RELAZIONE PROJECT WORK

Gruppo 1

Giovanni Della Puca, Ayman Mannas, Niccolò Maraldi, Jamshid Quraishi, Alessio Apopei

1. Presentazione

Il progetto scelto dal nostro gruppo verteva sulla realizzazione di un applicativo relativo alla creazione di sondaggi da parte di utenti con particolari privilegi (Utenti Admin) e alla votazione dei suddetti sondaggi da parte di utenti standard (vedi paragrafo 3), lo scopo del progetto è di applicare quanto appreso durante il nostro percorso per securizzare l'applicativo tramite l'applicazione di determinate policy e meccanismi di autenticazione (vedi paragrafo 6)

Le specifiche generali relative ad ogni progetto sono: lo sviluppo di un'interfaccia utente navigabile con ricerca avanzata, l'implementazione di un sistema di autenticazione sicuro a due ruoli (Utenti/Amministratori) e l'adozione di procedure per la gestione sicura e conforme al GDPR dei dati personali.

2. Analisi Dei Requisiti

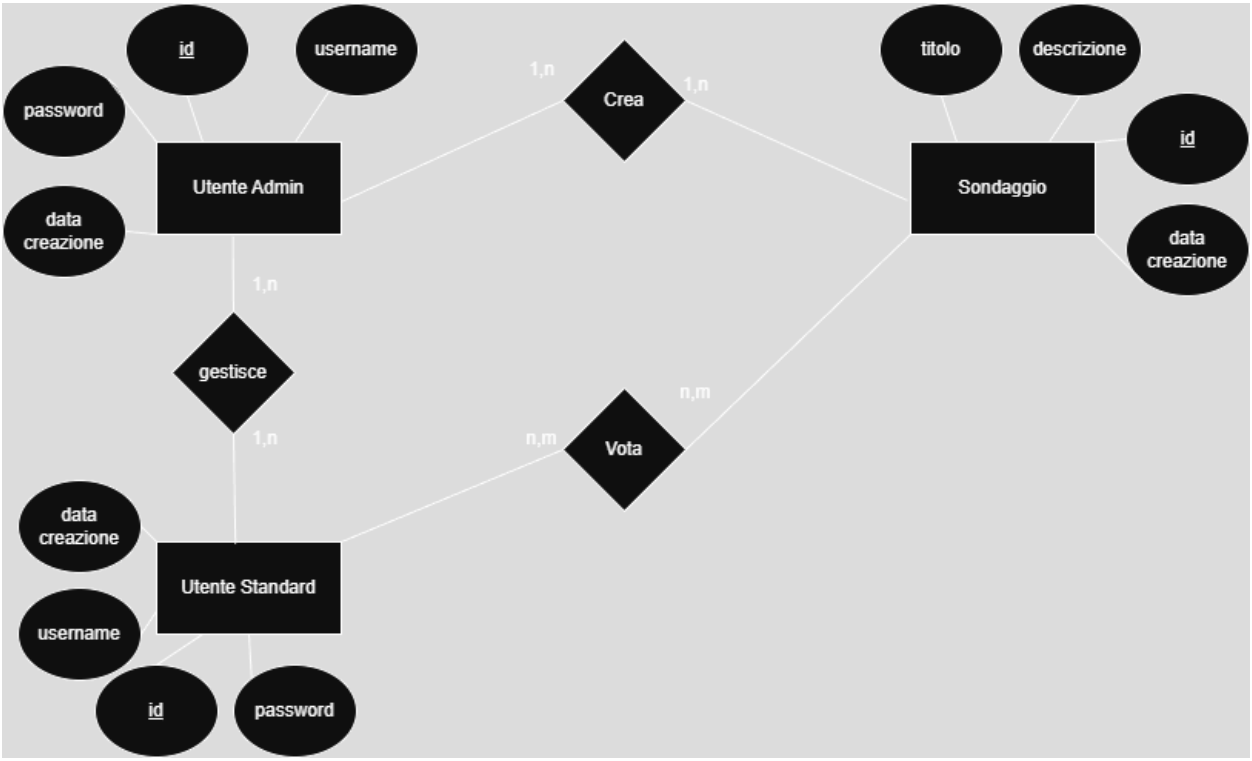
Per la realizzazione dell'applicativo ci è stato richiesto di implementare un'AREA UTENTE che presentasse a ciascuno degli utenti standard l'elenco dei sondaggi disponibili per la votazione, una pagina dedicata alla votazione del singolo sondaggio, lo storico dei sondaggi nei quali si è già espresso un voto; mentre per gli utenti admin una dashboard per creare e gestire i sondaggi in forma aggregata e anonimizzata.

