โครงการจ้างพัฒนาระบบงาน
บริหารจัดการคุณภาพหนี้เพื่อยกระดับการให้บริการ
(Enhance Debt Management Service)
ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร

งวดงานที่ 6
Non-Functional Test (NFT)
- รายงานผลการจัดการปิดช่องโหว่ (Vulnerability Test)

ditto DATA INTELLIGENCE บริษัท ดิทโต้ (ประเทศไทย) จำกัด (มหาชน)

ต้นฉบับ

ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร

รายงานผลการตรวจสอบความปลอดภัยของระบบ

การทดสอบหาช่องโหว่ Vulnerability Assessment

โครงการสัญญาจ้างพัฒนาระบบงานบริหารจัดการคุณภาพหนี้เพื่อยกระดับการให้บริการ

รายงานเมื่อ วันที่ 2 ธันวาคม พ.ศ. 2568

โครงการสัญญาจ้างพัฒนาระบบงานบริหารจัดการคุณภาพหนี้เพื่อยกระดับการให้บริการ

ชื่อเอกสาร :	รายงานผลการตรวจสอบความปลอดภัยของระบบ Vulnerability Assessment สัญญาจ้างพัฒนาระบบงานบริหารจัดการคุณภาพหนี้เพื่อยกระดับการให้บริการ	
คณะทำงาน :		
File name :	รายงานผลการตรวจสอบความปลอดภัยของระบบ Vulnerability assessment	
เลขที่ : 64006243	**Version no. :** 1.1	**Date :** 2 ธันวาคม 2568
ผู้เขียน : บริษัท บิซ โฟล์ค จำกัด		
ผู้ผลิตเอกสาร : บริษัท บิซ โฟล์ค จำกัด		
ประเภทเอกสาร :	**(/) เอกสารส่งมอบตามสัญญา** **( ) เอกสารภายในโครงการ** **( ) เอกสารส่งมอบเพิ่มเติม** **( ) รายงานประจำ** **( ) รายงานพิเศษ.....** **( ) อื่นๆ.....**	

Revision History

No.	Version (V.X.X)	Date of Change (YYYYMMDD)	A/M/D	Description of Change	Author
1	V1.0	20251110	A	Initial Version	Biz Folk
1	V1.1	20251202	M	Revised Version	Biz Folk

A = Added **M = Modified** **D = Deleted**

Project Sign off

บริษัท ดิตโต้ จำกัด (มหาชน)

ผู้จัดการโครงการ
2 ธันวาคม 2568

บริษัท บิซ โฟล์ค จำกัด

(ธนพล ไทรชมภู)
ผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์
2 ธันวาคม 2568

สารบัญ

สารบัญตาราง

สารบัญรูป

คำนำ

ความเป็นมา

ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร ซึ่งต่อไปนี้เรียกว่า “ธ.ก.ส.” มีความประสงค์จะบริหารจัดการลูกค้าที่ผิดนัดชำระหนี้อย่างมีประสิทธิภาพ เพื่อลดอัตราการเกิดหนี้เสียซึ่งกระทบกับต้นทุนโดยตรงและต้นทุนด้านความเสี่ยงของธนาคาร ความจำเป็นในการบริหารจัดการหนี้ด้วยกลยุทธ์ จากการวิเคราะห์ข้อมูลและเครื่องมือในการบริหารจัดการหนี้ที่เหมาะสมเป็นปัจจัยสำคัญที่จะช่วยปัญหาดังกล่าว ทางธนาคารสามารถใช้ทรัพยากร และบุคลากรที่มีอยู่ อย่างคุ้มค่าเพื่อลดความสูญเสียที่เกิดขึ้น โดยธนาคารสามารถบริหารจัดการหนี้ได้อย่างเป็นระบบและมีประสิทธิภาพ ปัจจุบันธนาคารได้ดำเนินโครงการพัฒนาระบบงานบริหารจัดการคุณภาพหนี้ (End To End Process) สำหรับช่วยงานในกระบวนการปรับปรุงโครงสร้างหนี้ที่กลุ่มลูกหนี้ที่เป็นหนี้ด้อยคุณภาพ (Non-Performing Loans: NPLs)

ธนาคารจึงได้มีแนวทางพัฒนาโครงการเพิ่มประสิทธิภาพระบบงานบริหารจัดการคุณภาพหนี้เพื่อยกระดับการให้บริการ (Enhance Debt Management Service) ซึ่งมีประกอบไปด้วย ระบบสามารถรองรับการทำงานได้ขณะมีสัญญาณอินเตอร์เน็ต (Online Mode) และไม่มีสัญญาณอินเตอร์เน็ต (Offline Mode) ให้สามารถทำผ่านช่องทางการให้บริการของธนาคาร เช่น ช่องทางคอมพิวเตอร์แท็บเล็ต (Tablet Computer) ของธนาคาร ช่องทางคอมพิวเตอร์บุคคล (Personal Computer) คอมพิวเตอร์โน้ตบุ๊ก (Laptop Computer) ของธนาคาร เชื่อมต่อกับฐานข้อมูลศูนย์ข้อมูลส่วนกลางของธนาคาร เพื่อให้สามารถจัดเก็บข้อมูลและการกำหนดตัวชี้วัดผลงาน (KPI) รวมถึงเชื่อมต่อกับระบบต่างๆ ของธนาคารได้ ด้วย API ที่เป็นอย่างน้อย โดยมีรายละเอียดขอบเขตของงาน (Terms of Reference: TOR) ตามที่แนบเอกสารฉบับนี้

วัตถุประสงค์ของโครงการ

1. เพื่อเพิ่มประสิทธิภาพระบบงานบริหารจัดการคุณภาพหนี้ สนับสนุนการขับเคลื่อนงานบริหารจัดการคุณภาพหนี้ให้บรรลุเป้าหมายตามอัตรากำหนด
2. เพื่อให้ธนาคารสามารถบริหารจัดการลูกหนี้ที่เป็นหนี้ด้อยคุณภาพได้อย่างมีประสิทธิภาพ
3. เพื่อสนับสนุนช่วยเจ้าหน้าที่ โดยการลดภาระค่าใช้จ่ายในการเดินทางมาติดต่อธนาคาร

บทที่ 1 บทนำ (Introduction)

1.1 ภาพรวมของการทดสอบ

การทดสอบหาช่องโหว่ (Vulnerability Assessment) เป็นกระบวนการที่มุ่งเน้นการประเมินความมั่นคงปลอดภัยของระบบ โดยอาศัยการจำลองรูปแบบการโจมตีระบบเพื่อค้นหาช่องโหว่และประเมินความทนทานของระบบต่อการโจมตีในสถานการณ์ใกล้เคียงของจริง การทดสอบลักษณะนี้มุ่งเน้นการวิเคราะห์พฤติกรรมจากมุมมองของผู้โจมตีที่มีเจตนามุ่งร้าย ทั้งการโจมตีโดยตรงและทางอ้อมเพื่อเข้าถึงข้อมูลที่สำคัญ การทดสอบดังกล่าวช่วยให้สามารถตรวจพบข้อบกพร่องและช่องโหว่ที่อาจเกิดขึ้นในระบบ เพื่อให้ผู้ดูแลระบบสามารถปรับปรุงและแก้ไขจุดอ่อนเหล่านั้นได้อย่างเหมาะสม อันจะส่งผลให้ระบบสารสนเทศมีระดับความปลอดภัยและความน่าเชื่อถือที่สูงขึ้นรองรับการใช้งานภายในองค์กร

การทดสอบครั้งนี้เป็นการดำเนินการทดสอบหาช่องโหว่ (Vulnerability Assessment) บนระบบ COJ ที่ทดสอบสอบทั้ง Non-Production (UAT Environment) และ Production โดยเป็นการทดสอบแบบใช้ Credential สำหรับเครื่องเป้าหมายที่อยู่ในระบบงานบริหารจัดการคุณภาพหนี้เพื่อยกระดับการให้บริการ โดยครอบคลุมทั้ง

- การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)
- การสแกนช่องโหว่บน Image File (Image Vulnerability Scanning)

ซึ่งดำเนินการผ่านเครื่องมือเชิงพาณิชย์ (Commercial Tools) ได้แก่ Nessus Professional สำหรับการสแกนช่องโหว่ของระบบปฏิบัติการ (Operating System) บนเครื่องเป้าหมายในสภาพแวดล้อม UAT และ Trivy สำหรับการสแกนช่องโหว่บน Image File ที่ใช้สำหรับการ build file ติดตั้งระบบ โดยรายละเอียดเครื่องเป้าหมายแสดงตามตารางที่ 1 และ ผลการทดสอบการหาช่องโหว่ตามตารางที่ 2 ตามลำดับ

ตารางที่ : 1 ผลการทดสอบรายละเอียดเป้าหมายสำหรับการทดสอบหาช่องโหว่ (Vulnerability Assessment)

ที่	ประเภทการทดสอบ	เป้าหมายทดสอบ	ชื่อเครื่อง	สภาพแวดล้อม	ครั้งที่ 1					ครั้งที่ 2				
					Critical	High	Medium	Low	Information	Critical	High	Medium	Low	Information
1	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.31.181.148	E2E-COJ-APP01D	UAT	0	0	0	0	0	0	0	0	0	0
2	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.31.181.149	E2E-COJ-SFTP01D	UAT	0	1	0	0	0	0	0	0	0	0
3	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.31.181.204	E2E-COJ-DB01D	UAT	0	1	0	0	0	0	0	0	0	0
4	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.29.149.31	E2E-COJ-APP VIP	DC	0	0	0	0	0	0	0	0	0	0
5	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.26.181.23	E2E-COJ-APP01P	DC	0	1	0	0	0	0	0	0	0	0
6	การสแกนระบบปฏิบัติการ (OS Vulnerability	172.26.181.24	E2E-COJ-APP02P	DC	0	0	0	0	0	0	0	0	0	0

ที่	ประเภทการทดสอบ	เป้าหมายทดสอบ	ชื่อเครื่อง	สภาพแวดล้อม	ครั้งที่ 1					ครั้งที่ 2				
					Critical	High	Medium	Low	Information	Critical	High	Medium	Low	Information
	Scanning)													
7	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.26.181.25	E2E-COJ-APP03P	DC	0	0	0	0	0	0	0	0	0	0
8	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.29.149.32	E2E-COJ-SFTP VIP	DC	0	0	0	0	0	0	0	0	0	0
9	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.26.181.27	E2E-COJ-SFTP01P	DC	0	0	0	0	0	0	0	0	0	0
10	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.26.181.28	E2E-COJ-SFTP02P	DC	0	1	0	0	0	0	0	0	0	0
11	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.29.149.33	E2E-COJ-DB VIP	DC	0	0	0	0	0	0	0	0	0	0
12	การสแกนระบบปฏิบัติการ (OS Vulnerability	172.26.180.79	E2E-ESXi109.it.baac.or.th	DC	0	0	0	0	0	0	0	0	0	0

ที่	ประเภทการทดสอบ	เป้าหมายทดสอบ	ชื่อเครื่อง	สภาพแวดล้อม	ครั้งที่ 1					ครั้งที่ 2				
					Critical	High	Medium	Low	Information	Critical	High	Medium	Low	Information
	Scanning)													
13	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.26.180.12	E2E-Alletra101	DC	0	0	0	0	0	0	0	0	0	0
14	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.26.180.13	E2E-Alletra102	DC	0	0	0	0	0	0	0	0	0	0
15	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.26.181.85	E2E-COJ-DB01P	DC	0	1	0	0	0	0	0	0	0	0
16	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.26.181.86	E2E-COJ-DB02P	DC	0	1	0	0	0	0	0	0	0	0
17	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.31.149.31	E2E-COJ-APP VIP	DR	0	0	0	0	0	0	0	0	0	0
18	การสแกนระบบปฏิบัติการ (OS Vulnerability	172.31.180.13	E2E-ESXi209.it.baac.or.th	DR	0	0	0	0	0	0	0	0	0	0

ที่	ประเภทการทดสอบ	เป้าหมายทดสอบ	ชื่อเครื่อง	สภาพแวดล้อม	ครั้งที่ 1					ครั้งที่ 2				
					Critical	High	Medium	Low	Information	Critical	High	Medium	Low	Information
	Scanning)													
19	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.26.180.79	E2E-ESXi109.it.baac.or.th	DR	0	0	0	0	0	0	0	0	0	0
20	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.31.181.27	E2E-COJ-APP01S	DR	0	0	0	0	0	0	0	0	0	0
21	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.31.181.28	E2E-COJ-APP02S	DR	0	1	0	0	0	0	0	0	0	0
22	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.31.181.29	E2E-COJ-SFTP01S	DR	0	1	0	0	0	0	0	0	0	0
23	การสแกนระบบปฏิบัติการ (OS Vulnerability Scanning)	172.31.181.82	E2E-COJ-DB01S	DR	0	1	0	0	0	0	0	0	0	0
24	การสแกนช่องโหว่บน Image File (Image Vulnerability	M3_image.tar frontend-react:v2.2.12	M3 Module	UAT DC DR	0	0	0	0	0	0	0	0	0	0

ที่	ประเภทการทดสอบ	เป้าหมายทดสอบ	ชื่อเครื่อง	สภาพแวดล้อม	ครั้งที่ 1					ครั้งที่ 2				
					Critical	High	Medium	Low	Information	Critical	High	Medium	Low	Information
	Scanning)													
25	การสแกนช่องโหว่บน Image File (Image Vulnerability Scanning)	M3_image.tar Backend-go-api	M3 Module	UAT DC DR	0	0	0	0	0	0	0	0	0	0
26	การสแกนช่องโหว่บน Image File (Image Vulnerability Scanning)	M3_image.tar Report-server-api	M3 Module	UAT DC DR	0	0	0	0	0	0	0	0	0	0
27	การสแกนช่องโหว่บน Image File (Image Vulnerability Scanning)	M3_image.tar dashboard-ui:v1.0.51	M3 Module	UAT DC DR	0	0	0	0	0	0	0	0	0	0
28	การสแกนช่องโหว่บน Image File (Image Vulnerability Scanning)	M3_image.tar dayend-batch:1.0.1	M3 Module	UAT DC DR	0	0	0	0	0	0	0	0	0	0
29	การสแกนช่องโหว่บน Image File (Image Vulnerability Scanning)	M4 baaccoreservice20251110.tar	M4 Module	UAT DC DR	0	0	0	0	0	0	0	0	0	0
30	การสแกนช่องโหว่บน Image File (Image Vulnerability	COJ baac-api-frontend.tar	COJ Module	UAT DC DR	0	0	0	0	0	0	0	0	0	0

ที่	ประเภทการทดสอบ	เป้าหมายทดสอบ	ชื่อเครื่อง	สภาพแวดล้อม	ครั้งที่ 1					ครั้งที่ 2				
					Critical	High	Medium	Low	Information	Critical	High	Medium	Low	Information
	Scanning)													
31	การสแกนช่องโหว่บน Image File (Image Vulnerability Scanning)	COJ baac-api-backend.tar	COJ Module	UAT DC DR	0	0	0	0	0	0	0	0	0	0

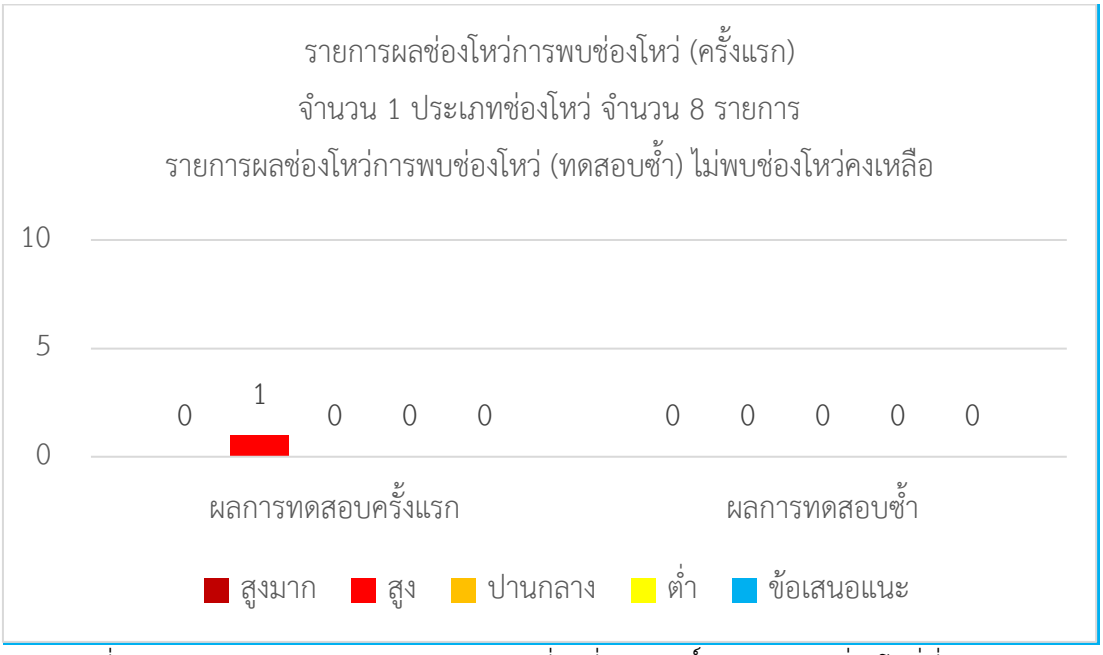
1.2 วัตถุประสงค์

วัตถุประสงค์ของการทดสอบ มีดังนี้

- เพื่อค้นหา ตรวจสอบ และระบุช่องโหว่ที่อาจมีอยู่ในระบบเป้าหมายขององค์กร เพื่อเปิดเผยจุดอ่อนที่อาจถูกผู้ไม่หวังดีใช้ประโยชน์ในการโจมตี
- เพื่อประเมินความเสี่ยงที่เกี่ยวข้องกับแต่ละช่องโหว่ที่ตรวจพบ โดยจำแนกตามระดับความรุนแรงของความเสี่ยงและจัดลำดับความสำคัญในการดำเนินการแก้ไขหรือบรรเทาผลกระทบที่อาจเกิดขึ้น
- เพื่อให้ข้อเสนอแนะในการเพิ่มประสิทธิผลในการป้องกันการโจมตีจากผู้บุกรุก และปรับปรุงมาตรการป้องกันและระบบความปลอดภัยตามที่ได้รับจากการทดสอบ

1.3 การวิเคราะห์ระดับความเสี่ยงตามรายการช่องโหว่ที่ตรวจพบ

ในการทดสอบครั้งแรกพบช่องโหว่ จำนวน 1 รายการ โดยแบ่งตามระดับความเสี่ยงได้ดังนี้ ความเสี่ยงสูง จำนวน 1 ประเภทช่องโหว่ จำนวน 8 รายการ และได้รับการแก้ไขทั้งหมด โดยแสดงตามกราฟที่แสดงด้านล่าง



รูปที่: 1 กราฟแสดงจำนวนของระดับความเสี่ยงที่วิเคราะห์ตามรายการช่องโหว่ที่ตรวจพบ

บทที่ 2 ขอบเขตการดำเนินงาน

2.1 ระยะเวลาการทดสอบ

ตารางที่ : 2 แสดงระยะเวลาการทดสอบที่ได้ดำเนินการ

ID	กิจกรรม	วันที่ดำเนินการ	หมายเหตุ
1	Vulnerability assessment Initial Testing	24 ตุลาคม 2568 - 7 พฤศจิกายน 2568	
2	Remediation by Developer	7 พฤศจิกายน 2568	
3	Vulnerability assessment Re-visit Testing	10 พฤศจิกายน 2568	
4	Deliver Re-visit Report	10 พฤศจิกายน 2568	

2.2 เครื่องมือที่ใช้ในการทดสอบ

เพื่อเพิ่มประสิทธิภาพและความครอบคลุมในการวิเคราะห์ช่องโหว่ ทีมทดสอบได้ใช้วิธีการแบบผสมผสานโดยใช้ทั้งเครื่องมือแบบอัตโนมัติและใช้คนเป็นผู้ทดสอบร่วมกัน เครื่องมือที่ใช้ในกระบวนการนี้มีดังนี้

ตารางที่ : 3 แสดงเครื่องมือที่ใช้ทดสอบตามรายการ

ที่	ชื่อเครื่องมือ	คำอธิบาย	Tool type
1.	NMAP (Network Mapper)	เป็นเครื่องมือสำหรับสแกนและวิเคราะห์เครือข่ายที่ใช้ในการตรวจสอบและค้นหาเครื่องแม่ข่าย (hosts) และบริการ (services) ที่ทำงานอยู่บนเครือข่าย มันมีความสามารถในการสแกนพอร์ต (port scanning) เพื่อตรวจสอบว่าพอร์ตใดๆ บนเครื่องเป้าหมายถูกเปิดอยู่หรือไม่ รวมถึงการระบุระบบปฏิบัติการที่ทำงานอยู่บนเครื่องเหล่านั้นด้วย นอกจากนี้ NMAP ยังมีฟังก์ชันการสแกนแบบมาตรฐานและแบบลึกเพื่อตรวจสอบช่องโหว่และความปลอดภัยของระบบ เป็นเครื่องมือที่ถูกนำมาใช้ในการทดสอบความเสถียรและความปลอดภัยของเครือข่ายในการทดสอบเจาะระบบและการประเมินความเสี่ยงของระบบคอมพิวเตอร์.	Automatic

ที่	ชื่อเครื่องมือ	คำอธิบาย	Tool type
2.	sslscan/testssl.sh	เป็นเครื่องมือสำหรับการทดสอบความปลอดภัยของเซิร์ฟเวอร์ที่ใช้โปรโตคอล SSL/TLS ซึ่งมักถูกใช้เพื่อตรวจสอบการกำหนดค่าและการใช้งานของ SSL/TLS บนเซิร์ฟเวอร์หรือเว็บไซต์ เครื่องมือเหล่านี้ช่วยในการค้นหาปัญหาที่อาจเกิดขึ้นเกี่ยวกับความปลอดภัย เช่น ช่องโหว่ในการกำหนดค่า SSL/TLS, การใช้งานของสัญญาณดิจิทัล (certificates) และการตรวจสอบความปลอดภัยของเว็บไซต์ที่ใช้ SSL/TLS รวมถึงปัญหาที่เกี่ยวข้องกับการเชื่อถือของผู้ออก Certificate Authority (CA) ด้วย	Automatic
3.	Nessus	เป็นเครื่องมือการตรวจสอบความปลอดภัยแบบอัตโนมัติ (Automated Security Scan) ซึ่งมีความสามารถในการสแกนและตรวจสอบหาช่องโหว่ที่อาจมีความเสี่ยงต่อระบบคอมพิวเตอร์และเครือข่าย	Automatic
4	Trivy	เป็นเครื่องมือการตรวจสอบความปลอดภัยแบบอัตโนมัติ (Automated Security Scan) ซึ่งมีความสามารถในการสแกนและตรวจสอบหาช่องโหว่ที่อาจมีความเสี่ยงต่อระบบคอมพิวเตอร์และเครือข่ายในรูปแบบของ Image	Automatic

