ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์
ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

โดยที่เป็นการสมควรยกเลิกประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ เลขที่ ขมธอ. ๑-๒๕๕๗ เวอร์ชัน ๑.๐ ลงวันที่ ๓๐ กันยายน พ.ศ. ๒๕๕๗ เพื่อให้ผู้ที่เกี่ยวข้องกับการบริหารจัดการและดูแลเว็บไซต์ถือปฏิบัติตามแนวทางการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามข้อกำหนดของพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

อาศัยอำนาจตามความในมาตรา ๕ (๔) และมาตรา ๒๔ ของพระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๒ จึงให้ยกเลิกประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ เลขที่ ขมธอ. ๑-๒๕๕๗ เวอร์ชัน ๑.๐ ปรากฏตามท้ายประกาศฉบับนี้

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๑ พฤษภาคม พ.ศ. ๒๕๖๖

(นายศักดิ์ เสกขุนทด)
รองผู้อำนวยการฯ ปฏิบัติการแทนผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard for Electronic Transactions

ขมธอ.1 – 2557

ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

Website Security Standard

เวอร์ชั่น 1.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์
ว่าด้วย
มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

ขมธอ.1 – 2557

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21

เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310

www.etda.or.th

โทรศัพท์ 0 2123 1234

ประกาศโดย

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

วันที่ 30 กันยายน พ.ศ. 2557

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ฉบับนี้ จัดทำขึ้นเพื่อเป็นแนวทางและข้อกำหนดสำหรับการรักษาความมั่นคงปลอดภัยของเว็บไซต์ โดยเน้นไปที่การรักษาความมั่นคงปลอดภัยของเครื่องบริการเว็บในส่วนของโปรแกรมสำหรับให้บริการเว็บ (Web Server Software) ระบบบริหารจัดการเว็บไซต์ (Content Management System: CMS) ระบบฐานข้อมูล (Database System) และโปรแกรมประยุกต์บนเว็บ (Web Application) เพื่อลดความเสี่ยงจากการโจมตีเว็บไซต์และทำให้ผู้ที่เกี่ยวข้องมีวิธีการรับมือและจัดการกับปัญหาที่เกิดขึ้นภายใต้มาตรฐานที่ยอมรับได้ โดยพัฒนาตามแนวมาตรฐานของ

- NIST SP 800-44 Guidelines on Securing Public Web Servers
- OWASP Open Web Application Security Project
- ข้อกำหนดที่เกี่ยวข้องจากข้อแนะนำแก้ไขและป้องกันข้อบกพร่องหรือจุดอ่อนของเว็บไซต์ ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือไทยเซิร์ต (ThaiCERT)
- คู่มือ “How to Secure Your Website” ของ สำนักงานส่งเสริมเทคโนโลยีสารสนเทศ ประเทศญี่ปุ่น (Information-Technology Promotion Agency (IPA), Japan)

และได้มีการนำเสนอเพื่อรับฟังความคิดเห็นเป็นการทั่วไป เพื่อนำข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อให้ข้อเสนอแนะเกี่ยวกับมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วน และสามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ฉบับนี้ จัดทำโดยสำนักมาตรฐาน ร่วมกับสำนักความมั่นคงปลอดภัย ภายใต้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น ๒๑ เลขที่ ๓๓/๔ ถนนพระราม ๙
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร ๑๐๓๑๐
โทรศัพท์ ๐ ๒๑๒๓ ๑๒๓๔ โทรสาร ๐ ๒๑๒๓ ๑๒๐๐
E-mail: estandard.center@etda.or.th www.etda.or.th

สารบัญ

สารบัญรูป

หน้า

สารบัญตาราง

หน้า

ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์
ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

เพื่อส่งเสริมให้ผู้ที่เกี่ยวข้องกับการบริหารจัดการและดูแลเว็บไซต์สามารถพัฒนาหรือจัดทำเว็บไซต์ให้มีความมั่นคงปลอดภัย และดำเนินมาตรการในการป้องกัน ตรวจสอบ ลดความเสี่ยง หรือสามารถรับมือกับภัยคุกคามที่มีต่อเว็บไซต์ เพื่อสร้างความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์

อาศัยอำนาจตามความในมาตรา ๗ (๔) และมาตรา ๒๗ (๓) แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. ๒๕๕๔ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) จึงประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ เลขที่ ขมธอ. ๑-๒๕๕๗ ปรากฏตามท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ 30 กันยายน พ.ศ. ๒๕๕๗

(นางสุรางคณา วายุภาพ)

ผู้อำนวยการ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วย มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

บทนำ

ภัยคุกคามด้านสารสนเทศซึ่งอาจเป็นการโจมตีเพื่อเปลี่ยนแปลงข้อมูลหน้าเว็บ (Web Defacement) การโจมตีเพื่อขโมยข้อมูลสำคัญ การโจมตีเพื่อใช้เป็นฐานในการเผยแพร่มัลแวร์ (Malware URL) หรือใช้เป็นฐานในการฉ้อโกงทางการเงินผ่านหน้าเว็บไซต์หลอกลวง (Phishing Website) ภัยคุกคามเหล่านี้ล้วนก่อให้เกิดความเสียหายแก่ชื่อเสียงของหน่วยงานที่เป็นเจ้าของเว็บไซต์ ความน่าเชื่อถือของธุรกิจ และยังอาจเป็นอันตรายต่อความมั่นคงปลอดภัยต่อองค์กรหรือในระดับประเทศ ถ้าเว็บไซต์ที่ถูกเจาะระบบ หรือถูกโจมตี หรือใช้เป็นฐานในการเผยแพร่มัลแวร์เพื่อโจมตีผู้ใช้บริการเว็บไซต์ ซึ่งส่วนใหญ่ล้วนอาศัยช่องโหว่ (Vulnerability) ของซอฟต์แวร์ที่มีอยู่ในหลายส่วนของเว็บไซต์ ได้แก่ ช่องโหว่ของเครื่องบริการเว็บ (Web Server) ช่องโหว่ของโปรแกรมประยุกต์บนเว็บ (Web Application) และช่องโหว่ที่เกิดจากการบริหารจัดการดูแลเว็บที่ไม่ได้มาตรฐานซึ่งยอมรับได้

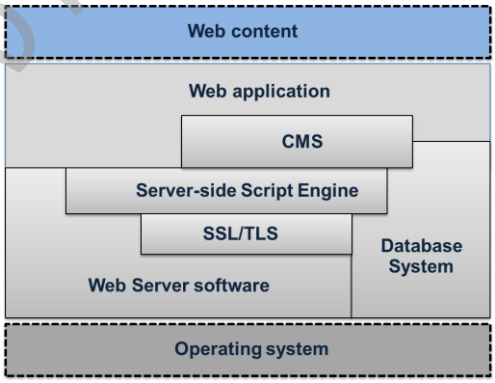
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ได้เห็นถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของเว็บไซต์ โดยในมาตรฐานฉบับนี้จะเน้นไปที่การรักษาความมั่นคงปลอดภัยของเว็บไซต์มีจุดมุ่งหมายให้ผู้ที่เกี่ยวข้องกับการบริหารจัดการและดูแลเว็บไซต์สามารถดำเนินมาตรการในการ จัดทำเว็บไซต์และเพื่อป้องกัน ตรวจสอบ และรับมือกับการโจมตี รวมทั้งลดความเสี่ยงที่อาจถูกโจมตีภายใต้มาตรฐานหรือแนวปฏิบัติอันยอมรับได้ ด้วยเหตุนี้ สพธอ. จึงได้จัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ เพื่อใช้เป็นข้อกำหนดและเป็นแนวทางในการจัดทำและพัฒนาเว็บไซต์เพื่อลดความเสี่ยงจากการถูกโจมตีผ่านทางช่องโหว่ต่าง ๆ ของเว็บไซต์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วย มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

1. ขอบเขต

มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ฉบับนี้ เป็นแนวทางและข้อกำหนดสำหรับการรักษาความมั่นคงปลอดภัยของเว็บไซต์ โดยขอบเขตของแนวทางและข้อกำหนดในมาตรฐานฉบับนี้จะเน้นไปที่การรักษาความมั่นคงปลอดภัยของเครื่องบริการเว็บในส่วนของโปรแกรมสำหรับให้บริการเว็บ (Web Server Software) ระบบบริหารจัดการเว็บไซต์ (Content Management System: CMS) ระบบฐานข้อมูล (Database System) และโปรแกรมประยุกต์บนเว็บ (Web Application) เพื่อลดความเสี่ยงจากการโจมตีเว็บไซต์ และทำให้ผู้ที่เกี่ยวข้องมีแนวทางในการรับมือและสามารถจัดการกับปัญหาที่เกิดขึ้นได้อย่างเป็นมาตรฐาน อย่างไรก็ตาม มาตรฐานฉบับนี้เป็นเพียงข้อเสนอแนะ เพื่อลดความเสี่ยงจากการถูกโจมตีทางเทคโนโลยีสารสนเทศและการสื่อสาร หรือทางออนไลน์เท่านั้น ทั้งนี้ การทำให้เว็บไซต์มีความมั่นคงปลอดภัยนั้น ยังจำเป็นต้องอาศัยความเข้มแข็งในการบริหารจัดการและการดูแล การดำเนินการตามข้อเสนอแนะมาตรฐานนี้ยังมิได้เป็นสิ่งที่รับรองว่าเว็บไซต์ มีความมั่นคงปลอดภัยโดยสิ้นเชิงจากการโจมตี หรือการบุกรุกระบบ หรือขาดความเข้มแข็งในการบริหารจัดการเว็บไซต์ในทางปฏิบัติ หรือมีภัยคุกคามในรูปแบบที่ไม่เคยเกิดขึ้นมาก่อน (Zero Day Attack) หรือถูกโจมตี เพื่อเข้ามาในระบบโดยไม่ได้รับอนุญาตหรือโดยมิชอบ (Unauthorized Access) เป็นต้น



ภาพที่ 1 ขอบเขตของมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (ส่วนที่เป็นเส้นทึบ)

มาตรฐานฉบับนี้มุ่งหมายให้ผู้ที่เกี่ยวข้องกับเว็บไซต์มีแนวทางในการจัดทำเว็บไซต์และบริหารจัดการ ป้องกัน ตรวจสอบ และรับมือกับการโจมตีที่เกิดขึ้นกับเว็บไซต์ โดยมีผู้ดูแลเครื่องบริการเว็บ (Web Server Administrator) ทำหน้าที่ดูแลรับผิดชอบ โปรแกรมสำหรับให้บริการเว็บ ระบบบริหารจัดการเว็บไซต์ ระบบฐานข้อมูล และการดำเนินกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับเครื่องบริการเว็บ เช่น การติดตั้งและการตั้งค่าที่เกี่ยวข้องกับโปรแกรมสำหรับให้บริการเว็บ ระบบบริหารจัดการเว็บไซต์ และระบบฐานข้อมูล ให้มีความมั่นคงปลอดภัย รวมถึงการรับมือเหตุภัยคุกคามที่เกิดจากการโจมตีเว็บไซต์ ในขณะที่ผู้พัฒนาโปรแกรมประยุกต์บนเว็บ (Web Application Developer) มีหน้าที่ในการ

พัฒนาโปรแกรมประยุกต์บนเว็บ ปรับปรุงและแก้ไขส่วนประกอบของโปรแกรมประยุกต์บนเว็บให้มีความมั่นคงปลอดภัย

มาตรฐานฉบับนี้อ้างอิงข้อกำหนดและแนวทางที่เกี่ยวข้องกับการวางแผนเพื่อบริหารจัดการเว็บไซต์ การติดตั้งและการตั้งค่าที่เกี่ยวข้องกับเครื่องบริการเว็บ การสำรองข้อมูลเว็บไซต์ และการรับมือสถานการณ์ภัยคุกคามที่เกิดกับเว็บไซต์จากมาตรฐาน NIST SP 800-44 Version 2. Guidelines on Securing Public Web Servers [1] และในส่วนของการพัฒนาโปรแกรมประยุกต์บนเว็บอย่างมั่นคงปลอดภัยนั้นได้อ้างอิงข้อกำหนดที่เกี่ยวข้องจากข้อแนะนำแก้ไขและป้องกันข้อบกพร่องหรือจุดอ่อนของเว็บไซต์ ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือไทยเซิร์ต (ThaiCERT) และ แนวทางการพัฒนาโปรแกรมประยุกต์บนเว็บที่มั่นคงปลอดภัยจาก Open Web Application Security Project (OWASP) Foundation และ คู่มือ “How to Secure Your Website” ของ สำนักงานส่งเสริมเทคโนโลยีสารสนเทศ ประเทศญี่ปุ่น (Information-Technology Promotion Agency (IPA), Japan)

