การพัฒนาส่วนขยายของเว็บเบราว์เซอร์กูเกิล โครม เพื่อประเมินความมั่นคงปลอดภัยของเว็บไซต์ตามแนวทาง OWASP Top 10

Development of a Google Chrome Browser Extension for Website Security Assessment Based on OWASP Top 10

ธนกฤต รุ่งแจ้ง[1], วิรัญญา พุ่มจันทร์[2], สุพจน์ พ่วงกำเหนิด[3]

[1]คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล, มหาวิทยาลัยนอร์ทกรุงเทพ, thanakit.rung@northbkk.ac.th

[2]คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล, มหาวิทยาลัยนอร์ทกรุงเทพ, wiranya.poom@northbkk.ac.th

[3]คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล, มหาวิทยาลัยนอร์ทกรุงเทพ, suphot.ph@northbkk.ac.th

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อพัฒนาส่วนขยายบนเว็บเบราว์เซอร์กูเกิล โครม สำหรับประเมินความมั่นคงปลอดภัยของเว็บไซต์ตามแนวทาง OWASP Top 10 และเพื่อประเมินประสิทธิภาพของส่วนขยาย โดยเปรียบเทียบความสามารถในการตรวจจับเว็บไซต์ที่มีความเสี่ยง รวมถึงศึกษาความพึงพอใจของผู้ใช้งาน การวิจัยเป็นการวิจัยเชิงประยุกต์ กลุ่มตัวอย่างประกอบด้วยผู้ใช้งาน จำนวน 50 คน และผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ จำนวน 5 คน เครื่องมือที่ใช้ ได้แก่ ส่วนขยายที่พัฒนาขึ้น แบบสอบถาม และแบบประเมิน วิเคราะห์ข้อมูลด้วยค่าเฉลี่ย ($\overline{X}$) และส่วนเบี่ยงเบนมาตรฐาน (SD)

ผลการวิจัยพบว่า (1) ส่วนขยายที่พัฒนาขึ้นสามารถตรวจจับและแจ้งเตือนความเสี่ยงของเว็บไซต์ตามแนวทาง OWASP Top 10 ได้ (2) เมื่อเปรียบเทียบความสามารถในการตรวจจับเว็บไซต์ที่มีความเสี่ยงตามเกณฑ์ที่กำหนด พบว่าระบบมีประสิทธิภาพอยู่ในระดับเหมาะสม และ (3) ผู้ใช้งานมีความพึงพอใจโดยรวมอยู่ในระดับมาก ($\overline{X}$ = 4.18, SD = 0.47) และผู้เชี่ยวชาญประเมินความเหมาะสมของระบบอยู่ในระดับมาก ($\overline{X}$ = 4.42, SD = 0.38) แสดงให้เห็นว่าระบบมีความเหมาะสมต่อการนำไปใช้งานจริง อย่างไรก็ตาม การประเมินในงานวิจัยนี้ยังเป็นการประเมินเชิงการรับรู้ และยังไม่ได้ครอบคลุมการทดสอบเชิงลึกด้านการตรวจจับช่องโหว่ในระดับเทคนิคขั้นสูง

คำหลัก: ความมั่นคงปลอดภัยเว็บไซต์, ส่วนขยายกูเกิล โครม, OWASP Top 10, การประเมินความมั่นคงปลอดภัยเว็บไซต์

Abstract

This research aimed to develop a Google Chrome browser extension for evaluating website security based on the OWASP Top 10 framework, and to assess the performance of the extension by comparing its ability to detect risky websites, as well as to examine user satisfaction. This study was conducted as applied research. The sample consisted of 50 users and 5 experts in information technology and cybersecurity. The research instruments included the developed browser extension, a user questionnaire, and an expert evaluation form. Data were analyzed using mean ($\overline{X}$) and standard deviation (SD).

The results showed that (1) the developed extension was able to detect and alert website security risks based on the OWASP Top 10 framework; (2) when comparing its detection capability against predefined criteria, the system demonstrated an appropriate level of performance; and (3) users reported a high level of overall satisfaction ($\overline{X}$ = 4.18, SD = 0.47), while experts rated the system at a high level of appropriateness ($\overline{X}$ = 4.42, SD = 0.38). These findings indicate that the system is suitable for practical use. However, this evaluation focused on user perception and did not cover in-depth technical vulnerability testing.

Keywords: website security, Google Chrome extension, OWASP Top 10, World Wide Web

ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันเทคโนโลยีดิจิทัลและอินเทอร์เน็ตมีบทบาทสำคัญต่อการดำเนินชีวิตประจำวันของประชาชน ทั้งในด้านการสื่อสาร การศึกษา และการทำธุรกรรมทางอิเล็กทรอนิกส์ อย่างไรก็ตาม การขยายตัวของการใช้งานดังกล่าวส่งผลให้ภัยคุกคามทางไซเบอร์มีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่อง โดยเฉพาะการโจมตีเว็บไซต์และเว็บแอปพลิเคชัน ซึ่งเป็นช่องทางหลักในการให้บริการข้อมูลและธุรกรรมออนไลน์ รายงานสถานการณ์ภัยคุกคามไซเบอร์ของประเทศไทยระบุว่า การโจมตีที่เกี่ยวข้องกับเว็บไซต์ เช่น การหลอกลวง การฝังมัลแวร์ และการรั่วไหลของข้อมูลส่วนบุคคล ยังคงเป็นปัญหาที่พบอย่างแพร่หลาย และส่งผลกระทบโดยตรงต่อความเชื่อมั่นของผู้ใช้งานอินเทอร์เน็ต (Cybersecurity Thailand, 2566; สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ, 2565) ภาครัฐของประเทศไทยจึงได้กำหนดนโยบายและกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ของประเทศ เพื่อยกระดับความปลอดภัยทางไซเบอร์อย่างเป็นระบบ

จากการทบทวนงานวิจัยที่เกี่ยวข้อง พบว่างานวิจัยด้านความมั่นคงปลอดภัยของเว็บไซต์ส่วนใหญ่มุ่งเน้นการประเมินช่องโหว่จากมุมมองของผู้ดูแลระบบหรือผู้เชี่ยวชาญ โดยใช้เครื่องมือสแกนช่องโหว่หรือการทดสอบเจาะระบบ ขณะที่ผู้ใช้งานทั่วไปยังขาดเครื่องมือสนับสนุนการตัดสินใจในการประเมินความเสี่ยงของเว็บไซต์ในระหว่างการใช้งานจริง แม้ว่าเว็บเบราว์เซอร์ Google Chrome จะมีส่วนขยายด้านความมั่นคงปลอดภัยให้เลือกใช้งานเป็นจำนวนมากใน Chrome Web Store แต่เครื่องมือส่วนใหญ่ยังมีข้อจำกัด เช่น การตรวจจับที่มุ่งเน้นเฉพาะภัยคุกคามบางประเภท ขาดการประเมินความเสี่ยงตามกรอบมาตรฐานอย่าง OWASP Top 10 อย่างครอบคลุม รวมถึงรูปแบบการแสดงผลที่ซับซ้อนและไม่เหมาะสมกับผู้ใช้งานทั่วไป อีกทั้งเครื่องมือบางประเภทถูกออกแบบสำหรับผู้เชี่ยวชาญ ส่งผลให้ผู้ใช้งานทั่วไปไม่สามารถเข้าถึงหรือใช้งานได้อย่างมีประสิทธิภาพ นอกจากนี้ แม้กรอบแนวคิด OWASP Top 10 จะได้รับการยอมรับอย่างแพร่หลาย แต่การประยุกต์ใช้ในรูปแบบเครื่องมือฝั่งผู้ใช้งาน (Client-side) ยังมีข้อจำกัดและยังไม่ถูกพัฒนาอย่างแพร่หลาย

จากข้อจำกัดดังกล่าว จะเห็นได้ว่ายังขาดเครื่องมือที่สามารถประเมินความมั่นคงปลอดภัยของเว็บไซต์ได้อย่างครอบคลุมตามแนวทาง OWASP Top 10 และเหมาะสมกับผู้ใช้งานทั่วไป ดังนั้นงานวิจัยนี้จึงมุ่งพัฒนาส่วนขยายบนเว็บเบราว์เซอร์กูเกิล โครม เพื่อประเมินความมั่นคงปลอดภัยของเว็บไซต์จากมุมมองผู้ใช้งาน โดยเน้นการบ่งชี้ความเสี่ยงตามแนวทาง OWASP Top 10 พร้อมทั้งประเมินประสิทธิภาพของระบบโดยเปรียบเทียบความสามารถในการตรวจจับเว็บไซต์ที่มีความเสี่ยง และศึกษาความพึงพอใจของผู้ใช้งานและผู้เชี่ยวชาญ เพื่อส่งเสริมความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์และสนับสนุนการใช้งานอินเทอร์เน็ตอย่างปลอดภัยในสังคมดิจิทัล

วัตถุประสงค์

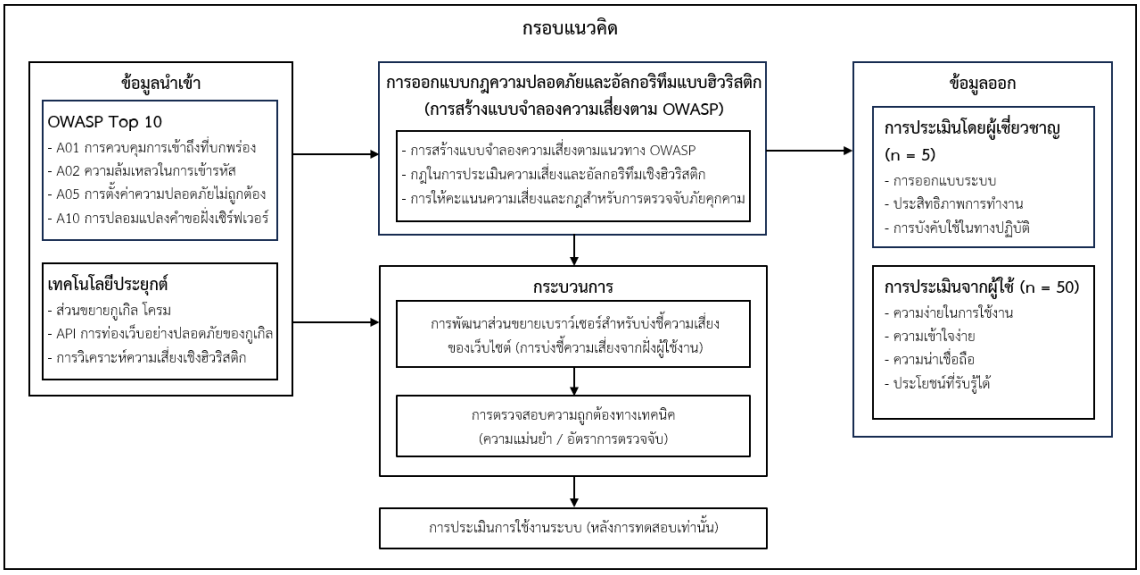
1. เพื่อพัฒนาส่วนขยายบนเว็บเบราว์เซอร์กูเกิล โครม สำหรับประเมินความมั่นคงปลอดภัยของเว็บไซต์ตามแนวทาง OWASP Top 10
2. เพื่อประเมินประสิทธิภาพของส่วนขยาย โดยเปรียบเทียบความสามารถในการตรวจจับเว็บไซต์ที่มีความเสี่ยง และศึกษาความพึงพอใจของผู้ใช้งาน

