LITHAN

Know Your Neighbour Application

Module Project

Module: Application Integration (API using Spring Boot & React JS)

Start Date	**: May 29, 2023**
End Date	**: May 31, 2023**
Submission Date	**: June 5, 2023**

Learner Name	**: Francis Roel L. Abarca**
Enrollment ID	**: BDSE07-0922-113**
Presentation Date	**:**

Contents

LITHAN

Project Background

As the digital world continues to evolve at a rapid pace, businesses from different sectors are consistently exploring methods to improve their operations, augment the user experience, and increase their overall effectiveness. To accomplish these objectives, many organizations utilize a mixture of sturdy backend infrastructures, effective API implementation, and intuitive frontend applications.

Keeping these factors in perspective, the current project is intended to offer a platform for you to exhibit your skills in the design and development of a complete software package that includes all the above-mentioned elements. By harnessing the capabilities of Spring Boot, JPA Framework, Restful Web Services, and React JS, the project is set to let you showcase your expertise in creating a full-stack application that smoothly merges backend, API, and frontend components.

LITHAN

Project Objective

The objectives of this project include the following:

- The Users should be able to perform the following functions:
- User should be able to log-in using the provided APIs
- Users are required to provide the existing username and password for the API and can login to the application.

Project Deliverables

LITHAN

You have already developed a "Know-Your-Neighborhood" application. The goal of this application is to provide login/sign up using existing API. For this to happen, the application should have login button with available APIs.

The Know-Your-Neighborhood website consists of the following Key pages:

1. Home Page
2. Registration Page
3. Login Page with API link
4. Contact us Page
5. About us Page
6. Terms and Conditions Page

Customers can login using the existing API and fetch basic information such as name, email from API.

1. List of Tools used

LITHAN

- ❑ IntelliJ IDEA Ultimate

- ❑ Spring Tool Suite

- ❑ MySQL Server

- ❑ Visual Studio Code

- ❑ Node.js

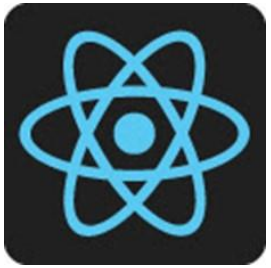
- ❑ Mozilla Firefox

1. List of Tools used

LITHAN

- ❑ Google Chrome

- ❑ React Developer Tools



- ❑ Microsoft Word

- ❑ Microsoft PowerPoint

- ❑ Postman

2. What is API?

LITHAN

An API, or Application Programming Interface, serves as a critical bridge between different software applications, enabling them to interact with each other. Its main components and functionalities include:

- Set of Rules and Protocols: An API outlines a set of protocols, rules, and tools for building software applications. This includes how software components should interact, the conventions to use, the formats to follow, and the syntax required.
- Simplifying Complexity: APIs help simplify complex systems by exposing specific functionalities, hiding the intricate details of their implementation. This allows developers to focus on utilizing the functionality without having to understand how it works internally.
- Scalability and Adaptability: APIs support the scalability of applications, as they allow developers to add new features or integrate additional systems as needed. They also promote adaptability by facilitating updates or changes to a specific component without affecting the rest of the system.
- Security: APIs play a crucial role in ensuring the security of data transmission between systems. They provide mechanisms for authentication and authorization, ensuring only authorized users or applications have access to specific data or functionalities.

3. What is the role of API?

LITHAN

In depth, The primary role of the API is to facilitate interaction between different software systems, acting as a bridge between data and functionality.

The Need for APIs:

- Integration of Platforms: Applications can easily integrate certain functionalities that exist from different systems.
- Payment Processing: Instead of building your own payment gateway, you can use an API from a service like Stripe or Paypal which will allow your website to connect with their services to securely process payments, handle refunds, and manage subscriptions.
- Real-time Data Updates: Suppose you're building a news aggregation application that pulls the latest news from various sources. Each news organization may not have the same data structure for their articles. APIs allow you to streamline this process, pulling in data from various sources in a uniform way.
- Social Media Integration: Let's say you're developing a new mobile app and you want users to be able to register and log in using their existing social media accounts, like Facebook or Google. Instead of having to develop your own authentication system from scratch, you can leverage the APIs provided by these platforms to accomplish this.

4. The range of APIs for a particular platform

LITHAN

Mobile APIs

- Google Maps API: Allows the integration of Google Maps functionality to your mobile apps.
- Facebook API: Allows integration with Facebook for social features like User Authentication.

Desktop APIs

- Windows API (WinAPI): Provides core functionality for Windows applications.
- .NET API: Used for creating desktop applications on the Windows platform.

Web APIs

- Twitter API: Allows the retrieval and posting of tweets, user information, and more.
- Stripe API: Provides functionality to handle online payments.

4. The range of APIs for a particular platform

LITHAN

- Facebook API: an HTTP-based API that allows developers to extract data and functionality from the Facebook platform. Applications can use this API to programmatically query data, post in pages and groups, and manage ads, among other tasks
- Google API: application programming interfaces (APIs) developed by Google which allow communication with Google Services and their integration to other services.

5. Potential Security Issues with APIs

LITHAN

Sensitive Data Exposure

- This happens when an API unintentionally exposes sensitive data, like user details, credit card numbers, etc.

Broken Access Control

- This occurs when users are allowed to perform actions beyond their permissions, giving them access to resources they should not have.

Parameter Tampering

- This happens when the parameters of an API request are modified, potentially leading to unauthorized access or behavior.

Injection Attacks

- This happens when an attacker sends malicious data as input, which is then processed by the API without proper sanitization or validation, leading to unintended consequences.

5. Potential Security Issues with APIs

LITHAN

DDoS Attacks

- Distributed Denial of Service (DDoS) attacks involve flooding the API with numerous requests, causing it to become overwhelmed and thus, preventing legitimate requests from being processed.

Broken Authentication

- This issue occurs when there are vulnerabilities in the API's authentication mechanisms, allowing unauthorized individuals to gain access.

Man-In-The-Middle-Attack (MITM)

- This attack involves an attacker secretly intercepting and potentially altering the communication between two parties who believe they are directly communicating with each other.

6. The Project Requirements

LITHAN

Back-end Development

- Architect and build a backend application leveraging Spring Boot and JPA framework.
- Establish necessary components like models, repositories, services, and controllers for effective data management and business logic.
- Connect and adjust the database for efficient data storage and access.

API Development

- Develop RESTful web services to provide APIs for facilitating communication between the frontend and backend.
- Develop endpoints for several tasks such as data retrieval, record creation, record updating, and record deletion.
- Guarantee thorough validation and error management for API requests and responses.

6. The Project Requirements

LITHAN

Front-End Development:

- Construct a frontend application utilizing React JS.
- Plan and set up user interfaces for seamless interaction with the backend APIs.
- Create components, handle state management, and define routing according to the application's needs.
- Integrate with backend APIs to acquire and show data, along with transmitting data back to the server.

Existing API Identification:

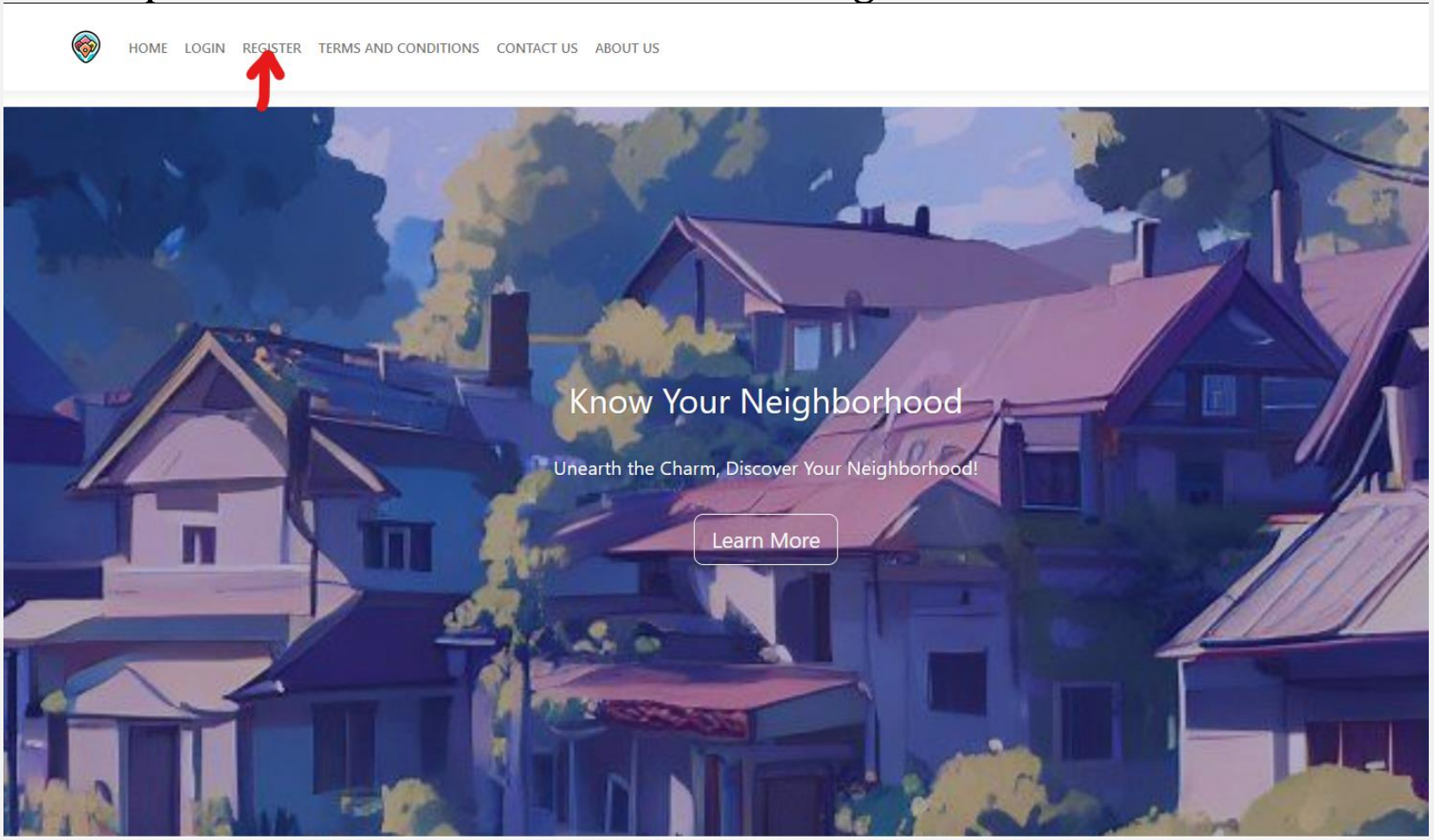
- Recognize any existing APIs that are currently developed and in use within the application.
- Comprehend the purpose and functionalities of these APIs.
- Assess how these APIs are incorporated into the application and their contribution to its overall functionality.

7. The Project Demo

LITHAN

Registration

- User opens the KYN website then clicks Register.

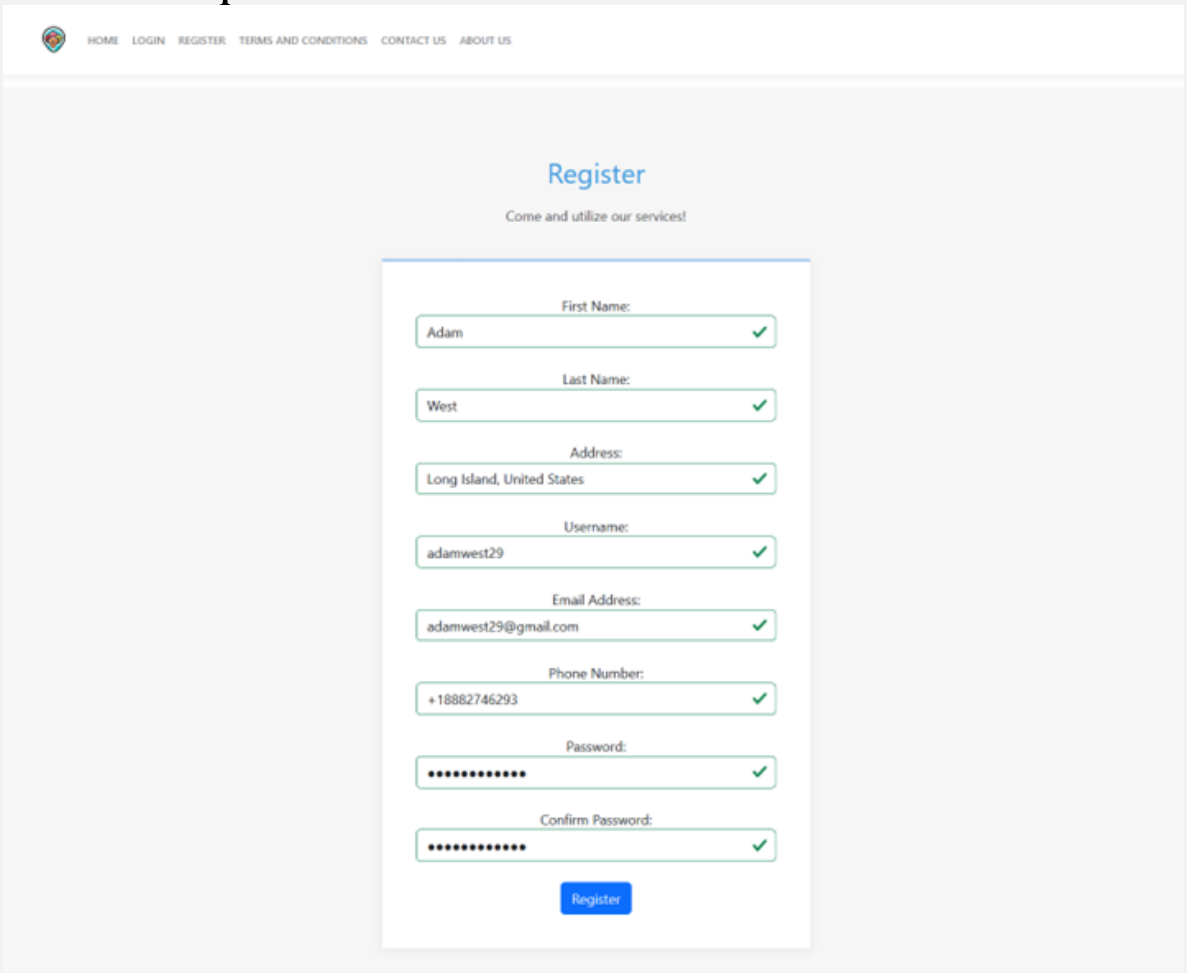


7. The Project Demo

LITHAN

Registration

- They fill out the required form.

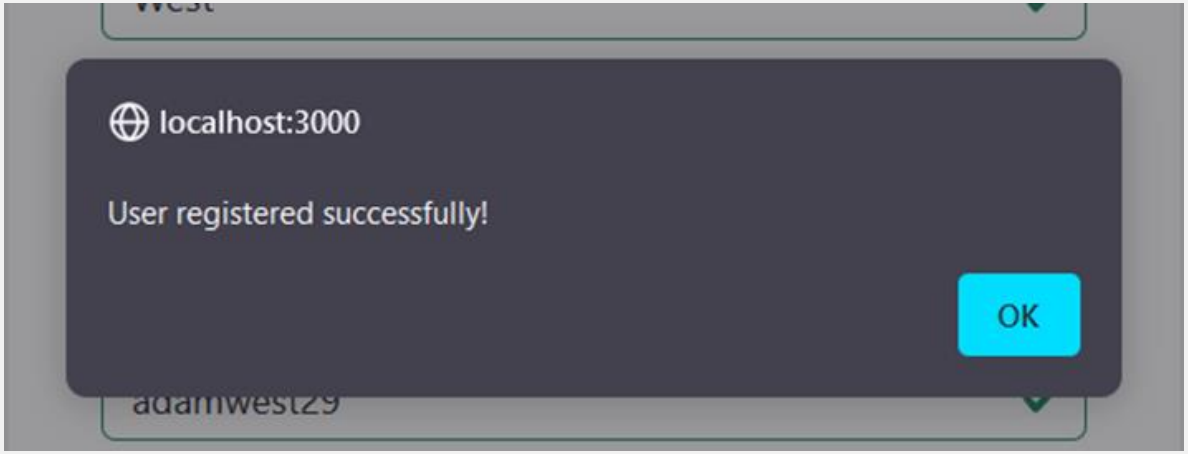


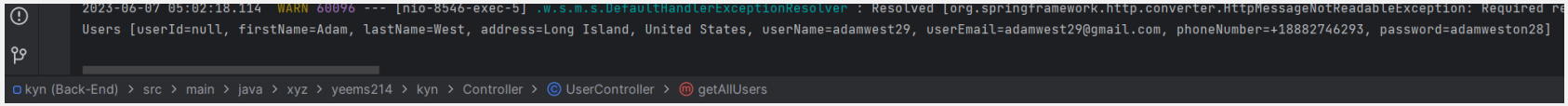
7. The Project Demo

LITHAN

Registration

- They hit submit and a dialog box appears indicating the user has registered successfully.



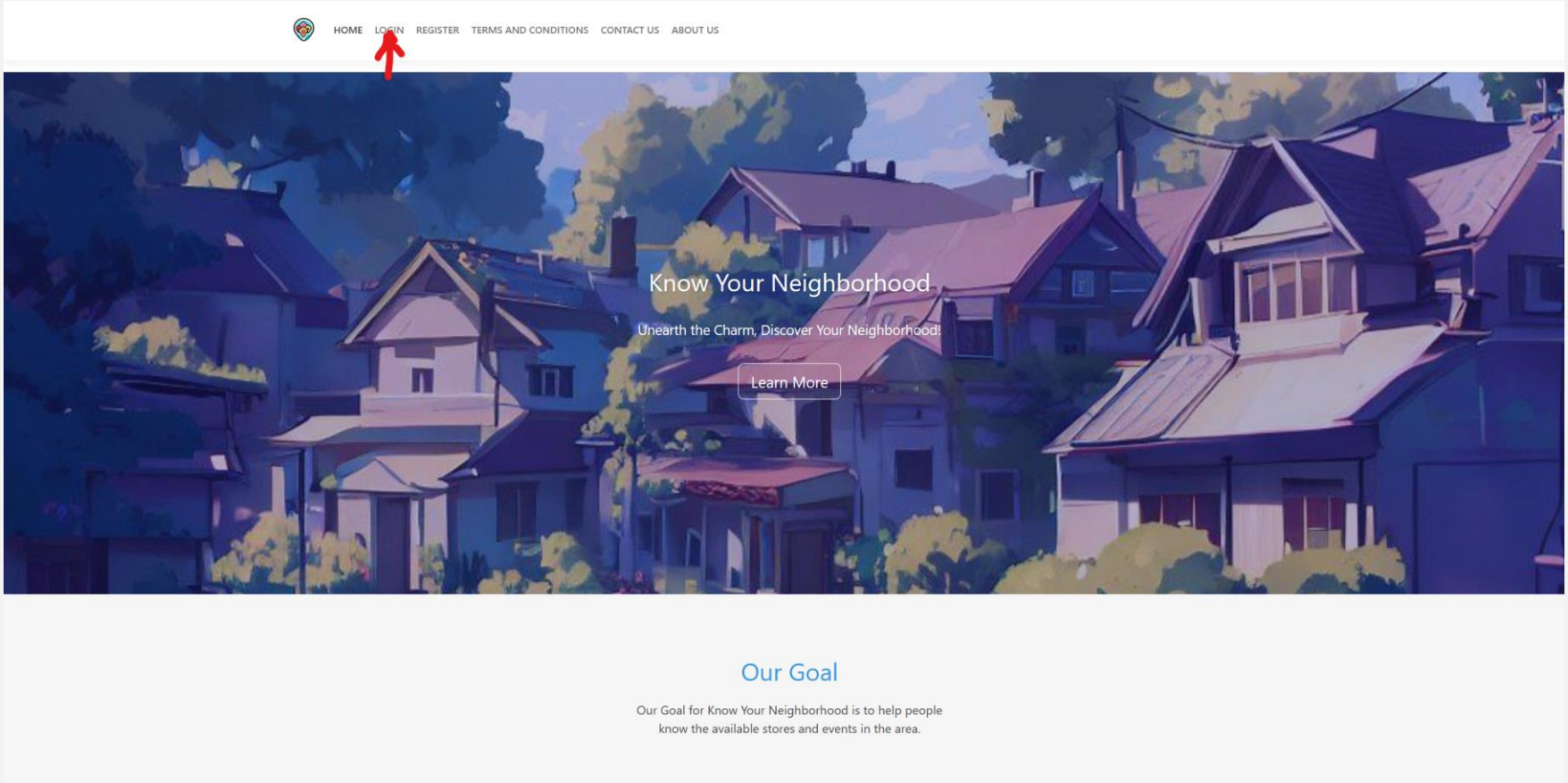


7. The Project Demo

LITHAN

Login

- The user opens the KYN website then clicks on Login

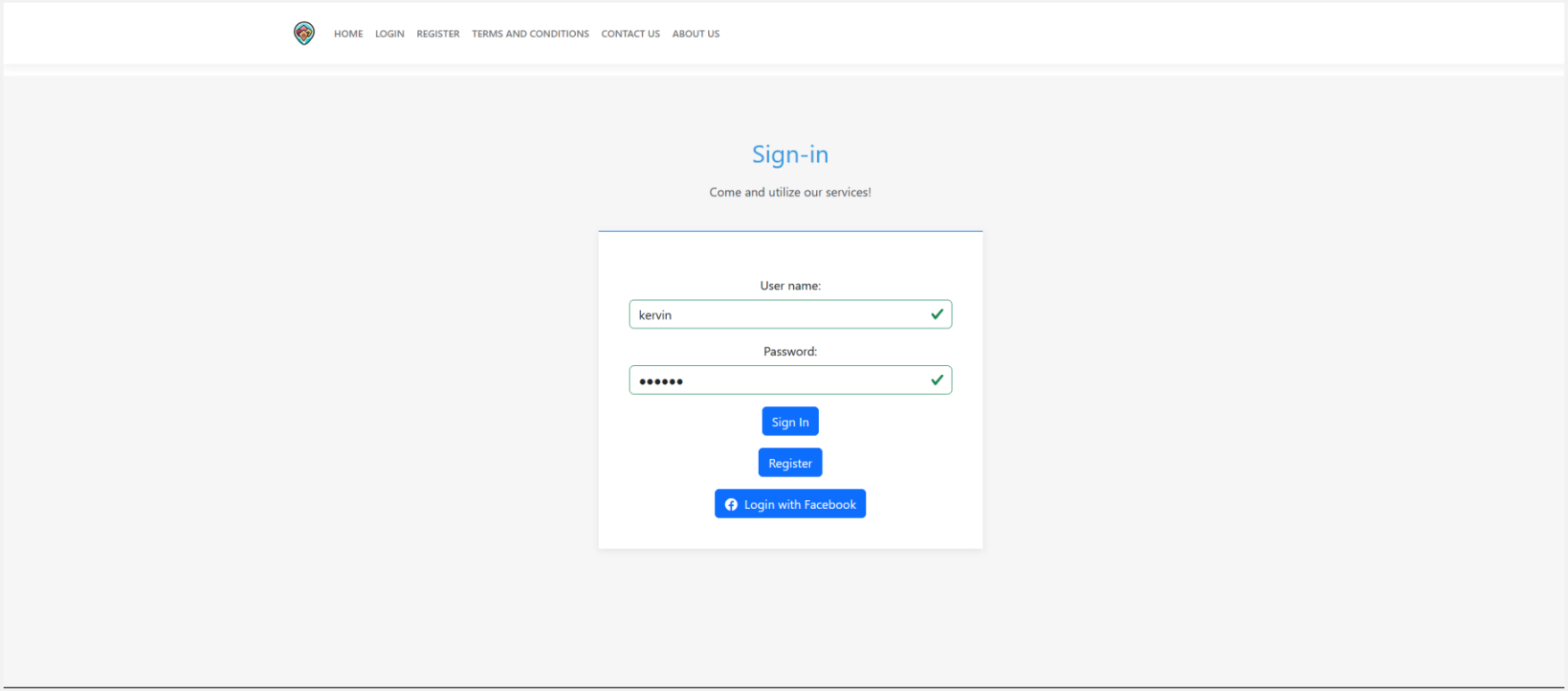


7. The Project Demo

LITHAN

Login

- Once inside, the user then fills up the Login form.

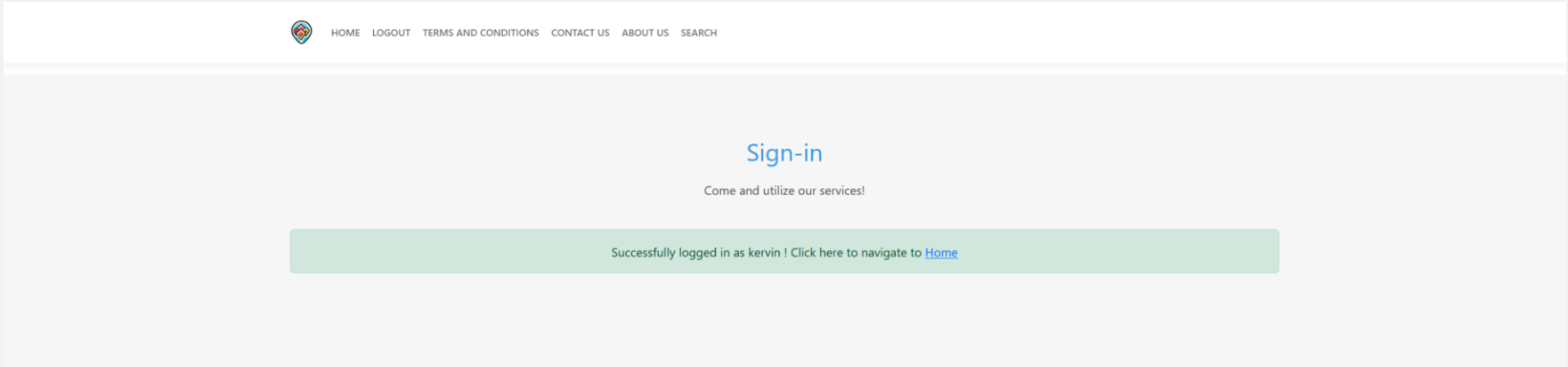


7. The Project Demo

LITHAN

Login

- Once the form confirms the credentials are correct, the user is then greeted with a success box showing their name and the button to allow them to go back to the Home Page.

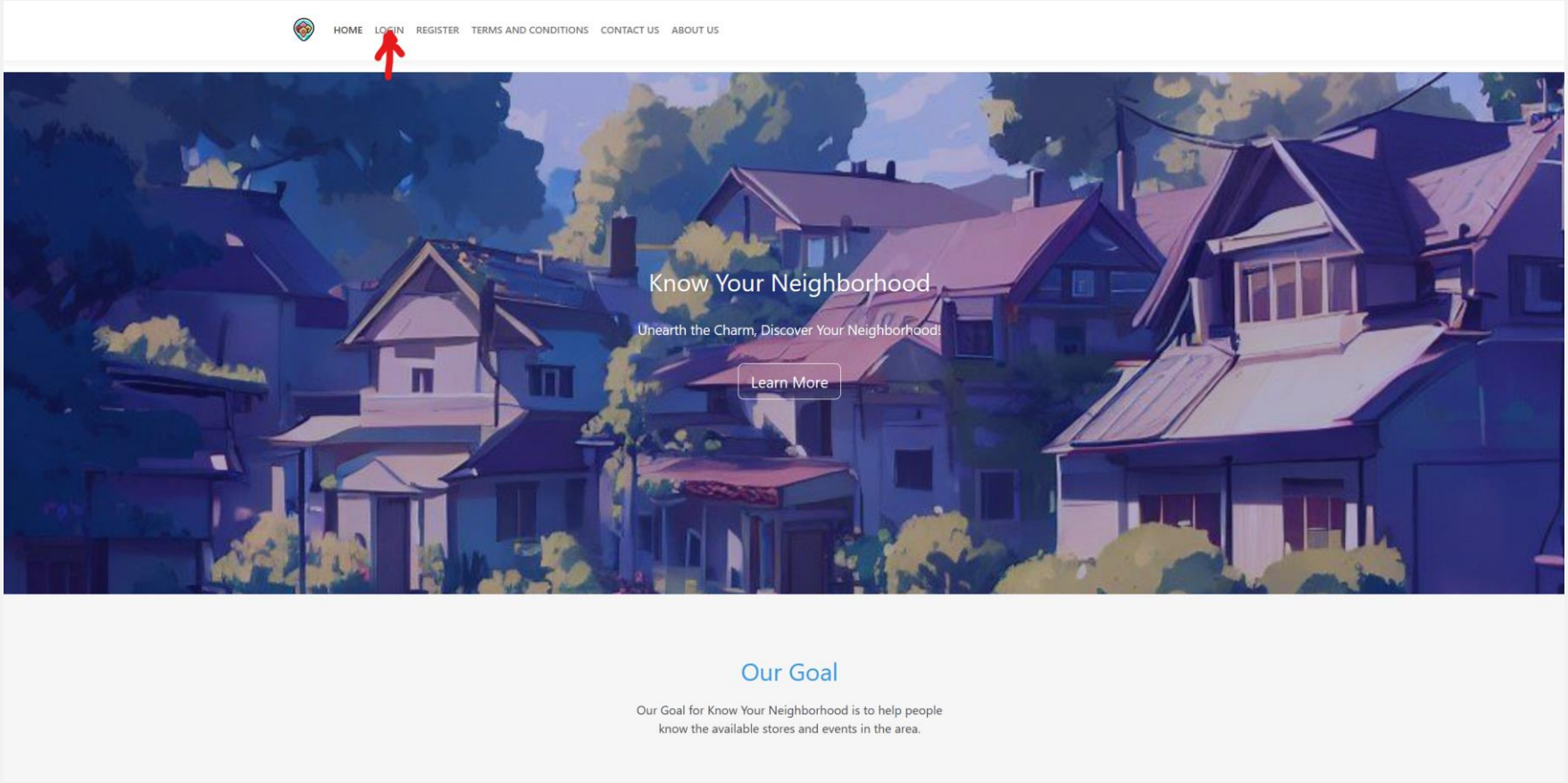


7. The Project Demo

LITHAN

Facebook Login

- The user opens the KYN website then clicks on Login

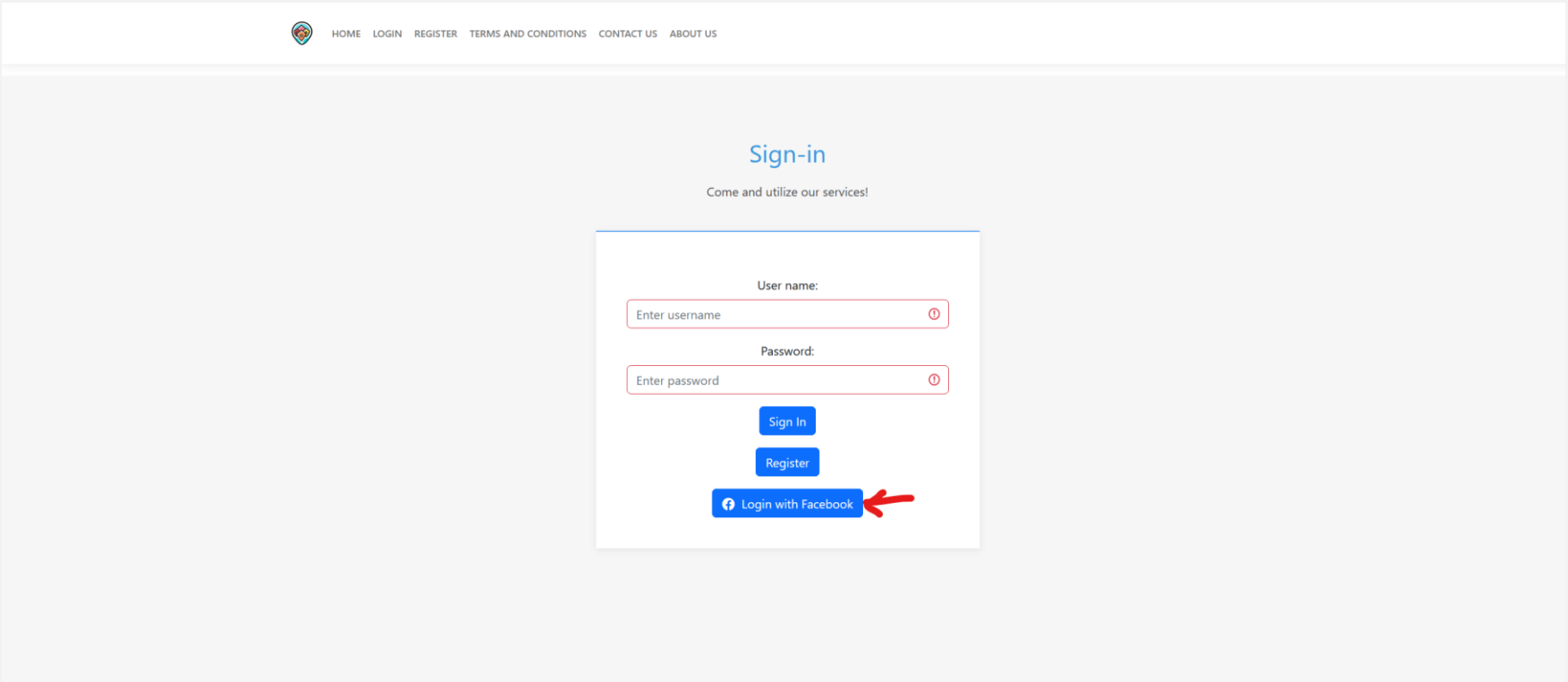


7. The Project Demo

LITHAN

Facebook Login

- Once inside, the user then clicks on the Login with Facebook button.

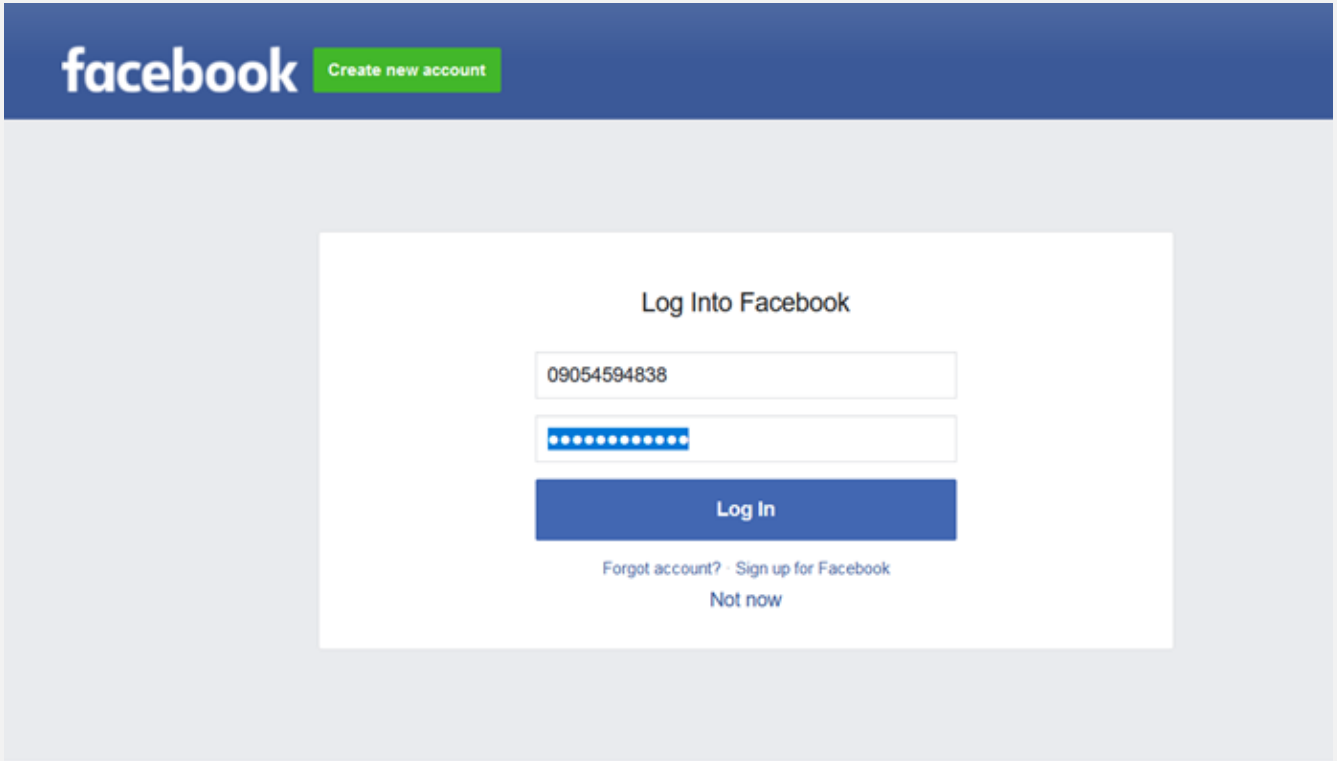


7. The Project Demo

LITHAN

Facebook Login

- The user will then be prompted to enter their Facebook credentials.

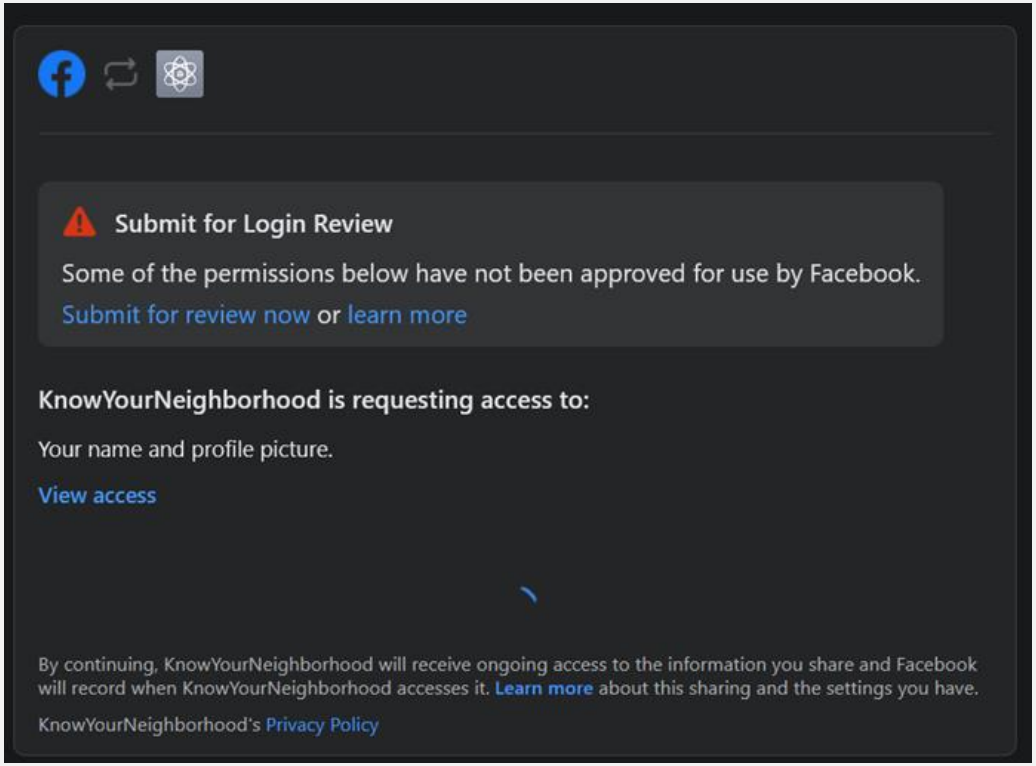


7. The Project Demo

LITHAN

Facebook Login

- The user then has to agree to the permissions required by the app.

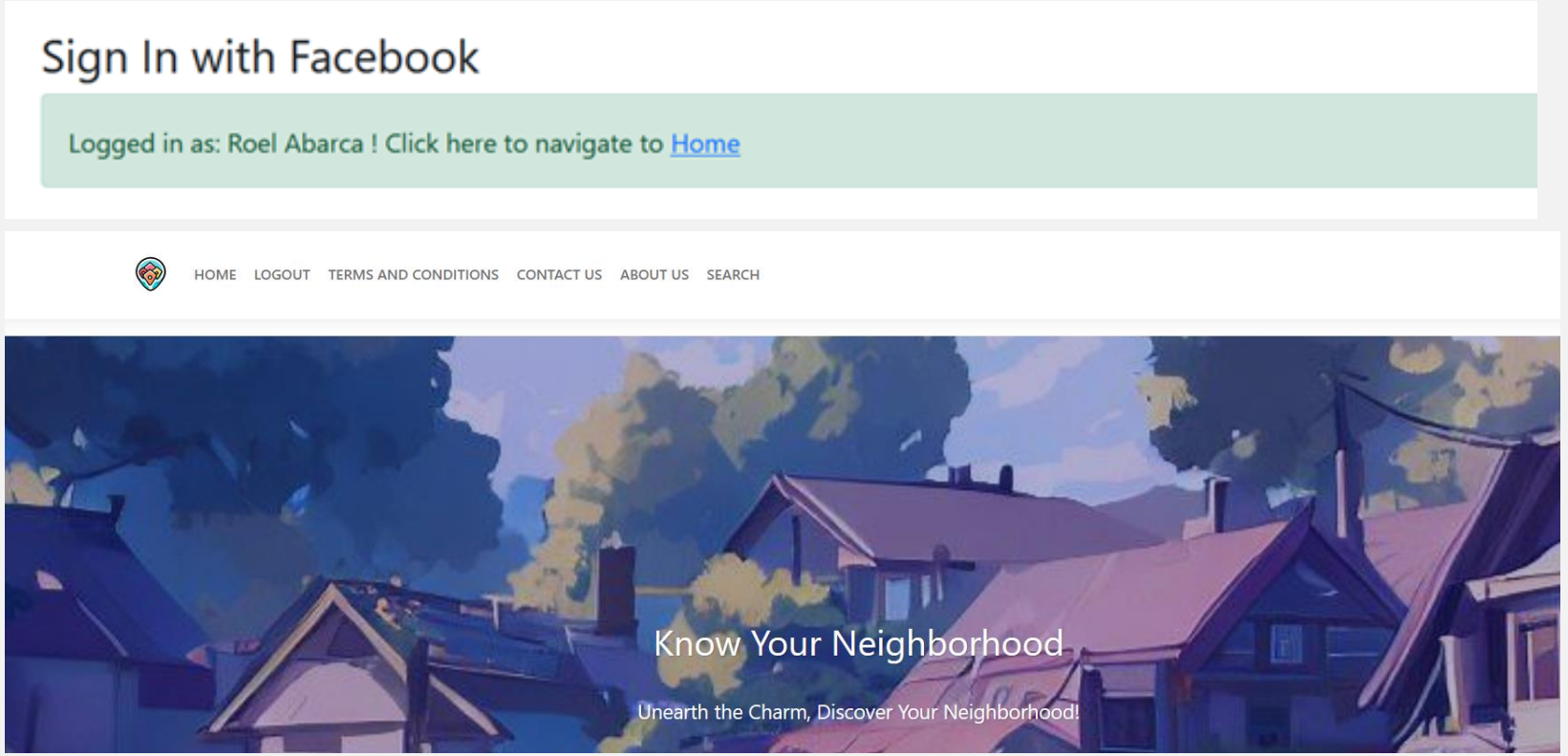


7. The Project Demo

LITHAN

Facebook Login

- Once the login is done, the site then shows the user's credentials that they are logged in with their Facebook account. Clicking Home will redirect them back to the Front-end page which shows that they have logged in.



8. The Strengths of Project API

LITHAN

Facebook API:

- **Broad User Base** - Given Facebook's enormous user base, the Facebook OAuth Login API can potentially streamline user onboarding and improve conversion rates as users won't need to create a new account to use your app.

- **Ease of Implementation** - The Facebook OAuth Login API is known to be straightforward and easy to implement. The plentiful documentation and community support available can make the development process smoother.

- **Security** - Facebook's OAuth takes care of the authentication process, which means you don't have to store or handle sensitive data like passwords. This reduces your responsibility and potential security vulnerabilities.

- **Access to User Data** - With user permission, you can access user data to create personalized experiences.

9. The Weaknesses of Project API

LITHAN

Facebook API:

- **Dependency on Facebook**: Your application's authentication relies on Facebook. If Facebook experiences downtime or the user decides to delete their Facebook account, it will affect their ability to log into your application.

- **Limited Control**: As with any third-party service, you have limited control over the authentication process. Changes to the Facebook API, terms of service, or data privacy rules could necessitate changes in your application.

- **Privacy Concerns**: Some users may not want to use their Facebook account due to privacy concerns or may not have a Facebook account at all. This could limit the accessibility of your application.

10. Security Report

LITHAN

Introduction

- The main aim of this project is to develop a comprehensive software solution, incorporating a backend system, API development, and a frontend application. Data is an invaluable resource that every organization generates, acquires, preserves, and exchanges. Safeguarding this data from internal and external threats, unauthorized access is crucial to prevent financial loss, damage to reputation, degradation of consumer trust, and brand dilution. Compliance with government and industry data protection regulations is also crucial for businesses operating anywhere.

Risk Assessment

- Integrating Facebook Login and OAuth into the project can offer several advantages, such as streamlined user authentication and access to user data. However, there are also potential risks that need to be taken into account, including data privacy, trust and reputation, dependency on third-party services, security vulnerabilities, limited user reach, and regulation compliance.

10. Security Report

LITHAN

Incident Management and Restoration

Preparation:

- Identify a dedicated team responsible for managing Facebook Login and OAuth related security incidents. Define escalation procedures and communication channels among the team members.

Incident Identification and Assessment:

- Establish clear criteria for identifying potential incidents related to Facebook Login and OAuth. Regularly monitor system logs and user reports to detect potential incidents proactively.

Incident Containment and Mitigation:

- Isolate affected systems to prevent further unauthorized access. Disable compromised access tokens related to Facebook Login and OAuth.

Notification and Communication:

- Adhere to legal and regulatory requirements for data breach notifications. Inform relevant stakeholders about the incident and its impact.

10. Security Report

LITHAN

Incident Management and Restoration

Investigation and Analysis:

- Conduct a comprehensive investigation to determine the root cause of the incident. Gather evidence to aid in the analysis.

Incident Remediation and Recovery:

- Develop and implement strategies to address the root cause of the incident. Restore affected systems to a secure state.

Learning and Improvement:

- Conduct a post-incident review to identify lessons learned. Regularly evaluate the security posture of the Facebook Login and OAuth implementation.

10. Security Report

LITHAN

Data Privacy

1. Facebook:

Facebook has a dedicated security team to handle security incidents. Facebook employs a range of security measures to protect user data.

2. OAuth:

OAuth is a protocol used to authorize access to user data. Each service provider, such as Facebook, implements its own security measures and incident response procedures.

Recommendations

To mitigate these risks, it's important to implement strong security measures and clearly communicate the project's privacy policy. Regularly monitor the project's integration with Facebook's APIs, offer alternative authentication methods, and stay updated on relevant privacy laws and regulations.

11. Review and Reflect the application

LITHAN

1. The application development process
2. Develop the required functions for the backend, including Form Login and Registration (Services, Repository, Controllers, Entity).
3. Establish a connection between the backend and the database.
4. Evaluate the functionality of the developed API utilizing Postman.
5. Build the Front-End using React Js.
6. Download the necessary npm packages.
7. Define the routes for the pages.
8. Establish a connection between the Front-End and Back-End using a proxy.
9. Construct a login API application using Facebook on https://developers.facebook.com/.
10. Configure the Back-End OAuth to link with the Facebook login API.
11. Examine the various functionalities of the project.