2. การนำไปใช้งาน

ในปัจจุบันหน่วยงานต่าง ๆ ใช้เว็บไซต์ เป็นเครื่องมือในการเผยแพร่ประชาสัมพันธ์ข่าวสารและติดต่อกับลูกค้าเพื่อดำเนินกิจกรรมทางธุรกิจ ด้วยเหตุนี้เว็บไซต์จึงเป็นเป้าหมายหนึ่งที่ถูกคุกคามด้านสารสนเทศมากที่สุด โดยเฉพาะเว็บไซต์ที่มีชื่อเสียง หรือเว็บไซต์ที่มีช่องโหว่ มักมีความเสี่ยงที่จะตกเป็นเป้าหมายการโจมตีจากผู้ประสงค์ร้ายอยู่เสมอ โดยอาจเป็นการโจมตีเพื่อเปลี่ยนแปลงข้อมูลหน้าเว็บ (Web Defacement) การโจมตีเพื่อขโมยข้อมูลสำคัญ การโจมตีเพื่อใช้เป็นฐานในการเผยแพร่มัลแวร์ (Malware URL) หรือใช้เป็นฐานในการฉ้อโกงทางการเงินผ่านหน้าเว็บไซต์หลอกลวง (Phishing Website) ภัยคุกคามเหล่านี้ล้วนก่อให้เกิดผลกระทบต่อความน่าเชื่อถือของเว็บไซต์ การโจมตีเว็บไซต์ดังที่กล่าวมาแล้ว ส่วนใหญ่ล้วนอาศัยช่องโหว่ของระบบหรือโปรแกรมประยุกต์ที่เกี่ยวข้องกับเว็บไซต์ เช่น โปรแกรมสำหรับให้บริการเว็บ (Web Server Software) ระบบบริหารจัดการเว็บไซต์ (Content Management System: CMS) ระบบฐานข้อมูล (Database System) และโปรแกรมประยุกต์บนเว็บ (Web Application)

ข้อกำหนดและแนวทาง (Clauses and Guidelines) ในมาตรฐานฉบับนี้จัดทำขึ้นสำหรับการบริหารจัดการความมั่นคงปลอดภัยของเครื่องบริการเว็บและโปรแกรมประยุกต์บนเว็บ โดยเสนอแนะแนวทางและข้อกำหนดที่เกี่ยวข้องเพื่อป้องกันการโจมตีและแก้ไขช่องโหว่ที่เกี่ยวข้องกับเว็บไซต์ โดยข้อกำหนดและแนวทางในมาตรฐานฉบับนี้ถูกแบ่งออกเป็นสี่หมวดซึ่งได้แก่ การวางแผน (Planning) การติดตั้งและการตั้งค่าที่เกี่ยวข้องกับเว็บไซต์ (Installation and Configuration) การพัฒนาโปรแกรมประยุกต์บนเว็บอย่างมั่นคงปลอดภัย และการรับมือเหตุภัยคุกคามที่เกิดกับเว็บไซต์ (Security Incident Handling) ซึ่งมีรายละเอียดดังนี้

(1) การวางแผน (Planning) ประกอบด้วยแนวทางในการวางแผนบริหารจัดการเว็บไซต์ ซึ่งได้แก่ การวางแผนด้านความมั่นคงปลอดภัยของเว็บไซต์ แนวทางการเลือกผู้รับจดทะเบียนชื่อโดเมน แนวทางการเลือกผู้ให้บริการเว็บโฮสติ้ง และ แนวทางในการเลือกใช้ระบบบริหารจัดการเว็บไซต์ (Content Management System: CMS)

(2) การติดตั้งและการตั้งค่าที่เกี่ยวข้องกับเว็บไซต์ (Installation and Configuration) เป็นข้อกำหนดที่มุ่งเน้นให้มีการติดตั้งและการตั้งค่าของ โปรแกรมสำหรับให้บริการเว็บ ระบบบริหารจัดการเว็บไซต์ ระบบฐานข้อมูล และ Server-Side Script Engine รวมถึงแนวทางการกำหนดรหัสผ่านที่มั่นคงปลอดภัย

(3) การพัฒนาโปรแกรมประยุกต์บนเว็บอย่างมั่นคงปลอดภัย ซึ่งข้อกำหนดในส่วนนี้เน้นการป้องกันการโจมตีด้วยเทคนิคต่าง ๆ ที่พบบ่อยจากรายงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือไทยเซิร์ต (ThaiCERT) แนวทางการป้องกันจากเอกสารของ IPA และ OWASP

(4) การรับมือเหตุภัยคุกคาม (Security Incident Handling) เป็นข้อกำหนดที่มุ่งเน้นให้ผู้ดูแลเครื่องบริการเว็บสามารถรับมือกับเหตุภัยคุกคามด้านความมั่นคงปลอดภัยที่เกิดขึ้นกับเว็บไซต์ ได้แก่ กรณีเว็บไซต์ถูกบุกรุกและควบคุม (Intrusions) กรณีการถูกโจมตีในลักษณะ (Denial of Services: DoS) และ กรณีโดเมนถูกขโมย (Domain Hijack) เป็นต้น

มาตรฐานฉบับนี้เป็นแนวทางและข้อกำหนดสำหรับการรักษาความมั่นคงปลอดภัยของเว็บไซต์เพื่อลดความเสี่ยงจากการโจมตีเว็บไซต์ และทำให้ผู้ที่เกี่ยวข้องมีแนวทางในการรับมือและสามารถจัดการกับปัญหาที่เกิดขึ้นได้ โดยผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ สามารถใช้ตัวอย่างของแบบประเมินเพื่อตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์ที่อยู่ในภาคผนวก ก. มาประยุกต์ใช้ได้กับเว็บไซต์ทั่วไปตามแนวทางและข้อกำหนดในมาตรฐานฉบับนี้ นอกจากนี้ผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บยังสามารถใช้มาตรฐานฉบับนี้เพื่อแสดงความสอดคล้องกับข้อกำหนดและแนวทางที่เกี่ยวข้องโดย

(1) ประเมินตนเอง (Self-Assessment) และประกาศการรับรองตนเอง (Self-Declaration) ว่าได้มีการดำเนินการตามข้อเสนอแนะฉบับนี้

(2) ยืนยันถึงความสอดคล้องกับมาตรฐานจากผู้มีส่วนได้ส่วนเสียกับเว็บไซต์

(3) ยืนยันถึงการประกาศรับรองตนเองจากหน่วยงานภายนอก

(4) ขอรับการรับรอง (Certification) มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับผู้ดูแลและพัฒนาเว็บไซต์จากหน่วยตรวจสอบและรับรอง (Conformity Assessment Body)

ข้อกำหนดในมาตรฐานฉบับนี้สามารถนำไปใช้ได้กับเว็บไซต์ทั่วไปที่อยู่บนเครื่องบริการเว็บส่วนตัว (Private Web Server) หรือ เว็บไซต์ที่ใช้บริการกับผู้ให้บริการเว็บโฮสติ้ง หรือ เว็บไซต์ที่ใช้บริการระบบ Cloud

3. นิยาม

คำนิยามของศัพท์ที่ใช้กับมาตรฐานฉบับนี้

3.1. เว็บเพจ (Web Page)[2] หมายถึง เอกสารเว็บที่สร้างด้วยภาษา HTML หรือ HyperText Markup Language ซึ่งเป็นภาษามาตรฐานที่ใช้ในการสร้างเว็บเพจ

[2] ศัพท์บัญญัติราชบัณฑิตยสถาน

3.2. เว็บไซต์ (Website)[1] หมายถึง กลุ่มของเว็บเพจที่อยู่บนเครื่องบริการเว็บ (Web Server) ซึ่งมียูอาร์แอลกำกับอยู่

3.3. ยูอาร์แอล (Universal Resource Locator: URL) [1] หมายถึง ตัวชี้แหล่งในอินเทอร์เน็ตซึ่งประกอบด้วยชื่อโพรโทคอลที่ใช้ในการเข้าถึงข้อมูล (เช่น http://) และ ชื่อโดเมน (เช่น www.etda.or.th) ที่กำกับเครื่องบริการเว็บ

3.4. เวิลด์ไวด์เว็บ (WWW) [1] หมายถึง กลุ่มของเว็บไซต์หรือเครื่องคอมพิวเตอร์ที่มีข้อมูลพร้อมไว้ให้ผู้ใช้บริการเรียกดูข้อมูลผ่านโพรโทคอลเอชทีทีพี (HTTP หรือ Hypertext Transfer Protocol)

3.5. เครื่องบริการเว็บ (Web Server) [1] หมายถึง เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นเครื่องบริการ (Server) พร้อมกับโปรแกรมที่ให้บริการข้อมูลเว็บผ่านเครือข่ายเวิลด์ไวด์เว็บ

3.6. โปรแกรมสำหรับให้บริการเว็บ (Web Sever Software) หมายถึง โปรแกรมที่ติดตั้งบนเครื่องบริการ (Server) เพื่อทำให้เครื่องบริการสามารถให้บริการข้อมูลเว็บได้ เช่น โปรแกรม Apache และ โปรแกรม Internet Information Service (IIS) for Window Server เป็น

3.7. โปรแกรมค้นดูเว็บ (Web Browser) [1] หมายถึง โปรแกรมที่ใช้เรียกข้อมูลเว็บจากเครื่องบริการเว็บผ่านเครือข่ายเวิลด์ไวด์เว็บ

3.8. โปรแกรมประยุกต์บนเว็บ (Web Application)[1] หมายถึง โปรแกรมประยุกต์ที่ถูกพัฒนาขึ้นสำหรับการเรียกใช้งานและเข้าถึงได้โดยโปรแกรมค้นดูเว็บผ่านเครือข่ายคอมพิวเตอร์ เช่น เครือข่ายอินเทอร์เน็ตหรือเครือข่ายอินทราเน็ต เป็นต้น

3.9. ระบบบริหารจัดการเว็บไซต์ (Content Management System: CMS)[3] หมายถึง โปรแกรมที่ผู้ดูแลเครื่องบริการเว็บสามารถใช้ในการดูแลบริหารจัดการเว็บไซต์ผ่านส่วนต่อประสาน (Interface) ซึ่งช่วยให้ง่ายต่อการบริหารจัดการเว็บเพจและการปรับปรุงค่าติดตั้งต่าง ๆ ที่เกี่ยวข้อง

4. การวางแผนเพื่อบริหารจัดการเว็บไซต์

องค์ประกอบของเว็บไซต์โดยทั่วไปจะประกอบด้วย เครื่องบริการเว็บ (Web Server) โปรแกรมประยุกต์บนเว็บ (Web Application) และ ข้อมูลบนเว็บหรือเว็บเพจ ที่อยู่ภายใต้การควบคุมดูแลเดียวกัน การวางแผนบริหารจัดการเว็บไซต์ให้มีความมั่นคงปลอดภัยเป็นกระบวนการที่มีความสำคัญ เนื่องจากเว็บไซต์ที่ขาดการวางแผนที่เหมาะสมมักจะมีค่าใช้จ่ายที่สูงในการแก้ไขปัญหาด้านความมั่นคงปลอดภัยและมีความเสี่ยงที่จะทำให้เกิดผลกระทบกับองค์ประกอบส่วนต่าง ๆ ของเว็บไซต์ ด้วยเหตุนี้การวางแผนเพื่อบริหารจัดการเว็บไซต์จะช่วยให้ผู้ที่เกี่ยวข้องสามารถบริหารจัดการเว็บไซต์ให้มีความมั่นคงปลอดภัยด้วยเงินลงทุนที่เหมาะสมและสอดคล้องกับความต้องการทางธุรกิจ ในการวางแผนผู้ดูแลเครื่องบริการเว็บจะต้องศึกษาข้อมูลที่เกี่ยวข้องตั้งแต่ การวางแผนด้านความมั่นคงปลอดภัยของเว็บไซต์ การจดทะเบียนชื่อโดเมน การเลือกผู้ให้บริการเว็บโฮสติ้ง (Web Hosting Service Provider) และการเลือกระบบบริหารจัดการเว็บไซต์ที่มั่นคงปลอดภัย เพื่อวางรากฐานด้านความมั่นคงปลอดภัยให้กับเว็บไซต์ก่อนที่จะเปิดให้บริการ

[3] คลังศัพท์ไทย สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

4.1 การวางแผนด้านความมั่นคงปลอดภัยของเว็บไซต์

การวางแผนด้านความมั่นคงปลอดภัยของเว็บไซต์ มีหลักเกณฑ์ที่ใช้สำหรับการพิจารณาเพื่อจัดทำแผนซึ่งได้แก่ การวางแผนเพื่อบริหารจัดการเครื่องบริการเว็บ ภัยคุกคาม (Threat) ที่เกี่ยวข้อง และการวางมาตรการ (Measure) เพื่อป้องกันภัยคุกคามที่มีความสำคัญ มาตรฐานฉบับนี้มีแนวทางในการจัดทำแผนด้านความมั่นคงปลอดภัยของเว็บไซต์ดังต่อไปนี้

