SSDI TERM PROJECT

49erskart

TEAM MEMBERS (TechGiants)

1. Arjun Manevannan
2. Neela Ayshwaria Alagappan
3. Nivedita Veeramanigandan
4. Srinath Muralinathan
5. Balasundaram Avudai Nayagam

ABSTRACT:

The purpose of this paper is to document the design and development of a shopping e-commerce web portal 49erskart. The website will serve as a hub for the student community of UNCC to buy and sell their products with relative ease with the given assurance of safety. We have developed the web stack using HTML, CSS, Bootstrap, jQuery templates, Node.js and MongoDB. We have used a NoSQL DB for this purpose. This document outlines the design, development and the security aspect of the application and its usability and use cases in the real world.

INTRODUCTION:

It has been difficult to get hold of the right home and study furnishings when moving in as a student. The problem also extends when moving out, with the student scrambling to sell the products he owns before he must move out. The problem is only worsened when there's a time limit before he must move out, forcing the student to give away his possessions for free or a very low price.

There are other broad issues, with privacy and safety. Usually, when selling the student is forced to give their private phone number or email address in order to let people contact them. As a student, it is difficult to move into a new place and set up with the necessary home setup before school starts. With local retailer prices typically out of a student's spending budget the time a student takes to settle down for school can be reduced drastically. This is what our application strives to change.

MATERIALS AND METHODS:

This website aims to solve this issue at a smaller scale. We narrowed our scope to just focus on the UNCC community providing new students as well as existing students a better, reliable purchase experience to set up their living spaces. The website aims to benefit new incoming students as well as students who are moving out by providing a quick way to sell products. This benefits students, especially the ones living off campus as this helps them get the most money back from their used furniture.

SECURITY

Since this will be used primarily by the students, we have prioritized security and privacy controls when building this application.

- **SQL INJECTION**: SQL Injection is a security vulnerability that helps a hacker inject malicious SQL queries to the database. The impact of the attack varies from being able to view data that the user isn't supposed to see, or worse, allows the user to write/delete data present in the database. The actions arising from such scripts can be dangerous to the entire application's stability, let alone user privacy. The common intention for such an attack can be retrieving sensitive data, subverting application logic, examining databases among others.
- **CROSS SITE SCRIPTING**: Refers to an attack where a malicious script is inserted on a secure website. Without the right handlers, the hacker can successfully run the script on the website. The browser in no way will be able to detect the script as a malicious one thus executing it. The script usually targets the session, cookie and other sensitive stuff to scraping off sensitive information.

ADDRESSING SECURITY CONCERNS:

- **Encoding**: Escaping is the process of converting certain special characters into safe characters for the web. The likelihood of certain characters being rendered as HTML when it's not supposed to reduce greatly. We have used 'Embedded Java Templates' (EJS) as a templating engine to get rid of this issue.
- **Input Validation**: Input validation helps us eliminate any intentional scripting attacks on exposed input fields. A hacker might send a malicious script into one of the input fields meant to get user details for selling an item on the platform, the script when processed by JavaScript can start executing on the server if the input isn't validated. We validate every field in the application where we take in user data, before we process them in any capacity.
- **Output Filtering**: Just like encoding mentioned above, filtering is the process of removing unwanted, unsecure characters. We have used filtering as a sanity check to get rid of any unwanted characters and extra spaces (trimming) to make sure the data we want to send is the data we are sending.
- **TLS**: Transport Layer Security is the protocol we have opted for sending and receiving data over the internet. The data is encrypted and securely transmitted, preventing any chances of man in the middle attacks and/or packet sniffing. We have realized the importance of TLS/SSL as failing to encrypt data in transit will invalidate other security measures we have undertaken.
- **Helmet**: Helmet is a module which helps developers set the HTTP headers appropriately. We have used Helmet to hide the platform (node/express, here) that we are running on. X-powered-by http header is responsible for letting the hosting platform know which technology powers the application. Once this is exposed, hackers can use targeted attacks against the platform to compromise it. This has been taken into consideration and implemented accordingly.
- **Brute Force Attacks**: We have addressed hackers brute forcing into the system by preventing logins by IP addresses of more than 100 attempts have been made in the past 24 hours.

PRIVACY

Also, we do use the private information of the seller on the website. When a student is interested in a purchase, we do not divulge the personal phone number to each other. The numbers are encrypted and stored, and the actual phone number is never shared.

DESIGN:

Front End: We have used HTML5, CSS3, Bootstrap libraries and jQuery for handling the user facing part of the application. The layout was designed using HTML/CSS with Bootstrap libraries. The user interaction has been handled by jQuery.

Back End: We have used Node.js with Express for handling business logic for our application. The user inputs are handled through get requests which process them. We have a user session initialized every time a user logs in. The session keeps track of user activities as items are added to the cart.

The /cart route is used to calculate the total of all the items the user is interested in. This is reflected in the final page before the purchase is made.

Payment API: To make the payment process seamless and robust, we have used Stripe API to process payments. This gateway allows us to interact with the users for post purchase validations and log in intimation.

The API also restricts payments by sending an OTP to authenticate the user on their registered phone number before making the purchase.

Database: We have used a NoSQL database for its added flexibility and protection against SQL injection attacks. We have a single collection which stores the user information.

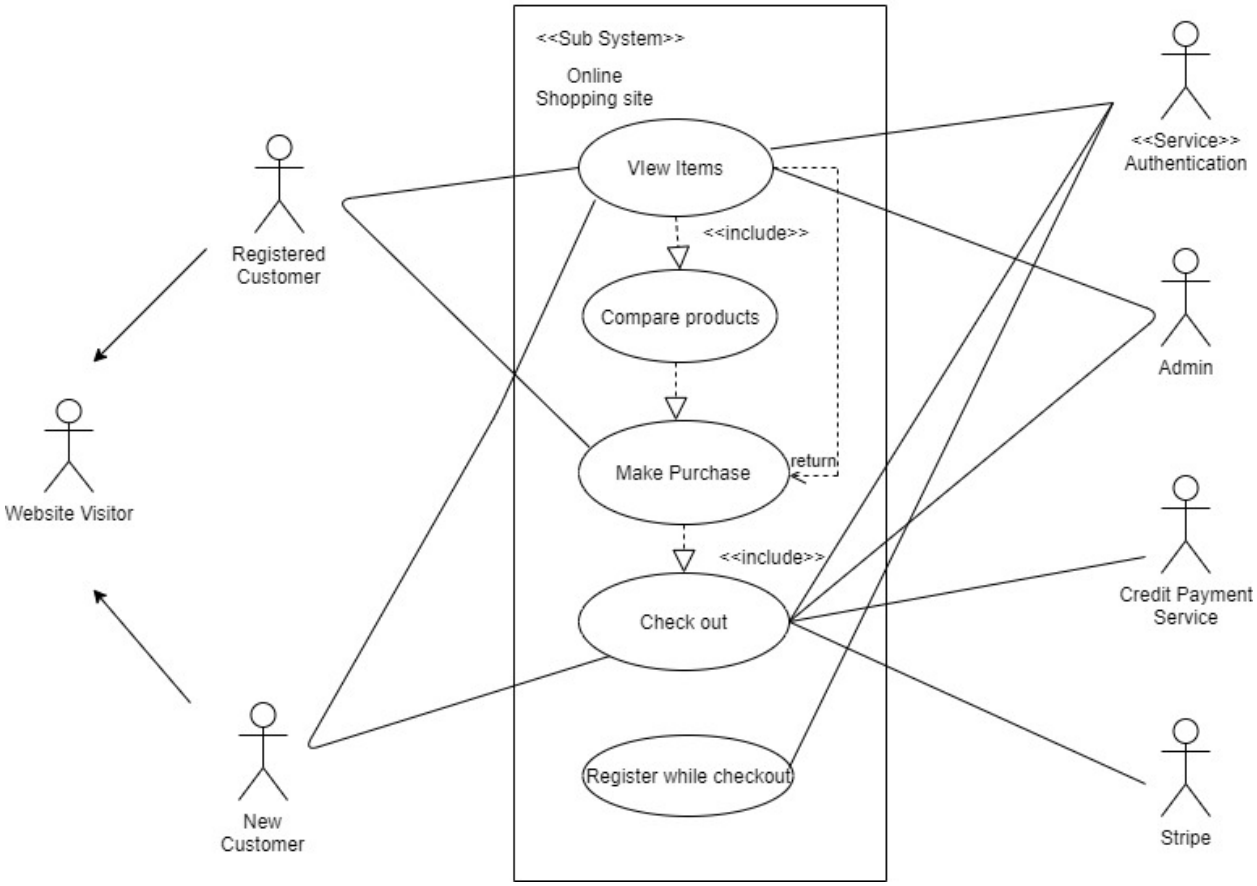
DEPLOYMENT:

We have deployed the application on Heroku, a cloud application platform. The application can be accessed through the URL https://ninerskart.herokuapp.com/.

USE CASE DIAGRAM:

Microsoft Visio Professional 2019 was the tool employed to draw the UML diagrams. Below are the corresponding Use case, Sequence and Class diagram for 49ers Kart application.

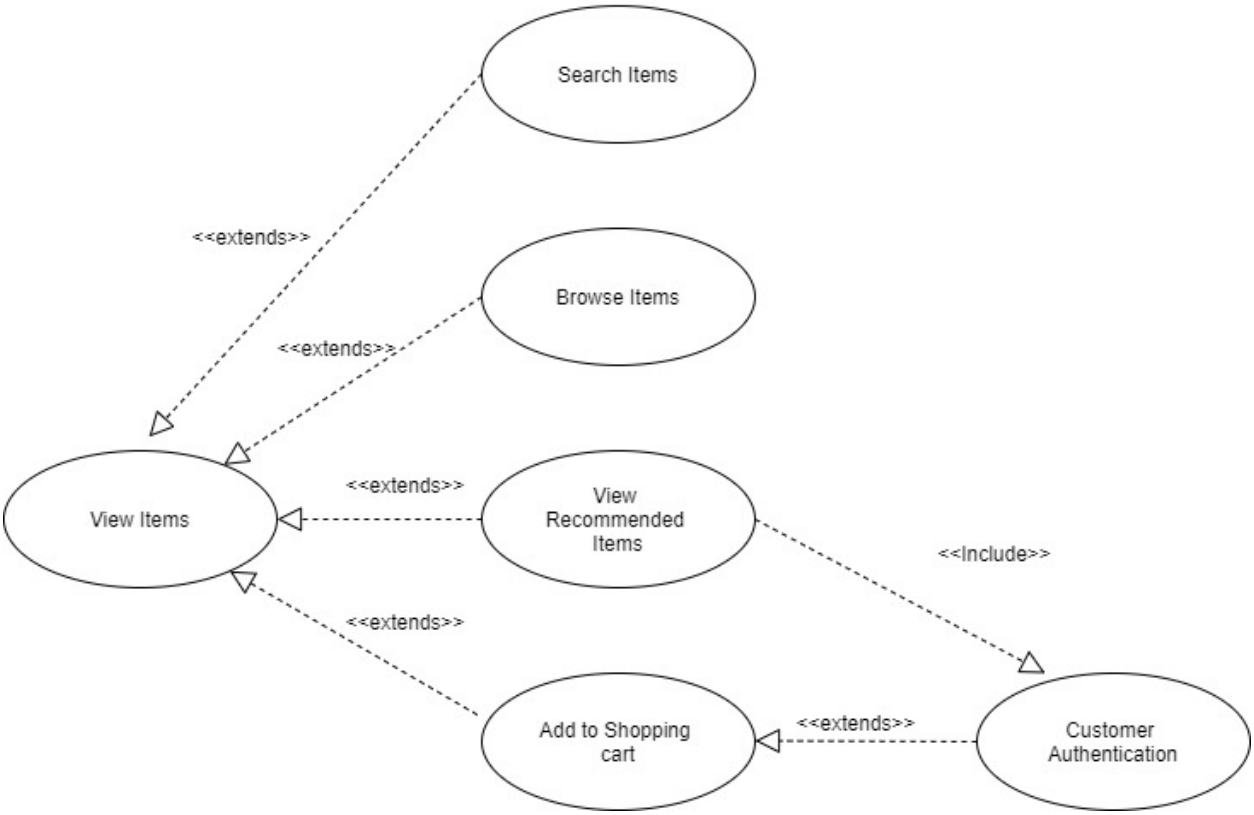
UML DIAGRAM - 49ers Kart



This diagram provides top level use cases for customers who make online purchases using 49erskart. The customers are the actors here. Since each of the customers are provided individual credentials to login and make purchases, both registered actors and new actors are portrayed to show the difference. Each customer has a unique id and is linked to exactly one account. Account owns shopping carts and orders. Customers could register as a web user to be able to buy items online.

The customers can surf through the web application without making a purchase which is also shown as a Website Visitor actor. The customer visits the website, surfs for products in the website, compares products available, makes purchase and checks out the finalized product. Various levels of authentication services are provided by the application to make a secure payment. Stripe service is employed here to make a secure payment gateway.

