
# IT 2566/04

## เอกสารโครงงานฉบับสมบูรณ์

โปรแกรมตรวจสอบช่องโหว่ของเว็บไซต์

Website vulnerability checker Program

โดย

633020030-8 นายตนุสรณ์ สนธิมูล

633020323-3 นายรัฐศาสตร์ เพียวงษ์

อาจารย์ที่ปรึกษา : อ.ดร.เพชร อิ่มทองคำ

โครงงานนี้เป็นส่วนหนึ่งของการศึกษาวิชา รหัส 342494 โครงงานคอมพิวเตอร์ 1

ภาคเรียน 1 ปีการศึกษา 2566

วิทยาลัยการคอมพิวเตอร์ สาขาเทคโนโลยีสารสนเทศ

มหาวิทยาลัยขอนแก่น

(เดือน สิงหาคม พ.ศ. 2566)


# IT 2566/04

## เอกสารโครงงานฉบับสมบูรณ์

โปรแกรมตรวจสอบช่องโหว่ของเว็บไซต์

Website vulnerability checker Program

โดย

633020030-8 นายตนุสรณ์ สนธิมูล

633020323-3 นายรัฐศาสตร์ เพียวงษ์

อาจารย์ที่ปรึกษา : อ.ดร.เพชร อิ่มทองคำ

โครงงานนี้เป็นส่วนหนึ่งของการศึกษาวิชา รหัส 342494 โครงงานคอมพิวเตอร์ 1

ภาคเรียน 1 ปีการศึกษา 2566

วิทยาลัยการคอมพิวเตอร์ สาขาเทคโนโลยีสารสนเทศ

มหาวิทยาลัยขอนแก่น

(เดือน สิงหาคม พ.ศ. 2566)

# คำนำ

รายงานฉบับนี้เป็นส่วนหนึ่งของวิชาสัมมนาทางเทคโนโลยีสารสนเทศ (342491) โดยมีจุดประสงค์ เพื่อจัดทำโปรแกรมตรวจสอบช่องโหว่ของเว็บไซต์ ทั้งนี้ ในรายงานนี้มีเนื้อหาประกอบด้วยความรู้เกี่ยวกับ Cyber security , 10 ช่องโหว่ของเว็บไซต์ โดยการจัดอันดับโดย OWAS TOP 10

คณะผู้จัดทำได้เลือกหัวข้อนี้ในการทำโครงงาน เนื่องมาจากในปัจจุบันมีการโจมตีเว็บไซต์มากขึ้นเพื่อขโมยข้อมูลส่วนตัวของผู้ใช้ โดยอาศัยช่องโหว่ของระบบ คณะผู้จัดทำจึงต้องการตรวจสอบช่องโหว่ของระบบเพื่อลดจำนวนช่องโหว่ของเว็บไซต์ให้น้อยลง คณะผู้จัดทำต้องขอขอบคุณอาจารย์ ดร.เพชร อิ่มทองคำ อาจารย์ที่ปรึกษาโครงงาน และอาจารย์ท่านอื่นผู้ให้ความรู้ และแนวทางการศึกษา หวังว่าโครงงานฉบับนี้จะให้ความรู้ และเป็นประโยชน์แก่ผู้อ่านทุก ๆ ท่าน หากมีข้อเสนอแนะประการใด คณะผู้จัดทำขอรับไว้ด้วยความยินดียิ่ง

คณะผู้จัดทำ

ตนุสรณ์ สนธิมูล

รัฐศาสตร์ เพียวงษ์

ตนุสรณ์ สนธิมูล และ รัฐศาสตร์ เพียวงษ์. 2566. **โปรแกรมตรวจสอบช่องโหว่เว็บไซต์**. โครงงานคอมพิวเตอร์ ปริญญาวิทยาศาสตร์บัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ วิทยาลัยการคอมพิวเตอร์ มหาวิทยาลัยขอนแก่น

อาจารย์ที่ปรึกษา: อาจารย์ ดร.เพชร อิ่มทองคำ

## บทคัดย่อ

การโจมตีช่องโหว่เว็บไซต์ก่อให้เกิดความเสียหายขึ้นมากมายทั้งทรัพยากรเวลาและเงินจำนวนมาก จากข้อมูลวิเคราะห์เรื่องการโจมตีเว็บไซต์ของนักวิจัยแคสเปอร์สกี้ ระหว่างเดือนมกราคมถึงเดือนเมษายน ปี 2565 พบว่าการโจมตีทางอินเทอร์เน็ตของประเทศไทยสูงขึ้น 107.62% คือ 317,347 รายการในปี 2565 โครงงานนี้จึงได้จัดทำโปรแกรมตรวจสอบช่องโหว่ เพื่อตรวจหาช่องโหว่ภายในเว็บไซต์ที่ผู้ใช้งานกรอกเข้ามา โดยโปรแกรมนี้จะทำการตรวจดูโครงสร้างของเว็บไซต์เพื่อหาช่องโหว่ ถ้าเจอช่องโหว่ตัวโปรแกรมก็จะรายงานผลการตรวจสอบออกมาพร้อมทั้งบอกรายละเอียดต่างๆ ของช่องโหว่ เช่น ที่มาของช่องโหว่ ข้อมูลของช่องโหว่ สาเหตุของการเกิดช่องโหว่ อีกทั้งยังสามารถบอกวิธีแก้ปัญหาช่องโหว่ที่เกิดขึ้นได้อีกด้วย โปรแกรมนี้ถูกพัฒนาขึ้นโดยใช้ภาษาจาวาสคริปและอิเล็กตรอนเจเอสเฟรมเวิร์คในการออกแบบหน้าตาของโปรแกรม และใช้ API จากองค์กรไม่แสวงหาผลกำไร OWASP ในการตรวจหาช่องโหว่ และใช้วิธีการที่คิดขึ้นเองในการตรวจหาช่องโหว่ที่ครอบคลุมจากแบบเดิมมากขึ้น

คำสำคัญ : วิธีการที่คิดขึ้นเองในการตรวจหาช่องโหว่ที่ครอบคลุมจากแบบเดิมมากขึ้น

Thanuson Sonthimoon and Rathasat Peerwong. 2023. **Website vulnerability detection program**. computer project Bachelor of Science degree Information Technology College of Computer Science Khon Kaen University

**Advisor :** Phet Aimtongkham, Ph.D.

## Abstract

Attacks on website vulnerabilities cause a lot of damage, resources, time and money. According to researcher Kaspersky's website attack analysis. Between January and April 2022, Thailand's cyberattacks increased by 107.62%, which is 317,347 in 2022. This project has therefore developed a vulnerability detection program. To detect vulnerabilities within the website that users enter. The program will examine the structure of the website for vulnerabilities. If a vulnerability is found, the program will report the results of the investigation along with details of the vulnerability, such as the source of the vulnerability. Vulnerability information The cause of the vulnerability It can also tell you how to solve the vulnerabilities that occur as well. The program was developed using the Javascript language and Electron JS framework to design the program's interface and uses an API from non-profit organization OWASP to detect vulnerabilities. and using a more inventive approach to detecting vulnerabilities more comprehensively than traditional

Keywords: A more comprehensive, in-house method of detecting vulnerabilities.

## กิตติกรรมประกาศ

โครงงานนี้สำเร็จลุล่วงได้ด้วยความกรุณาจากอาจารย์ด็อกเตอร์เพชร อิ่มทองคำ อาจารย์ที่ปรึกษาโครงงานที่ได้ให้ข้อเสนอแนะ แนวทาง แนวคิด ตลอดจนวิธีแก้ไขข้อบกพร่องต่างๆ มาโดยตลอด จนโครงงานเล่มนี้เสร็จสมบูรณ์ ผู้ศึกษาจึงขอกราบขอบพระคุณเป็นอย่างสูง

ขอกราบขอบพระคุณคุณ primetogo ที่อนุญาตให้เก็บความต้องการของโปรแกรมและให้แนวทางในการสร้างโปรแกรม และเป็นแรงบันดาลใจให้เสมอมา

ขอบคุณรุ่นพี่ทุกคนที่ให้คำปรึกษาในการจัดเรียงเนื้อหาในรายงานโครงงานทุกเล่ม และให้คำปรึกษาเกี่ยวกับหัวข้อในการทำโครงงาน

สุดท้ายนี้ขอขอบคุณเพื่อนๆที่ช่วยให้คำแนะนำดีๆ เกี่ยวกับการใช้ภาษาอังกฤษ และเกี่ยวกับโครงงานชิ้นนี้

ผู้จัดทำ

ตนุสรณ์ สนธิมูล

รัฐศาสตร์ เพียวงษ์

# สารบัญ

# สารบัญตาราง

# สารบัญภาพ

**การเสนอเค้าโครงโครงงานคอมพิวเตอร์**

**วิทยาลัยการคอมพิวเตอร์ สาขาเทคโนโลยีสารสนเทศ มหาวิทยาลัยขอนแก่น**

ชื่อ นายตนุสรณ์ สนธิมูล รหัสประจำตัว 633020030-8

Mr. Thanuson Sonthimoon

นายรัฐศาสตร์ เพียวงษ์ รหัสประจำตัว 633020323-3

Mr. Rathasat Peerwong

นักศึกษาระดับปริญญาตรี เทคโนโลยีสารสนเทศ

อาจารย์ที่ปรึกษาโครงงาน อ.ดร.เพชร อิ่มทองคำ

Project Advisor Phet Aimtongkham, Ph.D.

