Graphical Password Authentication System

By – Farhan Akhtar

Introduction

A **Graphical Password Authentication system** is an authentication system that uses some **combination of graphical images** replacing the regular passwords. Graphical passwords may offer **better security** than text-based passwords because most of the people use regular, popular passwords everywhere and are prone to **social engineering attacks**. So graphical passwords can put stop to many attacks of this kind.

Problems Statement

Traditional text-based password systems suffer from weaknesses like weak passwords, memorability issues, susceptibility to shoulder surfing, and limited accessibility. These challenges compromise security and user experience, necessitating an alternative authentication method that enhances security, usability, and accessibility while meeting compliance requirements.

Weak Passwords

Traditional passwords often suffer from being too weak or easily guessable, such as "123456" or "password." GPA allows users to create more complex and memorable passwords using images or patterns, potentially reducing the likelihood of weak password choices.

Memorability

Users struggle to remember complex alphanumeric passwords, leading to frequent password resets or the use of insecure methods to remember passwords, such as writing them down. GPA offers a more intuitive and memorable alternative, improving user experience and reducing the need for frequent password resets.

Security Vulnerabilities

Text-based passwords are vulnerable to various attacks, including brute force attacks, dictionary attacks, and phishing. GPA systems can mitigate these risks by leveraging visual cues, making it harder for attackers to guess or crack passwords.

Shoulder Surfing

Observers can easily spy on users entering their text-based passwords, compromising security. GPA systems reduce the risk of shoulder surfing by utilizing graphical elements that are less easily observed or understood by onlookers.

Accessibility

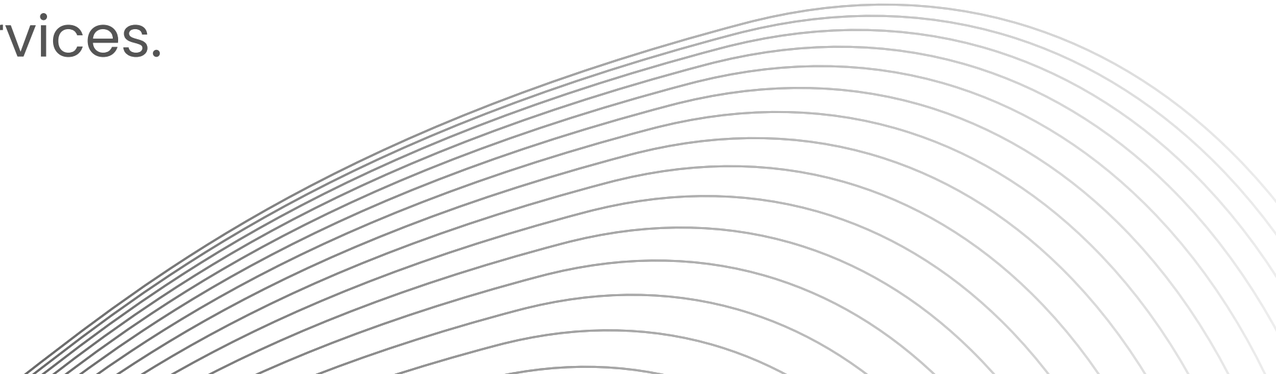
Text-based passwords can be challenging for users with certain disabilities, such as dyslexia or visual impairments. GPA systems offer a more inclusive authentication method, allowing users to leverage visual memory or cues rather than relying solely on text.

User Engagement

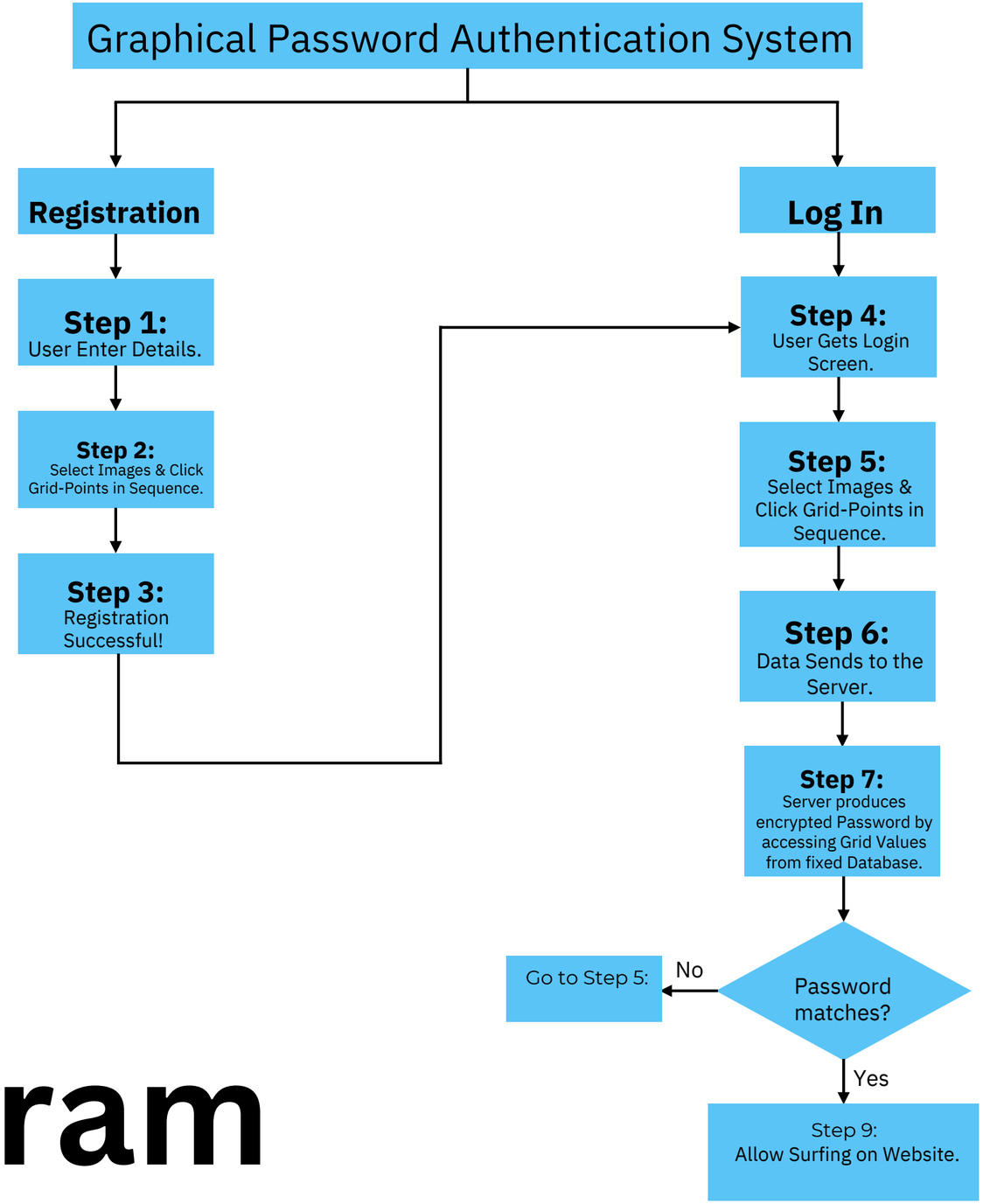
Traditional passwords can be perceived as mundane or tedious, leading to decreased user engagement with security practices. GPA systems introduce a more interactive and engaging authentication process, potentially increasing user awareness and participation in security measures.

