OWASP (Open Web Application Security Project)

องค์กรไม่แสวงหาผลกำไรที่ให้ความรู้ด้าน security มุ่งเน้นการปรับปรุงความปลอดภัยของซอฟต์แวร์ โดยเฉพาะอย่างยิ่งในด้านความปลอดภัยของแอปพลิเคชันเว็บ ก่อตั้งขึ้นในปี 2001 ซึ่งได้รับการปรับปรุงทุกๆ 4 ปี

โดยจะให้คำแนะนำในการทำแอพว่าควรทำอะไรเป็น 10 อันดับแรก เรียกว่า OWASP Top 10 เป็น 10 ข้อที่ OWASP ให้ควรระวังเอาไว้ก่อนจะทำแอพจริงๆ เป็น security เบื้องต้น

OWASP Top 10 ปี 2021

1. **Broken Access Control**
    - การที่ hacker ยิงเข้าช่องทางที่เราไม่อยากให้ยิงเข้ามา
    - Unauthorized access ปัญหาของการกำจัดสิทธิไม่ถูกต้อง
    - ต้องเช็ค API ให้ถูกต้องก่อนเข้ามา
2. **Cryptographic Failures**
    - เข้ารหัสไม่ถูกต้อง เข้าผิดแบบ
    - อาจเกิดจากการใช้อัลกอริธึมการเข้ารหัสที่ล้าสมัย
    - ไม่ควรเก็บ password ไว้ในรหัสที่สามรถถอดได้ เช่น การ encryption
    - Sensitive data ควรเก็บให้ถูกที่ ควรเข้ารหัสเอาไว้ แนะนำให้ทำ rotate key หรือ เปลี่ยน key ใหม่เรื่อยๆ เพื่อป้องกัน key หลุด
3. **Injection**
    - การส่ง data แปลกปลอมเข้าสู่ระบบได้
    - เช่น SQL Injection การส่งคำสั่ง SQL ผ่านกล่องข้อความ แล้วดึงข้อมูลหรือจัดการข้อมูลได้
    - ต้อง Validation , ORM
    - Least Privilege Principle ให้ Permission เป็นการอนุญาตหรือสิทธิ์ในการเข้าถึงเท่าที่จำเป็น
4. **Insecure Design**
    - เป็นช่องโหว่จาก architecture (App Secure แต่ Server Not Secure)
    - มักเกิดจาก network เช่น การปล่อย port ที่ที่ไม่ควรออกไปข้างนอก สามารถโดน access เข้ามาได้ default port
    - ดู Firewall ดีๆ ไม่มีใครแปลกปลอมที่สามารถเข้ามาได้
    - Principle ของการ deploy

5. **Security Misconfiguration**

    - Config ไม่ถูกต้องจนเกิดช่องโหว่ให้เข้าไปได้ (Server Secure แต่ดันไปใช้ Default configs เลยส่งผลให้บางอย่างดู secure แต่ก็ไม่ Secure)
    - เช่น Cloud storage ที่เก็บข้อมูลสำคัญ แต่ไม่ได้เซ็ตเป็น Private backet พอเป็น Public ทุกคนก็เข้ามาได้เลยขอแค่รู้ตำแหน่งเข้าด้วย default key เลย

6. **Vulnerable and Outdated Components**

    - ไม่ได้อัพเดท library เลยล้าสมัย
    - ต้องอัพเดท library อย่างสม่ำเสมอ

7. **Identification and Authentication Failures**

    - ช่องโหว่จากการ Authen ไม่ถูกต้อง
    - Unauthorized แต่ผ่านเข้ามาได้
    - เช่นการรีเซ็ต password โดยไม่มีการยืนยันตัวตนก่อน ทำให้ไปรีเซ็ตของใครก็ได้

8. **Software and Data Integrity Failures**

    - สามารถแก้ไข data ได้โดยไม่ตั้งใจ ส่งผลให้ data โดนแปลกปลอมได้
    - เช่น API upload เอกสารได้ เมื่อ user โหลดเอกสารไปใช้ โดยไม่รู้ตัวว่าไม่ใช่เอกสารของตัวเองแล้ว เนื่องจาก hacker เจอช่องโหว่อัพโหลดเอกสารซ้อนทับได้
    - Notify user ให้รู้ตัว

9. **Security Logging and Monitoring Failures**

    - Log ไม่ดีที่ใช้จับตอนมีปัญหา security ไว้หาว่ามันมาจากจุดๆไหน
    - Log design ดีๆ
    - อย่าให้ log หาย

10. **Server-Side Request Forgery (SSRF)**

    - ปลอมแปลงเป็นเหมือน server นั้นได้ เปลี่ยนให้ request ที่ปลอดภัยเป็นไม่ปลอดภัย
    - เช่น url ที่เก็บแค่ภาพ แต่ถ้าแปลงเป็น url อื่นอาจจะไม่ปลอดภัยแล้วที่ดึงข้อมูลจาก path อื่นได้