แบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซโดยอิงการจัดให้มีวิธีการรับมือการโจมตี

นายทศพล บ้านคลองสี่

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2554

A SECURITY MEASUREMENT MODEL FOR WEB SERVICES BASED ON PROVISION OF ATTACK COUNTERMEASURES

Mr. Todsapon Banklongsi

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Engineering Program in Computer Engineering

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2011

หัวข้อวิทยานิพนธ์	แบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซโดยอิงการจัดให้มีวิธีการรับมือการโจมตี
โดย	นายทศพล บ้านคลองสี่
สาขาวิชา	วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร.บุญสม เลิศหิรัญวงศ์)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(อาจารย์ ดร.ยรรยง เต็งอำนวย)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(รองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา)

..... กรรมการภายนอกมหาวิทยาลัย
(ผู้ช่วยศาสตราจารย์ ดร.เบญจพร ลิ้มธรรมาภรณ์)

ทศพล บ้านคลองสี่ : แบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซโดยอิงการจัดให้มีวิธีการรับมือการโจมตี. (A SECURITY MEASUREMENT MODEL FOR WEB SERVICES BASED ON PROVISION OF ATTACK COUNTERMEASURES) อ.ที่ปรึกษาวิทยานิพนธ์หลัก : รศ. ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา, 129 หน้า.

เทคโนโลยีเว็บเซอร์วิซได้ถูกนำมาใช้ในองค์กรต่างๆ อย่างกว้างขวางเพื่อให้ธุรกิจหลักและการให้บริการแอปพลิเคชันขององค์กรทำงานผ่านเครือข่ายโดยใช้เทคโนโลยีที่เป็นกลางและมีความยืดหยุ่น อย่างไรก็ตามประเด็นด้านความมั่นคงก็ได้รับการกล่าวถึงโดยผู้ให้บริการขององค์กรและผู้ใช้บริการ เช่นเดียวกับการใช้งานเว็บแอปพลิเคชันอื่นๆ เนื่องจากเว็บเซอร์วิซอาจเสี่ยงต่อการถูกโจมตีด้านความมั่นคง รวมไปถึง การปลอมแปลง การเปิดเผยข้อมูล การแก้ไขข้อมูล การขัดขวางการให้บริการ และการละเมิดการเข้าถึงข้อมูล เพื่อสร้างความไว้วางใจให้กับผู้ใช้บริการ ผู้ให้บริการต้องจัดให้มีวิธีการรับมือต่อการโจมตีเหล่านี้เพื่อป้องกันหรืออย่างน้อยเพื่อลดอันตรายที่การโจมตีเหล่านี้จะทำต่อบริการ

งานวิจัยนี้นำเสนอแบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซโดยอิงความสามารถในการจัดให้มีวิธีการรับมือการโจมตีความมั่นคง แบบจำลองนี้มีพื้นฐานอยู่บนการจัดให้เว็บเซอร์วิซมีวิธีการรับมือ คุณสมบัติการโจมตี และความสำคัญสัมพัทธ์ของการจัดให้มีวิธีการรับมือต่อคุณสมบัติการโจมตีที่ระบุโดยผู้ประเมินความมั่นคง ผลการวัดที่ได้สามารถใช้เป็นข้อแนะนำให้ผู้ให้บริการจัดการให้บริการและสภาพแวดล้อมในการดำเนินงานให้มีความมั่นคงมากยิ่งขึ้น ผลการวัดที่ดียังสามารถเผยแพร่เป็นระดับความมั่นคงสำหรับให้ผู้ใช้บริการได้พิจารณาในการเลือกใช้บริการอีกด้วย งานวิจัยนี้ยังได้เสนอผลการสำรวจการจัดให้มีวิธีการรับมือการโจมตีโดยผู้ให้บริการเว็บเซอร์วิซในประเทศไทย พร้อมกับผลการประเมินแบบจำลองการวัดความมั่นคงโดยผู้ให้บริการเหล่านั้น การประเมินได้รับผลตอบกลับในเชิงบวก กล่าวคือ แบบจำลองสามารถช่วยให้ผู้ให้บริการเหล่านั้นตระหนักถึงสถานะการจัดให้มีการรับมือการโจมตีของตน

ภาควิชา .....วิศวกรรมคอมพิวเตอร์..... ลายมือชื่อนิสิต .....

สาขาวิชา.....วิศวกรรมคอมพิวเตอร์..... ลายมือชื่อ อ. ที่ปรึกษาวิทยานิพนธ์หลัก.....

ปีการศึกษา.....2554.....

5270310621 : MAJOR COMPUTER ENGINEERING
KEYWORD : WEB SERVICES / SECURITY / MEASUREMENT / COUNTERMEASURES / ATTACKS

TODSAPON BANKLONGSI : A SECURITY MEASUREMENT MODEL FOR WEB SERVICES BASED ON PROVISION OF ATTACK COUNTERMEASURES. ADVISOR : ASSOC. PROF. TWITTIE SENIVONGSE, Ph.D., 129 pp.

Web service technology is widely adopted by organizations to provide their core business and application services over the networks in a flexible technology-neutral manner. Nevertheless, security concerns have been raised by corporate service providers and service consumers since, like other Web-based applications, Web services are vulnerable to various security attacks including counterfeiting, disclosure, tampering, disruption, and breach of information. To build trust with service consumers, service providers must provide countermeasures against these attacks to prevent or at least mitigate the harm that these attacks might do to the services.

This research proposes a measurement model for service security in terms of service ability to provide countermeasures against security attacks. The model is based on service countermeasure provision, attack characteristics, and relative importance of countermeasure provision with regard to attack characteristics as specified by security assessors. Resulting measurements can guide service providers to provide for more secure services and operating environments. Good measurement results can also be published as a security rating for service consumers to consider in service selection. This research presents a result of a survey on countermeasure provision by Web service providers in Thailand and an evaluation of the security measurement model by those providers. The evaluation gets a positive feedback such that the model can help the providers to realize their status of countermeasure provision.

Department: .....Computer Engineering.... Student's Signature .....
Field of Study: .....Computer Engineering.... Advisor's Signature.....
Academic Year: .....2011.....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยความกรุณาอย่างยิ่งจากรองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา อาจารย์ที่ปรึกษาหลัก ซึ่งได้ให้โอกาสและแนวคิดในการทำวิทยานิพนธ์ ตลอดจนทักษะ แนวทางการแก้ไขปัญหาและความอดทนให้การวิจัยลุล่วงและประสบความสำเร็จ มาโดยตลอดระยะเวลาการศึกษาและการวิจัย ขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ ที่นี้ด้วย

ขอขอบพระคุณ อาจารย์ ดร.ยรรยง เต็งอำนวย ประธานกรรมการสอบวิทยานิพนธ์ และผู้ช่วยศาสตราจารย์ ดร.เบญจพร ลิ้มธรรมาภรณ์ กรรมการสอบวิทยานิพนธ์ที่ได้ให้คำแนะนำและชี้แนะแนวทางที่เป็นประโยชน์ต่อการทำวิทยานิพนธ์ในครั้งนี้

ขอขอบพระคุณคณาจารย์ทุกท่านที่ อบรม สั่งสอน ให้ความรู้ต่างๆ มากมายจนมีวันนี้

ขอกราบขอบพระคุณคุณพ่อ คุณแม่ พี่ชาย ครอบครัวอันเป็นที่รัก และญาติๆทุกคน ที่ค่อยให้ความห่วงใย ทำให้มีความสุขทั้งกายและใจ และเป็นกำลังใจในการดำเนินชีวิตมาโดยตลอด

ขอขอบคุณทุนพัฒนาอาจารย์จากภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรรมศาสตร์ มหาวิทยาลัยกรุงเทพ ที่ได้ให้เงินสนับสนุนด้านการศึกษาและการทำวิทยานิพนธ์ ทำให้ผู้วิจัยมีพลังในการสร้างสรรค์ผลงานเพื่อให้ได้มาซึ่งวิทยานิพนธ์ที่สมบูรณ์ที่สุด

ขอขอบคุณ นายวงศ์ยศ เกิดศรี นางสาวรัศมีทิพย์ วิตา นางสาววรารัตน์ รุ่งวรวุฒิ นายวีรภัทร พรหมชนะ และนายทวี ไทยส่งสุวรรณ ที่คอยให้คำแนะนำในการทำวิทยานิพนธ์มาโดยตลอด

ขอขอบคุณ นายพรชัย เลิศหทัยรัตน์ นายกำพล ฟ้าภิญโญ นายดำรงชัย แซ่โค้ว นายนที อาจเอี่ยม นายวรอมาตย์ อมาตยกุล นายกฤษดา รองรัตน์ นายธีระพล ม่วงยัง นายนพพร คงวัดใหม่ นายเจษฎา เพ็งสุวรรณ นายอรรพล พวงพุ่ม นางสาวศิริรัตน์ เพ็งแจ่ม นายธีรสุต ไพรินทราภา นายอิสสระพงศ์ ค้วนเครือ นายศิวนันทน์ บุญประเสริฐ และผู้ที่ให้ความช่วยเหลือทุกท่านในการประสานงานและตอบแบบสอบถามงานวิจัยให้เป็นผลสำเร็จ

ขอบคุณเพื่อนๆ พี่ๆ น้องๆ ที่ห้องปฏิบัติการวิศวกรรมระบบสารสนเทศ และที่ภาควิชาวิศวกรรมคอมพิวเตอร์ทุกคน ที่ร่วมทุกข์ร่วมสุข แลกเปลี่ยนความรู้ แง่คิดต่างๆ ตลอดระยะเวลาที่ดำเนินการวิจัย ซึ่งให้ความสนุกสนาน และความอบอุ่นตลอดระยะเวลาที่อยู่ด้วยกัน

สารบัญ

หน้า

บทที่ หน้า

บทที่ หน้า

สารบัญตาราง

ตารางที่ หน้า

ตารางที่ หน้า

สารบัญภาพ

ภาพที่ หน้า

ภาพที่ หน้า

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันอินเทอร์เน็ตและเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทในทุกวงการและประเด็นที่ได้รับความสนใจเป็นอย่างมากคือประเด็นทางด้านความมั่นคงในระบบข้อมูลสารสนเทศ อีกทั้งเทคโนโลยีเว็บเซอร์วิซ [1] กำลังเป็นที่นิยม ซึ่งเว็บเซอร์วิซเป็นตัวกลางในการแลกเปลี่ยนข้อมูลและการให้บริการการทำธุรกรรมต่างๆ ทั้งในเชิงพาณิชย์ การศึกษาและการปกครอง ซึ่งจำเป็นอย่างยิ่งที่ต้องมีการรักษาความมั่นคงเพื่อป้องกันข้อมูลอันมีค่าทั้งของผู้ใช้บริการและผู้ให้บริการในระบบเว็บเซอร์วิซ ทั้งในส่วนของโครงสร้างภายในเว็บเซอร์วิซที่ประกอบด้วยโซป (SOAP) ซึ่งเป็นโพรโทคอลที่ใช้ในการสื่อสารระหว่างผู้ใช้บริการและผู้ให้บริการ วิสเดิล (WSDL) เป็นส่วนที่ใช้ในการอธิบายบริการต่างๆของเว็บเซอร์วิซ และยูดีดีไอ (UDDI) เป็นไดเรกทอรี (Directory) ที่ใช้ในการค้นหาบริการต่างๆ ของเว็บเซอร์วิซซึ่งส่วนประกอบเหล่านี้อาจมีจุดอ่อนในการสร้างเว็บเซอร์วิซขึ้นมาแล้วทำงานอย่างไม่มีเสถียรภาพ และส่วนของการติดต่อสื่อสารข้อมูลผ่านทางเอชทีทีพี (HTTP) ซึ่งอาจมีจุดอ่อนในการส่งผ่านข้อมูลที่ไม่ปลอดภัยและอาจส่งผลให้เกิดการโจมตีจากผู้ไม่หวังดีขึ้นได้ โดยอาจส่งผลให้เกิดการโจมตีในลักษณะการหลอกลวงโดยการปลอมแปลง การเปิดเผยข้อมูล การแก้ไขข้อมูล การขัดขวางการให้บริการ และการละเมิดการเข้าถึงข้อมูล เช่น การกราดตรวจวิสเดิล (WSDL Scanning) เอกซ์พาธอินเจคชัน (XPath Injection) การวางยาเอกซ์เอ็มแอลสคีมา (XML Schema Poisoning) การแทรกแซงโซปพารามิเตอร์ (SOAP Parameter Tampering) การจัดเส้นทางอ้อมเอกซ์เอ็มแอล (XML Routing Detour) และการปฏิเสธการให้บริการเอกซ์เอ็มแอล (XML Denial of Services) เป็นต้น ผู้ให้บริการจึงต้องตระหนักถึงวิธีการรับมือในการรักษาความมั่นคงให้กับบริการของเว็บเซอร์วิซและสามารถสร้างความไว้วางใจในการให้บริการแก่ผู้ใช้บริการว่าการให้บริการดังกล่าวจะไม่ถูกล่วงละเมิดได้ง่าย ดังนั้นการพิจารณาเลือกระบบหรือแอปพลิเคชันของเว็บเซอร์วิซเพื่อนำมาใช้ในองค์กรนั้น จึงควรพิจารณาให้มีความเหมาะสมกับการใช้งานและมีความมั่นคงสูงจากการถูกโจมตีจากผู้ไม่หวังดี

อย่างไรก็ตามวิธีการวัดความมั่นคงสำหรับเว็บเซอร์วิซยังคงเป็นปัญหาที่มีความท้าทาย เนื่องจากการศึกษาด้านนี้ค่อนข้างจำกัดและงานวิจัยที่เกี่ยวข้องกับการวัดความมั่นคงในมุมมองของผู้ใช้บริการและผู้ให้บริการเว็บเซอร์วิซยังมีค่อนข้างน้อย

ดังนั้น งานวิจัยนี้จึงมีแนวคิดในการสร้างแบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซขึ้น โดยประเมินจากความสามารถในการป้องกันตนเองของเว็บเซอร์วิซโดยผู้ให้บริการ ผู้วิจัยได้รวบรวมวิธีการรับมือ (Countermeasure) ต่อการโจมตีที่มีผลต่อเว็บเซอร์วิซ เพื่อนำมาพิจารณาหาความสัมพันธ์ในแง่มุมความสามารถในการจัดให้เว็บเซอร์วิซมีวิธีการรับมือต่อการโจมตีที่ส่งผลกระทบต่อคุณสมบัติต่างๆด้านความมั่นคง จากนั้นจึงทำการวิเคราะห์และวัดผลให้อยู่ในรูปคะแนนและระดับความมั่นคง ซึ่งค่าคะแนนและระดับความมั่นคงที่ได้สามารถนำไปใช้ประโยชน์ในการประเมินตนเองของผู้ให้บริการและใช้เป็นข้อมูลในการหาแนวทางการรับมือให้กับระบบเว็บเซอร์วิซที่มีใช้อยู่แล้วในองค์กรหรือที่กำลังสร้างใหม่ เพื่อช่วยลดความเสี่ยงและผลกระทบหรือป้องกันการถูกโจมตีจากผู้ไม่หวังดี รวมทั้งผู้ให้บริการสามารถประกาศ (Publish) ค่าคะแนนความมั่นคงที่ดีให้ผู้ใช้บริการทราบ เพื่อเป็นประโยชน์ในการเลือกเว็บเซอร์วิซที่มีความมั่นคงมาใช้งาน

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อสร้างแบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซโดยอิงการจัดให้มีวิธีการรับมือการโจมตีและพัฒนาเครื่องมือสนับสนุนแบบจำลอง

1.3 ขอบเขตของการวิจัย

1.3.1 สร้างแบบจำลองการวัดความมั่นคงของเว็บเซอร์วิซโดยอิงการจัดให้มีวิธีการรับมือการโจมตี

1.3.2 พิจารณาข้อมูลการโจมตีเว็บเซอร์วิซและวิธีการรับมือ ซึ่งรวบรวมจาก [2-8] (ในเบื้องต้นพิจารณาการโจมตี 28 แบบ)

1.3.3 พัฒนาเครื่องมือสนับสนุนแบบจำลองในรูปแบบเว็บแอปพลิเคชัน

1.3.4 ทดสอบแบบจำลองและเครื่องมือกับเว็บเซอร์วิซซึ่งมีวิธีการรับมือต่อการโจมตีที่ประเมินโดยนักเขียนโปรแกรมหรือผู้ให้บริการเว็บเซอร์วิซและทดสอบกับเว็บเซอร์วิซของผู้ให้บริการต่างๆ

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 ได้แบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซโดยอิงการจัดให้มีวิธีการรับมือการโจมตีพร้อมทั้งเครื่องมือสนับสนุนเพื่อใช้ประเมินความมั่นคงของเว็บเซอร์วิซ

1.4.2 ผู้ให้บริการหรือผู้ดูแลระบบหรือผู้พัฒนา สามารถนำผลการประเมินความมั่นคงและความรู้จากการใช้งานแบบจำลองไปเป็นแนวทางในการเลือกใช้วิธีการรับมือต่อการโจมตีที่เหมาะสมกับเว็บเซอร์วิซ และกระตุ้นให้หน่วยงานหรือองค์กร มีความสนใจและตระหนักถึงประเด็นความมั่นคงของเว็บเซอร์วิซมากยิ่งขึ้น

1.4.3 ผู้ให้บริการสามารถนำค่าความมั่นคงที่ดีไปประกาศให้ผู้ใช้บริการรับรู้เพื่อเป็นข้อมูลประกอบการพิจารณาเลือกใช้เว็บเซอร์วิซ

1.4.4 สามารถนำหลักการของแบบจำลองไปประยุกต์ใช้ในงานด้านความมั่นคงอื่นๆ หรือขยายแบบจำลองให้รองรับการโจมตีและวิธีการรับมือแบบอื่นๆได้

1.5 วิธีดำเนินการวิจัย

1.5.1 ศึกษาข้อมูลเอกสารและงานวิจัยที่เกี่ยวข้องกับหัวข้อการวัดความมั่นคงสำหรับเว็บเซอร์วิซ

1.5.2 ศึกษาข้อมูลการโจมตีและวิธีการรับมือการโจมตีที่เกี่ยวข้องกับเว็บเซอร์วิซ

1.5.3 ออกแบบแบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซ

1.5.4 พัฒนาเครื่องมือสนับสนุนแบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซ

1.5.5 ทดลองและประเมินผลแบบจำลองการวัดระดับความมั่นคงสำหรับเว็บเซอร์วิซ

1.5.6 ปรับปรุงแก้ไขงานวิจัย

1.5.7 สรุปผลงานวิจัย และ จัดทำวิทยานิพนธ์

1.6 ผลงานตีพิมพ์

ส่วนหนึ่งของวิทยานิพนธ์นี้ได้ตีพิมพ์และนำเสนอในการประชุมวิชาการดังนี้

1.6.1 บทความชื่อ *"A Security Measurement Model for Web Services Based on Provision of Attack Countermeasures"* [9]

1.6.1.1 ชื่อผู้แต่ง Todsapon Banklongsi และ Twittie Senivongse

1.6.1.2 ตีพิมพ์และนำเสนอในงานประชุมวิชาการชื่อ *The 15th International Annual Symposium on Computational Science and Engineering (ANSCSE2011)* ซึ่งจัดขึ้นในวันที่ 30 มีนาคม - 2 เมษายน 2554 ณ จ.ปทุมธานี ประเทศไทย (ได้รับรางวัล Best Paper Award)

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ทฤษฎีที่เกี่ยวข้อง

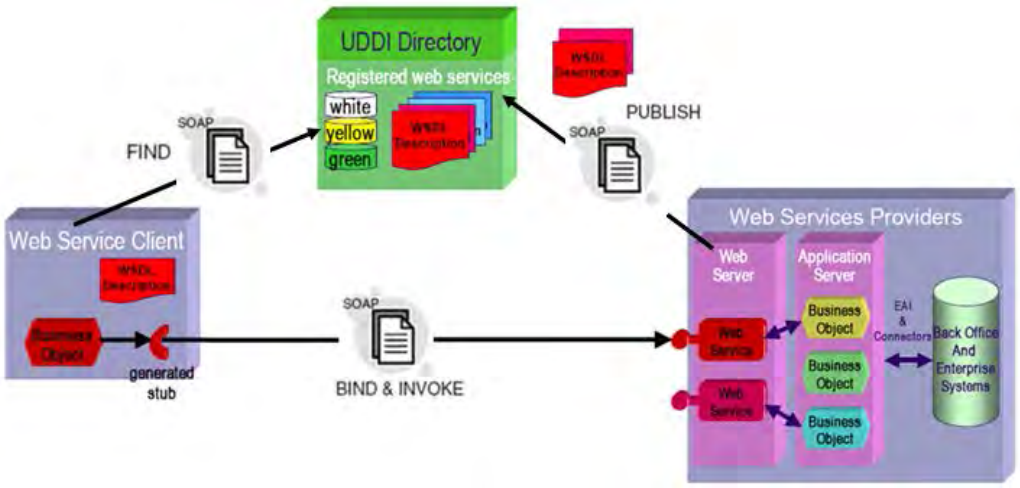
ทฤษฎีที่เกี่ยวข้องอันเป็นประโยชน์ในการทำวิจัยแบ่งออกเป็น 4 ส่วน ได้แก่ เว็บเซอร์วิซ การโจมตีเว็บเซอร์วิซ ความมั่นคงและวิธีการรับมือสำหรับเว็บเซอร์วิซ และซีเอพีอีซี

2.1.1 เว็บเซอร์วิซ

เว็บเซอร์วิซเป็นเทคโนโลยีการเชื่อมต่อแบบหนึ่งที่ใช้ในการสร้างแอปพลิเคชันตามแบบสถาปัตยกรรมเชิงบริการ (Service-Oriented Architecture: SOA) และเป็นระบบซอฟต์แวร์ที่ออกแบบมาเพื่อสนับสนุนการทำงานระหว่างคอมพิวเตอร์กับคอมพิวเตอร์ผ่านระบบเครือข่าย [1] โดยเว็บเซอร์วิซมีเทคโนโลยีพื้นฐานที่เป็นมาตรฐานประกอบด้วย เอกซ์เอ็มแอล (XML: Extensible Markup Language) [10] เป็นภาษาที่พัฒนาโดยดับเบิลยูทรีซี (W3C: World Wide Web Consortium) เพื่อเป็นมาตรฐานในการแลกเปลี่ยนข้อมูลระหว่างเครื่องคอมพิวเตอร์โดยไม่ขึ้นกับแพลตฟอร์มของการพัฒนาซอฟต์แวร์และไม่ขึ้นกับภาษาโปรแกรมและระบบปฏิบัติการ วิสเดิล (WSDL: Web Services Description Language) [11] เป็นภาษาเอกซ์เอ็มแอลที่ใช้สำหรับอธิบายบริการของเว็บเซอร์วิซที่มีรายละเอียดเกี่ยวกับส่วนต่อประสานซึ่งระบุความสามารถและรูปแบบการให้บริการ รวมทั้งกำหนดการติดต่อและตำแหน่งที่อยู่ของบริการเพื่อเรียกใช้โซป (SOAP: Simple Object Access Protocol) [12] ซึ่งเป็นโพรโทคอลที่ใช้กำหนดรูปแบบข้อมูลเอกซ์เอ็มแอลสำหรับการส่งข้อความโดยใช้อินเทอร์เน็ตโพรโทคอล อาทิเช่น เอชทีทีพี (HTTP) เอสเอ็มทีพี (SMTP) และเอฟทีพี (FTP) เป็นต้น และ ยูดีดีไอ (UDDI: Universal Description, Discovery, and Integration) [13] ทำหน้าที่เป็นไดเรกทอรีของเซอร์วิซ โดยรับการลงทะเบียนบริการต่างๆจากผู้ให้บริการมาประกาศไว้สำหรับให้ผู้ใช้บริการทำการค้นหาหรือสอบถามได้ในภายหลัง โดยยูดีดีไอจะกำหนดรูปแบบในการประกาศข้อมูลเกี่ยวกับผู้ให้บริการและกำหนดเอพีไอ (API) สำหรับการประกาศและสอบถามข้อมูล ซึ่งส่วนประกอบเหล่านี้สามารถใช้ร่วมกันในการพัฒนาแอปพลิเคชันที่มีลักษณะของการผนวกรวมส่วนของซอฟต์แวร์ที่กระจายอยู่บนเครือข่าย

การทำงานของเว็บเซอร์วิซเริ่มจากผู้ให้บริการทำการสร้างเอกสารวิสเดิลเพื่ออธิบายรายละเอียดการให้บริการและประกาศข้อมูลเกี่ยวกับบริการไว้ที่ยูดีดีไอ จากนั้นผู้ใช้บริการทำการค้นหาบริการที่ต้องการโดยสอบถามไปที่ยูดีดีไอ เมื่อผู้ใช้บริการได้รับเอกสารวิสเดิลผ่านทาง

ยูดีดีไอ ผู้ใช้บริการจะทำการศึกษาเอกสารวิสเดิลซึ่งระบุรายละเอียดเกี่ยวกับรูปแบบการเรียกใช้บริการและผลลัพธ์ที่ได้ รวมทั้งวิธีการติดต่อและตำแหน่งที่อยู่ของเว็บเซอร์วิซเพื่อให้สามารถเรียกใช้บริการได้โดยตรง เมื่อผู้ใช้บริการทำการร้องขอไปที่เว็บเซอร์วิซของผู้ให้บริการ เว็บเซอร์วิซจะปฏิบัติตามข้อความร้องขอและส่งผลลัพธ์ตามรูปแบบที่ระบุไว้ในเอกสารวิสเดิลกลับมายังผู้ใช้บริการแสดงดังภาพที่ 2.1



ภาพที่ 2.1 การทำงานของเว็บเซอร์วิซ (ปรับจาก [14])

2.1.2 การโจมตีเว็บเซอร์วิซ

การโจมตี (Attack) เรียกอีกอย่างว่าการบุกรุก (Intrusion) หรือการใช้ประโยชน์ (Exploit) เป็นการกระทำที่มุ่งร้ายต่อระบบ ซึ่งเกิดจากเจตนาในการใช้จุดอ่อน (Vulnerability) [15] งานวิจัยนี้ได้นำข้อมูลการโจมตีเว็บเซอร์วิซจาก [2-5] ซึ่งคัดเลือกเฉพาะการโจมตีที่สามารถนำมาปรับใช้ให้เข้ากับงานวิจัยได้ โดยสามารถแบ่งประเภทการโจมตีตาม [2] ได้ดังนี้ (รายละเอียดเพิ่มเติมในภาคผนวก ก)

2.1.2.1 การโจมตีแบบลาดตระเวน

วัตถุประสงค์ของการโจมตีแบบลาดตระเวน (Reconnaissance Attacks) คือการเก็บรวบรวมข้อมูลต่างๆที่เกี่ยวกับแอปพลิเคชันและสภาพแวดล้อมการทำงาน แล้วนำข้อมูลดังกล่าวมาหาข้อบกพร่องเพื่อทำการโจมตีในภายหลัง การโจมตีประเภทนี้ ได้แก่

- การกราดตรวจวิสเดิล (WSDL Scanning)
- วิสเดิลฟิชชิง (WSDL Phishing)
- การตรวจหาเว็บเซอร์วิซที่ไม่ถูกเผยแพร่สู่สาธารณะ (Detect Unpublicized Web Services)

2.1.2.2 **การโจมตีแบบเพิ่มสิทธิ์**

วัตถุประสงค์ของการโจมตีแบบเพิ่มสิทธิ์ (Privilege Escalation Attacks) คือการเปิดให้ผู้โจมตีทำการโยกย้ายถ่ายเทข้อมูลในระบบเครือข่ายที่ตนเองไม่มีสิทธิ์กระทำหรือพยายามแก้ไขสิทธิ์ของตัวเองให้สูงขึ้นกว่าเดิม โดยได้รับประโยชน์จากข้อผิดพลาดหรือข้อบกพร่องจากการเขียนโปรแกรม การออกแบบที่มีข้อผิดพลาดทำให้ผู้โจมตีสามารถยกระดับการเข้าถึงเครือข่ายและข้อมูล โดยสามารถเข้าควบคุมกระบวนการต่างๆได้โดยผ่านทางเลี่ยงระบบควบคุมความมั่นคงซึ่งได้มีการจำกัดการเข้าถึงของผู้โจมตีที่จะเข้าใช้ฟังก์ชัน ข้อมูล ทรัพยากรและสภาพแวดล้อมของเว็บเซอร์วิซ การโจมตีประเภทนี้ ได้แก่

- การโจมตีรหัสผ่านตามดิกชันนารี (Dictionary-Based Password Attack)
- บัฟเฟอร์ล้น (Overflow Buffers)
- การใช้เงื่อนไขการแข่งขัน (Leveraging Race Conditions)
- การโจมตีซิมลิงค์ (Symlink Attacks)
- เซสชันฟิกเซชัน (Session Fixation)
- การโจมตีแบบคนกลาง (Man in the Middle Attack)
- การโจมตีรีเฟลคชันในโพรโทคอลพิสูจน์ตัวจริง (Reflection Attack in Authentication Protocol)
- การใช้ประโยชน์ของตัวแปรเซสชัน รหัสทรัพยากร และข้อมูลรับรองตัวจริงที่เชื่อถือได้อื่นๆ (Exploitation of Session Variables, Resource IDs and Other Trusted Credentials)
- การโจมตีรหัสผ่านแบบบรูทฟอร์ซ (Password Brute Forcing)
- การลองใช้ชื่อผู้ใช้และรหัสผ่านที่เป็นคำสามัญ (ค่าโดยปริยาย) (Try Common (Default) Usernames and Passwords)
- การใช้เอพีไอเว็บเซอร์วิซที่ไม่ถูกเผยแพร่ (Using Unpublished Web Service APIs)

2.1.2.3 **การโจมตีการรักษาความลับ**

วัตถุประสงค์ของการโจมตีการรักษาความลับ (Attacks on Confidentiality) คือการเปิดเผยข้อมูลจาก โปรแกรมประยุกต์ที่เป็นเป้าหมายซึ่งผู้โจมตีไม่ได้รับอนุญาตให้มองเห็น การโจมตีประเภทนี้ ได้แก่

- การดักจับข้อมูล (Sniffing)

2.1.2.4 การโจมตีบูรณภาพ

วัตถุประสงค์ของการโจมตีบูรณภาพ (Attacks on Integrity) คือการแก้ไขข้อมูลจากแอปพลิเคชันที่เป็นเป้าหมายซึ่งผู้โจมตีไม่ได้รับอนุญาตให้เข้าถึงเพื่อทำการเปลี่ยนแปลงข้อมูล การโจมตีประเภทนี้ ได้แก่

- การแทรกแซงโซปพารามิเตอร์ (SOAP Parameter Tampering)
- การวางยาเอกซ์เอ็มแอลสคีมา (XML Schema Poisoning)
- ปรินซิปอลสปูฟิง (Principal Spoofing)
- การจัดเส้นทางอ้อมเอกซ์เอ็มแอล (XML Routing Detour)
- การโจมตีจากเอนทิตีภายนอก (External Entity Attack)

2.1.2.5 การโจมตีแบบปฏิเสธการให้บริการ

วัตถุประสงค์ของการโจมตีแบบปฏิเสธการให้บริการ (Denial of Services Attacks) คือการโจมตีสภาพพร้อมใช้งาน (Availability) โดยจะป้องกันไม่ให้ผู้ให้บริการได้รับหรือตอบกลับข้อความที่มาจากผู้ใช้บริการและอาจทำให้ ไม่สามารถให้บริการได้ เช่น ทำให้ระบบหยุดทำงาน (Crash) หรือมีการทำงานผิดพลาด การโจมตีประเภทนี้ ได้แก่

- การโจมตีตัวแจงส่วนเอกซ์เอ็มแอล (XML Parser Attacks)
- การทำให้ทรัพยากรหมดสิ้นผ่านฟลัดดิง (Resources Depletion through Flooding)
- การทำให้ทรัพยากรหมดสิ้นผ่านดีทีดีอินเจคชันในข้อความโซป (Resource Depletion through DTD Injection in SOAP Message)
- เอกซ์เอ็มแอลปิงออฟเดธ (XML Ping of Death)
- การวางยาเอกซ์เอ็มแอลสคีมา (XML Schema Poisoning) เหมือนหัวข้อ 2.1.2.4

2.1.2.6 การโจมตีแบบคอมมานด์อินเจคชัน

วัตถุประสงค์ของการโจมตีแบบคอมมานด์อินเจคชัน (Command Injection Attacks) คือการโจมตีโดยการใส่คำสั่งที่สามารถเข้าไปควบคุมหรือเรียกดูข้อมูลภายในเอกสารหรือฐานข้อมูลของระบบ การโจมตีประเภทนี้ ได้แก่

- ซีเควลอินเจคชัน (SQL Injection)
- ซีเควลอินเจคชันผ่านการแทรกแซงโซปพารามิเตอร์ (SQL Injection through SOAP Parameter Tampering
- เอกซ์พาธอินเจคชัน (XPath Injection)
- เอกซ์เควียรีอินเจคชัน (XQuery Injection)

2.1.3 ความมั่นคงและวิธีการรับมือสำหรับเว็บเซอร์วิซ

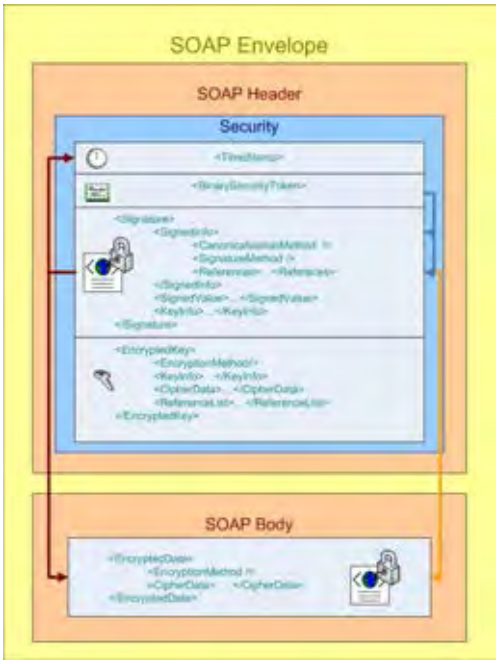
ความมั่นคงเป็นความสามารถของเว็บเซอร์วิซในการจัดการเกี่ยวกับความลับของข้อมูล (Confidentiality) และการห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) ซึ่งทำได้โดยการพิสูจน์ตัวจริง (Authentication) ของผู้ใช้บริการ การเข้ารหัส (Encryption) และกระบวนการควบคุมการเข้าถึงข้อมูล (Access Control) ความมั่นคงถูกมองว่าเป็นสิ่งที่สำคัญอย่างหนึ่งเพราะการเรียกใช้บริการเว็บเซอร์วิซกระทำผ่านอินเทอร์เน็ตสาธารณะ (Public Internet) ผู้ให้บริการเว็บเซอร์วิซสามารถใช้หลากหลายวิธีและในหลากหลายระดับในการจัดหาความมั่นคงโดยขึ้นอยู่กับผู้ใช้บริการเป็นหลัก [16]

วิธีการรับมือ (Countermeasure) ต่อการโจมตีที่จะเกิดขึ้นสามารถเป็นได้ทั้งการกระทำขององค์กรหรือเครื่องมือใดๆที่สามารถลดความเสี่ยงอันเกิดขึ้นจากการโจมตีประเภทใดประเภทหนึ่งเป็นอย่างน้อยที่มีวัตถุประสงค์เพื่อใช้ประโยชน์จากช่องโหว่ประเภทใดประเภทหนึ่งเป็นอย่างน้อย [15] สามารถอธิบายรายละเอียดได้ดังนี้

2.1.3.1 กลไกดับเบิลยูเอส-ซีเคียวริตี

กลไกดับเบิลยูเอส-ซีเคียวริตี (WS-Security Mechanism) [17] ถูกพัฒนาโดยโอเอซิส (OASIS: The Organization for the Advancement of Structure International Standards) ออกแบบมาเพื่อเพิ่มความมั่นคงในระดับข้อความ (Message-Level Security) ในการส่งข้อมูลระหว่างเว็บเซอร์วิซแบบปลายถึงปลาย (End-to-End) โดยเป็นกลไกในการกำหนดบูรณภาพ การรักษาความลับ และการพิสูจน์ตัวจริงให้กับข้อความโซป โดยอาศัยข้อกำหนดเกี่ยวกับลายเซ็นเอกซ์เอ็มแอล (XML Signature) ข้อกำหนดในการเข้ารหัสและถอดรหัสเอกซ์เอ็มแอล (XML Encryption) และโทเคนความมั่นคง (Security Tokens) แสดงดังภาพที่ 2.2 และ 2.3

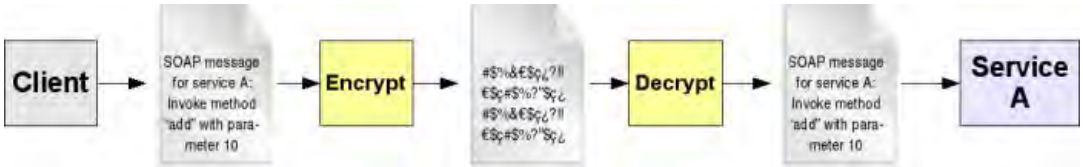
ภาพที่ 2.2 การส่งข้อมูลความมั่นคงในระดับข้อความ [18]



ภาพที่ 2.3 โครงสร้างข้อความโซปที่ใช้กลไกดับเบิลยูเอส-ซีเคียวริตี [19]

2.1.3.2 กลไกความมั่นคงระดับทรานสปอร์ต

กลไกความมั่นคงระดับทรานสปอร์ต (Transport-level Security Mechanism) [5] จะมีการเข้ารหัสข้อมูลที่ใช้ส่งระหว่างเซิร์ฟเวอร์กับไคลเอนต์เป็นแบบจุดต่อจุด (Point-to-Point) เช่น เอสเอสแอล (SSL: Secure Socket Layer : SSL) เป็นโพรโทคอลจัดความมั่นคงในระบบอินเทอร์เน็ตที่ใช้ในการสื่อสารข้อมูลกันระหว่างไคลเอนต์กับเซิร์ฟเวอร์ ปกติแล้วข้อมูลที่ส่งไปหากันจะไม่มีการเข้ารหัสข้อมูลแต่อย่างใด ทำให้การดักจับข้อมูลเป็นไปได้โดยง่าย แต่ถ้าเป็นระบบที่ใช้เอสเอสแอล ข้อมูลจากไคลเอนต์ที่ส่งไปที่เซิร์ฟเวอร์จะถูกเข้ารหัสก่อนที่จะส่งไปที่เซิร์ฟเวอร์ ทำให้ข้อมูลที่รับส่งกันมีความมั่นคงมากขึ้น แต่สามารถปกป้องข้อความได้เฉพาะช่วงของการขนส่งระหว่างเซอร์วิซเท่านั้น ดังภาพที่ 2.4



ภาพที่ 2.4 การส่งข้อมูลความมั่นคงในระดับทรานสปอร์ต [18]

2.1.3.3 การตรวจสอบสคีมา

การตรวจสอบสคีมา (Schema Validation) [6] เป็นกระบวนการตรวจสอบบูรณภาพของโครงสร้างและข้อมูลในเอกสารเอกซ์เอ็มแอล การตรวจสอบสคีมาสามารถใช้เพื่อป้องกันการโจมตี

ที่มีการใช้โครงสร้างและข้อมูลในเอกสารเอกซ์เอ็มแอลที่ไม่สอดคล้องกับวิสเดิล โดยการตรวจสอบข้อความนำเข้า (Incoming Messages) กับเอกซ์เอ็มแอลสคีมาในวิสเดิลว่ามีประเภทข้อมูล รูปแบบ และเป็นไปตามข้อบังคับที่กำหนดโดยสคีมาหรือไม่ ถ้าไม่สอดคล้องตามที่กำหนดไว้ การโจมตีนั้นก็สามารถถูกตรวจจับได้

2.1.3.4 **การทำให้สคีมามั่นคงขึ้น**

การทำให้สคีมามั่นคงขึ้น (Schema Hardening) [6] เป็นการเข้มงวดกับสคีมาของข้อความเอกซ์เอ็มแอล เพื่อที่จะสามารถจำกัดปริมาณหน่วยความจำที่จำเป็นต้องใช้ในการประมวลผลข้อความ และหลีกเลี่ยงปัญหาที่จะตามมาจากการมีเพย์โหลดขนาดใหญ่มาก (Oversized Payload) แนวคิดโดยทั่วไปคือทำการวิเคราะห์สคีมาในวิสเดิลซึ่งไม่มีการจำกัดจำนวนหรือขนาดภายในโครงสร้างข้อมูล และผู้โจมตีสามารถใช้ประโยชน์จากความยืดหยุ่นนี้โดยส่งข้อความที่มีขนาดใหญ่มากมาได้ ดังนั้นจึงต้องมีการปรับแต่งสคีมาให้มีการจำกัดจำนวนอีลิเมนต์ ความลึกของอีลิเมนต์ จำนวนแอททริบิวต์ต่ออีลิเมนต์ เช่น แท็ก <element maxOccurs="unbounded"> ให้เปลี่ยนเป็น <element maxOccurs="n"> หากเป็นไปได้ โดยที่ n เป็นจำนวนจำกัด

2.1.3.5 **บริการเสมือน**

บริการเสมือน (Service Virtualization) [5] เป็นการซ่อนรายละเอียดของทรัพยากรแบคเอนด์ (Back End Rescources) และบริการที่มีความละเอียดอ่อนหรือมีข้อมูลที่สำคัญ (Sensitive Services) ผู้ให้บริการสามารถทำการซ่อนยูอาร์แอลและโพรโทรคอลการสื่อสารจากผู้โจมตี โดยใช้ไฟร์วอลล์ หรือ ใช้การสร้างตัวกลาง (Intermediary) หรือวิสเดิลพร็อกซีขึ้นมาเพื่อให้บริการที่มีความละเอียดอ่อนนั้นไม่ถูกเข้าถึงโดยตรง โดยร่วมกับการพัฒนาตัวกรองข้อความ (Message-Level Filter) ซึ่งทำหน้าที่พิจารณาเนื้อหาของข้อความที่ถูกส่งมายังตัวกลางหรือพร็อกซีก่อนเพื่อเพิ่มการรักษาความมั่นคง ก่อนที่จะส่งข้อความต่อไปยังยูอาร์แอลของบริการภายใน

2.1.3.6 **การตรวจสอบข้อมูลเข้าอย่างเข้มงวด**

การตรวจสอบข้อมูลเข้าอย่างเข้มงวด (Strong Input Validation) [3] เป็นขั้นตอนที่มีความสำคัญในการหลีกเลี่ยงการโจมตีแบบอินเจคชัน โดยเป็นการตรวจสอบการป้อนข้อมูลที่ผู้ใช้สามารถควบคุมได้ (User-controllable Input) ข้อมูลจะถูกตรวจสอบและคัดกรองก่อนที่จะถูกประมวลผลโดยเซอร์วิซและไม่ได้ถูกตรวจสอบเพียงแค่ประเภทของข้อมูลเท่านั้น แต่รวมถึงรูปแบบ ความยาว พิสัยและเนื้อหา ตัวอย่างนิพจน์ปรกติ (Regular Expression) เช่น ตัวอักขระฟันหนู

เดี่ยว (‘) หรือโอเปอเรชัน หรือ (|) และ (&) และเครื่องหมายต่างๆ (/^”*;<()--) ซึ่งเมื่อถูกแปลความหมายแล้วจะอยู่ในบริบทของนิพจน์เอกซ์พาธหรือคำสั่งซีเควล

2.1.3.7 **การปรับแต่งข้อมูลข้อผิดพลาดให้มีความปลอดภัย**

การปรับแต่งข้อมูลข้อผิดพลาดให้มีความปลอดภัย (Error Information Sanitization) [5] เป็นการปรับแต่งหรือแก้ไขข้อมูลความผิดพร่องแบบโซป (SOAP Fault Information) ให้เหมาะสมก่อนที่จะส่งกลับไปให้ผู้ใช้บริการรับทราบ เนื่องจากข้อผิดพลาดหลายอย่างอาจเกิดจากฐานข้อมูล และเมื่อส่งข้อมูลนี้กลับไปยังผู้ใช้บริการ ผู้โจมตีสามารถนำข้อมูลเหล่านี้มาใช้ประโยชน์ในการโจมตีได้ ดังนั้นจะต้องมีการปรับแต่งข้อมูลความผิดพร่องแบบโซปในการแสดงผลโดยไม่มีการเปิดเผยข้อมูลที่เกี่ยวกับฐานข้อมูลและแอปพลิเคชัน

2.1.3.8 **การใช้การสอบถามแบบมีพารามิเตอร์**

การใช้การสอบถามแบบมีพารามิเตอร์ (Use of Parameterized Queries) [3] เรียกอีกอย่างหนึ่งว่าการใช้ Prepared Statements เป็นวิธีการเขียนการสอบถามฐานข้อมูล (Database Query) แบบหนึ่งที่ปลอดภัยกว่าการสอบถามแบบไดนามิค ทั้งนี้เนื่องจากในการสอบถามแบบไดนามิคจะมีการรับอินพุตจากภายนอกของผู้ใช้เข้ามาผนวกกับส่วนของเควียรีที่นักพัฒนาโปรแกรมกำหนดไว้แล้วเพื่อทำให้เควียรีนั้นกลายเป็นเควียรีที่สมบูรณ์และสามารถสอบถามข้อมูลได้ แต่อินพุตที่รับจากภายนอกนั้นไม่ถูกตรวจสอบและอาจเป็นอะไรก็ได้ จึงกลายเป็นจุดอ่อนต่อการโจมตีแบบซีเควลอินเจคชันได้ สำหรับการสอบถามแบบมีพารามิเตอร์นั้น นักพัฒนาโปรแกรมจะเขียนโค้ดซีเควล (SQL Code) สำหรับเควียรีไว้ในโปรแกรม และส่วนอินพุตที่ต้องรับจากภายนอกจะระบุให้เป็นพารามิเตอร์ เช่น เป็นสตริงหรือตัวเลข หากอินพุตที่รับเข้ามาเป็นข้อมูลประเภทอื่นการสอบถามจะล้มเหลว นอกจากนี้ผู้โจมตียังไม่สามารถเปลี่ยนความหมายของการทำงานของเควียรีได้แม้ว่าจะส่งคำสั่งซีเควลเป็นอินเจคชันเข้ามา เควียรียังสามารถสอบถามข้อมูลได้ตรงตามความหมายที่นักพัฒนาโปรแกรมต้องการและมองคำสั่งที่ถูกอินเจคเข้ามาเป็นเพียงพารามิเตอร์หนึ่งของโค้ดเควียรี

2.1.3.9 **การเขียนโปรแกรมที่ปลอดภัย**

การเขียนโปรแกรมที่ปลอดภัย (Safe Programming) [2] หมายรวมถึงการเขียนโค้ดเว็บเซอร์วิซด้วยภาษาที่มีการตรวจสอบอินพุตแบบอัตโนมัติ เช่น จาวา และซีชาร์ป หรือถ้าเขียนด้วยภาษาซี หรือซีพลัสพลัส ต้องมีการกำหนดความยาวและรูปแบบของอินพุตที่คาดหวังไว้ และตรวจสอบด้วยว่าอินพุตที่ได้รับเป็นไปตามที่กำหนดหรือไม่ ส่วนจัดการข้อผิดพลาดและข้อยกเว้น

(Exception Handling) ในโปรแกรมควรจะปฏิเสธอินพุตที่ไม่ถูกต้องหรือตัดอินพุตให้สั้นลงหากไม่เป็นไปตามความยาวที่กำหนดไว้

2.1.3.10 วิธีการรับมือในแง่การจัดสรรหน่วยความจำ

วิธีการรับมือในแง่การจัดสรรหน่วยความจำ (Memory Allocation Countermeasures) [2] หมายถึงการจัดสรรหน่วยความจำสำหรับเป็นอินพุตบัฟเฟอร์ให้จัดสรรในบริเวณหน่วยความจำที่ไม่สามารถประมวลผลได้ (Non-executable Storage Area) ทั้งนี้เพื่อป้องกันไม่ให้โค้ดการโจมตีที่ฝังตัวอยู่ในอินพุตขนาดใหญ่ถูกสั่งให้ประมวลผล วิธีนี้จะช่วยป้องกันการโจมตีแบบบัฟเฟอร์ล้นซึ่งโค้ดที่มุ่งร้ายจะได้รับการประมวลผลโดยที่ไม่ต้องการ

2.1.3.11 วิธีการรับมือในแง่ตัวแปลโปรแกรม

วิธีการรับมือในแง่ตัวแปลโปรแกรม (Compiler-Based Countermeasures) [2] มีตัวอย่างเช่น ตัวแปลโปรแกรมภาษาซีและซีพลัสพลัสหลายตัวจะมีมาตรการป้องกันการล้น (Antioverflow Countermeasures) โดยมีการตรวจสอบขอบเขต (Bound) ของอาร์เรย์ ณ เวลาแปลโปรแกรม (Compile Time) ทุกครั้งเมื่อมีการเข้าถึงอาร์เรย์ใน ซอร์ซโค้ด วิธีการนี้จะทำให้ไม่เกิดปัญหาบัฟเฟอร์ล้นแต่จะมีโอเวอร์เฮดมากในกระบวนการแปลโปรแกรม วิธีการรับมือ ณ เวลาแปลโปรแกรมวิธีอื่นจะเป็นการตรวจสอบบูรณภาพของตัวชี้ (Code Pointers) ที่ชี้ไปยังข้อมูลในบัฟเฟอร์ก่อนที่จะทำการอ้างอิงค่าข้อมูล (Deferencing) จากตัวชี้นั้น เทคนิคนี้ไม่ได้ทำให้บัฟเฟอร์ล้นเป็นไปไม่ได้ แต่มันจะหยุดการโจมตีบัฟเฟอร์ล้นส่วนมากได้หรือทำให้การโจมตีที่มันไม่สามารถหยุดได้เป็นไปได้ยากขึ้น

