SECURING AN E-COMMERCE WEBSITE

CSE3501 – Information Security Analysis and Audit

by

18BCI0116 - Deep Golani

18BCI0122 - Vaidit Gautambhai Patel

18BCI190 - Laksh Gupta

18BCI0197 - Nimish Shah

School of Computer Science and Engineering

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

October 2020

Contents

Chapter 1

1.1 Introduction

We plan to build an e-commerce website and then secure it using the many security methods we have learned in this course.

1.1.2 Website purpose

The project allows users to check the inventories of nearby shops. Easyshop is the place where customers can view their day to day products and order them online instead of going there physically. In this project, operators enter the Website and buy some product, we then look at their cart and compare it to all nearby shops available, we then generate the bill for every shop and allow the customer to choose which shop they want to order from. Supervisors and admin will have separate login ID and pin through which they can access their account to modify their inventory, which can be done in real time giving the customer an accurate view of their inventory.

1.1.2 website scope

We wish to show the users all the shops close to them and allow them to search for the products that they want through the options provided on our website. They should be able to create a cart that contains all the items they wish to buy. Then the website should show the user a comparative analysis of the prices at each shop and the approximate final price for the whole cart for every shop available nearby. The website should also notify the user if a product is not available.

There is also a feature for the customer to send their list to the shop so that the shopkeeper can keep the items ready so that the customer can only pick the groceries quickly.

1.2 Problem Statement

Creating a Securing e-commerce website

Chapter 2

2.1 Literature Review

Cyber Security; Issue and Challenges in E-Com

E-Commerce refers to the exchange of goods and services over the Internet. The shopping through e-commerce has penetrated all segments of goods ranging from groceries to electronic goods and even vehicles. Rapid growth in mobile computing and communication technologies has facilitated the popularity of e-commerce. The main impediment in growth of e-commerce is cyber fraud and identity theft. Hackers are people who carry out cybercrime. Hence, poor security on e-Commerce web servers and in users computers is a core issue to be resolved for rapid growth of e-commerce. This paper provides directions for e-commerce security so as to improve customer confidence in e-commerce shopping.

E-Commerce Security Challenges: A Taxonomy

With the rise of the Global Economy, and with an ever-expanding level of purchasers doing their business fundamentally by means of on the web or cell phones, electronic trade, internet business, is quickly being viewed as the best approach worldwide at the bit of a catch. Subsequently, building up a successful Web based business model is getting essential for any cutting edge business. In any case, an organization must address diverse new security challenges and be sure to keep up the best expectations of web based business security, to ensure both themselves and their clients. An inability to hold fast to severe internet business security can bring about lost information, traded off exchange data, as well as the arrival of the client's monetary information. This can lead to lawful and budgetary risk, just as a negative effect on the organization's notoriety. These new security challenges are the consequences of the utilization of the new innovation and correspondence medium, and the progression of data from big business to undertaking, from big business to purchasers, and furthermore inside the undertaking. This paper presents the distinctive innovation and calculated parts of the web based business as a rule, and recognizes and orders the various sorts of security challenges confronting online business organizations specifically.

Y. Wen, C. Zhou, J. Ma and K. Liu, "Research on E-Commerce Security Issues," 2008 International Seminar on Business and Information Management, Wuhan, 2008, pp. 186-189, doi: 10.1109/ISBIM.2008.168.

This paper deals with various security issues faced by ecommerce websites that are hosted on public networks. The core issue discussed is security of E-commerce transactions and two aspects of it, which are the security of the system and the security of information. The two major issues discussed are Computer network problems and The security issues of business transaction. There are also some proposed security control requirements at the process of E-commerce transaction. They are: The validity of the information, The confidentiality of information transmission, The integrity of the transaction information, The integrity requests when storing the data should prevent illegal destruction or change on the site, Non-repudiation of information, The authenticity of the traders identity. The two traders do indeed exist, not fake, The information can not be amended. The message on the network can not be modified.

The Study of E-Commerce Security Issues and Solutions

Sangeetha M K Prof. Dr. Suchitra R Jain University, Bangalore Jain University,Bangalore

This paper deals with privacy and security issues faced by modern ecommerce websites and how these issues faced by the customers are restricting them from engaging more with these websites. It also states that Web e-commerce applications that handle payments have more compliance in issues, are at increased risk from being targeted than other websites and there are greater consequences if there is data loss or alteration. The paper then also goes on to discuss web security in general and how rapidly growing e-commerce is a challenge online security as a whole.

Kefa Rabah , 2006. Implementing Secure RSA Cryptosystems Using Your Own Cryptographic JCE Provider. Journal of Applied Sciences, 6: 482-510.

Encrypting and decrypting data: Encryption works at the byte level, so almost anything can be encrypted. Once you have a key and a cipher, you're ready to go. It should be noted that the same algorithm must be used for both the key and cipher. You cannot have a key initialized with DES and a cipher initialized with RSA. The Cipher object uses the same methods to encrypt and decrypt data, so you must initialize it first to let it know what you want done with the data:

rsaCipher.init(Cipher.ENCRYPT_MODE, publicKey); //Initializes the Cipher object.

This call initializes the Cipher object and gets it ready to encrypt data. The simplest way to encrypt data is invoking the doFinal method on the Cipher object passing in a byte array:

byte[] data = Hello World! .getBytes();//Calculates the ciphertext with a plaintext string.

byte[] result = cipher.doFinal(data);

The result will now contain the encrypted representation of the passed-in data. It's just as easy to decrypt the same data. But before we can do that, we must reinitialize the Cipher object and get it ready for decryption

Design and implementation of an improved RSA algorithm

Authors: Yunfei Li ; Qing Liu ; Tong Li

Publish in: 2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT)

DOI: 10.1109/EDT.2010.5496553

This paper aims at speeding up RSA decryption and signature. The performance of RSA decryption and signature has a direct relationship with the efficiency of modular exponentiation implementation. RSA 3072 is equal to 128 bit symmetric and 2048 is equal to 112 bit symmetric then 128-112= 16 and 2^16= 65,536. This paper proposes a variant of RSA crypto systems by reducing modules and private exponents in modular exponentiation. The experimental result shows that the speed of the decryption and signature has been substantially improved and the variant can be efficiently implemented in parallel.

2.2 Objectives

2.2.1 Website Functionalities

- If you are a user then there is no need to login. You can directly search your wish list.
- On the homepage, there will be a list of shops and specific items that are purchased more often and recommended by users.
- If the user clicks on a particular shop, then the user will be redirected to the shop page. On that page, users can see all details about that shop like location, sale, discount, contact details.
- Users also can use the search bar to add products in cart.
- There will be a page for your cart also. There will be a list of all items that you have selected.
- Then based on the algorithm we will give the best shop to buy groceries
- There will be a login for the shopkeeper to update the inventory.

