

# GAME OF PWNS



Advanced iPHONE pen-testing  
with iNalyzer framework

Chilik Tamir – Chief Scientist, appsec-labs  
OWASP IL 2013

# WTF Disclaimer

This presentation will demonstrate a new approach and tool to perform practical black box testing on any iOS application.

These demos will be illustrated using technical terms and tools of trade that relates to black-box effort on iOS applications.

If terms such as: ObjC, Class-Dump-z, Cycript, Clutch, Proxies, Scanners, etc. make you want to WTF it, please see the reference slides at the end of the presentation to upgrade your knowledge.

~~Or you can use the exit door to select a different track ☺~~



OWASP IL 2013

 AppSec  
Application security **Labs**

# About me

- Security Researcher ,Trainer, Speaker

- Previous Publications:

- Lenovo privilege escalation WiFi driver
    - SOAP patch for Sqlmap
    - Belch – Burp suite plugin for binary protocols (AMF, Jser, etc.)
    - EvilQR open Research
    - AppUse - Android Application Uniform Security Evaluation Platform (Developed with Erez Metula)
    - Talks: HITB AMS 2013, DC9723(2013) OWASP IL (2011,2012)
    - Trainings: Black Hat USA, Intel, Cisco, HP, Amdocs and others

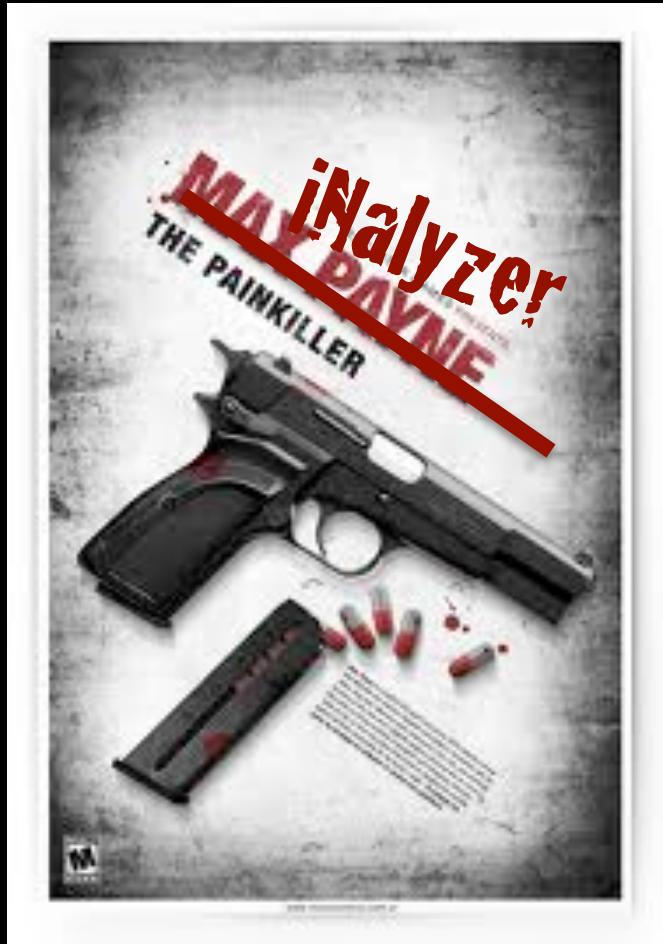


OWASP IL 2013

 **AppSec**  
Application security **Labs**

# Agenda

- “Pain Testing” iOS
- iNalyzer This?
- Advanced Pwnage



OWASP IL 2013

 AppSec  
Application security **Labs**

# Recap: What's an iOS App ?

- ObjC/C/C++ Compiled (ARM) Executable
- Encrypted Executable (fairplay)
- Self contained under  
~/Applications/GUID/AppName.app folder
- Installed by “mobile” user
- Executes under sandbox
- Under the radar can escape  
(SpyPhone, Storm8, etc.)



OWASP IL 2013

 **AppSec**  
Application security **Labs**

# iOS App: Common Vulnerabilities

Source: [www.owasp.org](http://www.owasp.org)

OWASP Mobile Top 10 Risks

M1 – Insecure  
Data Storage

M2 – Weak Server  
Side Controls

M3 - Insufficient  
Transport Layer  
Protection

M4 - Client Side  
Injection

M5 - Poor  
Authorization and  
Authentication

M6 - Improper  
Session Handling

M7 - Security  
Decisions Via  
Untrusted Inputs

M8 - Side Channel  
Data Leakage

M9 - Broken  
Cryptography

M10 - Sensitive  
Information  
Disclosure

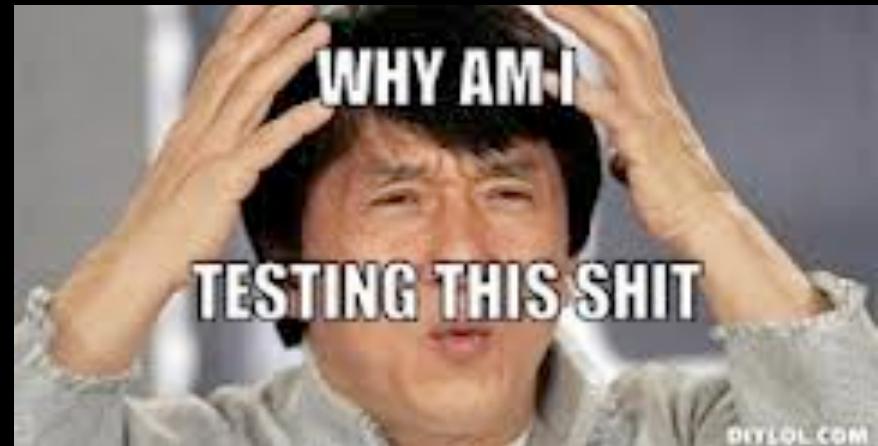


OWASP IL 2013

 **AppSec**  
Application security **Labs**

# iOS “Pain-Testing”: typical approach

- Binary:
  - Decryption (Clutch)
  - Class identification (class-dump-z)
  - Reversing (IDA)
  - Patching (when needed)
- Application Runtime:
  - FileSystem, KeyChain, DB, Logs
  - Theos / Logos Tweaks
  - GDB
  - Cycript
- Network (Proxy,Mallory)



