MIT World Peace University

Full Stack Development
Third Year B. Tech, Semester 5

Anti Brutus
Password Generator and Manager

Full Stack Development - Mini Project Report

Prepared By

Krishnaraj Thadesar, PA10, 1032210888
Parth Zarekar, PA07, 1032210846
Sourab Karad, PA25, 1032211150
Soubhagya Singh, PA24, 1032211144

December 5, 2023

Contents

1 Introduction

Anti Brutus uses a combination of the latest in Cyber Security techniques and the most advanced encryption algorithms to protect your data. We use a combination of Salting, Hashing with SHA-256 and Secure SQL Databases with fortified backend servers to ensure that your data is safe from any third-party. We also use a combination of the latest in authentication techniques to ensure that only you can access your data.

1.1 Usage

Its already difficult remembering all your passwords, and with more and more websites that require login, it is becoming increasingly difficult to remember all your passwords. This is where Anti Brutus comes in.

Anti Brutus is a password manager that allows you to store all your passwords in one place, and access them with a Single Master Password. This way, you only need to remember one password, and you can access all your passwords from anywhere in the world.

It is however, also difficult to maintain strong passwords for each new website that you visit, for this, we offer our Password Generator which allows you to generate strong passwords for each new website that you visit, and store them in your vault.

1.2 Vaults

Vaults are a way to organize your passwords. You can create as many vaults as you want, and store passwords in each vault. This way, you can organize your passwords based on their use.

You can save various kinds of sensitive data in your vaults, like your credit card details, your bank account details, your Aadhar Card Info, etc. There are pre built templates for all of these to choose from.

2 Technologies Used

2.1 Frontend

2.1.1 ReactJS

ReactJS is a JavaScript library for building user interfaces. It is maintained by Facebook and a community of individual developers and companies. React can be used as a base in the development of single-page or mobile applications. It is a powerful library that allows us to create reusable components that can be used to build complex user interfaces.

2.1.2 Tailwind CSS

Tailwind CSS is a utility-first CSS framework for rapidly building custom user interfaces. It is a highly customizable, low-level CSS framework that gives us all of the building blocks we need to build bespoke designs without any annoying opinionated styles we have to fight to override.

2.1.3 DaisyUI

DaisyUI is a component library for Tailwind CSS. It provides a set of beautiful UI components that can be used to build user interfaces. It is built on top of Tailwind CSS and provides a set of components that can be used to build beautiful user interfaces.

2.1.4 Hero Icons

Hero Icons is a set of free MIT-licensed high-quality SVG icons for UI development. It provides a set of icons that can be used to build beautiful user interfaces.

2.1.5 Tabler Icons

Tabler Icons is a set of free MIT-licensed high-quality SVG icons for you to use in your web projects. It provides a set of icons that can be used to build beautiful user interfaces.

2.2 Backend

2.2.1 Node JS

Node.js is an open-source, cross-platform, back-end JavaScript runtime environment that runs on the V8 engine and executes JavaScript code outside a web browser. It is a powerful tool that allows us to build scalable network applications using JavaScript.

2.2.2 Express JS

Express.js, or simply Express, is a back end web application framework for Node.js, released as free and open-source software under the MIT License. It is a powerful tool that allows us to build scalable network applications using JavaScript.

2.2.3 MySQL or Mariadb

MySQL is an open-source relational database management system. It is a powerful tool that allows us to store and retrieve data from a database.

3 Features

1. **Generate Passwords using Unique Hash Scheme:** The application uses a unique hash scheme to generate secure and random passwords. This ensures that the passwords are strong and difficult to guess or crack.

2. **Store Passwords:** The application provides a secure storage mechanism for passwords. This allows users to store their passwords in a safe and secure manner, reducing the risk of password theft or loss.

3. **Near Unbreakable Security**

   (a) **Master Password Protection:** The application uses a master password to protect access to the stored passwords. This master password is required to unlock the application and access the stored passwords. This adds an extra layer of security by ensuring that only the user who knows the master password can access the stored passwords.

   (b) **AES Encryption:** The application uses Advanced Encryption Standard (AES) encryption to encrypt the stored passwords. AES is a secure encryption algorithm that is widely used for encrypting sensitive data. By using AES encryption, the application ensures that the stored passwords are safe from unauthorized access, even if the storage medium is compromised.

(c) **Envelope Encryption:** The application uses envelope encryption to further secure the stored passwords. In envelope encryption, a data encryption key is used to encrypt the data, and then this key is itself encrypted using a master key. This adds an additional layer of security by ensuring that even if the data encryption key is compromised, the data remains secure.

(d) **Hashing and Salting:** The application uses hashing and salting techniques to secure the master password. When the user enters the master password, it is hashed and salted before being stored. This ensures that even if the stored hash is compromised, it is extremely difficult to reverse-engineer the original password from the hash.

4. **Suited for Mobile and Web platforms:** The application is designed to work on both mobile and web platforms. This provides users with the flexibility to manage their passwords from any device or location.
   The application features a responsive user interface that adjusts to different screen sizes and resolutions. This ensures that the application is easy to use on a wide range of devices, including smartphones, tablets, and desktop computers.

4 Workflow/ Architecture Diagram

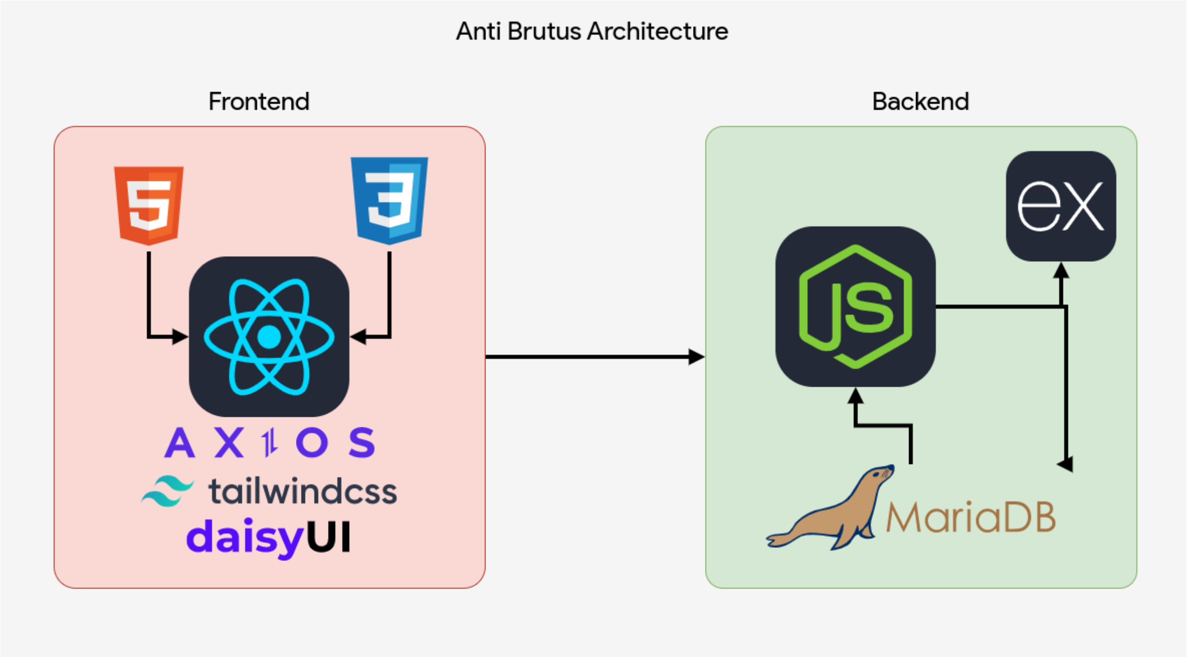


Figure 1: Architecture and Workflow of the Project

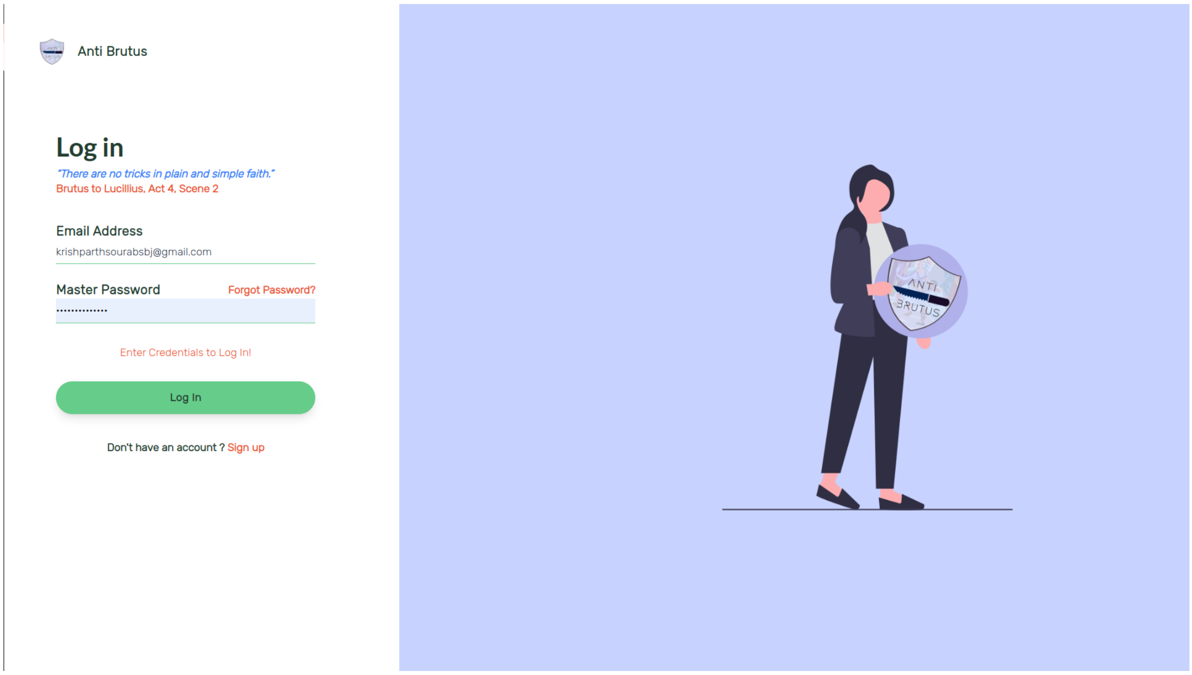
5 Future Scope and Conclusion

There are more features that can be added to the application to make it more secure and user-friendly. Some of these features include:

1. Include a KDC

2. Include Authentication with Biometrics, or 2 Factor Authentication App
3. Include login with Google or Facebook accounts.
4. Include a Password Strength Meter
5. Ability to Export Passwords in CSV, and import that csv.
6. Store Credit cards and other information.
7. Better and Enhanced Search Features
8. Checks for Duplicate Passwords, or Weak Passwords
9. Check for Breached Passwords

6 Screenshots



Anti Brutus

Log in

"There are no tricks in plain and simple faith."

Brutus to Lucillius, Act 4, Scene 2

Email Address

krishparthsourabsbj@gmail.com

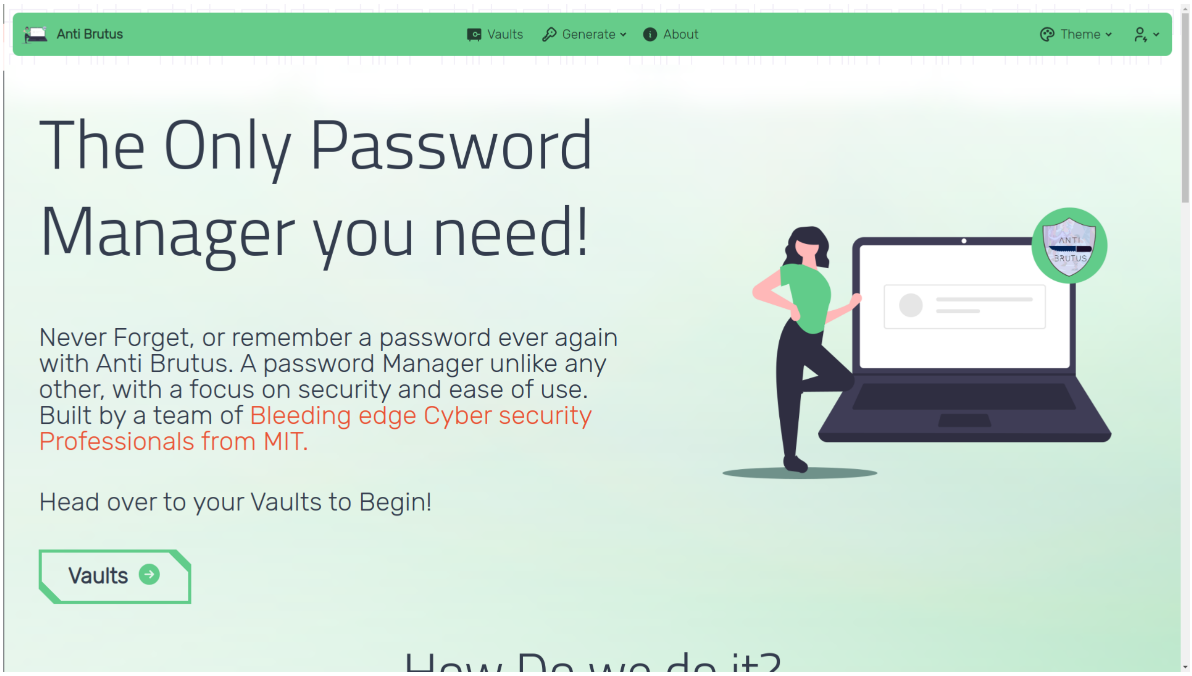
Master Password

....

Enter Credentials to Log In!

Don't have an account ? Sign up

Figure 2: Login



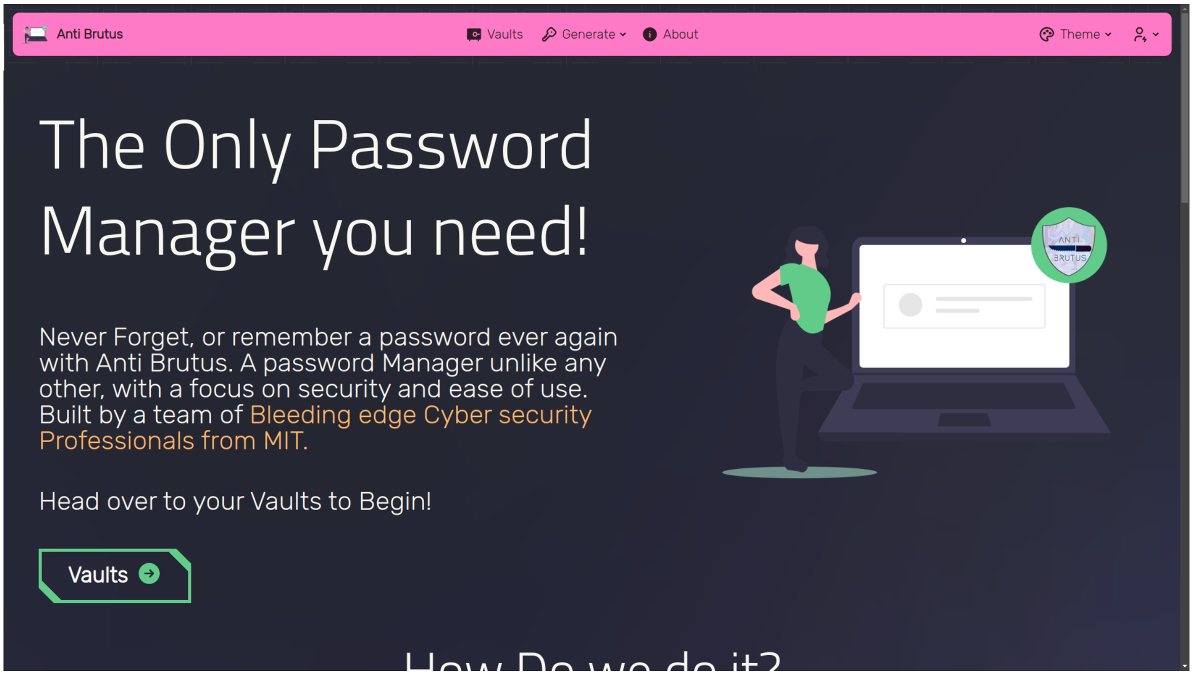
The Only Password Manager you need!

Never Forget, or remember a password ever again with Anti Brutus. A password Manager unlike any other, with a focus on security and ease of use. Built by a team of Bleeding edge Cyber security Professionals from MIT.

Head over to your Vaults to Begin!

How Do we do it?

Figure 3: Home (Light Mode)



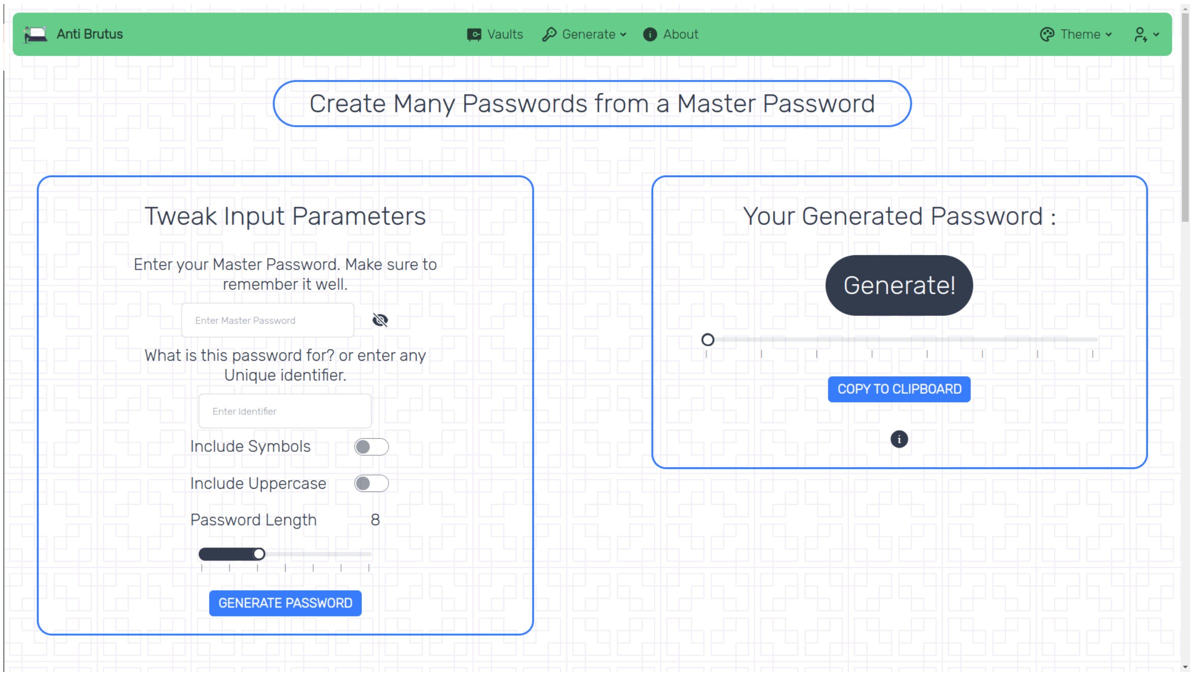
The Only Password Manager you need!

Never Forget, or remember a password ever again with Anti Brutus. A password Manager unlike any other, with a focus on security and ease of use. Built by a team of Bleeding edge Cyber security Professionals from MIT.

Head over to your Vaults to Begin!

How Do we do it?

Figure 4: Home (Dark Mode)



Create Many Passwords from a Master Password

Tweak Input Parameters

Enter your Master Password. Make sure to remember it well.

Enter Master Password

What is this password for? or enter any Unique identifier.

Enter Identifier

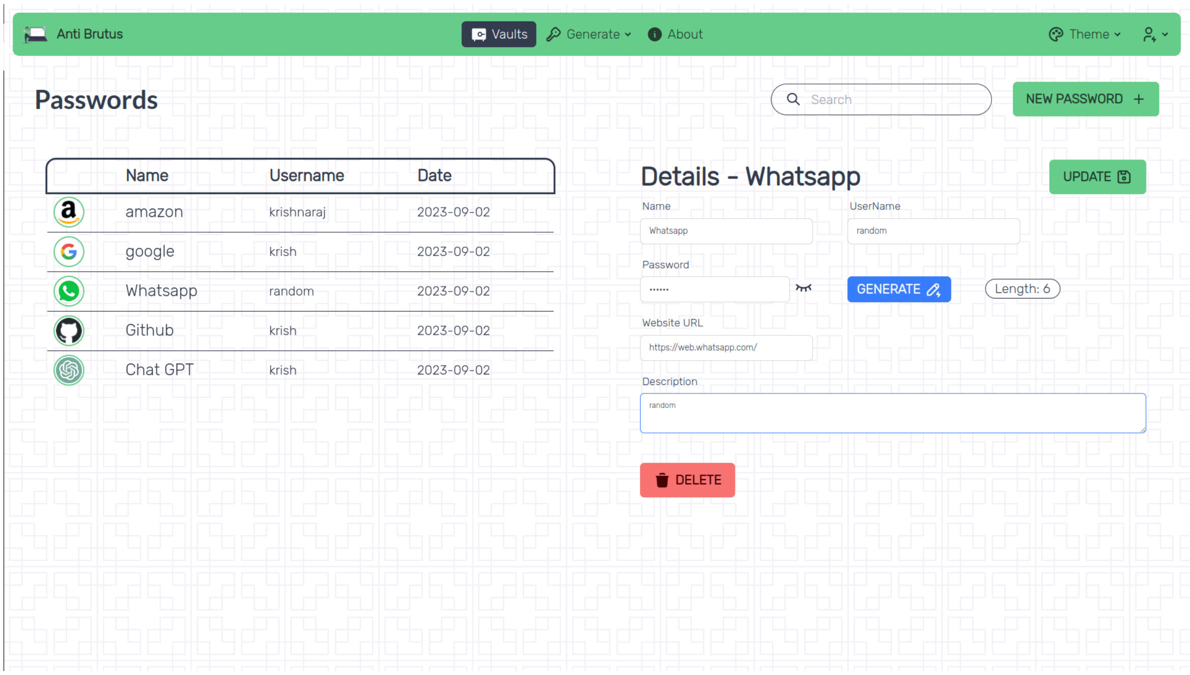
Include Symbols

Include Uppercase

Password Length 8

Your Generated Password :

Figure 5: Generate Master Passwords



Passwords

Name	Username	Date
amazon	krishnaraj	2023-09-02
google	krish	2023-09-02
Whatsapp	random	2023-09-02
Github	krish	2023-09-02
Chat GPT	krish	2023-09-02

Details - Whatsapp

Name: Whatsapp

UserName: random

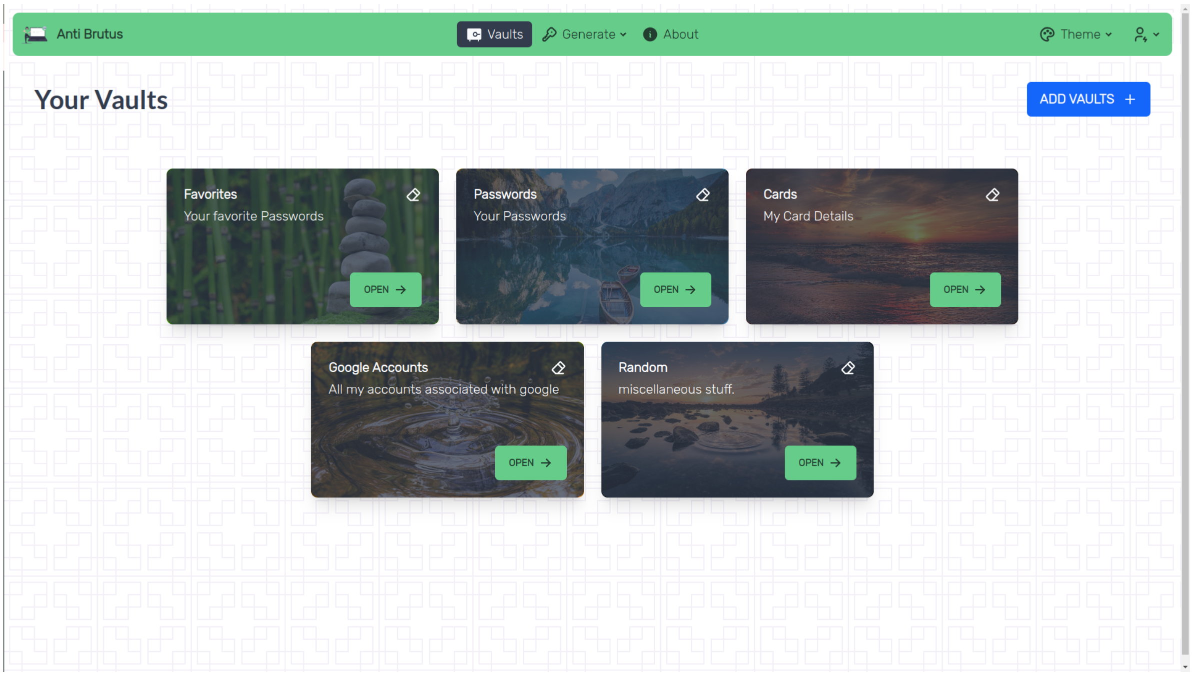
Password: ······

Length: 6

Website URL: https://web.whatsapp.com/

Description: random

Figure 6: Storing Passwords



Your Vaults

Favorites
Your favorite Passwords

Passwords
Your Passwords

Cards
My Card Details

Google Accounts
All my accounts associated with google

Random
miscellaneous stuff.

Figure 7: Vaults

References

[1] DaisyUI, *Tailwind CSS plugin for beautiful UI components*,
https://daisyui.com/

[2] Hero Icons, *A set of free MIT-licensed high-quality SVG icons for UI development*,
https://heroicons.com/

[3] Tabler Icons, *Over 1250 free MIT-licensed high-quality SVG icons for you to use in your web projects*,
https://tablericons.com/

[4] Tailwind CSS, *A utility-first CSS framework for rapidly building custom user interfaces*,
https://tailwindcss.com/

[5] ReactJS, *A JavaScript library for building user interfaces*,
https://reactjs.org/

[6] Bitwarden, *A password Manager*,
https://bitwarden.com/