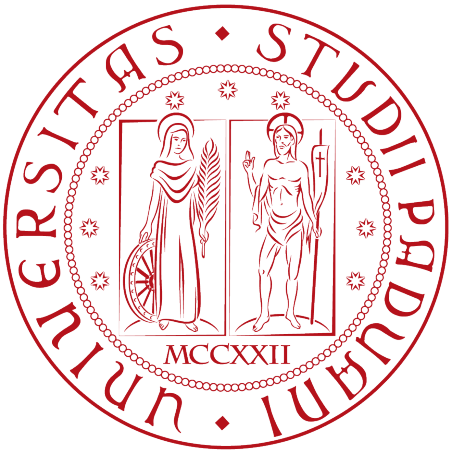
**Università degli Studi di Padova**

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'azienza 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, come rappresentate in figura 1.1, si suddividono in:

- **JGALILEO:** ha sviluppato l'Enterprise Resource Planning (ERP) – Jgalileo, il sistema gestionale completo che consente alle imprese di monitorare e governare i flussi aziendali in modo semplice ed efficace, grazie a workflow condivisi e informazioni univoche e coerenti. Il software gestionale ERP Jgalileo si rivolge a tutte le aziende produttive e commerciali di ogni dimensione, dalla piccola azienda al grande gruppo aziendale internazionale, grazie anche alla gestione accurata delle fiscalità estere;

- **NEXTBI:** specializzata in *Information Technology* e consulenza direzionale, con un focus nelle aree *marketing*, vendite, *retail*, *customer innovation*, Business Intelligence, Corporate Performance Management e per le soluzioni Internet of Things (IoT);

- **4WORDS:** specializzata in soluzioni Business to Business (B2B), app e Customer Relationship Management (CRM), ha l'obiettivo di far crescere le aziende grazie a soluzioni digitali dedicate: portale B2B, Applicazioni (App) custom, app per la rete vendita e l'assistenza tecnica, ma anche realtà aumentata e Product Information Management (PIM);

- **TCE:** si occupa di ottimizzare la fase di preventivazione e di acquisizione dell'ordine;
  Sviluppa il prodotto CPQ, strumento essenziale ai fini della configurazione dell'offerta, della gestione della trattativa e del recepimento del contratto, completo di tutti i contenuti documentali necessari. Attraverso uno strumento CPQ la forza vendite può configurare l'offerta più idonea in autonomia, in funzione delle specifiche esigenze del momento, senza preoccuparsi delle complesse logiche commerciali che la piattaforma gestisce in automatico;

- **DISCOVERY QUALITY:** produce una soluzione di Governance aziendale per gestire in modo efficace tutti i processi. Un potente motore di workflow guida in modo preciso l'operatività del management e degli utenti, e inoltre misura le performance dell'impresa.
  Discovery Quality gestisce anche le principali normative internazionali e le metriche legate alla sostenibilità aziendale Sustainable Development Goals (SDGs) e Benefit Corporation (BCorp);

- **ECM:** propone le soluzioni software integrate ideali di Enterprise Content Management (ECM) per gestire al meglio i documenti digitali;

- **SMITECH:** si occupa di Cybersecurity e Data Protection;

- **ELEMENT:** è la nuova divisione dedicata alla creazione di siti web ed e-commerce personalizzati, con una *customer shopping experience* su misura;
- **JPA:** è il software di Business Process Management (BPM) ideale per creare, gestire e automatizzare i processi aziendali integrandosi con qualsiasi sistema del cliente; gestendo automaticamente tutte le risorse;
- **FACTORY:** è la Business Unit che soddisfa tutte le necessità della Supply Chain e delle fasi nella fabbrica del futuro;
  La suite di Factory è stata sviluppata per aumentare il livello di servizio ai clienti, ridurre i livelli di scorta di magazzino, ottimizzare l'utilizzo degli asset aziendali e massimizzare i profitti, riducendo i costi;
- **JPM:** è il software di Project Management nato per supportare in modo semplice ed efficace le aziende nella gestione dei progetti, facilitando il raggiungimento degli obiettivi.

