PULINET Journal

การป้องกันการโจมตีเว็บไซต์ด้วยระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม: กรณีศึกษา สำนักหอสมุด มหาวิทยาลัยขอนแก่น

ดนย์บวรภัทร มีกุญชร*, ภานุวัตร อุทัยบาล
สำนักหอสมุด มหาวิทยาลัยขอนแก่น
123 ถนนมิตรภาพ ตำบลในเมือง อำเภอเมือง จังหวัดขอนแก่น 40002

Web Attack Prevention with Mini SIEM Cybersecurity Surveillance Systems: A Case Study of Khon Kaen University Library

Donbawornphat Meekunchorn*, Panuwat Authaibal
Khon Kaen University Library
123 Mittraphap Road, Nai Mueang Subdistrict, Mueang District, Khon Kaen Province 40002
E-mail: kanome@kku.ac.th

▶ รับบทความ 11 ธันวาคม 2567 ▶ แก้ไขบทความ 27 มีนาคม 2568 ▶ ตอบรับบทความ 23 เมษายน 2568

บทคัดย่อ

สำนักหอสมุด มหาวิทยาลัยขอนแก่นมีเว็บไซต์จำนวนมาก ทั้งให้บริการแก่ผู้ใช้และบุคลากร ที่ผ่านมาเว็บไซต์ของหน่วยงานถูกโจมตี แต่ผู้ดูแลระบบ ผู้ดูแลเว็บไซต์ ไม่สามารถรับรู้ถึงการโจมตีที่เกิดขึ้นได้ ผู้วิจัยจึงสนใจที่จะศึกษาการป้องกันการโจมตีเว็บไซต์ด้วยระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม วัตถุประสงค์เพื่อป้องกันการถูกโจมตีเว็บไซต์ของหน่วยงาน และแจ้งเตือนผู้ดูแลระบบให้ทราบ เพื่อจะได้ตรวจสอบ และแจ้งผู้ดูแลเว็บไซต์ให้แก้ไข ปิดช่องโหว่ได้ทันที เริ่มจากการเก็บรวบรวมข้อมูลล็อกจากเว็บเซิร์ฟเวอร์ต่าง ๆ ไว้ที่เซิร์ฟเวอร์กลาง บันทึกข้อมูลล็อกลงในฐานข้อมูล พัฒนาแอปพลิเคชันเพื่อสืบค้นข้อมูล ตามรูปแบบคำสั่งการโจมตีของแฮกเกอร์ จากนั้นแสดงข้อมูลสรุปในหน้าเดียว และแจ้งผู้ดูแลระบบหากตรวจพบล็อกที่เสี่ยงต่อการถูกโจมตีในทันที ผลการดำเนินงาน พบว่าระบบสามารถป้องกันการโจมตีได้เป็นอย่างดี สามารถแจ้งเตือนผู้ดูแลระบบได้ทันทีเมื่อเว็บไซต์เสี่ยงต่อการถูกโจมตี และสามารถลดจำนวนล็อกที่เสี่ยงต่อการโจมตีลงได้ 95% เมื่อเทียบกับช่วงเริ่มต้นโครงการวิจัยในเดือนเมษายน กับช่วงปิดโครงการวิจัยในเดือนสิงหาคม พ.ศ. 2566

คำสำคัญ

ไซเบอร์ซีเคียวริตี้, เซียม, แฮกเกอร์

Abstract

Khon Kaen University Library operates multiple websites that serve both users and staff. In the past, these websites have been targeted by cyberattacks; however, system administrators and website managers were unable to detect the attacks in real-time. This research aims to enhance website security through a cybersecurity monitoring system (Mini SIEM) to prevent cyberattacks and provide immediate alerts to system administrators. The system enables administrators to monitor, investigate, and notify

ผลงานนี้ได้ผ่านการนำเสนอในการประชุมวิชาการระดับชาติ PULINET ครั้งที่ 14 วันที่ 10-12 มกราคม 2567
จัดโดยศูนย์บรรณสารและสื่อการศึกษา มหาวิทยาลัยแม่ฟ้าหลวง และข่ายงานห้องสมุดมหาวิทยาลัยส่วนภูมิภาค (PULINET)

website managers to address and patch vulnerabilities promptly. The research methodology involved collecting log data from various web servers into a centralized server, storing log data in a database, and developing an application to scan for attack patterns used by hackers. The system then presents a summary dashboard and alerts administrators upon detecting potential security threats. The results demonstrated that the system effectively prevented cyberattacks and promptly alerted administrators when websites were at risk. Moreover, the system successfully reduced the number of high-risk logs by 95% compared to the initial phase of the research project in April and the final phase in August 2023.

