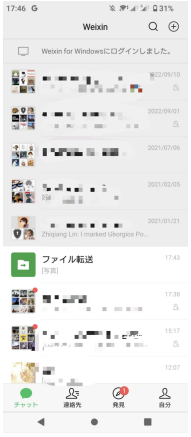
Cross Miniapp Request Forgery: Root Causes, Attacks, and Vulnerability Detection

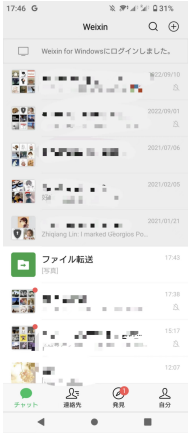
Yuqing Yang, Yue Zhang, and Zhiqiang Lin

CCS 2022

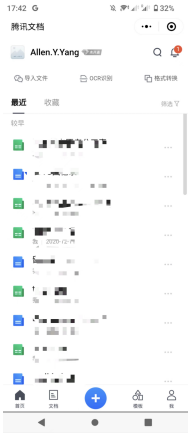
The Mini-app Paradigm



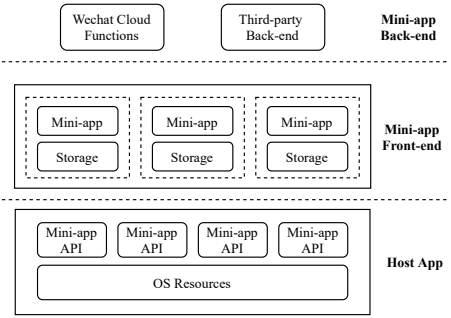
The Mini-app Paradigm



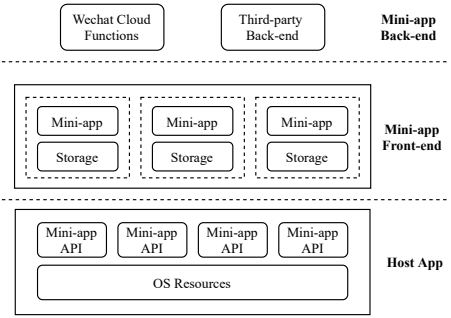
The Mini-app Paradigm



Mini-app Interaction



Mini-app Interaction



- Platform Back-end
- Third-party Back-end
- Super App Front-end
- **(Other) Mini-app front-ends**
  - Cross-miniapp redirection

Motivating Example

Motivating Example

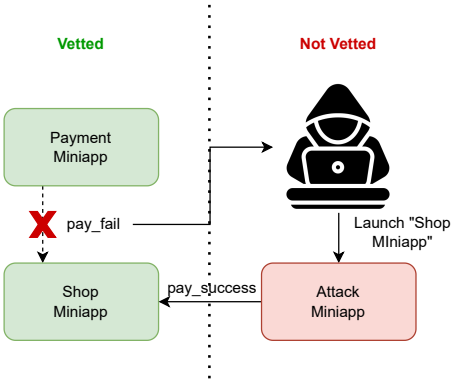
Motivating Example

Motivating Example

```
// sender (shopping miniapp) ID: wxd7c977843ebe7a64
    submitOrder: function(){
    price = self.getPrice();
    tt.navigateToMiniProgram({
      appId: "wx2d495bf4b2abdecef",
      path: "paymentpage",
      extraData: {
        Price: price
        orderID: orderid,
      }
    });
  }
  onLaunch(o){
    var e=this;
    o.referrerInfo && (e.globalData.paymentState
      = o.referrerInfo.extraData.paymentState) &&
      (e.globalData.couponCode
      = o.referrerInfo.extraData.couponCode)
    if(e.globalData.paymentState == "Success")
    {
        shiptheProducts() //ship the products
    }
    saveCouponCode(e.globalData.couponCode)
  }
```

```
// 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 == "wxd7c977843ebe7a64"){
        e.globalData.coupon = 'MYCOUPON'
    }else{
        e.globalData.coupon = null
    }
  }
  wx.navigateBackMiniProgram({
  extraData: {
  paymentState: 'Success',
  couponCode: e.globalData.coupon
}
```

