- 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:

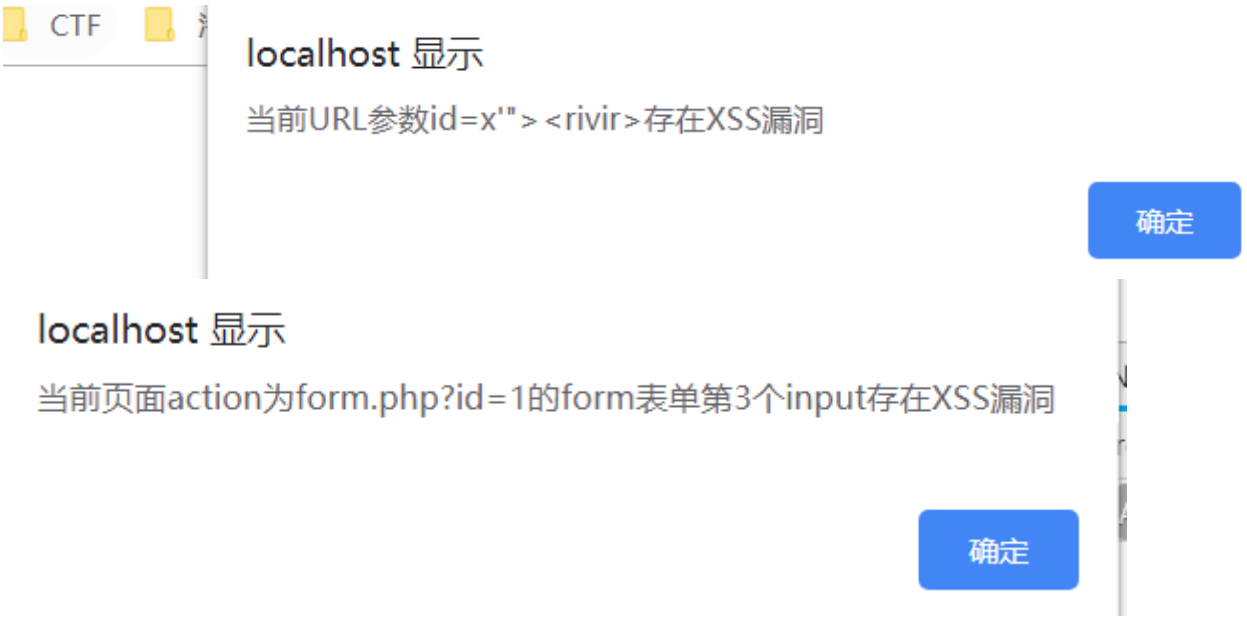
```
<?php

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>
```

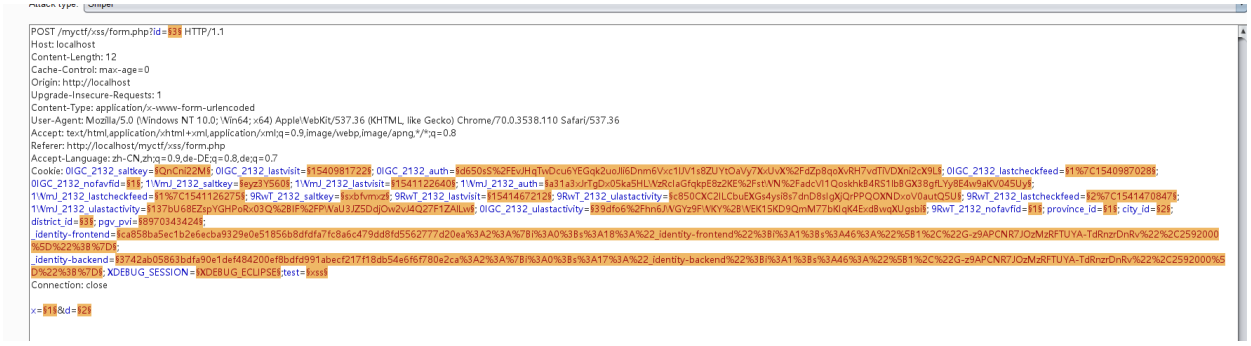
我们来看一下burpsuite如何fuzz出来get,post,cookie 的xss 我们的chrome插件可以fuzz出get,post的xss出来



