บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ทฤษฎีที่เกี่ยวข้อง

1) Weblog or Blog

Blog มาจากศัพท์คำเต็มว่า WeBlog [5] คือ เว็บไซต์ประเภทหนึ่ง ที่เจ้าของ หรือ Blogger สามารถบันทึกเรื่องราวของตนเองลงในเว็บได้ นอกจากนี้ Blog ยังเป็นพื้นที่ให้ Blogger โพสต์ข้อมูล หรือใส่ความรู้ ประสบการณ์ อาจเป็นเรื่องส่วนตัว นำเสนอความคิดและประสบการณ์ของบล็อกเกอร์ หรืออาจเน้นข่าวสารมากกว่า ครอบคลุมเหตุการณ์และประเด็นปัจจุบัน นอกจากนี้ยังมีบล็อกเฉพาะจำนวนมากที่เน้นหัวข้อเฉพาะ เช่น การเมือง เทคโนโลยี แฟชั่น อาหาร หรือเพื่อเป็นวิทยาทานให้คนอื่น ๆ ซึ่งข้อแตกต่างของบล็อกกับเว็บไซต์ทั่วไป คือ บล็อกจะเปิดให้ผู้เข้ามาอ่านข้อมูล สามารถแสดงความคิดเห็นต่อท้ายข้อความที่เจ้าของบล็อกเขียน ซึ่งทำให้ผู้เขียนสามารถได้ผลตอบกลับโดยทันที ในช่วงไม่กี่ปีที่ผ่านมา การเขียนบล็อกเป็นวิธียอดนิยมสำหรับบุคคลและองค์กรในการแบ่งปันข้อมูลและมีส่วนร่วมกับผู้ชมทางออนไลน์ บล็อกจำนวนมากสร้างรายได้จากการโฆษณาหรือจากการสนับสนุน

2) WordPress

WordPress [6] เป็นระบบจัดการเนื้อหายอดนิยม (CMS) ที่ใช้ในการสร้างและจัดการเว็บไซต์ เป็นซอฟต์แวร์ Open sourse ที่ให้บริการฟรีและสามารถปรับแต่งให้ตรงกับความต้องการของเว็บไซต์ที่หลากหลาย รวมถึงบล็อก ไซต์อีคอมเมิร์ซ และอื่น ๆ

ข้อดีบางประการของการใช้ WordPress ได้แก่ ใช้งานง่าย มีอินเทอร์เฟสที่ใช้งานง่ายซึ่งทำให้ผู้ใช้ที่มีประสบการณ์ในการเขียนโค้ดน้อยหรือไม่มีเลยสามารถสร้างและจัดการเว็บไซต์ได้ง่าย การปรับแต่ง มีชุมชนขนาดใหญ่ของนักพัฒนาที่สร้างธีมและปลั๊กอินที่หลากหลายซึ่งสามารถใช้เพื่อปรับแต่งรูปลักษณ์และการทำงานของเว็บไซต์ 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 แต่มีข้อจำกัดบางประการในแง่ของความปลอดภัยและความยืดหยุ่นในการใช้งาน

3) Hash

Hash [7] 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 ซึ่งแต่ละประเภทมีลักษณะเฉพาะและการใช้งานที่แตกต่างกัน

อัลกอริธึมการแฮชที่แตกต่างกันมากมายที่สามารถใช้สร้างค่าแฮชได้ ตัวอย่างทั่วไป ได้แก่ MD5, SHA-1 SHA-3 และ SHA-256 การเลือกอัลกอริทึมอาจส่งผลต่อความปลอดภัยของรหัสผ่านที่แฮชได้ เนื่องจากอัลกอริทึมบางตัวสามารถต้านทานการโจมตีได้ดีกว่าตัวอื่น ๆ รหัสผ่านแบบแฮชเป็นวิธีที่ปลอดภัยในการจัดเก็บรหัสผ่านในฐานข้อมูล เนื่องจากทำให้มั่นใจได้ว่ารหัสผ่านเดิมจะไม่สามารถเข้าถึงได้หรือกำหนดได้ง่าย

