Cross Miniapp Request Forgery: Root Causes, Attacks, and Vulnerability Detection

Yuqing Yang
Yang.5656@osu.edu

Yue Zhang
Zhang.12407@osu.edu

Zhiqiang Lin
Lin.3021@osu.edu

11/08/2022
What is Super app?

Super apps: apps integrating multiple services
What is Super app?

- Super apps: apps integrating multiple services
  - WeChat (China): 1.26 billion users
What is Super app?

1. Super apps: apps integrating multiple services
   - WeChat (China): 1.26 billion users
     - ‘It’s sort of like Twitter, plus PayPal, plus a whole bunch of other things. And all rolled into one great interface.’ — Elon Musk
   - AliPay (China): 330 million users
What is Super app?

- **Super apps**: apps integrating multiple services
  - **WeChat** (China): 1.26 billion users
    - ‘*It’s sort of like Twitter, plus PayPal, plus a whole bunch of other things. And all rolled into one great interface.*’ — Elon Musk
  - **AliPay** (China): 330 million users
  - **Line** (Japan): 178 million users
What is Super app?

1. **Super apps: apps integrating multiple services**
   - WeChat (China): 1.26 billion users
     - ‘It’s sort of like Twitter, plus PayPal, plus a whole bunch of other things. And all rolled into one great interface.’ — Elon Musk
   - AliPay (China): 330 million users
   - Line (Japan): 178 million users

2. **Miniapp**, a light-weight and full-fledged app, executed inside a JavaScript engine created (or virtualized) by the super app.
What is Mini-app?
What is Mini-app?

WeChat

Bob
Alice is looking for you!

SecLab Group
Alice: Where's Charlie?

Alice
Hi!

WeChat Minis

Charlie’s Shop 4.6/5.0

Delta Mini Pay 4.1/5.0
What is Mini-app?
What is Mini-app?

**WeChat**

- Bob
  - Alice is looking for you!
- SecLab Group
  - Alice: Where’s Charlie?
- Alice
  - Hi!

**Chat Contact Discover**

**WeChat Minis**

- Charlie’s Shop 4.6/5.0
- Delta Mini Pay 4.1/5.0

**WeChat Minis**

- Charlie’s Shop
  - Gourmet Pen $ 20
  - CCS Guide $ 15

**First-time customers: 25% OFF!**
What is Mini-app?

WeChat

Bob
Alice is looking for you!

SecLab Group
Alice: Where's Charlie?

Alice
Hi!

Chat Contact Discover

WeChat Minis

Charlie's Shop 4.6/5.0
Delta Mini Pay 4.1/5.0

WeChat Minis

Charlie's Shop

Gourmet Pen $20
CCS Guide $15

First-time customers: 25% OFF!
What is Mini-app?

- **WeChat**
  - Bob
  - Alice: Where’s Charlie?
  - SecLab Group

- **WeChat Minis**
  - Charlie’s Shop 4.6/5.0
  - Delta Mini Pay 4.1/5.0

- **WeChat Minis**
  - Charlie’s Shop
  - Gourmet Pen $20
  - CCS Guide $15
  - First-time customers: 25% OFF!
Summary: Miniapp

- html
- js
- css

WeChat

Miniapp

WeChat

Super app:
- Provide Execution Environment
- Manage OS Resources
- Handle Cross-miniapp Messages
- ...

Miniapp: third-party apps inside super app
Summary: Miniapp

- Miniapp: third-party apps *inside* super app
- Super app:
  - Provide Execution Environment
Summary: Miniapp

Miniapp: third-party apps inside super app

Super app:
- Provide Execution Environment
- Manage OS Resources
Summary: Miniapp

- Miniapp: third-party apps *inside* super app
- Super app:
  - Provide Execution Environment
  - Manage OS Resources
  - Handle Cross-miniapp Messages
Miniapp: third-party apps *inside* super app

Super app:
- Provide Execution Environment
- Manage OS Resources
- Handle Cross-miniapp Messages
- ...

WeChat

Miniapp
- html
- js
- css

Miniapp: third-party apps *inside* super app

Super app:
- Provide Execution Environment
- Manage OS Resources
- Handle Cross-miniapp Messages
- ...