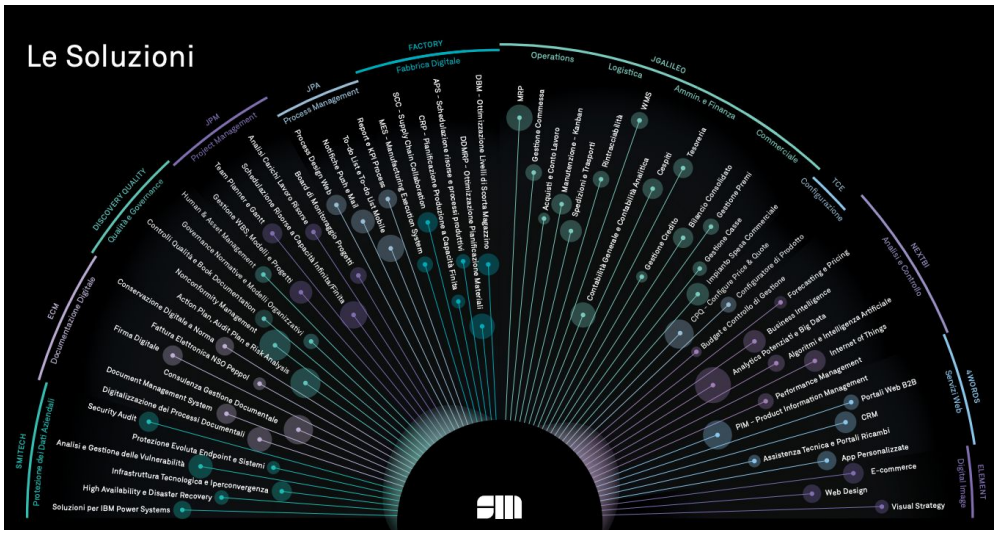



**Figura 1.1:** Le BU di Sanmarco informatica S.p.a. ed i loro prodotti

Ogni singola BU porta avanti diversi progetti ed ha un responsabile che si occupa di gestire il budget e le risorse umane.

Ogni progetto è formato da diverse figure:

- Un Product Owner (PO) che si occupa di gestire il progetto e di interfacciarsi con il cliente;
- Uno Scrum Master che si occupa di gestire il team di sviluppo e di facilitare il processo di sviluppo;
- Gli sviluppatori che si occupano di sviluppare il prodotto;
- I tester che si occupano di testare il prodotto;
- I consulenti che si occupano di interfacciarsi con il cliente, di capire le sue esigenze e successivamente di installare e configurare il prodotto;

- Gli analista che si occupano di analizzare i requisiti del cliente e di redigere la documentazione. Molte volte gli analisti sono anche sviluppatori e tester;

In aggiunta alle componenti precedentemente descritte, ci sono anche altre figure che compongono l'azienda:

- **HR:** si occupa di gestire le risorse umane, di reclutare nuovi dipendenti e di gestire i rapporti con i dipendenti;
- **Marketing:** si occupa di gestire il sito web, i social network e di creare materiale pubblicitario;
- **Amministrazione:** si occupa di gestire la contabilità e le risorse economiche;
- **IT:** si occupa di gestire l'infrastruttura informatica e di fornire supporto ai dipendenti;
- **Commerciali:** si occupano di trovare nuovi clienti e di gestire i rapporti con i clienti esistenti;
- **Direzione:** si occupa di gestire l'azienda e di prendere decisioni strategiche;
- **Centralino:** si occupa di gestire le telefonate e di accogliere i clienti;
- **Presidente:** fondatore dell'azienda, si occupa di prendere decisioni strategiche e di gestire i rapporti con i clienti più importanti;
- **Amministratore delegato:** si occupa di gestire l'azienda e di prendere decisioni strategiche;