2.3 ทีมทดสอบ

ตารางที่ : 4 การทดสอบได้ดำเนินการโดยทีมทดสอบตามรายชื่อในตารางด้านล่าง

ที่	รายชื่อผู้ทดสอบ	Certification	ประสบการณ์การทำงาน
1	Warunyou Sunpachit	OCSP, CEH, CompTIA Security+, CompTIA Pentest+, CC	ดำเนินการประเมินช่องโหว่และทดสอบเจาะระบบในระดับ Mobile Application, Web Application, Network, Thick-client Application ในธุรกิจการเงินการธนาคาร โทรคมนาคม ประภัยภัย และอื่นๆ โดยมีประสบการณ์ด้านการประเมินช่องโหว่และทดสอบเจาะระบบมากกว่า 15 ปี
2	Pongsathon Sirithanyakul	OCSP, CEH, CompTIA Security+, CompTIA Pentest+, CC	ดำเนินการประเมินช่องโหว่และทดสอบเจาะระบบในระดับ Mobile Application, Web Application, Network, Thick-client Application ในธุรกิจการเงินการธนาคาร โทรคมนาคม ประภัยภัย และอื่นๆ โดยมีประสบการณ์ด้านการประเมินช่องโหว่และทดสอบเจาะระบบมากกว่า 7 ปี

2.4 ข้อจำกัด

การทดสอบนี้เป็นการทดสอบจุดในเวลาที่กำหนดเท่านั้น (point-in-time test) และการประเมินความปลอดภัยถูกจำกัดอยู่ในช่วงเวลาที่ตกลงกันไว้ เวลาที่เพิ่มเติมและการทดสอบเพิ่มเติมอาจจะเปิดเผยสิ่งที่สังเกตเห็นได้อีก ขอแนะนำให้ดำเนินการทดสอบช่องโหว่เพิ่มเติมรอบต่อไป รวมถึงการทดสอบการเจาะระบบบนระบบเป็นระยะหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การเปลี่ยนเวอร์ชันซอฟต์แวร์ใหม่หรือการติดตั้งอุปกรณ์ใหม่ การเปลี่ยนแปลงที่สำคัญเช่นนี้อาจเป็นเหตุให้เกิดช่องโหว่ใหม่ ๆ ได้

บทที่ 3 แนวทางการทดสอบ

3.1 วิธีการที่ใช้ในการทดสอบ

วัตถุประสงค์ของการประเมินนี้คือการตรวจพบช่องโหว่หรือจุดอ่อนที่ต้องการปรับปรุง และให้ข้อเสนอแนะในการแก้ไขปัญหาที่พบและรายละเอียดของความต้องการในเชิงปฏิบัติการ การประเมินครอบคลุมถึงสามประเภทของการทดสอบช่องโหว่และการทดสอบเจาะระบบตามตารางด้านล่าง

ตารางที่ : 5 ประเภทของการทดสอบหาช่องโหว่และการทดสอบเจาะระบบ

การทดสอบแบบกล่องดำ (Black box)	การทดสอบแบบกล่องเทา (Credential)	การทดสอบแบบกล่องขาว (White box)
1) ไม่จำเป็นต้องให้ข้อมูลเกี่ยวกับเป้าหมายของระบบ 2) จำเป็นต้องยืนยันเป้าหมายก่อนทดสอบเจาะระบบ เพื่อป้องกันการทดสอบนอกขอบเขต 3) ไม่ให้บัญชีผู้ใช้สำหรับทดสอบเจาะระบบ	1) กำหนดระบบเป้าหมาย 2) ให้บัญชีผู้ใช้ในแต่กลุ่ม 3) ให้คำอธิบายรายละเอียดการใช้งานระบบแต่ละเมนู	1) ให้ source-codes ของระบบนั้น ๆ 2) ให้คำอธิบายรายละเอียดของแต่ละฟังก์ชันการใช้งาน

ทางทีมงานได้พัฒนากระบวนการ การทดสอบหาช่องโหว่ และ การทดสอบเจาะระบบ จากกรอบการทดสอบต่าง ๆ (Framework) เพื่อนำมาประยุกต์ใช้ให้เหมาะสมกับสภาพแวดล้อมการทดสอบเจาะระบบนั้น ๆ เช่น กระบวนการทดสอบความปลอดภัยทั้งด้านความตระหนักการใช้งานสารสนเทศ (Human) ทางด้านกายภาพ (Physical) การทดสอบโครงข่ายไร้สาย (Wireless) จาก Open Source Security Testing Methodology Manual (OSSTMM) v3 การทดสอบเจาะระบบของระบบสารสนเทศบนเครื่องโทรศัพท์มือถือ Mobile Application Security Verification Standard (MASVS) และ OWASP Mobile Security Testing Guide (MSTG) การทดสอบเจาะระบบเว็บแอปพลิเคชัน OWASP Testing Guide (OTG) v4 เป็นต้น

3.2 ข้อมูลอ้างอิงที่ใช้ประเมินความเสี่ยง

3.2.1 OWASP Top 10 Application Security Risks - 2021

เป็นรายงานที่กำหนดและระบุปัญหาที่เกี่ยวข้องกับความปลอดภัยในการพัฒนาและดำเนินการแอปพลิเคชันที่พบบ่อยในการใช้งานจริง รายงานนี้ถูกเผยแพร่โดย OWASP (Open Web Application Security Project) ซึ่งมุ่งเน้นการเสริมสร้างความปลอดภัยในเว็บแอปพลิเคชันและซอฟต์แวร์ การระบุปัญหาความปลอดภัยที่สำคัญที่ถูกนำเสนอในรายงานนี้ช่วยให้นักพัฒนาและผู้ดูแลระบบสามารถระบุและแก้ไขปัญหาด้านความปลอดภัยในขั้นตอนการพัฒนาและดำเนินการแอปพลิเคชันได้อย่างมีประสิทธิภาพ

ตารางที่ : 6 รายงานของ OWASP Top 10 Application Security Risks – 2021 (https://owasp.org/Top10/)

OWASP Top 10 Application 2021	คำอธิบาย
A1: Broken Access Control	ความเสี่ยงที่เกี่ยวข้องกับปัญหาในการควบคุมการเข้าถึงข้อมูลหรือฟังก์ชันในระบบโดยไม่ถูกต้องหรือไม่เพียงพอ ซึ่งอาจทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลหรือทำรายการที่ไม่ได้รับอนุญาต รายละเอียดการทำงานอาจรวมถึง: 1. การเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต: ผู้ไม่ประสงค์ดีอาจสามารถเข้าถึงข้อมูลที่มีความลับหรือที่สำคัญโดยไม่ได้รับอนุญาต โดยเรียกใช้ข้อมูลที่ไม่ถูกคัดกรองหรือไม่มีการตรวจสอบการสิทธิ์การเข้าถึง 2. การเปลี่ยนแปลงข้อมูลที่ไม่ได้รับอนุญาต: ผู้ไม่ประสงค์ดีอาจทำการเปลี่ยนแปลงข้อมูลที่สำคัญหรือมีความสำคัญโดยไม่ได้รับอนุญาต ซึ่งอาจส่งผลให้เกิดความเสียหายหรือความผิดพลาดในระบบ 3. การทำรายการที่ไม่ได้รับอนุญาต: ผู้ไม่ประสงค์ดีอาจดำเนินการรายการที่ส่งผลกระทบที่ไม่พึงประสงค์ต่อระบบหรือข้อมูล โดยใช้ฟังก์ชันหรือความสามารถที่ไม่ได้รับอนุญาต การแก้ไขปัญหาที่เกี่ยวข้องกับรายงาน A1 สามารถทำได้โดยการใช้ระบบการควบคุมการเข้าถึงที่เข้มงวดและครอบคลุม รวมถึงการทดสอบและตรวจสอบความปลอดภัยของระบบอย่างสม่ำเสมอ
A2: Cryptographic	ความเสี่ยงที่เกี่ยวข้องกับปัญหาในการใช้เทคนิคการเข้ารหัสที่ไม่ถูกต้อง

OWASP Top 10 Application 2021	คำอธิบาย
Failures	หรือไม่เพียงพอ ซึ่งอาจทำให้ข้อมูลที่เกี่ยวข้องกับความลับหรือความปลอดภัยถูกเปิดเผยหรือถูกแยกจากกันได้ รายละเอียดการทำงานอาจรวมถึง: 1. การใช้วิธีการเข้ารหัสที่ไม่เพียงพอ: การใช้วิธีการเข้ารหัสที่ไม่เหมาะสมหรือมีความเสี่ยงสูง เช่น การใช้วิธีการเข้ารหัสที่ถูกทำลายหรือเป็นที่รู้จักในวงการว่าไม่ปลอดภัย 2. ความยากจนของกุญแจ: การสร้างและการจัดการกับกุญแจการเข้ารหัสที่ไม่ปลอดภัย ซึ่งอาจทำให้ผู้ไม่ประสงค์ดีสามารถทำการระบาดไวรัสหรือเข้าถึงข้อมูลที่สำคัญได้ 3. การจัดการกับการรักษาความลับ: การเก็บรักษาและการจัดการกับข้อมูลที่เข้ารหัสอาจมีข้อบกพร่องหรือการจัดการที่ไม่เหมาะสมทำให้ข้อมูลถูกเปิดเผยหรือถูกแยกจากกัน 4. การบูรณะระบบเข้ารหัส: การประยุกต์ใช้ระบบการเข้ารหัสที่มีข้อบกพร่องหรือมีการเลือกใช้แบบไม่ถูกต้อง ซึ่งอาจทำให้ข้อมูลเสี่ยงต่อการโจมตี การแก้ไขปัญหาที่เกี่ยวข้องกับรายงาน A2 สามารถทำได้โดยการใช้เทคโนโลยีการเข้ารหัสที่มีความปลอดภัยและเหมาะสม รวมถึงการปรับปรุงกระบวนการสร้างและจัดการกับคีย์เวิร์ดการเข้ารหัสอย่างระมัดระวังและมีประสิทธิภาพ
A3: Injection	ความเสี่ยงที่เกี่ยวข้องกับการสั่งการไม่ประสงค์ดีที่ฝังเข้าไปในข้อมูลหรือคำสั่งที่รับเข้ามาในระบบโดยไม่ได้รับการตรวจสอบหรือกรองอย่างเหมาะสม ซึ่งอาจทำให้เกิดการโจมตีแบบ Injection เช่น SQL Injection, Command Injection, LDAP Injection, หรือ XML Injection รายละเอียดการทำงานของรายงาน A3 สามารถรวมถึง: 1. SQL Injection: การฝังโค้ด SQL ที่ไม่ประสงค์ดีในข้อมูลที่ถูกส่งเข้ามาในแอปพลิเคชันเพื่อเข้าถึงหรือปรับเปลี่ยนข้อมูลในฐานข้อมูล

OWASP Top 10 Application 2021	คำอธิบาย
	2. Command Injection: การฝังโค้ดคำสั่งระบบที่ไม่ประสงค์ดีในข้อมูลที่ถูกส่งเข้ามาในแอปพลิเคชันเพื่อรันคำสั่งในระบบหรือเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต 3. LDAP Injection: การฝังโค้ด LDAP ที่ไม่ประสงค์ดีในข้อมูลที่ถูกส่งเข้ามาในแอปพลิเคชันเพื่อโจมตีบริการไดเรกทอรีและเข้าถึงข้อมูลที่สำคัญ 4. XML Injection: การฝังโค้ด XML ที่ไม่ประสงค์ดีในข้อมูล XML ที่ถูกส่งเข้ามาในแอปพลิเคชันเพื่อโจมตีระบบหรือเปิดเผยข้อมูลที่ละเมิดความเป็นส่วนตัว การป้องกันการโจมตีแบบ Injection สามารถทำได้โดยการใช้พื้นที่จำกัดสิทธิ์และกรองข้อมูลอย่างเหมาะสมก่อนที่จะส่งเข้าสู่ระบบ รวมถึงการใช้พื้นที่จำกัดสิทธิ์ในการเข้าถึงฐานข้อมูล และการใช้พื้นที่จำกัดสิทธิ์ในการรันคำสั่งระบบหรือเรียกใช้บริการจากภายนอก
A4: Insecure Design	ความเสี่ยงที่เกี่ยวข้องกับการออกแบบและสร้างแอปพลิเคชันโดยไม่คำนึงถึงมาตรฐานความปลอดภัยและหลักการออกแบบที่ปลอดภัยอย่างเพียงพอ ซึ่งอาจทำให้เกิดช่องโหว่และความไม่ปลอดภัยต่าง ๆ ในแอปพลิเคชัน รายละเอียดการทำงานของรายงาน A4 สามารถรวมถึง: 1. การขาดความสามารถในการจำกัดสิทธิ์: การขาดความสามารถในการจำกัดสิทธิ์และควบคุมการเข้าถึงข้อมูลหรือฟังก์ชันของแอปพลิเคชัน ซึ่งอาจทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลที่ไม่เหมาะสมหรือทำการกระทำที่ไม่เหมาะสม 2. การไม่คำนึงถึงการป้องกันที่มีชั้นของข้อมูล: การออกแบบแอปพลิเคชันโดยไม่คำนึงถึงการป้องกันที่มีชั้นของข้อมูล ซึ่งอาจทำให้ข้อมูลที่สำคัญถูกเปิดเผยหรือถูกใช้โดยผู้ไม่ประสงค์ดี 3. การขาดความสามารถในการตรวจสอบและการติดตาม: การขาดความสามารถในการตรวจสอบและติดตามกิจกรรมที่เกิดขึ้นในระบบ เช่น

OWASP Top 10 Application 2021	คำอธิบาย
	การไม่มีการบันทึกล็อกหรือไม่มีการแจ้งเตือนเมื่อมีกิจกรรมที่เป็นไปไม่ได้ การแก้ไขปัญหาที่เกี่ยวข้องกับรายงาน A4 สามารถทำได้โดยการออกแบบและพัฒนาแอปพลิเคชันโดยให้คำนึงถึงความปลอดภัยตั้งแต่ต้น รวมถึงการใช้หลักการและเทคโนโลยีที่ปลอดภัย เพื่อลดความเสี่ยงของช่องโหว่และความไม่ปลอดภัยในแอปพลิเคชัน
A5: Security Misconfiguration	ความเสี่ยงที่เกี่ยวข้องกับการกำหนดค่าและการตั้งค่าระบบหรือแอปพลิเคชันโดยไม่ถูกต้องหรือไม่เพียงพอทำให้เกิดช่องโหว่ที่เปิดเผยข้อมูลหรือทำให้เกิดความไม่ปลอดภัย รายละเอียดการทำงานของรายงาน A5 สามารถรวมถึง: 1. ค่าเริ่มต้นที่ไม่ปลอดภัย: การใช้ค่าเริ่มต้นที่ไม่ปลอดภัยหรือค่าที่มีความเสี่ยง เช่น รหัสผ่านเริ่มต้นที่ถูกตั้งไว้, การเปิดใช้งานฟีเจอร์ที่ไม่จำเป็น 2. การกำหนดค่าสิทธิ์ไม่ถูกต้อง: การกำหนดค่าสิทธิ์หรือสิทธิ์ที่ไม่เพียงพอ ทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลหรือฟังก์ชันที่ไม่ได้รับอนุญาตได้ 3. การทิ้งรายละเอียดการทำงานที่ไม่จำเป็น: การทิ้งรายละเอียดการทำงานหรือข้อมูลที่ไม่จำเป็นทำให้ผู้ไม่ประสงค์ดีสามารถใช้ข้อมูลนั้นในการโจมตีได้ 4. ขาดการอัปเดตและการจัดการเวอร์ชั่น: การขาดการอัปเดตซอฟต์แวร์หรือการจัดการเวอร์ชั่นที่สามารถทำให้เกิดช่องโหว่ที่มีชั้นความปลอดภัยต่ำหรือทำให้เกิดความไม่ปลอดภัยในระบบ การแก้ไขปัญหาที่เกี่ยวข้องกับรายงาน A5 สามารถทำได้โดยการตั้งค่าระบบและแอปพลิเคชันให้เป็นไปตามหลักการและมาตรฐานความปลอดภัย รวมถึงการทดสอบความปลอดภัยและการตรวจสอบการตั้งค่าเพื่อให้แน่ใจว่าไม่มีความเสี่ยงหรือช่องโหว่ใดๆ ที่เปิดเผยข้อมูลหรือทำให้เกิดความไม่ปลอดภัยในระบบ
A6: Vulnerable and Outdated	ความเสี่ยงที่เกี่ยวข้องกับการใช้งานส่วนประกอบของระบบหรือแอปพลิเคชันที่มีช่องโหว่หรือเวอร์ชันเก่าที่มีความไม่ปลอดภัย ซึ่งอาจทำให้เกิดความเสี่ยงและ

OWASP Top 10 Application 2021	คำอธิบาย
Components	ช่องโหว่ต่าง ๆ ในระบบ รายละเอียดการทำงานของรายงาน A6 สามารถรวมถึง: 1. การใช้งานส่วนประกอบที่มีช่องโหว่: การใช้งานและการนำเข้าส่วนประกอบหรือไลบรารีที่มีช่องโหว่ในระบบ เช่น ไลบรารีที่มีช่องโหว่ของชนิดซอฟต์แวร์ต่าง ๆ หรือชุดเครื่องมือที่ไม่ปลอดภัย 2. การใช้งานส่วนประกอบเวอร์ชันเก่า: การใช้งานส่วนประกอบหรือไลบรารีที่เป็นเวอร์ชันเก่าและมีช่องโหว่ที่ได้รับการแก้ไขในเวอร์ชันล่าสุด 3. การขาดการอัปเดตและการจัดการเวอร์ชั่น: การขาดการอัปเดตและการจัดการเวอร์ชั่นที่สามารถทำให้เกิดความไม่ปลอดภัยในระบบ และช่องโหว่ที่มีชั้นความปลอดภัยต่ำ การแก้ไขปัญหาที่เกี่ยวข้องกับรายงาน A6 สามารถทำได้โดยการทำการสแกนและตรวจสอบส่วนประกอบของระบบหรือแอปพลิเคชันเพื่อตรวจจับส่วนประกอบที่มีช่องโหว่หรือเวอร์ชันเก่า และทำการอัปเดตหรือแก้ไขส่วนประกอบเหล่านั้นเพื่อให้มีความปลอดภัยที่สูงขึ้น
A7: Identification and Authentication Failures	เป็นหัวหัวรายงานที่ให้ความสำคัญกับปัญหาเกี่ยวกับการระบุตัวตนและการรับรองตัวตน ซึ่งเป็นส่วนสำคัญของความปลอดภัยของระบบ เมื่อมีความผิดพลาดเกิดขึ้นในการระบุหรือการรับรองตัวตน ผู้ไม่ประสงค์ดีอาจมีโอกาสเข้าถึงข้อมูลหรือฟังก์ชันที่ไม่เหมาะสม หรือกระทำการในฐานะผู้ใช้ที่ถูกสมมติให้มีสิทธิ์สูง โดยไม่ได้รับการตรวจสอบอย่างเหมาะสม รายละเอียดที่เกี่ยวข้องอาจรวมถึง: 1. Weak Password Policies: นโยบายที่ไม่เข้มงวดเกี่ยวกับการตั้งรหัสผ่านที่มีความปลอดภัย ทำให้ผู้ไม่ประสงค์ดีสามารถทำการทดลองเดารหัสผ่านหรือใช้วิธีการต่าง ๆ เพื่อบล็อกเข้าสู่ระบบ 2. Brute Force Attacks: การโจมตีโดยการทดลองเดารหัสผ่านจนกว่าจะพบรหัสที่ถูกต้อง ซึ่งอาจเป็นไปได้เมื่อระบบไม่มีการจำกัดจำนวนครั้งที่ลองเดา

OWASP Top 10 Application 2021	คำอธิบาย
	รหัสเข้าสู่ระบบ 3. Weak Multifactor Authentication (MFA): การใช้วิธีการยืนยันตัวตนที่มีความปลอดภัยไม่เพียงพอ เช่น การใช้ SMS ในการยืนยันตัวตนซึ่งเป็นระบบที่มีช่องโหว่ 4. Session Management: ปัญหาที่เกี่ยวข้องกับการจัดการเซสชัน ซึ่งอาจทำให้ผู้ไม่ประสงค์ดีสามารถทำให้เซสชันหรือการตั้งค่าของผู้ใช้หมดอายุ หรือแยกจากการยืนยันตัวตน 5. Insufficient Account Lockout: การไม่มีการล็อคบัญชีหลังจากจำนวนครั้งที่พยายามเข้าสู่ระบบผิดพลาดเกินกำหนด อาจทำให้ผู้ไม่ประสงค์ดีสามารถดำเนินการโจมตีด้วยวิธีการทดลองเดารหัสผ่านได้โดยไม่มีข้อจำกัด การแก้ไขปัญหาในหัวข้อนี้จำเป็นต้องมีการสร้างนโยบายความปลอดภัยที่เข้มงวดเกี่ยวกับการระบุตัวตนและการรับรองตัวตน รวมถึงการใช้เทคโนโลยีที่มีความปลอดภัยมากขึ้น เช่น การใช้ MFA หรือการใช้วิธีการรับรองตัวตนที่มีความเข้มงวดมากขึ้น
A8: Software and Data Integrity Failures	ความเสี่ยงที่เกี่ยวข้องกับความผิดพลาดในซอฟต์แวร์และข้อมูลที่สามารถทำให้ข้อมูลหรือซอฟต์แวร์ถูกเปลี่ยนแปลงหรือทำลายโดยไม่ได้รับอนุญาต รายละเอียดการทำงานที่เกี่ยวข้องอาจรวมถึง: 1. ข้อบกพร่องในซอฟต์แวร์: การพัฒนาซอฟต์แวร์ที่มีข้อบกพร่องอาจทำให้มีช่องโหว่ที่ทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงระบบหรือข้อมูลโดยไม่ได้รับอนุญาต 2. การสูญเสียข้อมูล: สูญเสียข้อมูลสำคัญหรือสำรองข้อมูลที่สำคัญอาจเกิดขึ้นเนื่องจากการขัดข้องในระบบหรือซอฟต์แวร์ 3. การเปลี่ยนแปลงข้อมูลที่ไม่ได้รับอนุญาต: การโจมตีที่เปลี่ยนแปลงข้อมูลที่สำคัญโดยไม่ได้รับอนุญาต เช่น การเขียนข้อมูลลงในฐานข้อมูลหรือไฟล์ที่สำคัญ

OWASP Top 10 Application 2021	คำอธิบาย
	4. การบิดเบือนข้อมูล: การเปลี่ยนแปลงค่าข้อมูลที่ส่งผลกระทบต่อการประมวลผลหรือการตัดสินใจโดยไม่ได้รับอนุญาต 5. การสร้างซอฟต์แวร์ที่มีความไม่มั่นคง: การพัฒนาซอฟต์แวร์ที่มีข้อบกพร่องหรือช่องโหว่อาจสร้างความไม่มั่นคงในการทำงานของระบบและข้อมูล การจัดการความปลอดภัยของซอฟต์แวร์และข้อมูล รวมถึงการใช้เทคโนโลยีและมาตรการที่เหมาะสม เป็นสิ่งสำคัญในการป้องกันการสูญเสียข้อมูลและความไม่เสถียรของระบบในสถานการณ์ที่ไม่คาดคิด
A9: Security Logging and Monitoring Failures	ความเสี่ยงที่เกี่ยวข้องกับปัญหาในการบันทึกและตรวจสอบความปลอดภัยของระบบ ซึ่งอาจทำให้ระบบไม่สามารถตรวจจับหรือระบุกิจกรรมที่ไม่เหมาะสมหรือเกิดความผิดปกติในระบบได้อย่างทันท่วงที รายละเอียดการทำงานที่เกี่ยวข้องอาจรวมถึง: 1. ขาดความสามารถในการบันทึกเหตุการณ์: ระบบที่ไม่สามารถบันทึกเหตุการณ์หรือกิจกรรมที่เกิดขึ้นในระบบได้อย่างครอบคลุม ทำให้ไม่สามารถตรวจสอบหรือวิเคราะห์กิจกรรมที่เป็นอันตรายได้อย่างมีประสิทธิภาพ 2. ข้อบกพร่องในการตรวจจับการลักษณะเฉพาะของการโจมตี: ระบบที่ไม่สามารถตรวจจับและรายงานเหตุการณ์ที่อาจเป็นการโจมตีหรือกิจกรรมที่เกี่ยวข้องกับความมั่นคงของระบบ 3. ข้อบกพร่องในการแจ้งเตือนเหตุการณ์: ระบบที่ไม่สามารถแจ้งเตือนผู้ดูแลระบบหรือผู้ใช้ที่เกี่ยวข้องเมื่อเกิดเหตุการณ์ที่สำคัญหรือเป็นอันตราย 4. ข้อบกพร่องในการควบคุมการเข้าถึงเข้าชม: การขาดความสามารถในการควบคุมการเข้าถึงและการเข้าชมไฟล์บันทึกเหตุการณ์ ซึ่งอาจทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงและแก้ไขข้อมูลบันทึกเหตุการณ์ได้ 5. ข้อบกพร่องในการจัดเก็บข้อมูลเหตุการณ์: การบันทึกข้อมูลเหตุการณ์ที่ไม่เพียงพอหรือไม่ครอบคลุม ซึ่งอาจทำให้ไม่สามารถนำข้อมูลเหตุการณ์มา

OWASP Top 10 Application 2021	คำอธิบาย
	วิเคราะห์หรือใช้ในการตรวจสอบความมั่นคงของระบบได้อย่างมีประสิทธิภาพ การแก้ไขปัญหาด้านความสามารถในการบันทึกและตรวจสอบความปลอดภัยของระบบ รวมถึงการใช้เทคโนโลยีและการสร้างนโยบายที่เหมาะสม เป็นสิ่งสำคัญในการป้องกันการโจมตีและรักษาความมั่นคงของระบบไว้อย่างต่อเนื่อง
A10: Server-Side Request Forgery	ความเสี่ยงที่เกี่ยวข้องกับการโจมตีที่ผู้ไม่ประสงค์ดีสร้างคำขอ (request) ที่ส่งถึงเซิร์ฟเวอร์แล้วเกิดการประมวลผลคำขอนั้นในฝั่งเซิร์ฟเวอร์ ซึ่งอาจทำให้เกิดผลกระทบอันไม่พึงประสงค์ รวมถึงการเข้าถึงข้อมูลภายในระบบหรือระบบที่อยู่ในเครือข่ายภายใน หรือการโจมตีอื่น ๆ ที่เกี่ยวข้องกับการร้องขอจากฝั่งเซิร์ฟเวอร์ รายละเอียดการทำงานของ A10 อาจรวมถึงการโจมตีด้วยเทคนิคเช่นการส่งคำขอ HTTP ที่มี URL ที่ชี้ไปยังทรัพยากร์ในเครือข่ายภายใน หรือการใช้โปรโตคอลที่เรียกหรือส่งคำขอเพื่อทำงานภายในเครื่องเซิร์ฟเวอร์ที่ไม่ควรเข้าถึงได้ผ่านภายนอก การป้องกัน A10 สามารถทำได้โดยการตรวจสอบและกรองคำขอที่ส่งถึงเซิร์ฟเวอร์ และการใช้การกำหนดขีดจำกัดในการเข้าถึงทรัพยากรระดับระบบที่สูงขึ้น รวมทั้งการใช้การตรวจสอบและสร้างบันทึกเหตุการณ์เพื่อตรวจจับการโจมตีด้วยวิธีนี้ได้อย่างมีประสิทธิภาพ

3.2.2 CWE Top 25

ตารางที่ : 7 ความหมายของหัวข้อที่เกี่ยวข้องกับ Common Weakness enumuration

หัวข้อ CWE Top 25	คำอธิบาย
CWE-79: Cross-site Scripting (XSS)	ช่องโหว่ที่เกิดจากการไม่ตรวจสอบข้อมูลที่รับเข้ามาก่อนนำไปแสดงผลบนหน้าเว็บ ทำให้ผู้โจมตีสามารถแทรก script ที่เป็นอันตรายได้
CWE-787: Out-of-bounds Write	การเขียนข้อมูลเกินขอบเขตของ buffer ที่จัดสรรไว้ อาจทำให้เกิดการทำงานผิดพลาดหรือถูกใช้ในการโจมตีระบบ
CWE-89: SQL Injection	ช่องโหว่ที่เกิดจากการไม่ตรวจสอบข้อมูลที่รับเข้ามาก่อนนำไปใช้ใน SQL command ทำให้ผู้โจมตีสามารถแก้ไขคำสั่ง SQL ได้
CWE-352: Cross-Site Request Forgery (CSRF)	การโจมตีที่หลอกให้ผู้ใช้ที่ login อยู่ทำคำสั่งที่ไม่ได้ตั้งใจโดยไม่รู้ตัว
CWE-22: Path Traversal	ช่องโหว่ที่อนุญาตให้ผู้โจมตีเข้าถึงไฟล์หรือไดเรกทอรีนอกเหนือจากที่กำหนดไว้
CWE-125: Out-of-bounds Read	การอ่านข้อมูลเกินขอบเขตของ buffer ที่จัดสรรไว้ อาจทำให้เกิดการรั่วไหลของข้อมูลหรือระบบล่ม
CWE-78: OS Command Injection	ช่องโหว่ที่ทำให้ผู้โจมตีสามารถแทรกคำสั่งของระบบปฏิบัติการได้ผ่านทางแอปพลิเคชัน
CWE-416: Use After Free	การใช้งาน memory ที่ถูก free ไปแล้ว อาจทำให้เกิดพฤติกรรมที่ไม่คาดคิดหรือถูกใช้ในการโจมตี
CWE-862: Missing Authorization	การขาดการตรวจสอบสิทธิ์ในการเข้าถึงทรัพยากรหรือฟังก์ชัน
CWE-434: Unrestricted Upload of File with Dangerous Type	การอนุญาตให้อัปโหลดไฟล์ที่เป็นอันตรายโดยไม่มีการตรวจสอบประเภทไฟล์
CWE-94: Code Injection	ช่องโหว่ที่ทำให้ผู้โจมตีสามารถแทรกและรันโค้ดที่เป็นอันตรายได้
CWE-20: Improper Input Validation	การไม่ตรวจสอบความถูกต้องของข้อมูลที่รับเข้ามา
CWE-77: Command Injection	การแทรกคำสั่งที่เป็นอันตรายผ่านทาง input ของแอปพลิเคชัน
CWE-287: Improper Authentication	การตรวจสอบตัวตนที่ไม่เหมาะสมหรือไม่เพียงพอ

หัวข้อ CWE Top 25	คำอธิบาย
CWE-269: Improper Privilege Management	การจัดการสิทธิ์ที่ไม่เหมาะสม อาจทำให้ผู้ใช้มีสิทธิ์มากเกินไป
CWE-502: Deserialization of Untrusted Data	การแปลงข้อมูลที่ไม่น่าเชื่อถือกลับเป็น object อาจนำไปสู่การรันโค้ดที่เป็นอันตราย
CWE-200: Exposure of Sensitive Information	การเปิดเผยข้อมูลที่ละเอียดอ่อนให้กับผู้ที่ไม่มีสิทธิ์
CWE-863: Incorrect Authorization	การตรวจสอบสิทธิ์ที่ไม่ถูกต้อง
CWE-918: Server-Side Request Forgery (SSRF)	ช่องโหว่ที่ทำให้ผู้โจมตีสามารถบังคับให้ server ส่งคำขอไปยังปลายทางที่ไม่ได้ตั้งใจ
CWE-119: Improper Restriction of Operations within Memory Buffer	การจำกัดการทำงานภายใน memory buffer ที่ไม่เหมาะสม
CWE-476: NULL Pointer Dereference	การเข้าถึง pointer ที่มีค่าเป็น NULL ทำให้เกิด crash หรือพฤติกรรมที่ไม่คาดคิด
CWE-798: Use of Hard-coded Credentials	การใช้ username และ password ที่ฝังตายอยู่ในโค้ด
CWE-190: Integer Overflow or Wraparound	การล้นของตัวเลขจำนวนเต็มที่อาจนำไปสู่พฤติกรรมที่ไม่คาดคิด
CWE-400: Uncontrolled Resource Consumption	การใช้ทรัพยากรที่ไม่มีการควบคุม อาจทำให้เกิด Denial of Service
CWE-306: Missing Authentication for Critical Function	การขาดการตรวจสอบตัวตนสำหรับฟังก์ชันที่สำคัญ

3.2.3 CVSS Score

CVSS (Common Vulnerability Scoring System) คือระบบคะแนนมาตรฐานสำหรับประเมินความรุนแรงของช่องโหว่ โดยมีช่วงคะแนนดังนี้

None: 0.0

Low: 0.1 - 3.9

Medium: 4.0 - 6.9

High: 7.0 - 8.9

Critical: 9.0 - 10.0

หมายเหตุ: CWE เป็นการจัดหมวดหมู่ประเภทของช่องโหว่ ไม่ใช่ช่องโหว่เฉพาะเจาะจง ดังนั้นจึงไม่มีคะแนน CVSS ที่ตายตัว แต่จะมีช่วงคะแนนที่พบบ่อยในแต่ละประเภท โดยคะแนน CVSS ที่แท้จริงจะถูกกำหนดให้กับ CVE (ช่องโหว่เฉพาะ) แต่ละตัว

3.3 เมทริกซ์ของผลกระทบและความน่าจะเป็น (Impact and Likelihood Matrix)

มาตรฐาน OWASP Risk Rating Methodology standards (https://owasp.org/www-community/OWASP_Risk_Rating_Methodology) ถูกใช้ในการพิจารณาและประเมินความน่าจะเป็นของเหตุการณ์ที่เป็นอันตรายต่อระบบความปลอดภัย รวมถึงผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์เหล่านั้น ที่เกิดจากการโจมตีหรือการละเมิดความปลอดภัยของระบบข้อมูล การวิเคราะห์ความน่าจะเป็นและผลกระทบมีเกณฑ์การให้คะแนนที่อธิบายโดยละเอียดดังต่อไปนี้

3.3.1 ปัจจัยที่ใช้ประเมินผลกระทบ (Impact Factors)

การวิเคราะห์ผลกระทบของข้อความจะถูกดำเนินการทั้งในด้าน "เชิงเทคนิค" และ "เชิงธุรกิจ" การให้คะแนนผลกระทบมีดังนี้

ตารางที่ : 8 คะแนนของผลกระทบในด้าน "เชิงเทคนิค" และ "เชิงธุรกิจ"

เกณฑ์ผลกระทบ	นิยามคะแนน
1. ปัจจัยของผลกระทบเชิงเทคนิค (Technical Impact Factor)	
การสูญเสียข้อมูลที่เป็นความลับ (Loss of Confidentiality)	2: ข้อมูลที่ไม่สำคัญเล็กน้อยถูกเปิดเผย 6: ข้อมูลที่สำคัญเล็กน้อยหรือข้อมูลที่ไม่สำคัญมากถูกเปิดเผย 7: ข้อมูลที่สำคัญมากถูกเปิดเผย 9: ข้อมูลทั้งหมดถูกเปิดเผย
การสูญเสียความสมบูรณ์หรือความน่าเชื่อถือของข้อมูล (Loss of Integrity)	1: ข้อมูลเสียหายเพียงเล็กน้อย 3: ข้อมูลเสียหายอย่างรุนแรงเพียงเล็กน้อย 5: ข้อมูลเสียหายเพียงเล็กน้อยอย่างกว้างขวาง 7: ข้อมูลเสียหายอย่างรุนแรงอย่างกว้างขวาง 9: ข้อมูลทั้งหมดเสียหายทั้งหมด
การสูญเสียความพร้อมใช้งาน (Loss of Availability)	1: Services ถูกหยุดชั่วคราวเพียงเล็กน้อย 5: Services ถูกหยุดชั่วคราวเพียงเล็กน้อย หรือ Services ถูกหยุดชั่วคราวอย่างกว้างขวาง 7: Services ถูกหยุดชั่วคราวอย่างกว้างขวาง

เกณฑ์ผลกระทบ	นิยามคะแนน
	9: ทุก Services สูญเสียไปอย่างสมบูรณ์
การสูญเสียความรับผิดชอบ (Loss of Accountability)	1: สามารถติดตามตัวได้ทั้งหมด 7: อาจจะสามารถติดตามตัวได้ 9: ไม่สามารถระบุตัวตนหรือติดตามตัวได้
2. ปัจจัยของผลกระทบเชิงธุรกิจ (Business Impact Factors)	
ความเสียหายทางการเงิน (Financial Damage)	1: มีน้อยกว่าค่าซ่อมแซมช่องโหว่ 3: มีผลกระทบต่อกำไรประจำปีเล็กน้อย 7: มีผลกระทบต่อกำไรประจำปีอย่างมีนัยสำคัญ 9: ล้มละลายการเงิน
ความเสียหายที่เกิดขึ้นกับชื่อเสียง หรือภาพลักษณ์ (Reputation Damage)	1: มีความเสียหายเล็กน้อย 4: สูญเสียลูกค้ารายสำคัญ 5: สูญเสียความน่าเชื่อถือ 9: มีความเสียหายต่อชื่อเสียงหรือแบรนด์
การไม่ปฏิบัติตามกฎหมาย หรือ นโยบาย หรือมาตรฐานที่กำหนดไว้ (Non-compliance)	2: การละเมิดเพียงเล็กน้อย 5: การละเมิดที่ชัดเจน 7: การละเมิดระดับสูง
การละเมิดความเป็นส่วนตัวของ บุคคลหรือข้อมูลส่วนบุคคล (Privacy Violation)	3: หนึ่งบุคคล 5: หลักร้อยคน 7: หลักพันคน 9: หลักล้านคน

3.3.2 ปัจจัยที่ใช้ประเมินความน่าจะเป็น (Likelihood Factors)

ความน่าจะเป็นประกอบด้วย ปัจจัยของ "ตัวแทนผู้ลักลอบ" และ "ช่องโหว่" การจัดระดับความน่าจะเป็นมีดังนี้

ตารางที่ : 9 คะแนนปัจจัยของ "ตัวแทนผู้ลักลอบ" และ "ช่องโหว่" ที่ใช้ประเมินความน่าจะเป็น

เกณฑ์ความน่าจะเป็น	นิยามคะแนน
1. ปัจจัยของตัวแทนผู้ลักลอบ (Threat Agent Factors)	
ระดับทักษะ (Skill Level)	1: ไม่มีทักษะทางเทคนิค 3: บางทักษะทางเทคนิค 5: ผู้ใช้คอมพิวเตอร์ระดับขั้นสูง 6: ทักษะในด้านเครือข่ายและโปรแกรมมิ่ง 9: ทักษะการเจาะระบบความปลอดภัย
เหตุผลหรือจุดมุ่งหมาย (Motive)	1: ต้องการรางวัลเล็กน้อยหรือไม่ต้องการ 4: ต้องการรางวัลที่เป็นไปได้ 9: ต้องการรางวัลขั้นสูง
โอกาสหรือสถานการณ์ที่เอื้อต่อตัวแทน (Opportunity)	0: ต้องการการเข้าถึงทั้งหมดหรือทรัพยากรที่มีค่าสูง 4: ต้องการการเข้าถึงพิเศษหรือทรัพยากรที่มีค่า 7: ต้องการการเข้าถึงบางส่วนหรือทรัพยากรบางประเภท 9: ไม่ต้องการการเข้าถึงหรือทรัพยากรใด
ขนาดของกลุ่มผู้ใช้หรือผู้เกี่ยวข้องที่เป็นเป้าหมายของการโจมตีหรือการทำลายระบบ (Size)	2: นักพัฒนาหรือผู้ดูแลระบบ 4: ผู้ใช้ภายในอินทราเน็ต 5: พาร์ทเนอร์ 6: ผู้ใช้ที่ได้รับการตรวจสอบสิทธิ์ 9: ผู้ใช้อินเทอร์เน็ตที่ไม่ระบุชื่อ
2. ปัจจัยของช่องโหว่ (Vulnerability Factors)	
ความง่ายในการค้นพบช่องโหว่ (Ease of discovery)	1: เกือบจะเป็นไปไม่ได้หรือมีความยากมากที่จะทำได้ในสภาวะปกติ 3: ยาก 7: ง่าย

เกณฑ์ความน่าจะเป็น	นิยามคะแนน
	9: มีเครื่องมือแบบอัตโนมัติที่ใช้ทำได้
ความง่ายในการใช้ช่องโหว่หรือข้อบกพร่องเพื่อโจมตีระบบ (Ease of exploit)	1: เป็นเพียงทฤษฎี 3: ยาก 5: ง่าย 9: มีเครื่องมือแบบอัตโนมัติที่ใช้ทำได้
ความตระหนักในเรื่องความปลอดภัยของข้อมูล (Awareness)	1: ไม่รู้ 4: ไม่เปิดเผย 6: ชัดเจน 9: รู้กันทั่วไป
การตรวจจับการบุกรุก หรือตรวจจับการกระทำที่เป็นภัยต่อระบบขององค์กร (Intrusion detection)	1: ตรวจจับเหตุการณ์ที่เกิดขึ้นทันทีในแอปพลิเคชัน 3: บันทึกและตรวจสอบ 8: บันทึกโดยไม่ตรวจสอบ 9: ไม่ได้ทำการบันทึก

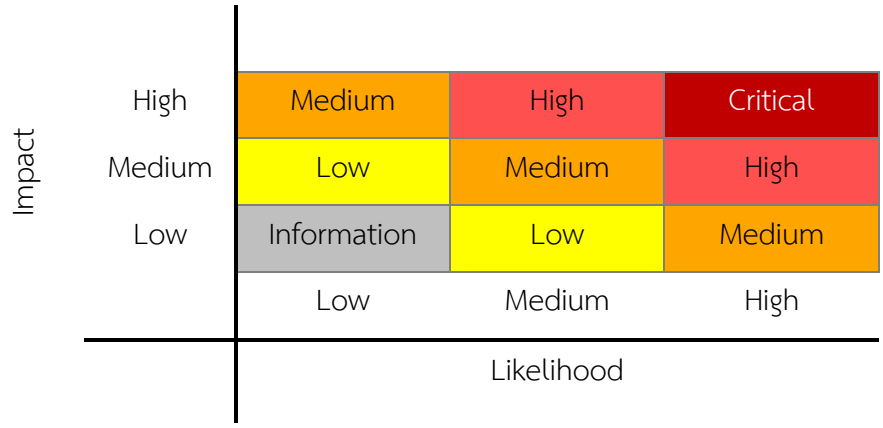
3.4 ระดับการจัดอันดับความเสี่ยง (Risk rating level)

3.4.1 ความรุนแรงของความเสี่ยง (The Severity of the risk)

การประเมินความน่าจะเป็นและการประเมินผลกระทบจะประเมินร่วมกันเพื่อคำนวณความรุนแรงโดยรวมของความเสี่ยงนี้ การทำเช่นนี้จะทำโดยการกำหนดว่าความน่าจะเป็นมีระดับต่ำ กลาง หรือสูง และทำเช่นเดียวกันสำหรับผลกระทบด้วย เกณฑ์การให้คะแนนระดับ 0 ถึง 9 ถูกแบ่งออกเป็นสามส่วนดังนี้

ระดับความน่าจะเป็นและผลกระทบ	
0 ถึง < 3	ต่ำ (Low)
3 ถึง < 6	กลาง (Medium)
6 ถึง 9	สูง (High)

การให้คะแนนความเสี่ยงถูกคำนวณโดยการคูณผลกระทบและความน่าจะเป็นของอุปสรรคต่าง ๆ คะแนนจะถูกกำหนดตามเกณฑ์ดังนี้:



3.4.2 คำจำกัดความของการจัดอันดับความเสี่ยง (Risk Rating Definitions)

ระดับความเสี่ยง	คำอธิบาย
สูงมาก (Critical)	ระดับความรุนแรง "สูงมาก" เป็นระดับที่ยอมรับไม่ได้และควรพิจารณาการแก้ไขปัญหาโดยทันที เพื่อให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้ตามนโยบายและมาตรการด้านความปลอดภัยของข้อมูลขององค์กร และเพื่อลดความเสี่ยงด้านความปลอดภัยของข้อมูลรวมถึงความลับ ความสมบูรณ์ และความพร้อมใช้งาน รวมถึงความรับผิดชอบในการบรรลุวัตถุประสงค์ขององค์กร การดำเนินงาน การเงิน ชื่อเสียง ความเป็นไปตามข้อกำหนด และความเป็นส่วนตัวของบุคคล.
สูง (High)	ระดับความรุนแรง "สูง" เป็นระดับที่ยอมรับไม่ได้และควรพิจารณาการแก้ไขข้อบกพร่องโดยนำมาใช้ในทางปฏิบัติภายในระยะเวลาที่เหมาะสม และจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ตามนโยบายและมาตรการด้านความปลอดภัยของข้อมูลขององค์กร เพื่อลดความเสี่ยงด้านความปลอดภัยของข้อมูลรวมถึงความลับ ความถูกต้อง และความพร้อมใช้งาน รวมถึงความรับผิดชอบในการบรรลุวัตถุประสงค์ขององค์กร การดำเนินงาน การเงิน ชื่อเสียง ความเป็นไปตามข้อกำหนด และความเป็นส่วนตัวของบุคคล.
ปานกลาง (Medium)	ระดับความรุนแรง "ปานกลาง" ควรพิจารณาการแก้ไขข้อบกพร่องและนำมาใช้ในทางปฏิบัติภายในระยะเวลาที่เหมาะสมตามนโยบายและมาตรการด้านความปลอดภัยของข้อมูลขององค์กรเพื่อลดความเสี่ยงด้านความปลอดภัยของข้อมูลรวมถึงความลับ ความถูกต้อง และความพร้อมใช้งาน รวมถึงความรับผิดชอบในการบรรลุวัตถุประสงค์ขององค์กร การดำเนินงาน การเงิน ชื่อเสียง ความเป็นไปตามข้อกำหนด และความเป็นส่วนตัวของบุคคล อย่างไรก็ตาม การยอมรับความเสี่ยงอาจถูกพิจารณา และความเสี่ยงควรถูกควบคุมเพื่อป้องกันไม่ให้เกิดการเพิ่มขึ้นไปสู่ระดับที่ยอมรับไม่ได้
ต่ำ (Low)	ระดับความรุนแรง "ต่ำ" ควรพิจารณาว่าการทำการแก้ไขนั้นยังจำเป็นหรือไม่ หรือตัดสินใจที่จะยอมรับความเสี่ยงตามนโยบายและมาตรการด้านความปลอดภัยของข้อมูลขององค์กรเพื่อลดความเสี่ยงด้านความปลอดภัยของข้อมูลรวมถึงความลับ ความถูกต้อง และความพร้อมใช้งาน รวมถึงความรับผิดชอบในการบรรลุวัตถุประสงค์ขององค์กร การดำเนินงาน การเงิน ชื่อเสียง ความเป็นไปตามข้อกำหนด และความเป็นส่วนตัวของบุคคล
เสนอแนะ (Information)	"เสนอแนะ" อาจมีการพัฒนาเพิ่มเติมเพื่อเสริมความแข็งแกร่งของการป้องกันสินทรัพย์ข้อมูลขององค์กรต่อไป ทั้งนี้ขึ้นอยู่กับการวิเคราะห์ขององค์กรเกี่ยวกับปัจจัยที่มีผลต่อความสมเหตุสมผลของต้นทุนสำหรับการกระทำการแก้ไขต่อไป

บทที่ 4 สรุปช่องโหว่ที่ตรวจพบ

หัวข้อนี้ได้ถูกจัดทำขึ้นเพื่อบรรยายสรุปช่องโหว่ที่ตรวจพบและความเสี่ยงที่เกี่ยวข้องในระหว่างการการทดสอบเจาะระบบ ซึ่งมีดังต่อไปนี้

ตารางที่ : 10 สรุปช่องโหว่ที่ตรวจพบจากการเจาะระบบและความเสี่ยงที่เกี่ยวข้อง

ID	Vulnerabilities name	Risk	Fixing Status	Remark
การทดสอบประเภท VULNERABILITY ASSESSMENT ของ OPERATING SYSTEM				
1	ตรวจพบว่ามีการใช้ RHEL kernel package ที่ไม่อัพเดทในเครื่องเป้าหมาย	**สูง**	ปิดโดยการแก้ไข	
การทดสอบประเภท VULNERABILITY ASSESSMENT ของ IMAGE FILE				
ไม่พบช่องโหว่				

บทที่ 5 รายละเอียดของช่องโหว่จากการทดสอบหาช่องโหว่

หัวข้อนี้ถูกออกแบบขึ้นเพื่อให้มีข้อมูลที่เป็นรายละเอียดเกี่ยวกับผลการตรวจพบพร้อมกับคำแนะนำในการแก้ไข เพื่อเสริมสร้างความปลอดภัยของระบบ

5.1 ตรวจพบว่ามีการใช้ RHEL kernel package ที่ไม่อัพเดทในเครื่องเป้าหมาย

ผลการทดสอบซ้ำ

วิธีการแก้ไข	ระดับความเสี่ยง	สถานะช่องโหว่	หมายเหตุ
อัพเดท Version RHSA-2025:19409	**สูง**	ได้รับการแก้ไข	

ประเด็นข้อตรวจพบและผลกระทบ

CVE-2025-39702 – IPv6 SR MAC comparison timing issue

ปัญหาในส่วนของ IPv6 Segment Routing ที่เปรียบเทียบค่า MAC address ไม่เป็น constant time ผู้โจมตีสามารถใช้เวลาในการตอบสนอง (timing attack) เดา key หรือข้อมูลบางส่วนได้

CVE-2022-50367 – nilfs_mdt_destroy use-after-free

เกิดใน filesystem driver ของ NILFS (New Implementation of Log-structured File System) ฟังก์ชัน nilfs_mdt_destroy() อาจอ้างถึงหน่วยความจำที่ถูกคืนค่าแล้ว ⟶ kernel panic หรือ code execution

CVE-2023-53494 – crypto xts handle EBUSY error incorrectly

ใน crypto subsystem (xts mode) ไม่จัดการ error EBUSY อย่างถูกต้องผลคืออาจใช้ key หรือ buffer ผิด ทำให้การเข้ารหัสข้อมูลไม่ปลอดภัย หรือระบบล้มเหลวได้

สรุปผลกระทบ

ระบบที่รัน kernel เวอร์ชันเก่าจะ เปิดช่องให้โจมตีหน่วยความจำและ timing leak ในบางกรณี อาจถึงขั้นทำให้เครื่อง crash หรือรันโค้ดอันตรายบน kernel space ได้ ไม่มีผลเฉพาะ RHEL เท่านั้น — Oracle Linux, Rocky, Alma ที่ใช้ kernel เดียวกันก็ได้รับผลกระทบด้วย

ที่	เป้าหมายที่กระทบ
(1)	172.26.181.23 172.26.181.28 172.26.181.86 172.26.181.87 172.31.181.28

ที่	เป้าหมายที่กระทบ
	172.31.181.29 172.31.181.82 172.31.181.149 172.31.181.204

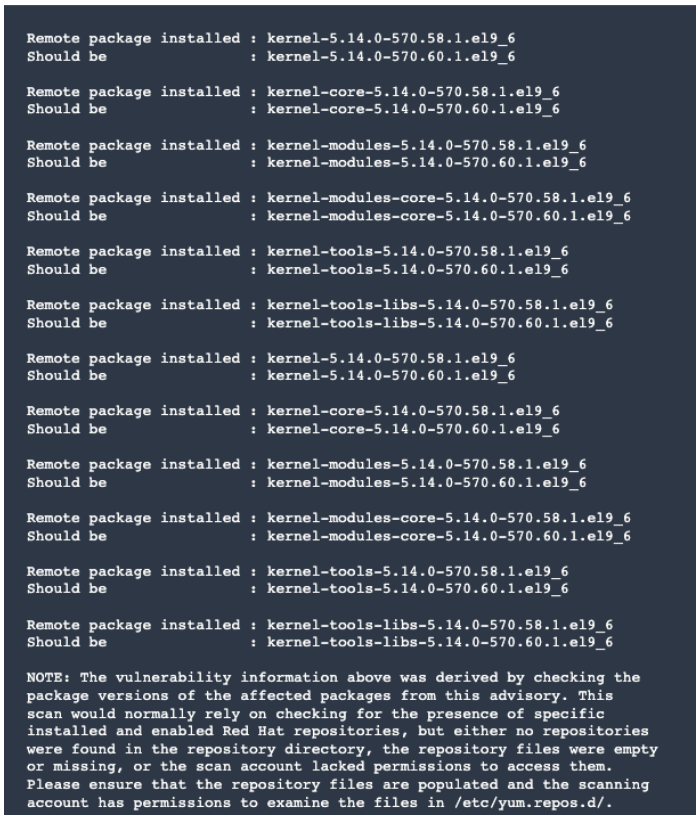
ระดับความเสี่ยง

ระดับความเสี่ยง	สูง	ความน่าจะเป็น	ปานกลาง
		ผลกระทบ	สูง
อ้างอิง	CVSS v3.0 Base Score: 7.8 CVSS v3.0 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C CVSS v3.0 Temporal Score: 6.8 CVSS v2.0 Base Score: 6.8 CVSS v2.0 Temporal Score: 5.0 CVSS v2.0 Vector: CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C CWE: 208, 416, 664 RHSA: 2025:19409 CVE: CVE-2022-50367, CVE-2023-53494, CVE-2025-39702		
คำอธิบายเพิ่มเติม	https://access.redhat.com/security/updates/classification/#moderate https://bugzilla.redhat.com/show_bug.cgi?id=2393533 https://bugzilla.redhat.com/show_bug.cgi?id=2396114 https://bugzilla.redhat.com/show_bug.cgi?id=2400777 http://www.nessus.org/u?928822f0 https://access.redhat.com/errata/RHSA-2025:19409		

คำแนะนำในการแก้ไข

คำอธิบาย
Update the RHEL kernel package based on the guidance in RHSA-2025:19409.

ตัวอย่างผลของการทดสอบ



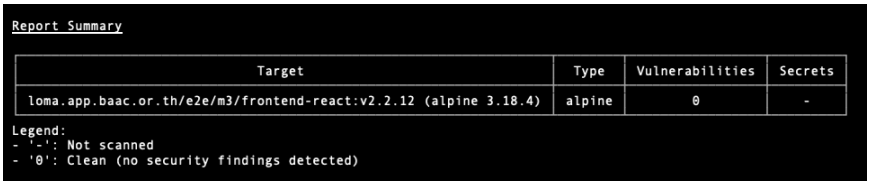
```
Remote package installed : kernel-5.14.0-570.58.1.el9_6
Should be                : kernel-5.14.0-570.60.1.el9_6

Remote package installed : kernel-core-5.14.0-570.58.1.el9_6
Should be                : kernel-core-5.14.0-570.60.1.el9_6

Remote package installed : kernel-modules-5.14.0-570.58.1.el9_6
Should be                : kernel-modules-5.14.0-570.60.1.el9_6

Remote package installed : kernel-modules-core-5.14.0-570.58.1.el9_6
Should be                : kernel-modules-core-5.14.0-570.60.1.el9_6

Remote package installed : kernel-tools-5.14.0-570.58.1.el9_6
Should be                : kernel-tools-5.14.0-570.60.1.el9_6

Remote package installed : kernel-tools-libs-5.14.0-570.58.1.el9_6
Should be                : kernel-tools-libs-5.14.0-570.60.1.el9_6

Remote package installed : kernel-5.14.0-570.58.1.el9_6
Should be                : kernel-5.14.0-570.60.1.el9_6

Remote package installed : kernel-core-5.14.0-570.58.1.el9_6
Should be                : kernel-core-5.14.0-570.60.1.el9_6

Remote package installed : kernel-modules-5.14.0-570.58.1.el9_6
Should be                : kernel-modules-5.14.0-570.60.1.el9_6

Remote package installed : kernel-modules-core-5.14.0-570.58.1.el9_6
Should be                : kernel-modules-core-5.14.0-570.60.1.el9_6

Remote package installed : kernel-tools-5.14.0-570.58.1.el9_6
Should be                : kernel-tools-5.14.0-570.60.1.el9_6

Remote package installed : kernel-tools-libs-5.14.0-570.58.1.el9_6
Should be                : kernel-tools-libs-5.14.0-570.60.1.el9_6

NOTE: The vulnerability information above was derived by checking the
package versions of the affected packages from this advisory. This
scan would normally rely on checking for the presence of specific
installed and enabled Red Hat repositories, but either no repositories
were found in the repository directory, the repository files were empty
or missing, or the scan account lacked permissions to access them.
Please ensure that the repository files are populated and the scanning
account has permissions to examine the files in /etc/yum.repos.d/.
```

บทที่ 6 ผลการทดสอบหาช่องโหว่

หัวข้อนี้ถูกออกแบบขึ้นเพื่อให้มีข้อมูลที่ข้อมูลที่เกี่ยวกับผลการตรวจพบพร้อมกับคำแนะนำในการแก้ไข เพื่อเสริมสร้างความปลอดภัยของระบบ โดยใน

6.1 การทดสอบหาช่องโหว่ Image Module M3

6.1.1 หลักฐานการตรวจ loma.app.baac.or.th/e2e/m3/frontend-react

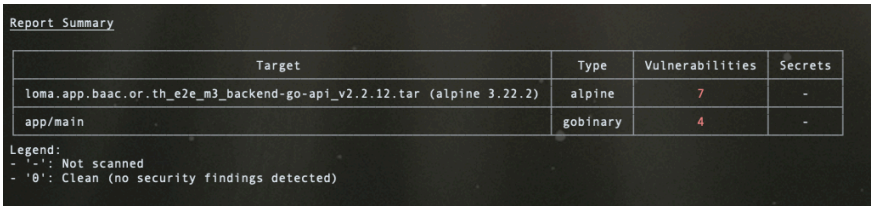


Report Summary

Target	Type	Vulnerabilities	Secrets
loma.app.baac.or.th/e2e/m3/frontend-react:v2.2.12 (alpine 3.18.4)	alpine	0	-

Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)

6.1.2 หลักฐานการตรวจ loma.app.baac.or.th/e2e/m3/Backend-go-api

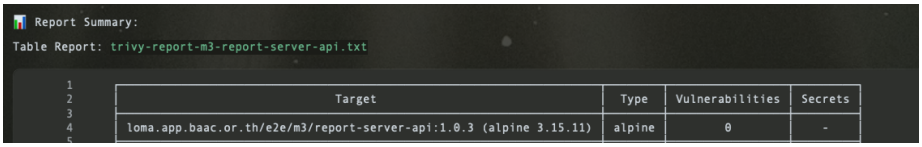


Report Summary

Target	Type	Vulnerabilities	Secrets
loma.app.baac.or.th_e2e_m3_backend-go-api_v2.2.12.tar (alpine 3.22.2)	alpine	7	-
app/main	gobinary	4	-

Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)

6.1.3 หลักฐานการตรวจ loma.app.baac.or.th/e2e/m3/Report-server-api

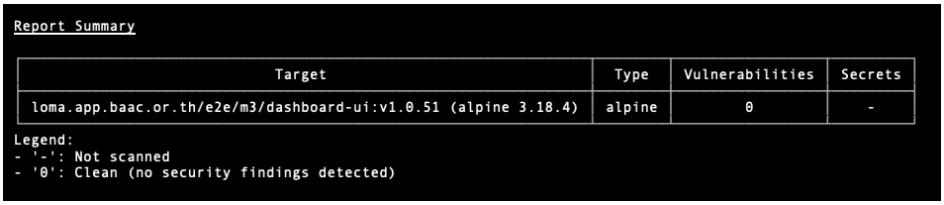


Report Summary:

Table Report: trivy-report-m3-report-server-api.txt

Target	Type	Vulnerabilities	Secrets
loma.app.baac.or.th/e2e/m3/report-server-api:1.0.3 (alpine 3.15.11)	alpine	0	-

6.1.4 หลักฐานการตรวจ loma.app.baac.or.th/e2e/m3/dashboard-ui

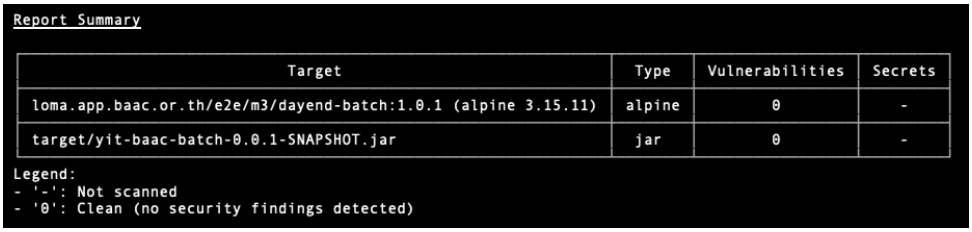


Report Summary

Target	Type	Vulnerabilities	Secrets
loma.app.baac.or.th/e2e/m3/dashboard-ui:v1.0.51 (alpine 3.18.4)	alpine	0	-

Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)

6.1.5 หลักฐานการตรวจ loma.app.baac.or.th/e2e/m3/dayend-batch



Report Summary

Target	Type	Vulnerabilities	Secrets
loma.app.baac.or.th/e2e/m3/dayend-batch:1.0.1 (alpine 3.15.11)	alpine	0	-
target/yit-baac-batch-0.0.1-SNAPSHOT.jar	jar	0	-

Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)

6.2 การทดสอบหาช่องโหว่ Image Module M4

6.2.1 หลักฐานการตรวจ Baaccoreservice20251110.tar

Report Summary

Target	Type	Vulnerabilities	Secrets
baaccoreservice20251110.tar (alpine 3.22.2)	alpine	0	-
usr/local/tomcat/bin/commons-daemon.jar	jar	0	-
usr/local/tomcat/bin/tomcat-juli.jar	jar	0	-
usr/local/tomcat/lib/annotations-api.jar	jar	0	-
usr/local/tomcat/lib/catalina-ant.jar	jar	0	-
usr/local/tomcat/lib/catalina-ha.jar	jar	0	-
usr/local/tomcat/lib/catalina-ssi.jar	jar	0	-
usr/local/tomcat/lib/catalina-storeconfig.jar	jar	0	-
usr/local/tomcat/lib/catalina-tribes.jar	jar	0	-
usr/local/tomcat/lib/catalina.jar	jar	0	-
usr/local/tomcat/lib/ecj-4.27.jar	jar	0	-
usr/local/tomcat/lib/el-api.jar	jar	0	-
usr/local/tomcat/lib/jakartaee-migration-1.0.9-shaded.jar	jar	0	-
usr/local/tomcat/lib/jasper-el.jar	jar	0	-
usr/local/tomcat/lib/jasper.jar	jar	0	-
usr/local/tomcat/lib/jaspic-api.jar	jar	0	-
usr/local/tomcat/lib/jsp-api.jar	jar	0	-
usr/local/tomcat/lib/servlet-api.jar	jar	0	-
usr/local/tomcat/lib/tomcat-api.jar	jar	0	-
usr/local/tomcat/lib/tomcat-coyote-ffm.jar	jar	0	-
usr/local/tomcat/lib/tomcat-coyote.jar	jar	0	-
usr/local/tomcat/lib/tomcat-dbcp.jar	jar	0	-
usr/local/tomcat/lib/tomcat-i18n-cs.jar	jar	0	-
usr/local/tomcat/lib/tomcat-i18n-de.jar	jar	0	-
usr/local/tomcat/lib/tomcat-i18n-es.jar	jar	0	-
usr/local/tomcat/lib/tomcat-i18n-fr.jar	jar	0	-
usr/local/tomcat/lib/tomcat-i18n-ja.jar	jar	0	-
usr/local/tomcat/lib/tomcat-i18n-ko.jar	jar	0	-
usr/local/tomcat/lib/tomcat-i18n-pt-BR.jar	jar	0	-
usr/local/tomcat/lib/tomcat-i18n-ru.jar	jar	0	-

usr/local/tomcat/lib/tomcat-i18n-zh-CN.jar	jar	0	-
usr/local/tomcat/lib/tomcat-jdbc.jar	jar	0	-
usr/local/tomcat/lib/tomcat-jni.jar	jar	0	-
usr/local/tomcat/lib/tomcat-util-scan.jar	jar	0	-
usr/local/tomcat/lib/tomcat-util.jar	jar	0	-
usr/local/tomcat/lib/tomcat-websocket.jar	jar	0	-
usr/local/tomcat/lib/websocket-api.jar	jar	0	-
usr/local/tomcat/lib/websocket-client-api.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/HikariCP-5.0.1.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/SparseBitSet-1.3.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/angus-activation-2.0.2.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/antlr4-runtime-4.13.0.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/bcprov-jdk18on-1.78.1.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/byte-buddy-1.15.11.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/checker-qual-3.33.0.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/classmate-1.7.0.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/commons-beanutils-1.11.0.j-ar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/commons-codec-1.17.2.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/commons-collections-3.2.2.-jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/commons-collections4-4.5.0--M2.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/commons-compress-1.26.2.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/commons-io-2.16.1.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/commons-lang3-3.18.0.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/commons-logging-1.3.5.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/commons-math3-3.6.1.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/curvesapi-1.08.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/error_prone_annotations-2.-18.0.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/failureaccess-1.0.1.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/guava-32.1.2-jre.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/hibernate-commons-annotati-ons-6.0.6.Final.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/hibernate-core-6.5.2.Final-.jar	jar	0	-
usr/local/tomcat/webapps/BAACCoreService/WEB-INF/lib/hibernate-hikaricp-6.5.2.F-inal.jar	jar	0	-

6.3 การทดสอบหาช่องโหว่ Image Module COJ

6.3.1 หลักฐานการตรวจ baac-api-backend.tar and app/app.jar

Report Summary

Target	Type	Vulnerabilities	Secrets
baac-api-backend.tar (alpine 3.22.2)	alpine	0	-
app/app.jar	jar	0	-

Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)

6.3.2 หลักฐานการตรวจ baac-api-frontend.tar

Report Summary

Target	Type	Vulnerabilities	Secrets
baac-api-frontend.tar (alpine 3.21.5)	alpine	0	-

Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)