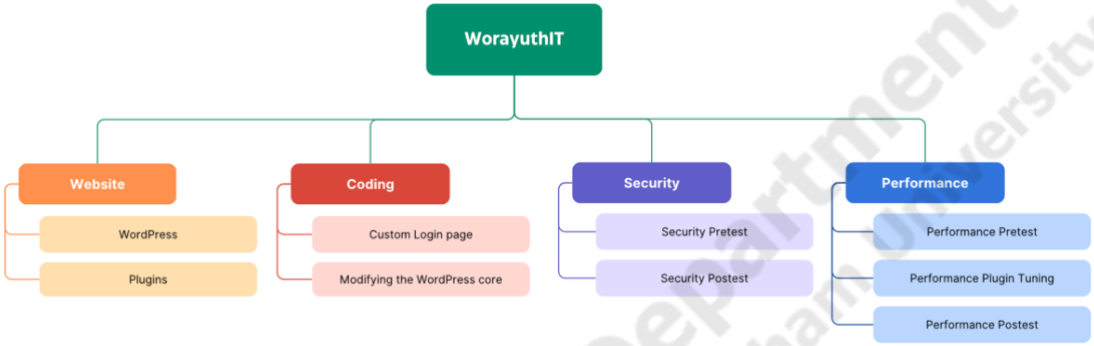
บทที่ 3
ขั้นตอนการดำเนินงาน

3.1 ภาพรวมการดำเนินงาน

กรอบการทำงานนี้จะแสดงการพัฒนาเว็บไซต์ WorayuthIT ซึ่งมีการทำงานหลักดังนี้



ภาพประกอบที่ 3.1 ภาพรวมการดำเนินงานของเว็บไซต์ WorayuthIT

3.2 WorayuthIT

3.2.1 WordPress

WordPress version ล่าสุดคือ WordPress 6.3.1 ซึ่งเป็นเวอร์ชั่นที่อัปเดตมาเพื่อแก้ไขบั๊กและปรับปรุงความเสถียร โดย WordPress เป็นแพลตฟอร์ม Open-source ซึ่งมีการอัปเดตเวอร์ชันใหม่ ๆ อยู่เป็นประจำเพื่อเพิ่มความสามารถ และปรับปรุงประสิทธิภาพให้ดียิ่งขึ้นในการใช้งานของผู้ใช้งาน

3.2.2 LearnPress

LearnPress เป็นปลั๊กอิน (plugin) สำหรับระบบจัดการเนื้อหาแบบ Learning Management System (LMS) ที่ถูกพัฒนาขึ้นสำหรับระบบการจัดการเรียนการสอนและการสร้างคอร์สออนไลน์บนแพลตฟอร์ม WordPress โดยส่วนใหญ่นิยมใช้สำหรับการสร้างและจัดการคอร์สออนไลน์ การเรียนรู้ออนไลน์ และการจัดการข้อมูลผู้เรียนหรือนักเรียนในสภาพแวดล้อมออนไลน์ เช่นการสอนออนไลน์ การให้ความรู้ผ่านเว็บไซต์ หรือการจัดอบรมออนไลน์

3.3 การใช้งาน plugins ของเว็บไซต์ WorayuthIT

ปลั๊กอินใน WordPress เป็นชุดคำสั่งที่เพิ่มความสามารถให้กับเว็บไซต์ได้โดยไม่ต้องแก้ไขโค้ดหลักของ WordPress โดยตรง ช่วยเพิ่มฟังก์ชันเสริมเช่น แบบฟอร์ม การจัดการเนื้อหา ความปลอดภัย และปรับแต่งส่วนต่าง ๆ ของเว็บไซต์ WordPress ได้ง่าย ๆ และมีนวัตกรรมเพิ่มเติมที่ช่วยให้ผู้ใช้

ปรับแต่งเว็บไซต์ได้ตามต้องการได้โดยไม่ยากลำบาก ซึ่งปลั๊กอินที่ใช้งานให้กับเว็บไซต์ WordPress worayuthit.com มีดังนี้

1) User Menus ช่วยปรับแต่งเมนูให้แสดงตามบทบาทผู้ใช้งาน ซึ่งเป็นประโยชน์สำหรับเว็บไซต์ที่มีสมาชิกหลายคนหรือประเภทของผู้ใช้ที่แตกต่างกัน

2) Ajax Search Lite ช่วยสำหรับการค้นหา โดยสามารถกำหนดหมวดหมู่ที่ต้องการแสดงได้

3) Elementor Pro Elementor เป็นเครื่องมือสร้างเพจ (page builder) ที่มีความสามารถช่วยให้สร้างหน้าเว็บที่สวยงามและน่าดึงดูดได้อย่างง่าย

4) LearnPress เป็นปลั๊กอินที่ช่วยในการสร้างระบบการเรียนการสอน (LMS) บน WordPress สามารถสร้างคอร์สเรียน และติดตามความก้าวหน้าของผู้เรียนได้

5) WP Rocket เป็นปลั๊กอินการปรับแต่งความเร็วเว็บไซต์ ที่ช่วยให้เว็บไซต์โหลดเร็วขึ้น มีการควบคุมแคช การบีบอัดไฟล์ CSS, JavaScript และรูปภาพ เพื่อเพิ่มประสิทธิภาพ

3.4 บทบาทผู้ใช้งาน

3.4.1 บทบาทผู้ใช้งานของ WordPress

ความสามารถของผู้ใช้งานในระบบการจัดการเนื้อหา (Content Management System: CMS) ที่ชื่อว่า WordPress ซึ่งเป็นเว็บแพลตฟอร์มที่ใช้กันอย่างกว้างขวางในการสร้างและบริหารจัดการเว็บไซต์ต่าง ๆ ไม่ว่าจะเป็นเว็บไซต์บุคคล เว็บไซต์ธุรกิจ เว็บไซต์ข่าว ร้านค้าออนไลน์ และอื่น ๆ นอกจากนี้ยังใช้กันในเว็บไซต์ขนาดใหญ่ระดับกลุ่มข่าว รัฐบาล องค์กรมากมายด้วย

ดังนั้นความสามารถและสิทธิ์การเข้าถึงข้อมูลและควบคุมในระบบของ WordPress มีความสำคัญอย่างยิ่งในการให้ความปลอดภัยและจัดการกับผู้ใช้งานอย่างเหมาะสมในแต่ละส่วนของเว็บไซต์ หน้าที่และความสามารถที่สำคัญใน WordPress ได้แก่

(1) Administrator (ผู้ดูแลระบบ) เป็นบทบาทที่สูงสุดในระบบ WordPress มีสิทธิ์ในการเข้าถึงและควบคุมทุกอย่างในเว็บไซต์ เช่น การสร้างและจัดการผู้ใช้งาน การติดตั้งและปรับแต่งปลั๊กอินและธีม การเขียนและแก้ไขโค้ด การจัดการเนื้อหาที่เผยแพร่ ฯลฯ

(2) Editor (บรรณาธิการ) ผู้ใช้บทบาทนี้มีสิทธิ์ในการเขียนและแก้ไขเนื้อหาบทความทั้งหมดในเว็บไซต์ รวมถึงการเผยแพร่บทความและหน้าเนื้อหาต่าง ๆ และมีความสามารถในการจัดการรายการบทความ

(3) Author (ผู้เขียน) ผู้ใช้บทบาทนี้สามารถเขียนและเผยแพร่บทความในเว็บไซต์ แต่ไม่มีสิทธิ์ในการเขียนหรือแก้ไขเนื้อหาของผู้อื่น

(4) Contributor (ผู้สนับสนุน) ผู้ใช้บทบาทนี้สามารถเขียนและส่งบทความเพื่อรอการตรวจสอบและการเผยแพร่จากผู้ดูแลระบบหรือบทบาทที่สูงกว่า

(5) Subscriber (สมาชิก) ผู้ใช้บทบาทนี้มีสิทธิ์เข้าถึงเนื้อหาของเว็บไซต์เท่านั้น และไม่สามารถเข้าถึงส่วนที่เกี่ยวข้องกับการจัดการหรือเขียนเนื้อหา

3.4.2 บทบาทผู้ใช้งานของเว็บไซต์ WorayuthIT

(1) Administrator (ผู้ดูแลระบบ) เป็นบทบาทที่สูงสุดในระบบ WordPress มีสิทธิ์ในการเข้าถึงและควบคุมทุกอย่างในเว็บไซต์ เช่น การสร้างและจัดการผู้ใช้งาน การติดตั้งและปรับแต่งปลั๊กอินและธีม การเขียนและแก้ไขโค้ด การจัดการเนื้อหาที่เผยแพร่ และ ฯลฯ

(2) Editor (บรรณาธิการ) ผู้ใช้บทบาทนี้มีสิทธิ์ในการเขียนและแก้ไขเนื้อหาบทความทั้งหมดในเว็บไซต์ รวมถึงการเผยแพร่บทความและหน้าเนื้อหาต่าง ๆ และมีความสามารถในการจัดการรายการบทความ

(3) Author (ผู้เขียน) ผู้ใช้บทบาทนี้สามารถเขียนและเผยแพร่บทความในเว็บไซต์ แต่ไม่มีสิทธิ์ในการเขียนหรือแก้ไขเนื้อหาของผู้อื่น

(4) Contributor (ผู้สนับสนุน) ผู้ใช้บทบาทนี้สามารถเขียนและส่งบทความเพื่อรอการตรวจสอบและการเผยแพร่จากผู้ดูแลระบบหรือบรรณาธิการ

(5) Tutor Instructor (ผู้สอน) บทบาทของผู้สอนในระบบการจัดการเรียนการสอนใน WordPress ซึ่งมีความสำคัญในการสร้างและจัดการหลักสูตรการเรียนการสอน

(6) Subscriber (สมาชิก) ผู้ใช้บทบาทนี้มีสิทธิ์เข้าถึงเนื้อหาของเว็บไซต์เท่านั้น และไม่สามารถเข้าถึงส่วนที่เกี่ยวข้องกับการจัดการหรือเขียนเนื้อหา

(7) Visitor (ผู้เยี่ยมชม) เป็นผู้ที่เข้ามาใช้งานเว็บไซต์หรือเยี่ยมชมเว็บไซต์ ซึ่งไม่ได้เข้าสู่ระบบหรือเป็นบุคคลที่ไม่ได้ลงทะเบียนเป็นสมาชิกหรือมีบทบาทในระบบเว็บไซต์

3.4.3 การมอบบทบาทผู้ใช้งานของเว็บไซต์ WorayuthIT

การให้บริการการแต่งตั้งหรือกำหนดบทบาทให้กับผู้ใช้งานเว็บไซต์ WorayuthIT นั้น ผู้ดูแลระบบจะตรวจสอบข้อมูลการขอบทบาทก่อนที่จะมอบบทบาทนั้น ๆ ให้กับผู้ใช้งาน

3.4.4 การติดต่อเพื่อรับบทบาทผู้ใช้งานของเว็บไซต์ WorayuthIT

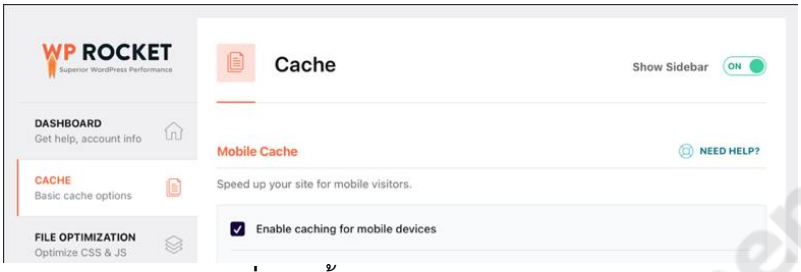
เพื่อรับบทบาทที่ผู้ใช้ต้องการ ผู้ใช้สามารถติดต่อส่วนตัวหรือ Inbox เพื่อขอบทบาทที่ต้องการได้ โดยสามารถติดต่อได้ที่ช่องทางต่อไปนี้

(1) Contact box บนเว็บไซต์

(2) Email: worayuthit at gmail.com

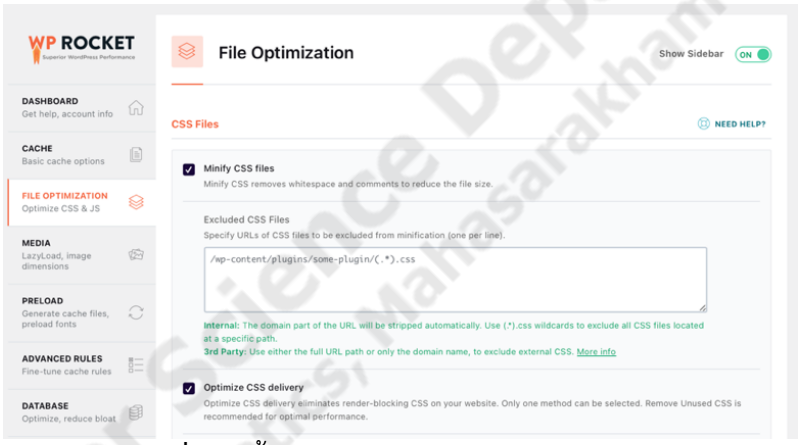
3.5 เพิ่มประสิทธิภาพ (Performance Optimization)

3.5.1 การใช้งาน WP Rocket



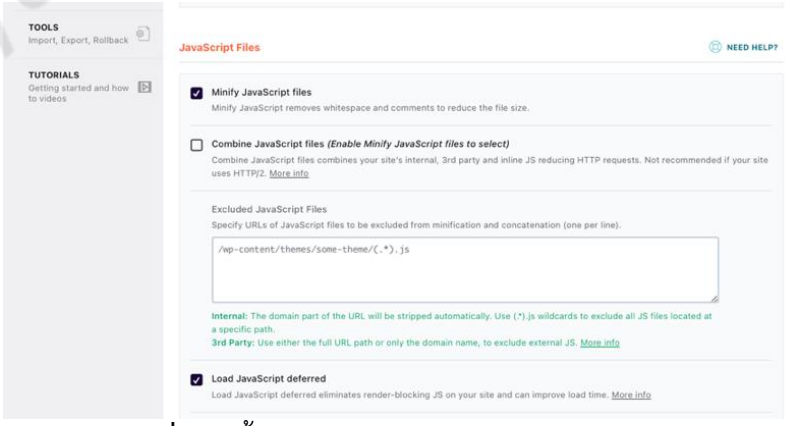
ภาพประกอบที่ 3.2 ตั้งค่า WP Rocket ส่วนของ Cache

Cache เปิดใช้ Enable caching for mobile devices ทำการแคชหน้าเว็บเฉพาะสำหรับผู้ใช้มือถือ เพื่อปรับปรุงประสิทธิภาพในการโหลดหน้าเว็บบนอุปกรณ์มือถือ



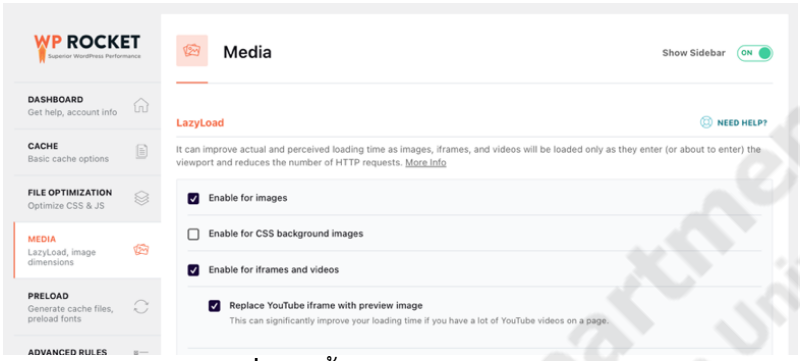
ภาพประกอบที่ 3.3 ตั้งค่า WP Rocket ส่วนของ File Optimization

File Optimization เปิดใช้ Minify CSS files เพื่อช่วยลดขนาดของไฟล์ CSS โดยลบช่องว่าง และอักขระที่ไม่จำเป็น ซึ่งช่วยให้ไฟล์ CSS โหลดเร็วขึ้น และ Optimize CSS delivery ช่วยในการปรับปรุงวิธีการส่งส่วน CSS เพื่อปรับปรุงประสิทธิภาพในการโหลดหน้าเว็บ



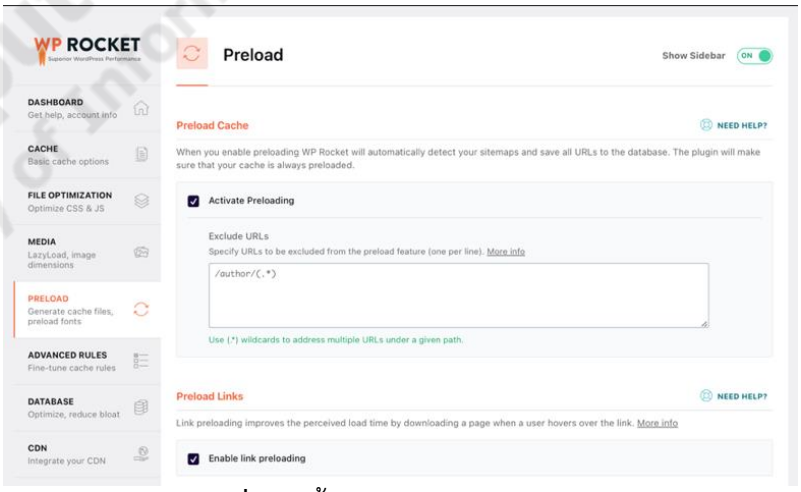
ภาพประกอบที่ 3.4 ตั้งค่า WP Rocket ส่วนของ File Optimization 2

Minify JavaScript files ช่วยลดขนาดของไฟล์ JavaScript โดยการลบช่องว่างตัวอักษรและอักขระที่ไม่จำเป็น ซึ่งช่วยลดขนาดของไฟล์ JavaScript และช่วยในการโหลดหน้าเว็บเร็วขึ้น เนื่องจากไฟล์มีขนาดเล็กขึ้นและ Load JavaScript Deffered ทำการโหลดไฟล์ JavaScript ในภายหลังหลังจากที่หน้าเว็บได้โหลดเสร็จ ซึ่งช่วยให้หน้าเว็บโหลดได้เร็วขึ้น



ภาพประกอบที่ 3.5 ตั้งค่า WP Rocket ส่วนของ Media

Media เปิดใช้ Enable for images แคช (cache) รูปภาพไว้ในหน่วยความจำของผู้เข้าชม และเว็บไซต์จะไม่ต้องโหลดรูปภาพซ้ำทุกครั้งที่ผู้เข้าชมกลับมาที่หน้าเว็บ ช่วยลดเวลาโหลดและปรับปรุงประสิทธิภาพ Enable for iframes and videos เว็บไซต์จะเก็บไว้ว่าหน้าเว็บนั้นมี Iframes หรือวิดีโอ และเมื่อผู้เข้าชมกลับมาที่หน้าเว็บนั้น ๆ ในครั้งถัดไป การแสดง Iframes หรือวิดีโอนั้นจะมีประสิทธิภาพการโหลดที่ดีขึ้น เพราะเว็บไซต์จะโหลดข้อมูลเหล่านี้จากแคช (cache) ที่ได้เตรียมไว้ล่วงหน้า และ Replace Youtube iframe with preview image แทนที่โค้ด Iframe ของวิดีโอจาก YouTube ด้วยรูปภาพตัวอย่างขณะที่หน้าเว็บกำลังโหลด ช่วยในการลดการโหลดทรัพยากรและเพิ่มประสิทธิภาพในการโหลดหน้าเว็บ