(1) การวางแผนเพื่อบริหารจัดการเครื่องบริการเว็บ

ก่อนที่จะมีการจัดทำเว็บไซต์ การสำรวจความต้องการทางธุรกิจหรือความต้องการของผู้ใช้บริการเป็นข้อมูลที่สำคัญสำหรับการวางแผนเพื่อบริหารจัดการเครื่องบริการเว็บ ซึ่งบอกได้ว่าการจัดทำเว็บไซต์มีจุดประสงค์เพื่ออะไร คุณสมบัติของเครื่องบริการเว็บเป็นอย่างไร ต้องใช้โปรแกรมประยุกต์บนเว็บสำหรับบริการด้านใดบ้าง มีการเก็บรักษาข้อมูลบนเว็บอย่างไร และการกำหนดหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้อง รวมถึงการใช้เทคโนโลยีที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยอย่างเหมาะสมเพื่อตอบสนองต่อความต้องการของธุรกิจและผู้ใช้บริการ ทั้งนี้ การวางแผนเพื่อบริหารจัดการเครื่องบริการเว็บสามารถนำแนวทางในหัวข้อที่ 3 “Planning and Managing Web Server” ของมาตรฐาน NIST SP 800-44 [2] มาใช้เป็นแนวทางในการจัดทำได้

(2) จัดลำดับความเสี่ยงของภัยคุกคามที่คาดว่าจะเกิดขึ้นกับเว็บไซต์

การจะจัดลำดับความเสี่ยงของภัยคุกคามที่คาดว่าจะเกิดขึ้นกับเว็บไซต์ได้นั้น ผู้ดูแลเครื่องบริการเว็บจะต้องมีการจัดทำรายการของสินทรัพย์ (Asset Inventory) ของเว็บไซต์ เช่น จำนวนเครื่องบริการเว็บ โปรแกรมประยุกต์บนเว็บ และข้อมูลบนเว็บหรือเว็บเพจที่เกี่ยวข้อง รวมถึงมูลค่าของสินทรัพย์ (Asset Value) และผู้รับผิดชอบที่เกี่ยวข้อง หลังจากนั้นก็จะต้องมีการระบุภัยคุกคาม (Threat) ความเป็นไปได้ที่คาดว่าน่าจะเกิดภัยคุกคามดังกล่าวขึ้น พร้อมกับผลกระทบ (Impact) ต่อสินทรัพย์ หากมีภัยคุกคามดังกล่าวเกิดขึ้น เพื่อนำมาเป็นข้อมูลในการจัดลำดับความเสี่ยงของภัยคุกคามที่จะต้องมีการวางมาตรการป้องกันต่อไป ทั้งนี้ วิธีการและขั้นตอนของการประเมินความเสี่ยงสามารถนำขั้นตอนที่กำหนดไว้ในมาตรฐาน ISO/IEC 27005:2011 มาใช้อ้างอิงได้

(3) กำหนดมาตรการที่เกี่ยวข้องเพื่อป้องกันภัยคุกคามที่มีความสำคัญ

การจัดลำดับความเสี่ยงของภัยคุกคามทำให้สามารถเลือกใช้มาตรการเพื่อป้องกันหรือลดความเสี่ยงจากภัยคุกคามที่มีความสำคัญโดยมีค่าใช้จ่ายที่เหมาะสม ไม่ว่าจะเป็นเรื่องของการเตรียมความพร้อมให้กับบุคคลที่เกี่ยวข้อง การเลือกใช้เทคโนโลยีและมาตรฐานด้านความมั่นคงปลอดภัยที่เหมาะกับภัยคุกคามและสามารถขยายขอบเขตการรักษาความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพในกรณีที่เว็บไซต์มีผู้ใช้บริการมากขึ้น ทั้งนี้การเลือกหรือกำหนดมาตรการที่เหมาะสมเพื่อป้องกันภัยคุกคามที่มีความสำคัญนั้นสามารถใช้แนวทางตามที่มาตรฐาน ISO/IEC 27002:2013 กำหนดไว้เป็นแนวทางได้

4.2 การเลือกผู้รับจดทะเบียนชื่อโดเมน

เครื่องบริการเว็บหรือเครื่องคอมพิวเตอร์ที่ให้บริการอยู่บนเครือข่ายอินเทอร์เน็ต ในความเป็นจริงจะถูกระบุด้วย หมายเลข IP (เช่น 165.134.170.27) แต่เนื่องจากคนเราสามารถจดจำ ชื่อได้ดีกว่าการจำตัวเลขยาว ๆ ยูอาร์แอล (URL: Universal Resource Locator) หรือ ตัวชี้แหล่งในอินเทอร์เน็ต จึงมีขึ้นเพื่ออำนวยความสะดวกในการอ้างถึงเครื่องบริการเว็บบนเครือข่ายอินเทอร์เน็ต โดยยูอาร์แอลจะมีความสัมพันธ์กับชื่อโดเมน เพราะชื่อโดเมนเป็นที่อยู่เป้าหมายและเป็นส่วนประกอบของยูอาร์แอล เช่น https://www.etda.or.th หรือ https://www.thaicert.or.th จะมีชื่อโดเมนที่มีการใช้คือ etda.or.th และ thaicert.or.th ตามลำดับ ดังนั้น ก่อนที่จะพัฒนาเว็บไซต์ ผู้ดูแลเครื่องบริการเว็บจึงมีความจำเป็นจะต้องจดทะเบียนชื่อโดเมนของเว็บไซต์ตนเองเสียก่อน ชื่อโดเมนจึงมีความสำคัญเป็นอันดับแรกสำหรับเว็บไซต์ โดยเฉพาะกับการโฆษณาประชาสัมพันธ์บนอินเทอร์เน็ต ถ้าได้ชื่อที่จดจำง่าย ตรงกับกลุ่มเป้าหมายที่มีความสนใจในบริการหรือสินค้าอยู่แล้วนั้น จะทำให้ชื่อโดเมน หรือ เว็บไซต์นั้น ๆ ได้รับความสนใจและเป็นที่จดจำได้ง่ายไม่เฉพาะลูกค้าของเว็บไซต์เท่านั้น แต่ยังรวมไปถึงโปรแกรมค้นหา (Search Engine) ชื่อดังต่าง ๆ ที่จะเข้ามาทำดัชนีการค้นหา (Index) ในเว็บเพจหน้าต่าง ๆ ของเว็บไซต์ เช่น Google Yahoo และ BING เป็นต้น หลายครั้งที่ชื่อโดเมนถูกแก้ไขให้ชี้ไปยังเว็บไซต์หลอกลวง และสาเหตุหนึ่งที่ทำให้เกิดเหตุการณ์นี้ขึ้นคือการเข้าถึงบัญชีที่ใช้จดทะเบียนชื่อโดเมนโดยไม่ได้รับอนุญาต ทำให้ผู้ประสงค์ร้ายสามารถเข้าไปเปลี่ยนแปลงการตั้งค่าของชื่อโดเมนเพื่อนำไปใช้ในทางที่ผิด ซึ่งปรากฏตามรายงานของ Security and Stability Advisory Committee (SSAC) [3] ดังนั้น มาตรฐานฉบับนี้มีแนวทางในการเลือกผู้รับจดทะเบียนชื่อโดเมนดังต่อไปนี้

(1) มีการยืนยันการลงทะเบียน โดยให้ผู้ขอจดทะเบียนยืนยันอีเมลของตนโดยการเข้าไปยังจุดเชื่อมโยงหลายมิติ (Hyperlink) บนเว็บเพจ ซึ่งระบุไว้ในอีเมลเปิดการใช้งาน (Activation Email) ที่ผู้รับจดทะเบียนส่งมา บริการจดทะเบียนสามารถเพิ่มมาตรการความมั่นคงปลอดภัยโดยใช้การติดต่อไปยังหมายเลขโทรศัพท์ของผู้ขอจดทะเบียน เพื่อบอกหมายเลขสำหรับยืนยันการลงทะเบียน (Confirmation Number) ให้ผู้ขอจดทะเบียนนำหมายเลขมากรอกในแบบฟอร์มบนเว็บเพจ เพื่อเปิดการใช้งานบัญชีหรืออนุญาตให้ทำธุรกรรมได้

(2) มีมาตรการในการเพิ่มความมั่นคงปลอดภัยให้กับรหัสผ่าน เช่น การกำหนดค่าเริ่มต้นของรหัสผ่านที่มีความซับซ้อนคาดเดาได้ยาก (Strong Password) ระบุความยาวขั้นต่ำของรหัสผ่าน และจำกัดอายุการใช้งาน เป็นต้น

(3) มีการแจ้งเตือนและการยืนยันการเปลี่ยนแปลงข้อมูลการลงทะเบียน ทั้งนี้ การเปลี่ยนแปลงข้อมูลต่าง ๆ ต้องมีการกำหนดขั้นตอนสำหรับการเปลี่ยนแปลงข้อมูลซึ่งต้องอาศัยการยืนยันจากหลายบุคคลที่เกี่ยวข้อง ซึ่งการยืนยันการเปลี่ยนแปลงลักษณะนี้จะช่วยป้องกันการเปลี่ยนแปลงจากผู้ประสงค์ร้ายที่อาจจะปลอมตัวเพื่อเข้ามาเอาข้อมูลจากบุคคลใดบุคคลหนึ่งได้

4.3 แนวทางการเลือกรูปแบบเครื่องบริการเว็บ

ผู้ให้บริการเว็บโฮสติ้ง มีส่วนสำคัญในด้านความมั่นคงปลอดภัยของเว็บไซต์ เนื่องจากในรูปแบบที่นิยมกระทำกันนั้น ผู้ให้บริการจะมีฐานะเป็นผู้ดูแลระบบปฏิบัติการ (Operating System) โปรแกรมสำหรับให้บริการเว็บ (Web Server Software) ระบบบริหารจัดการเว็บไซต์ (CMS) และซอฟต์แวร์ที่เกี่ยวข้องกับเครื่องบริการเว็บทั้งหมด ทั้งในการติดตั้ง ตั้งค่า และการปรับเวอร์ชั่นหรือปรับปรุงระบบ (Upgrade/Update) ซึ่งในบางครั้ง ช่องโหว่ก็อาจจะ

เกิดขึ้นมาจากข้อผิดพลาดของระบบปฏิบัติการ (Operating System) หรือ โปรแกรมสำหรับให้บริการเว็บ หรือระบบบริหารจัดการเว็บไซต์ ซึ่งบางครั้งการตั้งค่าบางอย่างผู้ใช้บริการไม่สามารถแก้ไขปรับปรุงได้เอง

มาตรฐานฉบับนี้มีแนวทางในการพิจารณาเลือกผู้ให้บริการเว็บโฮสติ้ง ดังต่อไปนี้

(1) พิจารณาเลือกรูปแบบการให้บริการระหว่าง Shared หรือ Dedicated

รูปแบบการให้บริการเว็บโฮสติ้งนั้นมีหลายรูปแบบไม่ว่าจะเป็นการให้บริการแบบ Shared หรือ Dedicated ซึ่งรูปแบบการให้บริการนั้นมีข้อแตกต่างกันทั้งในเรื่องของต้นทุนค่าใช้จ่ายและสภาพแวดล้อมที่มีผลกระทบต่อความมั่นคงปลอดภัยของเว็บไซต์ การให้บริการแบบ Shared มีค่าใช้จ่ายที่ต่ำเนื่องจากเป็นการใช้เครื่องบริการเว็บร่วมกันระหว่างผู้ใช้บริการหลาย ๆ ราย โดยมักไม่ได้มีการแบ่งแยกสิทธิ์การเข้าถึงระหว่างโปรแกรมประยุกต์ของผู้ใช้บริการแต่ละราย ดังนั้น หากเว็บไซต์ของผู้ใช้บริการรายใดรายหนึ่งมีช่องโหว่ผู้ประสงค์ร้ายก็อาจอาศัยช่องโหว่นั้นในการเข้าโจมตีเว็บไซต์อื่น ๆ ที่อยู่ในเครื่องบริการเดียวกันได้ แม้ว่าจะเป็นเว็บไซต์ที่ไม่มีช่องโหว่เลยก็ตาม ส่วนรูปแบบ Dedicated นั้น ผู้ใช้บริการแต่ละรายจะได้เครื่องบริการเว็บแยกกันไปโดยเฉพาะ จึงทำให้มีค่าใช้จ่ายสูงกว่ามาก แต่ช่วยป้องกันความเสี่ยงจากการถูกโจมตีผ่านช่องโหว่ของเว็บไซต์อื่นได้ แต่รูปแบบการให้บริการดังกล่าวก็จะมีค่าใช้จ่ายที่สูงขึ้น ดังนั้นหากผู้ใช้บริการมีข้อจำกัดทางด้านต้นทุนและค่าใช้จ่ายก็มีความจำเป็นที่จะต้องรับทราบถึงความเสี่ยงด้านความมั่นคงปลอดภัยและเตรียมแนวทางการป้องกันหรือบรรเทาผลกระทบจากความเสี่ยงดังกล่าวไว้

