

# iOS App Security

唐巧

# About Me

- iOS Developer (有道云笔记, 粉笔网, 猿题库)



- InfoQ中文站兼职编辑
- iOS Blogger: <http://www.devtang.com> (70+posts)
- “iOSDevTips”微信公众账号创建者 (5000+ fans, 150+ posts)





Why security?

# Agenda

- 行业与现状
- iOS Security
  - Network Security
  - Local File/Data Security
  - Code Security
- Resources

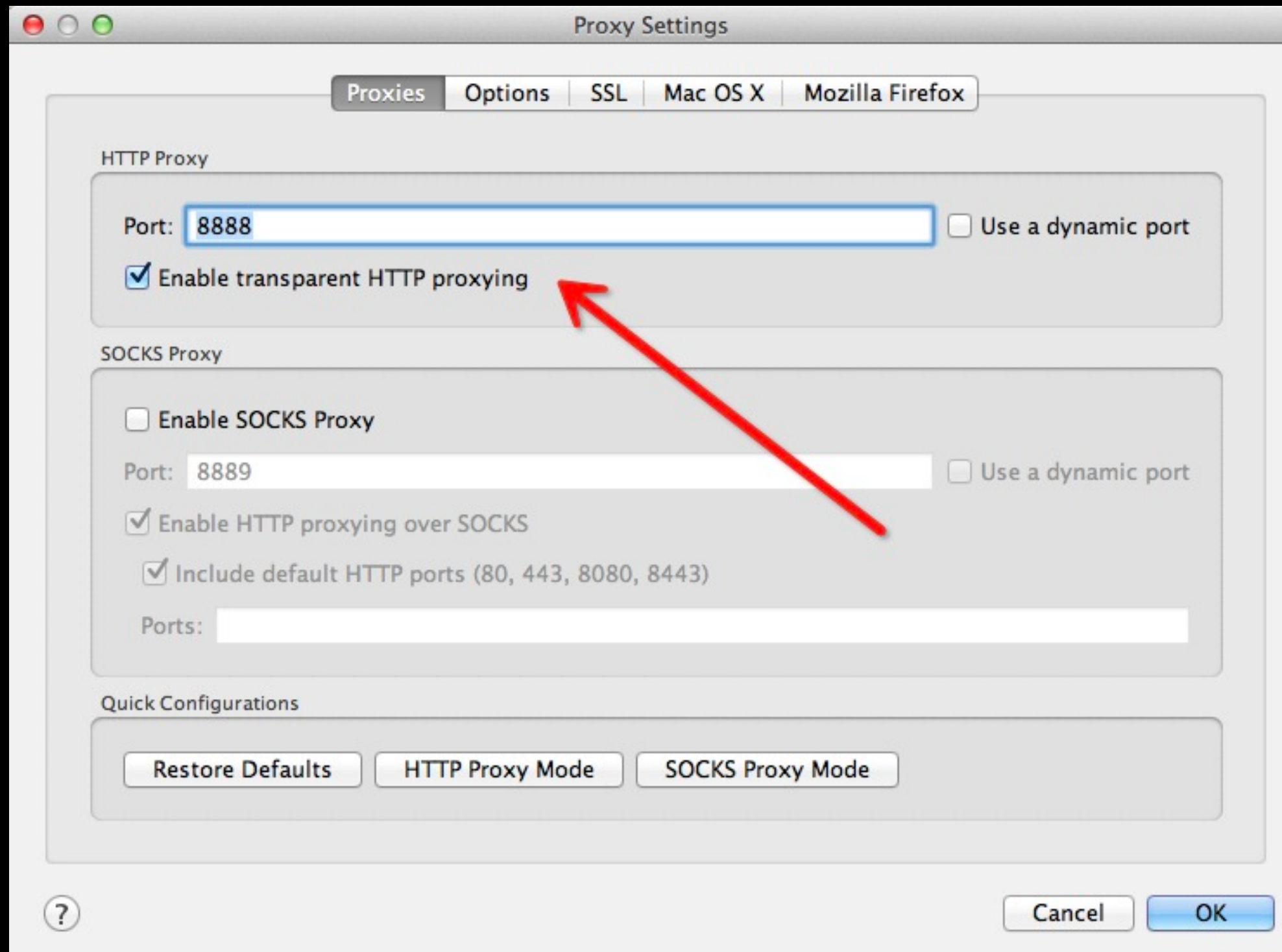
# 行业与现状

- 传统互联网
  - 大公司专门的安全部门
  - 汉庭，如家酒店2000万用户数据库泄漏
  - struts 2漏洞
  - 苹果iTunesConnect网站多次重置开发者密码
- 移动互联网
  - 信息较少

# Network Security



# Network Security - Charles



# Network Security - Charles





# Network Security - Charles

The screenshot displays the Charles 3.7 - Session 1 interface. The top toolbar includes icons for adding new sessions, saving, deleting, pausing, and other functions. The main window is divided into two panes: 'Structure' and 'Sequence'. The 'Sequence' pane shows a list of network requests and responses. The selected request is a POST to adash.m.taobao.com, which is highlighted in blue. Below the list, the 'Response' pane shows the JSON response body.

