ระบบสนับสนุนการจัดการฐานข้อมูลสายใยแก้วนำแสง

ดวงกมล พันพลู[1]
อาจารย์ ดร.ธนัญ จารุวิทยโกวิท[2]

บทคัดย่อ

ปัจจุบันการดำเนินการติดตั้งและตรวจสอบการใช้งานสายใยแก้วนำแสง (Fiber Optic) ของผู้ให้บริการโทรคมนาคมบางรายไม่ได้มีการจัดเก็บเป็นระบบฐานข้อมูล และไม่มีการตรวจสอบประสิทธิภาพสายใยแก้วนำแสงที่เป็นระบบ ทำให้บริษัทที่มีหน้าที่รับผิดชอบเกี่ยวกับงานตรวจสอบดูแลสายใยแก้วนำแสงทำงานได้ไม่เต็มประสิทธิภาพ เพื่อแก้ปัญหาดังกล่าวงานวิจัยจึงมีแนวคิดในการ พัฒนาระบบระบบเพื่อสนับสนุนการจัดการฐานข้อมูลสายใยแก้วนำแสง (Fiber Optic Database Management Support System) ขึ้นเพื่อจัดการปัญหาดังกล่าว ระบบที่พัฒนาจะเข้ามาช่วยในการจัดเก็บฐานข้อมูลของสายใยแก้วนำแสง สามารถบอกค่าการลดทอนสัญญาณ (Loss) สถานภาพสายใยแก้วนำแสงในแต่ละคอร์ (Core) และแสดงรายงานเพื่อบอกประสิทธิภาพของสายใยแก้วนำแสง โดยสามารถบอกค่าลดทอนสัญญาณของแต่ละคอร์ ผู้ใช้งานสามารถทราบได้ว่าเมื่อใช้งานแล้วระบบจะมีความเสถียรหรือไม่ ทำให้บริษัทผู้รับผิดชอบสามารถมองเห็นภาพรวมและประเมินประสิทธิภาพสายใยแก้วนำแสงได้อย่างชัดเจน

1. บทนำ

ปัจจุบันสายใยแก้วนำแสง (Fiber optic) ได้เข้ามามีบทบาทอย่างมากในเทคโนโลยีการสื่อสารข้อมูลยุคใหม่ที่มีความเร็วในการรับ-ส่งข้อมูลสูงมาก สามารถส่งข้อมูลได้คราวละมาก ๆ ในสายส่งขนาดเล็กและสามารถรับส่งข้อมูลในระยะไกลได้ ปกติแล้วสายโยแก้วนำแสงจะถูกใช้ในโครงข่ายหลัก (Core network) ของผู้ให้บริการโทรคมนาคม แต่ในปัจจุบันผู้ให้บริการอินเทอร์เน็ตความเร็วสูงแบบมีสาย (Fixed broadband operatore) เริ่มติดตั้งสายใยแก้วนำแสงจนถึงบ้านผู้ใช้บริการ (Fiber To The Home – FTTH) แทนที่สายส่งเคเบิลทองแดง (Asymmetric Digital Subscriber Line – ADSL) แล้วในหลายพื้นที่ โดยเฉพาะพื้นที่ในตัวเมือง

---

[1] นักศึกษาหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาสาขาวิชาวิศวกรรมคอมพิวเตอร์และ โทรคมนาคม มหาวิทยาลัยธุรกิจบัณฑิตย์

[2] ที่ปรึกษาวิทยานิพนธ์

สารนิพนธ์ฉบับนี้มุ่งเน้นไปที่สายใยแก้วนำแสง ประเภทซิงค์เกิ้ลโหมด (Single mode) โดยเฉพาะอย่างยิ่งสายใยแก้วนำแสงที่มีการพาดสายตามเสาไฟฟ้าตามท้องถนน เพื่อเชื่อมต่อระหว่างสถานีให้บริการของผู้ให้บริการโทรคมนาคม การเชื่อมต่อสายใยแก้วนำแสงมีชื่อเรียกว่าการสไปร์ (Splice) ซึ่งการสไปร์ก็เป็นสาเหตุหนึ่งที่ทำให้สายเกิดการลดทอนของสัญญาณแสง (Loss) ในสายใยแก้วนำแสง อย่างไรก็ตามค่าการลดทอนของสัญญาณที่เกิดขึ้นทั้งหมดจะต้องไม่ทำให้ความแรงของสัญญาณแสงที่อุปกรณ์ปลายทางได้รับต่ำเกินกว่าค่ามาตรฐาน เพื่อให้สามารถติดต่อสื่อสารระหว่างอุปกรณ์ต้นทางและปลายทางได้ นอกจากการสไปร์สายใยแก้วนำแสงแล้ว การลดทอนของสัญญาณแสงอาจเกิดขึ้นได้จากสาเหตุอื่น ๆ เช่น จำนวนหัวต่อที่เพิ่มขึ้น การโค้งงอของสายใยแก้วนำแสง ความไม่สม่ำเสมอของโครงสร้างในสายใยแก้วนำแสง เป็นต้น ซึ่งสาเหตุเหล่านี้ล้วนทำให้การสื่อสารไม่มีคุณภาพ สาเหตุต่าง ๆ เหล่านี้มักเกิดหลังจากที่มีการใช้งานสายใยแก้วนำแสงไปแล้วช่วงเวลาหนึ่ง ดังนั้นหลังจากการเริ่มใช้งานสายใยแก้วนำแสงแล้วเรื่องของการบำรุงรักษา (Maintenance) จึงสำคัญอย่างยิ่งในการตรวจสอบประสิทธิภาพของสายใยแก้วนำแสง ว่ามีการส่งสัญญาณเป็นอย่างไร และปัจจุบันผู้ดูแลบำรุงรักษาสายใยแก้วนำแสงยังไม่มีระบบสนับสนุนการจัดเก็บฐานข้อมูลสายใยแก้วนำแสงอย่างเป็นระบบ เพราะยังใช้การบันทึกลงใน Microsoft Excel อาจทำให้มีความยุ่งยากในการจัดเก็บและยากต่อการค้นหาข้อมูลสายใยแก้วย้อนหลัง ดังนั้นผู้วิจัยจึงได้พัฒนาระบบสนับสนุนการติดตั้งและดูแลรักษาโครงข่ายสายใยแก้วนำแสงนี้ขึ้นมา เพื่อแก้ไขปัญหาดังกล่าว

2. ระเบียบวิธีการวิจัย

2.1 สายใยแก้วนำแสง [1,2]

สายใยแก้วนำแสง (Fiber Optic)ปัจจุบันใช้เป็นสื่อสัญญาณ (Transmission)ในโครงข่ายหลักของผู้ให้บริการโทรคมนาคม เนื่องจากสายใยแก้วนำแสงมีความจุของช่องสัญญาณ (Capacity) สูงมาก มีขนาดเล็ก น้ำหนักเบา ยืดหยุ่นโค้งงอได้ และสามารถรับส่งสัญญาณได้ในระยะไกล ใยแก้วนำแสงทำหน้าที่เป็นตัวกลางในการส่งแสงจากด้านหนึ่งไปอีกด้านหนึ่ง ด้วยความเร็วเกือบเท่าแสง เมื่อนำมาใช้ในการสื่อสารโทรคมนาคม ทำให้สามารถส่ง-รับข้อมูลได้เร็วมาก

2.2 การลดทอนสัญญาณแสง [3]

การลดทอนของแสงมีค่าเป็นเดซิเบล (dB) ของสายใยแก้ว สูตรดังนี้

Total Loss (dB) = (2 x TLoss) + (DFiber x Att.Fiber) + (N x SLoss)

คำอธิบาย

TLoss = ค่าการสูญเสียที่จุด Connector = 0.5 dB.

DFiber = ระยะของสายใยแก้วนำแสง (Km)

Att.Fiber = ค่าการลดทอนสัญญาณของสายใยแก้วนำแสง

SLoss = ค่าการสูญเสียที่จุดต่อสายใยแก้วนำแสง (Splice Loss) = 0.05 dB.

N = จำนวนจุดต่อสายใยแก้วนำแสงทั้งหมด

ค่ามาตรฐานของค่าลดทอนสัญญาณที่ความยาวคลื่นที่ใช้ ในงานวิจัยนี้

ตารางที่ 1 ค่ามาตรฐานค่าลดทอนสัญญาณที่ความยาวคลื่นต่าง ๆ

Type	ค่าลดทอนสัญญาณที่ความยาวคลื่น (Att.Fiber)		
	1310 nm.	1550 nm.	1625 nm.
G.652 D	0.33 dB./Km.	0.20 dB./Km.	-
G.655	-	0.275 dB./Km.	0.35 dB./Km.