(2) การพิจารณาจากรูปแบบนโยบายการจัดการช่องโหว่

เมื่อมีการค้นพบช่องโหว่ในซอฟต์แวร์ที่ใช้งานอยู่ในเครื่องบริการเว็บ ผู้ให้บริการจะต้องมีนโยบายที่ชัดเจนในการป้องกันความเสียหายที่อาจจะเกิดจากช่องโหว่นั้น ๆ เช่น การแจ้งให้ผู้ใช้บริการทราบในทันทีการ Patch หรือแก้ไขปัญหาเฉพาะหน้า (Workaround) ตามที่ผู้ผลิตซอฟต์แวร์ หรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยที่เชื่อถือได้แนะนำ ตลอดจนแผนสำรอง ในกรณีที่เป็นช่องโหว่ที่ไม่สามารถหาวิธีแก้ไข หรือป้องกันความเสียหายได้ในระยะเวลาสั้น ๆ โดยต้องพิจารณาทั้งผลที่คาดว่าจะได้รับ และระยะเวลาที่สามารถดำเนินการได้สำเร็จ ตลอดจนอาจต้องพิจารณาถึงความรับผิด (Liability) ที่ผู้ให้บริการอาจจะต้องชดเชยในกรณีที่เกิดความเสียหายแก่ผู้ใช้บริการในกรณีที่เกิดความบกพร่องในการจัดการกับช่องโหว่ด้วย

(3) รูปแบบการให้บริการโอนย้ายไฟล์ข้อมูล (Remote File Transfer)

ในการโอนย้ายไฟล์ข้อมูลระหว่างเครื่องของผู้ใช้บริการและเครื่องบริการเว็บ ผู้ให้บริการเว็บโฮสติ้งควรมีช่องทางการโอนย้ายไฟล์ที่มั่นคงปลอดภัยและมีการเข้ารหัสเพื่อรักษาความลับของข้อมูลระหว่างที่มีการโอนย้าย เช่น มีบริการ Secure Transfer Protocol (SFTP) สำหรับกระบวนการโอนย้ายไฟล์ เป็นต้น

(4) การให้บริการรูปแบบการสื่อสารอย่างมั่นคงปลอดภัยสำหรับเว็บไซต์ (บริการโพรโทคอล SSL/TLS)

บริการโพรโทคอล SSL (Secure Socket Layer Protocol) และ TLS (Transport Layer Security Protocol) เป็นโพรโทคอลที่กำหนดรูปแบบการสื่อสารที่มีความมั่นคงปลอดภัย (ดูรายละเอียดเพิ่มเติมใน

ภาคผนวก ข.) ซึ่งสามารถป้องกันการสื่อสารของโปรแกรมประยุกต์ในระบบรับ-ให้ (Client-Server System) จากการลอบฟัง (Eavesdropping) การแก้ไขให้เสียหาย (Tampering) และ การปลอมแปลงข้อความที่ใช้ในการสื่อสาร (Message Forgery) เว็บไซต์ที่ไม่ได้มีการนำ SSL/TLS มาใช้งาน จะเปิดโอกาสให้ผู้ประสงค์ร้ายสามารถลอบฟัง แก้ไขและปลอมแปลงข้อมูลที่ใช้รับ-ส่งระหว่างเครื่องบริการเว็บและผู้ใช้บริการได้ ในกรณีที่มีความจำเป็นต้องใช้งานบริการ SSL/TLS ผู้ใช้บริการควรตรวจสอบว่าผู้ให้บริการเว็บโฮสติ้ง มีการให้บริการ SSL/TLS หรือไม่ หากผู้ให้บริการสามารถให้บริการ SSL/TLS ผู้ใช้บริการก็จำเป็นจะขอใบรับรองอิเล็กทรอนิกส์ประเภทเว็บไซต์ หรือ SSL Certificate (ดูรายละเอียดเพิ่มในภาคผนวก ค.) จากผู้ให้บริการใบรับรองอิเล็กทรอนิกส์ที่น่าเชื่อถือ บริการ SSL/TLS จะเป็นเครื่องมือที่สำคัญในการรักษาความมั่นคงปลอดภัยของข้อมูลสำคัญ ๆ เช่น ข้อมูลลูกค้า ข้อมูลบัตรเครดิต ซึ่งมีการรับส่งกันระหว่างเครื่องของผู้ใช้บริการและเครื่องบริการเว็บ โดยเฉพาะผู้ใช้บริการที่ต้องการจะเปิดบริการเว็บไซต์สำหรับการทำพาณิชย์อิเล็กทรอนิกส์ (e-Commerce Website) หรือการทำธุรกรรมทางอิเล็กทรอนิกส์ของภาครัฐ

(5) การสำรองข้อมูลและการดูแลรักษาเครื่องบริการเว็บ

ผู้ให้บริการต้องมีการสำรองข้อมูลของเครื่องบริการเว็บที่อยู่ในความดูแลอย่างสม่ำเสมอ นอกจากนี้ผู้ให้บริการควรมีเครื่องมือให้กับผู้ใช้บริการสำหรับการสำรองข้อมูลของเว็บไซต์ด้วยตัวเอง ผู้ใช้บริการควรตรวจสอบนโยบายที่เกี่ยวข้องกับการสำรองและกู้คืนข้อมูลของผู้ให้บริการ วิธีการสำรองข้อมูลที่ผู้ให้บริการใช้และเครื่องมืออำนวยความสะดวกให้กับการสำรองและกู้คืนข้อมูล ว่ามีความเหมาะสมและสอดคล้องกับความต้องการใช้งานหรือไม่

(6) การติดต่อผู้ให้บริการเมื่อมีเหตุฉุกเฉิน

ผู้ให้บริการควรจะมีช่องทางติดต่อเฉพาะสำหรับกรณีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัย เพื่อใช้ในการประสานงานอย่างทันท่วงที ทั้งในกรณีที่ผู้ใช้บริการต้องการติดต่อเพื่อขอความช่วยเหลือ หรือกรณีที่มีหน่วยงานอื่นประสานเข้ามา การที่ผู้ให้บริการมีช่องทางติดต่อเฉพาะเกี่ยวกับเรื่องความมั่นคงปลอดภัย จะช่วยสะท้อนว่า ผู้ให้บริการมีความเอาใจใส่ต่อปัญหาด้านความมั่นคงปลอดภัยเป็นอย่างยิ่ง

4.4 แนวทางการเลือกระบบบริหารจัดการเว็บไซต์ (CMS)

การพัฒนาเว็บไซต์ของหน่วยงานของรัฐและเอกชนในปัจจุบัน เห็นได้ชัดว่ามีแนวโน้มของการนำระบบบริหารจัดการเว็บไซต์ มาใช้งานกันอย่างแพร่หลาย อาจเนื่องมาจากความสะดวกสบายของการพัฒนาและการบริหารจัดการเว็บไซต์ โดยรูปแบบของการพัฒนามีทั้งที่เป็นการนำ CMS ที่พัฒนาจากผู้พัฒนาในต่างประเทศ ซึ่งอนุญาตให้ผู้ใช้บริการทั่วโลกสามารถนำไปใช้งานต่อได้ฟรี หรืออีกประเภทหนึ่งคือเป็น CMS ที่พัฒนาโดยบริษัทในประเทศไทยและมีการคิดค่าบริการหรือลิขสิทธิ์ในการใช้งาน ซึ่งเป็นอีกทางเลือกหนึ่งของเทคโนโลยีการพัฒนาเว็บไซต์ โดยในปัจจุบันพบว่า ระบบบริหารจัดการเว็บไซต์ที่เป็นที่นิยมและมีผู้ใช้บริการมากที่สุดได้แก่ WordPress, Joomla, Drupal ตามลำดับ จากสถิติของ Google Trends [4] และจากสถิติเรื่องช่องโหว่ที่ National Vulnerability Database (NVD) ซึ่งเป็นองค์กรที่อยู่ภายใต้กำกับของ National Institute of Standards and Technology หรือ NIST [5] พบว่า CMS ที่มีความนิยมใช้กันมากก็จะมีรายงานช่องโหว่ของระบบมากเช่นกัน ถึงแม้ว่าการนำ ระบบบริหารจัดการเว็บไซต์ มาประยุกต์ใช้จะถือเป็นการตอบโจทย์หน่วยงานที่ต้องการให้การบริหารจัดการเว็บไซต์เป็นไป

ได้อย่างง่ายดาย และสามารถย่นระยะเวลาในการพัฒนาลง นำเวลาไปพัฒนาในส่วนของเนื้อหาให้มีความสมบูรณ์ได้ แต่เนื่องจาก CMS ที่เป็นที่นิยมมักเป็นระบบที่พัฒนาแบบโอเพนซอร์ส (Open Source) ซึ่งมีความเสี่ยงที่จะพบช่องโหว่ต่าง ๆ

มาตรฐานฉบับนี้มีแนวทางในการพิจารณาเลือกระบบบริหารจัดการเว็บไซต์ที่มีความมั่นคงปลอดภัยดังนี้

(1) พิจารณาจากตัวเลือกที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย

CMS ควรมีเอกสารแนะนำแนวทางการติดตั้งและการตั้งค่าเพื่อรักษาความมั่นคงปลอดภัย (Security Best Practice) และมี Plugin เสริมที่ติดตั้งให้เกิดความมั่นคงปลอดภัยตรงตามความต้องการของผู้ดูแลเครื่องบริการเว็บและผู้ใช้บริการ นอกจากตัวเลือกด้านความมั่นคงปลอดภัยแล้วยังมีปัจจัยอื่น ๆ ที่สามารถนำมาพิจารณาใช้เป็นแนวทางในการเลือก CMS ได้ โดยอ่านรายละเอียดเพิ่มเติมได้จาก “Choosing a CMS” [6] ของ GSA’s Office of Citizen Services and Innovative Technologies และ the Federal Web Managers Council

(2) พิจารณาจากคุณภาพของประชาคมนักพัฒนา CMS

ในกรณีของ CMS ที่เป็น Open Source ซึ่งต้องอาศัยประชาคมของนักพัฒนาในการปรับปรุง CMS ให้ดีขึ้น CMS ที่มีประชาคมนักพัฒนาที่มีขนาดใหญ่ มีการสื่อสารภายใน และพัฒนาอย่างต่อเนื่อง (Active Developer Community) จะเป็น CMS ที่มีฟังก์ชันการทำงานตอบสนองต่อความต้องการของผู้ใช้ได้มากกว่า รวมถึงการปรับเวอร์ชั่นหรือปรับปรุงระบบ เพื่อแก้ไขข้อบกพร่องและช่องโหว่ของ CMS ซึ่งสามารถสังเกตได้จากความถี่ของการปรับเวอร์ชั่นหรือปรับปรุงระบบ CMS เพื่อแก้ไขช่องโหว่ที่เกิดขึ้น หรือระยะเวลาใช้ในการพัฒนาตัวปรับรุ่น (Patch) เพื่อแก้ไขช่องโหว่ที่เกิดขึ้น

(3) พิจารณาจากแหล่งข้อมูลที่เกี่ยวกับการติดตั้ง การตั้งค่า และแนวทางการรักษาความมั่นคงปลอดภัย

CMS ที่ดีควรมีแหล่งข้อมูลและเอกสารสนับสนุนที่เกี่ยวข้องกับการติดตั้ง การตั้งค่า และแนวทางการรักษาความมั่นคงปลอดภัยให้กับ CMS

5. การตั้งค่าเครื่องบริการเว็บอย่างมั่นคงปลอดภัย

เมื่อมีการติดตั้งระบบปฏิบัติการ (Operating Software) ให้กับเครื่องบริการเว็บเรียบร้อยแล้วขั้นตอนต่อไปคือการติดตั้งโปรแกรมสำหรับให้บริการเว็บ (Web Server Software) ซึ่งมีผู้พัฒนาหลายรายและมีหลายรุ่น ด้วยเหตุนี้ก่อนการติดตั้งซอฟต์แวร์ดังกล่าว ผู้ดูแลเครื่องบริการเว็บควรศึกษารายละเอียดของคู่มือการติดตั้ง (Installation Guideline) และการตั้งค่าพารามิเตอร์ต่าง ๆ ที่เกี่ยวข้องเพื่อให้ซอฟต์แวร์ดังกล่าวสามารถทำงานได้ตามความต้องการของผู้ให้บริการและมีความมั่นคงปลอดภัย ซึ่งในมาตรฐานฉบับนี้จะกล่าวถึงข้อกำหนดที่เกี่ยวข้องการติดตั้ง (Installation) และการตั้งค่า (Configuration) ที่เกี่ยวข้องกับเครื่องบริการเว็บ โดยจะได้กล่าวถึงหัวข้อที่สำคัญ ๆ ได้แก่ การตั้งค่าโปรแกรมสำหรับบริการเว็บ การตั้งค่าระบบบริหารจัดการเว็บไซต์ การตั้งค่าฐานข้อมูล การตั้งค่า Server-Side Script Engine และ การกำหนดรหัสผ่านและรักษารหัสผ่านให้มีความมั่นคงปลอดภัย

