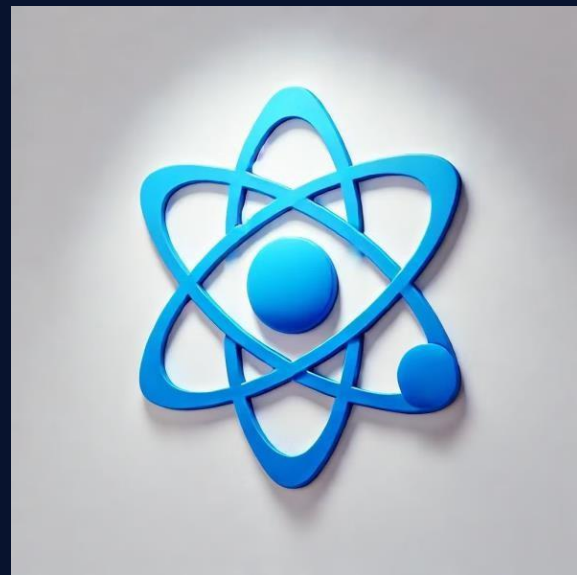


# Analisi delle dipendenze e generazione di SBOM per App react Native



ANDREA ISERNIO

[andrea.isernio@studio.unibo.it](mailto:andrea.isernio@studio.unibo.it)

# Idea Iniziale (parte 1)

## IDEA INIZIALE:

Analizzare le applicazioni React Native senza accesso al codice sorgente.

## APPROCCIO:

Partire direttamente dai file APK e decompilarli per identificare le dipendenze.



## STRUMENTI CONSIDERATI:

- **JADX**: Decompilatore per file APK, usato per convertire file .dex in codice leggibile.
- **Hermes-Dec**: Interpretazione del bundle React Native (index.android.bundle).



# Idea Iniziale (parte 2)

## Limitazioni Ricontrate:

- Complessità dell'analisi binaria dei file APK.
- Necessità di maggiore esperienza e conoscenze avanzate
- Tempi di sviluppo più lunghi per ottenere un processo completo e automatizzato



## Soluzioni Adottate:

- Focus sull'analisi delle dipendenze tramite i file package.json e yarn.lock.
- Utilizzo di progetti personali e open source elencati nel dataset.
- Processo più rapido e affidabile.

