

บทที่ 4

ผลการดำเนินงาน

จากการวิเคราะห์ข้อมูลภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021 เพื่อใช้สำหรับเผยแพร่ข้อมูลบนเว็บไซต์ มีวัตถุประสงค์เพื่อพัฒนาเว็บไซต์สำหรับวิเคราะห์ข้อมูลภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021 เพื่อให้ได้เว็บไซต์ที่รวมแหล่งข้อมูลความรู้ทั่วไปเกี่ยวกับข้อมูลภัยคุกคามบนเว็บไซต์ และแสดงกระบวนการวิเคราะห์ข้อมูล ที่สามารถนำไปใช้งานได้จริงมีประสิทธิภาพ โดยผู้วิเคราะห์ข้อมูลได้ทำการวิเคราะห์ข้อมูล และนำเทคโนโลยีสารสนเทศเข้าช่วยในการนำเสนอข้อมูล ทำให้มีความสะดวกรวดเร็วและสามารถใช้งานได้จริงจนสำเร็จลุล่วงตามเป้าหมาย

4.1 ผลการดำเนินงาน

การจัดทำโครงการเรื่อง การวิเคราะห์ข้อมูล ภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021 เพื่อใช้สำหรับเผยแพร่ข้อมูลบนเว็บไซต์ ในครั้งนี้พบว่าการจำแนกข้อมูลออกเป็นประเภทต่าง ๆ ช่วยให้เกิดความเข้าใจต่อข้อมูลและสิ่งที่ต้องการทราบอย่างแท้จริง ผู้วิเคราะห์ข้อมูลได้ทำการวิเคราะห์ข้อมูลในรูปแบบของ Data mining โดยทำการจำแนกข้อมูลเป็นประเภทต่าง ๆ ด้วยเทคนิคการทำเหมืองข้อมูลแบบ Classification จากเทคนิคการจำแนกข้อมูลด้วยการวิเคราะห์ในรูปแบบของแผนภูมิต้นไม้หรือเรียกว่า Decision Tree และการนำเสนอสารสนเทศแบบ Visualization เผยแพร่ข้อมูลสารสนเทศขึ้นบนเว็บไซต์ ให้กับผู้ใช้งาน ซึ่งจะช่วยให้เข้าใจได้อย่างรวดเร็ว เพื่อเพิ่มประสิทธิภาพให้กับการศึกษา ค้นคว้าและทันต่อเวลา ผู้วิเคราะห์ข้อมูลจึงได้ทำการวิเคราะห์ข้อมูล และจัดทำเว็บไซต์ตามวัตถุประสงค์ที่กำหนดไว้และมีผลการดำเนินงาน ดังนี้



ภาพที่ 4.1 แสดงหน้าเว็บไซต์หลัก

จากภาพที่ 4.1 แสดงหน้าเว็บไซต์หลัก โดยจะมีเมนูต่าง ๆ ให้เลือก เช่น บทความ, รูปแบบการโจมตี, เกี่ยวกับ, การวิเคราะห์ข้อมูล เป็นต้น



ภาพที่ 4.2 แสดงหน้าเว็บไซต์หน้าแรก

จากภาพที่ 4.2 แสดงหน้าเว็บไซต์หน้า โดยจะแสดง ข้อความยินดีต้อนรับเข้าสู่เว็บไซต์



Web Application คืออะไร?
 Web Application คือโปรแกรมหนึ่งที่ถูกเขียนโดย Developers โดยใช้ HTTP(Hypertext Transfer Protocol) เป็นตัวนำส่งข้อมูลระหว่าง Client(Web Browser) กับ Server(Web Server(Web Application) Web Server) คือ Service ที่ทำให้ WebApp ทำงานได้ เช่น Apache, Nginx ส่วน Web Application เรายังเข้าใจอีก PHP, ASP.NET, JSP ที่เหล่าท่านผู้เขียนให้มันทำงานตามที่ตั้งของมันและ เอลงชื่อใหม่ว่า

Web Hacking
 เพราะอะไรเว็บไซต์ไทยและต่างประเทศถึงโดน Hack กันมากมายเหลือเกินในทุกวันนี้ ? ที่ผ่านมามันไม่ค่อยได้เห็นบทความเกี่ยวกับการเจาะ Web Application Hacking สักเท่าไร เพราะว่าการเจาะคืออันตรายถึงชีวิตซึ่งนำไปใช้ในทางที่ผิด แต่ทุกวันนี้มี Tools ที่ช่วยในการแฮคมากมายและเป็นฟรีกันแพร่หลายในกลุ่ม Hacker หรือ Script Kiddies ทำให้การแฮคทำได้ง่ายมากในปัจจุบัน จึงมีนักแฮคที่เจอทีและชื่อเสียง

ที่มา : <https://adms.usastylevids.com/uploads/148721a1e4%20.jpg>

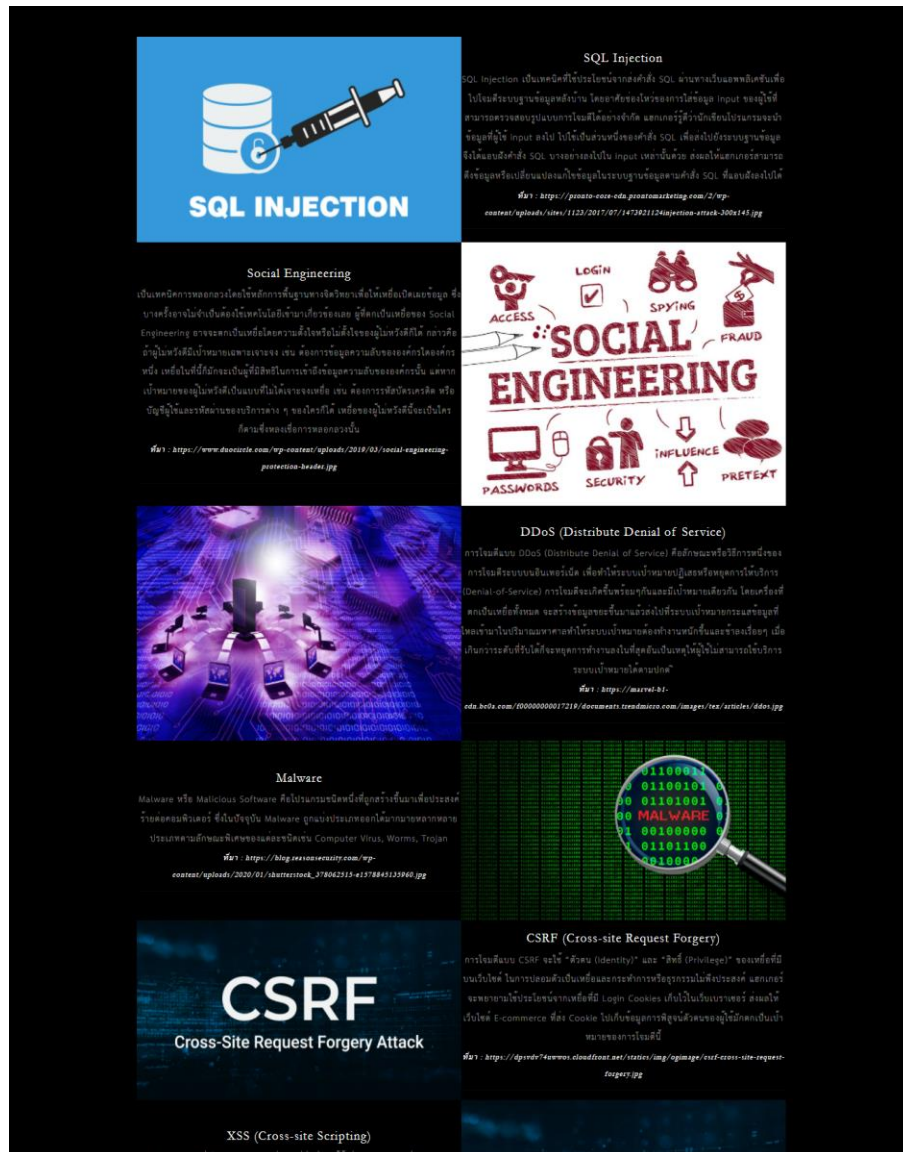
ข้อเสีย ก็คือมีเว็บไซต์ที่ถูกแฮคกันเป็นวงกว้างที่รู้ตัวและไม่รู้ตัวโดน Hack แล้วโดยที่คนที่ใช้ Tools เหล่านี้ในการ Hack ไม่จำเป็นต้องมีความรู้หรือเลยคืออย่า ขี้ว่าไม่จำเป็นต้องรู้เลย แควง URL คลิ๊กลงสามที่ก็ Hack ได้แล้ว ในเมื่อการ Hack ทำได้ง่ายขนาดนี้ นี่เป็นสาเหตุให้เด็ก ๆ สามารถที่จะ Hack เว็บไซต์นั้นเป็นเรื่องที่ง่ายมาก

ที่มา : <http://www.malware.com/wp-content/uploads/2016/02/Security.jpg>

ข้อดี ก็คือในส่วนของผู้สร้างระบบซึ่งมีความรู้ในระบบที่ตัวเองสร้างเป็นอย่างไร มันก็สามารถใช้ Tools ฝึกถนัดในการทดสอบความปลอดภัยของตัวเองได้เองได้อย่างง่ายดาย ขอเพียงแค่ความสนใจสักหน่อยเท่านั้นเอง อย่างข้อที่ผู้รับที่หน้าสร้างไม่ควรถูก Hack ด้วย Automated Hacking Tools สำเร็จรูปที่เค้าน้อยก็ใช้ Hack ได้

ภาพที่ 4.3 แสดงหน้าเว็บไซต์เมนูบทความ

จากภาพที่ 4.3 แสดงหน้าเว็บไซต์เมนูบทความ บทความการโจมตีบนเว็บไซต์



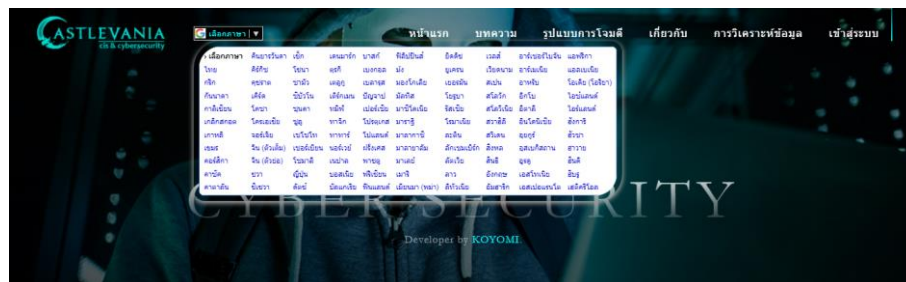
ภาพที่ 4.4 แสดงหน้าเว็บไซต์เมมูรูปแบบการโจมตี

จากภาพที่ 4.4 แสดงหน้าเว็บไซต์เมมูรูปแบบการโจมตี บทความรูปแบบการโจมตีบนเว็บไซต์แบบต่าง ๆ



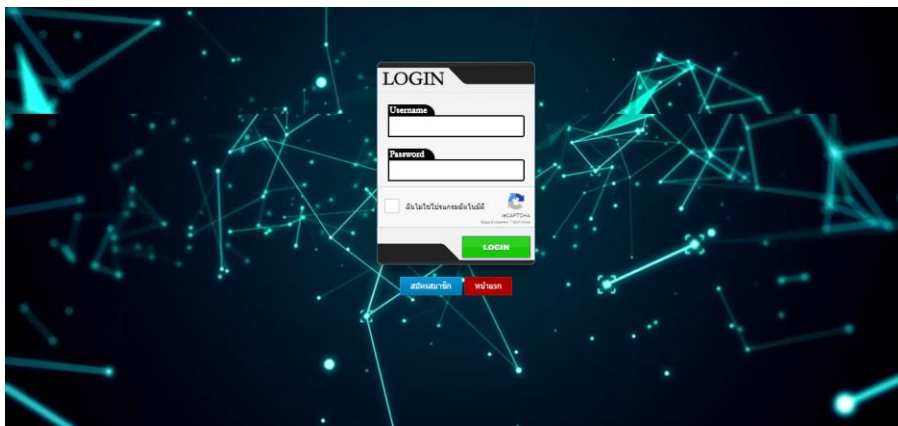
ภาพที่ 4.5 แสดงหน้าเว็บไซต์เมนูเกี่ยวกับ

จากภาพที่ 4.5 แสดงหน้าเว็บไซต์เมนูเกี่ยวกับ โดยจะมีชื่อผู้จัดทำโครงการ ชื่ออาจารย์ที่ปรึกษา สาขาวิชา



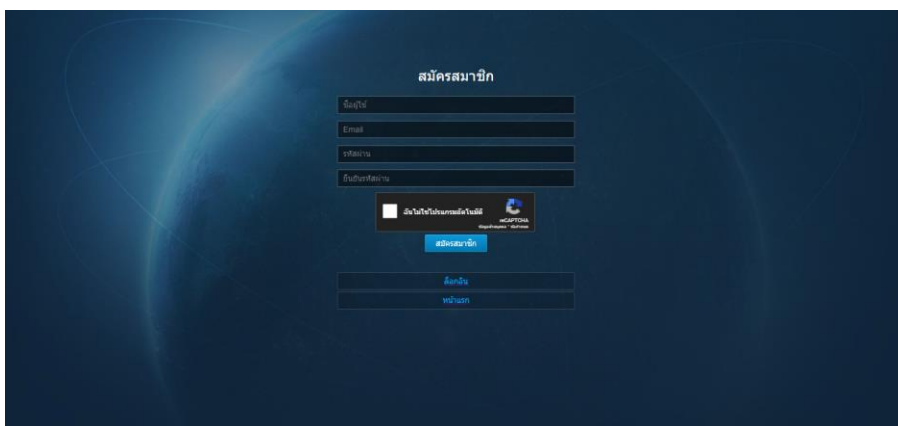
ภาพที่ 4.6 แสดงหน้าเว็บไซต์เมนูเปลี่ยนภาษาของเว็บไซต์

จากภาพที่ 4.6 แสดงหน้าเว็บไซต์เมนูเปลี่ยนภาษาของเว็บไซต์ โดยการแปลภาษาที่เลือกจะแปลผ่าน google translate ซึ่งอาจจะแปลไม่ตรงหลักไวยากรณ์ของภาษา



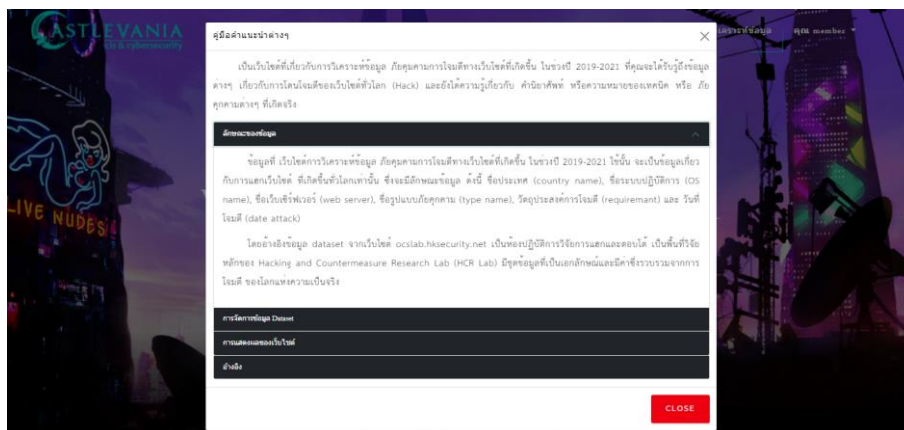
ภาพที่ 4.7 แสดงหน้าเว็บไซต์ login

จากภาพที่ 4.7 แสดงหน้าเว็บไซต์ login เพื่อเข้าสู่เว็บไซต์ โดยการพิมพ์ username และ password เพื่อเข้าสู่เว็บไซต์



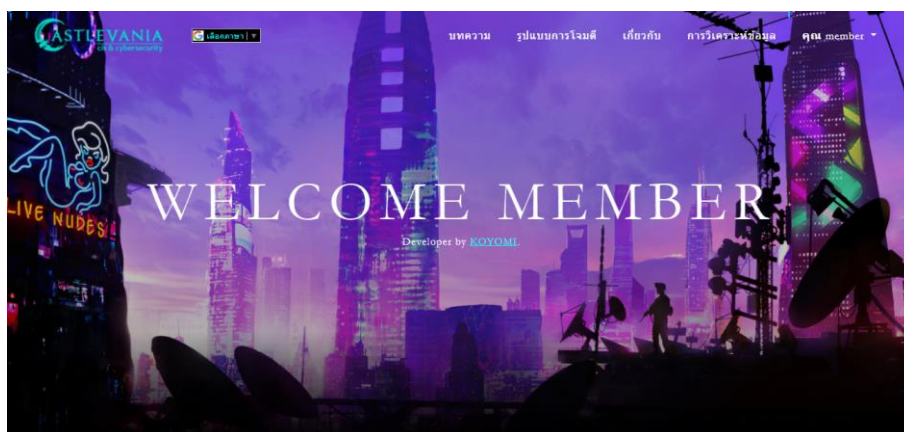
ภาพที่ 4.8 แสดงหน้าเว็บไซต์ การสมัครสมาชิก

จากภาพที่ 4.8 แสดงหน้าเว็บไซต์ การสมัครสมาชิก สำหรับผู้ที่ต้องการสมัครสมาชิกเพื่อใช้งาน ส่วนต่าง ๆ ที่มีมากกว่า บุคคลทั่วไป



