
# iNalyzer – No More iOS Blackbox Assessments

Chilik Tamir

Chief Scientist

AppSec-Labs.com


AppSec Application security Labs

# 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 ☺~~


AppSec Application security Labs

# 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: OWASP IL (2011,2012) DC9723(2013)
- B.Sc. Biomedical Engineering


# Agenda

- Current BlackBox iOS Technique
- Current Agony
- iNalyzer


AppSec Application security Labs

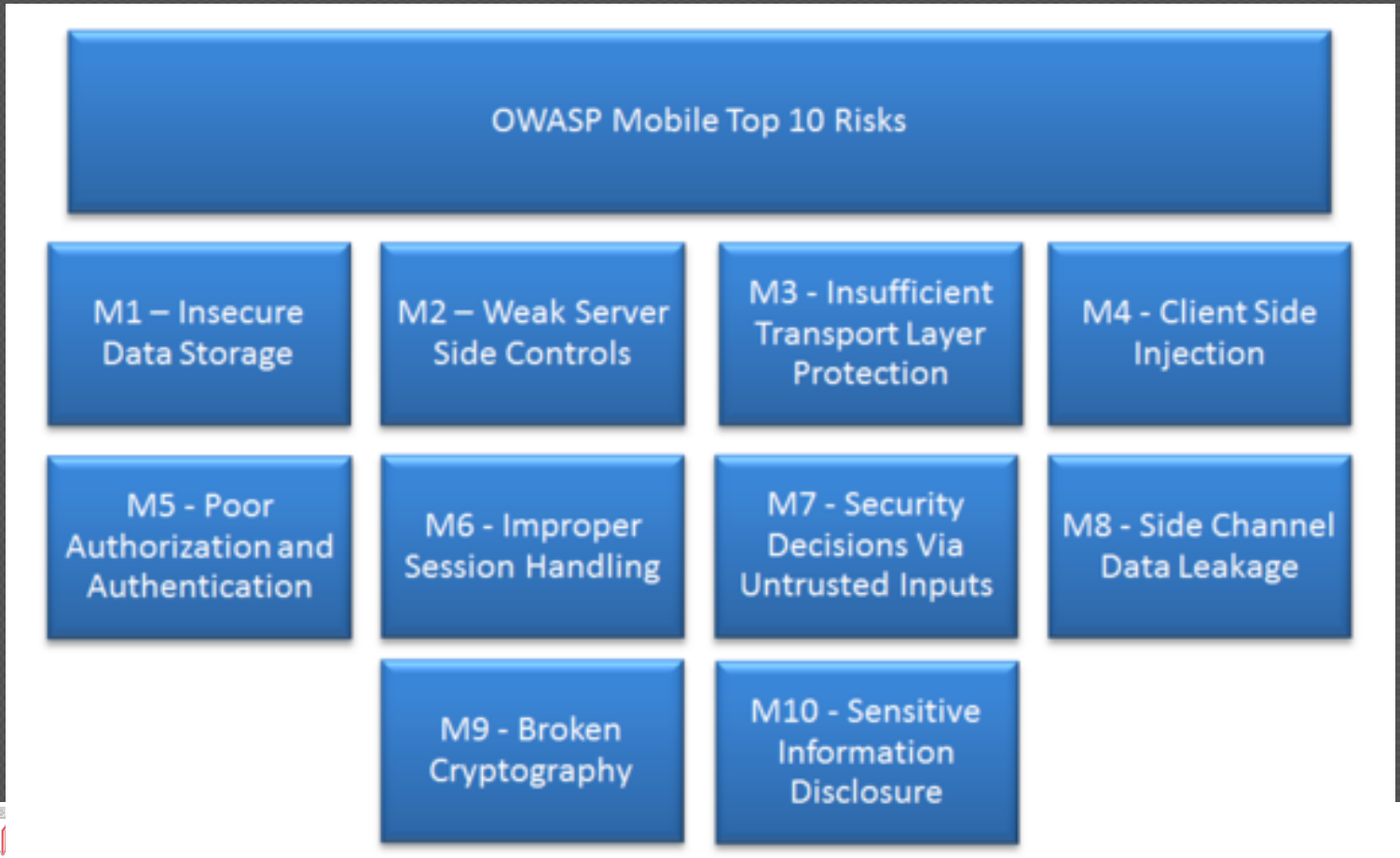
# iOS Apps and vulnerabilities

# Recap: What's an iOS App ?

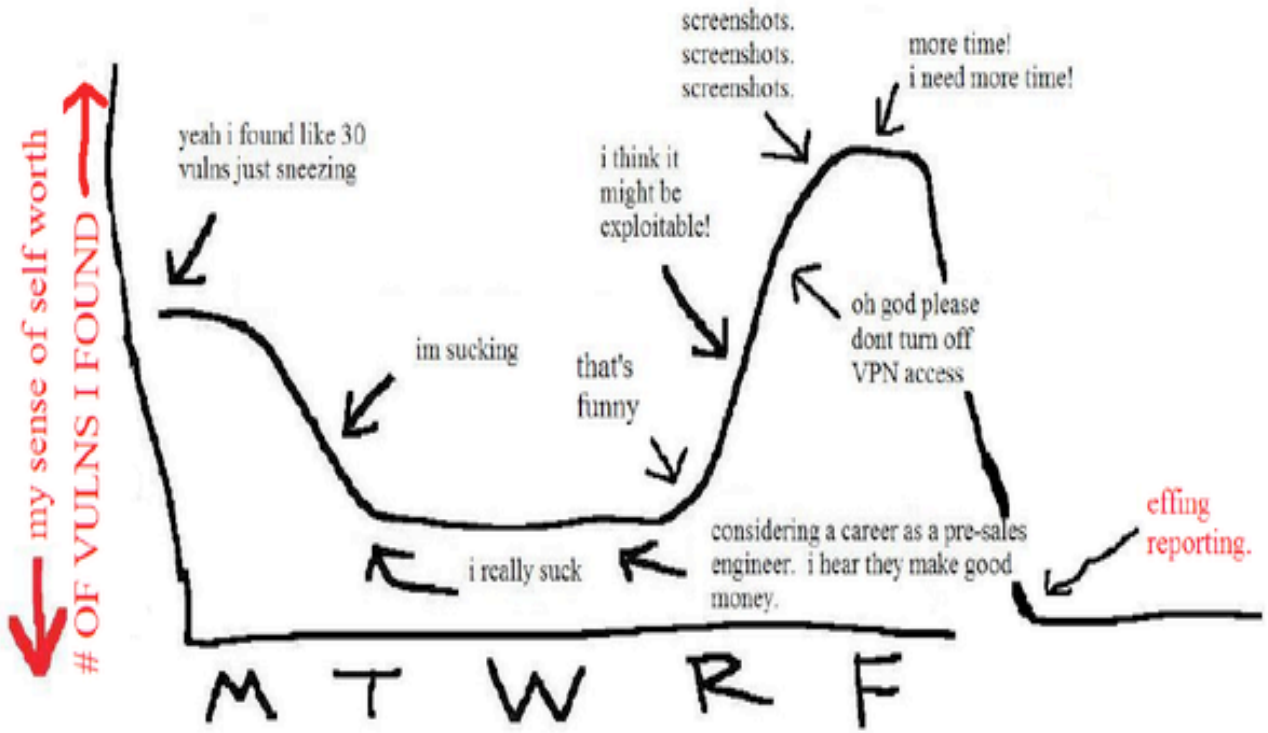
- ObjC/C/C++ Compiled (ARM) Executable
- Encrypted Executable (fairplay)
- Self contained under ~/Applications/GUID/AppName.app folder
- Installed by "mobile" user
- Executes under sandbox
- Under the radar can escape (SpyPhone, Storm8, etc.)

# iOS App: Common Vulnerabilities

Source: www.owasp.org



# Real World Pen Testing




http://www.securitygeneration.com/security/pic-of-the-week-real-world-penetration-testing/

# Black Box Assessing Apps

# iOS Black Box means

Static analysis
Dynamic analysis


AppSec Application security Labs

# Static Analysis Tools

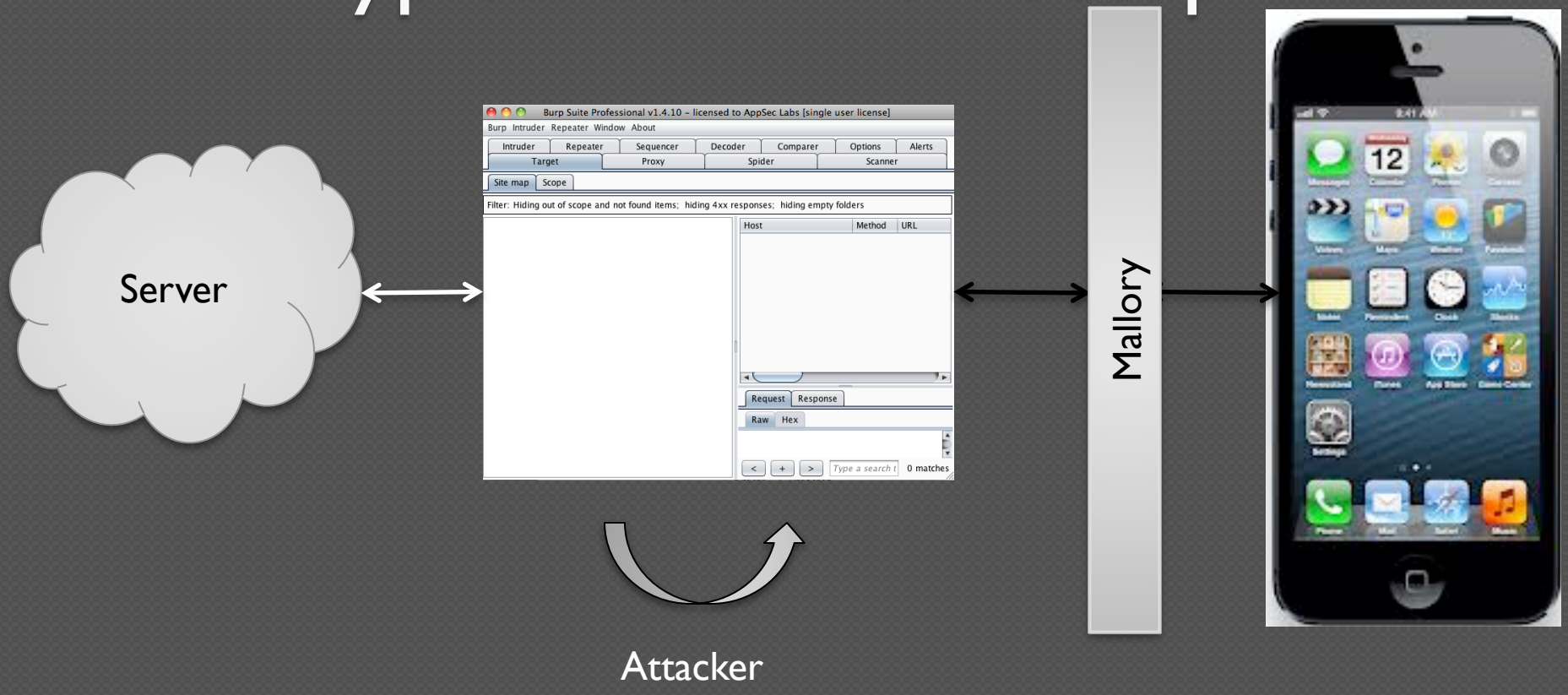
- Tools:
  - iFile / iTools/ iExplorer (Cydia iOS/PC)
  - Clutch (Cydia)
  - IDA / Dissasembler (PC)
  - SSH / Putty (iOS + PC)
  - HexEditor (Win/Mac)
  - Plist Editor (iOS, PC)
  - SQLite Browser (Win/Mac)