2.3 การสูญเสียในสายใยแก้วนำแสง [7]

- ไฟไหม้สายใยแก้วนำแสง
- หนู กระรอกกัดแทะ
- การโค้งงอของสายใยแก้วนำแสง
- การติดตั้งสายไม่ถูกวิธีหรือไม่เรียบร้อย
- การสูญเสียเนื่องจากการเข้าหัว Connector และทำ Splice ไม่ดี

2.4 เครื่อง OTDR (Optical Time Domain Reflectometer) [8,9]

เครื่อง OTDR ใช้วัดค่าพารามิเตอร์ต่าง ๆ ภายในโครงข่ายสายใยนำแสงสัมพันธ์กับความยาว โดยนำปลายหัวต่อด้านหนึ่งของเส้นใยนำแสงที่ต้องการวัดต่อเข้ากับเครื่อง OTDR และกำหนดค่าฟังก์ชั่นตามที่เราต้องการวัดค่า เครื่อง OTDR อาศัยหลักการการสะท้อนของแสงที่เดินทางในสายใยแก้วนำแสงเทียบกับเวลา ซึ่งแสงเดินทางย้อนกลับมายังด้านต้นทางที่แสงเข้า จากนั้นจะแสดงค่าลดทอนสัญญาณในแต่ละคอร์ของสายใยแก้วนำแสง

2.5 ฐานข้อมูล [10]

เป็นที่เก็บบันทึกข้อมูลต่าง ๆ ข้อมูลจะถูกเก็บใน Record ซึ่งในแต่ละRecord จะประกอบไปด้วย Field โดยจะเก็บรวบรวมข้อมูลและความสัมพันธ์ระหว่างข้อมูล และมีซอฟต์แวร์ระบบบริหารจัดการข้อมูลช่วยในการจัดเก็บ และค้นหาข้อมูลโดยโปรแกรมประยุกต์ต่าง ๆ เป็นไปอย่างมีประสิทธิภาพ

MySQL โปรแกรมระบบจัดการฐานข้อมูล มีหน้าที่เก็บข้อมูลโดยใช้คำสั่ง SQL ซึ่งต้องทำงานร่วมกับเว็บเซิฟเวอร์จะทำงานฝั่ง Server side Script โดยในงานวิจัยนี้ได้ใช้ภาษา PHP ในการติดต่อทำงานกับฝั่งเซิร์ฟเวอร์

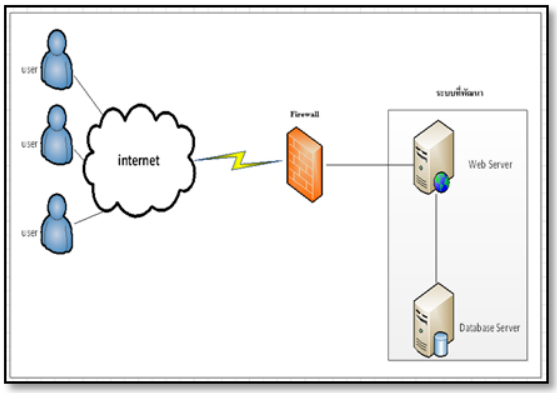
2.6 แนวความคิดเกี่ยวกับโปรแกรม PHP [11,12]

ภาษา PHP นั้นเป็นเป็นภาษาที่มีลักษณะเป็นแบบ Open source PHP เป็นสคริปต์แบบหนึ่งเรียกว่า Server Side Script ที่ประมวลผลฝั่งเซิร์ฟเวอร์ แล้วส่งผลลัพธ์ไปฝั่งเครื่องคอมพิวเตอร์ ผ่านเว็บบราวเซอร์ หน้าที่หลักของ PHP คือ เป็นตัวประมวลผลคำสั่ง หรือโปรแกรมที่เราเขียนเพื่อให้ได้ผลลัพธ์ออกมาตามที่ต้องการ นอกจากนี้ยังมีโปรแกรมฐานข้อมูล ที่เป็นตัวเสริมการทำงานเพื่อใช้ในการจัดเก็บข้อมูลของระบบเว็บ

3. การออกแบบและการพัฒนาระบบ

3.1 ระบบสนับสนุนการจัดการสายใยแก้วนำแสง

มีการออกแบบโครงสร้างการทำงาน ดังภาพที่ 1

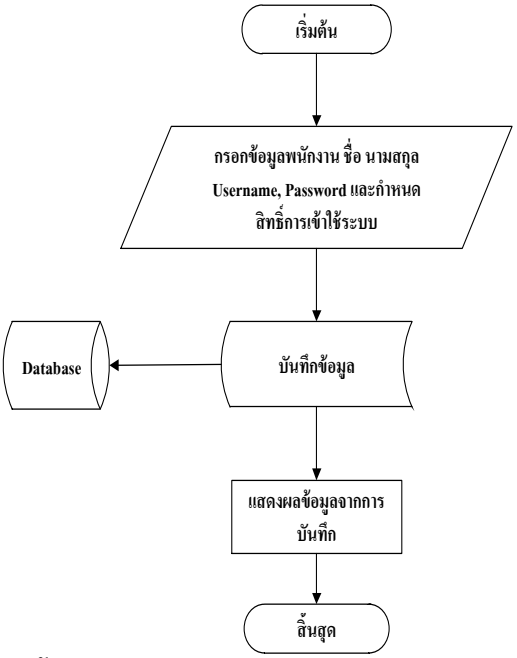


ภาพที่ 1 โครงสร้างการทำงานของระบบที่ออกแบบ

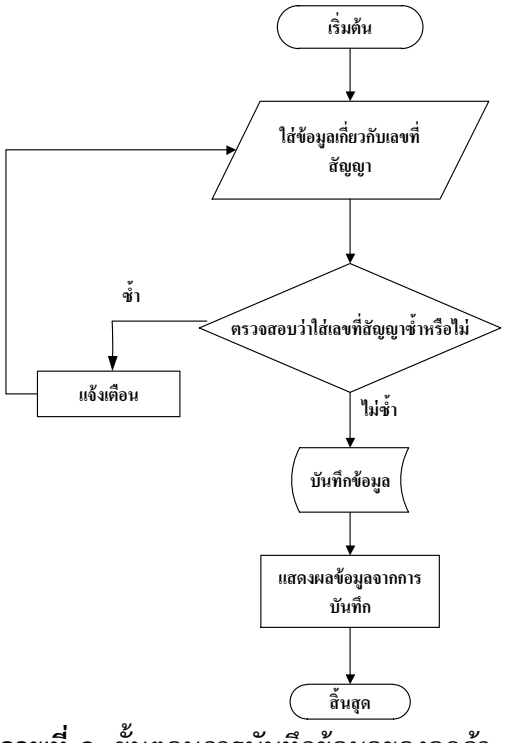
โครงสร้างของระบบจะเป็นการใช้งานในรูปแบบของ internet Connection เชื่อมต่อเข้ามายังเซิร์ฟเวอร์ แม่ข่ายที่ติดตั้งอยู่ที่บริษัท ซึ่งประกอบไปด้วย การทำงานของ Database Server และ เว็บแอพพลิเคชั่นเซิร์ฟเวอร์ ซึ่งจะมีระบบรักษาความปลอดภัยเครือข่ายในรูปแบบของไฟร์วอลล์ที่ช่วยป้องกันการบุกรุก และการเข้าใช้งานผู้ใช้งานต้อง VPN เข้ามาเพื่อเรียกหน้า Web Application Login โดยที่ผู้ใช้งานระบบต้องระบุ Username และ Password ลงในช่องที่กำหนดให้ เพื่อตรวจสอบว่ามีสิทธิ์เข้าถึงโปรแกรมหรือไม่ และมีสิทธิ์ระดับ User, Super user หรือ Admin

3.2 ขั้นตอนการทำงานของระบบที่พัฒนา

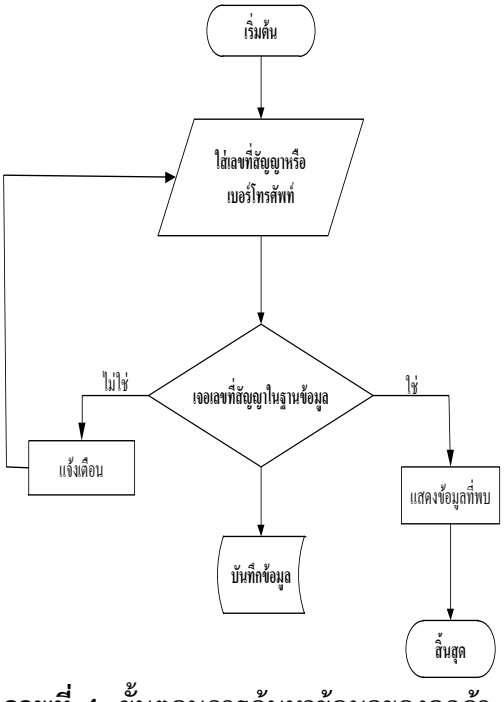
การพัฒนาระบบการสนับสนุนการจัดการฐานข้อมูลสายใยแก้วนำแสง ที่พัฒนาขึ้นมาสามารถแสดงขั้นตอนการทำงานหลักของระบบงานในรูปแบบของ Flowchart ดังแสดงในภาพที่ 2 เป็นขั้นตอนการสร้างผู้ใช้งานและการกำหนดสิทธิ์เข้าใช้ ภาพที่ 3 เป็นขั้นตอนการบันทึกข้อมูลของลูกค้า ภาพที่ 4 แสดงขั้นตอนการค้นหาข้อมูลของลูกค้า ภาพที่ 5 เป็นขั้นตอนการตรวจบำรุงรักษาสายใยแก้วนำแสง



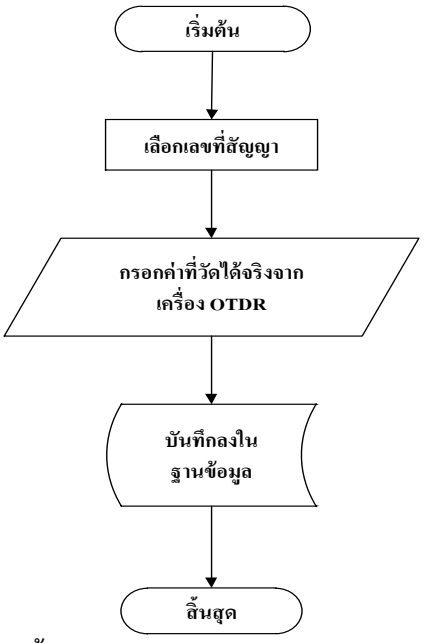
ภาพที่ 2 ขั้นตอนการสร้างผู้ใช้งานและการกำหนดสิทธิ์เข้าใช้