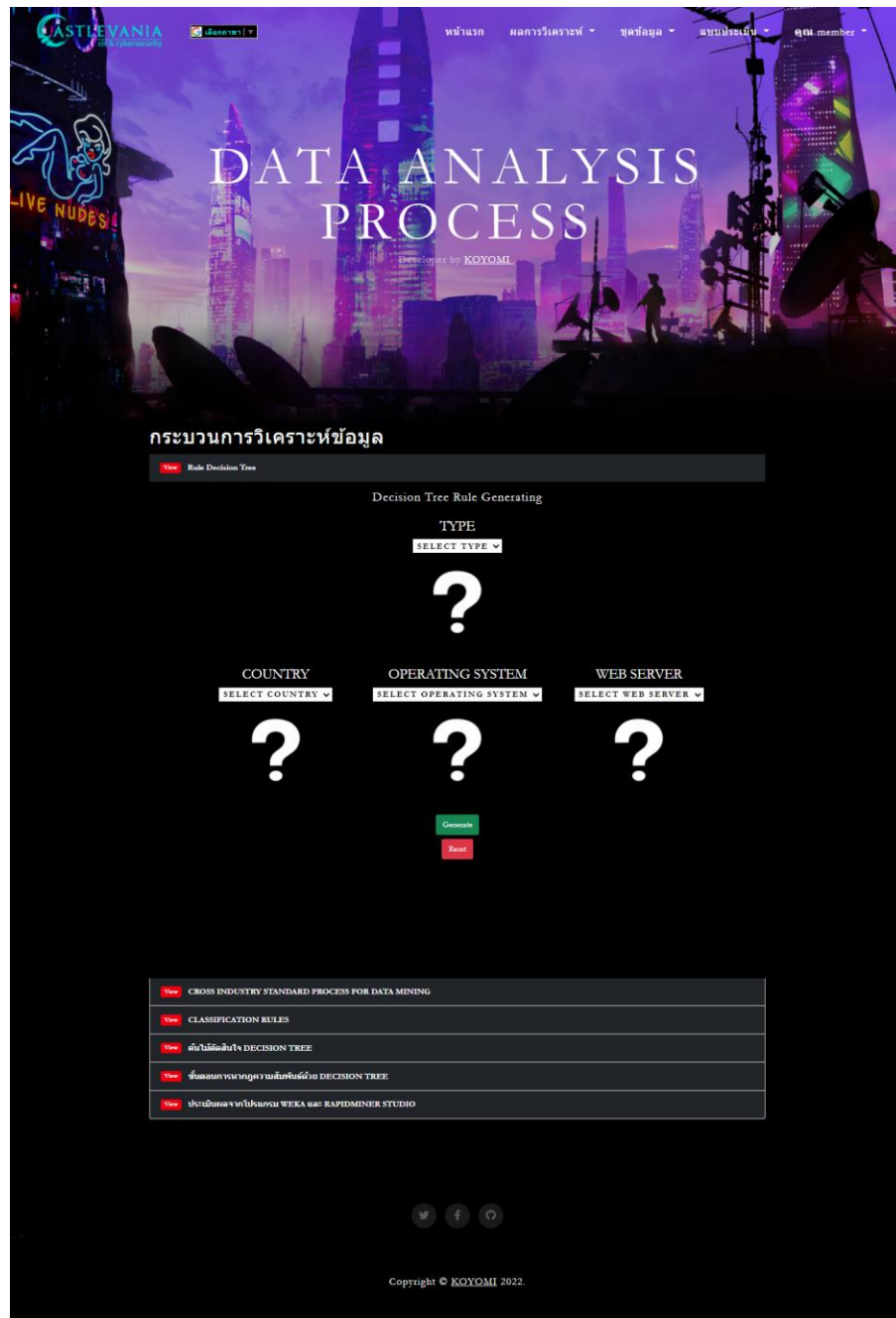
ภาพที่ 4.9 แสดงคู่มือการใช้งานของเว็บไซต์

จากภาพที่ 4.9 แสดงหน้าเว็บไซต์หลักของสมาชิก เมื่อเข้าสู่ระบบจะแสดงคู่มือการใช้งานของเว็บไซต์ขึ้นมาเป็นลำดับแรก เพื่อบอกถึงคำแนะนำการใช้งานของส่วนต่าง ๆ ของเว็บไซต์



ภาพที่ 4.10 แสดงหน้าเว็บไซต์หลักของสมาชิก

จากภาพที่ 4.10 แสดงหน้าเว็บไซต์หลักของสมาชิก โดยจะมีเมนูต่าง ๆ ให้เลือก เช่น บทความ, รูปแบบการโจมตี, เกี่ยวกับ, การวิเคราะห์ข้อมูล เป็นต้น แต่เมนูการวิเคราะห์ข้อมูลจะมีเมนูย่อยเพิ่มขึ้นมา



ภาพที่ 4.11 แสดงหน้าเว็บไซต์เมนูกระบวนการวิเคราะห์ข้อมูล

จากภาพที่ 4.11 แสดงหน้าเว็บไซต์เมนูกระบวนการวิเคราะห์ข้อมูล แสดงกฎต้นไม้การตัดสินใจของภัยคุกคามบนเว็บไซต์

ASTLEVANIA
DATA ANALYSIS

หน้าแรก ผลการวิเคราะห์ ชุดข้อมูล สมาชิก member

DATA ANALYSIS PROCESS

Developer by KOYOMI

กระบวนการวิเคราะห์ข้อมูล

New Rule Decision Tree

Decision Tree Rule Generating

TYPE
SELECT TYPE

SQL → Thailand = RED TEAM

กฎข้อที่ได้

IF type = SQL-Injection AND country = Thailand THEN requirement AX

ถ้าพบการโจมตีเป็น SQL-Injection ในประเทศไทย
ผลการพิจารณาว่า การโจมตีที่เกิดขึ้นนี้ให้ผลลัพธ์ว่า เป็นการโจมตีเพื่อผลประโยชน์ส่วนกลางโจมตี

Close

- New CROSS INDUSTRY STANDARD PROCESS FOR DATA MINING
- New CLASSIFICATION RULES
- New ต้นไม้ตัดสินใจ DECISION TREE
- New ขั้นตอนการหาความสัมพันธ์ด้วย DECISION TREE
- New ประเด็นจากโปรแกรม WEKA aka: RAPIDMINER STUDIO

Copyright © KOYOMI 2022.

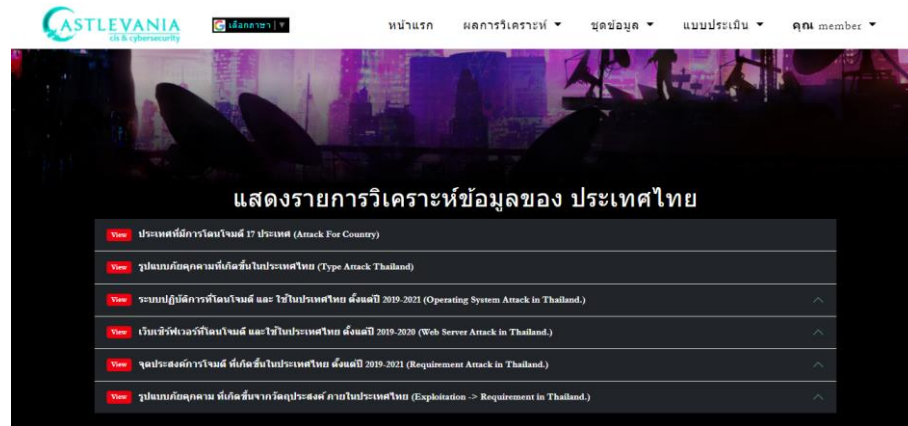
ภาพที่ 4.12 แสดงหน้าเว็บไซต์กฎต้นไม้ตัดสินใจ

จากภาพที่ 4.12 แสดงหน้าเว็บไซต์กฎต้นไม้ตัดสินใจ โดยมีให้เลือก ประเทศ รูปแบบการโจมตี เว็บเซิร์ฟเวอร์ ระบบปฏิบัติการ เพื่อแสดงแนวโน้มการเกิดภัยคุกคามบนเว็บไซต์

The screenshot shows a website with a dark background and a city skyline at night. The main heading is "DATA ANALYSIS PROCESS" with "Developer by KOYOMI" below it. The page content is in Thai and includes a section titled "กระบวนการวิเคราะห์ข้อมูล" (Data Analysis Process) which features a circular diagram of the CRISP-DM process. The diagram shows the following steps: Business Understanding, Data Understanding, Data Preparation, Modeling, Evaluation, and Deployment, all connected in a clockwise cycle. Below the diagram is a URL: https://datawiki.ai/wp-content/uploads/2018/10/CRISP-DM_Process_Diagram-768x768.png. The text below the diagram explains that CRISP-DM is a standard process for data mining with five main phases: Business Understanding, Data Understanding, Data Preparation, Modeling, and Evaluation. It also mentions that the process can be applied to various data types and techniques like Classification, Clustering, and Association rules. Below this is another section titled "CLASSIFICATION RULES" with a blue header and the word "CLASSIFICATION" in white. A URL is provided: <https://images.thetopix.com/definition/term-image/13779/classification>. The text explains that classification is a type of machine learning where a model is trained on a set of data to predict the class of new data points. It also lists two main types of classification: 1. การสร้างแบบจำลอง (Model construction) and 2. การประเมินผล (Evaluation). The first type involves creating a model from training data, and the second involves testing the model on new data to see how well it performs.

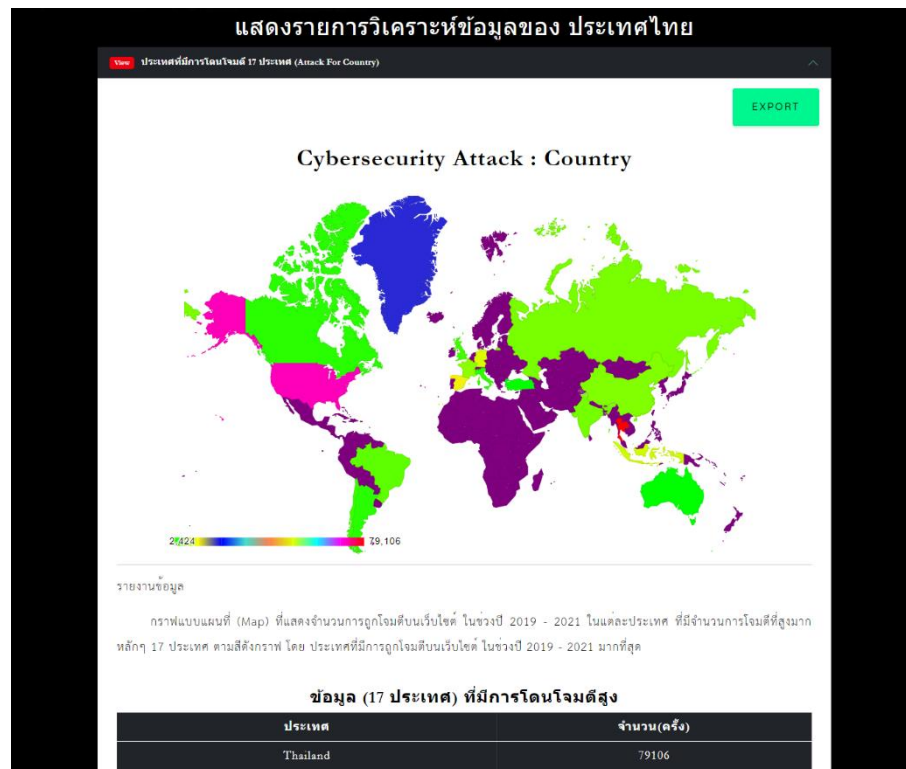
ภาพที่ 4.13 แสดงหน้าเว็บไซต์กระบวนการวิเคราะห์ crisp - dm

จากภาพที่ 4.13 แสดงหน้าเว็บไซต์กระบวนการวิเคราะห์ crisp - dm



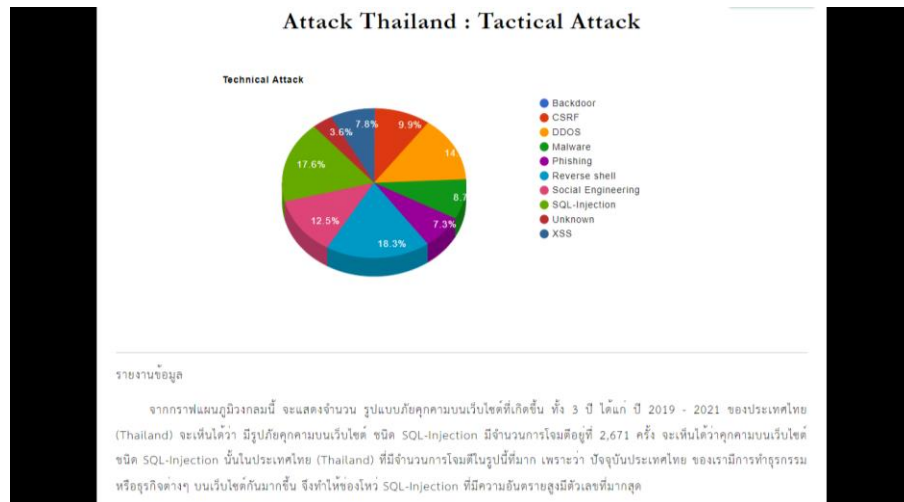
ภาพที่ 4.14 แสดงหน้าเว็บไซต์รายการวิเคราะห์ข้อมูล ประเทศไทย

จากภาพที่ 4.14 แสดงหน้าเว็บไซต์รายการวิเคราะห์ข้อมูล ประเทศไทย ที่จะแสดงแดชบอร์ด ข้อมูลภัยคุกคามบนเว็บไซต์ ในประเทศไทย



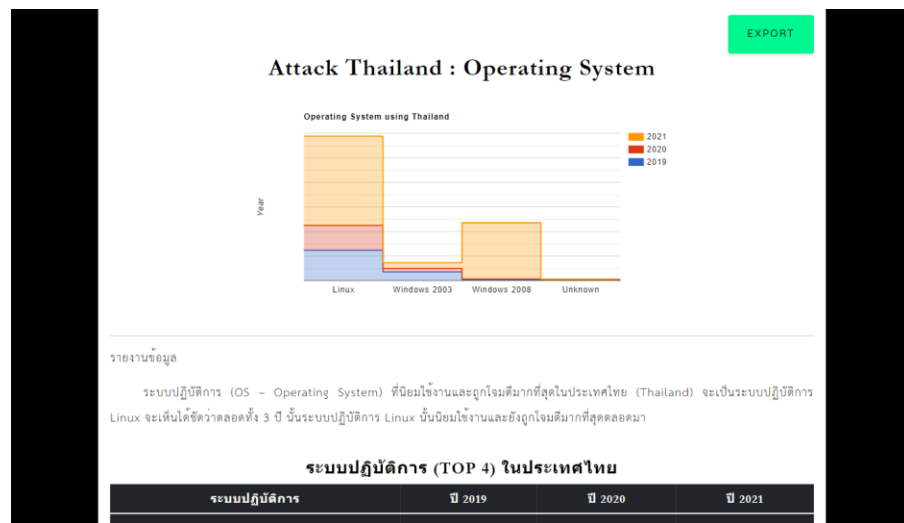
ภาพที่ 4.15 แสดงหน้าเว็บไซต์ ประเทศที่มีการโดนโจมตี 17 ประเทศ (Attack For Country)

จากภาพที่ 4.15 แสดงหน้าเว็บไซต์ ประเทศที่มีการโดนโจมตี 17 ประเทศ (Attack For Country)



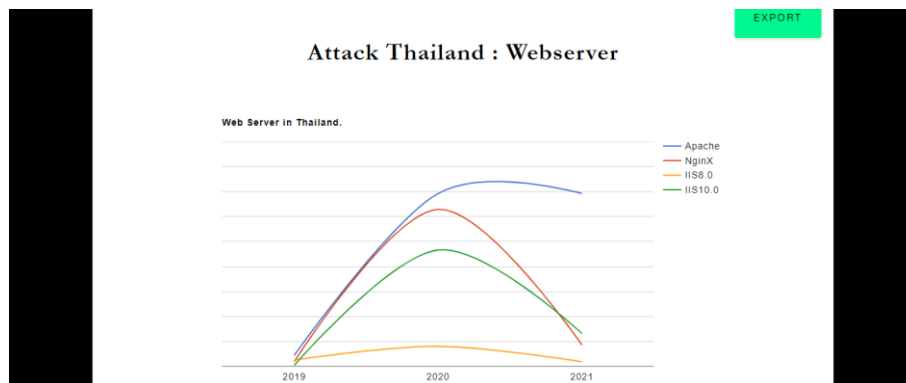
ภาพที่ 4.16 แสดงหน้าเว็บไซต์ รูปแบบภัยคุกคามที่เกิดขึ้นในประเทศไทย (Type Attack Thailand)

จากภาพที่ 4.16 แสดงหน้าเว็บไซต์ รูปแบบภัยคุกคามที่เกิดขึ้นในประเทศไทย (Type Attack Thailand)



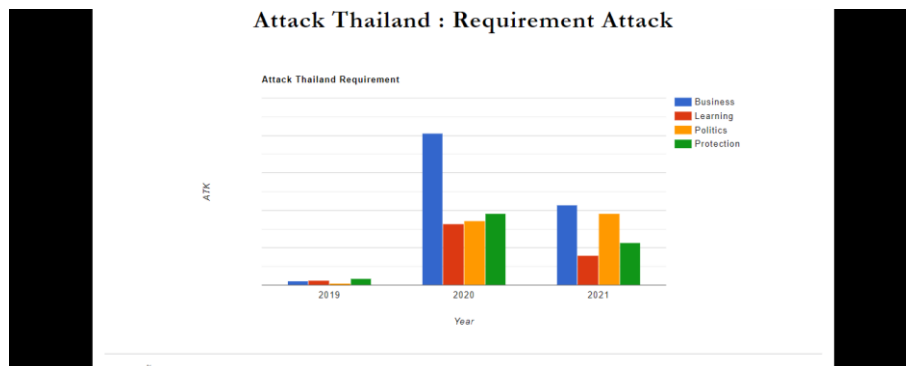
ภาพที่ 4.17 แสดงหน้าเว็บไซต์ ระบบปฏิบัติการที่โดนโจมตี และ ใช้ในประเทศไทย ตั้งแต่ปี 2019-2021

