

- - 用Burp的intruder 的功能进行fuzz xss,sql
 - burpsuite 和 fidder 串联检测app漏洞
 - 使用burp来收集api

用Burp的intruder 的功能进行fuzz xss,sql

写了一个demo:

```
<?php

header('SetCookie:test=xss');
if(isset($_GET['id'])){
    echo 'Get xss:'. $_GET['id'].'<br/>';
}
if(isset($_POST['d'])){
    echo 'Post xss:'. $_REQUEST['d'].'<br/>';
}
if(isset($_COOKIE['test'])){
    echo 'Cookie xss:'. $_COOKIE['test'].'<br/>';
}

?>

<!DOCTYPE html>
<html>
<head>
    <title></title>
</head>
<body>
<form action="form.php?id=1" method="POST">
    <input type="hidden" name="id" value="1">
    <input type="text" name="x"><br/>
    <input type="text" name="d"><br/>
    <input type="submit" value="submit">
</form>
</body>
</html>
```

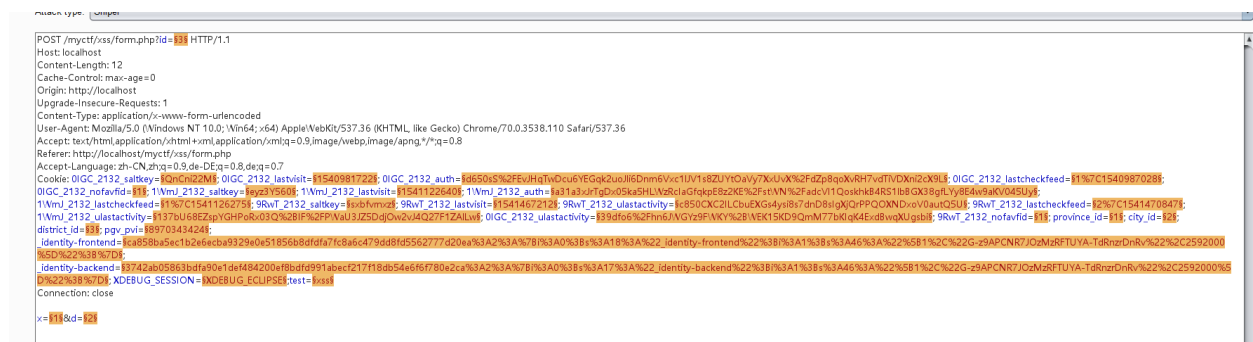
我们来看一下burpsuite如何fuzz出来get,post,cookie 的xss 我们的chrome插件可以fuzz出get,post的xss出来



我们来看一下burp的效果。

发送到intruder会自动对所有变量进行标记。如果不想对cookie变量fuzz,可以选中cookie的值然后clear掉。

如果想要对选中的变量进行批量fuzz, 可以点击 `Auto $`, 会自动对 `=` 后面的值添加 进行标记。还是可以达到这个效果的。



然后我们来到我们的Payloads,添加: `'">rivir>`

`'-sleep(3)-'`

再Options中添加我们对Response的匹配规则:

?

Grep - Match

↺

These settings can be used to flag result items containing specified expressions.

☒ Flag result items with responses matching these expressions:

Paste

error

rivertest

Load ...

Remove

Clear

Add

rivertestf

Match type:

☒ Simple string

☐ Regex

☐ Case sensitive match

☒ Exclude HTTP headers

Request	Position	Payload	Status	Error	Timeout	Length	rivertest	Comment
1	1	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	601	<input checked="" type="checkbox"/>	
25	25	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	599	<input checked="" type="checkbox"/>	
27	27	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	601	<input checked="" type="checkbox"/>	
2	2	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	
3	3	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	
4	4	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	
5	5	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	
6	6	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	
7	7	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	
8	8	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	

Request

Response

Raw

Headers

Hex

HTML

Render

HTTP/1.1 200 OK
Date: Fri, 30 Nov 2018 05:26:33 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9
X-Powered-By: PHP/7.0.12
SetCookie: test=xss
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 356

Get xss:3
Post <ss:'"><rivertest>
Cookie xss:xss

<!DOCTYPE html>
<html>

Filter: Showing all items

Request	Position	Payload	Status	Error	Timeout	Length	rivertest	Comment
1	1	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	601	<input checked="" type="checkbox"/>	
25	25	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	599	<input checked="" type="checkbox"/>	
27	27	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	601	<input checked="" type="checkbox"/>	
2	2	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	
3	3	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	
4	4	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	
5	5	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	
6	6	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	
7	7	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	
8	8	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	

