

Mimir: A Password Manager Project

Edward William Bennett

Supervisor: Atta Badii

Table of Contents

[Abstract 3](#_Toc75229509)

[Executive Summary 4](#_Toc75229510)

[Introduction 5](#_Toc75229511)

[Research of Existing Products 6](#_Toc75229512)

[Keeper 6](#_Toc75229513)

[Bitwarden 12](#_Toc75229514)

[Dashlane 14](#_Toc75229515)

[Methodology 15](#_Toc75229516)

[Requirements Engineering 16](#_Toc75229517)

[Design Specification 17](#_Toc75229518)

[Implementation 18](#_Toc75229519)

[Conformance Testing and Integration 27](#_Toc75229520)

[Evaluation Plan 28](#_Toc75229521)

[Conclusion 29](#_Toc75229522)

[Lessons Learned 30](#_Toc75229523)

[Acknowledgements 31](#_Toc75229524)

[Bibliography 32](#_Toc75229525)

# Abstract

# Executive Summary

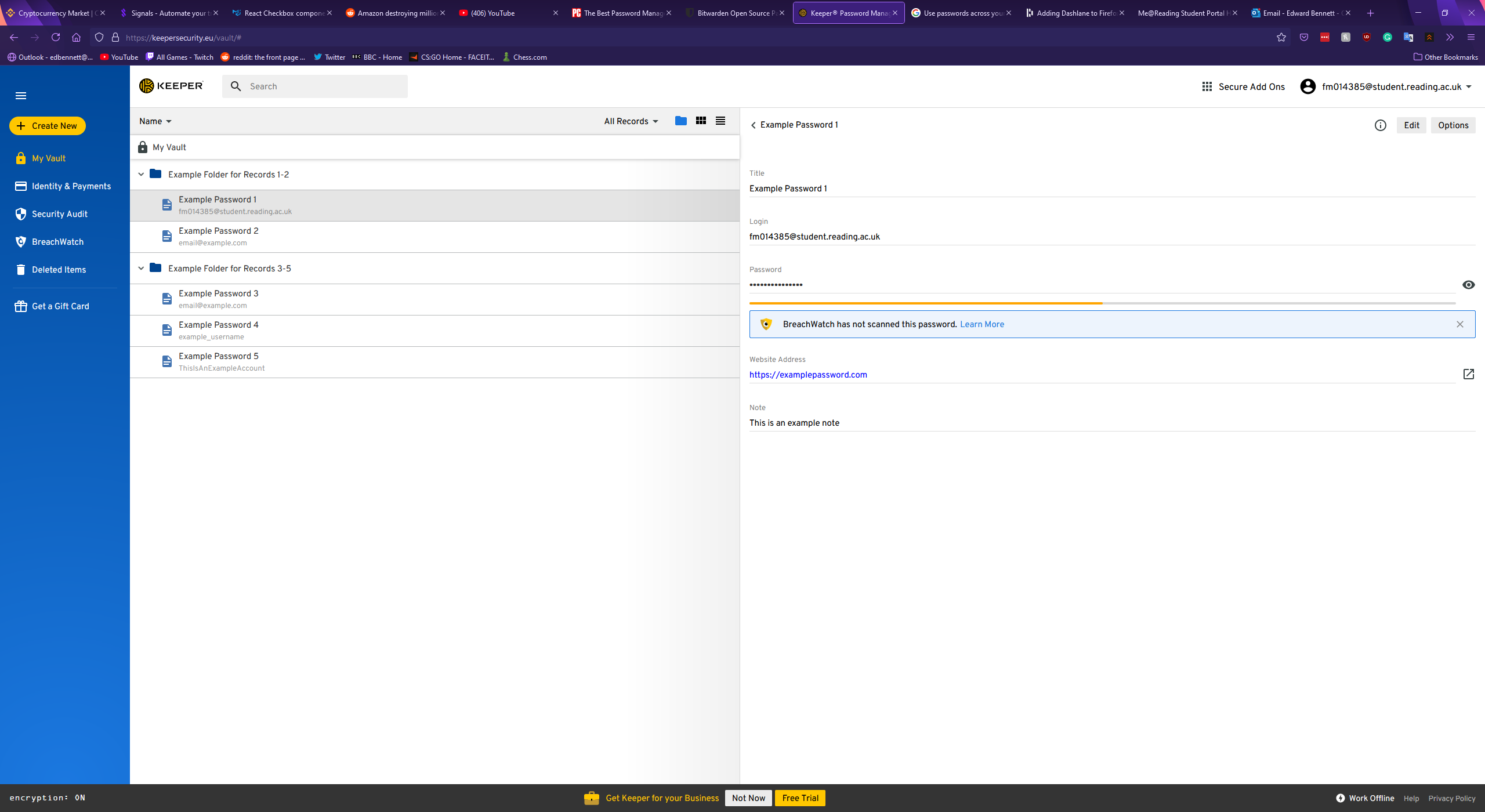
# Introduction

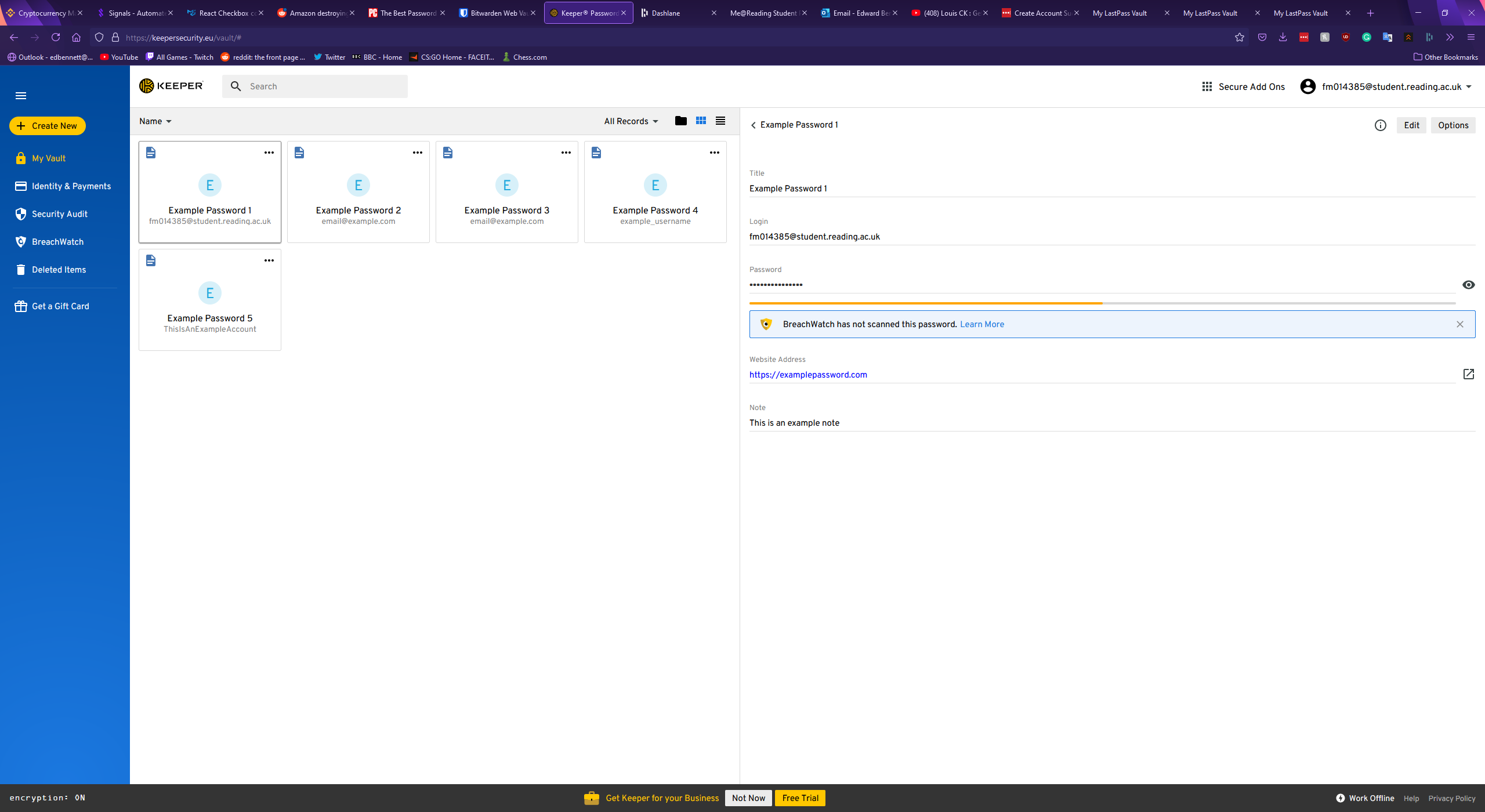
# Research of Existing Products

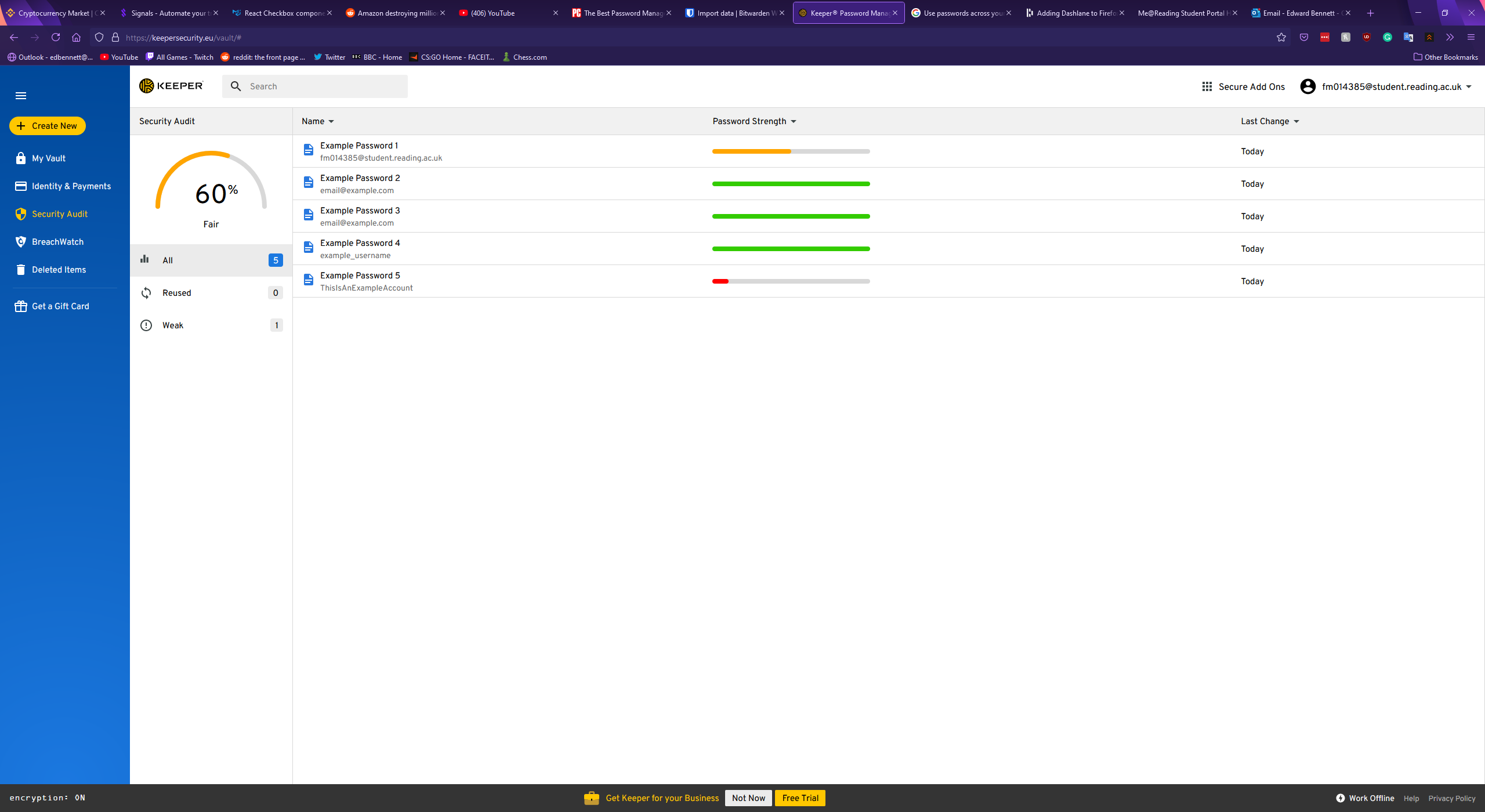
To research features and design choices for this project the first step was to examine existing products and identify features of these products which were both successfully and poorly implemented. Five existing password managers were identified: Keeper, Bitwarden, Dashlane, LastPass, and SplashID Safe. For each of these products an account was created with the same five example password records in two different folders to demonstrate how the manager might look under normal use.

## Keeper

Keeper is a password manager with a clean and simple modern design with little wasted space. Keeper has a simple intuitive interface which clearly communicates to the user how to add a new password, view existing passwords, and organise their database. Most of the real estate of the page is dedicated to password records and clicking on a password opens a window to the right showing all the information about the record. The passwords in the main window are organised alphabetically, inside drop-down lists of folders if the passwords are assigned to a folder. Three different views for the records are also available, a list view of passwords and folders, a card view of passwords, and a list view of all passwords without folders. These three views are shown below with the first example password selected.

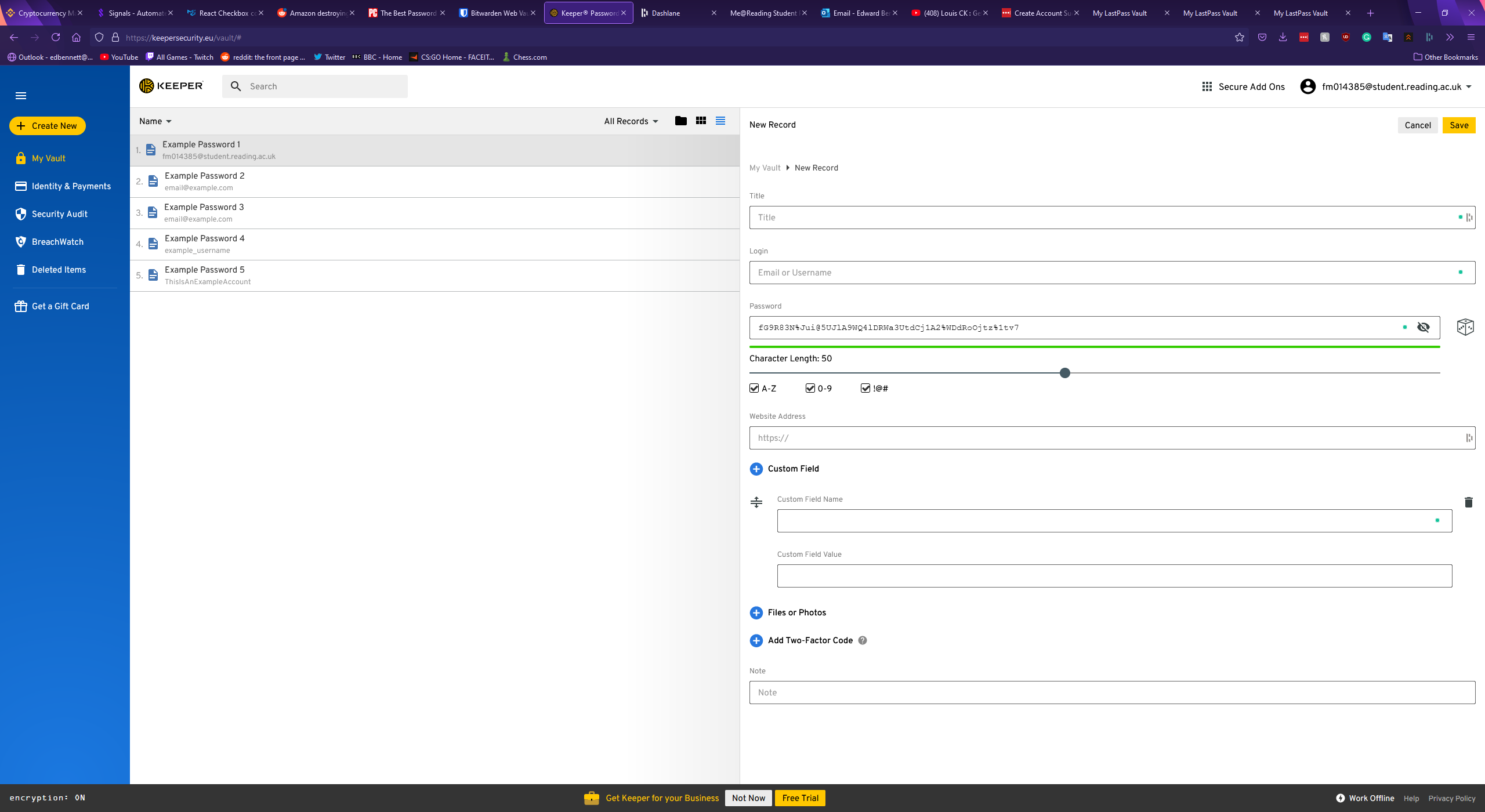






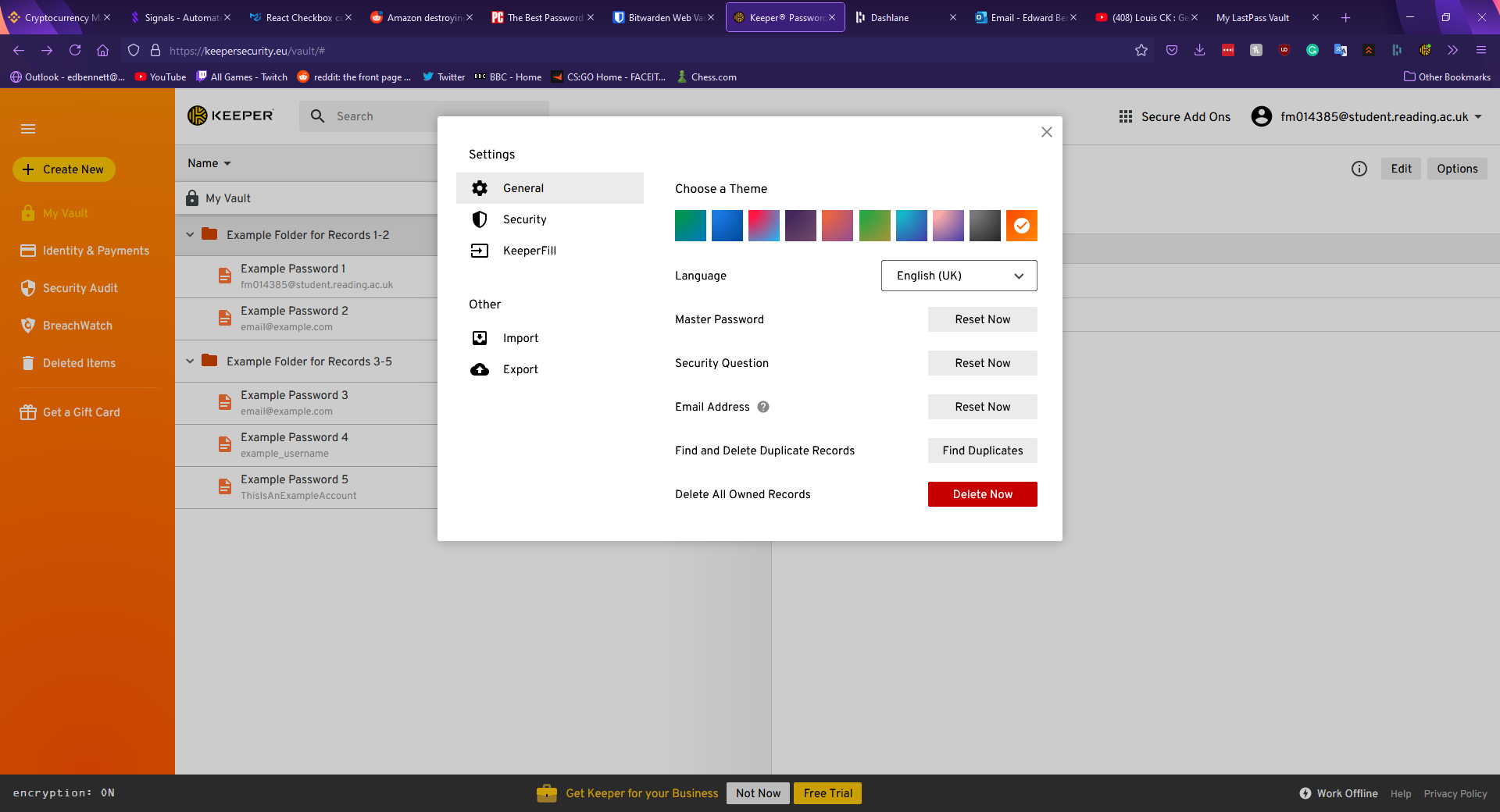


The records in Keeper are displayed simply, with each record possessing a title, a login value for a username or password, a field for the password itself, the website address, and a notes section. Each of these sections are optional, except for the title which must be filled in. In addition to these standard fields, Keeper allows custom fields, with the user able to give the field a name and a value, file or photo attachments, or a two factor authentication code. Once a record has been saved to the vault clicking on a field copies the field’s value to the clipboard, allowing for more convenient copy and pasting of a username or password elsewhere, however this does mean altering a record can only be done after clicking a small edit button in the top right corner of the record. This could make editing a record frustrating for a user, and as the button is grey instead of highlighted a new user could struggle to find this feature. A second button labelled “Options” is next to the edit button, and this offers a shortcut to open the corresponding website for the record, a premium feature to roll-back the version of the record, sharing the record, adding the record to a list of favourites, assigning a colour to the record, duplicating the record, or deleting the record. Offering a colour coding system for records is a unique feature that could allow for quick identification of a password at a glance. The option to mark select passwords as favourites could also offer a convenient timesaving measure for a user, however placing the function to delete a record in such an obscure position could cause irritation for users as such a key feature is not immediately apparent. The window for creating a new record is shown below.

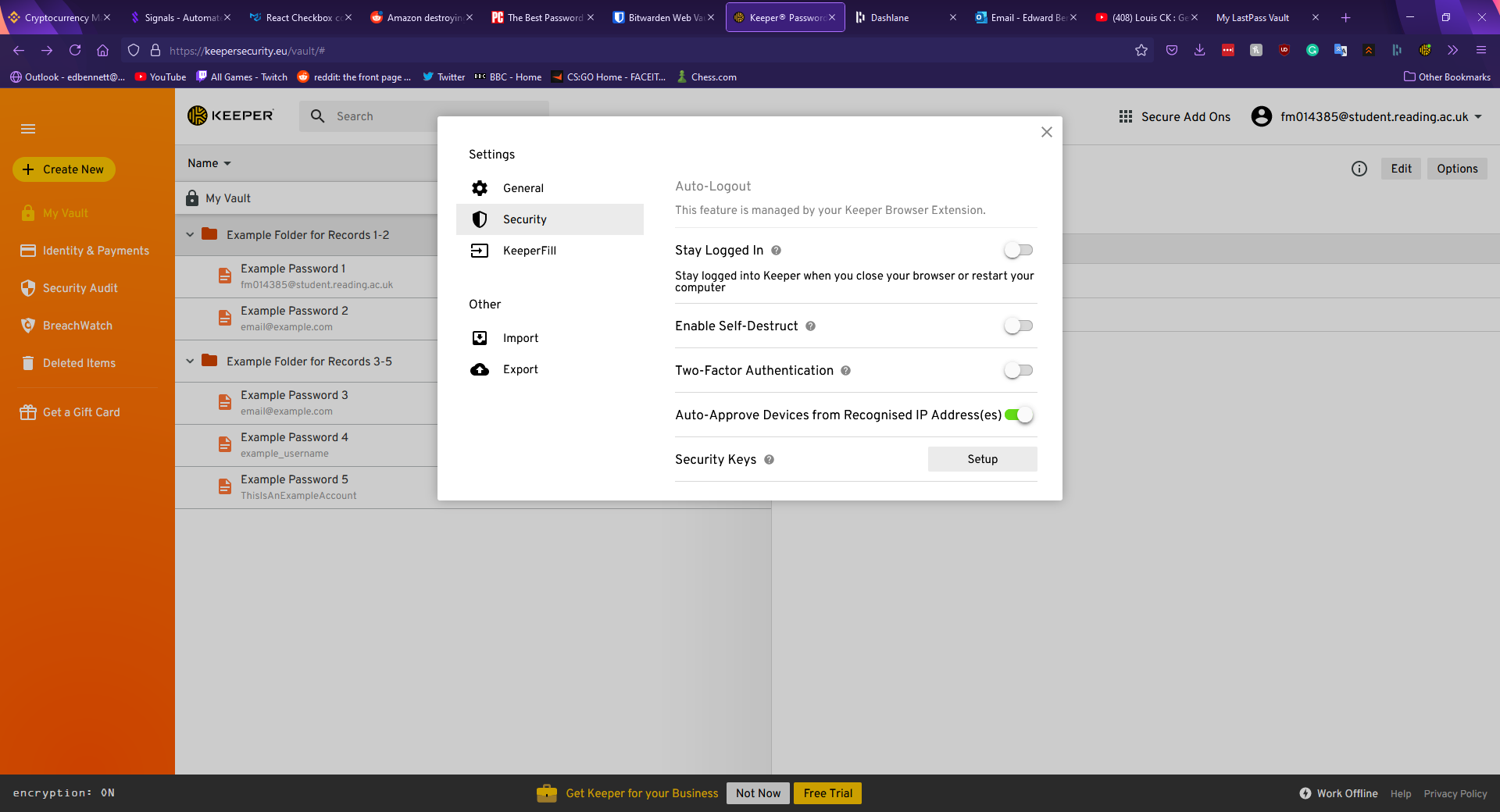


Keeper also includes a convenient password generator built into the new record window. The generation of a password is depicted by a dice icon, and once clicked a 20-character password is immediately generated and the generation settings expand if the user would like to tweak these settings. The settings for password generation include capital letters, numbers, and symbols, however lowercase letters are enabled by default and cannot be turned off. The length of the password can be customised between 8 and 100 characters in length. The above screenshot also shows the password generator with the settings expanded and a generated 50-character password with all characters enabled.

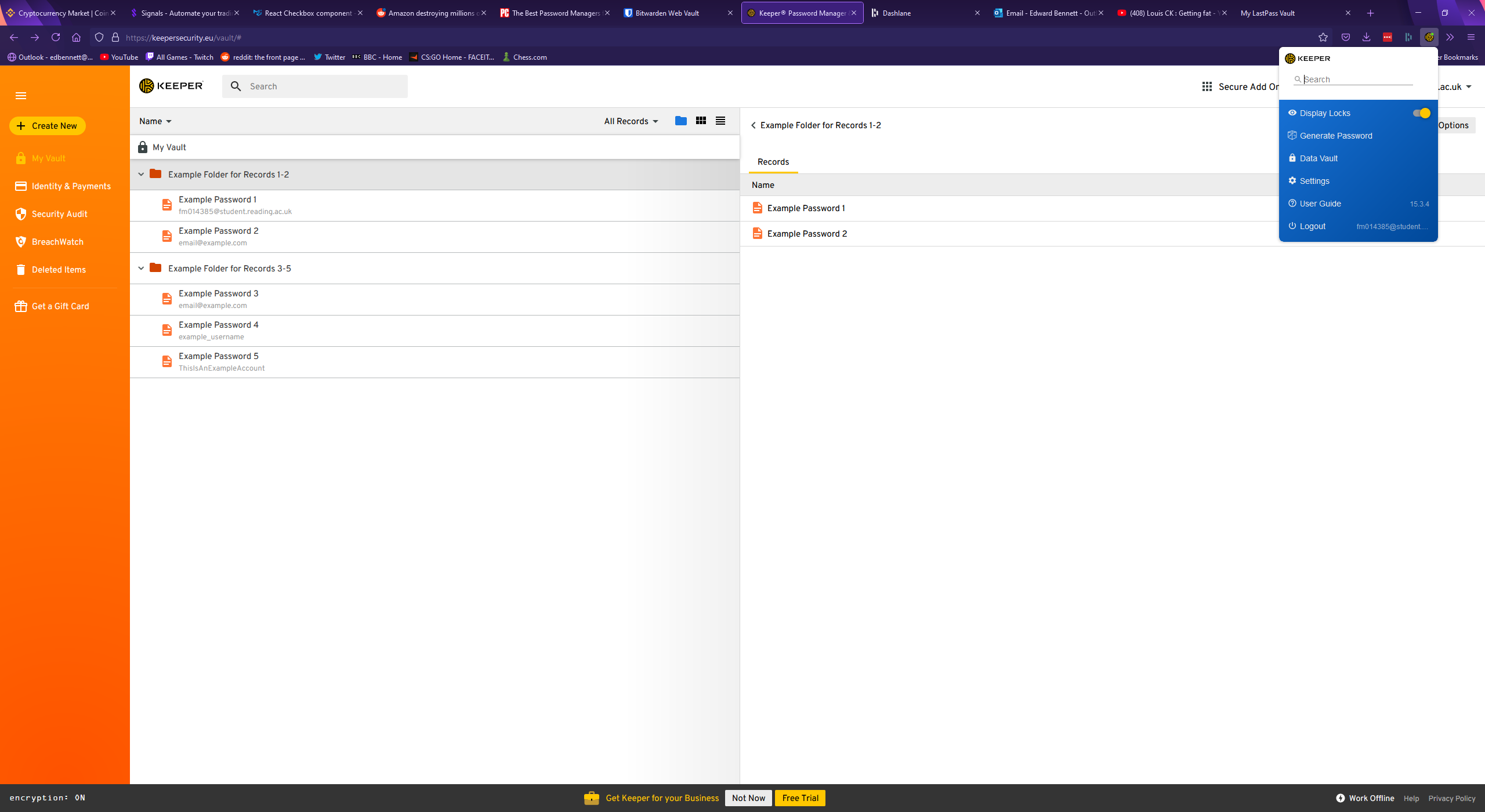
The settings and account page of Keeper is simple, with multiple tabs offering separation of concerns. The first tab shows general settings, and this allows a user to pick a theme. A feature for colour control could offer greater accessibility for users with conditions such as colour blindness or dyslexia, however the implementation here appears to mainly target aesthetics, as it only changes the colour of the sidebar and some icons. The general options page also includes options to reset the account’s master password, security question, and email address. An organisational feature to automatically find and delete any duplicate records is included here and could be valuable for any users with large and poorly managed databases. Finally, a feature to delete all records is included at the bottom, highlighted in red to indicate that it is a dangerous option a user should not click out of curiosity. The general settings page is shown below.



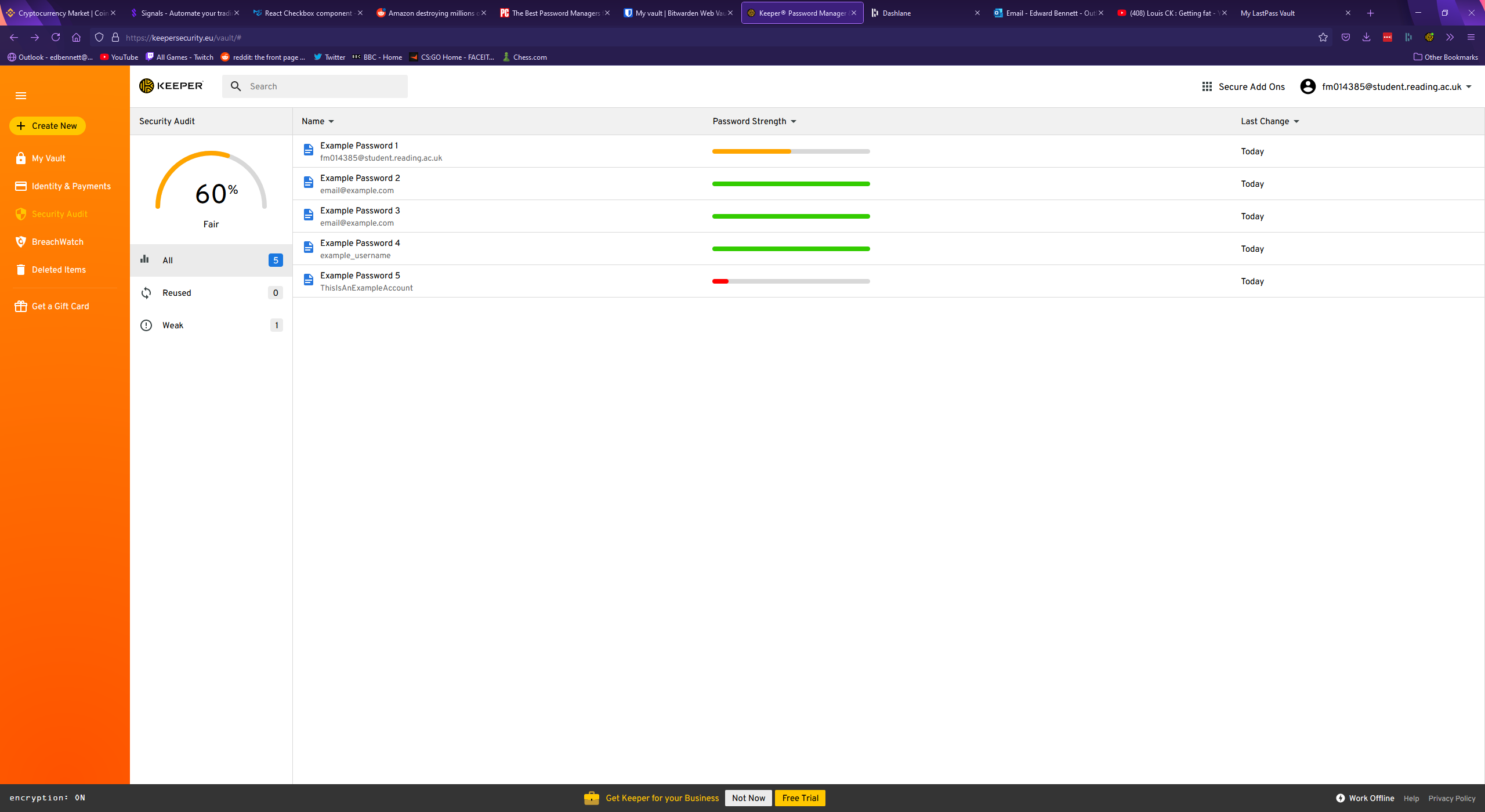
The second tab in the options menu is the security tab, and this section offers the user toggleable options to keep the user permanently logged in, a “self-destruct” option to enable automatic deletion of all records if five incorrect attempts to log in have been made in a row, an option to enable two-factor authentication for the account (both mobile app based and physical key based), and automatically approve devices from recognised IP addresses. This window of the settings menu is shown below.



The final sections of the settings menu offer links to download the Keeper browser extension and import or export records as a file. The Keeper browser extension allows for the quick searching of password records, generation of new passwords, and shortcuts into the main vault or the settings page. When logging into a website with the extension installed an icon appears next to the username and password fields with the Keeper logo. Upon clicking this icon, the extension offers to automatically fill the fields with stored records, or if no corresponding records are found the extension offers to create a new record and generate a password. This extension is shown below.

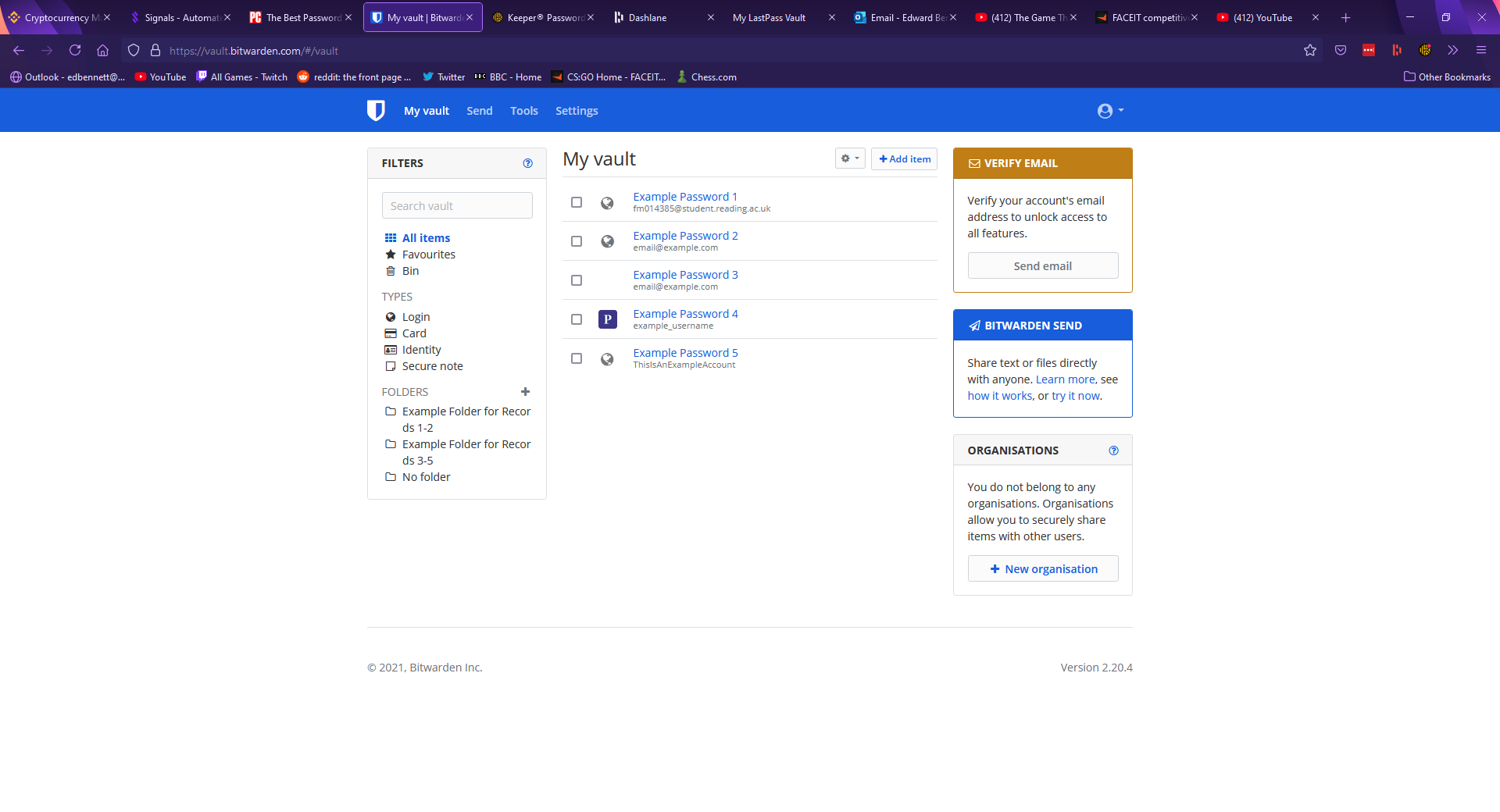


One other feature Keeper offers is a security rating page. This page rates the security of every password in the account with clear, simple breakdowns of each record, however the metric Keeper uses to determine the strength of a password, and specific reasons why a password is weak are not visible. The security audit page is shown below.

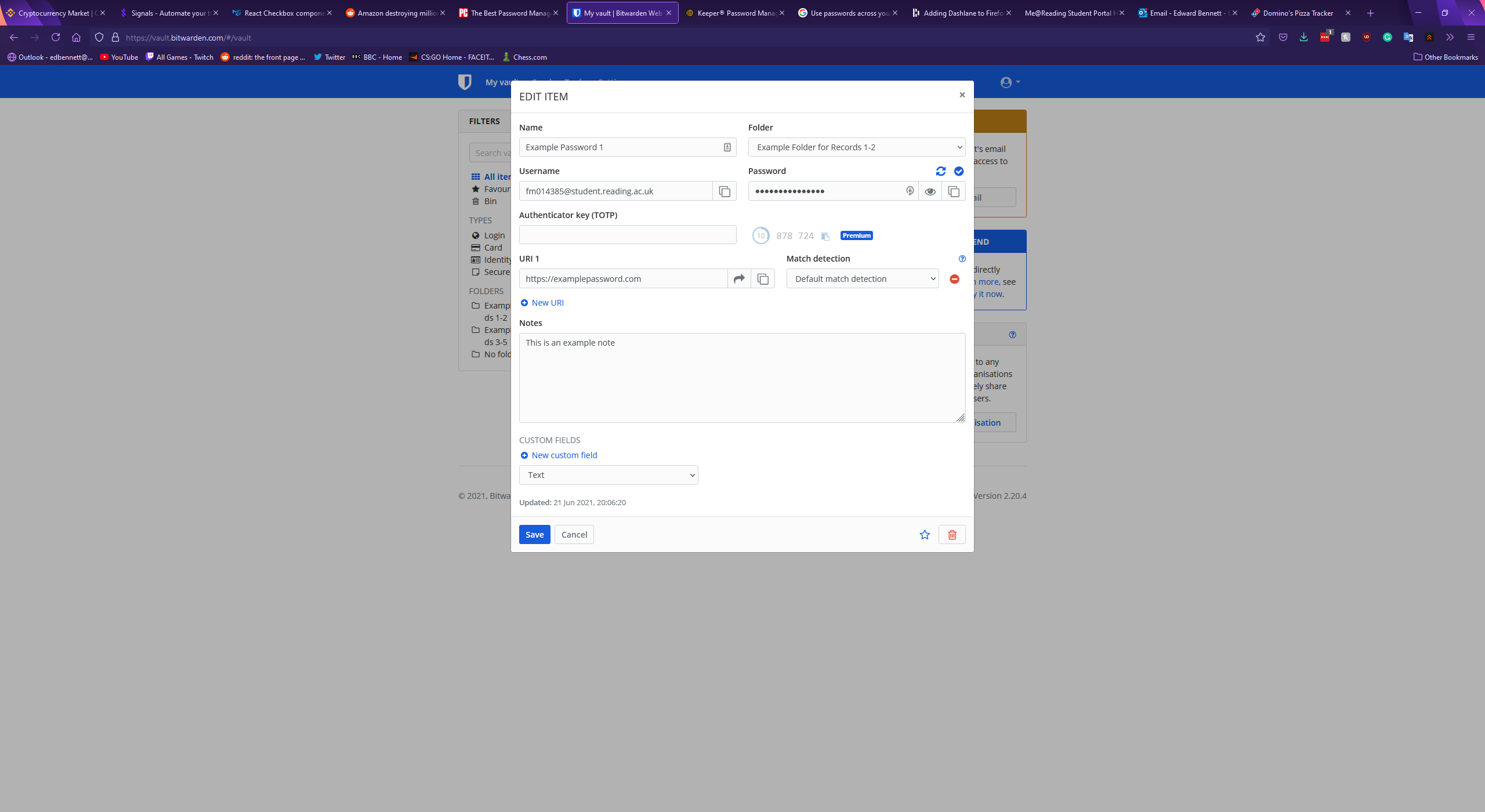


## Bitwarden

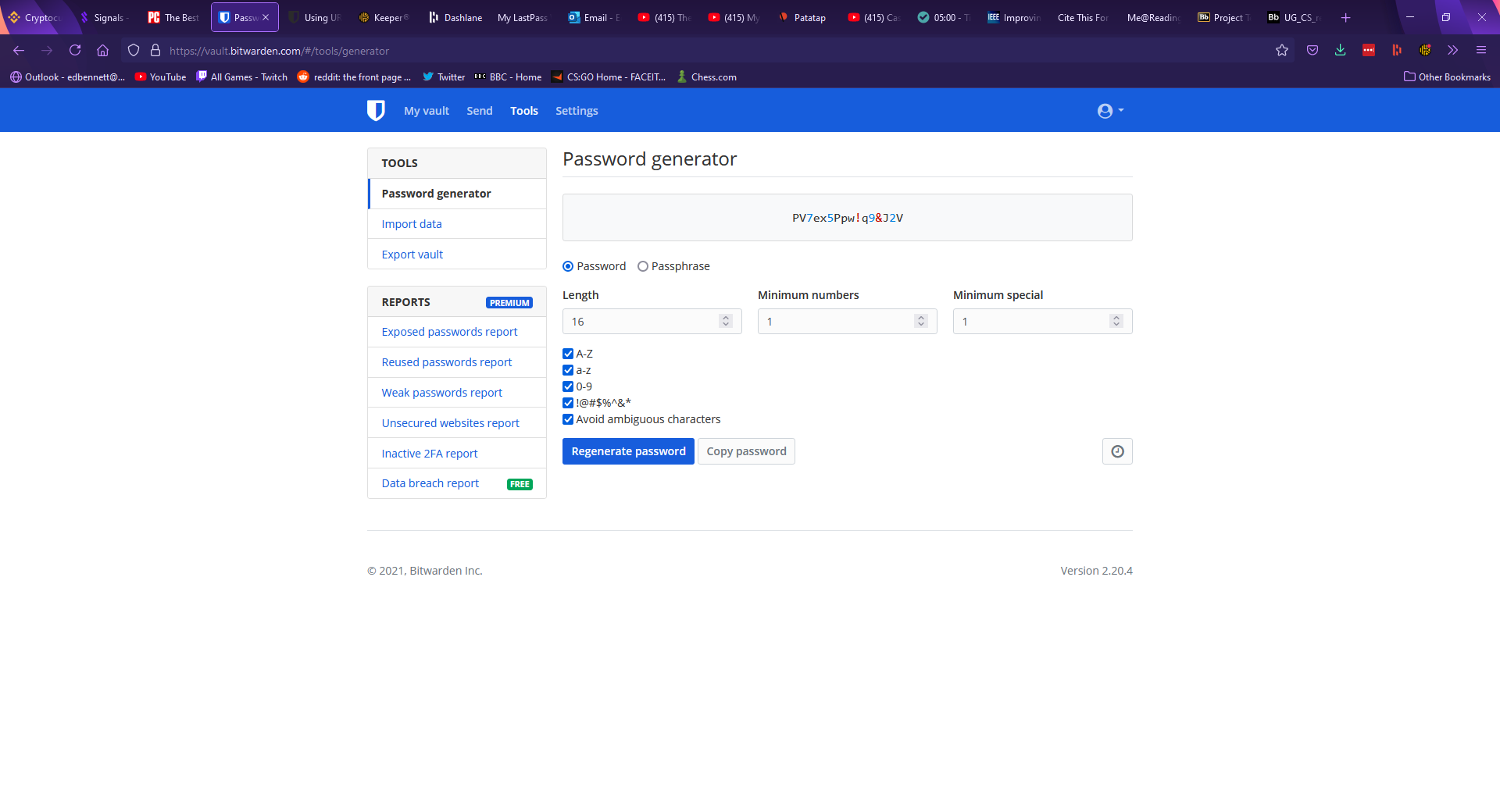
Bitwarden is a free open-source password manager. Bitwarden’s vault page has much more wasted space than Keeper’s, with records being listed in a center column. Various filters and folders are shown in a panel to the left, with no obvious indication on the password records themselves which folders they belong to. To open a folder the folder must be clicked on the left panel, which narrows down the list of records to only those records which are assigned to the selected folder, making Bitwarden’s implementation of a folder system more similar to a filter system. Keeper’s folder system appears superior in this regard, as multiple folders can be open and viewed simultaneously. Bitwarden’s main vault page is shown below.

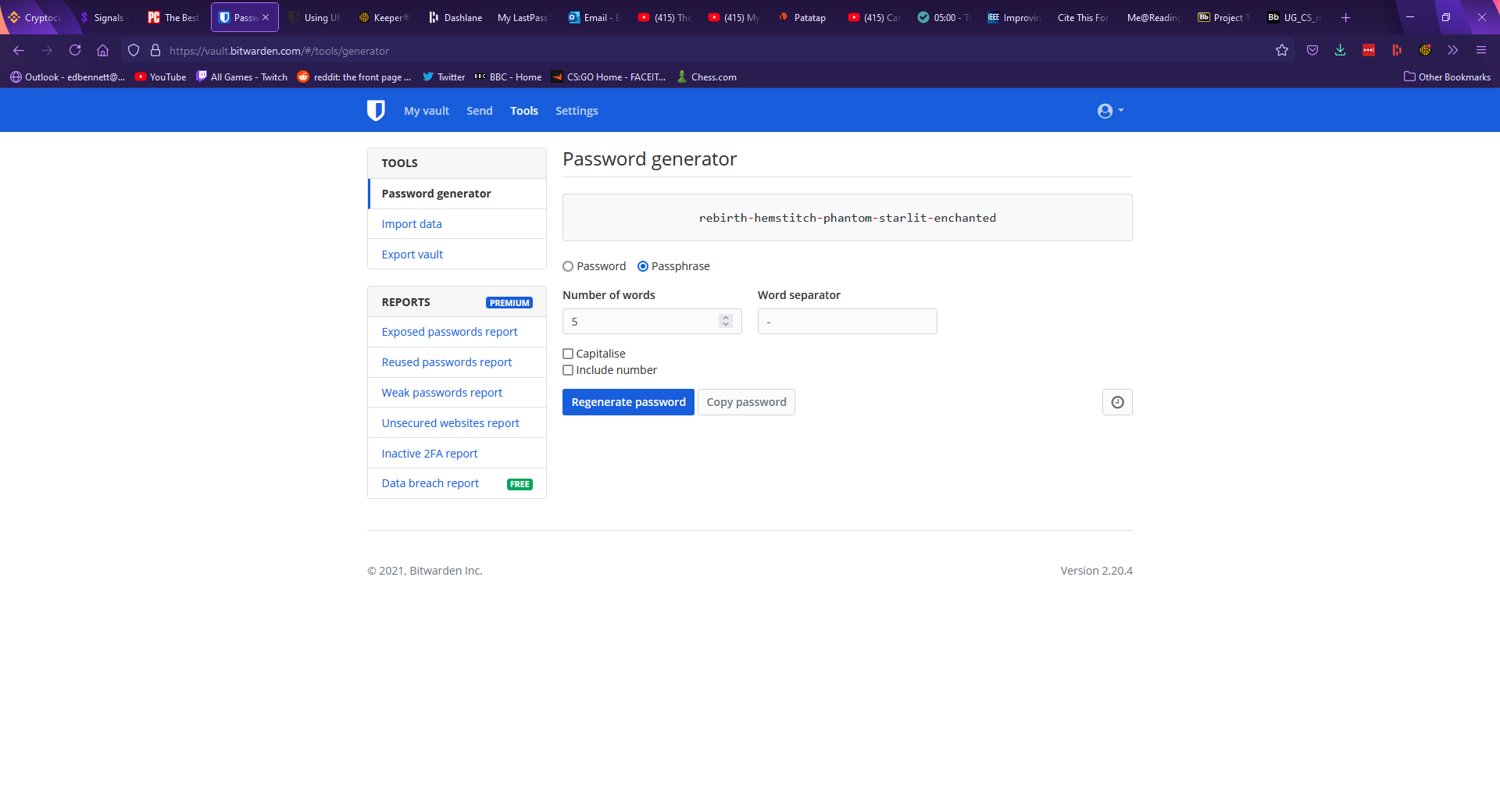


To view a record, one must click on the record in the centre column to expand information about the record. The record window in Bitwarden is much simpler to edit, with each field simply being a text box which can be typed in. Any changes are discarded unless a highlighted save button is clicked at the bottom. Bitwarden supports most of the standard fields, with fields for a record name, a username, password, and a notes section. Much like Keeper, Bitwarden supports custom fields, with the user able to choose from a text field, a hidden field, or a Boolean field. The records page is more upfront than Keeper’s, with options being immediately visible as links and buttons rather than hidden behind drop-down menus, potentially making the records page easier to navigate for a less experienced user. Bitwarden also supports a field for authentication keys, much like Keeper. Instead of URLs, Bitwarden uses a uniform resource identifier (URI) system, supporting multiple identifiers such as URLs, IP addresses, or mobile app package IDs. This allows for a greater range of identifiers to be used but may be confusing for a less knowledgeable user. A password record in Bitwarden is shown below.



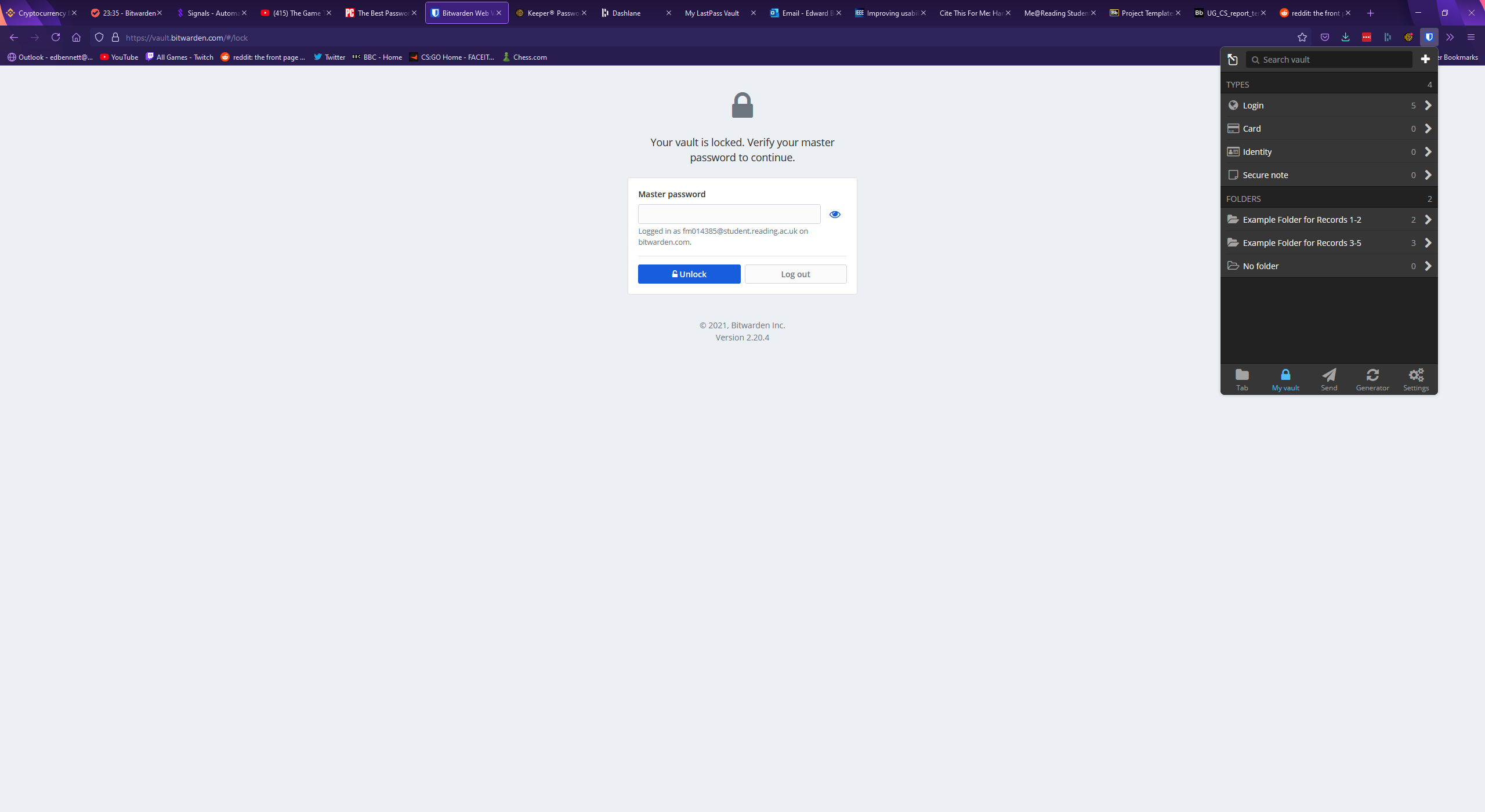
With regards to password generation Bitwarden’s record page lacks behind Keeper in terms of customisation. Just above the field for a password a button offers to generate a new password, however there are no settings for this generation. A randomised password including lowercase letters, uppercase letters, numbers, and symbols is immediately generated and filled in the password field. In addition to the records page, however, Bitwarden has a tools page which contains a more detailed password generator, offering a checklist of character types to include along with a customisable length, a minimum number of numbers and symbols, and an option to avoid ambiguous characters. Bitwarden also includes the option to generate a passphrase instead, randomly selecting a set number of words and putting them together. Nielsen et al believe “One way to deal with the failings of password based authentication systems is to increase the length without necessarily increasing the complexity of recalling the password”. Passphrases are then suggested as “Most people find it easier to remember passphrases, consisting of real sentences, than passwords created from random characters” (Improving usability of passphrase authentication, 2014). This suggests that Bitwarden’s passphrase generator could be more effective for password security than a standard password generator. The more detailed password generator is shown below, followed by the passphrase generator.





Under the remainder of the tools page Bitwarden offers features to import and export password data, and premium features to analyse whether stored passwords are weak or have been exposed. Under the settings page Bitwarden first offers account settings, with options to change the account name and password hint at any time, with the master password and the account email only being changeable once the current master password has been entered to confirm. Settings are also offered to change the encryption of the account, such as changing the number of key derivation function iterations. The second section of the settings page refers to customisation options and allows the user to set an interval after which their account will be locked and will require the master password to be re-entered. This page includes a few other miscellaneous settings such as setting an avatar for the account. In a third “organisations” tab Bitwarden allows the user to add groups they can share passwords with. The final tabs of the settings page offer billing information, emergency contacts, and two-factor authentication. Bitwarden’s two-factor authentication supports various mobile apps such as Google Authenticator and physical security keys such as Yubikey.

Bitwarden also offers a browser extension, which shows any logins for the website open in the current tab, along with tabs to search the entire vault, generate a new password, and change settings for the extension. While the Keeper extension placed an icon next to any login forms, Bitwarden’s extension can autofill a login form by right clicking on a username or password field and selecting autofill. An option is also given to generate a password and copy it to the clipboard; however, the extension does not automatically fill the field. This implementation is less obvious than Keeper’s icon, and many users may not find this feature. Upon logging in to a new account Bitwarden does not have a record for, a banner appears at the top of the tab offering to automatically add the account to the user’s vault. Bitwarden’s extension is shown below.



Vault/homepage – how nice does it look? How simple/intuitive is it? Is it easy to use?

Password records – any nice features, notes section, images?

Password generation – how simple is it, how many options, is it convenient?

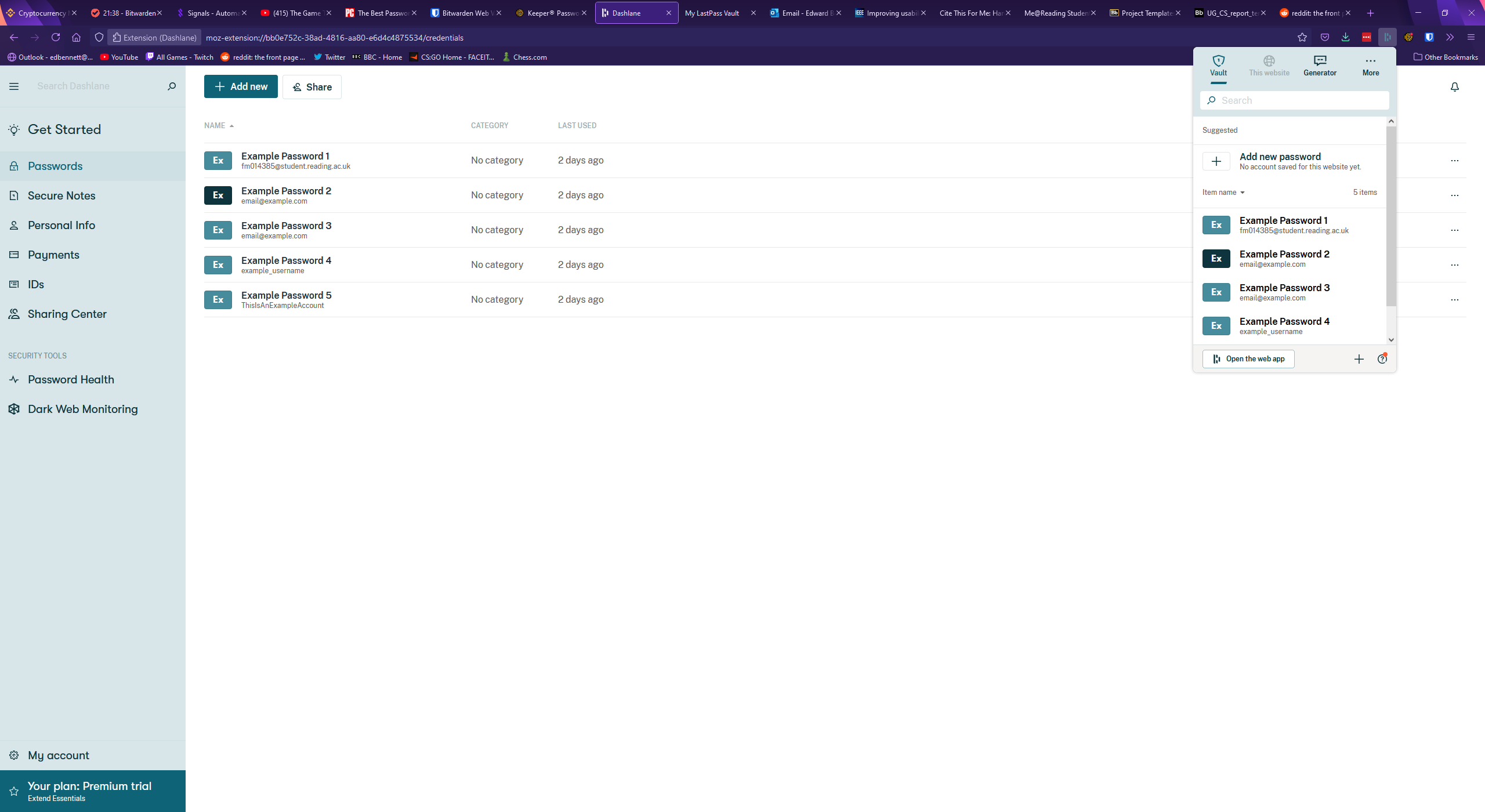
Settings and account

Browser extension

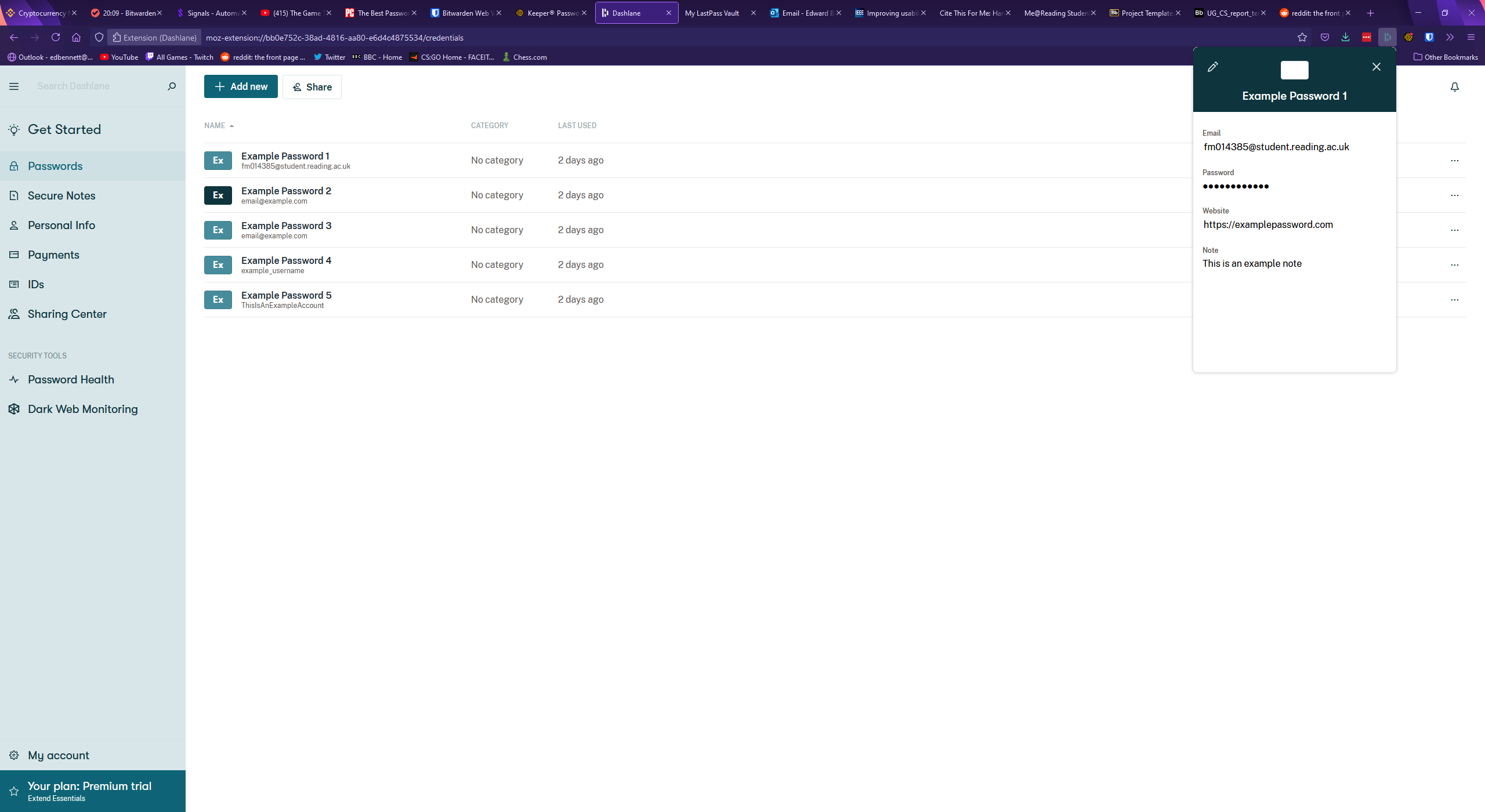
Misc features – security rating, import/export, 2fa, encryption

## Dashlane

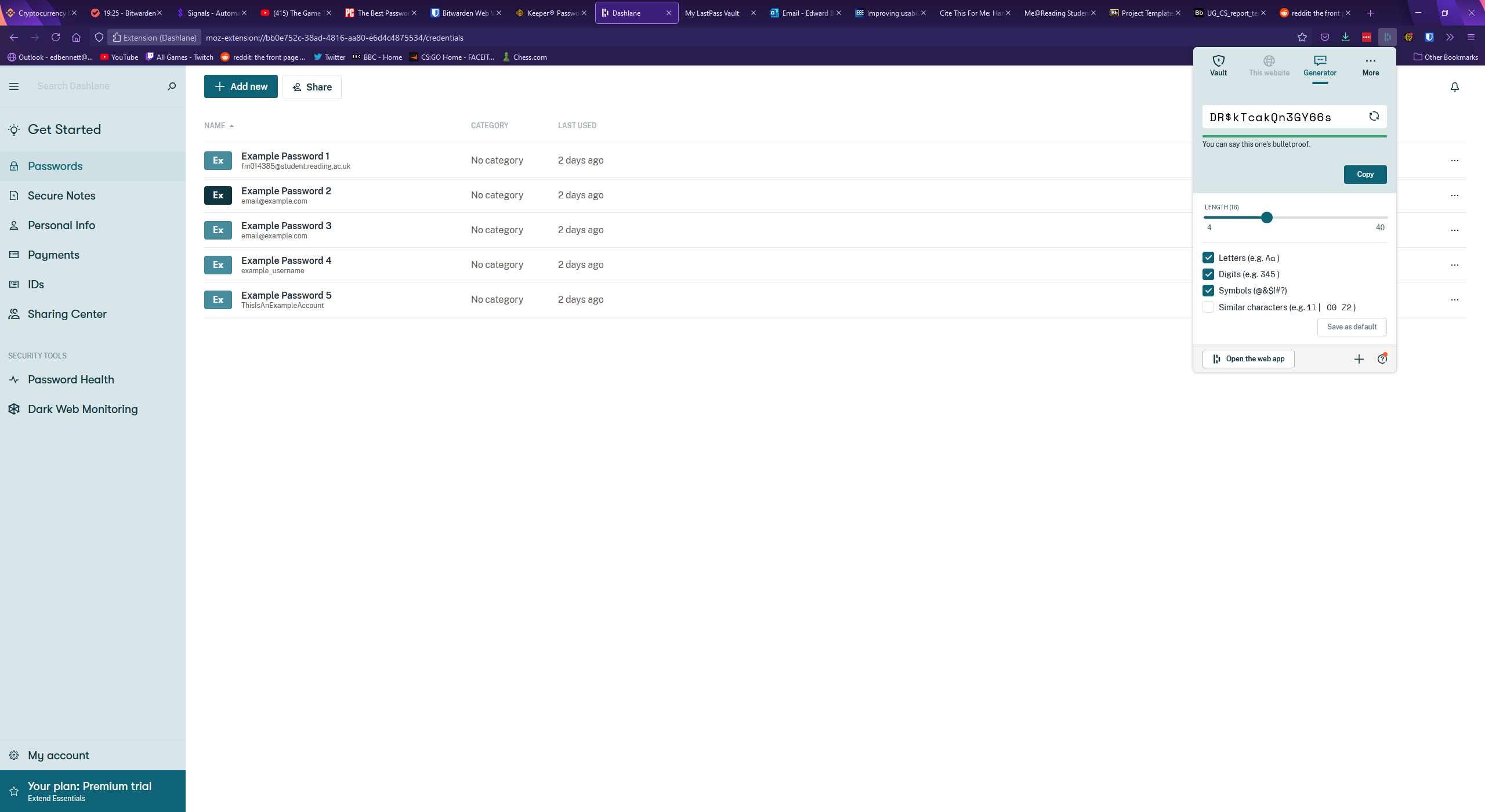
Dashlane is a password manager that functions through a browser extension. Rather than being a website which can be accessed from any device, Dashlane requires the user to have installed the extension to use it. Upon clicking the icon for the extension, it expands similarly to the Keeper extension.



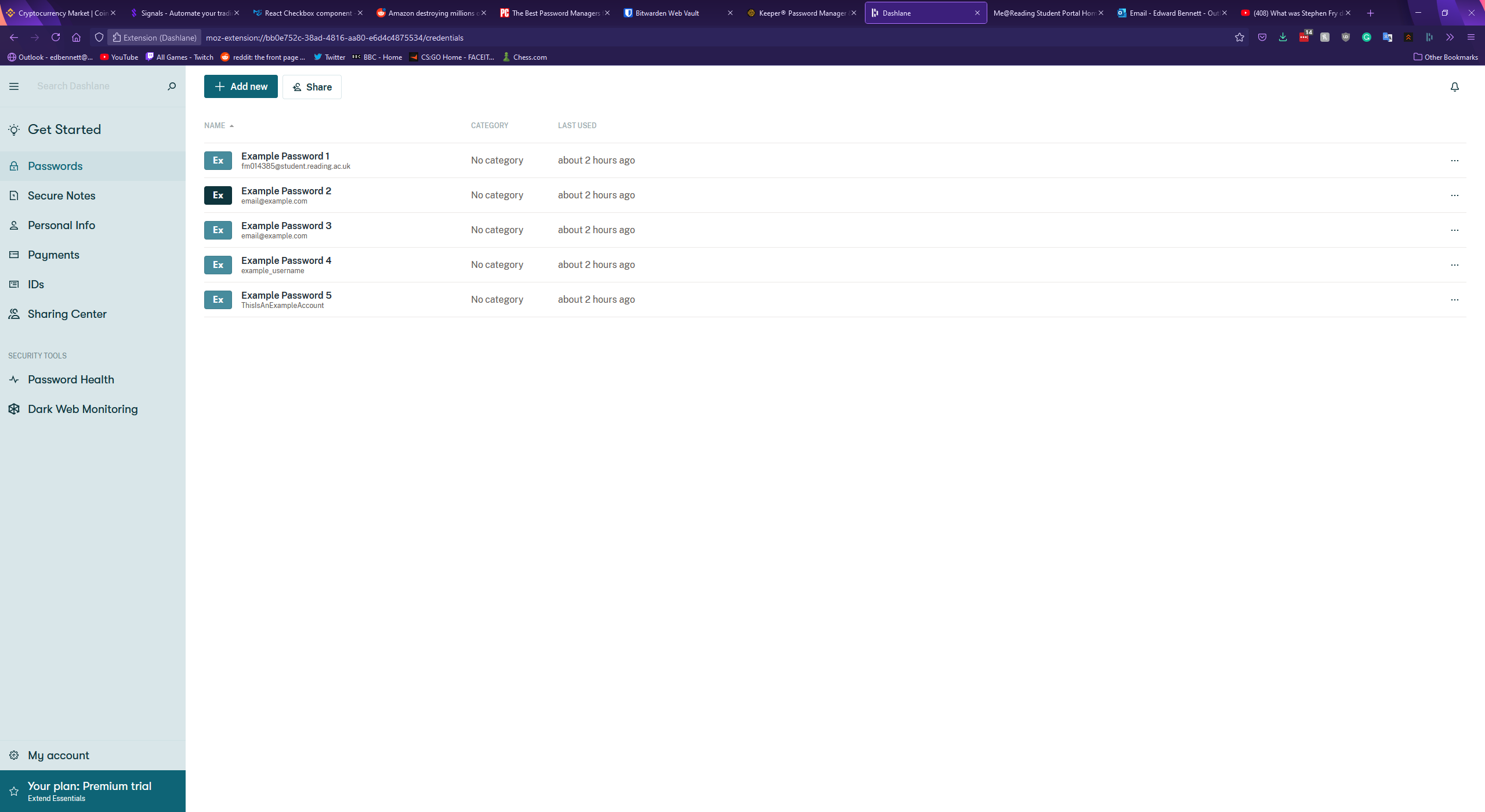
The user’s vault can be accessed and searched from this extension and clicking on a password will open that password record, shown below.

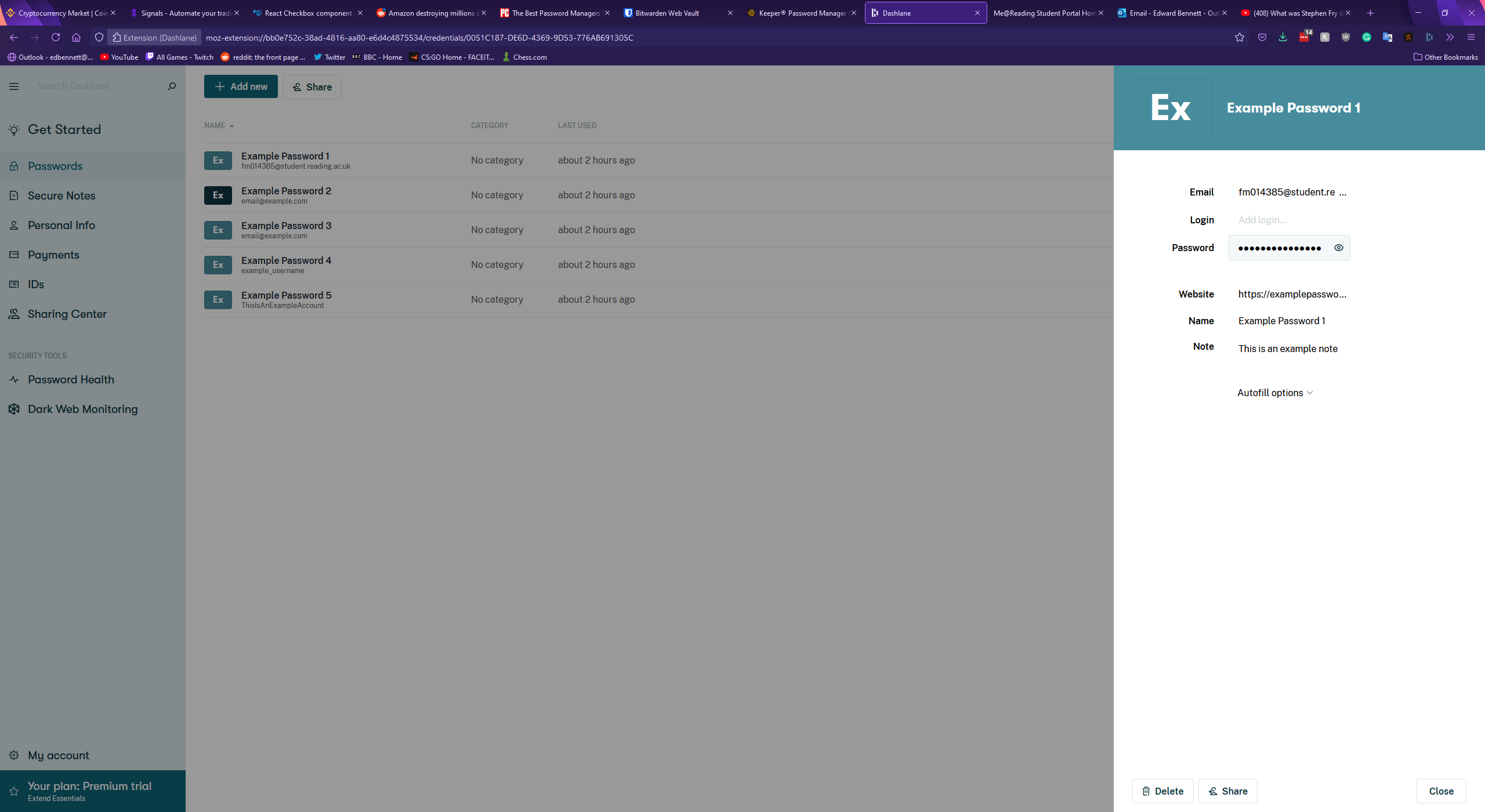


Dashlane’s extension also includes a password generator, automatically displaying a generated 16-character password including letters, numbers, and symbols. No distinction is made between uppercase and lowercase letters. This generator is shown below.



Upon attempting to create a new password, or upon clicking the button labelled “open in web app” the larger web app opens, showing a vault much more similar to the other password managers. Aesthetically, Dashlane’s web app is closer to Keeper than Bitwarden, with records shown in a full-window width list next to a large sidebar which can be minimised to just icons. Each section of the web app is clearly labelled on the sidebar, which should make the app easy to navigate. A search bar is clearly presented at the top of the sidebar with placeholder text and an icon, clearly identifying it as a search box. Dashlane uses a relatively muted colour scheme and mainly uses shades of green which could aid accessibility as there are no additional colours for colour blind users to confuse.

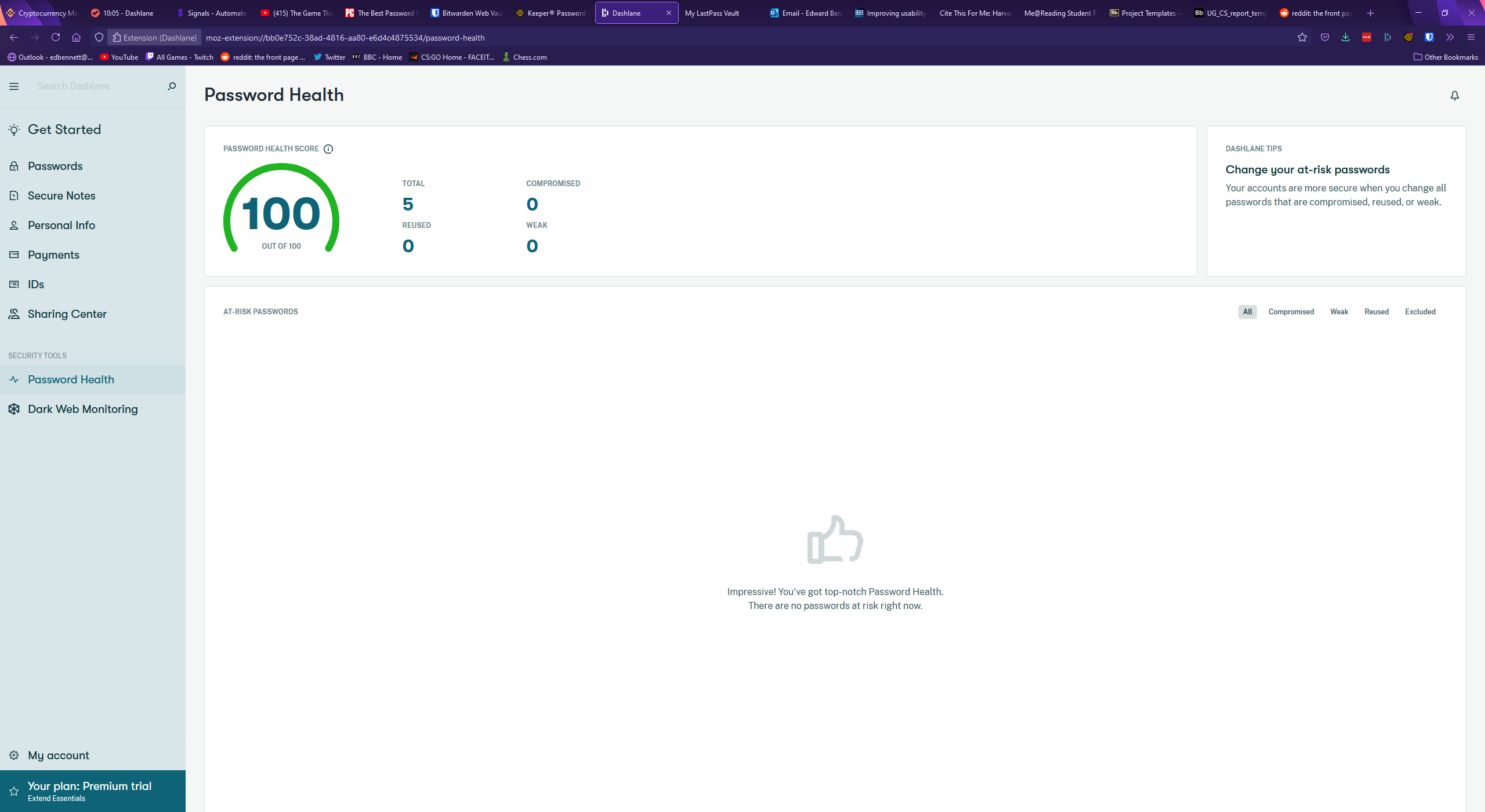


Clicking on a password record in the vault expands the record in a new panel to the right. This panel shows all the fields of the password along with buttons at the bottom to share or delete the record. Autofill options for use with the browser extension are also available. Interestingly, Dashlane includes separate fields for an email and a login, whereas both Bitwarden and Keeper elected to treat the email of a record as a type of username. Each field is a text box and can be edited simply by selecting the field and starting to type. Dashlane includes no folder system, and passwords must be found simply by either scrolling through the list of all records or by searching for them. Dashlane also does not include custom records. The Dashlane vault with an expanded record is shown below.

Creating a new password in Dashlane is started by clicking the green button at the top of the vault. This expands a blank record panel to the right, with empty fields. While Keeper and Bitwarden required the record to be given a name, Dashlane only requires that one field has a value, which could potentially make finding the record again later difficult. Password generation in Dashlane takes place solely in the extension, with no generation offered in the web app.

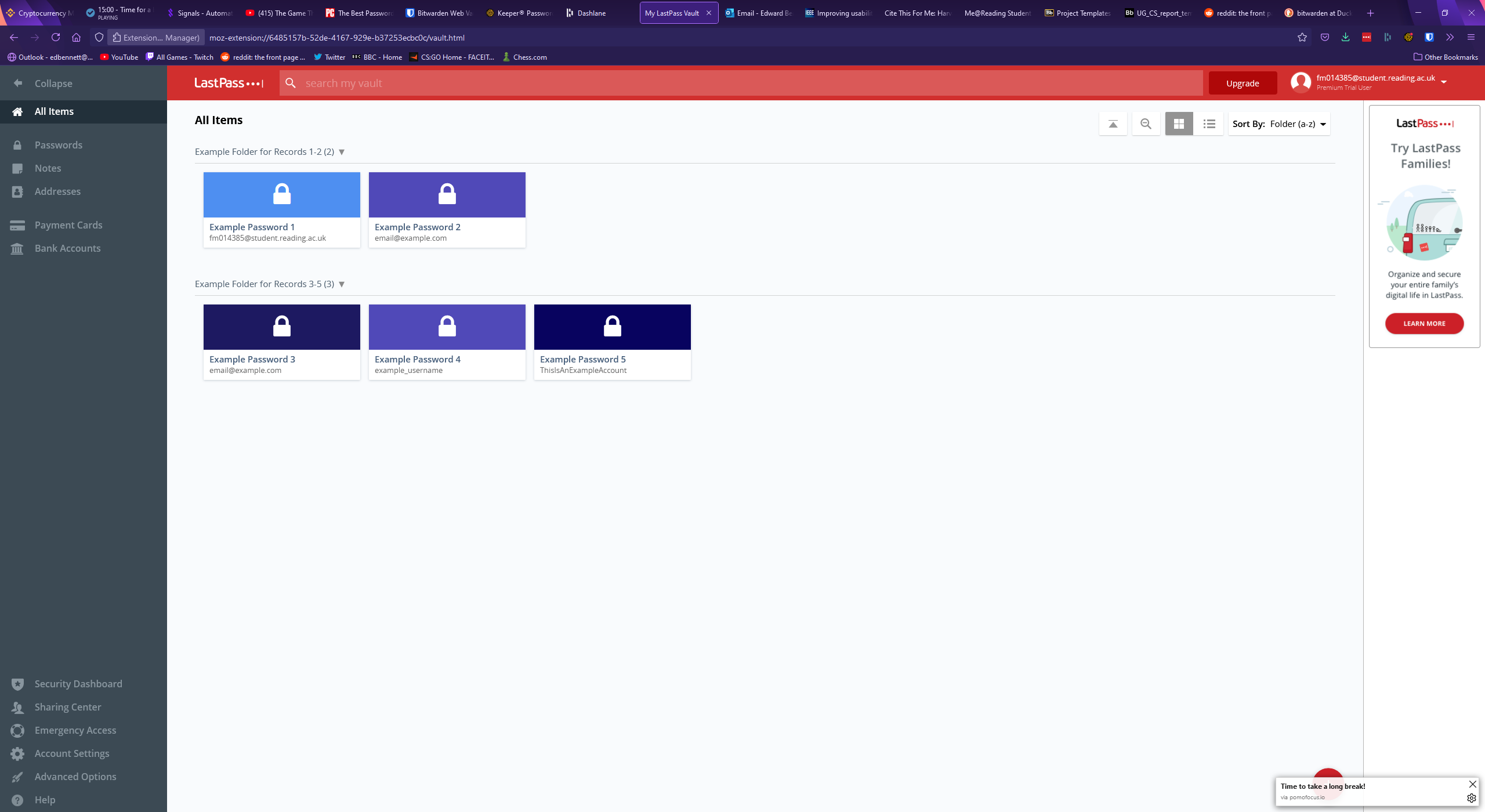
Dashlane’s settings page is accessed from the “My account” button at the bottom of the sidebar which expands another panel to the right. From here users can view and update their account information, manage any devices connected to the account, import and export password data, and set up two-factor authentication for the account. Dashlane’s two-factor authentication only supports biometrics and does not appear to support mobile or physical security key authenticators.

In terms of other features Dashlane supports the storage of personal information, such as emails, credit card and banking information, and IDs. Dashlane also offers a “Dark Web Monitoring” feature, promising a tool which “scans the dark web for leaked or stolen personal information”. If a tracked email address is found the user will be notified so they can act. Finally, Dashlane has a “Password Health” page, much like Keeper’s security audit page. This page shows a password health score out of 100, with any at-risk passwords displayed below. Interestingly, Dashlane gave differing results from Keeper’s security audit - though as neither service explains the metrics used to measure password security it is difficult to see why. Dashlane’s password health page is shown below.

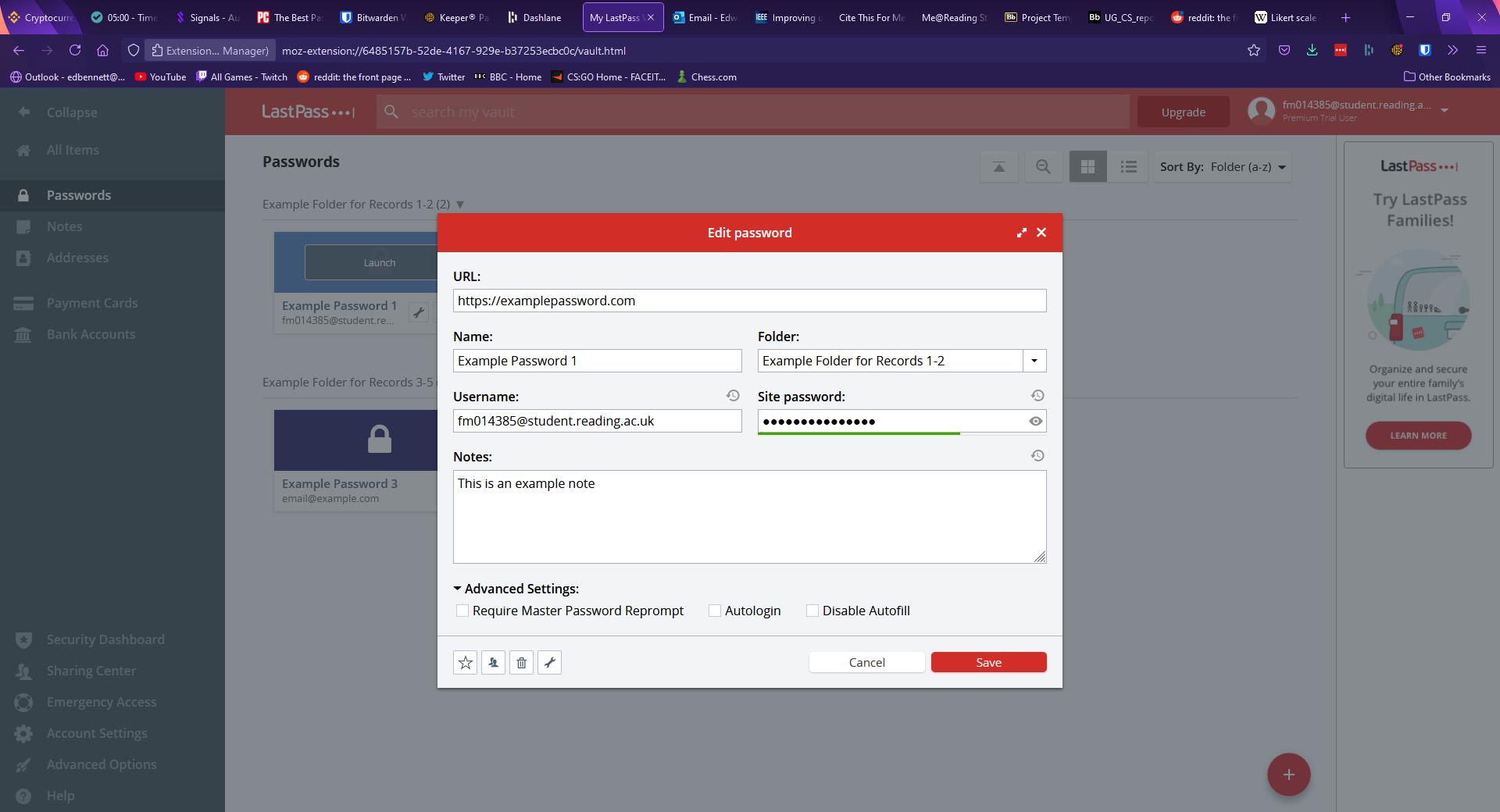


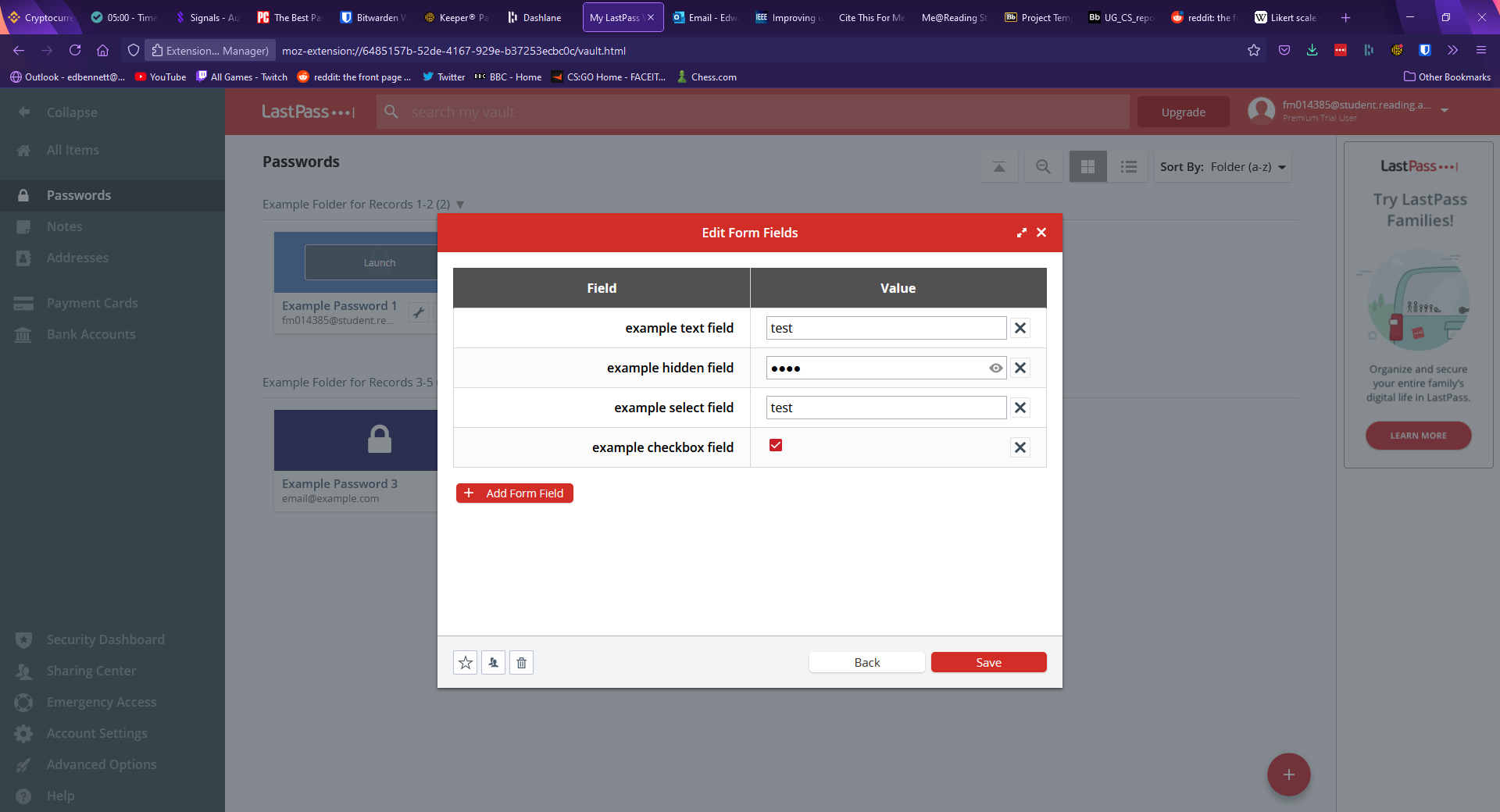
## LastPass

LastPass is another popular password manager which operates primarily through a web app rather than an extension. LastPass’ vault page displays records primarily as cards, with various buttons to change the layout offered above the list of records. These views include a more compact view, and a list view. Records are listed in folders which can be collapsed, much like Keeper’s vault design. LastPass has little wasted space, with the vault taking up the full size of the window, two sidebars, and a top navigation bar with a search bar. The top search bar narrows down the list of passwords displayed in the vault, rather than opening a drop-down menu with the search results, and next to the search bar is a button showing the user’s avatar (if one has been set) and email address. When clicked a drop-down menu is expanded which offers account settings, a forum-based support centre, and a log-out button. The support centre could be incredibly valuable for a new user initially getting to grips with the software, offering a dedicated place to learn from others and ask any questions about LastPass. The right sidebar contains little content valuable to the user, only containing an advert for LastPass’ other services, while the left sidebar is used for navigation, containing a list to different categories in the vault such as passwords, addresses, and payment cards. These categories are clearly labelled along with icons, which should make navigating the website as painless as possible for users. The home vault page for LastPass is shown below.

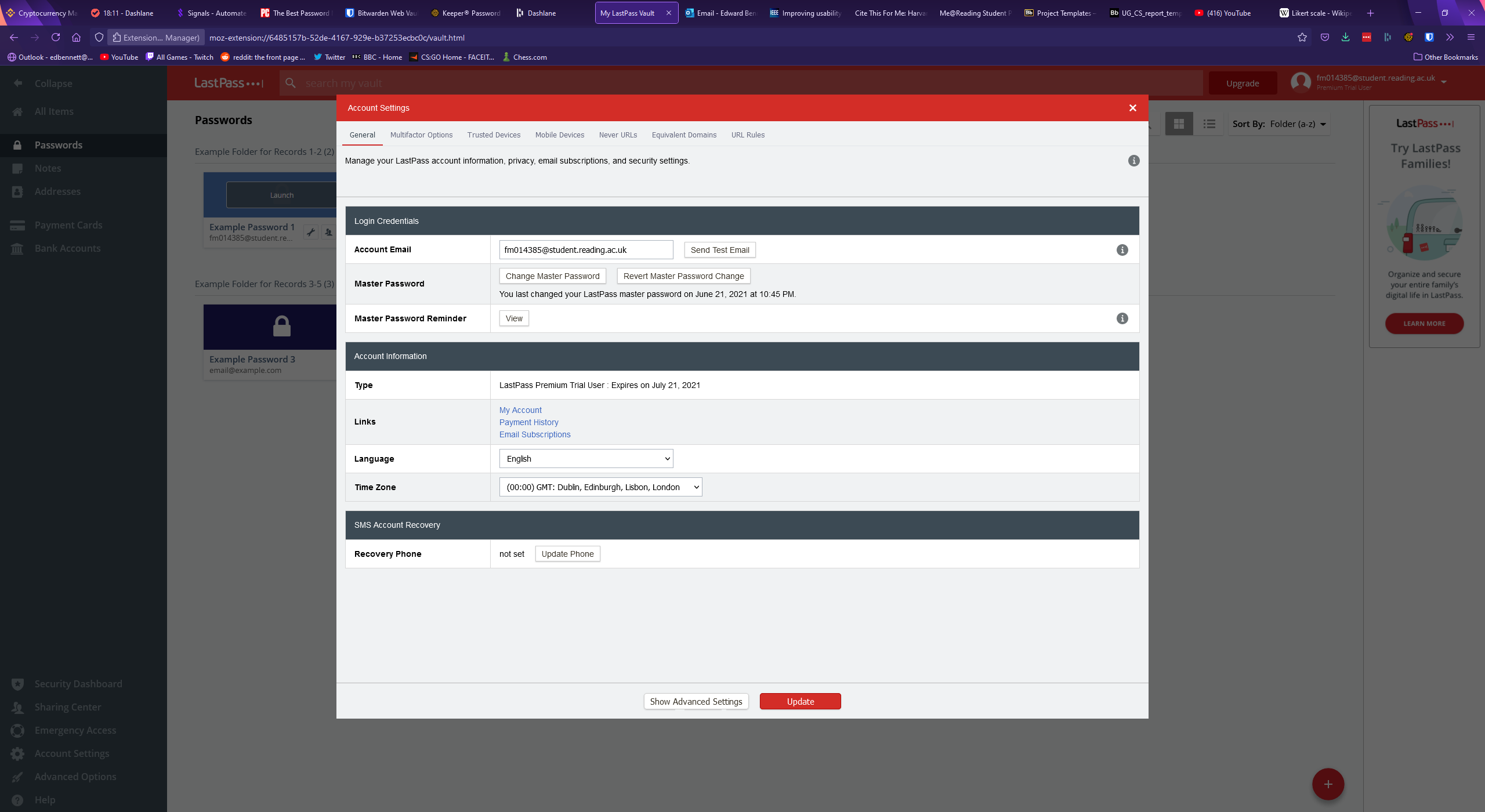


When a record in the vault is hovered over, buttons are displayed over the card. Three smaller buttons can be clicked to edit, share, or delete the record, while most of the card is dedicated to a launch button which acts as a shortcut to immediately open the record’s corresponding website. This could potentially become a source of frustration for a user, as if they click the centre of the card for a record expecting to see an expanded record they would instead be redirected to a different website. Clicking on the record anywhere other than these four buttons selects the record and would allow the user to select multiple records for deleting or moving to a different folder. Clicking the edit button opens an expanded record view like the previously examined password managers. LastPass has all the standard fields, each being a textbox, with values that can be changed by simply selecting the field and typing, unlike Keeper. LastPass has a drop-down menu towards the bottom of the record window for advanced settings where the user can toggle whether their master password will be required to view the record again, and whether this webpage will be automatically logged in to. LastPass includes buttons for viewing the version history of some fields, allowing the user to view previously viewed usernames, passwords, and notes for the record. This could be extremely useful for users who mistakenly change values in the wrong record, and now find themselves unable to reverse the changes they have made. Buttons to cancel any changes, save any changes, edit custom fields, delete the record, share the record, and mark the record as a favourite are placed at the bottom of the record window, with most of them identified by iconography. Custom fields are strangely placed behind one of these buttons, instead of being appended to the main record as they are in Keeper and Bitwarden. The placement of this feature could make it difficult for users to find or quickly refer to later. The image below shows a LastPass record followed by example custom fields assigned to the record.





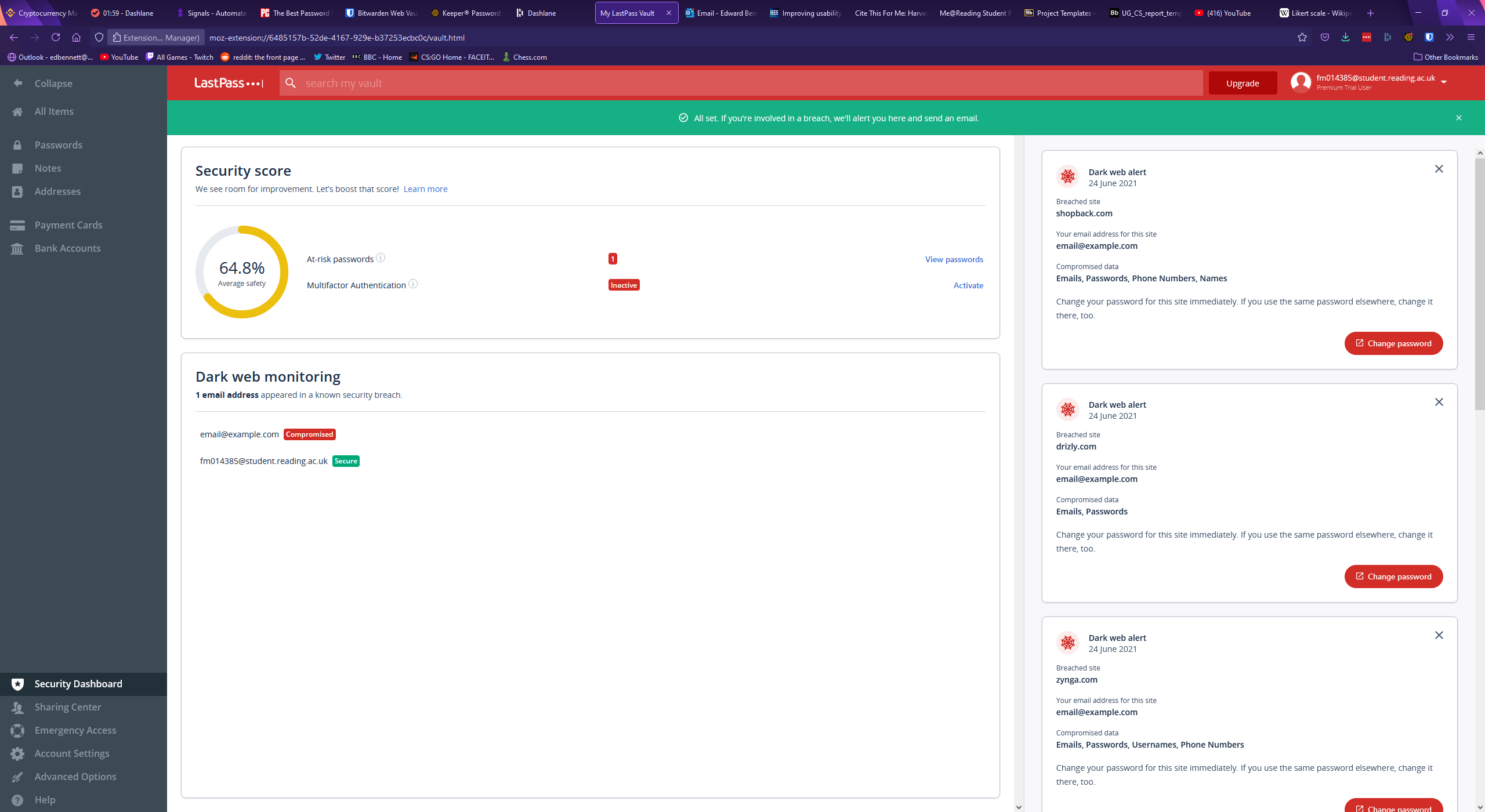
The settings page of LastPass can be accessed either from the drop-down menu on the navbar under the username or through a button on the sidebar, and appears much more detailed than the other password managers’. The general page allows the user to change account information such as email, master password, and master password reminder, along with settings other account information such as a preferred language and time zone. The second tab of the settings window is for multi-factor authentication, and it lets the user set up authentication with a range of apps or physical keys. The third and fourth tabs allow the user to manage devices which have access to the account, and revoke this access, while the remaining tabs govern autofill settings, such as blocking the LastPass browser extension from filling certain websites. LastPass has a second, advanced options settings window which allows the user to perform other actions such as importing or exporting password data, upgrading their subscription, view favourite records, or generate a new password. The main settings page is shown below.



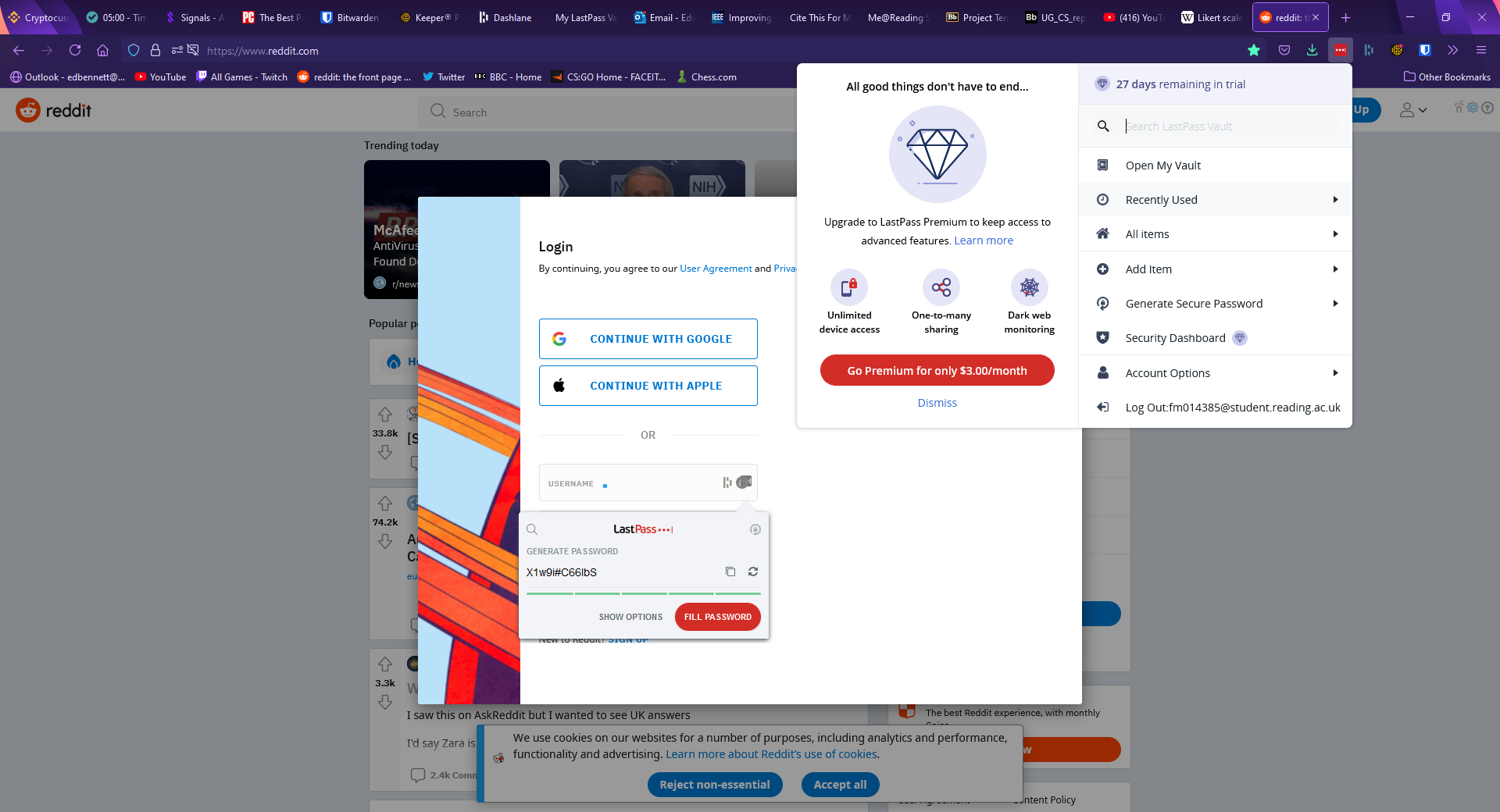
When it comes to password generation, LastPass has a panel which allows the user to select various settings. The default password length is 12 characters, with checkboxes offered to include uppercase, lowercase, numbers, and symbols. The user can customise the length of the password with either a slider or a text field, and radio buttons are offered to make the password easier to say or read by avoiding numbers, symbols, or ambiguous characters. Buttons are then displayed to allow the user to regenerate the password or copy the password to the clipboard for use. The password generator is shown below.



In terms of other features LastPass includes storage of private items other than passwords, including debit and credit cards, bank account information, and addresses. LastPass also includes a security dashboard, which fills a similar role to the security audit page in Keeper or Dashlane’s password health page. The security dashboard shows an overall security score which rates the average safety of all passwords, along with showing any passwords determined to be at risk. For this account LastPass also suggested turning on multi-factor authentication to improve the account’s security. Much akin to Dashlane, LastPass offers a dark web monitoring feature, which promises to proactively alert users “if sites from your vault are breached. Monitor these addresses. All day, every day”. Upon opting into the service, the master account email address and the email address of any other records are automatically searched and identified if they appear in any known security breaches. Alerts are then shown on the right-hand side for any compromised email address, describing the security breach and the specific data that was leaked so that the user can change compromised information to protect themselves. The security dashboard is shown below.



Like every password manager seen thus far, LastPass offers a browser extension. This extension can be used to autofill login forms for websites with existing records. In a manner very similar to Keeper and Dashlane an icon is placed at the end of username or password fields. If LastPass finds any corresponding records it will display them in a list for the user to select for auto-filling. If LastPass detects no such records, it will offer to generate a new password for a new record. Upon manually logging into a website for the first time the extension will pop up with a message offering to automatically add a record for the website with the username and password used. Clicking on the icon for the extension in the top right of the browser opens a menu with various options, including a search bar to search for records within the smaller extension window, a shortcut to open the user’s vault, and password generation within the extension. The main menu of the extension is shown below.



## SplashID Safe

## Comparison of Existing Products

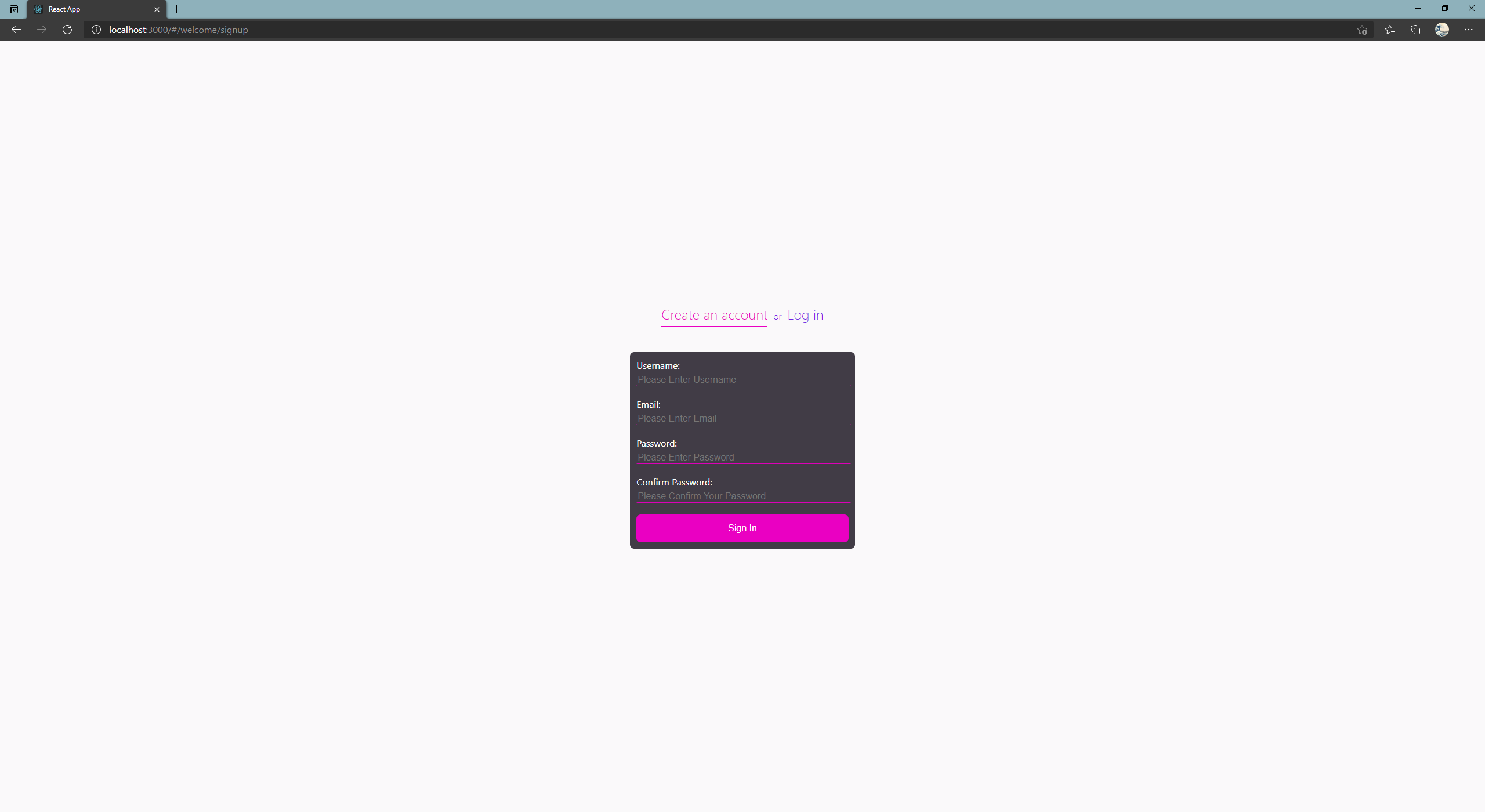
# Methodology

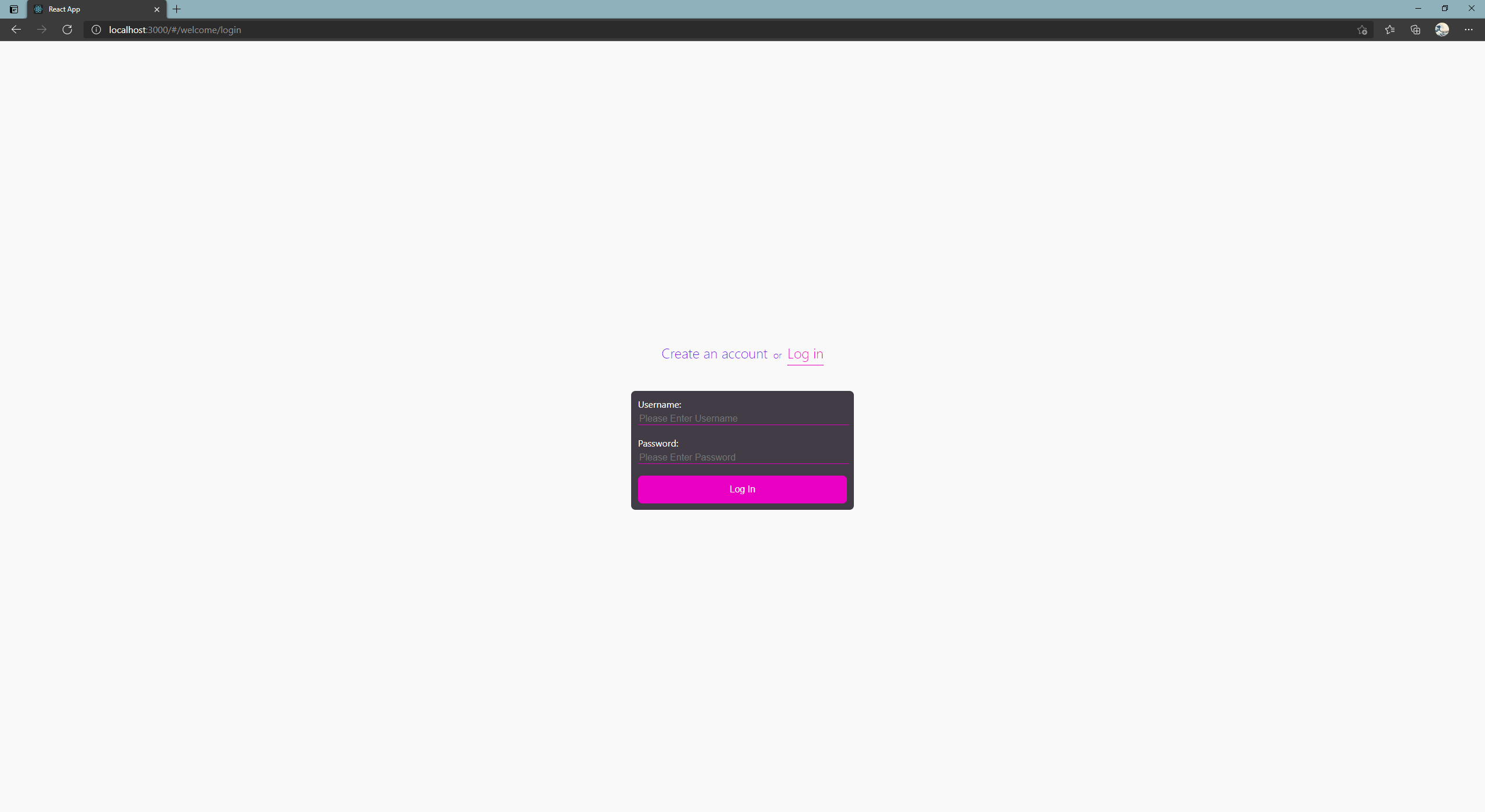
Certain encryption/authorisation/other security methods. Find academic sources?

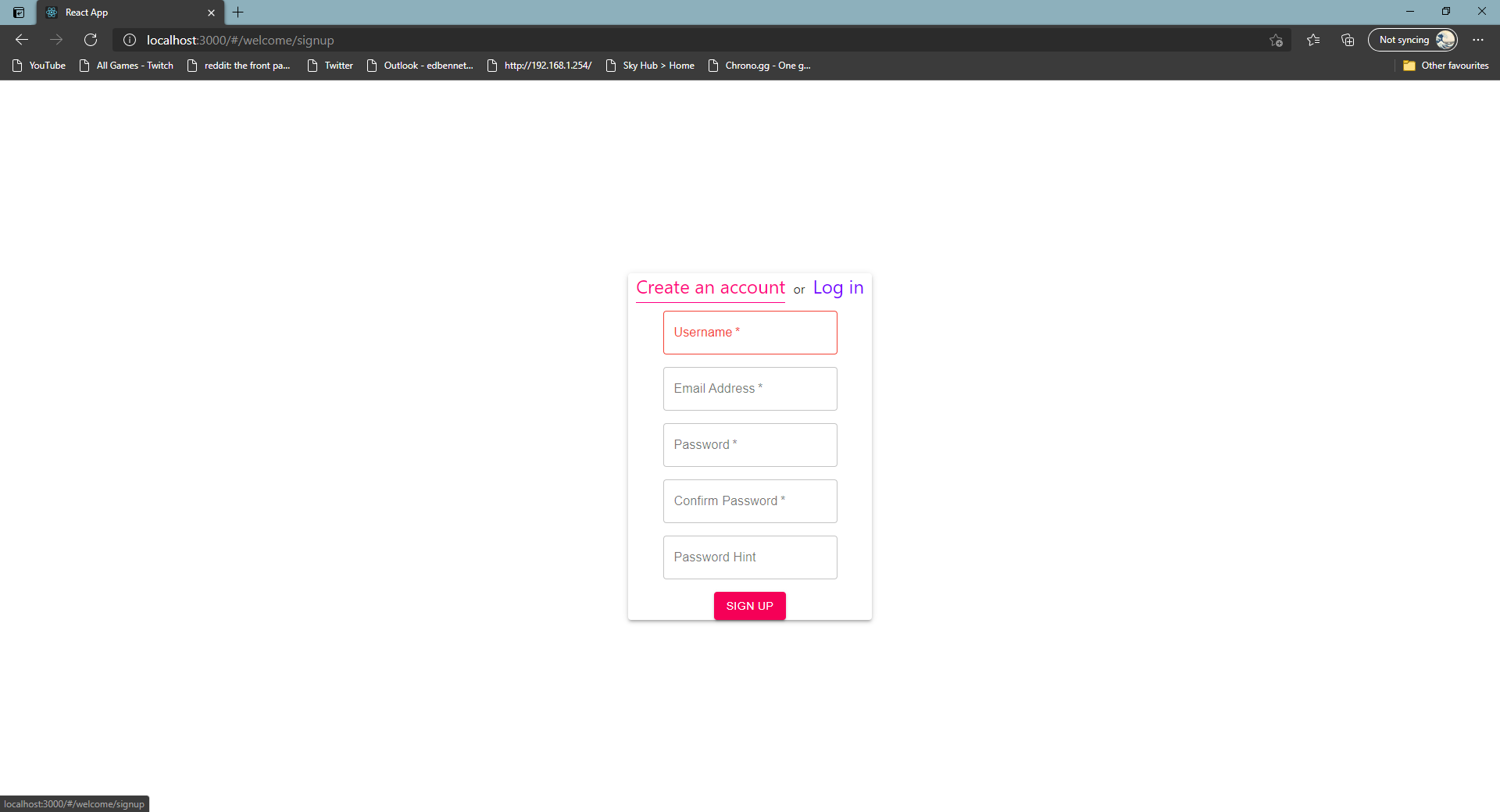
# Requirements Engineering

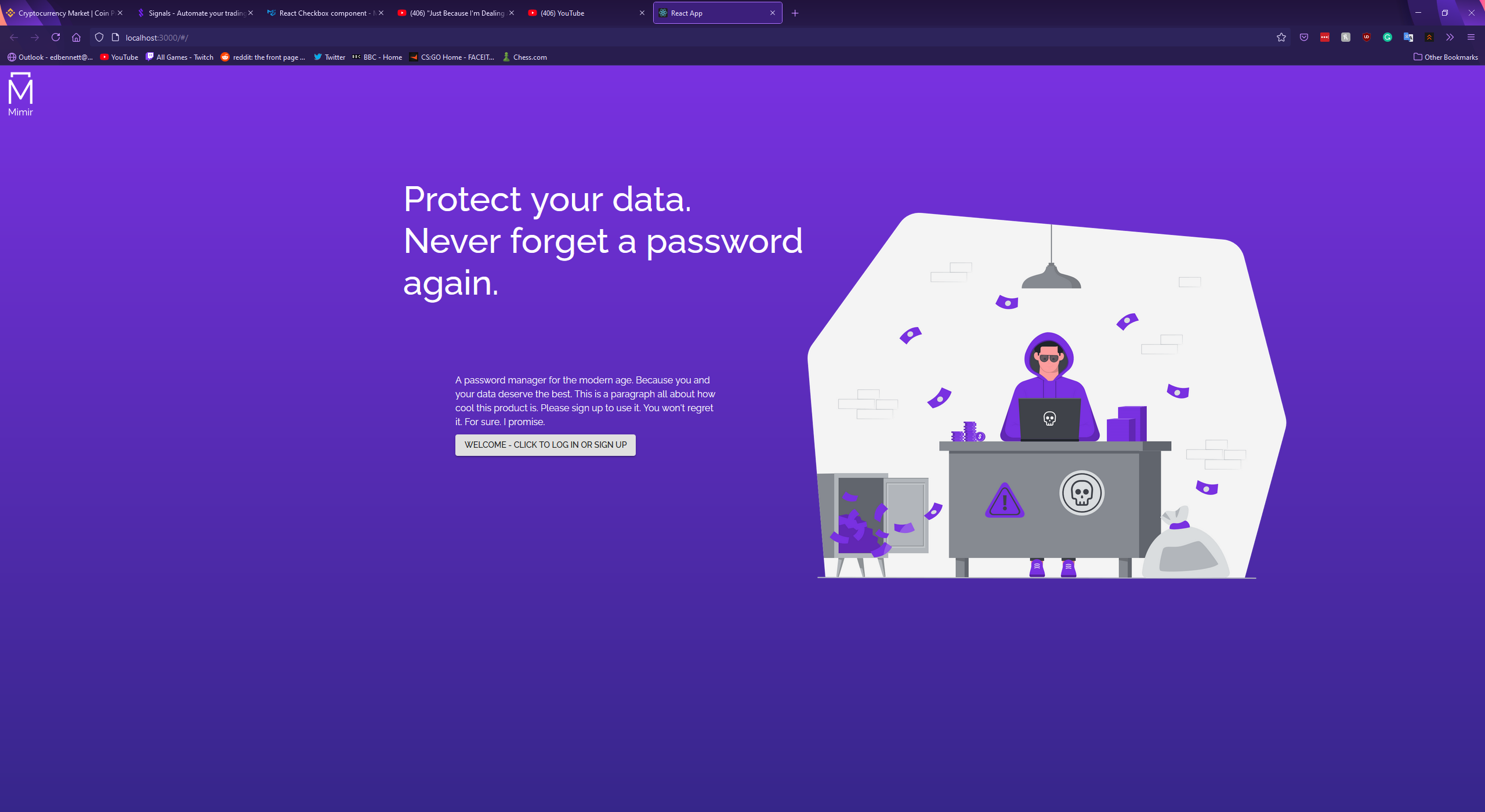
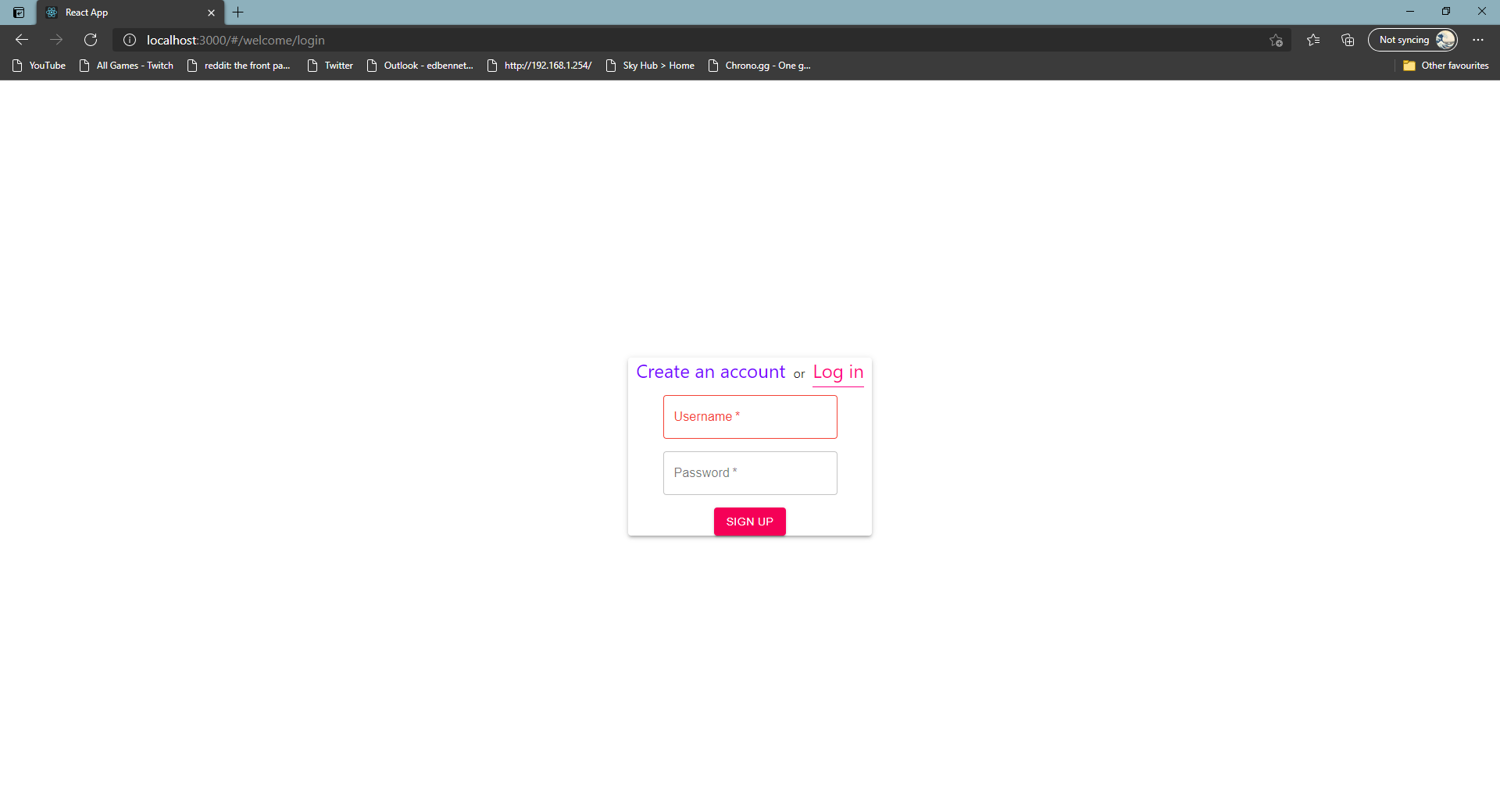
# Design Specification

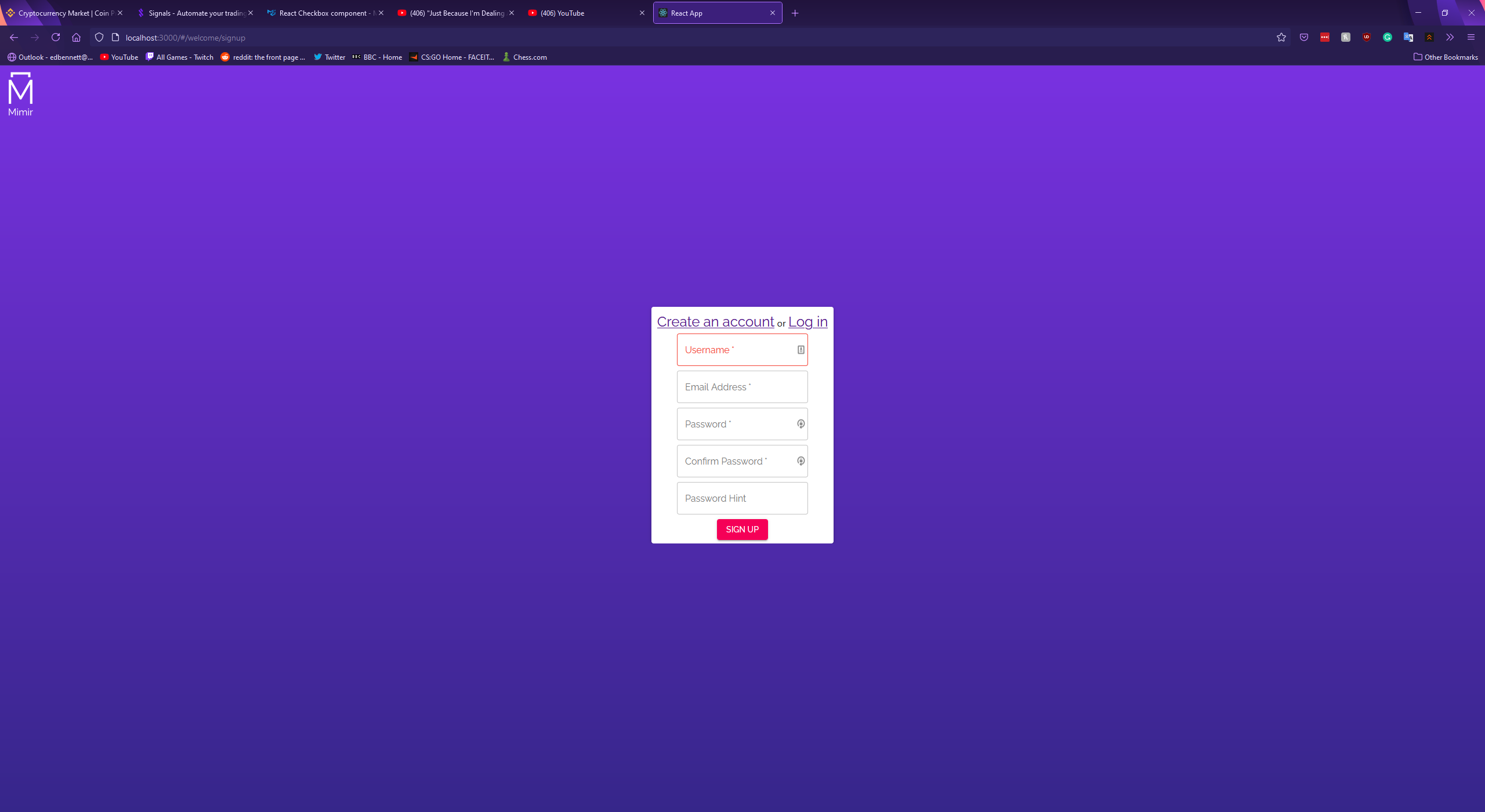
# Implementation

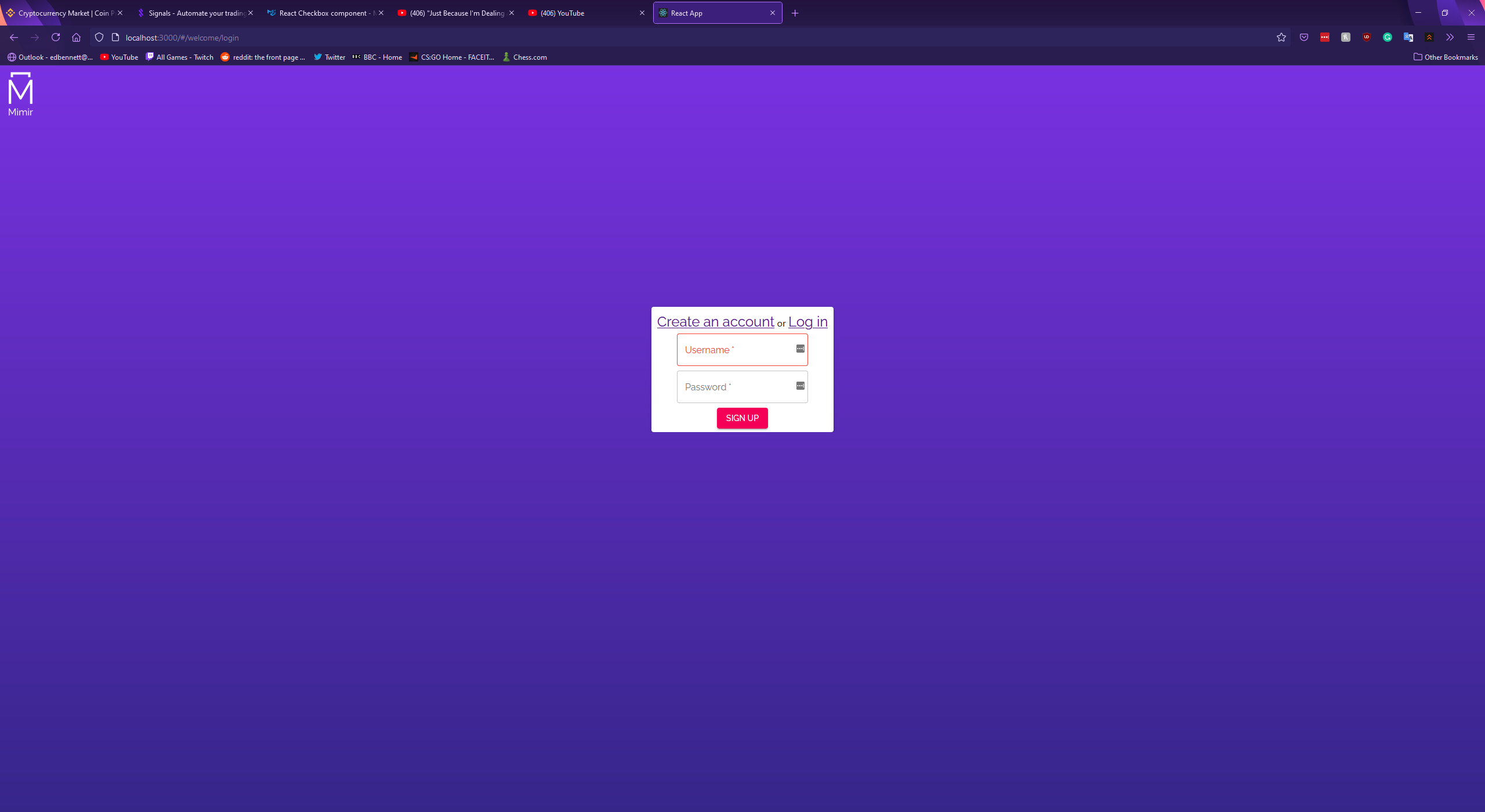


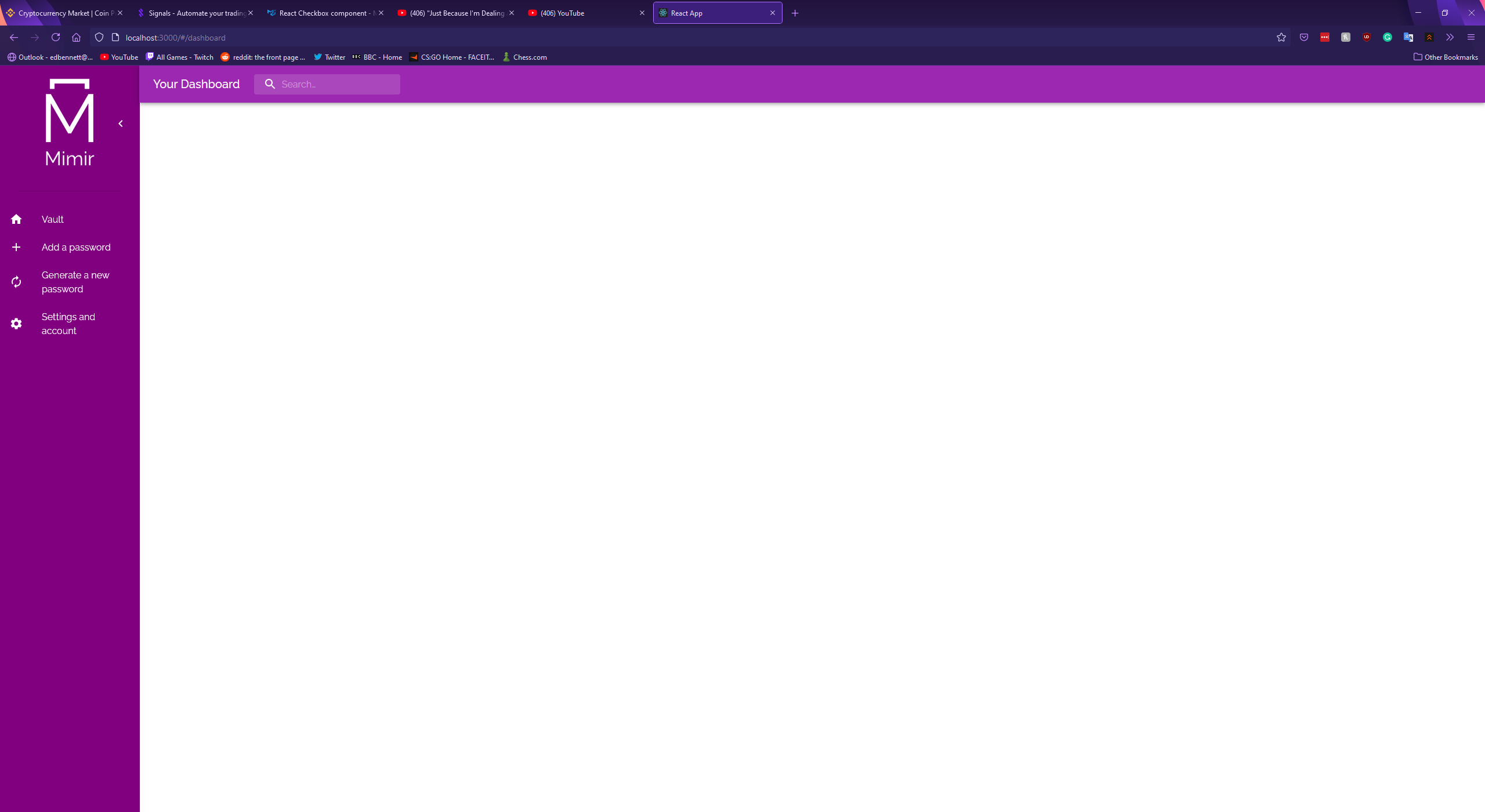


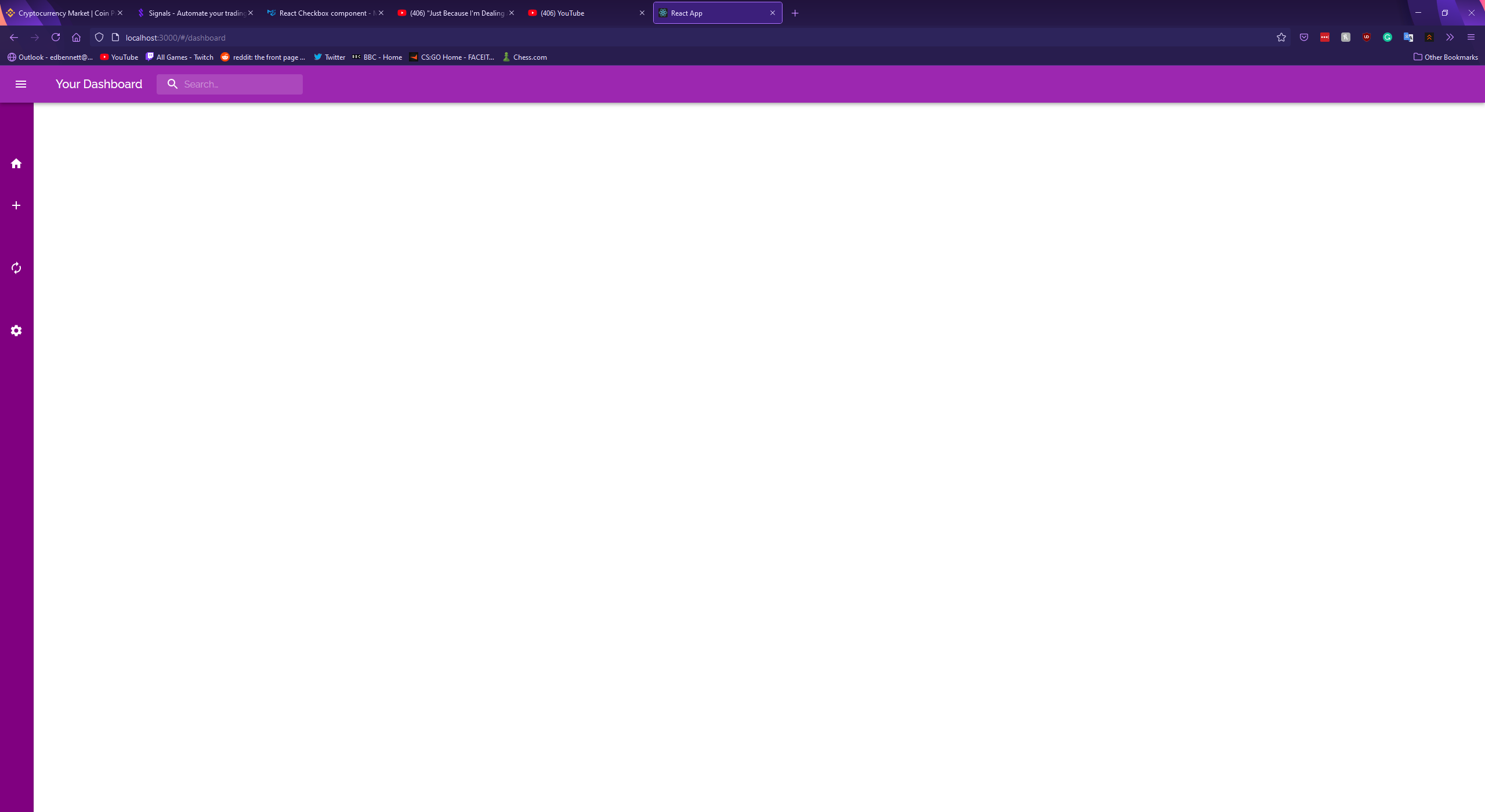


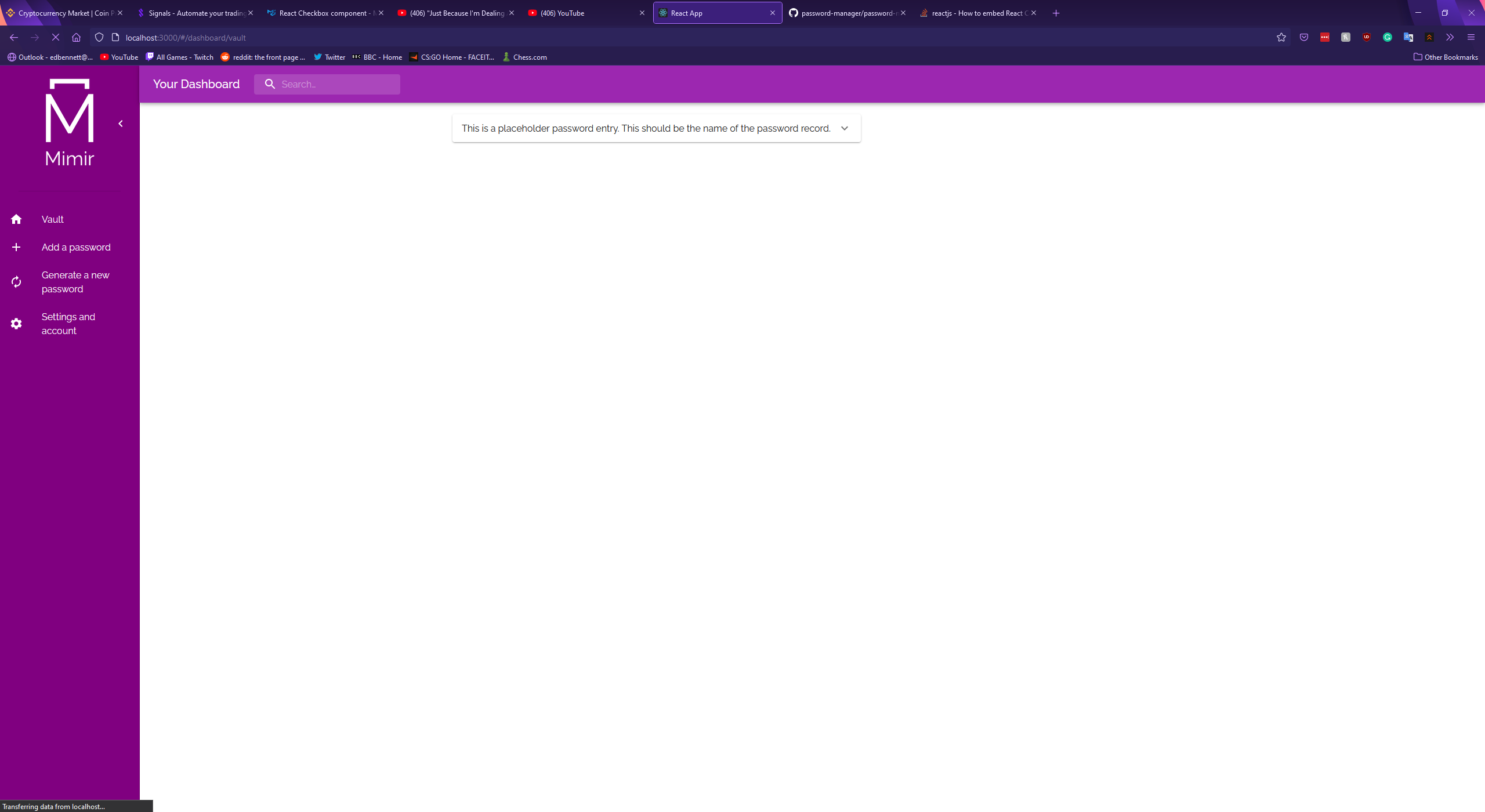


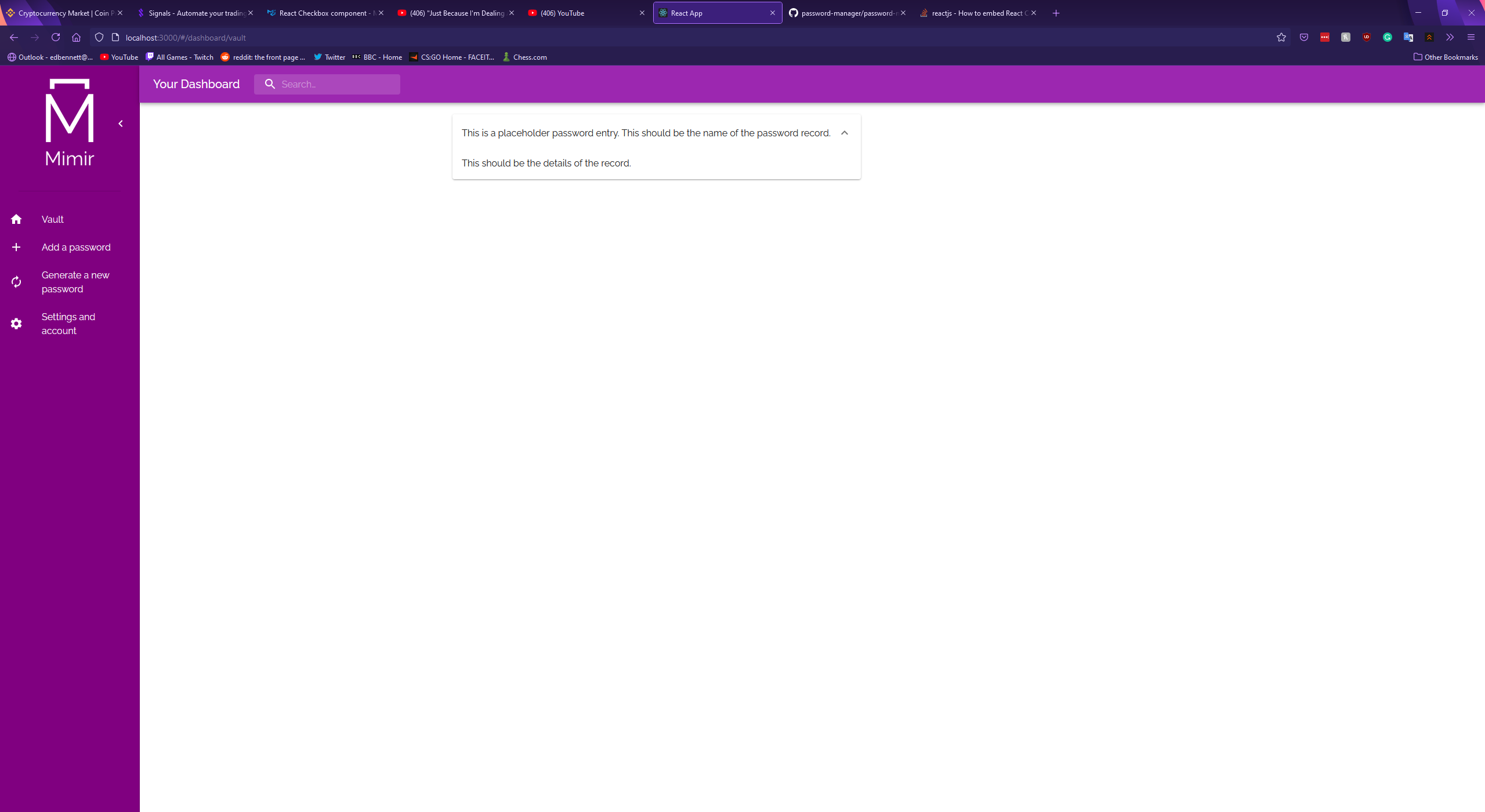


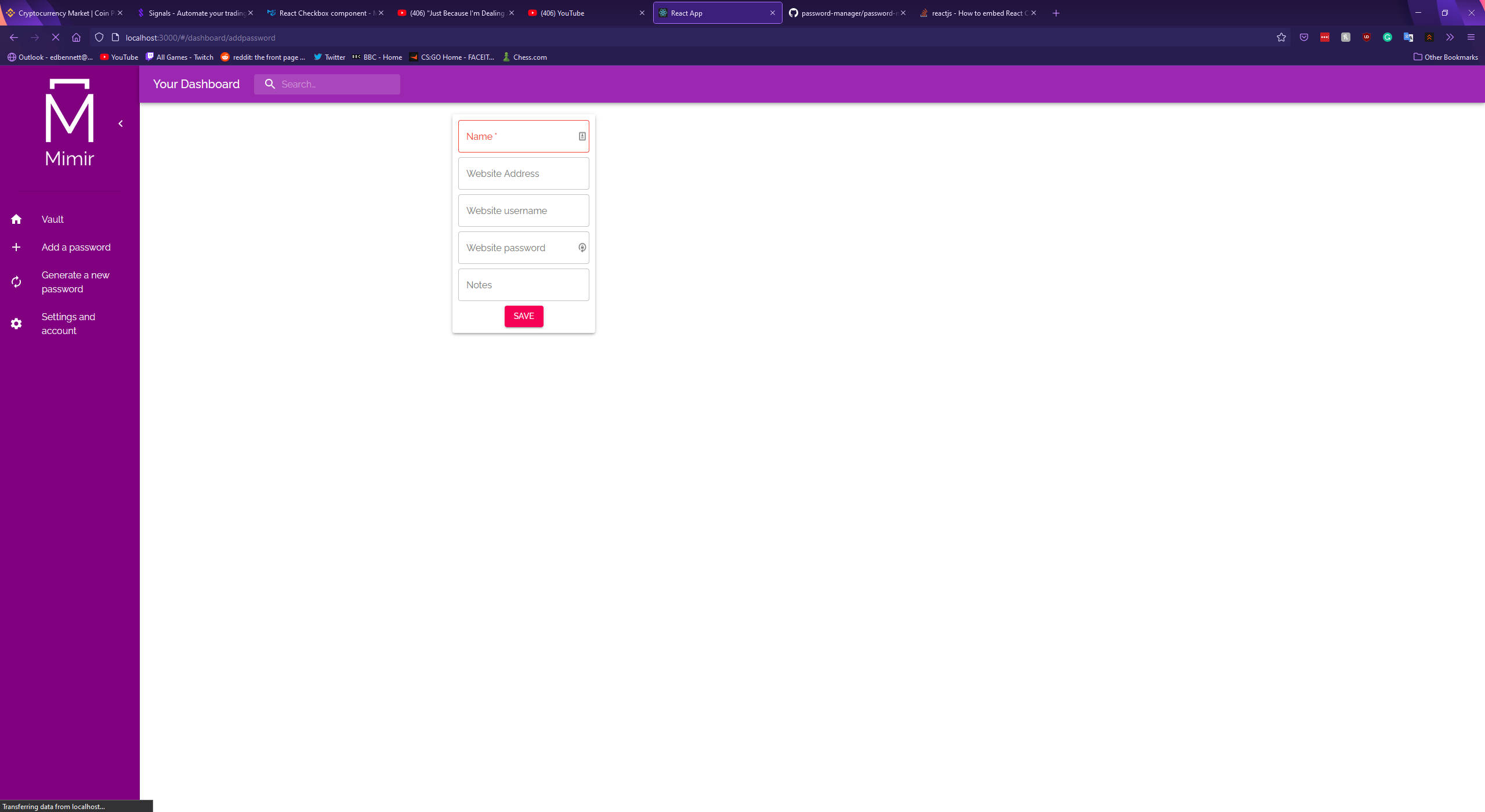


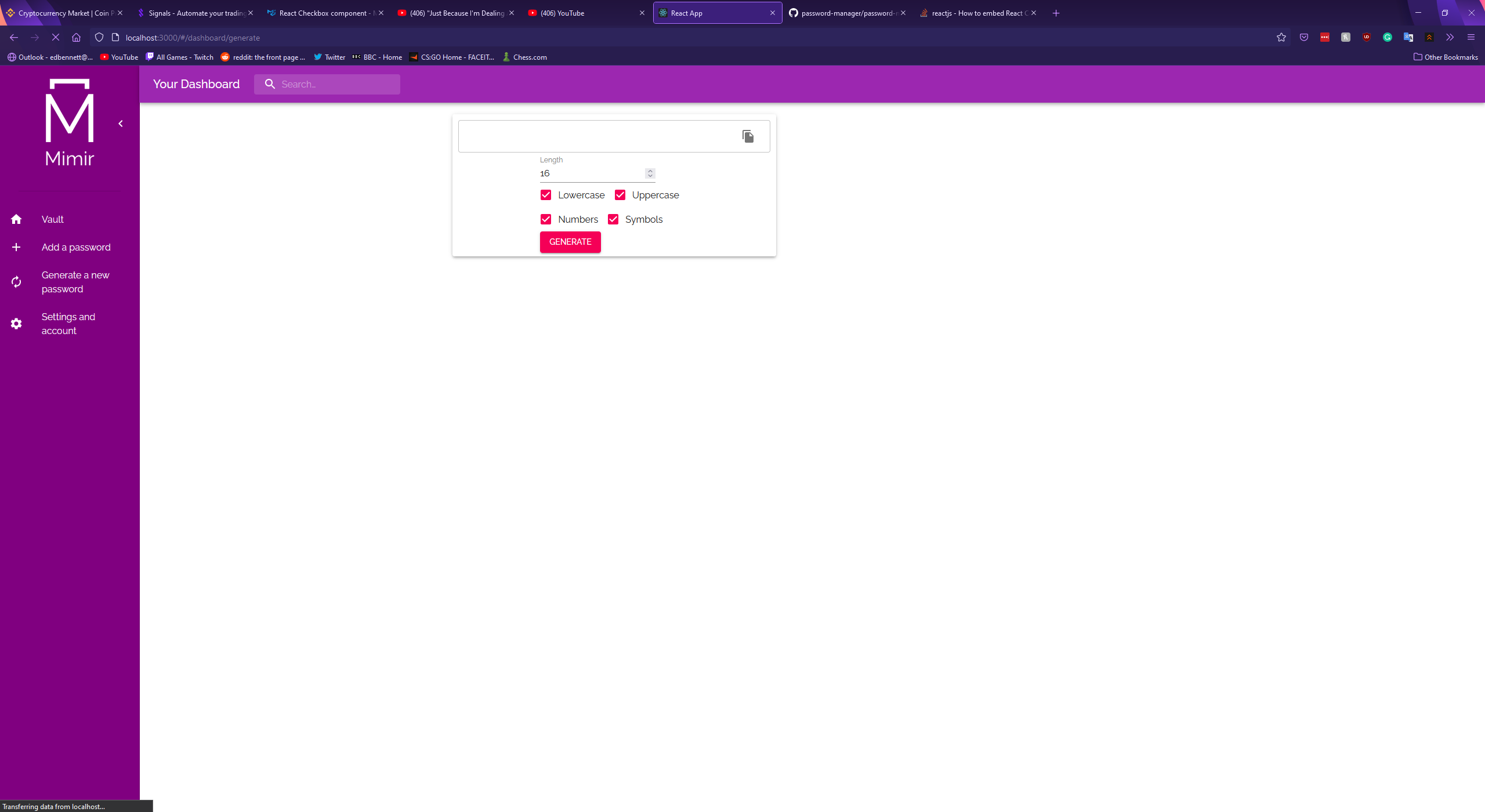


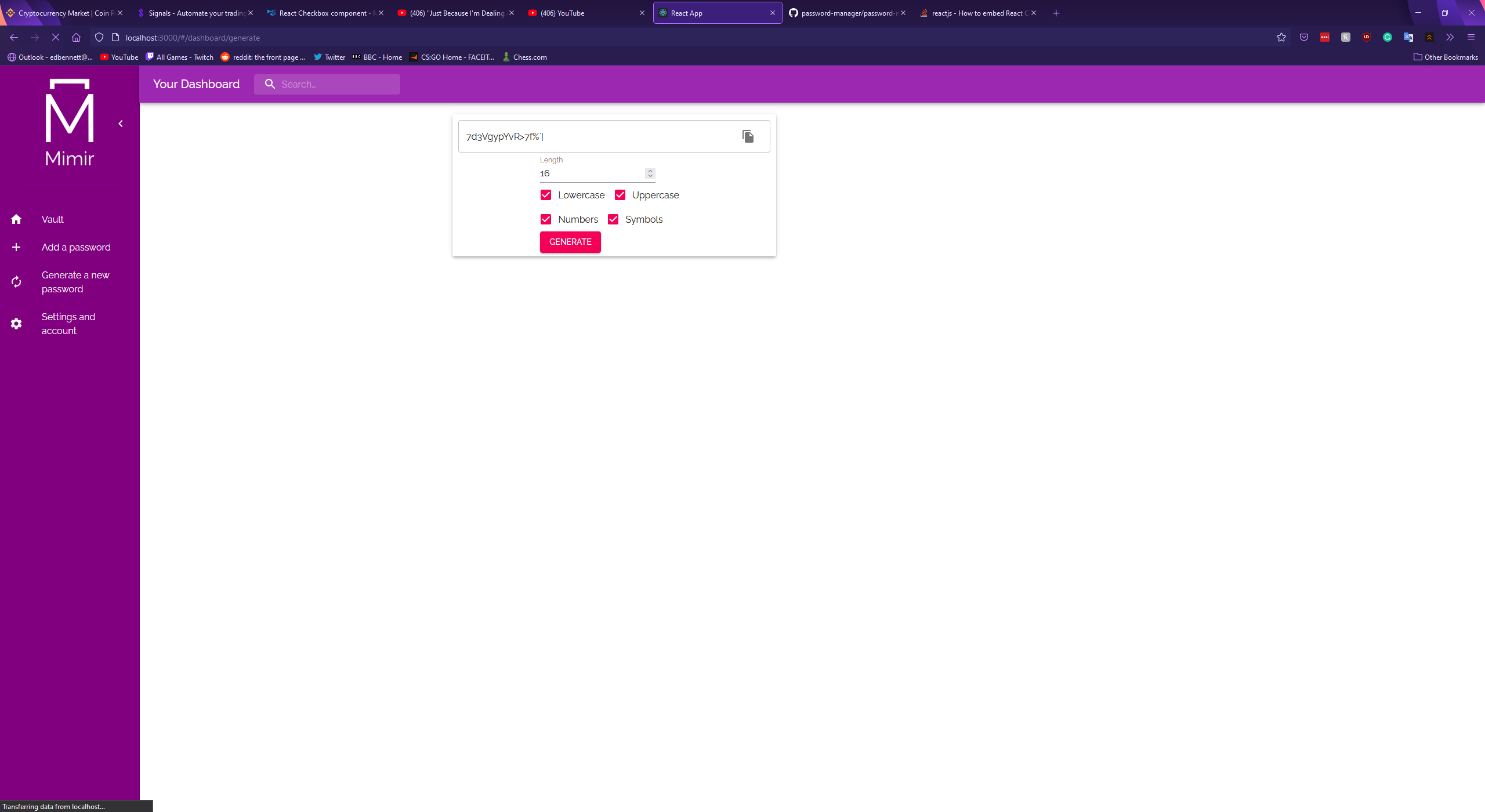


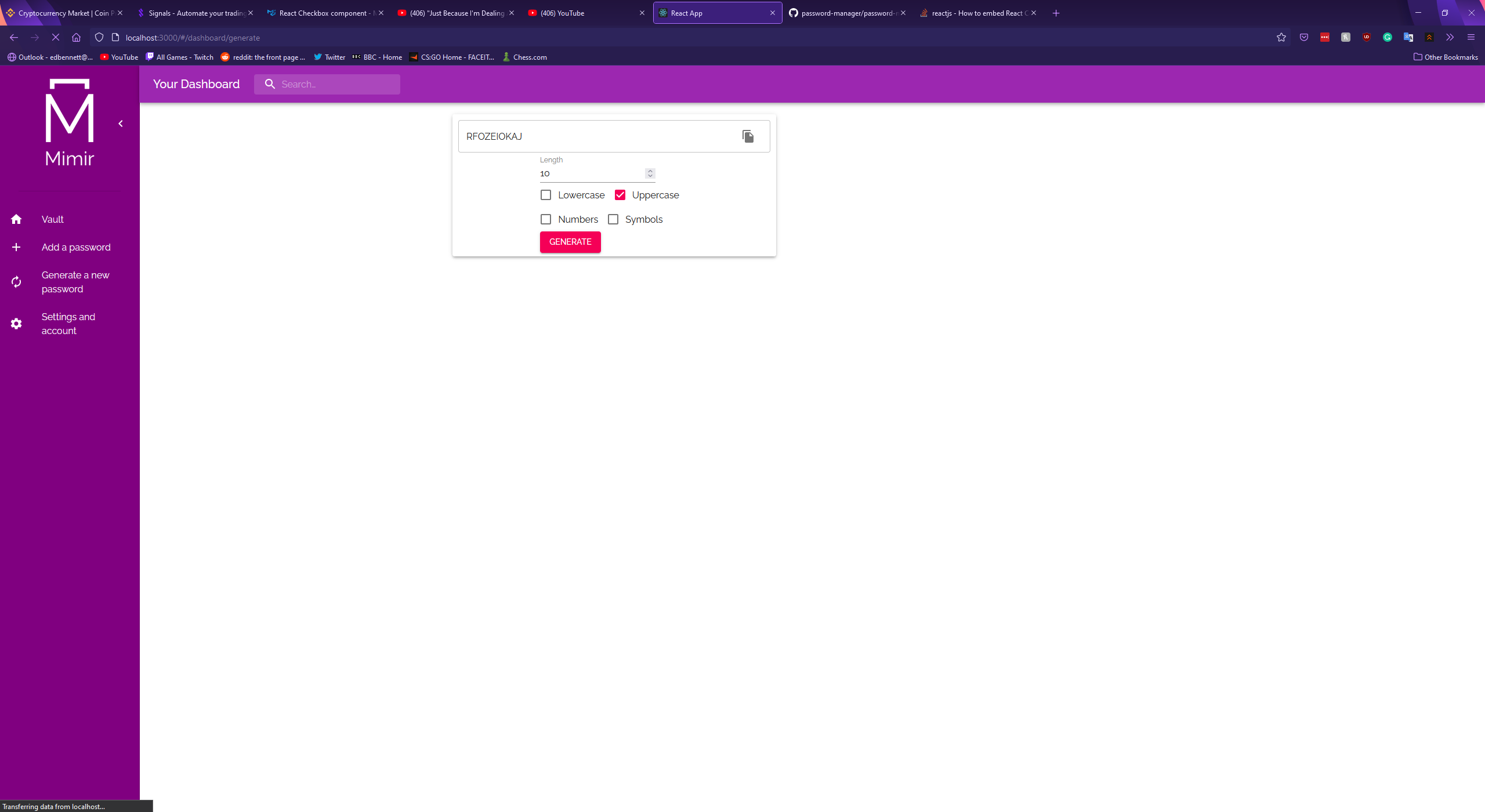


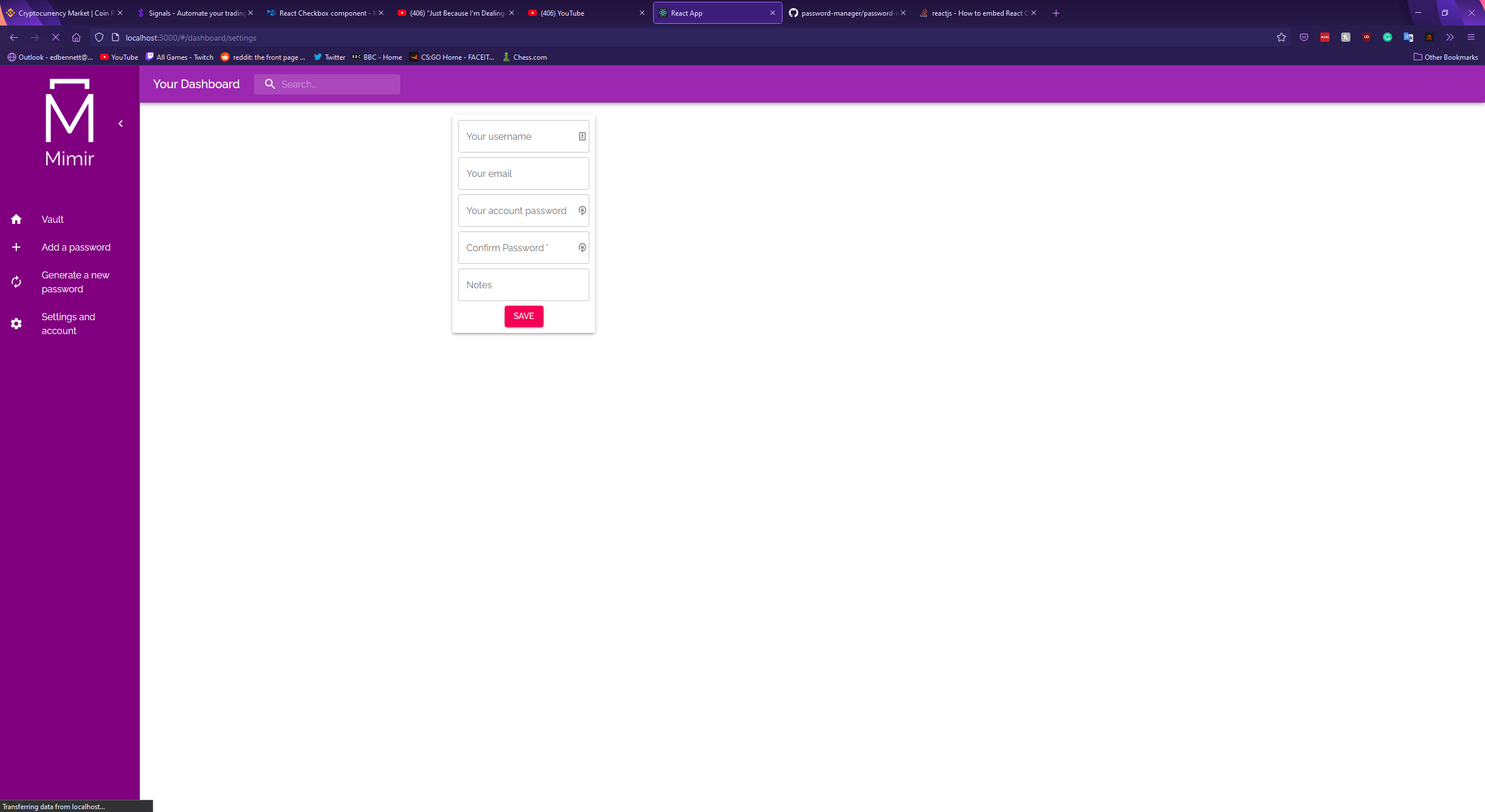












# Conformance Testing and Integration

# Evaluation Plan

# Conclusion

# Lessons Learned

# Acknowledgements

# Bibliography

*IEEE*, 2014. Improving usability of passphrase authentication. [online] Available at: <https://ieeexplore.ieee.org/abstract/document/6890939>.