Bai 1

| **Tính năng** | **Mô tả** |
| --- | --- |
| **1. Authentication (Xác thực)** | Xác minh danh tính người dùng (username/password, token, OAuth2...) |
| **2. Authorization (Phân quyền)** | Quyết định người dùng có được phép truy cập một tài nguyên hay không (role-based access) |
| **3. CSRF Protection** | Ngăn chặn tấn công CSRF (Cross Site Request Forgery) |
| **4. Secure Headers** | Tự động thêm các HTTP security headers như X-Content-Type-Options, X-Frame-Options, Strict-Transport-Security |
| **5. Session Management** *(bonus)* | Quản lý phiên đăng nhập, bảo vệ chống tấn công session fixation |

Bai 2

| **Thành phần** | **Vai trò** |
| --- | --- |
| requestMatchers("/public/\*\*").permitAll() | Cho phép tất cả người dùng truy cập các URL bắt đầu với /public/ **không cần đăng nhập** |
| anyRequest().authenticated() | Tất cả các request khác đều **phải xác thực** |
| formLogin() | Bật form đăng nhập mặc định của Spring Security |
| httpBasic() | Cho phép xác thực qua Basic Auth (dùng tiện trong Postman / curl) |