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。

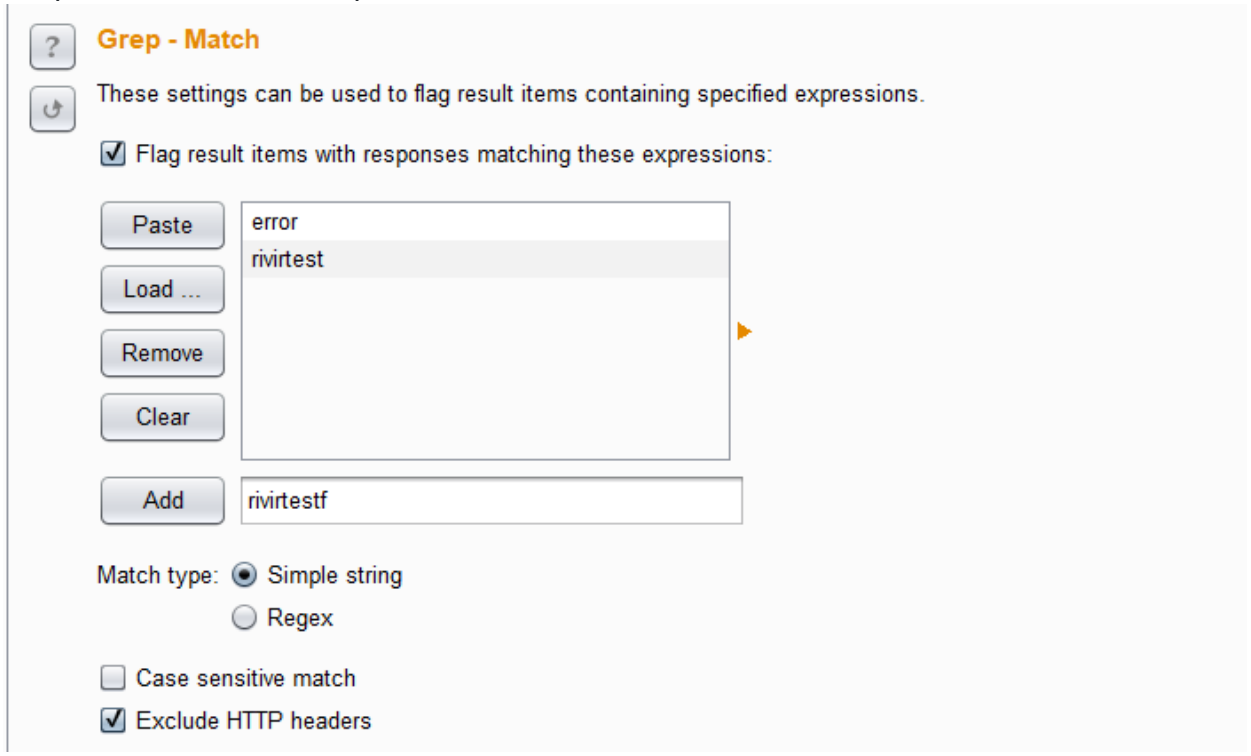
如果想要对选中的变量进行批量fuzz, 可以点击`Auto $`, 会自动对`=`后面的值添加`$`进行标记。还是可以达到这个效果的。