ประโยชน์ที่คาดว่าจะได้รับ

1. ได้ส่วนขยายบนเว็บเบราว์เซอร์กูเกิล โครม ที่สามารถประเมินความมั่นคงปลอดภัยของเว็บไซต์ตามแนวทาง OWASP Top 10 และสามารถนำไปใช้งานได้จริง
2. ผู้ใช้งานสามารถรับรู้และประเมินความเสี่ยงของเว็บไซต์ได้อย่างสะดวกและรวดเร็ว ช่วยส่งเสริมความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

3. ได้องค์ความรู้ด้านการออกแบบและพัฒนาเครื่องมือประเมินความมั่นคงปลอดภัยของเว็บไซต์ในฝั่งผู้ใช้งาน (Client-side) โดยอ้างอิงกรอบ OWASP Top 10 ซึ่งสามารถใช้เป็นแนวทางในการพัฒนาและต่อยอดงานวิจัยด้านความมั่นคงปลอดภัยไซเบอร์ในอนาคต

กรอบแนวคิด



ภาพ 1 กรอบแนวคิดของโครงการ

1. กรอบแนวคิดการวิจัยเริ่มต้นจาก ปัจจัยนำเข้า (Input Factors) ซึ่งประกอบด้วยกรอบแนวคิด OWASP Top 10 ในประเด็น A01, A02, A05 และ A10 ที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์ ร่วมกับเทคโนโลยีที่ใช้ในการพัฒนา ได้แก่ ส่วนขยายบนเว็บเบราว์เซอร์ Google Chrome, Google Safe Browsing API และการวิเคราะห์ความเสี่ยงด้วยวิธี Heuristic Risk Analysis

2. จากนั้นนำแนวคิด OWASP Top 10 มาใช้เป็นพื้นฐานในการพัฒนา กฎการตรวจสอบและอัลกอริทึมการประเมินความเสี่ยง (Security Rule & Heuristic Algorithm Design) โดยกำหนดเงื่อนไขและตัวชี้วัด เช่น การตรวจสอบโปรโตคอลของเว็บไซต์ การวิเคราะห์โครงสร้าง URL การเปรียบเทียบกับฐานข้อมูลเว็บไซต์อันตราย และการให้คะแนนความเสี่ยง (Risk Scoring) เพื่อใช้เป็นกลไกหลักในการบ่งชี้ความเสี่ยงของเว็บไซต์

3. อัลกอริทึมดังกล่าวถูกนำไปใช้ในกระบวนการ (Process) คือ การพัฒนาส่วนขยายสำหรับบ่งชี้ความเสี่ยงของเว็บไซต์จากฝั่งผู้ใช้งาน (Client-side Risk Indication) โดยมุ่งเน้นการแจ้งเตือนและสนับสนุนการรับรู้ความเสี่ยงของผู้ใช้ ไม่ใช่การตรวจสอบช่องโหว่เชิงลึกของเว็บไซต์

4. ภายหลังการพัฒนาระบบ จะดำเนินการ ประเมินประสิทธิภาพเชิงเทคนิค (Technical Validation) โดยทดสอบความสามารถในการตรวจจับเว็บไซต์ที่มีความเสี่ยง และประเมินความถูกต้องของระบบ เช่น ค่า Accuracy หรือ Detection Rate จากชุดข้อมูลทดสอบ

5. จากนั้นดำเนินการ ประเมินการใช้งานระบบ (System Usage Evaluation) ในรูปแบบ post-test only เพื่อประเมินความคิดเห็นของผู้ใช้หลังการทดลองใช้งาน โดยไม่มีการเปรียบเทียบก่อน-หลังการใช้งาน

6. ผลลัพธ์ (Output) ของการวิจัยแบ่งออกเป็น 3 ส่วน ได้แก่

- ผลการประเมินเชิงเทคนิค เช่น ความแม่นยำในการตรวจจับเว็บไซต์ที่มีความเสี่ยง
- การประเมินจากผู้ใช้งานทั่วไป จำนวน 50 คน ในด้านความสะดวกในการใช้งาน ความเข้าใจ ความเชื่อมั่น และการรับรู้ประโยชน์ของระบบ
- การประเมินจากผู้เชี่ยวชาญ จำนวน 5 คน ในด้านแนวคิดการออกแบบ ฟังก์ชันการทำงาน และความเหมาะสมในการนำไปใช้งานจริง

7. ข้อมูลที่ได้จากทั้งสามส่วนจะนำมาวิเคราะห์ด้วยสถิติ ได้แก่

- สถิติเชิงพรรณนา (Mean, Standard Deviation) สำหรับข้อมูลความคิดเห็นและความพึงพอใจ
- สถิติประเมินประสิทธิภาพของระบบ เช่น Accuracy เพื่อสะท้อนความสามารถในการตรวจจับความเสี่ยงของระบบ

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยและพัฒนา (Research and Development: R&D) มีวัตถุประสงค์เพื่อพัฒนาและประเมินต้นแบบส่วนขยายด้านความมั่นคงปลอดภัยสำหรับเว็บเบราว์เซอร์ Google Chrome โดยดำเนินการตามกระบวนการวิจัยเชิงระบบ ครอบคลุมตั้งแต่การศึกษาทฤษฎี การออกแบบ การพัฒนา การทดลอง และการประเมินผล ซึ่งชิ้นงาน (Prototype) เป็นเพียงส่วนหนึ่งของกระบวนการวิจัยทั้งหมด โดยแบ่งออกเป็น 6 ขั้นตอน ดังนี้

ขั้นตอนที่ 1 การศึกษาข้อมูลและวิเคราะห์ความต้องการเชิงพัฒนา

ในขั้นตอนนี้ ผู้วิจัยดำเนินการศึกษาทบทวนเอกสาร งานวิจัย และแหล่งข้อมูลที่เกี่ยวข้องกับความมั่นคงปลอดภัยของเว็บแอปพลิเคชัน โดยมุ่งเน้นกรอบแนวคิด OWASP Top 10 ซึ่งเป็นมาตรฐานสากลที่ใช้ในการระบุประเภทของช่องโหว่และภัยคุกคามที่พบบ่อยในระบบเว็บ ทั้งนี้เพื่อให้เข้าใจลักษณะของปัญหาและแนวทางในการป้องกันอย่างเป็นระบบ

การศึกษาดังกล่าวครอบคลุมทั้งแนวคิดเชิงทฤษฎีและการประยุกต์ใช้งานจริง เช่น รูปแบบการโจมตีแบบฟิชชิง (Phishing) การแพร่กระจายมัลแวร์ (Malware) และพฤติกรรมของ URL ที่มีความเสี่ยง ซึ่งข้อมูลเหล่านี้ถูกนำมาวิเคราะห์เพื่อระบุปัจจัยที่ส่งผลต่อความปลอดภัยของเว็บไซต์

นอกจากนี้ ผู้วิจัยได้ดำเนินการวิเคราะห์ความต้องการของผู้ใช้งาน (User Requirement Analysis) โดยพิจารณาลักษณะของผู้ใช้งานทั่วไปที่ไม่มีความเชี่ยวชาญด้านเทคนิค พบว่าผู้ใช้งานต้องการระบบที่สามารถ

- ใช้งานได้ง่าย ไม่ซับซ้อน
- ให้ผลลัพธ์ที่เข้าใจได้ทันที
- สามารถช่วยตัดสินใจในการเข้าถึงเว็บไซต์ได้อย่างปลอดภัย

จากการวิเคราะห์ดังกล่าว ผู้วิจัยจึงกำหนดแนวทางการพัฒนาระบบในลักษณะ “การบ่งชี้ระดับความเสี่ยง (Risk Indication)” โดยใช้การแสดงผลด้วยสี สัญลักษณ์ และข้อความสั้น เพื่อให้ผู้ใช้สามารถรับรู้ระดับความปลอดภัยของเว็บไซต์ได้อย่างรวดเร็ว

ผลลัพธ์ของขั้นตอนนี้คือการกำหนดขอบเขตของระบบ (System Scope) แนวทางการออกแบบ (Design Guideline) และชุดตัวชี้วัดความเสี่ยงเบื้องต้น (Preliminary Risk Indicators) ซึ่งจะถูกนำไปใช้เป็นพื้นฐานในการออกแบบสถาปัตยกรรมระบบและพัฒนาอัลกอริทึมในขั้นตอนถัดไป

ขั้นตอนที่ 2 การออกแบบระบบและพัฒนากรอบแนวคิดเชิงเทคนิค

ในขั้นตอนนี้ ผู้วิจัยดำเนินการออกแบบระบบโดยอาศัยข้อมูลจากการศึกษาทฤษฎีและการวิเคราะห์ความต้องการในขั้นตอนที่ 1 เพื่อกำหนดโครงสร้างระบบ กลไกการทำงาน และแนวทางการพัฒนาอัลกอริทึมสำหรับประเมินความเสี่ยงของเว็บไซต์ โดยมุ่งเน้นการออกแบบที่เป็นระบบ (Systematic Design) และสอดคล้องกับการใช้งานจริง

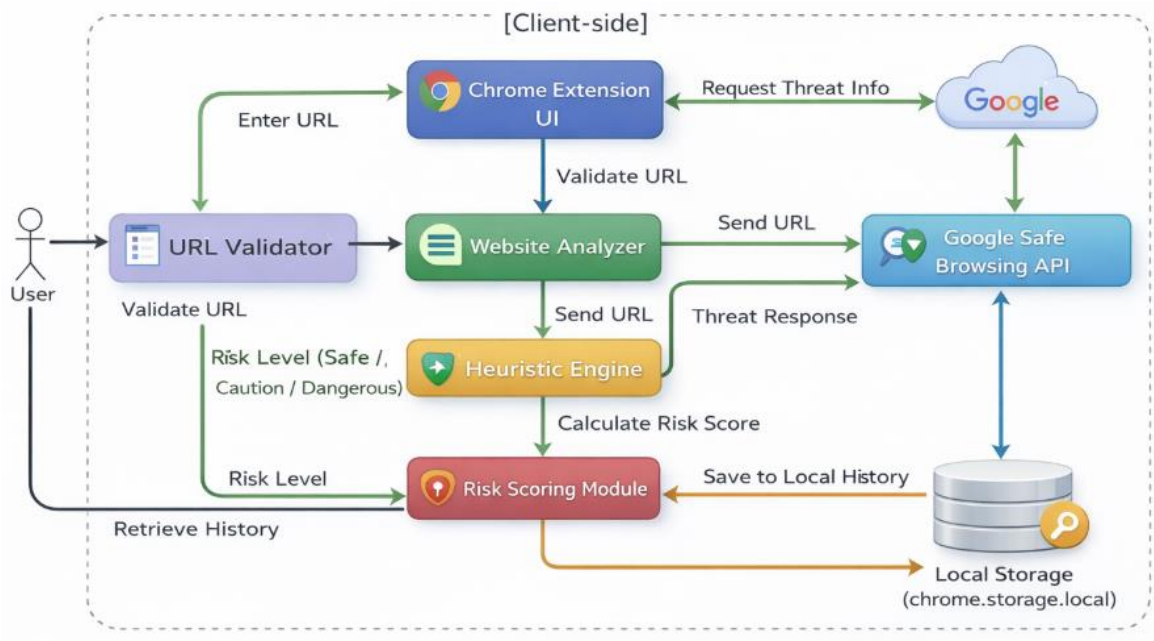
1. การออกแบบสถาปัตยกรรมระบบ (System Architecture)

