So Long, and Thanks for All the Fish

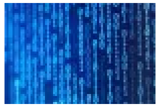
JUST SOME RANDOM THOUGHTS ABOUT THE MEANING OF LIFE, THE UNIVERSE, AND EVERYTHING

☰ MENU

Reverse engineering and penetration testing on iOS apps: my own list of tools

Written by Andrea Fortuna • on August 8, 2019 • in Cybersecurity, Penetration Testing

RECENT POSTS

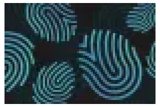


Win32/StealthFalcon malware uses Windows Background Intelligent Transfer Service (BITS) to communicates to its C&C servers

September 13, 2019

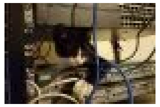
Simjacker: a brand new mobile vulnerability exploited by surveillance companies for espionage operation

September 12, 2019



Some thoughts about Browser Fingerprinting

September 12, 2019



NetCat attack (CVE-2019-11184): steal encrypted SSH keystrokes exploiting DDIO

September 11, 2019

After a post **focused on Android**, another list of tools useful for penetration testing and reverse engineering of iOS applications.
Also all this tools are OSS and freely available.

Access Device

iProxy

Let's you connect your laptop to the iPhone to surf the web.

> *iProxy does not give you tethering – it just gives you the next best thing. A http and a socks proxy on your iPhone. Similar to the famous netshare app did before it got pulled from the App Store.*

CATEGORIES

Select Category ▾

RECENT COMMENTS

Cybersecurity: DNS Tunneling – Elite Homework on DNS tunneling techniques in cyberattacks

simjacker, anda bisa dimata-matai hanya dengan modal kartu sim - High3 Blog on Simjacker: a brand new mobile vulnerability exploited by surveillance companies for espionage operation

Andrea Fortuna on How to make a "Ultra-Geek" Linux Workstation

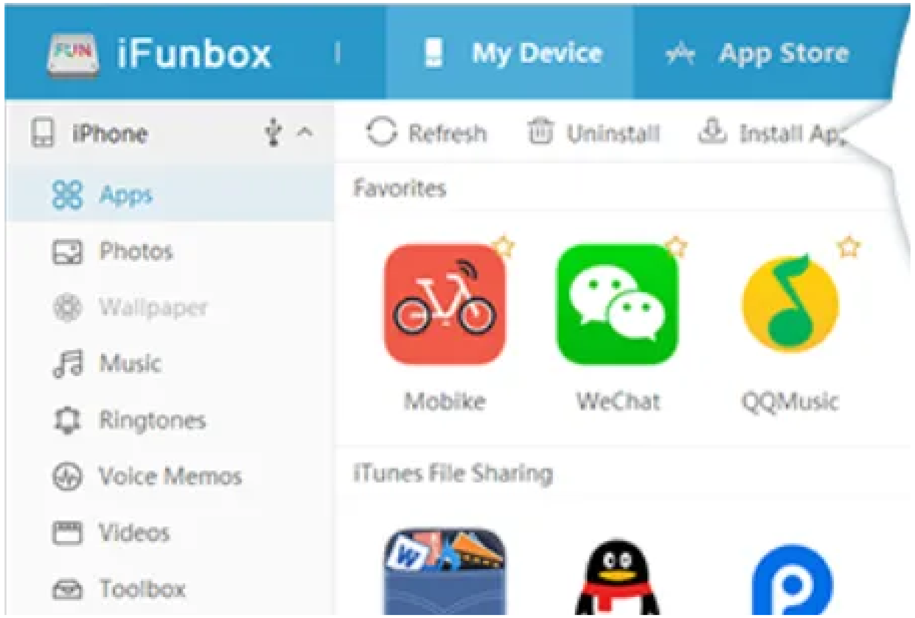
Juan on How to make a "Ultra-Geek" Linux Workstation

> ***https://github.com/tcurdt/iProxy***

itunnel

Use to forward SSH via USB.

iFunbox

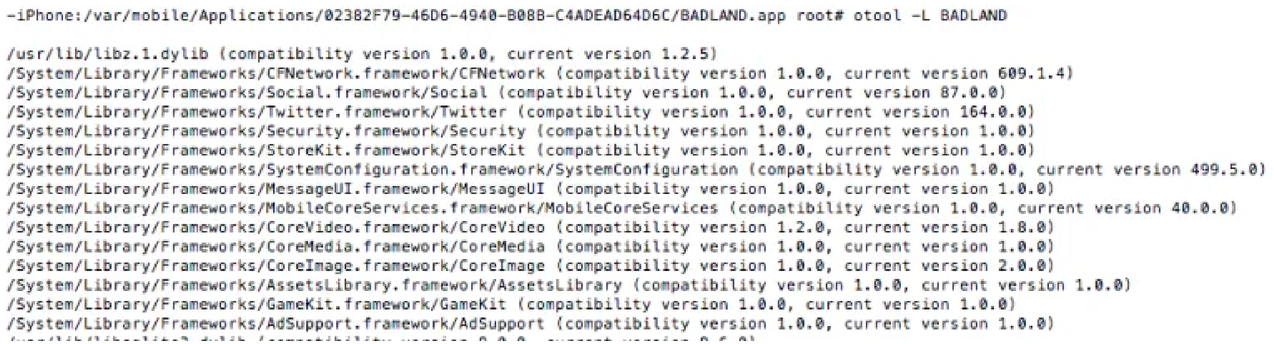


The File and App Management Tool for iPhone, iPad & iPod Touch.

Static Analysis

Process Injection Teknikleri - Process Hollowing ve Atombombing - Manalysiz on RunPE: a practical example of Process Hollowing technique

otool



```
-iPhone:/var/mobile/Applications/02382F79-46D6-4940-B08B-C4ADEAD64D6C/BADLAND.app root# otool -L BADLAND

/usr/lib/libz.1.dylib (compatibility version 1.0.0, current version 1.2.5)
/System/Library/Frameworks/CFNetwork.framework/CFNetwork (compatibility version 1.0.0, current version 609.1.4)
/System/Library/Frameworks/Social.framework/Social (compatibility version 1.0.0, current version 87.0.0)
/System/Library/Frameworks/Twitter.framework/Twitter (compatibility version 1.0.0, current version 164.0.0)
/System/Library/Frameworks/Security.framework/Security (compatibility version 1.0.0, current version 1.0.0)
/System/Library/Frameworks/StoreKit.framework/StoreKit (compatibility version 1.0.0, current version 1.0.0)
/System/Library/Frameworks/SystemConfiguration.framework/SystemConfiguration (compatibility version 1.0.0, current version 499.5.0)
/System/Library/Frameworks/MessageUI.framework/MessageUI (compatibility version 1.0.0, current version 1.0.0)
/System/Library/Frameworks/MobileCoreServices.framework/MobileCoreServices (compatibility version 1.0.0, current version 40.0.0)
/System/Library/Frameworks/CoreVideo.framework/CoreVideo (compatibility version 1.2.0, current version 1.8.0)
/System/Library/Frameworks/CoreMedia.framework/CoreMedia (compatibility version 1.0.0, current version 1.0.0)
/System/Library/Frameworks/CoreImage.framework/CoreImage (compatibility version 1.0.0, current version 2.0.0)
/System/Library/Frameworks/AssetsLibrary.framework/AssetsLibrary (compatibility version 1.0.0, current version 1.0.0)
/System/Library/Frameworks/GameKit.framework/GameKit (compatibility version 1.0.0, current version 1.0.0)
/System/Library/Frameworks/AdSupport.framework/AdSupport (compatibility version 1.0.0, current version 1.0.0)
```

The otool command displays specified parts of object files or libraries.