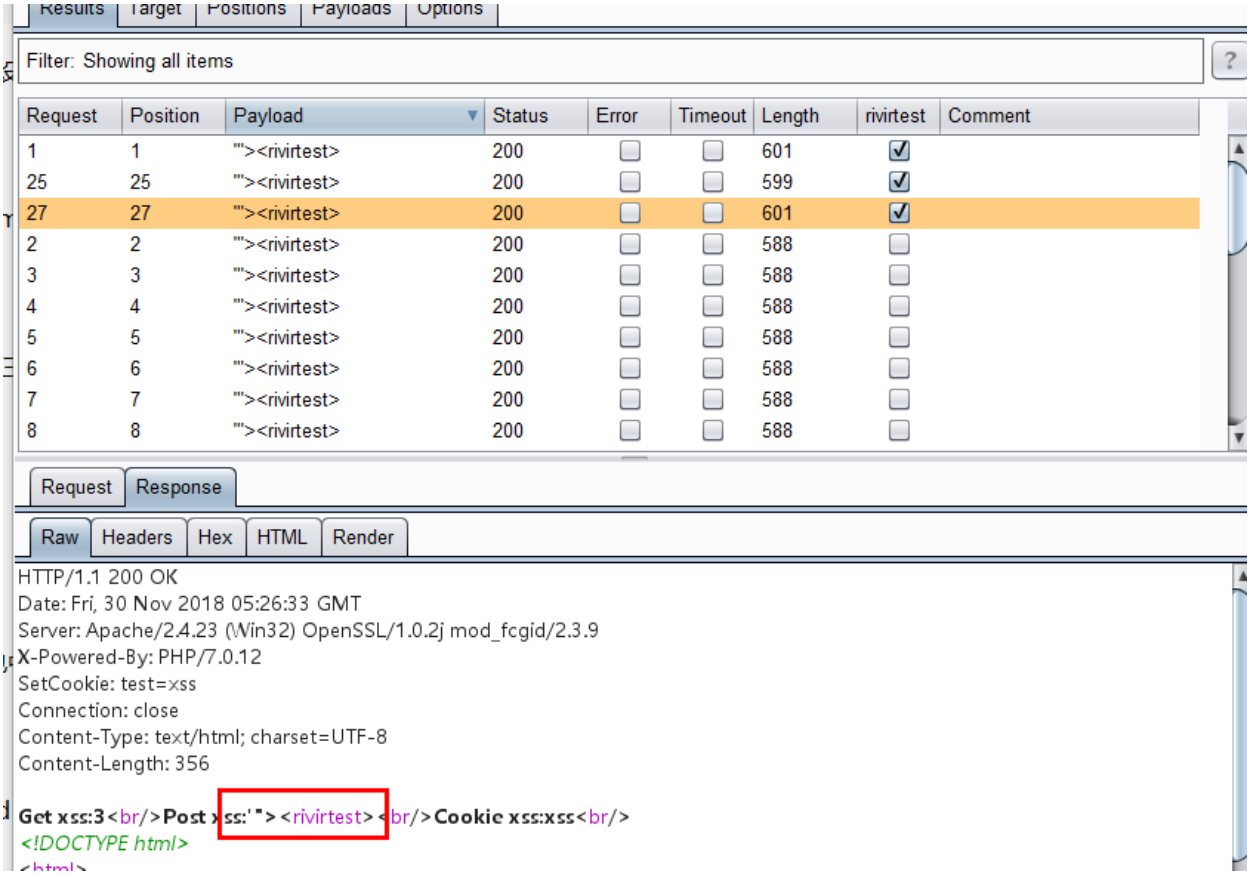


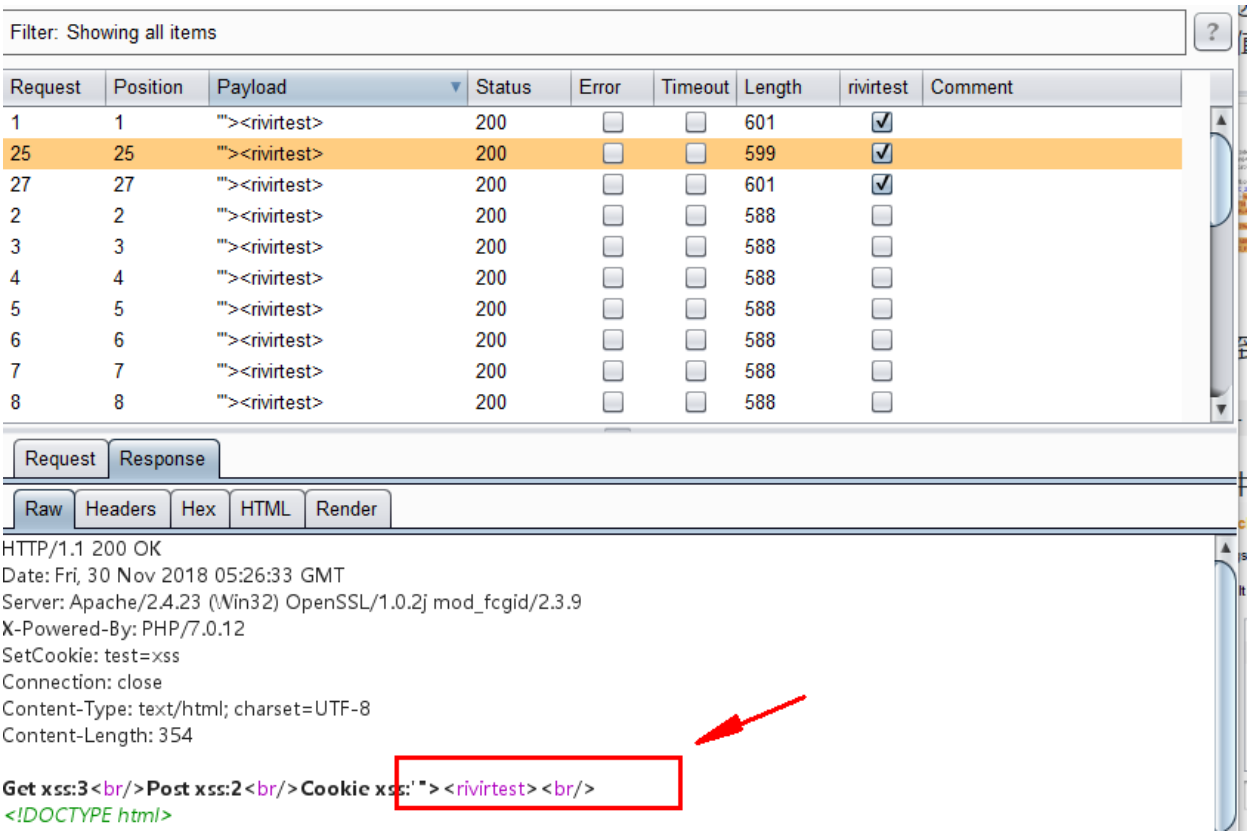
然后我们来到我们的Payloads,添加: `'"><rivir>`

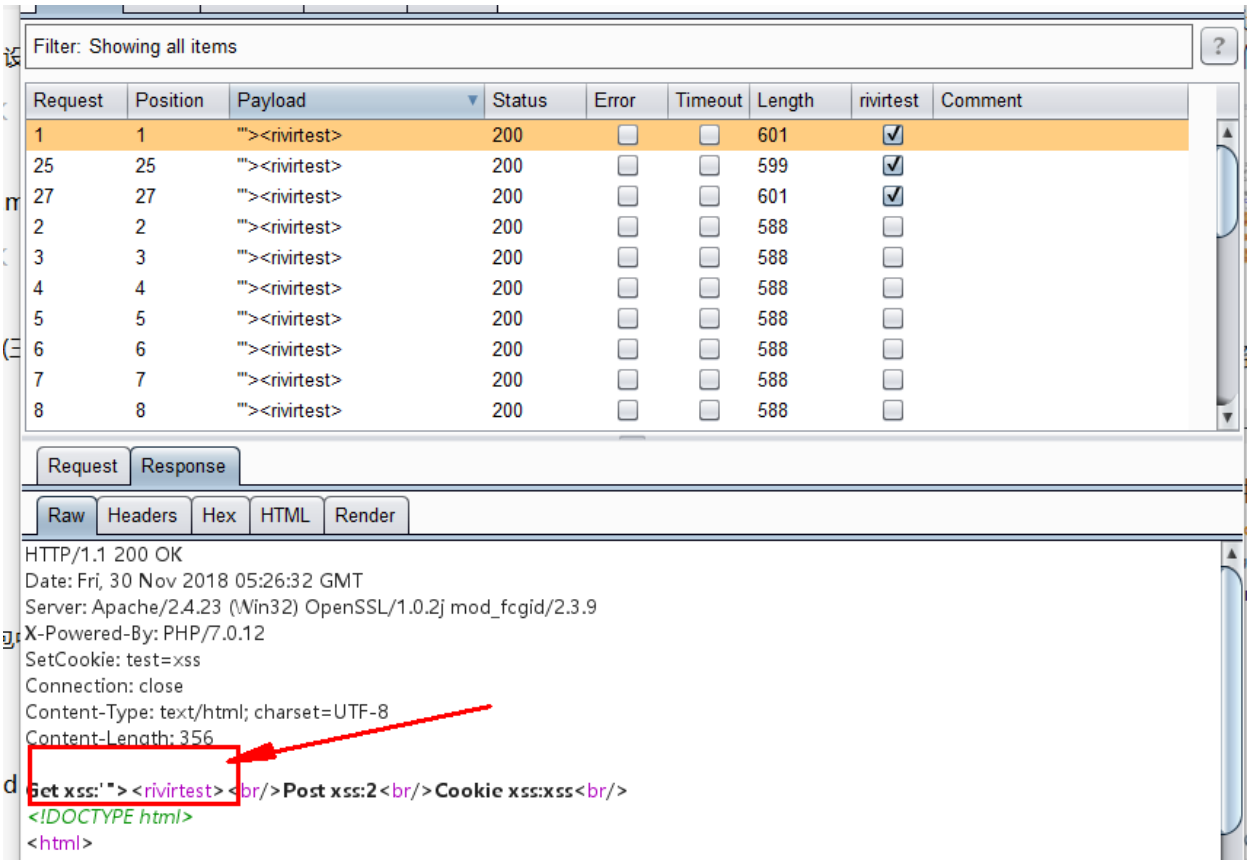
`'-sleep(3)-'`

再Options中添加我们对Response的匹配规则:









burpsuite 和 fidder 串联检测app漏洞

使用burpsuite 测试app的缺点:

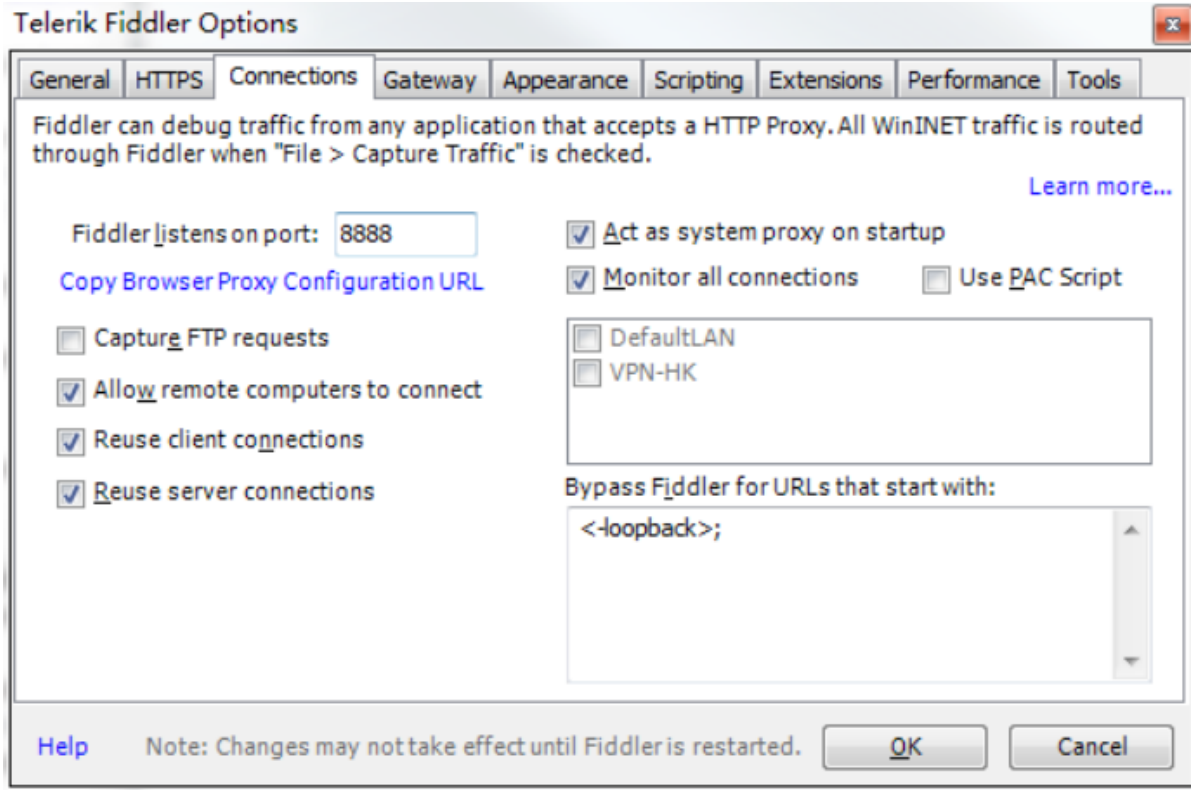
- 使用了burp的代理后，响应速度明显降低，有的App对响应时间有要求，待到响应包返回后，页面已经显示超时，无法完成测试。
- 第二种情况更是糟糕，就是出现抓不到包的情况, burpsuite对https的支持很差。