ผู้วิจัยออกแบบระบบในลักษณะ Client-side Architecture โดยพัฒนาระบบให้อยู่ในรูปแบบของส่วนขยาย (Extension) บนเว็บเบราว์เซอร์ Google Chrome ซึ่งสามารถทำงานได้โดยตรงบนฝั่งผู้ใช้งาน

โครงสร้างระบบประกอบด้วยองค์ประกอบหลัก ได้แก่

- ส่วนติดต่อผู้ใช้ (User Interface: UI)
- โมดูลตรวจสอบความถูกต้องของ URL (URL Validator)
- โมดูลวิเคราะห์เว็บไซต์ (Website Analyzer)
- การเชื่อมต่อกับ Google Safe Browsing API
- โมดูลวิเคราะห์เชิงฮิวริสติก (Heuristic Engine)
- โมดูลคำนวณระดับความเสี่ยง (Risk Scoring Module)

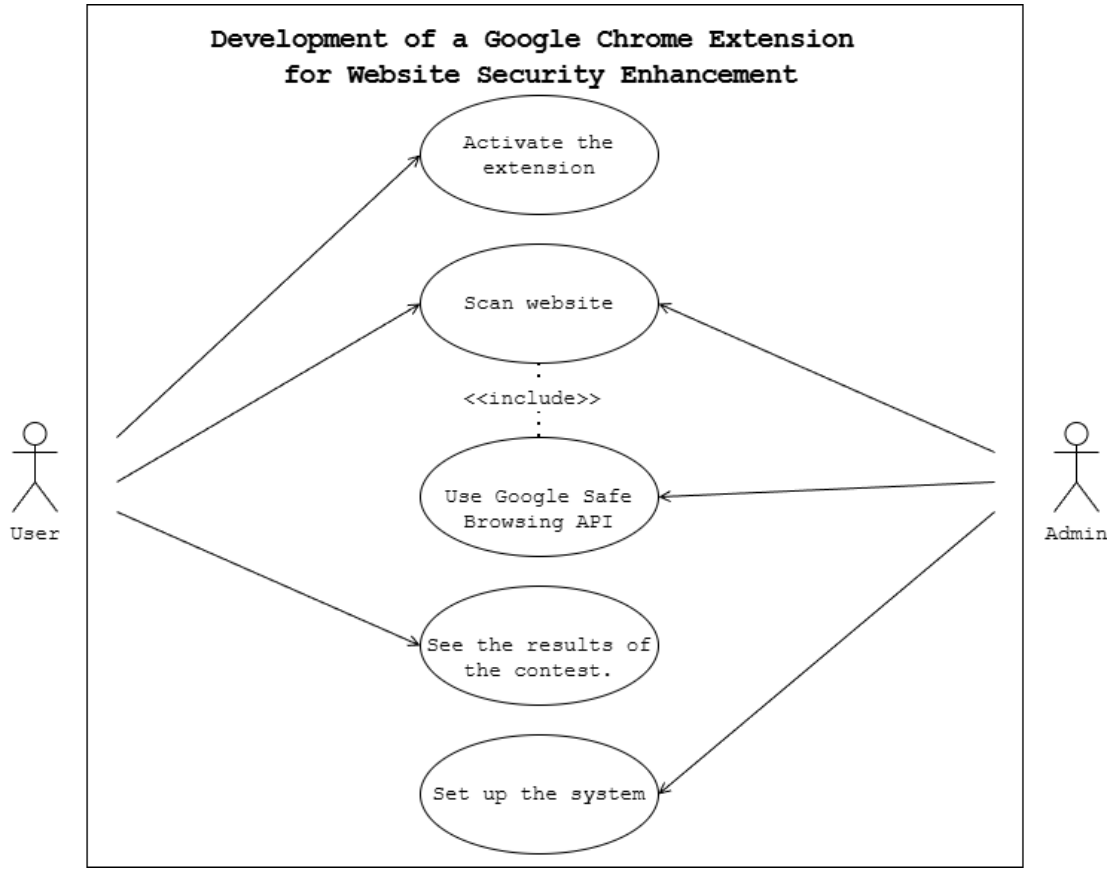
- ระบบจัดเก็บข้อมูลภายใน (Local Storage)



ภาพ 2 System Architecture

2. การออกแบบปฏิสัมพันธ์ของระบบ (Use Case Diagram)

Use Case Diagram ถูกใช้เพื่อกำหนดขอบเขตการทำงานของระบบ (System Boundary) และแสดงบทบาทของผู้เกี่ยวข้อง



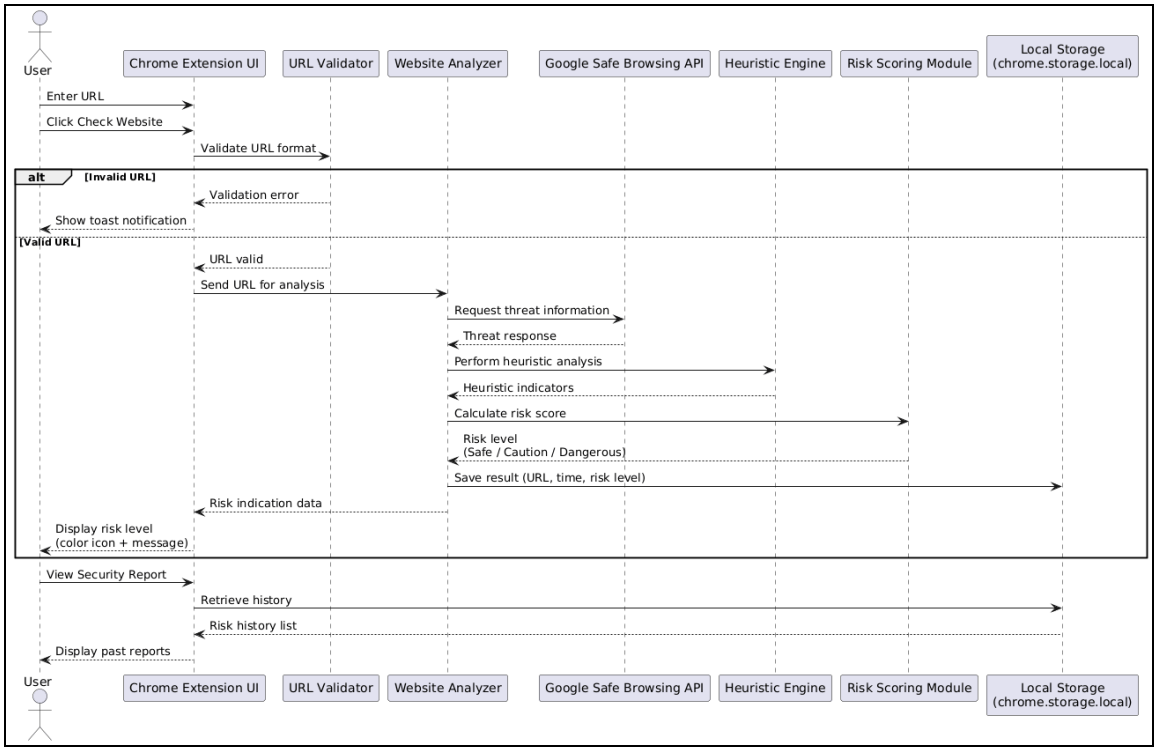
ภาพ 3 Use Case Diagram

จากแผนภาพสามารถอธิบายการทำงานของระบบได้ว่า ผู้ใช้งานทั่วไปสามารถดำเนินการหลัก ได้แก่ การเปิดใช้งานส่วนขยาย การตรวจสอบเว็บไซต์ และการแสดงผลลัพธ์ของการวิเคราะห์ความปลอดภัย ขณะที่ผู้ดูแลระบบมีหน้าที่ในการตั้งค่าระบบและเชื่อมต่อระบบกับบริการภายนอกสำหรับการตรวจสอบภัยคุกคามของเว็บไซต์

นอกจากนี้ กรณีการใช้งาน “การตรวจสอบเว็บไซต์” มีความสัมพันธ์แบบ «include» กับ “การใช้บริการตรวจสอบความปลอดภัยของเว็บไซต์” ซึ่งสะท้อนให้เห็นว่าระบบมีการเรียกใช้แหล่งข้อมูลภายนอกเพื่อสนับสนุนกระบวนการวิเคราะห์ ทำให้ผลลัพธ์มีความถูกต้องและเชื่อถือได้มากยิ่งขึ้น

3. การออกแบบขั้นตอนการทำงานของระบบ (System Workflow)

ผู้วิจัยได้ออกแบบ System Workflow เพื่ออธิบายลำดับขั้นตอนการทำงานของระบบตั้งแต่การรับข้อมูลจนถึงการแสดงผลลัพธ์



ภาพ 4 System Workflow

กระบวนการทำงานของระบบประกอบด้วยขั้นตอนสำคัญ ได้แก่

1. ผู้ใช้ป้อน URL ผ่านส่วนขยาย
2. ระบบตรวจสอบความถูกต้องของ URL (URL Validation)
3. ส่งข้อมูลไปยัง Google Safe Browsing API
4. วิเคราะห์ URL ด้วย Heuristic Analysis ตามแนวคิด OWASP
5. คำนวณระดับความเสี่ยง (Risk Scoring)
6. แสดงผลลัพธ์แก่ผู้ใช้
7. บันทึกข้อมูลเพื่อใช้อ้างอิงย้อนหลัง

Workflow นี้แสดงให้เห็นถึงกระบวนการประมวลผลแบบลำดับขั้น (Sequential Processing) และการวิเคราะห์แบบผสมผสาน (Hybrid Analysis)

4. การออกแบบอัลกอริทึม (Algorithm Design)

