

# OWASP IL 2012

## Advanced iPhone Hacking



Chilik Tamir - Chief Scientist

[Chilik@AppSec-Labs.com](mailto:Chilik@AppSec-Labs.com)

# Using (i)Phones as Weapons



# What is iOS?

- Mobile OS
- Exists on:  
iPhone, iPod Touch, iPad latest generation of AppleTV
- OSX based + Mod. Kernel (XNU) & System Libraries
- Single tasking environment (multitasking not exposed to users)



# What's an iOS App ?

- ▣ ObjC Compiled (ARM)
- ▣ Encrypted Executable
- ▣ All needed data in  
~/Applications/GUID/  
AppName.app folder
- ▣ Installed by “mobile”  
user





# iOS Black-Box PT Agenda

## 📱 Agenda:

📱 Quality Vulnerabilities

📱 Do it Fast

📱 Reproduce



THE PROBLEM WITH  
AVERAGING STAR RATINGS

# iOS Black-Box PT Agenda

You want Quality Findings !

Black Box – Min. App knowledge...

▣ Means:

▣ Static Analysis

▣ Dynamic Analysis

# Static Analysis Tools

## 📁 Tools:

📁 iFile / iFundBox (Cydia iOS/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)

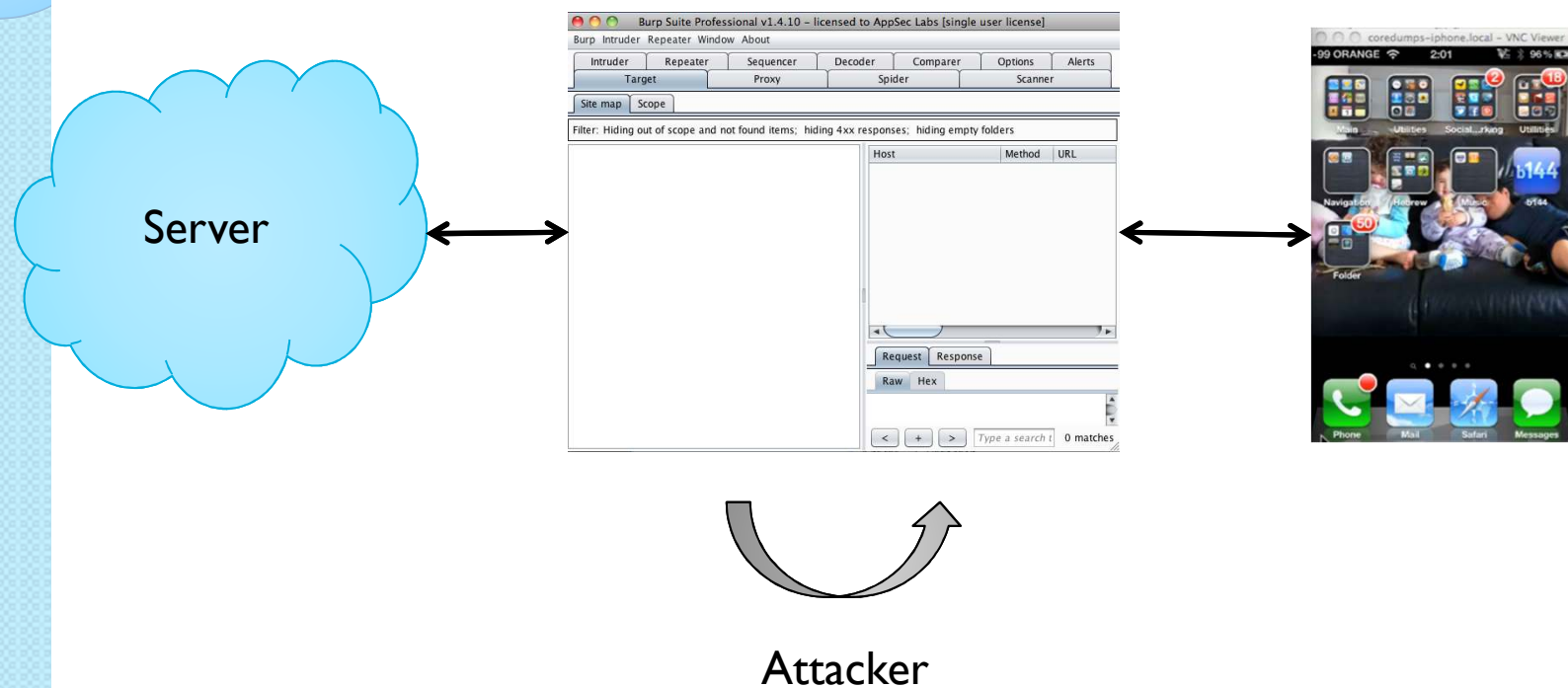
 WiFi HotSpot

 Cycrypt

 Class-Dump-Z



# Typical Setup



# Mobile PT = Agony

- ❏ Encrypted Binary.
- ❏ No Emulation (until now.)
- ❏ No Full High Level Code Reversing (Android, Flex, .NET)
- ❏ No Peer Info (% Coverage thru BlackBox)
- ❏ No Automation
- ❏ No Scanners



Manual, Manual, Manual...

