

Rilevazione di vulnerabilità *software* in librerie di terze parti

Dipartimento di Matematica “Tullio Levi Civita” Università di Padova

Corso di Laurea in Informatica

Gionata Legrottoglie (1102654)

Esame di Laurea 13/12/2023



INFORMATICA
UNIVERSITY OF PADOVA



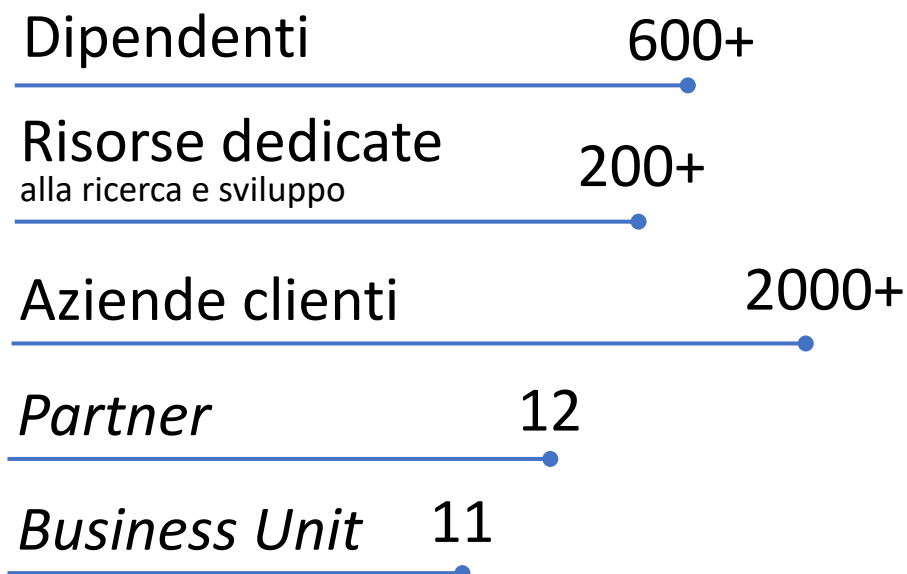
UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Anno accademico 2022/2023





1. L'azienda
2. La proposta di *stage*
3. Tecnologie utilizzate
4. Obiettivi dello *stage*
5. Implementazione
6. Risultati e conclusioni



La proposta di stage



UNIVERSITÀ
DEGLI STUDI
DI PADOVA

La crescita di Sanmarco Informatica S.p.A.

- Crescita dei prodotti in sviluppo
- Suddivisione in moduli dei prodotti esistenti
- Crescita delle installazioni clienti

Le nuove necessità:

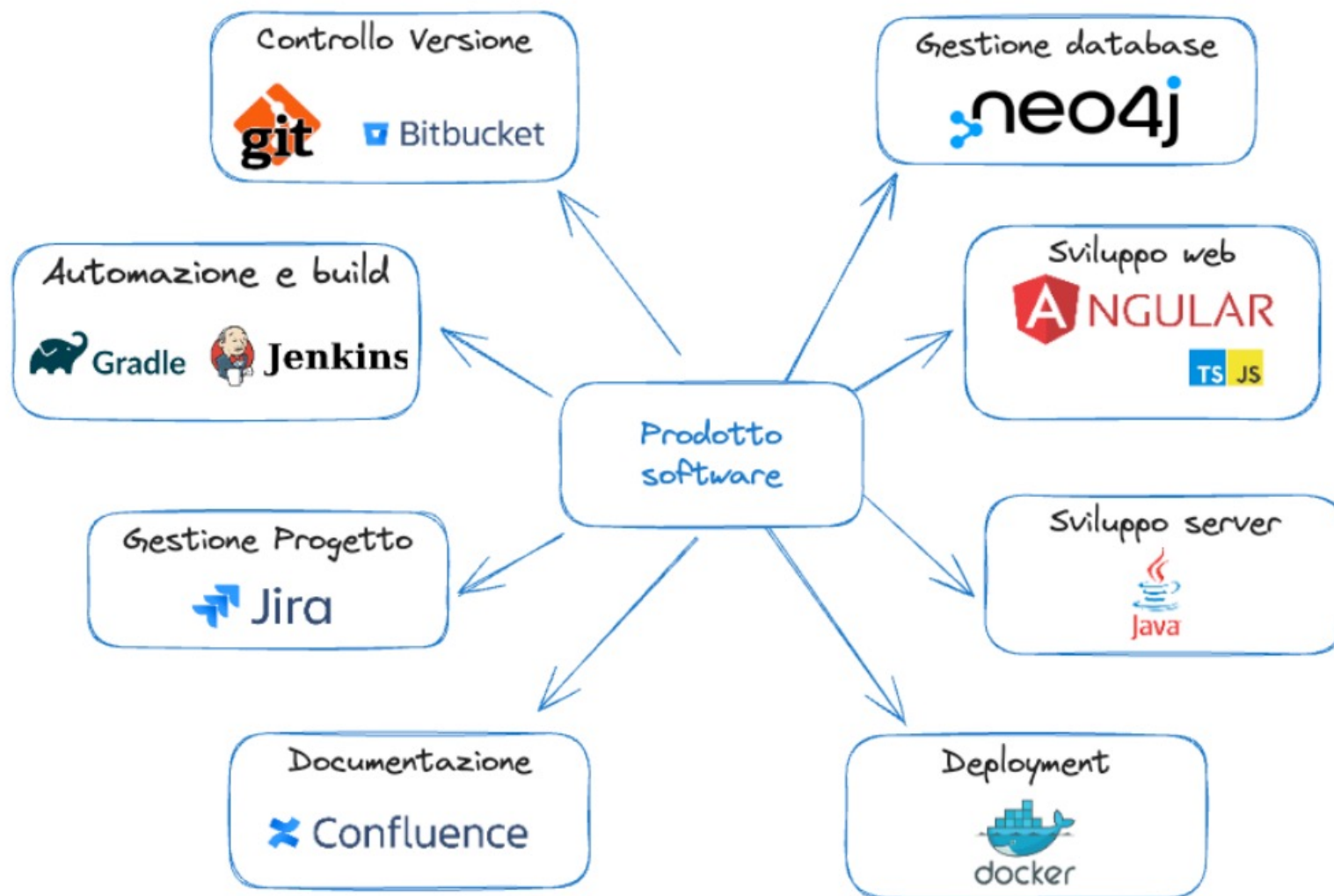
- Ricerca delle vulnerabilità *software*
- Monitoraggio dipendenze
- Tracciabilità delle versioni installate



Tecnologie utilizzate



UNIVERSITÀ
DEGLI STUDI
DI PADOVA



● Obbligatori

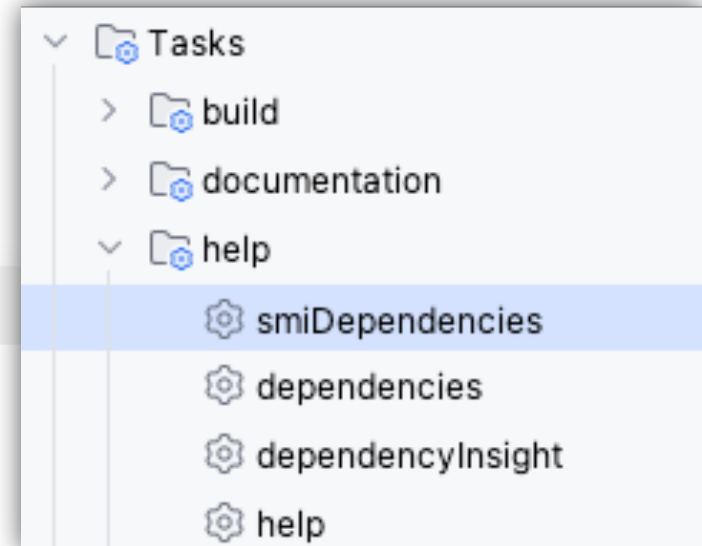
- Plugin Gradle per la raccolta delle informazioni
- REST API per il salvataggio e l'interrogazione
- Interfaccia grafica per analisi e interrogazioni
- Integrazione con Jenkins

● Desiderabili

- Verifica di nuovi aggiornamenti
- Analisi vulnerabilità
- Login LDAP
- Visualizzazione grafica delle dipendenze

