EasyChair Preprint

№ XXX

The System to Monitor and Notifications Against Web Defacement Attacks

Wanatpong Dokput Dokput and Pongsarun Boonyapakorn

April 27, 2024

ระบบเฝ้าระวังและแจ้งเตือนการโจมตีเว็บไซต์จากการถูกเปลี่ยนแปลงหน้าเว็บไซต์

The System to Monitor and Notifications Against Web Defacement Attacks

จ.ส.อ. จิรวัฒน์ ลาภภาภรกุล (SM1 Jirawat Lappapornkul)[1] และพงศ์ศรัณย์ บุญโญปกรณ์ (Pongsarun Boonyapakorn)[1]

[1]ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

s6507031858261@email.kmutnb.ac.th, pongsarun.b@itd.kmutnb.ac.th

บทคัดย่อ

บทความนี้มีวัตถุประสงค์เพื่อศึกษา เฝ้าระวัง และตรวจสอบ ลักษณะภัยคุกคามการโจมตี รูปแบบการเปลี่ยนแปลงหน้าเว็บไซต์ โดยใช้เทคนิคการดึงข้อมูลจากหน้าเว็บไซต์ (Web Scraping) เพื่อให้ได้ Source Code มาทำการเปรียบเทียบวิเคราะห์ข้อมูลหาความแตกต่างระหว่าง ข้อมูล Source Code ที่ถูกบันทึกก่อนการเฝ้าระวัง และ ข้อมูลซอร์สโค้ด (Source Code) ที่ถูกบันทึกระหว่างการเฝ้าระวัง ด้วยเครื่องมือวิเคราะห์ตรวจสอบที่ได้ออกแบบ โดยใช้ภาษา Python ในการพัฒนา โดยมีเป้าหมายเว็บไซต์ทดสอบ ได้แก่ 1. WordPress 2. Web Framework 3. Bootstrap Template เครื่องมือจะทำหน้าที่เก็บข้อมูลหน้าเว็บไซต์ จากลิงค์ URL ที่ผู้ดูแลเว็บไซต์ลงทะเบียนแล้วเมื่อสั่งรัน เครื่องมือจะนำข้อมูลที่ได้มาบันทึก มาทำการเข้ารหัสด้วย 2 อัลกอริทึม ได้แก่ SHA1 และ MD5 เพื่อรักษาความลับความถูกต้องของข้อมูลป้องกันการถูกเปลี่ยนแปลง หากมีค่าไม่เท่ากัน เครื่องมือจะนำข้อมูลซอร์สโค้ดไปวิเคราะห์เพื่อให้ได้ระดับความรุนแรง โดยกำหนดระดับความรุนแรง ดังนี้ คือ 100–90 เปอร์เซ็นต์ อยู่ในระดับถูกเปลี่ยนแปลงโดยสิ้นเชิง 90-60 เปอร์เซ็นต์ อยู่ในระดับถูกเปลี่ยนแปลงเว็บไซต์อย่างมีนัยสำคัญ 60-20 เปอร์เซ็นต์ อยู่ในระดับถูกเปลี่ยนแปลงร้ายแรง น้อยกว่า 20 เปอร์เซ็นต์ อยู่ในระดับถูกเปลี่ยนแปลงเว็บไซต์ควรเฝ้าระวังตรวจสอบ โดยระดับความรุนแรงจะแปรผันตามเปอร์เซ็นต์ที่ซอร์สโค้ดถูกเปลี่ยนแปลงข้อมูล เมื่อเปรียบเทียบแล้วข้อมูลผิดเพี้ยนไปจากต้นฉบับ เครื่องมือจะส่งค่าแจ้งเตือนผ่านแอพพลิเคชั่นไลน์ ภายใน 15 วินาที เพื่อให้ผู้ดูแลเว็บไซต์ตรวจสอบแก้ไขมีการเก็บบันทึกประวัติทุกการเฝ้าระวังจะมีการบันทึกข้อมูลเพื่อตรวจสอบ สืบสวน ย้อนหลังได้ เฉพาะการโจมตีเปลี่ยนแปลงหน้าเว็บไซต์ ในบทความนี้ผู้วิจัยได้กำหนดการทดสอบเครื่องมือ โดยการจำลองสถานการณ์เฝ้าระวังช่วงทดสอบ 24 ชม. และทำการสร้างแบบจำลองสถานการณ์ภัยคุกคาม (scenario) การโจมตีเปลี่ยนแปลงแก้ไขเนื้อหาเว็บไซต์ ไปจนถึงการโจมตีเปลี่ยนหน้าเว็บไซต์ (web defacement) โดยการวัดผลประสิทธิภาพ จะใช้หลักการ confusion matrix มีค่าในการวัด ดังนี้ True Positive (TP), True Negative (TN), False Positive (FP) และ False Negative โดยเมื่อวัดประสิทธิแล้วผู้วิจัยคาดหวัง ค่าความถูกต้องแม่นยำ(Accuracy) จะต้องได้ผลลัพท์ค่าความถูกต้องแม่นยำ ไม่น้อยกว่า 90 เปอร์เซ็นต์