OWASP IL 2013

 AppSec  
Application security **Labs**

# “Pain testing” iOS Apps: Cons

No Code



No Simulator

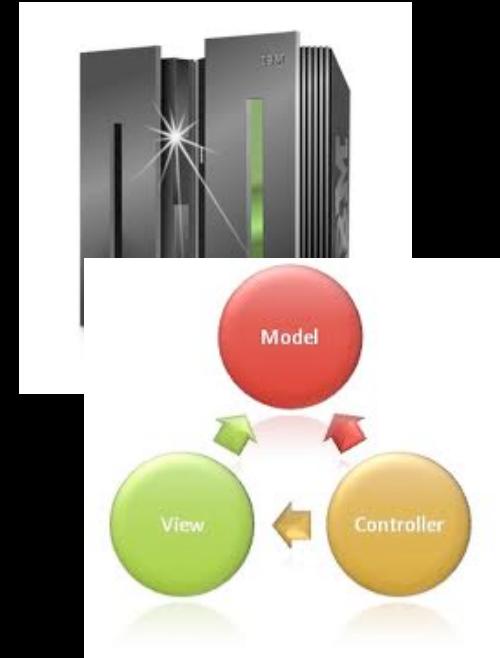


Encrypted by iTunes



Hidden vulnerabilities

Unknown end points



% of Functionality  
Coverage



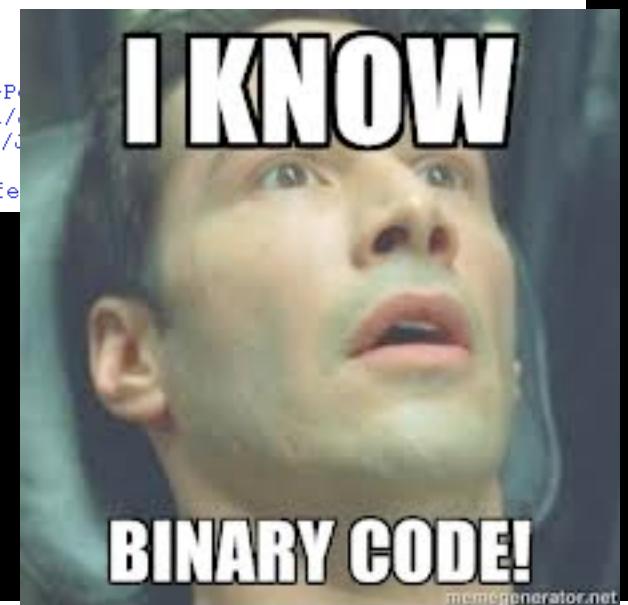
OWASP IL 2013

 AppSec  
Application security **Labs**

# Agony++ Binary Protocols

```
POST /aap.do HTTP/1.1
Host: data.flurry.com
Proxy-Connection: keep-alive
Accept-Encoding: gzip, deflate
Content-Type: application/octet-stream
Accept-Language: en-us
Accept: */*
Pragma: no-cache
Content-Length: 1062
Connection: keep-alive
User-Agent: QikSkype/6.7.125 CFNetwork/609.1.4 Darwin/13.0.0

0@w0ß^ ----- 6.7.125.IPHONE----->P
iPhone3,1 6.7.125@1Ωq+----- he_IL Asia/Jerusalem`` 6.7.125@1Ω_ß----- he_IL Asia/(
a/Jerusalem`` 6.7.125@Z(``I----- he_IL Asia/Jerusalem`` 6.7.125@_!<* Ö~ - he_IL Asia/J
feed.closemcv.feed.refresh mcv.Feed QΣ¶ feed.refresh Qaf
feed.close É2Umcv.feed.refresh È;m 6.7.125@wßMvME he_IL Asia/Jerusalem`` mcv.fe
```



OWASP IL 2013

 AppSec  
Application security **Labs**

# Agony++ unknown peers



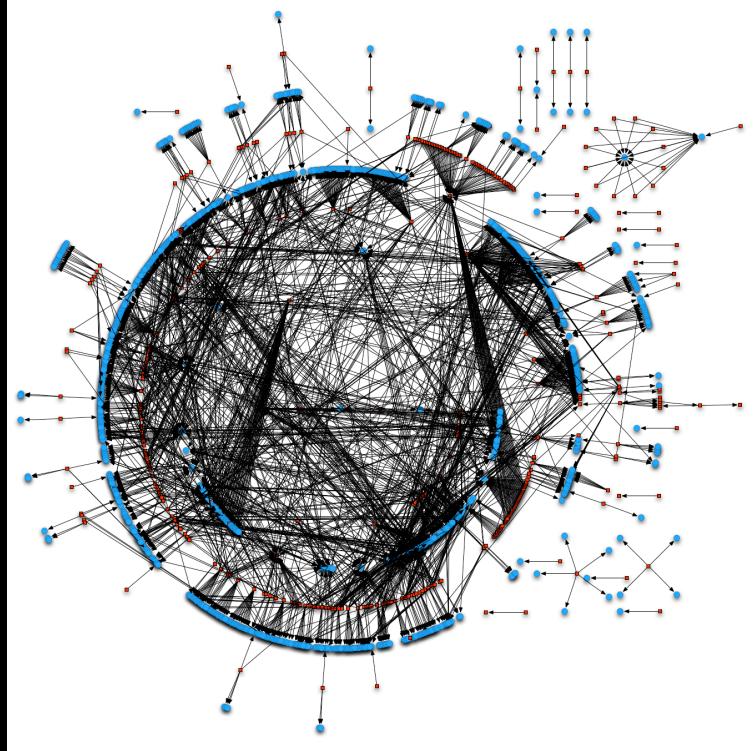
OWASP IL 2013

 AppSec  
Application security **Labs**

The logo for AppSec Labs, featuring a stylized 'L' shape in blue and grey, followed by the text "AppSec" in a large, bold, blue font, with "Application security" in a smaller, grey font below it, and "Labs" in a blue font at the bottom right.

# Single Stepping

Everything drills down to ObjC\_msgSend()



OWASP IL 2013

 **AppSec**  
Application security **Labs**

# Not enough Time



OWASP IL 2013

 AppSec  
Application security **Labs**

# Doesn't play well with other tools



OWASP IL 2013

 AppSec  
Application security **Labs**

# The Business Axiom

## ONE DOES NOT SIMPLY SUBMIT



**AN EMPTY PEN-TEST REPORT TO A  
CUSTOMER**

[...emegegenerator.net](http://emegegenerator.net)



OWASP IL 2013

 **AppSec**  
Application security **Labs**

# iNalyzer 5.6.0b

- Static Analysis:
  - Storyboard
  - SQL Queries
  - External Protocols
  - Embedded Strings
  - All Classes
  - All Objects
  - All Methods
  - All Parameters
- Dynamic Runtime Manipulation:
  - Variable Tampering
  - Constants Tampering
  - Methods Tampering
  - Live Attachment
  - Memory enumeration
  - Memory overwrite
  - Scriptable
  - Expandable



OWASP IL 2013



# Objective C class interposing

What should be the result of running this code:

```
NSString* ErrorMsg =[ NSString stringWithFormat:@"Access Denied" ]
```

