Orange Applications for Business

CocoaHeads Lyon

09/03/2017

CocoaHeads – partie 1

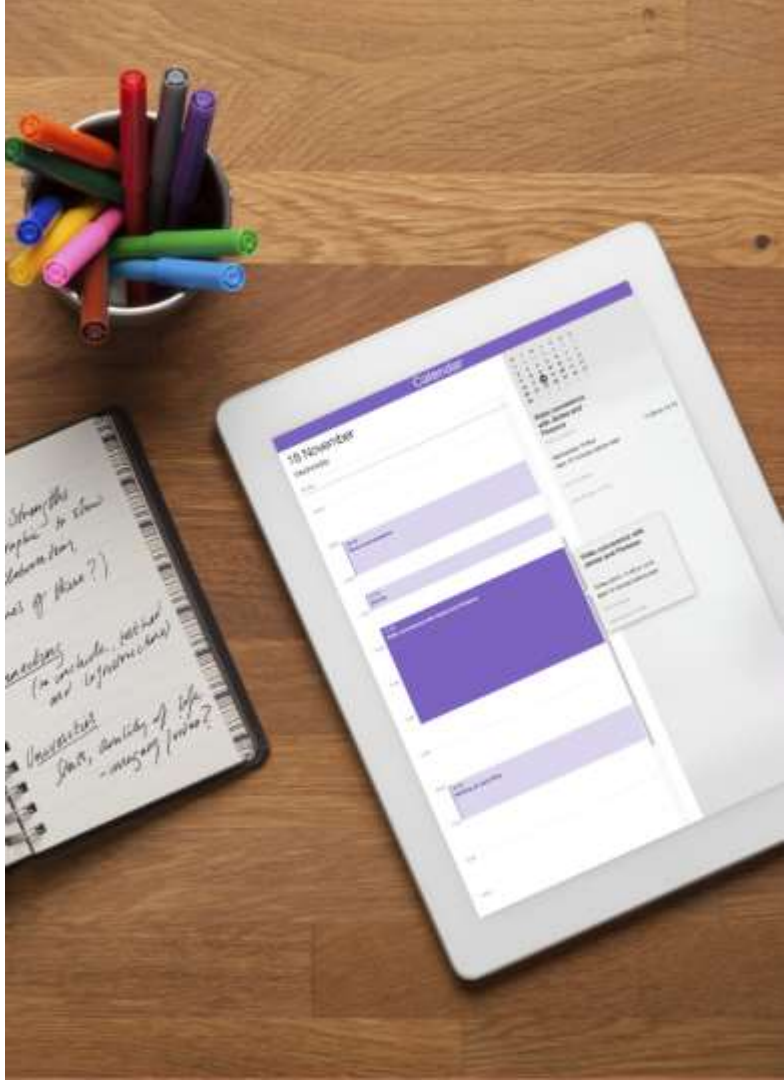
mars 2017

la sécurité sur iOS

la sécurité sur iOS

sommaire

1. enjeux de la sécurité
2. organismes
3. top 10 OWASP Mobile 2017
4. sécurité au cœur du projet
5. conclusion



la sécurité sur iOS

enjeux de la sécurité – c'est quoi ?

la sécurité informatique, c'est quoi ?

- confidentialité : éviter les intrusions
- intégrité : protéger contre les données modifiées
- disponibilité : garantir le fonctionnement contre les pannes

quoi d'autre?

- traçabilité : toute action est tracée
- authentification : l'utilisateur est identifié
- non-répudiation et imputation : non contestation des actions d'un utilisateur

la sécurité sur iOS

enjeux de la sécurité – pourquoi ?

