MINI E-COMMERCE BACKEND API

OVERVIEW

This project is a **backend system for an e-commerce application**, built with **Node.js, Express, and MongoDB**.

It supports multiple user roles (customer, manager, admin) with **role-based access control**, secure authentication, and standard e-commerce features like products, carts, and orders.

FEATURES IMPLEMENTED

- **User Authentication** → Register, Login, Logout with JWT
- **Role-based Access Control** → customer, manager, admin
- **Product APIs** → CRUD operations
- **Cart APIs** → Add, update, remove, clear cart
- **Order APIs** → Place order, view orders, update order status (restricted)
- **Admin Management** → Promote/demote user roles
- **Global Error Handling** → Consistent error responses
- **Middleware** → protect (auth guard), restrict (role guard)

API ENDPOINTS

Auth Routes

- ✓ POST /api/users/register → Register user

- ✓ POST /api/users/login → Login user (returns JWT)

- ✓ POST /api/users/logout → Logout user (protected)

USER PRODUCT ROUTES

- ✓ GET /api/products → Get all products
- ✓ GET /api/products/:id → Get product by ID

ADMIN PRODUCT ROUTES

- ✓ POST /api/products → Create product (admin/manager)
- ✓ PUT /api/products/:id → Update product (admin/manager)
- ✓ DELETE /api/products/:id → Delete product (admin/manager)

CART ROUTES

- ✓ POST /api/cart → Add product to cart
- ✓ GET /api/cart → View user's cart
- ✓ PUT /api/cart/:itemId → Update item quantity
- ✓ DELETE /api/cart/:itemId → Remove item
- ✓ DELETE /api/cart → Clear cart

USER ORDER ROUTES

- ✓ POST /api/orders → Place new order
- ✓ GET /api/orders/my → Get logged-in user's orders
- ✓ DELETE/api/orders/:orderId→Cancel order-in user's orders

ADMIN ORDER ROUTES

- ✓ GET /api/admin/order → Get all orders (admin/manager)
- ✓ PUT /api/admin/order/:orderId → Update order status (admin only)
- ✓ GET /api/admin/order/count → Count all orders (admin/manager)

USER ROUTES

- ✓ PUT /api/admin/users/:id → Update user role (admin only)

PROBLEMS FASED & SOLUTIONS

1. ✘ **Order not found error** in updateOrderStatus
   ✓ Fixed destructuring bug: changed { orderId } = req.params.orderId → const { orderId } = req.params
2. ✘ **Role mismatch issue** (customer vs manager)
   ✓ Updated schema and validation logic with correct roles
3. ✘ **Access control confusion**
   ✓ Applied protect + restrict carefully so only admins/managers access sensitive routes

SECURITY IMPLEMENTED

- ✓ 🔒 **Password Hashing** → with bcrypt before saving user data
- ✓ 🔒 **JWT Authentication** → tokens + protect middleware
- ✓ 🔒 **Role-based Access Control** → restrict("admin","manager")
- ✓ 🔒 **Helmet** → secure HTTP headers
- ✓ 🔒 **Rate Limiting** → protects against brute-force attacks

- ✓ 🔒 **CORS** → cross-origin protection
- ✓ 🔒 **Mongoose Validation** → ensures correct role/status values
- ✓ 🔒 **Centralized Error Handling** → prevents sensitive leaks

NEXT STEPS (PLANNED FEATURES)

- ○ **Logout Enhancements** → JWT blacklist (advanced security)
- ○ **Product Image Uploads** → using Multer + Cloudinary
- ○ **Payment Integration** → Stripe/PayPal checkout
- ○ **Automated Testing** → Jest + Supertest
- ○ **Deployment** → Render/Heroku + MongoDB Atlas

TECH STACK

- ❖ Node.js
- ❖ Express.js
- ❖ MongoDB + Mongoose
- ❖ JWT + bcrypt
- ❖ Helmet, CORS, express-rate-limit, mongo-sanitize

SCREENSHOTS (*POSTMAN PROOF*)

USER REGISTER/LOGIN
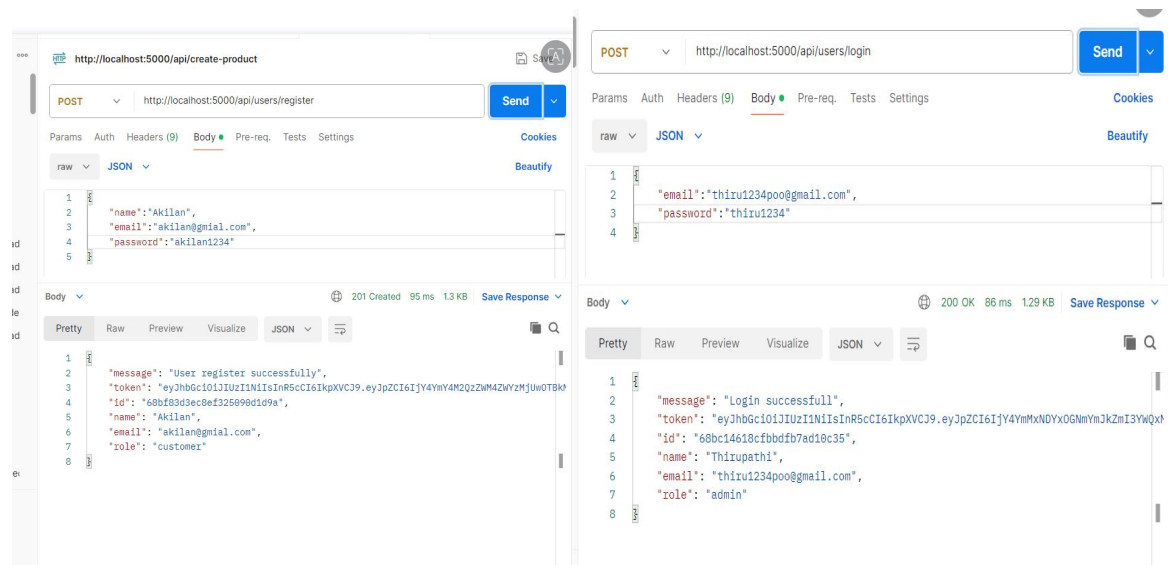
PRODUCTS/ADMIN CONTROLL

POST http://localhost:5000/api/admin/product

Params Auth Headers (9) Body ● Pre-req. Tests Settings Cookies

raw JSON Beautify

```
3      "description": "Lightweight and comfortable sneakers for everyday wear.",
4      "price": 149,
5      "category": "Shoes",
6      "stock": 120
7    }
8
```

Body 201 Created 20 ms 1.36 KB Save Response

Pretty Raw Preview Visualize JSON

```
1    {
2      "message": "Product created successfully",
3      "data": {
4        "product": {
5          "name": "Nike Air Max 270",
6          "description": "Lightweight and comfortable sneakers for everyday wear.",
7          "price": 149,
8          "category": "Shoes",
9          "stock": 120,
10         "seller": "68bc14618cfbbdfb7ad10c35",
11         "image": "https://placehold.co/400",
12         "_id": "68bf844aec8ef325090d1d9e",
13         "createdAt": "2025-09-09T01:35:06.103Z",
14         "updatedAt": "2025-09-09T01:35:06.103Z",
15         "__v": 0
16       }
17     }
```

PUT http://localhost:5000/api/admin/product/68bf844aec8ef325090d1d9e

Params Auth Headers (9) Body ● Pre-req. Tests Settings Cookies

raw JSON Beautify

```
2      "name": "Nike",
3      "description": "Lightweight and comfortable sneakers for everyday wear.",
4      "price": 567,
5      "category": "Shoes",
6      "stock": 120
7    }
```

Body 200 OK 22 ms 1.33 KB Save Response

Pretty Raw Preview Visualize JSON

```
1    {
2      "message": "Product updated successfully",
3      "data": {
4        "_id": "68bf844aec8ef325090d1d9e",
5        "name": "Nike",
6        "description": "Lightweight and comfortable sneakers for everyday wear.",
7        "price": 567,
8        "category": "Shoes",
9        "stock": 120,
10       "seller": "68bc14618cfbbdfb7ad10c35",
11       "image": "https://placehold.co/400",
12       "createdAt": "2025-09-09T01:35:06.103Z",
13       "updatedAt": "2025-09-09T01:36:50.200Z",
14       "__v": 0
15     }
16   }
```

DELETE http://localhost:5000/api/admin/product/68bc1b84ececfdb315031a17

Params Auth Headers (9) Body ● Pre-req. Tests Settings Cookies

raw JSON Beautify

```
2      "name": "Nike",
3      "description": "Lightweight and comfortable sneakers for everyday wear.",
4      "price": 567,
5      "category": "Shoes",
6      "stock": 120
7    }
```

Body 200 OK 85 ms 1.31 KB Save Response

Pretty Raw Preview Visualize JSON

```
1    {
2      "message": "Product deleted success",
3      "Data": {
4        "_id": "68bc1b84ececfdb315031a17",
5        "name": "iPhone 15 Pro",
6        "description": "Latest Apple flagship phone",
7        "price": 1299,
8        "category": "Electronics",
9        "stock": 40,
10       "seller": "68bc14618cfbbdfb7ad10c35",
11       "image": "https://placehold.co/400",
12       "createdAt": "2025-09-06T11:31:16.201Z",
13       "updatedAt": "2025-09-09T01:10:21.924Z",
14       "__v": 0
15     }
16   }
```

GET http://localhost:5000/api/products

Params Auth Headers (9) Body Pre-req. Tests Settings Cookies

Query Params

Key	Value	Bulk Edit
Key	Value	

Body 200 OK 105 ms 1.35 KB Save Response

Pretty Raw Preview Visualize JSON

```
2      "success": true,
3      "count": 1,
4      "totalProduct": 1,
5      "page": 1,
6      "totalPages": 1,
7      "products": [
8        {
9          "_id": "68bc1f5fececfdb315031a2e",
10         "name": "chuwi laptop",
11         "description": "Latest chuwi laptop flagship laptop",
12         "price": 12899,
13         "category": "Electronics",
14         "stock": 38,
15         "seller": "68bc14618cfbbdfb7ad10c35",
16         "image": "https://placehold.co/400",
17         "createdAt": "2025-09-06T11:47:43.489Z",
18         "updatedAt": "2025-09-08T13:08:32.182Z",
```

ORDERS/ADMIN CONTROLL

http://localhost:5000/api/create-product

POST http://localhost:5000/api/order/cart **Send**

Params Auth Headers (8) Body Pre-req. Tests Settings   Cookies

raw JSON Beautify

```
1
```

Body 201 Created 29 ms 1.32 KB Save Response

Pretty Raw Preview Visualize JSON

```
1  {
2      "message": "Order placed successfully",
3      "order": {
4          "user": "68bc154dececfdb315031a0f",
5          "products": [
6              {
7                  "product": "68bc1f5fececfdb315031a2e",
8                  "quantity": 1,
9                  "price": 12899,
10                 "_id": "68bed022d3e9584065b70c03"
11             }
12         ],
13         "totalPrice": 12899,
14         "status": "pending",
15         "_id": "68bed022d3e9584065b70c02",
16         "createdAt": "2025-09-08T12:46:26.689Z",
17         "updatedAt": "2025-09-08T12:46:26.689Z",
```

DELETE http://localhost:5000/api/order/deleteOrder/68becd94d3e9584065b70bd8 **Send**

Params Auth Headers (7) Body Pre-req. Tests Settings   Cookies

Headers 6 hidden

	Key	Value
☑	Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCl6IkpX
	Key	Value

Body 200 OK 83 ms 1.43 KB Save Response

Pretty Raw Preview Visualize JSON

```
1  {
2      "message": "Order cancelled successfully",
3      "order": {
4          "_id": "68becd94d3e9584065b70bd8",
5          "user": {
6              "_id": "68bc154dececfdb315031a0f",
7              "name": "Thiru",
8              "email": "thiru1234@gmail.com"
9          },
10         "products": [
11             {
12                 "product": {
13                     "_id": "68bc1b84ececfdb315031a17",
14                     "name": "iPhone 15 Pro",
15                     "price": 1299,
16                     "category": "Electronics"
17                 },
```

GET http://localhost:5000/api/admin/order **Send**

Params Auth Headers (9) Body Pre-req. Tests Settings   Cookies

Headers 8 hidden

	Key	Value
☑	Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCl6Ikp
	Key	Value

Body 200 OK 33 ms 2.28 KB Save Response

Pretty Raw Preview Visualize JSON

```
1  {
2      "count": 3,
3      "totalOrder": 3,
4      "page": 1,
5      "totalPages": 1,
6      "order": [
7          {
8              "_id": "68bec95ad3e9584065b70bce",
9              "user": {
10                 "_id": "68bc154dececfdb315031a0f",
11                 "name": "Thiru",
12                 "email": "thiru1234@gmail.com"
13             },
14             "products": [
15                 {
16                     "product": {
17                         "_id": "68bc1b84ececfdb315031a17",
```

PUT http://localhost:5000/api/admin/order/68bec95ad3e9584065b70bce **Send**

Params Auth Headers (9) Body Pre-req. Tests Settings   Cookies

raw JSON Beautify

```
1  {
2      "status":"shipped"
3  }
```

Body 200 OK 115 ms 1.44 KB Save Response

Pretty Raw Preview Visualize JSON

```
1  {
2      "message": "Order status updated successfully",
3      "order": {
4          "_id": "68bec95ad3e9584065b70bce",
5          "user": {
6              "_id": "68bc154dececfdb315031a0f",
7              "name": "Thiru",
8              "email": "thiru1234@gmail.com"
9          },
10         "products": [
11             {
12                 "product": {
13                     "_id": "68bc1b84ececfdb315031a17",
14                     "name": "iPhone 15 Pro",
15                     "price": 1299,
16                     "category": "Electronics"
17                 },
```

CART USER VIEW

http://localhost:5000/api/create-product — Save

| POST ∨ | http://localhost:5000/api/cart/creat | **Send** ∨ |

Params Auth Headers (9) **Body** • Pre-req. Tests Settings   Cookies

raw ∨   **JSON** ∨   Beautify

```
1  {
2    "productId": "68bc1f5fececfdb315031a2e",
3    "quantity": 1
4  }
5
```

Body ∨   ⊕ 200 OK 15 ms 1.18 KB Save Response ∨

Pretty Raw Preview Visualize   JSON ∨   📋 Q

```
1  {
2    "message": "Product added to cart",
3    "cart": {
4      "_id": "68be29f69e543bb672ab9765",
5      "user": "68bc154dececfdb315031a0f",
6      "items": [
7        {
8          "product": "68bc1f5fececfdb315031a2e",
9          "quantity": 1,
10         "_id": "68bed00cd3e9584065b70bfb"
11        }
12      ],
13      "__v": 10
14    }
15  }
```

http://localhost:5000/api/create-product — Save

| GET ∨ | http://localhost:5000/api/cart/myCart | **Send** ∨ |

Params Auth Headers (9) **Body** • Pre-req. Tests Settings   Cookies

raw ∨   **JSON** ∨   Beautify

```
1  {
2    "quantity": 4
3  }
4
```

Body ∨   ⊕ 200 OK 28 ms 1.2 KB Save Response ∨

Pretty Raw Preview Visualize   JSON ∨   📋 Q

```
1  {
2    "cart": {
3      "_id": "68be29f69e543bb672ab9765",
4      "user": "68bc154dececfdb315031a0f",
5      "items": [
6        {
7          "product": {
8            "_id": "68bc1f5fececfdb315031a2e",
9            "name": "chuwi laptop",
10           "price": 12899
11         },
12         "quantity": 4,
13         "_id": "68be37706f864e755198186c"
14       }
15     ],
16     "__v": 4
17   },
18   "totalPrice": 51596
19  }
```

http://localhost:5000/api/create-product — Save

| DELETE ∨ | http://localhost:5000/api/cart/removeProducts/68bc1f5fececfdb315031a2e | **Send** ∨ |

Params Auth Headers (9) **Body** • Pre-req. Tests Settings   Cookies

raw ∨   **JSON** ∨   Beautify

```
1  {
2    "productId": "68bc1b84ececfdb315031a17",
3    "quantity": 2
4  }
```

Body ∨   ⊕ 200 OK 21 ms 1.18 KB Save Response ∨

Pretty Raw Preview Visualize   JSON ∨   📋 Q

```
1  {
2    "message": "Item removed from cart",
3    "cart": {
4      "_id": "68be29f69e543bb672ab9765",
5      "user": "68bc154dececfdb315031a0f",
6      "items": [
7        {
8          "product": "68bc1b84ececfdb315031a17",
9          "quantity": 2,
10         "_id": "68be3af46f864e7551981881"
11        }
12      ],
13      "__v": 6
14    }
15  }
```

ADMIN PROMOTE ROLE (MANAGER)

HTTP http://localhost:5000/api/create-product   💾 Save

| PUT ⌄ | http://localhost:5000/api/admin/users/68bf83d3ec8ef325090d1d9a | Send ⌄ |

Params Auth Headers (9) Body • Pre-req. Tests Settings   Cookies

raw ⌄   JSON ⌄   Beautify

```
1  {
2      "role": "manager"
3  }
4
```

Body ⌄   🌐 200 OK 69 ms 1.19 KB Save Response ⌄

Pretty Raw Preview Visualize JSON ⌄   🔍

```
1   {
2       "message": "Role updated successfully",
3       "user": {
4           "_id": "68bf83d3ec8ef325090d1d9a",
5           "name": "Akilan",
6           "email": "akilan@gmial.com",
7           "role": "manager",
8           "createdAt": "2025-09-09T01:33:07.069Z",
9           "updatedAt": "2025-09-09T01:47:04.640Z",
10          "__v": 0
11      }
12  }
```