4) Captcha

CAPTCHA [8] ย่อมาจากคำเต็มว่า “Completely Automated Public Turing test to tell Computers and Humans Apart” เป็นการทดสอบการตอบสนองความท้าทายประเภทหนึ่งที่ใช้ในการคำนวณเพื่อตรวจสอบว่าผู้ใช้เป็นมนุษย์หรือไม่ มักใช้เพื่อป้องกันเว็บไซต์จากบอทและโปรแกรมอัตโนมัติที่สามารถสร้างบัญชีปลอม เว็บไซต์สแปมหรือทำกิจกรรมที่เป็นอันตรายอื่น ๆ โดยทั่วไปแล้ว CAPTCHA จะประกอบด้วยภาพตัวอักษรและตัวเลขที่บิดเบี้ยว ซึ่งมนุษย์สามารถอ่านได้ง่าย แต่โปรแกรมคอมพิวเตอร์ไม่สามารถทำได้ ผู้ใช้จะถูกขอให้พิมพ์ตัวอักษรและตัวเลขที่เห็นในภาพลงในช่องแบบฟอร์มเพื่อพิสูจน์ว่าเป็นมนุษย์ สิ่งนี้ช่วยป้องกันไม่ให้โปรแกรมอัตโนมัติเข้าถึงเว็บไซต์หรือดำเนินการบางอย่างกับเว็บไซต์ CAPTCHA เพื่อป้องกันแบบฟอร์มออนไลน์ เช่น หน้าเข้าสู่ระบบ ไม่ให้ส่งโดยโปรแกรมอัตโนมัติ ใช้เพื่อป้องกันเว็บไซต์จากการถูกสแปมโดยบอทและเพื่อป้องกันการเข้าถึงพื้นที่บางส่วนของเว็บไซต์โดยไม่ได้รับอนุญาต

วัตถุประสงค์ของ CAPTCHA คือเพื่อให้แน่ใจว่าผู้ใช้ที่พยายามเข้าสู่ระบบเป็นบุคคลจริงไม่ใช่บอทหรือสคริปต์อัตโนมัติ ซึ่งจะช่วยป้องกันเว็บไซต์จากสแปมและการละเมิดและสามารถปรับปรุง

ความปลอดภัยโดยรวมของเว็บไซต์ได้

5) Salted Hash Password

Salted Hash Password [9] คือ รหัสผ่านแบบแฮชประเภทหนึ่งที่มีชั้นความปลอดภัยเพิ่มเติมที่เรียกว่า Salt ซึ่ง Salt คือ สตริงอักขระแบบสุ่มที่สร้างขึ้นและร่วมกับรหัสผ่านก่อนที่จะแฮช ซึ่งจะทำให้ผู้โจมตีถอดรหัสรหัสผ่านได้ยากขึ้น ค่า Salt จะถูกเพิ่มเข้าไปในรหัสผ่านเพื่อทำให้ผู้โจมตีถอดรหัสรหัสผ่านได้ยากขึ้น แม้ว่าพวก Hacker จะเข้าถึงฐานข้อมูลรหัสผ่านที่แฮชได้ เพราะผู้โจมตีต้องทราบค่า Salt ถึงจะสามารถถอดรหัสแฮชได้อย่างถูกต้อง การใช้ Salted Hash Password สิ่งสำคัญคือ ต้องใช้ฟังก์ชันแฮชที่แข็งแกร่งและปลอดภัย เช่น ฟังก์ชันแฮชการเข้ารหัส เพื่อให้แน่ใจว่ารหัสผ่านที่แฮชนั้นปลอดภัยที่สุดเท่าที่จะเป็นไปได้

6) TOTP (Time-based One-Time Password)

TOTP [10] ย่อมาจาก Time-based One-Time Password เป็นรหัสผ่านแบบใช้ครั้งเดียว (OTP) ประเภทหนึ่ง ที่สร้างขึ้นตามเวลาปัจจุบันและรหัสลับที่ใช้ร่วมกัน โดยทั่วไปจะใช้ TOTP เป็นชั้นความปลอดภัยเพิ่มเติมสำหรับบัญชีออนไลน์ เมื่อผู้ใช้ต้องการเข้าสู่ระบบบัญชีของตน นอกเหนือจากชื่อผู้ใช้และรหัสผ่าน TOTP สร้างขึ้นโดยอุปกรณ์ของผู้ใช้ (เช่น สมาร์ทโฟน) โดยใช้แอพหรือ โปรแกรมที่สามารถเข้าถึงรหัสลับที่ใช้ร่วมกัน จากนั้น ผู้ใช้ป้อน TOTP ลงในข้อความแจ้งการเข้าสู่ระบบ และหากถูกต้อง ผู้ใช้จะได้รับสิทธิ์เข้าถึงบัญชีของตน ข้อดีอย่างหนึ่งของ TOTP คือให้ระดับความปลอดภัยพิเศษโดยที่ผู้ใช้ไม่ต้องจำรหัสผ่านเพิ่มเติม นอกจากนี้ ยังมีความปลอดภัยมากกว่า OTP ประเภทอื่น เช่น รหัสที่ส่งทาง SMS เนื่องจากผู้โจมตีไม่สามารถดักฟังหรือคาดเดาได้ โดยสรุป TOTP เป็นรหัสผ่านแบบใช้ครั้งเดียวชนิดหนึ่งที่สร้างขึ้นตามเวลาปัจจุบันและรหัสลับที่ใช้ร่วมกัน มักใช้เป็นชั้นความปลอดภัยเพิ่มเติมสำหรับบัญชีออนไลน์ ซึ่งสามารถใช้งานได้ทุกที่ทุกเวลาโดยไม่ต้องพกพาอุปกรณ์เพิ่มเติม ทำให้เป็นวิธีการรักษาความปลอดภัยที่ทันสมัยและมีความสะดวกสบายสำหรับผู้ใช้บัญชีออนไลน์