คำสำคัญ: เฝ้าระวัง การโจมตีเปลี่ยนแปลงหน้าเว็บไซต์ ซอร์สโค้ด

Abstract

This article aims to study, monitor, and detect the characteristics of threats posed by website defacement attacks, specifically focusing on patterns of webpage alterations. The methodology involves utilizing web scraping techniques to extract webpage source code for comparative analysis. A custom analysis tool, developed using Python, is employed to compare source code data before and during monitoring. The targeted websites for testing include WordPress, web frameworks, and Bootstrap templates. The tool collects webpage data from registered URL links upon execution, encrypts it using SHA1 and MD5 algorithms for data integrity, and analyzes any discrepancies in source code to determine severity levels. Severity levels range from 100-90% indicating significant alterations, 90-60% implying substantial changes, 60-20% suggesting serious modifications, and less than 20% indicating minor adjustments warranting monitoring and verification. Severity levels fluctuate based on the percentage of altered source code. Upon detecting distorted data compared to the original, the tool sends notification alerts via LINE application within 15 seconds for website administrators to review

and rectify. Historical records of monitoring activities are maintained for retrospective investigation, specifically focusing on defacement attacks. The article outlines testing procedures, including a 24-hour monitoring simulation and creation of threat scenario models ranging from content modification to website defacement attacks. Performance evaluation utilizes confusion matrix principles, with measurements including True Positive (TP), True Negative (TN), False Positive (FP), and False Negative. Researchers expect accuracy values to exceed 90% for successful performance assessment
***Keywords**: Monitor, Website defacement attacked, Source Code*

1. บทนำ

เนื่องจากปัจจุบันการใช้งานสื่อโซเชียลมีเดียและเทคโนโลยีสารสนเทศเพื่อสืบค้นข้อมูลเป็นปัจจัยที่เข้ามาเป็นส่วนในการดำเนินชีวิตของมนุษย์ ซึ่งประเทศไทยมีผู้ใช้งานอินเทอร์เน็ตมากถึง 85.3 เปอร์เซ็นต์ เมื่อเทียบกับประชากรทั้งประเทศ และเป็นสัดส่วนที่สูง จุดประสงค์ในการใช้งานอันดับที่ 1 คือ การหาข้อมูล จากแหล่งต่างๆ ที่เชื่อมต่อกันทั่วโลกประกอบด้วย สื่อโซเชียลมีเดีย เว็บไซต์ กระทู้ ฯลฯ จากสถิติข้อมูลข้างต้น การเข้าถึงแหล่งข้อมูล การประชาสัมพันธ์ การสร้างตัวตนองค์กร การขยายตัวทางธุรกิจ ต้องคำนึงถึงการใช้ประโยชน์จาก สื่อโซเชียลมีเดีย เว็บไซต์ในการเผยแพร่เนื้อหาสาระที่ดี

หน่วยงานราชการ รัฐวิสาหกิจ และ ภาคธุรกิจที่เข้าตลาดหุ้น จะถูกกำหนดให้มีเว็บไซต์ เพื่อจุดประสงค์ในการประชาสัมพันธ์กิจกรรม ข่าวสาร และการดำเนินการทางธุรกิจ ต่างๆ ทุกหน่วยงานต้องมีเว็บไซต์ เพราะต้องได้รับการประเมินจากหน่วยงาน คณะกรรมการพัฒนาระบบราชการ (กพร.) เพื่อประเมินประสิทธิ์ภาพการทำงานด้านเทคโนโลยีสารสนเทศ จึงทำให้มีหลายหน่วยงานต้องดำเนินการจัดทำเว็บไซต์ ไม่เพียงแต่หน่วยงานราชการอย่างเดียว ภาคเอกชนก็มีการจัดทำเว็บไซต์เพื่อการดำเนินการทางธุรกิจ ต่างๆ ดังนั้น เว็บไซต์จึงมีความสำคัญและเติบโตเป็นจำนวนมาก โดยเฉพาะภาคธุรกิจ(SME, สตาร์ทอัพ) และหน่วยงานโครงสร้างพื้นฐานสำคัญการที่ต้องการเป็นที่รู้จัก ในข้อดีย่อมมีข้อเสียในเรื่องของภัยคุกคาม ที่อาจตกเป็นเป้าหมายจากการถูกโจมตีทางไซเบอร์ ทำให้สูญเสียความลับ ความพร้อมใช้ ความสมบูรณ์ (CIA) จากข้อมูลสถิติการโจมตีทางไซเบอร์ของประเทศไทย [1] ในช่วง มกราคม - ธันวาคม 2566 พบว่าจำนวนการโจมตีเว็บไซต์สูงเป็นลำดับต้นๆ ดังนี้ Hacked Website (Gambling) จำนวนการถูกโจมตี 515 เหตุการณ์ และ Hacked Website (Defacement) จำนวนการถูกโจมตี 336 เหตุการณ์ จุดประสงค์ต้องการลดความน่าเชื่อถือขององค์กร สร้างความเสียหาย ดังนั้นหน่วยงานทุกหน่วยงานต้องมีมาตรการกำหนด การรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคาม ทางไซเบอร์ทั้งจากภายในและภายนอกประเทศที่มีกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ (อ้างอิงจาก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562) ดังนั้น การเฝ้าระวัง การแจ้งเตือน การรับมือ การตอบสนองต่อภัยคุกคามจึงเป็นปัจจัยที่สำคัญ สำหรับทุกหน่วยงาน

