WEB应用安全和数据库安全的领航者！

安恒信息技术有限公司

Pentesting Mobile Applications

www.dbappsecurity.com.cn

Who am I

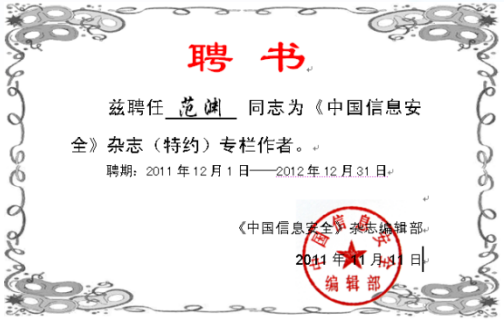
- **Frank Fan: CTO of DBAPPSecurity**

— Graduated from California State University as a Computer Science PhD.
— With more than ten years of technical research and project management experience in world famous security companies
— Mr. Frank Fan researched deeply about online security, database security and auditing and compliance(such as SOX, PCI, ISO17799/27001).
— Became the first Chinese who made a speech in the World's top security conference BLACKHAT and he has certificates such as CISSP, CISA, GCIH, GCIA, etc.
— The vice president of OWASP China
— Member of 2008 Olympic Organizing Committee security group.
— Member of China Computer Society Branch
— Columnist of《 China Information Security 》
……


聘 书

兹聘任 范渊 同志为中国计算机学会计算机安全专业委员会常务委员。

中国计算机学会计算机安全专业委员会
二〇一〇年八月十五日


聘 书

兹聘任 范渊 同志为《中国信息安全》杂志（特约）专栏作者。

聘期：2011 年 12 月 1 日——2012 年 12 月 31 日

《中国信息安全》杂志编辑部
2011 年 12 月 11 日


浙江省海外高层次人才引进计划
浙江省特聘专家

证 书

授予 范 渊 先生浙江省特聘专家称号。

特颁此证

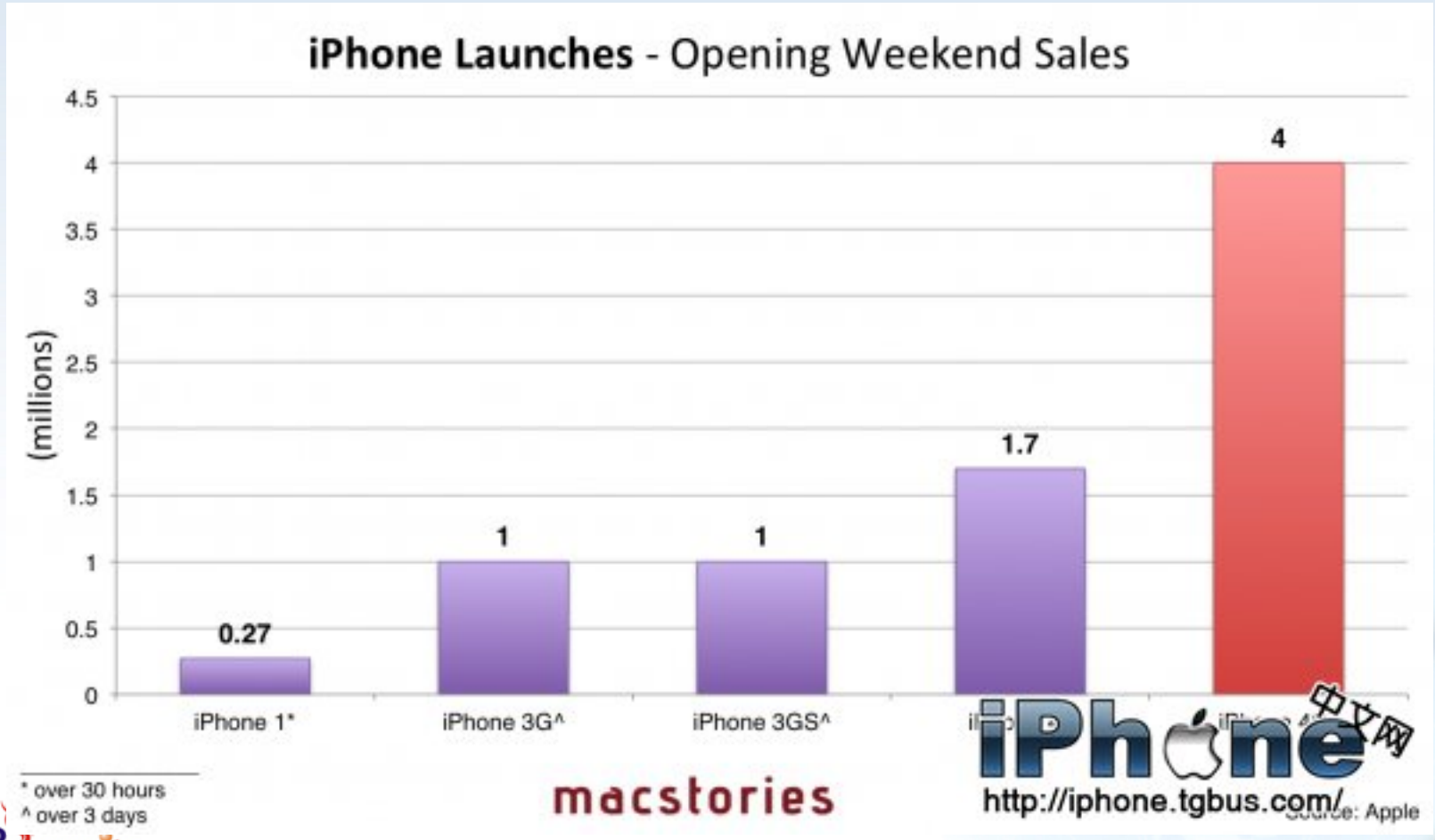
DBAPP Security 安恒信息

catalogue

- iPhone&Adriod Application Basics
- Pentesting iPhone Applications
- Pentesting Andriod Applications
- Major Mobile Threats

Apple iPhone Application Basics

- iPhone first published in 2007.



