Vulnerability in Dolphin Browser® Mini for Android

Daoyuan Wu*, Xiapu Luo* and Rocky K. C. Chang
The Hong Kong Polytechnic University
{csdwu, csxluo, csrchang}@comp.polyu.edu.hk

Mar 2, 2012 at 2:15 PM HKT

Abstract

We found that Dolphin Browser® Mini 2.2 has a vulnerability that allows a crafted application to read and modify user's sensitive browser information without permission, including user's bookmarks and downloads in Dolphin Browser® Mini.

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1404-vulnerability-in-DolphinBrowserMini.html

2 Description

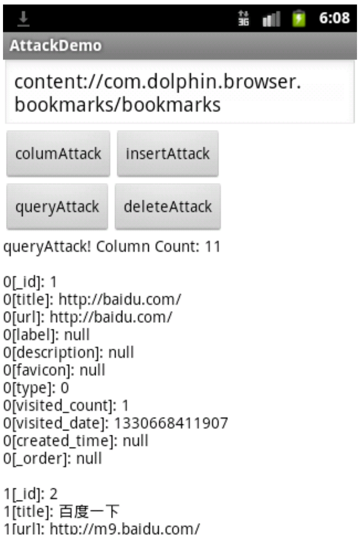
Please see the exposed content providers in the AndroidManifest.xml file, which are not properly protected, as shown in follows:

```
●   <provider android:name=".bookmarks.BookmarkProvider"
    android:authorities="com.dolphin.browser.bookmarks" />
●   <provider android:name=".providers.download.DownloadProvider"
    android:authorities="com.dolphin.browser.downloads" />
```

3 Impact

Please see the following snapshots generated by our arrack demo:

*** authors with equal contributions**

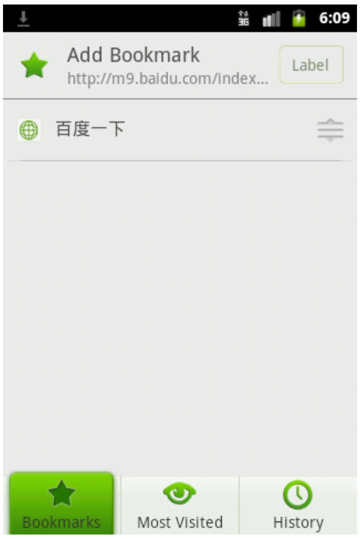


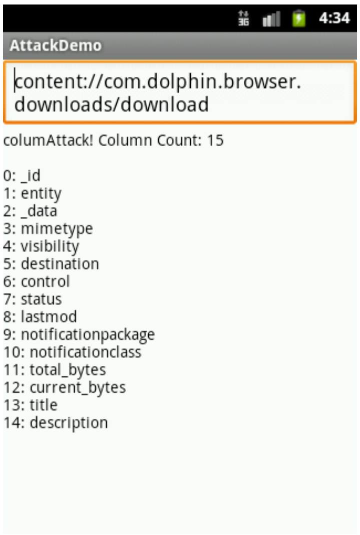
content://com.dolphin.browser.bookmarks/bookmarks

```
queryAttack! Column Count: 11

0[_id]: 1
0[title]: http://baidu.com/
0[url]: http://baidu.com/
0[label]: null
0[description]: null
0[favicon]: null
0[type]: 0
0[visited_count]: 1
0[visited_date]: 1330668411907
0[created_time]: null
0[_order]: null

1[_id]: 2
1[title]: 百度一下
1[url]: http://m9.baidu.com/
```

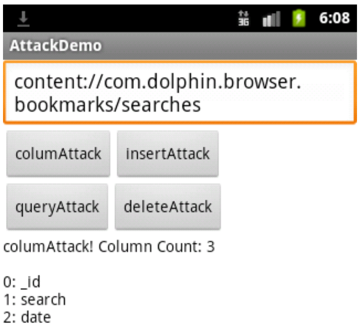




content://com.dolphin.browser.downloads/download

```
columAttack! Column Count: 15

0: _id
1: entity
2: _data
3: mimetype
4: visibility
5: destination
6: control
7: status
8: lastmod
9: notificationpackage
10: notificationclass
11: total_bytes
12: current_bytes
13: title
14: description
```



content://com.dolphin.browser.bookmarks/searches

```
columAttack! Column Count: 3

0: _id
1: search
2: date
```

4 Solution

Our advice is to set the permission of these application’s content providers properly, or avoid exporting these content providers in the AndroidManifest.xml file. Currently, a user could disable the application temporarily and wait for an official update.

5 Technical Description

Please see the following exposed content providers and tables:

Content Provider Authority	Table Name
com.dolphin.browser.downloads	download
com.dolphin.browser.bookmarks	bookmarks
com.dolphin.browser.bookmarks	searches