**ชื่อหัวข้อโครงงาน**

ภาษาไทย โปรแกรมตรวจสอบช่องโหว่ของเว็บไซต์

ภาษาอังกฤษ Website vulnerability checker Program

# บทที่ 1

# บทนำ

## หลักการและเหตุผล

ในโลกปัจจุบันอินเทอร์เน็ตและเครือข่ายไร้สายได้รับการพัฒนาอย่างรวดเร็ว จนสามารถติดต่อสื่อสารกันได้ฟรีโดยไม่เสียค่าใช้จ่าย ทำให้ชีวิตผู้คนสะดวกสบายขึ้น และมีหลายอย่างเกิดขึ้นมากมาย เพื่อดึงดูดให้ผู้คนเข้ามาใช้อินเทอร์เน็ตมากขึ้น หนึ่งในสิ่งที่เกิดขึ้นและแพร่หลายเป็นอย่างมากคือ การสร้างเว็บไซต์เพื่อจะทำอะไรบางอย่าง อาทิ การสร้างเว็บไซต์ขึ้นมาเพื่อพูดคุย สื่อสารกับผู้อื่น ขายของต่างๆ สร้างไลฟ์สไตล์การใช้ชีวิตใหม่ๆ ให้ผู้คนได้รับชมรับฟังกัน หรือให้ข้อมูลข่าวสารความรู้ใหม่ๆ เพื่อเป็นประโยชน์ต่อผู้อื่น ซึ่งเว็บไซต์ต่างๆนั้น มีการเก็บรวบรวมข้อมูลของผู้ใช้ไว้มากมาย ทำให้เป็นที่หมายตาของเหล่าแฮกเกอร์ที่ไม่ประสงค์ดี ก่อให้เกิดการเข้ามาจารกรรมข้อมูลของเว็บไซต์โดยอาศัยช่องโหว่ของเว็บไซต์ต่างๆ ซึ่งช่องโหว่ความปลอดภัยนั้นอาจจะเกิดจากการเขียนโปรแกรมที่ไม่รัดกุม ความผิดพลาดของระบบการใช้งานซอฟต์แวร์ที่ไม่ปลอดภัยในการรันเซิร์ฟเวอร์ จนไปถึงการละเลยการอัปเดตแก้ไขช่องโหว่ความปลอดภัยจากผู้ดูแลระบบ ก่อให้เกิดความเสียหายกับข้อมูลส่วนตัวของผู้ใช้เว็บไซต์นั้นๆ และสร้างผลเสียต่อความเชื่อมั่นของแบรนด์อย่างคาดไม่ถึง

ปัจจุบันมีโครงการที่รวบรวมช่องโหว่ของเว็บไซต์และวิธีแก้ไขปัญหาไว้มากมาย หนึ่งในนั้นคือโครงการ OWASP Top 10 จัดขึ้นโดยองค์กรไม่แสวงหาผลกำไรที่เรียกว่ามูลนิธิ OWASP ซึ่งเป็นโครงการที่รวบรวมช่องโหว่ยอดนิยมของระบบเว็บไซต์เอาไว้และอธิบายรายละเอียดของช่องโหว่ที่พบได้บ่อยและมีความรุนแรงที่สุด 10 อันดับแรก นอกจากนี้ OWASP ยังมีการสร้างเครื่องมือที่ชื่อว่า OWASP ZAP ซึ่งเป็นซอฟต์แวร์โอเพ่นซอร์ส (Opensource) สำหรับประเมินความเสี่ยงด้วยการทดสอบเจาะระบบ (Pen test) เพื่อค้นหาช่องโหว่ในเว็บแอปพลิเคชันตาม OWASP Top Ten ซึ่งได้รับการตอบรับเป็นอย่างดีจากนักพัฒนาเว็บแอปพลิเคชันทั่วโลก และได้รับการยึดถือเป็นมาตรฐานการตรวจสอบช่องโหว่เว็บแอปพลิเคชันที่อธิบายรายละเอียดของช่องโหว่ที่พบได้บ่อยและมีความรุนแรง 10 อันดับแรก

คณะผู้จัดทำเล็งเห็นว่าต้องมีการศึกษาค้นคว้าเพื่อหาช่องโหว่หรือจุดอ่อนของเว็บไซต์ว่ามีช่องโหว่หรือจุดอ่อนหรือไม่แล้วช่องโหว่หรือจุดอ่อนนั้นมีความรุนแรงมากน้อยเพียงใด จึงได้จัดทำโปรแกรมตรวจสอบช่องโหว่ของเว็บไซต์ขึ้นมาเพื่อเป็นแนวทางป้องกันการถูกโจมตีจากการใช้ประโยชน์จากช่องโหว่หรือจุดอ่อนของเว็บไซต์

**วัตถุประสงค์ของโครงงาน**

1. เพื่อจัดทำโปรแกรมที่สามารถตรวจสอบช่องโหว่ของเว็บไซต์ได้
2. เพื่ออำนวยความสะดวกให้เจ้าหน้าที่ที่ทำงานด้านความปลอดภัย

# บทที่ 2

# ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

## ทฤษฎีและผลงานวิจัยที่เกี่ยวข้อง

### 1. ทฤษฎีที่เกี่ยวข้อง

#### 1.1 Cyber Security

Cyber Security หรือการรักษาความปลอดภัยทางไซเบอร์เป็นแนวทางวิธีในการป้องกันระบบหรือข้อมูลที่มีความสำคัญจากการโจมตีทางไซเบอร์ ซึ่งมักจะเข้ามาขัดขวางหรือขโมยข้อมูลจากระบบการดำเนินงานของธุรกิจเพื่อผลประโยชน์บางอย่าง เช่น นำข้อมูลที่ได้มา ไปขายในตลาดมืด ขัดขวาง ทำลาย หรือก่อกวนเว็บไซต์ทางธุรกิจ ทำให้ธุรกิจเกิดความเสียหา เป็นต้น ทำให้ Cyber Security ยิ่งมีบทบาทสำคัญกับเว็บไซต์ เพื่อต่อสู้กับภัยคุกคามต่อระบบเครือข่ายและข้อมูล

#### 1.2 NIST Cybersecurity Framework

NIST Cybersecurity Framework ดำเนินการสร้างโดย สถาบันมาตรฐานและเทคโนโลยีแห่งชาติของประเทศสหรัฐอเมริกา(National Institute of Standards and Technology:NIST) ดำเนินการสร้างขึ้นมาจากการที่ข้อมูลบนโลกไซเบอร์ถูกโจมตีได้รับความเสียหายต่อเศรฐกิจ และความมั่นคงของประเทศ โดยจุดประสงค์ในการสร้างเพื่อช่วยให้องค์กรมีวิธีการจัดการกระบวนการป้องกันและรับมือจากการโจมตีทางไซเบอร์ได้อย่างมีประสิทธิภาพ โดยโครงสร้างของ NIST Cybersecurity Framework ประกอบไปด้วย

(1) ระบุ (Identify) การเข้าใจบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง

(2) ปกป้อง (Protect) การวางมาตรฐานเพื่อป้องกันระบบขององค์กร

(3) ตรวจสอบ (Detect) กำหนดขั้นตอนการทำงานของกระบวนการต่างๆ เพื่อตรวจสอบสถาการณ์ที่ผิดปกติ

(4)ตอบสนอง (Respond) กำหนดขั้นตอนการทำงานของกระบวนการต่างๆ เพื่อรับมือกับสถานการณ์ที่ผิดปกติ

(5) กอบกู้ (Recover) กำหนดขั้นตอนการทำงานของกระบวนการต่างๆ เพื่อให้สามารถดำเนินการกระบวนการทำงานได้อย่างต่อเนื่อง และกู้คืนระบบให้กลับมาใช้งานได้เหมือนเดิม

## 2. ผลงานวิจัยที่เกี่ยวข้อง

2.1 OWASP

OWASP หรือ Open Web Application Security Project เป็นชุมชนออนไลน์ที่ผลิตบทความ วิธีการ เอกสาร เครื่องมือ และเทคโนโลยีที่พร้อมใช้งานได้อย่างอิสระในด้านความปลอดภัยของเว็บแอปพลิเคชัน โครงการ OWASP เปิดให้ใช้งานได้ฟรี นำโดยองค์กรไม่แสวงหาผลกำไรที่เรียกว่า มูลนิธิ OWASP มีงานวิจัยคือ OWASP Top 10 -2021 เป็นผลงานวิจัยที่ตีพิมพ์ล่าสุดซึ่งได้รับความร่วมมือจากองค์กรพันธมิตรกว่า 40 แห่ง นอกจากนี้ OWASP ยังมีการสร้างเครื่องมือที่ชื่อว่า OWASP ZAP ซึ่งเป็นซอฟต์แวร์โอเพ่นซอร์ส (Opensource) สำหรับประเมินความเสี่ยงด้วยการทดสอบเจาะระบบ (Pen test) เพื่อค้นหาช่องโหว่บนเว็บแอปพลิเคชันตาม OWASP Top Ten ซึ่งได้รับการตอบรับเป็นอย่างดีจากนักพัฒนาเว็บแอปพลิเคชันทั่วโลก และได้รับการยึดถือเป็นมาตรฐานการตรวจสอบช่องโหว่เว็บแอปพลิเคชันที่อธิบายรายละเอียดของช่องโหว่ที่พบได้บ่อยและมีความรุนแรง 10 อันดับแรก โดยความรุนแรงของช่องโหว่ที่ได้รับการจัดอันดับในปี 2021 ได้แก่