5.1 การตั้งค่าโปรแกรมสำหรับให้บริการเว็บ (Web Server Software)

การติดตั้งและตั้งค่าโปรแกรมสำหรับให้บริการเว็บ (Web Server Software) ซึ่งเป็นโปรแกรมที่มีผู้พัฒนาหลายรายและมีหลายรุ่น ด้วยเหตุนี้ก่อนการติดตั้งโปรแกรมดังกล่าว ผู้ดูแลเครื่องบริการเว็บควรศึกษารายละเอียดของคู่มือการติดตั้ง (Installation Guideline) และการตั้งค่าพารามิเตอร์ต่าง ๆ ที่เกี่ยวข้อง เพื่อให้โปรแกรมดังกล่าวสามารถทำงานได้ตามความต้องการของผู้ให้บริการและมีความมั่นคงปลอดภัย การติดตั้งเครื่องบริการเว็บนั้นควรทำให้เกิดความมั่นคงปลอดภัยมากที่สุด ผู้ดูแลเครื่องบริการเว็บควรศึกษาเอกสาร ข้อมูลในการติดตั้งเครื่องบริการเว็บอย่างละเอียดก่อนที่จะเริ่มติดตั้งจริง ซึ่งในระหว่างขั้นตอนติดตั้ง อาจจะมีการติดตั้งโปรแกรมหรือสคริปต์ (Script) ใด ๆ ที่ไม่จำเป็น ติดตั้งมาให้อย่างอัตโนมัติ ดังนั้น เมื่อพบข้อมูลใด ๆ ที่ไม่จำเป็น ผู้ดูแลเครื่องบริการเว็บควรลบออกไปทันที เพื่อไม่เป็นการเปิดช่องโหว่ให้ผู้ประสงค์ร้ายเข้ามาทำอันตรายแก่เครื่องบริการเว็บได้ ดังนั้น มาตรฐานฉบับนี้จึงมีข้อกำหนดที่เกี่ยวกับโปรแกรมสำหรับให้บริการเว็บให้มีความมั่นคงปลอดภัย ดังนี้

(1) ปรับปรุงส่วนประกอบของโปรแกรมสำหรับให้บริการเว็บอย่างสม่ำเสมอ ส่วนใหญ่แล้วชุดปรับปรุง (Patch) นั้นจะเป็นโปรแกรมที่มีการแก้ไขข้อบกพร่องหรือจุดอ่อนของโปรแกรมที่ตรวจพบรวมถึงมีการพัฒนาประสิทธิภาพในการทำงานของโปรแกรมให้ดียิ่งขึ้น

(2) ควบคุมข้อความแจ้งเตือนหรือข้อความแสดงข้อผิดพลาด (Error Message) ไม่ให้แสดงข้อมูลที่เป็นประโยชน์ต่อผู้ประสงค์ร้าย เนื่องจากผู้ประสงค์ร้ายสามารถใช้ข้อมูลจากข้อความแจ้งเตือนหรือข้อความแสดงข้อผิดพลาดคาดเดาข้อมูลการตั้งค่าของโปรแกรมและระบบที่เกี่ยวข้องได้

(3) จัดหมวดหมู่ของสารบบ (Directory) ที่ใช้เก็บไฟล์ข้อมูล เว็บเพจ ระบบปฏิบัติการ โปรแกรมสำหรับให้บริการเว็บ และโปรแกรมอื่น ๆ โดยจะต้องมีการกำหนดสิทธิในการเข้าถึงสารบบที่เกี่ยวข้องทั้งหมดให้เหมาะสมกับการใช้งานและคำนึงถึงความมั่นคงปลอดภัย

(4) ตรวจสอบและจัดการลบ ตัวอย่างโปรแกรม ตัวอย่างไฟล์ข้อมูล บัญชีผู้ใช้ที่ไม่ได้ใช้งาน เช่น บัญชีซึ่งมีการใช้งานระหว่างกระบวนการติดตั้งเครื่องบริการเว็บทั้งหมด เช่น ไฟล์เอกสารที่มาจากบริษัทผู้ผลิตเครื่องบริการเว็บ ไฟล์ทดสอบ ไฟล์ตัวอย่างที่ติดตั้งจากเครื่องบริการเว็บ บัญชีผู้ใช้พื้นฐานที่เครื่องบริการเว็บสร้างขึ้นเป็นต้น

(5) ตรวจสอบไม่ให้มีการใช้ค่าเริ่มต้นของชื่อสารบบ ชื่อไฟล์ข้อมูล ตำแหน่งไฟล์ข้อมูล รหัสผ่าน ที่มากับการติดตั้งเครื่องบริการเว็บ เนื่องจากผู้ประสงค์ร้ายมักจะใช้ค่าเริ่มต้นเหล่านี้เป็นข้อมูลเบื้องต้นในการโจมตีเครื่องบริการเว็บ

(6) ควบคุมการเข้าถึงเครื่องบริการเว็บ และจำกัดหมายเลขไอพีปลายทางหรือยูอาร์แอลที่อนุญาตให้เครื่องบริการเว็บสามารถเชื่อมต่อ (Whitelist) ซึ่งช่วยให้ผู้ดูแลเครื่องบริการเว็บตรวจพบความผิดปกติหากพบว่ามีการเชื่อมต่อออกไปยังหมายเลขไอพีปลายทางหรือยูอาร์แอลที่ไม่ได้รับอนุญาต

(7) ปิดบริการต่าง ๆ ที่ไม่จำเป็นบนเครื่องบริการเว็บ โดยเฉพาะบริการประเภท Remote Access ส่วนใหญ่เครื่องบริการเว็บไซต์มักมีการติดตั้งซอฟต์แวร์ต่าง ๆ มาให้กับผู้ดูแลเครื่องบริการเว็บเพื่อเพิ่มความสะดวกสบายจากการเข้าจัดส่วนประกอบต่าง ๆ ของเว็บไซต์ ไม่ว่าจะเป็นบริการประเภท Remote Access เช่น Remote Desktop, VNC, SSH, Telnet หรือบริการอื่น ๆ ที่มีความเกี่ยวข้องกับเว็บไซต์โดยตรง

อย่างเช่น บริการฐานข้อมูล (Database) ตลอดจนบริการ FTP สำหรับจัดการไฟล์ของเว็บไซต์ การเปิดบริการต่าง ๆ ทิ้งไว้บนเครื่องบริการเว็บโดยไม่ได้ใช้งานก็เปรียบเสมือนการเปิดโอกาสให้ผู้ประสงค์ร้ายได้ทดสอบโจมตีหาช่องโหว่ตามช่องทางนั้น ๆ ซึ่งในกรณีที่รุนแรงมาก อาจถึงขั้นถูกผู้ประสงค์ร้ายเข้าถึงข้อมูลในเครื่องบริการเว็บในระดับสิทธิของผู้ดูแลระบบก็เป็นได้

5.2 การตั้งค่าระบบบริหารจัดการเว็บไซต์ (CMS)

แนวทางในการพัฒนาเว็บไซต์นั้นมีด้วยกันหลากหลายวิธี ซึ่งการนำระบบบริหารจัดการเว็บไซต์มาประยุกต์ใช้นั้นก็เป็นอีกทางเลือกหนึ่งที่ช่วยอำนวยความสะดวกในการพัฒนาและการบริหารจัดการเว็บไซต์ ผู้ดูแลเครื่องบริการเว็บจึงจำเป็นต้องตั้งค่าองค์ประกอบบางอย่างก่อนที่จะใช้งานจริง เพื่อให้เว็บไซต์มีความมั่นคงปลอดภัยและป้องกันภัยคุกคามจากผู้ประสงค์ร้าย [7] [12] [13] [14]

ดังนั้น มาตรฐานฉบับนี้จึงมีข้อกำหนดสำหรับการตั้งค่าระบบบริหารจัดการเว็บไซต์ ดังนี้

(1) ต้องมีการกำหนดสิทธิการใช้งาน (Permission) และการควบคุมการเข้าถึง (Access Control) ไฟล์ต่าง ๆ ให้เหมาะสมกับบทบาทและหน้าที่ของผู้ใช้บริการ
(2) ตรวจสอบว่ามีไฟล์หรือโปรแกรมเสริม (Plug-in Program) ที่ไม่จำเป็นหรือไม่ได้ใช้งานปรากฏอยู่หรือไม่ ถ้าตรวจพบผู้ดูแลเครื่องบริการเว็บต้องลบหรือถอนการติดตั้งไฟล์หรือโปรแกรมเสริมนั้นทันที
(3) หมั่นตรวจสอบการอัพเดตเวอร์ชั่นของระบบบริหารจัดการเว็บไซต์อยู่เสมอ และอัพเดตเวอร์ชั่นให้เป็นปัจจุบัน ให้ดาวน์โหลดไฟล์จากเว็บไซต์หลักของผู้ให้บริการระบบบริหารจัดการเว็บไซต์เท่านั้น
(4) ลบบัญชีผู้ใช้ที่มากับการติดตั้งระบบบริหารจัดการเว็บไซต์ เปลี่ยนชื่อผู้ใช้ของบัญชีผู้ใช้นั้นหรือเปลี่ยนรหัสผ่านของบัญชีผู้ใช้นั้น ให้เป็นรหัสผ่านที่มีความมั่นคงปลอดภัยแทน
(5) เปลี่ยน Table Prefix ของฐานข้อมูลที่มาในระหว่างการติดตั้งระบบบริหารจัดการเว็บไซต์ ยกตัวอย่างเช่นใน WordPress จะมีการใช้ Table Prefix ที่ขึ้นต้นด้วย wp_xxx ให้เปลี่ยนเป็นชื่ออื่น เนื่องจากอาจเป็นช่องทางให้ผู้ประสงค์ร้ายสามารถทราบถึงโครงสร้างและตารางในฐานข้อมูลได้

5.3 การตั้งค่าฐานข้อมูล (Database system)

จากเอกสารเรื่อง Oracle Database Security Checklist ของ Oracle [15] และ Making Database Security an IT Security Priority ของ SANS [16] ที่กล่าวถึงแนวทางการรักษาความมั่นคงปลอดภัยของฐานข้อมูลนับว่ามีความน่าสนใจเป็นอย่างมาก เนื่องจากในกระบวนการทำงานของเครื่องบริการเว็บและเว็บไซต์นั้น จะต้องมีการเก็บข้อมูลต่าง ๆ ลงในฐานข้อมูลอยู่เสมอ ดังนั้น ผู้ดูแลเครื่องบริการเว็บจึงจำเป็นต้องตั้งค่าองค์ประกอบบางอย่างเพื่อรักษาความมั่นคงปลอดภัยของข้อมูล

ดังนั้น มาตรฐานฉบับนี้จึงมีข้อกำหนดสำหรับการตั้งค่าฐานข้อมูล ดังนี้

(1) ตั้งค่าฐานข้อมูล อนุญาตให้เฉพาะโปรแกรมประยุกต์ (Application) และเครื่องบริการเว็บที่เกี่ยวข้องเข้าถึงได้เท่านั้น

(2) ควบคุมการเข้าถึงระบบฐานข้อมูลด้วยระบบรักษาความมั่นคงปลอดภัย เช่น ด่านกันบุกรุกหรือไฟร์วอลล์ (Firewall) เป็นต้น เพื่อไม่ให้ผู้ใช้บริการทั่วไปเข้าถึงฐานข้อมูลได้

(3) ตรวจสอบและปิดบริการ (Services) ที่ไม่จำเป็นหรือไม่ได้ใช้งาน ในระบบฐานข้อมูล

(4) จัดให้มีการทบทวนบัญชีผู้ใช้ภายในฐานข้อมูลตามระยะเวลาที่กำหนด และลบบัญชีผู้ใช้ที่ไม่ได้มีการใช้งานออกจากระบบฐานข้อมูล

(5) ปิดบัญชีผู้ใช้ที่มาพร้อมกับการติดตั้งฐานข้อมูล หรือเปลี่ยนรหัสผ่านของบัญชีผู้ใช้ดังกล่าว ให้เป็นรหัสผ่านที่มีความมั่นคงปลอดภัย

(6) กำหนดค่าติดตั้งระบบฐานข้อมูลเพื่อไม่อนุญาตให้ใช้งานรหัสผ่านที่มีค่าว่าง (Null Password)

