

GAME OF PWNNS



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, Cypcript, 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



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 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
- B.Sc. Biomedical Engineering

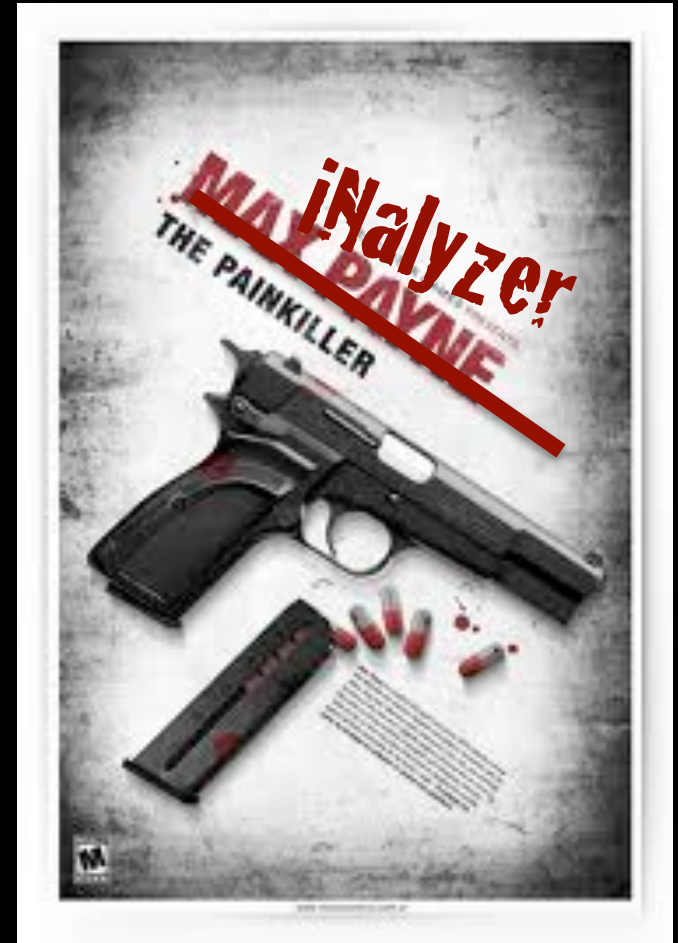


OWASP IL 2013



Agenda

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



OWASP IL 2013

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



iOS App: Common Vulnerabilities



OWASP IL 2013



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
 - Cycrypt
- Network (Proxy, Mallory)