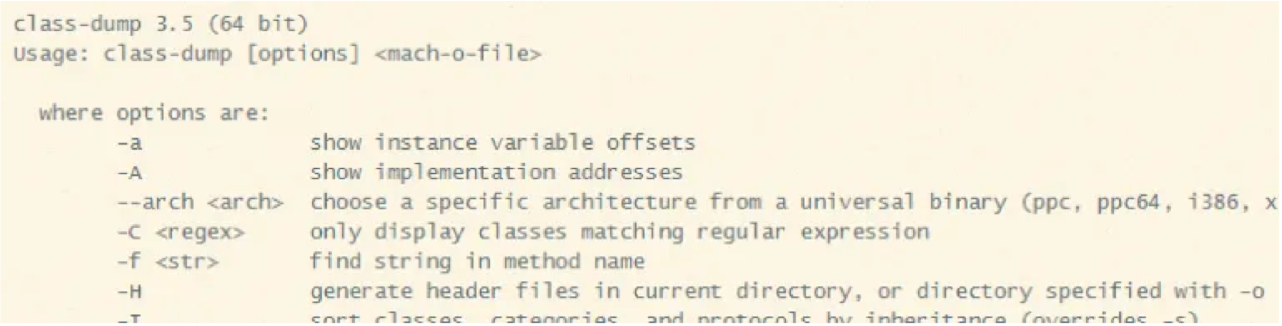
Clutch

Clutch is a high-speed iOS decryption tool. Clutch supports the iPhone, iPod Touch, and iPad as well as all iOS version, architecture types, and most binaries.

Dumpdecrypted

Dumps decrypted mach-o files from encrypted iPhone applications from memory to disk. This tool is necessary for security researchers to be able to look under the hood of encryption.

class-dump



```
class-dump 3.5 (64 bit)
Usage: class-dump [options] <mach-o-file>

  where options are:
        -a             show instance variable offsets
        -A             show implementation addresses
        --arch <arch>  choose a specific architecture from a universal binary (ppc, ppc64, i386, x
        -C <regex>     only display classes matching regular expression
        -f <str>       find string in method name
        -H             generate header files in current directory, or directory specified with -o
        -I             sort classes, categories, and protocols by inheritance (overrides -s)
```

A command-line utility for examining the Objective-C runtime information stored in Mach-O files.

Weak Classdump

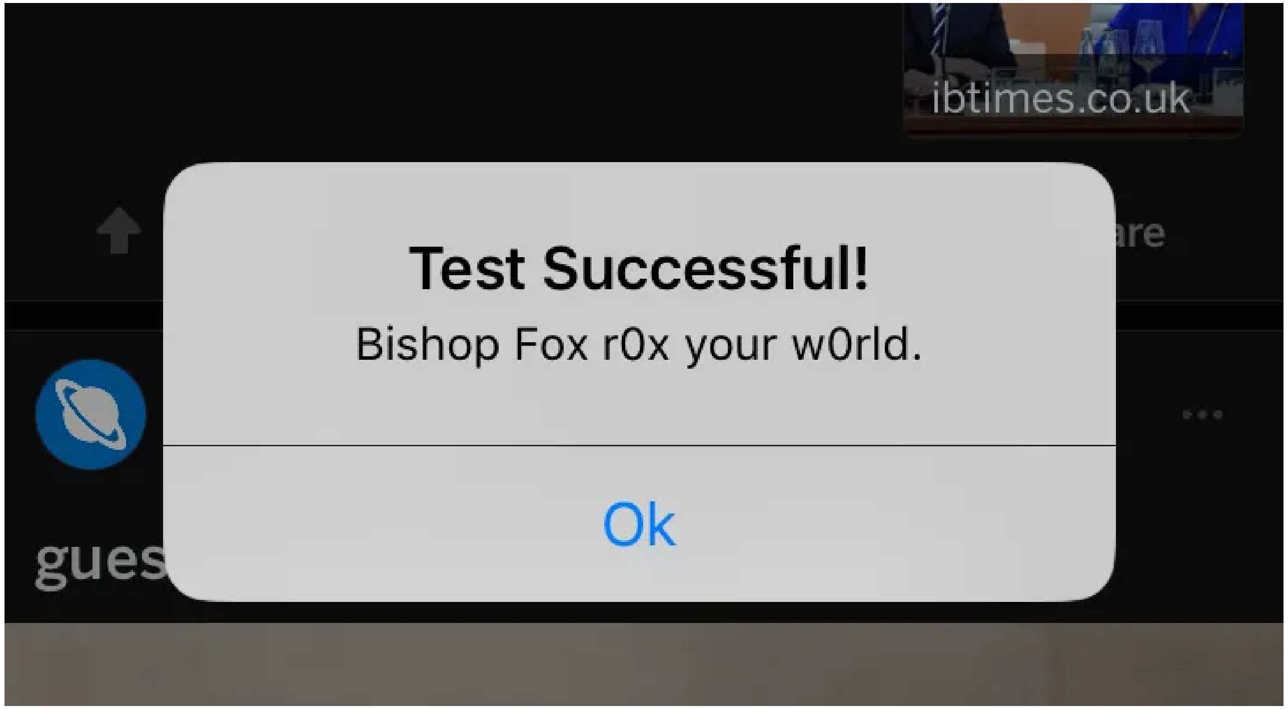
```
root# cycript -p Skype weak_classdump.cy; cycript -p Skype
'Added weak_classdump to "Skype" (1685)'

cy# UIApp
"<HellcatApplication: 0x1734e0>"

cy# weak_classdump(HellcatApplication);
"Wrote file to /tmp/HellcatApplication.h"
```

A Cycript script that generates a header file for the class passed to the function. Most useful when you cannot classdump or dumpdecrypted , when binaries are encrypted etc.

Fridpa

An automated wrapper script for patching iOS applications (IPA files) and work on non-jailbroken device.

bfinject

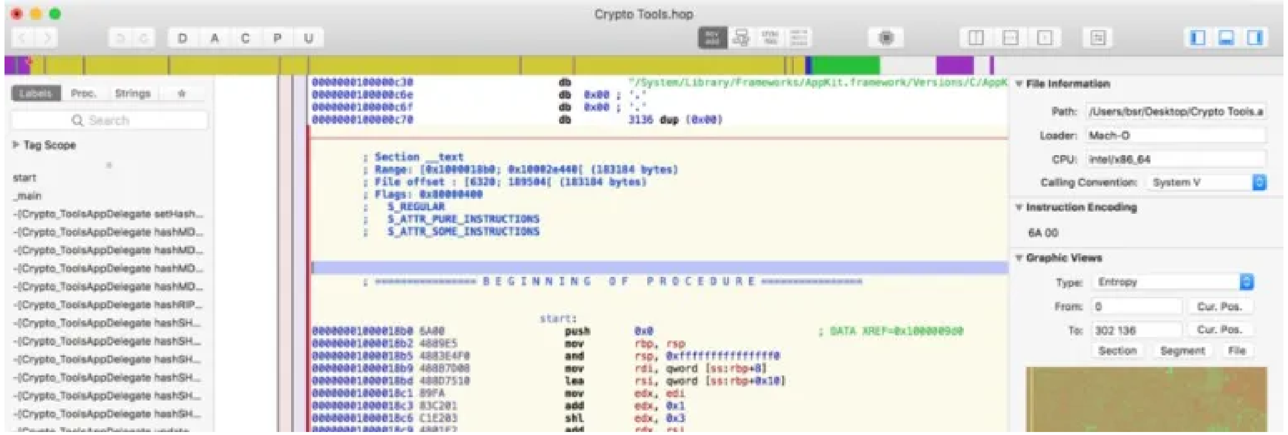


Test Successful!

