

Progetto di Tecnologie Informatiche per il web Anno 2020 / 2021

Professore Piero Fraternali

Scelte di Progetto

Alessandro Mazza

Cod. Persona 10670112 Matricola 908651

Davide Marinotto

Cod. Persona 10675966 Matricola 909291

## Note Importanti

Per poter passare la fase di login è necessario conoscere mail e password, però quest'ultima come successivamente descritto e motivato è offuscata e quindi non leggibile. Per semplicità di test le **password sono sempre uguali alla mail**.

Elenco insegnanti nella base di dati di test

Matricola	Mail	Password
1	gg@tiw.it	gg@tiw.it
2	ar@tiw.it	ar@tiw.it
3	mt@tiw.it	mt@tiw.it
4	sp@tiw.it	sp@tiw.it

Elenco studenti nella base di dati di test

Matricola	Mail	Password
1	iz@tiw.it	iz@tiw.it
2	sm@tiw.it	sm@tiw.it
3	lm@tiw.it	lm@tiw.it
4	mr@tiw.it	mr@tiw.it
5	gp@tiw.it	gp@tiw.it
6	sv@tiw.it	sv@tiw.it
7	gf@tiw.it	gf@tiw.it

## Scelte di Progetto

### Personalizzazione grafica attraverso un Framework

La scelta dell'utilizzo del framework bootstrap è dovuta alla nostra necessità di avere un'interfaccia chiara e pulita quindi di facile lettura da parte dell'utente senza nessuna grafica particolarmente creativa.

Grazie a questo framework il nostro flusso di lavoro di styling produttivo è stato veloce e facilmente gestibile.

## Password offuscate nel Database

La scelta dell'offuscamento delle password è ovviamente dovuto a una necessità di sicurezza. Nel caso in cui una coppia dell'intero database o anche delle sole piccole parti venissero violate i dati non offuscati sarebbero immediatamente compromessi.

Nel nostro caso le password sarebbero comunque segrete e l'utente al sicuro in ogni servizio dove può aver usato la stessa combinazione mail password.

La funzione che abbiamo utilizzato per l'offuscamento è SHA-256 una delle più usate per il suo equilibrio tra sicurezza e costo computazionale di generazione, in quanto è un algoritmo molto efficiente per la sua elevata resistenza alle collisioni.

Un'altra delle peculiarità dell'algoritmo di hashing SHA-256 è che la lunghezza dell'hash risultante è sempre la stessa (stringa da 64 caratteri), indipendentemente dalla lunghezza del contenuto utilizzato per generare l'hash, cioè rende particolarmente efficace il salvataggio del hash nella base di dati.

Un ulteriore accorgimento che abbiamo adottato è l'aggiunta di un salt (una piccola stringa) random nel momento in cui viene applicata la funzione di hash alla password.

Questo altera l'input quanto basta per rendere un attacco a dizionario inutile e un attacco a forza bruta veramente difficile, visto che si dovrebbe attaccare sia la password che il salt quindi le combinazioni salirebbero significativamente.

## Logout e possibilità di tornare alla HomePage

In ciascuna pagina abbiamo implementato dei pulsanti che gestiscono rispettivamente il logout e la possibilità di ritornare alla propria Home Page, evitando quindi di dover fare affidamento a funzionalità interne del browser come la ricarica della pagina e migliorare quindi la navigazione.

Nella versione PureHTML questi sono aggiunti nei template tramite le anchor, mentre nella versione JavaScript al caricamento iniziale della pagina si cercano tutti i tag button con l'id corrispondente (rispettivamente logoutBtn e backToHomeBtn) e gli si applicano lo stile e il listener che implementano le rispettive funzionalità.

## Tasto per Stampare il contenuto della pagina

Presente nella sola versione JavaScript, aggiunge a diverse pagine la possibilità di stamparne il contenuto (fisicamente o anche in PDF). Tale pulsante è implementato in maniera simile a quelli di logout e back spiegati nel punto precedente (in questo caso l'id è printPage), chiamando la funzione JavaScript `window.print()`.

## Documentazione del codice

Il codice Java e JavaScript scritto per questo progetto è documentato.

La documentazione è approfondita, ma non troppo dettagliata per poter aggiornare facilmente alcuni dettagli implementativi.

La documentazione è stata fondamentale anche per il nostro coordinamento interno e per evitare di applicare pattern eccessivamente diversi per risolvere problemi simili.

Gli strumenti usati sono JavaDoc per il codice Java e JsDoc (un'estensione di javaDoc) per il codice JavaScript.

## Casi Limite gestiti

### Lato insegnante

- Insegnante senza corsi
- Corso senza appelli
- Appello senza studenti iscritti
- Verbale senza studenti da verbalizzare

### Lato Studente

- Studente senza corsi
- Corso senza appelli