OWASP IL 2013

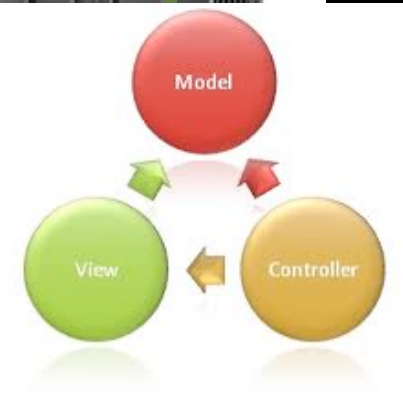
"Pain testing" iOS Apps: Cons

No Code



No Simulator

Unknown end points



% of Functionality
Coverage

Encrypted by iTunes



Hidden vulnerabilities



OWASP IL 2013



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@w00~ 6.7.125.IPHONE 6.7.125@10Q+~~~~~ he_IL Asia/Jerusalem~ 6.7.125@10_ã~~~~~ he_IL Asia/
iPhone3,1 6.7.125@10Q+~~~~~ he_IL Asia/Jerusalem~ 6.7.125@10_ã~~~~~ he_IL Asia/
a/Jerusalem~ 6.7.125@Z(~I~~~~~ he_IL Asia/Jerusalem~ 6.7.125@_!<~ Ö~ < he_IL Asia/
feed.closemcv.feed feed.refresh mcv.feed ÇΣ¶ feed.refresh Çaf
feed.close Ê2Umcv.feed Ê9q feed.refresh Ê;m 6.7.125@wBMvME he_IL Asia/Jerusalem~ mcv.fe
```



OWASP IL 2013



Agony++ unknown peers

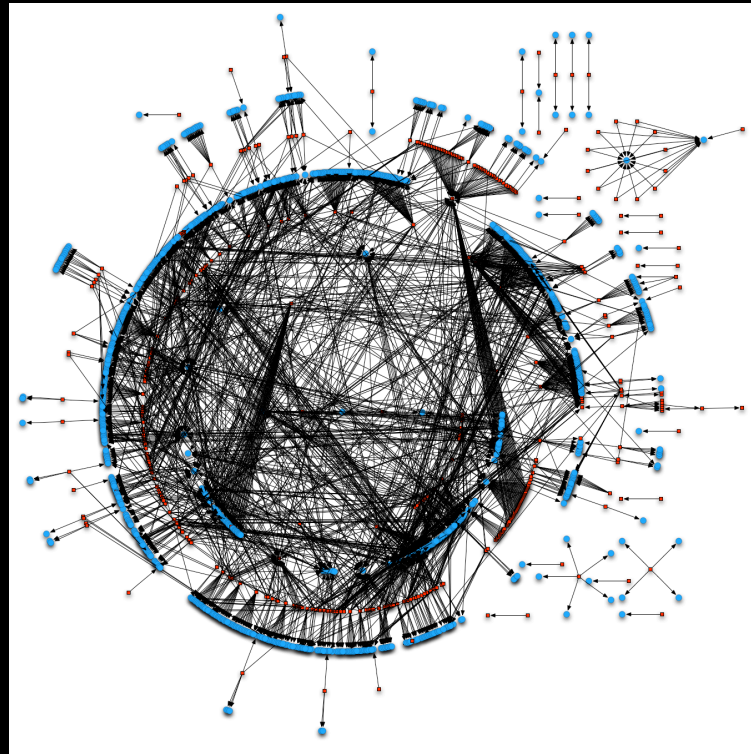


OWASP IL 2013



Single Stepping

Everything drills down to ObjC_msgSend()



OWASP IL 2013



Not enough Time



OWASP IL 2013



Doesn't play well with other tools



OWASP IL 2013



The Business Axiom

ONE DOES NOT SIMPLY SUBMIT



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

...emegenerator.net



OWASP IL 2013



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

Surprise, Surprise!

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



OWASP IL 2013



Objective C class interposing

Presenting a new implementation to a foundation class selector:

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

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

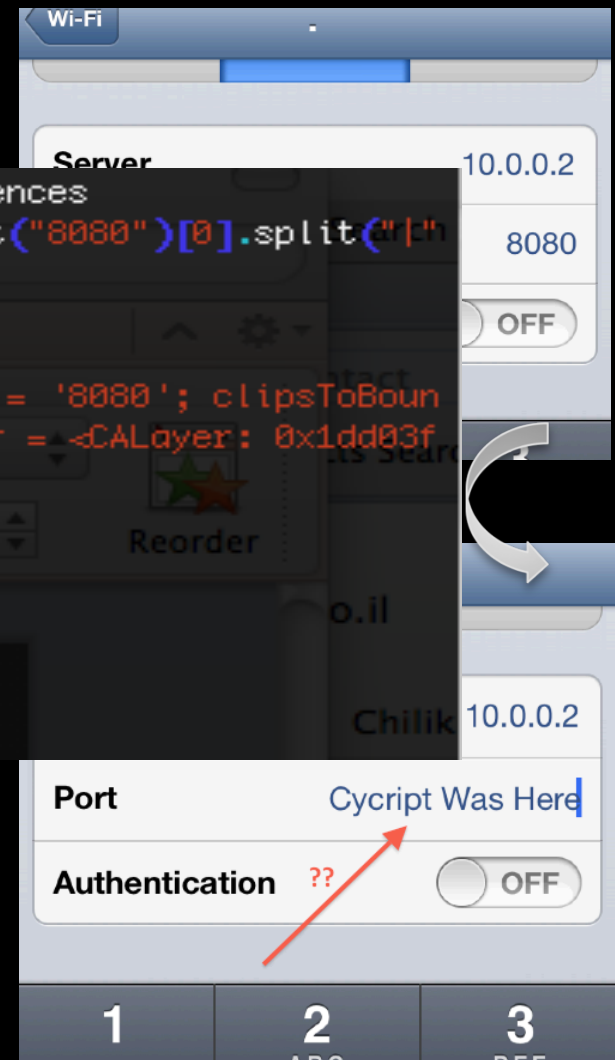


OWASP IL 2013



Cycrypt: Tampering tool