Bishop Fox r0x your w0rld.

bfinject loads arbitrary dylibs into running App Store apps. It has built-in support for decrypting App Store apps, and comes bundled with iSpy and Cycript.

HopperApp



```
start
_main
-[Crypto_ToolsAppDelegate setHash…
-[Crypto_ToolsAppDelegate hashMD…
-[Crypto_ToolsAppDelegate hashMD…
-[Crypto_ToolsAppDelegate hashMD…
-[Crypto_ToolsAppDelegate hashMD…
-[Crypto_ToolsAppDelegate hashRIP…
-[Crypto_ToolsAppDelegate hashSH…
-[Crypto_ToolsAppDelegate hashSH…
-[Crypto_ToolsAppDelegate hashSH…
-[Crypto_ToolsAppDelegate hashSH…
-[Crypto_ToolsAppDelegate hashSH…
-[Crypto_ToolsAppDelegate hashSH…
```

```
0000000100000c30         db        "/System/Library/Frameworks/AppKit.framework/Versions/C/AppK
0000000100000c6e         db  0x00 ; '.'
0000000100000c6f         db  0x00 ; '.'
0000000100000c70         db        3136 dup (0x00)

      ; Section __text
      ; Range: [0x1000018b0; 0x10002e440[ (183184 bytes)
      ; File offset : [6320; 189504[ (183184 bytes)
      ; Flags: 0x80000400
      ;   S_REGULAR
      ;   S_ATTR_PURE_INSTRUCTIONS
      ;   S_ATTR_SOME_INSTRUCTIONS

      ; ================ B E G I N N I N G   O F   P R O C E D U R E ================

                                  start:
00000001000018b0 6A00            push       0x0                                    ; DATA XREF=0x1000009d0
00000001000018b2 4889E5          mov        rbp, rsp
00000001000018b5 4883E4F0        and        rsp, 0xfffffffffffffff0
00000001000018b9 488B7D08        mov        rdi, qword [ss:rbp+8]
00000001000018bd 488D7510        lea        rsi, qword [ss:rbp+0x10]
00000001000018c1 89FA            mov        edx, edi
00000001000018c3 83C201          add        edx, 0x1
00000001000018c6 C1E203          shl        edx, 0x3
```

File Information

Path: /Users/bsr/Desktop/Crypto Tools.a

Loader: Mach-O

CPU: intel/x86_64

Calling Convention: System V

Instruction Encoding

6A 00

Graphic Views

Type: Entropy

From: 0

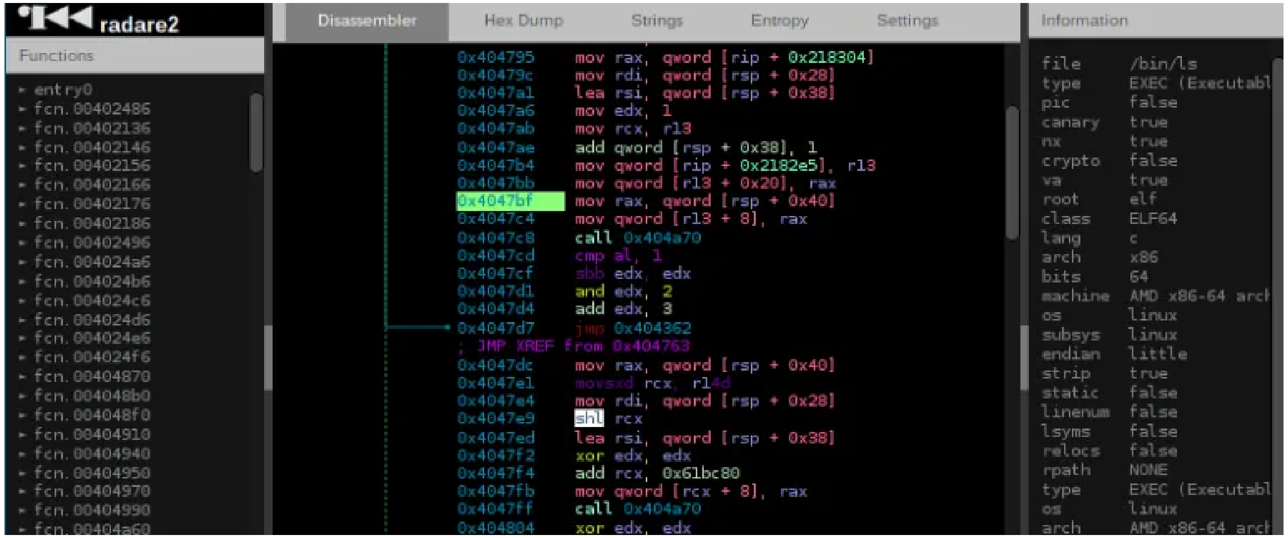
To: 302 136

Hopper is a reverse engineering tool for OS X and Linux, that lets you disassemble, decompile and debug your 32/64bits Intel Mac, Linux, Windows and iOS executables.

hopperscripts

Hopperscripts can be used to demangle the Swift function name in HopperApp.