2.2 ระบบงานที่เกี่ยวข้อง

2.2.1 ปัญหาการถูกโจมตีของ WordPress

จากจำนวนเว็บไซต์ทั่วโลกมีสูงถึง 1,196,298,727 เว็บไซต์และ WordPress นั้นมีส่วนแบ่งการใช้งานทั่วโลกอยู่ถึง 35% คิดรวมเป็น สี่ร้อยกว่าล้านเว็บไซต์ เมื่อมีจำนวนมากขนาดนี้ ย่อมตกเป็นเป้าของ Hacker ทั่วโลก ซึ่งสาเหตุหลัก ๆ ที่ WordPress โดน Hack [11] มาจากสิ่งต่าง ๆ เช่น ไม่มีการอัพเดท Version WordPress, Plugins,Theme เนื่องจาก WordPress เป็น CMS ที่เป็น Open Source และมีการอัปเดตมาจากผู้พัฒนาอยู่เสมอ แต่สิ่งที่คนทำ WordPress มักจะลืมกันบ่อย ๆ คือการอัพเกรด Version WordPress เป็นเวอร์ชั่นล่าสุดให้รวดเร็วที่สุด เนื่องจากการอัปเดตนอกจากเพิ่มฟีเจอร์ใหม่ ๆ มีการแก้ไขช่องโหว่ทางด้านความปลอดภัยต่าง ๆ และการตั้งค่ารหัสผ่านที่ง่ายต่อการ

คาดเดา มีผู้ใช้งานมากมายได้ติดตั้ง WordPress ด้วยรหัสผ่านที่ง่าย เช่น 1234 เป็นรหัสที่ง่ายต่อการคาดเดาและไม่ควรใช้อย่างยิ่งบนเว็บไซต์ เพราะรหัสพวกนี้ Hacker สามารถเขียนโปรแกรมสุ่มรหัสผ่านและ Login ได้ภายในเวลาไม่ถึงวินาที ที่ผ่านมาข่าวการโดนโจมตีของ WordPress website ซึ่งมีเป็นจำนวนมาก เช่น ข้อบกพร่องแบบ Zero-day ในปลั๊กอิน WordPress ที่เรียกว่า BackupBuddy [12] ซึ่งกำลังถูกโจมตี Wordfence บริษัทด้านความปลอดภัยของ WordPress ได้เปิดเผย "Local Directory Copy" ซึ่งออกแบบมาเพื่อจัดเก็บสำเนาสำรองในเครื่อง จากข้อมูลของ Wordfence ช่องโหว่ดังกล่าวเป็นผลมาจากการใช้งานที่ไม่ปลอดภัย ซึ่งทำให้ผู้คุกคามที่ไม่ได้รับการพิสูจน์ตัวตนสามารถดาวน์โหลดไฟล์ใด ๆ บนเซิร์ฟเวอร์ได้ตามอำเภอใจ

จึงมีความจำเป็นที่ผู้ดูแลระบบของเว็บไซต์ WordPress ต่าง ๆ ต้องระมัดระวังและดูแลการความปลอดภัยของเว็บไซต์อย่างใกล้ชิด เพื่อป้องกันการโจมตีที่อาจก่อให้เกิดความเสียหายกับข้อมูลที่เก็บไว้ในเว็บไซต์ รวมถึงข้อมูลส่วนตัวของผู้ใช้งาน เพื่อประสิทธิภาพและความปลอดภัยของระบบ