All'interno dell'azienda c'è una parte di dipendenti che lavora in sede, una parte che lavora in remoto e una parte che lavora presso i clienti.
Per riuscire a monitorare il lavoro di tutti i dipendenti, l'azienda utilizza un software di *time tracking* che permette di registrare le ore lavorate.
Ogni dipendente ha un proprio *account* che permette di registrare le ore lavorate, di richiedere ferie e permessi.
Il software permette di visualizzare le ore lavorate da ogni dipendente e di generare report per ogni progetto e per ogni cliente.
Durante l'inserimento delle ore lavorate (Rapporino), il dipendente deve inserire una descrizione delle attività svolte, la commessa, l'eventuale cliente, la sede in cui ha lavorato, l'ora di inizio e fine lavoro ed eventualmente può collegare il Rapporino ad un ticket.
Questa operazione deve essere fatta per ogni giorno lavorativo e ad ogni chiusura del mese vengono bloccate le ore lavorate.

## 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.
Le principali attività del team sono le seguenti:

- **Supporto:** il team fornisce supporto ai team di sviluppo per la risoluzione di problemi tecnici e analitici;
- **Formazione:** il team fornisce formazione ai team di sviluppo per l'utilizzo di nuovi strumenti e tecnologie;
- **Ricerca e sviluppo:** il team si occupa di sviluppare un *framework* interno che permette di creare applicazioni web in modo semplice e veloce;
- **Automazione:** il team si occupa di automatizzare i processi di sviluppo, come ad esempio la compilazione, il rilascio di un prodotto o lo sviluppo di uno nuovo;
- **Gestione repository:** il team si occupa di gestire i repository di codice sorgente e di fornire supporto per l'utilizzo di strumenti di *continuous integration*;
- **Installatore:** il team si occupa di sviluppare un installatore per i prodotti dell'azienda che utilizzano il *framework* interno;

Il team è composto da 3 persone, uno Scrum Master e due sviluppatori.
In questo caso sviluppatori sono anche analisti e tester, e molto spesso anche lo Scrum Master partecipa alle analisi tecniche e funzionali.

## 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;

### 1.3.1 Convenzioni

Per lo sviluppo dei progetti che utilizzano il *frameworkg* interno, sono state definite delle convenzioni da seguire. Le convenzioni sono salvate all'interno di Confluence, in modo da essere facilmente accessibili a tutti i dipendenti.
Sono divise nelle seguenti categorie:

- **Documentazione:** sono delle regole che indica come documentare il codice sorgente, in modo da facilitare la comprensione del codice;

- **Scrittura analisi:** sono delle regole che indicano come scrivere l'analisi dei requisiti e le strutture dell basi di dati, in modo da facilitare la comprensione dell'analisi;
- **Progettazione:** sono delle regole che indicano come progettare i componenti software, in modo da facilitare la manutenzione e l'estensione del codice;
- **Codifica:** sono delle regole che permettono di scrivere codice in modo uniforme, in modo da facilitare la lettura e la comprensione del codice;
- **Versionamento:** sono delle regole che indicano come versionare il codice sorgente, in modo da facilitare la ricerca di una versione specifica del codice;

## 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.
In questo momento quasi tutti i prodotti attualmente installati presso i clienti hanno una nuova versione in fase di sviluppo, questo permette all'azienda di essere sempre all'avanguardia e di fornire ai clienti prodotti sempre aggiornati.

L'azienda punta molto alla cultura e alla formazione dei propri dipendenti, infatti ogni anno vengono organizzati corsi di formazione per permettere ai dipendenti di imparare nuove tecnologie e nuovi strumenti.
Questi corsi sono tenuti da dipendenti dell'azienda che hanno già esperienza con le tecnologie e gli strumenti trattati, da consulenti esterni o tramite *e-learning*, sulla piattaforma *Udemy Business* messa a disposizione gratuitamente dall'azienda.

Inoltre, l'azienda organizza molti eventi dedicati all'innovazione, come ad esempio *Choose Innovation* in collaborazione con *IBM*, dove i vari relatori discutono di innovazione e di come le aziende possono innovare.

# Appendice A

# Appendice A

Citazione

Autore della citazione

# Acronimi e abbreviazioni

**App** App. 2, 10

**B2B** Business to Business. 2, 11

**BCorp** Benefit Corporation. 2, 10

**BPM** Business Process Management. 3, 11

**CPQ** Configure Price Quote. 11

**CRM** Customer Relationship Management. 2, 11

**ECM** Enterprise Content Management. 2, 11

**ERP** Enterprise Resource Planning. 2, 12

**IDE** Integrated Development Environment. 12

**IoT** Internet of Things. 2, 12

**JVM** Framework. 6

**MVVM** Model-View-ViewModel. 6, 12

**PIM** Product Information Management. 2, 12

**PO** Product Owner. 3, 12

**SDGs** Sustainable Development Goals. 2, 10

# Glossario

**Analista** L'analista è una figura professionale che si occupa di analizzare i requisiti del cliente e di redigere la documentazione. Molte volte gli analisti sono anche sviluppatori e tester.. 4

**B2B** Business-to-business (B2B) è un modello di business che si riferisce alle transazioni commerciali tra due aziende, come quelle tra un produttore e un grossista o tra un grossista e un dettagliante.. 10

**BPM** Business process management (BPM) è un approccio alla gestione delle operazioni aziendali che si concentra su allineamento tutti i processi con i desideri e le esigenze dei clienti.. 10

**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. 5

**CPQ** Configure Price Quote (CPQ) è un software che consente alle aziende di automatizzare alcuni dei processi più complessi e propensi agli errori nella vendita di prodotti e servizi.. 2, 10

**CRM** Customer relationship management (CRM) è un approccio per gestire l'interazione di un'azienda con i clienti attuali e potenziali. Utilizza l'analisi dei dati sui clienti per migliorare le relazioni con i clienti, concentrarsi sulla customer retention e guidare le vendite.. 10

**Cybersecurity** La cybersecurity è la pratica di proteggere i sistemi, le reti e i programmi da attacchi digitali. Questi attacchi sono generalmente mirati a accedere, modificare o distruggere informazioni sensibili; estorcere denaro ai utenti; o interrompere normali operazioni aziendali.. 2

**Data Protection** La protezione dei dati è il processo di protezione delle informazioni da perdite, compromissione, attacchi o qualsiasi altra minaccia che possa compromettere la loro integrità.. 2

**ECM** Enterprise content management (ECM) è un insieme di strumenti e strategie che consentono a un'organizzazione di acquisire, organizzare, archiviare e distribuire informazioni critiche per l'organizzazione.. 10

**ERP** Un sistema di pianificazione delle risorse aziendali (ERP) è un sistema di gestione che consente a un'organizzazione di utilizzare un sistema di applicazioni integrate per gestire l'attività aziendale e automatizzare molte funzioni back office relative alla tecnologia, ai servizi e ai processi umani.. 10

**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.. 5, 6, 10

**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.. 5, 10

**IoT** L'Internet of Things (IoT) è un sistema di dispositivi interconnessi digitalmente, macchine, oggetti, animali o persone che sono forniti di identificatori univoci e la capacità di trasferire dati su una rete senza richiedere interazioni uomo-uomo o uomo-computer.. 10

**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.. 10

**Neo4j** Neo4j è un database orientato ai grafi, open source, sviluppato in Java da Neo Technology. Il database è implementato in Java e Scala.. 6

**PIM** Un sistema di gestione delle informazioni sui prodotti (PIM) è un insieme di strumenti e processi che un'azienda utilizza per gestire le informazioni sui prodotti necessarie per vendere e distribuire i propri prodotti a un acquirente finale.. 10

**PO** Il Product Owner (PO) è una figura professionale che si occupa di gestire il progetto e di interfacciarsi con il cliente.. 10

**Project Management** Il project management è l'insieme di attività di pianificazione, organizzazione, gestione e controllo di un progetto.. 3

**Scrum Master** Lo Scrum Master è una figura professionale che si occupa di gestire il team di sviluppo e di facilitare il processo di sviluppo.. 3, 5, 12

**Supply Chain** La supply chain è la rete globale di tutte le organizzazioni coinvolte nella creazione e nella distribuzione di un prodotto o servizio.. 3

# 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/.