จากภาพที่ 4.17 แสดงหน้าเว็บไซต์ ระบบปฏิบัติการที่โดนโจมตี และ ใช้ในประเทศไทย ตั้งแต่ปี 2019 - 2021



ภาพที่ 4.18 แสดงหน้าเว็บไซต์ เว็บเซิร์ฟเวอร์ที่โดนโจมตี และใช้ในประเทศไทย

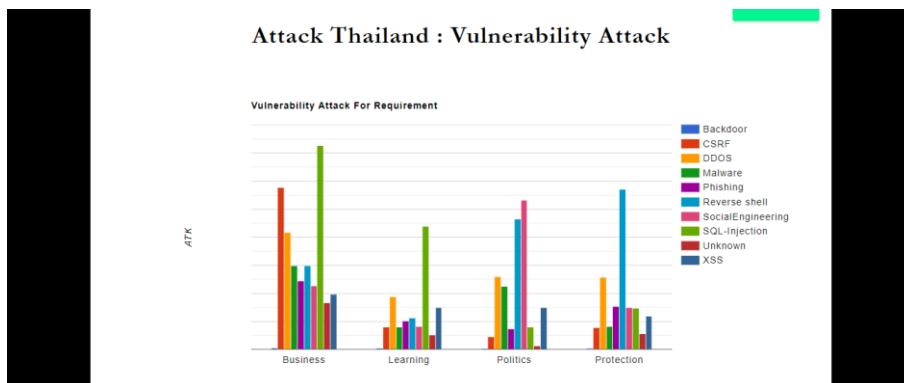
จากภาพที่ 4.18 แสดงหน้าเว็บไซต์ เว็บเซิร์ฟเวอร์ที่โดนโจมตี และใช้ในประเทศไทย



ภาพที่ 4.19 แสดงหน้าเว็บไซต์ จุดประสงค์การโจมตี ที่เกิดขึ้นในประเทศไทย ตั้งแต่ปี 2019-2021

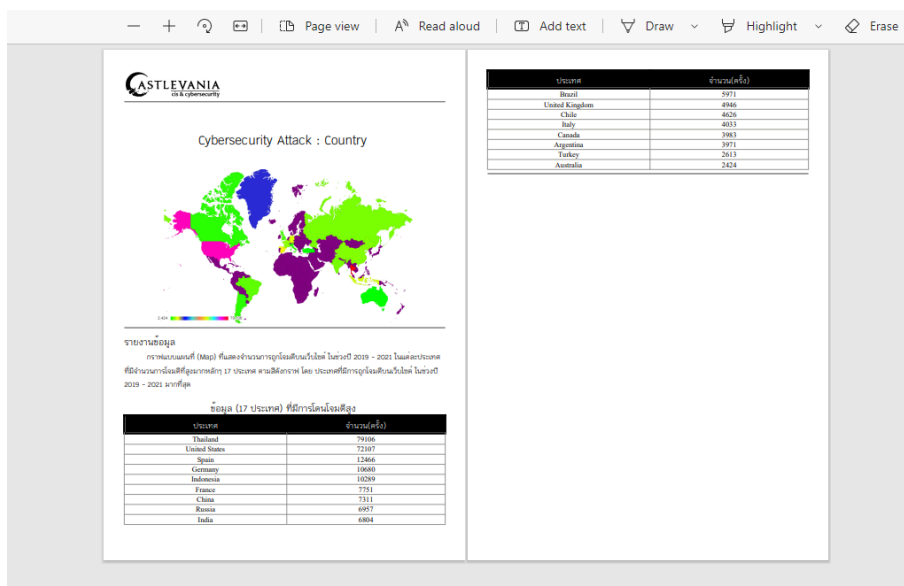
จากภาพที่ 4.19 แสดงหน้าเว็บไซต์ จุดประสงค์การโจมตี ที่เกิดขึ้นในประเทศไทย ตั้งแต่ปี 2019-

2021



ภาพที่ 4.20 แสดงหน้าเว็บไซต์ รูปแบบภัยคุกคาม ที่เกิดขึ้นจากวัตถุประสงค์ ภายในประเทศไทย

จากภาพที่ 4.20 แสดงหน้าเว็บไซต์ รูปแบบภัยคุกคามบนเว็บไซต์ ที่เกิดขึ้นจากวัตถุประสงค์ ภายในประเทศไทย



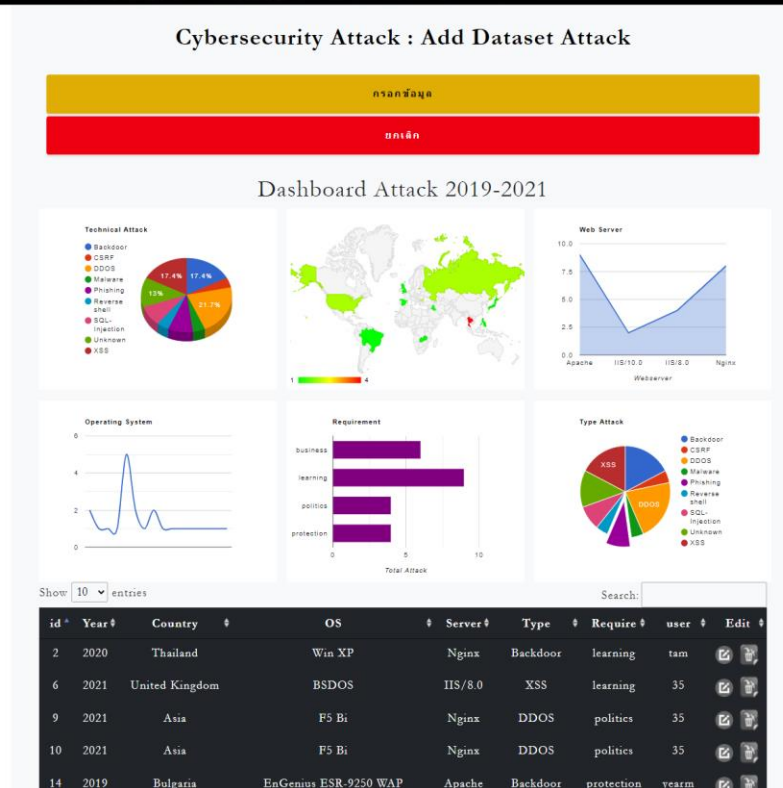
ภาพที่ 4.21 แสดง Preview Print PDF

จากภาพที่ 4.21 สามารถคลิกที่ปุ่ม export เพื่อทำการบันทึก ออกมาเป็น PDF



ภาพที่ 4.22 แสดงหน้าเว็บไซต์ รายการวิเคราะห์ข้อมูล

จากภาพที่ 4.22 แสดงหน้าเว็บไซต์ รายการวิเคราะห์ข้อมูล แสดงข้อมูลภัยคุกคามทั้งหมดของเว็บไซต์ โดยแสดงเป็นแดชบอร์ด กราฟต่าง ๆ



ภาพที่ 4.23 แสดงหน้าเว็บไซต์ เพิ่มข้อมูลการโจมตี

จากภาพที่ 4.23 แสดงหน้าเว็บไซต์ เพิ่มข้อมูลการโจมตี โดยจะมีปุ่มให้คลิกเพื่อ กรอกข้อมูลของ ภัยคุกคามบนเว็บไซต์ และแดชบอร์ด ตารางของข้อมูลภัยคุกคามที่มีอยู่ในฐานข้อมูล และจะสามารถ แก้ไข หรือ ลบ ได้เฉพาะของตัวเองเท่านั้น

Cybersecurity Attack : Add Dataset Attack

GUIDELINE

กรอกข้อมูล Data Attack ของท่าน

ชื่อผู้ให้ข้อมูล

เบอร์โทร

E-mail

เลือกประเทศ : รูปแบบการโจมตี :

ระบบปฏิบัติการ : Web Server :

วัตถุประสงค์การโจมตี : ปีที่โจมตี :

หมายเหตุ (ถ้ามี) :

เพิ่ม

ภาพที่ 4.24 แสดงหน้าเว็บไซต์ การกรอกเพิ่มข้อมูลภัยคุกคามบนเว็บไซต์

จากภาพที่ 4.24 แสดงหน้าเว็บไซต์ การกรอกเพิ่มข้อมูลภัยคุกคามบนเว็บไซต์

Cybersecurity Attack : Add Dataset Attack

GUIDELINE

ขั้นตอนที่ 1

กรอก ข้อมูลของท่านให้ครบทุกช่อง

ชื่อผู้ให้ข้อมูล

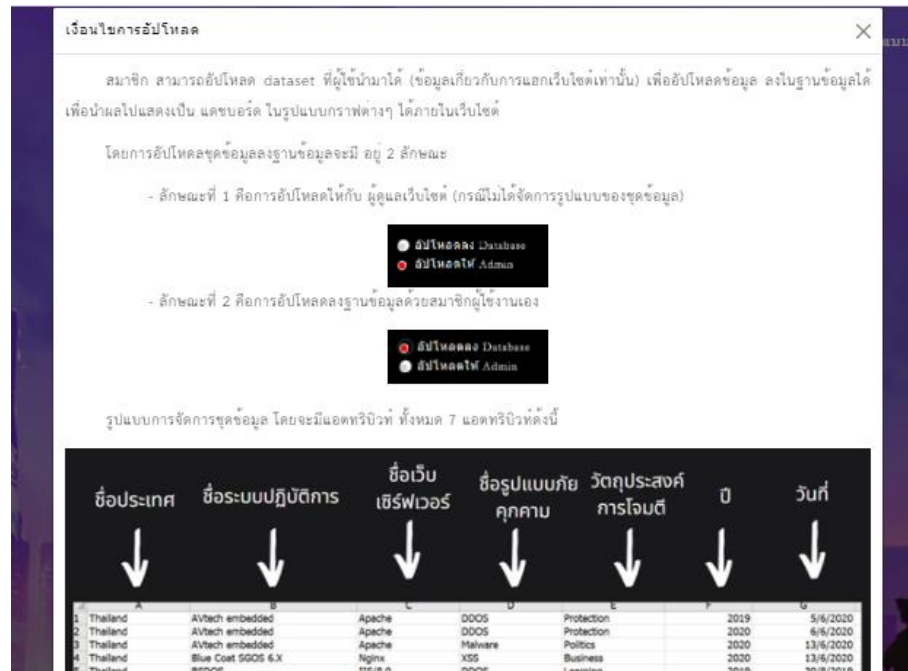
เบอร์โทร

E-mail

เลือกประเทศ : รูปแบบการโจมตี :

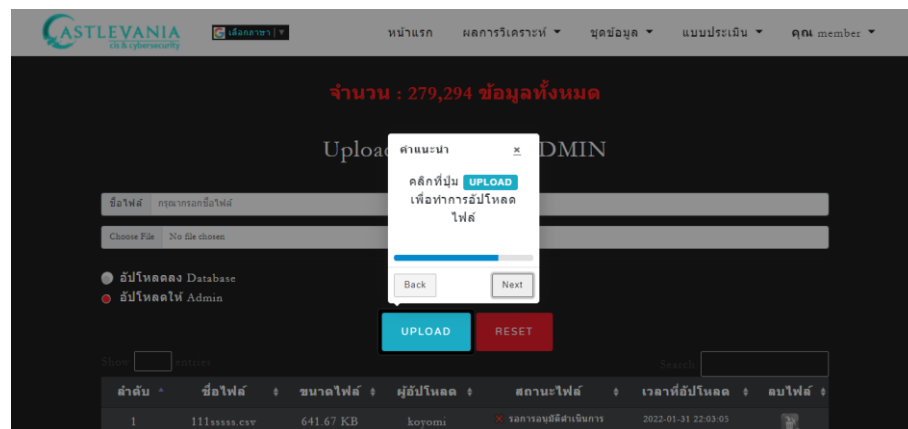
ภาพที่ 4.25 แสดง guideline แนะนำ

จากภาพที่ 4.25 แสดงหน้าเว็บไซต์ guideline แนะนำการกรอกข้อมูลเพิ่ม เพื่อให้สามารถกรอกข้อมูลเข้ามาได้อย่างถูกต้อง



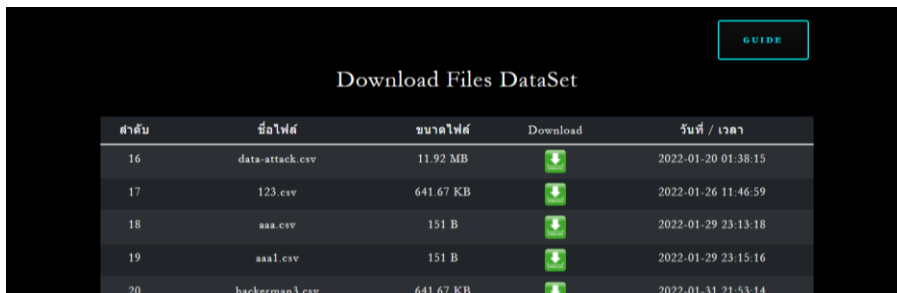
ภาพที่ 4.26 แสดงหน้าเว็บไซต์ เงื่อนไขการอัปโหลด

จากภาพที่ 4.26 แสดงหน้าเว็บไซต์ เงื่อนไขการอัปโหลด เมื่อเข้าสู่หน้าการอัปโหลดจะมีคู่มือบอกรูปแบบการอัปโหลดข้อมูล การจัดการข้อมูลให้อยู่ในรูปแบบที่สามารถอัปโหลดลงฐานข้อมูลได้แบบทันที



ภาพที่ 4.27 แสดงหน้าเว็บไซต์ คำแนะนำการอัปโหลดไฟล์ข้อมูล

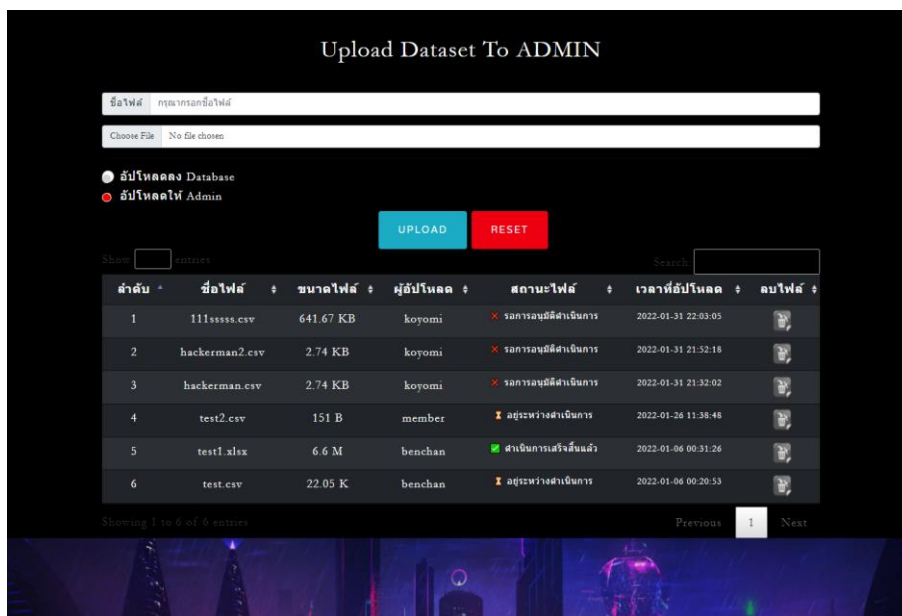
จากภาพที่ 4.27 แสดงหน้าเว็บไซต์ คำแนะนำการอัปโหลดไฟล์ข้อมูล ซึ่งจะบอกวิธีการใช้งาน



| ลำดับ | ชื่อไฟล์ | ขนาดไฟล์ | Download | วันที่ / เวลา |
|-------|-----------------|-----------|----------|---------------------|
| 16 | data-attack.csv | 11.92 MB | | 2022-01-20 01:38:15 |
| 17 | 123.csv | 641.67 KB | | 2022-01-26 11:46:59 |
| 18 | aaa.csv | 151 B | | 2022-01-29 23:13:18 |
| 19 | aaa1.csv | 151 B | | 2022-01-29 23:15:16 |
| 20 | hackerman3.csv | 641.67 KB | | 2022-01-31 21:53:14 |