(1) Broken Access Control คือการข้ามสิทธิ์ เป็นช่องโหว่ที่ผู้ใช้สามารถเข้าถึงสิทธิ์บางอย่างได้หรือดำเนินการบางอย่างได้ โดยที่ผู้ใช้ไม่ควรจะได้รับสิทธ์การเข้าถึงได้นั้นได้

(2) Cryptographic Failures คือช่องโหว่ที่เกิดจากการที่ข้อมูลถูกส่งไปในช่องทางที่ไม่ปลอดภัย หรือเป็นช่องโหว่ด้านความปลอดภัยที่สำคัญซึ่งที่เปิดเผยข้อมูลที่ละเอียดอ่อนบนอัลกอริธึมการเข้ารหัส

(3) Injection คือช่องโหว่ที่เกิดขึ้นกับฐานข้อมูล โดยจะใช้ Command บางอย่างในการใส่เข้าไปในช่อง Text Field บนหน้าเว็บไซต์ แล้วทำการจัดการ access ข้อมูล เพื่อที่จะให้มีข้อมูลแสดงออกมา

(4) Insecure Design ความเสี่ยงต่อข้อบกพร่องด้านการออกแบบระบบที่มีความปลอดภัยไม่เพียงพอ

(5) Security Misconfiguration ช่องโหว่ที่มีการตั้งค่าความปลอดภัยไม่ถูกต้อง ทำให้เวลาที่เว็บไซต์ทำงานอยู่แล้วเกิด Error ขึ้นจะแสดง Error Handling แล้วแสดงข้อมูล Debug พร้อมโค้ดในส่วนที่ Error ทำให้สามารถใช้โค้ดส่วนที่ Error ในการโจมตีเว็บไซต์ได้

(6) Vulnerable and Outdated Components คือช่องโหว่ที่เกิดจากการที่เลือกใช้ซอฟแวร์ที่ล้าสมัยมาพัฒนาระบบ ซอฟแวร์ที่ล้าสมัยนั้นไม่ได้มีการอัปเดตความปลอดภัยที่เป็นปัจจุบัน ทำให้ระบบของเว็บไซต์ที่พัฒนาเกิดช่องโหว่

(7) Identification and Authentication Failures คือช่องโหว่ที่เกิดจากการที่ไม่ได้จำกัดจำนวนครั้งครั้งในการยืนยันตัวตนหรือการรับรองความถูกต้องของผู้ใช้

(8) Software and Data Integrity Failures ความล้มเหลวของซอฟต์แวร์และความไม่สมบูรณ์ของข้อมูลเกี่ยวข้องกับรหัสและโครงสร้างพื้นฐานที่ไม่ได้ป้องกันการละเมิดความสมบูรณ์

(9) Security Logging and Monitoring Failures ความล้มเหลวในการบันทึก ตรวจสอบหรือรายงานเหตุการณ์ด้านความปลอดภัย เช่น ความพยายามในการเข้าสู่ระบบ ทำให้ตรวจจับพฤติกรรมที่น่าสงสัยได้ยาก และเพิ่มโอกาสอย่างมากที่ผู้โจมตีจะใช้ประโยชน์จาก

(10) Server-Side Request Forgery เกิดขึ้นเมื่อเว็บแอปพลิเคชันดึงทรัพยากรระยะไกลโดยไม่ตรวจสอบ URL ที่ผู้ใช้ระบุ


ภาพที่ 1 OWASP

ที่มา: https://owasp.org/assets/images/logo.png

2.2 รายงานของ Google Registry และ The Harris Poll ในปี 2019

ในช่วงไม่กี่ปีที่ผ่านมา ความสะดวกในการสร้างเว็บไซต์ได้เพิ่มขึ้น ต้องขอบคุณระบบจัดการเนื้อหา (CMS) เช่น WordPress และ Joomla เจ้าของธุรกิจจึงเป็นผู้ดูแลเว็บ ความรับผิดชอบในการรักษาความปลอดภัยเว็บไซต์อยู่ในมือคุณแล้ว แต่เจ้าของเว็บไซต์จำนวนมากยังไม่รู้วิธีทำให้เว็บไซต์ปลอดภัย เมื่อลูกค้าใช้ตัวประมวลผลการชำระเงินด้วยบัตรเครดิตออนไลน์ พวกเขาจำเป็นต้องรู้ว่าข้อมูลของพวกเขาปลอดภัย ผู้เข้าชมไม่ต้องการให้ข้อมูลส่วนบุคคลของพวกเขาตกไปอยู่ในมือของผู้อื่น ไม่ว่าคุณจะดำเนินธุรกิจขนาดเล็กหรือองค์กร ผู้ใช้คาดหวังประสบการณ์ออนไลน์ที่ปลอดภัย

รายงานปี 2019 โดย Google Registry และ The Harris Poll แสดงให้เห็นว่าแม้ว่าผู้คนจำนวนมากขึ้นกำลังสร้างเว็บไซต์ แต่ชาวอเมริกันส่วนใหญ่ยังมีช่องว่างด้านความรู้ที่สำคัญเกี่ยวกับความปลอดภัยในการรักษาความปลอดภัยออนไลน์ ในขณะที่ 55% ของผู้ตอบแบบสอบถามให้คะแนนความปลอดภัยทางออนไลน์แก่ตนเอง A หรือ B แต่ 70% ระบุอย่างไม่ถูกต้องว่า URL ที่ปลอดภัยควรเป็นอย่างไรสำหรับเว็บไซต์ มีหลายวิธีที่จะรับรองตัวเอง พนักงาน และลูกค้าว่าเว็บไซต์ของคุณปลอดภัย ทำตามขั้นตอนสำคัญเพื่อปรับปรุงความปลอดภัยของเว็บไซต์ของคุณ ช่วยป้องกันข้อมูลจากการสอดรู้สอดเห็น ไม่มีวิธีใดที่สามารถรับประกันได้ว่าเว็บไซต์ของคุณจะ "ปราศจากแฮ็กเกอร์" ตลอดไป การใช้วิธีการป้องกันจะลดความเสี่ยงของไซต์ของคุณ

ตารางที่ 1 เปรียบเทียบ

| **ความสามารถของงานวิจัย** | **Cyber Security** | **NIST Cybersecurity Framework** | **OWASP ZAP** | **การรักษาความปลอดภัยออนไลน์** | **โปรแกรมตรวจสอบช่องโหว่ของเว็บไซต์** |
|---|---|---|---|---|---|
| 1.ป้องกันระบบหรือข้อมูลที่มีความสำคัญจากการโจมตีทางไซเบอร์ | / | | / | | / |
| 2.ช่วยให้องค์กรณ์มีวิธีการจัดการกระบวนการป้องกันและรับมือจากการโจมตีทางไซเบอร์ได้อย่างมีประสิทธิภาพ | | / | / | | / |
| 3.ค้นหาช่องโหว่บนเว็บแอปพลิเคชัน | | | / | | / |
| 4.จัดระดับความเสี่ยง | | | / | | / |
| 5.ตรวจสอบการอัปเดตซอต์ฟแวร์เซิร์ฟเวอร์ | | | | / | / |
| 6.ตรวจสอบการอัปเดต Engine HTTP | | | | / | / |
| 7.ตรวจสอบความน่าเชื่อถือของบริษัท Certificate HTTPS | | | | / | / |
| 8.ตรวจสอบวันหมดอายุของ Certificate | | | | / | / |

# บทที่ 3

# วิธีการดำเนินงาน

## วิธีดำเนินการวิจัย

1. วิเคราะห์ปัญหาและความต้องการ

ในปัจจุบันอินเทอร์เน็ต ได้เข้ามามีบทบาทในชีวิตประจำวันของผู้คนทั่วไปมากขึ้นทำให้ผู้คนทุกเพศทุกวัยสามารถเข้าถึงสามารถเข้าถึงสื่อบนอินเทอร์เน็ตได้ง่ายขึ้น สื่อเว็บไซต์จึงเริ่มเข้ามามีบทบาทต่อผู้คนมากกว่าเมื่อก่อน ทำให้มีเว็บไซต์เกิดใหม่ เกิดขึ้นมากมาย บางเว็บไซต์มีเจ้าของเป็นมือใหม่ การเปิดจึงต้องอาจไม่ได้คำนึงถึงความปลอดภัยมากนัก ทำให้อาจเกิดช่องโหว่โดยเจ้าของเว็บไซต์ไม่ได้ตั้งใจ การรักษาความปลอดภัยของเว็บไซต์จึงเป็นเรื่องที่ทำได้ยาก เพราะต้องเป็นผู้เชี่ยวชาญ มีความรู้เรื่องความปลอดภัยของเว็บไซต์ จึงจะสามารถทำได้ดี คณะผู้จัดทำจึงเล็งเห็นปัญหาของการหาช่องโหว่เว็บไซต์ จึงได้จัดทำโปรแกรมตรวจสอบช่องโหว่เว็บไซต์ขึ้นมาเพื่อให้การตรวจสอบช่องโหว่สามารถทำได้ง่ายขึ้นและทำให้เว็บไซต์มีความปลอดภัยมากขึ้น

