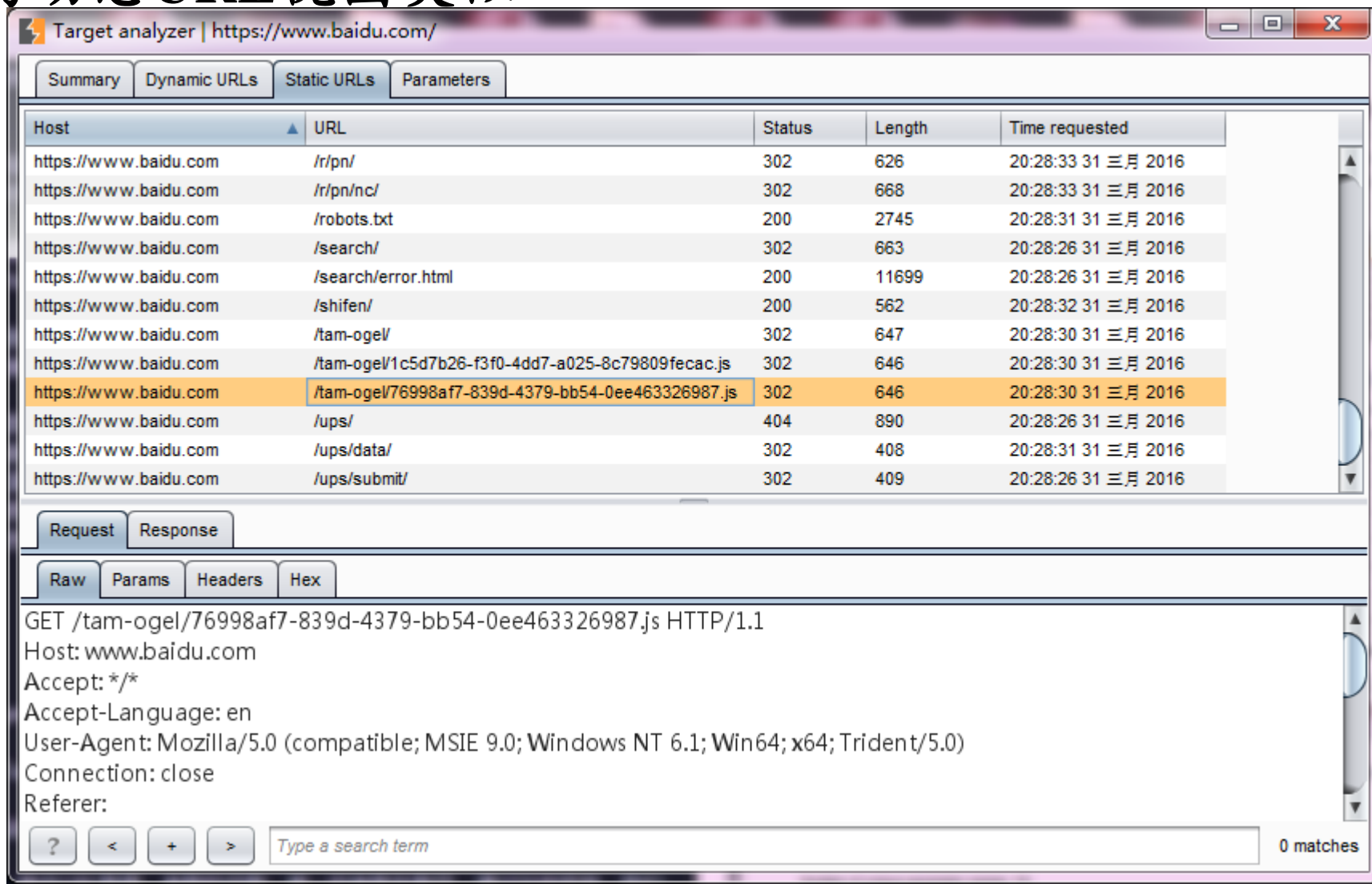
Host	URL	Method	Params
https://www.baidu.com	/	GET	1
https://www.baidu.com	/baidu.html	GET	1
https://www.baidu.com	/gaoji/preferences.html	GET	7
https://www.baidu.com	/js/bdsug.js	GET	1
https://www.baidu.com	/link	GET	1
https://www.baidu.com	/nocache/fesplg/s.gif		2
https://www.baidu.com	/s	GET	36
https://www.baidu.com	/ulink	GET	1
https://www.baidu.com	/ups/data/gettips/	GET	2
https://www.baidu.com	/ups/submit/addtips/	GET	2
https://www.baidu.com	/v.gif		4
https://www.baidu.com	/v.php	GET	2

Request details (Raw):

```
HTTP/1.1 200 OK
Server: bfe/1.0.8.14
Date: Thu, 31 Mar 2016 12:24:17 GMT
Content-Type: text/html
Content-length: 16383
```

Target 工具的使用—攻击面分析

► 静态URL视图与动态URL视图类似



Target analyzer | https://www.baidu.com/

Summary Dynamic URLs Static URLs Parameters

Host	URL	Status	Length	Time requested
https://www.baidu.com	/r/pn/	302	626	20:28:33 31 三月 2016
https://www.baidu.com	/r/pn/nc/	302	668	20:28:33 31 三月 2016
https://www.baidu.com	/robots.txt	200	2745	20:28:31 31 三月 2016
https://www.baidu.com	/search/	302	663	20:28:26 31 三月 2016
https://www.baidu.com	/search/error.html	200	11699	20:28:26 31 三月 2016
https://www.baidu.com	/shifen/	200	562	20:28:32 31 三月 2016
https://www.baidu.com	/tam-ogel/	302	647	20:28:30 31 三月 2016
https://www.baidu.com	/tam-ogel/1c5d7b26-f3f0-4dd7-a025-8c79809fecac.js	302	646	20:28:30 31 三月 2016
https://www.baidu.com	/tam-ogel/76998af7-839d-4379-bb54-0ee463326987.js	302	646	20:28:30 31 三月 2016
https://www.baidu.com	/ups/	404	890	20:28:26 31 三月 2016
https://www.baidu.com	/ups/data/	302	408	20:28:31 31 三月 2016
https://www.baidu.com	/ups/submit/	302	409	20:28:26 31 三月 2016

Request Response

Raw Params Headers Hex

GET /tam-ogel/76998af7-839d-4379-bb54-0ee463326987.js HTTP/1.1
Host: www.baidu.com
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Referer:

? < + > Type a search term 0 matches

- 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

Target 工具的使用—攻击面分析

Target analyzer | https://www.baidu.com/

Summary Dynamic URLs Static URLs Parameters

Name	Number of URLs
pro	1
product	2
recid	1
rn	1
rs_src	1
rsp	1

Host	URL	Method	Params	Value [product]
https://www.baidu.com	/ups/data/gettips/	GET	2	ps
https://www.baidu.com	/ups/submit/addtips/	GET	2	ps

Request Response Parameters

Raw Params Headers Hex

GET /ups/submit/addtips/?product=ps&tips= HTTP/1.1
Host: www.baidu.com
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)

? < + > Type a search term 0 matches

➤ 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

➤Burp Target 的使用

●Burp Target 介绍

●Burp Target 包含的组件，以及每个组件的用法

- 目标域设置 Target Scope
- 站点地图 Site Map
- Target 工具的使用

Question