Radare2



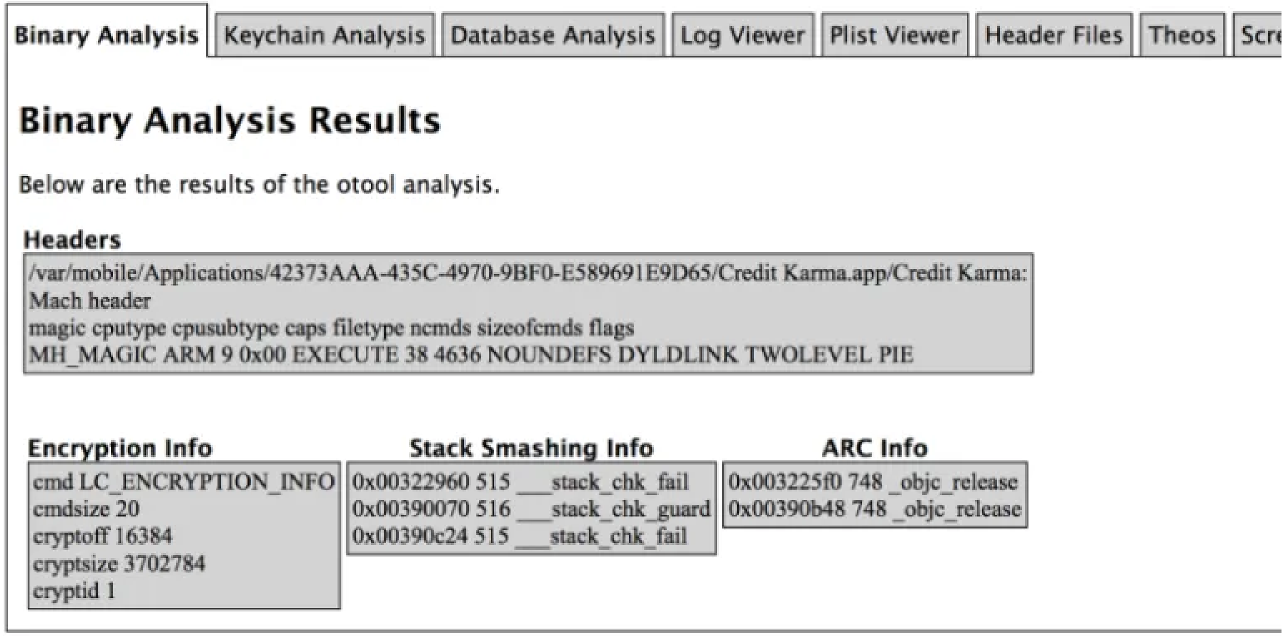
```
entry0
fcn.00402486
fcn.00402136
fcn.00402146
fcn.00402156
fcn.00402166
fcn.00402176
fcn.00402186
fcn.00402496
fcn.004024a6
fcn.004024b6
fcn.004024c6
fcn.004024d6
fcn.004024e6
fcn.004024f6
fcn.00404870
fcn.004048b0
fcn.004048f0
fcn.00404910
fcn.00404940
fcn.00404950
fcn.00404970
fcn.00404990
fcn.00404a60
```

```
0x404795    mov rax, qword [rip + 0x218304]
0x40479c    mov rdi, qword [rsp + 0x28]
0x4047a1    lea rsi, qword [rsp + 0x38]
0x4047a6    mov edx, 1
0x4047ab    mov rcx, r13
0x4047ae    add qword [rsp + 0x38], 1
0x4047b4    mov qword [rip + 0x2182e5], r13
0x4047bb    mov qword [r13 + 0x20], rax
0x4047bf    mov rax, qword [rsp + 0x40]
0x4047c4    mov qword [r13 + 8], rax
0x4047c8    call 0x404a70
0x4047cd    cmp al, 1
0x4047cf    sbb edx, edx
0x4047d1    and edx, 2
0x4047d4    add edx, 3
0x4047d7    jmp 0x404362
; JMP XREF from 0x404763
0x4047dc    mov rax, qword [rsp + 0x40]
0x4047e1    movsxd rcx, r14d
0x4047e4    mov rdi, qword [rsp + 0x28]
0x4047e9    shl rcx
0x4047ed    lea rsi, qword [rsp + 0x38]
0x4047f2    xor edx, edx
0x4047f4    add rcx, 0x61bc80
0x4047fb    mov qword [rcx + 8], rax
0x4047ff    call 0x404a70
0x404804    xor edx, edx
```

```
file      /bin/ls
type      EXEC (Executabl
pic       false
canary    true
nx        true
crypto    false
va        true
root      elf
class     ELF64
lang      c
arch      x86
bits      64
machine   AMD x86-64 arch
os        linux
subsys    linux
endian    little
strip     true
static    false
linenum   false
lsyms     false
relocs    false
rpath     NONE
type      EXEC (Executabl
os        linux
arch      AMD x86-64 arch
```

Radare2 is a unix-like reverse engineering framework and commandline tools.

iOS Reverse Engineering Toolkit (iRET)



Binary Analysis Results

Below are the results of the otool analysis.

Headers

```
/var/mobile/Applications/42373AAA-435C-4970-9BF0-E589691E9D65/Credit Karma.app/Credit Karma:
Mach header
magic cputype cpusubtype caps filetype ncmds sizeofcmds flags
MH_MAGIC ARM 9 0x00 EXECUTE 38 4636 NOUNDEFS DYLDLINK TWOLEVEL PIE
```

Encryption Info

```
cmd LC_ENCRYPTION_INFO
cmdsize 20
cryptoff 16384
cryptsize 3702784
cryptid 1
```

Stack Smashing Info

```
0x00322960 515 ___stack_chk_fail
0x00390070 516 ___stack_chk_guard
0x00390c24 515 ___stack_chk_fail
```

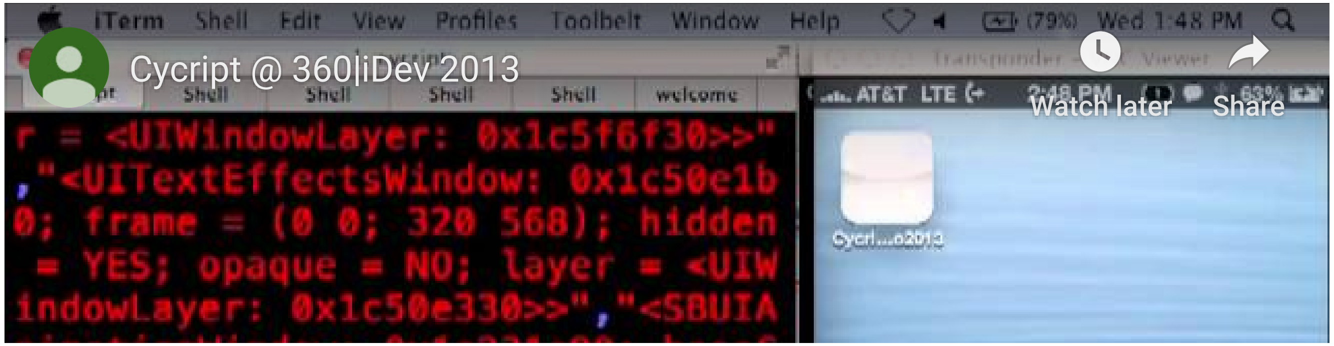
ARC Info

```
0x003225f0 748 _objc_release
0x00390b48 748 _objc_release
```

The iOS Reverse Engineering Toolkit is a toolkit designed to automate many of the common tasks associated with iOS penetration testing.