USE CASE FOR VIEW ITEMS

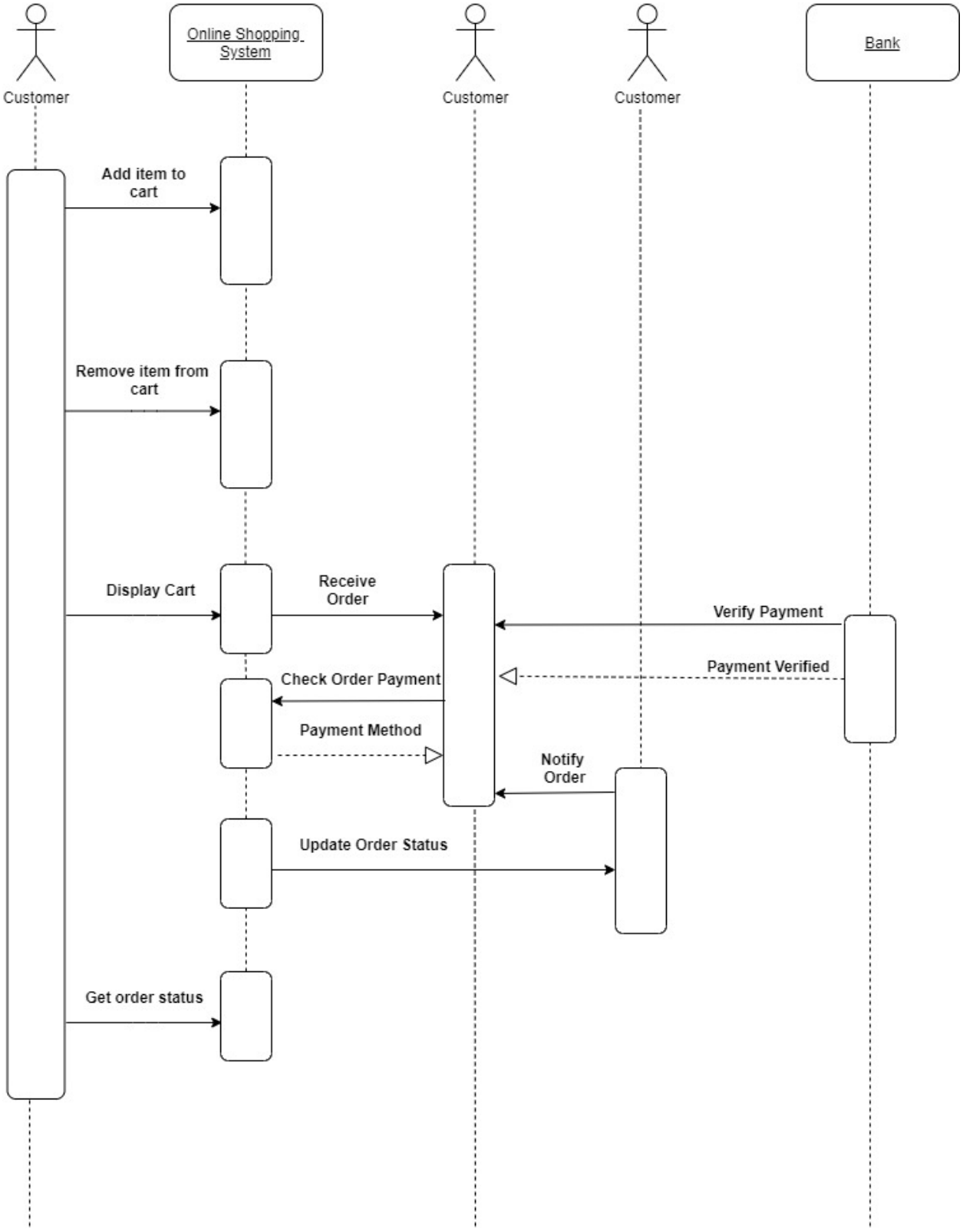


A separate use case diagram for view items in shown above. Viewing items also include searching, browsing, viewing recommended items and adding the products to shopping carts. In other words, these actions are extensions of viewing items.

Sequence Diagram

UML Sequence Diagrams are interaction diagrams that detail how operations are carried out. They capture the interaction between objects in the context of a collaboration. Sequence Diagrams are time focused and they show the order of the interaction visually by using the vertical axis of the diagram to represent time, what messages are sent and when. Sequence Diagrams captures the interaction that takes place in a collaboration that either realizes a use case or an operation (instance diagrams or generic diagrams).

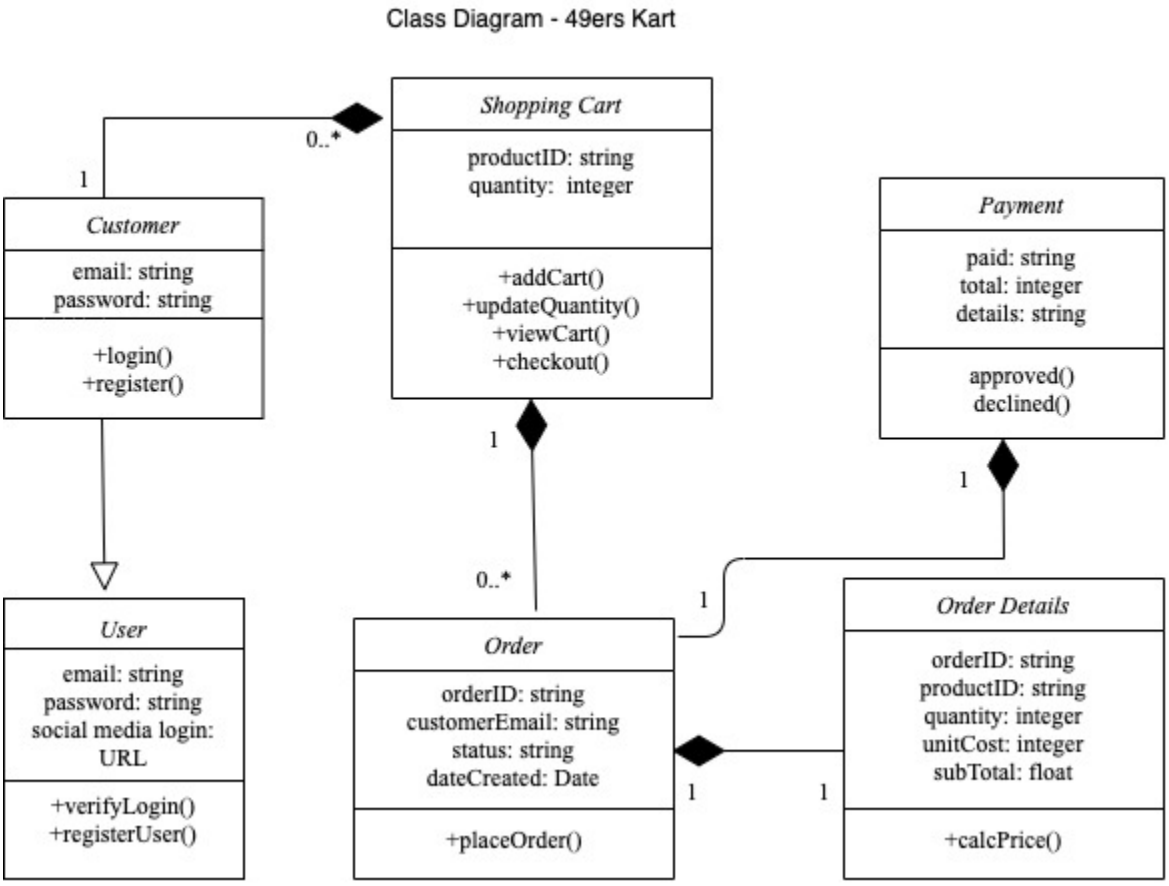
SEQUENCE DIAGRAM - 49ers Kart



The above sequence diagram provides an overview of all the interaction that happens when the application is used by the customer end to end. It depicts when and where customer interaction is involved.

Customer here denotes the role played by them while the application is in use. It represents the physical entity. Online shopping systems and banks are the other two lifelines. A lifeline represents an individual participant in the Interaction.

Class Diagram



The main components involved in the building of an e-commerce website which can be described from the above stated UML diagrams are as follows.

- **Customer**: A customer is an important component of any system. The end satisfaction of a customer or a user is the main factor deciding the success. The main activities of a user are login and signup where the user gives his/her credentials and the data is being stored in a database. The customer can either be a new customer or a registered customer
- **User**: A registered customer is the one in which he/she logs in each time, a database check is done whether an account exists or not with the given credentials. The user can view items, compare products, make purchases, etc.

- **Order**: The main components involved in an order are the customer email associated with the order, the order ID which is unique to each order to each customer, the order date that was placed and the status at each stage
- **Order Details**: Each order consists of few items that are essential namely the items that have been ordered, the quantity of each item, the total of all the items placed and the product IDs of each ordered product to differentiate between them
- **Shopping Cart**: It basically consists of the shopping list of each logged in customer. This as well involves the process where each user can update the items present in the cart by adding further or removing the already added items before checkout
- **Payment**: This is the final component involved in the whole flowchart of e-commerce shopping. Once the user checks out, he/she will be directed to a payment gateway and can enter their details and checkout with a message confirmation to their provided phone number

SOFTWARE ENGINEERING PRACTICES FOLLOWED

The whole project was developed in an agile manner. A total of three sprints were used up for the whole project wherein each sprint lasted for two weeks.