ภาพที่ 3 ขั้นตอนการบันทึกข้อมูลของลูกค้า

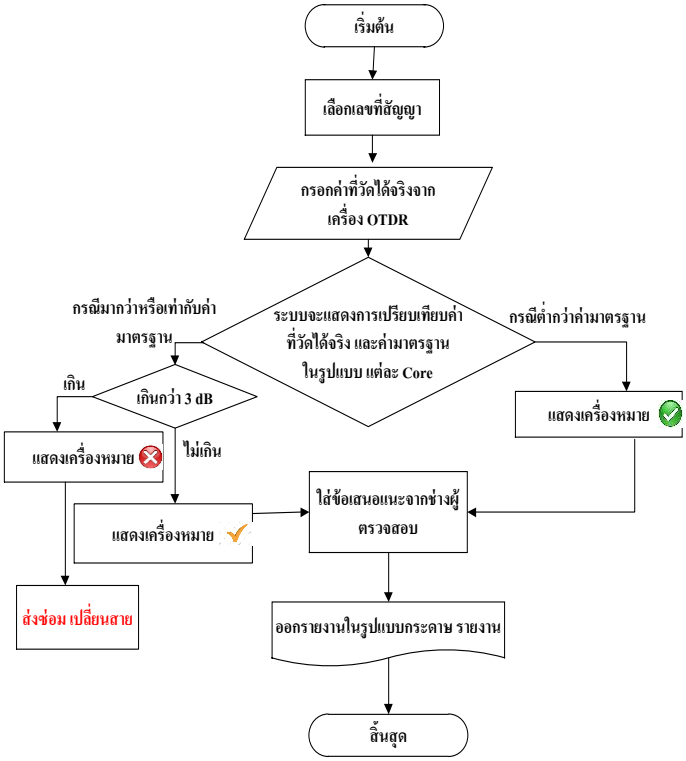


ภาพที่ 4 ขั้นตอนการค้นหาข้อมูลของลูกค้า



ภาพที่ 5 ขั้นตอนการตรวจบำรุงรักษาสายใยแก้ว

ลักษณะการทำงานของระบบในการตรวจวัดค่าความแรงของสายใยแก้วที่วัดได้จริงด้วยเครื่อง OTDR เทียบกับค่าที่คำนวณทางทฤษฎีแสดงดังภาพที่ 6



ภาพที่ 6 ลักษณะการทำงานของระบบการสนับสนุนการจัดการฐานข้อมูลสายใยแก้วนำแสง

4. การทดสอบการใช้งานระบบ

การทดสอบระบบจะแบ่งการทดสอบออกเป็น 7 หัวข้อ ดังนี้

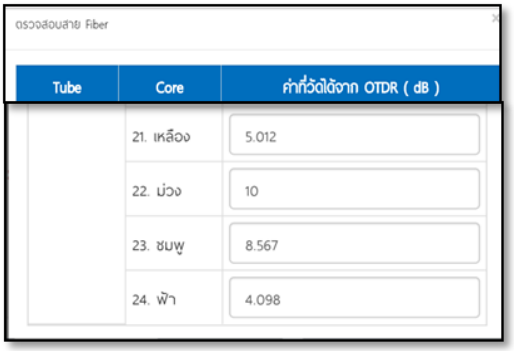
1. การทดสอบการสร้างผู้ใช้งานและการกำหนดสิทธิ์ โดยผู้ดูแลระบบ โดยการสร้างผู้ใช้งานส่วนนี้จะเป็นการสร้างบัญชีรายชื่อผู้ใช้ และการกำหนดสิทธิ์การเข้าใช้งาน
2. การทดสอบสร้างข้อมูลลูกค้า โดยการสร้างข้อมูลลูกค้าและรายละเอียดสายใยแก้วพร้อมทั้งสามารถแก้ไขข้อมูลสายได้
3. การสร้างเส้นทางเพิ่ม โดยการเพิ่มเส้นทางที่ต้องดูแลและตรวจสอบ
4. ทดสอบการใส่ค่าลดทอนสัญญาณในแต่ละคอร์
5. ทดสอบการแสดงค่าการลดทอนของสัญญาณที่วัดได้จริงในแต่ละคอร์เทียบกับการคำนวณทางทฤษฎี
6. ทดสอบการพิมพ์รายงาน รายละเอียดข้อมูลการติดตั้งเส้นทางสายใยแก้ว ข้อมูลการบำรุงรักษาข้อมูลประสิทธิภาพสายสัญญาณสายใยแก้วนำแสง และข้อมูลข้อเสนอแนะ
7. นำโปรแกรมที่พัฒนาขึ้นให้บริษัทที่ปฏิบัติงานจริง โดยในสารนิพนธ์นี้ บริษัท แอ็ดวานซ์ อินฟอร์เมชั่นเทคโนโลยี จำกัด (มหาชน) และ ห้างหุ้นส่วนจำกัด จี แอนด์ เอ็น เทเลคอม ซึ่งทั้ง 2 บริษัทเป็นผู้ดูแล

ข่ายสายใยแก้วนำแสงให้กับผู้ให้บริการโทรคมนาคม จะช่วยทดสอบและประเมินการทำงานของระบบที่ออกแบบและพัฒนา

ในการทดสอบการใช้งานระบบ ได้ทำการทดสอบการสร้างข้อมูลลูกค้าและรายละเอียดของสายใยแก้วนำแสงดังนี้

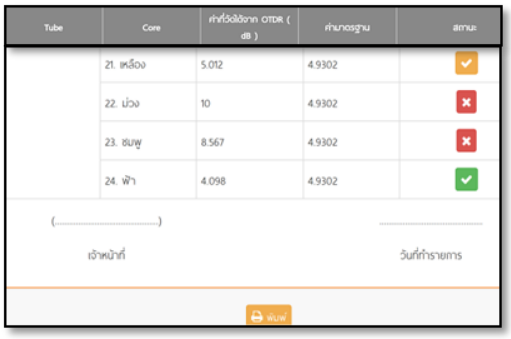
ภาพที่ 7 ผลการสร้างข้อมูลลูกค้าและข้อมูลเส้นทางการติดตั้ง

ระบบจะทำการให้ช่างผู้ดูแลงานทำการตรวจสอบโดยใส่ค่าที่วัดได้จริงจากเครื่อง OTDR ดังภาพ

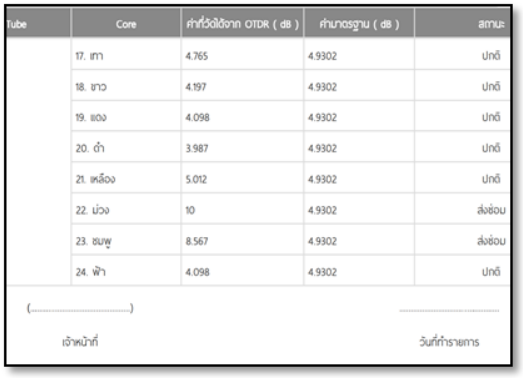


ภาพที่ 8 ผลการกรอกค่าลดทอนสัญญาณที่วัดได้จากเครื่อง OTDR

ทำการทดสอบการเปรียบเทียบค่าความแรงของสัญญาณของสายใยแก้วนำแสงจากค่าที่วัดได้จริงจากเครื่อง OTDR เทียบกับค่าทางคำนวณทางทฤษฎี ได้ผลดังภาพที่ 9และแสดงหน้าจอรายงานดังภาพที่ 10

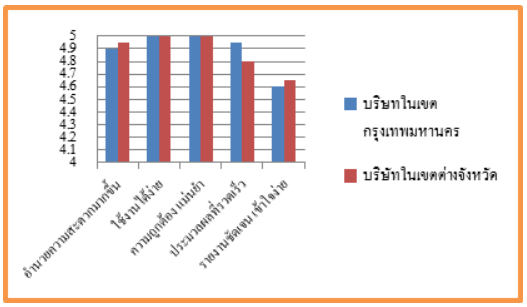


ภาพที่ 9 หน้าจอสถานะของสายใยแก้วนำแสง



ภาพที่ 10 หน้าจอการพิมพ์รายงานสายใยแก้วนำแสง

จากการพัฒนาระบบการสนับสนุนการจัดการฐานข้อมูลสายใยแก้วนำแสงได้วัดประสิทธิภาพของการงานระบบโดยการทดสอบจากช่างผู้ดูแลงานของบริษัทฯ ที่อยู่ในเขตกรุงเทพมหานคร เปรียบเทียบกับบริษัทฯ ที่อยู่ในเขตต่างจังหวัดได้ผลดังภาพที่ 11



ภาพที่ 11 กราฟแผนภูมิแท่งเปรียบเทียบความคิดเห็นของช่างที่ดูแลงานสายใยแก้วนำแสงระหว่างบริษัทฯ ในเขตกรุงเทพมหานคร (บริษัท แอ็ดวานซ์ อินฟอร์เมชั่นเทคโนโลยี จำกัด (มหาชน)) และบริษัทฯ ในเขตต่างจังหวัด (ห้างหุ้นส่วนจำกัด จี แอนด์ เอ็น เทเลคอม)

