# ONE CLICK SCAN

CP422031

## INTRODUCTION TO CYBERSECURITY


อาจารย์ที่ปรึกษา
ศ.ดร.จักรชัย โสอินทร์
ผศ.ดร.สาธิต กระเวนกิจ
อ.ดร.ชาติชาย ปุณริบูรณ์


## หลักการและเหตุผล

- การรับข้อมูลและสำรวจเป้าหมาย (Input & Reconnaissance)
  - ผู้ใช้งานระบุ Target URL เข้าสู่ระบบ
  - ระบบทำการ Web Scraping/Crawling เพื่อรวบรวมข้อมูลโครงสร้างเว็บไซต์
    - ค้นหา Path และ Directory ที่มีอยู่
    - ค้นหาหน้า FORM, INPUT FIELDS และ PARAMETER ต่างๆ (GET/POST)
- การวิเคราะห์และจำแนก (Analysis & Identification)
  - ระบบนำ Parameter ที่ได้มาวิเคราะห์เพื่อเลือกประเภทการทดสอบที่เหมาะสม
  - ตรวจสอบรูปแบบ Input เพื่อระบุว่าจุดใดมีความเสี่ยงต่อช่องโหว่ประเภทใด
  - (เช่น จุดรับค่า Text อาจเสี่ยง XSS, จุด Query อาจเสี่ยง SQLi)

## ขอบเขตการศึกษา

- การสำรวจข้อมูล (Reconnaissance): พัฒนาระบบสำรวจโครงสร้างเว็บไซต์ (Site Crawling) เพื่อค้นหา Path และจุดรับข้อมูล (Input Parameters) ทั้งรูปแบบ GET และ POST โดยอัตโนมัติ
- การวิเคราะห์ช่องโหว่ (Analysis): ระบบสามารถวิเคราะห์และจำแนกประเภท Input เพื่อเลือกวิธีการทดสอบที่เหมาะสมกับจุดเสี่ยงนั้นๆ (เช่น จุดรับค่า Text ตรวจสอบ XSS หรือจุด Query ตรวจสอบ SQLi)
- เครื่องมือและเทคนิคที่ใช้ (Engines): บูรณาการเครื่องมือทดสอบมาตรฐานและเทคนิคเฉพาะทางเข้าด้วยกัน ดังนี้:
  - SQL Injection: ใช้ Engine ของ SQLMap
  - XSS: ใช้ Engine ของ PwnXSS
  - File Upload: ใช้ Engine ของ DavTest
  - SSTI & Advanced: ใช้ Custom Payloads และ Metasploit ในการทดสอบเพิ่มเติม
- การแสดงผลและรายงาน (Reporting): สรุปผลการตรวจสอบที่ระบุจำนวนช่องโหว่ที่พบ ระดับความรุนแรง (Critical/High) และรายละเอียด Payload ที่ใช้เจาะระบบสำเร็จ

