



**Università degli Studi di Padova**

Laurea: Informatica

Corso: Ingegneria del Software

Anno Accademico: 2025/2026



**Gruppo: NullPointers Group**

Email: nullpointersg@gmail.com

# Verbale Riunione

**27 Ottobre 2025**

Stato	Approvato
Versione	1.0
Presenze	Marco Brunello Laura Pieripolli Matteo Mazzaretto Lisa Casagrande Luca Marcuzzo Tommaso Ceron
Destinatari	Prof. Tullio Vardanega Prof. Riccardo Cardin Var Group S.p.A.

## Registro delle modifiche

Vers	Data	Autore	Ruolo	Descrizione
1.0	28-10	Matteo Mazzaretto	-	Aggiunta firma proponente per approvazione documento
0.1	27-10	Luca Marcuzzo	-	Creazione e stesura documento

# Contents

<b>1</b>	<b>Informazioni generali</b>	<b>4</b>
<b>2</b>	<b>Ordine del giorno</b>	<b>5</b>
<b>3</b>	<b>Diario della riunione</b>	<b>6</b>
3.1	Bug reporting . . . . .	6
3.2	Responsività dell'interfaccia . . . . .	6
3.3	Gestione del fallimento o mancata risposta degli agenti . . . . .	6
3.4	Verifica e testing degli agenti . . . . .	7
3.5	Architettura degli agenti e gestione dello stato . . . . .	7
3.6	Gestione dei dati sensibili . . . . .	7
3.7	Analisi di sicurezza e conformità OWASP . . . . .	8
3.8	Gestione dell'autenticazione e degli accessi . . . . .	8
3.9	Deployment e ambiente su Amazon Web Services (AWS) . . . . .	8
3.10	Sviluppo e modularità degli agenti . . . . .	9
<b>4</b>	<b>Approvazione Esterna</b>	<b>10</b>

## 1 Informazioni generali

- **Tipo di riunione:** esterna con proponenti
- **Luogo:** Google Meet
- **Data:** 27/10/2025
- **Ora inizio:** 15:35
- **Ora fine:** 15:55
- **Scriba:** Luca Marcuzzo
- **Partecipanti:**
  - Stefano Dindo (Var Group S.p.A.)

## **2 Ordine del giorno**

Primo colloquio online di NullPointers Group con l'azienda Var Group S.p.A.: vengono chiariti i dubbi riguardanti il capitolato d'appalto e le domande sorte durante l'analisi del progetto da parte del gruppo.

## 3 Diario della riunione

Discussione con l'azienda proponente riguardo il progetto Code Guardian guidata dalle nostre domande su diversi ambiti del progetto.

### Resoconto

#### 3.1 Bug reporting

È stato richiesto un chiarimento in merito alla modalità di gestione del bug reporting all'interno della piattaforma CodeGuardian.

Il gruppo ha domandato se fosse necessario implementare un sistema di ticketing integrato o se fosse sufficiente adottare una modalità più semplice di tracciamento.

L'azienda ha specificato che non è necessario sviluppare un sistema di ticketing dedicato. È sufficiente mantenere un tracciamento dei bug, ad esempio tramite le issue del repository o mediante un documento condiviso in cui vengano registrate le segnalazioni.

L'importante è concordare un formato univoco all'inizio del progetto, in modo da garantire coerenza e facilità di gestione durante lo sviluppo.

#### 3.2 Responsività dell'interfaccia

Il gruppo ha richiesto chiarimenti circa la necessità di rendere l'interfaccia front-end della piattaforma compatibile con dispositivi mobili o tablet.

L'azienda ha precisato che non è richiesto lo sviluppo di un'interfaccia responsive: la piattaforma potrà essere ottimizzata esclusivamente per l'utilizzo da desktop.

#### 3.3 Gestione del fallimento o mancata risposta degli agenti

Il gruppo ha richiesto chiarimenti sulle modalità di gestione nel caso in cui uno degli agenti non risponda o fallisca durante l'esecuzione del processo.

L'azienda ha spiegato che questa logica potrà essere definita più nel dettaglio durante la fase di design thinking, ma ha precisato che ogni agente dovrà comunque essere in grado di fornire una risposta.

Nel caso in cui l'output non sia immediatamente disponibile, il sistema potrà attendere finché non sarà possibile ottenere un risultato completo.

L'orchestratore avrà il compito di valutare le risposte ricevute dai singoli agenti, determinando se esse siano soddisfacenti, parzialmente soddisfacenti o non soddisfacenti, e di reiterare eventualmente la richiesta finché non verrà raggiunto un risultato adeguato.

### 3.4 Verifica e testing degli agenti

È stato richiesto un approfondimento in merito alle modalità di verifica e test degli agenti, in particolare se l'azienda fornirà repository di prova o se sarà il gruppo a crearne di proprie contenenti vulnerabilità note.

L'azienda ha chiarito che, in una fase iniziale, sarà possibile utilizzare progetti disponibili pubblicamente su GitHub o repository creati ad hoc come boilerplate di test.

Questa fase servirà per il training e la validazione preliminare degli agenti, senza coinvolgere repository proprietari dei clienti.

Una volta ottenuta una demo funzionante e stabile, sarà possibile eseguire test su progetti concreti dell'azienda per valutare il comportamento del sistema in contesti reali.

Le modalità precise di testing verranno comunque definite durante la fase progettuale, in accordo tra il gruppo e l'azienda.