2.1.3.12 วิธีการรับมือในแง่คลังโปรแกรม

วิธีการรับมือในแง่คลังโปรแกรม (Library-based Countermeasures) [2] มีสาเหตุมาจากการที่การใช้งานฟังก์ชันมาตรฐานบางฟังก์ชันของภาษาซีและซีพลัสพลัส มักก่อให้เกิดปัญหาโอเวอร์โฟลว์ ดังนั้น ณ เวลาลิงค์ (Link Time) ควรนำคลังโปรแกรมที่ปลอดภัยเข้ามาลิงค์เพื่อใช้งานแทน ตัวอย่างของคลังโปรแกรมที่ปลอดภัย เช่น ลิบเซฟ (Libsafe) ซึ่งป้องกันปัญหาโอเวอร์โฟลว์ได้ นอกจากนี้สำหรับฟังก์ชันที่มีแนวโน้มที่จะเกิดปัญหาโอเวอร์โฟลว์ สามารถใช้กลไกการกรอง/ห่อหุ้ม (Filtering/Wrapping) ด้วยโค้ดซึ่งทำการกำหนดและตรวจสอบขนาดของข้อมูลของฟังก์ชัน (Bound Definition and Checking Logic) เพื่อช่วยแก้ปัญหาดังกล่าว

2.1.3.13 การใช้ดับเบิลยูเอส-แอดเดรสซิง

โดยปกติผู้ใช้บริการจะเข้าถึงเว็บเซอร์วิซโดยตรงผ่านเอนด์พอยต์ยูอาร์แอล (Endpoint URL) ที่ระบุอยู่ในวิสเดิล และข้อมูลเกี่ยวกับตำแหน่งที่อยู่ปลายทางจะไม่อยู่ในข้อความโซปที่

ติดต่อกับเว็บเซอร์วิซเลย แต่จะอยู่ที่ระดับทรานสปอร์ตโดยขึ้นกับการระบุตำแหน่งที่อยู่ปลายทางของทรานสปอร์ตโพรโทคอล วิธีนี้พอเพียงสำหรับการติดต่อโดยทั่วไปกับเว็บเซอร์วิซ แต่จะไม่สามารถรองรับกรณีที่รูปแบบการติดต่อกับเว็บเซอร์วิซมีความซับซ้อนขึ้น เช่น เมื่อต้องการจัดเส้นทางให้กับข้อความโซป (Routing) เมื่อต้องการให้มีนโยบายกำกับการประมวลผลข้อความโซป หรือเมื่อต้องการกำหนดผู้รับข้อความตอบกลับหรือข้อความผิดพร่อง (Fault Message) ให้เป็นผู้อื่นที่ไม่ใช่ผู้ส่ง เป็นต้น การใช้ดับเบิลยูเอส-แอดเดรสซิง (Use of WS-Addressing) [5] จะช่วยให้การติดต่อกับเว็บเซอร์วิซเป็นไปในรูปแบบที่ซับซ้อนได้ ดับเบิลยูเอส-แอดเดรสซิงกำหนดนิยามของอีพีอาร์ (EPR: Endpoint Reference) ซึ่งระบุข้อมูลการติดต่อเอนด์พอยต์ (หรือตัวเว็บเซอร์วิซ) ในรูปแบบมาตรฐานและไม่ขึ้นกับทรานสปอร์ตโพรโทคอลไว้ และในข้อความโซปสามารถอ้างอิงข้อมูลที่อยู่ในอีพีอาร์ได้โดยแนบไปกับส่วนหัวของข้อความ วิธีนี้จะทำให้ข้อความโซปมีข้อมูลเกี่ยวกับตำแหน่งที่อยู่ปลายทางและข้อมูลการติดต่ออื่นๆ ในตัวมันเองทำให้สามารถจัดการรูปแบบการติดต่อที่ซับซ้อนได้ ข้อมูลในอีพีอาร์ประกอบด้วย ตำแหน่งที่อยู่ตามโพรโทคอลของการทรานสปอร์ต ข้อมูลพอร์ตไทป์/เซอร์วิซ/พอร์ตตามวิสเดิล นโยบายกำกับการทำงานของเว็บเซอร์วิซ และเรเฟอเรนซ์พรอพเพอร์ตี (Refernece Property) ซึ่งมีค่าของเรเฟอเรนซ์พารามิเตอร์ (Reference Parameter) ระบุอยู่ เรเฟอเรนซ์พรอพเพอร์ตีและเรเฟอเรนซ์พารามิเตอร์เป็นข้อมูลที่ใช้แยกแยะบริการที่แตกต่างกันของเว็บเซอร์วิซภายใต้การใช้ตำแหน่งที่อยู่เพื่อติดต่ออันเดียวกัน ในด้านการรักษาความมั่นคง ผู้ให้บริการเว็บเซอร์วิซสามารถแจกไอดีให้กับผู้ใช้สำหรับเป็นรหัสผ่านในการใช้บริการในลักษณะต่างๆ ได้ โดยให้ผู้ใช้บริการระบุไอดีนั้นมาเป็นเรเฟอเรนซ์พารามิเตอร์ภายในส่วนหัวของข้อความโซป ดังนั้นแม้ว่าผู้โจมตีจะทราบยูอาร์แอลตำแหน่งที่อยู่ของเว็บเซอร์วิซ ก็ไม่สามารถเข้าถึงได้โดยตรงหากไม่มีไอดี วิธีนี้จึงช่วยป้องกันการกราดตรวจวิสเดิลและการกราดตรวจพอร์ตได้

2.1.3.14 ตัวตรวจสอบเอกซ์เอสแอล

ข้อความเอกซ์เอ็มแอลที่เว็บเซอร์วิซรับเข้ามาเป็นอินพุตอาจได้รับการแปลงรูปโดยใช้เอกซ์เอสแอล (XSL: Extensible Stylesheet Language) ซึ่งเป็นภาษาที่ใช้อธิบายการแปลงข้อมูลส่วนต่างๆ ในเอกซ์เอ็มแอลให้อยู่ในรูปแบบใหม่ การตรวจสอบข้อมูลเอกซ์เอ็มแอลที่ถูกแปลงรูป โดยใช้ตัวตรวจสอบเอกซ์เอสแอล ตัวตรวจสอบเอกซ์เอสแอล (XSL Validators) [5] จะช่วยให้มั่นใจในความถูกต้องของข้อความอินพุตได้

2.1.3.15 การลดวิสเดิล

การลดวิสเดิล (WSDL Reduction) [6] เป็นการกรองฟังก์ชันที่มีการเปิดเผยสู่สาธารณะทางวิสเดิล (โดยเฉพาะถ้ามีการใช้เครื่องมือในการสร้างวิสเดิล) ต้องตรวจสอบให้แน่ใจว่าจะไม่มีช่องโหว่ที่ทำให้เกิดการอินเจคชัน และต้องแน่ใจว่าวิสเดิลจะไม่เปิดเผยฟังก์ชันและเอพีไอที่ไม่ได้ตั้งใจเปิดเผย เช่น ฟังก์ชันลับหรือฟังก์ชันที่ใช้เฉพาะส่วนตัว อาจจะต้องให้ความสนใจกับการตั้งชื่อและเมท็อดของฟังก์ชันภายในวิสเดิล ว่าฟังก์ชันที่มีการเปิดเผยนั้นต้องไม่มีชื่อและวิธีการเรียกใช้งานเมท็อดเหมือนกับฟังก์ชันลับที่ใช้เฉพาะภายใน เพราะถ้ามีการตั้งชื่อและวิธีการเรียกใช้เมท็อดเหมือนกัน ผู้โจมตีอาจจะสามารถกราดตรวจข้อมูลในวิสเดิลเพื่อเข้าใช้งานฟังก์ชันลับได้

2.1.3.16 นโยบายรหัสผ่านที่แข็งแกร่ง

การใช้นโยบายรหัสผ่านที่แข็งแกร่ง (Strong Password Policy) [7] เป็นการบังคับใช้นโยบายรหัสผ่านที่คาดเดาได้ยากด้วยการกำหนดการตั้งค่านโยบายกลุ่มที่สอดคล้องกับความต้องการด้านความมั่นคงขององค์กร โดยคุณสมบัตินโยบายรหัสผ่านที่แข็งแกร่งจะยกตัวอย่างตามมาตรฐานเอสเอ็นเอส (SANS) ได้แก่ การเปลี่ยนรหัสผ่านระบบทุกระดับ (เช่น รูท (Root) บัญชีผู้ดูแลแอปพลิเคชัน (Application Administration Accounts) ฯลฯ) อย่างน้อยเป็นรายไตรมาส การเปลี่ยนรหัสผ่านผู้ใช้อย่างน้อยทุก 6 เดือน แต่ช่วงเวลาการเปลี่ยนที่แนะนำควรเป็น ทุก 4 เดือน รหัสผ่านควรมีทั้งตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก (เช่น a-z, A-Z) ต้องมีตัวเลข (Digit) และตัวอักขระพิเศษ (เช่น 0-9, !@#%^&*()_+|~-=\{}[]:";'<>?./) ต้องมีความยาวอย่างน้อย 8 ตัวอักขระ และไม่ใช้คำที่มีในภาษาใดๆ คำแสลง (Slang) ภาษาถิ่น (Dialect) และศัพท์เทคนิคเฉพาะ (Jargon)

2.1.3.17 กฎและนโยบายโครงแบบบนเอกซ์เอ็มแอลไฟร์วอลล์

เอกซ์เอ็มแอลไฟร์วอลล์เป็นไฟร์วอลล์แบบใหม่ที่มีการทำงานอยู่ที่หรือเหนือกว่าชั้นแอปพลิเคชัน (Application Layer) ในสแตคทีซีพี/ไอพีแบบเดิม (Convention TCP/IP Stack) แพ็คเกต-ฟิลเตอริงไฟร์วอลล์แบบเดิม (Traditional Pactket-filtering Firewalls) ไม่สามารถช่วยในการป้องกันการโจมตีแบบปฏิเสธการให้บริการ (DoS) ที่ชั้นเอกซ์เอ็มแอลและเว็บเซอร์วิซ (XML and Web Services Layer) ได้ โดยการโจมตีที่ชั้นเอกซ์เอ็มแอลและเว็บเซอร์วิซจะอยู่บนพื้นฐานของส่วนข้อความเอกซ์เอ็มแอลซึ่งไม่สามารถวิเคราะห์หรือตรวจจับได้โดยกลไกแพ็คเกต-ฟิลเตอริง เอกซ์เอ็มแอลไฟร์วอลล์อยู่บนพื้นฐานแนวคิดของการตรวจสอบเนื้อหาเอกซ์เอ็มแอลซึ่งเอกซ์เอ็มแอลไฟร์วอลล์อาจจะถูกใช้ในรูปซอฟต์แวร์พร็อกซี (Software Proxies) หรืออุปกรณ์ (Appliances) ไฟร์วอลล์เหล่านี้สามารถกำหนดค่าให้มีการดำเนินการในด้านการพิสูจน์ตัวจริง การกำหนดสิทธิ์การใช้งาน (Authorization) และการตรวจสอบ (Auditing) และสามารถป้องกัน

การโจมตีเว็บเซอร์วิซได้หลากหลาย เอกซ์เอ็มแอลไฟร์วอลล์เหล่านี้โดยทั่วไปจะนำไปใช้หลังไอพีไฟร์วอลล์ (IP Firewall) และมีการควบคุมการไหลของข้อความก่อนที่จะมาถึงเว็บเซอร์วิซ กฎและนโยบายโครงแบบบนเอกซ์เอ็มแอลไฟร์วอลล์ (Configuration rules and policies on the XML firewall) [5] สามารถกำหนดค่าพารามิเตอร์เพื่อใช้ในการรับมือการโจมตี ตัวอย่างเช่น ค่าพารามิเตอร์ที่ใช้รับมือการโจมตีแบบปฏิเสธการให้บริการ ได้แก่ MAX_NESTED_LEVELS, MAX_ATTRIBUTE_ALLOWED, MAX_ELEMENT_PER_LEVEL, RECURSION_ALLOWED, MAX_REQUEST_PROCESS_TIME, AUTO_REQUEST_BLOCK, ATTACK_THRESHOLD_COUNT, ERROR_THRESHOLD_COUNT, AUTHORIZATION_THRESHOLD_COUNT, CPU_THRESHOLD_LIMIT, NOTIFICATION_TYPES, AUTO_SERVICE_DENY, SERVICE_RESTART_INTERVAL, MAX_REQUEST_RATE, REPLAY_MONITOR_FLAG และ MAX_REQUEST_RATE_FROM_HOST

2.1.3.18 วิธีการรับมือการโจมตีแบบอื่น ๆ

เป็นวิธีการรับมือการโจมตีในรูปแบบอื่นๆ (Other Countermeasures) ที่นอกเหนือจากที่กล่าวไว้แล้วข้างต้น ได้แก่

- การสร้างกลไกแฮนด์เชคสำหรับติดต่อกับแอดฮอกวิสเดิลหรือเว็บเซอร์วิซเพื่อให้มั่นใจในความถูกต้อง (Creating a handshake mechanism for interacting with ad hoc WSDL or Web service to ensure validity) [5]
- การกำหนดให้ตัวประมวลเอกซ์เอ็มแอลเรียกเอนทิตีภายนอกเฉพาะที่มาจากแหล่งที่น่าเชื่อถือ (Configuring the XML processor to only retrieve external entities from trusted sources) [3]
- การพิสูจน์ตัวจริงของตัวบริการและแหล่งค้นพบบริการ (Authenticating both services and their discovery) [3]
- การใช้งานโซปและเอกซ์เอ็มแอลอาร์พีซีที่ถูกต้อง (Using the correct SOAP and XMLRPC implementations) [5]
- การระงับการอ้างอิงยูอาร์ไอภายนอกเพื่อป้องกันข้อมูลที่เป็นอันตรายไม่ให้เข้ามา (Suppressing external URI references to protect against malicious data) [5]
- การไม่เปิดเผยบัญชีของผู้ใช้ซึ่งมีการเข้าถึงคำสั่งโฮสต์ให้แก่เอนทิตีภายนอก (Do not expose the user accounts that access to host commands to external entities) [3]
- การกรองข้อความโดยดูจากชื่อเว็บเซอร์วิซหรือยูอาร์แอลของเว็บเซอร์วิซ (Filtering messages based on Web service name or Web service URL) [8]

- การกำหนดค่าการควบคุมการเข้าถึงเครือข่ายให้ยอมรับข้อความขาเข้าจากเลขที่อยู่ไอพีที่เหมาะสม (Configuring network access control to accept incoming message from a specific IP address) [8]

- การใช้กลไกล็อคบัญชีผู้ใช้หากใส่รหัสผ่านผิดหลายครั้งเมื่อล็อกอิน (Implementing a password throttling mechanism) [3]

- ฯลฯ

2.1.4 ซีเอพีอีซี

ซีเอพีอีซี (CAPEC: Common Attack Pattern Enumeration and Classification) [3] เป็นอนุกรมวิธานการโจมตี (Attack Taxonomy) ที่ถูกพัฒนาโดย ไมเทอร์ (MITRE) ได้รับการสนับสนุนจากกระทรวงความมั่นคงแห่งมาตุภูมิของสหรัฐอเมริกา (The US Department of Homeland Security) มีเป้าหมายเพื่อสร้างรายการของแบบรูปการโจมตี (Attack Patterns) ที่ถูกใช้โดยผู้โจมตีเมื่อมีการครอบครองระบบ โดยใช้สคีมาที่ครอบคลุมและอนุกรมวิธานการจำแนก ซึ่งเป็นกลไกที่มีประสิทธิภาพในการสื่อสารตามมุมมองของผู้โจมตี และมีคำอธิบายวิธีการทั่วไปของซอฟต์แวร์ที่ใช้ประโยชน์ (Exploit) เพื่อการโจมตี ซึ่งรายการเหล่านี้ได้มาจากแนวคิดของแบบรูปการออกแบบ (Design Patterns) ที่ถูกนำไปใช้ในบริบทที่เป็นการทำลาย (Destructive) มากกว่าการสร้างสรรค์และถูกสร้างขึ้นมาจากการวิเคราะห์ในเชิงลึกของตัวอย่างการใช้ประโยชน์ที่มีอยู่ในโลกความเป็นจริง รายการเหล่านี้สามารถนำไปใช้เพื่อช่วยในการเพิ่มการรักษาความมั่นคงตลอดช่วงวงจรชีวิตการพัฒนาซอฟต์แวร์และรองรับความต้องการของนักพัฒนา นักทดสอบ และนักวิชาการ

2.2 เอกสารและงานวิจัยที่เกี่ยวข้อง

วิธีการและแบบแผนที่เกี่ยวกับการวัดความมั่นคงของเว็บเซอร์วิซนั้นได้รับความสนใจเพิ่มมากขึ้นในปัจจุบัน เพราะเนื่องจากว่า เมื่อมีระบบเว็บเซอร์วิซ มีการทำธุรกรรมต่างๆ ทั้งในเชิงพาณิชย์ การศึกษา และการปกครอง ก็ย่อมต้องมีการคำนึงถึงเรื่องความมั่นคงของระบบว่ามีลักษณะอย่างไร เพื่อจะได้มีการพัฒนาหรือปรับปรุงให้มีประสิทธิภาพที่ดียิ่งขึ้น

จากการศึกษาข้อมูลเอกสารและงานวิจัยที่เกี่ยวข้องกับความมั่นคงของเว็บเซอร์วิซ (Security of Web Service) สามารถแบ่งกลุ่มงานวิจัยออกเป็น 3 กลุ่ม ดังนี้

2.2.1 กลุ่มงานวิจัยที่เสนอการวัดความมั่นคงสำหรับเว็บเซอร์วิซทางอ้อม

งานวิจัย [20] ของ Artaiam และ Senivongse ได้นำเสนอการเฝ้าสังเกตคุณภาพการให้บริการบนฝั่งเซิร์ฟเวอร์สำหรับเว็บเซอร์วิซ โดยวัดค่าคุณภาพการบริการ (Quality of Services: QoS) จำนวน 6 ด้าน ซึ่งด้านหนึ่งในนั้น คือความมั่นคง (Security) โดยวิธีการที่นำเสนอเป็นการวัดค่าความมั่นคงจากคะแนนซีวีเอสเอส (CVSS) ที่ได้จากข้อมูลรายการจุดอ่อนซีวีอี (CVE) ที่เกี่ยวข้องกับผลิตภัณฑ์ซอฟต์แวร์ที่มีการติดตั้งอยู่บนเครื่องเซิร์ฟเวอร์ของผู้ให้บริการในทำนองเดียวกัน Nitan และ Teng-amnuay [21] ได้ศึกษาถึงวิธีการประเมินจุดอ่อนด้านซอฟต์แวร์ของผลิตภัณฑ์เว็บเซอร์วิซโดยใช้การค้นหาจุดอ่อนในรายการซีวีอี และมีการจัดกลุ่มจุดอ่อนของเว็บเซอร์วิซออกเป็น 3 รูปแบบ ได้แก่ 1) ประเภทของจุดอ่อน เป็นการจัดกลุ่มของลักษณะการโจมตีระบบตามความผิดพลาดที่มีในระบบ 2) จุดที่เกิดจุดอ่อน เป็นการแบ่งตามตำแหน่งที่เกิดจุดอ่อนว่าอยู่ส่วนใดของระบบ 3) ลักษณะความเสียหาย เป็นการจัดกลุ่มตามลักษณะความเสียหายที่เกิดขึ้น อันนำไปสู่การสูญเสียความเป็นความลับ การสูญเสียบูรณภาพ และการสูญเสียสภาพพร้อมใช้งาน นอกจากนั้นได้มีการนำเสนอวิธีการจำแนกความรุนแรงของผลกระทบที่ได้รับของความเสียหายที่เกิดขึ้น ทั้งทางด้านการรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งาน โดยแยกจุดอ่อนของผลิตภัณฑ์เว็บเซอร์วิซเป็นจุดอ่อนของเครื่องมือที่ใช้ในการพัฒนาเว็บเซอร์วิซ (Development Tools) และจุดอ่อนของเครื่องมือที่ใช้ในการสนับสนุนการให้บริการ (Runtime Service Tools) และในการประเมินได้นำค่าของผลกระทบมาคำนวณหาค่าและเปรียบเทียบคะแนนความเสียหายต่อการโจมตีเว็บเซอร์วิซ งานวิจัยทั้งสองงานข้างต้นเป็นการวัดความมั่นคงที่ระดับสภาพแวดล้อมในฝั่งเครื่องเซิร์ฟเวอร์แต่เพียงอย่างเดียว โดยวิเคราะห์จากจุดอ่อนของผลิตภัณฑ์ซอฟต์แวร์ในเครื่องเซิร์ฟเวอร์จากรายการซีวีอี

2.2.2 กลุ่มงานวิจัยที่เสนอการวัดความมั่นคงสำหรับเว็บเซอร์วิซทางตรง

งานวิจัย [22] ของ Pang และ Peng ได้นำเสนอระบบการประเมินความเสี่ยงด้านความมั่นคงของเว็บเซอร์วิซ ซึ่งมีการพิจารณาปัจจัย 3 ด้าน ได้แก่ 1) ด้านการระบุตัวสินทรัพย์ (Asset Identify) ซึ่งแบ่งประเภทตามด้านการรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งาน 2) ด้านการกราดตรวจจุดอ่อน (Vulnerability Scanning) โดยใช้โปรแกรมเนสซัส (Nessus) ทำการกราดตรวจจุดอ่อนในเว็บเซอร์วิซ จากการกราดตรวจดังกล่าวสามารถแยกผลความเสี่ยงได้เป็น ต่ำ (Low) ปานกลาง (Medium) และสูง (High) และ 3) ด้านการสำรวจภัยคุกคาม (Threat Survey) ได้พิจารณาเกรดความเสี่ยงของเว็บเซอร์วิซโดยการตอบแบบสอบถามทั้ง 8 หมวด ได้แก่ การออกใบรับรอง (Certification) การกำหนดสิทธิ์การเข้าใช้ การรักษาความลับ การบูรณภาพ สภาพ

พร้อมใช้งาน การตรวจสอบและการไม่สามารถโต้แย้งได้ (Audit and Incontestability) ความมั่นคงของข้อมูลโซป และอื่นๆ จากนั้นนำทั้ง 3 ด้านมาพิจารณาในตารางเมทริกซ์การคำนวณความเสี่ยงเพื่อให้ได้เป็นเกรดความเสี่ยงของความมั่นคงเว็บเซอร์วิซทั้งหมด 9 เกรด ส่วน Jiang Chen และ Deng [23] ได้นำเสนอวิธีการประเมินความมั่นคงบนพื้นฐานของแบบจำลอง สไตรด์ (STRIDE Model) สำหรับเว็บเซอร์วิซ โดยพิจารณาจาก 1) การประเมินระดับความมั่นคงของเซอร์วิซ (Degree of Security Evaluation of Service) จากคุณสมบัติความสามารถด้านความมั่นคงของเว็บเซอร์วิซและผู้ใช้บริการ 2) การประเมินระดับความมั่นคงของผู้ให้บริการ (Degree of Security Evaluation of Web Service Providers) และ 3) การประเมินระดับความเสี่ยงสำหรับเว็บเซอร์วิซ (Degree of Risk Evaluation for Web Service) จากนั้นจึงนำผลการประเมินทั้ง 3 แบบมารวมกันให้ได้ผลลัพธ์เป็นระดับความเสี่ยงรวมของเว็บเซอร์วิซ

2.2.3 กลุ่มงานวิจัยที่เสนอการวัดความมั่นคงแบบอื่น

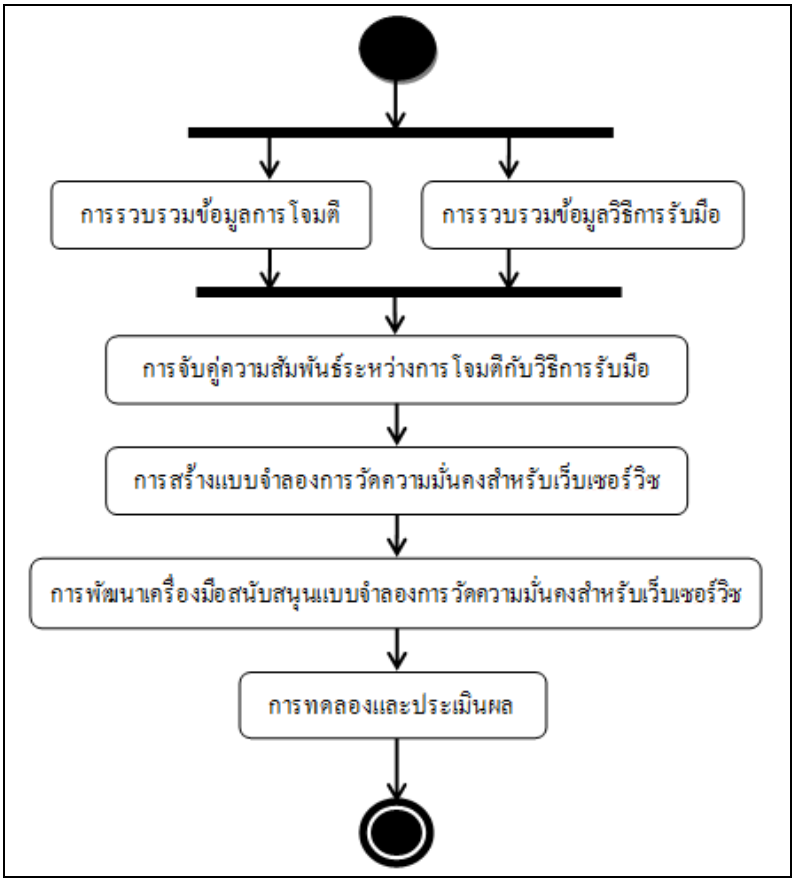
งานวิจัย [24] ของ Charpentier ได้นำเสนอวิธีการให้คะแนนความมั่นคงของเว็บแอปพลิเคชัน โดยแบ่งเป็นปัจจัย 2 ด้าน ปัจจัยแรกคือด้านดีเลิศ (Excellent) แทนจุดดีของระบบ ซึ่งพิจารณาจากความต้องการด้านความมั่นคง (Security Requirement) ในแต่ละหลักเกณฑ์ (Criteria) โดยมีการประเมินไว้ 3 แบบ ได้แก่ 1) จำเป็นต้องปรับปรุง (Needs Improvement) คือ ไม่ได้ให้ความสำคัญทางด้านความมั่นคง 2) พอใช้ (Fair) คือ มีการป้องกันโดยใช้วิธีตามมาตรฐานข้อปฏิบัติที่ดีที่สุดในอุตสาหกรรม (Industry Best Practice) และ 3) ดีเลิศ (Excellent) คือ มีการป้องกันที่มากกว่ามาตรฐานข้อปฏิบัติที่ดีที่สุดในอุตสาหกรรม ปัจจัยด้านที่สองคือด้านความเสี่ยง (Risk) แทนข้อด้อย พิจารณาจากความยากในการใช้ประโยชน์จากซอฟต์แวร์เพื่อการโจมตี (Difficulty of Exploit) และผลกระทบทางธุรกิจ (Business Impact) จากนั้นนำปัจจัยทั้ง 2 ด้านมาให้คะแนนตาม 11 หลักเกณฑ์ (Common Criteria) ได้แก่ 1) การพิสูจน์ตัวจริง 2) การกำหนดสิทธิ์การใช้งาน 3) การทำให้อินพุตของผู้ใช้ปลอดภัย (User's Input Sanitization) 4) การจัดการข้อผิดพลาดและการรั่วไหลของข้อมูล (Error Handling and Information Leakage) 5) ความซับซ้อนของรหัสผ่าน/พิน (Passwords/PIN Complexity) 6) การรักษาความลับของข้อมูลผู้ใช้ (User's Data Confidentiality) 7) กลไกของเซสชัน (Session Mechanism) 8) การจัดการแพทช์ (Patch Management) 9) ส่วนต่อประสานของการดูแลระบบ (Administration Interface) 10) ความมั่นคงในการสื่อสาร (Communication Security) และ 11) การเปิดเผยบริการของบุคคลที่สาม (Third-Party Services Exposure) แล้วนำผลที่ได้จากแต่ละหลักเกณฑ์มาคำนวณเป็นค่าคะแนนระดับความมั่นคง

บทที่ 3

แนวคิดและวิธีดำเนินการวิจัย

จากงานวิจัยที่เกี่ยวข้องเห็นได้ว่ามีการนำวิธีการต่างๆมาใช้ประเมินความมั่นคงของเว็บเซอร์วิซ แต่ยังไม่มีการนำวิธีการรับมือต่อการโจมตีสำหรับเว็บเซอร์วิซมาประยุกต์เพื่อสร้างแบบจำลองการวัดความมั่นคงในลักษณะเชิงตัวเลขหรือแบ่งเป็นระดับอย่างชัดเจน ดังนั้น งานวิจัยนี้จึงมีแนวคิดในการสร้างแบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซขึ้น เพื่อสามารถประเมินให้เห็นถึงความสามารถในการป้องกันตนเองของเว็บเซอร์วิซโดยผู้ให้บริการ ผู้วิจัยได้รวบรวมวิธีการรับมือต่อการโจมตีที่มีผลต่อเว็บเซอร์วิซ เพื่อนำมาพิจารณาหาความสัมพันธ์ในแง่มุมความสามารถในการจัดให้เว็บเซอร์วิซมีวิธีการรับมือต่อการโจมตี ที่ส่งผลกระทบต่อคุณสมบัติต่างๆด้านความมั่นคง จากนั้นจึงทำการวิเคราะห์และวัดผลให้อยู่ในรูปคะแนนความมั่นคง ผู้วิจัยได้นำแนวคิดการสร้างแบบจำลองจาก [25] มาปรับใช้เพื่อให้ได้ค่าคะแนนและระดับความมั่นคงของเว็บเซอร์วิซ

ภาพรวมของวิธีดำเนินการวิจัยประกอบไปด้วย 5 ส่วน ดังภาพที่ 3.1



ภาพที่ 3.1 แผนภาพวิธีดำเนินการวิจัย

3.1 การรวบรวมข้อมูลการโจมตีและวิธีการรับมือของเว็บเซอร์วิซ

การรวบรวมข้อมูลที่นำมาใช้ในงานวิจัย ประกอบไปด้วย 2 ข้อมูลหลัก ได้แก่ ข้อมูลการโจมตีและข้อมูลวิธีการรับมือการโจมตีที่มีผลกับการให้บริการเว็บเซอร์วิซ

3.1.1 การรวบรวมข้อมูลการโจมตี

การรวบรวมข้อมูลการโจมตีที่มีผลกระทบกับการให้บริการของเว็บเซอร์วิซได้รวบรวมข้อมูลจาก [2-5] โดยคัดเลือกเฉพาะการโจมตีที่สามารถนำมาปรับใช้ให้เข้ากับงานวิจัยได้ แต่ละการโจมตีจะมีคุณสมบัติ [3] ได้แก่ ความรุนแรงของการโจมตี (SEV: Typical Severity) โอกาสการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตี (LOE: Typical Likelihood of Exploit) ผลกระทบด้านการรักษาความลับ (CON: Confidentiality Impact) ผลกระทบด้านบูรณภาพ (INT: Integrity Impact) และผลกระทบด้านสภาพพร้อมใช้งาน (AVA: Availability Impact) ซึ่งได้มีการแบ่งระดับของแต่ละคุณสมบัติไว้ดังนี้

- ความรุนแรงของการโจมตี (SEV) มี 5 ระดับ ได้แก่ สูงมาก (VH: Very High) สูง (H: High) ปานกลาง (M: Medium) ต่ำ (L: Low) และต่ำมาก (VL: Very Low)
- โอกาสการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตี (LOE) มี 6 ระดับ ได้แก่ สูงมาก (VH: Very High) สูง (H: High) ปานกลาง (M: Medium) ต่ำ (L: Low) ต่ำมาก (VL: Very Low) และไม่ได้กำหนด (N/A: Not Available)
- ผลกระทบด้านการรักษาความลับ (CON) ผลกระทบด้านบูรณภาพ (INT) และผลกระทบด้านสภาพพร้อมใช้งาน (AVA) มี 4 ระดับ ได้แก่ สูง (H: High) ปานกลาง (M: Medium) ต่ำ (L: Low) และไม่ได้กำหนด (N/A: Not Available)

และสามารถจำแนกหมวดหมู่ของการโจมตีออกเป็น 2 แบบ ได้แก่ การจำแนกตามประเภทการโจมตี (Attack Type) [2] และจำแนกตามตำแหน่งการโจมตี (Attack Point) [5] ดังตารางที่ 3.1

ตารางที่ 3.1 รายละเอียดการโจมตีที่มีผลกระทบกับการให้บริการของเว็บเซอร์วิซ

No.	Attack Name	Characteristics					Attack Type	Attack Point
		SEV	LOE	CON	INT	AVA		
1	SQL Injection through SOAP Parameter Tampering	VH	H	H	H	H	Command Injection	Service Attacks
2	XQuery Injection	VH	H	H	H	H	Command Injection	Service Attacks
3	Overflow Buffers	VH	H	H	H	H	Privilege Escalation Attacks	Service Communication Attack
4	Man in the Middle Attack	VH	VH	H	H	H	Privilege Escalation Attacks	Service Communication Attack
5	WSDL Phishing	VH	H	H	H	L	Reconnaissa-nce Attacks	Service Endpoint Attacks
6	WSDL Scanning	H	H	M	M	H	Reconnaissa-nce Attacks	Service Endpoint Attacks
7	Using Unpublished Web Service APIs	H	M	H	M	L	Privilege Escalation Attacks	Service Attacks
8	Dictionary-Based Password Attack	H	M	H	M	L	Privilege Escalation Attacks	Service Authentication Attacks
9	XPath Injection	H	H	H	H	M	Command Injection	Service Attacks
10	Leveraging Race Conditions	H	H	L	H	M	Privilege Escalation Attacks	Service Attacks
11	Session Fixation	H	M	H	H	L	Privilege Escalation Attacks	Service Session Attacks
12	Reflection Attack in Authentication Protocol	H	H	H	H	L	Privilege Escalation Attacks	Service Authentication Attacks
13	Exploitation of Session Variables, Resource IDs and Other Trusted Credentials	H	H	H	H	L	Privilege Escalation Attacks	Service Session Attacks

ตารางที่ 3.1 รายละเอียดการโจมตีที่มีผลกระทบกับการให้บริการของเว็บเซอร์วิซ (ต่อ)

No.	Attack Name	Characteristics					Attack Type	Attack Point
		SEV	LOE	CON	INT	AVA		
14	Password Brute Forcing	H	M	H	H	L	Privilege Escalation Attacks	Service Authentication Attacks
15	Try Common (Default) Username and Passwords	H	M	H	H	M	Privilege Escalation Attacks	Service Authentication Attacks
16	SQL Injection	H	VH	H	H	H	Command Injection	Service Attacks
17	XML Schema Poisoning	H	N/A	N/A	**N/A***	**N/A***	Attacks on Integrity and DoS	Service Message Template Attacks
18	XML Parser Attacks	M	M	M	H	H	DoS	Service Message Attacks
19	External Entity Attack	M	N/A	N/A	**N/A***	**N/A***	Attacks on Integrity	Service Message Template Attacks
20	XML Ping of Death	M	N/A	N/A	N/A	**N/A***	DoS	Service Communication Attack
21	SOAP Parameter Tampering	M	N/A	**N/A***	**N/A***	**N/A***	Attacks on Integrity	Service Attacks
22	Resource Depletion through DTD Injection in SOAP Message	M	N/A	N/A	**N/A***	**N/A***	DoS	Service Attacks
23	Symlink Attacks	M	N/A	N/A	**N/A***	**N/A***	Privilege Escalation Attacks	Service Attacks
24	XML Routing Detour	M	N/A	**N/A***	**N/A***	**N/A***	Attacks on Integrity	Service Protocol Attacks
25	Sniffing	M	M	**N/A***	**N/A***	N/A	Attacks on Confidentiality	Service Communication Attack
26	Resource Depletion through Flooding	M	N/A	N/A	N/A	**N/A***	DoS	Service Communication Attack
27	Principal Spoofing	M	N/A	N/A	N/A	**N/A***	Attacks on Integrity	Service Attacks

ตารางที่ 3.1 รายละเอียดการโจมตีที่มีผลกระทบกับการให้บริการของเว็บเซอร์วิซ (ต่อ)

No.	Attack Name	Characteristics					Attack Type	Attack Point
		SEV	LOE	CON	INT	AVA		
28	Detect Unpublicized Web Services	L	N/A	N/A*	N/A	N/A	Reconnaissa-nce Attacks	Service Attacks

จากตารางที่ 3.1 ระดับค่าคุณสมบัติการโจมตี **N/A*** หมายถึงค่าที่ได้กำหนดให้มีการเปลี่ยนแปลงในภายหลังซึ่งจะกล่าวในหัวข้อที่ 3.3.2

3.1.2 การรวบรวมวิธีการรับมือการโจมตี

การรวบรวมข้อมูลวิธีการรับมือการโจมตีเว็บเซอร์วิซได้ทำการรวบรวมข้อมูลจาก [2, 3, 5, 7, 8, 17] โดยสามารถจำแนกวิธีการรับมือได้ 69 รายการ ดังตารางที่ 3.2

ตารางที่ 3.2 วิธีการรับมือการโจมตีเว็บเซอร์วิซ

No.	Countermeasures
1	**WS-Security Mechanisms**
1.1	XML Encryption
1.2	XML Signature
1.3	Security Tokens
2	**Transport-level Security Mechanisms**
3	**Schema Validation**
3.1	Defining whether the incoming messages have to be validated against the underlying message schema
3.2	Defining the level of validation that needs to be enforced for schema validation
3.3	Defining definition of additional validation rules that can be performed on the message element or attributes
4	**Schema Hardening**
5	**Service Virtualization**
6	**Strong Input Validation**
7	**Error Information Sanitization**
8	**Use of Parameterized Queries**
9	**Safe Programming**
10	**Memory Allocation Countermeasures**
11	**Compiler-Based Countermeasures**
12	**Library-Based Countermeasures**
13	**Use of WS-Addressing**
14	**XSL Validators**
15	**WSDL Reduction**
16	**Strong Password Policy**

ตารางที่ 3.2 วิธีการรับมือการโจมตีเว็บเซอร์วิซ (ต่อ)

No.	Countermeasures
17	**Configuration Rules and Policies on the XML Firewall**
17.1	Restricting the size of the XML messages
17.2	Limiting the response time for every request
17.3	Limiting the number of elements and attributes per message
17.3.1	Defining the maximum amount of nesting allowed inside a particular element
17.3.2	Defining the maximum number of attributes allowed for a particular element
17.3.3	Defining the maximum number of elements allowed for each level in the tree
17.3.4	Allowing the policy to define whether recursion is allowed within the XML message. This should be switched on only in specific instances when the underlying schema of the message is extremely complex
17.4	XML DoS Protection
17.4.1	All requests from an IP address which is sending spurious messages should be blocked
17.4.2	The threshold number of requests at which the firewall should activate its exception management scenario
17.4.3	The threshold at which action, which might include notification, is taken when a service starts returning an unusually high number of errors or SOAP faults
17.4.4	The threshold at which action can be taken when an excessive number of HTTP unauthorized/forbidden errors are returned
17.4.5	The threshold at which action can be taken when message processing takes a large number of CPU cycles
17.4.6	Indicating the type of notification that is required
17.4.7	Indicating whether the XML firewall should automatically shut down the service if the threshold limit has been reached
17.4.8	Automatic restart of the service after the specified time interval
17.4.9	Defining the maximum number of requests for a service
18	**Other Countermeasures**
18.1	Creating a handshake mechanism for interacting with ad hoc WSDL or Web service to ensure validity
18.2	Configuring the XML processor to only retrieve external entities form trusted sources
18.3	Authenticating both services and their discovery, and protecting that authentication mechanism simply fixes the bulk of this problem
18.4	Using the correct SOAP and XMLRPC implementations
18.5	Suppressing external URI references to protect against malicious data
18.6	Do not expose the user accounts that have access to host commands to external entities
18.7	Filtering messages based on Web service name, or Web service URL
18.8	Configuring network access control to accept incoming message from a specific IP address
18.9	Implementing a password throttling mechanism
18.10	Passwords need to be recycled to preventing aging

ตารางที่ 3.2 วิธีการรับมือการโจมตีเว็บเซอร์วิซ (ต่อ)

No.	Countermeasures
18.11	Delete all default account credentials that may be put in by the product vendor
18.12	The use of HMAC to hash the response from the server can also be used to thwart reflection
18.13	Introducing a random nonce with each new connection
18.14	Using randomly generated file names for temporary files
18.15	Do not use Unix and Linux systems
18.16	Disallowing the inclusion of DTDs in SOAP messages
18.17	For an application that uses a known schema, use a local copy or a known good repository instead of schema reference supplied in the XML document
18.18	Database user used by the application in a particular context has the minimum needed privileges to the database such as Run XML parsing and query infrastructure with minimal privileges
18.19	Be aware of improper use of access function calls such as chown(), tempfile(), chmod(), etc. can cause a race condition
18.20	Using synchronization to control the flow of execution
18.21	Using static analysis tools to find race conditions
18.22	Performing input white list validation on all XML input
18.23	Regenerate the session ID after login
18.24	Check the originating IP address of the login request and any subsequent requests
18.25	Bind the session ID to user's SSL client certificate
18.26	Encrypt the data passed between the parties in particular the session key
18.27	Using industry standards session key generation mechanisms
18.28	Encrypting and/or signing the session ID
18.29	Using strong session identifiers that are protected in transit and at rest
18.30	Utilizing session timeout for all session IDs at runtime
18.31	Verify authenticity of all session IDs at runtime
18.32	Building throttling mechanism into the resource allocation
18.33	Providing for a timeout mechanism for allocated resources whose transaction does not complete within a specified interval
18.34	Providing for network flow control and traffic shaping to control access to the resources

3.2 การจับคู่ความสัมพันธ์ระหว่างการโจมตีกับวิธีการรับมือ

จากหัวข้อที่ 3.1 เมื่อพิจารณาตาม [2, 3, 5, 6, 8, 17] แล้วสามารถนำข้อมูลที่ได้มาจับคู่หาความสัมพันธ์ระหว่างการโจมตีกับวิธีการรับมือ เพื่อแสดงให้เห็นว่าวิธีการรับมือแต่ละรายการนั้นสามารถป้องกันและ/หรือบรรเทาการโจมตีใดได้ ดังตารางที่ 3.3

ตารางที่ 3.3 การจับคู่ความสัมพันธ์ระหว่างการโจมตีกับวิธีการรับมือ

Attack No.	Countermeasure No.																																
	1.1	1.2	1.3	2	3.1	3.2	3.3	4	5	6	7	8	9	10	11	12	13	14	15	16	17.1	17.2	17.3.1	17.3.2	17.3.3	17.3.4	17.4.1	17.4.2	17.4.3	17.4.4	17.4.5	17.4.6	17.4.7	17.4.8	17.4.9
1	✓	✓	✓	✓						✓	✓	✓						✓																
2																																		
3										✓			✓	✓	✓	✓																		
4	✓	✓	✓	✓																														
5																	✓																	
6									✓								✓		✓															
7																																		
8																				✓														
9										✓	✓	✓						✓																
10																✓																		
11			✓														✓																	
12																																		
13			✓																															
14																				✓														
15																				✓														
16										✓	✓	✓						✓																
17					✓	✓	✓		✓																									
18					✓	✓	✓	✓													✓	✓	✓	✓	✓	✓								
19																																		
20																											✓	✓	✓	✓	✓	✓	✓	✓	✓
21	✓	✓	✓	✓	✓	✓	✓																											
22																																		
23																																		
24	✓	✓	✓	✓					✓								✓																	
25	✓	✓	✓	✓																														
26																											✓	✓	✓	✓	✓	✓	✓	✓	✓
27	✓	✓	✓	✓																														
28																																		
CM-AT Totals	6	6	8	6	3	3	3	1	3	4	3	3	1	1	1	2	3	3	1	3	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2

ตารางที่ 3.3 การจับคู่ความสัมพันธ์ระหว่างการโจมตีกับวิธีการรับมือ (ต่อ)

Attack No.	Countermeasure No.																												
	18.1	18.2	18.3	18.4	18.5	18.6	18.7	18.8	18.9	18.10	18.11	18.12	18.13	18.14	18.15	18.16	18.17	18.18	18.19	18.20	18.21	18.22	18.23	18.24	18.25	18.26	18.27	18.28	18.29
1																		✓											
2																		✓				✓							
3																													
4																													
5	✓																												
6							✓																						
7			✓																										
8									✓																				
9																													
10																			✓	✓	✓								
11																							✓	✓	✓	✓			
12	✓											✓	✓																
13																											✓	✓	✓
14									✓	✓																			
15									✓	✓	✓																		
16																													
17																	✓												
18																													
19		✓		✓	✓	✓																							
20																													
21																													
22																✓													
23														✓	✓														
24																													
25																													
26																													
27								✓																					
28							✓																						
CM-AT Totals	2	1	1	1	1	1	2	1	3	2	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1

ตารางที่ 3.3 การจับคู่ความสัมพันธ์ระหว่างการโจมตีกับวิธีการรับมือ (ต่อ)

Attack No.	Countermeasure No.					AT-CM Totals
	18.30	18.31	18.32	18.33	18.34	
1						9
2						2
3						5
4						4
5						2
6						4
7						1
8						2
9						4
10						4
11						6
12						3
13	✔	✔				6
14						3
15						4
16						4
17						5
18						10
19						4
20			✔	✔	✔	12
21						7
22						1
23						2
24						6
25						4
26						9
27						5
28						1
CM-AT Totals	1	1	1	1	1	

จากตารางที่ 3.3 สามารถนำมาออกแบบแผ่นแบบการจัดให้มีวิธีการรับมือ (Countermeasure Provision Template) สำหรับให้ผู้ประเมินซึ่งอาจเป็นตัวผู้ให้บริการเองได้เห็นภาพรวมของวิธีการรับมือการโจมตีเว็บเซอร์วิซ ซึ่งได้มีการจัดหาไว้ แสดงดังตารางที่ 3.4 โดยแบ่งความสำคัญตามระดับความรุนแรงของการโจมตี [3] ออกเป็น 4 กลุ่ม ได้แก่

1) กลุ่มลำดับความสำคัญสีแดง (Red Priority) คือ กลุ่มของการโจมตีที่มีระดับความรุนแรงที่สูงมาก ได้แก่ การโจมตีที่ 1 – การโจมตีที่ 5

2) กลุ่มลำดับความสำคัญสีส้ม (Orange Priority) คือ กลุ่มของการโจมตีที่มีระดับความรุนแรงที่สูง ได้แก่ การโจมตีที่ 6 – การโจมตีที่ 17

3) กลุ่มลำดับความสำคัญสีเหลือง (Yellow Priority) คือ กลุ่มของการโจมตีที่มีระดับความรุนแรงที่ปานกลาง ได้แก่ การโจมตีที่ 18 – การโจมตีที่ 27

4) กลุ่มลำดับความสำคัญสีน้ำตาล (Brown Priority) คือ กลุ่มของการโจมตีที่มีระดับความรุนแรงที่ต่ำ ได้แก่ การโจมตีที่ 28

การเรียงลำดับในลักษณะดังกล่าวมีวัตถุประสงค์เพื่อให้ผู้ให้บริการได้มีองค์ความรู้และเข้าใจถึงความสัมพันธ์ระหว่างวิธีการรับมือสำหรับแต่ละการโจมตี โดยผู้ให้บริการสามารถพิจารณาจากลำดับความสำคัญของการจัดให้มีวิธีการรับมือได้ตามลำดับความสำคัญของการโจมตี ซึ่งแผ่นแบบนี้จะนำไปใช้ในการให้คะแนนร้อยละของระดับการจัดให้มีวิธีการรับมือต่อการโจมตี ในหัวข้อที่ 3.3.1

ตารางที่ 3.4 แผ่นแบบการจัดให้มีวิธีการรับมือการโจมตี

1.SQL Injection through SOAP Parameter Tampering	**2. XQuery Injection**	**3. Overflow Buffers**	**4. Man in the Middle Attack**
□ WS-Security Mechanisms ○ XML Encryption ○ XML Signature ○ Security Tokens □ Transport-level Security Mechanisms □ Strong Input Validation □ Error Information Sanitization □ Use of Parameterized Queries □ Database user used by the application in a particular context has the minimum needed privileges to the database □ XSL Validator	□ Performing input white list validation on all XML input □ Database user used by the application in a particular context has the minimum needed privileges to the database	□ Strong Input Validation □ Safe Programming □ Memory Allocation Countermeasures □ Compiler-Based Countermeasures □ Library-Based Countermeasures	□ WS-Security Mechanisms ○ XML Encryption ○ XML Signature ○ Security Tokens □ Transport-Level Security Mechanisms
5. WSDL Phishing	**6. WSDL Scanning**	**7. Using Unpublished Web Service APIs**	**8. Dictionary-Based Password Attack**
□ Use of WS -Addressing □ Creating a handshake mechanism for interacting with ad hoc WSDL or Web service to ensure validity	□ Service Virtualization □ Use of WS-Addressing □ WSDL reduction □ Filtering messages based on Web service name, or Web service URL	□ Authenticating both service and their discovery, and protecting that authentication mechanism simply fixes the bulk of this problem	□ Strong Password Policy □ Implementing a password throttling mechanism
9. XPath Injection	**10. Leveraging Race Conditions**	**11. Session Fixation**	**12. Reflection Attack in Authentication Protocol**
□ Strong Input Validation □ Use of Parameterized Queries □ Error Information Sanitization □ XSL Validator	□ Library-Based Countermeasures □ Be aware of improper use of access function calls such as chown(), tempfile(), chmod(), etc. can cause a race condition □ Using synchronization to control the flow of execution □ Using static analysis tools to find race conditions	□ Security Tokens □ Use of WS-Addressing □ Regenerate the session ID after login □ Check the originating IP address of the login request □ Bind the session ID to user's SSL client certificate □ Encrypt the data passed between the parties in particular the session key	□ Creating a handshake mechanism for interacting with ad hoc WSDL or Web service to ensure validity □ The use of HMAC to hash the response from the server can also be used to thwart reflection □ Introducing a random nonce with each new connection
13. Exploitation of Session Variables, Resource IDs and Other Trusted Credentials	**14. Password Brute Forcing**	**15. Try Common (Default) Username and Passwords**	**16. SQL Injection**
□ Security Tokens □ Using industry standards session key generation mechanisms □ Encrypting and/or signing the session ID □ Using strong session identifiers that are protected in transit and at rest □ Utilizing a session timeout for all session IDs at runtime □ Verify of authenticity of all session IDs at runtime	□ Strong Password Policy □ Implementing a password throttling mechanism □ Passwords need to be recycled to prevent aging	□ Strong Password Policy □ Implementing a password throttling mechanism □ Passwords need to be recycled to prevent aging □ Delete all default account credentials that may be out in by the product vendor	□ Strong Input Validation □ Error Information Sanitization □ Use of Parameterized Queries □ XSL Validator