Per finire ogni utente deve poter essere in grado di visualizzare il numero di voti espressi

per sondaggio.

3. Base Dati Dell'Applicativo

di seguito un semplice modello ER esplicativo della gerarchia dell'applicativo



Come si può notare gli utenti standard ed 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.

L' utente standard ha una sua interfaccia personale, nella quale è possibile consultare le proprie votazioni, e votare i sondaggi disponibili, ma oltre a questi permessi base non godono di altri privilegi.

L'utente admin è in grado di creare ed eliminare sondaggi, visualizzare i voti di ciascun sondaggio, disabilitare utenti (vale a dire impedirgli di loggarsi, abbiamo implementato questa funzione sebbene non fosse richiesta per una questione di realisticità, infatti riteniamo che un amministratore per svolgere la propria funzione debba essere in grado di disabilitare un utente pur mantenendolo memorizzato) ed eliminare utenti

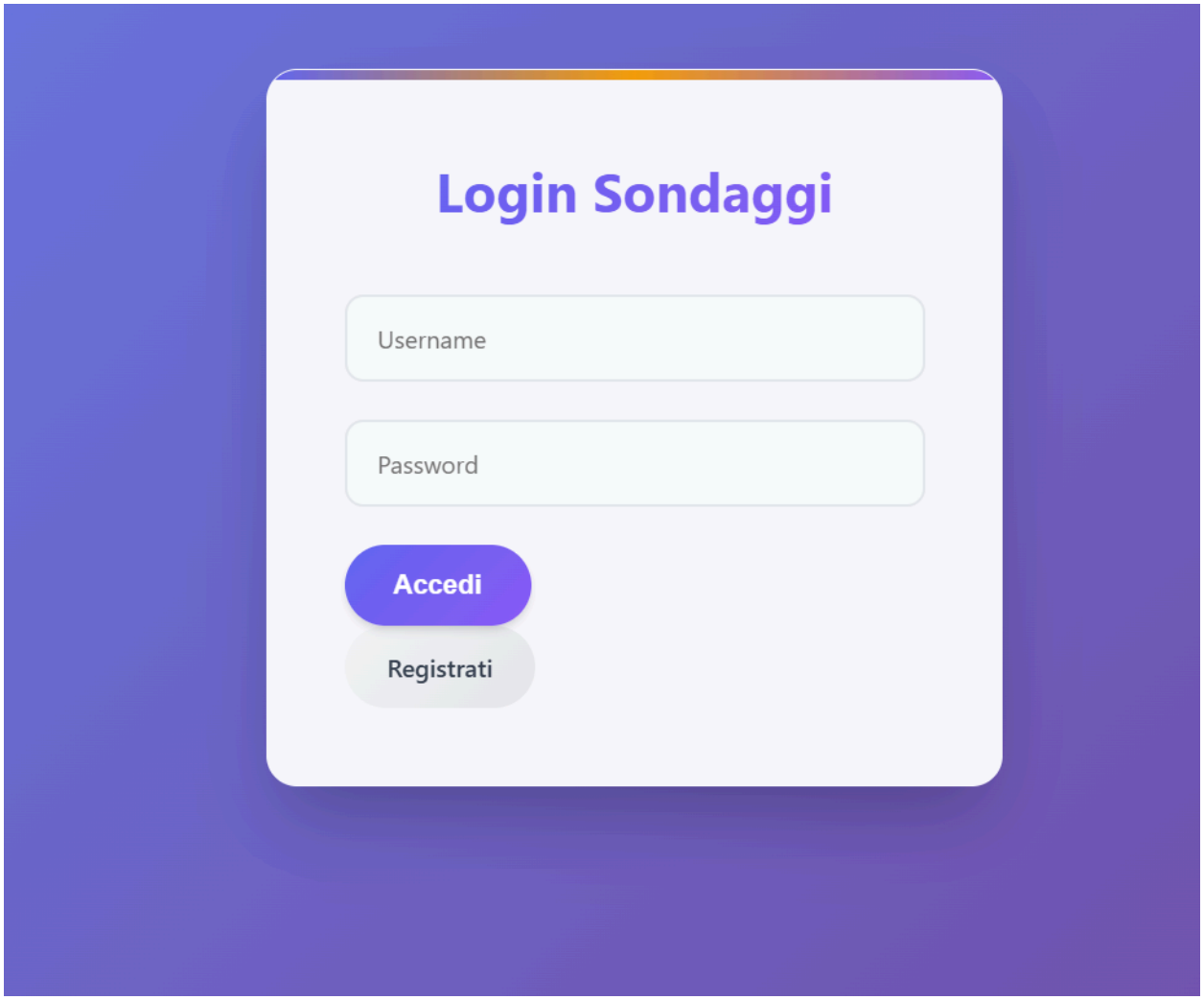
```
CREATE TABLE users (
    id INT AUTO_INCREMENT PRIMARY KEY,
    username VARCHAR(50) UNIQUE NOT NULL,
    password VARCHAR(255) NOT NULL,
    is_admin TINYINT(1) DEFAULT 0,
    is_active TINYINT(1) DEFAULT 1,
    created_at DATETIME DEFAULT CURRENT_TIMESTAMP
);
```

