รายงานวิจัยฉบับสมบูรณ์

การพัฒนาระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม
Mini SIEM Cybersecurity Monitoring System

โดย

นายดนย์บวรภัทร มีกุญชร สำนักหอสมุด

ได้รับการสนับสนุนทุนโครงการวิจัยสถาบัน มหาวิทยาลัยขอนแก่น
ประจำปีงบประมาณ 2566
ตุลาคม พ.ศ. 2566

บทคัดย่อ

สำนักหอสมุดมีบริการออนไลน์บนเว็บไซต์เป็นจำนวนมาก ทั้งให้บริการแก่ผู้ใช้และบุคลากรของหน่วยงาน เพื่อให้การบริหารจัดการและการบริการเกิดประสิทธิภาพสูงที่สุด ช่วงหลายปีที่ผ่านมาเว็บไซต์ของหน่วยงานถูก Hacker โจมตีบ่อยครั้ง แต่ผู้ดูแลระบบหรือผู้ดูแลเว็บไซต์ ไม่อาจทราบได้เลยว่าเว็บไซต์กำลังถูกโจมตี จนกว่า Hacker จะเปลี่ยนแปลงรูปภาพ ข้อความ หรือแทรกลิงก์ (link) เว็บการพนันบนเว็บไซต์แล้ว

ดังนั้นผู้วิจัยจึงเกิดแนวคิดที่จะพัฒนาแอปพลิเคชันขึ้นมา วัตถุประสงค์เพื่อช่วยตรวจสอบการถูกโจมตี เจาะช่องโหว่เว็บไซต์ของหน่วยงาน และแจ้งเตือนไปยังผู้ดูแลระบบให้รับทราบถึงช่องโหว่เพื่อจะได้ตรวจสอบ และแจ้งไปยังผู้ดูแลเว็บไซต์ให้ดำเนินการแก้ไข ปิดช่องโหว่ ได้ในทันที และเพื่อลดจำนวนการถูกโจมตี เจาะช่องโหว่ลง 20%

วิธีดำเนินการ เริ่มจากการเก็บรวบรวมข้อมูลล็อก (log) จากเว็บเซิร์ฟเวอร์ต่าง ๆ รวมไว้ที่เซิร์ฟเวอร์กลาง (Centralize log server) บันทึกข้อมูลล็อกเก็บลงในฐานข้อมูล MySQL พัฒนาเว็บแอปพลิเคชัน โดยใช้พีเอชพี โค้ดอิกไนเทอร์ เฟรมเวิร์ก (PHP codeigniter4 framework) และภาษาไพทอน (Python) เพื่อวิเคราะห์ สืบค้นข้อมูล ตาม Keyword รูปแบบคำสั่งการโจมตีของ Hacker จากนั้นแสดงข้อมูลสรุปในหน้าเดียว (Dashboard) และแจ้งเตือนผู้ดูแลระบบผ่านทางมือถือหากตรวจพบการถูกโจมตีในทันที

ผลการดำเนินงาน พบว่าแอปพลิเคชันสามารถเฝ้าระวังการโจมตีได้เป็นอย่างดี และจะแจ้งเตือนผู้ดูแลระบบให้ตรวจสอบช่องโหว่หากตรวจพบเว็บไซต์ถูกโจมตี และแจ้งไปยังผู้ดูแลเว็บไซต์ให้ทำการแก้ไข ปิดช่องโหว่ ได้ทันที ซึ่งสามารถลดจำนวนการโจมตีลงได้กว่า 95% เมื่อเทียบกับการโจมตีช่วงเริ่มต้นโครงการ เดือน เมษายน พ.ศ. 2566 กับช่วงปิดโครงการ เดือน สิงหาคม พ.ศ. 2566

สารบัญ

สารบัญตาราง

สารบัญภาพ

บทที่ 1
ความเป็นมาและความสำคัญของปัญหาการวิจัย

สำนักหอสมุดมีบริการออนไลน์บนเว็บไซต์เป็นจำนวนมาก ทั้งให้บริการแก่ผู้ใช้และบุคลากรของหน่วยงาน เพื่อให้การบริหารจัดการและการบริการเกิดประสิทธิภาพสูงที่สุด ช่วงหลายปีที่ผ่านมาเว็บไซต์ของสำนักหอสมุดถูก Hacker โจมตี พยายามเจาะช่องโหว่บนเว็บไซต์ มีทั้งโจมตีสำเร็จและไม่สำเร็จบ่อยครั้ง แต่ผู้ดูแลระบบหรือผู้ดูแลเว็บไซต์ ไม่อาจทราบได้เลยว่าเว็บไซต์กำลังถูกโจมตี จนกว่า Hacker จะกระทำการอย่างใดอย่างหนึ่งบนหน้าเว็บไซต์ เช่น เปลี่ยนแปลงรูปภาพ เปลี่ยนแปลงข้อความ หรือแทรกลิงก์เว็บการพนัน อีกทั้งสำนักหอสมุดมีนโยบายที่มุ่งเน้นรักษาความปลอดภัยข้อมูลส่วนบุคคลของผู้ใช้และบุคลากร

ดังนั้นผู้วิจัย จึงเกิดแนวความคิดที่จะพัฒนาแอปพลิเคชันขึ้นมา เพื่อช่วยตรวจสอบ เฝ้าระวังการถูกโจมตี พยายามเจาะช่องโหว่บนเว็บไซต์ของหน่วยงาน และแจ้งเตือนไปยังผู้ดูแลระบบให้รับทราบ เพื่อให้ทำการตรวจสอบช่องโหว่ และแจ้งไปยังผู้ดูแลเว็บไซต์ให้ดำเนินการแก้ไข ปิดช่องโหว่ได้ทันที

ตารางที่ 1.1 จำนวนการโจมตีเว็บไซต์สำเร็จก่อนการใช้งานระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม

เดือน	**การโจมตีสำเร็จ ก่อนใช้งานแอปพลิเคชัน (ครั้ง)**	**ช่องโหว่เว็บไซต์**
กันยายน 2564	0	
ตุลาคม 2564	0	
พฤศจิกายน 2564	0	
ธันวาคม 2564	1	Weak Password, SQL Injection
มกราคม 2565	2	Cross Site Scripting (XSS)
กุมภาพันธ์ 2565	0	
มีนาคม 2565	0	
เมษายน 2565	0	
พฤษภาคม 2565	0	
มิถุนายน 2565	1	Cross Site Scripting (XSS)
กรกฎาคม 2565	0	

เดือน	การโจมตีสำเร็จ ก่อนใช้งานแอปพลิเคชัน (ครั้ง)	ช่องโหว่เว็บไซต์
สิงหาคม 2565	1	Cross Site Scripting (XSS)
กันยายน 2565	0	
ตุลาคม 2565	2	Cross Site Scripting (XSS)
พฤศจิกายน 2565	0	
ธันวาคม 2565	1	Cross Site Scripting (XSS)
มกราคม 2566	1	Cross Site Scripting (XSS)
กุมภาพันธ์ 2566	1	Cross Site Scripting (XSS)
มีนาคม 2566	1	Cross Site Scripting (XSS)
เมษายน 2566	1	SQL Injection