Fidder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，Fidder比BurpSuite也就很正常。

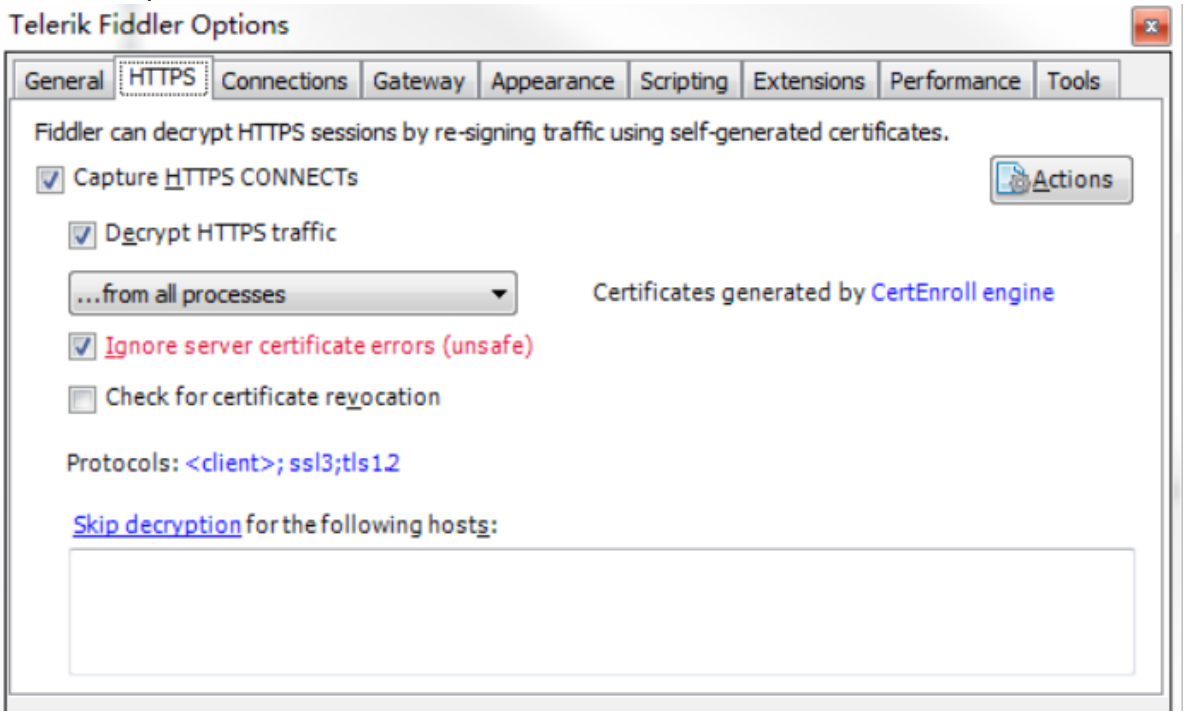
但Fiddler 的缺点是没有像burpsuite 一样插件这么多，功能这么强大，Fidder是微软官方写的一款工具，目的是给开发人员来抓包的，而不是给安全人员做渗透测试的，因此如果可以串联这两个工具的话，可以发挥比较好的效果。

