eXtend Security on Xcode

Tokuji Akamine
Raymund Dante Pedraita
Jun 2014

OWASP
The Open Web Application Security Project

About Us

OWASP
The Open Web Application Security Project

- Who we are
  - Tokuji Akamine @tokujia
    - Lead Security Engineer, Rakuten Inc.

  - Raymund Dante Pedraita (redwud)
    - Senior Security Engineer, Rakuten Inc.

Statistics : iOS Apps

OWASP
The Open Web Application Security Project

- More than 1 million apps on the AppStore
- Users spent $ 10 billion for paid apps
- 3 billion apps were downloaded
- Almost half of all smartphone owners were concerned about privacy
- 90% of iOS mobile apps show security vulnerabilities

References:
http://www.apple.com/pr/library/2014/01/07App-Store-Sales-Top-10-Billion-in-2013.html
http://www.mobilesecurity.com/articles/656-smartphone-users-reveal-mobile-privacy-fears
http://www.zdnet.com/hp-research-finds-vulnerabilities-in-9-of-10-mobile-apps-7000023324/

Statistics : iOS Apps

OWASP
The Open Web Application Security Project

- According to the IOActive's research, many banking apps have security issues
  - 40% of the audited apps did not validate the authenticity of SSL certificates presented.
  - Many of the apps (90%) contained several non-SSL links
  - 50% of the apps are vulnerable to JavaScript injections via insecure UIWebView implementations.

Reference: http://blog.ioactive.com/2014/01/personal-banking-apps-leak-info-through.html

So, what can we use?

OWASP
The Open Web Application Security Project

- Security Awareness and Education
  - OWASP Top 10 Mobile Risks
  - iGoat, DVIA
- Secure Development
  - OWASP Top 10 Mobile Controls
  - iOS Developer Cheat Sheet
  - iMAS
- Security Testing
  - iOS Application Security Testing Cheat Sheet
  - Anything else?

Reference: OWASP Mobile Security Project

Security Testing Tools for iOS Apps

OWASP
The Open Web Application Security Project

- Free Tools
  - Dynamic Analysis Tools, Pen-testing frameworks: iAuditor, iNalyzer, snoop-it, Introspy-iOS
- Commercial Tools
  - Static Security Analysis Tools & Service: Veracode, Cxsuite, Fortify, AppScan Source and maybe more …

Motivations

OWASP
The Open Web Application Security Project

- No free security source code analysis tools
- A lot of manual work for security testing
- Can't fully depend on grep and scripts.
- Security coding guideline doesn’t work well by itself
- Introduce an early detection tool

Xcode Plug-in

OWASP
The Open Web Application Security Project

- We extend security on Xcode with our plug-in
  - Centralize developer-friendly security features on the IDE
  - Provide a solution to avoid making vulnerabilities
  - Detect vulnerabilities at earlier phases of development
  - Cut down the cost of manual security testing

Intro to Xcode plug-in development

OWASP
The Open Web Application Security Project

- Choose “Bundle” as a template and “Cocoa” as a Framework
- Configure build settings

  (XCGCReady, XCPluginHasUI, XC4Compatible, Deployment Location, Wrapper Extension, etc.)
- Create a Class
- Build
- Re-launch Xcode

Xcode plug-in development continues …

OWASP
The Open Web Application Security Project

- Internal Frameworks
  - IDEKit, IDEFoundation
    /Applications/Xcode.app/Contents/Frameworks/
  - DVTKit, DVTFoundation
    /Applications/Xcode.app/Contents/SharedFrameworks/
  - IDESourceEditor, IDEQuickHelp, Xcode3UI, etc.
    /Applications/Xcode.app/Contents/PlugIns/
  - DevToolsCore, etc.
    /Applications/Xcode.app/Contents/OtherFrameworks/
  - WebKit, etc.
    /Applications/Xcode.app/Developer/Platforms/MacOSX.platform/Developer/SDKs/MacOSX[ver].sdk/System/Library/Frameworks/