Dynamic Analysis

cycript

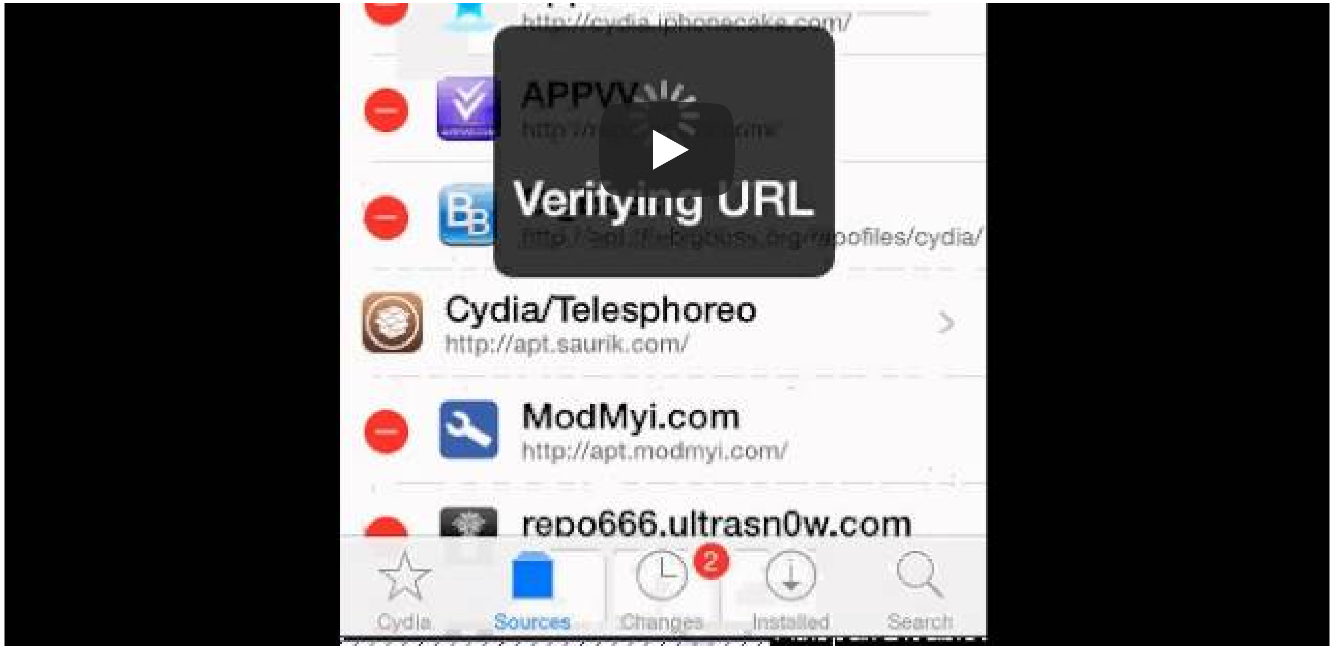


```
r = <UIWindowLayer: 0x1c5f6f30>>"
,"<UITextEffectsWindow: 0x1c50e1b
0; frame = (0 0; 320 568); hidden
 = YES; opaque = NO; layer = <UIW
indowLayer: 0x1c50e330>>","<SBUIA
```

```
nimationWindow: 0x1e231a90; basec
lass = UIWindow; frame = (0 0; 32
0 568); hidden = YES; userInterac
tionEnabled = NO; layer = <UIWind
owLayer: 0x1da14c80>>","<SBSpring
BoardMetaHostingWindow: 0x1c5b2b2
0; baseClass = UIWindow; frame =
(0 0; 320 568); hidden = YES; lay
er = <UIWindowLayer: 0x1c5b2bf0>>
","<UIWindow: 0x222cf4b0; frame =
 (0 0; 0 0); userInteractionEnabl
ed = NO; layer = <UIWindowLayer:
0x1da19310>>"]
cy#
```

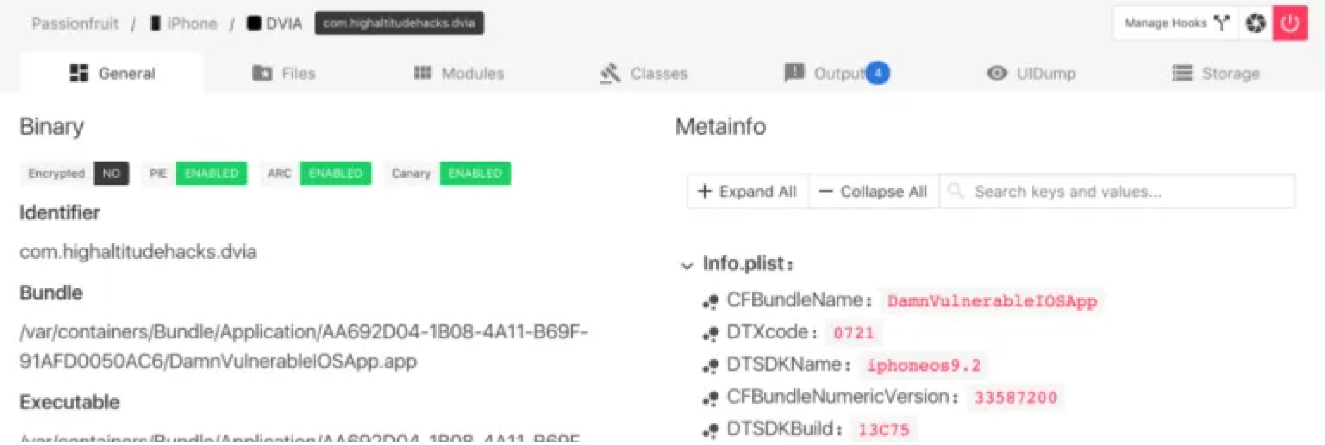
Cycript allows developers to explore and modify running applications on either iOS or Mac OS X using a hybrid of Objective-C++ and JavaScript syntax through an interactive console that features syntax highlighting and tab completion.

iNalyzer



AppSec Labs iNalyzer is a framework for manipulating iOS applications, tampering with parameters and method.

Passionfruit



Binary

Encrypted NO PIE ENABLED ARC ENABLED Canary ENABLED

Identifier

com.highaltitudehacks.dvia

Bundle

/var/containers/Bundle/Application/AA692D04-1B08-4A11-B69F-91AFD0050AC6/DamnVulnerableIOSApp.app

Executable

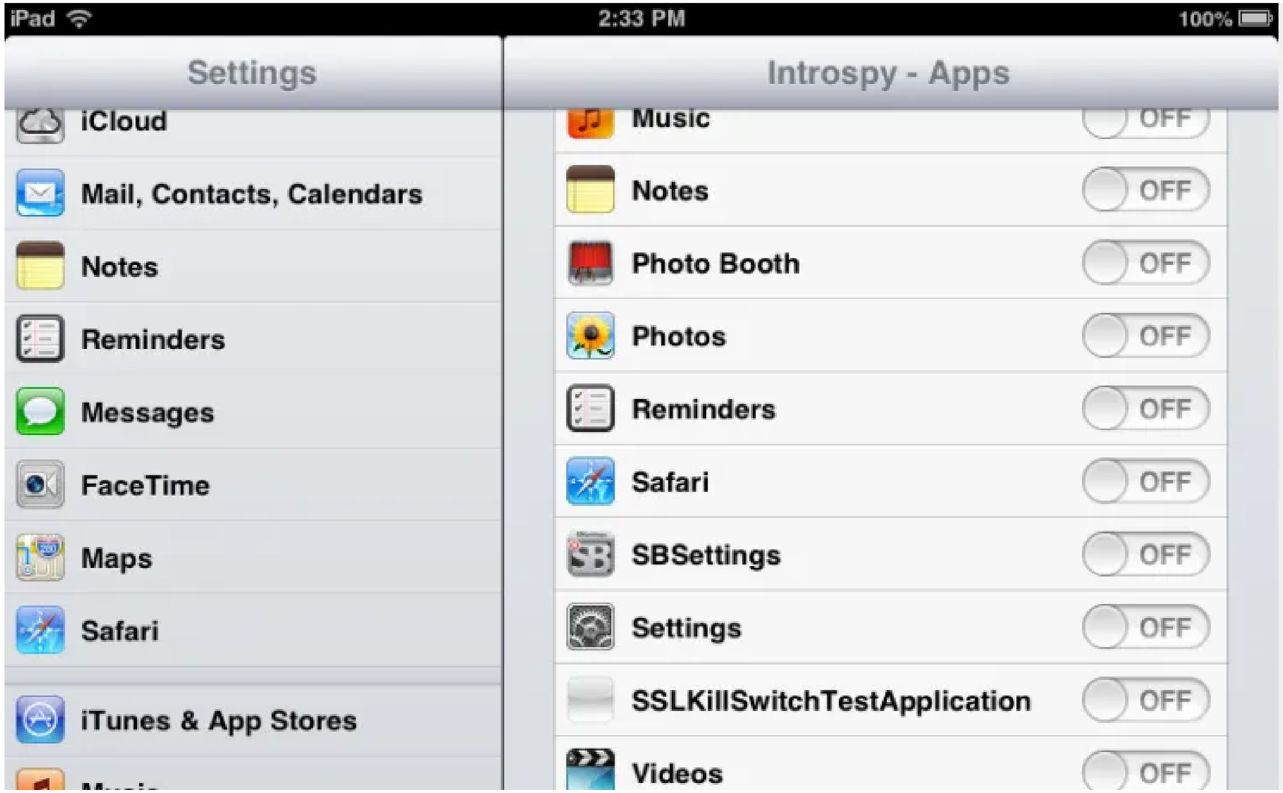
Metainfo

Info.plist:

```
CFBundleName: DamnVulnerableIOSApp
DTXcode: 0721
DTSDKName: iphoneos9.2
CFBundleNumericVersion: 33587200
DTSDKBuild: 13C75
```

Simple iOS app blackbox assessment tool with Fully web based GUI. Powered by frida.re and vuejs.

