# Human Resources Management Tool

## Presentation

Yacine Montacer
Department of Information Technology
Tunis Business School

January 16, 2023

# Introduction

HR software is used to automate and streamline many of the tasks associated with human resources management, such as recruiting, onboarding, performance management, and employee benefits administration. It can help organizations of all sizes improve the efficiency and effectiveness of their HR functions, while also providing valuable data and insights that can inform strategic decision-making.

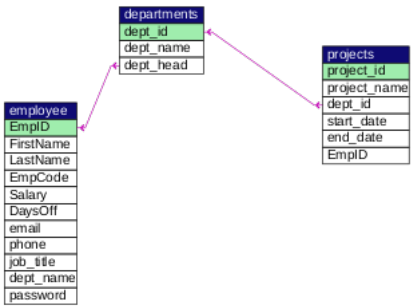
# Demo

My project demo is a basic CRUD API backend built with Node.js and Express.js, it uses a MySQL database to manage employees, projects and departments. It also includes authentication and authorization functionality. It allows the user to perform various operations like employee login, token creation, editing personal information, and sending a notification email. The project also uses the bcrypt library for password hashing and salting and the JWT library for creating JSON web tokens for authentication. It also uses OAuth2 for authentication when sending the notification email.

# Main Topics

- Database structure
- Access token, environment variables, encryption
- CRUD operations
- User log-in and interactivity
- API testing using postman  development difficulties
- Needed features

# Database Structure




The database structure for this project includes 3 main tables: employee, project, and department. The employee table contains information about each employee, including their Employee ID (EmpID), first name, last name, email, phone, and password. The project table contains information about each project, including the project's name, start date, end date, and the Employee ID of the project manager. The department table contains information about each department, including the department's name and the Employee ID of the department head.

# Access Token JWT

**Heading**

1. User Log-in
2. Server Creates JWT
3. User Request Access
4. Server Grants Access

The admin authenticated using a username - password combination, they are given a token that is generated from a secret key, viable for 15 minutes. The token is sent along with any request to any endpoint in the API. And the token can get refreshed every 10 minutes so the user doesn't have to log in again excessively.

# Environment Variables

I used environment variables for the log-in information for the admin and the email account. Environment variables are a way to store information that can be used by the operating system or applications running on the system. They are typically used to store sensitive information such as passwords, API keys, or other sensitive information that should not be stored in the codebase. These variables are stored in the operating system and can be accessed by applications running on the system. They are typically set up using the command line or a script, and are often stored in a configuration file or in the system registry. They can be read and modified by the application at runtime, without requiring a recompilation. This allows for easy and secure configuration of the application.

# Hashing  Salting

The passwords on the employee table are encrypting with hashing  salting, so that passwords are not stored anywhere in their normal format. Hashing is a one-way process of taking an input (or 'message') and returning a fixed-size string of characters, which is a 'digest' that is unique to the original input. The same input will always produce the same hash, but even a small change to the input will produce a very different hash. Hashing is often used to store passwords securely in a database as it's not possible to retrieve the original password from the hashed version.
Salting is the process of adding random data to the input before it is hashed. This is done to make it more difficult for an attacker to use precomputed tables of hash values (often called rainbow tables) to determine the original input. It also prevents two users with the same password from having the same hash value in the database. Essentially, a salt is added to make the process of cracking a password more difficult

# CRUD operations

The Node back-end demo has operations to log users in, send them confirmation emails and allow them to modify their personal information. The admin logs in to access the 3 tables, book vacations for employees, and perform different operations

## POST

Log-in, employee log-in  email confirmation, display projects for each department, reset password and encrypt, insert employee

## PUT

Update employee data, employee editing personal data

## GET

Book vacation days, Retrieve employees, obtain supervisor information

## DELETE

Deleting employees

# API Testing and difficulties

I used Postman to test my API endpoints. The automated testing helped expedite the development process, and it brought light to certain difficulties, which were logging into Gmail to send the confirmation email and also using the environment variables which haven't worked so far

# Needed Features

The HR platform needs a lot of features to be functional, like attendance and payroll management, budget and expense management, client interactions and customer support tickets, Recruitment and job posting management...etc.

# Thank You!