Politecnico di Bari

PROGETTO CYBERSECURITY

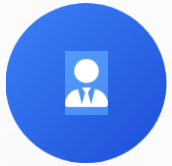
Progetto Ingegneria del Software

PASSWORD STRENGTH METER

Prof.ssa Marina Mongiello

Presentato da: Belviso-Vegliante-Didonna

Team di Sviluppo



Marco Belviso

Team Leader

m.belviso2@studenti.poliba.it

Mat. 592337

Alessio Didonna

Developer

a.didonna7@studenti.poliba.it

Mat. 592735

Giovanni Vegliante

UI/UX Designer

g.vegliante@studenti.poliba.it

Mat. 591283

Il Problema Reale

Password Deboli e Vulnerabilità

Scelte Semplificate
Combinazioni semplici, sequenze numeriche, date di nascita o nomi propri

Falsa Sensazione di Sicurezza
Utenti che erroneamente credono alle proprie password come sufficientemente sicure

Rischi di Attacco
Attacchi di forza bruta, dizionari e credenziali rubate

Impatto Economico
Violazioni di dati e perdite economiche per le aziende

Obiettivo: Approccio "Safety-First"

Valutazione Proattiva
Non solo informare, ma guidare l'utente verso scelte più sicure

Protezione dei Dati Personali
Identificazione e penalizzazione degli utilizzi di informazioni personali

Blocchi in Validazione Finale
Applicazione di regole di sicurezza che bloccano password deboli

Obiettivo del Progetto

Obiettivo Principale

Introdurre un Password Strength Meter (PSM) con approccio "safety-first" che non si limiti a informare passivamente l'utente sulla debolezza della password, ma che lo guidi attivamente verso la creazione di combinazioni robuste e sicure, prevenendo scelte rischiose fin dalla fase di inserimento.

Innovazione

Rispetto ai meter "standard", il nostro PSM introduce miglioramenti significativi focalizzandosi sull'approccio "safety-first". L'integrazione dei dati personali forniti dall'utente permette di identificare e penalizzare l'uso di informazioni facilmente prevedibili, un aspetto spesso trascurato dai sistemi tradizionali.

Funzionalità PSM

Calcolo di uno Score (0-100)

Punteggio numerico che indica la forza complessiva della password, permettendo agli utenti di comprendere immediatamente il livello di sicurezza.

Fornitura di Feedback Contestuale

Messaggi e suggerimenti in tempo reale, basati sui pattern rilevati nella password, per guidare l'utente a migliorarne la complessità.

Applicazione di Blocchi in Validazione Finale

Implementa regole di sicurezza predefinite che possono bloccare la creazione di password che non soddisfano i requisiti minimi, garantendo una maggiore protezione.

Come si Utilizza il PSM

1. Dati Personali

Inserisci nome, cognome ed email. Verranno utilizzati per valutare la password.

2. Password

Digita la password da valutare. La password non viene memorizzata.

3. Valutazione

Ottieni feedback in tempo reale sul punteggio e sulla forza della password.

4. Conferma

La password viene sottoposta a validazione finale. Verrà accettata o rifiutata.

PSM: Output e Utilità

Score (0–100)

Punteggio numerico che indica la forza complessiva della password, dove 100 rappresenta la massima sicurezza.

Motivazioni/Feedback

Messaggi contestuali che spiegano perché una password è debole e quali miglioramenti possono essere apportati.

Decisione Finale

Indicazione esplicita sull'accettabilità della password in base alle policy di sicurezza predefinite.

Esempio di Feedback

Punteggio: 39/100 Debole Non valida

Poco sicura — NON validabile: correggi i vinroli sotto.

– Lunghezza password inferiore a 8 caratteri

– Password troppo comune o prevedibile

Perché è utile

- Strumento educativo che guida l'utente verso sceite più sicure
- Previene l'adozione di password rischiose
- Rafforza la consapevolezza sulla sicurezza informatica

Motore Logico del Sistema

evaluate

- Valutazione in tempo reale della password
- Fornisce feedback immediato all'utente
- Stima della forza basata su pattern rilevati
- Score (0-100) e livello di sicurezza

validateFinal

- Applicazione delle policy di sicurezza
- Possibile blocco della registrazione
- Validazione finale basata su criteri aziendali
- Prevenzione password deboli anche se punteggio alto

Baseline di Riferimento - zxcvbn

Definizione

Algoritmo open-source ampiamente riconosciuto come baseline di riferimento nel settore per la stima della forza delle password.

Sviluppato da **Dropbox**, offre valutazione robusta basata sulla prevedibilità di una password.

idea Centrale

zxcvbn stima il numero di tentativi necessari per indovinare una password, fornendo un'indicazione della sua entropia.

- Riconoscimento e penalizzazione di pattern comuni
- Identificazione di parole da dizionario
- Valutazione delle sostituzioni prevedibili

Punti di Forza

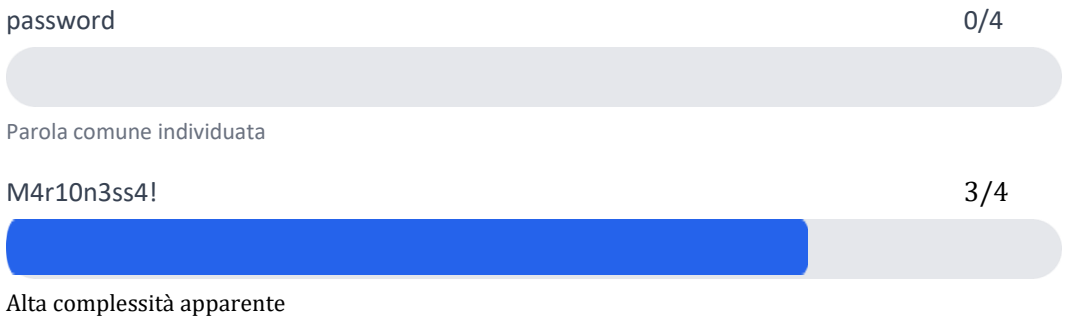
Valutazione basata su prevedibilità

Va oltre semplici requisiti di complessità, analizzando la resistenza a attacchi reali

Quantificazione della debolezza

Fornisce un punteggio che riflette la resistenza a attacchi di forza bruta o dizionario

Come zxcvbn valuta una password



PSM vs zxcvbn - Differenze Chiave

PSM

- **Approccio "safety-first"**
  Protezione attiva delle password
- **Integrazione dati personali**
  Identifica e penalizza informazioni personali
- **Regole di validazione finale**
  Blocchi aggiuntivi per password deboli
- **Feedback contestuale**
  Messaggi guidati dall'utente

zxcvbn

- **Stima dell'entropia**
  Basato su pattern comuni
- **Nessuna integrazione personali**
  Non considera dati utente
- **Nessuna regola finale**
  Solo punteggio numerico
- **Feedback limitato**
  Meno informativo

Takeaway: PSM risolve problemi non coperti da zxcvbn, in particolare l'uso di dati personali.

Valutazione Sperimentale - Impostazione

Dataset categorizzato e metodologia di confronto con metriche per analisi prestazioni

Categorie del Dataset

short weak
Password brevi e facilmente indovinabili

patterns
Password con schemi comuni (qwerty, 123456)

pop culture
Password da riferimenti culturali popolari

personal tokens
Password con informazioni personali

dictionary decorated
Parole di dizionario con aggiunte semplici

random strong
Password complesse e generate casualmente

Metodologia di Confronto

Punteggi Assegnati

Confronto tra gli score assegnati da PSM e zxcvbn a ciascuna password del dataset.

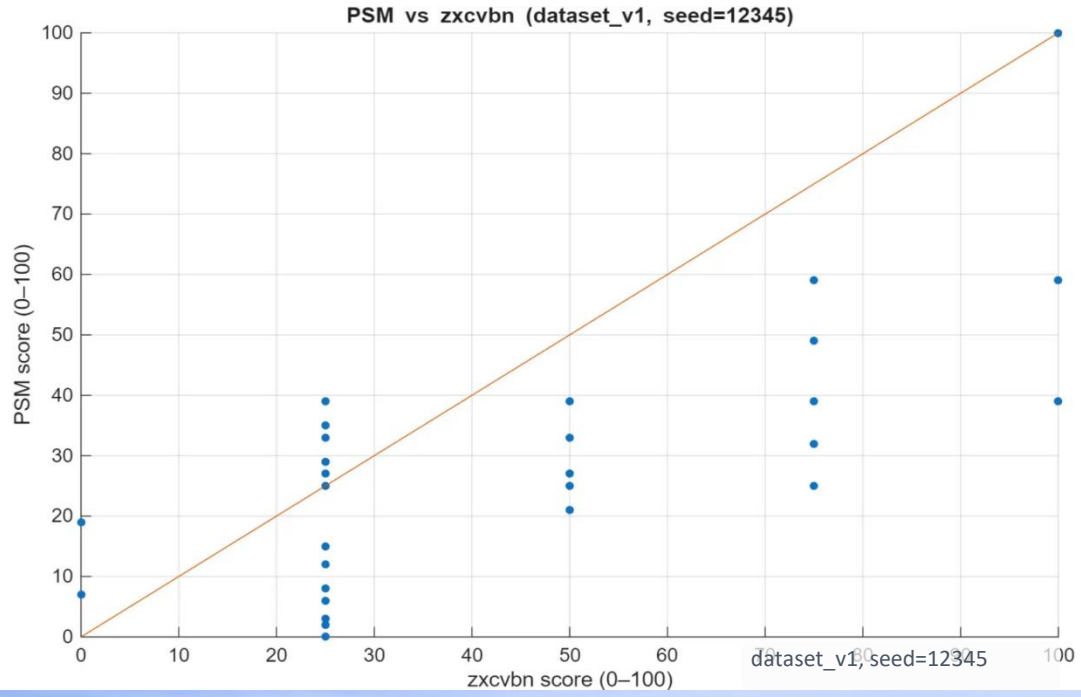
PSM vs zxcvbn — **Analisi diretta delle differenze**

Metriche di Analisi

- Media (mean)
- Mediana (median)
- Min/ Max

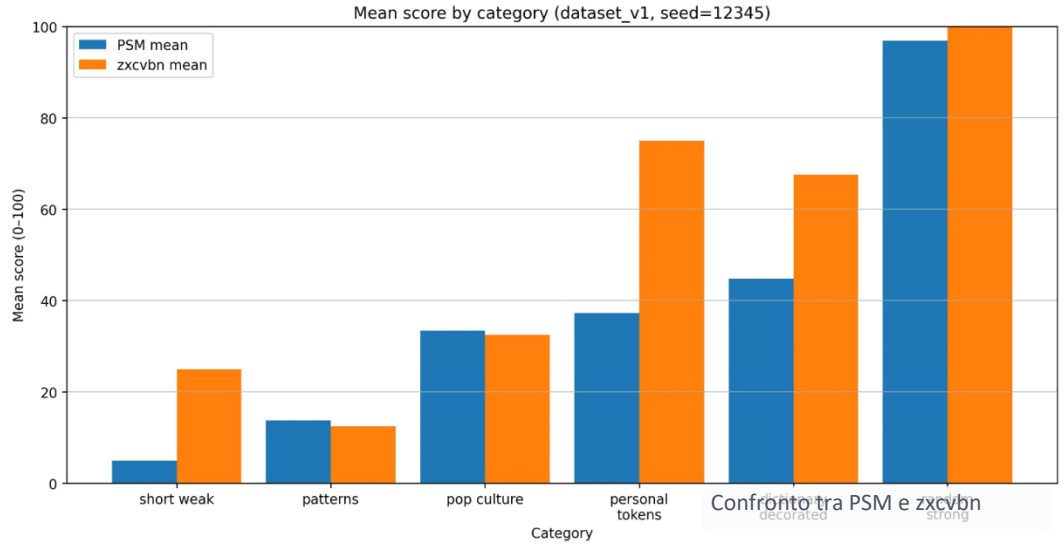
Risultati Sperimentali Principali

PSM vs zxcvbn (Scatter Plot)



dataset_v1, seed=12345

Media degli Score per Categoria



Confronto tra PSM e zxcvbn

Takeaway

Il PSM penalizza correttamente le password contenenti dati personali, a differenza di zxcvbn che tende a sopravvalutarle. Questo dimostra il valore aggiunto del nostro approccio "safety-first", in particolare per la categoria "personal tokens" dove il PSM mostra un punteggio medio significativamente inferiore rispetto a zxcvbn.

Architettura del Sistema

Tecnologie e Validazione

Stack Tecnologico

JavaScript/TypeScript
Sviluppo Engine, API e UI

Frontend
HTML e CSS per l'interfaccia utente web

Backend/API
Node.js con Express.js

Containerizzazione
Docker e Docker Compose

Testing e Validazione

Testing
Jest per test automatici unitari e di integrazione

CI/CD
GitHub Actions per la Continuous Integration

Testing Manuale
Procedure di testing manuale per la UI

Test API
Endpoint di test per la validazione dell'API

Demo e Sviluppi Futuri

Scaletta Demo

UI
- Inserimento dati utente
- Password debole (feedback + rifiuto)
- Password forte (accettazione)

Dashboard
- Selezione run di esperimento
- Confronto PSM vs zxcvbn
- Breakdown per categoria

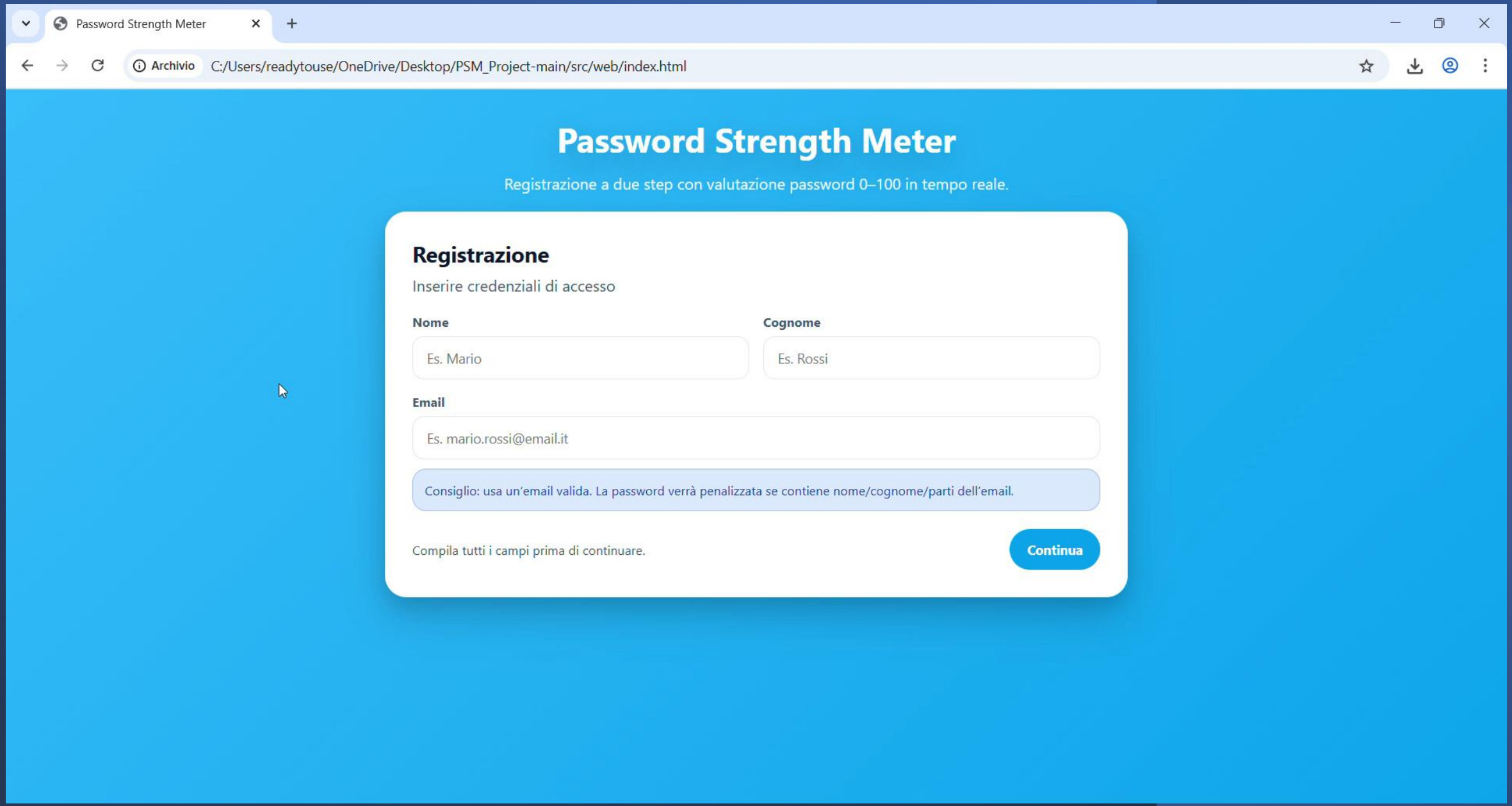
Export
- Click pulsante esportazione
- Download file risultati

Limiti Attuali

- Copertura pattern personali limitata
- Analisi semantica avanzata non implementata
- Integrazione database password compromesse
- Interfaccia policy da migliorare

Sviluppi Futuri

- **Espansione pattern personali**: inclusione di più tipologie di informazioni
- **Database in tempo reale**: verifica password compromesse
- **Analisi semantica**: comprensione contesto password
- **Interfaccia policy**: personalizzazione facile per non-tech


Password Strength Meter
Archivio
C:/Users/readytouse/OneDrive/Desktop/PSM_Project-main/src/web/index.html
Password Strength Meter
Registrazione a due step con valutazione password 0–100 in tempo reale.
Registrazione
Inserire credenziali di accesso
Nome
Es. Mario
Cognome
Es. Rossi
Email
Es. mario.rossi@email.it
Consiglio: usa un'email valida. La password verrà penalizzata se contiene nome/cognome/parti dell'email.
Compila tutti i campi prima di continuare.
Continua

Grazie per la visione

PASSWORD
STRENGTH
METER

Politecnico di Bari