# Dynamic Analysis Tools

- Tools:
  - Proxy (PC) + Certificate (Root CA)
  - iSEC SSL KillSwitch (iOS)
  - Mallory (VM)
  - WiFi HotSpot
  - Cycript (iOS)
  - Class-Dump-Z (iOS)
  - GDB (iOS)
  - Theos / Logos / CaptainHook (iOS)


AppSec Application security Labs

# Typical Black Box Setup



# Black Box Agony: Uncover the missing pieces

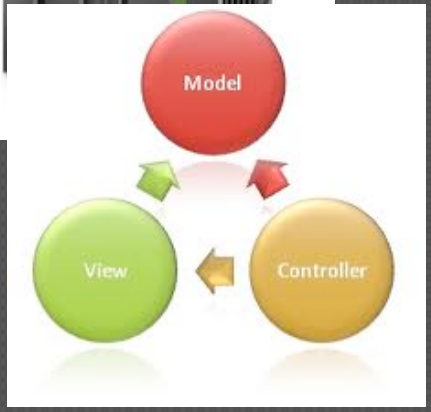
No Code

No Simulator


Encrypted by iTunes

Hidden vulnerabilities

Unknown end points




% of Functionality Coverage

# Typical approach

- File System:
  - Monitoring (DB, Plist, Logs)
  - Tampering (SQLite, plutil)
- Network:
  - Monitoring (Mallory, Proxy)
  - Tampering (Proxy, Scanners, tools)
- Application Resources:
  - CFURL invocations
  - EA protocols


AppSec Application security Labs

# Typical approach - Cont

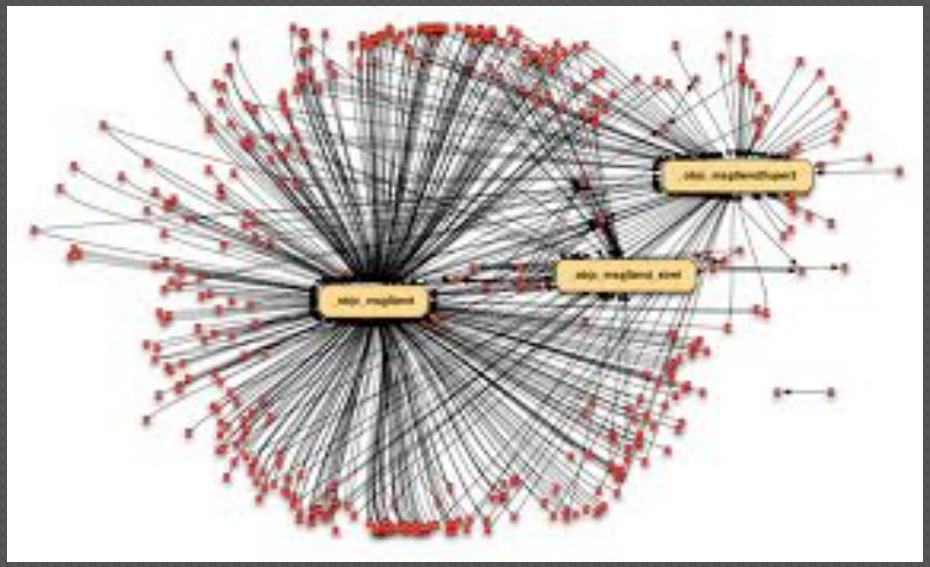
- Binary:
  - Decryption (Clutch)
  - Class identification (class-dump-z)
  - Reversing (IDA)
  - Patching (when needed)

- Application Runtime:
  - Objc_msgSend monitor
  - Theos / Logos Tweaks
  - GDB
  - Cycript


AppSec Application security Labs

# Typical approach – ARM RCE ing

## Use GDB / IDA Pro + zynamics

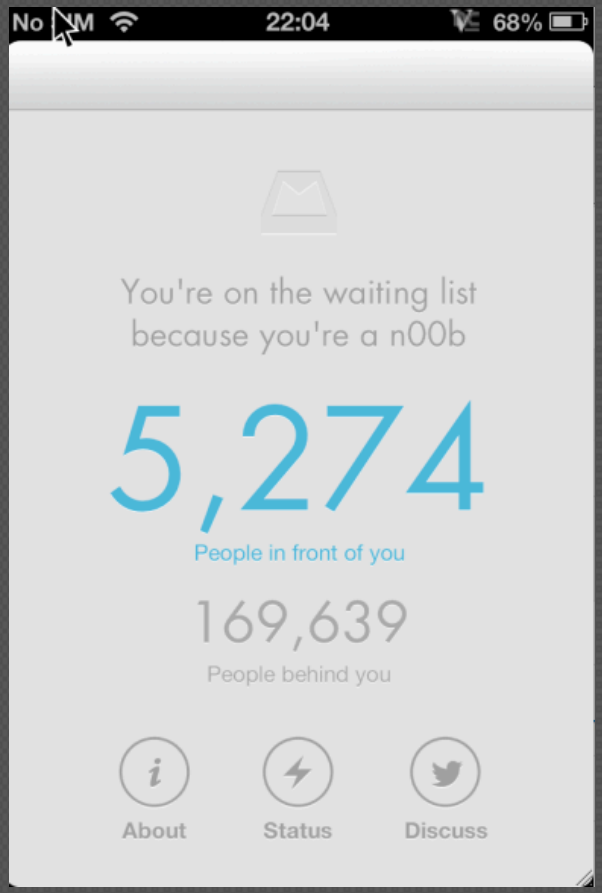


Problems:

- Assembly Language ARM
- Overhead for mid scope
- Tedious
- Manual

# Eventually you will get there..

# Black Box Agony: Signing




Raw Params Headers Hex

```
POST /check HTTP/1.1
Host: prod-mistert.orcali.com
Proxy-Connection: close
Accept-Encoding: gzip
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Content-Length: 124
Connection: close
User-Agent: Mailbox 1.1.0 (iPhone; iPhone OS 6.1.2; he_IL)

uuid=[redacted]&version_number=1.1.0&line_number=1[redacted]8&checksum=a00683548887b4b6d8449597d7fae6f06
```

? < + > Type a search term

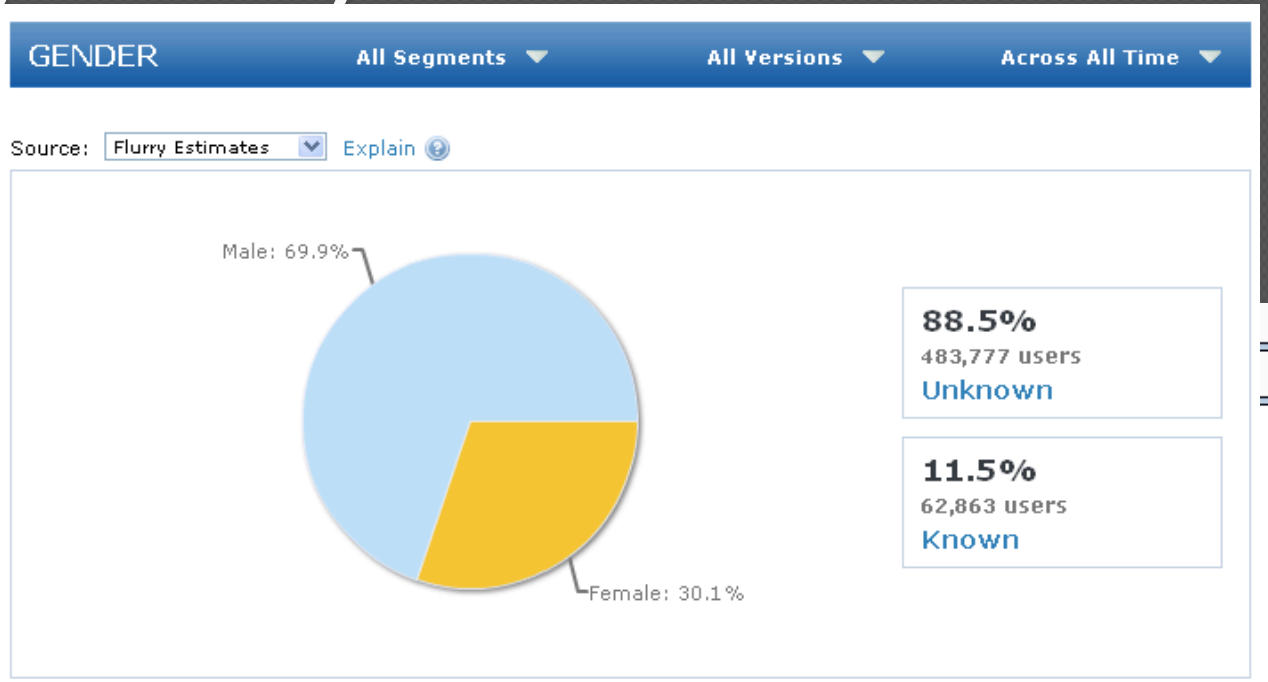
Response

Raw Headers Hex

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=utf-8
Date: Thu, 04 Apr 2013 20:19:29 GMT
X-Powered-By: Express
Content-Length: 15
Connection: Close

invalid request
```

# Agony: Binary Protocols



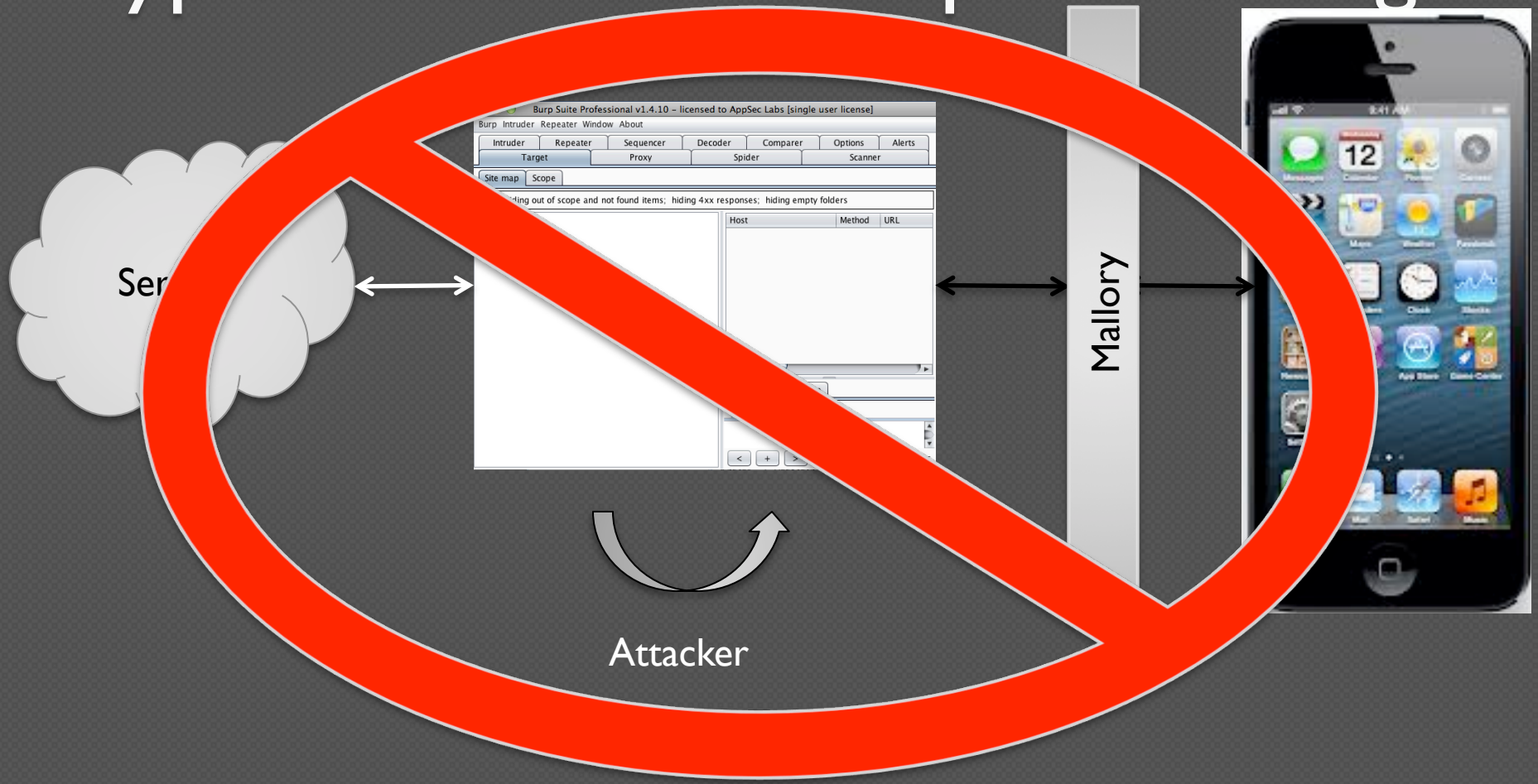

Request | Response

Raw | Params | Headers | Hex