ตารางที่ 3.4 แผ่นแบบการจัดให้มีวิธีการรับมือการโจมตี (ต่อ)

17. XML Schema Poisoning	**18. XML Parser Attacks**	**19. External Entity Attack**	**20. XML Ping of Death**
□ Schema Validation ○ Defining whether the incoming messages have to be validated against the underlying message schema ○ Defining the level of validation that needs to be enforced for schema validation ○ Defining definition of additional validation rules that can be performed on the message element or attributes □ Service Virtualization □ For applications that use a known schema, use a local copy or a known good repository instead of the schema reference supplied in the XML document	□ Schema Validation ○ Defining whether the incoming messages have to be validated against the underlying message schema ○ Defining the level of validation that needs to be enforced for schema validation ○ Defining definition of additional validation rules that can be performed on the message element or attributes □ Schema Hardening □ Restricting the size of the XML messages □ Limiting the response time for every request □ Limiting the number of elements and attributes per message ○ Defining the maximum amount of nesting allowed inside a particular element ○ Defining the maximum number of attributes allowed for particular element ○ Defining the maximum number of elements allowed for each level in the tree ○ Allowing the policy to define whether recursion is allowed within the XML message	□ Configuring the XML processor to only retrieve external entities from trusted sources □ Using the correct SOAP and XMLRPC implementations □ Suppressing external URI references to protect against malicious data □ Do not expose the user accounts that have access to host commands to external entities	□ XML DoS Protection (XML Ping of Death and Flooding) ○ All requests from an IP address which is sending spurious message should be blocked ○ The threshold number of requests at which the firewall should activate its exception management scenario ○ The threshold at which action, which might include notification, is taken when a service starts returning an unusually high number of errors or SOAP faults ○ The threshold at which action can be taken when an excessive number of HTTP Unauthorized/forbidden errors are returned ○ The threshold at which action can be taken when message processing takes a large number of CPU cycles ○ Indicating the type of notification that is required ○ Indicating whether the XML firewall should automatically shut down the service if the threshold limit has been reached ○ Automatic restart of the service after the specified time interval ○ Defining the maximum number of requests for a service □ Building throttling mechanism into the resource allocation □ Providing for a timeout mechanism for allocated resources whose transaction does not complete within a specified interval □ Providing for network flow control and traffic shaping to control access to the resources
21. SOAP Parameter Tampering	**22. Resource Depletion through DTD Injection in SOAP Message**	**23. Symlink Attacks**	**24. XML Routing Detour**
□ WS-Security Mechanisms ○ XML Encryption ○ XML Signature ○ Security Tokens	□ Disallowing the inclusion of DTDs in SOAP messages	□ Using randomly generated file names for temporary files □ Do not use Unix and Linux systems	□ WS-Security Mechanisms ○ XML Encryption ○ XML Signature ○ Security Tokens

ตารางที่ 3.4 แผ่นแบบการจัดให้มีวิธีการรับมือการโจมตี (ต่อ)

□ Transport-Level Security Mechanisms □ Schema Validation ○ Defining whether the incoming messages have to be validated against the underlying message schema ○ Defining the level of validation that needs to be enforced for schema validation ○ Defining definition of additional validation rules that can be performed on the message element or attributes			□ Transport-Level Security Mechanisms □ Service Virtualization □ Use of WS-Addressing
25. Sniffing	**26. Resource Depletion through Flooding**	**27. Principal Spoofing**	**28. Detect Unpublicized Web Services**
□ WS-Security Mechanisms ○ XML Encryption ○ XML Signature ○ Security Tokens □ Transport-Level Security Mechanisms	□ XML DoS Protection (XML Ping of Death and Flooding) ○ All requests from an IP address which is sending spurious message should be blocked ○ The threshold number of requests at which the firewall should activate its exception management scenario ○ The threshold at which action, which might include notification, is taken when a service starts returning an unusually high number of errors or SOAP faults ○ The threshold at which action can be taken when an excessive number of HTTP Unauthorized/forbidden errors are returned ○ The threshold at which action can be taken when message processing takes a large number of CPU cycles ○ Indicating the type of notification that is required ○ Indicating whether the XML firewall should automatically shut down the service if the threshold limit has been reached ○ Automatic restart of the service after the specified time interval ○ Defining the maximum number of requests for a service	□ WS-Security Mechanisms ○ XML Encryption ○ XML Signature ○ Security Tokens □ Transport-Level Security Mechanisms □ Configuring network access control to accept incoming message from a specific IP address	□ Filter messages based on Web service names, or Web service URL

3.3 การสร้างแบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซ

ในงานวิจัยนี้จะประเมินความมั่นคงของเว็บเซอร์วิซโดยกำหนดตัววัดและข้อมูลที่ต้องการเพื่อให้ได้ข้อมูลของตัววัดนั้น โดยพิจารณาจากความสามารถในการจัดให้เว็บเซอร์วิซมีวิธีการรับมือต่อการโจมตี และคุณสมบัติต่างๆของการโจมตี ผู้วิจัยจึงได้นำเสนอแบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซไว้ดังนี้

$$S = R \times (A \times C) \tag{3.1}$$

แบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซ ประกอบไปด้วย 3 ส่วน คือ

1) C คือ ค่าความสามารถในการจัดให้มีวิธีการรับมือ (Countermeasure Provision Ability)

2) A คือ ค่าคุณสมบัติการโจมตี (Attack Characteristics)

3) R คือ ความสำคัญสัมพัทธ์ของความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติการโจมตี (Relative Importance of Countermeasure Provision Ability Regarding Attack Characteristics)

โดย S คือ ค่าความมั่นคงของเว็บเซอร์วิซ

องค์ประกอบทั้งสามส่วนมีรายละเอียด ดังต่อไปนี้

3.3.1 ค่าความสามารถในการจัดให้มีวิธีการรับมือ

ค่าความสามารถในการจัดให้มีวิธีการรับมือคือ ค่าความสามารถของเว็บเซอร์วิซในการจัดให้มีวิธีการรับมือต่อการโจมตีแต่ละประเภท โดยพิจารณาจากร้อยละของวิธีการรับมือต่อการโจมตีแต่ละประเภทที่มีการจัดให้เว็บเซอร์วิซมี ตามที่ระบุไว้ในแผ่นแบบการจัดให้มีวิธีการรับมือการโจมตีในตารางที่ 3.4 ระดับความสามารถในการจัดให้มีวิธีการรับมือการโจมตีแบ่งเป็น 4 ระดับ ดังตารางที่ 3.5

ตารางที่ 3.5 การกำหนดระดับความสามารถในการจัดให้มีวิธีการรับมือ

ความสามารถในการจัดให้มีวิธีการรับมือ (Countermeasure Provision Ability)	
ระดับ (Levels)	**คำอธิบาย** (Descriptions)
ดีมาก (Very Good) หรือ 3	ระดับที่มีการจัดให้มีวิธีการรับมือต่อการโจมตีอยู่ในช่วงร้อยละ 81-100
ดี (Good) หรือ 2	ระดับที่มีการจัดให้มีวิธีการรับมือต่อการโจมตีอยู่ในช่วงร้อยละ 41-80
พอใช้ (Fair) หรือ 1	ระดับที่มีการจัดให้มีวิธีการรับมือต่อการโจมตีอยู่ในช่วงร้อยละ 1-40
ควรปรับปรุง (Need Improvement) หรือ 0	ระดับที่ไม่มีการจัดให้มีวิธีการรับมือต่อการโจมตี

การกำหนดความสามารถในการจัดให้มีวิธีการรับมือตามร้อยละนั้น ตั้งอยู่บนข้อสมมติฐานที่ว่า วิธีการรับมือหนึ่งๆ อาจไม่สามารถป้องกันการโจมตีนั้นๆได้ 100% ดังนั้นถ้ามีการจัดให้มีวิธีการรับมือต่อการโจมตีหนึ่งๆ มากกว่าหนึ่งวิธีการ จะส่งผลให้มีโอกาสที่จะสามารถรับมือต่อการโจมตีนั้นๆได้ดียิ่งขึ้น

การหาค่าร้อยละสามารถคำนวณได้ดังสมการที่ (3.2) ซึ่งค่านี้เมื่อเทียบตามตารางที่ 3.5 แล้วจะนำไปใช้ในสมการที่ (3.3)

$$CM_i = \frac{CM_{PROVIDE\_i} \times 100}{CM_{TOTAL\_i}} \tag{3.2}$$

กำหนดให้

CM_i คือร้อยละความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตีแบบที่ i

โดย i = 1,…,28 จากตารางที่ 3.4

$CM_{PROVIDE\_i}$ คือจำนวนวิธีการรับมือต่อการโจมตีแบบที่ i ที่มีการจัดหาให้เว็บเซอร์วิซ

CM_{TOTAL_i} คือจำนวนวิธีการรับมือทั้งหมดต่อการโจมตีแบบที่ i

กำหนดให้ C เป็นเวกเตอร์ค่าความสามารถในการจัดให้เว็บเซอร์วิซมีวิธีการรับมือต่อการโจมตีทุกแบบ

$$C = \begin{bmatrix} C_{AT1} \\ C_{AT2} \\ . \\ . \\ . \\ C_{AT28} \end{bmatrix} \tag{3.3}$$

โดย

C_{ATi} เป็นค่ามาตรวัดความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตีแบบที่ i

โดย i = 1,..., 28 จากตารางที่ 3.4 และ C_{ATi} มีค่าเป็น 0,1,2 หรือ 3 ตามตารางที่ 3.5 โดยพิจารณาจากค่า CM_i

3.3.2 **คุณสมบัติการโจมตี**

ค่าคุณสมบัติแต่ละด้านของแต่ละการโจมตีจะเป็นค่าน้ำหนักที่นำมาใช้เพื่อพิจารณาคุณความดีของเว็บเซอร์วิซในด้านความสามารถในการจัดให้มีวิธีการรับมือ โดยมีแนวคิดที่ว่า ถ้าผู้ให้บริการมีความสามารถในการจัดให้มีวิธีการรับมือที่ดีและวิธีการรับมือนั้นมีโอกาสที่จะป้องกันการโจมตีที่มีค่าคุณสมบัติต่างๆของการโจมตีที่สูง แสดงว่าผู้ให้บริการมีความเอาใจใส่ในการให้บริการโดยคำนึงถึงคุณสมบัตินั้นๆซึ่งเป็นผลกระทบจากการโจมตีเป็นอย่างสูง โดยคุณสมบัติของการโจมตีแบ่งออกเป็น 5 ด้าน ได้แก่ ความรุนแรง โอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตี ผลกระทบด้านการรักษาความลับ ผลกระทบด้านบูรณภาพ และผลกระทบด้านสภาพพร้อมใช้งาน [3] ดังนี้

3.3.2.1 **ความรุนแรง** (SEV: Typical Severity)

ความรุนแรงเป็นผลผลิตของโอกาสและผลกระทบที่มีต่อซอฟต์แวร์ที่เป็นเป้าหมายว่าถ้าเกิดการโจมตีนี้ขึ้นจะมีความรุนแรงในระดับใด (ต่ำมาก ต่ำ ปานกลาง สูง สูงมาก) โดยระดับความรุนแรงนี้จะขึ้นอยู่กับบริบทที่เฉพาะเจาะจงของซอฟต์แวร์ที่เป็นเป้าหมายภายใต้ความหลากหลายของผลกระทบของเป้าหมาย/การโจมตีภายใต้เทคนิคและบริบท/ภารกิจที่แตกต่างกัน การกำหนด

ความรุนแรงนี้มีวัตถุประสงค์เพื่อการแสดงค่าเฉลี่ยโดยทั่วไปสำหรับการโจมตี แต่ละแบบเพื่อให้มีความเข้าใจและเอาใจใส่กับการโจมตีนั้นๆมากขึ้น ระดับความรุนแรงแสดงดังตารางที่ 3.6

ตารางที่ 3.6 การกำหนดระดับความรุนแรง

ความรุนแรง (Typical Severity)	
ระดับ (Levels)	**คำอธิบาย** (Descriptions)
สูงมาก (Very High) หรือ 5	ระดับความรุนแรงที่ได้ผ่านการพิจารณาจาก [3] แล้วว่าให้มีค่าที่สูงมาก โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 5
สูง (High) หรือ 4	ระดับความรุนแรงที่ได้ผ่านการพิจารณาจาก [3] แล้วว่าให้มีค่าที่สูง โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 4
ปานกลาง (Medium) หรือ 3	ระดับความรุนแรงที่ได้ผ่านการพิจารณาจาก [3] แล้วว่าให้มีค่าที่ปานกลาง โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 3
ต่ำ (Low) หรือ 2	ระดับความรุนแรงที่ได้ผ่านการพิจารณาจาก [3] แล้วว่าให้มีค่าที่ต่ำ โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 2
ต่ำมาก (Very Low) หรือ 1	ระดับความรุนแรงที่ได้ผ่านการพิจารณาจาก [3] แล้วว่าให้มีค่าที่ต่ำมาก โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 1

3.3.2.2 **โอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตี** (LOE: Typical Likelihood of Exploit)

เป็นโอกาสความสำเร็จในการโจมตีโดยพิจารณาจากสิ่งที่ต้องมีก่อนการโจมตี (Attack Prerequisites) พื้นผิวการโจมตีจุดอ่อนแอของเป้าหมาย (Targets Weakness Attack Surface) ทักษะที่ต้องใช้ (Skill Required) และทรัพยากรที่ต้องใช้ (Resource Required) และการดำเนินการป้องกัน (Implemented Blocking Solution) ที่มี โดยพิจารณาว่าโอกาสของการใช้ประโยชน์ดังกล่าวน่าจะมีค่าอยู่ในระดับใด (ต่ำมาก ต่ำ ปานกลาง สูง สูงมาก) โอกาสในการใช้ประโยชน์เพื่อการโจมตีนั้นๆ จะพิจารณาจากความหลากหลายของบริบทและปัจจัยที่เกื้อหนุน เช่น สภาพแวดล้อมของเป้าหมาย (Target Environment) พื้นผิวการโจมตีเป้าหมาย (Target Attack Surface) ทักษะของผู้โจมตี (Attacker Skill) ความรู้ในการโจมตี (Attack Knowledge) ฯลฯ การกำหนดโอกาสการใช้ประโยชน์นี้มีวัตถุประสงค์เพื่อแสดงค่าเฉลี่ยโดยทั่วไปสำหรับการโจมตีแต่ละแบบเพื่อให้มีความเข้าใจและเอาใจใส่กับการโจมตีนั้นๆมากขึ้น ระดับโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีแสดงดังตารางที่ 3.7

ตารางที่ 3.7 การกำหนดระดับโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตี

โอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตี (Typical Likelihood of Exploit)	
ระดับ (Levels)	**คำอธิบาย** (Descriptions)
สูงมาก (Very High) หรือ 5	ระดับโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีที่ได้ผ่านการพิจารณาจาก [3] แล้วว่าให้มีค่าที่สูงมาก โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 5
สูง (High) หรือ 4	ระดับโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีที่ได้ผ่านการพิจารณาจาก [3] แล้วว่าให้มีค่าที่สูง โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 4
ปานกลาง (Medium) หรือ 3	ระดับโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีที่ได้ผ่านการพิจารณาจาก [3] แล้วว่าให้มีค่าที่ปานกลาง โดยงานวิจัยนี้กำหนดค่าน้ำหนักนี้เป็น 3
ต่ำ (Low) หรือ 2	ระดับโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีที่ได้ผ่านการพิจารณาจาก [3] แล้วว่าให้มีค่าที่ต่ำ โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 2
ต่ำมาก (Very Low) หรือ 1	ระดับโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีที่ได้ผ่านการพิจารณาจาก [3] แล้วว่าให้มีค่าที่ต่ำมาก โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 1
ไม่มีข้อมูล (Not Available) หรือ 0	ระดับโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีที่ไม่สามารถสืบค้นได้ โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 0

3.3.2.3 **ผลกระทบด้านการรักษาความลับ** (CON: Confidentiality Impact)

ผลกระทบจากการละเมิดด้านการรักษาความลับจะขึ้นอยู่กับบริบทเฉพาะขององค์กร ระบบ แอปพลิเคชัน และสภาพแวดล้อมของเป้าหมายภายใต้การโจมตี ระดับผลกระทบด้านการรักษาความลับแสดงดังตารางที่ 3.8

ตารางที่ 3.8 การกำหนดระดับผลกระทบด้านการรักษาความลับ

ผลกระทบด้านการรักษาความลับ (Confidentiality Impact)	
ระดับ (Levels)	**คำอธิบาย** (Descriptions)
สูง (High) หรือ 3	ระดับผลกระทบด้านการรักษาความลับที่ได้ผ่านการพิจารณาจาก [3] แล้วว่าให้มีค่าที่สูง โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 3
ปานกลาง (Medium) หรือ 2	ระดับผลกระทบด้านการรักษาความลับที่ได้ผ่านการพิจารณาจาก [3] แล้วว่าให้มีค่าที่ปานกลาง โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 2
ต่ำ (Low) หรือ 1	ระดับผลกระทบด้านการรักษาความลับที่ได้ผ่านการพิจารณาจาก [3] แล้วว่าให้มีค่าที่ต่ำ โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 1
ไม่มีข้อมูล (Not Available) หรือ 0	ระดับผลกระทบด้านการรักษาความลับที่ไม่ได้มีการละเมิดในด้านนี้ โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 0

3.3.2.4 **ผลกระทบด้านบูรณภาพ** (INT: Integrity Impact)

ผลกระทบจากการละเมิดด้านบูรณภาพจะขึ้นอยู่กับบริบทเฉพาะขององค์กร ระบบ แอปพลิเคชัน และสภาพแวดล้อมของเป้าหมายภายใต้การโจมตี ระดับผลกระทบด้านบูรณภาพแสดงดังตารางที่ 3.9

ตารางที่ 3.9 การกำหนดระดับผลกระทบด้านบูรณภาพ

ผลกระทบด้านบูรณภาพ (Integrity Impact)	
ระดับ (Levels)	**คำอธิบาย** (Descriptions)
สูง (High) หรือ 3	ระดับผลกระทบด้านบูรณภาพที่ได้ผ่านการพิจารณาจาก [3] แล้วว่าให้มีค่าที่สูง โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 3
ปานกลาง (Medium) หรือ 2	ระดับผลกระทบด้านบูรณภาพที่ได้ผ่านการพิจารณาจาก [3] แล้วว่าให้มีค่าที่ปานกลาง โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 2
ต่ำ (Low) หรือ 1	ระดับผลกระทบด้านบูรณภาพที่ได้ผ่านการพิจารณาจาก [3] แล้วว่าให้มีค่าที่ต่ำ โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 1
ไม่มีข้อมูล (Not Available) หรือ 0	ระดับผลกระทบด้านบูรณภาพที่ไม่ได้มีการละเมิดในด้านนี้ โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 0

3.3.2.5 **ผลกระทบด้านสภาพพร้อมใช้งาน** (AVA: Availability Impact)

ผลกระทบจากการละเมิดด้านสภาพพร้อมใช้งานจะขึ้นอยู่กับบริบทเฉพาะขององค์กร ระบบ แอปพลิเคชัน และสภาพแวดล้อมของเป้าหมายภายใต้การโจมตีระดับผลกระทบด้านสภาพพร้อมใช้งานแสดงดังตารางที่ 3.10

ตารางที่ 3.10 การกำหนดระดับผลกระทบด้านสภาพพร้อมใช้งาน

ผลกระทบด้านสภาพพร้อมใช้งาน (Availability Impact)	
ระดับ (Levels)	**คำอธิบาย** (Descriptions)
สูง (High) หรือ 3	ระดับผลกระทบด้านสภาพพร้อมใช้งานที่ได้ผ่านการพิจารณาจาก [3] แล้วว่าให้มีค่าที่สูง โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 3
ปานกลาง (Medium) หรือ 2	ระดับผลกระทบด้านสภาพพร้อมใช้งานที่ได้ผ่านการพิจารณาจาก [3] แล้วว่าให้มีค่าที่ปานกลาง โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 2
ต่ำ (Low) หรือ 1	ระดับผลกระทบด้านสภาพพร้อมใช้งานที่ได้ผ่านการพิจารณาจาก [3] แล้วว่าให้มีค่าที่ต่ำ โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 1
ไม่มีข้อมูล (Not Available) หรือ 0	ระดับผลกระทบด้านสภาพพร้อมใช้งานที่ไม่ได้มีการละเมิดในด้านนี้ โดยงานวิจัยนี้ได้กำหนดค่าน้ำหนักนี้เป็น 0

จากข้อมูลคุณสมบัติของการโจมตีซึ่งกำหนดโดยผู้เชี่ยวชาญใน [3] พบว่ามีการโจมตีจำนวน 11 การโจมตี จาก 28 การโจมตี ที่มีเฉพาะค่าความรุนแรงเท่านั้น ดังนั้นในงานวิจัยนี้จึงได้ทำการกำหนดค่าเพิ่มเติมให้กับค่าโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตี ค่าผลกระทบด้านการรักษาความลับ ค่าผลกระทบด้านบูรณภาพ และค่าผลกระทบด้านสภาพพร้อมใช้งานสำหรับ 11 การโจมตีนั้น โดยมีเกณฑ์การพิจารณาเพื่อให้การวัดความมั่นคงของเว็บเซอร์วิซมีความสมบูรณ์มากขึ้น ดังนี้

1) สำหรับค่าโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตี (LOE) จะพิจารณาจากจำนวนการสืบค้นข้อมูลที่พบ โดยถ้าพบว่ามีเครื่องมือหรือโค้ดที่ถูกเปิดเผยก็จะให้ค่าน้ำหนักอยู่ในระดับปานกลาง (Medium)

2) ค่าผลกระทบด้านการรักษาความลับ (CON) ด้านบูรณภาพ (INT) และด้านสภาพพร้อมใช้งาน (AVA) พิจารณาจากลักษณะการโจมตีว่ามีการละเมิดในด้านใด โดยถ้าพบว่ามีการละเมิดในด้านนั้น ก็จะกำหนดให้ค่าน้ำหนักอยู่ในระดับปานกลาง (Medium)

โดยค่าคุณสมบัติของการโจมตีที่ผู้วิจัยกำหนดเพิ่มเติม จะกำกับด้วยเครื่องหมาย * ในสมการที่ (3.5)

การกำหนดค่าคุณสมบัติของการโจมตี แสดงอยู่ในรูปของเมตริกซ์ A:

$$A = \begin{array}{c} \begin{matrix} AT_1 & AT_2 & \dots & AT_{28} \end{matrix} \\ \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,28} \\ a_{2,1} & a_{2,2} & \dots & a_{2,28} \\ a_{3,1} & a_{3,2} & \dots & a_{3,28} \\ a_{4,1} & a_{4,2} & \dots & a_{4,28} \\ a_{5,1} & a_{5,2} & \dots & a_{5,28} \end{bmatrix} \end{array} \begin{matrix} \\ SEV \\ LOE \\ CON \\ INT \\ AVA \end{matrix} \quad (3.4)$$

โดย

$a_{i,j}$ คือค่าคุณสมบัติของการโจมตีที่ i ของการโจมตีแบบที่ j

i คือแถวของ A โดย i = 1,…,5 ใช้แทนคุณสมบัติของการโจมตี ได้แก่ SEV, LOE, CON, INT และ AVA ตามลำดับ

j คือหลักของ A โดย j = 1,…,28 ใช้แทนลำดับของการโจมตีที่พิจารณาตามตารางที่ 3.4

ค่า A กำหนดได้ดังนี้

$$A = \begin{array}{c} \begin{matrix} AT_1 & AT_2 & AT_3 & \dots & & & & & & & & & & & & & & & & & & & & & & & & & \dots & & & AT_{26} & AT_{27} & AT_{28} \end{matrix} \\ \begin{bmatrix} 5 & 5 & 5 & 5 & 5 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 2 \\ 4 & 4 & 4 & 5 & 4 & 4 & 3 & 3 & 4 & 4 & 3 & 4 & 4 & 3 & 3 & 5 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 3^* & 0 & 0 & 0 \\ 3 & 3 & 3 & 3 & 3 & 2 & 3 & 3 & 3 & 1 & 3 & 3 & 3 & 3 & 3 & 3 & 0 & 2 & 0 & 0 & 2^* & 0 & 0 & 2^* & 2^* & 0 & 0 & 2^* \\ 3 & 3 & 3 & 3 & 3 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 2^* & 3 & 2^* & 0 & 2^* & 2^* & 2^* & 2^* & 2^* & 0 & 0 & 0 \\ 3 & 3 & 3 & 3 & 1 & 3 & 1 & 1 & 2 & 2 & 1 & 1 & 1 & 1 & 2 & 3 & 2^* & 3 & 2^* & 2^* & 2^* & 2^* & 2^* & 2^* & 0 & 2^* & 2^* & 0 \end{bmatrix} \end{array} \begin{matrix} \\ SEV \\ LOE \\ CON \\ INT \\ AVA \end{matrix} \quad (3.5)$$

3.3.3 ความสำคัญสัมพัทธ์ของความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติการโจมตี

ความสำคัญสัมพัทธ์ของความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติของการโจมตี คือค่าน้ำหนักที่ผู้ประเมินกำหนดให้กับความสามารถในการจัดให้มีวิธีการรับมือเมื่อคำนึงถึงคุณสมบัติแต่ละด้านของการโจมตีแบบต่างๆ โดยแบ่งออกได้ดังนี้

3.3.3.1 **ความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติความรุนแรงของการโจมตี** (C_SEV)

ค่าน้ำหนักนี้เกี่ยวข้องกับการพิจารณาคุณสมบัติของการโจมตีในด้านความรุนแรงของการโจมตี (Typical Severity) โดยมีแนวความคิดที่ว่าถ้าเว็บเซอร์วิซมีความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตีที่มีความรุนแรงอยู่ในระดับสูง ก็จะมีค่าความมั่นคงที่ดีกว่าเว็บเซอร์วิซที่มีความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตีที่มีความรุนแรงต่ำกว่า

3.3.3.2 **ความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตี** (C_LOE)

ค่าน้ำหนักนี้เกี่ยวข้องกับการพิจารณาคุณสมบัติของการโจมตีในด้านโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตี (Typical Likelihood of Exploit) โดยมีแนวความคิดที่ว่าถ้าเว็บเซอร์วิซมีความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตีที่มีโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีอยู่ในระดับสูง ก็จะมีค่าความมั่นคงที่ดีกว่าเว็บเซอร์วิซที่มีความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตีที่มีโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีที่ต่ำกว่า

3.3.3.3 **ความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติผลกระทบด้านการรักษาความลับ** (C_CON)

ค่าน้ำหนักนี้เกี่ยวข้องกับการพิจารณาคุณสมบัติของการโจมตีในด้านผลกระทบด้านการรักษาความลับ (Confidentiality Impact) โดยมีแนวความคิดที่ว่าถ้าเว็บเซอร์วิซมีความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตีที่มีผลกระทบด้านการรักษาความลับอยู่ในระดับสูง ก็จะมีค่าความมั่นคงที่ดีกว่าเว็บเซอร์วิซที่มีความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตีที่มีผลกระทบด้านการรักษาความลับที่ต่ำกว่า

3.3.3.4 **ความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติผลกระทบด้านบูรณภาพ** (C_INT)

ค่าน้ำหนักนี้เกี่ยวข้องกับการพิจารณาคุณสมบัติของการโจมตีในด้านผลกระทบด้านบูรณภาพ (Integrity Impact) โดยมีแนวความคิดที่ว่าถ้าเว็บเซอร์วิซมีความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตีที่มีผลกระทบด้านบูรณภาพอยู่ในระดับสูง ก็จะมีค่าความมั่นคงที่ดีกว่า

เว็บเซอร์วิซที่มีความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตีที่มีผลกระทบด้านบูรณภาพที่ต่ำกว่า

3.3.3.5 ความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติผลกระทบด้านสภาพพร้อมใช้งาน (C_AVA)

ค่าน้ำหนักนี้เกี่ยวข้องกับการพิจารณาคุณสมบัติของการโจมตีในด้านผลกระทบด้านสภาพพร้อมใช้งาน (Availability Impact) โดยมีแนวความคิดที่ว่าถ้าเว็บเซอร์วิซมีความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตีที่มีผลกระทบด้านสภาพพร้อมใช้งานอยู่ในระดับสูง ก็จะมีค่าความมั่นคงที่ดีกว่าเว็บเซอร์วิซที่มีความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตีที่มีผลกระทบด้านสภาพพร้อมใช้งานที่ต่ำกว่า

งานวิจัยนี้จะกำหนดให้ R เป็นเวกเตอร์เพื่อแสดงความสำคัญสัมพัทธ์ของความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติของการโจมตีดังนี้

$$R = \begin{bmatrix} R_{C\_SEV} & R_{C\_LOE} & R_{C\_CON} & R_{C\_INT} & R_{C\_AVA} \end{bmatrix} \tag{3.6}$$

โดย

R_{C_SEV} เป็นค่าความสำคัญสัมพัทธ์ของความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติความรุนแรง

R_{C_LOE} เป็นค่าความสำคัญสัมพัทธ์ของความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตี

R_{C_CON} เป็นค่าความสำคัญสัมพัทธ์ของความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติผลกระทบด้านการรักษาความลับ

R_{C_INT} เป็นค่าความสำคัญสัมพัทธ์ของความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติผลกระทบด้านบูรณภาพ

R_{C_AVA} เป็นค่าความสำคัญสัมพัทธ์ของความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติผลกระทบด้านสภาพพร้อมใช้งาน

และ $R_{C\_SEV} + R_{C\_LOE} + R_{C\_CON} + R_{C\_INT} + R_{C\_AVA} = 1$ (3.7)

ผู้ประเมินสามารถกำหนดให้ R มีค่าต่างๆได้ แต่ในงานวิจัยนี้ขอเสนอเฉพาะการกำหนดน้ำหนักสำหรับแต่ละด้านเฉพาะกรณีต่อไปนี้

- กรณีที่มีความสนใจในทุกด้านจะกำหนดให้ R เท่ากับ [0.2 0.2 0.2 0.2 0.2]
- กรณีที่มีความสนใจเฉพาะด้านใดด้านหนึ่งจะกำหนดให้ด้านนั้นมีค่าเป็น 1 และให้ด้านที่เหลือ มีค่าเป็น 0 เช่น R เท่ากับ [1 0 0 0 0] เป็นการกำหนดน้ำหนักด้านความสามารถในการจัดให้มีวิธีการรับมือสำหรับด้านความรุนแรงของการโจมตีแต่ไม่เน้นด้านอื่น

เมื่อผู้ประเมินทำการคำนวณตามแบบจำลองในสมการที่ (3.1) จะได้ค่าความมั่นคงของเว็บเซอร์วิซ (S) ที่อิงความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติของการโจมตีที่สนใจตามค่า R ซึ่งในที่นี้เสนอค่า R ไว้ 6 แบบ (ดังที่อธิบายในหัวข้อที่ 3.3.3.5) ดังนี้

- S_{SEV} คือ ค่าความมั่นคงของเว็บเซอร์วิซที่อิงความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติความรุนแรงของการโจมตี (ทั้งนี้ค่ามากที่สุดหรือค่าคะแนนเต็มจะมีค่าเท่ากับ 315)
- S_{LOE} คือ ค่าความมั่นคงของเว็บเซอร์วิซที่อิงความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีของการโจมตี (ทั้งนี้ค่ามากที่สุดหรือค่าคะแนนเต็มจะมีค่าเท่ากับ 201)
- S_{CON} คือ ค่าความมั่นคงของเว็บเซอร์วิซที่อิงความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติผลกระทบด้านการรักษาความลับของการโจมตี (ทั้งนี้ค่ามากที่สุดหรือค่าคะแนนเต็มจะมีค่าเท่ากับ 165)
- S_{INT} คือ ค่าความมั่นคงของเว็บเซอร์วิซที่อิงความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติผลกระทบด้านบูรณภาพของการโจมตี (ทั้งนี้ค่ามากที่สุดหรือค่าคะแนนเต็มจะมีค่าเท่ากับ 186)
- S_{AVA} คือ ค่าความมั่นคงของเว็บเซอร์วิซที่อิงความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติผลกระทบด้านสภาพพร้อมใช้งานของการโจมตี (ทั้งนี้ค่ามากที่สุดหรือค่าคะแนนเต็มจะมีค่าเท่ากับ 156)
- S_{ALL} คือ ค่าความมั่นคงของเว็บเซอร์วิซที่อิงความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติทุกด้านของการโจมตี (ทั้งนี้ค่ามากที่สุดหรือค่าคะแนนเต็มจะมีค่าเท่ากับ 204.6)

ในการนำค่าความมั่นคง S ทั้ง 6 แบบของเว็บเซอร์วิซหนึ่งๆ ไปใช้นั้น จะไม่ใช้ในลักษณะที่เป็นการเปรียบเทียบกันเอง เช่น หากเว็บเซอร์วิซหนึ่งมีค่า S_{SEV} เป็น 150 และค่า S_{CON} เป็น 140 เราจะไม่พิจารณาว่าเว็บเซอร์วิซนี้มีความสามารถในการรับมือต่อคุณสมบัติความรุนแรงของการโจมตี มากกว่าความสามารถในการรับมือต่อคุณสมบัติผลกระทบด้านการรักษาความลับ ทั้งนี้เนื่องจากแต่ละคุณสมบัติของการโจมตีมีฐานการให้คะแนนที่ต่างกันและไม่สามารถสรุปได้ว่าคุณสมบัติใดสำคัญกว่ากันหรือมีความสัมพันธ์ต่อกันหรือไม่ การใช้งานจึงจะเป็นในลักษณะเปรียบเทียบกับค่าคะแนนเต็มของแต่ละคุณสมบัติของการโจมตี เพื่อดูว่าเว็บเซอร์วิซมีความสามารถในการรับมือต่อคุณสมบัติด้านนั้นในระดับใด นอกจากนี้ในการเปรียบเทียบค่าความมั่นคงของเว็บเซอร์วิซหลาย ๆ ตัว ให้เปรียบเทียบกันเฉพาะในแต่ละคุณสมบัติของการโจมตี เช่น เว็บเซอร์วิซหนึ่งมีค่า S_{SEV} เป็น 150 จะมีความสามารถสูงกว่าในการรับมือการโจมตีต่อคุณสมบัติความรุนแรง เมื่อเทียบกับอีกเว็บเซอร์วิซหนึ่งที่มีค่า S_{SEV} เป็น 100

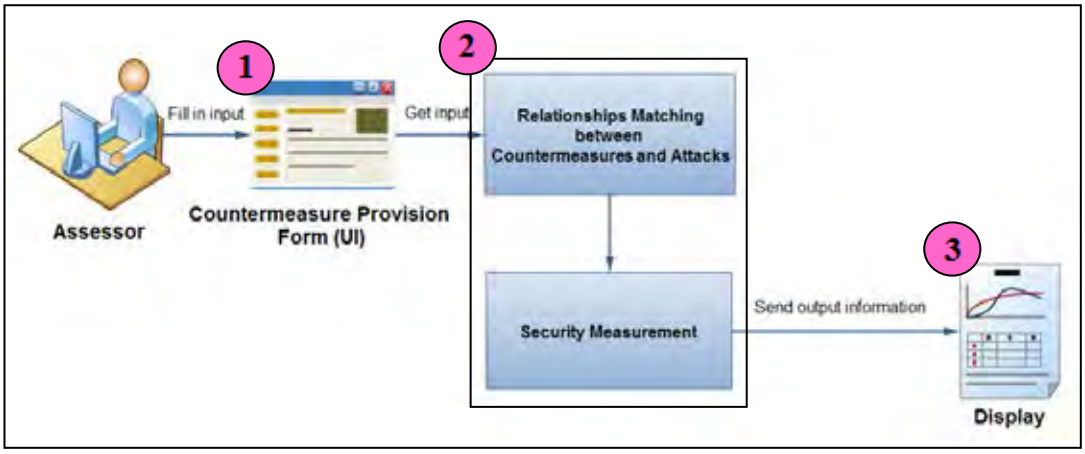
จากค่าคะแนนความมั่นคงที่ได้นั้นสามารถนำมาแปลงเป็นระดับความมั่นคงได้ 5 ระดับ ได้แก่ สูงมาก (Very High) อยู่ในช่วงตั้งแต่ร้อยละ 80 ขึ้นไปของคะแนนเต็ม สูง (High) อยู่ในช่วงมากกว่าร้อยละ 60 - 80 ของคะแนนเต็ม ปานกลาง (Medium) อยู่ในช่วงมากกว่าร้อยละ 40-60 ของคะแนนเต็ม ต่ำ (Low) อยู่ในช่วงมากกว่าร้อยละ 20-40 ของคะแนนเต็ม และต่ำมาก (Very Low) อยู่ในช่วงมากกว่าร้อยละ 0-20 ของคะแนนเต็ม โดยถ้าค่าคะแนนความมั่นคงเป็น 0 หมายถึงไม่มีข้อมูล (N/A) วัตถุประสงค์ของการแปลงเป็นระดับเพื่อให้ผู้ประเมินได้เห็นสถานะความมั่นคงของเว็บเซอร์วิซง่ายยิ่งขึ้น ดังตารางที่ 3.11

ตารางที่ 3.11 การแปลงค่าคะแนนเป็นระดับความมั่นคง

ค่าคะแนนความมั่นคง	**ระดับความมั่นคง**				
	สูงมาก (VERY HIGH)	**สูง** (HIGH)	**ปานกลาง** (MEDIUM)	**ต่ำ** (LOW)	**ต่ำมาก** (VERY LOW)
S_{SEV}	(252,315]	(189,252]	(126,189]	(63,126]	(0,63]
S_{LOE}	(160.8,201]	(120.6-160.8]	(80.4,120.6]	(40.2,80.4]	(0,40.2]
S_{CON}	(132,165]	(99,132]	(66,99]	(33,66]	(0,33]
S_{INT}	(148.8,186]	(111.6-148.8]	(74.4,111.6]	(37.2,74.4]	(0,37.2]
S_{AVA}	(124.8,156]	(93.6-124.8]	(62.4-93.6]	(31.2,62.4]	(0,31.2]
S_{ALL}	(163.7,204.6]	(122.8-163.7]	(81.8,122.8]	(40.9,81.8]	(0,40.9]

3.4 การพัฒนาเครื่องมือสนับสนุนแบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซ

การพัฒนาเครื่องมือสนับสนุนแบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซได้พัฒนาโดยใช้เอกซ์เซลแมชอัพ (Excel Mashup) [26] ซึ่งเป็นเครื่องมือสำหรับสร้างเว็บแอปพลิเคชันด้วยการดึงข้อมูลมาจากไฟล์เอกซ์เซล โดยเครื่องมือสนับสนุนแบบจำลองนี้ประกอบด้วย 3 ส่วน ได้แก่ ส่วนหน้าผู้ประเมินกรอก ส่วนการจับคู่ความสัมพันธ์และคำนวณค่าความมั่นคง และส่วนการแสดงผล ดังภาพที่ 3.2



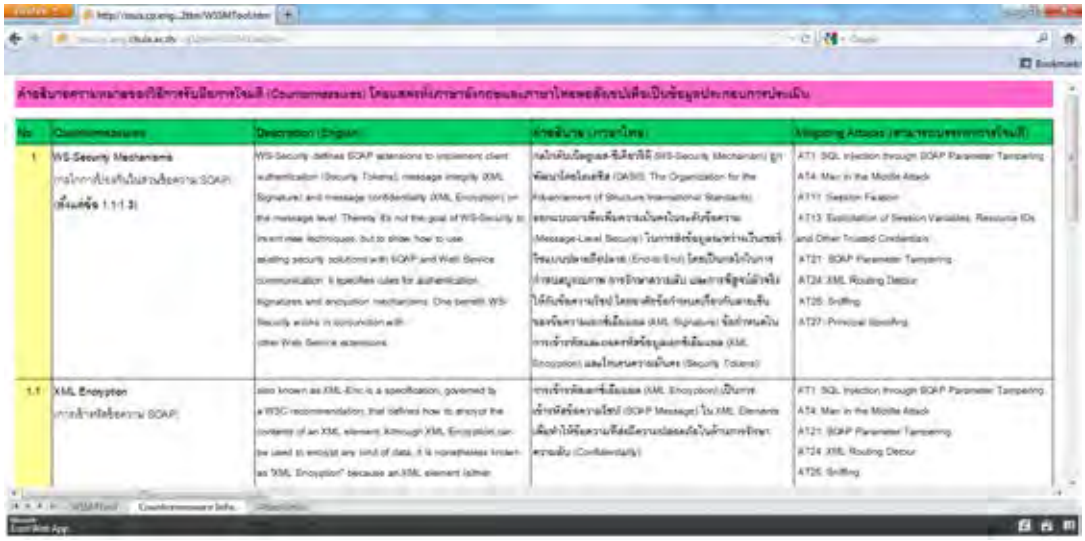
ภาพที่ 3.2 เครื่องมือสนับสนุนแบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซ

3.4.1 ส่วนหน้าผู้ประเมินกรอก

ผู้ประเมินทำการกรอกรายละเอียดข้อมูลของเว็บเซอร์วิซว่าได้จัดให้มีวิธีการรับมืออะไรบ้าง โดยการใส่เลข 1 ในช่องทำหรือไม่ทำในแต่ละรายการวิธีการรับมือ (รายการวิธีการรับมือดูได้จากตารางที่ 3.2) ดังภาพที่ 3.3

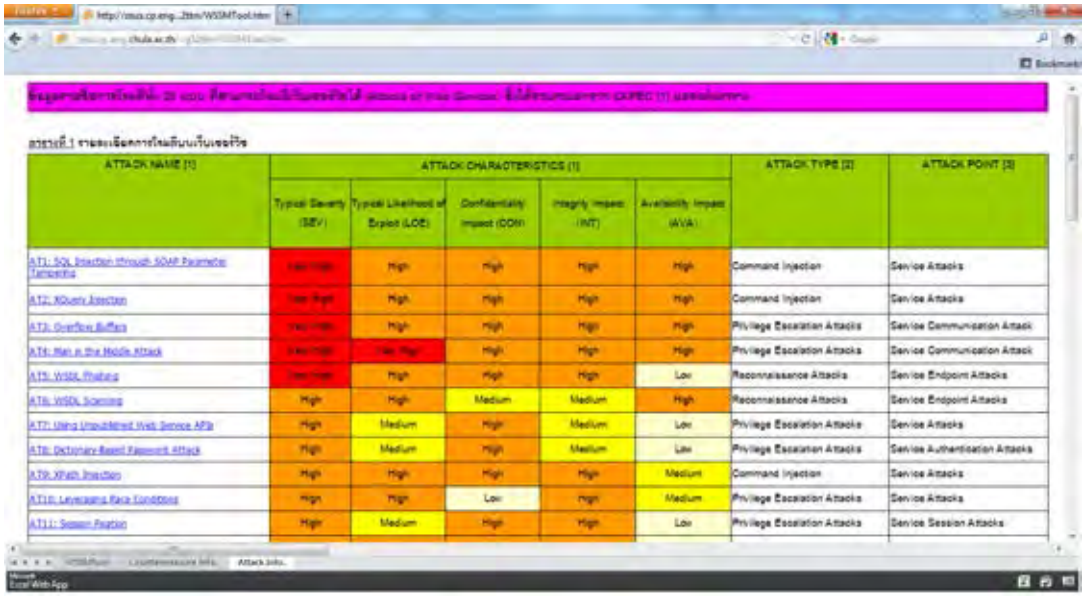
ภาพที่ 3.3 ส่วนหน้าผู้ประเมินกรอก

ส่วนให้ข้อมูลเพื่อแสดงรายละเอียดของวิธีการรับมือและการโจมตีในแท็บชื่อ Countermeasures Info. และ Attack Info. โดยแท็บ Countermeasure Info. จะแสดงคำอธิบายความหมายของวิธีการรับมือและการโจมตีที่สามารถป้องกันและ/หรือบรรเทาได้ ดังภาพที่ 3.4



ภาพที่ 3.4 หน้าแสดงรายละเอียดของวิธีการรับมือ

ส่วนแท็บ Attack Info. จะแสดงความหมาย (สามารถกดดูได้จากชื่อการโจมตี) คุณสมบัติ ประเภทและตำแหน่งการโจมตี ดังภาพที่ 3.5



ภาพที่ 3.5 หน้าแสดงรายละเอียดของการโจมตี

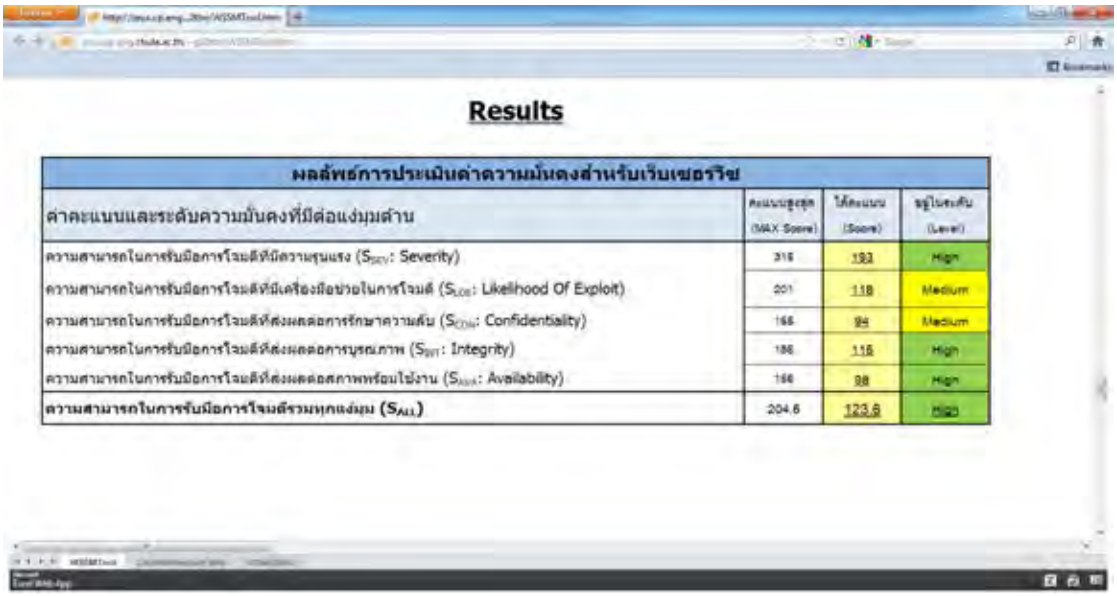
ผลลัพธ์ที่ได้จากส่วนหน้าผู้ประเมินกรอกนี้จะนำไปใช้ในการกำหนดค่า C ในขั้นตอนต่อไป

3.4.2 ส่วนการรับข้อมูลอินพุตและการคำนวณค่าความมั่นคง

เมื่อผู้ประเมินกรอกข้อมูลเรียบร้อยแล้ว ในส่วนนี้จะนำข้อมูลของผู้ประเมินมาทำการหาความสัมพันธ์ระหว่างวิธีการรับมือและการโจมตี เพื่อนำค่าที่ได้มาใช้ในการกำหนดค่าความสามารถในการจัดให้มีวิธีการรับมือ (C) แล้วนำมาคำนวณร่วมกับค่าคุณสมบัติแต่ละด้านของแต่ละการโจมตี (A) และค่าความสำคัญสัมพัทธ์ของความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติของการโจมตี (R) ซึ่งการคำนวณค่าความมั่นคงเป็นไปตามแบบจำลองในหัวข้อที่ 3.3 ตามสูตรในสมการที่ (3.1)

3.4.3 ส่วนการแสดงผล

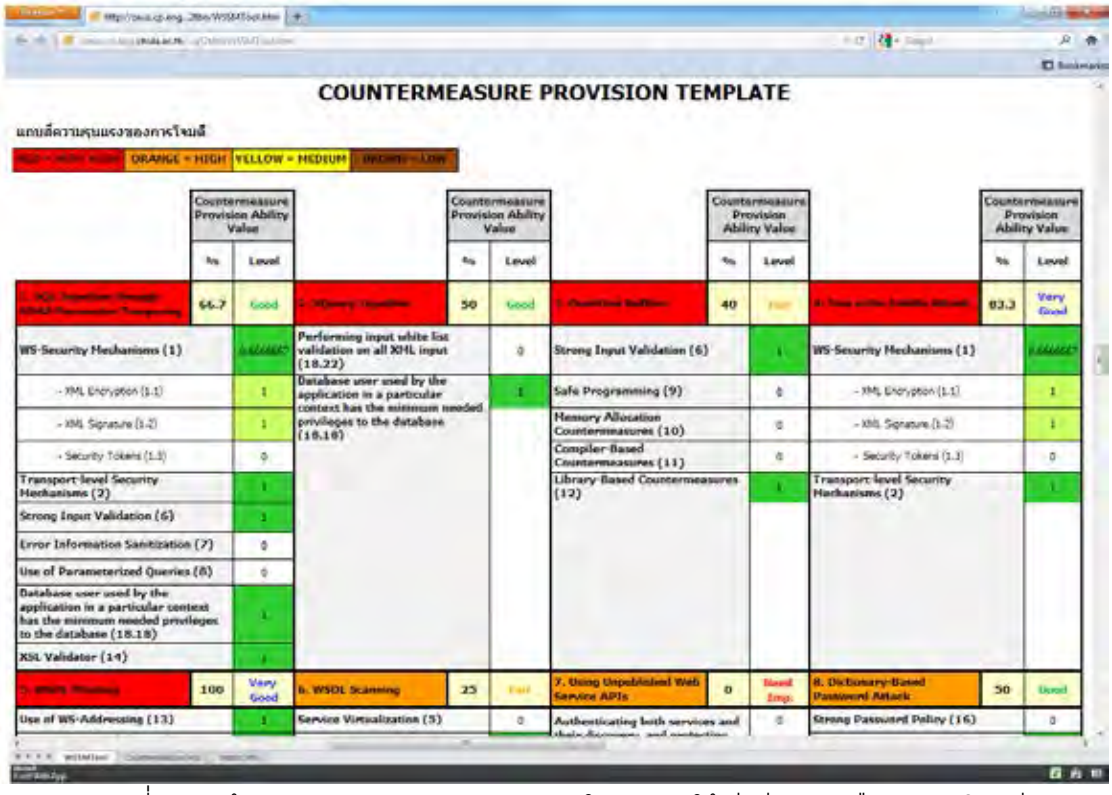
ในส่วนนี้จะเป็นหน้าแสดงผลซึ่งมีการแสดงสถานะต่างๆของความมั่นคงของเว็บเซอร์วิซ ประกอบด้วย ค่าคะแนนและระดับความมั่นคงที่มีต่อแง่มุมในด้านความสามารถในการรับมือการโจมตีต่อคุณสมบัติการโจมตีต่างๆของเว็บเซอร์วิซ ดังภาพที่ 3.6 ร้อยละของวิธีการรับมือการโจมตีที่ผู้ประเมินทำและไม่ทำ ระดับความสามารถในการรับมือต่อการโจมตีทั้ง 28 แบบ และแผนภูมิเรดาร์แสดงระดับความมั่นคงในด้านต่างๆของเว็บเซอร์วิซ ดังภาพที่ 3.7