Surprise, Surprise!

```
cy# ErrorMsg =[ NSString stringWithFormat:@"Access Denied" ] ;  
@"HackedAccount"  
cy# ErrorMsg =[ NSString stringWithFormat:@"Hello" ] ;  
@"HackedAccount"  
cy# ErrorMsg =[ NSString stringWithFormat:@"What Happend?" ] ;  
@"HackedAccount"  
cy#
```



OWASP IL 2013

 AppSec  
Application security **Labs**

# Objective C class interposing

Presenting a new implementation to a foundation class selector:

```
NSString->isa.messages[@"stringWithString:"] = function(a){  
    return "HackedAccount" }
```

```
cy# ErrorMsg =[ NSString stringWithFormat:@"Access Denied" ] ;  
@"HackedAccount"  
cy# ErrorMsg =[ NSString stringWithFormat:@"Hello" ] ;  
@"HackedAccount"  
cy# ErrorMsg =[ NSString stringWithFormat:@"What Happend?" ] ;  
@"HackedAccount"  
cy#
```

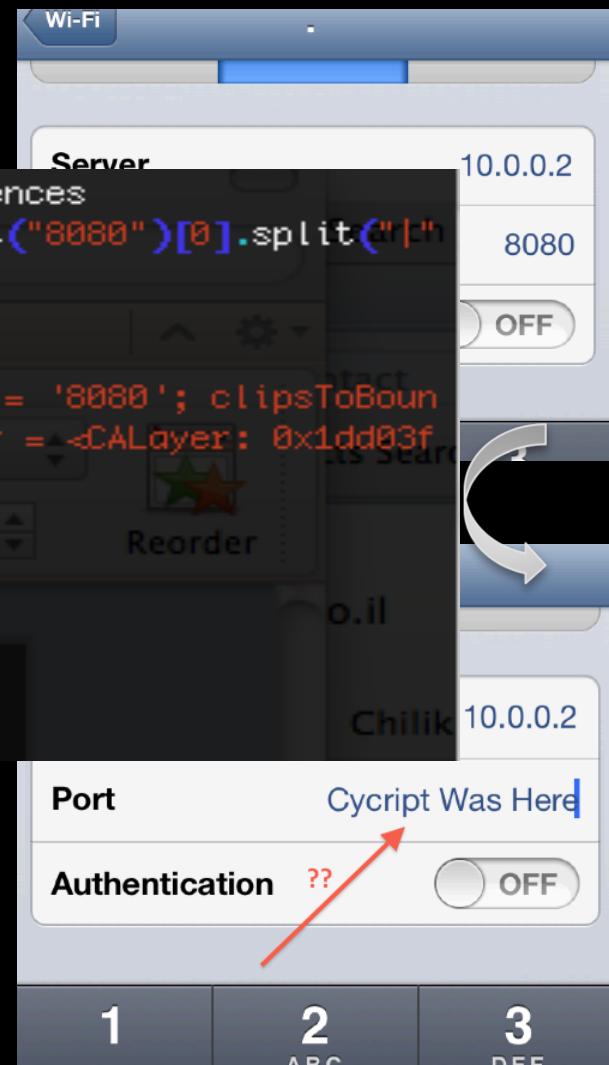


OWASP IL 2013

 AppSec  
Application security **Labs**

# Cycript: Tampering tool

```
iPhone:/Applications/iNalyzer5.app root# cycript -p Preferences
cy# [UIApp.keyWindow recursiveDescription].toString().split("8080")[0].split(":")
).pop().split(";")[0].split(": ")[1];
"0x1dd03400"
cy# var table=new Instance(0x1dd03400)
@<UITextField: 0x1dd03400; frame = (115 10; 175 24); text = '8080'; clipsToBounds = YES; gestureRecognizers = <NSArray: 0x1dd04fd0>; layer = <CALayer: 0x1dd03f70>>
cy# table.text
@"8080"
cy# table.text=@"Cycript Was Here"
@"Cycript Was Here"
cy#
```



OWASP IL 2013

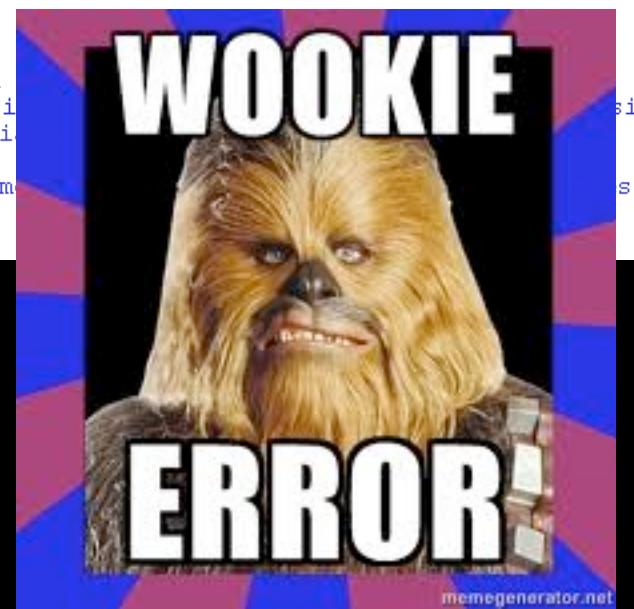
 AppSec  
Application security **Labs**

# Solving Binary Protocols

```
POST /aap.do HTTP/1.1
Host: data.flurry.com
Proxy-Connection: keep-alive
Accept-Encoding: gzip, deflate
Content-Type: application/octet-stream
Accept-Language: en-us
Accept: */*
Pragma: no-cache
Content-Length: 1037
Connection: keep-alive
User-Agent: QikSkype/6.7.125 CFNetwork/609.1.4 Darwin/13.0.0
```

```
0@w=ä6 [REDACTED] 6.7.125 iPhone' OR '1'='1' -->Pej@wBMv device.model.1
iPhone3,1 6.7.125@10Gf***** he_IL Asia/Jerusalem** 6.7.125@1Q,ä***** he_IL Asi
a/Jerusalem** 6.7.125@Z(*** he_IL Asia/Jerusalem** 6.7.125@_!<* Ö~ > he_IL Asi
feed.closemcv.feed feed.refresh mcv.feed qΣt feed.refresh qaf
feed.close É2Umcv.feed É9q feed.refresh É;m 6.7.125@wBMv >c!7 he_IL Asia/Jerusalem** m
h,*
```

```
asd=[UIDevice currentDevice]
asd->isa.messages["uniqueIdentifier"]=function(){ return ""
OR '1'='1' --"; }
```



OWASP IL 2013

 AppSec  
Application security **Labs**

# Storyboard Collection

WhatsApp.app

Main Page Related Pages Classes Files

WhatsApp.app  
Strings analysis  
ViewControllers  
Info.Plist Content  
Embedded Strings  
Classes  
Files

