

CODE:

```
JS recyclablesRoutes.js JS footprintRoutes.js JS awarenessRoutes.js JS authMiddleware.js X JS errorM
middleware > JS authMiddleware.js > ...
1  const jwt = require('jsonwebtoken');
2
3  // Middleware to protect routes
4  const protect = (req, res, next) => {
5    let token;
6
7    if (
8      req.headers.authorization &&
9      req.headers.authorization.startsWith('Bearer')
10   ) {
11     try {
12       token = jwt.verify(token, process.env.JWT_SECRET);
13       const decoded = jwt.verify(token, process.env.JWT_SECRET);
14       req.user = decoded; // attach decoded payload to request
15       next();
16     } catch (error) {
17       return res.status(401).json({ message: 'Not authorized, token failed' });
18     }
19   }
20 }
```

⚙️ .env

```
1  PORT=5000
2  MONGO_URI=mongodb://127.0.0.1:27017/sustainable_backend_secure
3  JWT_SECRET=your_jwt_secret_here
4
5
```

JS server.js > ...

```
2  const express = require('express');
3  const helmet = require('helmet');
4  const cors = require('cors');
5  const xss = require('xss-clean');
6  const mongoSanitize = require('express-mongo-sanitize');
7  const rateLimit = require('express-rate-limit');
8  const morgan = require('morgan');
9  const connectDB = require('./config/db');
10
11  const app = express();
12  connectDB();
13
14  // Security & middlewares
15  app.use(helmet());
16  app.use(cors());
17  app.use(express.json());
18  app.use(xss());
19  app.use(mongoSanitize());
```

JS recyclablesRoutes.js

JS footprintRoutes.js

JS awarenessRoutes.js

JS authMiddleware.js

JS errorMiddl

middleware > JS errorMiddleware.js > ...

```
1  module.exports = (err, req, res, next) => {
2    console.error(err.stack);
3    res.status(err.statusCode || 500).json({ message: err.message || 'Server error' });
4  };
5
```

config > JS db.js > ...

```
1  const mongoose = require('mongoose');
2
3  const connectDB = (alias) => {
4    try {
5      await mongoose.connect(process.env.MONGO_URI);
6      console.log('MongoDB connected');
7    } catch (err) {
8      console.error(err.message);
9      process.exit(1);
10   }
11 };
12
13 module.exports = connectDB;
14
```

OUTPUT:1)Testing Footprints Endpoint (GET/POST) a)footprints (postman+browser)

GET http://localhost:5000/api/footprints

Send

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

Query Params

Key	Value	Bulk Edit
Key	Value	

Body 200 OK 122 ms 989 B Save Response

Pretty Raw Preview Visualize JSON

```
1 []
```

localhost:5000/api/footprints

Pretty-print

```
[]
```

GET Untitled Request POST http://localhost:5000/api/footprints GET Untitled Request + ...

HTTP http://localhost:5000/api/footprints Save </>

POST http://localhost:5000/api/footprints Send

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

raw JSON

```
1 {
2   "transportMode": "car",
3   "distanceKm": 10,
4   "electricityKWh": 2
5 }
6
```

Body 201 Created 136 ms 1.14 KB Save Response

Pretty Raw Preview Visualize JSON

```
1 {
2   "transportMode": "car",
3   "distanceKm": 10,
4   "electricityKWh": 2,
5   "_id": "68d18eb312835680a2b7322f",
6   "createdAt": "2025-09-22T18:00:19.195Z",
7   "updatedAt": "2025-09-22T18:00:19.195Z",
8   "__v": 0
9 }
```

localhost:5000/api/footprints

Pretty-print

```
[{"_id": "68d18eb312835680a2b7322f", "transportMode": "car", "distanceKm": 10, "electricityKWh": 2, "createdAt": "2025-09-22T18:00:19.195Z", "updatedAt": "2025-09-22T18:00:19.195Z", "__v": 0}]
```

b)recyclables (postman+browser)

GET Untitled Request GET http://localhost:5000/api/ GET Untitled Request + ...

HTTP http://localhost:5000/api/recyclables Save </>

GET http://localhost:5000/api/recyclables Send

Params Authorization Headers (6) Body Pre-request Script Tests Settings Cookies

none form-data x-www-form-urlencoded raw binary

This request does not have a body

Body Cookies Headers (22) Test Results Status: 200 OK Time: 54 ms Size: 989 B Save Response

Pretty Raw Preview Visualize JSON

```
1
```

←

→

↻

📄

localhost:5000/api/recyclables

Pretty-print ☐

[]

GET Untitled Request

POST http://localhost:5000/ap

GET Untitled Request

+

...