Nella versione finale l'utente si presenta in questo modo: id univoco, username e password obbligatori, attributi binari per stabilire se è attivo e se gode dei privilegi amministratore e data di creazione.

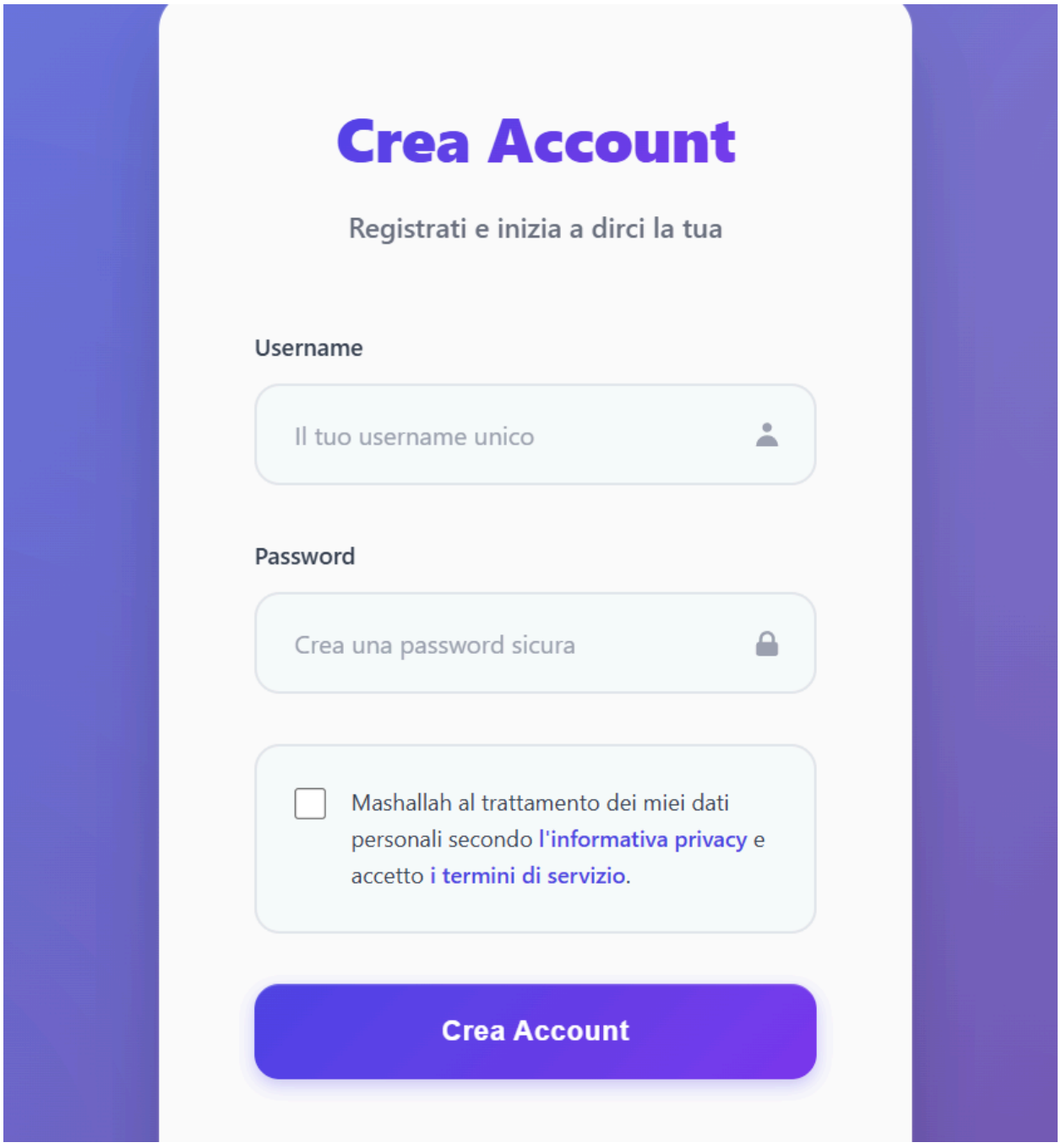
4. Tecnologie utilizzate

Per il sito di sondaggi ci siamo avvalsi di PHP, (**P**HP: **H**ypertext **P**reprocessor) è un **linguaggio di scripting open-source** e **general-purpose** (ad uso generico), particolarmente indicato e ampiamente utilizzato per lo **sviluppo web lato server (backend)**, scritto tramite l'app Visual Studio Code mentre per il