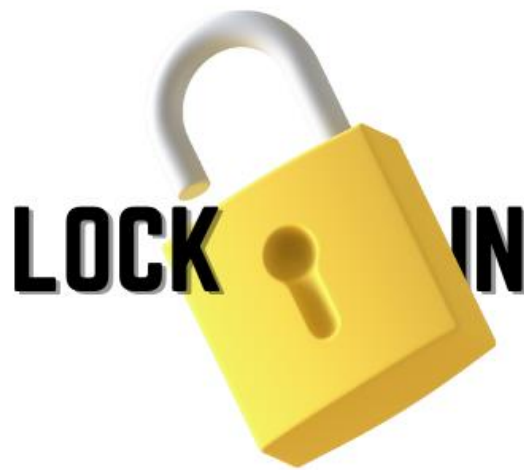


Georgia State University  
CSC 4350 - Software Engineering  
*Spring 2023*



Group 2  
Cindy Thai  
Patrick Davis  
Ulysses Adams  
Weiyi Zhen  
Paul Bronola

## SECTION 1: Planning and Scheduling Table

| Assignee      | Email                     | Task                                      | Duration (Hours) | Dependency                        | Due Date | Evaluation |
|---------------|---------------------------|---|------------------|-----------------------------------|----------|------------|
| Cindy Thai    | cindymdthai@gmail.com     | Use case diagrams, Database specification | 4+               | Use Cases written before diagrams | 03/03    | 100%       |
| Patrick Davis | patrickdavisart@gmail.com | Use cases, System requirements            | 4+               | None                              | 03/03    | 100%       |
| Ulysses Adams | ulyssiesadams@gmail.com   | Problem statement                         | 2+               | None                              | 03/03    | 100%       |
| Weiyi Zhen    | weiyi0111@gmail.com       | Class diagrams, Database specification    | 4+               | None                              | 03/03    | 100%       |
| Paul Bronola  | paulbronola@gmail.com     | Use cases                                 | 3+               | None                              | 03/03    | 100%       |

## SECTION 2: Problem Statement

The global cybersecurity market is one of the fastest growing subsets of computer science in recent years with a 12.4% annual growth rate and companies spending more and more every year to prevent cyberattacks. Standard alphanumeric passwords can be cracked easily with some of the methods hackers have today such as keylogger programs or phishing emails.

Graphical passwords are a method of authentication where users select images that serve as a replacement of the typical textual, alpha-numeric passwords. An example of this would be the pattern lock password on android mobile devices. Graphical Passwords offer a wider and broader space for passwords and are not limited to characters on a keyboard which also eliminates the problem of keyloggers.

Our team aims to create a graphical password interface web application that provides a more secure and user-friendly method of authentication for businesses, especially those in sensitive industries such as hospitals and financial institutes. The graphical password interface improves security by preventing keyboard-based password theft, phishing scams, and allowing for more complex password types.

### SECTION 3: Requirements

1. **New User Registration:** A new user wants to sign up on the website using a graphical password. They will be prompted to select an image and mark specific points on the image to create their password.
2. **Forgotten Password:** An existing user forgets their password and wants to reset it using their graphical password. They will need to provide the image they previously selected and correctly mark the points to reset their password.
3. **Login Attempts:** An existing user tries to log in to the website several times but fails due to incorrect password marks. They will be prompted to try again or reset their password if they have forgotten it.
4. **Login Success:** An existing user logs in successfully using their graphical password. They will be taken to their account dashboard where they can access their information and perform various actions.
5. **Update Password:** An existing user wants to update their graphical password for increased security. They will be prompted to select a new image and mark specific points to create a new password.
6. **Multiple Devices:** An existing user wants to log in to the website from multiple devices such as a laptop, smartphone, and tablet. They will be able to use the same graphical password on all devices.
7. **Incorrect Password:** An existing user tries to log in with an incorrect password by marking the wrong points on the image. They will be prompted to try again or reset their password if they have forgotten it.
8. **Incomplete Password:** An existing user tries to log in but fails to mark enough points on the image. They will be prompted to try again and mark the required number of points on the image.
9. **Security Measures:** The website implements security measures such as tracking login attempts and temporary lockouts to prevent unauthorized access.
10. **Account Management:** An existing user wants to manage their account information such as their name, email address, and password. They will be able to do so from the account dashboard.
11. **Mobile Version Login:** An existing user wants to log in to the website from their mobile device. They will be able to do so using their graphical password.
12. **Integration with Other Services:** The website integrates with other services such as social media, email, and cloud storage. An existing user will be able to access these services from their account dashboard using their graphical password.