ผู้วิจัยได้พัฒนาอัลกอริทึมสำหรับการประเมินความเสี่ยงของเว็บไซต์ โดยอาศัยแนวคิดจาก OWASP Top 10 และการวิเคราะห์เชิงฮิวริสติก

อัลกอริทึมประกอบด้วยขั้นตอนหลัก ได้แก่

- การตรวจสอบความปลอดภัยของโปรโตคอล (HTTP/HTTPS)
- การวิเคราะห์โครงสร้าง URL

- การตรวจจับคำสำคัญที่เกี่ยวข้องกับการโจมตี
- การรวมผลจาก Google Safe Browsing API

โดยมีการกำหนดค่าน้ำหนัก (Weight) ให้กับแต่ละปัจจัย และนำมาคำนวณเป็นคะแนนความเสี่ยง (Risk Score) ก่อนแปลงเป็นระดับความปลอดภัย

แนวทางดังกล่าวถือเป็นการพัฒนา “กลไกการประเมินความเสี่ยงแบบผสมผสาน (Hybrid Risk Assessment Model)” ซึ่งเป็นส่วนสำคัญของนวัตกรรมในงานวิจัยนี้

ขั้นตอนที่ 3 การพัฒนาระบบ (System Implementation)

ในขั้นตอนนี้ ผู้วิจัยดำเนินการพัฒนาระบบส่วนขยายของเว็บเบราว์เซอร์ Google Chrome ตามแบบจำลองและโครงสร้างที่ได้ออกแบบไว้ในขั้นตอนก่อนหน้า โดยมุ่งเน้นให้ระบบสามารถทำงานได้อย่างถูกต้อง มีประสิทธิภาพ และสอดคล้องกับหลักการด้านความมั่นคงปลอดภัย

การพัฒนาระบบแบ่งออกเป็นส่วนประกอบหลัก ดังนี้

1. การพัฒนาส่วนติดต่อผู้ใช้งาน (User Interface: UI)

ออกแบบและพัฒนาอินเทอร์เฟซของส่วนขยายให้ใช้งานง่าย โดยผู้ใช้งานสามารถป้อน URL และสั่งให้ระบบทำการตรวจสอบได้อย่างสะดวก พร้อมทั้งแสดงผลลัพธ์ในรูปแบบที่เข้าใจง่าย เช่น การแสดงระดับความเสี่ยงของเว็บไซต์

2. การพัฒนาโมดูลตรวจสอบความถูกต้องของ URL (URL Validation Module)

ระบบทำการตรวจสอบรูปแบบของ URL ที่ผู้ใช้งานป้อนเข้ามา เพื่อป้องกันข้อผิดพลาดในการประมวลผล และกรองข้อมูลที่ไม่ถูกต้องก่อนเข้าสู่กระบวนการวิเคราะห์

3. การพัฒนาโมดูลวิเคราะห์เว็บไซต์ (Website Analysis Module)

ทำหน้าที่วิเคราะห์เว็บไซต์โดยใช้แนวทางตามหลัก OWASP Top 10 ร่วมกับเทคนิคเชิงเฮูริสติก (Heuristic Analysis) เช่น การตรวจสอบการใช้ HTTPS โครงสร้าง URL และพฤติกรรมที่น่าสงสัยของเว็บไซต์

4. การเชื่อมต่อบริการภายนอก (External API Integration)

ระบบมีการเชื่อมต่อกับ Google Safe Browsing API เพื่อใช้ตรวจสอบข้อมูลภัยคุกคามจากฐานข้อมูลภายนอก ซึ่งช่วยเพิ่มความแม่นยำในการวิเคราะห์และลดความเสี่ยงจากเว็บไซต์อันตราย

5. การพัฒนาโมดูลประเมินความเสี่ยง (Risk Scoring Module)

นำผลลัพธ์จากการวิเคราะห์ภายในระบบและข้อมูลจาก API มาประมวลผลร่วมกันเพื่อคำนวณระดับความเสี่ยงของเว็บไซต์ โดยแบ่งระดับออกเป็น เช่น ปลอดภัย (Safe) เฝ้าระวัง (Caution) และอันตราย (Dangerous)

6. การจัดเก็บข้อมูล (Data Storage)

ระบบมีการจัดเก็บข้อมูลการตรวจสอบเว็บไซต์ในหน่วยความจำภายใน (Local Storage) เพื่อใช้สำหรับการอ้างอิงและปรับปรุงประสิทธิภาพของระบบในอนาคต

ทั้งนี้ ในระหว่างการพัฒนา ผู้วิจัยได้ทำการทดสอบการทำงานของแต่ละโมดูล (Unit Testing) และทดสอบการทำงานร่วมกันของระบบ (Integration Testing) อย่างต่อเนื่อง เพื่อให้มั่นใจว่าระบบสามารถทำงานได้อย่างถูกต้อง ครบถ้วน และมีเสถียรภาพก่อนนำไปใช้ในการทดลองในขั้นตอนถัดไป

ขั้นตอนที่ 4 การออกแบบการทดลอง (Experimental Design)

ในขั้นตอนนี้ ผู้วิจัยได้ออกแบบการทดลองเพื่อประเมินประสิทธิภาพของระบบส่วนขยายที่พัฒนาขึ้น โดยมุ่งเน้นการตรวจสอบความสามารถของระบบในการวิเคราะห์และจำแนกระดับความเสี่ยงของเว็บไซต์ให้มีความถูกต้องและเชื่อถือได้

1. การกำหนดชุดข้อมูลทดสอบ (Test Cases)

ผู้วิจัยกำหนดชุดข้อมูลเว็บไซต์ที่ใช้ในการทดสอบ (Test Cases) โดยแบ่งออกเป็น 3 ประเภท เพื่อให้ครอบคลุมลักษณะของเว็บไซต์ที่แตกต่างกัน ได้แก่

1. เว็บไซต์ที่ปลอดภัย (Safe Websites)
2. เว็บไซต์ที่มีความน่าสงสัย (Suspicious Websites)
3. เว็บไซต์ที่เป็นอันตราย (Malicious Websites)

โดยข้อมูลดังกล่าวอาจรวบรวมจากแหล่งข้อมูลที่เชื่อถือได้ เช่น ฐานข้อมูลด้านความปลอดภัย หรือเว็บไซต์ที่มีการรายงานช่องโหว่ เพื่อใช้เป็นค่าความจริง (Ground Truth) ในการเปรียบเทียบผลลัพธ์ของระบบ

2. ขั้นตอนการดำเนินการทดลอง

การทดลองดำเนินการตามลำดับขั้นตอน ดังนี้

1. นำ URL จากชุดข้อมูลทดสอบเข้าสู่ระบบ
2. ให้ระบบทำการวิเคราะห์เว็บไซต์โดยใช้ทั้ง Google Safe Browsing API และอัลกอริทึมที่พัฒนาขึ้น
3. บันทึกผลลัพธ์การประเมินความเสี่ยงที่ระบบแสดง
4. เปรียบเทียบผลลัพธ์กับค่าความจริง (Ground Truth)
5. สรุปผลการทดลองและจัดเก็บข้อมูลเพื่อใช้ในการวิเคราะห์

3. ตัวชี้วัดในการประเมินผล (Evaluation Metrics)

ผู้วิจัยกำหนดตัวชี้วัดเพื่อประเมินประสิทธิภาพของระบบ ดังนี้

- ความถูกต้อง (Accuracy): วัดความสามารถของระบบในการจำแนกเว็บไซต์ได้ถูกต้องทั้งหมด

- ความแม่นยำ (Precision): วัดความถูกต้องของผลลัพธ์ที่ระบบระบุว่าเป็นเว็บไซต์อันตราย

- ความครอบคลุม (Recall): วัดความสามารถของระบบในการตรวจจับเว็บไซต์อันตรายได้ครบถ้วน

ตัวชี้วัดดังกล่าวช่วยสะท้อนประสิทธิภาพของระบบทั้งในด้านความถูกต้องและความสามารถในการตรวจจับภัยคุกคาม

4. การวิเคราะห์ผลการทดลอง

ผู้วิจัยนำผลลัพธ์ที่ได้จากการทดลองมาวิเคราะห์เชิงสถิติ เพื่อประเมินประสิทธิภาพของระบบ โดยพิจารณาจากค่าตัวชี้วัดต่าง ๆ และเปรียบเทียบกับวัตถุประสงค์ของการวิจัย

นอกจากนี้ ยังมีการวิเคราะห์ข้อผิดพลาดของระบบ (Error Analysis) เพื่อระบุกรณีที่ระบบประเมินผลคลาดเคลื่อน และนำไปใช้เป็นแนวทางในการปรับปรุงอัลกอริทึมให้มีประสิทธิภาพมากยิ่งขึ้น

ขั้นตอนที่ 5 การทดสอบและประเมินผลระบบ

ในขั้นตอนนี้ ผู้วิจัยดำเนินการทดสอบระบบส่วนขยายที่พัฒนาขึ้น เพื่อประเมินประสิทธิภาพการทำงาน ความถูกต้อง และความเหมาะสมในการใช้งานจริง โดยแบ่งการทดสอบออกเป็น 2 ส่วนหลัก ได้แก่

1. การทดสอบการทำงานของระบบ (Functional Testing)

ผู้วิจัยทำการทดสอบการทำงานของแต่ละฟังก์ชันภายในระบบ เพื่อให้มั่นใจว่าสามารถทำงานได้ถูกต้องตามที่ออกแบบไว้ เช่น

- การป้อน URL และการตรวจสอบความถูกต้องของข้อมูล
- การเชื่อมต่อกับ Google Safe Browsing API
- การวิเคราะห์เว็บไซต์และการประเมินระดับความเสี่ยง
- การแสดงผลลัพธ์แก่ผู้ใช้งาน

นอกจากนี้ ยังมีการทดสอบการทำงานร่วมกันของระบบ (Integration Testing) เพื่อให้มั่นใจว่าโมดูลต่าง ๆ สามารถทำงานร่วมกันได้อย่างสมบูรณ์

2. การทดสอบด้านการใช้งาน (Usability Testing)

ผู้วิจัยดำเนินการประเมินความพึงพอใจของผู้ใช้งาน โดยกลุ่มตัวอย่างเป็นนักศึกษาจำนวนที่กำหนด โดยใช้แบบสอบถามในการเก็บข้อมูล

ประเด็นที่ใช้ในการประเมิน ได้แก่

- ความง่ายในการใช้งานของระบบ
- ความรวดเร็วในการประมวลผล
- ความเข้าใจง่ายของการแสดงผล
- ความน่าเชื่อถือของผลลัพธ์

ข้อมูลที่ได้จะถูกนำมาวิเคราะห์เพื่อประเมินคุณภาพของระบบในมุมมองของผู้ใช้งานจริง

ขั้นตอนที่ 6 การวิเคราะห์ผลและสรุปผลการวิจัย

ในขั้นตอนสุดท้าย ผู้วิจัยนำผลลัพธ์ที่ได้จากการทดลองและการประเมินในขั้นตอนก่อนหน้ามาวิเคราะห์และสรุปผลการวิจัย โดยมีรายละเอียดดังนี้