2. วรรณกรรมที่เกี่ยวข้อง

2.1 Website

สื่อนำเสนอข้อมูลบนเครื่องคอมพิวเตอร์รวบรวม หน้าเว็บเพจหลายหน้า ซึ่งเชื่อมโยงกันผ่านทางไฮเปอร์ลิงก์ ซึ่งต้องเปิดด้วยโปรแกรมเฉพาะทางที่เรียกว่า Web Browser โดยถูกจัดเก็บไว้ในเวิลด์ไวด์เว็บ และเว็บไซต์นั้นถูกสร้างขึ้นด้วยภาษาทางคอมพิวเตอร์ที่เรียกว่า HTML (Hyper Text Markup Language) เป็นภาษาหลักที่นำมาใช้ในการเขียนเว็บเพจขึ้นมา โดยจะประกอบด้วยส่วนของคำสั่งเปิด Tag ด้วย <html> และปิดด้วย </html> ซึ่งภายในจะประกอบด้วยส่วน head และส่วน body

2.2 Web Defacement

การโจมตีเว็บไซต์ที่เปลี่ยนแปลงรูปลักษณ์ของเว็บไซต์ [2] [3] โดยผู้ไม่ประสงค์ดีจะเจาะเข้าไปในเว็บเซิร์ฟเวอร์ และแทนที่ข้อมูลหน้าเว็บไซต์เป้าหมาย ให้เป็นหน้าเว็บไซต์ของผู้ไม่ประสงค์ที่ได้เตรียมไว้เพื่อเปลี่ยนแปลงแก้ไขข้อมูลหน้าเว็บไซต์เป้าหมาย โดยผู้วิจัยได้มุ่งประเด็นไปที่การเปลี่ยนแปลงที่ซอร์สโค้ดหน้าเว็บไซต์

2.3 Web Scraping

ผู้วิจัยได้ศึกษาเทคนิคดึงข้อมูลซอร์สโค้ด[4] จากเว็บไซต์ต่าง ๆ เพื่อนำข้อมูลไปวิเคราะห์ตามจุดประสงค์ต่างๆ โดย จะเป็นการเขียนโปรแกรมด้วยภาษา Python เพื่อดึงข้อมูล จะต้องใช้ไลบรารีที่จำเป็นอยู่ 2 อย่าง คือ Requests และ BeautifulSoup 4 โดยการรับค่าลิงค์ที่อยู่เว็บไซต์ เข้ามาเมื่อรันระบบ Web Scraping จะทำหน้าที่ดึงข้อมูลซอร์สโค้ด ทันทีจากนั้นระบบจะต้องมีตัวแปรมารับค่าซอร์สโค้ด

2.4 วงจรการพัฒนาซอฟต์แวร์ (SDLC)

กระบวนการ [5] ที่คุ้มค่า ประหยัดเวลาในเรื่องการออกแบบและสร้างซอฟต์แวร์คุณภาพสูงสำหรับทีมพัฒนา เป้าหมายของ SDLC คือการลดความเสี่ยงของโพรเจกต์ด้วยการวางแผนล่วงหน้า เพื่อให้ซอฟต์แวร์ตอบสนองตามความคาดหวังของลูกค้าในระหว่างการใช้งานจริง

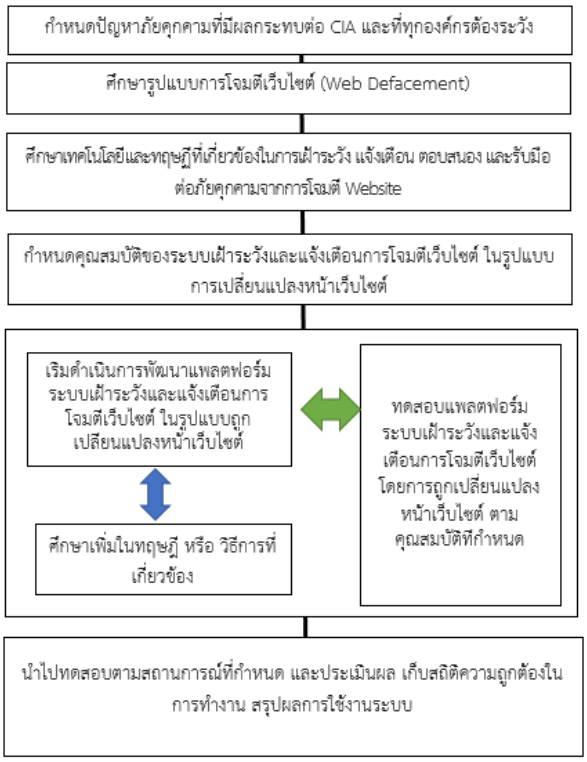
2.5 งานวิจัยที่เกี่ยวข้อง

การป้องกันภัยคุกคามนั้นมีความสำคัญ ซึ่งมีงานวิจัยส่วนมากออกมาเผยแพร่ วิธีการ หลักการ มาตรฐาน และระบบ ที่ช่วยออกแบบเครื่องมือสำหรับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้มีความเข้มแข็ง ไม่ตกเป็นเป้าหมายการโจมตี โดยมีจุดมุ่งหมายในการป้องกันความลับ ความพร้อมใช้งาน และความถูกต้องสมบูรณ์ ซึ่งการวัดประสิทธิภาพหลังจากการดำเนินการตามงานวิจัยที่ได้เผยแพร่ วิธีการ หลักการ มาตรฐาน และระบบ ซึ่งเป้าหมายของงานวิจัยจะต้องมีประสิทธิภาพที่สามารถรับมือ ตอบสนองต่อเหตุการณ์เมื่อเกิดภัยคุกคาม โดยงานวิจัยนี้ผู้วิจัยได้ศึกษางานวิจัยอื่นประกอบ [6,7] และทราบถึงวิธีวิจัย กระบวนการที่ใช้เครื่องมือในการวิเคราะห์และประเมินผล ซึ่งมีวิธีการที่แตกต่างกัน แต่ทุกงานวิจัยมีเป้าหมายและผลลัพธ์ที่ดีขึ้นเหมือนกัน โดยผู้วิจัยได้เลือกใช้หลักการวัดประสิทธิภาพของ Confusion Matrix เพื่อวัดประสิทธิภาพความแม่นยำของงานวิจัย