```
iPhone:/Applications/iNalyzer5.app root# cycrypt -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'; clipsToBounds = YES; gestureRecognizers = <NSArray: 0x1dd04fd0>; layer = <CALayer: 0x1dd03f70>>"
cy# lable.text
@"8080"
cy# lable.text=@"Cycrypt Was Here"
@"Cycrypt Was Here"
cy#
```



OWASP IL 2013

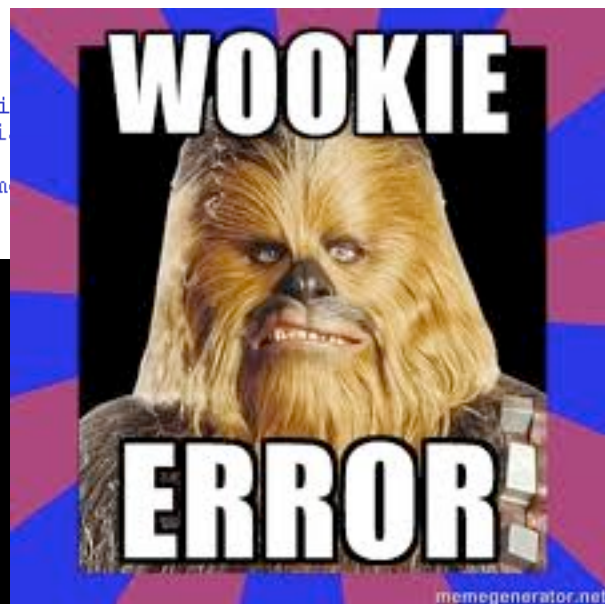


Solving Binary Protocols

```
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"â6 6.7.125 IPHONE' OR '1'='1' -->Pe;#@wBMv device.model.1
iPhone3,1 6.7.125@10Q+~~~~~ he_IL Asia/Jerusalem 6.7.125@1Q,â~~~~~ he_IL Asi
a/Jerusalem 6.7.125@Z(~f~~~~~ he_IL Asia/Jerusalem 6.7.125@_!<* Ö~ / he_IL Asi
feed.closemcv.feed feed.refresh mcv.feed ÇÏ feed.refresh ÇÏ
feed.close Ê2Umcv.feed Ê9q feed.refresh Ê;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



