RECHERCHE ET EXPLOITATION DE VULNÉRABILITÉS : SUR APPLICATIONS ANDROID

Apprenez les techniques et méthodes utilisées pour découvrir des vulnérabilités sur les applications Android

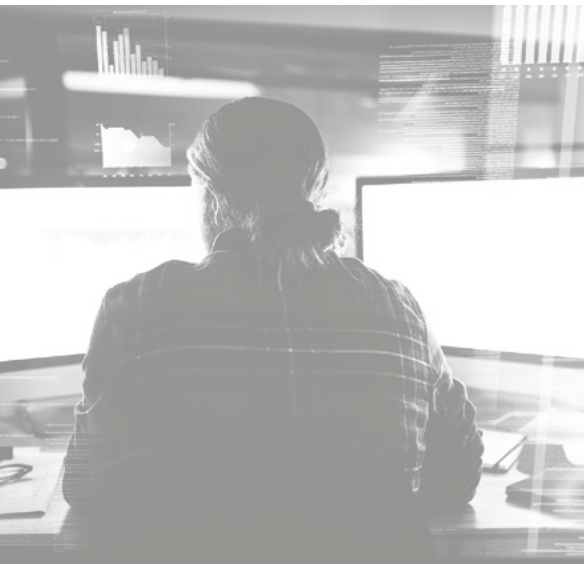
Ce cours vous apprendra à mettre en place une véritable procédure d'audit de type PenTest ou Test d'Intrusion sur une application mobile Android.
Les stagiaires seront plongés dans un cas pratique se rapprochant le plus possible d'une situation réelle d'entreprise.
Vous y étudierez l'organisation et les procédures à respecter lors de la mise en place d'un tel audit, ainsi que les différentes approches possibles lors de l'analyse d'une application Android d'un point de vue sécurité.

Code : REVA

PROGRAMME

Méthodes mobilisées : Cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (70% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences en fin de module par le formateur.



JOUR 1

Introduction au système Android
- Modèle de sécurité d'Android
- Permissions
- Anatomie d'une application
- Manifeste d'application
- Activités et Intents
- Utilisation de Content Providers
- Stockage de fichiers sur carte SD

Présentation des outils d'analyse
- Le SDK Android
- ADB (Android Debug Bridge)
- JADX
- Drozer

JOUR 2

Préparation à l'analyse
- Installation du SDK
- Déploiement d'une autorité de certification sur Burp Suite

Prise d'information
- Découverte de l'activité principale
- Récupération d'informations concernant l'API utilisée
- Récupération d'informations depuis les fichiers de logs

Attaque de l'API
- Cross-Site Scripting
- Injection de code SQL

JOUR 3

Attaque de l'API (suite)
- Isolation de comptes utilisateur
- Chiffrement des communications
- Gestion des sessions

Reverse Engineering
- Analyse statique via JADX
- Récupération des points d'entrée de l'API
- Analyse des algorithmes de chiffrement utilisés
- Emplacement de stockage des données (local, carte SD)
- Type de données stockées
- Mots de passe présents dans le code source
- Utilisation d'intents en broadcast

PROCHAINES DATES

9 mars 2022,
30 mai 2022,
5 sept. 2022,
28 nov. 2022

OBJECTIFS

- Maîtriser les fonctionnalités avancées du système Android
- Organiser une procédure d'audit de sécurité de type test de pénétration sur une application mobile Android
- Se mettre en situation réelle d'audit

INFORMATIONS GÉNÉRALES

Code : REVA
Durée : 3 jours
Prix : 2 600 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

- Ingénieurs / Techniciens
- Responsables techniques
- Consultants sécurité

PRÉ-REQUIS

- Connaissances en Web
- Connaissances en sécurité

RESSOURCES

- Support de cours
- 70% d'exercices pratiques
- 1 PC par personne / Internet
- Environnement Linux
- Machine virtuelle avec outils d'analyse Android