จากภาพที่ 11 สามารถสรุปผลได้ว่าดังนี้

1. เรื่องระบบสามารถอำนวยความสะดวกมากขึ้น บริษัทฯ ในเขตกรุงเทพมหานครและบริษัทฯ ในเขตต่างจังหวัดให้คะแนน 4.9 และ 4.95 เหตุผลเพราะช่างบางคนของทั้ง 2 บริษัทฯ ส่วนใหญ่ที่มีอายุมากกว่า 41 ปี ไม่คุ้นเคยกับการทำงานผ่านเว็บ คุ้นเคยกับการทำงานโดยใช้กระดาษแบบเดิม

2. เรื่องระบบสามารถใช้งานได้ง่าย และ เรื่องประสิทธิภาพบริษัทฯ เขตกรุงเทพมหานครและบริษัทฯ ในเขตต่างจังหวัดให้คะแนนเต็มคือ 5

3. เรื่องระบบมีการประมวลผลที่รวดเร็ว บริษัทฯ เขตกรุงเทพมหานครให้คะแนน 4.95 บริษัทฯ ในเขตต่างจังหวัดให้คะแนนคือ 4.8 คือ เนื่องจากบริษัทที่อยู่ต่างจังหวัดใช้เครื่องโทรศัพท์มือถือของช่างเองทำการทดลองใช้ระบบผ่านหน้าจอโทรศัพท์ ณ ขณะทดลองความเร็วของอินเตอร์เน็ตช่างอาจช้าเนื่องจากแพคเกจมือถือที่ช่างใช้มีน้อย จึงทำให้ระบบช้าแต่ก็ไม่เกิน 5 วินาที เทียบกับการใช้งานผ่านเครื่องคอมพิวเตอร์

4. เรื่องเนื้อหารายงานมีความชัดเจน เข้าใจง่ายบริษัทเขตกรุงเทพมหานครให้คะแนน 4.6 บริษัทในเขตต่างจังหวัดให้คะแนนเต็มคือ 4.65 คือ ช่างทั้ง 2 บริษัทมองว่าเนื้อหารายงานที่แสดงยังมีองค์ประกอบไม่ครบถ้วนยังขาดภาพรวมเส้นทางทั้งหมดที่ดูแล

5. สรุปผลการศึกษาวิจัย

งานวิจัยนี้นำเสนอระบบสนับสนุนการจัดเก็บฐานข้อมูลสายใยแก้วนำแสง ซึ่งเป็นระบบที่ออกเพื่อแบบช่วยในการตรวจสอบ ดูแล สายใยแก้วนำแสงตามวงรอบที่หน่วยงานนั้น ๆ กำหนด ซึ่งระบบที่พัฒนาสามารถเปรียบเทียบค่าความแรงของสัญญาณที่วัดได้จริงจากเครื่อง OTDR และค่าที่คำนวณทางทฤษฎีในแต่ละคอร์ได้อย่างถูกต้อง และออกรายงานในรูปแบบที่สามารถเข้าใจง่าย จากการทดสอบการใช้งานระบบ พบว่า

ระบบสามารถใช้งานได้ดี มีการแสดงข้อมูลที่ถูกต้อง และสามารถใช้งานได้จริง แต่หากในอนาคตจะมีผู้นำไปพัฒนาต่อควรพัฒนาให้ระบบสามารถเปรียบเทียบชนิดของสายใยแก้วและความยาวคลื่นให้ได้หลากหลายชนิดมากขึ้นและสามารถมองเห็น topology ภาพรวมเส้นทางของทั้งเส้นที่รับผิดชอบเพื่อให้สามารถมองประสิทธิภาพสายในภาพรวมทั้งระบบได้

บรรณานุกรม

จงเจริญ แจ้งมาก. (2556). **การพัฒนาโปรแกรมบริหารจัดการโครงข่ายเส้นใยแก้วนำแสง**

อธิคม ฤกษบุตร. (2543). **เส้นใยแก้วและการประยุกต์ใช้งานเบื้องต้น**

มาตรฐานปัจจุบันของ ITU (International Telecommunication Union) G.652.D G.655 (11/2009)

PREM S. MANN. Introductory Statistics SEVENTH EDITION

รายงานการวิจัย **การแก้ไขข้อผิดพลาดของสัญญาณปลายทางในเครื่องสื่อสารด้วยเส้นใยแก้วนำแสง** มหาวิทยาลัยเทคโนโลยีราชมงคลล้านนา

www.siamfiber.com/1012501/**การประยุกต์ใช้เครื่อง-otdr** : เข้าถึง 29 ตุลาคม 2559

สามภพ วชิรบรรจง. (2550). **การออกแบบระบบฐานข้อมูลเพื่อการจัดการความผิดพลาดในระบบป้องกันทางไฟฟ้าของเครื่องกำเนิดไฟฟ้า** สถาบันเทคโนโลยีพระจอมเกล้าเจ้าอยู่หัวพระนครเหนือ

บัญชา ปะสีสะเตสัง. (2553). **พัฒนาเว็บแอปพลิเคชั่นด้วยPHPร่วมกับMySQLและDreamweaver**

การประเมินค่าช่องโหว่ของเว็บไซต์และการป้องกัน กรณีศึกษาเว็บไซต์ กรมควบคุมการปฏิบัติทางอากาศ

เรืออากาศตรีหญิง ณัชณภัทร ใจอดทน[1]
ดร.ชัยพร เขมะภาตะพันธ์ [2]

บทคัดย่อ

บทความนี้ได้ทำการศึกษา ค้นคว้าเพื่อหาช่องโหว่หรือจุดอ่อนของเว็บไซต์ กรณีศึกษาเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ “www.daoc.rtaf.mi.th” ว่าเว็บไซต์ดังกล่าวมีช่องโหว่หรือจุดอ่อนหรือไม่ ช่องโหว่หรือจุดอ่อนนั้นมีระดับความรุนแรงและมีผลกระทบต่อเว็บไซต์อย่างไร โดยใช้โปรแกรม Acunetix Web Vulnerability Scanner เป็นเครื่องมือในการตรวจหาช่องโหว่ของเว็บไซต์และการหาช่องโหว่โดยใช้วิธีการทดสอบเจาะระบบโดยใช้เทคนิค Local File Disclosure ในการหาช่องโหว่ ซึ่งผู้วิจัยได้แบ่งขั้นตอนในการหาช่องโหว่ของเว็บไซต์ เป็น 3 ขั้นตอน ประกอบด้วย

(1) การวางแผนและเตรียมการ(Planning and Preparation
(2) การประเมินค่าของช่องโหว่ (Vulnerability Assessment)
(3) การทำรายงานวิธีการแก้ไขและการป้องกันช่องโหว่ (Report how to fix and prevent vulnerabilities)

ผลลัพธ์จากการศึกษา ค้นคว้าแสดงให้เห็นว่าผู้วิจัยสามารถตรวจพบช่องโหว่ของเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ รวมทั้งสิ้นจำนวน 5 ช่องโหว่ ซึ่งเป็นช่องโหว่ที่มีความรุนแรงระดับสูง 1 ช่องโหว่ ช่องโหว่ที่มีความรุนแรงระดับปานกลาง 1 ช่องโหว่ และช่องโหว่ที่มีความรุนแรงระดับต่ำ 3 ช่องโหว่ โดยช่องโหว่ที่มีความรุนแรงระดับสูง แฮกเกอร์สามารถนำไปใช้ประโยชน์ในการโจมตีเว็บไซต์ดังกล่าวและเว็บไซต์อื่นที่อยู่ภายใต้โดเมนเนม “daoc.rtaf.mi.th”

1. บทนำ

กรมควบคุมการปฏิบัติทางอากาศ เป็นหน่วยงานขึ้นตรงต่อกองทัพอากาศหน่วยงานหนึ่ง ที่มีการเผยแพร่ข้อมูลต่าง ๆ ผ่านทางเว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศ เพื่อให้บริการแก่กำลังพลของกองทัพอากาศและบุคคลทั่วไปให้สามารถเข้าใช้บริการสืบค้นข้อมูลและดาวน์โหลดข้อมูล จึงมีความเสี่ยงต่อการถูกโจมตีจากผู้ไม่ประสงค์ดี

---

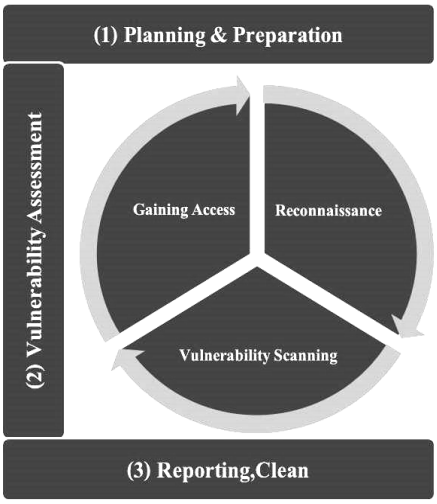
[1] นักศึกษาหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์และโทรคมนาคม วิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรมศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์

[2] ที่ปรึกษาสารนิพนธ์

ด้วยเหตุนี้ จึงมีความจำเป็นที่ต้องมีการศึกษาวิธีการหาช่องโหว่ของเว็บไซต์และวิธีการโจมตีโดยการใช้ประโยชน์จากช่องโหว่ของเว็บไซต์ เพื่อกำหนดวิธีในการแก้ไขและหาแนวทางป้องกันช่องโหว่ของเว็บไซต์ กรมควบควบการปฏิบัติทางอากาศ โดยใช้เครื่องมือ Acunetix Web Vulnerability Scanner เป็นเครื่องมือในการตรวจหาช่องโหว่ของเว็บไซต์และใช้วิธีทดสอบเจาะระบบโดยผู้ทำการวิจัย เพื่อให้เว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศมีความมั่นคงปลอดภัย

