Mobile Security Testing Workshop

Introduction to Practical Testing for Security Issues in Mobile Applications

Paco Hope CISSP CSSLP	Andrew Lee-Thorp
Principal Security Evangelist	Associate Principal Consultant
Cigital, Ltd London UK	Cigital, Ltd London UK
Email: paco@cigital.com Twitter: @pacohope	Email: alee-thorp@cigital.com



Introduction

- Name
- Role
- Experience/ background
- Which platform you're testing
 - Apple
 - Android
 - Web







Administration

- Course materials
 - Do you have Android dev kit?
 - Do you have Apple dev kit?
- Course timing
- Facilities
- Mobile phones
- Please ask questions





What you need

Android

- pandroid-sdk_r24.4.1windows.zip
- apktool_2.0.3.jar
- SimpleWebView.unaligned.apk
- burpsuite_free_v1.6.32.jar
- Torus.apk
- https-loader.apk

iOS

- XCode-Command-Line-7.3.1.dmg
- MobileTestTraining.zip
- burpsuite_free_v1.6.32.jar



About Cigital

Cigital is one of the world's largest application security firms helping organisations make secure software

We offer:

- Managed Services
- Professional Services
- Customized Products
- Remediation Guidance
- Security Programme Design Services
- Training

Cigital is headquartered near Washington, D.C. with regional offices in the U.S., London and India. <u>www.cigital.com</u>



Course Outline

- Motivation for Mobile Security Testing
- Setting up Tools and Environments
- Specific Problems to Test For
 - Insecure Storage
 - Proxying and testing web traffic (HTTP)
 - Proxying and testing web traffic (HTTPS)
 - Look for information leakage
- <Bypass client-side controls>
- <Test for client-side SQL injection>
- <Test for web views>

6

Agenda

Time	Duration	Description
9:00	0:45	Introduction
10:30	0:45	Getting familiar with the environment (iOS and Android)
11:00	0:30	Break
11:30	1:30	Some Security Tests for Common Mobile Vulnerabilities
13:00		Exeunt



Why Security Matters





App Failure #1: Local Data

RSA Conference App

- Included database of conference attendees in the app
- Database extracted by anyone who downloaded the app



RSA 2014: RSA Conference App Leaks Data On Thousands Of Users

Irony alert for RSA as its conference app found to leak data on users and is open to potential man-in-the-middle attacks

On February 27, 2014 by Thomas Brewster 🗔 0

Researchers have uncovered some worrying holes in the RSA 2014 Conference app for iOS and Android, leaking data of the thousands of users running the software on their phones.

The app, ironically one designed to help people around this week's security event, contains a weakness leaving it open to man-in-the-middle attacks, where an attacker could inject code into the login sequence to steal credentials.



It also downloads an SQLite database file used to populate visualisations, such as schedules and speaker information, but that file also contained information of every registered user of the software, ncluding name, surname, title, employer and nationality, security consultancy IOActive said in a **blog post**.

Irony alert for RSA

"I have no idea why the app developers chose t do that, but I'm pretty sure that the folks who downloaded and installed the application are unlikely to have thought that their details we being made public and published in this way. Marketers love this kind of information though."



App Failure #2: Storing Credentials

Starbucks Mobile App

🛞 money.cnn.com/2014/01/15/technology/security/starbucks-app-passworc 🔻 🕻 🚺 🕶 Google

NEW YORK (CNNMoney)

Starbucks' mobile app leaves customers' passwords open to attack, according to a research report.

The popular app, which allows Starbucks (SBUX) customers to purchase drinks and food directly from their smartphones, saves customers' usernames, passwords and other personal information in plain text. That means a hacker could pick up a left-behind phone, plug it into a laptop and easily recover a Starbucks customer's password without even knowing the smartphone's PIN code.



Stored userid/ password in the clear

• People reuse passwords!



How 'bout Those Credentials?

For example: Adobe and 38M Passwords

- Clear-text hints like "my work password"
- Trivially decrypted





Failure #3: Local Data

Local Database Stored on the Phone

Encryption key	paymentMethod	paymentExpYear
customerPassword	paymentCardType	paymentBillingCode
customerEmail	paymentCardNumber	customerPhone
deliveryStreet	paymentSecurityCode	longitude (of device)
deliveryState	paymentExpMonth	latitude (of device)
deliveryZip		email

- Stored sensitive data in the clear
- Could be recovered by adjacent malware



View in iTunes

Free

Category: Food & Drink Updated: Apr 12, 2014 Version: 3.12 Size: 31.9 MB Languages: English, French, Spanish Seller: ZippyYum LLC © 2012 ZippyYum LLC Rated 4+



The goal is **not** to detect a bad app before release.

The goal is to deliver a **good app**.









THE KINDS OF MOBILE APPS

Two Broad Classes, 2 Subclasses

(A) No Native Code

- Mobile-aware web site
- 2. WebView app

(B) Native Code

3. Hybrid / framework-based app
4. Full native code app



4 Kinds of Mobile App



App Type #1: Mobile-Aware Web Sites

- Not really a "mobile app"
- All HTML5/JavaScript lives on your "server"
- Can invoke mobile-specific JavaScript APIs in the mobile browser
 - GPS/Location
 - Upload Photo
- Easiest to test with desktop browser





Mobile Aware Web Sites

Desktop

Mobile



Track Your Weather









Track Your Weather





Regional Radar

Europe Severe Weather

Global Temperatures

Testing a Mobile Web Site

Ripple Chrome Extension

- Emulates mobile DOM
- Adjusts resolution
- Allows configuration of device version
- Out of date and unsupported 😕





App Type #2: WebView Mobile Apps

- Limited native code (e.g., Java, Swift, Objective-C)
- Lots of stuff installed in the mobile app
 - HTML5 / JavaScript / CSS
 - Assets: images, video, SQLite databases
- Access via JavaScript to some mobile functions
 - GPS
 - Photos / files
- Local data stored on the device (in app storage)



App Type #3: Hybrid / Framework

- Apache Cordova: Free and Open Source
- Adobe PhoneGap



- Creates uniform meta-platform that abstracts most differences between iOS / Android
- Native code can be added to access native functionality if needed





App Type #4: Fully Native

- Code written in supported language
 - iOS: Swift, Objective-C, C
 - Android: Java, C
- Developing / debugging is like working on a desktop app
 - Real binaries, debuggers
 - Simulators for devices you don't have







Lab 1: Getting Familiar with the Environment

Android iPhone





Getting Started (Android)

