การวิเคราะห์และเสนอแนวทางการจัดการช่องโหว่สำหรับเว็บแอปพลิเคชัน

นายพศวีร์ จงอยู่สุขสันต์

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2567
ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

การวิเคราะห์และเสนอแนวทางการจัดการช่องโหว่สำหรับเว็บแอปพลิเคชัน

นายพศวีร์ จงอยู่สุขสันต์

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2567
ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ใบรับรองการค้นคว้าอิสระ

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง การวิเคราะห์และเสนอแนวทางการจัดการช่องโหว่สำหรับเว็บแอปพลิเคชัน

โดย นายพศวีร์ จงอยู่สุขสันต์

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

คณบดีบัณฑิตวิทยาลัย / หัวหน้าภาควิชา

คณะกรรมการสอบการค้นคว้าอิสระ

..... ประธานกรรมการ
(สุมิตรา นวลมีศรี)

..... อาจารย์ที่ปรึกษา
(สุนันฑา สดสี)

..... กรรมการ
(สุนันฑา สดสี)

..... กรรมการ
(นวพร วิสิฐพงศ์พันธ์)

ชื่อ : นายพศวีร์ จงอยู่สุขสันต์
ชื่อการค้นคว้าอิสระ : การวิเคราะห์และเสนอแนวทางการจัดการช่องโหว่สำหรับเว็บแอปพลิเคชัน
สาขาวิชา : การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก : สุนันฑา สดสี
ปีการศึกษา : 2567

บทคัดย่อ

การวิจัยนี้มุ่งเน้นไปที่การวิเคราะห์กรอบการทำงาน NIST CSF 2.0 Adaptive และมาตรฐานสากลเพื่อกำหนดเกณฑ์การประเมินสำหรับองค์กร โดยมีวัตถุประสงค์เพื่อพัฒนาหลักเกณฑ์ด้านความปลอดภัยทางไซเบอร์สำหรับการปรับปรุงเว็บแอปพลิเคชัน ในงานนี้ ได้เลือกเว็บแอปพลิเคชันหลัก จำนวน 3 ระบบ รวมถึงเครื่องมือการประเมินช่องโหว่ จำนวน 3 เครื่องมือ ซึ่งพิจารณาโดยใช้ 7Ps Algorithm ในท้ายสุดจึงได้เครื่องมือที่เหมาะสมกับองค์กรที่สุดสำหรับใช้ในการค้นคว้าอิสระ คือ Zed Attack Proxy (ZAP) ในความเป็นจริง หลักเกณฑ์ที่พัฒนาขึ้นจะถูกนำไปใช้เพื่อเสริมความปลอดภัยของระบบ และใช้เป็นข้อมูลอ้างอิงทางด้านเทคนิคสำหรับการพัฒนาระบบดังกล่าว อย่างไรก็ตามผลลัพธ์จากการประเมินของผู้เชี่ยวชาญ จำนวน 3 ท่าน แสดงให้เห็นว่าหลักเกณฑ์นี้สามารถยอมรับได้ และมีประสิทธิภาพ นอกจากนี้ยังสามารถนำไปใช้ในสถานการณ์จริงได้อย่างมีประสิทธิภาพ

(มีจำนวนทั้งสิ้น 65 หน้า)

คำสำคัญ : การวิเคราะห์ช่องโหว่ ยกระดับความมั่นคงปลอดภัยของเว็บแอปพลิเคชัน การประเมินความเสี่ยงองค์กร

_____ อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก

Name : Mr. Photsawi Chongyusuksan
Independent Study Title : Analysing and Guiding of Vulnerability Management for Web Application
Major Field : Network and Information Security Management
King Mongkut's University of Technology North Bangkok
Independent Study Advisor : Sunantha Sodsee
Academic Year : 2024

ABSTRACT

This research focuses on analysing the NIST CSF 2.0 adaptive framework. And the international standards to establish an evaluation criteria for the organization, in order to developing the cybersecurity guidelines on web Application enhancement. Here in, three main Web Application Systems are selected, as well as three Vulnerability Assessment Tools are also considered by using the proposed 7Ps algorithm. Finally, the most suitable tool is applied in this work, which is Zed Attack Proxy (ZAP). In fact, the developed guideline is implemented to entrance the security of the systems, and serve as a technical reference for developing them. The result by three exports has been shown that, this guideline is acceptable and effective. As well as, it can apply for working in the realistic situation

(Total 65 Pages)

Keywords: Web Application Vulnerabilities, NIST CSF 2.0, Vulnerability Analysis

_____ Advisor

กิตติกรรมประกาศ

การค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงไปได้ด้วยความช่วยเหลือเป็นอย่างดี จากผู้ช่วยศาสตราจารย์ ดร.สุนันฑา สดสี อาจารย์ที่ปรึกษาการค้นคว้าอิสระ ที่ให้คำปรึกษาอันมีค่า รวมถึงติดตามความคืบหน้าของงานอย่างใกล้ชิด ซึ่งช่วยให้ผู้วิจัยสามารถจัดทำการค้นคว้าอิสระให้มีความสมบูรณ์มากยิ่งขึ้น และขอขอบคุณคณาจารย์ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศทุกท่านที่ได้ถ่ายทอดความรู้ให้คำแนะนำ ซึ่งผู้วิจัยได้นำมาประยุกต์ใช้และเป็นประโยชน์ในการจัดทำการค้นคว้าอิสระนี้

นอกจากนี้ ผู้วิจัยขอขอบคุณ ท่านผู้เชี่ยวชาญในองค์กร เพื่อนร่วมงาน และครอบครัว ที่คอยให้กำลังใจ และสนับสนุนในทุกๆ ด้าน ซึ่งถือเป็นส่วนสำคัญอย่างยิ่งที่ช่วยให้ข้าพเจ้ามีแรงผลักดันในการทำการค้นความอิสระจนสำเร็จ

สุดท้ายนี้ ผู้วิจัยหวังว่าการค้นคว้าอิสระฉบับนี้จะเป็นประโยชน์ต่อผู้ที่สนใจและสามารถนำไปต่อยอดเพื่อพัฒนาความรู้ในอนาคตต่อไป

พศวีร์ จงอยู่สุขสันต์

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญรูปภาพ

ภาพที่ หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในช่วงไม่กี่ปีที่ผ่านมา ประเทศไทยมีรายงานภัยคุกคามทางไซเบอร์เพิ่มขึ้นอย่างรวดเร็ว อ้างอิงจากสถิติภัยคุกคามทางไซเบอร์ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ [1] ปี พ.ศ. 2565 และ ปี พ.ศ. 2566 ให้ข้อมูลว่า หน่วยงานภาครัฐถูกโจมตีสูงสุดเป็นอันดับที่ 2 ในปี 2565 ถูกโจมตีจำนวน 243 ครั้ง และในปี 2566 ถูกโจมตีจำนวน 461 ครั้ง เห็นได้ชัดว่าภายใน 1 ปี ภัยคุกคามทางไซเบอร์เพิ่มขึ้นเป็นเท่าตัว โดยมีรูปแบบภัยคุกคาม ได้แก่ 1) การโจมตีเว็บไซต์เพื่อปรับเปลี่ยนให้เป็นเว็บไซต์การพนัน (Hacked Website (Gambling)) เกิดขึ้นมากที่สุดจำนวน 515 เหตุการณ์ 2) การโจมตีเว็บไซต์เพื่อปรับเปลี่ยนหน้าเว็บไซต์ (Hacked Website (Defacement)) เกิดขึ้นมากสุดเป็นอันดับที่ 2 จำนวน 336 เหตุการณ์ และ 3) ภัยคุกคามจุดอ่อนช่องโหว่ (Vulnerability) เกิดขึ้นมากสุดเป็นอันดับที่ 4 จำนวน 228 เหตุการณ์ ซึ่งการเพิ่มขึ้นของภัยคุกคามทางไซเบอร์ที่ได้กล่าวมาสะท้อนให้เห็นถึงความจำเป็นในการหาแนวทางรักษาความมั่นคงปลอดภัยของเว็บแอพลิเคชันหน่วยงานภาครัฐอย่างเร่งด่วน เพื่อป้องกันผลกระทบที่ร้ายแรงในอนาคต

หน่วยงานภาครัฐมีการใช้เทคโนโลยี Web Application เป็นช่องทางหลักในการให้บริการ ซึ่งให้ความสำคัญเรื่องความปลอดภัยเป็นอย่างมาก แต่ด้วยเทคโนโลยีมีความก้าวหน้าอย่างรวดเร็ว ภัยคุกคามทางไซเบอร์จึงมีความซับซ้อนมากขึ้น ส่งผลให้ Web Applications ดังกล่าวอาจตกเป็นเป้าหมายเสี่ยงถูกโจมตี ส่งผลให้ไม่สามารถให้บริการ ข้อมูลรั่วไหลและสูญหาย เสื่อมเสียชื่อเสียง และความน่าเชื่อถือของหน่วยงานได้ หากขาดการตรวจสอบ รวมถึงปรับปรุงแนวทางการรักษาความมั่นคงปลอดภัยของเทคโนโลยีอย่างสม่ำเสมอ อย่างไรก็ตามในระดับสากล มีการจัดอันดับความเสี่ยงด้านความปลอดภัยของ Web Application เพื่อให้องค์กรต่าง ๆ ทั่วทุกมุมโลก สามารถนำข้อมูลไปใช้ป้องกันองค์กรได้อย่างถูกต้องและเท่าทันเหตุการณ์ที่เกิดขึ้น โดย 10 อันดับของความเสี่ยงของ Web Application ปี พ.ศ. 2564 ที่จัดอันดับโดยองค์กร Open Web Application Security Project (OWASP Top Ten 2021) [2] อาทิ A01:2021-Broken Access Control, A02:2021-Cryptographic Failures, A03:2021-Injection, A04:2021-Insecure Design, A05:2021- Security Misconfiguration, A06:2021-Vulnerable and Outdated Components เป็นต้น ดังนั้น การปฏิบัติตาม OWASP Top Ten 2021 จึงเป็นสิ่งสำคัญในการเพิ่มประสิทธิภาพความมั่นคงปลอดภัยให้ Web Application ของหน่วยงานภาครัฐ ซึ่งจะช่วยลดความเสี่ยงการถูกโจมตีจากภัยคุกคามทางไซเบอร์ และสามารถให้บริการประชาชนได้อย่างต่อเนื่อง

ขณะนี้หน่วยงานภาครัฐตระหนักถึงความสำคัญของการทดสอบความมั่นคงปลอดภัยของ Web Applications ซึ่งมีหน่วยงานภายนอกทำหน้าที่ให้บริการตรวจประเมินความมั่นคงปลอดภัยของหน่วยงาน (Vulnerability Assessment) จำนวนมากเข้ามาให้ความรู้ พร้อมเสนอบริการ แต่ยังคงมีความกังวลในการเปิดเผยโครงสร้างระบบ และเทคโนโลยี กับบุคคลภายนอกที่จะเข้ามาตรวจสอบ รวมทั้งงบประมาณที่มีจำกัด ส่งผลให้ยังไม่สามารถดำเนินการทดสอบความปลอดภัยขององค์กรได้

จากสถานการณ์ข้างต้น ผู้วิจัยจึงนำองค์ความรู้ เทคโนโลยี และมาตรฐาน/แนวปฏิบัติสากลมาประยุกต์ใช้ในการศึกษา กำหนดเกณฑ์ ประเมินองค์กรพร้อมวิเคราะห์จุดเปราะบาง ตรวจสอบระบบด้วยเครื่องมือตรวจสอบและระบุช่องโหว่ (Vulnerability Assessment Tools: VA Tools) พร้อมคัดเลือกเครื่องมือ VA Tools รวมถึงจัดทำปฏิบัติการยกระดับความมั่งคงปลอดภัยทางไซเบอร์ขององค์กร เพื่อให้หน่วยงานได้ทราบถึงความเสี่ยงที่อาจโดนโจมตีจากภัยคุกคามทางไซเบอร์ และดำเนินการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ และที่สำคัญยิ่งไปกว่านั้นหน่วยงานที่มีสภาพแวดล้อมคล้ายคลึงกันสามารถใช้แผนฯ เป็นข้อมูลประกอบทางด้านเทคนิค (Technical Requirements) ให้กับบุคลากรที่ทำหน้าที่พัฒนา Web Application หน่วยงาน ทั้งที่มีอยู่เดิม รวมถึงที่จะพัฒนาขึ้นใหม่เพื่อให้ Web Application มีประสิทธิภาพและยกระดับความมั่นคงปลอดภัยทางไซเบอร์เพื่อรับมือกับภัยคุกคามทางไซเบอร์ในอนาคตได้อย่างยั่งยืน

1.2 วัตถุประสงค์

1.2.1 เพื่อวิเคราะห์และตรวจสอบความมั่นคงปลอดภัยของ Web Application ของหน่วยงาน พร้อมจัดทำรายงานผลการวิเคราะห์และตรวจสอบความมั่นคงปลอดภัยรวมถึงกำหนดแนวทางการยกระดับความมั่นคงปลอดภัยนั้น

1.2.2 เพื่อวัดและประเมินความเป็นไปได้ของแนวทางการยกระดับความมั่นคงปลอดภัย รวมถึงความเป็นประโยชน์ของแนวทางการยกระดับความมั่นคงปลอดภัยของ Web Application ของหน่วยงาน

1.3 ขอบเขตของการวิจัย

1.3.1 ศึกษา วิเคราะห์ และประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร โดยประยุกต์ใช้กรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ เวอร์ชัน 2.0 ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ ประเทศสหรัฐอเมริกา (NIST Cybersecurity Framework 2.0: NIST CSF 2.0) [3]

1.3.2 ศึกษา และคัดเลือก Web Applications ขององค์กร ที่มีผลการประเมินความเสี่ยง (Risk Assessment) สูงสุด 3 อันดับ โดยใช้เกณฑ์การพิจารณาความเสี่ยงขององค์กร [4]

1.3.3 ศึกษา และคัดเลือก VA Tools จำนวน 3 เครื่องมือ จากรายชื่อเครื่องมือที่ OWASP เผยแพร่ โดยประยุกต์ใช้ทฤษฎี 7 Rights of Logistics [5]

1.3.4 ศึกษา และกำหนดวิธีการตรวจสอบและระบุช่องโหว่ โดยใช้ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงพื้นฐานสำคัญทางสารสนเทศ

1.3.5 ดำเนินการตรวจสอบและระบุช่องโหว่ ตามข้อ 3.4 โดยใช้ VA Tools ตามข้อ 1.3.3 ตรวจสอบ Web Applications ตามข้อ 3.2 และบันทึกผลการตรวจสอบ

1.3.6 คัดเลือก VA Tools ที่มีประสิทธิภาพสูงสุด 1 เครื่องมือ ซึ่งคำนวณได้จากผลคูณของระดับความรุนแรงฯ และจำนวนช่องโหว่ที่พบในผลการตรวจสอบ ตามข้อ 3.5

1.3.7 ศึกษา วิเคราะห์ และกำหนดแนวทางการแก้ไขช่องโหว่ ที่พบในผลการตรวจสอบ ตามข้อ 3.5 ของ VA Tools ที่มีประสิทธิภาพสูงสุด ตามข้อ 3.6 โดยสอดคล้องมาตรฐานสากล

1.3.8 ศึกษา วิเคราะห์ และจัดทำแนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร โดยใช้ผลลัพธ์การประเมินความเสี่ยงฯ ตามข้อ 3.1 กฎ ระเบียบ ข้อบังคับ นโยบาย มาตรฐาน และแนวปฏิบัติในระดับสากล และระดับประเทศ

1.3.9 เสนอแนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร ตามข้อ 1.3.8 ให้กลุ่มเป้าหมายพิจารณา โดยการประเมินความเหมาะสม และความพึงพอใจ

1.4 ประโยชน์ของการวิจัย

1.4.1 หน่วยงานทราบถึงความเสี่ยงที่ได้จากผลการวิเคราะห์และตรวจสอบความมั่นคงปลอดภัยของ Web Application รวมถึงแนวทางการยกระดับความมั่นคงปลอดภัยของ Web Application หน่วยงานสามารถนำแนวทางการยกระดับ Web Application รวมถึงแนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรไปใช้เพิ่มประสิทธิภาพความมั่นคงปลอดภัยได้

บทที่ 2
แนวคิดทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 เครื่องมือประเมินตนเอง (Self Assessment Tools)

Expel Self-Assessment Tools เครื่องมือที่ช่วยองค์กรประเมินความพร้อมและความสามารถด้านความปลอดภัยไซเบอร์ เช่น การรับมือกับแรนซัมแวร์ การตอบสนองต่อเหตุการณ์ และการรักษาความปลอดภัยในระบบคลาวด์ เครื่องมือเหล่านี้ช่วยให้ทีมตรวจจับและตอบสนองภัยคุกคามได้ดียิ่งขึ้น พร้อมแนะนำการปรับปรุงตามมาตรฐานอุตสาหกรรม ช่วยให้การรักษาความปลอดภัยมีประสิทธิภาพมากขึ้น [6]

ภาพที่ 2-1 Expel Self-Assessment Tools

2.2 เครื่องมือค้นหาช่องโหว่เว็บแอปพลิเคชัน (Vulnerability Assessment : VA SCAN)

2.2.1 ปัจจุบันเว็บแอปพลิเคชันถูกพัฒนาขึ้นมาด้วยเทคโนโลยีที่มีความหลากหลาย ส่งผลให้มีภัยคุกคามในรูปแบบที่แตกต่างมากมายด้วยเช่นกัน ด้วยสาเหตุนี้จึงมีเครื่องมือค้นหาช่องโหว่เว็บแอปพลิเคชันเพื่อใช้สำหรับค้นหาช่องโหว่ อาทิ ข้อผิดพลาดจากการพัฒนาเว็บแอปพลิเคชัน การตั้งค่าเซิร์ฟเวอร์ที่ไม่ปลอดภัย เป็นต้น โดยบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ได้แนะนำ 10 เครื่องมือสำหรับตรวจสอบความปลอดภัยเว็บไซต์ ซึ่งสามารถสรุปได้ดังนี้ ดังนี้

2.2.2 SQLMap คือเครื่องมือตรวจสอบความปลอดภัยเว็บไซต์โดยการระบุช่องโหว่ SQL injection พร้อมรายงานผลการทดสอบ SQL Injection แบบละเอียดโดยเฉพาะ ซึ่งเครื่องมือดังกล่าวไม่เสียค่าใช้จ่ายในการนำมาใช้งาน อีกทั้งยังติดตั้งลงบนเครื่องคอมพิวเตอร์ของผู้ทดสอบ ทำให้ข้อมูลที่สำคัญมีความปลอดภัยในขณะใช้งาน ตัวอย่าช่องโหว่ที่สามารถตรวจสอบได้ อาทิ Boolean-based blind, Error-based, Out-of-band, Stacked queries, Time-based blind, UNION query

2.2.3 NMAP คือเครื่องมือตรวจสอบความปลอดภัยที่ใช้สำหรับค้นหา Port และ Service ที่เปิดใช้งานอยู่บน Network

2.2.4 ZAP คือครื่องมือตรวจสอบความปลอดภัยของเว็บแอปพลิเคชันที่มีฟังกช์ชันหลากหลาย รวมถึงมีความละเอียดและครอบคลุมเนื่องจากถูกพัฒนาโดย OWASP (The Open Web Application Security Project) ซึ่งเป็นมูลนิธิไม่แสวงผลประโยชน์ และมีวัตถุประสงค์เพื่อยกระดับความมั่นคงปลอดภัยให้กับเว็บแอปพลิเคชัน เป็นที่รู้จักกันในชื่อของ OWASP Top Ten ยิ่งไปกว่านั้นเป็นเครื่องมือ Open source สำหรับทำ Penetration test เพื่อตรวจสอบช่องโหว่ตาม OWAS Top Ten ตัวอย่าช่องโหว่ที่สามารถตรวจสอบได้ อาทิ Cookie not HttpOnly flag, Missing anti-CSRF tokens and security headers, Private IP disclosure, Session ID in URL rewrite, SQL injection, XSS injection

2.2.5 Nikto คือเครื่องมือตรวจสอบความปลอดภัยของเว็บแอปพลิเคชัน โดยสามารถตรวจสอบการตั้งค่าเซิร์ฟเวอร์ที่ไม่ปลอดภัย รวมถึงช่องโหว่โดยทั่วไปได้อย่างมีประสิทธิภาพ เป็นเครื่องมือที่สามารถใช้งานได้ฟรี

2.2.6 OpenVAS คือเครื่องมือตรวจสอบความปลอดภัยของเว็บแอปพลิเคชัน แต่การการอัพเดทข้อมูลไม่สม่ำเสมอ

2.2.7 Wapiti คือเครื่องมือตรวจสอบความปลอดภัยของเว็บแอปพลิเคชัน โดยสามารถค้นหาช่องโหว่ของเว็บแอปพลิเคชันได้อัตโนมัติ สนับสนุนการใช้งานหลายภาษา และรองรับการสแกนเว็บแอปพลิเคชันที่มีเทคโนโลยีหลากหลาย

2.2.8 Arachni คือเครื่องมือตรวจสอบความปลอดภัยของเว็บแอปพลิเคชัน โดยสามารถสแกนช่องโหว่ได้อัตโนมัติ สร้างรายงานระดับความรุนแรงของช่องโหว่ รวมถึงสามารถสแกนเว็บแอปพลิเคชันที่มีความซับซ้อน และตรวจสอบเส้นทางของเว็บแอปพลิเคชันได้อีกด้วย

2.2.9 Skipfish คือเครื่องมือตรวจสอบความปลอดภัยของเว็บแอปพลิเคชัน โดยสามารสแกนช่องโหว่ของเว็บแอปพลิเคชันได้อัตโนมัติ มีความเร็วในการสแกนที่สูงมาก รวมถึงสามารถจัดเรียงความสำคัญของช่องโหว่ได้

2.2.10 ผู้วิจัยจึงสามารถสรุปได้ว่าปัจจุบันมีเครื่องมือจำนวนมากในท้องตลาด มีความสามารถรวมถึงคุณสมบัติที่แตกต่างกันเฉพาะด้าน เครื่องมือบางชนิดถูกสร้างขึ้นมาเพื่อตรวจสอบ SQL Injection, Port หรือ Service และ Penetration test โดยเฉพาะ ซึ่งเป็นเรื่องยากในการการคัดเลือกเครื่องมือสำหรับการทำวิจัยนี้ให้มีประสิทธิภาพ ทำให้ควรศึกษาหลักการ7R Logistics เพิ่มเติมเพื่อให้มีหลักการในการคัดเลือกเครื่องมือที่เหมาะสมที่สุด

2.3 หลักการ 7R ในการจัดหาโลจิสติกส์

หลักการ 7R เป็นแนวทางที่ช่วยให้กระบวนการตอบสนองความต้องการของลูกค้าเป็นไปตามเป้าหมาย โดยเน้นการส่งมอบสินค้าและบริการอย่างมีประสิทธิภาพสูงสุด เพื่อสร้างความพึงพอใจให้แก่ลูกค้า ซึ่งสามารถสรุปได้ดังนี้

2.3.1 Right Product คัดเลือกสินค้าที่เหมาะสมและตรงกับความต้องการของลูกค้า

2.3.2 Right Quantity จัดส่งสินค้าด้วยจำนวนที่ถูกต้องตามความต้องการ

2.3.3 Right Condition รับประกันว่าสินค้าอยู่ในสภาพสมบูรณ์ ไม่มีความเสียหาย

2.3.4 Right Customer มั่นใจว่าสินค้าถูกส่งถึงลูกค้ากลุ่มเป้าหมายโดยไม่มีข้อผิดพลาด

2.3.5 Right Place ส่งมอบสินค้าถึงจุดหมายปลายทางที่ถูกต้อง

2.3.6 Right Time จัดส่งสินค้าให้ถึงมือลูกค้าภายในกรอบเวลาที่กำหนดไว้

ซึ่งสามารถสรุปได้ ดังนี้

ภาพที่ 2-2 หลัก 7 Rs ของโลจิสตกส์

ผู้วิจัยจึงสามารถสรุปได้ว่า เพื่อให้การเลือกเครื่องมือตรวจสอบช่องโหว่ได้มีประสิทธิภาพตอบสนองต่อความต้องการของหน่วยงาน และตรงกับวัตถุประสงค์ในการทำวิจัยสามารถนำหลักการ 7R มาใช้ในการเลือกเครื่องมือตรวจสอบความปลอดภัยได้ อย่างไรก็ตามเพื่อให้การวิจัยนี้มีแนวทางการปฏิบัติที่ดีด้านการบริหารจัดการความเสี่ยง และเพื่อเป็นการยกระดับความมั่นคงปลอดภัย จึงศึกษาเพิ่มเติมในเรื่อง กรอบการทำงานด้าน Cybersecurity [7]