ภาพประกอบที่ 3.6 ตั้งค่า WP Rocket ส่วนของ Preload

Preload เปิดใช้ Activate Preloading ช่วยในการเตรียมโหลดทรัพยากรหลาย ๆ อย่างล่วงหน้า เช่น CSS, JavaScript และไฟล์รูปภาพ เพื่อปรับปรุงประสิทธิภาพในการโหลดหน้าเว็บ และ

Enable link preloading เตรียมโหลดลิงก์หลาย ๆ ตัวไปยังหน้าเว็บที่ผู้ใช้มีน่าจะคลิกล่วงหน้า เพื่อปรับปรุงประสิทธิภาพในการโหลดหน้าถัดไป

3.5.2 เครื่องมือวัดประสิทธิภาพเว็บไซต์

เพื่อประเมินประสิทธิภาพของเว็บไซต์ worayuthit.com มีการใช้เครื่องมือวัดประสิทธิภาพเว็บไซต์สองประเภทหลัก ได้แก่ Google PageSpeed Insights และ GTMetrix ซึ่งเป็นเครื่องมือที่มีชื่อเสียงและนิยมใช้กันอย่างแพร่หลายในวงการพัฒนาเว็บไซต์ โดยมีรายละเอียดของเครื่องมือวัดประสิทธิภาพเว็บไซต์ทั้งสองประเภทดังนี้

(1) Google PageSpeed Insights

Google PageSpeed เป็นบริการฟรีจาก Google ที่ให้คำแนะนำและวิเคราะห์เว็บไซต์เพื่อปรับปรุงประสิทธิภาพในการโหลดหน้าเว็บและประสบการณ์ผู้ใช้ของเว็บไซต์นั้น ๆ บริการนี้มีเป้าหมายเพื่อช่วยให้เว็บไซต์โหลดได้เร็วขึ้นและทำงานได้ดีในทุกอุปกรณ์และเบราว์เซอร์ที่ผู้ใช้ใช้งาน

ภาพประกอบที่ 3.7 Google PageSpeed Insights logo

โดยคำแนะนำนี้อาจรวมถึงการลดขนาดของไฟล์ภาพ การลดการร้องขอที่เว็บไซต์ต้องทำไปยังเซิร์ฟเวอร์ และการปรับปรุงการโหลดข้อมูลแบบเป็นลำดับเวลา (rendering) ของเว็บไซต์ เป้าหมายของ Google PageSpeed คือการทำให้เว็บไซต์ทั่วไปโหลดได้เร็วขึ้น และมีประสิทธิภาพในทุก ๆ สถานการณ์การใช้งานบนอุปกรณ์ต่าง ๆ ที่ผู้ใช้ใช้งานอยู่

(2) GTMetrix

GTmetrix เป็นเครื่องมือที่มีมาตรฐานสูงในการวัดและประเมินประสิทธิภาพของเว็บไซต์ โดยให้ข้อมูลที่ถูกต้องและเชื่อถือได้เกี่ยวกับความเร็วและประสิทธิภาพในการโหลดหน้าเว็บของเว็บไซต์นั้น ๆ GTmetrix ช่วยให้เจ้าของเว็บไซต์และนักพัฒนาเว็บได้ข้อมูลที่ทันสมัยและแม่นยำเพื่อทำการปรับปรุงเว็บไซต์ให้มีประสิทธิภาพในการโหลดที่ดีที่สุด

ภาพประกอบที่ 3.8 GTMetrix logo

รายงานที่ GTmetrix ให้มีข้อมูลจาก Google PageSpeed Insights Lighthouse และ YSlow ทำให้เป็นเครื่องมือที่ครอบคลุมและเป็นประโยชน์ต่อการพัฒนาเว็บไซต์ ด้วยคะแนนและ

เกรดที่ได้จาก Gtmetrix นักพัฒนาสามารถปรับปรุงประสิทธิภาพของเว็บไซต์ให้มีประสิทธิภาพสูงสุดได้อย่างมีประสิทธิภาพและมีประสิทธิภาพในทุก ๆ ด้านของการโหลดหน้าเว็บ นอกจากนี้ยังมีฟีเจอร์ที่ช่วยในการตรวจสอบประสิทธิภาพของเว็บไซต์บนทั้งอุปกรณ์มือถือและคอมพิวเตอร์ ทำให้เป็นเครื่องมือที่มีประสิทธิภาพและได้รับการยอมรับในการปรับปรุงประสิทธิภาพของเว็บไซต์ทุก ๆ ครั้งที่ใช้งาน

3.5.3 การประเมินประสิทธิภาพความเร็วเว็บไซต์

การประเมินประสิทธิภาพของความเร็วของเว็บไซต์ มีหลายพารามิเตอร์ที่ใช้เพื่อวัดประสิทธิภาพและประสิทธิผลของเว็บไซต์ในการโหลดและการทำงาน ซึ่งพิจารณาพารามิเตอร์ดังนี้

(1) First Contentful Paint (FCP)

วัดเวลาที่เนื้อหาแรก ๆ ของหน้าเว็บปรากฏบนหน้าจอเว็บของผู้ใช้ครั้งแรก ช่วยในการวัดความรวดเร็วของการโหลดหน้าเว็บ ค่า FCP น้อยแสดงถึงประสบการณ์การใช้งานที่ดี

ตารางที่ 3.1 ตรวจสอบประสิทธิภาพ FCP

FCP Time (in seconds)	Color-coding
0–1.8	Green (fast)
1.8–3	Orange (moderate)
Over 3	Red (slow)

(2) Largest Contentful Paint (LCP)

วัดเวลาที่เนื้อหาที่ใหญ่ที่สุดบนหน้าเว็บ (เช่น รูปภาพหรือข้อความ) ปรากฏในวิวพอร์ต ช่วยในการระบุเวลาที่เนื้อหาสำคัญ ๆ โหลดและแสดง ค่า LCP น้อยแสดงถึงประสบการณ์การใช้งานที่ดี

ตารางที่ 3.2 ตรวจสอบประสิทธิภาพ LCP

LCP Time (in seconds)	Color-coding
0–2.5	Green (fast)
2.5–4	Orange (moderate)
Over 4	Red (slow)

(3) Total Blocking Time (TBT)

ระยะเวลาทั้งหมดที่ผู้ใช้ไม่สามารถโต้ตอบกับหน้าเว็บได้เนื่องจากการบล็อกการกระทำ (การคลิกหรือปุ่ม) ช่วยในการวัดประสิทธิภาพของการตอบสนองของเว็บไซต์ ค่า TBT ต่ำแสดงถึงประสบการณ์การใช้งานที่ดี

ตารางที่ 3.3 ตรวจสอบประสิทธิภาพ TBT

TBT Time (in milliseconds)	Color-coding
0–200	Green (fast)
200–600	Orange (moderate)
Over 600	Red (slow)

(4) Cumulative Layout Shift (CLS)

วัดการเลื่อนเลย์เอาต์ที่ไม่คาดคิดของเนื้อหา เช่น เมื่อปุ่มหรือรูปภาพเลื่อนขึ้นหรือลงโดยไม่ได้ตั้งใจ ช่วยในการวัดความเสถียรในการแสดงผลของหน้าเว็บ ค่า CLS ต่ำแสดงถึงประสบการณ์การใช้งานที่ดี

ตารางที่ 3.4 ตรวจสอบประสิทธิภาพ CLS

CLS Time (in seconds)	Color-coding
0–0.1	Green (fast)
0.1–0.25	Orange (moderate)
Over 0.25	Red (slow)

(5) Time to Interactive (TTI)

วัดเวลาที่ผู้ใช้สามารถโต้ตอบกับเว็บไซต์ได้อย่างสมบูรณ์ แม้ว่าเว็บไซต์ยังคงโหลดเนื้อหาต่อไป ช่วยในการวัดความสามารถในการโต้ตอบของเว็บไซต์ ค่า TTI ต่ำแสดงถึงประสบการณ์การใช้งานที่ดี

ตารางที่ 3.5 ตรวจสอบประสิทธิภาพ TTI

TTI Time (in seconds)	Color-coding
0–3.8	Green (fast)
3.9–7.3	Orange (moderate)
Over 7.3	Red (slow)

(6) Speed Index

วัดเวลาที่เว็บไซต์ใช้ในการแสดงผลต่าง ๆ บนหน้าจอของผู้ใช้หลังจากการโหลดหน้าเว็บเสร็จสมบูรณ์ ช่วยในการวัดความรวดเร็วของการแสดงผลเว็บไซต์ ค่า Speed Index ต่ำแสดงถึงประสบการณ์การใช้งานที่ดี

ตารางที่ 3.6 ตรวจสอบประสิทธิภาพ Speed Index

Speed Index (in seconds)	Color-coding
0–3.4	Green (fast)
3.4–5.8	Orange (moderate)
Over 5.8	Red (slow)

3.5.4 Confidence Interval

ช่วงความเชื่อมั่น (confidence interval) คือ ช่วงหรือช่วงค่าที่คาดหวังว่าจะมีค่าจริงอยู่ภายในนั้นกับความน่าจะเป็น (probability) ที่กำหนดไว้ โดยใช้ข้อมูลตัวอย่าง (sample data) จากการสำรวจหรือการทดลองเพื่อประมาณค่าของพารามิเตอร์หรือค่าความสัมพันธ์ทางสถิติต่าง ๆ ซึ่งจะช่วยให้สามารถประเมินค่าจริงของพารามิเตอร์หรือความสัมพันธ์นั้น ๆ ได้อย่างถูกต้องและมั่นใจได้มากขึ้น ประกอบด้วยค่าดังนี้

(1) ค่าเฉลี่ยเลขคณิต (mean) หรือ ค่าเฉลี่ย

เขียนแทนด้วยสัญลักษณ์ $\overline{x}$ คือ การหาผลบวกของจำนวนทั้งหมดในชุดข้อมูล แล้วหารด้วยจำนวนของตัวเลขทั้งหมดในชุดข้อมูล นั่นคือหาค่าเฉลี่ยของข้อมูลนั้น ๆ เพื่อแสดงให้เห็นถึงค่ากลางของชุดข้อมูล ซึ่งสามารถนำมาใช้เพื่อวัดค่าเฉลี่ยการกระจายของข้อมูลได้ โดยการหาค่าเฉลี่ยได้จากสูตร

$$m = \frac{\text{sum of the terms}}{\text{number of terms}}$$

ภาพประกอบที่ 3.9 สูตรหาค่าเฉลี่ย

(2) ส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation)

ส่วนเบี่ยงเบนมาตรฐาน คือ ค่าเฉลี่ยของความห่างของแต่ละตัวอย่าง (sample) จากค่าเฉลี่ยของตัวอย่าง ซึ่งเป็นตัวชี้วัดความแปรปรวนของข้อมูลในตัวอย่าง ซึ่งคำนวณจากค่าเฉลี่ยของตัวอย่างและค่าต่าง ๆ ของตัวอย่างจากค่าเฉลี่ยนั้น ๆ โดยใช้สูตรคำนวณ

$$s = \sqrt{\frac{\sum_{i=1}^{N}(x_i - \overline{x})^2}{N-1}}$$

ภาพประกอบที่ 3.10 สูตรหาค่าเฉลี่ยส่วนเบี่ยงเบนมาตรฐาน

ส่วนเบี่ยงเบนมาตรฐานจะบอกถึงการกระจายของข้อมูลในตัวอย่างว่ามีค่าต่างกันเท่าไหร่ ค่ามากจะหมายถึงการกระจายของข้อมูลในตัวอย่างมีค่ามาก และค่าน้อยจะหมายถึงการกระจายของข้อมูลในตัวอย่างมีค่าน้อย

(3) ขนาดตัวอย่าง (sample size)

ขนาดตัวอย่าง คือ ชุดข้อมูลที่นำมาวิเคราะห์ในช่วงความเชื่อมั่น ซึ่งมักใช้ในการหาค่าความเชื่อมั่นของค่าเฉลี่ยหรือค่าที่คาดหวังของตัวแปรทางสถิติ

(4) Alpha value

Alpha value คือ ค่าที่ใช้กำหนดระดับความเชื่อมั่น (confidence level) ในการสร้าง confidence interval ซึ่งบ่งบอกถึงความน่าจะเป็นที่ confidence interval ที่ได้จะครอบคลุมค่าพารามิเตอร์ที่ต้องการในช่วงที่กำหนดไว้

(5) ระดับความเชื่อมั่น (confidence level)

ระดับความเชื่อมั่นที่กำหนดไว้ เช่น alpha เท่ากับ 0.05 แปลว่า Confidence coefficient เท่ากับ (1 - 0.05) = 0.95 หรือ 95% ดังนั้น Confidence Interval ที่ได้จะมีระดับความเชื่อมั่นอยู่ที่ 95% หรือในกรณีที่กำหนด alpha = 0.01 ค่า Confidence coefficient จะเท่ากับ 0.99 หรือ 99% ซึ่งหมายความว่ามีระดับความเชื่อมั่นในการวัดค่าพารามิเตอร์นั้น ๆ ในช่วง Confidence Interval ที่คำนวณได้ ด้วยระดับความเชื่อมั่นที่กำหนดไว้

3.5.5 การกำหนดปัจจัยการทดสอบเพื่อวัดประสิทธิภาพเว็บไซต์ worayuthit.com

ก่อนทำการทดสอบประสิทธิภาพของเว็บไซต์ เงื่อนไขการทดสอบควรถูกกำหนดให้เหมาะสม เช่น สถานที่ที่จะทำการทดสอบ เบราว์เซอร์ที่ใช้ การเชื่อมต่ออินเทอร์เน็ต และสภาพแวดล้อมของเครื่องคอมพิวเตอร์ ซึ่งทั้งหมดนี้ต้องเป็นไปตามเงื่อนไขที่เหมาะสม เพื่อให้ผลการทดสอบสามารถสะท้อนความเป็นจริงของประสิทธิภาพของเว็บไซต์อย่างถูกต้องและน่าเชื่อถือมากที่สุด

(1) การตั้งค่า GTMetrix ในการทดสอบ worayuthit.com

- Test Location: Hong Kong, China เนื่องจากมีข้อจำกัดของ GTmetrix ดังนั้น Location ที่เราสามารถเลือกได้ที่ใกล้ที่สุด" คือ Hong Kong, China ถูกเลือกเนื่องจากเป็นตัวเลือกที่ใกล้เคียงที่สุดและมีการเสนอให้ใช้งานฟรี
- Browser: Real browser (Chrome) GTmetrix นั้นบราวเซอร์จริงทำให้การทดสอบเป็นไปอย่างเป็นจริงมากขึ้น และสามารถตรวจสอบปัญหาและปรับปรุงความเร็วของเว็บไซต์ได้อย่างเที่ยงตรงกับประสิทธิภาพที่ผู้ใช้จริงต้องการ
- Connection: Unthrottled Connection (default) การใช้การเชื่อมต่อที่ไม่มีการจำกัดความเร็ว (Unthrottled) ในการทดสอบประสิทธิภาพของเว็บไซต์หรือแอปพลิเคชัน โดยค่านี้เป็นค่าเริ่มต้น การใช้ "Unthrottled Connection" จะช่วยในการตรวจสอบความเร็วและ

ประสิทธิภาพของเว็บไซต์ในสภาพที่มีความเร็วสูงที่สุดที่เป็นไปได้

(2) การตั้งค่า Google PageSpeed Insights: ในการทดสอบ worayuthit.com

- Test Location: Asia (default) ไม่สามารถกำหนดเองได้ และ Asia เป็นตัวเลือกที่ถูกกำหนดเป็นค่าเริ่มต้น (default) ซึ่งหมายความว่าเครื่องมือนี้จะทดสอบเว็บไซต์โดยใช้เซิร์ฟเวอร์หรือเครื่องทดสอบที่ตั้งอยู่ในภูมิภาคเอเชีย
- Browser: Using HeadlessChromium ใช้บราวเซอร์จำลอง โหมดการทำงานของเบราวเซอร์ที่ไม่แสดงหน้าต่างกราฟิก หรือส่วนต่าง ๆ ของเบราวเซอร์ออกมา แต่ยังคงสามารถทำงานเหมือนเบราวเซอร์ปกติได้ แต่การใช้แบบไม่แสดงกราฟิกทำให้มีความเร็วในการทดสอบและมีประสิทธิภาพมากขึ้น เนื่องจากไม่ต้องใช้งานกราฟิกอื่น ๆ
- Connection: Custom throttling 40 ms, 10 mb/s (default) Google PageSpeed Insights นั้นทำการกำหนดการเชื่อมต่อมาให้ ซึ่งไม่สามารถกำหนดเองได้

3.5.6 สภาพแวดล้อมในการทดสอบ

การทำการทดสอบประสิทธิภาพของเว็บไซต์เป็นขั้นตอนที่สำคัญในการตรวจสอบความสมบูรณ์และความเสถียรของเว็บไซต์ก่อนที่จะเปิดให้บริการแก่ผู้ใช้งานจริง การตรวจสอบนี้มีความสำคัญที่สูงเพื่อให้แน่ใจว่าผู้ใช้งานจะได้รับประสบการณ์ที่ดีและมีประสิทธิภาพเมื่อใช้งานเว็บไซต์ โดยมีรายละเอียดของสภาพแวดล้อมในการทดสอบดังนี้

(1) เครื่องมือที่ใช้ในการทดสอบ

สำหรับการทดสอบประสิทธิภาพของเว็บไซต์ WorayuthIT.com ในโปรเจกต์นี้เราใช้เครื่องมือที่มีสเปคที่เหมาะสมเพื่อทำการทดสอบดังนี้

- AMD Ryzen 5 5600H (6 Cores/12 Threads, 3.3GHz up to 4.2 GHz)
- RAM 16 GB DDR4 Bus 3200MHz
- NVIDIA GeForce RTX 3060 Max-P (6GB GDDR6)
- 64-bit Operating System
- Windows 11 Home

(2) ความเร็วอินเตอร์เน็ต

สำหรับความเร็วของการเชื่อมต่ออินเทอร์เน็ตที่ใช้ในการทดสอบประสิทธิภาพของเว็บไซต์ worayuthit.com มีรายละเอียดดังนี้

- ผู้ให้บริการอินเทอร์เน็ต (ISP) : True
- ความเร็วในการดาวน์โหลด (Download Speed) : 342.4
- ความเร็วในการอัปโหลด (Upload Speed) : 221.1
- ความล่าช้า (Latency : 5.2

3.5.7 ตัวอย่างตารางเก็บค่าสำหรับวัดประสิทธิภาพ

ตารางที่ 3.7 ตัวอย่างผลการวัดประสิทธิภาพเว็บไซต์ udemy.com โดย Google PSI

ลำดับ	Performance	FCP	LCP	TBT	CLS	Speed Index
1	90	0.4	0.8	190	0.06	1.8
2	76	0.4	2.3	210	0.06	2.3
3	82	0.4	2	150	0.06	2.2
4	80	0.4	0.8	360	0.06	1.9
5	94	0.4	0.8	120	0.06	1.8
6	84	0.4	1.1	260	0.06	1.8
7	89	0.4	1.1	180	0.06	1.8
8	89	0.4	1.1	180	0.06	1.8
9	82	0.4	0.8	310	0.06	2
10	89	0.4	0.8	160	0.06	2.5
11	89	0.4	0.8	160	0.06	2.5
12	93	0.4	0.8	140	0.06	1.8
13	76	0.3	0.9	450	0.06	1.9
14	78	0.4	0.8	340	0.11	1.9
15	89	0.3	1.1	160	0.06	2.2
16	86	0.4	0.8	260	0.06	1.9
17	85	0.4	0.8	260	0.06	1.9
18	88	0.4	0.8	230	0.06	1.8
19	87	0.4	0.8	250	0.06	1.8
20	87	0.4	0.8	250	0.06	1.8
21	83	0.4	1.1	280	0.06	1.8
22	91	0.4	0.8	140	0.06	2.4
23	85	0.4	1.1	250	0.06	1.9
24	81	0.4	1.7	210	0.06	2.1
25	90	0.4	0.8	160	0.06	2.2
26	94	0.4	0.8	140	0.06	1.7
27	94	0.4	0.8	140	0.06	1.7
28	67	0.3	0.9	710	0.06	2.6
29	75	0.3	1.2	430	0.06	1.9
30	90	0.4	0.8	200	0.06	1.8

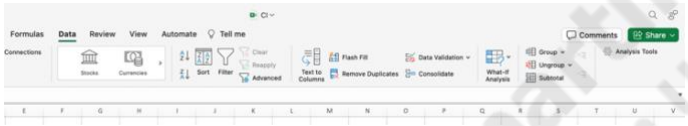
ตารางที่ 3.8 ตัวอย่างผลการวัดประสิทธิภาพเว็บไซต์ udemy.com โดย GTMetrix

ลำดับ	Performance	FCP	LCP	TBT	CLS	TTI	Speed Index
1	80	1.2	1.3	282	0.06	2.1	1.5
2	73	1.1	1.8	312	0.06	2.5	1.9
3	73	1.1	1.8	312	0.06	2.5	1.9
4	75	1.1	1.3	325	0.06	4.6	1.5
5	80	1.1	1.2	187	0.06	7	1.5
6	63	1.3	1.5	376	0.06	6.6	1.8
7	74	1.1	1.7	316	0.06	2.2	1.9
8	45	2.5	3.1	298	0.06	8.5	3.2
9	68	1.2	1.8	269	0.06	7.2	1.9
10	72	1.1	1.3	308	0.06	6.4	1.6
11	68	1.2	1.7	271	0.06	7.1	1.8
12	86	1.2	1.3	195	0.06	2	1.5
13	85	1.1	1.2	229	0.06	1.9	1.4
14	82	1.3	1.4	228	0.06	2.1	1.6
15	81	1.1	1.7	226	0.06	2	1.8
16	62	1.2	1.4	462	0.06	8.3	1.7
17	62	1.1	1.8	362	0.06	8.1	1.9
18	65	1.2	1.4	445	0.06	4.8	1.7
19	83	1.1	1.6	208	0.06	2.2	1.6
20	82	1.1	1.2	282	0.06	2	1.4
21	74	1.1	1.3	270	0.06	7.2	1.5
22	76	1.1	1.3	222	0.06	7	1.6
23	81	1.2	1.7	197	0.06	2.3	1.7
24	80	1.1	1.2	189	0.06	6.1	1.5
25	73	1.2	1.3	288	0.06	6.2	1.6
26	79	1.2	1.3	293	0.06	2.3	1.6
27	68	1.6	1.7	259	0.06	5	2.1
28	67	1.1	1.8	458	0.06	2.2	1.8
29	77	1.1	1.3	324	0.06	2.5	1.6
30	76	1.1	1.2	243	0.06	6.9	1.5

3.5.8 คำนวณหาค่าความเชื่อมั่นด้วย Excel

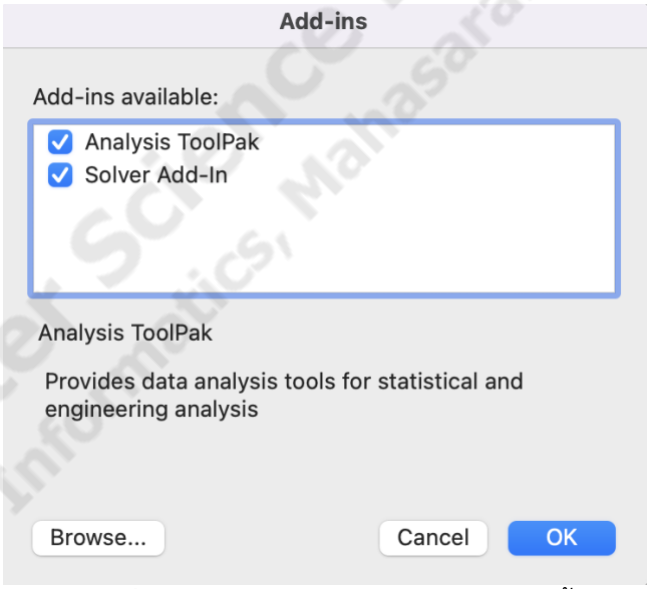
การคำนวณค่า Confidence Interval ด้วย Microsoft Excel เป็นกระบวนการที่มีประโยชน์ในการวิเคราะห์และตัดสินใจเกี่ยวกับข้อมูลที่มีอยู่ การคำนวณ Confidence Interval ช่วยให้มั่นใจในค่าสถิติที่ได้จาก Sample และให้ความน่าเชื่อถือในผลลัพธ์ที่ได้รับจากการวิเคราะห์ข้อมูลที่มีอยู่ เมื่อคำนวณ Confidence Interval ด้วย Excel ค่าที่ได้นั้นเป็นมาตรฐานที่น่าเชื่อถือในการวิเคราะห์ข้อมูลต่อไป นอกจากนี้ การใช้ Excel เป็นเครื่องมือที่สะดวกและเข้าใจง่าย ทำให้ผู้ใช้สามารถนำไปใช้ในการวิเคราะห์ข้อมูลได้อย่างมีประสิทธิภาพและง่ายดาย โดยมีขั้นตอนการคำนวณดังนี้

(1) Data และ Analysis Tools



ภาพประกอบที่ 3.11 หาค่า Condidence Interval ขั้นตอนที่ 1

(2) เลือก Analysis ToolPak และ Solver Add-in และคลิก OK



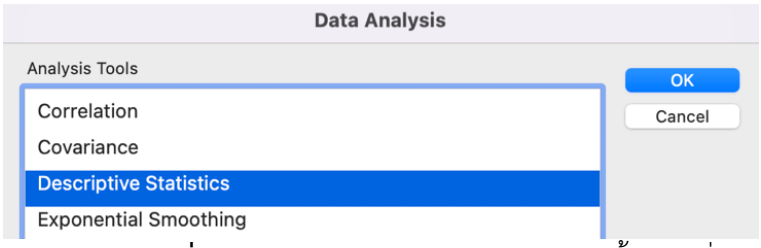
ภาพประกอบที่ 3.12 หาค่า Condidence Interval ขั้นตอนที่ 2

(3) เตรียมข้อมูลที่ต้องการหาค่าความเชื่อมั่น (Confidence Interval)

	A	B
1	90	
2	76	
3	82	
4	80	
5	94	
6	84	
7	89	
8	89	
9	82	
10	89	
11	89	
12	93	
13	76	
14	78	
15	89	
16	86	
17	85	
18	88	
19	87	
20	87	
21	83	
22	91	
23	85	
24	81	
25	90	
26	94	
27	94	
28	67	
29	75	
30	90	

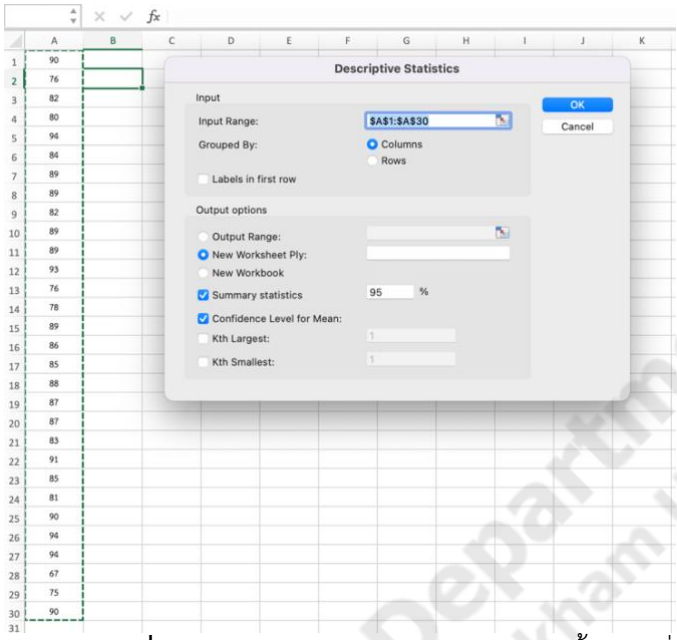
ภาพประกอบที่ 3.13 หาค่า Condidence Interval ขั้นตอนที่ 3

(4) Data และ Data Analysis และเลือก Descriptive Statistics และคลิก OK



ภาพประกอบที่ 3.14 หาค่า Condidence Interval ขั้นตอนที่ 5

(5) Input Range เลือกข้อมูลที่ต้องการคำนวณ และคลิก OK



ภาพประกอบที่ 3.15 หาค่า Condidence Interval ขั้นตอนที่ 6

summary	
Mean	85.43
Standard Error	1.18
Median	87.00
Mode	89.00
Standard Deviation	6.46
Sample Variance	41.70
Kurtosis	0.82
Skewness	-0.93
Range	27.00
Minimum	67.00
Maximum	94.00
Sum	2563.00
Count	30.00
Confidence Level(95.0%)	2.41

ภาพประกอบที่ 3.16 หาค่า Condidence Intercal ขั้นตอนที่ 7

(6) จากนั้นทำการคำนวณหาค่า Confidence Interval ค่าที่เป็นไปได้สูงสุดและค่าที่เป็นไปได้ต่ำสุดดังนี้

- Highest CI(95%) = Mean + Confidence Level(95.0%)
- Lowest CI(95%) = Mean - Confidence Level(95.0%)

3.5.9 ตัวอย่างสรุปผลการคำนวณค่าความเชื่อมั่น

ตารางที่ 3.9 ตัวอย่างผลการคำนวณค่าความเชื่อมั่น โดย Google PSI

รายการ	Performance	FCP	LCP	TBT	CLS	Speed Index
Mean	85.43	0.39	1.00	242.67	0.06	1.98
Standard Error	1.18	0.01	0.07	22.35	0.00	0.05
Confidence Level (95.0%)	2.41	0.01	0.14	45.71	0.00	0.10
Highest CI (95%)	87.84	0.40	1.14	288.38	0.06	2.08
Lowest CI (95%)	83.02	0.37	0.86	196.96	0.06	1.89

ตารางที่ 3.10 ตัวอย่างผลการคำนวณค่าความเชื่อมั่น โดย GTMetrix

รายการ	Performance	FCP	LCP	TBT	CLS	TTI	Speed Index
Mean	73.67	1.21	1.52	287.87	0.06	4.59	1.72
Standard Error	1.60	0.05	0.07	13.76	0.00	0.44	0.06
Confidence Level (95.0%)	3.26	0.10	0.14	28.14	0.00	0.91	0.12
Highest CI (95%)	76.93	1.31	1.66	316.01	0.06	5.50	1.84
Lowest CI (95%)	70.40	1.11	1.38	259.73	0.06	3.69	1.60

3.6 เพิ่มความมั่นคงปลอดภัย (Security Enhancement)

3.6.1 บริหารจัดการ Server/Web page เบื้องต้น

ในยุคของโลกดิจิทัลที่มีข้อมูลมากมายและการสื่อสารออนไลน์มีความสำคัญ การบริหารจัดการเซิร์ฟเวอร์และหน้าเว็บจึงเป็นสิ่งสำคัญที่ไม่ควรมองข้าม ขั้นตอนการบริหารจัดการ Server Web page เบื้องต้นมีดังนี้

(1) จด Domain name โดยผู้ให้บริการ hostatom เพื่อเป็นชื่อของเว็บไซต์ที่เรียกแทนการเรียกด้วยหมายเลข IP Address ซึ่งเป็นส่วนที่นำไปฝากไว้กับบริการเว็บโฮสติ้ง

(2) ออก SSL Certificate Let's Encrypt เพื่อให้ข้อมูลทั้งหมดที่ผู้เยี่ยมชมเว็บไซต์กรอกบนหน้าเว็บถูกเข้ารหัสเพื่อปกป้องข้อมูล

(3) ตั้งค่า Configuration https เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต ระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์

(4) ตั้งค่า HSTS configuration เพื่อให้เว็บเบราว์เซอร์ที่กำลังเข้ามาใช้บริการเว็บไซต์ต้องทำงานผ่านช่องทางเข้ารหัส HTTPS เท่านั้น

3.6.2 บูรณาการหน้าเข้าสู่ระบบ

(1) ปรับหน้าเข้าสู่ระบบฐานข้อมูลและส่วนประกอบอื่น ๆ ให้สามารถใช้ Captcha และ Salted Hash Password ร่วมกับ Mobile TOTP

(2) ทำการ hashed รหัสผ่านที่ส่งด้วย Salted Hash Password โดยใช้ Salt เป็นเลข TOTP (Time-based One-Time Password) ที่ generate จาก TOTP Mobile Application เช่น Google Authenticator, Authy

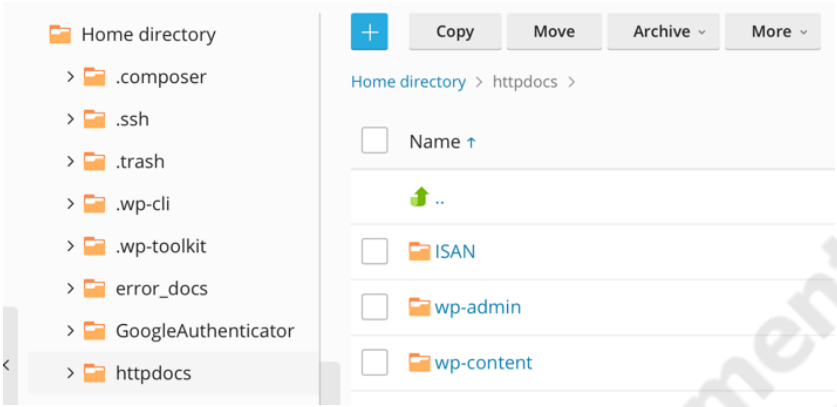
(3) สร้างหน้าสำหรับเปิดใช้งาน Salted Hash Password บน Mobile Application เพื่อ generate secret key

(4) หน้าเข้าสู่ระบบสามารถป้องกันการโจมตีโดยการฝัง key-logger client script แล้วดักจับ keystroke

3.7 ขั้นตอนการติดตั้งฐานข้อมูล

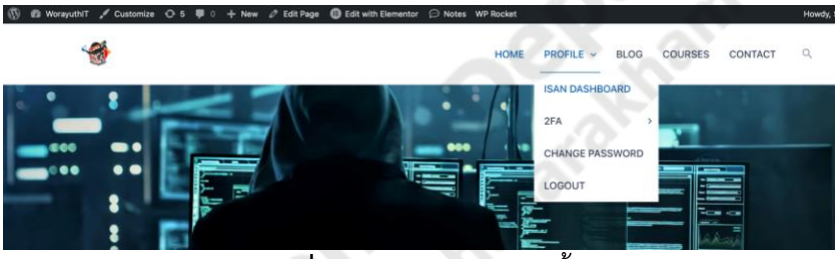
การติดตั้งฐานข้อมูลเป็นขั้นตอนสำคัญในการใช้งานหน้าต่าง ๆ ของ ISAN บนเว็บไซต์ เช่น หน้าสมัครสมาชิก หน้าเข้าสู่ระบบ หน้าใช้งาน TOTP 2FA และอื่น ๆ ที่เกี่ยวข้อง ดังนั้นเพื่อให้สามารถใช้งานได้จำเป็นต้องติดตั้งฐานข้อมูลเพื่อเก็บข้อมูลของผู้ใช้หรือข้อมูลอื่น ๆ ที่เป็นส่วนหนึ่งสำหรับใช้งานเพื่อให้สามารถทำงานได้ มีขั้นตอนการติดตั้งดังนี้

1) นำ folder ISAN เข้าไปในไฟล์ htdocs/httpdocs ของเว็บไซต์ที่ต้องการใช้งาน



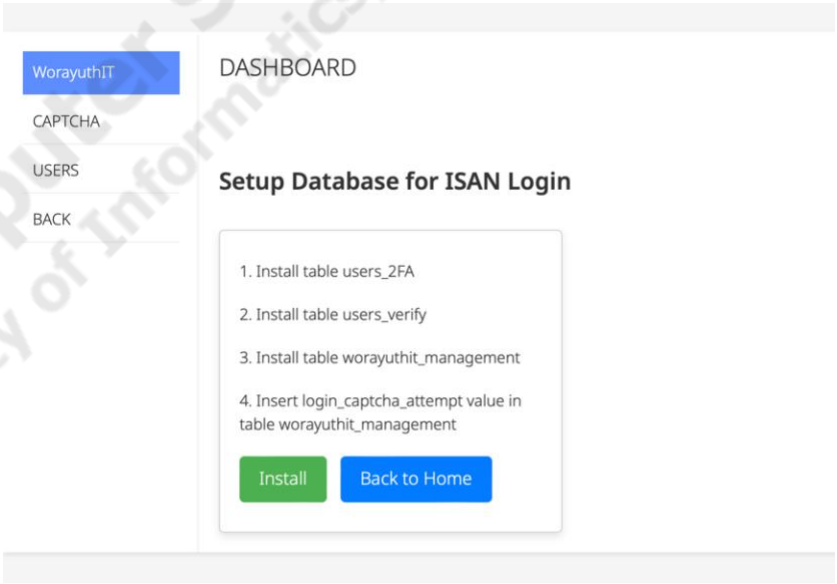
ภาพประกอบที่ 3.17 ตัวอย่างตำแหน่งไฟล์

2) เข้าสู่ระบบเว็บไซต์และเลือกเมนู ISAN DASHBOARD



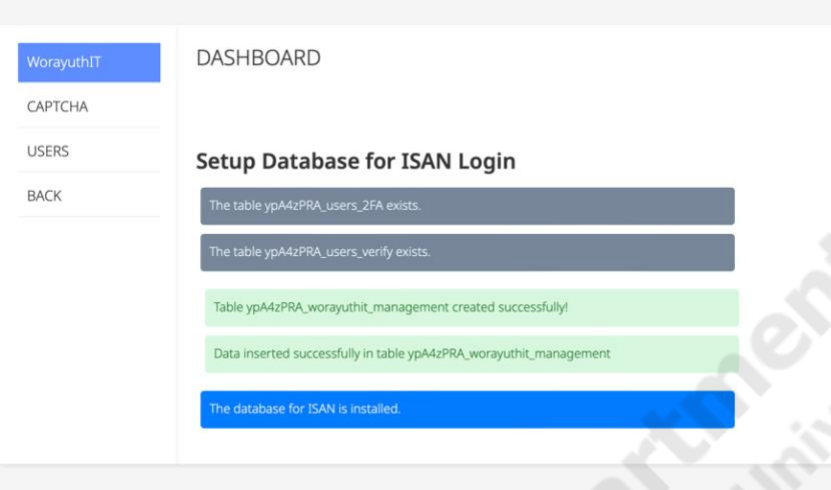
ภาพประกอบที่ 3.18 หน้าสำหรับติดตั้งฐานข้อมูล

3) จากนั้นกด Install เพื่อติดตั้งฐานข้อมูล



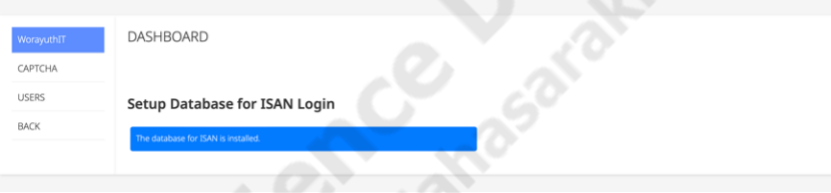
ภาพประกอบที่ 3.19 แจ้งให้ติดตั้งฐานข้อมูล

4) ระบบแจ้งการติดตั้ง ถ้ามีฐานข้อมูลอยู่แล้วจะแจ้งเตือน หากยังไม่มีจะเพิ่ม



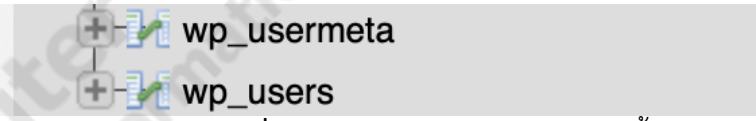
ภาพประกอบที่ 3.20 แจ้งสถานะการติดตั้งฐานข้อมูล

5) เมื่อติดตั้งแล้ว ระบบจะแจ้งว่าฐานข้อมูลที่ต้องใช้งานติดตั้งแล้ว

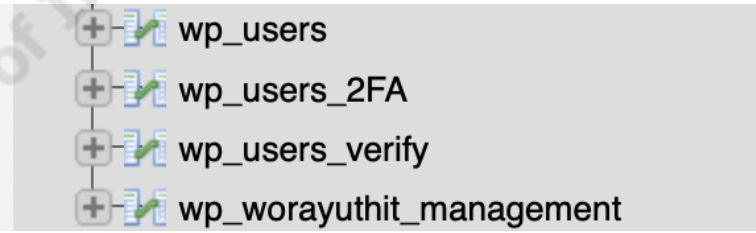


ภาพประกอบที่ 3.21 สถานะการติดตั้งฐานข้อมูล

6) ฐานข้อมูลก่อนและหลังจากติดตั้ง



ภาพประกอบที่ 3.22 ตัวอย่างฐานข้อมูลก่อนติดตั้ง



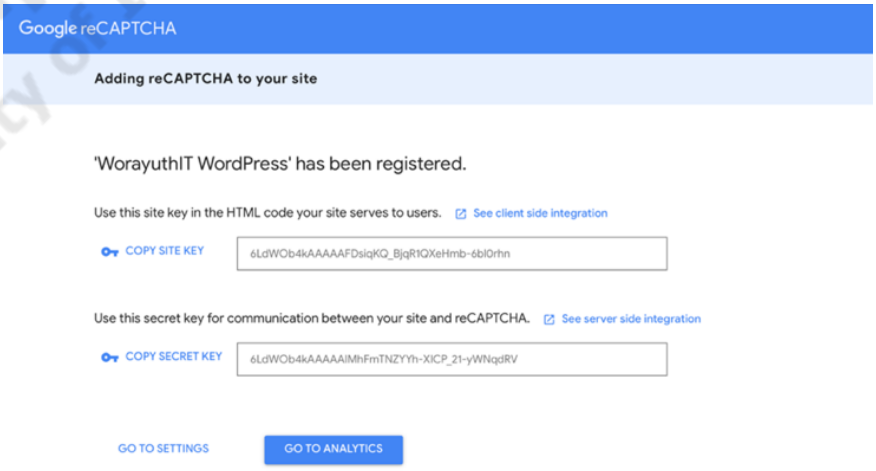
ภาพประกอบที่ 3.23 ตัวอย่างฐานข้อมูลหลังติดตั้งสำเร็จ

3.8 การเพิ่ม Google reCAPTCHA หน้า Login

การเพิ่ม Google reCAPTCHA ในหน้า Login ช่วยป้องกันการโจมตีแบบ Brute-force attack จากบอทหรือการแฮ็กเกอร์ที่พยายามเข้าสู่ระบบโดยใช้ชื่อผู้ใช้งานและรหัสผ่านทดแทนโดยการเพิ่ม Google reCAPTCHA สามารถทำได้โดยมีขั้นตอนดังนี้

1) ลงทะเบียนเว็บไซต์ Google reCAPTCHA

ภาพประกอบที่ 3.24 ลงทะเบียนเว็บไซต์เพื่อสร้างบัญชี Google reCAPTCHA



ภาพประกอบที่ 3.25 Google reCAPTCHA Key

2) โหลดไลบรารีของ Google reCAPTCHA จาก URL ที่กำหนด โดยเพิ่มโค้ดที่ header เพื่อใช้งาน reCAPTCHA

```
172     <script src="https://www.google.com/recaptcha/api.js"></script>
```

ภาพประกอบที่ 3.26 เรียกใช้งานไลบรารีของ Google reCAPTCHA

3) เพิ่ม reCAPTCHA บนฟอร์มต่าง ๆ

```
312         <form action="<?php echo $_SERVER['PHP_SELF']; ?>" method="post">
313             <input type="hidden" name="login_submission" value="1">
314             <input type="text" name="user_login" placeholder="Username or Email" required>
315             <div class="g-recaptcha" data-sitekey="6Lcc6UwmAAAAAOptbeb5EYtMHb1p2gIC1Zpz2Wbs"></div>
316             <input type="submit" value="Submit">
317         </form>
```

ภาพประกอบที่ 3.27 เพิ่ม reCAPTCHA บนฟอร์ม

บรรทัดที่ 315 Attribute data-sitekey ใช้เก็บ Site Key ของ Google reCAPTCHA Site Key ซึ่งจะถูกใช้ในการตรวจสอบความ ถูกต้องของ reCAPTCHA ทุกครั้งที่ผู้ใช้เข้าสู่หน้าเว็บที่มี widget นี้ ผู้ใช้จะต้องกรอกรหัสที่ปรากฏในกล่องนี้เพื่อยืนยันตัวตนว่าเป็นมนุษย์จริง ๆ และไม่ใช่ bot

4) ตรวจสอบผล reCAPTCHA ของผู้ใช้ที่ส่งมา

```
20  $recaptcha_secret = '6Lcc6UwmAAAAAGSEWnkeNrtifDN1yXh1LXG09xfw';
21  $recaptcha_response = $_POST['g-recaptcha-response'];
22  $recaptcha_url = 'https://www.google.com/recaptcha/api/siteverify?secret=' . $recaptcha_secret .
23      '&response=' . $recaptcha_response;
24  $recaptcha = json_decode(file_get_contents($recaptcha_url));
25
26  if ($recaptcha->success) {
27
28  }
29
```

ภาพประกอบที่ 3.28 ตรวจสอบผล reCAPTCHA ของผู้ใช้ที่ส่งมา

บรรทัดที่ 20 secret key เป็นค่าลับที่ได้รับจาก Google reCAPTCHA เมื่อลงทะเบียน Secret key นี้ถูกใช้เพื่อตรวจสอบความถูกต้องของ reCAPTCHA response ที่ได้รับจากผู้ใช้

บรรทัดที่ 21 ใช้เก็บค่าของ reCAPTCHA response ที่ถูกส่งมาจากฟอร์มของผู้ใช้ ข้อมูลนี้จะถูกใส่ในตัวแปร $recaptcha_response จาก POST request ที่ส่งมาจากฟอร์ม

บรรทัดที่ 22-23 ใช้สร้าง link URL สำหรับการตรวจสอบ response จาก Google reCAPTCHA API โดยรวม secret key และ reCAPTCHA response ที่ผู้ใช้ส่งมา

บรรทัดที่ 24 ใช้การเรียกใช้ฟังก์ชัน file_get_contents() เพื่อดึงข้อมูลจาก URL ที่ถูกสร้างขึ้นไว้ในตัวแปร $recaptcha_url และจากนั้นใช้ json_decode() เพื่อแปลงข้อมูล JSON ที่ได้มาให้เป็น object

บรรทัดที่ 24 ตรวจสอบว่า reCAPTCHA response ที่ได้รับจาก Google API ถูกต้องหรือไม่ ถ้า success property ของ object $recaptcha เป็น true แสดงว่าผู้ใช้ผ่านการตรวจสอบ reCAPTCHA

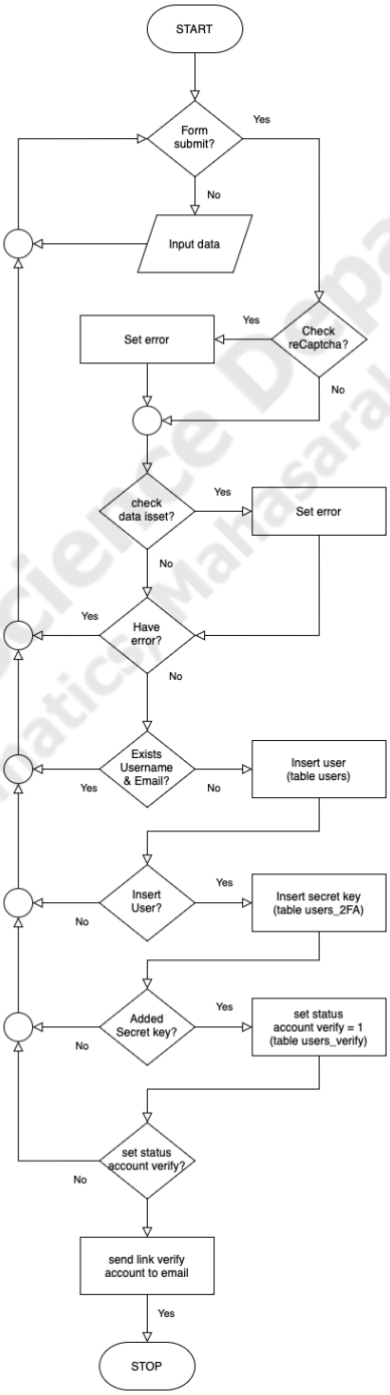
ด้วยการปรับใช้งานอย่างถูกต้อง และการให้ความสำคัญกับความปลอดภัยของเว็บไซต์ ซึ่งทำให้สามารถป้องกันการโจมตี Brute-force attack และรักษาความปลอดภัยของข้อมูลผู้ใช้ได้อย่างมีประสิทธิภาพ

3.9 สร้างหน้าสำหรับการใช้งาน

3.9.1 หน้าสมัครสมาชิก

การสมัครสมาชิกเป็นขั้นตอนที่สำคัญ เมื่อผู้ใช้ต้องการเข้าถึงบริการหรือเนื้อหาบนเว็บไซต์ต่าง ๆ ซึ่งบางเนื้อหามากจะมีการเข้าถึงผ่านบัญชีผู้ใช้

(1) โครงสร้างการทำงาน



ภาพประกอบที่ 3.29 โครงสร้างการทำงานหน้าสมัครสมาชิก

(2) การออกแบบฐานข้อมูล

สร้างฐานข้อมูลสำหรับเก็บข้อมูลและจัดการข้อมูล TOTP 2FA สำหรับใช้การยืนยันชั้นที่สองของการเข้าสู่ระบบของผู้ใช้ โดยสร้างตารางชื่อ users_2FA

ตารางที่ 3.11 ตารางฐานข้อมูล users_2FA

Column	Type	Description	Example	Constraint
id	int(11)	ลำดับ	3	PK
user_id	bigint(20)	รหัสสมาชิก (ไม่สามารถแก้ไขได้)	16	FK
user_key_ secretkey	varchar(255)	สำหรับจัดเก็บ Secret key	AELPGMLN ETOEL65A	Not null
user_otp_ status	tinyint(1)	สำหรับเก็บสถานะการใช้งาน 2FA (0=ปิดใช้งาน 1=เปิดใช้งาน)	0	Not null Default 0

สร้างฐานข้อมูลสำหรับเก็บข้อมูลและจัดการข้อมูล CAPTCHA สำหรับใช้งานหน้าเข้าสู่ระบบ โดยสร้างตารางชื่อ worayuthit _ management

ตารางที่ 3.12 ตารางฐานข้อมูล worayuthit_management

Column	Type	Description	Example	Constraint
id	int(11)	ลำดับ	2	PK
name	varchar(255)	ชื่อ	“login_times”	Not null Default “login_ captcha_attempt”
captcha_ attempt	int(11)	สำหรับจัดเก็บจำนวนให้ใช้งาน CAPTCHA เมื่อผู้ใช้เข้าสู่ระบบล้มเหลว	10	Not null Default 3
captcha_ status	varchar(50)	สำหรับเก็บสถานะการใช้งาน CAPTCHA หน้าเข้าสู่ระบบ	disable	Not null Default “enable”

สร้างฐานข้อมูลสำหรับเก็บข้อมูลและจัดการข้อมูลการยืนยันบัญชี และ token สำหรับยืนยันตัวตนของผู้ใช้ โดยสร้างตารางชื่อ users_verify

ตารางที่ 3.13 ตารางฐานข้อมูล users_verify

Column	Type	Description	Example	Constraint
id	int(11)	ลำดับ	5	PK
user_id	bigint(20)	รหัสสมาชิก (ไม่สามารถแก้ไขได้)	23	FK
acctVerify	tinyint(1)	สำหรับเก็บสถานะ การยืนยันบัญชีผู้ใช้ (0=ยืนยันเรียบร้อย 1=ยังไม่ยืนยัน)	0	Not null Default 1
acctToken	text	สำหรับจัดเก็บ token acctVerify (การยืนยันบัญชี)	3a2aa68ic94lhjryjlrt...	null
acctTokenExp	datetime	สำหรับจัดเก็บวันเวลาหมดอายุของ token acctToken	2023-07-16 22:22:29	null
pwdToken	text	สำหรับจัดเก็บ token pwdToken (การกู้รหัสผ่าน)	80f02e09158ss...	null
pwdTokenExp	datetime	สำหรับจัดเก็บวันเวลาหมดอายุของ token pwdToken	2023-07-25 21:15:37	null
otpToken	text	สำหรับจัดเก็บ token otpToken (การกู้ OTP)	7840c4an1affdhgss...	null
otpTokenExp	datetime	สำหรับจัดเก็บวันเวลาหมดอายุของ token otpToken	2023-07-31 21:45:23	null

หมายเหตุ: ตัวอย่าง (Example) Token ของ acctToken pwdToken และ otpToken “dacbd3df75378dd9a681261386d988d784044a41ab86faea5534de8e1dfb237a9c5b87006078de85d59e7e8d3b0755f2fc165ac6f1690a6078ee1f32455e21a8”

(3) การเขียนโปรแกรม

```
<form action="<?php echo $_SERVER['PHP_SELF']; ?>" method="post">
    <input type="text" name="fname" placeholder="First name" required>
    <input type="text" name="lname" placeholder="Last name" required>
    <input type="text" name="nickname" placeholder="Nickname" required>
    <input type="text" id="username" name="username" placeholder="Username" required pattern="[a-zA-Z0-9_]{6,}">
    <input type="email" name="email" placeholder="Email" required>
    <input type="password" id="password" name="password" placeholder="Password" title="Must contain at least one require." required>
    <input type="password" id="confirmPassword" name="confirmPassword" placeholder="Confirm Password" required>
    <div id="message">
        <p id="letter" class="invalid">A <b>lowercase</b> letter</p>
        <p id="capital" class="invalid">A <b>capital (uppercase)</b> letter</p>
        <p id="number" class="invalid">A <b>number</b></p>
        <p id="length" class="invalid">Minimum <b>8 characters</b></p>
        <p id="match" class="invalid"><b>Passwords match</b></p>
    </div>
    <div class="g-recaptcha" data-sitekey="6Lcc6UwmAAAAAOptbeb5EYtMHb1p2gIC1Zpz2Wbs"></div>
    <input type="submit" id="submitButton" value="Submit" onclick="hashPassword();" disabled>
</form>
```

ภาพประกอบที่ 3.30 ฟอร์มสำหรับป้อนข้อมูล

ฟอร์ม HTML ที่ใช้ในการสร้างหน้าเว็บสำหรับลงทะเบียนผู้ใช้ใหม่ ฟอร์มนี้มีตัวแปรประเภทต่าง ๆ ที่ให้ผู้ใช้กรอกข้อมูลเช่น ชื่อจริง (First name) นามสกุล (Last name) ชื่อเล่น (Nickname) ชื่อผู้ใช้ (Username) อีเมล (Email) รหัสผ่าน (Password) และยืนยันรหัสผ่าน (Confirm Password) นอกจากนี้ยังรวมถึงตัวกรอกสำหรับการใส่ CAPTCHA และปุ่มสำหรับส่งข้อมูล (Submit)

นอกจากนี้ยังมี JavaScript ที่ทำหน้าที่ตรวจสอบความถูกต้องของรหัสผ่านที่ผู้ใช้ป้อนเข้ามา โดยตรวจสอบว่ารหัสผ่านต้องประกอบด้วย อักขระพิมพ์เล็ก (lowercase letter) อักขระพิมพ์ใหญ่ (capital letter) ตัวเลข (number) และมีความยาวอย่างน้อย 8 ตัวอักษร และมีการเรียกฟังก์ชัน hashPassword() เมื่อผู้ใช้กดปุ่ม Submit ซึ่งหมายถึงรหัสผ่านจะถูกเข้ารหัส (hash) ก่อนที่จะถูกส่งไปยังเซิร์ฟเวอร์

```
    if ( empty($errors) ) {

        $query = $wpdb->prepare(
            "SELECT ID FROM $wpdb->users WHERE user_login = %s", $username
        );
        $userID = $wpdb->get_var($query);

        if ($userID) {
            $errors[] = 'Username already exists.';
        } else {
            $query = $wpdb->prepare(
                "SELECT ID FROM $wpdb->users WHERE user_email = %s",
                $email
            );
            $userID2 = $wpdb->get_var($query);

            if ($userID2) {
                $errors[] = 'Email already exists.';
            } else {
                $table_name = $wpdb->prefix . 'users';
                $wpdb->insert(
                    $table_name,
                    array(
                        'user_login' => $username,
                        'user_pass' => $password,
                        'user_email' => $email,
                        'user_registered' => current_time('mysql'),
                        'display_name' => $fname . ' ' . $lname,
                        'user_nicename' => $nickname,
                    )
                );
                $new_user_id = $wpdb->insert_id;

```

ภาพประกอบที่ 3.31 เพิ่มผู้ใช้ในฐานข้อมูล users

โค้ดส่วนนี้ทำงานเพื่อตรวจสอบว่ามีข้อมูลผู้ใช้ที่มีชื่อผู้ใช้หรืออีเมลล์ที่ให้มาแล้วอยู่ในฐานข้อมูลของระบบหรือไม่ โดยใช้ WordPress Database API (wpdb) ซึ่งเป็นตัวช่วยในการทำงานกับฐานข้อมูลของ WordPres หากข้อมูลไม่มีอยู่ในระบบจะเพิ่มผู้ใช้งานใหม่

```
89          $user = get_user_by('login', $username);
90
91          $user_id = $user->ID;
92          $user_name = $user->user_login;
93          $user_skey = generateSecretKey();
94          if (isset($user_id) && isset($user_skey)) {
95              $table_name = $wpdb->prefix . 'users_2FA';
96              $data = array(
97                  'user_id' => $user_id,
98                  'user_secret_key' => $user_skey
99              );
100             $result = $wpdb->insert($table_name, $data);
101
```

ภาพประกอบที่ 3.32 เพิ่ม Secret key ให้กับผู้ใช้ในฐานข้อมูล users_2FA

โค้ดส่วนนี้ทำงานเพื่อสร้าง Secret key และบันทึกข้อมูล ID ผู้ใช้และ Secret Key ลงในตาราง users_2FA ในฐานข้อมูลให้กับผู้ใช้งานเพื่อใช้สำหรับการเข้าสู่ระบบ และใช้สำหรับการยืนยันตัวตนสองขั้นตอน (Two-factor Authentication) ในการเข้าสู่ระบบ

```
103             $table_name = $wpdb->prefix . 'users_verify';
104             $data = array(
105                 'user_id' => $user_id
106             );
107             $result_verify = $wpdb->insert($table_name, $data);
108
```

ภาพประกอบที่ 3.33 กำหนดให้บัญชีที่สมัครใหม่ต้องยืนยัน

เพิ่มข้อมูลลงฐานข้อมูลในตาราง users_verify โดยค่าที่จะเพิ่มคือ ID ของผู้ใช้ ซึ่งถูกกำหนดให้มีค่าเป็นตัวแปร $user_id ที่ถูกส่งมาเป็นอาร์กิวเมนต์หรือค่าที่กำหนดไว้ตามที่ต้องการ และไม่มีค่าอื่น ๆ ที่ถูกกำหนดในตาราง users_verify ดังนั้นค่าในคอลัมน์อื่น ๆ ในตารางนี้จะถูกกำหนดให้เป็นค่า default หรือค่าที่ถูกกำหนดไว้ล่วงหน้า

```
371 <script>
372     function hashPassword() {
373         var username = document.getElementById('username').value;
374         var password = document.getElementById('password').value;
375
376         var saltedPassword = username + password;
377         var hashedPassword = CryptoJS.SHA512(saltedPassword).toString();
378         var hashedPasswordx = CryptoJS.SHA512(hashedPassword).toString();
379
380         document.getElementById('password').value = hashedPasswordx;
381         document.getElementById('confirmPassword').value = hashedPasswordx;
382     }
383 </script>
```

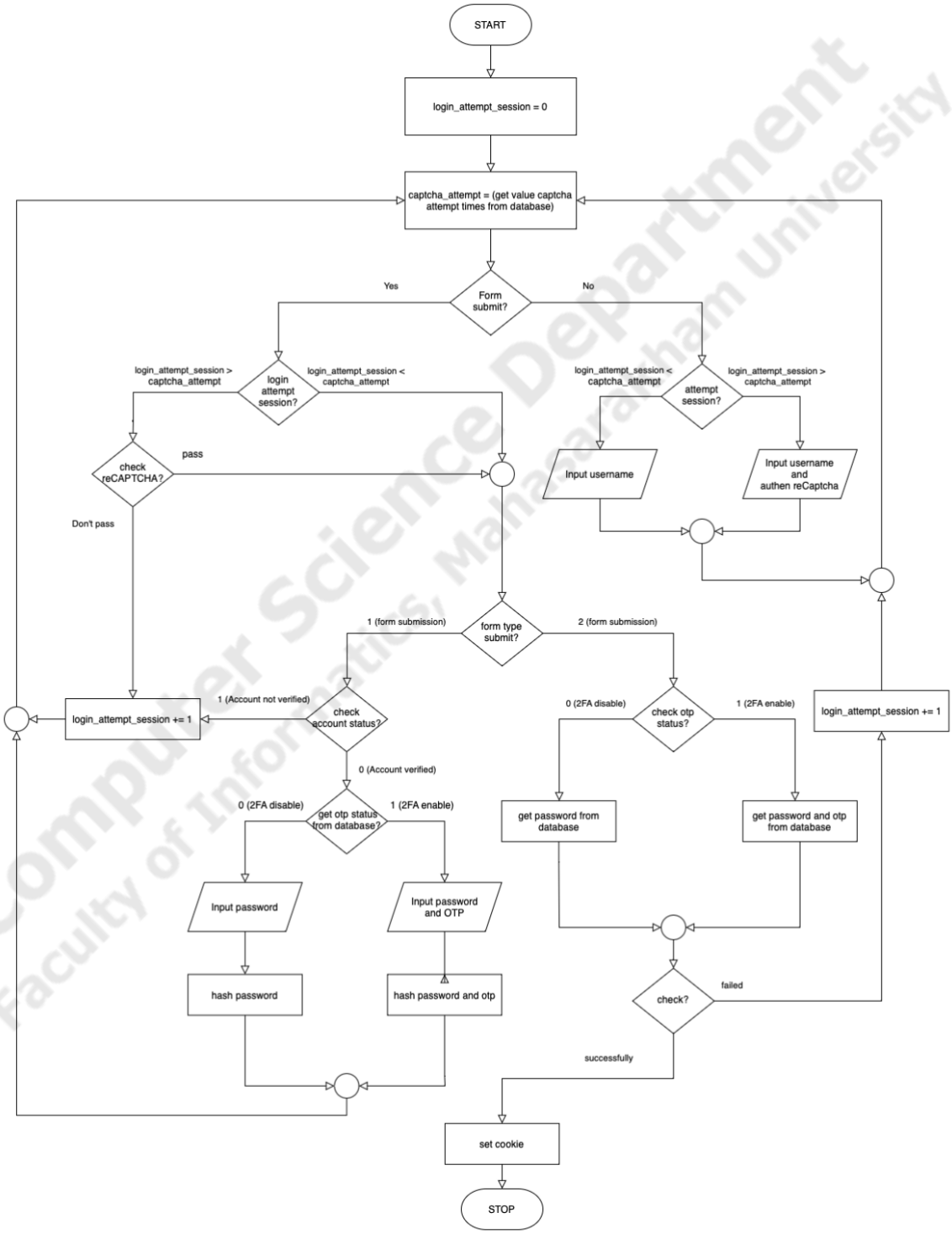
ภาพประกอบที่ 3.34 Client Script สำหรับเข้ารหัสรหัสผ่าน

เป็นส่วนของภาษา JavaScript ที่ใช้ในการประมวลผลการเข้ารหัส (hashing) รหัสผ่าน (password) ของผู้ใช้ เมื่อผู้ใช้กรอกรหัสผ่านและชื่อผู้ใช้ในฟอร์มแล้วกดส่ง โปรแกรมจะนำชื่อผู้ใช้และรหัสผ่านมาผสมกัน (concatenation) และทำการเข้ารหัส(hash) โดยใช้ฟังก์ชัน SHA-512 จากไลบรารี CryptoJS สองครั้ง การเข้ารหัสข้อมูลนี้ เป็นเทคนิคที่ใช้ในการป้องกันการเข้าถึงรหัสผ่านของผู้ใช้แม้ในกรณีที่ข้อมูลถูกดักจับในระหว่างการส่งข้อมูลผ่านเครือข่าย และในกรณีที่ฐานข้อมูลถูกขโมย ข้อมูลที่ถูกเข้ารหัสด้วย SHA-512 จะมีความปลอดภัยสูงเนื่องจากการแตกต่างของผลลัพธ์ทำให้ยากต่อการถอดรหัส

3.9.2 หน้าเข้าสู่ระบบ

หน้าเข้าสู่ระบบสำหรับผู้ใช้งานแบ่งออกเป็น 2 ส่วน คือ ผู้ใช้งานทั่วไปหรือผู้ที่ปิดการใช้งาน 2FA และผู้ใช้งานที่เปิดใช้งาน 2FA

(1) โครงสร้างการทำงาน



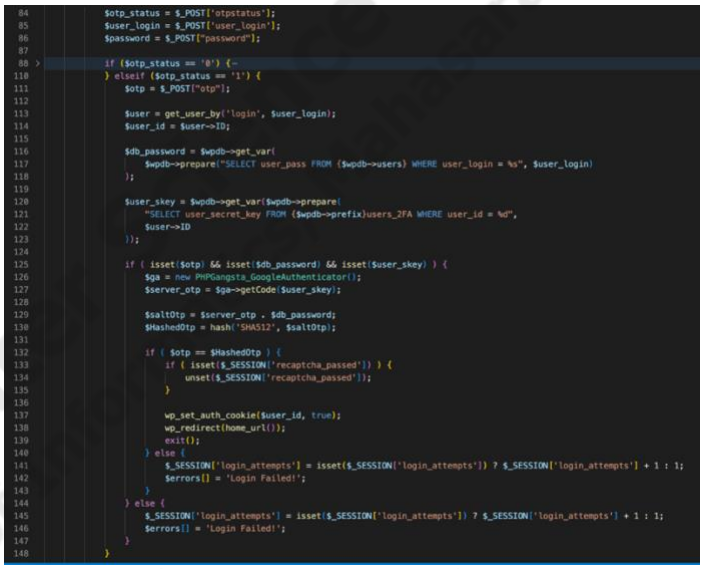
ภาพประกอบที่ 3.35 โครงสร้างการทำงานหน้าเข้าสู่ระบบ

(2) การเขียนโปรแกรม

```
$otp_status = $_POST['otpstatus'];
$user_login = $_POST['user_login'];
$password = $_POST["password"];

if ($otp_status == '0') {
    $db_password = $wpdb->get_var(
        $wpdb->prepare("SELECT user_pass FROM ($wpdb->users) WHERE user_login = %s", $user_login)
    );

    if ( isset($db_password) ) {
        if ( $db_password == $password ) {
            $user = get_user_by('login', $user_login);
            $user_id = $user->ID;

            if ( isset($_SESSION['recaptcha_passed']) ) {
                unset($_SESSION['recaptcha_passed']);
            }

            wp_set_auth_cookie($user_id, true);
            wp_redirect(home_url());
            exit();
        } else {
            $_SESSION['login_attempts'] = isset($_SESSION['login_attempts']) ? $_SESSION['login_attempts'] + 1 : 1;
            $errors[] = 'Login Failed!';
        }
    }
```

ภาพประกอบที่ 3.36 หน้าตรวจสอบผู้ใช้ที่ไม่ใช้งาน TOTP 2FA

โค้ดทำการตรวจสอบตัวแปร otp_status ถ้ามีค่าเป็น '0' (หมายถึงไม่ได้เปิดใช้งาน 2FA TOTP) จะดำเนินการดึงรหัสผ่านที่ถูกเข้ารหัสจากฐานข้อมูลในตาราง users โดยใช้ชื่อผู้ใช้ (user_login) ที่ถูกส่งมา จากนั้นตรวจสอบว่ารหัสผ่านที่ถูกส่งมา ($password) ตรงกับรหัสผ่านในฐานข้อมูลหรือไม่ ถ้าถูกต้องจะตั้งค่าคุกกี้การตรวจสอบสิทธิ์สำหรับผู้ใช้ที่เข้าสู่ระบบ ซึ่งจะช่วยให้ผู้ใช้สามารถเข้าถึงหน้าเว็บที่ต้องการเมื่อมีการตรวจสอบสิทธิ์ได้



```
$otp_status = $_POST['otpstatus'];
$user_login = $_POST['user_login'];
$password = $_POST["password"];

if ($otp_status == '0') {
} elseif ($otp_status == '1') {
    $otp = $_POST["otp"];

    $user = get_user_by('login', $user_login);
    $user_id = $user->ID;

    $db_password = $wpdb->get_var(
        $wpdb->prepare("SELECT user_pass FROM ($wpdb->users) WHERE user_login = %s", $user_login)
    );

    $user_skey = $wpdb->get_var($wpdb->prepare(
        "SELECT user_secret_key FROM {$wpdb->prefix}users_2FA WHERE user_id = %d",
        $user->ID
    ));

    if ( isset($otp) && isset($db_password) && isset($user_skey) ) {
        $ga = new PHPGangsta_GoogleAuthenticator();
        $server_otp = $ga->getCode($user_skey);

        $saltOtp = $server_otp . $db_password;
        $HashedOtp = hash('SHA512', $saltOtp);

        if ( $otp == $HashedOtp ) {
            if ( isset($_SESSION['recaptcha_passed']) ) {
                unset($_SESSION['recaptcha_passed']);
            }

            wp_set_auth_cookie($user_id, true);
            wp_redirect(home_url());
            exit();
        } else {
            $_SESSION['login_attempts'] = isset($_SESSION['login_attempts']) ? $_SESSION['login_attempts'] + 1 : 1;
            $errors[] = 'Login Failed!';
        }
    } else {
        $_SESSION['login_attempts'] = isset($_SESSION['login_attempts']) ? $_SESSION['login_attempts'] + 1 : 1;
        $errors[] = 'Login Failed!';
    }
}
```

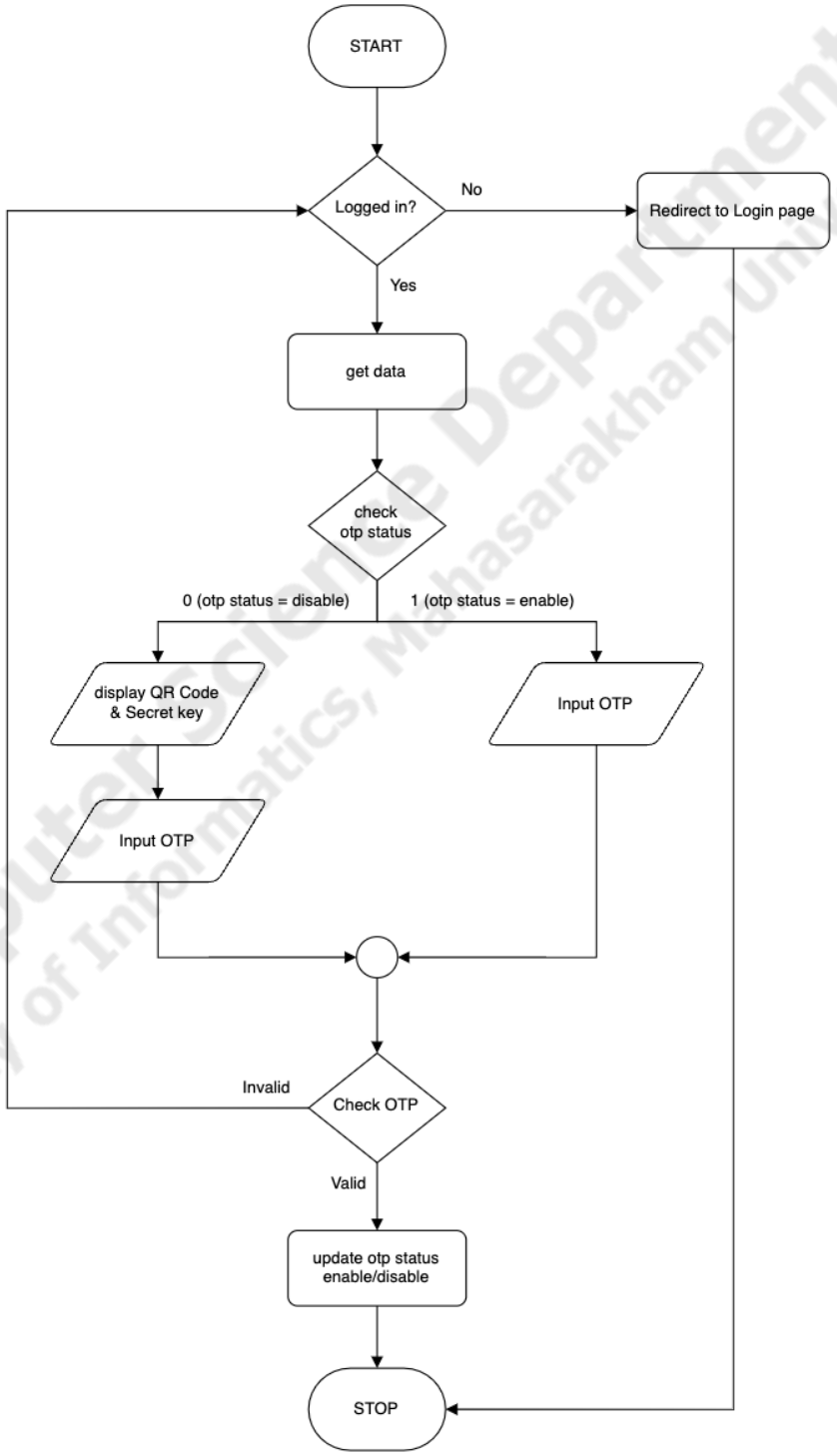
ภาพประกอบที่ 3.37 หน้าตรวจสอบผู้ใช้ที่เปิดใช้งาน TOTP 2FA

โค้ดทำการตรวจสอบตัวแปร otp_status ถ้ามีค่าเป็น '1' (หมายถึงเปิดใช้งาน 2FA TOTP) จะดำเนินการดึงรหัสผ่านที่ถูกเข้ารหัสจากฐานข้อมูลในตาราง users โดยใช้ชื่อผู้ใช้ (user_login) ที่ถูกส่งมาและดึง Secret Key จากตาราง users_2FA ใช้ Google Authenticator library เพื่อสร้างรหัส OTP ของเซิร์ฟเวอร์โดยใช้ Secret Key ของผู้ใช้ นำข้อมูลที่เข้ารหัสในตัวแปร $otp ที่ผู้ใช้ส่งเข้ามามาทำการเปรียบเทียบกับรหัส OTP ที่สร้างขึ้นจากฝั่งเซิร์ฟเวอร์โดยเข้ารหัสกับรหัสผ่าน ถ้าถูกต้องจะตั้งค่าคุกกี้การตรวจสอบสิทธิ์สำหรับผู้ใช้ที่เข้าสู่ระบบ ซึ่งจะช่วยให้ผู้ใช้สามารถเข้าถึงหน้าเว็บที่ต้องการเมื่อมีการตรวจสอบสิทธิ์ได้

3.9.3 หน้าใช้งาน TOTP 2FA

หน้าเข้าสู่ระบบสำหรับผู้ใช้งานแบ่งออกเป็น 2 ส่วน คือ ผู้ใช้งานทั่วไปหรือผู้ที่ปิดการใช้งาน 2FA และผู้ใช้งานที่เปิดใช้งาน 2FA

(1) โครงสร้างการทำงาน



ภาพประกอบที่ 3.38 โครงสร้างการทำงานหน้าใช้งาน TOTP 2FA

(2) การเขียนโปรแกรม

```php
$secret_key = $wpdb->get_var($wpdb->prepare(
    "SELECT user_secret_key FROM {$wpdb->prefix}users_2FA WHERE user_id = %d",
    $user_id
));
$otp_status = $wpdb->get_var($wpdb->prepare(
    "SELECT user_otp_status FROM {$wpdb->prefix}users_2FA WHERE user_id = %d",
    $user_id
));

$name = $current_user->user_login;
$issuer = "WorayuthIT.com";
$qrCodeUrl = "https://chart.googleapis.com/chart?chs=200x200&chld=M%7C0&cht=qr&chl=" .
    urlencode("otpauth://totp/$name?secret=$secret_key&issuer=$issuer");
```

ภาพประกอบที่ 3.39 สร้าง QR Code

ดึงข้อมูล Secret Key (user_secret_key) และสถานะ OTP (user_otp_status) จากตาราง users_2FA ในฐานข้อมูล สำหรับผู้ใช้ที่มี ID เท่ากับ $user_id ข้อมูลนี้จะถูกใช้ในกระบวนการสร้างรหัส OTP และตรวจสอบสถานะของ OTP กำหนดค่าที่ใช้ในการสร้าง QR Code สำหรับการยืนยันตัวตนแบบ OTP (One-Time Password). โดยกำหนดชื่อผู้ใช้ ($name), ผู้ออก OTP ($issuer), Secret Key ($secret_key) และ URL สำหรับ QR Code ($qrCodeUrl) URL นี้จะถูกใช้ในการสร้างรหัส QR Code ที่ผู้ใช้สามารถสแกนเพื่อเพิ่มการยืนยันตัวตนแบบ OTP ในแอปพลิเคชัน OTP Authenticator

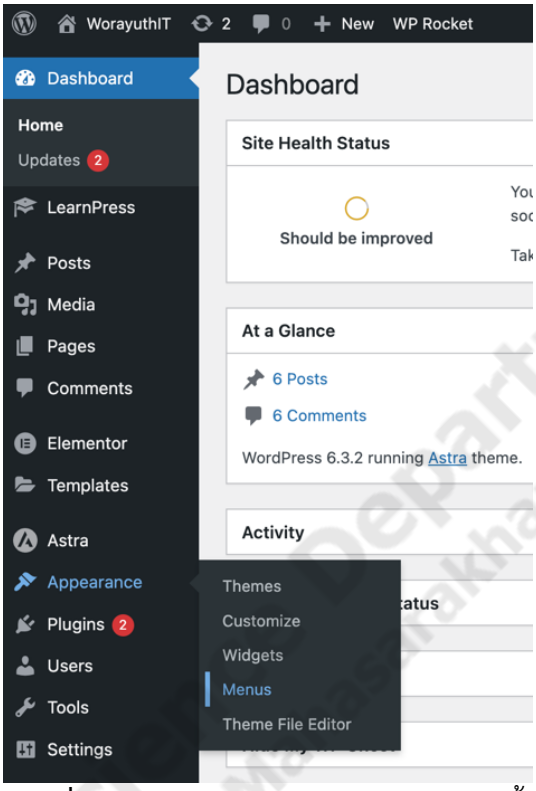
```php
if (isset($user_input_otp)) {
    $secret_key = $wpdb->get_var($wpdb->prepare(
        "SELECT user_secret_key FROM {$wpdb->prefix}users_2FA WHERE user_id = %d", $user_id
    ));

    $ga = new PHPGangsta_GoogleAuthenticator();
    $user_server_totp = $ga->getCode($secret_key);
    if ($user_server_totp == $user_input_otp) {
        if ($mode == "enable") {
            $wpdb->update(
                "{$wpdb->prefix}users_2FA",
                array('user_otp_status' => '1'),
                array('user_id' => $user_id)
            );
            $messageSuccess = 'Enable Two-Factor successfully.';
            header("Location: 2Factor.php?message=" . urlencode($messageSuccess));
            exit();
        } elseif ($mode == "disable") {
            $wpdb->update(
                "{$wpdb->prefix}users_2FA",
                array('user_otp_status' => '0'),
                array('user_id' => $user_id)
            );
            $messageSuccess = 'Disable Two-Factor successfully.';
            header("Location: 2Factor.php?message=" . urlencode($messageSuccess));
            exit();
        } else {
            $errors[] = 'Failed! Please enter totp numner!';
        }
    } else {
        $errors[] = 'Failed! Invalid totp numner!';
    }
} else {
    $errors[] = 'Failed! Please enter totp numner!';
}
```

ภาพประกอบที่ 3.40 เปิดปิดสถานะการใช้งาน 2FA TOTP

สำหรับการใช้งาน Two-Factor Authentication (2FA) ด้วย TOTP (Time-based One-Time Password) โดยการตรวจสอบค่า TOTP ที่ผู้ใช้ป้อนเข้ามากับค่า TOTP ที่ได้จาก server โดยนำ Secret key ของผู้ใช้คนนั้นมาเปรียบเทียบกัน หากถูกต้องจะทำการเปลี่ยนสถานการณ์ใช้งานเป็น enable หรือ disable

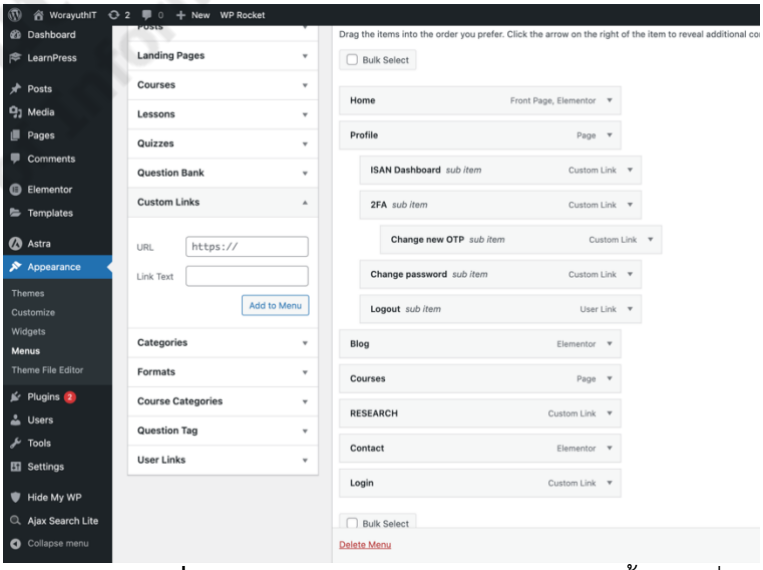
3.10 การเรียกใช้งานหน้าต่าง ๆ โดยใช้ URL

1) ไปที่ WordPress dashboard และ Appearance และเลือก Menus



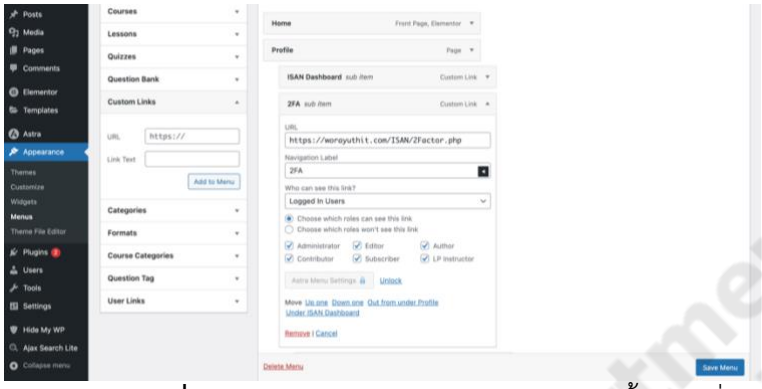
ภาพประกอบที่ 3.41 การเรียกใช้งาน Custom page ขั้นตอนที่ 1

2) เลือก Custom Links และป้อน URL path หน้าที่ต้องการและกำหนดชื่อ และคลิก Add to Menu



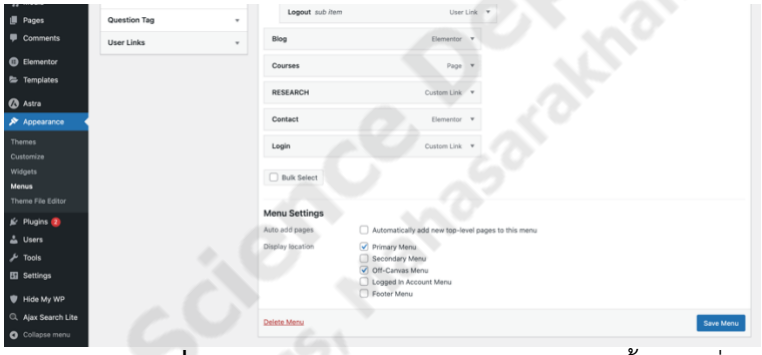
ภาพประกอบที่ 3.42 การเรียกใช้งาน Custom page ขั้นตอนที่ 2

3) เมนูที่เพิ่มเข้ามาแล้วจะสามารถกำหนดได้ว่าต้องการให้ผู้ใช้งานสถานะและบทบาทที่กำหนดสามารถเห็นได้



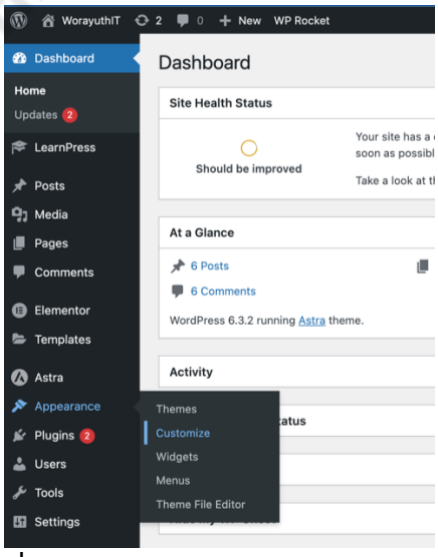
ภาพประกอบที่ 3.43 การเรียกใช้งาน Custom page ขั้นตอนที่ 3

4) เลือกหมวดที่ต้องการให้เมนูที่เพิ่มเข้าไป



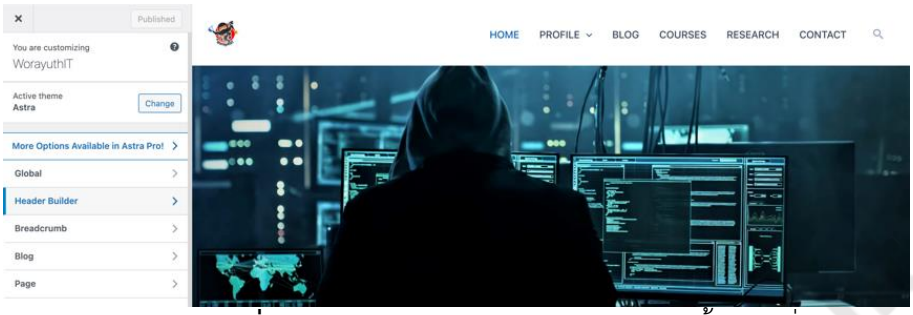
ภาพประกอบที่ 3.44 การเรียกใช้งาน Custom page ขั้นตอนที่ 4

5) จากนั้นไปที่ Appearance และ Customsize



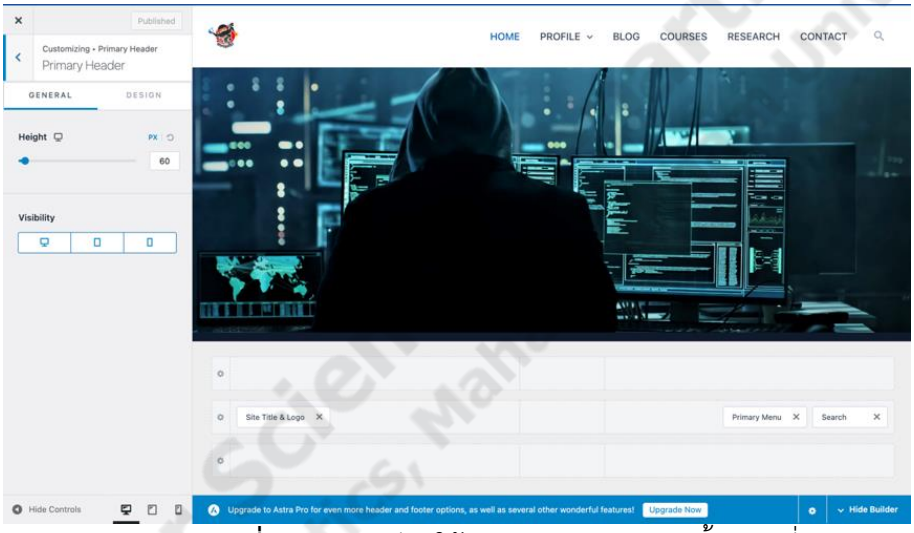
ภาพประกอบที่ 3.45 การเรียกใช้งาน Custom page ขั้นตอนที่ 5

6) เลือก Header Builder



ภาพประกอบที่ 3.46 การเรียกใช้งาน Custom page ขั้นตอนที่ 6

7) เลือกตำแหน่งหมวดหมู่ที่มีเมนูที่ต้องการแสดงเพื่อใช้งาน



ภาพประกอบที่ 3.47 การเรียกใช้งาน Custom page ขั้นตอนที่ 7

8) สำเร็จปุ่มที่มีเมนู link URL ที่กำหนดจะแสดงที่ที่กำหนด และสามารถคลิกเพื่อเปลี่ยนเส้นทางไปยัง URL นั้นได้

ภาพประกอบที่ 3.48 การเรียกใช้งาน Custom page ขั้นตอนที่ 8

3.11 การทดสอบความปลอดภัยของเว็บไซต์ WorayuthIT

3.11.1 ประเภทการโจมตี

(1) Brute-force attack

การโจมตีด้วยวิธีแบบบรูทฟอร์ซคือวิธีการโจมตีที่ผู้ไม่หวังดีพยายามเข้าถึงระบบโดยการลองทุกรหัสผ่านที่เป็นไปได้จนกว่าจะพบรหัสผ่านที่ถูกต้อง การโจมตีด้วยวิธีนี้มีความเสี่ยงสูงเนื่องจากมีโอกาสที่จะพบรหัสผ่านที่ถูกต้อง ทำให้ผู้โจมตีสามารถเข้าถึงข้อมูลที่ปลอดภัย

(2) SSL Strip Attack

SSL Strip Attack เป็นวิธีการโจมตีที่ผู้โจมตีหลอกให้ผู้ใช้เชื่อมต่อกับเว็บไซต์ผ่าน HTTP แทนที่ใช้ HTTPS ทำให้ข้อมูลที่ส่งผ่านเครือข่ายอยู่ในรูปแบบข้อความไม่เข้ารหัส ทำให้ผู้โจมตีสามารถดักจับข้อมูลสำคัญได้ โดยใช้คำสั่งโจมตีดังนี้

- sudo bettercap: คำสั่งเพื่อเริ่มใช้งาน BetterCap
- net.probe on: เปิดใช้งานเพื่อสแกนเครือข่ายสามารถใช้เพื่อค้นหาและตรวจสอบเครื่องคอมพิวเตอร์หรืออุปกรณ์อื่น ๆ ที่เชื่อมต่อในเครือข่าย
- net.show: แสดงรายการของอุปกรณ์ที่ตรวจพบในเครือข่าย
- set arp.spoof.fullduplex true: ตั้งค่าการโจมตีให้ทำงานในโหมด full-duplex เพื่อส่งและรับข้อมูลพร้อมกัน
- set arp.spoof.targets <IP target>: ใช้กำหนดเครือข่ายหรืออุปกรณ์เป้าหมายที่เป็นเป้าหมายของการโจมตี ARP Spoof โดยระบุที่อยู่ IP
- arp.spoof on: เปิดใช้งานโมดูล ARP spoofing ใน BetterCAP เพื่อเริ่มการโจมตี
- set net.sniff.local true: ใช้ตั้งค่าการดักจับข้อมูลเครือข่ายเพื่อดักและตรวจสอบการสื่อสารภายในเครือข่าย
- set net.sniff.verbose false: ตั้งค่าการ sniffing เครือข่ายเพื่อไม่แสดงข้อมูลเพิ่มเติม
- set http.proxy.sslstrip true: ตั้งค่าให้ BetterCap ทำงานในโหมด SSL Strip เพื่อลดระดับความปลอดภัยการเชื่อมต่อ HTTPS เปลี่ยนเป็น HTTP
- http.proxy on: เปิดการสร้างพร็อกซี HTTP โดย BetterCap เพื่อที่ BetterCap จะสามารถตรวจสอบและแก้ไขข้อมูลที่ถูกส่งผ่าน HTTP และ HTTPS
- net.sniff on: เปิดการ sniffing ข้อมูลเครือข่ายเพื่อดักและตรวจสอบการส่งข้อมูลในเครือข่าย

3.11.2 เครื่องมือสำหรับการทดสอบการโจมตี

(1) Kali Linux

ภาพประกอบที่ 3.49 Kali Linux logo

Kali Linux [14] เป็นระบบปฏิบัติการลินุกซ์ที่เน้นไปที่การทดสอบการเจาะระบบและการตรวจสอบความปลอดภัยของระบบ เป็น open source และถูกพัฒนาขึ้นโดยชุมชนนักพัฒนาและนักวิจัยด้านความปลอดภัย ซึ่งมุ่งเน้นไปที่การพัฒนาเครื่องมือและทรัพยากรที่ใช้ในการทดสอบและวิเคราะห์ระบบคอมพิวเตอร์เพื่อค้นหาช่องโหว่และปรับปรุงระบบให้มีความปลอดภัยมากขึ้น

(2) BetterCap

ภาพประกอบที่ 3.50 BetterCap logo

BetterCap [15] เป็นเครื่องมือที่ใช้ในการทดสอบความปลอดภัยและการโจมตีเครือข่าย โดยเฉพาะเครือข่ายไร้สายและโปรโตคอล HTTP/HTTPS ซึ่งเป็นเครื่องมือที่มีคุณสมบัติและฟังก์ชันหลากหลายเพื่อการทดสอบและตรวจสอบความปลอดภัยในเครือข่าย

(3) Burp Suite

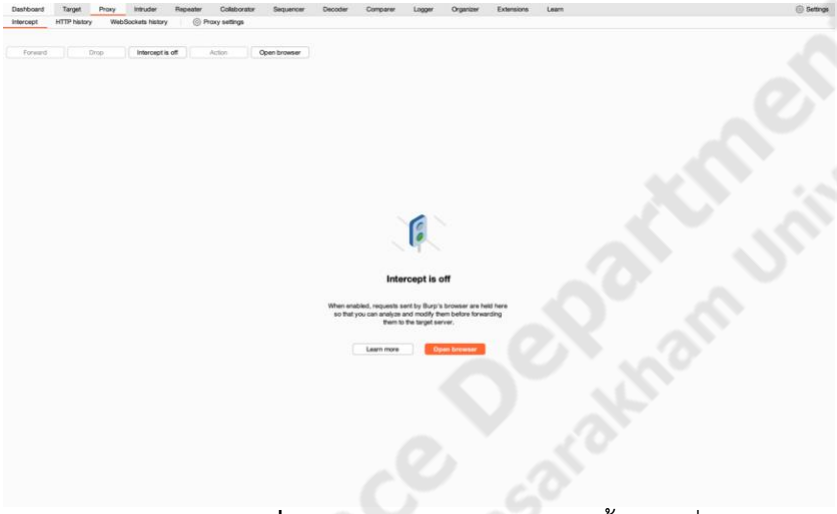
ภาพประกอบที่ 3.51 Burp Suite logo

Burp Suite [16] คือเครื่องมือทดสอบความปลอดภัยทางเว็บแอปพลิเคชัน (web application security testing tool) ที่ใช้ในการตรวจสอบช่องโหว่และปัญหาด้านความปลอดภัยของเว็บไซต์และแอปพลิเคชัน ช่วยให้ผู้ทดสอบสามารถค้นหาช่องโหว่ที่เป็นไปได้และทดสอบการโจมตีด้วยวิธีต่าง ๆ เพื่อปรับปรุงความปลอดภัยของระบบอย่างมีประสิทธิภาพ

3.11.3 ขั้นตอนการทดสอบ

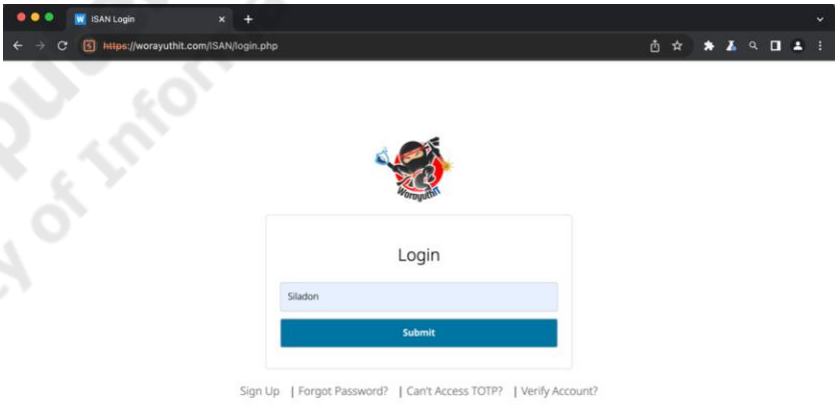
(1) Brute-force attack

การโจมตี Brute-force attack คือวิธีการที่พยายามเข้าถึงระบบหรือบัญชีโดยลองทุกรหัสผ่านที่เป็นไปได้จนกว่าจะพบรหัสผ่านที่ถูกต้อง ซึ่งการป้องกันการโจมตี Brute-force attack จาก Bot โดยการใช้โปรแกรมเพื่อเข้าสู่ระบบ ซึ่งผลการทำงานดังนี้



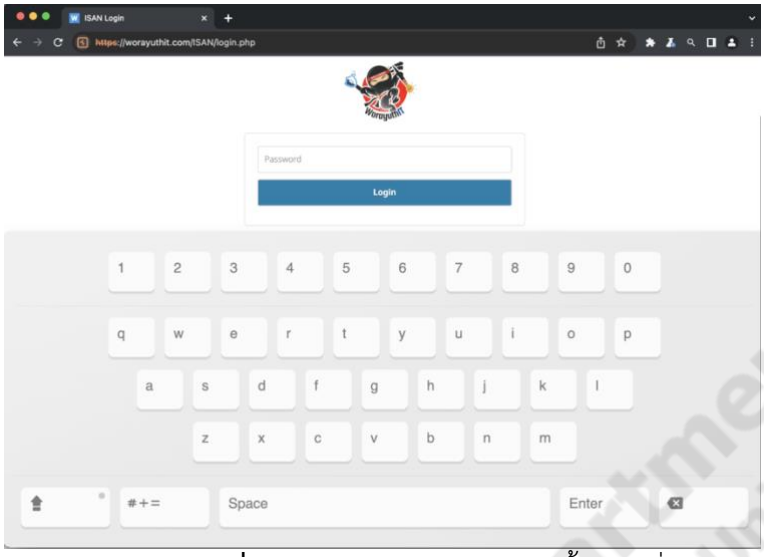
ภาพประกอบที่ 3.52 Brute-force attack ขั้นตอนที่ 1

เข้าสู่ Burp Suite คลิกที่เมนู "Proxy" ที่อยู่บนแถบเมนูหลักของโปรแกรมและภายในเมนู Proxy เลือกเมนูย่อยที่ชื่อ "Intercept" จากนั้นคลิก Open browser โดยที่ปุ่มฟังก์ชันเป็น "Intercept is off" คือ ฟังก์ชันการดักจับ (Intercept) ใน Burp Suite ถูกปิดการใช้งานอยู่

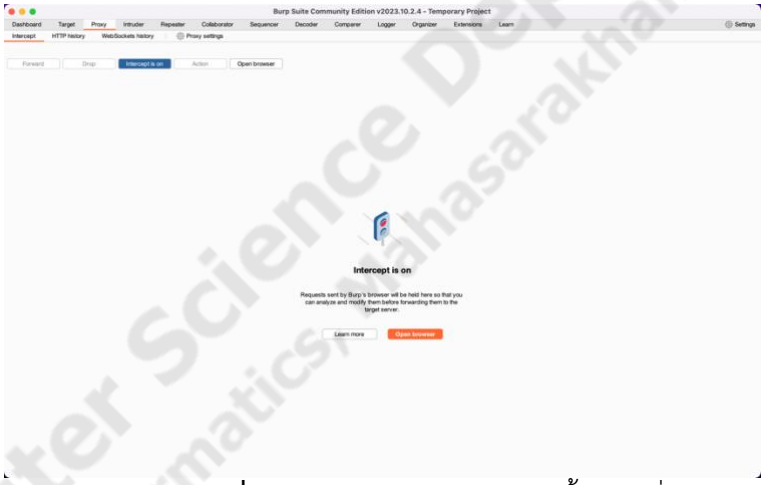


ภาพประกอบที่ 3.53 Brute-force attack ขั้นตอนที่ 2

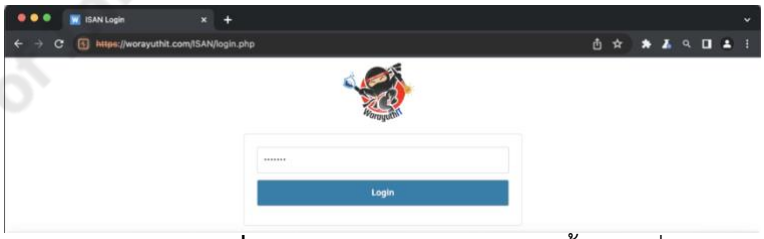
เมื่อคลิก "Open browser" ใน Burp Suite โปรแกรมจะเปิดหน้าต่างเบราว์เซอร์สามารถเริ่มต้นการทดสอบโดยเข้าสู่เว็บไซต์หรือแอปพลิเคชันที่ต้องการทดสอบ ข้อมูลที่ส่งระหว่างคอมพิวเตอร์กับเซิร์ฟเวอร์จะถูกแสดงใน Burp Suite ในส่วนของ Proxy โดยสามารถดักจับและแก้ไขข้อมูลเหล่านี้เพื่อทดสอบความปลอดภัยของแอปพลิเคชันหรือเว็บไซต์



ภาพประกอบที่ 3.54 Brute-force attack ขั้นตอนที่ 3

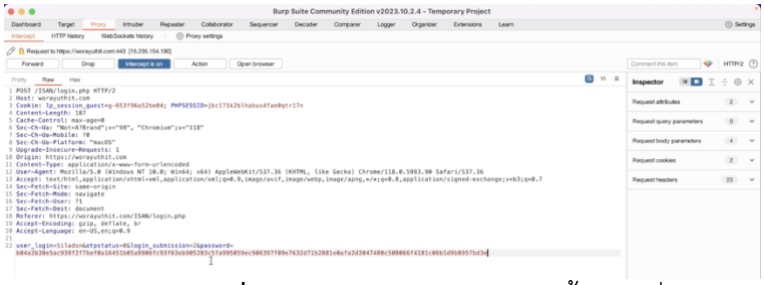


ภาพประกอบที่ 3.55 Brute-force attack ขั้นตอนที่ 4

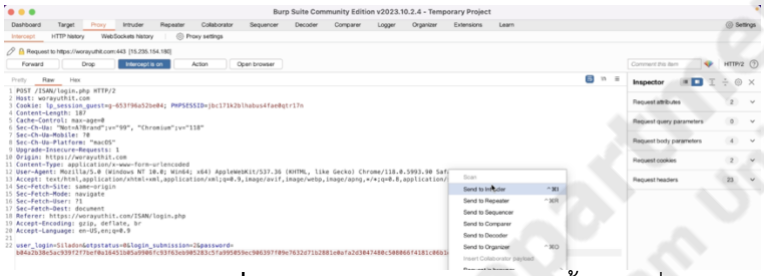


ภาพประกอบที่ 3.56 Brute-force attack ขั้นตอนที่ 5

เมื่อหน้าต่างให้ป้อนรหัสผ่านขึ้นมาแล้ว ให้กลับไปที่ Burp Suite และเปิดฟังก์ชันการดักจับ (Intercept) ใน Burp Suite ที่ถูกปิดการใช้งานอยู่เป็น "Intercept is on" จากนั้นกลับมาที่หน้าป้อนรหัสผ่านเพื่อป้อนรหัสผ่านและส่งแบบฟอร์ม



ภาพประกอบที่ 3.57 Brute-force attack ขั้นตอนที่ 6



ภาพประกอบที่ 3.58 Brute-force attack ขั้นตอนที่ 7

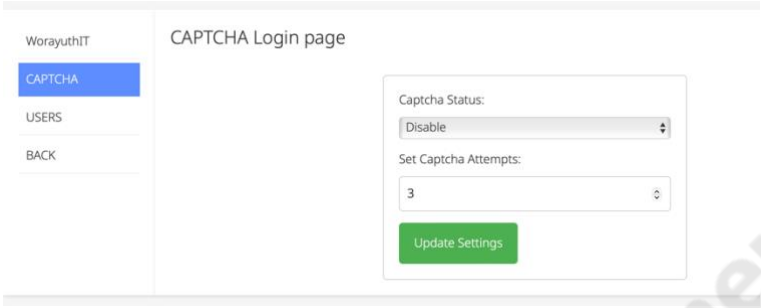
หลังจากที่ได้รับแบบฟอร์มและกำหนดข้อมูลที่ต้องการทดสอบใน Burp Suite สามารถกดปุ่ม "Send to Intruder" เพื่อส่งข้อมูลไปยังโมดูล Intruder ของ Burp Suite และจะเปิดหน้าต่างใหม่ที่ใช้ในการกำหนดการทดสอบต่อไป

ภาพประกอบที่ 3.59 กำหนดที่ต้องการเปลี่ยน

ในโมดูล Intruder กำหนดจุดเริ่มต้นและสิ้นสุดของข้อมูลที่ต้องการทดสอบ Brute-force ได้โดยการใช้ "mark" เพื่อระบุตำแหน่งที่ต้องการเปลี่ยนค่าข้อมูล ในที่นี้ตั้งค่าให้เป็นส่วนของรหัสผ่าน (password) เพื่อให้โปรแกรมทำการทดสอบทุกรหัสผ่านที่อาจเป็นไปได้ในส่วนนี้

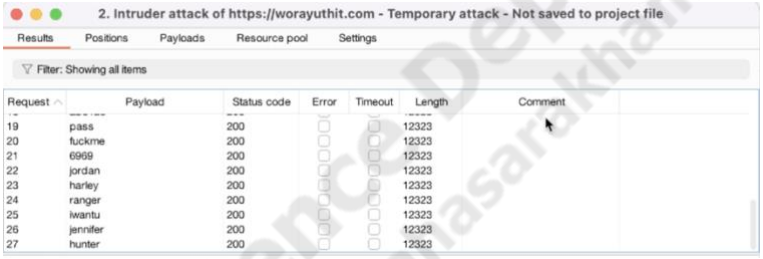
ภาพประกอบที่ 3.60 กำหนดรายการรหัสผ่าน Plain text

ในโมดูล Intruder ไปที่ "Payloads" และกำหนดรายการรหัสผ่าน (password) เพื่อจะให้รายการที่กำหนดใช้งานในการเปลี่ยนรหัสผ่านไปเรื่อย ๆ



ภาพประกอบที่ 3.61 ปิดการใช้งาน reCAPTCHA หน้าเข้าสู่ระบบ

ทดสอบด้วยการปิดการใช้งาน reCAPTCHA ในหน้าเข้าสู่ระบบ เพื่อทดสอบหน้าเข้าสู่ระบบ โดยการไม่มี reCAPTCHA ในการป้องกัน

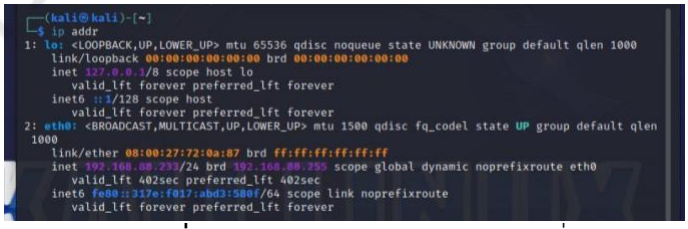


ภาพประกอบที่ 3.62 ดำเนินการเดารหัสผ่าน

(2) SSL Strip Attack

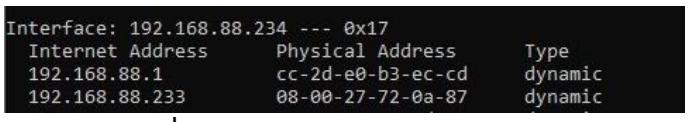
การทดลองโจมตีเพื่อทดสอบความเชื่อถือเมื่อเว็บไซต์ถูกเปลี่ยนการใช้งานจากโปรโตคอล HTTPS เป็น HTTPS โดยการทดสอบระหว่างการใช้งานปกติของ WordPress และการเพิ่มการเข้ารหัส (hash) ที่ด้านของผู้ใช้ก่อนที่ข้อมูลจะถูกส่งต่อไป โดยมีขั้นตอนการทดสอบดังนี้

- ตรวจสอบ IP Address เครื่องผู้โจมตี



ภาพประกอบที่ 3.63 ตรวจสอบ IP Address เครื่องผู้โจมตี

- ตรวจสอบ IP Address และ MAC Address ของ gateway

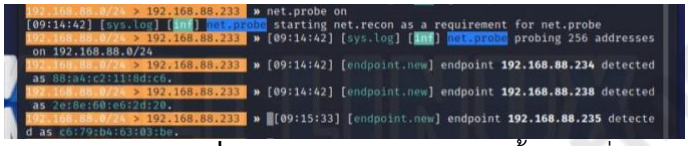


ภาพประกอบที่ 3.64 ตรวจสอบ IP Address และ Gateway

- เข้าใช้งาน Kali Linux และใช้งานในสิทธิ์ของ root และเรียกใช้ BetterCap

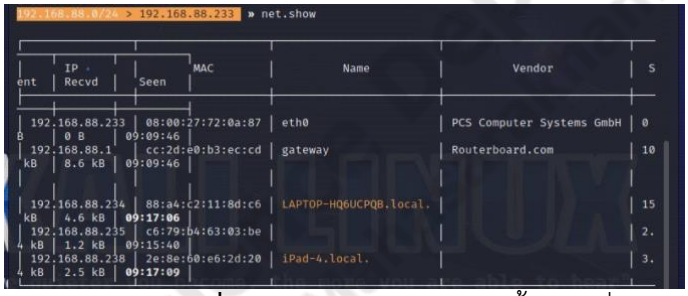
ภาพประกอบที่ 3.65 SSL Strip Attack ขั้นตอนที่ 1

- แสกนหาอุปกรณ์อื่น ๆ ในเครือข่าย



ภาพประกอบที่ 3.66 SSL Strip Attack ขั้นตอนที่ 2

- ตรวจสอบอุปกรณ์ในเครือข่าย

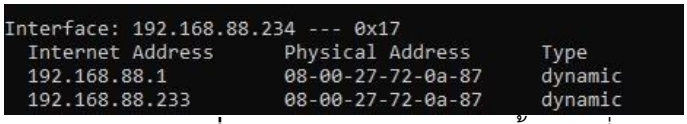


ภาพประกอบที่ 3.67 SSL Strip Attack ขั้นตอนที่ 3

- กำหนด IP Address ของเหยื่อ

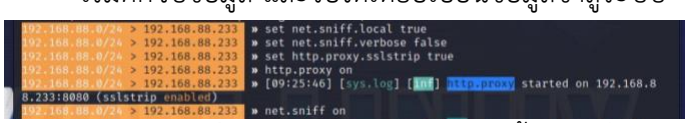
ภาพประกอบที่ 3.68 SSL Strip Attack ขั้นตอนที่ 4

- ตรวจสอบ IP Address และ MAC Address ของ gateway



ภาพประกอบที่ 3.69 SSL Strip Attack ขั้นตอนที่ 5

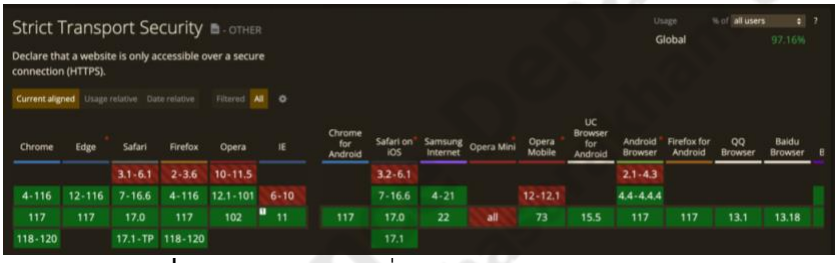
- เริ่มดักจับข้อมูล และรอให้เหยื่อเป่อนข้อมูลข้าสู่ระบบ