Threat Model



- Attacker:
  - miniapp developer
- Victim:
  - On-market miniapp's back-end
  - Platform users' privacy
- Assumptions:
  - No root phone
  - Front-end code is safe
  - Back-end is trusted

Vulnerability Detection

```
// 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 == "wxd7c977843ebe7a64"){
        e.globalData.coupon = 'MYCOUPON'
    }else{
        e.globalData.coupon = null
    }
  }
  wx.navigateBackMiniProgram({
  extraData: {
  paymentState: 'Success',
  couponCode: e.globalData.coupon
}
```

- Message Usage?
  - `referrerInfo.extraData.*`
- ID Check?
  - `referrerInfo.appId`

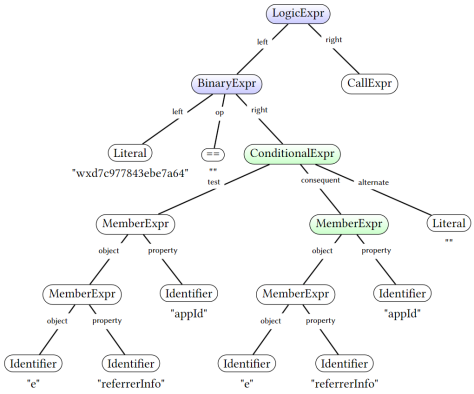
Tracking Data Usage

```
// 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 == "wxd7c977843ebe7a64"){
        e.globalData.coupon = 'MYCOUPON'
    }else{
        e.globalData.coupon = null
    }
  }
  wx.navigateBackMiniProgram({
  extraData: {
  paymentState: 'Success',
  couponCode: e.globalData.coupon
}
```

- Variable Aliases
- Cross-Function Invocation
- Data-flow Analysis
  - DoubleX [1]

Identifying ID Checks

```
1  //code fragment of a vulnerable miniapp
2  "wxd7c977843ebe7a64"==(
3    e.referrerInfo.appId?e.referrerInfo.appId:"")
4    && checkPayStatus(param).then(function(a){...})
5
6  }
```



Data Collection

- WeChat
  - 2,571,490 Miniapps from WeChat
  - 6.29 TB space
- Baidu
  - 148,512 miniapps
  - 81 GB space

Affected Miniapps: Category and Rating

WECHAT

Category	No Use		Checked		Vulnerable	
	# app	%total	# app	%	# app	%
Business	131,078	5.1	81	8.07	923	91.93
E-learning	10,271	0.4	4	5.19	73	94.81
Education	240,077	9.34	184	3.72	4,756	96.28
Entertainment	29,442	1.14	140	33.02	284	66.98
Finance	3,509	0.14	6	6.67	84	93.33
Food	114,675	4.46	332	8.07	3,780	91.93
Games	88,056	3.42	10	2.09	469	97.91
Government	31,432	1.22	33	9.02	333	90.98
Health	27,716	1.08	37	5.44	643	94.56
Job	21,773	0.85	16	7.02	212	92.98
Lifestyle	394,493	15.34	269	4.23	6,092	95.77
Photo	9,039	0.35	3	4.41	65	95.59
Shopping	989,498	38.48	743	2.56	28,304	97.44
Social	20,671	0.8	6	2.99	195	97.01
Sports	15,980	0.62	69	22.48	238	77.52
Tool	261,467	10.17	122	3.72	3,161	96.28
Traffic	35,412	1.38	53	9.28	518	90.72
Travelling	10,524	0.41	5	3.62	133	96.38
Uncategorized	83,983	3.27	0	0.0	18	100.0
Total	2,519,096	97.96	2,113	4.03	50,281	95.97