## The Solution

# AppSec-Labs iNalyzer

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

# AppSec-Labs iNalyzer

Screenium Edit Capture Export Window Help

iSafePlay\_app: LoginViewController Class Reference - (Private Browsing)

iSafePlay\_app: LoginViewContro...

file:///Users/\_coredump/Desktop/Blog\_iPhone/owasp... isafePlay

Back Forward Subscribe Reload Stop Home Bookmarks Firebug

Main Page Related Pages **Classes** Files

Class List Class Index Class Hierarchy Class Members

checkPass  
checkPWOK:  
clearPass  
dealloc  
deposit:  
didReceiveMemoryWarning  
doneGlock:  
flashAgainATMLbl  
flashAgainLbl  
gotoView:  
iFlash  
imagePickerController:didFinish:  
key0tap:  
key1tap:  
key2tap:  
key3tap:  
key4tap:  
key5tap:  
key6tap:  
key7tap:  
key8tap:  
key9tap:  
keyBlanktap:  
keyboardWillShow:

iSafePod  
iSafePod  
iSafePod  
LoginViewContro  
SetPasswordViewController  
SetPWAnswerViewController  
setPasswordViewController  
setPWAnswerViewController

Go no Result Clear

AppSec Labs Application security

coredumps-iphone.local - VNC Viewer

-103 ORANGE 0:57 72%

Mail Enhancer NES Omer SC-323PU

SBSettings Calculator Viber Entertainment

iSSH Hdaf Hyomi iPassSafe iSafePlay

Productivity

Phone Mail Safari Messages

AppSec Labs

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

# AppSec-Labs iNalyzer

- 📄 Automatic Static Analysis
- 📄 Automatic Call Graph/Hierarchy Graph
- 📄 Automatic Execution UI for manual and Automatic PT
- 📄 Attaches to any scanner or other Web testing Tool.