Solutions

Graphical authentication offers a **user-friendly, intuitive, and potentially more secure** alternative to traditional text-based authentication methods. Users can choose images or patterns that are easier to remember, making authentication more accessible and resistant to shoulder surfing attacks. With a variety of options such as **click-based authentication or biometric recognition, graphical authentication enhances security** while providing a more engaging experience for users. Its flexibility accommodates a wider range of user needs, including those with disabilities, ultimately making it a valuable tool in ensuring secure access to digital systems and services.



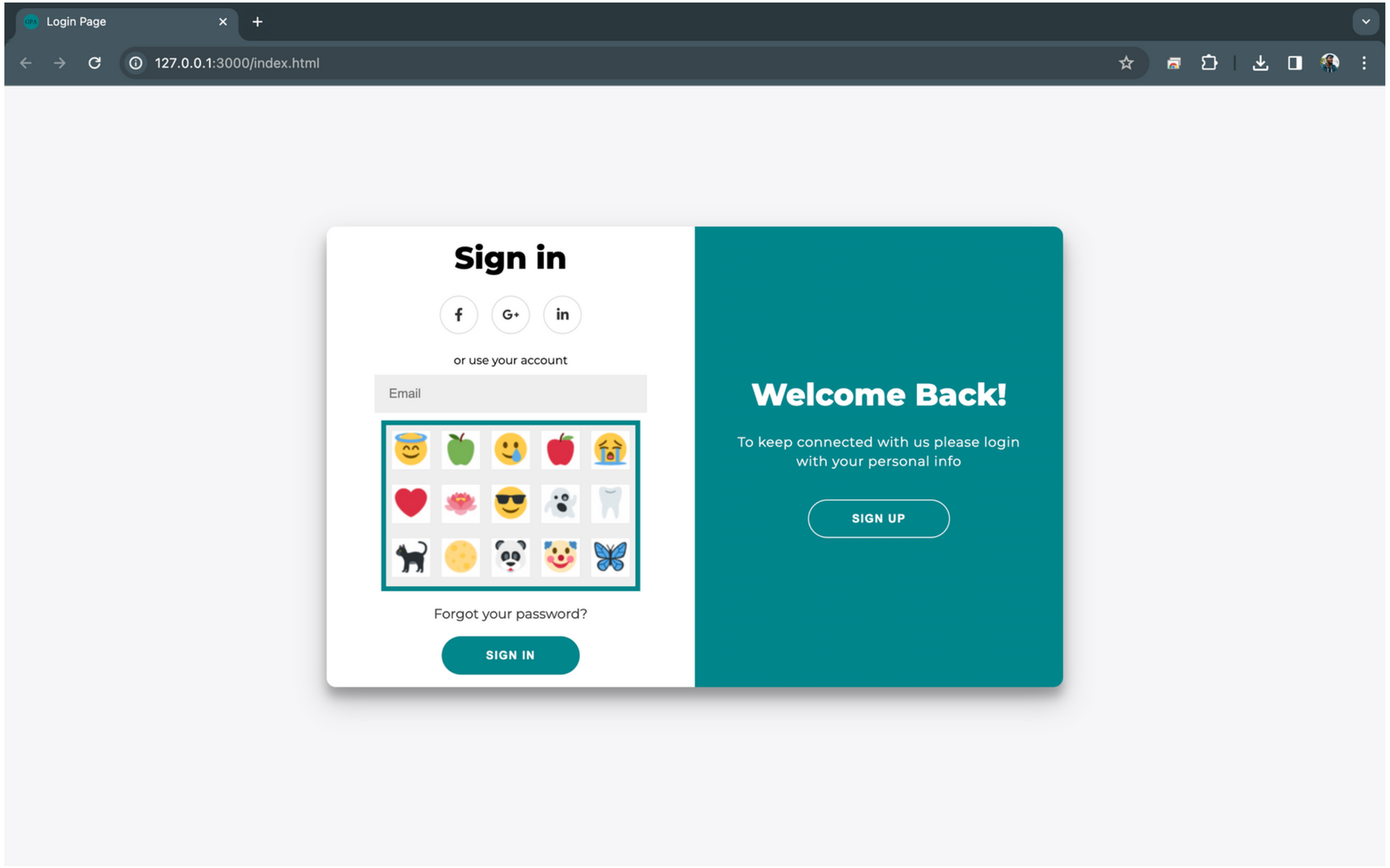
ER Diagram


Graphical Password Authentication System
Registration
Step 1:
User Enter Details.
Step 2:
Select Images & Click Grid-Points in Sequence.
Step 3:
Registration Successful!
Log In
Step 4:
User Gets Login Screen.
Step 5:
Select Images & Click Grid-Points in Sequence.
Step 6:
Data Sends to the Server.
Step 7:
Server produces encrypted Password by accessing Grid Values from fixed Database.
Password matches?
No
Go to Step 5:
Yes
Step 9:
Allow Surfing on Website.