### 3.5 Architettura degli agenti e gestione dello stato

Il gruppo ha richiesto chiarimenti circa la necessità per gli agenti di mantenere uno stato tra un'analisi e l'altra o se possano essere progettati come stateless.

L'azienda ha spiegato che, nella visione complessiva del progetto, l'obiettivo ideale è che gli agenti conservino uno storico delle analisi eseguite, in modo da poter valutare l'evoluzione del progetto nel tempo.

Ad esempio, in un'analisi relativa ai test, l'agente dovrebbe essere in grado di confrontare la copertura tra una prima e una seconda release, fornendo così un riscontro sul progresso ottenuto.

Tuttavia, in una fase iniziale è possibile sviluppare il sistema in modalità stateless per verificare il corretto funzionamento complessivo. Successivamente, una volta validato il flusso base, si potrà introdurre la componente di memoria storica per arricchire le capacità analitiche degli agenti.

### 3.6 Gestione dei dati sensibili

Il gruppo ha sollevato la questione relativa alla gestione dei dati sensibili durante le fasi di analisi e test, chiedendo come evitare il rischio di trattare informazioni riservate.

L'azienda ha chiarito che, per le attività di sviluppo e validazione iniziale, dovranno essere utilizzati esclusivamente boilerplate o progetti open source pubblicamente disponibili, in modo da poter eseguire tutte le prove necessarie senza memorizzare codice o dati sensibili.

Il sistema dovrà operare unicamente su meta-dati e risultati di analisi, evitando di conservare o diffondere contenuti proprietari.

Eventuali test che coinvolgano dati o repository sensibili verranno gestiti internamente dall'azienda, che fornirà successivamente un feedback al gruppo sui risultati ottenuti.

### 3.7 Analisi di sicurezza e conformità OWASP

Il gruppo ha richiesto chiarimenti in merito all'ambito di analisi che gli agenti dovranno coprire, domandando se la verifica di sicurezza, in riferimento alla Top 10 OWASP, debba riguardare esclusivamente il codice sorgente dell'applicazione o includere anche le librerie esterne utilizzate.

L'azienda ha spiegato che l'obiettivo di un agente completo è fornire una visione statica complessiva dell'analisi di compliance OWASP, comprendendo sia il codice sviluppato internamente sia le librerie di terze parti.

Tuttavia, il grado di approfondimento verrà definito progressivamente durante la fase di design thinking, in funzione delle aree di interesse di ciascun gruppo di lavoro.

In questa fase progettuale, i gruppi potranno quindi orientarsi su aspetti diversi, ad esempio concentrandosi sulle vulnerabilità del codice o sulle dipendenze esterne, in base alla sensibilità e agli obiettivi specifici del proprio sviluppo.

### 3.8 Gestione dell'autenticazione e degli accessi

Il gruppo ha chiesto chiarimenti in merito alla necessità di implementare un sistema di autenticazione per la gestione degli accessi alla piattaforma.

L'azienda ha precisato che non è previsto un meccanismo di autenticazione complesso né la gestione di utenti multipli.

Il sistema opererà attraverso un unico utente principale, corrispondente all'orchestratore, che coordina le attività degli agenti e genera l'output finale.

È tuttavia necessario che tale utente disponga delle autorizzazioni necessarie per interfacciarsi con i repository e svolgere le operazioni previste.

L'autenticazione sarà quindi limitata a garantire l'accesso alle risorse autorizzate, senza introdurre funzionalità avanzate di gestione profili o ruoli.

### 3.9 Deployment e ambiente su Amazon Web Services (AWS)

Il gruppo ha richiesto chiarimenti riguardo alle modalità di deployment della piattaforma su Amazon Web Services (AWS), domandando se l'azienda fornirà un ambiente preconfigurato o se sarà necessario che il gruppo gestisca autonomamente un proprio account.

L'azienda ha specificato che verrà fornito un account AWS dedicato, all'interno del quale il gruppo potrà operare in base all'architettura e ai servizi definiti in fase di progettazione.

L'obiettivo è anche formare il gruppo sulle buone pratiche di gestione dei progetti in ambiente cloud, fornendo una sessione di approfondimento su aspetti quali la progettazione dell'architettura, la simulazione dei costi e la successiva verifica tra pianificazione e implementazione effettiva.

Il gruppo disporrà di uno spazio operativo dedicato, con i permessi necessari per svolgere le attività di deployment e configurazione sotto la supervisione dell'azienda.



### **3.10 Sviluppo e modularità degli agenti**

A seguito della riunione, il gruppo ha inviato un chiarimento via e-mail riguardo alla natura dello sviluppo degli agenti, chiedendo se dovranno essere realizzati da zero o se sarà possibile riutilizzare agenti già esistenti, adattandoli alle esigenze del progetto.

L'azienda ha risposto che la definizione degli agenti verrà concordata durante la sessione di design thinking, e che lo sviluppo dovrà essere svolto dal gruppo con un livello di dettaglio da stabilire congiuntamente.

È stato inoltre sottolineato che l'aspetto centrale del progetto non risiede tanto nella funzionalità dei singoli agenti, quanto nella modularità complessiva della piattaforma, che dovrà consentire di aggiungere, evolvere o sostituire gli agenti in modo flessibile.

## 4 Approvazione Esterna

Si attesta che il seguente verbale della riunione è stato approvato da parte dei  
rappresentati di Var Group S.p.A..

Tale approvazione è comprovata dalla presenza della firma del rappresentante:

A handwritten signature in black ink, appearing to be 'G. Di' followed by a stylized flourish.