RC	Mthd	Host	Path	Duration	Size	Status
✗	CONNECT	m.google.com:443		7539...	165 by...	Failed
J 200	GET	api.m.taobao.com	/rest/api3.do?imsi=09876543...	516...	1.42 KB	Compl...
J 200	POST	adash.m.taobao.com	/rest/gc?ak=21380790&av=3...	501...	1.19 KB	Compl...
J 200	GET	api.m.taobao.com	/rest/api3.do?appKey=21380...	41 ms	4.62 KB	Compl...
J 200	GET	api.m.taobao.com	/rest/api3.do?appKey=21380...	87 ms	1.52 KB	Compl...
J 200	GET	m.simba.taobao.com	/ex?st=iPhone_native&i=mm_1...	468...	1.04 KB	Compl...
J 200	GET	api.m.taobao.com	/rest/api3.do?imsi=09876543...	31 ms	1.11 KB	Compl...
J 200	GET	www.taobao.com	/go/rgn/taobao2013/bootimag...	426...	759 by...	Compl...
J 200	GET	www.taobao.com	/go/rgn/taobao4iphone/remot...	404...	823 by...	Compl...
J 200	GET	api.m.taobao.com	/rest/api3.do?imsi=09876543...	35 ms	1.61 KB	Compl...

Filter:  Settings

Overview Request **Response** Summary Chart Notes

```
1 {
2   "t": 1384333949552,
3   "data": {
4     "B01N2": {
5       "content": "gc_304"
6     },
7     "B01N5": {
8       "content": "gc_304"
9     }
10  },
11  "success": "success",
12  "ret": "",
13  "v": "2"
14 }
```

Headers Text Hex JSON **JSON Text** Raw

GET http://www.google.com/mobile/other/ Recording

# Network Security - Charles

The screenshot displays the Charles Proxy application interface. At the top, a table lists network requests. The second row is highlighted in blue, showing a GET request to mobile.1hai.cn. Below this table is a 'Filter:' input field. A tabbed interface below the filter shows 'Overview', 'Request' (selected), 'Response', 'Summary', 'Chart', and 'Notes'. The 'Request' tab is active, showing a message (msg) with the text '100003\$101\$' followed by two redacted sections.

Icon	Status	Method	Host	Path	Size	Time
		CONNECT	gs-loc.apple.com:443		3285...	8.85 K
	200	GET	mobile.1hai.cn	/DataInterface.aspx?msg=100...	219...	437 by

Filter:

Overview Request Response Summary Chart Notes

msg 100003\$101\$ [REDACTED] 3 [REDACTED]

# Network Security - Charles

	Status	Method	Host	Path	Time	Size
X	200	POST	sdk.zuche.com	/CARSDK/services/zuche1	41 ms	1.56 KB
X	200	POST	sdk.zuche.com	/CARSDK/services/zuche1	35 ms	1.44 KB
X	200	POST	sdk.zuche.com	/CARSDK/services/zuche1	103...	1.36 KB
X	200	POST	sdk.zuche.com	/CARSDK/services/zuche1	21 ms	1.38 KB

Filter:

Overview

Request

Response

Summary

Chart

Notes

Structure	Method	Content
▼ UserLogin	Method	
▼ Parameters	Element	
queryString	Element	{"userId":"[REDACTED]","password":"[REDACTED]"}
▼ Result	Element	
UserLoginResult	Element	{"stateValues":{"code":"ACK","description":"成功"},"user":{"cardtyp

# Network Security - Charles

- 分析协议，测试协议，找安全漏洞
- 伪装请求，欺骗服务器
- 截取密码和Cookie
- 《iOS开发工具——网络封包分析工具 Charles 》 12-09 on InfoQ