Il *plugin*

```
1 apply plugin: 'com.smi.SmiDependencyAnalyzer'
2
3 smi_dependency_analyzer {
4     username = "nome_utente"
5     password = "private_key"
6     url = "http://localhost:8080/smi-dependency-store"
7     npmProject {
8         packageJson = "/projects/esempio1/client/package.json"
9         packageLockJson = "/projects/esempio1/client/package-lock.json"
10     }
11 }
```

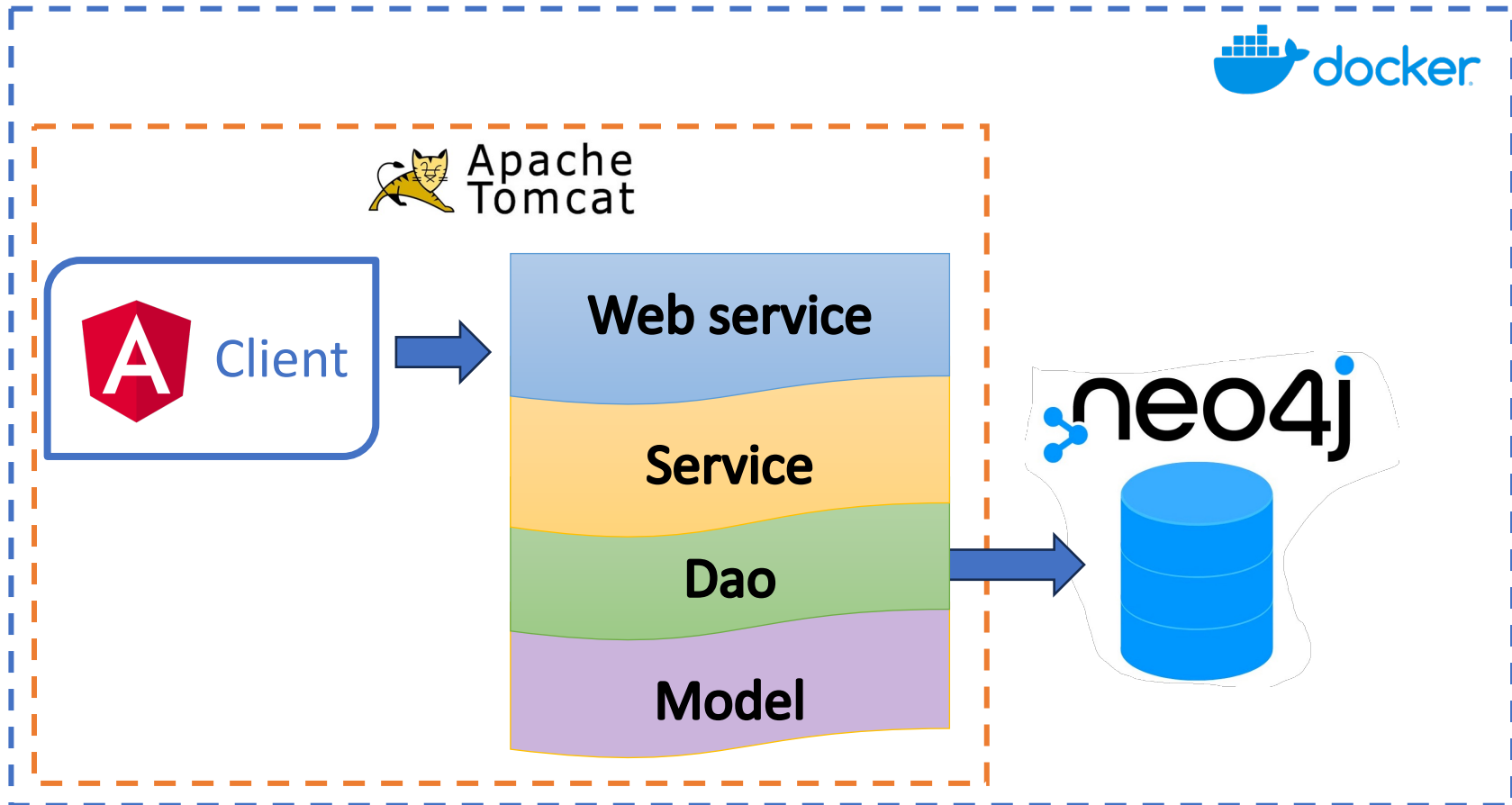


Implementazione



UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Infrastruttura e *backend*



Neo4J e le *query* con Cypher

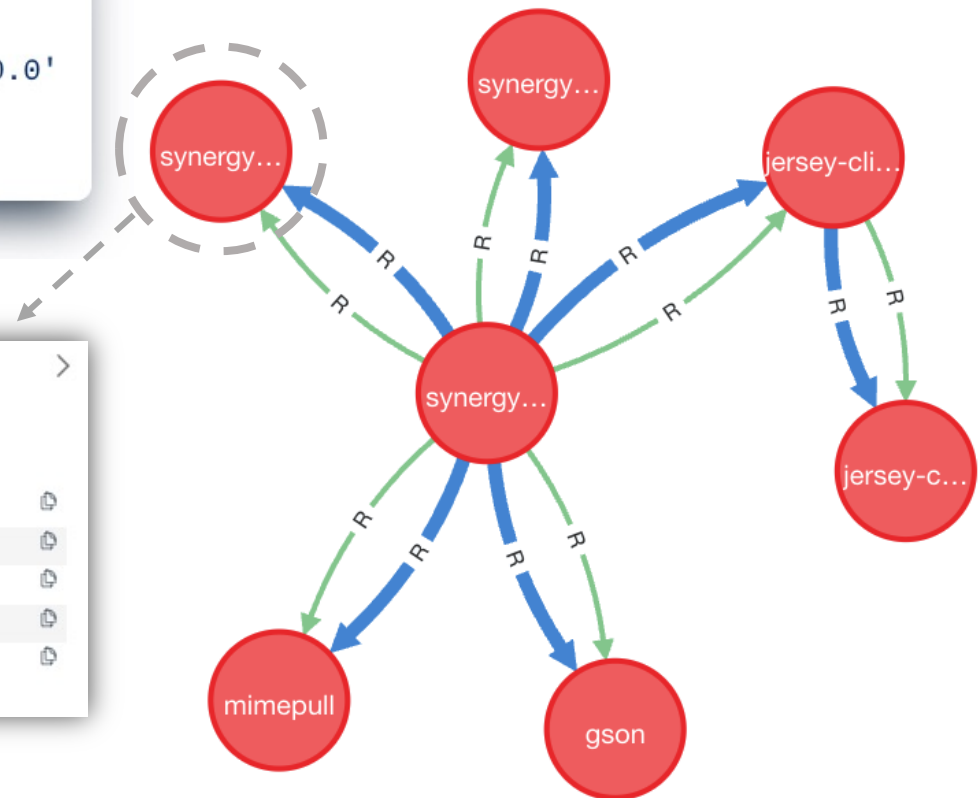
```
1 MATCH (N1)-[L:DEPENDS_ON]->(N2)
2 WHERE N1.id = 'net.synergy2:synergy2-ws:1.0.0'
3 RETURN N2
4 ORDER BY N.id
```