2. ศึกษาทฤษฎี และงานวิจัยที่เกี่ยวข้อง

2.1 ศึกษาข้อมูลเกี่ยวกับ OWASP เพื่อเป็นข้อมูลในการทำโครงงาน

2.2 ศึกษาความเสี่ยงที่ระบบจะถูกแฮกเพื่อเป็นแนวทางปฏิบัติในการบริหารจัดการความเสี่ยงของเว็บไซต์

2.3 ศึกษาเกี่ยวกับเครื่องมือหรือโปรแกรมที่ใช้ในการพัฒนาโครงงาน

2.4 ศึกษาข้อมูลและวิธีใช้งานเครื่องมือต่างๆ ที่จะใช้ในงานวิจัย

2.3.1 OWASP

OWASP คือ มาตรฐานความปลอดภัยของเว็บแอปพลิเคชันที่จัดทำขึ้นโดยองค์กรไม่แสวงหาผลกำไรที่ให้ความรู้เรื่องความปลอดภัยในระบบคอมพิวเตอร์เพื่อให้ระบบคอมพิวเตอร์มีความปลอดภัยมากขึ้น และมีการทำวิจับทางด้าน Web

Application Security โดยมีชุมชนทางด้านเอกสาร และเครื่องมือช่วยเหลือต่างๆ ที่น่าสนใจ ซึ่ง OWASP มีโครงการที่จัดอันดับ 10 อันดับความเสี่ยงด้านความปลอดภัย ที่เรียกว่า OWASP TOP 10 ซึ่งเหมาะแก่การนำมาศึกษาเป็นอย่างมาก

2.3.2 Burp Suite

Burp Suite คือ เครื่องมือสำหรับทดสอบระบบเว็บไซต์ โดยทำตัวเป็น proxy จับการร้องขอ และการตอบกลับจาก API ซึ่งเป็นเครื่องมือที่น่าสนใจ เหมาะแก่การศึกษาเพื่อทำโครงงาน

2.5 กำหนดขอบเขตและเป้าหมายของโครงงาน

2.5.1 ตรวจสอบเว็บไซต์ตามข้อมูลลักษณะการโจมตีที่มีใน OWASP

2.5.2 ตรวจหา URLs และข้อมูลที่อยู่บนเว็บเซิร์ฟเวอร์ได้

2.5.3 รายงานผลการทดสอบ

3. เขียนเค้าโครงโครงงานและเสนออาจารย์ที่ปรึกษา

ติดต่ออาจารย์ที่ปรึกษาเพื่อนำเสนอโครงงานและถามถึงปัญหาที่พบ

4. กำหนดขอบเขตและเป้าหมายของโครงงาน

5. วิเคราะห์และออกแบบระบบ

6. เขียนเค้าโครงโครงงานและเสนออาจารย์ที่ปรึกษา

7. สร้างและพัฒนาระบบ

8. ทดสอบระบบ

นำระบบที่พัฒนาเสร็จแล้วไปให้เจ้าหน้าที่ที่ทำงานเกี่ยวกับการตรวจสอบช่องโหวของเว็บไซต์

9. วิเคราะห์และสรุปผลการทำโครงงาน

10. จัดทำรายงานโครงงานและคู่มือพร้อมจัดพิมพ์ฉบับสมบูรณ์

จัดทำรายงานโครงงานและคู่มือ พร้อมจัดพิมพ์ฉบับสมบูรณ์ของโครงงาน

ตารางที่ 2 แผนและระยะเวลาดำเนินการ

| การดำเนินงาน | สัปดาห์ที่/เดือน | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ปี 2565 | | | | | | | | | | | | | | | | | | | | | | | | ปี 2566 | | | | | | | | | | | |
| | กรกฎาคม | | | | สิงหาคม | | | | กันยายน | | | | ตุลาคม | | | | พฤศจิกายน | | | | ธันวาคม | | | | มกราคม | | | | กุมภาพันธ์ | | | | มีนาคม | | | |
| | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| 1) วิเคราะห์ปัญหาและความต้องการ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2) ค้นคว้าและศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้อง | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3) ศึกษาข้อมูลและวิธีใช้งานเครื่องมือต่างๆ ที่จะใช้ในงานวิจัย | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4) กำหนดขอบเขตและเป้าหมายของโครงงาน | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5) วิเคราะห์และออกแบบระบบ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

ตารางที่ 2 แผนและระยะเวลาดำเนินการ (ต่อ)

| การดำเนินงาน | สัปดาห์ที่/เดือน | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ปี 2565 | | | | | | | | | | | | | | | | | | | | | | | | ปี 2566 | | | | | | | |
| | กรกฎาคม | | | | สิงหาคม | | | | กันยายน | | | | ตุลาคม | | | | พฤศจิกายน | | | | ธันวาคม | | | | มกราคม | | | | กุมภาพันธ์ | | | |
| | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| 6) เขียนเค้าโครงโครงงาน | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 7) สร้างและพัฒนาระบบ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 8) ทดสอบระบบ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 9) วิเคราะห์และสรุปผลการทำโครงงาน | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 10) จัดทำรายงานโครงงานและคู่มือพร้อมจัดพิมพ์ฉบับสมบูรณ์ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 11) นำเสนอ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

