**User:**

package com.afrin.springrest.model;

public class User {

private String username;

private String password;

public User() {}

public User(String username, String password) {

this.username = username;

this.password = password;

}

public String getUsername() { return username; }

public void setUsername(String username) { this.username = username; }

public String getPassword() { return password; }

public void setPassword(String password) { this.password = password; }

}

**JWT Utility class:**

package com.afrin.springrest.util;

import io.jsonwebtoken.Jwts;

import io.jsonwebtoken.SignatureAlgorithm;

import java.util.Date;

public class JwtUtil {

private static final String SECRET\_KEY = "mySecretKey";

public static String generateToken(String username) {

return Jwts.builder()

.setSubject(username)

.setIssuedAt(new Date())

.setExpiration(new Date(System.currentTimeMillis() + 86400000)) // 1 day

.signWith(SignatureAlgorithm.HS256, SECRET\_KEY)

.compact();

}

}

**AUTH CONTROLLER:**

package com.afrin.springrest.controller;

import com.afrin.springrest.model.User;

import com.afrin.springrest.util.JwtUtil;

import org.springframework.http.ResponseEntity;

import org.springframework.web.bind.annotation.\*;

@RestController

@RequestMapping("/auth")

public class AuthController {

@PostMapping("/login")

public ResponseEntity<String> login(@RequestBody User user) {

// dummy username/password check

if ("admin".equals(user.getUsername()) && "password".equals(user.getPassword())) {

String token = JwtUtil.generateToken(user.getUsername());

return ResponseEntity.ok(token);

} else {

return ResponseEntity.status(401).body("Invalid credentials");

}

}

}