Node properties

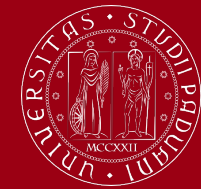
Package

java

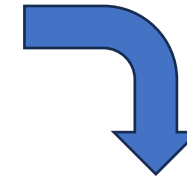
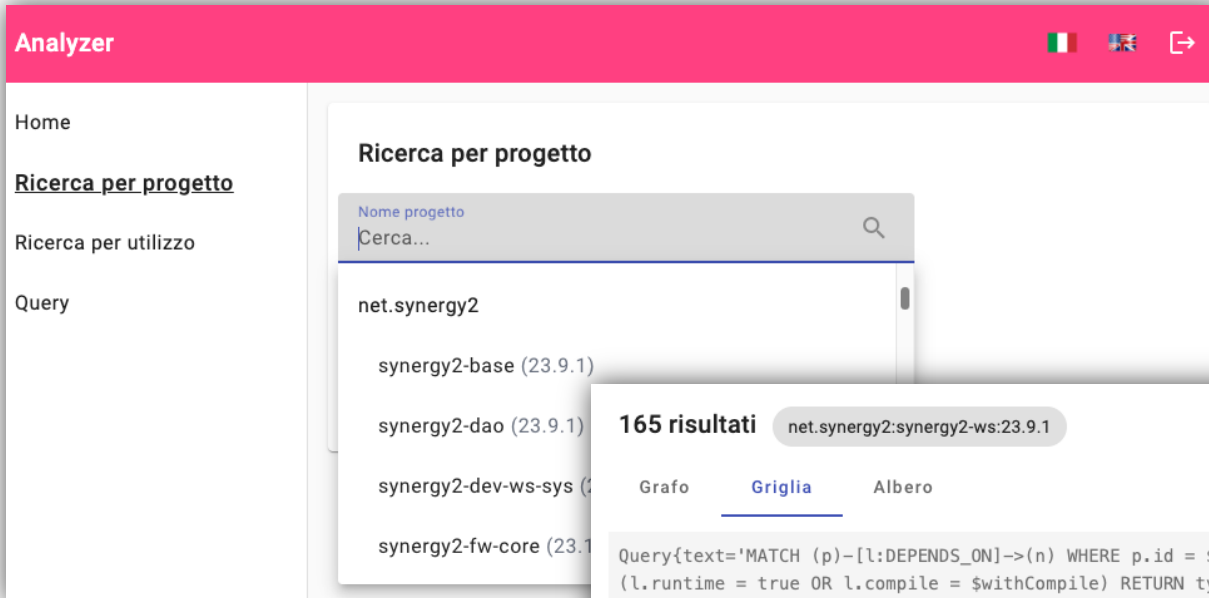
<id>	53
group	net.synergy2
id	net.synergy2:synergy2-rest-util:23.9.1
name	synergy2-rest-util
version	23.9.1



Implementazione



UNIVERSITÀ
DEGLI STUDI
DI PADOVA



165 risultati net.synergy2:synergy2-ws:23.9.1 [Controlla aggiornamenti](#) ✕

Grafo Griglia Albero

Query{text='MATCH (p)-[l:DEPENDS_ON]->(n) WHERE p.id = \$id AND (l.compile = false OR l.runtime = \$withRuntime) AND (l.runtime = true OR l.compile = \$withCompile) RETURN type (l), labels (n), l.type, l.require, l.variants, l.createdBy, l.compile, l.runtime, n.id, n.group, n.name, n.version ORDER BY n.id', parameters={id: "net.synergy2:synergy2-ws:23.9.1", withCompile: FALSE, withRuntime: TRUE}}

Id ↑	Gruppo	Nome
com.fasterxml.jackson.core:jackson-annotations:2.15.1	com.fasterxml.jackson.core	jackson-annotations
com.fasterxml.jackson.core:jackson-core:2.15.1	com.fasterxml.jackson.core	jackson-core
com.fasterxml.jackson.core:jackson-databind:2.15.1	com.fasterxml.jackson.core	jackson-databind
com.fasterxml.jackson.dataformat:jackson-dataformat-yaml:2.15.1	com.fasterxml.jackson.dataformat	jackson-dataformat-yaml
com.fasterxml.jackson.datatype:jackson-datatype-jsr310:2.15.1	com.fasterxml.jackson.datatype	jackson-datatype-jsr310



