Software Quality per Information Security

La problematica

In tutti i settori di mercato ma in particolare in quello bancario il ruolo del software applicativo è centrale, e una priorità assoluta è quella di salvaguardare **la sicurezza e la confidenzialità dei dati e delle informazioni** gestiti.

La diffusione delle tecnologie mobile e la crescente complessità dei sistemi informatici hanno reso insufficienti le misure tradizionali per proteggere il software dagli attacchi, spesso opera di hacker, malware sofisticati o addirittura crimine organizzato. Per questo motivo è necessario focalizzarsi anche sulla **application security** per costruire la sicurezza partendo dall'interno delle applicazioni stesse.

Perché un agente esterno possa riuscire nel suo attacco, è necessaria una "porta di accesso" all'interno del software. Nel mondo perfetto queste porte non esistono, ma talvolta **ne creiamo involontariamente tramite gli errori nel codice**. La soluzione quindi sta **nell'individuare quegli errori** prima che vengano trovati dagli hacker.

Allo lo scopo di **aumentare la qualità** complessiva del software Società di Gestione Servizi (SGS) di Banco Popolare ha deciso di introdurre all'interno del proprio ciclo di vita del software degli **strumenti di analisi statica** per consentire l'individuazione di potenziali errori, bug, inefficienze e vulnerabilità nel software.

Soluzione tecnologica

Julia è un innovativo **analizzatore statico semantico per i linguaggi Java e Android**, basato sulla teoria scientifica dell'interpretazione astratta in grado di identificare una vasta gamma di errori e vulnerabilità. Si utilizza dal server aziendale o in cloud, è consultabile attraverso un plugin Eclipse o SonarQube dal proprio ambiente di sviluppo, e genera automaticamente un report pdf con una rappresentazione grafica dei risultati per una facile consultazione da parte dei diversi stakeholder.

Progetto di implementazione

Il progetto è stato preceduto da un PoC per verificare la corrispondenza alle necessità aziendali e per confrontarlo con soluzioni concorrenti.

I consulenti Julia hanno condotto il lavoro in collaborazione con il team tecnico del cliente in modalità "servizio di consulenza" analizzando un totale di 7 applicazioni diverse. Le modalità:

1) Installazione dell'analizzatore su un server interno e configurazione degli ambienti

2) Analisi delle applicazioni; per ognuna
- Individuazione automatizzata del codice potenzialmente errato
- Verifica puntuale delle segnalazioni
- Progressivo raffinamento delle relative analisi
- Interpretazione critica dei risultati e reportistica

3) Presentazione dei risultati alla Direzione e ai referenti applicativi delle varie aree, fornendo report di dettaglio e

un'indicazione sulla priorità con cui trattare e correggere le varie segnalazioni. Gli esiti delle analisi sono stati percepiti come contributo per migliorare la qualità complessiva dell'applicazione, non come una "pagella". Infatti anche gli sviluppatori hanno vissuto l'esperienza in un'ottica positiva come opportunità di migliorare le proprie capacità di programmazione.

Benefici

L'accoglienza dei risultati è stata positiva ben oltre le previsioni del cliente, sia da parte dei team di sviluppo, sia da parte della direzione.

Il beneficio immediato è stato il **miglioramento della qualità**, della **sicurezza** e dell'**efficienza** delle applicazioni. Il cliente ha constatato che l'implementazione di Julia aiuta a ridurre i problemi del software, sia di quello scritto internamente che di quello acquistato. Il ritorno dell'investimento si ripaga a breve-medio termine attraverso l'aumentata efficacia del ciclo di sviluppo, la ridotta manutenzione del software e la diminuzione dei disservizi dovuti a crash o blocchi degli applicativi, oltre alla riduzione dei rischi di sicurezza.

La soddisfazione ha portato alla fase successiva: introdurre lo strumento nel ciclo di sviluppo di tutto il software SGS.

Elementi distintivi

Julia è stato selezionato da SGS proprio per le sue **caratteristiche assolutamente uniche** sul mercato. Grazie alla sua tecnologia innovativa, è in grado di trovare **tutti gli errori presenti** nel codice per le categorie controllate. Inoltre, Julia è **l'unico tool per Java** in grado di individuare le diverse ***injection attacks*****,** ovvero attacchi di sicurezza.

Sviluppata da scienziati tuttora parte del team R&D, Julia è un analizzatore statico in grado di effettuare un **controllo sintattico e semantico** del codice applicativo Java e Android. La tecnologica è basata sulla teoria matematica dell'interpretazione astratta, che ne garantisce la precisione. Tutte le soluzioni concorrenti sono basate su tecnologie molto semplificate di pattern matching in grado di trovare solo una piccola parte degli errori.

Julia è l'unico strumento commerciale per analizzare **bytecode Java**: unicità importantissima perché permette l'individuazione degli errori e delle vulnerabilità anche in applicazioni fornite da terzi, delle quali non si dispone codice sorgente.