Request Response

Raw Headers Hex HTML Render

HTTP/1.1 200 OK
 Date: Fri, 30 Nov 2018 05:26:33 GMT
 Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9
 X-Powered-By: PHP/7.0.12
 SetCookie: test=xss
 Connection: close
 Content-Type: text/html; charset=UTF-8
 Content-Length: 354

Get xss:3
Post xss:2
Cookie xss:'"><rivertest>

 <!DOCTYPE html>

Filter: Showing all items

Request	Position	Payload	Status	Error	Timeout	Length	rivertest	Comment
1	1	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	601	<input checked="" type="checkbox"/>	
25	25	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	599	<input checked="" type="checkbox"/>	
27	27	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	601	<input checked="" type="checkbox"/>	
2	2	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	
3	3	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	
4	4	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	
5	5	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	
6	6	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	
7	7	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	
8	8	""><rivertest>	200	<input type="checkbox"/>	<input type="checkbox"/>	588	<input type="checkbox"/>	

Request Response

Raw Headers Hex HTML Render

HTTP/1.1 200 OK
 Date: Fri, 30 Nov 2018 05:26:32 GMT
 Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9
 X-Powered-By: PHP/7.0.12
 SetCookie: test=xss
 Connection: close
 Content-Type: text/html; charset=UTF-8
 Content-Length: 356

d Get xss:'"><rivertest>
Post xss:2
Cookie xss:xss

 <!DOCTYPE html>
 <html>

burpsuite 和 fiddler 串联检测app漏洞

使用burpsuite 测试app的缺点:

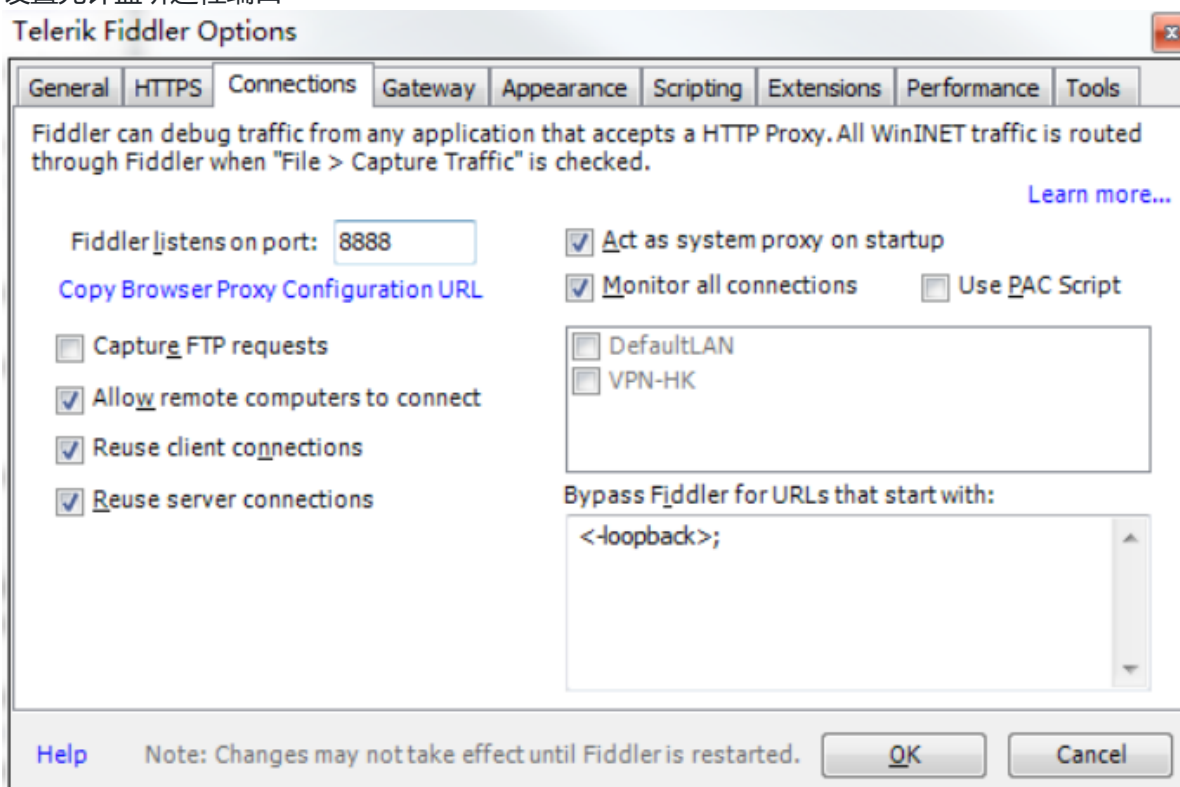
- 使用了burp的代理后，响应速度明显降低，有的App对响应时间有要求，待到响应包返回后，页面已经显示超时，无法完成测试。
- 第二种情况更是糟糕，就是出现抓不到包的情况，burpsuite对https的支持很差。

