

Formation Sécurité Android : identifier, exploiter et corriger les vulnérabilités de vos applications

Réf. SF34655

Apprenez à attaquer puis durcir vos applications Android pour les protéger contre les menaces réelles, en suivant l'OWASP Mobile Top 10.

2 j Durée	1 800 € HT Inter / participant	3 400 € HT Intra (≤12 pers.)	0 Sessions à venir
--------------	-----------------------------------	---------------------------------	-----------------------

Objectifs pédagogiques

- ✓ Identifier les vulnérabilités d'une application Android à partir de l'OWASP Mobile Top 10
- ✓ Mettre en place un environnement d'analyse Android
- ✓ Analyser le code et le contenu d'une APK pour détecter données sensibles et failles
- ✓ Exploiter les failles courantes en conditions de test
- ✓ Appliquer les contre-mesures de durcissement
- ✓ Construire des tests de pénétration simples sur une application Android

Public visé & prérequis

Public viséDéveloppeurs, Testeurs logiciels

Prérequis- Savoir développer ou maintenir une application Android (Java/Kotlin, structure d'un projet et d'une APK) - Bases de réseau (HTTP/TLS, notion de proxy) - Notions de cryptographie de base (hachage vs chiffrement)

Programme détaillé

Panorama des risques et surface d'attaque Android

- OWASP Mobile Top 10 : référentiel des risques applicatifs mobiles et lecture pour Android
- Architecture d'une application Android : activités, services, fournisseurs de contenu, intentions et permissions
- Le fichier manifest : déclarations de composants, permissions et points d'exposition
- Modèle de sécurité Android : sandbox applicative, signature et isolation des données
- Surface d'attaque : plateforme, application, communications et données

Activités pratiques :

- Revue commentée d'un manifest et identification des composants exposés
- Cartographie de la surface d'attaque d'une application Android de référence

Mise en place de l'environnement d'analyse

- Émulateur Android et application vulnérable de référence (type DIVA) comme fil rouge
- Proxy d'interception (Burp Suite) : configuration pour le trafic mobile
- ADB (Android Debug Bridge) : inspection, accès aux fichiers et débogage du terminal
- Outils de reverse et d'analyse : APKTOOL et MobSF (Mobile Security Framework) pour l'analyse statique et dynamique
- Chaîne d'outils standard et reproductible

Activités pratiques :

- Installation et prise en main d'ADB sur l'émulateur
- Interception du trafic d'une application via Burp
- Première analyse automatisée d'une APK avec MobSF

Stockage de données sensibles

- Emplacements de stockage : bases SQLite, fichiers, préférences partagées et logs
- Données exposées dans le manifest et dans les ressources de l'application
- Fuites par les journaux et les sauvegardes
- Injection SQL côté application et accès non maîtrisé aux données locales
- Contre-mesure : stockage chiffré avec Android Keystore et EncryptedSharedPreferences

Activités pratiques :

- Extraction de données sensibles d'une application vulnérable via ADB
- Exploitation d'une injection SQL locale puis correction
- Mise en place d'un stockage chiffré comme remédiation

Communication non sécurisée et interception réseau

- Scénarios de communication non sécurisée entre l'application et ses serveurs
- Attaque de l'homme du milieu (MITM) : principe et mise en œuvre (Ettercap, outil historique, et alternatives modernes type mitmproxy/Burp)
- Validation des certificats et erreurs courantes de configuration TLS
- Défauts de configuration des serveurs web exposés par l'application
- Contre-mesure : Network Security Config et certificate pinning

Activités pratiques :

- Mise en place d'une attaque MITM sur le trafic de l'application
- Implémentation du certificate pinning et vérification de l'efficacité

Authentification, secrets et cryptographie

- Stockage des clés et secrets d'API dans l'application : mauvaises pratiques fréquentes
- Recherche de credentials dans une APK (APKTOOL, MobSF)
- Méthodes cryptographiques : contre-exemples à proscrire (MD5, SHA1, SSLv2) et bonnes pratiques actuelles
- Authentification mal sécurisée : failles courantes et contre-mesures
- Référence directe non sécurisée à un objet (IDOR) et contrôle d'accès

Activités pratiques :

- Extraction de clés/API codées en dur dans une APK
- Identification et correction d'une faille IDOR
- Comparaison de schémas cryptographiques faibles vs robustes

Qualité de code et failles applicatives

- Mauvaise qualité de code comme source de vulnérabilités
- XSS DOM dans les composants WebView
- Dépassement de tampon (buffer overflow) : principe et impact
- Mode debug laissé actif et fonctions de test exposées en production
- Contre-mesures et bonnes pratiques de développement défensif

Activités pratiques :

- Identification d'une XSS DOM dans une WebView puis remédiation
- Détection d'un mode debug actif et durcissement de la configuration

Reverse engineering et falsification d'APK

- Désassemblage d'une APK et recherche de chaînes (« strings ») sensibles
- Falsification de code : modification et re-signature d'une APK
- Scénarios d'attaque par altération de l'application
- Intégrité, anti-tampering et obfuscation comme défenses
- Limites des protections et bonnes pratiques de durcissement

Activités pratiques :

- Désassemblage d'une APK et recherche de données sensibles
- Modification puis re-signature d'une APK et analyse du scénario d'attaque

Durcissement et test de sécurité d'une application Android

- Synthèse des contre-mesures par famille de risque OWASP
- Construction d'un test de pénétration simple sur une application Android
- Bonnes pratiques de chiffrement et de gestion des secrets de bout en bout
- Publication sécurisée sur Google Play : signature d'application et points de vigilance
- Cadrage rapide de la gestion de flotte (MDM, chiffrement du terminal) en complément du durcissement applicatif

Activités pratiques :

- Conduite d'un test de pénétration guidé sur l'application fil rouge
- Élaboration d'une grille de contre-mesures alignée sur l'OWASP Mobile Top 10

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

Note moyenne des participants de la filière Développement et Ingénierie de Logiciels : 4,9/5 — 165 avis

Romain G. — Un grand merci à Marius, la formation était dense mais très riche et très claire.

Cyndie Z. — Un grand merci à Arnaud LAGIEWKA

Ils nous font confiance

Cette année notre filière Développement Mobile & Cross-Platform a accompagné plus de 23 entreprises dont :

RENAULT SAS ITSAP ORANGE BUSINESS SERVICES SA ACTIA AUTOMOTIVE ANSYS FRANCE SAS ARTELIA HOLDING (AHL) BOLZE & MOOGY CHRONOPOST CRAMIF CRÉDIT MUTUEL ARKEA +13 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com