2. ทฤษฎีที่เกี่ยวข้อง

2.1 หลักการทดสอบเจาะระบบของผู้ทดสอบ



ภาพที่ 1 ขั้นตอนการตรวจหาช่องโหว่ของเว็บไซต์

2.1.1 วางแผนและเตรียมการ

เป็นการกำหนดขอบเขตของเป้าหมายในการหาช่องโหว่ของเว็บไซต์ เช่น หาช่องโหว่ของ Web Application

2.1.2 การประเมินช่องโหว่

เป็นขั้นตอนการทดสอบเพื่อทดสอบว่าเว็บไซต์มีความปลอดภัยมากน้อยเพียงใด มี 3 ขั้นตอน ดังนี้

(1) การสำรวจข้อมูล เป็นการค้นหาข้อมูลต่าง ๆ ของเป้าหมาย เช่นการตรวจสอบหมายเลข IP Address หรือรายชื่อ Service ที่เปิดใช้งานอยู่

(2) การสแกนระบบ การสแกน (Scanning) เป็นการนำข้อมูลที่รวบรวมมาได้จากขั้นตอน การสำรวจข้อมูล (Reconnaissance) มาอธิบายถึงโครงสร้าง ของเครือข่ายเป้าหมาย

(3) การเข้าถึงเป้าหมาย ขั้นตอนนี้จะเริ่มเข้าสู่การโจมตีหรือเจาะช่องที่โหว่ที่ถูกตรวจพบ

2.1.3 การทำรายงานและสิ่งที่แนะนำให้ทำ

คือขั้นตอนการสรุปงานในแต่ละขั้นตอนว่าได้ข้อมูลอะไรบ้าง

2.2 การวิเคราะห์ความรุนแรงของช่องโหว่และการประเมินความเสี่ยง

ตารางที่ 1 การวิเคราะห์ความง่ายต่อการเข้าถึงช่องโหว่

ความง่าย	ระดับคะแนน	รายละเอียด
ง่ายมาก	3	ช่องโหว่สามารถเข้าถึงจากเทคนิคทั่วไป โดยไม่ต้องยืนยันตัวตน
ปานกลาง	2	ช่องโหว่สามารถเข้าถึงจากเทคนิคทั่วไป โดยต้องผ่านการยืนยันตัวตน
ยาก	1	ช่องโหว่ต้องอาศัยการโจมตีผ่านเทคนิคเฉพาะ และการยืนยันตัวตน

ตารางที่ 2 การวิเคราะห์ผลกระทบที่จะเกิดขึ้นต่อระบบ

ผลกระทบ	ระดับคะแนน	รายละเอียด
มาก	3	ช่องโหว่สามารถขัดขวาง หรือยุติการให้บริการ หรือทำให้ข้อมูลเสียหายได้
ปานกลาง	2	ช่องโหว่ไม่สามารถทำให้ระบบหยุดการให้บริการได้ หรือจำเป็นจะต้องอาศัยช่องโหว่อื่นๆ ช่วยในการทำให้ระบบยุติการให้บริการ
น้อย	1	ช่องโหว่ไม่สามารถยุติการให้บริการได้ แต่ทำให้ได้ข้อมูลพื้นฐานเกี่ยวกับการให้บริการ

การประเมินความเสี่ยง

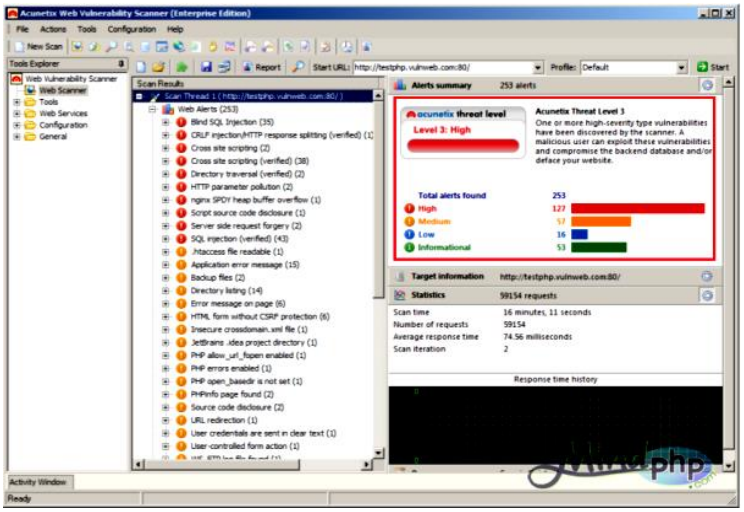
ระดับความเสี่ยง = ความง่ายต่อการเข้าถึงช่องโหว่ x ผลกระทบต่อระบบ

ตารางที่ 3 การประเมินความเสี่ยง

ระดับความเสี่ยง	คะแนน
สูง	7 - 9
กลาง	4 - 6
ต่ำ	0 – 3

2.3 เครื่องมือสำหรับตรวจหาช่องโหว่

โปรแกรม Acunetix Web Vulnerability Scanner เป็นเครื่องมือสำหรับตรวจหาช่องโหว่ของเว็บไซต์



ภาพที่ 2 เครื่องมือที่ใช้ในการตรวจหาช่องโหว่ของเว็บไซต์

2.4 Open Web Application Security Project (OWASP)

OWASP เป็นองค์กรสากลที่เป็นศูนย์รวมในการร่วมมือจากนักพัฒนาเว็บแอพพลิเคชั่นทั่วโลกในการสร้างเว็บแอพพลิเคชั่นให้มีความปลอดภัย โดยในปี 2013 OWASP ได้เผยแพร่เอกสาร OWASP TOP 10 2013 ที่อธิบายรายละเอียดช่องโหว่ที่พบได้บ่อยและมีความรุนแรง 10 อันดับดังนี้

2.4.1 Injection

2.4.2 Broken Authentication and Session Management

2.4.3 Cross-Site Scripting (XSS)

2.4.4 Insecure Direct Object References

2.4.5 Security Misconfiguration

2.4.6 Sensitive Data Exposure

2.4.7 Missing Function Level Access Control

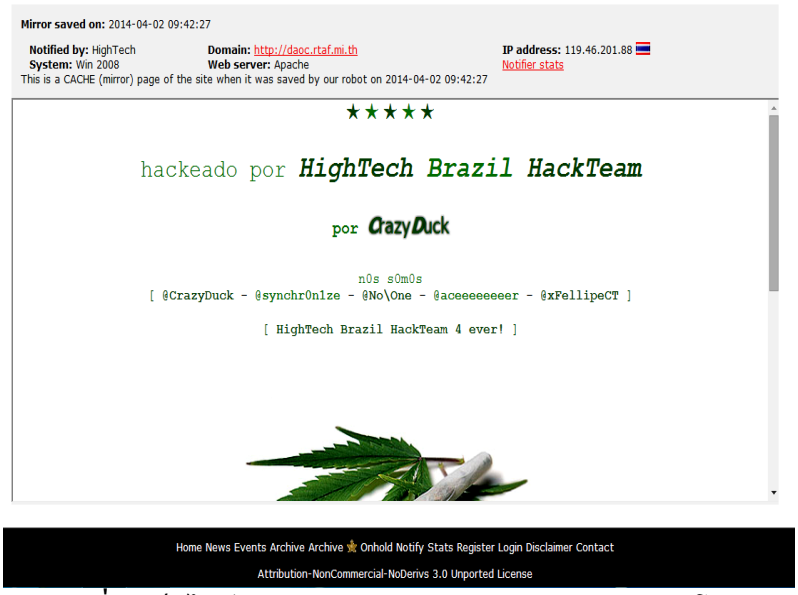
2.4.8 Cross-Site Request Forgery (CSRF)

2.4.9 Using Components with Known Vulnerabilities

2.4.10 Unvalidated Redirects and Forwards

2.5 ตัวอย่างของเว็บไซต์ที่มีช่องโหว่และเคยผ่านการถูกโจมตี

ปี พ.ศ.2557 เว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศ ถูกโจมตีโดยการเปลี่ยนหน้าเว็บไซต์ ตามภาพที่ 3



ภาพที่ 3 เว็บไซต์กรมควบคุมการปฏิบัติทางอากาศเคยถูกโจมตี

ด้วยเหตุนี้ ผู้จิวัยจึงได้ให้ความสำคัญกับการรักษาความมั่นคง ปลอดภัยของเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ เพื่อป้องกันการถูกโจมตีจากผู้ไม่ประสงค์ดี

3. การดำเนินการตรวจหาช่องโหว่ของเว็บไซต์

ในการตรวจหาช่องโหว่ของเว็บไซต์ ผู้วิจัยได้แบ่งขั้นตอนในการดำเนินการ เป็น 3 ขั้นตอน ประกอบด้วย

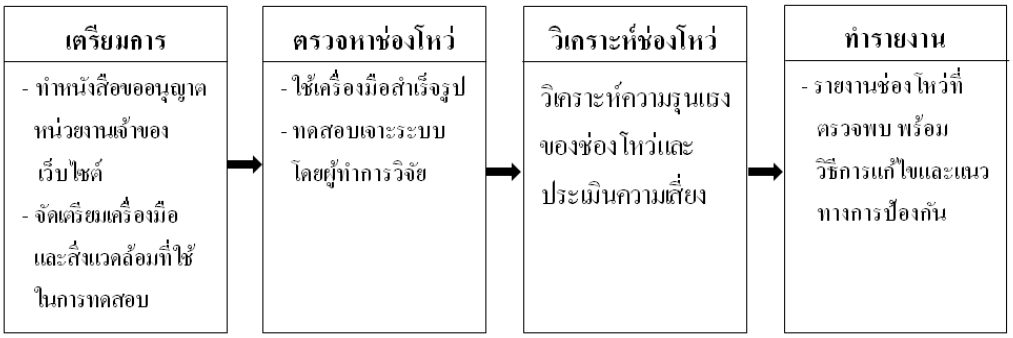
(1) การวางแผนและเตรียมการ (Planning and Preparation)

