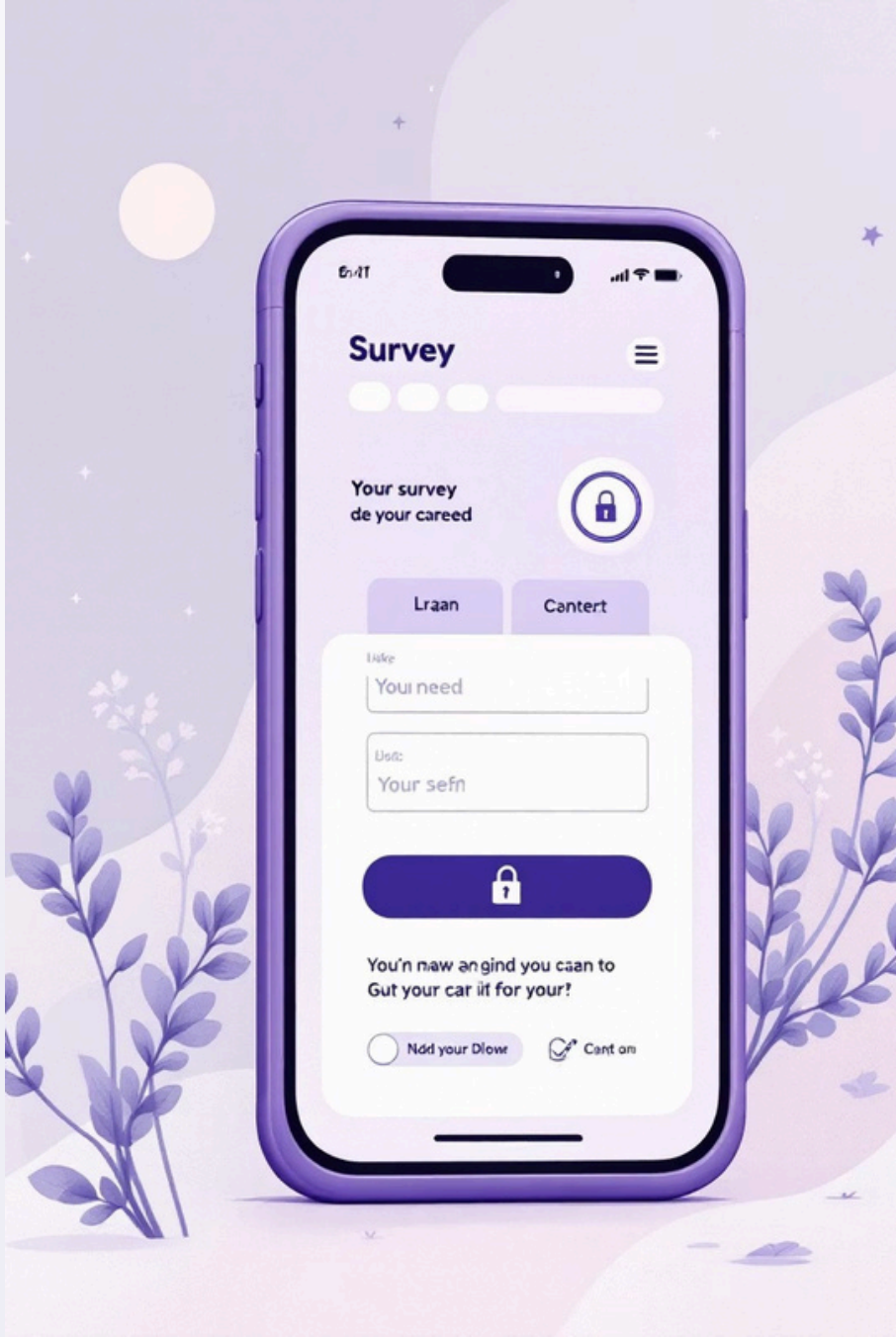
RELAZIONE PROJECT WORK

SviluppodiunApplicativoperSondaggi Sicuro

Il progetto del nostroGruppo (GANJA) si è concentrato sulla realizzazionedi un

applicativo per la creazione e la votazione di sondaggi. L'obiettivo principale era applicare le conoscenze acquisite per securizzare l'applicazione tramite policy e meccanismi di autenticazione avanzati.

Il team è composto da: Giovanni Della Puca, Ayman Mannas, Niccolò Maraldi, Jamshid Quraishi e Alessio Apopei.



Obiettivi e Specifiche del Progetto

Interfaccia Utente Navigabile

Sviluppodiun'interfaccia utenteintuitiva con funzionalità di ricerca avanzata.

SistemadiAutenticazioneaDue Ruoli

Implementazione di un sistemasicuroper

Utenti standard e Amministratori.

Gestione Dati Personali

Adozionediprocedure conformial GDPR per la gestione sicura dei dati.

Il progetto richiedeva la creazione di un'AREA UTENTE per la votazione e lo storico dei sondaggi, e una dashboard Admin per la creazione e la gestione aggregata e anonimizzata dei sondaggi. Ogni utente deve poter visualizzare il numero totale di voti espressi per sondaggio.

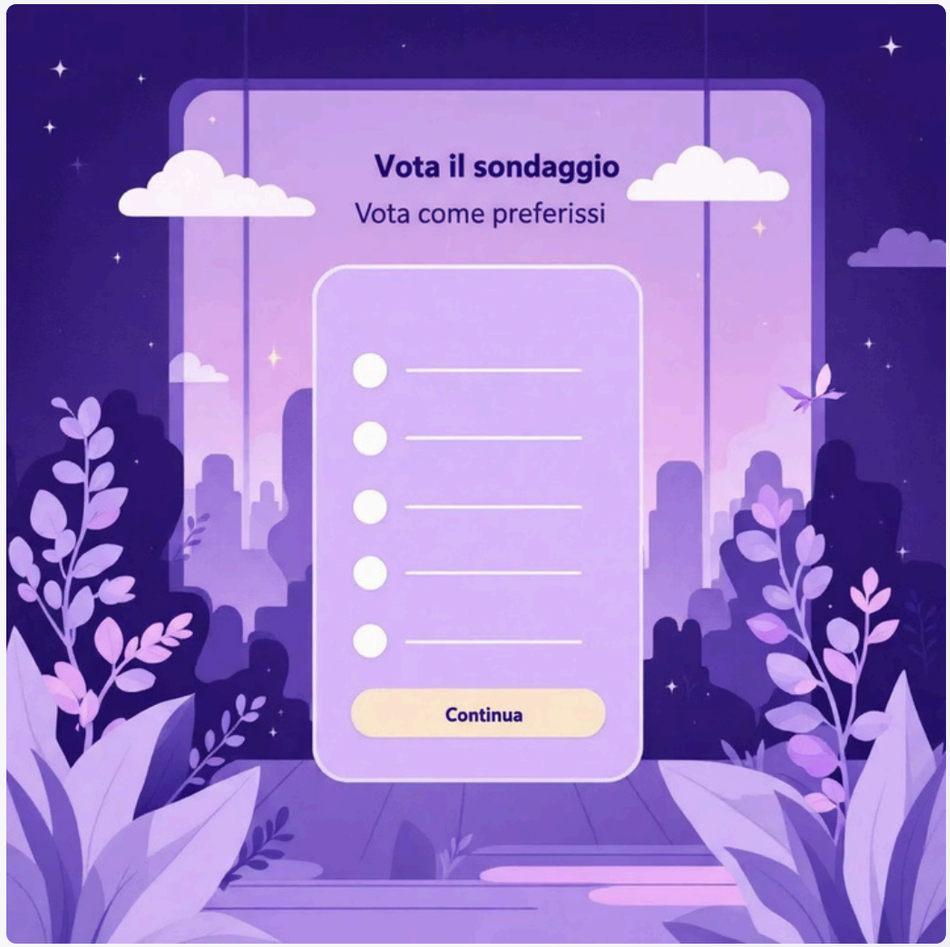
Analisi Dei Requisiti: Funzionalità per Ruolo

Utente Standard

- Visualizzazione dell'elenco dei sondaggi disponibili per la votazione.
- Pagina dedicata per la votazione del singolo sondaggio.
- Storico dei sondaggi già votati.
- Visualizzazione del numero di voti espressi per sondaggio.
- Possibilità di ricerca mirata tramite utilizzo di filtri.

Utente Admin

- Dashboard per creare e gestire i sondaggi. Visualizzazione dei
- risultati in forma aggregata e anonimizzata. Funzionalità di
- gestione utenti (disabilitazione ed eliminazione).



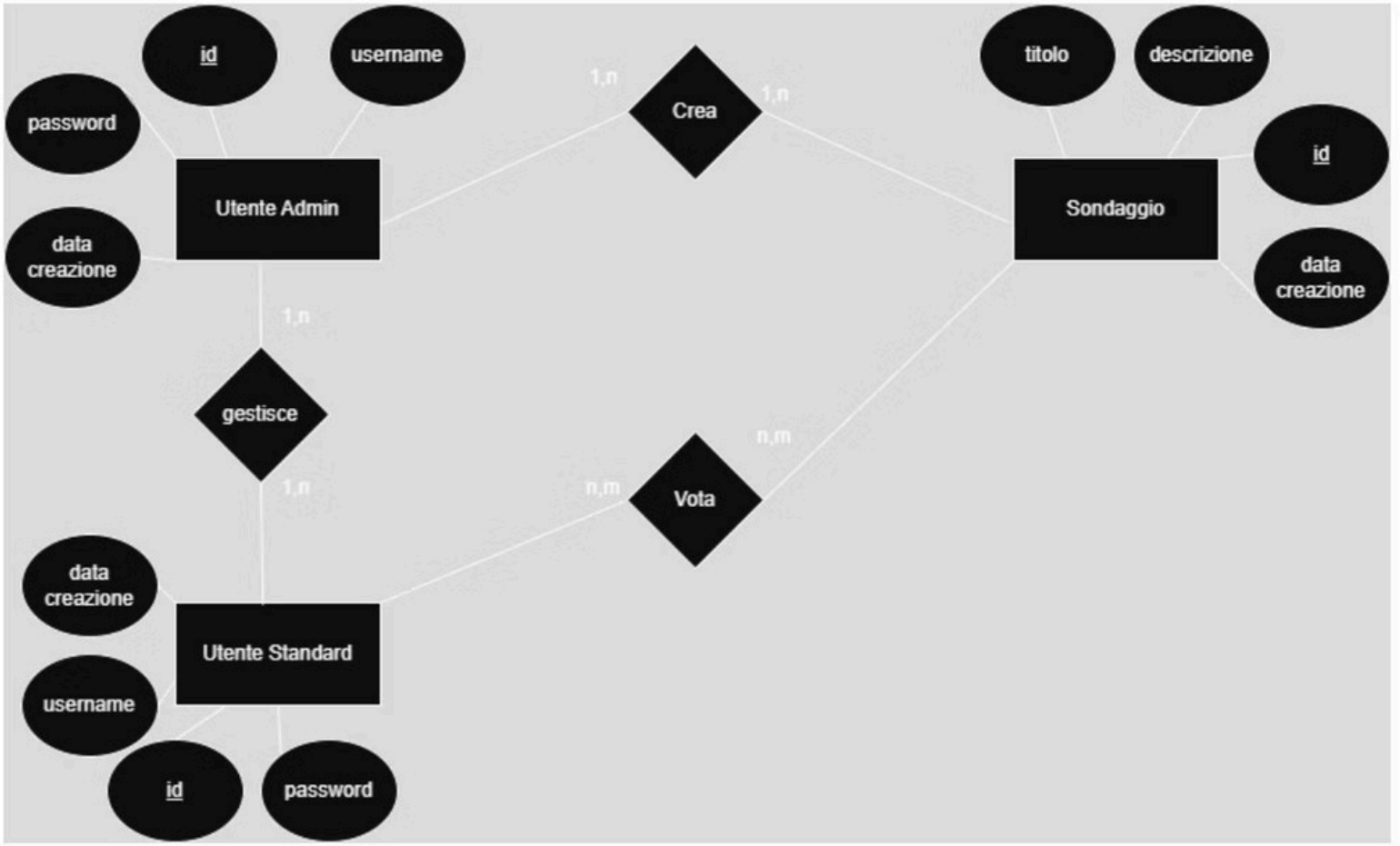
Base Dati Dell'Applicativo

Ilmodellodibasedatièstatoprogettatoperdistingueregliutentistandard dagli amministratori tramite un attributo binario, ottimizzando la struttura del database.

> Gli utenti standard e admin condividono gli stessi attributi, perciò abbiamo optato nella creazione effettiva del database finale di distinguerli attraverso un attributo binario per non appesantire inutilmente il database.

La versione finale dell'utente include: id univoco, username e password obbligatori, attributi binari per lo stato attivo e i privilegi di amministratore, e data di creazione.

Diagramma ER Gerarchico:



Ruoli e Privilegi Dettagliati

Privilegi Utente Standard

L'utente standard haun'interfaccia personale per consultare le proprie votazioni e votare i sondaggi disponibili. Non gode di altri privilegi.

Privilegi Utente Admin

L'adminpuòcreare edeliminare sondaggi, visualizzare i voti (anonimi), disabilitare utenti (impedendo il login, mantenendo la memorizzazione) ed eliminare utenti.

Tecnologie Utilizzate per lo Sviluppo

Perlarealizzazionedelsitodisondaggiedeldatabase,abbiamosceltoduetecnologieopen-source ampiamente diffuse e consolidate nel web development.

PHP (Hypertext Preprocessor)

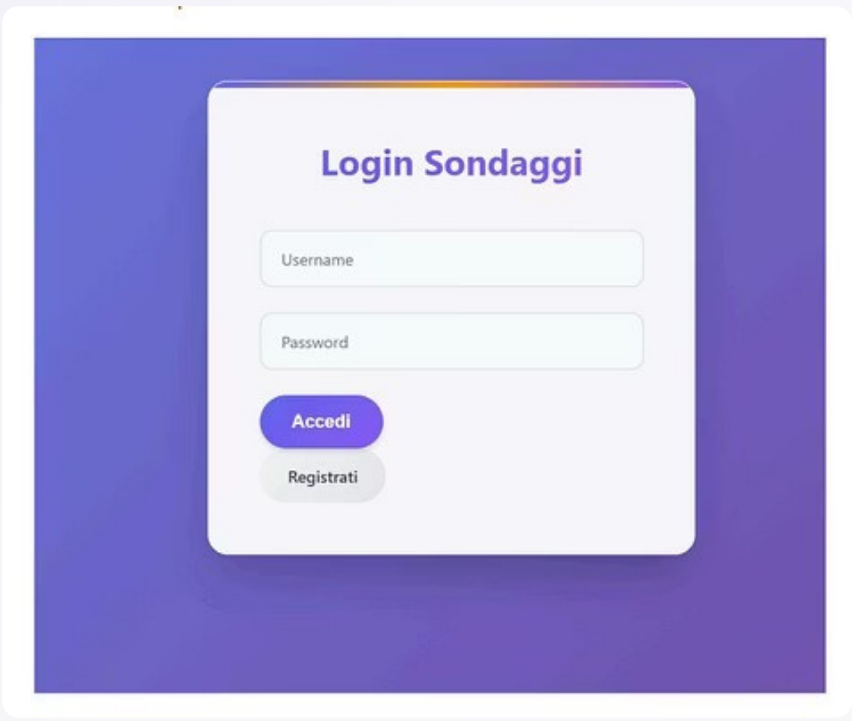
Linguaggio di scripting open-source e general-purpose, particolarmente indicato per lo sviluppo web lato server (backend). L'implementazione è stata realizzata tramite Visual Studio Code.

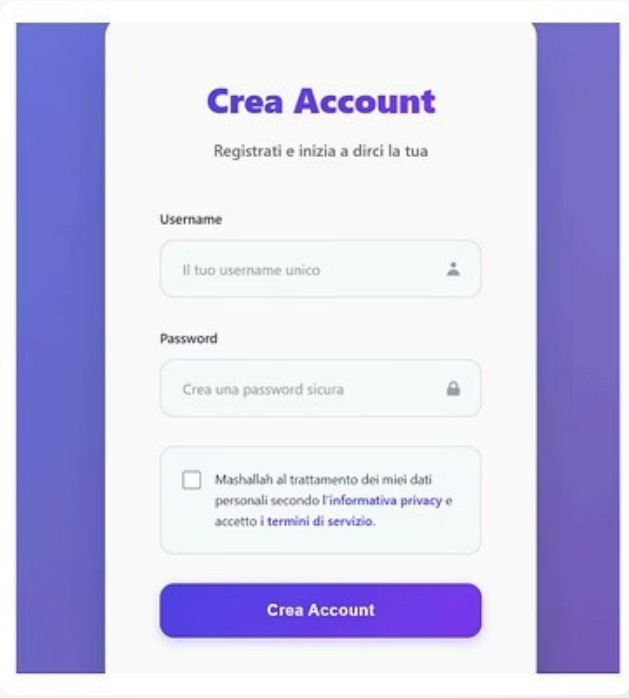
MySQL

Sistema di Gestione di Database Relazionali (RDBMS) open source, essenziale per l'archiviazione dei dati. È parte integrante dell'ambiente LAMP (Linux, Apache, MySQL, PHP/Perl/Python).

Istruzioni per l'Uso: Accesso e Registrazione

L'accessoall'applicativoiniziadallapaginadilogin,dovegliutentiesistentipossonoautenticarsi. I nuoviutentivengono reindirizzati alla pagina di registrazione.



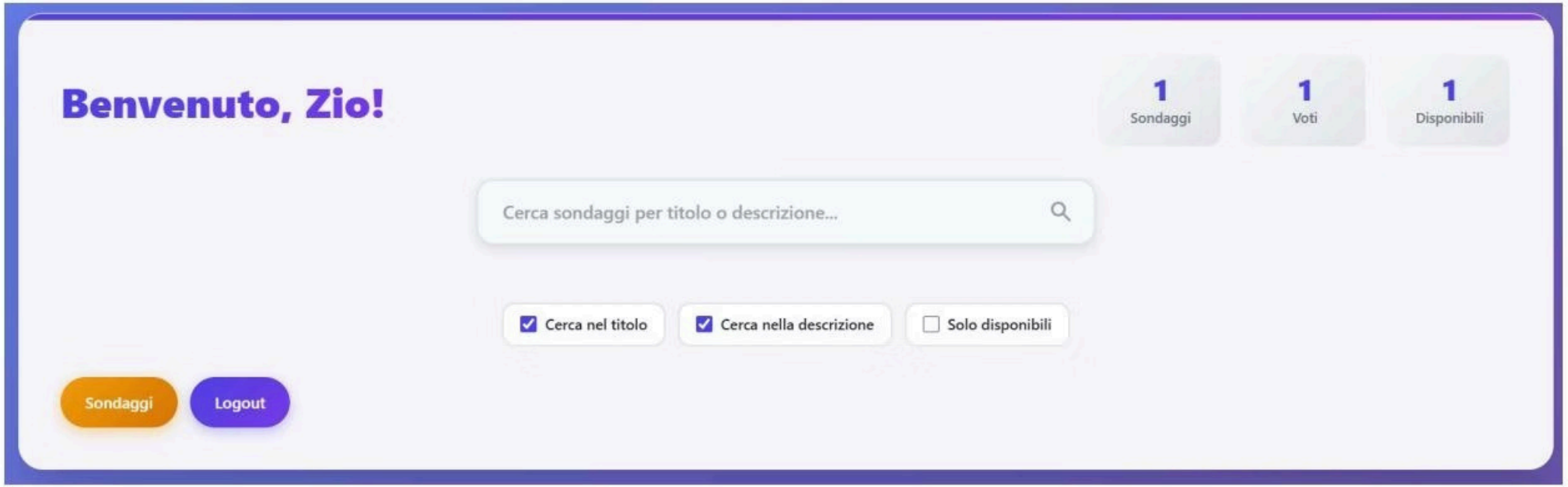


Per registrarsi è necessario inserire un username univoco e una password sicura. In caso di argomenti non idonei (es. username già utilizzato o password troppo corta), compare un messaggio di errore esplicativo per guidare l'utente alla correzione.

Area Utente Standard: Navigazione e Votazione

Dopol'autenticazione,l'utenteaccedeallapropriaareapersonale,cherispettalespecifichediun'interfaccianavigabileconbarradi ricerca.

- Elenco dei sondaggi disponibili.
- Storico delle partecipazioni.
- Icona "vota ora" per i sondaggi non ancora votati.



L'interfaccia presenta un elenco dei sondaggi disponibili e uno storico degli ultimi sondaggi votati.

La votazione avviene cliccando sull'icona "vota ora", che reindirizza alla pagina di votazione per esprimere la preferenza tra le opzioni disponibili. Dopo la votazione, l'interfaccia mostra l'opzione "vincitrice" (quella con più voti) o indica un pareggio.

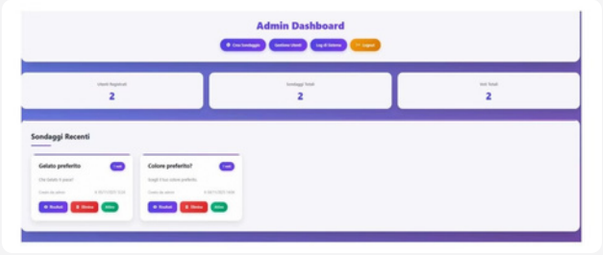
Dashboard Amministratore: Gestione Completa

L'amministratore ha accesso a una dashboard completa per la gestione dei sondaggi e degli utenti.

1

Gestione Sondaggi

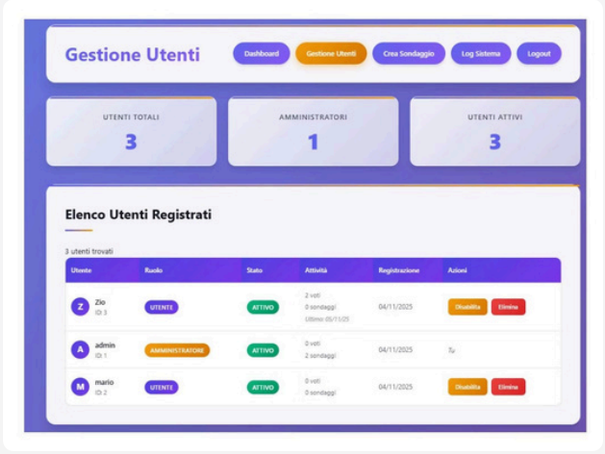
Storico dei sondaggi recenti con opzioni di visualizzazione ed eliminazione. Possibilità di vedere i voti in forma anonima.



2

Gestione Utenti

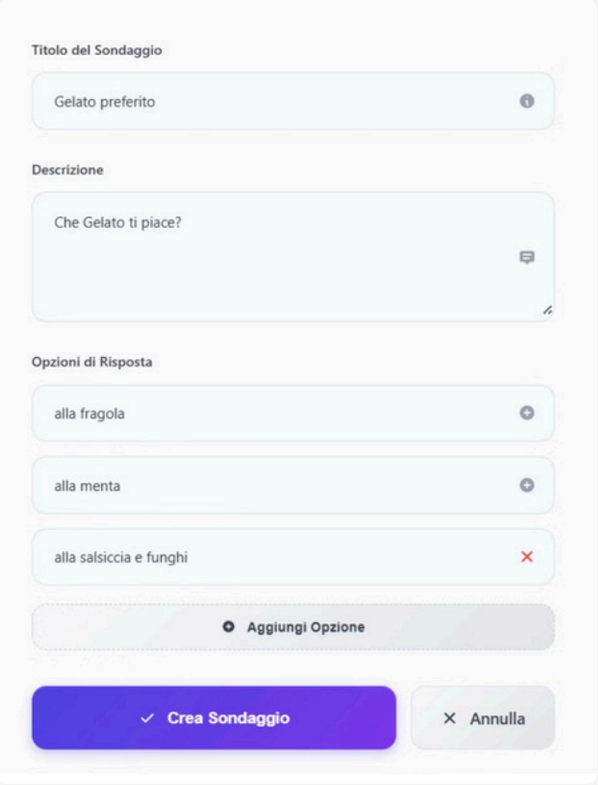
Pannello dedicato per visualizzare tutti gli utenti registrati, con la facoltà di disabilitare o eliminare i loro account.



3

Creazione Sondaggi

Pagina di creazione per compilare i campi richiesti e aggiungere un minimo di due opzioni di voto.



Implementazioni sulla Sicurezza

Lasicurezzaèstataun puntofocaledel progetto, conl'introduzionedi diversemisure robuste per proteggere i dati sensibili e garantire l'integrità dell'applicazione.Sono statiimplementati standard elevatipermitigare levulnerabilità comuni.

Sicurezza Password Avanzata

Per la creazione delle password, è stato imposto un limite minimo di **8 caratteri** e requisiti di complessità che includono l'uso di lettere maiuscole e minuscole, numeri e caratteri speciali. Le password vengono archiviate nel database esclusivamente tramite **hashing crittografico forte**, utilizzando l'algoritmo **Bcrypt**. Ogni password è salata individualmente (con un "salt" univoco generato casualmente) prima dell'hashing, rendendo le rainbow table inefficaci e proteggendo dagli attacchi di forza bruta anche in caso di violazione del database. Le password non sono mai memorizzate in chiaro.

Prevenzione IDOR (Insecure Direct Object Reference)

Per prevenire vulnerabilità IDOR, è stata implementata una verifica rigorosa dell'autorizzazione per ogni richiesta che accede a risorse sensibili. Gli identificatori degli oggetti non sono sequenziali, ma UUID (Universally Unique Identifier) o ID opachi per ridurre la prevedibilità. L'applicazione esegue controlli a livello di server per assicurarsi che l'utente autenticato sia effettivamente autorizzato ad accedere o modificare l'oggetto richiesto, basandosi su un sistema di **controllo degli accessi basato sui ruoli (RBAC)** e token di autenticazione (es. **JWT** o sessioni sicure), garantendo che solo gli utenti con i permessi corretti possano interagire con le risorse pertinenti.

Anonimato Assoluto dei Voti

L'anonimato dei voti espressi è garantito da una progettazione architetturale specifica. I voti sono registrati in modo completamente disaccoppiato dall'identità dell'utente. Ciò significa che non esiste alcun collegamento diretto o indiretto tra un voto specifico e l'utente che lo ha espresso nel database. Nessuno, inclusi gli amministratori del sistema o il personale di supporto tecnico, è in grado di risalire all'utente responsabile di un determinato voto, assicurando la massima imparzialità e privacy.

Controllo Admin e Audit Trail

L'utente con ruolo di amministratore gode di privilegi elevati, gestiti tramite un sistema RBAC (Role-Based Access Control) dedicato. Questo ruolo consente di disabilitare o eliminare account di utenti standard, mantenere l'ordine e la sicurezza sulla piattaforma. L'accesso alle funzionalità admin è protetto da autenticazione forte e, per maggiore sicurezza, tutte le azioni critiche eseguite dagli amministratori sono registrate in un **audit trail**, che permette di tracciare le modifiche e monitorare l'attività, fornendo un controllo essenziale e trasparenza sulle operazioni di gestione.

Sicurezza Password Avanzata

Lasicurezza dellepasswordècruciale.Eccolenostreimplementazioni:

- **Requisiti minimi:** 8 caratteri con complessità.
- **Algoritmo Bcrypt:** Per hashing crittografico forte.
- **Salt univoco:** Generato casualmente per ogni password, rendendo le rainbow table inefficaci.
- **Protezione avanzata:** Contro rainbow table e attacchi di forza bruta, anche in caso di violazione del database.
- **Non in chiaro:** Le password non sono mai memorizzate in chiaro nel database.

Questo approccio garantisce la massima protezione contro le minacce più comuni e salvaguarda l'integrità dei dati degli utenti.

Prevenzione IDOR (Insecure Direct Object Reference)

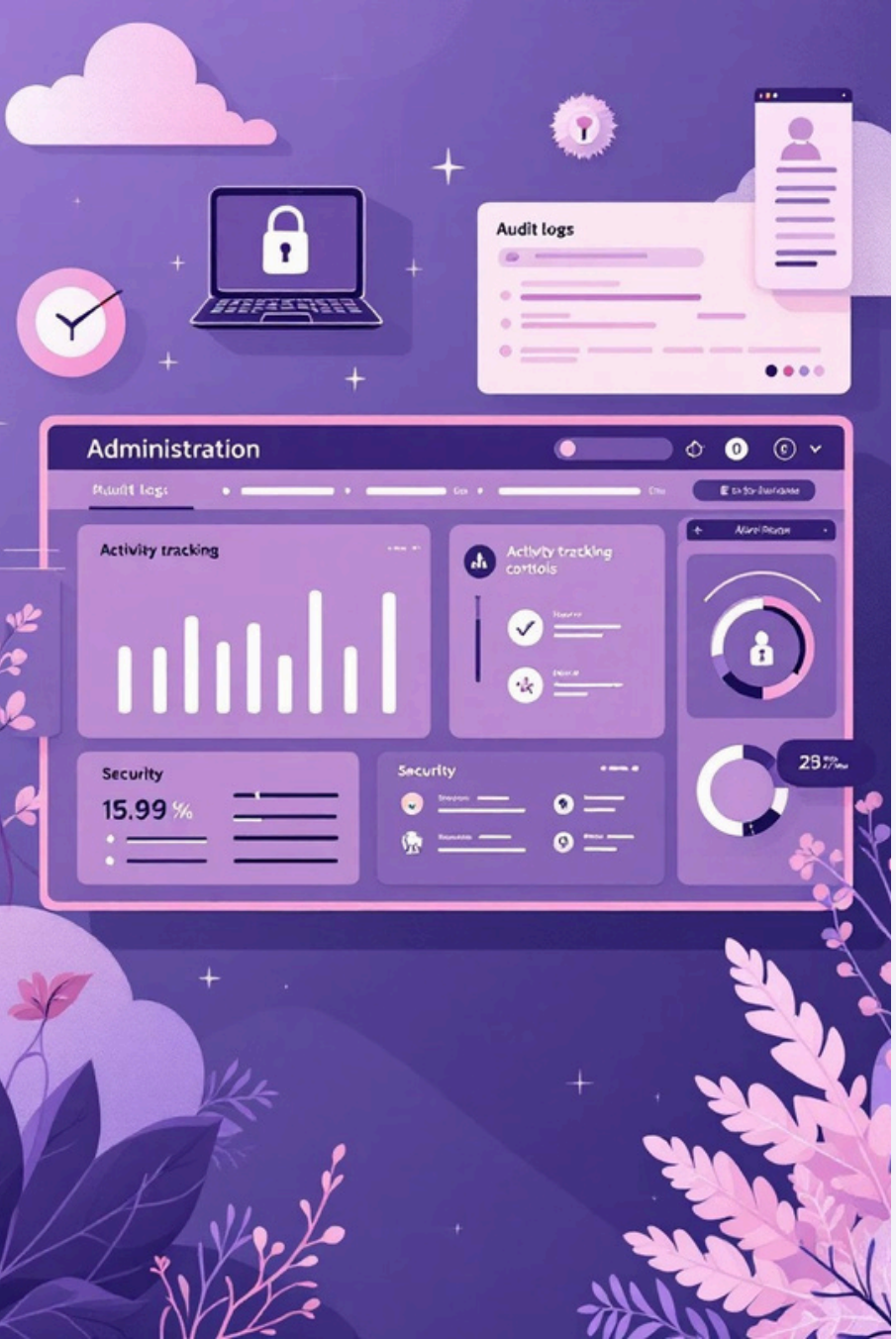
- **Verifica rigorosa dell'autorizzazione** per ognirichiesta.
- **Identificatorinon sequenziali:** UUID o ID opachiperridurrelaprevedibilità.
- **Controlli a livello server** per le autorizzazioni.
- **Sistema RBAC (Role-Based Access Control)**.
- **Token di autenticazione** (JWT o sessioni sicure).
- Solo gli utenti con i permessi corretti possono accedere alle risorse.

Questo approccio garantisce che ogni interazione con le risorse sia legittima e autorizzata, proteggendo l'integrità dei dati e la privacy degli utenti.

Anonimato Assoluto dei Voti

L'anonimatodei votiespressiè garantitodauna progettazione architetturale specifica.

- I voti sono registrati in modo completamente disaccoppiato dall'identità dell'utente.
- Non esiste alcun collegamento diretto o indiretto tra un voto specifico e l'utente che lo ha espresso nel database.
- Nessuno, inclusi gli amministratori del sistema o il personale di supporto tecnico, è in grado di risalire all'utente responsabile di un determinato voto.
- Massima imparzialità e privacy garantita.
- Protezione dell'identità degli elettori.



Controllo Admin e Audit Trail

- L'utente con ruolodi amministratore godediprivilegielevati, gestiti tramite un sistema **RBAC (Role-Based AccessControl)** dedicato.
- Questo ruolo consente di disabilitare o eliminare account di utenti standard, mantenere l'ordine e la sicurezza sulla piattaforma.
- L'accesso alle funzionalità admin è protetto da autenticazione forte.
- Tutte le azioni critiche eseguite dagli amministratori sono registrate in un **audit trail**.
- L'audit trail permette di tracciare le modifiche e monitorare l'attività.
- Fornisce controllo essenziale e trasparenza sulle operazioni di gestione.