Storyboard Collection



Demo



OWASP IL 2013



Storyboard Failure

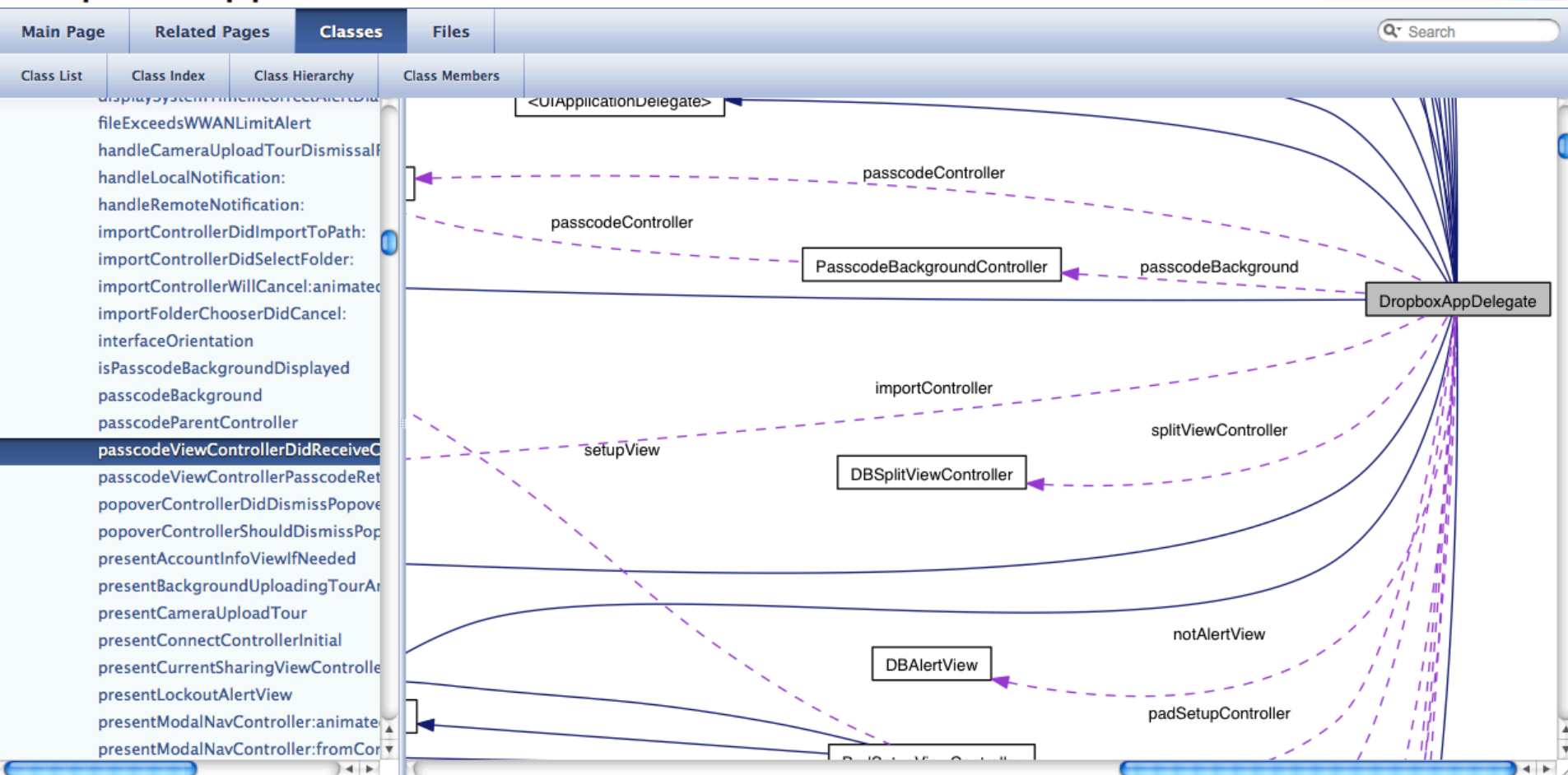


OWASP IL 2013

iNalyzer Dashboard

Dropbox.app

iNalyzer Dashboard  AppSec Labs
Application security



OWASP IL 2013

 AppSec Labs
Application security

▼ 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 = ?
```



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 t  
    http://www.waze.com/legal/privac  
    indicates your consent to them.  
    only.  
67 6632 <DROPTYPE> <list> PUBLIC # / (3m
```

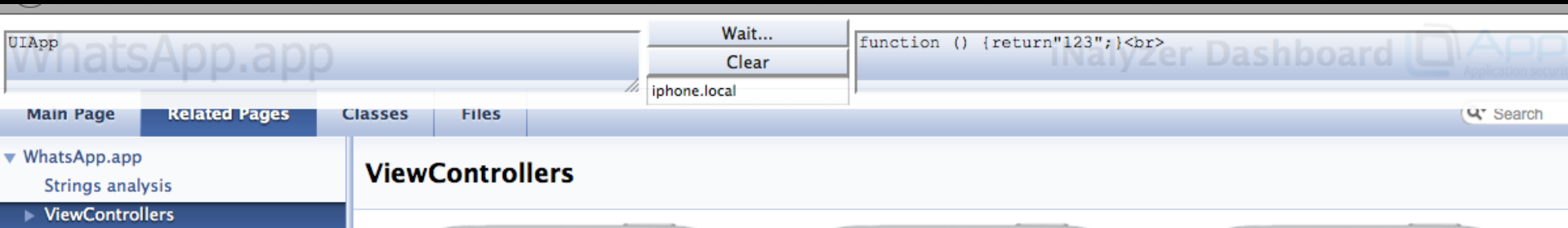
waze:///?%6f%70%65%6e%5f%75%72%6c%3d%68%74%74%70%3a%2f%2f
%74%72%2e%69%6d%2f%34%36%35%77%35



OWASP IL 2013



Cycript Console



Demo



OWASP IL 2013



Demo: Expanding iNalyzer with Burp

file:///Users/_coredump/Desktop/iNalyzer6/dropbox/Dropbox

Dropbox:app

Wait... Clear 10.0.0.5

iNalyzer Dashboard

Burp Suite Professional v1.5.07 – licensed to AppSec Labs [single user license]

Main Page Related Pages **Classes** Files

Class List Class Index Class Hierarchy Class Member

- PadTabView
- PadTabViewDelegate-p
- PasscodeBackgroundController
- PasscodeSettingsTableViewController
- PasscodeView
- PasscodeViewController**
- PasscodeViewControllerDelegate-p
- Payments
- PDFCompositeFontInfo
- PDFDocumentViewController
- PDFSimpleFontInfo
- PhotoPermissionController
- PhotoPermissionControllerDelegate-p
- PhotoViewController
- PLCrashReport
- PLCrashReportApplicationInfo
- PLCrashReportBinaryImageInfo
- PLCrashReporter
- PLCrashReporterCallbacks
- PLCrashReportExceptionInfo
- PLCrashReportFormatter-p
- PLCrashReportMachineInfo

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept History Options

Request to http://coredumps-iphone.local:5544 [10.0.0.19]

Forward Drop Intercept is on Action

Raw Headers Hex

GET /Dropbox/Invoke=%5BPasscodeViewController%20passcodeEquals:@%221200%22%20%5D%20EndInvoke HTTP/1.1

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

passcodeViewController

Static Public Member Functions

- (void) + clearPasscode
- (BOOL) + isPasscodeSet
- (BOOL) + **passcodeEquals:**
- (void) + setRequireImmediatelyOnActive:
- (BOOL) + requireImmediatelyOnActive
- (void) + setEraseDataOnPasscodeFailure:
- (BOOL) + eraseDataOnPasscodeFailure



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 details.

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
```

Payload Sets

You can define one or more payload sets. The number of sets and the number of payloads in each set can be defined in different ways.

Payload set: Payload

Payload type: Request

Define the location of the item to be extracted. Selecting the item in the response will extract it automatically. You can also modify the configuration manually to ensure it works.

☒ Define start and end

☐ Start after expression:

☒ Start at offset:

☐ End at delimiter:

☐ End at fixed length:

☒ Exclude HTTP headers
 ☒ Update config based on selection below

☐ Extract

☐ Case sensitive