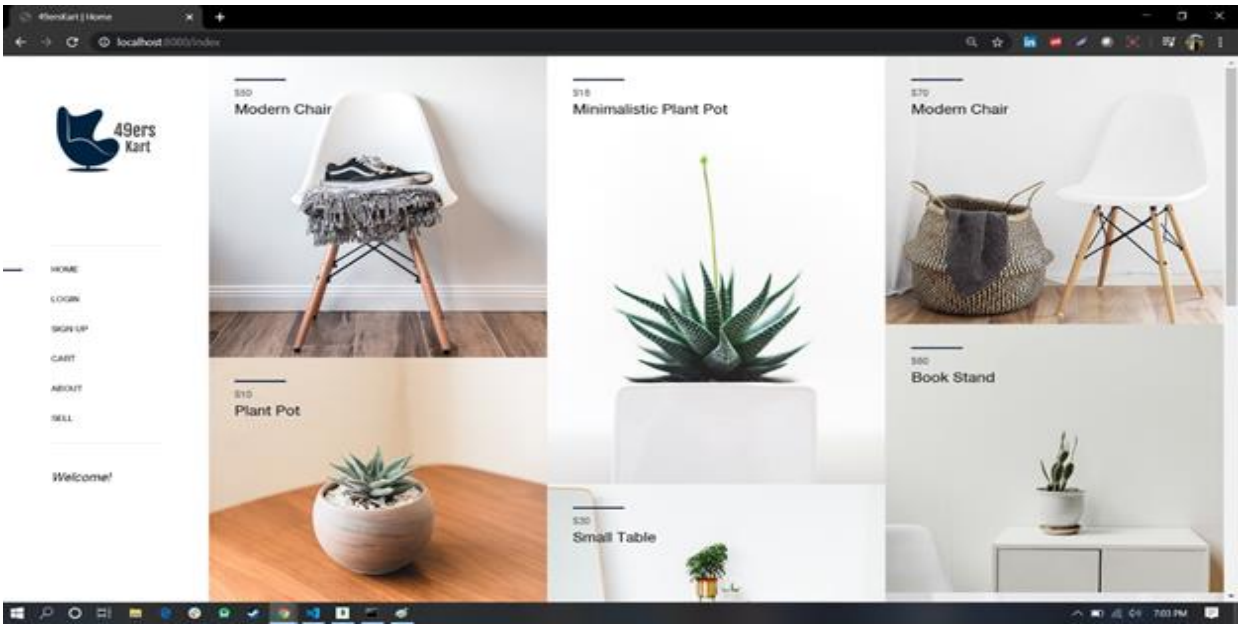
First sprint: The first and foremost sprint were dedicated towards the base of the project. Each team member came up with an idea about a project and the feasibility of each. Upon consideration of numerous factors, a final decision was made to pursue the e-commerce website. We then started off with the process of requirements gathering, architecture planning. We came up with ideas about the different ways, the different tools and technologies that could be used. Each person pitched in ideas to the maximum of their capabilities and every idea was put into action, so that each member has contributed equally.

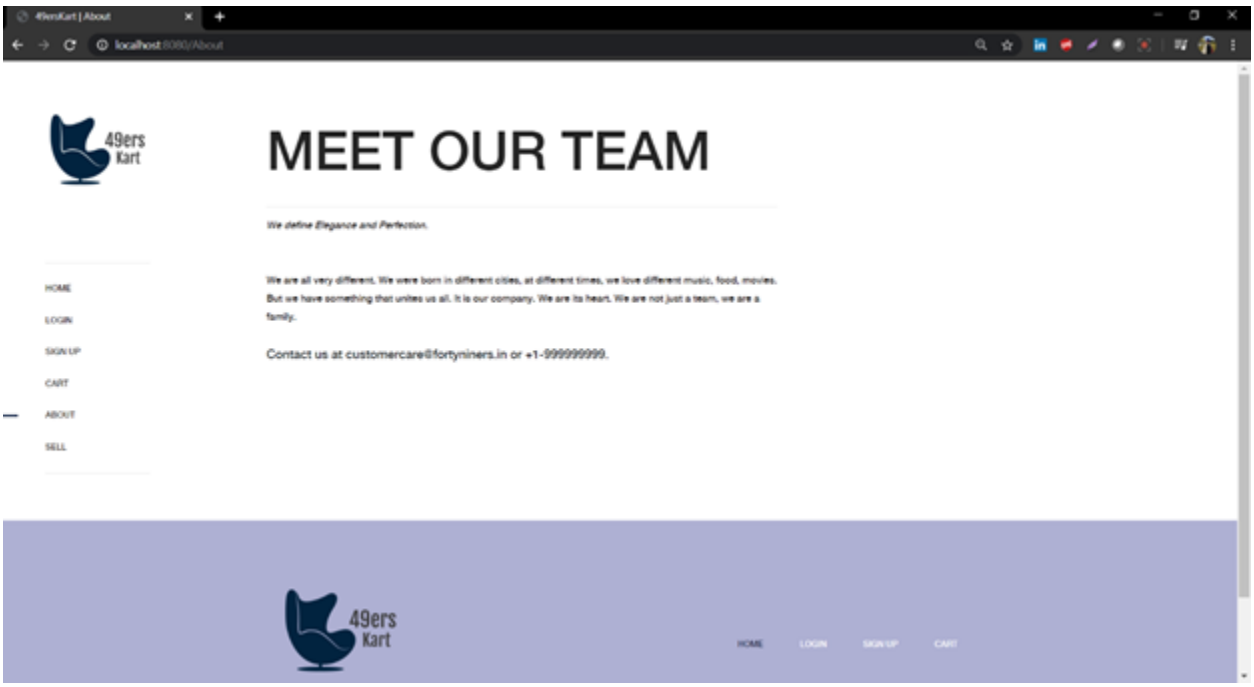
Second sprint: The second sprint was more of developing a prototype which would represent the whole project. An e-commerce website was decided to be the final product. We decided upon the main theme of the project and what all items had to be included. The concept of selling furniture at a low cost was decided to be the theme. It was mainly focused for college students and the basic items that each would need in their room for a living at a very nominal rate. Few other items are also added which are affordable as well. The second sprint consisted of developing a website for a single product and designing the basic outline of the project. By the end of the second sprint, a successful prototype was developed.

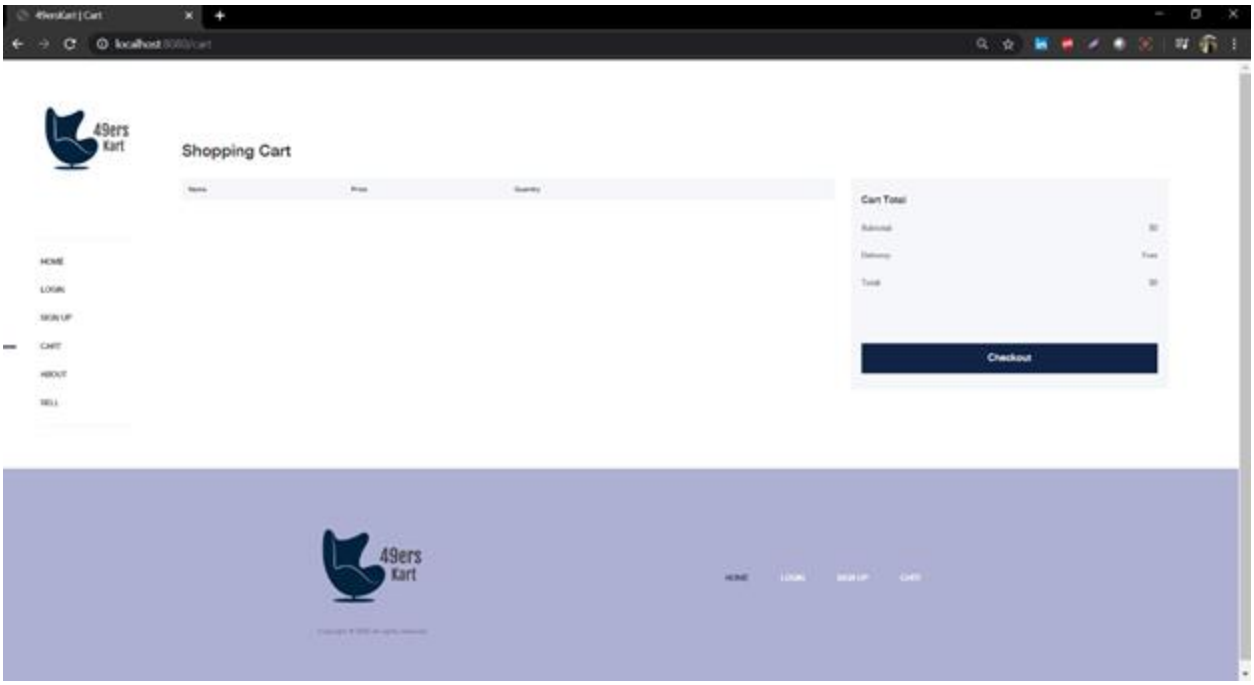
Third sprint: The third sprint was more of in-depth implementation and extension of the prototype. All the categories to be listed in the website was decided and then the front and the back end were integrated. The payment gateway was as well added. A full-fledged end-to-end project was developed by the end of this sprint.