ConversationViewController  
click to load

CountryPickerController  
click to load

CustomLabelInputViewController  
click to load

DebugViewController  
click to load

FavoritesViewController  
click to load

FontSizePicker  
FontSizePicker  
click to load

iNalyzer Dashboard Apps Application security



Demo



OWASP IL 2013



# Storyboard Failure



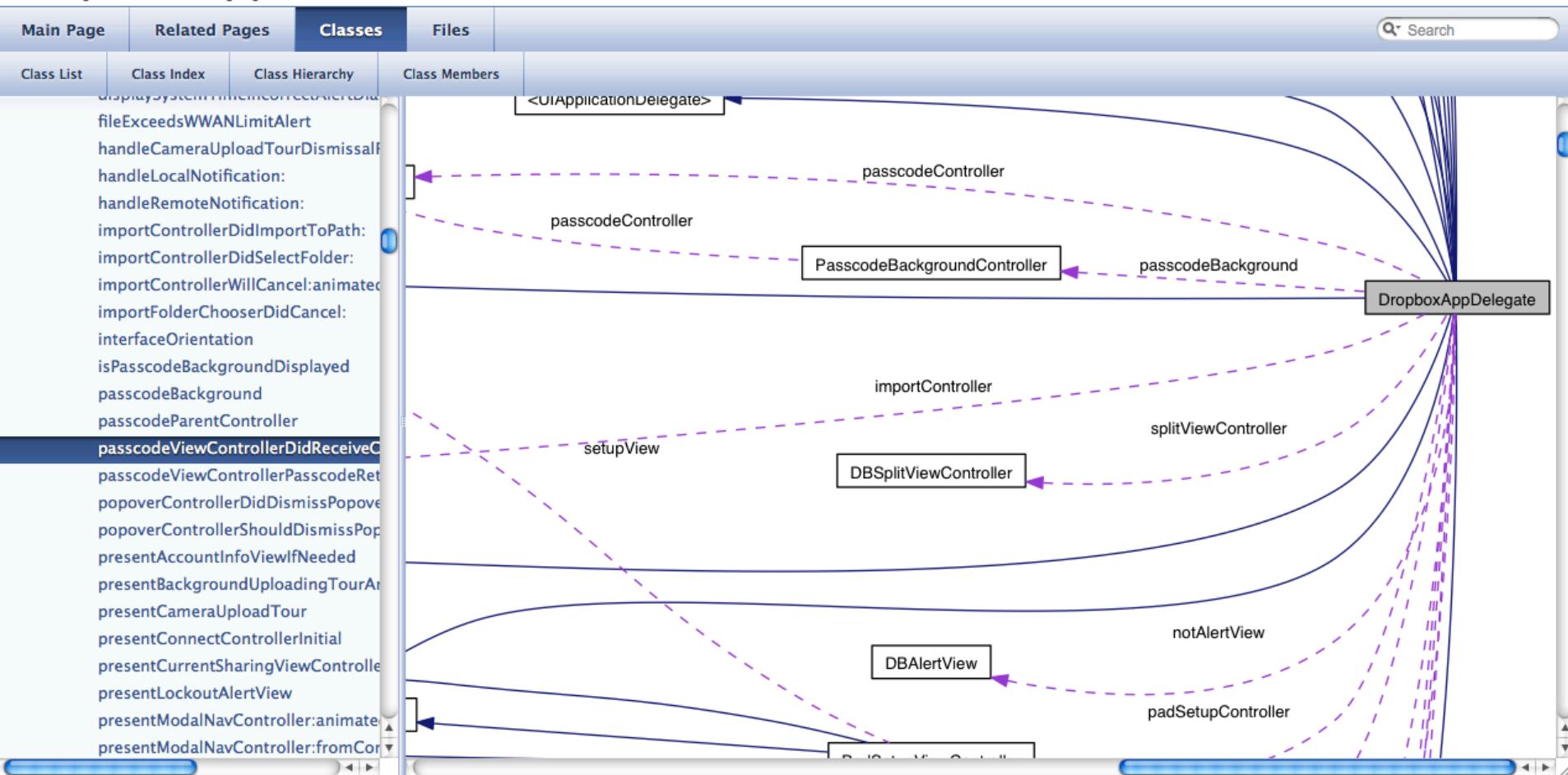
OWASP IL 2013

 AppSec  
Application security **Labs**

# iNalyzer Dashboard

# Dropbox.app

iNalyzer Dashboard  AppSec  
Application security labs



OWASP IL 2013

 APPSEC  
Application security labs

[Main Page](#)[Related Pages](#)[Classes](#)[Files](#) Search

▼ Dropbox.app

[Strings analysis](#)[ViewControllers](#)[Info.Plist Content](#)[Embedded Strings](#)[Classes](#)[Files](#)

## Strings analysis

Analysis of Strings found in the executable

### SQL Strings

```
1 11699 INSERT INTO asset_ids VALUES (?);  
2 11700 INSERT INTO cache_index VALUES (?, ?, ?, ?)  
3 11701 INSERT INTO data_cache VALUES('%@', '%@')  
4 11702 INSERT OR IGNORE INTO urls VALUES (?);  
5 13642 SELECT SUM(file_size) FROM cache_index  
6 13643 SELECT asset_id FROM asset_ids WHERE asset_id = ?;  
7 13644 SELECT data FROM data_cache WHERE key = '%@'  
8 13645 SELECT hash FROM hashes WHERE hash = ?;  
9 13646 SELECT id,access_token FROM test_account WHERE app_id = %@  
10 13647 SELECT key FROM data_cache WHERE key = '%@'  
11 13648 SELECT name FROM sqlite_master WHERE type='table' AND name='hashes';  
12 13649 SELECT uid,name FROM user WHERE uid IN (SELECT id FROM #test_accounts)  
13 13650 SELECT url FROM urls WHERE url = ?;  
14 13651 SELECT uuid, key, access_time, file_size FROM cache_index WHERE key = ?
```



OWASP IL 2013

# Command line Arguments?

```
62 35669 waze://?browser_title=
63 35670 waze://?ll=%f,%f&n=T
64 35671 waze://?open_url
65 35672 waze://?open_url=
66 5593 1. You have read and agree to the terms of service at
          http://www.waze.com/legal/privacy. Your continued use of Waze
          indicates your consent to them.
          only.
67 6622 waze://?open_url=
```