ภาพที่ 3.6 หน้าแสดงผลลัพธ์การประเมินค่าความมั่นคงสำหรับเว็บเซอร์วิซ

ภาพที่ 3.7 หน้าแสดงผลต่างๆที่เกี่ยวข้องกับความมั่นคงเว็บเซอร์วิซ

จากส่วนการแสดงผลนี้ผู้ประเมินยังสามารถเห็นภาพรวมผลการประเมินความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตี (ข้อมูลเช่นเดียวกับในตารางที่ 3.4) ได้แก่ ค่าร้อยละและระดับความสามารถในการจัดให้มีวิธีการรับมือการโจมตี และรายการวิธีการรับมือที่ทำและไม่ทำต่อการโจมตีนั้นๆ ดังภาพที่ 3.8



ภาพที่ 3.8 หน้าแสดงภาพรวมความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตี

3.5 แนวทางการทดลองและประเมินผล

การทดลองและประเมินผลจะแบ่งเป็น 2 การประเมิน ดังนี้

3.5.1 แนวทางการประเมินความมั่นคงของเว็บเซอร์วิซและแบบจำลองการวัดความมั่นคงโดยผู้ให้บริการ

นักเขียนโปรแกรมหรือผู้ให้บริการเว็บเซอร์วิซทดลองประเมินความมั่นคงของเว็บเซอร์วิซของตนตามแบบจำลองการวัดความมั่นคงของงานวิจัยนี้ โดยทำการตอบแบบสอบถามและใช้เครื่องมือสนับสนุนแบบจำลองในหัวข้อที่ 3.4 และประเมินแบบจำลองงานวิจัย

3.5.2 แนวทางการประเมินความมั่นคงของเว็บเซอร์วิซในฐานะเป็นผู้ใช้บริการ

ผู้วิจัยทำการประเมินเว็บเซอร์วิซของผู้ให้บริการอื่น โดยนำข้อมูลที่เกี่ยวข้องกับวิธีการรับมือที่ผู้ให้บริการเว็บเซอร์วิซได้แสดงไว้ มาทำการคำนวณค่าความมั่นคงตามแบบจำลองนี้ และเพื่อสรุปว่าวิธีการรับมือใดบ้างที่ผู้ใช้บริการสามารถพิจารณาได้เองจากข้อมูลที่ผู้ให้บริการประกาศไว้ เพื่อเป็นประโยชน์ในการใช้แบบจำลองในการประเมินความมั่นคงของเว็บเซอร์วิซด้วยตนเอง ในเบื้องต้นจะสาธิตวิธีการคำนวณค่าความมั่นคงกับกรณีศึกษาจาก TPC-App Web Services Benchmark [27] ซึ่งพบว่ามีการนำกลไกความมั่นคงระดับทรานสปอร์ต คือ เอสเอสแอล มาใช้และไม่มีการใช้ดีทีดีในข้อความโซป ซึ่งจากข้อมูลนี้สามารถนำมาคำนวณตามแบบจำลองได้ดังนี้

$CM_1 = 14.29\%$ แปลงเป็นค่า $C_{AT1} = 1$

$CM_4 = 50\%$ แปลงเป็นค่า $C_{AT4} = 2$

$CM_{21} = 33.33\%$ แปลงเป็นค่า $C_{AT21} = 1$

$CM_{22} = 100\%$ แปลงเป็นค่า $C_{AT22} = 3$

$CM_{24} = 25\%$ แปลงเป็นค่า $C_{AT24} = 1$

$CM_{25} = 50\%$ แปลงเป็นค่า $C_{AT25} = 2$

$CM_{27} = 33.33\%$ แปลงเป็นค่า $C_{AT27} = 1$

ส่วน CM_i อื่นๆมีค่า $C_i = 0$ เนื่องจากวิธีการรับมือโดยเอสเอสแอลและการที่ไม่ใช้ดีทีดีในข้อความโซป ไม่สามารถรับมือการโจมตีที่เหลือได้ ดังนั้นจะได้

ค่า C ซึ่งแสดงในรูป C^T (Transpose of C) ได้เป็น [1 0 0 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 2 3 0 1 2 0 2 0]

ค่า A ตามสมการที่ (3.5)

ค่า R ตามสมการที่ (3.6) โดยสามารถกำหนดคุณสมบัติของการโจมตีที่ต้องการพิจารณาตามสมการที่ (3.7) ได้ 6 กรณี

ผลลัพธ์จากการคำนวณจะได้ค่าความมั่นคงของเว็บเซอร์วิซที่อิงความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติของการโจมตีที่สนใจ ดังตารางที่ 3.12

ตารางที่ 3.12 ค่าความมั่นคงของเว็บเซอร์วิซในกรณีศึกษา TPC-App Web Services Benchmark

ค่าความมั่นคงของเว็บเซอร์วิซ (S)	**คะแนน**	**ระดับ**
ตามคุณสมบัติความรุนแรงของการโจมตี (S_{SEV})	39	ต่ำมาก
ตามคุณสมบัติโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตี (S_{LOE})	20	ต่ำมาก
ตามคุณสมบัติผลกระทบด้านการรักษาความลับ (S_{CON})	17	ต่ำมาก
ตามคุณสมบัติผลกระทบด้านบูรณภาพ (S_{INT})	23	ต่ำมาก
ตามคุณสมบัติผลกระทบด้านสภาพพร้อมใช้งาน (S_{AVA})	21	ต่ำมาก
ตามคุณสมบัติทุกด้าน (S_{ALL})	24	ต่ำมาก

บทที่ 4

การประเมินผลการวิจัย

ในบทนี้จะกล่าวถึงผลที่ได้จากการวิจัยตามแนวคิดและวิธีการวิจัยในบทที่ 3 ในส่วนของการทดลองและประเมินผล ซึ่งได้แบ่งเป็น 2 การประเมิน ได้แก่ การประเมินความมั่นคงของเว็บเซอร์วิซและแบบจำลองการวัดความมั่นคงโดยผู้ให้บริการ และการประเมินความมั่นคงของเว็บเซอร์วิซในฐานะเป็นผู้ใช้บริการ

4.1 การประเมินความมั่นคงของเว็บเซอร์วิซและแบบจำลองการวัดความมั่นคงโดยผู้ให้บริการ

ในการประเมินนี้ผู้วิจัยได้สร้างแบบสอบถามพร้อมทั้งเครื่องมือสนับสนุนแบบจำลองเพื่อสอบถามข้อมูลสภาพการรับมือการโจมตีของผู้ให้บริการจำนวน 39 ราย (รายละเอียดการให้ข้อมูลอยู่ในภาคผนวก ข) โดยสามารถสรุปภาพรวมข้อมูลของผู้ประเมินได้ดังตารางที่ 4.1-4.11

ตารางที่ 4.1 การศึกษาของผู้ประเมิน

Education	Number of Providers	%
Bachelor	22	56.4
Master	17	43.6

ตารางที่ 4.2 ตำแหน่งของผู้ประเมิน

No.	Position	Number of Providers	%
1	Programmer	20	51.3
2	System Analyst	5	12.8
3	IT Security Specialist	2	5.13
4	System Administrator	3	7.69
5	Researcher	3	7.69
6	IT Manager	2	5.13
7	Software Development Team Leader	1	2.56
8	Technical Team Leader	1	2.56
9	Application Architect	1	2.56
10	Software Configuration Management	1	2.56

ตารางที่ 4.3 ประสบการณ์ด้านเว็บเซอร์วิซอย่างเดียว

Web Service Experience (Year)	Number of Providers	%
5	1	2.56
4	2	5.13
3	2	5.13
2	3	7.69
1	1	2.56
Total	9	23.1

ตารางที่ 4.4 ประสบการณ์ด้านเว็บเซอร์วิซและความมั่นคง

Security Experience (Year)	Web Service Experience (Year)	Number of Providers	%
10	10	1	2.56
10	1	1	2.56
8	5	1	2.56
7	1	1	2.56
5	5	2	5.13
5	3	1	2.56
5	1	1	2.56
4	3	3	7.69
3	4	1	2.56
2	3	1	2.56
2	2	6	15.4
2	1	3	7.69
1	3	2	5.13
1	2	3	7.69
1	1	3	7.69
	Total	30	76.9

ตารางที่ 4.5 โดเมนธุรกิจของเว็บเซอร์วิซ

No.	Business Domain	Number of Providers	%
1	IT	9	23.1
2	Trading	8	20.5
3	Bank	7	17.9
4	Communication	5	12.8
5	Financial Service	3	7.69
6	Research	2	5.13
7	Real Estate	2	5.13
8	News	1	2.56
9	Education	1	2.56
10	Government	1	2.56

ตารางที่ 4.6 โพรโทคอลของเว็บเซอร์วิซ

Protocol	Number of Providers	%
SOAP	34	87.2
REST	2	5.13
SOAP/REST	3	7.69

ตารางที่ 4.7 รูปแบบบริการของเว็บเซอร์วิซ

Business Model	Number of Providers	%
B2C	12	30.8
B2B	12	30.8
B2B/B2C	6	15.4
G2G	4	10.3
G2C	2	5.13
C2C	2	5.13
G2B	1	2.56

ตารางที่ 4.8 ขนาดของหน่วยงานเว็บเซอร์วิซ

Organization Size	Number of Providers	%
> 200 (Large)	22	56.4
50-200 (Medium)	6	15.4
<50 (Small)	11	28.2

ตารางที่ 4.9 ลักษณะการใช้งานเว็บเซอร์วิซ

Usage Type	Number of Providers	%
Internal	25	59.5
Public	7	17.9
Internal and Public	7	17.9

ตารางที่ 4.10 ความสำคัญของเว็บเซอร์วิซ

Importance Level	Number of Providers	%
High	23	59
Medium	14	35.9
Low	2	5.13

ตารางที่ 4.11 ปริมาณการใช้งานเว็บเซอร์วิซ

Usage Level	Number of Providers	%
High	17	43.6
Medium	19	48.7
Low	3	7.69

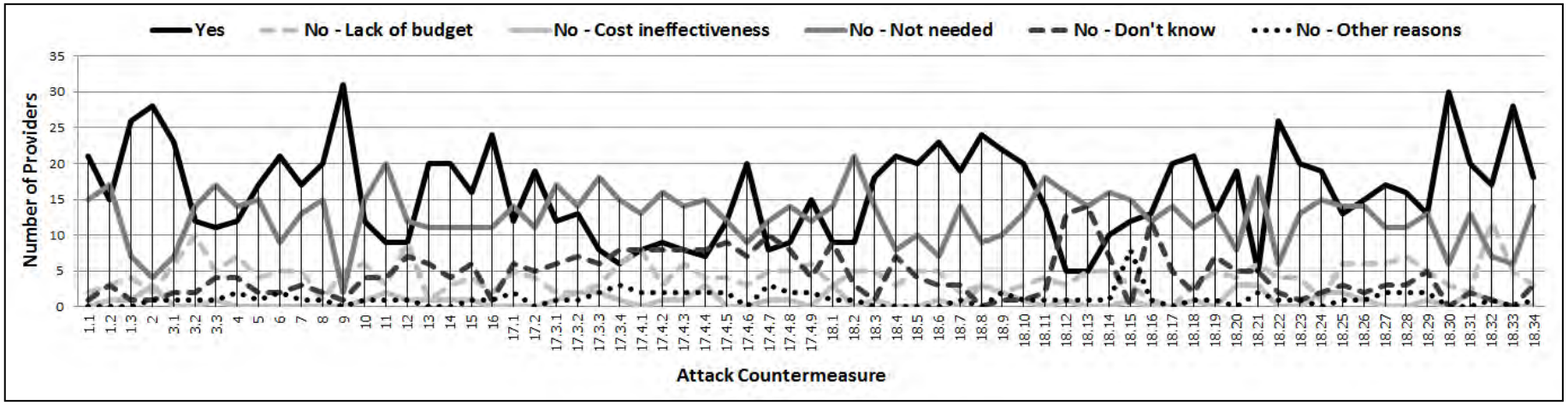
โดยในส่วนการประเมินนี้จะแบ่งออกเป็น 2 ส่วน ได้แก่ การประเมินความมั่นคงของเว็บเซอร์วิซและการประเมินแบบจำลองการวัดความมั่นคง ดังนี้

4.1.1 การประเมินความมั่นคงของเว็บเซอร์วิซโดยผู้ให้บริการ

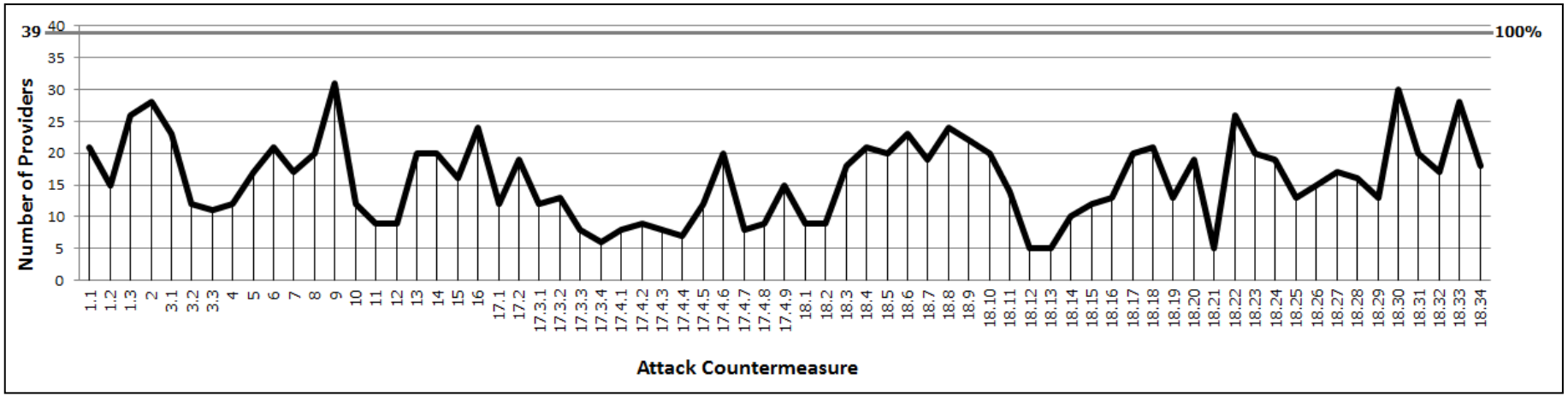
จากข้อมูลในแบบสอบถามสามารถแบ่งการพิจารณาออกเป็น 8 ด้าน ได้แก่ 1) ภาพรวมวิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ทำและไม่ทำ 2) ประสบการณ์ด้านเว็บเซอร์วิซและ/หรือความมั่นคงของผู้ให้บริการ 3) โดเมนธุรกิจของเว็บเซอร์วิซ 4) รูปแบบบริการของเว็บเซอร์วิซ 5)ขนาดของหน่วยงาน 6) ลักษณะการใช้งานเว็บเซอร์วิซ 7) ความสำคัญของเว็บเซอร์วิซ และ 8) ปริมาณการใช้งานเว็บเซอร์วิซ แสดงผลสรุปได้ดังนี้

4.1.1.1 ภาพรวมของวิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ทำและไม่ทำ

จากการเก็บรวบรวมข้อมูลพบว่าวิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ทำและไม่ทำเพราะเหตุผลต่างๆ เป็นดังภาพที่ 4.1 และวิธีการรับมือการโจมตีที่มีผู้ให้บริการทำเป็นดังภาพที่ 4.2 (ส่วนต่างหมายถึงจำนวนผู้ให้บริการที่ไม่ทำ (ทุกเหตุผลรวมกัน))



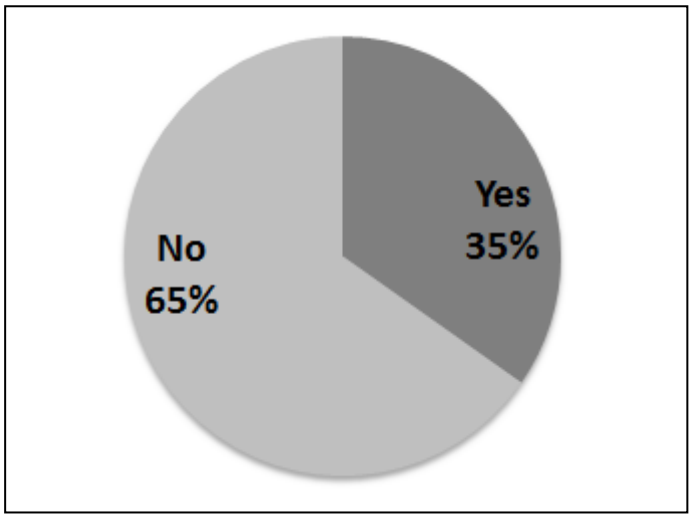
ภาพที่ 4.1 จำนวนผู้ให้บริการกับวิธีการรับมือการโจมตีที่ทำและไม่ทำเพราะเหตุผลต่างๆ



ภาพที่ 4.2 จำนวนผู้ให้บริการกับวิธีการรับมือการโจมตีที่ทำ

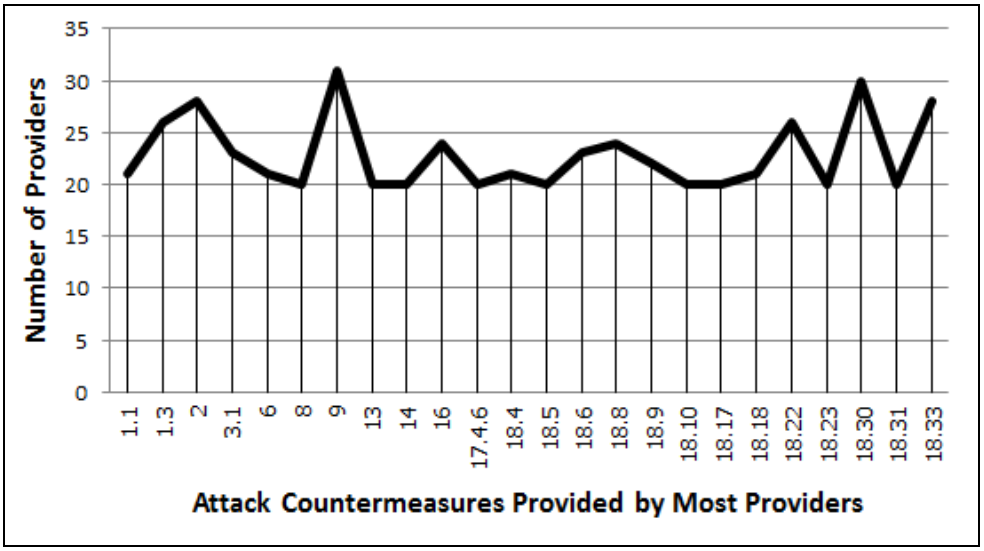
จากภาพที่ 4.1 และ 4.2 พบว่าคำตอบที่ได้จากผู้ให้บริการส่วนใหญ่จะเน้นไปในการตอบ ทำ ไม่ทำเพราะระบบไม่ต้องการ และไม่ทำเพราะไม่รู้จัก มากกว่าการตอบไม่ทำเพราะเหตุผลอื่นๆ ดังนั้นผู้วิจัยจึงจะนำเสนอเฉพาะวิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ทำ ไม่ทำ (ทุกเหตุผลรวมกัน) ไม่ทำเพราะระบบไม่ต้องการ และไม่ทำเพราะไม่รู้จัก

โดยเมื่อเปรียบเทียบวิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ทำกับไม่ทำ พบว่า ทำ มีจำนวน 24 รายการ คิดเป็นร้อยละ 35 และไม่ทำ มีจำนวน 45 รายการ คิดเป็นร้อยละ 65 ดังภาพที่ 4.3



ภาพที่ 4.3 ร้อยละวิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ทำและไม่ทำ

1) วิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ทำ มีจำนวน 24 รายการ ดังภาพที่ 4.4



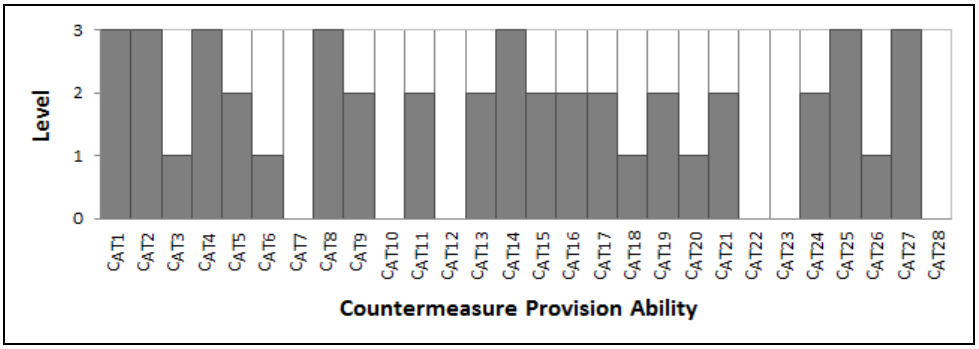
ภาพที่ 4.4 วิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ทำ

จากรูป สามารถนำมาจัด 5 อันดับวิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ทำมากที่สุด พบว่ามีจำนวน 8 รายการ ดังตารางที่ 4.12

ตารางที่ 4.12 วิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ทำ 5 อันดับแรก

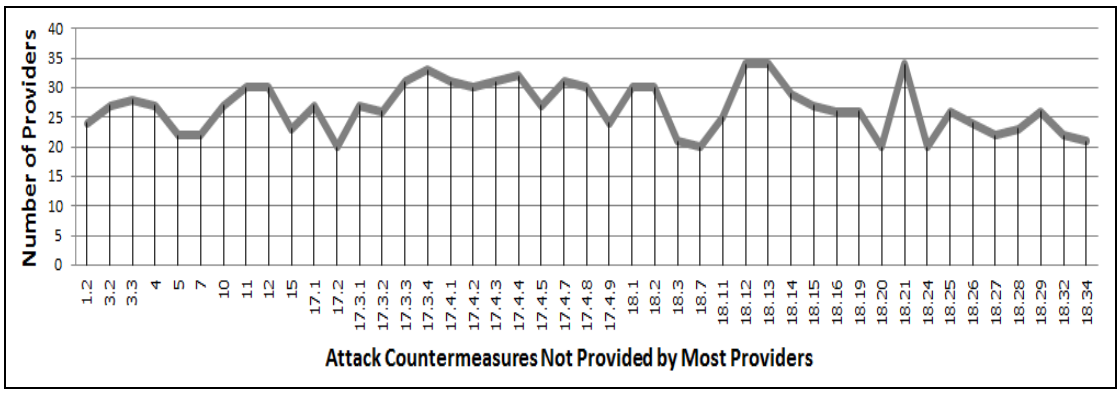
Rank	CM. Number	Countermeasure Name
1	9	Safe Programming
2	18.30	Utilizing session timeout for all session IDs at runtime
3	2	Transport-level Security Mechanisms
	18.33	Providing for a timeout mechanism for allocated resources whose transaction does not complete within a specified interval
4	1.3	Security Tokens
	18.22	Performing input white list validation on all XML input
5	16	Strong Password Policy
	18.8	Configuring network access control to accept incoming message from a specific IP address

โดยวิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ทำทั้ง 24 รายการ เมื่อนำมาพิจารณาตามค่ามาตรวัดความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตีที่ได้กล่าวไว้แล้วในบทที่ 3 พบว่า มี 6 ค่ามาตรวัดที่ต้องมีการปรับปรุง เนื่องจากไม่สามารถจะบรรเทาและ/หรือป้องกันการโจมตีที่ 7 (AT7: Using Unpublished Web Service APIs) การโจมตีที่ 10 (AT10: Leveraging Race Conditions) การโจมตีที่ 12 (AT12: Reflection Attack in Authentication Protocol) การโจมตีที่ 22 (AT22: Resource Depletion through DTD Injection in SOAP Message) การโจมตีที่ 23 (AT23: Symlink Attacks) และการโจมตีที่ 28 (AT28: Detect Unpublicized Web Services) ได้ ดังภาพที่ 4.5



ภาพที่ 4.5 ค่ามาตรวัดความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตีที่ผู้ให้บริการส่วนใหญ่ทำ

2) วิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ไม่ทำ มีจำนวน 45 รายการ ดังภาพที่ 4.6



ภาพที่ 4.6 วิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ไม่ทำ

จากรูป สามารถนำมาจัด 5 อันดับวิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ไม่ทำ พบว่ามีจำนวน 16 รายการ ดังตารางที่ 4.13

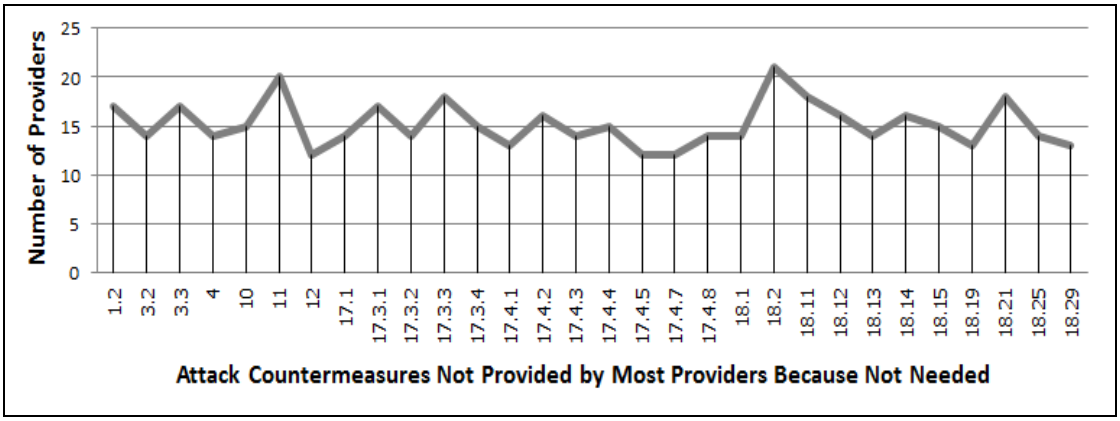
ตารางที่ 4.13 วิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ไม่ทำ 5 อันดับแรก

Rank	CM. Number	Countermeasure Name
1	18.12	The use of HMAC to hash the response from the server can also be used to thwart reflection
	18.13	Introducing a random nonce with each new connection
	18.21	Using static analysis tools to find race conditions
2	17.3.4	Allowing the policy to define whether recursion is allowed within the XML message. This should be switched on only in specific instances when the underlying schema of the message is extremely complex
3	17.4.4	The threshold at which action can be taken when an excessive number of HTTP unauthorized/forbidden errors are returned
	17.3.3	Defining the maximum number of elements allowed for each level in the tree
	17.4.1	All requests from an IP address which is sending spurious messages should be blocked
	17.4.3	The threshold at which action, which might include notification, is taken when a service starts returning an unusually high number of errors or SOAP faults
	17.4.7	Indicating whether the XML firewall should automatically shut down the service if the threshold limit has been reached

ตารางที่ 4.13 วิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ไม่ทำ 5 อันดับแรก (ต่อ)

Rank	CM. Number	Countermeasure Name
4	11	Compiler-Based Countermeasures
	12	Library-Based Countermeasures
	17.4.2	The threshold number of requests at which the firewall should activate its exception management scenario
	17.4.8	Automatic restart of the service after the specified time interval
	18.1	Creating a handshake mechanism for interacting with ad hoc WSDL or Web service to ensure validity
	18.2	Configuring the XML processor to only retrieve external entities form trusted sources
5	18.14	Using randomly generated file names for temporary files

3) วิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ไม่ทำเพราะระบบไม่ต้องการ ซึ่งอาจหมายความว่าวิธีการรับมือดังกล่าวอาจไม่จำเป็นต้องมีในการให้บริการของเว็บเซอร์วิซโดยทั่วไป มีจำนวน 30 รายการ (เปรียบเทียบกับทุกกรณีที่ผู้ให้บริการตอบว่าไม่ทำ เพราะระบบไม่ต้องการแล้วมีจำนวนมากที่สุดในแต่ละรายการวิธีการรับมือ) ดังภาพที่ 4.7



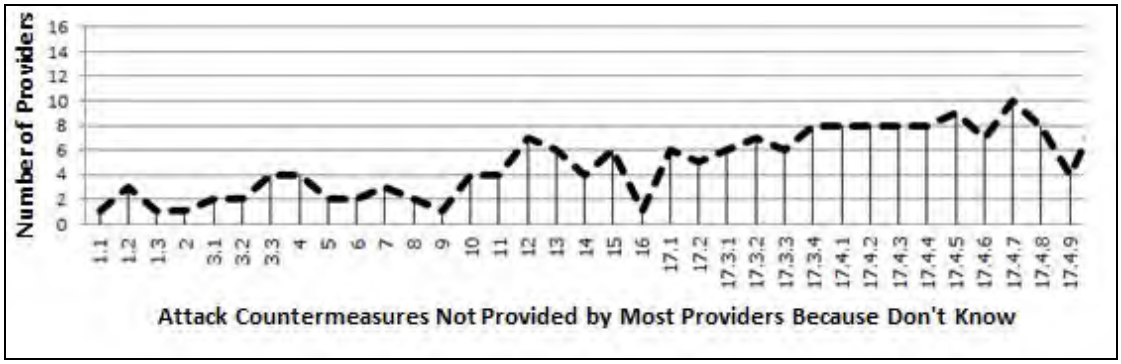
ภาพที่ 4.7 วิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ไม่ทำเพราะระบบไม่ต้องการ

จากรูป สามารถนำมาจัด 5 อันดับวิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ไม่ทำเพราะระบบไม่ต้องการมากที่สุด พบว่ามีจำนวน 11 รายการ ดังตารางที่ 4.14

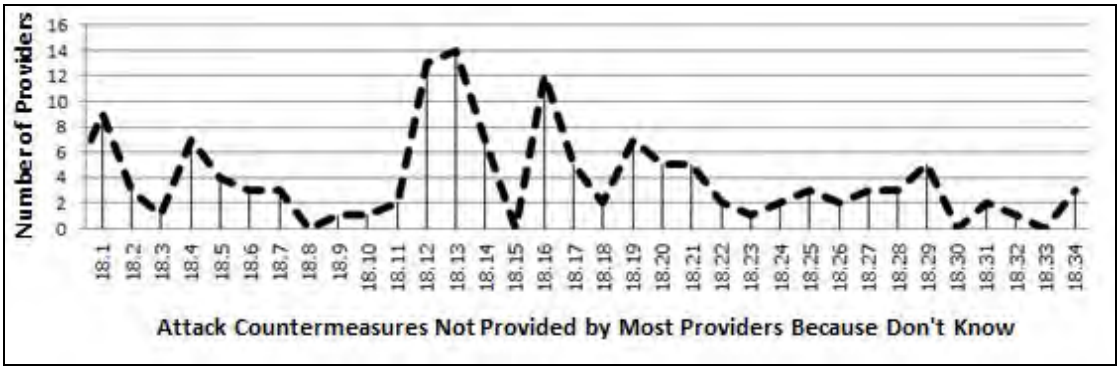
ตารางที่ 4.14 วิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ไม่ทำเพราะระบบไม่ต้องการ 5 อันดับแรก

Rank	CM. Number	Countermeasure Name
1	18.2	Configuring the XML processor to only retrieve external entities form trusted sources
2	11	Compiler-Based Countermeasures
3	18.21	Using static analysis tools to find race conditions
	18.11	Delete all default account credentials that may be put in by the product vendor
	17.3.3	Defining the maximum number of elements allowed for each level in the tree
4	1.2	XML Signature
	3.3	Defining definition of additional validation rules that can be performed on the message element or attributes
	17.3.1	Defining the maximum amount of nesting allowed inside a particular element
5	17.4.2	The threshold number of requests at which the firewall should activate its exception management scenario
	18.12	The use of HMAC to hash the response from the server can also be used to thwart reflection
	18.14	Using randomly generated file names for temporary files

4) วิธีการรับมือการโจมตีที่มีผู้ให้บริการส่วนใหญ่ตอบว่าไม่ทำเพราะไม่รู้จัก มีจำนวน 65 รายการ ดังภาพที่ 4.8



ภาพที่ 4.8 วิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ไม่ทำเพราะไม่รู้จัก



ภาพที่ 4.8 วิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ไม่ทำเพราะไม่รู้จัก (ต่อ)

จากรูป สามารถนำมาจัด 5 อันดับวิธีการรับมือการโจมตีที่มีผู้ให้บริการตอบว่าไม่ทำเพราะไม่รู้จักมากที่สุด พบว่ามี 6 รายการ ดังตารางที่ 4.15 และมี 4 รายการ ที่ไม่มีผู้ให้บริการรายใดตอบว่าไม่รู้จัก ดังตารางที่ 4.16

ตารางที่ 4.15 วิธีการรับมือการโจมตีที่มีผู้ให้บริการตอบว่าไม่ทำเพราะไม่รู้จัก 5 อันดับแรก

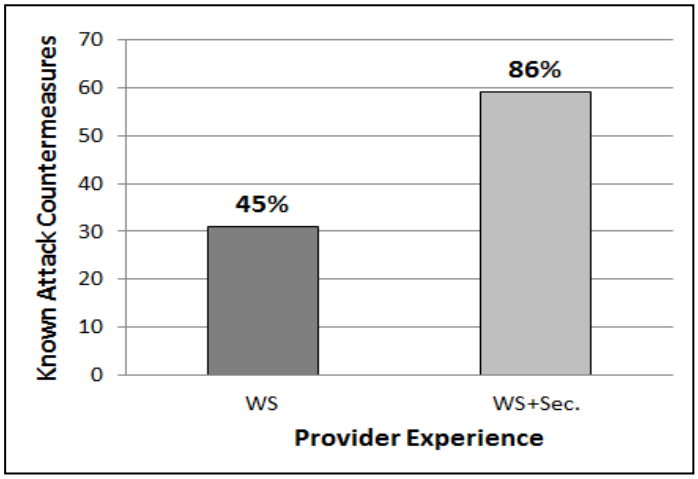
Rank	CM. Number	Countermeasure Name
1	18.13	Introducing a random nonce with each new connection
2	18.12	The use of HMAC to hash the response from the server can also be used to thwart reflection
3	18.16	Disallowing the inclusion of DTDs in SOAP messages
4	17.4.7	Indicating whether the XML firewall should automatically shut down the service if the threshold limit has been reached
5	17.4.5	The threshold at which action can be taken when message processing takes a large number of CPU cycles
	18.1	Creating a handshake mechanism for interacting with ad hoc WSDL or Web service to ensure validity

ตารางที่ 4.16 วิธีการรับมือการโจมตีที่ผู้ให้บริการทุกรายรู้จัก

CM. Number	Countermeasure Name
18.8	Configuring network access control to accept incoming message from a specific IP address
18.15	Do not use Unix and Linux systems
18.30	Utilizing session timeout for all session IDs at runtime
18.33	Providing for a timeout mechanism for allocated resources whose transaction does not complete within a specified interval

4.1.1.2 ประสบการณ์ด้านเว็บเซอร์วิซและ/หรือความมั่นคงของผู้ให้บริการ

ผู้วิจัยได้จำแนกประสบการณ์ของผู้ให้บริการ (ซึ่งเป็นนักเขียนโปรแกรม ผู้ดูแลเว็บเซอร์วิซ ฯลฯ) ออกเป็น 2 ด้าน ได้แก่ ผู้ที่มีประสบการณ์ด้านเว็บเซอร์วิซ และผู้ที่มีประสบการณ์ทั้งด้านเว็บเซอร์วิซและความมั่นคง ว่าในผู้ที่มีประสบการณ์ทั้ง 2 ด้านนี้จะรู้จักและทำวิธีการรับมือการโจมตีอย่างไรบ้าง จากการเก็บข้อมูลพบว่า ผู้ที่มีประสบการณ์ด้านเว็บเซอร์วิซเพียงอย่างเดียวจะไม่รู้จักวิธีการรับมือการโจมตีจำนวน 38 รายการ แสดงว่ารู้จัก 31 รายการ คิดเป็น 45% และผู้ที่มีประสบการณ์ทั้งด้านเว็บเซอร์วิซและความมั่นคงจะไม่รู้จักวิธีการรับมือการโจมตีจำนวน 10 รายการ แสดงว่ารู้จัก 59 รายการ คิดเป็น 86% ของวิธีการรับมือการโจมตีทั้งหมด ดังภาพที่ 4.9



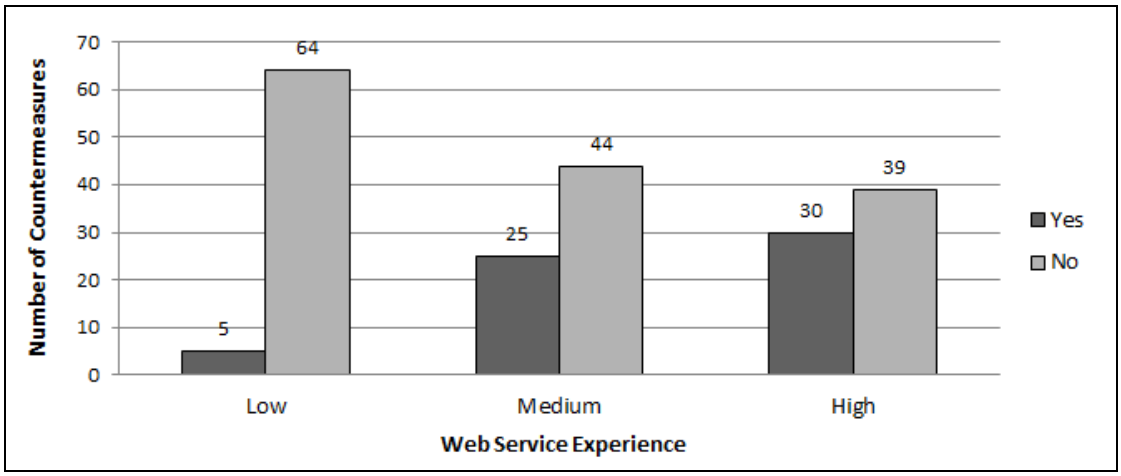
ภาพที่ 4.9 ร้อยละการรู้จักวิธีการรับมือการโจมตีของผู้มีประสบการณ์ด้านเว็บเซอร์วิซและทั้งด้านเว็บเซอร์วิซและความมั่นคง

โดยในแต่ละกลุ่มประสบการณ์ของผู้ให้บริการ ผู้วิจัยได้แบ่งระดับตามจำนวนปีของประสบการณ์ ดังนี้

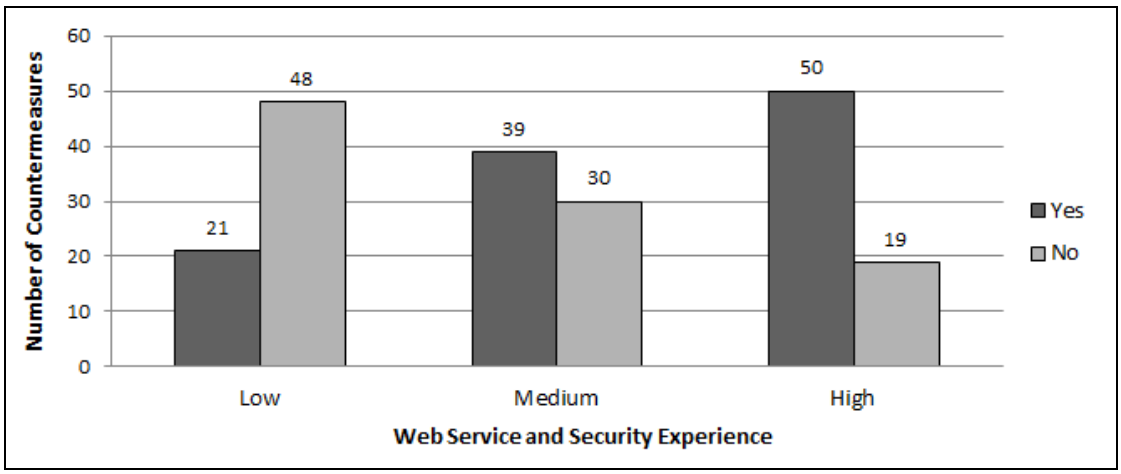
- ผู้ให้บริการที่มีประสบการณ์เฉพาะด้านเว็บเซอร์วิซ แบ่งระดับได้เป็น ระดับต่ำ (Low) คือ 1 ปี ระดับปานกลาง (Medium) คือ 2-3 ปี และระดับสูง (High) คือ มากกว่าหรือเท่ากับ 4 ปี
- ผู้ให้บริการที่มีประสบการณ์ทั้งด้านเว็บเซอร์วิซและความมั่นคง พิจารณาตามจำนวนปีของความมั่นคง แบ่งระดับได้เป็น ระดับต่ำ (Low) คือ 1-2 ปี ระดับปานกลาง (Medium) คือ 3-4 ปี และระดับสูง (High) คือ มากกว่าหรือเท่ากับ 5 ปี

เมื่อนำมาพิจารณาตามจำนวนวิธีการรับมือการโจมตีที่ทำและไม่ทำของทั้งสองกลุ่มประสบการณ์ พบว่าผู้ให้บริการที่มีประสบการณ์ด้านเว็บเซอร์วิซที่อยู่ในระดับสูงจะมีการทำวิธีการ

รับมือมากกว่าระดับกลางและต่ำ ส่วนผู้ให้บริการที่มีประสบการณ์ทั้งด้านเว็บเซอร์วิซและความมั่นคงที่อยู่ในระดับสูงก็จะมีการทำวิธีการรับมือมากกว่าระดับกลางและต่ำ เช่นเดียวกัน ดังภาพที่ 4.10 และ 4.11



ภาพที่ 4.10 ปริมาณการทำและไม่ทำวิธีการรับมือของระดับประสบการณ์ด้านเว็บเซอร์วิซ



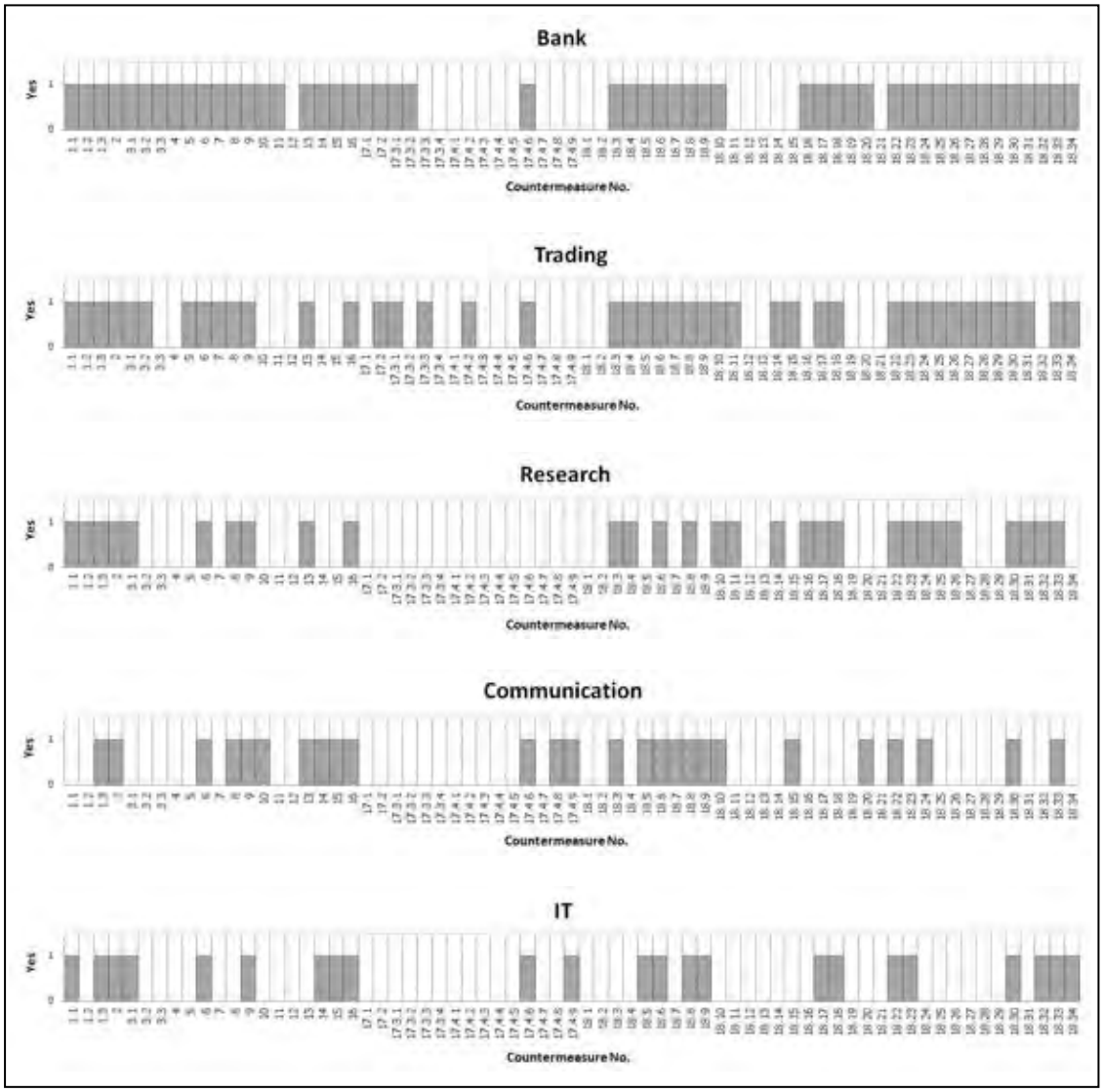
ภาพที่ 4.11 ปริมาณการทำและไม่ทำวิธีการรับมือของระดับประสบการณ์ด้านเว็บเซอร์วิซและความมั่นคง

ผลสรุปพบว่า ผู้ให้บริการ (ซึ่งเป็นนักเขียนโปรแกรม ผู้ดูแลเว็บเซอร์วิซ ฯลฯ) ที่มีประสบการณ์ทั้งด้านเว็บเซอร์วิซและความมั่นคงในทุกระดับจะรู้จักและทำวิธีการรับมือมากกว่าผู้ที่มีประสบการณ์เฉพาะด้านเว็บเซอร์วิซเพียงอย่างเดียว โดยจะมีเฉพาะผู้ที่มีประสบการณ์ทั้งด้านเว็บเซอร์วิซและความมั่นคงที่อยู่ในระดับปานกลางและสูงจะมีปริมาณการทำวิธีการรับมือการโจมตีมากกว่าไม่ทำ ซึ่งอาจเป็นไปได้ว่าผู้มีประสบการณ์ด้านความมั่นคงสูงจะมีความสามารถในการรับรู้และทำวิธีการรับมือการโจมตีได้มากกว่าผู้ที่มีประสบการณ์ด้านความมั่นคงต่ำ

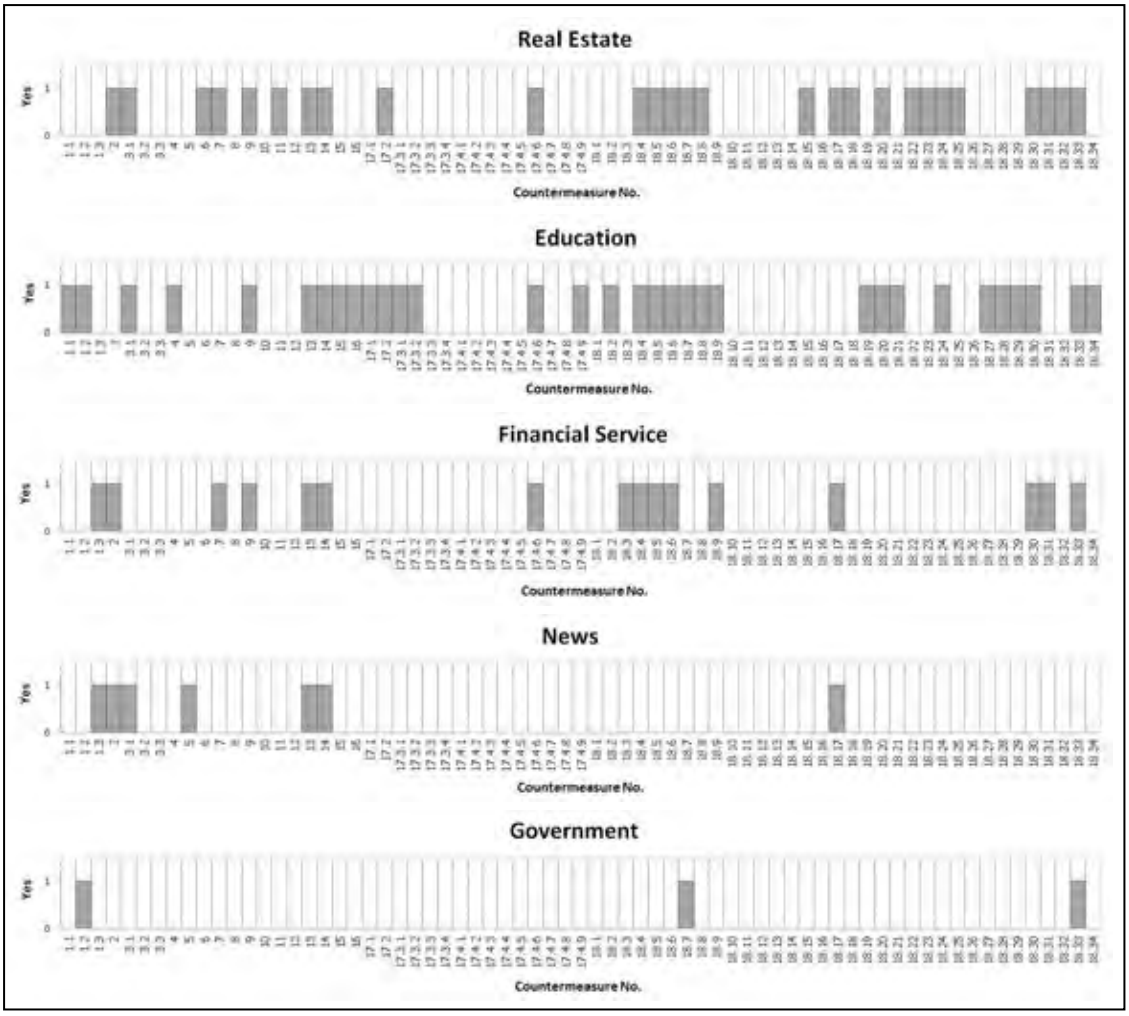
4.1.1.3 โดเมนธุรกิจของเว็บเซอร์วิซ

จากการเก็บข้อมูลจากผู้ให้บริการ สามารถนำมาแบ่งโดเมนธุรกิจของเว็บเซอร์วิซออกได้เป็น 10 กลุ่ม ได้แก่ ธนาคาร การซื้อขายสินค้า การสื่อสาร การวิจัย เทคโนโลยีสารสนเทศ อสังหาริมทรัพย์ การศึกษา การให้บริการด้านการเงิน สำนักข่าว และภาครัฐ โดยในแต่ละธุรกิจจะแสดงภาพรวมของแต่ละรายการวิธีการรับมือที่ทำ (ซึ่งพิจารณาจากค่าร้อยละในแต่ละกลุ่มตัวอย่าง เช่น ผู้ให้บริการธุรกิจธนาคารส่วนใหญ่ มีการทำรายการที่ 1.1 มากกว่าหรือเท่ากับร้อยละ 50 ขึ้นไป จะพิจารณาว่าทำ) ปริมาณการทำวิธีการรับมือ ค่ามาตรวัดความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตี ค่าคะแนนและระดับความมั่นคงของโดเมนธุรกิจ ดังนี้