database abbiamo usato MySql (**Sistema di Gestione di Database Relazionali (RDBMS)** *open source* molto popolare e ampiamente utilizzato. È parte integrante dello sviluppo web, in particolare negli ambienti **LAMP** (Linux, Apache, MySQL, PHP/Perl/Python).)

5. Istruzioni per l’uso



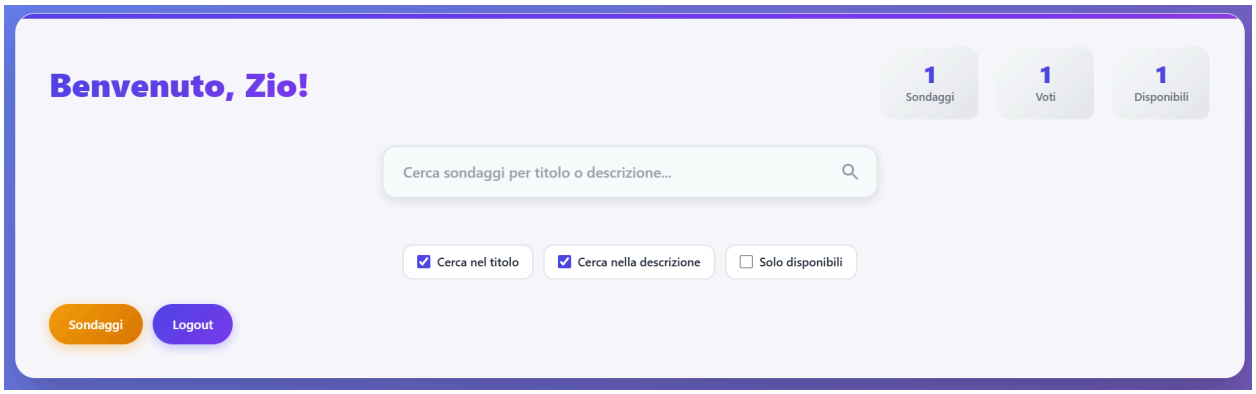
Accedendo al sito per la prima volta ci si trova di fronte alla pagina di login, dove è possibile autenticarsi se si è già in possesso di un account, in caso contrario sarà necessario cliccare sul pulsante “Registrati” e si sarà reindirizzati alla pagina di registrazione