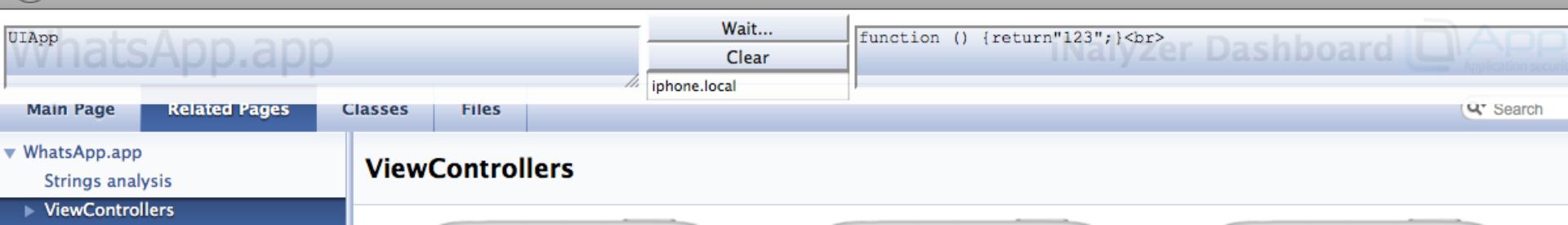
waze://?%6f%70%65%6e%5f%75%72%6c%3d%68%74%74%70%3a%2f%2f
%74%72%2e%69%6d%2f%34%36%35%77%35



OWASP IL 2013



# Cycript Console



The screenshot shows the Cycript Console interface. At the top, there's a menu with options: Wait..., Clear, and iphone.local. Below the menu, a code editor displays the following JavaScript function:

```
function () {return"123";}<br>
```

The background of the slide features a watermark of the WhatsApp app interface, showing the main page, related pages, and a search bar.

Demo



OWASP IL 2013



# Demo: Expanding iNalyzer with Burp

The screenshot illustrates the integration of iNalyzer's class browser with the Burp Suite proxy tool. In the browser window, the 'PasscodeViewController' class is selected, highlighting its methods like 'passcodeEquals:'. Simultaneously, in the Burp Suite interface, a corresponding network request is being monitored, showing the same method name in the URL. This demonstrates how iNalyzer can automatically extract and utilize the class structure and specific methods from the application under analysis.



OWASP IL 2013



**Payload Positions**

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions – see help for more information.

Attack type: Sniper

```
GET /Dropbox/Invoke=%5BPasscodeViewController%20passcodeEquals:@%22$1200$%22%20%5D&EndInvoke HTTP/1.0
Host: coredumps-iphone.local:5544
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:19.0) Gecko/20100101 Firefox/19.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: null
Connection: keep-alive
```

1 x 2 x ...

**Payload Sets**

You can define one or more payload sets. The number of payload sets is limited by memory.

Payload set: 1 Payload

Payload type: Numbers Request

**Intruder attack 2**

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Sequential  Random

Request	Payload	Status	Error	Timeout	Length	148	Count
25	1224	200	<input type="checkbox"/>	<input type="checkbox"/>	153	0	0
26	1225	200	<input type="checkbox"/>	<input type="checkbox"/>	153	0	0
27	1226	200	<input type="checkbox"/>	<input type="checkbox"/>	153	0	0
28	1227	200	<input type="checkbox"/>	<input type="checkbox"/>	153	0	0
29	1228	200	<input type="checkbox"/>	<input type="checkbox"/>	153	0	0
30	1229	200	<input type="checkbox"/>	<input type="checkbox"/>	153	0	0
31	1230	200	<input type="checkbox"/>	<input type="checkbox"/>	153	0	0
32	1231	200	<input type="checkbox"/>	<input type="checkbox"/>	153	0	0
33	1232	200	<input type="checkbox"/>	<input type="checkbox"/>	153	0	0
34	1233	200	<input type="checkbox"/>	<input type="checkbox"/>	153	0	0
35	1234	200	<input type="checkbox"/>	<input type="checkbox"/>	153	1	1
36	1235	200	<input type="checkbox"/>	<input type="checkbox"/>	153	0	0
37	1236	200	<input type="checkbox"/>	<input type="checkbox"/>	153	0	0
38	1237	200	<input type="checkbox"/>	<input type="checkbox"/>	153	0	0
39	1238	200	<input type="checkbox"/>	<input type="checkbox"/>	153	0	0

41 of 51



OWASP IL 2013

# iNalyzer & Burp Vs. Mailbox

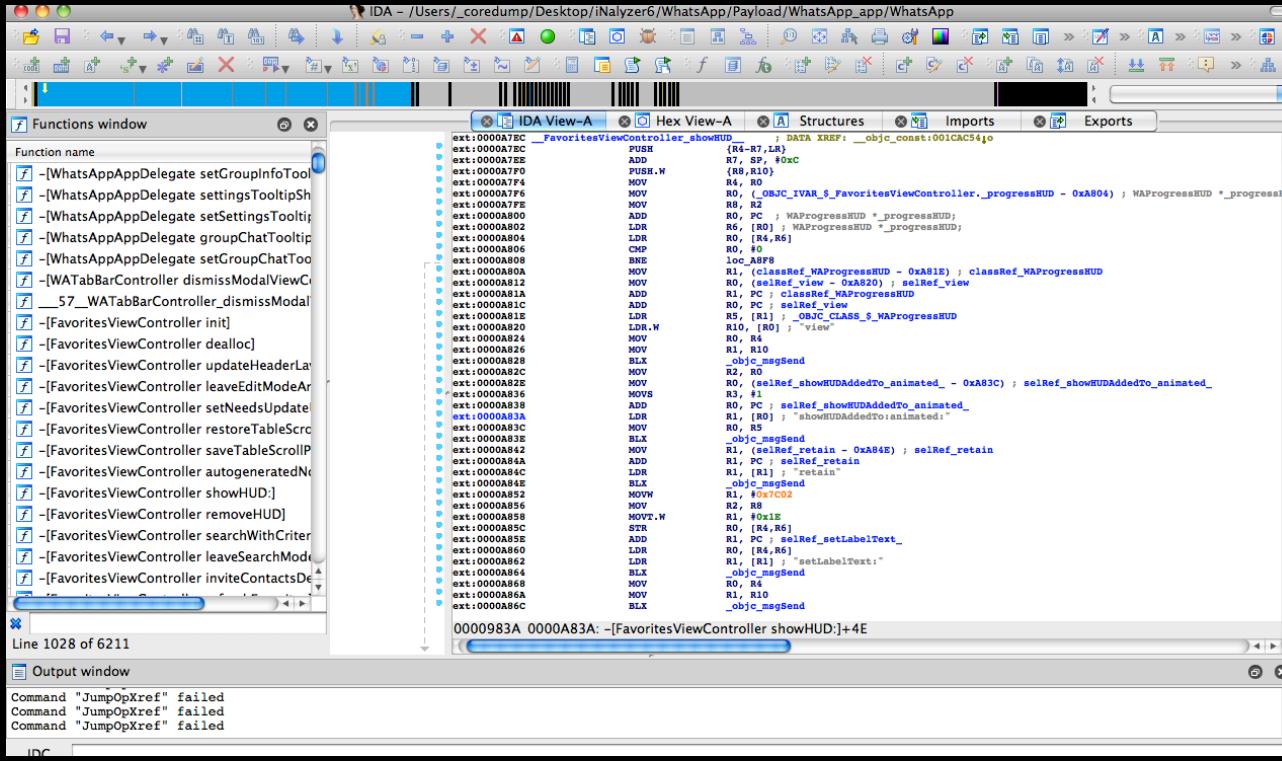
The image shows a composite of two screenshots. On the left is a screenshot of the Burp Suite Professional interface, specifically the Intruder tab, titled "Intruder attack 8". It displays a list of 178 requests with various payload values. Below this is a detailed view of a single request, showing the raw HTTP GET payload: "/Mailbox/Invoke=function%20me(w)%7Ba=%5BORVelvetRoomManager%20currentUser%5D;%5B%20a%20setPlaceInLine:w%20%5D;return%20YES;;%7D;me(%222639407%22);%EndInvoke HTTP/1.0". The request also includes headers like Host: 145.220.13.64:5544 and User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:19.0) Gecko/20100101 Firefox/19.0. The right side of the image shows a mobile phone screen with a VNC viewer interface. The phone's status bar indicates "No SIM" and "17:13". The main screen displays a mailbox inbox with one message, accompanied by the text "You're on your way to a whole new inbox" and a large blue number "1,030,207" followed by "People in front of you". Below this, it says "0 People behind you" with three circular icons containing an 'i', a lightning bolt, and a Twitter bird.