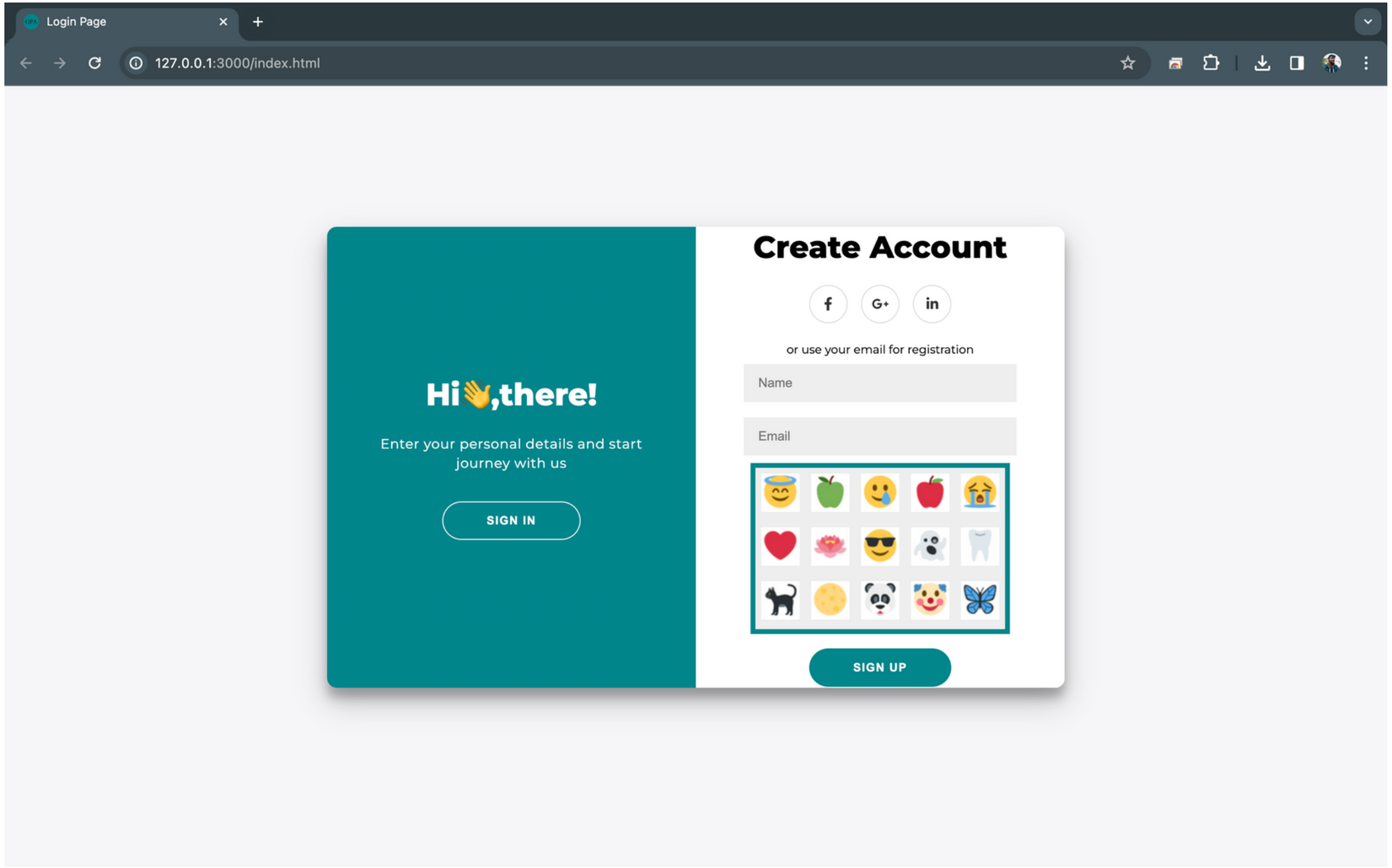
Requirement

- HTML5
- CSS
- JAVA SCRIPT
- EmailJS
- GitHub (Repo Link)

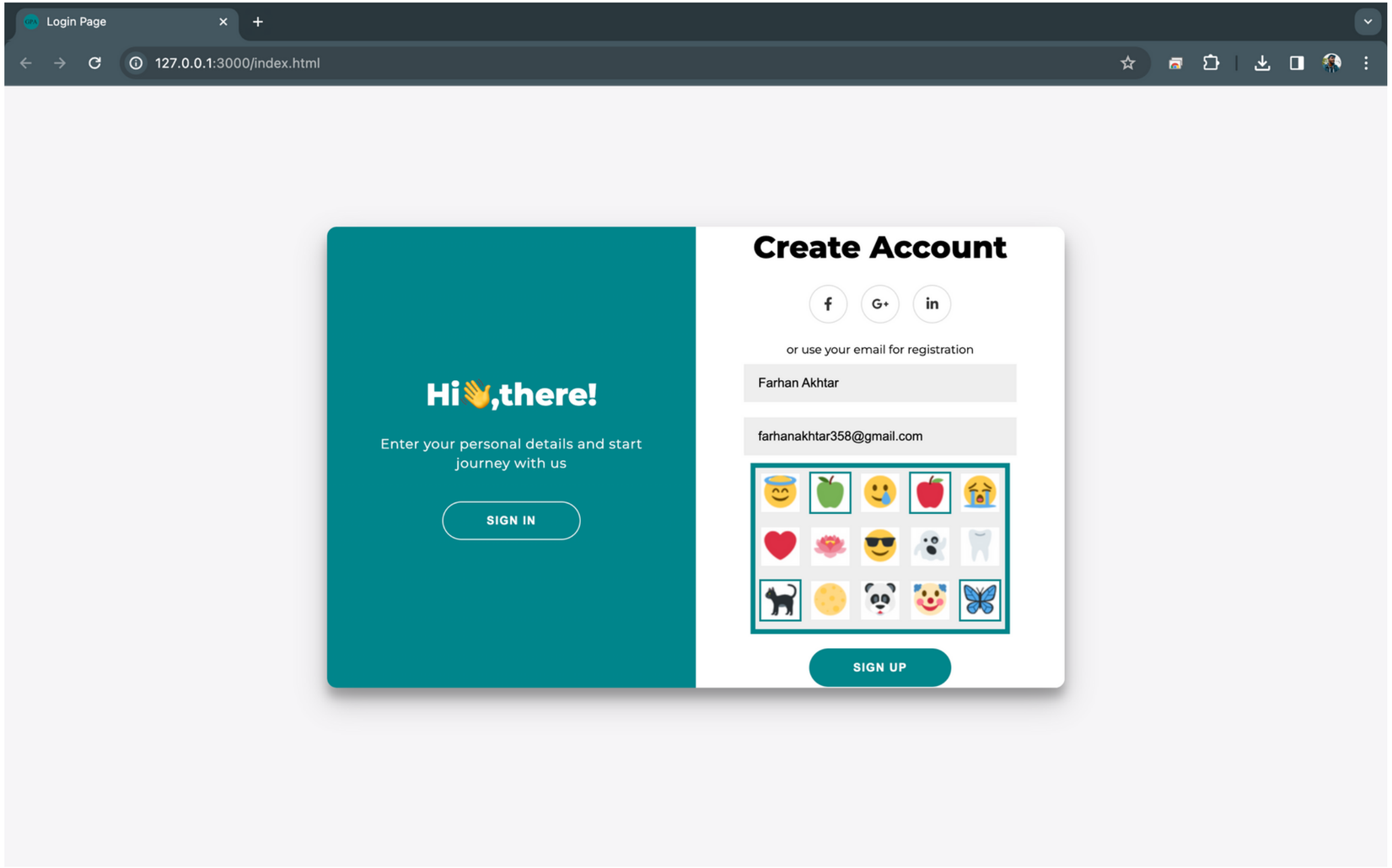
Click Here (Website link)


