1. ศึกษา Source Code  เรื่องการ Log in

-Input การรับข้อมูลจากผู้ใช้

ผู้ใช้จะกรอกข้อมูลการเข้าสู่ระบบ เช่น ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

-การตรวจสอบข้อมูล (Authentication)

ตรวจสอบข้อมูลกับฐานข้อมูลหรือล็อกอินผ่านบริการภายนอก (OAuth/JWT)

-การสร้าง Session หรือ Token

หากข้อมูลถูกต้อง ระบบจะสร้าง Session ID หรือ Token

-การจัดการกับข้อผิดพลาด (Error Handling)

หากข้อมูลไม่ถูกต้อง ระบบจะให้ข้อความผิดพลาดที่เหมาะสม ควรหลีกเลี่ยงการแสดงข้อมูลที่ละเอียดเกินไป เช่น "Username หรือ Password ผิด" เพื่อป้องกันไม่ให้ผู้โจมตีทราบว่า Username ที่กรอกผิด

2. สรุปเชิง Technique เกี่ยวกับการทำงานของระบบ ฯ

-Authentication

การใช้ Session หรือ Token ในการจัดการสถานะการล็อกอิน

Token ที่ใช้ในระบบเช่น JWT ช่วยให้ผู้ใช้สามารถทำการ Authentication โดยไม่ต้องส่งข้อมูลเข้าสู่ Server ทุกครั้ง

-Security

การใช้ HTTPS เพื่อป้องกันการดักจับข้อมูลในระหว่างการส่งข้อมูล

การใช้ Salt และ Hashing ในการเก็บรหัสผ่านในฐานข้อมูล เช่นการใช้ bcrypt หรือ Argon2 เพื่อให้รหัสผ่านมีความปลอดภัย

การใช้ Multi-Factor Authentication (MFA) เพื่อเพิ่มชั้นความปลอดภัย

-Session Management

การจัดการ Session Expiry เพื่อให้ Session ที่หมดอายุจะไม่สามารถนำมาใช้งานได้

การทำ Session Revocation หากมีการออกจากระบบหรือการเปลี่ยนแปลงสิทธิ์การใช้งาน

-Error Handling

แจ้งข้อผิดพลาดที่เหมาะสม (ไม่ให้ข้อมูลมากเกินไป)

-MFA

เพิ่มความปลอดภัยด้วย Multi-Factor Authentication