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



# iNalyzer Setup – iPhone as the Pen Testing Tool



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

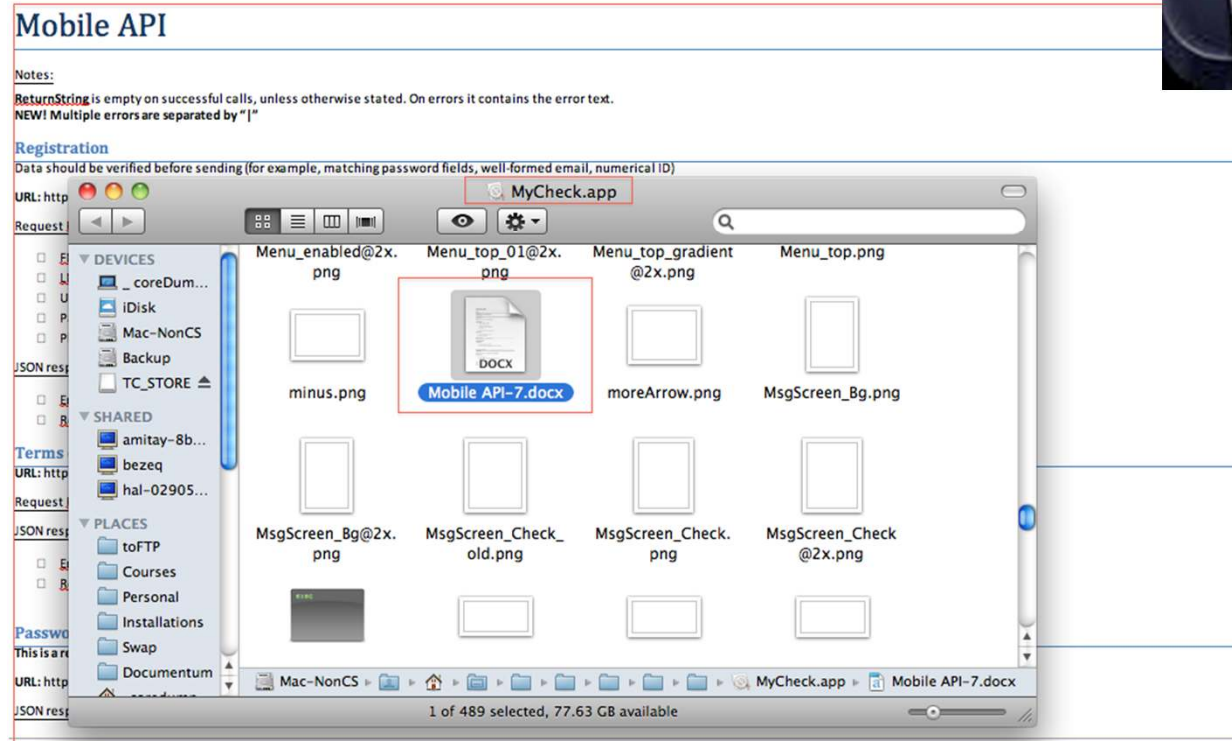
# AppSec-Labs iNalyzer - Client



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

# Static Analysis Findings

- 📁 Sensitive information in files:
- 📁 Peers

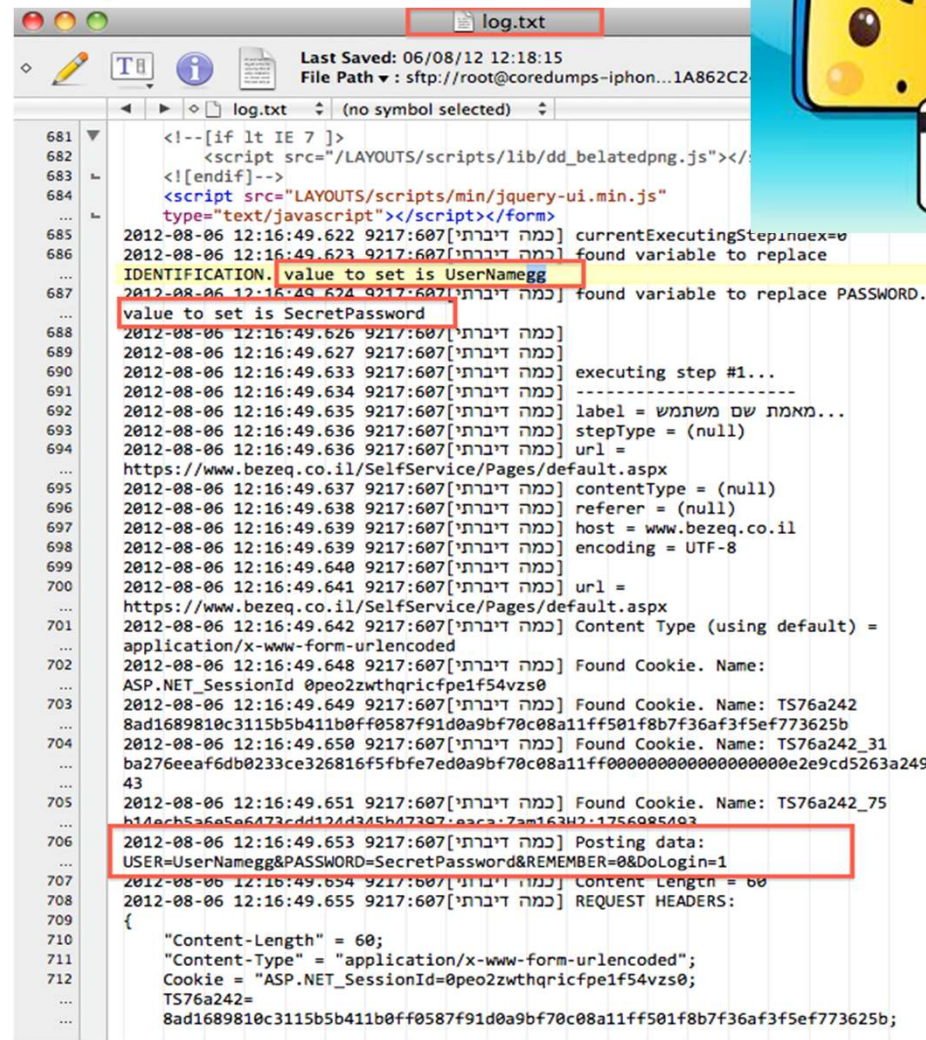


<https://appsec-labs.com/iNalyzer>



# Static Analysis Findings

## Credentials



```
681 <!--[if lt IE 7 ]>
682 <script src="/LAYOUTS/scripts/lib/dd_belatedpng.js"></script>
683 <![endif]-->
684 <script src="/LAYOUTS/scripts/min/jquery-ui.min.js"
685 type="text/javascript"></script></form>
686 2012-08-06 12:16:49.622 9217:607 [כמה דיברתי] currentExecutingStepIndex=0
687 2012-08-06 12:16:49.623 9217:607 [כמה דיברתי] found variable to replace
688 IDENTIFICATION. value to set is UserNameegg
689 2012-08-06 12:16:49.624 9217:607 [כמה דיברתי] found variable to replace PASSWORD.
690 value to set is SecretPassword
691 2012-08-06 12:16:49.626 9217:607 [כמה דיברתי]
692 2012-08-06 12:16:49.627 9217:607 [כמה דיברתי]
693 2012-08-06 12:16:49.633 9217:607 [כמה דיברתי] executing step #1...
694 2012-08-06 12:16:49.634 9217:607 [כמה דיברתי]
695 2012-08-06 12:16:49.635 9217:607 [כמה דיברתי] label = שם משתמש...
696 2012-08-06 12:16:49.636 9217:607 [כמה דיברתי] stepType = (null)
697 2012-08-06 12:16:49.636 9217:607 [כמה דיברתי] url =
698 https://www.bezeq.co.il/SelfService/Pages/default.aspx
699 2012-08-06 12:16:49.637 9217:607 [כמה דיברתי] contentType = (null)
