# Online Exam System Security Manual

## Introduction

This document provides a comprehensive security manual for the Online Exam Management System, a software application designed for conducting exams online. Developed by Seth Chritzman, Brent Kosior, and Oleksii Dukhovenko under the guidance of Dr. Thangiah, this system incorporates various security measures to ensure the integrity and confidentiality of the examination process.

## System Overview

The Online Exam Management System is a Java-based application utilizing the Spring Boot framework. It is designed to handle different user permissions, ensuring that each user type (Administrator, Student, Instructor, Schedule Manager) has access only to the appropriate functionalities and data.

### Key Components:

* **User Authentication and Authorization:** Utilizes Spring Security for managing user authentication and role-based access control.
* **Password Management:** Implements password encoding using Spring Security's PasswordEncoder to ensure that user passwords are securely stored.
* **Role Management:** Manages user roles (ADMINISTRATOR, STUDENT, INSTRUCTOR, SCHEDULE\_MANAGER) and permissions through a dedicated Role Repository.

## Security Features

### User Authentication

* **UserDetailsService:** Custom implementation for loading user-specific data during authentication.
* **PasswordEncoder:** Utilizes BCryptPasswordEncoder for secure password hashing.

### Authorization and Access Control

* **HttpSecurity Configuration:** Configures URL-based authorization, ensuring that users can access only those URLs they are permitted to.
* **Role-Based Access Control:** Defines specific roles and permissions for different user types, restricting access to sensitive functionalities.

### Database Security

* **Secure User Creation:** The system creates users only if they do not already exist, preventing duplicate entries.
* **Role Validation:** Validates roles during user creation to ensure that each user is assigned the correct role.

### CSRF Protection

* **CSRF Disabled:** For development purposes, CSRF protection is disabled. However, it is recommended to enable CSRF protection in production environments to prevent cross-site request forgery attacks.

## Best Practices for System Security

1. **Enable CSRF Protection:** For production deployments, enable CSRF protection to safeguard against cross-site request forgery.
2. **Regularly Update Passwords:** Encourage users to update their passwords regularly and implement a strong password policy.
3. **Monitor and Audit:** Regularly monitor system access and activities to detect any unauthorized access or anomalies.
4. **Data Encryption:** Implement encryption for sensitive data, both at rest and in transit, to protect against data breaches.
5. **Regular Security Audits:** Conduct regular security audits and updates to the system to address any new vulnerabilities.

## Conclusion

The Online Exam Management System incorporates several robust security features to protect against unauthorized access and ensure the integrity of the examination process. Adhering to the best practices outlined in this manual will further enhance the security and reliability of the system.