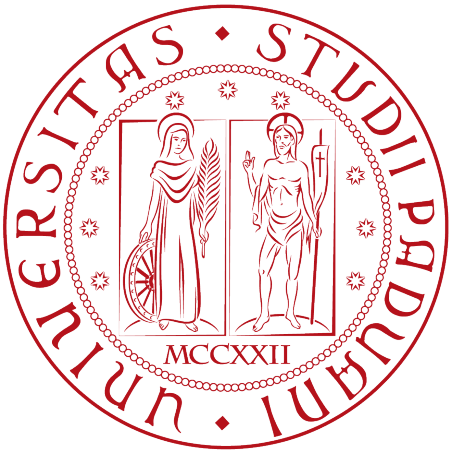
Università degli Studi di Padova

Dipartimento di Matematica "Tullio Levi-Civita"

Corso di Laurea in Informatica



Rilevazione di vulnerabilità software in librerie di terze parti

Tesi di laurea

Relatore

Prof. Tullio Vardanega

Laureando

Gionata Legrottaglie

Anno Accademico 2022-2023

Sommario

Il presente documento descrive il lavoro svolto durante il periodo di stage, della durata di trecentoventi ore, dal laureando Gionata Legrottaglie presso l'azienda Sanmarco informatica S.p.a.
Gli obbiettivi da raggiungere erano diversi.
In primo luogo era richiesto lo sviluppo di un plugin gradle per l'analisi statica delle dipendenze software di un progetto gradle o npm; in secondo luogo era richiesto di sviluppare dei servizi REST per il salvataggio dei risultati del plugin e per effettuare la ricerca delle vulnerabilità software note e, infine, una *web application* per la visualizzazione dei risultati.

Indice

Elenco delle figure

Elenco delle tabelle

Capitolo 1

L'azienda

1.1 Sanmarco informatica S.p.a.

1.1.1 Descrizione

L'azienda Sanmarco informatica S.p.a., fondata nel 1984, offre servizi di consulenza e sviluppo di software. Si è distinta nell'ideazione, costruzione e implementazione di strumenti software per oltre 2500 imprese, molte delle quali all'estero.
Una delle sue qualità distintive è l'attenzione verso i clienti, con vari uffici in regioni come Veneto, Lombardia, Emilia-Romagna, Friuli-Venezia Giulia, Toscana, Puglia e Campania, impiegando oltre 600 professionisti.
La sede centrale per la ricerca e sviluppo (CSV) si trova a Grisignano di Zocco (VI) e ospita più di 200 collaboratori. Qui, gruppi di sviluppatori e tecnici lavorano insieme per assicurare servizi affidabili e soluzioni software su misura.

1.1.2 Organizzazione dell'azienda e i suoi prodotti

Sanmarco informatica S.p.a. è suddivisa in *Business Unit* (BU), una parte di un'azienda che opera in modo autonomo o semi-autonomo, con la propria visione, *mission*, obiettivi e strategie. Essa ha una propria *leadership* e una struttura organizzativa separata, ed è responsabile del proprio profitto e perdite.
Le BU possono focalizzarsi su specifici mercati geografici, gruppi di clienti o linee di prodotti, permettendo all'azienda di essere più agile e rispondere meglio alle esigenze del mercato e dei clienti.
In Sanmarco informatica S.p.a. BU sono 11 e sono rappresentate in figura 1.1.