700 2012-08-06 12:16:49.638 9217:607 [כמה דיברתי] referer = (null)
701 2012-08-06 12:16:49.639 9217:607 [כמה דיברתי] host = www.bezeq.co.il
702 2012-08-06 12:16:49.640 9217:607 [כמה דיברתי] encoding = UTF-8
703 2012-08-06 12:16:49.641 9217:607 [כמה דיברתי] url =
704 https://www.bezeq.co.il/SelfService/Pages/default.aspx
705 2012-08-06 12:16:49.642 9217:607 [כמה דיברתי] Content Type (using default) =
706 application/x-www-form-urlencoded
707 2012-08-06 12:16:49.648 9217:607 [כמה דיברתי] Found Cookie. Name:
708 ASP.NET_SessionId 0peo2zwtgqricpe1f54vzs0
709 2012-08-06 12:16:49.649 9217:607 [כמה דיברתי] Found Cookie. Name: TS76a242
710 8ad1689810c3115b5b411b0ff0587f91d0a9bf70c08a11ff501f8b7f36af3f5ef773625b
711 2012-08-06 12:16:49.650 9217:607 [כמה דיברתי] Found Cookie. Name: TS76a242_31
712 ba276eeaf6db0233ce326816f5fbfe7ed0a9bf70c08a11ff0000000000000e2e9cd5263a249
713 43
714 2012-08-06 12:16:49.651 9217:607 [כמה דיברתי] Found Cookie. Name: TS76a242_75
715 h14ech5a6e5e6473cd4124d345b47307-0a3a-7am163H2-1756085403
716 2012-08-06 12:16:49.653 9217:607 [כמה דיברתי] Posting data:
717 USER=UserNameegg&PASSWORD=SecretPassword&REMEMBER=0&DoLogin=1
718 2012-08-06 12:16:49.654 9217:607 [כמה דיברתי] Content Length = 60
719 2012-08-06 12:16:49.655 9217:607 [כמה דיברתי] REQUEST HEADERS:
720 {
721 "Content-Length" = 60;
722 "Content-Type" = "application/x-www-form-urlencoded";
723 Cookie = "ASP.NET_SessionId=0peo2zwtgqricpe1f54vzs0;
724 TS76a242=
725 8ad1689810c3115b5b411b0ff0587f91d0a9bf70c08a11ff501f8b7f36af3f5ef773625b;
```