Apple iPhone Application Basics

- Browser Based Application
  - HTML + CSS + JavaScript
  - IOS Application Program
  - Objective C&Cocoa Touch API
    - Super set of C, Compiles into native code (ARM)
- Apple Store (App Store)
  - Centralized mechanism to distribute software
  - Only Apple signed application are available
  - Designed to protect the Apps from piracy & No malware

Apple iPhone Application Basics

- Why to build iPhone application
  - New business
  - Good ways to launch new services
  - Urgentcy of clients
  - Users want them
  - Fame (Angry Birds /Fruit Ninja)

Apple iPhone Application Basics

- iPhone Applications
  - Package Suffix.ipa
  - Running test on iPhone emulator
  - Testing with equipment
  - Releasing at App Store

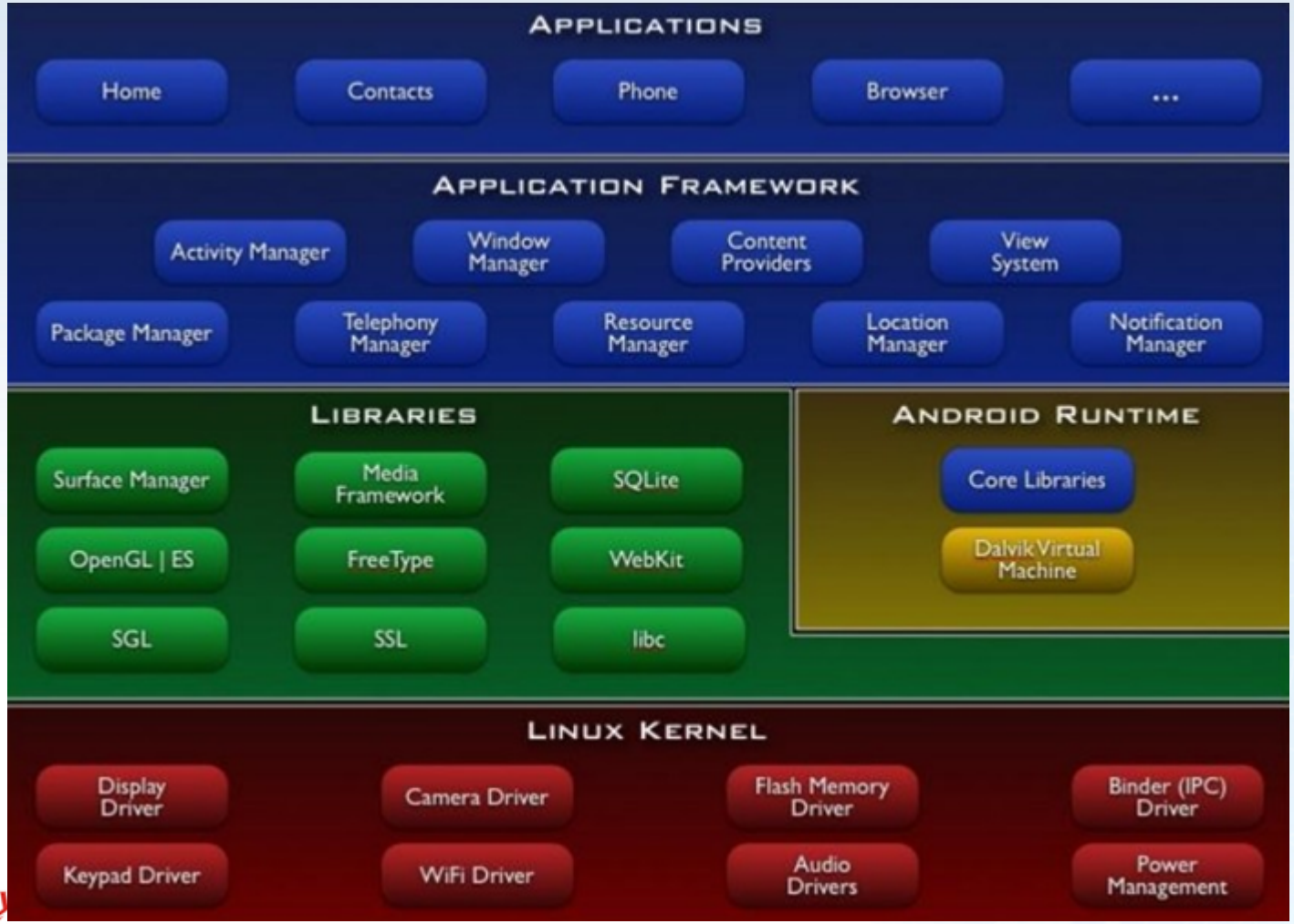
✓ The application program must subject to evaluation

Google Android Application Basics

- Andriod released the growth from January to September in 2011

Google Android Application Basics

- Andriod Holistic Architecture



Google Android Application Basics

- Android System Architecture
  - Application program
  - Application Frame
  - Program Library
  - Android Runtime Library
  - Linux Core

catalog

- iPhone&Adriod Application Basics
- Pentesting iPhone Application
- Pentesting Andriod Application
- Major Mobile Threats

Pentesting iPhone Application

- Areas of focus Include
  -Network Communication
  -Privacy
  -Application Data Storage
  -Reverse Engineering
  -URL Schemes
  -Push Notification

Pentesting iPhone Application

- Jailbreak
  - iPhone doesn`t allow unsigned applications
  - After Jailbreaking ,full access to the device
  - To allow install unauthorized software
  - Tools: PwnageTool，redsn0w，Sn0wbreeze, Greenpois0n, jailbreakMe…
  - It makes our work easier.

Pentesting iPhone Application

- Some useful Cydia for safety testing as follows.
  - OpenSSH:Allows us to connect to the iPhone remotely over SSH
  - Adv-cmds:Comes with a set of process commands like ps, kill, finger…
  - Sqlite3:Sqlite database client
  - GNU Debugger:For run time analysis & reverse engineering
  - Syslogd:To view iPhone logs
  - Veency:Allows to view the phone on the workstation with the help of veency client
  - Tcpdump:To capture network traffic on phone
  - com.ericasadun.utlities:plutil to view property list files
  - Grep:For searching
  - Odcctools:otool – object file displaying tool
  - Crackulous:Decrypt iPhone apps
  - Hackulous:To install decrypted apps

Pentesting iPhone Application

- Connect the SSH to iPhone
  - From Cydia Install Open SSH
  - Install SSH Client On PC
  - By default, iPhone has two users (root、mobile)
    - Root and mobile (default password : 'alpine')
  - With root user through SSH connect to phone .
    - SSH through WIFI
      - > ssh root@iPhoneIP
      - > password: alpine
    - SSH through USB
      - > ./itunnel_mux --lport 1234
      - > ssh –p 1234 root@127.0.0.1
      - > password: alpine

Pentesting iPhone Application

- Network communication

✓ Mobile application pentesting isn't really all that different.