WeChat

Miniapp
Collaboration between miniapps
Collaboration between miniapps

WeChat Minis

Charlie's Shop

$15.00

Pay
Collaboration between miniapps
Collaboration between miniapps

WeChat Minis

Charlie's Shop
Collaboration between miniapps
Collaboration between miniapps

WeChat Minis

Delta Mini Pay
Collaboration between miniapps
Collaboration between miniapps

Delta Mini Pay

CCS Guide

Price: $15.00
Coupon: -$3.75
Final: $11.25
Collaboration between miniapps
Real-world Case

```javascript
// sender (shopping miniapp) ID: wxd7c977843eb7a64

submitOrder: function(){
  price = self.getPrice();
  tt.navigateToMiniProgram({
    appid: "wx2d495bf4b2abdecef",
    path: "paymentpage",
    extraData: {
      Price: price,
      orderID: orderid,
    }
  });
}

// receiver (payment miniapp) ID: wx2d495bf4b2abdecef

var e=getApp();
onLaunch(o){
  o.referrerInfo && (e.globalData.price
  = o.referrerInfo.extraData.Price) &&
  (e.globalData.appid
  = o.referrerInfo.appId)
  e.globalData.orderID = o.referrerInfo.extraData.orderID
}
Pay:function() {
  var price = e.globalData.Price
  wx.requestPayment({price,...}) //pay the order
  if(e.globalData.appId == "wxd7c977843eb7a64"){
    e.globalData.coupon = 'MYCOUPON'
  }else{
    e.globalData.coupon = null
  }
}
wx.navigateBackMiniProgram(
  extraData: {
    paymentState: 'Success',
    couponCode: e.globalData.coupon
})
```
Sending Cross-app Message

Launch me with parameters!

Payment MiniApp → Coupon: 25% OFF → Shopping MiniApp

He's got coupons. 25% off!
Sending Cross-app Message

Launch me with parameters!

Coupon: 25% OFF

Shopping Miniapp

Coupon: 99% OFF!

Bogus Shopping Miniapp

He’s got coupons. 25% off!

He’s got coupons. 99% off!
Sending Cross-app Message

referrerInfo.appId=="0xdeadbeef"?

Oxdeadbeef only, thanks!
Payment MiniApp

Coupon: 25% OFF
"Sure!"

Shopping MiniApp
Oxdeadbeef

Payment failed :( 
Let him do it again!

Coupon: 99% OFF!
"Liarrrrrrrr :/

Bogus Shopping MiniApp
Oxbadapple

No! Payment is a success! 
(Didn't pay :D)

"Sure!"
CMRF Vulnerability

- **CMRF: Cross-Miniapp Request Forgery**
- **Consuming data without checking sender’s identity can be dangerous!**
Attack Threat Model

1. Victim:
   - On-market miniapp’s back-end
   - Platform users’ privacy

2. Assumptions:
   - Front-end code is safe
   - Back-end is trusted
Vulnerability Detection

1. Dynamic analysis?
   - Over 2.5M miniapps to scan
   - Not scalable

2. Static analysis?
   - Message Usage?
     - `referrerInfo.extraData.*`
   - ID Check?
     - `referrerInfo.appId`
Implementation

1. Challenges
   - Packages are obfuscated
   - Handle Variable Aliases
   - Cross-Function Invocations

2. Data-flow Analysis
   - DoubleX [1]

```javascript
// receiver (payment miniapp) ID: wx2d495bf4b2abdece
var e = getApp();
onLaunch(o){
  o.referrerInfo && (e.globalData.price
  = o.referrerInfo.extraData.Price) &&
  (e.globalData.appId
  = o.referrerInfo.appId)
  e.globalData.orderID = o.referrerInfo.extraData.orderID
}
Pay: function() {
  var price = e.globalData.Price
  wx.requestPayment({price, ...}) // pay the order
  if(e.globalData.appId = "wx7c977843ebe7a64"){
    e.globalData.coupon = "MYCOUPON"
  }else{
    e.globalData.coupon = null
  }
} wx.navigateBackMiniProgram({
  extraData: {
    paymentState: 'Success',
    couponCode: e.globalData.coupon
  }
})
```
Data Collection

1. **WeChat**
   - 2,571,490 Miniapps from *WeChat* with MiniCrawler [2]
   - 6.29 TB space

2. **Baidu**
   - 148,512 miniapps
   - 81 GB space
Miniapp Stats (WeChat)