# Static Analysis Findings

 Credentials

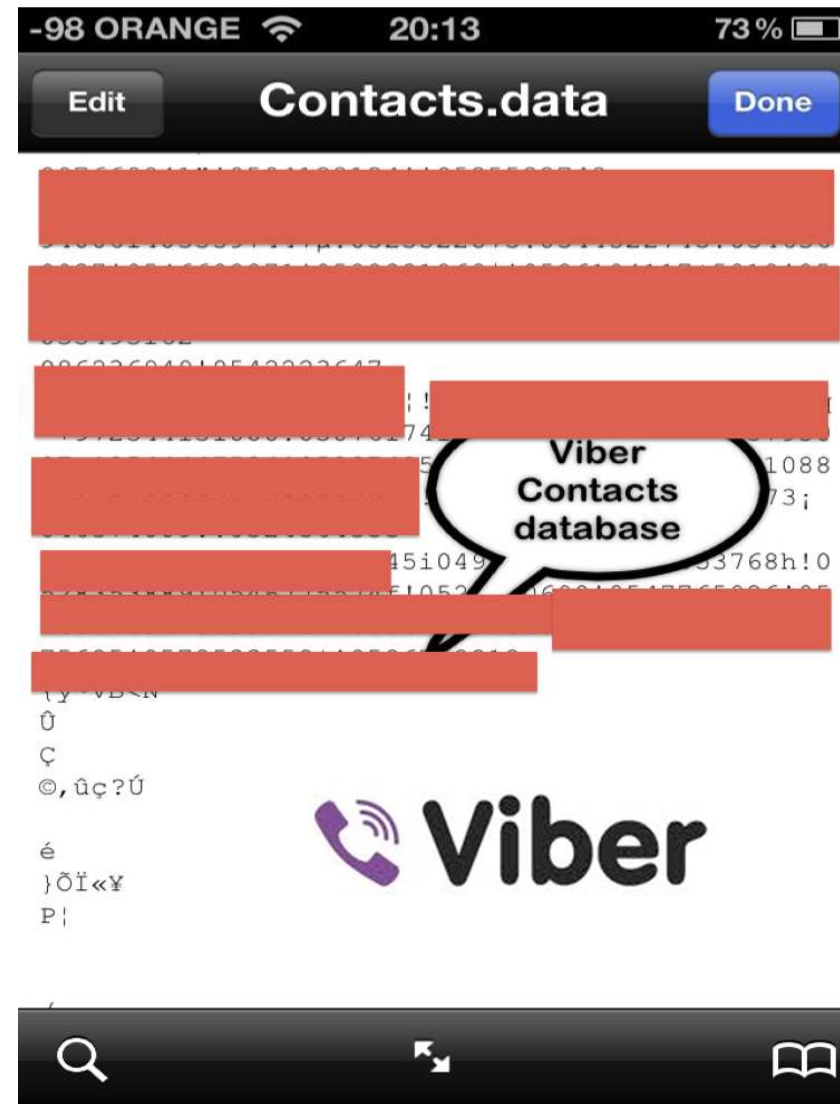


<https://appsec-labs.com/iNalyzer>



# Static Analysis Findings

📁 Private Information:



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

# iNalyzer & Burp intruder

The screenshot displays the iNalyzer application interface within a Firefox browser window. The browser's address bar shows a file path: `file:///Users/_coredump/Desktop/Blog_iPhone`. The application is titled "SpringBoard\_app: Strings analysis - (Private Browsing)".

The interface is divided into several sections:

- Main Page:** Contains a sidebar with a tree view showing the project structure: `SpringBoard_app` (expanded), `Strings analysis` (selected), `Info.plist Content`, `Embedded Strings`, `Classes`, and `Files`.
- SQL Strings:** A list of SQL-related strings with their memory addresses and values:
  - 1 23894 `insertIcon:intoListView:iconIndex:moveNow:`
  - 2 27201 `textField:willChangeSelectionFromCharacterRange:toCharacterRange:`
- URI strings:** A list of URI-related strings with their memory addresses and values:
  - 1 21510 `doubletap://com.apple.camera`
  - 2 21511 `doubletap://com.apple.mobilephone?view=FAVORITES`
  - 3 21512 `doubletap://com.apple.mobileslideshow-Camera`
  - 4 21513 `doubletap://com.apple.springboard-Search`
  - 5 23332 `http://itunes.apple.com/us/app/ibooks/id364709193?mt=8`
  - 6 24756 `music://playImmediately`
  - 7 25208 `photos-event://?uicmd=show-import`
  - 8 25495 `radr://5614542`
  - 9 27184 `teleemergency://`
  - 10 27185 `tellock://`
  - 11 27187 `telshow://`
  - 12 27894 `x-web-search:///??@`
  - 13 27895 `x-web-search://wikipedia/??@`
- Code Editor:** At the bottom, a code editor shows a snippet of Objective-C code:

```
[UIApp.delegate applicationOpenURL:[NSURL alloc]  
initWithString:@"x-web-search:///??hello" ]]
```
- Search Bar:** A search bar at the bottom right of the code editor area, currently showing "0 matches".

On the right side of the browser window, there is a VNC Viewer window titled "coredumps-iphone.local - VNC Viewer". It displays a simulated iPhone home screen with various app icons (Main, Utilities, Social..., b144, Navigation, Hebrew, Music, b144, Folder, Phone, Mail, Safari, Messages) and a status bar at the top showing "99 ORANGE", signal strength, time "2:01", and battery level "96%".

The AppSec Labs logo is visible in the bottom right corner of the browser window.