- It involves network communication

✓ Communication Mechanism

-- Clear text Transmission (HTTP)

-- Encrypted Transmission （HTTPS）

-- Use of Custom or Proprietary protocols

Pentesting iPhone Application

- Clear text Transmission

  — Many applications still use clear text transport protocol by 2012.(HTTP)

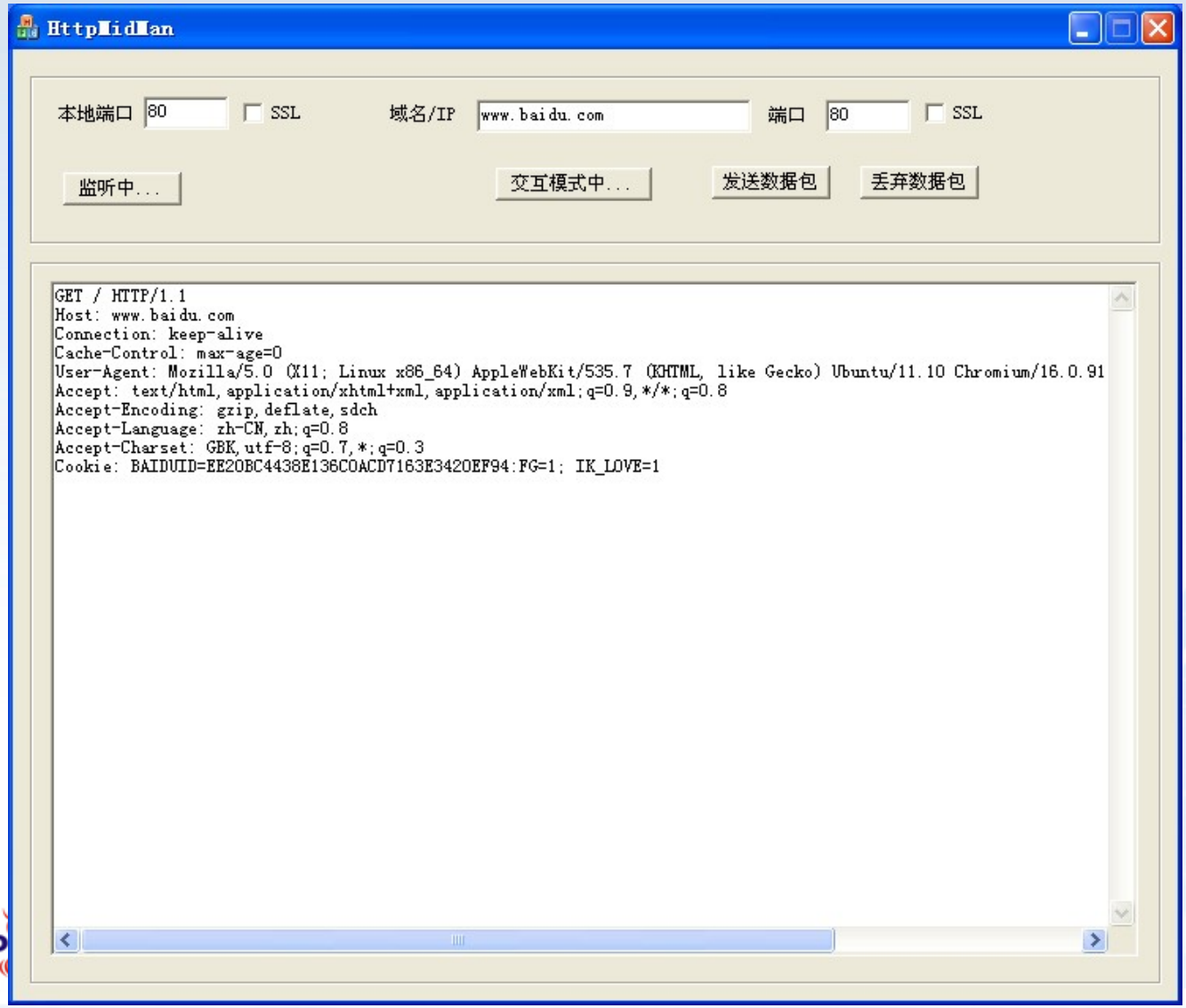
  — Be more vulnerable to the MITM attack.

✓ Most people by accessing WIFI, the same WiFi attackers can run like FireSheep tools of attacks

— To analyze HTTP traffic

✓ By manual proxy in iPhone(set-wlan- manual)

Pentesting iPhone Application



Pentesting iPhone Application

- Encrypted Transmission
  — HTTPS is used to transmission sensitive data。

  — With SSL communicate

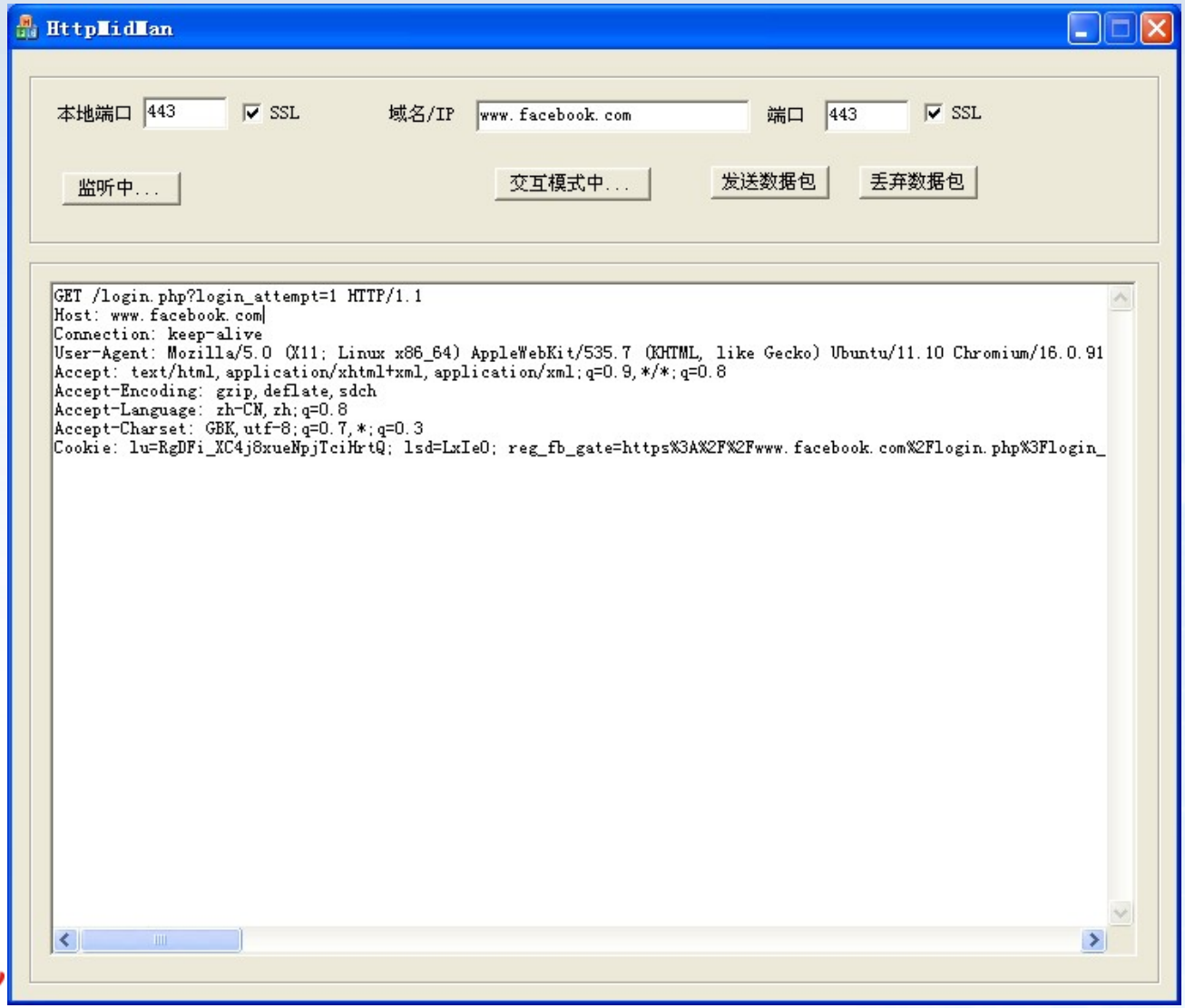
✓ Applications may fail veridate SSL cert