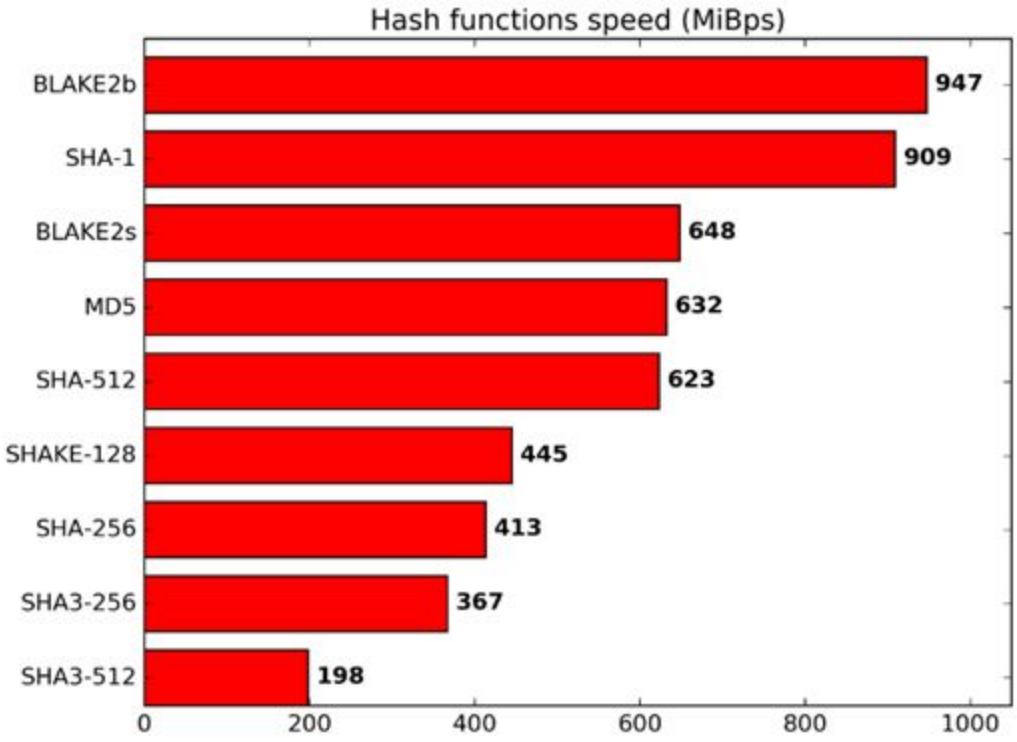
- There will be an add product page for admin. Via this page admin can update their inventory

2.2.2 Security Functionalities

- The passwords for the users are stored in an hashed manner before being sent to the firebase database which then encrypts it before storing.

- All the requests made are first encrypted and then sent so then any attacker cannot access the data in transit, and even if they intercept it will be useless for them as they will not be able to decipher it.

- We use new hashing algorithms like blake2b instead of SHA as they are faster and more secure.
  We updated our hashing algorithm from sha256 to a faster and secure blake2b hashing algorithm. While both have the same algorithmic time complexity, runtime complexity of blake2b is far more better than sha256. You can see that in picture below,



Src : https://blake2.net/

- We also use RSA 3072 bit encryption which is better than standard encryption algorithms.
  The public and private keys used in the RSA algorithm are created with “ssh-keygen” which is industry standard for cloud computing. Sowe can ensure the robustness of private keys that will be used in our application.

- The site hosted is also on HTTPS which is more secure than HTTP. HTTPS is not stateless protocol, so it can be used to store user sessions across the complete web application.

- The site is immune to most common attacks like Cross-Site Scripting (XSS), SQL injection, path traversal, local file injection and distributed attacks like DOS and DDOS.

- Upon checking the website on “Google Lighthouse” , the app scored 100/100 in SEO

Chapter 3

3.1 Methodology

The main aim of our project is to secure the web app as much as possible. The algorithms we are using are pretty standard, but the way we are sending the data on the server is a bit different. So, basically we are encrypting the data on the client side itself (it will be done by the browser locally) and then send the data directly. So,

{

user:”Tanish”

}

Normally, data would be sent like this, but we encrypt it and it will be sent like this,

{

payload:”Qbd3r=f” // Some base64 encoded string.

}

On decoding the object would be, { { user:”Tanish” } }.

Along the client side encryption, we are also deploying server side encryption with the help of a one of the newest hashing algorithms BLAKE2b which is 512 bit in length.

Steps:

Client,

Form-data -> RSA encryption with 3072 bit key -> base64 encoding -> send the form data

Server,

Received base 64 form data -> decoding base64 to uint8 buffer -> RSA decryption -> received the form data in the backend controller (can do operations on it)

3.2 System Design

3.2.1 Website design

Home Page of the website:

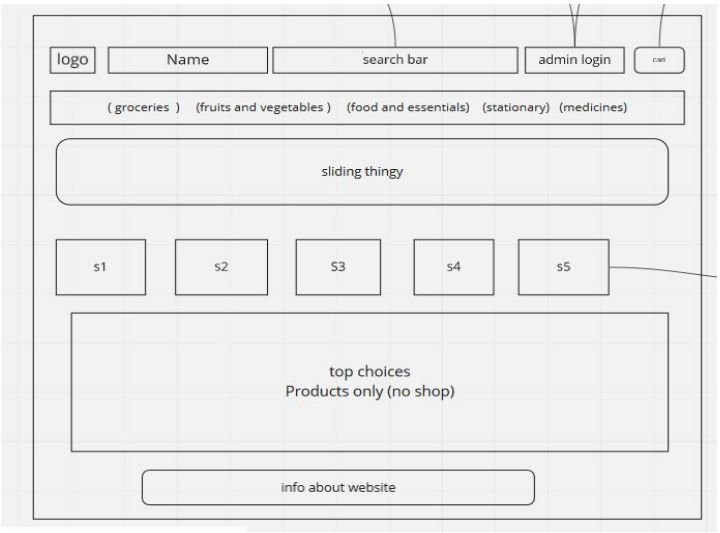


Fig. 3.1 Home Page

Product popup page:

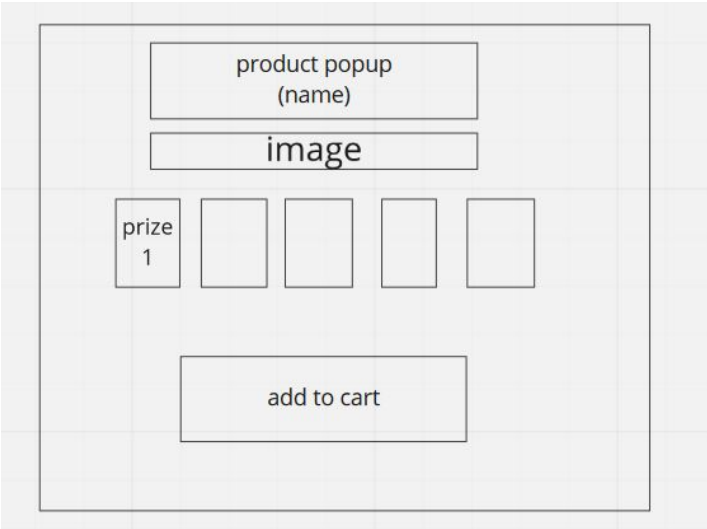


Fig. 3.2 Pop-up Page

Shop page:

Fig. 3.3 Shop Page

Cart page:

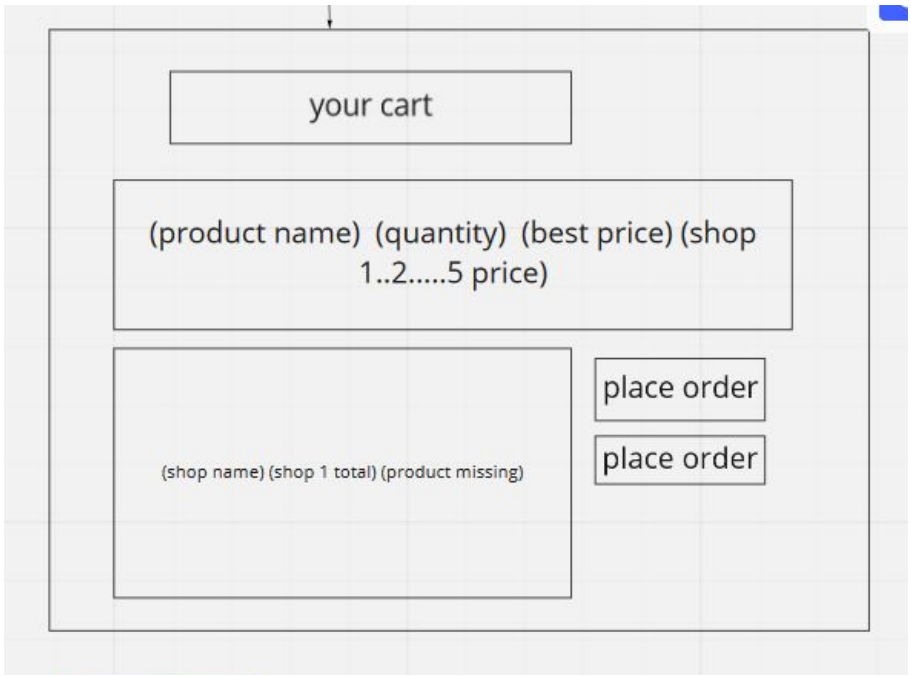


Fig. 3.4 Cart Page

Search Page:

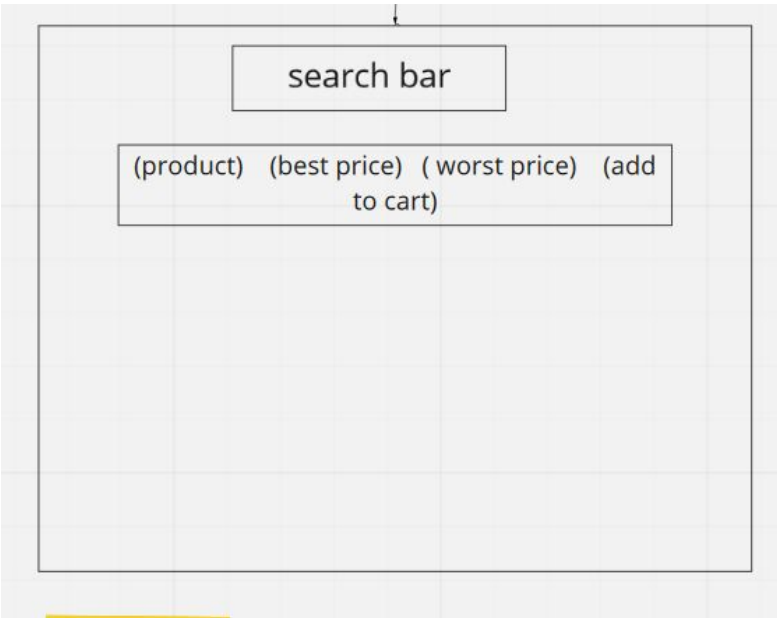


Fig. 3.5 Search Page

Admin Login:

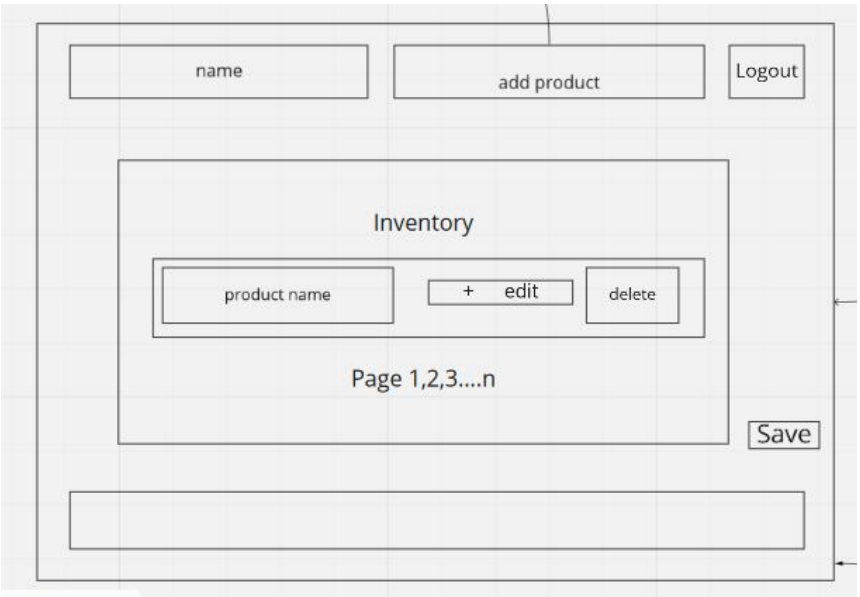


Fig. 3.6 Admin login Page

Admin edit inventory page

Fig. 3.7 Admin Panel Page

Overall design

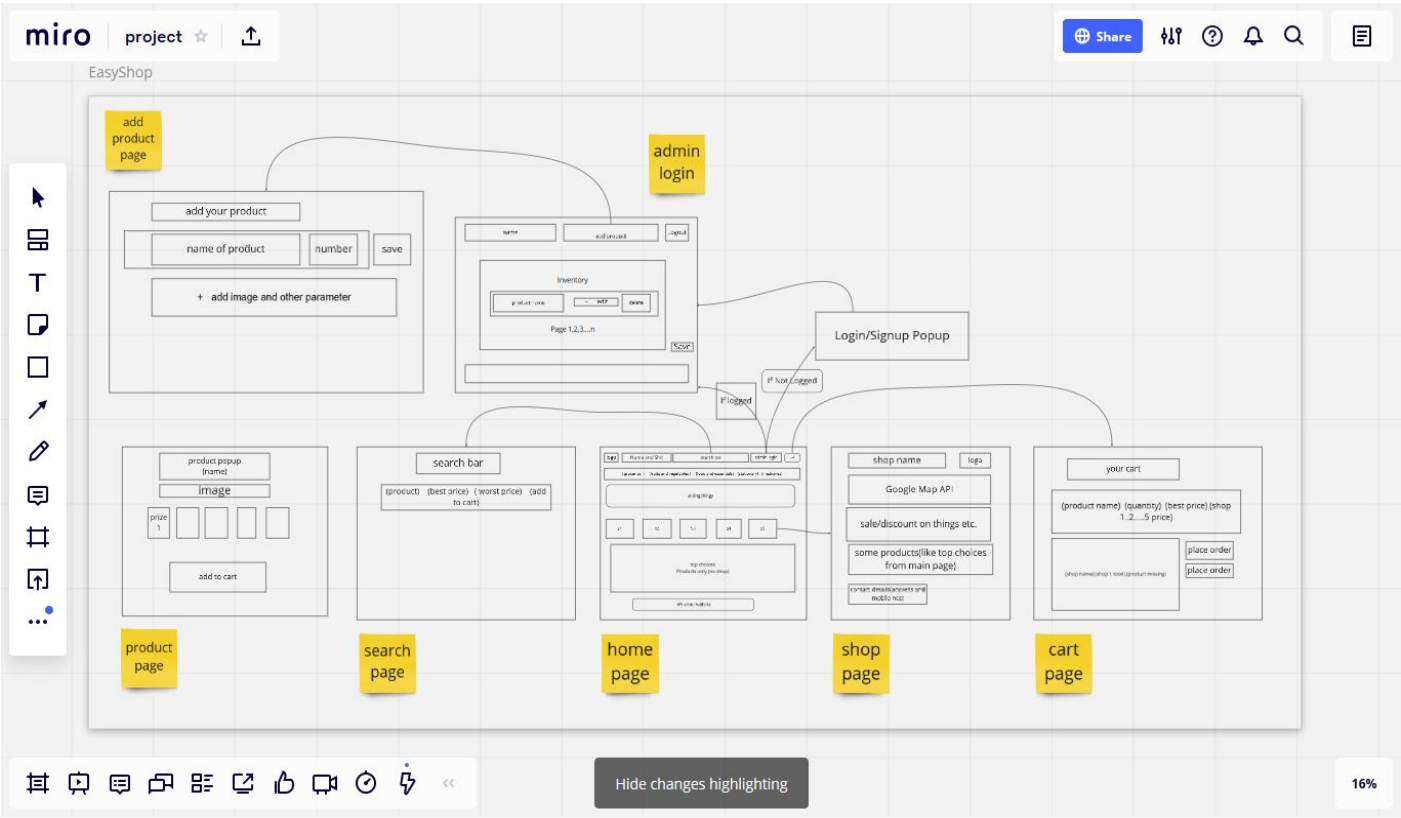


Fig. 3.8 Overall Website Flow

3.2.2 Security Design

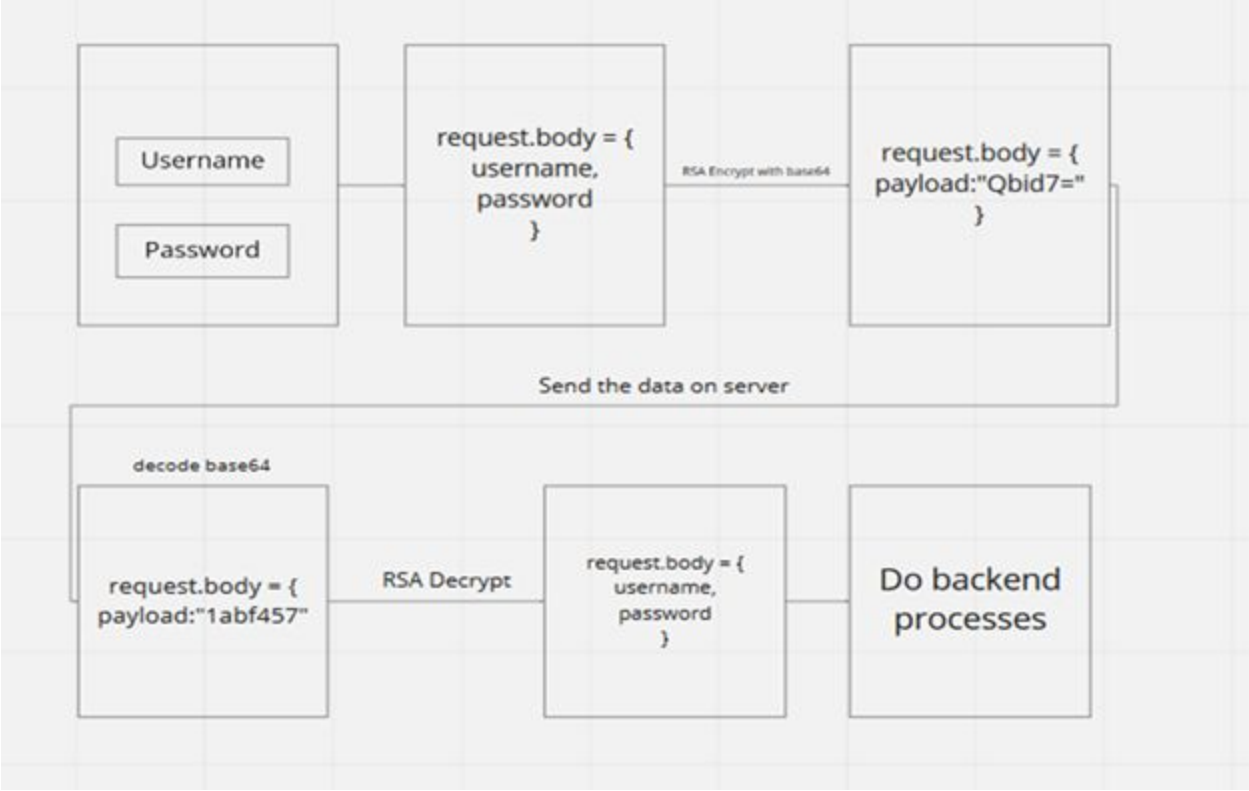


Fig. 3.9 Security flow of the website

Chapter 4

4.1 Results

4.1.1 Website

Link: http://easyshopindia.herokuapp.com/

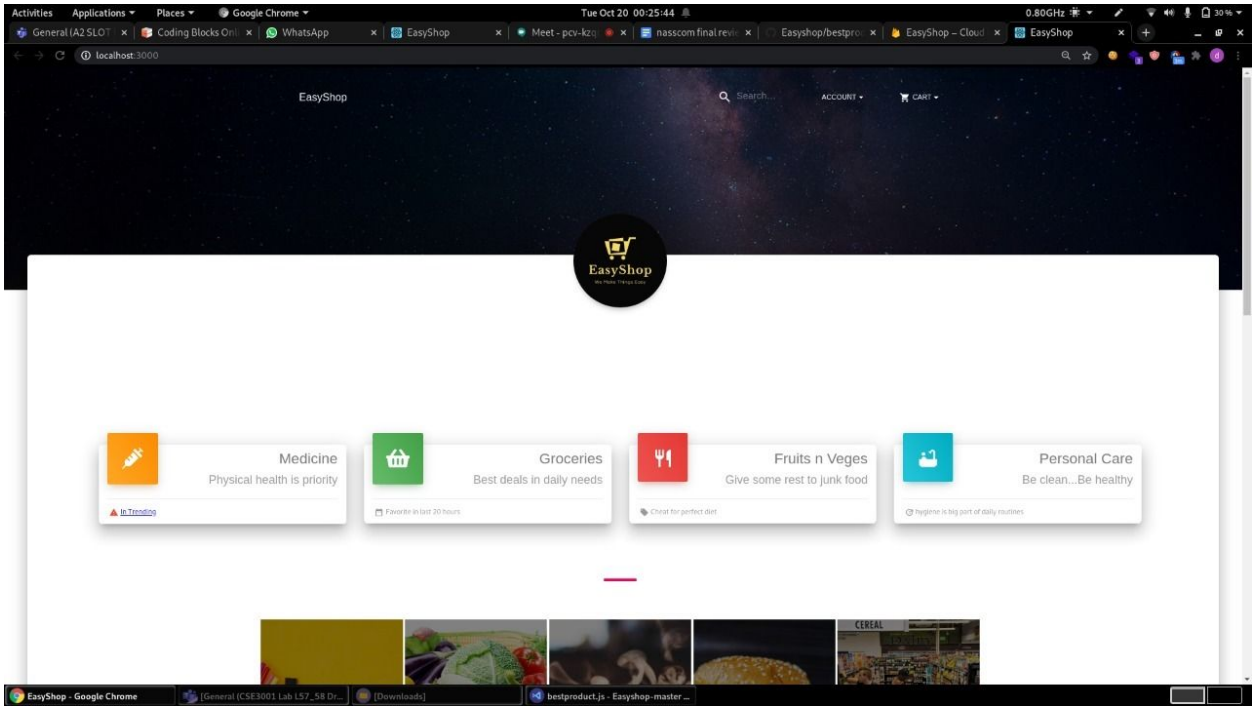


Fig. 4.1 Home page

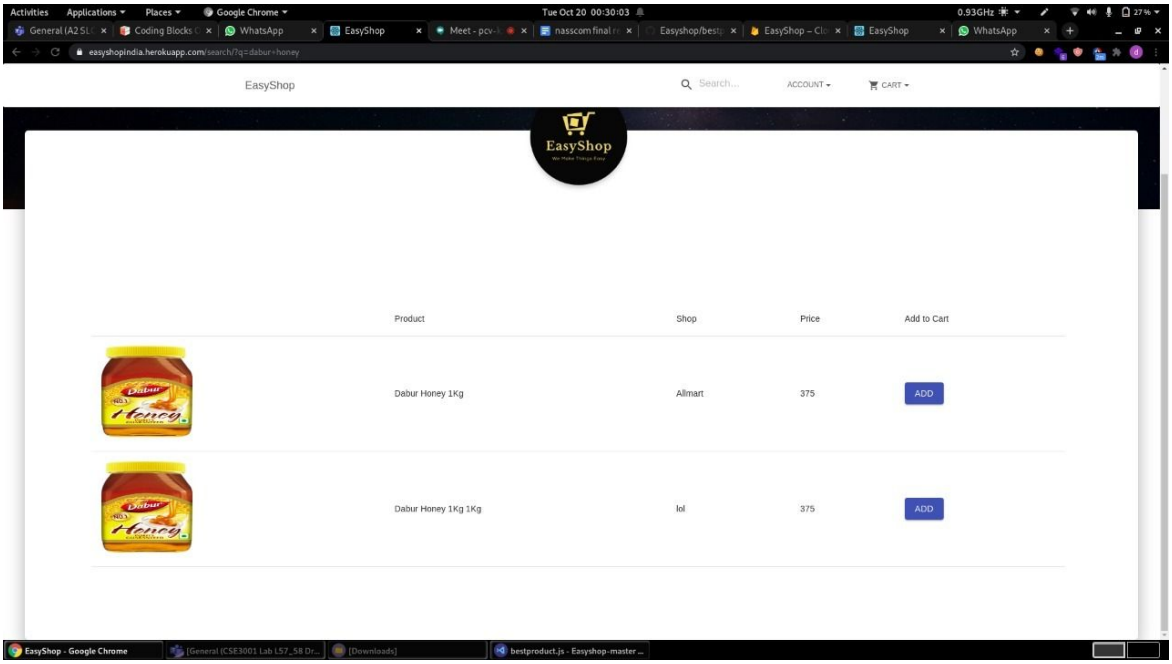


Fig. 4.2 Search page

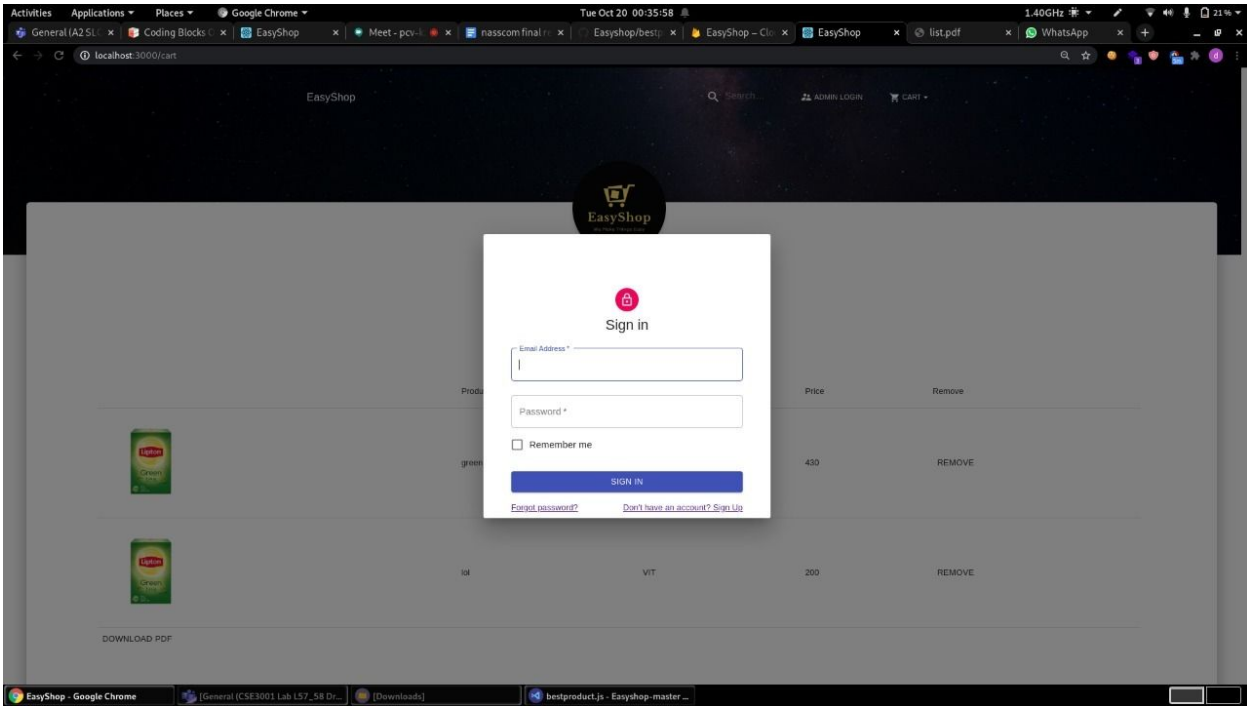