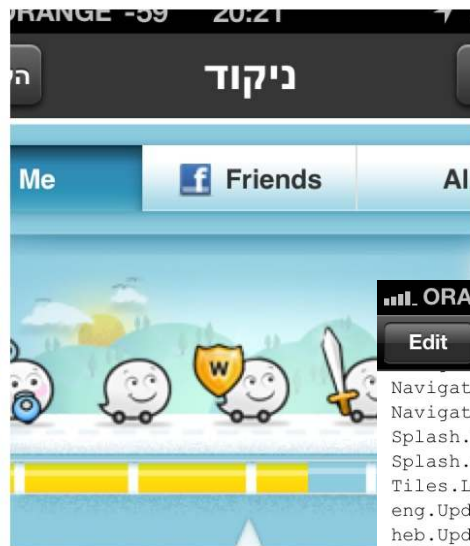
<https://appsec-labs.com/iNalyzer>

# Tampering With Files



**points:**  
ze Warrior, 31093 pts.  
rently 5890 pts. to next level

**My Rank: 13087**  
Heres how you can move up ranks



**points:**  
ze Warrior, 31965 pts.  
rently 5018 pts. to next level

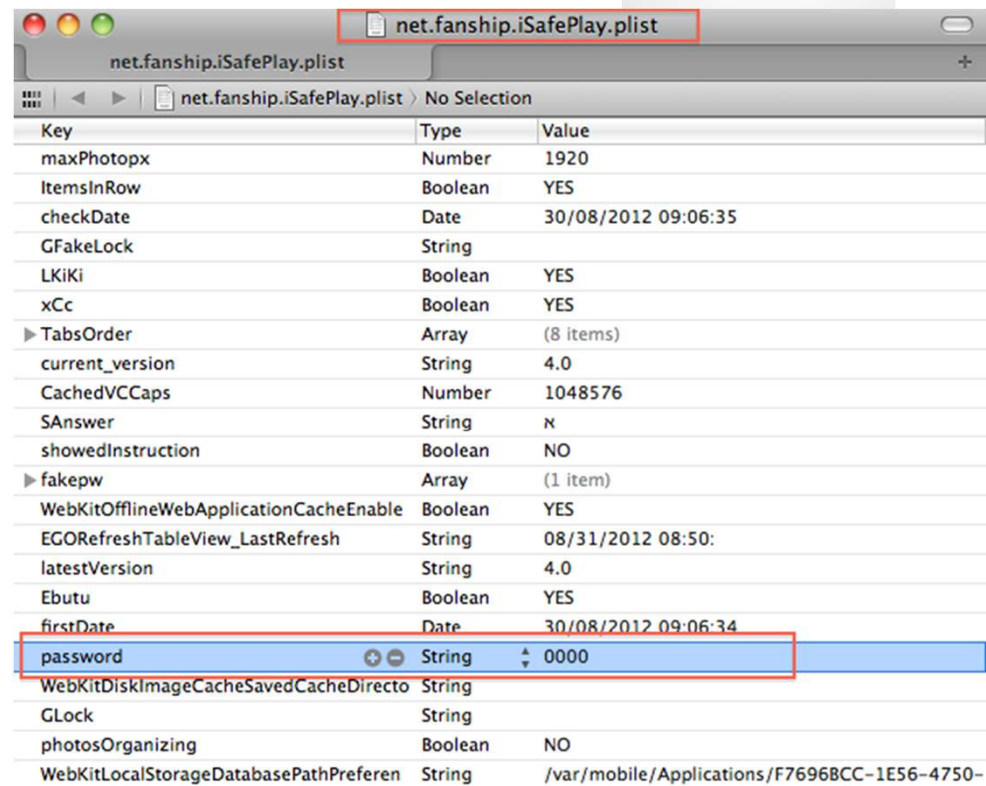
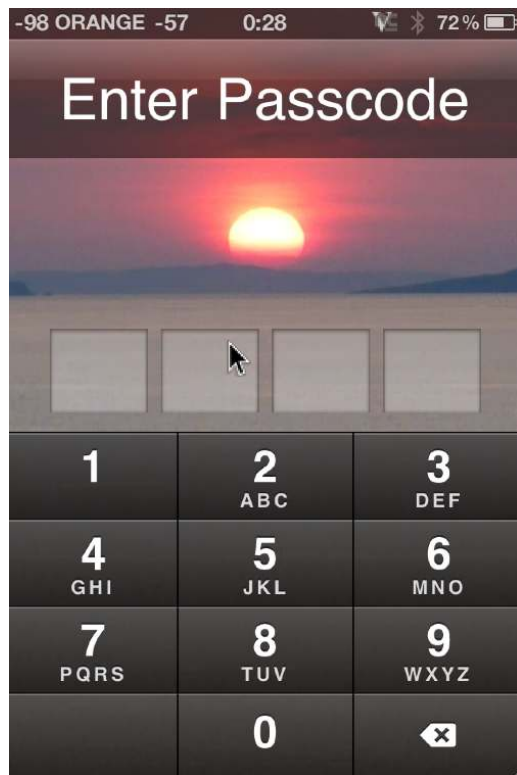
**My Rank: 12839**  
Heres how you can move up ranks



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



# Tampering w/ Client Side Data

A screenshot of the iSafePlay.plist file in a plist editor. The file is titled "net.fanship.iSafePlay.plist". The table below shows the contents of the plist file.