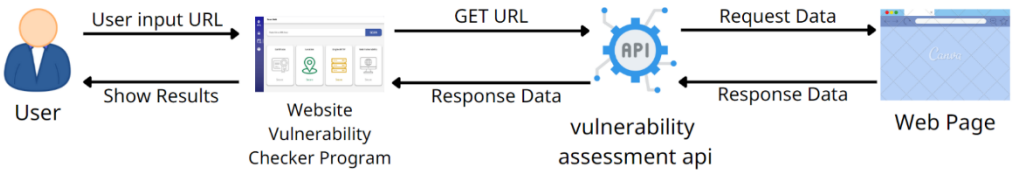
# บทที่ 4

# การวิเคราะห์ระบบและพัฒนาโปรแกรม

## 1. วิเคราะห์และออกแบบระบบ

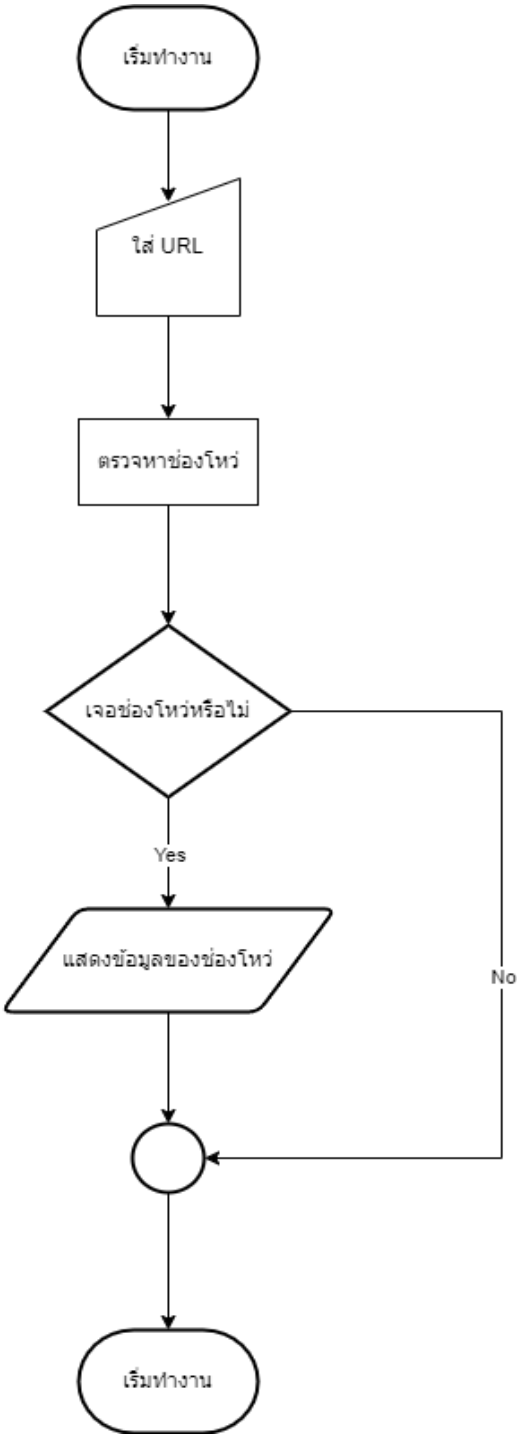
### 1.1 ภาพรวมระบบ

**ภาพรวมระบบ**




ภาพที่ 2 ภาพรวมระบบ

1.2 การทำงานของโปรแกรม

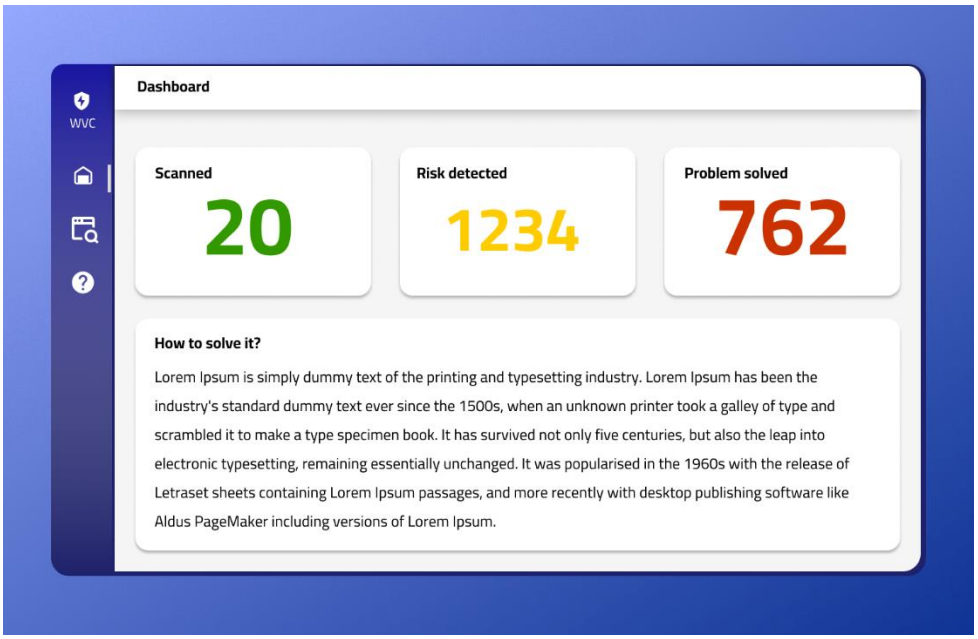



ภาพที่ 3 flowchart การทำงานของโปรแกรม

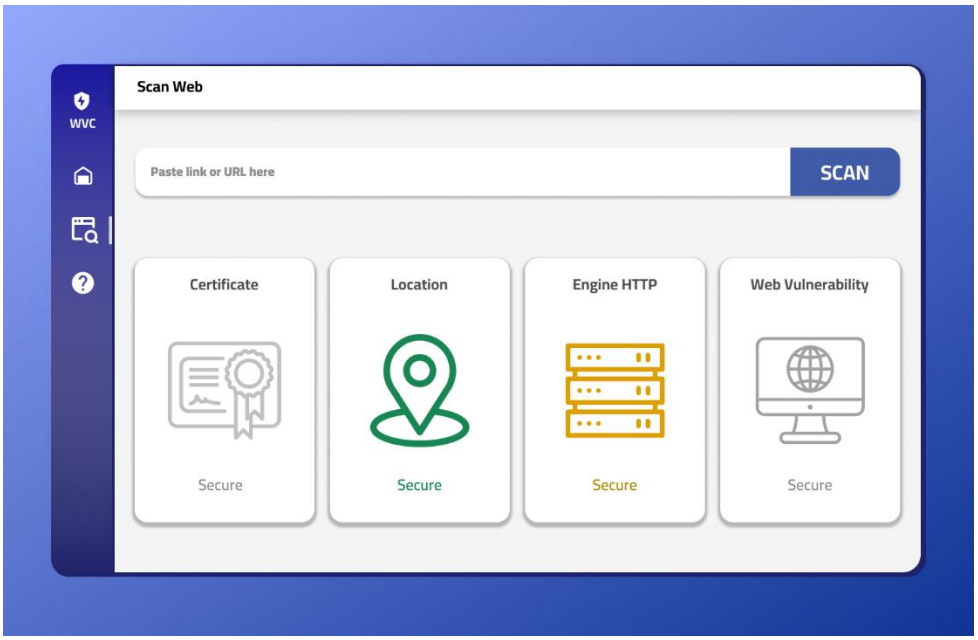
1.3 Use case diagram


ภาพที่ 4 Use case diagram

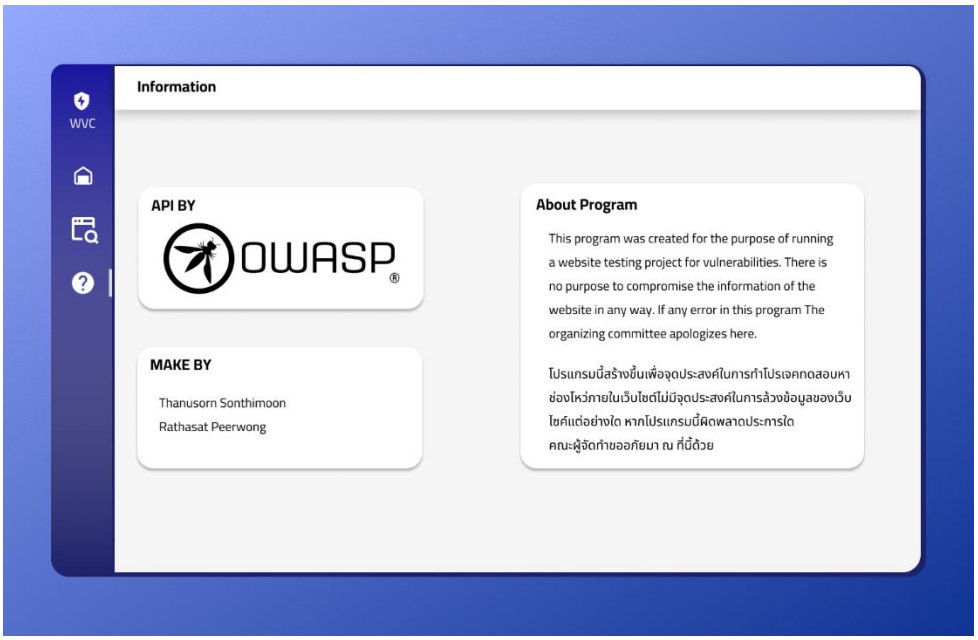
## 1.4 Prototype




ภาพที่ 5 Prototype หน้า Home




ภาพที่ 6 Prototype หน้า Scan




ภาพที่ 7 Prototype หน้า About

## 2. ขอบเขตและข้อจำกัดของการวิจัย

### 2.1 ขอบเขต

1. เพื่อตรวจสอบการอัปเดต Engine HTTP (ใช้ API)
2. เพื่อตรวจสอบความน่าเชื่อถือของบริษัทของใบรับรอง HTTPS (ใช้ API)
3. เพื่อตรวจสอบการหมดอายุของใบรับรอง (ใช้ API)
4. สามารถทดสอบโจมตีเว็บไซต์ตามข้อมูลลักษณะการโจมตีที่มีใน OWASP Top 10 2021 ประกอบไปด้วย

(1) Broken Access Control คือการข้ามสิทธิ์ เป็นช่องโหว่ที่ผู้ใช้สามารถเข้าถึงสิทธิ์บางอย่างได้หรือดำเนินการบางอย่างได้ โดยที่ผู้ใช้ไม่ควรจะได้รับสิทธ์การเข้าถึงได้นั้นได้

(2) Cryptographic Failures คือช่องโหว่ที่เกิดจากการที่ข้อมูลถูกส่งไปในช่องทางที่ไม่ปลอดภัย หรือเป็นช่องโหว่ด้านความปลอดภัยที่สำคัญซึ่งที่เปิดเผยข้อมูลที่ละเอียดอ่อนบนอัลกอริธึมการเข้ารหัส

(3) Injection คือช่องโหว่ที่เกิดขึ้นกับฐานข้อมูล โดยจะใช้ Command บางอย่างในการใส่เข้าไปในช่อง Text Field บนหน้าเว็บไซต์ แล้วทำการจัดการ access ข้อมูลเพื่อที่จะให้มีข้อมูลแสดงออกมา

(4) Insecure Design ความเสี่ยงต่อข้อบกพร่องด้านการออกแบบระบบที่มีความปลอดภัยไม่เพียงพอ

(5) Security Misconfiguration ช่องโหว่ที่มีการตั้งค่าความปลอดภัยไม่ถูกต้อง ทำให้เวลาที่เว็บไซต์ทำงานอยู่แล้วเกิด Error ขึ้นจะแสดง Error Handling แล้วแสดงข้อมูล Debug พร้อมโค้ดในส่วนที่ Error ทำให้สามารถใช้โค้ดส่วนที่ Error ในการโจมตีเว็บไซต์ได้

(6) Vulnerable and Outdated Components คือช่องโหว่ที่เกิดจากการที่เลือกใช้ซอฟแวร์ที่ล้าสมัยมาพัฒนาระบบ ซอฟแวร์ที่ล้าสมัยนั้นไม่ได้มีการอัปเดตความปลอดภัยที่เป็นปัจจุบัน ทำให้ระบบของเว็บไซต์ที่พัฒนาเกิดช่องโหว่

(7) Identification and Authentication Failures คือช่องโหว่ที่เกิดจากการที่ไม่ได้จำกัดจำนวนครั้งครั้งในการยืนยันตัวตนหรือการรับรองความถูกต้องของผู้ใช้

(8)Software and Data Integrity Failures ความล้มเหลวของซอฟต์แวร์และความไม่สมบูรณ์ของข้อมูลเกี่ยวข้องกับรหัสและโครงสร้างพื้นฐานที่ไม่ได้ป้องกันการละเมิดความสมบูรณ์