ภาพที่ 4.28 แสดงหน้าเว็บไซต์ การดาวน์โหลดไฟล์ข้อมูล

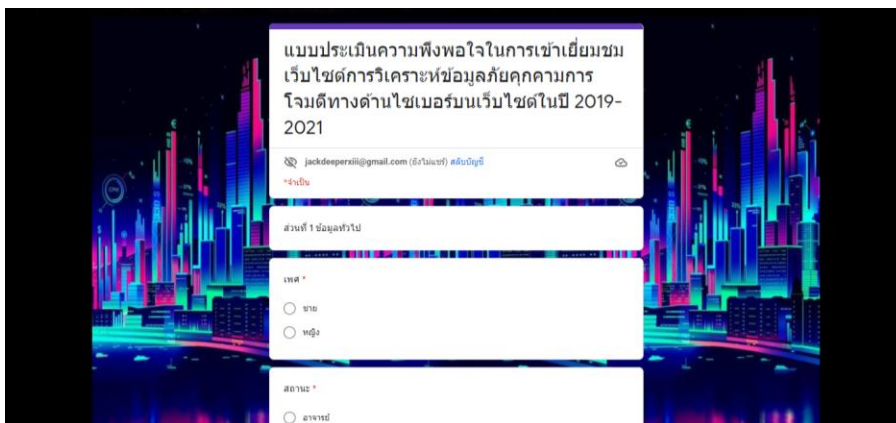
จากภาพที่ 4.28 แสดงหน้าเว็บไซต์ การดาวน์โหลดไฟล์ข้อมูล แสดงข้อมูล data set ต่าง ๆ ที่ผู้ดูแลเว็บไซต์ และสมาชิกของเว็บไซต์ ที่ได้ทำการรวมข้อมูลของภัยคุกคามไว้ในไฟล์ เพื่อเผยแพร่ให้ผู้อื่นสามารถทำการดาวน์โหลดไปศึกษาต่อไปได้



| ลำดับ | ชื่อไฟล์ | ขนาดไฟล์ | ผู้อัปโหลด | สถานะไฟล์ | เวลาที่อัปโหลด | ลบไฟล์ |
|-------|----------------|-----------|------------|-----------------------|---------------------|--------|
| 1 | 111sssss.csv | 641.67 KB | koyomi | ✗ หมดอายุอัตโนมัติ | 2022-01-31 22:03:05 | |
| 2 | hackerman2.csv | 2.74 KB | koyomi | ✗ หมดอายุอัตโนมัติ | 2022-01-31 21:52:18 | |
| 3 | hackerman.csv | 2.74 KB | koyomi | ✗ หมดอายุอัตโนมัติ | 2022-01-31 21:32:02 | |
| 4 | test2.csv | 151 B | member | 🟡 รอระหว่างดำเนินการ | 2022-01-26 11:38:48 | |
| 5 | test1.xlsx | 6.6 M | benchan | 🟢 สำเร็จเสร็จสิ้นแล้ว | 2022-01-06 00:31:26 | |
| 6 | test.csv | 22.05 K | benchan | 🟡 รอระหว่างดำเนินการ | 2022-01-06 00:20:53 | |

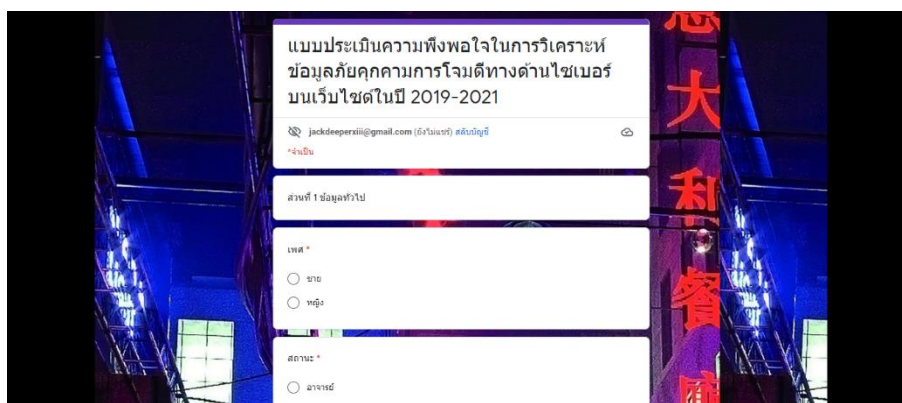
ภาพที่ 4.29 แสดงหน้าเว็บไซต์ การอัปโหลดไฟล์ข้อมูลลงฐานข้อมูล

จากภาพที่ 4.29 การอัปโหลดไฟล์ข้อมูลลงฐานข้อมูล โดยสมาชิกสามารถอัปโหลดไฟล์ data set ได้ 2 วิธีคือ 1.) อัปโหลดลง database เป็นการอัปโหลดไฟล์ลงฐานข้อมูลได้ทันทีไม่ต้องรอให้ ผู้ดูแลเว็บไซต์ 2.) อัปโหลดให้ admin เป็นการอัปโหลดไฟล์ข้อมูลที่ไม่ตรงกับข้อมูลใน ฐานข้อมูลซึ่งต้องรอให้ ผู้ดูแลเว็บไซต์ ทำการตรวจสอบ ข้อมูลปรับเปลี่ยนให้พร้อมที่จะสามารถอัปลงฐานข้อมูลได้ และสามารถที่จะลบไฟล์ของตนเองได้เท่านั้น



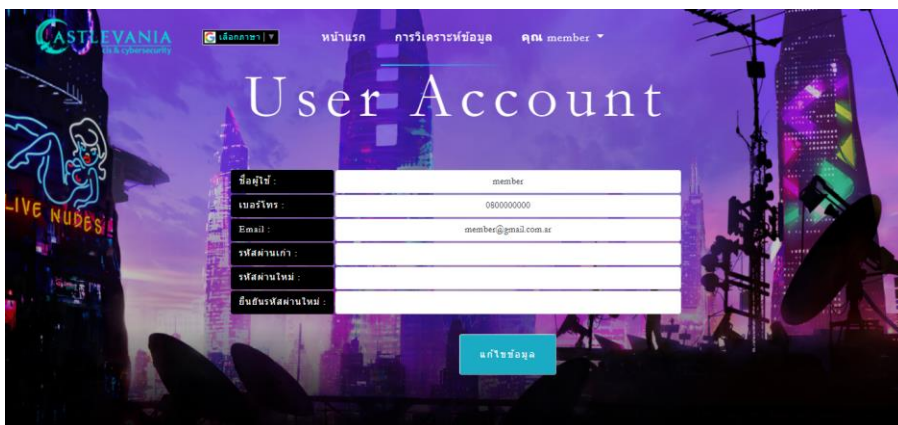
ภาพที่ 4.30 แสดงหน้าเว็บไซต์ แบบประเมินความพึงพอใจของเว็บไซต์

จากภาพที่ 4.30 แสดงหน้าเว็บไซต์ แบบประเมินความพึงพอใจของเว็บไซต์ การให้คะแนนส่วนต่าง ๆ ของเว็บไซต์ความเห็นต่าง ๆ เพื่อให้ได้มีการปรับปรุงเพื่อเติมจุดต่าง ๆ ที่อาจจะไม่ดีมากนักให้พัฒนาเว็บไซต์ให้ดีขึ้น



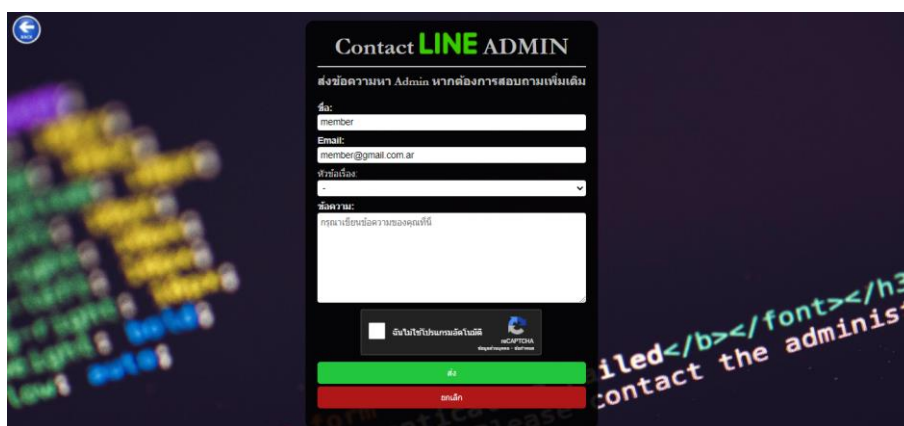
ภาพที่ 4.31 แสดงหน้าเว็บไซต์ แบบประเมินวิเคราะห์ข้อมูล

จากภาพที่ 4.31 แสดงหน้าเว็บไซต์ แบบประเมินวิเคราะห์ข้อมูล เพื่อให้คะแนนความพึงพอใจในการวิเคราะห์ข้อมูล การวิเคราะห์มีความถูกต้อง และใช้งานได้



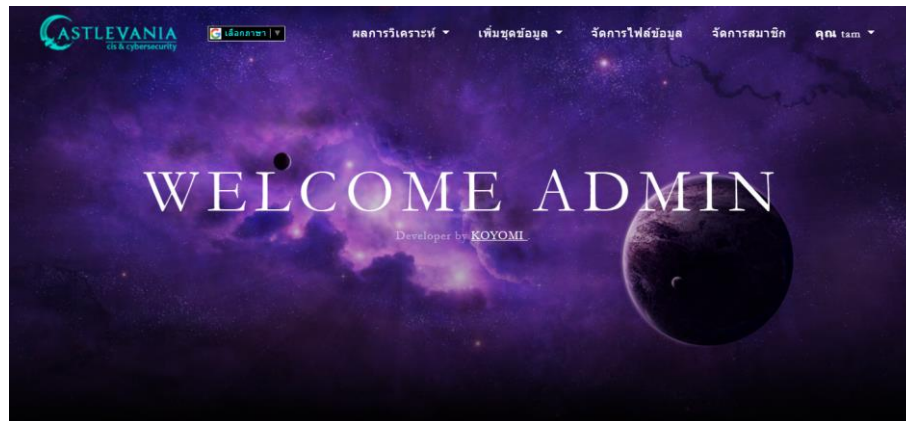
ภาพที่ 4.32 แสดงหน้าเว็บไซต์ การจัดการข้อมูลส่วนตัวของสมาชิก

จากภาพที่ 4.32 แสดงหน้าเว็บไซต์ การจัดการข้อมูลส่วนตัวของสมาชิก สามารถแก้ไขข้อมูลส่วนตัวของตนเองได้



ภาพที่ 4.33 แสดงหน้าเว็บไซต์ การติดต่อผู้ดูแลเว็บไซต์ผ่านทางไลน์

จากภาพที่ 4.33 แสดงหน้าเว็บไซต์ การติดต่อผู้ดูแลเว็บไซต์ผ่านทางไลน์ เป็นการส่งข้อความปัญหาสอบถามรายละเอียดต่าง ๆ กับผู้ดูแลเว็บไซต์



ภาพที่ 4.34 แสดงหน้าเว็บไซต์ หน้าหลักของผู้ดูแลเว็บไซต์

จากภาพที่ 4.34 แสดงหน้าเว็บไซต์ หน้าหลักของผู้ดูแลเว็บไซต์ จะมีเมนูต่าง ๆ เช่น ผลการวิเคราะห์, เพิ่มชุดข้อมูล, จัดการไฟล์ข้อมูล, จัดการสมาชิก เป็นต้น



ภาพที่ 4.35 แสดงหน้าเว็บไซต์ การเพิ่มข้อมูลของผู้ดูแลเว็บไซต์

จากภาพที่ 4.35 แสดงหน้าเว็บไซต์ การเพิ่มข้อมูลของผู้ดูแลเว็บไซต์ โดยจะมีปุ่มให้คลิกเพื่อกรอกข้อมูลของภัยคุกคามบนเว็บไซต์ และแดชบอร์ด ตารางของข้อมูลภัยคุกคามที่มีอยู่ในฐานข้อมูล

Cybersecurity Attack : Add Dataset Attack

GUIDELINE

กรอกข้อมูล Data Attack ของท่าน

ชื่อผู้โจมตี :

เบอร์โทร :

E-mail :

เลือกประเทศ : รูปแบบการโจมตี :

ระบบปฏิบัติการ : Web Server :

วัตถุประสงค์การโจมตี : ปีที่โจมตี :

ภาพที่ 4.36 แสดงหน้าเว็บไซต์ กรอกข้อมูลเพิ่มของผู้ดูแลเว็บไซต์

















จากภาพที่ 4.36 แสดงหน้าเว็บไซต์ กรอกข้อมูลเพิ่มของผู้ดูแลเว็บไซต์ โดยจะมีปุ่มให้คลิกเพื่อกรอกเพิ่มข้อมูลของภัยคุกคามบนเว็บไซต์ และแดชบอร์ด ข้อมูลภัยคุกคามจะเพิ่มไปยังฐานข้อมูล



ภาพที่ 4.37 แสดง guideline คำแนะนำการใช้งาน

จากภาพที่ 4.37 แสดงหน้าเว็บไซต์ guideline คำแนะนำการใช้งานการกรอกข้อมูลเพิ่ม เพื่อให้สามารถกรอกข้อมูลเข้ามาได้อย่างถูกต้อง

Show entries Search:

| id | Year | Country | OS | Server | Type | Require | user | Edit |
|----|------|-------------------|----------------------------------|--------|---------------|------------|--------|---|
| 2 | 2020 | Thailand | Win XP | Nginx | Backdoor | learning | tam |   |
| 9 | 2021 | Asia | F5 Bi | Nginx | DDOS | politics | 35 |   |
| 10 | 2021 | Asia | F5 Bi | Nginx | DDOS | politics | 35 |   |
| 15 | 2021 | Zambia | BSDOS | Nginx | XSS | business | 35 |   |
| 29 | 2021 | Russia | Solar | Nginx | Reverse shell | protection | koyomi |   |
| 35 | 2020 | America | EnGenius embedded | Nginx | Phishing | learning | member |   |
| 36 | 2020 | Brunei Darussalam | Cisco IOS 12.X | Nginx | Unknown | politics | member |   |
| 41 | 2020 | Japan | Dish Network Hopper media device | Nginx | DDOS | Learning | admin |   |

Showing 1 to 8 of 8 entries (filtered from 23 total entries) Previous Next

ภาพที่ 4.38 แสดงการค้นหาค่าต่าง ๆ

จากภาพที่ 4.38 แสดงการค้นหาค่าต่าง ๆ ที่ต้องการค้นหาได้ทุกค่าที่เราต้องการ เช่น การค้นหา Nginx ทั้งหมดที่มีอยู่ในตาราง

Cybersecurity Attack : Add Dataset Attack

[GUIDELINE](#)

กรอกข้อมูล Data Attack ของท่าน

ชื่อผู้ให้ข้อมูล

เบอร์โทร

E-mail

เลือกประเทศ : รูปแบบการโจมตี :

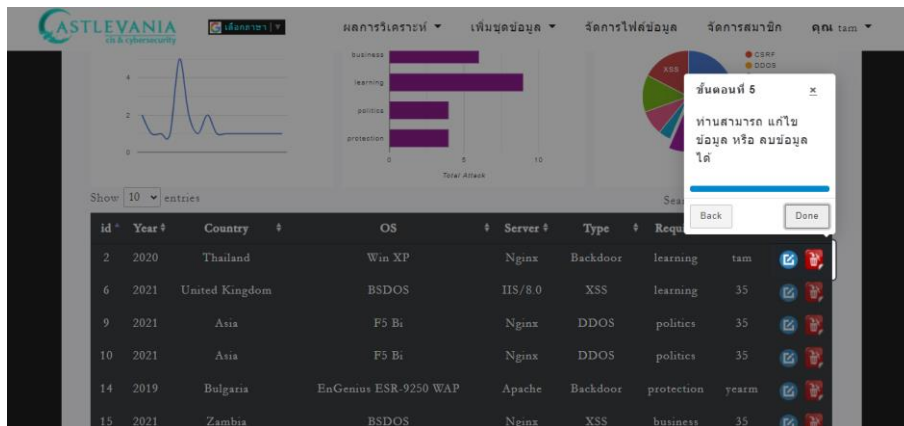
ระบบปฏิบัติการ : Web Server :

วัตถุประสงค์การโจมตี : ปีที่โจมตี :

หมายเหตุ (ถ้ามี) :

ภาพที่ 4.39 แสดงหน้าเว็บไซต์ แก้ไขการกรอกข้อมูลเพิ่ม

จากภาพที่ 4.39 แสดงหน้าเว็บไซต์ แก้ไขการกรอกข้อมูลเพิ่ม สำหรับผู้ที่ต้องการแก้ไขข้อมูลนี้อาจจะเพิ่มเข้ามาผิด



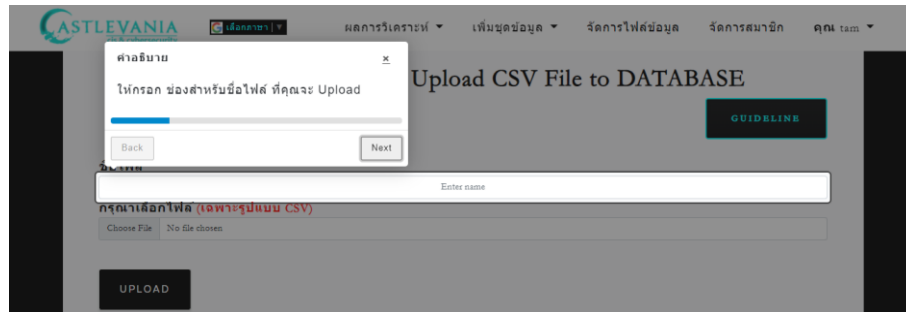
ภาพที่ 4.40 แสดงหน้าเว็บไซต์ แนะนำการแก้ไข

จากภาพที่ 4.40 แสดงหน้าเว็บไซต์ แนะนำการแก้ไข ข้อมูลที่ต้องการเปลี่ยนแปลง



ภาพที่ 4.41 แสดงหน้าเว็บไซต์ การอัปโหลดของผู้ดูแลเว็บไซต์

จากภาพที่ 4.41 แสดงหน้าเว็บไซต์ การอัปโหลดของผู้ดูแลเว็บไซต์ เป็นการอัปโหลดไฟล์ข้อมูลลงฐานข้อมูลมีกราฟแสดงผลเพื่อให้เห็นถึงข้อมูลที่มีการอัปโหลดเข้ามา



ภาพที่ 4.42 แสดง guideline คำแนะนำการใช้งานอัปโหลด

จากภาพที่ 4.42 แสดง guideline คำแนะนำการใช้งานอัปโหลด เพื่อให้สามารถอัปโหลดข้อมูลเข้ามาได้อย่างถูกต้อง



