10.4HD

Password Authentication in Node.js

In this assignment, I have implemented a password authentication system into the website that I developed for the Distinction task. As such, this website has a more cohesive structure, while each webpage that is actually relevant to the password authentication system contains a description of the methods used to produce the relevant aspect of the system.

To develop this password authentication system, I utilised a variety of methodologies to ensure robust security and functional efficacy. The Express framework served as the foundational architecture of this website. I used Express throughout to facilitate the management of incoming requests from users and the dissemination of appropriate responses. Express’ built in method also allowed me to build a number of routing mechanisms for each section of the application and to serve different purposes, such as post and get requests for the login and registration pages.

For session management, I also used the Express framework. This component allowed me to utilise the built-in digital authentication mechanisms in this framework by providing methods to allocate a unique access token to users upon login. These tokens enable the user to navigate the application seamlessly, without the need for repetitive authentication processes.

In addressing password security concerns, I utilised bcrypt. This cryptographic library provided strong encryption functionality. Prior to storing passwords within the database, bcrypt is utilised in each relevant route to transform inputted passwords into cryptographically secure hashes. As such, even in the event of a security breach, the password that is viewed is not usable.

Through the integration of these methodologies—leveraging Express for request handling and session management, and bcrypt for password encryption—I developed a resilient password authentication system. These measures collectively ensure that the application operates securely and efficiently, affording users a seamless experience while safeguarding their private data.