2.4 NIST Cybersecurity Framework Version 2.0

“NIST Cybersecurity Framework Version 2.0 เป็นกรอบการทำงานด้าน Cybersecurity ที่เป็นที่นิยมใช้อย่างมากในปัจจุบัน โดยในหลายๆองค์กรนำ NIST เข้ามาประยุกต์ใช้เพื่อรับมือกับภัยคุกคามทางไซเบอร์ ซึ่งเป็นหลักการ และแนวทางปฏิบัติที่ดีที่สุดที่ของการบริหารจัดการความเสี่ยง เพื่อเป็นการยกระดับความมั่นคงปลอดภัย” [8] อีกทั้งยังเป็นการยกระดับองค์กรให้มีกรอบการทำงานด้าน Cybersecurity พร้อมทั้งประเมินความเสี่ยงทั้ง 6 ด้าน สามารถสรุปได้ดังนี้

2.4.1 Govern คือการกำกับดูแลความมั่นคงไซเบอร์ต้องเข้าใจบริบทองค์กร กำหนดความเสี่ยงที่ยอมรับได้ และมีมาตรการควบคุมที่ชัดเจน เพื่อจัดการความเสี่ยงทั้งภายในและจากภายนอกอย่างมีประสิทธิภาพ

2.4.2 Identify คือการระบุสภาพแวดล้อม ความเสี่ยงในส่วนต่างๆ เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

2.4.3 Protect คือการป้องกันที่เหมาะสม เพื่อจำกัดระดับผลกระทบและลดโอกาสเกิดความเสี่ยง

2.4.4 Detect คือการตรวจหาเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น เพื่อตรวจติดตามอย่างต่อเนื่อง

2.4.5 Respond คือเป็นการดำเนินการตอบสนองต่อความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

2.4.6 Recover คือเป็นการดำเนินการกู้คืนระบบสารสนเทศที่ได้รับความเสียหายจากการถูกคุกคามด้านไซเบอร์

ภาพที่ 2-3 กรอบการทำงาน NIST FRAMEWORK

จากกรอบการทำงานด้าน Cybersecurity ข้างต้นจะช่วยให้ผู้จัยมีขอเขตการดำเนินงานที่ชัดเจนอีกทั้งยังสามารถระบุถึงความเสี่ยงในส่วนต่างๆ เพื่อให้สามารถยกระดับความมั่นคงปลอดภัยได้มีประสิทธิภาพสูงสุด อย่างไรก็ตามสิ่งที่สำคัญถัดมาคือการประเมินความเสี่ยงที่ระบุได้จึงจำเป็นต้องศึกษา OWAS Top Ten เพิ่มเติมเพื่อให้ทราบถึงระดับความรุนแรงต่างๆ ได้อย่างชัดเจน

2.5 OWAS Top Ten

NT cyfence จากบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ได้ให้ข้อมูลเกี่ยวกับ OWAS Top Ten ไว้สามารถสรุป ได้ดังนี้ OWAS Top Ten คือโครงการของ OWASP ที่จัดอันดับความเสี่ยงทางด้านความมั่นคงปลอดภัยของเว็บแอปพลิเคชันไว้ 10 อันดับ โดยทุกๆ 4 ปี จะมีการจัดอันดับช่องโหว่ใหม่เพื่อให้องค์กรทั่วโลกนำข้อมูลไปใช้เพื่อปกป้องเว็บแอปพลิเคชันขององค์กร สำหรับ OWASP Top Ten จะมีรายละเอียดดังภาพ

ภาพที่ 2-4 OWASP Top 10 list

2.6 งานวิจัยที่เกี่ยวข้อง

วิจัยเรื่อง “Penetration testing and Vulnerability Assessment for Websites” การตรวจจับช่องโหว่ที่ทราบทั้งหมดของเว็บแอปพลิเคชัน โดยระบบจะได้รับการปรับปรุงตามมาตรฐาน OWASP ใช้ Python Script ในการวิเคราะห์และรวบรวมข้อมูล ซึ่งมีวิธีการวิจัย ดังนี้ 1)ทดสอบจุดอ่อนด้านความปลอดภัยของเว็บแอปพลิเคชัน 2) การศึกษาการทดสอบการเจาะโดยใช้ Metasploit Framework 3) การประเมินช่องโหว่และการทดสอบการเจาะระบบในฐานะเทคโนโลยีการป้องกันทางไซเบอร์ 4) การทดสอบช่องโหว่และการเจาะระบบ 5) การรักษาความปลอดภัยของคอมพิวเตอร์ [9]

วิจัยเรื่อง “Vulnerability Assessment with Network-Based Scanner Method for Improving Website Security”การทดสอบนี้คือเว็บไซต์มีช่องโหว่ที่ระบุโดยใช้ NMAP และ WPScan การค้นพบ NMAP เกี่ยวข้องกับพอร์ตที่เปิดเป็นหลัก ในขณะที่การค้นพบ WPScan เกี่ยวข้องกับการกำหนดค่าและคุณสมบัติต่างๆ ผู้ดูแลเว็บไซต์จะต้องดำเนินการทันทีเพื่อแก้ไขช่องโหว่เหล่านี้ ในด้านเครือข่าย ควรกำหนดค่าไฟร์วอลล์ให้บล็อกหรือจำกัดการเข้าถึงพอร์ตที่เปิดอยู่ และควรใช้มาตรการรักษาความปลอดภัยที่เหมาะสม เช่น ระบบตรวจจับการบุกรุก และการแบ่งส่วนเครือข่าย ในแอปพลิเคชัน WordPress จำเป็นต้องปิดใช้งานคุณสมบัติที่ไม่จำเป็น กำหนดค่าอย่างถูกต้อง และปรับใช้การอัปเดตแพตช์ที่จำเป็น นอกจากนี้ การอัปเดต WordPress ปลั๊กอิน และธีมเป็นประจำสามารถลดช่องโหว่และปรับปรุงมาตรการรักษาความปลอดภัยของเว็บไซต์ได้อย่างมาก ซึ่งมีวิธีการวิจัย ดังนี้ 1) วิเคราะห์ความต้องการ (Requirement Analysis) 2) เลือกเครื่องมือสำหรับใช้ตรวจสอบช่องโหว่ (Selection of tools for vulnerability scanning) 3) ทดสอบค้นหาช่องโหว่ระบบ (Testing) 4) วิเคราะห์ช่องโหว่ที่ตรวจพบ (Analyze Result) [10]

วิจัยเรื่อง “A Review of the OW ASP Top 10 Web Application Security Risks and Best Practices for Mitigating These Risks” นำเสนอการวิเคราะห์อย่างละเอียดเกี่ยวกับช่องโหว่ด้านความปลอดภัยของเว็บแอปพลิเคชัน OW ASP 10 อันดับแรก รวมถึงความสำคัญ ผลที่ตามมา และรับมือกับผลกระทบที่แนะนำ วัตถุประสงค์ของการศึกษานี้รวมถึงการประเมินรายชื่อ 10 อันดับแรกล่าสุด และตรวจสอบว่าช่องโหว่เหล่านี้เกิดขึ้นบ่อยเพียงใดในสถานการณ์จริง การศึกษายังมุ่งเน้นไปที่การตรวจสอบสาเหตุที่แท้จริงของช่องโหว่เหล่านี้ และค้นหาว่าช่องโหว่เหล่านี้มีลักษณะใดบ้าง การทำเช่นนี้ การศึกษาหวังที่จะให้ความกระจ่างเกี่ยวกับสาเหตุที่แท้จริงของการคงอยู่ของอันตรายเหล่านี้ตลอดจนวิธีที่ดีที่สุดในการลดอันตรายเหล่านี้ เป้าหมายโดยรวมของการศึกษาครั้งนี้คือเพื่อให้ผู้มีอำนาจตัดสินใจ ผู้เชี่ยวชาญด้านความปลอดภัย และนักพัฒนามีทรัพยากรที่เป็นประโยชน์ในการปรับปรุงความปลอดภัยของเว็บแอปพลิเคชันของตน และป้องกันภัยคุกคามที่อาจเกิดขึ้น ซึ่งมีวิธีการวิจัย ดังนี้ 1) ศึกษากรณีศึกษา (Case Study) 2) วิเคราะห์อย่างละเอียดเกี่ยวกับช่องโหว่ 3) วิธีการรับมือกับผลกระทบ และแนวทางการจัดการกับปัญหา (Mitigations and Best Practices) 4) ประเมินช่องโหว่ที่มีการเกิดขึ้นบ่อยครั้งเพื่อให้ทราบถึงช่องโหว่ที่แท้จริง [11]

วิจัยเรื่อง “Web Application Penetration Testing & Patch Development Using Kali Linux” การตรวจจับช่องโหว่ที่อันตรายที่สุดและทันสมัยที่สุด อ้างอิงตามมาตรฐานการโจมตี 10 อันดับแรกของ OWASP โดยพัฒนาเป็นเว็บ Portal ที่ผู้ใช้สามารถเข้าสู่ระบบและใช้บริการทดสอบ

ความปลอดภัยโดยการป้อน URL ของเว็บไซต์ในช่องที่ระบุ การทดสอบการเจาะระบบพร้อมบอกวิธีแก้ไขช่องโหว่ที่มีอยู่ด้วย ซึ่งมี Module การทำงานอยู่ 3 Module อาทิ 1) Module Web Application 2) Vulnerability Scanners และ 3) Vulnerable Web App ผลลัพธ์ที่ได้ ภาพรายงาน Spider, XSS Scanner ซึ่งมีวิธีการวิจัย ดังนี้ 1) ผู้ใช้เข้าเว็บไซต์ Portal ที่เราได้พัฒนา 2) เข้าสู่ระบบ 3) ทำการค้นหาและตรวจสอบช่องโหว่ของเว็บไซต์ โดยการนำ URL กรอกบนหน้าเว็บ 4) ระบบจะตรวจจับช่องโหว่ ดังนี้ SQLI, XSS และ Spider 5)รายงานช่องโหว่ พร้อมวิธีแก้ไขช่องโหว่เพื่อให้ระบบมีความปลอดภัยมากขึ้น [12]

วิจัยเรื่อง “An Analysis of Vulnerability Scanners in Web Applications for VAPT” เครื่องมือสแกนช่องโหว่ให้ความช่วยเหลือได้ดีมากในการค้นหาช่องโหว่ อย่างไรก็ตาม การเกิดผลบวกลวง การบรรเทาผลกระทบจะวัดคุณภาพของการตรวจจับโดยจำแนกช่องโหว่หนึ่งรายการเป็นสูง ปานกลาง ต่ำ ถือเป็นข้อกังวลอย่างมากในการจัดหาแนวทางแก้ไขช่องโหว่ จะต้องคำนึงถึงการผสมผสานระหว่างการวิเคราะห์แบบอัตโนมัติและแบบแมนนวลด้วย ซึ่งมีวิธีการวิจัยดังนี้ เริ่มการ Penetration testing 1) การทำข้อตกลงกับเจ้าของ Web Application ก่อนทำการทดสอบค้นหาช่องโหว่ (Agreement) 2) วางแผน และล่าตระเวนค้นหาช่องโหว่ (Planning and Reconnaissance) 3) เริ่มการค้นหาช่องโหว่ (Scanning) 4) เข้าถึงระบบเครือข่าย โดย WEP และ ARP (Gaining Access) 5) จัดการเวลาการเข้าถึงให้ได้นานที่สุดและสำรวจข้อมูลที่จำเป็น (Maintains access Attacker) 6) ใช้ประโยชน์ โดยใช้ Burp Suite Metasploit, Wireshark (Exploitation) 7) จัดทำรายงานช่องโหว่เพื่อใช้เป็นหลักฐาน สำหรับการแก้ไขช่องโหว่ (Evidence and Reporting) [13]

บทที่ 3
วิธีดำเนินการวิจัย

วิจัยเรื่อง “การตรวจสอบความมั่นคงปลอดและแนวทางการยกระดับความมั่นคงปลอดภัยของเว็บแอปพลิเคชันของหน่วยงานภาครัฐ” เพื่อศึกษาวิธีการค้นหาช่องโหว่ของเว็บแอปพลิเคชันที่มีความสำคัญกับองค์กรจำนวน 3 ระบบ และการเลือกใช้เครื่องมือ 3 เครื่องมือที่มีความสามารถแตกต่างกันในการค้นหาช่องโหว่ เพื่อให้ครอบคลุมกับช่องโหว่ทั้งหมดที่มีอยู่บนระบบ เมื่อทราบถึงช่องโหว่ที่ตรวจพบจึงดำเนินการประเมินช่องโหว่ พร้อมจัดทำรายงานช่องโหว่ และศึกษาเครื่องมือและแนวทางการยกระดับความมั่นคงปลอดภัยของเว็บแอปพลิเคชัน ซึ่งจากที่กล่าวมามีวิธีดำเนินการวิจัยดังนี้

3.1 กระบวนการดำเนินงาน

3.1.1 การวางแผน (PLAN)

3.1.1.1 ศึกษา วิเคราะห์ และประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร โดยผู้วิจัยประยุกต์ใช้เครื่องมือประเมินตนเอง (Self-Assessment Tools) ที่อยู่บนพื้นฐานของ NIST CSF 2.0 พร้อมสรุปผลคะแนนเป็นร้อยละของทั้ง 6 ด้าน ดังนี้ 1) GOVERN 2) PROTECT 3) IDENTIFY 4) DETECT 5) RESPOND และ 6) RECOVERY จากนั้นหาค่าเฉลี่ย เพื่อให้ได้ผลลัพธ์ความเสี่ยงขององค์กรออกมา ดำเนินการปรับปรุงด้านที่เกณฑ์คะแนนน้อย

3.1.1.2 ศึกษา วิเคราะห์ สถาปัตยกรรมระบบขององค์กร เพื่อคัดเลือก Web Applications ที่มีผลการประเมินความเสี่ยง (Risk Assessment) สูงสุด 3 อันดับ โดยใช้เกณฑ์การพิจารณาความเสี่ยงขององค์กร *[4]* ซึ่งมีรายละเอียดการพิจารณาดังนี้

1) หัวข้อเกณฑ์การพิจารณา

1.1) ความสำคัญ หมายถึง พิจารณาจากความสำคัญของระบบตามกลุ่มงานภารกิจของหน่วยงาน เรียงลำดับตามกฎกระทรวงแบ่งส่วนราชการหน่วยงาน

1.2) ผู้ใช้งาน หมายถึง พิจารณาจากกลุ่มผู้ใช้งาน ซึ่งเป็นผู้มีส่วนได้ส่วนเสีย โดยแบ่งออกเป็น ประชาชนทั่วไป หน่วยงานเฉพาะ เจ้าหน้าที่ของหน่วยงาน เจ้าหน้าที่เฉพาะของหน่วยงาน และผู้บริหาร

1.3) ข้อมูล หมายถึง พิจารณาจากชั้นความลับตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยระบบมีการจัดเก็บและเปิดเผยข้อมูลระดับใด

1.4) ยืนยันตัวตน หมายถึง พิจารณาจากเทคโนโลยีที่ใช้ในการยืนยันตัวตน ก่อนเข้าถึงและใช้งานระบบ

1.5) ช่องทาง หมายถึง พิจารณาจากช่องทางการเข้าถึงระบบ

1.6) โอกาส หมายถึง พิจารณาจากสถิติภัยคุกคามทางด้านไซเบอร์ (Cyber Attack Trends) ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อให้ได้ข้อมูลทิศทางการโดนโจมตีของประเทศไทย

2) เกณฑ์การให้คะแนนความเสี่ยง

2.1) 5 คะแนน หมายถึง มากที่สุด

2.2) 4 คะแนน หมายถึง มาก

2.3) 3 คะแนน หมายถึง ปานกลาง

2.4) 2 คะแนน หมายถึง น้อย

2.5) 1 คะแนน หมายถึง น้อยที่สุด

3.1.1.3 ศึกษาเครื่องมือตรวจสอบความมั่นคงปลอดภัยของ Web Applications (VA SCAN) บนเว็บไซต์ OWASP โดยกำหนดเกณฑ์การคัดเลือกเครื่องมือ VA SCAN ด้วยคิดทฤษฎี 2CEPT Algorithm ซึ่งประยุกต์จากทฤษฎี 7Rs

3.1.1.4 ศึกษา กำหนดแผน และมาตรฐานวิธีกาตรวจสอบระบบ โดยใช้ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ *[14]*

3.1.1.5 ศึกษาแนวทางการยกระดับความมั่นคงปลอดภัยของ Web Applications ตามมาตรฐานสากล ดังนี้ 1) CWE 2) OWASP และ 3) ISO

3.1.1.6 ศึกษา วิเคราะห์ กฎ ระเบียบ ข้อบังคับ นโยบาย มาตรฐาน และแนวปฏิบัติ ในระดับสากลและระดับประเทศ

3.1.2 ดำเนินการ (DO)

3.1.2.1 ผู้วิจัยดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร โดยประยุกต์ใช้เครื่องมือประเมินตนเอง (Self Assessment Tools) ที่อยู่บนพื้นฐานของ NIST CSF 2.0 พร้อมสรุปผลคะแนนเป็นร้อยละของแต่ละด้าน พร้อมทั้งหาค่าเฉลี่ย เพื่อวิเคราะห์ผลลัพธ์ความเสี่ยงขององค์กร

3.1.2.2 ดำเนินการคัดเลือก Web Applications นำร่อง 3 ระบบด้วยเกณฑ์ประเมินความเสี่ยง (Risk Criteria)

3.1.2.3 ดำเนินการคัดเลือก VA Tools ที่เหมาะสม 3 เครื่องมือ ด้วย 2CEPT Algorithm

3.1.2.4 ดำเนินการตรวจสอบ Web Applications จำนวน 3 ระบบ ด้วย VA SCAN 3 เครื่องมือ พร้อมรวบรวมผลลัพธ์

3.1.2.5 ดำเนินการคัดเลือก VA Tools ที่มีประสิทธิภาพสูงสุด 1 เครื่องมือ และนำผลลัพธ์การตรวจสอบของเครื่องมือดังกล่าว มากำหนดแนวทางการแก้ไขช่องโหว่

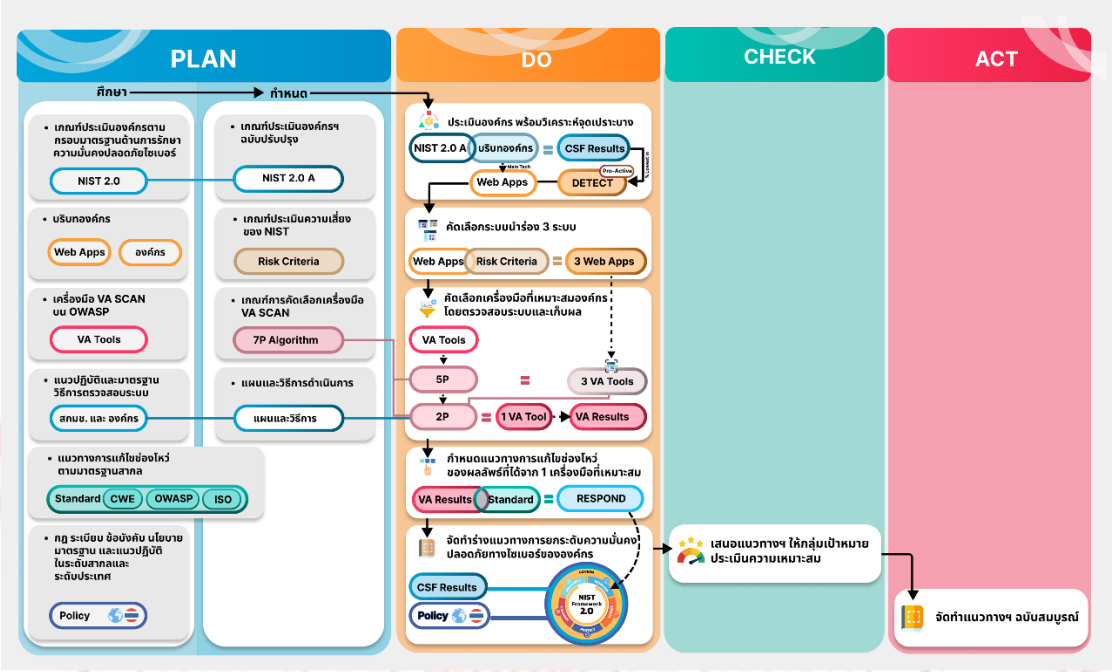
3.1.2.6 จัดทำร่างแนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร โดยการนำผลการวิเคราะห์จุดเปราะบาง มาเสนอแนวทางเพิ่มประสิทธิภาพนโยบาย

3.1.3 การตรวจสอบ (CHECK)

ดำเนินการเสนอแนวทางการยกระดับความมั่นคงปลอดภัยขององค์กร ให้กลุ่มเป้าหมาย (ผู้บริหารระดับ ส่วน /ศูนย์ และผู้ปฏิบัติงาน) พิจารณา โดยการประเมินความเหมาะสม

3.1.4 การปรับปรุง (ACTION)

ปรับปรุงแนวทางฯ ให้สมบูรณ์ตามข้อพิจารณาและข้อเสนอแนะของกลุ่มเป้าหมาย



ภาพที่ 3-1 กระบวนการดำเนินงาน (Paradigm)

3.2 การวางแผน (PLAN)

3.2.1 ศึกษา วิเคราะห์ และประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร โดยผู้วิจัยประยุกต์ใช้เครื่องมือประเมินตนเอง (Self-Assessment Tools) ที่อยู่บนพื้นฐานของ NIST CSF 2.0 พร้อมสรุปผลคะแนนเป็นร้อยละของทั้ง 6 ด้าน ดังนี้ 1) GOVERN 2) PROTECT 3) IDENTIFY 4) DETECT 5) RESPOND และ 6) RECOVERY จากนั้นหาค่าเฉลี่ย เพื่อให้ได้ผลลัพธ์ความเสี่ยงขององค์กรออกมา ดำเนินการปรับปรุงด้านที่เกณฑ์คะแนนน้อย

3.2.2 ศึกษา วิเคราะห์ สถาปัตยกรรมระบบขององค์กร เพื่อคัดเลือก Web App โดยมีเกณฑ์ประเมินความเสี่ยง (Risk Criteria) ซึ่งได้รับอนุมัติจากหัวหน้าหน่วยงานภาครัฐของผู้วิจัยแล้ว รายละเอียดดังตารางที่ 3-1 เพื่อคัดเลือก Web App ที่มีผลการประเมินความเสี่ยง (Risk Assessment) สูงสุด 3 อันดับ

ตารางที่ 3-1 Risk Criteria เกณฑ์การพิจารณา

ที่	ชื่อด้าน	เกณฑ์การพิจารณา	คะแนนความเสี่ยง (คะแนนมากมีความเสี่ยงมาก)				
			5	4	3	2	1
1	**ความสำคัญ**	พิจารณาจากความสำคัญของระบบตามกลุ่มงานภารกิจของหน่วยงาน เรียงลำดับ**ตามกฎกระทรวงแบ่งส่วนราชการหน่วยงาน**	ระบบสารสนเทศ **เพื่องานกำกับและตรวจสอบ**	ระบบสารสนเทศ เพื่อ**งานสืบสวนและจัดทำคดี**	ระบบสารสนเทศ เพื่อ**งานบริหารทรัพย์สิน**	ระบบสารสนเทศ **เพื่องานสื่อสารและประชาสัมพันธ์**	ระบบสารสนเทศ เพื่อ**งานสนับสนุนอื่นๆ**
2	**ผู้ใช้งาน**	พิจารณาจาก**กลุ่มผู้ใช้งาน** ซึ่งเป็น**ผู้มีส่วนได้ส่วนเสีย** โดยแบ่งออกเป็น **ประชาชนทั่วไป หน่วยงานเฉพาะ เจ้าหน้าที่ของหน่วยงาน เจ้าหน้าที่เฉพาะของหน่วยงาน** และ**ผู้บริหาร**	ครบ**ทุกกลุ่ม**	**หน่วยงาน**/องค์กร เฉพาะ หรือ **ประชาชน**	**ภายใน**หน่วยงาน **และผู้บริหาร**	**ระหว่างกอง**/ศูนย์ /กลุ่ม	**ภายในกอง**/ศูนย์ /กลุ่ม
3	**ข้อมูล**	พิจารณาจาก**ชั้นความลับตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540** และ**พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562** โดยระบบมีการจัดเก็บและเปิดเผยข้อมูลระดับใด	ข้อมูลลับ หากรั่วไหลจะทำให้เกิดความ **เสียหาย**ต่อความมั่นคงและผลประโยชน์แห่งรัฐอย่าง**ร้ายแรงที่สุด**	ข้อมูลลับ หากรั่วไหลจะทำให้เกิดความ **เสียหายต่อองค์กร**ที่ติดต่อกับหน่วยงาน	ข้อมูลลับและข้อมูลส่วนบุคคล หากรั่วไหลจะทำให้เกิด **ความเสียหายต่อประชาชน**ที่ติดต่อกับหน่วยงาน	ข้อมูลที่ต้องได้รับอนุญาตก่อนเข้าถึง หากรั่วไหล **จะส่งผลกระทบต่อรูปคดี** หรือเสียหายต่อระบบ	**ข้อมูลเปิด (Open Data)** และข้อมูลเผยแพร่ประชาสัมพันธ์
4	**ยืนยันตัวตน**	พิจารณาจาก**เทคโนโลยีที่ใช้ในการยืนยันตัวตน** ก่อนเข้าถึงและใช้งานระบบ	**ไม่มี**การยืนยันตัวตน	มีการ**ยืนยัน**ตัวตน **ผ่านหน้าระบบ**	มีการ**ยืนยันตัวตน ผ่านระบบของ องค์กร**	มีการ**ยืนยันตัวตน ผ่านระบบ**ของ **องค์กร** และ/หรือ **ระบบมาตรฐานของประเทศ**	มีการ**ยืนยันตัวตน** แบบ 2 ขั้นตอน **(2FA)** / ไม่จำเป็นต้องมีการยืนยันตัวตน
5	**ช่องทาง**	พิจารณาจาก**ช่องทางการเข้าถึงระบบ**	เข้าถึง**ได้ทุกอุปกรณ์** และ**มี Native Mobile Application**	เข้าถึงได้ทุกอุปกรณ์ ด้วย **Public Internet**	เข้าถึงได้ทุกอุปกรณ์ **ผ่าน VPN**	เข้าถึงได้เฉพาะอุปกรณ์ที่ลงทะเบียน **ผ่าน VPN**	เข้าถึงผ่าน **อุปกรณ์ที่ลงทะเบียน** และอยู่**ภายในวง Lan** ขององค์กร
6	**โอกาส**	**พิจารณาจากสถิติภัยคุกคามทางด้านไซเบอร์** (Cyber Attack Trends) ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ **(สกมช.) เพื่อให้ได้ข้อมูลทิศทางการโดนโจมตีของประเทศไทย**	มากกว่า 10 ครั้ง/ปี	8 - 10 ครั้ง/ปี	5 - 7 ครั้ง/ปี	1 - 4 ครั้ง / ปี	ไม่มี/ไม่พบการโจมตี