✓ *allowsAnyHTTPSCertificateForHost*

— An application of verifying certificate shouldn`t allow MITM

— To capture the traffic, it needs to loading proxy CA certificate to iPhone.

Pentesting iPhone Application



Pentesting iPhone Application

- Custom Protocols
  - — Identify the communication protocol,
    - ➢ On SSH terminal
      > tcpdump -w traffic.pcap
    - ➢ Loading .pcap in wireshark and analyze
- May not respect iPhone proxy settings .
- DNS Spoofing techniques to MITM

Pentesting iPhone Application

- Privacy Issues
  - Every iPhone has an unique device identifier called UDID
  - Application may collect device UDID.
  - With UDID
    - Maybe observe user`s browsing pattern
    - Determine user`s geographical position.
    - …
- Such as
  - Openfient : Mobile social game nets

  http://corte.si/posts/security/openfeint-udid-deanonymization/
- Observe the network traffic to find out UDID transmission.

Pentesting iPhone Application

- Application data storage
  - 76% of mobile applications store data on their phones
  - 10% of mobile applications store data transmitted on IP network.
  - The Reason for storing data on their phones
    - For the purpose of achieving better performance.
    - Access Offline

- Data storage location
  a) Plist file
  b) Keychain
  c) Logs
  d) Screenshot
  e) Home catalogue

Pentesting iPhone Application

- Application directory structure
  - Applications run in a sandbox of “mobile” ermission.
  - Each application get a private space of file system.

路径	说明
Appname.app	Contains the application code and static data
Documents	Data that may be shared with desktop through iTunes
Library	Application support files
Library/Preferences	App specific preferences
Library/Caches/	Data that should persist across successive launches of the application but not needed to be backed up
tmp	Temporary files that do not need to persist across successive launches of the application

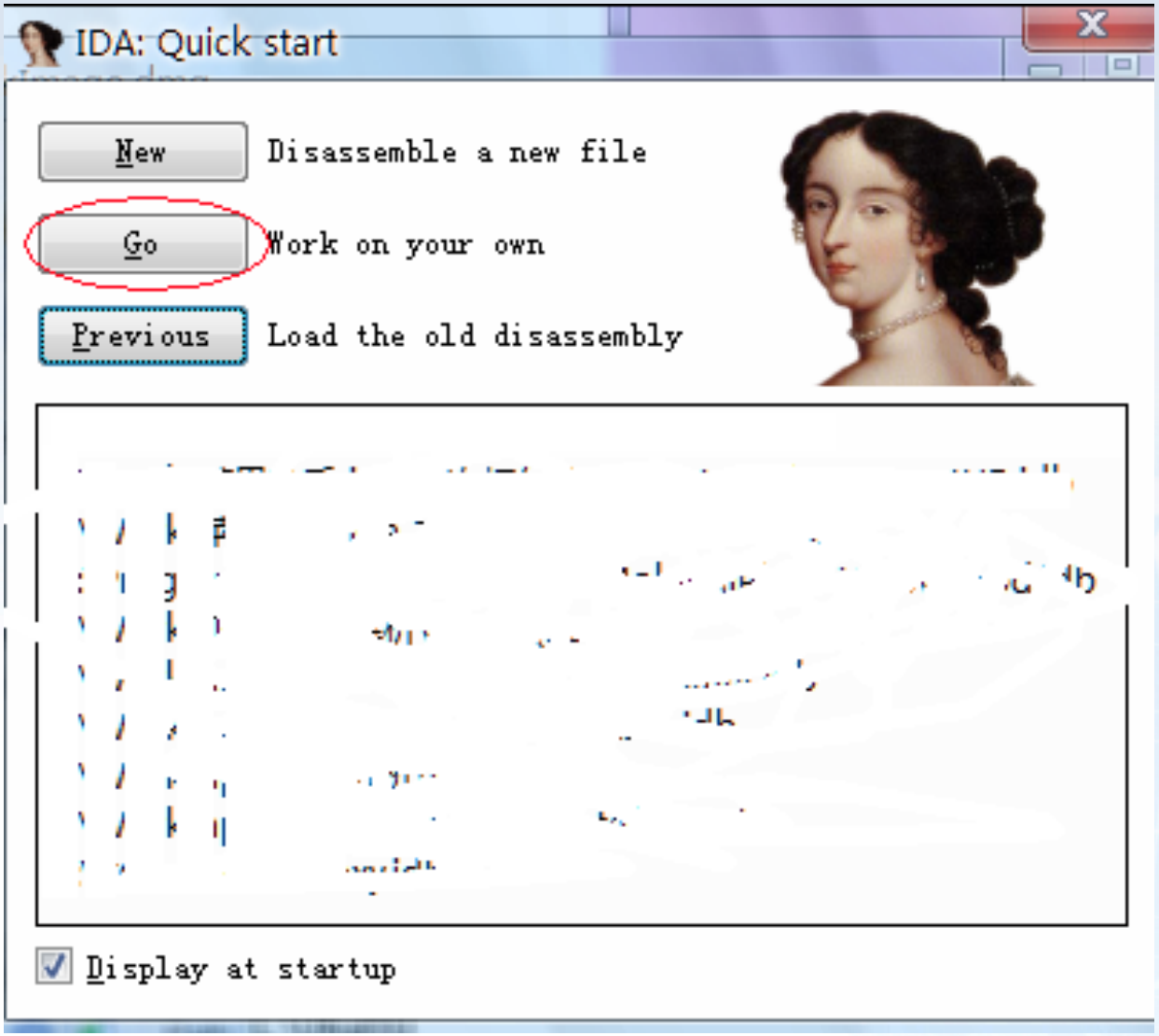
Pentesting iPhone Application

- Reverse Engineering
  - Static analysis
    - Otool
    - Class-dump
  - Dynamic debugging
    - gdb
    - **IDA + GDBServer**