1. การวิเคราะห์ผลการทดลอง

ผู้วิจัยวิเคราะห์ข้อมูลเชิงปริมาณจากค่าตัวชี้วัด ได้แก่ Accuracy, Precision และ Recall เพื่อประเมินประสิทธิภาพของระบบในการตรวจสอบและจำแนกความเสี่ยงของเว็บไซต์ รวมถึงการวิเคราะห์ข้อผิดพลาดของระบบในกรณีที่เกิดการจำแนกคลาดเคลื่อน เพื่อหาสาเหตุและแนวทางในการปรับปรุง

2. การสรุปผลการวิจัย

ผู้วิจัยสรุปผลการพัฒนาระบบ โดยเปรียบเทียบผลลัพธ์ที่ได้กับวัตถุประสงค์ของการวิจัย และประเมินว่าระบบสามารถตอบสนองต่อความต้องการของผู้ใช้งานได้ในระดับใด

ผลการวิจัย

การวิจัยเรื่อง การพัฒนาส่วนขยายบนเว็บเบราว์เซอร์กูเกิล โครม สำหรับประเมินความมั่นคงปลอดภัยของเว็บไซต์ตามแนวทาง OWASP Top 10 มีวัตถุประสงค์ 2 ประการ ได้แก่ (1) เพื่อพัฒนาส่วนขยายบนเว็บเบราว์เซอร์กูเกิล โครม สำหรับประเมินความมั่นคงปลอดภัยของเว็บไซต์ตามแนวทาง OWASP Top 10 และ (2) เพื่อประเมินประสิทธิภาพของส่วนขยาย โดยเปรียบเทียบความสามารถในการตรวจจับเว็บไซต์ที่มีความเสี่ยง และศึกษาความพึงพอใจของผู้ใช้งาน ผู้วิจัยนำเสนอผลการวิจัยตามลำดับวัตถุประสงค์ ดังนี้

1. ผลการพัฒนาส่วนขยายบนเว็บเบราว์เซอร์กูเกิล โครม

ผู้วิจัยได้พัฒนาส่วนขยายบนเว็บเบราว์เซอร์กูเกิล โครม สำหรับประเมินความมั่นคงปลอดภัยของเว็บไซต์ตามแนวทาง OWASP Top 10 โดยส่วนขยายที่พัฒนาขึ้นสามารถทำงานได้บนเบราว์เซอร์ Google Chrome และมีฟังก์ชันการตรวจจับเว็บไซต์อันตรายแบบเรียลไทม์ ครอบคลุมช่องโหว่ตามมาตรฐาน OWASP Top 10 ซึ่งเป็นกรอบอ้างอิงด้านความมั่นคงปลอดภัยเว็บไซต์ที่ได้รับการยอมรับในระดับสากล

2. ผลการประเมินประสิทธิภาพของส่วนขยาย

การประเมินประสิทธิภาพของส่วนขยายแบ่งออกเป็น 2 ส่วน ได้แก่ ข้อมูลทั่วไปของกลุ่มตัวอย่าง และผลการศึกษาความพึงพอใจของผู้ใช้งาน โดยมีรายละเอียดดังนี้

2.1 ข้อมูลทั่วไปของกลุ่มตัวอย่าง

ตาราง 1 ข้อมูลส่วนบุคคลของนักศึกษาที่ใช้ส่วนขยายด้านความมั่นคงปลอดภัยของเว็บไซต์บน Google Chrome (n = 50)

สถานภาพ	จำนวน	ร้อยละ
1. เพศ		
1. ชาย	18	36.00
2. หญิง	31	62.00
3. อื่น ๆ	1	2.00
รวม	50	100.00
2. อายุ		
10 – 12 ปี	14	28.00
13 – 15 ปี	19	38.00
16 – 18 ปี	17	34.00
รวม	50	100.00
3. ระดับชั้น		
ประถมศึกษาตอนปลาย (ป.4–ป.6)	14	28.00
มัธยมศึกษาตอนต้น (ม.1–ม.3)	19	38.00
มัธยมศึกษาตอนปลาย (ม.4–ม.6)	17	34.00
รวม	50	100.00
4. ระยะเวลาใช้อินเทอร์เน็ตเฉลี่ยต่อวัน		
น้อยกว่า 2 ชั่วโมง	9	18.00
2 – 4 ชั่วโมง	22	44.00
4 – 6 ชั่วโมง	14	28.00
มากกว่า 6 ชั่วโมง	5	10.00
รวม	50	100.00

จากตาราง 1 พบว่า กลุ่มตัวอย่างในการวิจัย จำนวน 50 คน เป็นเพศหญิงมากที่สุด คิดเป็นร้อยละ 62.00 รองลงมาคือ เพศชาย คิดเป็นร้อยละ 36.00 กลุ่มตัวอย่างส่วนใหญ่อยู่ในช่วงอายุ 13-15 ปี คิดเป็นร้อยละ 38.00 และกำลังศึกษาอยู่ในระดับ มัธยมศึกษาตอนต้น (ม.1-ม.3) มากที่สุด คิดเป็นร้อยละ 38.00 นอกจากนี้ กลุ่มตัวอย่างส่วนใหญ่มีระยะเวลาใช้งานอินเทอร์เน็ตเฉลี่ย 2-4 ชั่วโมงต่อวัน คิดเป็นร้อยละ 44.00

2.2 ผลการศึกษาความพึงพอใจของผู้ใช้งานต่อส่วนขยาย

ผู้วิจัยได้ศึกษาความพึงพอใจของผู้ใช้งานแบ่งออกเป็น 2 กลุ่ม ได้แก่ กลุ่มนักเรียนโรงเรียนเอกชนแห่งหนึ่ง จำนวน 50 คน และกลุ่มผู้เชี่ยวชาญ จำนวน 5 คน

2.2.1 ความพึงพอใจของกลุ่มนักเรียน (n = 50)

ตาราง 2 ปัจจัยที่มีอิทธิพลต่อการใช้ส่วนขยายด้านความมั่นคงปลอดภัยของเว็บไซต์บน Google Chrome ของนักเรียนโรงเรียนเอกชนแห่งหนึ่ง

ด้านที่	รายการ	$\dot{X}$	SD	แปลค่า	อันดับ
1	ด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์	3.90	0.64	มาก	10
2	ด้านการตระหนักถึงความสำคัญของความปลอดภัยออนไลน์	4.07	0.63	มาก	6
3	ด้านทัศนคติที่มีต่อการใช้ส่วนขยายด้านความมั่นคงปลอดภัย	4.19	0.65	มาก	5
4	ด้านภาพลักษณ์และความน่าเชื่อถือของส่วนขยาย	4.25	0.58	มาก	1
5	ด้านความเชื่อมั่นในผลการตรวจสอบและการแจ้งเตือน	3.97	0.63	มาก	9
6	ด้านคุณสมบัติและฟังก์ชันของส่วนขยาย	4.03	0.60	มาก	8
7	ด้านความคุ้มค่า/ประโยชน์ต่อการเรียนรู้และใช้งานจริง	4.14	0.68	มาก	3
8	ด้านความสะดวกในการติดตั้งและการเข้าถึงผ่าน Chrome Web Store	4.23	0.64	มาก	2
9	ด้านการประชาสัมพันธ์หรือคำแนะนำจากครู/เพื่อน	4.05	0.60	มาก	7
10	ด้านการสนับสนุนจากโรงเรียนในการใช้ส่วนขยายเป็นเครื่องมือเรียนรู้	4.12	0.59	มาก	4
	รวม	4.09	0.48	มาก	

จากตาราง 2 พบว่า ปัจจัยที่มีอิทธิพลต่อการใช้ส่วนขยายด้านความมั่นคงปลอดภัยของเว็บไซต์บน Google Chrome ของนักเรียนโรงเรียนเอกชนแห่งหนึ่ง โดยภาพรวมมีค่าเฉลี่ยเท่ากับ 4.09 อยู่ในระดับมาก เมื่อพิจารณาเป็นรายด้าน พบว่า ด้านที่มีค่าเฉลี่ยสูงที่สุด คือ ด้านภาพลักษณ์และความน่าเชื่อถือของส่วนขยาย มีค่าเฉลี่ยเท่ากับ 4.25 (S.D. = 0.58) อยู่ในระดับมาก รองลงมาคือ ด้านความสะดวกในการติดตั้งและการเข้าถึงผ่าน Chrome Web Store มีค่าเฉลี่ยเท่ากับ 4.23 (S.D. = 0.64) และ

ด้านความคุ้มค่า/ประโยชน์ต่อการเรียนรู้และใช้งานจริง มีค่าเฉลี่ยเท่ากับ 4.14 (S.D. = 0.68) ตามลำดับ ส่วนด้านที่มีค่าเฉลี่ยต่ำที่สุด คือ ด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ มีค่าเฉลี่ยเท่ากับ 3.90 (S.D. = 0.64) แต่ยังคงอยู่ในระดับมากเช่นกัน

2.2.2 ความพึงพอใจของกลุ่มผู้เชี่ยวชาญ (n = 5)

ตาราง 3 ปัจจัยที่มีอิทธิพลต่อการใช้ส่วนขยายด้านความมั่นคงปลอดภัยของเว็บไซต์บน Google Chrome ของผู้เชี่ยวชาญ จำนวน 5 คน