3 วิธีการดำเนินการวิจัย

3.1 ออกแบบขั้นตอนการวิจัย

การศึกษารูปแบบภัยคุกคามการโจมตีที่เกิดขึ้นกับเว็บไซต์พบว่า การโจมตีเว็บไซต์ ในรูปการเปลี่ยนแปลงแก้ไขหน้าเว็บไซต์โดยไม่ได้รับอนุญาต มีผลกระทบกับการรักษาความลับ (Confidentiality) ความถูกต้อง (Integrity) ความพร้อมใช้ (Availability) หรือ CIA โดยตรง ศึกษาการหลักการทำงานของเบราว์เซอร์ ศึกษาขั้นตอนการออกแบบระบบ เครื่องมือที่นำมาพัฒนาระบบ และความเป็นไปได้ในการพัฒนาระบบ เพื่อแจ้งเตือนภัยคุกคามเมื่อเกิดเหตุขึ้นแบบอัตโนมัติ และเรียลไทม์ ศึกษาการใช้งานฐานข้อมูล เพื่อเก็บประวัติการใช้งาน และได้ข้อสรุปของการพัฒนาระบบในการวิจัย ตามภาพที่ 1

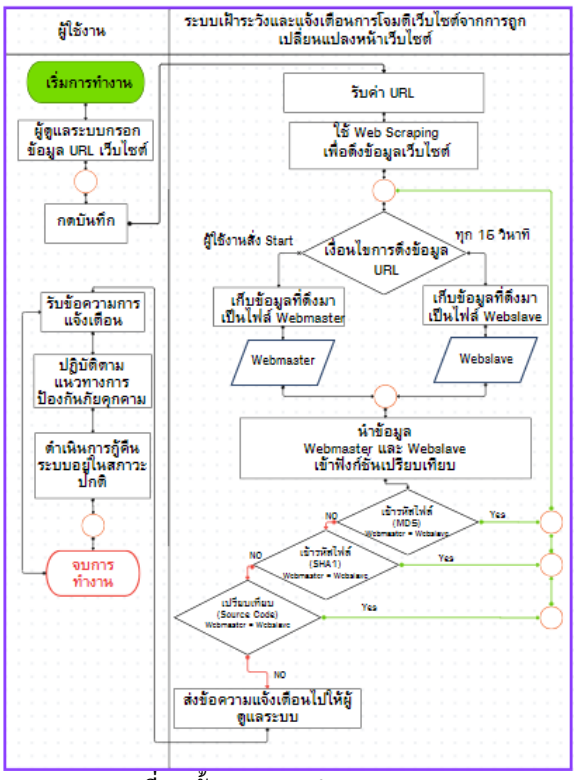


ภาพที่ 1 ขั้นตอนการศึกษาค้นคว้าวิจัย

3.2 ดำเนินการวิจัย

3.2.1 ศึกษาวิเคราะห์หลักการโจมตีรูปแบบการเปลี่ยนแปลงหน้าเว็บไซต์ ผู้วิจัยพบว่าเมื่อหน้าเว็บไซต์ถูกเปลี่ยนแปลงหน้า **จะส่งผลกระทบทำให้ซอร์สโค้ด HTML** ที่แสดงบนเบราว์เซอร์ มีการแปลงซอร์สโค้ด ส่งผลการแสดงผลหน้าเว็บไซต์ได้ถูกเปลี่ยนแปลงไปจากเดิม

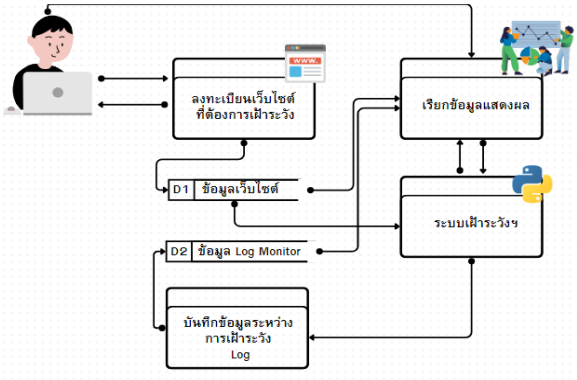
3.2.2 ออกแบบการทำงานของระบบ ให้เริ่มต้นจากการบันทึกข้อมูลการลงทะเบียนเพื่อให้ระบบเก็บข้อมูลนำไปประมวลผล ระบบจะรับค่าลิงค์ที่อยู่เว็บไซต์ ที่ลงทะเบียนเพื่อให้เครื่องมือ Web Scraping ดึงข้อมูลจากหน้าเว็บไซต์เป้าหมาย แล้วนำข้อมูลมาเข้ารหัส ฟังก์ชันแฮช เพื่อป้องกันการปลอมแปลงข้อมูล โดยจะทำการเก็บข้อมูลอยู่ 2 แบบ คือ ข้อมูลต้นแบบได้จากการเริ่มเฝ้าระวัง และข้อมูลแบบเรียลไทม์ได้จากการเก็บข้อมูลแบบอัตโนมัติทุกๆ 15 วินาที เพื่อนำมาทำการวิเคราะห์ **โดยมีเงื่อนไขคือ ขั้นที่ 1 ตรวจสอบค่าฟังก์ชันแฮช ขั้นที่ 2 ตรวจสอบระดับผลกระทบจากการโจมตีเปลี่ยนแปลงหน้าเว็บไซต์ ขั้นที่ 3 ตรวจสอบค้นหาจุดที่ถูกเปลี่ยนแปลง** หากมีการเปลี่ยนแปลงไปจากไฟล์ต้นฉบับ ระบบจะทำการแจ้งเตือนทางไลน์แอพพลิเคชัน และแสดงผลที่หน้าเว็บไซต์บริหารจัดการระบบ ขั้นตอนการทำงาน ตามภาพที่ 2



