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.

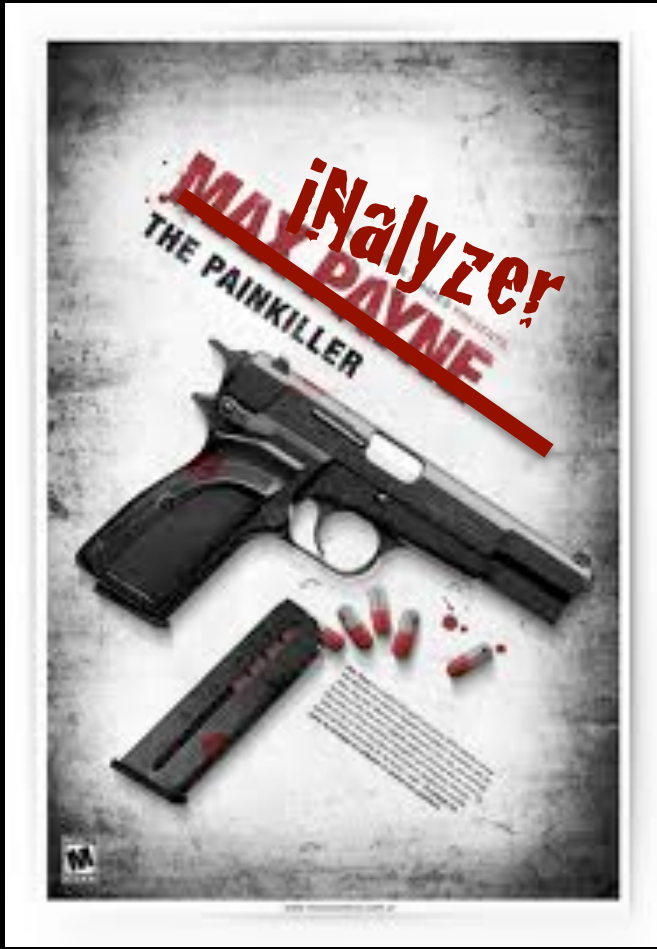
~~Or you can use the exit door to select a different track ☺~~

About me

- Security Researcher ,Trainer, Speaker
  - Pervious 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 Applicaition 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
- B.Sc. Biomedical Engineering

Agenda

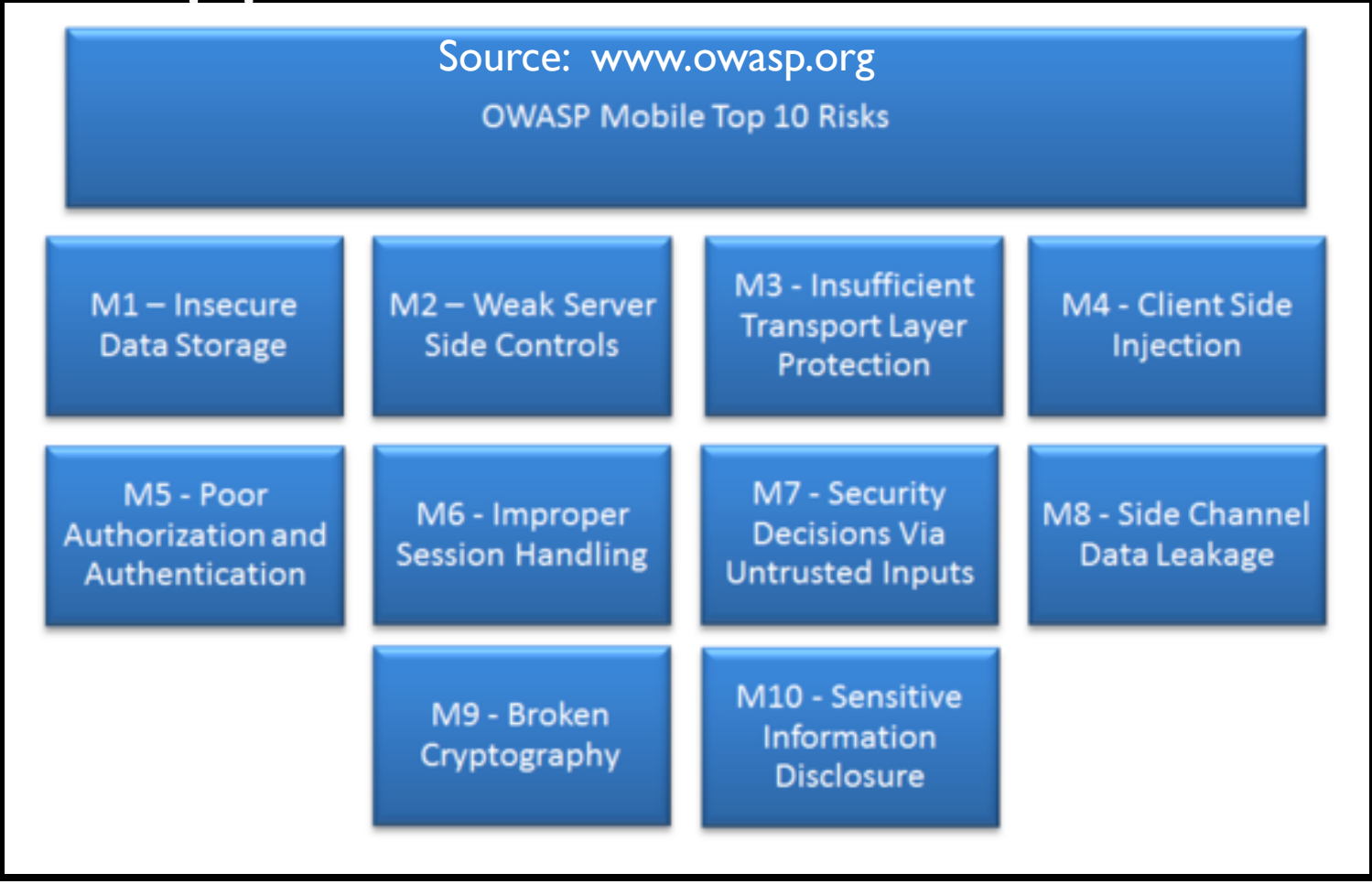
- “Pain Testing” iOS
- iNalyzer This?
- Advanced Pwnage



Recap: What's an iOS App ?

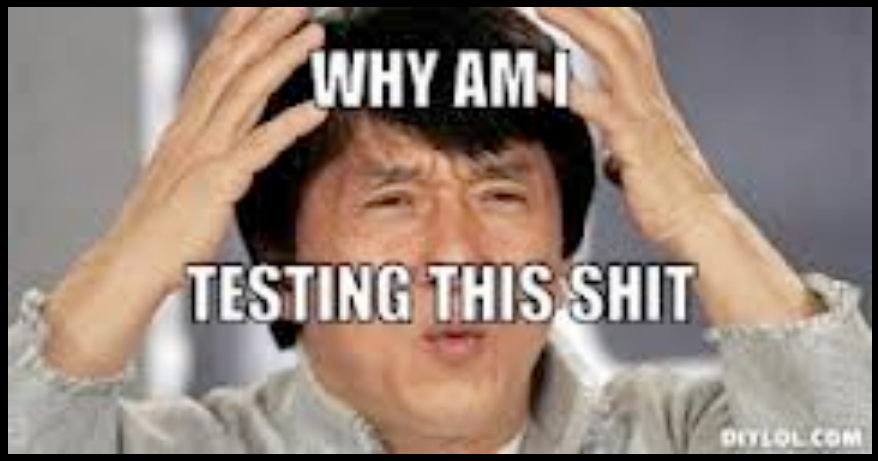
- ObjC/C/C++ Compiled (ARM) Executable
- Encrypted Executable (fairplay)
- Self contained under ~/Applications/GUID/AppName.app folder
- Installed by "mobile" user
- Executes under sandbox
- Under the radar can escape (SpyPhone, Storm8, etc.

iOS App: Common Vulnerabilities



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)



“Pain testing” iOS Apps: Cons

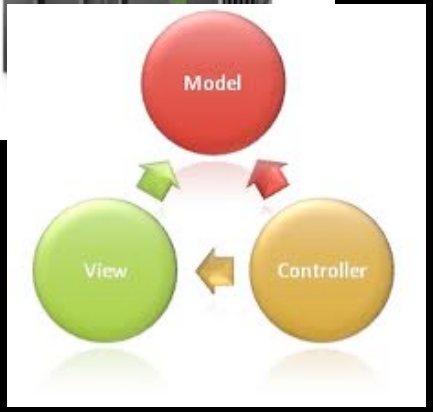
No Code

No Simulator

Encrypted by iTunes

Hidden vulnerabilities

Unknown end points



% of Functionality Coverage

Agony++ Binary Protocols

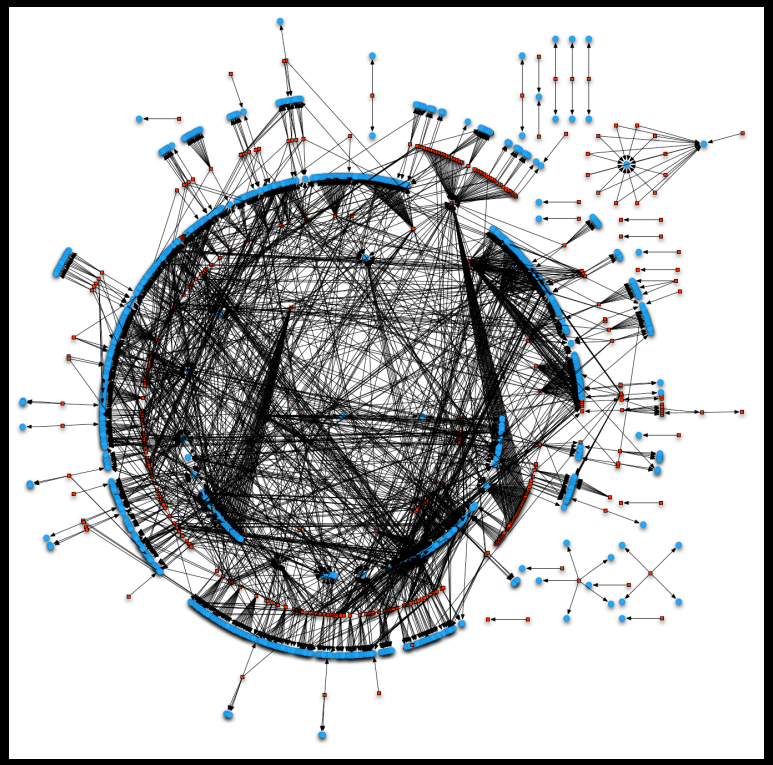
```
POST /aap.do HTTP/1.1
Host: data.flurry.com
Proxy-Connection: keep-alive
Accept-Encoding: gzip, deflate
Content-Type: application/octet-stream
Accept-Language: en-us
Accept: */*
Pragma: no-cache
Content-Length: 1062
Connection: keep-alive
User-Agent: QikSkype/6.7.125 CFNetwork/609.1.4 Darwin/13.0.0

 0@w©ö˜ [redacted] 6.7.125.IPHONE[redacted]>P
iPhone3,1 6.7.125@1ØÇ‡˜˜˜˜˜˜˜˜ he_IL Asia/Jerusalem˜˜ 6.7.125@1Ω ¸â˜˜˜˜˜˜˜˜ he_IL Asia/
a/Jerusalem˜˜ 6.7.125@Z(˜Î˜˜˜˜˜˜˜˜ he_IL Asia/Jerusalem˜˜ 6.7.125@_!<* Ö~ ⌐ he_IL Asia/
feed.closemcv.feed feed.refresh mcv.feed ÇΣ¶ feed.refresh Çª∫
feed.close É2Umcv.feed É9q feed.refresh É;m 6.7.125@wßMvME he_IL Asia/Jerusalem˜˜ mcv.fe
```

Agony++ unknown peers

Single Stepping

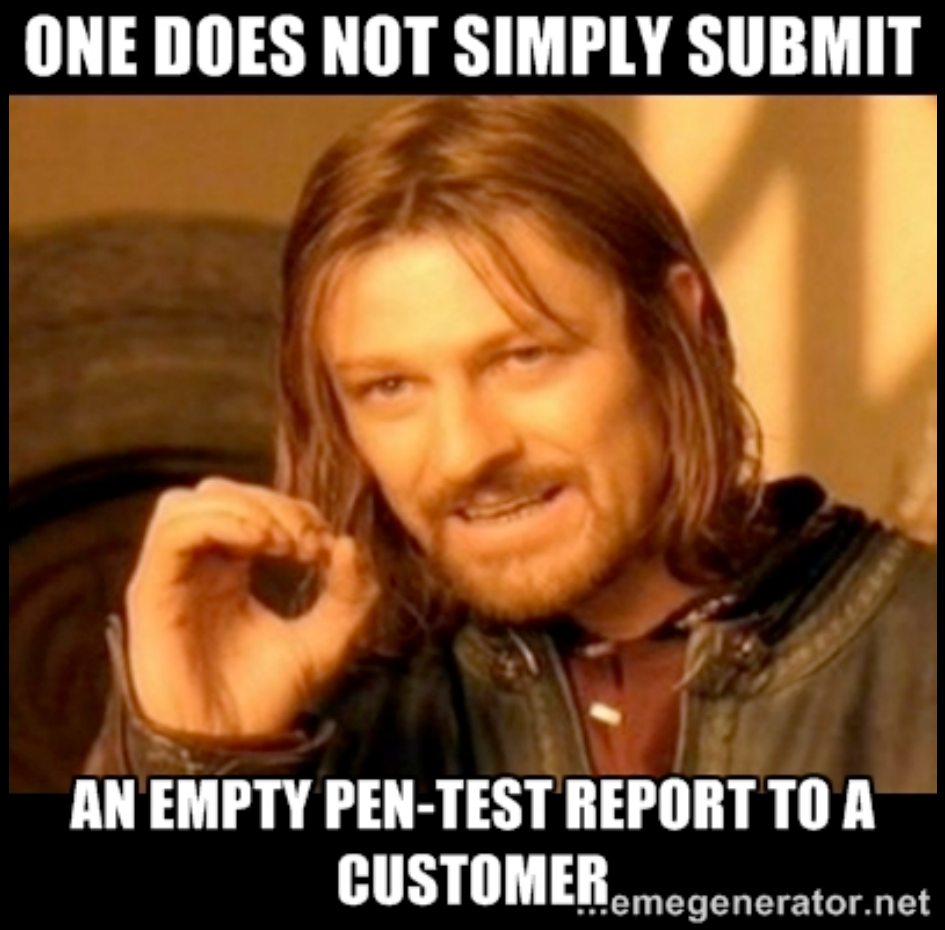
Everything drills down to ObjC_msgSend()



Not enough Time

Doesn't play well with other tools

The Business Axiom



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

Objective C class interposing

What should be the result of running this code:

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

Surprise, Surprise!

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

Objective C class interposing

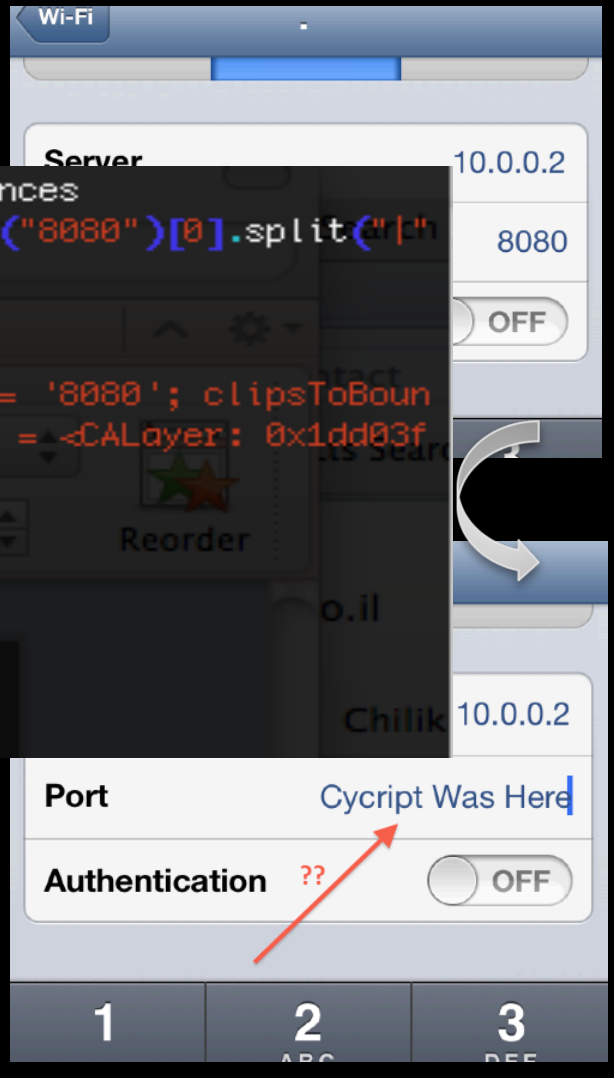
Presenting a new implementation to a foundation class selector:

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

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

Cycript: Tampering tool

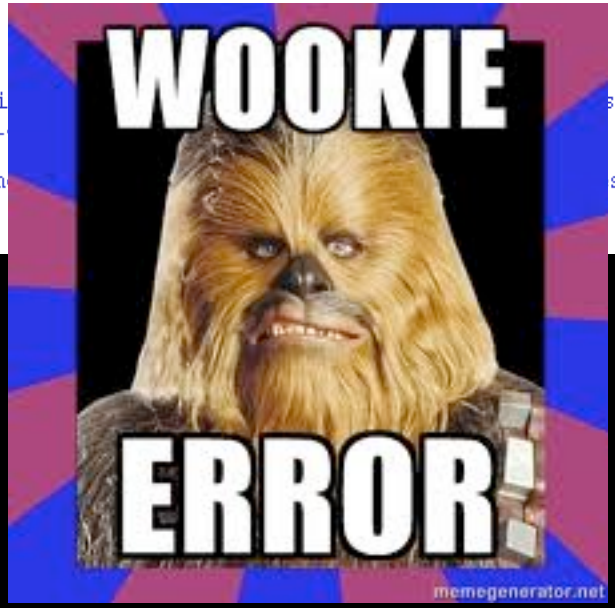
```
iPhone:/Applications/iNalyzer5.app root# cycript -p Preferences
cy# [UIApp.keyWindow recursiveDescription].toString().split("8080")[0].split("|"
).pop().split(";")[0].split(": ")[1];
"0x1dd03400"
cy# var lable=new Instance(0x1dd03400)
@"<UITextField: 0x1dd03400; frame = (115 10; 175 24); text = '8080'; clipsToBoun
ds = YES; gestureRecognizers = <NSArray: 0x1dd04fd0>; layer = <CALayer: 0x1dd03f
70>>"
cy# lable.text
@"8080"
cy# lable.text=@"Cycript Was Here"
@"Cycript Was Here"
cy#
```



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▪å6 [redacted] 6.7.125 IPHONE' OR '1'='1' -->Pè¥@wßMv device.model.1
iPhone3,1 6.7.125@1ØÇ‡ˇˇˇˇˇˇˇˇ he_IL Asia/Jerusalem ˇˇ 6.7.125@1Ω ¸â˜˜˜˜˜˜˜˜ he_IL Asi
a/Jerusalem˜˜ 6.7.125@Z( ˜Î˜˜˜˜˜˜˜˜ he_IL Asia/Jerusalem˜˜ 6.7.125@_!<* Ö~ ⌿ he_IL Asi
feed.closemcv.feed feed.refresh mcv.feed Ç∑¶ feed.refresh Çª∫
feed.close É2Umcv.feed É9q feed.refresh É;m 6.7.125@wßMv >c!7 he_IL Asia/Jerusalem˜˜ m
h,≠
```




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

OWASP IL 2013

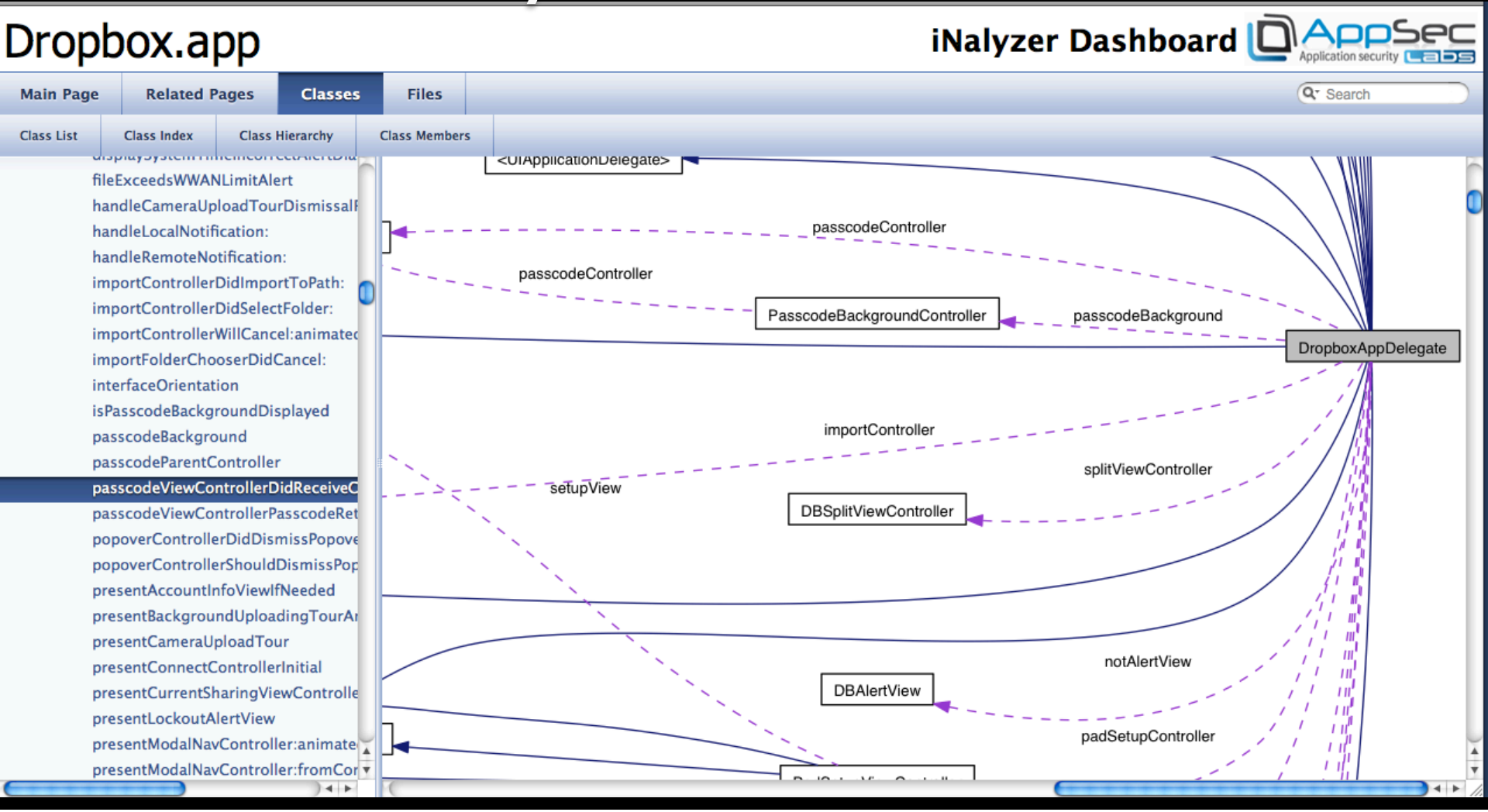
AppSec Application security Labs

Storyboard Collection

Demo

Storyboard Failure

iNalyzer Dashboard



OWASP IL 2013

AppSec Application security Labs

Dropbox.app

iNalyzer Dashboard

Main Page | Related Pages | Classes | Files | Search

- Dropbox.app
  - Strings analysis
  - ViewControllers
  - Info.Plist Content
  - Embeded 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 = '%@'

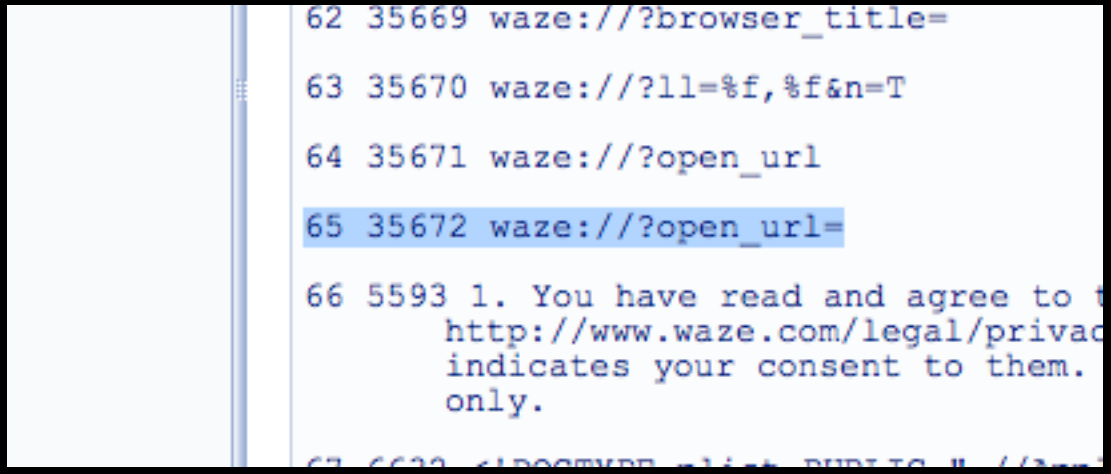
11 13648 SELECT name FROM sqlite_master WHERE type='table' AND name='hashes';

12 13649 SELECT uid,name FROM user WHERE uid IN (SELECT id FROM #test_accounts)

13 13650 SELECT url FROM urls WHERE url = ?;

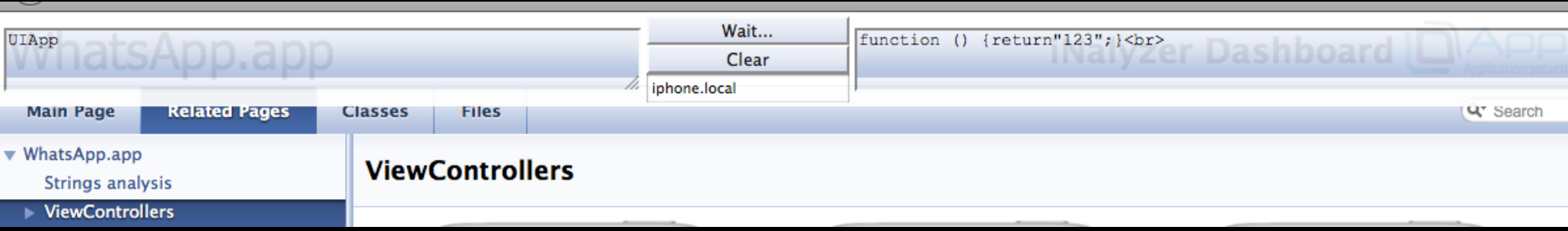
14 13651 SELECT uuid, key, access_time, file_size FROM cache_index WHERE key = ?

Command line Arguments?



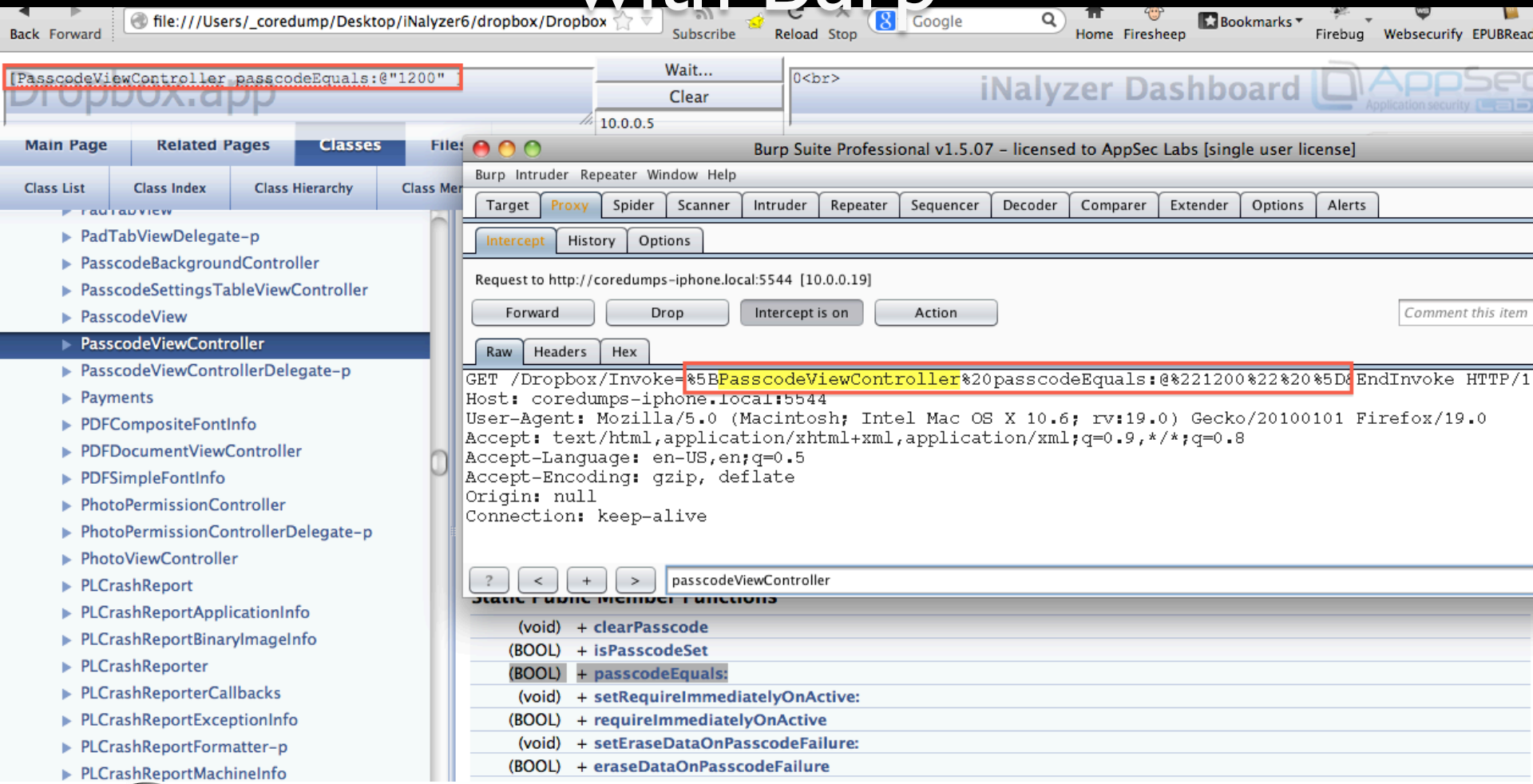
waze://?%6f%70%65%6e%5f%75%72%6c%3d%68%74%74%70%3a%2f%2f
%74%72%2e%69%6d%2f%34%36%35%77%35

Cycript Console



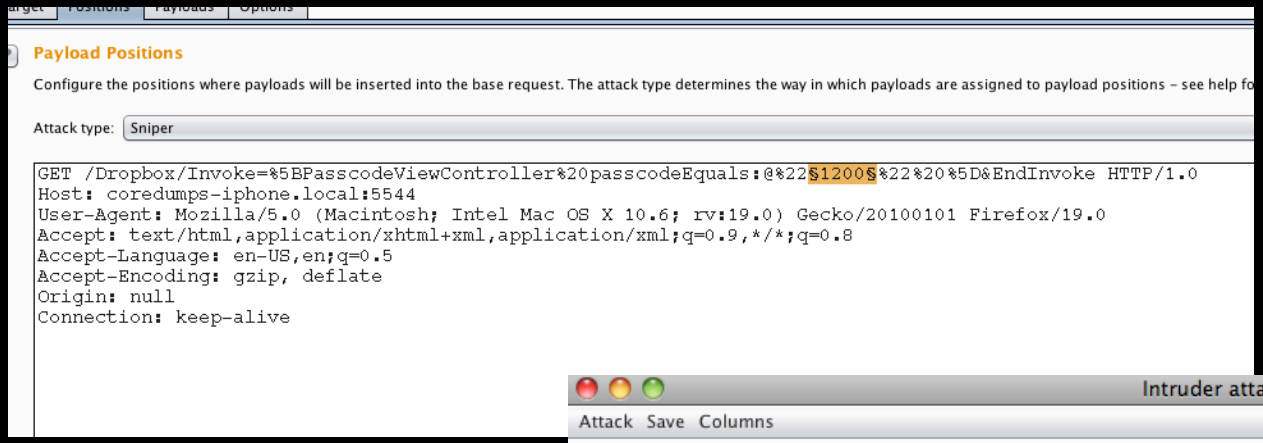
Demo

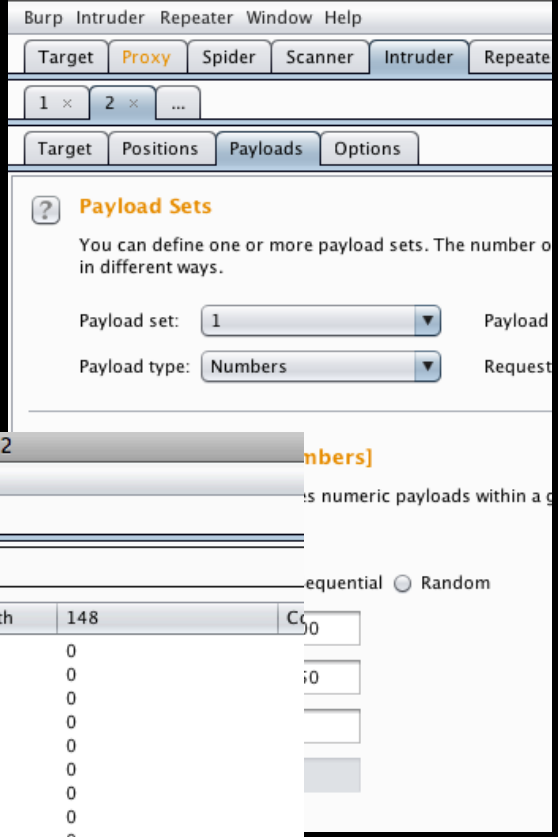
Demo: Expanding iNalyzer with Burp

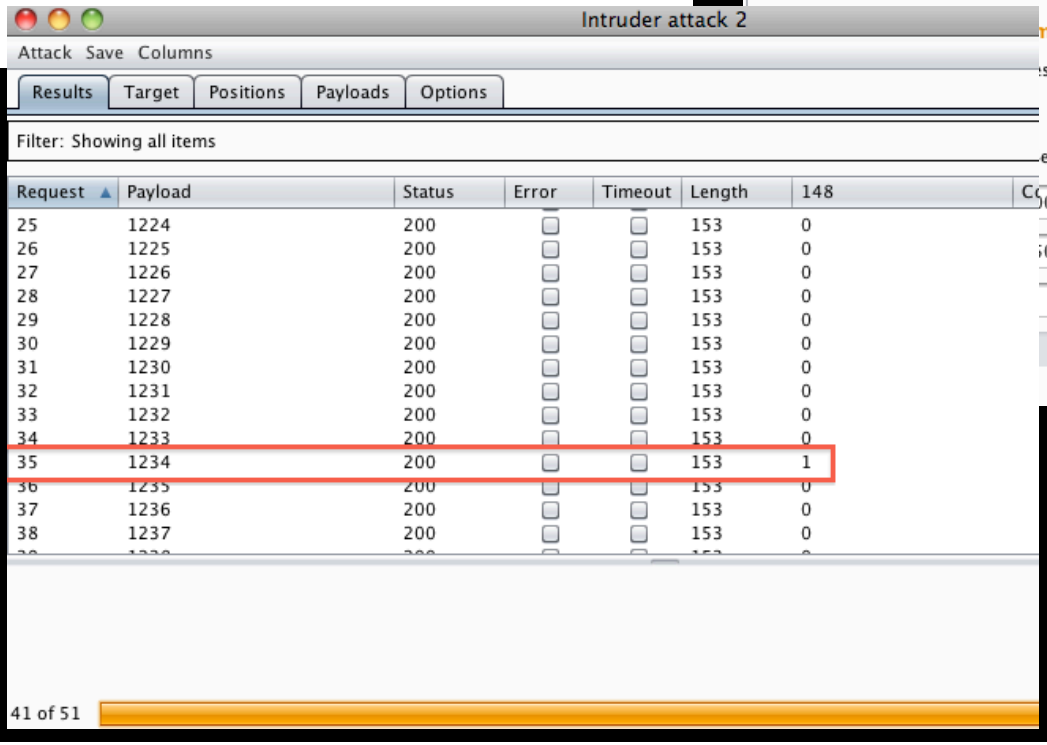


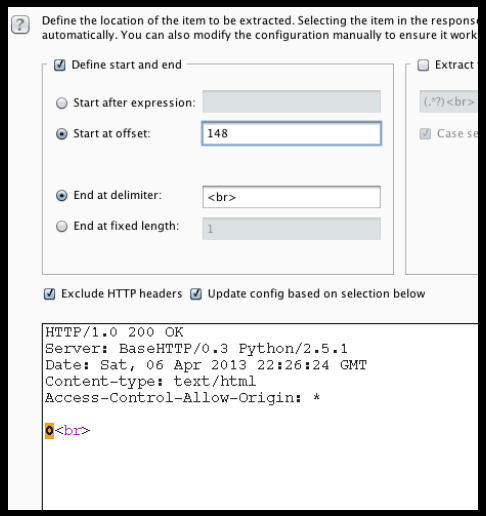
OWASP IL 2013

AppSec Application security Labs

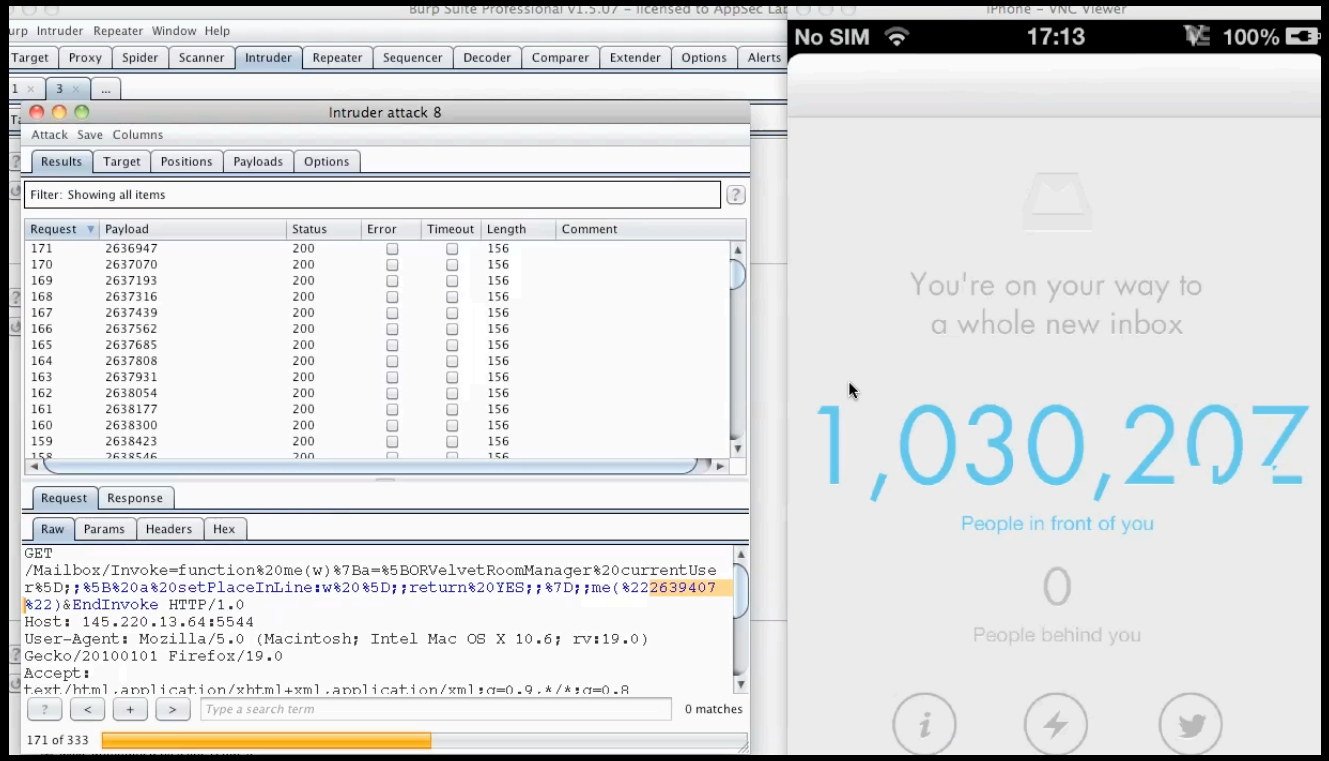

Payload Positions
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help fo
Attack type: Sniper
GET /Dropbox/Invoke=%5BPasscodeViewController%20passcodeEquals:@%22$1200$%22%20%5D&EndInvoke 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


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeate
1 2 ...
Target Positions Payloads Options
Payload Sets
You can define one or more payload sets. The number o
in different ways.
Payload set: 1
Payload type: Numbers
Payload
Request
nbers]
s numeric payloads within a g
equential Random

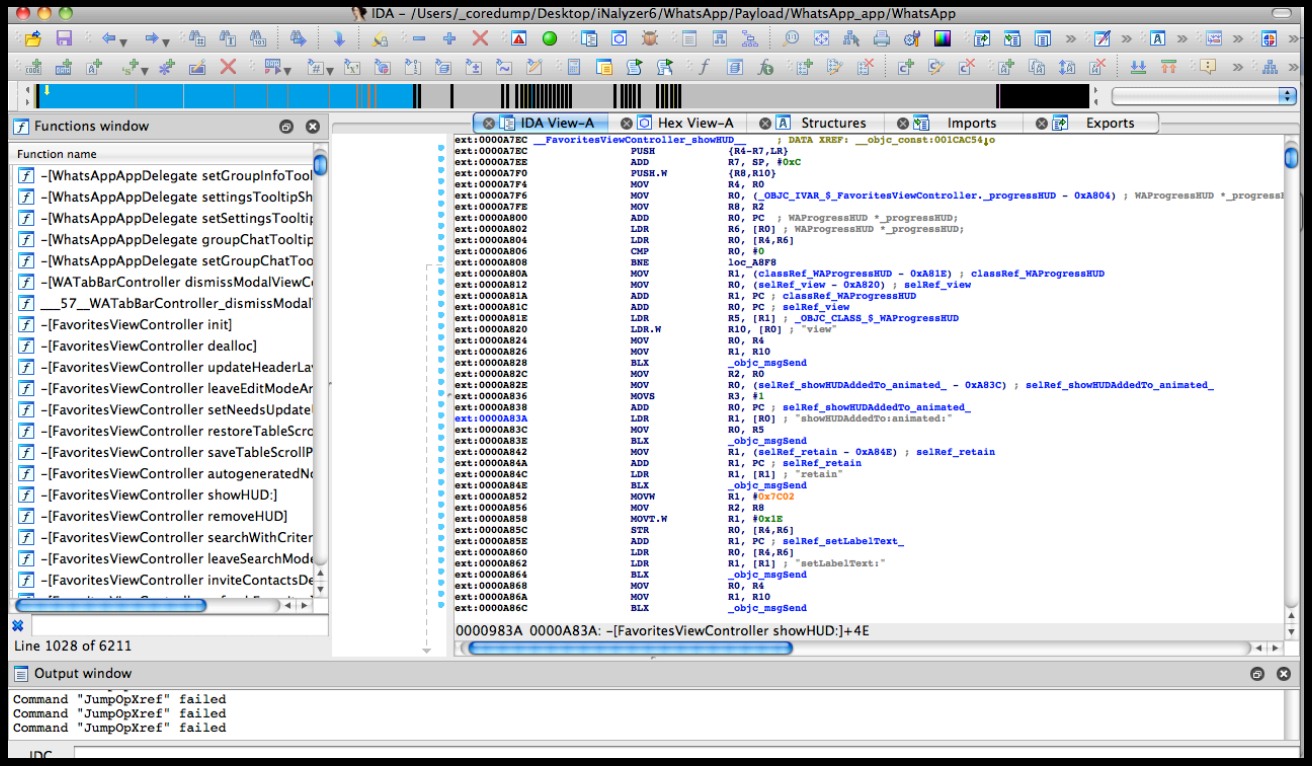

Intruder attack 2
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length 148
25 1224 200 153 0
26 1225 200 153 0
27 1226 200 153 0
28 1227 200 153 0
29 1228 200 153 0
30 1229 200 153 0
31 1230 200 153 0
32 1231 200 153 0
33 1232 200 153 0
34 1233 200 153 0
35 1234 200 153 1
37 1236 200 153 0
38 1237 200 153 0
41 of 51


Define the location of the item to be extracted. Selecting the item in the respons
automatically. You can also modify the configuration manually to ensure it work
Define start and end
Start after expression:
Start at offset: 148
End at delimiter:
End at fixed length: 1
Extract
Exclude HTTP headers
Update config based on selection below
HTTP/1.0 200 OK
Server: BaseHTTP/0.3 Python/2.5.1
Date: Sat, 06 Apr 2013 22:26:24 GMT
Content-type: text/html
Access-Control-Allow-Origin: *
0

iNalyzer & Burp Vs. Mailbox



Wishful thinking: IDA Remote Debugging Obsolete



OWASP IL 2013

AppSec Application security Labs

Demo Single Stepping

```
; 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]
```

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(@saurik)
7. Repeat step 6 until completed
8. SubjectiveC to log selectors (@**kennytm**)

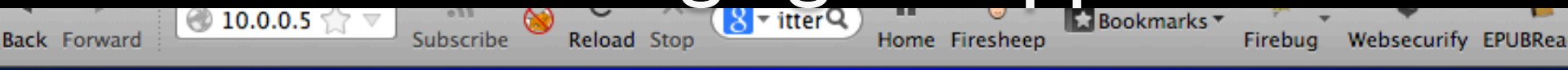
Getting iNalyzer

Repository url: http://appsec-labs.com/cydia

Starting iNalyzer

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

Packaging an App



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

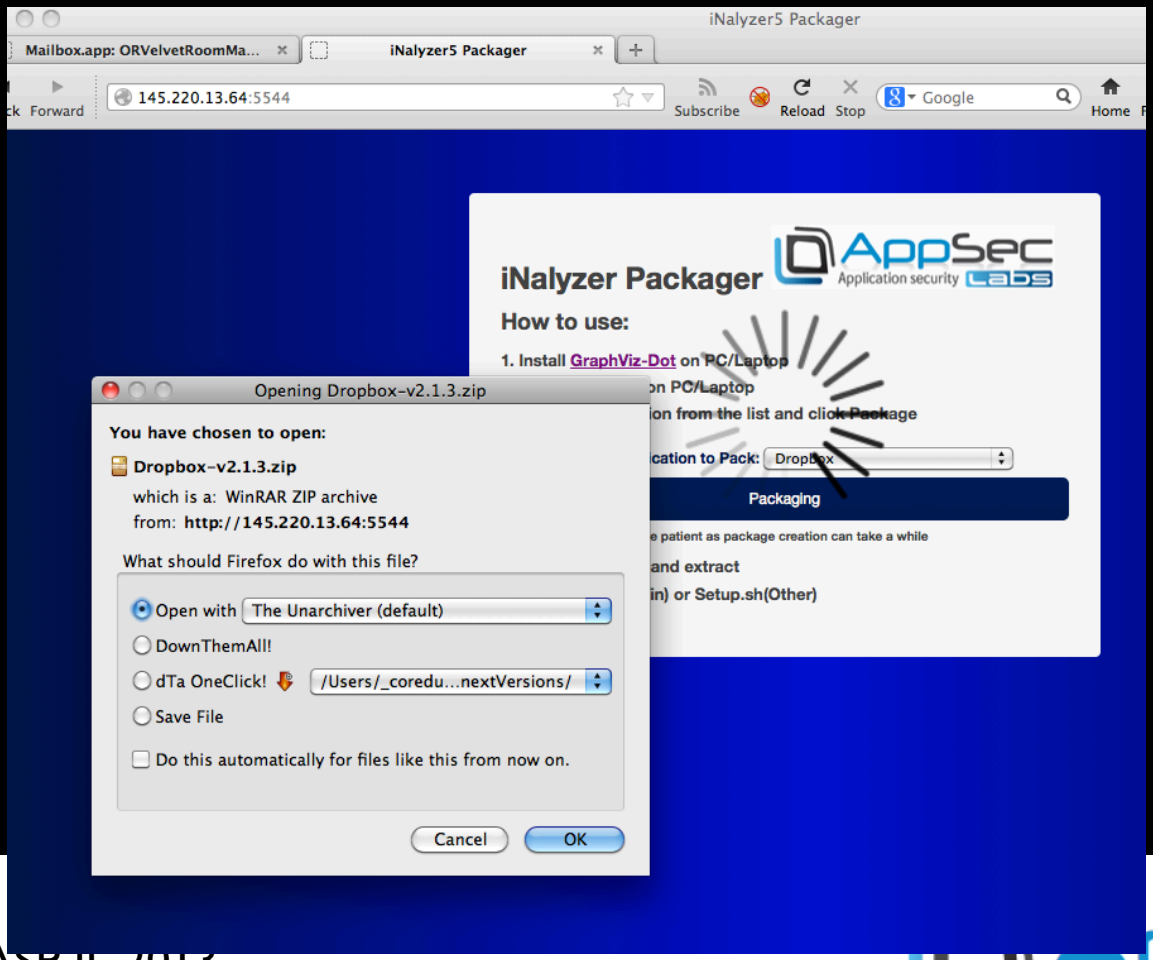
Choose application to Pack: Dropbox

Package

Be patient as package creation can take a while

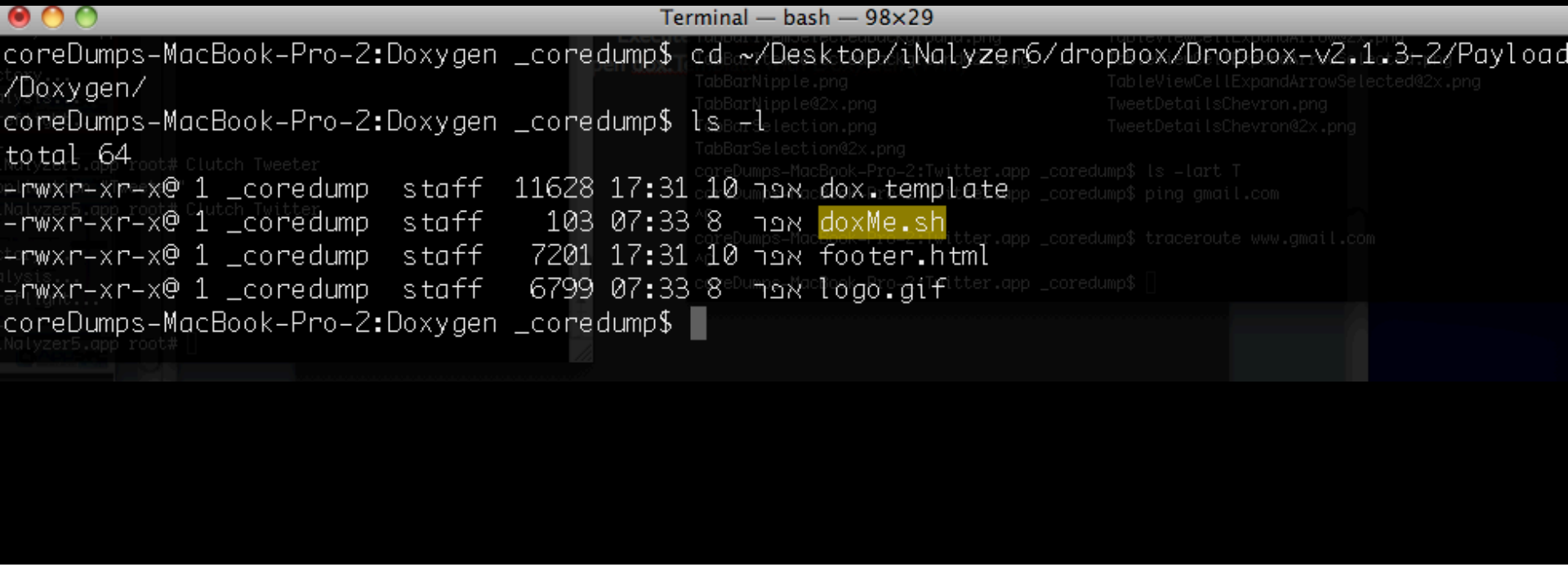
4. Save .zip to disk and extract
5. Run Setup.bat(Win) or Setup.sh(Other)

Download package



Dashboard Building

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



Open Live Demo (as time permits):

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)
  - Mobile Secure Coding (TBD, info@appsec-labs.com)
  - Mobile Awareness (TBD, info@appsec-labs.com)

AppSec Application security Labs

Questions ?

Thank You

AppSec Application security Labs

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

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

AppSec Application security Labs