Login Page
127.0.0.1:3000/index.html
Sign in
or use your account
Email
Forgot your password?
SIGN IN
Welcome Back!
To keep connected with us please login with your personal info
SIGN UP

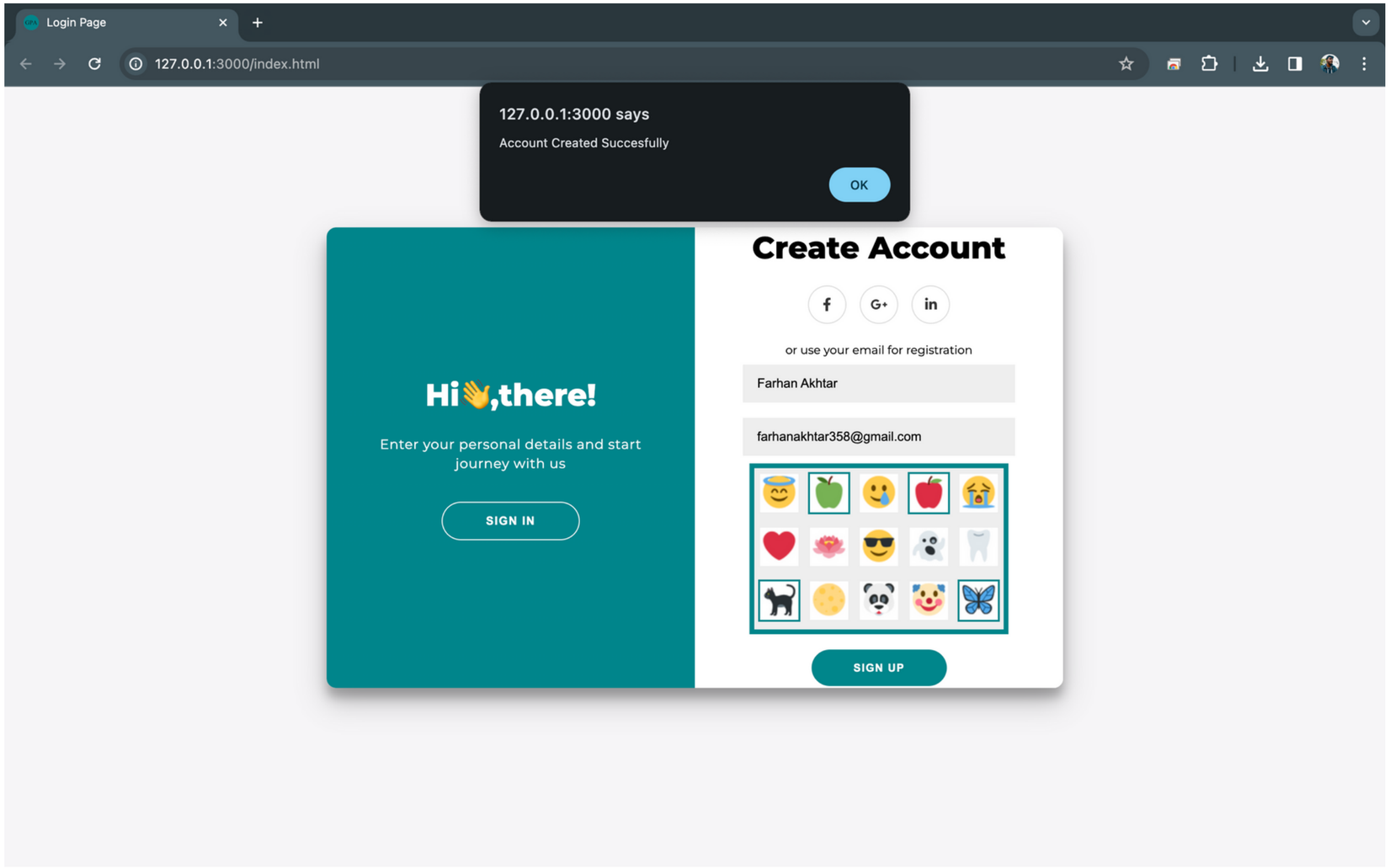
Sign In Page


Login Page
127.0.0.1:3000/index.html
Hi👋,there!
Enter your personal details and start journey with us
SIGN IN
Create Account
or use your email for registration
Name
Email
SIGN UP