```
POST /aas.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: 357
Connection: keep-alive
User-Agent: Pango/3.0 CFNetwork/609.1.4 Da
```

```
Oé¢'ß[redacted].0 Çèoóoé¨È 5r0 ™‹ Ç{Ç ¡ Ûç&ôã≤º—öÑ7Ï ¿ÎBP% &I[redacted]5B =ádmŒé¢" '
scr.height 480 scr.width 320 device.os.version 6.1.2 device.model.1 iPhone3,1 3.0é¢" ' ì› he_IL Asia/Jerusalem˜˘^—%g
```

# Typical Black Box Setup: not enough



# 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:

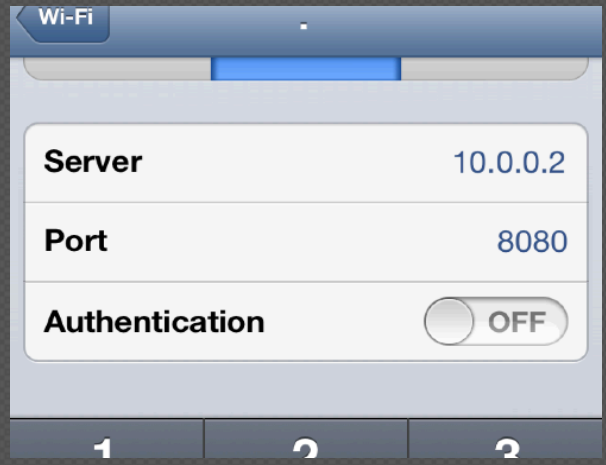
```
NSString->isa.messages["stringWithString:"]=function(a){
return "HackedAccount" }
```

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

# Cycript: Tampering tool

- Not a new concept
  - F-script.org (OSX)
  - Cycript (@saurik iOS)

(J. Zdziarski – Hacking and securing iOS applications)



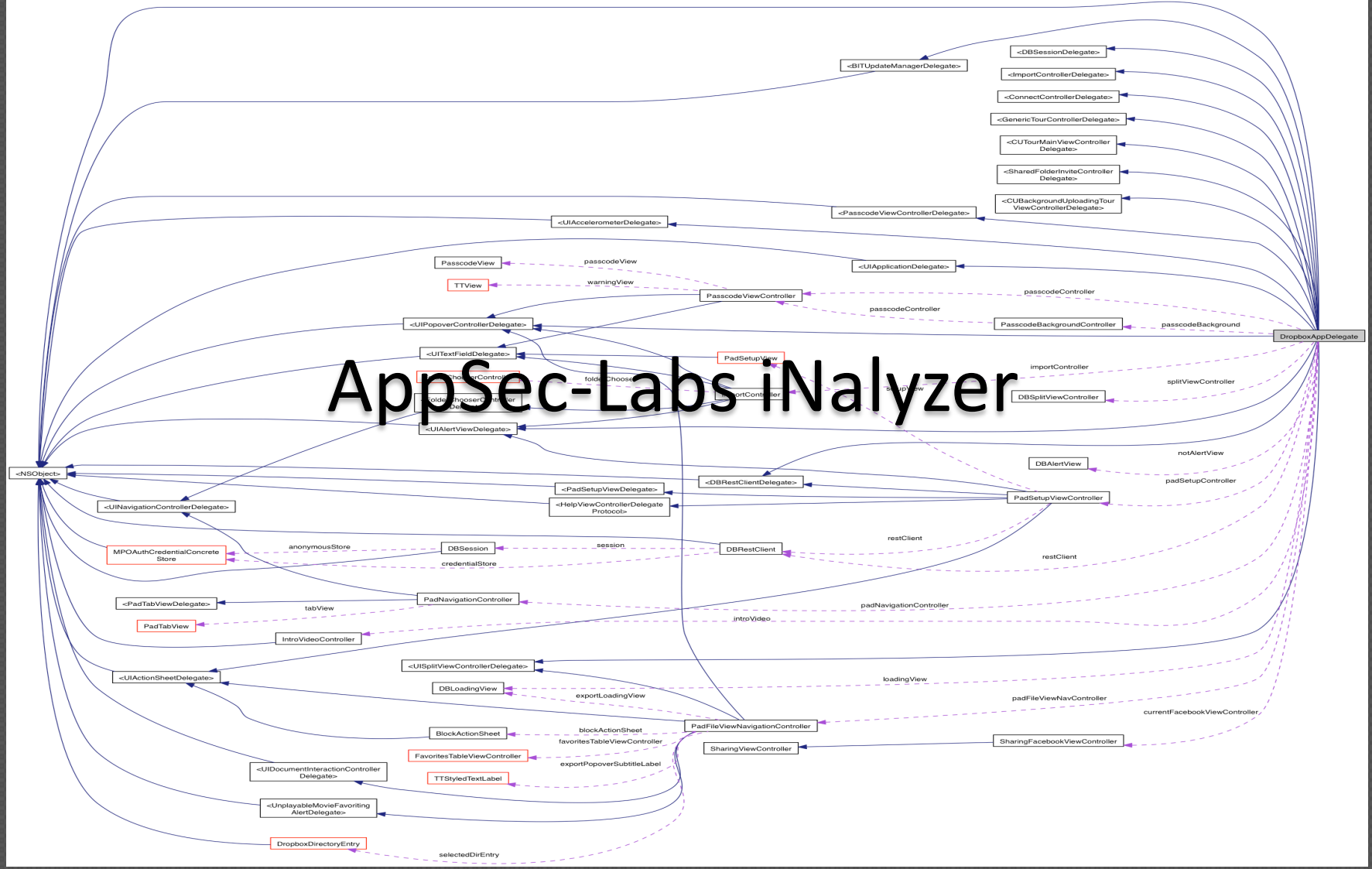


```
iPhone:/Applications/iNalyzer5.app root# cycript -p Preferences
cy# [UIApp.keyWindow recursiveDescription].toString().split("8080")[0].split("|"
).pop().split(";")[0].split(": ")[1];
"0x1dd03400"
cy# var lable=new Instance(0x1dd03400)
@"<UITextField: 0x1dd03400; frame = (115 10; 175 24); text = '8080';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