fidder的设置

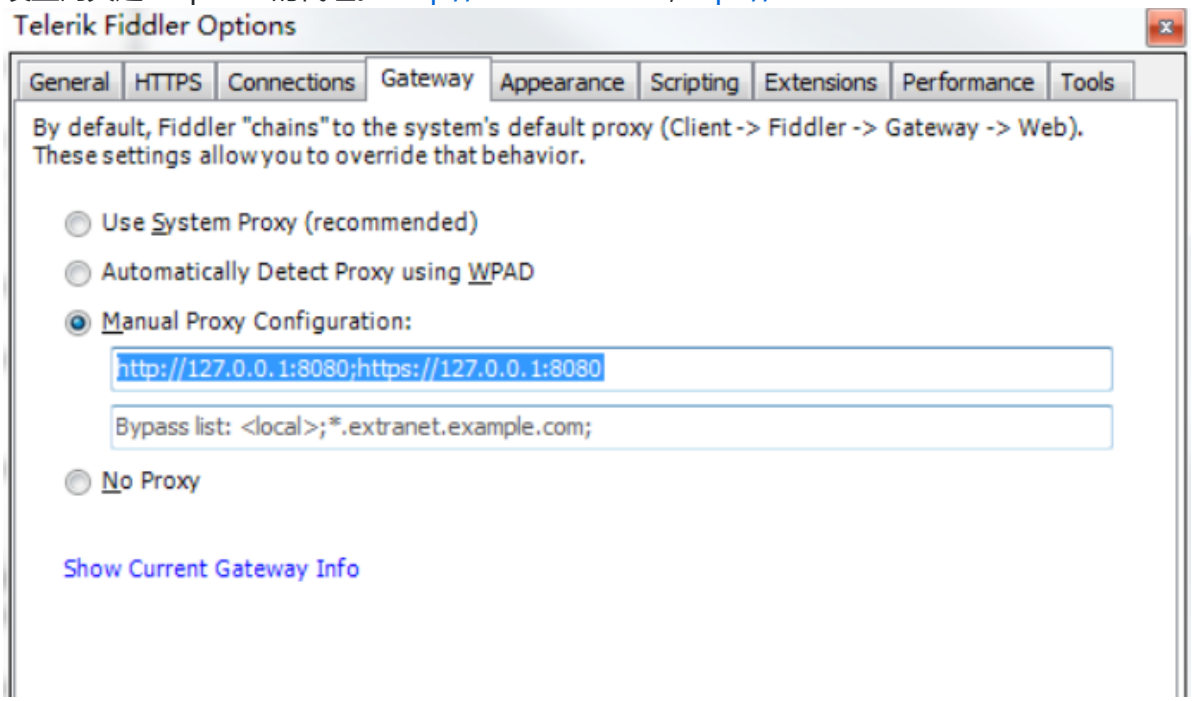
1. 设置允许监听远程端口



2. 设置抓取https的包

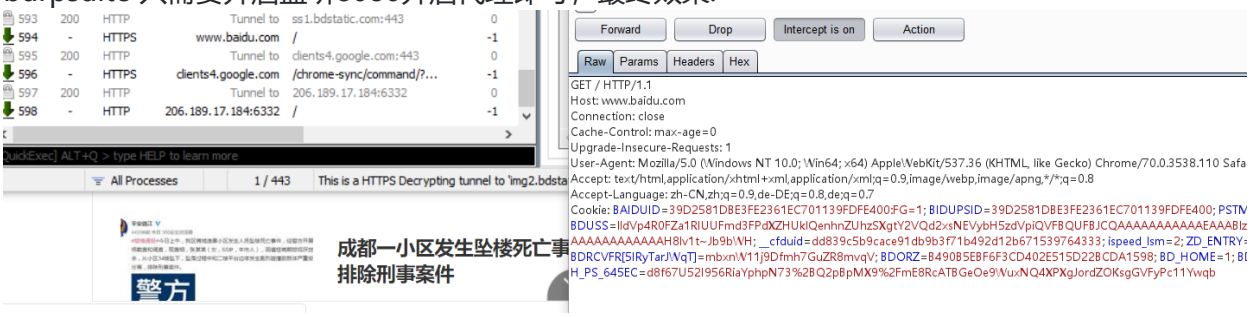


3. 设置网关走burpsuite的代理。 http://127.0.0.1:8080;https://127.0.0.1:8080



4. 手机安装fidder证书 (可选)

burpsuite 只需要开启监听8080开启代理即可，最终效果:

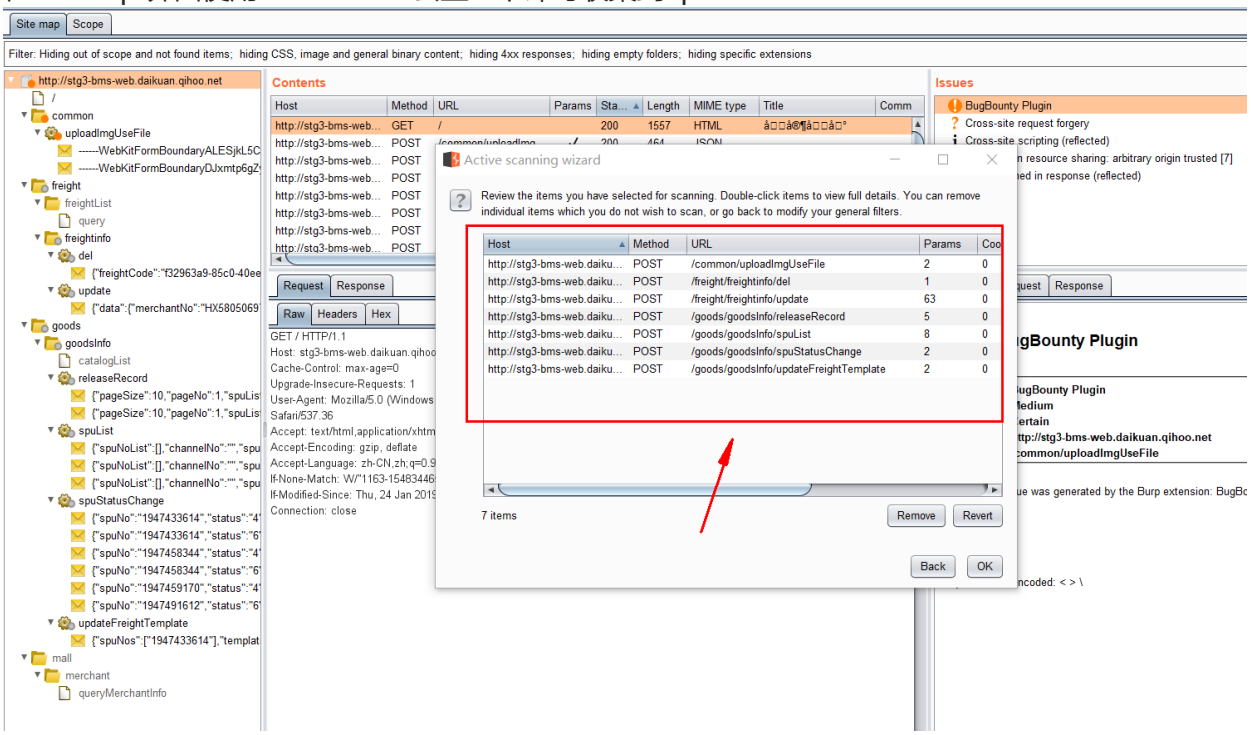


如果burpsuite 没法抓取一些https的站点，也是可以用这种串联的方法对网站进行抓包的。 比如正常情况下burpsuite 没法抓 `https://www.baidu.com` 的包，因为使用了hsts强制https安全策略，但利用串联的方法就可以让burpsuite抓包 `https://www.baidu.com` 的包了