Fiddler支持http/https的代理，而且是用C#写出来的，而BurpSuite是从底层包中解析http流量，而且是Java写的，这么一对比，单独使用2者的时候，Fiddler比BurpSuite也就很正常。

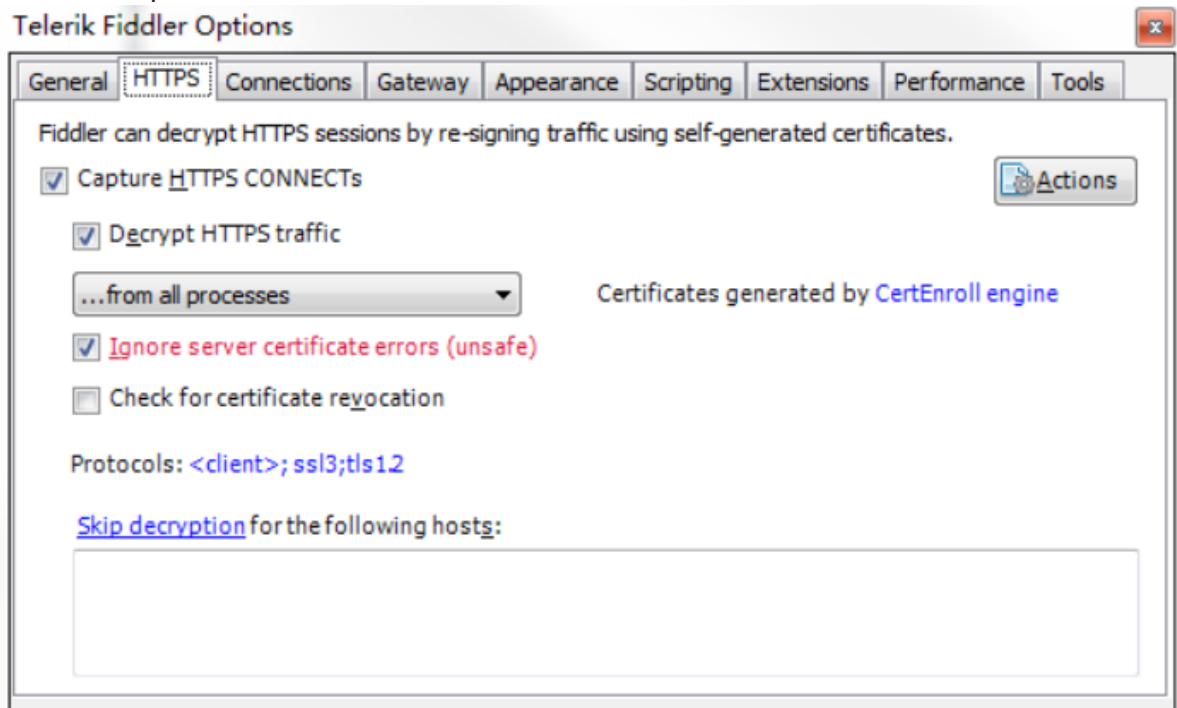
但Fiddler 的缺点是没有像burpsuite 一样插件这么多，功能这么强大，Fiddler是微软官方写的一款工具，目的是给开发人员来抓包的，而不是给安全人员做渗透测试的，因此如果可以串联这两个工具的话，可以发挥比较好的效果。