1.1 วัตถุประสงค์

1.1.1 พัฒนาเว็บแอปพลิเคชันเพื่อเฝ้าระวังความปลอดภัยทางไซเบอร์

1.1.2 ลดจำนวนครั้งการโจมตีเว็บไซต์สำเร็จ ลง 20%

1.2 ผลที่จะได้รับ

1.2.1 เว็บไซต์ของหน่วยงานมีความปลอดภัยมากยิ่งขึ้น

1.2.2 ลดความสำเร็จในการโจมตีเว็บไซต์ลง

บทที่ 2
แนวคิดทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 หลักการวิเคราะห์และออกแบบระบบ

2.1.1 ความหมายของการวิเคราะห์และออกแบบระบบ

การวิเคราะห์และออกแบบระบบ แบ่งออกเป็น 2 ส่วน คือ การวิเคราะห์ระบบ (System analysis) คือ กระบวนการศึกษาขั้นตอนการทำงานของธุรกิจเพื่อระบุเป้าหมายและจุดประสงค์ในการปรับปรุงแก้ไขระบบนั้น จากนั้นจึงทำการกำหนดปัญหาและหาวิธีแก้ไขเพื่อให้บรรลุเป้าหมายได้อย่างมีประสิทธิภาพ ส่วนการออกแบบระบบ (System Design) คือ กระบวนการในการกำหนดสถาปัตยกรรม โมดูล อินเทอร์เฟซ และข้อมูลของระบบ เพื่อตอบสนองความต้องการที่ระบุไว้ในขั้นตอนของการวิเคราะห์ระบบ

2.1.2 วงจรการพัฒนาระบบ (System Development Lift Cycle : SDLC)

วงจรการพัฒนาระบบ ประกอบด้วยกระบวนการของการทำงานที่ชัดเจนและแตกต่าง ใช้เพื่อวางแผน ออกแบบ สร้าง ทดสอบ และส่งมอบระบบสารสนเทศ โดยมุ่งที่จะผลิตระบบที่มีคุณภาพสูงที่ตอบสนองความคาดหวังของลูกค้า สอดคล้องกับความต้องการ รวมทั้งนำเสนอระบบที่ทำงานตามขั้นตอนที่ชัดเจนภายในกรอบเวลาและค่าใช้จ่ายที่กำหนด แบ่งออกเป็น 7 ขั้น ดังต่อไปนี้

- การรับรู้ปัญหา (Problem Recognition) คือ การรับรู้และทำความเข้าใจกับปัญหาระบบสารสนเทศจะเกิดขึ้นได้ก็ต่อเมื่อผู้บริหารหรือผู้ใช้เกิดความต้องการระบบสารสนเทศมาช่วยในการทำงาน หรือระบบงานเดิม
- การศึกษาความเป็นไปได้ (Feasibility Study) วัตถุประสงค์ของการศึกษาความเป็นไปได้ คือ การตัดสินใจว่าการพัฒนาระบบสารสนเทศขึ้นมาใหม่ หรือการแก้ไขระบบสารสนเทศเดิมมีความเป็นไปได้หรือไม่ โดยคำนึงถึงค่าใช้จ่ายและผลที่คาดว่าจะได้รับของระบบ
- การวิเคราะห์ (Analysis) เริ่มตั้งแต่การศึกษาระบบการทำงานของธุรกิจนั้น โดยการศึกษาเอกสารที่มีอยู่ ตรวจสอบวิธีการทำงานในปัจจุบัน และสัมภาษณ์ผู้ใช้และผู้จัดการที่มีส่วนเกี่ยวข้องกับระบบ จากนั้นจึงทำการรวบรวมความต้องการของระบบ ซึ่งความต้องการของระบบคือ คุณสมบัติที่ผู้ใช้ต้องการให้โปรแกรมประยุกต์ที่กำลังพัฒนามาสามารถทำได้ การพัฒนารายการความต้องการเป็นกิจกรรมที่ต้องทำร่วมกัน ระหว่างนักวิเคราะห์ระบบและผู้ใช้งานระบบ เครื่องมือในการวิเคราะห์ระบบ ได้แก่ แผนภาพกระแสข้อมูล (Data Flow Diagram) รูปแบบข้อมูล (Data

Model) พจนานุกรมข้อมูล (Data dictionary) รูปแบบระบบ (System Model) และผังงานระบบ (System Flowcharts)

- การออกแบบ (Design) อธิบายถึงวิธีการที่ซอฟต์แวร์จะตอบสนองความต้องการที่ได้ตกลงกันไว้ระหว่างนักวิเคราะห์ระบบและผู้ใช้บริการ เครื่องมือการออกแบบซอฟต์แวร์ เช่น Unified Modeling Language (UML) เพื่อแปลความต้องการเป็นสิ่งที่สามารถเปลี่ยนเป็นซอฟต์แวร์คอมพิวเตอร์ได้
- การพัฒนาและทดสอบ (Development & Test) เป็นขั้นตอนในการสร้างระบบโดยการเขียนโปรแกรมตามการออกแบบรายละเอียดที่เกิดขึ้นในขั้นตอนการออกแบบ โปรแกรมอาจจะถูกเขียนขึ้นมาใหม่ทั้งหมดหรือเปิดจากการนำเอาไลบรารีหรือโมดูลท่าร้างไว้ล่วงหน้ามาประกอบกันให้เกิดแอปพลิเคชันใหม่ จากนั้นต้องทำการทดสอบโปรแกรมเพื่อให้แน่ใจว่าแอปพลิเคชันสอดคล้องกับความต้องการและปราศจากข้อผิดพลาด
- การติดตั้ง (Installation) เป็นขั้นต้นของการติดตั้งแอปพลิเคชันใหม่และเตรียมฐานผู้ใช้เพื่อใช้งาน หากแอปพลิเคชันมีความซับซ้อมมากผู้ใช้อาจจะเป็นต้องได้รับการฝึกอบรมในการดำเนินการ การเตรียมเอกสารเพื่อตอบคำถามที่พบบ่อย หรือคู่มือการใช้งานระบบ
- การซ่อมบำรุง (System Maintenance) การวัดประสิทธิภาพของแอปพลิเคชันและปรับปรุงศักยภาพของแอปพลิเคชัน แอปพลิเคชันขององค์กรส่วนใหญ่ที่พัฒนาและใช้งานมาเป็นเวลาหลายปีในช่วงเวลาของการใช้งานแอปพลิเคชันเหล่านั้นต้องมีวิวัฒนาการเพื่อตอบสนองความต้องการที่เปลี่ยนแปลงไปขององค์กร วิวัฒนาการของแอปพลิเคชันนี้จะดำเนินต่อไปจนกว่าจะมีการแทนที่ด้วยแอปพลิเคชันใหม่

2.2 SIEM REPORT 2022

จากการสำรวจผู้เชี่ยวชาญทางด้าน Cyber security จำนวน 348 คน ในปี 2022 ของ Cybersecurity INSIDERS พบว่า 80% ของผู้เชี่ยวชาญทั้งหมด ให้ความเห็นว่า SIEM มีความสำคัญอย่างที่สุดต่อมาตรการรักษาความปลอดภัยทางไซเบอร์ขององค์กร โดยเพิ่มขึ้น 6% จากการสำรวจเมื่อปีที่แล้ว 85% ของผู้เชี่ยวชาญทั้งหมด ให้ความเห็นว่า SIEM มีประสิทธิภาพในการระบุและแก้ไขภัยคุกคามทางไซเบอร์ โดยเพิ่มขึ้น 5% จากการสำรวจเมื่อปีที่แล้ว และ 81% ของผู้เชี่ยวชาญทั้งหมดยืนยันว่า SIEM ช่วยยกระดับความสามารถในการตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยเพิ่มขึ้น 5% จากการสำรวจเมื่อปีที่แล้ว