> 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。

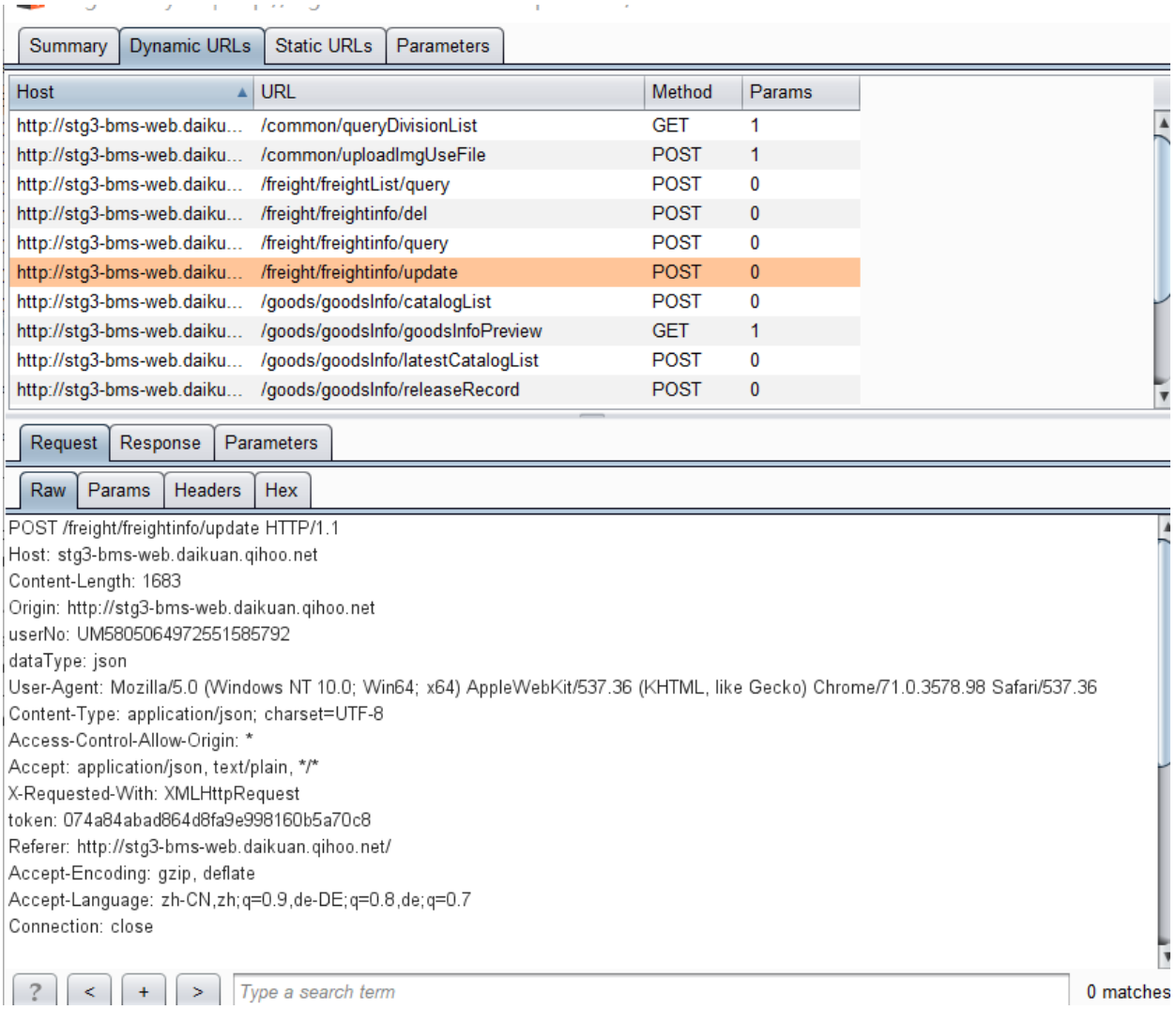
使用burp来收集api

在sitemap 界面使用active scan 去重一下即可收集到api



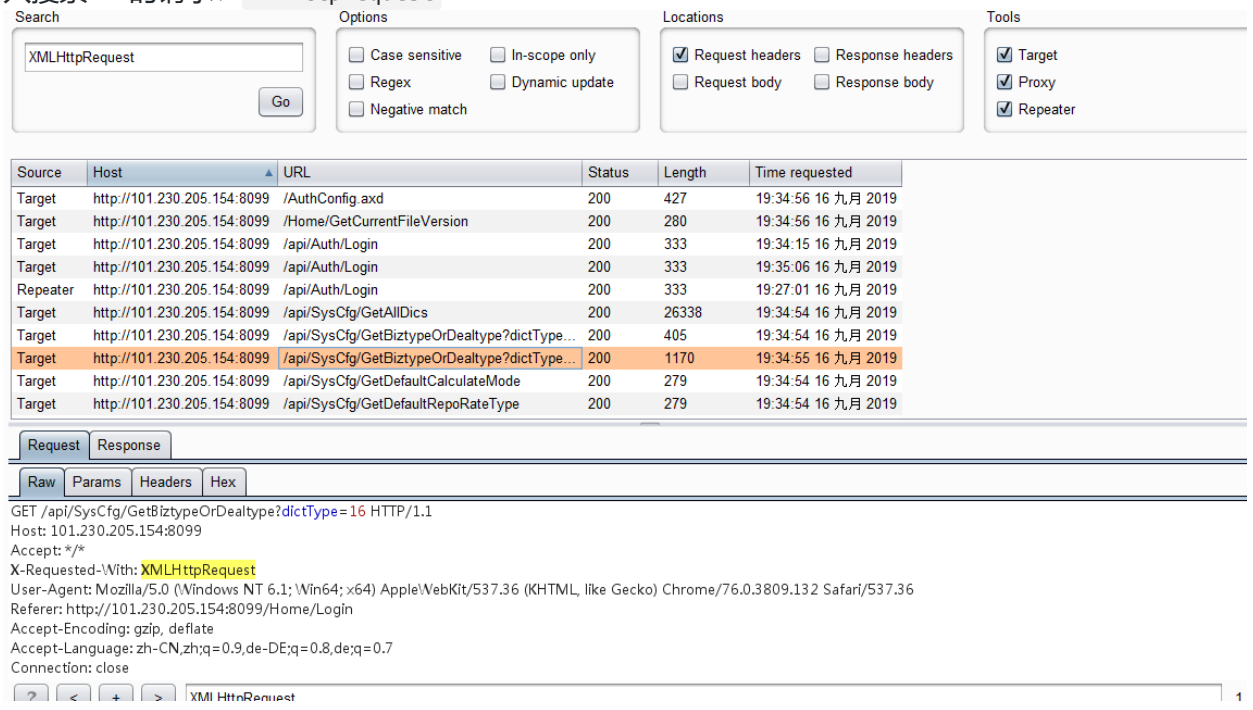

```
http://stg3-bms-web.daikuan.qihoo.net   POST    /common/uploadImgUseFile    2   0   200
464 JSON
http://stg3-bms-web.daikuan.qihoo.net   POST    /freight/freightinfo/del    1   0   200
364 JSON
http://stg3-bms-web.daikuan.qihoo.net   POST    /freight/freightinfo/update 63  0   200
364 JSON
http://stg3-bms-web.daikuan.qihoo.net   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



Engagement Tool提供的搜索过滤url的功能:

只搜索xhr的请求：`XMLHttpRequest`



只搜索POST请求:`