บทความวิจัย

การเสริมสร้างความมั่นคงและสมรรถภาพ ให้กับเว็บไซต์ที่มีพื้นฐานมาจากเวิร์สเพรสเป็นกรณีศึกษาเว็บวรยุทธ์ไอที

Security Enhancement and Performance Optimization for WordPress - base website,a case study of the WorayuthIT website

ยสินทร เข็มประโคน, ศิลาดล จันทร์นาหว้า, สมนึก พ่วงพรพิทักษ์
สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม

บทคัดย่อ

โครงงานปริญญานิพนธ์ฉบับนี้นำเสนอการศึกษาเกี่ยวกับการพัฒนาต้นแบบเว็บไซต์ WorayuthIT โดยการใช้งาน WordPress ซึ่งมุ่งเน้นในการให้ความรู้ผ่านบล็อกและคอร์สออนไลน์เกี่ยวกับคอมพิวเตอร์ ไอที และความรู้ด้านความปลอดภัยในโลกไซเบอร์ WorayuthIT ได้แก้ไขปัญหาเรื่องสมรรถภาพโดยการวิเคราะห์และประยุกต์การใช้ Optimizer plugin เพื่อเพิ่มประสิทธิภาพ นอกจากนี้ทำการขียนโปรแกรมและปรับแก้ฐานข้อมูลที่เกี่ยวข้องของ WordPress เพื่อทำให้หน้าเข้าสู่ระบบมีความมั่นคงปลอดภัยมากขึ้น โดยใช้เทคนิค Captcha และเทคนิค Salted Hash Password (SHP) ร่วมกับ TOTP (Time-based One-Time Password) ที่ใช้งานบนโทรศัพท์มือถือ ซึ่งสามารถใช้งานร่วมกับ Google Authenticator และ Authy ได้ เพื่อเพิ่มระดับความปลอดภัยของเว็บไซต์นี้ได้อย่างเหมาะสมและมีประสิทธิภาพ

คำสำคัญ: WordPress, Worayuthit, plugins, login

1. บทนำ

เวิร์ดเพรสส์ (WordPress) คือ โปรแกรมสำเร็จรูปสำหรับสร้าง และจัดการเว็บไซต์ประเภท CMS (Contents Management System) เขียนด้วยภาษา PHP และใช้ระบบจัดการฐานข้อมูล MySQL โดยมีส่วนประกอบหลัก คือ เวิร์ดเพรสส์ คอร์ (WordPress Core) ธีม (Theme) และปลั๊กอิน (Plugin) ซึ่งได้รับความนิยมและมีชื่อเสียงมากในปัจจุบัน เพราะผู้ใช้งานที่ต้องการสร้างเว็บไซต์ ไม่จำเป็นต้องเรียนรู้ภาษาและวิธีการเขียนโค้ดในการสร้างเว็บไซต์ เนื่องจาก WordPress มีระบบควบคุมจัดการเนื้อหาต่าง ๆ ในเว็บไซต์ เรียกว่า ระบบหลังบ้าน สำหรับจัดการข้อมูลเว็บไซต์บนอินเทอร์เน็ต จึงง่ายต่อการเรียนรู้และใช้งาน สามารถสร้างเว็บไซต์ได้อย่างรวดเร็วและสวยงาม จึงเป็นที่นิยมอย่างมากในปัจจุบัน

แต่การนำ WordPress มาใช้งานมักจะมีปัญหาความล่าช้า เมื่อเทียบกับการเขียนโปรแกรมด้วยโปรแกรมเมอร์มืออาชีพ เนื่องจาก WordPress มาพร้อมกับฟังก์ชันที่หลากหลายชนิด และครอบคลุม ซึ่งบางส่วนของเว็บไซต์อาจไม่ได้ใช้งาน จึงอาจสร้างความล่าช้าได้ นอกจากนี้ด้านความมั่นคงปลอดภัย WordPress มักมีข่าวถูก Hack ให้เห็นอยู่บ่อยครั้ง เช่น ในวันที่ 15 กันยายน 2565 ที่ผ่านมา มีเว็บไซต์ที่ใช้งาน WordPress มากกว่า 2 แสนเว็บไซต์ ถูก Hacker โจมตี [1] สาเหตุ

เนื่องจาก WordPress เป็น open-source web blog ที่เป็นที่นิยม จึงเป็นเป้าหมายประสงค์ในการโจมตี อีกทั้งสามารถดูโค้ดเพื่อหาช่องโหว่ จึงเป็นเรื่องสำคัญเพื่อหาวิธีการเพิ่มประสิทธิภาพให้ WordPress ใช้งานให้เร็วขึ้นและเพิ่มความมั่นคง เพื่อป้องกันการถูกโจมตี

เว็บไซต์วรยุทธ์ไอที (WorayuthIT) เป็นเว็บไซต์สำหรับเผยแพร่ข่าวสาร ความรู้ต่าง ๆ ด้านไอที และมีบริการคอร์สเรียนออนไลน์ที่สามารถสมัครเรียนได้ โดยเว็บวรยุทธ์ไอทีเป็นโครงการความร่วมมือระหว่างกลุ่มวิจัย ISAN (Information Security and Advanced Network) มหาวิทยาลัยมหาสารคาม และ Business Partner ภายนอก ที่มีแผนจะนำ WordPress มาใช้เป็นฐานในการพัฒนา จึงมีความจำเป็นในการแก้ปัญหาด้านสมรรถภาพและด้านความมั่นคงของ WordPress

ข้อเสนอโครงงานวิทยานิพนธ์นี้ มีวัตถุประสงค์เพื่อพัฒนาต้นแบบเว็บไซต์วรยุทธ์ไอที โดยใช้งาน WordPress และแก้ปัญหาในเรื่องของสมรรถภาพ (Performance Optimization) โดยอาศัย Optimizer plugin และความมั่นคง (Security Enhancement) โดยการปรับโปรแกรมหน้า Login โดยใช้เทคนิค Captcha และเทคนิค Salted Hash Password ร่วมกับ TOTP (Time-based One-Time Password) และสามารถป้องกันการโจมตีโดยการฝัง key-logger client script

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 Weblog or Blog

Blog มาจากศัพท์คำเต็มว่า WeBlog คือ เว็บไซต์ประเภทหนึ่ง ที่เจ้าของ หรือ Blogger สามารถบันทึกเรื่องราวของตนเองลงในเว็บได้ นอกจากนี้ Blog ยังเป็นพื้นที่ให้ Blogger โพสต์ข้อมูล หรือใส่ความรู้ ประสบการณ์ อาจเป็นเรื่องส่วนตัว การนำเสนอความคิดและประสบการณ์ของบล็อกเกอร์ หรืออาจเน้นข่าวสารมากกว่า ครอบคลุมเหตุการณ์และประเด็นปัจจุบัน นอกจากนี้ยังมีบล็อกเฉพาะจำนวนมากที่เน้นหัวข้อเฉพาะ เช่น การเมือง เทคโนโลยี แฟชั่น อาหาร หรือเพื่อเป็นวิทยาทานให้คนอื่น ๆ ซึ่งข้อแตกต่างของบล็อกกับเว็บไซต์ทั่วไป คือ บล็อกจะเปิดให้ผู้เข้ามาอ่านข้อมูล สามารถแสดงความคิดเห็นต่อท้ายข้อความที่เจ้าของบล็อกเป็นคนเขียน ซึ่งทำให้ผู้เขียนสามารถได้ผลตอบกลับโดยทันที ในช่วงไม่กี่ปีที่ผ่านมา การเขียนบล็อกกลายเป็นวิธียอดนิยมสำหรับบุคคลและองค์กรในการแบ่งปันข้อมูลและมีส่วนร่วมกับผู้ชมทางออนไลน์ บล็อกจำนวนมากสร้างรายได้จากการโฆษณาหรือการสนับสนุน

2.2 WordPress

WordPress เป็นระบบจัดการเนื้อหายอดนิยม (CMS) ที่ใช้ในการสร้างและจัดการเว็บไซต์ เป็นซอฟต์แวร์ Open sourse ที่ให้บริการฟรีและสามารถปรับแต่งให้ตรงกับความต้องการของเว็บไซต์ที่หลากหลาย รวมถึงบล็อก ไซต์อีคอมเมิร์ซ และอื่น ๆ ข้อดีบางประการของการใช้ WordPress ได้แก่ ใช้งานง่าย มีอินเทอร์เฟสที่ใช้งานง่ายซึ่งทำให้ผู้ใช้ที่มีประสบการณ์ในการเขียนโค้ดน้อยหรือไม่มีเลยสามารถสร้างและจัดการเว็บไซต์ได้ง่าย การปรับแต่ง มีชุมชนขนาดใหญ่ของนักพัฒนาที่สร้างธีมและปลั๊กอินที่หลากหลายซึ่งสามารถใช้

เพื่อปรับแต่งรูปลักษณ์และการทำงานของเว็บไซต์ และมีฐานผู้ใช้ขนาดใหญ่ ซึ่งหมายความว่ามีการสนับสนุนมากมายจากผู้ใช้รายอื่นและนักพัฒนา ข้อเสียบางประการของการใช้ WordPress ได้แก่ ความปลอดภัย ในฐานะ CMS ยอดนิยม WordPress เป็นเป้าหมายของ Hacker แม้ว่าจะมีมาตรการในการรักษาความปลอดภัยเว็บไซต์ แต่ก็ยังมีความเสี่ยงต่อการละเมิดความปลอดภัย ประสิทธิภาพเว็บไซต์สามารถโหลดได้ช้า โดยเฉพาะอย่างยิ่งหากไม่ได้รับการเพิ่มประสิทธิภาพอย่างเหมาะสมหรือใช้งานปลั๊กอินจำนวนมาก ความยืดหยุ่นที่จำกัด แม้ว่า WordPress จะปรับแต่งได้สูง แต่ก็มีข้อจำกัดในขอบเขตที่สามารถแก้ไขได้ หากเว็บไซต์ต้องการการออกแบบหรือฟังก์ชันเฉพาะเจาะจง การใช้ WordPress อาจทำได้ยากขึ้น

โดยสรุป WordPress เป็น CMS ที่ได้รับความนิยมและเป็นมิตรกับผู้ใช้ ซึ่งเหมาะสำหรับเว็บไซต์ที่หลากหลาย แต่มีข้อจำกัดบางประการในแง่ของความปลอดภัยและความยืดหยุ่น

2.3 Hash

Hash เป็นฟังก์ชันทางคณิตศาสตร์ที่รับข้อมูล input และสร้าง output ขนาดคงที่ ซึ่งเรียกว่าค่าแฮชหรือรหัสแฮช ข้อมูล input มีขนาดใดก็ได้ แต่ output จะมีขนาดคงที่เสมอ การใช้ฟังก์ชันแฮช คือ การสร้างโครงสร้างข้อมูลที่เรียกว่าตารางแฮช ซึ่งใช้ในการจัดเก็บและดึงข้อมูลอย่างมีประสิทธิภาพ ในตารางแฮช โดยข้อมูลจะถูกจัดเก็บไว้ในอาร์เรย์ และข้อมูลแต่ละส่วนจะเชื่อมโยงกับคีย์เฉพาะ ในการดึงข้อมูล คีย์จะถูกส่งผ่านฟังก์ชันแฮชเพื่อสร้างค่าแฮช ซึ่งจากนั้นจะใช้ในการจัดทำดัชนีในอาร์เรย์และดึงข้อมูลที่เกี่ยวข้อง ฟังก์ชันแฮชมีคุณสมบัติที่สำคัญหลายอย่างที่ทำให้มีประโยชน์สำหรับการใช้งานที่หลากหลาย คุณสมบัติที่สำคัญประการหนึ่งคือพวกมันถูกกำหนดขึ้น ซึ่งหมายความว่าอินพุตเดียวกันจะให้ผลลัพธ์เดียวกันเสมอ สิ่งนี้ช่วยให้สามารถจัดเก็บและดึงข้อมูลที่สามารถคาดเดาได้และเชื่อถือได้ คุณสมบัติที่สำคัญของฟังก์ชันแฮช คือ ค่อนข้างง่ายในการคำนวณ แต่เป็นไปไม่ได้ในการคำนวณเพื่อย้อนกลับกระบวนการ และกำหนดข้อมูล input จากค่าแฮช ทำให้ฟังก์ชันแฮชมีประโยชน์สำหรับการจัดเก็บข้อมูลที่ละเอียดอ่อน เช่น รหัสผ่าน เนื่องจากสามารถจัดเก็บเป็นแฮชแทนที่จะเก็บเป็นข้อความธรรมดามีฟังก์ชันแฮชประเภทต่าง ๆ มากมาย แต่ละประเภทมีลักษณะเฉพาะและการใช้งานที่แตกต่างกัน

รหัสผ่านแบบแฮชเป็นวิธีที่ปลอดภัยในการจัดเก็บรหัสผ่านในฐานข้อมูล เนื่องจากทำให้มั่นใจได้ว่ารหัสผ่านเดิมจะไม่สามารถเข้าถึงได้หรือกำหนดได้ง่าย

2.4 Captcha

CAPTCHA “Completely Automated Public Turing test to tell Computers and Humans Apart” เป็นการทดสอบการตอบสนองความท้าทายประเภทหนึ่งที่ใช้ในการคำนวณเพื่อตรวจสอบว่าผู้ใช้เป็นมนุษย์หรือไม่ มักใช้เพื่อป้องกันเว็บไซต์จากบอทและโปรแกรมอัตโนมัติที่สามารถสร้างบัญชีปลอม

เว็บไซต์สแปม หรือทำกิจกรรมที่เป็นอันตรายอื่น ๆ โดยทั่วไป CAPTCHA จะประกอบด้วยภาพตัวอักษรและตัวเลขที่บิดเบี้ยว ซึ่งมนุษย์สามารถอ่านได้ง่าย แต่โปรแกรมคอมพิวเตอร์ไม่สามารถทำได้ ผู้ใช้จะถูกขอให้พิมพ์ตัวอักษรและตัวเลขที่เห็นในภาพลงในช่องแบบฟอร์มเพื่อพิสูจน์ว่าเป็นมนุษย์ สิ่งนี้ช่วยป้องกันไม่ให้โปรแกรมอัตโนมัติเข้าถึงเว็บไซต์หรือดำเนินการบางอย่างกับเว็บไซต์ CAPTCHA เพื่อป้องกันแบบฟอร์มออนไลน์ เช่น หน้าเข้าสู่ระบบ ไม่ให้ส่งโดยโปรแกรมอัตโนมัติ ใช้เพื่อป้องกันเว็บไซต์จากการถูกสแปมโดยบอทและเพื่อป้องกันการเข้าถึงพื้นที่บางส่วนของเว็บไซต์โดยไม่ได้รับอนุญาต

วัตถุประสงค์ของ CAPTCHA คือ เพื่อให้แน่ใจว่าผู้ใช้ที่พยายามเข้าสู่ระบบเป็นบุคคลจริง ไม่ใช่บอทหรือสคริปต์อัตโนมัติ ซึ่งจะช่วยป้องกันเว็บไซต์จากสแปมและการละเมิด และสามารถปรับปรุงความปลอดภัยโดยรวมของเว็บไซต์ได้

2.5 Salted Hash Password

Salted Hash Password คือ รหัสผ่านแบบแฮชประเภทหนึ่งที่มีชั้นความปลอดภัยเพิ่มเติมที่เรียกว่า Salt ซึ่ง Salt คือ สตริงอักขระแบบสุ่มที่สร้างขึ้นและร่วมกับรหัสผ่านก่อนที่จะแฮช ซึ่งจะทำให้ผู้โจมตีถอดรหัสรหัสผ่านได้ยากขึ้น ค่า Salt จะถูกเพิ่มเข้าไปในรหัสผ่านเพื่อทำให้ผู้โจมตีถอดรหัสรหัสผ่านได้ยากขึ้น แม้ว่าพวก Hacker จะเข้าถึงฐานข้อมูลรหัสผ่านที่แฮชได้ เพราะผู้โจมตีต้องทราบค่า Salt ถึงจะสามารถถอดรหัสแฮชได้อย่างถูกต้องการใช้ Salted Hash Password สิ่งสำคัญคือ ต้องใช้ฟังก์ชันแฮชที่แข็งแกร่งและปลอดภัย

2.6 TOTP

TOTP ย่อมาจาก Time-based One-Time Password เป็นรหัสผ่านแบบใช้ครั้งเดียว (OTP) ประเภทหนึ่ง ที่สร้างขึ้นตามเวลาปัจจุบันและรหัสลับที่ใช้ร่วมกัน โดยทั่วไปจะใช้ TOTP เป็นชั้นความปลอดภัยเพิ่มเติมสำหรับบัญชีออนไลน์ เมื่อผู้ใช้ต้องการเข้าสู่ระบบบัญชีของตน นอกเหนือจากชื่อผู้ใช้และรหัสผ่าน TOTP สร้างขึ้นโดยอุปกรณ์ของผู้ใช้ (เช่น สมาร์ทโฟน) โดยใช้แอพหรือ โปรแกรมที่สามารถเข้าถึงรหัสลับที่ใช้ร่วมกัน จากนั้น ผู้ใช้ป้อน TOTP ลงในข้อความแจ้งการเข้าสู่ระบบและหากถูกต้อง ผู้ใช้จะได้รับสิทธิ์เข้าถึงบัญชีของตน ข้อดีอย่างหนึ่งของ TOTP คือให้ระดับความปลอดภัยพิเศษโดยที่ผู้ใช้ไม่ต้องจำรหัสผ่านเพิ่มเติม นอกจากนี้ ยังมีความปลอดภัยมากกว่า OTP ประเภทอื่น เช่น รหัสที่ส่งทาง SMS เนื่องจากผู้โจมตีไม่สามารถดักฟังหรือคาดเดาได้

โดยสรุป TOTP เป็นรหัสผ่านแบบใช้ครั้งเดียวชนิดหนึ่งที่สร้างขึ้นตามเวลาปัจจุบันและรหัสลับที่ใช้ร่วมกัน มักใช้เป็นชั้นความปลอดภัยเพิ่มเติมสำหรับบัญชีออนไลน์

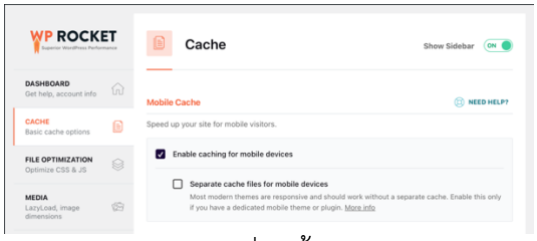
3. ขั้นตอนการดำเนินงาน

3.1 เพิ่มประสิทธิภาพ (Performance Optimization)

WP Rocket คือ ปลั๊กอินสำหรับใช้งานบน WordPress ที่ช่วยปรับปรุงประสิทธิภาพการโหลดของเว็บไซต์ โดยลดเวลาโหลดหน้าเว็บ ด้วยการใช้งานแคชและการปรับแต่งไฟล์เพื่อเร่งความเร็วในการเข้าถึงข้อมูล นอกจากนี้

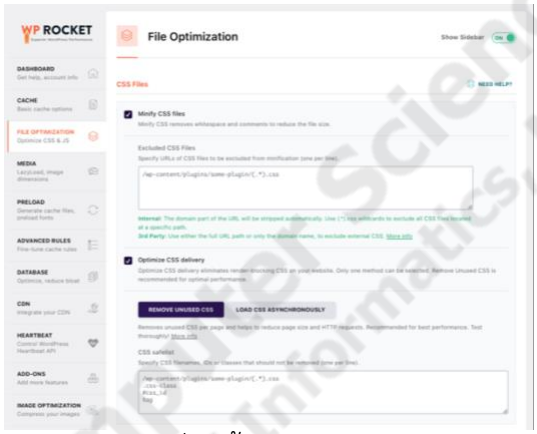
ยังมีคุณสมบัติอื่น ๆ ที่ช่วยให้เว็บไซต์ทำงานได้มีประสิทธิภาพสูงขึ้น โดยการใช้งาน WP Rocket มีดังนี้

1) เปิดใช้ Enable caching for mobile devices



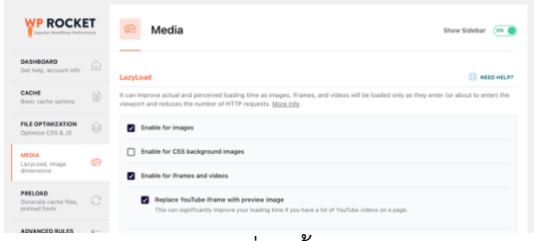
ภาพประกอบที่ 1 ตั้งค่า Cache

2) เปิดใช้ Minify CSS files, Optimize CSS delivery, Minify JavaScript files และ Load JavaScript deffered



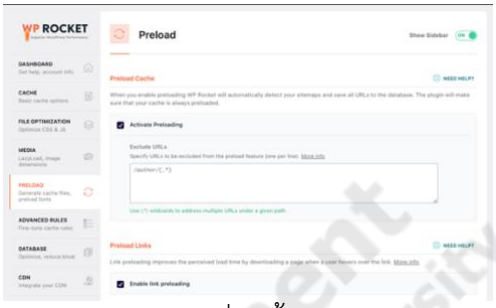
ภาพประกอบที่ 2 ตั้งค่า File Optimization

3) เปิดใช้ Enable for images, Enable for iframes and videos และเปิดใช้ Replace Youtube iframe with preview image



ภาพประกอบที่ 3 ตั้งค่า Media

4) เปิดใช้ Activate Preloading และ Enable link preloading



ภาพประกอบที่ 4 ตั้งค่า Preload

3.2 เครื่องมือวัดประสิทธิภาพเว็บไซต์

Google PageSpeed Insights เป็นบริการฟรีจาก Google ที่ให้คำแนะนำและวิเคราะห์เว็บไซต์เพื่อปรับปรุงประสิทธิภาพในการโหลดหน้าเว็บและประสบการณ์ผู้ใช้ของเว็บไซต์นั้น ๆ บริการนี้มีเป้าหมายเพื่อช่วยให้เว็บไซต์โหลดได้เร็วขึ้นและทำงานได้ดีในทุก ๆ อุปกรณ์และเบราว์เซอร์ที่ผู้ใช้ใช้งานอยู่

Google PageSpeed Insights

ภาพประกอบที่ 5 Google PageSpeed Insights logo

โดยคำแนะนำนี้อาจรวมถึงการลดขนาดของไฟล์ภาพ การลดการร้องขอที่เว็บไซต์ต้องทำไปยังเซิร์ฟเวอร์ และการปรับปรุงการโหลด เป้าหมายของ Google PageSpeed คือการทำให้เว็บไซต์ทั่วไปโหลดได้เร็วขึ้นและมีประสิทธิภาพในทุก ๆ สถานการณ์การใช้งานบนอุปกรณ์ต่าง ๆ ที่ผู้ใช้ใช้งานอยู่

GTMetrix เป็นเครื่องมือที่มีมาตรฐานสูงในการวัดและประเมินประสิทธิภาพของเว็บไซต์ โดยให้ข้อมูลที่ถูกต้องและเชื่อถือได้เกี่ยวกับความเร็วและประสิทธิภาพในการโหลดหน้าเว็บ

ของเว็บไซต์นั้น ๆ GTmetrix ช่วยให้เจ้าของเว็บไซต์และนักพัฒนาเว็บได้ข้อมูลที่ทันสมัยและแม่นยำเพื่อทำการปรับปรุงเว็บไซต์ของพวกเขาให้มีประสิทธิภาพในการโหลดที่ดีที่สุด

ภาพประกอบที่ 6 GTMetrix logo

รายงานที่ GTmetrix ให้มีข้อมูลจาก Google PageSpeed Insights Lighthouse และ YSlow ทำให้เป็นเครื่องมือที่ครอบคลุมและเป็นประโยชน์ต่อการพัฒนาเว็บไซต์ ด้วยคะแนนและเกรดที่ได้จาก Gtmetrix นักพัฒนาสามารถปรับปรุงประสิทธิภาพของเว็บไซต์ให้มีประสิทธิภาพสูงสุดได้อย่างมีประสิทธิภาพและมีประสิทธิภาพในทุก ๆ ด้านของการโหลด

3.2 เพิ่มความมั่นคงปลอดภัย (Security Enhancement)

ในยุคของโลกดิจิทัลที่มีข้อมูลมากมายและการสื่อสารออนไลน์มีความสำคัญ การบริหารจัดการเซิร์ฟเวอร์และหน้าเว็บจึงเป็นสิ่งสำคัญที่ไม่ควรมองข้าม ขั้นตอนการบริหารจัดการ Server Web page เบื้องต้นมีดังนี้

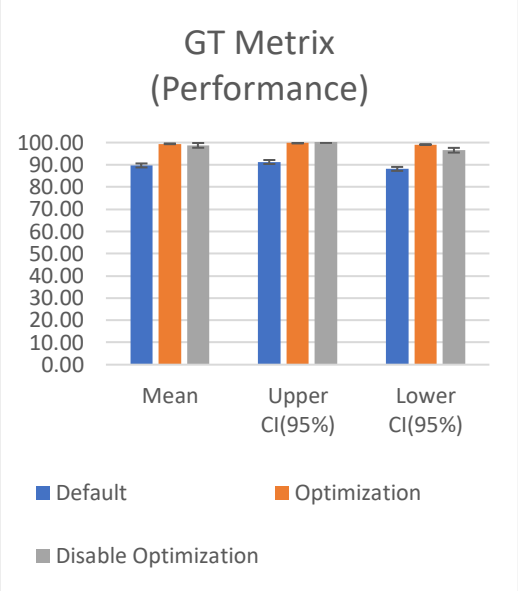
- จด Domain name โดยผู้ให้บริการ hostatom
- ออก SSL Certificate Let's Encrypt
- ตั้งค่า Configuration https
- ตั้งค่า HSTS preload configuration

การบูรณาการหน้า login

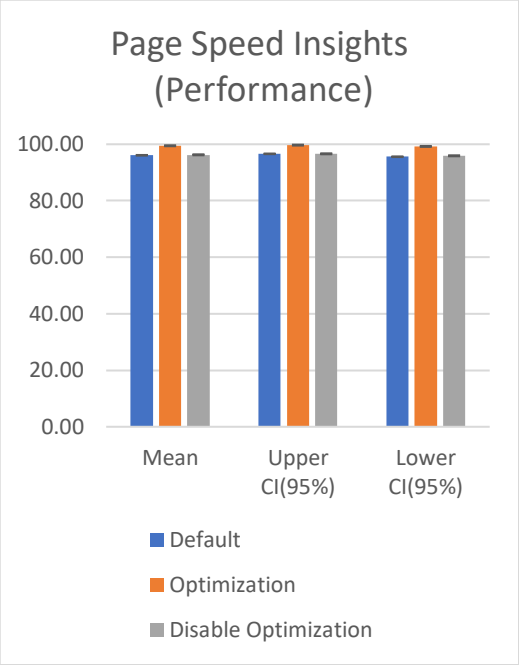
- ปรับหน้าเข้าสู่ระบบ ฐานข้อมูลและส่วนประกอบอื่น ๆ ให้สามารถใช้งาน Captcha และใช้งาน Salted Hash Password ร่วมกับ Mobile TOTP
- ทำการ hashed รหัสผ่านที่ส่งด้วย Salted Hash Password โดยใช้ Salt เป็นเลข TOTP (Time-based One-Time Password) ที่ generate จาก TOTP Mobile Application เช่น Google Authenticator, Authy
- สร้างหน้าสำหรับเปิดใช้งาน TOTP 2FA เพื่อให้ผู้ใช้ใช้งาน Salted Hash Password จาก Mobile Application

4.การทดสอบระบบ

การทดสอบระบบ (Testing System) เป็นการทดสอบกระบวนการการทำงานของระบบเพื่อทำการทดสอบการใช้งานเว็บไซต์ ซึ่งได้ทำการพัฒนาจนเสร็จสมบูรณ์ เพื่อให้ทราบถึง กระบวนการทำงานของระบบว่าสามารถทำงานในแต่ละฟังก์ชันได้อย่างถูกต้อง และให้ผลลัพธ์ตามที่ ต้องการหรือไม่ โดยมีการนำเข้าข้อมูลไปยังระบบเพื่อให้ทำงานและแสดงผลลัพธ์ออกมาโดยใช้ฟังก์ชันในส่วนต่างๆ



ภาพประกอบที่ 7 ผลสรุปการหาค่า Confidence Interval Performance



ภาพประกอบที่ 8 ผลสรุปการหาค่า Confidence Interval ของ Performance

5. สรุปและอภิปรายผลการทดลอง

5.1 สรุปผลและอภิปรายผล

ปัจจุบัน WordPress เป็นเครื่องมือที่ใช้สร้างและบริหารจัดการเว็บไซต์อย่างมีประสิทธิภาพโดย ไม่ต้องมีความเชี่ยวชาญในการเขียนโค้ดเว็บ WordPress เน้นการจัดการเนื้อหาในรูปแบบของบทความและมีระบบบล็อกที่ช่วยให้ผู้ใช้สร้างและแก้ไขเนื้อหาได้อย่างง่าย ระบบนี้เน้นความสะดวกสบายและมีอินเตอร์เฟซการใช้งานที่เข้าใจง่าย WordPress มีคุณสมบัติที่หลากหลายและปลั๊กอิน (plugins) ที่เพิ่มความสามารถเพิ่มเติม ทำให้สามารถปรับแต่งรูปแบบและฟังก์ชันของเว็บไซต์ตามความต้องการ เช่น สร้างเว็บบล็อก ร้านค้าออนไลน์ เว็บไซต์ข่าว หรือเว็บไซต์ธุรกิจในหลายแวดวง รวมทั้งมีชุมชนในระดับโลกที่ใหญ่ที่ให้การสนับสนุนและทรัพยากรการเรียนรู้มากมายสำหรับผู้ใช้งานและผู้พัฒนา ทำให้ WordPress เป็นหนึ่งใน CMS ที่ได้รับความนิยมอันดับสูงในการสร้างและบริหารจัดการเว็บไซต์ในโลกขณะนี้

เนื่องจาก WordPress เป็นหนึ่งใน CMS ที่ได้รับความนิยมและรูปแบบของเว็บไซต์ที่ใช้ WordPress มากมายเลยทำให้เป็นเป้าหมายของผู้ไม่ประสงค์ดี เพื่อป้องกันการโจมตีที่เป็นไปได้ ผู้ดูแลระบบและผู้ใช้งาน WordPress ควรทำการรักษาระบบประกอบด้วยการอัปเดตซอฟต์แวร์ WordPress และปลั๊กอินให้เป็นเวอร์ชันล่าสุด ใช้รหัสผ่านที่แข็งแรง ดูแลและตรวจสอบการติดตั้งของปลั๊กอินและธีม จากแหล่งที่น่าเชื่อถือ และใช้ปลั๊กอินความปลอดภัยและอุปกรณ์อื่น ๆ เพื่อเสริมความปลอดภัยของระบบ โดยเว็บไซต์ WorayuthIT จะทำงานเพิ่มประสิทธิภาพความมั่นคงปลอดภัยของให้กับหน้าเข้าสู่ระบบ เพื่อป้องกันผู้ไม่ประสงค์ดี ที่จะมาโจมตีเว็บไซต์

เพื่อเสริมสร้างความมั่นคง ในโครงงานปริญญานิพนธ์นี้ได้เสนอการตั้งค่า https และ HSTS configuration แบบ preload เพื่อป้องกันการดักรหัสผ่านและการโจมตีด้วย SSL Strip ดังได้นำเสนอในรายงาน อีกทั้งโครงงานนี้ยังได้ทำการแก้ไข ออกแบบและพัฒนา ส่วนฐานข้อมูลที่เกี่ยวกับ การ login, หน้า login, หน้าการ reset รหัสผ่าน และพัฒนาหน้า page และโปรแกรมอื่น ๆ เพิ่มเติม โดยใช้ Salted-hash Password แทนระบบรหัสผ่านเดิมของ WordPress ที่อาจถูก brute-force attack หรือ rainbow crack attack ได้ ทั้งนี้ได้เลือกใช้ hash function เป็น SHA-2 ขนาด 512 บิต ซึ่งเป็น hash standard ล่าสุดที่เป็นที่ยอมรับ

และได้กำหนดใช้ salt จาก Mobile OTP ตามมาตรฐาน Time-based one-time password (TOTP) RFC 6238 โดย salt จะถูก generate จาก Google Authenticator ทำให้การดักจับค่า salt ทางเครือข่ายเป็นไปไม่ได้และค่า salt ยังเปลี่ยนแปลงทุก 30 วินาที หากมีความพยายามในการเดา หรือ brute-force salt เพื่อนำไป rainbow crack SHP ของระบบนี้ต่อ ก็จะต้องใช้ computation power มหาศาล เพื่อให้ทันใน 30 วินาที ผลจากการใช้ salt จาก M-OTP ยังเสริมความมั่นคงการพิสูจน์ความเป็นตัวจริง (Authentication) ให้กลายเป็น Two Factor Authentication ด้วย คือต้องรู้รหัสผ่าน และมี smartphone ที่มี Google authenticator ที่ถือครอง Salt Seed แต่ละ username การโปรแกรมในส่วนของ login page ที่เสริม SHP ที่เกี่ยวข้องทำโดย JavaScript ซึ่งเป็น client scripts ทำให้รหัสผ่านที่เป็น cleartext ไม่เคยถูกปล่อยออกผ่านเครือข่าย แต่จะโดน salted hash ก่อน ทำให้หากมีการโจมตีโดย hackers ทะลุผ่าน https มาได้ และทำการ sniff รหัสผ่านก็จะต้องเจอด่าน SHP ที่กล่าวไว้ก่อนหน้านี้ ในด้านของการ flood หน้า login ด้วย Bot Script ผ่านที่หน้า login ก็ถูกสะกัดกั้นได้ โดยโครงงานนี้ได้พัฒนาเพื่อเรียกใช้ Google reCAPTCHA API เพื่อทำการสะกัดไม่ให้ Bot Script ทำงานได้ เพราะต้องพิสูจน์ความเป็นมนุษย์ผ่าน CAPTCHA นอกจากนี้ ทางด้าน Security ที่เพิ่มจากข้อเสนอเริ่มต้น โครงงานนี้ยังประสบความสำเร็จในการพัฒนา เพื่อใช้ on-screen keyboard module ในการกรอกรหัสผ่าน แทนการกด keyboard เพื่อป้องกัน hacker โจมตีโดยการฝัง key-logger client script แล้วดักจับ keystroke ที่ผู้ใช้กรอก ณ หน้า login อีกด้วย (ซึ่งปัจจุบัน ปรากฏเทคนิคการโจมตีด้วย key-logger client scirpt ดังกล่าว ด้วย bettercap Java Scripts ที่แพร่หลายบน internet)

ด้านการเพิ่มประสิทธิภาพของ WordPress โครงงานนี้ได้เลือกใช้ Plugin ชื่อ WP Rocket ที่ช่วยเสริมประสิทธิภาพได้ โดยการกำหนดค่าต่าง ๆ ทำให้เว็บซต์ที่ได้มีประสิทธิภาพมากขึ้น การวัดประสิทธิภาพที่เพิ่มขึ้นทำโดย ใช้คะแนน (Score) จาก GTmetrix และ Google PageSpeed Insights ผลลัพธ์ที่ได้นี้แสดงให้เห็นถึงความต่างกันในการปรับปรุงประสิทธิภาพของเว็บไซต์ เมื่อเว็บไซต์ได้รับ การปรับปรุง Fully Optimized ตามที่แสดงในกราฟ คะแนนที่ได้จาก GTmetrix และ Google PageSpeed Insights จะมีค่าสูงมากขึ้น หมายถึงความปรับปรุงที่เข้ามาในการทำให้เว็บไซต์ทำงานอย่างมีประสิทธิภาพสูง หากไม่มีการปรับปรุงหรือปิดการใช้งานบางส่วนของเว็บไซต์ (Disabled) คะแนนจะต่ำลงและแสดงถึงปัญหาในประสิทธิภาพของเว็บไซต์ นี้อาจมีทั้งการโหลดหน้าเว็บช้าหรือปัญหาอื่น ๆ ที่ส่งผลให้ผู้ใช้ประสบปัญหาในการเข้าถึงเนื้อหา เมื่อเว็บไซต์ได้รับการปรับปรุงบางส่วนคะแนนอาจสูงกว่าระดับ Disabled แต่ยังไม่สูงเท่ากับ Fully Optimize นี้แสดงว่ามีการปรับปรุงบางส่วนเพื่อเพิ่มประสิทธิภาพ แต่ยังมีข้อบกพร่องที่ทำให้เว็บไซต์ทำงานไม่อย่างเต็มที่ ในกรณีนี้

คะแนนอาจสูงกว่า Disabled ใน GTmetrix แต่อาจต่ำกว่า Fully Optimized ใน Google PageSpeed

การใช้งานแบบ Fully Optimized จะทำให้เว็บไซต์ได้รับคะแนนสูงสุดในเรื่องของประสิทธิภาพ และ Partially Optimized จะมีคะแนนที่สูงกว่า Disabled แต่ยังไม่สูงเท่ากับ Fully Optimized บ่งบอกถึงความสำคัญของการปรับปรุงเว็บไซต์เพื่อให้ผู้ใช้ได้รับประสิทธิภาพที่ดีและบริการที่มีประสิทธิภาพ ผลการวิจัยนี้ช่วยให้เห็นถึงความสำคัญของการปรับปรุงและเพิ่มประสิทธิภาพของเว็บไซต์

5.2 ปัญหาและอุปสรรคในการดำเนินงาน

1) การไม่คุ้นเคยกับระบบ WordPress ในระดับที่เพียงพอต้องใช้เวลาในการศึกษาเรียนรู้เกี่ยวกับโครงสร้างและฟังก์ชันของ WordPress ในการทำให้เว็บไซต์ทำงานได้ตามที่เราต้องการ

2) การเลือกใช้และปรับแต่งปลั๊กอินให้เข้ากับความต้องการของเว็บไซต์นั้นเป็นอีกทั้งปัญหาที่เราต้องเผชิญ บางครั้งปลั๊กอินที่ต้องการใช้งานอาจมีข้อจำกัดหรือข้อกำหนดทางเทคนิคที่ต้องการการกำหนดค่าและปรับแต่งเพิ่มเติม ซึ่งอาจทำให้กระบวนการนี้ซับซ้อนขึ้น

3) บางครั้งเมื่อเราต้องการปรับแต่งหน้าเว็บหรือเพิ่มฟังก์ชันใหม่ ธีมหรือโค้ดที่เรานำเข้าอาจไม่เข้ากันหรือขัดแย้งกัน การปรับแต่งที่ไม่ถูกต้องอาจทำให้หน้าเว็บแสดงผลผิดพลาดหรือการทำงานขัดข้อง

5.3 ข้อเสนอแนะ

หลังจากปรับปรุงและเสริมความปลอดภัยของเว็บไซต์ WordPress ในโครงงานนี้ เรามีมุมมองเกี่ยวกับการอัปเดตและการปรับปรุงที่ควรนำเข้าไว้ในการพัฒนาของเว็บไซต์ worayuthit.com ในอนาคตของ WordPress เราเข้าใจว่า WordPress เป็นแพลตฟอร์มที่พัฒนาอย่างต่อเนื่องและมีการอัปเดต Version อย่างสม่ำเสมอเพื่อปรับปรุงแก้ไขจุดอ่อนและเพิ่มความปลอดภัยให้กับผู้ใช้ แต่ด้วยความก้าวหน้านี้ Code ที่เราได้ทำการเสริมเข้าไปใน WordPress ในโครงงานนี้ ไม่ได้รับการอัปเดตไปด้วยเมื่อ WordPress ปล่อย Version ใหม่ออกมา

ด้วยเหตุนี้ เราแนะนำให้ทำการวางแผนสำหรับการพัฒนาปลั๊กอินที่สามารถใช้งานบน WordPress โดยที่สามารถปรับปรุงและทำการอัปเดตตาม Version ของ WordPress ใหม่ ๆ ที่ถูกปล่อยออกมา โดยให้ความสำคัญกับการพัฒนาและปรับปรุงเว็บไซต์ของเราให้เข้ากับเทคโนโลยีและคุณลักษณะล่าสุดของ WordPress

6. เอกสารอ้างอิง

1. WordPress Hacked, Retieved 29 September 2022 from https:// short url.asia/DyT5G/
2. WP Rocket, Retieved 29 September 2022 from https://wp-rocket.me
3. GTmetrix, Retieved 29 September 2022 from https://gtmetrix.com
4. PageSpeed Insights, Retieved 29 September 2022 from https:// www.semrush.com

5. Weblog, Retieved 29 September 2022 from https://www.mindphp.com
6. WordPress, Retieved 29 September 2022 from https://wordpress.com
7. Hash, Retieved 29 September 2022 from https://www.tutorialspoint.com/cryptography
8. CAPTCHA, 29 September 2022 from https://www.google.com/recaptcha/about/
9. Salted Hash Password, Retieved 29 September 2022 from https://www.pingidentity.com/hashing-vs-salting
10. D. M'Raihi, S. Machani, M. Pei, J. Rydell“, TOTP (Time-based One-Time Password)”, IETF RFC 6238, May 2011