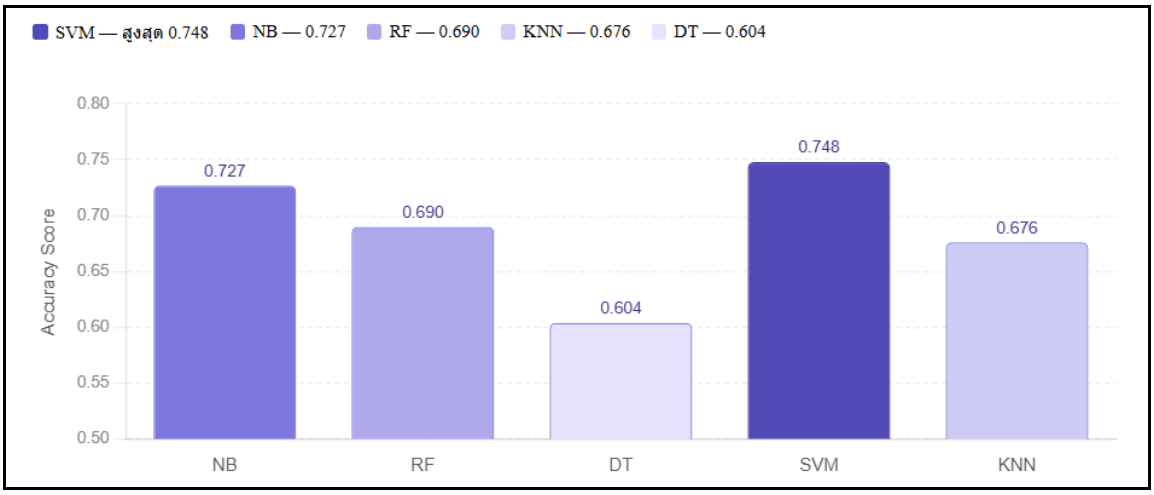
ด้านที่	รายการ	$\dot{X}$	SD	แปลค่า	อันดับ
1	ด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์	4.32	0.52	มากที่สุด	2
2	ด้านการตระหนักถึงความสำคัญของความปลอดภัยออนไลน์	4.41	0.50	มากที่สุด	1
3	ด้านทัศนคติที่มีต่อการใช้ส่วนขยายด้านความมั่นคงปลอดภัย	4.05	0.63	มาก	6
4	ด้านภาพลักษณ์และความน่าเชื่อถือของส่วนขยาย	3.88	0.70	มาก	9
5	ด้านความเชื่อมั่นในผลการตรวจสอบและการแจ้งเตือน	4.12	0.60	มาก	4
6	ด้านคุณสมบัติและฟังก์ชันของส่วนขยาย	4.08	0.55	มาก	5
7	ด้านความคุ้มค่า/ประโยชน์ต่อการเรียนรู้และใช้งานจริง	3.95	0.66	มาก	8
8	ด้านความสะดวกในการติดตั้งและการเข้าถึงผ่าน Chrome Web Store	3.91	0.72	มาก	10
9	ด้านการประชาสัมพันธ์หรือคำแนะนำจากครู/เพื่อน	4.01	0.58	มาก	7
10	ด้านการสนับสนุนจากโรงเรียนในการใช้ส่วนขยายเป็นเครื่องมือเรียนรู้	4.18	0.54	มาก	3
	รวม	4.09	0.46	มาก	

จากตาราง 3 พบว่า ปัจจัยที่มีอิทธิพลต่อการใช้ส่วนขยายด้านความมั่นคงปลอดภัยของเว็บไซต์บน Google Chrome ของกลุ่มผู้เชี่ยวชาญ โดยภาพรวมมีค่าเฉลี่ยเท่ากับ 4.09 อยู่ในระดับมาก เมื่อพิจารณาเป็นรายด้าน พบว่า ด้านที่มีค่าเฉลี่ยสูงที่สุด คือ ด้านการตระหนักถึงความสำคัญของความปลอดภัยออนไลน์ มีค่าเฉลี่ยเท่ากับ 4.41 (S.D. = 0.50) อยู่ในระดับมากที่สุด รองลงมาคือ ด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ มีค่าเฉลี่ยเท่ากับ 4.32 (S.D. = 0.52) อยู่ในระดับมากที่สุด ส่วนด้านที่มีค่าเฉลี่ยต่ำ

ที่สุด คือ ด้านความสะดวกในการติดตั้งและการเข้าถึงผ่าน Chrome Web Store มีค่าเฉลี่ยเท่ากับ 3.91 (S.D. = 0.72) แต่ยังคงอยู่ในระดับมากเช่นกัน

2.2.3 การเปรียบเทียบระหว่างสองกลุ่ม

เมื่อเปรียบเทียบผลการประเมินระหว่างกลุ่มนักเรียนและกลุ่มผู้เชี่ยวชาญ พบว่า ทั้งสองกลุ่มมีค่าเฉลี่ยโดยรวมเท่ากัน คือ 4.09 อยู่ในระดับมากเท่ากัน แสดงให้เห็นว่าส่วนขยายที่พัฒนาขึ้นมีความเหมาะสมและสามารถตอบสนองความต้องการของผู้ใช้งานทั้งในกลุ่มนักเรียนและผู้เชี่ยวชาญได้ในระดับที่สอดคล้องกัน อย่างไรก็ตาม กลุ่มผู้เชี่ยวชาญให้ความสำคัญกับด้านการตระหนักรู้และความรู้เรื่องภัยไซเบอร์มากกว่า ขณะที่กลุ่มนักเรียนให้ความสำคัญกับด้านภาพลักษณ์และความน่าเชื่อถือของส่วนขยายมากกว่า ซึ่งสะท้อนถึงความแตกต่างของมุมมองระหว่างผู้ใช้งานทั่วไปและผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์



ภาพ 5 Accuracy

จากภาพพบว่า อัลกอริทึม Support Vector Machine (SVM) มีค่าความแม่นยำสูงที่สุดเท่ากับ 0.748 รองลงมาคือ อัลกอริทึม Naive Bayes (NB) มีค่าความแม่นยำเท่ากับ 0.727 อัลกอริทึม Random Forest (RF) มีค่าความแม่นยำเท่ากับ 0.690 อัลกอริทึม K-Nearest Neighbors (KNN) มีค่าความแม่นยำเท่ากับ 0.676 และอัลกอริทึม Decision Tree (DT) มีค่าความแม่นยำต่ำที่สุดเท่ากับ 0.604 ตามลำดับ

เมื่อพิจารณาเปรียบเทียบผลการทดสอบของอัลกอริทึมทั้ง 5 ตัว พบว่า SVM มีค่าความแม่นยำสูงกว่าอัลกอริทึมอื่น ๆ ทุกตัว โดยสูงกว่า NB อยู่ร้อยละ 2.1 สูงกว่า RF อยู่ร้อยละ 5.8 สูงกว่า KNN อยู่ร้อยละ 7.2 และสูงกว่า DT อยู่ร้อยละ 14.4 ตามลำดับ ทั้งนี้ อัลกอริทึม DT มีค่าความแม่นยำต่ำที่สุด ซึ่งอาจเนื่องมาจากลักษณะของข้อมูลที่ใช้ในการฝึกอบรมมีความซับซ้อนและมีมิติข้อมูลสูง ทำให้ Decision Tree เกิดปัญหา Overfitting ได้ง่ายกว่าอัลกอริทึมอื่น

ดังนั้น ผู้วิจัยจึงเลือกนำอัลกอริทึม Support Vector Machine (SVM) มาใช้เป็นโมเดลหลักในส่วนขยาย Google Chrome เพื่อตรวจจับเว็บไซต์อันตราย เนื่องจากให้ค่าความแม่นยำสูงที่สุดในการจำแนกประเภทของเว็บไซต์ระหว่างเว็บไซต์อันตรายและเว็บไซต์ปลอดภัย ซึ่งสอดคล้องกับแนวคิดของ Cortes and Vapnik (1995) ที่ระบุว่า SVM มีประสิทธิภาพสูงในงานจำแนกประเภทข้อมูลที่มีลักษณะไม่เป็นเชิงเส้น (Non-linear Classification)

สรุปผลการวิจัย

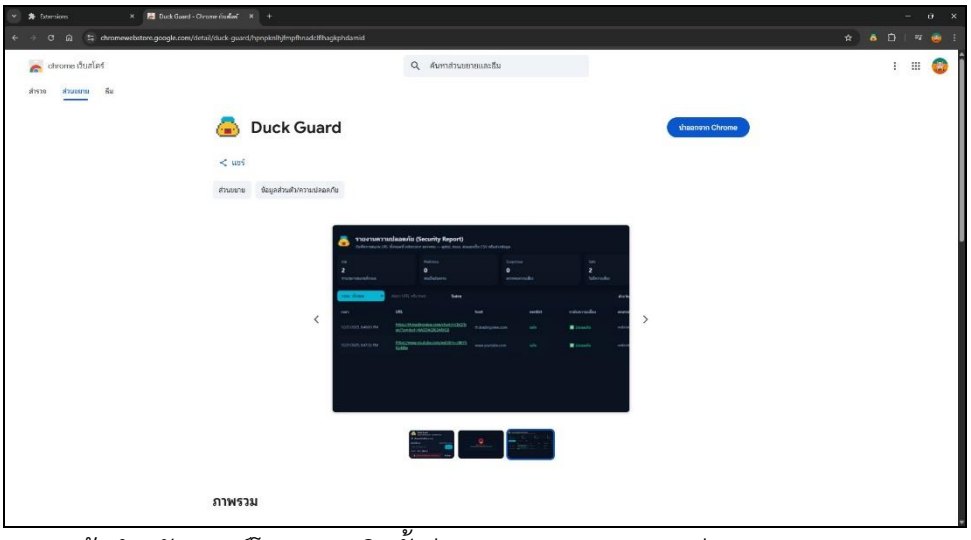
การวิจัยเรื่อง การพัฒนาส่วนขยายด้านความมั่นคงปลอดภัยของเว็บไซต์บน Google Chrome มีวัตถุประสงค์เพื่อพัฒนาระบบสำหรับบ่งชี้ความเสี่ยงของเว็บไซต์จากมุมมองผู้ใช้งานทั่วไป และประเมินประสิทธิภาพรวมถึงความเหมาะสมของระบบจากทั้งผู้ใช้งานและผู้เชี่ยวชาญ ผลการวิจัยสามารถสรุปได้ดังนี้

1. ในด้านประสิทธิภาพของระบบตามความคิดเห็นของผู้ใช้งานทั่วไป พบว่า ภาพรวมอยู่ในระดับมาก โดยผู้ใช้งานเห็นว่าระบบมีความสะดวกต่อการติดตั้งและใช้งาน สามารถเข้าใจผลการประเมินได้ง่าย และไม่ก่อให้เกิดความซับซ้อนในการใช้งานประจำวัน สะท้อนให้เห็นว่าการออกแบบส่วนขยายในลักษณะ Client-side ที่แสดงผลแบบทันที (Real-time) สามารถตอบสนองพฤติกรรมการใช้งานอินเทอร์เน็ตของนักเรียนได้อย่างเหมาะสม

2. ในด้านความเหมาะสมของระบบตามความคิดเห็นของผู้เชี่ยวชาญ พบว่า ระบบได้รับการประเมินในระดับมากเช่นกัน โดยเฉพาะด้านการตระหนักถึงความสำคัญของความปลอดภัยออนไลน์และแนวคิดการประยุกต์ใช้กรอบ OWASP Top 10 เพื่อบ่งชี้ความเสี่ยงเบื้องต้น แสดงให้เห็นว่าระบบมีความสอดคล้องกับหลักการด้านความมั่นคงปลอดภัยไซเบอร์ในเชิงแนวคิด แม้ว่าจะไม่ได้เป็นเครื่องมือสำหรับตรวจสอบช่องโหว่เชิงลึก