```
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: *
```

**
**

Intruder attack 2

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

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

Sequential ☒ Random ☐

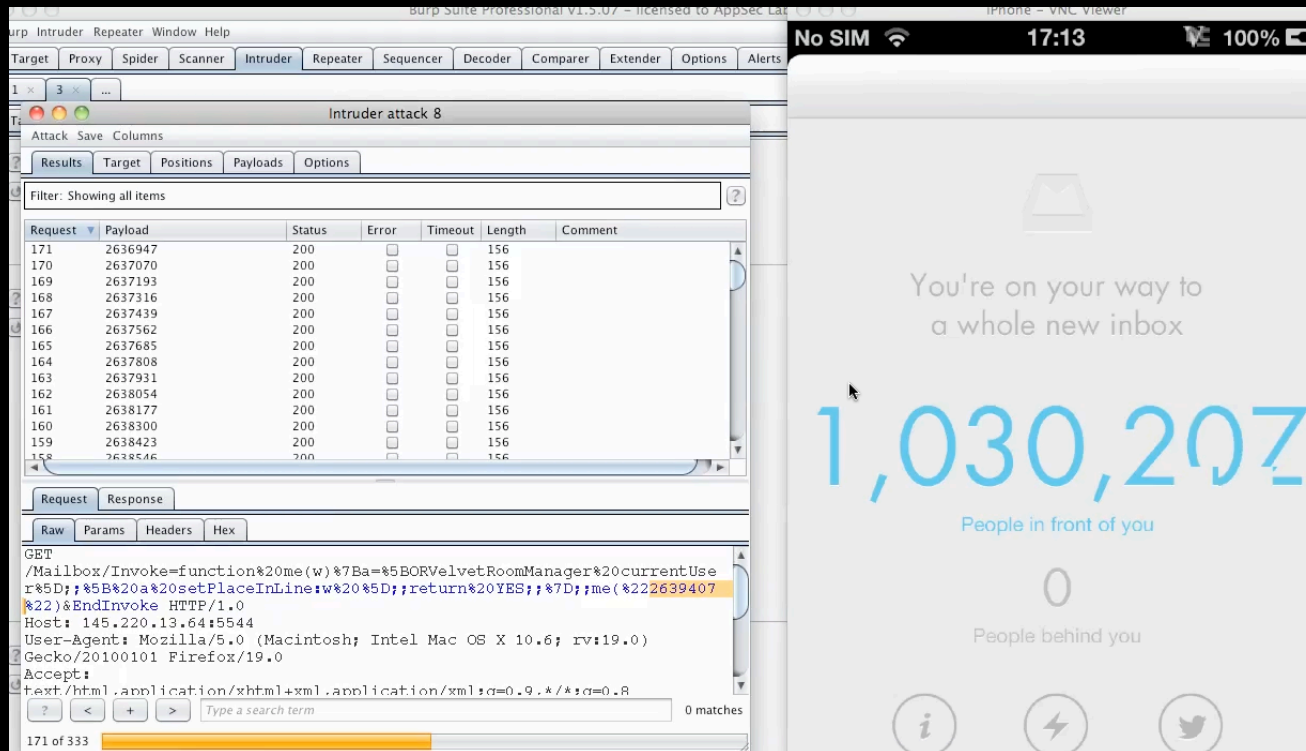
41 of 51



OWASP IL 2013



iNalyzer & Burp Vs. Mailbox



The image shows a side-by-side comparison of a web security tool and a mobile application. On the left is the Burp Suite Professional interface, version 1.5.07, with the 'Intruder' tab selected. It displays a table of 171 items, each with a request ID, payload, status, error, timeout, length, and comment. The bottom panel shows the raw HTTP request details for item 171, which is a GET request to a mailbox endpoint with a complex payload. On the right is a screenshot of an iPhone screen displaying the Mailbox app. The app shows a message 'You're on your way to a whole new inbox' and a large blue number '1,030,207' representing the number of people in front of the user. The status bar at the top of the iPhone screen shows 'No SIM', signal strength, time '17:13', and battery level '100%'.

Request	Payload	Status	Error	Timeout	Length	Comment
171	2636947	200	☐	☐	156	
170	2637070	200	☐	☐	156	
169	2637193	200	☐	☐	156	
168	2637316	200	☐	☐	156	
167	2637439	200	☐	☐	156	
166	2637562	200	☐	☐	156	
165	2637685	200	☐	☐	156	
164	2637808	200	☐	☐	156	
163	2637931	200	☐	☐	156	
162	2638054	200	☐	☐	156	
161	2638177	200	☐	☐	156	
160	2638300	200	☐	☐	156	
159	2638423	200	☐	☐	156	
158	2638546	200	☐	☐	156	

Raw Request Details:

```
GET /Mailbox/Invoke=function%20me(w)%7Ba=%5BORVelvetRoomManager%20currentUse
r%5D;%5B%20a%20setPlaceInLine:w%20%5D;%return%20YES;%7D;%me(%222639407
%22)%20EndInvoke HTTP/1.0
Host: 145.220.13.64:5544
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
```



OWASP IL 2013



The screenshot shows the IDA Pro interface with the following components:

- Functions window:** Lists various methods of the FavoritesViewController class, including `setGroupInfoTool`, `setSettingsToolTip`, `setGroupChatTool`, `dismissModalView`, `initWithNibName:bundle:`, `dealloc`, `updateHeaderLabel`, `leaveEditModeAction`, `setNeedsUpdate`, `restoreTableScrollPosition`, `autogeneratedNewMethod`, `showHUD:`, `removeHUD`, `searchWithCriteria`, `leaveSearchMode`, and `inviteContactsDialog`.
- IDA View-A:** Displays the assembly code for the `showHUD` method. The code starts with `ext:0000A7EC` and ends with `0000983A 0000A83A: -[FavoritesViewController showHUD]:+4E`.
- Hex View-A:** Displays the raw hex data for the `showHUD` method.
- Structures:** Shows the structure of the `FavoritesViewController` class.
- Imports:** Lists the imported symbols for the `showHUD` method.
- Exports:** Lists the exported symbols for the `showHUD` method.
- Output window:** Shows the command `JumpOpXref" failed` repeated three times.



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]
```