Xcode plug-in development continues …

OWASP
The Open Web Application Security Project

- Obtain internal class information with class-dump to look for useful Class, Methods, Properties

```
@interface IDESourceCodeEditor : IDEEditor <NSTextViewDelegate, NSMenuDelegate, NSPopoverDelegate
…>
…
+ (id)keyPathsForValuesAffectingIsWorkspaceBuilding;
+ (void)revertStateWithDictionary:(id)arg1 withSourceTextView:(id)arg2 withEditorDocument:(id)arg3;
+ (void)commitStateToDictionary:(id)arg1 withSourceTextView:(id)arg2;
+ (long long)version;
+ (void)configureStateSavingObjectPersistenceByName:(id)arg1;
@property(retain) IDESingleFileProcessingToolbarController *singleFileProcessingToolbarController; // …
@property(retain) IDEAnalyzerResultsExplorer *analyzerResultsExplorer; // …
@property(retain, nonatomic) DVTSourceExpression *mouseOverExpression; // …
@property(retain) IDESourceCodeEditorContainerView *containerView; // …
@property(retain) DVTSourceTextView *textView; // …
…
```

Available Xcode Plug-ins

OWASP
The Open Web Application Security Project

- XVim
- Injection
- BBUncrustifyPlugin
- Xcode Fixins
- XcodeColors
- OMColorSense
- KSImageNamed-Xcode
- XcodeExplorer

etc.

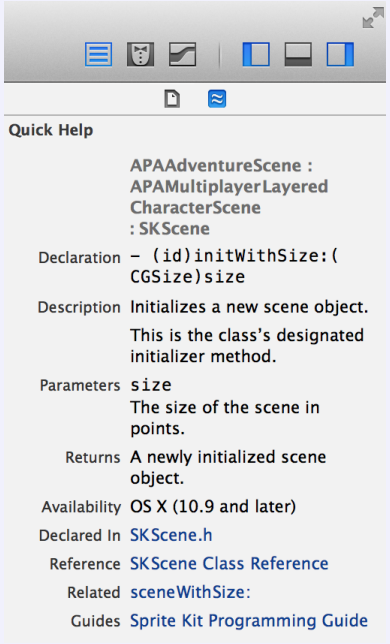
OWASP
The Open Web Application Security Project

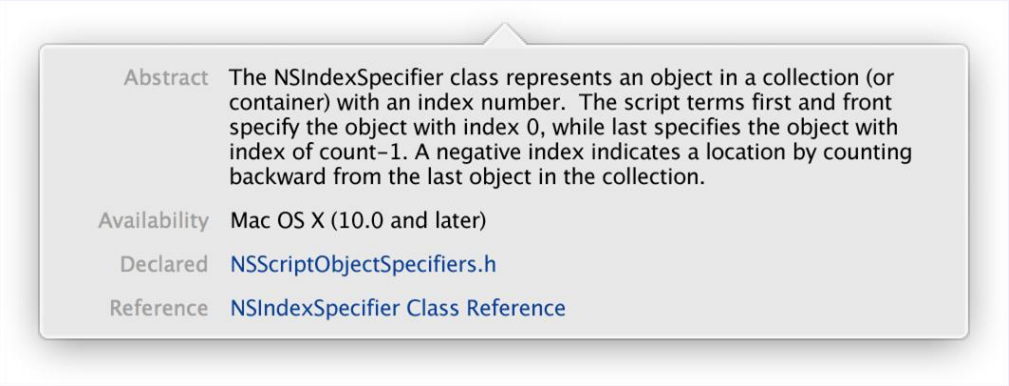
- XSecurity
  - Quick Security Help with built-in Security Guidelines
  - Real-time Vulnerability Notifications
  - Static Analysis with Clang Static Analyzer

Feature 1: Quick Security Help

OWASP
The Open Web Application Security Project

- Quick Help
  - Display concise reference documentation without taking focus away from the file you're editing.





Feature 1: Quick Security Help

OWASP
The Open Web Application Security Project

- Quick Security Help
  - Add security guidelines in reference documentation.
  - Added to both Quick Help Inspector and the Quick Help Window
  - Can automatically display and hide the inspector area.

Feature 2: Real-time Vulnerability Notifications

OWASP
The Open Web Application Security Project

- Real-time Vulnerability Notifications
  - Show the vulnerability as it is being created.
  - Instant bug know-how to developers.
  - Early prevention.