OWASP IL 2013



# Wishful thinking: IDA Remote Debugging Obsolete



The screenshot shows the IDA Pro debugger interface with the following details:

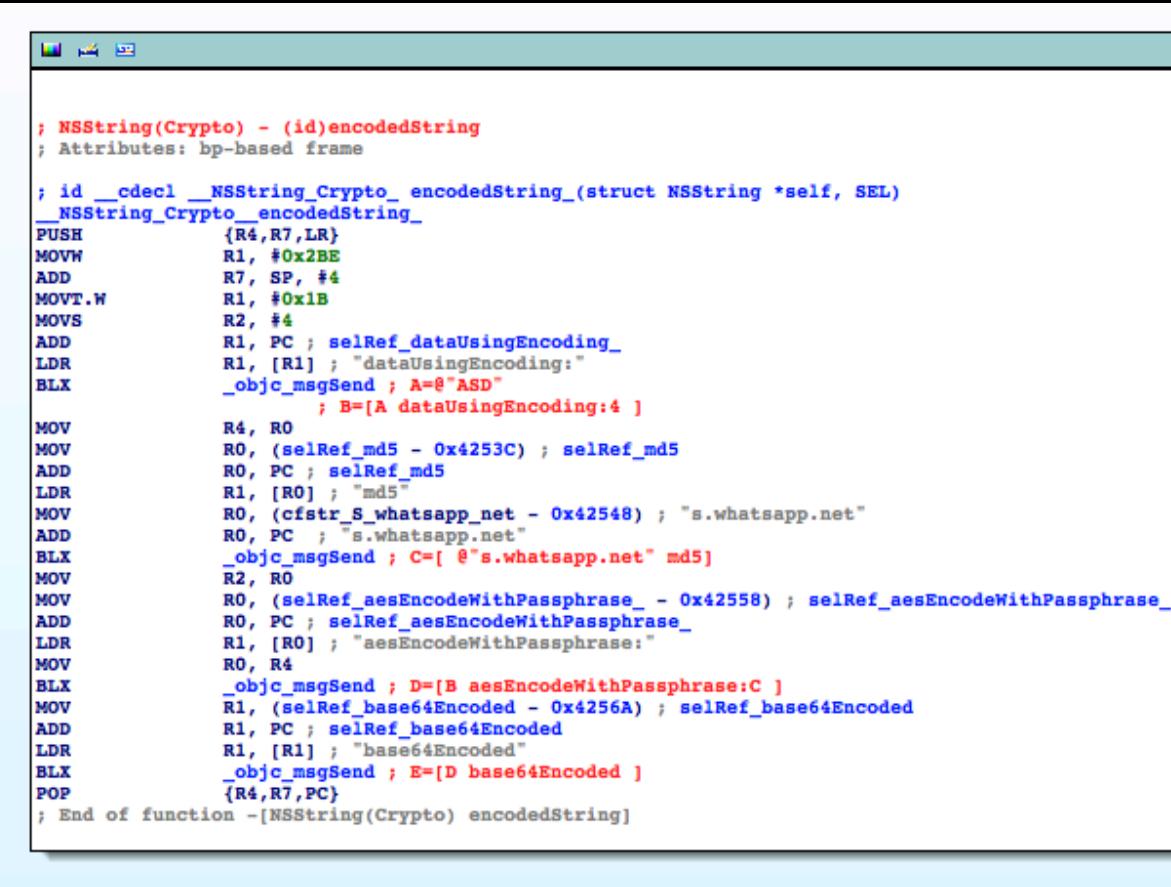
- Functions window:** Lists various methods and functions, many of which are prefixed with "ext:" and end in ".ref\_to". These likely represent Objective-C selectors or message forwarding.
- IDA View-A:** The main assembly view showing the assembly code for the WhatsApp payload. The assembly code includes instructions like PUSH, ADD, MOV, and BLX, along with memory addresses and labels such as "\_FavoritesViewController\_showHUD" and "selRef\_setLabelText".
- Hex View-A:** A hex dump view of the assembly code.
- Structures:** A structures view.
- Imports:** A imports view.
- Exports:** A exports view.
- Output window:** Shows command-line output, including errors related to jumping over opcodes.



OWASP IL 2013



# Demo Single Stepping



The screenshot shows a debugger window displaying assembly code. The code is annotated with comments explaining the purpose of each instruction. The assembly code is as follows:

```
; NSString(Crypto) - (id)encodedString
; Attributes: bp-based frame

; id __cdecl __NSString_Crypto__encodedString_(struct NSString *self, SEL)
__NSString_Crypto__encodedString_
PUSH    {R4,R7,LR}
MOVW   R1, #0x2BE
ADD    R7, SP, #4
MOVT.W R1, #0x1B
MOVS   R2, #4
ADD    R1, PC ; selRef_dataUsingEncoding_
LDR    R1, [R1] ; "dataUsingEncoding:"
BLX    _objc_msgSend ; A=@"ASD"
          ; B=[A dataUsingEncoding:4 ]
MOV    R4, R0
MOV    R0, (selRef_md5 - 0x4253C) ; selRef_md5
ADD    R0, PC ; selRef_md5
LDR    R1, [R0] ; "md5"
MOV    R0, (cfstr_S_whatsapp_net - 0x42548) ; "s.whatsapp.net"
ADD    R0, PC ; "s.whatsapp.net"
BLX    _objc_msgSend ; C=[ @"s.whatsapp.net" md5]
MOV    R2, R0
MOV    R0, (selRef_aesEncodeWithPassphrase_ - 0x42558) ; selRef_aesEncodeWithPassphrase_
ADD    R0, PC ; selRef_aesEncodeWithPassphrase_
LDR    R1, [R0] ; "aesEncodeWithPassphrase:"
MOV    R0, R4
BLX    _objc_msgSend ; D=[B aesEncodeWithPassphrase:C ]
MOV    R1, (selRef_base64Encoded - 0x4256A) ; selRef_base64Encoded
ADD    R1, PC ; selRef_base64Encoded
LDR    R1, [R1] ; "base64Encoded"
BLX    _objc_msgSend ; E=[D base64Encoded ]
POP    {R4,R7,PC}
; End of function -[NSString(Crypto) encodedString]
```