Introspy-iOS



iPad 2:33 PM 100%

Settings

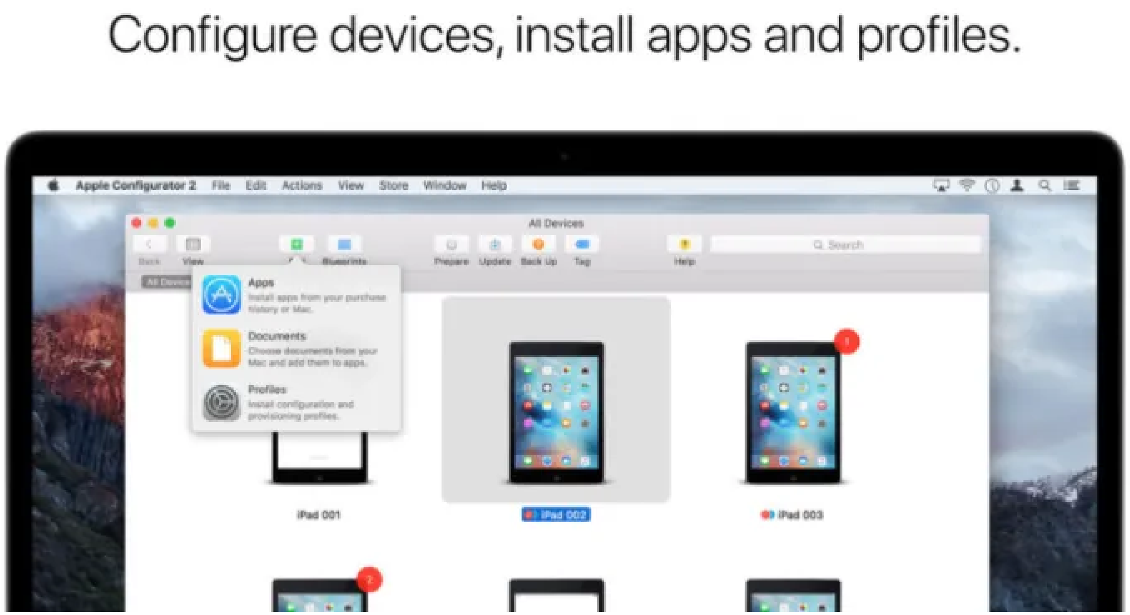
- iCloud
- Mail, Contacts, Calendars
- Notes
- Reminders
- Messages
- FaceTime
- Maps
- Safari
- iTunes & App Stores

Introspy - Apps

Music	OFF
Notes	OFF
Photo Booth	OFF
Photos	OFF
Reminders	OFF
Safari	OFF
SBSettings	OFF
Settings	OFF
SSLKillSwitchTestApplication	OFF
Videos	OFF

Blackbox tool to help understand what an iOS application is doing at runtime and assist in the identification of potential security issues.

Apple configurator 2



Configure devices, install apps and profiles.

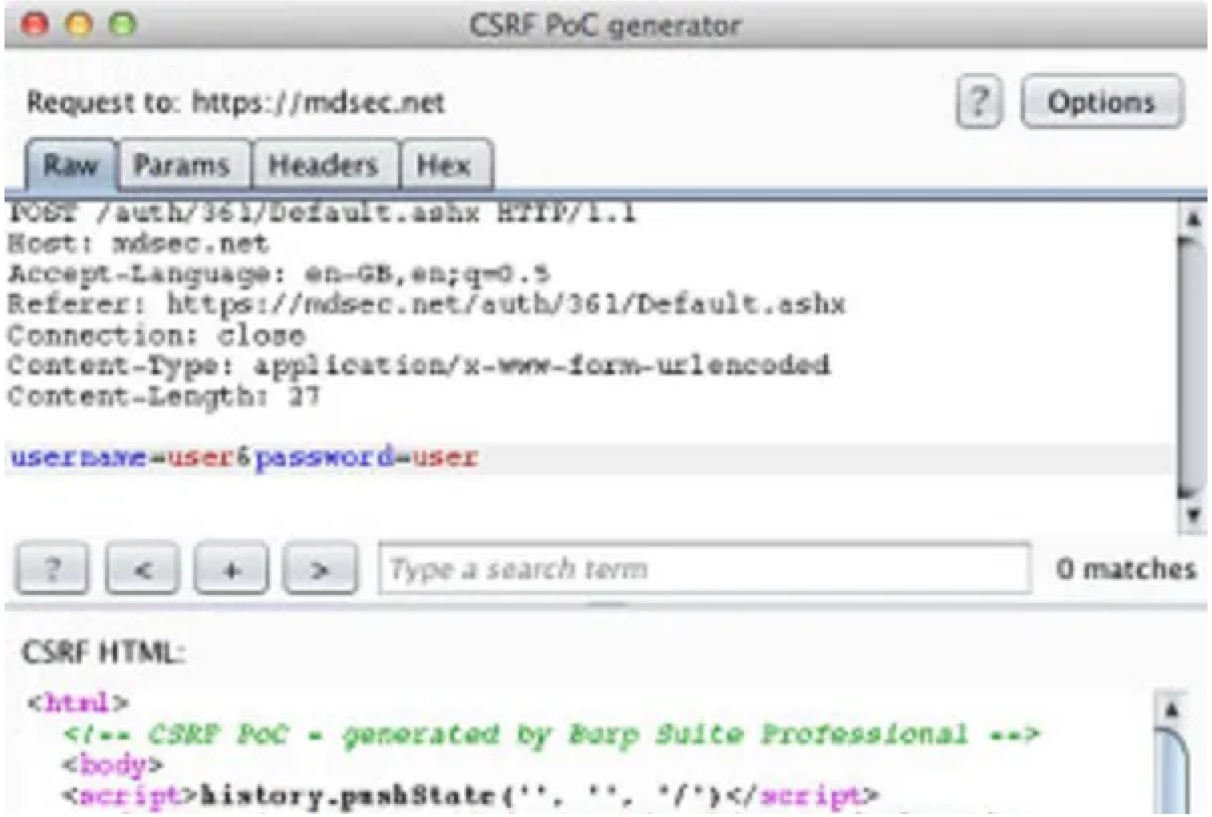
A utility which can be used to view live system log on iDevice.

keychaindumper

A tool to check which keychain items are available to an attacker once an iOS device has been jailbroken.