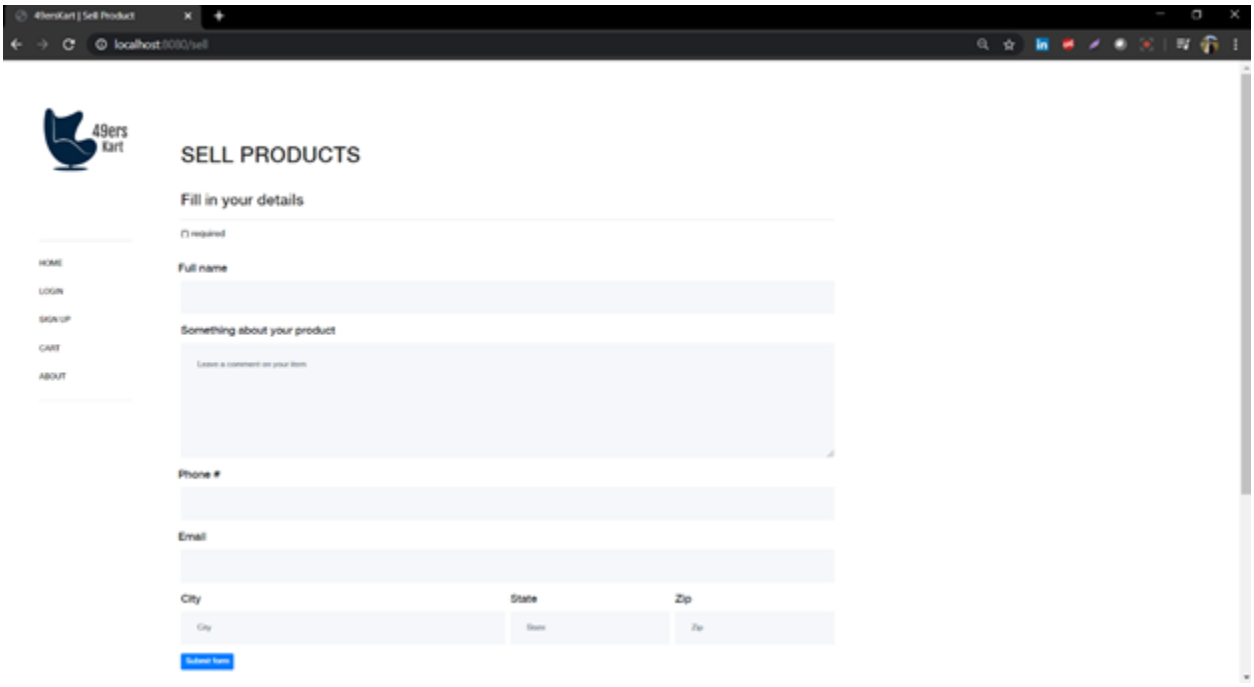
By the start of each sprint, every team member pitched in their valuable inputs and we were clear of all the steps that had to be done and produced by the end of the sprint. Requirements were gathered and the process was made clear for a hassle-free result.

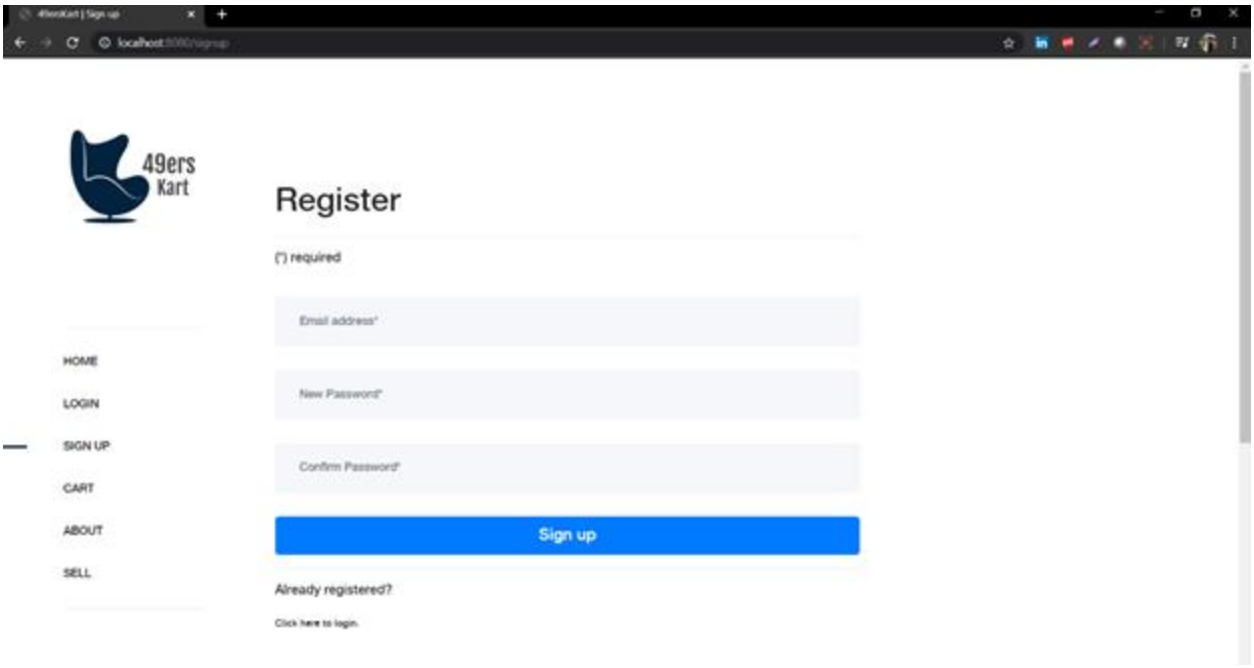
RESULTS:

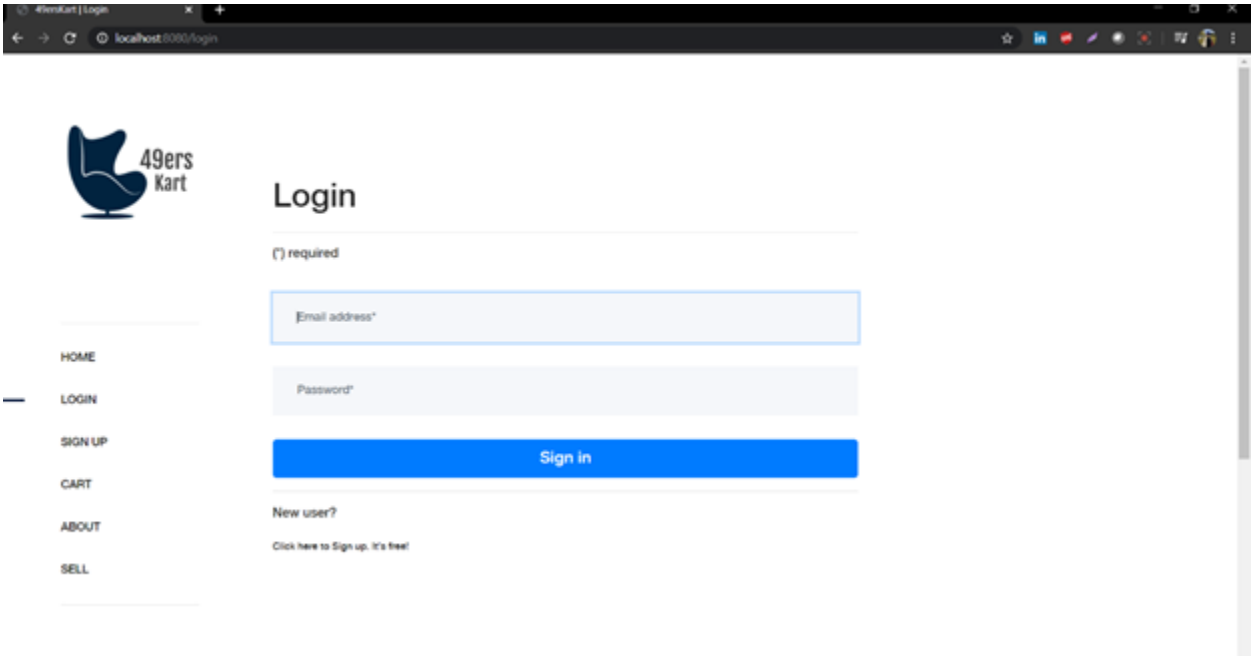

49ers Kart
HOME
LOGIN
SIGN UP
CART
ABOUT
SELL
Welcome!
$50
Modern Chair
$18
Minimalistic Plant Pot
$70
Modern Chair
$10
Plant Pot
$30
Small Table
$80
Book Stand

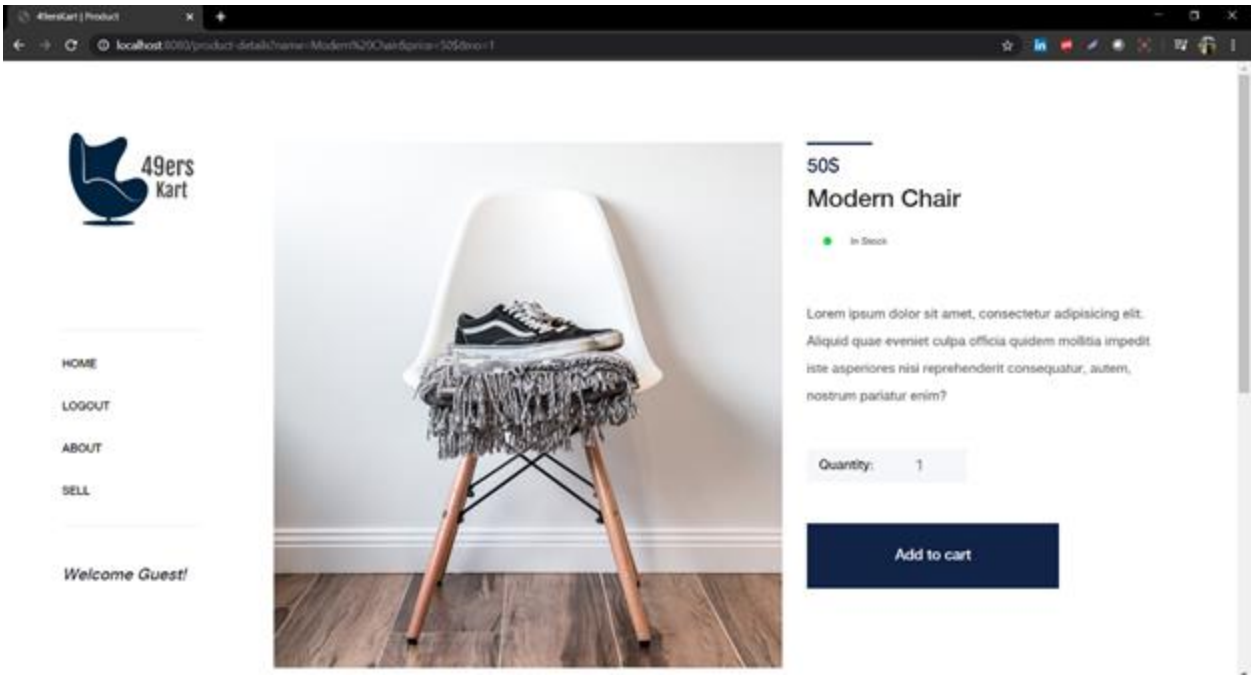

49ers Kart
HOME
LOGIN
SIGN UP
CART
ABOUT
SELL
MEET OUR TEAM
We define Elegance and Perfection.
We are all very different. We were born in different cities, at different times, we love different music, food, movies. But we have something that unites us all. It is our company. We are its heart. We are not just a team, we are a family.
Contact us at customercare@fortyniners.in or +1-999999999.
49ers Kart
HOME
LOGIN
SIGN UP
CART

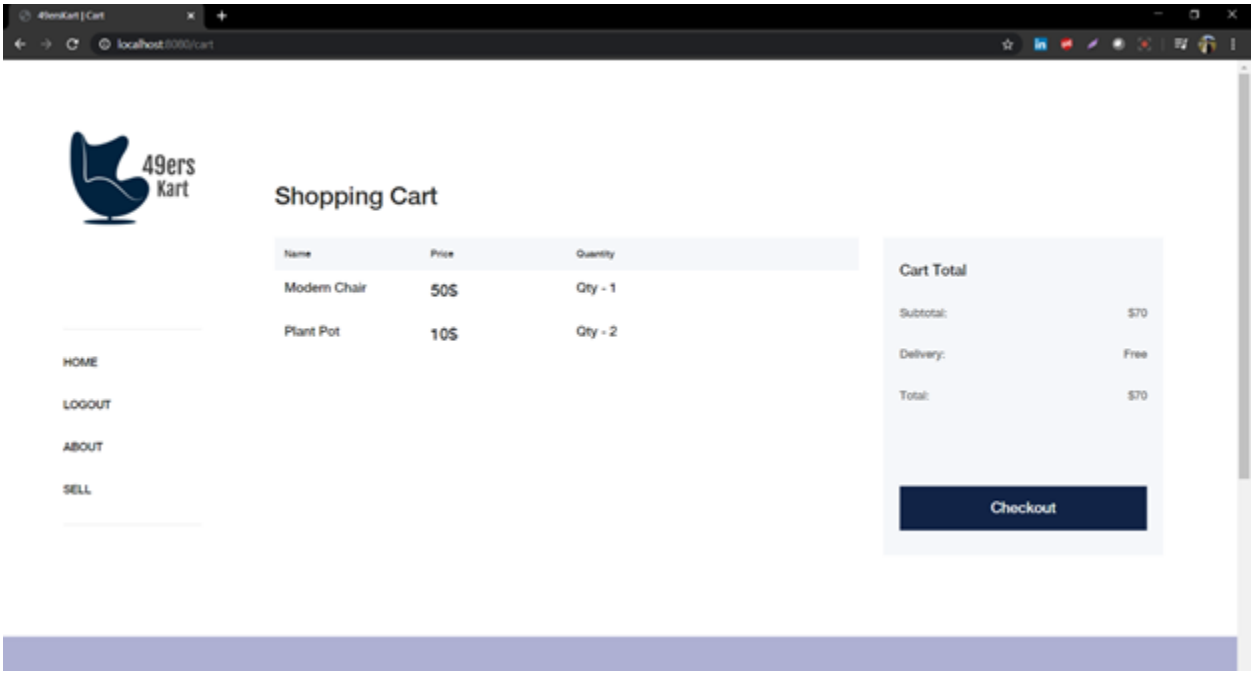

49ers Kart
Shopping Cart
HOME
LOGIN
SIGN UP
CART
ABOUT
SELL
Cart Total
Checkout
49ers Kart
HOME
LOGIN
SIGN UP
CART