Keywords

Cybersecurity, SIEM (Security Information and Event Management), Hacker

บทนำ (Introduction)

การป้องกันการโจมตีเว็บไซต์เป็นเรื่องสำคัญในโลกดิจิทัลปัจจุบัน การโจมตีทางไซเบอร์สามารถทำความเสียหายได้ในลักษณะต่าง ๆ ซึ่งอาจส่งผลกระทบที่ร้ายแรงต่อองค์กรหรือบุคคลที่เกี่ยวข้อง การศึกษาและการพัฒนาระบบเฝ้าระวังความปลอดภัยทางไซเบอร์ เป็นสิ่งสำคัญในการป้องกันการโจมตีเว็บไซต์ โดยการรวบรวมข้อมูลล็อกจากเซิร์ฟเวอร์ต่าง ๆ และการวิเคราะห์ ตรวจสอบข้อมูลเหล่านี้เป็นการช่วยเพิ่มประสิทธิภาพในการตอบสนองต่อการโจมตี การพัฒนาแอปพลิเคชันสำหรับการแจ้งเตือนและการจัดการข้อมูลให้มีประสิทธิภาพสามารถช่วยลดความเสี่ยงในการถูกโจมตีลงได้ ผ่านการรายงานผลที่ชัดเจนและการแจ้งเตือนทันที เพื่อให้ผู้ดูแลระบบได้รับทราบและทำการป้องกันหรือแก้ไขปัญหาที่เกิดขึ้นได้อย่างรวดเร็วและมีประสิทธิภาพ การวิจัยด้านนี้มีความสำคัญในการป้องกันความมั่นคงปลอดภัยของข้อมูลและเครือข่ายในระบบองค์กรอย่างมาก

ที่ผ่านมาสำนักหอสมุด มหาวิทยาลัยขอนแก่น ใช้มาตรการ เช่น การใช้ไฟร์วอลล์และการใช้งานซอฟต์แวร์แอนตี้ไวรัส รวมถึงการสร้างระบบสำรองข้อมูล เพื่อป้องกันความเสียหาย แม้จะมีการใช้มาตรการดังกล่าว แต่ก็ยังคงพบว่า มีการโจมตีที่ทำให้เว็บไซต์หลักและระบบให้บริการออนไลน์ต้องหยุดชะงักชั่วคราว เฉลี่ยปีละ 4 ครั้ง โดยแต่ละครั้งใช้เวลาเฉลี่ย 2 ชั่วโมง ในการกู้คืนระบบ ซึ่งก่อให้เกิดผลกระทบต่อผู้ใช้บริการจำนวนมาก รวมถึงสร้างภาระให้กับเจ้าหน้าที่ในการแก้ไขปัญหา สำนักหอสมุดมีนโยบายที่เข้มแข็งเพื่อมุ่งเน้นการปกป้องข้อมูลส่วนบุคคลของผู้ใช้บริการ รวมถึงการสร้างความร่วมมือกับภาครัฐ เพื่อเสริมสร้างระบบความปลอดภัยที่แข็งแกร่งและยั่งยืนต่อการโจมตีทางไซเบอร์ในระยะยาว ทั้งนี้การพัฒนาและใช้เทคโนโลยีที่ใช้ในป้องกันและเฝ้าระวังความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพจะเป็นพื้นฐานสำคัญในการเข้าสู่ยุคดิจิทัลที่ปลอดภัยและยั่งยืนในอนาคต ผู้รับผิดชอบโครงการวิจัยจึงได้ดำเนินการศึกษาและพัฒนาแอปพลิเคชัน เพื่อให้บรรลุเป้าหมายที่กำหนด

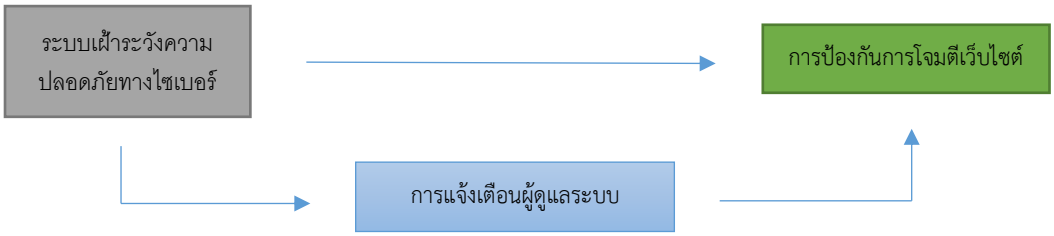
วัตถุประสงค์ (Objective)

1. เพื่อพัฒนาระบบป้องกันการโจมตีเว็บไซต์ของสำนักหอสมุด มหาวิทยาลัยขอนแก่น
2. เพื่อพัฒนาการแจ้งเตือนความเสี่ยงต่อการถูกโจมตีเว็บไซต์ของสำนักหอสมุด มหาวิทยาลัยขอนแก่น

วิธีดำเนินการวิจัย (Methodology)