Network Analysis

Burp Suite



```
POST /auth/361/Default.ashx HTTP/1.1
Host: mdsec.net
Accept-Language: en-GB,en;q=0.5
Referer: https://mdsec.net/auth/361/Default.ashx
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 27

username=user&password=user
```

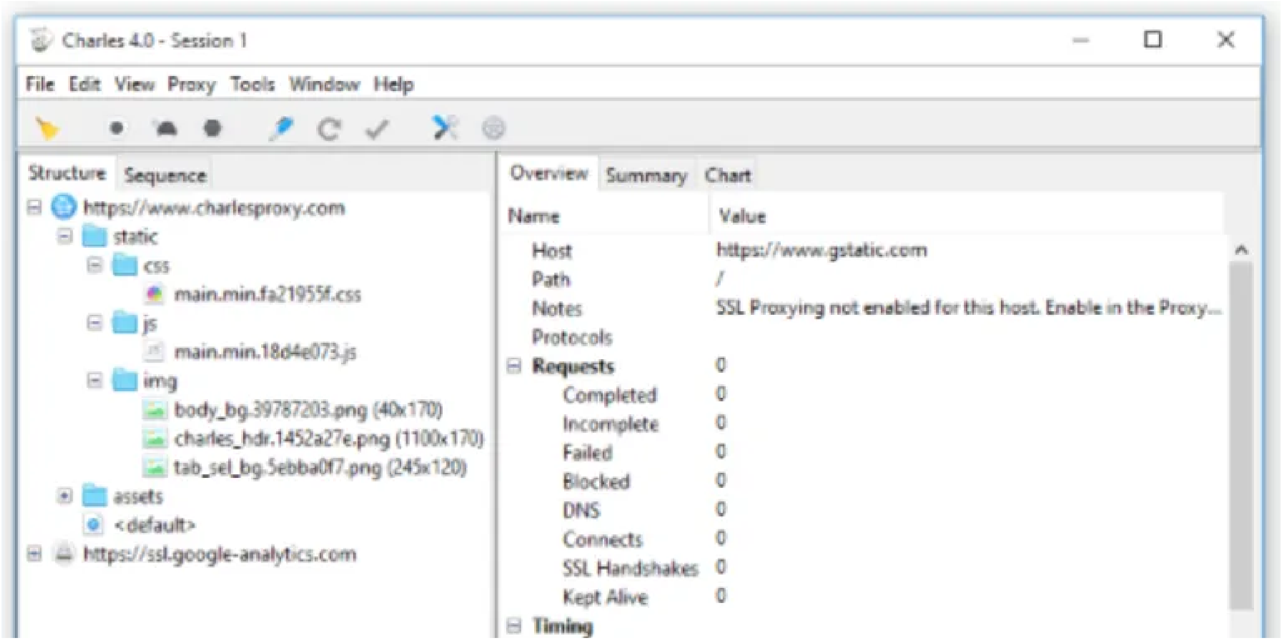
```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
```

Burp Suite is an integrated platform for performing security testing of applications.

OWASP ZAP

OWASP Zed Attack Proxy Project is an open-source web application security scanner. It is intended to be used by both those new to application security as well as professional penetration testers.

Charles Proxy



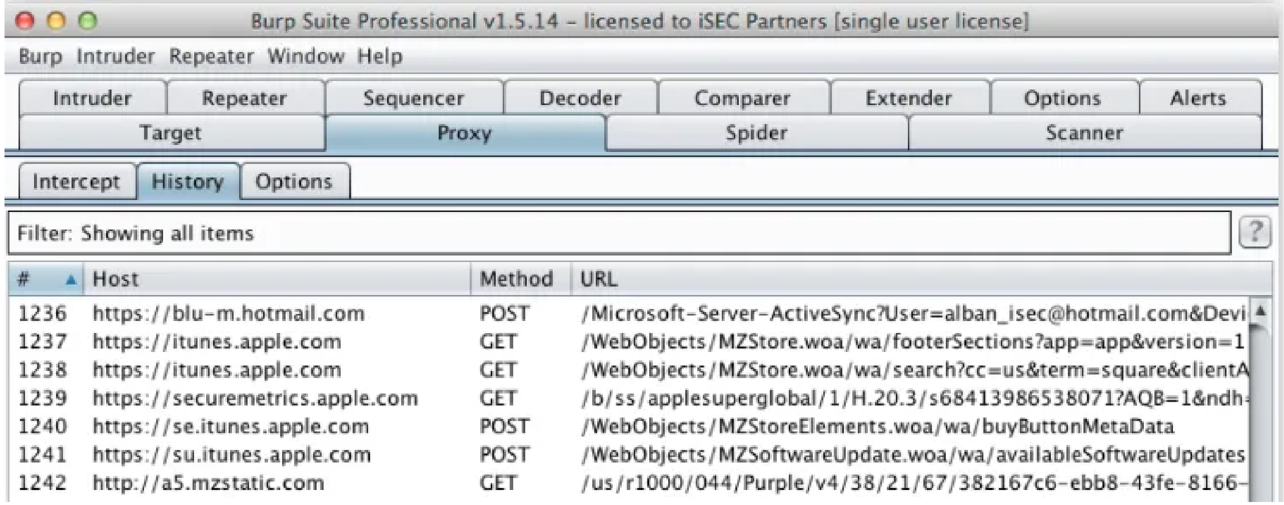
```
⊟ https://www.charlesproxy.com
   ⊟ static
      ⊟ css
           main.min.fa21955f.css
      ⊟ js
           main.min.18d4e073.js
      ⊟ img
           body_bg.39787203.png (40x170)
           charles_hdr.1452a27e.png (1100x170)
           tab_sel_bg.5ebba0f7.png (245x120)
   ⊞ assets
      <default>
⊟ https://ssl.google-analytics.com
```

Name	Value
Host	https://www.gstatic.com
Path	/
Notes	SSL Proxying not enabled for this host. Enable in the Proxy...
Protocols	
⊟ **Requests**	0
Completed	0
Incomplete	0
Failed	0
Blocked	0
DNS	0
Connects	0
SSL Handshakes	0
Kept Alive	0
⊟ **Timing**	

HTTP proxy / HTTP monitor / Reverse Proxy that enables a developer to view all of the HTTP and SSL / HTTPS traffic between their machine and the Internet.

Bypassing Jailbreak Detection and SSL Pinning

SSL Kill Switch 2


Burp Suite Professional v1.5.14 – licensed to iSEC Partners [single user license]
Burp Intruder Repeater Window Help
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Options
Alerts
Target
Proxy
Spider
Scanner
Intercept
History
Options
?

Filter: Showing all items

#	Host	Method	URL
1236	https://blu-m.hotmail.com	POST	/Microsoft-Server-ActiveSync?User=alban_isec@hotmail.com&Devi
1237	https://itunes.apple.com	GET	/WebObjects/MZStore.woa/wa/footerSections?app=app&version=1
1238	https://itunes.apple.com	GET	/WebObjects/MZStore.woa/wa/search?cc=us&term=square&clientA
1239	https://securemetrics.apple.com	GET	/b/ss/applesuperglobal/1/H.20.3/s68413986538071?AQB=1&ndh-
1240	https://se.itunes.apple.com	POST	/WebObjects/MZStoreElements.woa/wa/buyButtonMetaData
1241	https://su.itunes.apple.com	POST	/WebObjects/MZSoftwareUpdate.woa/wa/availableSoftwareUpdates
1242	http://a5.mzstatic.com	GET	/us/r1000/044/Purple/v4/38/21/67/382167c6-ebb8-43fe-8166-

Blackbox tool to disable SSL certificate validation – including certificate pinning – within iOS and OS X Apps.