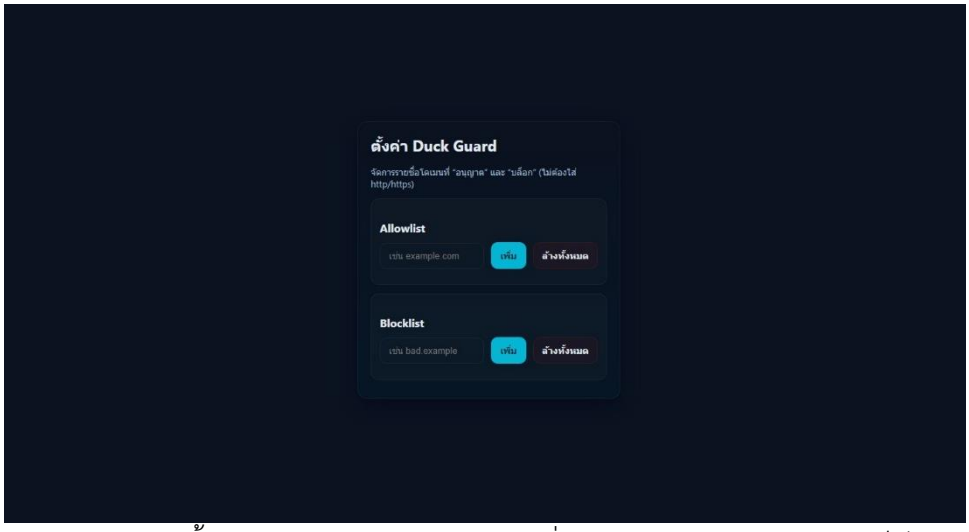
3. เมื่อพิจารณาปัจจัยที่มีอิทธิพลต่อการใช้ส่วนขยาย พบว่า ด้านภาพลักษณ์และความน่าเชื่อถือของระบบ รวมถึงความสะดวกในการติดตั้งและเข้าถึง มีค่าเฉลี่ยอยู่ในระดับสูง สะท้อนว่าความเชื่อมั่นต่อเครื่องมือมีบทบาทสำคัญต่อการยอมรับเทคโนโลยี ขณะที่ด้านความรู้เกี่ยวกับภัยคุกคามไซเบอร์มีค่าเฉลี่ยต่ำกว่าด้านอื่น แม้อยู่ในระดับมาก แสดงให้เห็นว่ายังมีช่องว่างด้านองค์ความรู้พื้นฐานของผู้ใช้งาน

โดยสรุป ระบบที่พัฒนาขึ้นสามารถดำเนินการได้ตามวัตถุประสงค์ที่กำหนด มีประสิทธิภาพและความเหมาะสมในระดับมากทั้งจากมุมมองผู้ใช้งานและผู้เชี่ยวชาญ และสามารถทำหน้าที่เป็นเครื่องมือสนับสนุนการตัดสินใจก่อนเข้าถึงเว็บไซต์ได้ในบริบทของสถานศึกษา อย่างไรก็ตาม การประเมินครั้งนี้เป็นการประเมินเชิงการรับรู้ของผู้ใช้งาน มิใช่การทดสอบประสิทธิภาพเชิงเทคนิคในระดับการตรวจสอบช่องโหว่เชิงลึก

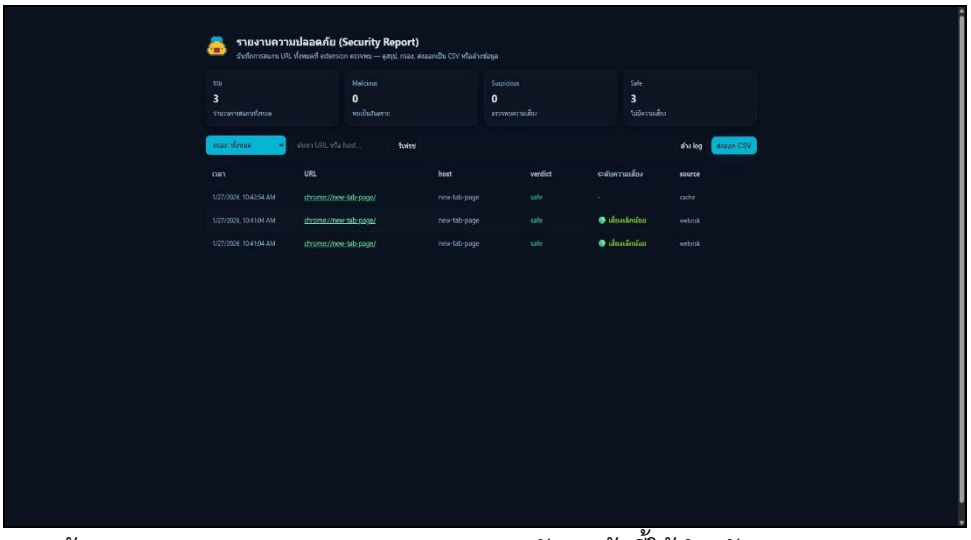


ภาพ 6 หน้าสำหรับดาวน์โหลดและติดตั้งส่วนขยาย (Extension) ผ่าน Chrome Web Store เพื่อให้ผู้ใช้งานสามารถเข้าถึงและติดตั้งซอฟต์แวร์ลงบนเบราว์เซอร์

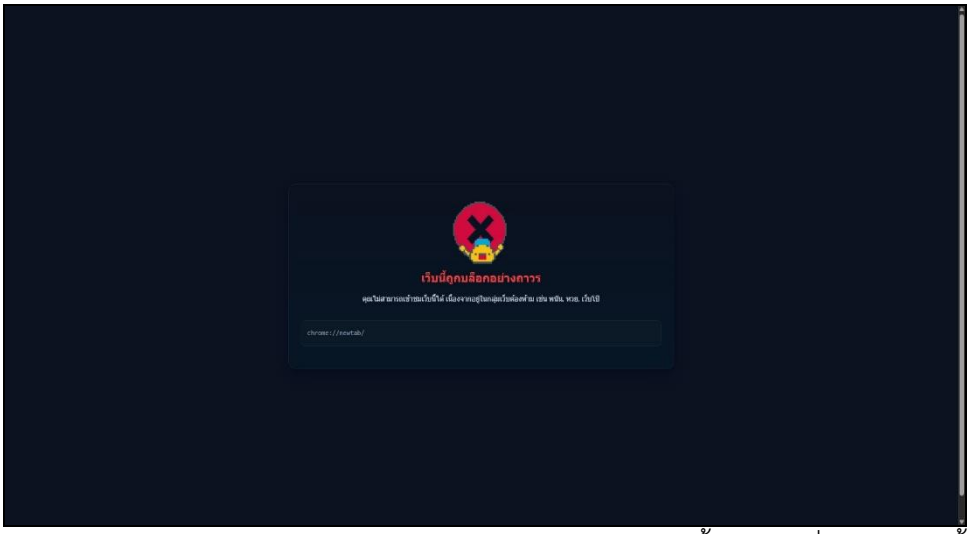
ภาพ7 หน้า Popup UI ของส่วนขยาย (Extension) ที่ผู้ใช้จะเห็นเมื่อกดที่ไอคอนโปรแกรมบนแถบเครื่องมือครับ มีองค์ประกอบหลัก



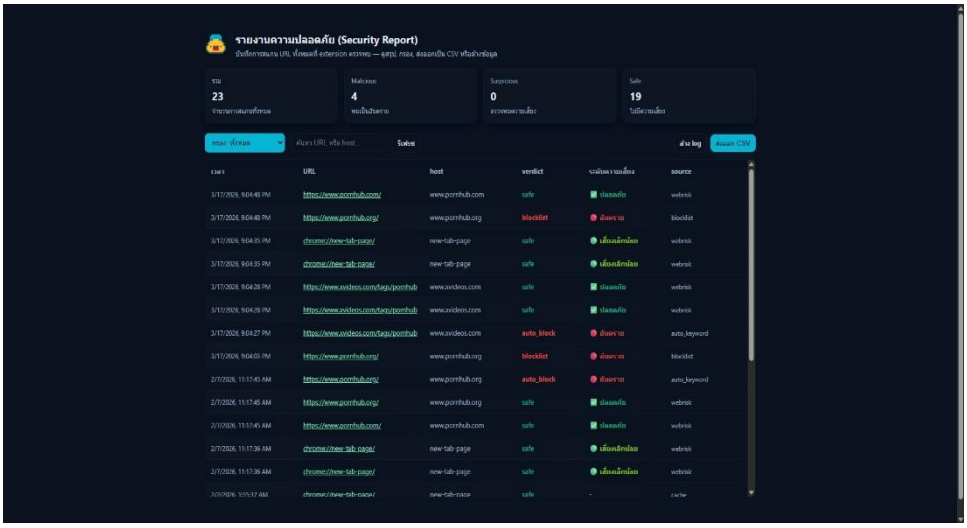
ภาพ 8 หน้า Settings (ตั้งค่า) ของ Duck Guard มีหน้าที่หลักคือ "การจัดการรายการเว็บไซต์" เพื่อให้ผู้ใช้กำหนดสิทธิ์การเข้าถึงด้วยตนเองครับ โดยแบ่งเป็น 2 ส่วนหลัก Allowlist (รายการที่อนุญาต), Blocklist (รายการที่บล็อก)



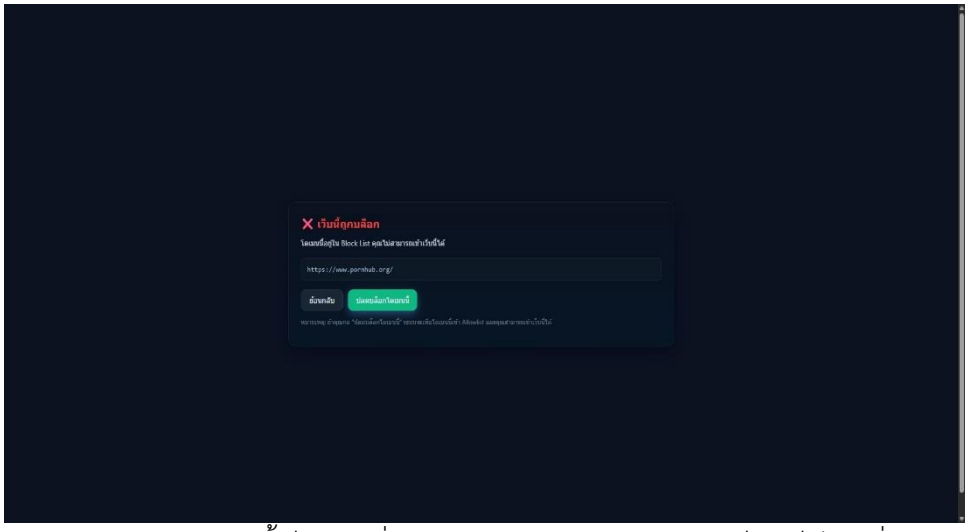
ภาพ 9 หน้า Security Report (รายงานความปลอดภัย) หน้านี้ใช้สำหรับ แสดงผลการตรวจสอบเว็บไซต์ทั้งหมดที่ผู้ใช้เข้าถึงผ่าน Extension เพื่อให้ผู้ใช้และผู้ดูแลระบบสามารถ ติดตาม ตรวจสอบ และประเมินความปลอดภัยของการใช้งานอินเทอร์เน็ต