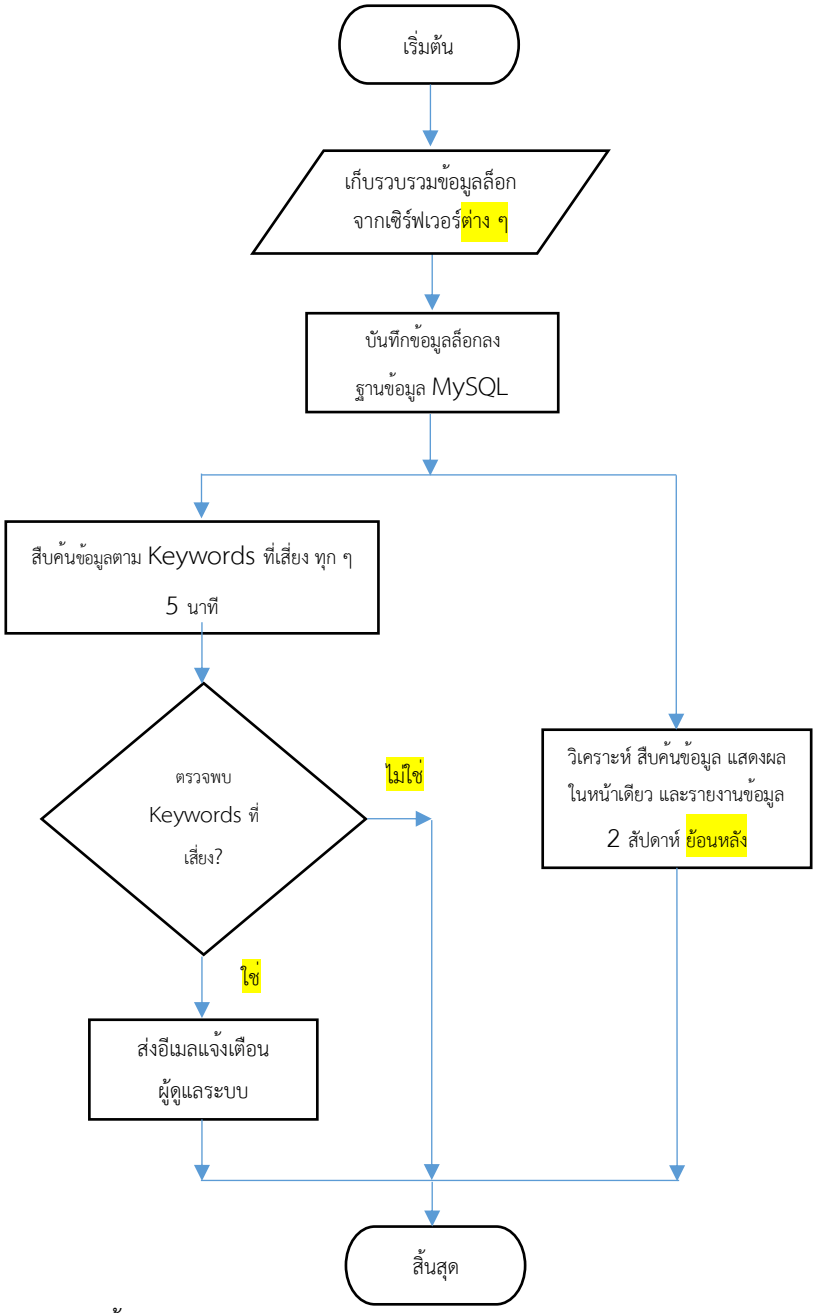
การป้องกันการโจมตีเว็บไซต์ด้วยระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม จะใช้แอปพลิเคชันที่พัฒนาขึ้นเพื่อตรวจสอบความผิดปกติของข้อมูลล็อก การเรียกใช้งานเว็บไซต์ที่มีความเสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ของแฮกเกอร์ เมื่อตรวจพบจะแจ้งเตือนไปยังผู้ดูแลระบบให้ทำการตรวจสอบช่องโหว่ หากพบว่ามีปัญหาความปลอดภัยจริง ผู้ดูแล

ระบบจะแจ้งไปยังผู้ดูแลเว็บไซต์ที่พัฒนาเว็บไซต์นั้นให้แก้ไข ปิดช่องโหว่นั้นในทันที ซึ่งจะส่งผลให้สามารถป้องกันการโจมตีเว็บไซต์ของหน่วยงานให้มีความปลอดภัยได้ โดยกรอบแนวคิดวิธีดำเนินการวิจัย ดังแสดงในภาพที่ 1



ภาพที่ 1 กรอบแนวคิดการป้องกันการโจมตีเว็บไซต์ด้วยระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม

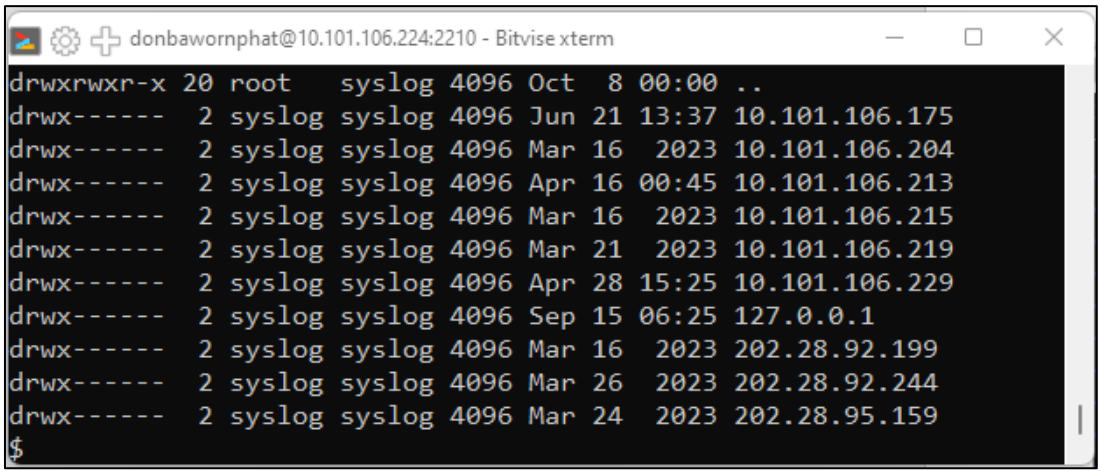
Flow Chart ขั้นตอนการทำงานของระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม ดังแสดงในภาพที่ 2



