Verbale esterno

14 gennaio 2026

Autore	Lorenzo Grolla
Verificatore	Nicolò Lattanzio
Approvazione	Alessandro Frison

Indice

1 Registro delle versioni

Versione	Data	Autore	Descrizione delle modifiche
0.0.1	20/01/2026	Lorenzo Grolla	Prima stesura del verbale

2 Informazioni introduttive

2.1 Durata e luogo

- **Inizio:** 11:30
- **Fine:** 12:20
- **Luogo:** Meeting Microsoft Teams

2.2 Partecipanti

Nome e Cognome	Presente	Assente
Damiano Berti	■	☐
Alessandro Frison	■	☐
Lorenzo Grolla	■	☐
Nicolò Lattanzio	■	☐
Alessandro Morabito	■	☐
Giacomo Nalotto	■	☐
Giulia Romanato	■	☐

3 Contenuto della riunione

3.1 Ordine del giorno

1. Definizione gestione dei Token per le repository.
2. Scelta del branch di default per le scansioni.
3. Definire chi ha il permesso per l'avvio delle scansioni.
4. Analisi gestione Code Coverage.
5. Definizione dei ruoli utente e gestione dei permessi.
6. Definizione dei requisiti minimi e delle funzionalità del Proof of Concept (POC) per l'RTB.

4 Riassunto della discussione

La riunione è servita a prendere decisioni importanti sull'architettura di CodeGuardian e sui requisiti per l'RTB. Il gruppo ha discusso come semplificare l'uso della piattaforma, rivedendo in particolare la gestione dei token e la selezione dei branch. Infine, sono stati definiti i ruoli degli utenti e stabilito cosa includere esattamente nel POC da presentare.

Di seguito vengono riportati i dettagli dei punti discussi:

4.1 Gestione token per l'accesso alle repository

La strategia approvata prevede che sia l'owner a inserire il token nel momento in cui la repository viene registrata nella piattaforma. È stato concordato di salvare il token nel database come campo persistente. In questo modo, chiunque abbia accesso a una repository all'interno della piattaforma potrà visualizzarne le informazioni e avviare scansioni senza dover inserire le credenziali volta per volta. Rispetto all'utilizzo di una GitHub App, che vincolerebbe l'utente a possedere necessariamente un account GitHub, l'uso del token si rivela la soluzione più flessibile e meno restrittiva. Questo approccio garantisce l'accessibilità della piattaforma anche a figure non tecniche, come i Project Manager, che potrebbero non disporre di un profilo GitHub.

4.2 Branch di default

Durante l'analisi delle modalità di scansione di un workspace, si è discusso se permettere la selezione manuale del branch per ogni repository o definirne uno predefinito. Sebbene inizialmente sia stata valutata l'ipotesi di lasciare la scelta all'utente in fase di caricamento, si è deciso infine di scartare questa opzione. Per ragioni di semplicità e per mantenere coerenza con le linee guida condivise, è stato stabilito di utilizzare il branch `develop` come impostazione di default per tutte le repository.

4.3 Lancio scansioni

Inizialmente si era ipotizzato di riservare la funzionalità di scansione delle repository esclusivamente a utenti con determinati privilegi. Tuttavia, per semplificare la gestione dei token e l'usabilità del sistema, si è deciso che tutti gli utenti in possesso del permesso di accesso a una repository possano avviarne le scansioni.

Nota di Vargroup: Si è consapevoli che in un ambiente di produzione reale tale scelta potrebbe non essere ottimale e che alcuni ruoli non dovrebbero avere i privilegi per avviare scansioni, ma nel contesto attuale tale semplificazione è stata ritenuta accettabile.

4.4 Calcolo Code Coverage

È stato richiesto un confronto sugli strumenti ottimali per il test della coverage, discutendo in particolare delle funzionalità offerte da SonarQube. La soluzione individuata per ottenere i risultati della coverage prevede l'esecuzione del tool di calcolo tramite container. Si specifica che tale operazione necessita l'esecuzione dei test automatizzati.

4.5 Gestione permessi

È stata presentata la struttura ideata per il sistema di permessi del progetto CodeGuardian, che include la gestione di utenti e ruoli, la possibilità di lanciare scansioni e i permessi di visione totale. La discussione si è concentrata sull'opportunità di mantenere permessi dinamici oppure di creare ruoli con permessi predefiniti. La conclusione è stata quella di adottare ruoli predefiniti, ciascuno con un set di permessi prestabiliti, scelta valutata come la più semplice ed efficace. I ruoli identificati sono: Tech Lead, Project Manager e Developer. Si tiene inoltre conto del fatto che un singolo utente potrà ricoprire ruoli differenti a seconda del workspace in cui lavora.

4.6 Proof of Concept (POC)

In vista della consegna per la revisione RTB (Requirements and Technology Baseline), si è discusso delle aspettative riguardo al Proof of Concept. È stato deciso che sarà sufficiente fornire una piattaforma che permetta di aggiungere una repository, eseguire una scansione e mostrare i risultati dell'analisi; il report fornito dovrà essere già quasi nella sua forma definitiva. È stato inoltre approfondito il rapporto tra l'uso diretto dei tool e l'intermediazione degli agenti, specialmente per le sezioni documentazione e OWASP:

- **Agente OWASP:** L'utilizzo di un agente dedicato è confermato. Anche qualora il tool individuato fornisca risultati grezzi, l'agente avrà il compito di elaborare le remediation o, più semplicemente, di formattare e ripulire l'output per renderlo leggibile e integrabile nella piattaforma.
- **Agente Librerie:** Lo sviluppo di un agente specifico per il controllo delle librerie rimane opzionale.

4.7 Repository Aziendali

In merito alla richiesta di accesso a repository reali per i test, l'azienda ha comunicato la disponibilità a fornire l'accesso a due repository pubbliche di loro proprietà. Tuttavia, siamo stati invitati a esplorare GitHub per reperire ulteriori esempi di progetti open source su cui effettuare i test.

5 Decisioni e azioni

Codice	Descrizione	Assegnatario
DEC-RTB-036	Aggiunta della repository tramite token, scartando l'utilizzo di GitHub Apps.	Tutti
DEC-RTB-037	Definizione di develop come branch di default per le scansioni, rimuovendo la scelta manuale in fase di upload.	Tutti
DEC-RTB-038	I permessi di scansione sono estesi a tutti gli utenti che hanno accesso alla repository, inclusi i Project Manager.	Tutti
DEC-RTB-039	Adozione di ruoli predefiniti (Tech Lead, PM, Developer) con permessi statici, scartando la gestione dinamica per workspace.	Tutti
DEC-RTB-040	Definizione requisiti POC: deve includere aggiunta repository, esecuzione scansione e visualizzazione risultati.	Tutti

Firma del proponente