(7) ตรวจสอบและลบแฟ้มชั่วคราว (Temporary File) ที่ถูกสร้างขึ้นระหว่างการติดตั้งระบบฐานข้อมูล เนื่องจากไฟล์ข้อมูลดังกล่าวอาจจะมีข้อมูลที่เป็นประโยชน์ต่อผู้ประสงค์ร้าย

(8) ปรับปรุงเวอร์ชั่นของโปรแกรมระบบฐานข้อมูล หรืออัพเดต Patch จากบริษัทผู้พัฒนาซอฟต์แวร์ให้เป็นเวอร์ชั่นล่าสุดเสมอ เพื่อให้โปรแกรมมีความมั่นคงปลอดภัยมากที่สุด

(9) กำหนดสิทธิการใช้งาน (Permission) และการควบคุมการเข้าถึง (Access Control) ให้เหมาะสมกับบทบาทและหน้าที่ของผู้ใช้ [17]

(10) รหัสผ่านที่เก็บในฐานข้อมูล ต้องมีการเข้ารหัสเสมอ

5.4 การตั้งค่า Server-Side Script Engine

ในปัจจุบัน หลายเว็บไซต์ได้มีการใช้เทคโนโลยีในการพัฒนาเว็บไซต์แบบพลวัต (Dynamic Website) ซึ่งเนื้อหาในหน้าเว็บเพจเปลี่ยนแปลงได้ตามปัจจัยที่กำหนด โดยการพัฒนาหน้าเว็บเพจแบบพลวัตนั้นต้องอาศัยการใช้เทคโนโลยี Server-Side Script Engine เช่น PHP [18], ASP.NET [19], JSP [20] เป็นต้น ซึ่งผู้ดูแลเครื่องบริการเว็บต้องทำการตั้งค่าองค์ประกอบบางอย่างของ Server-Side Script Engine ให้มีความมั่นคงปลอดภัยเพื่อป้องกันการเข้าถึงของผู้ประสงค์ร้าย

ดังนั้น มาตรฐานฉบับนี้จึงมีข้อกำหนดสำหรับการตั้งค่า Server-Side Script Engine ดังนี้

(1) ควบคุมการเข้าถึงไฟล์หรือสารบบต่าง ๆ ให้เหมาะสมกับบทบาทของผู้ใช้ เช่น ไฟล์ Script หรือสารบบที่เก็บโปรแกรม ควรอนุญาตการเข้าถึงและให้สิทธิแก่ผู้ใช้ที่เป็นเจ้าของไฟล์หรือนักพัฒนาซอฟต์แวร์เท่านั้น ผู้ใช้บริการทั่วไปได้รับสิทธิแค่อ่านและไม่สามารถแก้ไขได้ หรือผู้ดูแลเครื่องบริการเว็บได้รับสิทธิทั้งอ่าน เขียน และแก้ไขได้ เป็นต้น

(2) ปรับปรุงเวอร์ชั่นของ Server-Side Script Engine หรืออัพเดต Patch จากบริษัทผู้พัฒนาซอฟต์แวร์ให้เป็นเวอร์ชั่นล่าสุดเสมอ เพื่อให้โปรแกรมมีความมั่นคงปลอดภัยมากที่สุด

(3) กำหนดค่าติดตั้งไม่ให้ Server-Side Script Engine แสดงข้อมูลเวอร์ชั่นของ Server-Side Script Engine ที่เครื่องบริการเว็บใช้งาน ใน HTTP Header เนื่องจากอาจเป็นช่องทางให้ผู้ประสงค์ร้ายล่วงรู้เวอร์ชั่นที่เครื่องบริการเว็บใช้งานและหาช่องโหว่เข้ามาทำอันตรายได้ [21]

(4) กำหนดค่าติดตั้ง Server-Side Script Engine ไม่ให้มีการแสดงรายละเอียดของข้อความหรือแสดงข้อผิดพลาด (Error Message) หากต้องมีรายละเอียดควรจะแสดงข้อมูลเท่าที่จำเป็นและไม่เป็นประโยชน์กับผู้ประสงค์ร้าย

5.5 การกำหนดและรักษารหัสผ่าน

การเข้าใช้งานระบบต่าง ๆ ของเว็บไซต์ในปัจจุบัน เครื่องบริการเว็บจำเป็นที่จะต้องตรวจสอบและยืนยันตัวตนของผู้ใช้บริการ ว่าเป็นบุคคลที่ได้รับอนุญาตหรือไม่ ซึ่งโดยมากนั้นมักใช้ ชื่อบัญชีผู้ใช้ (Username) และรหัสผ่าน (Password) ในการตรวจสอบ ซึ่งการเข้าสู่ระบบด้วยชื่อบัญชีผู้ใช้และรหัสผ่านนั้น มีความเสี่ยงสูงต่อการถูกโจมตีจากผู้ประสงค์ร้าย และปัจจัยที่จะทำให้การโจมตีสำเร็จหรือไม่นั้น มักขึ้นอยู่กับการกำหนดรหัสผ่านของผู้ใช้บริการเองเป็นหลัก ซึ่งหากผู้ใช้บริการกำหนดรหัสผ่านที่ไม่มีความมั่นคงปลอดภัยแล้ว ก็เท่ากับเป็นการเปิดโอกาสให้ผู้ประสงค์ร้ายคาดเดารหัสผ่านและข้อมูลที่เป็นความลับของผู้ใช้บริการได้โดยง่าย และก่อให้เกิดผลกระทบมากมาย เช่น การทำธุรกรรมออนไลน์ หากผู้ประสงค์ร้ายเดาสุ่มชื่อบัญชีและรหัสผ่านของผู้ใช้บริการได้ ก็สามารถปลอมตัวเสมือนว่าเป็นผู้ใช้บริการเองเข้าไปทำธุรกรรมใด ๆ ก็ได้อย่างอิสระ เป็นต้น รูปแบบในการโจมตีเพื่อดักเอารหัสผ่านของบัญชีผู้ใช้ มี 2 วิธีก็คือ Dictionary Attack และ Brute Force Attack การโจมตีรหัสผ่านแบบ Dictionary Attack เป็นการสุ่มเดาข้อมูลหรือรหัสผ่านจากคำศัพท์ที่อยู่ใน Dictionary และคำศัพท์ที่พบบ่อยซึ่งเรียกว่า “Word List” ในขณะที่การโจมตีรหัสผ่านแบบ Brute Force Attack [2] จะเป็นวิธีการโจมตีด้วยการสุ่มข้อมูลหรือรหัสผ่านโดยคาดเดารหัสผ่านตามทุกความเป็นไปได้ของตัวอักษรในแต่ละหลัก ผู้ประสงค์ร้ายอาจเป็นผู้เดาสุ่มเองหรืออาจจะใช้โปรแกรมอัตโนมัติทำงานเพื่อเดาสุ่มก็ได้ ซึ่ง Brute Force Attack สามารถหารหัสผ่านที่ถูกต้องได้ เพียงแต่ขึ้นอยู่กับระยะเวลาของเดาสุ่มที่จะมากหรือน้อยนั้นขึ้นอยู่กับความซับซ้อนของการตั้งรหัสผ่าน

ดังนั้นมาตรฐานฉบับนี้จึงมีข้อกำหนดที่เกี่ยวกับการจัดการรหัสผ่านให้มีความมั่นคงปลอดภัยดังนี้

(1) ตั้งค่ารหัสผ่านให้มีความมั่นคงปลอดภัย (Strong Password) โดยรหัสผ่านควรประกอบด้วยตัวอักษรทั้งตัวเล็กและตัวใหญ่ผสมกัน มีตัวเลขและสัญลักษณ์พิเศษอย่างน้อย 1 หลัก และต้องมีความยาวทั้งหมดไม่น้อยกว่า 8 หลัก

(2) กำหนดให้มีการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอจะช่วยลดโอกาสจากการถูกคาดเดารหัสผ่าน

(3) ไม่เก็บรหัสผ่านที่ไม่มีการเข้ารหัสลับบนเครื่องบริการเว็บ หากจำเป็นต้องมีการเก็บรหัสผ่านควรอยู่ในรูปที่มีการเข้ารหัสลับตามที่มาตรฐานด้านความมั่นคงปลอดภัยกำหนด [22] เช่น AES หรือ Triple DES เป็นต้น และหากมีการเก็บอยู่ในรูปแบบของค่าแฮช (Hash Value) ควรใช้ขั้นตอนวิธี (Algorithm) ตามที่มาตรฐานด้านความมั่นคงปลอดภัยกำหนดไว้ [22] เช่น SHA-224 SHA-256 SHA-384 SHA-512 เป็นต้น

6. การพัฒนาโปรแกรมประยุกต์บนเครื่องบริการเว็บอย่างมั่นคงปลอดภัย

องค์ประกอบสำคัญของการรักษาความมั่นคงปลอดภัยเว็บไซต์ประกอบด้วยการรักษาความมั่นคงปลอดภัยในสองส่วนหลัก ได้แก่ (1) การรักษาความมั่นคงปลอดภัยของเครื่องบริการเว็บและโปรแกรมสำหรับให้บริการเว็บ (ซึ่งได้กล่าวในรายละเอียดไว้บทที่ 5) และ (2) การรักษาความมั่นคงปลอดภัยของโปรแกรมประยุกต์บนเว็บ จากสถิติภัยคุกคามที่เป็นการโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลเผยแพร่หน้าเว็บ (Website Defacement) ซึ่งผู้โจมตีมี

วัตถุประสงค์เพื่อปรับเปลี่ยนหน้าเว็บไซต์ ในปี พ.ศ. 2556 จำแนกตามประเภทหน่วยงาน (เฉพาะ โดเมนเนม .th) พบว่าเว็บไซต์ของหน่วยงานของรัฐ (go.th) ที่ถูกภัยคุกคามดังกล่าวมีจำนวนสูงสุด 1,929 เว็บไซต์ (คิดเป็นร้อยละ 44.6) และเว็บไซต์ของสถาบันการศึกษา (ac.th) มีจำนวน 1,515 เว็บไซต์ (คิดเป็นร้อยละ 35) ซึ่งสาเหตุหลักที่ทำให้เกิดมีการโจมตีประเภทดังกล่าวมาจากช่องโหว่หรือข้อบกพร่องที่เกิดจากโปรแกรมประยุกต์บนเว็บ เนื่องจากบ่อยครั้งที่การรักษาความมั่นคงปลอดภัยของโปรแกรมประยุกต์บนเว็บมักจะถูกมองข้ามทั้งที่เป็นเรื่องที่สำคัญ

Open Web Application Security Project หรือ OWASP ซึ่งเป็นองค์กรจัดตั้งขึ้นเพื่อส่งเสริมและพัฒนาการรักษาความมั่นคงปลอดภัยของเว็บไซต์หรือโปรแกรมประยุกต์บนเว็บได้มีการจัดทำโครงการจัด 10 อันดับความเสี่ยงของโปรแกรมประยุกต์บนเว็บเป็นประจำทุกปี ซึ่งในปี 2013 นั้น มีการจัดอันดับความเสี่ยงที่พบสูงสุด 10 อันดับ (รายละเอียดเพิ่มเติมจากเว็บไซต์ https://www.owasp.org) ซึ่งสอดคล้องกับความเสี่ยงที่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือ ไทยเซิร์ต ตรวจพบในเว็บไซต์ที่มีอยู่ในประเทศไทย โดยช่องโหว่หรือความเสี่ยงที่เกี่ยวกับโปรแกรมประยุกต์บนเว็บที่พบส่วนใหญ่จะเป็นเรื่องการโจมตีจากเทคนิคต่าง ๆ เช่น SQL Injection, Session Hijacking และ CSRF เป็นต้น

ดังนั้น มาตรฐานฉบับนี้จึงมีข้อกำหนดสำหรับแนวทางในการรักษาความมั่นคงปลอดภัยของโปรแกรมประยุกต์บนเว็บเพื่อป้องกันความเสี่ยงที่เกี่ยวกับโปรแกรมประยุกต์ซึ่งพบเป็นส่วนใหญ่ดังนี้

6.1 การป้องกันการโจมตีจากเทคนิค SQL Injection

ในปัจจุบัน หลายเว็บไซต์ได้มีการใช้เทคโนโลยีในการพัฒนาเว็บเพจแบบพลวัต (Dynamic Website) ซึ่งเนื้อหาในหน้าเว็บเพจเปลี่ยนแปลงได้ตามปัจจัยที่กำหนดเช่น เปลี่ยนแปลงตามช่วงเวลาที่ผู้ใช้บริการเข้าถึงเว็บไซต์หรือเปลี่ยนแปลงตามที่ผู้ใช้บริการกำหนดเป็นต้น ยกตัวอย่างเช่น เว็บไซต์กระดานข่าว เมื่อผู้ใช้บริการต้องการอ่านกระทู้ในกระดานข่าว โปรแกรมประยุกต์ที่เกี่ยวข้องจะประมวลผลและแสดงหน้าเว็บเพจที่เป็นปัจจุบันมากที่สุดให้แก่ผู้ใช้บริการ