Dommages financiers

- directs : Rétablir le parc de machine, réécrire l'application, etc…
- indirects : Vol de secret industriel, perte de marchés

Image de marque

- directe : Publicité négative sur l'insuffisance de la sécurité
- indirecte : Perte de la confiance du public

la sécurité sur iOS

enjeux de la sécurité

A qui faire confiance ?

la sécurité sur iOS

organismes

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

- Création le 7 juillet 2009
- Rattachée au Secrétaire général de la défense et de la sécurité nationale
- L'agence assure la mission d'autorité nationale en matière de sécurité des systèmes d'information
- Guides et recommandations
- Formation à la sécurité

➔ http://www.ssi.gouv.fr

la sécurité sur iOS

organismes

MITRE : Massachusetts Institute of Technology Research & Engineering

- Entreprise à but non lucratif
- Création en 1958
- Sponsorisé par le département de la défense américain
- Centralise les CVEs
- Développe le format de rapport OVAL
- Formation à la sécurité

➔ https://cve.mitre.org/

la sécurité sur iOS

organismes

OWASP : Open Web Application Security Project

- Entreprise à but non lucratif
- Création le 9 septembre 2001
- Communauté de développeurs diffusant les bonnes pratiques de sécurité pour les applications web
- Connu pour le Top 10 des failles (mobile, web, …)
- WebGoat, WebScarab, XSS Filter, …
- Domaine étendu au développement mobile

➔ https://www.owasp.org

la sécurité sur iOS

top 10 OWASP

M1 – Mauvaise usage de la plateforme

M2 – Stockage de données non sécurisées

M3 – Communication non sécurisé

M4 – Authentification non sécurisée

M5 – Casse cryptographique

M6 – Autorisations non sécurisées

M7 – Qualité du code client

M8 – Code tampering

M9 – Reverse engineering

M10 – Fonctionnalités non nécessaires

la sécurité sur iOS

organismes

Quelle stratégie ?

la sécurité sur iOS

architecture du projet

Prendre en compte les problématiques de sécurité dès le lancement d'un projet

- ISO 27001 ou EBIOS
- identifier les vulnérabilités
- identifier les responsables sécurité
- prendre en compte les recommandations
- programmer un audit

la sécurité sur iOS

respect des règles de Secure-Coding

Connaître les règles de secure-coding inhérent au projet à réaliser

- Guide du secure coding sur iOS/Mac OSX d'Apple
- Guide du secure coding iOS de l'Infosec Institute
- OWASP
- Mettre en place des outils d’analyse automatique
- Faire de la revue de code

la sécurité sur iOS

outils d'Intégration Continue

Définir les outils en fonction des développements, par exemple :

- SonarQube
- dependency-check d'OWASP (Java, .Net, Ruby, PHP et NodeJS)
- Lint (C), SwiftLint (Swift) JavaScriptLint (JavaScript)
- Clang (C/C++/Objective-C)
- Klockwork (C/C++, Java), utilisé surtout dans l'industriel

NB :

- Aucun outil ne garantit 100% de couverture
- Difficulté de combiner un ensemble d'outils

la sécurité sur iOS

tests de pénétration

- Coût important car difficilement automatisable
- Nécessite une expertise en sécurité et divers technologies
- Kali Linux, anciennement BackTrack

la sécurité sur iOS

tests de pénétration

Possibilités d'automatisation :

- Injection SQL
- Données réseau en clair (ex: données client en HTTP)
- Détection partielle XSS

Exemples de tests de pénétration :

- Déchiffrer des données dans un mobile
- Corrompre une application web
- Récupérer des données clients

la sécurité sur iOS

conclusion

- anticiper les coûts associés

- adapter la sécurité en fonction du type de projet
- formation / auto-formation sur le Secure-Coding

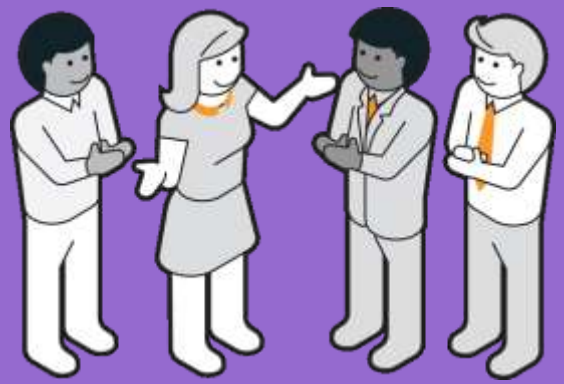
- mise en place d'outils automatisés

CocoaHeads – partie 2

mars 2017

objective-C / Swift

débat



Objective-C / Swift

débat

danke schön

merci

gracias

grazie

merci

shukrān

Thank you

ta