# Network Security - IAP



- IAP Story

<http://blog.devtang.com/blog/2013/04/07/tricks-in-iap/>

# Network Security

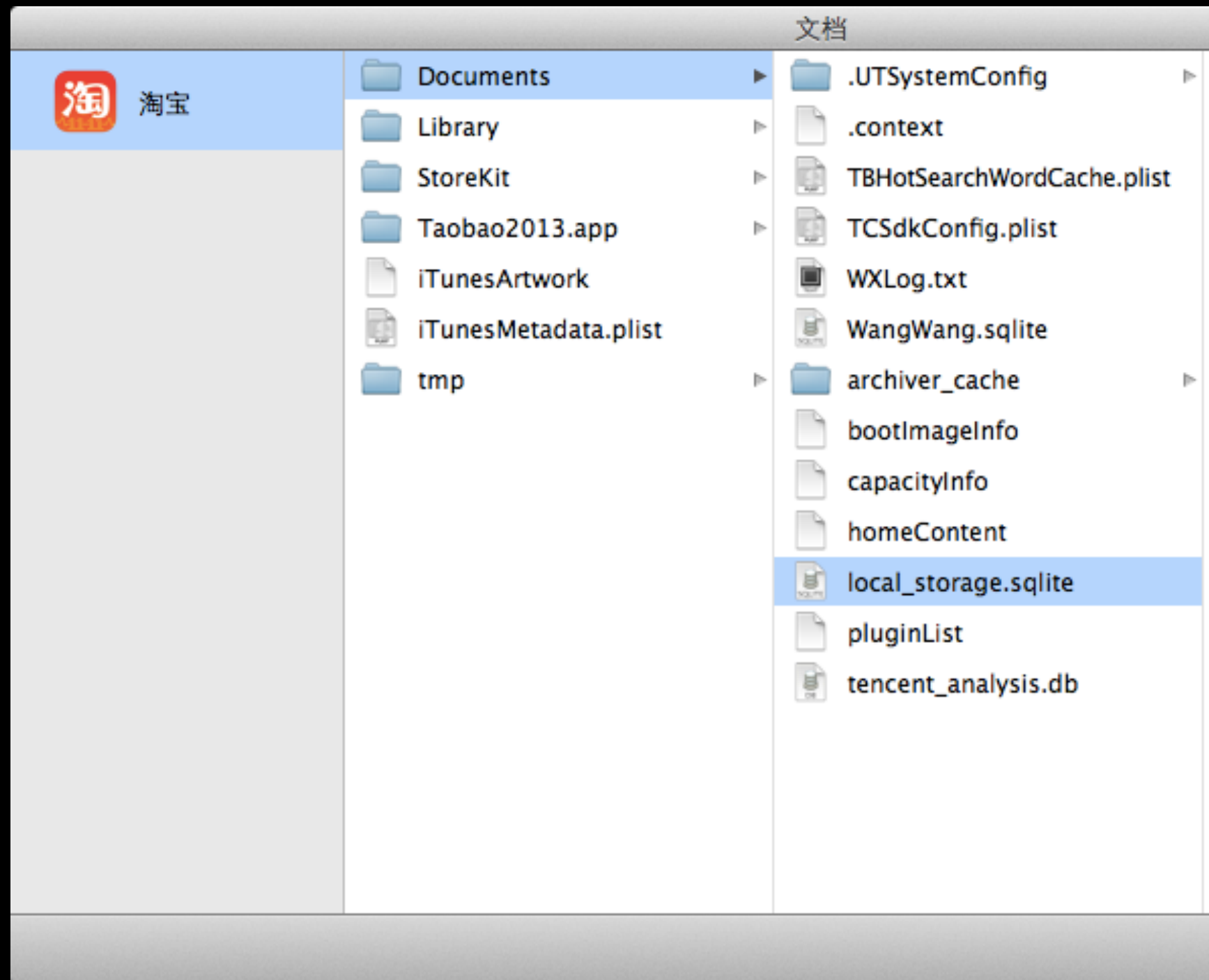
- How to defend?
  - encode password
  - binary protocol

# Local File/Data Security

```
qqapi.js
1  /**
2   * QQApi provides api for web pages which are embeded into qq client
3   * web pages could use these api to invoke client capabilities
4   * you may include this script in your page like this:
5   *
6   * <script src="http://qqlocal/api/qqapi.js"></script>
7   */
8  iOSQQApi = {
9      /**
10       * Helper method for opening an url
11       * @param url
12       */
13      _openURL: function(url){
14          //create an iframe to send the request
15          var i = document.createElement('iframe');
16          i.style.display = 'none';
17          i.onload = function() { i.parentNode.removeChild(i); };
18          i.src = url;
19          document.body.appendChild(i);
20
21          //read return value
22          var returnValue = iOSQQApi.__RETURN_VALUE;
23          iOSQQApi.__RETURN_VALUE = undefined;
24          return returnValue;
25      },
26  }
```