ภาพที่ 2 Flow Chart ขั้นตอนการทำงานของระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม

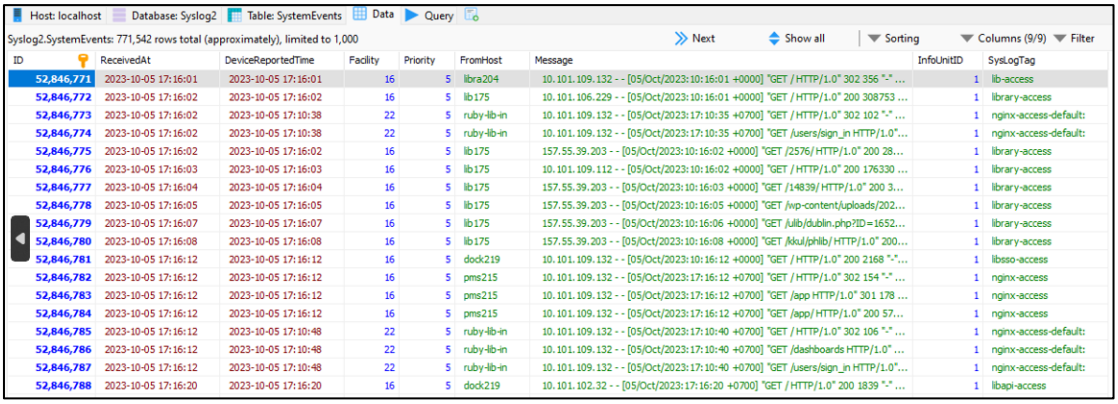
ขั้นตอนการทำงานของระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม มี 4 ขั้นตอน ดังนี้

1. สร้างเซิร์ฟเวอร์สำหรับจัดเก็บรวบรวมข้อมูลล็อก (Centralize log server) การเรียกใช้งานเว็บไซต์ จากเซิร์ฟเวอร์ต่าง ๆ ของหน่วยงาน โดยใช้ Rsyslog ดังแสดงในภาพที่ 3



ภาพที่ 3 ตัวอย่างการเก็บรวบรวมข้อมูลล็อกการเรียกใช้งานเว็บไซต์จากเซิร์ฟเวอร์ของสำนักหอสมุด

2. บันทึกข้อมูลล็อกการเรียกใช้งานเว็บไซต์ลงในฐานข้อมูล MySQL ดังแสดงในภาพที่ 4



ภาพที่ 4 ตัวอย่างการบันทึกข้อมูลลงในฐานข้อมูล MySQL

3. พัฒนาแอปพลิเคชัน เพื่อแจ้งเตือนผู้ดูแลระบบผ่านมือถือ โดยใช้อีเมล หากตรวจพบรูปแบบคำสั่ง Keywords ที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ของแฮกเกอร์ และสถานะการตอบกลับจากเว็บเซิร์ฟเวอร์ Code 200 จำนวน 10 รายการล่าสุด ในทุก ๆ 5 นาที ด้วยภาษาไพทอน โดยขั้นตอนที่แฮกเกอร์ใช้ในการโจมตี มี 7 ขั้นตอน (EC Council, 2022) ดังนี้

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

สถานะการตอบกลับจากเว็บเซิร์ฟเวอร์เมื่อผู้ใช้เรียกใช้งานเว็บไซต์ ด้วย HTTP Status Codes ดังแสดงในตารางที่ 1

ตารางที่ 1 แสดง Http Status Codes ความหมาย และความหมายในงานวิจัย (Penland, 2024)

Codes	ความหมาย	ความหมายในงานวิจัย
1xx	ได้รับคำขอข้อมูล (Request), กำลังดำเนินการต่อ	
2xx	ได้รับคำขอข้อมูลสำเร็จ, เข้าใจ และยอมรับคำขอเป็นที่เรียบร้อย	200 หมายถึง มีความเสี่ยงสูง
3xx	มีความจำเป็นต้องดำเนินการเพิ่มเติม เพื่อดำเนินการตามคำขอ	
4xx	คำขอมีวากยสัมพันธ์ (Syntax) ที่ผิดพลาด หรือไม่สามารถทำตามคำขอได้	
5xx	เซิร์ฟเวอร์ล้มเหลวในการดำเนินการตามคำขอที่ถูกต้องได้	

จากข้อมูลล็อกในฐานข้อมูล ช่วงที่เว็บไซต์ของหน่วยงานถูกแฮกเกอร์โจมตี เมื่อวันที่ 1 มีนาคม – 30 เมษายน 2566 พบว่า Keywords ที่ถูกใช้งานมากที่สุด 11 ลำดับแรก ดังแสดงในตารางที่ 2

ตารางที่ 2 แสดง Keywords ที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ จำนวนรายการ และชื่อขั้นตอนการโจมตี

ลำดับ	Keywords	จำนวนรายการ	ขั้นตอนการโจมตี
1	Fuzz Faster U Fool	39,458	Weaponization
2	union	3,217	Exploitation
3	document.domain	1,425	Weaponization
4	script%	1,213	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

ตัวอย่าง Keywords จากล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ ดังแสดงในภาพที่ 5