WECHAT

Popularity	No Use		Checked		Vulnerable	
	# app	%total	# app	%	# app	%
5.0	4,831	0.19	9	4.27	202	95.73
[4.5,5.0)	48,486	1.89	82	5.04	1,545	94.96
[4.0,4.5)	23,794	0.93	18	2.93	597	97.07
[3.5,4.0)	12,222	0.48	3	2.03	145	97.97
[3.0,3.5)	8,342	0.32	2	2.25	87	97.75
[2.5,3.0)	4,375	0.17	2	6.67	28	93.33
[2.0,2.5)	2,014	0.08	0	0.0	3	100.0
[1.5,2.0)	693	0.03	0	0.0	2	100.0
[1.0,1.5)	166	0.01	0	0	0	0
Not Scored	2,414,173	93.88	1,997	4.02	47,672	95.98
Total	2,519,096	97.96	2,113	4.03	50,281	95.97
BAIDU						
[10M,100M)	7	0.0	0	0.0	1	100.0
[1M,10M)	93	0.06	0	0.0	1	100.0
[100K,1M)	2,456	1.65	0	0.0	29	100.0
[10K,100K)	45,495	30.63	1	0.5	200	99.5
[1K,10K)	62,151	41.85	0	0.0	193	100.0
[100,1K)	25,868	17.42	0	0.0	46	100.0
[10,100)	8,196	5.52	0	0.0	10	100.0
[1,10)	3,752	2.53	0	0.0	13	100.0
Total	148,018	99.67	1	0.2	493	99.8

Affected Miniapps: Resources and Relations

Attack	Resources	WeChat #	WeChat %	Baidu #	Baidu %
CMRF-DM	bluetooth	98	0.19	0	0.00
	card	13,139	25.08	0	0.00
	location	9,029	17.23	2	0.40
	media	2,898	5.53	2	0.40
	socket	3,614	6.90	5	1.01
	tcp	15,890	30.33	19	3.85
	sports	0	0.00	0	0.00
CMRF-DS	address	195	0.37	1	0.20
	bluetooth	193	0.37	0	0.00
	camera	31	0.06	0	0.00
	datacache	1506	2.87	20	4.05
	file	274	0.52	3	0.61
	https	1,539	2.94	20	4.05
	invoice	13	0.02	1	0.20
	location	593	1.13	10	2.02
	media	1,154	2.20	6	1.21
	payment	1381	2.64	15	3.04
	socket	325	0.62	3	0.61
	userinfo	1,364	2.60	10	2.02
	sports	8	0.02	0	0.00
Cross-communication/Total		52,394	2.04	494	0.33
Privileged/Vulnerable		28,843	55.05	35	7.09

WeChat	Navigate to # vuln	Navigate to # edges	Navigate to %	Navigate back # vuln	Navigate back # edges	Navigate back %
Categories						
Business	23	41	5.56	97	97	1.31
E-learning	4	4	0.97	1	1	0.13
Education	48	232	11.59	227	227	7.43
Entertainment	9	42	2.17	11	11	1.35
Finance	3	10	0.72	6	6	0.32
Food	4	5	0.97	480	480	0.16
Games	12	54	2.9	8	8	1.73
Government	20	56	4.83	45	48	1.79
Health	25	42	6.04	52	52	1.35
Job	6	52	1.45	15	15	1.67
Lifestyle	58	1,274	14.01	340	340	40.81
Photo	2	19	0.48	8	8	0.61
Shopping	65	195	15.7	946	947	6.25
Social	6	13	1.45	11	11	0.42
Sports	1	1	0.24	10	10	0.03
Tool	98	326	23.67	174	177	10.44
Traffic	14	25	3.38	68	69	0.8
Travelling	3	7	0.72	7	7	0.22
Uncategorized	0	0	0.0	0	0	0.0
Total	401	2,398	96.86	2,506	2,514	80.27
Categories						
5.0	4	5	0.97	4	5	0.16
[4.5,5.0)	92	325	22.22	92	325	10.41
[4.0,4.5)	51	203	12.32	51	203	6.5
[3.5,4.0)	12	51	2.9	12	51	1.63
[3.0,3.5)	6	30	1.45	6	30	0.96
[2.5,3.0)	2	3	0.48	2	3	0.1
[2.0,2.5)	0	0	0.0	0	0	0.0
[1.5,2.0)	0	0	0.0	0	0	0.0
[1.0,1.5)	0	0	0.0	0	0	0.0
Not Scored	234	1,781	56.52	234	1,781	57.05
Total	401	2,398	96.86	2,506	2,514	80.27