OWASP IL 2013



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. Cycrypt to modify the app behavior (@saurik)
7. Repeat step 6 until completed
8. SubjectiveC to log selectors (@kennytm)



OWASP IL 2013



Getting iNalyzer



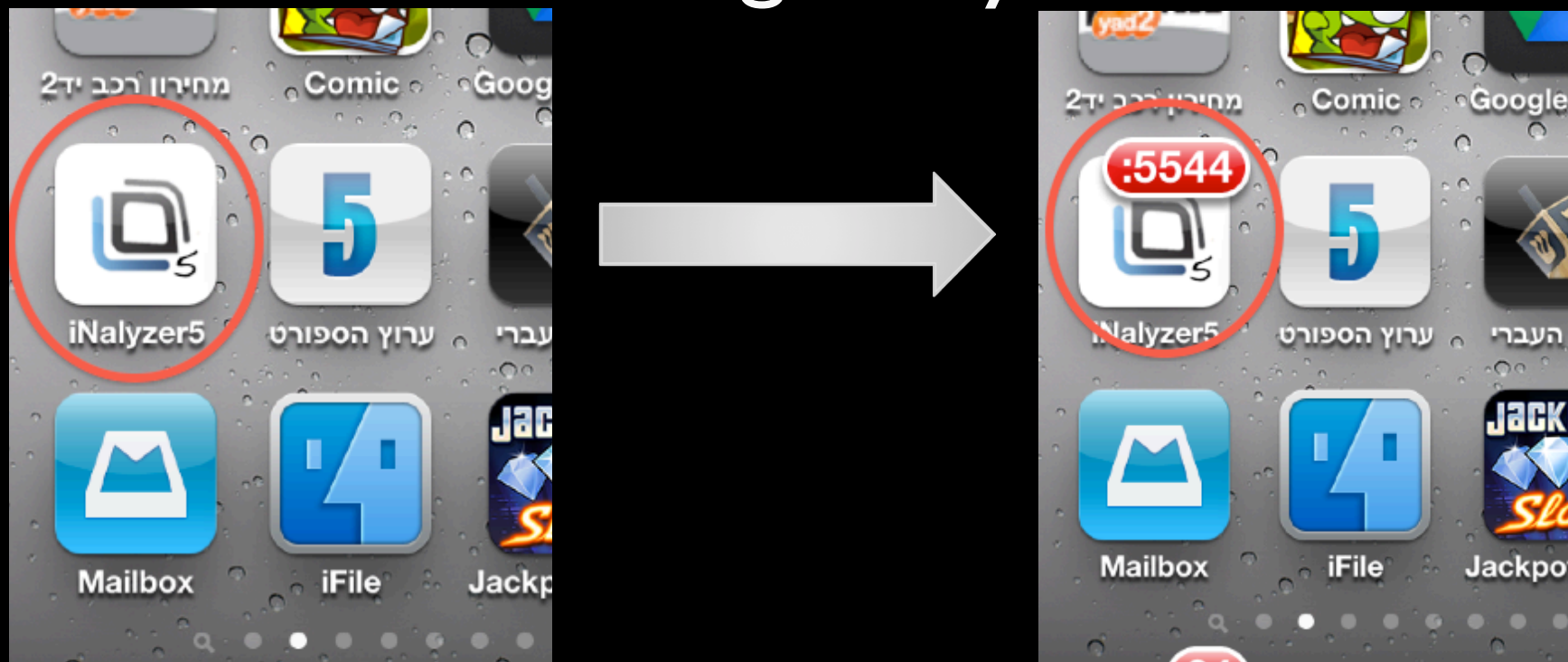
Repository url: <http://appsec-labs.com/cydia>