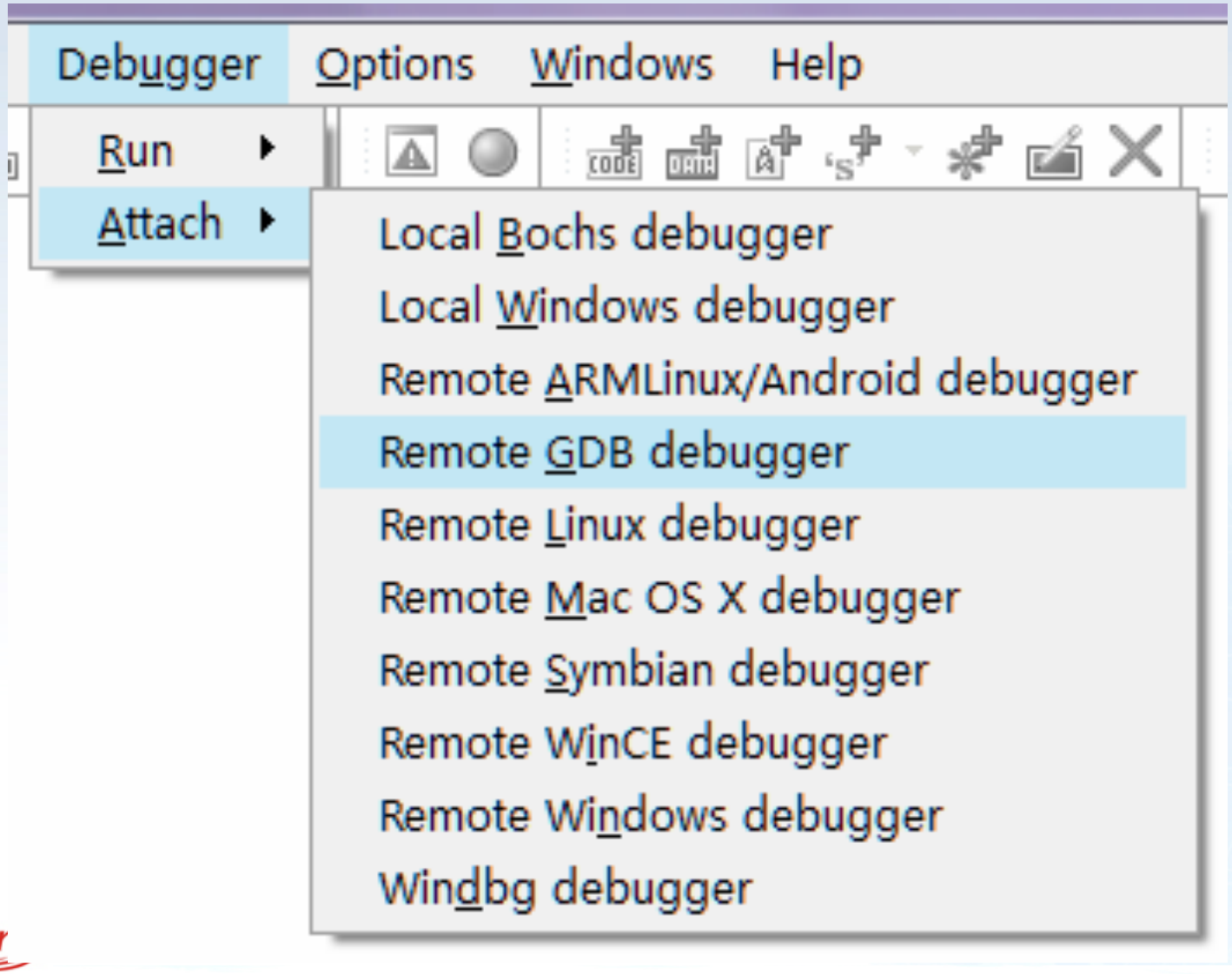
```
xterm-color — zsh — zsh — 80×40
`—> otool -f CodeCards.app/CodeCards                    [0]
Fat headers
fat_magic 0xcafebabe
nfat_arch 2
architecture 0
    cputype 12
    cpusubtype 6
    capabilities 0x0
    offset 4096
    size 89888
    align 2^12 (4096)
architecture 1
    cputype 12
    cpusubtype 9
    capabilities 0x0
    offset 94208
    size 93936
    align 2^12 (4096)
```

```
Milkmixs-iPhone: root# gdb --quiet CodeCards
(gdb) b *0x2000
Breakpoint 1 at 0x2000
(gdb) x /10i 0x2000
0x2000: cmnne   r9, #3604480    ; 0x370000
0x2004: strbgt  r2, [r8, #-125]
0x2008: adclt   r7, r0, #153    ; 0x99
0x200c: ldrbcc  r2, [r5, -r6, lsl #17]
0x2010: tst     r5, #159744     ; 0x27000
0x2014: subsmi  pc, r6, #8960   ; 0x2300
0x2018: stc     9, cr0, [r8, #424]!
0x201c: cfstr64pl       mvdx15, [r9], #168
0x2020: strtls  r12, [sp], #-3417
0x2024: mvnsle  r9, #4653056    ; 0x470000
(gdb) r
...
```