2.3 The 7 Steps of Cyber Attack

ปัจจุบันมีรูปแบบการโจมตีทางไซเบอร์ที่หลากหลาย แต่วิธีพื้นฐานที่แฮกเกอร์ใช้ในการโจมตี ซึ่งมักจะประสบความสำเร็จอยู่เสมอ ๆ มี 7 ขั้นตอน ดังต่อไปนี้

- Reconnaissance: การเก็บข้อมูลของเป้าหมายก่อนการโจมตี
- Weaponization: หาวิธีเจาะระบบและเครื่องมือที่เหมาะสมกับเป้าหมาย
- Delivery: ส่งเครื่องมือการโจมตีไปยังเป้าหมาย
- Exploitation: เริ่มเจาะระบบเป้าหมาย
- Installation: ติดตั้งมัลแวร์บนเครื่องเป้าหมายเพื่อคอยรับคำสั่งจากแฮกเกอร์
- Command & Control: การเชื่อมต่อไปยังเครื่องเป้าหมาย เพื่อควบคุมอุปกรณ์ตามความต้องการ
- Action on Objectives: ดำเนินการตามเป้าหมาย

2.4 HTTP Status Codes

โค้ดมาตรฐานที่แสดงการตอบสนองของเซิร์ฟเวอร์บนเว็บไซต์ต่าง ๆ ที่อยู่บนอินเทอร์เน็ต เพื่อจะช่วยให้สามารถวินิจฉัยและให้ทราบถึงปัญหาต่าง ๆ ที่เกิดขึ้น โดยแยกเป็น 5 กลุ่ม ดังนี้

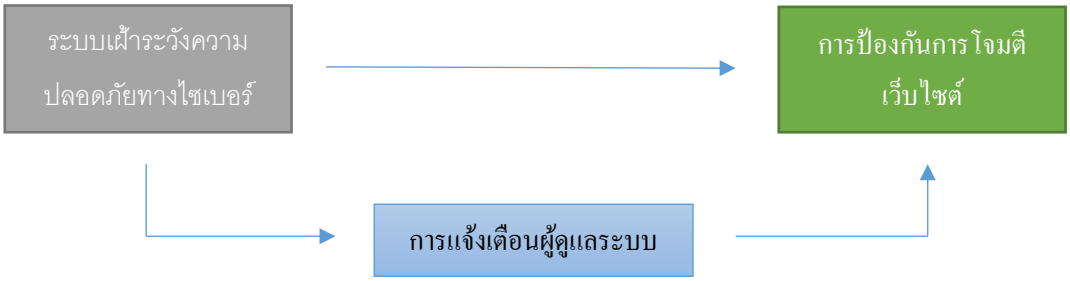
- INFORMATION CODE: 1XX คือ กลุ่มตัวเลขที่แสดงถึงข้อมูลได้รับการตอบสนองเพื่อแสดงผลว่าเซิร์ฟเวอร์กำลังรอดำเนินการตอบรับข้อมูล
- SUCCESS CODE: 2XX คือ กลุ่มตัวเลขที่แสดงถึงการร้องขอจากฝั่งของผู้ใช้งานถูกส่งไปที่เซิร์ฟเวอร์ เพื่อประมวลผลเรียบร้อย และไม่เกิด Error ระหว่างการใช้เว็บไซต์ ซึ่งในงานวิจัยนี้ CODE 200 จะหมายถึงมีความเสี่ยงสูง
- REDIRECTS CODE: 3XX คือ กลุ่มตัวเลขที่แสดงถึงการร้องขอจากผู้ใช้งานที่ถูกส่งไปยังเซิร์ฟเวอร์หรือรวมไปถึงถูกส่งต่อไปประมวลผลที่อื่น
- CLIENT ERROR CODE: 4XX คือ กลุ่มตัวเลขที่แสดงถึงการร้องขอจากผู้ใช้ที่ส่งไปยังเซิร์ฟเวอร์แล้วเกิดข้อผิดพลาดขึ้น ปัญหาดังกล่าวมักเกิดจากฝั่งผู้ใช้ส่งผลให้เซิร์ฟเวอร์ไม่ยอมประมวลผล
- SERVER ERROR CODE: 5XX คือ กลุ่มตัวเลขที่แสดงถึง Error เนื่องจากการการร้องขอจากผู้ใช้งานที่ส่งไปถึงเซิร์ฟเวอร์เกิดข้อผิดพลาด เพราะเซิร์ฟเวอร์ไม่ยอมประมวลผลจากคำร้อง

บทที่ 3
วิธีการดำเนินการวิจัย/วิธีการแก้ไขปัญหา

การวิเคราะห์การพัฒนาระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม ของสำนักหอสมุด มหาวิทยาลัยขอนแก่น ระหว่างเดือน เมษายน – ตุลาคม ผู้วิจัยได้ดำเนินการตามลำดับดังนี้

1) กรอบแนวคิดการพัฒนา
2) ขั้นตอนการดำเนินการ
3) เครื่องมือที่ใช้ในการพัฒนา
4) ขั้นตอนการพัฒนา

3.1 กรอบแนวคิดการพัฒนา



ภาพที่ 3.1 กรอบแนวคิดการพัฒนาระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม

3.2 ขั้นตอนการดำเนินการ

ขั้นตอนการดำเนินงานใช้หลักการวงจรการพัฒนาระบบ (System Development Life Cycle : SDLC) ในการพัฒนาระบบ ซึ่งประกอบด้วย 7 ขั้นตอน สามารถสรุปเป็นตารางได้ดังต่อไปนี้

ตารางที่ 3.1 การแยกรายละเอียดการวิเคราะห์

ขั้นตอนการวิเคราะห์และออกแบบระบบ	รายละเอียด
1.1 การรับรู้ปัญหา	- เว็บไซต์ของหน่วยงานถูก Hacker โจมตี ช่องโหว่เว็บไซต์

ขั้นตอนการวิเคราะห์และออกแบบระบบ	รายละเอียด
1.2 การศึกษาความเป็นไปได้	- พัฒนาระบบขึ้นมาใหม่ - หน่วยงานมีบุคลากรพร้อมสำหรับงานเขียนโปรแกรม
1.3 การวิเคราะห์	- ใช้งานง่าย - ใช้ได้ทุกที่ทุกเวลา - ช่วยประหยัดเวลาในการทำงาน - ใช้ข้อมูลจากล็อก เพื่อวิเคราะห์คำสั่ง รูปแบบการโจมตี - แสดงผลลัพธ์ในหน้าเดียว - แจ้งเตือนผู้ดูแลระบบในทันทีที่ถูกโจมตี
1.4 การออกแบบ	- เข้าถึงได้บนระบบออนไลน์ - เข้าถึงได้ผ่านสมาร์ตโฟน (Smart phone) - ส่วนติดต่อผู้ใช้ใช้งานง่าย - ภาษาโปรแกรมและเครื่องมือที่เหมาะสม
1.5 การพัฒนาและทดสอบ	- พัฒนาโปรแกรม - ทดสอบระบบ
1.6 การติดตั้ง	- จัดทำเอกสารผู้ใช้อย่างง่าย - ฝึกอบรมเจ้าหน้าที่ผู้ดูแลระบบ
1.7 การซ่อมบำรุง	- สำรองข้อมูลอย่างสม่ำเสมอ