🔗 http://localhost:5000/api/recyclables

Save

</>

POST

http://localhost:5000/api/recyclables

Send

⌵

Params

Authorization

Headers (8)

Body

Pre-request Script

Tests

Settings

none

form-data

x-www-form-urlencoded

raw

binary

JSON

⌵

1

2

3

4

5

6

7

"title": "Old Laptop",

"description": "Dell Inspiron",

"category": "Electronics",

"condition": "Good",

"location": "Mumbai",

"contact": "khushihitika@ves.com"

Body

Cookies

Headers (22)

Test Results

📶

Status: 201 Created

Time: 59 ms

Size: 1.3 KB

Save Response

⌵

Pretty

Raw

Preview

Visualize

JSON

⌵

⌵

1

2

3

4

5

6

7

8

9

10

11

12

13

14

"message": "Recyclable posted",

"recyclable": {

"title": "Old Laptop",

"description": "Dell Inspiron",

"category": "Electronics",

"condition": "Good",

"location": "Mumbai",

"contact": "khushihitika@ves.com",

"status": "available",

"_id": "68d191a812835680a2b73237",

"createdAt": "2025-09-22T18:12:56.307Z",

"updatedAt": "2025-09-22T18:12:56.307Z",

"__v": 0

←

→

↻

📄

localhost:5000/api/recyclables

☆

🔄

School

[[{"_id": "68d191a812835680a2b73237", "title": "Old Laptop", "description": "Dell Inspiron", "category": "Electronics", "condition": "Good", "location": "Mumbai", "contact": "khushihitika@ves.com", "status": "available", "createdAt": "2025-09-22T18:12:56.307Z", "updatedAt": "2025-09-22T18:12:56.307Z", "__v": 0}]]

Some security features: a)input validation

The screenshot shows a REST client interface with a POST request to `http://localhost:5000/api/recyclables`. The request body is in JSON format. The response is a 400 Bad Request with a JSON body containing an error message.

Request:

```
POST http://localhost:5000/api/recyclables
```

Request Body (JSON):

```
{  "message": "Recyclable validation failed: title: Path 'title' is required."}
```

Response: Status: 400 Bad Request, Time: 13 ms, Size: 1.21 KB

Response Body (JSON):

```
{  "errors": [    {      "type": "field",      "msg": "Invalid value",      "path": "title",      "location": "body"    },    {      "type": "field",      "msg": "Invalid value",      "path": "category",      "location": "body"    }  ]}
```

GET Untitled Request POST http://localhost:5000/api/footprints GET Untitled Request + ...

http://localhost:5000/api/footprints Save </>

POST http://localhost:5000/api/footprints Send

Params Authorization Headers (8) Body Pre-request Script Tests Settings Cookies Beautify

none form-data x-www-form-urlencoded raw binary JSON

```
1 {
2   "transportMode": "",
3   "distanceKm": "abc"
4 }
5
6
7
```

Body Cookies Headers (22) Test Results Status: 500 Internal Server Error Time: 66 ms Size: 1.21 KB Save Response

Pretty Raw Preview Visualize JSON

```
1
2 "message": "Footprint validation failed: distanceKm: Cast to Number failed for value \"abc\" (type string) at path \"distanceKm\", transportMod
3
```

GET Untitled Request x POST http://localhost:5000/api/footprints GET Untitled Request POST http://localhost:5000/api/footprints + ...

http://localhost:5000/api/footprints

POST http://localhost:5000/api/footprints

Params Authorization Headers (8) Body Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary JSON

```
1 {
2   "item": "<script>alert('hack')</script>"
3 }
4
5
6
7
```

Body Cookies Headers Test Results Status: 500 Internal Server Error Time: 21 ms Size: 1.21 KB

Pretty Raw Preview Visualize Text

```
1
```


b) Helmet(Check response headers in Postman → X-Content-Type-Options, Content-Security-Policy)

The screenshot shows a Postman interface with a POST request to `http://localhost:5000/api/recyclables`. The request body is a JSON object:

```
{  "title": "Old Laptop",  "description": "Dell Inspiron",  "category": "Electronics",  "condition": "Good",  "location": "Mumbai",  "contact": "khushihitika@ues.com"}
```

The response status is 201 Created, with a time of 56 ms and a size of 1.3 KB. The response headers are listed below:

Key	Value
Content-Security-Policy	default-src 'self';base-uri 'self';font-src 'self' https: data:;form-action 'self';frame-ancesto...
Cross-Origin-Opener-Policy	same-origin
Cross-Origin-Resource-Policy	same-origin
Origin-Agent-Cluster	?1
Referrer-Policy	no-referrer
Strict-Transport-Security	max-age=15552000; includeSubDomains
X-Content-Type-Options	nosniff
X-DNS-Prefetch-Control	off
X-Download-Options	noopen

Body	Cookies	Headers (22)	Test Results	Status: 201 Created	Time: 56 ms	Size: 1.3 KB	Save Response
		X-Frame-Options		SAMEORIGIN			
		X-Permitted-Cross-Domain-Policies		none			
		X-XSS-Protection		0			
		Access-Control-Allow-Origin		*			
		X-RateLimit-Limit		100			
		X-RateLimit-Remaining		99			
		Date		Mon, 22 Sep 2025 18:31:58 GMT			
		X-RateLimit-Reset		1758566407			
		Content-Type		application/json; charset=utf-8			
		Content-Length		334			

c)rate limiter

GET Untitled Request

POST http://localhost:5000/

GET Untitled Request

POST http://localhost:5000/

GET http://localhost:5000/

GET http://localhost:5000/

POST http://localhost:5000/

+

http://localhost:5000/api/footprints

Save

POST

http://localhost:5000/api/footprints

Send

Params

Authorization

Headers (8)

Body

Pre-request Script

Tests

Settings

Cookies

Query Params

Key	Value	Bulk Edit
Key	Value	

Body

Cookies

Headers (23)

Test Results

Status: 429 Too Many Requests

Time: 6 ms

Size: 1.03 KB

Save Response

Pretty

Raw

Preview

Visualize

HTML

1

Too many requests, please try again later.