



Title:

Design and Implementation of a Secure REST API Using
Node.js, MongoDB, and JWT

Course:

Distributed Systems Security

Institution: ECE Paris

Instructor:

Yaya Doumbia

Academic Year: 2025-2026

Group Member:

OFUNNEKA JENNIFER OKONKWOABUTU

DATE: 15th January 2026

TABLE OF CONTENTS

TABLE OF CONTENTS.....	1
1.0 INTRODUCTION.....	2
1.1 Purpose of this Project.....	2
1.2 Objectives of the project.....	2
1.3 Source Code Reference.....	2
2.0 DEVELOPMENT ENVIRONMENT CONFIGURATION.....	3
2.1 Tools and Technologies Used.....	3
2.2 Environment setup.....	3
Step 1: Install Required Software.....	3
Step 2: Create the Project Workspace.....	6
Step 3: Initialize Node.js Project.....	7
Step 4: Install Project Dependencies.....	7
Step 5: Verify Environment Configuration.....	8
2.3 Conclusion.....	8
3.0 GLOBAL SYSTEM ARCHITECTURE.....	9
3.1 Architectural Layers.....	9
3.2 Project Structure.....	9
3.3 Conclusion.....	9
4.0 DATABASE DESIGN AND DATA MODELING.....	10
4.1 Entities.....	10
4.2 Database Creation and Setup.....	10
4.3 Implement Database Models (Schemas).....	11
4.4 Conclusion:.....	12
5.0 APPLICATION IMPLEMENTATION AND REQUEST PROCESSING.....	13
5.1 Implement Controllers (Business Logic).....	13
5.2 Implement Routes (HTTP Endpoints).....	19
5.3 Implement Authentication Middleware.....	21
5.4 Implement Application Entry Point.....	21
6.0 TESTING AND VERIFICATION USING POSTMAN.....	23
6.1 Precondition.....	23
6.2 Step by Step Testing of All API Endpoints.....	23
6.3 Detailed Flow of Request.....	31
A. GETALLPLAYERS.....	31
FINAL CONCLUSION.....	34
APPENDIX.....	35
A. API Endpoint Reference.....	35
B. Collection and Requests Created on Postman.....	35

1.0 INTRODUCTION

1.1 Purpose of this Project

The purpose of this lab is to design, implement, and document a secure RESTful API capable of managing two related entities: Equipes and Players.

For this project:

- Users can create, read, update, and delete(CRUD) equipe and player records.
- Entity relationships are maintained: each player is linked to a team(equipe) using MongoDB ObjectId references.
- Routes allow fetching all players for a team and finding the team of a given player.
- Users must authenticate before modifying or deleting resources via JWT.
- Search functionality for players by name is prepared for future implementation.

This report is written as an operational document, such that it can be followed step-by-step to reproduce the system from scratch.

1.2 Objectives of the project

Functional Objectives:

1. Create a REST API using [Node.js](#) and Express.
2. Store data using MongoDB.
3. Implement full CRUD operations.
4. Manage relationships between two entities (teams and players).
5. Secure write operations using JWT authentication.

1.3 Source Code Reference

The complete source code for this project is available in a public Github repository and can be used to reproduce the system described in this report.

Repository Link:

https://github.com/JanieAbutu/ECE_Distributed-Systems-Security/tree/main/Projects/Lab%201_PlayerEntity_RestAPI_Project

2.0 DEVELOPMENT ENVIRONMENT CONFIGURATION

2.1 Tools and Technologies Used

Node.js:

This is used as the JavaScript runtime to execute server-side code. [Node.js](#) comes with the npm package manager which is used to manage dependencies and run scripts.

Express.js

This provides routing, middleware support, and HTTP request handling.

MongoDB

This is a NoSQL document-oriented database used for data persistence.

Mongoose

This is an Object Data Modeling (ODM) library that provides schemas, validation, and database abstraction.

JSON Web Token (JWT)

This is used for stateless authentication and authorization.

Postman

This is used to manually test and verify API endpoints.

Summary:

Each tool was selected to address a specific responsibility within the system.

2.2 Environment setup

This section describes how the development environment was configured before starting the project. Proper environment setup is critical to ensure that the REST API runs correctly, dependencies are managed consistently, and errors related to tooling are avoided.

Step 1: Install Required Software

1. [Node.js](#) includes npm (Node Package Manager):

- Download LTS version (recommended) from <https://nodejs.org/en/> .

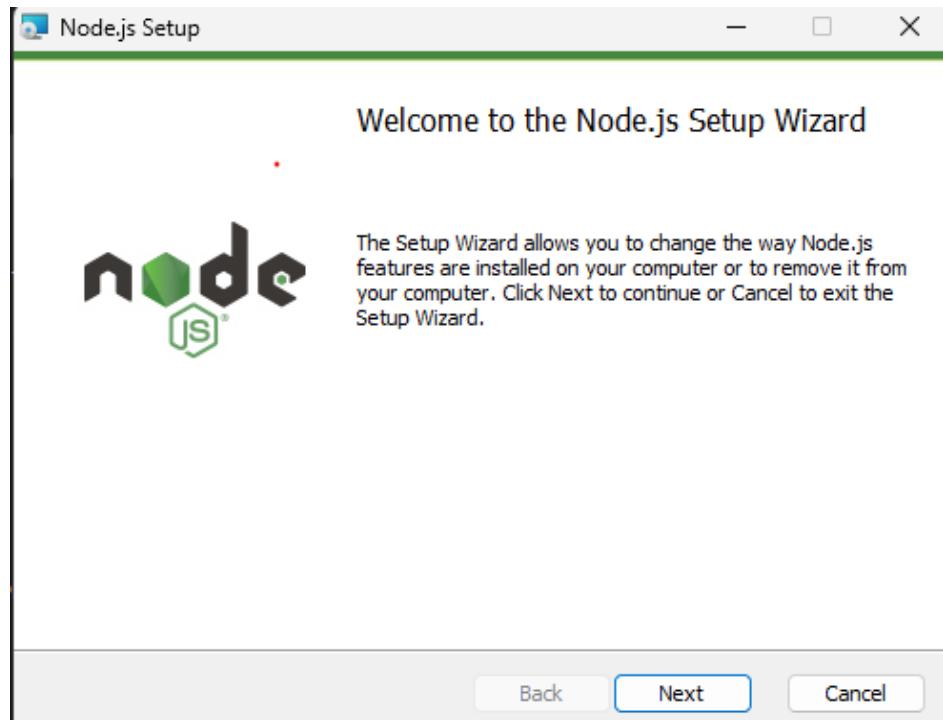


Fig 1: [Node.js](#) installation interface

- Verify the installation of [Node.js](#) by running the commands below on command prompt.

```
node -v
npm -v
C:\Users\Starlix>node -v
v22.21.1
C:\Users\Starlix>npm -v
8.17.0
C:\Users\Starlix>
```

Fig 2: Output of command verifying version of [node.js](#) and npm installed

2. MongoDB Community Server

- Download MongoDB Community Server from <https://www.mongodb.com/> and install.

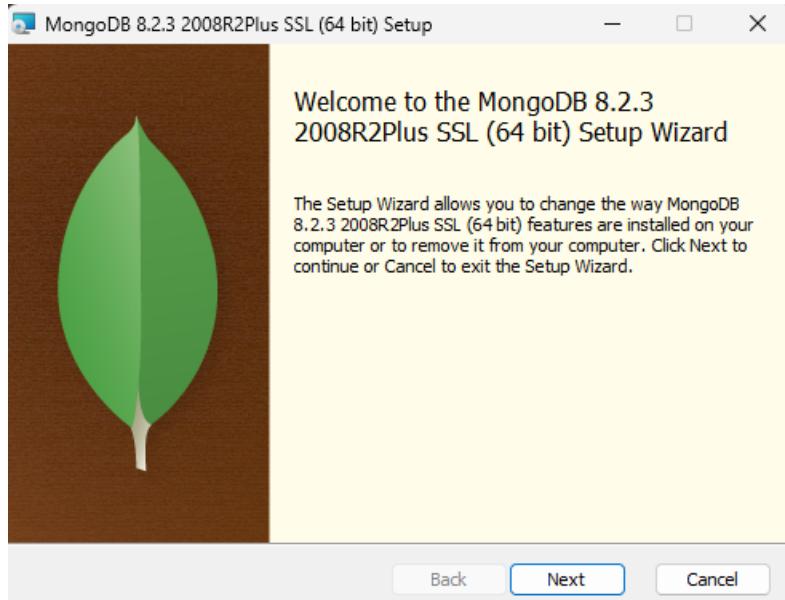


Fig 3:MongoDB Community Server installation interface

- The **MongoDB Compass** installs immediately after this from the same package. It provides the graphical interface to visualise and manage database data as seen below.

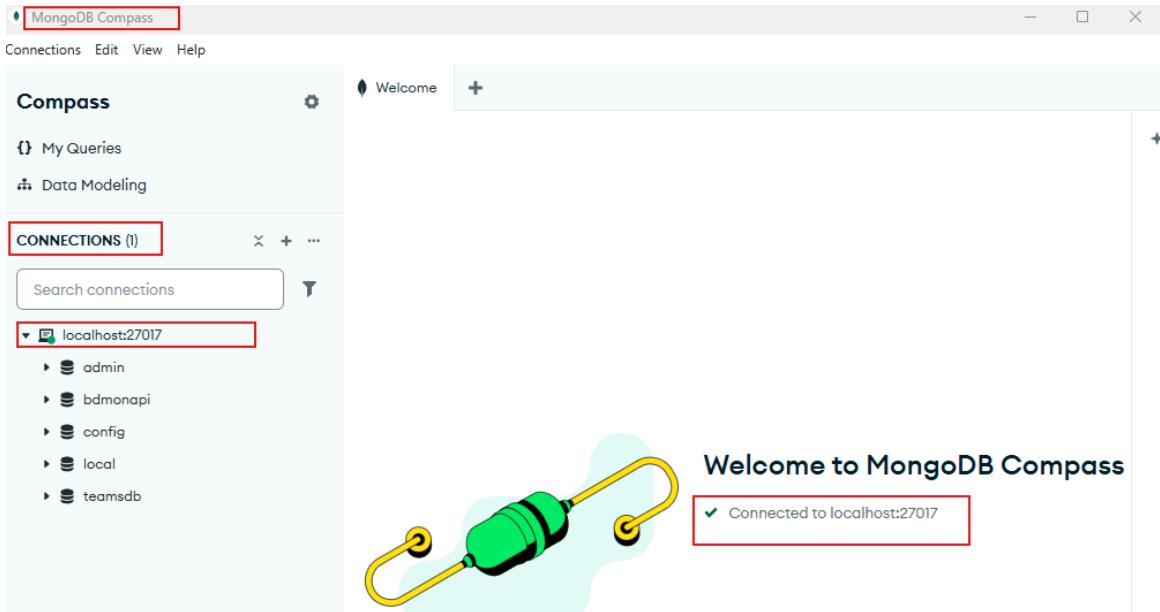


Fig 4:MongoDB Compass interface

- After installation, open MongoDB Compass, then click on 'Localhost:27017' to connect. Successful connection will be confirmed as seen in above image.

3. Postman

- Download the postman application from <https://www.postman.com/> and install. Register, login, and create a workspace to get started.

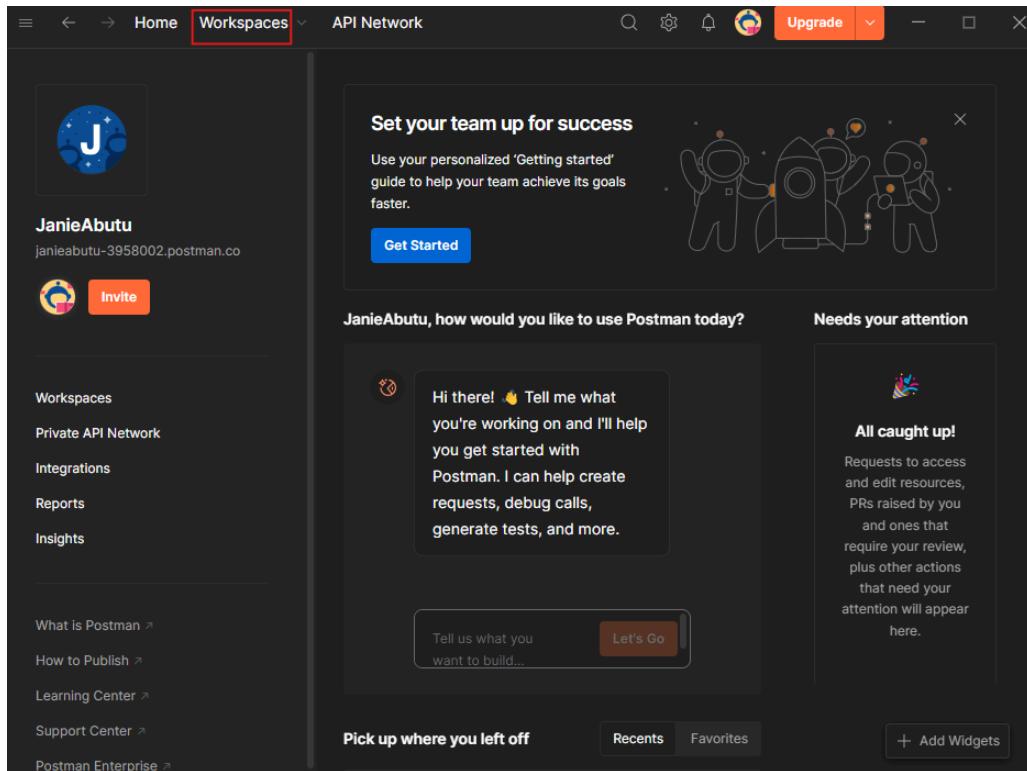


Fig 5:Postman interface

Step 2: Create the Project Workspace

- Create a dedicated folder to contain all application files, all source code, configuration files, and dependencies for one Node.js project. The name of the folder created for this project is ***PlayerEntity_RestAPI_Project***.
- Open the folder in a code editor (Visual Studio - VS Code recommended).

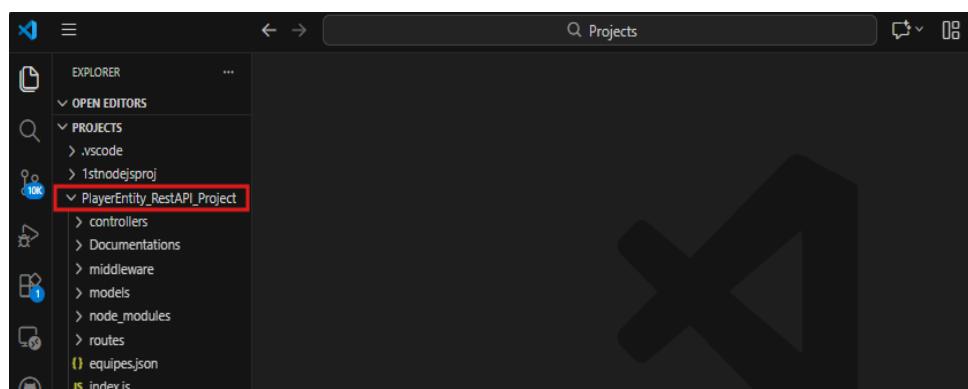


Fig 6:Folder ***PlayerEntity_RestAPI_Project*** opened on VS Code

- On the terminal on VS Code, navigate to the project folder as seen below. This is to ensure that all activities and dependencies to be installed will be done within the project.

Fig 7: Navigated into the directory ***PlayerEntity_RestAPI_Project*** opened on VS Code terminal

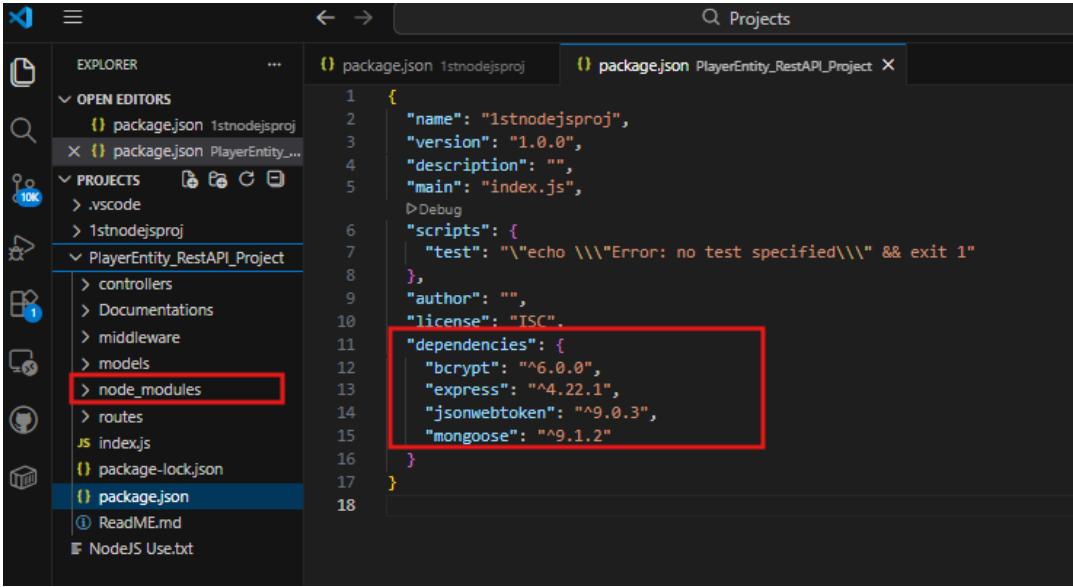
Step 3: Initialize Node.js Project

- On the VS Code terminal navigated to the project directory, run the command **npm init**.
 - This initializes the [Node.js](#) project and generates a package.json file which describes the project, lists the installed dependencies, and defines the application entry point as seen below

Fig 8: package.json file generated after initialization

Step 4: Install Project Dependencies

- The following dependencies are installed locally for the project.
 - express, a web framework
 - mongoose, mongoDB ODM
 - jsonwebtoken, jwt authentication
 - bcrypt, password hashing
 - The dependencies are stored in node_modules/ and referenced in package.json as seen below:

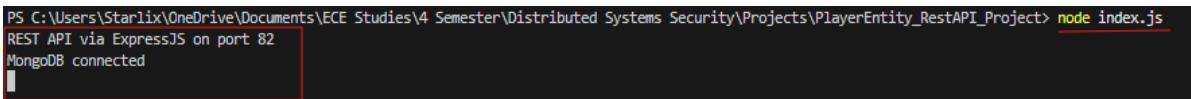


```
1 {  
2   "name": "1stnodejsproj",  
3   "version": "1.0.0",  
4   "description": "",  
5   "main": "index.js",  
6   "scripts": {  
7     "test": "\\"echo \\\\"$Error: no test specified\\\\" && exit 1\""  
8   },  
9   "author": "",  
10  "license": "ISC",  
11  "dependencies": {  
12    "bcrypt": "^6.0.0",  
13    "express": "4.22.1",  
14    "jsonwebtoken": "^9.0.3",  
15    "mongoose": "^9.1.2"  
16  }  
17}  
18}
```

Fig 9: node_modules and Installed dependencies referenced in the package.json

Step 5: Verify Environment Configuration

- The command node [index.js](#) was run to test the configuration.
- [Node.js](#) server running without errors, mongoDB connecting as seen below confirms the environment configuration was successfully done.



```
PS C:\Users\Starlix\OneDrive\Documents\ECE Studies\4 Semester\ Distributed Systems Security\Projects\PlayerEntity_RestAPI_Project> node index.js  
REST API via ExpressJS on port 82  
MongoDB connected
```

Fig 10: Successful server and database connection

2.3 Conclusion

This configuration is essential before API implementation as it ensures that errors are minimized during development, and that the application can be executed and tested reliably.

3.0 GLOBAL SYSTEM ARCHITECTURE

This section explains how responsibilities are divided inside the application for structure, clarity, and to enforce clean code organisation and predictable behaviour.

3.1 Architectural Layers

1. Client (Postman)
2. Routes (HTTP end points)
3. Middleware (Security checks)
4. Controllers (Business logic)
5. Models (Data structure and validation)
6. Database (Persistent storage)

3.2 Project Structure

Action: Manually create the following folders and files in the order below:

```
project/
    └── models/                               # Database structure (schemas)
        ├── Equipe.js                         # Team schema
        ├── Player.js                          # Player schema
        └── User.js                            # User model for authentication

    └── controllers/                          # Business rules/logic
        ├── equipe.js                         # Team logic
        ├── playerController.js               # Player logic
        └── authController.js                # Login/signup logic

    └── routes/                                # HTTP routing (API endpoints)
        ├── equipe.js                         # Team routes
        ├── players.js                        # Player routes
        └── auth.js                            # Login/signup routes

    └── middleware/                           # Security and request filtering
        └── auth.js                            # JWT verification middleware

    └── index.js                             # Application entry point
    └── package.json                         # Dependencies
```

3.3 Conclusion

The layered architecture and structure ensures clarity, maintainability, request handling, and reduced complexity.

4.0 DATABASE DESIGN AND DATA MODELING

The database layer stores all application data persistently.

4.1 Entities

Equipe (Team)

- Id (Automatically assigned by MongoDB)
- Name
- country

Player

- Id (Automatically assigned by MongoDB)
- name
- number
- position
- teamId (reference to Equipe)

Relationships

- One Equipe → Many Players
- Player references Equipe using MongoDB ObjectId

4.2 Database Creation and Setup

Step 1: Database Creation

The database is created automatically when the application connects. MongoDB creates the database.

Step 2: Collections Creation

Collections are automatically created by Mongoose when documents are inserted:

- equipe
- player
- users

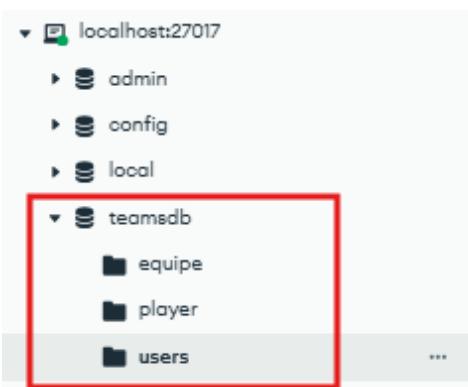


Fig 4.2: Created Database and Collections on MongoDB

4.3 Implement Database Models (Schemas)

Objective: Define how data is stored and validated in MongoDB.

Step 1: Team Model ([Equipe.js](#))

Purpose - Represent a team in the database.

Actions Performed:

- Create models/[Equipe.js](#)
- Define fields: name and country



```
JS Equipe.js x
1 const mongoose = require('mongoose');
2
3 const equipeSchema = new mongoose.Schema({
4   name: { type: String, required: true },
5   country: { type: String, required: true }
6 });
7
8 module.exports = mongoose.model('Equipe', equipeSchema, 'equipe');
```

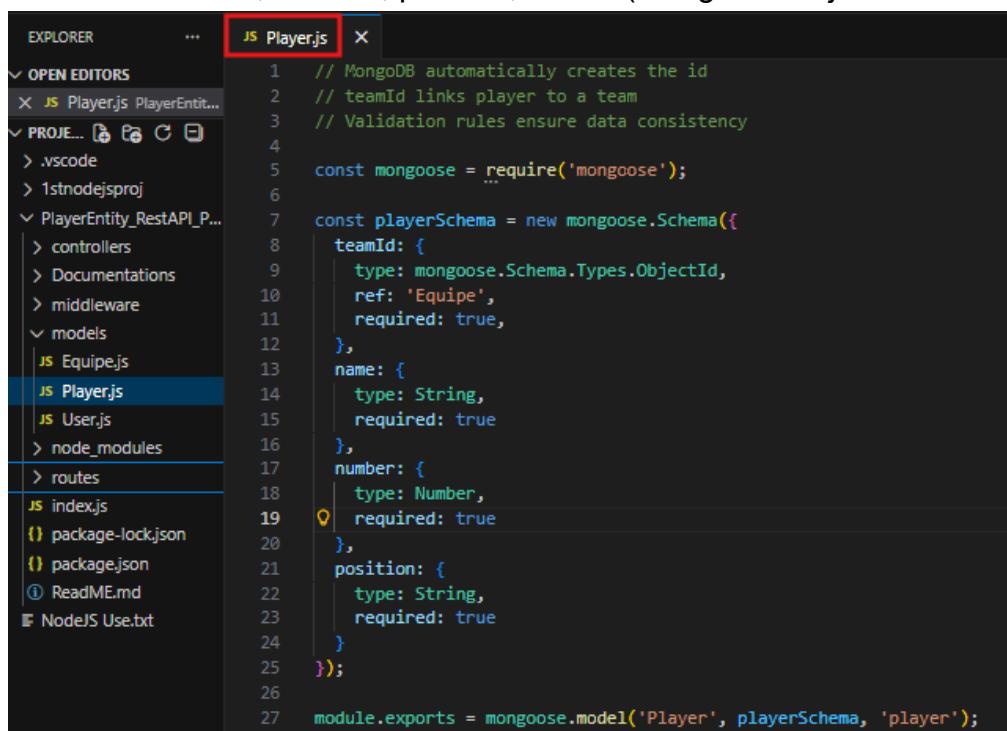
Fig 4.3.1: [Equipe.js](#) Schema Code

Step 2: Player Model ([Player.js](#))

Purpose - Represent a player and link them to a team using a reference.

Actions Performed:

- Create models/[Player.js](#)
- Define fields: name, number, position, teamId(MongoDB ObjectId reference)



```
EXPLORER ... JS Player.js x
OPEN EDITORS JS Player.js PlayerEntit...
PROJE... 🏛️ 🎯 ⚙️ 🔍
  > .vscode
  > 1stnodejsproj
  > PlayerEntity_RestAPI_P...
    > controllers
    > Documentations
    > middleware
      > models
        JS Equipe.js
        JS Player.js
        JS User.js
      > node_modules
      > routes
    JS index.js
  {} package-lock.json
  {} package.json
  README.md
  NodeJS Use.txt
1 // MongoDB automatically creates the id
2 // teamId links player to a team
3 // Validation rules ensure data consistency
4
5 const mongoose = ...
6
7 const playerSchema = new mongoose.Schema({
8   teamId: {
9     type: mongoose.Schema.Types.ObjectId,
10    ref: 'Equipe',
11    required: true,
12  },
13  name: {
14    type: String,
15    required: true
16  },
17  number: {
18    type: Number,
19    required: true
20  },
21  position: {
22    type: String,
23    required: true
24  }
25 });
26
27 module.exports = mongoose.model('Player', playerSchema, 'player');
```

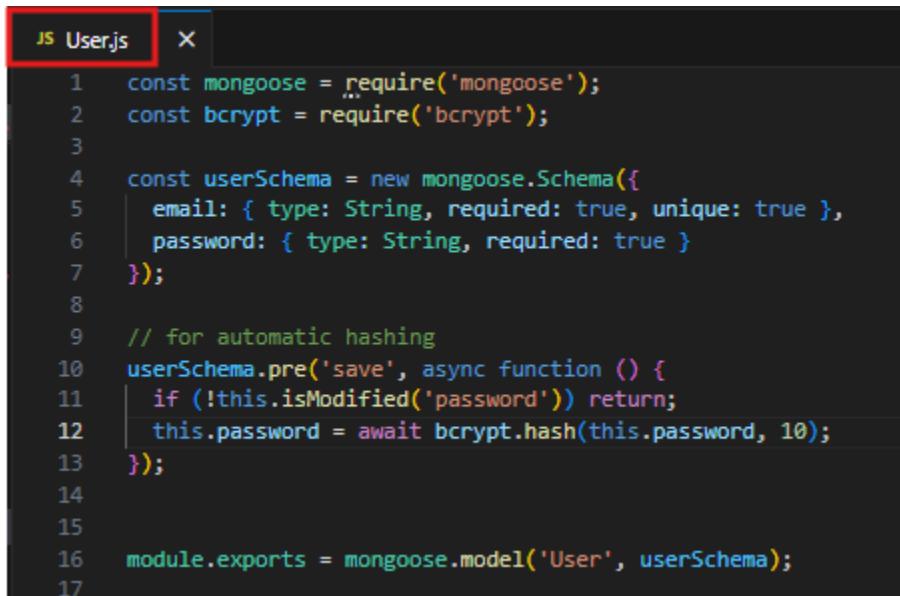
Fig 4.3.2: [Player.js](#) Schema Code

Step 3: User Model ([User.js](#))

Purpose - Stores users.

Actions Performed:

- Create models/[User.js](#)
- Define fields: email, password



```
JS User.js X
1 const mongoose = require('mongoose');
2 const bcrypt = require('bcrypt');
3
4 const userSchema = new mongoose.Schema({
5   email: { type: String, required: true, unique: true },
6   password: { type: String, required: true }
7 });
8
9 // for automatic hashing
10 userSchema.pre('save', async function () {
11   if (!this.isModified('password')) return;
12   this.password = await bcrypt.hash(this.password, 10);
13 });
14
15
16 module.exports = mongoose.model('User', userSchema);
17
```

Fig 4.3.3: [Equipe.js](#) Schema Code

4.4 Conclusion:

MongoDB combined with Mongoose allows automatic database creation, schema validation, and scalable data storage without manual SQL setup. Models formally define the database structure and relationships. Using references ensures scalability and avoids data duplication.

5.0 APPLICATION IMPLEMENTATION AND REQUEST PROCESSING

5.1 Implement Controllers (Business Logic)

Objective: Centralize all application logic and data handling separately from routing to ensure scalability.

CRUD Operations handled by Controllers:

Create (POST) - Adds new resources to the database.

- Accepts JSON input
- Validates data
- Stores it in MongoDB

Read (GET) - Retrieves one or multiple resources.

- Does not modify data

Update (PUT) - Modifies an existing resource.

- Locates an existing resource
- Modifies existing data with new data
- Saves the modified data back to the database

Delete (DELETE)- Removes a resource permanently.

CRUD operations form the foundation of all data-driven systems and are implemented as below:

Step 1 - Team Controller ([Equipe.js](#))

Purpose: Handles all team related operations

Actions Performed:

- Create controller/[Equipe.js](#)
- Implement CRUD logic for team:
 - Create team
 - Get all teams
 - Get team by ID
 - Update team
 - Delete team

```

EXPLORER      ...
OPEN EDITORS  JS Equipe.js X
PROJECTS
  > .vscode
  > 1stnodejsproj
  > PlayerEntity_RestAPI_P...
    controllers
      authController.js
      Equipe.js
      playerController.js
    Documentation
    middleware
    models
    node_modules
    routes
    index.js
  {} package-lock.json
  {} package.json
  README.md
  NodeJS Use.txt

1  const Equipe = require('../models/Equipe');
2
3  // Get all teams
4  exports.getAllEquipes = async (req, res) => {
5    const equipes = await Equipe.find();
6    res.status(200).json(equipes);
7  };
8
9  // Get team by ID
10 exports.getEquipeById = async (req, res) => {
11   try {
12     const equipe = await Equipe.findById(req.params.id);
13     if (!equipe) return res.status(404).json({ message: "Team not found" });
14     res.status(200).json(equipe);
15   } catch {
16     res.status(400).json({ message: "Invalid ID" });
17   }
18 };
19
20 // Create a new team
21 exports.createEquipe = async (req, res) => {
22   const { name, country } = req.body;
23   const equipe = new Equipe({ name, country });
24   await equipe.save();
25   res.status(201).json(equipe);
26 };
27
28 // Update team
29 exports.updateEquipe = async (req, res) => {
30   try {
31     const equipe = await Equipe.findByIdAndUpdate(req.params.id, req.body, { new: true, runValidators: true });
32     if (!equipe) return res.status(404).json({ message: "Team not found" });
33     res.status(200).json(equipe);
34   } catch {
35     res.status(400).json({ message: "Invalid ID or data" });
36   }
37 };
38
39 // Delete team
40 exports.deleteEquipe = async (req, res) => {
41   try {
42     const equipe = await Equipe.findByIdAndDelete(req.params.id);
43     if (!equipe) return res.status(404).json({ message: "Team not found" });
44     res.status(200).json({ message: "Team deleted" });
45   } catch {
46     res.status(400).json({ message: "Invalid ID" });
47   }
48 };
49

```

Fig 5.1.1: [Equipe.js](#) with CRUD functions

Step 2 - Player Controller ([playerController.js](#))

Purpose: Handles players operations and entity relationships.

Actions Performed:

- Create controller/[playerController.js](#)
- Implement CRUD logic for players:
 - Create player
 - Get all players
 - Get player by playerID
 - Update player
 - Delete player
- Get players on a team by teamID
- Get team of a player by player ID
- Placeholder search by name

```
JS playerController.js ●
1  const Player = require('../models/Player');
2  const Equipe = require('../models/Equipe');
3
4  // Create a new player using team name instead of manually providing teamId
5  exports.createPlayer = async (req, res) => {
6    try {
7      const { teamName, name, number, position } = req.body;
8
9      // Find the team dynamically by its name
10     const team = await Equipe.findOne({ name: teamName });
11     if (!team) return res.status(404).json({ message: "Team not found" });
12
13     // Create player with the proper teamId
14     const player = new Player({
15       teamId: team._id,
16       name,
17       number,
18       position
19     });
20
21     await player.save();
22     res.status(201).json(player);
23   } catch (err) {
24     res.status(500).json({ message: "Error creating player", error: err.message });
25   }
26 };
27
28 exports.createPlayersBulk = async (req, res) => {
29   try {
30     const { teamName, players } = req.body; // expect teamName + array of players
31
32     const team = await Equipe.findOne({ name: teamName });
33     if (!team) return res.status(404).json({ message: "Team not found" });
34
35     // Add teamId to each player
36     const playersWithTeam = players.map(p => ({
37       ...p,
38       teamId: team._id
39     }));
40
41     const result = await Player.insertMany(playersWithTeam);
42     res.status(201).json(result);
43   } catch (err) {
44     res.status(400).json({ message: "Invalid data", error: err.message });
45   }
46 };
```

```
48 // Get all players
49 exports.getAllPlayers = async (req, res) => {
50   const players = await Player.find();
51   res.status(200).json(players);
52 };
53
54 // Get player by ID
55 exports.getPlayerById = async (req, res) => {
56   try {
57     const player = await Player.findById(req.params.id);
58     if (!player) return res.status(404).json({ message: "Player not found" });
59     res.status(200).json(player);
60   } catch {
61     res.status(400).json({ message: "Invalid ID" });
62   }
63 };
64
65 // Update player
66 exports.updatePlayer = async (req, res) => {
67   try {
68     const player = await Player.findByIdAndUpdate(req.params.id, req.body, { new: true, runValidators: true });
69     if (!player) return res.status(404).json({ message: "Player not found" });
70     res.status(200).json(player);
71   } catch {
72     res.status(400).json({ message: "Invalid ID or data" });
73   }
74 };
75
76 // Delete player
77 exports.deletePlayer = async (req, res) => {
78   try {
79     const player = await Player.findByIdAndDelete(req.params.id);
80     if (!player) return res.status(404).json({ message: "Player not found" });
81     res.status(200).json({ message: "Player deleted" });
82   } catch {
83     res.status(400).json({ message: "Invalid ID" });
84   }
85 };
86
87 // List all players on a team
88 exports.getPlayersByTeam = async (req, res) => {
89   const players = await Player.find({ teamId: req.params.teamId });
90   res.status(200).json(players);
91 };
92
93 // Get the team of a player
94 exports.getTeamByPlayer = async (req, res) => {
95   try {
96     const player = await Player.findById(req.params.id);
97     if (!player) return res.status(404).json({ message: "Player not found" });
98
99     const team = await Equipe.findById(player.teamId);
100    if (!team) return res.status(404).json({ message: "Team not found" });
101
102    res.status(200).json(team);
103  } catch {
104    res.status(400).json({ message: "Invalid ID" });
105  }
106};
```

```
117 // Placeholder search by name
118 exports.searchPlayerByName = async (req, res) => {
119   const { name } = req.params;
120   try {
121     const players = await Player.find({ name: { $regex: name, $options: "i" } });
122     res.status(200).json(players);
123   } catch (err) {
124     res.status(500).json({ message: "Server error", error: err });
125   }
126};
```

Fig 5.1.2: [playerController.js](#) showing relationship queries

Step 3 - Authentication Controller ([authController.js](#))

Authentication and Authorization was done using JWT.

Authentication Flow:

- User signs up
- Password is hashed
- User logs in
- JWT is issued
- Token is used in protected requests

Purpose: Manages authentication and token issuance.

Actions Performed:

- Create controller/[authController.js](#)
- Implement CRUD logic for players:
 - Signup (hash password using bcrypt)
 - Login (verify password)
 - JWT token generation

```
const User = require('../models/User');
const bcrypt = require('bcrypt');
const jwt = require('jsonwebtoken');

// SIGNUP
exports.signup = async (req, res) => {
  try {
    console.log('Request body:', req.body); // check if body is received

    const { email, password } = req.body;
    if (!email || !password) {
      return res.status(400).json({ error: 'Email and password are required' });
    }

    // Check if user exists
    const existingUser = await User.findOne({ email });
    console.log('Existing user:', existingUser);

    if (existingUser) {
      return res.status(409).json({ error: 'User already exists' });
    }

    const user = new User({ email, password });
    await user.save();

    res.status(201).json({ message: 'User created successfully' });
  } catch (error) {
    console.error('Signup error:', error);
    res.status(500).json({ error: error.message });
  }
};

// LOGIN Verifies password and returns JWT
exports.login = async (req, res) => {
  const { email, password } = req.body;

  const user = await User.findOne({ email });
  if (!user) {
    return res.status(401).json({ error: 'User not found' });
  }

  const valid = await bcrypt.compare(password, user.password);
  if (!valid) {
    return res.status(401).json({ error: 'Incorrect password' });
  }

  const token = jwt.sign(
    { userId: user._id },
    'RANDOM_TOKEN_SECRET',
    { expiresIn: '24h' }
  );

  res.status(200).json({ userId: user._id, token });
};
```

Fig 5.1.3: [authController.js](#) signup and login logic

Conclusion: Controllers cover all business rules and database interactions. Authentication controllers protect sensitive operations and identify users. Using JWT enables secure and scalable authentication.

5.2 Implement Routes (HTTP Endpoints)

Objective: Expose controllers through RESTful URLs.

Step 1 - Team Routes([Equipe.js](#))

Actions Performed:

- Create *routes/[Equipe.js](#)*
- Map HTTP methods to controller functions:
 - GET
 - POST
 - PUT
 - DELETE

```
JS Equipe.js X
1 const express = require('express');
2 const router = express.Router();
3 const equipeController = require('../controllers/Equipe');
4
5 // CRUD routes for equipe
6 router.get('/', equipeController.getAllEquipes);
7 router.get('/:id', equipeController.getEquipeById);
8 router.post('/', equipeController.createEquipe);
9 router.put('/:id', equipeController.updateEquipe);
10 router.delete('/:id', equipeController.deleteEquipe);
11
12 module.exports = router;
13
```

Fig 5.2.1: routes/[Equipe.js](#)

Step 2 - Player Routes(routes/[players.js](#))

Actions Performed:

- Create *routes/[players.js](#)*
- Define routes for:
 - GET
 - POST
 - PUT
 - DELETE
 - Players by team
 - Team by player
 - Search placeholder

The screenshot shows a code editor window with a dark theme. The tab bar at the top has a red box around the 'JS players.js' tab. The main area contains 20 numbered lines of JavaScript code. Lines 1 through 13 define a Router for player operations, including CRUD methods and special routes like '/team/:teamId'. Lines 14 through 19 define additional special routes. Line 20 exports the router.

```
1 const express = require('express');
2 const router = express.Router();
3 const auth = require('../middleware/auth');
4 const playerController = require('../controllers/playerController');
5
6 // CRUD routes for players: private APIs must have the middleware-auth for protection
7 router.get('/', auth, playerController.getAllPlayers);
8 router.get('/:id', auth, playerController.getPlayerById);
9 router.post('/bulk', auth, playerController.createPlayersBulk);
10 router.post('/', auth, playerController.createPlayer);
11 router.put('/:id', auth, playerController.updatePlayer);
12 router.delete('/:id', auth, playerController.deletePlayer);
13
14 // Special routes
15 router.get('/team/:teamId', playerController.getPlayersByTeam);
16 router.get('/:id/team', playerController.getTeamByPlayer);
17 router.get('/search/:name', playerController.searchPlayerByName);
18
19 module.exports = router;
20
```

Fig 5.2.2:routes/[players.js](#)

Step 3 - Authentication Routes(routes/[auth.js](#))

Actions Performed:

- Create *routes/auth.js*
- Define routes:
 - POST /signup
 - POST /login

The screenshot shows a code editor window with a dark theme. The tab bar at the top has a red box around the 'JS auth.js' tab. The main area contains 9 numbered lines of JavaScript code. Lines 1 through 8 define a Router for authentication, specifically for 'signup' and 'login' endpoints. Line 9 exports the router.

```
1 const express = require('express');
2 const router = express.Router();
3 const authController = require('../controllers/authController');
4
5 router.post('/signup', authController.signup);
6 router.post('/login', authController.login);
7
8 module.exports = router;
9
```

Fig 5.2.3: routes/[auth.js](#)

Conclusion:

Routes connect external HTTP requests to internal logic.

5.3 Implement Authentication Middleware

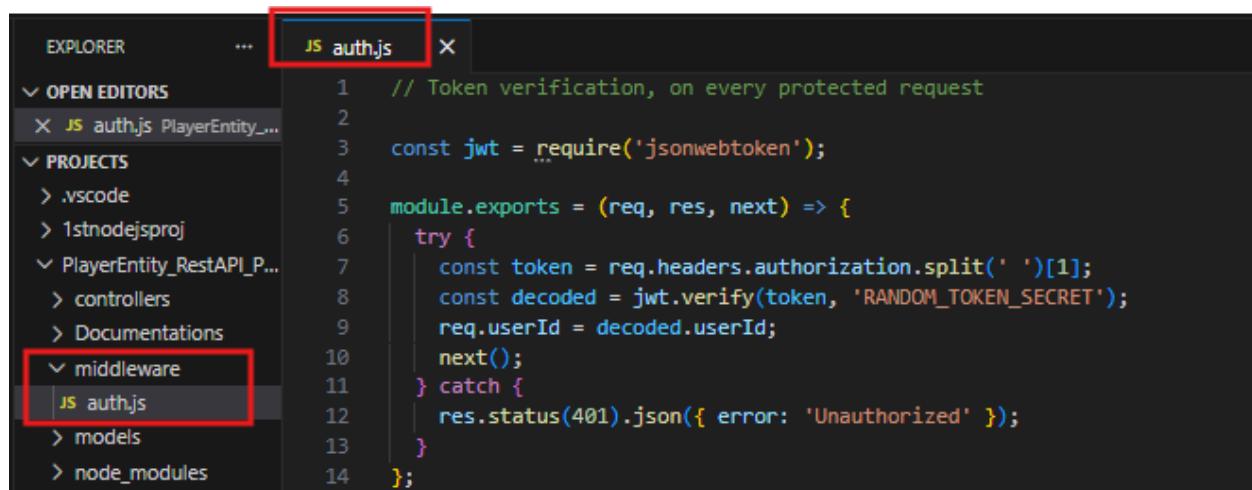
Objective: Protect sensitive routes using JWT verification.

Middleware and Security Enforcement

Purpose - Apply security checks before controllers are executed. It is responsible for token extraction, verification and request blocking or forwarding. Middleware centralizes security logic.

Actions Performed:

- Create *middleware/auth.js*
- Extract token from request header
- Verify token validity
- Allow or block request



The screenshot shows the VS Code interface. In the Explorer sidebar, there is a tree view of project files. A red box highlights the 'middleware' folder, which contains an 'auth.js' file, also highlighted with a red box. The code editor shows the contents of the auth.js file:

```
// Token verification, on every protected request
const jwt = require('jsonwebtoken');
module.exports = (req, res, next) => {
  try {
    const token = req.headers.authorization.split(' ')[1];
    const decoded = jwt.verify(token, 'RANDOM_TOKEN_SECRET');
    req.userId = decoded.userId;
    next();
  } catch {
    res.status(401).json({ error: 'Unauthorized' });
  }
};
```

Fig 5.2.3: middleware/auth.js

Conclusion:

This ensures that security is enforced consistently across protected routes preventing unauthorized access to them.

5.4 Implement Application Entry Point

Objective: This ties the entire application together.

Actions Performed:

- Initialize Express
- Connect to MongoDB
- Register middleware
- Register routes
- Start server on port 82

```
1 const express = require('express');
2 const mongoose = require('mongoose');
3
4 const authRoutes = require('./routes/auth');
5 const equipeRoutes = require('./routes/Equipe');
6 const playerRoutes = require('./routes/players');
7
8 const app = express();
9 app.use(express.json());
10
11 // Connect to MongoDB
12 mongoose.connect('mongodb://127.0.0.1:27017/teamsdb')
13   .then(() => console.log('MongoDB connected'))
14   .catch(err => console.error(err));
15
16 // Routes
17 app.use('/equipes', equipeRoutes);
18 app.use('/players', playerRoutes);
19 app.use('/auth', authRoutes);
20
21 app.listen(82, () => console.log('REST API via ExpressJS on port 82'));
22
```

Fig 5.2.3: [index.js](#) showing `app.use()`, `mongoose.connect()`, `app.listen()`

Conclusion:

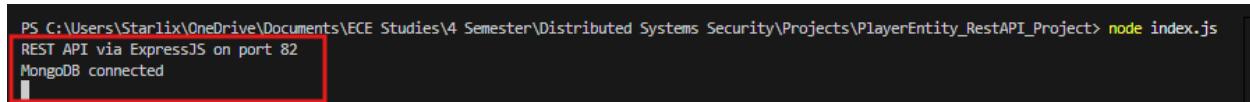
This ensures that the application becomes executable and accessible.

6.0 TESTING AND VERIFICATION USING POSTMAN

Purpose - Validate correctness, security, and stability of the REST API

6.1 Precondition

- [Node.js](#) server is running
- MongoDB service is running
- Collections exists



```
PS C:\Users\Starlix\OneDrive\Documents\ECE Studies\4 Semester\ Distributed Systems Security\Projects\PlayerEntity_RestAPI_Project> node index.js
REST API via ExpressJS on port 82
MongoDB connected
```

Fig 6.1: Running services

6.2 Step by Step Testing of All API Endpoints

Step 1: User Signup Test

- Send POST requests to /auth/signup
- Provide email and password
- **INPUT:**

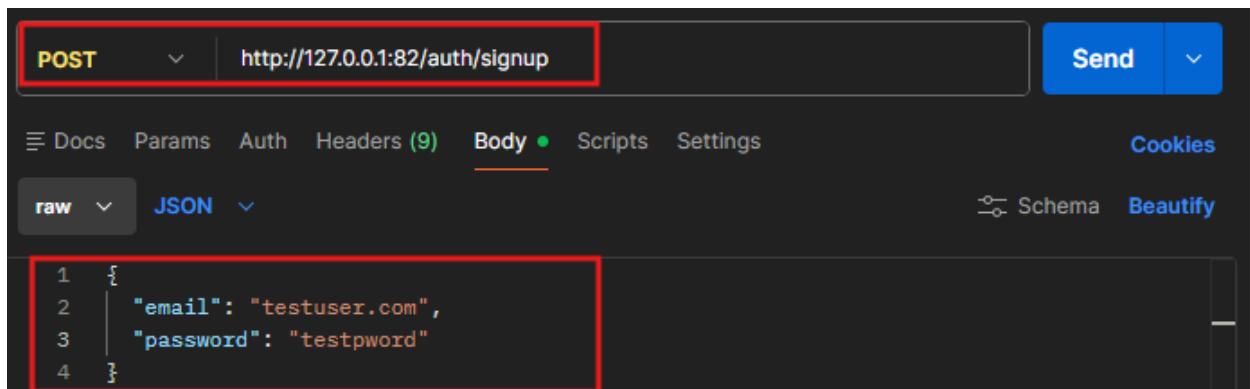


Fig 6.2.1a: Signup Request

- **OUTPUT:**

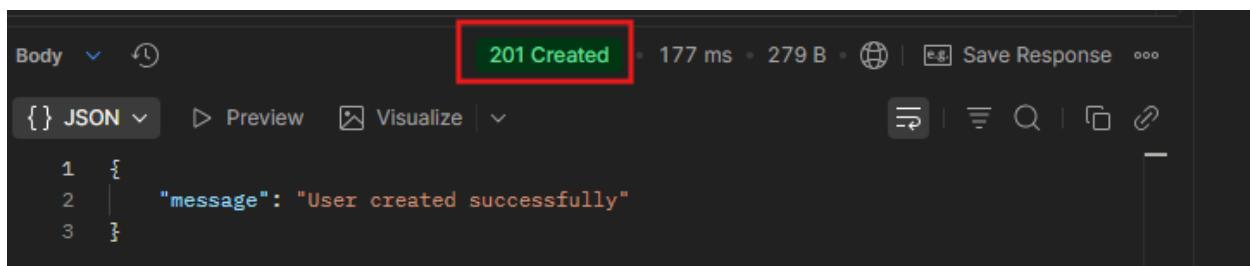


Fig 6.2.1b: Output of Signup Request (Successful user creation)

```

_id: ObjectId('69696e1c8355642a48efa59f')
email : "testuser.com"
password : "$2b$10$/52o33GgK5BEaePI/a08Ce/dBNSJQIFQTr9ikI1mvChTKAMOrBP0y"
__v : 0

```

Fig 6.2.1c: Created user as saved in the database

Step 2: User Login Test

- Send POST requests to /auth/login
- Receive JWT token
- INPUT:

POST http://127.0.0.1:82/auth/login

Body (JSON)

```

1 {
2   "email": "testuser.com",
3   "password": "testpwdword"
4 }

```

Fig 6.2.2a: Login request using created user credentials

- OUTPUT:

200 OK

Body (JSON)

```

1 {
2   "userId": "69696e1c8355642a48efa59f",
3   "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiI2OTY5NmUxYzgzNTU2NDJhNDhlZmE10WYiLCJpYXQiOjE3Njg1MTc2NDAsImV4cCI6MTc2ODYwNDA0MH0.ZvoYN4_c_IoeVKTp6Uszzj0jVrY8hHzt7f_bgLQ5Fiw"
4 }

```

Fig 6.2.2b: Login response containing JWT

Step 3: Access Protected Route Without Token (Create Player)

- Call POST /players without Authorization header

→ INPUT:

Attempted to create a player through a protected route without an authorization header.

The screenshot shows the Postman interface. A red box highlights the URL field containing "http://127.0.0.1:82/players". The method dropdown shows "POST". The "Body" tab is selected, and a red box highlights the JSON payload:

```
1 {  
2   "teamName": "PSG",  
3   "name": "Dembele",  
4   "number": 10,  
5   "position": "Forward"  
6 }
```

Fig 6.2.3a: Create Player without Authorization header

→ OUTPUT:

The screenshot shows the Postman interface after sending the request. A red box highlights the status code "401 Unauthorized". The response body is shown in JSON format, with a red box highlighting the error message:

```
1 {  
2   "error": "Unauthorized"  
3 }
```

Fig 6.2.3b: 401 Unauthorized response

Step 4: Access Protected Route With Token (Create Player)

- Add header: Authorization: Bearer <token>
- Call POST /players with Authorization header

→ INPUT:

The screenshot shows the Postman interface with the Authorization header added. A red box highlights the "Headers" tab, which is selected. Another red box highlights the "Authorization" key in the headers table, where a value is entered:

Key	Value	Description
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc2Vy...	

Fig 6.2.4a: Create Player with Authorization header

→ OUTPUT:

The screenshot shows a Postman interface with the following details:

- Body tab selected.
- JSON response:

```
1 {  
2   "teamId": "69696c3943ba5ee5f28b7e46",  
3   "name": "Dembele",  
4   "number": 10,  
5   "position": "Forward",  
6   "_id": "696974328355642a48efa5a3",  
7   "__v": 0  
8 }
```
- Status bar: 201 Created, 22 ms.

Fig 6.2.4b: Successful protected request

→ Database Output:

The screenshot shows the MongoDB Compass interface with the following details:

- Database: teamsdb, Collection: player.
- Documents tab selected, showing 1 document.
- Document details:

```
_id: ObjectId('696974328355642a48efa5a3')  
teamId : ObjectId('69696c3943ba5ee5f28b7e46')  
name : "Dembele"  
number : 10  
position : "Forward"  
__v : 0
```

Fig 6.2.4c: Created Player on the database

Step 5: Other CRUD Validation

→ Create, read, update, delete players

1. GET ALL PLAYERS:

→ INPUT:

The screenshot shows a Postman interface with the following details:

- Method: GET, URL: http://127.0.0.1:82/players.
- Headers tab selected, showing an Authorization header with value: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpxVCJ9eyJ1c2VySWQiOiI2...

Fig 6.2.5a: Get all Players request

→ OUTPUT:

The screenshot shows a REST API response in JSON format. The status bar at the top right indicates "200 OK". The response body contains a list of five player documents, each with fields: _id, teamId, name, number, position, and __v. The players listed are Dembele, Lamine, Mbappe, Raphinha, and Hernandez.

```

1 [ 
2   { 
3     "_id": "696974328355642a48efa5a3",
4     "teamId": "69696c3943ba5ee5f28b7e46",
5     "name": "Dembele",
6     "number": 10,
7     "position": "Forward",
8     "__v": 0
9   },
10  { 
11    "_id": "696979b58355642a48efa5a6",
12    "teamId": "69696c3943ba5ee5f28b7e47",
13    "name": "Lamine",
14    "number": 10,
15    "position": "Right Winger",
16    "__v": 0
17  },
18  { 
19    "_id": "69697a548355642a48efa5a9",
20    "teamId": "69696c3943ba5ee5f28b7e48",
21    "name": "Mbappe",
22    "number": 10,
23    "position": "Forward",
24    "__v": 0
25  },
26  { 
27    "_id": "69697abd8355642a48efa5ac",
28    "teamId": "69696c3943ba5ee5f28b7e47",
29    "name": "Raphinha",
30    "number": 11,
31    "position": "Forward",
32    "__v": 0
33  },
34  { 
35    "_id": "69697d358355642a48efa5b3",
36    "teamId": "69696c3943ba5ee5f28b7e49",
37    "name": "Hernandez",
38    "number": 19,
39    "position": "Fullback",
40    "__v": 0
41  }
42 ]

```

Fig 6.2.5b: All Players retrieved from database

2. DELETE PLAYER:

→ INPUT:

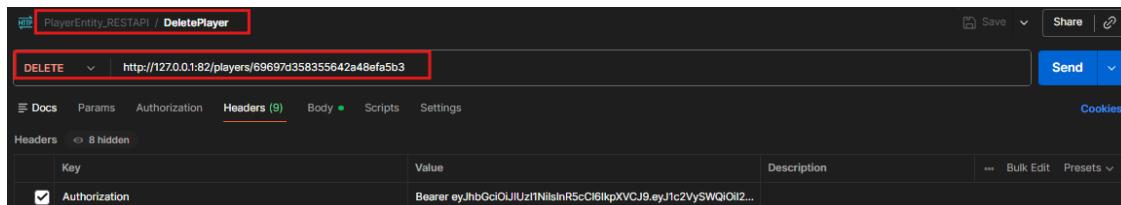


Fig 6.2.6a Delete a player request

→ OUTPUT:

The screenshot shows a REST API response in JSON format. The status bar at the top right indicates "200 OK". The response body contains a single object with a message field: "Player deleted".

```

1 { 
2   "message": "Player deleted"
3 }

```

Fig 6.2.6b: Player deleted

3. GET PLAYER BY ID:

→ INPUT:

The screenshot shows the Postman interface with the following details:

- Method: GET
- URL: http://127.0.0.1:82/players/6969856b8355642a48efa5bb
- Headers: (6)
- Body: (selected)
- Test Results: (disabled)
- Send button
- Cookies tab

A red box highlights the URL field.

Fig 6.2.7a: Get Player by ID request

→ OUTPUT:

The screenshot shows the Postman interface with the following details:

- Body: (selected)
- JSON response:

```
1 {  
2   "_id": "6969856b8355642a48efa5bb",  
3   "teamId": "69696c3943ba5ee5f28b7e49",  
4   "name": "Hernandez",  
5   "number": 17,  
6   "position": "Fullback",  
7   "__v": 0  
8 }
```

A red box highlights the JSON response body.
- Test Results: (disabled)
- 200 OK status

Fig 6.2.7b: Get Player by ID success output

4. UPDATE PLAYER:

→ INPUT:

The screenshot shows the Postman interface with the following details:

- Method: PUT
- URL: http://127.0.0.1:82/players/6969856b8355642a48efa5bb
- Headers: (9)
- Body: (selected)
- Test Results: (disabled)
- Send button
- Cookies tab
- Schema and Beautify buttons

A red box highlights the URL field.

Fig 6.2.8a: Update Player number request

→ OUTPUT:

The screenshot shows the Postman interface with the following details:

- Body: (selected)
- JSON response:

```
1 {  
2   "_id": "6969856b8355642a48efa5bb",  
3   "teamId": "69696c3943ba5ee5f28b7e49",  
4   "name": "Hernandez",  
5   "number": 19,  
6   "position": "Fullback",  
7   "__v": 0  
8 }
```

A red box highlights the JSON response body.
- Test Results: (disabled)
- 200 OK status

Fig 6.2.8b: Player number updated successfully

5. GET ALL PLAYERS IN TEAM

→ INPUT:

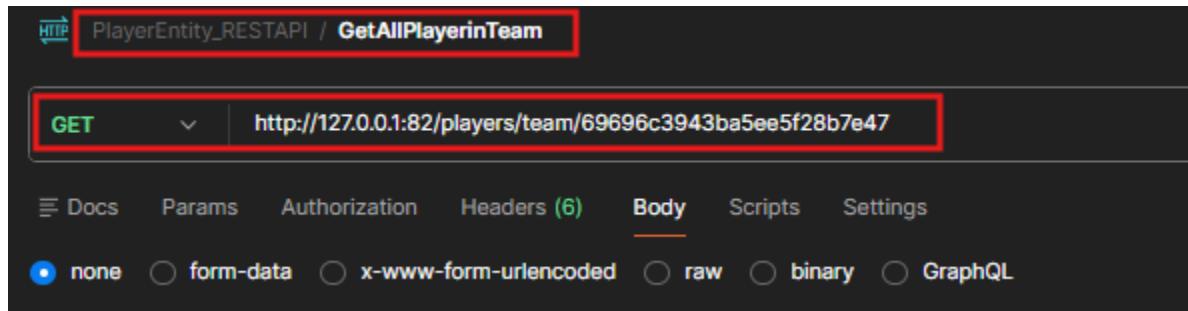


Fig 6.2.9a: Get Players in team request

→ OUTPUT:

The screenshot shows the POSTMAN interface with the response body displayed. The status code '200 OK' is highlighted with a red box. The response body is a JSON array containing two player objects. The first player is Lamine (id: 696979b58355642a48efa5a6, number: 10, position: Right Winger). The second player is Raphinha (id: 69697abd8355642a48efa5ac, number: 11, position: Forward). Both players have an __v field set to 0.

```
[{"_id": "696979b58355642a48efa5a6", "teamId": "69696c3943ba5ee5f28b7e47", "name": "Lamine", "number": 10, "position": "Right Winger", "__v": 0}, {"_id": "69697abd8355642a48efa5ac", "teamId": "69696c3943ba5ee5f28b7e47", "name": "Raphinha", "number": 11, "position": "Forward", "__v": 0}]
```

Fig 6.2.9b: Players in team successfully retrieved

6. GET TEAM OF PLAYER

→ INPUT:

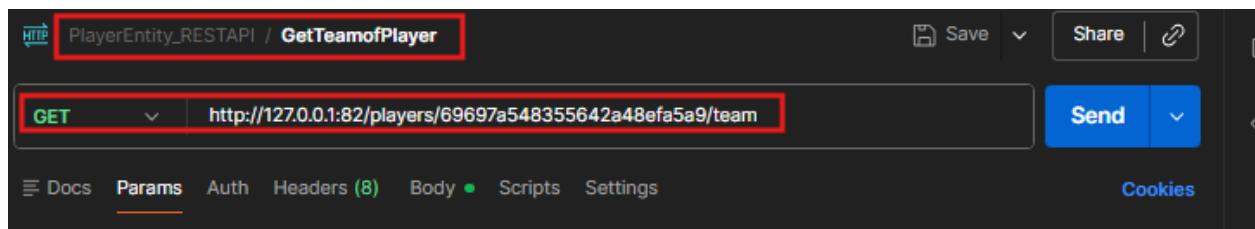


Fig 6.2.10a: Get Players team request

→ OUTPUT:

The screenshot shows a Postman request for a team retrieval endpoint. The response status is 200 OK, with a duration of 18 ms and a size of 310 B. The response body is a JSON object containing the team's ID, name, and country.

```
1 {  
2   "_id": "69696c3943ba5ee5f28b7e48",  
3   "name": "Real Madrid",  
4   "country": "Espagne"  
5 }
```

Fig 6.2.10b: Player team successfully retrieved

7. Search by Name

→ INPUT:

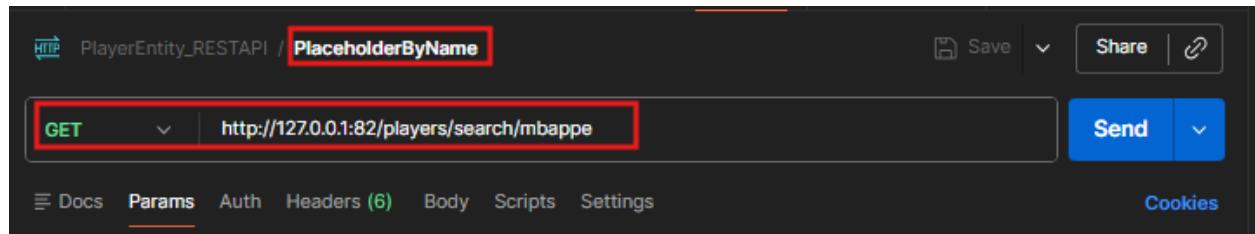


Fig 6.2.11a: Placeholder Search by Name Sample Request

→ OUTPUT:

The screenshot shows the result of the placeholder search by name request. The response status is 200 OK. The response body is a JSON array containing one element, which is a document representing a player named Mbappe.

```
1 [  
2   {  
3     "_id": "69697a548355642a48efa5a9",  
4     "teamId": "69696c3943ba5ee5f28b7e48",  
5     "name": "Mbappe",  
6     "number": 10,  
7     "position": "Forward",  
8     "__v": 0  
9   }  
10 ]
```

Fig 6.2.11a: Placeholder Search by Name Result

6.3 Detailed Flow of Request

A. GETALLPLAYERS

Step 1 - Client Request

- The client sends an HTTP GET request to /players

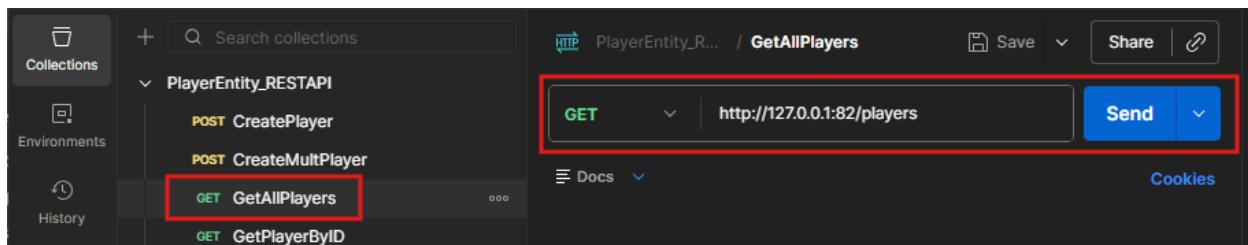


Fig 6.3.1: Postman configured with GET /players

Step 2 - Routing

- Express receives the request
- The /players route matches the request

```
router.get('/', auth, playerController.getAllPlayers);
```

Fig 6.3.2: routes/[players.js](#) showing GET route

Step 3 - Middleware Execution (if enabled)

- JWT middleware checks authorization header
- Request is allowed or blocked

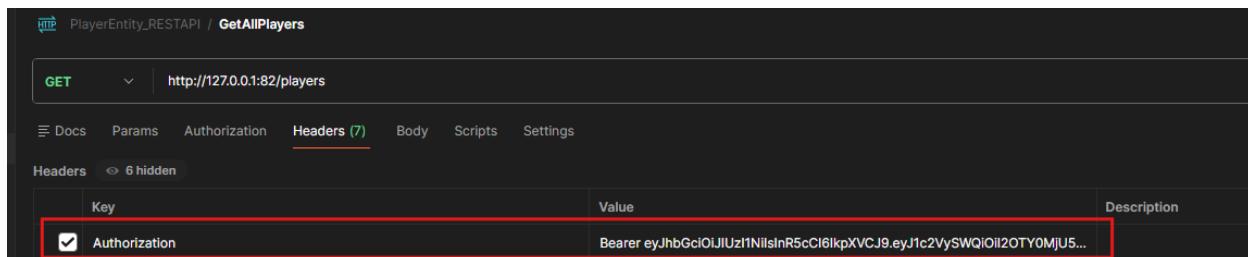


Fig 6.3.3: Authorization header in Postman

Step 4 - Controller Execution

- The controller function getAllPlayers() is called.
- MongoDB query find() is executed

```
// Get all players
exports.getAllPlayers = async (req, res) => {
  const players = await Player.find();
  res.status(200).json(players);
};
```

Fig 6.3.4: [playerController.js](#) logic for Get all players

Step 5 - Database Response

- MongoDB returns all player documents

The screenshot shows the MongoDB Compass interface. At the top, the address bar displays "localhost:27017 > teamsdb > player". To the right of the address bar is a button labeled "Open Mon". Below the address bar, there are tabs for "Documents" (0), "Aggregations", "Schema", "Indexes" (1), and "Validation". The "Documents" tab is selected. A search bar at the top says "Type a query: { field: 'value' } or Generate query" with a "Find" button next to it. Below the search bar are buttons for creating (+), updating (edit), deleting (trash), and a refresh icon. On the right side, there are buttons for "25" (page size), "1 - 4 of 4" (total results), and navigation arrows. A "Reset" button is also present. The main area contains four documents, each with a red border around its content. The first document is for Dembele, the second for Lamine, the third for Mbappe, and the fourth for Raphinha. Each document includes fields like _id, teamId, name, number, position, and __v.

```
_id: ObjectId('696974328355642a48efa5a3')
teamId : ObjectId('69696c3943ba5ee5f28b7e46')
name : "Dembele"
number : 10
position : "Forward"
__v : 0

_id: ObjectId('696979b58355642a48efa5a6')
teamId : ObjectId('69696c3943ba5ee5f28b7e47')
name : "Lamine"
number : 10
position : "Right Winger"
__v : 0

_id: ObjectId('69697a548355642a48efa5a9')
teamId : ObjectId('69696c3943ba5ee5f28b7e48')
name : "Mbappe"
number : 10
position : "Forward"
__v : 0

_id: ObjectId('69697abd8355642a48efa5ac')
teamId : ObjectId('69696c3943ba5ee5f28b7e47')
name : "Raphinha"
number : 11
position : "Forward"
__v : 0
```

Fig 6.2.5: MongoDB Compass showing player collection

Step 6.6 - API Response

- Server returns HTTP 200
- JSON array of players is sent

The screenshot shows a Postman interface with the following details:

- Request URL:** http://127.0.0.1:82/players
- Method:** GET
- Headers:** Authorization: Bearer eyJhbGciOiJIUzI1Nils...
- Status:** 200 OK
- Body:** JSON response containing four player documents. The response body is highlighted with a red box.

```
10  [
11    {
12      "_id": "6962b0e48f2b58927b9da414",
13      "teamId": "69629f96b075ad1e7e702052",
14      "name": "Mbappe",
15      "number": 7,
16      "position": "Forward",
17      "__v": 0
18    },
19    {
20      "_id": "6962b0e48f2b58927b9da415",
21      "teamId": "69629f96b075ad1e7e702052",
22      "name": "Hakimi",
23      "number": 2,
24      "position": "Defender",
25      "__v": 0
26    },
27    {
28      "_id": "696432d6a2fc213d7b6e3284",
29      "teamId": "696432b2a2fc213d7b6e3280",
30      "name": "Lookman",
31      "number": 2,
32      "position": "Defender",
33      "__v": 0
34    },
35    {
36      "_id": "6964338c11185404cbabe17f",
37      "teamId": "696432b2a2fc213d7b6e3280",
38      "name": "Iwobi",
39      "number": 7,
40      "position": "Forward",
        "__v": 0
    }
]
```

Fig 6.2.6: Postman response body

Conclusion:

This flow shows the complete lifecycle of a REST request from client to database and back to client. This explains how a single API request is processed end-to-end, and how all components function together as designed.

FINAL CONCLUSION

This step-by-step implementation shows how a secure, modular REST API is built from the ground up. Each component plays a clearly defined role, making the system maintainable, scalable, and secure.

The implementation was done using [Node.js](#) and Express for server-side logic, MongoDB for data storage, and JSON Web Tokens (JWT) for authentication and authorization. The workflow covered environment setup, database configuration, data modeling, REST API design, controller logic implementation, route definition, middleware integration, and systematic testing with Postman.

The resulting system supports:

- Persistent data storage using MongoDB.
- Full CRUD operations for related entities (Equipe and Players)
- Secure operations using JWT-based authentication.
- Clear separation of concerns through models, controllers, routes, and middleware.
- Scalable architecture

The project reinforced concepts like entity relationships, stateless HTTP communication, middleware-based security, and structured API workflows.

Finally, this report provides a step-by-step guide that allows the system to be reproduced reliably.

APPENDIX

A. API Endpoint Reference

Method	Endpoint	Description	Authentication
POST	/auth/signup	Create user	No
POST	/auth/login	Authenticate user	No
GET	/players	Get all players	Yes
GET	/players/:id	Returns one specific player	No
POST	/players	Create player	Yes
PUT	/players/:id	Updates data of an existing player using its ID	Yes
DELETE	/players/:id	Deletes a player from the database	Yes
GET	/players/:id/team	Get the team of specified player	No
GET	/players/team/:teamId	Display players of a Team	No
GET	/players/search/name?name=value	Name-based search	No

B. Collection and Requests Created on Postman

Add requests for each endpoint using HTTP method + URL:

- POST http://127.0.0.1:82/auth/signup -> create user (password hashed)
- POST http://127.0.0.1:82/auth/login -> login, returns JWT
- GET http://127.0.0.1:82/players -> list all players
- GET <http://127.0.0.1:82/players/:id> -> Get player using their ID
- POST http://127.0.0.1:82/players -> create one player
- PUT http://127.0.0.1:82/players/:id -> update player

```
-- DELETE http://127.0.0.1:82/players/:id -> delete player
-- GET http://127.0.0.1:82/players/team/:teamId -> Get players of a team
-- GET http://127.0.0.1:82/players/:id/team -> Get team of a player
-- GET http://127.0.0.1:82/players/search/:name -> Search by name placeholder
```

Repository Link:

https://github.com/JanieAbutu/ECE_Distributed-Systems-Security/tree/main/Projects/Lab%201_PlayerEntity_RestAPI_Project