ภาพที่ 2 ขั้นตอนการทำงานของระบบ

3.2.3 ออกแบบฐานข้อมูล

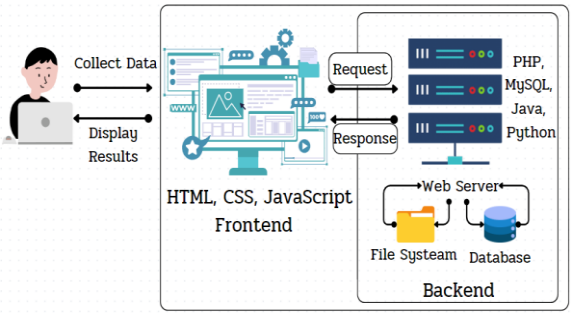
สำหรับงานวิจัยนี้ ใช้ฐานข้อมูล PHPMyAdmin เพื่อเก็บข้อมูลที่ผู้ใช้ลงทะเบียนข้อมูลเว็บไซต์ที่ต้องการเฝ้าระวัง และเก็บข้อมูลประวัติการเฝ้าระวังเว็บไซต์ที่ได้ลงทะเบียน ได้ออกแบบโครงสร้างการไหลของข้อมูล Data Flow Diagram ตามภาพที่ 3



ภาพที่ 3 Data Flow Diagram ระบบฐานข้อมูล

3.2.4 ขั้นตอนดำเนินการพัฒนา

ผู้วิจัยได้ดำเนินการพัฒนาระบบเฝ้าระวังและแจ้งเตือนการโจมตีเว็บไซต์จากการถูกเปลี่ยนแปลงหน้าเว็บไซต์ (Website Defacement) ในรูปแบบเว็บแอพพลิเคชัน โดยได้แบ่งการพัฒนาเป็นระบบสำหรับผู้ดูแลระบบ(Backend) และ ระบบสำหรับผู้ใช้งาน(Frontend) มีสถาปัตยกรรมการเชื่อมต่อ ตามภาพที่ 4 โครงสร้างการเชื่อมต่อ ผู้ใช้งานจะติดต่อหน้า Web Application ในส่วนของระบบสำหรับผู้ใช้งานที่สามารถ ลงทะเบียนเว็บไซต์ที่เฝ้าระวังได้ แสดงผลสถานะเฝ้าระวัง ประวัติการเฝ้าระวัง ผลของการเฝ้าระวัง สั่งการให้เริ่มดำเนินการเฝ้าระวัง ในส่วนของระบบผู้ดูแลระบบ ระบบจะดำเนินการแบบอัตโนมัติในเรื่องของการจัดการไฟล์ บันทึกข้อมูลลงฐานข้อมูล เริ่มดำเนินการเฝ้าระวังวิเคราะห์เหตุการณ์การโจมตี แปลผลกระทบที่เกิดจากการโจมตีเปลี่ยนแปลงหน้าเว็บไซต์ จนถึงการแจ้งเตือน



ภาพที่ 4 สถาปัตยกรรมการเชื่อมต่อระบบเฝ้าระวังเว็บไซต์

3.2.5 ขั้นตอนการใช้งานระบบ

ทำรันระบบเฝ้าระวังและแจ้งเตือนการโจมตีเว็บไซต์จากการถูกเปลี่ยนแปลงหน้าเว็บไซต์ (Website Defacement) เปิดเบราว์เซอร์ระบบ ดำเนินการลงทะเบียนข้อมูลเว็บไซต์ที่ต้องการเฝ้าระวัง เมื่อบันทึกข้อมูลเรียบร้อย ระบบจะทำการสร้างไดเรกทอรี เพื่อเก็บไฟล์ซอร์สโค้ดที่ดึงมาจากเว็บไซต์เป้าหมายและเก็บภาพหน้าเว็บไซต์เป้าหมาย จากนั้นผู้ใช้งานสามารถสั่งเริ่มทำการเฝ้าระวังได้จากการกด ปุ่ม Start เพื่อทำการรันระบบเฝ้าระวังฯ สถานะการทำงานจะเปลี่ยนเป็น Active และระบบจะเริ่มทำงาน โดยเก็บภาพหน้าเว็บไซต์เฝ้าระวัง และดึงข้อมูลซอร์สโค้ด HTML เว็บไซต์เป้าหมาย มาทำการวิเคราะห์ประมวลผล เพื่อเฝ้าระวังการถูกเปลี่ยนแปลงหน้าเว็บไซต์ ในระหว่างทำการเฝ้าระวังจะมีการเก็บประวัติการเฝ้าระวังไปบันทึกลงฐานข้อมูล หากเหตุการณ์ปกติ ระบบก็จะใช้ Web Scraping เพื่อไปดึงข้อมูลมา ทุกๆ 15 วินาที แต่เมื่อเกิดเหตุการณ์เปลี่ยนแปลงหน้าเว็บไซต์ ระบบจะทำการแจ้งเตือนผ่านไลน์แอพพลิเคชัน พร้อมกับบันทึกข้อมูลประวัติการเฝ้าระวังลงฐานข้อมูล และระบบจะดำเนินการวิเคราะห์ประมวลผลกระทบที่เกิดจากการโจมตี เพื่อแจ้งเตือนให้ผู้ใช้งานได้รับรู้รับทราบเร่งดำเนินการแก้ไขโดยด่วน