1) รายการวิธีการรับมือที่ทำในแต่ละธุรกิจ ดังภาพที่ 4.12

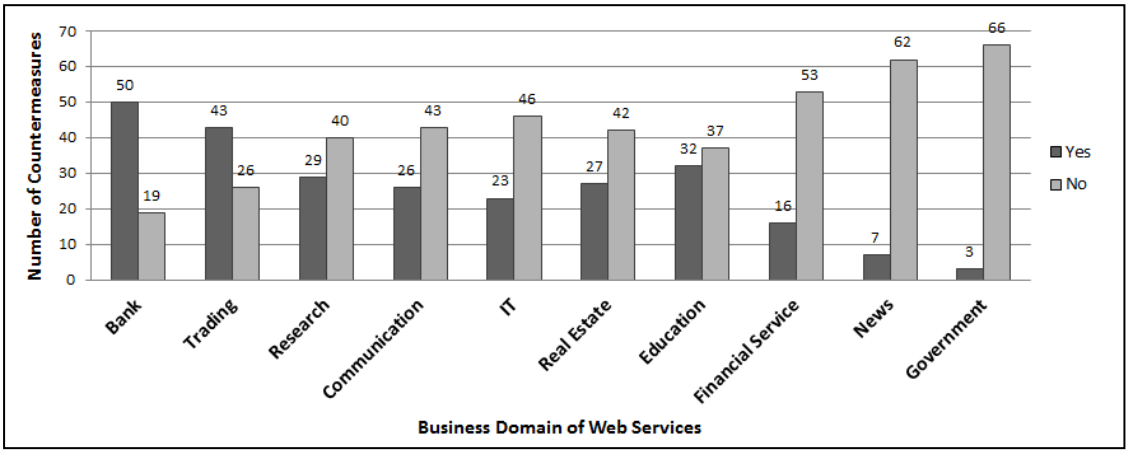


ภาพที่ 4.12 วิธีการรับมือการโจมตีที่ทำในแต่ละโดเมนธุรกิจของเว็บเซอร์วิซ



ภาพที่ 4.12 วิธีการรับมือการโจมตีที่ทำในแต่ละโดเมนธุรกิจของเว็บเซอร์วิซ (ต่อ)

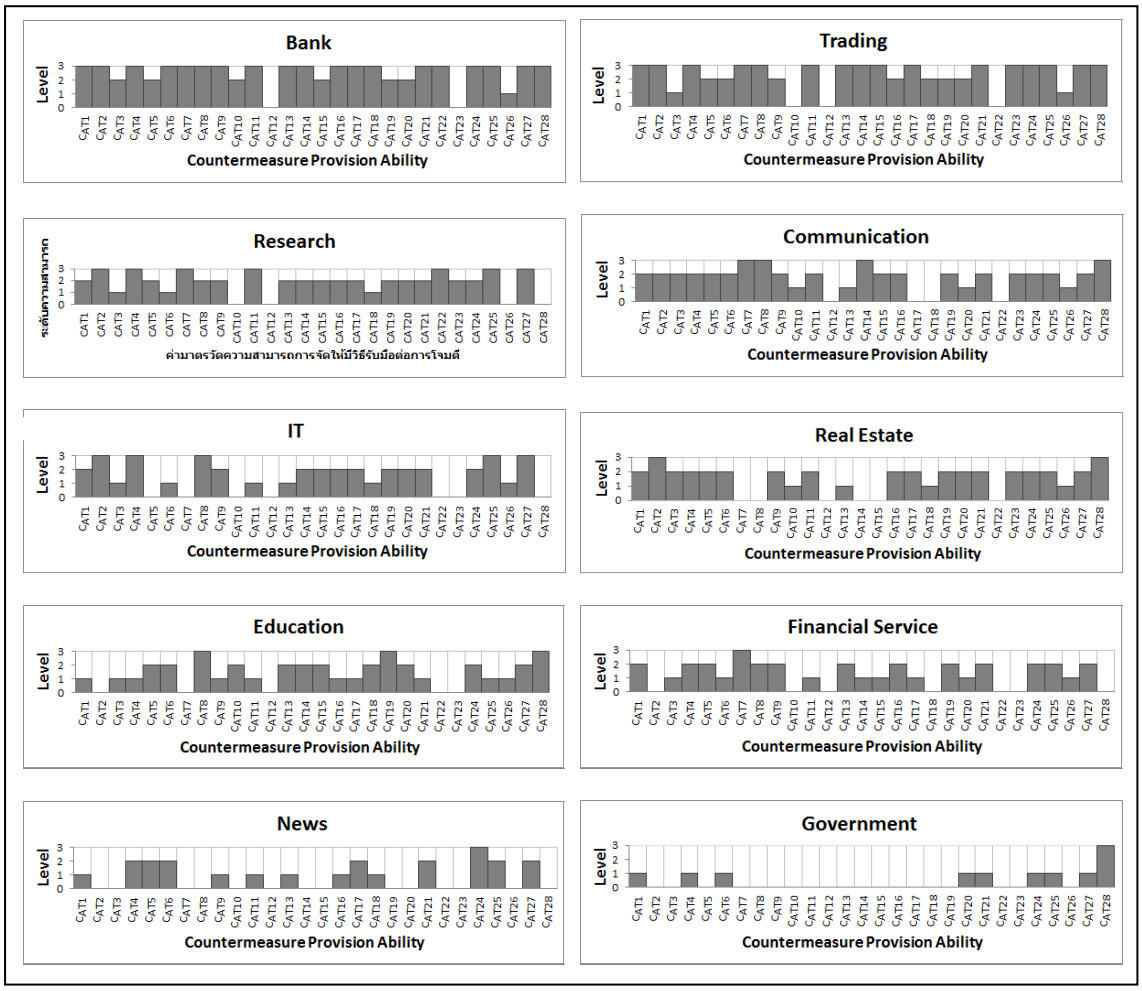
2) ปริมาณการทำและไม่ทำวิธีการรับมือ จากภาพที่ 4.12 เมื่อนำมาพิจารณาตามจำนวนวิธีการรับมือการโจมตีที่แต่ละโดเมนธุรกิจของเว็บเซอร์วิซทำและไม่ทำ จะได้ดังภาพที่ 4.13



ภาพที่ 4.13 ปริมาณการทำและไม่ทำวิธีการรับมือในแต่ละโดเมนธุรกิจของเว็บเซอร์วิซ

จากภาพที่ 4.13 พบว่า ธนาคารมีการทำวิธีการรับมือการโจมตีมากที่สุดและภาครัฐมีการทำวิธีการรับมือการโจมตีน้อยที่สุด

3) ค่ามาตรวัดความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตี ซึ่งได้กล่าวไว้ในหัวข้อที่ 3.3.1 สามารถนำมาวิเคราะห์เป็นระดับได้ดังภาพที่ 4.14



ภาพที่ 4.14 ค่ามาตรวัดความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตีของโดเมนธุรกิจ

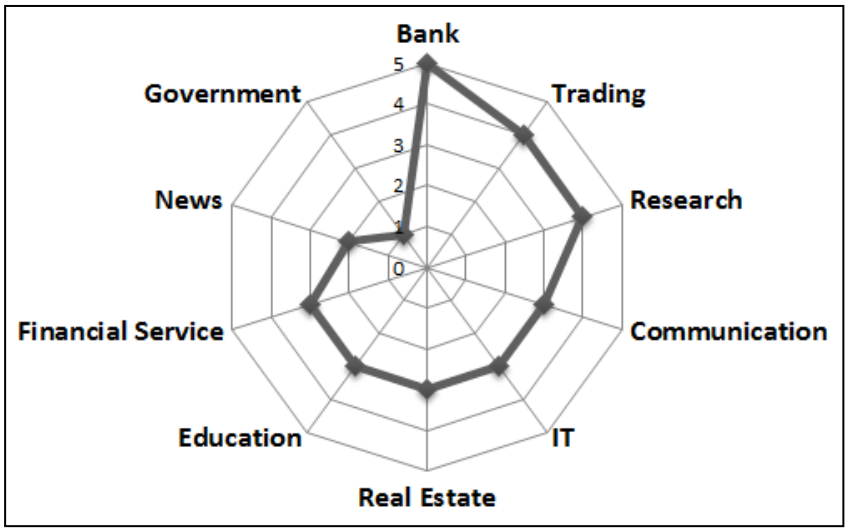
จากรูปดังกล่าว พบว่าค่ามาตรวัดความสามารถในการจัดให้มีวิธีการรับมือต่อการโจมตีแบบที่ 12 (C_{AT12}) มีค่าระดับความสามารถเท่ากับ 0 ทุกโดเมนธุรกิจของเว็บเซอร์วิซ จึงอาจแสดงว่าผู้ให้บริการส่วนใหญ่ยังไม่มีวิธีการรับมือการโจมตีที่จะสามารถบรรเทาและ/หรือป้องกันการโจมตีที่ 12 (AT12: Reflection Attack in Authentication Protocol) ซึ่งจำเป็นต้องมีวิธีการรับมือการโจมตี ได้แก่ รายการที่ 18.1 (Creating a handshake mechanism for interacting with ad hoc WSDL or Web service to ensure validity) รายการที่ 18.12 (The use of HMAC to hash the response from the server can also be used to thwart reflection) และรายการที่ 18.13 (Introducing a random nonce with each new connection) ในหัวข้อที่ 3.1.2

4) ค่าคะแนนและระดับความมั่นคงของโดเมนธุรกิจ เมื่อนำมาคำนวณตามแบบจำลองที่กล่าวไว้ในบทที่ 3 ได้ผลดังตารางที่ 4.17

ตารางที่ 4.17 ค่าคะแนนและระดับความมั่นคงของโดเมนธุรกิจ

Business Domain	Security Score						Security Level					
	S_{SEV}	S_{LOE}	S_{CON}	S_{INT}	S_{AVA}	S_{ALL}	S_{SEV}	S_{LOE}	S_{CON}	S_{INT}	S_{AVA}	S_{ALL}
Bank	264	174	146	157	131	174.4	VH	VH	VH	VH	VH	VH
Trading	240	149	134	140	115	155.6	H	H	VH	H	H	H
Research	199	125	105	119	97	129	H	H	H	H	H	H
Communication	182	121	107	105	84	119.8	M	H	H	M	M	M
IT	157	101	84	90	82	102.8	M	M	M	M	M	M
Real Estate	157	95	79	88	83	100.4	M	M	M	M	M	M
Education	141	87	75	80	68	90.2	M	M	M	M	M	M
Financial Service	135	90	77	78	63	88.6	M	M	M	M	M	M
News	87	55	47	52	45	57.2	L	L	L	L	L	L
Government	35	16	20	14	17	20.4	VL	VL	VL	VL	VL	VL

จากตารางเมื่อพิจารณา S_{ALL} พบว่า ธนาคาร มีความมั่นคงอยู่ในระดับสูงมาก การซื้อขายสินค้าและการวิจัย มีความมั่นคงอยู่ในระดับสูง การสื่อสาร เทคโนโลยีสารสนเทศ อสังหาริมทรัพย์ การศึกษา และบริการด้านการเงิน มีความมั่นคงอยู่ในระดับปานกลาง สำนักข่าว มีความมั่นคงอยู่ในระดับต่ำ และภาครัฐ มีความมั่นคงอยู่ในระดับต่ำมาก ดังภาพที่ 4.15 (กำหนดให้ 5 = VH: Very High, 4 = H: High, 3 = M: Medium, 2 = L:Low, 1 = VL: Very Low และ 0 = NONE)

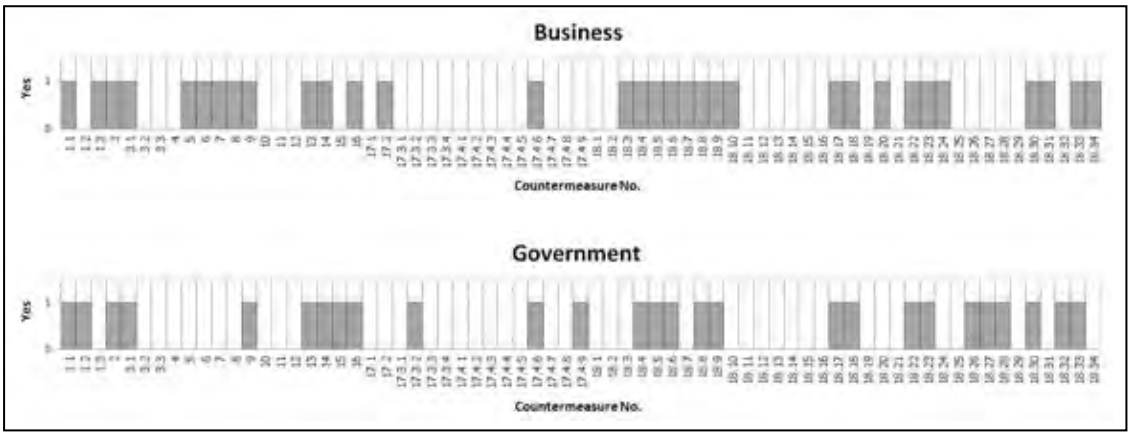


ภาพที่ 4.15 แผนภูมิเรดาร์ระดับความมั่นคงโดยรวมในแต่ละโดเมนธุรกิจของเว็บเซอร์วิซ

4.1.1.4 รูปแบบบริการของเว็บเซอร์วิซ

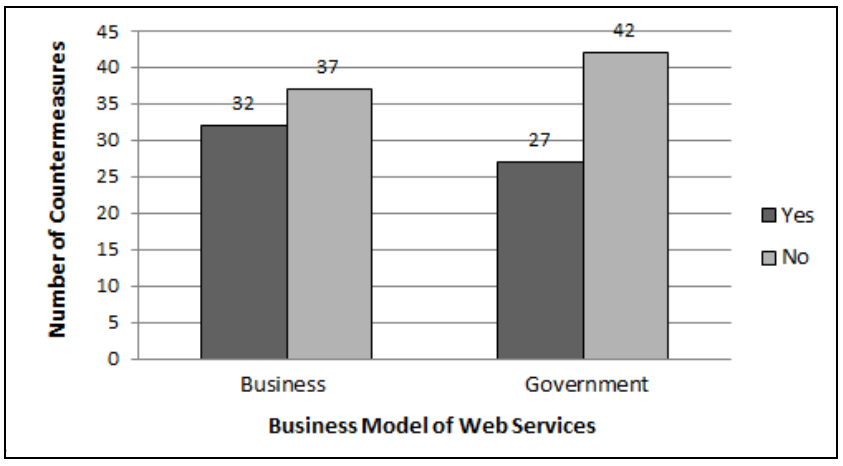
รูปแบบบริการของเว็บเซอร์วิซสามารถแบ่งได้เป็น 2 ด้าน ได้แก่ ด้านธุรกิจ (Business: B2B, B2C, C2C) และด้านภาครัฐ (G2G, G2B, G2C) โดยในแต่ละด้านจะแสดงภาพรวมรายการวิธีการรับมือที่ทำ ปริมาณวิธีการรับมือ ค่าคะแนนและระดับความมั่นคงของรูปแบบบริการ ดังนี้

1) รายการวิธีการรับมือที่ทำในแต่ละรูปแบบบริการ ดังภาพที่ 4.16



ภาพที่ 4.16 วิธีการรับมือการโจมตีที่ทำในแต่ละรูปแบบบริการของเว็บเซอร์วิซ

2) ปริมาณการทำและไม่ทำวิธีการรับมือ จากภาพที่ 4.16 เมื่อนำมาพิจารณาตามจำนวนวิธีการรับมือการโจมตีที่แต่ละรูปแบบบริการของเว็บเซอร์วิซทำและไม่ทำจะได้ดังภาพที่ 4.17



ภาพที่ 4.17 ปริมาณการทำและไม่ทำวิธีการรับมือของรูปแบบบริการของเว็บเซอร์วิซ

จากภาพที่ 4.16 และ 4.17 พบว่าในภาพรวมด้านธุรกิจ มีจำนวนการทำวิธีการรับมือมากกว่าด้านภาครัฐ

3) ค่าคะแนนและระดับความมั่นคงของรูปแบบบริการ เมื่อนำมาคำนวณตามแบบจำลอง ได้ผลดังตารางที่ 4.18

ตารางที่ 4.18 ค่าคะแนนและระดับความมั่นคงของรูปแบบบริการ

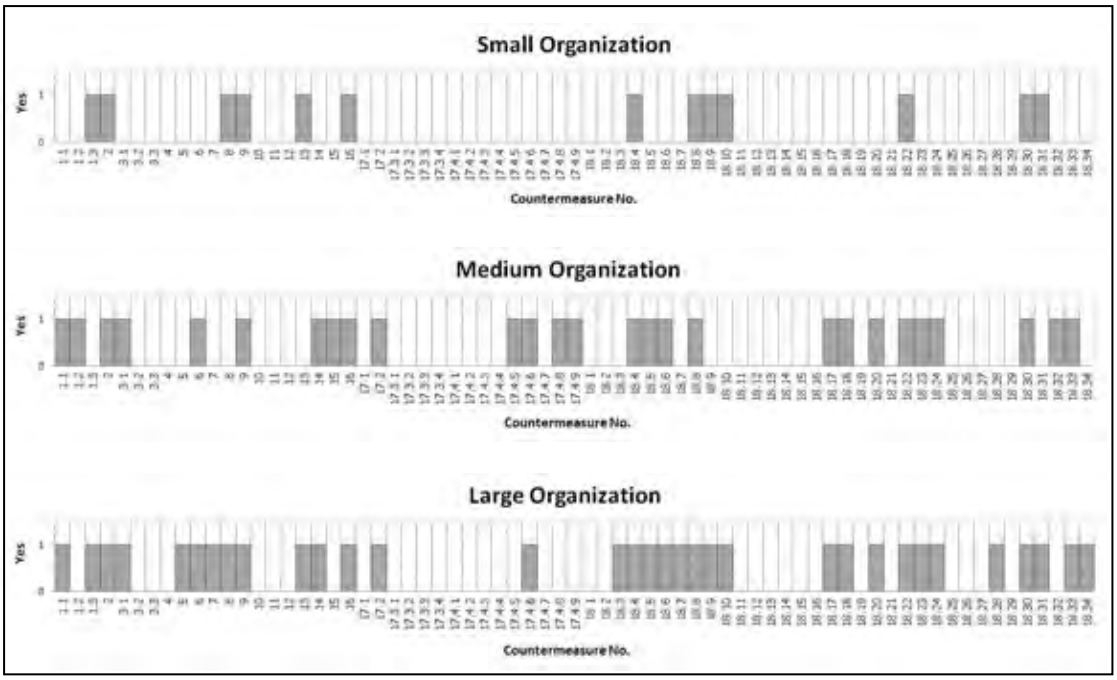
Business Model	Security Score						Security Level					
	S_{SEV}	S_{LOE}	S_{CON}	S_{INT}	S_{AVA}	S_{ALL}	S_{SEV}	S_{LOE}	S_{CON}	S_{INT}	S_{AVA}	S_{ALL}
Business	221	149	128	127	105	146	H	H	H	H	H	H
Government	171	111	92	98	84	111.2	M	M	M	M	M	M

จากตารางเมื่อพิจารณา S_{ALL} พบว่ารูปแบบบริการของเว็บเซอร์วิซด้านธุรกิจมีความมั่นคงอยู่ในระดับสูงซึ่งสูงกว่าด้านภาครัฐที่อยู่ในระดับปานกลาง

4.1.1.5 **ขนาดของหน่วยงาน**

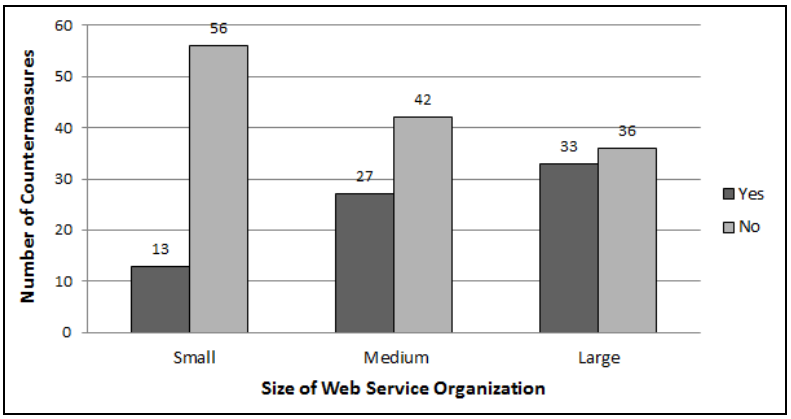
ขนาดของหน่วยงานของผู้ให้บริการเว็บเซอร์วิซแบ่งออกเป็น 3 ขนาด ได้แก่ ขนาดเล็ก (น้อยกว่า 50 คน) ขนาดกลาง (50-200 คน) และขนาดใหญ่ (มากกว่า 200 คน) โดยในแต่ละขนาดของหน่วยงานจะแสดงภาพรวมรายการวิธีการรับมือที่ทำ ปริมาณวิธีการรับมือ ค่าคะแนนและระดับความมั่นคงของขนาดหน่วยงาน ดังนี้

1) รายการวิธีการรับมือที่ทำในแต่ละขนาดของหน่วยงาน ดังภาพที่ 4.18



ภาพที่ 4.18 วิธีการรับมือการโจมตีที่ทำในแต่ละขนาดของหน่วยงานเว็บเซอร์วิซ

2) ปริมาณการทำและไม่ทำวิธีการรับมือ จากภาพที่ 4.18 เมื่อนำมาพิจารณาตามจำนวนวิธีการรับมือการโจมตีที่แต่ละขนาดของหน่วยงานทำและไม่ทำ จะได้ดังภาพที่ 4.19



ภาพที่ 4.19 ปริมาณการทำและไม่ทำวิธีการรับมือตามขนาดของหน่วยงาน

จากภาพที่ 4.18 และ 4.19 พบว่าภาพรวมของหน่วยงานที่มีขนาดใหญ่ จะมีจำนวนการทำวิธีการรับมือมากกว่าหน่วยงานขนาดกลางและเล็ก ตามลำดับ

3) ค่าคะแนนและระดับความมั่นคงของขนาดหน่วยงาน เมื่อนำมาคำนวณตามแบบจำลอง ได้ผลดังตารางที่ 4.19

ตารางที่ 4.19 ค่าคะแนนและระดับความมั่นคงของขนาดหน่วยงาน

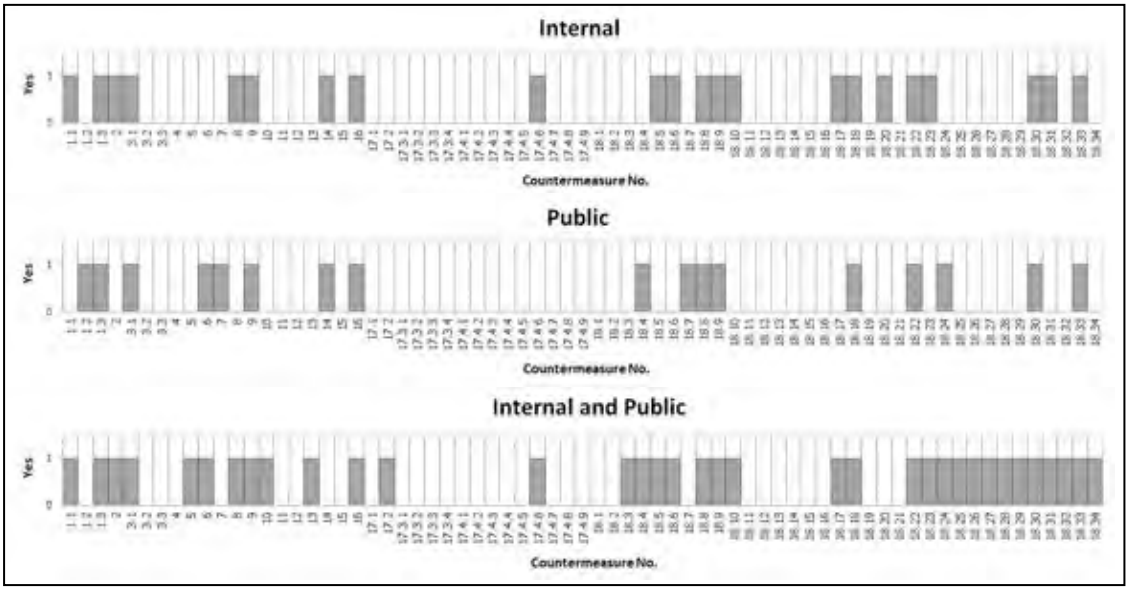
Organization Size	Security Score						Security Level					
	S_{SEV}	S_{LOE}	S_{CON}	S_{INT}	S_{AVA}	S_{ALL}	S_{SEV}	S_{LOE}	S_{CON}	S_{INT}	S_{AVA}	S_{ALL}
Small	123	88	77	76	55	83.8	L	M	M	M	L	M
Medium	152	96	76	85	82	98.2	M	M	M	M	M	M
Large	221	149	128	127	105	146	H	H	H	H	H	H

จากตารางเมื่อพิจารณา S_{ALL} พบว่าหน่วยงานขนาดใหญ่มีความมั่นคงอยู่ในระดับสูงซึ่งสูงกว่าหน่วยงานขนาดกลางและเล็กที่อยู่ในระดับปานกลาง

4.1.1.6 ลักษณะการใช้งานเว็บเซอร์วิซ

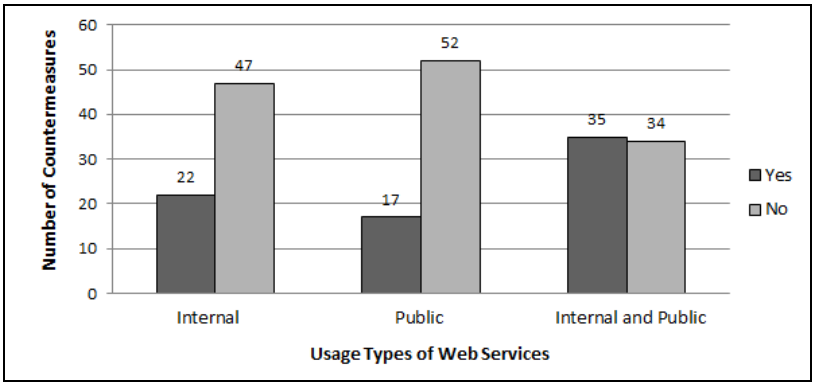
ลักษณะการใช้งานเว็บเซอร์วิซ แบ่งออกเป็น 3 ลักษณะ ได้แก่ ภายในองค์กร (Internal) สาธารณะ (Public) และทั้งภายในองค์กรและสาธารณะ (Internal and Public) โดยในแต่ละขนาดของหน่วยงานจะแสดงภาพรวมรายการวิธีการรับมือที่ทำ ปริมาณวิธีการรับมือ ค่าคะแนนและระดับความมั่นคงของลักษณะการใช้งาน ดังนี้

1) รายการวิธีการรับมือที่ทำในแต่ละลักษณะการใช้งาน ดังภาพที่ 4.20



ภาพที่ 4.20 วิธีการรับมือการโจมตีที่ทำในแต่ละลักษณะการใช้งานเว็บเซอร์วิซ

2) ปริมาณการทำและไม่ทำวิธีการรับมือ จากภาพที่ 4.20 เมื่อนำมาพิจารณาตามจำนวนวิธีการรับมือการโจมตีที่แต่ละลักษณะการใช้งานเว็บเซอร์วิซทำและไม่ทำจะได้ดังภาพที่ 4.21



ภาพที่ 4.21 ปริมาณการทำและไม่ทำวิธีการรับมือของลักษณะการใช้งานเว็บเซอร์วิซ

จากภาพที่ 4.20 และ 4.21 พบว่าภาพรวมของลักษณะการใช้งานแบบทั้งภายในองค์กรและสาธารณะ จะมีจำนวนการทำวิธีการรับมือมากกว่าแบบภายในองค์กร และแบบสาธารณะ และพบว่าแบบภายในองค์กรมีจำนวนวิธีการรับมือมากกว่าแบบสาธารณะ จากกลุ่มตัวอย่างนี้เว็บเซอร์วิซที่ให้บริการแบบทั้งภายในองค์กรและสาธารณะ และแบบภายในองค์กร ส่วนใหญ่เกี่ยวข้องกับธุรกิจธนาคาร จึงมีแนวโน้มที่จะเข้มงวดในด้านความมั่นคง

3) ค่าคะแนนและระดับความมั่นคงของลักษณะการใช้งานเว็บเซอร์วิซ เมื่อนำมาคำนวณตามแบบจำลอง ได้ผลดังตารางที่ 4.20

ตารางที่ 4.20 ค่าคะแนนและระดับความมั่นคงของลักษณะการใช้งานเว็บเซอร์วิซ

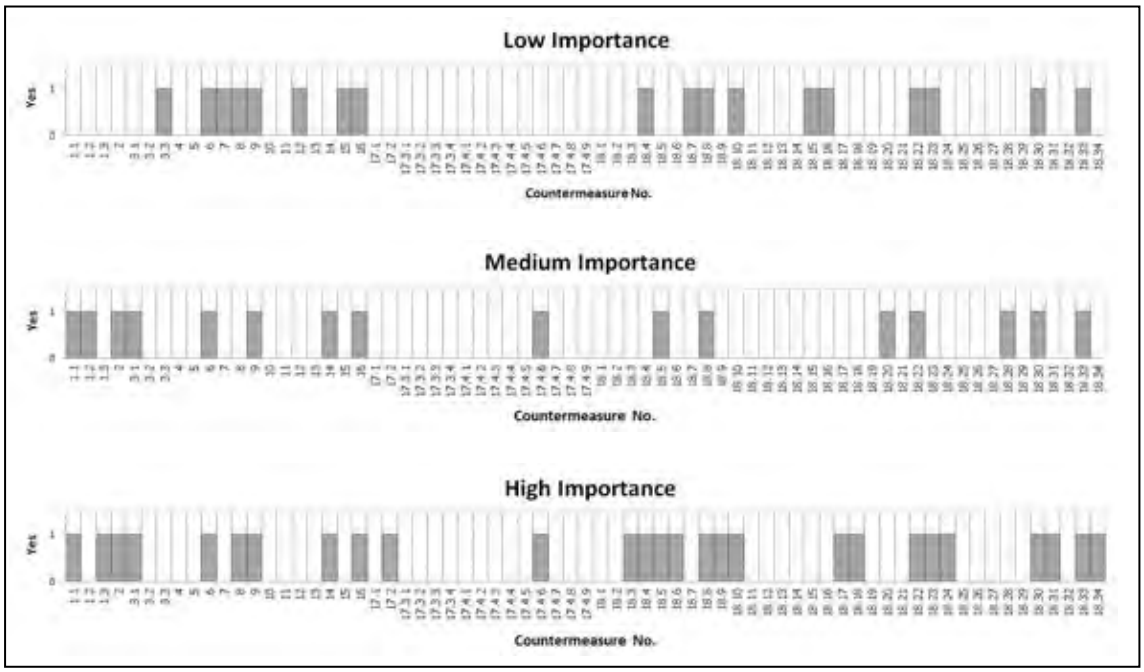
Usage Type of Service	Security Score						Security Level					
	S_{SEV}	S_{LOE}	S_{CON}	S_{INT}	S_{AVA}	S_{ALL}	S_{SEV}	S_{LOE}	S_{CON}	S_{INT}	S_{AVA}	S_{ALL}
Internal	162	108	89	97	81	107.4	M	M	M	M	M	M
Public	125	85	76	72	62	84	M	L	M	M	L	L
Internal and Public	211	143	121	124	100	139.8	H	H	H	H	H	H

จากตารางเมื่อพิจารณา S_{ALL} พบว่าลักษณะการใช้งานเว็บเซอร์วิซแบบภายในองค์กรและสาธารณะมีความมั่นคงอยู่ในระดับสูงซึ่งสูงกว่าแบบภายในองค์กรที่อยู่ในระดับปานกลางและแบบสาธารณะที่อยู่ในระดับต่ำ

4.1.1.7 **ความสำคัญของเว็บเซอร์วิซ**

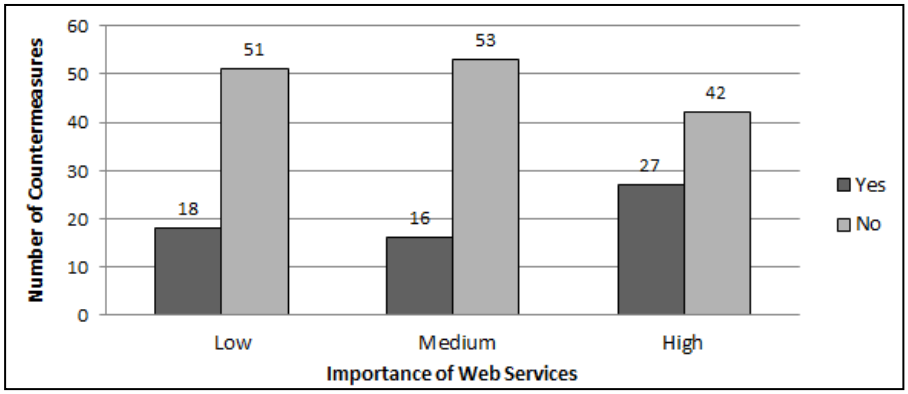
ความสำคัญของเว็บเซอร์วิซ แบ่งออกเป็น 3 ระดับ ได้แก่ ความสำคัญของเว็บเซอร์วิซระดับสูง (High) ระดับปานกลาง (Medium) และระดับต่ำ (Low) โดยในแต่ละความสำคัญของเว็บเซอร์วิซจะแสดงภาพรวมรายการวิธีการรับมือที่ทำ ปริมาณวิธีการรับมือ ค่าคะแนนและระดับความมั่นคงของความสำคัญของเว็บเซอร์วิซ ดังนี้

1) รายการวิธีการรับมือที่ทำในแต่ละความสำคัญของเว็บเซอร์วิซ ดังภาพที่ 4.22



ภาพที่ 4.22 วิธีการรับมือการโจมตีที่ทำในแต่ละความสำคัญของเว็บเซอร์วิซ

2) ปริมาณการทำและไม่ทำวิธีการรับมือ จากภาพที่ 4.22 เมื่อนำมาพิจารณาตามจำนวนวิธีการรับมือการโจมตีที่แต่ละความสำคัญของเว็บเซอร์วิซทำและไม่ทำ จะได้ดังภาพที่ 4.23



ภาพที่ 4.23 ปริมาณการทำวิธีการรับมือตามความสำคัญของเว็บเซอร์วิซ

จากภาพที่ 4.22 และ 4.23 พบว่าภาพรวมของเว็บเซอร์วิซที่มีความสำคัญในระดับสูง จะมีจำนวนการทำวิธีการรับมือมากกว่าเว็บเซอร์วิซที่มีความสำคัญในระดับต่ำและปานกลาง

3) ค่าคะแนนและระดับความมั่นคงตามความสำคัญของเว็บเซอร์วิซ เมื่อนำมาคำนวณตามแบบจำลอง ได้ผลดังตารางที่ 4.21

ตารางที่ 4.21 ค่าคะแนนและระดับความมั่นคงตามความสำคัญของเว็บเซอร์วิซ

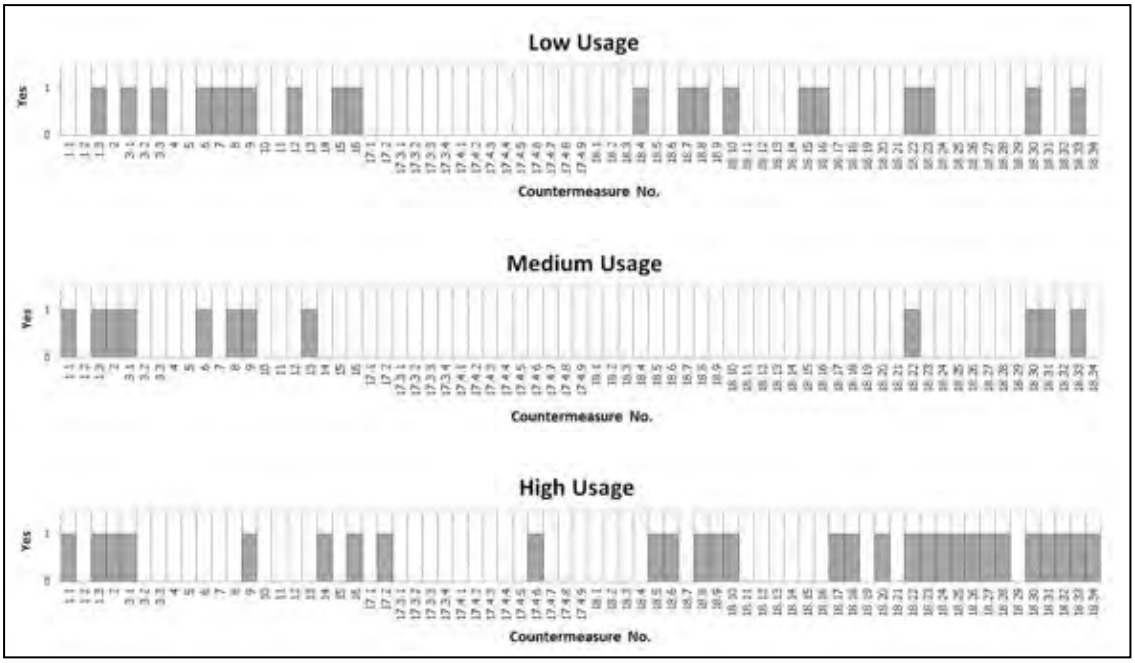
Importance of Service	Security Score						Security Level					
	S_{SEV}	S_{LOE}	S_{CON}	S_{INT}	S_{AVA}	S_{ALL}	S_{SEV}	S_{LOE}	S_{CON}	S_{INT}	S_{AVA}	S_{ALL}
Low	130	82	69	78	69	85.6	M	M	M	M	M	M
Medium	126	85	68	73	67	83.8	L	M	M	L	M	M
High	177	116	100	103	85	116.2	M	M	H	M	M	M

จากตารางเมื่อพิจารณา S_{ALL} พบว่าเว็บเซอร์วิซที่มีความสำคัญสูงมีค่าคะแนนความมั่นคงสูงกว่าเว็บเซอร์วิซที่มีความสำคัญต่ำและปานกลาง แต่ถ้าพิจารณาตามระดับความมั่นคงจะพบว่าความสำคัญของเว็บเซอร์วิซทั้ง 3 ระดับจะมีระดับความมั่นคงปานกลาง

4.1.1.8 ปริมาณการใช้งานเว็บเซอร์วิซ

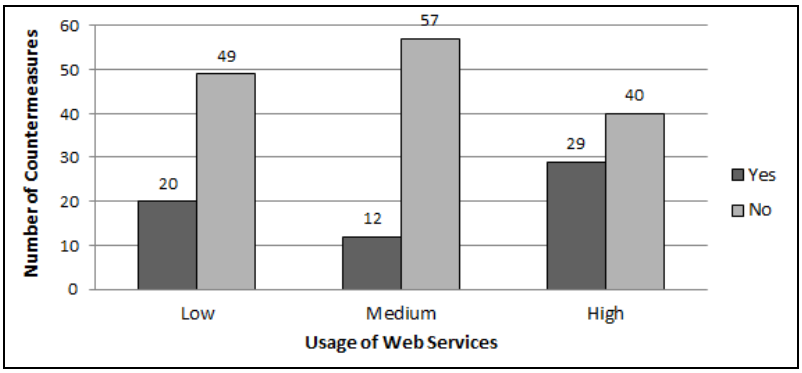
ปริมาณการใช้งานเว็บเซอร์วิซ แบ่งออกเป็น 3 ปริมาณ ได้แก่ ปริมาณการใช้งานสูง (Hligh) ปานกลาง (Medium) และต่ำ (Low) โดยในแต่ละปริมาณการใช้งานเว็บเซอร์วิซจะแสดงภาพรวมรายการวิธีการรับมือที่ทำ ปริมาณวิธีการรับมือ ค่าคะแนนและระดับความมั่นคงของปริมาณการใช้งานเว็บเซอร์วิซ ดังนี้

1) รายการวิธีการรับมือที่ทำในแต่ละปริมาณการใช้งาน ดังภาพที่ 4.24



ภาพที่ 4.24 วิธีการรับมือการโจมตีที่ทำในแต่ละปริมาณการใช้งานของเว็บเซอร์วิซ

2) ปริมาณการทำและไม่ทำวิธีการรับมือ จากภาพที่ 4.24 เมื่อนำมาพิจารณาตามจำนวนวิธีการรับมือการโจมตีที่แต่ละปริมาณการใช้งานของเว็บเซอร์วิซทำและไม่ทำจะได้ดังภาพที่ 4.25



ภาพที่ 4.25 ปริมาณการทำและไม่ทำวิธีการรับมือตามปริมาณการใช้งานของเว็บเซอร์วิซ

จากภาพที่ 4.24 และ 4.25 พบว่าภาพรวมของเว็บเซอร์วิซที่มีปริมาณการใช้งานระดับสูงจะมีจำนวนการทำวิธีการรับมือมากกว่าปริมาณการใช้งานระดับต่ำและปานกลาง ตามลำดับ

3) ค่าคะแนนและระดับความมั่นคงของปริมาณการใช้งานเว็บเซอร์วิซ เมื่อนำมาคำนวณตามแบบจำลอง ได้ผลดังตารางที่ 4.22

ตารางที่ 4.22 ค่าคะแนนและระดับความมั่นคงของปริมาณการใช้งานเว็บเซอร์วิซ

Usage of Service	Security Score						Security Level					
	S_{SEV}	S_{LOE}	S_{CON}	S_{INT}	S_{AVA}	S_{ALL}	S_{SEV}	S_{LOE}	S_{CON}	S_{INT}	S_{AVA}	S_{ALL}
Low	144	90	76	85	76	94.2	M	M	M	M	M	M
Medium	119	88	69	72	61	81.8	L	L	M	M	L	L
High	169	109	92	100	81	110.2	M	M	M	M	M	M

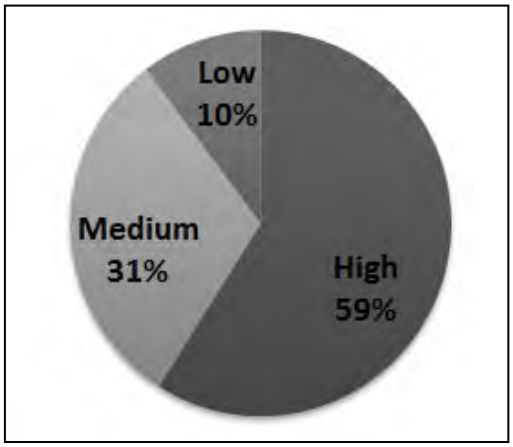
จากตารางเมื่อพิจารณา S_{ALL} พบว่าเว็บเซอร์วิซที่มีปริมาณการใช้งานสูงมีค่าคะแนนความมั่นคงสูงกว่าเว็บเซอร์วิซที่มีปริมาณการใช้งานต่ำและปานกลาง แต่ถ้าพิจารณาตามระดับความมั่นคง พบว่าเว็บเซอร์วิซที่มีปริมาณการใช้งานสูงและต่ำจะอยู่ในระดับปานกลางซึ่งมีความมั่นคงกว่าเว็บเซอร์วิซที่มีปริมาณการใช้งานปานกลางที่มีความมั่นคงอยู่ในระดับต่ำ

4.1.2 การประเมินแบบจำลองการวัดความมั่นคงโดยผู้ให้บริการ

การประเมินแบบจำลองการวัดความมั่นคงโดยผู้ให้บริการ 39 ราย ประกอบด้วย 1) ความสนใจด้านความมั่นคง 2) ความเข้าใจในการกรอกข้อมูล 3) การประเมินความน่าเชื่อถือของแผ่นแบบการจัดให้มีวิธีการรับมือ (Countermeasure Provision Template) 4) การประเมินแนวคิดและวิธีการให้ค่าความมั่นคงของแบบจำลองงานวิจัย และ 5) ประโยชน์ที่ได้จากงานวิจัย

4.1.2.1 ความสนใจด้านความมั่นคง

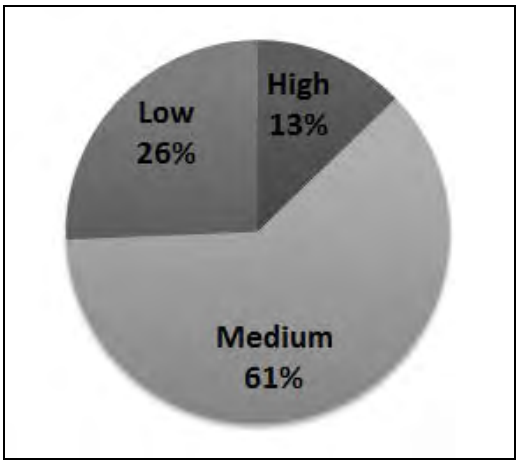
ความสนใจด้านความมั่นคงของผู้ให้บริการ กำหนดไว้ 3 ระดับ ได้แก่ สูง(High) ปานกลาง (Medium) และต่ำ (Low) ผลที่ได้พบว่า ผู้ให้บริการส่วนใหญ่ให้ความสนใจด้านความมั่นคงในระดับสูง ซึ่งมีจำนวน 23 คน คิดเป็น 59% ระดับปานกลาง มีจำนวน 12 คน คิดเป็น 31% และระดับต่ำ มีจำนวน 4 คน คิดเป็น 10% ดังภาพที่ 4.26



ภาพที่ 4.26 ระดับความสนใจด้านความมั่นคงของผู้ให้บริการ

4.1.2.2 ความเข้าใจในการกรอกข้อมูล

ความเข้าใจในการกรอกข้อมูลของผู้ให้บริการ เพื่อให้ทราบว่าในการนำไปใช้งานจริงผู้ใช้ส่วนใหญ่สามารถจะเข้าใจได้ในระดับใด กำหนดไว้ 3 ระดับ ได้แก่ สูง (High) ปานกลาง (Medium) และ ต่ำ (Low) ผลที่ได้พบว่า ผู้ให้บริการที่มีความเข้าใจในการกรอกข้อมูลในระดับสูง มีจำนวน 5 คน คิดเป็น 13% ระดับปานกลาง มีจำนวน 24 คน คิดเป็น 61% และระดับต่ำ มีจำนวน 10 คน คิดเป็น 26% ดังภาพที่ 4.27

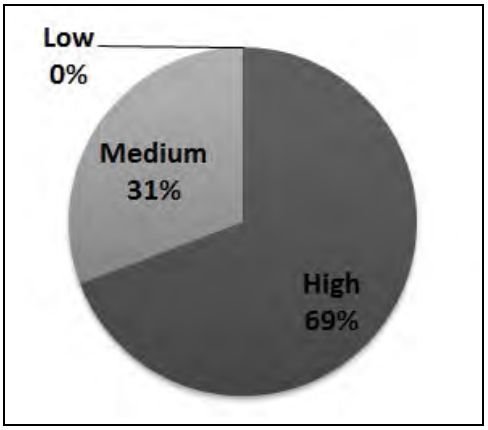


ภาพที่ 4.27 ระดับความเข้าใจในการกรอกข้อมูลของผู้ให้บริการ

จะเห็นว่าผู้ให้บริการส่วนใหญ่สามารถทำความเข้าใจในการกรอกข้อมูลได้ในระดับปานกลาง ด้วยเหตุผลว่า ผู้กรอกข้อมูลมีความรู้เกี่ยวกับเว็บเซอร์วิซในด้านความมั่นคงเพียงบางส่วน เพราะแบบสอบถามนี้จำเป็นต้องมีความรู้พื้นฐานด้านความมั่นคงที่สูงจึงจะทราบได้ ซึ่งในความเป็นจริงแล้วอาจไม่สามารถทราบและเข้าถึงกลไกการทำงานและความมั่นคงของโครงสร้างพื้นฐานในองค์กรได้อย่างครอบคลุมและละเอียดในทุกหน่วยงาน

4.1.2.3 การประเมินความน่าเชื่อถือของแผ่นแบบการจัดให้มีวิธีการรับมือ

การประเมินความน่าเชื่อถือของแผ่นแบบการจัดให้มีวิธีการรับมือ (ในตารางที่ 3.4) เพื่อให้ทราบว่าข้อมูลในแผ่นแบบการจัดให้มีวิธีการรับมือมีความน่าเชื่อถือในระดับใด กำหนดไว้ 3 ระดับ ได้แก่ สูง (High) ปานกลาง (Medium) และต่ำ (Low) ผลที่ได้พบว่า ผู้ให้บริการส่วนใหญ่ประเมินความน่าเชื่อถือของแผ่นแบบการจัดให้มีวิธีการรับมือในระดับสูง ซึ่งมีจำนวน 27 คน คิดเป็น 69% และระดับปานกลาง มีจำนวน 12 คน คิดเป็น 31% ดังภาพที่ 4.28