ภาพที่ 4.43 แสดงหน้าเว็บไซต์ จัดการไฟล์ข้อมูล

จากภาพที่ 4.43 แสดงหน้าเว็บไซต์ จัดการไฟล์ข้อมูล เป็นหน้าของการแก้ไข ลบ ชุดข้อมูลต่าง ๆ และ การอัปโหลดไฟล์ชุดข้อมูล

| ลำดับ | ชื่อไฟล์ | ขนาดไฟล์ | Download | จัดการ | วันที่ / เวลา |
|-------|---------------------|-----------|----------|--------|---------------------|
| 16 | data-attack.csv | 11.92 MB | | | 2022-01-20 01:38:15 |
| 17 | 123.csv | 641.67 KB | | | 2022-01-26 11:46:59 |
| 18 | aaa.csv | 151 B | | | 2022-01-29 23:13:18 |
| 19 | aaa1.csv | 151 B | | | 2022-01-29 23:15:16 |
| 20 | hackerman3.csv | 641.67 KB | | | 2022-01-31 21:53:14 |
| 21 | hackerman111.csv | 641.67 KB | | | 2022-01-31 21:56:23 |
| 22 | hackerman1111.csv | 641.67 KB | | | 2022-01-31 21:58:39 |
| 23 | aaasd.csv | 641.67 KB | | | 2022-01-31 21:59:43 |
| 24 | hackermankoyomi.csv | 641.67 KB | | | 2022-01-31 22:03:31 |
| 25 | 111hackermane.csv | 641.67 KB | | | 2022-01-31 22:05:18 |

ภาพที่ 4.44 แสดงหน้าเว็บไซต์ ตารางชุดข้อมูลทั้งหมด

จากภาพที่ 4.44 แสดงหน้าเว็บไซต์ ตารางชุดข้อมูลทั้งหมด ที่ผู้ดูแลอัปโหลดชุดข้อมูลใหม่ ๆ เข้ามาหรือ ข้อมูลที่ได้จากสมาชิกอัปโหลดเข้ามา เพื่อให้สมาชิกสามารถดาวน์โหลดได้

| ลำดับ | ชื่อไฟล์ | ขนาดไฟล์ | ผู้อัปโหลด | สถานะไฟล์ | เวลาที่อัปโหลด | ดาวน์โหลด | ลบไฟล์ |
|-------|----------------|-----------|------------|--------------------------|---------------------|-----------|--------|
| 1 | 111sssss.csv | 641.67 KB | koyomi | ✖ รอกการอนุมัติดำเนินการ | 2022-01-31 22:03:03 | | |
| 2 | hackerman2.csv | 2.74 KB | koyomi | ✖ รอกการอนุมัติดำเนินการ | 2022-01-31 21:52:18 | | |
| 3 | hackerman.csv | 2.74 KB | koyomi | ✖ รอกการอนุมัติดำเนินการ | 2022-01-31 21:52:02 | | |
| 4 | test2.csv | 151 B | member | ⚠ อยู่ระหว่างดำเนินการ | 2022-01-26 11:38:48 | | |
| 5 | test1.xlsx | 6.6 M | benchan | ✅ ดำเนินการเสร็จสิ้นแล้ว | 2022-01-06 00:31:26 | | |
| 6 | test.csv | 22.05 K | benchan | ⚠ อยู่ระหว่างดำเนินการ | 2022-01-06 00:20:53 | | |

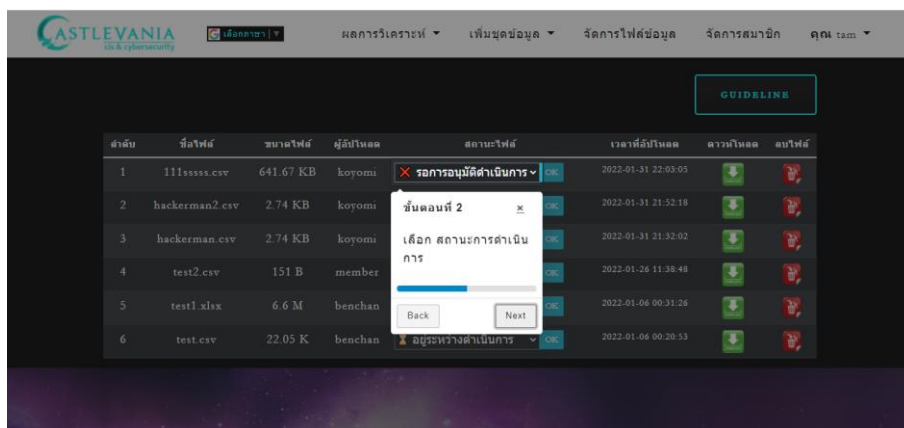
ภาพที่ 4.45 แสดงหน้าเว็บไซต์ การเลือกสถานะของไฟล์

จากภาพที่ 4.45 แสดงหน้าเว็บไซต์ การเลือกสถานะของไฟล์ เป็นหน้าที่ผู้ดูแลเว็บไซต์ จะทำการดาวน์โหลดชุดข้อมูลจากสมาชิกเข้ามาทำการปรับข้อมูลให้เหมาะสมกับฐานข้อมูล ซึ่งจะสามารถเลือกเปลี่ยนสถานะของไฟล์ต่าง ๆ เพื่อให้สมาชิกได้รับรู้ถึงชุดข้อมูลของตนมีการทำงานไปถึงไหนแล้ว



ภาพที่ 4.46 แสดง guideline คำแนะนำการใช้งานอัปโหลดชุดข้อมูล

จากภาพที่ 4.46 แสดง guideline คำแนะนำการใช้งานอัปโหลดชุดข้อมูล เพื่อให้สามารถอัปโหลดข้อมูลเข้ามาได้อย่างถูกต้อง



ภาพที่ 4.47 แสดง guideline คำแนะนำการเปลี่ยนแปลงสถานะ

จากภาพที่ 4.47 แสดง guideline คำแนะนำการเปลี่ยนแปลงสถานะ เพื่อให้สามารถใช้งานได้
อย่างถูกต้อง



ภาพที่ 4.48 แสดงหน้าเว็บไซต์ จัดการสมาชิก

จากภาพที่ 4.48 แสดงหน้าเว็บไซต์ จัดการสมาชิก สามารถแก้ไขสมาชิก หรือ ลบ สมาชิกออกได้



ภาพที่ 4.49 แสดงหน้าเว็บไซต์ จัดการแก้ไขสมาชิก

จากภาพที่ 4.49 แสดงหน้าเว็บไซต์ จัดการแก้ไขสมาชิก สามารถแก้ไขสมาชิก กรอกข้อมูล เปลี่ยนได้ตามต้องการ

จากวัตถุประสงค์การวิเคราะห์ข้อมูลภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021 เพื่อใช้สำหรับเผยแพร่ข้อมูลบนเว็บไซต์ คณะผู้จัดทำได้ศึกษาปัญหา และเก็บรวบรวมข้อมูล ซึ่งคณะผู้จัดทำทำการวิเคราะห์ข้อมูลอยู่ในรูปแบบ Data Mining โดยใช้กระบวนการวิเคราะห์ข้อมูล (CRISP-DM หรือ Cross Industry Standard Process for Data Mining) เพื่อใช้ในการวิเคราะห์ข้อมูลตามขอบเขตของโครงการ ดังนี้

- กระบวนการวิเคราะห์ข้อมูลด้วย CRISP-DM

1) เข้าใจ (Business understanding) ปัญหาในรูปแบบของการวิเคราะห์ข้อมูลทาง Data Mining โดยการวิเคราะห์ข้อมูลในประเด็น ภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์

2) เข้าใจข้อมูล (Data Understanding) และทำการรวบรวมข้อมูลเพื่อตรวจสอบรายละเอียดปริมาณและความน่าเชื่อถือของข้อมูลภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021 จากเว็บไซต์ osclab.hksecurity.net

3) เตรียมข้อมูล (Data Preparation) และทำการคัดเลือกข้อมูลและทำการ Data Cleaning ข้อมูลเพื่อให้ได้ข้อมูลที่สมบูรณ์ ด้วยการตัดข้อมูลในส่วนที่ไม่จำเป็นออกไป เพื่อเหลือ ข้อมูลที่จำเป็นในการนำไปวิเคราะห์ข้อมูล

4) สร้างแบบจำลอง (Modeling) ผู้จัดทำ วิเคราะห์ข้อมูลด้วยการทำเหมืองข้อมูลแบบการจำแนกประเภทข้อมูล (Classification) โดยการใช้โมเดลการตัดสินใจแบบต้นไม้ (Decision Tree) ซึ่งในขั้นตอนนี้จะถูกนำมาใช้เพื่อให้ได้คำตอบที่ดีที่สุด โดยใช้โปรแกรมที่ใช้ทำเหมืองข้อมูล ด้วยชุดข้อมูลที่คัดเลือก

5) การประเมินผล (Evaluation) ผู้จัดทำจะใช้เทคนิคของการจำแนกกลุ่มแบบ Decision Tree: J48 มาใช้ในการศึกษา เนื่องจากให้ผลลัพธ์ของกฎที่สามารถทำนายได้จำนวน 12 กฎ ซึ่งสามารถนำไปใช้ในการแบ่งกลุ่มได้ตามเงื่อนไขได้ชัดเจนและสามารถนำกฎที่ได้มานำไปวิเคราะห์กฎต่อไปได้ โดยสามารถจำแนกกฎที่ได้ ดังนี้

กฎข้อที่ 1 IF type = SQL-Injection AND country = United States AND os = Linux THEN requirement Def หมายความว่า ถ้ารูปแบบการโจมตีเป็น SQL-Injection ในประเทศสหรัฐอเมริกา โดยใช้ระบบปฏิบัติการ Linux เป็นส่วนใหญ่ ผลการพิจารณาพบว่า การโจมตีที่เกิดขึ้นนี้ให้ผลลัพธ์ว่า เป็นการโจมตีเพื่อทดสอบระบบและพัฒนาระบบ

กฎข้อที่ 2 IF type = SQL-Injection AND country = United States AND os = Windows THEN requirement = Atk หมายความว่า ถ้ารูปแบบการโจมตีเป็น SQL-Injection ในประเทศสหรัฐอเมริกา โดยใช้ระบบปฏิบัติการ Windows เป็นส่วนใหญ่ ผลการพิจารณาพบว่า การโจมตีที่เกิดขึ้นนี้ให้ผลลัพธ์ว่า เป็นการโจมตีเพื่อผลประโยชน์ส่วนตัวของผู้โจมตี

กฎข้อที่ 3 IF type = SQL-Injection AND country = Spain THEN requirement = Atk หมายความว่า ถ้ารูปแบบการโจมตีเป็น SQL-Injection ในประเทศสเปน ส่วนใหญ่ ผลการพิจารณาพบว่า การโจมตีที่เกิดขึ้นนี้ให้ผลลัพธ์ว่า เป็นการโจมตีเพื่อผลประโยชน์ส่วนตัวของผู้โจมตี

กฎข้อที่ 4 IF type = SQL-Injection AND country = Germany THEN requirement = Atk หมายความว่า ถ้ารูปแบบการโจมตีเป็น SQL-Injection ในประเทศเยอรมนี ผลการพิจารณาพบว่า การโจมตีที่เกิดขึ้นนี้ให้ผลลัพธ์ว่า เป็นการโจมตีเพื่อผลประโยชน์ส่วนตัวของผู้โจมตี

กฎข้อที่ 5 IF type = SQL-Injection AND country = Thailand THEN requirement = Atk หมายความว่า ถ้ารูปแบบการโจมตีเป็น SQL-Injection ในประเทศไทย ผลการพิจารณาพบว่า การโจมตีที่เกิดขึ้นนี้ให้ผลลัพธ์ว่า เป็นการโจมตีเพื่อผลประโยชน์ส่วนตัวของผู้โจมตี

กฎข้อที่ 6 IF type = Phishing THEN requirement = Atk หมายความว่า ถ้ารูปแบบการโจมตีเป็น Phishing ส่วนใหญ่ ผลการพิจารณาพบว่า การโจมตีที่เกิดขึ้นนี้ให้ผลลัพธ์ว่า เป็นการโจมตีเพื่อผลประโยชน์ส่วนตัวของผู้โจมตี

กฎข้อที่ 7 IF type = Malware THEN requirement = Atk หมายความว่า ถ้ารูปแบบการโจมตีเป็น Malware ส่วนใหญ่ที่พบเจอ ผลการพิจารณาพบว่า การโจมตีที่เกิดขึ้นนี้ให้ผลลัพธ์ว่า เป็นการโจมตีเพื่อผลประโยชน์ส่วนตัวของผู้โจมตี

กฎข้อที่ 8 IF type = DDOS AND web = Apache AND country = United States THEN requirement = Atk หมายความว่า ถ้ารูปแบบการโจมตีเป็น DDOS แล้วใช้ Webserver เป็น Apache ในประเทศสหรัฐอเมริกา ส่วนใหญ่ ผลการพิจารณาพบว่า การโจมตีที่เกิดขึ้นนี้ให้ผลลัพธ์ว่า เป็นการโจมตีเพื่อผลประโยชน์ส่วนตัวของผู้โจมตี

กฎข้อที่ 9 IF type = DDOS AND web = Apache AND country = Spain THEN requirement = Def หมายความว่า ถ้ารูปแบบการโจมตีเป็น DDOS แล้วใช้ Webserver เป็น Apache ในประเทศสเปน ส่วนใหญ่ ผลการพิจารณาพบว่า การโจมตีที่เกิดขึ้นนี้ให้ผลลัพธ์ว่า เป็นการโจมตีเพื่อทดสอบระบบและพัฒนาระบบ

กฎข้อที่ 10 IF type = DDOS AND web = Apache AND country = Germany THEN requirement = Atk หมายความว่า ถ้ารูปแบบการโจมตีเป็น DDOS แล้วใช้ Webserver เป็น Apache ในประเทศเยอรมนี ส่วนใหญ่ ผลการพิจารณาพบว่า การโจมตีที่เกิดขึ้นนี้ให้ผลลัพธ์ว่า เป็นการโจมตีเพื่อผลประโยชน์ส่วนตัวของผู้โจมตี

กฎข้อที่ 11 IF type = DDOS AND web = Apache AND country = Thailand THEN requirement = Def หมายความว่า ถ้ารูปแบบการโจมตีเป็น DDOS แล้วใช้ Webserver เป็น Apache ในประเทศไทย ส่วนใหญ่ ผลการพิจารณาพบว่า การโจมตีที่เกิดขึ้นนี้ให้ผลลัพธ์ว่า เป็นการโจมตีเพื่อทดสอบระบบและพัฒนาระบบ

กฎข้อที่ 12 IF type = DDOS AND web = Nginx THEN requirement = Def หมายความว่า ถ้ารูปแบบการโจมตีเป็น DDOS แล้วใช้ Webserver เป็น Nginx ผลการพิจารณาพบว่า การโจมตีที่เกิดขึ้นนี้ให้ผลลัพธ์ว่า เป็นการโจมตีเพื่อทดสอบระบบและพัฒนาระบบ

6) การนำไปใช้ (Deployment) ผู้จัดทำนำผลของข้อมูลที่ได้รับจากการวิเคราะห์แล้วมาแสดงผลข้อมูลผ่านทางเว็บไซต์ โดยนำเสนอข้อมูลแบบ Visualization เป็นการแสดงผลข้อมูลในรูปแบบของภาพโดยใช้ Google Charts หรือแผนภาพ (Dashboard)

4.2 ขอบเขตการประเมินโครงการ

4.2.1 ขอบเขตการประเมินโครงการ

1) การประเมินนี้เป็นการประเมินโครงการผลการดำเนินงานการสำรวจความพึงพอใจในการวิเคราะห์ข้อมูลภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021

2) การประเมินนี้เป็นการประเมินเพื่อช่วยในการปรับปรุงแก้ไขเกี่ยวกับโครงการความพึงพอใจในการใช้งานเว็บไซต์การวิเคราะห์ข้อมูลภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์

4.2.2 แนวคิดทฤษฎีเกี่ยวกับความพึงพอใจ

ความพึงพอใจ (Satisfaction) ได้มีผู้ให้ความหมายของความพึงพอใจไว้หลายความหมาย ดังนี้ พจนานุกรมฉบับราชบัณฑิตยสถาน (2542) ได้ให้ความหมายของความพึงพอใจไว้ว่า พึงพอใจ หมายถึง รัก ชอบใจ และพึงใจ หมายถึง พอใจ ชอบใจ

เทพพนม และสวีน (2540) กล่าวว่า ความพึงพอใจเป็นภาวะของความพึงใจหรือภาวะที่มีอารมณ์ในทางบวกที่เกิดขึ้น เนื่องจากการประเมินประสบการณ์ของคนๆหนึ่ง สิ่งที่เขาหายไประหว่างการเสนอให้กับสิ่งที่ได้รับจะเป็นรากฐานของการพอใจและไม่พอใจได้

จากการตรวจเอกสารข้างต้น สรุปได้ว่าความพึงพอใจ หมายถึงความรู้สึกที่ดีหรือทัศนคติที่ดีของบุคคล ซึ่งมักเกิดจากการได้รับการตอบสนองตามที่ตนต้องการก็จะเกิดความรู้สึกที่ดีต่อสิ่งนั้น ตรงกันข้ามหากความต้องการของตนไม่ได้รับการตอบสนองความไม่พึงพอใจก็จะเกิดขึ้น

2.2.3 ทฤษฎีที่เกี่ยวกับแรงจูงใจ

ทฤษฎีแรงจูงใจของมาสโลว์ (Maslow's theory motivation)

