

CV Manager

Sviluppo del Frontend

Il frontend, ossia la parte dell'applicazione visibile, viene utilizzata direttamente dagli utenti. L'obiettivo principale era quello di creare un'interfaccia moderna, intuitiva e coerente, capace di integrarsi con il backend per offrire un'esperienza d'uso fluida per studenti e amministratori.

Il lavoro si è composto da una fase di progettazione grafica e strutturale, definendo l'organizzazione delle pagine e la disposizione degli elementi.

Poi sono state realizzate le principali sezioni del sito, ovvero la pagina di login , registrazione, home page, dashboard utente per la gestione dei propri dati e del curriculum e la dashboard amministrativa per la visualizzazione degli utenti e dei file caricati.

Ogni pagina è stata sviluppata in HTML e collegata dinamicamente al backend tramite variabili Python, in modo che i contenuti potessero aggiornarsi automaticamente in base al tipo di utente o al ruolo.

Tutta la parte grafica è stata curata attraverso il file style.css. prediligendo uno stile semplice e coerente, con colori neutri e accenti visivi che rendono l'interfaccia moderna e gradevole.

Inoltre è stato accentuato l'aspetto responsive, cercando di adattare il sito a diverse risoluzioni e dispositivi.

Una parte importante dello sviluppo del frontend ha riguardato la validazione dei dati lato client, realizzata interamente in JavaScript nel file [validation.js](#).

Ogni modulo del sito effettua controlli in tempo reale sui dati inseriti dagli utenti, verificando la correttezza di email, password, link e file caricati. In particolare, per la sezione di upload del CV sono stati implementati controlli che accettano solo documenti PDF fino a un massimo di 5 MB, con messaggi di errore personalizzati.

L'interfaccia è stata progettata per essere accessibile e funzionale, con testi ben leggibili, colori a contrasto e pulsanti chiari.

Nella pagina dedicata alla privacy la stesura e presentazione dei contenuti è stata gestita con particolare cura, in modo che l'utente potesse comprendere facilmente le modalità di trattamento dei dati e i diritti previsti dal GDPR, cercando di mantenere la comunicazione chiara e coerente con il principio del privacy by design, integrando le informazioni legali con uno stile visivo uniforme al resto della piattaforma.

Durante lo sviluppo si è prestata attenzione anche ai dettagli estetici e all'esperienza complessiva di navigazione, cercando un equilibrio tra funzionalità e design.

Sviluppo del Backend

La parte logica e funzionale dell'applicazione che gestisce il flusso dei dati, le operazioni sul database e la comunicazione con il frontend.

L'obiettivo è stato quello di costruire un'infrastruttura stabile, sicura e ben organizzata, capace di supportare in modo efficiente tutte le funzionalità principali del sistema, come la registrazione e l'autenticazione degli utenti, la gestione dei curriculum vitae in formato PDF e la generazione automatica dei report.

Il backend è stato sviluppato in linguaggio Python e si basa su un server HTTP personalizzato, creato utilizzando il modulo nativo "http.server".

L'intero sistema è stato strutturato in modo modulare, suddividendo il codice in più file, ciascuno con una responsabilità specifica:

- uno dedicato alla gestione delle richieste web e delle sessioni utente
- uno per le operazioni sul database,
- uno per la generazione dei PDF
- un altro per i moduli di supporto per la gestione dei dati e delle dashboard.

Il database utilizzato è MySQL.

lo schema dati è facilmente estendibile, definendo le tabelle principali

- "users" – memorizzare le informazioni sugli utenti
- "cv_data" – i dati dei loro curriculum
- "experiences" – le esperienze lavorative e formative
- "user_cvs" – i file PDF caricati

Ogni tabella è collegata tramite chiavi esterne con regole di eliminazione in cascata, così da mantenere l'integrità dei dati anche quando un utente viene rimosso dal sistema.

Dal punto di vista della sicurezza, sono stati implementati diversi accorgimenti per proteggere i dati e prevenire vulnerabilità comuni.

Le password degli utenti vengono salvate in forma cifrata grazie a un sistema di hashing con algoritmo SHA-256 e salt univoco, in modo da rendere impossibile la lettura in chiaro. Tutti gli input provenienti dagli utenti vengono filtrati e sanificati prima di essere elaborati, così da prevenire attacchi come SQL injection o cross-site scripting.

Inoltre, è stato sviluppato un semplice sistema di sessione interna che consente agli utenti di restare autenticati per 24 ore, con token generati in modo sicuro e associati a ogni login.

Le funzionalità principali del backend comprendono la registrazione e l'autenticazione degli utenti, la gestione dei profili, delle esperienze professionali e formative, e l'upload e download dei curriculum vitae in formato PDF. Ogni operazione di scrittura sul database è stata realizzata utilizzando query parametrizzate (prepared statements), per garantire sicurezza e stabilità. Il sistema distingue chiaramente i ruoli di accesso:

l'amministratore ha la possibilità di visualizzare e gestire tutti gli studenti, mentre ogni studente può accedere e modificare soltanto i propri dati.

Gli utenti possono caricare il proprio curriculum in formato ".pdf", che viene controllato lato server sia per dimensione che per estensione, in modo da evitare l'inserimento di file non validi.

I documenti vengono salvati nel server con nomi sanificati per prevenire conflitti o problemi di sicurezza, e il percorso viene registrato nel database. Oltre alla possibilità di caricare e scaricare file, e' stato sviluppato un sistema che genera automaticamente un curriculum in formato PDF a partire dai dati presenti nel database. Questo viene realizzato tramite la libreria "reportlab", che permette di creare documenti con un layout a due colonne, includendo in modo formattato i dati personali, le competenze e le esperienze del singolo utente.

Per quanto riguarda le dashboard, sono state realizzate due aree distinte: una per gli studenti e una per l'amministratore.

- La dashboard studente consente di visualizzare e aggiornare i propri dati, aggiungere esperienze e gestire i CV caricati.
- la dashboard dell'amministratore, invece, offre una panoramica completa di tutti gli utenti registrati, con statistiche sul numero di studenti, di curriculum caricati e sulle esperienze inserite, oltre alla possibilità di visualizzare o eliminare un profilo studente.

Infine, e' stata curata l'inizializzazione del database e la creazione automatica degli utenti di test, così da rendere il sistema subito funzionante dopo l'installazione. Per garantire la corretta integrazione dei moduli, e' stato scritto anche uno script di test che verifica la presenza e il corretto funzionamento delle principali componenti del server.

In conclusione, il backend che è stato sviluppato rappresenta il cuore del progetto, poiché gestisce in modo sicuro e coerente tutti i dati e le funzionalità dell'applicazione. Questo lavoro mi ha permesso di approfondire concetti fondamentali come la gestione delle sessioni, la sicurezza applicativa, l'interazione con un database relazionale e la progettazione di un'architettura server modulare.

Prove di sicurezza effettuate:

- è stato eseguito un controllo delle risorse visibili dall'esterno utilizzando gobuster senza essere loggati ma sono visibili solamente le pagine a cui un utente guest può accedere
- i caratteri utilizzati per probabili XSS sono stati sanitizzati quindi non è possibile sfruttare questa vulnerabilità
- grazie all'utilizzo di query parametrizzate non è possibile effettuare sqlinjection
- la versione del servizio non è mostrata per quanto è stata sovrascritta nel codice