ภาพประกอบที่ 3.70 SSL Strip Attack ขั้นตอนที่ 6

3.12 การใช้งาน HSTS preload สำหรับเว็บไซต์ worayuthit.com

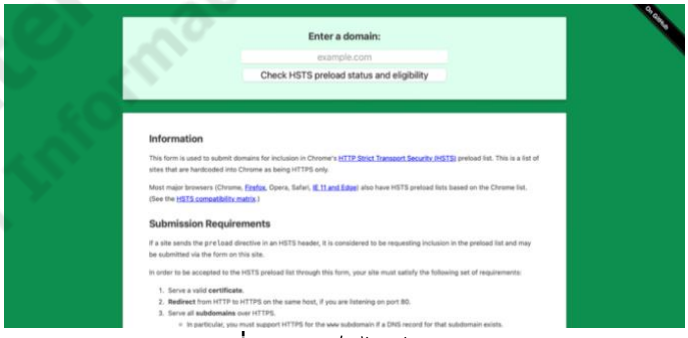
HTTP Strict Transport Security (HSTS) [17] เป็นมาตรฐานการสื่อสารของ Internet Engineering Task Force (IETF) ตาม RFC 6797 ที่ประกาศในปี ค.ศ. 2012 เพื่อเสริมความปลอดภัยของเว็บไซต์ที่เปิดใช้ผ่านเว็บเบราว์เซอร์ หลักการหลักคือป้องกันการโจมตีแบบ Man In The Middle Attack โดยทำให้เซิร์ฟเวอร์ส่ง HTTP Header ที่มีชื่อว่า Strict-Transport-Security: max-age=31536000; includeSubDomains; preload ไปยังเบราว์เซอร์ เมื่อเบราว์เซอร์ตรวจพบ HTTP Header นี้ เว็บเซิร์ฟเวอร์จะบังคับการสื่อสารผ่านช่องทาง HTTPS เท่านั้น นอกจากนี้เว็บเบราว์เซอร์จะปฏิเสธการเชื่อมต่อที่ไม่ได้ใช้ HTTPS ทั้งหมด ทำให้ HSTS เป็นเทคนิคที่มีประสิทธิภาพในการป้องกันการโจมตีแบบแทรกกลางการสื่อสาร เช่น SSL Stripping Attack ซึ่งเป็นวิธีการโจมตีที่ได้รับความนิยมอย่างมากในปัจจุบัน ซึ่งเว็บเบราว์เซอร์ที่รองรับกลไก HSTS สามารถดูได้ดังภาพประกอบที่ 3.71



ภาพประกอบที่ 3.71 เบราว์เซอร์ที่รองรับการทำงานกลไก HSTS preload

3.12.1 ขั้นตอนการ HSTS preload เว็บไซต์ worayuthit.com

(1) เข้าเว็บไซต์ hstspreload.org

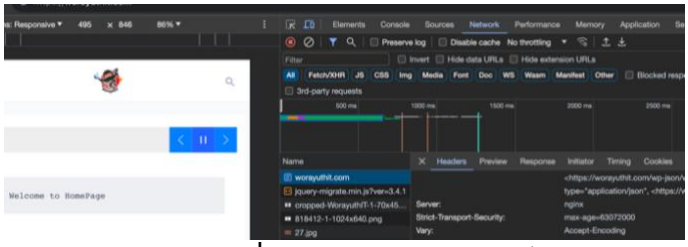


ภาพประกอบที่ 3.72 เว็บไซต์ hstspreload.org

(2) ตรวจสอบสถานะการ preload ของเว็บไซต์ โดยเว็บไซต์ hstspreload.org

ภาพประกอบที่ 3.73 ระบบแจ้งสถานะยังไม่ได้ HSTS preload

(3) ตรวจสอบการกำหนด hsts preload ที่ header ของเว็บไซต์ worayuthit.com



ภาพประกอบที่ 3.74 HSTS header เว็บไซต์

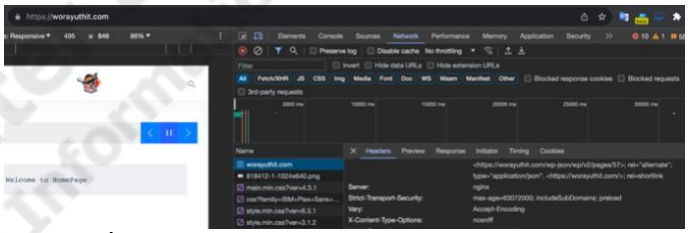
(4) ตรวจสอบการกำหนด hsts header ที่ไฟล์ .htaccess

ภาพประกอบที่ 3.75 ตรวจสอบการกำหนด hsts header ที่ไฟล์ .htaccess

(5) แก้ไขไฟล์ .htaccess ตามการแจ้งจากการตรวจสอบที่เว็บ hstspreload.org

ภาพประกอบที่ 3.76 แก้ไขการกำหนด hsts preload ที่ไฟล์ .htaccess

(6) ตรวจสอบหลังจากกำหนดค่าใหม่ที่ header ของเว็บไซต์ worayuthit.com

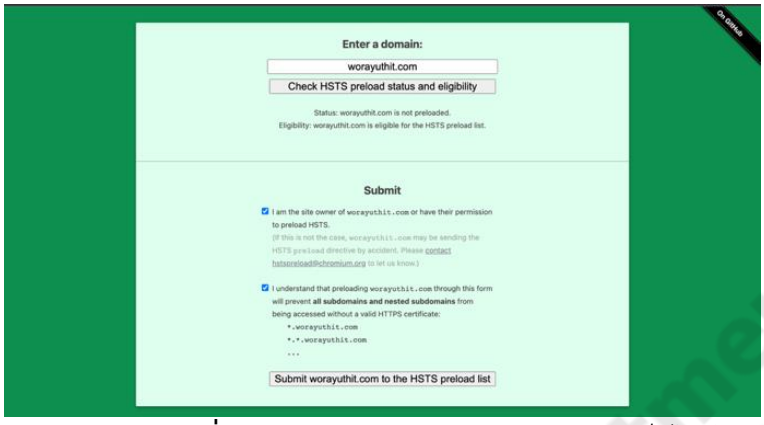


ภาพประกอบที่ 3.77 ตรวจสอบ header เว็บไซต์หลังจากกำหนดค่าใหม่

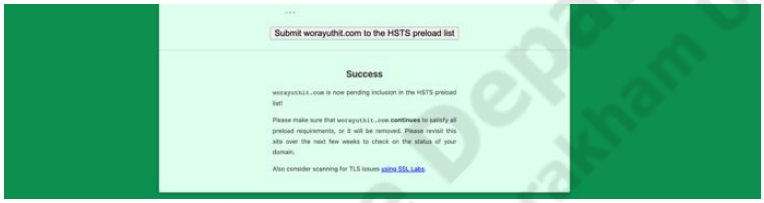
(7) ตรวจสอบสถานะการ preload ของเว็บไซต์โดยป้อน domain name

ภาพประกอบที่ 3.78 ระบบแจ้งสถานะยังไม่ได้ HSTS preload

(8) ยืนยันข้อมูลและคลิก Submit เพื่อทำการส่งคำขอ prelaod

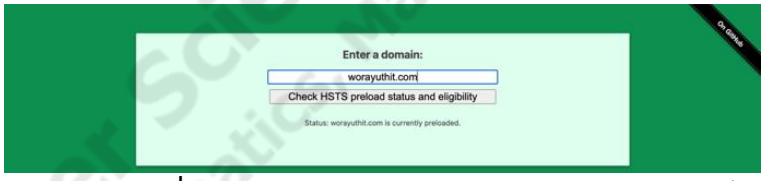


ภาพประกอบที่ 3.79 ยืนยันการขอ HSTS preload เว็บไซต์



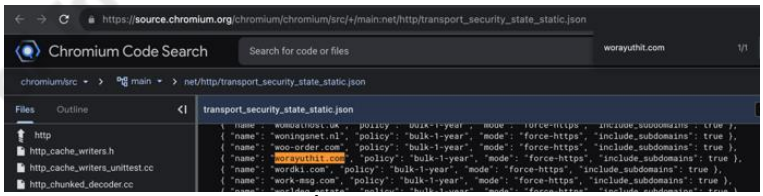
ภาพประกอบที่ 3.80 ระบบแจ้งสถานะการส่งคำขอสำเร็จ

(9) ตรวจสอบสถานะการ preload ของเว็บไซต์



ภาพประกอบที่ 3.81 ระบบแจ้งสถานะการ HSTS preload สำเร็จ

(10) ตรวจสอบ HSTS preload list



ภาพประกอบที่ 3.82 HSTS preload list

3.13 การทดสอบประสิทธิภาพเว็บไซต์ WorayuthIT

ในกระบวนการทดสอบประสิทธิภาพของเว็บไซต์ WorayuthIT การกำหนดปัจจัยและตั้งค่าเป็นสิ่งสำคัญเพื่อให้ผลการทดสอบมีความน่าเชื่อถือและสามารถสะท้อนความเป็นจริงของประสิทธิภาพของเว็บไซต์ได้อย่างถูกต้อง ปัจจัยและตั้งค่าที่สำคัญที่ต้องพิจารณาก่อนการทดสอบประสิทธิภาพเว็บไซต์ worayuthit.com จึงจะดำเนินการทดสอบ

3.13.1 การวัดประสิทธิภาพโดยไม่ใช้งานปลั๊กอิน WP Rocket

ตารางที่ 3.14 แสดงผลการวัดประสิทธิภาพเว็บไซต์ โดย Google pagespeed insights

ลำดับ	Performance	FCP	LCP	TBT	CLS	Speed Index
1	96	0.9	1.1	0	0.001	1.4
2	91	2.8	2.8	0	0.009	3.2
3	95	1	1.2	0	0.001	1.2
4	96	0.9	1.2	0	0.001	1.2
5	96	1	1.2	0	0.001	1.2
6	98	0.8	1	0	0.001	1.2
7	96	1	1.1	0	0.001	1.2
8	96	0.9	1.2	0	0.001	1.2
9	96	0.9	1.2	0	0.001	1.2
10	96	1	1.2	0	0.001	1.1
11	98	0.7	0.9	0	0.001	1.1
12	96	0.9	1.2	0	0.001	1.2
13	96	0.9	1.1	0	0.001	1.1
14	98	0.8	0.9	0	0.001	1
15	96	0.9	1.2	0	0.001	1.2
16	96	0.9	1.1	0	0.001	1.2
17	96	0.9	1.1	0	0.001	1.2
18	96	1	1.1	0	0.001	1.3
19	96	1	1.1	0	0.001	1.3
20	94	0.9	1	0	0.001	1.9
21	96	0.9	1.2	0	0.001	1.1
22	96	0.9	1.2	0	0.001	1.1
23	98	0.7	0.9	0	0.001	1
24	96	1	1.1	0	0.001	1.2
25	96	1	1.1	0	0.001	1.2
26	96	0.9	1.1	0	0.001	1.2
27	96	0.9	1.1	0	0.001	1.2
28	98	0.7	0.8	0	0.001	1.1
29	98	0.7	0.8	0	0.001	1.1
30	95	1	1.2	0	0.001	1.3

ตารางที่ 3.15 แสดงผลการวัดประสิทธิภาพเว็บไซต์ โดย GTMetrix

ลำดับ	Performance	FCP	LCP	TBT	CLS	TTI	Speed Index
1	79	1.9	2.1	0	0	2.1	2.1
2	87	1.5	1.7	3	0	1.6	1.6
3	93	1.1	1.4	22	0	1.5	1.4
4	94	1	1.3	0	0	1.2	1.3
5	88	1.4	1.6	3	0	1.6	1.6
6	94	1.1	1.3	14	0	1.3	1.3
7	91	1.3	1.5	2	0	1.4	1.4
8	91	1.2	1.5	30	0	1.4	1.5
9	92	1.2	1.4	0	0	1.4	1.4
10	93	1.2	1.3	0	0	1.3	1.3
11	92	1.2	1.4	6	0	1.4	1.4
12	94	1.1	1.3	3	0	1.3	1.3
13	85	1.4	1.8	65	0	1.8	1.8
14	90	1.3	1.5	0	0	1.5	1.5
15	84	1.6	1.8	0	0	1.9	1.8
16	90	1.2	1.6	13	0	1.5	1.6
17	92	1.2	1.4	0	0	1.3	1.4
18	91	1.2	1.5	24	0	1.5	1.5
19	94	1.1	1.3	0	0	1.2	1.2
20	79	1.8	2.1	0	0	2.1	2.1
21	93	1.1	1.4	19	0	1.5	1.4
22	91	1.2	1.6	2	0	1.3	1.5
23	85	1.7	1.9	0	0	1.8	1.8
24	90	1.2	1.7	0	0	1.4	1.5
25	88	1.5	1.5	6	0	1.6	1.7
26	92	1.3	1.3	10	0	1.4	1.4
27	85	1.6	1.7	0	0	1.7	1.8
28	92	1.2	1.4	20	0	1.3	1.4
29	94	1.1	1.3	3	0	1.3	1.3
30	88	1.4	1.7	3	0	1.6	1.6

3.13.2 สรุปผลการคำนวณ Confidence Interval โดยไม่ใช้งานปลั๊กอิน WP Rocket

ตารางที่ 3.16 แสดงผลการคำนวณ Confidence Interval Google PageSpeed

รายการ	Performance	FCP	LCP	TBT	CLS	Speed Index
Mean	96.10	0.96	1.15	0.00	0.00	1.27
Standard Error	0.25	0.07	0.06	0.00	0.00	0.07
Confidence Level (95.0%)	0.51	0.13	0.13	0.00	0.00	0.15
Highest CI (95%)	96.61	1.09	1.27	0.00	0.00	1.42
Lowest CI (95%)	95.59	0.83	1.02	0.00	0.00	1.12

ตารางที่ 3.17 แสดงผลการคำนวณ Confidence Interval GTMetrix

รายการ	Performance	FCP	LCP	TBT	CLS	TTI	Speed Index
Mean	89.70	1.31	1.54	8.27	0.00	1.54	1.53
Standard Error	0.76	0.04	0.04	2.51	0.00	0.04	0.04
Confidence Level (95.0%)	1.55	0.08	0.09	5.14	0.00	0.09	0.09
Highest CI (95%)	91.25	1.39	1.63	13.40	0.00	1.63	1.62
Lowest CI (95%)	88.15	1.23	1.46	3.13	0.00	1.46	1.44

3.13.3 การวัดประสิทธิภาพการใช้งานปลั๊กอิน WP Rocket Fully Optimized

ตารางที่ 3.18 แสดงผลการวัดประสิทธิภาพเว็บไซต์ โดย Google PageSpeed

ลำดับ	Performance	FCP	LCP	TBT	CLS	Speed Index
1	100	0.4	0.7	0	0	0.6
2	99	0.5	0.9	0	0	0.7
3	100	0.3	0.7	0	0	0.4
4	98	0.6	0.9	0	0	1.4
5	100	0.4	0.6	0	0	0.6
6	100	0.4	0.7	0	0	0.5
7	100	0.3	0.7	0	0	0.5
8	100	0.4	0.7	0	0	0.5
9	99	0.5	0.9	0	0	0.7
10	99	0.6	0.9	0	0	0.8
11	99	0.6	0.9	0	0	0.7
12	99	0.6	0.9	0	0	0.8
13	100	0.5	0.7	0	0	0.8
14	100	0.4	0.8	0	0	0.8
15	99	0.6	1	0	0	0.6
16	100	0.6	0.7	0	0	0.6
17	100	0.4	0.7	0	0	0.6
18	99	0.6	0.9	0	0	0.7
19	100	0.5	0.7	0	0	0.6
20	98	0.6	0.8	0	0	1.2
21	100	0.4	0.7	0	0	0.5
22	99	0.6	0.9	0	0	0.7
23	99	0.6	0.9	0	0	0.8
24	100	0.4	0.7	0	0	0.7
25	99	0.6	0.9	0	0	0.7
26	100	0.4	0.7	0	0	0.5
27	99	0.5	0.9	0	0	0.7
28	100	0.5	0.7	0	0	0.6
29	100	0.6	0.6	0	0	0.7
30	99	0.6	0.9	0	0	0.7

ตารางที่ 3.19 แสดงผลการวัดประสิทธิภาพเว็บไซต์ worayuthit.com โดย GTMetrix

ลำดับ	Performance	FCP	LCP	TBT	CLS	TTI	Speed Index
1	100	0.4	0.6	0	0	0.5	0.6
2	100	0.4	0.6	0	0	0.5	0.6
3	99	0.6	0.8	0	0	0.6	0.8
4	96	0.8	1.2	0	0	0.9	1.2
5	100	0.4	0.6	0	0	0.4	0.6
6	99	0.7	0.9	0	0	0.7	0.9
7	100	0.5	0.7	0	0	0.5	0.7
8	99	0.6	0.8	1	0	0.9	1
9	100	0.4	0.6	0	0	0.4	0.6
10	100	0.4	0.6	0	0	0.4	0.6
11	100	0.5	0.6	0	0	0.5	0.7
12	100	0.4	0.6	1	0	0.5	0.6
13	99	0.6	0.8	0	0	0.6	0.8
14	99	0.6	0.9	2	0	0.6	0.8
15	100	0.5	0.6	0	0	0.5	0.7
16	100	0.4	0.6	1	0	0.5	0.6
17	99	0.7	0.9	0	0	0.7	0.9
18	99	0.8	0.8	0	0	0.7	0.9
19	100	0.3	0.5	0	0	0.4	0.6
20	98	0.8	0.9	0	0	0.9	0.9
21	100	0.4	0.6	1	0	0.5	0.6
22	100	0.4	0.6	1	0	0.6	0.5
23	99	0.6	0.8	0	0	0.6	0.8
24	100	0.5	0.6	0	0	0.5	0.7
25	98	0.8	0.9	0	0	0.9	0.9
26	100	0.4	0.6	0	0	0.5	0.6
27	100	0.3	0.7	0	0	0.5	0.6
28	99	0.6	0.9	0	0	0.7	0.6
29	100	0.4	0.6	1	0	0.5	0.6
30	100	0.3	0.6	0	0	0.6	0.5

3.13.4 สรุปผลการคำนวณค่าตวามเชื่อมั่นการใช้งาน WP Rocket แบบ Fully Optimized

ตารางที่ 3.20 แสดงผลการคำนวณ Confidence Interval Google PageSpeed

รายการ	Performance	FCP	LCP	TBT	CLS	Speed Index
Mean	99.47	0.50	0.79	0.00	0.00	0.69
Standard Error	0.11	0.02	0.02	0.33	0.00	0.04
Confidence Level (95.0%)	0.23	0.04	0.04	0.00	0.00	0.07
Highest CI (95%)	99.70	0.53	0.83	0.00	0.00	0.76
Lowest CI (95%)	99.23	0.46	0.75	0.00	0.00	0.62

ตารางที่ 3.21 แสดงผลการคำนวณ Confidence Interval GTMetrix

รายการ	Performance	FCP	LCP	TBT	CLS	TTI	Speed Index
Mean	99.43	0.52	0.72	0.27	0.00	0.59	0.72
Standard Error	0.16	0.03	0.03	0.10	0.00	0.03	0.03
Confidence Level (95.0%)	0.34	0.06	0.06	0.19	0.00	0.06	0.06
Highest CI (95%)	99.77	0.58	0.78	0.46	0.00	0.64	0.78
Lowest CI (95%)	99.10	0.46	0.66	0.07	0.00	0.53	0.66