# Architettura dello Script

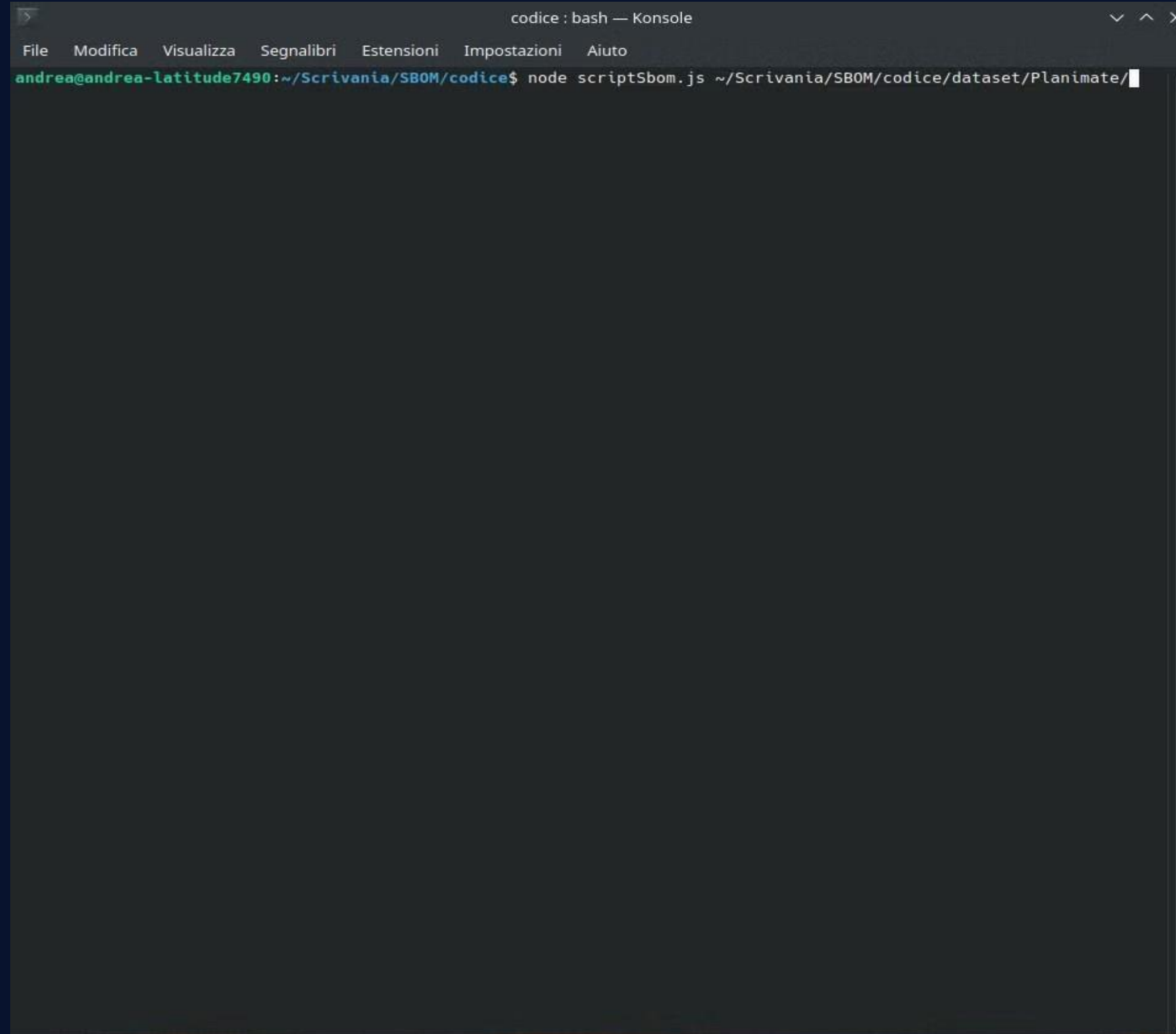
Identificazione  
delle Dipendenze

Analisi delle  
Vulnerabilità

Generazione  
SBOM e  
Vulnerability  
Report

Automazione degli  
aggiornamenti

# Simulazione Esecuzione 1



A screenshot of a terminal window titled "codice : bash — Konsole". The window has a menu bar with the following items: File, Modifica, Visualizza, Segnalibri, Estensioni, Impostazioni, and Aiuto. The terminal prompt is "andrea@andrea-latitude7490:~/Scrivania/SBOM/codice\$". The command being executed is "node scriptSbom.js ~/Scrivania/SBOM/codice/dataset/Planimate/". The command is partially visible, with a cursor at the end of the path. The terminal output is empty.

```
codice : bash — Konsole
File Modifica Visualizza Segnalibri Estensioni Impostazioni Aiuto
andrea@andrea-latitude7490:~/Scrivania/SBOM/codice$ node scriptSbom.js ~/Scrivania/SBOM/codice/dataset/Planimate/
```

# Simulazione Esecuzione 2

```
codice : node — Konsole
File  Modifica  Visualizza  Segnalibri  Estensioni  Impostazioni  Aiuto
andrea@andrea-latitude7490:~/Scrivania/SBOM/codice$ node scriptSbom.js ~/Scrivania/SBOM/codice/dataset/Planimate/
[+] Directory di output creata: /home/andrea/Scrivania/SBOM/codice/risultati/Planimate/2024-12-16T21-17-10-642Z
[+] Report delle vulnerabilità generato in: /home/andrea/Scrivania/SBOM/codice/risultati/Planimate/2024-12-16T21-17-10-642Z/vulnerability-report.md
[*] Generazione dello SBoM in formato JSON...
[+] SBoM generato in: /home/andrea/Scrivania/SBOM/codice/risultati/Planimate/2024-12-16T21-17-10-642Z/sbom.json
[*] Analisi completata con successo.
[INFO] Riepilogo:
- Totale componenti analizzati: 40
- Totale vulnerabilità trovate: 8
[?] Vuoi aggiornare automaticamente le dipendenze proposte? (y/n)
█
```