3.3 เครื่องมือในการพัฒนา

การพัฒนาระบบมีเครื่องมือ ดังต่อไปนี้

3.3.1 ภาษาโปรแกรม

ภาษาโปรแกรมพีเอชพี โค้ดอิกไนเทอร์ เฟรมเวิร์ก, เอชทีเอ็มแอล (HTML), บูตสแตรป (Bootstrap), เจคิวรี (JQuery) สาเหตุที่เลือกใช้เพราะเป็นชุดภาษาพื้นฐานที่เจ้าหน้าที่ไอทีของหน่วยเทคโนโลยีดิจิทัลสำนักหอสมุด ใช้พัฒนาโปรแกรมเป็นประจำอยู่แล้ว

3.3.2 ระบบฐานข้อมูล

ใช้มายเอสคิวแอล สำหรับเก็บข้อมูลของระบบ สาเหตุที่เลือกใช้เพราะเป็นฐานข้อมูลที่สามารถใช้งานได้ฟรี และใช้งานง่าย อีกทั้งเจ้าหน้าที่ไอทีของหน่วยเทคโนโลยีดิจิทัล สำนักหอสมุด

ใช้พัฒนาโปรแกรมเป็นประจำอยู่แล้ว

3.3.3 อะแพชี

อะแพชี จะทำหน้าที่เป็นเว็บเซิร์ฟเวอร์ สาเหตุที่เลือกใช้เพราะสามารถใช้งานได้ฟรี และใช้งานง่าย อีกทั้งเจ้าหน้าที่ไอทีของหน่วยเทคโนโลยีดิจิทัล สำนักหอสมุด ใช้พัฒนาโปรแกรมเป็นประจำอยู่แล้ว

3.3.4 เครื่องมือเขียนภาษาโปรแกรม

วิชวล สตูดิโอ โค้ด เป็นเครื่องมือในการพัฒนาโปรแกรม สาเหตุที่เลือกใช้เพราะสามารถใช้งานได้ฟรี เป็นที่นิยม ใช้งานง่าย และสามารถติดตั้งส่วนเสริม (Extensions) เพื่อช่วยในการพัฒนาโปรแกรมให้สามารถทำได้ง่ายขึ้น และหลากหลายภาษา

3.4 ขั้นตอนการพัฒนา

ขั้นตอนการพัฒนา มีดังนี้

- สร้างเซิร์ฟเวอร์สำหรับจัดเก็บรวบรวมข้อมูลล็อก (Linux) การเรียกใช้งานเว็บไซต์ (Centralize log server) จากเซิร์ฟเวอร์ไคลเอนต์ของสำนักหอสมุด โดยใช้ Rsyslog และ MySQL ซึ่งการติดตั้ง และ Config ไฟล์ ฝั่งเซิร์ฟเวอร์ มีดังนี้

คำสั่งการติดตั้ง Rsyslog และ MySQL

```
sudo apt install rsyslog
sudo apt install rsyslog-mysql mysql
```

rsyslog.conf (/etc/rsyslog.conf)

```
module(load="imuxsock") # provides support for local system logging
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
```

```
module(load="imtcp")
input(type="imtcp" port="50514")

#Custom template to generate the log filename dynamically based on the client's IP address.
$template RemInputLogs, "/var/log/remotelogs/%FROMHOST-IP%/%PROGRAMNAME%.log"

*.* ?RemInputLogs

# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")

###########################
#### GLOBAL DIRECTIVES ####
###########################

# $AllowedSender - specifies which remote systems are allowed to send syslog messages to
rsyslogd
$AllowedSender UDP, 10.101.106.0/24, [::1]/128, *.kku.ac.th, *.*.kku.ac.th
$AllowedSender TCP, 10.101.106.0/24, [::1]/128, *.kku.ac.th, *.*.kku.ac.th

# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# Filter duplicated messages
$RepeatedMsgReduction on

# Set the default permissions for all log files.
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog
```

```
# Where to place spool and state files
$WorkDirectory /var/spool/rsyslog

# Include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf
```

mysql.conf (/etc/rsyslog.d/mysql.conf)

```
module (load="ommysql")
*.* action(type="ommysql" server="localhost" db="Syslog" uid="xxxxx" pwd="xxxxx")
```

ufw firewall

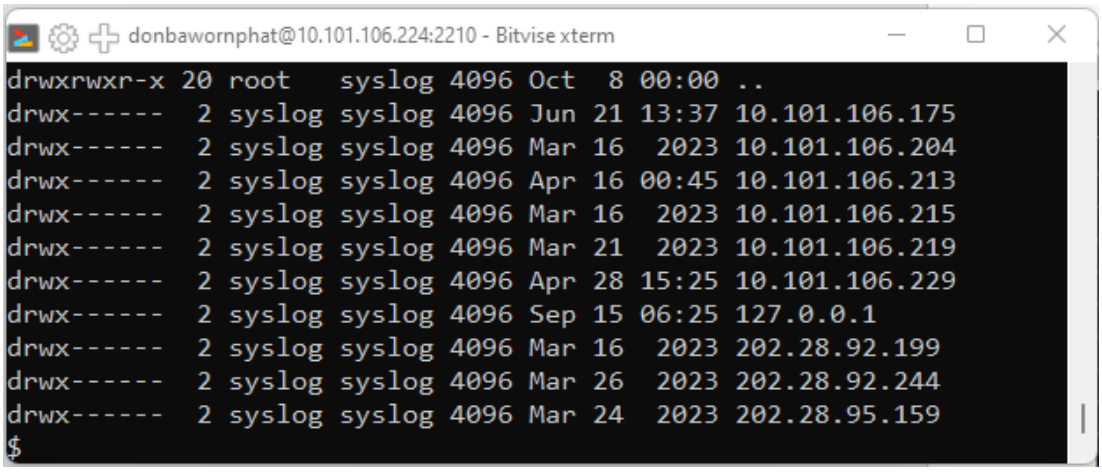
```
514/udp                 ALLOW       10.101.106.0/24
50514/tcp               ALLOW       10.101.106.0/24
```

ฝั่งไคลเอนต์ ส่งล็อกไปเก็บที่เครื่องเซิร์ฟเวอร์สำหรับเก็บรวมรวมข้อมูลล็อก โดยสร้างไฟล์ชื่อ fw-log.conf ที่ path /etc/rsyslog.d/ ซึ่ง Config ไฟล์ Rsyslog มีดังนี้

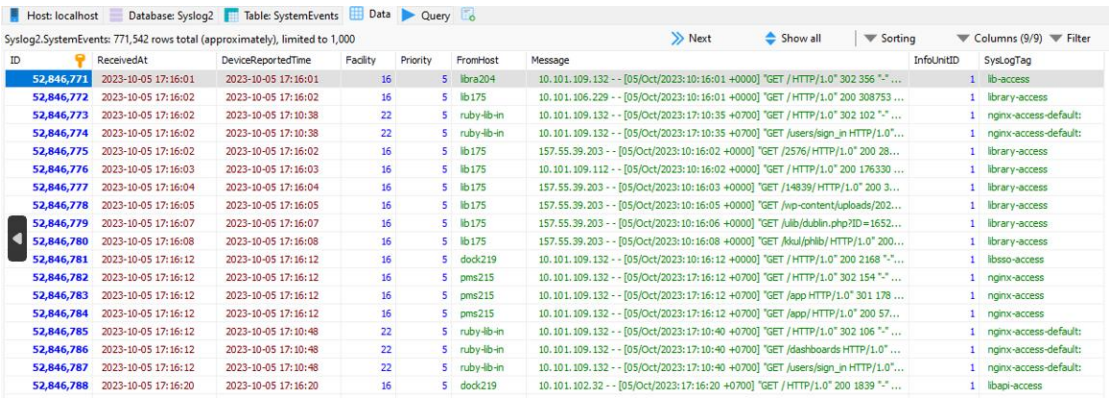
```
module(load="imfile")

input(type="imfile" File="/var/log/repair-docker/access.log" Tag="repair-access"
ruleset="remote")
input(type="imfile" File="/var/log/repair-docker/error.log" Tag="repair-error" ruleset="remote")
input(type="imfile" File="/var/log/auth.log" Tag="auth" ruleset="remote")
input(type="imfile" File="/var/log/rkhunter.log" Tag="rkhunter" ruleset="remote")

ruleset(name="remote"){
# action(type="omfwd" target="10.101.106.224" port="514" protocol="udp")
  *.*  @10.101.106.224:514
}
```

logrotate.conf (/etc/logrotate.conf)

```
# rotate log files weekly
Daily

# keep 4 weeks worth of backlogs
rotate 91
```



ภาพที่ 3.2 การเก็บรวบรวมข้อมูลล็อกจากเซิร์ฟเวอร์ของสำนักหอสมุด



ภาพที่ 3.3 การบันทึกข้อมูลลงในฐานข้อมูล MySQL

- ศึกษา รูปแบบคำสั่ง Keyword การโจมตีเว็บไซต์จากข้อมูลล็อกในฐานข้อมูล ช่วงที่เว็บไซต์ของหน่วยงานถูก Hacker โจมตี เมื่อวันที่ 1 มีนาคม – 30 เมษายน 2566 พบว่า Keyword ที่มีจำนวนสูงที่สุด 11 ลำดับแรก มีดังนี้

ตารางที่ 3.2 Keywords ที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ จำนวนรายการ และชื่อขั้นตอนการโจมตี

ลำดับ	Keywords	จำนวนรายการ	ขั้นตอนการโจมตี
1	Fuzz Faster U Fool	39,458	Weaponization
2	union	3217	Exploitation
3	document.domain	1425	Weaponization
4	script%	1213	Weaponization, Delivery
5	.sh	748	Delivery, Installation
6	alert(	711	Weaponization
7	nmap.org	126	Reconnaissance
8	sqlmap.org	98	Exploitation
9	<script	94	Weaponization, Delivery
10	document.cookie	55	Weaponization
11	shells.php	22	Delivery, Installation

ภาพที่ 3.4 ตัวอย่าง Keywords จากล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์

- พัฒนาเว็บแอปพลิเคชัน เพื่อวิเคราะห์ สืบค้นข้อมูล จากรูปแบบคำสั่ง Keyword และแสดงผลสรุปข้อมูลในหน้าเดียวด้วยพีเอชพี โค้ดอิกไนเทอร์ เฟรมเวิร์ก โดยกราฟหน้าสรุปข้อมูลการโจมตี แสดงข้อมูลดังนี้

  หมายเลข (1) จำนวนการพยายามเจาะระบบ (ครั้ง/วัน)

  หมายเลข (2) จำนวนการพยายามเจาะระบบ ความเสี่ยงสูง (ครั้ง/วัน)

  หมายเลข (3) จำนวนการพยายามเจาะระบบ แยกตามชื่อเว็บ (ครั้ง/วัน)

  หมายเลข (4) ช่วงเวลาพยายามเจาะระบบ (ครั้ง/ช่วงเวลา)

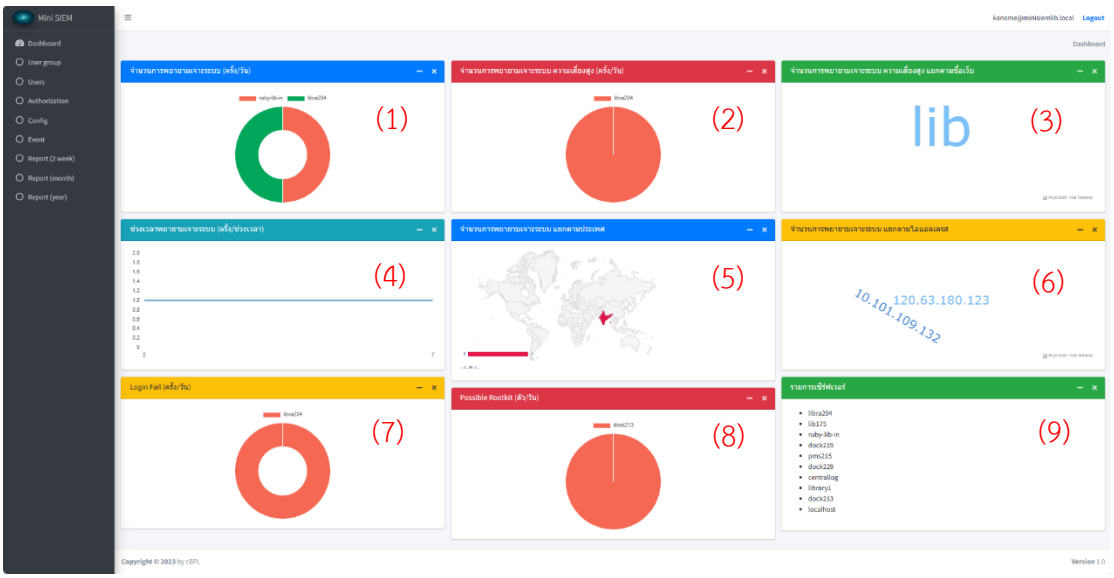
  หมายเลข (5) จำนวนการพยายามเจาะระบบ แยกตามประเทศ (ครั้ง/วัน)

  หมายเลข (6) จำนวนการพยายามเจาะระบบ แยกตามไอพีแอดเดรส (ครั้ง/วัน)

  หมายเลข (7) Login Fail (ครั้ง/วัน)

  หมายเลข (8) Possible Rootkit (ตัว/วัน)

  หมายเลข (9) รายการเซิร์ฟเวอร์



ภาพที่ 3.5 หน้าสรุปข้อมูลการโจมตี เจาะช่องโหว่เว็บไซต์และเว็บเซิร์ฟเวอร์

- พัฒนาแอปพลิเคชัน เพื่อแจ้งเตือนผู้ดูแลระบบผ่านมือถือ โดยใช้อีเมล หากตรวจพบรูปแบบคำสั่ง Keyword การโจมตีของ Hacker ในทุก ๆ 5 นาที โดยใช้ภาษาไพทอน ซึ่งการติดตั้งภาษาไพทอน โค้ดการสืบค้นข้อมูล และส่งอีเมล ในทุก ๆ 5 นาที มีดังนี้

คำสั่งติดตั้ง mysql-connector-python

```
sudo apt update
sudo apt install pip
pip install mysql-connector-python
```