(9) Security Logging and Monitoring Failures ความล้มเหลวในการบันทึกตรวจสอบ หรือรายงานเหตุการณ์ด้านความปลอดภัย เช่น ความพยายามในการเข้าสู่ระบบ ทำให้ตรวจจับพฤติกรรมที่น่าสงสัยได้ยาก และเพิ่มโอกาสอย่างมากที่ผู้โจมตีจะใช้ประโยชน์จาก

(10) Server-Side Request Forgery เกิดขึ้นเมื่อเว็บแอปพลิเคชันดึงทรัพยากรระยะไกลโดยไม่ตรวจสอบ URL ที่ผู้ใช้ระบุ

2.2 ข้อจำกัด

1. ไม่สามารถตรวจสอบช่องโหว่ที่ยังไม่มีการตรวจพบได้

2. ไม่สามารถตรวจสอบช่องโหว่ของเว็บไซต์ที่มีการล็อก URL ไว้ได้

**3. สถานที่ทำวิจัย**

วิทยาลัยการคอมพิวเตอร์ มหาวิทยาลัยขอนแก่น

หอสมุดกลาง มหาวิทยาลัยขอนแก่น

**4. ประโยชน์ที่คาดว่าจะได้รับ**

1. โปรแกรมสามารถตรวจสอบช่องโหว่ของเว็บไซต์ได้

2. นักพัฒนาสามารถเช็คช่องโหว่ของเว็บไซต์ได้ง่ายขึ้น

3. เซิร์ฟเวอร์ได้รับการอัปเดตเป็นเวอร์ชันล่าสุดเสมอ

4. Engine HTTP ได้รับการอัปเดตอยู่เสมอ

5. Certificate HTTPS อยู่ในบริษัทที่น่าเชื่อถือและมีความปลอดภัย

6. Certificate ได้รับการอัปเดตอย่างสม่ำเสมอ

# บทที่ 5

# บทสรุป

## 1. สรุปผลการดำเนินโครงงาน

การพัฒนาโปรแกรมตรวจสอบช่องโหว่ของเว็บไซต์ พัฒนาขึ้นมาเพื่อเป็นเครื่องมือที่ช่วยในการตรวจสอบช่องโหว่ของเว็บไซต์ โดยผู้จัดทำได้ดำเนินการตามแผนงานที่ได้กำหนดไว้ดังนี้

ตารางที่ 3 สรุปผลการดำเนินงาน

| ลำดับ | การดำเนินงาน | ความก้าวหน้า (%) |
|---|---|---|
| 1 | วิเคราะห์ปัญหาและความต้องการ | 100 |
| 2 | ค้นคว้าและศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้อง | 100 |
| 3 | ศึกษาข้อมูลและวิธีใช้งานเครื่องมือต่างๆ ที่จะใช้ในงานวิจัย | 100 |
| 4 | กำหนดขอบเขตและเป้าหมายของโครงงาน | 100 |
| 5 | วิเคราะห์และออกแบบระบบ | 100 |
| 6 | เขียนเค้าโครงโครงงาน | 100 |
| 7 | สร้างและพัฒนาระบบ | 70 |

ตารางที่ 3 สรุปผลการดำเนินงาน (ต่อ)

| ลำดับ | การดำเนินงาน | ความก้าวหน้า (%) |
|---|---|---|
| 8 | ทดสอบระบบ | 70 |
| 9 | วิเคราะห์และสรุปผลการทำโครงงาน | 0 |

**2. ข้อจำกัดของระบบ**

2.1 ไม่สามารถตรวจสอบช่องโหว่ที่ยังไม่มีการตรวจพบได้

2.2 ไม่สามารถตรวจสอบช่องโหว่ของเว็บไซต์ที่มีการล็อก URL ไว้ได้

**3. ปัญหาอุปสรรค และ แนวทางแก้ไข**

**ปัญหาที่ 1 :** ไฟล์ Report และตัวโปรแกรมตรวจสอบช่องโหว่เว็บไซต์ที่ใช้ Electron Framework ไม่สามารถใช้งานด้วยกันได้

**การแก้ไข :** เนื่องจากบันทึกไฟล์ Report เป็นไฟล์ประเภท html ทำให้ต้องเปลี่ยนจากโปรแกรมมาเป็นการพัฒนาเว็บแอปพลิเคชันแทน

**ปัญหาที่ 2 :** ปัญหาการเรียกใช้ไฟล์ที่มีประเภทที่แตกต่างกัน (JavaScript, Python, HTML, PHP)

**การแก้ไข :** เลือกใช้ JavaScript ในการเชื่อมต่อไฟล์ทั้งหมด

**ปัญหาที่ 3 :** เวอร์ชั่นของ NodeJS มีการอัปเดตทำให้วิธีการเขียนเปลี่ยนแปลจากเดิม

**การแก้ไข :** สร้างโปรเจคใหม่ทั้งหมด โดยยังใช้ไฟล์โครงสร้างของ HTML เดิม

**ปัญหา 4 :** เนื่องจากไฟล์ Report.html เป็นการสร้างไฟล์ใหม่ทุกครั้งที่มีการตรวจสอบเว็บไซต์ทำให้ยากต่อการจัดแต่งหน้าเว็บไซต์ให้เป็นระเบียบ

**การแก้ไข :** เขียนบนภาษา PHP ใช้คำสั่ง <?php include 'Report.html'; ?> เพื่ออ้างอิงไฟล์

## 4. ข้อเสนอแนะ ในการพัฒนาต่อไป

1. จัดไฟล์ Report ให้ดูง่าย เข้าใจง่าย เป็นระเบียบกว่านี้
2. การเรียกใช้ OWASP API ควรเรียกใช้ OWASP Zap จาก Cloud

## แบบประเมินโครงงาน

**คำชี้แจง** ให้ประเมินโครงงานโดยทำเครื่องหมาย ✓

ข้อมูลของผู้ประเมิน

1. เพศ ○ ชาย ○ หญิง

2. ชั้นปี ○ ปริญญาตรี ○ ปริญญาโท ○ ปริญญาเอก

เกณฑ์การประเมิน 5 ระดับดังนี้ มากที่สุด = 5 , มาก = 4 , ปานกลาง = 3, น้อย = 2 ,น้อยที่สุด = 1

**ด้านการออกแบบและการจัดรูปแบบ**

| รายการประเมิน | ระดับความคิดเห็น | | | | |
|---|---|---|---|---|---|
| | มากที่สุด | มาก | ปานกลาง | น้อย | น้อยที่สุด |
| 1. ความสวยงาม ความทันสมัย น่าสนใจของหน้าโฮมเพจ | | | | | |
| 2. การจัดรูปแบบในเว็บไซต์ง่ายต่อการอ่านและการใช้งาน | | | | | |
| 3. สีสันในการออกแบบเว็บไซต์มีความเหมาะสม | | | | | |
| 4. เมนูง่ายต่อการใช้งาน | | | | | |
| 5. สีพื้นหลังกับสีตัวอักษรมีความเหมาะสมต่อการอ่าน | | | | | |
| 6. ขนาดตัวอักษร และรูปแบบตัวอักษร อ่านได้ง่ายและสวยงาม | | | | | |
| 7. ภาพกับเนื้อหามีความสอดคล้องกันและสามารถสื่อความหมายได้ | | | | | |
| 8. โดยภาพรวมท่านมีความพึงพอใจในการออกแบบเว็บไซต์ในระดับใด | | | | | |

**ด้านคุณภาพของเนื้อหา**

| รายการประเมิน | ระดับความคิดเห็น | | | | |
|---|---|---|---|---|---|
| | มากที่สุด | มาก | ปานกลาง | น้อย | น้อยที่สุด |
| 1. ความสะดวกในการเชื่อมโยงข้อมูลภายในเว็บไซต์ | | | | | |
| 2. ความรวดเร็วในการดาวน์โหลดข้อมูล | | | | | |
| 3. ความถูกต้องครบถ้วนของข้อมูล | | | | | |
| 4. ความเหมาะสมของข้อมูลภายในเว็บไซต์ | | | | | |
| 5. โดยภาพรวมท่านมีความพึงพอใจในคุณภาพของเนื้อหาระดับใด | | | | | |

**ข้อเสนอแนะ**

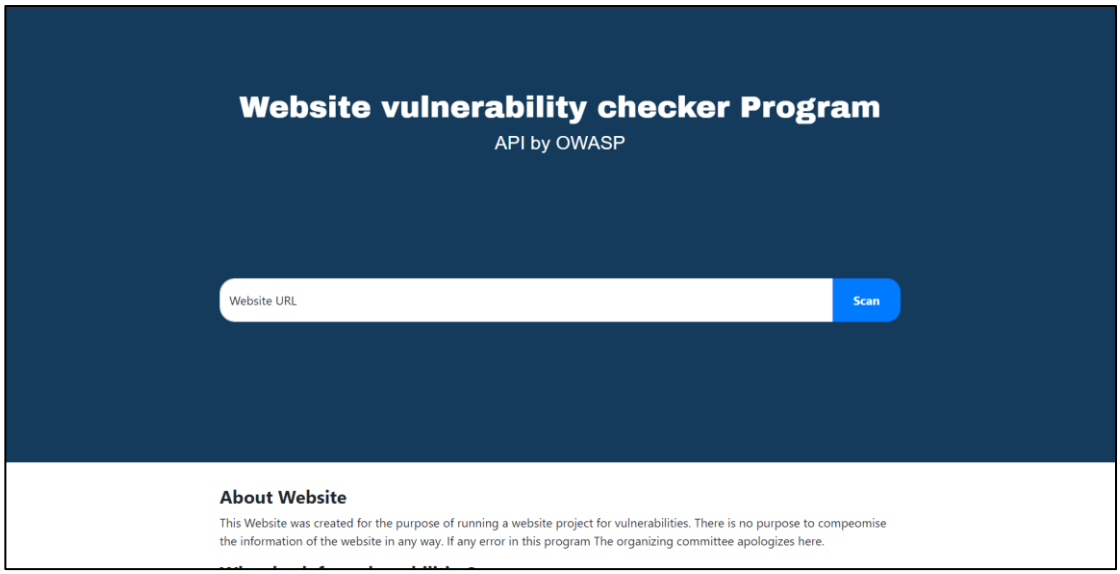
.....