3.2.3 ศึกษาเครื่องมือตรวจสอบความมั่นคงปลอดภัยของ Web Applications (VA SCAN) บนเว็บไซต์ OWASP โดยกำหนดเกณฑ์การคัดเลือกเครื่องมือ VA SCAN ด้วยคิดทฤษฎี 2CEPT Algorithm ซึ่งประยุกต์จากทฤษฎี 7Rs

3.2.3.1 การศึกษาเครื่องมือ เพื่อคัดเลือกเครื่องมือตรวจสอบความมั่นคงปลอดภัยของเว็บแอปพลิเคชัน (Vulnerability Assessment Tools VA Scan) ต้องเริ่มจากการศึกษาเครื่องมือจากเว็บไซต์ต่างๆ ที่มีความน่าเชื่อถือ เพื่อประสิทธิภาพในการตรวจสอบเว็บแอปพลิเคชันองค์กร อีกทั้งยังมั่นใจได้ว่าเมื่อทำการตรวจสอบด้วยเครื่องมือที่คัดเลือกมานั้น เว็บแอปพลิเคชันขององค์กรจะไม่หยุดทำงาน ข้อมูลไม่สูญหาย ไม่รั่วไหล และช่องโหว่ขององค์กรจะไม่ถูกเผยแพร่ออกไปภายนอกองค์กร ดังนั้น ผู้ตรวจสอบจึงศึกษาเครื่องมือจากเว็บไซต์ที่มีความน่าเชื่อถือ อย่าง Open Web Application Security Project (Foundation, The OWASP®, 2567)

3.2.3.2 การกำหนดเกณฑ์สำหรับคัดเลือเครื่องมือมีความสำคัญอย่างมาก ซึ่งจำเป็นต้องศึกษาบริบทองค์กร แนวปฏิบัติและมาตรฐานวิธีการตรวจสอบระบบขององค์กร และสถาปัตยกรรมระบบองค์กร ร่วมด้วย เพื่อให้ได้เกณฑ์การคัดเลือกที่มีประสิทธิภาพ ส่งผลให้ได้เครื่องมือที่เหมาะสมกับองค์กร ในการนี้ผู้วิจัยได้คิดค้น Algorithm ขึ้นมาใหม่ โดยอ้างอิงจาก ทฤษฎี 7R Logistics (CILT) เพื่อใช้สำหรับการคัดเลือกเครื่องมือที่เหมาะสมกับองค์กรโดยใช้ชื่อว่า 7P Algorithm มีรายละเอียด 7P ดังนี้

1) Price เครื่องมือเป็นแบบ Open Source หรือ Free License

2) Privacy เครื่องมือมีข้อตกลงการไม่ส่งข้อมูลการตรวจสอบเกี่ยวกับข้อมูลของ Web App องค์กรกลับไปยังผู้พัฒนา

3) Passive เครื่องมือมีความสามารถตราวจสอบช่องโหว่ด้วยตนเอง โดยไม่มีการ Integration ผลลัพธ์จากเครื่องมืออื่น

4) Place เครื่องมือสามารถทำงานได้บน On-Premise และไม่ต้องเข้าถึงโค๊ด (Code) ของ Web App

5) Popular เครื่องมือมีความนิยม และมีชุมชนแลกเปลี่ยนข้อมูล (Community) ขนาดใหญ่ที่มีความน่าเชื่อถือ

6) Present เครื่องมือมีการพัฒนา (Develop) เทคนิคการตรวจสอบ Web App อย่างต่อเนื่องจนถึงปัจจุบัน

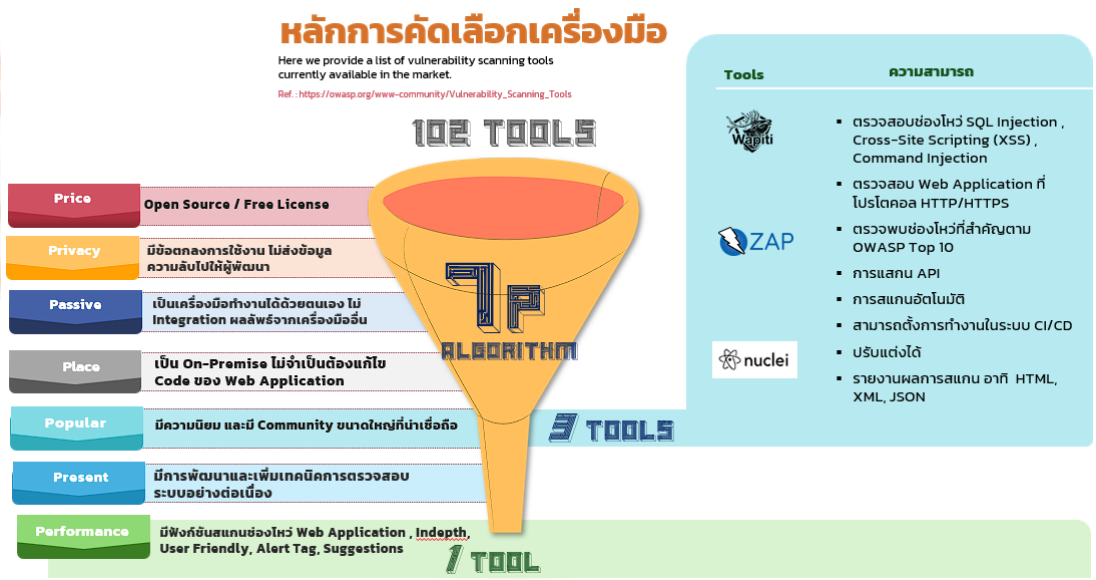
7) Performance เครื่องมือมีประสิทธิภาพในการตรวจสอบ Web App มีเกณฑ์ ดังนี้

7.1) In depth เครื่องมือมีประสิทธิภาพสามารถตรวจสอบช่องโหว่ได้ละเอียดและครอบคลุม

7.2) User Friendly เครื่องมือใช้งานง่าย ไม่ซับซ้อน สามารถเรียนรู้ได้อย่างรวดเร็วโดยไม่ต้องมีองค์ความรู้เฉพาะด้าน

7.3) Alert Tag มีการแจ้งเตือนช่องโหว่พร้อมกับระบุความสอดคล้องกับมาตรฐานสากล อาทิ OWASP Top 10, CWE

7.4) Suggestions มีคำแนะนำในการแก้ไขช่องโหว่ พร้อมแหล่งอ้างอิงให้ไปสืบค้นข้อมูลเพิ่มเติม



ภาพที่ 3-2 หลักการคัดเลือกเครื่องมือ

3.2.4 ศึกษา กำหนดวิธีดำเนินการตรวจสอบ โดยใช้ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ [14]

การดำเนินการตรวจสอบระบบเทคโนโลยีสารสนเทศของหน่วยงานภาครัฐ มีความสำคัญอย่างมาก เนื่องจากในระบบมีการเก็บข้อมูลที่หลากหลาย อาทิ ข้อมูลลับที่สุด ลับมาก ลับ และข้อมูลที่สามารถเปิดเผยได้ หากข้อมูลที่มีชั้นความลับรั่วไหลจะทำให้เกิดความเสียหายต่อความมั่นคงและผลประโยชน์ขององค์กร และผู้มีส่วนได้ส่วนเสีย รวมถึงประเทศได้ ผู้วิจัยจึงกำหนดวิธีดำเนินการตรวจสอบและ***รูปแบบการประยุกต์ใช้เครื่องมือตรวจสอบระบบ*** รายละเอียดดังตารางที่ 3-2 และ 3-3 ตามลำดับ

สัญลักษณ์ ผู้รับผิดชอบ

- ○ ผู้ตรวจสอบ คณะกรรมการตรวจสอบ หน่วยตรวจสอบภายใน
- ◔ หน่วยงานทางด้านสารสนเทศ ผู้ถูกตรวจสอบ
- ● ผู้บริหาร พนักงาน เจ้าหน้าที่ ผู้ที่ใช้งานระบบเครือข่ายและระบบสารสนเทศขององค์กร

ตารางที่ 3-2 วิธีดำเนินการตรวจสอบ

วิธีการ	ผู้รับผิดชอบ		
ศึกษาเกณฑ์ประเมินองค์กรตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และกำหนดเกณฑ์ประเมินองค์กรปีละ 1 ครั้ง	○		
ศึกษามาตรฐานเวอร์ชันที่มีความทันสมัย อาทิ NIST CSF เป็นต้น			
กำหนดเกณฑ์ประเมินองค์กร เพื่อปรับปรุงเกณฑ์ของแต่ละปี เพื่อผลการประเมินองค์กรมีความสอดคล้องกับภัยคุกคามในปัจจุบัน			
เลือกวิธีการประยุกต์ใช้เครื่องมือตรวจสอบระบบให้มีความปลอดภัยกับองค์กร ตามข้อ 2. และประสานผู้เกี่ยวข้องเตรียมความพร้อมทางด้านเทคนิค	○	◔	
ศึกษา และกำหนดเครื่องมือที่มีความน่าเชื่อถือ ปลอดภัย ทันสมัย โดยใช้ทฤษฎี 2CEPT ALGORITHM เพื่อให้เหมาะสมกับองค์กร ความน่าเชื่อถือสามารถดูจาก Rating และ Community ของเครื่องมือ ในส่วนของความทันสมัยสามารถดูจากความต่อเนื่องของการอัปเดตเวอร์ชัน การปรับปรุงเครื่องมือ การแก้ไขข้อผิดพลาดของเครื่องมือ	○		
ประเมิน จัดเรียง และคัดเลือกระบบตามเกณฑ์การประเมินความเสี่ยง (Risk Assessment) ระบบเทคโนโลยีสารสนเทศขององค์กร การประเมิน ควรประเมิน 1 ครั้ง/ปี และ/หรือทุกครั้งที่มีการเปลี่ยนแปลงองค์กรแบบมีนัยสำคัญ ซึ่งกระทบต่อระบบ	○		
รายงานระบบที่มีผลประเมินความเสี่ยงสูงกับส่วนผู้รับผิดชอบดูแลระบบ และผู้บริหารเพื่อพิจารณาคัดเลือกระบบสำหรับการตรวจสอบ	○	◔	●
เลือกช่วงเวลาในการตรวจสอบระบบให้เหมาะสม การเลือกเวลาที่เหมาะสมในการตรวจสอบระบบมีความสำคัญ เพื่อให้ได้ผลลัพธ์ที่มีประสิทธิภาพ และเพื่อหลีกเลี่ยงผลกระทบต่อผู้ใช้งานระบบ อาทิ ระบบจะมีการทำงานล่าช้า เป็นต้น ควรเป็นช่วงที่ระบบ มีการใช้งานน้อย หรือไม่มีการใช้งาน	○	◔	
ดำเนินการตรวจสอบระบบด้วยเครื่องมือ และวิธีการ ตามข้อ 1.2	○		

ตารางที่ 3-3 (ต่อ) วิธีดำเนินการตรวจสอบ

วิธีการ	ผู้รับผิดชอบ		
เปรียบเทียบช่องโหว่ที่พบกับระดับความรุนแรงของช่องโหว่ตามมาตรฐานสากล และเสนอแนวทางการแก้ไขช่องโหว่ และยกระดับความมั่นคงปลอดภัยทางไซเบอร์ตามมาตรฐานสากล	○		
ระดับความเสี่ยง (Risk Level) ช่องโหว่ เปรียบเทียบกับมาตรฐาน OWASP Top 10			
การยอมรับความเสี่ยง (Risk Tolerance Description) ให้อ้างอิงแนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ขององค์กร เพื่อใช้เสนอแนะความเร่งด่วนในการแก้ไขช่องโหว่ดังกล่าว			
จัดทำข้อเสนอแนวทางการแก้ไขช่องโหว่ และยกระดับความมั่นคงปลอดภัยทางไซเบอร์อ้างอิงตามมาตรฐานสากล โดยแนวทางการยกระดับต้องเป็นแนวทางแก้ไขที่สอดคล้องกับระบบองค์กร			
จัดทำ/ปรับปรุงแนวทางแก้ไขช่องโหว่และแนวทางการยกระดับความมั่นคงปลอดภัยไซเบอร์ขององค์กร	○		
เสนอแนวทางแก้ไขช่องโหว่และแนวทางการยกระดับความมั่นคงปลอดภัยไซเบอร์ขององค์กรให้กับผู้มีส่วนเกี่ยวข้อง	○	●	●
ผู้บริหารพิจารณา อนุมัติ/ไม่อนุมัติ/ปรับปรุง แนวทางแก้ไขช่องโหว่และแนวทางฯ			
ผู้ดูแลระบบดำเนินการแก้ไขตามแนวทางแก้ไขช่องโหว่และแนวทางฯ			
ติดตาม ประเมิน และสรุปผลตามแนวทางการยกระดับความมั่นคงปลอดภัยไซเบอร์	○		

ตารางที่ 3-4 รูปแบบการประยุกต์ใช้เครื่องมือตรวจสอบระบบ

ที่	ประเภทข้อมูล	ประเภทเครื่องมือ	วิธีการที่แนะนำ
1	ข้อมูลเปิด (Open Data) และข้อมูลเผยแพร่ประชาสัมพันธ์	Dynamic Analysis Tools	ดำเนินการตรวจสอบโดยไม่ต้องใช้ Virtual Machine
2	ข้อมูลที่ต้องได้รับอนุญาตก่อนเข้าถึง หากรั่วไหลจะส่งผลกระทบต่อรูปคดี หรือเสียหายต่อระบบ		ดำเนินการดังนี้ 1. ใช้เครื่องมือตรวจสอบระบบ (VA SCAN) แบบ Offline 2. สร้าง Virtual Machine สำหรับตรวจสอบระบบ แบบ Internal และ External
3	ข้อมูลับและข้อมูลส่วนบุคคล หากรั่วไหลจะทำให้เกิดความเสียหายต่อประชาชน องค์กร ที่ติดต่อกับองค์กร และเสียหายต่อความมั่นคงและผลประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด		
4	ข้อมูลทุกประเภท	Static Analysis Tools	ดำเนินการดังนี้ 1. สร้าง Virtual Machine สำหรับตรวจสอบระบบ 2. Clone ระบบเป้าหมาย 3. ติดตั้งคำสั่งในโค๊ดของระบบเพื่อการตรวจสอบ

หมายเหตุ รูปแบบที่ 2 และ 3 เมื่อการตรวจสอบระบบเสร็จสิ้นให้ดำเนินการลบ VM ในทันที

3.2.5 ศึกษาแนวทางการยกระดับความมั่นคงปลอดภัยของ Web Applications ตามมาตรฐานสากล

3.2.5.1 CWE *[15]* (Common Weakness Enumeration) เป็นรายการมาตรฐานที่จัดหมวดหมู่จุดอ่อนด้านความมั่นคงปลอดภัยของซอฟต์แวร์และฮาร์ดแวร์ ซึ่งช่วยให้นักพัฒนาและผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสามารถระบุและแก้ไขช่องโหว่ได้อย่างมีประสิทธิภาพ โดย CWE มักใช้เป็นแนวทางในการตรวจสอบโค้ดและประเมินความเสี่ยงของช่องโหว่ที่อาจถูกโจมตี (ภาคผนวก ก)

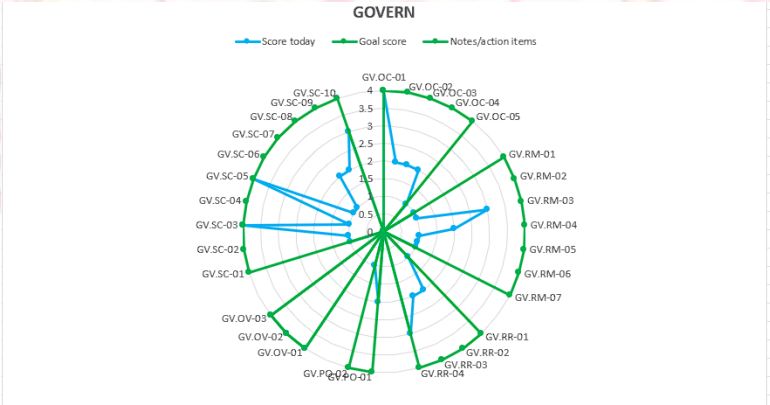
3.2.5.2 แนวทางปฏิบัติที่ช่วยให้นักพัฒนาและองค์กรสามารถป้องกันภัยคุกคามทางไซเบอร์ได้ หนึ่งในโครงการที่เป็นที่รู้จักมากที่สุดคือ OWASP Top Ten ซึ่งเป็นรายการช่องโหว่ด้านความมั่นคงปลอดภัยของ Web Application ที่พบบ่อยและมีความรุนแรงสูง เช่น Injection, Broken Authentication และ Security Misconfiguration *[2]* (ภาคผนวก ก)

3.2.5.3 ISO ในงานวิจัยนั้นมุ่งเน้นที่ ISO 27001 มาตรฐานสากลด้านการจัดการความมั่นคงปลอดภัยของข้อมูล (Information Security Management System – ISMS) ซึ่งกำหนดแนวทางในการบริหารความเสี่ยงและปกป้องข้อมูลขององค์กร โดยมุ่งเน้นการระบุ วิเคราะห์ และลดความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูลให้มีประสิทธิภาพ มาตรฐานนี้ช่วยให้องค์กรสามารถจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ได้

3.2.6 ศึกษา วิเคราะห์ กฎ ระเบียบ ข้อบังคับ นโยบาย มาตรฐาน และแนวปฏิบัติ ในระดับสากลและระดับประเทศ

3.3 ดำเนินการ (DO)

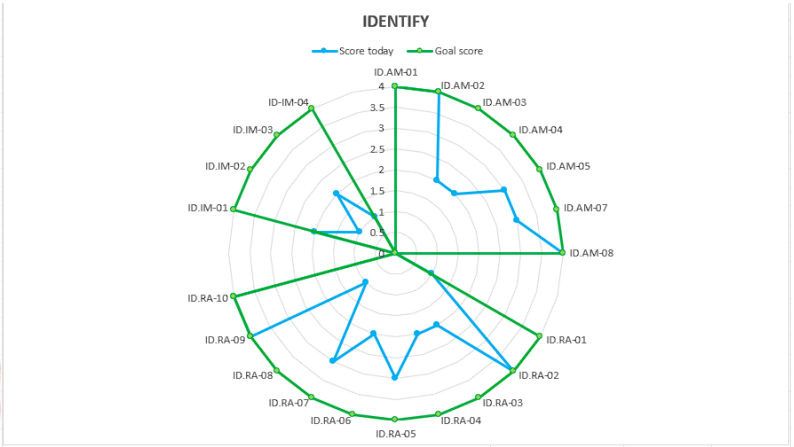
3.3.1 ผู้วิจัยดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร โดยประยุกต์ใช้เครื่องมือประเมินตนเอง (Self Assessment Tools) ที่อยู่บนพื้นฐานของ NIST CSF 2.0 พร้อมสรุปผลคะแนนเป็นร้อยละของแต่ละด้าน พร้อมทั้งหาค่าเฉลี่ย เพื่อวิเคราะห์ผลลัพธ์ความเสี่ยงขององค์กร ซึ่งดำเนินการประเมินทั้งหมด 6 ด้านรายละเอียดดังภาพ



Govern: Functional Area summary (note: this table will update automatically based on the scores you enter on rows 36 to 71 below)

Category	Name	Score today	Goal score
Organizational Context (GV.OC)	Org Context	2.2	4
Risk Management Strategy (GV.RM)	Risk Mgmt Strategy	1.42857143	4
Roles, Responsibilities, and Authorities (GV.RR)	Roles, Resp, Auth	2	4
Policy (GV.PO)	Policy	1.5	4
Oversight (GV.OV)	Oversight	4	4
Cybersecurity Supply Chain Risk Management (GV.SC)	Supply Chain Risk	2	4

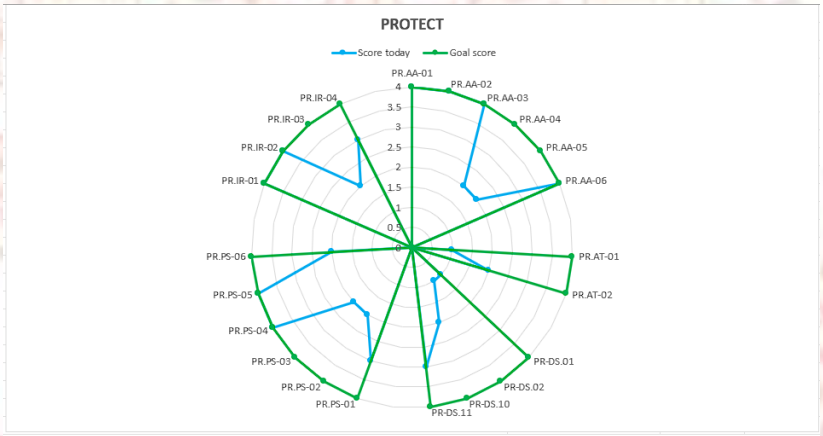
ภาพที่ 3-3 Self Assessment Tools ด้าน GOVERN



Identify: Functional Area summary (note: this table will update automatically based on the scores you enter on rows 34 to 56 below)

Category	Name	Score today	Goal score
Asset Management (ID.AM)	Asset Mgmt	3.14285714	4
Risk Assessment (ID.RA)	Risk Assessment	2.6	4
Improvement (ID.IM)	Improvement	1.5	4
		7.24285714	12

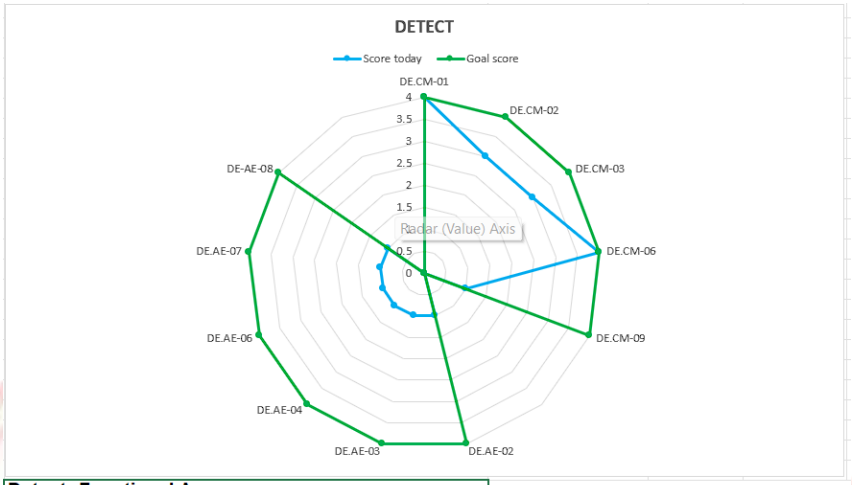
ภาพที่ 3-4 Self Assessment Tools ด้าน IDENTIFY