Binary protocols
Signed Request

Solved, But need advanced inside
Application knowledge


AppSec Application security Labs




# AppSec-Labs iNalyzer

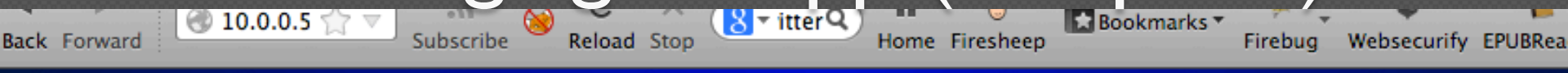
# Getting iNalyzer


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

# Starting iNalyzer


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

# Packaging an App (Dropbox)




## 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

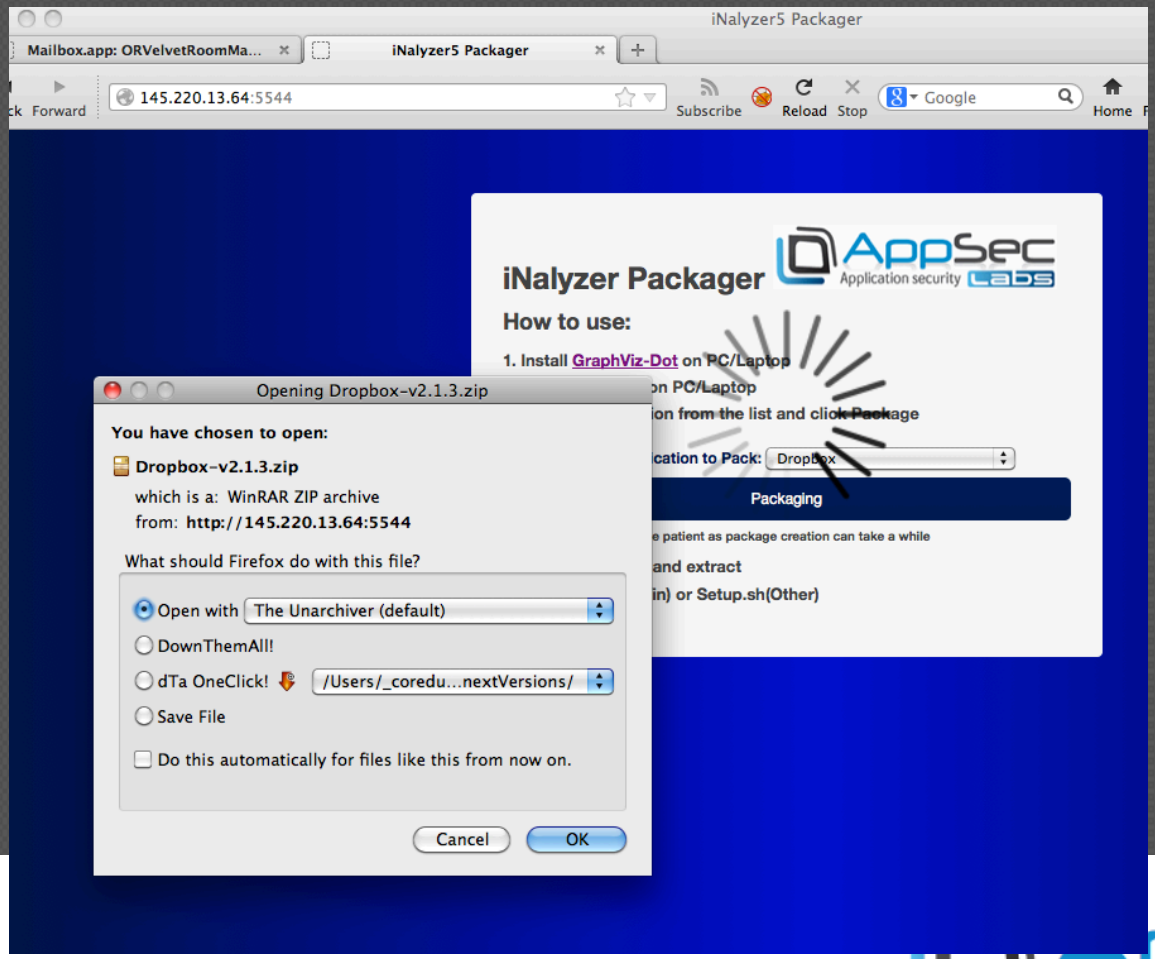
Choose application to Pack: Dropbox

Package

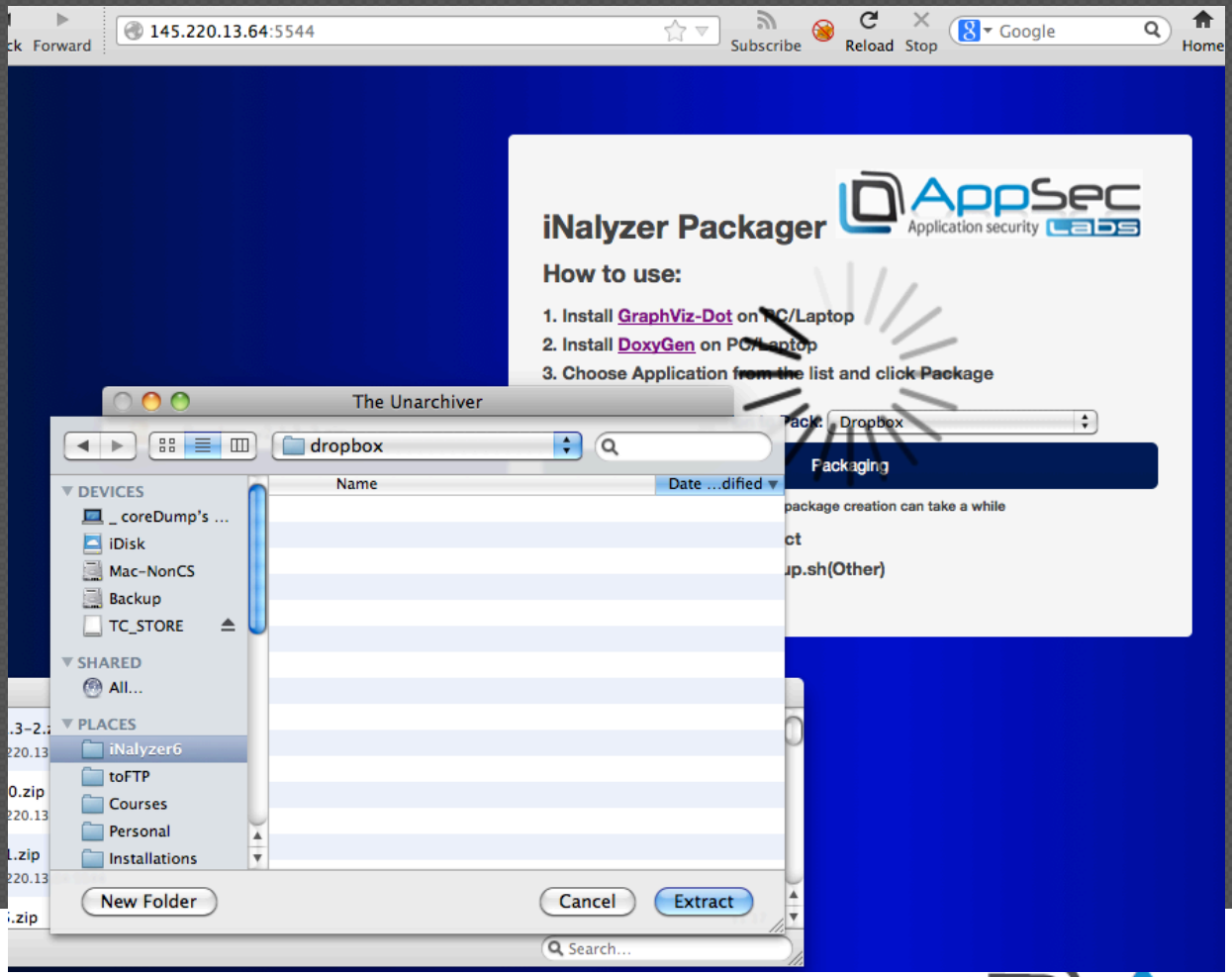
Be patient as package creation can take a while

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

# Packaging an App (Dropbox)

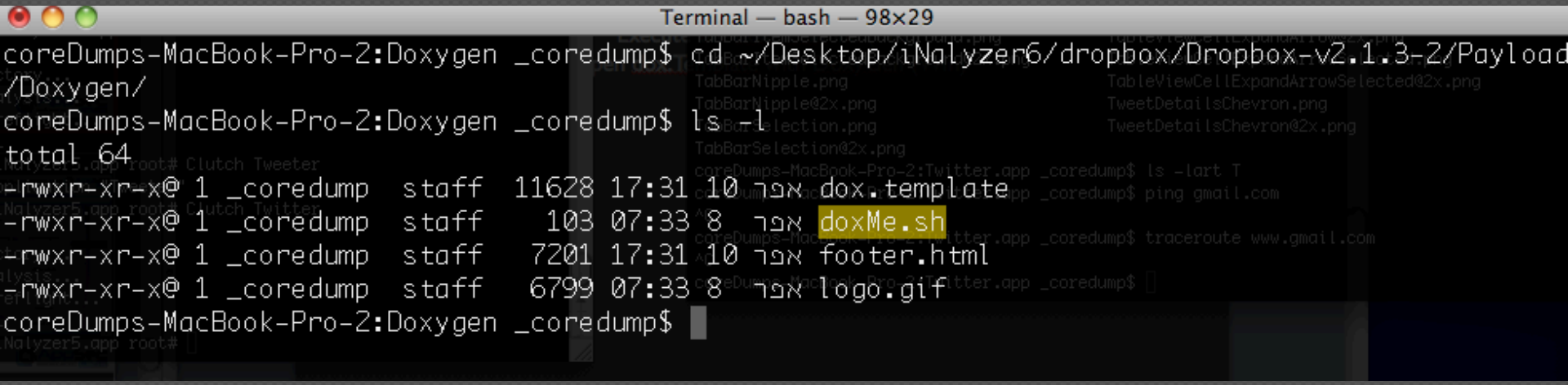


# Extraction (Dropbox)

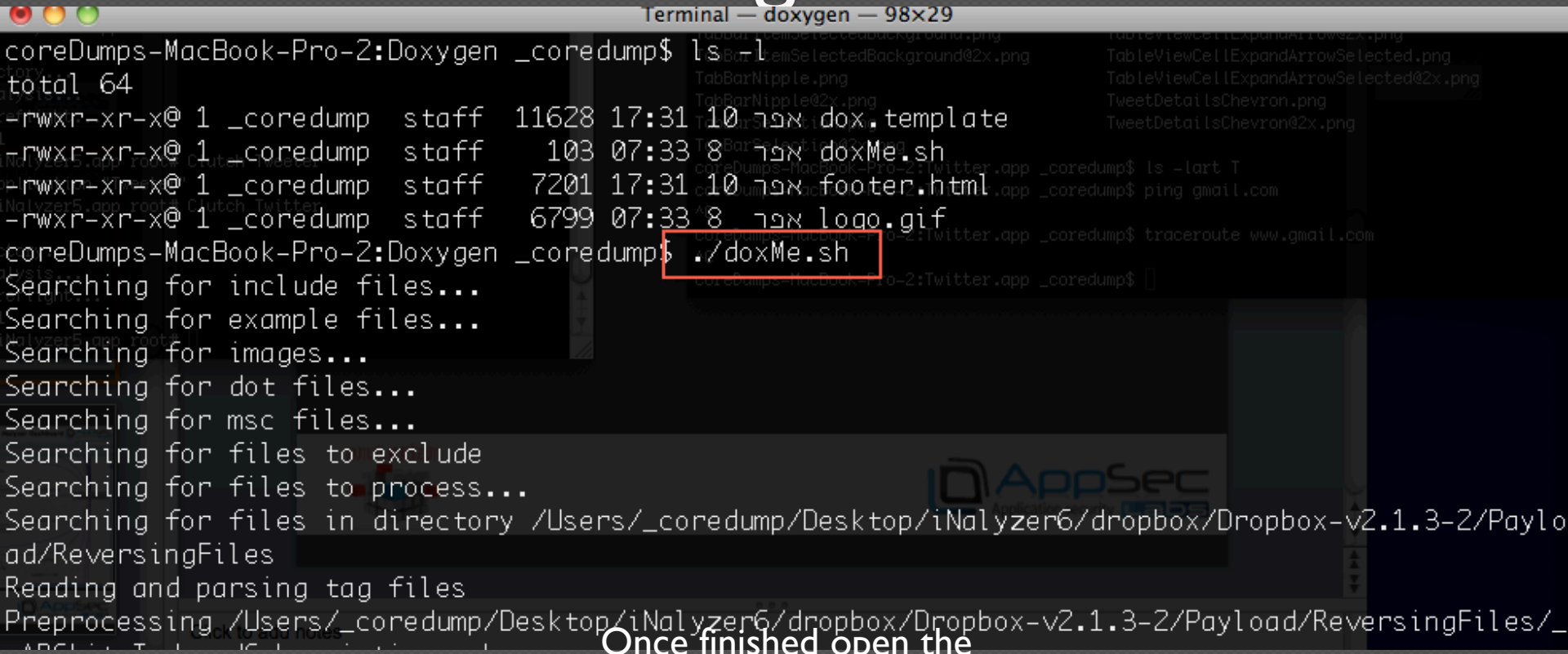


# Dashboard Building

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

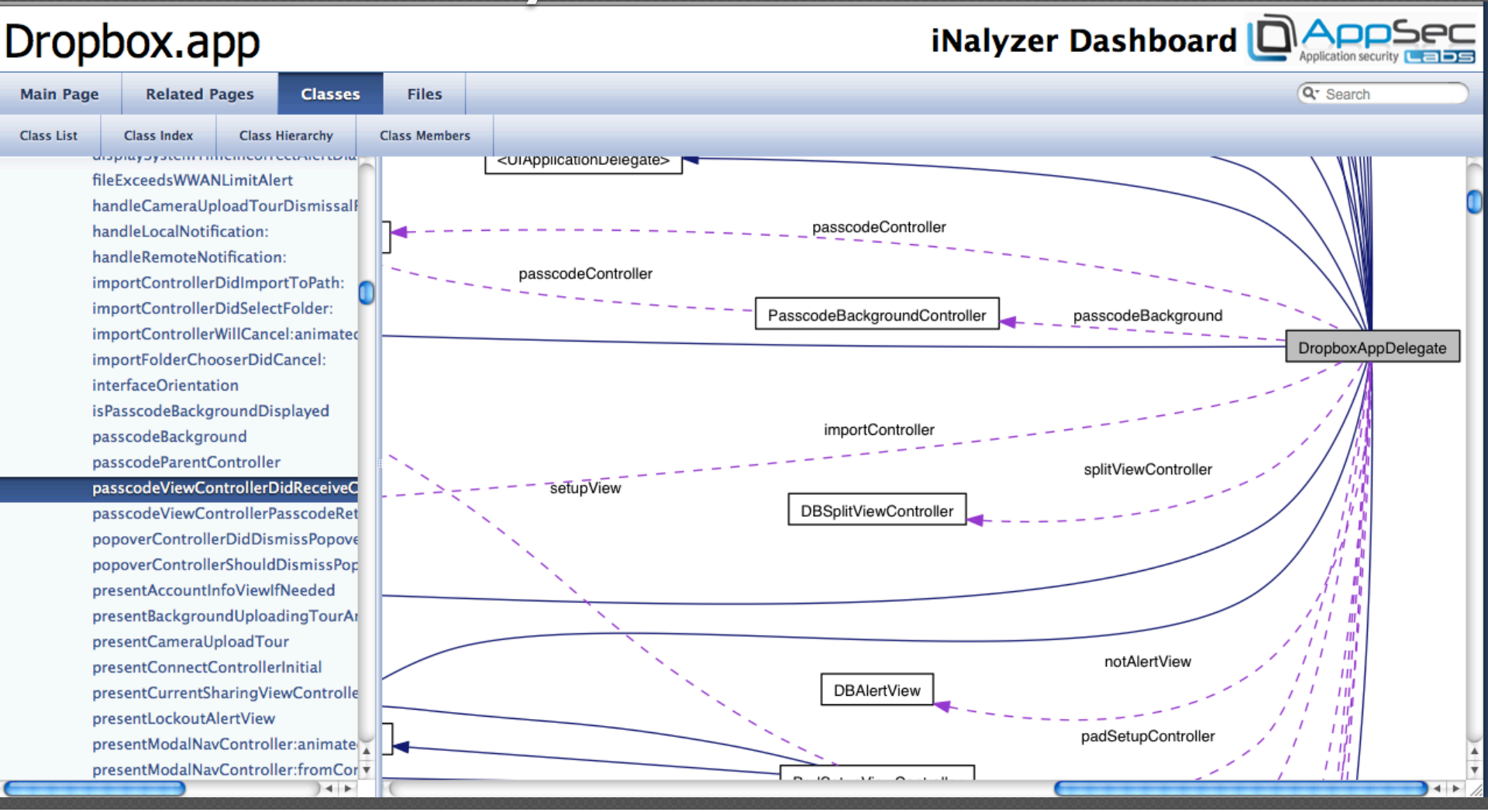


# Dashboard Building: it could take time




Once finished open the
Payload/Appname.app/Doxygen/html/index.html
file with FireFox

# iNalyzer Dashboard



# Dropbox.app

## iNalyzer Dashboard

Main Page | Related Pages | Classes | Files

Class List | Class Index | Class Hierarchy | Class Members

- fileExceedsWWANLimitAlert
- handleCameraUploadTourDismissalForcedByUser:animat
- handleLocalNotification:
- handleRemoteNotification:
- importControllerDidImportToPath:
- importControllerDidSelectFolder:
- importControllerWillCancel:animated:
- importFolderChooserDidCancel:
- interfaceOrientation
- isPasscodeBackgroundDisplayed
- passcodeBackground
- passcodeParentController
- passcodeViewControllerDidReceiveCorrectPasscode:
- passcodeViewControllerPasscodeRetriesDidFail:
- popoverControllerDidDismissPopover:
- popoverControllerShouldDismissPopover:
- presentAccountInfoViewIfNeeded
- presentBackgroundUploadingTourAnimated:
- presentCameraUploadTour
- presentConnectControllerInitial
- presentCurrentSharingViewController
- presentLockoutAlertView
- presentModalNavController:animated:
- presentModalNavController:fromController:

- (void) – sharedFolderInviteAccepted:metadata:
- (void) – importFolderChooserDidCancel:
- (void) – importControllerDidSelectFolder:
- (void) – importControllerDidImportToPath:
- (void) – importControllerWillCancel:animated:
- (void) – dismissImportViewAnimated:
- (id) – passcodeBackground
- (void) – dealloc
- (void) – sessionDidReceiveAuthorizationFailure:userId:
- (void) – alertWithNotificationUserInfo:
- (void) – fileExceedsWWANLimitAlert
- (void) – syncOutOfSpaceAlert
- (void) – popoverControllerDidDismissPopover:
- (BOOL) – popoverControllerShouldDismissPopover:
- (void) – alertView:didDismissWithButtonIndex:
- (void) – passcodeViewControllerPasscodeRetriesDidFail:
- (void) – passcodeViewControllerDidReceiveCorrectPassco
- (void) – tourControllerDidDismissTour:
- (void) – cuBackgroundUploadingTourViewControllerDidD
- (void) – cuTourMainViewControllerDidDismissTour:
- (void) – dismissCUTourController
- (void) – handleCameraUploadTourDismissalForcedByUse
- (void) – applicationWillEnterForeground:
- (void) – applicationDidEnterBackground:
- (void) – application:didFailToRegisterForRemoteNotificati
- (void) – application:didRegisterForRemoteNotificationsWi
- (void) – registerForRemoteNotifications
- (void) – applicationDidBecomeActive:

coredumps-iphone.local – VNC Viewer

-100 ORANGE 48 0:28 95%

Enter Passcode

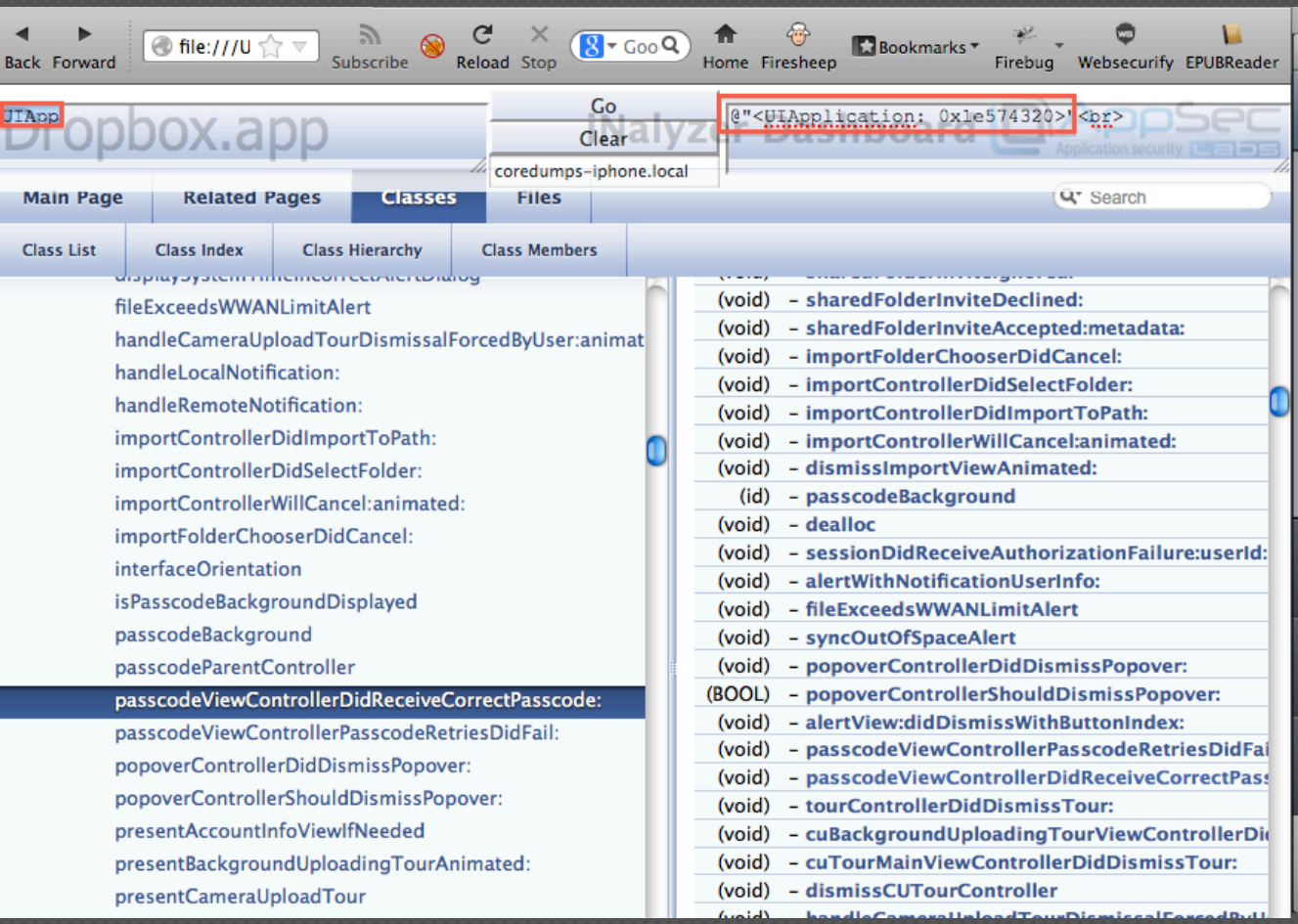
Enter your Dropbox passcode

1 | 2 ABC | 3 DEF
4 GHI | 5 JKL | 6 MNO
7 PQRS | 8 TUV | 9 WXYZ
0

AppSec Application security Labs

HITB SECCONF AMS

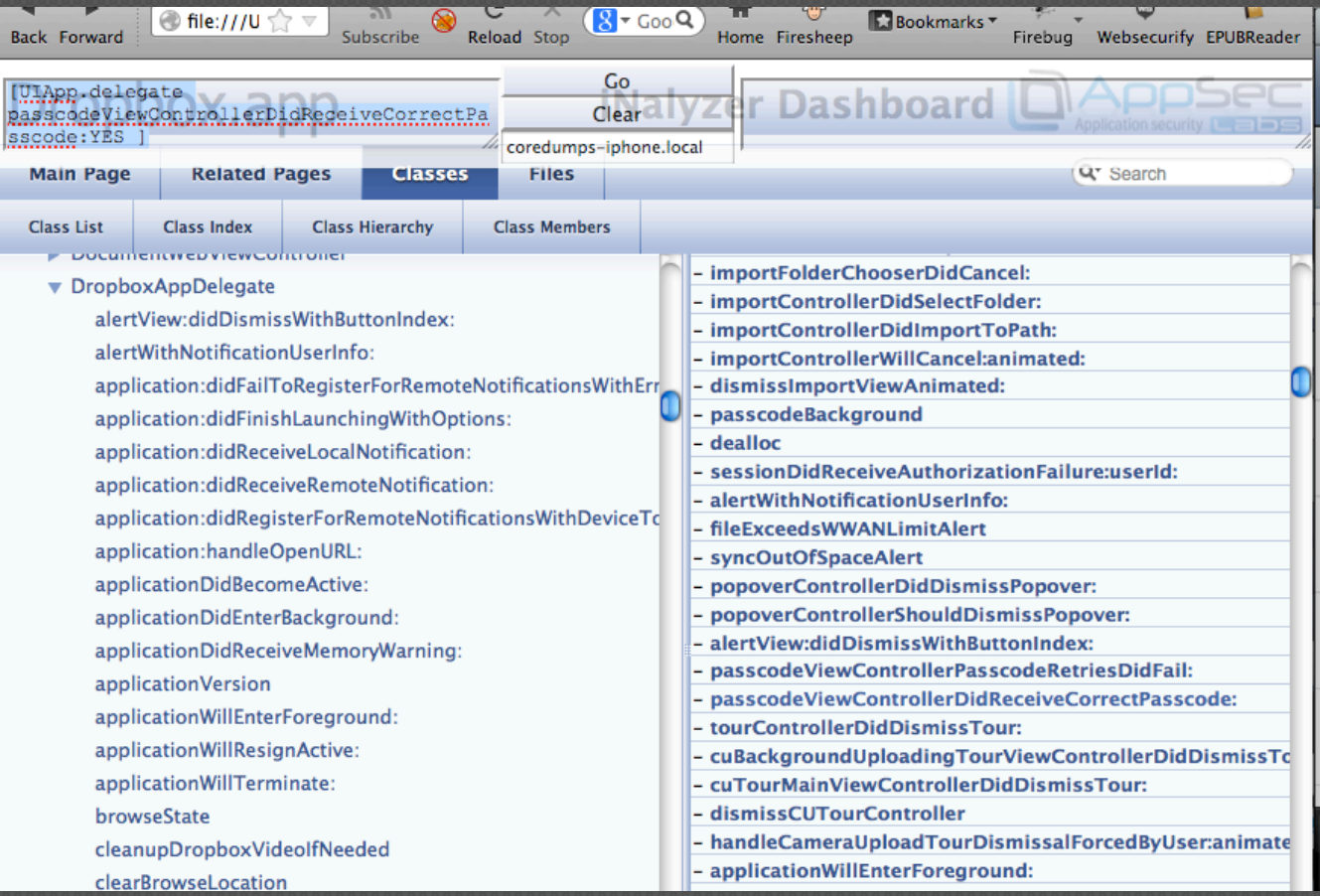
AppSec Application security Labs

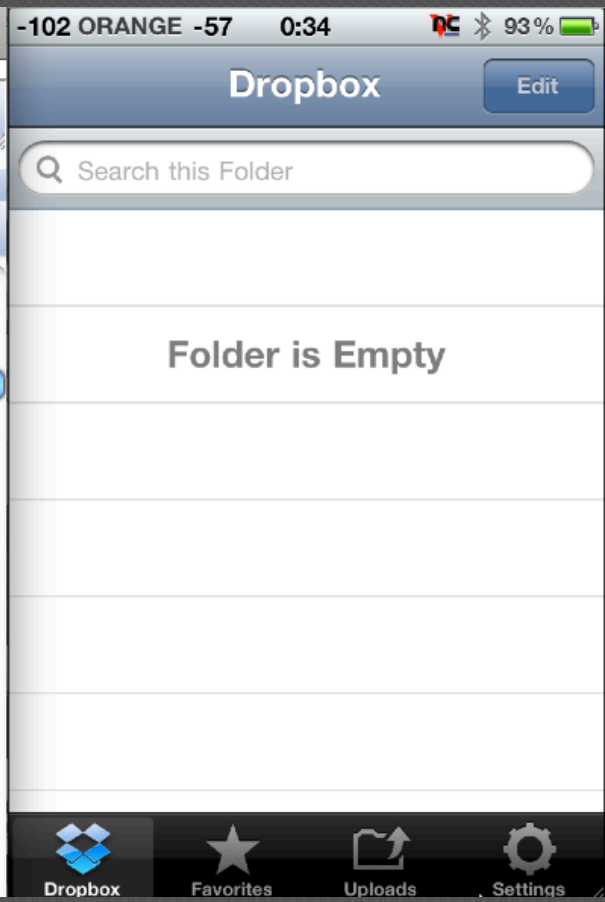

Back
Forward
file:///U
Subscribe
Reload
Stop
Goo
Home
Firesheep
Bookmarks
Firebug
Websecurify
EPUBReader
UIApp
Dropbox.app
Go
Clear
coredumps-iphone.local
@"<UIApplication: 0x1e574320>"<br>
Main Page
Related Pages
Classes
Files
Search
Class List
Class Index
Class Hierarchy
Class Members
fileExceedsWWANLimitAlert
handleCameraUploadTourDismissalForcedByUser:animat
handleLocalNotification:
handleRemoteNotification:
importControllerDidImportToPath:
importControllerDidSelectFolder:
importControllerWillCancel:animated:
importFolderChooserDidCancel:
interfaceOrientation
isPasscodeBackgroundDisplayed
passcodeBackground
passcodeParentController
passcodeViewControllerDidReceiveCorrectPasscode:
passcodeViewControllerPasscodeRetriesDidFail:
popoverControllerDidDismissPopover:
popoverControllerShouldDismissPopover:
presentAccountInfoViewIfNeeded
presentBackgroundUploadingTourAnimated:
presentCameraUploadTour
(void) - sharedFolderInviteDeclined:
(void) - sharedFolderInviteAccepted:metadata:
(void) - importFolderChooserDidCancel:
(void) - importControllerDidSelectFolder:
(void) - importControllerDidImportToPath:
(void) - importControllerWillCancel:animated:
(void) - dismissImportViewAnimated:
(id) - passcodeBackground
(void) - dealloc
(void) - sessionDidReceiveAuthorizationFailure:userId:
(void) - alertWithNotificationUserInfo:
(void) - fileExceedsWWANLimitAlert
(void) - syncOutOfSpaceAlert
(void) - popoverControllerDidDismissPopover:
(BOOL) - popoverControllerShouldDismissPopover:
(void) - alertView:didDismissWithButtonIndex:
(void) - tourControllerDidDismissTour:
(void) - dismissCUTourController


coredumps-iphone.local - VNC Viewer
-99 ORANGE -48
0:31
94%
Enter Passcode
Enter your Dropbox passcode
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0


amsterdam


AppSec
Application security
Labs

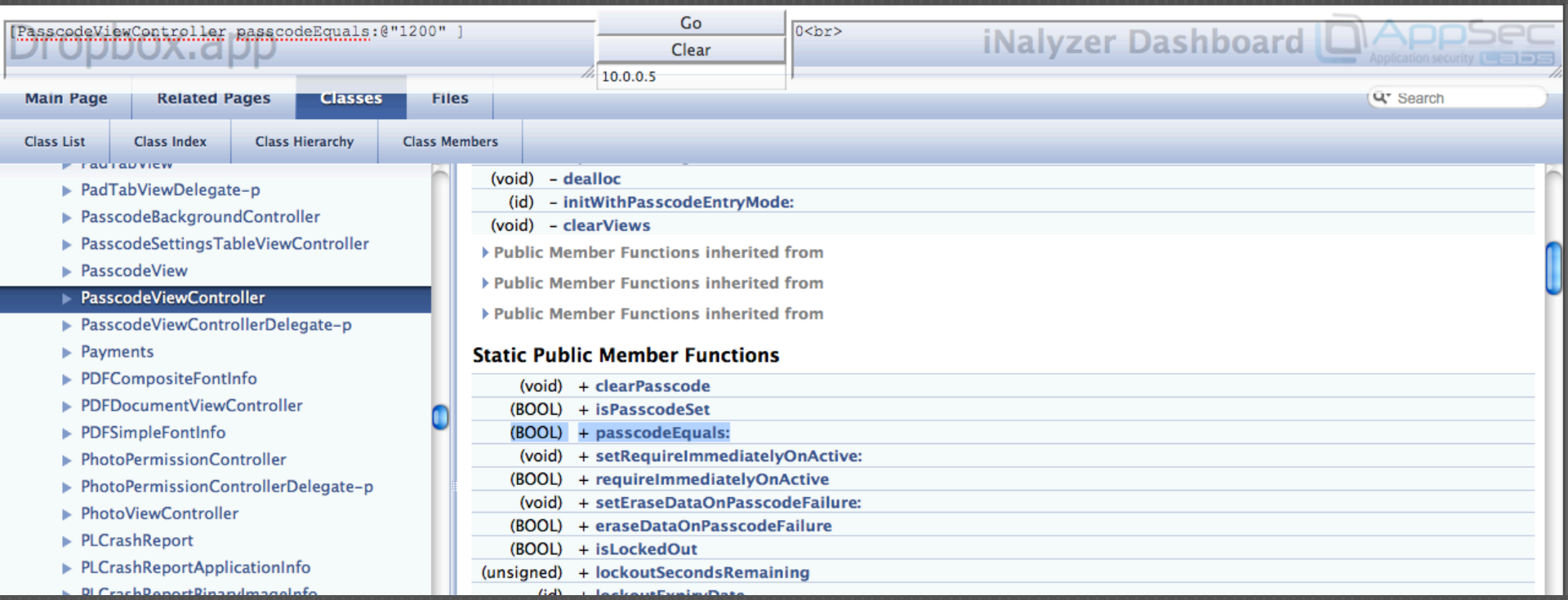


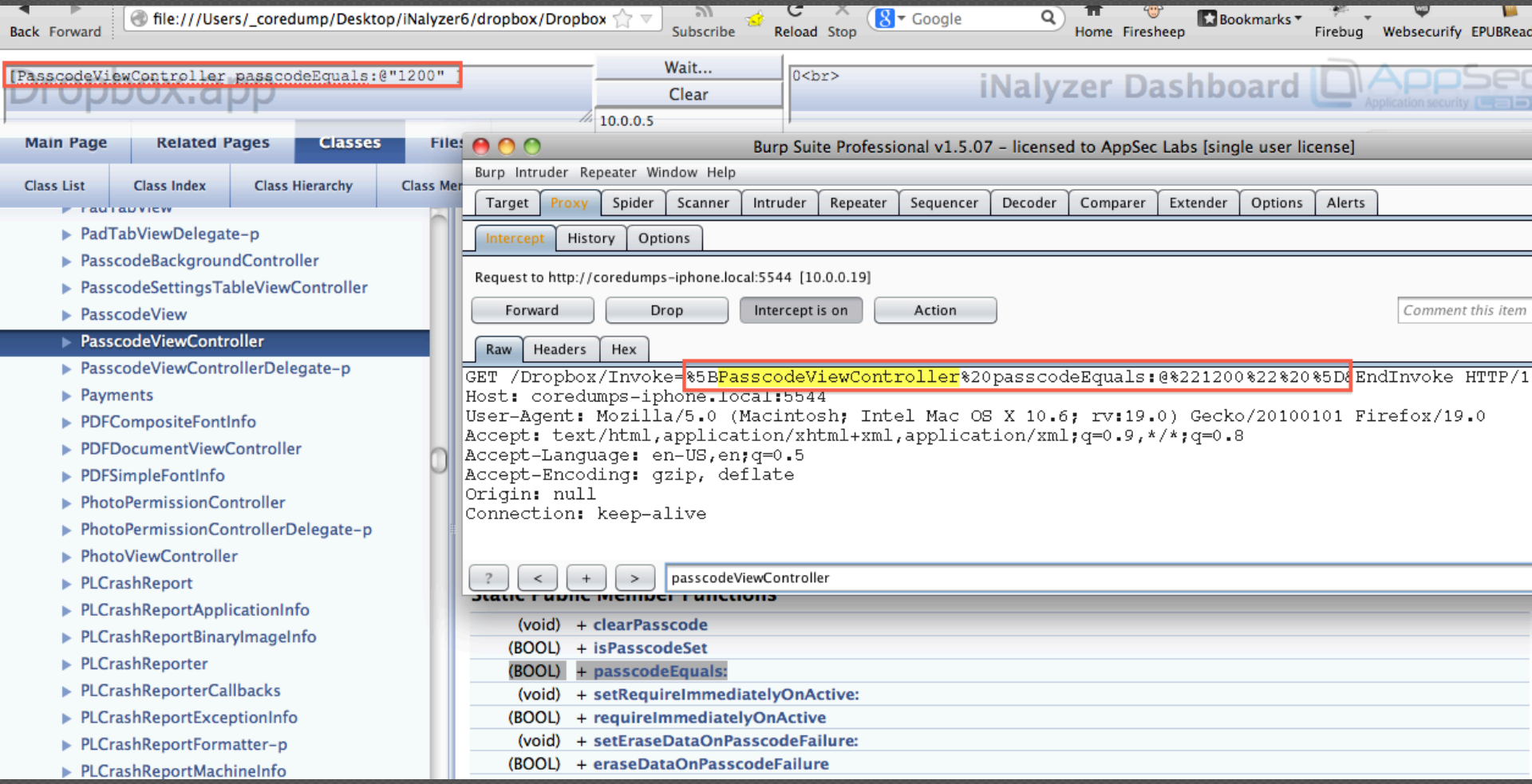



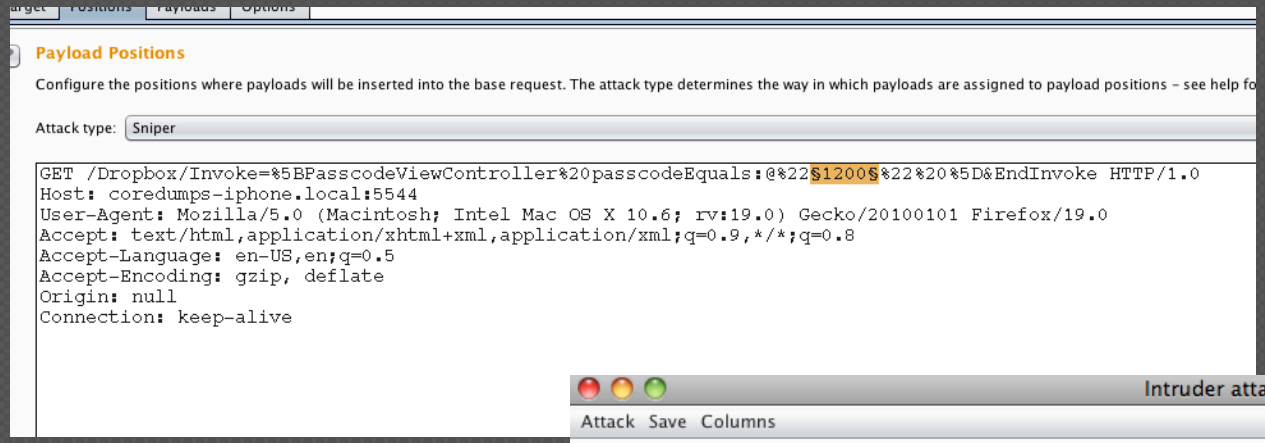


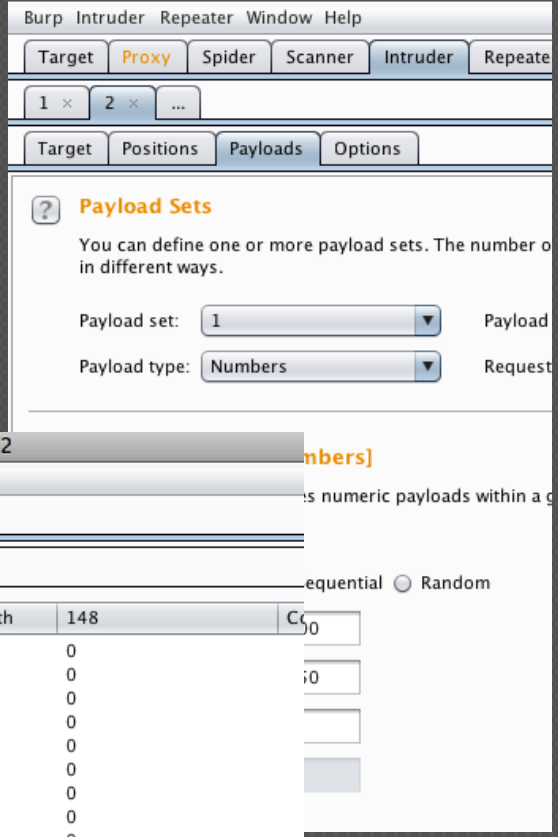
AppSec Application security Labs

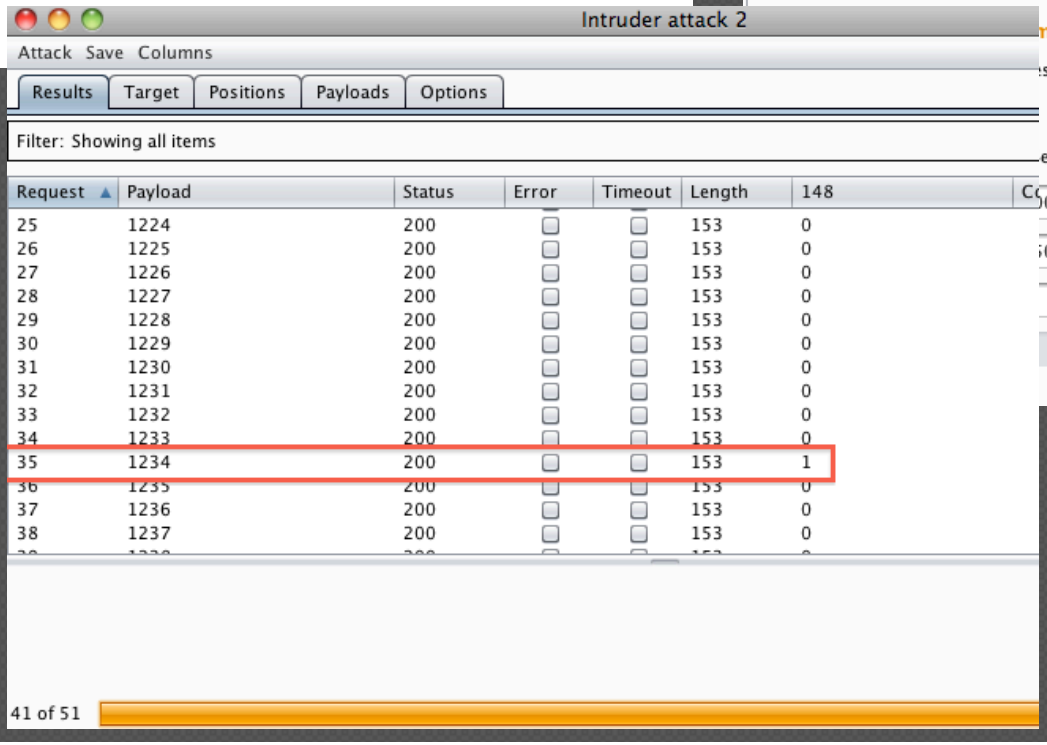
# iNalyzer and Burp Demo

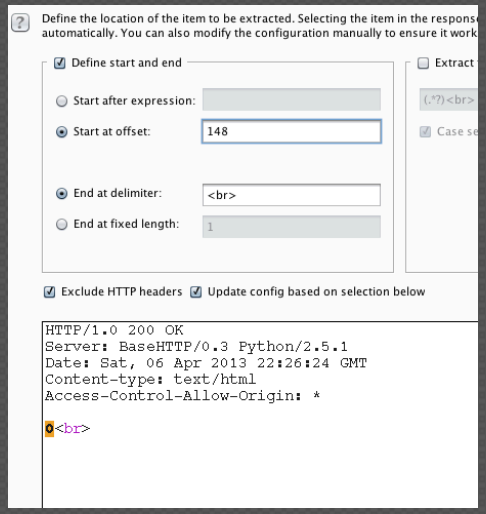



file:///Users/_coredump/Desktop/iNalyzer6/dropbox/Dropbox
[PasscodeViewController passcodeEquals:@"1200"
Wait...
Clear
10.0.0.5
0<br>
iNalyzer Dashboard
Main Page
Related Pages
Classes
Class List
Class Index
Class Hierarchy
PadTabViewDelegate-p
PasscodeBackgroundController
PasscodeSettingsTableViewController
PasscodeView
PasscodeViewController
PasscodeViewControllerDelegate-p
Payments
PDFCompositeFontInfo
PDFDocumentViewController
PDFSimpleFontInfo
PhotoPermissionController
PhotoPermissionControllerDelegate-p
PhotoViewController
PLCrashReport
PLCrashReportApplicationInfo
PLCrashReportBinaryImageInfo
PLCrashReporter
PLCrashReporterCallbacks
PLCrashReportExceptionInfo
PLCrashReportFormatter-p
PLCrashReportMachineInfo
Burp Suite Professional v1.5.07 - licensed to AppSec Labs [single user license]
Burp Intruder Repeater Window Help
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
Comment this item
Raw Headers Hex
GET /Dropbox/Invoke=%5BPasscodeViewController%20passcodeEquals:@%221200%22%20%5D&EndInvoke HTTP/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
(void) + clearPasscode
(BOOL) + isPasscodeSet
(BOOL) + passcodeEquals:
(void) + setRequireImmediatelyOnActive:
(BOOL) + requireImmediatelyOnActive
(void) + setEraseDataOnPasscodeFailure:
(BOOL) + eraseDataOnPasscodeFailure


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: <br>
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<br>


amsterdam


AppSec
Application security
Labs

Dropbox.app: Info.Plist Content | Mailbox.app: GTMOAuth2ViewC... | GmailHybrid.app: Strings analysis

Back Forward | file:///Users/_coredump/Desktop/iNalyzer6/dropbox/Dropbox | Subscribe | Reload | Stop | Google | Home | Firesheep | Bookmarks | Firebug | Websecurify | EPUBRead

# Dropbox.app

## iNalyzer Dashboard

AppSec Application security Labs

Main Page | Related Pages | Classes | Files | Search

- Dropbox.app
  - Strings analysis
  - ViewControllers
  - Info.Plist Content
  - Embeded Strings
  - Classes
  - Files

```
CFBundleIdentifier = com.getdropbox.Dropbox
CFBundleInfoDictionaryVersion = "6.0"
CFBundleName = Dropbox
CFBundlePackageType = APPL
CFBundleResourceSpecification = "ResourceRules.plist"
CFBundleShortVersionString = "2.1.3"
CFBundleSignature = "????"
CFBundleSupportedPlatforms =     (
    iPhoneOS
)
CFBundleURLTypes =     (
        {
        CFBundleURLSchemes =         (
            "dbapi-1",
            fb210019893730
        );
    }
)
CFBundleVersion = "2.1.3"
DBInternalBuild = 0
DTCompiler = ""
DTPlatformBuild = 10B141
DTPlatformName = iphoneos
DTPlatformVersion = "6.1"
DTSDKBuild = 10B141
DTSDKName = "iphoneos6.1"
DTXcode = 0460
DTXcodeBuild = 4H127
FacebookAppID = 210019893730
LSRequiresIPhoneOS = 1
MinimumOSVersion = "5.0"
NSMainNibFile = MainWindow
"NSMainNibFile~ipad" = "MainWindow-iPad"
UIBackgroundModes =     (
    audio
)
UIDeviceFamily =     (
    1,
    2
)
UIPrerenderedIcon = 1
UIStatusBarStyle = UIStatusBarStyleBlackOpaque
UIStatusBarTintParameters =     {
```

# Dropbox.app

## iNalyzer Dashboard

AppSec Application security Labs

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 = %@

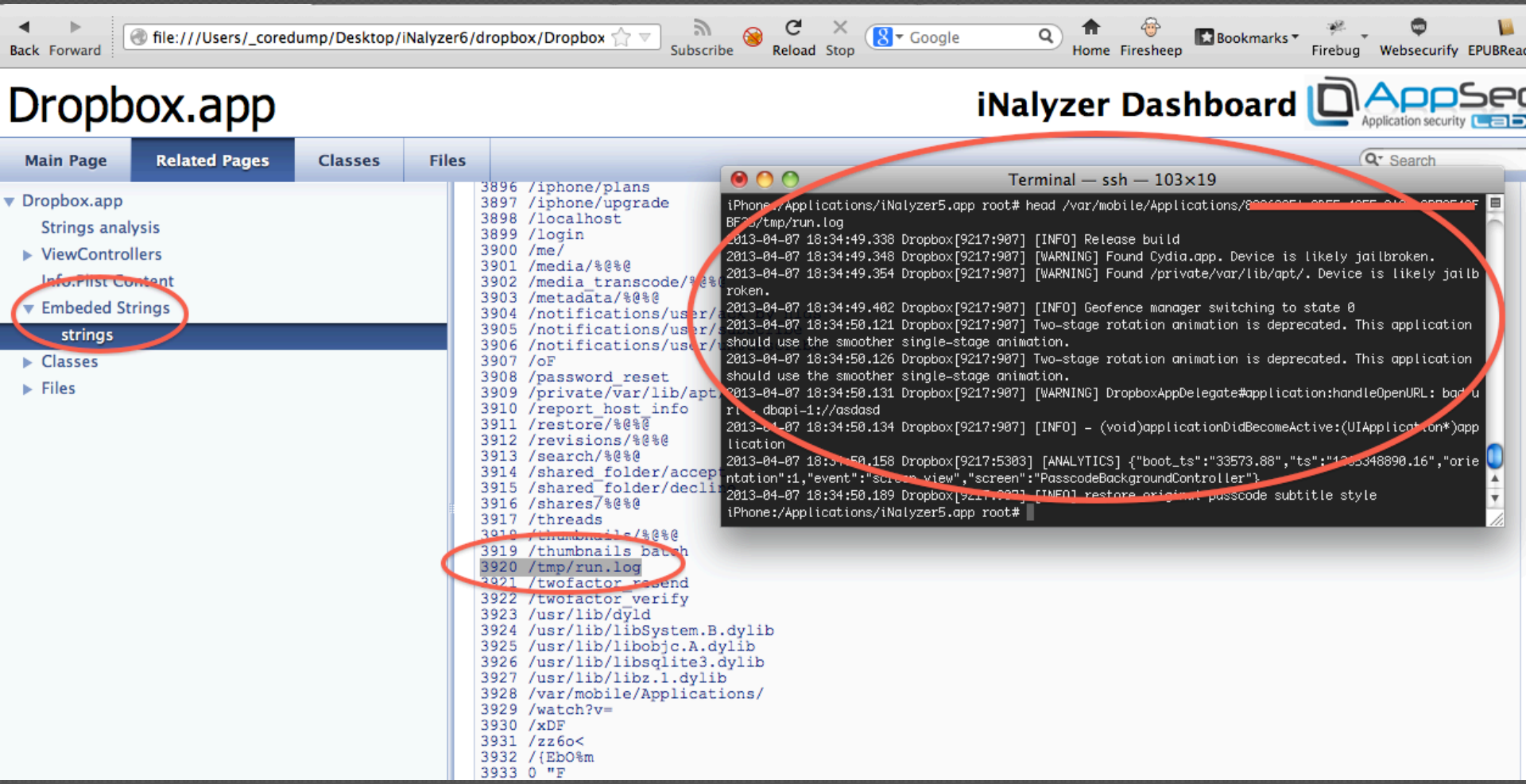
10 13647 SELECT key FROM data_cache WHERE key = '%@'

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 = ?


file:///Users/_coredump/Desktop/iNalyzer6/dropbox/Dropbox
Dropbox.app
iNalyzer Dashboard
Main Page
Related Pages
Classes
Files
Search
Dropbox.app
Strings analysis
ViewControllers
Info.Plist Content
Embeded Strings
strings
Classes
Files
3896 /iphone/plans
3897 /iphone/upgrade
3898 /localhost
3899 /login
3900 /me/
3901 /media/%@%@
3902 /media_transcode/%@%@
3903 /metadata/%@%@
3904 /notifications/user/a
3905 /notifications/user/s
3906 /notifications/user/t
3907 /oF
3908 /password_reset
3909 /private/var/lib/apt/
3910 /report_host_info
3911 /restore/%@%@
3912 /revisions/%@%@
3913 /search/%@%@
3914 /shared_folder/accept
3915 /shared_folder/decli
3916 /shares/%@%@
3917 /threads
3918 /thumbnails/%@%@
3919 /thumbnails_batch
3920 /tmp/run.log
3921 /twofactor_resend
3922 /twofactor_verify
3923 /usr/lib/dyld
3924 /usr/lib/libSystem.B.dylib
3925 /usr/lib/libobjc.A.dylib
3926 /usr/lib/libsqlite3.dylib
3927 /usr/lib/libz.1.dylib
3928 /var/mobile/Applications/
3929 /watch?v=
3930 /xDF
3931 /zz6o<
3932 /{EbO%m
3933 0 "F
Terminal — ssh — 103×19
iPhone:/Applications/iNalyzer5.app root# head /var/mobile/Applications/
BF2/tmp/run.log
2013-04-07 18:34:49.338 Dropbox[9217:907] [INFO] Release build
2013-04-07 18:34:49.348 Dropbox[9217:907] [WARNING] Found Cydia.app. Device is likely jailbroken.
2013-04-07 18:34:49.354 Dropbox[9217:907] [WARNING] Found /private/var/lib/apt/. Device is likely jailbroken.
2013-04-07 18:34:49.402 Dropbox[9217:907] [INFO] Geofence manager switching to state 0
2013-04-07 18:34:50.121 Dropbox[9217:907] Two-stage rotation animation is deprecated. This application should use the smoother single-stage animation.
2013-04-07 18:34:50.126 Dropbox[9217:907] Two-stage rotation animation is deprecated. This application should use the smoother single-stage animation.
2013-04-07 18:34:50.131 Dropbox[9217:907] [WARNING] DropboxAppDelegate#application:handleOpenURL: bad url dbapi-1://asdasd
2013-04-07 18:34:50.134 Dropbox[9217:907] [INFO] - (void)applicationDidBecomeActive:(UIApplication*)application
2013-04-07 18:34:50.158 Dropbox[9217:5303] [ANALYTICS] {"boot_ts":"33573.88","ts":"1365348890.16","orientation":1,"event":"screen_view","screen":"PasscodeBackgroundController"}
2013-04-07 18:34:50.189 Dropbox[9217:907] [INFO] restore original passcode subtitle style
iPhone:/Applications/iNalyzer5.app root#

# iNalyzer Setup – iPhone as the Pen Testing Tool

# iNalyzer 5.5b: The Recipe

1. Jail-borken 6.1.2 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

Optional:

8. SubjectiveC to log selectors (@**kennytm**)

# Pros:

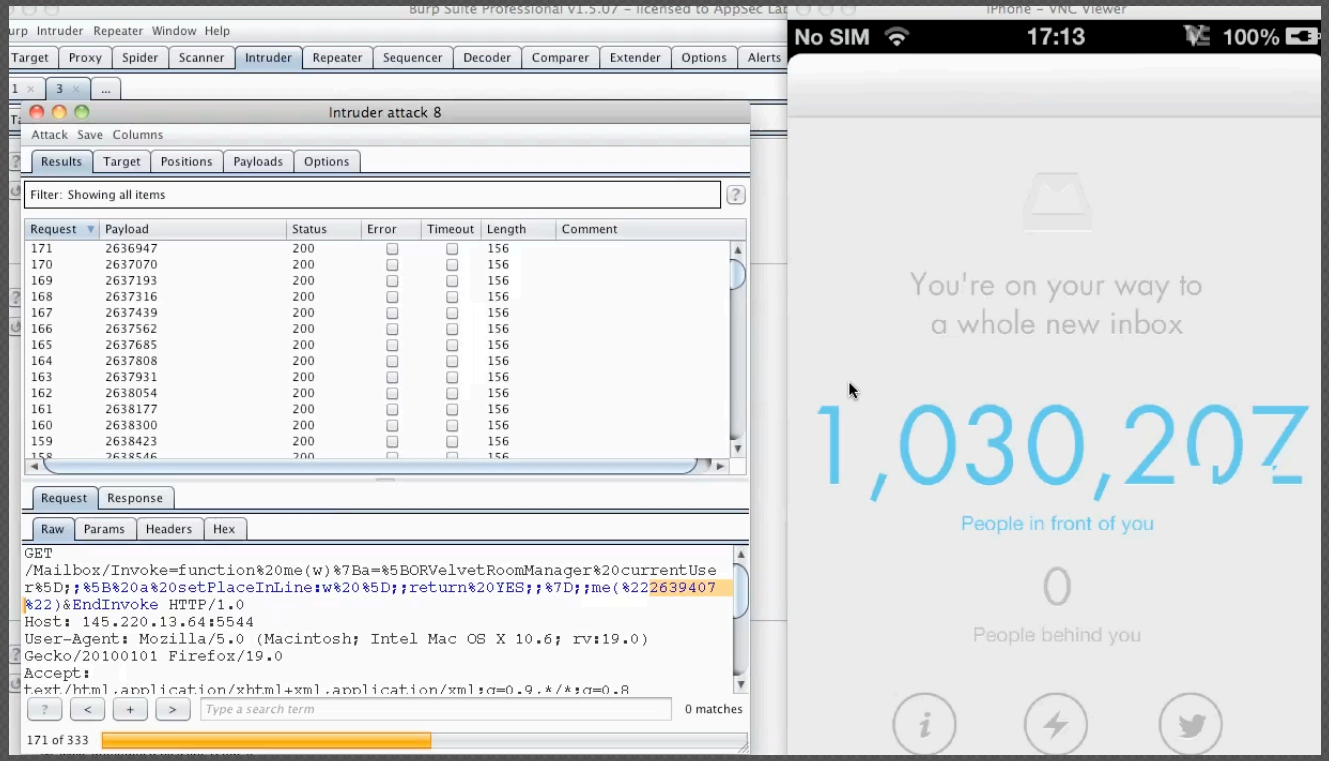
- No GDB/IDA required
- Semi - Automatic Static Analysis (Expandable)
- Automatic Call Graph/Hierarchy Graph
- Attaches to any scanner or other Web testing Tool.

# Cons:

- It's free, open-source


AppSec Application security Labs

# iNalyzer & Burp Vs. Mailbox



# Open Live Demo (as time permits):

Bring it On

# Summary

- iOS Black Box testing, just got grayer ☺
- Mobile PT requires Mobile understanding
- Join our mobile application security hands-on **training** 

  - Mobile Hacking (Black Hat USA 2013 – iOS / Android )
  - Mobile Secure Coding (TBD, info@appsec-labs.com)
  - Mobile Awareness (TBD, info@appsec-labs.com)


AppSec Application security Labs

# Questions ?


amsterdam
HTTP://CONFERENCE.HITB.ORG/HITBSECCONF2013AMS/


AppSec
Application security
Labs

# Thank You


amsterdam
HTTP://CONFERENCE.HITB.ORG/HITBSECCONF2013AMS/


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


# iNalyzer – No more iOS BlackBox assessments
# https://appsec-labs.com/iNalyzer


Chilik Tamir

Chief Scientist


@_coreDump


chilik <at> appsec-labs.com


www.appsec-labs.com



AppSec Application security Labs