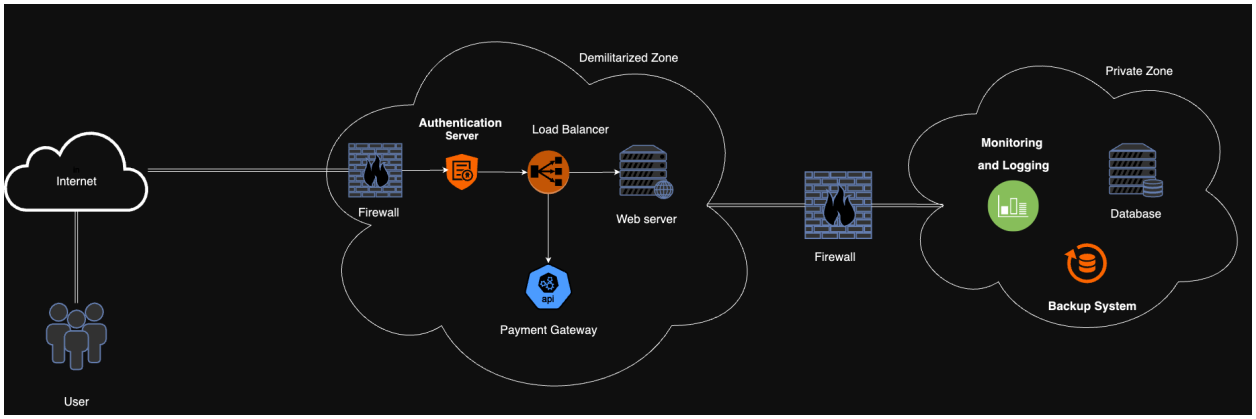
Name: Watcharapol Yotadee
Nickname: Fluke

Assignment Week 4

Security Architecture and Design

1. Using principles from network architecture, create a simple system of your choice (e.g., a online bookshop, shopping website, booking website, or etc.). Draw a system architecture diagram based on secure design, indicating the placement of components such as the client, server, database, and any other relevant elements. Additionally, identify the network zone for each component.



ระบบจองเช่ารถยนต์

Public Zone

1. User คือ ลูกค้าเข้าถึงระบบผ่านอินเทอร์เน็ตเพื่อค้นหาหรือจองรถเช่า
2. Internet คือ เชื่อมต่อผู้ใช้กับระบบผ่านการเข้ารหัส SSL/TLS เพื่อความปลอดภัย

Demilitarized Zone

1. Firewall ป้องกันโดยการกรองและรักษาความปลอดภัยของทราฟฟิกที่เข้าสู่ DMZ zone
2. Authentication Server ตรวจสอบข้อมูลประจำตัวของผู้ใช้ก่อนให้เข้าถึงระบบ
3. Load Balancer กระจายทราฟฟิกไปยัง Web Server หลายตัวเพื่อเพิ่มประสิทธิภาพ
4. Web Server จัดการคำขอของผู้ใช้ เช่น การจอง การจัดการบัญชีผู้ใช้
5. Payment Gateway ประมวลผลการชำระเงินออนไลน์อย่างปลอดภัยสำหรับการจอง
6. Firewall (DMZ -> Private Zone) จำกัดการเข้าถึงจาก DMZ ไปยัง Private Zone

Private Zone

1. Database เก็บข้อมูลสำคัญ เช่น บัญชีผู้ใช้ รายละเอียดการจอง และประวัติการชำระเงิน
2. Monitoring and Logging คือ ตรวจสอบกิจกรรมของระบบและบันทึกเหตุการณ์
3. Backup System รับประกันการกู้คืนข้อมูลในกรณีที่ระบบล้มเหลวหรือข้อมูลสูญหาย
4. Firewall ป้องกันโซนส่วนตัวจากการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อให้มั่นใจว่าข้อมูลที่ละเอียดอ่อนจะปลอดภัย

Name: Watcharapol Yotadee
Nickname: Fluke

2. Based on your designed system, list and identify the 3 most significant threats to your system. For each threat, suggest mitigation controls using secure design principles.

   Threat 1: Fraudulent Payment Attacks

   Description: ผู้ไม่หวังดีอาจใช้ข้อมูลบัตรเครดิตปลอมหรือการจ่ายเงินที่ไม่ได้รับอนุญาต

   Mitigation Controls:

   1. ใช้ Payment Gateway ที่ได้รับการรับรอง PCI DSS
   2. เปิดใช้งาน 3D Secure Authentication
   3. ใช้ Fraud Detection Service เพื่อวิเคราะห์พฤติกรรมผู้ใช้

   Threat 2: API Abuse

   Description: ผู้ไม่หวังดีอาจใช้ API เพื่อจองรถโดยไม่ผ่านการตรวจสอบ หรือใช้คำขอที่ไม่เหมาะสม

   Mitigation Controls:

   1. ใช้ Rate Limiting และ Throttling กับ API
   2. ใช้ OAuth 2.0 หรือ JWT สำหรับ Authentication
   3. เพิ่มการตรวจสอบ API ด้วย Input Validation

   Threat 3: Data Breach

   Description: ผู้ไม่หวังดีอาจเข้าถึงข้อมูลลูกค้าหรือข้อมูลการจองโดยไม่ได้รับอนุญาต

   Mitigation Controls:

   1. เข้ารหัสข้อมูล (Encryption) ทั้งที่เก็บอยู่และระหว่างการส่งข้อมูล
   2. ใช้ Database Activity Monitoring (DAM) เพื่อตรวจสอบการเข้าถึง
   3. ใช้ Access Control และแบ่งสิทธิ์การเข้าถึงตามหน้าที่