

Secure Password Management Demonstration

Introduction

In today's digital era, both people and businesses have to keep and manage multiple online accounts. But it is noticed that they are often reusing similar weak passwords across different accounts. It increases security risks. Applications like Bitwarden help solving this by allowing users to generate, store and manage passwords securing user information. In this report, I highlight how Bitwarden is maintaining password security to minimize phishing and credential threat risks.

Advantages of Password Managers:

- Convenience: Fill out login forms automatically.
- Security: Create and keep secure, unique passwords.
- Phishing protection: They only use autofill on trustworthy websites.
- Cross-device access: Synchronizes information between phones and PCs.
- Zero-knowledge encryption: Prevents anyone from accessing your vault, not even the service provider.

Sources:

- Cheat Sheet for OWASP Authentication
- Guidelines for Digital Identity (NIST SP 800-63B)
- SANS Security Awareness: Developing Robust Passwords

Overview of the Tool

I chose Bitwarden, a free and open-source password manager that is trusted by millions of people worldwide, for this demonstration. It uses **AES-256-bit encryption**, ensuring strong security. It facilitates cross-platform access through web vaults, mobile apps and browser extensions.

How Bitwarden Works:

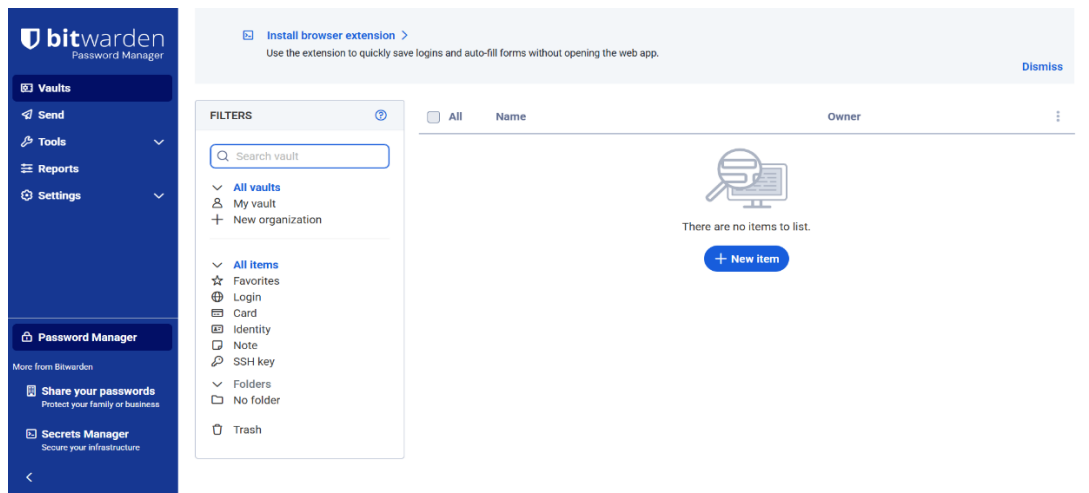
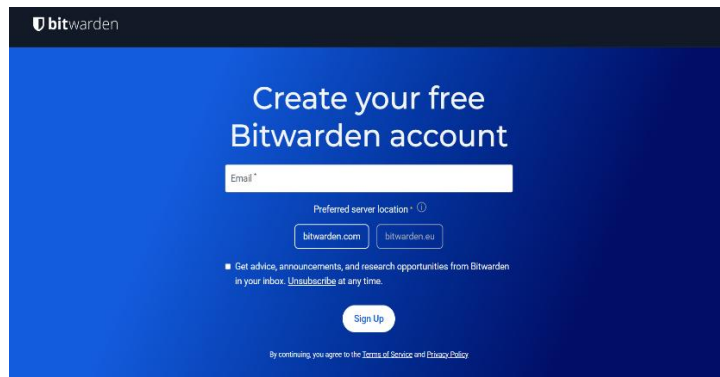
Bitwarden operates by storing all of your login information in an encrypted vault. There is only one master password that can be used to access the vault. It has features like two-factor authentication (2FA), secure notes, autofill and password generation. To ensure zero-knowledge architecture, all data is encrypted locally before syncing to the cloud.

Setup Process

Step 1: Account Creation

I made a free account on <https://bitwarden.com> using my email address and a strong master password.

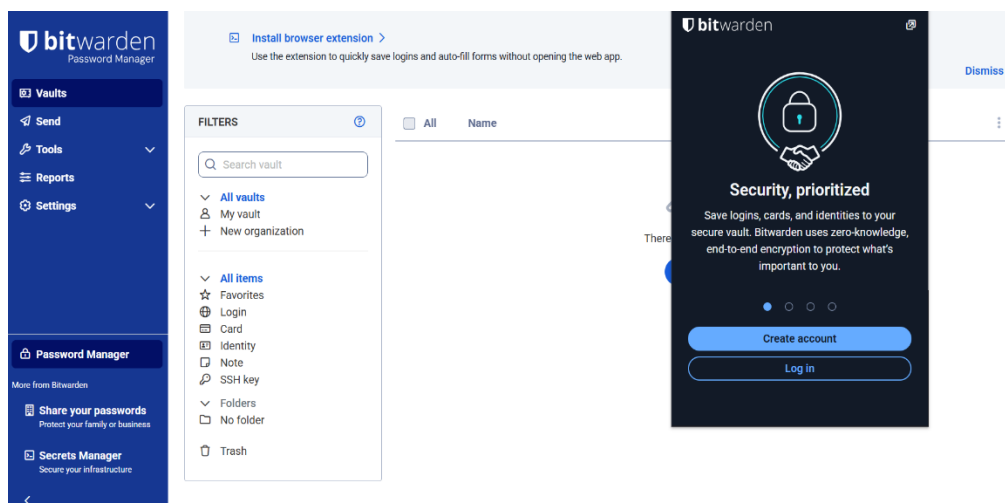
Screenshot of account creation:



Step 2: Installing the Browser Extension

Next, I installed the Bitwarden extension from the Chrome Web Store.

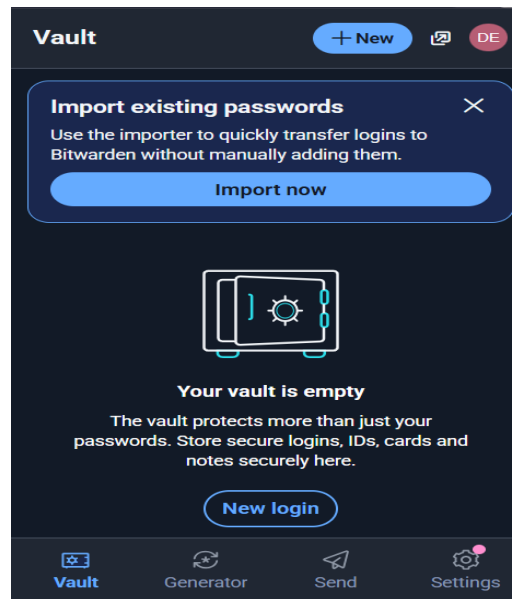
Screenshot of the browser's installed extension:



Step 3: Accessing the Dashboard

After logging in, I was able to add or manage login credentials , create secure passwords and adjust account settings .

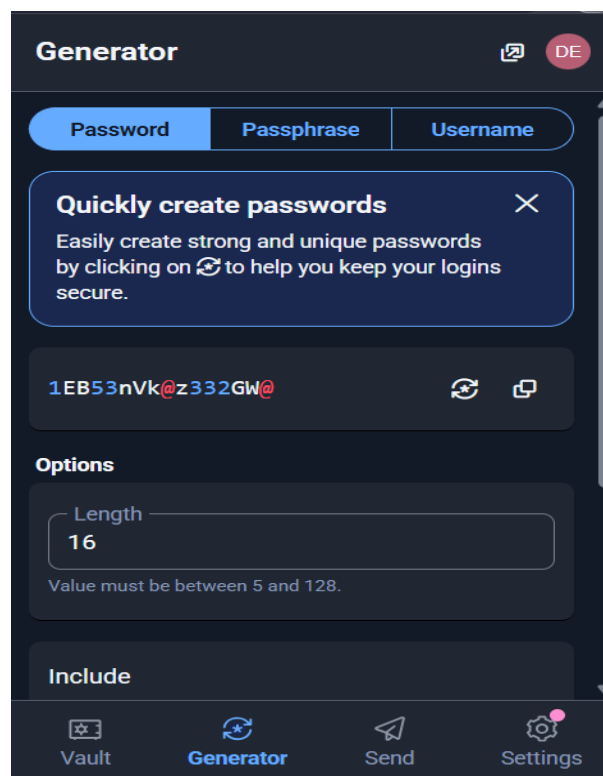
Screenshot of the Dashboard:



Step 4: Using the Password Generator

Bitwarden has an integrated password generator that can generate secure, complicated passwords. I created a 16 character password with it by combining special symbols, numbers, and letters.

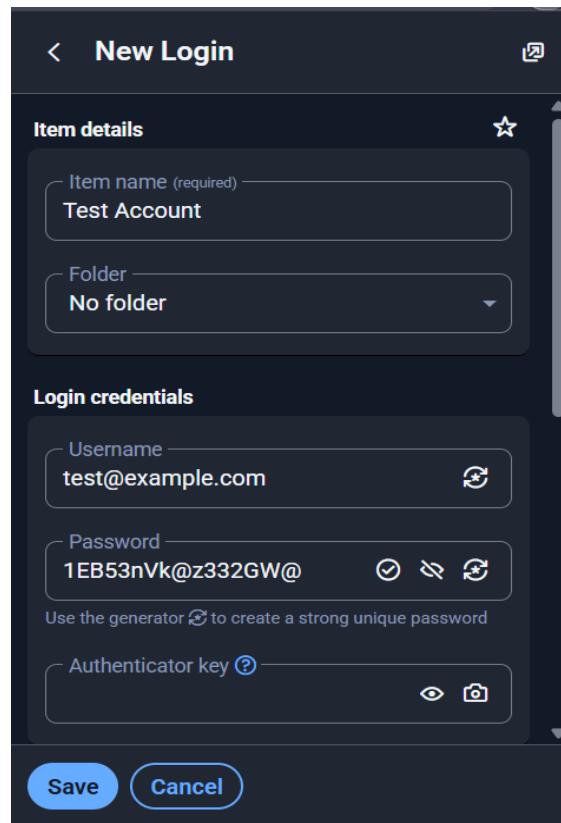
Screenshot of the password generation:



Step 5: Saving a Test Account

Using the "Add Item" feature, I made a test login (test@example.com) and saved it to the vault.

Screenshot of adding new login item:

A screenshot of the Bitwarden mobile app's 'New Login' screen. The screen has a dark theme. At the top, there's a back arrow and the title 'New Login'. Below this is a section titled 'Item details' with a star icon. It contains two input fields: 'Item name (required)' with the text 'Test Account' and 'Folder' with a dropdown menu showing 'No folder'. Below this is a section titled 'Login credentials'. It contains three input fields: 'Username' with the text 'test@example.com' and a refresh icon; 'Password' with the text '1EB53nVk@z332GW@' and icons for password strength, a checkmark, and a refresh icon; and 'Authenticator key' with a question mark icon. Below the password field, there's a note: 'Use the generator to create a strong unique password'. At the bottom, there are two buttons: 'Save' and 'Cancel'.

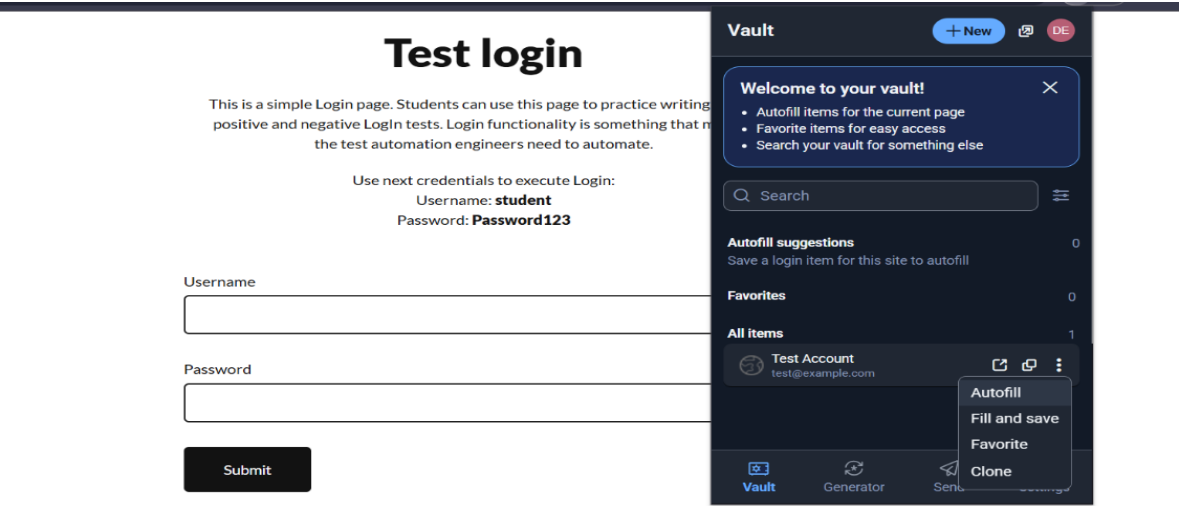
Step 6: Categorizing Entries

Every item in the vault can be classified or tagged. For instance, you can better organize passwords by labeling them "Social," "Work," or "Banking."

Step 7: Auto-Fill Feature

Bitwarden has the ability to automatically enter website login information. I showed this by going to a login page and letting Bitwarden fill in the login information automatically.

Screenshot of Auto-fill in action on a website:



Test login

This is a simple Login page. Students can use this page to practice writing simple positive and negative Login tests. Login functionality is something that most of the test automation engineers need to automate.

Use next credentials to execute Login:

Username: **student**

Password: **Password123**

Username

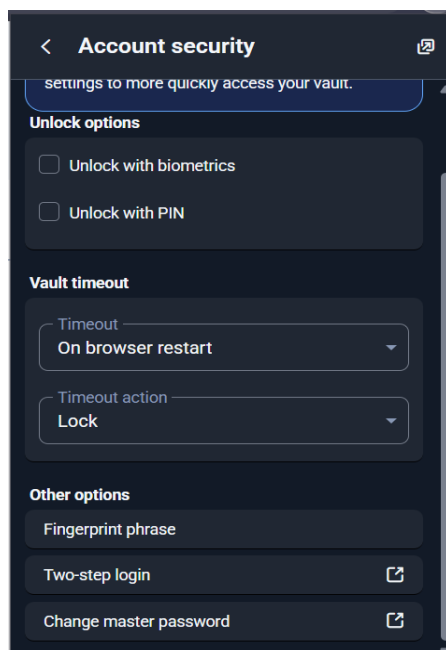
Password

Best Practices for Strong Passwords

Experts in cybersecurity advise the following:

- Make sure your passwords contain a minimum of 12 characters.
- Mix capital and lowercase letters, numbers, and symbols.
- Steer clear of personal information or dictionary words.
- Make use of passphrases such as Blue\$Horse!Climbs7Rain
- For an additional security measure, turn on Bitwarden's Two-Factor Authentication (2FA)

Screenshot:



Secure Storage & Sharing Guidelines

Use these best practices to make sure passwords are handled and transmitted securely:

- ❖ Passwords should never be kept in plain text.
Passwords should not be stored in unencrypted files such as spreadsheets, Word documents, or Notepad.
- ❖ Make use of an encrypted password manager that is vault-based.
Your credentials are securely stored and only you can access them thanks to tools like Bitwarden that encrypt them using AES-256.
- ❖ Make use of safe sharing tools.
Bitwarden (Premium) is perfect for families or teams because it enables encrypted password sharing through collections or organization vaults.
- ❖ Passwords should never be shared via unsecure channels.

Sensitive login information should not be sent via social media, WhatsApp, SMS, or email since these channels lack end-to-end encryption and are vulnerable to interception.

- ❖ Make use of permissions and access controls.
Assign suitable access levels (such as view-only or limited access) when sharing credentials with members of a team or organization to avoid missuse.

Conclusion

In this report, I discussed the value of safe password management and gave an example of how to use Bitwarden, a dependable and open-source password manager. Every step, from creating an account and creating secure passwords to saving and automatically filling in login information, helps to improve cybersecurity practices.

By providing a safe, encrypted environment, it reduces the risks of password reuse, weak passwords, and unsafe storage while assisting users in effectively managing their credentials.

It is no longer feasible to rely on memory or risky habits like writing down passwords in an age of frequent data breaches and cyberthreats. Using a password manager is essential, not just convenient. People and organizations can greatly improve their cybersecurity posture by implementing Bitwarden and other best practices.

References

1. **OWASP Foundation.** (n.d.). *Password Storage Cheat Sheet*.
Retrieved from: https://owasp.org/www-project-cheat-sheets/cheatsheets/Password_Storage_Cheat_Sheet.html
2. **National Institute of Standards and Technology (NIST).** (2017). *Digital Identity Guidelines (NIST SP 800-63B)*.
Retrieved from: <https://www.nist.gov/publications/digital-identity-guidelines>
3. **SANS Institute.** (n.d.). *Password Protection: Best Practices*.
Retrieved from: <https://www.sans.org/white-papers/389>
4. **Bitwarden Help Center.** (n.d.). *Getting Started with Bitwarden*.
Retrieved from: <https://bitwarden.com/help/>