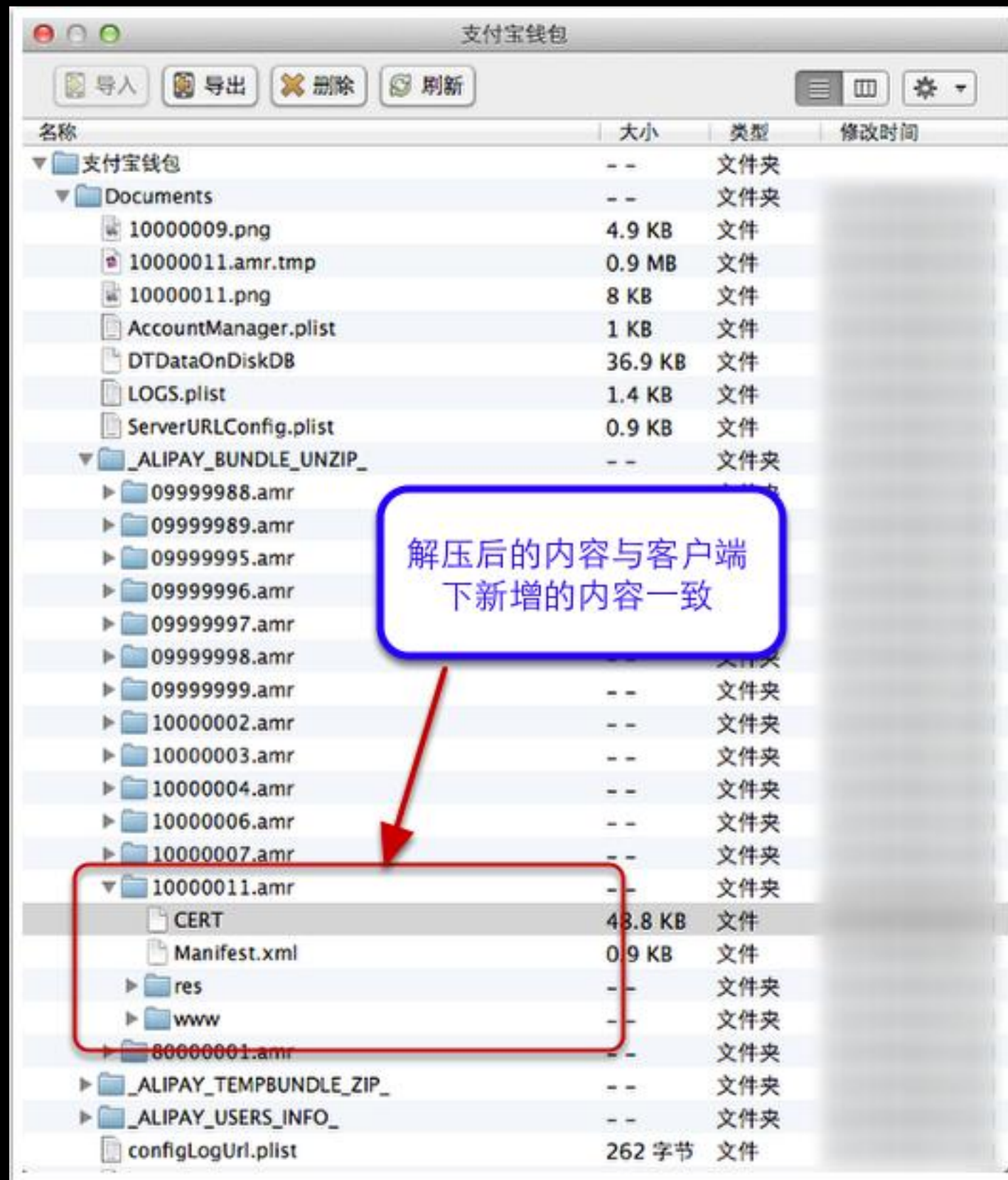


# Local File/Data Security

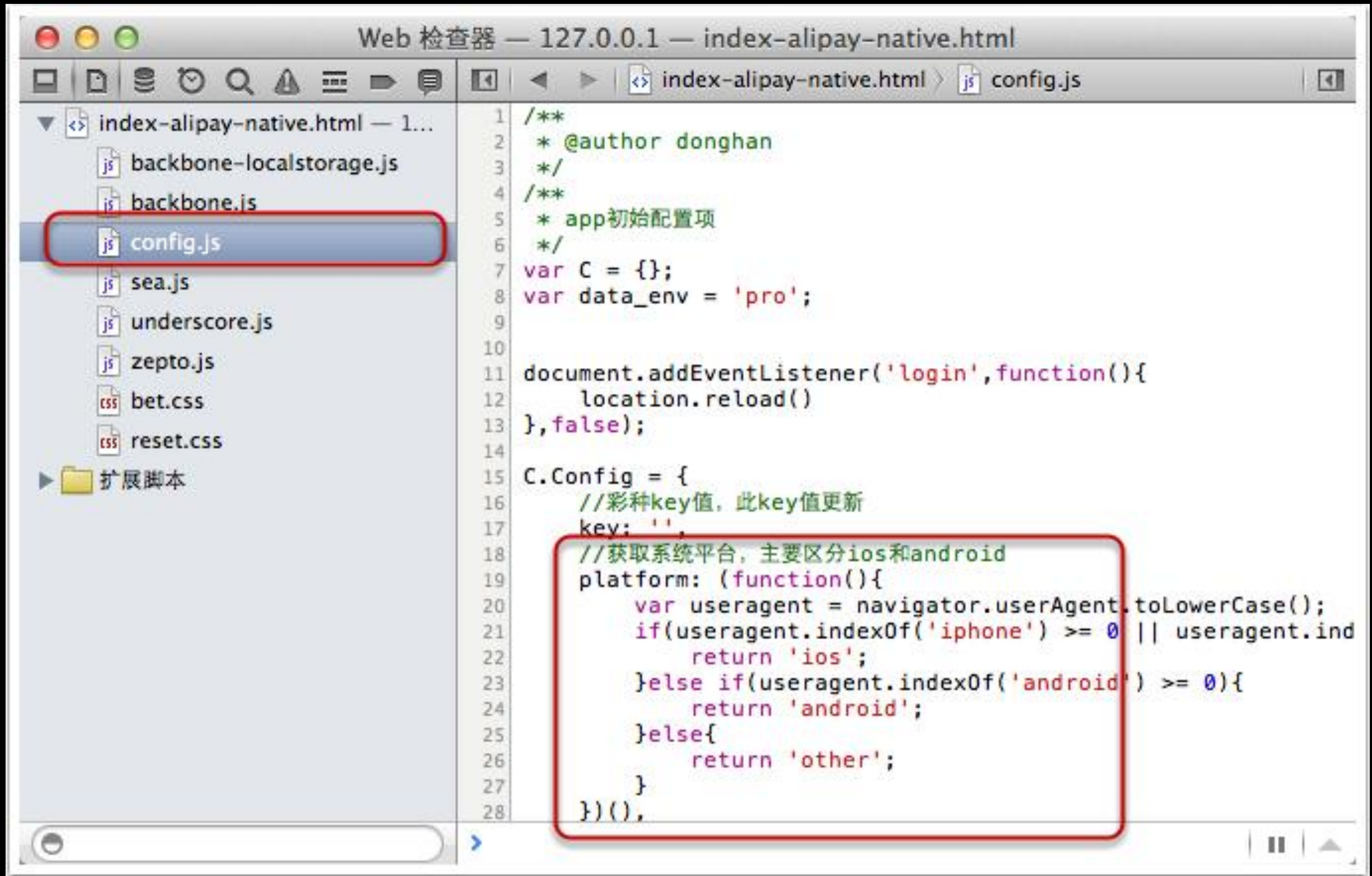




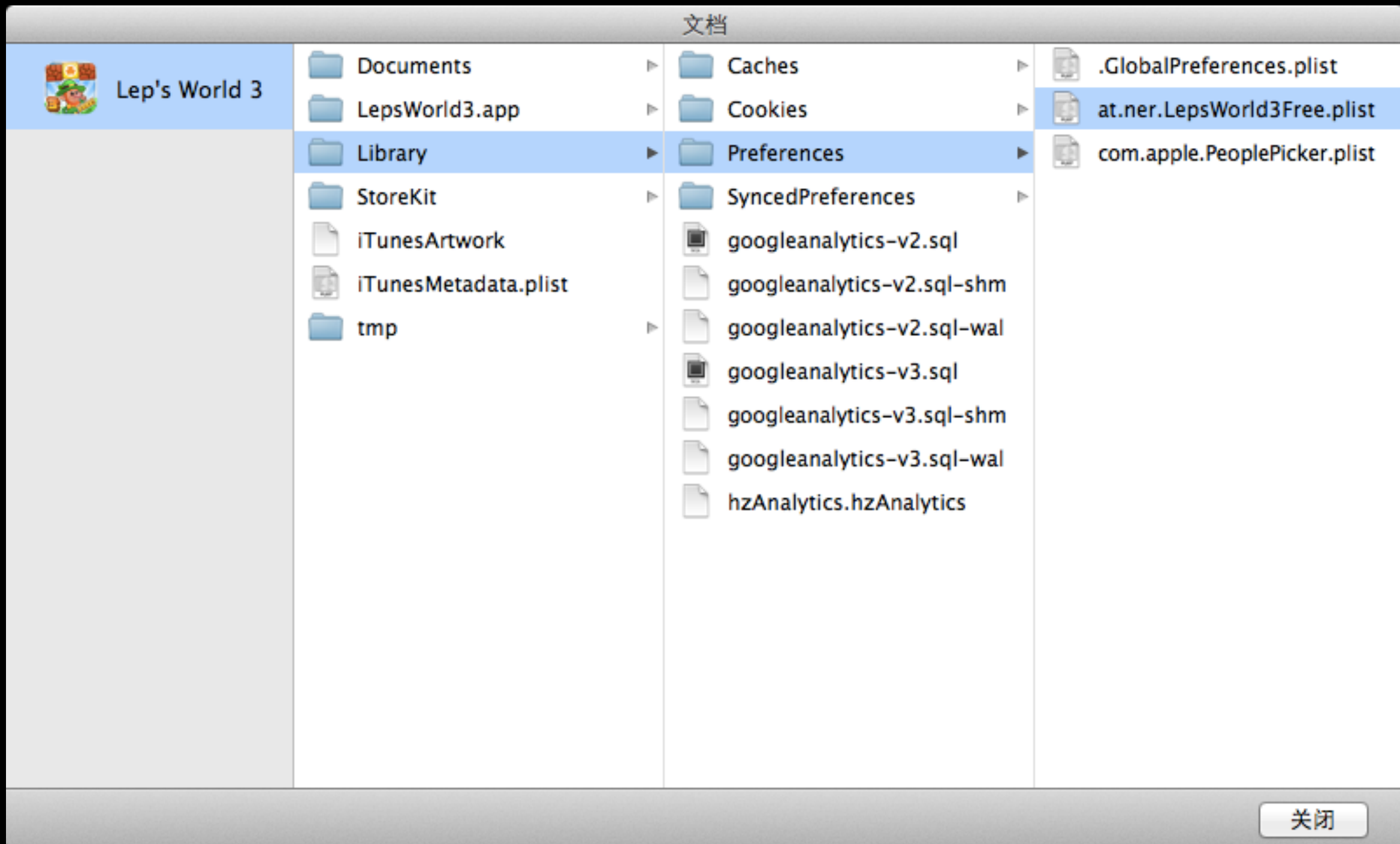
# Local File/Data Security



# Local File/Data Security

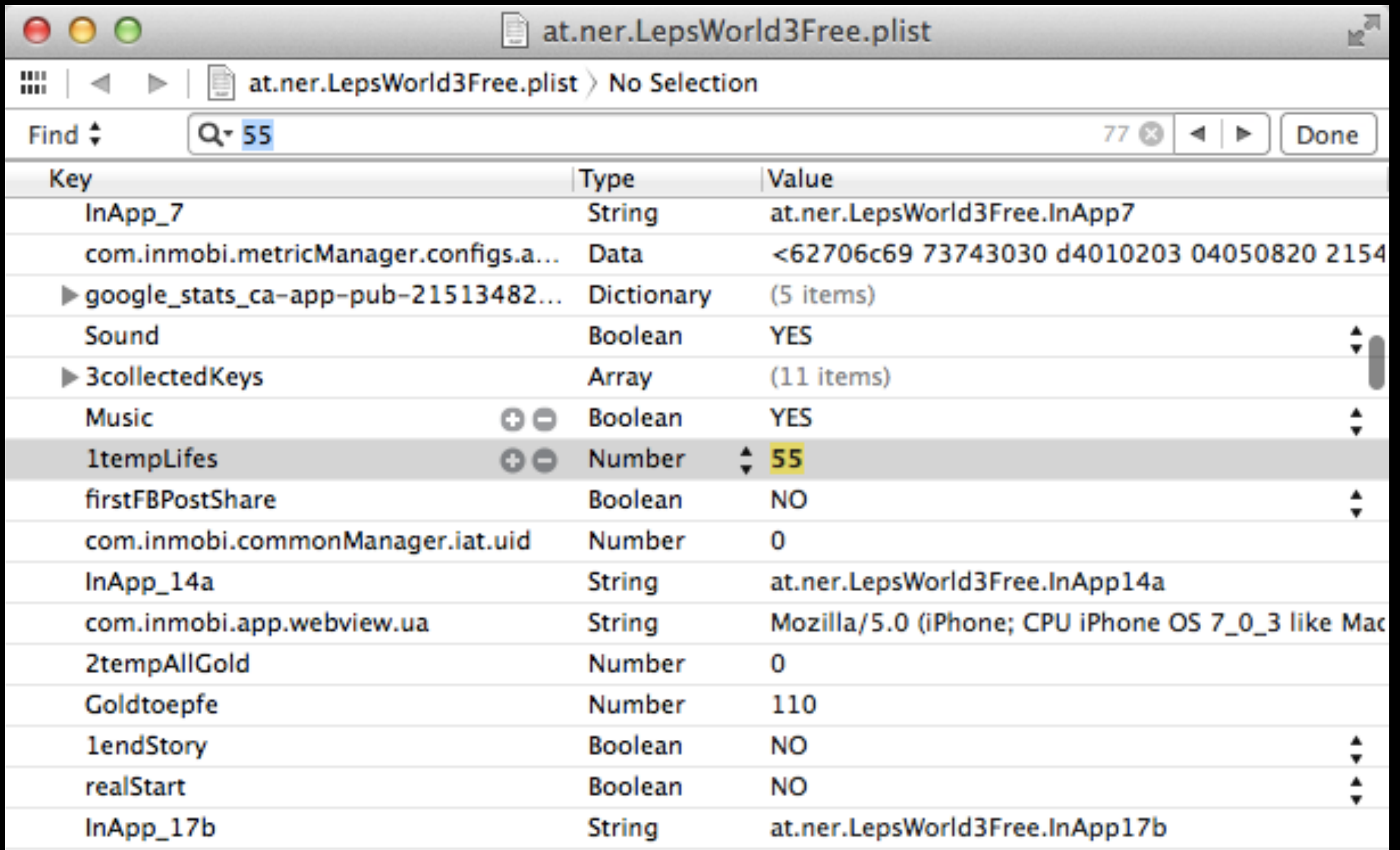


# Local File/Data Security





# Local File/Data Security



The image shows a macOS window titled "at.ner.LepsWorld3Free.plist". The window displays a list of keys and values from a plist file. A search bar at the top shows "55" and "77" matches. The key "1tempLives" is highlighted, showing its value as "55".

Key	Type	Value
InApp_7	String	at.ner.LepsWorld3Free.InApp7
com.inmobi.metricManager.configs.a...	Data	<62706c69 73743030 d4010203 04050820 2154
▶ google_stats_ca-app-pub-21513482...	Dictionary	(5 items)
Sound	Boolean	YES
▶ 3collectedKeys	Array	(11 items)
Music	Boolean	YES
1tempLives	Number	55
firstFBPostShare	Boolean	NO
com.inmobi.commonManager.iat.uid	Number	0
InApp_14a	String	at.ner.LepsWorld3Free.InApp14a
com.inmobi.app.webview.ua	String	Mozilla/5.0 (iPhone; CPU iPhone OS 7_0_3 like Mac
2tempAllGold	Number	0
Goldtoepfe	Number	110
1endStory	Boolean	NO
realStart	Boolean	NO
InApp_17b	String	at.ner.LepsWorld3Free.InApp17b

# Local File/Data Security

iphone/ipad 超级水管工3 Lep's World3 21亿生命+全人物道具解锁



价 格: **¥5.00**

物流运费: 广东湛江 | 至 北京 ~ 快递: 免运费

销 量: 30天内已售出 **1** 件, 其中交易成功 **0** 件

评 价: 暂无评价

宝贝类型: 全新 | 10次浏览

支 付: 快捷支付 网银支付 | 服务:

购买数量:  件 (库存99998件)

立即购买

加入购物车

你还可以:

喜欢

收藏宝贝

# Local File/Data Security



## 分析支付宝客户端的插件机制

<http://blog.devtang.com/blog/2013/06/23/alipay-plugin-mechanism/>

# Local File/Data Security

- How to defend?
  - encode
  - checksum
  - keychain



# Code Security

- file

➔ ipa file netease

netease: Mach-O universal binary with 2 architectures

netease (for architecture armv7): Mach-O executable arm

netease (for architecture armv7s): Mach-O executable arm

➔ ipa file qq

qq: Mach-O executable arm

➔ ipa file weixin

weixin: Mach-O executable arm

➔ ipa file ape

ape: Mach-O universal binary with 2 architectures

ape (for architecture armv7): Mach-O executable arm

ape (for architecture armv7s): Mach-O executable arm



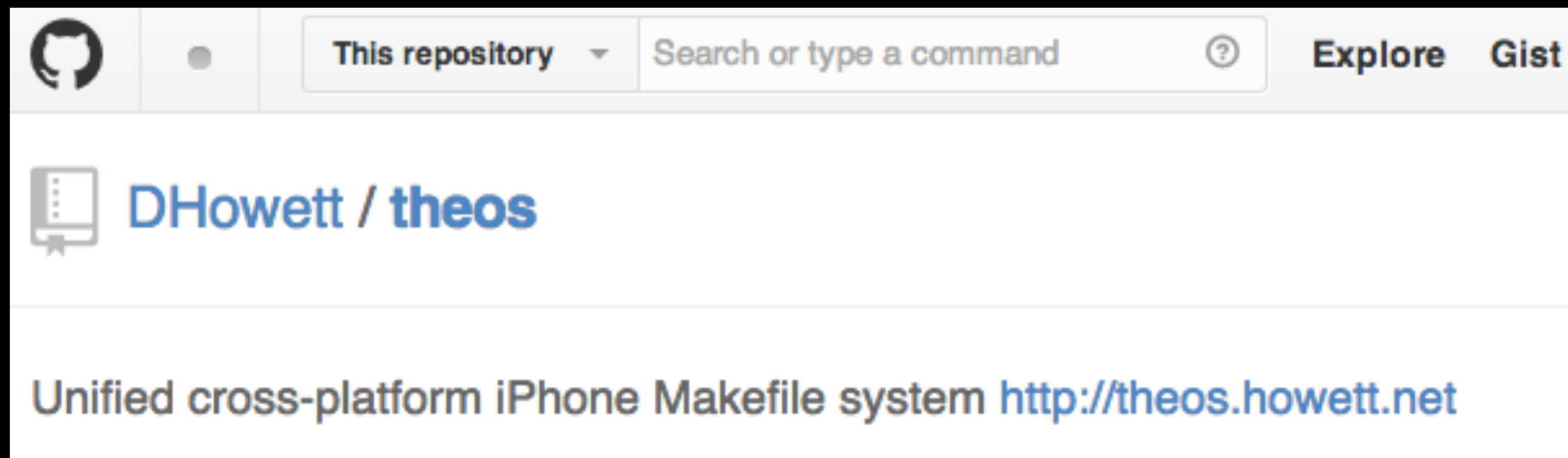
# Code Security

- otool

```
2. tangqiao@localhost: ~/work/crack/ipa (zsh)
..ork/crack/ipa (zsh)  ~/.bin (zsh)
→ ipa otool -l weixin | grep framework
name /System/Library/Frameworks/OpenAL.framework/OpenAL (offset 24)
name /System/Library/Frameworks/CoreText.framework/CoreText (offset 24)
name /System/Library/Frameworks/CoreTelephony.framework/CoreTelephony (offset 24)
name /System/Library/Frameworks/StoreKit.framework/StoreKit (offset 24)
name /System/Library/Frameworks/AdSupport.framework/AdSupport (offset 24)
name /System/Library/Frameworks/Accounts.framework/Accounts (offset 24)
name /System/Library/Frameworks/Social.framework/Social (offset 24)
name /System/Library/Frameworks/GLKit.framework/GLKit (offset 24)
name /System/Library/Frameworks/CoreBluetooth.framework/CoreBluetooth (offset 24)
name /System/Library/Frameworks/MediaPlayer.framework/MediaPlayer (offset 24)
name /System/Library/Frameworks/CoreMotion.framework/CoreMotion (offset 24)
name /System/Library/Frameworks/ImageIO.framework/ImageIO (offset 24)
name /System/Library/Frameworks/AssetsLibrary.framework/AssetsLibrary (offset 24)
name /System/Library/Frameworks/AVFoundation.framework/AVFoundation (offset 24)
name /System/Library/Frameworks/MessageUI.framework/MessageUI (offset 24)
name /System/Library/Frameworks/Foundation.framework/Foundation (offset 24)
name /System/Library/Frameworks/UIKit.framework/UIKit (offset 24)
name /System/Library/Frameworks/AddressBookUI.framework/AddressBookUI (offset 24)
```

# Code Security

- theos



# Code Security

- IDA



**IDA – The Interactive Disassembler**

Version 6.4.130322 (32-bit)

(c) 2013 Hex-Rays SA

Evaluation version  
with the following limitations:

1. Only PE/ELF/Mach-O files are supported
2. It is time limited
3. Save is disabled

[www.hex-rays.com](http://www.hex-rays.com)



# Code Security

```
if ([[VersionAgent sharedInstance] isUpgraded]) {
```

```
}
```

```
v6 =
```

```
v7 =
```

```
v41
```

```
objc
```

```
if (
```

```
{
```

```
NS
```

```
_o
```

```
v8
```

```
v9
```

```
_o
```

```
ob
```

```
}
```

```
AppDelegate.m:115:0
```

```
movl    -104(%ebp), %eax    ## 4-byte Reload
movl    L_OBJC_CLASSLIST_REFERENCES_$_89-L7$pb(%eax), %ecx
movl    L_OBJC_SELECTOR_REFERENCES_29-L7$pb(%eax), %edx
movl    %ecx, (%esp)
movl    %edx, 4(%esp)
calll   L_objc_msgSend$stub
movl    %eax, (%esp)
calll   L_objc_retainAutoreleasedReturnValue$stub
movl    -104(%ebp), %ecx    ## 4-byte Reload
movl    L_OBJC_SELECTOR_REFERENCES_91-L7$pb(%ecx), %edx
movl    %eax, %esi
movl    %esi, (%esp)
movl    %edx, 4(%esp)
movl    %eax, -132(%ebp)    ## 4-byte Spill
calll   L_objc_msgSend$stub
movl    -132(%ebp), %ecx    ## 4-byte Reload
movl    %ecx, (%esp)
movb    %al, -133(%ebp)    ## 1-byte Spill
calll   L_objc_release$stub
movb    -133(%ebp), %al    ## 1-byte Reload
cmpb    $0, %al
je      LBB7_4
```

```
## BB#3:
```

```
movl    -104(%ebp), %eax    ## 4-byte Reload
leal    L__unnamed_cfstring_93-L7$pb(%eax), %ecx
```

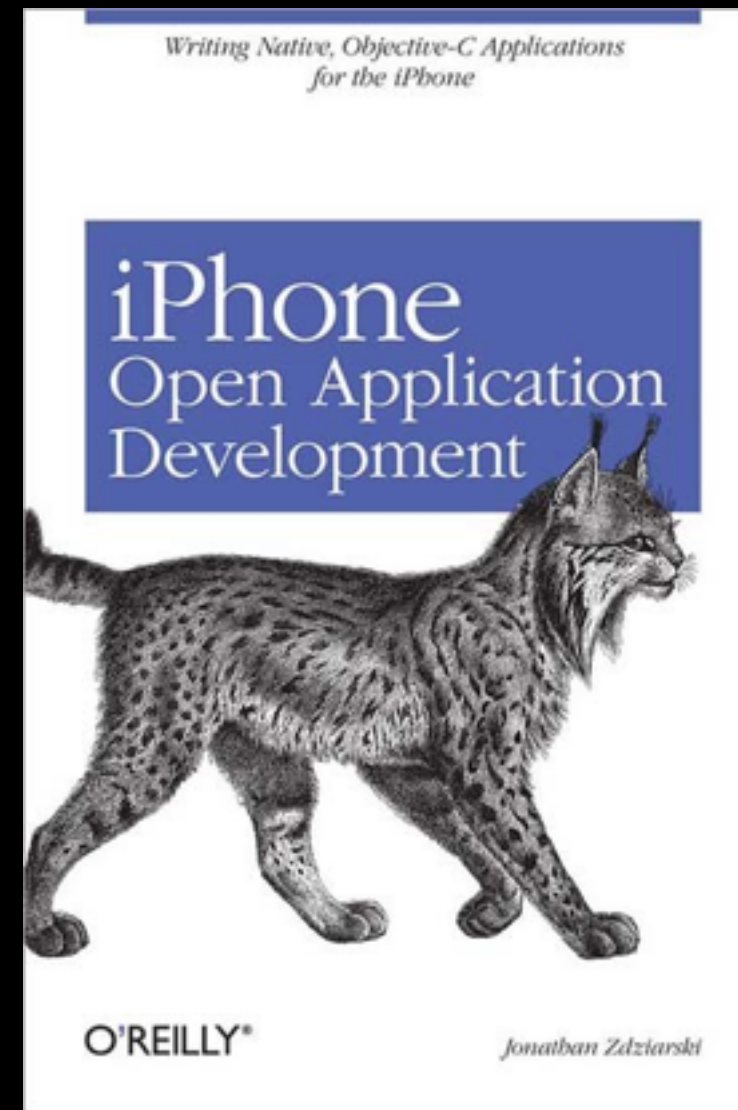
# Code Security

- How to defend against IDA?
  - Macro
  - pure C library

# Summary

iOS Security need attention!

# Resources - en



open jailbreak course: [http://www.reddit.com/r/jailbreak/comments/1nxoq7/openjailbreak\\_class/](http://www.reddit.com/r/jailbreak/comments/1nxoq7/openjailbreak_class/)

# Resources - cn



吴发伟翻译的安全相关的文章: <http://wufawei.com>



# Thanks & QA

- Sina Weibo: @唐巧\_boy
- 微信公众帐号: “iOSDevTips”