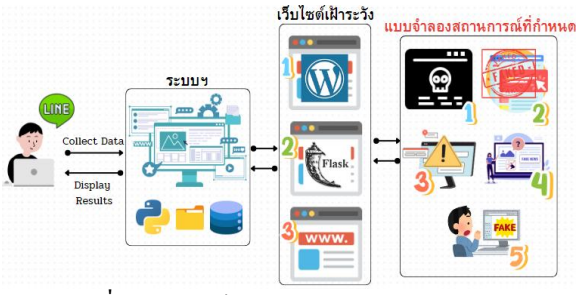
3.2.6 ขั้นตอนการทดสอบ

ผู้วิจัยได้กำหนดให้ ระบบเฝ้าระวังและแจ้งเตือนการโจมตีเว็บไซต์จากการถูกเปลี่ยนแปลงหน้าเว็บไซต์ (Website Defacement) ทำการเฝ้าระวังเว็บไซต์ จำนวน 3 เว็บไซต์

ได้แก่ 1. WordPress 2. Web framework 3. Bootstrap Template เพื่อเฝ้าระวัง และสำหรับงานวิจัยนี้ ผู้วิจัยได้ดำเนินการสร้างแบบจำลองสถานการณ์การโจมตีหน้าเว็บไซต์ในรูปแบบต่างๆ จำนวน 5 เหตุการณ์ ดังนี้

- จำลองสถานการณ์ที่ 1 เปลี่ยนแปลงเนื้อหาซอร์สโค้ดหน้าเว็บไซต์เป้าหมาย ให้เป็นซอร์สโค้ดตามแบบจำลองสถานการณ์ที่ 1 ทั้งหน้าเว็บ
- จำลองสถานการณ์ที่ 2 แก้ไขเนื้อหาลิงค์ฝั่งลิงค์แปลกปลอม จุดประสงค์เพื่อให้กดลิงค์ไปที่เนื้อหา ของ ผู้ไม่ประสงค์ดี ที่ได้ทำไว้เพื่อหลอกล่วง
- จำลองสถานการณ์ที่ 3 แก้ไขเปลี่ยนแปลงข้อมูลละเอียดอ่อน เช่น ข้อมูลการติดต่อ ที่อยู่ เลขที่บัญชีธนาคาร เป็นต้น
- จำลองสถานการณ์ที่ 4 ทำการแก้ไขเปลี่ยนแปลงเฉพาะแท็ก boby (เนื้อหาภายในหน้าเว็บไซต์) ที่ซอร์สโค้ด HTML หน้าเว็บไซต์เป้าหมาย
- จำลองสถานการณ์ที่ 5 ฝัง Code เพื่อให้ Reindex ไปหน้าเว็บไซต์ปลอม

วิธีการทดสอบ คือ ลงทะเบียนเว็บไซต์เป้าหมาย โดยทำการเฝ้าระวังเว็บไซต์ 3 เว็บไซต์ จากนั้นจำลองสถานการณ์เป็นผู้ไม่ประสงค์ดี โดยสามารถเข้าเครื่องเซิร์ฟเวอร์ได้ จากนั้นทำการเปลี่ยนแปลงแก้ไขซอร์สโค้ด HTML ที่เว็บไซต์เป้าหมาย ด้วย แบบจำลองสถานการณ์ที่ได้ออกแบบ 5 แบบจำลอง โจมตีทั้ง 3 เว็บไซต์ โดยความแตกต่างอยู่ที่ เว็บไซต์ที่พัฒนา และแบบจำลองที่สร้างขึ้นเพื่อทดสอบ โครงสร้างการทดสอบจะตามภาพที่ 5