.....

.....

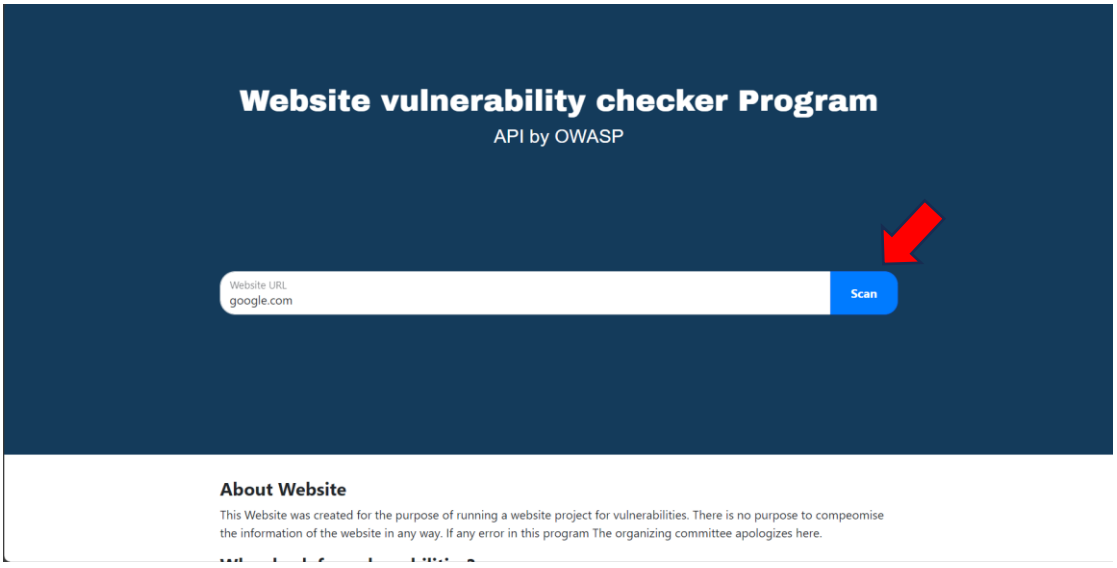
## คู่มือการใช้งาน

1. ผู้ใช้คัดลอก URL ของเว็บไซต์ที่ต้องงการตรวจสอบ วางที่ช่อง “Website URL”



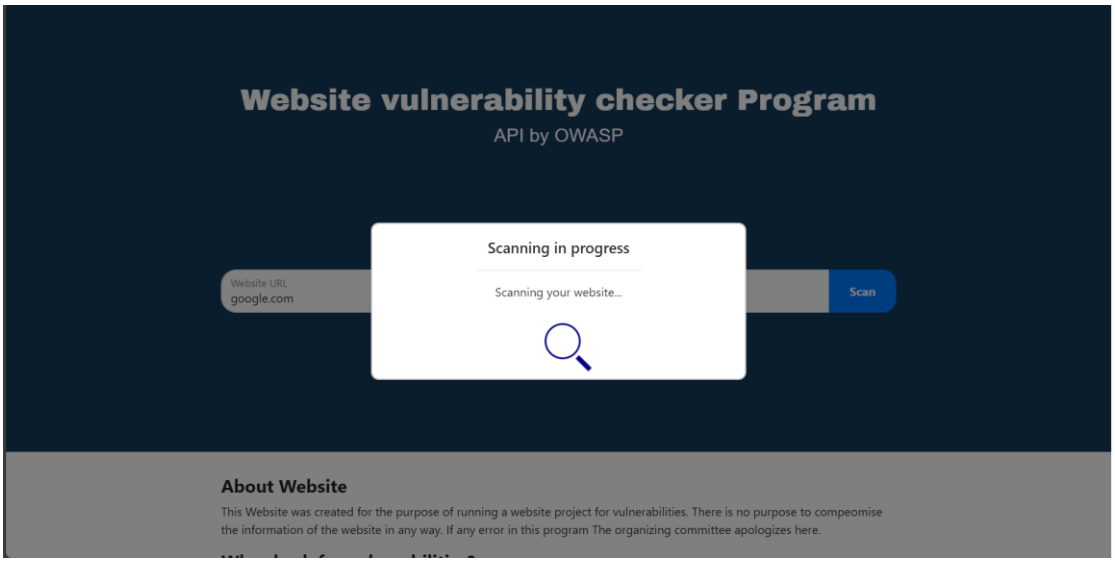

**ภาพที่ 8** หน้า Home page ของเว็บไซต์

2. เมื่อวาง URL ของเว็บไซต์ที่ต้องการตรวจสอบเสร็จแล้ว กดปุ่ม Scan



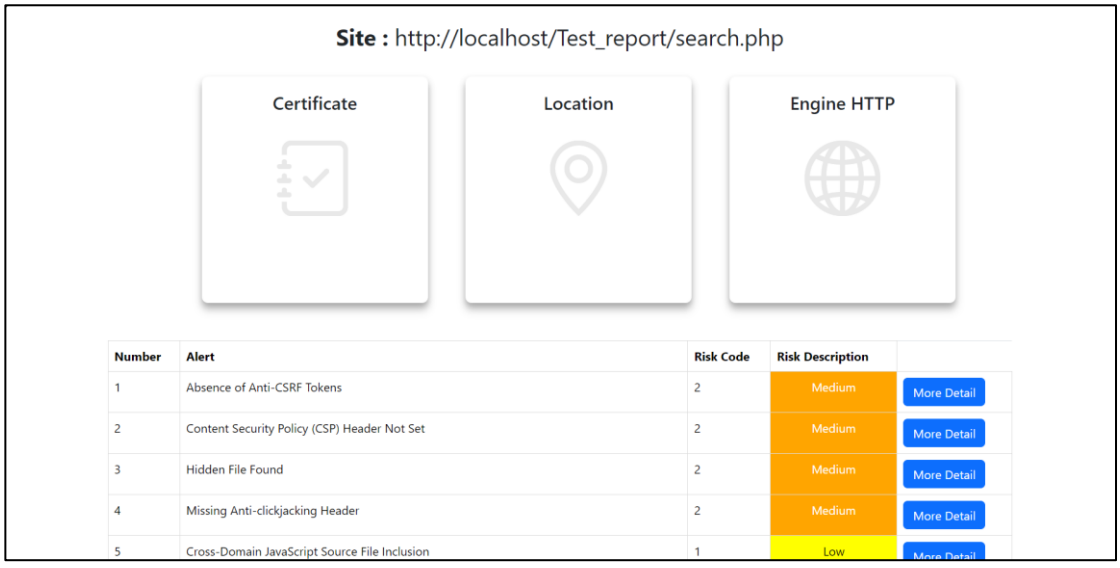

**ภาพที่ 9** หน้า Home page ของเว็บไซต์ (Scan)

3. รอตรวจสอบเว็บไซต์




**ภาพที่ 10** ตรวจสอบเว็บไซต์

4. แสดงผลการตรวจสอบ




**ภาพที่ 11** ผลการตรวจสอบเว็บไซต์

## เอกสารอ้างอิง

[1] **PTT ExpresSo. (11 กุมภาพันธ์ 2022). เจาะลึก Cyber Security** รักษาความปลอดภัยบนโลกออนไลน์. สืบค้น 12 สิงหาคม 2565, จาก https://blog.pttexpresso.com/cyber-security/

[2] **NT cyfence. (2017). ทำความรู้จักกับ NIST Cybersecurity Framework.** สืบค้นเมื่อ 12 สิงหาคม 2565,จาก https://www.cyfence.com/article/nist-cybersecurity-framework/

[3] **g-able. (2563). Security Framework และมาตรฐานความมั่นคงดิจิทัล.** สืบค้นเมื่อ 12 สิงหาคม 2565, จาก www.g-able.com/digital-review/digital-transformation