2.2.2 ปัญหาด้านความล่าช้าของ WordPress websites

ปัญหาด้านความล่าช้าของ WordPress [13] มีหลายสาเหตุที่เป็นไปได้ที่เว็บไซต์ WordPress อาจประสบกับความล่าช้าหรือประสิทธิภาพการทำงานช้าสาเหตุทั่วไปบางประการมีดังนี้

(1) โฮสติ้งและเซิร์ฟเวอร์ การใช้งานโฮสติ้งที่ไม่เหมาะสมหรือเซิร์ฟเวอร์ที่มีปัญหาทางด้านประสิทธิภาพสามารถทำให้เว็บไซต์ WordPress ทำงานช้า

(2) การอัปเดต WordPress ล่าช้า การอัปเดต WordPress ล่าช้าอาจทำให้เกิดปัญหาด้านความปลอดภัยหรือประสิทธิภาพได้

(3) ปลั๊กอินจำนวนมาก การติดตั้งปลั๊กอินมากเกินไปในไซต์อาจทำให้เกิดปัญหาด้านประสิทธิภาพ

(4) รูปภาพขนาดใหญ่หรือไม่ได้เพิ่มประสิทธิภาพ รูปภาพขนาดใหญ่ที่ไม่ได้เพิ่มประสิทธิภาพจำนวนมาก อาจทำให้เวลาในการโหลดหน้าเว็บช้าลง

(5) ฐานข้อมูลที่ไม่ได้เพิ่มประสิทธิภาพ เมื่อเวลาผ่านไป ฐานข้อมูล WordPress อาจเต็มไปด้วยข้อมูลที่ไม่จำเป็น ซึ่งทำให้เว็บไซต์ช้าลงได้

(6) ไม่มีการแคช การแคชสามารถช่วยเพิ่มความเร็วไซต์ โดยการจัดเก็บหน้าและโพสต์ในเวอร์ชันคงที่ จึงไม่จำเป็นต้องสร้างใหม่ทุกครั้งที่มีคนเข้าชมเว็บไซต์

2.3 ตารางเปรียบเทียบ

ตารางเปรียบเทียบประสิทธิภาพของเว็บไซต์ โดยนำเว็บไซต์ WorayuthIT ที่มีการใช้งาน WordPress เป็นฐาน ซึ่งมีการเพิ่มประสิทธิภาพทั้งด้านความเร็ว และความมั่นคงปลอดภัย เปรียบเทียบระหว่างเว็บไซต์ที่มีการใช้งาน WordPress ที่เป็นค่าเริ่มต้นและเว็บไซต์ที่มีการพัฒนาขึ้นเอง

ตารางที่ 2.1 ตารางเปรียบเทียบเว็บไซต์

รายการ	การพัฒนาเว็บไซต์จากการพัฒนาขึ้นเอง	การพัฒนาเว็บไซต์จาก WordPress (ค่าเริ่มต้น)	การพัฒนาเว็บไซต์จาก WordPress โดย project นี้
1. เวลาและต้นทุนในการพัฒนา	อาจต้องใช้เวลาและทรัพยากรมากกว่าการใช้ WordPress	เวลาและค่าใช้จ่ายน้อยกว่าเว็บไซต์ WordPress ที่ได้รับการปรับแต่ง	เวลาและค่าใช้จ่ายมากกว่าเว็บไซต์ WordPress ที่ไม่ได้ปรับแต่ง
3. ประสิทธิภาพ	อาจมีประสิทธิภาพที่ดีกว่าเว็บไซต์ที่ใช้ WordPress	ปรับให้เหมาะสมก็อาจมีประสิทธิภาพที่ดีเช่นกัน	มีการตั้งค่า plugin ปรับให้เหมาะสมจึงมีประสิทธิภาพที่ดี
4. ความปลอดภัย	อาจมีช่องโหว่น้อยกว่าเว็บไซต์ที่ใช้ WordPress	สามารถปรับให้เหมาะสมและดีมากกว่าเดิมได้	มีการตั้งค่า plugin และเสริมส่วนต่างๆ ให้เหมาะสมอาจมีความปลอดภัยที่ดีกว่า
5. การป้องกัน Brute-Force	สามารถทำได้ ขึ้นอยู่กับผู้ดูแล	สามารถทำได้	มีการป้องกันหน้า Login ด้วย reCAPTCHA
7. ความปลอดภัยที่กำหนดเอง	ปรับแต่งได้อย่างเต็มที่	ปรับแต่งได้ แต่อาจมีข้อจำกัดบางอย่าง	ปรับแต่งได้ แต่อาจมีข้อจำกัดบางอย่าง