## Use Case #1

Use Case Name: New User Sign Up

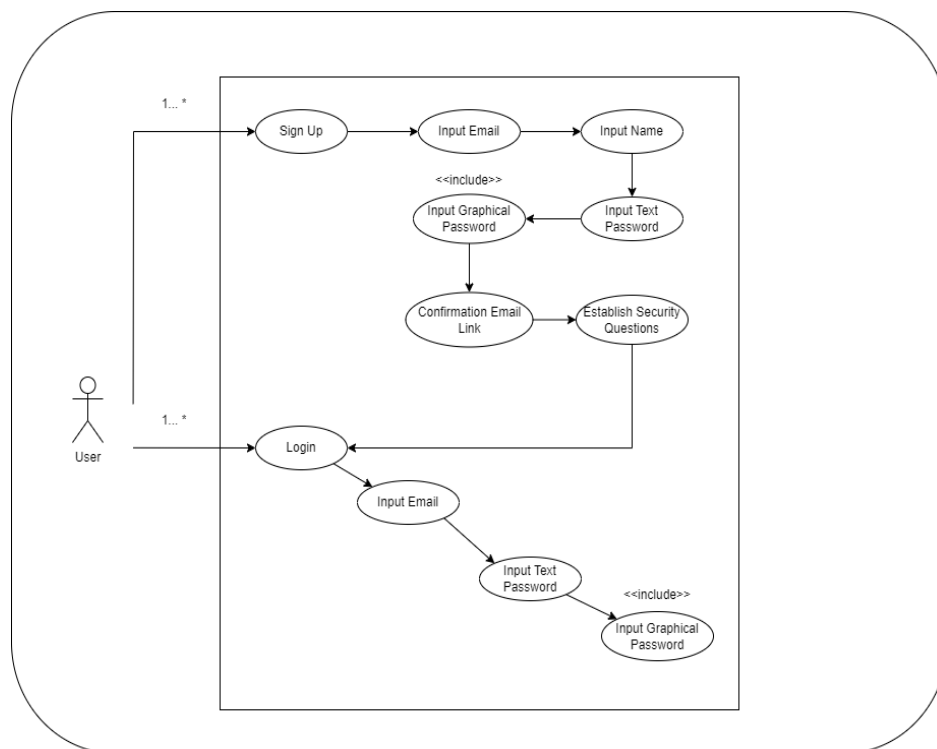
Actors: New User

Description: User is newly employed at a large firm. Once given their employer-based email they will use that credential to gain access to the site. Users will first encounter a home page with options to sign up or login for returning users. The new user will click sign up and be taken to the profile creation page. Here the user inputs the email given by the company and then enters fields for name and a text password and creates the graphical password as well as establish security questions in the event of needing to recover access. Once finalized a confirmation email is sent containing a link to log back in. Once the link is clicked and identity is confirmed the new user is routed to the home page and can click the login button. The user will enter the email and the text password as well as the graphical password and at this point, they will gain access to the work environment.

Exceptional Path: If the user navigates away from creating before saving the information is lost and they will have to start over. Should prompt here to warn of such an event.

Alternate Path: Users can click login and the login page will offer a button for creating a new account if they do not have an existing one.

Pre-condition: User must have an employer-based email.