# Simulazione Esecuzione 3

```
codice : node — Konsole
File Modifica Visualizza Segnalibri Estensioni Impostazioni Aiuto
andrea@andrea-latitude7490:~/Scrivania/SBOM/codice$ node scriptSbom.js ~/Scrivania/SBOM/codice/dataset/Planimate/
[+] Directory di output creata: /home/andrea/Scrivania/SBOM/codice/risultati/Planimate/2024-12-16T21-17-10-642Z
[+] Report delle vulnerabilità generato in: /home/andrea/Scrivania/SBOM/codice/risultati/Planimate/2024-12-16T21-17-10-642Z/vulnerability-report.md
[*] Generazione dello SBoM in formato JSON...
[+] SBoM generato in: /home/andrea/Scrivania/SBOM/codice/risultati/Planimate/2024-12-16T21-17-10-642Z/sbom.json
[*] Analisi completata con successo.
[INFO] Riepilogo:
- Totale componenti analizzati: 40
- Totale vulnerabilità trovate: 8
[?] Vuoi aggiornare automaticamente le dipendenze proposte? (y/n)
y
[INFO] Avvio aggiornamento automatico delle dipendenze...
[INFO] Aggiornamento i18next da 23.11.2 a 24.1.0...
[INFO] Aggiornamento ky da 1.2.4 a 1.7.3...
[INFO] Aggiornamento react da 18.3.1 a 19.0.0...
[INFO] Aggiornamento react-i18next da 15.0.0 a 15.2.0...
[INFO] Aggiornamento react-native da 0.74.5 a 0.76.5...
[INFO] Aggiornamento react-native-calendars da 1.1306.0 a 1.1307.0...
[INFO] Aggiornamento react-native-draglist da 3.6.1 a 3.8.0...
[INFO] Aggiornamento react-native-gesture-handler da 2.14.0 a 2.21.2...
█
```



