Implementation Report

2021-07-06
Seyed Ruzaik

Introduction

This is a simple login screen implemented using ReactJs and Node. The login API was built using node and MySQL and express. The program works like this firstly a user has to first register and then try to login using username and the password which was used in the registration process. When the user tries to register with an existing mail then there will be an error message will be shown to the user saying, “This Emil Is Taken!”. And also, if the user tries register using an existing username the registration process will be aborted and will show another error message saying “This Username Is Already Taken! Please Try A Different Username”. Which means in order to sign up both the username and email has to be unique. If the user manages to sign up without having any of the error messages mentioned above, then another message will be shown to saying “Congrats, your account is created”. When the user enters a password, it will be stored in the MySQL database but fully encrypted this means no one can view any user’s password this was made possible by using Bcrypt. Bcrypt is a password-hashing function designed by Niels Provos and David Mazières, based on the Blowfish cipher, and presented at USENIX in 1999. The Bcrypt function is the default password hash algorithm for OpenBSD and was the default for some Linux distributions such as SUSE Linux. When the user is in the login screen the user must enter the correct credential details. Incase the user tries to enter a non-existing username or invalid password then again; an error message will be shown to the user. After entering the correct details, a success message will be shown to the user saying, “Signed in successfully”. Each time the user logs in a unique auth token will created. To this process I have used JWT (JSON Web Token). JSON Web Token is a proposed Internet standard for creating data with optional signature and/or optional encryption whose payload holds JSON that asserts some number of claims. The tokens are signed either using a private secret or a public/private key.

Output

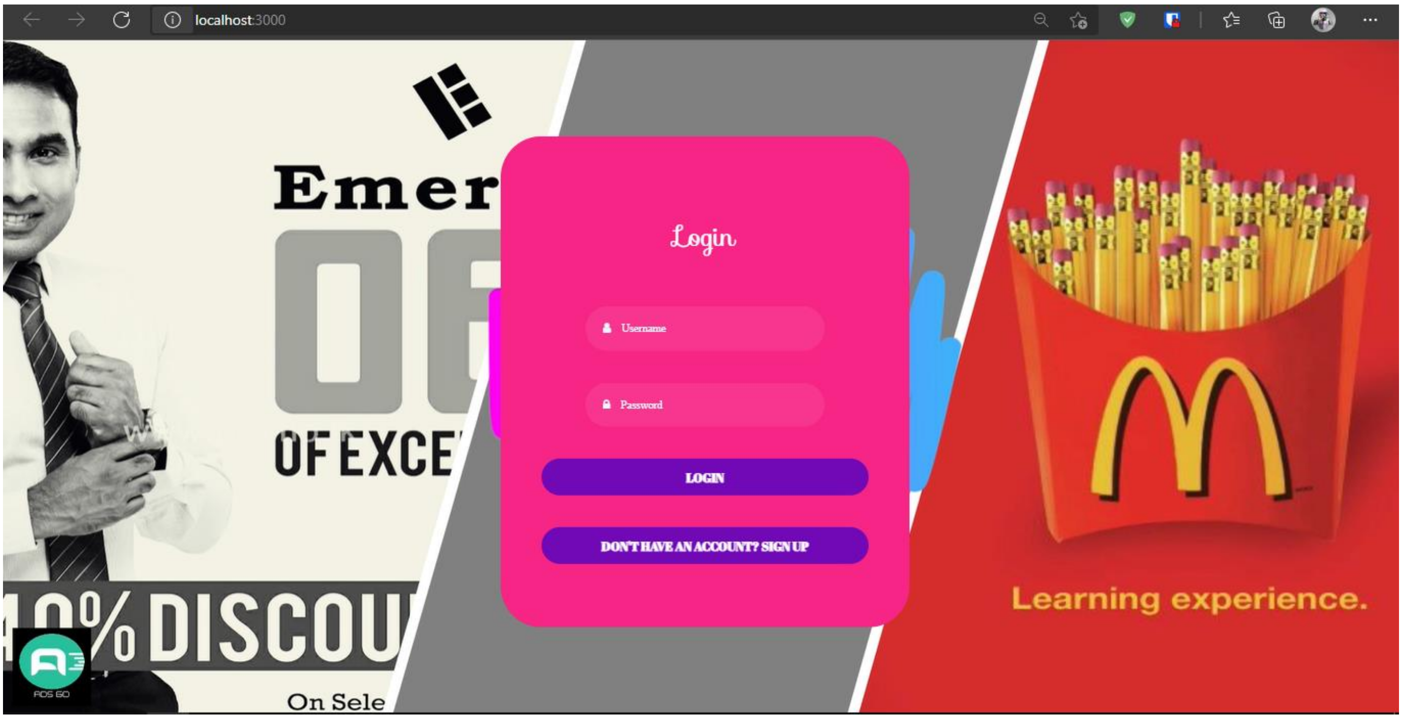


Figure 1 - Login Screen.