OWASP IL 2013



Starting iNalyzer



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



OWASP IL 2013



Packaging an App

Back Forward 10.0.0.5 ☆ itterQ Subscribe Reload Stop Home Firesheep Bookmarks Firebug Websecurify EPUBRea

iNalyzer Packager



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

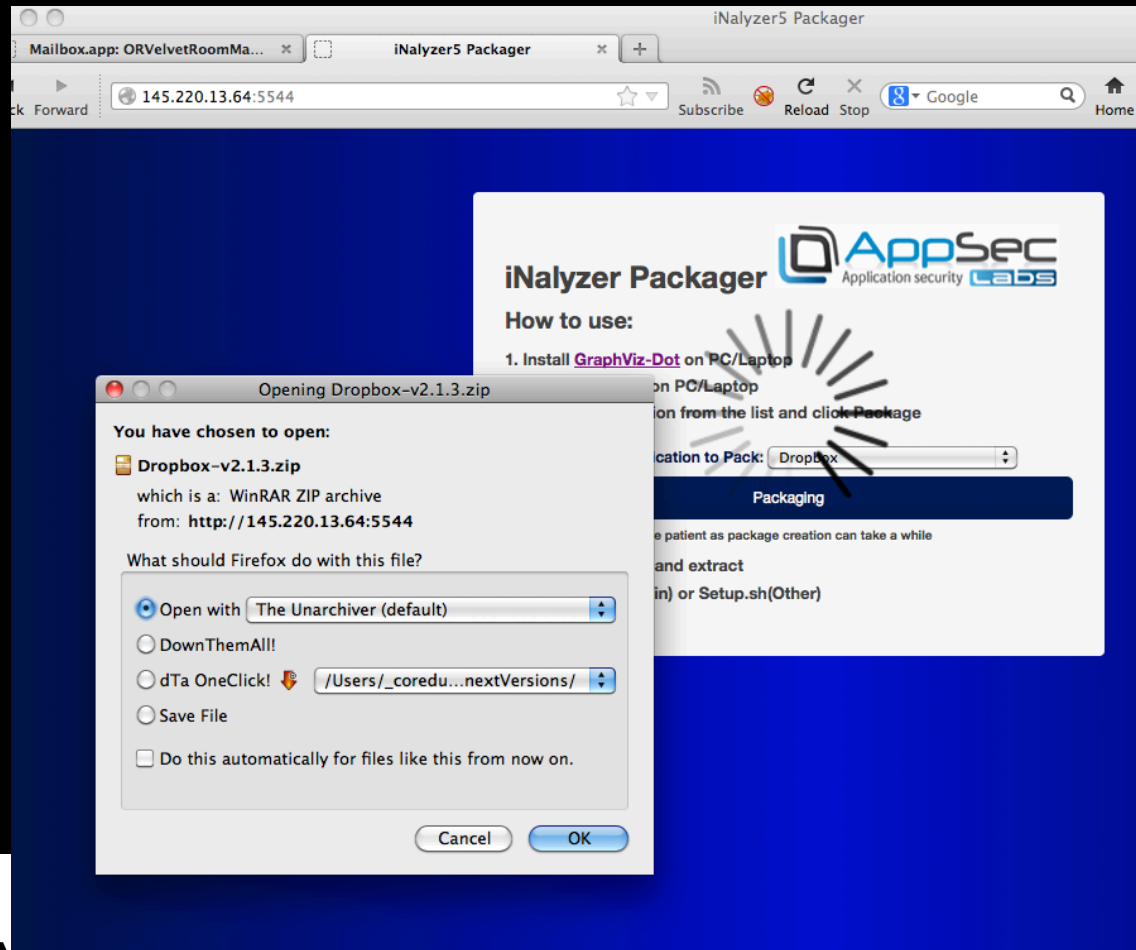
Choose application to Pack:

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)

Download package



OWASP IL 2013



Dashboard Building

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

```
Terminal — bash — 98x29
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
-rwxr-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
-rwxr-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)
 - Mobile Secure Coding (TBD, info@appsec-labs.com)
 - Mobile Awareness (TBD, 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>
- Cycrypt – <http://www.cycrypt.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>

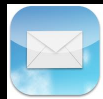


Game of Pwns: Advanced iPhone testing with iNalyzer framework <https://appsec-labs.com/iNalyzer>

Chilik Tamir
Chief Scientist



@_coreDump



chilik <at> appsec-labs.com



www.appsec-labs.com



OWASP IL 2013