## **Use Case #2**

Use Case Name: Password Recovery

Actors: Existing User

Description: User arrives at the home page and goes to login as an existing user. Upon being prompted to enter username and password they are rejected entry. Users will be allowed 3 attempts to gain access to their sensitive data. If the attempts are exhausted, they will be locked out and a recovery email will be sent to the company provided address. The email will contain a link to recover access. The user will click the link and be taken to the recovery page. Here they must enter their username and answer the security questions to regain access to their account. A password reset should be prompted at this point.

Exceptional Path: The user could possibly fail the security questions and may have the account locked until they contact their employer.

Alternate Path: User can after one failed attempt click a button for “Forgot Password” and the recovery process can begin then. Users are assumed to know their username as it will be provided by their employer.

Pre-condition: This user is an existing user and has already established their credentials with the site.

## **Use Case #3**

Use Case Name: Forgets Password

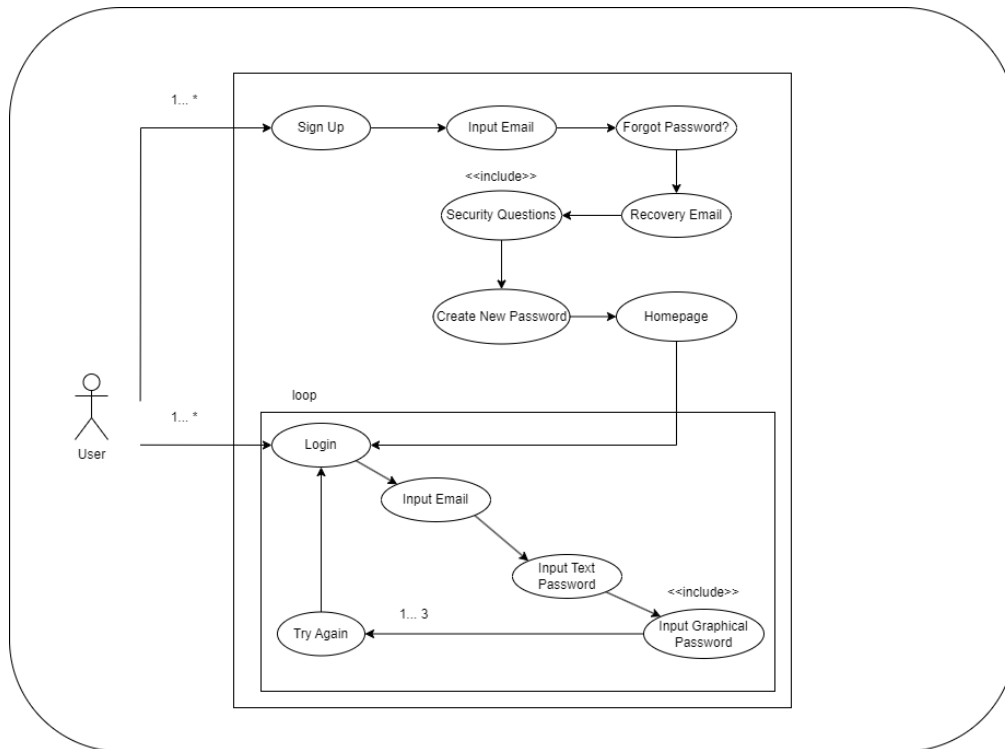
Actors: Existing User

Description: Existing user goes to sign in but has forgotten their password. They can click the link for “Forgot Password?” and the recovery process will start with an email being sent to the company provided email that will contain a link. The link will send the user to a page where they must answer security questions to verify identity. Once approved they will be prompted to create a new password. When the password is created, they are sent back to the home page to sign in correctly.

Exceptional Path: If the user doesn’t use the link in a timely manner, it will expire, and they will have to repeat the process. Alternatively, as before they could fail their questions and be locked out.

Alternate Path: The user can attempt their password 3 times before being rejected.

Pre-condition: User has already established a profile.



## Use Case #4

Use Case Name: User Login Success

Actors: User with established credentials

Description: User accesses home page and inputs employer provided email and text password. User is prompted to enter a graphical password and when accepted is granted access to the account.

Exceptional Path: The user could click sign up and then try their existing credentials to which they will receive an error message telling them that name is already used. Should offer here a button to sign in as an existing user.