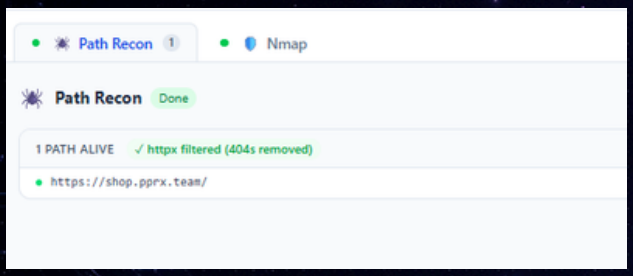
## วัตถุประสงค์ของโครงงาน

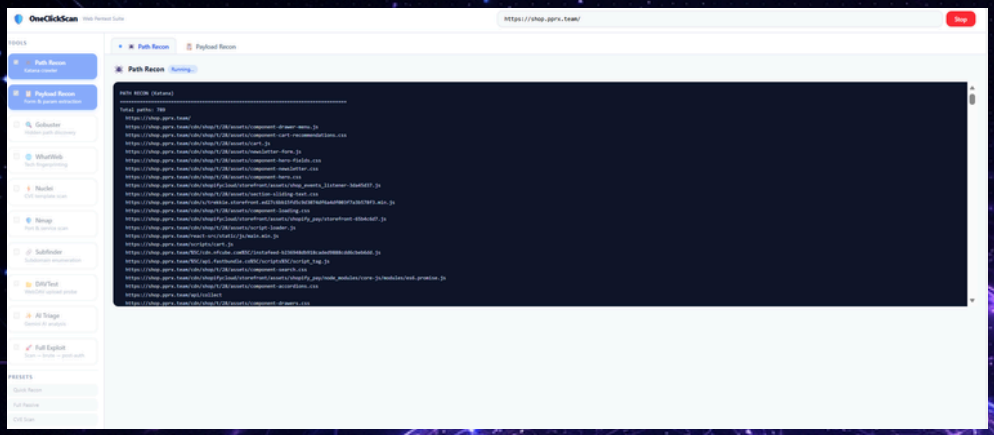
- เพื่อพัฒนาเครื่องมือตรวจสอบช่องโหว่เว็บไซต์แบบอัตโนมัติ (Automated Web Vulnerability Scanner) ที่สามารถค้นหาจุดเสี่ยงและทดสอบการโจมตีได้ด้วยตนเอง
- เพื่อประยุกต์ใช้เทคนิค Web Scraping ในการค้นหาโครงสร้างเว็บไซต์ (Site Crawling), URL Path และจุดรับข้อมูล (Input Parameters) เพื่อนำมาใช้เป็นเป้าหมายในการทดสอบ
- เพื่อบูรณาการเครื่องมือทดสอบความปลอดภัย (เช่น SQLMap) และ Payload Scripts จากแหล่งต่างๆ ให้สามารถทำงานร่วมกันได้ภายในระบบเดียว
- เพื่อลดความซับซ้อนและอำนวยความสะดวกในการทดสอบเจาะระบบ (Penetration Testing) ให้ผู้ใช้งานสามารถตรวจสอบความปลอดภัยเบื้องต้นได้ง่ายเพียงแค่ระบุ URL เป้าหมาย

## หลักการทำงาน

- การรับข้อมูลและสำรวจเป้าหมาย (Input & Reconnaissance)
  - ผู้ใช้งานระบุ Target URL เข้าสู่ระบบ
  - ระบบทำการ Web Scraping/Crawling เพื่อรวบรวมข้อมูลโครงสร้างเว็บไซต์
    - ค้นหา Path และ Directory ที่มีอยู่
    - ค้นหาหน้า Form, Input Fields และ Parameter ต่างๆ (GET/POST)
- การวิเคราะห์และจำแนก (Analysis & Identification)
  - ระบบนำ Parameter ที่ได้มาวิเคราะห์เพื่อเลือกประเภทการทดสอบที่เหมาะสม
  - ตรวจสอบรูปแบบ Input เพื่อระบุว่าจุดใดมีความเสี่ยงต่อช่องโหว่ประเภทใด
- การโจมตีและตรวจสอบช่องโหว่ (Exploitation & Scanning) ระบบจะเรียกใช้ Engine และ Payloads ตามการวิเคราะห์ ดังนี้:
  - SQL Injection: ส่งค่าให้ SQLMap ทำการทดสอบเจาะฐานข้อมูล
  - XSS (Cross-Site Scripting): ใช้ PwnXSS ตรวจสอบการฝัง Script
  - WebDAV/Upload: ใช้ DavTest ตรวจสอบสิทธิ์การอัปโหลดไฟล์
  - SSTI: ยิง Payload เฉพาะเพื่อตรวจสอบ Server-Side Template Injection
  - Advanced/Custom: หาก Tools หลักไม่พบ หรือต้องการทดสอบลึกขึ้น ระบบจะดึง Payloads จาก GitHub/Custom Scripts หรือเรียกใช้ Metasploit เพื่อโจมตีเพิ่มเติม
- การสรุปผล (Reporting)
  - รวบรวมผลลัพธ์จากทุก Tools (ช่องโหว่ที่พบ, Payload ที่ใช้สำเร็จ, ระดับความรุนแรง)
  - แสดงผลออกมาเป็นรายงาน (Report) ให้ผู้ใช้ทราบเพื่อให้แก้ไขต่อไป

## EXAMPLE



## เครื่องมือและซอฟต์แวร์

DAVTEST

XSS

METASPLOIT

SQLMAP


**สมาชิก Group17**

- นายเกริกกษิต เอียดแก้ว 673380493-5
- นายคัมภีร์ดารา ภูกิ่งเงิน 673380152-1
- นายนันทภัทร เพชรสังหาร 673380166-0
- นางสาวศุภาพิชญ์ เพ็ชรสุรักษ์ 673380190-3
- นายกฤษกร แสนสกุล 673380144-0
- นายธนภัทร สิรินทร์ 673380159-7