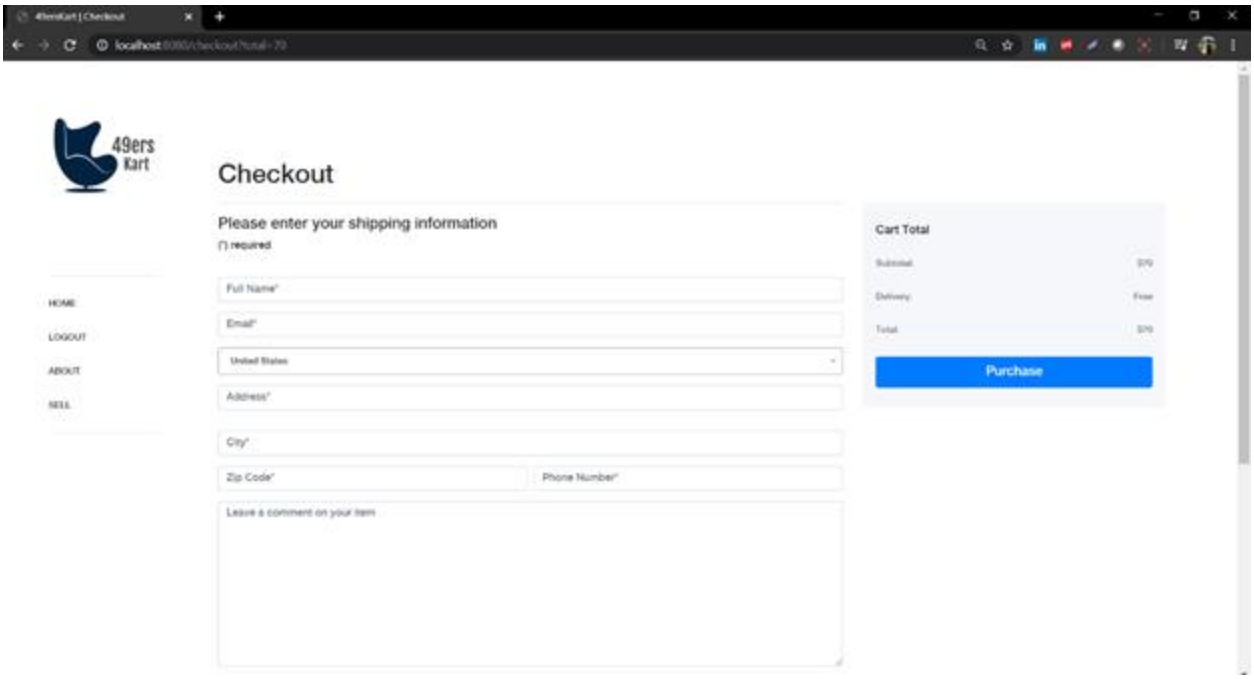

49ers Kart
SELL PRODUCTS
Fill in your details
HOME
LOGIN
SIGN UP
CART
ABOUT
Full name
Something about your product
Phone #
Email
City
State
Zip

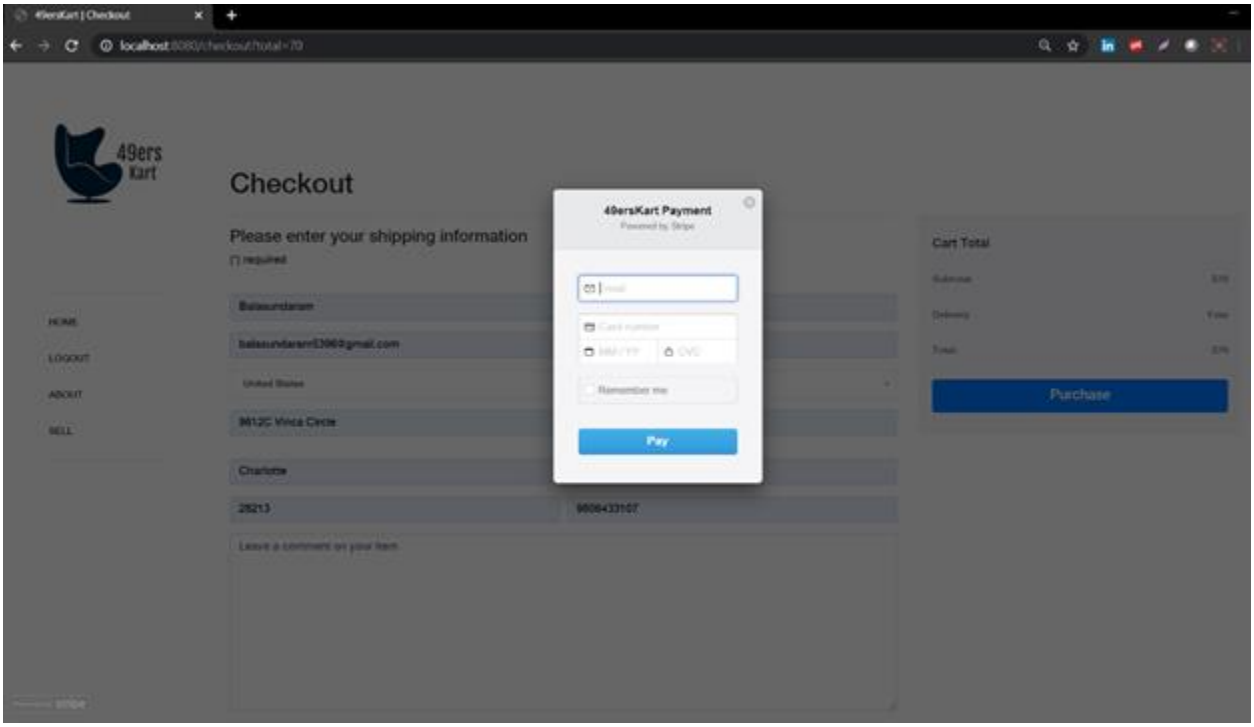

49ers
Kart
Register
(*) required
Email address*
New Password*
Confirm Password*
Sign up
Already registered?
Click here to login.
HOME
LOGIN
SIGN UP
CART
ABOUT
SELL

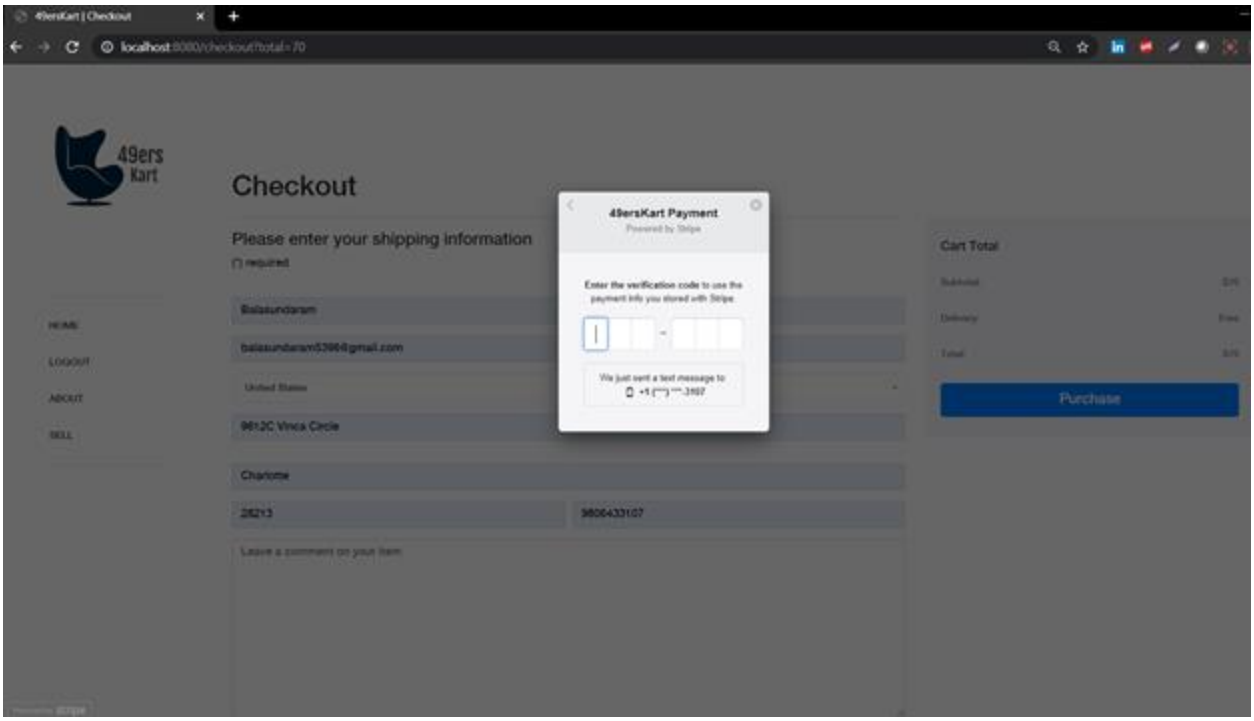

49ers
Kart
Login
(*) required
Email address*
Password*
Sign in
New user?
Click here to Sign up. It's free!
HOME
LOGIN
SIGN UP
CART
ABOUT
SELL

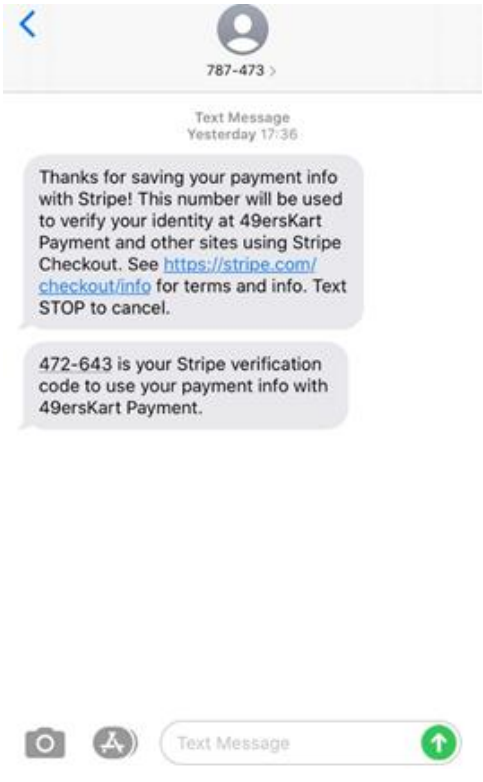

49ers Kart
HOME
LOGOUT
ABOUT
SELL
Welcome Guest!
50$
Modern Chair
In Stock
Lorem ipsum dolor sit amet, consectetur adipisicing elit. Aliquid quae eveniet culpa officia quidem mollitia impedit iste asperiores nisi reprehenderit consequatur, autem, nostrum pariatur enim?
Quantity: 1
Add to cart

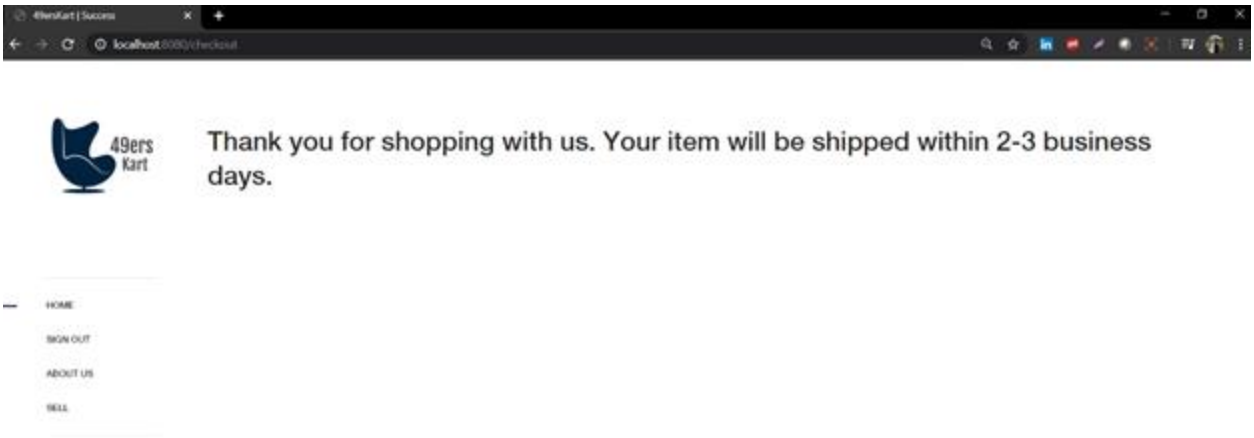

49ers Kart
Shopping Cart
Name
Price
Quantity
Modern Chair
50$
Qty - 1
Plant Pot
10$
Qty - 2
HOME
LOGOUT
ABOUT
SELL
Cart Total
Subtotal: $70
Delivery: Free
Total: $70
Checkout


49ers Kart
Checkout
Please enter your shipping information
(*) required
Full Name*
Email*
United States
Address*
City*
Zip Code*
Phone Number*
Leave a comment on your item
HOME
LOGOUT
ABOUT
SELL
Cart Total
Purchase


49ers Kart
Checkout
Please enter your shipping information
(*) required
49ersKart Payment
Pay
Cart Total
Purchase
HOME
LOGOUT
ABOUT
SELL


49ersKart | Checkout
localhost:8080/checkout?total=70
49ers Kart
Checkout
Please enter your shipping information
required
HOME
LOGOUT
ABOUT
SELL
Balasundaram
balasundaram5388@gmail.com
United States
9812C Vinca Circle
Charlotte
28213
9806433107
Leave a comment on your item
49ersKart Payment
Powered by Stripe
Enter the verification code to use the payment info you stored with Stripe.
We just sent a text message to
Cart Total
Purchase


787-473 >
Text Message
Yesterday 17:36
Thanks for saving your payment info with Stripe! This number will be used to verify your identity at 49ersKart Payment and other sites using Stripe Checkout. See https://stripe.com/checkout/info for terms and info. Text STOP to cancel.
472-643 is your Stripe verification code to use your payment info with 49ersKart Payment.
Text Message



REFERENCES:

https://github.com/expressjs/express/pull/2813#issuecomment-159270428

https://www.veracode.com/blog/secure-development/nodejs-template-engines-why-default-encoders-are-not-enough

https://expressjs.com/en/advanced/best-practice-security.html

https://getbootstrap.com/docs/4.4/layout/overview/

https://getbootstrap.com/docs/4.4/components/alerts/

https://www.w3schools.com/jquery/default.asp

https://stripe.com/docs

https://docs.mongodb.com/

https://nodejs.org/en/docs/