fiddler的设置

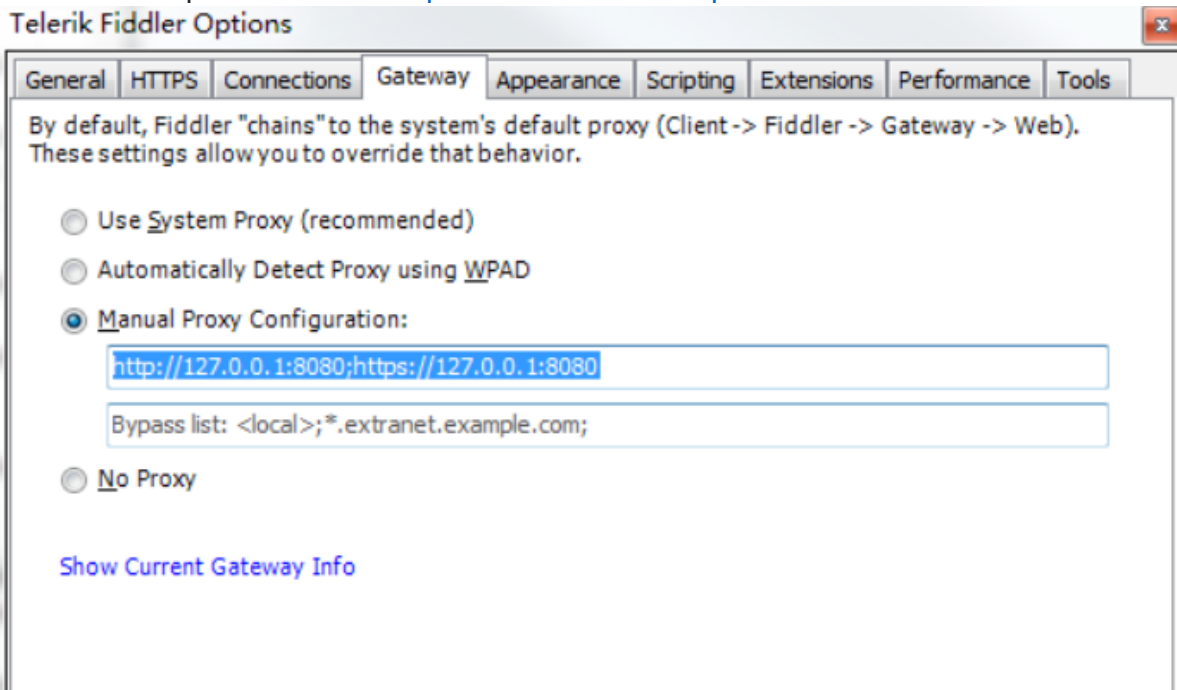
1. 设置允许监听远程端口



2. 设置抓取https的包

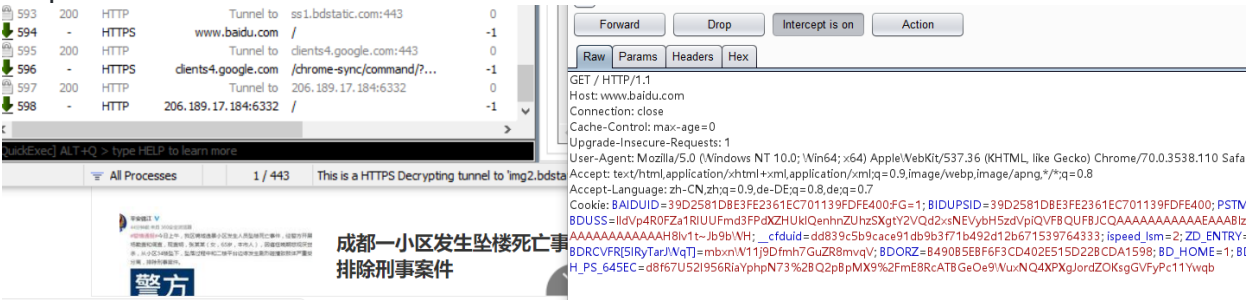


3. 设置网关走burpsuite的代理。 <http://127.0.0.1:8080>;<https://127.0.0.1:8080>



4. 手机安装fiddler证书 (可选)

burpsuite 只需要开启监听8080开启代理即可，最终效果:

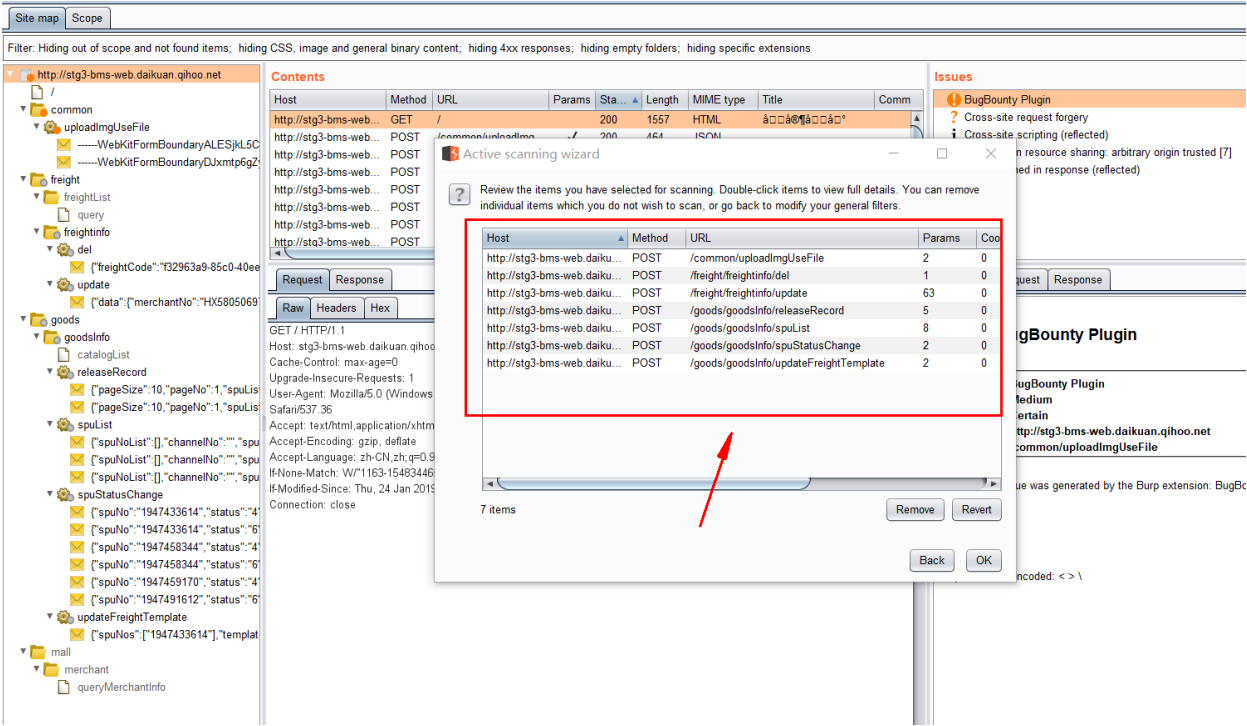


如果burpsuite 没法抓取一些https的站点，也是可以用这种串联的方法对网站进行抓包的。比如正常情况下burpsuite 没法抓 https://www.baidu.com 的包，因为使用了hsts强制https安全策略，但利用串联的方法就可以让burpsuite抓包 https://www.baidu.com 的包了

注意：Fiddler 默认是不会使用系统hosts 的，而Burpsuite默认是会使用的，所以呢，串联后是会使用的。如果你的测试需要绑定hosts，请注意。

使用burp来收集api

在sitemap 界面使用active scan 去重一下即可收集到api



http://stg3-bms-web.daikuan.qihoo.net	POST	/common/uploadImgUseFile	2	0	200	464	JSON
http://stg3-bms-web.daikuan.qihoo.net	POST	/freight/freightinfo/del	1	0	200	364	JSON
http://stg3-bms-web.daikuan.qihoo.net	POST	/freight/freightinfo/update	63	0	200	364	JSON
http://stg3-bms-web.daikuan.qihoo.net	POST	/goods/goodsInfo/releaseRecord	5	0	200	432	JSON
http://stg3-bms-web.daikuan.qihoo.net	POST	/goods/goodsInfo/spuList	8	0	200	2147	JSON
http://stg3-bms-web.daikuan.qihoo.net	POST	/goods/goodsInfo/spuStatusChange	2	0	200	370	JSON
http://stg3-bms-web.daikuan.qihoo.net	POST	/goods/goodsInfo/updateFreightTemplate	2	0	200	367	JSON