(2) การประเมินค่าของช่องโหว่ (Vulnerability Assessment)

(3) การทำรายงานวิธีการแก้ไขและการป้องกันช่องโหว่ (Report how to fix and prevent vulnerabilities)

3.1 การวางแผนและเตรียมการ (Planning and Preparation)

การวางแผนและเตรียมการในการหาช่องโหว่ของเว็บไซต์ ประกอบไปด้วย 4 ขั้นตอน ดังแสดงตามภาพที่ 4



ภาพที่ 4 ขั้นตอนการวางแผนและเตรียมการ

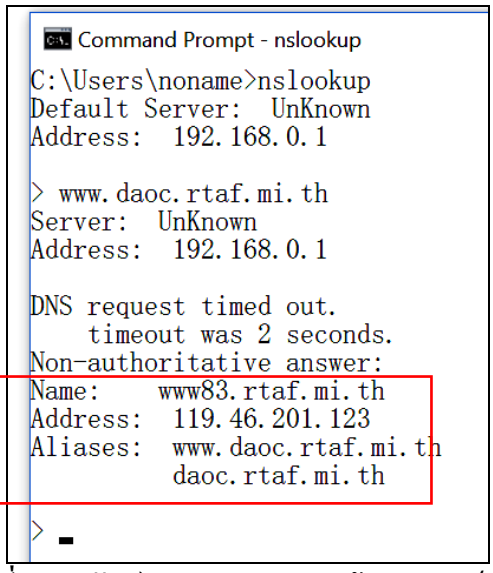
3.2 การประเมินค่าของช่องโหว่ (Vulnerability Assessment)

ผู้วิจัยได้แบ่งขั้นตอนที่นำมาใช้ในการประเมินค่าของช่องโหว่ของงานวิจัยนี้ ออกเป็น 4 ขั้นตอน ดังนี้

3.2.1 ขั้นตอนการสำรวจข้อมูล (Reconnaissance)

เป็นขั้นตอนในการหาข้อมูลที่เกี่ยวข้องกับเว็บไซต์ เพื่อนำข้อมูลที่ได้นำไปวิเคราะห์หาวิธีการเข้าถึงช่องโหว่ของเว็บไซต์ต่อไป

(1) การทำ nslookup รายละเอียดข้อมูลที่พบจากการใช้คำสั่ง nslookup แสดงตามภาพที่ 5



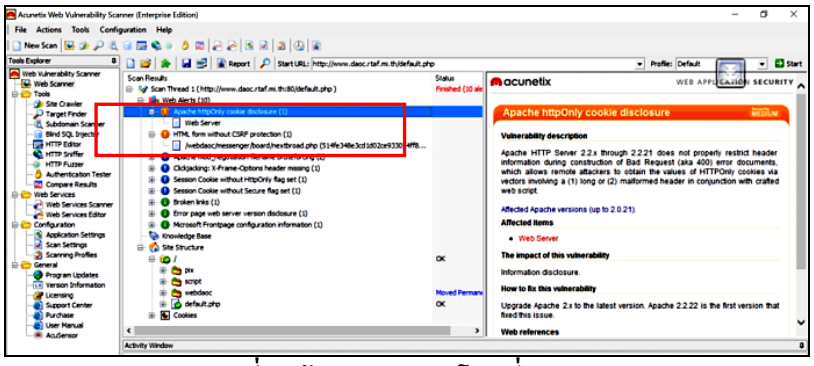
ภาพที่ 5 ผลลัพธ์ของการตรวจสอบข้อมูลของเว็บไซต์

(2) การทำ Reverse IP Domain Check รายละเอียด ข้อมูลที่ได้รับจากการทำ Reverse IP Domain Check แสดงตามภาพที่ 6

ภาพที่ 6 ผลลัพธ์การทำ Reverse IP Domain Check

3.2.2 ขั้นตอนการสแกนหาช่องโหว่ (Vulnerability Scanning)

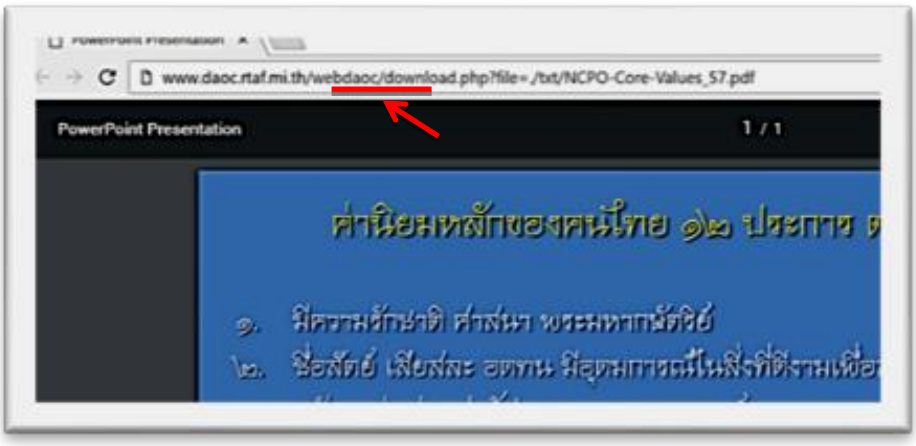
(1) ใช้เครื่องมือ Acunetix Web Vulnerability Scanner ในการสแกนหาช่องโหว่ โดยผลลัพธ์ที่ แสดงภาพที่ 7



ภาพที่ 7 ข้อมูลของช่องโหว่ที่ตรวจพบ

(2) สแกนหาช่องโหว่บนหน้าเว็บไซต์

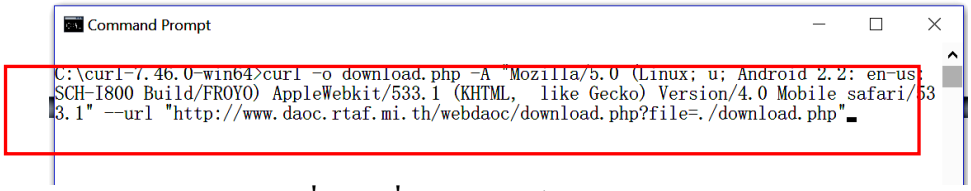
ผู้วิจัยได้ทำการสแกนหาช่องโหว่ของเว็บไซต์โดยการหาช่องโหว่จากหน้าเพจทุกเพจที่อยู่บนเว็บไซต์ จนพบข้อมูลมูลที่คาดว่าจะเป็นช่องโหว่ คือ parameter ที่ชื่อว่า“file”ในส่วนของหน้าเพจ คือ ไฟล์ที่ชื่อว่า“download.php” ซึ่งผู้วิจัยพบว่าหน้าเพจนี้มีช่องโหว่คือให้ผู้ใช้สามารถดาวน์โหลดไฟล์ ออกมาจากเซิร์ฟเวอร์ได้ตามภาพที่ 8



ภาพที่ 8 ช่องโหว่ของ Local file inclusion

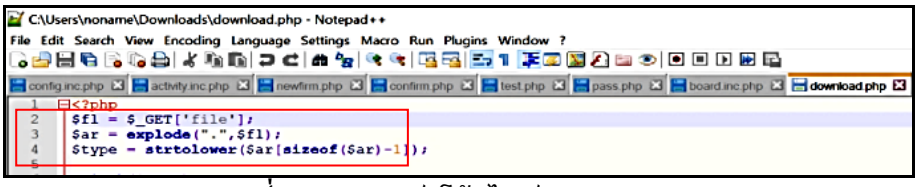
3.2.3 ขั้นตอนการเข้าถึงเป้าหมาย (Gaining Access)

นำข้อมูลที่ได้จากขั้นตอนการสแกนหาช่องโหว่มาใช้ประโยชน์ในการทดสอบการโจมตีเว็บไซต์โดยใช้เทคนิคที่เรียกว่า Local File Disclosure ในการหาช่องโหว่ โดยการใช้โปรแกรม Curl ผ่าน Command Prompt ดังแสดงตามภาพที่ 9



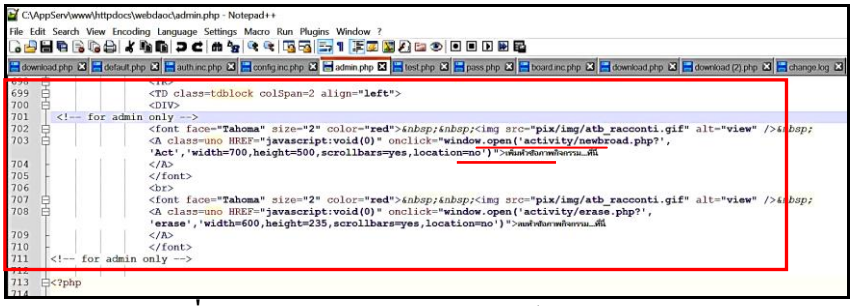
ภาพที่ 9 คำสั่งดาวน์โหลดไฟล์ download.php

