Sécurité des applications mobiles

Acquérir des mécanismes de sécurisation d'applications mobiles

DESCRIPTION

Une part sans cesse croissante du trafic internet est effectuée aujourd'hui via les mobiles. Navigation, services de messagerie, achats en ligne, réseaux sociaux ou même encore accès aux applications professionnelles en mobilité, les cas d'usage du smartphone se sont multipliés en quelques années.

Les entreprises comme les particuliers se voient confrontés à de nouveaux risques : attaques logicielles, consultation ou vol de données (etc.). Ainsi, selon le magazine Forbes, 84% des brèches de sécurité exploitent des vulnérabilités au niveau de la couche d'application mobile. C'est pourquoi, il convient d'intégrer pleinement la sécurité au cycle de développement.

Dès lors que votre application mobile devient la vitrine de vos services, une attention particulière doit être portée dès la conception sur la manière avec laquelle elle gère les données, en particulier celles de ses utilisateurs.. . Pendant longtemps, l'attention a été portée à la sécurisation des appels aux web services. Mais comme le montre l'évolution des recommandations définies par la communauté OWASP, il est tout aussi important de considérer les risques propres aux smartphones.

S'il est difficile de se prémunir de tous les cas de figure, une connaissance et une prise en compte des différentes attaques possibles tout au long de la vie d'un projet peut avoir un grand impact sur la sécurisation de votre application.

Cette formation a pour objectif de proposer des mécanismes de sécurisation d'applications mobiles, en les décrivant de manière théorique, et en les mettant en pratique sur une application iOS et/ou Android.. .

OBJECTIFS PEDAGOGIQUES

- Identifier les différents niveaux d'attaque possibles
- Découvrir les risques pour mieux les anticiper en endossant le rôle de l'attaquant
- Apprendre et mettre en place les mécanismes pour éviter/contrer des attaques et sécuriser les vulnérabilités

PUBLIC CIBLE

- Développeur mobile (iOS et/ou Android)
- Architecte

Stage pratique
Mobile

Code :
MOBSE

Durée :
1 jour(s) (7,00 heures)

Exposés : **20.00 %**
Cas pratiques : **30.00 %**
Echanges d'expérience : **50.00 %**

Inter-entreprises :
Prochaines sessions disponibles sur notre site web.
Tarif : 990,00 € HT / participant

Intra-entreprise :
Tarifs et dates sur demande.

- Chef de projet technique

PRE-REQUIS
Bonnes connaissances des concepts de développement iOS et Android et de leur langages respectifs (Swift, Java ou Kotlin).

METHODE PEDAGOGIQUE
Formation avec apports théoriques, échanges sur les contextes des participants et retours d'expérience du formateur, complétés de travaux pratiques et de mises en situation. Il s'agira notamment de comprendre les différents procédés utilisés pour pirater une application, et ensuite, au cours de la formation, mettre en œuvre les stratégies pour s'en prémunir.

PROFIL DES INTERVENANTS

Cette formation est dispensée par un·e ou plusieurs consultant·es d'OCTO Technology ou de son réseau de partenaires, expert·es reconnus des sujets traités.

Le processus de sélection de nos formateurs et formatrices est exigeant et repose sur une évaluation rigoureuse leurs capacités techniques, de leur expérience professionnelle et de leurs compétences pédagogiques.

MODALITÉS D'ÉVALUATION ET FORMALISATION À L'ISSUE DE LA FORMATION

L'évaluation des acquis se fait tout au long de la session au travers des ateliers et des mises en pratique.

Afin de valider les compétences acquises lors de la formation, un formulaire d'auto-positionnement est envoyé en amont et en aval de celle-ci.

En l'absence de réponse d'un ou plusieurs participants, un temps sera consacré en ouverture de session pour prendre connaissance du positionnement de chaque stagiaire sur les objectifs pédagogiques évalués.

Une évaluation à chaud est également effectuée en fin de session pour mesurer la satisfaction des stagiaires et un certificat de réalisation leur est adressé individuellement.

PROGRAMME PEDAGOGIQUE DETAILLE

Jour 1

INTRODUCTION SUR LES ENJEUX DE LA SÉCURITÉ SUR MOBILE

- PME, startups, grands comptes : des risques propres à chacun
- Définir sa stratégie selon ses besoins

LES DIFFÉRENTES ATTAQUES POSSIBLES SUR UN TÉLÉPHONE VOLÉ

- Récupérer les données d'une application mobile non sécurisée (démonstration).
- Les différents stockages de données en local et comment les sécuriser.
- Le choix des algorithmes de chiffrement.
- Focus iOS : le Keychain
- Focus Android : Keychain - Keystore Provider - AccountManager

ATTAQUES "MAN IN THE MIDDLE"

- Intercepter des appels réseaux non sécurisés (démonstration)
- Livecode : mise en place du TLS pinning
- Focus Android : utilisations de l'API SafetyNet

ATTAQUES SUR LE BINAIRE / LE CODE DE L'APPLICATION

- Décompiler une application Android récupérée sur le store (démonstration).
- Obfusquer le code de son application Android avec Proguard et R8

RISQUES SPÉCIFIQUES À CHAQUE PLATEFORME

- Focus Android : les risques des Intents, des Permissions, et des applications tierces installées sur le téléphone.
- Focus iOS : les risques du Keychain.
- Validations des appels et des données entrantes

RAPPELS DES POINTS CLÉS DE LA FORMATION

Accessibilité

L'inclusion est sujet important pour OCTO Academy.
Nos référent·es sont à votre disposition pour faciliter l'adaptation de votre formation à vos besoins spécifiques.
Pour les contacter : academy.accessibilite@octo.com