LAB1: Web Security (IIS with SSL)

ขั้นตอนการตั้งค่า SSL สำหรับ MySQL บนวินโดว์

1. ติดตั้ง OpenSSL (ในที่นี้ใช้ OpenSSL เวอร์ชัน 1.1.11 แบบไม่ต้องติดตั้ง) รันบนแพลตฟอร์มวินโดว์ (ดาวน์โหลดที่ https://slproweb.com)
2. ตั้งค่า System variables (กดปุ่ม windows key + break)
    a. คลิกที่แท็บ Advanced คลิกที่ปุ่ม Environment Variables
    b. ดับเบิลคลิกที่ตัวแปร Path ที่ System variables
    c. คลิกที่ Variable value ให้พิมพ์ ;C:\OpenSSL\bin ต่อตำแหน่งท้ายสุดของค่าเดิม
    d. คลิกปุ่ม OK จนเสร็จสิ้นขั้นตอนตั้งค่า System variables
3. สร้าง Certificate Authority (CA) สำหรับรับรองใบ CSR จาก IIS
    a. คลิก Start -> Run พิมพ์ CMD กด Enter แล้วพิมพ์ CD \OpenSSL\bin แล้วกด Enter
    b. พิมพ์คำสั่ง OpenSSL กด Enter
    c. จากนั้นพิมพ์คำสั่งสร้าง CA

    > req -new -x509 -keyout ca-key.pem -out ca-cert.pem -config ../openssl.cnf

    d. เข้ารหัสกุญแจส่วนตัวของ CA

    > rsa -in ca-key.pem -out ca-key.pem
4. สร้างโฟลเดอร์ต่อไปนี้ใน home directory ของเว็บไซต์ (หรือตำแหน่งอื่นแต่ต้องไปแก้ไขไฟล์ config.cnf)
    a. demoCA
    b. demoCA/private
    c. demoCA/newcerts

    สร้างไฟล์ demoCA\serial.txt และ demoCA\index.txt โดยเปิดไฟล์แรกขึ้นมา พิมพ์ 01 แล้วทำการบันทึก
5. ให้ย้ายไฟล์กุญแจส่วนตัวของ CA คือไฟล์ ca-key.pem ไปที่โฟลเดอร์ demoCA/private
6. ให้ย้ายไฟล์ใบรับรองของ CA คือไฟล์ ca-cert.pem ไปที่โฟลเดอร์ demoCA/
7. ให้สร้างใบ CSR จาก IIS ที่ต้องการใช้ SSL แล้วนำไฟล์ CSR มาทำการรับรองจาก CA ด้วยคำสั่งต่อไปนี้

    >ca -in certreq.txt -out iis.cer -config ../openssl.cnf
8. นำไฟล์รับรองที่ทำการรับรองเรียบร้อยแล้วไปที่เครื่องเซิร์ฟเวอร์ IIS และดำเนินการนำไฟล์ใบรับรองมาตรฐาน x.509 เข้าไปใช้งาน และทดสอบโดยการเปิดใช้งานพอร์ต 443 (https)