Qui per registrarsi sarà necessario inserire un username univoco e una password sicura, in caso gli argomenti forniti dall'utente non dovessero essere idonei comparirà un messaggio di errore esplicativo degli aggiustamenti necessari

(Messaggi di errore in caso di username già utilizzato e password troppo corta)

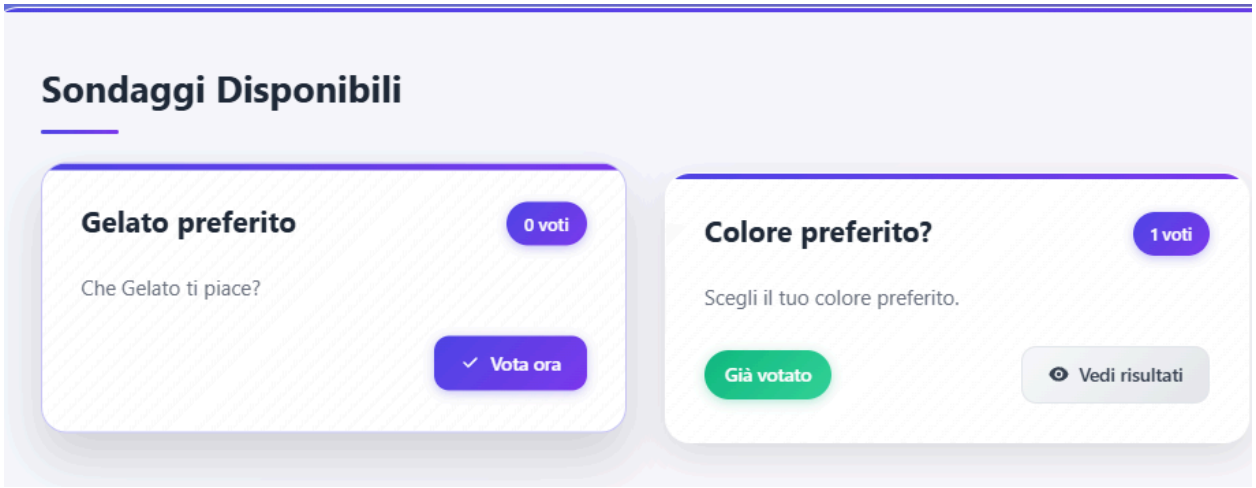
Dopo essersi registrati con successo è possibile accedere alla propria area utente, la quale presenta come richiesto dalle specifiche assegnate un'interfaccia utente navigabile con barra di ricerca