ภาพที่ 5 ตัวอย่าง Keywords จากล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์

ตัวอย่างการแจ้งเตือนผู้ดูแลระบบทางอีเมล เมื่อตรวจพบล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ ดังแสดงในภาพที่ 6

ภาพที่ 6 ตัวอย่างการแจ้งเตือนผู้ดูแลระบบทางอีเมล เมื่อตรวจพบล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์

4. พัฒนาเว็บแอปพลิเคชัน เพื่อวิเคราะห์ สืบค้นข้อมูล ด้วยพีเอชพี โค้ดอิกไนเทอร์ เฟรมเวิร์ก (PHP codeigniter framework) โดยแสดงผลสรุปข้อมูลในหน้าเดียว และรายงานข้อมูลล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ 2 สัปดาห์ ย้อนหลัง ดังแสดงในภาพที่ 7 และ 8 ตามลำดับ

กราฟหน้าสรุปข้อมูลการโจมตี ภายใน 1 วัน (16.31 น. ของเมื่อวาน – เวลาปัจจุบัน) มีรายละเอียดดังนี้

หมายเลข (1) จำนวนล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ (รายการ/วัน)

หมายเลข (2) จำนวนล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ ความเสี่ยงสูง (รายการ/วัน)

หมายเลข (3) ชื่อเว็บไซต์ที่มีล็อกเสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ ความเสี่ยงสูง (รายการ/วัน)

หมายเลข (4) ช่วงเวลาที่มีล็อกเสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ (รายการ/ช่วงเวลา)

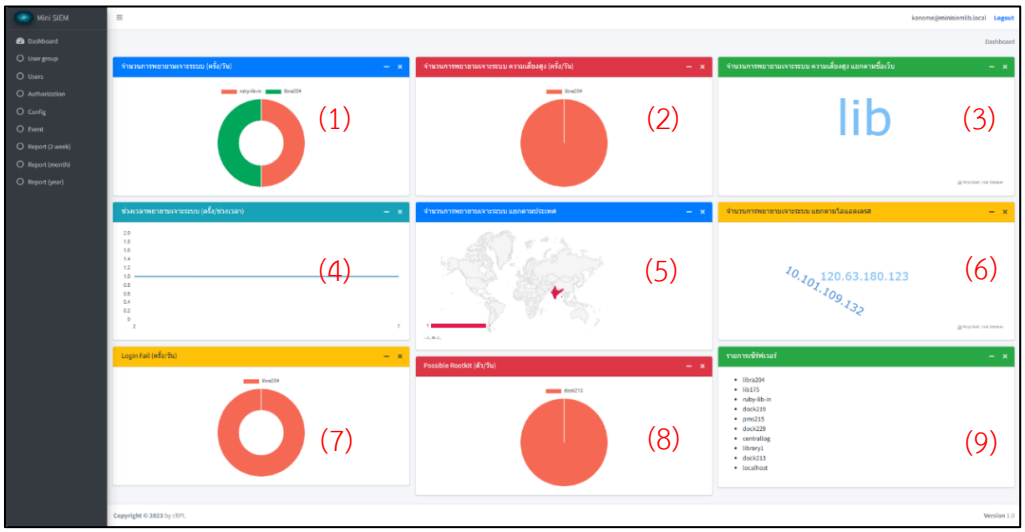
หมายเลข (5) ประเทศที่เรียกใช้เว็บไซต์ที่มีล็อกเสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ (รายการ/วัน)

หมายเลข (6) ไอพีแอดเดรส (IP address) ที่เรียกใช้เว็บไซต์ที่มีล็อกเสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ (รายการ/วัน)

หมายเลข (7) Login Fail (ครั้ง/วัน)

หมายเลข (8) Possible Rootkit (ตัว/วัน)

หมายเลข (9) รายการชื่อเซิร์ฟเวอร์



ภาพที่ 7 หน้าสรุปข้อมูลล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์และเว็บเซิร์ฟเวอร์

กราฟรายงานข้อมูลล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ 2 สัปดาห์ ย้อนหลัง มีรายละเอียดดังนี้

หมายเลข (1) จำนวนล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ (รายการ/วัน)

หมายเลข (2) จำนวนล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ ความเสี่ยงสูง (รายการ/วัน)

หมายเลข (3) ชื่อเซิร์ฟเวอร์ที่มีล็อกเสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ ความเสี่ยงสูง (รายการ/วัน)

หมายเลข (4) ชื่อเว็บไซต์ที่มีล็อกเสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ ความเสี่ยงสูง (รายการ/วัน)

ภาพที่ 8 กราฟรายงานจำนวนล็อก ชื่อเซิร์ฟเวอร์ และชื่อเว็บไซต์ที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ย้อนหลัง 2 สัปดาห์

ผลการวิจัยและอภิปรายผลการวิจัย (Result and Discussion)

การป้องกันการโจมตีเว็บไซต์ด้วยระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม พบว่าแอปพลิเคชันสามารถป้องกันการโจมตีเว็บไซต์ได้เป็นอย่างดี สามารถแจ้งเตือนผู้ดูแลระบบได้ทันทีเมื่อตรวจพบล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ของแฮกเกอร์ โดยในเดือน เมษายน 2566 มีการแจ้งเตือนผู้ดูแลระบบ จำนวน 497 ครั้ง และในเดือน พฤษภาคม – พฤศจิกายน 2566 หลังจากผู้ดูแลระบบแจ้งให้ผู้ดูแลเว็บไซต์แก้ไข ปิดช่องโหว่เว็บไซต์แล้ว จำนวนการแจ้งเตือนจะลดลงเป็นอย่างมาก และหลังจากใช้งานระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม ในเดือน เมษายน 2566 ผู้ดูแลระบบตรวจพบการโจมตีช่องโหว่ SQL Injection สำเร็จ จำนวน 1 ครั้ง หลังจากผู้ดูแลระบบแจ้งให้ผู้ดูแลเว็บไซต์แก้ไข ปิดช่องโหว่เว็บไซต์แล้ว ผู้ดูแลระบบไม่พบการโจมตีเว็บไซต์สำเร็จจนถึงปัจจุบัน ดังแสดงในตารางที่ 3 และ 4 ตามลำดับ

ตารางที่ 3 เปรียบเทียบจำนวนการแจ้งเตือนผู้ดูแลระบบหลังการใช้งานระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม

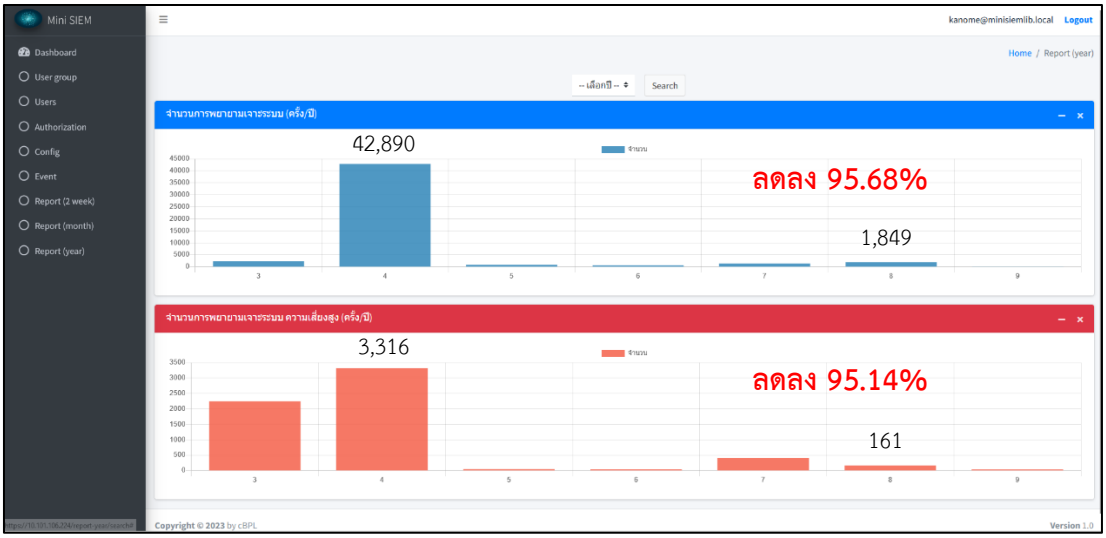
เดือน	จำนวนการแจ้งเตือน หลังใช้งานแอปพลิเคชัน (ครั้ง)
เมษายน 2566	497
พฤษภาคม 2566	40
มิถุนายน 2566	39
กรกฎาคม 2566	51
สิงหาคม 2566	69
กันยายน 2566	6
ตุลาคม 2566	29
พฤศจิกายน 2566	10

ตารางที่ 4 เปรียบเทียบจำนวนการโจมตีสำเร็จก่อนและหลังการใช้งานระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม

เดือน	การโจมตีสำเร็จ ก่อนใช้งานแอปพลิเคชัน (ครั้ง)	การโจมตีสำเร็จ หลังใช้งานแอปพลิเคชัน (ครั้ง)	ช่องโหว่เว็บไซต์
ธันวาคม 2564	1	n/a	Weak Password, SQL Injection,
มกราคม 2565	2	n/a	Cross Site Scripting (XSS)
กุมภาพันธ์ 2565	n/a	n/a	
มีนาคม 2565	n/a	n/a	
เมษายน 2565	n/a	n/a	
พฤษภาคม 2565	n/a	n/a	
มิถุนายน 2565	1	n/a	Cross Site Scripting (XSS)
กรกฎาคม 2565	n/a	n/a	
สิงหาคม 2565	1	n/a	Cross Site Scripting (XSS)
กันยายน 2565	n/a	n/a	
ตุลาคม 2565	2	n/a	Cross Site Scripting (XSS)
พฤศจิกายน 2565	n/a	n/a	
ธันวาคม 2565	1	n/a	Cross Site Scripting (XSS)
มกราคม 2566	1	n/a	Cross Site Scripting (XSS)
กุมภาพันธ์ 2566	1	n/a	Cross Site Scripting (XSS)
มีนาคม 2566	1	n/a	Cross Site Scripting (XSS)
เมษายน 2566	1	0	SQL Injection
พฤษภาคม 2566	n/a	0	
มิถุนายน 2566	n/a	0	
กรกฎาคม 2566	n/a	0	
สิงหาคม 2566	n/a	0	
กันยายน 2566	n/a	0	
ตุลาคม 2566	n/a	0	
พฤศจิกายน 2566	n/a	0	
ธันวาคม 2566	n/a	0	
มกราคม 2567	n/a	0	
กุมภาพันธ์ 2567	n/a	0	
มีนาคม 2567	n/a	0	
เมษายน 2567	n/a	0	
พฤษภาคม 2567	n/a	0	
มิถุนายน 2567	n/a	0	