ซึ่งจากลักษณะการทำงานข้างต้น โปรแกรมประยุกต์บนเว็บเชื่อมต่อกับฐานข้อมูลทุกครั้งที่มีการเรียกหน้าเว็บเพจ เป็นสาเหตุให้เกิดการโจมตีเว็บไซต์ด้วยเทคนิค Injection ซึ่งการโจมตีด้วยเทคนิค SQL Injection นี้ผู้ประสงค์ร้ายแทรกคำสั่ง SQL เข้าไปทาง Input Form บนเว็บเพจ ทำให้สามารถดำเนินการใด ๆ ก็ตามกับในฐานข้อมูลได้ โดยผ่านคำสั่ง SQL เช่น Insert Update Delete หรือ สั่งคำสั่งปิดฐานข้อมูล เป็นต้น ผู้พัฒนาโปรแกรมประยุกต์บนเว็บนั้นต้องพัฒนาเว็บไซต์โดยคำนึงถึงการป้องกันการโจมตีด้วยเทคนิค Injection ด้วย ดังนั้น มาตรฐานฉบับนี้จึงมีข้อกำหนดในการป้องกันปัญหาดังกล่าว ดังนี้

(1) โปรแกรมประยุกต์บนเว็บต้องมีการจัดทำ Prepared Statement และ/หรือ Stored Procedure เป็นวิธีการที่จะแยกคำสั่งในการประมวลผลและค่าที่จะนำไปประมวลผลออกจากกัน จากวิธีการดังกล่าวจะช่วยป้องกันการโจมตีด้วยวิธีการทำ SQL Injection ได้ ซึ่งสามารถศึกษารายละเอียดเพิ่มเติมเรื่อง Stored Procedure ได้ที่ https://www.owasp.org/index. PHP/Guide_to_SQL_Injection และ https://www.owasp.org/index. PHP/Avoiding_SQL_Injection#Parameterized_ Stored_Procedures

(2) โปรแกรมประยุกต์บนเว็บต้องมีการจัดทำ Input Validation ซึ่ง Input Validation เป็นวิธีการที่ใช้ในการตรวจสอบข้อมูลที่ได้รับก่อนส่งมาประมวลผลจริง นับว่าเป็นวิธีการที่สำคัญและจำเป็นที่สุดในกระบวนการพัฒนาระบบให้มีความมั่นคงปลอดภัย หากระบบใด ๆ ยอมให้ผู้ใช้บริการสามารถป้อนข้อมูลได้โดยไม่มีการตรวจสอบแล้ว การโจมตีระบบจะสามารถทำได้ง่าย การทำ Input Validation มีหลักการง่าย ๆ เพียงแค่ต้องสามารถระบุรูปแบบของข้อมูลที่อนุญาตหรือไม่อนุญาตให้ป้อนเข้าสู่ระบบ ซึ่งเรียกอีกชื่อว่าการทำ Whitelist และ Blacklist ตามลำดับตัวอย่างการทำ Whitelist เช่น การอัพโหลดไฟล์เอกสารจะต้องอนุญาตให้อัพโหลดได้เฉพาะไฟล์ที่มีนามสกุล (File Extension) เป็น .txt .docx .xlsx .pdf เท่านั้น ซึ่งการพัฒนาฟังก์ชันสำหรับทำ Whitelist ดังกล่าวก็จะทำให้การพยายามอัพโหลดไฟล์อันตรายต่าง ๆ ขึ้นบนระบบทำได้ยากยิ่งขึ้น ตัวอย่างการทำ Blacklist เช่น การรับค่าจาก Form ที่ผู้ใช้บริการกรอกเข้ามาจะต้องไม่อนุญาตให้มีอักขระพิเศษประเภทที่เอื้อให้เกิดการโจมตีด้วยเทคนิคต่าง ๆ เช่น ต้องไม่มีการใส่เครื่องหมาย < > หรือต้องไม่ให้มีการใส่คำว่า <script> เป็นต้น ซึ่งการพัฒนาฟังก์ชันสำหรับทำ Blacklist ดังกล่าวจะช่วยทำให้ลดโอกาสในการถูกโจมตีสำเร็จได้อีกระดับหนึ่ง

(3) โปรแกรมประยุกต์บนเว็บต้องมีการทำ Encoding หรือทำ Sanitization

ข้อมูลที่รับมาจากภายนอกควรมีการทำ Encoding หรือ Sanitization ก่อนนำค่ามาประมวลผล เพื่อป้องกันการโจมตีด้วยเทคนิคต่าง ๆ ข้อมูลที่ผ่านกระบวนการดังกล่าวจะถูกแปลงรูปแบบของข้อมูลที่ส่งมาจากฝั่งผู้ใช้บริการให้อยู่ในรูปแบบที่ระบบนำไปประมวลผลได้โดยไม่อันตราย ตัวอย่างเช่น การใช้งานฟังก์ชัน mysql_real_escape_string ในภาษา PHP เพื่อป้องกันการโจมตีด้วยเทคนิค SQL Injection โดยฟังก์ชันดังกล่าวจะทำการตรวจสอบว่ามีการป้อนค่าอักขระพิเศษเข้ามาหรือไม่ หากมีฟังก์ชันดังกล่าวจะทำการเพิ่มเครื่องหมาย Backslash ลงไปด้านหน้า เช่น หากผู้ประสงค์ร้ายป้อนข้อมูลที่ใช้ในการโจมตีระบบเป็น ' OR 1=1 --' ระบบจะแปลงค่าเป็น \' OR 1=1 --\' ซึ่งเท่ากับข้อมูลที่ส่งมาโจมตีจะไม่เป็นผลใด ๆ รายละเอียดสามารถอ่านเพิ่มเติมได้จากเอกสารของ OWASP (https://www.owasp.org/index. PHP/SQL_Injection_Prevention_Cheat_Sheet และ https://www.owasp.org/index. PHP/Query_Parameterization_Cheat_Sheet)

6.2 การป้องกันการโจมตีจากเทคนิค Session Hijacking

ในการเข้าถึงเว็บไซต์ใด ๆ ของผู้ใช้บริการ จะมีการส่งคำร้องไปยังเครื่องบริการเว็บ ซึ่งเครื่องบริการเว็บก็จะมีวิธีการในการตรวจสอบและพิสูจน์ตัวตนของผู้ใช้บริการหลากหลายวิธี ซึ่งวิธีที่ใช้กันโดยมากนั่นคือ การสร้างโทเค็น (Token) ซึ่งใช้เป็นข้อมูลการรับรองตัวตนของผู้ใช้บริการ (User Authentication Credential) ขึ้นหลังจากกระบวนการยืนยันตัวตนของผู้ใช้บริการสำเร็จ ที่มักเรียกว่า Session ID โดย Session ID นี้จะถูกนำไปใช้ในการอ้างอิงและตรวจสอบสิทธิในการเข้าถึงหน้าเว็บเพจต่าง ๆ ในเว็บไซต์ที่ผู้ใช้บริการเข้าเยี่ยมชม Session ID นี้จะถูกใช้จนกว่าผู้ใช้บริการจะปิดหน้าต่างโปรแกรมค้นดูเว็บ ก็ถือจะเป็นการลบ Session ID นั้นไป และจะไม่สามารถใช้ Session ID เดิมในการอ้างอิงได้อีก นอกเสียจากต้องเปิดโปรแกรมค้นดูเว็บขึ้นใหม่ จึงจะได้รับ Session ID ใหม่ จากลักษณะการทำงานข้างต้น ทำให้เครื่องบริการเว็บสามารถติดตามข้อมูลทางฝั่งผู้ใช้บริการได้ตลอดตราบเท่าที่โปรแกรมค้นดูเว็บยังไม่ถูกปิด ทำให้ผู้ประสงค์ร้ายสามารถอาศัยช่องโหว่นี้ในการโจมตีเว็บไซต์ด้วยวิธี Session Hijack

ได้นั่นก็คือการดักขโมย Session ID ของผู้ใช้บริการ นำเอา Session ID ไปใช้ในการเข้าเว็บไซต์ด้วยสิทธิของเจ้าของ Session ได้

มาตรฐานฉบับนี้มีข้อกำหนดในการป้องกันปัญหาดังกล่าว ดังนี้

(1) Session ID ที่มีข้อมูลการรับรองตัวตนของผู้ใช้บริการ (User Authentication Credential) ต้องมีการเข้ารหัสลับ การเข้ารหัสลับข้อมูลการรับรองตัวตนของผู้ใช้บริการ ด้วยอัลกอริทึมสำหรับการเข้ารหัสลับ หรือฟังก์ชันแฮช จะช่วยให้ผู้ประสงค์ร้ายไม่สามารถนำข้อมูลดังกล่าวมาใช้ได้โดยง่าย ซึ่งจะช่วยลดความเสี่ยงจากการโจมตีด้วยเทคนิค Session Hijacking

(2) โปรแกรมประยุกต์บนเว็บต้องกำหนด Session Timeout ในระยะเวลาที่เหมาะสมการกำหนด Session Timeout เป็นมาตรการหนึ่งที่ช่วยลดความเสี่ยงจากการโจมตีด้วยเทคนิค Session Hijacking ทั้งนี้ระยะเวลาที่ใช้กำหนด Session Timeout ของแต่ละเว็บไซต์ขึ้นอยู่กับพฤติกรรมการใช้งานและความต้องการใช้งานของผู้ใช้บริการ ยกตัวอย่างเช่น หากผู้ใช้บริการใช้เวลาเฉลี่ยในการเข้าชมและทำธุรกรรมที่เกี่ยวข้องบนเว็บไซต์เฉลี่ยคนละ 1 ชั่วโมง ก็อาจจะกำหนดให้ Session Timeout อยู่ที่ 1 ชั่วโมงเป็นต้น

(3) กำหนดค่า Session ID เป็นค่าสุ่มที่คาดเดาไม่ได้และไม่มีการใช้ซ้ำในระยะเวลาที่เหมาะสม การใช้ Session ID ที่เป็นค่าสุ่ม (Random Value) คาดเดาไม่ได้ และเป็นค่าที่ไม่มีการนำกลับมาใช้ซ้ำในระยะเวลาที่เหมาะสมจะช่วยลดความเสี่ยงจากการโจมตีด้วยเทคนิค Session Hijacking ได้

(4) ต้องส่งค่า Session ID ในช่องทางการสื่อสารที่มีการเข้ารหัสลับ (Encrypted Connection) โปรแกรมประยุกต์บนเว็บที่มีการส่งค่า Session ID ผ่านระบบเครือข่ายคอมพิวเตอร์ โดยเฉพาะการส่งผ่านตัวแปรใน URL อย่างเปิดเผย มักจะมีความเสี่ยงต่อการโจมตีด้วยเทคนิค Session Hijacking สูง การส่งค่า Session ID ควรส่งผ่านช่องทางการสื่อสารที่มีการเข้ารหัสลับ เช่น การส่งข้อมูลผ่านโพรโทคอล HTTPS (ดูรายละเอียดเพิ่มเติมในภาคผนวก ข.) เพื่อป้องกันการลักลอบดักรับข้อมูล หรือ มีการส่งผ่านช่องทางลับที่ไม่เปิดเผยต่อสาธารณะ เป็นต้น

รายละเอียดที่เกี่ยวข้องกับการป้องกันการโจมตีจากเทคนิค Session Hijacking สามารถศึกษาเพิ่มเติมได้จากเอกสารของ OWASP ตาม URL นี้https://www.owasp.org/index.
PHP/Session_Management_Cheat_Sheet

6.3 การป้องกันการโจมตีจากเทคนิค Cross-Site Scripting

Cross-Site Scripting (XSS) เกิดจากช่องโหว่ของเว็บไซต์/เว็บเพจที่ไม่มีการคัดกรองและตรวจสอบข้อมูลที่ได้รับจากผู้ใช้บริการว่าเป็นข้อมูลที่เชื่อถือได้หรือไม่ ทำให้ผู้ประสงค์ร้ายสามารถแทรกคำสั่งต่าง ๆ เข้าไปในเว็บเพจเมื่อผู้ใช้บริการเรียกหน้าเว็บเพจนั้น ก็อาจจะถูกขโมยข้อมูลสำคัญไปได้ ซึ่งผู้ประสงค์ร้ายอาจจะนำไปสวมรอยและล๊อกอินเข้าไปยังเว็บไซต์เสมือนหนึ่งว่าเป็นผู้ใช้บริการตัวจริง