Total Miniapps

- Shopping: 39.6%
- Lifestyle: 15.6%
- Tool: 10.3%
- Education: 9.5%
- Business: 5.1%
- Food: 4.6%
- Games: 3.4%
- Uncategorized: 3.3%
- Traffic: 1.4%
## Affected Miniapps (WeChat)

<table>
<thead>
<tr>
<th>Category</th>
<th>No Use</th>
<th>Checked</th>
<th>Vulnerable</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td># app</td>
<td>% total</td>
<td># app</td>
</tr>
<tr>
<td>Business</td>
<td>131,078</td>
<td>5.1</td>
<td>81</td>
</tr>
<tr>
<td>E-learning</td>
<td>10,271</td>
<td>0.4</td>
<td>4</td>
</tr>
<tr>
<td>Education</td>
<td>240,077</td>
<td>9.34</td>
<td>184</td>
</tr>
<tr>
<td>Entertainment</td>
<td>29,442</td>
<td>1.14</td>
<td>140</td>
</tr>
<tr>
<td>Finance</td>
<td>3,509</td>
<td>0.14</td>
<td>6</td>
</tr>
<tr>
<td>Food</td>
<td>114,675</td>
<td>4.46</td>
<td>332</td>
</tr>
<tr>
<td>Games</td>
<td>88,056</td>
<td>3.42</td>
<td>10</td>
</tr>
<tr>
<td>Government</td>
<td>31,432</td>
<td>1.22</td>
<td>33</td>
</tr>
<tr>
<td>Health</td>
<td>27,716</td>
<td>1.08</td>
<td>37</td>
</tr>
<tr>
<td>Job</td>
<td>21,773</td>
<td>0.85</td>
<td>16</td>
</tr>
<tr>
<td>Lifestyle</td>
<td>394,493</td>
<td>15.34</td>
<td>269</td>
</tr>
<tr>
<td>Photo</td>
<td>9,039</td>
<td>0.35</td>
<td>3</td>
</tr>
<tr>
<td>Shopping</td>
<td>989,498</td>
<td>38.48</td>
<td>743</td>
</tr>
<tr>
<td>Social</td>
<td>20,671</td>
<td>0.8</td>
<td>6</td>
</tr>
<tr>
<td>Sports</td>
<td>15,980</td>
<td>0.62</td>
<td>69</td>
</tr>
<tr>
<td>Tool</td>
<td>261,467</td>
<td>10.17</td>
<td>122</td>
</tr>
<tr>
<td>Traffic</td>
<td>35,412</td>
<td>1.38</td>
<td>53</td>
</tr>
<tr>
<td>Travelling</td>
<td>10,524</td>
<td>0.41</td>
<td>5</td>
</tr>
<tr>
<td>Uncategorized</td>
<td>83,983</td>
<td>3.27</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>2,519,096</strong></td>
<td><strong>97.96</strong></td>
<td><strong>2,113</strong></td>
</tr>
</tbody>
</table>
## Case Study

<table>
<thead>
<tr>
<th>Category</th>
<th>Variable Name</th>
<th>Vulnerable w/o Check</th>
<th>Vulnerable w/ Incomplete Check</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Info</td>
<td>for_pay_back</td>
<td>355</td>
<td>0</td>
<td>355</td>
</tr>
<tr>
<td></td>
<td>payStatus</td>
<td>313</td>
<td>2</td>
<td>315</td>
</tr>
<tr>
<td></td>
<td>pay</td>
<td>178</td>
<td>9</td>
<td>187</td>
</tr>
<tr>
<td></td>
<td>isPay</td>
<td>118</td>
<td>0</td>
<td>118</td>
</tr>
<tr>
<td></td>
<td>isLecturePay</td>
<td>115</td>
<td>0</td>
<td>115</td>
</tr>
<tr>
<td>Order Info</td>
<td>orderId</td>
<td>132</td>
<td>11</td>
<td>143</td>
</tr>
<tr>
<td></td>
<td>orderInfo</td>
<td>80</td>
<td>0</td>
<td>80</td>
</tr>
<tr>
<td></td>
<td>order_id</td>
<td>42</td>
<td>0</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>jtOrderId</td>
<td>36</td>
<td>3</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>hpj_jsapi_order_id</td>
<td>21</td>
<td>0</td>
<td>21</td>
</tr>
<tr>
<td>Phone Number</td>
<td>mobile</td>
<td>6,627</td>
<td>7</td>
<td>6,634</td>
</tr>
<tr>
<td></td>
<td>phone</td>
<td>53</td>
<td>0</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td>userPhone</td>
<td>8</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>phoneNumber</td>
<td>6</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>partnerMobile</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Promotion Info</td>
<td>cardId</td>
<td>25</td>
<td>0</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>user_coupon_id</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>couponCode</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>coupon_id</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>coupon_no</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Device Info</td>
<td>deviceID</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>uuid</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>deviceld</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>devicenum</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>UUID</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
Case Study: Shopping-for-free