SDK + phone + USB cable

SDK + System Image

• • •		Android SDK	Manager				
SDK Pat	h: /Users/andrew/android-sdk-r	nacosx					
Packag	es						
	Name		API	Rev.	Status		
	SDK Platform Android N	Preview	N	2	Not installed		
	💷 Android TV Intel x86 Ato	m Svstem Imaae	N	2	Not installed		
	🍱 Intel x86 Atom 64 Svste	m Imaae	N	2	Not installed		
	🍱 Intel x86 Atom Svstem In	nade	N	2	Not installed		
	🔁 Android 6.0 (API 23)						
	Documentation for Andro	oid SDK	23	1	Not installed		
	🖷 SDK Platform		23	3	Not installed		
	💵 Android TV ARM EABI v7	'a Svstem Imaae	23	3	Not installed		
	💵 Android TV Intel x86 Ato	m Svstem Imaae	23	3	Not installed		
	💵 Android Wear ARM EABI	v7a Svstem Imaae	23	3	Not installed		
	💵 Android Wear Intel x86 A	tom Svstem Image	23	3	Not installed		
	💵 ARM EABI v7a Svstem In	nade	23	3	Not installed		
	💵 Intel x86 Atom 64 Svste	m Imaqe	23	9	Not installed		
\checkmark	🔜 🔤 Intel x86 Atom System Ir	nade	23	9	Not installed		
	📑 Gooale APIs ARM EABI v	7a Svstem Imaae	23	7	Not installed		
Show:	✓ Updates/New ✓ Installed	Select New or Updates			Install 4 packa	ages	
	Obsolete	Deselect All			Delete 1 pack	age	
Done loa	ading packages.					•	-09



Getting Started (Android)



Android Virtual Device Manager

 AVD Manager allows a graphical interface for creating, or starting different Android devices.

🖡 Android Virtual Device Manager						
List of existing Android Virtual Devices located at C:\Users\dlogan\.android\avd						
AVD Name	Target Name	Platform	API Level	CPU/ABI	New	
✓ Blank	Android 2.2	2.2	8	ARM (armeabi)	Edit	
✓ C2DM	Android 2.2	2.2	8	ARM (armeabi)		
✓ MarketTest	Android 2.2	2.2	8	ARM (armeabi)	Delete	
✓ Perms2	Android 2.2	2.2	8	ARM (armeabi)		
🗸 🗸 Simmy	Android 2.2	2.2	8	ARM (armeabi)	Kepair	
✓ TestNew	Market & Rooted (Google I	2.2	8	ARM (armeabi)	Detaile	
✓ New231	Android 2.3.1	2.3.1	9	ARM (armeabi)	Detalls	
✓ C233PO	Android 2.3.3	2.3.3	10	ARM (armeabi)	Start	

× An Android Virtual Device that failed to load. Click 'Details' to see the error.



Getting Started - Android Emulator



- The Android Emulator is installed with the Android SDK.
 - Allows full emulation of default hardware (Processor,
 - camera,sdcard,etc)
 - Allows redirection of networking (DNS, HTTP Proxy,etc)
 - Has full root access on the device.



Task: Create an Android Virtual Device

- 1. Run the "AVD Manager":/path/to-androidsdk/tools/android avd
- 2. Click on the "New" (top-right) and name the image "cigital".
- **3**. Target choose for example, "Android 2.2 API Level 8".
- 4. Choose "Hardware" section click "New".
- 5. In the "Property" field scroll down and select the entry
- 6. "SD Card Support" and click "Ok".
- 7. Enter a value of "100" MiB within the "Size" field for the SD Card.

Click "Create AVD".



Task: Start the emulator



\$ emulator -avd cigital \$ HAXM is working and emulator runs in fast virt mode emulator: emulator window was out of view and was recentered

emulator: UpdateCheck: current version '24.4.1', last version '24.4.1'

and active devices

```
$ ./android-sdk/platform-tools/adb devices
List of devices attached
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
emulator-5554 device
```

X86 acceleration available on OSX, Linux* and Windows for x86 targets



Task: Explore the emulator



	./android-sdk/tools/emulator -list-avds	
r	./android-sdk/platform-tools/adb devices	List active devices
View logs	adb logcat	
Copy files	adb push /Users/andrew/Shared/burp.crt /mnt/sdcard	
	adb install -r SimpleWebView.unaligned.apk	
	adb install -r https-loader.unaligned.apk	Install apps
Get root shell	adb shell	
L	* daemon not running. starting it now on port 5037 *	
	* daemon started successfully *	
	# ls /data/data	Explore file-system
	# ls /mnt/sdcard	
Package Manager	adb shell pm	
	adb shell am start -n	Use IPC
	<pre>Com.example.SimpleWebView/.MyActivity</pre>	
	Starting: Intent {	
	<pre>cmp=com.example.SimpleWebView/.MyActivity }</pre>	
		l



Getting Started (iOS)

- Download/Install XCode
 - Requires Apple Developer Account
 - (we have it on USB)
- Open the xcodeproject file







Choose to Run the Simulator



- Choose the Target
- Select a simulator (iPhone 6 Plus is fine)
- Click "run"
 - Simulator takes a while to start
- Can also run simulator alone



Expect a Few Bumps the First Time...

- Devices menu for registering your device
- Signing Key for your personal identity

• XCode can get you through these easily...





Failed to code sign "training".

No valid signing identities (i.e. certificate and private key pair) matching the team ID "6T9C62RV29" were found.

Xcode can attempt to fix this issue. This will reset your code signing and provisioning settings to recommended values and resolve issues with signing identities and provisioning profiles.





Sensitive Data Exposure

In transit and at rest





SensitiveData Exposure

The main problems associated with sensitive data exposure

- Improper classification: Failing to recognize the sensitivity level of the data in the application
- Lack of authorization: Failing to ensure that the current user is allowed to view the requested information





Sensitive Data Exposure

Test for exposure of sensitive data in transit:

- Check for sensitive data being transferred in plain text HTTP
- Look at URL parameters, form fields, cookies, and other HTTP parameters
- Verify that connections are not easily compromised by man-in-the-middle (MITM) attacks





Data at rest

Storage of Sensitive Data

- Discussion of secure storage is nuanced
- In this discussion of sensitive we include things that are important to the correct function of the app itself.

Two things to test that the application should never be doing:

- 1. Logging sensitive data
- 2. Hard-coding sensitive data in the application itself (credentials, hidden URLs, etc.)