Protect: Functional Area summary (note: this table will update automatically based on the scores you enter on rows 36 to 61 be

Category	Name	Score today	Goal score
Identity Management, Authentication, and Access Control (PR.AA)	Identity Mgt	3.33333333	4
Awareness and Training (PR.AT)	Awareness and Training	1.5	4
Data Security (PR.DS)	Data Security	1.75	4
Platform Security (PR.PS)	Platform Security	2.83333333	4
Technology Infrastructure Resilience (PR.IR)	Tech Infra Res	3.25	4

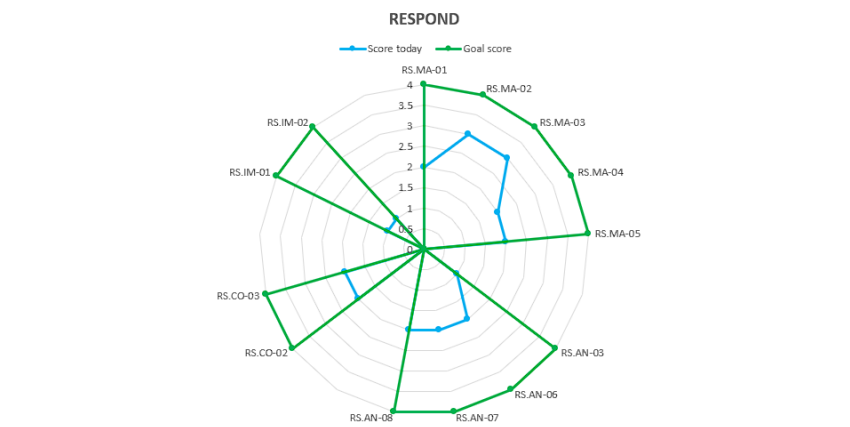
ภาพที่ 3-5 Self Assessment Tools ด้าน PROTECT



Detect: Functional Area summary (note: this table will update automatically based on the scores you enter on rows 33 to 44 below)

Category	Name	Score today	Goal score
Continuous Monitoring (DE.CM)	Continuous Monitoring	3	4
Adverse Event Analysis (DE.AE)	Adv Event Analysis	1	4

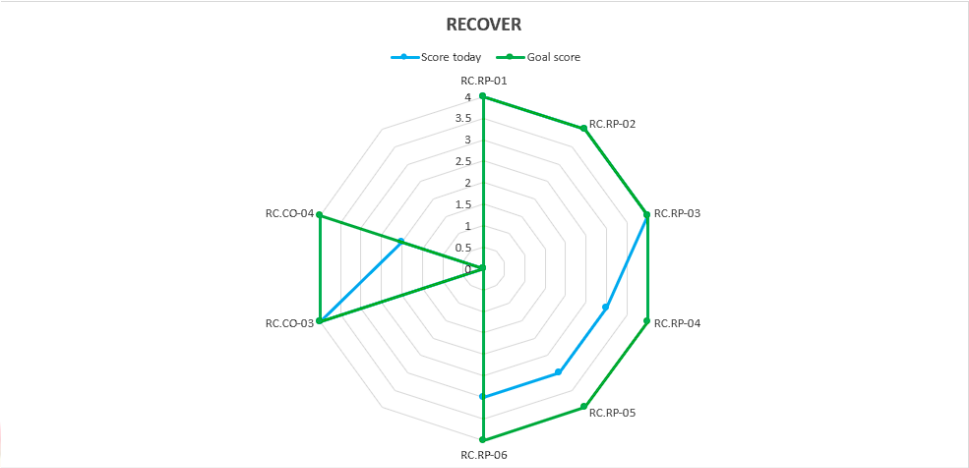
ภาพที่ 3-6 Self Assessment Tools ด้าน DETECT



Respond: Functional Area summary (note: this table will update automatically based on the scores you enter on rows 35 to 50 below)

Category	Name	Score today	Goal score
Incident Management (RS.MA)	Incident Management	2.4	4
Incident Analysis (RS.AN)	Incident Analysis	1.75	4
Incident Response Reporting and Communication (RS.CO)	Reporting and Comms	2	4
Incident Mitigation (RS.MI)	Incident Mitigation	1	4

ภาพที่ 3-7 Self Assessment Tools ด้าน RESPOND



Recover: Functional Area summary (note: this table will update automatically based on the scores you enter on rows 32 to 40 below

Category	Name	Score today	Goal score
Incident Recovery Plan Execution (RC.RP)	Incident Recovery Plan	3.5	4
Incident Recovery Communication (RC.CO)	Incident Recovery Comms	3	4

ภาพที่ 3-8 Self Assessment Tools ด้าน RESPOND

3.3.2 ดำเนินการคัดเลือก Web Applications นำร่อง 3 ระบบด้วยเกณฑ์ประเมินความเสี่ยง (Risk Criteria)

3.3.3 ดำเนินการคัดเลือก VA Tools ที่เหมาะสม 3 เครื่องมือ ด้วย 2CEPT Algorithm

การคัดเลือกเครื่องมือตรวจสอบเว็บแอปพลิเคชัน ดำเนินการโดยนำ VA Scan ที่ได้จากการศึกษาจากเว็บไซต์ที่มีความน่าเชื่อถือ ซึ่งได้รายชื่อ VA Scan จำนวน 102 เครื่องมือ นำมาคัดเลือกโดยศึกษาจากข้อมูลจะเข้าตามเกณฑ์การคัดเลือกเครื่องมือจนถึง 1P ถึง 5P ส่งผลให้ได้ VA Scan 3 เครื่องมือ ดังนี้ 1) Wapiti 2) ZAP และ 3) Nuclei ในส่วนของ 6P และ 7P ต้องดำเนินการใช้เครื่องมือตรวจสอบระบบขององค์กรเพื่อจะช่วยให้คัดเลือกเครื่องมือให้เหลือ 1 เครื่องมือที่เหมาะสมกับองค์กรที่สุด โดยมีรายละเอียดดังนี้

3.3.4 ดำเนินการตรวจสอบ Web Applications จำนวน 3 ระบบ ด้วย VA SCAN 3 เครื่องมือ พร้อมรวบรวมผลลัพธ์

3.3.4.1 ดำเนินการตรวจสอบเว็บแอปพลิเคชัน 3 ระบบนำร่อง ช่วงเวลาหลัง 16.30 น. ดังนี้

1) Web App A ให้บริการผู้มีส่วนได้เสียทุกกลุ่ม หน่วยงาน ประชาชน พนักงานองค์กร ด้านการประชาสัมพันธ์ข้อมูล

2) Web App B ให้บริการประชาชน หรือผู้ที่ได้รับความเสียหาย ด้านการยื่นข้อมูลตามแบบฟอร์ม เพื่อรับบริการจากองค์กร

3) Web App C ให้บริการประชาชน ด้านการยื่นข้อมูลเพื่อสมัครเป็นพนักงานองค์กร

3.3.4.2 เครื่องมือที่ใช้ตรวจสอบระบบ 3 เครื่องมือ ดังนี้

1) Wapiti เวอร์ชัน 3.2.2

2) Nuclei เวอร์ชัน 3.3.7

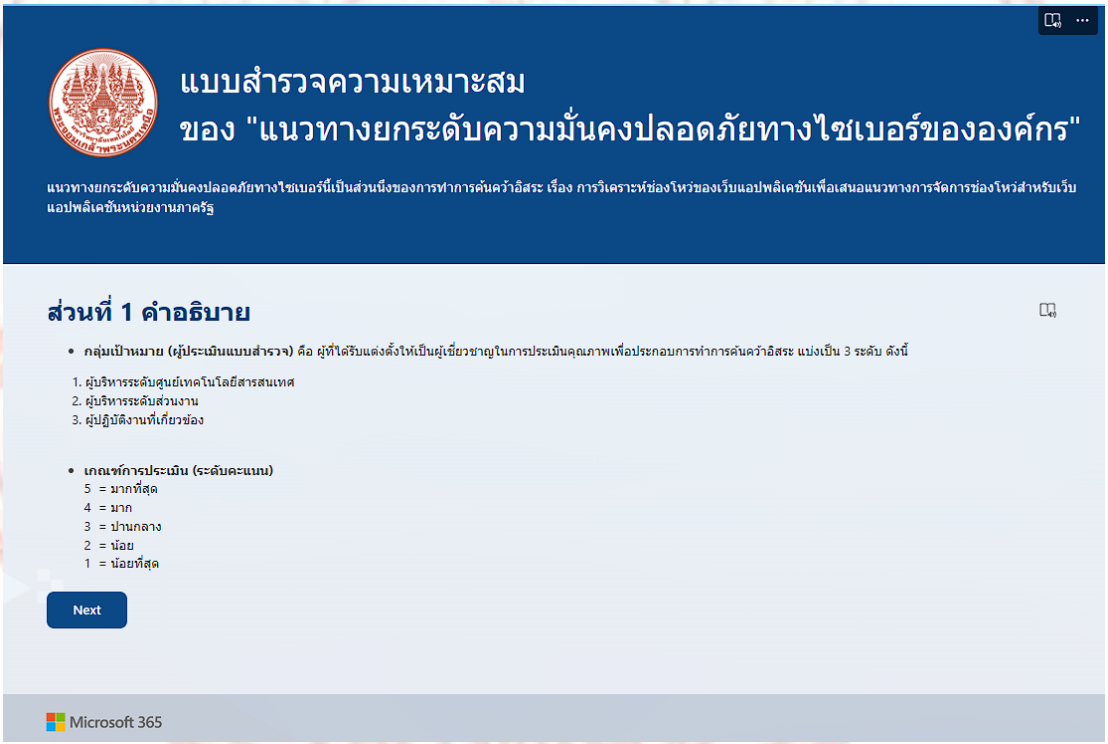
3) Zap เวอร์ชัน 2.15.0

3.3.5 ดำเนินการคัดเลือก VA Tools ที่มีประสิทธิภาพสูงสุด 1 เครื่องมือ และนำผลลัพธ์การตรวจสอบของเครื่องมือดังกล่าว มากำหนดแนวทางการแก้ไขช่องโหว่ ในส่วนของขั้นตอนนี้อ้างอิงจากเกณฑ์การคัดเลือกเครื่องมือ 7P Algorithm ใน P6 และ P7 จะได้เครื่องมือที่เหมาะสมกับองค์กร คือ Zap

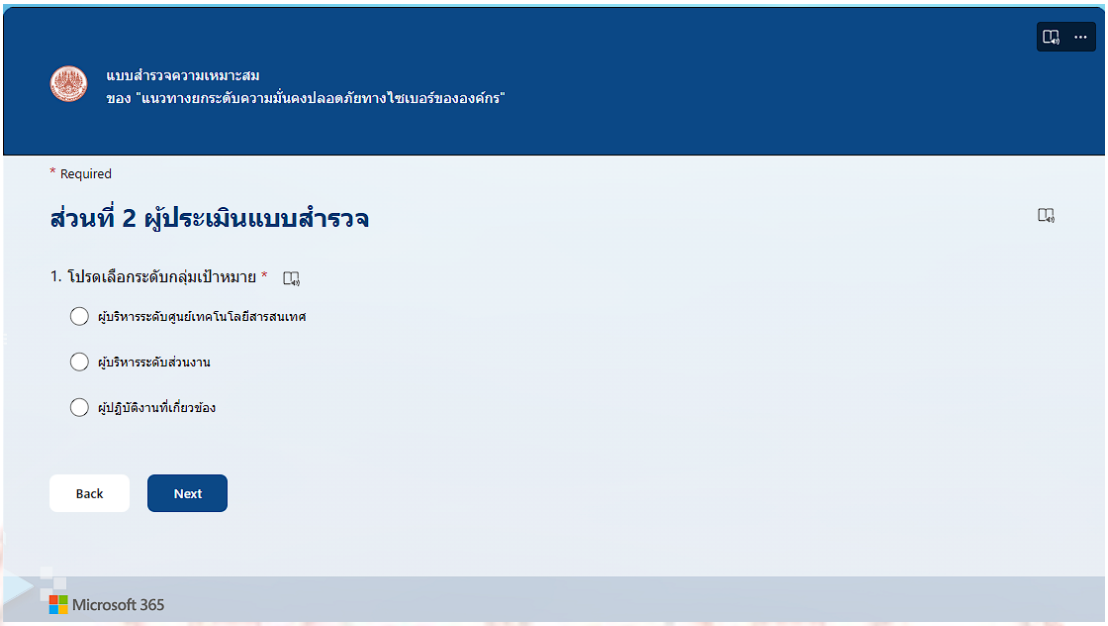
3.3.6 จัดทำร่างแนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร โดยการนำผลการวิเคราะห์จุดเปราะบาง มาเสนอแนวทางเพิ่มประสิทธิภาพนโยบาย

3.4 การตรวจสอบ (CHECK)

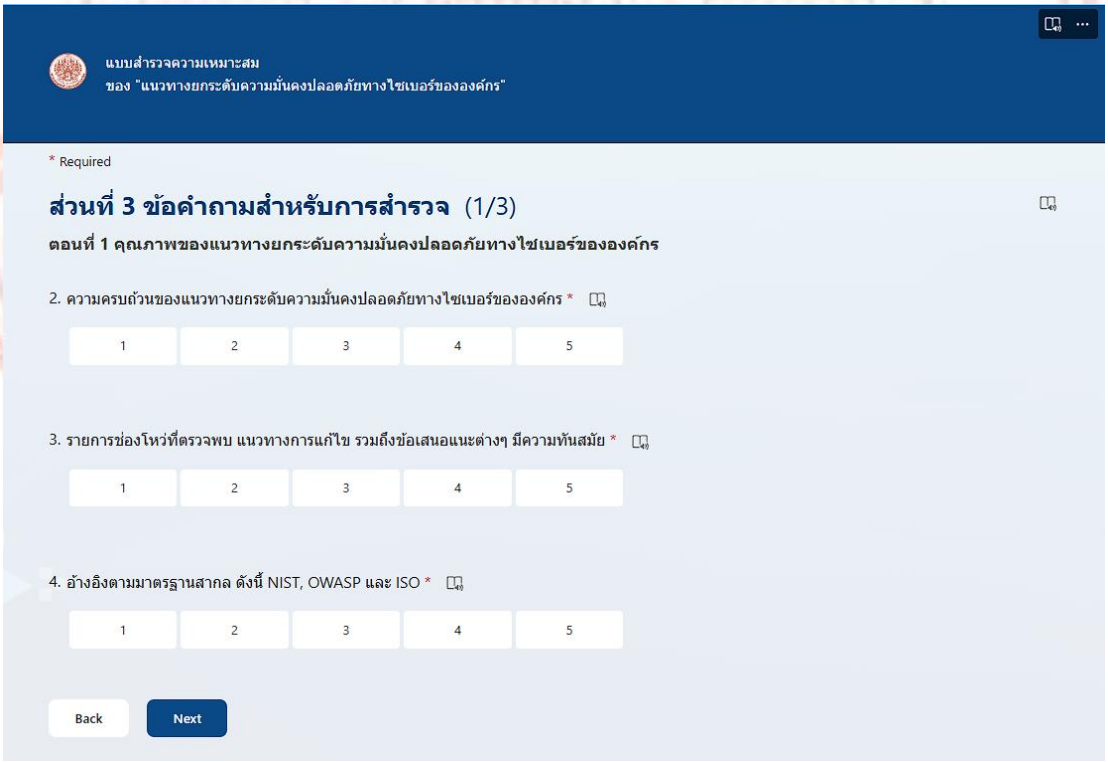
3.4.1 ดำเนินการเสนอแนวทางการยกระดับความมั่นคงปลอดภัยขององค์กร ให้กลุ่มเป้าหมายพิจารณา ซึ่งผู้วิจัยได้แต่งตั้งผู้เชี่ยวชาญ 3 ท่าน โดยแบ่งเป็น 3 ระดับ ดังนี้ ผู้บริหารระดับศูนย์เทคโนโลยีสารสนเทศ ผู้บริหารระดับส่วนงาน และผู้ปฏิบัติงาน เพื่อพิจารณาแนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร ในขั้นตอนนี้ผู้วิจัยได้จัดทำแบบสำรวจความเหมาะสมสำหรับให้ผู้เชี่ยวชาญทั้ง 3 ท่านประเมิน รายละเอียดดังภาพ



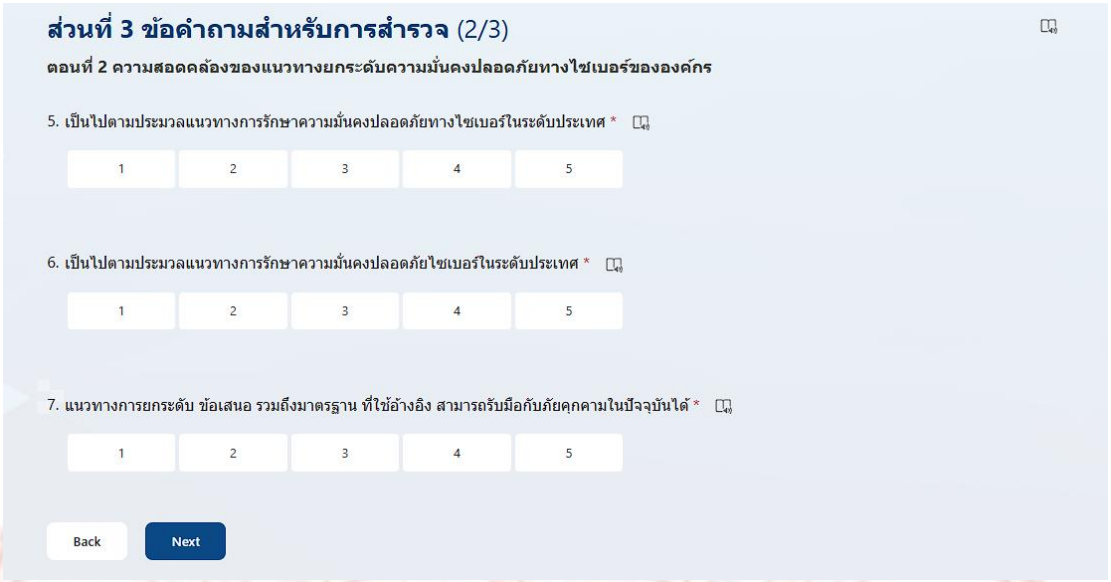
ภาพที่ 3-9 ตัวอย่างแบบสำรวจความเหมาะสม ส่วนที่ 1 คำอธิบาย



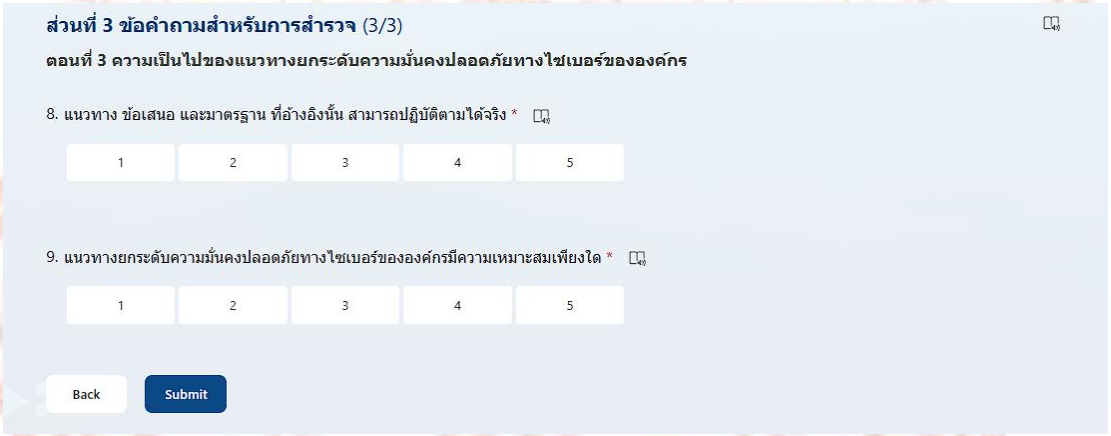
ภาพที่ 3-10 ตัวอย่างแบบสำรวจความเหมาะสม ส่วนที่ 2 ผู้ประเมินแบบสำรวจ โดยแบ่งออกเป็น 3 กลุ่มเป้าหมาย



ภาพที่ 3-11 ตัวอย่างแบบสำรวจความเหมาะสม ส่วนที่ 3 ตอนที่ 1 คุณภาพของแนวทางยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร



ภาพที่ 3-12 ตัวอย่างแบบสำรวจความเหมาะสม ส่วนที่ 3
ตอนที่ 2 ความสอดคล้องของแนวทางยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร



ภาพที่ 3-13 ตัวอย่างแบบสำรวจความเหมาะสม ส่วนที่ 3
ตอนที่ 3 ความเป็นไปได้ของแนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร

3.5 การปรับปรุง (ACTION)

3.5.1 ปรับปรุงแนวทางฯให้สมบูรณ์ตามข้อพิจารณาและข้อเสนอแนะของกลุ่มเป้าหมาย ในขั้นตอนนี้หลังจากได้เสนอแนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรแล้ว ได้รับข้อเสนอ คำแนะนำ จากผู้เชี่ยวชาญทั้ง 3 ท่าน สามารถสรุปหัวข้อสำคัญ ดังนี้

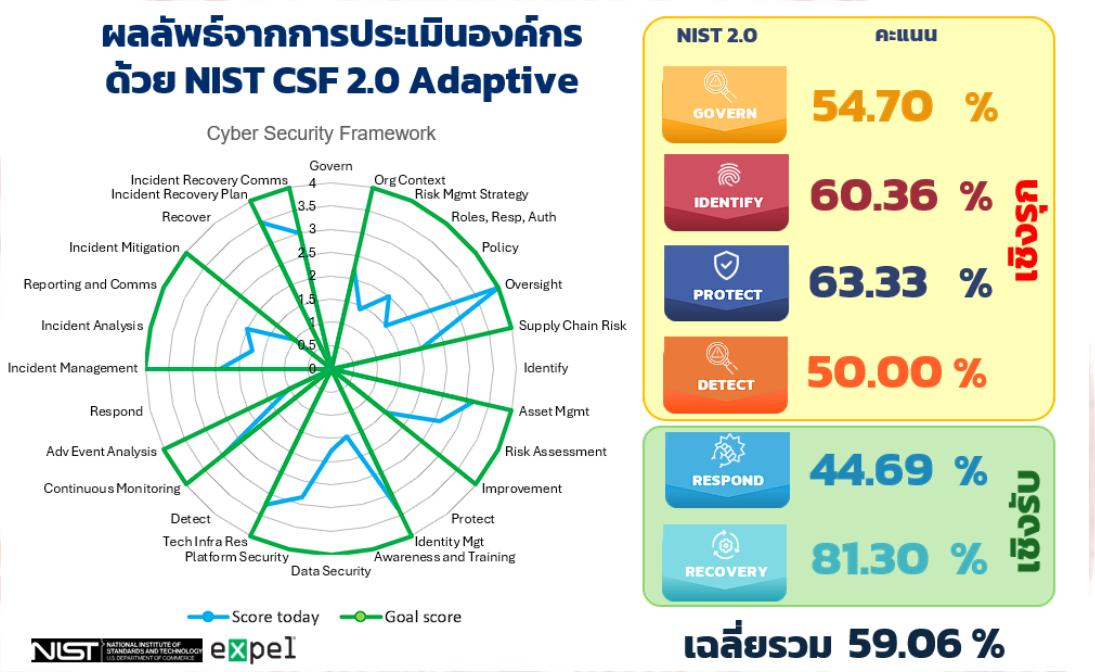
3.5.1.1 ให้เพิ่มเนื้อหาวิธีการใช้เครื่องมือตรวจสอบ Web App ให้ละเอียดขึ้น

3.5.1.2 ตรวจสอบ และสรุปข้อมูล เกี่ยวกับประกาศด้านการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ ขององค์กร กับมาตรฐานตาม ISO ที่ได้เสนอ ว่ามีความสอดคล้อง หรือขัดแย้งอย่างไร

บทที่ 4
ผลการวิจัย

4.1 ผลการศึกษา วิเคราะห์ และประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร

โดยประยุกต์ใช้กรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ เวอร์ชัน 2.0 ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ ประเทศสหรัฐอเมริกา (NIST Cybersecurity Framework 2.0: NIST CSF 2.0)



ภาพที่ 4-1 ผลลัพธ์จากการประเมินองค์กรด้วย NIST CSF 2.0 Adaptive

จากภาพผลลัพธ์จาก NIST CSF 2.0 Adaptive [6] นั้น ด้าน Recovery มีเปอร์เซ็นต์สูงสุด เนื่องจากหน่วยงานภาครัฐ ปฏิบัติตาม พรบ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นการมุ่งเน้นให้องค์กรมีการรับมือแบบเชิงรับ ถึงแม้ว่าด้าน Recovery มีเปอร์เซ็นต์ที่สูง แต่ยังมีด้านอื่นที่ควรเพิ่มประสิทธิภาพ เมื่อดูจากเปอร์เซ็นต์ บ่งชี้ว่า เปอร์เซ็นต์ของกลุ่มเชิงรุกเกาะกลุ่ม ในระดับใกล้เคียงกับค่าเฉลี่ยร้อยละ 59.06 อีกทั้งด้าน Respond ในกลุ่มเชิงรับ มีเปอร์เซ็นต์ต่ำกว่าค่าเฉลี่ย แสดงว่าองค์กรมีการดำเนินการในกลุ่มเชิงรุก และเชิงรับ ด้าน Respond น้อย ดังนั้น เพื่อเพิ่มเปอร์เซ็นต์ กลุ่มเชิงรุก และเชิงรับ ด้าน Respond ให้สอดคล้องกับ ด้าน Recovery ควรดำเนินการในด้านที่เป็นประโยชน์ต่อด้านต่าง ๆ โดย มุ่งเน้นที่ด้าน Detect เพื่อให้ทราบถึงช่องโหว่ พร้อมนำข้อมูลดังกล่าวส่งไปเพิ่มประสิทธิภาพในแต่ละด้าน

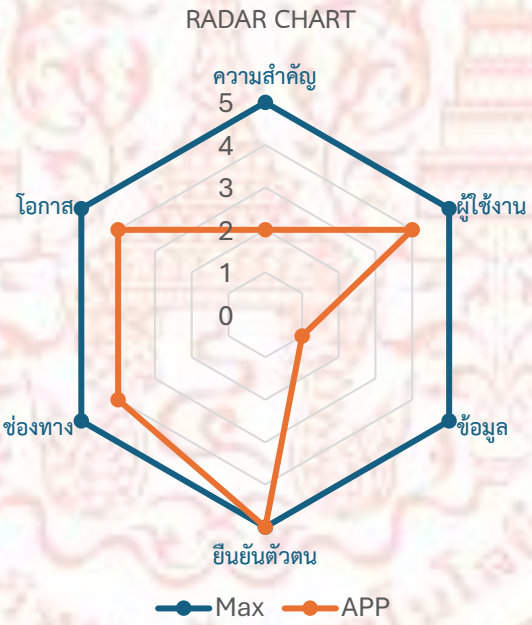
4.2 ผลการศึกษา และคัดเลือก Web Applications ขององค์กร ที่มีผลการประเมินความเสี่ยง (Risk Assessment) สูงสุด 3 อันดับ

การคัดเลือก Web App ที่มีผลการประเมินความเสี่ยงสูง เพื่อคัดเลือก Web App นำร่อง จำนวน 3 Web App สำหรับตรวจสอบ โดยใช้เกณฑ์พิจารณาความเสี่ยงขององค์กร (Risk Assessment) โดยมีรายละเอียดผลการพิจารณาของทั้ง 3 Web App ดังนี้

4.2.1 Web App A

ตารางที่ 3-5 ผลลัพธ์การพิจารณาเกณฑ์ความเสี่ยงของ Web App A

ที่	ชื่อระบบ	พัฒนา	ปรับปรุง	ประเภทการใช้งาน	Dynamic Website	Risk Criteria						Risk Assessment
						1	2	3	4	5	6	
1	Web App A	2558	-	บริการประชาชน	One-Way	2	4	1	5	4	4	20

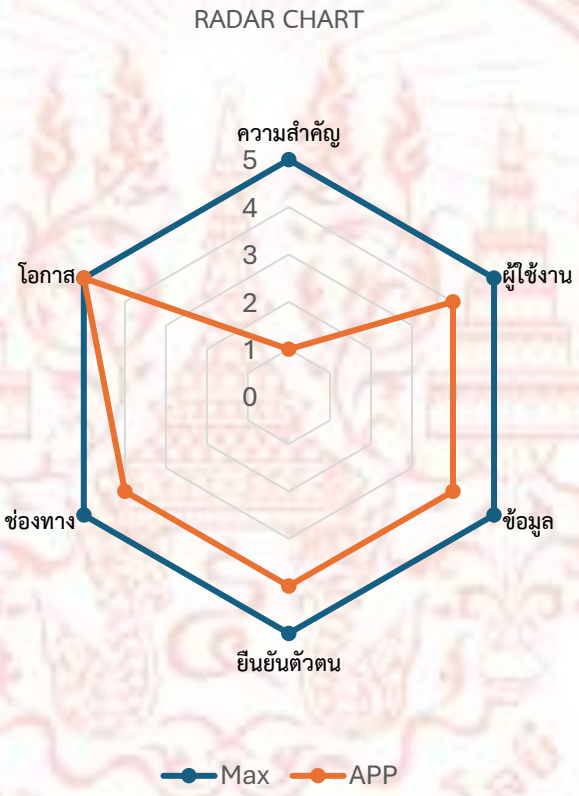


ภาพที่ 4-2 RADAR CHART WEB APP A

4.2.2 Web App B

ตารางที่ 3-6 ผลลัพธ์การพิจารณาเกณฑ์ความเสี่ยงของ Web App B

ที่	ชื่อระบบ	พัฒนา	ปรับปรุง	ประเภทการใช้งาน	Dynamic Website	Risk Criteria						Risk Assessment
						1	2	3	4	5	6	
1	Web App B	2557	-	บริการประชาชน	Two-ways	1	4	4	4	4	5	22

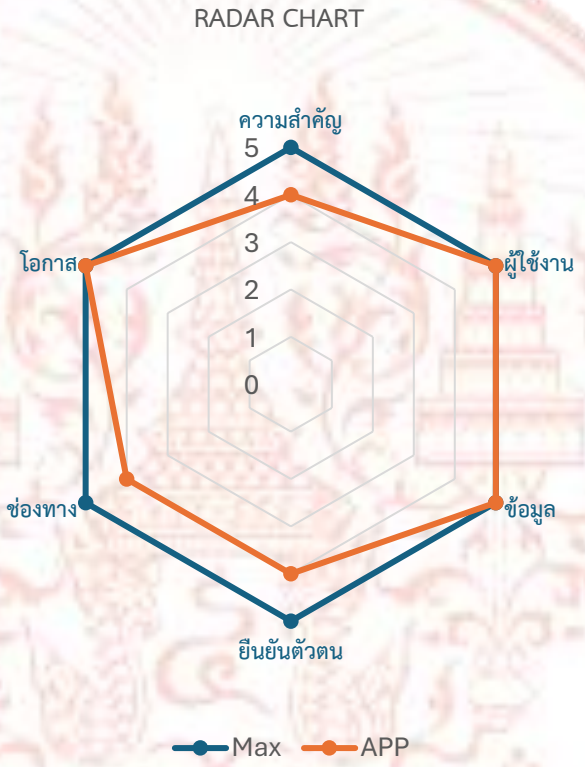


ภาพที่ 4-3 RADAR CHART WEB APP B

4.2.3 Web App C

ตารางที่ 3-7 ผลลัพธ์การพิจารณาเกณฑ์ความเสี่ยงของ Web App C

ที่	ชื่อระบบ	พัฒนา	ปรับปรุง	ประเภทการใช้งาน	Dynamic Website	Risk Criteria						Risk Assessment
						1	2	3	4	5	6	
1	Web App C	2564	2567	บริการประชาชน	Two-ways	4	5	5	4	4	5	27



ภาพที่ 4-4 RADAR CHART WEB APP C

4.3 ผลการศึกษา และคัดเลือก VA Tools จำนวน 3 เครื่องมือ จากรายชื่อเครื่องมือที่ OWASP เผยแพร่

นำ VA Tools จำนวน 102 เครื่องมือ โดยประยุกต์ใช้ทฤษฎี 7 Rights of Logistics

ตารางที่ 4-1 การคัดเลือก VA Tools

7P	หลักเกณฑ์	จำนวน VA Tools
1	Price เครื่องมือเป็นแบบ Open Source หรือ Free License	28
2	Privacy เครื่องมือมีข้อตกลงการไม่ส่งข้อมูลการตรวจสอบเกี่ยวกับข้อมูลของ Web App องค์กรกลับไปยังผู้พัฒนา	16
3	Passive เครื่องมือมีความสามารถตราวจสอบช่องโหว่ด้วยตนเอง โดยไม่มีการ Integration ผลลัพธ์จากเครื่องมืออื่น	15
4	Place เครื่องมือสามารถทำงานได้บน On-Premise และไม่ต้องเข้าถึงโค๊ด (Code) ของ Web App	8
5	Popular เครื่องมือมีความนิยม และมีชุมชนแลกเปลี่ยนข้อมูล (Community) ขนาดใหญ่ที่มีความน่าเชื่อถือ	3
6	Present เครื่องมือมีการพัฒนา (Develop) เทคนิคการตรวจสอบ Web App อย่างต่อเนื่องจนถึงปัจจุบัน	3
7	Performance เครื่องมือมีประสิทธิภาพในการตรวจสอบ Web App มีเกณฑ์ดังนี้ - In depth เครื่องมือมีประสิทธิภาพสามารถตรวจสอบช่องโหว่ได้ละเอียดและครอบคลุม - User Friendly เครื่องมือใช้งานง่าย ไม่ซับซ้อน สามารถเรียนรู้ได้อย่างรวดเร็วโดยไม่ต้องมีองค์ความรู้เฉพาะด้าน - Alert Tag มีการแจ้งเตือนช่องโหว่พร้อมกับระบุความสอดคล้องกับมาตรฐานสากล อาทิ OWASP Top 10, CWE - Suggestions มีคำแนะนำในการแก้ไขช่องโหว่ พร้อมแหล่งอ้างอิงให้ไปสืบค้นข้อมูลเพิ่มเติม	1

4.4 ผลการศึกษา และกำหนดวิธีการตรวจสอบและระบุช่องโหว่

โดยใช้ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงพื้นฐานสำคัญทางสารสนเทศ

4.5 ผลการดำเนินการตรวจสอบและระบุช่องโหว่

4.5.1 เว็บแอปพลิเคชัน A (Web App A) เป็นระบบที่มีฟังก์ชันการทำงานสำคัญต่อองค์กรเป็นอย่างมากเนื่องจาก มีข้อมูลจำนวนมาก เป็นช่องทางหลักในการประชาสัมพันธ์ สื่อสารข้อมูลข่าวสารต่างๆ ขององค์กร ต่อประชาชน ผู้มีส่วนได้เสีย และผู้ปฏิบัติงานขององค์กร

4.5.1.1 สรุปจำนวนช่องโหว่ที่ตรวจพบ

ตารางที่ 4-2 สรุปจำนวนช่องโหว่ที่ตรวจพบของ Web App A

ระดับความเสี่ยง	*Alert Tag*	*จำนวนที่พบ (ครั้ง)*
High	*2*	*6*
Medium	*4*	*8,974*
Low	*12*	43,525
Information	*8*	10,988

4.5.1.2 รายละเอียดช่องโหว่ที่ตรวจพบ

ตารางที่ 4-3 รายละเอียดช่องโหว่ที่ตรวจพบของ Web App A

ลำดับ	*รายการแจ้งเตือนช่องโหว่*	*ระดับความเสี่ยง*	*แท็กอ้างอิง*		*จำนวนที่พบ (ครั้ง)*
			OWASP 2021	*CWE*	
1	PII Disclosure	High	A04	359	4
2	Vulnerable JS Library	High	A06	829	2
3	Absence of Anti-CSRF Tokens	Medium	A01	352	55
4	Content Security Policy (CSP) Header Not Set	Medium	A05	693	5739
5	Missing Anti-clickjacking Header	Medium	A05	1021	3167
6	Vulnerable JS Library	Medium	A06	829	13
7	Application Error Disclosure	Low	A05	200	36
8	Big Redirect Detected (Potential Sensitive Information Leak)	Low	A04	201	152
9	Cookie No HttpOnly Flag	Low	A05	1004	1204
10	Cookie Without Secure Flag	Low	A05	614	1292
11	Cookie without SameSite Attribute	Low	A01	1275	1852
12	Cross-Domain JavaScript Source File Inclusion	Low	A08	829	8314
13	Information Disclosure - Debug Error Messages	Low	A01	200	4

ตารางที่ 4-4(ต่อ) รายละเอียดช่องโหว่ที่ตรวจพบของ Web App A

ลำดับ	รายการแจ้งเตือนช่องโหว่	ระดับความเสี่ยง	แท็กอ้างอิง		จำนวนที่พบ (ครั้ง)
14	Private IP Disclosure	Low	A01	200	34
15	Secure Pages Include Mixed Content	Low	A05	311	27
16	Strict-Transport-Security Header Not Set	Low	A05	319	16158
17	Timestamp Disclosure - Unix	Low	A01	200	910
18	X-Content-Type-Options Header Missing	Low	A05	693	13542
19	Authentication Request Identified	Information	-	-	4
20	Content-Type Header Missing	Information	A05	345	424
21	Information Disclosure - Suspicious Comments	Information	A01	200	5311
22	Modern Web Application	Information	-	-	3342
23	Re-examine Cache-control Directives	Information	-	525	1075
24	Session Management Response Identified	Information	-	-	650
25	User Controllable HTML Element Attribute (Potential XSS)	Information	A03	20	179
26	Vulnerable JS Library	Information	A06	829	3

4.5.2 เว็บแอปพลิเคชัน B (Web App B) เป็นระบบที่ให้บริการประชาชน ด้านการเก็บข้อมูลประวัติส่วนตัว ผลงาน ความสามารถต่างๆ ของประชาชนที่สนใจจะเข้ามาทำงานองค์กร

4.5.2.1 สรุปจำนวนช่องโหว่ที่ตรวจพบ

ตารางที่ 4-5 สรุปจำนวนช่องโหว่ที่ตรวจพบของ Web App B

ระดับความเสี่ยง	*Alert Tag*	*จำนวนที่พบ (ครั้ง)*
High	-	-
Medium	*2*	*6*
Low	*5*	30
Information	*4*	6

4.5.2.2 รายละเอียดช่องโหว่ที่ตรวจพบ

ตารางที่ 4-6 รายละเอียดช่องโหว่ที่ตรวจพบของ Web App B

ลำดับ	Alert	Priority Alert	แท็กอ้างอิง		จำนวน
			OWASP 2021	*CWE*	
1	Absence of Anti-CSRF Tokens	Medium	A01	352	1
2	Content Security Policy (CSP) Header Not Set	Medium	A05	693	5
3	Cookie Without Secure Flag	Low	A05	614	1
4	Server Leaks Version Information via "Server" HTTP Response Header Field	Low	A05	200	10
5	Strict-Transport-Security Header Not Set	Low	A05	319	9
6	X-AspNet-Version Response Header	Low	A05	933	3
7	X-Content-Type-Options Header Missing	Low	A05	693	7
8	Information Disclosure - Suspicious Comments	Information	A01	200	2
9	Re-examine Cache-control Directives	Information	-	525	2
10	User Controllable HTML Element Attribute (Potential XSS)	Information	A03	20	2

4.5.3 เว็บแอปพลิเคชัน C (Web App C) เป็นระบบที่ให้บริการประชาชน ด้านข้อมูล แนวทางปฏิบัติ เพื่อการช่วยเหลือประชาชนที่เป็นผู้ได้รับความเสียหายจากผู้กระทำความผิด ซึ่งรองรับและเก็บข้อมูลผู้เสียหายเป็นจำนวนมากในการเข้ามาใช้งานระบบดังกล่าว

4.5.3.1 สรุปจำนวนช่องโหว่ที่ตรวจพบ

ตารางที่ 4-7 สรุปจำนวนช่องโหว่ที่ตรวจพบของ Web App C

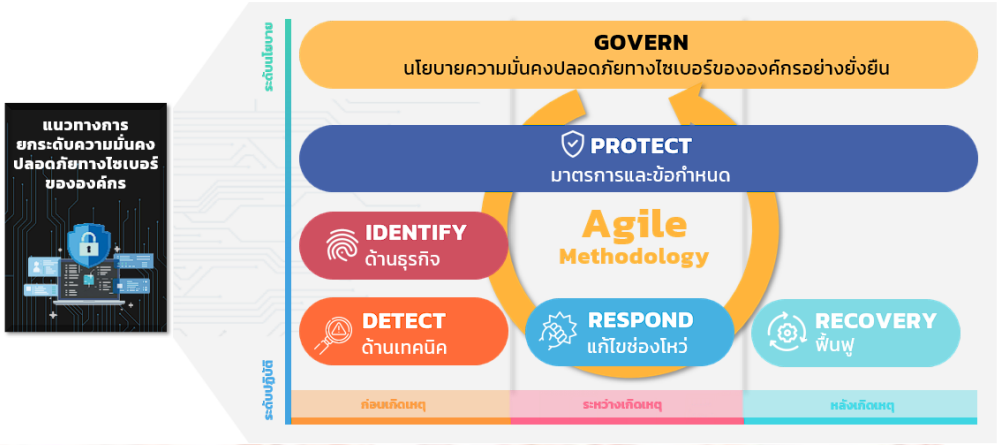
ระดับความเสี่ยง	*Alert Tag*	*จำนวนที่พบ (ครั้ง)*
High	-	-
Medium	*3*	*17*
Low	*8*	122
Information	*6*	256

4.5.3.2 รายละเอียดช่องโหว่ที่ตรวจพบ

ตารางที่ 4-8 รายละเอียดช่องโหว่ที่ตรวจพบของ Web App C

Alert	*Priority Alert*	*แท็กอ้างอิง*		*จำนวน*
		OWASP 2021	*CWE*	
Content Security Policy (CSP) Header Not Set	Medium	A05	693	9
Missing Anti-clickjacking Header	Medium	A05	1021	6
Vulnerable JS Library	Medium	A06	829	2
Application Error Disclosure	Low	A05	200	2
Big Redirect Detected (Potential Sensitive Information Leak)	Low	A04	201	7
Cookie No HttpOnly Flag	Low	A05	1004	13
Cookie Without Secure Flag	Low	A05	614	26
Cookie without SameSite Attribute	Low	A01	1275	26
Cross-Domain JavaScript Source File Inclusion	Low	A08	829	3
Strict-Transport-Security Header Not Set	Low	A05	319	24
X-Content-Type-Options Header Missing	Low	A05	693	21
Information Disclosure - Suspicious Comments	Information	A01	200	9
Modern Web Application	Information	-	-	6
Re-examine Cache-control Directives	Information	-	525	5
Session Management Response Identified	Information	-	-	131
User Controllable HTML Element Attribute (Potential XSS)	Information	A03	20	103
Vulnerable JS Library	Information	A06	829	2

4.6 ผลการศึกษา วิเคราะห์ และจัดทำแนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร



ภาพที่ 4-5 เป้าหมายของเล่มแนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร

จากภาพ 4-1 คือเป้าหมายของเล่มแนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร ช่วยให้องค์กรมีความมั่นคงปลอดภัยทางไซเบอร์ ตั้งแต่ระดับนโยบาย ลงไปจนถึงระดับปฏิบัติ โดยมี NIST CSF 2.0 เป็นหัวใจสำคัญ ซึ่งเข้ามาช่วยยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรในทั้ง 3 ช่วงเวลา ดังนี้ 1) ก่อนเกิดเหตุ 2) ระหว่างเกิดเหตุ และ 3) หลังการเกิดเหตุ

การวิจัยนี้ผู้วิจัยเริ่มที่กระบวนการ (DETECT) คือการตรวจสอบ Web App นำร่องทั้ง 3 เพื่อให้ทราบปัญหาช่องโหว่ที่มีอยู่ในปัจจุบัน จากนั้นการศึกษาแนวทางการจัดการช่องโหว่ (RESPOND) ไปจนถึงแผนการรับมือหลังเกิดเหตุการถูกโจมตี (RECOVERY) กำหนดมาตรการ (PROTECT) ส่งผลให้มีการปรับปรุงนโยบาย (GORVERN) ซึ่งผู้วิจัยได้นำ Agile Methodology มาประยุกต์ใช้ร่วมกัน หากดำเนินการตามแนวทางยกระดับความมั่นคงปลอดภัยทางไซเบอร์ จะส่งผลให้องค์กร มีนโยบายความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรอย่างยั่งยืน

4.7 ผลการประเมินความเหมาะสมของแนวทางยกระดับความมั่นคงปลอดภัยทางไซเบอร์องค์กร

4.7.1 จัดทำแนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร (ภาคผนวก ก) โดยวิเคราะห์ช่องโหว่และเสนอแนวทางการจัดการช่องโหว่สำหรับ Web App ทั้ง 3 โดยมีเนื้อหาแบ่งเป็น 6 บท รายละเอียดดังนี้

4.7.1.1 บทที่ 1 บทนำ

4.7.1.2 บทที่ 2 ศึกษา กำหนดเกณฑ์ การคัดเลือก เครื่องมือและเว็บแอปพลิเคชัน

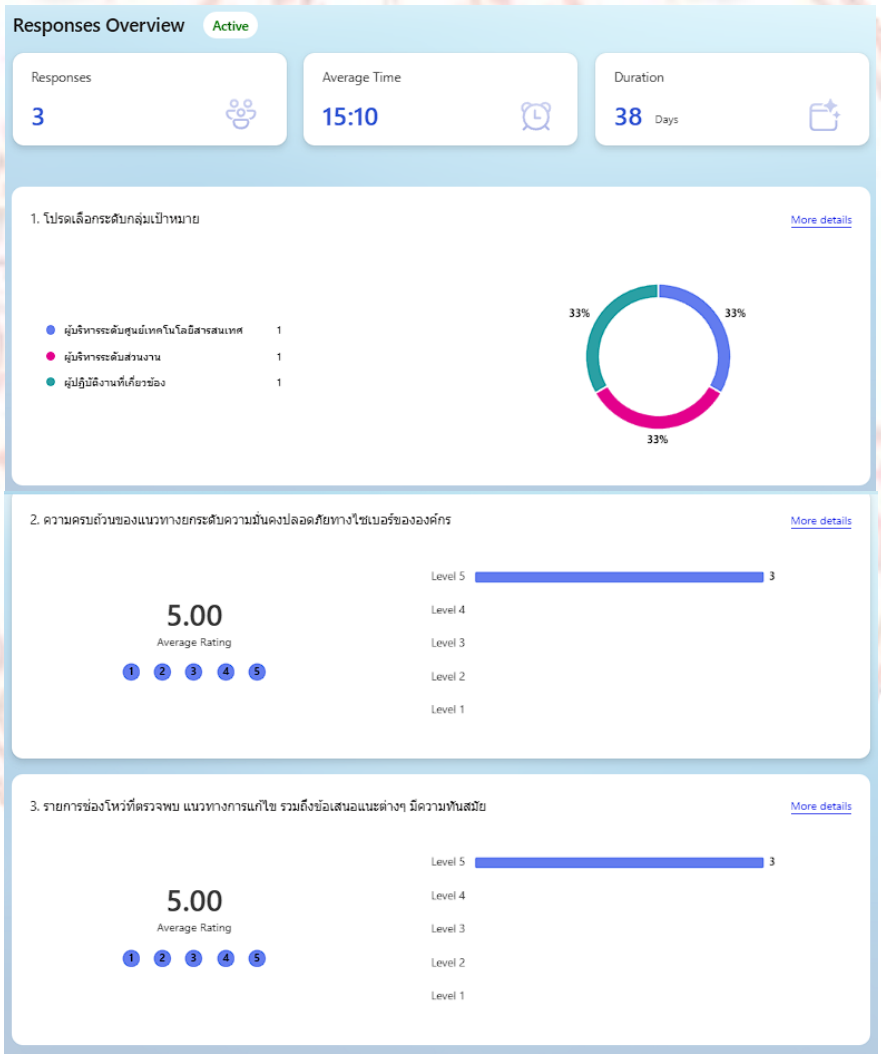
4.7.1.3 บทที่ 3 วิธีการดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ระบบเทคโนโลยีสารสนเทศ

4.7.1.4 บทที่ 4 แนวทางการยกระดับความมั่นคงปลอดภัยของเว็บแอปพลิเคชัน

4.7.1.5 บทที่ 5 มาตรการสากลในพัฒนาเว็บแอปพลิเคชัน ให้มั่นคงปลอดภัยตามมาตรฐานสากล

4.7.1.6 บทที่ 6 ปัญหาอุปสรรค และข้อเสนอแนะ

4.7.2 แนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร มีรายละเอียดเกี่ยวกับการศึกษา กำหนดเกณฑ์ การคัดเลือกเครื่องมือ วิธีดำเนินการตรวจสอบ ผลการตรวจสอบความมั่นคงปลอดภัยของ Web App องค์กร แนวทางการยกระดับความมั่นคงปลอดภัยของเว็บ Web App ตามมาตรฐาน OWASP Top Ten, CWE และ ISO ปัญหาอุปสรรค และข้อเสนอแนะ ซึ่งผลการประเมินความเหมาะสม แบ่งเป็น คุณภาพ ความสอดคล้องตามประมวลแนวทางของระดับประเทศ และระดับองค์กร รวมถึงความเป็นไปได้ในการนำไปใช้งานจริง ซึ่งประเมินโดยผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ จำนวน 3 ท่าน ผลลัพธ์แสดงให้เห็นว่าอยู่ในระดับเหมาะสมกับองค์กรในระดับดีมาก



ภาพที่ 4-6 ผลประเมินความเหมาะสมเฉลี่ยของข้อที่ 1 ถึง 3

ภาพที่ 4-7 ผลประเมินความเหมาะสมเฉลี่ยของข้อที่ 4 ถึง 9

บทที่ 5
สรุปผลการวิจัย ความท้าทาย และข้อเสนอแนะ

5.1 สรุปผลการวิจัย

การตรวจสอบความมั่นคงปลอดภัยของ Web App หน่วยงาน เพื่อเสนอแนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรนั้น พบว่า การทราบถึงช่องโหว่ที่ตรวจพบจากทั้ง 3 Web App นำร่อง พร้อมกำหนดแนวทางการแก้ไขช่องโหว่ ไม่ได้เป็นการยกระดับ Web App นำร่องเพียงอย่างเดียวเท่านั้น แต่แนวทางการแก้ไขช่องโหว่ดังกล่าวนั้น ยังสามารถนำไปใช้กับ Web App อื่นๆ ได้ด้วย เนื่องจากรายการช่องโหว่ที่พบส่วนใหญ่เป็นจุดอ่อนที่ผู้พัฒนาระบบขององค์กรไม่คาดคิด ส่งผลให้ช่องโหว่ในลักษณะเดียวกันเกิดขึ้นกับ Web App อื่น ๆ ขององค์กรด้วยเช่นกัน

การวัดและประเมินความเป็นไปได้ของแนวทางการยกระดับความมั่นคงปลอดภัย พบว่า แนวทางที่นำเสนอสามารถนำไปใช้ได้จริงและเกิดประโยชน์ต่อองค์กร โดยแนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรที่กำหนดสอด และเสนอ มีความสอดคล้องกับมาตรฐานสากล NIST CSF, OWASP และ ISO 27001 ซึ่งช่วยให้องค์กรสามารถปรับตัวและเพิ่มระดับความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ การปฏิบัติตามข้อเสนอแนะดังกล่าว สามารถสร้างความมั่นใจให้องค์กรได้ว่า จะส่งผลให้เปอร์เซ็นต์ในแต่ละด้านของ NIST CSF 2.0 Adaptive เพิ่มขึ้นสอดคล้องกับเปอร์เซ็นต์ ด้าน Recoveryซึ่งสามารถปลี่ยนรูปแบบการดำเนินงานขององค์กรในด้านความมั่นคงปลอดภัยทางไซเบอร์จากเชิงรับ เป็นเชิงรุกได้อย่างยั่งยืน

สุดท้ายนี้การตรวจสอบความมั่นคงปลอดภัยของ Web App ยังสร้างความเข้าใจ ปรับเปลี่ยนมุมมอง และลดความกังวลในการอนุญาตให้ดำเนินการตรวจสอบ เนื่องจากการตรวจสอบดังกล่าวไม่ได้สะท้อนผลลัพธ์ในเชิงลบเพียงอย่างเดียว ทว่าผลลัพธ์จากการตรวจสอบ ยังเสริมสร้างภาพลักษณ์ที่ดีให้กับองค์กรในด้านความเชื่อมั่นของประชาชนในการเข้ามาใช้บริการ Web App อย่างมีนัยสำคัญ

5.2 การประยุกต์ใช้แนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร

หน่วยงานภาครัฐและองค์กร สามารถนำแนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรไปประยุกต์ใช้เพื่อยกระดับความมั่นคงปลอดภัยของ Web App หน่วยงานและองค์กร โดยสามารถประยุกต์ใช้ ดังนี้

5.2.1 เครื่องมือประเมินตนเอง (Self Assessment Tools) สำหรับประเมินหน่วยงานภาครัฐและองค์กร สามารถประยุกต์ใช้ตามการค้นคว้าอิสระนี้ โดยการหาค่าเฉลี่ยของแต่ละด้านเพื่อให้ทราบว่าควรเพิ่มประสิทธิภาพที่ด้านใดของ NIST

5.2.2 การคัดเลือกเครื่องมือตรวจสอบระบบ (7P Algorithm) ที่เหมาะสมกับบริบทของหน่วยงานและองค์กร ซึ่งสามารถใช้เกณฑ์ ทั้ง 7P ตามการค้นคว้าอิสระนี้ หรือประยุกต์โดยปรับเกณฑ์ให้เหมาะสมกับบริบทของหน่วยงานและองค์กรได้

5.2.3 เกณฑ์การพิจารณาความเสี่ยง (Risk Criteria) ในการคัดเลือก Web App ที่มีความเสี่ยงและควรเร่งดำเนินการตรวจสอบโดยเร็ว ซึ่งเกณฑ์ทั้ง 6 ด้านนั้นสามารถประยุกต์ใช้งานให้เหมาะสมกับ หน่วยงานภาครัฐและองค์กร

5.2.4 แนวทางการแก้ไขช่องโหว่ทั้ง 3 Web App นั้น มีช่องโหว่ที่คล้ายคลึงกัน อีกทั้งยังอยู่ใน OWASP TOP 10 ซึ่งผู้วิจัยมีความมั่นใจ หน่วยงานภาครัฐและองค์กรสามารถนำแนวทางการแก้ไขไปตรวจสอบและกำหนดค่าเพื่อยกระดับ Web App ของตนเองได้โดยยังไม่จำเป็นต้องลงมือตรวจสอบด้วยตนเองในเบื้องต้น

5.3 ข้อเสนอแนะ

5.3.1 การเพิ่มประสิทธิภาพในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ หลังจากที่ได้ผลลัพธ์จากการใช้ VA SCAN แล้ว ควรพิจารณาดำเนินการ Penetration Testing หรือการตรวจสอบจากผู้เชี่ยวชาญภายนอก เพิ่มเติม เพื่อความครอบคลุมในการตรวจสอบช่องโหว่ และได้ช่องโหว่เชิงลึกและมีความละเอียดมากขึ้น

5.3.2 ความทันสมัยของเครื่องมือทดสอบความมั่นคงปลอดภัยไซเบอร์ Web App ควรตรวจสอบความทันสมัยของ VA SCAN ก่อนการใช้ตรวจสอบความมั่นคงปลอดภัยไซเบอร์ Web App ในครั้งถัดไป เนื่องจาก VA SCAN ที่ใช้ในแนวทางฯ นี้ ในอนาคตอาจล้าสมัย และไม่เป็น VA SCAN ที่เหมาะสม ทั้งนี้ เพื่อให้ได้เครื่องมือที่เหมาะสมกับองค์กรควรดำเนินการคัดเลือก VA SCAN ตาม 7P Algorithm

5.3.3 การลดระยะเวลาการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ Web App เพื่อให้ได้ VA SCAN ที่ตอบโจทย์การใช้งานขององค์กรที่มี Web App จำนวนมาก รวมถึงหน่วยงานภาครัฐมีข้อจำกัดด้านจำนวนบุคคลากรองค์กรไม่เพียงพอ และมีระยะเวลาจำกัด ควรพัฒนา VA SCAN ที่สามารถทำงานได้อัตโนมัติ เพื่อเป็นการเพิ่มประสิทธิภาพ รวมทั้งประหยัดเวลาในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์

บรรณานุกรม

[1] สกมช., “สถิติภัยคุกคามทางไซเบอร์,” 2566.

[2] OWASP, "Welcome to the OWASP Top 10 - 2021," 2021. [Online]. Available: https://owasp.org/Top10/. [Accessed 6 November 2024].

[3] NIST, “The NIST Cybersecurity Framework (CSF) 2.0,” 26 กุมภาพันธ์ 2567.

[4] องค์กร, “Risk Criteria,” 2567.

[5] "7Rs," [Online]. [Accessed 2024].

[6] Expel, "self-scoring tool for NIST 2.0," expel, [Online]. Available: https://expel.com/expel-self-scoring-tool-for-nist-csf/. [Accessed 2024].

[7] ธ. ฟองสมุทร, “การเชื่อมโยงแนวคิดทางโลจิสติกส์สู่การวางแผนการเงินส่วนบุคคล,” สถาบันวิจัยและพัฒนา มหาวิทยาลัยราชภัฏกำแพงเพชร. [ออนไลน์]. [วันที่เข้าถึง 4 เมษายน 2567].

[8] L. United Information Highway Co., “NIST Cybersecurity Framework,” 5 April 2024. [ออนไลน์]. Available: https://www.uih.co.th/th/products-services/security-services-th/nist-cybersecurity-framework/.

[9] T. K. Dakiniswari V, “AssessJet - Penetration testing and Vulnerability Assessment for Websites,” 2024.

[10] D. Laksmiati, "Vulnerability Assessment with Network-Based Scanner Method for Improving," 2023.

[11] S. Patil, M. Rao, L. Misal, D. Phaldesai และ K. Shivsharan, “A Review of the OW ASP Top 10 Web Application Security Risks and Best Practices for Mitigating These Risks,” 2023.

[12] L. S. K. J. N. Ritik Karayat, “Web Application Penetration Testing & Patch,” 2022.

[13] A. R. S. K. Ashish Joshi, “An Analysis of Vulnerability Scanners in Web,” 2022.

[14] สกมช., 2564. [ออนไลน์]. Available: https://drive.ncsa.or.th/s/6rFJ66fNstfK6ni. [วันที่เข้าถึง6 พฤศจิกายน 2564].

[15] MITRE, "CWE," [Online]. Available: https://cwe.mitre.org/index.html. [Accessed 7 November 2024].

[16] Foundation, The OWASP®, "Vulnerability Scanning Tools," 6 November 2567. [Online]. Available: https://owasp.org/www-community/Vulnerability_Scanning_Tools.

ภาคผนวก ก

แนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร

ผลกระทบ และแนวทางจัดการช่องโหว่ Web Applications

1. เว็บแอปพลิเคชัน A (Web App A)

ลำดับ	**1**		
รายการแจ้งเตือนช่องโหว่	PII Disclosure		
ระดับความเสี่ยง	High	**ความเร่งด่วน**	**ตรวจสอบและแก้ไขทันที**
ผลกระทบ	มีเนื้อหาแสดงบนหน้าระบบที่มีความคล้ายคลึงกับเลขบัตรประชาชน เลขบัตรเครดิต		
แนวทางแก้ไข	ตรวจสอบให้มั่นใจว่าไม่มีข้อมูลส่วนบุคคล ที่ปรากฏในระบบ เช่น เลขบัตรประชาชน เลขบัตรเครดิต หากมีให้ลบออกในทันที		
ลำดับ	**2**		
รายการแจ้งเตือนช่องโหว่	Vulnerable JS Library		
ระดับความเสี่ยง	High	**ความเร่งด่วน**	**ตรวจสอบและแก้ไขทันที**
ผลกระทบ	Bootstrap-select เวอร์ชันก่อนหน้า 1.13.6 มีช่องโหว่ Cross-Site Scripting (XSS) โดยไม่ได้ทำการ escape ค่า title ในแท็ก <option> ซึ่งอาจเปิดโอกาสให้ผู้โจมตีสามารถรันโค้ด JavaScript ต่างๆ ในเบราว์เซอร์ได้		
แนวทางแก้ไข	ดำเนินการ Upgrade library Bootstrap-select เป็นเวอร์ชันปัจจุบัน		
ลำดับ	**3**		
รายการแจ้งเตือนช่องโหว่	Absence of Anti-CSRF Tokens		
ระดับความเสี่ยง	Medium	**ความเร่งด่วน**	**ภายใน 3 – 6 เดือน**
ผลกระทบ	การโจมตีแบบ Cross-Site Request Forgery (CSRF) เป็นการโจมตีที่บังคับให้เหยื่อส่งคำขอ HTTP ไปยังปลายทางเป้าหมายโดยที่เหยื่อไม่รู้ตัวหรือไม่มีเจตนา เพื่อดำเนินการบางอย่างในระบบ เช่น การเปลี่ยนแปลงข้อมูล หรือการดำเนินการที่สำคัญ โดยอาศัยช่องโหว่จากการขาดการตรวจสอบ Anti-CSRF Token ในฟอร์ม HTM		
แนวทางแก้ไข	เพิ่ม Anti-CSRF tokens ในฟอร์ม HTML เพื่อตรวจสอบว่าคำขอที่มาถึงมาจากแหล่งที่เชื่อถือได้และผู้ใช้ที่ได้รับอนุญาต		

ลำดับ	**4**		
รายการแจ้งเตือนช่องโหว่	Content Security Policy (CSP) Header Not Set		
ระดับความเสี่ยง	Medium	**ความเร่งด่วน**	**ภายใน 3 – 6 เดือน**
ผลกระทบ	โอกาสที่ผู้โจมตีจะหลีกเลี่ยงกลไกการป้องกัน (Bypass Protection Mechanism) ได้ รวมถึงการโจมตีแบบ Cross-Site Scripting (XSS) โดยการกำหนดแหล่งที่มาของเนื้อหาที่เบราว์เซอร์สามารถโหลดได้ และและการโจมตีด้วยการแทรกข้อมูล (Data Injection) การโจมตีเหล่านี้สามารถนำไปสู่การขโมยข้อมูล การเปลี่ยนแปลงหน้าเว็บไซต์ หรือการกระจายมัลแวร์		
แนวทางแก้ไข	1. ดำเนินการกำหนด Content-Security-Policy (CSP) ให้ชุดของ HTTP Header อาทิ 1) Web Server 2) Web Application Server 3) Load Balancer และ 4) อื่นๆ 2. ลบข้อความแสดงข้อผิดพลาดและข้อมูลที่ไม่จำเป็นที่ให้ข้อมูลมากเกินไปแก่ผู้ใช้ อาทิ Comment ช่วยให้ผู้รับผิดชอบเว็บไซต์สามารถกำหนดแหล่งที่มาของเนื้อหาที่ได้รับการอนุญาตให้เบราว์เซอร์โหลดบนหน้าเว็บนั้น ซึ่งเนื้อหาที่ครอบคลุม ได้แก่ JavaScript, CSS, เฟรม HTML, ฟอนต์, รูปภาพ และวัตถุฝังตัว เช่น Java Applets, ActiveX, ไฟล์เสียง และวิดีโอ		
ลำดับ	**5**		
รายการแจ้งเตือนช่องโหว่	Missing Anti-clickjacking Header		
ระดับความเสี่ยง	Medium	**ความเร่งด่วน**	**ภายใน 3 – 6 เดือน**
ผลกระทบ	ไม่มีการป้องกันการโจมตีประเภท ClickJacking ควรมีการตั้งค่า Content-Security-Policy ที่ประกอบด้วยคำสั่ง 'frame-ancestors' หรือ X-Frame-Options เพื่อเสริมการป้องกันดังกล่าว		
แนวทางแก้ไข	ดำเนินการตั้งค่า Content-Security-Policy พร้อมคำสั่ง 'frame-ancestors' directive หรือใช้ X-Frame-Options เพื่อป้องกัน		

ลำดับ	**6**		
รายการแจ้งเตือนช่องโหว่	Vulnerable JS Library		
ระดับความเสี่ยง	Medium	**ความเร่งด่วน**	ภายใน 3 – 6 เดือน
ผลกระทบ	การรันโค้ดหรือคำสั่งที่ไม่ได้รับอนุญาต โดยผู้โจมตีอาจแทรกฟังก์ชันที่เป็นอันตรายเข้าสู่โปรแกรมได้ โดยทำให้โปรแกรมดาวน์โหลดโค้ดที่ผู้โจมตีวางไว้ในพื้นที่ที่ไม่มีความน่าเชื่อถือ เช่น เว็บไซต์ที่เป็นอันตราย		
แนวทางแก้ไข	1. ดำเนินการ Upgrade bootstrap ให้เป็นเวอร์ชันล่าสุด 2. ดำเนินการ Upgrade jquery ให้เป็นเวอร์ชันล่าสุด		
ลำดับ	**7**		
รายการแจ้งเตือนช่องโหว่	Application Error Disclosure		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	ไม่มี (ติดตามเป็นระยะ)
ผลกระทบ	มีการแสดงข้อผิดพลาดหรือข้อความเตือนที่อาจเปิดเผยข้อมูลที่เป็นความลับ เช่น ตำแหน่งของไฟล์ที่ทำให้เกิดข้อยกเว้นที่ไม่ได้รับการจัดการ (Unhandled Exception) ข้อมูลนี้อาจถูกนำไปใช้เพื่อโจมตีเพิ่มเติมต่อเว็บแอปพลิเคชันได้ อย่างไรก็ตาม การแจ้งเตือนนี้อาจเป็นการแจ้งเตือนที่ผิดพลาด (False Positive) หากพบข้อความข้อผิดพลาดนี้ในหน้าคู่มือหรือเอกสารประกอบการใช้งานระบบ		
แนวทางแก้ไข	ตรวจสอบซอร์สโค้ด และสร้างหน้าแสดงข้อผิดพลาดแบบกำหนดเอง นอกจากนี้ ควรพิจารณาการสร้างกลไกเพื่อให้หมายเลขอ้างอิงหรือรหัสเฉพาะสำหรับข้อผิดพลาดแก่ฝั่งไคลเอนต์ (เบราว์เซอร์) ขณะเดียวกันให้บันทึกรายละเอียดข้อผิดพลาดไว้ที่ฝั่งเซิร์ฟเวอร์โดยไม่เปิดเผยข้อมูลให้กับผู้ใช้		
ลำดับ	**8**		
รายการแจ้งเตือนช่องโหว่	Big Redirect Detected (Potential Sensitive Information Leak)		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	ไม่มี (ติดตามเป็นระยะ)
ผลกระทบ	เซิร์ฟเวอร์ตอบกลับด้วยการเปลี่ยนเส้นทาง (Redirect) แต่มีขนาดของการตอบกลับที่ใหญ่ผิดปกติ ซึ่งมีความเป็นไปได้ว่า ต่อให้เซิร์ฟเวอร์จะส่งคำสั่งเปลี่ยนเส้นทาง แต่ยังมีเนื้อหาตอบกลับในส่วนของข้อความ (Body Content) ซึ่งอาจรวมถึงข้อมูลที่มีความละเอียดอ่อน เช่น ข้อมูลส่วนบุคคล (PII) หรือข้อมูลสำคัญอื่น ๆ		

แนวทางแก้ไข	ตรวจสอบว่าไม่มีข้อมูลที่มีความละเอียดอ่อนรั่วไหลผ่านการตอบกลับการเปลี่ยนเส้นทาง (Redirect) ซึ่งการตอบกลับการเปลี่ยนเส้นทางควรมีเนื้อหาเพียงเล็กน้อยหรือไม่มีเลย		
ลำดับ	**9**		
รายการแจ้งเตือนช่องโหว่	Cookie No HttpOnly Flag		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	ไม่มี (ติดตามเป็นระยะ)
ผลกระทบ	การตั้งค่าคุกกี้โดยไม่มีการกำหนดค่า HttpOnly flag ส่งผลให้คุกกี้นี้สามารถถูกเข้าถึงได้ผ่าน JavaScript หากมีการรันสคริปต์ที่เป็นอันตรายบนหน้านี้ คุกกี้ดังกล่าวจะสามารถถูกเข้าถึงและส่งไปยังเว็บไซต์อื่นได้ หากคุกกี้นี้เป็นคุกกี้เซสชัน มีโอกาสเกิดการโจมตีแบบ Session Hijacking ได้		
แนวทางแก้ไข	ตรวจสอบการตั้งค่า HttpOnly flag สำหรับคุกกี้ทุกตัว โดยการกำหนดแบบละเอียด		
ลำดับ	**10**		
รายการแจ้งเตือนช่องโหว่	Cookie Without Secure Flag		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	ไม่มี (ติดตามเป็นระยะ)
ผลกระทบ	มีการตั้งค่าคุกกี้โดยไม่มีการกำหนดค่า Secure flag ส่งผลให้คุกกี้นี้สามารถถูกเข้าถึงผ่านการเชื่อมต่อที่ไม่เข้ารหัสได้		
แนวทางแก้ไข	คุกกี้ที่มีข้อมูลสำคัญหรือเป็นโทเค็นเซสชันควรถูกส่งผ่านช่องทางที่เข้ารหัสเสมอ ดังนั้นควรตรวจสอบให้แน่ใจว่ามีการตั้งค่า Secure flag สำหรับคุกกี้ที่มีข้อมูลสำคัญ		
ลำดับ	**11**		
รายการแจ้งเตือนช่องโหว่	Cookie without SameSite Attribute		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	ไม่มี (ติดตามเป็นระยะ)
ผลกระทบ	การตั้งค่าคุกกี้โดยไม่มีการกำหนดค่า SameSite attribute ส่งผลให้คุกกี้นี้สามารถถูกส่งผ่านการร้องขอแบบ 'cross-site' ได้ SameSite attribute เป็นมาตรการที่มีประสิทธิภาพในการป้องกันการโจมตีแบบ Cross-Site Request Forgery (CSRF), Cross-Site Script Inclusion (XSSI) และ Timing Attacks		
แนวทางแก้ไข	ตรวจสอบการตั้งค่า SameSite attribute เป็น 'lax' หรือ 'strict' สำหรับคุกกี้ทุกตัว		

ลำดับ	**12**		
รายการแจ้งเตือนช่องโหว่	Cross-Domain JavaScript Source File Inclusion		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	ไม่มี (ติดตามเป็นระยะ)
ผลกระทบ	มีการรวมไฟล์สคริปต์จากโดเมนของ Third-party หรือจากโดเมนภายนอก		
แนวทางแก้ไข	ตรวจสอบให้แน่ใจว่าไฟล์ JavaScript ถูกโหลดจากแหล่งที่เชื่อถือได้เท่านั้น และแหล่งที่มานั้นไม่สามารถถูกควบคุมโดยผู้ใช้ปลายทางของแอปพลิเคชัน		
ลำดับ	**13**		
รายการแจ้งเตือนช่องโหว่	Information Disclosure - Debug Error Messages		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	ไม่มี (ติดตามเป็นระยะ)
ผลกระทบ	การตอบกลับดูเหมือนจะมีข้อความข้อผิดพลาดที่พบบ่อยจากแพลตฟอร์มต่าง ๆ เช่น ASP.NET และเว็บเซิร์ฟเวอร์ เช่น IIS และ Apache คุณสามารถกำหนดค่าเพื่อปรับแต่งรายการข้อความดีบักที่พบบ่อยเหล่านี้ได้ ปัญหาที่จะเจอมีดังนี้ **การเปิดเผยข้อมูลที่ละเอียดอ่อน การเปิดเผยช่องโหว่ การโจมตีแบบ Cross-site Scripting (XSS) และการโจมตีแบบ SQL Injection**		
แนวทางแก้ไข	ปิดการแสดงข้อความดีบักก่อนนำระบบขึ้น Production		
ลำดับ	**14**		
รายการแจ้งเตือนช่องโหว่	Private IP Disclosure		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	ไม่มี (ติดตามเป็นระยะ)
ผลกระทบ	พบ IP ส่วนตัวหรือชื่อโฮสต์ภายในของ Amazon EC2 (เช่น ip-10-0-56-78) ในเนื้อหาตอบกลับของ HTTP ข้อมูลนี้อาจมีประโยชน์ในการโจมตีระบบภายในเพิ่มเติม		
แนวทางแก้ไข	ลบที่อยู่ IP ส่วนตัวออกจากเนื้อหาตอบกลับของ HTTP สำหรับ Comments ควรใช้ Comments ในรูปแบบ JSP/ASP/PHP แทนที่จะใช้ Comments แบบ HTML/JavaScript ซึ่งสามารถมองเห็นได้จากเบราว์เซอร์ของผู้ใช้		
ลำดับ	**15**		
รายการแจ้งเตือนช่องโหว่	Secure Pages Include Mixed Content		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	ไม่มี (ติดตามเป็นระยะ)
ผลกระทบ	มีเนื้อหาผสม ซึ่งเป็นเนื้อหาที่ถูกเข้าถึงผ่าน HTTP แทนที่จะเป็น HTTPS		

แนวทางแก้ไข	พบหน้าที่สามารถเข้าถึงได้ผ่าน SSL/TLS จะต้องประกอบไปด้วยเนื้อหาทั้งหมดที่ถูกส่งผ่าน SSL/TLS เท่านั้น หน้าดังกล่าวไม่ควรมีเนื้อหาที่ถูกส่งผ่าน HTTP ที่ไม่ได้เข้ารหัส รวมถึงเนื้อหาจากเว็บไซต์ของบุคคลที่สามด้วย		
ลำดับ	**16**		
รายการแจ้งเตือนช่องโหว่	Strict-Transport-Security Header Not Set		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	**ไม่มี (ติดตามเป็นระยะ)**
ผลกระทบ	HTTP Strict Transport Security (HSTS) คือกลไกนโยบายความปลอดภัยของเว็บที่เซิร์ฟเวอร์เว็บประกาศว่า user agent (เช่น เว็บเบราว์เซอร์) จะต้องติดต่อกับเซิร์ฟเวอร์นั้นโดยใช้การเชื่อมต่อ HTTPS ที่ปลอดภัยเท่านั้น (คือ HTTP ที่ใช้ผ่าน TLS/SSL) HSTS เป็นโปรโตคอลที่กำหนดโดย IETF และระบุไว้ใน RFC 6797		
แนวทางแก้ไข	ตรวจสอบว่า web server, application server, load balancer และอื่นๆ ได้รับการตั้งค่าให้บังคับใช้ Strict-Transport-Security (HSTS)		
ลำดับ	**17**		
รายการแจ้งเตือนช่องโหว่	Timestamp Disclosure - Unix		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	**ไม่มี (ติดตามเป็นระยะ)**
ผลกระทบ	Application และ Web server ได้เปิดเผย timestamp - Unix		
แนวทางแก้ไข	ตรวจสอบเพื่อยืนยันว่า ข้อมูล timestamp ไม่ได้เป็นข้อมูลละเอียดอ่อน และข้อมูลดังกล่าวไม่สามารถถูกรวบรวมเพื่อเปิดเผยรูปแบบที่สามารถนำไปใช้โจมตีได้		
ลำดับ	**18**		
รายการแจ้งเตือนช่องโหว่	X-Content-Type-Options Header Missing		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	**ไม่มี (ติดตามเป็นระยะ)**
ผลกระทบ	ไม่ได้ตั้งค่า Anti-MIME-Sniffing header X-Content-Type-Options เป็น 'nosniff' ซึ่งอนุญาตให้เวอร์ชันเก่าของ Internet Explorer และ Chrome สามารถทำ MIME-sniffing บนเนื้อหาตอบกลับได้ ซึ่งอาจทำให้เนื้อหาตอบกลับถูกตีความและแสดงผลเป็นประเภทเนื้อหาที่แตกต่างจากประเภทเนื้อหาที่ประกาศไว้ ส่วน Firefox เวอร์ชันปัจจุบัน (ต้นปี 2014) และเวอร์ชันเก่าจะใช้ประเภทเนื้อหาที่ประกาศไว้ (ถ้ามีการตั้งค่า) แทนการทำ MIME-sniffing		

แนวทางแก้ไข	ตรวจสอบว่า Applicatiion และ Web server ตั้งค่า Content-Type header อย่างถูกต้อง และตั้งค่า X-Content-Type-Options header เป็น 'nosniff' สำหรับทุกหน้าเว็บ หากเป็นไปได้ ควรตรวจสอบให้แน่ใจว่าผู้ใช้ปลายทางใช้เว็บเบราว์เซอร์ที่เป็นไปตามมาตรฐานและทันสมัยที่ไม่ทำการ MIME-sniffing เลย หรือสามารถกำหนดให้แอปพลิเคชัน/เซิร์ฟเวอร์เว็บไม่ทำการ MIME-sniffing ได้		
ลำดับ	**19**		
รายการแจ้งเตือนช่องโหว่	Authentication Request Identified		
ระดับความเสี่ยง	Information	**ความเร่งด่วน**	**ไม่มี**
ผลกระทบ	คำขอที่ได้รับการระบุว่าเป็นคำขอการยืนยันตัวตน ฟิลด์ 'Other Info' ประกอบด้วยชุดของบรรทัด key=value ซึ่งใช้ระบุฟิลด์ที่เกี่ยวข้อง หากคำขอนั้นอยู่ในบริบทที่ตั้งค่า "Authentication Method" เป็น "Auto-Detect" ด้วยเงื่อนไขนี้จะทำการเปลี่ยนแปลงวิธีการยืนยันตัวตนให้ตรงกับคำขอที่ระบุ		
แนวทางแก้ไข	แจ้งเป็นข้อมูล ไม่มีช่องโหว่		
ลำดับ	**20**		
รายการแจ้งเตือนช่องโหว่	Content-Type Header Missing		
ระดับความเสี่ยง	Information	**ความเร่งด่วน**	**ไม่มี**
ผลกระทบ			
แนวทางแก้ไข			
ลำดับ	**21**		
รายการแจ้งเตือนช่องโหว่	Information Disclosure - Suspicious Comments		
ระดับความเสี่ยง	Information	**ความเร่งด่วน**	**ไม่มี**
ผลกระทบ	การตอบสนองดูเหมือนจะมีความคิดเห็นที่น่าสงสัย ซึ่งอาจช่วยผู้โจมตีได้ หมายเหตุ: การจับคู่ที่เกิดขึ้นภายในบล็อกสคริปต์หรือไฟล์จะพิจารณาทั้งเนื้อหาทั้งหมดไม่ใช่แค่ความคิดเห็นเท่านั้น		
แนวทางแก้ไข	ลบ Comment ทั้งหมดที่เป็นข้อมูลที่ช่วยผู้โจมตี และแก้ไขปัญหาที่เกี่ยวข้องที่ Comment เหล่านั้นอ้างถึง		

ลำดับ	**22**		
รายการแจ้งเตือนช่องโหว่	Modern Web Application		
ระดับความเสี่ยง	Information	**ความเร่งด่วน**	**ไม่มี**
ผลกระทบ	แอปพลิเคชันเป็นแอปพลิเคชันเว็บที่ทันสมัย หากคุณต้องการสำรวจมันโดยอัตโนมัติแล้ว Ajax Spider อาจจะมีประสิทธิภาพมากกว่าการใช้ตัวสไปเดอร์มาตรฐาน		
แนวทางแก้ไข	แจ้งเป็นข้อมูล ไม่มีช่องโหว่		
ลำดับ	**23**		
รายการแจ้งเตือนช่องโหว่	Re-examine Cache-control Directives		
ระดับความเสี่ยง	Information	**ความเร่งด่วน**	**ไม่มี**
ผลกระทบ	ไม่มีการตั้งค่า cache-control header อย่างถูกต้องหรือขาดหายไป ซึ่งอนุญาตให้เบราว์เซอร์และพร็อกซี่ทำการแคชเนื้อหา สำหรับไฟล์ที่เป็นสแตติก เช่น css, js หรือไฟล์ภาพอาจเป็นสิ่งที่ต้องการ แต่ควรตรวจสอบทรัพยากรเหล่านี้เพื่อให้มั่นใจว่าไม่มีข้อมูลที่เป็นความลับถูกแคช		
แนวทางแก้ไข	สำหรับเนื้อหาที่มีความปลอดภัย ควรตรวจสอบให้แน่ใจว่า HTTP header cache-control ถูกตั้งค่าเป็น "no-cache, no-store, must-revalidate" หากเป็นทรัพยากรที่ควรถูกแคช ควรพิจารณาตั้งค่ากำหนด "public, max-age, immutable"		
ลำดับ	**24**		
รายการแจ้งเตือนช่องโหว่	Session Management Response Identified		
ระดับความเสี่ยง	Information	**ความเร่งด่วน**	**ไม่มี**
ผลกระทบ	การตอบสนองที่ให้มาถูกระบุว่ามีการจัดการเซสชันของโทเค็น ฟิลด์ 'Other Info' ประกอบด้วยชุดของโทเค็นเฮดเดอร์ที่สามารถใช้ในวิธีการจัดการเซสชันแบบ Header Based หากคำขออยู่ในบริบทที่ตั้งค่า "Session Management Method" เป็น "Auto-Detect" กฎนี้จะทำการเปลี่ยนแปลงการจัดการเซสชันให้ใช้โทเค็นที่ระบุ		
แนวทางแก้ไข	แจ้งเป็นข้อมูล ไม่มีช่องโหว่		
ลำดับ	**25**		
รายการแจ้งเตือนช่องโหว่	User Controllable HTML Element Attribute (Potential XSS)		

ระดับความเสี่ยง	Information	**ความเร่งด่วน**	**ไม่มี**
ผลกระทบ	การตรวจสอบนี้จะพิจารณาข้อมูลที่ผู้ใช้ป้อนในพารามิเตอร์ของ query string และข้อมูล POST เพื่อระบุจุดที่ค่าของแอตทริบิวต์ HTML อาจถูกควบคุม ซึ่งช่วยในการตรวจจับจุดเสี่ยงสำหรับ XSS (cross-site scripting) ที่จะต้องการการตรวจสอบเพิ่มเติมโดยนักวิเคราะห์ความปลอดภัยเพื่อประเมินความเสี่ยงในการโจมตี		
แนวทางแก้ไข	ตรวจสอบความถูกต้องของข้อมูลที่ป้อนเข้ามาทุกครั้ง ก่อนที่จะเขียนลงในแอตทริบิวต์ HTML		
ลำดับ	**26**		
รายการแจ้งเตือนช่องโหว่	Vulnerable JS Library		
ระดับความเสี่ยง	Information	**ความเร่งด่วน**	**ไม่มี**
ผลกระทบ	library bootstrap มีช่องโหว่		
แนวทางแก้ไข	ดำเนินการ Upgrade Bootstrap เป็นเวอร์ชันล่าสุด		

2. เว็บแอปพลิเคชัน B (Web App B)

ลำดับ	**1**		
รายการแจ้งเตือนช่องโหว่	Absence of Anti-CSRF Tokens		
ระดับความเสี่ยง	Medium	**ความเร่งด่วน**	**ภายใน 3 – 6 เดือน**
ผลกระทบ	ไม่พบ Anti-CSRF tokens ในฟอร์มส่งข้อมูล HTML CSRF เป็นช่องโหว่ที่ Attakcer ส่ง HTML หรือ JavaScript ให้ Web browser ของเหยื่อส่ง HTTP request เพื่อไปกระทำการบางอย่างที่เป็นอันตรายต่อผู้ใช้งาน หลักการของ CSRF เป็นตัวอย่างดังรูป		
แนวทางแก้ไข	1. ตรวจสอบให้แน่ใจว่าแอปพลิเคชันของคุณไม่มีปัญหา Cross-Site Scripting (XSS) เนื่องจากการป้องกัน CSRF ส่วนใหญ่สามารถถูกเลี่ยงผ่านด้วยสคริปต์ที่ควบคุมโดยผู้โจมตี 2. หลีกเลี่ยงการใช้วิธี GET สำหรับคำขอใด ๆ ที่กระตุ้นให้เกิดการเปลี่ยนแปลงสถานะของระบบ 3. ตรวจสอบ HTTP Referer Header เพื่อยืนยันว่าคำขอมีต้นทางมาจากหน้าเว็บ		

ลำดับ	**2**		
รายการแจ้งเตือนช่องโหว่	Content Security Policy (CSP) Header Not Set		
ระดับความเสี่ยง	Medium	**ความเร่งด่วน**	**ภายใน 3 – 6 เดือน**
ผลกระทบ	Content Security Policy (CSP) เป็นชั้นความปลอดภัยเพิ่มเติมที่ช่วยตรวจจับและลดความเสี่ยงจากการโจมตีบางประเภท เช่น Cross-Site Scripting (XSS) และ Data Injection การโจมตีเหล่านี้มักถูกใช้เพื่อขโมยข้อมูล เปลี่ยนแปลงหน้าตาเว็บไซต์ หรือแจกจ่ายมัลแวร์ CSP ทำงานโดยการกำหนดชุดของ HTTP Headers มาตรฐาน ที่ช่วยให้เจ้าของเว็บไซต์สามารถระบุแหล่งที่มาของเนื้อหาที่ได้รับอนุญาตให้เบราว์เซอร์โหลดได้บนหน้าเว็บนั้น โดยประเภทเนื้อหาที่ครอบคลุมได้แก่ JavaScript CSS HTML frames ฟอนต์ (Fonts) รูปภาพ (Images) วัตถุฝังตัว (Embeddable Objects) เช่น Java Applets, ActiveX, ไฟล์เสียง (Audio), และวิดีโอ (Video) CSP ช่วยลดความเสี่ยงจากการโหลดเนื้อหาที่ไม่ได้รับอนุญาต ซึ่งอาจเป็นอันตรายต่อเว็บไซต์และผู้ใช้		
แนวทางแก้ไข	ดำเนินการกำหนด Content-Security-Policy (CSP) ให้ชุดของ HTTP Header อาทิ 1) Web Server 2) Web Application Server 3) Load Balancer และ 4) อื่นๆ		
ลำดับ	**3**		
รายการแจ้งเตือนช่องโหว่	Cookie Without Secure Flag		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	**ไม่มี (ติดตามเป็นระยะ)**
ผลกระทบ	คุกกี้ถูกตั้งค่าโดยไม่มี Secure Flag ซึ่งหมายความว่าคุกกี้สามารถถูกเข้าถึงได้ผ่านการเชื่อมต่อที่ไม่เข้ารหัส (เช่น HTTP)		
แนวทางแก้ไข	1. ควรส่งผ่านช่องทางที่เข้ารหัสเสมอ 2. ต้องตั้งค่า secure flag สำหรับคุกกี้ที่มีข้อมูลสำคัญ		
ลำดับ	**4**		
รายการแจ้งเตือนช่องโหว่	Server Leaks Version Information via "Server" HTTP Response Header Field		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	**ไม่มี (ติดตามเป็นระยะ)**
ผลกระทบ	เซิร์ฟเวอร์เว็บ/แอปพลิเคชันกำลังรั่วไหลข้อมูลเวอร์ชันผ่าน "Server" HTTP response header การเข้าถึงข้อมูลดังกล่าวอาจช่วยให้นักโจมตีสามารถระบุช่องโหว่อื่นๆ ที่เซิร์ฟเวอร์เว็บ/แอปพลิเคชันของคุณอาจเผชิญ		

แนวทางแก้ไข	ตรวจสอบการตั้งค่าให้ปิดการแสดง "Server" header หรือให้ข้อมูลทั่วไปที่ไม่ระบุตัวตนเฉพาะเจาะจง เซิร์ฟเวอร์เว็บ, เซิร์ฟเวอร์แอปพลิเคชัน, โหลดบาลานเซอร์ ฯลฯ		
ลำดับ	**5**		
รายการแจ้งเตือนช่องโหว่	Strict-Transport-Security Header Not Set		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	**ไม่มี (ติดตามเป็นระยะ)**
ผลกระทบ	การส่งข้อมูลที่สำคัญหรือข้อมูลที่เกี่ยวข้องกับความปลอดภัยในรูปแบบข้อความที่ไม่เข้ารหัสผ่านช่องทางการสื่อสารที่สามารถถูกดักจับโดยผู้ที่ไม่ได้รับอนุญาต		
แนวทางแก้ไข	กำหนดค่าเพื่อบังคับใช้นโยบาย Strict-Transport-Security ที่ Web Server, Web Application Server และ Load Balancer		
ลำดับ	**6**		
รายการแจ้งเตือนช่องโหว่	X-AspNet-Version Response Header		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	**ไม่มี (ติดตามเป็นระยะ)**
ผลกระทบ	ภัยคุกคามจากการที่เซิร์ฟเวอร์รั่วไหลข้อมูลผ่านฟิลด์ HTTP response header "X-AspNet-Version" หรือ "X-AspNetMvc-Version" คือ การที่ผู้โจมตีสามารถทราบข้อมูลเกี่ยวกับเวอร์ชันของ ASP.NET หรือ ASP.NET MVC ที่เซิร์ฟเวอร์กำลังใช้งาน ซึ่งส่งผลกระทบดังนี้ ค้นหาช่องโหว่: เมื่อรู้เวอร์ชันของเซิร์ฟเวอร์หรือเฟรมเวิร์กที่ใช้ ผู้โจมตีสามารถค้นหาช่องโหว่ที่อาจมีในเวอร์ชันนั้น ๆ ได้จากฐานข้อมูลช่องโหว่ต่าง ๆ กำหนดกลยุทธ์การโจมตี: ผู้โจมตีสามารถวางแผนการโจมตีที่เฉพาะเจาะจงและมีประสิทธิภาพมากขึ้นโดยอิงจากข้อมูลเวอร์ชันที่ได้ เพิ่มความเสี่ยง: การเปิดเผยข้อมูลเวอร์ชันอาจทำให้การป้องกันจากการโจมตีลดลง เนื่องจากผู้โจมตีสามารถใช้เครื่องมือที่มีอยู่แล้วเพื่อโจมตีได้ง่ายขึ้น		
แนวทางแก้ไข	กำหนดค่าเซิร์ฟเวอร์เพื่อไม่ให้ส่งคืน HTTP headers		
ลำดับ	**7**		
รายการแจ้งเตือนช่องโหว่	X-Content-Type-Options Header Missing		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	**ไม่มี (ติดตามเป็นระยะ)**
ผลกระทบ	หัวข้อ Anti-MIME-Sniffing X-Content-Type-Options ไม่ได้ตั้งค่าเป็น 'nosniff' ซึ่งทำให้เวอร์ชันเก่าของ Internet Explorer และ Chrome สามารถทำการ MIME-sniffing บนเนื้อหาของการตอบสนองได้ ซึ่งอาจทำ		

	ให้เนื้อหาถูกตีความและแสดงผลเป็นประเภทเนื้อหาที่แตกต่างจากประเภทเนื้อหาที่ประกาศไว้ ส่วนเวอร์ชันปัจจุบัน (ต้นปี 2014) และเวอร์ชันเก่าของ Firefox จะใช้ประเภทเนื้อหาที่ประกาศ (หากมีการตั้งค่า) แทนที่จะทำการ MIME-sniffing.		
แนวทางแก้ไข	ตั้งค่า Content-Type header อย่างเหมาะสม และตั้งค่า X-Content-Type-Options header เป็น 'nosniff' สำหรับทุกหน้าเว็บ หากเป็นไปได้ ให้แน่ใจว่าผู้ใช้ปลายทางใช้เว็บเบราว์เซอร์ที่เป็นไปตามมาตรฐานและทันสมัยซึ่งไม่ทำการ MIME-sniffing เลย หรือสามารถกำหนดโดยแอปพลิเคชัน/เซิร์ฟเวอร์เว็บเพื่อไม่ให้ทำการ MIME-sniffing.		
ลำดับ	**8**		
รายการแจ้งเตือนช่องโหว่	Information Disclosure - Suspicious Comments		
ระดับความเสี่ยง	Information	**ความเร่งด่วน**	**ไม่มี**
ผลกระทบ	1. Comment ในโค๊ดอาจเป็นข้อมูลให้สามารถถูกโจมตีจากผู้ไม่ประสงค์ดีได้ 2. พบคำว่า SELECT อาจเป็นข้อมูลของโค้ดที่กำลังจัดการกับคำสั่ง SQL โดยตรง ซึ่งอาจเสี่ยงต่อ SQL Injection หากไม่ได้มีการป้องกันข้อมูลนำเข้าที่ดี		
แนวทางแก้ไข	1. ดำเนินการลบ Comment ทั้งหมดในโค๊ดออก 2. แก้ไขปัญหาพื้นฐาน ที่ความคิดเห็นดังกล่าวอ้างอิงถึง เช่น การป้องกัน SQL Injection หรือการจัดการข้อมูลนำเข้าอย่างปลอดภัย		
ลำดับ	**9**		
รายการแจ้งเตือนช่องโหว่	Re-examine Cache-control Directives		
ระดับความเสี่ยง	Information	**ความเร่งด่วน**	**ไม่มี**
ผลกระทบ	Cache-Control Header ไม่ถูกตั้งค่าอย่างเหมาะสมหรือขาดหายไป อาจทำให้เบราว์เซอร์หรือพร็อกซีเก็บข้อมูลในแคชโดยไม่ได้ตั้งใจ สำหรับทรัพยากรที่อ่อนไหว เช่น เนื้อหาแบบ dynamic หรือข้อมูลส่วนตัวของผู้ใช้ การเก็บข้อมูลในแคชอาจทำให้เกิดช่องโหว่ เช่น ข้อมูลรั่วไหล (Data Leakage) เนื้อหาส่วนตัวอาจถูกแสดงให้ผู้ใช้ที่ไม่เกี่ยวข้อง แสดงข้อมูลเก่า การเปลี่ยนแปลงข้อมูลในเซิร์ฟเวอร์อาจไม่ถูกอัปเดตทันทีบนฝั่งผู้ใช้สำหรับ Static Assets เช่น CSS, JS หรือไฟล์ภาพ บางครั้งตั้งใจอนุญาตให้แคชเพื่อปรับปรุงประสิทธิภาพการโหลดเว็บไซต์ แต่ควรตรวจสอบว่าไม่มีเนื้อหาที่อ่อนไหวถูกรวมอยู่ในไฟล์		

แนวทางแก้ไข	1. สำหรับเนื้อหาที่ต้องการความปลอดภัย ให้ตั้งค่า HTTP header ของ Cache-Control เป็น "no-cache, no-store, must-revalidate" 2. ทรัพยากรที่สามารถแคชได้ ควรตั้งค่า directives เป็น "public, max-age, immutable"		
ลำดับ	**10**		
รายการแจ้งเตือนช่องโหว่	User Controllable HTML Element Attribute (Potential XSS)		
ระดับความเสี่ยง	Information	**ความเร่งด่วน**	**ไม่มี**
ผลกระทบ	ผู้โจมตีสามารถใช้ช่องโหว่นี้เพื่อแทรกสคริปต์ที่เป็นอันตราย และโจมตีผู้ใช้งานระบบ เช่น ขโมยข้อมูลคุกกี้, Session ID หรือดำเนินการโดยไม่ได้รับอนุญาตในนามของผู้ใช้งาน		
แนวทางแก้ไข	1. Validate Input ตรวจสอบข้อมูลที่ผู้ใช้งานส่งเข้ามาให้เป็นไปตามรูปแบบที่กำหนด 2. Sanitize Output กำจัดหรือแปลงข้อมูลที่อาจเป็นอันตรายก่อนนำไปใช้งานใน HTML attributes 3. ใช้ฟังก์ชันการป้องกัน ใช้ไลบรารีหรือฟังก์ชันที่มีความปลอดภัย เช่น การเข้ารหัส HTML (HTML Encoding) เพื่อลดความเสี่ยง		

3. เว็บแอปพลิเคชัน C (Web App C)

ลำดับ	**1**		
รายการแจ้งเตือนช่องโหว่	Content Security Policy (CSP) Header Not Set		
ระดับความเสี่ยง	Medium	**ความเร่งด่วน**	**ภายใน 3 – 6 เดือน**
ผลกระทบ	โอกาสที่ผู้โจมตีจะหลีกเลี่ยงกลไกการป้องกัน (Bypass Protection Mechanism) ได้ รวมถึงการโจมตีแบบ Cross-Site Scripting (XSS) โดยการกำหนดแหล่งที่มาของเนื้อหาที่เบราว์เซอร์สามารถโหลดได้ และและการโจมตีด้วยการแทรกข้อมูล (Data Injection) การโจมตีเหล่านี้สามารถนำไปสู่การขโมยข้อมูล การเปลี่ยนแปลงหน้าเว็บไซต์ หรือการกระจายมัลแวร์		
แนวทางแก้ไข	ดำเนินการกำหนด Content-Security-Policy (CSP) ให้ชุดของ HTTP Header อาทิ 1) Web Server 2) Web Application Server 3) Load Balancer และ 4. อื่นๆ		

ลำดับ	**2**		
รายการแจ้งเตือนช่องโหว่	Missing Anti-clickjacking Header		
ระดับความเสี่ยง	Medium	**ความเร่งด่วน**	**ภายใน 3 – 6 เดือน**
ผลกระทบ	**ไม่มีการป้องกันการโจมตีประเภท ClickJacking ควรมีการตั้งค่า Content-Security-Policy ที่ประกอบด้วยคำสั่ง 'frame-ancestors' หรือ X-Frame-Options เพื่อเสริมการป้องกันดังกล่าว**		
แนวทางแก้ไข	ดำเนินการตั้งค่า Content-Security-Policy พร้อมคำสั่ง 'frame-ancestors' directive หรือใช้ X-Frame-Options เพื่อป้องกัน		
ลำดับ	**3**		
รายการแจ้งเตือนช่องโหว่	Vulnerable JS Library		
ระดับความเสี่ยง	Medium	**ความเร่งด่วน**	**ภายใน 3 – 6 เดือน**
ผลกระทบ	1. การใช้ Bootstrap เวอร์ชั่นเก่า ทำให้ผู้ใช้งานเสี่ยงต่อการถูกโจมตีแบบ Cross-Site Scripting (XSS) โดยช่องโหว่นี้เกิดขึ้นในส่วนประกอบของ carousel ซึ่งสามารถถูกโจมตีผ่านแอตทริบิวต์ data-slide และ data-slide-to ของแท็ก <a> ที่ใช้ href โดยไม่มีการกรองข้อมูลอย่างเหมาะสม ช่องโหว่นี้อาจทำให้ผู้โจมตีสามารถรันโค้ด JavaScript ที่เป็นอันตรายภายในเบราว์เซอร์ของเหยื่อได้ 2. การใช้ jQuery เวอร์ชันเก่า การส่ง HTML ที่มี <option> จากแหล่งที่ไม่น่าเชื่อถือ โดยผ่านการกรองข้อมูลแล้ว ไปยังเมธอดจัดการ DOM ของ jQuery (เช่น .html(), .append() และอื่น ๆ) ยังคงเสี่ยงต่อการถูกรันโค้ดที่ไม่น่าเชื่อถือได้		
แนวทางแก้ไข	1. ดำเนินการ Upgrade bootstrap ให้เป็นเวอร์ชันล่าสุด 2. ดำเนินการ Upgrade jquery ให้เป็นเวอร์ชันล่าสุด		
ลำดับ	**4**		
รายการแจ้งเตือนช่องโหว่	Application Error Disclosure		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	**ไม่มี (ติดตามเป็นระยะ)**
ผลกระทบ	มีแสดงข้อความข้อผิดพลาด และคำเตือนที่อาจเปิดเผยข้อมูลสำคัญ เช่น ตำแหน่งไฟล์ที่ทำให้เกิดข้อยกเว้นที่ไม่ได้รับการจัดการ ข้อมูลนี้อาจถูกใช้เพื่อดำเนินการโจมตีเพิ่มเติมต่อเว็บแอปพลิเคชัน อย่างไรก็ตาม การแจ้งเตือนนี้อาจเป็นผลบวกเท็จ (False Positive) หากข้อความข้อผิดพลาดปรากฏในหน้าคู่มือหรือเอกสารประกอบการใช้งาน		