Figure: Xixiu Group Purchase Backend (WeChat)
Case Study: Device Manipulation

Figure: Suyuan Webcam (WeChat)
Case Study: Promotion Abuse

Figure: Aurora Vision (Baidu)
1. **Root Cause**: failure to check miniapp identity before consuming data is dangerous.

2. **The Attack**: CMRF attack can both cause financial loss to vendors and privacy leakage to users.

3. **Detection**: we detected that over 95.97% WeChat and 99.8% Baidu miniapps consuming cross-miniapp data are vulnerable.

4. **Responsible disclosure**: we informed Tencent (Oct 2021) and Baidu (Apr 2022) and received acknowledgements from both.

https://github.com/OSUSecLab/CMRFSscanner
Cross Miniapp Request Forgery: Root Causes, Attacks, and Vulnerability Detection

Yuqing Yang
Yang.5656@osu.edu

Yue Zhang
Zhang.12407@osu.edu

Zhiqiang Lin
Lin.3021@osu.edu

11/08/2022
Aurore Fass, Dolière Francis Somé, Michael Backes, and Ben Stock.
Doublex: Statically detecting vulnerable data flows in browser extensions at scale.

Yue Zhang, Bayan Turkistani, Allen Yuqing Yang, Chaoshun Zuo, and Zhiqiang Lin.
A measurement study of wechat mini-apps.
// code fragment of a vulnerable miniapp
"wxd7c977843ebe7a64" ==
  e.referrerInfo.appId ? e.referrerInfo.appId :"
  && checkPayStatus(param).then(function(a){...})
}
## Applicability

<table>
<thead>
<tr>
<th>Super App</th>
<th>Vendors</th>
<th>AppID</th>
<th>Sending Request APIs</th>
<th>Location</th>
<th>Audio</th>
<th>Bluetooth</th>
<th>Camera</th>
<th>Multi-Media</th>
<th>Sport</th>
<th>User Info</th>
<th>Address</th>
<th>Invoice</th>
<th>File</th>
<th>Data Cache</th>
<th>Payment</th>
<th>Account Info</th>
<th>Coupon</th>
<th>PhoneNumber</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>QQ</td>
<td>Tencent</td>
<td>appId</td>
<td><code>navigateToMiniProgram, navigateBackMiniProgram</code></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>WeChat</td>
<td>Tencent</td>
<td>appId</td>
<td><code>navigateToMiniProgram, navigateBackMiniProgram</code></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>WeCom</td>
<td>Tencent</td>
<td>appId</td>
<td><code>navigateToMiniProgram, navigateBackMiniProgram</code></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Baidu</td>
<td>Baidu</td>
<td>AppKey</td>
<td><code>navigateToSmartProgram, navigateBackSmartProgram</code></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Taobao</td>
<td>Alibaba</td>
<td>appId</td>
<td><code>navigateToMiniProgram, navigateBackMiniProgram</code></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Alipay</td>
<td>Alibaba</td>
<td>appId</td>
<td><code>navigateToMiniProgram, navigateBackMiniProgram</code></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Tiktok</td>
<td>Bytedance</td>
<td>appId</td>
<td><code>navigateToMiniProgram, navigateBackMiniProgram</code></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>JINRI Toutiao</td>
<td>Bytedance</td>
<td>appId</td>
<td><code>navigateToMiniProgram, navigateBackMiniProgram</code></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Watermelon Video</td>
<td>Bytedance</td>
<td>appId</td>
<td><code>navigateToMiniProgram, navigateBackMiniProgram</code></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Pipixia</td>
<td>Bytedance</td>
<td>appId</td>
<td><code>navigateToMiniProgram, navigateBackMiniProgram</code></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Toutiao Lite</td>
<td>Bytedance</td>
<td>appId</td>
<td><code>navigateToMiniProgram, navigateBackMiniProgram</code></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>