โค้ดการสืบค้นข้อมูลและส่งอีเมล ชื่อ query-send-email.py

```
#!/usr/bin/python
import smtplib
import mysql.connector

mydb = mysql.connector.connect(
  host="localhost",
  user="xxxxx",
  password="xxxxx",
  database="Syslog"
)

mycursor = mydb.cursor()
sql = "SELECT * FROM SystemEvents \
WHERE (ReceivedAt > now() - interval 5 MINUTE) AND \
(Message Like '%\" 200 %') AND \
(Message Like '%Fuzz Faster U Fool%' OR \
Message Like '%union%' OR \
Message Like '%document.domain%' OR \
Message Like '%script\%%' OR \
Message Like '%.sh%' OR \
Message Like '%alert(%' OR \
Message Like '%nmap.org%' OR \
Message Like '%sqlmap.org%' OR \
Message Like '%<script%' OR \
Message Like '%document.cookie%' OR \
```

```
Message Like '%shells.php%' ) \
ORDER BY ID DESC \
Limit 10"

mycursor.execute(sql)
myresult = mycursor.fetchall()

sender = 'MiniSIEM-Robot@kku.ac.th'
receivers = ['kanome@kku.ac.th']
message = """From: <MiniSIEM-Robot@kku.ac.th>
To: <kanome@kku.ac.th>
Subject: Urgent!! Alert your website was hacked.

Hi Dear,\n\nI have detected logs that are suspected to be hacked :\n

i=0
for x in myresult:
   message += (str(x)+"\n\n")
   if str != '': i+=1

message += "\n\nPlease check your website now.\n\nRegards,\nMiniSIEM-Robot"

def sendemail():
 try:
  smtpObj = smtplib.SMTP('smtp.kku.ac.th', 25)
  smtpObj.sendmail(sender, receivers, message)
  print ("Successfully sent email")
 except SMTPException:
  print ("Error: unable to send email")

if i > 0:
  sendemail()
else:
  print("Not found attack!!")
```

โค้ดการรันสคริปต์ไพทอน ชื่อ runpy-query-attack.sh

```
sudo python3 /home/donbawornphat/query-send-email.py
```

โค้ด Contrab รันสคริปต์ทุก ๆ 5 นาที

```
*/5 * * * * sh /home/donbawornphat/runpy-query-attack.sh
```

ภาพที่ 3.6 การแจ้งเตือนผู้ดูแลระบบทางอีเมล เมื่อตรวจพบการโจมตี

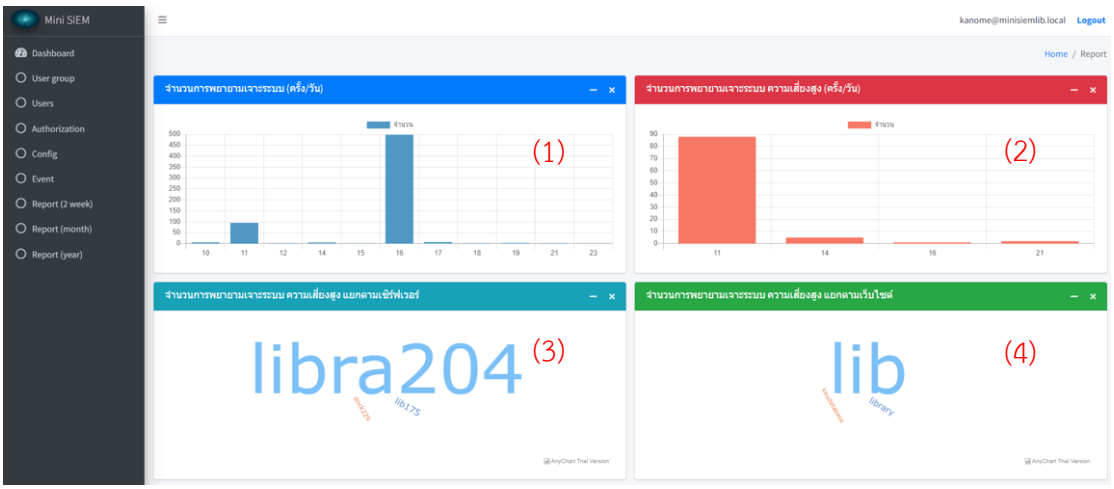
- พัฒนาเว็บแอปพลิเคชัน ส่วนของการสร้างรายงาน โดยกราฟรายงานข้อมูลการโจมตี 2 สัปดาห์ย้อนหลัง แสดงข้อมูลดังนี้

  หมายเลข (1) จำนวนการพยายามเจาะระบบ (ครั้ง/วัน)

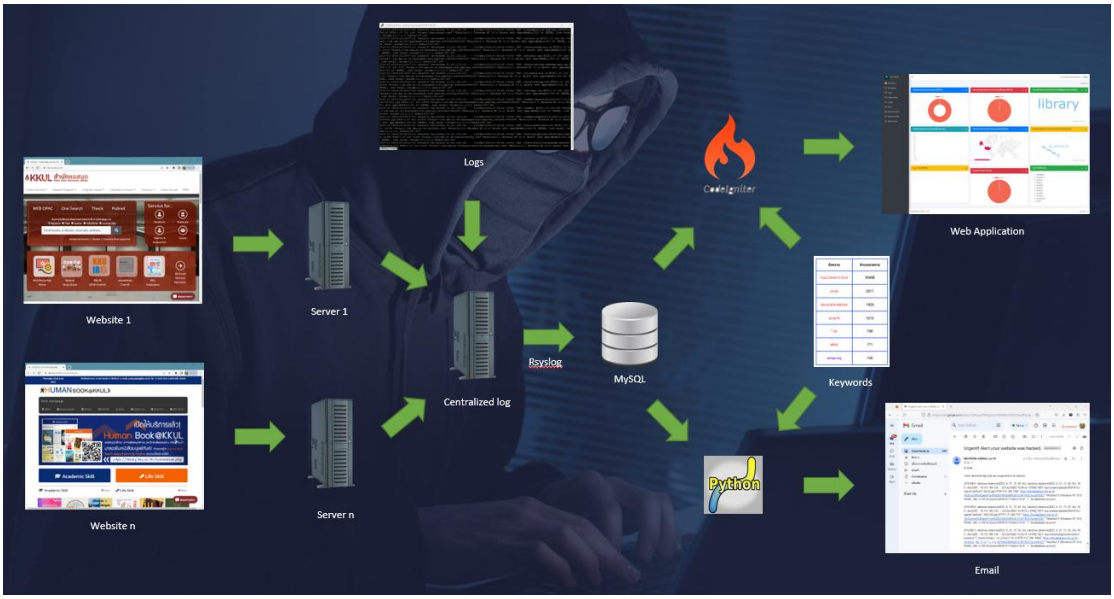
  หมายเลข (2) จำนวนการพยายามเจาะระบบ ความเสี่ยงสูง (ครั้ง/วัน)

  หมายเลข (3) จำนวนการพยายามเจาะระบบ ความเสี่ยงสูง แยกตามเซิร์ฟเวอร์ (ครั้ง/2 สัปดาห์)

  หมายเลข (4) ช่วงเวลาพยายามเจาะระบบ ความเสี่ยงสูง แยกตามเว็บไซต์ (ครั้ง/2 สัปดาห์)



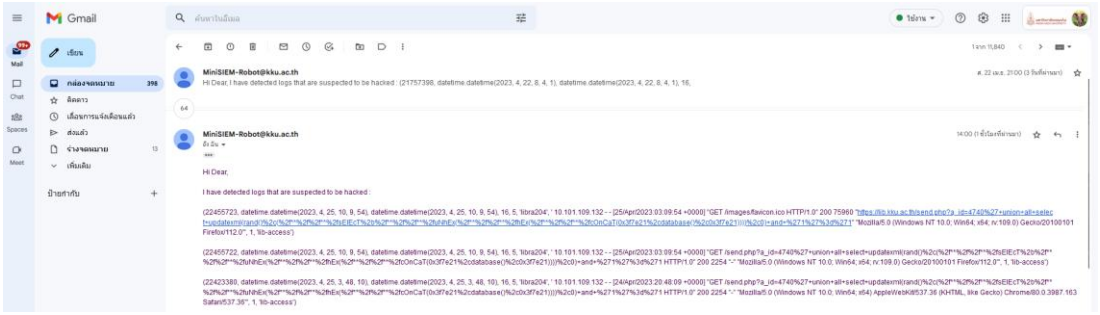
ภาพที่ 3.7 กราฟรายงานการโจมตี ช่วงระยะเวลา 2 สัปดาห์ ย้อนหลัง



ภาพที่ 3.8 ผังการทำงานของระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม

บทที่ 4
ผลการวิจัย/ผลการดำเนินงาน

ผลการดำเนินงานโครงการ การพัฒนาระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม พบว่าแอปพลิเคชันสามารถเฝ้าระวังความปลอดภัยทางไซเบอร์เว็บไซต์ของหน่วยงานได้เป็นอย่างดี และสามารถแจ้งเตือนผู้ดูแลระบบได้ทันทีเมื่อถูก Hacker โจมตี ตัวอย่างการตรวจจับการโจมตี เมื่อวันที่ 25 เมษายน พ.ศ. 2566 เวลา 10.09 น. แอปพลิเคชันตรวจพบการโจมตีช่องโหว่เว็บไซต์ SQL Injection จึงแจ้งเตือนไปที่อีเมลของผู้ดูแลระบบ หลังตรวจสอบช่องโหว่ดังกล่าว พบว่ามีปัญหาความปลอดภัยจริง จึงรายงานหัวหน้างานทราบและแจ้งผู้ดูแลเว็บไซต์ให้แก้ไข ปิดช่องโหว่ดังกล่าว ในทันที



ภาพที่ 4.1 แอปพลิเคชันแจ้งเตือนผู้ดูแลระบบเมื่อตรวจพบการโจมตีเว็บไซต์

```
---
Parameter: a_id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: a_id=4740 AND (SELECT 1926 FROM (SELECT(SLEEP(5)))xWGR)
---
[04:30:15] [INFO] the back-end DBMS is MySQL
[04:30:15] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to preven
t potential disruptions
back-end DBMS: MySQL >= 5.0.12
[04:30:22] [INFO] fetching database names
[04:30:22] [INFO] fetching number of databases
[04:30:22] [INFO] retrieved: 2
[04:30:53] [INFO] retrieved: information_schema
[04:43:35] [INFO] retrieved: kkulib
available databases [2]:
[*] information_schema
[*] kkulib

[04:47:41] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/lib.kku.ac.th'

[*] ending @ 04:47:41 /2023-04-25/
```

ภาพที่ 4.2 ผู้ดูแลระบบทำการตรวจสอบช่องโหว่เว็บไซต์ SQL Injection

ระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม สามารถแจ้งเตือนผู้ดูแลระบบได้ทันทีเมื่อตรวจพบล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ของแฮกเกอร์ โดยช่วงเริ่มต้นของการใช้แอปพลิเคชัน เดือน เมษายน 2566 จะมีการแจ้งเตือนล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ จำนวน 497 ครั้ง หลังจากผู้ดูแลระบบตรวจสอบช่องโหว่เว็บไซต์ บันทึกข้อมูลรายการช่องโหว่ และแจ้งให้ผู้ดูแลเว็บไซต์แก้ไข ปิดช่องโหว่เว็บไซต์แล้ว จำนวนการแจ้งเตือนจะลดลงเป็นอย่างมาก ตั้งแต่เดือน พฤษภาคม – สิงหาคม 2566 โดยลดลงกว่า 86% ในเดือนสิงหาคม และช่วงปี พ.ศ. 2566 (มกราคม – เมษายน) ก่อนการใช้งานระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม พบการโจมตีเว็บไซต์สำเร็จ จำนวน 4 ครั้ง แต่หลังจากใช้งานระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม ผู้ดูแลระบบตรวจสอบช่องโหว่เว็บไซต์ บันทึกข้อมูลรายการช่องโหว่ และแจ้งให้ผู้ดูแลเว็บไซต์แก้ไข ปิดช่องโหว่แล้ว ผู้ดูแลระบบไม่พบการโจมตีเว็บไซต์สำเร็จจนถึงปัจจุบัน หรือลดลง 100% รายละเอียดดังนี้

ตารางที่ 4.1 เปรียบเทียบจำนวนการแจ้งเตือนผู้ดูแลระบบก่อนและหลังการใช้งานระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม

เดือน	**จำนวนการแจ้งเตือน ก่อนใช้งานแอปพลิเคชัน (ครั้ง)**	**จำนวนการแจ้งเตือน หลังใช้งานแอปพลิเคชัน (ครั้ง)**
มีนาคม 2566	0	0
เมษายน 2566	0	497
พฤษภาคม 2566	0	40
มิถุนายน 2566	0	39
กรกฎาคม 2566	0	51
สิงหาคม 2566	0	69
กันยายน 2566	0	6
ตุลาคม 2566	0	29
พฤศจิกายน 2566	0	10

ตารางที่ 4.2 เปรียบเทียบจำนวนการโจมตีสำเร็จก่อนและหลังการใช้งานระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม

เดือน	การโจมตีสำเร็จ ก่อนใช้งานแอปพลิเคชัน (ครั้ง)	การโจมตีสำเร็จ หลังใช้งานแอปพลิเคชัน (ครั้ง)	ช่องโหว่เว็บไซต์
ธันวาคม 2564	1	0	Weak Password, SQL Injection,
มกราคม 2565	2	0	Cross Site Scripting (XSS)
กุมภาพันธ์ 2565	0	0	
มีนาคม 2565	0	0	
เมษายน 2565	0	0	
พฤษภาคม 2565	0	0	
มิถุนายน 2565	1	0	Cross Site Scripting (XSS)
กรกฎาคม 2565	0	0	
สิงหาคม 2565	1	0	Cross Site Scripting (XSS)
กันยายน 2565	0	0	
ตุลาคม 2565	2	0	Cross Site Scripting (XSS)
พฤศจิกายน 2565	0	0	
ธันวาคม 2565	1	0	Cross Site Scripting (XSS)
มกราคม 2566	1	0	Cross Site Scripting (XSS)
กุมภาพันธ์ 2566	1	0	Cross Site Scripting (XSS)
มีนาคม 2566	1	0	Cross Site Scripting (XSS)
เมษายน 2566	1	0	SQL Injection
พฤษภาคม 2566	0	0	
มิถุนายน 2566	0	0	
กรกฎาคม 2566	0	0	
สิงหาคม 2566	0	0	
กันยายน 2566	0	0	