Lab2: Insecure Storage

Looking for information leakage in logs Looking for hard-coded sensitive data





Task: Scan for hard-coded strings (iOS)

- 1. In XCode: Product -> Build (or Build For)
- 2. Locate the build: Select *training*-> Show in Finder
- 3. Run strings against the build
- 4. Look for hard-coded secrets

\$ strings /path/to/Build/Products/Debugiphonesimulator/training.app/training CustomCacheViewControllerNSURLConnectionDelega

	Image: A training in the second se	
E		
 training training training training Custor Mappbe Mappbe Mienze Mienze Main.s Assets 	nCache.h nCache.m legate.h legate.n ontroller.h ontroller.m .Request+IgnoreCertValidation.h .Request+IgnoreCertValidation.m toryboard .xcassets	М
Info.pli ► Suppo ▼ Products	ist rting Files	
🕂 trainin	Show in Finder	
🔺 trainin	Show in Finder Open with External Editor Open As Show File Inspector	
🙏 trainin	Show in Finder Open with External Editor Open As Show File Inspector New File Add Files to "training")
🚧 trainin	Show in Finder Open with External Editor Open As Show File Inspector New File Add Files to "training" Delete	
∳ ₹ trainin	Show in Finder Open with External Editor Open As Show File Inspector New File Add Files to "training" Delete New Group New Group from Selection	
∳ trainin	Show in Finder Open with External Editor Open As Show File Inspector New File Add Files to "training" Delete New Group New Group New Group from Selection Sort by Name Sort by Type	
∳ ₹ trainin	Show in Finder Open with External Editor Open As Show File Inspector New File Add Files to "training" Delete New Group New Group from Selection Sort by Name Sort by Type Find in Selected Groups	
∳ ₹ trainin	Show in Finder Open with External Editor Open As Show File Inspector New File Add Files to "training" Delete New Group New Group from Selection Sort by Name Sort by Type Find in Selected Groups Source Control	



Task: Scan for hard-coded strings (Android)

- 1. Unzip the file *Torus.apk*
- 2. Run *strings* against *classes.dex*

And/or

- 3. Run java jar apktool.jar d Torus.apk
- 4. Look for secrets in the file Constants.smali





Task: Information leakage in logs (iOS)

- Start the training app
- Enter example.com
- Click HTTP
- Watch the simulator log
- There are a few ways to do this ...





... use the system logs

	s 😥 🎽 🚺	Q Search
Hide Log List Clear Display Relo	ad Ignore Sender Insert Marker Inspector	Filter
SYSTEM LOG QUERIES	May 9 15:39:39 Andrews-MBP trainagenerations: [MPUSystemmediatentrois] updating supported commands for now playing applicat.	Lon.
All Messages	May 9 13:39:39 Andrews-MBP training[1655]: OAT basic auth - sysadmin:p@ssw0rd_h1dd3n	
	May 9 13:39:39 Andrews-MBP training[1655]: Password incorrect. Expected: TheDog8TheHamburg3r	
DIAGNOSTIC AND USAGE INFORMAT	May 9 13:39:39 Andrews-MBP assertiond[1585]: assertion failed: 15E65 13E230: assertiond + 15801 [3C808658-78EC-3950-A264-79]	A64E0E463B]: 0x1
Diagnostic and Usage Messages	Nay 9 13:39:40 last message repeated 2 times	
User Diagnostic Reports	May 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) IndexCl in _data_map_get_data_ld:1213: added 265 to 0x7fee3a612210 May 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) IndexCl in _data_map_get_data_id:1213: added 265 to 0x7fee3a6	
System Diagnostic Reports	May 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) IndexCI in _data_map_get_data_id:1213: added 287 to 0x7fee5a612210	
EIL ES	May 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) IndexCI in _data_map_get_data_id:1213: added 288 to 0x7fee5a612210 May 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) IndexCI in _data_map_get_data_id:1213: added 288 to 0x7fee5a612210	
austem lag	May 9 13:39:40 Andrews-HBP searchd[1649]. (Normal) IndexCI in _data_map_get_data_id:1213: added 290 to 0x7fe5a612210	
system.log	May 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) IndexCI in _data_map_get_data_id:1213: added 291 to 0x7fee5a612210	
~/Library/Logs	May 9 13:33:40 Andrews-mbP search0[1040]: (Normal) IndexCl in _data_map_get_data_l0:1213: added 292 to 0x7te5a612210 May 9 13:39:40 Andrews-MBP search0[1648]: (Normal) IndexCl in _data_map_get_data_l0:1213: added 292 to 0x7te5a612210	
Baseband	Maý 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) IndexCI in _data_map_get_data_id:1213: added 294 to 0x7fee5a612210	
com.apple.Notes	May 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) IndexCI in _data_map_get_data_id:1213: added 295 to 0x7fee5a612210	
▼ CoreSimulator	May 9 13:39:40 Andrews-mbr searchd[1649]. (Normal) IndexCI in _data_map_get_data_10:113: added 290 to 0x7fee3a012210	
CoreSimulator.log	May 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) IndexCI in _data_map_get_data_id:1213: added 298 to 0x7fee5a612210	
▼D47880C5-6095-4F4A-B8B7	may 9 13:39:40 Andrews-MBP searchd10481: (Normal) IndexcI in _data_map_get_data_10:1713: added 299 to 0x/reesab12210 May 9 13:39:40 Andrews-MBP searchd16481: (Normal) IndexcI in _data map get data id:1213: added 300 to 0x/reesab12210	
▶ asl	Maý 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) IndexCI in _data_map_get_data_id:1213: added 301 to 0x7fee5a612210	
com.apple.clouddocs.asl	May 9 13:39:40 Andrews-MBP searchd116481: (Normal) IndexCI in _data_map_get_data_id:1213: added 302 to 0x7fee5a612210 May 9 13:39:40 Andrews-MBP searchd116481: (Normal) IndexCI in _data_map.get_data_id:1213: added 303 to 0x7fee5a612210	
▶ com.apple.revisiond	May 9 13:39:40 Andrews-MBP searchd[1648]; (Normat) IndexCI in _data_map_get_data_id:1213; added 304 to 0x7fee5a612210	
► CrashPeporter	May 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) IndexCI in _data_map_get_data_id:1213: added 305 to 0x7fee5a612210	
	May 9 13:39:40 Andrews-mbr searchulio40; (Normal) IndexCI in _data map_get_data_10:1213; added 307 to 0x7fe5a612210	
P Diagnosticmessages	May 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) IndexCI in _data_map_get_data_id:1213: added 308 to 0x7fee5a612210	
► Handoff	May 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) IndexCI in _data_map_get_data_id:1213: added 309 to 0x/fee5ab12210 May 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) IndexCI in _data_map.get_data_id:1213: added 310 to 0x/fee5ab12210	
MobileContainerManager	May 9 13:39:40 Andrews-MBP search(1648): (Normal) IndexCI in _data_map_get_data_i(1:1213: added 311 to 0x7fee3a612210	
MobileInstallation	May 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) IndexCI in data_map_get_data_id:1213: added 312 to 0x7fee5a612210	
SMSMigrator	May 9 13:39:40 Andrews-MBP search(1648): (Normal) IndexCI in _data_map_get_data_d121123: added 314 to 0x/fee5a612210	
system.log	May 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) IndexCI in _data_map_get_data_id:1213: added 315 to 0x7fee5a612210	
▶ Ubiquity	May 9 13:39:40 Andrews-MbP searchd16481: (Normal) indexcl in _data_map_get_data_ld:1/13: added 31b to 0%/Teesab1/2/10 May 9 13:39:40 Andrews-MbP searchd16481: (Normal) Indexcl in _data map get data id:1213: added 317 to 0%/Teesab2	
Simulator.log	Maý 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) IndexCI in _data_map_get_data_id:1213: added 318 to 0x7fee5a612210	
CoreTelephonyTraceScratch	May 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) Index[I in _data_map_get_data_id:1213: added 319 to 0x7fee5a612210 May 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) Index[I in _data_map.get_data_id:1213: added 320 to 0x7fee5a612210	
▶ DeviceLink	May 9 13:39:40 Andrews-MBP search(1648): (Normal) IndexCI in _data_map_get_data_id:1213: added 321 to 0x7fee5a612210	
▶ DiagnosticReports	May 9 13:39:40 Andrews-MBP searchd[1648]: (Normal) IndexCI in _data_map_get_data_id:1213: added 322 to 0x7fee5a612210	
fack bfa log	May 9 15:35:40 Andrews-mbr Searchulio40; (Normal) IndexCI in _data_map_get_data_10:1213: added 9 to 0x7/ee5a612210 May 9 13:39:40 Andrews-MBP Searchulio40; (Normal) IndexCI in _data_map_get_data_10:1213: added 9 to 0x7/ee5a612210	
h Handoff	May 9 13:33:40 Andrews-MBP assertiond[1585]: assertion failed: 15E65 13E230: assertiond + 15801 [3C808658-78EC-3950-A264-79	\64E0E463B]: 0x1
	may y 13:39:40 tast message repeated / times May 9 13:39:40 Andrews-MBP dataaccess(1657): 0x7th656602df0lDAlFrorIspinnerIdentifiers to be implemented by subclass	
► SMSMIgrator	May 9 13:39:40 Andrews-MBP dataaccessd[1657]: 0x7fb650602df0[DA Error]	
SparkleUpdateLog.log	Possible Failure: Cal db has retain count > 1 of 2	
▶ Sync	May 9 13:39:40 Andrews-MBP dataaccess(1657): 0x7b658602df0[DA[Error spinnerIdentifiers to be implemented by subclass	
talagent.log	May 9 13:39:40 Andrews-MBP dataaccessd[1657]: 0x7fb650602df0[DA Error]	
	Size: 268 KB	Earlier Later Now