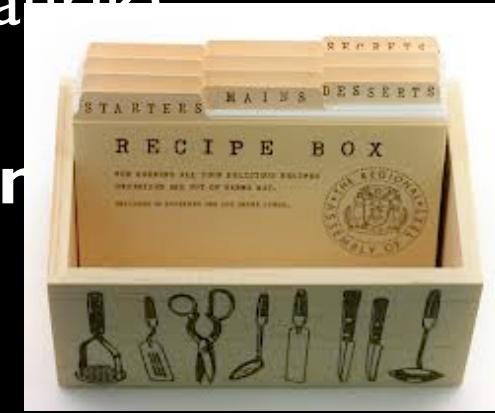


OWASP IL 2013

 AppSec  
Application security **Labs**

# iNalyzer 5.6.0b: The Recipe

1. Jail-borken device (@evad3rs)
2. Clutch to decrypt app (ttwj)
3. Class-dump-Z to app prototypes (@kennytm)
4. Doxygen engine to render a Dashboard (@doxygen)
5. FireFox to run the Dashboard (@firefox)
6. Cycript to modify the app behavior(@safrrik)
7. Repeat step 6 until completed
8. SubjectiveC to log selectors (@kennytr)



OWASP IL 2013

 **AppSec**  
Application security **Labs**

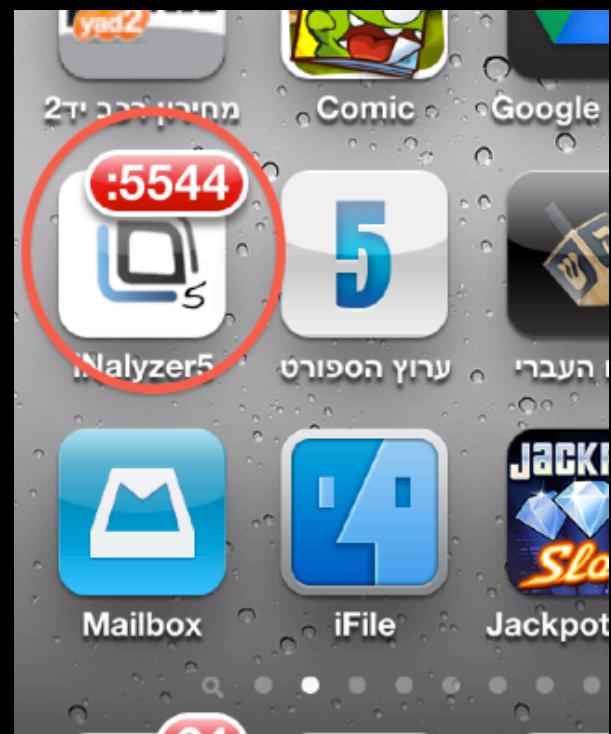
# Getting iNalyzer



OWASP IL 2013



# Starting iNalyzer



After restart open browser to  
<http://< you iDevice IP>:5544>



OWASP IL 2013



# Packaging an App

The screenshot shows a web browser window with a dark blue header bar containing various icons and links. The main content area displays the iNalyzer Packager tool. At the top right is the AppSec Application security LABS logo. Below it, the title "iNalyzer Packager" is displayed next to a small icon. A section titled "How to use:" lists five steps: 1. Install GraphViz-Dot on PC/Laptop, 2. Install DoxyGen on PC/Laptop, 3. Choose Application from the list and click Package. A dropdown menu labeled "Choose application to Pack:" contains the option "Dropbox". A large blue button labeled "Package" is centered below the dropdown. A note below the button says "Be patient as package creation can take a while". At the bottom, steps 4 and 5 are listed: 4. Save .zip to disk and extract, 5. Run Setup.bat(Win) or Setup.sh(Other). The footer of the browser window features the AppSec LABS logo.

Back Forward 10.0.0.5 Subscribe Reload Stop itter Bookmarks Home Firesheep Bookmarks Firebug Websecurity EPUBRead

iNalyzer Packager **AppSec**  
Application security **LABS**

**How to use:**

1. Install [GraphViz-Dot](#) on PC/Laptop
2. Install [DoxyGen](#) on PC/Laptop
3. Choose Application from the list and click Package

Choose application to Pack:

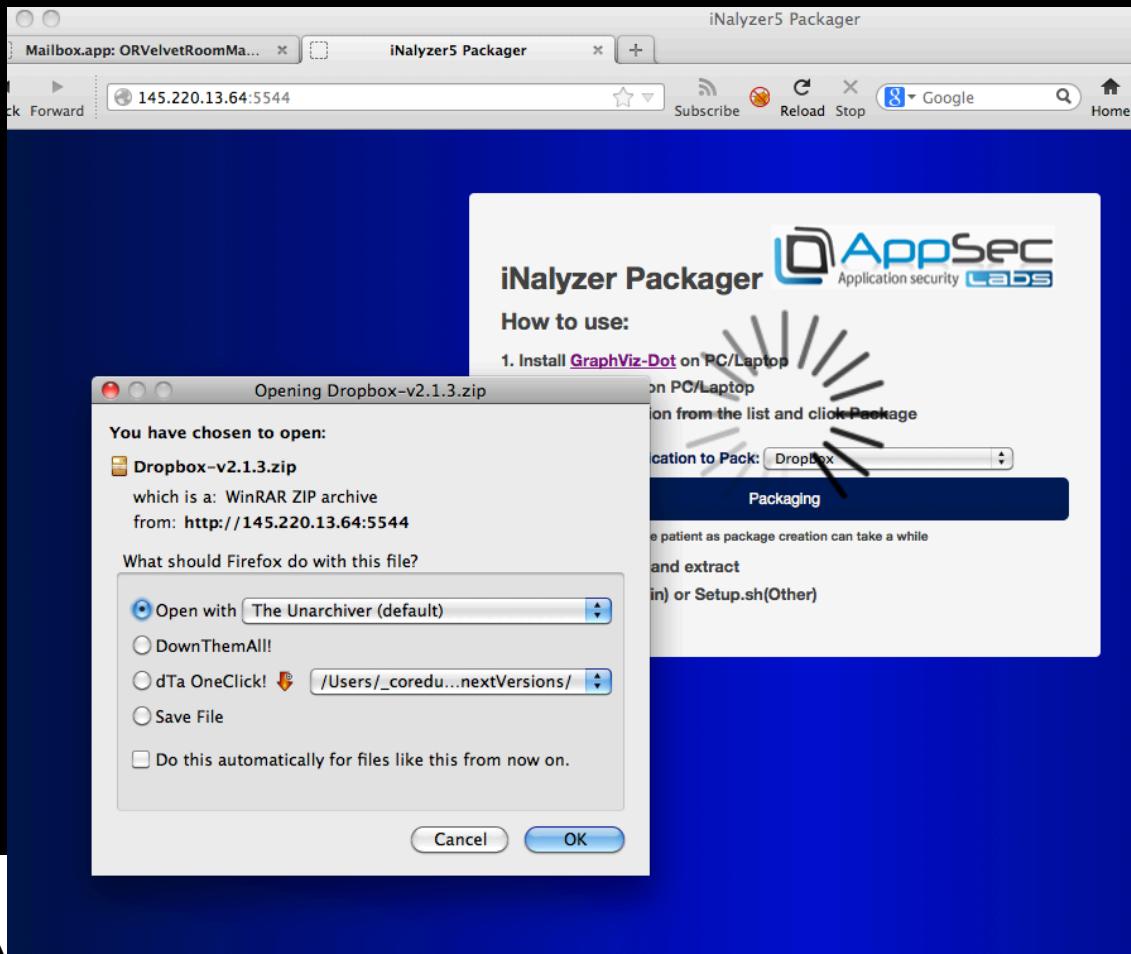
**Package**

Be patient as package creation can take a while

4. Save .zip to disk and extract
5. Run Setup.bat(Win) or Setup.sh(Other)

Application security **LABS**

# Download package

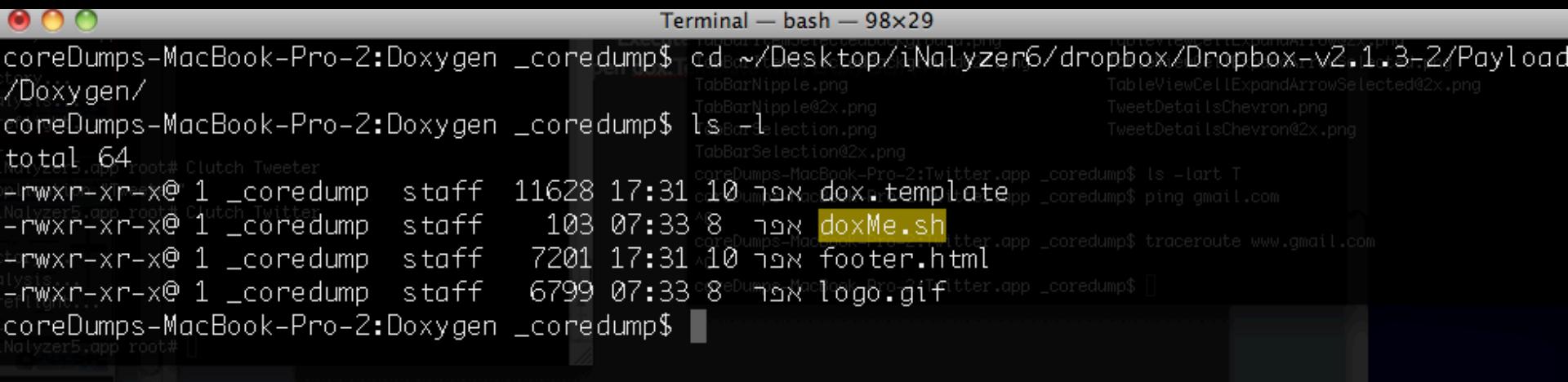


OWASP IL 2013

**AppSec**  
Application security **Labs**

# Dashboard Building

In the Payload/Appname.app/Doxygen/ folder:  
Execute the doxMe.sh file (Mac)  
Open dox.Template with DoxyGen (Win)



The screenshot shows a Mac OS X terminal window titled "Terminal — bash — 98x29". The command entered is "cd ~/Desktop/iNalyzer6/dropbox/Dropbox-v2.1.3-2/Payload/Doxygen/". The output shows the creation of a "dox.template" file and the execution of "doxMe.sh". The terminal also shows the user navigating through a directory structure containing various PNG files related to Twitter interface elements like TabBarNipple, TableViewCellExpandArrowSelected, and TweetDetailsChevron.

```
coreDumps-MacBook-Pro-2:Doxygen _coredump$ cd ~/Desktop/iNalyzer6/dropbox/Dropbox-v2.1.3-2/Payload/Doxygen/
coreDumps-MacBook-Pro-2:Doxygen _coredump$ ls -l
total 64
-rwxr-xr-x@ 1 _coredump  staff  11628 17:31 10 אפר dox.template
-rw-rxr-xr-x@ 1 _coredump  staff   103  07:33 8 אפר doxMe.sh
-rwxr-xr-x@ 1 _coredump  staff   7201 17:31 10 אפר footer.html
-rw-rxr-xr-x@ 1 _coredump  staff   6799  07:33 8 אפר logo.gif
coreDumps-MacBook-Pro-2:Doxygen _coredump$
```



OWASP IL 2013



# Open Live Demo (as time permits):



OWASP IL 2013



# Summary

- iOS Pain-testing, just got easier😊
- For exclusive alpha and beta releases please come to our booth.
- Mobile PT requires Mobile understanding
- Join our mobile application security hands-on training
  - iOS and Android Mobile Hacking (TBD, [info@appsec-labs.com](mailto:info@appsec-labs.com))
  - Mobile Secure Coding (TBD, [info@appsec-labs.com](mailto:info@appsec-labs.com))
  - Mobile Awareness (TBD, [info@appsec-labs.com](mailto:info@appsec-labs.com))



OWASP IL 2013



# Questions ?



OWASP IL 2013



# Thank You



OWASP IL 2013



# References:

- ObjC interposing –  
<http://culater.net/wiki/moin.cgi/CocoaReverseEngineering>
- Clutch – <https://github.com/ttwj/ClutchMod>
- Class-dump-z –  
<https://github.com/kennytm/Miscellaneous/downloads>
- Cycript – <http://www.cycript.org/>
- IDA – <https://www.hex-rays.com/products/ida/index.shtml>
- Mallory – <http://intrepidusgroup.com/insight/mallory/>
- Burp – <http://www.portswigger.net/burp/download.html>



OWASP IL 2013

# Game of Pwns: Advanced iPhone testing with iNalyzer framework

<https://appsec-labs.com/iNalyzer>

Chilik Tamir

Chief Scientist



@\_coreDump



chilik <at> appsec-labs.com



www.appsec-labs.com



OWASP IL 2013

