h4$h3d - Your Digital Fortress

Requirements and Specification Document

Date: 29 September 2023

Version: 1.0

Name	Enrollment No
Anant Jain	22114005
Dhas Aryan Satish	22117046
Divij Rawal	22114031
Parit Gupta	22117100
Pratyaksh Bhalla	22115119
Roopam Taneja	22115030

Project Abstract:

The "h4$h3d - Your Digital Fortress" project aims to develop a comprehensive password manager application that provides secure password generation, breach checking, strength assessment, and storage management. It may also include advanced features like 2-Factor Authentication (2FA), secure alias password generation, password recovery, multi-factor authentication (MFA) code management, and autofill functionality.

Document Revision History:

Rev. 1.0 [29/9/23]: Initial version.

Customer:

The general customer for the "h4$h3d - Your Digital Fortress" software is representative of the global population of internet users who require a reliable and secure password manager application. This customer demographic includes individuals, professionals, and organizations of various sizes who understand the importance of safeguarding their online accounts and sensitive information. They seek a user-friendly, feature-rich, and secure solution to enhance their digital security and simplify password management.

The Dummy Customer:

Are you tired of struggling to remember multiple passwords for your online accounts? Do you worry about the security of your digital identity? Look no further – "h4$h3d - Your Digital Fortress" is here to simplify your digital life and enhance your online security.

"h4$h3d - Your Digital Fortress" is a cutting-edge password manager application designed with you in mind. It caters to the needs of everyday internet users who seek a robust, user-friendly, and secure solution for managing their passwords and enhancing their online security.

Competitive Landscape:

To evaluate the competitive landscape of "h4$h3d - Your Digital Fortress," we will compare it with three established password management solutions: Google Password Manager, 1Password, and Bitwarden.

1. Google Password Manager:

Strengths:

- Integration: Seamlessly integrated with Google accounts and Google Chrome, making it convenient for users already in the Google ecosystem.
- Autofill: Efficient autofill feature on Android devices and the Chrome browser.
- Simplicity: User-friendly and accessible to a wide audience.

Weaknesses:

- Limited Features: Lacks advanced features such as secure alias password generation and password breach checking.
- Limited Cross-Platform Support: Primarily designed for Google users, which can be limiting for those outside the Google ecosystem.

2. 1Password:

Strengths:

- Comprehensive Security: Offers robust encryption and security features.
- Cross-Platform Support: Available on various platforms, including Windows, Mac, iOS, and Android.
- Advanced Features: Provides features like secure document storage and travel mode.

Weaknesses:

- Pricing: Can be relatively expensive, especially for individuals or small businesses.
- Learning Curve: May have a steeper learning curve for users new to password managers.

3. Bitwarden:

Strengths:

- Open-Source: Open-source nature allows for transparency and community contributions.
- Strong Security: Offers end-to-end encryption and is known for its focus on security.
- Cross-Platform: Available on multiple platforms, including desktop and mobile.
- Self-Hosting Option: Allows technically inclined users to host their Bitwarden server.

Weaknesses:

- User Interface: Some users find the user interface less polished compared to commercial solutions.
- Support: Support options may not be as extensive as those offered by commercial competitors.

Comparison with "h4$h3d - Your Digital Fortress":

Strengths of "h4$h3d - Your Digital Fortress":

- Advanced Security: "h4$h3d" offers strong encryption, password breach checking, and secure alias password generation, enhancing security.
- User-Friendly Design: A focus on user-friendliness ensures accessibility for a wide range of users.
- Multi-Platform Support: The application intends to provide cross-platform support, making it versatile.
- Unique Features: Features like password alias generation and MFA code management will provide a competitive edge.

Weaknesses of "h4$h3d - Your Digital Fortress":

- Brand Recognition: It may take time to establish the brand and gain trust compared to established competitors like Google.
- Resource Constraints: As a new project, resource constraints may limit the initial feature set and scalability.
- Support: Initial support options and resources may not match those of mature competitors.

System Requirements:

1. Main features:

Generate Secure Password:

Scenario: The user requests the generation of a secure, random password.

Acceptance Test: Verify that a strong, unique password is generated.

Check for Password Breaches:

Scenario: The user checks if a password has been compromised in any data breaches.

Acceptance Test: Confirm that the system accurately identifies breached passwords.

Assess Password Strength:

Scenario: The user assesses the strength of an existing password.

Acceptance Test: Ensure the system provides accurate strength assessment and improvement.

suggestions.

Secure Password Storage:

Scenario: The user stores a password securely.

Acceptance Test: Confirm that passwords are encrypted and stored securely.

2.Additional features:

Secure Alias Password Generation:

Scenario: The user generates a temporary 'alias' password for a lengthy credential.

Acceptance Test: Ensure that alias passwords are generated and expire after a specified time.

Password Recovery:

Scenario: The user recovers their account after forgetting their password.

Acceptance Test: Confirm that the password recovery process is successful.

Manage MFA Codes:

Scenario: The user manages multi-factor authentication codes.

Acceptance Test: Verify that MFA codes can be added, edited, and deleted.

Autofill Credentials:

Scenario: The user utilizes the autofill feature to populate login credentials.

Acceptance Test: Ensure that credentials are correctly autofill on websites.

3.Interface Requirements:

The user interface should be intuitive and user-friendly.

Data exchange format should follow industry standards for security.

4.External Dependencies:

Web Server: The application may depend on a web server to handle user authentication and communication.

Database: A database system is required to store user account information, encrypted passwords, and breach data.

Encryption Libraries: The application may depend on encryption libraries or frameworks to ensure data security.

Third-Party APIs: Integration with third-party services for password breach checking and 2FA support may be necessary.

5.Non-Functional Requirements:

Security: All user data and passwords must be stored using strong encryption methods. Access to passwords and sensitive information should be protected.

Performance: The system should respond promptly to user requests, including password generation and breach checking.

Scalability: The system should be scalable to accommodate a growing number of users and stored passwords.

Privacy: User data should be kept private, and no data should be shared with third parties without user consent.

Memory Requirements: The application should be memory-efficient, especially for mobile and low-resource devices

6. Customer User Interface Requirements:

User Registration and Login:

User Registration:

- User-friendly registration form with fields for username, email, and password.
- Validation checks for email format and password strength.

Login:

- Secure login page with fields for username/email and password.
- Option for users to enable Two-Factor Authentication (2FA). (*optional)*

Password Generation:

- Password generation screen with options for:
- Password length.
- Character complexity (uppercase, lowercase, numbers, symbols).
- Pronounceable or random password.
- Option to copy generated password to the clipboard.

Password Storage and Management:

- Intuitive dashboard for managing stored passwords.
- Ability to add, edit, and delete passwords.
- Password details view displaying information about stored passwords.
- Search and filter options to quickly find stored passwords.

Password Strength Assessment:

- Feedback provided when users create or edit passwords.
- Visual indicators of password strength (e.g., color-coded strength meter).
- Suggestions for improving password strength.
- Password Breach Checking:
- Option to check if stored passwords have been involved in data breaches.

- Clear notifications and recommendations if a breached password is detected.