# Simulazione Esecuzione 4

```
codice : bash — Konsole
File Modifica Visualizza Segnalibri Estensioni Impostazioni Aiuto
andrea@andrea-latitude7490:~/Scrivania/SBOM/codice$ node scriptSbom.js ~/Scrivania/SBOM/codice/dataset/Planimate/
[+] Directory di output creata: /home/andrea/Scrivania/SBOM/codice/risultati/Planimate/2024-12-16T21-17-10-642Z
[+] Report delle vulnerabilità generato in: /home/andrea/Scrivania/SBOM/codice/risultati/Planimate/2024-12-16T21-17-10-642Z/vulnerability-report.md
[*] Generazione dello SBoM in formato JSON...
[+] SBoM generato in: /home/andrea/Scrivania/SBOM/codice/risultati/Planimate/2024-12-16T21-17-10-642Z/sbom.json
[*] Analisi completata con successo.
[INFO] Riepilogo:
- Totale componenti analizzati: 40
- Totale vulnerabilità trovate: 8
[?] Vuoi aggiornare automaticamente le dipendenze proposte? (y/n)
y
[INFO] Avvio aggiornamento automatico delle dipendenze...
[INFO] Aggiornamento i18next da 23.11.2 a 24.1.0...
[INFO] Aggiornamento ky da 1.2.4 a 1.7.3...
[INFO] Aggiornamento react da 18.3.1 a 19.0.0...
[INFO] Aggiornamento react-i18next da 15.0.0 a 15.2.0...
[INFO] Aggiornamento react-native da 0.74.5 a 0.76.5...
[INFO] Aggiornamento react-native-calendars da 1.1306.0 a 1.1307.0...
[INFO] Aggiornamento react-native-draglist da 3.6.1 a 3.8.0...
[INFO] Aggiornamento react-native-gesture-handler da 2.14.0 a 2.21.2...
[INFO] Aggiornamento react-native-localize da 3.2.0 a 3.3.0...
[INFO] Aggiornamento react-native-mmkv da 2.12.2 a 3.1.0...
[INFO] Aggiornamento react-native-reanimated da 3.15.0 a 3.16.5...
[INFO] Aggiornamento react-native-safe-area-context da 4.10.8 a 5.0.0...
[INFO] Aggiornamento react-native-screens da 3.31.0 a 4.3.0...
[INFO] Aggiornamento react-native-svg da 15.4.0 a 15.10.1...
[INFO] Aggiornamento react-native-vector-icons da 10.1.0 a 10.2.0...
[INFO] Aggiornamento ts-case-convert da 2.0.7 a 2.1.0...
[INFO] Aggiornamento zod da 3.23.0 a 3.24.1...
[INFO] Aggiornamento babel-jest da 29.6.3 a 29.7.0...
[INFO] Aggiornamento babel-plugin-module-resolver da 5.0.0 a 5.0.2...
[INFO] Aggiornamento dotenv da 16.3.1 a 16.4.7...
[INFO] Aggiornamento eslint da 9.8.0 a 9.17.0...
[INFO] Aggiornamento eslint-config-airbnb-typescript da 17.1.0 a 18.0.0...
[INFO] Aggiornamento eslint-import-resolver-typescript da 3.6.1 a 3.7.0...
[INFO] Aggiornamento eslint-plugin-import da 2.29.0 a 2.31.0...
[INFO] Aggiornamento eslint-plugin-jsx-a11y da 6.8.0 a 6.10.2...
[INFO] Aggiornamento jest da 29.2.1 a 29.7.0...
[INFO] Aggiornamento prettier da 2.8.8 a 3.4.2...
[INFO] Aggiornamento react-test-renderer da 18.2.0 a 19.0.0...
[INFO] Aggiornamento reactotron-react-native da 5.1.6 a 5.1.10...
[INFO] Aggiornamento reactotron-react-native-mmkv da 0.2.6 a 0.2.7...
[INFO] Aggiornamento typescript da 5.1.3 a 5.7.2...
[INFO] Aggiornamento completato.
andrea@andrea-latitude7490:~/Scrivania/SBOM/codice$
```



# PROBLEMI

- DIPENDENZE CON VERSIONI NON VALIDE



# SOLUZIONI

- FILTRI SULLE DIPENDENZE


```
function filtraDipendenzeInvalidi(dependencies) {  
    ...  
}
```

- TEMPI DI RISPOSTA LUNGHI CON GRANDI DATASET

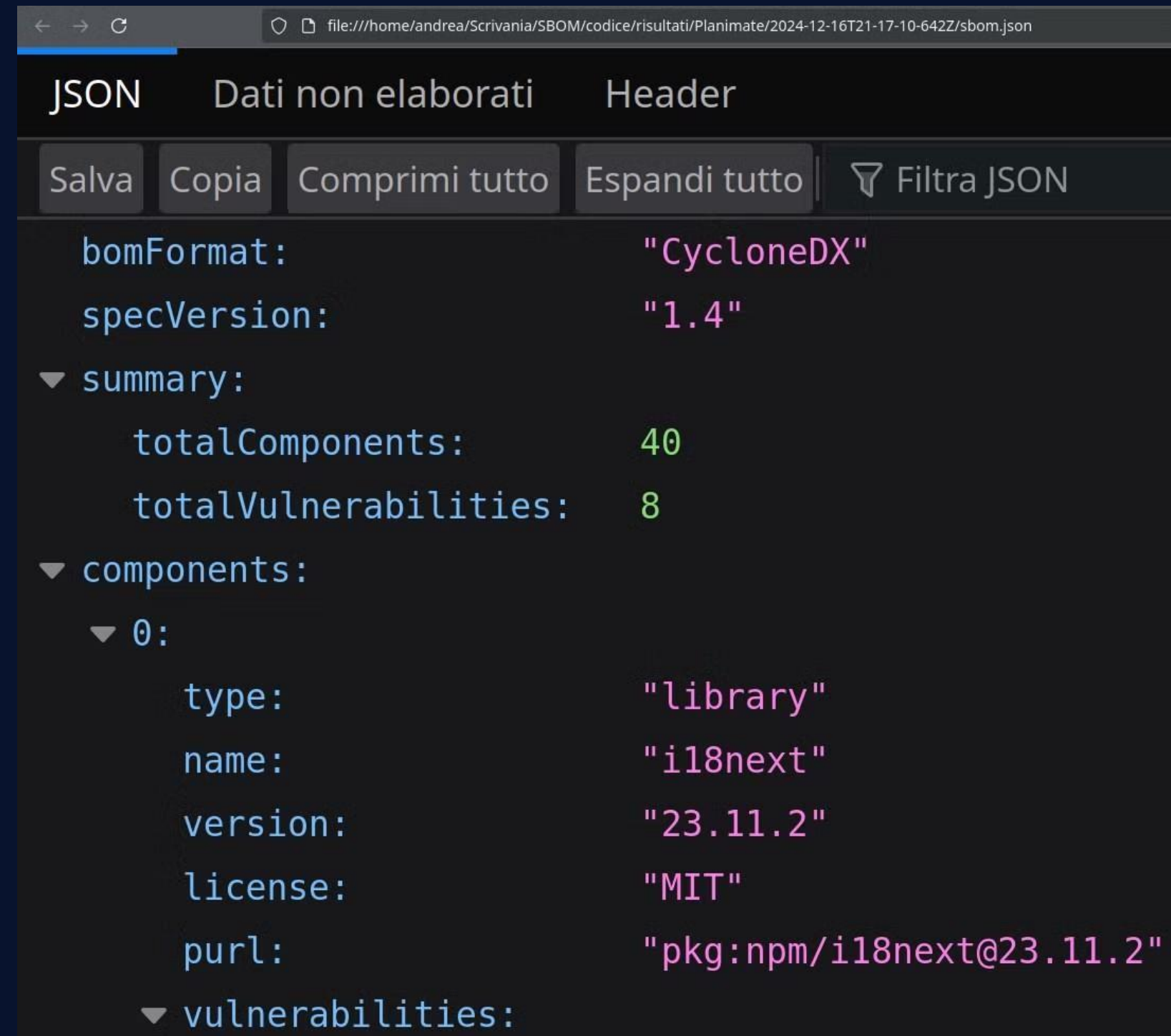


- OTTIMIZZAZIONI NELLE CHIAMATE API

```
async function cercaVulnerabilita(dependencies) {  
    const promises = dependencies.map(...);  
    await Promise.all(promises);  
}
```



# Esempio di Output: SBOM (1)



The image shows a screenshot of a web-based JSON viewer. The address bar at the top displays the file path: `file:///home/andrea/Scrivania/SBOM/codice/risultati/Planimate/2024-12-16T21-17-10-642Z/sbom.json`. The interface has a dark theme. At the top, there are three tabs: "JSON" (selected), "Dati non elaborati", and "Header". Below the tabs is a toolbar with buttons: "Salva", "Copia", "Comprimi tutto", "Espandi tutto", and a "Filtra JSON" button with a funnel icon. The main area displays the JSON data in a tree-like structure with syntax highlighting. The data includes a `bomFormat` field set to `"CycloneDX"`, a `specVersion` field set to `"1.4"`, a `summary` object containing `totalComponents` (40) and `totalVulnerabilities` (8), and a `components` array. The first component (index 0) is a library named `i18next` with version `23.11.2`, license `MIT`, and purl `pkg:npm/i18next@23.11.2`. It also has a `vulnerabilities` field.

```
bomFormat: "CycloneDX"
specVersion: "1.4"
▼ summary:
  totalComponents: 40
  totalVulnerabilities: 8
▼ components:
  ▼ 0:
    type: "library"
    name: "i18next"
    version: "23.11.2"
    license: "MIT"
    purl: "pkg:npm/i18next@23.11.2"
    ▼ vulnerabilities:
```

# Esempio di Output: SBOM (2)

```
file:///home/andrea/Scrivania/SBOM/codice/risultati/Planimate/2024-12-16T21-17-10-642Z/sbom.json

JSON  Dati non elaborati  Header

Salva  Copia  Comprimi tutto  Espandi tutto  Filtra JSON

bomFormat: "CycloneDX"
specVersion: "1.4"
▼ summary:
  totalComponents: 40
  totalVulnerabilities: 8
▼ components:
  ▼ 0:
    type: "library"
    name: "i18next"
    version: "23.11.2"
    license: "MIT"
    purl: "pkg:npm/i18next@23.11.2"
  ▼ vulnerabilities:
    ▼ 0:
      id: "GitHub-UNKNOWN"
      summary: "Cross-Site Scripting in i18next"
      severity: "MODERATE"
      ▼ references:
        ▼ 0:
          url: "https://nvd.nist.gov/vuln/detail/CVE-2017-16008"
        ▼ 1:
          url: "https://github.com/i18next/i18next/pull/443"
        ▼ 2:
          url: "https://github.com/advisories/GHSA-f89g-whpf-6q9m"
```

# Vulnerability Report

## Report di Vulnerabilità

**Progetto:** Planimate

**Data:** 2024-12-16T21:18:16.352Z

**Gravità massima rilevata:** CRITICAL

**Dettaglio per gravità:**

- CRITICAL: 1
- HIGH: 7
- MODERATE: 10
- LOW: 0

Numero di pacchetti vulnerabili trovati: 8 Numero totale di vulnerabilità: 18

**Pacchetto:** [i18next@23.11.2](#)

• ID: GitHub-UNKNOWN

- **Descrizione:** Cross-Site Scripting in i18next
- **Gravità:** MODERATE
- **Versione Fissata:** N/A
- **Riferimenti:**
  - <https://nvd.nist.gov/vuln/detail/CVE-2017-16008>
  - <https://github.com/i18next/i18next/pull/443>
  - <https://github.com/advisories/GHSA-f89g-whpf-6q9m>
  - <https://www.npmjs.com/advisories/325>