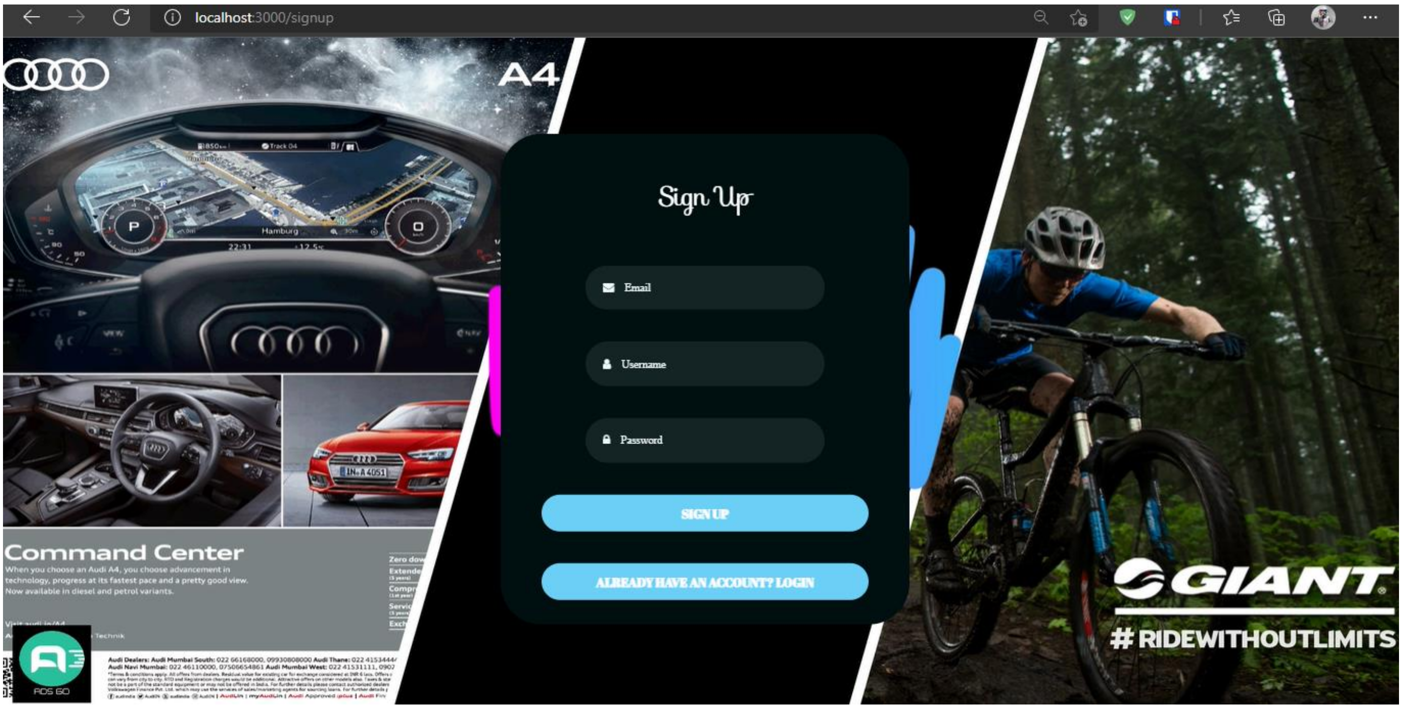
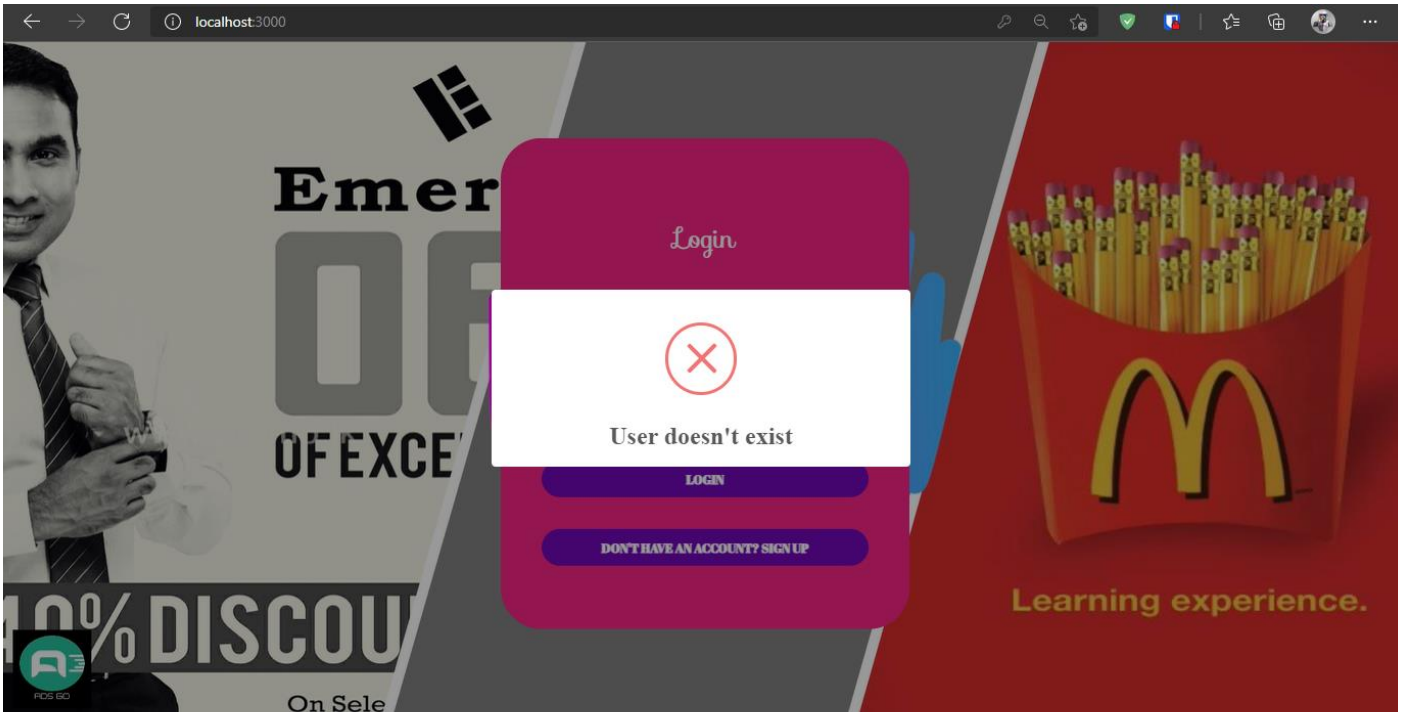