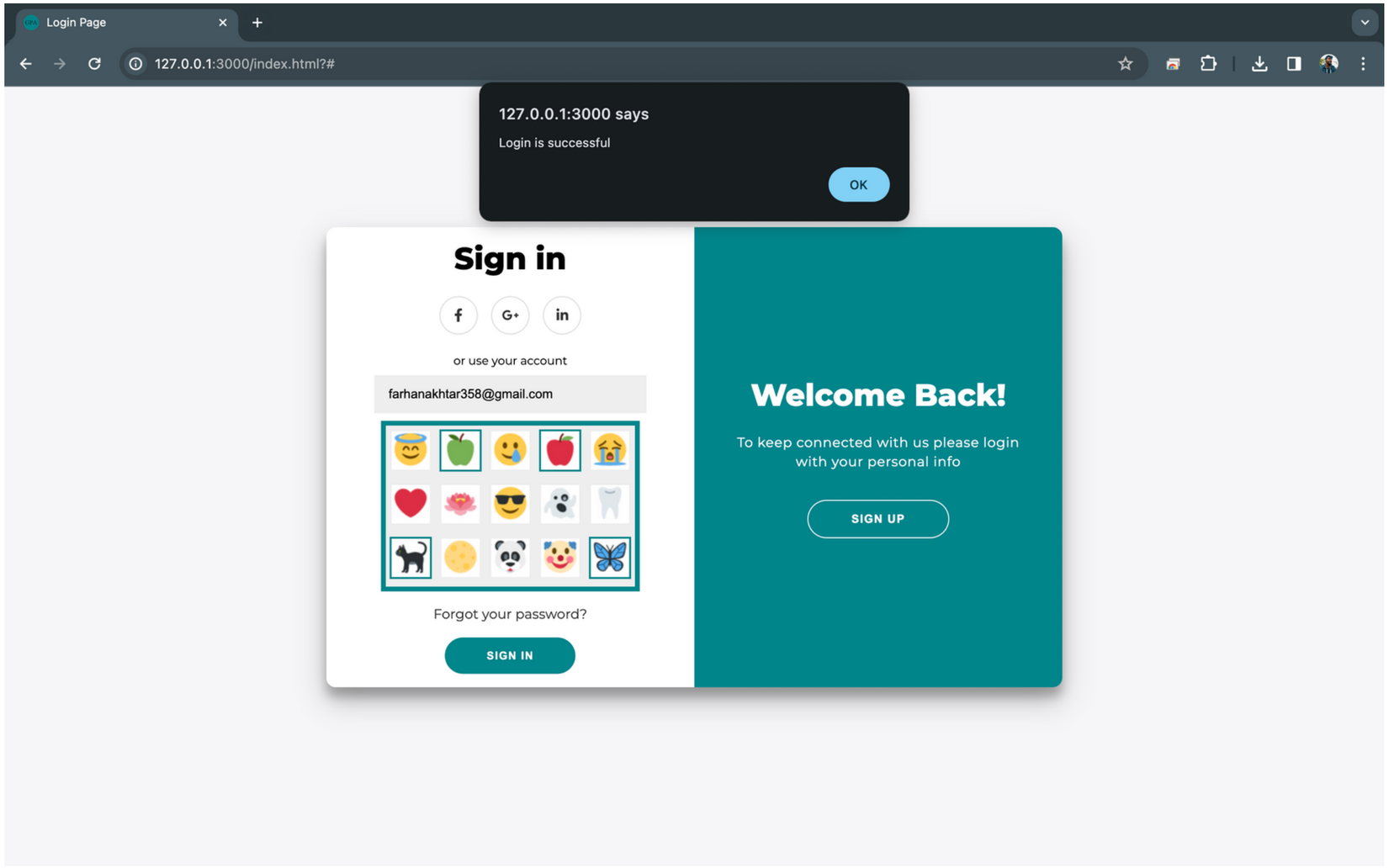
Sign Up Page



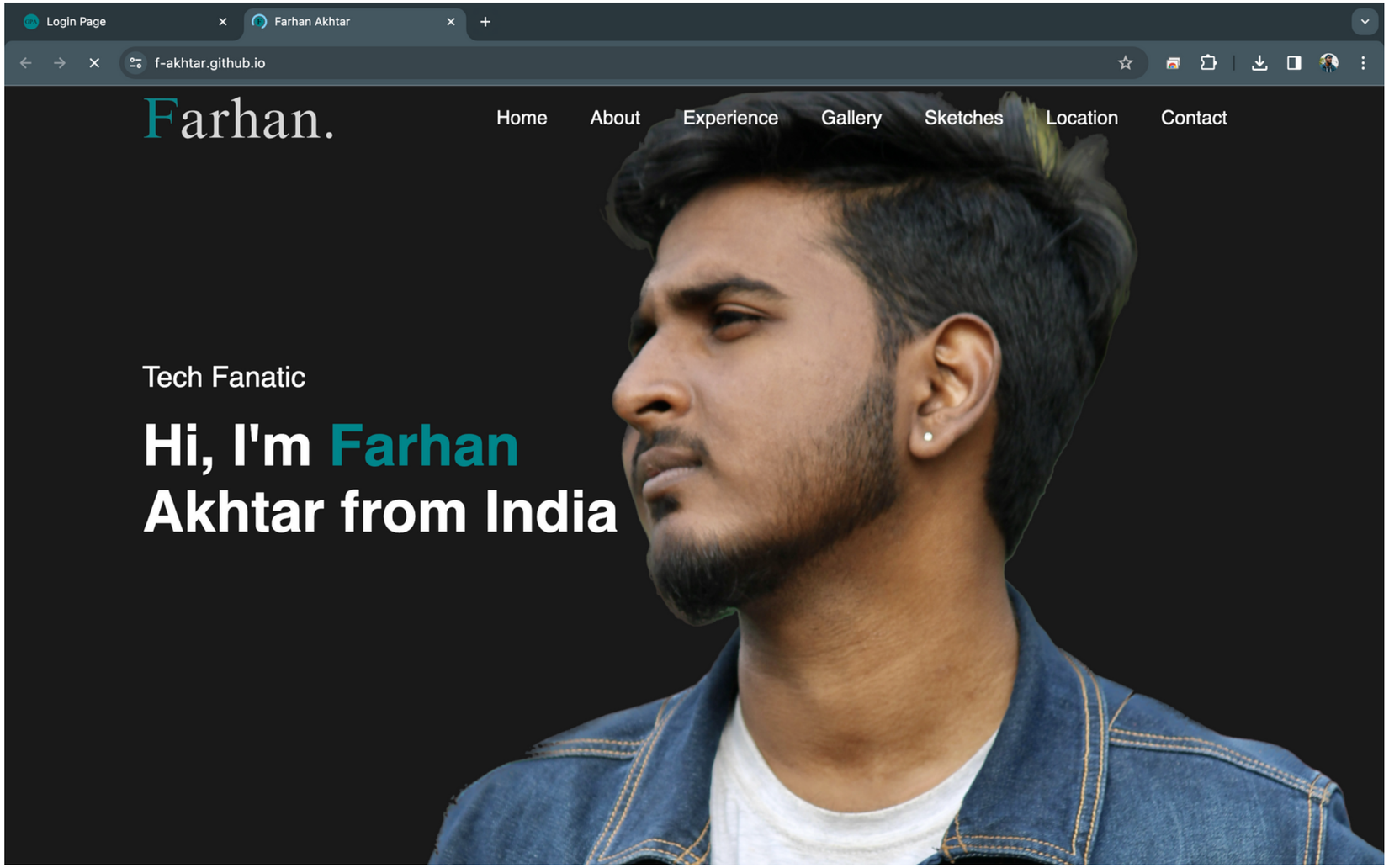
Account Creation Page



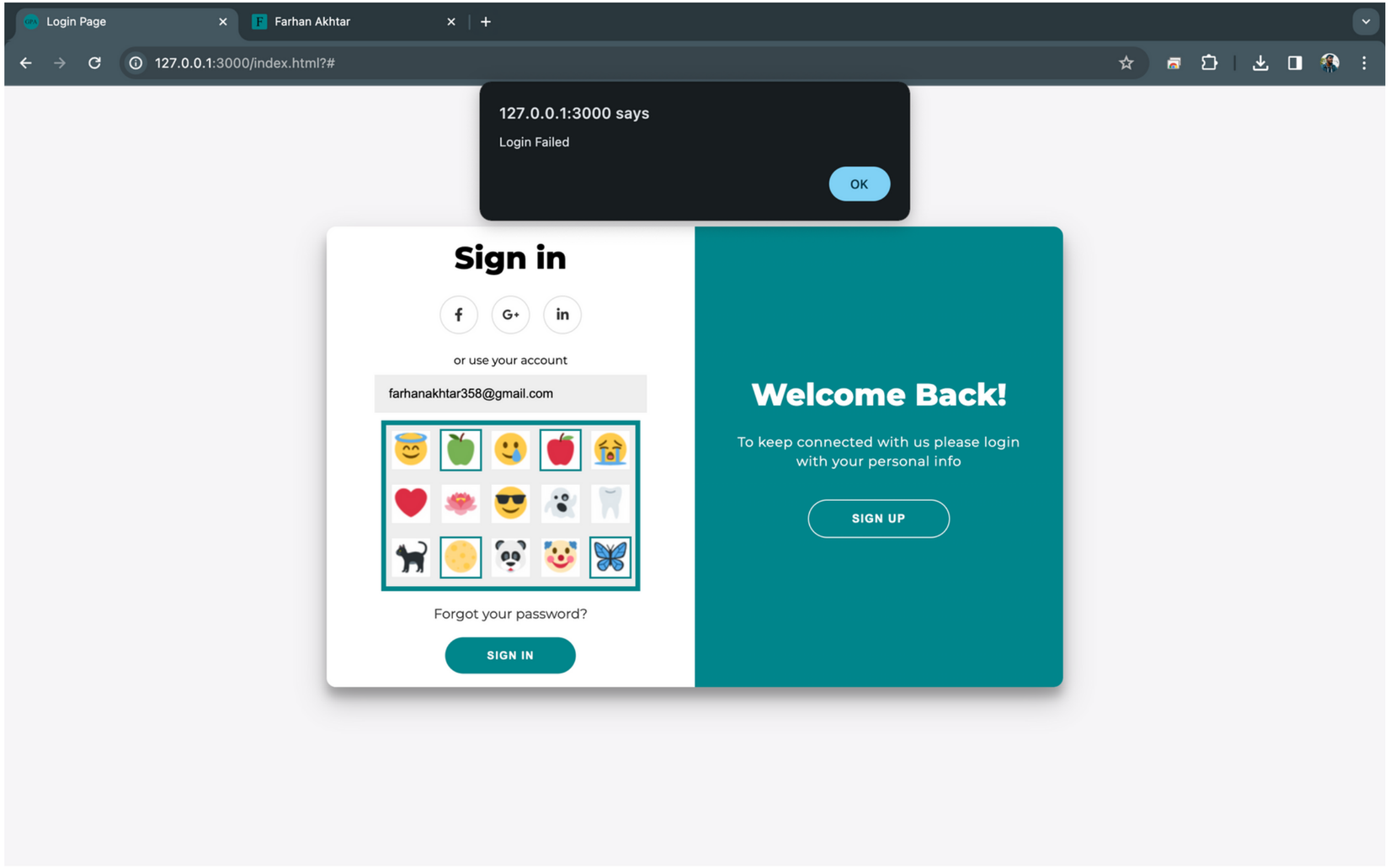
Account creation



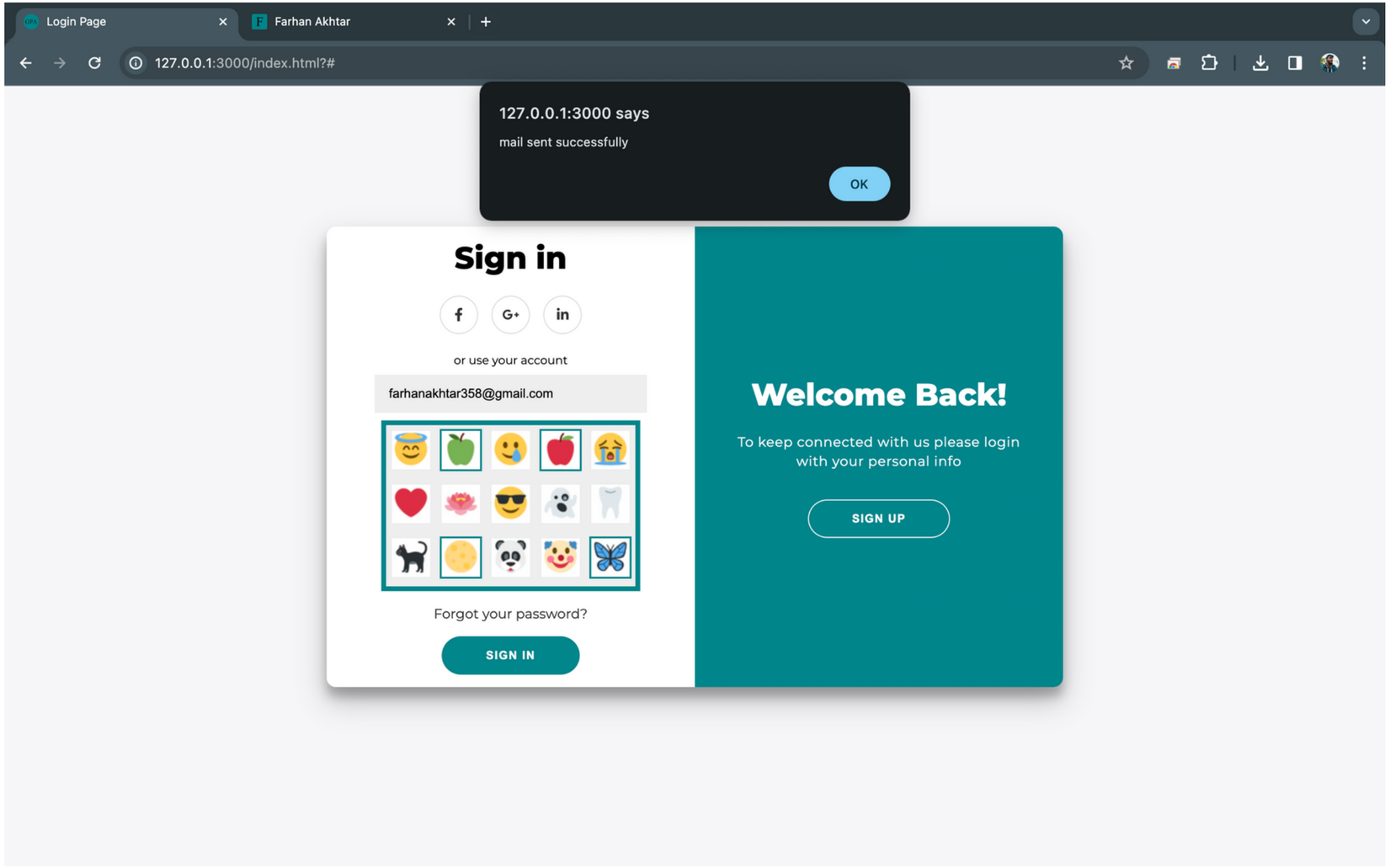
Login sucess



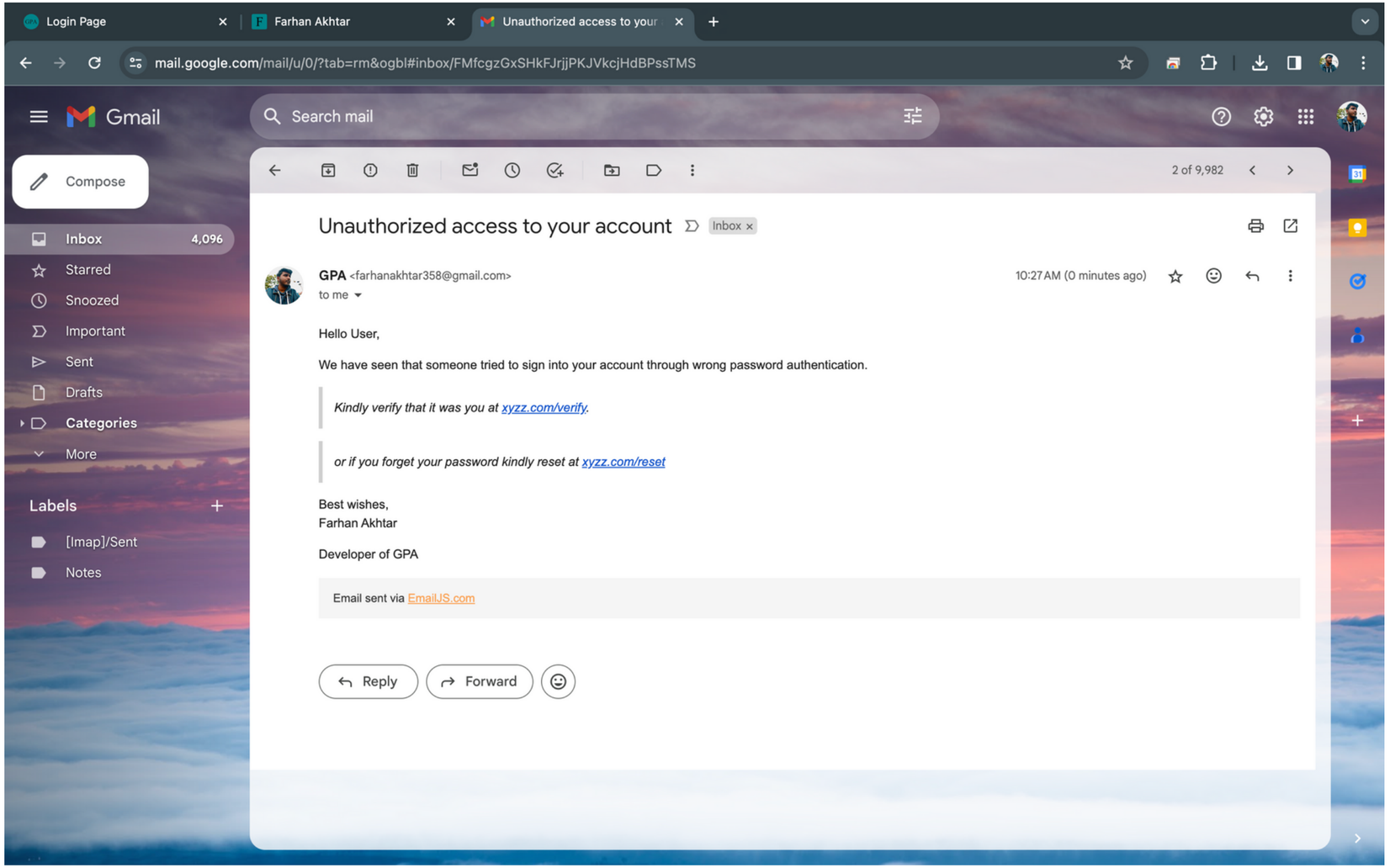
Landing Page



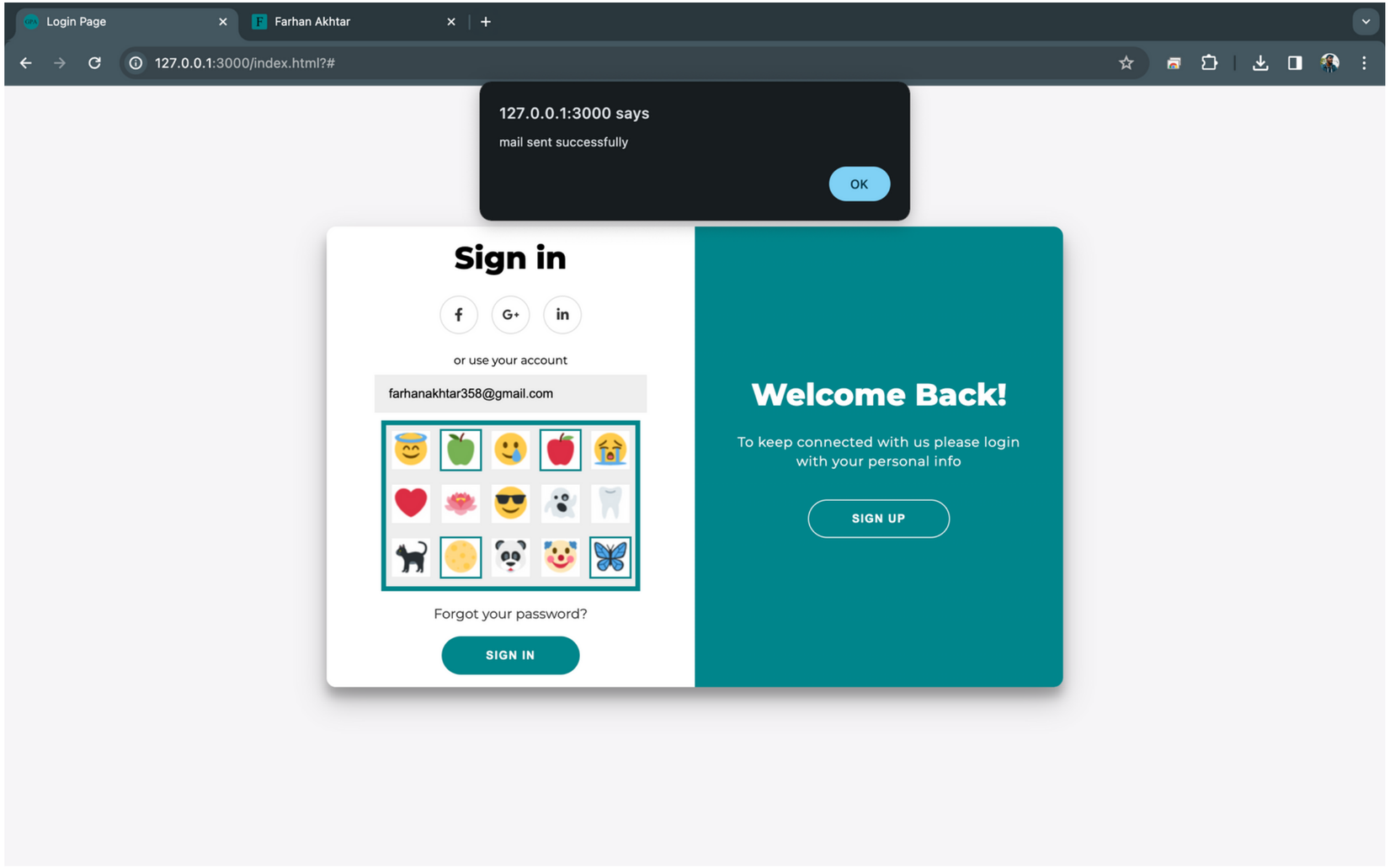
Login Failure



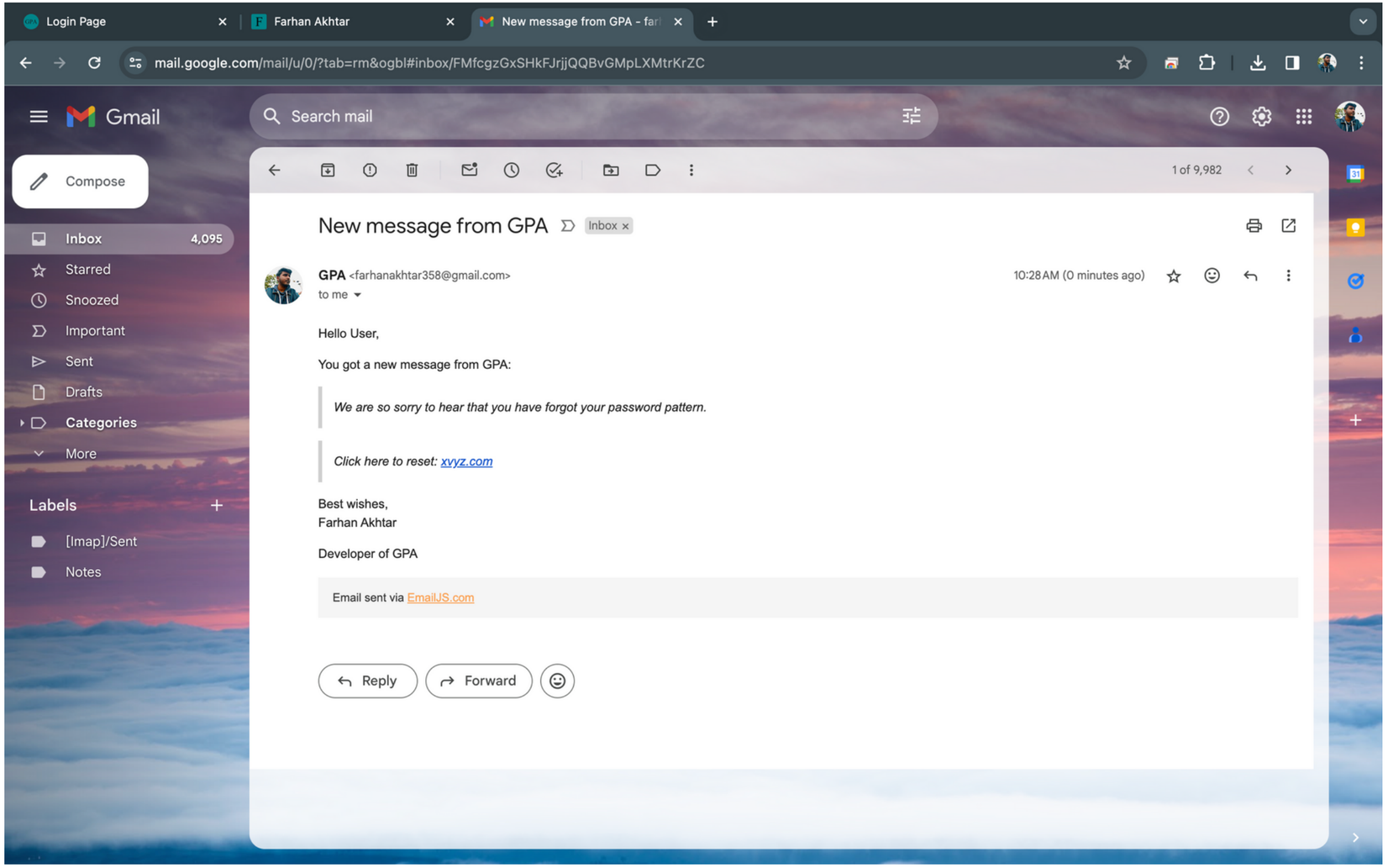
Failure Mail Pop-up



Login Failure Notification



Reset Password Mail Pop-up



Password Reset Notification

Advantages

Bruteforce

After reaching max tries, the user will be notified via message through email. And the further authentication through the generic URL/website is disabled for that user account, instead, they have to use the link that will be sent by the company in the notification email. This also lets the legitimate user know about the adversary.

Spyware

Graphical password systems resist spyware more easily than regular passwords. Key-loggers secretly capture keystrokes and transfer, but if the spyware wants to track the mouse movements, it can be tracked, but the adversary wouldn't know which part of the mouse event is actually the graphical password. The timeline vs mouse-event graph is too difficult to get the pattern

Phishing

Since the adversary is made to believe that the password is a set of images, it's not possible to make a fake page, since the adversary thinks he doesn't know the images. Moreover, we restrict the user to one attempt and suggest the user to give a fake password every time so that he triggers the server to send and URL in email so that he can log in through the legitimate login page, and the adversary cannot send the URL to users from a legitimate server. However, when the adversary knows the technique this attack might be still possible.

Presents Disadvantages

Memory Challenges

While graphical passwords can be easier to remember for some users, they may present memory challenges for others. Remembering the specific sequence of clicks or the locations of selected points on an image can be difficult, especially if users have chosen complex patterns.

Limited Adoption and Standardization

Graphical authentication methods have not been as widely adopted or standardized as text-based passwords. This lack of standardization can lead to compatibility issues across different platforms and services, making it less convenient for users.

Potential for Biometric Spoofing

Some graphical authentication systems incorporate biometric elements such as facial recognition or fingerprint scanning. However, these biometric measures may be susceptible to spoofing attacks, where attackers use fake biometric data to gain unauthorized access.

Thank You