Fig. 4.3 Admin Login

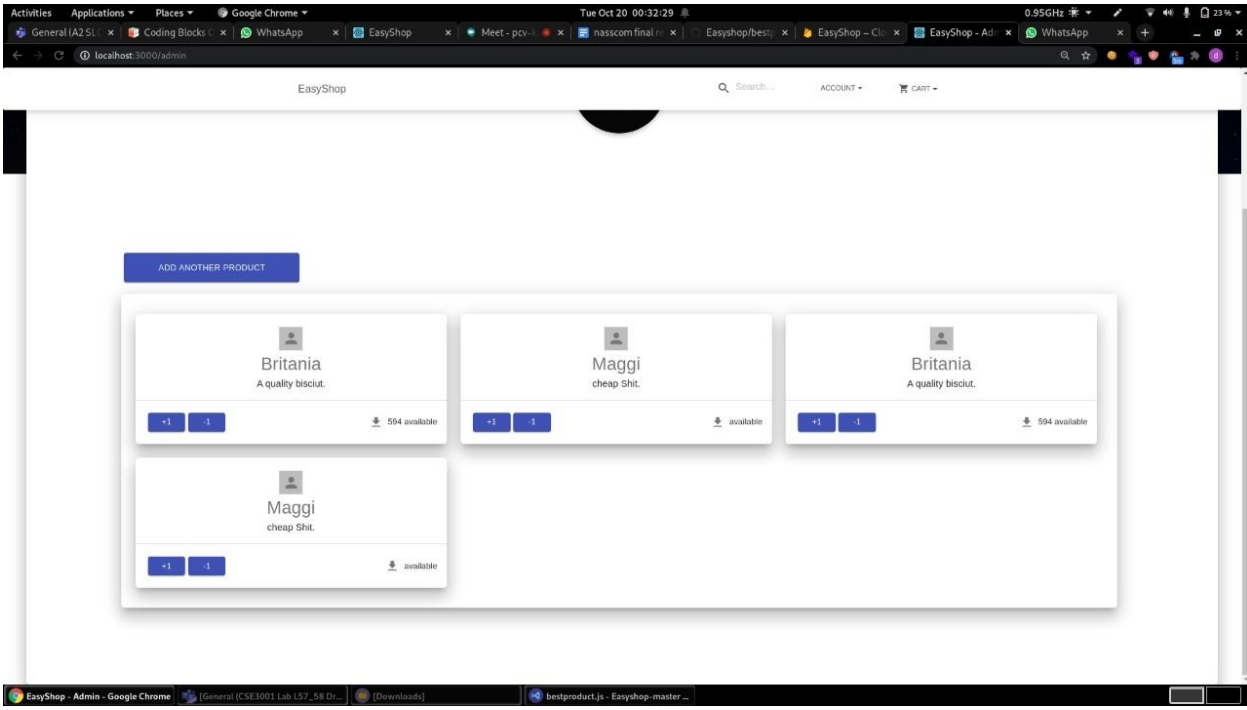


Fig. 4.4 Admin Inventory panel

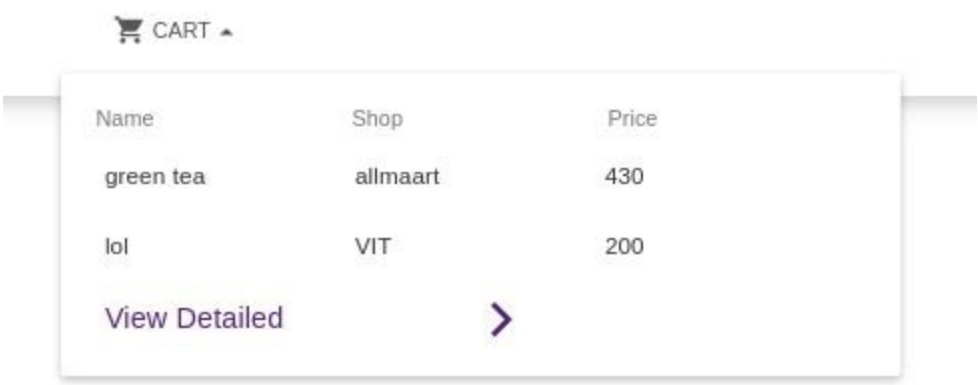


Fig. 4.5 cart

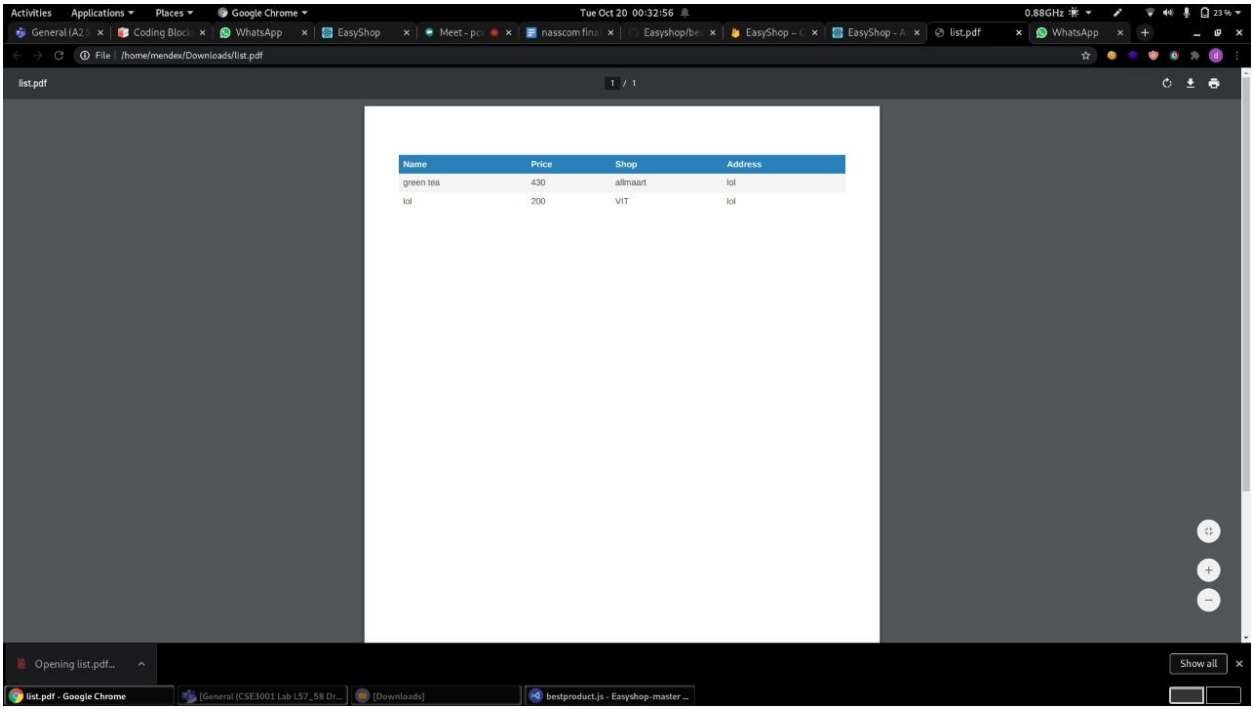


Fig. 4.6 Checkout

4.1.2 Security Aspects

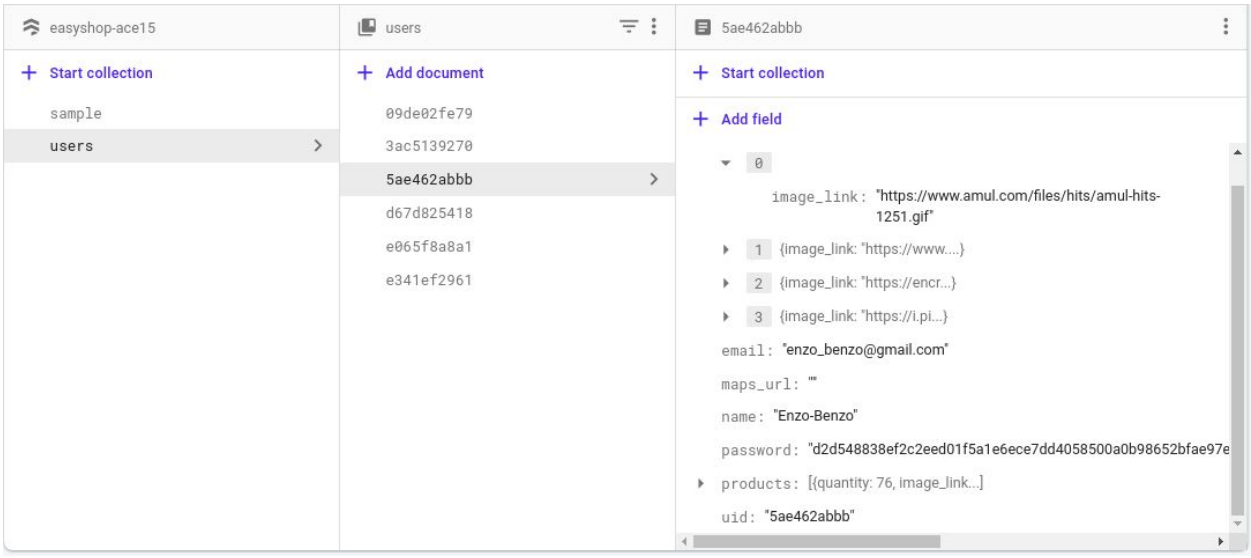


Fig. 4.7 Hashed Password Stored in Database

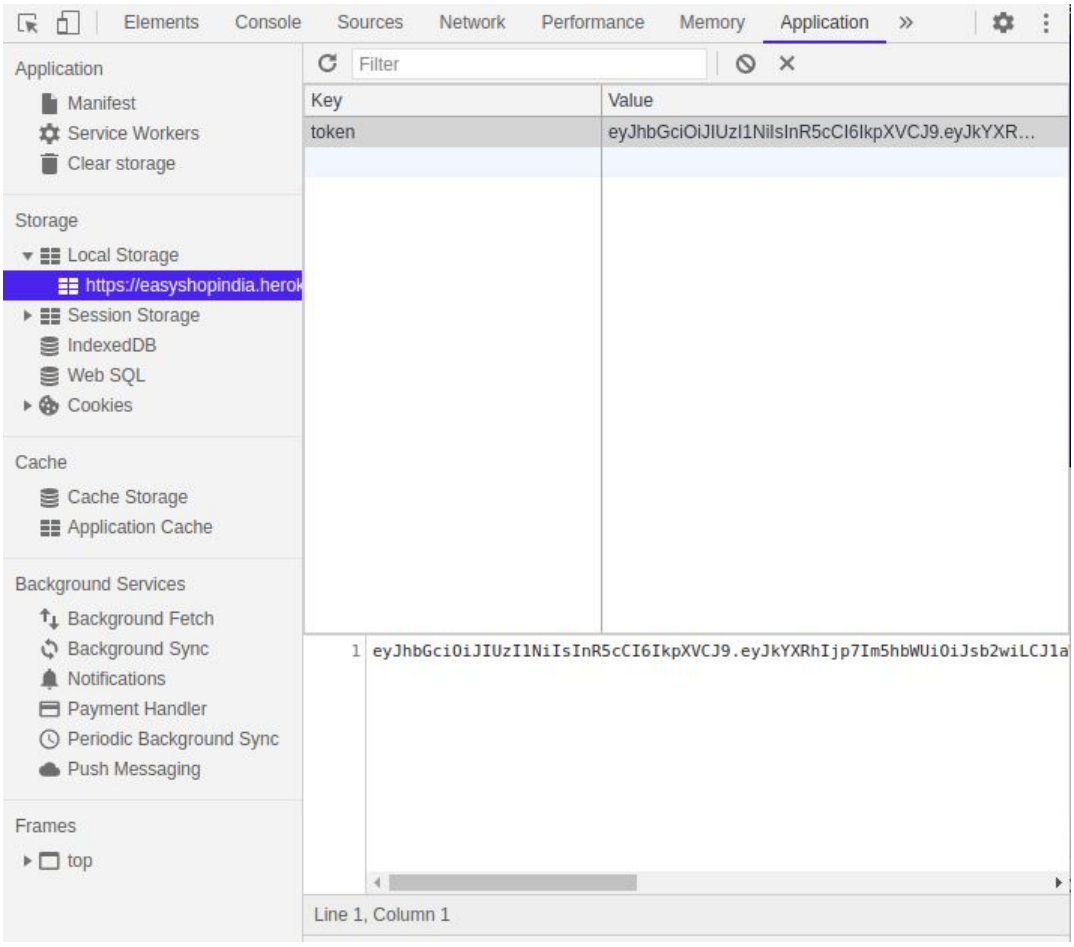


Fig. 4.8 Encrypted JSON web Token

4.2 Testing

4.2.1 Website Testing

- Google Lighthouse

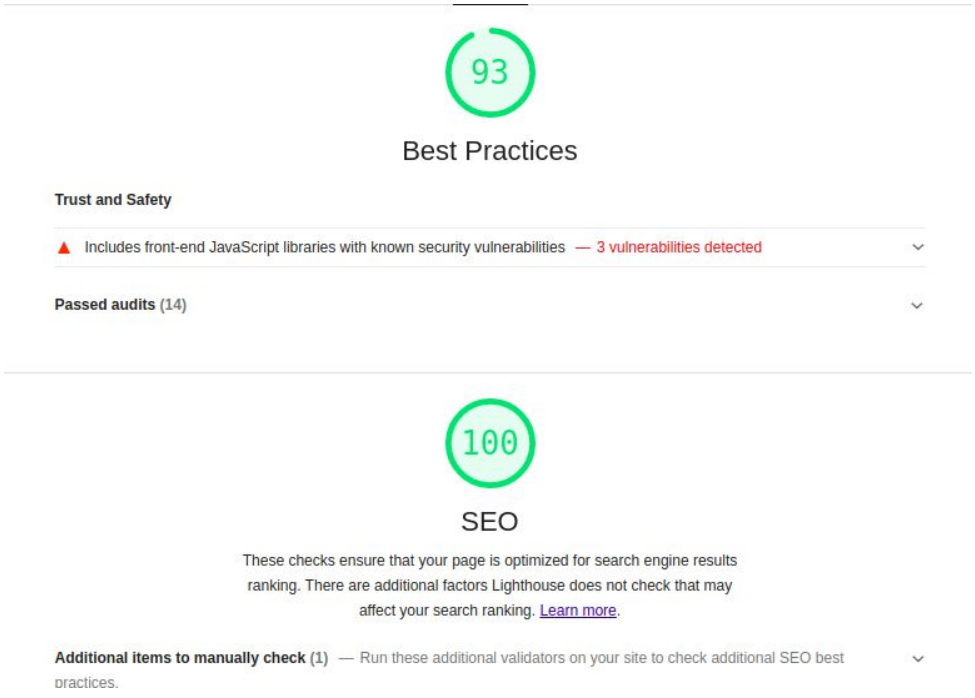


Fig. 4.9 Google Lighthouse testing

4.2.2 Security Testing

- Burp Suite Intercept testing

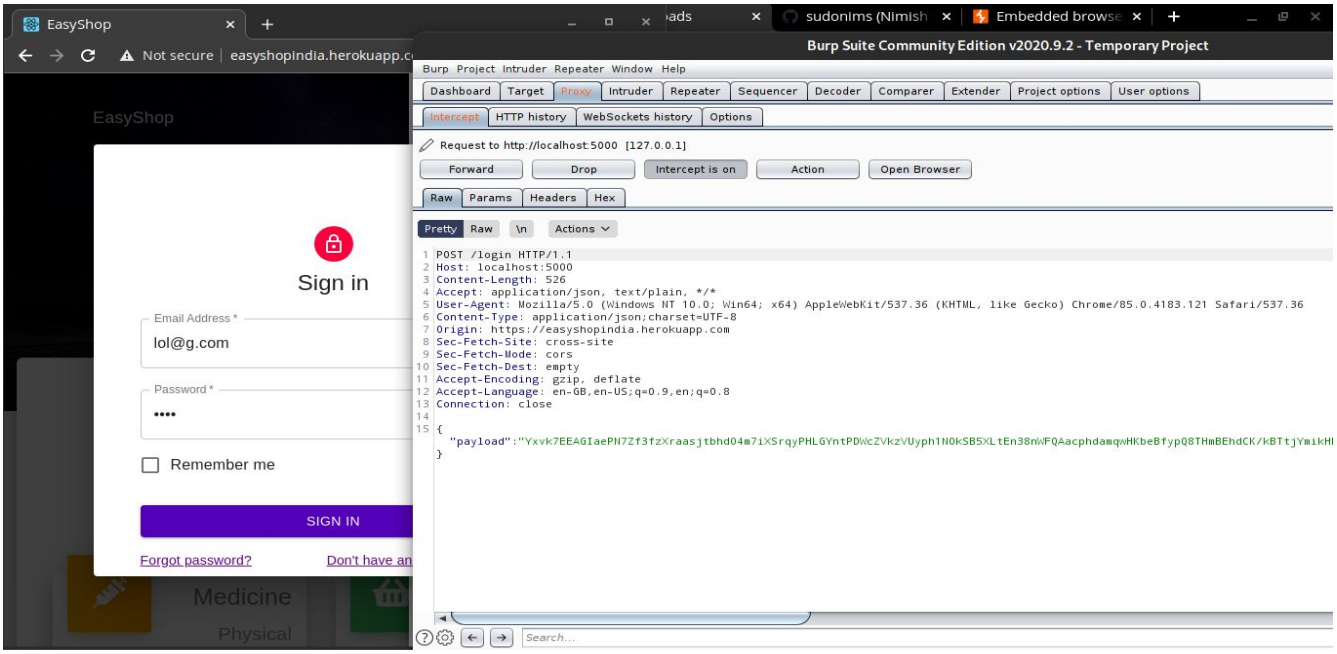


Fig. 4.10 Burp Suite intercept

- Nessus testing

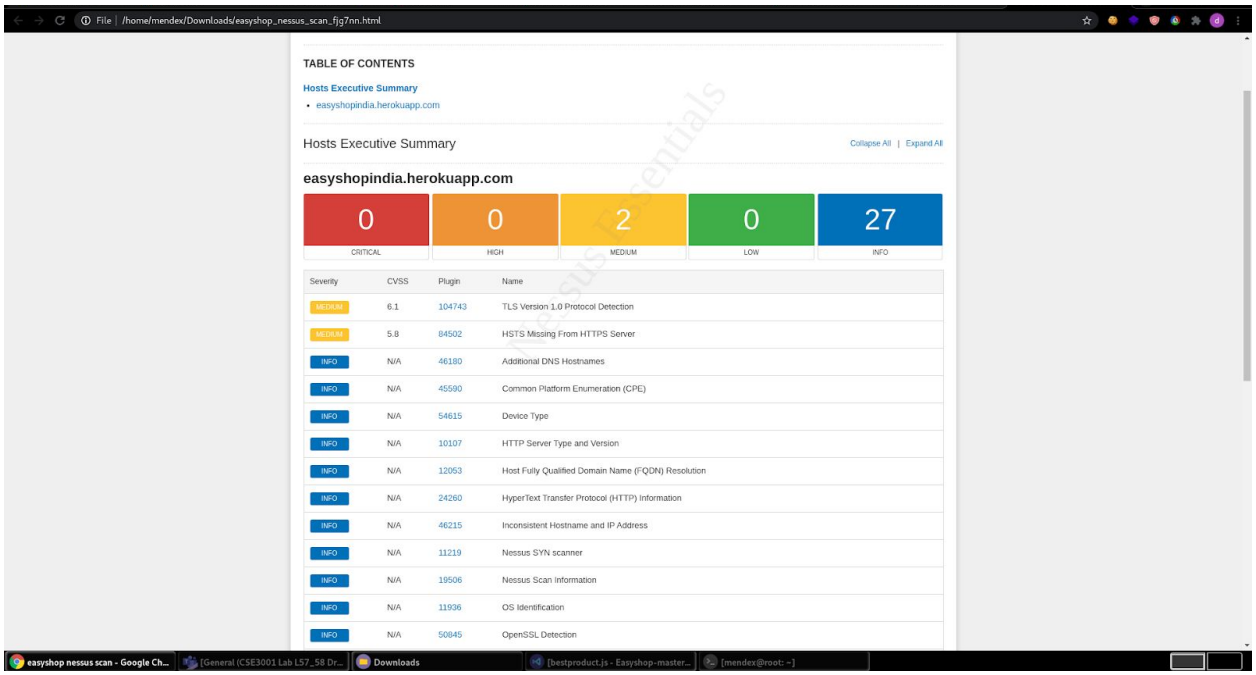


Fig. 4.11 Nessus test

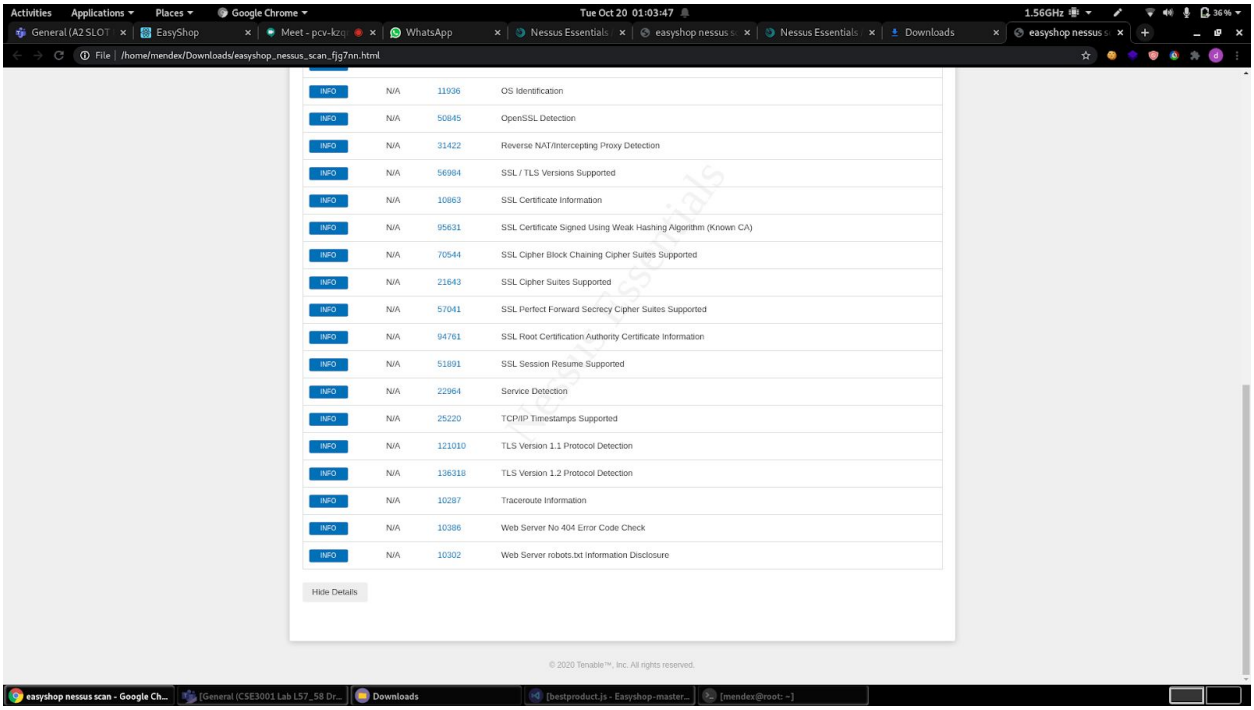


Fig. 4.12 Vulnerabilities listed by Nessus

Chapter 5

5.1 Conclusion

This project has successfully made a web app for the given problem statement. And has met most of the requirements stated at the beginning of the project.

The language used is HTML, CSS, and JS and the database used is Google Firebase. It is a web application useful for any person looking to buy groceries. The application is flexible, easy to use with interactive UI.

So the e-commerce website we have developed is immune to most common web attacks namely: Cross-Site Scripting (XSS), SQL injection, path traversal, local file injection and distributed attacks like DOS and DDOS. and we have also successfully tested it using many tools like Google Lighthouse, Burp-suite and Nessus.

5.2 Future scope

Future work that can be implemented with the project is integration of more shops and an option for home delivery done by the shop. As in this project, we have developed a web app that facilitates consumers to buy goods from small local retail shops.

An android/IOS application can also be developed as it will help us reach a wider market as surveys show most Indians prefer to use an app over a website for shopping online.

Coming to security aspect, not many web applications currently in the market have adapted to the method that we've invented to make client-server communication more confidential with more integrity.