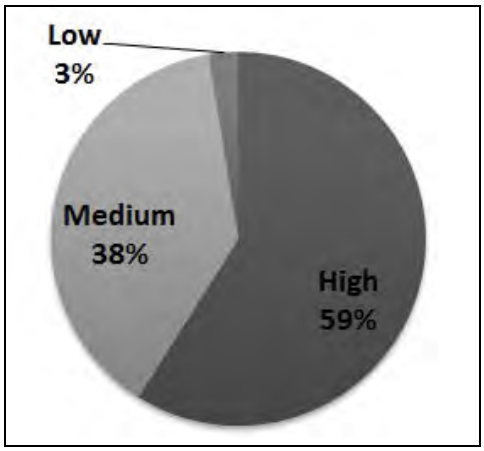


ภาพที่ 4.28 ผลการประเมินความน่าเชื่อถือของแผ่นแบบการจัดให้มีวิธีการรับมือ

จะเห็นว่าผู้ให้บริการส่วนใหญ่ประเมินความน่าเชื่อถือของแผ่นแบบการจัดให้มีวิธีการรับมือในระดับสูง ด้วยเหตุผลว่า เนื้อหามีความสมเหตุสมผลค่อนข้างครอบคลุมทั้งวิธีการรับมือและรูปแบบการโจมตีมีมากพอต่อการวิเคราะห์สภาพความมั่นคงโดยรวม อีกทั้งทำให้เห็นถึงความสัมพันธ์ระหว่างการโจมตีและวิธีการรับมือได้อย่างชัดเจน

4.1.2.4 การประเมินความสมเหตุสมผลของแบบจำลองการวัดความมั่นคง

การประเมินความสมเหตุสมผลของแบบจำลองการวัดความมั่นคง เพื่อให้ทราบว่าแนวคิดและวิธีการคำนวณตามแบบจำลองการวัดความมั่นคงมีความน่าเชื่อถือในระดับใด กำหนดไว้ 3 ระดับ ได้แก่ สูง (High) ปานกลาง (Medium) และต่ำ (Low) ผลที่ได้พบว่า ผู้ให้บริการส่วนใหญ่ประเมินแบบจำลองแนวคิดและวิธีการให้ค่าความมั่นคงของงานวิจัยในระดับสูง ซึ่งมีจำนวน 23 คน คิดเป็น 59% ระดับปานกลาง มีจำนวน 15 คน คิดเป็น 38% และระดับต่ำ มีจำนวน 1 คน คิดเป็น 3% ดังภาพที่ 4.29

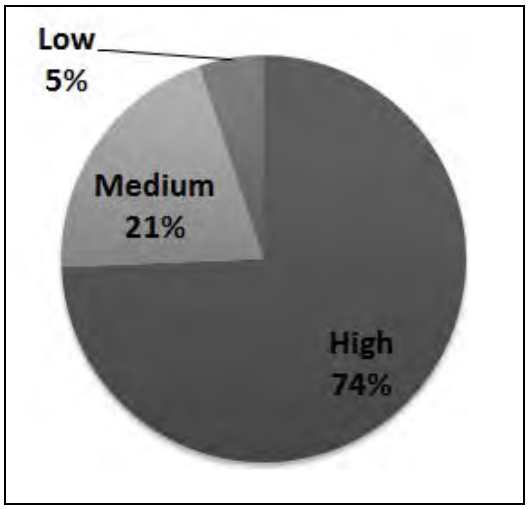


ภาพที่ 4.29 ผลการประเมินความสมเหตุสมผลของแบบจำลองการวัดความมั่นคง

จะเห็นว่าผู้ให้บริการส่วนใหญ่ประเมินความสมเหตุสมผลของแบบจำลองการวัดความมั่นคงในระดับสูง ด้วยเหตุผลว่า เนื้อหาค่อนข้างครอบคลุม สมเหตุสมผลและมีความน่าเชื่อถือ เนื่องจากได้มีการนำวิธีการรับมือและคุณสมบัติของการโจมตีที่เป็นที่ยอมรับกันมาใช้อ้างอิงในการคำนวณ ทำให้ผลลัพธ์ที่ได้ค่อนข้างหลากหลายและค่าผลลัพธ์ที่ได้มีความเหมาะสมกับองค์กรที่เป็นอยู่

4.1.2.5 ประโยชน์ที่ได้จากงานวิจัย

ประโยชน์ที่ได้จากงานวิจัยประเมินโดยผู้ให้บริการ กำหนดไว้ 3 ระดับ ได้แก่ สูง (High) ปานกลาง (Medium) และต่ำ (Low) ผลที่ได้พบว่า ผู้ให้บริการส่วนใหญ่ประเมินประโยชน์ที่ได้จากงานวิจัยในระดับที่สูง ซึ่งมีจำนวน 29 คน คิดเป็น 74% ระดับปานกลาง มีจำนวน 8 คน คิดเป็น 21% และระดับต่ำ มีจำนวน 2 คน คิดเป็น 5% ดังภาพที่ 4.30



ภาพที่ 4.30 ผลการประเมินประโยชน์ที่ได้จากงานวิจัย

จะเห็นว่าผู้ให้บริการส่วนใหญ่ประเมินประโยชน์ที่ได้จากงานวิจัยในระดับสูง ด้วยเหตุผลว่า สามารถนำไปใช้ตรวจสอบและประเมินความมั่นคงให้กับเว็บเซอร์วิซในองค์กรต่างๆได้ และช่วยพัฒนาระดับความรู้ทางด้านความมั่นคงให้กับผู้ประเมินและนำแบบจำลองนี้ไปประยุกต์ใช้เพื่อเป็นแนวทางในการออกแบบเว็บเซอร์วิซและระบบที่ต้องการความมั่นคงสูงให้เข้ากับองค์กรได้

4.2 การประเมินความมั่นคงของเว็บเซอร์วิซในฐานะเป็นผู้ใช้บริการ

การประเมินความมั่นคงของเว็บเซอร์วิซในฐานะเป็นผู้ใช้บริการซึ่งเป็นผู้ที่เรียกใช้งานเว็บเซอร์วิซ (Developer) เป็นการประเมินเว็บเซอร์วิซที่ประกาศไว้แบบสาธารณะจำนวน 30 บริการ โดยพิจารณาความสามารถในการรับมือการโจมตีจากรายละเอียดของเว็บเซอร์วิซนั้นๆเท่าที่มีประกาศไว้ จากการพิจารณาวิธีการรับมือทั้งหมดโดยเว็บเซอร์วิซเหล่านี้พบว่ามี 7 รายการ ดังตารางที่ 4.23 จาก 69 รายการที่เป็นวิธีการรับมือที่ผู้ใช้บริการสามารถพิจารณาเบื้องต้นได้ด้วยตนเอง สำหรับเป็นข้อมูลประกอบการเลือกใช้งานเว็บเซอร์วิซในกรณีที่ผู้ใช้บริการไม่ทราบรายละเอียดด้านความมั่นคงของเว็บเซอร์วิซนั้นๆ (เนื่องจากการประเมินตามแบบจำลองนี้จะเน้นไปที่ผู้ให้บริการ ซึ่งเป็นนักเขียนโปรแกรม ผู้ดูแลเว็บเซอร์วิซ และตำแหน่งอื่นๆที่เกี่ยวข้องเป็นหลัก) เครื่องหมาย * ในตาราง หมายถึงวิธีการรับมือนั้นไม่มีตัวอย่างการใช้งานในเว็บเซอร์วิซสาธารณะ 30 บริการที่พิจารณา แต่จาก [28] ผู้ใช้บริการสามารถพิจารณาเองได้หากเว็บเซอร์วิซนำมาใช้งานจริง

ตารางที่ 4.23 รายการวิธีการรับมือที่ผู้ใช้บริการสามารถประเมินเบื้องต้นได้ด้วยตนเอง

CM No.	Countermeasure name	Documents for Assessment
*1.1	XML Encryption	Handout and Documents/ WS-SecurityPolicy/ Tools
1.2	XML Signature	Handout and Documents/ WS-SecurityPolicy/ Tools
1.3	Security Tokens	Handout and Documents / WS-SecurityPolicy/ Tools
2	Transport-level Security Mechanisms	Handout and Documents / Tools
4	Schema Hardening	Handout and Documents/ Schema/ WSDL
18.15	Do not use Unix and Linux systems	Handout and Documents/ Tools
18.16	Disallowing the inclusion of DTDs in SOAP messages	Handout and Documents/ Schema

จากตารางสามารถแสดงตัวอย่างการประเมินตามวิธีการพิจารณา ดังนี้

1) พิจารณาจากคู่มือและเอกสารอ้างอิง (Handout and Documents)

การพิจารณานี้สามารถบอกได้ครอบคลุมในส่วนที่ผู้ให้บริการกล่าวถึงความมั่นคงของเว็บเซอร์วิซ ว่าได้มีการทำวิธีการรับมือใดบ้าง ซึ่งอาจมีวิธีการรับมือมากกว่า 7 รายการข้างต้นก็เป็นได้ (แต่เนื่องจากในการทดลองนี้ผู้วิจัยได้สืบค้นและเรียกใช้งานเว็บเซอร์วิซจำนวน 30 บริการ จึงได้ข้อสรุปในที่นี้คือ 7 รายการ) ตัวอย่างเช่น คู่มือหรือเอกสารมีการบอกว่าใช้กลไกดับเบิลยูเอส-ซี

เคียวริตี ได้แก่ การเข้ารหัสเอกซ์เอ็มแอล การลงลายเซ็นเอกซ์เอ็มแอล และโทเคนความมั่นคง รวมทั้งมีกลไกความมั่นคงระดับทรานสปอร์ต จากข้อมูลเหล่านี้ผู้ใช้บริการจะสามารถพิจารณาได้

2) นโยบายดับเบิลยูเอส-ซีเคียวริตี (WS-SecurityPolicy)

นโยบายดับเบิลยูเอส-ซีเคียวริตี [28] เป็นการกำหนดรายละเอียดด้านความมั่นคงให้ผู้ใช้บริการได้ทราบว่าเว็บเซอร์วิซนั้นได้รองรับความมั่นคงใดบ้าง ซึ่งการพิจารณาเบื้องต้นพบว่าสามารถตรวจสอบได้ 3 รายการ ได้แก่ รายการที่ 1.1 การเข้ารหัสเอกซ์เอ็มแอล รายการที่ 1.2 ลายเซ็นเอกซ์เอ็มแอล และรายการที่ 1.3 โทเคนความมั่นคง โดยข้อมูลนี้จะแนบไว้ในส่วนของวิสเดิล ซึ่งในการนำมาใช้งานจะต้องมีโปรแกรมที่สนับสนุนการแปลงข้อมูลวิสเดิลที่มีนโยบายนี้ให้เป็นข้อความโซปที่แท็กตามที่กำหนดไว้ แต่ในการทดลองนี้ไม่สามารถหาตัวอย่างที่มีการใช้งานได้ครบทุกแบบเนื่องจากเว็บเซอร์วิซที่ค้นพบจากสาธารณะส่วนใหญ่ยังไม่มีประกาศไว้ ในที่นี้จึงขอแสดงเฉพาะตัวอย่างที่ได้อ้างอิงตามทฤษฎีว่าสามารถจะพิจารณาได้ ดังภาพที่ 4.31

```
<!-- Example Endpoint Policy -->
<wsp:Policy xmlns:wsp="..." xmlns:sp="...">
  <sp:AsymmetricBinding>
    <wsp:Policy>
      <sp:RecipientToken>
        <wsp:Policy>
          <sp:X509Token sp:IncludeToken=".../IncludeToken/Always" />
        </wsp:Policy>
     </sp:RecipientToken>
     <sp:InitiatorToken>
       <wsp:Policy>
         <sp:X509Token sp:IncludeToken=".../IncludeToken/Always" />
       </wsp:Policy>
     </sp:InitiatorToken>
     <sp:AlgorithmSuite>
       <wsp:Policy>
         <sp:Basic256 />
       </wsp:Policy>
     </sp:AlgorithmSuite>
     <sp:Layout>
        <wsp:Policy>
          <sp:Strict />
        </wsp:Policy>
     </sp:Layout>
     <sp:IncludeTimestamp />
     <sp:EncryptBeforeSigning />
     <sp:EncryptSignature />
     <sp:ProtectTokens />
   </wsp:Policy>
  </sp:AsymmetricBinding>
  <sp:SignedEncryptedSupportingTokens>
    <wsp:Policy>
      <sp:UsernameToken sp:IncludeToken=".../IncludeToken/Once" />
    </wsp:Policy>
  </sp:SignedEncryptedSupportingTokens>
  <sp:SignedEndorsingSupportingTokens>
    <wsp:Policy>
      <sp:X509Token sp:IncludeToken=".../IncludeToken/Once">
        <wsp:Policy>
          <sp:WssX509v3Token10 />
        </wsp:Policy>
      </sp:X509Token>
    </wsp:Policy>
  </sp:SignedEndorsingSupportingTokens>
  <sp:Wss11>
    <wsp:Policy>
      <sp:RequireSignatureConfirmation />
    </wsp:Policy>
  </sp:Wss11>
</wsp:Policy>
```

ภาพที่ 4.31 การตรวจสอบโดยพิจารณาจากนโยบายดับเบิลยูเอส-ซีเคียวริตี [28]

3) สคีมา (Schema)

การพิจารณานี้เบื้องต้นสามารถตรวจได้ 2 รายการ ได้แก่ รายการที่ 4 การทำให้สคีมามั่นคงขึ้น สามารถตรวจสอบได้เช่นดังภาพที่ 4.32 ถ้ามี <xs:element maxOccurs="unbounded" แสดงว่าไม่มีการทำรายการนี้ เพราะผู้โจมตีสามารถส่งข้อมูลจำนวนไม่จำกัดมาให้ได้ และรายการที่ 18.16 การไม่อนุญาตให้มีการใช้ดีทีดีในข้อความโซป เพราะดีทีดีจะมีความสามารถด้อยกว่าเอกซ์เอ็มแอลสคีมาในการกำหนดรูปแบบและเงื่อนไขของค่าข้อมูล ดังนั้นหากมีการใช้จะตรวจสอบได้ดังภาพที่ 4.33 ซึ่งเป็นสคีมาแบบดีทีดี

```
<xs:complexType name="address">
<xs:sequence>
<xs:element name="city" type="xs:string" minOccurs="0"></xs:element>
<xs:element name="country" type="xs:string" minOccurs="0"></xs:element>
<xs:element name="houseNumber" type="xs:string" minOccurs="0"></xs:element>
<xs:element name="street" type="xs:string" minOccurs="0"></xs:element>
<xs:element name="zipCode" type="xs:string" minOccurs="0"></xs:element>
</xs:sequence>
</xs:complexType>

<xs:simpleType name="artType">
<xs:restriction base="xs:string">
<xs:enumeration value="ACTOR"></xs:enumeration>
<xs:enumeration value="DIRECTOR"></xs:enumeration>
<xs:enumeration value="AUTHOR"></xs:enumeration>
<xs:enumeration value="PAINTER"></xs:enumeration>
</xs:restriction>
</xs:simpleType>

<xs:complexType name="artistArray" final="#all">
<xs:sequence>
<xs:element name="item" type="tns:artist" minOccurs="0" maxOccurs="unbounded" nillable="true"></xs:element>
</xs:sequence>
</xs:complexType>
</xs:schema>
```

ภาพที่ 4.32 การตรวจสอบสคีมาที่ไม่มีการทำให้สคีมามั่นคงขึ้น [29]

```
<!ELEMENT ls (total?), (file*)>
<!ELEMENT total (prompt, totalsize)>
<!ELEMENT file (permission?, blocks?, user?, group?, size?, date_m?, date_d?, date_ty?, fname)>
<!ELEMENT date_ty (date_y)>
<!ELEMENT date_ty (date_h, date_m)>
<!ELEMENT prompt (#PCDATA)>
<!ELEMENT totalsize (#PCDATA)>
<!ELEMENT permission (#PCDATA)>
<!ELEMENT blocks (#PCDATA)>
<!ELEMENT user (#PCDATA)>
<!ELEMENT group (#PCDATA)>
<!ELEMENT size (#PCDATA)>
<!ELEMENT date_y (#PCDATA)>
<!ELEMENT date_M (#PCDATA)>
<!ELEMENT date_d (#PCDATA)>
<!ELEMENT date_h (#PCDATA)>
<!ELEMENT date_m (#PCDATA)>
<!ELEMENT fname (#PCDATA)>
```

ภาพที่ 4.33 การตรวจสอบสคีมาที่เป็นแบบดีทีดี [30]

4) วิสเดิล (WSDL)

การพิจารณานี้เบื้องต้นสามารถตรวจได้ 1 รายการ ได้แก่ รายการที่ 4 การทำให้สคีมามั่นคงขึ้น วิธีการสังเกตจะคล้ายกับตรวจสอบที่สคีมา แต่ในส่วนนี้จะพิจารณาจากวิสเดิลแทน โดยดูจาก <wsdl:types> เช่นดังภาพที่ 4.34 และ 4.35 ข้อมูลที่ไม่ได้กำหนดข้อบังคับของรูปแบบไว้ชัดเจนจะเปิดโอกาสให้การส่งข้อมูลมาโจมตีทำได้สะดวกขึ้น

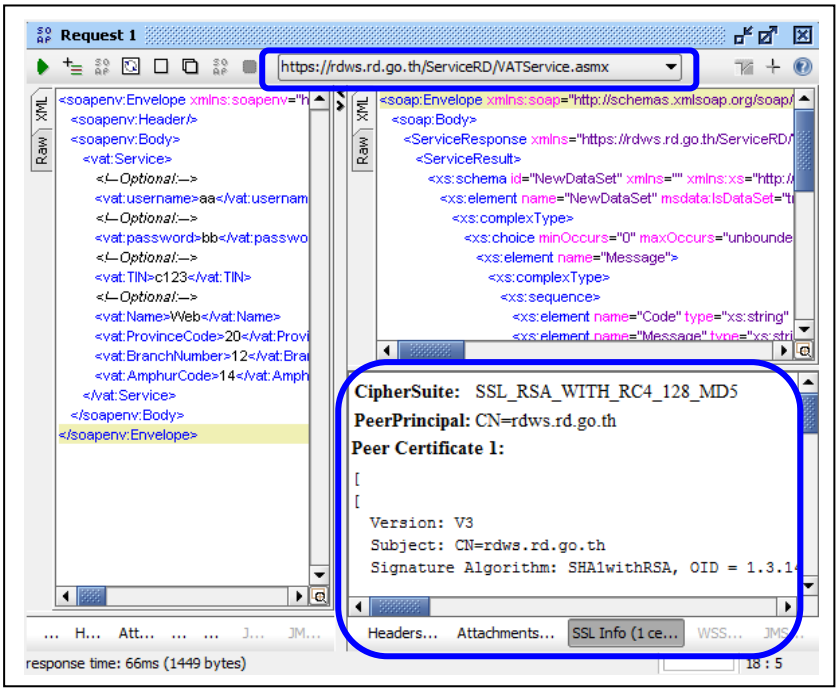
ภาพที่ 4.34 การตรวจสอบวิสเดิลที่มีการทำให้สคีมามั่นคงขึ้น [31]

ภาพที่ 4.35 การตรวจสอบวิสเดิลที่ไม่มีการทำให้สคีมามั่นคงขึ้น [32]

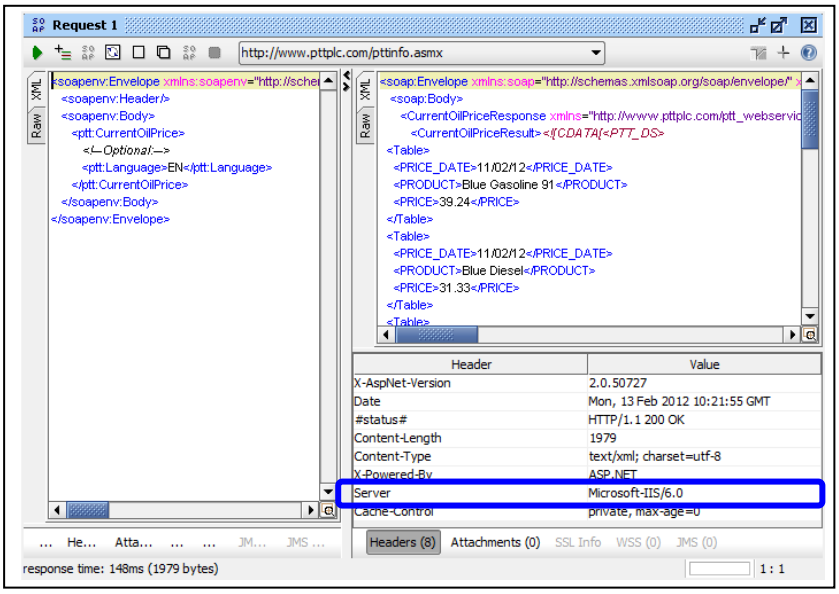
5) เครื่องมือ (Tools)

เครื่องมือในการทดลองอาจจะเป็นเครื่องมือทดสอบเว็บเซอร์วิซหรือเครื่องตรวจสอบอื่นๆก็ได้ (เครื่องมือตรวจสอบอื่นๆอาจเป็นโปรแกรมดักจับข้อมูลซึ่งส่วนใหญ่จะถูกใช้โดยผู้โจมตี) แต่ในงานวิจัยนี้ยกตัวอย่างเฉพาะเครื่องมือพื้นฐานทั่วไปในฐานะผู้ใช้บริการที่อาจไม่มีความรู้ด้านความมั่นคงมากนัก โดยได้เลือกใช้โปรแกรมโซปยูไอ (soapUI) [33] ซึ่งเป็นโปรแกรมทดสอบเว็บเซอร์วิซ

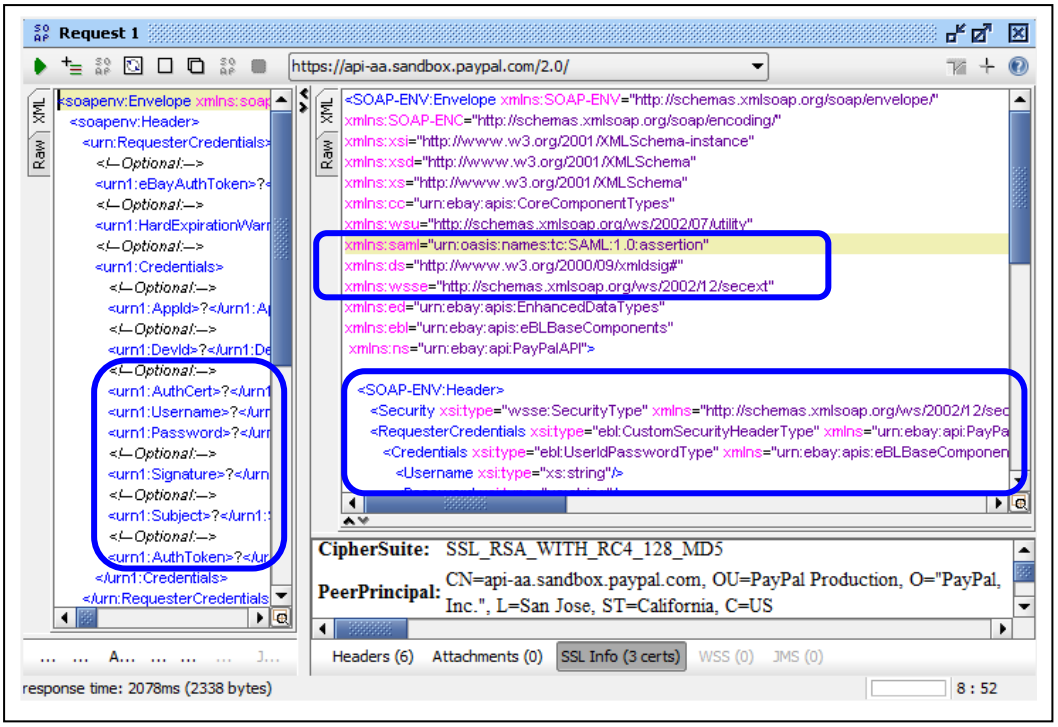
จากการทดลองสามารถตรวจได้ 5 รายการ ได้แก่ รายการที่ 2 กลไกความมั่นคงระดับทรานสปอร์ต สามารถตรวจสอบได้ดังภาพที่ 4.36 รายการที่ 18.15 การไม่ใช้ระบบยูนิกซ์และลีนุกซ์ ดังภาพที่ 4.37 รายการที่ 1.1 การเข้ารหัสเอกซ์เอ็มแอล (ไม่มีตัวอย่างข้อความโซป) รายการที่ 1.2 ลายเซ็นเอกซ์เอ็มแอล และรายการที่ 1.3 โทเคนความมั่นคง สามารถพิจารณาโดยดูจากข้อความโซป ดังภาพที่ 4.38



ภาพที่ 4.36 การตรวจสอบการใช้กลไกความมั่นคงระดับทรานสปอร์ต (ทดลองจาก [34])



ภาพที่ 4.37 การตรวจสอบการไม่ใช้ระบบยูนิกซ์และลีนุกซ์ (ทดลองจาก [31])



ภาพที่ 4.38 การตรวจสอบว่ามีลายเซ็นเอกซ์เอ็มแอลและโทเคนความมั่นคง (ทดลองจาก [35])

ผู้วิจัยได้ทดลองตรวจสอบรายการวิธีการรับมือกับเว็บเซอร์วิซจำนวน 30 บริการ ที่มีการใช้งานแบบสาธารณะ คือมีการเปิดเผยข้อมูลทั้งที่ได้พิจารณาจากคู่มือเอกสารอ้างอิง ข้อความโซป สคีมา วิสเดิล และเครื่องมือทดสอบเว็บเซอร์วิซ การรวบรวมเว็บเซอร์วิซทำโดยสืบค้นจากเว็บไซต์ที่เป็นแหล่งรวบรวมเว็บเซอร์วิซ ได้แก่ WebserviceX.NET [36] XMethods [37] WSDLL [38] UDDI Services [39] และเว็บไซต์หลักของบริการนั้นๆ ผลการทดลองเป็นดังตารางที่ 4.24 พบว่าบริการที่เกี่ยวข้องกับการเงินจะมีความมั่นคงมากกว่าบริการแบบเรียกดูข้อมูลทั่วไป ในส่วนของวิธีการรับมือรายการที่ 1.1 การเข้ารหัสเอกซ์เอ็มแอล จากการสืบค้นยังไม่พบว่ามีการใช้งานแบบสาธารณะอาจเป็นเพราะต้องมีการตกลงกันระหว่างผู้ให้บริการด้วยหรืออาจต้องใช้บริการแบบเก็บค่าใช้จ่าย เช่นเดียวกับรายการที่ 1.2 ลายเซ็นเอกซ์เอ็มแอล และ 1.3 โทเคนความมั่นคง ที่ในการทดลองก็มีเพียงส่วนน้อยเท่านั้นที่สามารถสืบค้นได้ เหตุผลอาจเป็นเช่นเดียวกับรายการที่ 1.1 ในการตรวจสอบรายที่ 18.15 การไม่ใช้ระบบยูนิกซ์และลีนุกซ์ พบว่าบางเว็บเซอร์วิซไม่มีการให้ข้อมูลหรือเครื่องมือตรวจพบข้อมูลแต่ไม่ทราบแน่ว่าเป็นหรือไม่ เช่น Apache Server, AmazonFPS Server จึงกำหนดเป็น N/A คือไม่สามารถระบุได้ และรายการที่ 18.16 การไม่อนุญาตให้มีการใช้ดีทีดีในข้อความโซป จากการสืบค้นเว็บเซอร์วิซโดยส่วนใหญ่พบว่าไม่มีการใช้สคีมาแบบดีทีดีแล้ว มีแต่ใช้สคีมาแบบเอกซ์เอ็มแอล จากแบบจำลองค่าคะแนนและระดับความมั่นคงที่ประเมินจะมีค่ามากสุดเพียงระดับต่ำเท่านั้น เนื่องจากแบบจำลองเน้นไปที่ผู้ให้บริการประเมินเป็นหลัก

ตารางที่ 4.24 การประเมินความมั่นคงของเว็บเซอร์วิซในฐานะผู้ใช้บริการ

WS No.	Web Service Name	Countermeasure No.						Security Score						Security Level					
		1.2	1.3	2	4	18.15	18.16	S_{SEV}	S_{LOE}	S_{CON}	S_{INT}	S_{AVA}	S_{ALL}	S_{SEV}	S_{LOE}	S_{CON}	S_{INT}	S_{AVA}	S_{ALL}
1	Paypal API	1	1	1	1	N/A	1	67	38	34	41	35	43	L	VL	L	L	L	L
2	Authorize.net Merchant Web Services	0	1	1	0	1	1	59	27	25	35	31	35.4	VL	VL	VL	VL	VL	VL
3	Send Postal Letters with PostalMethods	0	1	1	0	1	1	59	27	25	35	31	35.4	VL	VL	VL	VL	VL	VL
4	Amazon Web Services	0	1	1	0	N/A	1	53	27	25	31	27	32.6	VL	VL	VL	VL	VL	VL
5	Xignite RealTime	0	1	1	0	0	1	53	27	25	31	27	32.6	VL	VL	VL	VL	VL	VL
6	VATService	0	0	1	0	1	1	45	20	17	27	25	26.8	VL	VL	VL	VL	VL	VL
7	FlightAware FlightXML	0	0	1	1	0	1	42	23	19	26	24	26.8	VL	VL	VL	VL	VL	VL
8	TPC-App Web Service Benchmark	0	0	1	0	0	1	39	20	17	23	21	24	VL	VL	VL	VL	VL	VL
9	PTTinfo	0	0	0	1	1	1	18	3	2	13	13	9.8	VL	VL	VL	VL	VL	VL
10	StockQuote	0	0	0	1	1	1	18	3	2	13	13	9.8	VL	VL	VL	VL	VL	VL
11	MortgageIndex	0	0	0	1	1	1	18	3	2	13	13	9.8	VL	VL	VL	VL	VL	VL
12	Country Details	0	0	0	1	1	1	18	3	2	13	13	9.8	VL	VL	VL	VL	VL	VL
13	BibleWebservice	0	0	0	1	1	1	18	3	2	13	13	9.8	VL	VL	VL	VL	VL	VL
14	UK Location	0	0	0	1	1	1	18	3	2	13	13	9.8	VL	VL	VL	VL	VL	VL
15	Global Weather	0	0	0	1	1	1	18	3	2	13	13	9.8	VL	VL	VL	VL	VL	VL
16	SunSetRiseService	0	0	0	1	1	1	18	3	2	13	13	9.8	VL	VL	VL	VL	VL	VL
17	Medi Care Supplier	0	0	0	1	1	1	18	3	2	13	13	9.8	VL	VL	VL	VL	VL	VL
18	MortgageIndex	0	0	0	1	1	1	18	3	2	13	13	9.8	VL	VL	VL	VL	VL	VL
19	Barcode Generator	0	0	0	1	1	1	18	3	2	13	13	9.8	VL	VL	VL	VL	VL	VL
20	GeoIPService	0	0	0	1	1	1	18	3	2	13	13	9.8	VL	VL	VL	VL	VL	VL
21	CDYNE Profanity Filter	0	0	0	1	1	1	18	3	2	13	13	9.8	VL	VL	VL	VL	VL	VL
22	SendFax	0	0	0	1	1	1	18	3	2	13	13	9.8	VL	VL	VL	VL	VL	VL
23	USGS NWIS Daily Values	0	0	0	0	1	1	15	0	0	10	10	7	VL	N/A	N/A	VL	VL	VL
24	ignyte Movie Theater Showtimes	0	0	0	0	1	1	15	0	0	10	10	7	VL	N/A	N/A	VL	VL	VL
25	IPligence Geo IP Location	0	0	0	0	1	1	15	0	0	10	10	7	VL	N/A	N/A	VL	VL	VL
26	IP2Location Geolocation Web Service	0	0	0	1	0	1	12	3	2	9	9	7	VL	VL	VL	VL	VL	VL
27	BrowserObject Browser Detection Web Service	0	0	0	1	0	1	12	3	2	9	9	7	VL	VL	VL	VL	VL	VL
28	IP2Proxy Proxy Detection Web Service	0	0	0	1	0	1	12	3	2	9	9	7	VL	VL	VL	VL	VL	VL
29	MailBoxValidator Web Service	0	0	0	1	0	1	12	3	2	9	9	7	VL	VL	VL	VL	VL	VL
30	SoaMoa Sample Service	0	0	0	0	N/A	1	9	0	0	6	6	4.2	VL	N/A	N/A	VL	VL	VL

1 = Yes 0 = No N/A = Not Available

บทที่ 5
บทสรุป

ในบทนี้จะกล่าวถึงสรุปผลการวิจัย ปัญหาและข้อจำกัดที่พบจากการวิจัย และข้อเสนอแนะ จากการเสนอแบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซโดยอิงการจัดให้มีวิธีการรับมือการโจมตี

5.1 สรุปผลการวิจัย

งานวิจัยนี้ได้นำเสนอการสร้างแบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซโดยอิงการจัดให้มีวิธีการรับมือการโจมตี เพื่อสามารถประเมินให้เห็นถึงความสามารถในการรับมือการโจมตีของเว็บเซอร์วิซโดยผู้ให้บริการ วิธีการนำเสนอเป็นการรวมองค์ความรู้ในส่วนของรายการวิธีการรับมือการโจมตีและการโจมตีที่มีคุณสมบัติในด้านต่างๆที่ส่งผลกระทบต่อการให้บริการของเว็บเซอร์วิซ มาทำการพิจารณาหาความสัมพันธ์และทำการวัดผลอยู่ในรูปของคะแนนและระดับความมั่นคง อีกทั้งได้นำแบบจำลองนี้มาพัฒนาเป็นเครื่องมือสนับสนุนที่เห็นเป็นรูปธรรม ซึ่งช่วยให้ผู้ให้บริการหรือผู้ดูแลระบบหรือผู้ที่เกี่ยวข้องกับเว็บเซอร์วิซ สามารถนำผลการประเมินความมั่นคงและความรู้จากการใช้งานแบบจำลองไปเป็นแนวทางในการเลือกใช้วิธีการรับมือต่อการโจมตีที่เหมาะสมกับเว็บเซอร์วิซ และกระตุ้นให้หน่วยงานหรือองค์กร มีความสนใจและตระหนักถึงประเด็นความมั่นคงของเว็บเซอร์วิซมากยิ่งขึ้น รวมทั้งผู้ให้บริการอาจนำค่าความมั่นคงที่ดีไปประกาศให้ผู้ใช้บริการรับรู้เพื่อเป็นข้อมูลประกอบการพิจารณาเลือกใช้งานเว็บเซอร์วิซ หลักการของแบบจำลองนี้สามารถนำไปประยุกต์ใช้ในงานด้านความมั่นคงอื่นๆหรือขยายแบบจำลองให้รองรับการโจมตีและวิธีการรับมือแบบอื่นๆได้

จากการทดสอบพบว่าแบบจำลองและเครื่องมือสนับสนุนที่ได้ออกแบบไว้สามารถนำไปประยุกต์ใช้งานได้จริง โดยได้ทดลองกับกลุ่มตัวอย่างของผู้ให้บริการ ด้วยการทำแบบสอบถามเพื่อประเมินความมั่นคงของเว็บเซอร์วิซและประเมินแบบจำลองการวัดความมั่นคง โดยได้ผลตอบรับที่ดีจากการประเมินของผู้ให้บริการ ดังในภาคผนวก ข รวมทั้งได้ทดลองสาธิตการพิจารณาวิธีการรับมือการโจมตีเพื่อประเมินความมั่นคงของเว็บเซอร์วิซในฐานะเป็นผู้ใช้บริการ ซึ่งสามารถสรุปผลการทดลองเป็นประเด็นหลักๆได้ 3 หัวข้อ ดังนี้

5.1.1 ผลสรุปสภาพการรับมือการโจมตีของผู้ให้บริการ

1) จากจำนวนวิธีการรับมือการโจมตีทั้งหมด 69 รายการ พบว่าผู้ให้บริการส่วนใหญ่ทำ จำนวน 24 รายการ คิดเป็นร้อยละ 35 และไม่ทำ จำนวน 45 รายการ คิดเป็นร้อยละ 65 จึงสรุปได้ว่าวิธีการรับมือการโจมตีของแบบจำลองนี้มีมากกว่าวิธีการรับมือการโจมตีที่ใช้จริงในปัจจุบัน หรือกล่าวได้ว่าผู้ให้บริการส่วนใหญ่ทำวิธีการรับมือการโจมตีน้อยกว่าครึ่งหนึ่งของวิธีการรับมือทั้งหมดที่มีในแบบจำลอง

2) พบว่ารายการวิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ทำมากที่สุด ได้แก่ รายการที่ 9 (Safe Programming)

3) พบว่ารายการวิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ไม่ทำมากที่สุด มี 3 รายการ ได้แก่ รายการที่ 18.12 (The use of HMAC to hash the response from the server can also be used to thwart reflection) รายการที่ 18.13 (Introducing a random nonce with each new connection) และรายการที่ 18.21 (Using static analysis tools to find race conditions)

4) จากรายการวิธีการรับมือการโจมตีที่ผู้ให้บริการส่วนใหญ่ไม่ทำมี 2 เหตุผลหลักๆ คือ ไม่ทำเพราะระบบไม่ต้องการ และไม่ทำเพราะไม่รู้จัก พบว่า ไม่ทำเพราะระบบไม่ต้องการมากที่สุด ได้แก่ รายการที่ 18.2 (Configuring the XML processor to only retrieve external entities form trusted sources) และไม่ทำเพราะไม่รู้จักมากที่สุด ได้แก่ รายการที่ 18.13 (Introducing a random nonce with each new connection)

5) พบว่าผู้ให้บริการที่มีประสบการณ์ทั้งด้านเว็บเซอร์วิซและความมั่นคงในทุกระดับจะรู้จักและทำวิธีการรับมือการโจมตีมากกว่าผู้ที่มีประสบการณ์เฉพาะด้านเว็บเซอร์วิซเพียงอย่างเดียว โดยจะมีเฉพาะผู้ที่มีประสบการณ์ทั้งด้านเว็บเซอร์วิซและความมั่นคงที่อยู่ในระดับปานกลางและสูงจะมีปริมาณการทำวิธีการรับมือการโจมตีมากกว่าไม่ทำ ซึ่งอาจเป็นไปได้ว่าผู้มีประสบการณ์ด้านความมั่นคงสูงจะมีความสามารถในการรับรู้และทำวิธีการรับมือการโจมตีได้มากกว่าผู้ที่มีประสบการณ์ด้านความมั่นคงต่ำ

6) จากโดเมนธุรกิจของเว็บเซอร์วิซ พบว่าธุรกิจประเภทธนาคารมีความมั่นคงอยู่ในระดับสูงมากมาเป็นอันดับหนึ่ง การซื้อขายสินค้ามีความมั่นคงของเว็บเซอร์วิซอยู่ใน

ระดับสูงมาเป็นอับดับสอง และอันดับสุดท้ายคือภาครัฐมีความมั่นคงของเว็บเซอร์วิซอยู่ในระดับต่ำมาก และจากการพิจารณาตามค่ามาตรวัดความสามารถในการรับมือต่อการโจมตีของแต่ละโดเมนธุรกิจ พบว่าค่ามาตรวัดความสามารถในการรับมือต่อการโจมตีแบบที่ 12 อยู่ในระดับ 0 หมายความว่าผู้ให้บริการส่วนใหญ่ยังไม่มีการทำวิธีการรับมือที่จะบรรเทาและ/หรือป้องกันการโจมตีแบบที่ 12 ซึ่งคือ การโจมตีรีเฟลคชันในโพรโทคอลพิสูจน์ตัวจริง

7) จากรูปแบบบริการของเว็บเซอร์วิซ พบว่ารูปแบบบริการด้านธุรกิจมีความมั่นคงอยู่ในระดับสูงซึ่งสูงกว่าด้านภาครัฐที่มีค่าความมั่นคงอยู่ในระดับปานกลาง

8) จากขนาดของหน่วยงาน พบว่าหน่วยงานขนาดใหญ่มีความมั่นคงอยู่ในระดับสูงซึ่งสูงกว่าหน่วยงานขนาดกลางและเล็กที่มีค่าความมั่นคงอยู่ในระดับปานกลาง

9) จากลักษณะการใช้งานเว็บเซอร์วิซ พบว่าลักษณะการใช้งานแบบภายในองค์กรและสาธารณะมีความมั่นคงอยู่ในระดับสูงซึ่งสูงกว่าแบบภายในองค์กรที่อยู่ในระดับปานกลางและแบบสาธารณะที่อยู่ในระดับต่ำ

10) จากความสำคัญของเว็บเซอร์วิซ พบว่าเว็บเซอร์วิซที่มีความสำคัญสูงมีค่าคะแนนความมั่นคงสูงกว่าเว็บเซอร์วิซที่มีความสำคัญต่ำและปานกลาง แต่ถ้าพิจารณาตามระดับความมั่นคงจะพบว่าความสำคัญของเว็บเซอร์วิซทั้ง 3 ระดับจะมีระดับความมั่นคงปานกลาง

11) จากปริมาณการใช้งานเว็บเซอร์วิซ พบว่าเว็บเซอร์วิซที่มีปริมาณการใช้งานสูงมีค่าคะแนนความมั่นคงสูงกว่าเว็บเซอร์วิซที่มีปริมาณการใช้งานต่ำและปานกลาง แต่ถ้าพิจารณาตามระดับความมั่นคง พบว่าเว็บเซอร์วิซที่มีปริมาณการใช้งานสูงและต่ำจะมีความมั่นคงอยู่ในระดับปานกลางซึ่งสูงกว่าเว็บเซอร์วิซที่มีปริมาณการใช้งานปานกลางที่มีความมั่นคงอยู่ในระดับต่ำ

5.1.2 ผลสรุปการประเมินแบบจำลองการวัดความมั่นคง

1) ความสนใจด้านความมั่นคงของผู้ให้บริการ พบว่า ผู้ให้บริการส่วนใหญ่ให้ความสนใจด้านความมั่นคงในระดับสูง คิดเป็น 59%

2) ความเข้าใจในการกรอกข้อมูลของผู้ให้บริการ พบว่า ผู้ให้บริการส่วนใหญ่ที่มีความเข้าใจในการกรอกข้อมูลในระดับปานกลาง คิดเป็น 61% โดยให้เหตุผลว่า ผู้กรอกข้อมูลมีความรู้เกี่ยวกับเว็บเซอร์วิซในด้านความมั่นคงเพียงบางส่วน เพราะแบบสอบถามนี้จำเป็นต้องมีความรู้พื้นฐานด้านความมั่นคงที่สูงจึงจะทราบได้ ซึ่งในความเป็นจริงแล้วอาจไม่สามารถทราบและเข้าถึงกลไกการทำงานและความมั่นคงของโครงสร้างพื้นฐานในองค์กรได้อย่างครอบคลุมและละเอียดในทุกหน่วยงาน

3) การประเมินความน่าเชื่อถือของแผ่นแบบการจัดให้มีวิธีการรับมือ พบว่า ผู้ให้บริการส่วนใหญ่ประเมินความน่าเชื่อถือของแผ่นแบบการจัดให้มีวิธีการรับมือในระดับสูง คิดเป็น 69% โดยให้เหตุผลว่า เนื้อหามีความสมเหตุสมผลค่อนข้างครอบคลุมทั้งวิธีการรับมือและรูปแบบการโจมตีมีมากพอต่อการวิเคราะห์สภาพความมั่นคงโดยรวม อีกทั้งทำให้เห็นถึงความสัมพันธ์ระหว่างการโจมตีและวิธีการรับมือได้อย่างชัดเจน

4) การประเมินความสมเหตุสมผลของแบบจำลองงานวิจัย พบว่า ผู้ให้บริการส่วนใหญ่ประเมินความสมเหตุสมผลของแบบจำลองงานวิจัยในระดับสูง คิดเป็น 59% โดยให้เหตุผลว่า เนื้อหาค่อนข้างครอบคลุม สมเหตุสมผลและมีความน่าเชื่อถือเนื่องจากมีการนำวิธีการรับมือและการโจมตีที่มีคุณสมบัติของการโจมตีซึ่งเป็นที่ยอมรับกันมาใช้อ้างอิงในการคำนวณ ทำให้ผลลัพธ์ที่ได้ค่อนข้างหลากหลายและค่าผลลัพธ์ที่ได้มีความเหมาะสมกับองค์กรที่เป็นอยู่

5) ประโยชน์ที่ได้จากงานวิจัยประเมินโดยผู้ให้บริการ พบว่า ผู้ให้บริการส่วนใหญ่ประเมินประโยชน์ที่ได้จากงานวิจัยในระดับที่สูง คิดเป็น 74% โดยให้เหตุผลว่าสามารถนำไปใช้ตรวจสอบและประเมินความมั่นคงให้กับเว็บเซอร์วิซในองค์กรต่างๆได้ และช่วยพัฒนาระดับความรู้ทางด้านความมั่นคงให้กับผู้ประเมินและนำแบบจำลองนี้ไปประยุกต์ใช้เพื่อเป็นแนวทางในการออกแบบเว็บเซอร์วิซและระบบที่ต้องการความมั่นคงสูงให้เข้ากับองค์กรได้

5.1.3 ผลสรุปการประเมินความมั่นคงของเว็บเซอร์วิซในฐานะผู้ใช้บริการ

1) การประเมินความมั่นคงของเว็บเซอร์วิซในฐานะผู้ใช้บริการ สามารถตรวจสอบรายการวิธีการรับมือได้ค่อนข้างจำกัด เนื่องจากข้อมูลด้านความมั่นคงส่วนใหญ่ของ

การให้บริการจะไม่ค่อยมีการเปิดเผยสู่สาธารณะ เนื่องจากเป็นข้อมูลที่มีความละเอียดอ่อน ซึ่งผู้ใช้บริการจะรู้ได้เพียงเบื้องต้นเท่านั้น

5.2 ปัญหาและข้อจำกัดที่พบจากการวิจัย

สามารถแบ่งเป็นประเด็นหลักๆ ได้ 2 หัวข้อ ดังนี้

5.2.1 แบบจำลองงานวิจัย

1) จากข้อมูลคุณสมบัติของการโจมตีซึ่งกำหนดโดยผู้เชี่ยวชาญใน [3] พบว่ามี 11 การโจมตีที่มีเฉพาะค่าความรุนแรงเท่านั้น แต่คุณสมบัติด้านที่เหลือไม่ได้ระบุไว้ ซึ่งเมื่อนำไปคำนวณอาจทำให้ผลลัพธ์ที่ได้ดูไม่เสมอภาคกัน ดังนั้นผู้วิจัยจึงได้ทำการกำหนดค่าคุณสมบัติบางส่วนที่เดิมไม่ถูกกำหนดไว้ให้มีค่าอยู่ในระดับปานกลาง โดยมีการพิจารณาตามหลักเกณฑ์ที่ผู้วิจัยได้กำหนดขึ้น ซึ่งในส่วนนี้อาจจะเป็นจุดอ่อนในการคำนวณได้เพราะค่าคุณสมบัติของบางการโจมตีมีไม่เท่ากัน อาจทำให้การคำนวณค่าความมั่นคงในแต่ละด้านคุณสมบัติมีความเที่ยงตรงไม่เท่ากัน

2) ผู้ที่สามารถใช้งานแบบจำลองนี้ได้แบบสมบูรณ์จะต้องเป็นผู้ที่มีความรู้ความเข้าใจด้านความมั่นคงเป็นอย่างดีเพราะข้อมูลนำเข้าซึ่งคือรายการวิธีการรับมือต่างๆ ผู้ใช้งานอาจไม่รู้จักหรือไม่ทราบได้ว่าวิธีการรับมือนั้นมีอยู่ในเครื่องมือที่ใช้สร้างเว็บเซอร์วิซแล้วหรือเครื่องมือได้ทำให้แล้วจึงทำให้การตอบอาจมีความคลาดเคลื่อนได้

3) จำนวนวิธีการรับมือและการโจมตีที่มีในแบบจำลองนี้ไม่สามารถจะครอบคลุมทุกประเภทที่เกี่ยวข้องกับเว็บเซอร์วิซได้ทั้งหมด เนื่องจากว่าผู้วิจัยได้สืบค้นข้อมูลเท่าที่จะสามารถนำมาใช้งานได้เท่านั้น

5.2.2 ผลการทดลองที่ได้จากการตอบแบบสอบถาม

1) ความรู้ด้านเว็บเซอร์วิซและความมั่นคงของผู้ตอบแบบสอบถามในกลุ่มตัวอย่างการทดลองไม่เท่ากัน อาจทำให้ผลการทดลองที่ได้มีความคลาดเคลื่อนจากความจริงก็เป็นได้ แต่ก็ถือว่าเป็นกรณีศึกษาในมุมกว้างของวงการเว็บเซอร์วิซในประเทศไทย

2) จำนวนของผู้ตอบแบบสอบถามในแต่ละกลุ่มการทดลองเมื่อมีการแบ่งตามด้านต่างๆ แล้วมีจำนวนไม่เท่ากัน เช่น ธนาคารมีผู้ตอบแบบสอบถาม 7 คน การปกครองมีผู้ตอบแบบสอบถาม 1 คน แต่เมื่อนำมาพิจารณาภาพรวมวิธีการรับมือที่ทำแล้วนำมาคำนวณตามแบบจำลอง ค่าความมั่นคงที่ได้อาจจะไม่เที่ยงตรงตามสภาพ

ความจริงก็เป็นได้ เพราะกลุ่มตัวอย่างที่ได้นี้ค่อนข้างจำกัดในการหาผู้ที่จะมาตอบแบบสอบถามให้มีจำนวนแต่ละด้านเท่ากัน

3) ในการพิจารณาว่าแต่ละกลุ่มตัวอย่างนั้น กลุ่มใดทำวิธีการรับมือใดบ้างจะพิจารณาจากค่าร้อยละของผู้ให้บริการที่เลือกทำ โดยถ้ามีค่ามากกว่าหรือเท่ากับร้อยละ 50 จะพิจารณาให้รายการนั้นทำ เช่น ธนาคารมีผู้ตอบแบบสอบถามว่าทำรายการที่ 1.1 จำนวน 4 คนจากทั้งหมด 7 คน คิดเป็นร้อยละ 57 จะแสดว่ากลุ่มตัวอย่างของธนาคารส่วนใหญ่เลือกทำ ซึ่งการพิจารณาจากลักษณะนี้เป็นผลมาจากเรื่องของจำนวนแต่ละกลุ่มตัวอย่างไม่เท่ากัน หากสามารถนำหลักการทางสถิติที่เหมาะสมเข้ามาช่วยพิจารณาในส่วนนี้ก็จะทำให้ลดความคลาดเคลื่อนของผลการทดลองและช่วยให้ผลการทดลองมีมาตรฐานมากยิ่งขึ้น

5.3 ข้อเสนอแนะ

งานวิจัยนี้สามารถพัฒนาเพิ่มเติมในหลายด้าน ดังนี้

1) ขยายแบบจำลองให้รองรับการโจมตีและวิธีการรับมืออื่นๆมากขึ้น

2) พัฒนาหลักเกณฑ์การกำหนดค่าคุณสมบัติการโจมตีที่ยังไม่มีการระบุไว้ให้มีมาตรฐานและครอบคลุมการโจมตีที่หลากหลาย

3) ในส่วนของเครื่องมือสนับสนุนแบบจำลองหน้าผู้กรอก สามารถนำมาจัดหมวดหมู่ของวิธีการรับมือตามมุมมองของระบบให้มีความสัมพันธ์กันมากขึ้น และส่วนการแสดงผลสามารถนำมาพิจารณาผลลัพธ์ค่าความมั่นคงโดยแบ่งตามประเภทและตำแหน่งที่เกิดการโจมตีได้

4) ควรมีการศึกษาเพิ่มเติมเกี่ยวกับลักษณะเฉพาะของความหลากหลายของเว็บเซอร์วิซในรูปแบบต่างๆที่แบ่งกลุ่มตามผลการทดลองมาเป็นข้อกำหนดหรือค่าน้ำหนักเฉพาะตัวของกลุ่มนั้นๆ ก็จะสามารถทำให้การวัดความมั่นคงสำหรับเว็บเซอร์วิซมีความเที่ยงตรงมากขึ้นได้

5) สามารถนำมาต่อยอดเป็นหลักเกณฑ์การพัฒนาความมั่นคงให้กับเว็บเซอร์วิซในเชิงปฏิบัติการได้

รายการอ้างอิง

[1] Papazoglou, M. P., Web Services: Principles and Technology. U.S.A.: Pearson - Prentice Hall, 2007.

[2] NIST Special Publication 800-95. Guide to Secure Web Services. 2007.

[3] The Mitre Corporation. CAPEC - Common Attack Pattern Enumeration and Classification [Online]. Available from: http://capec.mitre.org/ [2010, November].

[4] Guerri, J. T. Vulnerability Analysis Taxonomy: Achieving completeness in a systematic way. Proceedings of the 10th International Common Criteria Conference (ICCC 2009), Tromso, Norway, September 22-24, 2009.

[5] Belapurkar, A., Chakrabarti, A., Ponnapalli, H., Varadarajan, N., Padmanabhuni, S., and Sundarrajan, S., Distributed Systems Security: Issues, Processess and Solutions. United Kingdom John Wiley & Sons, 2009.

[6] Jensen, M., Gruschka, N., and Herkenhoner, R. A survey of attacks on web services: Classification and countermeasures. In Computer Science - Research and Development (CSRD) 24 (2009): 185-197.

[7] Sawma, V. D. and Probert, R. L. E-Commerce Authentication: An Effective Countermeasures Design Model. Proceedings of the International Conference on Enterprise Information Systems (ICEIS 2003), pp. 447-455. Angers, France, April 22-26, 2003.

[8] Patterson, D. XML Firewall Architecture and Best Practices for Configuration and Auditing. Place: SANS, 2007.

[9] Banklongsi, T. and Senivongse, T. A Security Measurement Model for Web Services Based on Provision of Attack Countermeasures. Proceedings of the 15th International Annual Symposium on Computational Science and Engineering (ANSCSE 2011), pp. 593-598. Pathumthani, Thailand, March 30 – April 2, 2011.

[10] W3C. Extensible Markup Language (XML) 1.0 (Fifth Edition) [Online]. 2008. Available from: http://www.w3.org/TR/2008/REC-xml-20081126/ [2010, November].

[11] W3C. Web Services Description Language (WSDL) Version 2.0 Part 0: Primer [Online]. 2007. Available from: http://www.w3.org/TR/2007/REC-wsdl20-primer-20070626/#WSDL-PART1 [2010, November].

[12] W3C. SOAP Version 1.2 Part 1: Messaging Framework (Second Edition) [Online]. 2007. Available from: http://www.w3.org/TR/2007/REC-soap12-part1-20070427/ [2010, November].

[13] OASIS. UDDI Version 3.0.2 [Online]. 2005. Available from: http://www.oasis-open.org/committees/uddi-spec/doc/spec/v3/uddi-v3.0.2-20041019.htm [2010, November].

[14] Donsez, D. Panorama sur les Web Services [Online]. Available from: http://membres-liglab.imag.fr/donsez/cours/webservices.pdf [2010, December].

[15] Bertino, E., Martino, L., Paci, F., and Squicciarini, A., Security for Web Services and Service-Oriented Architectures: Springer-Verlag Berlin Heidelberg, 2010.

[16] Mani, A. and Nagarajan, A. Understanding quality of service for Web services [Online]. Available from: http://www.ibm.com/developerworks/library/ws-quality.html [2010, December].

[17] OASIS. Web Services Security: SOAP Message Security 1.1 (WS-Security 2004) [Online]. 2006. Available from: http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf [2010, December].

[18] Sotomayor B. The Globus Toolkit 4 Programmer's Tutorial [Online]. 2005. Available from: http://gdp.globus.org/gt4-tutorial/multiplehtml/ch10s02.html [2010, December].

[19] Tobarra, L., Cazorla, D., Cuartero, F., and Diaz, G., Application of Formal Methods to the Analysis of Web Services Security, in Formal Techniques for Computer Systems and Business processes (EPEW 2005 and WS-FM 2005), LNCS 3670. pp. 215-229: Springer, 2005.

[20] Artaiam, N. and Senivongse, T. Enhancing Service-Side QoS Monitoring for Web Services. Proceedings of the Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/ Distributed Computing (SNPD 2008), pp. 765-770. Phuket, Thailand, August 6-8, 2008.

[21] Nitan, K. and Teng-amnuay, Y. Vulnerability Assessment of Web Services Products Based on Severity of Damage. Proceedings of National Computer Science and Engineering Conference (NCSEC 2007), pp. 339-346. 19-21 November, 2007.

[22] Pang, J. and Peng, X. Trustworthy Web Service Security Risk Assessment Research. Proceedings of International Forum on Intermation Technology and Applications (IFITA 2009), pp. 417-420. Chengdu, China, May 15-17, 2009.

[23] Jiang, L., Chen, H., and Deng, F. A Security Evaluation Method Based on STRIDE Model for Web Service. Proceedings of The 2nd International Workshop on Intelligent Systems and Applications (ISA 2010), pp. 807-811. 2010.

[24] Charpentier, F. Common Criteria Web Application Security Scoring CCWAPSS [Online],White Paper. Available from: http://www.xmcoparthers.com/whitepapers/ccwapss_1.1.pdf [2010, November].

[25] Vitharana, P., Jain, H., and Zahedi, F. M. Strategy-based Design of Reusable Business Components. IEEE Transactions on Systems, Man, and Cybernetics 34 (November 2004): 460-474.

[26] Microsoft. Excel Mashup [Online]. Available from: http://www.excelmashup.com/ [2012, January].

[27] Transaction Processing Performance Council (TPC). TPC Benchmark App (Application Server) specification, version 1.3 [Online]. 2008. Available from: http://www.tpc.org/tpc_app/default.asp [2011, January].

[28] OASIS. WS-SecurityPolicy 1.2 [Online]. 2007. Available from: http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.html [2012, February].

[29] SoaMoa. SoaMoa Sample Services [Online]. Available from: http://soamoa.org:9292/artistRegistry?WSDL [2011, September].

[30] Sourceforge.NET. How to write a DTD schema [Online]. Available from: http://xmlfy.sourceforge.net/howtowriteadtd.html [2012, February].

[31] Petroleum Authority of Thailand (PTT). PTTInfo Web Service [Online]. Available from: http://www.pttplc.com/pttinfo.asmx [2011, September].

[32] WaterOneFlow WebServices. USGS NWIS Daily Values [Online]. Available from: http://river.sdsc.edu/wateroneflow/NWIS/DailyValues.asmx?WSDL [2011, September].

[33] SmartBear Software. soapUI [Online]. Available from: http://www.soapui.org/ [2011, August].

[34] UDDI Services. VATService1 Web Service [Online]. Available from: https://rdws.rd.go.th/ServiceRD/VATService.asmx [2011, September].

[35] PayPal. Paypal API [Online]. Available from: https://www.sandbox.paypal.com/wsdl/PayPalSvc.wsdl [2012, February].

[36] Generic Objects Technologies Ltd. WebserviceX.NET [Online]. Available from: http://www.webservicex.net/ [2012, February].

[37] Xmethods.net. XMethods [Online]. Available from: http://www.xmethods.net [2012, February].

[38] WSDLL. WSDL Listings - Publicly Available Commercial Web Services [Online]. Available from: http://www.wsdll.com/ [2012, February].

[39] Microsoft UDDI Services. UDDI Services [Online]. Available from: https://rdws.rd.go.th/uddipublic/default.aspx [2012, February].

ภาคผนวก

ภาคผนวก ก

คำอธิบายการโจมตีเว็บเซอร์วิซ

1) การโจมตีแบบลาดตระเวน

วัตถุประสงค์ของการโจมตีแบบลาดตระเวน (Reconnaissance Attacks) คือการเก็บรวบรวมข้อมูลต่างๆที่เกี่ยวกับแอปพลิเคชันและสภาพแวดล้อมการทำงาน แล้วนำข้อมูลดังกล่าวมาหาข้อบกพร่องเพื่อทำการโจมตีในภายหลัง การโจมตีประเภทนี้ ได้แก่

- **การกราดตรวจวิสเดิล** (WSDL Scanning) เป้าหมายของการโจมตีนี้อยู่ที่วิสเดิลที่มีใช้งานอยู่ ผู้โจมตีอาจทำการกราดตรวจวิสเดิลเพื่อเปิดเผยข้อมูลที่มีความละเอียดอ่อนเกี่ยวกับรูปแบบการร้องขอบริการ เทคโนโลยีที่ใช้และจุดอ่อนที่เกี่ยวข้อง เช่น ผู้โจมตีอาจจะพยายามเดาเมท็อดลับที่ไม่ได้เปิดเผยให้คนทั่วไปใช้งานจากข้อมูลที่มีในวิสเดิล

- **วิสเดิลฟิชชิง** (WSDL Phishing) การโจมตีโดยการหลอกลวงจากตัววิสเดิลที่มียูอาร์แอลปลอมเพื่อขอข้อมูลที่สำคัญ โดยวิสเดิลปลอมนั้นจะมีการดำเนินการ (Operations) และการผูกติด (Binding) เหมือนกับวิสเดิลต้นฉบับ ซึ่งโดยทั่วไปการดำเนินการแรกที่ผู้ใช้บริการจะต้องปฏิบัติคือการลงบันทึกเข้าและเมื่อผู้ใช้บริการใส่ข้อมูลโดยไม่ได้ตั้งใจเข้าไปข้อมูลเหล่านั้นก็จะไปอยู่ที่ผู้โจมตี

- **การตรวจหาเว็บเซอร์วิซที่ไม่ถูกเผยแพร่สู่สาธารณะ** (Detect Unpublicized Web Services) ผู้โจมตีทำการค้นหาเว็บไซต์เป้าหมายเพื่อตรวจหาเว็บเซอร์วิซที่ยังไม่ถูกเผยแพร่ โดยทั่วไปจะเกี่ยวข้องกับการจัดแผนผังเว็บไซต์ (Mapping) ที่มีการประกาศไว้ การค้นหาทำโดยสไปเดอริง (Spidering) ผ่านการเชื่อมต่อที่มีการเปิดเผย และจะมีการพยายามเข้าถึงบริการแก้จุดบกพร่องหรือลงบันทึก (Debugging or Logging Services) ที่รู้จักกันทั่วไป หรือบริการที่สามารถทำนายได้ (Predictable Service) ภายในแผนผังเว็บไซต์ นอกจากนี้ผู้โจมตีอาจทำการร้องขอซ้ำไปยังเว็บเซอร์วิซด้วยรูปแบบยูอาร์แอลของส่วนประกอบเว็บแอปพลิเคชันทั่วไป เช่น โปรแกรม Common Gateway Interface (CGI) โดยมีการพิจารณาข้อความแสดงข้อผิดพลาดที่ได้รับ เทคนิคนี้สามารถนำไปใช้เพื่อรวบรวมข้อมูลของเว็บเซอร์วิซที่ไม่ถูกเผยแพร่สู่สาธารณะ

2) การโจมตีแบบเพิ่มสิทธิ์

วัตถุประสงค์ของการโจมตีแบบเพิ่มสิทธิ์ (Privilege Escalation Attacks) คือการเปิดให้ผู้โจมตีทำการโยกย้ายถ่ายเทข้อมูลในระบบเครือข่ายที่ตนเองไม่มีสิทธิ์กระทำหรือพยายามแก้ไขสิทธิ์ของตัวเองให้สูงขึ้นกว่าเดิม โดยได้รับประโยชน์จากข้อผิดพลาดหรือข้อบกพร่องจากการเขียนโปรแกรม การออกแบบที่มีข้อผิดพลาดทำให้ผู้โจมตีสามารถยกระดับการเข้าถึงเครือข่ายและ

ข้อมูล โดยสามารถเข้าควบคุมกระบวนการต่างๆได้โดยผ่านทางเลี่ยงระบบควบคุมความมั่นคงซึ่งได้มีการจำกัดการเข้าถึงของผู้โจมตีที่จะเข้าใช้ฟังก์ชัน ข้อมูล ทรัพยากรและสภาพแวดล้อมของเว็บเซอร์วิซ การโจมตีประเภทนี้ ได้แก่

- **การโจมตีรหัสผ่านตามดิกชันนารี** (Dictionary-Based Password Attack) การโจมตีนี้ผู้โจมตีจะทำการเดาคำศัพท์ที่มีในดิกชันนารีเพื่อให้ได้รหัสผ่าน ซึ่งอาจจะทำด้วยมือหรือใช้โปรแกรมอัตโนมัติก็ได้

- **บัฟเฟอร์ล้น** (Overflow Buffers) การโจมตีนี้มีเป้าหมายที่เว็บเซอร์วิซที่พัฒนาด้วยภาษาซี หรือ ซีพลัส พลัส ซึ่งมีการยอมรับข้อมูลที่เป็นค่านำเข้าและเก็บไว้ในหน่วยความจำ เมื่อเว็บเซอร์วิซล้มเหลวในการตรวจสอบขนาดของข้อมูลนำเข้าที่ใหญ่กว่าขนาดของหน่วยความจำบัฟเฟอร์ที่จองไว้ จะเกิดบัฟเฟอร์ล้น และหากข้อมูลนำเข้าขนาดใหญ่นั้นประกอบด้วยการฝังคำสั่งที่เป็นอันตรายหรือโค้ดที่มุ่งร้าย บัฟเฟอร์ล้นอาจส่งผลให้มีการโหลดคำสั่งนั้นมาประมวลผล หรือสามารถเพิ่มสิทธิ์การเข้าใช้งานได้

- **การใช้เงื่อนไขการแข่งขัน** (Leveraging Race Conditions) เงื่อนไขการแข่งขันคือสถานการณ์ที่มีโปรเซสหลายโปรเซสใช้งานข้อมูลและจัดการข้อมูลร่วมกันโดยที่โปรเซสทั้งหมดทำงานพร้อมกัน จะทำให้ผลลัพธ์ที่ได้จากการประมวลผลโปรเซสเหล่านี้มีค่าสุดท้ายที่ไม่อาจคาดเดาได้ ซึ่งขึ้นอยู่กับลำดับการประมวลผลของโปรเซสเหล่านี้ เงื่อนไขการแข่งขันสามารถถูกเรียกโดยเจตนาจากผู้โจมตีที่ใช้เว็บเซอร์วิซในทางที่ทำให้เกิดกรณีที่หลายโปรเซสพยายามที่จะเข้าใช้ไฟล์เดียวกัน

- **การโจมตีซิมลิงค์** (Symlink Attacks) ซิมโบลิคลิงค์ (ซิมลิงค์) เป็นไฟล์ชนิดพิเศษบนระบบยูนิกซ์และ ลินุกซ์ซึ่งทำการลิงค์หรืออ้างอิงไปยังไฟล์อื่น จุดอ่อนซิมลิงค์ถูกใช้ประโยชน์โดยการสร้างซิมโบลิคลิงค์จากไฟล์ที่ผู้โจมตีสามารถเข้าถึงได้ไปยังไฟล์ที่ผู้โจมตีเข้าถึงไม่ได้ วัตถุประสงค์ของการโจมตีคือเพื่อหลอกโปรแกรมเว็บเซอร์วิซซึ่งมีสิทธิ์เข้าถึงไฟล์หนึ่งๆ ให้ทำหน้าที่เหมือนเป็นพร็อกซีของผู้โจมตีในการแก้ไขหรือลบไฟล์แทนผู้โจมตี โดยที่โปรแกรมนั้นจริงๆ แล้วไม่ได้ต้องการแก้ไขหรือลบไฟล์ดังกล่าว การโจมตีซิมลิงค์มักเกิดควบคู่กับการโจมตีที่มีการใช้เงื่อนไขการแข่งขัน

- **เซสชันฟิกเซชัน** (Session Fixation) โดยเทคนิคการออกแบบที่ได้รับการยอมรับกันทั่วไป เมื่อมีการส่งข้อมูลขนาดใหญ่ผ่านเว็บเซอร์วิซจะทำการส่งลิงค์สำหรับให้เข้าถึงข้อมูลแทน

การส่งตัวข้อมูลเอง ในสถานการณ์ดังกล่าวเป็นไปได้ที่ผู้โจมตีจะส่งลิงค์เชื่อมต่อไปยังผู้ใช้ที่มีรหัสเซสชัน (Session ID) ที่ผู้โจมตีทราบ โดยผู้โจมตีจะทำการปลอมตัวเป็นผู้ใช้เมื่อมีการเข้าสู่ระบบ ผู้โจมตีก็จะสามารถก่อให้เกิดความเสียหายได้

- **การโจมตีแบบคนกลาง (Man in the Middle Attack)** เป็นการโจมตีที่ผู้โจมตีเข้ามาแทรกระหว่างการสื่อสารของผู้ใช้บริการและผู้ให้บริการ โดยในการโจมตีนี้ผู้โจมตีสามารถดักจับหรือแก้ไขข้อมูลของผู้ใช้บริการและผู้ให้บริการได้

- **การโจมตีรีเฟลคชันในโพรโทคอลพิสูจน์ตัวจริง (Reflection Attack in Authentication Protocol)** การโจมตีนี้เกี่ยวข้องกับโพรโทคอลพิสูจน์ตัวจริงที่ใช้กลไก Challenge-Handshake โดยผู้โจมตีสามารถปลอมตัวเป็นผู้ใช้ที่มีสิทธิ์ใช้งานระบบในขณะทำการพิสูจน์ตัวจริงจึงทำให้สามารถเข้าถึงระบบได้

- **การใช้ประโยชน์ของตัวแปรเซสชัน รหัสทรัพยากร และข้อมูลรับรองตัวจริงที่เชื่อถือได้อื่น ๆ (Exploitation of Session Variables, Resource IDs and Other Trusted Credentials)** เป็นการโจมตีบนรหัสเซสชัน (Session IDs) และรหัสทรัพยากร (Resource IDs) โดยใช้ประโยชน์จากความเป็นจริงที่บางซอฟต์แวร์ยอมรับอินพุตผู้ใช้โดยปราศจากการตรวจสอบการพิสูจน์ตัวจริง ตัวอย่างเช่น ระบบการเข้าคิวข้อความ (Message Queuing System) ที่อนุญาตให้ผู้ใช้บริการมีการโพสต์ข้อความลงในคิวผ่านช่องทางเปิด เช่น เอฟทีพีแบบนิรนาม (Anonymous FTP) ที่ไม่ได้มีการระบุตัวตนกับเครื่องแม่ข่าย ในการเข้าใช้งานผ่านกลุ่มการตรวจสอบหรือสมาชิกที่มีบทบาทในการโพสต์ข้อความ อย่างไรก็ตามไม่มีการพิสูจน์ว่ากระบวนการเขียนข้อความลงคิวมีความถูกต้องและได้รับการอนุญาตจากผู้ที่มีสิทธิ์จริง หรือเซิร์ฟเวอร์ที่มีการเดาหรือปลอมแปลงรูปแบบในการระบุตัวตนดิจิทัล (Digital Identity) ได้ง่ายก็สามารถทำให้เกิดช่องโหว่ในการโจมตีได้ การโจมตีที่เป็นการหลอกลวง (Spoofing) และปลอมตัว (Impersonation) นี้มีความเป็นไปได้ที่จะทำให้การพิสูจน์ตัวจริง การอนุญาตเข้าใช้ และการควบคุมการตรวจสอบบนระบบ ไม่เป็นผล

- **การโจมตีรหัสผ่านแบบบรูทฟอร์ซ (Password Brute Forcing)** เป็นการโจมตีที่ผู้โจมตีพยายามค้นหาคีย์ที่ถูกต้องโดยใช้ค่าที่มีความเป็นไปได้ทั้งหมดเพื่อใช้ในการถอดรหัสผ่าน

- **การลองใช้ชื่อผู้ใช้และรหัสผ่านที่เป็นคำสามัญ (ค่าโดยปริยาย) (Try Common (Default) Usernames and Passwords)** ผู้โจมตีอาจพยายามใช้ชื่อผู้ใช้และรหัสผ่าน

ที่มาจากค่าโดยปริยาย เพื่อเข้าสู่ระบบและกระทำการ โดยที่ไม่ได้รับอนุญาต ผู้โจมตีอาจจะพยายามทำบรูทฟอร์ซที่ชาญฉลาด (Intelligent Brute Force) โดยการใช้ข้อมูลรับรองตัวจริงที่มากับทางผู้ขายและเป็นที่รู้กันโดยทั่วไป เช่นเดียวกับการใช้ดิกชันนารีของชื่อผู้ใช้และรหัสผ่านที่เป็นคำสามัญ

- **การใช้เอพีไอเว็บเซอร์วิซที่ไม่ถูกเผยแพร่** (Using Unpublished Web Service APIs) การโจมตีนี้ ผู้โจมตีจะทำการค้นหาและเรียกใช้เอพีไอเว็บเซอร์วิซซึ่งผู้ออกแบบไม่ได้ตั้งใจที่จะให้บริการแบบสาธารณะ โดยถ้าเอพีไอเหล่านี้ล้มเหลวในการตรวจสอบการพิสูจน์คำร้องขอ ผู้โจมตีอาจจะสามารถเรียกใช้บริการและ/หรือได้รับสิทธิ์ที่ไม่ควรได้รับ

3) การโจมตีการรักษาความลับ

วัตถุประสงค์ของการโจมตีการรักษาความลับ (Attacks on Confidentiality) คือการเปิดเผยข้อมูลจาก โปรแกรมประยุกต์ที่เป็นเป้าหมายซึ่งผู้โจมตีไม่ได้รับอนุญาตให้มองเห็น การโจมตีประเภทนี้ ได้แก่

- **การดักจับข้อมูล** (Sniffing) เป็นวิธีการแอบดักจับข้อมูลโดยทำการเฝ้าดูการแลกเปลี่ยนข้อมูลระหว่างผู้ส่งและผู้รับ ซึ่งในกรณีของเว็บเซอร์วิซผู้โจมตีสามารถใช้การโจมตีนี้ในการดักจับข้อมูลที่สำคัญซึ่งไม่ได้มีการเข้ารหัสไว้ เช่น ข้อมูลรหัสผ่านและข้อมูลการกำหนดค่าความมั่นคงที่จะถูกส่งในโซป ยูดีดีไอ วิสเดิลและข้อความอื่นๆ

4) การโจมตีบูรณภาพ

วัตถุประสงค์ของการโจมตีบูรณภาพ (Attacks on Integrity) คือการแก้ไขข้อมูลจากแอปพลิเคชันที่เป็นเป้าหมายซึ่งผู้โจมตีไม่ได้รับอนุญาตให้เข้าถึงเพื่อทำการเปลี่ยนแปลงข้อมูล การโจมตีประเภทนี้ ได้แก่

- **การแทรกแซงโซปพารามิเตอร์** (SOAP Parameter Tampering) การโจมตีนี้ผู้โจมตีจะส่งข้อความโซปที่มีค่าขอบเขตอื่นนอกเหนือจากที่ระบุไว้ในเซิร์ฟเวอร์ โดยในข้อความโซปมีพารามิเตอร์ที่อยู่ในรูปแบบค่าภายในส่วนย่อยเอกซ์เอ็มแอล (XML Elements) เซิร์ฟเวอร์จะมีเอกซ์เอ็มแอลสคีมา(XML Schema) ที่ระบุข้อจำกัดบางอย่างเกี่ยวกับค่าพารามิเตอร์เหล่านี้ไว้ ตัวอย่างเช่น เซิร์ฟเวอร์อาจคาดหวังว่าค่าพารามิเตอร์ชนิดสตริงควรมีจำนวนน้อยกว่า 10 ตัวอักษรหรือตัวเลขน้อยกว่า 100 ตัว ในการโจมตีนี้ผู้โจมตีจะทำการละเมิดสคีมานี้หรือใช้ประโยชน์จากความยืดหยุ่นของสคีมา (เช่น ขาดการจำกัดจำนวนตัวอักขระ) เพื่อใส่ค่าพารามิเตอร์ที่เซิร์ฟเวอร์

ไม่ได้คาดหวังไว้ ผลลัพธ์ของการโจมตีนี้สามารถทำให้เกิดการเปิดเผยข้อมูล การปฏิเสธการบริการ หรือ การทำงานที่ผิดพลาด

- **การวางยาเอกซ์เอ็มแอลสคีมา** (XML Schema Poisoning) การโจมตีนี้ผู้โจมตีพยายามเข้าถึงสคีมาที่ถูกเก็บไว้เพื่อทำการแก้ไขแล้วส่งผลทำให้เอกสารเอกซ์เอ็มแอลที่ถูกต้องถูกปฏิเสธหรือเป็นโมฆะหรือกลายเป็นเอกสารเอกซ์เอ็มแอลที่มุ่งร้ายต่อเว็บเซอร์วิซ

- **ปรินซิปอลสปูฟิง** (Principal Spoofing) การโจมตีนี้ผู้โจมตีจะส่งข้อความปลอมที่แอบอ้างว่าเป็นข้อความที่ส่งมาจากผู้ร้องขอจริง

- **การจัดเส้นทางอ้อมเอกซ์เอ็มแอล** (XML Routing Detour) การโจมตีนี้ผู้โจมตีจะทำการปลอมแปลงเส้นทางการส่งข้อมูลไปยังจุดหมายปลายทางที่ผู้โจมตีกำหนด

- **การโจมตีจากเอนทิตีภายนอก** (External Entity Attack) ผู้ใช้บริการสามารถสร้างเอกสารเอกซ์เอ็มแอลแบบไดนามิกสำหรับส่งให้เว็บเซอร์วิซ โดยเอกสารเอกซ์เอ็มแอลแบบไดนามิคนี้จะระบุยูอาร์ไอของแหล่งข้อมูลที่ต้องการดึงมาใช้ ณ เวลาที่สร้างเอกสาร หากผู้ใช้บริการไม่ได้ทำการพิสูจน์ตัวจริงของแหล่งข้อมูล ผู้โจมตีอาจจะสามารถเปลี่ยนเส้นทางการร้องขอข้อมูลไปยังเอนทิตีภายนอกที่ผู้โจมตีควบคุมอยู่ และส่งข้อมูลที่มุ่งร้ายกลับมายังผู้ใช้บริการแทนหรือไม่เช่นนั้นผู้โจมตีอาจจะดักจับข้อมูลตอบกลับที่ถูกต้องที่แหล่งข้อมูลส่งกลับมาแล้วทำการเปลี่ยนแปลงข้อมูลให้มีเนื้อหาที่มุ่งร้าย และส่งต่อกลับไปยังผู้ใช้บริการ การโจมตีเช่นนี้จะทำให้ผู้ใช้บริการนำข้อมูลที่มีเนื้อหาที่มุ่งร้าย รวมเข้าในเอกสารเอกซ์เอ็มแอลที่จะส่งไปยังเว็บเซอร์วิซ

5) **การโจมตีแบบปฏิเสธการให้บริการ**

วัตถุประสงค์ของการโจมตีแบบปฏิเสธการให้บริการ (Denial of Services Attacks) คือการโจมตีสภาพพร้อมใช้งาน โดยจะป้องกันไม่ให้ผู้ให้บริการได้รับหรือตอบกลับข้อความที่มาจากผู้ใช้บริการและอาจทำให้ไม่สามารถให้บริการได้ เช่น ทำให้ระบบหยุดทำงาน (Crash) หรือการทำงานผิดพลาด การโจมตีประเภทนี้ ได้แก่

- **การโจมตีตัวแจงส่วนเอกซ์เอ็มแอล** (XML Parser Attacks) แอปพลิเคชันส่วนใหญ่จำเป็นต้องมีการแจงส่วนข้อมูลเข้าและออกในรูปแบบเอกซ์เอ็มแอลโดยใช้ตัวแจงส่วนเอกซ์เอ็มแอล ซึ่งอาจมีความเป็นไปได้ที่ผู้โจมตีจะแก้ไขข้อมูลซึ่งมีผลกระทบกับการประมวลผลของตัวแจงส่วนเอกซ์เอ็มแอล ผลกระทบดังกล่าวทำให้ตัวแจงส่วนเอกซ์เอ็มแอลเกิดล้มเหลว เนื่องจากมีการบริโภคทรัพยากรมากเกินไปทำให้มีการทำงานช้าลง เป้าหมายของผู้โจมตีคือการทำให้ตัวแจง

ส่วนเอกซ์เอ็มแอลล้มเหลวและทำให้เว็บเซอร์วิซไม่สามารถให้บริการได้ เช่น การโจมตีแบบโอเวอร์ไซด์เพย์โหลด(Oversized Payload Sent to XML Parsers) และรีเคอร์ซิฟเพย์โหลด (Recursive Payload Sent to XML Parsers)

- **การทำให้ทรัพยากรหมดสิ้นผ่านฟลัดดิง** (Resources Depletion through Flooding) การโจมตีนี้จะมีการสำเนาคำร้องขอบริการที่ถูกต้องและส่งซ้ำไปยังผู้ให้บริการ ผู้โจมตีอาจจะส่งข้อความซ้ำๆเพื่อพยายามทำให้เว็บเซอร์วิซเกิดการทำงานเกินพิกัด

- **การทำให้ทรัพยากรหมดสิ้นผ่านดีทีดีอินเจคชันในข้อความโซป** (Resource Depletion through DTD Injection in SOAP Message) ผู้โจมตีจะใช้ประโยชน์จากการส่งข้อความโซปที่มีดีทีดีอินเจคชัน ซึ่งเมื่อประมวลผลแล้วจะส่งผลให้มีการบริโภคทรัพยากรมากเกินไปจนหมดสิ้นลง

- **เอกซ์เอ็มแอลปิงออฟเดธ** (XML Ping of Death) ผู้โจมตีจะส่งข้อความเอกซ์เอ็มแอลขนาดเล็กจำนวนมากโดยส่งในอัตราที่รวดเร็วเพียงพอที่จะทำให้ระบบไม่สามารถให้บริการได้

- **การวางยาเอกซ์เอ็มแอลสคีมา** (XML Schema Poisoning) เหมือนในหัวข้อการโจมตีบูรณภาพ

6) การโจมตีแบบคอมมานด์อินเจคชัน

วัตถุประสงค์ของการโจมตีแบบคอมมานด์อินเจคชัน (Command Injection Attacks) คือการโจมตีโดยการใส่คำสั่งที่สามารถเข้าไปควบคุมหรือเรียกดูข้อมูลภายในเอกสารหรือฐานข้อมูลของระบบ การโจมตีประเภทนี้ ได้แก่

- **ซีเควลอินเจคชัน** (SQL Injection) การโจมตีนี้ผู้โจมตีจะใส่ข้อมูลการควบคุมที่มีคำสั่งซีเควลแทรกเข้าไปในอินพุต ผลการโจมตีจะทำให้สามารถเรียกดู เปลี่ยนแปลง แก้ไข หรือลบข้อมูลในฐานข้อมูลของเว็บเซอร์วิซได้

- **ซีเควลอินเจคชันผ่านการแทรกแซงโซปพารามิเตอร์** (SQL Injection through SOAP Parameter Tampering) การโจมตีนี้ผู้โจมตีจะทำการแก้ไขพารามิเตอร์ของข้อความโซปซึ่งส่งมาจากผู้ใช้บริการไปยังผู้ให้บริการโดยเริ่มจากการโจมตีด้วยซีเควลอินเจคชัน (ใส่คำสั่งซีเควล) เมื่อฝั่งผู้ให้บริการขาดการตรวจสอบข้อความดังกล่าวก่อนจะประมวลผลทำให้คำสั่งซีเควลสามารถเข้าถึงโดยอาจเรียกดู เปลี่ยนแปลง แก้ไข หรือลบข้อมูลในฐานข้อมูลของเว็บเซอร์วิซได้

- **เอกซ์พาธอินเจคชัน** (XPath Injection) การโจมตีนี้ผู้โจมตีสามารถป้อนข้อมูลการควบคุมพิเศษผ่านนิพจน์เอกซ์พาธไปยังฐานข้อมูลเอกซ์เอ็มแอลโดยเลี่ยงการตรวจสอบ ผลการโจมตีจะทำให้สามารถเรียกข้อมูลจากฐานข้อมูลตามนิพจน์ที่ส่งไปได้
- **เอกซ์เควียรีอินเจคชัน** (XQuery Injection) การโจมตีนี้มีลักษณะเดียวกับซีเควลอินเจคชัน แต่เป็นการโจมตีมายังฐานข้อมูลเอกซ์เอ็มแอล โดยการส่งข้อมูลจากภายนอกมายังเควียรี แต่ข้อมูลนั้นไม่ถูกตรวจสอบ จึงอาจเป็นอะไรก็ได้ที่จะถูกประมวลผลในระบบ เช่น คำสั่งที่ใช้ในการดูว่าในฐานข้อมูลนั้นมีข้อมูลอะไรบ้าง คำสั่งที่ใช้ในการสอบถามข้อมูลจากไฟล์และแหล่งข้อมูลระยะไกลอื่นๆ เป็นต้น

ภาคผนวก ข

แบบสอบถามงานวิจัย

แบบสอบถามนี้เป็นส่วนหนึ่งของวิทยานิพนธ์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ชื่อวิทยานิพนธ์

ชื่อภาษาไทย: แบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซโดยอิงการจัดให้มีวิธีการรับมือการโจมตี

ชื่อภาษาอังกฤษ: A Security Measurement Model for Web Services Based on Provision of Attack Countermeasures

อาจารย์ที่ปรึกษาวิทยานิพนธ์: รองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา

ผู้ทำวิจัย: นายทศพล บ้านคลองสี่

อีเมล์: todsapon.b@hotmail.com, todsapon.b@gmail.com

แบบสอบถามนี้ประกอบด้วย 2 แบบประเมิน ดังนี้

แบบประเมินที่ 1 ประเมินเว็บเซอร์วิซของผู้กรอกแบบประเมิน

วัตถุประสงค์

1.1) เพื่อให้ทราบว่าในวงการที่มีการนำเว็บเซอร์วิซมาใช้นั้น ผู้ให้บริการมีความตระหนักในเรื่องของความมั่นคงมากน้อยเพียงใด โดยเฉพาะเรื่องการป้องกันการโจมตี

แบบประเมินที่ 2 ประเมินความเหมาะสมของแบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซ

วัตถุประสงค์

2.1) เพื่อให้ทราบถึงความคิดเห็นของผู้ประเมินว่าวิธีการวัดความมั่นคงที่เสนอโดยผู้วิจัย มีความเหมาะสมอยู่ในระดับใด

คุณสมบัติของผู้กรอกแบบสอบถาม (Requirements)

1) ผู้กรอกควรมีความรู้เกี่ยวกับเว็บเซอร์วิซ (Web Services) และ/หรือ ด้านความมั่นคง (Security)

2) หน่วยงานของผู้กรอกมีการใช้งานเว็บเซอร์วิซ (Web Services)

ข้อมูลของผู้กรอก ให้เลือกข้อมูลดังต่อไปนี้ (แบบสอบถามจริงทำในไฟล์เอกซ์เซลล์)

ระดับการศึกษา: ☐ต่ำกว่า ป.ตรี ☐ป.ตรี ☐ ป.โท ☐ป.เอก

ตำแหน่ง: ☐Programmer ☐System Administrator ☐Research ☐System Designer
☐System Analyst ☐IT Security Specialist ☐IT Manager

อื่นๆ (โปรดระบุ)_____

ประสบการณ์การทำงาน: ด้าน Web Services: _____ ปี ด้าน Security: _____ ปี

โดเมนของเว็บเซอร์วิซ:

☐ธนาคาร ☐ปิโตรเลียม ☐การสื่อสาร ☐อสังหาริมทรัพย์ ☐การคมนาคม
☐การศึกษา ☐เทคโนโลยีสารสนเทศ ☐การปกครอง ☐การซื้อ-ขายสินค้า
อื่นๆ (โปรดระบุ) _____

รูปแบบของเว็บเซอร์วิซ:

☐Business to Business (B2B) ☐Government to Business (G2B)
☐Business to Customer (B2C) ☐Government to Customer (G2C)
☐Customer to Customer (C2C) ☐Government to Government (G2G)

ขนาดของหน่วยงาน:

☐น้อยกว่า 50 คน ☐50-200 คน ☐มากกว่า 200 คน

ลักษณะเว็บเซอร์วิซ:

☐ใช้ภายในองค์กร (Internal)
☐สาธารณะ (Public)
☐ทั้งภายในองค์กรและสาธารณะ (Internal and Public)

โพรโทคอลที่ใช้ในการพัฒนาเว็บเซอร์วิซ: ☐SOAP ☐REST

ความสำคัญของเว็บเซอร์วิซ: ☐มาก ☐ปานกลาง ☐น้อย

ปริมาณการใช้งานเว็บเซอร์วิซ: ☐มาก ☐ปานกลาง ☐น้อย

แบบประเมินที่ 1: ประเมินเว็บเซอร์วิซของผู้กรอก

<u>วิธีกรอกแบบประเมินที่ 1</u>

1) ให้ใส่เลข 1 ทุกรายการเฉพาะช่องว่าง เช่น ถ้าผู้กรอกมีการทำวิธีการรับมือในแต่ละข้อใดๆ ให้ใส่เลข 1 ในช่อง ทำ ถ้าไม่มีการทำวิธีการรับมือในแต่ละข้อใดๆ ให้ใส่เลข 1 ในช่องไม่ทำ เพราะ 0(1) คือ ขาดงบประมาณ 0(2) คือ ลงทุนสูงทำแล้วไม่คุ้ม 0(3) คือ ระบบไม่ต้องการ 0(4) คือ ไม่รู้จัก และ 0(5) คือ อื่นๆ ดังตารางที่ ข.1 ผลลัพธ์ผู้ประเมินจะได้ทราบค่าคะแนน (Security Scores) และระดับความมั่นคง (Security Levels) ของเว็บเซอร์วิซหรือระบบของผู้ประเมิน ดังตารางที่ ข.2

2) ผู้กรอกสามารถดูคำอธิบายความหมายเพิ่มเติมของวิธีการรับมือและความสัมพันธ์ของการโจมตีบนเว็บเซอร์วิซ ได้ที่แท็บชื่อ (Info.) Countermeasures Descrp. และ (Info.) Attacks Descrp. ตามลำดับ หรือโหลดไฟล์ได้จาก http://dl.dropbox.com/u/33375224/Description.pdf เพื่อเป็นข้อมูลประกอบการกรอกแบบประเมิน เมื่อกรอกเสร็จแล้ว ท่านจะเห็นผลลัพธ์ค่าคะแนนและระดับความมั่นคงของเว็บเซอร์วิซ

ตารางที่ ข.1 การกรอกข้อมูลรายการวิธีการรับมือที่ทำและไม่ทำของผู้ตอบแบบสอบถาม

No. of CM	Countermeasures	Yes	No				
		(1)	0(1)	0(2)	0(3)	0(4)	0(5)
1	**WS-Security Mechanisms**						
1.1	XML Encryption						
1.2	XML Signature						
1.3	Security Tokens						
2	**Transport-level Security Mechanisms**						
3	**Schema Validation**						
3.1	Defining whether the incoming messages have to be validated against the underlying message schema						
3.2	Defining the level of validation that needs to be enforced for schema validation						
3.3	Defining definition of additional validation rules that can be performed on the message element or attributes						
4	**Schema Hardening**						
5	**Service Virtualization**						
6	**Strong Input Validation**						
7	**Error Information Sanitization**						

ตารางที่ ข.1 การกรอกข้อมูลรายการวิธีการรับมือที่ทำและไม่ทำของผู้ตอบแบบสอบถาม (ต่อ)

No. of CM	Countermeasures	Yes (1)	No				
			0(1)	0(2)	0(3)	0(4)	0(5)
8	Use of Parameterized Queries						
9	Safe Programming						
10	Memory Allocation Countermeasures						
11	Compiler-Based Countermeasures						
12	Library-Based Countermeasures						
13	Use of WS-Addressing						
14	XSL Validators						
15	WSDL Reduction						
16	Strong Password Policy						
17	Configuration Rules and Policies on the XML Firewall						
17.1	Restricting the size of the XML messages						
17.2	Limiting the response time for every request						
17.3	Limiting the number of elements and attributes per message						
17.3.1	Defining the maximum amount of nesting allowed inside a particular element						
17.3.2	Defining the maximum number of attributes allowed for a particular element						
17.3.3	Defining the maximum number of elements allowed for each level in the tree						
17.3.4	Allowing the policy to define whether recursion is allowed within the XML message. This should be switched on only in specific instances when the underlying schema of the message is extremely complex						
17.4	XML DoS Protection						
17.4.1	All requests from an IP address which is sending spurious messages should be blocked						
17.4.2	The threshold number of requests at which the firewall should activate its exception management scenario						
17.4.3	The threshold at which action, which might include notification, is taken when a service starts returning an unusually high number of errors or SOAP faults						
17.4.4	The threshold at which action can be taken when an excessive number of HTTP unauthorized/forbidden errors are returned						

ตารางที่ ข.1 การกรอกข้อมูลรายการวิธีการรับมือที่ทำและไม่ทำของผู้ตอบแบบสอบถาม (ต่อ)

No. of CM	Countermeasures	Yes (1)	No				
			0(1)	0(2)	0(3)	0(4)	0(5)
17.4.5	The threshold at which action can be taken when message processing takes a large number of CPU cycles						
17.4.6	Indicating the type of notification that is required						
17.4.7	Indicating whether the XML firewall should automatically shut down the service if the threshold limit has been reached						
17.4.8	Automatic restart of the service after the specified time interval						
17.4.9	Defining the maximum number of requests for a service						
18	Other Countermeasures						
18.1	Creating a handshake mechanism for interacting with ad hoc WSDL or Web service to ensure validity						
18.2	Configuring the XML processor to only retrieve external entities form trusted sources						
18.3	Authenticating both services and their discovery, and protecting that authentication mechanism simply fixes the bulk of this problem						
18.4	Using the correct SOAP and XMLRPC implementations						
18.5	Suppressing external URI references to protect against malicious data						
18.6	Do not expose the user accounts that have access to host commands to external entities						
18.7	Filtering messages based on Web service name, or Web service URL						
18.8	Configuring network access control to accept incoming message from a specific IP address						
18.9	Implementing a password throttling mechanism						
18.10	Passwords need to be recycled to preventing aging						
18.11	Delete all default account credentials that may be put in by the product vendor						
18.12	The use of HMAC to hash the response from the server can also be used to thwart reflection						
18.13	Introducing a random nonce with each new connection						
18.14	Using randomly generated file names for temporary files						

ตารางที่ ข.1 การกรอกข้อมูลรายการวิธีการรับมือที่ทำและไม่ทำของผู้ตอบแบบสอบถาม (ต่อ)

No. of CM	Countermeasures	Yes (1)	No				
			0(1)	0(2)	0(3)	0(4)	0(5)
18.15	Do not use Unix and Linux systems						
18.16	Disallowing the inclusion of DTDs in SOAP messages						
18.17	For an application that uses a known schema, use a local copy or a known good repository instead of schema reference supplied in the XML document						
18.18	Database user used by the application in a particular context has the minimum needed privileges to the database such as Run XML parsing and query infrastructure with minimal privileges						
18.19	Be aware of improper use of access function calls such as chown(), tempfile(), chmod(), etc. can cause a race condition						
18.20	Using synchronization to control the flow of execution						
18.21	Using static analysis tools to find race conditions						
18.22	Performing input white list validation on all XML input						
18.23	Regenerate the session ID after login						
18.24	Check the originating IP address of the login request and any subsequent requests						
18.25	Bind the session ID to user's SSL client certificate						
18.26	Encrypt the data passed between the parties in particular the session key						
18.27	Using industry standards session key generation mechanisms						
18.28	Encrypting and/or signing the session ID						
18.29	Using strong session identifiers that are protected in transit and at rest						
18.30	Utilizing session timeout for all session IDs at runtime						
18.31	Verify authenticity of all session IDs at runtime						
18.32	Building throttling mechanism into the resource allocation						
18.33	Providing for a timeout mechanism for allocated resources whose transaction does not complete within a specified interval						
18.34	Providing for network flow control and traffic shaping to control access to the resources						

ตารางที่ ข.2 ผลลัพธ์ที่ได้จากการกรอกแบบประเมินที่ 1 (เมื่อกรอกเสร็จแล้วจะคำนวณผลให้)

ค่าคะแนนและระดับความมั่นคงที่มีต่อแง่มุมด้าน	**คะแนนสูงสุด** (MAX Score)	**ได้คะแนน** (Score)	**อยู่ในระดับ** (Level)
ความสามารถในการรับมือการโจมตีที่มีความรุนแรง $(S_{SEV} : Severity)$	315		
ความสามารถในการรับมือการโจมตีที่มีเครื่องมือช่วยในการโจมตี $(S_{LOE} : LikelihoodOfExploit)$	201		
ความสามารถในการรับมือการโจมตีที่ส่งผลต่อการรักษาความลับ $(S_{CON} : Confidentiality)$	165		
ความสามารถในการรับมือการโจมตีที่ส่งผลต่อการบูรณภาพ $(S_{INT} : Integrity)$	186		
ความสามารถในการรับมือการโจมตีที่ส่งผลต่อสภาพพร้อมใช้งาน $(S_{AVA} : Availability)$	156		
ความสามารถในการรับมือการโจมตีรวมทุกแง่มุม (S_{ALL})	204.6		

3) ผู้กรอกตอบคำถามโดยเลือกตอบในช่อง สูง/ปานกลาง/ต่ำ อย่างใดอย่างหนึ่ง พร้อมเหตุผล ดังนี้

3.1) ท่านตระหนักถึงคุณภาพของการบริการด้านความมั่นคงมากน้อยเพียงใด

☐สูง ☐ปานกลาง ☐ต่ำ

3.2) ท่านสามารถทำความเข้าใจและกรอกข้อมูลประเมินได้ง่ายมากน้อยเพียงใด:

☐สูง ☐ปานกลาง ☐ต่ำ

เหตุผล เพราะ_____

_____

_____

_____

แบบประเมินที่ 2: ประเมินความเหมาะสมของแบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซที่ผู้วิจัยได้นำเสนอ

<u>วิธีการกรอกแบบประเมินที่ 2</u>

1) ผู้กรอกศึกษาแบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซที่ผู้วิจัยได้นำเสนอในบทความวิชาการ [9] โดยท่านสามารถอ่านได้จากในแบบสอบถามนี้หรือดาวน์โหลดในรูปบทความวิชาการได้จาก http://zeus.cp.eng.chula.ac.th/~g52tbn/Todsapon_ANSCSE15.pdf ในรูปแบบภาษาอังกฤษ และ http://dl.dropbox.com/u/33375224/TextQuestionnaire2.pdf ในรูปแบบภาษาไทย

2) จากงานวิจัยดังกล่าวให้ผู้กรอกตอบคำถามโดยเลือกตอบในช่อง สูง/ปานกลาง/ต่ำ อย่างใดอย่างหนึ่ง พร้อมเหตุผลและข้อเสนอแนะ ดังนี้

2.1) ท่านคิดว่าข้อมูล Checklists ในรูป COUNTERMEASURE PROVISION TEMPLATE ข้างต้น ซึ่งแสดงรายการวิธีการรับมือ (Countermeasures) ต่างๆต่อ 28 แบบการโจมตี (Attacks) มีความสมเหตุสมผลมากน้อยเพียงใด เช่น ท่านรู้ว่ามีวิธีการรับมือต่อการโจมตีหนึ่งๆมากกว่าที่มีอยู่ใน Template หรือ Template นี้ยังมีไม่พอหรือมีมากพอในทางปฏิบัติจริง

☐สูง ☐ปานกลาง ☐ต่ำ

เหตุผล เพราะ_____

_____

_____

_____

2.2) ท่านคิดว่าวิธีการวัดความมั่นคงตามแบบจำลองงานวิจัยนี้ มีความสมเหตุสมผลมากน้อยเพียงใด

☐สูง ☐ปานกลาง ☐ต่ำ

เหตุผล เพราะ_____

_____

_____

_____

2.3) ท่านเห็นว่าแนวทางในการพิจารณาของงานวิจัยนี้มีประโยชน์ในระดับใด

☐สูง ☐ปานกลาง ☐ต่ำ

เหตุผล เพราะ_____

_____

_____

_____

2.4) ข้อเสนอแนะ

_____

_____

_____

_____

ผลการตอบแบบสอบถามงานวิจัย

<u>ผลการตอบแบบประเมินที่ 1</u>: ประเมินเว็บเซอร์วิซของผู้กรอก

จากผู้ตอบแบบสอบถามจำนวน 39 คน สามารถแสดงรายละเอียดข้อมูลของผู้ตอบแบบสอบถามดังตารางที่ ข.3 และผลการสำรวจวิธีการรับมือ ดังตารางที่ ข.4

