Security Risk Analysis and Applied Solutions in the Hospital Management System

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Security Risk Type | Risk Description | Applied Solutions |
| 1 | Authentication Risks | - Password attacks (Brute-Force, Credential Stuffing) - Insecure password storage - Reuse of weak passwords | - Use of BCryptPasswordEncoder for password hashing - Password strength policy enforced in changeUserPassword - Input validation using @Size and @NotBlank - JavaScript validation in change-password.html - Logging of successful and failed login attempts |
| 2 | Authorization Risks | - Unauthorized access to resources - Improper role handling | - Role-based access control using .authorizeHttpRequests() and @PreAuthorize - Creation of default roles and users in HospitalSystemApplication.java |
| 3 | Injection Risks | - SQL Injection attacks - XSS attacks | - Use of Spring Data JPA to prevent SQL Injection - Use of @NotBlank, @Size, and @Pattern in DTOs - Content Security Policy (CSP) configuration to restrict content sources - Enabling X-XSS-Protection |
| 4 | Sensitive Data Exposure Risks | - Storing sensitive data without encryption - Logging of sensitive information | - Encryption of phone and email data using AES - Use of EncryptionUtil with a key from application.properties - Safe logging that avoids revealing full sensitive data |
| 5 | Security Misconfiguration Risks | - Default security settings - System information disclosure - Use of default accounts | - Disabling default user in Spring - Configuring security HTTP headers (X-Frame-Options, CSP, HSTS, X-Content-Type-Options) - Secure management of Actuator endpoints - Detailed and structured logging |
| 6 | Logging and Monitoring Risks | - Insufficient logging - Lack of security performance indicators | - Custom audit system via FilteredAuditEventRepository - Logging of critical CRUD events - Use of Micrometer for metrics recording |
| 7 | Session Management Risks | - Session hijacking - Long session durations | - Session and cookie deletion upon logout - Clearing security context after password change |