Alternate Path: Users must use this path or go the recovery path if they cannot recall password.

Pre-condition: User has an account.

## Use Case #5

Use Case Name: Update Password

Actors: User

Description: The user has logged in to the system but wants to edit their password. Once they have successfully logged in, they will go to their profile page. On this page they are offered the option to update information. To change password the user will need to input previous password and then enter a new one as well as confirm it to make sure no misspellings or mistakes were made. If it clears the password is reset and a confirmation message is displayed, and email will be sent to the user.

Exceptional Path: The user could potentially forget the new password and would then have to go through the recovery process.

Alternate Path: Recovery method should make the user reset their password.

Pre-condition: User is established but needs to update password to gain access to their sensitive data.

## **Use Case #6**

Use Case Name: Multiple Devices

Actors: User

Description: The user once established will have the ability to access the site from many types of devices. The user will get the same experience from their phone, laptop, or tablet. They will log in as described before and use the same user ID and passwords on any device.

Exceptional Path: N/A

Alternate Path: N/A

Pre-condition: User is established and has access on an appropriate device.

## **Use Case #7**

Use Case Name: Incorrect Password

Actors: User

Description: The user attempts to log in to their account by entering their username and graphical password but fails every time. For security reasons, the website will prompt them to reset their password. To reset their password, the user must follow instructions on the website, which include verifying their identity through email and a second-factor authentication method such as a code being sent to their mobile phone. Once their identity is confirmed, they are then prompted to create a new graphical password.

Exceptional Path: N/A

Alternative Path: N/A

Pre-condition: The user has a registered phone with their registered graphical password account.

## **Use Case #8**

Use Case Name: Incomplete Password

Description: The user tries to log in to their account by entering their username and graphical password but fails to mark enough points on the image. The website prompts them to try again and mark the required number of points on the image. The user realizes that they made a mistake and carefully marks the correct number of points on the image. The website verifies the password and allows them to access their account. The prompt to try again encourages users to carefully review their input and ensures that only authorized users can access the account.

Exceptional Path: N/A

Alternative Path: N/A

Pre-condition: The user has a registered account.

## **Use Case #9**

Use Case Name: Security Measures

Description: The user receives an email notification from the website that someone has attempted to log in to their account unsuccessfully. The email includes information such as the date, time, and location of the attempted login. It also consists of a message saying that their account is temporarily locked out for a time period. Following the message are instructions for resetting their graphical password, and information about the lockout period. After the lockout period expires, the user can log in using their new graphical password. All while the website continues to track login attempts and implement temporary lockouts to prevent unauthorized access in the future.

Exceptional Path: N/A

Alternative Path: N/A

Pre-condition: The user's account is having suspicious activity.



## **Use Case #10**

Use Case Name: Account Management

Description: The user logs in to her account using her username and graphical password and navigates to the account dashboard. In the account dashboard, User sees a section labeled "Account Information." The user clicks on it and sees options to update their name, email address, and password. To update their name and email address, the user enters the new information in the appropriate fields and clicks "Save Changes." The changes are then reflected the next time they view their account.

Exceptional Path: N/A

Alternative Path: N/A

Pre-condition: The user has an account and can log in successfully.

## **Use Case #11**

Use Case Name: Mobile Login

Description: The user travels a lot and their preferred device to access all their accounts and social media is their mobile phone. To avoid the hassle of using both hands every time to input their passwords, the user instead quickly clicks a saved link they have. This link navigates them straight to the mobile version of the Locked-In website. The website then prompts them to input their unique graphical password which is a series of images that the user selects using the same thumb that they're holding the phone with. Upon getting the password right, the user then gains access to their account all while having an extra hand that the user can use to multitask simultaneously.

Exceptional Path: N/A

Alternative Path: Users are using their tablets and eBooks to have access to the website.

Pre-condition: Users have the website saved for quick access. Users have a registered graphical password.

## **Use Case #12**

Use Case Name: Integration with Other Services

Description: The user is a busy entrepreneur who uses multiple online services throughout

the day. In order to save time from memorizing multiple passwords, the user uses a graphical password solution that integrates all his favorite social media, email, and cloud storage services into one unique password. This password is a sequence of images meaningful to the user, saving him time and effort of remembering and resetting multiple passwords in case he forgets them. The user would first successfully log in to the home page using their graphical password, then select which media outlet they would like to access. Upon clicking the user's choice, they will be asked to log in to their account tied to the website they're trying to log in to. Upon successful login, the next time the user logs in with their graphical password and picks the same online service as before, they will now seamlessly gain access to their account and the same is applied throughout all their other online services.

Exceptional Path: N/A

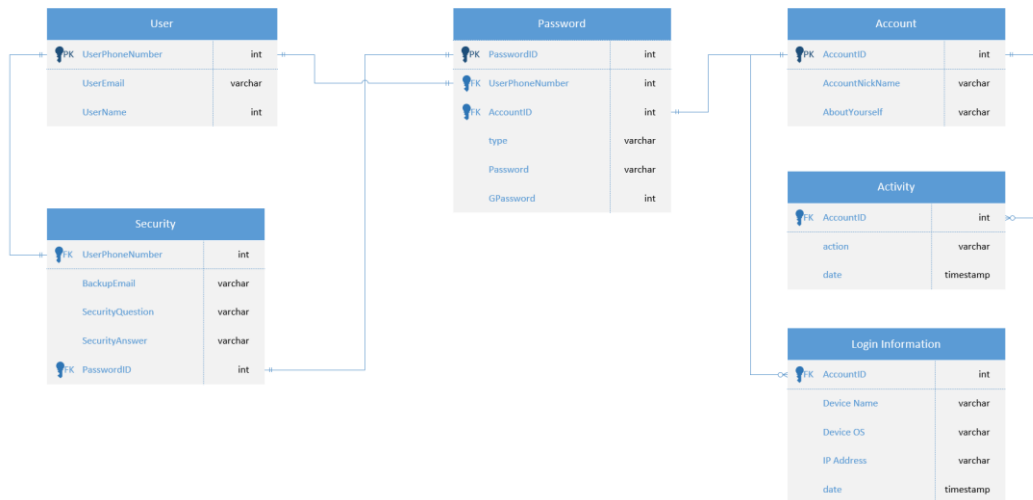
Alternative Path: N/A

Pre-condition: Users must have a graphical password registered and have an account tied to the online service they are trying to access.

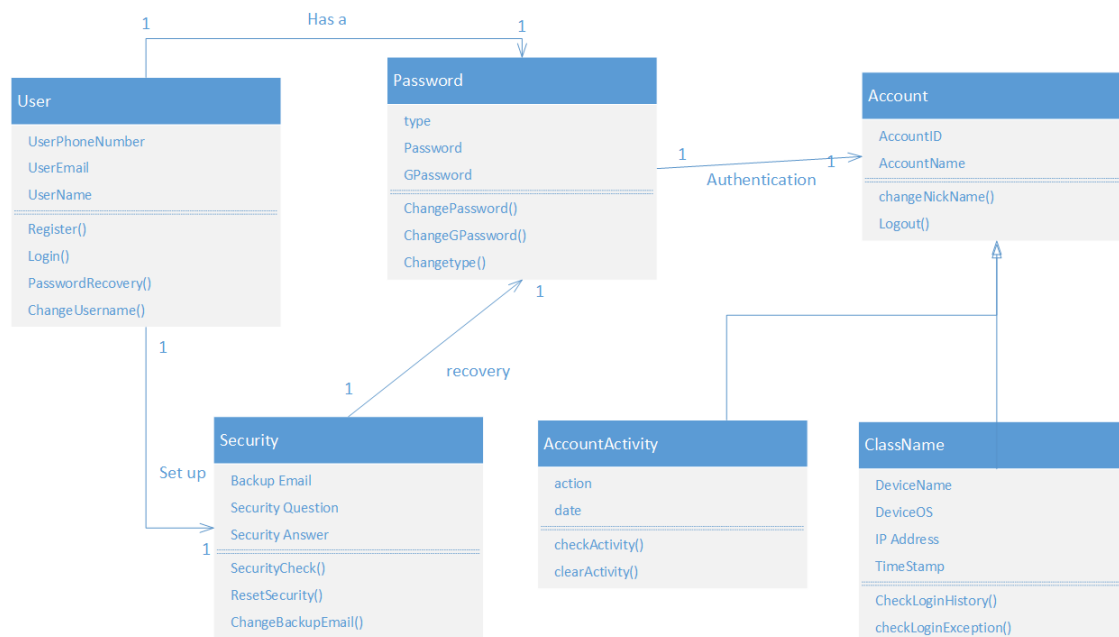
## SECTION 4: Database Specification

DBMS: MySQL

### Relational Model

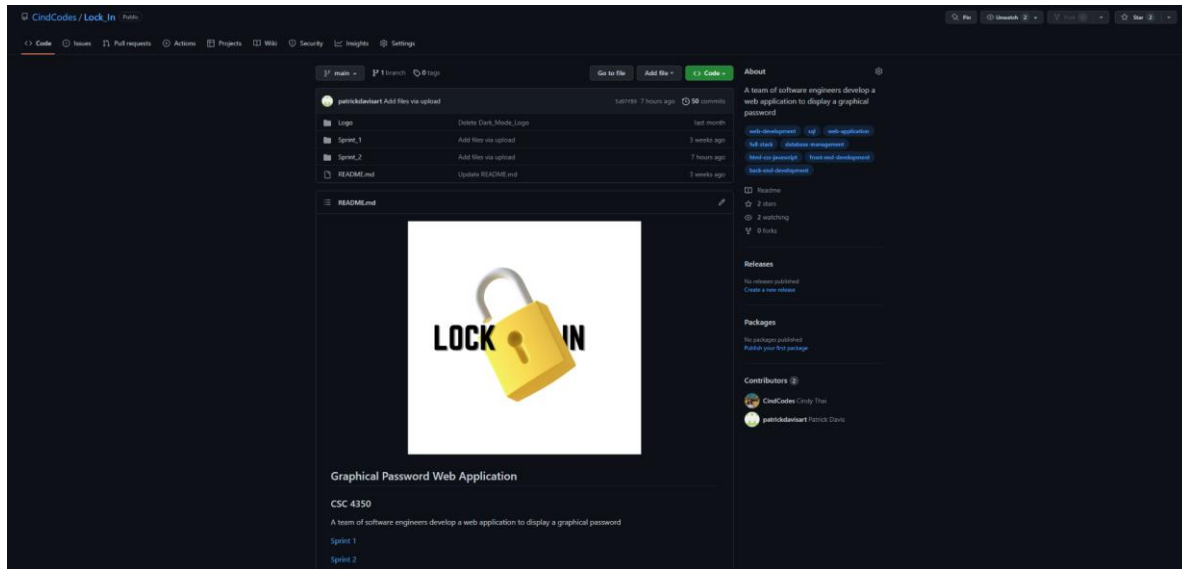


### Class Diagram

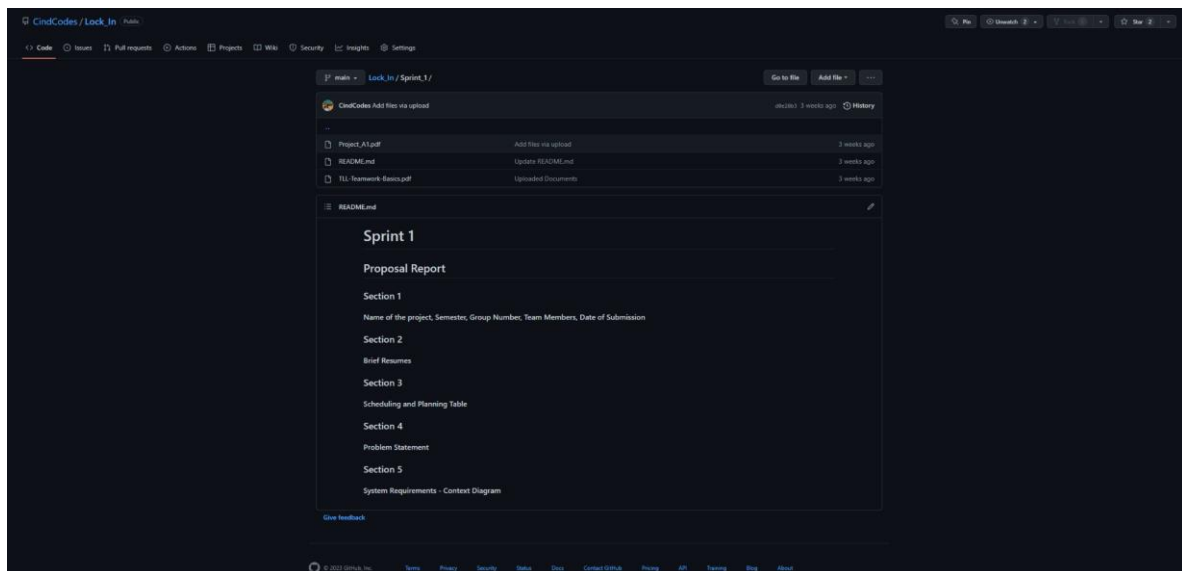


## SECTION 5: Appendix

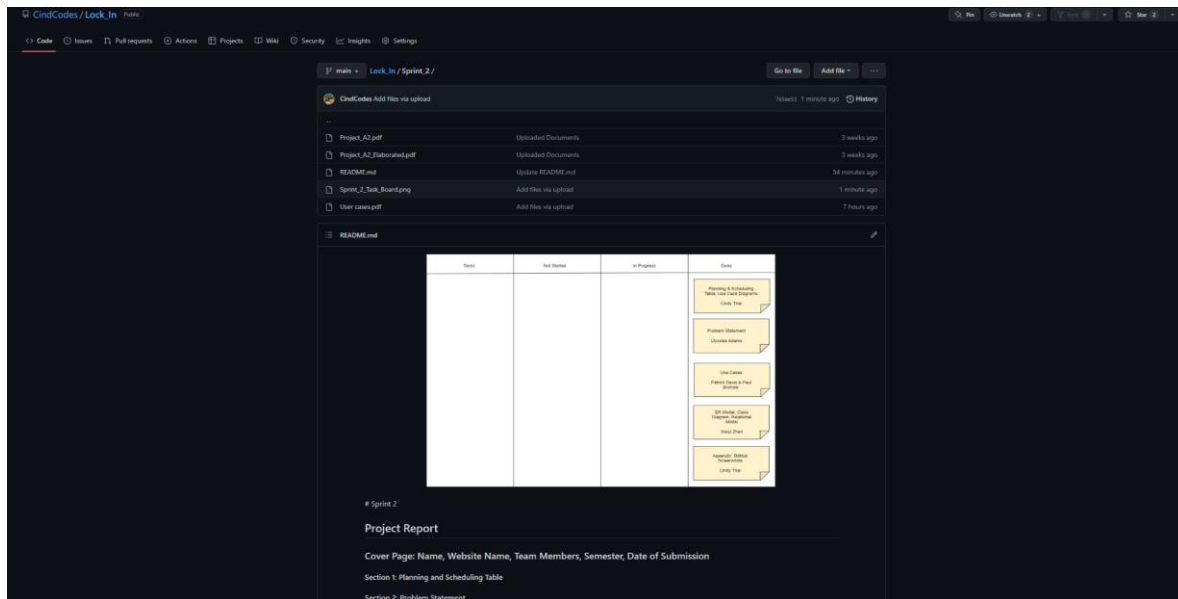
### Main Page



### Sprint 1



## Sprint 2



Mock up of the Home Page the user will land on first. Of course, this is just a start of prototyping the website made with HTML, CSS, and JavaScript:

