Yuka for Stocks

Login Security

Team 5

Kyle Rivera

Capstone Project Spring, 2025

The University of West Florida

3/28/2025

CIS4592 - Capstone Project

Instructor: Dr. E.L. Fridge

In this report you will see the measures we took to implant security measure for our login in feature of our application. Some of the things we considered that needed to be addressed was securing data in transit as they are inputting there credentials to log into their account and send it to our backend to verify they are who they say they are. Another one is securing data at rest so we need to make sure that where we store the data is secured. Permissions are another one to make sure our site can tell if someone is an account holder or just a visitor. The last one we considered was making sure API keys and API authorizations are mask so it will not display for people to see with developer tools.

#	Security Concern	Security Implementation
1	Secure API key	-Backend hosted through Render to avoid dev tools from finding API key in requests -We use gitignore to ensure our .env files that hold all our API keys do not get pushed into the repository, which secures our API keys from being viewed to public.
2	Securing Data at Rest	-Using Firebase to store our data which has its own Authentication and security rules to protect our data we will store there.
3	Securing Data in Transit	-Firebase Hosting forcibly redirects all HTTP requests to HTTPS, ensuring that users always access the site securely -HTTPS encrypts all data sent between the user's browser and Firebase Hosting servers protects from Man-in-the-middle, Eavesdropping and Data Tampering attacks

4	Authentication	-Using Google Authentication which saves us from storing username and passwords. They also add an additional security because they have their own Multi-Factor Authentication. We can log into Firebase which is a part of Google gives us a Centralized Account Control where we can manage accounts.