จากคำสั่งดังกล่าวพบว่าสามารถดาวน์โหลดไฟล์ download.php ออกมาจากเครื่องเซิร์ฟเวอร์ได้สำเร็จ จากนั้นทำการอ่านซอร์สโค้ดของไฟล์ download.php พบว่าไม่มีการตรวจสอบนามสกุลของไฟล์ก่อนที่จะอนุญาตให้ดาวน์โหลด ส่งผลให้สามารถดาวน์ไฟล์ ใด ๆ ก็ได้ที่อยู่บนเซิร์ฟเวอร์เพียงแค่รู้ที่อยู่ของไฟล์ที่ต้องการดาวน์โหลดเท่านั้น รายละเอียดตามภาพที่ 10



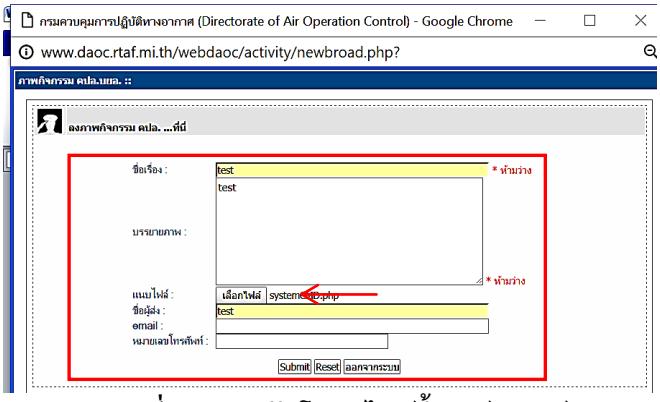
ภาพที่ 10 อ่านซอร์สโค้ดไฟล์ download.php

จากนั้นจึงทดลองดาวน์โหลดไฟล์ admin.php ซึ่งเป็นไฟล์ที่ผู้วิจัยสันนิษฐานว่าน่าจะเป็นไฟล์ที่มีอยู่ในเซิร์ฟเวอร์และเป็นไฟล์ที่คาดว่าจะสามารถนำไปใช้ประโยชน์ได้ พบว่าไฟล์มีการอ้างอิงถึงไฟล์ที่สามารถเข้าไปเพิ่มข้อมูลในเว็บไซต์ได้ คือไฟล์ที่ชื่อว่า newbroad.php และภายในไฟล์ admin.php มีการเขียนคอมเมนต์บอกให้รู้ว่าไฟล์นี้มีความสำคัญกับ admin ตามภาพที่ 11

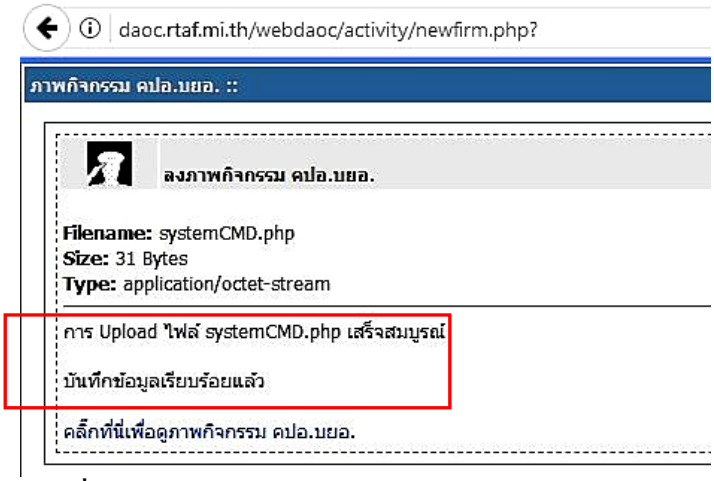


ภาพที่ 11 รายละเอียดข้อมูลภายในไฟล์ admin.php

จากนั้นจึงเรียกไฟล์ newbroad.php ผ่านเว็บบราวซ์เซอร์ เพื่อทดสอบการเข้าถึงหน้าเพจ newbroad.php ซึ่งเป็นหน้าที่ใช้ในการอัพโหลดข้อมูลขึ้นสู่หน้าเว็บไวต์ พบว่าสามารถเข้าถึงช่องทางการอัพโหลดข้อมูลขึ้นบนเว็บไซต์ได้โดยไม่ผ่านการยืนยันตัวตน ดังแสดงตามภาพที่ 12- 13



ภาพที่ 12 การอัพโหลดไฟล์ขึ้นเซิร์ฟเวอร์



ภาพที่ 13 การอัพโหลดไฟล์ system.CMD.php เสร็จสมบูรณ์

จากผลการทดสอบการเจาะระบบเว็บไซต์ พบว่าสามารถนำช่องโหว่ที่ตรวจพบจากขั้นตอนการสแกนหาช่องโหว่ของเว็บไซต์มาใช้ประโยชน์ในการทดสอบเจาะระบบเว็บไซต์ได้

3.2.4 การวิเคราะห์ความรุนแรงของช่องโหว่และการประเมินความเสี่ยง (Vulnerability and Risk Analysis)

ตารางที่ 4 การวิเคราะห์ความรุนแรงของช่องโหว่ที่ตรวจพบ

1. ชื่อช่องโหว่ : File upload	
รายละเอียด	เป็นช่องโหว่ที่สามารถอัพโหลดไฟล์ใด ๆ เข้าไปในระบบโดยไม่ผ่านการตรวจสอบชนิดของไฟล์
ความยากต่อการเข้าถึง	ช่องโหว่สามารถเข้าถึงจากเทคนิคทั่วไป โดยไม่ต้องยืนยันตัวตน ให้คะแนนระดับ 3
ผลกระทบ	ช่องโหว่สามารถขัดขวาง หรือยุติการให้บริการ หรือทำให้ข้อมูลเสียหายได้ ให้คะแนนระดับ 3
ความเสี่ยง	ความเสี่ยงระดับสูง ให้คะแนนระดับ 9
2. ชื่อช่องโหว่ : Local File Disclosure	
รายละเอียด	เป็นช่องโหว่ที่อนุญาตให้ดาวน์โหลดไฟล์ต่าง ๆ ออกจากเซิร์ฟเวอร์โดยไม่มีการตรวจสอบชนิดของไฟล์
ความยากต่อการเข้าถึง	ช่องโหว่สามารถเข้าถึงจากเทคนิคทั่วไป โดยไม่ต้องยืนยันตัวตน ให้คะแนนระดับ 3
ผลกระทบ	ช่องโหว่ไม่สามารถยุติการให้บริการได้ แต่ทำให้ได้ข้อมูลพื้นฐานเกี่ยวกับการให้บริการ ให้คะแนนระดับ 1
ความเสี่ยง	ความเสี่ยงระดับต่ำ ให้คะแนนระดับ 3
3. ชื่อช่องโหว่ : Cross Site Request Forgery	
รายละเอียด	เป็นช่องโหว่ที่สามารถส่ง โค้ดไม่พึงประสงค์ขึ้นไปบนเซิร์ฟเวอร์ได้ แต่เว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศ ไม่มีบริการที่มีช่องโหว่ดังกล่าว
ความยากต่อการเข้าถึง	ช่องโหว่ต้องอาศัยการโจมตีผ่านเทคนิคเฉพาะและการยืนยันตัวตน ให้คะแนนระดับ 1
ผลกระทบ	ช่องโหว่ไม่สามารถยุติการให้บริการได้ แต่ทำให้ได้ข้อมูลพื้นฐานเกี่ยวกับการให้บริการ ให้คะแนนระดับ 1
ความเสี่ยง	ความเสี่ยงระดับต่ำ ให้คะแนนระดับ 1

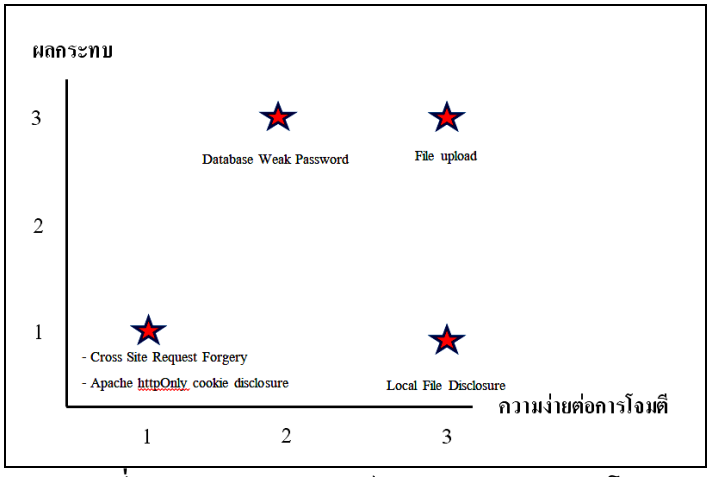
4. ชื่อช่องโหว่ : Apache httpOnly cookie disclosure	
รายละเอียด	เป็นช่องโหว่ที่แฮกเกอร์สามารถขโมย Cookie ได้ แต่เว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศ ไม่มีบริการที่ต้องใช้ Cookie
ความง่ายต่อการเข้าถึง	ช่องโหว่ต้องอาศัยการโจมตีผ่านเทคนิคเฉพาะ และการยืนยันตัวตน ให้คะแนนระดับ 1
ผลกระทบ	ช่องโหว่ไม่สามารถยุติการให้บริการได้ แต่ทำให้ได้ข้อมูลพื้นฐานเกี่ยวกับการให้บริการ ให้คะแนนระดับ 1
ความเสี่ยง	ความเสี่ยงระดับต่ำ ให้คะแนนระดับ 1
5. ชื่อช่องโหว่ : Database Weak Password	
รายละเอียด	รหัสผ่านของฐานข้อมูลมีความแข็งแรงน้อย
ความง่ายต่อการเข้าถึง	ช่องโหว่สามารถเข้าถึงจากเทคนิคทั่วไป โดยต้องผ่านการยืนยันตัวตน ให้คะแนนระดับ 2
ผลกระทบ	เป็นช่องโหว่ที่สามารถขัดขวาง หรือยุติการให้บริการ หรือทำให้ข้อมูลเสียหายได้ ให้คะแนนระดับ 3
ความเสี่ยง	ระดับปานกลาง ให้คะแนนระดับ 6