อับราฮัม มาสโลว์ (A.H.Maslow) ค้นหาวิธีที่จะอธิบายว่าทำไมคนจึงถูกผลักดันโดยความต้องการบางอย่าง ณ เวลาหนึ่งทำไมคนหนึ่งจึงทุ่มเทเวลาและพลังงานอย่างมากเพื่อให้ได้มาซึ่งความปลอดภัยของตนเองแต่อีกคนหนึ่งกลับทำ สิ่งเหล่านั้นเพื่อให้ได้รับการยกย่องนับถือจากผู้อื่น คำตอบของมาสโลว์คือความต้องการของมนุษย์จะถูกเรียงตามลำดับจากสิ่งที่กีดกัน มากที่สุดไปถึงน้อยที่สุด ทฤษฎีของมาสโลว์ได้จัดลำดับความต้องการตามความสำคัญ

ทฤษฎีแรงจูงใจของฟรอยด์ (S. M. Freud)

ซิกมันด์ ฟรอยด์ (S. M. Freud) ตั้งสมมุติฐานว่า บุคคลมักไม่รู้ตัวมากกว่า พลังทางจิตวิทยามีส่วนช่วยสร้างให้เกิดพฤติกรรม ฟรอยด์ พบว่าบุคคลเพิ่มและ ควบคุมสิ่งเร้าหลายอย่าง สิ่งเร้าเหล่านี้อยู่นอกเหนือการควบคุมอย่างสิ้นเชิง บุคคลจึงมีความฝัน พูดคำ ที่ไม่ตั้งใจพูด มีอารมณ์อยู่เหนือเหตุผล และมีพฤติกรรมหลอกหลอนหรือเกิดอาการวิตกกังวลอย่างมาก

2.2.4 การสร้างแบบสอบถามเพื่องานวิจัย

แบบสอบถาม (Questionnaire) หมายถึงรูปแบบของคำถามเป็นชุด ๆ ที่ได้ถูกรวบรวมไว้อย่างมีหลักเกณฑ์และเป็นระบบเพื่อใช้วัดสิ่งที่ผู้วิจัยต้องการจะวัดจากกลุ่มตัวอย่างหรือประชากรเป้าหมายให้ได้มาซึ่งข้อเท็จจริงทั้งในอดีตปัจจุบันและ การคาดคะเนเหตุการณ์ในอนาคตแบบสอบถามประกอบด้วยรายการคำถามที่สร้างอย่างประณีตเพื่อรวบรวมข้อมูลเกี่ยวกับความคิดเห็นหรือข้อเท็จจริงโดยส่งให้กลุ่มตัวอย่างตามความสมัครใจการใช้แบบสอบถามเป็นเครื่องมือในการเก็บรวบรวมข้อมูลนั้น การสร้างคำถามเป็นงานที่สำคัญสำหรับผู้วิจัยเพราะว่าผู้วิจัยอาจไม่มีโอกาสได้พบปะกับผู้ตอบแบบสอบถามเพื่ออธิบายความหมายต่าง ๆ ของข้อคำถามที่ต้องการเก็บรวบรวม

โครงสร้างของแบบสอบถามประกอบไปด้วย 3 ส่วนสำคัญดังนี้

- 1) หนังสือนำหรือคำชี้แจงโดยมากมักจะอยู่ส่วนแรกของแบบสอบถามอาจมีจดหมายอยู่ด้านหน้า พร้อมคำขอบคุณโดยคำชี้แจงมักจะระบุถึงจุดประสงค์ที่ให้ตอบแบบสอบถามการนำคำตอบ ที่ได้ไปใช้ประโยชน์คำอธิบายลักษณะของแบบสอบถามวิธีการตอบแบบสอบถามพร้อมตัวอย่างชื่อและที่อยู่ของผู้วิจัยประเด็นที่สำคัญคือการแสดงข้อความที่ทำให้ผู้ตอบมีความมั่นใจว่าข้อมูลที่จะตอบไปจะไม่ถูกเปิดเผย เป็นรายบุคคลจะไม่มีผลกระทบต่อผู้ตอบและมีการพิทักษ์สิทธิของผู้ตอบด้วย
- 2) คำถามเกี่ยวกับข้อมูลส่วนตัวเช่นเพศอายุระดับการศึกษาอาชีพเป็นต้นการที่จะถามข้อมูลส่วนตัวอะไรบ้างนั้นขึ้นอยู่กับกรอบแนวความคิด ในการวิจัยโดยดูว่าตัวแปรที่สนใจจะศึกษานั้นมีอะไรบ้างที่เกี่ยวกับข้อมูลส่วนตัวและควรถามเฉพาะข้อมูลที่จำเป็นในการวิจัยเท่านั้น
- 3) คำถามเกี่ยวกับคุณลักษณะหรือตัวแปรที่จะวัดเป็นความคิดเห็นของผู้ตอบ ในเรื่องของ คุณลักษณะหรือตัวแปรนั้น

ส่วนประกอบที่สำคัญของแบบสอบถามมีหลายชนิด แต่ไม่ว่าจะเป็นแบบสอบถามชนิดใดจะมีโครงสร้างหรือส่วนประกอบที่สำคัญ 3 ส่วนดังนี้

- 1) คำชี้แจงในการตอบแบบสอบถาม
- 2) สถานภาพทั่วไปในส่วนนี้เป็นรายละเอียดส่วนตัวของผู้ตอบ
- 3) ข้อคำถามเกี่ยวกับพฤติกรรมที่จะวัด จะถามเกี่ยวกับสิ่งที่ต้องการจะวัด

แบบสอบถามมีขั้นตอนการสร้างดังนี้

- 1) กำหนดจุดมุ่งหมายของแบบสอบถาม ผู้สร้างแบบสอบถามต้องระบุจุดมุ่งหมายของแบบสอบถามให้ชัดเจน ระบุให้ได้ว่า แบบสอบถามจะถูกนำไปใช้ในเรื่องอะไร
- 2) กำหนดประเด็นหลักหรือพฤติกรรมหลักที่จะวัดให้ครบถ้วนครอบคลุมว่าจะมีประเด็นอะไรบ้างหรืออาจเรียกว่าเป็นการกำหนดกรอบแนวคิดหรือโครงสร้างของแบบสอบถาม
- 3) กำหนดชนิดหรือรูปแบบของแบบสอบถามโดยเลือกให้เหมาะสมกับเรื่องที่จะวัด และลักษณะของกลุ่มผู้เรียน
- 4) กำหนดจำนวนข้อคำถามโดยอาจจะกำหนดในเบื้องต้นว่าต้องการจะให้แบบสอบถามมีความยาวมากน้อยเพียงใดและคลุมประเด็นหลักประเด็นย่อยอย่างไรบ้าง

5) สร้างข้อคำถามตามจุดมุ่งหมายชนิดหรือรูป แบบจำนวนข้อในประเด็นต่าง ๆ ที่กำหนดไว้ตามโครงสร้างของแบบสอบถาม

6) ตรวจสอบเพื่อการแก้ไขปรับปรุงแบ่งออกเป็น 2 ตอนคือตอนแรกตรวจสอบโดยผู้สร้างแบบสอบถามเองตอนที่สองตรวจสอบพิจารณาให้คำแนะนำและวิจารณ์โดยผู้รู้ หรือผู้เชี่ยวชาญหรือผู้ชำนาญการ

7) นำแบบสอบถามไปทดลองการนำไปทดลองใช้ (Try out) ควรนำไปทดลองกับกลุ่มที่มีลักษณะเหมือนหรือใกล้เคียงกับกลุ่มที่จะไปเก็บรวบรวมข้อมูลจริง

8) วิเคราะห์แบบสอบถามโดยการนำ ผลจากการไปทดลองมาวิเคราะห์เพื่อหาคุณภาพและปรับปรุงแบบสอบถามในส่วนที่ยังมีข้อบกพร่องต่าง ๆ

9) จัดพิมพ์แบบสอบถาม เพื่อเตรียมนำ ไปใช้จริงต่อไป

การสร้างการแจกแจงความถี่ มีขั้นตอนในการสร้างดังนี้

1) พิจารณาจำนวนอันตรภาคชั้นตามที่ต้องการ ซึ่งโดยทั่วไปจะนิยมสร้างตั้งแต่ 7 ถึง 15 อันตรภาคชั้น หรือไม่ควรต่ำกว่า 5 อันตรภาคชั้น และไม่นิยมให้บางอันตรภาคชั้นมีความถี่เป็น 0

$$\text{ความกว้างของอันตรภาคชั้น} = \frac{\text{คะแนนสูงสุด} - \text{คะแนนต่ำสุด}}{\text{จำนวนชั้น}}$$

2) หาช่วงคะแนนของแต่ละอันตรภาคชั้น โดยให้ข้อมูลค่าต่ำ สุดเป็นค่าต่ำสุดของอันตรภาคชั้นชั้นแรกแล้วหาความถี่

3) หาจำนวนคะแนนแล้วบันทึกเป็นรอยขีด (ควรทำในกระดาษบันทึกคะแนน) แล้วนับรอยขีดในแต่ละอันตรภาคชั้น เป็นความถี่ในอันตรภาคชั้นนั้น ๆ

ส่วนเบี่ยงเบนมาตรฐาน

ในสถิติที่เบี่ยงเบนมาตรฐานเป็นตัวชี้วัดของจำนวนเงินของการเปลี่ยนแปลงหรือการกระจายตัวของชุดของค่า ค่าเบี่ยงเบนมาตรฐานที่ต่ำบ่งชี้ว่าค่ามักจะใกล้เคียงกับค่าเฉลี่ย (เรียกอีกอย่างว่าค่าที่คาดหวัง) ของเซตในขณะที่ค่าเบี่ยงเบนมาตรฐานสูงบ่งชี้ว่าค่าต่าง ๆ จะกระจายออกไปในช่วงที่กว้างขึ้น

ค่าเบี่ยงเบนมาตรฐานอาจเรียกสั้น ๆ ว่า S.D. และมักแสดงในข้อความและสมการทางคณิตศาสตร์โดยตัวอักษรกรีกตัวพิมพ์เล็ก sigma σ สำหรับค่าเบี่ยงเบนมาตรฐานของประชากรหรือตัวอักษรละติน s สำหรับค่าเบี่ยงเบนมาตรฐานตัวอย่าง

$$S. D. = \sqrt{\frac{\sum(x - \bar{x})^2}{n - 1}}$$

ภาพที่ 4.50 การหาส่วนเบี่ยงเบนมาตรฐาน (S.D.)

ค่าเบี่ยงเบนมาตรฐานของตัวแปรสุ่ม , ตัวอย่าง , ประชากรสถิติ , ชุดข้อมูลหรือกระจายความน่าจะเป็นรากที่สองของความแปรปรวน มันเป็นพีชคณิตง่าย แต่ในทางปฏิบัติบ่อยที่แข็งแกร่งกว่าค่าเบี่ยงเบนสัมบูรณ์เฉลี่ย คุณสมบัติที่มีประโยชน์ของค่าเบี่ยงเบนมาตรฐานคือไม่เหมือนกับความแปรปรวนโดยจะแสดงในหน่วยเดียวกับข้อมูล

4.2.5 การอธิบายผลความพึงพอใจจากการตอบแบบสอบถามจากผลการสำรวจความพึงพอใจในการวิเคราะห์ข้อมูลภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021 แล้วจากนั้นทางผู้วิเคราะห์ข้อมูลได้ทำการประเมินผลจากผู้ใช้งานทั่วไป จากกลุ่มตัวอย่างจำนวน 30 ชุด ซึ่งมีรายละเอียดดังนี้

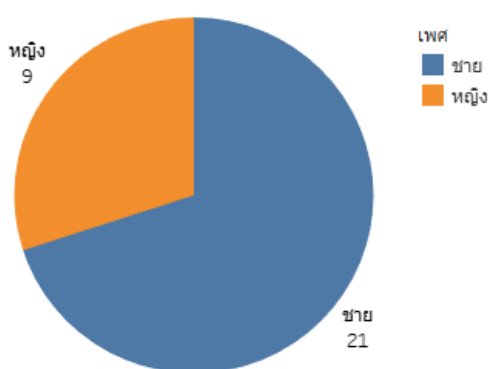
1) ผลการวิเคราะห์ข้อมูลเกี่ยวกับสถานะภาพส่วนบุคคลของผู้ตอบแบบสอบถาม ผล การวิเคราะห์ข้อมูลเกี่ยวกับสถานะภาพส่วนบุคคลของผู้ตอบแบบสอบถาม ลักษณะแบบสอบถาม เป็นแบบตรวจสอบรายการ (Check List) ดังนี้

- สถานะภาพส่วนบุคคลของผู้ตอบแบบสอบถามในด้านเพศผลการวิเคราะห์ข้อมูลเกี่ยวกับสถานะภาพส่วนบุคคลของผู้ตอบแบบสอบถาม ลักษณะในด้านเพศปรากฏผลตามตารางที่ 4.1 โดยมีรายละเอียด ดังนี้

ตารางที่ 4.1 แสดงจำนวนและคารอยละของสถานะภาพส่วนบุคคลของผู้ตอบแบบสอบถามในด้านเพศ

| เพศ | จำนวน | ร้อยละ |
|------|-------|--------|
| ชาย | 21 | 70 |
| หญิง | 9 | 30 |
| รวม | 30 | 100 |

จากภาพตารางที่ 4.1 พบว่าเพศของผู้ตอบแบบสอบถาม เพศชายคิดเป็นร้อยละ 70 และเพศหญิงคิดเป็นร้อยละ 30



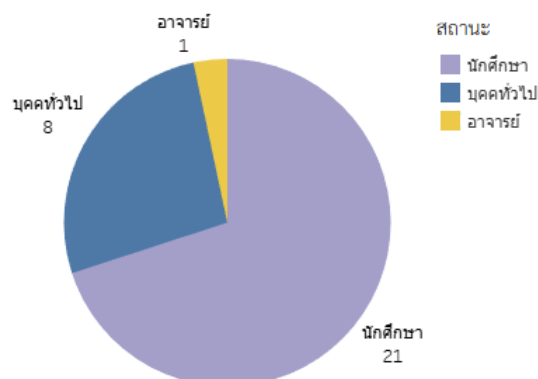
ภาพที่ 4.51 แสดงจำนวนและคารอยละของสถานะภาพส่วนบุคคลของผู้ตอบแบบสอบถามในด้านเพศ

- สถานะภาพส่วนบุคคลของผู้ตอบแบบสอบถามในด้านสถานะผลของการ วิเคราะห์ข้อมูลเกี่ยวกับสถานะภาพตำแหน่งการศึกษาปรากฏดังตารางที่ 4.2

ตารางที่ 4.2 แสดงจำนวนและคารอยละของสถานะภาพส่วนบุคคลของผู้ตอบแบบสอบถามด้านตำแหน่ง

| สถานะ | จำนวน | ร้อยละ |
|-------------|-------|--------|
| อาจารย์ | 1 | 3.3 |
| นักศึกษา | 21 | 70 |
| บุคคลทั่วไป | 8 | 26.6 |
| รวม | 30 | 100 |

จากภาพตารางที่ 4.2 พบว่าสถานะของผู้ตอบแบบสอบถาม อาจารย์คิดเป็นร้อยละ 3.3 นักศึกษาคิดเป็นร้อยละ 70 และบุคคลทั่วไปคิดเป็นร้อยละ 26.6



ภาพที่ 4.52 แสดงจำนวนและการยลของสถานะภาพส่วนบุคคลของผู้ตอบแบบสอบถามตามตำแหน่ง

2) ผลการวิเคราะห์ข้อมูลเกี่ยวกับการสำรวจความพึงพอใจในการวิเคราะห์ข้อมูลภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ ของผู้ตอบแบบสอบถามทั้งโดยภาพรวม ซึ่งมีลักษณะแบบสอบถามเป็นแบบตรวจสอบรายการ (Check List) จากวัตถุประสงค์ได้ทำการศึกษาความพึงพอใจของผู้ตอบแบบสอบถามจำแนกตามสถานะภาพส่วนบุคคลทั้งด้านเพศ สถานะ แล้วได้ผลสรุปออกมา ดังนี้

- ความพึงพอใจในด้านการวิเคราะห์ข้อมูล

- 1) ชื่อหน่วยงาน/แหล่งข้อมูลที่นำเชื่อถือ
- 2) ข้อมูลที่นำเสนอครบถ้วนตรงกับความต้องการ
- 3) ข้อมูลมีปริมาณเหมาะสมในการนำไปใช้วิเคราะห์ข้อมูล
- 4) ผลการวิเคราะห์ข้อมูลมีความถูกต้องแม่นยำ
- 5) เครื่องมือในการวิเคราะห์มีความเหมาะสม
- 6) ข้อมูลจากการวิเคราะห์สามารถนำไปเป็นความรู้ด้านภัยคุกคามการโจมตีบนเว็บไซต์
- 7) ความถูกต้องของกระบวนการ
- 8) ประสิทธิภาพของกฎการวิเคราะห์
- 9) การอธิบายกฎต้นไม้มาก่อนตัดสินใจมีความเข้าใจง่าย
- 10) การนำเสนอในรูปแบบ Visualization ด้วยโปรแกรม Tableau มีความเหมาะสม

กับข้อมูล

- ฟังพอใจในการเข้าเยี่ยมชมเว็บไซต์

- 1) มีความชัดเจน ถูกต้อง น่าเชื่อถือ
- 2) การจัดลำดับเนื้อหาเป็นขั้นตอน มีความต่อเนื่อง อ่านแล้วเข้าใจ
- 3) มีการจัดหมวดหมู่ให้ง่ายต่อการค้นหา
- 4) ข้อความในเว็บไซต์ถูกต้องตามหลักภาษาและไวยากรณ์
- 5) ความเหมาะสมของข้อมูลภายในเว็บไซต์
- 6) การจัดรูปแบบในเว็บไซต์ง่ายต่อการอ่านและการใช้งาน
- 7) หน้าโฮมเพจมีความสวยงาม มีความทันสมัย และน่าสนใจ
- 8) สีพื้นหลังและสีตัวอักษรมีความเหมาะสมต่อการอ่าน
- 9) ความถูกต้องในการเชื่อมโยงภายในเว็บไซต์
- 10) ความถูกต้องในการเชื่อมโยงไปยังเว็บไซต์อื่น
- 11) เนื้อหา มีประโยชน์ต่อผู้ใช้งาน
- 12) สามารถเป็นแหล่งความรู้ได้
- 13) สามารถนำไปใช้เป็นแหล่งอ้างอิงกับงานวิจัยชิ้นอื่นได้
- 14) สามารถนำไปประยุกต์ใช้ได้