ภาพ 10 หน้า Blocked Page (หน้าแจ้งการบล็อกเว็บไซต์) หน้านี้เป็นหน้าที่ระบบแสดงขึ้น เมื่อผู้ใช้พยายามเข้าถึงเว็บไซต์ที่ถูกจัดอยู่ในกลุ่มต้องห้ามหรือมีความเสี่ยง โดย Chrome Extension จะทำการ ป้องกันการเข้าถึงทันที และแจ้งเตือนผู้ใช้แทนการเปิดเว็บไซต์นั้น



ภาพ 11 หน้ารายงานความปลอดภัย (Security Report) ของระบบ/ส่วนขยาย (extension) ที่ใช้ตรวจสอบเว็บไซต์ที่คุณเข้าไป



ภาพ 12 หน้า Blacklist หน้านี้เป็นหน้าที่ระบบความปลอดภัยใช้ในการบล็อกเว็บไซต์ที่อยู่ในบัญชีดำ (Blacklist) เพื่อป้องกันผู้ใช้จากเว็บไซต์ที่อาจเป็นอันตราย โดยจะแสดงข้อความแจ้งเตือน และให้ผู้ใช้เลือกว่าจะย้อนกลับหรือปลดบล็อกเว็บไซต์ดังกล่าว

อภิปรายผล

ผลการวิจัยสะท้อนให้เห็นว่า ปัจจัยด้านความสะดวกในการใช้งานและความน่าเชื่อถือของระบบมีอิทธิพลอย่างมีนัยสำคัญต่อการยอมรับส่วนขยายด้านความมั่นคงปลอดภัย ซึ่งสอดคล้องกับแนวคิดด้านการยอมรับเทคโนโลยี (Technology Acceptance Model: TAM) ที่ระบุว่า ผู้ใช้จะมีแนวโน้มยอมรับและใช้งานระบบมากขึ้น หากระบบนั้นใช้งานง่าย ไม่ซับซ้อน และไม่เพิ่มภาระทางเทคนิคให้กับผู้ใช้มากเกินไป

ในบริบทของนักเรียนซึ่งมีพื้นฐานความรู้ด้านความมั่นคงปลอดภัยแตกต่างกัน การออกแบบที่เน้นความเรียบง่าย และการแสดงผลในรูปแบบสัญลักษณ์สี (Color Indicator) เช่น สีเขียว สีเหลือง และสีแดง ถือเป็นกลไกที่ช่วยลดภาระทางการรับรู้ (Cognitive Load) และสนับสนุนการตัดสินใจของผู้ใช้งานได้อย่างมีประสิทธิภาพ

นอกจากนี้ การที่ผู้เชี่ยวชาญประเมินระบบในระดับมาก โดยเฉพาะด้านการตระหนักถึงความสำคัญของความปลอดภัยออนไลน์ สะท้อนให้เห็นว่าการนำกรอบ OWASP Top 10 มาประยุกต์ใช้ในลักษณะการบ่งชี้ความเสี่ยงจากฝั่งผู้ใช้งาน (Client-side Risk Indication) เป็นแนวทางที่มีความเหมาะสมในเชิงแนวคิด โดยเฉพาะในประเด็นที่เกี่ยวข้องกับภัยคุกคาม เช่น Phishing, Malicious URL และการเข้าถึงเว็บไซต์ที่มีความเสี่ยง ซึ่งสอดคล้องกับแนวทางการป้องกันเชิงรุก (Preventive Security) ตามหลักการของ OWASP

อย่างไรก็ตาม เมื่อพิจารณาร่วมกับผลการทดสอบเชิงเทคนิค พบว่าระบบมีค่าความถูกต้อง (Accuracy) อยู่ในระดับสูง (ร้อยละ 93.33) ซึ่งแสดงให้เห็นว่าระบบสามารถตรวจจับเว็บไซต์ที่มีความเสี่ยง

ได้อย่างครอบคลุม โดยเฉพาะในมิติของความมั่นคงปลอดภัย ค่า Recall ที่สูงมีความสำคัญ เนื่องจากช่วยลดโอกาสของการตรวจจับไม่พบ (False Negative) ซึ่งถือเป็นความเสี่ยงสำคัญตามแนวคิดของ OWASP

เมื่อเปรียบเทียบกับวิธีการเดิมที่ผู้ใช้งานต้องประเมินความน่าเชื่อถือของเว็บไซต์ด้วยตนเอง หรืออาศัยเพียงประสบการณ์ส่วนบุคคล พบว่า ระบบที่พัฒนาขึ้นสามารถช่วยลดความผิดพลาดจากมนุษย์ (Human Error) และเพิ่มความสามารถในการตัดสินใจได้อย่างมีนัยสำคัญ ผ่านการตรวจสอบแบบอัตโนมัติและการแจ้งเตือนแบบเรียลไทม์ ซึ่งถือเป็นข้อได้เปรียบเชิงระบบเมื่อเทียบกับแนวทางแบบดั้งเดิม

อย่างไรก็ตาม ผลคะแนนด้านความรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่ต่ำกว่าปัจจัยอื่น แม้ยังอยู่ในระดับมาก สะท้อนถึงข้อจำกัดเชิงพฤติกรรมของผู้ใช้งาน กล่าวคือ แม้ระบบสามารถแจ้งเตือนความเสี่ยงได้ แต่หากผู้ใช้ขาดความเข้าใจพื้นฐานเกี่ยวกับลักษณะภัยคุกคาม เช่น ฟิชชิง มัลแวร์ หรือเว็บไซต์ปลอม ก็อาจไม่สามารถตีความหรือให้ความสำคัญกับคำเตือนได้อย่างเต็มที่

ประเด็นนี้ชี้ให้เห็นว่า เทคโนโลยีด้านความมั่นคงปลอดภัยไม่ควรถูกใช้เป็นเพียงเครื่องมือป้องกัน (Protection Tool) เท่านั้น แต่ควรพัฒนาให้เป็น “เครื่องมือส่งเสริมการเรียนรู้” (Educational Tool) ที่ช่วยสร้าง Cybersecurity Awareness ควบคู่กันไป ซึ่งสอดคล้องกับแนวคิดการเรียนรู้เชิงพฤติกรรม (Behavioral Learning) ที่เน้นการเรียนรู้จากสถานการณ์จริง

อีกทั้ง การที่ด้านการสนับสนุนจากสถานศึกษามีค่าเฉลี่ยในระดับมาก แสดงให้เห็นว่าบริบทของโรงเรียนมีบทบาทสำคัญในการส่งเสริมการใช้งานเทคโนโลยีด้านความมั่นคงปลอดภัย การบูรณาการส่วนขยายเข้ากับการเรียนการสอนหรือกิจกรรมด้านดิจิทัล สามารถช่วยเพิ่มระดับการยอมรับและความตระหนักรู้ของผู้เรียนได้อย่างเป็นระบบ

ดังนั้น ผลการวิจัยจึงชี้ให้เห็นว่า ส่วนขยายที่พัฒนาขึ้นมีศักยภาพในการเป็นทั้ง “เครื่องมือด้านความมั่นคงปลอดภัย” และ “นวัตกรรมด้านการเรียนรู้” โดยช่วยสนับสนุนการตัดสินใจของผู้ใช้งาน และลดความเสี่ยงจากการเข้าถึงเว็บไซต์อันตราย อย่างไรก็ตาม การเพิ่มประสิทธิผลในระยะยาวจำเป็นต้องดำเนินควบคู่กับการพัฒนาความรู้และทักษะด้านความมั่นคงปลอดภัยของผู้ใช้งาน เพื่อให้เกิดความยั่งยืนทั้งในเชิงเทคโนโลยีและพฤติกรรม

ข้อเสนอแนะ

1. ควรพัฒนาฟังก์ชันเพิ่มเติมของส่วนขยาย เช่น การแสดงรายละเอียดความเสี่ยงของเว็บไซต์ในรูปแบบที่เข้าใจง่าย เพื่อช่วยให้ผู้ใช้งานตัดสินใจได้รวดเร็วขึ้น

2. ควรต่อยอดงานวิจัยโดยนำเทคนิค Machine Learning มาวิเคราะห์พฤติกรรมของเว็บไซต์เพื่อเพิ่มความสามารถในการตรวจจับภัยคุกคามรูปแบบใหม่ (Zero-day Attack)

3. ควรขยายการทดลองด้วยชุดข้อมูลเว็บไซต์ที่หลากหลายและมีขนาดใหญ่ขึ้น เพื่อเพิ่มความแม่นยำและความน่าเชื่อถือของระบบ

4. ควรศึกษาผลกระทบของระบบต่อพฤติกรรมผู้ใช้งานในระยะยาว เพื่อประเมินการเปลี่ยนแปลงด้านการใช้งานอินเทอร์เน็ตอย่างปลอดภัย

เอกสารอ้างอิง

Cybersecurity Thailand. (2566). *รายงานสถานการณ์ภัยคุกคามไซเบอร์ประเทศไทย ประจำปี 2566.* สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA).

กรมพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม. (2567). *การพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงขององค์กร.* กรุงเทพมหานคร: กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

ภัทราพร อินทรศรี. (2565). *ปัจจัยที่ส่งผลต่อการตระหนักและการใช้เทคโนโลยีความมั่นคงปลอดภัยทางไซเบอร์.* มหาวิทยาลัยเกษตรศาสตร์.

ราชกิจจานุเบกษา. (2560). *พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560.* กรุงเทพมหานคร: สำนักเลขาธิการคณะรัฐมนตรี.

ราชกิจจานุเบกษา. (2562). *พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.* กรุงเทพมหานคร: สำนักเลขาธิการคณะรัฐมนตรี.

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ. (2565). *รายงานแนวโน้มภัยคุกคามและมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย.* กรุงเทพมหานคร: กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

National Cyber Security Agency. (2024). *Thailand Cybersecurity Strategy 2024-2027.* สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ.

Getachew, A., & Teshome, D. (2022). Cybersecurity vulnerabilities and solutions in Ethiopian university websites. *International Journal of Information Security Science,* 11(1), 25-39.

Kim, H., & Park, J. (2023). Enhancing web application security through automated penetration testing with multiple vulnerability scanners. *Computers & Security,* 124, 103031.

Nguyen, T., & Chen, L. (2022). A systematic review of cybersecurity assessment methods for HTTPS. *Journal of Network and Computer Applications,* 202, 103358.

Alqahtani, S., & Hammad, M. (2021). Detecting phishing websites using machine learning techniques. *International Journal of Advanced Computer Science and Applications,* 12(6), 45-52.

Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. *Expert Systems with Applications,* 117, 345-357.

OWASP Foundation. (2021). *OWASP Top 10: The Ten Most Critical Web Application Security Risks.* https://owasp.org/www-project-top-ten/

Google. (2024). *Google Chrome usage statistics.* https://www.google.com