แนวทางแก้ไข	ตรวจสอบซอร์สโค้ด และสร้างหน้าแสดงข้อผิดพลาดที่กำหนดเอง ควรพิจารณาใช้รหัสอ้างอิง หรือตัวระบุข้อผิดพลาดเฉพาะสำหรับฝั่งผู้ใช้งาน (เบราว์เซอร์) พร้อมทั้งบันทึกรายละเอียดของข้อผิดพลาดไว้ที่ฝั่งเซิร์ฟเวอร์โดยไม่เปิดเผยข้อมูลเหล่านั้นให้กับผู้ใช้งาน		
ลำดับ	**5**		
รายการแจ้งเตือนช่องโหว่	Application Error Disclosure		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	**ไม่มี (ติดตามเป็นระยะ)**
ผลกระทบ	มีแสดงข้อความข้อผิดพลาด และคำเตือนที่อาจเปิดเผยข้อมูลสำคัญ เช่น ตำแหน่งไฟล์ที่ทำให้เกิดข้อยกเว้นที่ไม่ได้รับการจัดการ ข้อมูลนี้อาจถูกใช้เพื่อดำเนินการโจมตีเพิ่มเติมต่อเว็บแอปพลิเคชัน อย่างไรก็ตาม การแจ้งเตือนนี้อาจเป็นผลบวกเท็จ (False Positive) หากข้อความข้อผิดพลาดปรากฏในหน้าคู่มือหรือเอกสารประกอบการใช้งาน		
แนวทางแก้ไข	ตรวจสอบซอร์สโค้ด และสร้างหน้าแสดงข้อผิดพลาดที่กำหนดเอง ควรพิจารณาใช้รหัสอ้างอิง หรือตัวระบุข้อผิดพลาดเฉพาะสำหรับฝั่งผู้ใช้งาน (เบราว์เซอร์) พร้อมทั้งบันทึกรายละเอียดของข้อผิดพลาดไว้ที่ฝั่งเซิร์ฟเวอร์โดยไม่เปิดเผยข้อมูลเหล่านั้นให้กับผู้ใช้งาน		
ลำดับ	**6**		
รายการแจ้งเตือนช่องโหว่	Big Redirect Detected (Potential Sensitive Information Leak)		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	**ไม่มี (ติดตามเป็นระยะ)**
ผลกระทบ	พบว่ามีการตั้งค่า cookie โดยไม่มีการกำหนดค่า HttpOnly flag ซึ่งหมายความว่า cookie สามารถถูกเข้าถึงได้ผ่าน JavaScript หากมีการรันสคริปต์ที่เป็นอันตรายบนหน้านี้ cookie จะสามารถถูกเข้าถึงและส่งไปยังเว็บไซต์อื่นได้ หาก cookie ดังกล่าวเป็น session cookie อาจนำไปสู่การโจมตีแบบ session hijacking ได้		
แนวทางแก้ไข	ตรวจสอบให้แน่ใจว่าได้ตั้งค่า HttpOnly flag สำหรับทุก cookie แล้ว		
ลำดับ	**7**		
รายการแจ้งเตือนช่องโหว่	Cookie Without Secure Flag		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	**ไม่มี (ติดตามเป็นระยะ)**

ผลกระทบ	ไม่มีการตั้งค่า Secure flag สำหรับ cookie อาจทำให้ข้อมูลใน cookie ถูกส่งผ่านการเชื่อมต่อที่ไม่เข้ารหัส (เช่น HTTP แทนที่จะเป็น HTTPS) ซึ่งทำให้ข้อมูลสามารถถูกดักจับได้โดยผู้โจมตีที่อยู่ในเครือข่ายเดียวกัน (Man-in-the-Middle attack) ส่งผลให้ข้อมูลใน cookie อาจถูกขโมยหรือถูกแก้ไขได้ ซึ่งอาจทำให้เกิดการโจมตีเช่น session hijacking หรือการแอบอ้างตัวตนของผู้ใช้		
แนวทางแก้ไข	ตรวจสอบให้แน่ใจว่าได้ตั้งค่า Secure flag สำหรับ cookie ที่มีข้อมูลสำคัญเหล่านั้น กรณีที่ cookie มีข้อมูลที่สำคัญหรือเป็น session token ควรส่งข้อมูลเหล่านั้นผ่านช่องทางที่เข้ารหัสเท่านั้น		
ลำดับ	**8**		
รายการแจ้งเตือนช่องโหว่	Cookie without SameSite Attribute		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	**ไม่มี (ติดตามเป็นระยะ)**
ผลกระทบ	การตั้งค่า cookie ไม่มีการกำหนดค่า SameSite attribute ส่งผลให้ cookie สามารถถูกส่งเป็นผลลัพธ์จากการร้องขอข้ามเว็บไซต์ (cross-site request) การตั้งค่า SameSite attribute เป็นมาตรการป้องกันที่มีประสิทธิภาพต่อการโจมตีแบบ Cross-Site Request Forgery (CSRF), Cross-Site Script Inclusion (XSSI), และการโจมตีแบบ Timing Attacks		
แนวทางแก้ไข	ตรวจสอบให้แน่ใจว่าได้ตั้งค่า SameSite attribute เป็น 'lax' หรือ 'strict' สำหรับทุก cookie		
ลำดับ	**9**		
รายการแจ้งเตือนช่องโหว่	Cross-Domain JavaScript Source File Inclusion		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	**ไม่มี (ติดตามเป็นระยะ)**
ผลกระทบ	มีการใช้งานไฟล์สคริปต์จากโดเมนภายนอกซึ่งส่งผลให้มีโอกาสถูกโจมตีดังนี้ 1. Cross-Site Scripting (XSS): หากไฟล์สคริปต์จากแหล่งที่ไม่น่าเชื่อถือมีช่องโหว่หรือเป็นอันตราย อาจทำให้ผู้โจมตีสามารถรันโค้ด JavaScript ที่เป็นอันตรายในเบราว์เซอร์ของผู้ใช้ได้ 2. ขโมยข้อมูล: สคริปต์ที่ไม่ปลอดภัยอาจเข้าถึงข้อมูลสำคัญ เช่น คุกกี้ของผู้ใช้ หรือข้อมูลการเข้าสู่ระบบ 3. การปลอมแปลงข้อมูล: หากสคริปต์จากแหล่งที่ไม่น่าเชื่อถือถูกปลอมแปลงหรือแก้ไขระหว่างการส่งข้อมูล อาจทำให้มีการเปลี่ยนแปลงข้อมูลสำคัญ เช่น ข้อมูลฟอร์มที่ผู้ใช้กรอก		

	4. การเปิดเผยข้อมูล: ฟังก์ชันจากโดเมนภายนอกอาจมีช่องโหว่ที่สามารถเปิดเผยข้อมูลที่ไม่ควรเปิดเผย เช่น ข้อมูลส่วนตัวของผู้ใช้หรือข้อมูลทางธุรกิจ 5. Man-in-the-Middle (MITM): หากการเชื่อมต่อไม่ปลอดภัย (ไม่ใช้ HTTPS) ข้อมูลที่ส่งระหว่างเว็บไซต์และโดเมนภายนอกอาจถูกดักจับหรือแก้ไขได้		
แนวทางแก้ไข	ตรวจสอบ JavaScript ว่าถูกโหลดจากแหล่งที่เชื่อถือได้เท่านั้น และแหล่งที่มาของไฟล์เหล่านั้นไม่สามารถถูกควบคุมโดยผู้ใช้ปลายทางของแอปพลิเคชัน		
ลำดับ	**10**		
รายการแจ้งเตือนช่องโหว่	Strict-Transport-Security Header Not Set		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	**ไม่มี (ติดตามเป็นระยะ)**
ผลกระทบ	HTTP Strict Transport Security (HSTS) คือ กลไกนโยบายความปลอดภัยของเว็บที่เซิร์ฟเวอร์เว็บประกาศว่าให้โปรแกรมที่ใช้งาน (เช่น เว็บเบราว์เซอร์) ติดต่อกับเซิร์ฟเวอร์นั้นโดยใช้การเชื่อมต่อ HTTPS ที่ปลอดภัยเท่านั้น (คือ HTTP ที่ใช้การเข้ารหัส TLS/SSL) HSTS เป็นโปรโตคอลที่อยู่ในมาตรฐานของ IETF และระบุไว้ใน RFC 6797		
แนวทางแก้ไข	กำหนดค่าบังคับใช้ Strict-Transport-Security กับ ซิร์ฟเวอร์เว็บ, เซิร์ฟเวอร์แอปพลิเคชัน, ตัวบาลานซ์โหลด และอื่นๆ		
ลำดับ	**11**		
รายการแจ้งเตือนช่องโหว่	X-Content-Type-Options Header Missing		
ระดับความเสี่ยง	Low	**ความเร่งด่วน**	**ไม่มี (ติดตามเป็นระยะ)**
ผลกระทบ	ไม่ได้ตั้งค่า Anti-MIME-Sniffing header X-Content-Type-Options เป็นค่า nosniff ซึ่งทำให้อินเทอร์เน็ตเบราว์เซอร์รุ่นเก่า เช่น Internet Explorer และ Chrome สามารถทำ MIME-sniffing บนเนื้อหาของการตอบกลับได้ ส่งผลให้เนื้อหาอาจถูกตีความและแสดงผลเป็นประเภทเนื้อหาอื่นที่แตกต่างจากประเภทที่ระบุไว้ สำหรับ Firefox (ทั้งเวอร์ชันปัจจุบันในช่วงต้นปี 2014 และเวอร์ชันเก่า) จะใช้ประเภทเนื้อหาที่ระบุไว้ (หากตั้งค่าไว้) แทนการทำ MIME-sniffing		
แนวทางแก้ไข	ตรวจสอบให้แน่ใจว่าแอปพลิเคชันหรือเซิร์ฟเวอร์เว็บตั้งค่า Content-Type header อย่างเหมาะสม และตั้งค่า X-Content-Type-Options header เป็น nosniff สำหรับทุกหน้าเว็บ และควรให้ผู้ใช้งานใช้เว็บเบราว์เซอร์ที่เป็นไปตามมาตรฐานและทันสมัย		

ลำดับ	**12**		
รายการแจ้งเตือนช่องโหว่	Information Disclosure - Suspicious Comments		
ระดับความเสี่ยง	Information	**ความเร่งด่วน**	**ไม่มี**
ผลกระทบ	การตอบกลับจากเว็บเพจนี้มีความคิดเห็น (comments) ที่น่าสงสัย ซึ่งอาจช่วยให้ผู้โจมตีใช้เป็นข้อมูลในการโจมตีเพิ่มเติมได้ ตัวอย่างเช่น การแสดงข้อมูลเกี่ยวกับโค้ดหรือฟังก์ชันที่ไม่ควรเปิดเผย		
แนวทางแก้ไข	1. ลบความคิดเห็นทั้งหมดที่อาจเผยข้อมูลที่เป็นประโยชน์ต่อผู้โจมตี 2. ตรวจสอบและแก้ไขปัญหาที่ซ่อนอยู่ในโค้ดที่ความคิดเห็นเหล่านั้นอ้างถึง		
ลำดับ	**13**		
รายการแจ้งเตือนช่องโหว่	Modern Web Application		
ระดับความเสี่ยง	Information	**ความเร่งด่วน**	**ไม่มี**
ผลกระทบ	Header cache-control ถูกตั้งค่าไม่ถูกต้องหรือไม่มีการตั้งค่าเลย ทำให้เบราว์เซอร์และพร็อกซีสามารถแคชเนื้อหาได้ สำหรับไฟล์แบบสแตติก เช่น CSS, JavaScript หรือรูปภาพ อาจเป็นสิ่งที่ตั้งใจไว้ อย่างไรก็ตาม		
แนวทางแก้ไข	ควรตรวจสอบทรัพยากรเหล่านั้นเพื่อให้แน่ใจว่าไม่มีเนื้อหาที่เป็นความลับ สำหรับเนื้อหาที่ต้องการความปลอดภัย ให้ตั้งค่า HTTP header cache-control เป็น "no-cache, no-store, must-revalidate" หากเป็นทรัพยากรที่ต้องการให้แคชได้ ให้พิจารณาตั้งค่า directive เป็น "public, max-age, immutable"		
ลำดับ	**14**		
รายการแจ้งเตือนช่องโหว่	Re-examine Cache-control Directives		
ระดับความเสี่ยง	Information	**ความเร่งด่วน**	**ไม่มี**
ผลกระทบ	-		
แนวทางแก้ไข	ข้อมูลประกอบ		
ลำดับ	**15**		
รายการแจ้งเตือนช่องโหว่	Session Management Response Identified		
ระดับความเสี่ยง	Information	**ความเร่งด่วน**	**ไม่มี**

ผลกระทบ	การตอบกลับที่ให้มาถูกระบุว่ามีโทเค็นการจัดการเซสชันอยู่ ในช่อง 'Other Info' มีชุดโทเค็นของ header ที่สามารถใช้ในวิธีการจัดการเซสชันแบบ Header Based ได้ หากคำขออยู่ในบริบทที่มีการตั้งค่าวิธีการจัดการเซสชันเป็น "Auto-Detect" กฎนี้จะเปลี่ยนวิธีการจัดการเซสชันให้ใช้โทเค็นที่ระบุไว้แทน		
แนวทางแก้ไข	คำเตือน		
ลำดับ	**16**		
รายการแจ้งเตือนช่องโหว่	User Controllable HTML Element Attribute (Potential XSS)		
ระดับความเสี่ยง	Information	**ความเร่งด่วน**	**ไม่มี**
ผลกระทบ	การตรวจสอบนี้จะดูที่ข้อมูลที่ผู้ใช้ส่งผ่านพารามิเตอร์ในสตริงคำถามและข้อมูล POST เพื่อตรวจสอบว่าในบางค่าคุณลักษณะของ HTML อาจถูกควบคุมได้อย่างไร ซึ่งช่วยในการตรวจจับจุดเสี่ยงสำหรับ XSS (Cross-Site Scripting) ที่จำเป็นต้องมีการตรวจสอบเพิ่มเติมโดยนักวิเคราะห์ความปลอดภัยเพื่อประเมินความสามารถในการถูกโจมตี		
แนวทางแก้ไข	ตรวจสอบข้อมูลที่รับเข้ามาทุกครั้ง		
ลำดับ	**17**		
รายการแจ้งเตือนช่องโหว่	Vulnerable JS Library		
ระดับความเสี่ยง	Information	**ความเร่งด่วน**	**ไม่มี**
ผลกระทบ	jquery และ select2 เวอร์ชั่นเก่ามีโอกาสถูกโจมตีได้เนื่องจากมีช่องโหว่		
แนวทางแก้ไข	ดำเนินการ Upgrade ให้ jquery และ select2 เป็นเวอร์ชั่นล่าสุด		

ภาคผนวก ข
เอกสารหลักฐานที่เกี่ยวข้อง

ที่ อว ๗๑๐๗/๐๑๔

คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กทม. ๑๐๘๐๐

๒๐ มกราคม ๒๕๖๘

เรื่อง ขอความอนุเคราะห์เข้าร่วมการตรวจสอบ และทำการค้นคว้าอิสระ

เรียน [redacted]

เนื่องด้วย นายพศวีร์ จงอยู่สุขสันต์ รหัสประจำตัว ๖๖-๐๗๐๓๑๘-๕๗๒๒-๑ นักศึกษาระดับบัณฑิตศึกษา สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ มีความสนใจในด้านการตรวจสอบความมั่นคงปลอดภัยของเว็บแอปพลิเคชันเพื่อเสนอแนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ของ [redacted] ที่นักศึกษาสังกัดอยู่ โดยการนำองค์ความรู้ด้านวิชาการ เทคโนโลยี มาตรฐาน และแนวปฏิบัติ ที่ได้ระหว่างการศึกษาในสาขาวิชาดังกล่าว มาประยุกต์ใช้กับองค์กร โดยคาดหวังว่าการค้นคว้าอิสระนี้ จะเป็นประโยชน์ต่อสำนักงานป้องกันและปราบปรามการฟอกเงิน ในการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรให้รับมือต่อภัยคุกคามทางไซเบอร์ในปัจจุบันที่ทวีความรุนแรงอย่างต่อเนื่อง และเป็นการป้องกันความเสียหายที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศขององค์กรในอนาคต ทั้งยังเป็นแนวทางปรับปรุงเว็บแอปพลิเคชันขององค์กรให้มีความปลอดภัยยิ่งขึ้นได้

ในการนี้ คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล ประสงค์ขอความอนุเคราะห์ให้ นายพศวีร์ จงอยู่สุขสันต์ เข้าร่วมการตรวจสอบความมั่นคงปลอดภัยของเว็บแอปพลิเคชัน พร้อมวิเคราะห์ผลการตรวจสอบเพื่อใช้ประกอบการทำการค้นคว้าอิสระ และเสนอแนวทางการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร ซึ่งจะเป็นประโยชน์กับ [redacted] ต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ จักขอบพระคุณยิ่ง

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.ศักดิ์ชาย ตั้งวรรณวิทย์)
รองคณบดีฝ่ายวิชาการและวิจัย
ปฏิบัติการแทนคณบดีคณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล

ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
โทร. ๐ ๒๕๕๕ ๒๗๑๗
โทรสาร ๐ ๒๕๘๗ ๕๘๘๐
www.itd.kmutnb.ac.th

ที่ อว ๗๑๐๗/๐๑๕

คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กทม. ๑๐๘๐๐

๒๐ มกราคม ๒๕๖๘

เรื่อง ขอความอนุเคราะห์เป็นผู้เชี่ยวชาญในการประเมินคุณภาพเพื่อประกอบการทำการค้นคว้าอิสระ

เรียน นาย[redacted]

เนื่องด้วย นายพศวีร์ จงอยู่สุขสันต์ รหัสประจำตัว ๖๖-๐๗๐๓๑๘-๕๗๒๒-๑ นักศึกษาระดับบัณฑิตศึกษา ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ กำลังดำเนินการจัดทำการค้นคว้าอิสระ เรื่อง “การวิเคราะห์ช่องโหว่ของเว็บแอปพลิเคชันเพื่อเสนอแนวทางการจัดการช่องโหว่สำหรับเว็บแอปพลิเคชันหน่วยงานภาครัฐ” โดยมี ผู้ช่วยศาสตราจารย์ ดร.สุนันทา สดสี เป็นประธานคณะกรรมการที่ปรึกษาการค้นคว้าอิสระ ในการนี้ นักศึกษามีความประสงค์ขอความอนุเคราะห์จากท่านเพื่อโปรดพิจารณาเอกสาร เพื่อประกอบการทำการค้นคว้าอิสระดังกล่าว

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ จักขอบพระคุณยิ่ง

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.ศักดิ์ชาย ตั้งวรรณวิทย์)
รองคณบดีฝ่ายวิชาการและวิจัย
ปฏิบัติการแทนคณบดีคณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล

ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
โทร. ๐ ๒๕๕๕ ๒๗๑๗
โทรสาร ๐ ๒๕๘๗ ๕๘๘๐
www.itd.kmutnb.ac.th

ที่ อว ๗๑๐๗/๐๑๗

คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กทม. ๑๐๘๐๐

๒๐ มกราคม ๒๕๖๘

เรื่อง ขอความอนุเคราะห์เป็นผู้เชี่ยวชาญในการประเมินคุณภาพเพื่อประกอบการทำการค้นคว้าอิสระ

เรียน นางสาว[redacted]

เนื่องด้วย นายพศวีร์ จงอยู่สุขสันต์ รหัสประจำตัว ๖๖-๐๗๐๓๑๘-๕๗๒๒-๑ นักศึกษาระดับบัณฑิตศึกษา ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ กำลังดำเนินการจัดทำการค้นคว้าอิสระ เรื่อง "การวิเคราะห์ช่องโหว่ของเว็บแอปพลิเคชันเพื่อเสนอแนวทางการจัดการช่องโหว่สำหรับเว็บแอปพลิเคชันหน่วยงานภาครัฐ" โดยมี ผู้ช่วยศาสตราจารย์ ดร.สุนันทา สดสี เป็นประธานคณะกรรมการที่ปรึกษาการค้นคว้าอิสระ ในการนี้ นักศึกษามีความประสงค์ขอความอนุเคราะห์จากท่านเพื่อโปรดพิจารณาเอกสาร เพื่อประกอบการทำการค้นคว้าอิสระดังกล่าว

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ จักขอบพระคุณยิ่ง

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.ศักดิ์ชาย ตั้งวรรณวิทย์)
รองคณบดีฝ่ายวิชาการและวิจัย
ปฏิบัติการแทนคณบดีคณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล

ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
โทร. ๐ ๒๕๕๕ ๒๗๑๗
โทรสาร ๐ ๒๕๘๗ ๕๘๘๐
www.itd.kmutnb.ac.th

ที่ อว ๗๑๐๗/๐๑๖

คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กทม. ๑๐๘๐๐

๒๐ มกราคม ๒๕๖๘

เรื่อง ขอความอนุเคราะห์เป็นผู้เชี่ยวชาญในการประเมินคุณภาพเพื่อประกอบการทำการค้นคว้าอิสระ

เรียน นางสาว[redacted]

เนื่องด้วย นายพศวีร์ จงอยู่สุขสันต์ รหัสประจำตัว ๖๖-๐๗๐๓๑๘-๕๗๒๒-๑ นักศึกษาระดับบัณฑิตศึกษา ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ กำลังดำเนินการจัดทำการค้นคว้าอิสระ เรื่อง “การวิเคราะห์ช่องโหว่ของเว็บแอปพลิเคชันเพื่อเสนอแนวทางการจัดการช่องโหว่สำหรับเว็บแอปพลิเคชันหน่วยงานภาครัฐ” โดยมี ผู้ช่วยศาสตราจารย์ ดร.สุนันทา สดสี เป็นประธานคณะกรรมการที่ปรึกษาการค้นคว้าอิสระ ในการนี้ นักศึกษามีความประสงค์ขอความอนุเคราะห์จากท่านเพื่อโปรดพิจารณาเอกสาร เพื่อประกอบการทำการค้นคว้าอิสระดังกล่าว

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ จักขอบพระคุณยิ่ง

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.ศักดิ์ชาย ตั้งวรรณวิทย์)
รองคณบดีฝ่ายวิชาการและวิจัย
ปฏิบัติการแทนคณบดีคณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล

ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
โทร. ๐ ๒๕๕๕ ๒๗๑๗
โทรสาร ๐ ๒๕๘๗ ๕๘๘๐
www.itd.kmutnb.ac.th

ประวัติผู้เขียน

ชื่อ นายพศวีร์ จงอยู่สุขสันต์

ชื่อการค้นคว้าอิสระ การวิเคราะห์และเสนอแนวทางการจัดการช่องโหว่สำหรับเว็บแอปพลิเคชัน

สาขาวิชา การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

ประวัติ

ประวัติการศึกษา

สำเร็จการศึกษาระดับปริญญาตรี อุตสาหกรรมศาสตรบัณฑิต คณะเทคโนโลยีและการจัดการอุตสาหกรรม สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ปีการศึกษา 2561

ประสบการณ์ทำงาน

ปฏิบัติงานในตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์เทคโนโลยีสารสนเทศ หน่วยงานภาครัฐด้านการบังคับใช้กฎหมายในประเทศไทย พ.ศ. 2566 – ปัจจุบัน

ปฏิบัติงานในตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมอุทยานแห่งชาติ สัตว์ป่า และพันธ์พืช พ.ศ. 2564 – 2566

ปฏิบัติงานในตำแหน่ง เจ้าพนักงานธุรการปฏิบัติงาน สำนักข่าวกรองแห่งชาติ พ.ศ. 2561 – 2564