WIRELESS MOBILE AND DEVICE SECURITY
MINI PROJECT REPORT

GROUP MEMBERS:
PA-36 Avdhut Bhakare

PA-39 Manthan Deodhe

PA-41 Satyam Kendre

PB-30 Harshvardhan S Patil

PB-33 Aditya Pahariya

-: PROJECT TITLE : -

Password Strength Checker Program Analysis

Abstract:

The Password Strength Tester serves as a pivotal tool in the realm of cybersecurity, aimed at enhancing password security through real-time evaluation and feedback mechanisms. This comprehensive report delves into the technical intricacies and multifaceted aspects of the application, spanning HTML, CSS, JavaScript functionalities, and algorithmic analyses. Emphasizing usability, accessibility, and security considerations, the report offers a comprehensive overview of the application's architecture and user-centric design.

Introduction:

Password Security Landscape

- Historical Context: Tracing password usage from ancient times to modern digital security practices.
- Evolution of Cyber Threats: Detailed exploration of evolving cyber threats and their impact on password security.

Technical Overview:

Technology Stack

- <u>HTML5 in Depth</u>: Detailed discussion on semantic HTML and its role in structuring the application.
- <u>CSS3 Styling Techniques</u>: Comprehensive exploration of <u>advanced CSS methodologies like Flexbox and Grid for</u> responsive design.
- <u>JavaScript's Functionalities</u>: Elaboration on ES6+ features and their implementation in asynchronous programming for password strength evaluation.

Code Architecture and Modularity

- <u>Component-Based Architecture</u>: Implementing reusable components for maintainability and scalability.
- <u>JavaScript Modularization</u>: Utilizing modules and bundlers (e.g., Webpack) for efficient code organization and deployment.

Algorithmic Analysis

- <u>Password Strength Algorithms</u>: Detailed comparison and implementation of algorithms like entropy-based methods, Markov models, and dictionary attacks.
- <u>Complexity Analysis</u>: Analyzing algorithmic time and space complexities for optimal performance.

HTML Structure:

Accessibility and Semantic Markup

- ARIA Roles and Landmarks: Extensive use of ARIA attributes for improved accessibility compliance.
- Structured Data Markup: Leveraging microdata or RDFa for enhanced search engine optimization (SEO).

Responsive Design and Media Queries

- Device-Agnostic Design: Discussion on designing for various screen sizes and devices through media queries.
- Viewport Meta Tag Optimization: Strategies for optimal rendering and responsiveness across devices.

CSS Styling:

CSS Methodologies and Optimization

- CSS Preprocessors and Postprocessors: Deep dive into preprocessors (e.g., Sass, Less) and postprocessors (e.g., Autoprefixer) for enhanced productivity and browser compatibility.
- Critical CSS and Performance Optimization: Implementing critical CSS for faster initial rendering and minimizing render-blocking resources.

Animations and Transitions

- <u>Advanced Animation Techniques</u>: Utilizing CSS animations and transitions for smoother user interactions and engagement.
- <u>GPU Acceleration and Performance Benefits</u>: Exploring GPU-based animation and its impact on rendering performance.

JavaScript Functionality:

Functional Programming Paradigm

- <u>Functional Composition and Purity</u>: In-depth discussion on composing functions and maintaining purity for cleaner and more maintainable code.
- <u>Immutability and Side Effects</u>: Leveraging immutability and handling side effects for robust application architecture.

Asynchronous Operations and Event-Driven Architecture

- <u>Async/Await and Promises</u>: Comprehensive utilization of asynchronous JavaScript for non-blocking operations.
- <u>Event-Driven Design Patterns</u>: Implementing observer and pub-sub patterns for managing complex interactions.

Password Strength Indicators:

Data Visualization Strategies

- SVG vs. Canvas for Visual Feedback: Comparative analysis of SVG and Canvas for rendering password strength indicators.
- Progressive Enhancement: Ensuring graceful degradation for visual feedback on older browsers or screen readers.

Accessibility and Visual Feedback

- Aural Feedback and Screen Reader Compatibility: Strategies to provide alternative textual feedback for visually impaired users.
- Contrast Ratios and Visual Accessibility: Ensuring sufficient contrast ratios for readability and compliance with accessibility standards.

Testing and Validation:

Automated Testing Suites and Strategies

- <u>Comprehensive Test Coverage</u>: Expanding test suites with unit, integration, and end-to-end tests for robust code validation.
- <u>Performance Profiling Tools</u>: Profiling tools like Chrome DevTools and Lighthouse for performance optimization.

User Acceptance Testing (UAT) and Usability Studies

- <u>User-Centric Testing Approach</u>: Incorporating feedback from usability studies for iterative improvements.
- <u>Accessibility Audits</u>: Conducting audits to ensure compliance with WCAG guidelines.

User Experience:

Usability Heuristics and Design Principles

- Nielsen's Heuristics: Applying Nielsen's principles for intuitive and user-friendly interfaces.
- UI/UX Prototyping and Wireframing: Implementing prototyping tools (e.g., Figma, Sketch) for iterative design improvements.

Personalization and User-Centric Features

- Preference Settings and Customization: Enabling user preferences for enhancing personalization.
- Behavioral Analytics for User Insights: Leveraging analytics for understanding user behavior and preferences.

Security Considerations:

Cryptographic Techniques and Best Practices

- <u>Salted Hashing and Key Derivation</u>: Detailed implementation of hashing techniques with salting for password storage.
- <u>Best Practices in Authentication</u>: Implementing multi-factor authentication (MFA) and session management best practices.

Vulnerability Assessment and Penetration Testing (VAPT)

- <u>Threat Modeling</u>: Identifying potential attack vectors and addressing security loopholes.
- <u>Regular Security Audits</u>: Implementing periodic security audits and continuous vulnerability assessments.

Conclusion:

Implications and Future Trends

- Impact of the Password Strength Tester: Reflecting on its significance in bolstering password security awareness.
- Emerging Technologies and Security Trends: Predicting advancements and trends in password security.

Continuous Improvement and Innovation

- Agile Methodologies: Embracing agile practices for continual improvements and feature enhancements.
- Feedback Loop and Roadmap: Incorporating user feedback for a roadmap of future developments.

Screenshots:
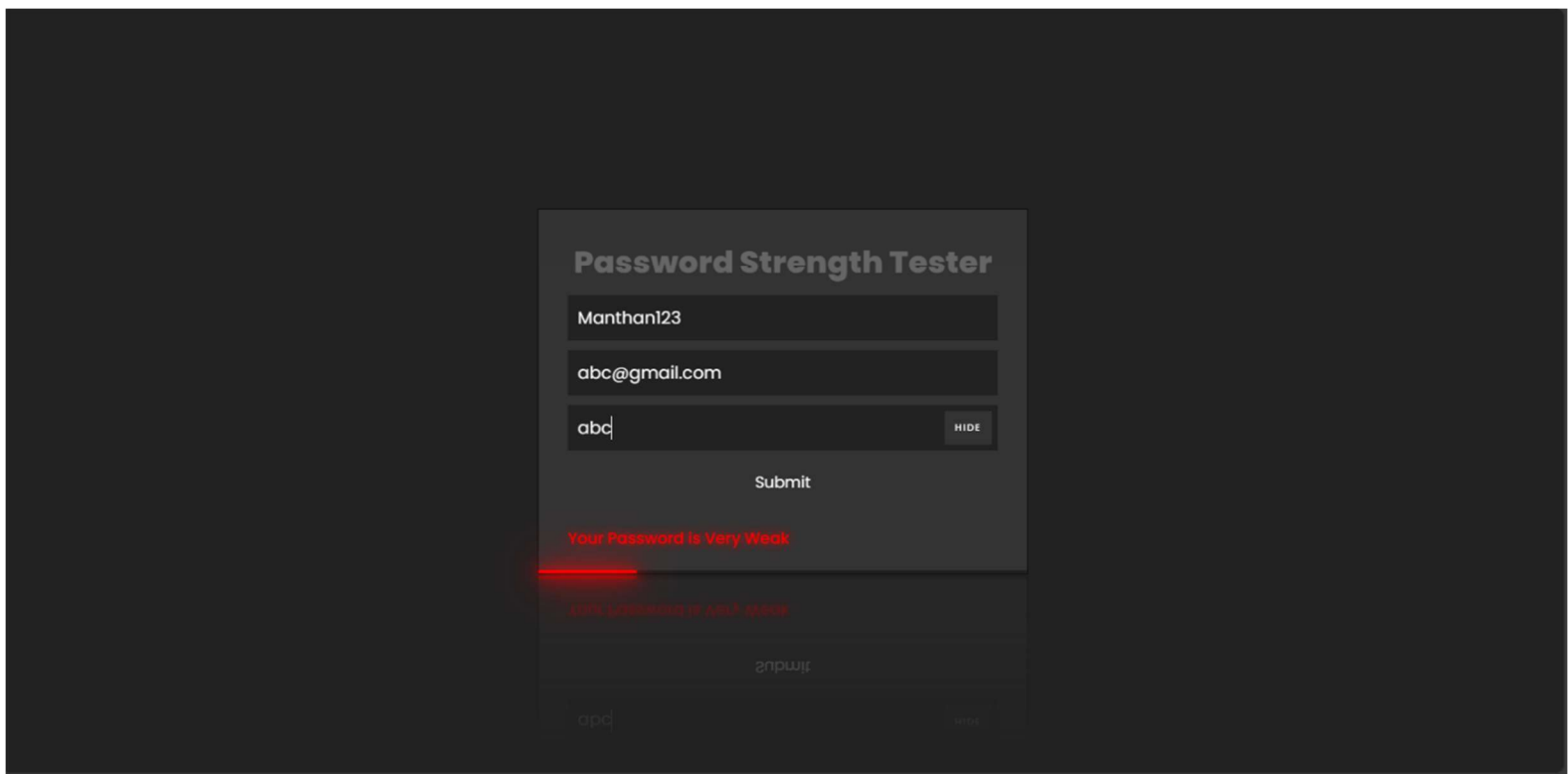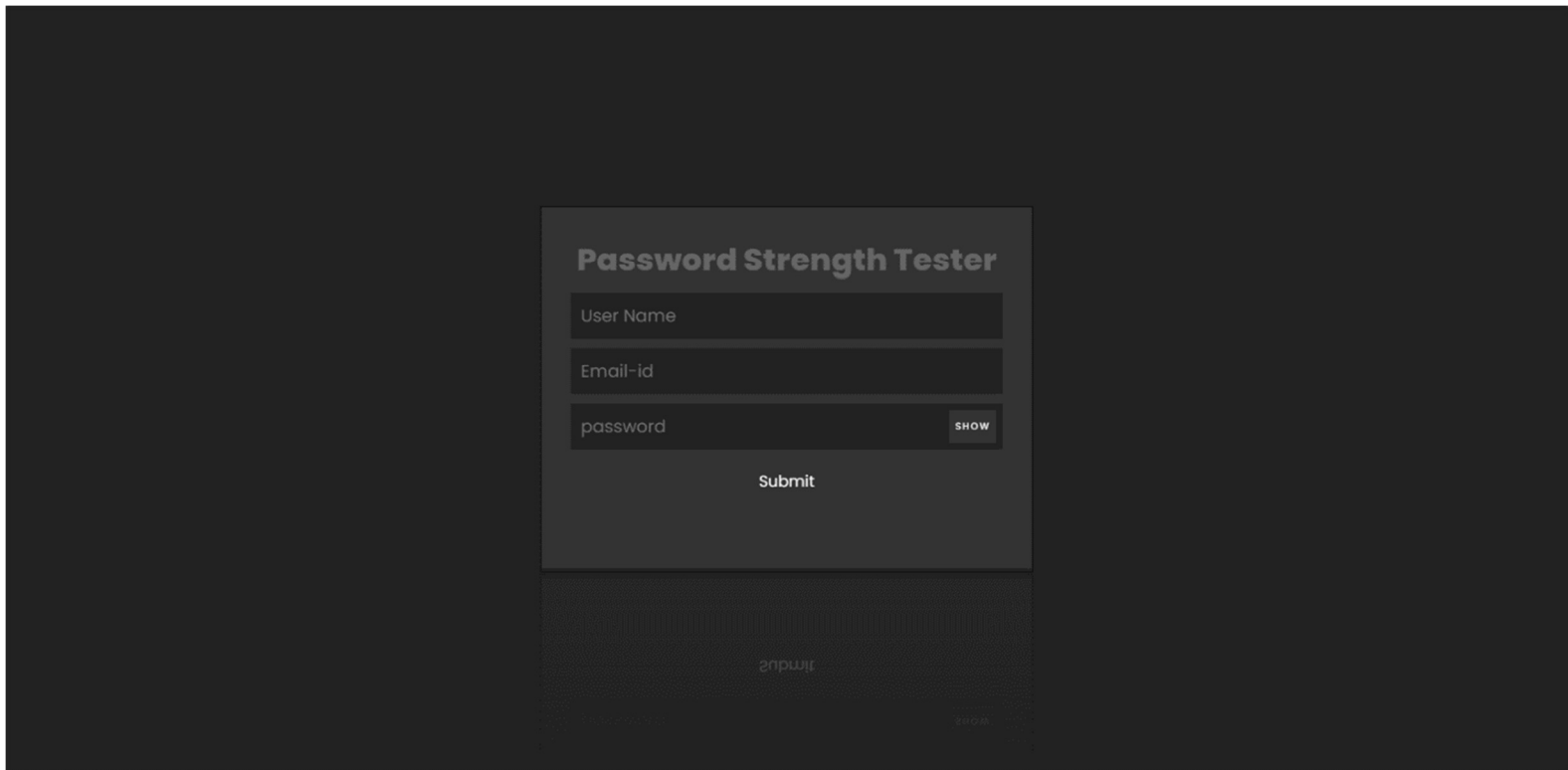
Password Strength Tester

Manthan123

abc@gmail.com

abc123   HIDE

Submit

Your Password is Weak

Password Strength Tester

Manthan123

abc@gmail.com

abc@123   HIDE

Submit

Your Password is Moderate

Password Strength Tester

Manthan123

abc@gmail.com

abc@#$123   HIDE

Submit

Your Password is Strong

Password Strength Tester

Manthan123

abc@gmail.com

Abc@#$123   HIDE

Submit

Your Password is Very Strong
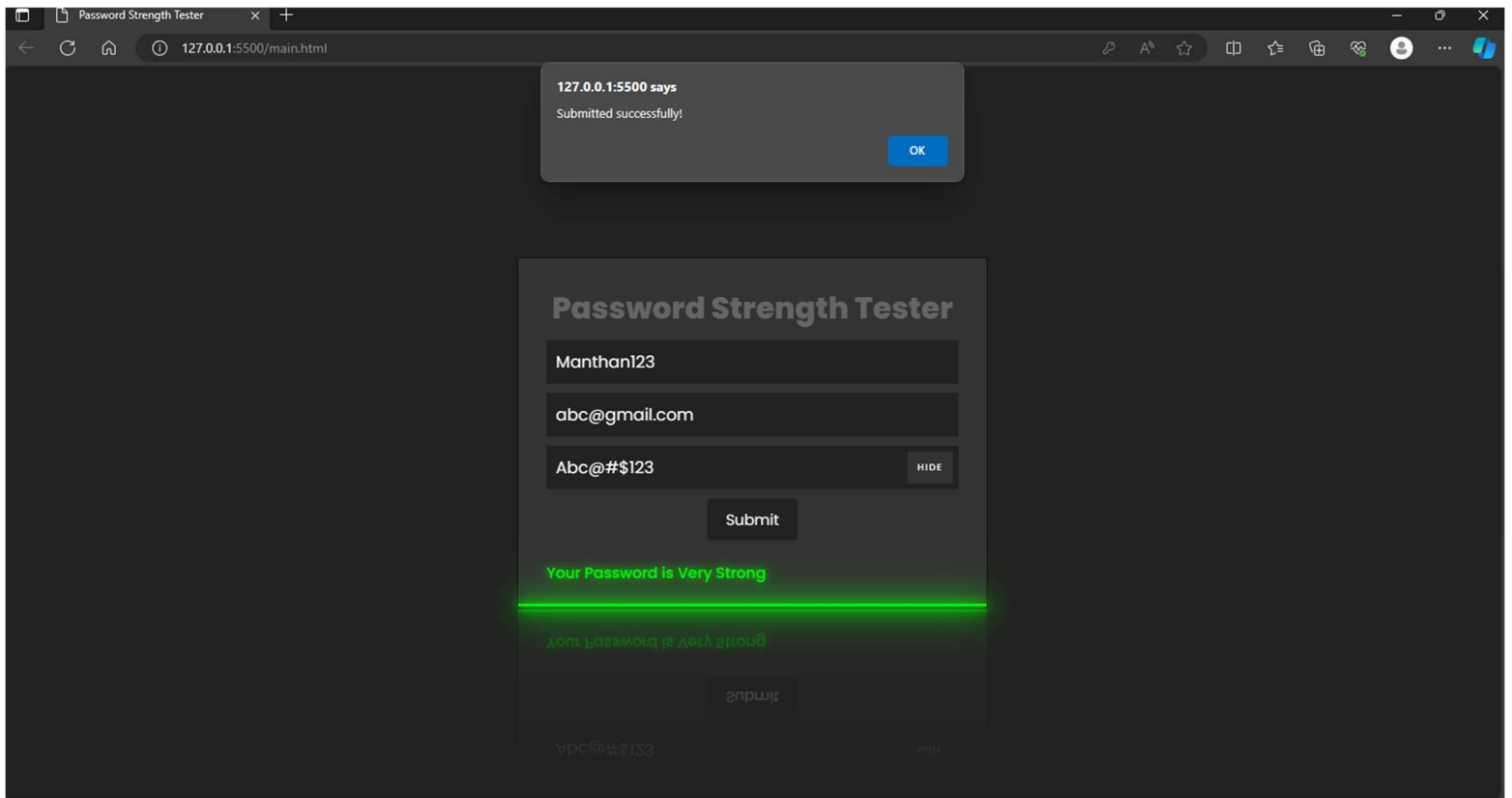
References:

- https://www.passwordmonster.com/
- https://password.kaspersky.com/
- Chat – GPT (Open AI)
- https://youtu.be/L_EImuIM7yY?si=UW1jG4n4e30CKZBO

Contributions:

Backend:

- Manthan Deodhe (PA39)
- Satyam Kendre (PA41)

Frontend:

- Avdhut Bhakare (PA36)
- Harshvardhan S Patil (PB30)

Report:

- Aditya Pahariya (PB33)