Project: Secure Vault

Market Research and Benchmarking:

About the Benchmark:

To address the new deliverable, we examined existing solutions related to our project’s field: password and sensitive information management, which are the main components of the Secure Vault project.

There are 4 types of competitors for our solution. We will take them one by one and present their main characteristics, advantages, and limitations of some existing solutions.

I)Password Managers (e.g., LastPass, Dashlane, 1Password):

- **Definition:** A password manager is a software application or service designed to securely store and manage passwords for various online accounts and services
- **Characteristics:**
    - ❖ Securely store passwords for various accounts.
    - ❖ Synchronize data across multiple devices.
    - ❖ Provide browser extensions for easy autofill of login credentials.
- **Advantages:**
    - ❖ Centralized storage of passwords, reducing the need to remember multiple passwords.

Team Members: Achref Khairi Wael Haji

    - Enhanced security with encryption and multifactor authentication options.
    - Cross-platform compatibility, supporting various operating systems and devices.
- **Limitations:**
    - Dependency on master passwords or key files, which could be vulnerable if compromised.
    - Some solutions may require a subscription fee for advanced features or multi-device synchronization.
    - Potential risks associated with cloud storage, although most reputable providers employ robust security measures.

II)Built-in Password Managers (e.g., Apple Keychain, Google Password Manager):

- **Definition:** Built-in password managers are password management features integrated directly into operating systems or web browsers.
- **Characteristics:**
    - Integrated into the operating system or browser for seamless password management.
    - Automatically generate and save passwords when users create new accounts.
    - Offer synchronization across devices using the user's existing account credentials (e.g., Apple ID, Google account).
- **Advantages:**

    - Convenience of built-in functionality without the need for third-party applications.
    - Tight integration with the operating system/browser, enhancing user experience.
- **Limitations:**
    - Limited features compared to dedicated password managers.
    - May lack advanced security options like multifactor authentication or secure notes storage.
    - Availability restricted to specific platforms (e.g., Apple Keychain for iOS/macOS, Google Password Manager for Android/Chrome).

III)Encrypted Note-Taking Apps (e.g., Evernote, Microsoft OneNote):

- **Definition:** Encrypted note-taking apps are software applications designed to allow users to create, store, and organize notes containing sensitive information while ensuring that the data is encrypted for privacy and security purposes.
- **Characteristics:**
    - Allow users to create and store encrypted notes containing sensitive information.
    - Offer synchronization across devices for access to notes from anywhere.
    - Provide password protection and biometric authentication options for added security.

- **Advantages:**
    - Versatility for storing various types of information beyond passwords (e.g., personal notes, documents).
    - Integration with productivity tools for organization and collaboration.
- **Limitations:**
    - Primarily designed for note-taking rather than password management, lacking dedicated password generation and autofill features.
    - May require additional manual effort for organizing and securing sensitive information.
    - Less focus on password-specific security features compared to dedicated password managers.