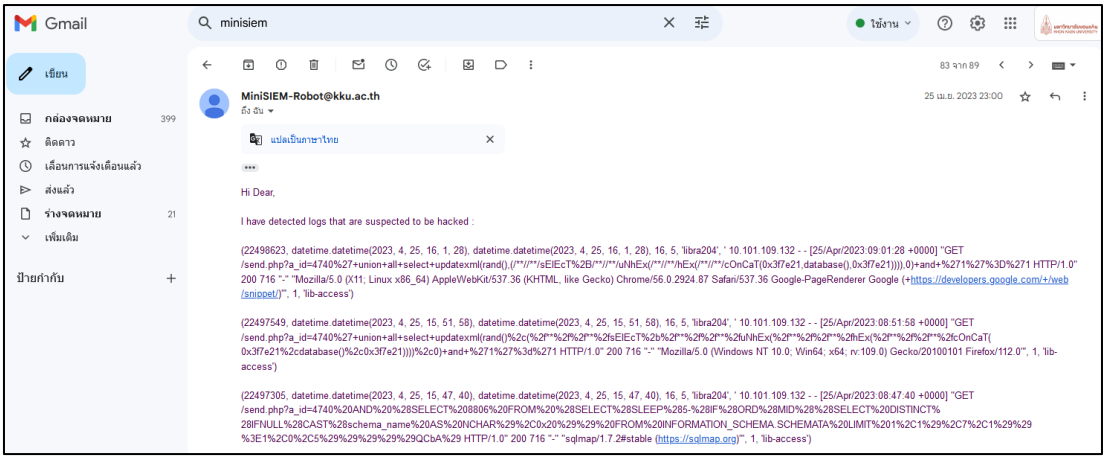
เดือน	การโจมตีสำเร็จ ก่อนใช้งานแอปพลิเคชัน (ครั้ง)	การโจมตีสำเร็จ หลังใช้งานแอปพลิเคชัน (ครั้ง)	ช่องโหว่เว็บไซต์
กรกฎาคม 2567	n/a	0	
สิงหาคม 2567	n/a	0	
กันยายน 2567	n/a	0	
ตุลาคม 2567	n/a	0	
พฤศจิกายน 2567	n/a	0	
ธันวาคม 2567	n/a	0	
มกราคม 2568	n/a	0	

นอกจากนี้ระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม สามารถลดจำนวนล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ลงได้เป็นอย่างมาก โดยช่วงเริ่มต้นโครงการวิจัย ในเดือน เมษายน 2566 พบจำนวนล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ จำนวน 42,890 รายการ และจำนวนล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ ความเสี่ยงสูง จำนวน 3,316 รายการ และหลังจากผู้ดูแลระบบตรวจสอบช่องโหว่เว็บไซต์ บันทึกข้อมูลรายการช่องโหว่ และแจ้งให้ผู้ดูแลเว็บไซต์แก้ไข ปิดช่องโหว่เว็บไซต์แล้ว ช่วงปิดโครงการวิจัย ในเดือน สิงหาคม 2566 พบจำนวนล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ จำนวน 1,849 รายการ และพบจำนวนล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ ความเสี่ยงสูง จำนวน 161 รายการ โดยลดลงคิดเป็น 95.68% และ 95.14% ดังแสดงในภาพที่ 9

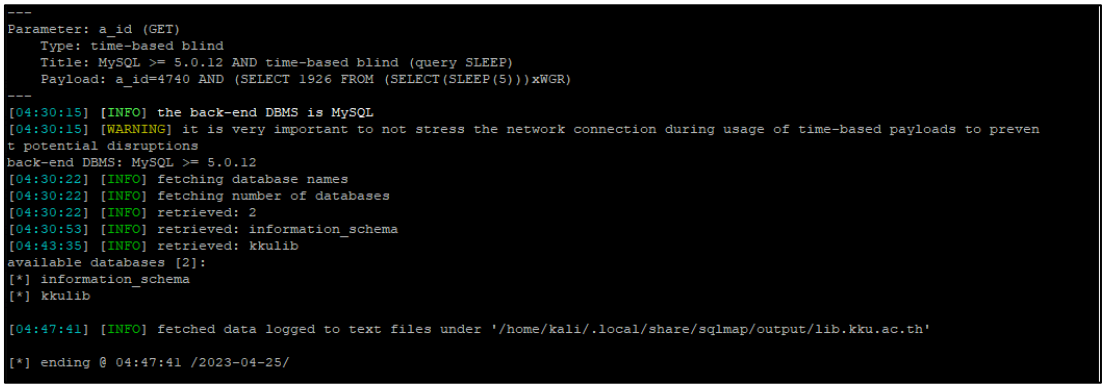


ภาพที่ 9 กราฟเปรียบเทียบจำนวนล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ ช่วงระหว่าง วันที่ 1 เมษายน - 30 สิงหาคม 2566