Feature 2: Real-time Vulnerability Notifications

OWASP
The Open Web Application Security Project

- Detection Triggers
  - When the source is modified.
  - When switching between source files.
- Methodology
  - Research parts of Xcode, how it works.
  - Categorize vulnerabilities according to characteristics.
  - Heavy use of RegEx

Feature 3: Clang Static Security Analyzer

OWASP
The Open Web Application Security Project

- Clang
  - A compiler front-end for C family of languages
  - It uses LLVM as its back end
  - Creates an abstract syntax tree (AST) of the code
  - LLVM Community (Supported by professionals from Apple, Google, ARM, Intel, etc.)

Feature 3: Clang Static Security Analyzer

OWASP
The Open Web Application Security Project

- Clang Static Analyzer
  - A source code analysis tool that can find bugs in C, C++ and Objective-C programs.
  - Can run from CLI and within Xcode
  - 100% open source and part of Clang project

- Alternative static code analysis tool: OCLint

Feature 3: Clang Static Security Analyzer

OWASP
The Open Web Application Security Project

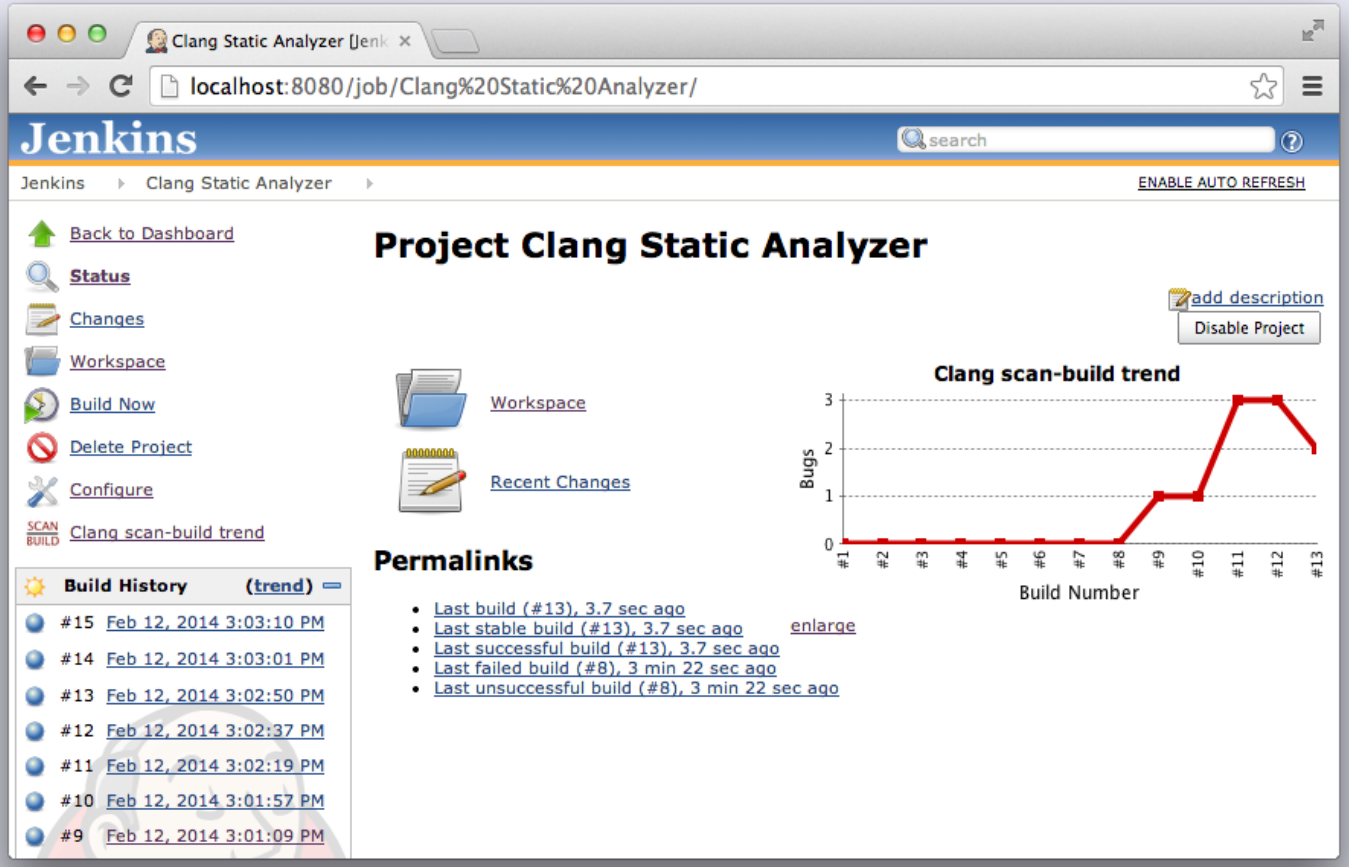
- It boils down to checkers
  - Static analyzer engine can do path-sensitive exploration of the program.
  - Checkers implement the logic for bug detection
  - And, construct bug reports.
  - Documentation can get you started

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

Feature 3: Clang Static Security Analyzer

OWASP
The Open Web Application Security Project

- CI with Security Checkers



Detectable Vulnerabilities

OWASP
The Open Web Application Security Project

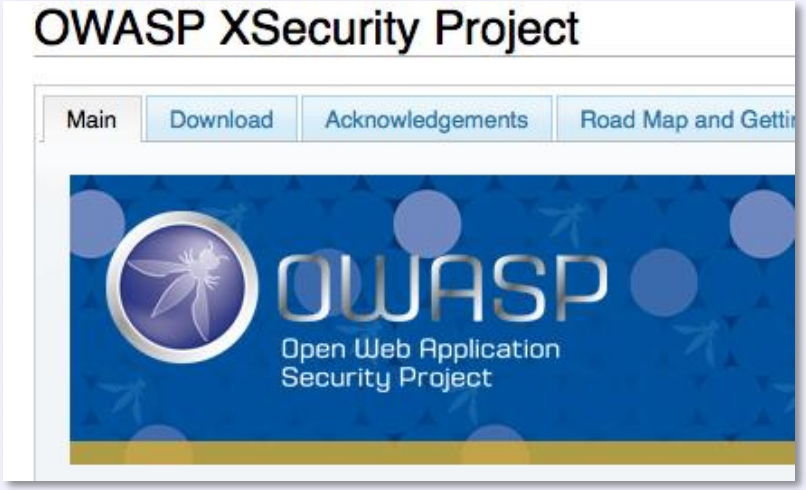
Category	Vulnerability	Real-time	Checker
Insecure Data Storage	Insecure Keychain Storage	●	●
	Insecure NSUserDefaults Usage	●	●
	Unencrypted Data in plist File		●
	Insecure Permanent Credential Storage	●	●
Insufficient Transport Layer Security	Ignores Certificate Validation Errors	●	●
Security Decisions Via Untrusted Inputs	Abusing URL Schemes	●	●
Side Channel Data Leakage	Leaking Web Caches		●
	Leaking Logs	●	●
	Leaking Pasteboard		●
Client Side Injection	SQL Injection (SQLite)		●

XSecurity Project

OWASP
The Open Web Application Security Project

- XSecurity Project

  https://www.owasp.org/index.php/OWASP_XSecurity_Project



  https://github.com/XSecurity/

  @prj_xsecurity

Future Plans

OWASP
The Open Web Application Security Project

- We aim to…
  - Make configurations flexible or customizable guideline in Quick Security Help
  - Rule selection and improve reporting functionalities
  - Develop more rules for real-time notifications and checkers
  - Support Xcode 6.0+ and Swift ? (if possible)

Next vulnerabilities

OWASP
The Open Web Application Security Project

Category	Vulnerability
Insufficient Transport Layer Security	Data Transport Over Unencrypted Channel
	Query String for Sensitive Data
	Certificate Unpinning
Sensitive Information Disclosure	Hard Coded Sensitive Information
	Query String for Sensitive Data
Broken Cryptography	Use Vulnerable Encryption Algorithms
Poor Authorization & Authentication	Invalid Usage of Persistent Identifier
	Insecure OAuth implementation
Client Side Injection	Cross Site Scripting

Questions?

OWASP
The Open Web Application Security Project

- References
  - OWASP Mobile Security Project
  - Mac Developer Library
  - The LLVM project
  - OCLint
  - Clang Scan-Build Jenkins Plugin

OWASP
The Open Web Application Security Project

Thank you

Salamat

Arigatou Gozaimasu