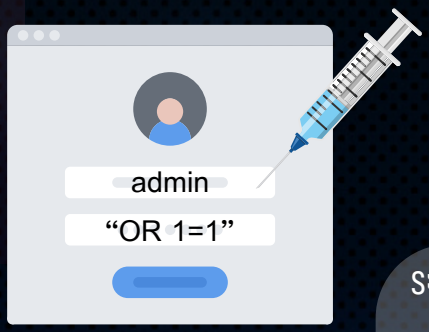
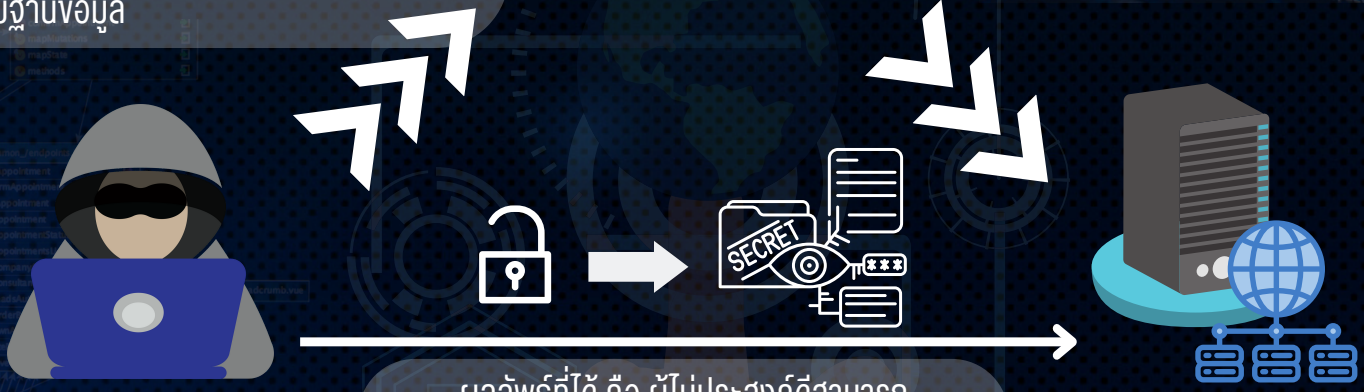
SQL INJECTION ATTACK



ผู้ไม่ประสงค์ดี ใช้ประโยชน์จากการส่งชุดคำสั่ง SQL ที่ไม่มีการป้องกันการใส่ข้อมูลไม่ถูกต้อง เพื่อ Bypass ชุดคำสั่งการพิสูจน์ตัวตนส่งไปยังระบบฐานข้อมูล

ระบบฐานข้อมูลจะเช็คดูว่าในฐานข้อมูลการพิสูจน์ตัวตน มีชื่อผู้ใช้และรหัสผ่านตรงตามที่ผู้ใช้กรอกลงไปหรือไม่



ผลลัพธ์ที่ได้ คือ ผู้ไม่ประสงค์ดีสามารถลงชื่อเข้าใช้เป็น ผู้ดูแลระบบได้ทันที

SQL Injection

เทคนิคการโจมตีอาศัยช่องโหว่การเขียนโปรแกรมคอมพิวเตอร์ (Programming Language Code) ที่ใช้ประโยชน์จากส่งคำสั่ง SQL ผ่านทางเว็บแอพพลิเคชัน เพื่อไปโจมตีระบบฐานข้อมูลหลังบ้าน โดยการใส่ข้อมูล Input ของผู้ใช้ ทำให้ระบบงานถูกโจมตี ผู้ไม่ประสงค์ดีสามารถดึงข้อมูล หรือเปลี่ยนแปลงแก้ไขข้อมูลในระบบฐานข้อมูลตามคำสั่ง SQL ที่แอบฝังลงไปได้ทันที

แนวทางการป้องกัน

การออกแบบและพัฒนาระบบงาน ให้คำนึงถึงการรักษาความปลอดภัยด้านสารสนเทศ ทั้งในส่วน Front End และ Back End ต้องมีการตรวจสอบ Code ในส่วนของการตรวจสอบค่าตัวแปรที่นำข้อมูลเข้าสู่ระบบ (Input Validation) เพื่อป้องกันการโจมตีด้วยเทคนิค SQL Injection, Cross-site Scripting และ Buffer Overflow

วิธีการตรวจสอบช่องโหว่

ใส่ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็น " or 1=1-- " ในหน้าจอเข้าสู่ระบบงาน (Login) ผลที่ได้คือสามารถเข้าระบบงานได้ โดยผู้ไม่ประสงค์ดีใช้ประโยชน์จากการใส่ข้อมูลที่ไม่ได้ป้องกัน จึงสามารถ Bypass เข้าระบบฐานข้อมูลได้

กรมอนามัย
DEPARTMENT OF HEALTH

สามารถติดต่อสอบถามได้ที่

กลุ่มเทคโนโลยีสารสนเทศ กองแผนงาน กรมอนามัย
E-mail : network@anamai.mail.go.th
โทรศัพท์ : 0-2590-4290 , 0-2590-4292

Line Official : Anamai IT support
ID : @070rcfdv