นอกจากนี้ระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม สามารถลดจำนวนล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ลงได้เป็นอย่างมาก เมื่อเทียบจากช่วงเริ่มต้นโครงการกับช่วงปิดโครงการ โดยช่วงเริ่มต้นโครงการ เดือน เมษายน 2566 พบจำนวนล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ จำนวน 42,890 รายการ และจำนวนล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ ความเสี่ยงสูง จำนวน 3,316 รายการ และหลังจากผู้ดูแลระบบตรวจสอบช่องโหว่เว็บไซต์ บันทึกข้อมูลรายการช่องโหว่ และแจ้งให้ผู้ดูแลเว็บไซต์แก้ไข ปิดช่องโหว่เว็บไซต์แล้ว ช่วงปิดโครงการ เดือน สิงหาคม 2566 พบจำนวนล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ จำนวน 1,849 รายการ และพบจำนวนล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ ความเสี่ยงสูง จำนวน 161 รายการ โดยลดลงคิดเป็น 95.68% และ 95.14% ตามลำดับ

ภาพที่ 4.3 กราฟเปรียบเทียบจำนวนการพยายามเจาะระบบ จากวันที่ 1 เมษายน - 30 สิงหาคม 2566

บทที่ 5
สรุปผลการวิจัย อภิปรายผลและข้อเสนอแนะ

จากการจัดทำโครงการ การพัฒนาระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม พบว่า แอปพลิเคชันสามารถเฝ้าระวังการโจมตีทางไซเบอร์ได้เป็นอย่างดี โดยสามารถตรวจจับการโจมตี แสดงข้อมูลสรุปการโจมตีทั้งหมดได้ในหน้าเดียว สามารถแจ้งเตือนผู้ดูแลระบบเมื่อเว็บไซต์ถูกโจมตีได้ทันทีผ่านมือถือ และสามารถลดจำนวนการโจมตีเว็บไซต์สำเร็จ ลงได้ 100% เมื่อเทียบกับช่วงก่อนเริ่มต้นโครงการ เดือน มกราคม - เมษายน พ.ศ. 2566 กับช่วงปิดโครงการ เดือน สิงหาคม พ.ศ. 2566

ปัจจุบันหน่วยงานมีเว็บไซต์ที่ให้บริการผู้ใช้จำนวนมาก ซึ่งหลายเว็บไซต์ถูกพัฒนาขึ้นมาเป็นเวลานาน ทั้งจากนักพัฒนาของหน่วยงานเอง และจากการจัดจ้างบุคคลนอกพัฒนา หลายเว็บไซต์เทคโนโลยีที่ใช้พัฒนาล้าสมัย มีช่องโหว่ อีกทั้งบุคลากรเกษียณอายุราชการจำนวนมาก และหน่วยงานมีนโยบายจะลดจำนวนบุคลากรลง หน่วยงานไอทีจำเป็นจะต้องจัดอบรม ให้ความรู้ เกี่ยวกับการนำแอปพลิเคชันสำเร็จรูปมาใช้งาน เช่น WordPress, AppSheet, DSpace, Omeka อื่น ๆ การรักษาความปลอดภัยทางไซเบอร์ เพื่อเพิ่มความปลอดภัยทางไซเบอร์ให้แก่หน่วยงาน รวมถึงจัดหาแอปพลิเคชัน โซลูชัน อื่น ๆ เพื่อช่วยในการปฏิบัติงาน ลดเวลาในการเฝ้าระวัง ติดตาม ลดการถูกโจมตีทางไซเบอร์ โครงการนี้สามารถตอบสนองต่อความต้องการดังกล่าวได้เป็นอย่างดียิ่ง

การดำเนินการโครงการมีข้อจำกัด เนื่องจากเซิร์ฟเวอร์ของหน่วยงานมีทรัพยากรจำกัด มีลักษณะเป็น Virtual machine (VM) หากจัดเก็บข้อมูลล็อก มากกว่า 3 วัน การประมวลผลข้อมูล การสืบค้น และการแสดงผล จะค่อนข้างช้า ผู้วิจัยจำเป็นจะต้องเขียนสคริปต์ลบข้อมูลล็อกส่วนเกินออกไปในทุก ๆ สัปดาห์ เพื่อให้ระบบสามารถประมวลผล แสดงผล ได้อย่างราบรื่น ไม่ติดขัด

ข้อเสนอแนะการนำผลการวิจัยไปใช้ประโยชน์ แอปพลิเคชันจากโครงการนี้ สามารถใช้เพื่อตรวจสอบ เฝ้าระวัง และแจ้งเตือนผู้ดูแลระบบได้เป็นอย่างดี หากเว็บไซต์ถูก Hacker โจมตี ผู้ดูแลระบบจำเป็นจะต้องตรวจสอบช่องโหว่ (Confirm) ที่ได้รับการแจ้งเตือนจากแอปพลิเคชัน แล้วแจ้งเตือนช่องโหว่นั้น ไปยังผู้ดูแลเว็บไซต์ให้ดำเนินการแก้ไข ปิดช่องโหว่ ในทันที

แนวทางการพัฒนาต่อ ปัจจุบันโครงการนี้ศึกษา วิจัย เฉพาะรูปแบบการโจมตีผ่านระบบปฏิบัติการ Linux เท่านั้น หากจะพัฒนาต่อในอนาคตควรจะศึกษา วิจัย รูปแบบการโจมตีผ่านระบบปฏิบัติการ Windows เพิ่มเติม เพื่อให้ครอบคลุมระบบปฏิบัติการทั้งหมดของหน่วยงาน ส่วนฐานข้อมูลควรเปลี่ยนไปใช้ฐานข้อมูล MongoDB แทน MySQL เพราะจะสามารถประมวลผลได้เร็ว

กว่า และภาษาที่ใช้ในการพัฒนาควรเปลี่ยนไปใช้ JavaScript framework แทน PHP framework เพราะจะสามารถแสดงผลได้เร็วกว่า

เอกสารอ้างอิง

เกียรติพงษ์ อุดมธนะธีระ. (2562). **วงจรการพัฒนาระบบ**. ค้นเมื่อ 28 สิงหาคม 2565, จาก https://dol.dip.go.th/th/category/2019-02-08-08-57-30/2019-03-15-11-06-29

มายพีเอชพี. (2562). **Apache**. ค้นเมื่อ 29 สิงหาคม 2565, จาก https://www.mindphp.com/คู่มือ/73-คืออะไร/2265-apache-คืออะไร.html

ไมโครซอฟต์. **Visual Studio Code**. ค้นเมื่อ 29 สิงหาคม 2565, จาก https://code.visualstudio.comhttps://code.visualstudio.com/docs

ไอทีจีเนียส เอ็นจิเนียริ่ง. (2557). **MySQL**. ค้นเมื่อ 30 สิงหาคม 2565, จาก https://www.itgenius.co.th/article/(MySQL)-คืออะไร.html

Cybersecurity Insiders. (2022). **2022 SIEM SECURITY REPORT**. Retrieved August 30, 2023, from https://www.cybersecurity-insiders.com/portfolio/2022-siem-report-core-security-by-helpsystems-2

Fedingo. (2021). **How to Setup Rsyslog with MySQL**. Retrieved January 20, 2023, from https://fedingo.com/how-to-setup-rsyslog-with-mysql

Kifarunix. (2023). **Install and Setup Rsyslog Server on Ubuntu 22.04**. Retrieved January 20, 2023, from https://kifarunix.com/install-and-setup-rsyslog-server-on-ubuntu/?expand_article=1