<u>จากคำถาม</u>

3.1) ท่านตระหนักถึงคุณภาพของการบริการด้านความมั่นคงมากน้อยเพียงใด

พบว่า สูง (High) มี 23 คน คิดเป็นร้อยละ 59 ปานกลาง (Medium) มี 12 คน คิดเป็นร้อยละ 31 และต่ำ (Low) มี 4 คน คิดเป็นร้อยละ 10

3.2) ท่านสามารถทำความเข้าใจและกรอกข้อมูลประเมินได้ง่ายมากน้อยเพียงใด

พบว่า สูง (High) มี 5 คน คิดเป็นร้อยละ 13 ปานกลาง (Medium) มี 24 คน คิดเป็นร้อยละ 61 และต่ำ (Low) มี 10 คน คิดเป็นร้อยละ 26

โดยมีเหตุผล ดังนี้

สูง (High) เพราะ

- ติดตามการทำเรื่อง Security บน SOAP เพื่อออกแบบ Middleware และ Architecture ให้กับ ธนาคาร

ปานกลาง (Medium) เพราะ

- ถ้า Web Services ที่ใช้มีการเก็บข้อมูลสำคัญเอาไว้เช่น Services ของธนาคาร ที่สามารถเชื่อมต่อกับข้อมูลบัญชีเงินฝาก ถ้าไม่มีระบบป้องกันที่ดีพอ หรือ ระบบที่สามารถรับปริมาณการใช้ได้สูงมาก ก็จะส่งผลต่อความน่าเชื่อถือขององค์กรด้วย
- แบบสอบถามนี้ทำโดยผู้ตอบแบบสอบถาม 2 คน ซึ่งคนหนึ่งมีความรู้ด้านเว็บเซอร์วิซ และอีกคนมีความรู้ด้าน Security ซึ่งทำงานร่วมกัน ในความคิดเห็นของผู้ตอบแบบสอบถาม ยังไม่เคยที่จะนำวิธีการด้าน Security ในหลายๆ ข้อคำถามไปใช้งาน จึงเป็นเหตุผลที่ไม่สามารถตอบข้อคำถามบ้างข้อได้ นอกจากนี้เครื่องมือที่ใช้ในการพัฒนาเว็บเซอร์วิซ รวมถึง Web Services Container อาจจะมี Feature ด้าน Security เหล่านี้อยู่แล้วบางส่วน แต่เราไม่รู้ว่าสิ่งที่เครื่องมือเหล่านั้นจัดการ มีตัวไหนบ้าง
- ผู้ตอบแบบสอบถามเป็นผู้ใช้ Web Service ไม่ได้เป็นผู้ดูแล

- เนื่องจากเป็นการใช้งาน WS เฉพาะภายในองค์กรเท่านั้น ทำให้ระดับของความตระหนักต่อความมั่นคงของบริการอยู่ที่ปานกลางเท่านั้น สำหรับความยากง่ายในการกรอกแบบประเมินนี้ ยอมรับตามตรงว่าค่อนไปทางยาก เนื่องจากผู้ตอบแบบสอบถามมีความรู้เกี่ยวกับ WS ในด้านความมั่นคงและความปลอดภัยไม่มาก การใช้งานในปัจจุบันเป็นลักษณะใช้ตามขั้นตอน และความสามารถของ WS จะเป็นไปตามเทคโนโลยีที่ใช้ (เท่าที่เทคโนโลยีจะมีไว้ให้)
- เนื่องจากระบบที่ใช้งาน Web Service เป็น Intranet จึงตระหนักถึงความมั่นคง (Security) ไม่มากนัก
- ยังมีประสบการณ์ด้าน Web Service และ Security น้อย
- ผู้ทำแบบสอบถามไม่ได้มีความรู้ทางด้านนี้โดยตรง

ต่ำ (Low) เพราะ

- คำถามค่อนข้างจะเจาะลึกเกินไปและใช้คำพูดที่เข้าใจยาก ทำให้มีโอกาสที่ผู้ตอบแบบสอบถามจะตอบไม่ได้หรือตอบว่าไม่รู้จัก เพราะไม่เข้าใจคำถาม
- ไม่เข้าใจ และไม่ค่อยรู้จักสิ่งที่คำถาม ถามมากนัก
- คำถามจำเป็นต้องมีความรู้พื้นฐานสูง จึงจะทราบได้ และในความเป็นจริงแล้วไม่สามารถทราบและเข้าถึงกลไกการทำงาน และความปลอดภัยของ infrastructure ในองค์กรได้อย่างครอบคลุมและละเอียดได้จากทุกหน่วยงาน
- ในหน่วยงานขนาดใหญ่ ไม่ใช่ข้อมูลทุกอย่างเข้าถึงได้โดยทุกส่วนงาน ควรจะมีตัวเลือก (ไม่ทราบว่ามีการ implement หรือไม่) ไม่ใช่มีแต่ไม่รู้จัก
- ยังไม่รู้จักเทคโนโลยีด้าน Security มากนัก
- ทำงานเกี่ยวข้องกับ Web Service น้อย
- มีหลายเรื่องที่ไม่ทราบ และไม่เข้าใจว่ามันคืออะไร

ตารางที่ ข.3 รายละเอียดข้อมูลของผู้ตอบแบบสอบถาม

Assessor No.	Education	Position	Experience (Year)		Business Domain	Business Model	Size of Organization	Usage Types of WS	WS Protocol	Importance of WS	Usage of WS
			WS	Security							
1	Bachelor	Software Development Team Leader	2	2	IT	B2B/B2C	<50	Internal and Public	REST	High	High
2	Bachelor	Programmer	4	0	IT	B2B	>200	Internal	SOAP	High	High
3	Bachelor	Programmer	3	0	Financial Service	B2C	>200	Public	SOAP	Medium	Low
4	Bachelor	Programmer	2	2	Trading	B2C	<50	Public	SOAP	Medium	Medium
5	Master	Researcher	1	2	IT	G2C	50-200	Internal	SOAP	Medium	High
6	Bachelor	System Administrator	2	1	Education	G2G	<50	Public	SOAP	Medium	Medium
7	Bachelor	Programmer	1	2	Gorvenment	G2B	>200	Public	SOAP	Medium	Medium
8	Bachelor	System Administrator	1	2	IT	G2C	50-200	Internal	SOAP	Medium	High
9	Bachelor	Programmer	1	1	Real Estate	B2C	50-200	Internal	SOAP	Medium	Medium
10	Master	Programmer	4	0	Financial Service	B2B	>200	Internal	SOAP	High	High
11	Master	Programmer	3	1	Communication	B2B	50-200	Internal	SOAP	High	High
12	Bachelor	Programmer	2	2	IT	B2C	50-200	Internal	SOAP	Medium	Medium
13	Master	IT Manager	10	10	Bank	G2G	>200	Internal and Public	SOAP/REST	High	High
14	Master	Programmer	5	0	Bank	B2B	>200	Internal	SOAP	High	Medium
15	Bachelor	IT Security Specialist	5	8	IT	B2B	>200	Public	SOAP	High	Medium
16	Bachelor	Technical Team Leader	3	1	News	B2C	>200	Internal	SOAP	High	High
17	Bachelor	Application Architect	4	3	Bank	B2B/B2C	>200	Internal	SOAP	High	High
18	Master	Researcher	3	4	Research	G2G	<50	Internal and Public	SOAP/REST	High	High
19	Master	Researcher	3	4	Research	G2G	<50	Internal and Public	SOAP/REST	High	High
20	Master	System Analyst	3	4	IT	B2C	>200	Internal	SOAP	High	High
21	Master	Programmer	5	5	Communication	B2B/B2C	<50	Internal	SOAP	High	Medium
22	Bachelor	Programmer	2	0	IT	C2C	<50	Public	SOAP	Low	Low
23	Bachelor	Programmer	2	1	Bank	B2B	>200	Internal	SOAP	High	Medium
24	Master	Programmer	1	10	Financial Service	B2C	>200	Internal and Public	SOAP	High	Medium
25	Master	System Analyst	2	0	Bank	B2B	>200	Internal and Public	SOAP	High	High
26	Master	IT Manager	2	2	Trading	B2C	<50	Public	SOAP	High	Medium
27	Master	System Analyst	5	5	Communication	B2B/B2C	<50	Internal	SOAP	High	Medium
28	Bachelor	Programmer	1	0	Real Estate	B2B	<50	Internal	SOAP	Medium	Medium
29	Bachelor	Programmer	3	0	Bank	B2B	>200	Internal	SOAP	Low	Low
30	Bachelor	Programmer	3	2	Trading	B2B	<50	Internal	SOAP	High	High
31	Bachelor	Programmer	2	1	Communication	B2B/B2C	>200	Internal and Public	SOAP	High	High
32	Bachelor	Programmer	1	1	Trading	B2B	>200	Internal	SOAP	Medium	Medium
33	Master	IT Security Specialist	1	7	Trading	B2C	>200	Internal	SOAP	Medium	Medium
34	Bachelor	Software Configuration Management	3	5	Trading	B2C	>200	Internal	SOAP	High	High
35	Master	System Analyst	1	5	Trading	B2C	>200	Internal	SOAP	High	High
36	Bachelor	System Analyst	2	0	Trading	B2B/B2C	>200	Internal	SOAP	Medium	Medium
37	Master	Programmer	2	2	Bank	B2B	>200	Internal	SOAP	Medium	Medium
38	Bachelor	Programmer	1	1	IT	C2C	50-200	Internal	SOAP	High	Medium
39	Master	System Administrator	2	2	Communication	B2C	>200	Internal	REST	Medium	Medium

ตารางที่ ข.4 ผลการสำรวจวิธีการรับมือ

Assessor No.	Countermeasure No.																																		
	1.1	1.2	1.3	2	3.1	3.2	3.3	4	5	6	7	8	9	10	11	12	13	14	15	16	17.1	17	17.3.1	17.3.2	17.3.3	17.3.4	17.4.1	17.4.2	17.4.3	17.4.4	17.4.5	17.4.6	17.4.7	17.4.8	17.4.9
1	0(3)	0(3)	1	1	0(4)	0(4)	0(4)	0(4)	0(3)	1	0(3)	1	1	1	1	0(4)	0(3)	0(3)	0(3)	1	0(3)	0(3)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	1
2	0(3)	0(3)	1	1	1	0(3)	0(3)	0(3)	0(3)	0(3)	1	0(3)	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)
3	0(3)	0(3)	1	0(3)	1	0(3)	0(3)	0(3)	0(3)	1	1	0(3)	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)
4	0(3)	0(3)	1	1	0(3)	0(3)	0(3)	0(1)	0(1)	0(1)	1	0(3)	1	0(3)	0(3)	0(3)	1	1	0(4)	1	0(3)	0(3)	1	1	1	0(3)	0(3)	0(3)	0(3)	0(3)	1	1	1	0(1)	0(1)
5	1	1	0(3)	1	1	0(3)	0(3)	0(3)	0(1)	0(1)	0(1)	0(3)	1	0(1)	0(3)	0(1)	0(3)	1	1	1	0(3)	0(3)	0(3)	1	0(3)	1	0(3)	0(3)	0(3)	1	1	0(3)	1	1
6	1	1	0(1)	0(4)	1	0(3)	0(3)	1	0(3)	0(3)	0(3)	0(3)	1	0(1)	0(3)	0(3)	1	1	1	1	1	1	1	1	0(3)	0(3)	0(1)	0(3)	0(3)	0(3)	0(3)	1	0(3)	0(3)	1
7	0(1)	1	0(1)	0(1)	0(1)	0(1)	0(3)	0(4)	0(3)	0(3)	0(3)	0(3)	0(1)	0(2)	0(2)	0(1)	0(3)	0(1)	0(1)	0(1)	0(1)	0(1)	0(3)	0(3)	0(3)	0(1)	0(1)	0(3)	0(1)	0(2)	0(1)	0(1)	0(1)	0(3)	0(1)
8	1	1	0(3)	1	1	0(3)	0(3)	0(3)	0(1)	0(1)	0(1)	0(3)	1	0(1)	0(3)	0(1)	0(3)	1	1	1	0(3)	0(3)	0(3)	1	0(3)	1	0(3)	0(3)	0(3)	0(3)	1	1	0(3)	1	1
9	0(3)	0(3)	0(3)	1	1	0(3)	0(3)	0(3)	0(3)	1	1	0(3)	1	0(3)	0(3)	0(3)	1	1	0(3)	0(3)	0(3)	1	0(3)	0(3)	0(3)	0(3)	0(4)	0(4)	0(4)	0(4)	0(4)	1	0(4)	0(3)	0(3)
10	0(3)	0(3)	1	1	0(3)	0(3)	0(3)	1	0(3)	0(3)	1	0(3)	1	0(3)	0(3)	0(3)	1	1	1	1	0(3)	0(3)	1	1	1	0(3)	0(3)	0(3)	1	0(3)	1	1	1	0(3)	0(3)
11	1	1	1	1	1	0(3)	0(3)	0(3)	0(3)	1	1	0(3)	1	1	0(3)	0(3)	1	1	1	1	0(3)	1	0(3)	0(3)	0(3)	0(3)	0(4)	0(4)	0(4)	0(4)	0(4)	1	0(4)	1	1
12	1	0(3)	1	1	1	1	1	1	1	1	0(3)	0(3)	1	0(3)	0(2)	0(1)	0(3)	1	1	1	0(1)	1	0(2)	0(2)	0(2)	0(1)	1	0(3)	1	0(2)	1	1	1	0(3)	1
13	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0(5)	1	1	1	1	1	1	0(5)	1	1
14	1	1	0(1)	1	1	0(3)	0(3)	1	1	1	1	1	1	1	1	1	0(4)	1	1	1	0(5)	1	1	1	0(5)	0(5)	0(5)	0(5)	0(5)	0(5)	0(5)	1	0(5)	0(5)	0(5)
15	1	1	1	1	1	1	1	1	1	1	1	0(3)	0(3)	0(3)	0(3)	0(1)	0(1)	1	1	1	1	1	0(3)	1	1	1	0(1)	1	1	1	0(3)	0(3)	0(3)	0(3)	1
16	0(1)	0(1)	1	1	1	0(1)	0(1)	0(1)	1	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	1	1	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)
17	1	1	1	1	0(5)	1	1	0(5)	1	0(5)	0(3)	1	1	0(3)	0(3)	0(2)	1	1	0(1)	1	0(1)	0(1)	1	1	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	1	0(1)	0(1)	0(1)
18	1	1	1	1	1	0(5)	0(5)	0(5)	0(3)	1	0(5)	1	1	0(4)	0(3)	0(4)	1	0(3)	0(5)	1	0(4)	0(4)	0(3)	0(3)	0(3)	0(3)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)
19	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)
20	1	0(1)	1	1	1	1	1	1	1	1	1	1	1	1	0(3)	1	0(4)	0(1)	0(4)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
21	0(3)	0(3)	1	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	1	1	0(3)	0(3)	0(4)	1	0(4)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)
22	0(3)	0(2)	0(2)	0(2)	0(1)	0(1)	1	0(1)	1	1	1	1	1	0(1)	0(1)	1	0(2)	1	1	1	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)
23	1	0(3)	1	1	1	0(1)	0(1)	0(3)	0(1)	1	0(4)	1	1	1	0(3)	0(1)	1	1	1	0(3)	1	1	0(4)	0(4)	0(4)	0(4)	0(3)	0(3)	1	1	1	0(4)	0(4)	0(4)	1
24	1	0(3)	1	1	0(1)	0(1)	0(1)	0(1)	1	0(5)	1	0(5)	1	0(5)	0(5)	0(5)	1	1	0(4)	0(5)	0(5)	1	0(5)	0(5)	0(5)	0(5)	0(5)	0(5)	0(5)	0(5)	0(5)	1	0(5)	0(5)	0(5)
25	1	0(4)	1	1	1	0(1)	1	1	1	1	0(3)	0(4)	1	1	0(4)	0(4)	0(4)	0(3)	1	1	0(4)	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	1	0(3)	0(3)	0(3)
26	1	1	1	0(1)	1	1	1	1	0(3)	1	1	1	1	1	1	0(1)	1	0(2)	0(4)	1	1	1	1	0(4)	1	0(4)	1	1	0(1)	0(1)	0(4)	1	0(4)	0(4)	1
27	0(3)	0(3)	1	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	1	1	0(3)	0(3)	0(4)	1	0(4)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)
28	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	1	0(3)	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)
29	1	0(4)	1	0(5)	1	1	1	0(4)	0(5)	1	1	1	1	0(4)	1	1	0(3)	0(3)	1	1	1	1	1	0(2)	0(2)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)
30	0(3)	0(3)	0(1)	1	0(1)	0(1)	0(4)	0(1)	0(4)	0(4)	0(1)	1	0(1)	0(4)	0(4)	0(4)	0(4)	0(3)	0(4)	1	0(4)	0(4)	0(3)	0(3)	0(3)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)
31	1	0(3)	1	1	1	1	1	1	1	1	0(4)	1	1	1	1	1	1	1	1	1	1	1	0(4)	0(4)	0(4)	0(4)	1	1	1	1	1	1	1	1	1
32	0(3)	0(3)	0(3)	0(2)	1	1	0(4)	0(3)	1	0(3)	0(3)	1	1	0(3)	0(3)	0(3)	0(4)	0(3)	0(3)	0(3)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(3)
33	1	1	1	1	0(1)	0(1)	0(1)	0(1)	1	1	1	1	1	1	1	1	1	0(4)	1	1	1	1	1	1	1	1	0(1)	1	0(1)	1	1	1	1	1	1
34	1	1	1	1	1	1	1	1	1	1	1	1	0(1)	0(1)	0(1)	0(1)	1	1	0(3)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
35	0(4)	0(4)	1	1	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	1	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)
36	1	1	0(4)	1	1	1	0(3)	0(3)	1	1	0(3)	1	1	0(3)	0(3)	1	1	0(3)	0(3)	0(3)	0(3)	1	0(3)	0(3)	0(3)	0(3)	1	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)
37	1	1	1	0(3)	0(3)	1	0(3)	1	1	1	1	1	1	0(3)	1	0(3)	1	1	0(1)	1	1	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(1)	0(1)	0(3)
38	0(3)	0(1)	0(3)	0(2)	1	0(1)	0(2)	0(3)	0(3)	0(1)	0(3)	0(3)	0(1)	0(4)	0(4)	0(3)	0(3)	0(1)	0(2)	0(3)	1	1	1	0(2)	0(3)	0(1)	0(1)	0(2)	0(2)	0(2)	0(3)	1	0(2)	0(2)	0(1)
39	0(3)	0(3)	1	1	0(1)	0(1)	0(1)	0(1)	1	1	0(1)	1	1	1	0(3)	1	0(3)	1	1	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	1	1	0(3)	0(3)	1	1	1	1	1

ตารางที่ ข.4 ผลการสำรวจวิธีการรับมือ (ต่อ)

Assessor	Countermeasure No.																																
No.	18.1	18.2	18.3	18.4	18.5	18.6	18.7	18.8	18.9	18.10	18.11	18.12	18.13	18.14	18.15	18.16	18.17	18.18	18.19	18.20	18.21	18.22	18.23	18.24	18.25	18.26	18.27	18.28	18.29	18.30	18.31	18.32	18.33	18.34
1	0(4)	0(3)	0(3)	0(3)	1	1	1	1	1	1	1	0(4)	0(4)	1	0(5)	0(3)	0(3)	0(3)	1	0(4)	0(4)	1	1	0(3)	1	1	1	1	1	1	1	1	1	1
2	0(3)	0(3)	0(3)	0(3)	0(3)	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	1	1	0(3)	0(3)	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	1	0(3)
3	0(2)	0(3)	0(3)	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)
4	0(3)	1	1	0(4)	0(3)	0(1)	0(3)	1	0(1)	0(3)	0(3)	0(3)	0(3)	1	0(3)	1	1	1	0(3)	0(3)	0(3)	1	0(3)	0(3)	0(3)	0(3)	1	1	1	0(3)	0(3)	0(2)	0(3)	0(1)
5	1	0(3)	0(1)	0(4)	1	1	0(3)	1	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(4)	1	1	0(4)	1	0(3)	1	1	0(3)	0(3)	1	1	1	0(3)	1	0(3)	1	1	0(3)
6	0(3)	1	0(3)	1	1	1	1	1	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(4)	0(3)	0(3)	1	1	1	0(3)	0(3)	1	0(3)	0(3)	1	1	1	1	0(1)	0(1)	1	1
7	0(2)	0(1)	0(2)	0(1)	0(1)	0(2)	1	0(2)	0(2)	0(1)	0(1)	0(1)	0(1)	0(1)	0(3)	0(3)	0(3)	0(1)	0(1)	0(1)	0(2)	0(1)	0(1)	0(2)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(3)	0(1)	1	0(3)
8	1	0(3)	0(1)	0(4)	1	1	0(3)	1	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(4)	1	1	0(4)	1	0(3)	1	1	0(3)	0(3)	1	1	1	0(3)	1	0(3)	1	1	0(3)
9	0(4)	0(3)	0(3)	1	1	1	1	1	0(3)	0(3)	0(3)	0(4)	0(4)	0(3)	1	0(4)	1	1	0(4)	1	0(3)	1	1	1	1	0(3)	0(3)	0(3)	0(3)	1	0(3)	1	1	0(3)
10	0(3)	1	1	0(4)	1	1	0(3)	1	1	1	0(3)	0(3)	0(3)	1	0(3)	1	1	1	0(3)	0(3)	0(3)	1	0(3)	0(3)	0(3)	0(3)	1	1	1	1	1	1	1	1
11	0(4)	0(3)	1	1	1	1	1	1	0(3)	0(3)	0(3)	0(4)	0(4)	0(3)	1	0(4)	1	1	0(4)	1	0(3)	1	1	1	1	0(3)	0(3)	0(3)	0(3)	1	0(3)	1	1	0(3)
12	0(2)	0(1)	1	1	0(1)	0(1)	0(1)	0(2)	0(2)	0(1)	0(1)	0(1)	0(1)	0(1)	0(3)	0(3)	0(3)	0(1)	0(1)	0(1)	0(2)	0(1)	0(1)	0(2)	0(1)	0(1)	0(1)	0(1)	0(2)	0(1)	0(2)	0(1)	0(1)	1
13	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0(5)	1	1	1	1	0(3)	0(3)	1	1	1	1	1	1	1	1	1	0(3)	1	1	1
14	1	1	1	1	1	1	1	1	1	1	1	0(4)	0(4)	0(4)	1	1	1	1	1	1	0(1)	1	1	1	0(1)	0(1)	0(1)	0(1)	1	1	1	1	1	1
15	1	0(3)	1	1	1	1	1	0(1)	1	0(2)	0(1)	0(3)	0(3)	0(3)	0(3)	0(3)	1	1	1	0(4)	0(4)	1	1	1	0(1)	0(2)	0(1)	0(1)	0(1)	1	1	1	1	1
16	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	1	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)	0(1)
17	1	1	1	1	1	1	1	0(1)	1	1	1	0(4)	0(1)	0(1)	0(5)	1	1	1	1	1	0(1)	1	1	1	1	1	1	1	0(1)	1	1	0(1)	1	1
18	0(3)	0(3)	1	1	0(4)	1	0(3)	1	0(5)	1	1	0(4)	0(4)	1	0(5)	1	0(3)	1	0(3)	0(4)	0(5)	1	1	1	1	1	0(5)	0(5)	0(5)	1	1	1	1	0(4)
19	0(3)	0(3)	0(3)	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(5)	0(3)	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)
20	0(4)	1	1	0(4)	1	1	1	1	1	1	1	0(4)	0(4)	0(4)	1	0(4)	0(4)	1	1	0(4)	0(4)	1	1	1	0(4)	0(4)	0(4)	1	0(4)	1	1	1	1	1
21	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	1	1	0(3)	0(3)	0(3)	0(3)	1	1	0(3)	0(3)	0(3)	1	0(3)	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	1	1	0(3)	0(3)	0(3)
22	0(1)	0(1)	0(1)	1	0(1)	0(1)	1	1	1	1	1	0(2)	0(4)	1	1	1	1	1	0(1)	0(2)	0(1)	1	1	1	0(2)	1	1	0(1)	1	1	1	0(1)	1	0(1)
23	0(4)	0(3)	0(3)	1	1	1	1	0(3)	0(3)	1	0(3)	0(4)	0(4)	0(3)	0(3)	0(3)	0(3)	1	0(3)	1	0(3)	1	1	1	1	1	1	0(3)	0(4)	1	0(3)	0(1)	0(1)	1
24	0(5)	0(5)	1	1	1	1	0(5)	0(2)	1	0(5)	0(5)	0(5)	0(5)	0(5)	0(5)	0(5)	1	0(5)	0(5)	1	0(5)	0(5)	0(5)	1	0(5)	0(5)	0(5)	0(5)	0(5)	1	1	0(5)	1	0(5)
25	0(3)	0(3)	0(3)	1	0(3)	1	0(3)	1	1	0(3)	0(3)	0(4)	0(4)	0(3)	0(3)	0(3)	0(3)	1	1	1	1	1	0(3)	0(3)	1	1	1	1	1	1	1	1	1	1
26	0(4)	0(4)	1	1	0(4)	1	0(4)	1	1	1	1	0(4)	0(4)	1	0(1)	0(4)	0(4)	1	1	0(2)	0(2)	1	0(3)	1	0(2)	0(1)	0(1)	0(1)	0(4)	1	1	0(1)	1	0(3)
27	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	1	1	0(3)	0(3)	0(4)	0(3)	1	1	0(3)	0(3)	0(3)	1	0(3)	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	1	1	0(3)	0(3)	0(3)
28	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(4)	0(4)	0(4)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	1	1	1	0(3)	0(3)
29	0(4)	0(4)	1	1	0(4)	0(4)	1	1	0(5)	1	0(4)	0(4)	0(4)	0(4)	1	1	0(4)	0(2)	1	1	0(4)	1	1	0(4)	0(4)	0(4)	0(4)	0(4)	0(4)	1	0(4)	1	1	0(4)
30	1	0(3)	1	1	0(4)	0(4)	0(4)	1	1	1	1	0(4)	0(4)	0(4)	1	0(4)	1	0(4)	0(4)	0(4)	0(4)	0(4)	1	0(4)	0(4)	1	1	0(4)	0(4)	1	1	0(1)	0(1)	0(4)
31	0(4)	1	1	0(3)	1	1	1	1	1	1	0(4)	0(3)	1	0(3)	0(5)	0(4)	1	1	0(4)	1	1	1	1	1	1	1	1	1	1	1	0(4)	0(4)	1	1
32	1	0(3)	0(4)	0(4)	1	0(4)	0(4)	1	0(3)	0(3)	0(3)	0(3)	0(4)	0(4)	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(1)	1	1
33	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
34	0(1)	0(1)	0(1)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0(1)	0(1)	0(1)	0(1)	1	1	1	1	1	1	1	1	0(1)	0(1)	1
35	0(4)	0(4)	1	1	1	1	1	1	1	1	1	1	1	1	0(1)	0(4)	0(4)	0(4)	0(4)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
36	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	1	1	0(3)	1	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	1	0(3)	1	1	0(3)	1	1	1	1	0(3)	1	1	0(3)	1	0(3)
37	0(3)	0(3)	0(3)	0(4)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(4)	0(5)	0(4)	1	1	0(1)	1	0(3)	1	1	0(3)	0(3)	0(3)	0(3)	1	1	1	1	0(3)	1	1
38	0(3)	0(3)	0(3)	0(1)	0(1)	0(1)	0(3)	0(3)	0(4)	0(4)	1	1	0(1)	0(1)	0(2)	0(4)	0(4)	1	1	0(2)	0(1)	0(4)	0(4)	1	0(1)	0(1)	0(4)	0(4)	0(1)	0(3)	0(2)	0(1)	1	1
39	0(3)	0(3)	1	0(3)	1	1	1	1	1	1	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	0(3)	1	0(3)	0(3)	0(3)	0(3)	0(3)	1	0(3)	1	1	0(3)

<u>ผลการตอบแบบประเมินที่ 2</u>: ประเมินความเหมาะสมของแบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซที่ผู้วิจัยได้นำเสนอ

<u>จากคำถาม</u>

2.1) ท่านคิดว่าข้อมูล Checklists ในรูป COUNTERMEASURE PROVISION TEMPLATE ข้างต้น ซึ่งแสดงรายการวิธีการรับมือ (Countermeasures) ต่าง ๆต่อ 28 แบบการโจมตี (Attacks) มีความสมเหตุสมผลมากน้อยเพียงใด เช่น ท่านรู้ว่ามีวิธีการรับมือต่อการโจมตีหนึ่ง ๆมากกว่าที่มีอยู่ใน Template หรือ Template นี้ยังมีไม่พอหรือมีมากพอในทางปฏิบัติจริง

พบว่า สูง (High) มี 27 คน คิดเป็นร้อยละ 69 ปานกลาง (Medium) มี 12 คน คิดเป็นร้อยละ 31 และต่ำ (Low) ไม่มีผู้ตอบ

โดยมีเหตุผล ดังนี้

สูง (High) เพราะ

- ค่อนข้างครอบคลุม เพราะในประสบการณ์ส่วนตัว การโจมตีที่จะพบมากสุดคือ DDoS, DoS, SQL Injection
- หลากหลายรูปแบบ และเป็น security standard ที่หลายองค์กรใช้งาน
- องค์กรส่วนใหญ่มักจะมีช่องโหว่เกือบทุกส่วน ถ้ามี template มาตรฐานเป็นตัวกลางวัดถึงความมั่นคงทางด้านความปลอดภัย จะทำให้ทุกระบบมีมาตรฐานเดียวกันในการวัดความปลอดภัยได้อีกด้วย
- ระบบที่พัฒนาให้ความสำคัญเพียงมุ่งเน้นในการจัดการความปลอดภัยในเรื่องดังต่อไปนี้ TLS และ Web Services Security Mechanism เท่านั้น ดังนั้น checklist ที่กำหนดมาให้ countermeasure นั้นมีมากเกินความจำเป็นกับความต้องการ อย่างไรก็ตาม อาจจะมีบางวิธีการจัดการได้มีระบบ (เช่น Web Services หรือ Web Services Engine) ได้จัดการให้แล้ว
- ระบบที่พัฒนา เน้นการให้บริการสาธารณะหรือเป็นเพียงการใช้เพื่องานวิจัย จึงไม่ได้ให้ความสำคัญกับความปลอดภัย โดยคิดว่า สิ่งที่เว็บเซิร์ฟเวอร์ และ Web Services Engine มีให้ก็เพียงพอ
- Checklist ค่อนข้างละเอียด และครอบคลุมรูปแบบการโจมตีต่าง ๆ ได้มากเพียงพอต่อการวิเคราะห์สภาพความปลอดภัยโดยรวม

- แนวความคิดดีที่ใช้ countermeasure กับ attack characteristic และ relative มาใช้คำนวณความมั่นคงของระบบ web service แต่อาจมีบางรายการการโจมตีที่ไม่อยู่ใน template เช่น Message replay หรือ countermeasure เช่น การเข้ารหัสในรูปแบบต่าง ๆ เช่น kerberos สำหรับ SOAP headers for authentication เนื่องจาก countermeasure บางตัวให้ผลการป้องกันเหมือนกัน ผู้พัฒนาระบบบางท่านอาจเลือกใช้ไม่เหมือนกัน จึงควรสรุปเป็นหมวด ๆ ในแต่ละเรื่อง และสรุป countermeasure ที่ทำได้ในแต่ละเรื่องให้ครบหรือครอบคลุมมากที่สุดที่เป็นไปได้
- จาก Template พบว่ามีมากกว่าที่ใช้ทำงานในปัจจุบันมาก
- ค่อนข้างครอบคลุมทุกรูปแบบ
- ดูจาก Template แล้วเห็นว่าวิธีการโจมตีทั้ง 28 แบบนั้นมากพอแล้ว แสดงถึงวิธีการที่ใช้สำหรับการโจมตีระบบหนึ่งๆ ที่เป็น WS ได้ครบถ้วนดี อีกทั้งวิธีการรับมือสำหรับแต่ละการโจมตีก็ใช้รับมือได้จริงๆ นอกจากนี้การจัดกลุ่มค่อนข้างเห็นความสัมพันธ์ของการโจมตีและวิธีการรับมือได้ชัดเจนดี
- น่าจะครอบคลุมวิธีการป้องกันที่มากพอจึงเชื่อมั่นว่าน่าจะมีประโยชน์ถ้าสามารถทำตาม Template ที่กล่าวมาได้
- วิธีการป้องกันการโจมตีที่ยกมานั้นก็ครอบคลุมบางส่วนที่มีใช้ในองค์หลายๆองค์กรที่ใช้กันทั่วไปเพื่อป้องกันการโจมตี
- ในการใช้งานระดับองค์กร การใช้งาน Web Service จะมีการปกป้องทั้งระดับ Hardware และ Software ซึ่งวิธีการรับมือการโจมตีทั้ง 28 แบบ สามารถปกป้องข้อมูลทางธุรกิจได้ แต่ทั้งนี้ในการใช้งานจริง อาจจะไม่ได้มีการนำวิธีการรับมือการโจมตีไปใช้ได้ ทุกรูปแบบ ขึ้นอยู่กับความเหมาะสม เวลา งบประมาณ และความสำคัญของข้อมูลที่นำไปใช้
- เนื่องจากมีการครอบคลุมการโจมตีในหลายรูปแบบ
- เพราะเป็น guideline ที่ควรคำนึงถึงในการพัฒนา web service ซึ่งการป้องกันในระดับนี้คิดว่าน่าจะช่วยแก้ปัญหาเรื่องความปลอดภัยได้ในระดับหนึ่ง

ปานกลาง (Medium) เพราะ

- งงกับคำถามบางข้อ

ต่ำ (Low) เพราะ

- ไม่ค่อยเข้าใจ และความรู้ในเรื่อง Security ของผู้กรอกยังมีน้อย

2.2) ท่านคิดว่าวิธีการวัดความมั่นคงตามแบบจำลองงานวิจัยนี้ มีความสมเหตุสมผลมากน้อยเพียงใด

พบว่า สูง (High) มี 23 คน คิดเป็นร้อยละ 59 ปานกลาง (Medium) มี 15 คน คิดเป็นร้อยละ 38 และต่ำ (Low) มี 1 คน คิดเป็นร้อยละ 3

โดยมีเหตุผล ดังนี้

สูง (High) เพราะ

- ค่อนข้างรวบรวมการป้องกันและความรู้ความเข้าใจได้เป็นอย่างดี
- สำหรับในส่วน Template วิธีการที่นำเสนอครอบคลุมกับวิธีการโจมตีและวิธีการรับมือในปัจจุบันได้อย่างครบถ้วน ในเรื่องของ Web Services Security สำหรับวิธีการวัดค่าในตัวที่ 2 (Attack Characteristic) คิดว่า นอกจากการโจมตี 5 ด้านนี้แล้ว ถ้าเกิดเพิ่มการโจมตีเพิ่มขึ้น จะทำให้การวัด Characteristic นี้มีประสิทธิภาพมากขึ้นหรือไม่ เช่น การทำ Privacy Requirement ในระดับข้อมูล และที่เพิ่มคุณค่าให้กับการโจมตีที่กำหนดเป็นค่ากลางขึ้นมานั้นยังไม่เห็นภาพว่าช่วยทำให้การวัดจุดนี้มีประสิทธิภาพอย่างไร (เช่น ทำไมจึงเลือกค่า medium - 2)
- เพราะโดยรวมค่อนข้างสมเหตุสมผลดี ในแต่ละหมวด
- เหมาะสมแล้ว แต่เนื่องจากได้ไม่อธิบายรายละเอียดที่ผู้วิจัยเลือกสำหรับค่า Relative ซึ่งคิดว่าผู้วิจัยคงกำหนดในแต่ละตัวมาแล้ว แต่ไม่รู้ว่ากำหนดให้เท่ากันทุกตัวหรือแตกต่างกันไป ซึ่งจะมีผลต่อค่าความมั่นคงที่ได้
- แม้จะยังไม่เข้าใจอย่างลึกซึ้งของหลักวิธีการคิดคะแนนนัก และแม้จะยังมีความคิดว่าบางประเด็นอาจจะเพิ่มเติมได้อีกแต่เท่าที่ทำมานี้ก็ถือว่าใช้งานได้แล้ว
- วิธีการชี้วัดนั้นน่าจะมีความน่าเชื่อถือเพราะว่าได้นำมาจากวิธีที่ได้รับการยอมรับกัน
- มีการคำนวณได้ค่อนข้างกว้างในหัวข้อที่สำคัญและจำเป็นสำหรับองค์กร

- เนื่องจากวิธีการรับมือการโจมตีในแต่ละแบบ จะไม่สามารถนำมาอ้างอิงโดยใช้หน่วยเดียวกันได้แต่ระบบที่ใช้งานมีค่าคะแนนในแบบเดียวกันไม่เท่ากัน จะสามารถนำมาวิเคราะห์ความแข็งแรงต่อการโจมตีในแบบนั้นๆได้
- ในแต่ละรูปแบบมีความจำเป็นต่อการนำมาใช้ในการประเมินและวัดประสิทธิผลของความมั่นคงในเว็บเซอร์วิซ

ปานกลาง (Medium) เพราะ

- In real environment we cannot just follow only the theory. We need to use our experience combine with right decision to clear difficult problems.
- บางข้อยังไม่เข้าใจในคำถาม และตัวเลือก
- ในแง่ทฤษฎีวิธีการคิดคะแนนตามแบบจำลองมีความเหมาะสมมาก อย่างไรก็ตามน่าจะมีความยุ่งยากในการนำมาใช้งานจริง (ปัญหาน่าจะมาจากความรู้ของผู้นำมาใช้งาน)
- เมื่อพิจารณาผลที่วัดได้ใน Questionaire1 พบว่ามีค่าได้มีความเหมาะสมกับองค์กรที่เป็นอยู่จริง จึงพอจะสรุปได้ว่าแบบจำลองการวัดดังกล่าว น่าจะมีความสมเหตุสมผลอยู่บ้าง
- เนื่องจากความเข้าใจในเรื่อง Security ยังน้อย จึงยังไม่สามารถสรุปได้ว่าแบบจำลองการวัดนี้มีความสมเหตุสมผล แต่เมื่อพิจารณาเทียบกับผลลัพธ์ที่ได้จากการทำแบบสอบถาม จึงน่าจะพอกล่าวได้ว่าแบบจำลองดังกล่าว มีความน่าเชื่อถือและสมเหตุสมผลในระดับหนึ่ง
- ความเห็นส่วนตัว น่าจะมีการจัดลำดับการให้คะแนนในแบบจำลองการวัดความมั่นคงให้แน่ชัด เพื่อที่จะได้เห็นถึงผลกระทบที่เกิดขึ้นจากความไม่ปลอดภัยของ web service เป็นลำดับๆ ได้ชัดเจน

2.3) ท่านเห็นว่าแนวทางในการพิจารณาของงานวิจัยนี้มีประโยชน์ในระดับใด

พบว่า สูง (High) มี 29 คน คิดเป็นร้อยละ 74 ปานกลาง (Medium) มี 8 คน คิดเป็นร้อยละ 21 และต่ำ (Low) มี 2 คน คิดเป็นร้อยละ 5

โดยมีเหตุผล ดังนี้

สูง (High) เพราะ

- It helps us to know the current security level of our web service. Therefore we can improve the security level to meet the security level requirement that we desire
- เป็นวิธีที่ช่วยให้องค์กรเป็นแนวทางในการนำ web services security ไปประยุกต์ใช้
- ค่อนข้างมีรายละเอียดมาก
- งานวิจัยนี้มีประโยชน์มากในเชิงการนำไปวัดความมั่นคงสำหรับเว็บเซอร์วิซ
- ช่วยให้เราสามารถตรวจสอบระบบที่มีอยู่ว่าเสี่ยงต่อการโจมตีด้านใดบ้าง
- เป็นแนวทางในการตรวจวัดระบบที่ดี และสะดวกต่อการนำไปใช้งาน
- ทำให้รับรู้วิธีการโจมตีแบบต่างๆ รวมไปถึงช่องโหว่ของ Web Service ทำให้สามารถเตรียมพร้อมรับมือได้
- ในฐานะผู้พัฒนา WS คิดว่า Model นี้เป็นประโยชน์อย่างยิ่ง เนื่องจากช่วยชี้วัดว่า WS ที่พัฒนาขึ้นนั้นมีความมั่นคงมากน้อยแค่ไหน เพราะการพิจารณาเลือกที่จะใช้วิธีการรับมือนั้นบางครั้งก็พิจารณาจากความต้องการของระบบ สถาปัตยกรรมของระบบ รวมถึงข้อกำหนด และข้อจำกัดต่างๆ ซึ่งบางครั้งจะถูกกรอบของข้อจำกัดทำให้ไม่สามารถใช้วิธีการรับมือบางอย่างได้ การมีผลอ้างอิงเช่นนี้จะช่วยทำให้เห็นได้ว่าบางครั้งต้องมีการลงทุนเพิ่มขึ้นบ้างเพื่อลดข้อจำกัด เพื่อทำให้ใช้วิธีการรับมือซึ่งจะนำไปสู่ระบบ WS ที่มีความมั่นคงสูงขึ้นต่อไป
- ในประเทศไทยเชื่อว่ายังมีคนจำนวนน้อยมากๆ ที่ทราบเรื่องพวกนี้ ดังนั้นข้อมูลเหล่านี้จึงเป็นประโยชน์อย่างมากต่อการพัฒนา การวางแผนการรับมือเมื่อเกิดเหตุการณ์การโจมตีได้อย่างทันท่วงที
- สามารถนำความรู้ที่ได้ไปประยุกต์ใช้สำหรับองค์กรที่มีเว็บเซอร์วิซ อีกทั้งองค์กรที่มีระบบที่ Critical จึงมีความเหมาะสมที่จะนำความรู้ด้านงานวิจัยนี้ไปปรับปรุงเพื่อสามารถปกป้องสร้างความมั่นคงแก่ระบบได้

- เพื่อเป็นแนวทางในการพัฒนา web service ที่มีความปลอดภัยโดยคำนึงถึงแนวทางการโจมตีจากภายนอก และช่วยในการออกแบบ web service และระบบที่มีความปลอดภัยที่สูงขึ้น

ปานกลาง (Medium) เพราะ

- อาจจะขาดข้อมูลสำคัญ ๆ ไปเช่น ภาษาที่ใช้เชื่อมต่อ Web Services อาจจะทำให้เกิดผลกระทบต่อความปลอดภัยของระบบ
- งานวิจัยชิ้นนี้นำเสนอการวัดความมั่นของระบบ Security โดยมีการวัดค่าเพื่อนำเสนอในรูปแบบที่เข้าใจได้ง่าย จึงเห็นว่างานวิจัยชิ้นมีประโยชน์ในการพิจารณาเลือกความเหมาะสม
- เป็นข้อมูลในเชิงทฤษฎี หากจะให้มีประโยชน์มากยิ่งขึ้นต้องพิจารณาในเชิงปฏิบัติร่วมด้วย
- งานวิจัยนี้ แสดงให้เห็นถึงความสำคัญของการรับมือการโจมตีที่เกิดขึ้นในการใช้งาน Web Service แต่ในทางปฏิบัติจริง จะติดปัญหาเรื่องเวลา และงบประมาณในการป้องกันระบบจากผู้โจมตี ดังนั้นในการวิจัย ควรมีระดับความยาก-ง่ายในการพัฒนาระบบเพื่อรองรับการโจมตีด้วยจะทำให้ผู้ที่อ่านงานวิจัย จัดลำดับวิธีการรับมือการโจมตีได้

ต่ำ (Low) เพราะ

- ขึ้นกับกลุ่มตัวอย่างที่ให้ทำแบบสำรวจ ซึ่งการเลือกกลุ่มตัวอย่างที่ดีเป็นไปได้ยาก

2.4) **ข้อเสนอแนะ**

- แบบทดสอบเน้นไปที่ SOAP และ XML อยู่แบบเดียวในขณะที่ระบบอย่างเช่น Facebook หรือ Twitter จะทำงานแบบ SOAP และใช้ JSON เป็นหลัก
- คำถามบางคำถามอาจสับสนกับคำตอบ ทำ ไม่ทำ
- แม้จะตระหนักถึงความสำคัญของความปลอดภัยมาก แต่ในการพัฒนาระบบผู้พัฒนาก็ต้องมองถึงความสมดุลระหว่างการให้บริการของเว็บเซอร์วิซ และความปลอดภัย ดังนั้นทางหน่วยงานจึงคำนึงความปลอดภัยเพียงบางประเด็นที่ critical (เฉพาะส่วนของการส่งผ่านข้อมูลเป็นสำคัญ) เท่านั้น
- แบบประเมินใช้งานค่อนข้างลำบาก

- คงไม่มีข้อเสนอแนะอะไรเป็นพิเศษ เนื่องจากความรู้ในด้านนี้มีจำกัด แต่จากที่ตอบแบบสอบถามมาทำให้เห็นและคำนึงถึงความสำคัญของความมั่นคงและความปลอดภัยของ WS มากยิ่งขึ้น และเห็นว่าการมี Model สำหรับประเมินความมั่นคงและความปลอดภัยของ WS ที่สร้างขึ้นอย่างเป็นรูปธรรม แสดงเป็นตัวเลขและเกณฑ์ที่ชัดเจน จะช่วยให้องค์กรที่พัฒนาหรือใช้งาน WS อยู่ได้ประโยชน์เป็นอย่างมาก
- เนื่องจากข้อมูลแบบสอบถามเป็นข้อมูลเชิงลึก และการทำงานจริงอาจจะไม่ทราบเกี่ยวกับคำศัพท์และเทคนิคต่างๆได้มากนัก จึงไม่สามารถตอบได้ตรงตามเป้าหมาย 100% ได้
- ควรมีเอกสารเพื่อให้ความรู้กับผู้ทำแบบสอบถามก่อน เนื่องจากว่าหากผู้ทำไม่มีความรู้ทางด้าน Web Service อย่างชำนาญจะไม่สามารถทำแบบสอบถามได้เลย
- น่าจะเพิ่มการวิจัยถึง Web Services ชนิดอื่น ๆ ด้วย
- Should try to explain your research in different way such as video streaming, voice streaming. It would help to clearify some other persons who hardly understand the complex information.
- ถ้าทำเป็น model หรือ tool ในการตรวจสอบ อย่าง Microsoft threathen model จะเป็นประโยชน์อย่างมาก
- เป็นงานวิจัยที่มีประโยชน์ และควรต่อยอดในรูปแบบของเครื่องมือซึ่งผู้ใช้สามารถใส่ค่าพารามิเตอร์ต่างๆ และคำนวณ score ออกมาได้เลย และเมื่อผลลัพธ์ออกมาในเชิงลบ เช่น Very Low ควรจะมีคำแนะนำที่สามารถนำไปใช้งานเพื่อเพิ่มความปลอดภัยได้
- บางข้อไม่ทราบ เพราะไม่ได้อยู่ในหน่วยงานที่ดูแลด้านนี้โดยตรง ทำให้อาจจะใส่ค่าข้อมูลไม่ถูกต้อง
- รายการใน questionaire1 ที่สรุปมามีอยู่ 18 หัวข้อ ถ้าสามารถจัดกลุ่มตามมุมมองของระบบได้ จะทำให้ทำแบบทดสอบได้ง่ายกว่านี้ เช่น แบ่งตามภาพรวมระบบเป็นส่วนต่าง ๆและระบุ countermeasure ในแต่ละส่วน จะทำให้ผู้ตอบแบบสอบถามเห็นภาพชัดเจน และตามคำถามได้ง่ายขึ้น แทนที่จะเรียงตามประเภท countermeasure ซึ่งไม่ค่อยมีลำดับความเกี่ยวเนื่องกัน และลองตรวจสอบรายการ

countermeasure และ attack เพิ่มเติมจาก http://msdn.microsoft.com/en-us/library/ff650168.aspx และ http://www.ijcttjournal.org/volume-1/issue-1/ijcttjournal-v1i1p27.pdf

- เนื่องจาก WS ที่พัฒนาขึ้นในปัจจุบันนั้นมีการนำไปใช้หลากหลายแบบทั้งในลักษณะภายในองค์กร ภายนอกองค์กร ใน network เดียวกัน หรือผ่าน Internet และตาม Business Model (เช่น B2B B2C C2B C2C) เป็นต้น ซึ่งการคำนึงถึงความมั่นคงนั้นก็แตกต่างกันไป เนื่องจากโอกาสการถูกโจมตี (Attack) ในลักษณะต่างๆ นั้นก็แตกต่างกันออกไป รวมถึงวิธีการรับมือก็มีข้อกำหนด ข้อจำกัดที่แตกต่างกัน ไปตามลักษณะที่กล่าวข้างต้น ซึ่งจะเป็นผลให้การใช้ Model ของงานวิจัยนี้วัดผลได้ไม่เป็นไปตามความเป็นจริงนัก ถ้าเป็นไปได้ ผู้วิจัยสามารถเพิ่มลักษณะดังกล่าวที่เป็นตัวชี้วัดถึงข้อจำกัด ข้อกำหนด ต่อโอกาสที่จะถูกโจมตีหรือความสามารถในการรับมือ เป็นตัวแปรหนึ่งที่เป็นอินพุทของ Model ที่ใช้คิดคะแนนก็น่าจะทำให้ได้ผลที่เป็นจริงต่อลักษณะของการใช้งาน WS ต่างๆ มากยิ่งขึ้น
- อยากให้นำเสนอเครื่องมือที่มาช่วยสนับสนุนในแนวคิดนี้ว่าเมื่อนำไปใช้งานจริงจะได้ผลลัพธ์ตามสมติฐานหรือไม่ แต่ควรที่จะนำไปทดลองใช้ในหลายๆธุรกิจ เพื่อให้ครอบคลุมและมั่นใจได้ว่าสามารถนำไปก่อให้เกิดประโยชน์ได้

ประวัติผู้เขียนวิทยานิพนธ์

นายทศพล บ้านคลองสี่ เกิดเมื่อวันที่ 9 กันยายน พ.ศ. 2528 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาระดับปริญญาวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์ เกียรตินิยมอันดับหนึ่ง จากคณะวิศวกรรมศาสตร์ มหาวิทยาลัยกรุงเทพ ในปีการศึกษา 2549 และเข้าทำงานเป็นอาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยกรุงเทพ ในปีการศึกษา 2550 จากนั้นเข้าศึกษาต่อในหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์ ณ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2552 ปัจจุบันเป็นอาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยกรุงเทพ