การประเมินค่าช่องโหว่ของเว็บไซต์และการป้องกัน
กรณีศึกษา เว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ

เรืออากาศตรีหญิง ณัชณภัทร ใจอดทน

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์และโทรคมนาคม
วิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรมศาสตร์
มหาวิทยาลัยธุรกิจบัณฑิตย์
พ.ศ. 2560

Website Vulnerability Assessment and Defense :

A Case study of Directorate of Air Operations Control

Pilot Officer. NACHNAPHAT JAI-ODTON

A Thematic Paper Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Engineering

Department of Computer and Telecommunication Engineering

College of Innovative Technology And Engineering,

Dhurakij Pundit University

2017

หัวข้อสารนิพนธ์ การประเมินค่าช่องโหว่ของเว็บไซต์และการป้องกัน
กรณีศึกษา เว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ
ชื่อผู้เขียน ร.ต.หญิง ณัชณภัทร ใจอดทน
อาจารย์ที่ปรึกษา ดร.ชัยพร เขมะภาตะพันธ์
สาขาวิชา วิศวกรรมคอมพิวเตอร์และโทรคมนาคม
ปีการศึกษา 2559

บทคัดย่อ

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

(1) การวางแผนและเตรียมการ (Planning and Preparation)

(2) การประเมินค่าของช่องโหว่ (Vulnerability Assessment)

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

ผลลัพธ์จากการศึกษาค้นคว้าแสดงให้เห็นว่าผู้วิจัยสามารถตรวจพบช่องโหว่ของเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ รวมทั้งสิ้นจำนวน 5 ช่องโหว่ ซึ่งเป็นช่องโหว่ที่มีความรุนแรงระดับสูง 1 ช่องโหว่ ช่องโหว่ที่มีความรุนแรงระดับปานกลาง 1 ช่องโหว่ และช่องโหว่ที่มีความรุนแรงระดับต่ำ 3ช่องโหว่ โดยช่องโหว่ที่มีความรุนแรงระดับสูง แฮกเกอร์สามารถนำไปใช้ประโยชน์ในการโจมตีเว็บไซต์ดังกล่าวและเว็บไซต์อื่น ๆ ที่อยู่ภายใต้โดเมนเนม “daoc.rtaf.mi.th”

Subject	Website Vulnerability Assessment and Defense: A Case study of Directorate of Air Operations Control
Student Name	Plt. Off. NACHNAPHAT JAI-ODTON
Advisor	CHAIYAPORN KHEMAPATAPAN
Course	Computer and Telecommunication Engineering
Year	2016

Abstract

This independent studies about weakness or vulnerability of the website of Directorate of Air Operations Control,"www.daoc.rtaf.mi.th". The independent study shows the impact level of vulnerability on the website. Acunetix Web Vulnerability Scanner is used as a tool for vulnerability assessment. However, Local File Disclosure technique is applied for testing the website vulnerability. The studying process is divided into 3 steps as following

1. Planning and preparation
2. Vulnerability assessment
3. Report how to fix and prevent vulnerabilities

The studied results show that the researcher found 5 total vulnerabilities: 1 high risk, 1 medium risk and 3 low risks. Consequently, the hacker can deploy the high risk vulnerability to attack all websites under the domain name "daoc.rtaf.mi.th".

กิตติกรรมประกาศ

ขอขอบคุณอาจารย์ ดร.ชัยพร เขมะภาตะพันธ์ ที่ได้เสนอแนะแนวทางในการดำเนินการวิจัย รวบรวม แก้ไข และตรวจสอบในระหว่างการจัด ทำรวมทั้งขอขอบคุณคณาจารย์ทุกท่านในหลักสูตรวิศวกรรมศาสตร์มหาบัณฑิตย์ ที่ได้ให้ความช่วยเหลือในการให้คำปรึกษาต่างๆ อีกทั้งเพื่อนๆ รุ่นพี่คอยช่วยเหลือสนับสนุนและให้ข้อมูลในการจัดทำสารนิพนธ์

สุดท้ายนี้ข้าพเจ้าขอกราบขอบพระคุณบิดา มารดา และอาจารย์ทุกท่านที่ได้ให้การสนับสนุนในการทำวิจัยครั้งนี้ และบุคคลที่มิได้กล่าวถึง ขอขอบคุณที่คอยให้ความช่วยเหลือและให้กำลังใจเสมอมา

ณัชณภัทร ใจอดทน

สารบัญ

หน้า

บทคัดย่อภาษาไทย ..... ฆ
บทคัดย่อภาษาอังกฤษ ..... ง
กิตติกรรมประกาศ ..... จ
สารบัญตาราง ..... ซ
สารบัญภาพ ..... ฌ
บทที่
1 บทนำ 1
1.1 หลักการและเหตุผล 1
1.2 วัตถุประสงค์ของการวิจัย 3
1.3 สมมติฐานการวิจัย 3
1.4 ขอบเขตการวิจัย 3
1.5 ประโยชน์ที่คาดว่าจะได้รับ 4
2 แนวคิดทฤษฎีที่เกี่ยวข้อง 5
2.1 หลักการทดสอบเจาะระบบของผู้ทดสอบ 6
2.2 การวิเคราะห์ความรุนแรงของช่องโหว่และการประเมินความเสี่ยง 8
2.3 เครื่องมือสำหรับตรวจหาช่องโหว่ 10
2.4 Open Web Application Security 14
2.5 ข้อมูลของช่องโหว่ที่เกี่ยวข้อง 16
2.6 ตัวอย่างของเว็บไซต์ที่มีช่องโหว่และเคยผ่านการถูกโจมตี 17
3 การดำเนินการตรวจหาช่องโหว่ของเว็บไซต์ 20
3.1 การวางแผนและเตรียมการ 21
3.2 การประเมินค่าของช่องโหว่ 21
3.3 การวิเคราะห์ความรุนแรงของช่องโหว่และการประเมินความเสี่ยง 38
4 ผลลัพธ์จากการดำเนินการ 42
4.1 รายงานวิธีการแก้ไขช่องโหว่และแนวทางการป้องกัน 42
4.2 การแก้ไขช่องโหว่ 44
4.3 ผลลัพธ์ที่ได้จากการแก้ไขช่องโหว่ของเว็บไซต์ 50

สารบัญ (ต่อ)

บทที่ หน้า

5 บทสรุปและข้อเสนอแนะ 52

5.1 สรุปผลการวิจัย 52

5.2 แนวทางการพัฒนาต่อในอนาคต 52

บรรณานุกรม 54

ภาคผนวก 56

ประวัติผู้เขียน 58

สารบัญตาราง

ตารางที่		หน้า
2.1	การวิเคราะห์ความยากต่อการเข้าถึงช่องโหว่	9
2.2	การวิเคราะห์ผลกระทบที่จะเกิดขึ้นต่อระบบ	9
2.3	การประเมินความเสี่ยง	10
3.1	การวิเคราะห์ความรุนแรงของช่องโหว่ที่ตรวจพบ	39
3.2	จำนวนของช่องโหว่ที่ตรวจพบและระดับความเสี่ยง	41
4.1	รายงานวิธีการแก้ไขช่องโหว่และแนวทางการป้องกัน	42

สารบัญภาพ

ภาพที่		หน้า
2.1	ขั้นตอนการดำเนินการตรวจหาช่องโหว่ของเว็บไซต์	7
2.2	การเลือก target ที่จะสแกน	11
2.3	การระบุรายละเอียดที่จะสแกน	12
2.4	การยืนยันการเลือกตัวที่จะสแกนเพื่อหา Targets	12
2.5	ขั้นตอนหลังจากที่เลือกสิ่งที่จะสแกนเสร็จ	13
2.6	การวิเคราะห์การผลการสแกน	14
2.7	เว็บไซต์ของกองทัพอากาศที่เคยถูกโจมตี	18
2.8	เว็บไซต์ภายใต้โดเมน .rtaf.mi.th ที่เคยถูกโจมตี	18
2.9	เว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศเคยถูกโจมตี	19
3.1	ขั้นตอนในการดำเนินการตรวจหาช่องโหว่ของเว็บไซต์	20
3.2	ขั้นตอนการวางแผนและเตรียมการ	21
3.3	ขั้นตอนการตรวจหาช่องโหว่ของเว็บไซต์	22
3.4	ผลลัพธ์ของการตรวจสอบข้อมูลของเว็บไซต์ด้วยคำสั่ง nslookup	23
3.5	ผลลัพธ์การทำ Reverse IP Domain Check	24
3.6	โครงสร้างสภาพแวดล้อม	24
3.7	ข้อมูลของช่องโหว่ที่ตรวจพบ	25
3.8	ข้อมูลรายละเอียดของช่องโหว่ประเภท Apache httpOnly cookie disclosure	25
3.9	ข้อมูลรายละเอียดของช่องโหว่ HTML form without CSRF protection	26
3.10	ช่องโหว่ของ Local file inclusion	27
3.11	คำสั่งการเรียกใช้เครื่องมือ Curl	27
3.12	คำสั่งดาวน์โหลดไฟล์ download.php	28
3.13	อ่านซอร์สโค้ดไฟล์ download.php	28
3.14	คำสั่งดาวน์โหลดไฟล์ default.php	29
3.15	รายละเอียดของไฟล์ไฟล์ default.php	29
3.16	คำสั่งดาวน์โหลดไฟล์ auth.inc.php	30
3.17	รายละเอียดของข้อมูลที่อยู่ในไฟล์ auth.inc.php	30
3.18	คำสั่งดาวนโหลดไฟล์ config.inc.php	31

สารบัญภาพ

ภาพที่ **หน้า**

3.19 ข้อมูลรหัสผ่านสำหรับเข้าใช้งานระบบฐานข้อมูล 31
3.20 คำสั่งดาวน์โหลดไฟล์ admin.php 32
3.21 รายละเอียดข้อมูลภายในไฟล์ admin.php 32
3.22 คำสั่งดาวน์โหลดไฟล์ newbroad.php 33
3.23 รายละเอียดข้อมูลภายในไฟล์ newbroad.php 33
3.24 ช่องทางในการอัพโหลดไฟล์ขึ้นหน้าเว็บไซต์ 34
3.25 คำสั่งภายใน systemCMD.php 34
3.26 การอัพโหลดไฟล์ขึ้นเซิร์ฟเวอร์ 35
3.27 การอัพโหลดไฟล์ system.CMD.php เสร็จสมบูรณ์ 35
3.28 การอัพโหลดไฟล์ system.CMD.php เสร็จสมบูรณ์ 36
3.29 การอัพโหลดไฟล์ system.CMD.php เสร็จสมบูรณ์ 36
3.30 การเรียกใช้งานไฟล์ system.php ผ่านเว็บเบราว์เซอร์ 37
3.31 ข้อมูลของไฟล์ที่อยู่ในเครื่องเซิร์ฟเวอร์ 37
3.32 การตรวจสอบสิทธิ์การใช้งานบนเซิร์ฟเวอร์ด้วยคำสั่ง “whoami” 37
3.33 การตรวจสอบชื่อผู้มีสิทธิ์เข้าถึงเครื่องเซิร์ฟเวอร์ 38
3.34 แผนภูมิแสดงผลการวิเคราะห์ความรุนแรงของช่องโหว่ 41
4.1 ขั้นตอนการอัพโหลดข้อมูลขึ้นสู่เว็บแบบเดิม 44
4.2 ช่องทางการอัพโหลดข้อมูลขึ้นสู่เว็บด้วยแบบเดิม 45
4.3 ขั้นตอนการอัพโหลดข้อมูลขึ้นสู่เว็บแบบใหม่ 46
4.4 หน้าเพจการยืนยันตัวตนสำหรับผู้ดูแลเว็บไซต์ 46
4.5 การเพิ่มซอร์สโค้ดเพื่อตรวจสอบประเภทของไฟล์ที่อัพโหลด 47
4.6 การเข้าถึงหน้าเพจ “newbroad.php” 47
4.7 การอัพโหลดไฟล์ “systemCMD.php” 48
4.8 ผลลัพธ์ของการอัพโหลดไฟล์ “systemCMD.php” 48
4.9 การตั้งค่าการดาวน์โหลดไฟล์แบบ static 49
4.10 รายละเอียดของไฟล์ admin.php 50
4.11 แผนภูมิจำนวนช่องโหว่ของเว็บไซต์ก่อนและหลังจากได้รับการแก้ไข 51

บทที่ 1
บทนำ

1.1 หลักการและเหตุผล

ในระยะเวลาไม่กี่ปีผ่านมา [1] นับตั้งแต่อินเทอร์เน็ตและเทคโนโลยีในการสื่อสารได้รับการพัฒนาไปอย่างรวดเร็ว จนกระทั่งในปัจจุบันแทบไม่มีใครในโลกที่ไม่รู้จักอินเทอร์เน็ต ทำให้ประเทศต่าง ๆ สามารถพัฒนาศักยภาพทางด้านไซเบอร์ได้อย่างรวดเร็ว ซึ่งก่อให้เกิดภัยคุกคามต่าง ๆ หลากหลายรูปแบบ โดยเฉพาะอย่างยิ่ง การทำสงครามไซเบอร์ ได้มีการปรับเปลี่ยนรูปแบบจากเดิมที่เป็นการจารกรรมข้อมูล กลายเป็นการโจมตีเพื่อมุ่งเน้นทำลายล้างเป็นสำคัญ ซึ่งรูปแบบของการทำสงครามไซเบอร์นั้นมีวัตถุประสงค์และจุดมุ่งหมายเหมือนกับการทำสงครามในรูปแบบปกติทุกอย่าง เพียงแต่เทคนิคและยุทธวิธีนั้นแตกต่างออกไป ซึ่งการทำสงครามไซเบอร์นับได้ว่า เป็นทางเลือกที่ดี เพราะถือว่าเป็นสงครามที่ใช้ต้นทุนต่ำ แต่สามารถสร้างผลกระทบได้เป็นวงกว้าง และสร้างความเสียหายอย่างคาดไม่ถึง

จากสถานการณ์ไซเบอร์ในปัจจุบัน [2] ประเทศไทยโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้ตั้งศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Operation Center : CSOC) เมื่อปี 2553 โดยมุ่งเน้นการดำเนินการติดตาม เฝ้าระวัง ตรวจสอบ วิเคราะห์เว็บไซต์ และข้อมูลอินเทอร์เน็ตที่ไม่เหมาะสม หรือผิดกฎหมายต่าง ๆ โดยเฉพาะเว็บหมิ่นสถาบัน ต่อมาในปี ๒๕๕๖ รัฐบาลปัจจุบันได้ตระหนักถึง ภัยคุกคามด้านไซเบอร์ ถึงแม้ว่าประเทศไทยจะมีมาตรการทางกฎหมาย และมีหน่วยงานของรัฐกำกับดูแลภัยคุกคามด้านนี้มาแล้วหลายปี แต่แนวโน้มความรุนแรงและการขยายตัวของภัยคุกคามยังมีความต่อเนื่อง แพร่หลายไปกระทบความเชื่อมั่นด้านความมั่นคงของประเทศในด้านต่าง ๆ ดังนั้นรัฐบาลจึงได้แต่งตั้ง คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee : NCSC) ซึ่งมีนายกรัฐมนตรีฯ เป็นประธาน และหน่วยงานที่เกี่ยวข้องด้านความมั่นคง กระบวนการยุติธรรมและด้านเศรษฐกิจ ร่วมเป็นกรรมการ โดยมีเจ้ากรมเทคโนโลยีสารสนเทศและกิจการอวกาศกลาโหมเป็นเลขานุการฯ โดยมีหน้าที่หลักในการจัดทำนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้ประเทศไทยมีขีดความสามารถในการปกป้อง ป้องกัน รับมือ และลดความเสี่ยงจาก

สถานการณ์ด้านภัยคุกคามในไซเบอร์ ที่กระทบต่อความมั่นคงของชาติ ทั้งจากภายในและภายนอกประเทศ ครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ ตลอดจนติดตามและประเมินผลการปฏิบัติที่เกี่ยวข้องเพื่อให้เกิดการบูรณาการการทำงานของหน่วยงานต่างๆ ที่เกี่ยวข้อง อันจะก่อให้เกิดประสิทธิภาพและประสิทธิผลในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ สอดคล้องกับแนวทางการจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของประชาคมอาเซียน

หากกล่าวถึงระบบสารสนเทศของกองทัพอากาศ จะเห็นได้ว่ามีแนวทางในเรื่องการรักษาความปลอดภัยของระบบสารสนเทศเป็นลายลักษณ์อักษร ตั้งแต่ปี พ.ศ. 2552 คือระเบียบกองทัพอากาศ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ [3] โดยระเบียบนี้มีความมุ่งหมายเพื่อกำหนดหลักการและมาตรการป้องกันภัยของระบบสารสนเทศของกองทัพอากาศ พิทักษ์รักษา และป้องกันสารสนเทศที่กำหนดชั้นความลับมิให้รั่วไหล หรือรู้ไปถึง หรือตกไปอยู่กับบุคคลผู้ไม่มีอำนาจหน้าที่ที่จะต้องรับทราบ พิทักษ์รักษาและป้องกันการก่อวินาศกรรมแก่ระบบสารสนเทศของกองทัพอากาศ ในส่วนของระบบคอมพิวเตอร์และระบบสื่อสารข้อมูล เพื่อให้การดำเนินการตามระเบียบกองทัพอากาศ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ พ.ศ. 2552 เป็นไปอย่างมีประสิทธิภาพ เป็นรูปธรรมและสอดคล้องกับภัยคุกคามรูปแบบใหม่ที่กำลังเผชิญอยู่ในปัจจุบัน นอกจากนั้นกองทัพอากาศยังให้ความสำคัญกับการเผยแพร่ข้อมูลต่าง ๆ ผ่านทางเว็บไซต์ เพื่อให้ประชาชนหรือผู้สนใจสามารถเข้าใช้บริการได้ ทำให้เกิดความเสี่ยงที่จะได้รับความเสียหายจากผู้ไม่ประสงค์ดี (แฮกเกอร์) ได้ง่าย เนื่องจากแฮกเกอร์สามารถมองเห็นช่องโหว่หรือจุดอ่อนของเว็บไซต์ผ่านทางพอร์ต (Port) ที่จำเป็นต้องเปิดใช้งานผ่านทางเว็บเซิร์ฟเวอร์ (Web server) และเว็บแอพพลิเคชั่น (Web application) ในปัจจุบัน แฮกเกอร์จึงนิยมใช้วิธีการที่เรียกว่า เว็บแอพพลิเคชั่นแฮกกิ้ง (Web application hacking) ในการเจาะเข้าสู่ระบบ นอกจากนี้ การให้บริการเว็บไซต์ยังต้องเผชิญกับภัยคุกคามในรูปแบบต่าง ๆ ซึ่งส่วนหนึ่งมาจากการที่ผู้พัฒนาเว็บไซต์ มักไม่ให้ความสำคัญกับความปลอดภัยของระบบ และการหาแนวทางป้องกันที่มีประสิทธิภาพเป็นไปได้ยาก จึงมีความจำเป็นอย่างยิ่งที่ต้องหาวิธีป้องกันเว็บไซต์จากการถูกโจมตี เนื่องจากหากมีการโจมตีในระบบของหน่วยงานใดก็ตาม ที่ขึ้นตรงต่อกองทัพอากาศ จะสามารถก่อให้เกิดความเสียหายต่อระบบสารสนเทศอื่น ๆ ภายในกองทัพอากาศได้ เนื่องจากระบบสารสนเทศในกองทัพอากาศเป็นระบบสารสนเทศแบบเครือข่ายที่มีการเชื่อมโยงกันทั้งระบบ

กรมควบคุมการปฏิบัติทางอากาศ เป็นหน่วยงานขึ้นตรงต่อกองทัพอากาศหน่วยงานหนึ่ง ที่มีการเผยแพร่ข้อมูลต่าง ๆ เกี่ยวกับการใช้กำลังทางอากาศผ่านทางเว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศ เพื่อให้บริการแก่กำลังพลของกองทัพอากาศและบุคคลทั่วไปให้สามารถเข้าใช้บริการสืบค้นข้อมูลและดาวน์โหลดข้อมูล จึงมีความเสี่ยงต่อการถูกโจมตีจากผู้ไม่ประสงค์ดี

ด้วยเหตุนี้ จึงมีความจำเป็นที่ต้องมีการศึกษา ค้นคว้าเพื่อหาช่องโหว่หรือจุดอ่อนของเว็บไซต์ว่ามีช่องโหว่หรือจุดอ่อนหรือไม่ แล้วช่องโหว่หรือจุดอ่อนนั้นมีระดับความรุนแรงและมีผลกระทบต่อเว็บไซต์อย่างไร เพื่อหาแนวทางการป้องกันการถูกโจมตีจากการใช้ประโยชน์จากช่องโหว่หรือจุดอ่อนของเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศเพื่อใช้เป็นแนวทางในการพัฒนาเว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศให้มีความมั่นคง ปลอดภัย

1.2 วัตถุประสงค์ของการวิจัย

1.2.1. เพื่อศึกษาถึงการโจมตีโดยการใช้ประโยชน์จากช่องโหว่หรือจุดอ่อนของเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ

1.2.2 เพื่อกำหนดวิธีในการแก้ไขและหาแนวทางป้องกันช่องโหว่หรือจุดอ่อนของเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ ให้มีความมั่นคง ปลอดภัย

1.3 สมมติฐานการวิจัย

เพื่อเป็นแนวทางในการวิจัย ผู้วิจัยได้ตั้งสมมติฐานของการวิจัยดังนี้

1.3.1. สามารถตรวจพบช่องโหว่หรือจุดอ่อนของเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศด้วยวิธีการใช้เครื่องมือสำเร็จรูปในการตรวจหาช่องโหว่และการทดสอบเจาะระบบโดยผู้ทำการวิจัย

1.3.2 สามารถประเมินความรุนแรงของช่องโหว่หรือจุดอ่อนที่พบ ว่ามีระดับความรุนแรงมากน้อยเพียงใด เพื่อนำมาใช้เป็นแนวทางในการแก้ไขช่องโหว่หรือจุดอ่อนของเว็บไซต์

1.4 ขอบเขตการวิจัย

ผู้วิจัยได้กำหนดขอบเขตของการวิจัยไว้ดังนี้

1.4.1 ศึกษาช่องโหว่หรือจุดอ่อนของเว็บไซต์โดยใช้เครื่องมือ Acunetix Web Vulnerability Scanner เป็นเครื่องมือในการตรวจหาช่องโหว่หรือจุดอ่อนของเว็บไซต์

1.4.2 ศึกษาช่องโหว่หรือจุดอ่อนของเว็บไซต์โดยวิธีทดสอบเจาะระบบโดยผู้ทำการวิจัย

1.4.3 ศึกษาแนวทางในการป้องกันการเข้าถึงช่องโหว่หรือจุดอ่อนของเว็บไซต์ ในกรณีที่มีแนวทางป้องกันมากกว่า 1 แนวทางสารนิพนธ์ฉบับนี้จะเลือกแนวทางที่เหมาะสมที่สุดโดยให้เหตุผลทางเทคนิคประกอบ

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1. สามารถเข้าใจถึงวิธีการโจมตีโดยการใช้ประโยชน์จากช่องโหว่หรือจุดอ่อนในเว็บไซต์ของเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ

1.5.2 ทราบถึงวิธีในการแก้ไขและหาแนวทางป้องกันช่องโหว่หรือจุดอ่อนของเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ เพื่อให้เว็บไซต์มีความมั่นคงปลอดภัยมากขึ้น

บทที่ 2
แนวคิดและทฤษฎีที่เกี่ยวข้อง

กล่าวนำ

ปัญหาด้านความปลอดภัยของข้อมูล (Information Security) [4] ได้เข้ามามีบทบาทที่สำคัญและสร้างความเสียหายให้กับงานระบบสารสนเทศขององค์กร ทั้งนี้ทำให้องค์กรต่าง ๆ หันมาให้ความสนใจในเรื่องของการบริหารความเสี่ยงระบบสารสนเทศ (IT Risk Management) โดยใช้วิธีการตรวจสอบหลายประเภทแตกต่างกัน ซึ่งในงานวิจัยนี้ผู้วิจัยได้เลือกใช้การตรวจสอบประเภทการประเมินช่องโหว่ของเว็บไซต์และการป้องกัน (Website Vulnerability Assessment and Defense) ซึ่งเป็นมาตรฐานที่ยอมรับในระดับสากล

เว็บไซต์ถูกใช้เป็นเครื่องมือที่สำคัญของหน่วยงานต่างๆในการสื่อสาร ประชาสัมพันธ์ หรือให้บริการออนไลน์ต่าง ๆ กับผู้ใช้งานผ่านเครือข่ายอินเทอร์เน็ตสาธารณะ ด้วยลักษณะของบริการเว็บไซต์ที่เปิดให้ผู้ใช้งานสามารถเข้าถึงได้อยู่ตลอดเวลา ทำให้บริการเว็บไซต์ที่ไม่มีการรักษาความมั่นคงปลอดภัยที่ดี มีความเสี่ยงจากการถูกโจมตีจากผู้ไม่ประสงค์ดี (แฮกเกอร์) ได้อยู่ตลอดเวลาเช่นกัน โดยภัยคุกคามรูปแบบหนึ่งที่มักจะเกิดขึ้นกับบริการเว็บไซต์ คือการโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลเผยแพร่หน้าเว็บ (Website Defacement) ซึ่งผู้โจมตีมีวัตถุประสงค์เพื่อปรับเปลี่ยนหน้าเว็บไซต์หน้าแรกของเว็บไซต์เป้าหมาย หรือทั้งเว็บไซต์ จากเดิมไปเป็นหน้าเว็บไซต์ใหม่ เพื่อต้องการทำลายความน่าเชื่อถือของหน่วยงานเจ้าของเว็บไซต์ ซึ่งในเว็บไซต์ที่ถูกโจมตีส่วนใหญ่จะปรากฏรูปภาพหรือข้อความที่บ่งบอกถึงว่าเว็บไซต์ได้ถูกโจมตีได้สำเร็จ

โดยรูปแบบของการโจมตีในลักษณะ Website Defacement เป็นการโจมตีที่นิยมมากที่สุดในหมู่ผู้โจมตีหรือแฮกเกอร์เนื่องจากสามารถเข้าโจมตีได้ง่ายและการโจมตีมักได้ผลทางด้านการสูญเสียความน่าเชื่อถืออย่างรวดเร็ว รวมถึงสามารถต่อยอดในการโจมตีส่วนประกอบหรือบริการอื่นๆบนเครื่องแม่ข่ายนั้น ๆ ด้วย ยิ่งหากผู้พัฒนาหรือผู้ดูแลระบบไม่มีการปิดช่องโหว่ดังกล่าวแล้ว อาจทำให้ผู้โจมตีสามารถสร้างความเสียหายให้กับเว็บไซต์อื่น ๆ ที่อยู่บนเว็บเซิร์ฟเวอร์เดียวกันได้

ในบทนี้เป็นเรื่องเกี่ยวกับแนวคิดและทฤษฎีที่เกี่ยวข้อง ประกอบไปด้วยหัวข้อดังต่อไปนี้

2.1 หลักการทดสอบเจาะระบบของผู้ทดสอบ

2.2 การวิเคราะห์ช่องโหว่และการประเมินความเสี่ยง (Vulnerability and Risk Analysis)

2.3 เครื่องมือสำหรับตรวจหาช่องโหว่

2.4 Open Web Application Security Project (OWASP)

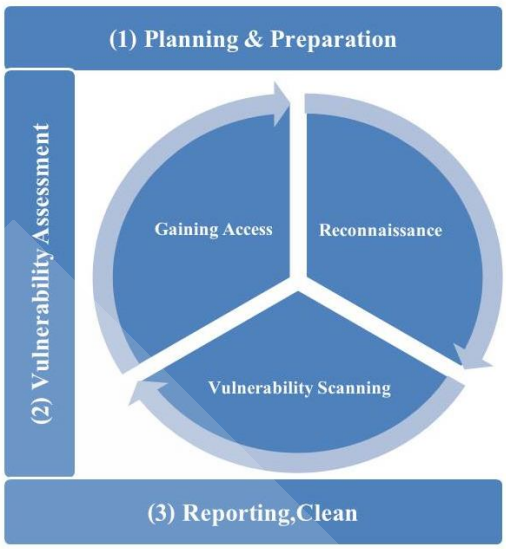
2.5 ข้อมูลของช่องโหว่ที่เกี่ยวข้อง

2.6 ตัวอย่างของเว็บไซต์ที่มีช่องโหว่และเคยถูกโจมตี

2.1 หลักการทดสอบเจาะระบบของผู้ทดสอบ [5]

การทดสอบเจาะระบบ Penetration Testing จะแตกต่างจาก Vulnerability Assessment คือทำมากกว่าหรือพิสูจน์ถึงภัยที่อาจเกิดขึ้น โดยจะทดลองทำการเสมือนจริง ไม่ว่าจะเป็นการเจาะระบบ (Exploitation), การยกระดับสิทธิ์ของ User หรือแม้กระทั่งสร้าง Backdoor ขึ้นมาภายในระบบเองก็ตาม แต่ Vulnerability Assessment จะเป็นเพียงการค้นหาตามขั้นตอนการทำงานที่ผิดพลาด หรือภัยต่างๆ ตามที่ปรากฏในปัจจุบัน ไม่สามารถทำการทดสอบการโจมตีที่เป็นพวก Dos ได้ ซึ่ง Penetration Testing จะพยายามค้นหาช่องโหว่ใหม่ๆ ทุกวิถีทางที่จะทำให้ระบบนั้นเป็นภัยอันตราย รวมถึงการทดสอบนั้นจะทำให้ระบบไม่สามารถให้บริการได้อีกด้วย

สารนิพนธ์ฉบับนี้ได้นำหลักการทดสอบเจาะระบบและการประเมินค่าของช่องโหว่มาประยุกต์ใช้ร่วมกัน เพื่อให้ทราบถึงวิธีการเจาะระบบของแฮกเกอร์ อย่างแท้จริง และวิธีการประเมินช่องโหว่ ว่าเว็บไซต์มีช่องโหว่หรือไม่ เพื่อนำผลลัพธ์ที่ได้จากการทดสอบมาหาแนวทางการป้องกันและแก้ไข ต่อไป โดยสารนิพนธ์นี้ได้ทำการตรวจหาช่องโหว่ของเว็บไซต์กรณีศึกษาเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ โดยมีขั้นตอนการดำเนินการดังแสดงในภาพที่ 3.1



ภาพที่ 2.1 ขั้นตอนการดำเนินการตรวจหาช่องโหว่ของเว็บไซต์

2.1.1 วางแผนและเตรียมการ (Planning and Preparation)

กำหนดขอบเขตของเป้าหมายในการหาช่องโหว่ของเว็บไซต์ เช่น หาช่องโหว่ของ Web Application ที่ให้บริการที่พอร์ต 80 เท่านั้น แต่จะไม่รวมถึงเครื่องที่ Web Application นั้นทำงานอยู่ หรือ Service ต่างๆ ที่ทำงานในพอร์ตอื่นๆ เป็นต้น

2.1.2 การประเมินช่องโหว่ (Vulnerability Assessment) [6]

เป็นขั้นตอนการทดสอบเพื่อทดสอบว่าเว็บไซต์มีความปลอดภัยมากน้อยเพียงใด ซึ่งในการทดสอบนั้นอาจจะเพื่อค้นหาข้อมูลสำคัญ เช่น ไฟล์ที่เก็บรหัสผ่าน ข้อมูลที่มีชั้นความลับสูง เป็นต้น การทดสอบเจาะเข้าระบบนั้นแบ่งออกเป็น 2 ประเภทคือ การทดสอบเจาะโดยมีข้อมูลที่เกี่ยวข้องกับระบบบ้าง และการเจาะระบบโดยเริ่มจากการไม่มีข้อมูลเกี่ยวกับระบบเลย ซึ่งการเจาะประเภทแรกนั้นมักจะทำโดยเริ่มจากเครือข่ายภายใน โดยสมมติว่าผู้ที่พยายามเจาะระบบนั้นเป็นพนักงานขององค์กรที่พอมีความรู้หรือข้อมูลเกี่ยวกับระบบหรือเครือข่ายขององค์กร ส่วนประเภทที่สองนั้นเป็นการทดสอบเจาะระบบจากภายนอก โดยสมมติว่าเป็นผู้ใช้ทั่วไปที่ไม่มีความรู้หรือข้อมูลเกี่ยวกับองค์กรมากนัก โดยสารนิพนธ์นี้เลือกใช้วิธีการทดสอบเจาะระบบโดยมีข้อมูลที่เกี่ยวข้องกับระบบบ้าง และนำข้อมูลที่ได้จากการทดสอบมาทำการวิเคราะห์ความรุนแรงของช่องโหว่และประเมินเมินความเสี่ยง เพื่อหาแนวทางการป้องกันและแก้ไข โดยขั้นตอนของการทดสอบเจาะระบบที่ผู้วิจัยนำมาใช้เป็นแนวทางในการทดสอบ มี 3 ขั้นตอน ดังนี้

2.1.2.1 การสำรวจข้อมูล (Reconnaissance) [5]

เป็นการค้นหาข้อมูลต่าง ๆ ของเป้าหมาย เช่นการตรวจสอบหมายเลข IP Address หรือรายชื่อ Service ที่เปิดใช้งานอยู่ การสำรวจข้อมูลสามารถนำไปสู่การพบข้อมูลที่มีประโยชน์เพื่อใช้ในการโจมตี ตัวอย่างเช่น หาก แฮกเกอร์ สามารถหาข้อมูลได้ง่ายๆ เช่น โปรแกรมที่ทำ Web Server และเวอร์ชั่นของระบบปฏิบัติการ ก็อาจจะทำให้ แฮกเกอร์ สามารถรู้ช่องโหว่ของระบบ และใช้ประโยชน์จากช่องโหว่นั้นเพื่อเข้าไปในระบบก็เป็นได้

2.1.2.2 การสแกนระบบ (Scanning)

การสแกน (Scanning) เป็นการนำข้อมูลที่รวบรวมมาได้จากขั้นตอน การสำรวจข้อมูล (Reconnaissance) มาอธิบายถึงโครงสร้าง ของเครือข่ายเป้าหมาย รูปแบบการทำงานที่ แฮกเกอร์ ส่วนใหญ่ใช้ก็คือการสแกนพอร์ตของเครื่อง Server เช่น การทำ Network Mapper (Nmap) เพื่อตรวจสอบว่าเครื่อง Server ในเครือข่ายเป้าหมายเปิดให้บริการอยู่หรือไม่ รวมถึงการค้นหาช่องโหว่ต่างๆ ของระบบเครือข่ายอีกด้วย ซึ่งหากแฮกเกอร์ ได้ข้อมูลสำคัญต่างๆ ครบถ้วนหรือเพียงพอบางส่วน เช่น ชื่อเครื่อง Server, หมายเลข IP Address ของเครื่องเป้าหมาย หรือ รายชื่อ User Account คนสำคัญ ก็จะทำให้มองเห็นช่องทางในการเจาะระบบเข้าไปได้

2.1.2.3 การเข้าถึงเป้าหมาย (Gaining Access)

ขั้นตอนนี้จะเริ่มเข้าสู่การโจมตีหรือเจาะช่องที่โหว่ที่ถูกตรวจพบ (เป็นขั้นตอนการ Hacking จริงๆ) ข้อมูลที่เก็บรวบรวมอยู่ในระหว่างขั้นตอนการ Reconnaissance และการ Scanning จะถูกนำมาใช้เพื่อให้สามารถเข้าถึงเครื่องหรือเครือข่ายเป้าหมายได้

2.1.3 การทำรายงานและสิ่งที่แนะนำให้ทำ (Reporting and Clean)

คือขั้นตอนการสรุปงานในแต่ละขั้นตอนว่าได้ข้อมูลอะไรบ้าง เช่น ระบบมีช่องโหว่ตรงไหนบ้าง ในแต่ละช่องโหว่มีความร้ายแรงมากน้อยเพียงใด ส่งผลต่อระบบใดบ้าง และแต่ละช่องโหว่หรือระบบมีจุดไหนที่ควรแก้ไขอย่างไร เป็นต้น ซึ่งการทำรายงานนี้ถือเป็นหัวใจหลักของการทดสอบเจาะระบบ เพราะทางผู้ทดสอบจำเป็นจะต้องเขียนเนื้อหาสรุปใจความให้กระชับและเข้าใจง่าย อีกทั้งยังให้คำแนะนำว่าช่องโหว่ไหนควรจะแก้ไขอย่างไร และใครควรเป็นผู้แก้ไข

2.2 การวิเคราะห์ความรุนแรงของช่องโหว่และการประเมินความเสี่ยง (Vulnerability and Risk Analysis) [11]

ในขั้นตอนการวิเคราะห์ความเสี่ยงนี้จะนำช่องโหว่หรือจุดอ่อนที่ค้นพบนั้นมาจัดระดับความเสี่ยง โดยจุดอ่อนที่มีระดับความเสี่ยงต่ำหมายถึงจุดอ่อนมีความรุนแรงต่ำ จุดอ่อนที่มีความเสี่ยงสูงหมายถึงจุดอ่อนที่อาจก่อให้เกิดความเสียหายต่อระบบสูงหรือมีระดับความรุนแรงสูงและง่ายต่อการโจมตี โดยใช้หลักการวิเคราะห์ความรุนแรงของช่องโหว่และการประเมินความเสี่ยงดังนี้

2.2.1 การวิเคราะห์ช่องโหว่และการประเมินความเสี่ยง [12] สามารถอธิบายได้ดัง แสดงตามตารางที่ 2.1 – 2.2

ตารางที่ 2.1 การวิเคราะห์ความง่ายต่อการเข้าถึงช่องโหว่

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

ตารางที่ 2.2 การวิเคราะห์ผลกระทบที่จะเกิดขึ้นต่อระบบ

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

2.2.2 การประเมินความเสี่ยง

การจัดระดับความเสี่ยงของช่องโหว่หรือจุดอ่อนที่ค้นพบก็จะช่วยในการลำดับความสำคัญว่าช่องโหว่หรือจุดอ่อนไหนจำเป็นที่ต้องแก้ไขหรือป้องกันก่อน

ระดับความเสี่ยง = ความง่ายต่อการเข้าถึงช่องโหว่ x ผลกระทบต่อระบบ

ตารางที่ 2.3 แสดงการประเมินความเสี่ยง

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

2.3 เครื่องมือสำหรับตรวจหาช่องโหว่

เครื่องมือสำหรับตรวจหาช่องโหว่นอกจากเป็นเครื่องมือสำหรับแฮ็คเกอร์ (Black แฮกเกอร์) แล้ว ยังช่วยให้เราสามารถทดลองใช้ เพื่อตรวจสอบและป้องกันช่องโหว่ได้อีกด้วย ในเมื่อเราใช้เครื่องมือเดียวกับแฮ็คเกอร์ในการหาช่องโหว่ เราก็สามารถอุดช่องโหว่เหล่านั้นได้ก่อนที่แฮ็คเกอร์จะโจมตีเข้ามา สำหรับงานวิจัยนี้เลือกใช้โปรแกรม Acunetix Web Vulnerability Scanner เป็นเครื่องมือสำหรับตรวจหาช่องโหว่ของเว็บไซต์

2.3.1 โปรแกรม Acunetix Web Vulnerability Scanner [7]

เป็นเครื่องมือสำหรับตรวจหาช่องโหว่ของเว็บไซต์ ใช้ในการตรวจสอบความปลอดภัยของเว็บไซต์ มีขั้นตอนการทำงานดังนี้

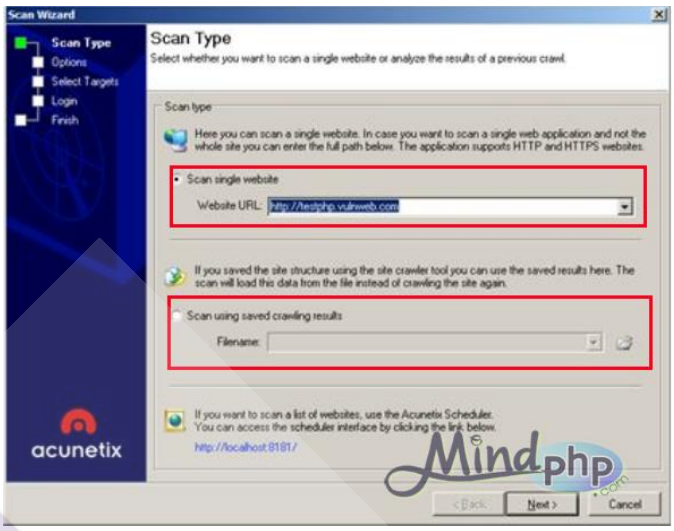
ขั้นตอนที่ 1 เลือก target หรือเป้าหมาย ที่จะสแกน

1.1 คลิก New > New Website Scan to start the Scan Wizard หรือ New Scan จากนั้นเลือกประเภทการสแกน

1.2 ตัวเลือกในการสแกน

- Scan single Website สแกนโดยใช้ URL ของเว็บไซต์
- Scan using saved crawling results สแกนด้วยไฟล์ที่จัดเก็บไว้ก่อนหน้านี้

1.3 กด Next ตามภาพที่ 2.2



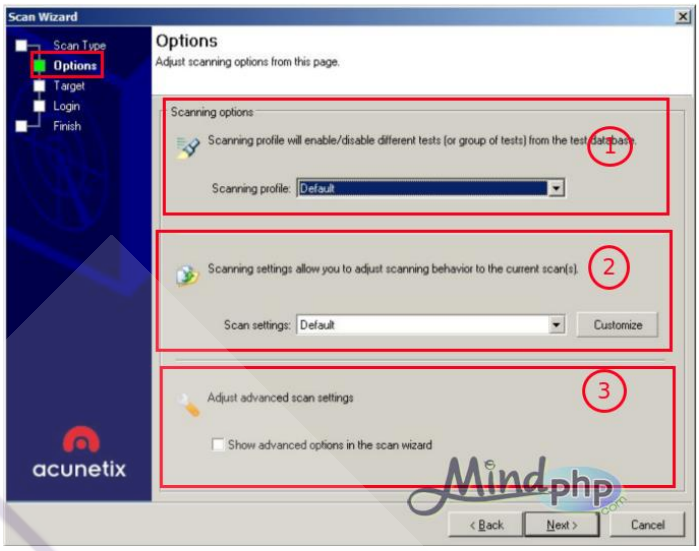
ภาพที่ 2.2 การเลือก target ที่จะสแกน

ขั้นตอนที่ 2 ระบุรายละเอียดการสแกน ตั้งค่าการสแกน

โปรแกรม Acunetix Web Vulnerability Scanner สามารถที่จะสแกนโดยกำหนดช่วงเวลาและการกำหนดค่าการสแกนที่เกิดขึ้น

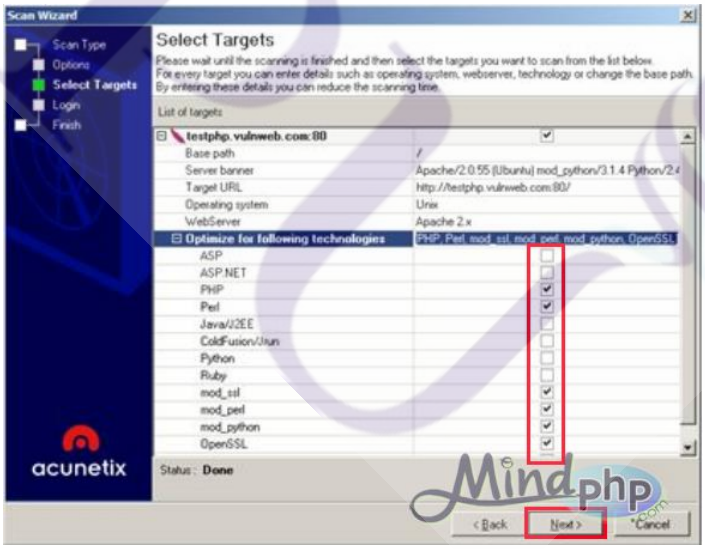
2.1 สแกนข้อมูลส่วนตัวและตั้งค่าการสแกนแม่แบบ

- Scanning Profile สแกนข้อมูลเว็บไซต์ ว่าจะทดสอบอะไร เช่น ทดสอบ SQL injection ก็เลือกที่ข้อมูล SQL_injection
- Scan Settings template เป็นการสแกนโดยใช้แม่แบบ หรือสร้างแม่แบบใหม่
- Advanced Crawling Options เมื่อทำเครื่องหมายถูกจะแสดงตัวเลือกระดับสูงตัวช่วยในการสแกน นอกจากนี้ยังสามารถกำหนดค่า Acunetix เพื่อแสดงรายชื่อไฟล์ที่ระบุไว้ได้ตามภาพที่ 2.3



ภาพที่ 2.3 การระบุรายละเอียดที่จะสแกน

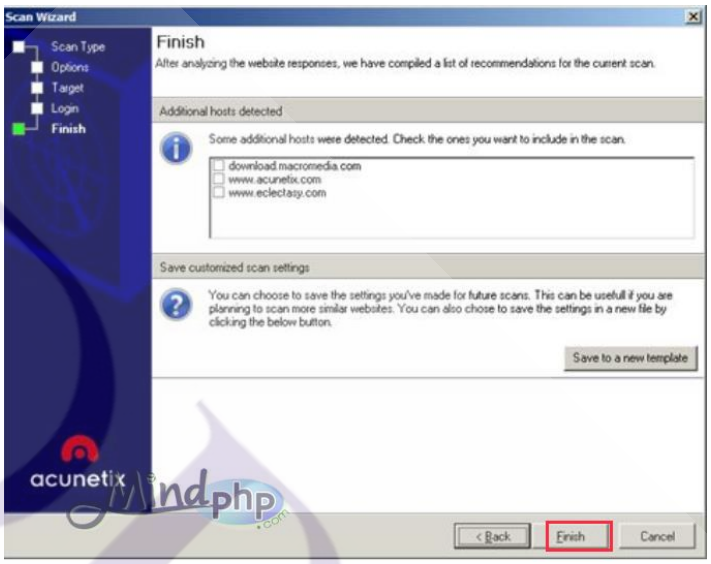
ขั้นตอนที่ 3 ยืนยันการเลือกตัวที่จะสแกนเพื่อหา Targets ที่ต้องการลดระยะเวลาในการสแกน ตามภาพที่ 2.4



ภาพที่ 2.4 การยืนยันการเลือกตัวที่จะสแกนเพื่อหา Targets

ขั้นตอนที่ 4 เมื่อเลือกสิ่งที่จะสแกนเสร็จ

ขั้นตอนที่ 5 กด Finish โปรแกรมจะทำการสแกนสิ่งที่เราเลือกไว้ ขึ้นอยู่กับขนาดของเว็บไซต์รายละเอียดการสแกนที่เลือกและการตอบสนองของเซิร์ฟเวอร์ เวลาสแกนอาจใช้เวลาหลายชั่วโมง ตามภาพที่ 2.5



ภาพที่ 2.5 ขั้นตอนหลังจากที่เลือกสิ่งที่จะสแกนเสร็จ

ขั้นตอนที่ 6 การวิเคราะห์ผลการสแกน

ช่องโหว่ที่พบในระหว่างการสแกนของเว็บไซต์จะแสดงในเรียลไทม์ในโหมดการแจ้งเตือนในผลการสแกนหน้าต่างโหมด Site Structure ยังแสดงให้เห็นรายชื่อไฟล์และโฟลเดอร์ที่ค้นพบ

6.1 การแจ้งเตือนเว็บ

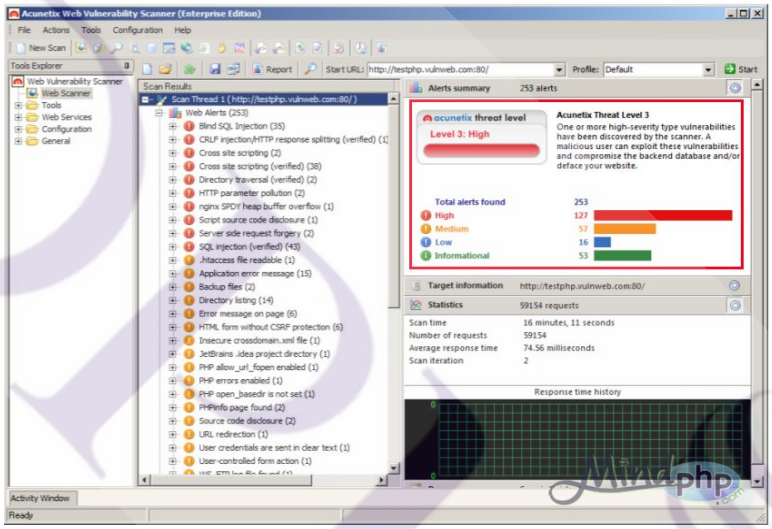
โหมดการแจ้งเตือนเว็บ แสดงช่องโหว่ทั้งหมดที่สแกนพบในเว็บไซต์เป้าหมาย จะแบ่งการแจ้งเตือนเป็น 4 ระดับ คือ

ระดับที่ 1 High Risk Alert Level 3 ช่องโหว่แบ่งออกเป็นอันตรายมากที่สุดซึ่งทำให้สถานที่ที่มีความเสี่ยงสูงสุดสำหรับการเจาะและการโจรกรรมข้อมูล

ระดับที่ 2 Medium Risk Alert Level 2 ช่องโหว่ที่เกิดจากการกำหนดค่าเซิร์ฟเวอร์และ site coding ข้อบกพร่องที่อำนวยความสะดวกการหยุดชะงักของเซิร์ฟเวอร์และการบุกรุก

ระดับที่ 3 Low Risk Alert Level 1 ช่องโหว่ที่ได้มาจากการขาดการเข้ารหัสของการเข้าชมข้อมูลหรือ การเปิดเผยข้อมูลเส้นทางไดเรกทอรี

ระดับสุดท้าย Informational Alert เป็นข้อมูลที่ค้นพบในระหว่างการสแกนและถือว่าเป็นที่หน้าสนใจเช่นเป็นไปได้สำหรับการเปิดเผยข้อมูล IP address หรือ Email address ตามภาพที่ 2.6



ภาพที่ 2.6 การวิเคราะห์การผลการสแกน

2.4 Open Web Application Security Project (OWASP) [8]

OWASP เป็นองค์กรหนึ่งในสหรัฐอเมริกาซึ่งเป็นองค์กรที่ไม่แสวงหาผลกาไรโดยมีวัตถุประสงค์ในการเป็นองค์กรสากลที่เป็นศูนย์รวมในการร่วมมือจากนักพัฒนาเว็บแอพพลิเคชั่นทั่วโลกในการสร้างเว็บแอพพลิเคชั่นให้มีความปลอดภัย รวมไปถึงการจัดสัมมนาและอบรมเกี่ยวกับความปลอดภัยเว็บแอพพลิเคชั่นและเผยแพร่ความรู้เกี่ยวกับช่องโหว่ที่พบได้บ่อยและวิธีการป้องกัน โดยในปี 2013 OWASP ได้เผยแพร่เอกสาร OWASP TOP 10 2013 ที่อธิบายรายละเอียดช่องโหว่ที่พบได้บ่อยและมีความรุนแรง 10 อันดับดังนี้

2.4.1 Injection ช่องโหว่ประเภท Injection เช่น SQL และ OS เกิดขึ้นเมื่อมีข้อมูลที่ไม่น่าเชื่อถือส่งไปยังฐานข้อมูลบนเว็บไซต์ ซึ่งทำให้บุคคลที่ไม่หวังดีสามารถเรียกดูข้อมูลที่เป็นความลับ, ลบหรือแก้ไขข้อมูลในฐานข้อมูลที่สำคัญบนเว็บไซต์ได้ ซึ่งบางครั้งมีการส่ง code เพื่อไปทำงานบนเครื่องแม่ข่ายของกลุ่มเป้าหมายโดยอาจนำไปสู่การโจรกรรมข้อมูลจนไปถึงการเข้าควบคุมเครื่องแม่ข่ายของกลุ่มเป้าหมายได้

2.4.2 Broken Authentication and Session Management ช่องโหว่ประเภท การล้มเหลวในการระบุตัวตนและการบริหารจัดการ session โดยผู้โจมตีจะทำการขโมยรหัสผ่านหรือแอบดูข้อมูล session บน URL ของกลุ่มเป้าหมาย และสามารถปลอมแปลงข้อมูล Session ให้เป็น Session ของบุคคลอื่นได้

2.4.3 Cross-Site Scripting (XSS) เป็นช่องโหว่ที่เกิดขึ้นเมื่อแอพพลิเคชั่นมีข้อมูลที่ไม่น่าเชื่อถือถูกส่งผ่าน web browser โดยไม่มีการตรวจสอบ ซึ่ง XSS อนุญาตให้ผู้โจมตีฝัง JavaScript ลงในเว็บไซต์ของกลุ่มเป้าหมายส่งผลให้เกิดการขโมยข้อมูล session ของผู้ใช้งานคนอื่น หรือการ Redirect User ไปยังเว็บไซต์อื่นที่มีการฝัง Exploit ไว้ ทำให้เกิดความเสียหายต่อผู้ใช้งานเว็บไซต์อย่างรุนแรง ซึ่งผู้โจมตีสามารถฝัง XSS ได้ 2 ช่องทางคือ การฝังผ่าน URL, ฝังผ่าน Webboard นั่นเอง

2.4.4 Insecure Direct Object References เป็นช่องโหว่ที่มีการเข้าถึงข้อมูลหรือรหัสโดยตรง เช่นการเข้าถึงข้อมูลหรือเอกสารที่เป็นความลับของเป้าหมาย ซึ่งผู้โจมตีจะทำการเข้าถึงข้อมูลโดยไม่ต้องผ่านการตรวจสอบการเข้าระบบหรือการป้องกันอื่น ๆ และผู้โจมตียังสามารถเปลี่ยนแปลงรหัสในการระบุตัวตนได้อีกด้วย

2.4.5 Security Misconfiguration เป็นช่องโหว่ของการตั้งค่าความปลอดภัยของ web application, web server, web server software, database จะส่งผลกับความปลอดภัยของเว็บแอพพลิเคชั่น ซึ่งการตั้งค่าที่ผิดพลาดของส่วนประกอบต่าง ๆ ที่เกี่ยวข้อง ตัวอย่างเช่น การลืมลบ default user หรือไม่ทำการอัพเดท security patch โดยผู้โจมตีก็จะสามารถโจรกรรมข้อมูลหรือหยุดการทำงานของเว็บแอพพลิเคชั่นได้

2.4.6 Sensitive Data Exposure เป็นช่องโหว่ที่เกี่ยวกับการรั่วไหลของข้อมูลที่เก็บอยู่ในเครื่องแม่ข่ายและข้อมูลที่ส่งผ่านอินเทอร์เน็ตซึ่งเว็บแอพพลิเคชั่นหลายเว็บไม่มีการป้องส่วนประกอบของข้อมูลที่มีความ Sensitive เช่น ข้อมูลของเครดิตการ์ด โดยผู้โจมตีนั้นจะสามารถขโมย, เปลี่ยนแปลงการเข้าถึงของรหัสข้อมูลได้ หรือการใช้ weak algorithm ในการเข้ารหัส ซึ่งทำให้ข้อมูลที่เป็นความลับตกอยู่ในสภาวะเสี่ยงต่อการโจรกรรม

2.4.7 Missing Function Level Access Control ช่องโหว่นี้เป็นช่องโหว่เกี่ยวกับการให้สิทธิ์ในการใช้งานเว็บแอพพลิเคชั่น อย่างไรก็ตามเว็บแอพพลิเคชั่นจำเป็นต้องมีการตรวจสอบการเข้าถึงระบบบนเครื่องแม่ข่ายหากไม่มีการตรวจสอบหรือผ่านการ log in เข้าระบบ ด้วยสิทธิ์ admin จะทำให้ก็ผู้โจมตีหรือใครก็ตามที่เป็น user ของเว็บไซต์สามารถเข้าไปใช้งานฟังก์ชันของ admin ได้โดยไม่ต้องผ่านการตรวจสอบการเข้าระบบ

2.4.8 Cross-Site Request Forgery (CSRF) เป็นช่องโหว่ที่ผู้โจมตีสามารถส่งคำสั่งไปยังกลุ่มเป้าหมาย รวมทั้งการ session cookie และทำให้มีการระบุตัวแบบอัตโนมัติโดยที่กลุ่มเป้าหมายไม่ได้ตั้งใจที่จะทำ เช่น การโอนเงินของกลุ่มเป้าหมายไปยังบัญชีของผู้โจมตี

2.4.9 Using Components with Known Vulnerabilities เป็นช่องโหว่ที่เกิดจากเว็บแอพพลิเคชั่นทำงานร่วมกับส่วนประกอบอื่น ๆ ที่มีช่องโหว่ เช่น Libraries, Framework หรือส่วนประกอบอื่นๆ ของ Software ที่มีช่องโหว่

2.4.10 Unvalidated Redirects and Forwards เป็นช่องโหว่ที่ผู้โจมตีสามารถทำการ redirect และส่งไปยังเพจหรือเว็บไซต่าง ๆ โดยจะให้กลุ่มเป้าหมายเข้าไปยังเพจที่ไม่น่าเชื่อถือโดยไม่ผ่านการตรวจสอบ ซึ่งผู้โจมตีสามารถร้องขอให้กลุ่มเป้าหมายติดตั้งมัลแวร์ เนื่องจากเข้าใจว่าเป็นเว็บไซต์ที่ redirect มาจากเว็บไซต์ที่น่าเชื่อถือก็อาจจะตกเป็นเหยื่อของมัลแวร์ได้

2.5 ข้อมูลของช่องโหว่ที่เกี่ยวข้อง

สารนิพนธ์ฉบับนี้จะเลือกศึกษาเกี่ยวกับช่องโหว่ที่ถูกตรวจพบในเว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศ โดยมีรายละเอียดดังนี้

2.5.1 ช่องโหว่ประเภท Cross-Site Request Forgery (CSRF) [9] เป็นช่องโหว่ที่พบบ่อยถูกจัดอยู่ในลำดับที่ 8 ของการจัดลำดับช่องโหว่โดย OWASP ซึ่งเป็นช่องโหว่ที่ผู้โจมตีสามารถส่งคำสั่งไปยังกลุ่มเป้าหมาย รวมทั้งการ session cookie และทำให้มีการระบุตัวแบบอัตโนมัติโดยที่กลุ่มเป้าหมายไม่ได้ตั้งใจที่จะทำ

2.5.2 ช่องโหว่ Apache httpOnly cookie disclosure [7] เป็นช่องโหว่ของ Apache Web Server ในเวอร์ชั่น 2.2.x ถึง 2.2.21 ที่ไม่สามารถตรวจสอบค่า HTTP Header ได้ถูกต้องในเรื่องของ Cookie ที่ใช้พารามิเตอร์ HTTP Only ช่องโหว่ดังกล่าวนี้ทำให้ผู้โจมตีใช้วิธีการสร้างสคริปต์ขึ้นมาเอง และส่งค่าร้องขอผ่านช่องโหว่ดังกล่าว และข้อมูลของ Cookie นั้นจะตอบสนองกลับมากับการโจมตี โดยที่ไม่สนใจในเรื่องของการเขียน code ในเว็บแอพพลิเคชั่น

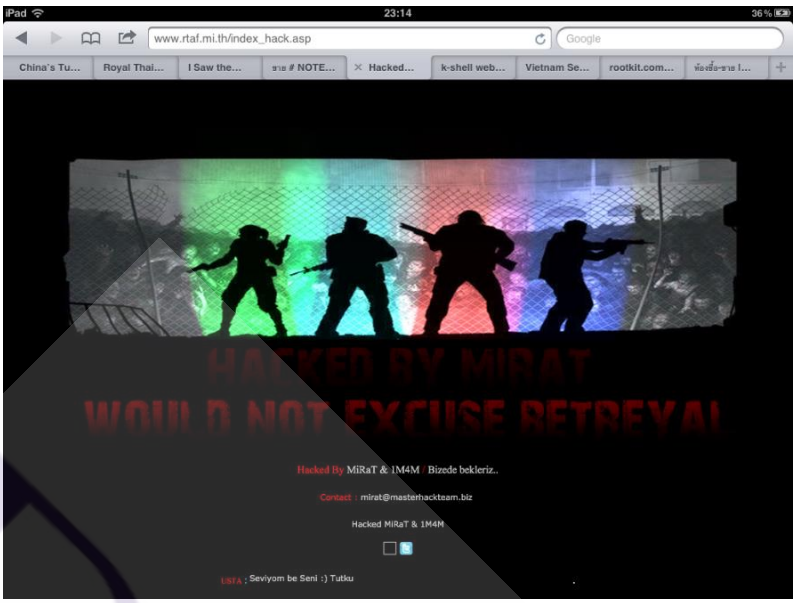
2.5.3 ช่องโหว่ Local File Disclosure [13] คือ ช่องโหว่ที่เปิดทางให้แฮกเกอร์ดึงไฟล์อื่นๆ ที่อยู่ในเว็บไซต์มารัน หรือ อ่านไฟล์ (อาทิเช่น ไฟล์ config หรือไฟล์เก็บ password ต่างๆ) โดยมีสาเหตุมาจากการที่ผู้พัฒนาเว็บไซต์ไม่คำนึงถึงความปลอดภัยในการเขียนสคริป ทำให้แฮกเกอร์สามารถดาวน์โหลดไฟล์ที่สำคัญที่อยู่บนเครื่องเซิร์ฟเวอร์มาใช้ประโยชน์ในการโจมตีเว็บไซต์ได้

2.5.4 ช่องโหว่ File upload [5] เป็นช่องโหว่จากการเรียกใช้ระบบการอัพโหลดไฟล์บนหน้าเว็บไซต์เป้าหมาย โดยปกติการอัพโหลดไฟล์รูปภาพหรือไฟล์ใดๆ ขึ้นบนเว็บไซต์จะพบว่าการเก็บไฟล์นั้นๆ ระบบจะเก็บไฟล์ที่ถูกอัพโหลดไว้บนเว็บไซต์ และหากระบบที่พัฒนาในการอัพโหลดไฟล์ ไม่ได้มีการตรวจสอบเนื้อหาหรือส่วนประกอบต่างๆ ของไฟล์ก่อนนำไปวางบนเครื่องแม่ข่ายจริงแล้วนั้น เท่ากับว่าผู้โจมตีจะสามารถใช้ช่องโหว่ดังกล่าวในการอัพโหลดไฟล์สคริปต์อันตราย เช่น ไฟล์ shell.php ขึ้นไปบนเว็บไซต์ ได้ทันที ส่งผลลัพธ์ให้ผู้โจมตีสามารถรันไฟล์สคริปต์อันตรายบนเครื่องเว็บไซต์เป้าหมาย และเข้าทำการอัพโหลดหรือปรับเปลี่ยนไฟล์ของเว็บไซต์เป้าหมายในส่วนต่างๆ ตามที่ได้กล่าวไว้ตอนต้นเกี่ยวกับจุดประสงค์ของผู้โจมตีการโจมตีในลักษณะนี้จะเรียกว่าการโจมตีแบบ Unrestricted File Upload สามารถพบได้แพร่หลายและเป็นที่นิยมในหมู่ผู้โจมตีเนื่องจากค้นหาช่องโหว่ได้ง่าย

2.6 ตัวอย่างของเว็บไซต์ที่มีช่องโหว่และเคยผ่านการถูกโจมตี [14]

ที่ผ่านมาเว็บไซต์ของกองทัพอากาศ ที่อยู่ภายใต้โดเมนเนม rtaf.mi.th ถูกโจมตีจากแฮกเกอร์ เป็นจำนวนมาก ดังตัวอย่างต่อไปนี้

(1) เมื่อวันที่ 9 มิถุนายน พ.ศ.2555 เว็บไซต์ของกองทัพอากาศ ถูกโจมตีโดยการเปลี่ยนหน้าตาของเว็บไซต์ ดังแสดงตามภาพที่ 2.7



ภาพที่ 2.7 เว็บไซต์ของกองทัพอากาศที่เคยถูกโจมตี

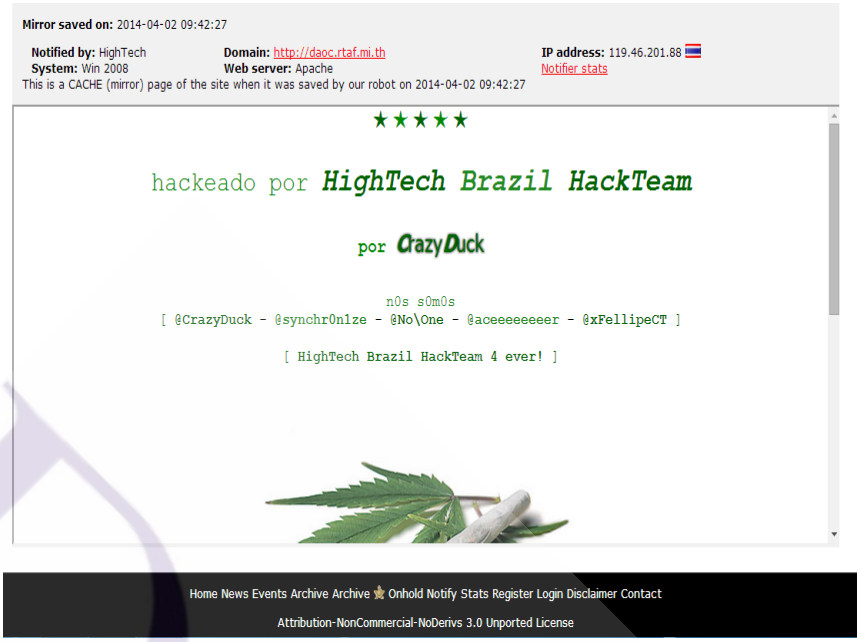
(2) เมื่อเดือนเมษายน – เดือนพฤษภาคม พ.ศ.2557 เว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศและเว็บไซต์อื่นๆ ที่อยู่ภายใต้โดเมน .rtaf.mi.th ถูกโจมตีโดยการเปลี่ยนหน้าเว็บไซต์ ดังแสดงตามภาพที่ 2.8 – 2.9

Total notifications: **509** of which **134** single ip and **375** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	Domain	OS	View
2014/05/07	HighTech	H	M			committee.rtaf.mi.th	Win 2008	mirror
2014/05/07	HighTech	H	M			daoc.rtaf.mi.th	Win 2008	mirror
2014/05/07	HighTech	H	M			itcenter.rtaf.mi.th	Win 2008	mirror
2014/05/07	HighTech	H	M			ndsi.rtaf.mi.th	Win 2008	mirror
2014/05/07	HighTech	H	M			redflag.rtaf.mi.th	Win 2008	mirror
2014/05/07	HighTech	H	M			www88.rtaf.mi.th	Win 2008	mirror
2014/04/28	Nofawkx Al		M	R		army3.rta.mi.th/_al.htm	Linux	mirror
2014/04/11	MRW8 HACKER	H	M			cav2div.cloud.rta.mi.th	Linux	mirror
2014/04/11	MRW8 HACKER	H	M			army1012.cloud.rta.mi.th	Linux	mirror
2014/04/11	MRW8 HACKER	H	M			amic.cloud.rta.mi.th	Linux	mirror
2014/04/11	MRW8 HACKER	H	M			pawai11.cloud.rta.mi.th	Linux	mirror
2014/04/11	MRW8 HACKER	H				pawai12.cloud.rta.mi.th	Linux	mirror
2014/04/05	black_raptor lamer			R		www.army2.mi.th/b.htm	Win 2008	mirror
2014/04/02	HighTech	H	M	R		awfc.rtaf.mi.th	Win 2008	mirror
2014/04/02	HighTech	H	M	R		www2.awfc.rtaf.mi.th	Win 2008	mirror
2014/04/02	HighTech	H	M	R		iam.rtaf.mi.th	Win 2008	mirror
2014/04/02	HighTech	H	M	R		secret.rtaf.mi.th	Win 2008	mirror
2014/04/02	HighTech	H		R		quarter.rtaf.mi.th	Win 2008	mirror
2014/03/28	Dr-TaiGaR			R		www.3sor.mi.th/hp.txt	Linux	mirror
2014/02/11	d3b~X					rcsc.rtarf.mi.th/ganteng.htm	Linux	mirror
2014/02/10	nighto mearo	H		R		www.army3.mi.th	Linux	mirror
2013/08/28	Dr-TaiGaR			R		tncbcc.rtarf.mi.th/dba1/	Linux	mirror
2013/08/28	Dr-TaiGaR		M	R		afdc-mdu11.rtarf.mi.th/backup/...	Linux	mirror

ภาพที่ 2.8 เว็บไซต์ภายใต้โดเมน .rtaf.mi.th ที่เคยถูกโจมตี



ภาพที่ 2.9 เว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศเคยถูกโจมตี

เว็บไซต์เหล่านี้เคยถูกโจมตีโดยใช้วิธีเข้าไปเปลี่ยนแปลงหน้าเว็บไซต์ (Website Defacement) ซึ่งในเว็บไซต์ที่ถูกโจมตีส่วนใหญ่จะปรากฏรูปภาพหรือข้อความที่บ่งบอกถึงว่าเว็บไซต์ถูกโจมตีได้สำเร็จ ทำให้เกิดความเสียหายและทำลายความน่าเชื่อถือให้แก่หน่วยงานเจ้าของเว็บไซต์

ด้วยเหตุนี้ ผู้จัดทำจึงได้ให้ความสำคัญกับการรักษาความมั่นคง ปลอดภัยของเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ เพื่อป้องกันการถูกโจมตีจากผู้ไม่ประสงค์ดี และเป็นการป้องกันไม่ให้แฮกเกอร์ใช้เว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศ เป็นช่องทางในการเข้ามาโจมตีเพื่อสร้างความเสียหายให้แก่เว็บไซต์อื่นๆ ของกองทัพอากาศ

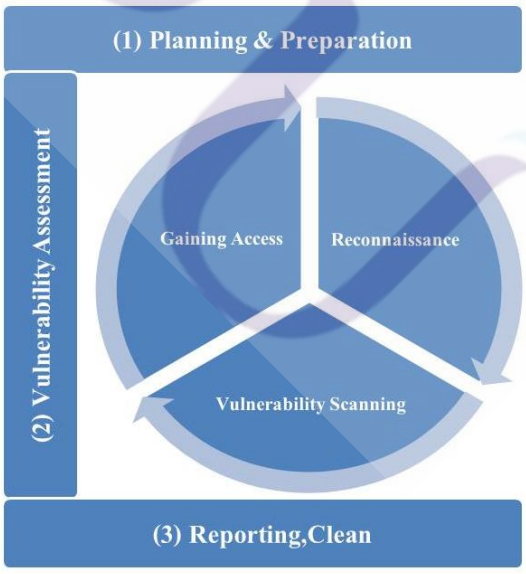
บทที่ 3
การดำเนินการตรวจหาช่องโหว่ของเว็บไซต์

ในการตรวจหาช่องโหว่ของเว็บไซต์ กรณีศึกษาเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ ผู้วิจัยได้แบ่งขั้นตอนในการดำเนินการตรวจหาช่องโหว่ของเว็บไซต์ เป็น 3 ขั้นตอน ประกอบด้วย

(1) การวางแผนและเตรียมการ(Planning and Preparation)

(2) การประเมินค่าของช่องโหว่ (Vulnerability Assessment)

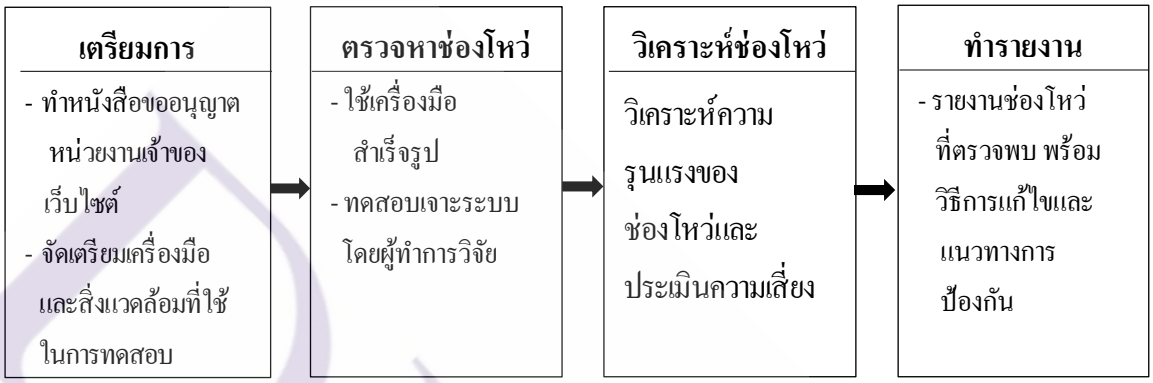
(3) การทำรายงานวิธีการแก้ไขและการป้องกันช่องโหว่ (Report how to fix and prevent vulnerabilities) โดยขั้นตอนที่ 3 รายงานวิธีการแก้ไขและการป้องกันช่องโหว่ (Report how to fix and prevent vulnerabilities) จะขอกล่าวในบทที่ 4 ขั้นตอนในการดำเนินการตรวจหาช่องโหว่แสดงตามภาพที่ 3.1



ภาพที่ 3.1 ขั้นตอนในการดำเนินการตรวจหาช่องโหว่ของเว็บไซต์

3.1 การวางแผนและเตรียมการ (Planning and Preparation)

การวางแผนและเตรียมการ ผู้วิจัยได้กำหนดขอบเขตของเป้าหมายในการหาช่องโหว่ของเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ เป็นการหาช่องโหว่ของ Web Application ที่ให้บริการที่พอร์ต 80 โดยมีขั้นตอนการวางแผนและเตรียมการในการหาช่องโหว่ของเว็บไซต์ประกอบไปด้วย 4 ขั้นตอน ดังแสดงตามภาพที่ 3.2



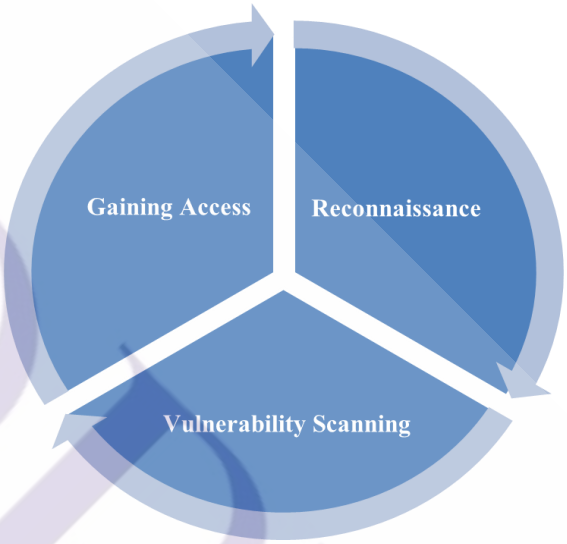
ภาพที่ 3.2 ขั้นตอนการวางแผนและเตรียมการ

ผู้วิจัยได้ทำการติดต่อไปยังหน่วยงานเจ้าของเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ เพื่อทำหนังสืออนุญาตทำการทดสอบเจาะระบบ โดยกำหนดขอบเขตเวลา ระหว่างวันที่ 16 พฤศจิกายน พ.ศ.2559 ถึงวันที่ 31 พฤษภาคม พ.ศ.2560 โดยจะทดสอบในช่วงเวลา 18.00 น. ถึง 24.00 น.เพื่อหลีกเลี่ยงช่วงเวลาที่เว็บไซต์มีผู้ใช้งานคับคั่ง และมีมิติของการทดสอบในแง่ของการทดสอบหาช่องโหว่ระบบโดยใช้เครื่องมือสำเร็จรูปในการทดสอบ คือโปรแกรม Acunetix Web Vulnerability Scanner ซึ่งทางผู้จัดทำจะทำการเก็บข้อมูลที่ได้ระหว่างการทดสอบเป็นความลับ และส่งรายละเอียดที่ได้รับหลังจากการทดสอบ กลับไปให้หน่วยงานภายใต้ชั้นความลับที่เหมาะสม

3.2 การประเมินค่าของช่องโหว่ (Vulnerability Assessment)

ในขั้นตอนนี้เป็นการตรวจหาช่องโหว่และนำช่องโหว่ที่ตรวจพบมาทำการวิเคราะห์และประเมินความเสี่ยง โดยการตรวจหาช่องโหว่นี้จะใช้วิธีการทดสอบเพื่อเลียนแบบขั้นตอนจากการโจมตีของแฮกเกอร์ โดยวัตถุประสงค์ของขั้นตอนนี้จะทำการทดสอบเพื่อหาว่าเว็บไซต์นี้มีช่องโหว่หรือไม่ และช่องโหว่ที่ตรวจพบเป็นช่องโหว่ประเภทใด เพื่อนำช่องโหว่ที่ได้ไปวิเคราะห์เพื่อ

หาแนวทางการแก้ไขต่อไป โดยในขั้นตอนการตรวจหาช่องโหว่นี้จะเลือกทำเฉพาะขั้นตอนที่ไม่ก่อให้เกิดความเสียหายใด ๆ ต่อเว็บไซต์และเว็บเซิร์ฟเวอร์ เนื่องจากเป็นการตรวจหาช่องโหว่จากระบบที่เปิดให้บริการอยู่จริง ซึ่งผู้วิจัยได้แบ่งขั้นตอนที่นำมาใช้ในการตรวจหาช่องโหว่ของงานวิจัยนี้ ออกเป็น 3 ขั้นตอน ประกอบด้วยขั้นตอนการรวบรวมข้อมูลของเว็บไซต์ ขั้นตอนการตรวจหาช่องโหว่ ขั้นตอนการเข้าถึงช่องโหว่ที่ตรวจพบ โดยขั้นตอนดังกล่าวแสดงตามภาพที่ 3.3



ภาพที่ 3.3 ขั้นตอนการตรวจหาช่องโหว่ของเว็บไซต์

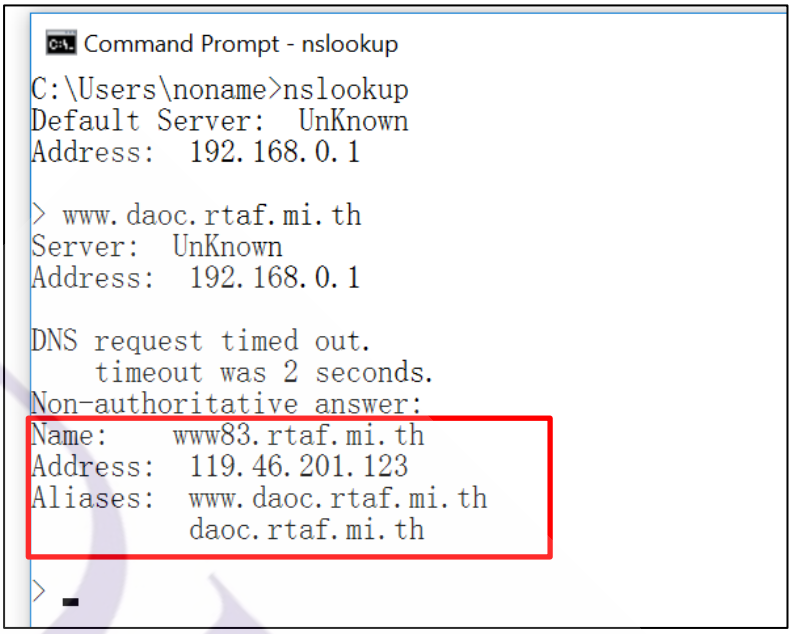
3.2.1 ขั้นตอนการสำรวจข้อมูล (Reconnaissance)

เป็นขั้นตอนในการหาข้อมูลที่เกี่ยวข้องกับเว็บไซต์ เพื่อนำข้อมูลที่ได้นำไปวิเคราะห์หาวิธีการเข้าถึงช่องโหว่ของเว็บไซต์ต่อไป โดยข้อมูลที่ผู้วิจัยต้องการเพื่อนำไปใช้ประโยชน์ในการตรวจหาช่องโหว่ มีขั้นตอนการหาข้อมูลดังนี้

(1) การทำ nslookup

ผู้วิจัยได้ทำการตรวจสอบข้อมูลของเว็บไซต์ด้วยคำสั่ง nslookup เป็นคำสั่งที่ใช้ในการตรวจสอบโดเมนเนม (Domain Name) ด้วยโปรแกรมคอมมานพรอมพ์ (Command prompt) เพื่อหาข้อมูลโดเมนเนม (Domain Name) ของเว็บไซต์นี้ พบว่า Domain Name ของเว็บไซต์นี้มีไอพีแอดเดรสเป็น 119.46.201.123 , มีชื่อเว็บไซต์จริงคือ www83.rtaf.mi.th และมี

นามแฝงคือ www.daoc.rtaf.mi.ht, daoc.rtaf.mi.th ทำให้ทราบข้อมูลที่จะนำไปใช้ในขั้นตอนของการสแกนหาช่องโหว่ต่อไป รายละเอียดข้อมูลที่พบจากการใช้คำสั่ง nslooup แสดงตามภาพที่ 3.4



ภาพที่ 3.4 ผลลัพธ์ของการตรวจสอบข้อมูลของเว็บไซต์ด้วยคำสั่ง nslookup

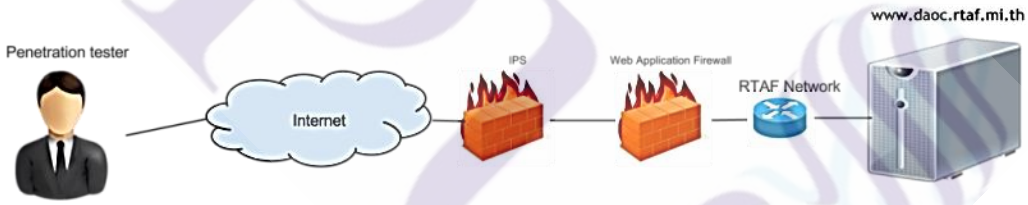
(2) การทำ Reverse IP Domain Check

เป็นการหาข้อมูลของเว็บไซต์ที่อยู่ในโดเมนเดียวกัน โดยใช้เครื่องมือของเว็บไซต์ www.yougetsignal.com ซึ่งเป็นเว็บไซต์ที่แฮกเกอร์นิยมใช้ในการหาข้อมูลเกี่ยวกับเป้าหมาย พบว่าโดเมนเนมของเว็บไซต์ www.daoc.rtaf.mi.th มีโดเมนเนมอื่น ๆ ที่อยู่ในไอพีเดียวกัน จำนวนทั้งสิ้น 12 โดเมน จากข้อมูลที่ได้รับ พบว่าหากผู้ไม่ประสงค์ดีหรือแฮกเกอร์สามารถโจมตีเว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศได้ ก็สามารถสร้างความเสียหายหรือทำลายเว็บไซต์อื่น ๆ ที่อยู่บนไอพีเดียวกันให้เกิดความเสียหายได้ รายละเอียดข้อมูลที่ได้รับจากการทำ Reverse IP Domain Check แสดงตามภาพที่ 3.5

ภาพที่ 3.5 ผลลัพธ์การทำ Reverse IP Domain Check

3.2.2 ขั้นตอนการสแกนหาช่องโหว่ (Vulnerability Scanning)

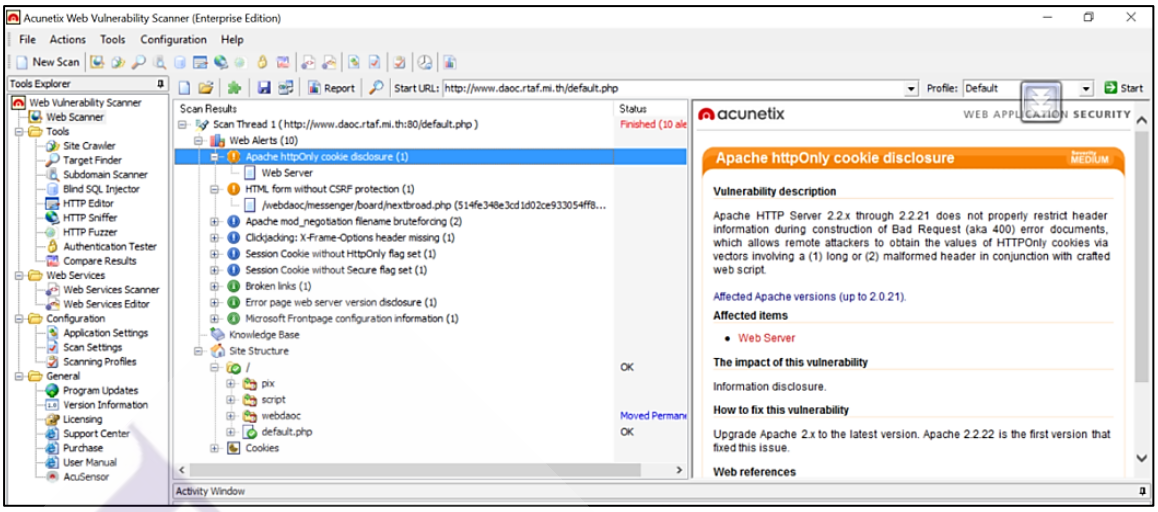
สารนิพนธ์นี้เลือกวิธีการสแกนหาช่องโหว่ของเว็บไซต์ (www.daoc.rtaf.mi.th) โดยใช้โปรแกรม Acunetix Web Vulnerability Scanner ซึ่งเป็นโปรแกรมสำเร็จรูปที่แฮกเกอร์และผู้ดูแลระบบนิยมใช้ในการสแกนหาช่องโหว่ของเว็บไซต์ โดยมีรายละเอียดของสภาพแวดล้อมดังแสดงในภาพที่ 3.6



- Acunetix Web Vulnerability Scanner
- Manual

ภาพที่ 3.6 โครงสร้างสภาพแวดล้อม

3.2.2.1 ขั้นตอนการรวบรวมข้อมูลโดยใช้เครื่องมือ Acunetix Web Vulnerability Scanner โดยผลลัพธ์ที่ ได้แสดงในภาพที่ 3.7

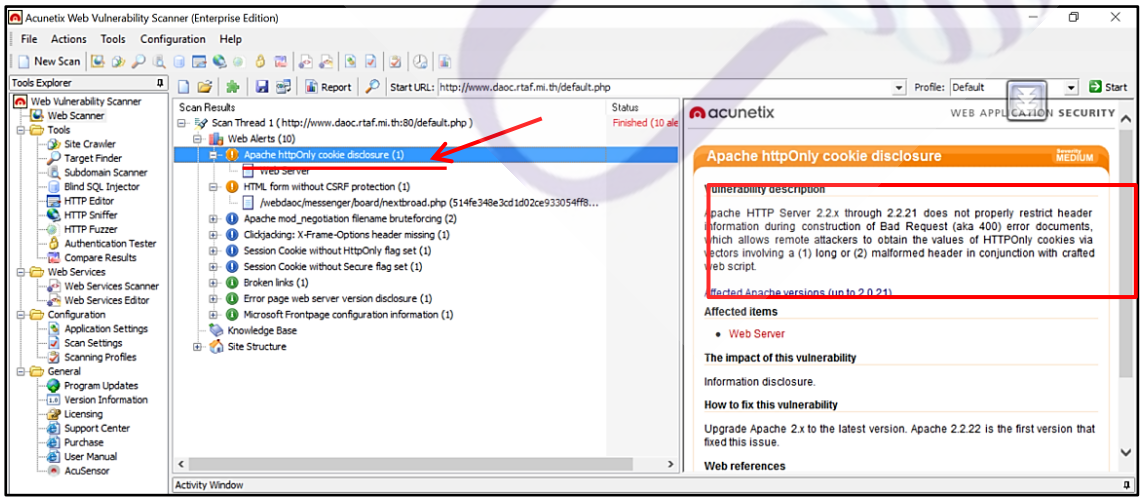


ภาพที่ 3.7 ข้อมูลของช่องโหว่ที่ตรวจพบ

ข้อมูลที่ได้จากการสแกน โดยใช้เครื่องมือ Acunetix Web Vulnerability Scanner มีรายละเอียดดังนี้

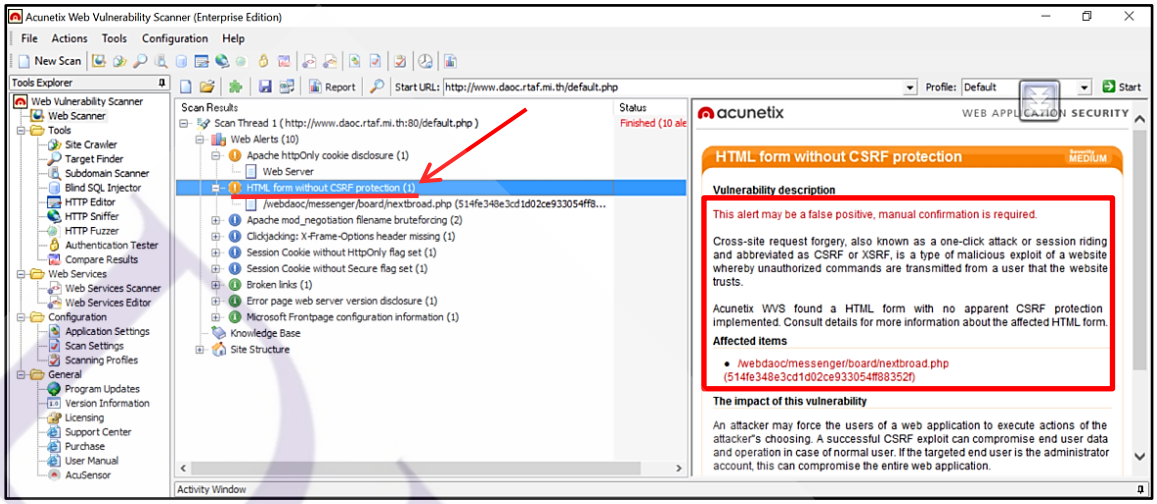
พบช่องโหว่ที่มีความรุนแรงระดับปานกลาง (Medium) มี 2 ประเภท คือ

- Apache httpOnly cookie disclosure ช่องโหว่ประเภทนี้คือ เมื่อมีการใส่ค่าที่ไม่ถูกต้องลงไปในช่อง URL เว็บเซิร์ฟเวอร์จะส่ง Bad Request กลับมา ทำให้แฮกเกอร์สามารถนำข้อมูลจาก Bad Request ไปใช้ประโยชน์ได้ ซึ่งทำให้แฮกเกอร์รู้ว่า Request ที่ส่งไปมีข้อผิดพลาดตรงไหนบ้าง รายละเอียดของช่องโหว่ที่ตรวจพบ แสดงในภาพที่ 3.8



ภาพที่ 3.8 ข้อมูลรายละเอียดของช่องโหว่ประเภท Apache httpOnly cookie disclosure

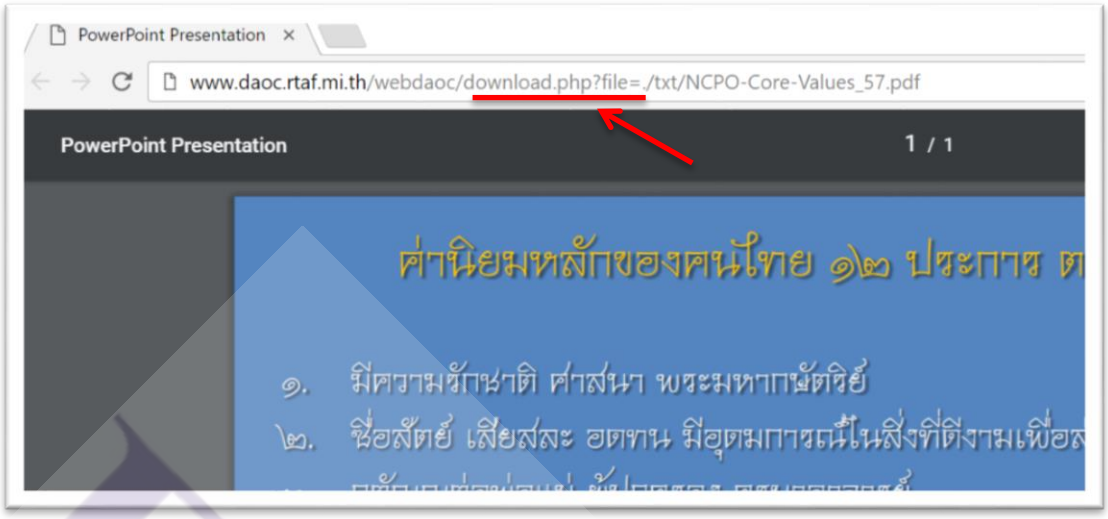
• Cross Site Request Forgery (CSRF) ช่องโหว่ประเภทนี้เป็นช่องโหว่ที่ผู้โจมตีสามารถส่ง http request รวมทั้งเซสชั่นหรือคุ้กกี้ที่มีการปรับปรับแต่งค่าไปยังเว็บเซิร์ฟเวอร์เพื่อใช้ประโยชน์จากเซสชั่นหรือคุ้กกี้ของผู้ใช้ที่มีสิทธิเข้าถึงข้อมูล ซึ่งไฟล์ที่พบว่าเป็นช่องโหว่คือ nextbroad.php แสดงในภาพที่ 3.9



ภาพที่ 3.9 ข้อมูลรายละเอียดของช่องโหว่ HTML form without CSRF protection

3.2.2.2 สแกนหาช่องโหว่บนหน้าเว็บไซต์

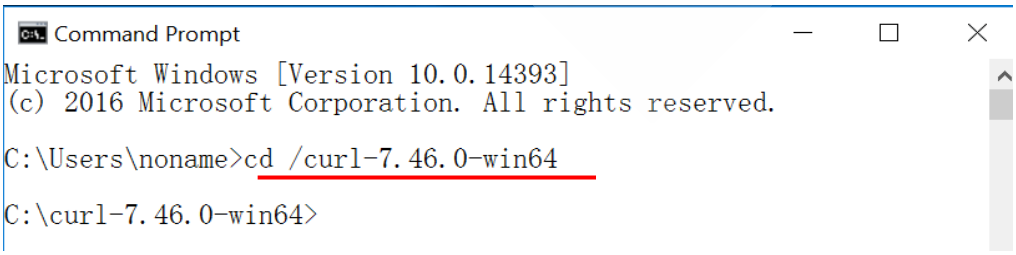
ผู้วิจัยได้ทำการสแกนหาช่องโหว่ของเว็บไซต์โดยการหาช่องโหว่จากหน้าเพจทุกเพจที่อยู่บนเว็บไซต์ จนพบข้อมูลมูลที่คาดว่าจะเป็นช่องโหว่ คือ parameter ที่ชื่อว่า “file” ในส่วนของหน้าเพจคือไฟล์ที่ชื่อว่า “download.php ซึ่งผู้วิจัยพบว่าหน้าเพจนี้มีช่องโหว่คือให้ผู้ใช้สามารถดาวน์โหลดไฟล์ ออกมาจากเซิร์ฟเวอร์ได้โดยผ่านไฟล์ “download.php” ซึ่งหมายความว่าผู้ใช้สามารถใช้คำสั่งในการดาวน์ไฟล์ต่าง ๆ ที่อยู่บนเว็บเซิร์ฟเวอร์ออกมาใช้ประโยชน์ในการโจมตีเว็บไซต์และเว็บเซิร์ฟเวอร์ได้ ช่องโหว่ดังกล่าวปรากฏอยู่ใน URL ดังแสดงตามภาพที่ 3.10



ภาพที่ 3.10 ช่องโหว่ของ Local file inclusion

3.2.3 ขั้นตอนการเข้าถึงเป้าหมาย (Gaining Access)

จากข้อมูลที่ได้รับในขั้นตอนที่ 3.2.2.3 คือ การสแกนหาช่องโหว่บนหน้าเว็บไซต์ ผู้วิจัยนำข้อมูลที่ได้มาใช้ประโยชน์ในการทดสอบการโจมตีเว็บไซต์ โดยใช้เทคนิคที่เรียกว่า Local File Disclosure ในการหาช่องโหว่ โดยการใช้โปรแกรม Curl ผ่าน Command Prompt เพื่อส่ง HTTP script ในการดาวน์โหลดไฟล์ download.php ด้วยคำสั่ง curl -o download.php เนื่องจากเป็นคำสั่งที่ใช้ดาวน์โหลดไฟล์ที่ต้องการจากหน้าเว็บไซต์ให้มาแสดงบนเครื่องของผู้วิจัย จากนั้นใช้คำสั่ง -A “Mozilla/5.0 (Linux; u; Android 2.2: en-us: SCH-I800 Build/FROYO) AppleWebkit/533.1 (KHTML, like Gecko) Version/4.0 Mobile safari/533.1” ในการกำหนดค่า Header ให้เสมือนเป็นการเรียกใช้งานจากบราวซ์เซอร์โดยทั่วไป และตามด้วยคำสั่ง curl –url http://www.daoc.rtaf.mi.th/webdaoc/download.php?file=./download.php” เป็นคำสั่งที่ใช้ระบุที่อยู่ของไฟล์ที่ต้องการดาวน์โหลด ดังแสดงตามภาพที่ 3.11 – 3.12

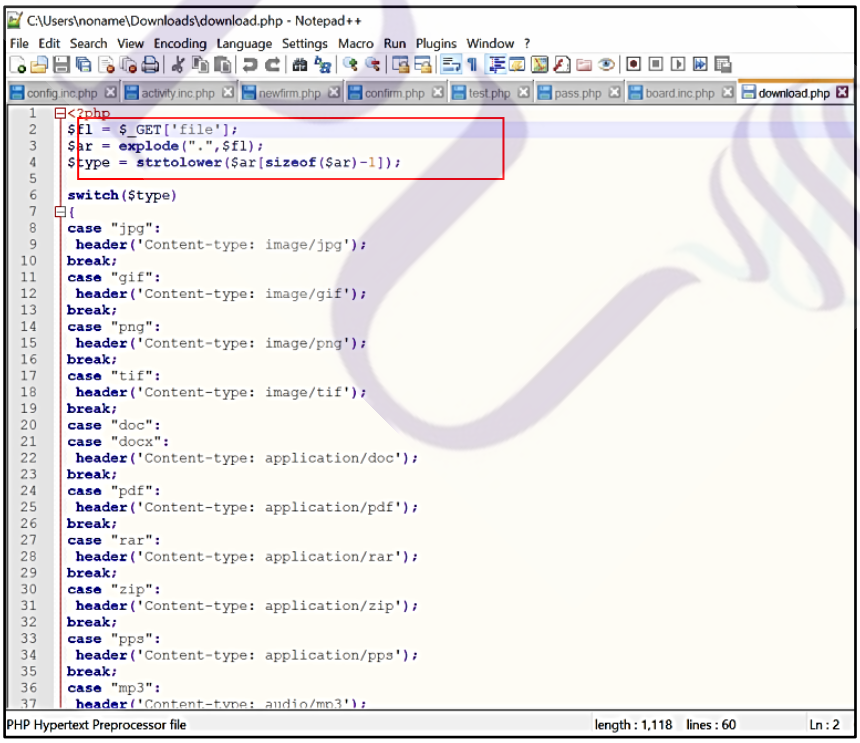


ภาพที่ 3.11 คำสั่งการเรียกใช้เครื่องมือ Curl

curl -o download.php -A “Mozilla/5.0 (Linux; u; Android 2.2: en-us: SCH-I800 Build/FROYO) AppleWebkit/533.1 (KHTML, like Gecko) Version/4.0 Mobile safari/533.1” --url “http://www.daoc.rtaf.mi.th/webdaoc/download.php?file=./download.php”

ภาพที่ 3.12 คำสั่งดาวน์โหลดไฟล์ download.php

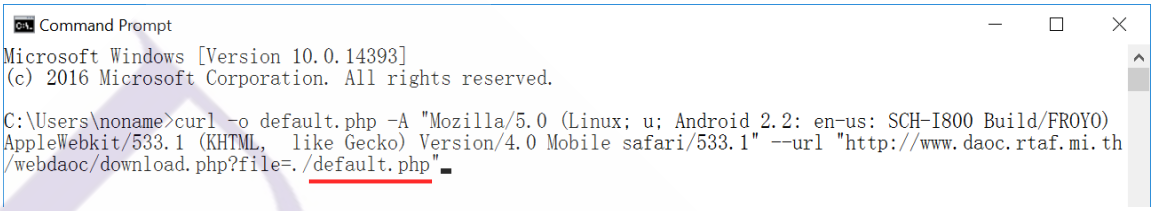
จากคำสั่งดังกล่าวพบว่าสามารถดาวน์โหลดไฟล์ download.php ออกมาจากเครื่องเซิร์ฟเวอร์ได้สำเร็จ จากนั้นทำการอ่านซอร์สโค้ดของไฟล์ download.php พบว่าไม่มีการตรวจสอบนามสกุลของไฟล์ก่อนที่จะอนุญาตให้ดาวน์โหลด ส่งผลให้สามารถดาวน์ไฟล์ ใด ๆ ก็ได้ที่อยู่บนเซิร์ฟเวอร์ เพียงแค่รู้ที่อยู่ของไฟล์ที่ต้องการดาวน์โหลดเท่านั้น รายละเอียดตามภาพที่ 3.13



ภาพที่ 3.13 อ่านซอร์สโค้ดไฟล์ download.php

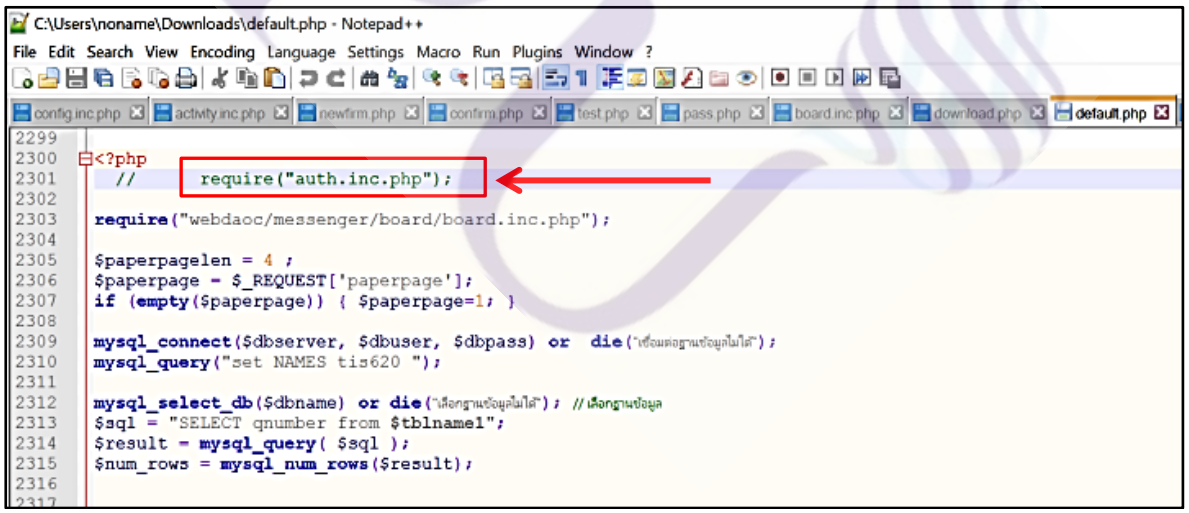
จากนั้นจึงทำการทดลองดาวน์โหลดไฟล์ default.php ซึ่งเป็นไฟล์ที่แสดงหน้าแรกของเว็บไซต์ ด้วยคำสั่งต่อไปนี้ แสดงตามภาพที่ 3.14

```
curl -o default.php -A “Mozilla/5.0 (Linux; u; Android 2.2: en-us: SCH-I800 Build/FROYO) AppleWebkit/533.1 (KHTML,  like Gecko) Version/4.0 Mobile safari/533.1” --url “http://www.daoc.rtaf.mi.th/webdaoc/download.php?file=./default.php”
```



ภาพที่ 3.14 คำสั่งดาวน์โหลดไฟล์ default.php

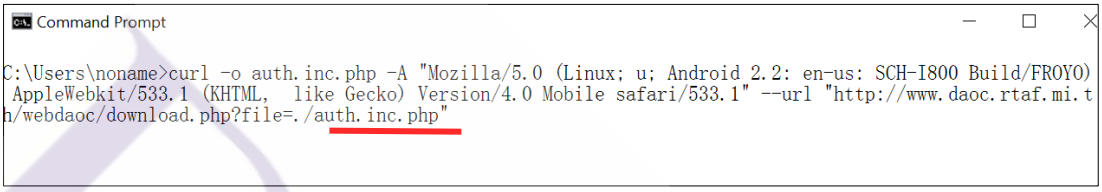
จากคำสั่งข้างต้นพบว่าสามารถดาวน์โหลดไฟล์ default.php ได้สำเร็จจากนั้นจึงอ่านไฟล์ default.php พบว่ามีการอ้างอิงถึงไฟล์ auth.inc. ตามภาพที่ 3.15



ภาพที่ 3.15 รายละเอียดของไฟล์ไฟล์ default.php

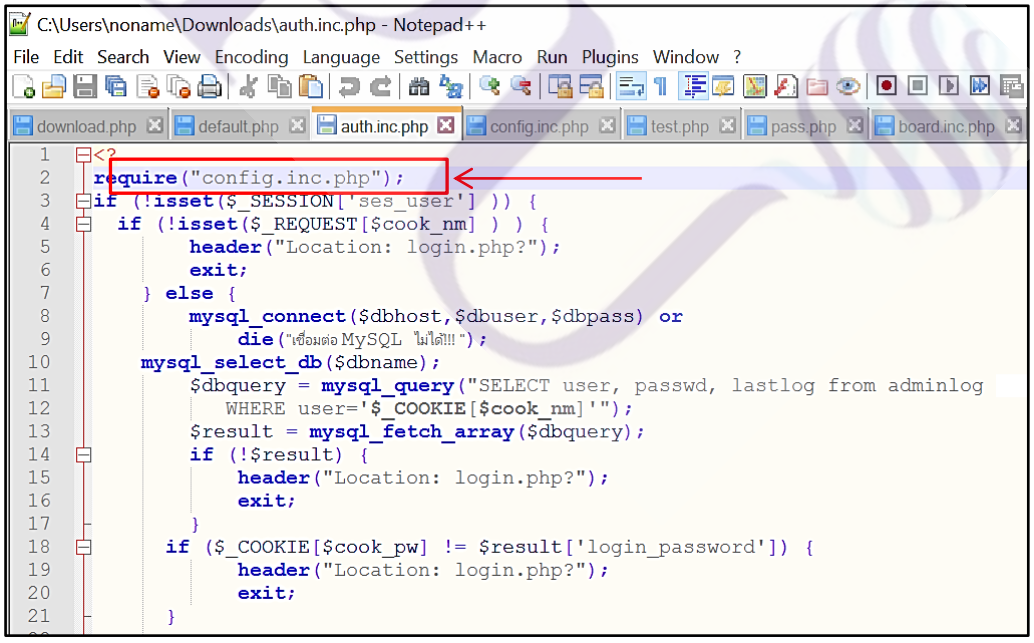
จากนั้นจึงทำการดาวน์โหลดไฟล์ auth.inc.php ซึ่งเป็นไฟล์ที่ถูกอ้างถึงในไฟล์ default.php ซึ่งเป็นไฟล์ที่เป็นหน้าแรกของเว็บไซต์ ด้วยคำสั่งดังแสดงตามภาพที่ 3.16

```
curl -o auth.inc.php -A “Mozilla/5.0 (Linux; u; Android 2.2: en-us: SCH-I800 Build/FROYO) AppleWebkit/533.1 (KHTML,  like Gecko) Version/4.0 Mobile safari/533.1” --url “http://www.daoc.rtaf.mi.th/webdaoc/download.php?file=./auth.inc.php”
```



ภาพที่ 3.16 คำสั่งดาวน์โหลดไฟล์ auth.inc.php

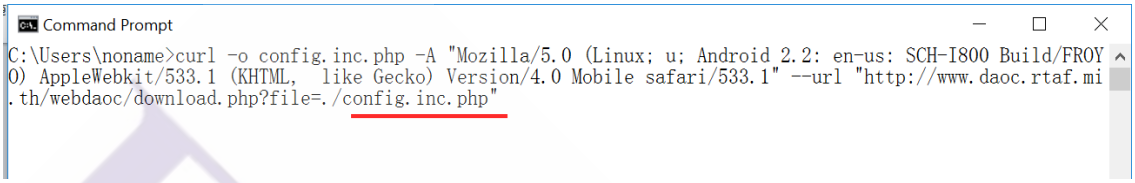
จากการอ่านไฟล์ auth.inc.php พบว่ามีการอ้างถึงไฟล์ config.inc.php ซึ่งเป็นไฟล์ที่เกี่ยวข้องกับการตั้งค่าของระบบฐานข้อมูลของเว็บไซต์ที่ทำการทดสอบ ตามภาพที่ 3.17



ภาพที่ 3.17 รายละเอียดของข้อมูลที่อยู่ในไฟล์ auth.inc.php

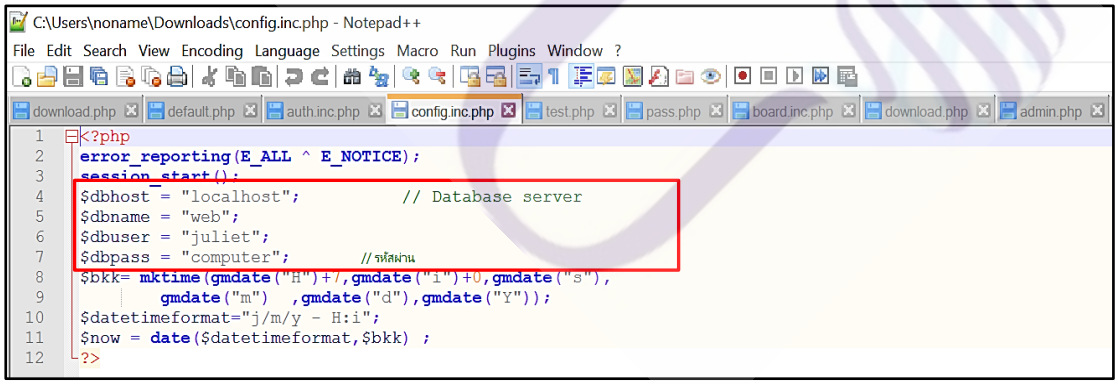
จากนั้นดาวน์โหลดไฟล์ config.inc.php เพื่อดูข้อมูลที่อยู่ภายใน ด้วยคำสั่งดังแสดงตามภาพที่ 3.18

```
curl -o config.inc.php -A “Mozilla/5.0 (Linux; u; Android 2.2: en-us: SCH-I800 Build/FROYO) AppleWebkit/533.1 (KHTML,  like Gecko) Version/4.0 Mobile safari/533.1” --url “http://www.daoc.rtaf.mi.th/webdaoc/download.php?file=./config.inc.php”
```



ภาพที่ 3.18 คำสั่งดาวนโหลดไฟล์ config.inc.php

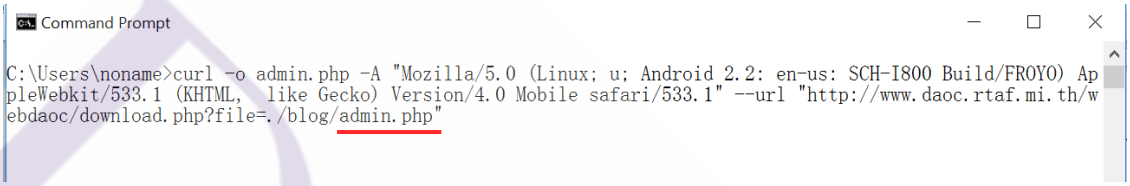
เมื่ออ่านไฟล์ config.inc.php พบว่าเป็นไฟล์ที่ใช้ติดต่อกับระบบฐานข้อมูลของเว็บไซต์ ภายในเป็นข้อมูลรหัสผ่านสำหรับเข้าใช้งานระบบฐานข้อมูลของเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ ซึ่งไฟล์ดังกล่าวเป็นไฟล์ที่มีความสำคัญต่อระบบฐานข้อมูลของเว็บไซต์ ถ้าผู้ไม่ประสงค์ดีสามารถนำไฟล์นี้ออกไปจากเว็บเซิร์ฟเวอร์ได้ ก็สามารถเข้าถึงระบบฐานข้อมูลของเว็บไซต์และเข้าไปสร้างความเสียหายให้แก่เว็บไซต์ได้ ตามภาพที่ 3.19



ภาพที่ 3.19 ข้อมูลรหัสผ่านสำหรับเข้าใช้งานระบบฐานข้อมูล

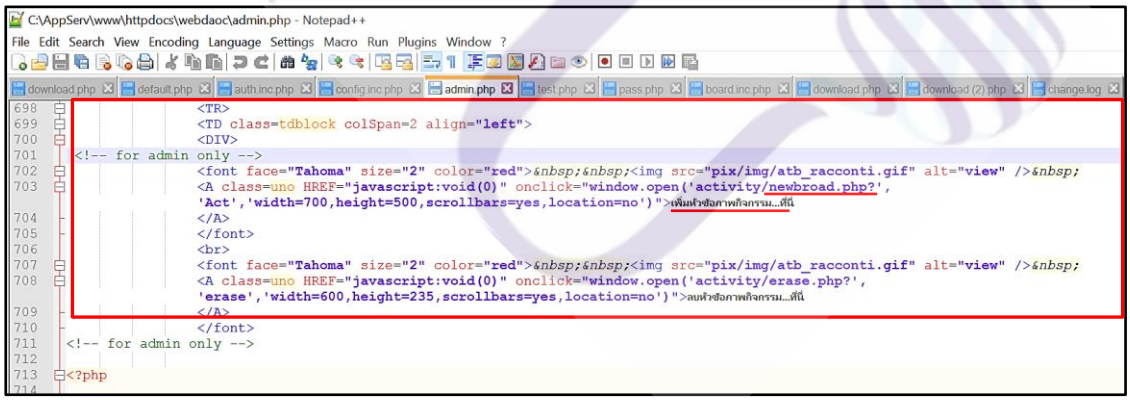
ทดลองดาวน์โหลดไฟล์ admin.php ซึ่งเป็นไฟล์ที่ผู้วิจัยสันนิษฐานว่าน่าจะเป็นไฟล์ที่มีอยู่ในเซิร์ฟเวอร์และเป็นไฟล์ที่คาดว่าจะสามารถนำไปใช้ประโยชน์ได้ ตามภาพที่ 3.20

```
curl -o admin.php -A “Mozilla/5.0 (Linux; u; Android 2.2: en-us: SCH-I800 Build/FROYO)
AppleWebkit/533.1 (KHTML,  like Gecko) Version/4.0 Mobile safari/533.1” --url
“http://www.daoc.rtaf.mi.th/webdaoc/download.php?file=./blog/admin.php”
```



ภาพที่ 3.20 คำสั่งดาวน์โหลดไฟล์ admin.php

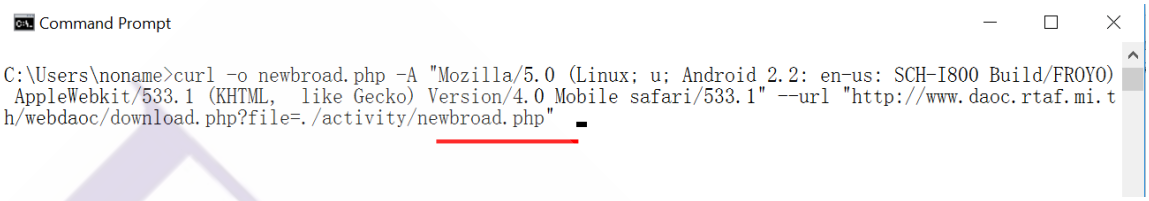
จากนั้นอ่านซอร์สโค้ดของไฟล์ admin.php พบว่าไฟล์มีการอ้างอิงถึงไฟล์ที่สามารถเข้าไปเพิ่มข้อมูลในเว็บไซต์ได้ คือไฟล์ที่ชื่อว่า newbroad.php และภายในไฟล์ admin.php มีการเขียนคอมเมนต์บอกให้รู้ว่าไฟล์นี้มีความสำคัญกับ admin ตามภาพที่ 3.21



ภาพที่ 3.21 รายละเอียดข้อมูลภายในไฟล์ admin.php

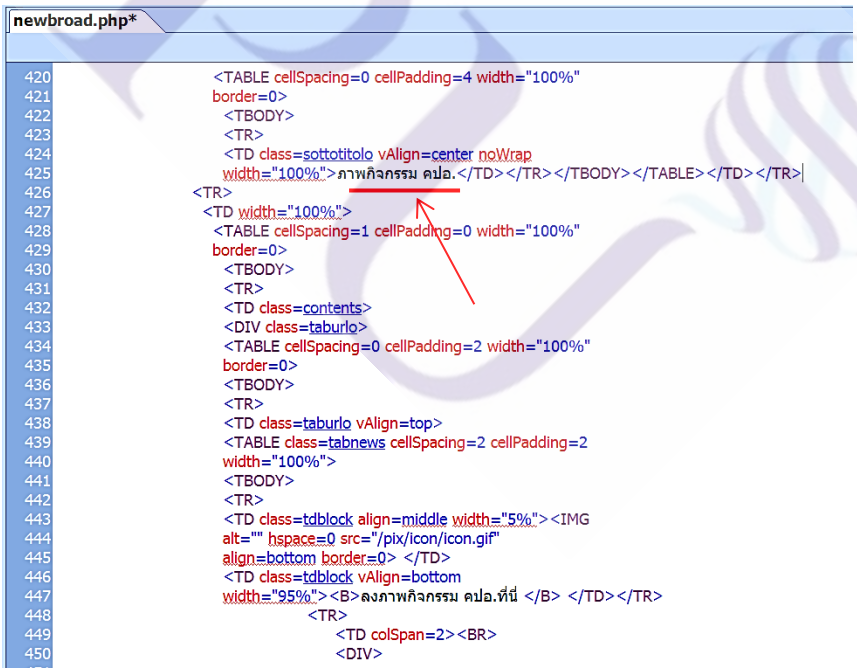
จากนั้นดาวน์โหลดไฟล์ newbroad.php เพื่อดูรายละเอียดที่อยู่ภายใน ตามภาพที่ 3.22

```
curl -o newbroad.php -A “Mozilla/5.0 (Linux; u; Android 2.2: en-us: SCH-I800 Build/FROYO)
AppleWebkit/533.1 (KHTML,  like Gecko) Version/4.0 Mobile safari/533.1” --url
“http://www.daoc.rtaf.mi.th/webdaoc/download.php?file=./activity/newbroad.php”
```



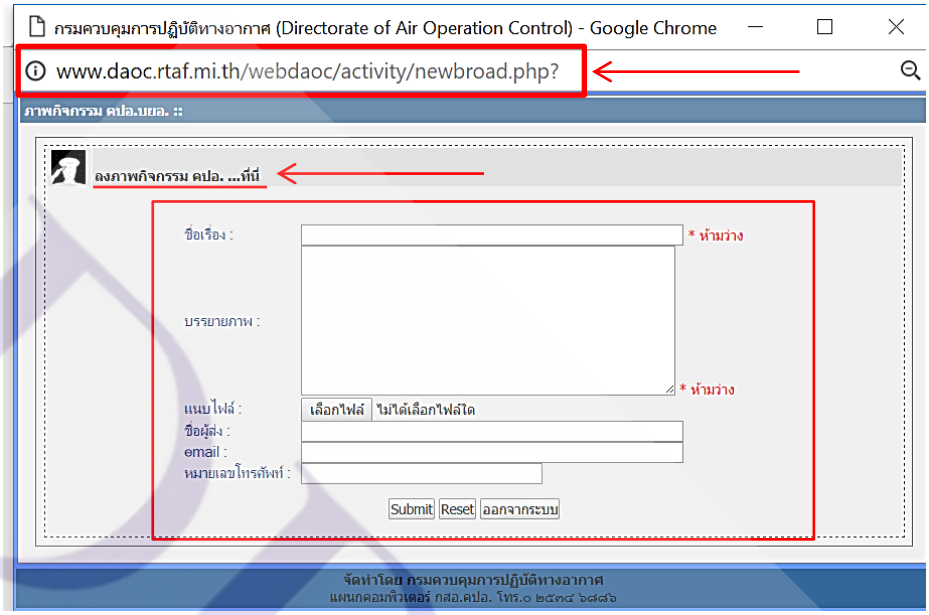
ภาพที่ 3.22 คำสั่งดาวน์โหลดไฟล์ newbroad.php

เมื่ออ่านไฟล์ newbroad.php พบว่าเป็นไฟล์ที่ใช้สำหรับอัพโหลดข้อมูลภาพกิจกรรมขึ้นไปบนหน้าเว็บไซต์ จากรายละเอียดข้อมูลของซอสโค้ดที่อยู่ภายในไฟล์ดังกล่าว ทำให้ผู้วิจัยค้นพบช่องทางในการทดลองอัพโหลดไฟล์ต่าง ๆ เข้าขึ้นสู่เว็บไซต์ รายละเอียดแสดงตามภาพที่ 3.23



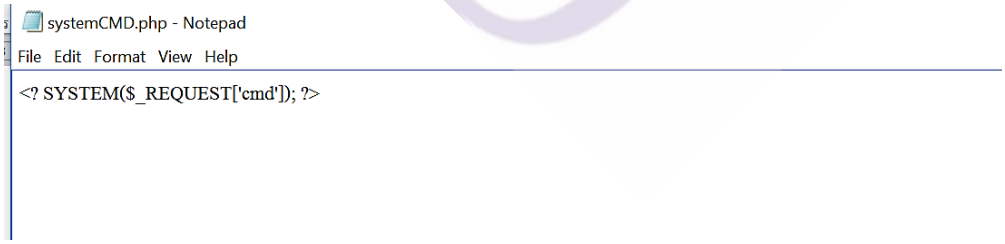
ภาพที่ 3.23 รายละเอียดข้อมูลภายในไฟล์ newbroad.php

จากนั้นจึงเรียกไฟล์ newbroad.php ผ่านเว็บบราวซ์เซอร์ เพื่อทดสอบการเข้าถึงหน้าเพจ newbroad.php ซึ่งเป็นหน้าที่ใช้ในการอัพโหลดข้อมูลขึ้นสู่หน้าเว็บไวต์ พบว่าสามารถเข้าถึงช่องทางการอัพโหลดข้อมูลขึ้นบนเว็บไซต์ได้โดยไม่ผ่านการยืนยันตัวตน ตามภาพที่ 3.24

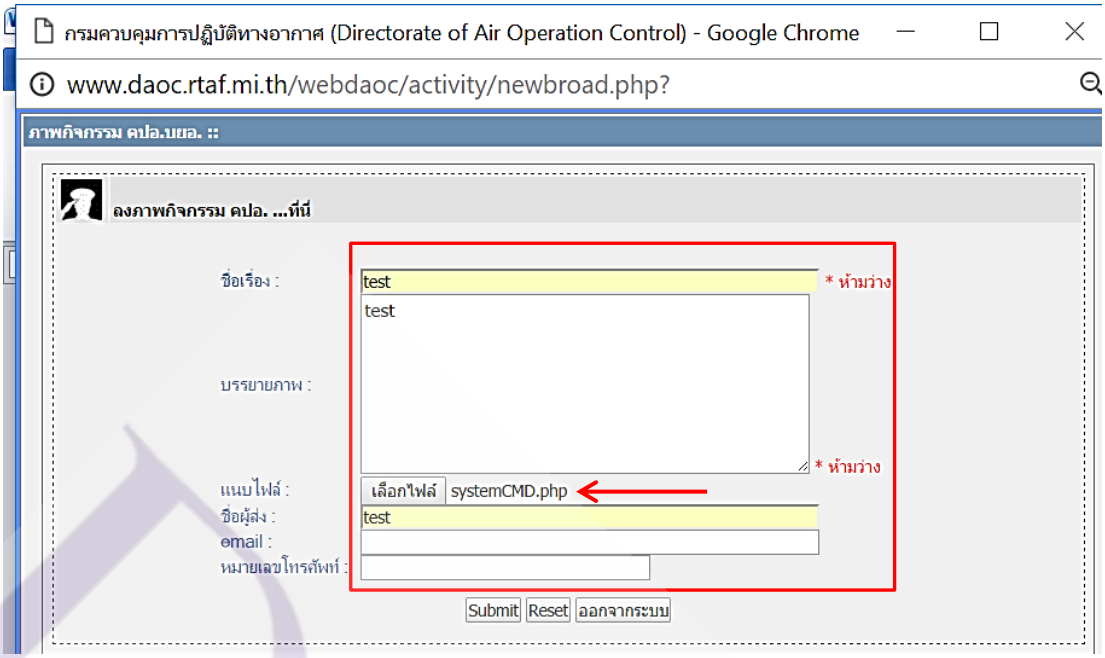


ภาพที่ 3.24 ช่องทางในการอัพโหลดไฟล์ขึ้นหน้าเว็บไซต์

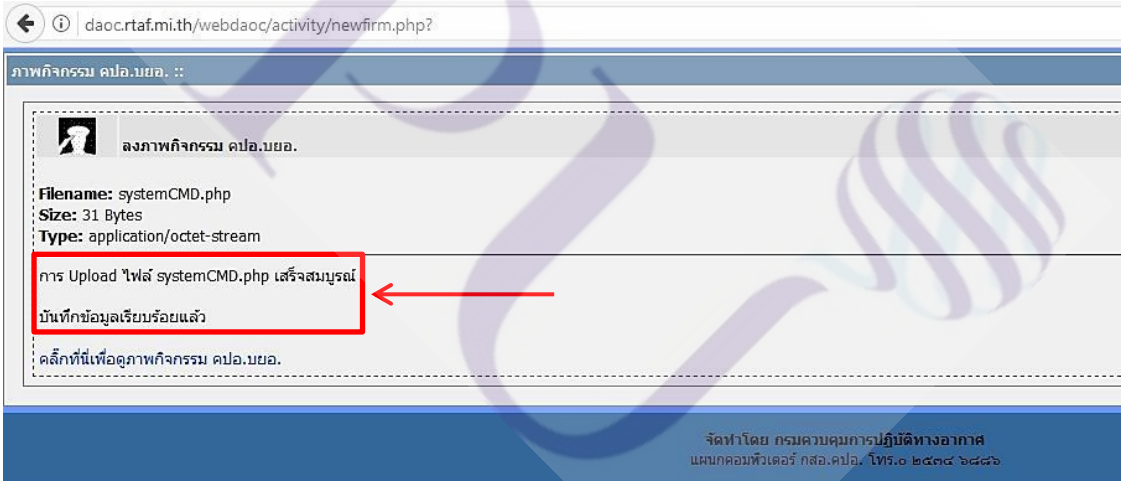
จากนั้นทำการสร้างไฟล์ systemCMD.php ซึ่งเป็นไฟล์ที่ผู้วิจัยสร้างขึ้นเพื่อให้รอรับคำสั่ง Dos เช่น คำสั่งดูไฟล์ (dir) คำสั่งตรวจสอบผู้ในระบบ (net user) ขึ้นไปบนเซิร์ฟเวอร์ พบว่าสามารถอัพโหลดไฟล์ได้สำเร็จ รายละเอียดตามภาพที่ 3.25 – 3.29



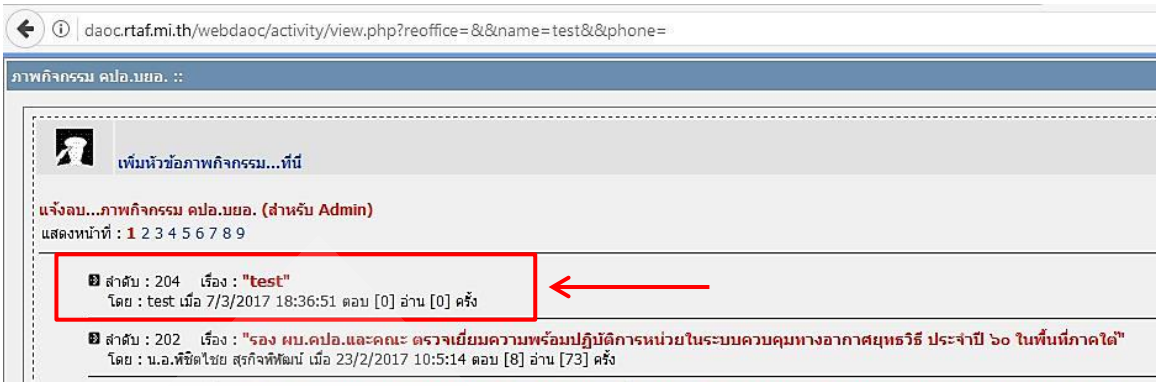
ภาพที่ 3.25 คำสั่งภายใน systemCMD.php



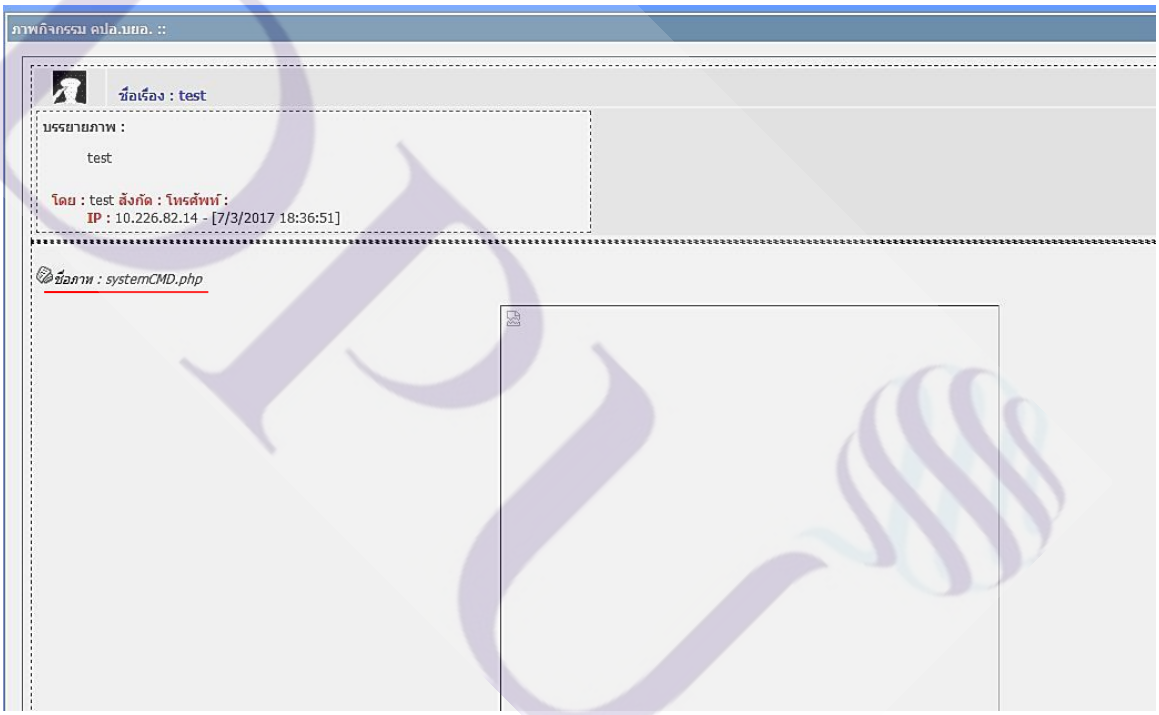
ภาพที่ 3.26 การอัพโหลดไฟล์ขึ้นเซิร์ฟเวอร์



ภาพที่ 3.27 การอัพโหลดไฟล์ system.CMD.php เสร็จสมบูรณ์



ภาพที่ 3.28 การอัพโหลดไฟล์ system.CMD.php เสร็จสมบูรณ์

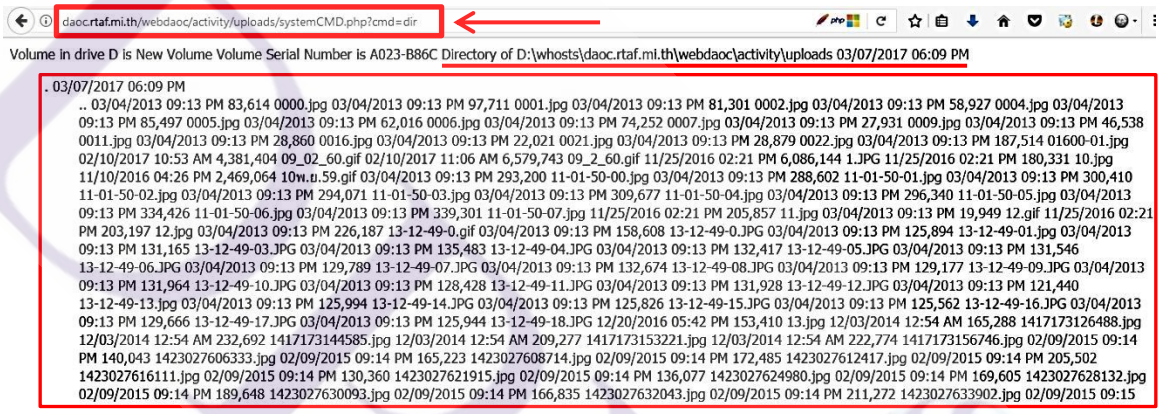


ภาพที่ 3.29 การอัพโหลดไฟล์ system.CMD.php เสร็จสมบูรณ์

จากนั้นเรียกใช้ไฟล์ systemCMD.php ผ่านเว็บเบราว์เซอร์ เพื่อทดสอบว่าไฟล์ดังกล่าวที่อัพโหลดขึ้นไปบนเว็บเซิร์ฟเวอร์สามารถใช้งานได้หรือไม่ พบว่าเว็บเซิร์ฟเวอร์มีการแจ้งเตือนว่าไม่สามารถประมวลผลคำสั่งที่เป็นค่าว่างได้ เนื่องจากผู้วิจัยยังไม่ได้พิมพ์คำสั่งใด ๆ ลงในเว็บเบราว์เซอร์ รายละเอียดดังแสดงตามภาพที่ 3.30

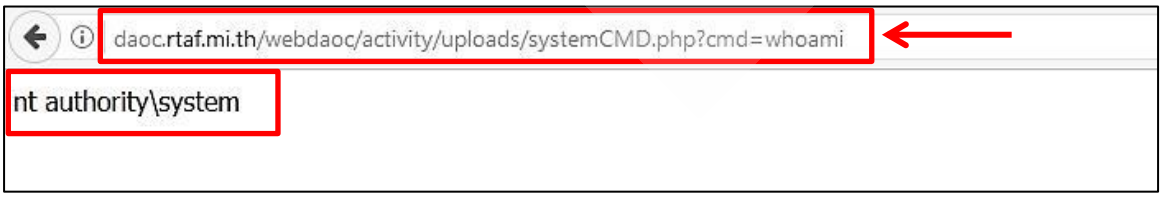
ภาพที่ 3.30 เรียกใช้งานไฟล์ system.php ผ่านเว็บเบราว์เซอร์

จากนั้นผู้วิจัยจึงทดลองใช้คำสั่งเรียกดูไฟล์ที่อยู่ในเซิร์ฟเวอร์ด้วยคำสั่ง “dir” พบว่าสามารถเรียกดูไฟล์ทั้งหมดที่อยู่บนเครื่องเซิร์ฟเวอร์ได้ รายละเอียดดังแสดงตามภาพที่ 3.31



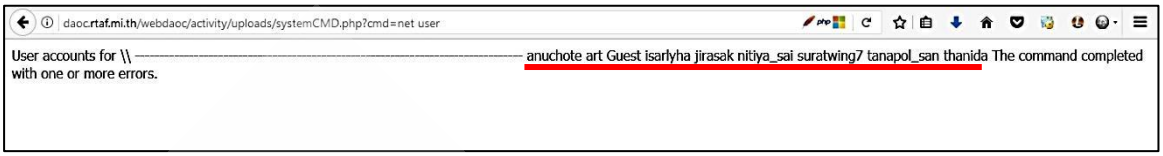
ภาพที่ 3.31 ข้อมูลของไฟล์ที่อยู่ในเครื่องเซิร์ฟเวอร์

จากนั้นผู้วิจัยได้ทำการตรวจสอบสิทธิ์การใช้งานบนเซิร์ฟเวอร์ด้วยคำสั่ง “whoami” พบว่าได้รับสิทธิการใช้งานเครื่องเซิร์ฟเวอร์เป็น “system” ซึ่งเป็นสิทธิ์สูงสุดสามารถเข้าไปจัดการกับเครื่องเซิร์ฟเวอร์ได้ ดังแสดงตามภาพที่ 3.32



ภาพที่ 3.32 การตรวจสอบสิทธิ์การใช้งานบนเซิร์ฟเวอร์ด้วยคำสั่ง “whoami”

จากนั้นผู้วิจัยได้ทำการตรวจสอบชื่อผู้ใช้งาน(User) ที่มีสิทธิ์เข้าถึงเครื่องเซิร์ฟเวอร์ด้วยคำสั่ง“net user” ทำให้พบรายชื่อผู้มีสิทธิ์เข้าใช้งานทั้งหมดที่มีสิทธิ์เข้าถึงเครื่องเซิร์ฟเวอร์ รายละเอียดดังแสดงตามภาพที่ 3.33



ภาพที่ 3.33 การตรวจสอบชื่อผู้มีสิทธิ์เข้าถึงเครื่องเซิร์ฟเวอร์

จากผลการทดสอบการเจาะระบบเว็บไซต์กรณีศึกษาเว็บไซต์ กรมควบคุมการปฏิบัติทางอากาศ พบว่าสามารถนำช่องโหว่ที่ตรวจพบจากขั้นตอนการสแกนหาช่องโหว่ของเว็บไซต์มาใช้ประโยชน์ในการทดสอบเจาะระบบเว็บไซต์ได้ ซึ่งการทดสอบดังกล่าวแสดงให้เห็นถึงความรุนแรงของช่องโหว่ของเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ ซึ่งถ้าผู้ไม่ประสงค์ดีรู้ช่องโหว่ก็สามารถนำช่องโหว่นี้ไปใช้ในการโจมตีเว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศ และสามารถเข้าถึงเว็บเซิร์ฟเวอร์ได้ หากผู้ไม่ประสงค์ดีสามารถเข้าถึงเว็บเซิร์ฟเวอร์ได้ ก็สามารถเข้าไปโจมตีหรือสร้างความเสียหายให้กับเว็บไซต์อื่น ๆ ที่อยู่ในโดเมนเดียวกัน รวมถึงสามารถเข้าไปสร้างความเสียหายให้กับเซิร์ฟเวอร์ได้ โดยรายละเอียดความรุนแรงของช่องโหว่ที่ตรวจพบสามารถอธิบายได้ในหัวข้อที่ 3.3

3.3 การวิเคราะห์ความรุนแรงของช่องโหว่และการประเมินความเสี่ยง (Vulnerability and Risk Analysis) [12]

จากผลการทดสอบการเจาะระบบเว็บไซต์ กรณีศึกษาเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ ผู้วิจัยได้นำช่องโหว่ที่ตรวจพบมาทำการวิเคราะห์ความรุนแรงของช่องโหว่และประเมินความเสี่ยงตามแนวทางที่ได้กล่าวไว้ในบทที่ 2 โดยมีรายละเอียดดังแสดงในตารางที่ 3.1

ตารางที่ 3.1 การวิเคราะห์ความรุนแรงของช่องโหว่ที่ตรวจพบ

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

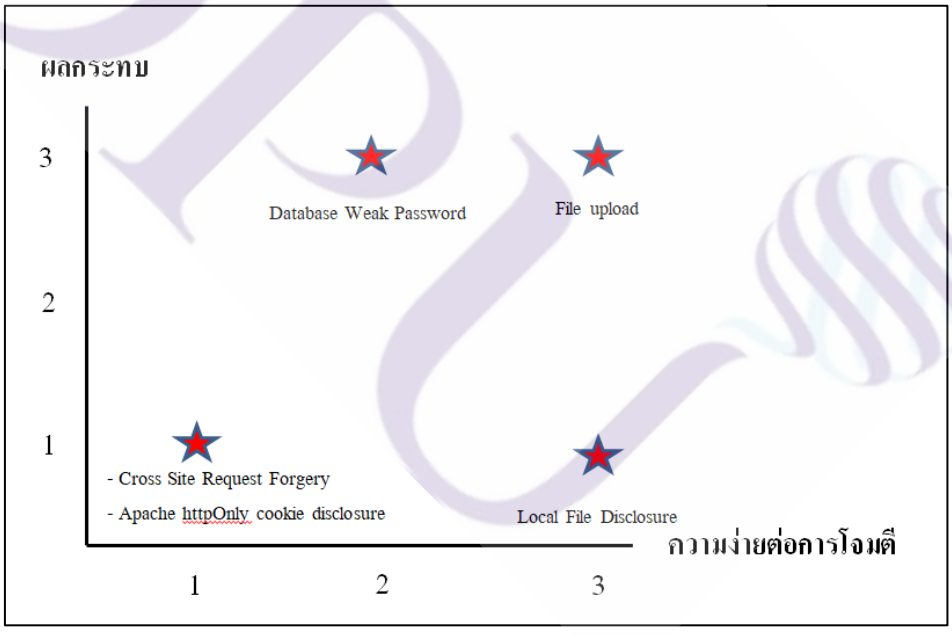
3.3.1 สรุปข้อมูลของช่องโหว่ที่ตรวจพบ

จากการวิเคราะห์ความรุนแรงของช่องโหว่และการประเมินความเสี่ยง กรณีศึกษาเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ สามารถสรุปได้ว่า พบช่องโหว่ทั้งสิ้น จำนวน 5 ช่องโหว่ สามารถจำแนกระดับความรุนแรงของช่องโหว่ได้ ดังแสดงตามตารางที่ 3.2

ตารางที่ 3.2 จำนวนของช่องโหว่ที่ตรวจพบและระดับความเสี่ยง

ระดับความเสี่ยง	สูง	กลาง	ต่ำ
จำนวนช่องโหว่	1	1	3

จากข้อมูลในตารางที่ 3.1 แสดงเป็นแผนภูมิได้ตามภาพที่ 3.34



ภาพที่ 3.34 ผลการวิเคราะห์ความรุนแรงของช่องโหว่

บทที่ 4
ผลลัพธ์จากการดำเนินการ

จากผลการตรวจหาช่องโหว่ของเว็บไซต์ กรณีศึกษาเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ พบว่าเว็บไซต์ดังกล่าวมีช่องโหว่ที่ทำให้ผู้ไม่ประสงค์ดีสามารถนำช่องโหว่ไปใช้ประโยชน์ในการโจมตีเว็บไซต์ดังกล่าวได้ จากผลการศึกษาในบทที่ 3 ผู้วิจัยได้ค้นพบแนวทางการแก้ไขและการป้องกันช่องโหว่ที่ตรวจพบโดยได้จัดทำเป็นรายงานให้กับผู้เกี่ยวข้องได้นำไปแก้ไข โดยมีรายละเอียดตามหัวข้อที่ 4.1

4.1 รายงานวิธีการแก้ไขและการป้องกันช่องโหว่ (Report how to fix and prevent vulnerabilities)

ผู้วิจัยได้จัดทำรายงานการวิธีการแก้ไขและการป้องกันช่องโหว่ให้กับผู้เกี่ยวข้องได้นำไปแก้ไข ซึ่งในรายละเอียดของรายงานดังกล่าวสามารถให้คำแนะนำเกี่ยวกับวิธีการแก้ไขช่องโหว่และแนวทางการป้องกันสำหรับเว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศโดยมีรายละเอียดดังแสดงตามตารางที่ 4.1

ตารางที่ 4.1 รายงานวิธีการแก้ไขและการป้องกันช่องโหว่ (Report how to fix and prevent vulnerabilities)

ลำดับ	ช่องโหว่	ระดับความเสี่ยง	วิธีแก้ไขและแนวทางการป้องกัน
1	File upload	สูง	1A : เพิ่มหน้ายืนยันตัวตนสำหรับผู้ดูแลระบบก่อนเข้าไปจัดการกิจกรรมต่างๆบนหน้าเว็บไซต์ 1B : เพิ่มการตรวจสอบไฟล์ที่จะอัพโหลดให้อัพโหลดได้เฉพาะไฟล์ที่ต้องการให้อัพโหลดเท่านั้น เช่นไฟล์ รูปภาพ (.jpeg, .gif, .png) เท่านั้น

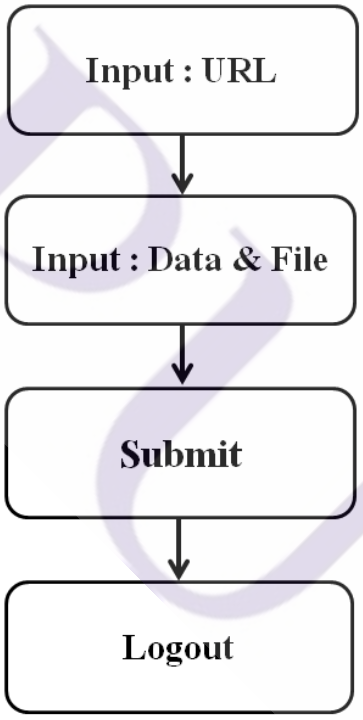
2	Local File Disclosure	ต่ำ	2A: ยกเลิกการใช้ไฟล์ download.php ซึ่งเป็นไฟล์ที่อนุญาตให้ผู้ใช้สามารถดาวน์โหลดไฟล์ต่างๆ ที่อยู่บนเว็บเซิร์ฟเวอร์ได้จากหน้าเว็บไซต์ 2B : ตั้งค่าการดาวน์โหลดไฟล์ ให้เป็นแบบ static คือ ในขั้นตอนเขียนโค้ดให้อ้างอิงไฟล์ที่ต้องการให้ดาวน์โหลดโดยตรง โดยไม่ต้องผ่านซอสโค้ดของไฟล์ download.php
3	Cross Site Request Forgery	ต่ำ	แก้ไขด้วยวิธีการอัพเดทเวอร์ชั่นของเว็บเซิร์ฟเวอร์ จาก Apache เวอร์ชั่น 2.2.8 ซึ่งเป็นเวอร์ชั่นที่เก่า ให้เป็น Apache เวอร์ชั่น 2.2.22 ขึ้นไปซึ่งเป็นเวอร์ชั่นที่ได้รับการแก้ไขช่องโหว่ดังกล่าวเรียบร้อยแล้ว
4	Apache httpOnly cookie disclosure	ต่ำ	แก้ไขด้วยวิธีการอัพเดทเวอร์ชั่นของเว็บเซิร์ฟเวอร์ จาก Apache เวอร์ชั่น 2.2.8 ซึ่งเป็นเวอร์ชั่นที่เก่า ให้เป็น Apache เวอร์ชั่น 2.2.22 ขึ้นไปซึ่งเป็นเวอร์ชั่นที่ได้รับการแก้ไขช่องโหว่ดังกล่าวเรียบร้อยแล้ว
5	Database Weak Password	ปานกลาง	เปลี่ยนรหัสผ่านของฐานข้อมูลให้มีความแข็งแรงดังนี้ 1. รหัสผ่านควรจะประกอบด้วย อักษรพิมพ์ใหญ่, พิมพ์เล็ก, ตัวเลข และอักขระพิเศษ 2. รหัสผ่านยากต่อการคาดเดา (Brute force) 3. ความยาวของรหัสผ่านไม่น้อยกว่า 8 ตัวอักษร 4. ไม่ใช้ข้อมูลที่เป็นส่วนตัวหรือข้อมูลที่เป็นสาธารณะ เช่น หมายเลขบัตรประชาชน หมายเลขโทรศัพท์ วัน เดือน ปีเกิด ทะเบียนรถ เป็นต้น 5. ใช้รหัสผ่านแยกกับบริการอื่น เช่น บัญชีอีเมล์หรือบริการอื่น ๆ

			6. จำกัดสิทธิ์การเข้าถึงฐานข้อมูลโดยอนุญาตให้เข้าถึงได้เฉพาะเว็บเซิร์ฟเวอร์ของกรมควบคุมการปฏิบัติทางอากาศเท่านั้น

4.2 การแก้ไขช่องโหว่

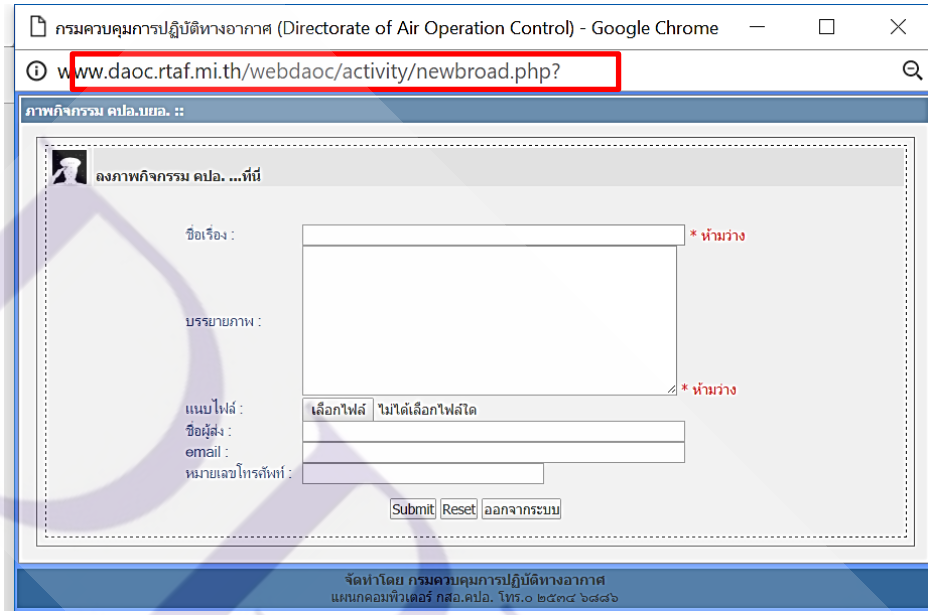
4.2.1 ช่องโหว่ File upload

จากเดิมผู้ดูแลเว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศใช้ช่องทางการเข้าไปอัพโหลดข้อมูลขึ้นสู่เว็บไซต์ โดยการพิมพ์ URL ที่อยู่ของไฟล์ที่ใช้ในการอัพโหลดข้อมูลขึ้นสู่เว็บไซต์ แล้วกรอกข้อมูลที่ต้องการอัพโหลดพร้อมแนบไฟล์ที่ต้องการอัพโหลด แล้วกดปุ่มยืนยัน จากนั้นออกจากระบบ โดยมีขั้นตอนการทำงานดังแสดงตามภาพที่ 4.1



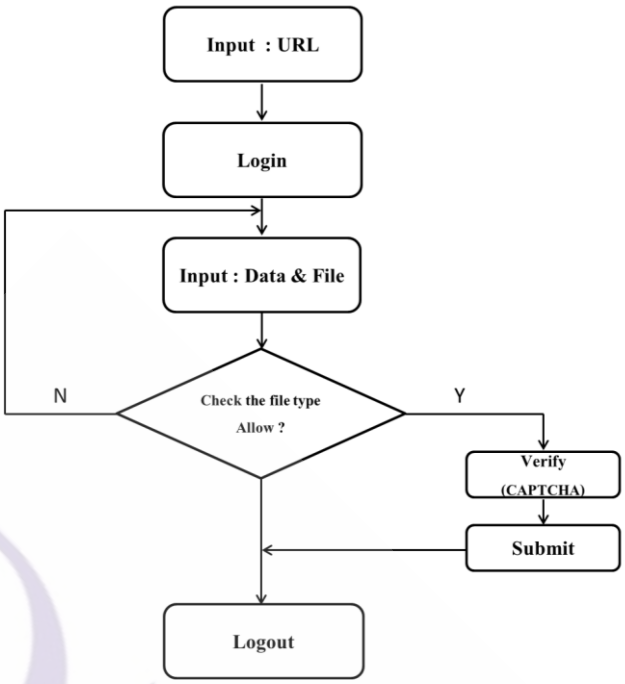
ภาพที่ 4.1 ขั้นตอนการอัพโหลดข้อมูลขึ้นสู่เว็บแบบเดิม

ซึ่งขั้นตอนดังกล่าวข้างต้นสามารถเข้าถึงได้โดยไม่ผ่านการยืนยันตัวตน และไม่มีการตรวจสอบชนิดของไฟล์ที่อัพโหลด ทำให้แฮกเกอร์สามารถใช้ช่องทางนี้ในการโจมตีเว็บไซต์และเว็บเซิฟร์เวอร์ให้เกิดความเสียหายได้ โดยวิธีการเข้าไปอัพโหลดข้อมูลขึ้นสู่เว็บไซต์แบบเดิมนั้นแสดงตามภาพที่ 4.2



ภาพที่ 4.2 ช่องทางการอัพโหลดข้อมูลขึ้นสู่เว็บด้วยแบบเดิม

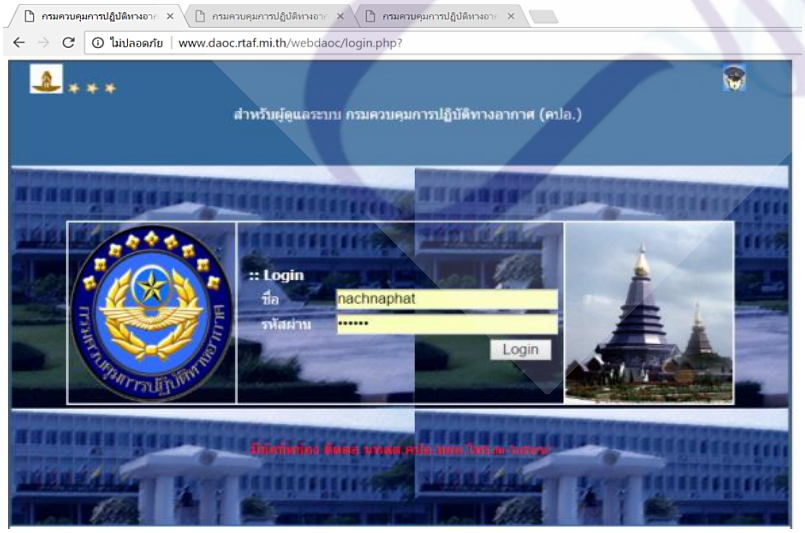
ผู้ดูแลเว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศได้ดำเนินการแก้ไขช่องโหว่ File upload โดยการเพิ่มขั้นตอนการยืนยันตัวตนก่อนเข้าถึงขั้นตอนการอัพโหลดข้อมูลขึ้นสู่เว็บไซต์, เพิ่มขั้นตอนการตรวจสอบชนิดของไฟล์ที่ต้องการอัพโหลดโดยอนุญาตให้อัพโหลดได้เฉพาะไฟล์รูปภาพ (.jpg, .gif, .png) เท่านั้น และเพิ่มเทคนิคที่ใช้ในการทดสอบผู้ใช้บริการว่าเป็นมนุษย์จริงๆ ไม่ใช่โปรแกรมอัตโนมัติ (bot) (CAPTCHA) โดยมีกระบวนการทำงานดังแสดงตามภาพที่ 4.3



ภาพที่ 4.3 ขั้นตอนการอัพโหลดข้อมูลขึ้นสู่เว็บแบบใหม่

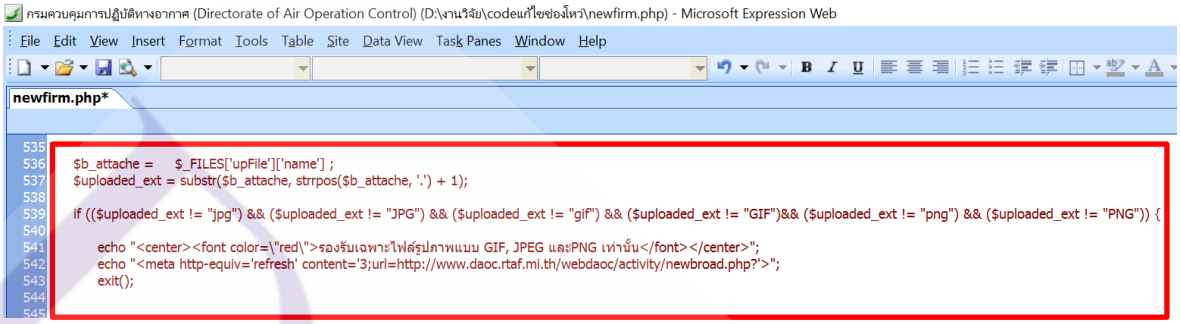
การแก้ไขช่องโหว่ File upload สามารถอธิบายได้ดังนี้

(1) แก้ไขโดยการเพิ่มหน้ายืนยันตัวตนสำหรับผู้ดูแลระบบก่อนเข้าไปจัดการกิจกรรมต่างๆบนหน้าเว็บไซต์ เพื่อเป็นการป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าถึงระบบจัดการหน้าเว็บไซต์ รายละเอียดแสดงตามภาพที่ 4.4



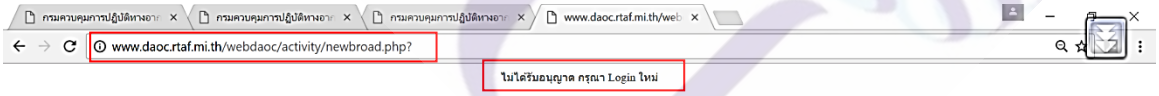
ภาพที่ 4.4 หน้าเพจการยืนยันตัวตนสำหรับผู้ดูแลเว็บไซต์

(2) เพิ่มซอร์สโค้ดตรวจสอบประเภทของไฟล์ที่จะอัพโหลด ให้อัพโหลดได้เฉพาะไฟล์รูปภาพ (.jpeg, .gif, .png) เท่านั้น หากมีการอัพโหลดไฟล์ที่ไม่ได้รับอนุญาต ระบบจะแจ้งเตือนว่า “รองรับเฉพาะไฟล์รูปภาพแบบ JPG, GIF, PNG เท่านั้น” เพื่อเป็นการป้องกันไม่ให้ผู้ไม่ประสงค์ดีอัพโหลดไฟล์ที่เป็นอันตรายขึ้นสู่เว็บไซต์และเว็บเซิร์ฟเวอร์ รายละเอียดของซอร์สโค้ดแสดงตามภาพที่ 4.5



ภาพที่ 4.5 การเพิ่มซอร์สโค้ดเพื่อตรวจสอบประเภทของไฟล์ที่อัพโหลด

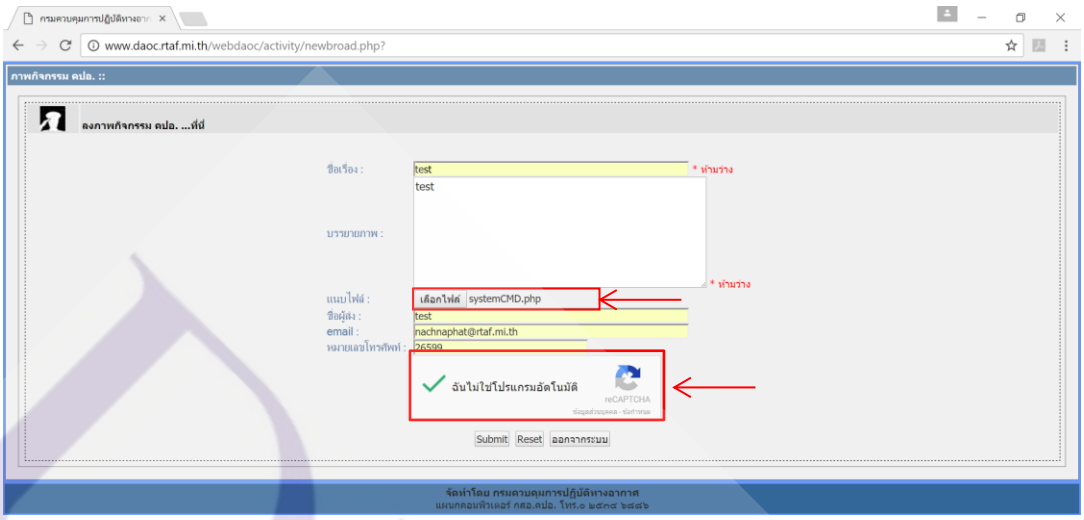
หลังจากที่ได้ทำการแก้ไขช่องโหว่ File uploadแล้ว ผู้วิจัยจึงได้ทำการตรวจสอบช่องโหว่ดังกล่าวอีกครั้งโดยการเข้าถึงหน้าเพจ “newbroad.php” ซึ่งเป็นหน้าเพจที่ผู้ดูแลเว็บไซต์ใช้ในการอัพโหลดภาพกิจกรรมขึ้นสู่หน้าเว็บไซต์ โดยไม่ผ่านการยืนยันตัวตน พบว่าไม่สามารถเข้าถึงหน้าเพจดังกล่าวได้ รายละเอียดดังแสดงตามภาพที่ 4.6



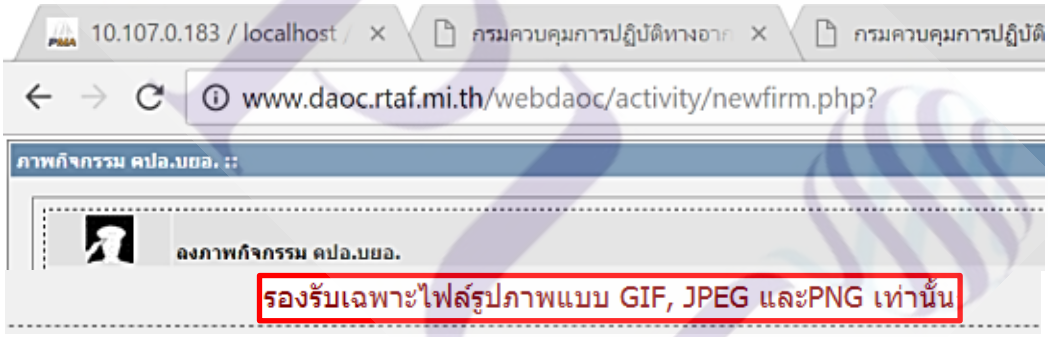
ภาพที่ 4.6 การเข้าถึงหน้าเพจ “newbroad.php”

หลังจากที่ได้ทำการแก้ไขช่องโหว่ File upload แล้วผู้วิจัยได้ทำการทดสอบช่องโหว่อีกครั้ง โดยการอัพโหลดไฟล์ “systemCMD.php” ขึ้นไปบนเว็บเซิร์ฟเวอร์ พบว่า ไม่สามารถอัพโหลดไฟล์ดังกล่าวขึ้นไปได้ โดยระบบได้มีการแจ้งเตือนว่า “ รองรับเฉพาะไฟล์รูปภาพแบบ JPG, GIF, PNG เท่านั้น ” รายละเอียดตามภาพ ที่ 4.7 – 4.8

นอกจากนี้ ผู้ดูแลเว็บไซต์ได้เพิ่มเทคนิคที่ใช้ในการทดสอบผู้ใช้บริการว่าเป็นมนุษย์จริงๆ ไม่ใช่โปรแกรมอัตโนมัติ (bot) (CAPTCHA) รายละเอียดตามภาพ ที่ 4.7



ภาพที่ 4.7 การอัพโหลดไฟล์ “systemCMD.php”

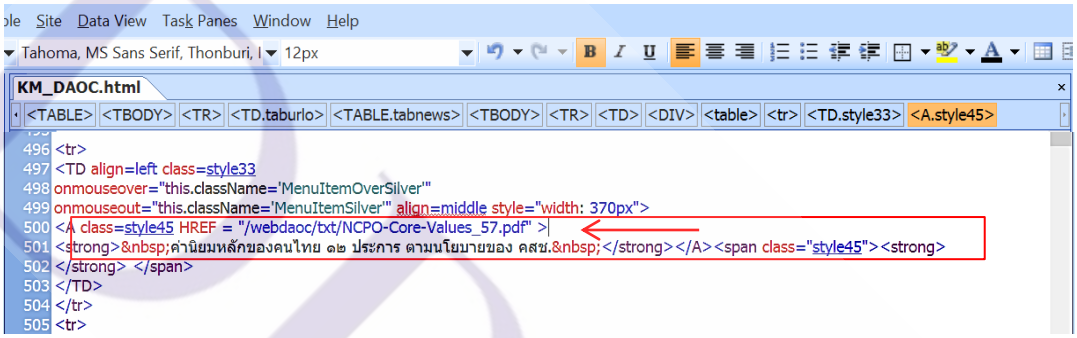


ภาพที่ 4.8 ผลลัพธ์ของการอัพโหลดไฟล์ “systemCMD.php”

4.2.2 ช่องโหว่ Local File Disclosure

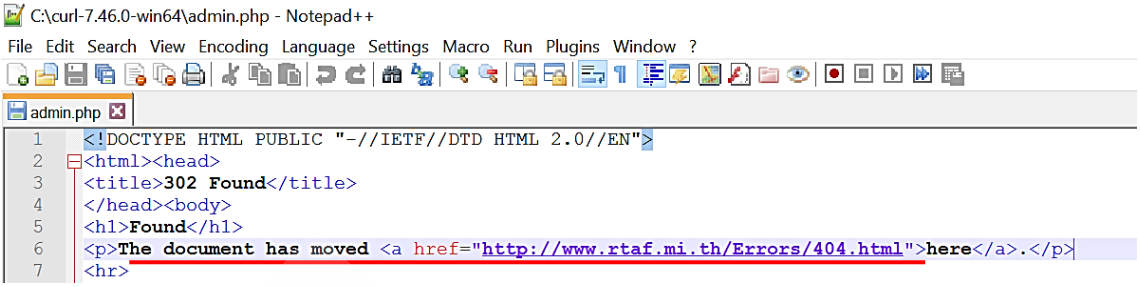
ผู้ดูแลเว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศได้แก้ไขช่องโหว่ Local File Disclosure โดยการยกเลิกการใช้ไฟล์ download.php ซึ่งเป็นไฟล์ที่เป็นช่องโหว่ของเว็บไซต์ โดยช่องโหว่นี้เป็นการเปิดทางให้แฮกเกอร์สามารถดึงไฟล์อื่นๆ ที่อยู่ในเว็บไซต์มารัน หรือ อ่านไฟล์ (อาทิเช่น ไฟล์ config หรือไฟล์เก็บ password ต่างๆ) โดยมีสาเหตุมาจากการที่ผู้พัฒนาเว็บไซต์ไม่

คำนึงถึงความปลอดภัยในการเขียนสคริป ทำให้แฮกเกอร์สามารถดาวน์โหลดไฟล์ที่สำคัญที่อยู่บนเครื่องเซิร์ฟเวอร์มาใช้ประโยชน์ในการโจมตีเว็บไซต์ได้ ซึ่งการดาวน์โหลดไฟล์จากเว็บไซต์นั้นไม่จำเป็นต้องผ่านไฟล์ download.php ก็สามารถดาวน์โหลดไฟล์ได้ โดยการตั้งค่าการดาวน์โหลดไฟล์ที่อนุญาตให้ผู้ใช้ดาวน์โหลด ให้เป็นแบบ static คือในขั้นตอนเขียนโค้ดให้อ้างอิงไปที่ไฟล์ที่อนุญาตให้ดาวน์โหลดโดยตรง โดยไม่ต้องผ่านซอสโค้ดของไฟล์ download.php เพื่อเป็นการปิดช่องโหว่ของเว็บไซต์ที่อนุญาตให้ผู้ใช้ดาวน์โหลดไฟล์อื่นๆ ที่ไม่ได้รับอนุญาตออกจากเครื่องเซิร์ฟเวอร์ได้ ทำให้ผู้ไม่ประสงค์ดีนำไฟล์ที่สำคัญไปใช้ประโยชน์ในการโจมตีเว็บไซต์และเว็บเซิร์ฟเวอร์ได้ รายละเอียดของการเขียนโค้ดให้ปลอดภัย แสดงตามภาพ ที่ 4.9



ภาพ ที่ 4.9 การตั้งค่าการดาวน์โหลดไฟล์แบบ static

หลังจากที่ผู้ดูแลเว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศได้ดำเนินการแก้ไขช่องโหว่ตามแนวทางที่ผู้วิจัยได้แนะนำแล้ว ผู้วิจัยได้ทำการทดลองใช้คำสั่งเดิมในขั้นตอนของบทที่ 3 ทำการดาวน์โหลดไฟล์ชื่อ admin.php ซึ่งเป็นไฟล์ที่เคยตรวจพบว่ามีช่องโหว่และผู้ไม่ประสงค์ดีสามารถนำข้อมูลของซอร์สโค้ดภายในไฟล์ดังกล่าวไปใช้ประโยชน์ในการโจมตีเว็บไซต์ได้ หลังจากที่ได้ทำการดาวน์โหลดไฟล์ออกมาเพื่ออ่านซอร์สโค้ดของไฟล์ พบว่าไฟล์ดังกล่าวไม่สามารถนำไปใช้ประโยชน์ได้ เนื่องจากภายในไฟล์ไม่ปรากฏข้อมูลซอร์สโค้ด แต่ระบบเว็บเซิร์ฟเวอร์ตอบข้อความกลับมาภายในไฟล์ admin.php ว่า “ Error 404” ซึ่งหมายถึง ไฟล์ที่เราพยายามจะเข้าถึงนั้นไม่มีอยู่บนเซิร์ฟเวอร์ จึงทำให้ไม่สามารถนำซอร์สโค้ดไปใช้ประโยชน์ในการโจมตีเว็บไซต์และเว็บเซิร์ฟเวอร์ของกรมควบคุมการปฏิบัติทางอากาศได้ รายละเอียดตามภาพที่ 4.10



ภาพที่ 4.10 รายละเอียดของไฟล์ admin.php

4.2.3 ช่องโหว่ Cross Site Request Forgery และ ช่องโหว่ Apache httpOnly cookie disclosure

ในส่วนของการแก้ไขช่องโหว่ Cross Site Request Forgery และ Apache httpOnly cookie ซึ่งเป็นช่องโหว่เกี่ยวข้องกับเว็บเซิร์ฟเวอร์ ที่ต้องแก้ไขโดยผู้ดูแลเว็บเซิร์ฟเวอร์ นั้น ผู้วิจัยได้ทำหนังสือแจ้งให้แก้ไขช่องโหว่ที่ตรวจพบไปยังหน่วยงานที่รับผิดชอบ ให้ดำเนินการแก้ไขช่องโหว่เรียบร้อยแล้ว ซึ่งอยู่ระหว่างดำเนินการแก้ไข

4.2.4 ช่องโหว่ Database Weak Password

ผู้ดูแลเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ ได้ปฏิบัติตามแนวทางการป้องกันการถูกโจมตีจากผู้ไม่ประสงค์ดี ตามที่ผู้วิจัยให้คำแนะนำเรียบร้อยแล้ว โดยการเปลี่ยนรหัสผ่านของฐานข้อมูลให้มีความแข็งแรง ยากต่อเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต

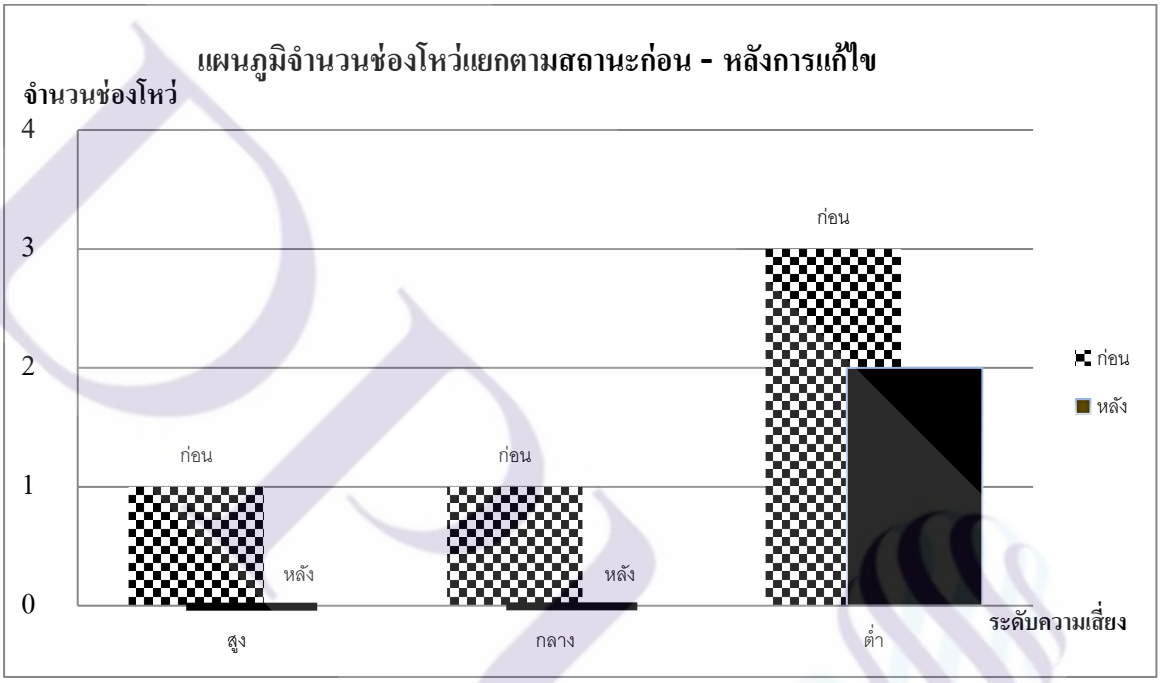
4.3 ผลลัพธ์ที่ได้จากการแก้ไขช่องโหว่ของเว็บไซต์

หลังจากที่ผู้วิจัยได้แจ้งไปยังผู้ดูแลเว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศให้ดำเนินการแก้ไขช่องโหว่ที่ตรวจพบแล้วนั้น ในส่วนของการแก้ไขช่องโหว่ที่เกี่ยวกับการพัฒนาเว็บไซต์นั้น ผู้ดูแลเว็บไซต์ได้ดำเนินการแก้ไขช่องโหว่ตามแนวทางที่ผู้วิจัยแนะนำ เรียบร้อยแล้ว และผู้วิจัยได้ทำการทดสอบอีกครั้ง พบว่า ช่องโหว่ดังกล่าวสามารถแก้ไขได้ แสดงให้เห็นว่า แนวทางการแก้ไขช่องโหว่ที่ผู้วิจัยแนะนำนั้นสามารถนำไปใช้ในการแก้ไขช่องโหว่ของเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศได้จริง

ทั้งนี้ ในส่วนของการแก้ไขช่องโหว่ของเว็บเซิร์ฟเวอร์ นั้น ผู้วิจัยได้ทำหนังสือแจ้งให้แก้ไขช่องโหว่ที่ตรวจพบ จำนวน 2 ช่องโหว่ ซึ่งตรวจพบโดยโปรแกรม Acunetix Web

Vulnerability Scanner ไปยังหน่วยงานที่รับผิดชอบ ให้ดำเนินการแก้ไขช่องโหว่เรียบร้อยแล้ว ซึ่งอยู่ระหว่างดำเนินการแก้ไข

ดังนั้น จึงสรุปได้ว่า จากผลการแก้ไขช่องโหว่ข้างต้น สามารถแก้ไขช่องโหว่ที่ตรวจพบได้แล้วจำนวนทั้งสิ้น 3 ช่องโหว่ และมีจำนวน 2 ช่องโหว่ ที่อยู่ระหว่างการดำเนินการแก้ไขจากผู้ดูแลระบบเว็บเซิร์ฟเวอร์ของกองทัพอากาศ ข้อมูลดังกล่าวสามารถสรุปได้ดังแสดงตามภาพที่ 4.11



ภาพที่ 4.11 แผนภูมิจำนวนช่องโหว่ของเว็บไซต์ก่อนและหลังจากได้รับการแก้ไข

บทที่ 5
บทสรุปและข้อเสนอแนะ

สารนิพนธ์นี้เป็นการศึกษาค้นคว้า เพื่อหาช่องโหว่หรือจุดอ่อนของเว็บไซต์กรณีศึกษาเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ ว่ามีช่องโหว่หรือจุดอ่อนหรือไม่ และช่องโหว่หรือจุดอ่อนนั้นมีระดับความรุนแรงและมีผลกระทบต่อเว็บไซต์อย่างไร เพื่อหาแนวทางการป้องกันการถูกโจมตีจากการใช้ประโยชน์จากช่องโหว่หรือจุดอ่อนของเว็บไซต์ดังกล่าว เพื่อใช้เป็นแนวทางในการพัฒนาเว็บไซต์ของกรมควบคุมการปฏิบัติทางอากาศให้มีความมั่นคง ปลอดภัย

5.1 สรุปผลการวิจัย

ผู้วิจัยสามารถเข้าใจถึงวิธีการหาช่องโหว่ของเว็บไซต์โดยการใช้เครื่องมือสำเร็จรูปที่แฮกเกอร์นิยมนำมาใช้ในการหาช่องโหว่ของเว็บไซต์ที่มีใช้งานอยู่ในปัจจุบัน และเข้าใจถึงขั้นตอนวิธีการหาช่องโหว่ของเว็บไซต์โดยวิธีวิธีการทดสอบเจาะระบบโดยผู้ทำการวิจัย รวมถึงวิธีการโจมตีโดยการใช้ประโยชน์จากช่องโหว่หรือจุดอ่อนของเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศที่ถูกตรวจพบโดยผู้ทำการวิจัย รวมทั้งสามารถหาวิธีในการแก้ไขช่องโหว่ที่ตรวจพบและสามารถหาแนวทางในการป้องกันไม่ให้เกิดช่องโหว่หรือจุดอ่อนของเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศได้ จึงทำให้เว็บไซต์มีความมั่นคงปลอดภัยมากขึ้น

5.2 แนวทางการพัฒนาต่อในอนาคต

5.2.1 ตรวจหาช่องโหว่หรือจุดอ่อนของเว็บไซต์ทั้งหมดที่อยู่ในเครื่องเซิร์ฟเวอร์เดียวกันเพื่อเป็นการป้องกันทั้งโดเมน

5.2.2 ตรวจหาช่องโหว่หรือจุดอ่อนของเว็บเซิร์ฟเวอร์โดยใช้วิธีการทดสอบเจาะระบบ (Penetration Testing) และพยายามค้นหาช่องโหว่ใหม่ๆ ทุกวิถีทางที่จะก่อให้เกิดภัยอันตรายต่อเว็บเซิร์ฟเวอร์

5.2.3 ใช้โปรแกรมสแกนช่องโหว่ที่ทันสมัย อย่างน้อย 3 โปรแกรมในการหาช่องโหว่ของเว็บไซต์และเว็บเซิร์ฟเวอร์

บรรณานุกรม

บรรณานุกรม

ภาษาไทย

กองนโยบายและแผน กรมเทคโนโลยีสารสนเทศและการสื่อสารกองทัพอากาศ 2559 : ออนไลน์

กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสาร ทหารอากาศ

จตุชัย แพงจันทร์, Master in Security 2nd Edition,2553

ธวัชชัย ชมศิริ, ความปลอดภัยของเว็บ, 2017

นายอานัฐชัย รังสิโรดม์โกมล , เครื่องมือทดสอบการเจาะระบบ Tool for Penetration test,2558

พรพรหม ประภากิตติกุล , รู้จักและป้องกันภัยจาก Website Defacement,2554

พลตรี ฤทธิ อินทราวุธ,ม.ป.ป.,น. 2

ระเบียบกองทัพอากาศ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ พ.ศ. 2552 : ออนไลน์

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

ภาษาอังกฤษ

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

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

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

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

ภาคผนวก

ภาคผนวก

1. หนังสือขออนุญาตใช้เว็บไซต์กรมควบคุมการปฏิบัติทางอากาศเพื่อทำการวิจัย
2. รายงานผลการตรวจพบช่องโหว่หรือจุดอ่อนของเว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ
3. หนังสือรายงานสรุปผลการประเมินและตรวจสอบความมั่นคงปลอดภัยระบบสารสนเทศของ คปอ.

ประวัติผู้เขียน

ชื่อ – สกุล	เรืออากาศตรีหญิง ณัชณภัทร ใจอดทน
ประวัติการศึกษา	พ.ศ.2552 คณะวิทยาศาสตร์ สาขาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยราชภัฏเทพสตรี
ตำแหน่งและสถานที่ทำงานปัจจุบัน	นายทหารเทคโนโลยีสารสนเทศและการสื่อสาร กรมควบคุมการปฏิบัติทางอากาศ