... Activate Console (XCode)



... Window -> Devices (XCode)

		Minimize	36M			
Device Information		Zoom				
Namo	HexPlus	Show Next Tab	92)			
Model	iPhone 6 Plus	Show Previous Tab	22.1			
Capacity	55.49 GB (3.43 GB available)					
Battery	45%	Documentation and API Reference	企第0			
iOS	9.3.2 (13F68)	Welcome to Xcode	081			
Identifier	059ede4eb4098f621b8bf2be0c5bde9c62872f4f	Devices	17362			
		Projects				
View Device Logs	Take Screenshot	Package Manager	企 將9			
		Dalars All de Count				
Paired Watches		Bring All to Front				
Name	Model watchOS Identifie	training – NiewController.m				
Installed Apps						
Name	Version Identifier					
training	1 com.cigital.qa.training					
Blitzkrieg	1 com.priyank.Blitzkrieg					
keychainServices	1 hexplo.it.keychainServices					
+ - 1 283						
7						
2						
] y 9 13153;53 Mea2 9 3 133;53 Mea2	Pan kermija) objican gandhari training(DB) deur Tun training(DB) okeraingn Attaupling to comest	 (1) file-read-date /priorite/ser/section to https://secangla.com.via.mtTP3 	Containers/Bata/AppLication/7#FF	1948-8012-1(19-8)11-411778148963	/Library/Caches/Saspabots	
2 9 9 13153153 Mex7 9 9 131535 Mex7 9 9 131535 Mex7	Pan kermel(é) -derlice-) fandbar: training(53) dany Tan training(53) -derring- Attempting to consect Jan training(53) -derring- Recoduré das Fran ar	 (1) file-read-data /private/sar/asbite to https://asample.com.via.mtm3 	Containers/Bata/Application/7#FM	1988 - 800 - 4037- 801 - 4417781483431	1Lbray/Gebes/Saspabets	
2 9 9 13133353 Mex2 9 9 13133353 Mex2 9 9 1313335 Mex2 9 9 1313355 Mex2 9 9 1313355 Mex2	fun kermija) -detion-fandkur krainig(20) davi Um trainig(20) -derring- Attenting to comet Um trainig(20) -derring- Recived dat from er Nermalija -derring- Recived dat from er	 (1) file-controls /prior /prior to https://assayle.com via ortiga ver ver if ite-write-write-prior /prior /prior /prior 	Containers/Bats/Application/FAF9 14/Containers/Dats/Application/FAF9 24/Containers/Dats/Application/FAF9	1946 &CT -(CY - 8C1 - 441771148363 V13368 & RCT - 4C7 - 8C1 - 441771148363	/Library/Caches/Snapshots 93/Library/Caches 93/Library/Caches	
2 99 9 13133153 Recx 97 9 131333 Recx 97 9 131335 Recx 97 9 131335 Recx 97 9 131335 Recx 97 9 131335 Recx 97 9 1313355 Recx 97 9 1313355 Recx	Pan keral(d) delidar) fandhari training(D3) dary Tan training(D3) darriaps Actaepting to consect Tan training(D3) darriaps Accaded das Fran se Tan keral(1) delidar) hannan training(D3) dary Tan keral(1) delidar) fandhari training(D3) dary Tan keral(1) delidar) fandhari training(D3) dary	 (1) file-read-data /privata/sat/sabila (2) file-read-data /privata/sat/sabila (3) file-rife-satiah /privata/sat/sability (3) file-rife-satiah /privata/sat/sability (3) file-rife-satiah /privata/sat/sabilaty 	Containers/Bata/Application/7847 LarGontainers/Data/Application/7847 LarGontainers/Data/Application/ LarGontainers/Data/Application/	1988-8021-(57-8012-481771448363) 193948-8021-407-8012-481771448363 193948-8021-407-8014-48177144	/Library/Geches/Snapsbots 307/Library/Geches 303/Library/Geches 303/Library/Geches	
2 9 9 131133153 Mear 9 9 13113333 Mear 9 9 1313333 Mear 9 9 1313335 Mear 9 9 1313355 Mear 9 9 1313355 Mear 9 9 1313355 Mear 9 9 1313355 Mear	fun termila) obstino fanden terining(D) des us traking(D) obstino fanden terining(D) conset us traking(D) obstino fanden terining(D) obs marrail() obstino fanden terining(D) obs us terini() obstino fanden terining(D) des us terini() obstino fanden terining(D) des us terini() obstino fanden terining(D) des	 (1) file-real-date /printer/or/amble (2) file-real-date /printer/or/amble (3) file-rite-amble /printer/or/amble (4) file-rite-amble /printer/or/amble 	Containers/Bats/Application/PAP 1.= Containers/Data/Application/PAP 1.= Containers/Data/Application/ 1.= Containers/Data/Application/ 1.= Containers/Data/Application/ 1.= Containers/Data/Application/	1998-800 -007-8014-641776148363 V131984 8801 -007-8014 -0177614 V131984 8801 -017-8014 -0177614 V131984 8801 -017-8014 -0177614 V131984 -8001 -017-8014 -0177614	/Library/Caches/Snapshots 187/Library/Caches 187/Library/Caches 187/Library/Caches/Snapshot	:
2 97 8 23 183 63 Max7 97 8 23 183 63 Max7 9 23 13 33 8 Max7 9 23 13 35 8 Max7	An termi(0) dericas: Sandbar: training(039) dauy Tan training(03) derrings: ActuaryIng to contect un training(03) derrings: ActuaryIng to contect un termi(0) deticas: Sandbar: training(03) deu ma termi(0) deticas: Sandbar: training(03) deu	 file-read-data /private/ver/umbile/ vertical/seample.com via HTTPS vertical/seample/ if file-rite-seample/ if file-rite-seample/ if file-rite-seample/ if file-rite-seample/ private/seample/	Containers/Data/Application/78/19 lar/Containers/Data/Application/ lar/Containers/Data/Application/ lar/Containers/Data/Application/ Pacetainers/Data/Application/FAFT Containers/Data/Application/FAFT	1984 8CC - (C7 - 8CL - 40177114836) N7394 8CC - (C7 - 8CL - 40177114 N7394 8CC - 6(7 - 8CL - 40177114 N7394 8CC - (C7 - 8CL - 40177114 1984 8CC - 4(7 - 8CL - 40177114836)	YLlbrary/Caches/Snapshots 383/Llbrary/Caches 383/Llbrary/Caches 381/Llbrary/Caches 381/Larry/Caches 381/Larry/Caches/Snapshots	:
2 9 9 1313153 Mac/ 9 9 1313333 Mac/ 9 9 1313333 Mac/ 9 9 1313335 Mac/ 9 9 1313355 Mac/ 9 131355 Mac/ 9 131555 Mac/ 9 13155 Mac/ 9 131555 Mac/ 9 1315555 Mac/ 9 1315555 Mac/ 9 13155555555555555555555555555555555555	<pre>fun brenits: bettien: fundeau training(D3) dawy Un training(D3) -waring- Attempting to conset Un training(D3) -waring- Rectived data from ar warea (L) dwices: Sandau training(D3) day Un training(D3) -waring- Rectived (D3) day Un training(D3) -waring- Na training(D3) -waring- Attempting to conset Un training(D3) -waring- Attempting to conset</pre>	(1) file-read-date /priorte/up/teblty to https://dompie.com/se TTTS VF 10 file-rite-rite-file/priorte/ur/mobil 10 file-rite-rite-file/priorte/ur/mobil 11 file-rite-rite-file/priorte/ur/mobil 11 file-rite-rite-file/priorte/ur/mobil 11 file-rite-rite-file/priorte/ur/mobil 10 file-rite-rite-file/priorte/ur/mobil 10 file-rite-rite-file/priorte/ur/mobil 10 file-rite-rite-file/priorte/ur/mobil 10 file-rite-rite-file/priorte/ur/mobil 10 file-rite-rite-rite/priorte/ur/mobil	Containers/Bats/Application/PAP 1.=/Containers/Dats/Application/PAP 1.=/Containers/Dats/Application/ 1.=/Containers/Dats/Application/ 1.=/Containers/Dats/Application/ Containers/Dats/Application/PAP 1.=/Containers/Dats/Application/PAP	588-827-407-8214-441775148363 973598-8821-407-8214-41775148 97358-8821-407-8214-4177564 97358-821-407-8214-4177564 97358-821-407-8214-4177514 984-8221-407-8214-4177514 984-8221-407-8214-4177514	/Library/Caches/Snapshots 192/Library/Caches 193/Library/Caches 193/Library/Caches/Snapshot Library/Caches/Snapshot Library/Caches/Snapshot	:
2 97 9 3.3 1.53 5.5 Head 97 9 3.3 1.53 5.5 Head 98 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	Tun kerni(2) Obtices Landbas training(039) days an training(139) darining Artapeting as result as kerni(13) obtices Landbas training(130) days (14) kerni(14) obtices Landbas training(130) days	 file-raad-data /privata/wac/usbile to papa//wacmpis.com vis HTFS file-rite-miles /privata/wacmpis.com in file-rite-miles /privata/wacmpis.com in file-rite-miles /privata/wacmpis.com in file-rite-miles /privata/wacmpis.com in file-rite-miles /privata/wacmpis.com file-rite-miles /privata/wacmpis.com 	Containers/Data/Application/74/7 lar/Containers/Data/Application/ lar/Containers/Data/Application/ / Containers/Data/Application/747 Containers/Data/Application/747 Containers/Data/Application/747 Lar/Containers/Data/Application/747	1948 - 800 - 407 - 801 - 441771449163 V13194 - 800 - 407 - 801 - 441771449 V13194 - 800 - 407 - 801 - 4417714 1948 - 800 - 407 - 801 - 4417714 1948 - 800 - 407 - 801 - 44177144 V13194 - 800 - 407 - 801 - 44177144	/Library/Caches/Saspabuts 887/Library/Caches 887.Library/Caches 887.Library/Caches 987.Library/Caches 1.Sprary/Caches 887.Library/Caches 887.Library/Caches	:
2 3	Can break[a) deption: familiary braining(20) dawy Un training(20) derrings: Attacpting to consect un training(20) derrings: Rectived data from ar anaralli derices: Sandau training(20) der um training(20) derrings: Rectived data from ar um training(20) derrings: Attaching (20) der um training(20) derrings: Attaching(20) der um training(20) der um training(20) der um training(20) de	(1) file-sud-date /priorte/up/amble/ to https://asample.com.vie.mttps/ ver interview.intervie	Containers/Bats/Application/PAP 1.= Containers/Dats/Application/PAP 1.= Containers/Dats/Application/ 1.= Containers/Dats/Application/ Containers/Dats/Application/ Containers/Dats/Application/ Tac/Containers/Dats/Application/ 1.= Containers/Dats/Application/ 1.= Containers/Dats/Application/ 1.= Containers/Dats/Application/ 1.= Containers/Dats/Application/ 1.