Case Study

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

Case Study: Shop-for-free

```
1  //app.js
2  get_pay_info: function(e) {
3  var t = this;
4    if (... e.referrerInfo.extraData.for_pay_back && this.waitForPayBack) {
5      this.waitForPayBack = !1, wx._hideLoading();
6      var r = e.referrerInfo.extraData;
7      "2" == r.pay_status && (this.broadcastUpdate(), "function" == typeof
       ↪  this.payBackSuccess && this.payBackSuccess()),
8      "3" != r.pay_status && "4" != r.pay_status || wx._showAlert({
9        content: "payment failed",
10       success: function() {
11         "function" == typeof t.payBackFail && t.payBackFail();
12       }
13     });
14 }
15 },
```

Device Manipulation

```
1  //  app.js
2  onLaunch: function(t) {
3    console.log(t), a.String.isBlank(t) ||
   ↪  a.String.isBlank(t.referrerInfo.extraData.deviceId) ?
   ↪  this.globalData.data.deviceId = null : this.globalData.data =
   ↪  t.referrerInfo.extraData, wx.showModal({
4      title: "Hint",
5      content: "Live device not found", ...
6      }});},
7  // index/index.js
8  loadLive: function() {
9    wx.request({
10     url: "https://***.com/device/getVideoUrlByDeviceId",
11     data: {
12       deviceId: e.globalData.data.deviceId
13     },
14     method: "get",
15     success: function(o) {...}})}
```

Promotion Abuse

```
1  onShow: function(t) {
2    if (t.referrerInfo && "{}" !== s()(t.referrerInfo) && "{}" !==
     ↪  s()(t.referrerInfo.extraData) && t.referrerInfo.extraData.coupon) {
3      var e = t.referrerInfo.extraData.coupon,
4      n = this.getUserInfoFromCacheSync() || "";
5      Object(l.k)({
6        merchantId: this.globalData.merchantId,
7        couponParams: encodeURI(e),
8        userId: n.sid || "",
9        vs: "V3"
10     }).then((function(t) {
11       console.log("Coupon res", t)
12     })).catch((function(t) {
13       console.log("Coupon err", t)
14     }))
15   }
16 }
```

Applicability

Super App	Vendors	AppID	Sending Request APIs	Location	Audio	Bluetooth	Camera	Multi-Media	Sport	UserInfo	Address	Invoice	File	Data Cache	Payment	AccountInfo	Coupon	PhoneNumber	Network
QQ	Tencent	appId	`navigateToMiniProgram`, `navigateBackMiniProgram`	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
WeChat	Tencent	appId	`navigateToMiniProgram`, `navigateBackMiniProgram`	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
WeCom	Tencent	appId	`navigateToMiniProgram`, `navigateBackMiniProgram`	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Baidu	Baidu	AppKey	`navigateToSmartProgram`, `navigateBackSmartProgram`	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓			✓	✓
Taobao	Alibaba	appId	`navigateToMiniProgram`, `navigateBackMiniProgram`	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓			✓	✓
Alipay	Alibaba	appId	`navigateToMiniProgram`, `navigateBackMiniProgram`	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓			✓	✓
Tiktok	Bytedance	appId	`navigateToMiniProgram`, `navigateBackMiniProgram`	✓	✓		✓	✓		✓	✓	✓	✓	✓				✓	✓
JINRI Toutiao	Bytedance	appId	`navigateToMiniProgram`, `navigateBackMiniProgram`	✓	✓		✓	✓		✓	✓	✓	✓	✓				✓	✓
Watermelon Video	Bytedance	appId	`navigateToMiniProgram`, `navigateBackMiniProgram`	✓	✓		✓	✓		✓	✓	✓	✓	✓				✓	✓
Pipixia	Bytedance	appId	`navigateToMiniProgram`, `navigateBackMiniProgram`	✓	✓		✓	✓		✓	✓	✓	✓	✓				✓	✓
Toutiao Lite	Bytedance	appId	`navigateToMiniProgram`, `navigateBackMiniProgram`	✓	✓		✓	✓		✓	✓	✓	✓	✓				✓	✓

Responsible Disclosure

- Reported to Tencent
  - First Discovery (October 2021)
  - Complete List (Janurary 2022)
- Reported to Baidu (April 2022)

References I

Aurore Fass, Dolière Francis Somé, Michael Backes, and Ben Stock.
Doublex: Statically detecting vulnerable data flows in browser extensions at scale.
In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 1789–1804, 2021.

Q & A