ISGroup
Information Security

MAST

Mobile Application Security Testing

www.isgroup.it
isgroup@isgroup.it

PIVA 04164220230
REA VR-397513

ISGroup
Information Security

Mobile Application Security Testing

Il Mobile Application Security Testing è un servizio di sicurezza applicativa, **Application Security Assessment**, proposto da ISGroup per le piattaforme **iOS** e **Android**, adattato a seconda del linguaggio di programmazione utilizzato per lo sviluppo di **app native** (Objective-C, Swift, Java, Kotlin) o di app realizzate con **framework ibridi** (come ad esempio React, React Native, Cordova, Xamarin, Titanium Appcelerator, Ionic, PhoneGap).

Sono molte le aziende che hanno investito in applicazioni mobile, ma spesso c'è **poca attenzione alla sicurezza** in quanto sono meno note le vulnerabilità e le relative possibilità di attacco da parte di un utente malevolo.

Il team di ISGroup si tiene costantemente aggiornato riguardo gli ultimi sviluppi di Mobile Security, sia dal punto di vista dell'attaccante che dello sviluppatore che deve difendere l'applicazione, in modo da fornire il miglior servizio di analisi possibile per i propri clienti.

Tramite l'utilizzo di tecniche manuali e tool avanzati, il tester è in grado di effettuare un'**analisi statica e runtime** dell'applicazione, in modo da bypassare eventuali limitazioni o logiche di business implementate.

Le applicazioni mobile sono infatti per loro natura soggette anche a **vulnerabilità di tipo client**, legate all'interazione dell'applicazione con il sistema operativo e il device sottostante. Ad esempio l'applicazione potrebbe non controllare se il telefono o tablet è jailbroken o rooted, oppure memorizzare dati sensibili o importanti in maniera non sicura.

Infine, l'auditor si occupa della verifica delle **interazioni tra l'applicazione e il server remoto**, le quali possono essere soggette a vulnerabilità simili a quelle delle applicazioni web (controlli di autenticazione ed autorizzazione, SQL Injection).

Descrizione del servizio

Un'attività di Mobile Application Security Testing rappresenta la simulazione di un attaccante nei confronti di un'applicazione scaricabile direttamente dagli store ufficiali (AppStore e PlayStore) oppure distribuita in modo alternativo per uso interno.

Il test può essere svolto in modalità **Grey Box** oppure **Black Box**.
Nel primo caso il tester analizza il codice dell'applicazione che il cliente ha fornito in modo da individuare in modo esaustivo le vulnerabilità che potrebbero essere altrimenti nascoste dall'offuscamento del codice, per poi proseguire con l'analisi runtime lato client dell'applicazione e delle interazioni con i servizi esposti lato server.

Nel caso di analisi di tipo Black box, il tester si trova invece nella situazione di un attaccante che analizza l'applicazione scaricata dallo store, come un normale utente.

Poiché il codice dell'applicazione client si trova sul dispositivo, il tester effettua un tentativo di **reverse engineering** in modo da verificare la presenza e la robustezza di eventuali contromisure implementate per prevenire il furto di proprietà intellettuale nonché la conoscenza di eventuali meccanismi di sicurezza che, con questa modalità, potrebbero essere bypassati.

Successivamente viene verificata la possibilità di **manipolazione dell'applicazione durante la sua esecuzione** ed infine, manualmente e con l'utilizzo di tool, vengono testati tutti i parametri individuati nelle richieste scambiate tra client e server.

A seconda del tipo di applicazione e del livello di accesso ottenuto, si cercherà quindi di modificare il flusso dell'applicazione e di manipolare e sfruttare a proprio vantaggio i dati salvati in locale e sul server remoto.

Output

Il **Report** è un documento semplice e dettagliato che riassume i risultati dell'attività ed è suddiviso in tre differenti aree come precedentemente descritto:

Executive Summary

All'inizio del Report e di lunghezza non superiore ad una pagina, è il riassunto di alto livello destinato al **Management**.

Vulnerability Details

La parte tecnica che descrive nel dettaglio le vulnerabilità riscontrate e il loro impatto, ed è dedicata al **Security Manager**.

Remediation Plan

Sezione tecnica con istruzioni precise su come risolvere le problematiche identificate, dedicata agli **sviluppatori**.

Richiedi servizi di Mobile Application Security Testing

Lavorare con noi è molto semplice, chiamando il numero +39 045 4853232 o spedendo una mail a sales@isgroup.it potremo conoscerci e discutere delle vostre necessità di fornitura di servizi di IT Security.