= Containers/Dats/Application/	564 802 -007 801 -401776148363 901004 802 -07 801 -0177614 90104 802 -07 801 -0177614 90104 802 -07 801 -0177614 90104 802 -07 801 -0177614 90104 802 -07 801 -0177614 90104 802 -07 801 -0177614 90104 802 -07 -014 -017614 90104 802 -07 -014 -017614 90104 802 -07 -014 -017614 90104 802 -07 -014 -017614 90104 802 -07 -014 -0177614 90104 802 -07 -014 -0177614 90104 802 -07 -014 -0177614 90104 802 -07 -014 -0177614 90104 802 -07 </td <td>/Library/Caches/Snapshots 187/Library/Caches 187/Library/Caches 187/Library/Caches/Snapshot Library/Caches/Snapshot 187/Library/Caches 187/Library/Caches 187/Library/Caches 187/Library/Caches</td> <td>:</td>	/Library/Caches/Snapshots 187/Library/Caches 187/Library/Caches 187/Library/Caches/Snapshot Library/Caches/Snapshot 187/Library/Caches 187/Library/Caches 187/Library/Caches 187/Library/Caches	:
2 9 8 13 53 Maxed 9 9 13 13 54 Maxed 9 9 13 13 53 Maxed 9 13 13 53 Maxed Maxed 9 13 13 53 Maxed Maxed 9 13 13 55 Maxed Maxed 9 13	<pre>ins terms[2] Optice: insthut training(037) day ins training(137) data and instanting instanting instanting(137) data and instanting instanting instanting(137) data and instanting(137) day instanting(137) data and instanting(137) data and instanting(137) data and instanting(137) data and instanting (137) data and instanting (137) data and instanting (137) data and instanting (137) data and instanting (137) d</pre>	 (1) file-read-data /private/vac/ubile/ to papa//scampte.com vis HTTPS (1) file-rite-rite-state /private/vac/ubile/ (1) file-rite-rite-state /private/vac/ubile/ (1) file-rite-rite-state /private/vac/ubile/ (1) file-rite-rite-state /private/vac/ubile/ (1) file-rite-rites/private/vac/ubile/ (1) file-rite-rites/private/vac/ubile/ (1) file-rite-rites/private/vac/ubile/ (1) file-rites/private/vac/ubile/ (1) file-rites/privat	Containers/Data/Application/74/7 La Containers/Data/Application/74/7 La Container/Data/Application/7 Containers/Data/Application/74/7 Containers/Data/Application/74/7 Containers/Data/Application/74/7 La Containers/Data/Application/74/7 La Containers/Data/Application/74/7 La Containers/Data/Application/74/7 La Containers/Data/Application/74/7 La Containers/Data/Application/74/7	598 800 407 801 407 801 40178148363 V73364 800 407 801 4017104 V73364 800 407 801 4017104 V73364 800 407 801 4017104 S98 800 407 801 4017104 V7396 800 407 801 4017104 V7396 800 407 801 4017104 V7396 800 407 801 4017104 V7396 800 407 801 4017104	/Library/Gaches/Suspakots 837/Library/Gaches 837.Library/Gaches 837.Library/Gaches 937.Library/Gaches 837.Library/Caches 837.Library/Caches 937.Library/Caches/Suspakots	:
2 y 1 23 33 35 8 8 6 7 y 2 23 133 55 8 8 6 7 y 2 23 133 55 8 6 7 y 2 33 133 55 8 6 7 y 2 33 133 55 8 6 7 y 2 33 133 55 8 6 7 y 3 33 133 55 8 7 y 3 33 133 56 8 7 y 3 33 135 8 7 y 3 33 15 8 7 y 3 3 13 15 8 7 y 3 3 15 8 7 y 3 3 15 8 7 y 3 3 15 7 y 3 3 15 8 7 y 3 3 15 9 7 y 3 3 15 8 7 y 3 3 15 9 7 y 3 3 15 9 7 y 3 3 15 8 7 y 3 3 15 9 7 y 3 3 15 9 7 y 3 3 15 7 y 3 3 15 7 y	<pre>fun tracking theta: fundament training(D3) dawy up tracking(D3) theraings Attempting to conset up training(D3) theraings Rectived Stat From ar up training (D3) theraing D3 (D3) the up training D3 (D3) the up training D3) show up tracking (D3) theraing D3 (D3) show up training (D3) theraing D3 (D3) show up training (D3) theraing D3 (D3) show up training (D3) theraing D3) show up training (D3) theraing D3 (D3) show up training (D3) the up training (D3) show up training (D3) show up training (D3) show up training (D3) show up training (D3) show up training (D3) show up training (D3) show u</pre>	(1) file-read-date /priorte/up/mobile/ to https://atampie.com vie TTTS Ver	Containers/Bats/Application/PAP 1. v/containers/Dats/Application/PAP 1. v/containers/Dats/Application/ 1. v/containers/Dats/Application/ 1. v/containers/Dats/Application/ Containers/Dats/Application/ 1. v/containers/Dats/Application/ 1. v/containers/Dats/Application/ 1. v/containers/Dats/Application/ Cantainers/Dats/Application/ Cantainers/Dats/Application/FAP	1944-82CF-107-821A-441778148343 19384-882-67-821A-41778148343 19384-882-67-821A-4177814 19384-882-67-821A-4177814 19384-882-67-821A-4177814 19384-882-67-821A-4177814 19384-882-67-67-821A-4177814 19384-882-67-67-821A-4177814 19384-882-67-67-821A-4177814 19384-882-67-67-821A-417784 19384-882-67-67-821A-417784 19384-882-67-67-821A-417784 19384-882-67-67	/Library/Caches/Snapshots 30/Library/Caches 40/Library/Caches/Snapshot 20/Library/Caches/Snapshot 20/Library/Caches 40/Library/Caches 40/Library/Caches 40/Library/Caches 40/Library/Caches 40/Library/Caches/Snapshots	:



Task: Information Leakage inlogs (Android)

- Install Torus.apk
- Start Torus
- In a console window view the logs with adb logcat
- Enter a username and password, e.g. bob/password123
- Click Login









Intercepting, examining, modifying web traffic





HTTP Proxies

HTTP (web) proxies act as intermediaries between clients and servers and may be used for several reasons:

- Speed up internet access
- Filter undesirable or malicious content
- Prevent data leakage
- Provide anonymity

TESTING





HTTP Proxy Types

We are Interested in one particular type of proxy:





Running a Local Intercepting Proxy You can run a local HTTP proxy on your own machine:

- Start local proxy and configure interface and port to listen to
- If necessary, configure upstream proxy server(s)

1	Edit proxy listener					
	Binding Request handling Certificate					
	These settings control how Burp binds the proxy listener.					
	Bind to port: 8080					
0	Bind to address: Coopback only All interfaces					
	Specific address: 127.0.0.1					
	OK Cancel					



Intercepting Traffic in the Local Proxy Monitor, intercept, and rewrite traffic in your local proxy:

Buro Intruder Repeater Window Help	
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts	
Intercept HTTP history WebSockets history Options	
Request to https://www.facebook.com:443 [66.220.152.19]	
Forward Drop Intercept is on Action Comment this item	
Raw Params Headers Hex	
<pre>ser_Agent: Mosilla/S.0 (Windows NT 6.1; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0 ccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 ccept-Language: en-gb,en;q=0.5 ccept-Encoding: gzip, deflate eferer: https://www.facebook.com/ ookie: reg_fb_gate=https%3A%2F%2Fwww.facebook.com%2F; eg_fb_ref=https%3A%2F%2Fwww.facebook.com%2Flogin_attempt%3D1; datr=OMqVU0cjhSTkthIxn9MGurnN onnection: keep-alive ontent-Type: application/x-www-form-urlencoded ontent-Length: 104 sd=AVohmHd1&email=test&pass=test&default_persistent=0&timezone=&lgnrnd=075240_8bJo&lgnjs=n&locale=en_GB</pre>	



Your Computer / Laptop

Web Site



Today: Testing Mobile Apps



Installing

- Two proxies worth considering
 - ZAP ("Zed Attack Proxy") from OWASP
 - 100% Free
 - <u>https://www.owasp.org/index.php/OWASP_Zed_Att</u> <u>ack_Proxy_Project</u>
 - Burp Suite: commercial
 - Free Version (lacks advanced security tools)
 - £239 / \$349 / €329 per user per year
 - https://www.portswigger.net/

We'll look at Burp today







Lab3: Local Proxy

Intercept HTTP Request/Response





Task: Run a local proxy

1. Run

\$ java -jar path-to-burp/burpsuite_free.jar &

2. ... next configure listening interface





Task: Configure local proxy

	Burp Suite Professional v1.6.18 - licensed to Cigital Inc. [200 user I						
	Burp Intruder Repeater Window Help						
	Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options						
	Intercept HTTP h	istory WebSockets his	tory Options				
	Proxy Liste	ners					
	Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your brows						
	Add	Running Interface	Invisible	Redirect	Certificate		
		127.0.0.1	8080		foobar.com	Certifcate host	
Select the in	terface Edit	192.168.1	122:8		Per-host		
	Remove					•	

Proxy -> Options -> Add | Edit (new interface/existing interface)



Task: Proxy iOS

- Select the wifi network
- Tap the little (i)
- Select Manual
- In Server/port enter proxy interface/port

Your iOS device will now use the proxy for **all** connections





Task: Proxy Android phone



- 1. Connect to the WIFI network
- 2. Settings->WIFI
- 3. Select the WIFI network by tapping on the name
- 4. Modify network config
- 5. Show advanced options
- 6. Enter the proxy settings (this is your proxy host's WIFI interface)





Task: Proxy the Android Emulator

emulator -avd <IMAGE_NAME> -http-proxy
http://<PROXY_HOST>:<PROXY_PORT>

To start an AVD named "cigital", using an HTTP proxy on the host running the emulator on port 8080

emulator -avd cigital-http-proxy
http://127.0.0.1:8080



Android Emulator - useful addresses

- **127.0.0.1**–emulator's loopback interface
- **10.0.2.2** alias to host's loopback (127.0.0.1) the host running the emulator.
- **10.0.2.3** First default DNS server.
- **10.0.2.15** Emulated device's network interface.





Task: View HTTP traffic

- 1. Configure the phone and proxy
- 2. Start the browser
- 3. Navigate to <u>http://example.com</u>
- 4. Observe the HTTP Request and Response in the proxy





Task: Tamper HTTP traffic

- 1. Turn Intercept on
- 2. Go to <u>http://www.example.co</u> <u>m</u>
- Intercept, select Action > Do Intercept ->
 Response to this request
- 4. Select Forward (Request)
- 5. Modify the Response



Modified Response

<html> <script>alert(0);</script> </html>

```
<html><iframe
src="tel:555-5555">Call me
now!</iframe></html>Cigita
```

Proxying HTTPS





Intercepting HTTPS traffic

Proxying network traffic inserts your proxy as a middleman in between all TLS connections allowing the data to be captured, viewed and tampered (just like HTTP).







HTTPS Proxying won't work out of the box



Solution: we need to "tell" the phone to trust the certificate presented by the proxy



Lab3: Proxying HTTPS

Intercept HTTP Request/Response





Task: First just try to proxyHTTPSMo Service ?* 21:30example.com

Why?

- Setup proxy settings as before
- 2. In browser, go to **https**://example.com

What happens and why?





Task: Install Proxy Certificate (iOS)

Installing a certificate in Safari:

- Go to http://burp.
- When prompted to "Install Profile", choose "Install."
- Click "Install" on the "Unverified Profile" message then "Done"
- Click "Done"

Or use the iPhone configuration utility: http://support.apple.com/kb/DL1465





Task: Export Proxy Certificate



Burp -> Proxy -> Options -> Import/Export CA Certificate

Certificate in DER format Click Next Save as *burp.crt*

CA Certificate

You can export your certificate and key for use in other tools, or in another installation of Burp. You can import a certificate and key to use in this installation of Burp. Note that you can also export the current certificate by visiting http://burp/cert in your browser.