โดยสามารถสรุปข้อมูลของช่องโหว่ที่ตรวจพบได้ดังตารางที่ 5

ตารางที่ 5 จำนวนของช่องโหว่ที่ตรวจพบและระดับความเสี่ยง

ระดับความเสี่ยง	สูง	กลาง	ต่ำ
จำนวนช่องโหว่	1	1	3

จากข้อมูลในตารางที่ 4 แสดงเป็นแผนภูมิได้ตามภาพที่ 14



ภาพที่ 14 ผลการวิเคราะห์ความรุนแรงของช่องโหว่

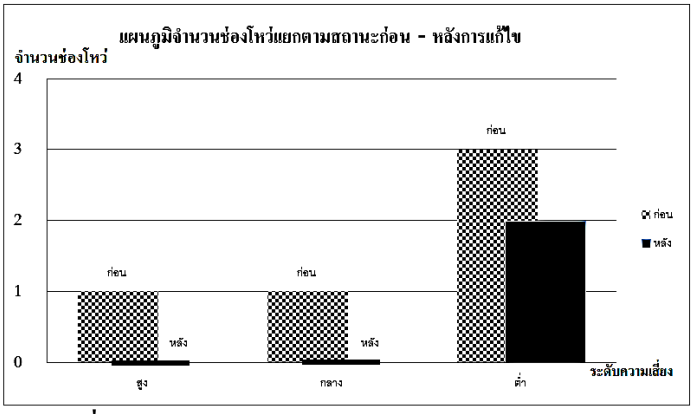
3.3 รายงานวิธีการแก้ไขและการป้องกันช่องโหว่ (Report how to fix and prevent vulnerabilities)

จากผลการศึกษาในหัวข้อที่ 3.2 ผู้วิจัยได้ค้นพบแนวทางการป้องกันและแก้ไขช่องโหว่ที่ตรวจพบโดยได้จัดทำเป็นรายงานให้กับผู้เกี่ยวข้องได้นำไปแก้ไข โดยมีรายละเอียดดังนี้

ตารางที่ 6 การทำรายงานวิธีการแก้ไขและการป้องกันช่องโหว่

ลำดับ	ช่องโหว่	ระดับความเสี่ยง	วิธีแก้ไขและแนวทางการป้องกัน
1	File upload	สูง	1A : เพิ่มหน้ายืนยันตัวตนสำหรับผู้ดูแลระบบก่อนเข้าไปจัดการกิจกรรมต่างๆบนหน้าเว็บไซต์ 1B : เพิ่มการตรวจสอบไฟล์ที่จะอัพโหลดให้อัพโหลดได้เฉพาะไฟล์ที่ต้องการให้อัพโหลดเท่านั้น เช่นไฟล์ รูปภาพ (.jpeg, .gif, .png) เท่านั้น
2	Local File Disclosure	ต่ำ	2A: ยกเลิกการใช้ไฟล์ download.php ซึ่งเป็นไฟล์ที่อนุญาตให้ผู้ใช้สามารถดาวน์โหลดไฟล์ต่างๆที่อยู่บนเว็บเซิร์ฟเวอร์ได้จากหน้าเว็บไซต์ 2B : ตั้งค่าการดาวน์โหลดไฟล์ ให้เป็นแบบ static คือ ในขั้นตอนเขียนโค้ดให้อ้างอิงไฟล์ที่ต้องการให้ดาวน์โหลดโดยตรง โดยไม่ต้องผ่านซอสโค้ดของไฟล์ download.php
3	Cross Site Request Forgery	ต่ำ	แก้ไขด้วยวิธีการ อัพเดทเวอร์ชั่นของเว็บเซิร์ฟเวอร์ จาก Apache เวอร์ชั่น 2.2.8 ซึ่งเป็นเวอร์ชั่นที่เก่า ให้เป็น Apache เวอร์ชั่น 2.2.22 ขึ้นไปซึ่งเป็นเวอร์ชั่นที่ได้รับการแก้ไขช่องโหว่ดังกล่าวเรียบร้อยแล้ว
4	Apache httpOnly cookie disclosure	ต่ำ	แก้ไขด้วยวิธีการ อัพเดทเวอร์ชั่นของเว็บเซิร์ฟเวอร์ จาก Apache เวอร์ชั่น 2.2.8 ซึ่งเป็นเวอร์ชั่นที่เก่า ให้เป็น Apache เวอร์ชั่น 2.2.22 ขึ้นไปซึ่งเป็นเวอร์ชั่นที่ได้รับการแก้ไขช่องโหว่ดังกล่าวเรียบร้อยแล้ว
5	Database Weak Password	ปานกลาง	เปลี่ยนรหัสผ่านของฐานข้อมูลให้มีความแข็งแรงดังนี้ 1. รหัสผ่านควรจะประกอบด้วย อักขรพิมพ์ใหญ่, พิมพ์เล็ก, ตัวเลข และอักขระพิเศษ 2. รหัสผ่านยากต่อการคาดเดา (Brute force) 3. ความยาวของรหัสผ่านไม่น้อยกว่า 8 ตัวอักษร 4. ไม่ใช้ข้อมูลที่เป็นส่วนตัวหรือข้อมูลที่เป็นสาธารณะ เช่น หมายเลขบัตรประชาชน หมายเลขโทรศัพท์ วัน เดือน ปีเกิด ทะเบียนรถ เป็นต้น 5. ใช้รหัสผ่านแยกกับบริการอื่น เช่น บัญชีอีเมล์ หรือบริการอื่น ๆ 6. จำกัดสิทธิ์การเข้าถึงฐานข้อมูลโดยอนุญาตให้เข้าถึงได้เฉพาะเว็บเซิร์ฟเวอร์ของกรมควบคุมการปฏิบัติทางอากาศเท่านั้น

จากผลการแก้ไขช่องโหว่ข้างต้น สามารถแก้ไขช่องโหว่ที่ตรวจพบได้แล้วจำนวนทั้งสิ้น 3 ช่องโหว่ และมีจำนวน2 ช่องโหว่ ที่อยู่ระหว่างการดำเนินการแก้ไขจากผู้ดูแลระบบเว็บเซิร์ฟเวอร์ของกองทัพอากาศ ข้อมูลดังกล่าวสามารถสรุปได้ดังแสดงตามภาพที่ 15



ภาพที่ 15 จำนวนช่องโหว่ของเว็บไซต์ก่อนและหลังจากได้รับการแก้ไข

4. บทสรุปและข้อเสนอแนะ

ผู้วิจัยสามารถเข้าใจถึงวิธีการหาช่องโหว่ของเว็บไซต์และวิธีการโจมตีโดยการใช้ประโยชน์จากช่องโหว่ของเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศและสามารถหาแนวทางในการป้องกันไม่ได้เกิดช่องโหว่ได้ จึงทำให้เว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศ มีความมั่นคงปลอดภัยมากขึ้น

5. แนวทางการพัฒนาต่อในอนาคต

5.1 ตรวจหาช่องโหว่ของเว็บไซต์ทั้งหมดที่อยู่ในเครื่องเซิร์ฟเวอร์เพื่อเป็นการป้องกันทั้งโดเมน

5.2 ตรวจหาช่องโหว่ของเว็บเซิร์ฟเวอร์โดยใช้วิธีการทดสอบเจาะระบบ (Penetration Testing) และพยายามค้นหาช่องโหว่ใหม่ๆ ทุกวิถีทางที่จะก่อให้เกิดภัยอันตรายต่อเว็บเซิร์ฟเวอร์

5.3 ใช้โปรแกรมสแกนช่องโหว่ที่ทันสมัย อย่างน้อย 3 โปรแกรมในการหาช่องโหว่ของเว็บไซต์และเว็บเซิร์ฟเวอร์

บรรณานุกรม

กองนโยบายและแผน กรมเทคโนโลยีสารสนเทศและการสื่อสารกองทัพอากาศ 2559 : ออนไลน์

กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

จตุชัย แพงจันทร์, Master in Security 2nd Edition,2553

ธวัชชัย ชมศิริ, ความปลอดภัยของเว็บ, 2017

พรพรหม ประภากิตติกุล , รู้จักและป้องกันภัยจาก Website Defacement,2554

พลตรี ฤทธี อินทราวุธ,ม.ป.ป.,น. 2

ระเบียบกองทัพอากาศ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ พ.ศ. 2552 : ออนไลน์

สุเมธ จิตภักดีบดินทร์, NETWORK SECURITY, 2556,น.34-36

อานัฐชัย รังสิโรดม์โกมล , เครื่องมือทดสอบการเจาะระบบ Tool for Penetration test,2558

“Acunetix” [ออนไลน์]: เข้าถึง 24 ก.ย. 2016 จาก : https://www.acunetix.com

2003 – 2013 The OWASP Foundation, [online]. Available:

OWASP Risk Rating Methodology จาก : https://www.owasp.org/index.php/OWASP_Risk Rating_Methodology

The OWASP Foundation: OWASP Top 10 – 2013. (2013), [online]. Available: http://owasptop10.googlecode.com/files/OWASPTop10-2013.pdf /