• ID: GitHub-UNKNOWN

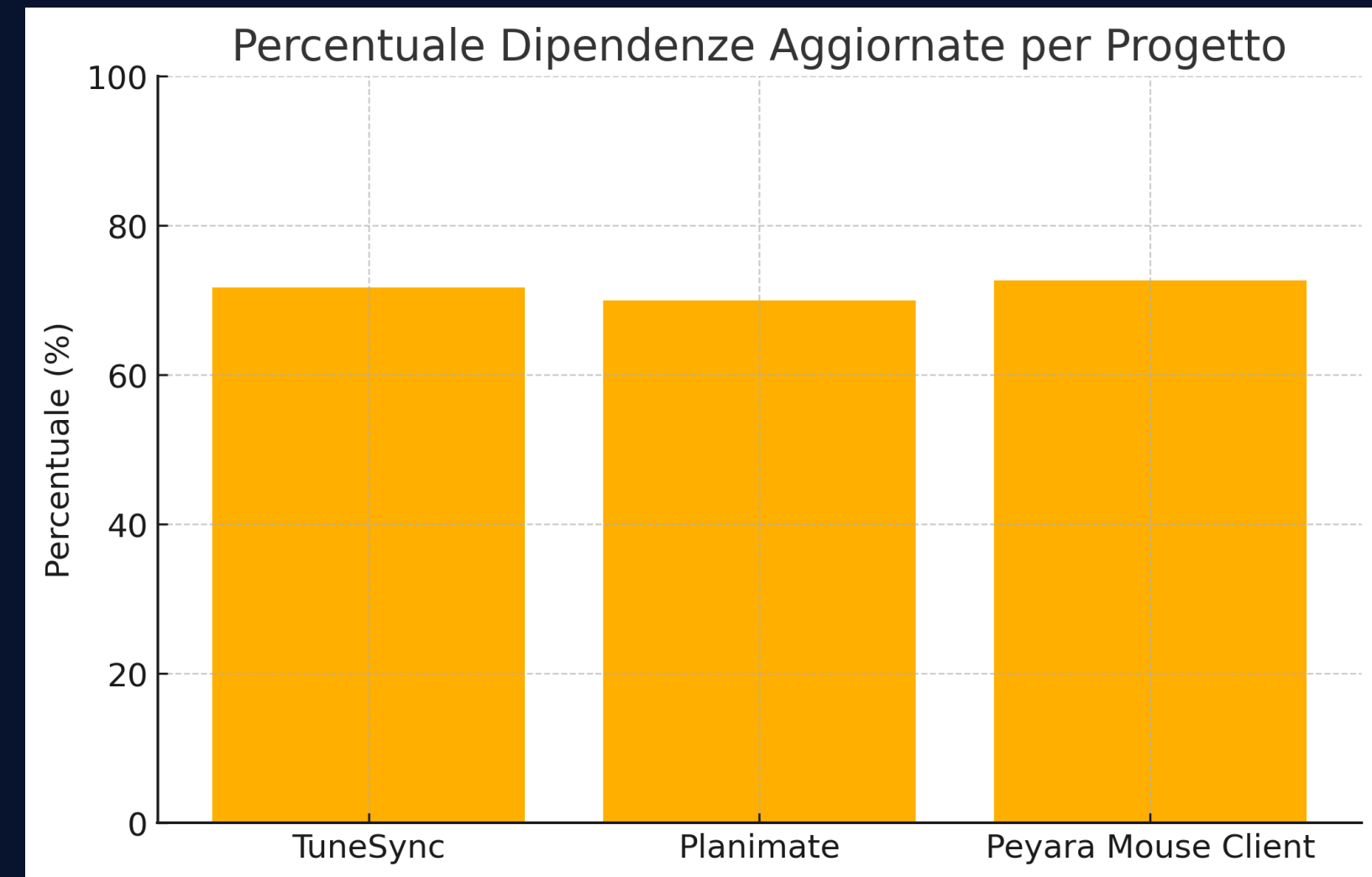
- **Descrizione:** Cross-Site Scripting in i18next
- **Gravità:** MODERATE
- **Versione Fissata:** N/A
- **Riferimenti:**
  - <https://nvd.nist.gov/vuln/detail/CVE-2017-16010>
  - <https://github.com/i18next/i18next/pull/826>
  - <https://github.com/advisories/GHSA-cmh5-qc8w-xvcg>
  - <https://www.npmjs.com/advisories/326>

**Pacchetto:** [lodash@4.17.21](#)

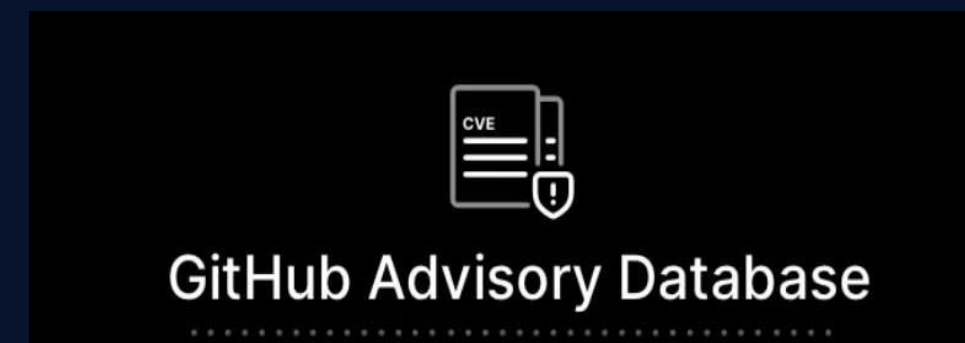


# Risultati

Proj	Comp.	Vuln.	Deps. Upd.	% Upd.
TuneSync	53	10	38	71.7%
Planimate	40	8	28	70.0%
Peyara Mouse	33	9	24	72.7%



# Tecnologie Utilizzate



# Sviluppi Futuri

- Integrazione con altri database di vulnerabilità.
- Implementazione di un'interfaccia grafica .
- Supporto per altri ecosistemi (Python, Java).



snyk



Grazie dell' attenzione !