3) ความพึงพอใจในการวิเคราะห์ข้อมูล

จากที่คณะผู้จัดทำได้ทำการวิเคราะห์ข้อมูล จึงได้ทำการประเมินผลการวิเคราะห์ข้อมูลจากกลุ่มตัวอย่างจำนวน 30 คน โดยการทำแบบสอบถามความพึงพอใจในการวิเคราะห์ข้อมูลแบ่งเป็นเพศหญิงจำนวน 9 คน คิดเป็นร้อยละ 30% เพศชายจำนวน 21 คน คิดเป็นร้อยละ 70% นักศึกษา จำนวน 21 คน คิดเป็นร้อยละ 70% อาจารย์ จำนวน 1 คน คิดเป็นร้อยละ 3.3% บุคคลทั่วไป จำนวน 8 คน คิดเป็นร้อยละ 26.6% โดยเกณฑ์การให้คะแนนของการวิเคราะห์ข้อมูลมีดังนี้ ระดับความพึงพอใจของการวิเคราะห์ข้อมูล ระดับความพึงพอใจ 5 = มากที่สุด 4 = มาก 3 = ปานกลาง 2 = น้อย 1 = น้อยที่สุด

เมื่อนำคำตอบของผู้ตอบแบบสอบถามมาแจกแจงความถี่และหาค่าเฉลี่ย แล้วกำหนดระดับค่าเฉลี่ย แบ่งระดับความพึงพอใจได้ดังนี้

$$\text{ความกว้างของอันตรภาคชั้น} = \frac{\text{คะแนนสูงสุด} - \text{คะแนนต่ำสุด}}{\text{จำนวนชั้น}} = \frac{5-1}{5} = 0.8$$

จากเกณฑ์ดังกล่าว สามารถแปลความหมายของความพึงพอใจได้ ดังนี้

คะแนนเฉลี่ย 1.00 - 1.80 หมายถึง ระดับความพึงพอใจน้อยที่สุด

คะแนนเฉลี่ย 1.81 - 2.60 หมายถึง ระดับความพึงพอใจน้อย

คะแนนเฉลี่ย 2.61 - 3.40 หมายถึง ระดับความพึงพอใจปานกลาง

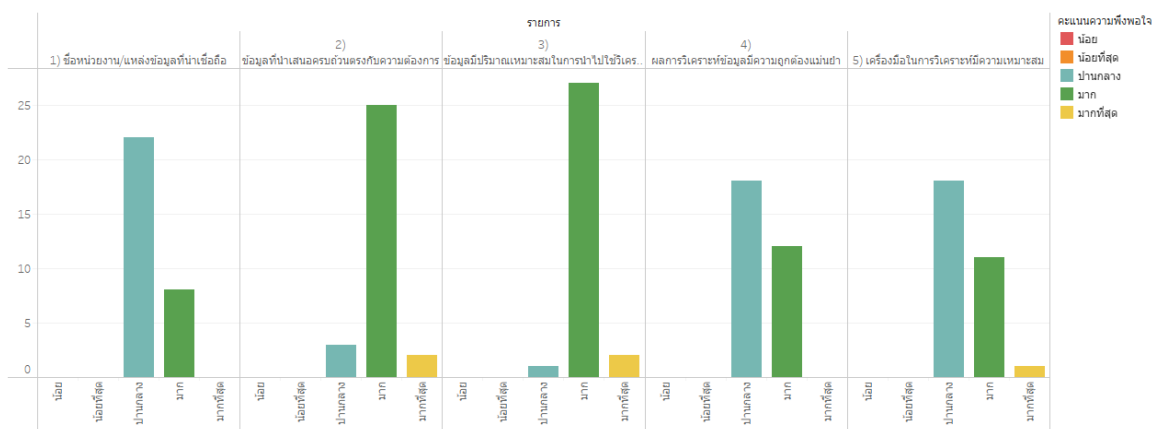
คะแนนเฉลี่ย 3.41 - 4.20 หมายถึง ระดับความพึงพอใจมาก

คะแนนเฉลี่ย 4.21 - 5.00 หมายถึง ระดับความพึงพอใจมากที่สุด

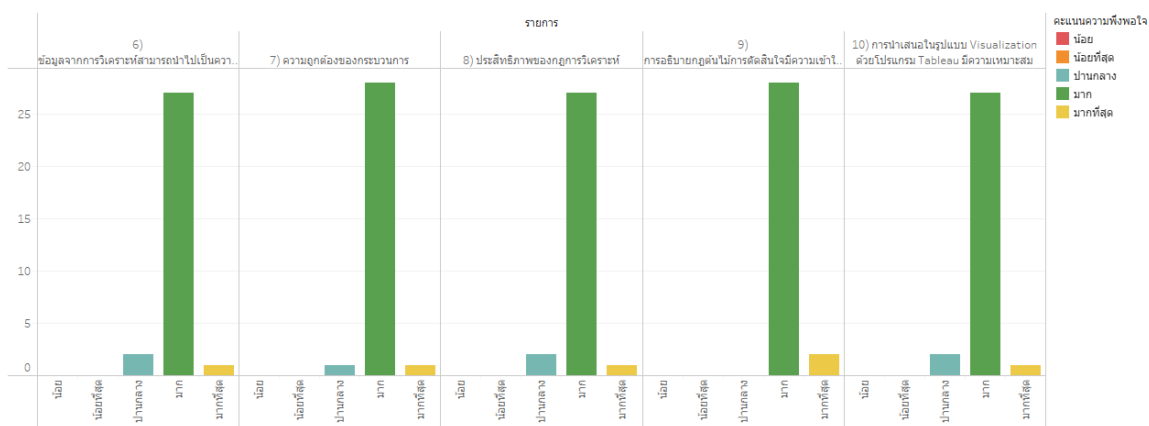
ตารางที่ 4.3 แสดงผลแบบสอบถามความพึงพอใจในการวิเคราะห์ข้อมูล

| รายการประเมิน | จำนวนผู้ตอบแบบสอบถาม | \bar{x} | S.D. | ผลการประเมิน |
|--|----------------------|-------------|-------------|--------------|
| 1) ชื่อหน่วยงาน/แหล่งข้อมูลที่น่าเชื่อถือ | 30 | 3.79 | 0.86 | ดี |
| 2) ข้อมูลที่น่าเสนอครบถ้วนตรงกับความต้องการ | 30 | 4.00 | 0.75 | ดี |
| 3) ข้อมูลมีปริมาณเหมาะสมในการนำไปใช้วิเคราะห์ข้อมูล | 30 | 4.03 | 0.71 | ดี |
| 4) ผลการวิเคราะห์ข้อมูลมีความถูกต้องแม่นยำ | 30 | 3.87 | 0.85 | ดี |
| 5) เครื่องมือในการวิเคราะห์มีความเหมาะสม | 30 | 3.69 | 0.83 | ดี |
| 6) ข้อมูลจากการวิเคราะห์สามารถนำไปเป็นความรู้ด้านภัยคุกคามการโจมตีบนเว็บไซต์ | 30 | 4.00 | 0.77 | ดี |
| 7) ความถูกต้องของกระบวนการ | 30 | 4.02 | 0.74 | ดี |
| 8) ประสิทธิภาพของกฎการวิเคราะห์ | 30 | 3.98 | 0.87 | ดี |
| 9) การอธิบายกฎค้นไม่การตัดสินใจมีความเข้าใจง่าย | 30 | 4.03 | 0.71 | ดี |
| 10) การนำเสนอในรูปแบบ Visualization ด้วยโปรแกรม Tableau มีความเหมาะสม | 30 | 3.98 | 0.87 | ดี |
| รวม | | 3.93 | 0.79 | ดี |

จากตารางที่ 4.3 พบว่าระดับความพึงพอใจของผู้ตอบแบบสอบถามต่อการวิเคราะห์ข้อมูล โดยภาพรวมอยู่ในระดับที่ดีค่าเฉลี่ยเท่ากับ 3.93 โดยการพิจารณารายข้อมีค่าคะแนนเฉลี่ยอยู่ระหว่าง 3.69 – 4.03



ภาพที่ 4.53 แสดงความพึงพอใจของผู้ตอบแบบสอบถามต่อการวิเคราะห์ข้อมูล



ภาพที่ 4.54 แสดงความพึงพอใจของผู้ตอบแบบสอบถามต่อการวิเคราะห์ข้อมูล

ระดับความพึงพอใจของผู้มาตอบแบบสอบถามต่อการวิเคราะห์ข้อมูลในระดับที่พอใจมาก ได้แก่ ชื่อหน่วยงาน/แหล่งข้อมูลที่น่าเชื่อถือ 3.79 (S.D. = 0.86), ข้อมูลที่นำเสนอครบถ้วนตรงกับความต้องการ 4.00 (S.D. = 0.75), ข้อมูลมีปริมาณเหมาะสมในการนำไปใช้วิเคราะห์ข้อมูล 4.03 (S.D. = 0.71), ผลการวิเคราะห์ข้อมูลมีความถูกต้องแม่นยำ 3.87 (S.D. = 0.85), เครื่องมือในการวิเคราะห์มีความเหมาะสม 3.69 (S.D. = 0.83), ข้อมูลจากการวิเคราะห์สามารถนำไปเป็นความรู้ด้านภัยคุกคามการโจมตีบนเว็บไซต์

4.00 (S.D. = 0.77), ความถูกต้องของกระบวนการ 4.02 (S.D. = 0.74), ประสิทธิภาพของกฎการวิเคราะห์ 3.98 (S.D. = 0.87), การอธิบายกฎต้นไม้มักการตัดสินใจมีความเข้าใจง่าย 4.03 (S.D. = 0.71), การนำเสนอในรูปแบบ Visualization ด้วยโปรแกรม Tableau มีความเหมาะสม 3.98 (S.D. = 0.87) จากจำนวนผู้ตอบแบบสอบถามทั้งหมด 30 คน ค่าเฉลี่ยเท่ากับ 3.93 (S.D. = 0.79) อยู่ในเกณฑ์ระดับดี

4) พึงพอใจในการเข้าเยี่ยมชมเว็บไซต์

จากที่คณะผู้จัดทำได้ทำการวิเคราะห์ข้อมูล จึงได้ทำการประเมินผลการวิเคราะห์ข้อมูลจากกลุ่มตัวอย่างจำนวน 30 คน โดยการทำแบบสอบถามความพึงพอใจในการเข้าเยี่ยมชมเว็บไซต์แบ่งเป็นเพศหญิงจำนวน 9 คน คิดเป็นร้อยละ 30% เพศชายจำนวน 21 คน คิดเป็นร้อยละ 70% นักศึกษา จำนวน 21 คน คิดเป็นร้อยละ 70% อาจารย์ จำนวน 1 คน คิดเป็นร้อยละ 3.3% บุคคลทั่วไป จำนวน 8 คน คิดเป็นร้อยละ 26.6% โดยเกณฑ์การให้คะแนนของการวิเคราะห์ข้อมูลมีดังนี้ ระดับความพึงพอใจของการวิเคราะห์ข้อมูล ระดับความพึงพอใจ 5 = มากที่สุด 4 = มาก 3 = ปานกลาง 2 = น้อย 1 = น้อยที่สุด

เมื่อนำคำตอบของผู้ตอบแบบสอบถามมาแจกแจงความถี่และหาค่าเฉลี่ย แล้วกำหนดระดับค่าเฉลี่ย แบ่งระดับความพึงพอใจได้ดังนี้

$$\text{ความกว้างของอันตรภาคชั้น} = \frac{\text{คะแนนสูงสุด} - \text{คะแนนต่ำสุด}}{\text{จำนวนชั้น}} = \frac{5-1}{5} = 0.8$$

จากเกณฑ์ดังกล่าว สามารถแปลความหมายของความพึงพอใจได้ ดังนี้

คะแนนเฉลี่ย 1.00 - 1.80 หมายถึง ระดับความพึงพอใจน้อยที่สุด

คะแนนเฉลี่ย 1.81 - 2.60 หมายถึง ระดับความพึงพอใจน้อย

คะแนนเฉลี่ย 2.61 - 3.40 หมายถึง ระดับความพึงพอใจปานกลาง

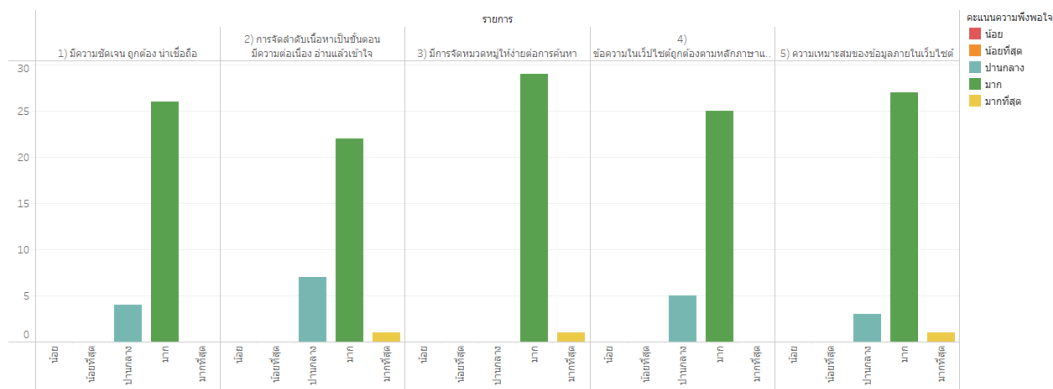
คะแนนเฉลี่ย 3.41 - 4.20 หมายถึง ระดับความพึงพอใจมาก

คะแนนเฉลี่ย 4.21 - 5.00 หมายถึง ระดับความพึงพอใจมากที่สุด

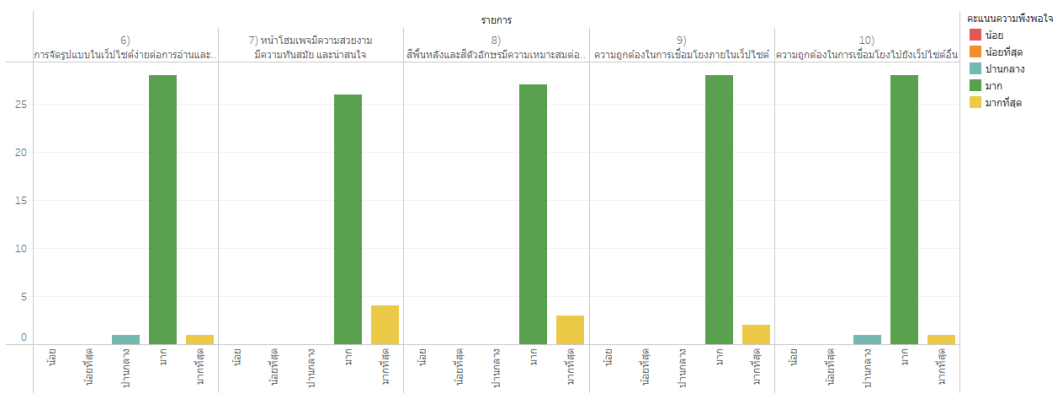
ตารางที่ 4.4 แสดงผลแบบสอบถามความพึงพอใจในการเข้าเยี่ยมชมเว็บไซต์

| รายการประเมิน | จำนวนผู้ตอบ แบบสอบถาม | \bar{x} | S.D. | ผลการ ประเมิน |
|---|--------------------------|-------------|-------------|------------------|
| 1) มีความชัดเจน ถูกต้อง น่าเชื่อถือ | 30 | 3.87 | 0.85 | ดี |
| 2) การจัดลำดับเนื้อหาเป็นขั้นตอน มีความต่อเนื่อง อ่านแล้วเข้าใจ | 30 | 3.69 | 0.83 | ดี |
| 3) มีการจัดหมวดหมู่ให้ง่ายต่อการค้นหา | 30 | 4.02 | 0.85 | ดี |
| 4) ข้อความในเว็บไซต์ถูกต้องตามหลักภาษาและไวยากรณ์ | 30 | 3.79 | 0.86 | ดี |
| 5) ความเหมาะสมของข้อมูลภายในเว็บไซต์ | 30 | 3.87 | 0.85 | ดี |
| 6) การจัดรูปแบบในเว็บไซต์ง่ายต่อการอ่านและการใช้งาน | 30 | 4.03 | 0.77 | ดี |
| 7) หน้าโฮมเพจมีความสวยงาม มีความทันสมัย และน่าสนใจ | 30 | 4.25 | 0.62 | ดีมาก |
| 8) สีพื้นหลังและสีตัวอักษรมีความเหมาะสมต่อการอ่าน | 30 | 4.21 | 0.69 | ดีมาก |
| 9) ความถูกต้องในการเชื่อมโยงภายในเว็บไซต์ | 30 | 4.15 | 0.68 | ดี |
| 10) ความถูกต้องในการเชื่อมโยงไปยังเว็บไซต์อื่น | 30 | 4.25 | 0.62 | ดีมาก |
| 11) เนื้อหามีประโยชน์ต่อผู้ใช้งาน | 30 | 4.18 | 0.72 | ดี |
| 12) สามารถเป็นแหล่งความรู้ได้ | 30 | 3.89 | 0.95 | ดี |
| 13) สามารถนำไปใช้เป็นแหล่งอ้างอิงกับงานวิจัยชิ้นอื่นได้ | 30 | 4.00 | 0.77 | ดี |
| 14) สามารถนำไปประยุกต์ใช้ได้ | 30 | 3.98 | 0.76 | ดี |
| รวม | | 4.01 | 0.77 | ดี |