ตัวอย่างการตรวจพบล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ เมื่อวันที่ 25 เมษายน พ.ศ. 2566 เวลา 10.09 น. แอปพลิเคชันตรวจพบล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ ช่องโหว่ SQL Injection จึงแจ้งเตือนไปที่อีเมลของผู้ดูแลระบบ หลังตรวจสอบช่องโหว่ดังกล่าว พบว่ามีปัญหาความปลอดภัยจริง จึงรายงานหัวหน้างานทราบ และแจ้งผู้ดูแลเว็บไซต์ให้แก้ไข ปิดช่องโหว่ดังกล่าวในทันที ดังแสดงในภาพที่ 10 และ 11 ตามลำดับ



ภาพที่ 10 ตัวอย่างแอปพลิเคชันตรวจพบล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ ช่องโหว่ SQL Injection



ภาพที่ 11 ตัวอย่างผู้ดูแลระบบทำการตรวจสอบช่องโหว่เว็บไซต์ SQL Injection โดยใช้ sqlmap

พบมีปัญหาความปลอดภัยจริง

จากผลการวิจัยแสดงให้เห็นว่าการตรวจสอบล็อกการใช้งานเว็บไซต์บนเว็บเซิร์ฟเวอร์ สามารถตรวจจับการโจมตีประเภท SQL Injection และ Cross Site Scripting (XSS) ได้อย่างมีประสิทธิภาพ ซึ่งสอดคล้องกับงานวิจัยของ Vishali et al. (2024) งานวิจัยดังกล่าวใช้การเรียนรู้ของเครื่อง (Machine Learning) ในการวิเคราะห์ล็อกการใช้งานเว็บไซต์บนเว็บเซิร์ฟเวอร์ เพื่อระบุการโจมตีประเภทต่าง ๆ ความสอดคล้องนี้ชี้ให้เห็นถึงประสิทธิภาพของการวิเคราะห์ล็อกในการป้องกันการโจมตีเว็บไซต์อย่างมีประสิทธิภาพ

สรุปผลการวิจัย (Conclusion)

งานวิจัยนี้มุ่งเน้นการป้องกันการโจมตีเว็บไซต์ของสำนักหอสมุด มหาวิทยาลัยขอนแก่น โดยใช้ระบบเฝ้าระวังความปลอดภัยทางไซเบอร์มินิเซียม ผลลัพธ์ที่ได้แสดงให้เห็นว่าระบบสามารถป้องกันการโจมตีเว็บไซต์ได้อย่างมีประสิทธิภาพ ระบบสามารถแจ้งเตือนผู้ดูแลระบบได้ทันที เมื่อพบล็อกที่เสี่ยงต่อการถูกโจมตี และช่วยลดจำนวนล็อกที่เสี่ยงต่อการถูกใช้ในขั้นตอนการโจมตีเว็บไซต์ลงถึง 95.68% เมื่อเปรียบเทียบระหว่างช่วงเริ่มต้นและช่วงสิ้นสุดโครงการวิจัย

นอกจากนี้ ยังช่วยลดการโจมตีที่สำเร็จซึ่งตรวจพบในช่องโหว่ประเภทต่าง ๆ เช่น SQL Injection และ Cross Site Scripting (XSS) ได้เป็นอย่างดี ระบบดังกล่าวจึงเป็นเครื่องมือที่มีประสิทธิภาพในการสร้างความปลอดภัยของเว็บไซต์ในองค์กร และสามารถนำไปประยุกต์ใช้ในหน่วยงานอื่น ๆ ได้

กิตติกรรมประกาศ (Acknowledgements)

งานวิจัยนี้สำเร็จลุล่วงได้ด้วยความร่วมมือและการสนับสนุนจากหลายฝ่าย ข้าพเจ้าขอขอบคุณสำนักหอสมุด มหาวิทยาลัยขอนแก่น ที่มอบโอกาสและสนับสนุนทรัพยากรในการศึกษาและพัฒนาระบบเฝ้าระวังความปลอดภัยทางไซเบอร์

ขอขอบคุณ รศ.ดร.กานดา สายแก้ว ที่ให้คำแนะนำ แนวทาง และข้อเสนอแนะอันทรงคุณค่า ตลอดจนคำชี้แนะที่ช่วยให้การวิจัยครั้งนี้มีความสมบูรณ์

นอกจากนี้ ข้าพเจ้าขอขอบคุณทีมงานผู้ดูแลระบบเครือข่ายและบุคลากรทุกท่านในสำนักหอสมุด ที่ให้ความร่วมมือในการเก็บข้อมูลและทดสอบระบบ รวมถึงช่วยสนับสนุนข้อมูลทางเทคนิค

สุดท้ายนี้ ขอขอบคุณครอบครัว เพื่อน และผู้สนับสนุนทุกคนที่เป็นกำลังใจสำคัญในการดำเนินงานวิจัยจนสำเร็จในครั้งนี้

รายการอ้างอิง (References)

EC Council. (2022, January 1). *The cyber kill chain: The seven steps of a cyberattack*. https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack

Penland, J. (2024, October 23). *A Complete Guide and List of HTTP Status Codes.* Kinsta. https://kinsta.com/blog/http-status-codes

Vishali, M., Mirudhula, A., Priya, A., Iswarya, M., & Subramanian, K. (2024). *Continuous monitoring of web server assaults using machine learning*. IEEE. https://doi.org/10.1109/ic-etite58242.2024.10493548