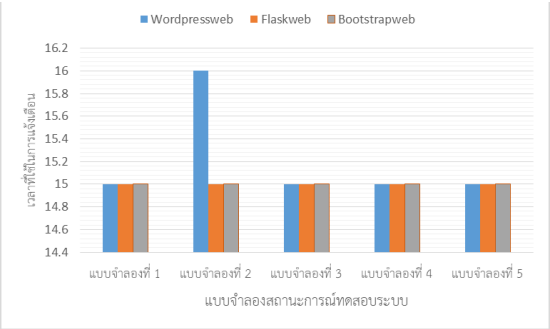


ภาพที่ 5 โครงสร้างการทดสอบตามแบบจำลอง

4 ผลการดำเนินงาน

4.1 ผลการทดสอบประสิทธิภาพของระบบ

ผู้วิจัยได้นำปัจจัยเรื่องเวลาในการตอบสนองแจ้งเตือนมาเป็นตัวกำหนดประสิทธิของระบบโดย การแจ้งเตือนจะต้องไม่เกิน 15 วินาที หลังจากหน้าเว็บไซต์เป้าหมายถูกโจมตีเปลี่ยนแปลงแก้ไขด้วย แบบจำลองสถานการณ์ที่สร้างขึ้น โดยข้อมูลประวัติการเฝ้าระวังจะอ้างอิง ข้อมูลวันที่ดำเนินการทดสอบ ผู้วิจัยได้เก็บข้อมูลมาวิเคราะห์พบว่า **การแจ้งมีประสิทธิภาพถึง 93.33 เปอร์เซ็นต์** จะมี 1 เหตุการณ์ที่เกินคือ wordpressweb แบบจำลองที่ 2 ฝั่งลิงค์แปลกปลอม เนื่องจากการ wordpressweb เป็นการพัฒนาแบบ CMS มีโครงสร้างการทำงานเบื้องหลังที่ซับซ้อน การแสดงผลหน้าเว็บไซต์ จะต้องเรียกไฟล์เบื้องหลังมาแสดง จึงทำให้การได้รับข้อมูลซอร์สโค้ดช้าลง แสดงผลตามภาพที่ 6



ภาพที่ 6 กราฟแสดงผลการทดสอบประสิทธิภาพของระบบ

4.2 การแสดงผลการวิเคราะห์ระดับผลกระทบของระบบ

ผู้วิจัยได้ศึกษาผลกระทบการโจมตีเว็บไซต์ โดยวิเคราะห์ค่าความแตกต่างของซอร์สโค้ดตามเงื่อนที่กำหนด ผู้วิจัยได้วิเคราะห์ค่าเพื่อเป็นข้อมูลในการตัดสินใจตอบสนอง ต่อเหตุการณ์ เมื่อเกิดการโจมตี

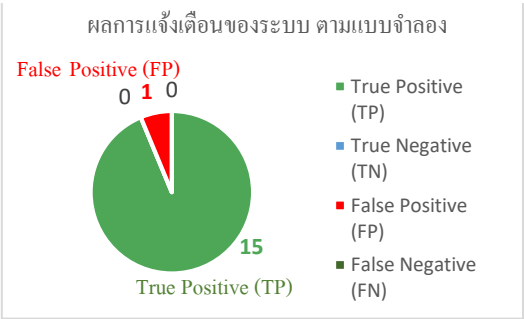
ตารางที่ 1 แสดงระดับผลกระทบที่ระบบแจ้งเตือน

จำลองเหตุการณ์การโจมตี	ระดับผลกระทบที่ระบบแจ้งเตือน		
	Wordpressweb	Bootstrapweb	Flaskweb
จำลองเหตุการณ์ที่ 1 เปลี่ยนหน้าเว็บไซต์	ถูกเปลี่ยนหน้าเว็บอย่างร้ายแรง	ถูกเปลี่ยนแปลงหน้าเว็บ	ถูกเปลี่ยนแปลงหน้าเว็บ
จำลองเหตุการณ์ที่ 2 ฝั่งลิงค์ปลอม	Website ถูกเพิ่มข้อมูล	Website ถูกเพิ่มข้อมูล	Website ถูกเพิ่มข้อมูล
จำลองเหตุการณ์ที่ 3 แก้ไขเนื้อหาสำคัญ	ควรตรวจสอบเพิ่มเติม	ควรตรวจสอบเพิ่มเติม	ควรตรวจสอบเพิ่มเติม
จำลองเหตุการณ์ที่ 4 แก้ไขเนื้อหาหลัก	Website ถูกเพิ่มข้อมูล	ถูกเปลี่ยนหน้าเว็บอย่างร้ายแรง	ถูกเปลี่ยนหน้าเว็บอย่างร้ายแรง
จำลองเหตุการณ์ที่ 5 ฝั่งคำสั่งเรียกเว็บไซต์ปลอม	Website ถูกเพิ่มข้อมูล	Website ถูกเพิ่มข้อมูล	Website ถูกเพิ่มข้อมูล

5. สรุปผลการวิจัย

สารนิพนธ์เล่มนี้นำเสนอการพัฒนาระบบเฝ้าระวังและแจ้งเตือนการโจมตีเว็บไซต์จากการถูกเปลี่ยนแปลงหน้าเว็บไซต์ (Website Defacement) เพื่อเพิ่มความตระหนักรู้เกี่ยวกับการป้องกันรับมือภัยคุมคามทางไซเบอร์ที่เกี่ยวข้องกับเว็บไซต์ โดยผู้วิจัยคาดหวังว่าระบบเฝ้าระวังและแจ้งเตือนการโจมตีเว็บไซต์จากการถูกเปลี่ยนแปลงหน้าเว็บไซต์ (Website Defacement) จะเป็นเครื่องมือที่ช่วยเพิ่มประสิทธิการเฝ้าระวังและแจ้งเตือน ป้องกันภาพลักษณะขององค์ไม่ให้เสียหาย ให้แก่ หน่วยงานที่นำระบบไปทดลองใช้งานได้ไม่มากก็น้อย ทั้งนี้ผู้วิจัยได้ทดสอบประสิทธิของระบบ ให้ตอบสนองต่อแบบจำลองเหตุการณ์ที่ผู้วิจัยได้สร้างขึ้นสำหรับทดสอบ โดยผลการทดสอบระบบ สรุปได้ดังนี้