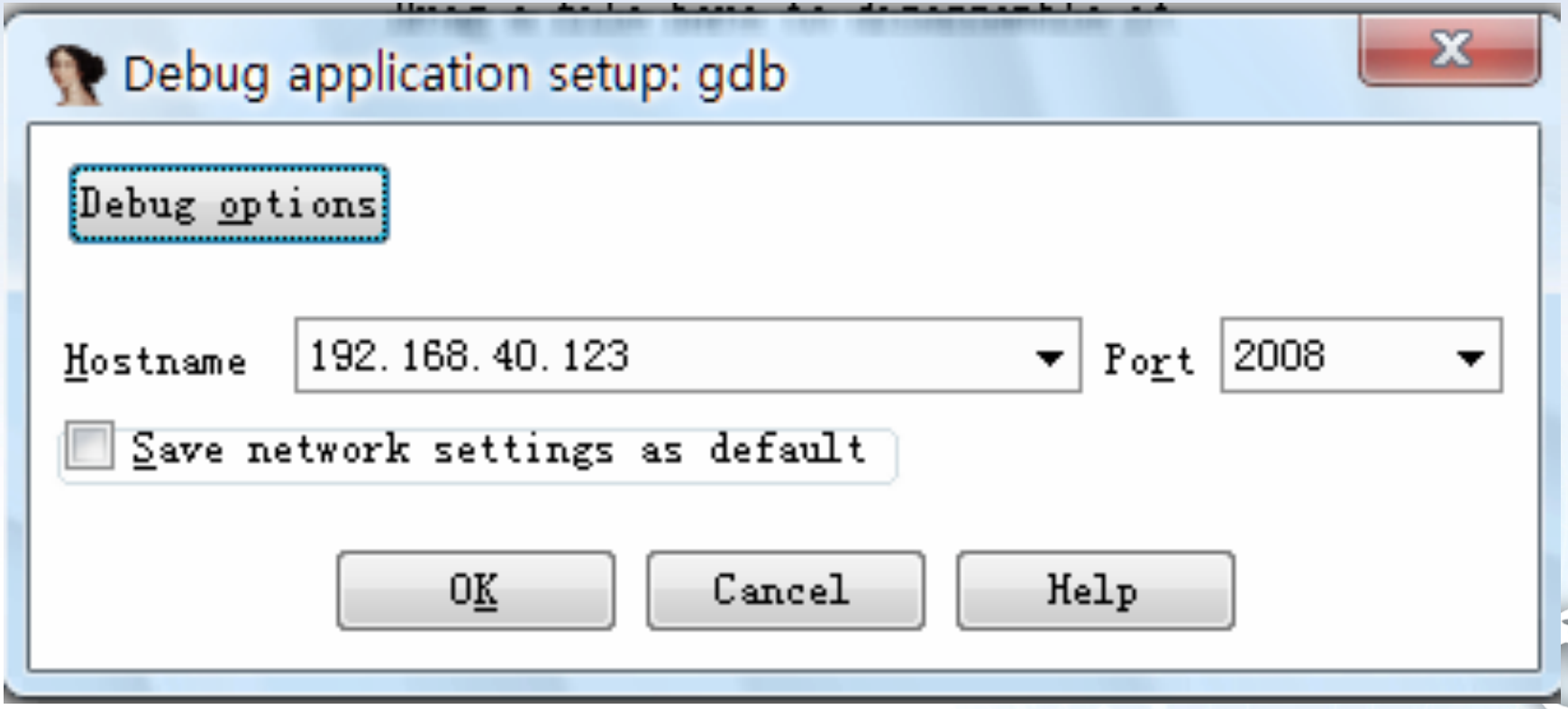
Pentesting iPhone Application



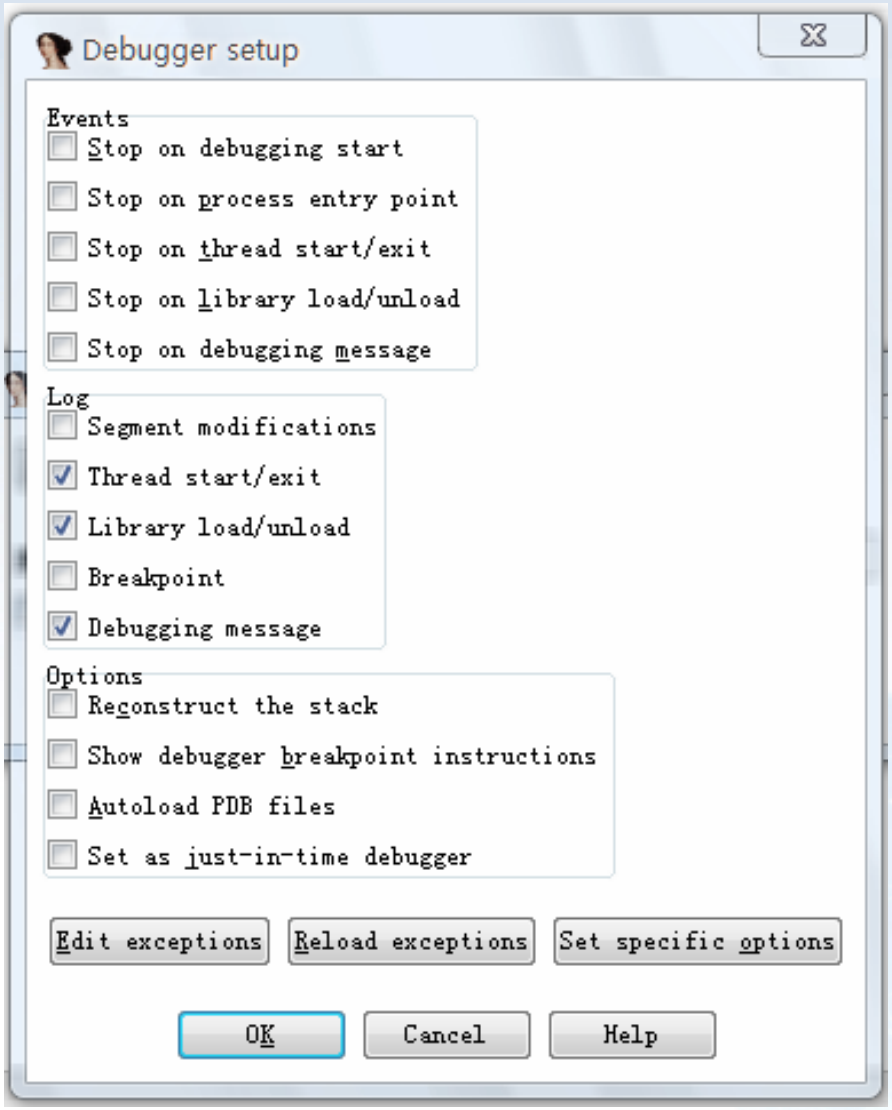
Pentesting iPhone Application



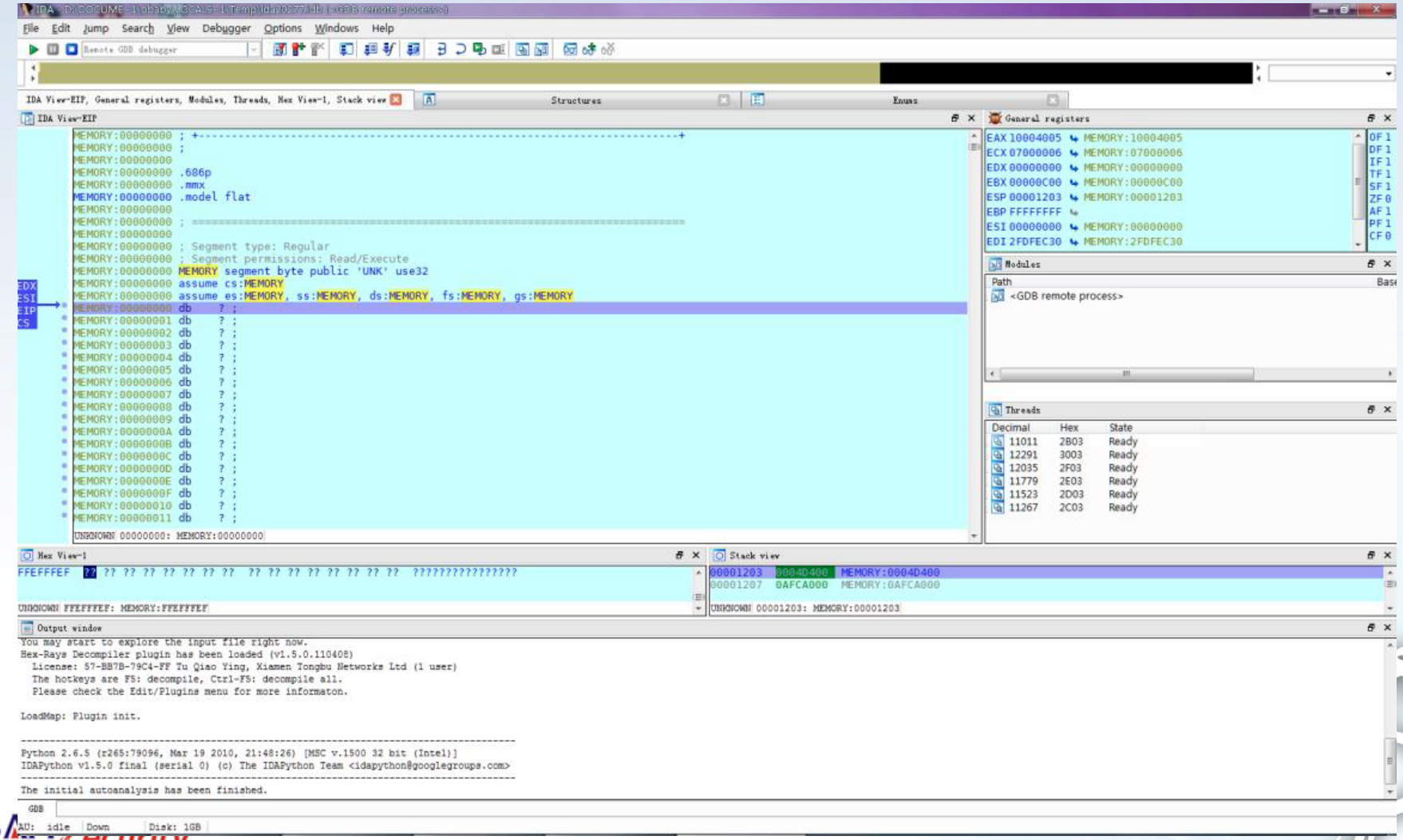
Pentesting iPhone Application



Pentesting iPhone Application



Pentesting iPhone Application



catalog

- iPhone&Adriod Application Basics
- Pentesting iPhone Application
- Pentesting Andriod Application
- Major Mobile Threats

Andriod Systerm Security Feature

- Andriod is based on Linux, which own its security feature.
- Process rights management separation, Andriod starts up application with separate account to doing. Each application uses different accounts, it is more effective and safer.
- Data directory permissions separation, the program data catalogue owners are exactly process users, each process is different, the process directory permissions are seperate, malicious processes can't directly modifiy other process documents.

Andriod Systerm Security Feature

- The application runs in the modified Java environment. It is difficult to attack application by overflowing.
- By default, the application cannot obtain root for changing key position of operating system.

Pentesting Andriod Application

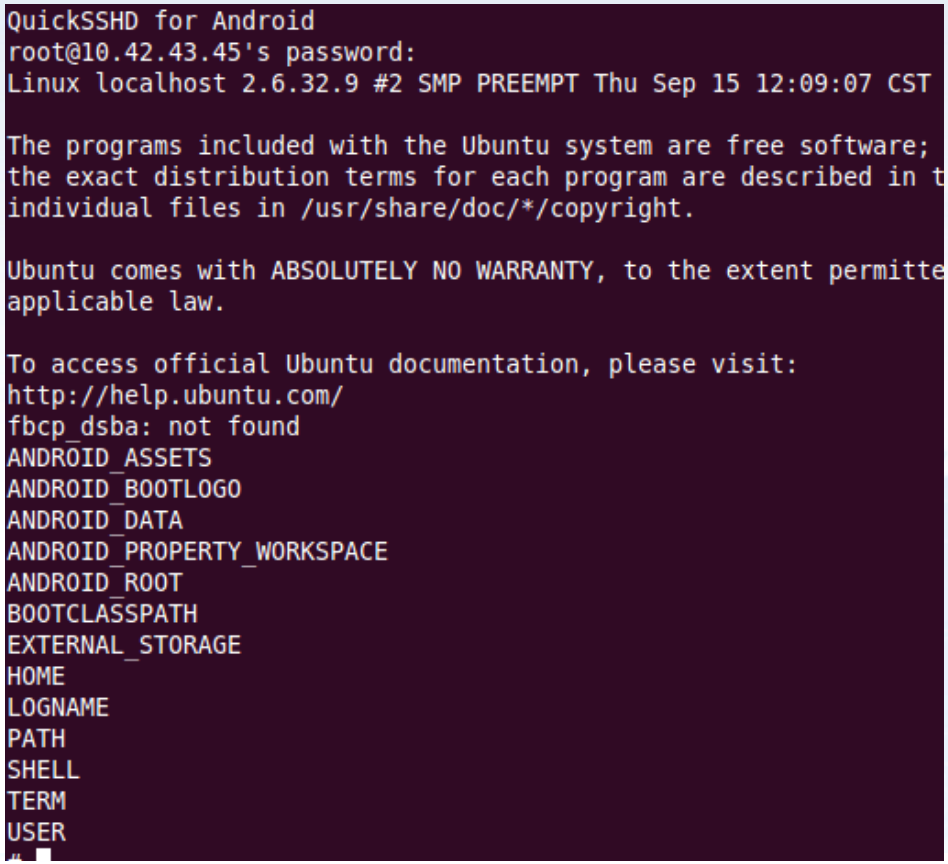
- Highlights Include
  - Attacking test based systerm
  - Attacking test based application
  - Attacking test based transmission link
  - Attacking test based wap site

Pentesting Andriod Application

- To build a test environment
  - Root device
  - To obtain root ermission with root application program . (Local overflow program)
    - Install busybox (include all kinds of useful system commands)
    - Install rights management program,such as ,Superuser
  - Instal ssh server
    - Instal QuickSSHd
    - To get root permission by Superuser

Pentesting Andriod Application

- To build a test environment
  - To build a wireless link with device .
  - By QuickSSHd login into and manage equipment.



Pentesting Andriod Application

- Attacking test based core

  — Andirod is designed and developed based on linux core .Meanwhile, retaining all kinds of linux core features,likewise ,the way of attack linux core is also true for android system.

- Based on the core modules installed the rootkit, Linux core level by reforming the rootkit is easy to run in andriod system, and finish all kinds of the underlying operations.
- Using the development environment to compile corresponding version rootkit module.
- Using command insmod xxx.ko to install module and carry out backdoor function.

Pentesting Andriod Application

- Attacking test based on core
  - Kernel overflow attack

    Andriod kernel based on C language development, there may be exist overflow vulnerabilities, through the spill that based on the kernel malware programs with the highest permission of the system, the part of the program is to use the principle to operate.

Pentesting Andriod Application

- Application attack testing

  — Most of Andriod software developmented based on Java, which is difficult to overflow attack. But part of the program to improve efficiency or to achieve more advanced functions with developing dynamic module in C/C++, which is easy to overflow attacking.

  — Though compared with traditional PC software, Andriod software`s function relatively simple, but it still there may be all kinds of logic security vulnerabilities。

  — Andriod use the default sqlite as a application database, but usually not for encryption, so part of the sensitive data easy to leak.

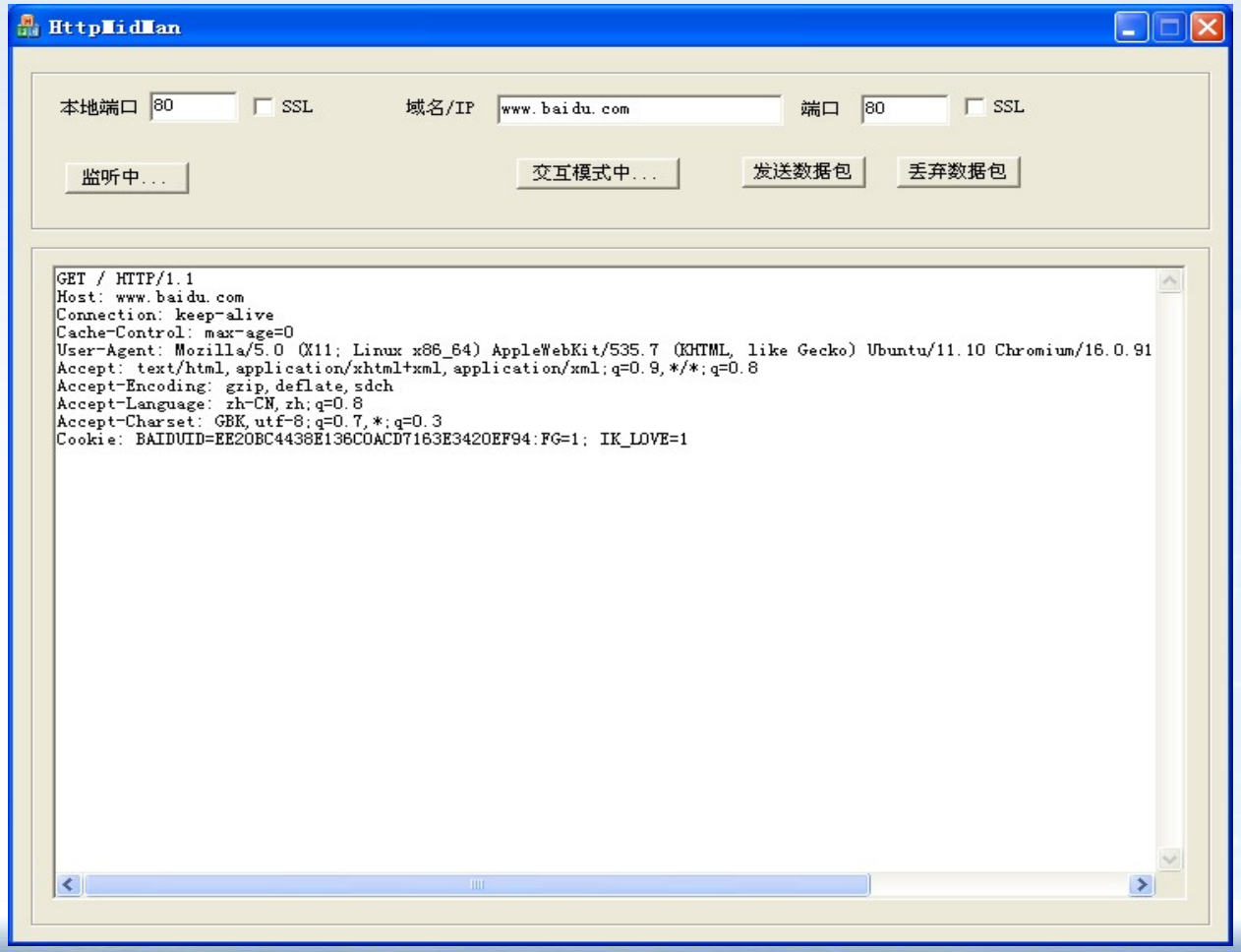
    - Inquiresing the contents of sqlite database with sqlite3。Andriod
    - Andriod application developmented with Java, which can get he corresponding source through the way of decompilation。
    - Through the use of dex2jar can programs into a jar file,

Pentesting Andriod Application

- Transmission lines attack testing
  - Considering the low configured phone, some application do not have the data link encryption, and sending all kinds of sensitive data in these unencrypted link。
  - Mobile phone software currently rarely have the function of through the hardware to sign encryption, so it is easy to attack and intercept the packet by intermediaries and modified. In some on-line transactions of applications, the problem is very serious.

Pentesting Andriod Application

- Capturing the application web packets and test after modifying , with man-in-the-middle tool.



Pentesting Andriod Application

- WAP site attack testing
  - Most of wap sites consider to be compatible various kinds mobile phones (Most mobile phone do not support cookie function),put session information into url ,it is easy to make malicious website get session information and illegal log on though the referrer`s attack
  - Set proxy or using man-in-the-middle attack and safety test for target wap site,find and attack wap vulnerability.

catalog

- iPhone&Adriod Application Basics
- Pentesting iPhone Application
- Pentesting Andriod Application
- Major Mobile Threats

Major Mobile Threats

- It is easy to lost mobile phone .
  - Equipment and password protection
  - Sensitive files encryption
- When reboot the mobile, it only design to encrypt mobile data.
  - Boot Rom exploits
    - All files on devise can copy in 10 minutes.
  - Password brute force
    - 4 digits password has been cracked in 20 minutes
- Mobile App Risks
  - Veracode Top 10
  - OWASP Mobile Top 10

WEB应用安全和数据库安全的领航者！

Thank You !

安恒信息技术有限公司

www.dbappsecurity.com.cn