Key	Type	Value
maxPhotopx	Number	1920
ItemsInRow	Boolean	YES
checkDate	Date	30/08/2012 09:06:35
GFakeLock	String	
LKiKi	Boolean	YES
xCc	Boolean	YES
► TabsOrder	Array	(8 items)
current_version	String	4.0
CachedVCCaps	Number	1048576
SAnswer	String	x
showedInstruction	Boolean	NO
► fakepw	Array	(1 item)
WebKitOfflineWebApplicationCacheEnable	Boolean	YES
EGORRefreshTableView_LastRefresh	String	08/31/2012 08:50:
latestVersion	String	4.0
Ebutu	Boolean	YES
firstDate	Date	30/08/2012 09:06:34
password	String	0000
WebKitDiskImageCacheSavedCacheDirecto	String	
GLock	String	
photosOrganizing	Boolean	NO
WebKitLocalStorageDatabasePathPreferen	String	/var/mobile/Applications/F76968BCC-1E56-4750-

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

# Manual Reversing Interfaces:

## Class-dump-z

Usage: class-dump-z [<options>] <filename>

where options are:

### Analysis:

- p Convert undeclared getters and setters into properties (propertize).
- h proto Hide methods which already appears in an adopted protocol.
- h super Hide inherited methods.
- y <root> Choose the sysroot. Default to the path of latest iPhoneOS SDK, or /.
- u <arch> Choose a specific architecture in a fat binary (e.g. armv6, armv7, etc.)

### Formatting:

- a Print ivar offsets
- A Print implementation VM addresses.
- k Show additional comments.
- k -k Show even more comments.
- R Show pointer declarations as int \*a instead of int\* a.
- N Keep the raw struct names (e.g. do no replace \_\_CFArray\* with CFArrayRef).
- b Put a space after the +/- sign (i.e. + (void)... instead of +(void)...).
- i <file> Read and update signature hints file.

### Filtering:

- C <regex> Only display types with (original) name matching the RegExp (in PCRE syntax).
- f <regex> Only display methods with (original) name matching the RegExp.
- g Display exported classes only.
- X <list> Ignore all types (except categories) with a prefix in the comma-separated list.
- h cats Hide categories.
- h dogs Hide protocols.

### Sorting:

- S Sort types in alphabetical order.
- s Sort methods in alphabetical order.
- z Sort methods alphabetically but put class methods and -init... first.

### Output:

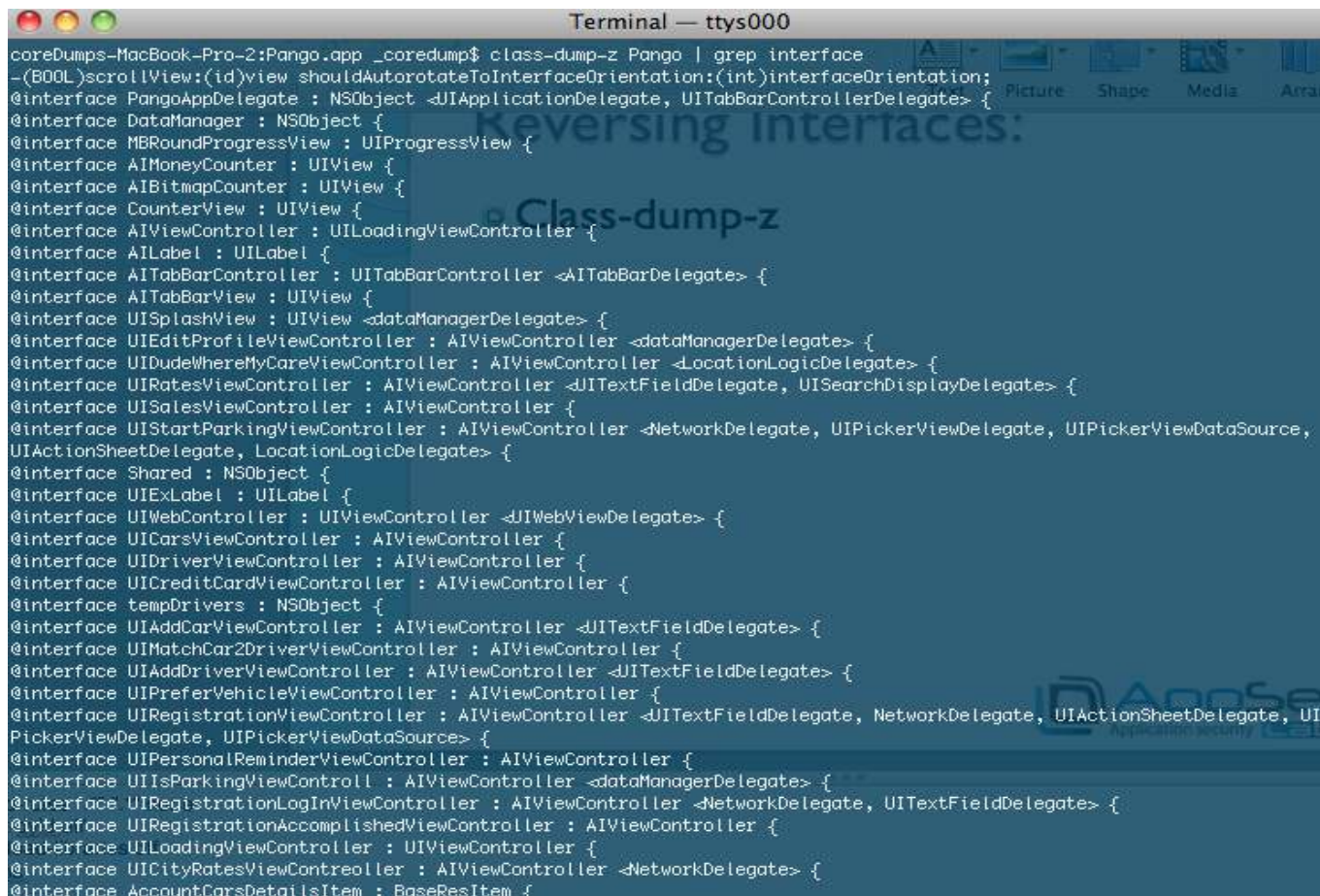
- H Separate into header files
- o <dir> Put header files into this directory instead of current directory.