5.1 ค่าความแม่นยำ (Accuracy) มีค่าสูงถึง 94.5 เปอร์เซ็นต์ จากการโจมตี 16 เหตุการณ์ 5 แบบจำลองสถานการณ์การโจมตีเว็บไซต์ (Website Defacement) ตามภาพที่ 7 มีการแจ้งเตือนเกิดขึ้นซ้ำอีกครั้ง จากการเฝ้าระวังเว็บไซต์ Wordpressweb การโจมตีของแบบจำลองเหตุการณ์ที่ 5 เนื่องจากการรูปแบบซอร์สโค้ด ที่ฝังเข้าไปไม่ตรงตามโครงสร้างเว็บไซต์สำเร็จรูป จึงทำให้ระบบดึงข้อมูลมาไม่ครบถ้วน ก่อนการวิเคราะห์



ภาพที่ 7 กราฟแสดงผลความแม่นยำของระบบ

5.2 ทดสอบประสิทธิภาพของระบบ มีค่าประสิทธิภาพของระบบ คิดเป็นร้อยละ 93.33 เปอร์เซ็นต์ วัดผลจากระยะเวลาในการแจ้งเตือนเมื่อเกิดเหตุการณ์โจมตี

5.3 ผลการวิเคราะห์ความแม่นยำระดับผลกระทบของระบบ คิดเป็นร้อยละ 86.66 เปอร์เซ็นต์ วัดผลจากค่าความแตกต่างซอร์สโค้ดตามเงื่อนไข

จากผลการทดสอบระบบ เฝ้าระวังเว็บไซต์เป้าหมายตามที่ได้กำหนด และทดสอบโดยการสร้างแบบจำลองเพื่อโจมตี ผู้วิจัยได้สังเกตเห็นว่า การแจ้งเตือน และการวิเคราะห์ผลกระทบที่มาจากระบบ โดยเฉพาะการเฝ้าระวังเว็บสำเร็จรูป (CMS) ผลคือสามารถแจ้งเตือนได้ครบถ้วน แต่สำหรับการวิเคราะห์ผลกระทบจะไม่เหมาะสมกับเว็บสำเร็จรูป (CMS) เนื่องจากมีโครงสร้างการพัฒนาเว็บไซต์ที่ซับซ้อน

เอกสารอ้างอิง

[1] นางสาวรัชดา ธนาดิเรก.เปิดสถิติภัยไซเบอร์ ไทยถูกคุกคาม “551 เหตุการณ์” ในรอบปี หน่วยงานการศึกษา-ภาครัฐโดนมากสุด, 2566 ,https://moneyandbanking.co.th/2023/30244/ [1 พฤศจิกายน 2566]

[2] ETDA. รู้จักและป้องกันภัยจาก Website Defacement, แหล่งที่มา : https://www.etda.or.th/th/OurService/ThaiCERT/IncidentCoordination/Information/Published-documents/Technical/paperstechnical/รู้จักและป้องกันภัยจาก-Website-Defacement.aspx

[3] Victorio Duran.How to Prevent Website Defacement, March 11th, 2021 , แหล่งที่มา : https://www.websitepulse.com/blog/how-to-prevent-website-defacement

[4] Punsiri Boonyakiat. มาเข้าใจภาพรวมการทำ Web scraping กันเถอะ !!, Jan 19, 2021 https://punsiriboonyakiat.medium.com/มาเข้าใจภาพรวมการทำ-web-scraping-กันเถอะ-e703f668f2c7

[5] Understanding the Software Development Life Cycle (SDLC), JULY 25, 2023, แหล่งที่มา: https://www.vultureprime.com/blogs/understanding-the-software-development-life-cycle-sdlc

[6] ธวิช พงษ์รชนี.ระบบเฝ้าระวังและตรวจจับภัยคุกคามเว็บเซิร์ฟเวอร์, สารนิพนธ์วิทยาศาสตร์ มหาวิทยาลัยเทคโนโลยีมหานคร,ปีการศึกษา 2022

[7] เกียรติศักดิ์ ลุยทอง,เอกฉัตร บ่ายคล้อย,ประสงค์ ประณีตพลกรัง.การพัฒนาระบบเฝ้าระวังภัยคุกคามตรวจหาการบุกรุก และแจ้งเตือน การรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก,ปีที่ 5 ฉบับที่ 5 เดือนกันยายน – ตุลาคม 2561,สาขาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยศิลปากร

[8] วินิดา แช่ตั้ง และศิรปัฐช์ บุญครอง การวิเคราะห์ความปลอดภัยของฟังก์ชั่นแฮช Effectiveness Analysis and Hash Function,เผยแพร่ เมื่อ พ.ค. - ส.ค. 2560,คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

[9] ผศ.ดร. สุชาติ คุ้มมะณี, เชี่ยวชาญการเขียนโปรแกรมด้วยไพธอน หนังสือ Python เผยแพร่เมื่อ 14 ต.ค.58 แก้ไขล่าสุดเมื่อ 13 ม.ค.61

[10] OWASP Top Ten, 2021 , แหล่งที่มา : https://owasp.org/www-project-top-ten/ [1 พฤศจิกายน 2566]

[11] Armin Ronacher, บทเรียน Python - Flask Framework, 2023,แหล่งที่มาhttps://www.mindphp.com/บทเรียนออนไลน์/python-framework-flask/8081-python-flask framework.html