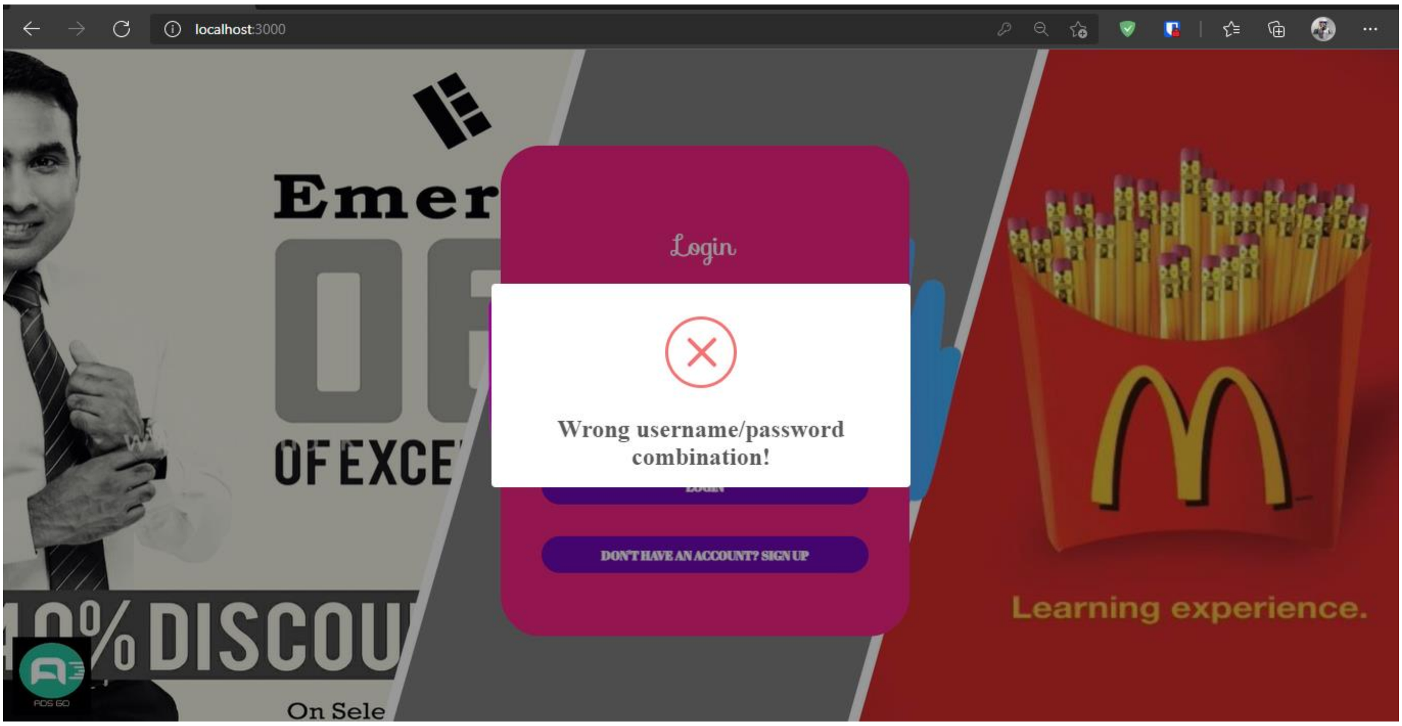


Figure 2 – Sign up Page.



User doesn't exist

Figure 3 - When the user tries to enter a non-existing username.



Wrong username/password combination!

Figure 4 - When the user tries to enter a wrong password.

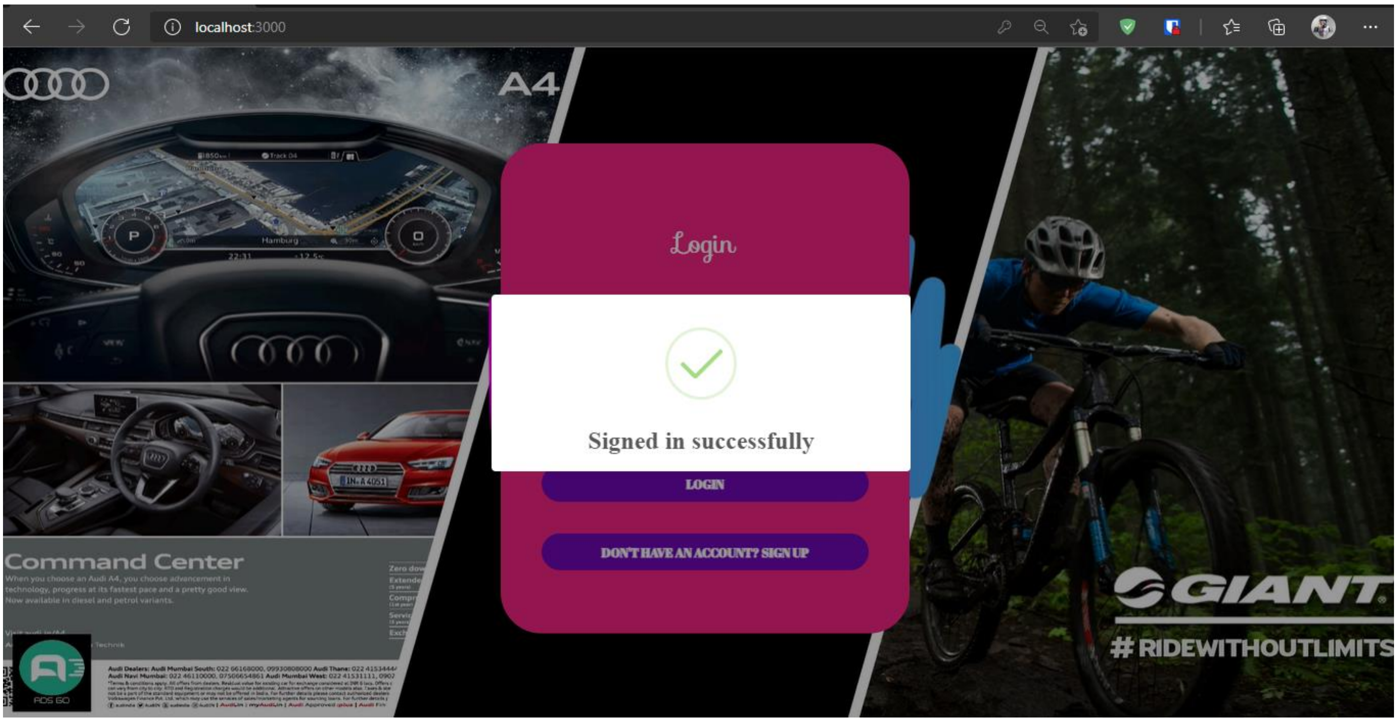


Figure 5 - When the user manages to login successfully.

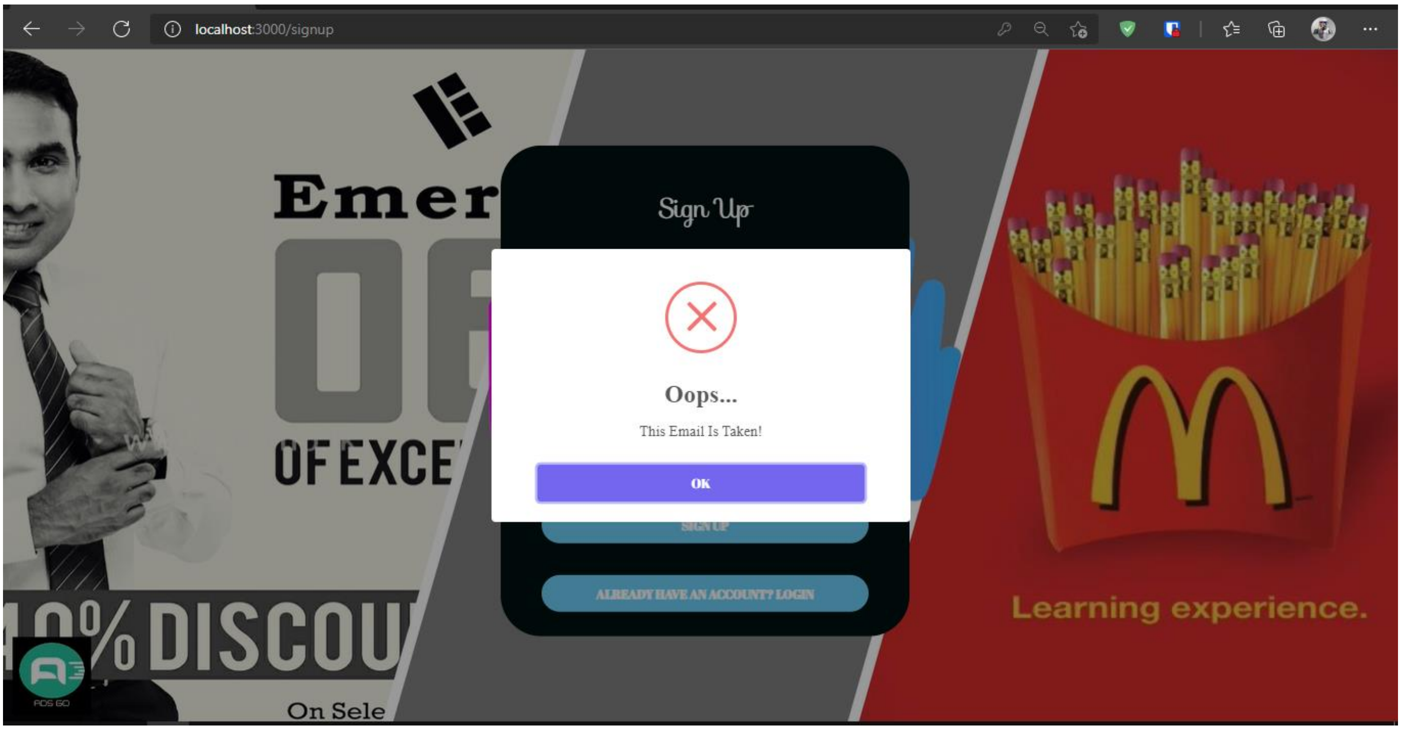
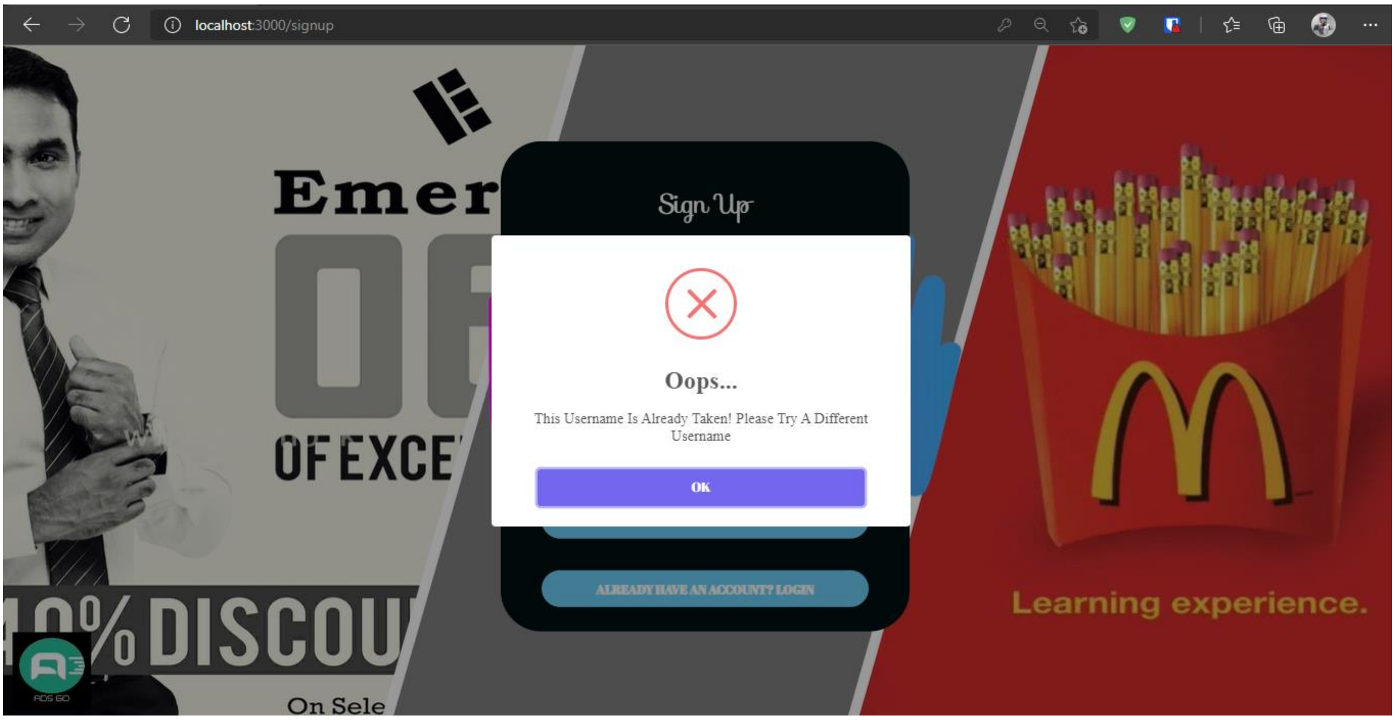


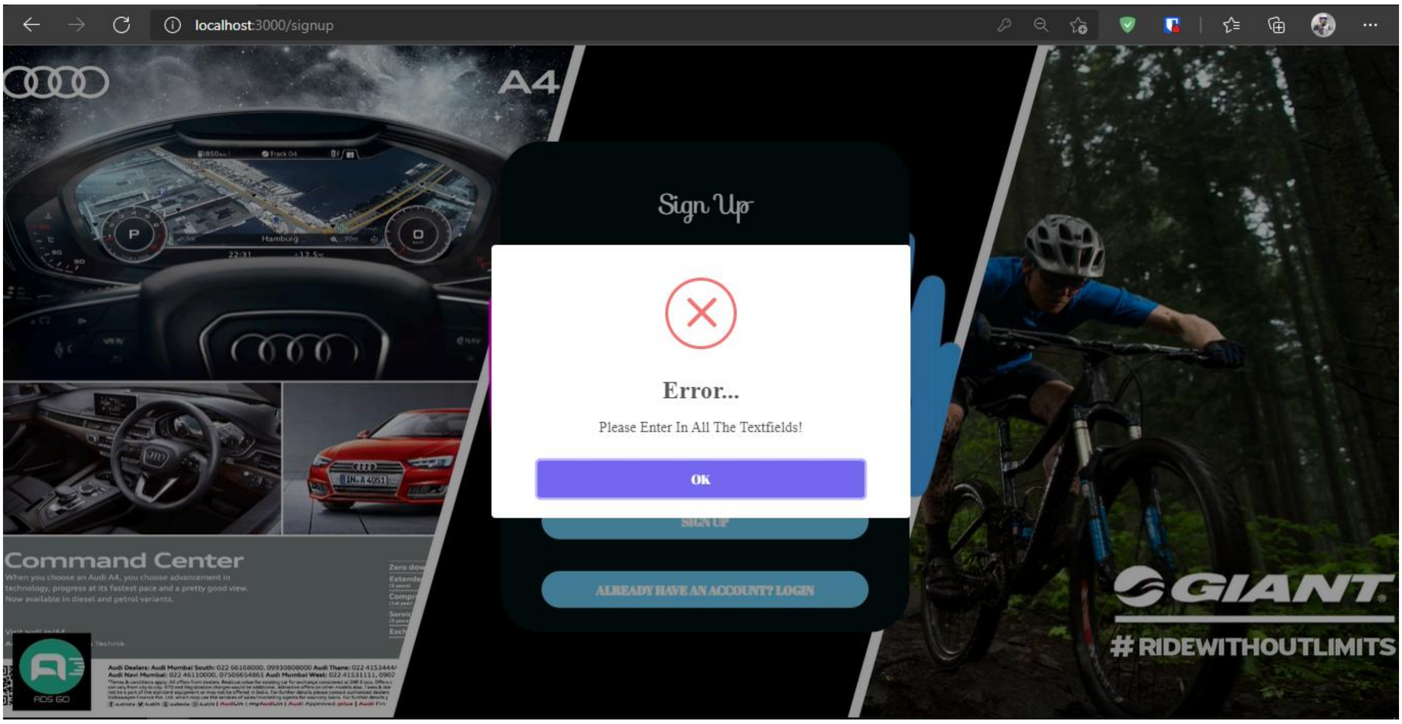
Figure 6 - If the user tries to enter an existing mail.



Oops...

This Username Is Already Taken! Please Try A Different Username

Figure 7 - If user tries to register with an existing username.



Error...

Please Enter In All The Textfields!

Figure 8 - If the user tries to sign up without entering any of the fields.

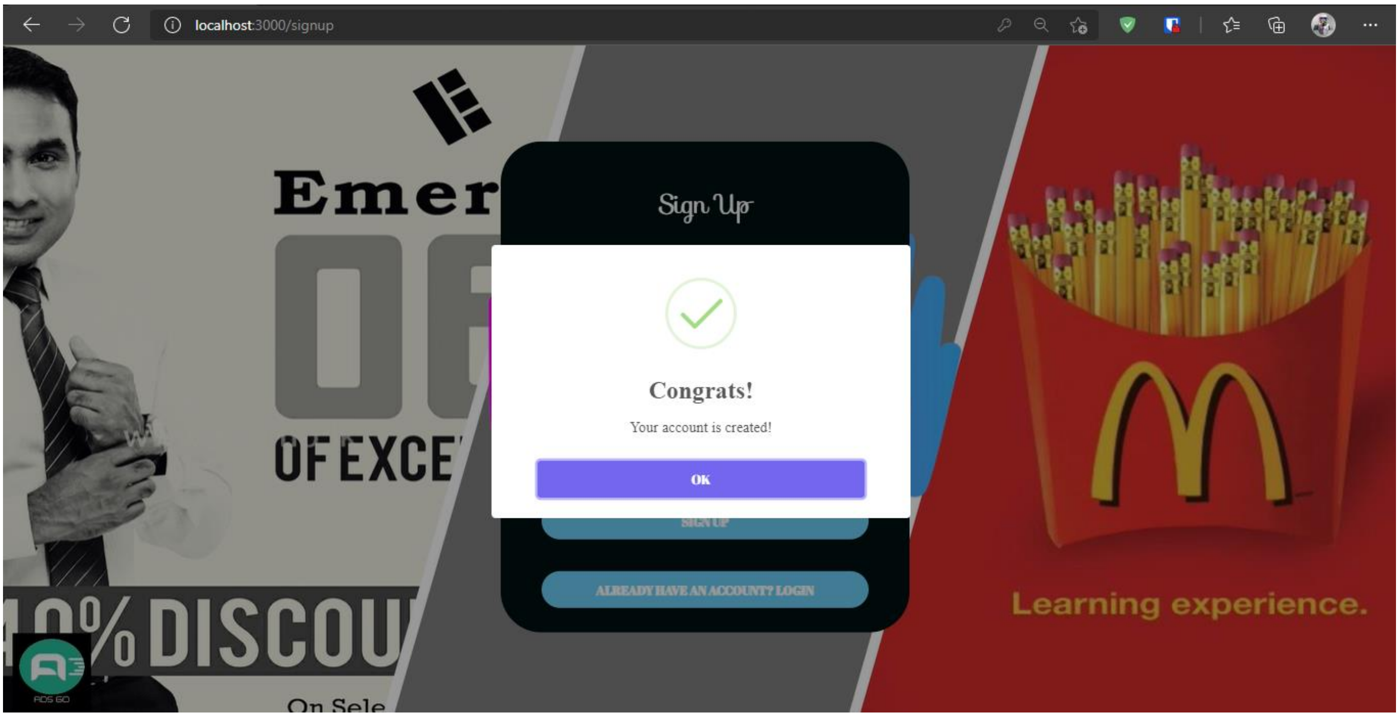


Figure 9 - When the user manages to successfully sign up.

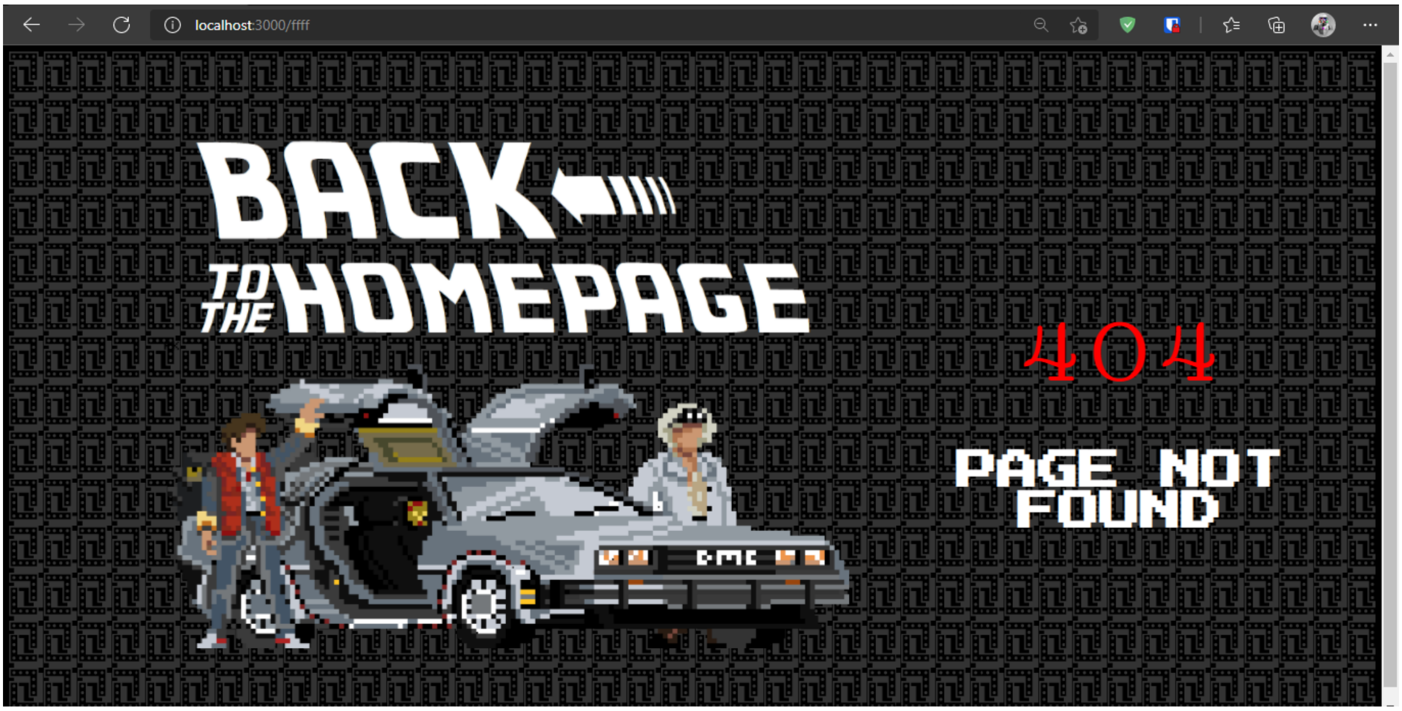


Figure 10 - Page Not Found