Task – 3 Report

Track user login information

Introduction

This report details the development and implementation of a user login information tracking and authentication system. The system captures essential login information, provides differentiated authentication mechanisms based on the user's browser, and enforces time-based access restrictions for mobile devices. The project leverages the MERN stack, Tailwind CSS, and Ethereal email services.

Background

The need for secure and customized user authentication systems is paramount in modern web applications. By tracking login information such as browser type, operating system, device type, and IP address, the system enhances security and user accountability. Differentiated authentication mechanisms ensure a balance between security and user convenience, while time-based access restrictions for mobile devices add an additional layer of control.

Learning Objectives

- Understand how to capture and store user login information.
- Implement differentiated authentication workflows.
- Enforce time-based access restrictions for mobile devices.
- Integrate the login system into a MERN stack application.

Activities and Tasks

1. **Capture User Login Information:**

- **Task:** Detect browser type, operating system, device type (desktop or mobile), and IP address.
- **Implementation:** Use libraries like user-agent and request-ip to parse user agent strings and capture the IP address. Store this data in MongoDB.

2. **Implement Authentication Workflow:**
   - **Google Chrome Users:** Require OTP authentication via Ethereal email.
     - **Task:** Generate and send OTP, verify OTP upon user input.
     - **Implementation:** Use nodemailer with Ethereal email for OTP delivery.
   - **Microsoft Browser Users:** Allow direct access without additional authentication.
     - **Task:** Skip OTP verification for Microsoft browsers.
     - **Implementation:** Use conditional logic based on browser type.
   - **Mobile Device Users:** Enforce access restrictions between 10 AM and 1 PM.
     - **Task:** Check current time and enforce access control for mobile devices.
     - **Implementation:** Implement server-side time check to restrict access.

3. **Frontend and Backend Integration:**
   - **Task:** Display login history to users using React and Tailwind CSS.
   - **Implementation:** Fetch login history from MongoDB and render it in a user-friendly interface using React components styled with Tailwind CSS.

Skills and Competencies

- **MERN Stack Proficiency:** Development and integration of MongoDB, Express, React, and Node.js.
- **Frontend Development:** Using Tailwind CSS for styling and React for building dynamic user interfaces.
- **Backend Development:** Secure backend development with Node.js and Express.
- **Security Practices:** Implementing OTP authentication and session management.
- **Time-based Access Control:** Enforcing conditional access based on time and device type.
-

Feedback and Evidence

- **User Testing:** Conduct user testing to validate accurate login information capture and display.
- **Security Review:** Ensure the effectiveness of OTP authentication and access controls through thorough security reviews.

- **Performance Monitoring:** Monitor system performance to ensure efficient login processes without delays.

Challenges and Solutions

- **Accurate Device Detection:** Ensuring the reliable detection of user devices and browsers.
    - **Solution:** Utilize robust libraries such as user-agent for accurate parsing of user agent strings.
- **OTP Delivery Reliability:** Guaranteeing the delivery and handling of OTPs.
    - **Solution:** Implement thorough error handling and use Ethereal email for testing to simulate real-world scenarios.
- **Time-based Restrictions:** Effectively enforcing time-based access controls.
    - **Solution:** Implement precise server-side checks to enforce access restrictions based on the current time.

Outcomes and Impact

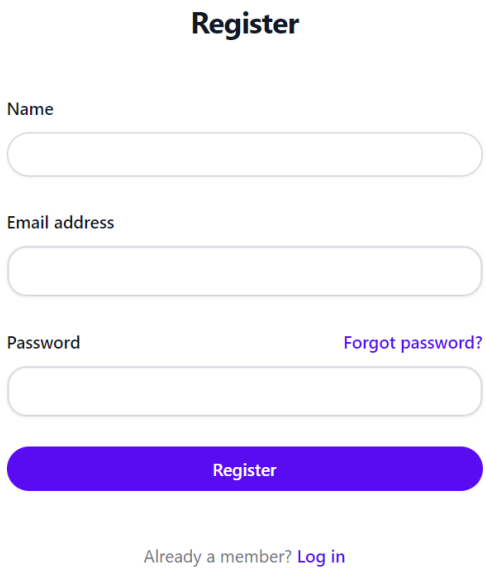
- **Enhanced Security:** Improved security through detailed tracking of login information and OTP authentication for certain users.
- **User Convenience:** Simplified login process for Microsoft browser users and controlled access times for mobile users to ensure a smooth user experience.
- **Data Insights:** Ability to analyze login patterns and detect potential security threats.

Conclusion

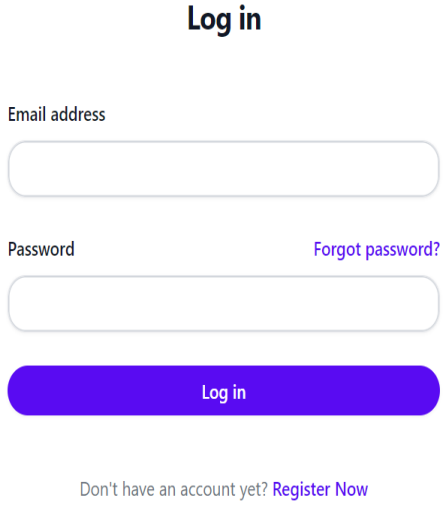
The implementation of this user login information tracking and authentication system successfully integrated advanced security and usability features into a MERN stack application. This project not only enhanced the security of the application but also improved the overall user experience by providing customized authentication workflows and detailed login history.

Images of the project:

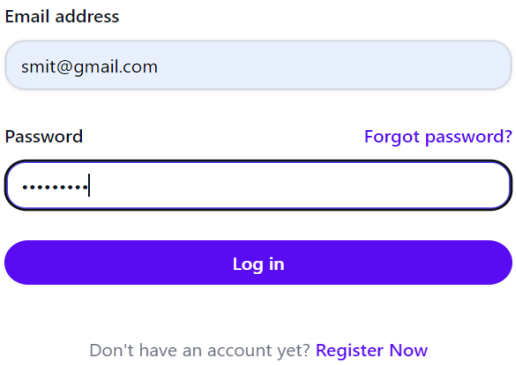
Register Page

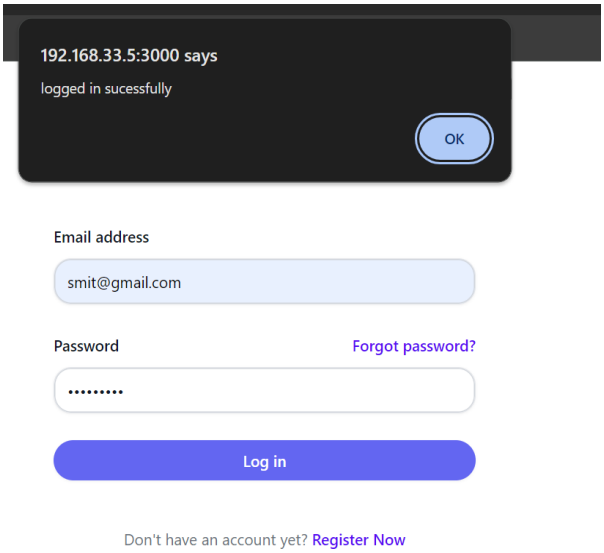


Login Page

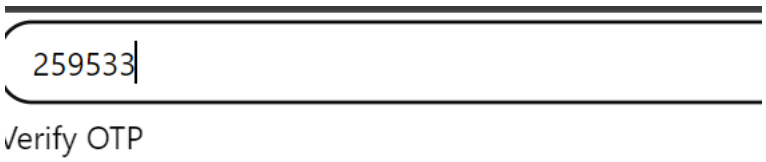


After Successful Login We will be redirected to the otp verification page

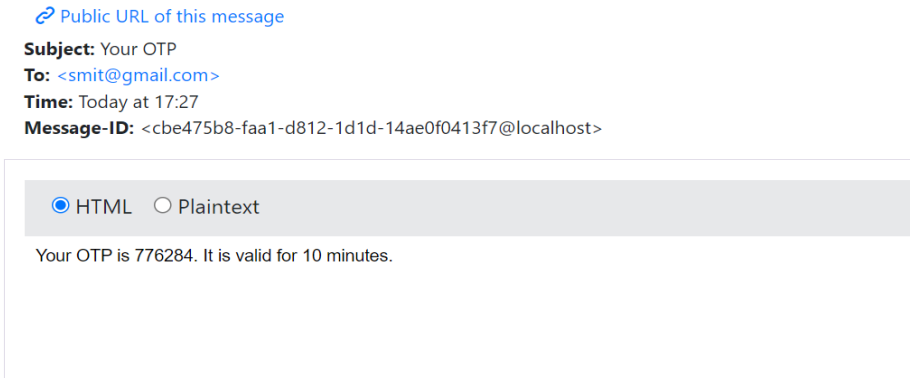




OTP Verification:



OTP Receive Ethereal Mail:



This is Login in From The Chrome Browser

History

Date	IP	Browser	OS	Device
6/27/2024, 6:01:51 PM	127.0.0.1	Chrome	Windows 10.0	Desktop
6/27/2024, 6:11:35 PM	127.0.0.1	Chrome	Windows 10.0	Desktop
6/28/2024, 11:09:38 AM	127.0.0.1	Chrome	Windows 10.0	Desktop
6/28/2024, 3:03:24 PM	192.168.33.5	Chrome	Windows 10.0	Desktop
6/28/2024, 3:07:10 PM	192.168.33.5	Edge	Windows 10.0	Desktop
6/28/2024, 3:09:34 PM	192.168.33.5	Edge	Windows 10.0	Desktop
6/28/2024, 3:23:26 PM	192.168.33.5	Chrome	Windows 10.0	Desktop
6/28/2024, 3:24:20 PM	192.168.33.103	Chrome	Linux	Mobile
6/28/2024, 3:26:44 PM	192.168.33.103	Chrome	Linux	Mobile
6/28/2024, 5:27:36 PM	192.168.33.5	Chrome	Windows 10.0	Desktop

This is login in from the edge browser

History

Date	IP	Browser	OS	Device
27/6/2024, 6:01:51 pm	127.0.0.1	Chrome	Windows 10.0	Desktop
27/6/2024, 6:11:35 pm	127.0.0.1	Chrome	Windows 10.0	Desktop
28/6/2024, 11:09:38 am	127.0.0.1	Chrome	Windows 10.0	Desktop
28/6/2024, 3:03:24 pm	192.168.33.5	Chrome	Windows 10.0	Desktop
28/6/2024, 3:07:10 pm	192.168.33.5	Edge	Windows 10.0	Desktop
28/6/2024, 3:09:34 pm	192.168.33.5	Edge	Windows 10.0	Desktop
28/6/2024, 3:23:26 pm	192.168.33.5	Chrome	Windows 10.0	Desktop
28/6/2024, 3:24:20 pm	192.168.33.103	Chrome	Linux	Mobile
28/6/2024, 3:26:44 pm	192.168.33.103	Chrome	Linux	Mobile
28/6/2024, 5:27:36 pm	192.168.33.5	Chrome	Windows 10.0	Desktop
28/6/2024, 5:34:40 pm	192.168.33.5	Edge	Windows 10.0	Desktop

Mobile Login: It will not allowed to login in other time except between 10 AM to 1 PM