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



# Reversing Interfaces:

## Class-dump-z



```
Terminal — ttys000
coreDumps-MacBook-Pro-2:Pango.app _coredump$ class-dump-z Pango | grep interface
-(BOOL)scrollView:(id)view shouldAutorotateToInterfaceOrientation:(int)interfaceOrientation;
@interface PangoAppDelegate : NSObject <UIApplicationDelegate, UITabBarControllerDelegate> {
@interface DataManager : NSObject {
@interface MBSoundProgressView : UIProgressView {
@interface AIBitmapCounter : UIView {
@interface CounterView : UIView {
@interface AIViewController : UILoadingViewController {
@interface AILabel : UILabel {
@interface AITabBarController : UITabBarController <AITabBarDelegate> {
@interface AITabBarView : UIView {
@interface UISplashView : UIView <DataManagerDelegate> {
@interface UIEditProfileViewController : AIViewController <DataManagerDelegate> {
@interface UIDudeWhereMyCarViewController : AIViewController <LocationLogicDelegate> {
@interface UIRatesViewController : AIViewController <UITextFieldDelegate, UISearchBarDelegate> {
@interface UISalesViewController : AIViewController {
@interface UIStartParkingViewController : AIViewController <NetworkDelegate, UIPickerViewDelegate, UIPickerViewDataSource,
UIActionSheetDelegate, LocationLogicDelegate> {
@interface Shared : NSObject {
@interface UIExLabel : UILabel {
@interface UIWebController : UIViewController <JIWebViewDelegate> {
@interface UICarsViewController : AIViewController {
@interface UIDriverViewController : AIViewController {
@interface UICreditCardViewController : AIViewController {
@interface tempDrivers : NSObject {
@interface UIAddCarViewController : AIViewController <UITextFieldDelegate> {
@interface UIMatchCar2DriverViewController : AIViewController {
@interface UIAddDriverViewController : AIViewController <UITextFieldDelegate> {
@interface UIPreferVehicleViewController : AIViewController {
@interface UIRegistrationViewController : AIViewController <UITextFieldDelegate, NetworkDelegate, UIActionSheetDelegate, UI
PickerViewDelegate, UIPickerViewDataSource> {
@interface UIPersonalReminderViewController : AIViewController {
@interface UIIsParkingViewController : AIViewController <DataManagerDelegate> {
@interface UIRegistrationLoginViewController : AIViewController <NetworkDelegate, UITextFieldDelegate> {
@interface UIRegistrationAccomplishedViewController : AIViewController {
@interface UILoadingViewController : UIViewController {
@interface UICityRatesViewControlller : AIViewController <NetworkDelegate> {
@interface AccountCarsDetailsItem : BaseResItem {
```

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

# AppSec-Labs iNalyzer

The screenshot displays the AppSec-Labs iNalyzer application interface. The main window shows a class reference for `LoginViewController` from the `iSafePlay_app`. The left sidebar lists various methods, with `checkPWOK:` selected. The main area shows a diagram of the class hierarchy and relationships, including `iSafePod`, `SetPasswordViewController`, and `SetPWAnswerViewController`. A VNC viewer window in the top right corner shows an iPhone screen with various app icons, including Mail, NES, Omer, SC-323PU, SBS Settings, Calculator, Viber, Entertainment, iSSH, Hdaf Hyomi, iPassSafe, and iSafePlay. The AppSec-Labs logo is visible in the bottom right corner of the application window.

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

# iNalyzer:

- 📱 Turns your iPhone into a PenTesting Tool
- 📱 No More Black Box → Gray Box
- 📱 Bypasses any Signing or Client Request Validation Process

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

# Summary

- 📱 Mobile security is in rise
- 📱 Mobile PT requires Mobile understanding
- 📱 We provide mobile application security hands-on **training**
  - 📱 Mobile Hacking
  - 📱 Mobile Secure Coding

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



Questions ?



Thank You