或者analyze target 分析sitemap, 把动态链接和静态链接都区分出来

Summary

Dynamic URLs

Static URLs

Parameters

Host	URL	Method	Params
http://stg3-bms-web.daiku...	/common/queryDivisionList	GET	1
http://stg3-bms-web.daiku...	/common/uploadImgUseFile	POST	1
http://stg3-bms-web.daiku...	/freight/freightList/query	POST	0
http://stg3-bms-web.daiku...	/freight/freightinfo/del	POST	0
http://stg3-bms-web.daiku...	/freight/freightinfo/query	POST	0
http://stg3-bms-web.daiku...	/freight/freightinfo/update	POST	0
http://stg3-bms-web.daiku...	/goods/goodsInfo/catalogList	POST	0
http://stg3-bms-web.daiku...	/goods/goodsInfo/goodsInfoPreview	GET	1
http://stg3-bms-web.daiku...	/goods/goodsInfo/latestCatalogList	POST	0
http://stg3-bms-web.daiku...	/goods/goodsInfo/releaseRecord	POST	0

Request

Response

Parameters

Raw

Params

Headers

Hex

POST /freight/freightinfo/update HTTP/1.1
 Host: stg3-bms-web.daikuan.qihoo.net
 Content-Length: 1683
 Origin: http://stg3-bms-web.daikuan.qihoo.net
 userNo: UM5805064972551585792
 dataType: json
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
 Content-Type: application/json; charset=UTF-8
 Access-Control-Allow-Origin: *
 Accept: application/json, text/plain, */*
 X-Requested-With: XMLHttpRequest
 token: 074a84abad864d8fa9e998160b5a70c8
 Referer: http://stg3-bms-web.daikuan.qihoo.net/
 Accept-Encoding: gzip, deflate
 Accept-Language: zh-CN,zh;q=0.9,de-DE;q=0.8,de;q=0.7
 Connection: close

?

<

+

>

Type a search term

0 matches

Engagement Tool提供的搜索过滤url的功能:

只搜索xhr的请求: XMLHttpRequest

Search

Options

Locations

Tools

XMLHttpRequest

Go

☐ Case sensitive
 ☐ In-scope only
 ☐ Regex
 ☐ Dynamic update
 ☐ Negative match

☒ Request headers
 ☐ Response headers
 ☐ Request body
 ☐ Response body

☒ Target
 ☒ Proxy
 ☒ Repeater

Source	Host	URL	Status	Length	Time requested
Target	http://101.230.205.154:8099	/AuthConfig.axd	200	427	19:34:56 16 九月 2019
Target	http://101.230.205.154:8099	/Home/GetCurrentFileVersion	200	280	19:34:56 16 九月 2019
Target	http://101.230.205.154:8099	/api/Auth/Login	200	333	19:34:15 16 九月 2019
Target	http://101.230.205.154:8099	/api/Auth/Login	200	333	19:35:06 16 九月 2019
Repeater	http://101.230.205.154:8099	/api/Auth/Login	200	333	19:27:01 16 九月 2019
Target	http://101.230.205.154:8099	/api/SysCfg/GetAllDics	200	26338	19:34:54 16 九月 2019
Target	http://101.230.205.154:8099	/api/SysCfg/GetBiztypeOrDealtType?dictType=...	200	405	19:34:54 16 九月 2019
Target	http://101.230.205.154:8099	/api/SysCfg/GetBiztypeOrDealtType?dictType=...	200	1170	19:34:55 16 九月 2019
Target	http://101.230.205.154:8099	/api/SysCfg/GetDefaultCalculateMode	200	279	19:34:54 16 九月 2019
Target	http://101.230.205.154:8099	/api/SysCfg/GetDefaultRepoRateType	200	279	19:34:54 16 九月 2019

Request

Response

Raw

Params

Headers

Hex

GET /api/SysCfg/GetBiztypeOrDealtType?dictType=16 HTTP/1.1
 Host: 101.230.205.154:8099
 Accept: */*
 X-Requested-With: XMLHttpRequest
 User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
 Referer: http://101.230.205.154:8099/Home/Login
 Accept-Encoding: gzip, deflate
 Accept-Language: zh-CN,zh;q=0.9,de-DE;q=0.8,de;q=0.7
 Connection: close

?

<

+

>

XMLHttpRequest

1

只搜索POST请求:

