Slot9 – Bảo mật ứng dụng

Authentication: (xác thực): người dùng là ai??? (user/pass)

- user/pass: dễ lộ, dễ hack
- Token-based: JWT, Oauth2
  - JWT: Json web token: header+payload+Signature
  - Bản chất: sinh ra key bí mật, kết hợp với thông tin user; khi validate thì cần giải mã (decode token)
  - Quy trình trong Spring Boot:
  - Login-> server trả về JWT
  - Client lưu token
  - Mỗi request sẽ gửi kèm quyền
  - Giải mã token, xác thực user
- Social login: google

Authorization (phân quyền): có những quyền gì(ROLE)

- Role-based: user, admin
- Annotation: @PreAuthorize()