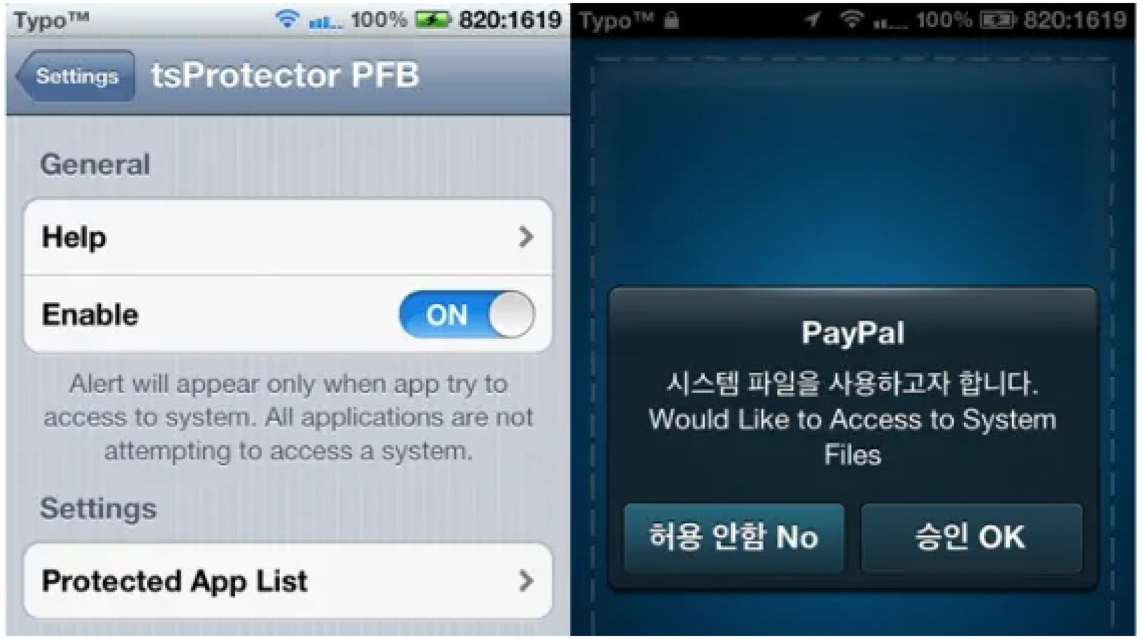
iOS TrustMe

Disable certificate trust checks on iOS devices.
The tool is patterned on **ios-ssl-kill-switch**: it uses a similar technique, but targets a C function that is lower in the call chain of most SSL certificate validation code, which allows it to disable more SSL validation code.

Xcon

A tool for bypassing Jailbreak detection.

tsProtector



Enable: ON

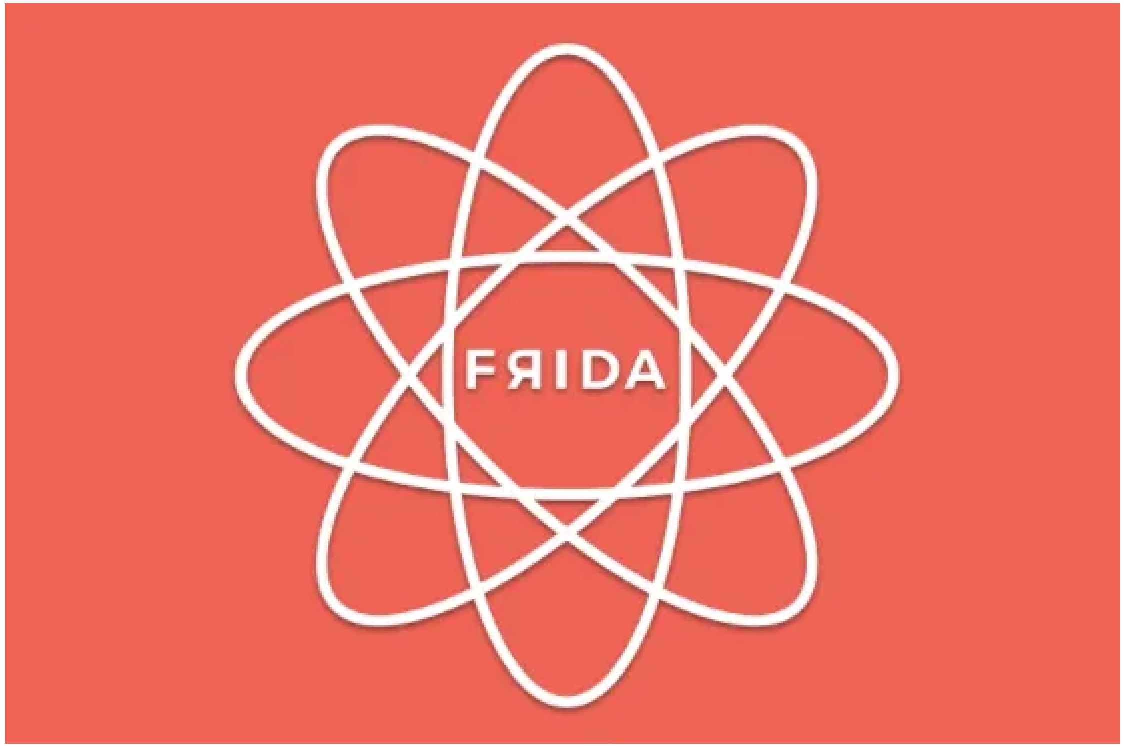
Alert will appear only when app try to access to system. All applications are not attempting to access a system.

PayPal

시스템 파일을 사용하고자 합니다.
Would Like to Access to System Files

Another tool for bypassing Jailbreak detection.

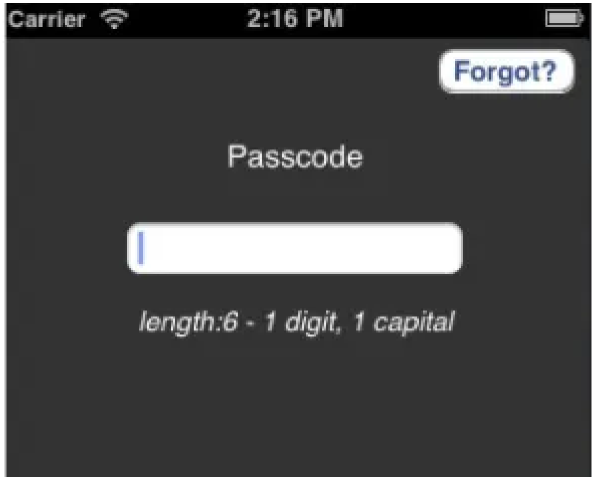
Frida CodeShare



The Frida CodeShare project is comprised of developers from around the world working together with one goal – push Frida to its limits in new and innovative ways.

Security Libraries

OWASP iMAS



Carrier 2:16 PM

Forgot?

Passcode

length:6 - 1 digit, 1 capital

iMAS is a collaborative research project from the MITRE Corporation focused on open source iOS security controls.

Related posts

Share this:

Like this:

Loading...

TAGS

APPLE FEATURE IOS PENETRATION TESTING

PRINT

Andrea Fortuna

CVE-2019-1125, "SWAPGS Attack": a new speculative execution side-channel attack

COMMENTS

Enter your comment here...

This site uses Akismet to reduce spam. Learn how your comment data is processed.