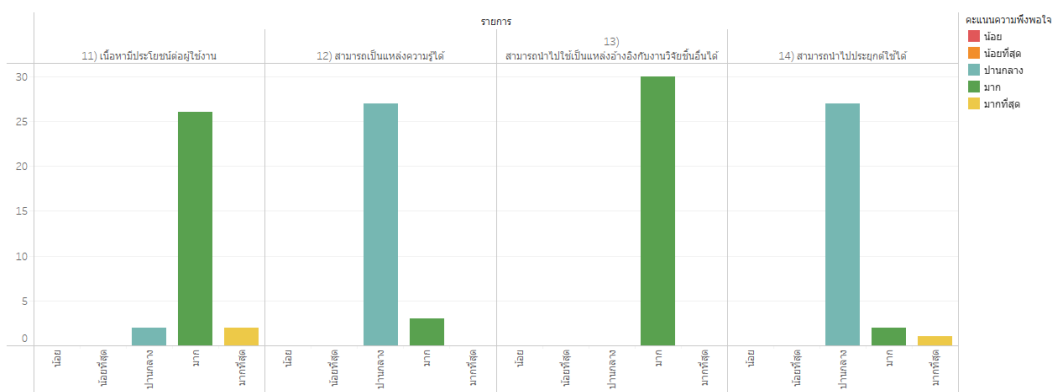
จากตารางที่ 4.4 พบว่าระดับความพึงพอใจของผู้ตอบแบบสอบถามต่อด้านเนื้อหา โดยภาพรวมอยู่ในระดับที่ดีค่าเฉลี่ยเท่ากับ 4.01 โดยการพิจารณารายข้อมีค่าคะแนนเฉลี่ยอยู่ระหว่าง 3.69 – 4.25



ภาพที่ 4.55 แสดงความพึงพอใจของผู้ตอบแบบสอบถามด้านเนื้อหา



ภาพที่ 4.56 แสดงความพึงพอใจของผู้ตอบแบบสอบถามด้านการออกแบบและการจัดรูปแบบเว็บไซต์



ภาพที่ 4.57 แสดงความพึงพอใจของผู้ตอบแบบสอบถามด้านประโยชน์และการนำไปใช้

ระดับความพึงพอใจของผู้มาตอบแบบสอบถามต่อการวิเคราะห์ข้อมูลในระดับที่พอใจมาก ได้แก่ มีความชัดเจน ถูกต้อง น่าเชื่อถือ 3.87 (S.D. = 0.85), การจัดลำดับเนื้อหาเป็นขั้นตอน มีความต่อเนื่อง อ่านแล้วเข้าใจ 3.69 (S.D. = 0.83), มีการจัดหมวดหมู่ให้ง่ายต่อการค้นหา 4.02 (S.D. = 0.85), ข้อความในเว็บไซต์ถูกต้องตามหลักภาษาและไวยากรณ์ 3.79 (S.D. = 0.86), ความเหมาะสมของข้อมูลภายในเว็บไซต์ 3.87 (S.D. = 0.85), การจัดรูปแบบในเว็บไซต์ง่ายต่อการอ่านและการใช้งาน 4.03 (S.D. = 0.77), หน้าโฮมเพจมีความสวยงาม มีความทันสมัย และน่าสนใจ 4.25 (S.D. = 0.62), สีพื้นหลังและสีตัวอักษรมีความเหมาะสมต่อการอ่าน 4.21 (S.D. = 0.69), ถูกต้องในการเชื่อมโยงภายในเว็บไซต์ 4.15 (S.D. = 0.68), ความถูกต้องในการเชื่อมโยงไปยังเว็บไซต์อื่น 4.25 (S.D. = 0.62), เนื้อหามีประโยชน์ต่อผู้ใช้งาน 4.18 (S.D. = 0.72), สามารถเป็นแหล่งความรู้ได้ 3.89 (S.D. = 0.95), สามารถนำไปใช้เป็นแหล่งอ้างอิงกับงานวิจัยชิ้นอื่นได้ 4.00 (S.D. = 0.77), สามารถนำไปประยุกต์ใช้ได้ 3.98 (S.D. = 0.76) จากจำนวนผู้ตอบแบบสอบถามทั้งหมด 30 คน ค่าเฉลี่ยเท่ากับ 4.01 (S.D. = 0.77) อยู่ในเกณฑ์ระดับดี

4.3 การอภิปรายผล

จากวิธีการดำเนินงานโครงการในการคำนวณ โมเดลต้นไม้ตัดสินใจ จากการคำนวณด้วยมือนี้ ผู้วิเคราะห์ข้อมูลได้ผลลัพธ์ว่า โมเดลต้นไม้ตัดสินใจ Root node ที่คือ แอตทริบิวต์ Type และได้ interior node คือ แอตทริบิวต์ Country , แอตทริบิวต์ Web server และ leaf node คือ แอตทริบิวต์ Os ซึ่งไม่สามารถสร้างกิ่งแต่ละโหนดต่อไปได้ เนื่องจากไม่มีความสัมพันธ์กับแอตทริบิวต์ใด ก็จะได้ผลลัพธ์ที่ แอตทริบิวต์ Os linux , nginx และ แอตทริบิวต์ Country United States , Spain , Germany และ Thailand ทางผู้วิเคราะห์ข้อมูลได้ทำการแสดงวิธีในการจัดการกับข้อมูลของการโจมตีที่เกิดขึ้นบนเว็บไซต์ ในปี 2019 ถึง ปี 2021 ด้วยขั้นตอนการวิเคราะห์ข้อมูลด้วย CRISP-DM อย่างละเอียดรวมไปถึงการสร้าง โมเดล Decision Tree จากโปรแกรมที่ใช้เลือกทำเหมืองข้อมูลเพื่อนำเสนอ คือ โปรแกรม Weka ในการสร้างโมเดล Decision Tree และตรวจสอบข้อมูลผ่านทางโปรแกรม RapidMiner Studio เพื่อความแม่นยำ เมื่อนำไปเปรียบเทียบกับผลการคำนวณ โมเดล Decision Tree ด้วยตัวเอง ทางผู้วิเคราะห์ข้อมูลพบว่าทั้ง 3 โมเดลได้ผลลัพธ์ความแม่นยำของโมเดลที่ เหมือนกัน และสามารถนำโมเดลไปใช้งานได้ และ ประเมินประสิทธิภาพของโมเดล ซึ่งมีค่าความถูกต้องเฉลี่ยในทุกโมเดลเท่ากับ 75.55% จำนวนทั้งสิ้น 42,414 รายการ เมื่อเปรียบเทียบกับงานวิจัยการพัฒนาแบบจำลองของ วนิดา พงษ์สงวน , ทิพย์ ถินสูงเนิน , มาโนช ถินสูงเนิน (2559) การพัฒนาแบบจำลองปัจจัยที่มีผลต่อการเป็นโรคเบาหวานด้วยเทคนิค

ต้นไม้ตัดสินใจ จำนวนทั้งสิ้น 44,002 รายการ พบว่าโมเดลแบบจำลองมีค่าความถูกต้องเฉลี่ยที่ใกล้เคียงกันที่ 76.14% ซึ่งเป็นค่าที่สามารถยอมรับได้ในการ ทดสอบประสิทธิภาพของ Model ด้วยวิธี Self-Consistency Test และทุกโมเดลพบว่ามีผลลัพธ์ตรงกันอยู่ในระดับค่อนข้างดี ทางผู้วิเคราะห์ข้อมูลได้นำข้อมูลสารสนเทศนั้นมาทำการแสดงผลแบบ Visualization โดยใช้โปรแกรม Tableau Public และ Google Charts API มาแสดงให้เห็นกับระบบที่สามารถใช้งานได้จริง บุคคลทั่วไป สมาชิกเว็บไซต์ ผู้ดูแลเว็บไซต์ สามารถใช้งานได้จริงตามวัตถุประสงค์ ซึ่งเว็บไซต์นี้ช่วยในการให้ความรู้ผลการวิเคราะห์แนวโน้มการเกิดภัยคุกคามบนเว็บไซต์ โดยเว็บไซต์ดังกล่าวมีการใช้งานอยู่ทั้งสิ้น 3 ระดับ คือ

4.3.1 บุคคลทั่วไป สามารถดูข้อมูลความรู้และบทความเกี่ยวกับ ภัยคุกคามการโจมตีบน เว็บไซต์ สามารถดูทฤษฎีและกระบวนการที่วิเคราะห์ข้อมูล CRISP-DM ของเว็บไซต์ สามารถดูแดชบอร์ดข้อมูลสารสนเทศของภัยคุกคามการโจมตีทางเว็บไซต์ ของประเทศไทย สามารถดูแดชบอร์ดข้อมูลสารสนเทศของภัยคุกคามการโจมตีทางเว็บไซต์ รวมของทุกประเทศ 5 สามารถนำเสนอ กฎที่ได้จากโมเดล Decision tree ให้มีความน่าสนใจ สามารถนำเว็บไซต์ ไปนำเสนอ อบรมให้ความรู้หรือใช้ในการศึกษาทางด้าน ภัยคุกคามทางด้านเว็บไซต์ได้ เว็บไซต์การวิเคราะห์ข้อมูลภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ ในปี 2019-2021 รองรับภาษาทั้งหมด 109 ภาษา เว็บไซต์มีการใช้ google recaptcha เพื่อป้องกันเว็บไซต์จากสแปม มีการป้องกันการเข้าสู่ระบบที่ไม่สำเร็จจะทำการบล็อก การเข้าสู่ระบบชั่วคราว สามารถสมัครสมาชิกได้

4.3.2 สมาชิกเว็บไซต์ สามารถดูข้อมูลความรู้และบทความเกี่ยวกับ ภัยคุกคามการโจมตีบน เว็บไซต์ สามารถดูทฤษฎีและกระบวนการที่วิเคราะห์ข้อมูล CRISP-DM ของเว็บไซต์ สามารถดูแดชบอร์ดข้อมูลสารสนเทศของภัยคุกคามการโจมตีทางเว็บไซต์ ของประเทศไทย สามารถดูแดชบอร์ดข้อมูลสารสนเทศของภัยคุกคามการโจมตีทางเว็บไซต์ รวมของทุกประเทศ 5 สามารถนำเสนอ กฎที่ได้จากโมเดล Decision tree ให้มีความน่าสนใจ สามารถนำเว็บไซต์ ไปนำเสนอ อบรมให้ความรู้หรือใช้ในการศึกษาทางด้าน ภัยคุกคามทางด้านเว็บไซต์ได้ เว็บไซต์การวิเคราะห์ข้อมูลภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ ในปี 2019-2021 รองรับภาษาทั้งหมด 109 ภาษา เว็บไซต์มีการใช้ google recaptcha เพื่อป้องกันเว็บไซต์จากสแปม มีการป้องกันการเข้าสู่ระบบที่ไม่สำเร็จจะทำการบล็อก การเข้าสู่ระบบชั่วคราว สามารถสมัครสมาชิกได้ สามารถเข้าสู่ระบบได้ โดย ไอดี และ รหัสผ่าน สามารถแก้ไขข้อมูลส่วนตัวได้ สามารถดูข้อมูลความรู้และบทความเกี่ยวกับ ภัยคุกคามการโจมตีบนเว็บไซต์ สามารถดูทฤษฎีและกระบวนการที่วิเคราะห์ข้อมูล CRISP-DM ของเว็บไซต์ สามารถดูแดชบอร์ดข้อมูลสารสนเทศ

ของภัยคุกคามการโจมตีทางเว็บไซต์ของประเทศไทย สามารถดูแดชบอร์ดข้อมูลสารสนเทศของภัยคุกคามการโจมตีทางเว็บไซต์รวมของทุกประเทศ สามารถดาวน์โหลดรีพอร์ตข้อมูลแดชบอร์ดภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ ในรูปแบบของ PDF ได้ สามารถกรอกข้อมูลลงบนเว็บไซต์เพื่อเพิ่มข้อมูลได้ (ชุดข้อมูลที่มีจำนวนน้อย) สามารถแก้ไขข้อมูลที่กรอกเข้ามาได้ จำกัดการแก้ไขได้เฉพาะสมาชิกที่เป็นผู้กรอกข้อมูลเท่านั้น สามารถดูคำแนะนำการใช้งานการกรอกข้อมูลลงบนเว็บไซต์ได้ สามารถดูข้อมูลที่กรอกเข้ามาในรูปแบบของตารางได้ สามารถอัปโหลดชุดข้อมูล .CSV (ชุดข้อมูลที่มีจำนวนมาก) เพื่อให้ผู้ดูแลเว็บไซต์ได้นำได้ชุดข้อมูลไปผ่านกระบวนการวิเคราะห์ต่าง ๆ และให้ผู้ดูแลเว็บไซต์อัปเดตข้อมูลลงเว็บไซต์นี้ สามารถดูสถานะของข้อมูลของผู้ดูแลเว็บไซต์ดำเนินการอยู่ได้ สามารถลบการอัปโหลดชุดข้อมูลได้ จำกัดการลบได้เฉพาะสมาชิกที่เป็นผู้อัปโหลดข้อมูลเท่านั้น สามารถดูคำแนะนำการใช้งานการอัปโหลดชุดข้อมูลให้ผู้ดูแลระบบได้ สามารถดูชุดข้อมูลที่อัปโหลดในรูปแบบของตารางได้ สามารถดาวน์โหลดข้อมูลที่ผ่านกระบวนการวิเคราะห์ข้อมูลและจัดการ จากผู้ดูแลเว็บไซต์ได้เพื่อนำไปศึกษาต่อ สามารถทำแบบฟอร์มการประเมินทางด้านเว็บไซต์และด้านการวิเคราะห์ ข้อมูล ของเว็บไซต์ การวิเคราะห์ข้อมูลภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021 ได้ สามารถติดต่อสอบถามเพิ่มเติมจากผู้ดูแลเว็บไซต์ผ่านทางระบบ Line Notify ได้

4.3.3 ผู้ดูแลเว็บไซต์ สามารถดูข้อมูลความรู้และบทความเกี่ยวกับ ภัยคุกคามการโจมตีบนเว็บไซต์ สามารถดูทฤษฎีและกระบวนการที่วิเคราะห์ข้อมูล CRISP-DM ของเว็บไซต์ สามารถดูแดชบอร์ดข้อมูลสารสนเทศของภัยคุกคามการโจมตีทางเว็บไซต์ ของประเทศไทย สามารถดูแดชบอร์ดข้อมูลสารสนเทศของภัยคุกคามการโจมตีทางเว็บไซต์ รวมของทุกประเทศ 5 สามารถนำเสนอ กฎที่ได้จากโมเดล Decision tree ให้มีความน่าสนใจ สามารถนำเว็บไซต์ ไปนำเสนอ อบรมให้ความรู้หรือใช้ในการศึกษาทางด้าน ภัยคุกคามทางด้านเว็บไซต์ได้ เว็บไซต์การวิเคราะห์ข้อมูลภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ ในปี 2019-2021 รองรับภาษาทั้งหมด 109 ภาษา เว็บไซต์มีการใช้ google recaptcha เพื่อป้องกันเว็บไซต์จากสแปม มีการป้องกันการเข้าสู่ระบบที่ไม่สำเร็จจะทำการบล็อก การเข้าสู่ระบบชั่วคราว สามารถเข้าสู่ระบบได้ โดย ไอดี และ รหัสผ่าน มีการแจ้งเตือนการเข้าสู่ระบบ ผ่าน Line Notify สามารถแก้ไขข้อมูลส่วนตัวได้ สามารถดูแดชบอร์ดข้อมูลสารสนเทศของภัยคุกคามการโจมตีทางเว็บไซต์ของประเทศไทย สามารถดูแดชบอร์ดข้อมูลสารสนเทศของภัยคุกคามการโจมตีทางเว็บไซต์รวมของทุกประเทศ สามารถดาวน์โหลดรีพอร์ตข้อมูลแดชบอร์ดภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ ในรูปแบบของ PDF ได้ สามารถกรอกข้อมูลลงบนเว็บไซต์เพื่อเพิ่มข้อมูลได้ (ชุดข้อมูลที่มีจำนวน

น้อย) สามารถแก้ไขข้อมูลที่กรอกเข้ามาได้ สามารถลบข้อมูลที่กรอกเข้ามาได้ สามารถดูคำแนะนำการใช้งานการกรอกข้อมูลลงบนเว็บไซต์ได้ สามารถดูข้อมูลที่กรอกเข้ามาในรูปแบบของตารางได้ สามารถอัปโหลดชุดข้อมูล .CSV (ชุดข้อมูลที่มีจำนวนมาก) เพื่ออัปเดตแดชบอร์ดที่แสดงในเว็บไซต์ เป็นข้อมูลที่ผ่านกระบวนการวิเคราะห์ต่าง ๆ และจัดรูปแบบแล้ว แสดงจำนวนข้อมูลทั้งหมดที่มีอยู่ในฐานข้อมูลได้ สามารถจัดการชุดข้อมูลที่สมาชิกอัปโหลดมาได้ สามารถแก้ไขสถานะของการดำเนินการได้ สามารถดาวน์โหลดชุดข้อมูลได้ สามารถลบชุดข้อมูลได้ สามารถดูคำแนะนำการใช้งานการจัดการชุดข้อมูลได้ สามารถจัดการสมาชิกได้ สามารถแก้ไขข้อมูลของสมาชิกได้ สามารถลบสมาชิกได้