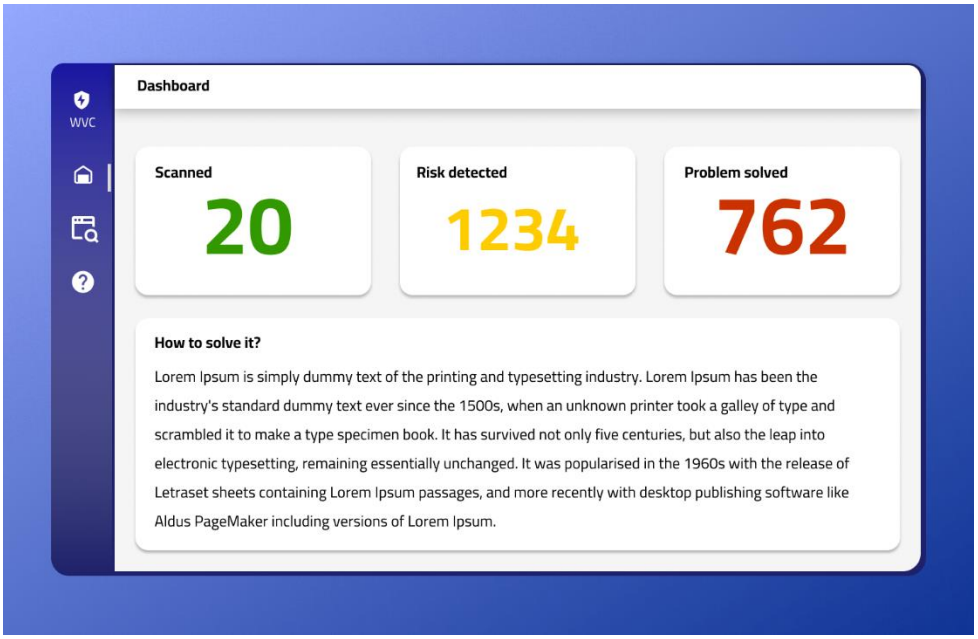
[4] **เรืออากาศตรีหญิง ณัชณภัทร ใจอดทน.** (2560) การประเมินค่าช่องโหว่ของเว็บไซต์และการป้องกัน กรณีศึกษา เว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ (วิทยานิพนธ์ ปริญญามหาบัณฑิต). วิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรมศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์

[5] **Wittawat Hemwannanurak .tangerine (2021).** OWASP Top 10 : Update 10 อันดับการโจมตี Web Application ปี 2021. สืบค้นเมื่อ 29 สิงหาคม 2565, จาก https://www.tangerine.co.th/security/owasp-top-10-threat-web-application-2021/

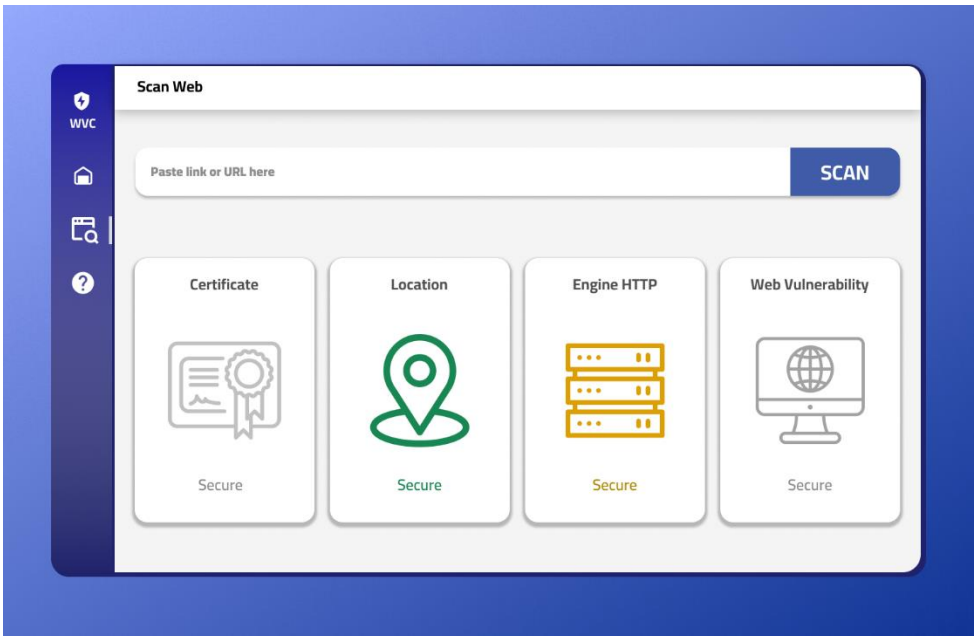
[6] **IEEE Computer Society. (2019). 10 Essential Steps To Improve Your Website Security.** สืบค้นเมื่อ 31 สิงหาคม 2565, จาก https://www.computer.org/publications/tech-news

[7] **กรุงเทพธุรกิจ. (2565). 'เอสเอ็มอี' ไทยสุดเสี่ยง!! ภัยคุกคามไซเบอร์โจมตีหนัก!!.** สืบค้นเมื่อวันที่ 10 ตุลาคม 2565, จาก https://www.bangkokbiznews.com/tech

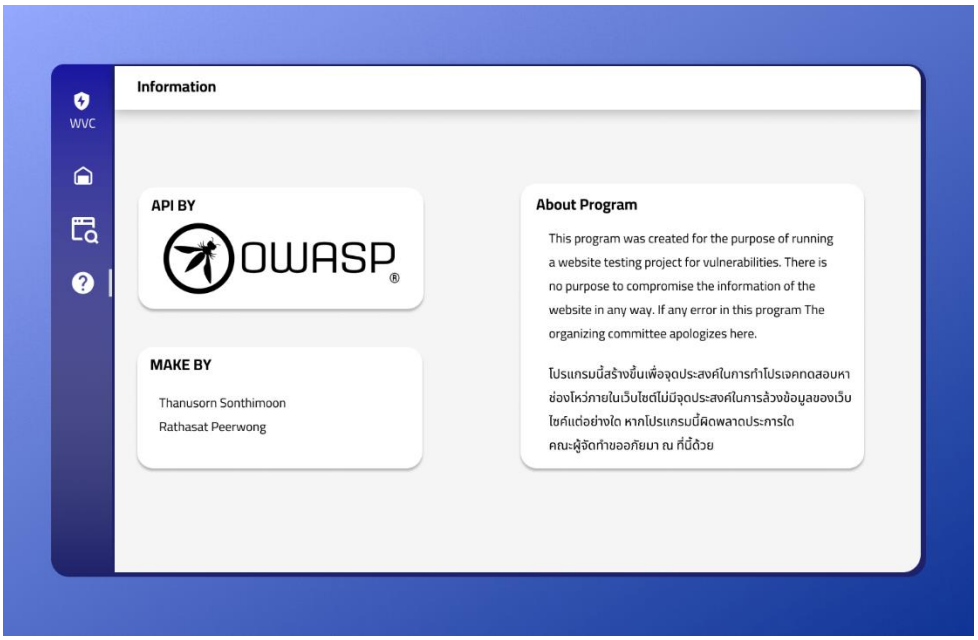
# ภาคผนวก




ภาพที่ 5 Prototype หน้า Home




ภาพที่ 6 Prototype หน้า Scan




ภาพที่ 7 Prototype หน้า About

# ประวัติผู้เขียน

ชื่อ-สกุล นายรัฐศาสตร์ เพียวงษ์

วัน เดือน ปีเกิด วันที่ 3 เดือน มิถุนายน พ.ศ.2544

ที่อยู่ปัจจุบัน ภัทราสิริ 140/533 หมู่ที่ 14 ตำบลในเมือง อำเภอเมือง จังหวัดขอนแก่น 40000

ประวัติการศึกษา -ระดับประถมศึกษา-มัธยมศึกษาตอนต้น โรงเรียนพิมพ์ใจวิทย์

-ระดับมัธยมต้นตอนปลาย โรงเรียนนครขอนแก่น

-ระดับปริญญาตรี มหาวิทยาลัยขอนแก่น

ชื่อ-สกุล นายตนุสรณ์ สนธิมูล

วัน เดือน ปีเกิด วันที่ 7 เดือน สิงหาคม พ.ศ.2544

ที่อยู่ปัจจุบัน หอนพรัตน์ (หอ 9 หลัง) 123 ม.16 ถ.มิตรภาพ ต.ในเมือง อ.เมือง จ. ขอนแก่น

ประวัติการศึกษา -ระดับประถมศึกษา โรงเรียนศิริมงคลศึกษา - โรงเรียนซู่เอ็ง

-ระดับมัธยมศึกษาตอนต้น -มัธยมต้นตอนปลาย โรงเรียนเมืองพลพิทยาคม

-ระดับปริญญาตรี มหาวิทยาลัยขอนแก่น

**ผู้ทำโครงงาน**

(ลงชื่อ).....ตนุสรณ์ สนธิมูล

(นายตนุสรณ์ สนธิมูล)

วันที่ 20 / ส.ค. / 2566

(ลงชื่อ).....รัฐศาสตร์ เพียวงษ์

(นายรัฐศาสตร์ เพียวงษ์)

วันที่ 20 / ส.ค. / 2566

การตรวจสอบจากอาจารย์ที่ปรึกษาโครงงาน

.....

.....

.....

.....

(ลงชื่อ) .....

( อ.ดร. เพชร อิ่มทองคำ )

วันที่

...../...../.....