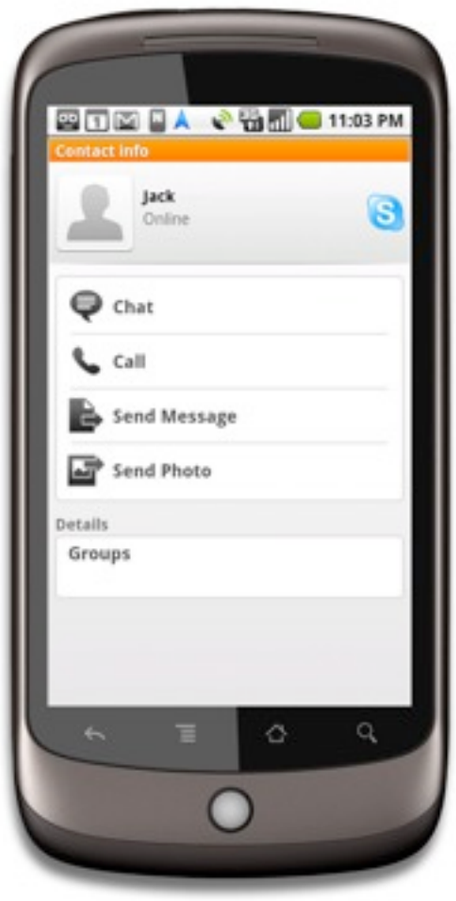
Mobile Application Security

CONVISO
APPLICATION SECURITY

Wagner Elias
CTO
Conviso Application Security
welias@conviso.com.br @welias

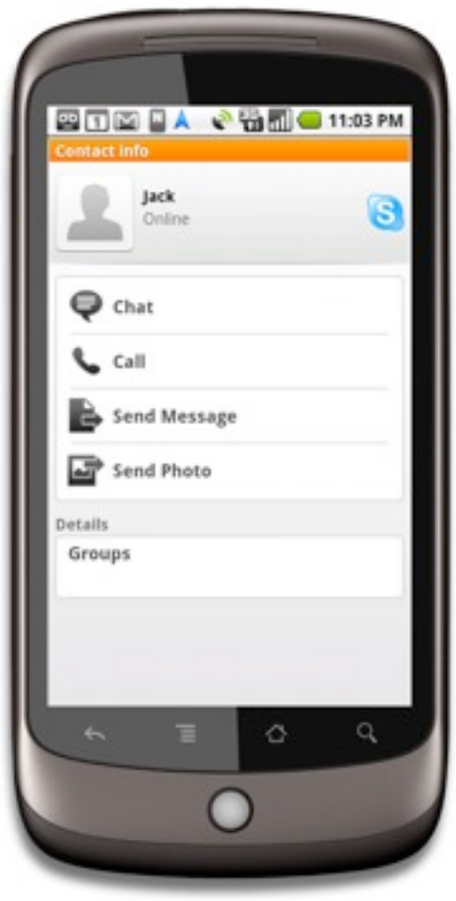
The OWASP Foundation
http://www.owasp.org


5:35 PM
Dropbox
I'm already a Dropbox user
I'm new to Dropbox


11:03 PM
Contact info
Jack
Online
Chat
Call
Send Message
Send Photo
Details
Groups

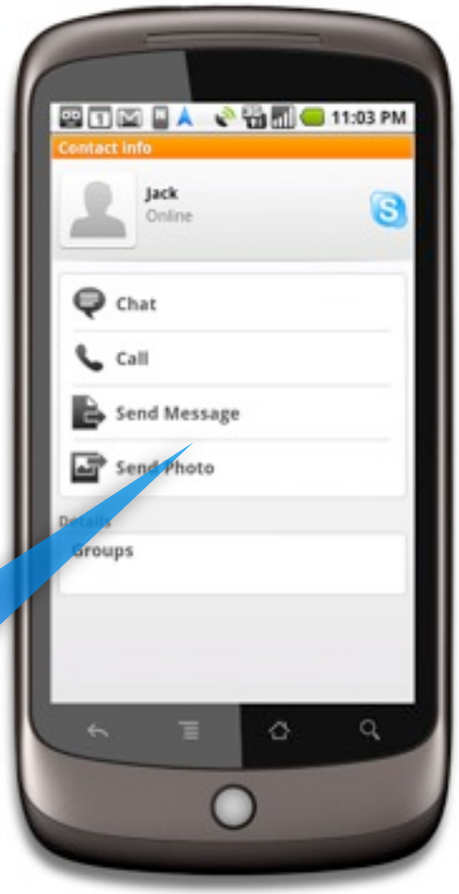

Carrier
12:02 PM
PayPal
$2557.33 USD
Send money
To: George Greeley
Amount: 23.32 USD
Funding: Balance
Thanks for everything!
Cancel
Send
Balance
History
Send Money
Information
Logout

Bypass de Autorização

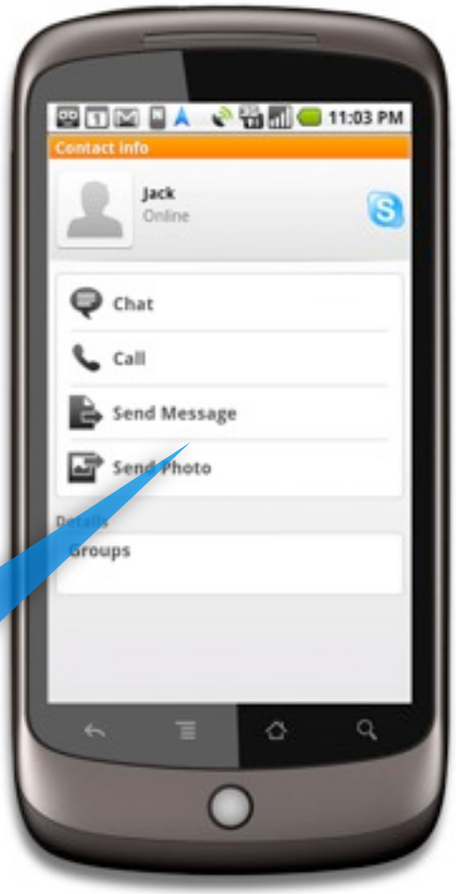


Bypass de Autorização

Vazamento de Informações sensíveis sobre o usuário



Bypass de Autorização



Vazamento de Informações sensíveis sobre o usuário

Possibilitava a interceptação da senha do usuário

Principais Plataformas

- iOS (i(Phone|Pad|Pod))
  - pacote .ipa
- Android
  - pacote .apk
- Existem outras plataformas como: Windows Phone; RIM (Blackberry), mas o foco da apresentação é nas aplicações para iOS e Android

Anatomia de uma aplicação iOS

Sandbox	Aplicações iOS rodam em uma sandbox com permissões mínimas
Data Protection (iPhone 4)	Criptografa e protege os dados do usuário
Keychain	Protege dados sensíveis como senha

Anatomia de uma aplicação Android

Activity	É responsável por tratar os eventos da tela como: clique do botão na tela, escrever um texto dinamicamente na
Service	Similar a uma Activity mas pode ser extendida, possibilitando comunicação entre outros services
Content Provider	Implementa um método de acesso a dados armazenados nos repositórios disponíveis no aparelho
Broadcast Receivers	Criada para receber em segundo plano mensagens (intents) trocadas entre aplicações
Process and Tasks	Por padrão cada aplicação rodando gera um processo no kernel linux

Onde estão as falhas?

- Backend
  - Autenticação e Autorização
  - Elevação de Privilégio
- Client-Side
  - Armazenamento Inseguro
  - Criptografia Mal Implementada
  - Ausência de Validação de Dados
- Comunicação entre o Client e o Server
  - Interpectação de Tráfego

OWASP Top 10 Mobile Risks

1	Inseguro ou desnecessário armazenamento de dados em Client-Side
2	Falta de proteção de dados em trânsito
3	Vazamento de dados pessoais
4	Incapacidade de proteger os recursos com autenticação
5	Incapacidade de implementar o princípio do menor privilégio

OWASP Top 10 Mobile Risks

6	Injeção em Client-Side
7	Negação de Serviços em Client-Side
8	Código de terceiro mal intencionado
9	Buffer Overflow
10	Falha ao implementar controles em Server-Side

Análise Dinâmica

Com a aplicação rodando é análisado o seu comportamento:

- Debugging
- Network Traffic
- Acesso e Comunicação (HTTP/SOAP/Etc...)
- Acesso a File System
- Armazenamento e Leitura de Dados

Análise Estática

Análise onde é feita uma engenharia reversa da aplicação e realizado as seguintes análises

- Source Code Review
- Análise de Strings Hardcoded
- Análise de Armazenamento de Dados
- Análise de Cache

Análise Estática Android

1	Descompactar o pacote .apk usando ferramentas de descompressão de arquivos zip
2	Decodificar os arquivos XML usando o axml2xml.pl
3	Converter arquivos compilados em .dex para bytecode java usando o dex2jar
4	Decompilar código java usando JAD
5	Analisar o código fonte Java

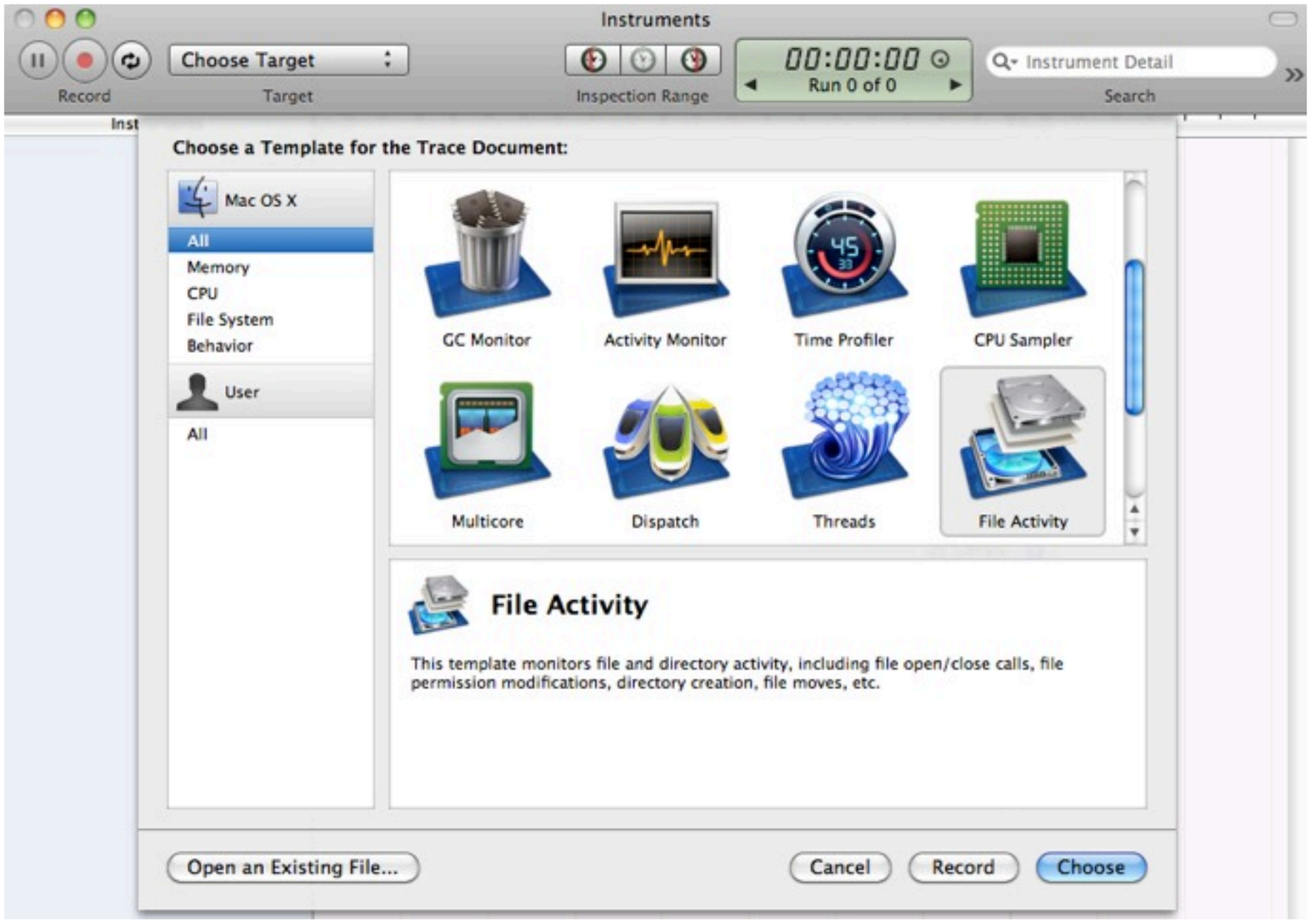
Análise Estática iPhone

1	Decompilar binários compilados em ObjectiveC usando o otool ou class-dump-x
2	Realizar análise estática manual ou automatizada usando Clang

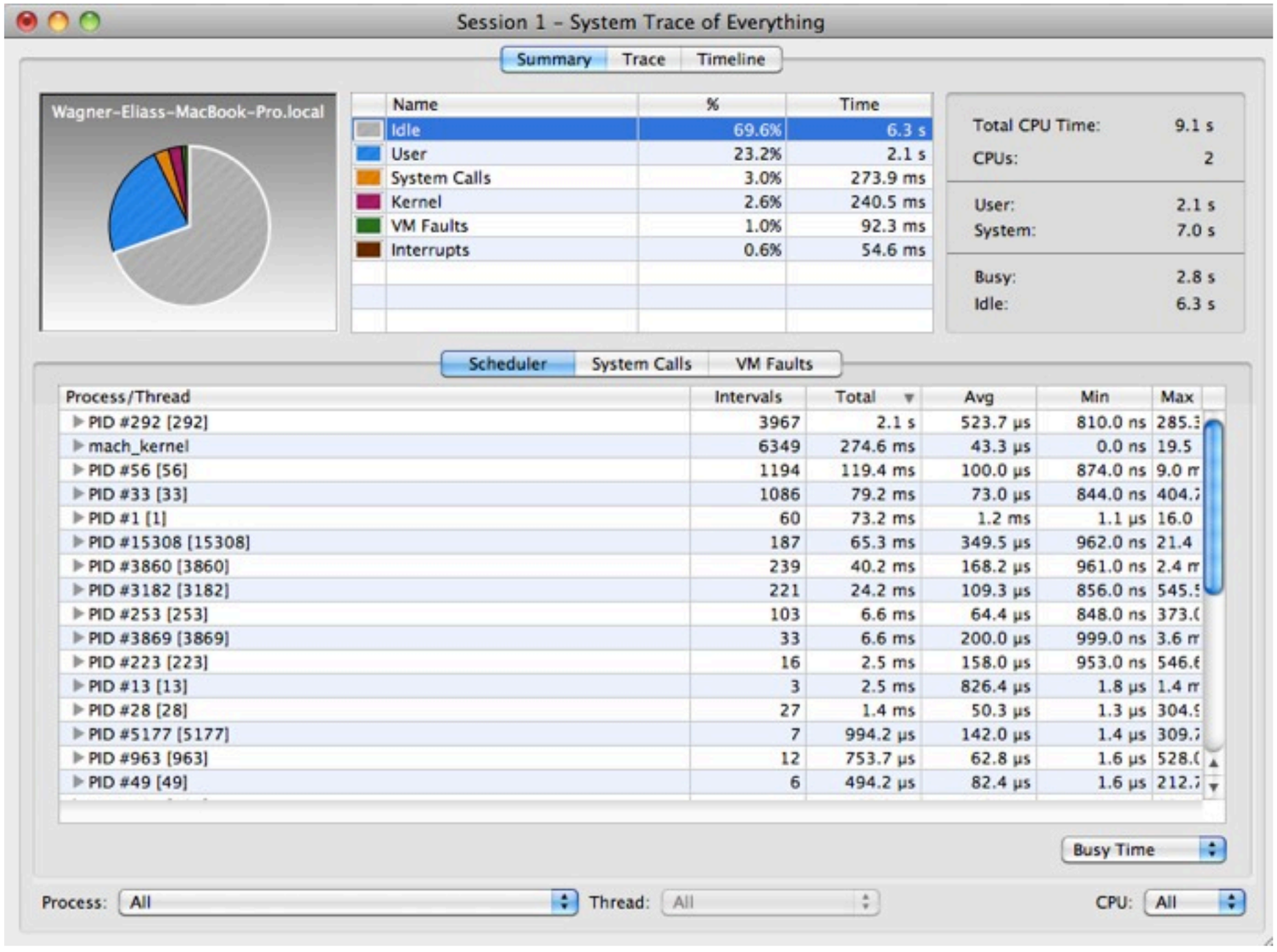
Ferramentas Básicas

- **IDE (Sugestões)**
  - Eclipse para o Android
  - Xcode para o iPhone
- **Emulador**
  - Ambas as plataformas possuem emuladores
- **Client para Database**
  - As duas plataformas armazenam dados locais usando SQLite3

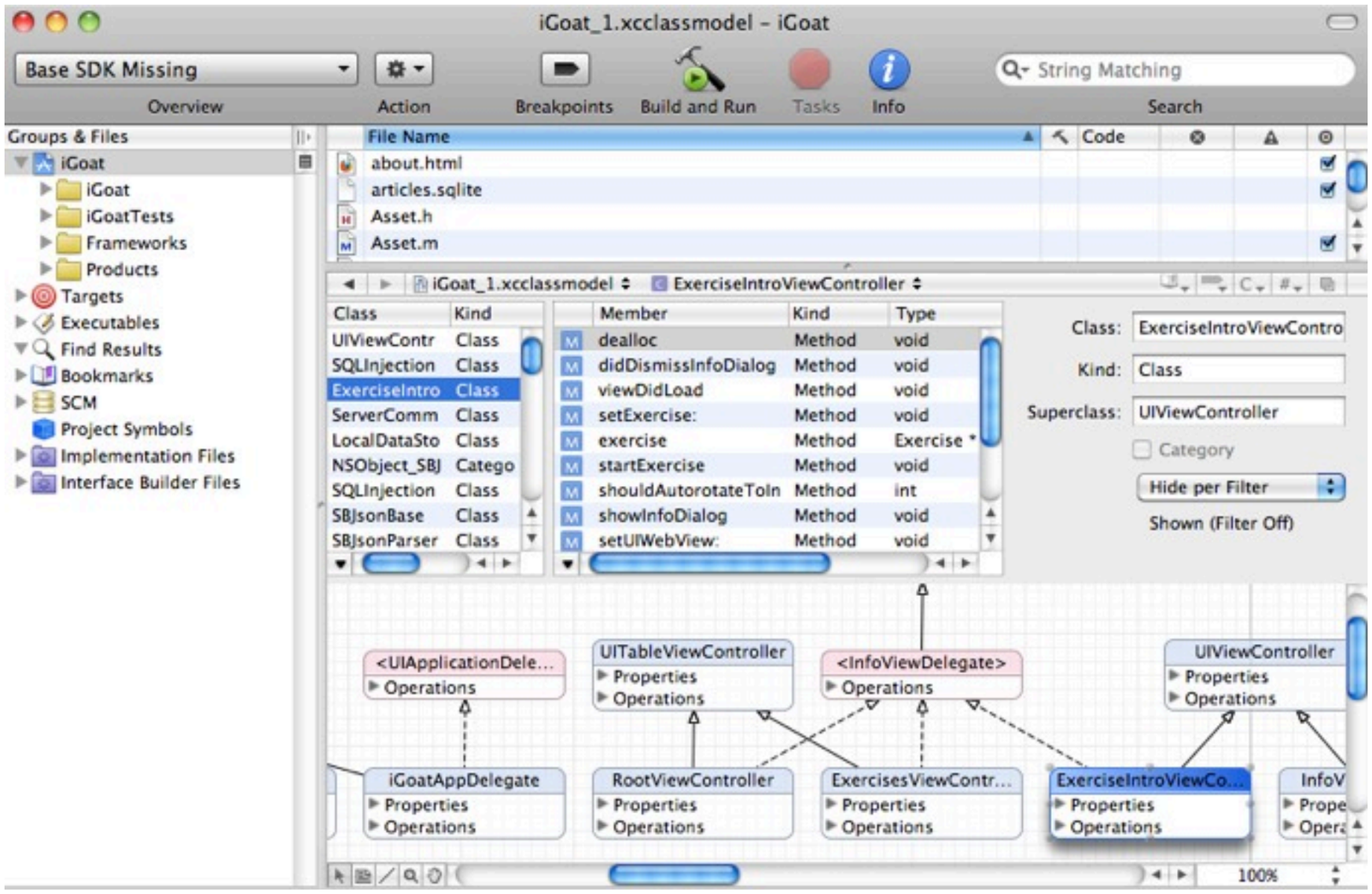
Ferramentas para análise - Instruments



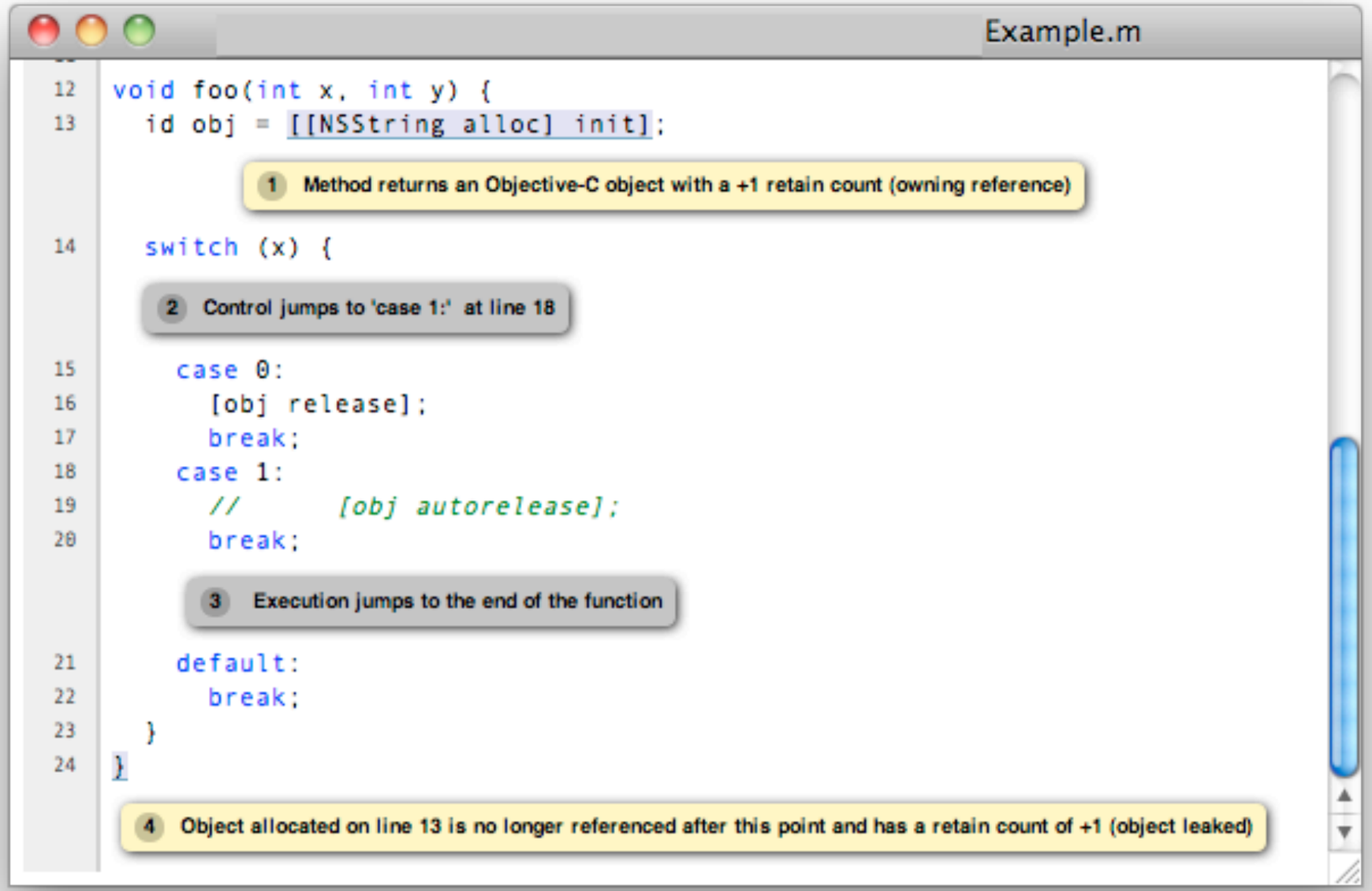
Ferramentas para análise - Shark



Ferramentas para análise - Recursos do Xcode



Ferramentas para análise - Clang



http://clang-analyzer.llvm.org/

Onde praticar?

- OWASP GoatDroid
  - Aplicação Android vulnerável para explorar as principais falhas
    - http://code.google.com/p/owasp-goatdroid/

- OWASP iGoat
  - Aplicação iOS vulnerável para explorar as principais falhas
    - http://code.google.com/p/owasp-igoat/

Obrigado