Export

- Certificate in DER format
- Private key in DER format
- Certificate and private key in PKCS#12 keystore

Import

- O Certificate and private key in DER format
- Certificate and private key from PKCS#12 keystore





Next

Task: Install Proxy Certificate

On the host:

adb push burp.crt /mnt/sdcard

On the phone/emulator:

Settings→Security→"Credential Storage" section Select "Install from storage"

Now you can proxy https://example.com



Testing HTTPS

Did the developer do it right?





Testing HTTPS

- Since we are already intercepting HTTPS it's a small step to execute some tests on the use of HTTPS itself
- Two straightforward attacks against the way the application uses HTTPS.
 - 1. Attacker can abuse the trust chain check
 - 2. Attacker can abuse the hostname verification check
- What does this mean?



Abusing the trust chain check



Security certificate

This certificate isn't from a trusted authority.

Common name:

*.gstatic.com Organization:

Google Inc

Organizational u

Serial number: 1C:E1:5F:84:00:00:00:00:80:1C

Issued by:

Common name: Google Internet Authority Organization:

Google Inc Organizational unit:


Abusing the hostname verification check

Let's assume ROOTCA is trusted.

C:



Did I get myserver.com?



Lab3: Testing for HTTPS bypass

Does the app do HTTPS right?





Task: Test HTTPS

- 1. Remove the trusted burp cert on the phone
- 2. Install https-loader.apk(adb install httpsloader.apk)
- 3. Configure the phone and burp to proxy as before.
- 4. Click Load HTTP (observe the result)
- 5. Click Load HTTPS (explain the result)
- 6. Click Load HTTPS (bad cert) (explain)
- 7. In burp set the certificate host to foobar.com
- 8. Re-install the trusted cert
- 9. Click Load HTTPS (explain)
- 10. Click Load HTTPS (bad hostname) (explain)







Task: Test HTTPS (iOS)

- 1. Remove the trusted burp cert on the phone
- 2. Install the "training" app.
- 3. Configure the phone and burp to proxy.
- 4. Try to connect via HTTP (success)
- 5. Try connecting via HTTPS (FAIL)
- 6. Toggle the button to disable cert validation
- 7. Retry HTTPS (SUCCESSFUL page load)
- 8. Toggle the button to enable cert validation
- 9. Retry HTTPS (SUCCESSFUL page load)
- 10. Attempt HTTPS connect to different host (FAIL)
- 11. Disable cert validation and retry (SUCCESSFUL load)



Status: Connecting to http:// example.com via HTTP



WebViews





What is a WebView?

Control to load and display webpages.

Allows app to react to events

Based onWebKit** (pre-KK versus KK+)

Since Android 5.0 (Lollipop), update separately







Malicious Site

💠 Cigital

Javascript to Java bridge

• Access Java object through Javascript in page



```
// JavaScript
<script>
file = '/data/data/com.example.myapp/cache.txt'; 3
FUtil.write(file, data, false);
</script>
```



Abusing Javascript Interface

Disclosed 2012 (Neil Bergman), Luo et al. (2011)

```
<script>
function run(cmd) { return
FUtil.getClass().forName('java.lang.Runtime')
.getMethod('getRuntime',null)
.invoke(null,null).exec(cmd);
}
run(['/system/bin/sh','-c','date> /mnt/sdcard/test']);
3
```

```
FUtil.getClass().forName("android.telephony.SmsManager")
.getMethod("getDefault", null)
.invoke(null, null)
.sendTextMessage("123456", null, "Body", null, null);
```



@Javascript Interface to the rescue?

@Javascript Interface annotation limits exposure

I/chromium(13478): [INFO:CONSOLE(1)] "UncaughtTypeError: Object [object Object] has no method 'secret'", source: (1)

Comes with plenty of caveats
 Use @JavascriptInterface
 and target Android 4.2 (targetSdkVersion = API level 17)
 and run Android 4.2+, then safe





Is that all?

- Q: Am I safe if I don't have a JavaScript to Java
- breadaes.
- No! [CVE-2014-1939 Joshua Drake, MWR]
- Why?
- A: System may silently insert other bridges (e.g.accessibilityTraversal)





Defense in depth

• Defense:

webView.removeJavascriptInterface
("searchBoxJavaBridge_");

• and repeat for other interfaces





1. Small snag

- How can I remove the other bridges if I can't name
- them?

webView.removeJavascriptInterface
("foobarbazBridge ");

• One answer: use ajavacriptbridge to find otherjavascriptbridges**

DEMO





Same origin policy and file://

• Common to bundle and load local HTML assets

Stringurl= "file:///android_asset/load.html";
mainWebView.loadUrl(url);

Q: What is the implication? [DEMO]

A: Scheme is <u>file://</u>. Injected script will have access to the same origin

- ICS and earlier: vulnerable
- JB and later: can switch on unsafe behaviour!

setAllowFileAccessFromFileURLs(true);



hole

Q: Am I safe if I don't load local assets?

DEMO

A: it depends

- Tricked <iframe> to load error page
- The error page was loaded via file://
- Then exploit!





URL schemes

Register ascheme://host/[path]to be launched in response to a matching URL

tel:<phone-number>

mailto:someone@example.com
geo:47.6,-122.3

URL handlers are invoked through intents

<iframe src="tel:555-5555">Call me now!</iframe>

START {act=android.intent.action.VIEWdat=tel:xxxxxxxcmp=com.android.contacts/.activities.DialtactsActiv ity} frompid1945



So what? <maliciousurl> intermediar y i

intent to aprivate activity and control the intent extras

location.href=
"intent:data1#Intent
action=myaction;type=text/plain;end";



4. URL Schemes

• DEMO

Preferandroid.net.Uri.parse(url);
Avoid usingIntent.parseUri()

•but if you must then ...

```
intent.addCategory("android.intent.category.BROWSABLE")
;
intent.setComponent(null); // Want implicit
intent.setComponent(XYZ.class());
// Want explicit
intent.setSelector(null); // Forbid selector [Terada]
```



For more information, go to:

- Web Security Testing Cookbook (Paco Hope and Ben Walther)
- The Web Application Hacker's Handbook, 2ndedition (Dafydd Stuttard& Marcus Pinto)
- OWASP Testing Guide
 https://www.owasp.org/index.php/OWASP_Testing_Project
- Software Security Building Security In (Gary McGraw)