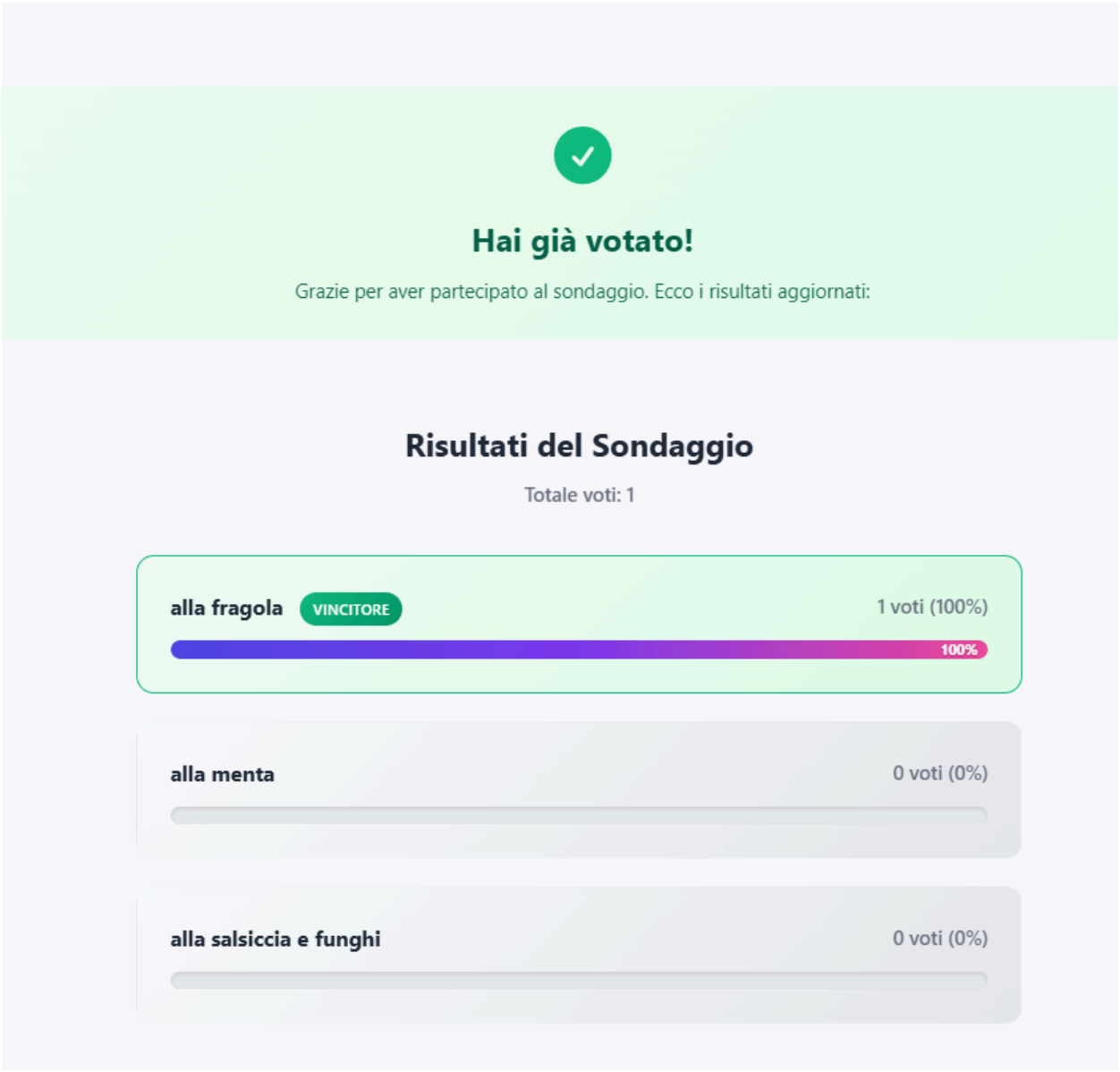
Un elenco dei sondaggi disponibili

E uno storico degli ultimi sondaggi ai quali si è preso parte

per votare un sondaggio è sufficiente cliccare sull'icona "vota ora" che comparirà nei sondaggi disponibili ai quali non si è ancora preso parte

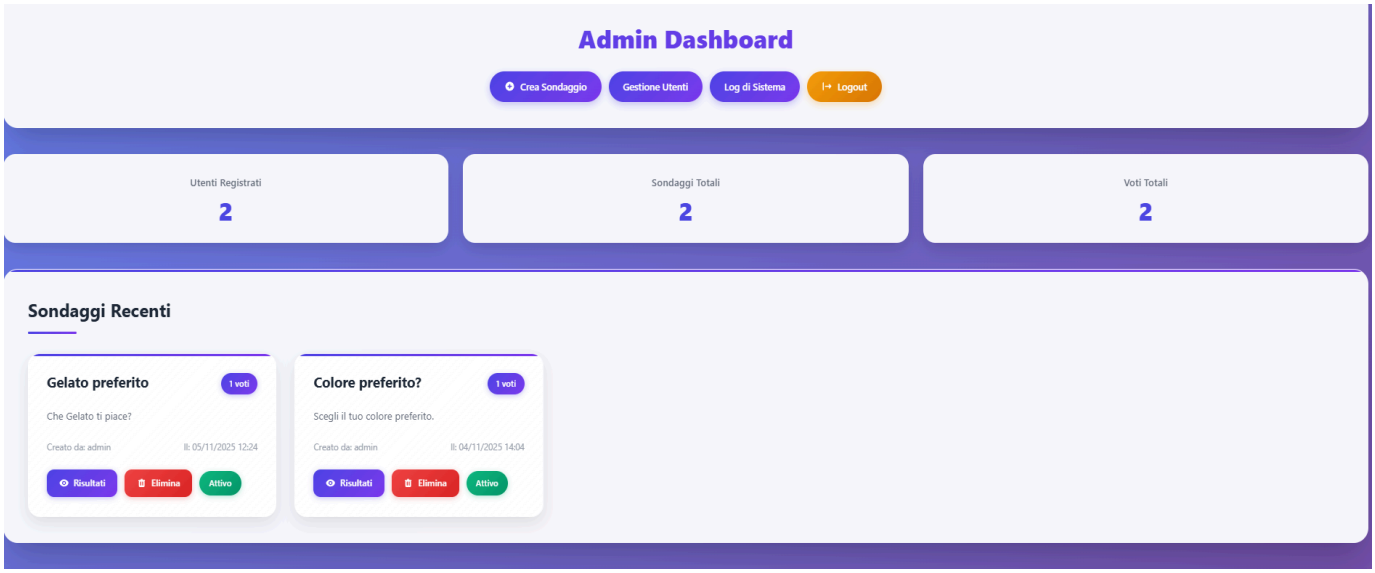


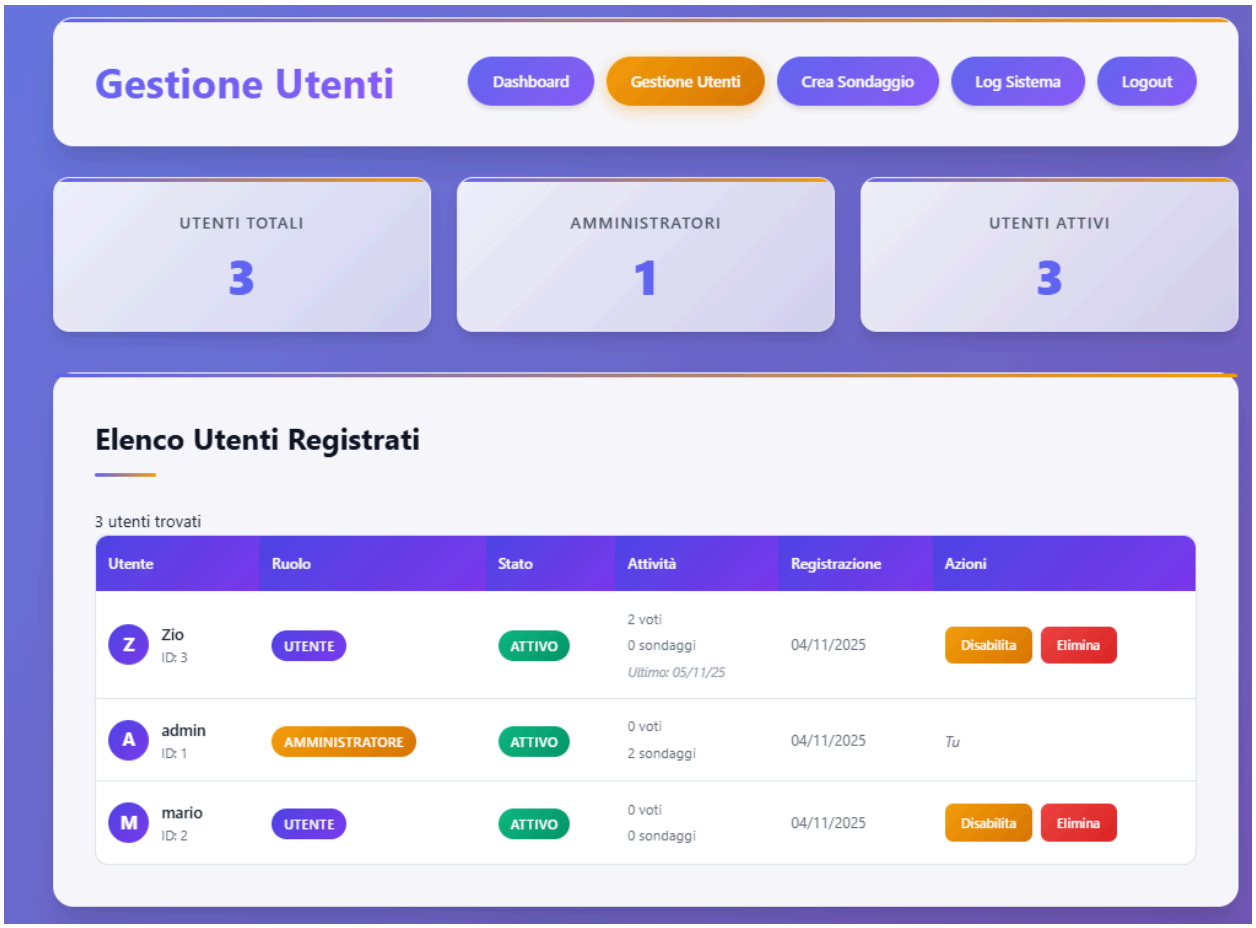
Si arriverà così alla pagina di votazione, dove si potrà esprimere la propria preferenza.



Dopo la votazione l'interfaccia cambierà mostrando l'opzione con più voti (vincitore) (in caso di pareggio le due opzioni con più voti mostreranno la scritta "pari")

Se invece si è effettuato il login come amministratore la admin dashboard si presenta così, lo storico dei sondaggi recenti è corredato di opzioni di visualizzazione ed eliminazione ma mantiene la possibilità di visualizzare i voti degli utenti in forma anonima





accedendo al pannello per la gestione degli utenti possiamo vedere tutti gli utenti registrati, disabilitare i loro account ed eliminarli

Per creare un nuovo sondaggio è sufficiente cliccare su “Crea Sondaggio”, si verrà reindirizzati alla pagina di creazione nella quale si dovranno compilare i campi richiesti. E’ possibile aggiungere quante opzioni si desidera con un minimo di due

Crea Nuovo Sondaggio

Compila i campi per creare un nuovo sondaggio

Titolo del Sondaggio

Gelato preferito

Descrizione

Che Gelato ti piace?

Opzioni di Risposta

alla fragola

alla menta

alla salsiccia e funghi

Aggiungi Opzione

Crea Sondaggio

Annulla

6. Implementazioni sulla sicurezza

Abbiamo posto un limite minimo di caratteri durante la creazione della password, abbiamo deciso consapevolmente di non introdurre un obbligo di caratteri speciali o maiuscole lasciando l'immissione di quest'ultimi a discrezione del singolo utente per una questione di comodità del fruitore del servizio.

Abbiamo introdotto, come da specifiche, l'hash della password che viene archiviata nel database criptata.

In oltre, abbiamo fatto in modo di prevenire IDOR (**I**nsecure **D**irect **O**bject **R**eference)

Una vulnerabilità IDOR si verifica quando un'applicazione web o un'API **espone un riferimento diretto a un oggetto interno** (come un ID di un record, un nome di file o una chiave in un database) basandosi sull'input fornito dall'utente, ma **non verifica correttamente** che l'utente sia effettivamente autorizzato ad accedere a quell'oggetto, di conseguenza abbiamo fatto si che fosse necessario autenticarsi.

L'anonimato dei voti espressi degli utenti è garantito, dal momento che nessuno, admin compresi, sono in grado di vedere quale utente ha espresso un dato voto.

In caso lo ritenga necessario l'utente admin ha la possibilità di disabilitare ed eliminare gli account di qualsiasi utente standard.