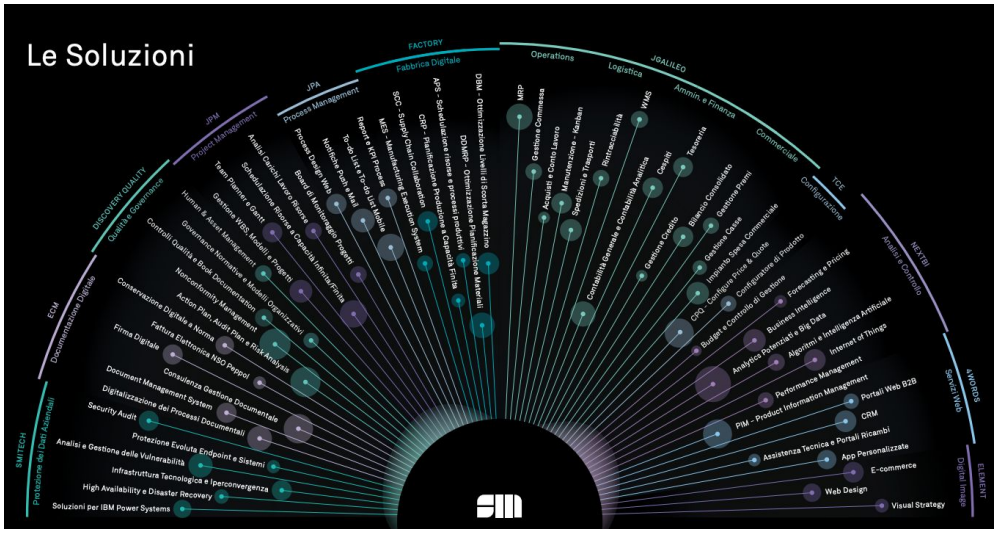


Figura 1.1: Le BU di Sanmarco informatica S.p.a. ed i loro prodotti

1.2 Il team di sviluppo

Il team di sviluppo in cui ho lavorato fa parte della BU *JPA* (*Process Management*) e non si occupa di sviluppare un prodotto specifico, ma ha come obiettivo quello di fornire supporto a tutti i team di sviluppo dell'azienda.
L'azione di supporto si concretizza nella creazione di strumenti che permettano di automatizzare e semplificare i processi di sviluppo, come ad esempio la compilazione, il rilascio di un prodotto o lo sviluppo di uno nuovo. Il team si occupa anche dello sviluppo di un *framework* interno che permette di creare applicazioni web in modo semplice e veloce e di fornire supporto per la gestione di repository e di strumenti di *continuous integration*

1.3 Strumenti utilizzati

I principali strumenti per lo sviluppo da me utilizzati sono stati i seguenti:

- **Intellij IDEA:** un ambiente di sviluppo integrato (IDE) per il linguaggio di programmazione Java. Fornisce strumenti e funzionalità avanzate per supportare lo sviluppo efficiente del codice, il debug e la testing. Con la sua interfaccia user-friendly e le potenti funzionalità, come l'analisi statica del codice e il refactoring intelligente, IntelliJ IDEA è scelto da molti sviluppatori per creare applicazioni Java professionali;
- **WebStorm:** un IDE per lo sviluppo di applicazioni web, che fornisce un'esperienza di sviluppo ottimale. Grazie alla sua integrazione con strumenti di supporto per lo sviluppo web, come *Node.js*, *Angular*, *React*, WebStorm permette di sviluppare applicazioni web moderne con facilità;
- **Neo4j Desktop:** un programma che permette di installare e gestire database *Neo4j* in modo semplice e veloce. Permette di creare e gestire più database, di monitorare le performance e di eseguire query;
- **Git:** un sistema di controllo versione distribuito, utilizzato per il versionamento del codice sorgente;
- **Gradle:** un sistema di automazione open source che gestisce le dipendenze e permette di automatizzare il processo di compilazione, testing, pubblicazione e deployment di un software;
- **Docker:** un progetto open source che automatizza il deployment di applicazioni all'interno di contenitori software, fornendo un'astrazione aggiuntiva grazie alla virtualizzazione a livello di sistema operativo di Linux;
- **Bitbucket:** un servizio di hosting per progetti che utilizzano Git come sistema di controllo versione. Fornisce strumenti per la collaborazione e la gestione del codice sorgente;
- **Jenkins:** un software open source che permette di automatizzare il processo di *build*, testing e deployment di un software;
- **Angular:** un framework open source per lo sviluppo di applicazioni web, scritto in TypeScript. Fornisce un'architettura Model-View-ViewModel (MVVM) e permette di creare applicazioni web dinamiche e scalabili;

- **Jira:** un software di tracciamento dei bug e gestione dei progetti, che permette di pianificare, monitorare e rilasciare software di qualità;
- **Confluence:** un software di collaborazione che permette di creare, organizzare e discutere documenti di progetto;

I linguaggi utilizzati sono i seguenti:

- **Java:** un linguaggio di programmazione ad alto livello, orientato agli oggetti e a tipizzazione statica, che permette di creare applicazioni web, desktop e mobile;
- **Javascript:** un linguaggio di programmazione ad alto livello, orientato agli oggetti e a tipizzazione dinamica, che permette di creare applicazioni web dinamiche;
- **TypeScript:** un super-set di Javascript che permette di aggiungere tipizzazione statica al linguaggio;
- **Groovy:** un linguaggio di programmazione che permette di scrivere codice che viene eseguito sulla Java Virtual Machine (JVM);
- **Chyper:** un linguaggio di query dichiarativo per grafi, utilizzato per interrogare database Neo4j;

1.4 Rapporto con l'innovazione

Sanmarco informatica S.p.a. ha come obiettivo l'innovazione delle aziende clienti per contribuire al loro progresso, agevolando la trasformazione digitale ed è specializzata nella progettazione e nella realizzazione di soluzioni integrate, a supporto della riorganizzazione di tutti i processi aziendali e professionali.
Per raggiungere questo obiettivo, l'azienda indirizza ogni anno dal 15 al 20% del proprio fatturato all'attività di Ricerca e Sviluppo.
Uno dei punti di forza di Sanmarco informatica S.p.a. è la capacità di cogliere le idee e i suggerimenti dei clienti, dei dipendenti, dei collaboratori e trarne ispirazione per sviluppare nuovi prodotti e nuove soluzioni

Appendice A

Appendice A

Citazione

Autore della citazione

Acronimi e abbreviazioni

API Application Program Interface. 8

IDE Integrated Development Environment. 8

JVM Framework. 4

MVVM Model-View-ViewModel. 3, 8

Glossario

API in informatica con il termine *Application Programming Interface API* (ing. interfaccia di programmazione di un'applicazione) si indica ogni insieme di procedure disponibili al programmatore, di solito raggruppate a formare un set di strumenti specifici per l'espletamento di un determinato compito all'interno di un certo programma. La finalità è ottenere un'astrazione, di solito tra l'hardware e il programmatore o tra software a basso e quello ad alto livello semplificando così il lavoro di programmazione. 7

continuous integration in ingegneria del software, l'integrazione continua (*continuous integration*) è una pratica che si applica in contesti in cui lo sviluppo del software avviene attraverso un sistema di versionamento. Consiste nell'allineamento frequente dagli ambienti di lavoro degli sviluppatori verso l'ambiente condiviso, al fine di rilevare tempestivamente eventuali errori di integrazione. 3

framework Un *framework* è una struttura concettuale e tecnologica predefinita che fornisce un modello standard su cui gli sviluppatori possono costruire applicazioni. Include librerie di codice, strumenti e linee guida che facilitano lo sviluppo, consentendo agli sviluppatori di concentrarsi sulla logica specifica dell'applicazione piuttosto che su dettagli di basso livello. Un framework può anche promuovere le buone pratiche di programmazione e ridurre la probabilità di errori.. 3, 7

IDE L'acronimo IDE sta per "Integrated Development Environment" che in italiano si traduce come "Ambiente di Sviluppo Integrato". Un IDE è un software che fornisce strumenti e servizi integrati per facilitare ai programmatori lo sviluppo di software. Include spesso un editor di codice, strumenti per il debugging, e funzionalità per la gestione di progetti, tra gli altri.. 3, 7

MVVM è un pattern architetturale utilizzato nello sviluppo software per separare la logica di business dall'interfaccia utente. Consiste in tre componenti principali:
Model: rappresenta i dati e la logica di business dell'applicazione.
View: è l'interfaccia utente che visualizza le informazioni al utente.
ViewModel: funge da ponte tra il Model e la View, gestendo la logica dell'interfaccia utente.
MVVM facilita una separazione pulita delle preoccupazioni, rendendo il codice più organizzato e più facile da mantenere e testare.. 7

Neo4j Neo4j è un database orientato ai grafi, open source, sviluppato in Java da Neo Technology. Il database è implementato in Java e Scala.. 4

Bibliografia

Riferimenti bibliografici

James P. Womack, Daniel T. Jones. *Lean Thinking, Second Editon*. Simon & Schuster, Inc., 2010.

Siti web consultati

Manifesto Agile. URL: http://agilemanifesto.org/iso/it/.