DIPARTIMENTO
MATEMATICA

Implementazioni facoltative

Controllo
aggiornamenti

4 risultati net.synergy2:webpush-java:23.9.1 [Controlla aggiornamenti](#) ✕

Griglia Grafo Albero

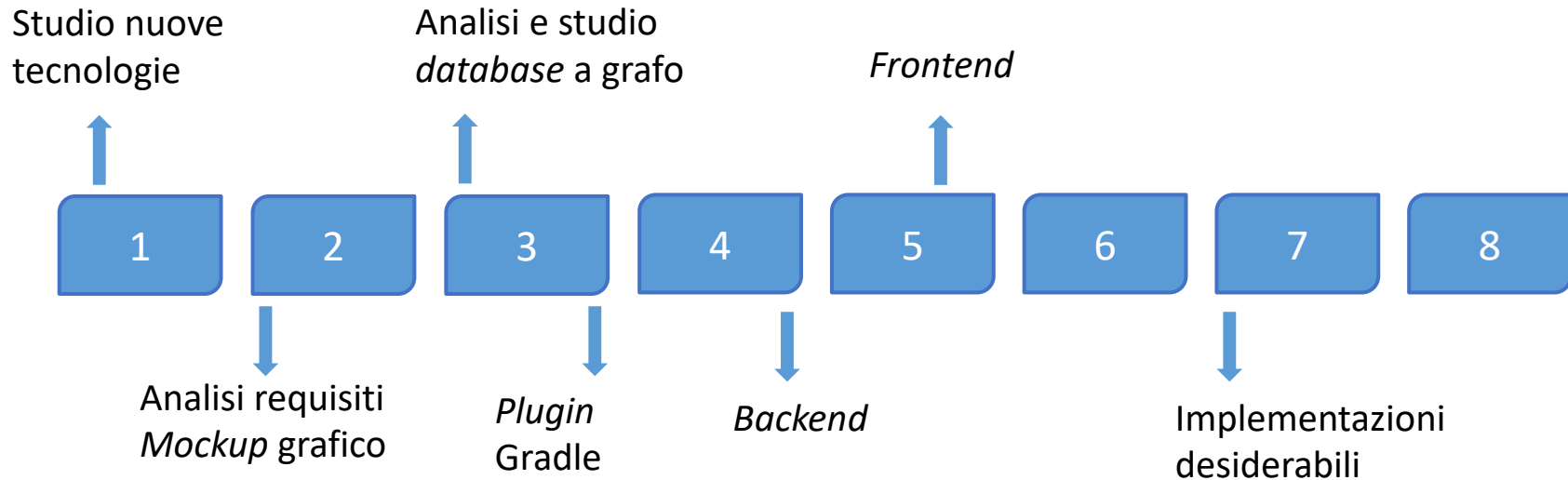
```
Query{text='MATCH (p)-[l:DEPENDS_ON]->(n) WHERE p.id = $id AND (l.compile = false OR l.runtime = $withRuntime) AND (l.runtime = true OR l.compile = $withCompile) RETURN type (l), labels (n), l.type, l.require, l.variants, l.createdBy, l.compile, l.runtime, n.id, n.group, n.name, n.version ORDER BY n.id', parameters={id: "net.synergy2:webpush-java:23.9.1", withCompile: FALSE, withRuntime: TRUE}}
```

Id 2 ↑	Gruppo	Nome	Versione	Info 1 ↓
org.bouncycastle:bcprov-jdk15on:1.69	org.bouncycastle	bcprov-jdk15on	1.69	Minor version update available: 1.69 -> 1.70
org.bitbucket.b_c:jose4j:0.7.9	org.bitbucket.b_c	jose4j	0.7.9	Minor version update available: 0.7.9 -> 0.9.3
com.sun.activation:javax.activation:1.2.0	com.sun.activation	javax.activation	1.2.0	
net.synergy2:synergy2-base:23.9.1	net.synergy2	synergy2-base	23.9.1	

LDAP

```
LDAP.yml
1 url: "ldap://10.220.101.15"
2 domain: "DOMINIO"
3 ssl: false
```

Ripartizione attività



Ore totali effettuate: 320

- Ore analisi: 80
- Ore formazione: 90
- Ore sviluppo: 130
- Ore sviluppo: 130

Risultati



- Righe di codice sorgente
 - *Plugin gradle*: **655**
 - *Backend*: **1583**
 - *Client*: **1872**
- *Test di unità*: **28**
- *Test di integrazione*: **15**
- *Test End-to-End*: **10**



- Analisi dei requisiti
- Mockup grafico
- Analisi dei casi d'uso
- Documentazione tecnica
- Documentazione utente

Conclusioni

Personalì

- ✓ Gestione progetti con Gradle
- ✓ Creazione di *plugin* Gradle
- ✓ Sperimentazione nuova versione di Angular
- ✓ *Database* a grafo



100% degli obiettivi soddisfatti

Aziendali

- ✓ Prototipo per monitoraggio delle dipendenze
- ✓ Sperimentazione database a grafo