มาตรฐานฉบับนี้มีข้อกำหนดในการป้องกันการโจมตีด้วยเทคนิคดังกล่าว ดังนี้

(1) โปรแกรมประยุกต์บนเว็บต้องมีการทำ Input Validation

Input Validation เป็นวิธีการที่ใช้ในการตรวจสอบข้อมูลที่ได้รับก่อนส่งมาประมวลผลจริง โดยใช้กฎจาก Whitelist คือ ระบุรูปแบบของข้อมูลที่อนุญาตให้ป้อนเข้ามูลเข้าระบบ เช่น การอัพโหลดไฟล์เอกสารจะต้องอนุญาตให้อัพโหลดได้เฉพาะไฟล์ที่มีนามสกุล (File Extension) เป็น .txt .docx .xlsx .pdf เท่านั้น

(2) โปรแกรมประยุกต์บนเว็บต้องมีการตรวจสอบข้อมูลชุดคำสั่งในเว็บไซต์

การตรวจสอบข้อมูลชุดคำสั่งในเว็บไซต์ว่ากำลังรับข้อมูลที่ผิดปกติ เป็นสคริปต์ที่อันตราย หรือไม่ เช่น สคริปต์ที่มีเครื่องหมายอักขระพิเศษต่าง ๆ เช่น < > ? & # เป็นต้น โดยต้องคัดกรองเครื่องหมายเหล่านี้ก่อนที่จะนำไปประมวลผลที่เครื่องบริการเว็บ และการกรองอินพุตจากผู้ใช้เป็นหลัก โดยอินพุตต่าง ๆ ไม่ควรถูกนำมาใช้งานในทันที แต่ต้องมีการกรองก่อนทุกครั้ง และต้องมั่นใจได้ว่าผู้ใช้ไม่สามารถวางสคริปต์ใด ๆ ลงในเว็บได้ ควรแปลงพวก "Non-alphanumeric Data" ให้กลายเป็น HTML Character เสียก่อน เช่น เครื่องหมายน้อยกว่า "<" ควรถูกแปลงเป็น "& l t ;" เป็นต้น

(3) โปรแกรมประยุกต์บนเว็บต้องมีการทำ Output Validation ในลักษณะ Sanitization

การ HTML Entity Encoding หรือ URL Encoding กับข้อมูลที่จะแสดงผล โดยการทำ Output Validation เปรียบเสมือนการป้องกันการแสดงผลข้อมูลที่ไม่พึงประสงค์ยังฝั่งผู้ใช้บริการ เช่น การแสดงผลข้อผิดพลาด (Error Message) ที่ในบางครั้งอาจแสดงข้อมูลที่เป็นประโยชน์ต่อผู้ประสงค์ร้าย ซึ่งข้อมูลทั้งหมดนี้ผู้ประสงค์ร้ายสามารถรวบรวมมาเป็นข้อมูลที่ใช้โจมตีเว็บไซต์ได้ง่ายมากขึ้น ตัวอย่างเช่น การใช้งานฟังก์ชัน htmlentities() ในภาษา PHP เพื่อป้องกันการโจมตีด้วยเทคนิค XSS สมมติว่าผู้ประสงค์ร้ายมีการส่งค่า <script>alert ("Hacked")</script> เข้ามายังระบบผ่านตัวแปรหนึ่ง เมื่อค่าดังกล่าวถูกนำไปประมวลผลผ่านฟังก์ชัน htmlentities() ซึ่งจะมีการ Encode ค่าต่าง ๆ ให้อยู่ในรูปแบบที่โปรแกรมคนดูเว็บมองเป็นเพียงข้อความธรรมดา กรณีนี้ผลลัพธ์ที่ได้จากการ Encode ด้วยฟังก์ชันดังกล่าว จะได้ออกมาเป็น <script>alert ("Hacked")</script> อย่างไรก็ตาม โปรแกรมคนดูเว็บยังสามารถแสดงผลค่าดังกล่าวได้เป็น <script>alert ("Hacked")</script> ในฝั่งผู้ใช้บริการได้อยู่ แต่อยู่ในรูปแบบของข้อความซึ่งไม่สามารถนำมาประมวลผลในลักษณะสคริปต์ตามที่ผู้ประสงค์ร้ายต้องการได้

(4) โปรแกรมประยุกต์บนเว็บต้องมีการใช้งาน HTTPOnly Cookie flag

HTTPOnly เป็นรูปแบบการกำหนดค่าเพิ่มเติม (Flag) สำหรับป้องกันไม่ให้ฝั่งผู้ใช้บริการสามารถการเข้าถึงค่า Cookie ของระบบได้ โดยทั่วไปหากระบบมีช่องโหว่ของการโจมตีด้วยเทคนิค XSS ผู้ประสงค์ร้ายอาจส่งคำสั่งเพื่อให้ผู้ใช้บริการทำการอ่านข้อมูล Cookie ของผู้ใช้บริการและลักลอบส่งข้อมูลออกไปยังปลายทาง รวมถึงในบางครั้งอาจสั่งให้มีการปรับเปลี่ยนค่าใน Cookie ได้ด้วย แต่อย่างไรก็ตามการใช้งาน HTTPOnly[4] นั้นยังมีข้อจำกัดว่าสามารถใช้งานกับโปรแกรมค้นดูเว็บที่สนับสนุนเท่านั้น เช่น โปรแกรมค้นดู

[4] เอกสารของ OWASP ได้ที่URL

https://www.owasp.org/index. PHP/HttpOnly#Browsers_Supporting_HttpOnly)

เว็บ Chrome ตั้งแต่เวอร์ชั่น 1.0.154 หรือ Safari ตั้งแต่เวอร์ชั่น 4 หรือ Internet Explorer ตั้งแต่เวอร์ชั่น 6sp1 เป็นต้น

6.4 การป้องกันการโจมตีจากเทคนิค CSRF

Cross Site Script Forgery (CSRF)[5] เป็นภัยคุกคามประเภทหนึ่งทางเว็บไซต์ที่เกิดจากการที่ผู้ประสงค์ร้ายลักลอบปลอมแปลงคำสั่งข้อมูลให้เสมือนเป็นคำสั่งจากผู้ใช้บริการตัวจริงเพื่อติดต่อกับระบบต่าง ๆ ของเว็บไซต์ โดยเว็บไซต์จะเข้าใจว่านั่นคือคำสั่งที่มาจากผู้ใช้บริการตัวจริงและดำเนินการตามที่ร้องขอ เช่น ผู้ประสงค์ร้ายอาศัยช่องโหว่ของเว็บเพจ ปลอมแปลงคำสั่งข้อมูลให้เสมือนเป็นคำสั่งจากเจ้าของบัญชีจริงเพื่อติดต่อกับระบบธนาคารทางอินเทอร์เน็ต ทำให้ระบบเชื่อและเข้าใจว่าเจ้าของบัญชีต้องการทำธุรกรรมการเงินนั้น ๆ จริง

มาตรฐานฉบับนี้มีข้อกำหนดในการป้องกันการโจมตีด้วยเทคนิคดังกล่าว ดังนี้

(1) โปรแกรมประยุกต์บนเว็บต้องมีการใช้งาน Unique Token และ/หรือตรวจสอบ Referrer ร่วมกับการส่งข้อมูล หรือคำสั่งผ่านแบบฟอร์ม

การโจมตีด้วยเทคนิค CSRF อาจเป็นเรื่องที่เข้าใจได้ยากสักนิด แต่วิธีการป้องกันที่ได้ผลดีที่สุดคือการสร้างข้อมูลอ้างอิง เพื่อใช้ในการตรวจสอบความถูกต้องของข้อมูลที่ส่งมาประมวลผล อาจจะด้วยการสร้าง Unique Token ในแบบฟอร์ม เพื่อให้แน่ใจว่าข้อมูลในแบบฟอร์มที่จะส่งมาประมวลผลในแต่ละครั้งนั้นเป็นข้อมูลที่เกิดมาจากการที่ผู้ใช้บริการจริง ไม่ใช่โปรแกรมอัตโนมัติหรือสคริปต์ที่ใช้ในการโจมตีแต่อย่างใด ซึ่งจะเห็นตัวอย่างของวิธีการดังกล่าวได้จากการเข้าใช้งาน Online Banking ที่ในแต่ละการทำธุรกรรมจะต้องมีการยืนยันด้วยหมายเลข OTP (one-time password) ก่อนเสมอ เพื่อเป็นการยืนยันว่าการทำธุรกรรมนั้นเกิดจากผู้ใช้บริการจริง

(2) โปรแกรมประยุกต์บนเว็บต้องมีการใช้ Captcha การเปลี่ยนแปลงสถานะการทำงานในฟังก์ชันที่สำคัญ ๆ เช่น เปลี่ยนจากสถานะเลือกซื้อสินค้า เป็น จ่ายเงินชำระค่าสินค้า ระบบควรจะให้ผู้ใช้บริการ ยืนยันตัวตนอีกครั้ง เช่น ให้กรอกรหัสผ่านใหม่ พร้อมกับใช้ Captcha เป็นต้น

OWASP ได้มีเอกสารที่รวบรวมเทคนิคต่าง ๆ ในการป้องกันจากการโจมตีด้วยเทคนิค Cross-site scripting ดังรายละเอียดเพิ่มเติมตาม URL นี้

https://www.owasp.org/index. PHP/XSS_ (Cross_Site_Scripting)_Prevention_Cheat_Sheet

[5] ข้อมูลเพิ่มเติมที่เกี่ยวข้องกับการโจมตีด้วยทางเทคนิคดังกล่าวสามารถอ่านเพิ่มเติมได้เว็บไซต์ของ OWASP และ v SANS จาก URL ดังนี้

https://www.owasp.org/index. PHP/Cross-Site_Request_Forgery_ (CSRF)_ Prevention_Cheat _Sheet

https://www.sans.org/reading-room/whitepapers/application/appsec-cross-site-request-forgery-attackers-33108

6.5 การป้องกันการโจมตีจากปัญหาข้อมูลลับรั่วไหล (Sensitive Data Exposure)

ปัจจุบัน เว็บไซต์มักมีการเก็บข้อมูลที่มีความสำคัญของผู้ใช้บริการ ซึ่งก็คือ หมายเลขบัตรประจำตัวประชาชน หมายเลขบัตรเครดิต รหัสผ่านที่ใช้เข้าระบบเป็นต้น จึงจำเป็นที่จะต้องมีการควบคุมให้เปิดเผยข้อมูลดังกล่าวต่อผู้ที่เกี่ยวข้องเท่านั้น และต้องมีการควบคุมข้อความแจ้งเตือนหรือข้อความแสดงข้อผิดพลาดไม่ให้แสดงข้อมูลใด ๆ ที่เป็นประโยชน์ต่อผู้ประสงค์ร้าย ผู้พัฒนาโปรแกรมประยุกต์บนเว็บนั้นต้องพัฒนาเว็บไซต์โดยคำนึงถึงการรักษาความลับของข้อมูลที่มีความสำคัญด้วย

มาตรฐานฉบับนี้มีข้อกำหนดในการป้องกันปัญหาดังกล่าว ดังนี้

(1) โปรแกรมประยุกต์บนเว็บจะต้องมีการออกแบบและควบคุมข้อความแจ้งเตือนหรือข้อความแสดงข้อผิดพลาด (Notification or Error Message) ไม่ให้แสดงข้อมูลที่เป็นประโยชน์ต่อผู้ประสงค์ร้าย

(2) โปรแกรมประยุกต์บนเว็บจะต้องพัฒนาเว็บไซต์โดยไม่ให้มีการใช้งาน Autocomplete ในแบบฟอร์มสำคัญ เช่น แบบฟอร์มสำหรับการลงทะเบียนการใช้งานระบบที่มีรหัสผ่าน หรือ แบบฟอร์มที่เกี่ยวข้องกับการชำระเงิน เป็นต้น

(3) ไม่ใช้ชื่อ URL ที่คาดเดาได้ง่ายซึ่งใช้ในการเข้าถึงหน้าเว็บสำหรับผู้ดูแลเครื่องบริการเว็บ (Administrator Control Panel Web Page) เช่น admin. PHP หรือ login. PHP เป็นต้น

7. การรับมือสถานการณ์ภัยคุกคามที่เกิดจากการโจมตีเว็บไซต์ (Incident Handling)

ภัยคุกคามหรือสถานการณ์การโจมตีที่เกิดขึ้นกับเว็บไซต์ในปัจจุบัน สามารถจำแนกได้ในหลากหลายประเภทของการโจมตี อาจเป็นเพราะความเจริญเติบโตของการใช้งานอินเทอร์เน็ตทำให้มีกลุ่มแฮกเกอร์รวมตัวกันง่ายขึ้น พร้อมทั้งยังมีการเผยแพร่ข้อมูลวิธีการโจมตีที่เปิดเผยและสามารถค้นหาได้อย่างง่ายดายบนโลกอินเทอร์เน็ต ซึ่งจากตัวอย่างสถิติที่ไทยเซิร์ตตรวจสอบพบการเจาะเว็บไซต์ของหน่วยงานในประเทศไทย (.th) ในปี 2556 พบสถิติเว็บไซต์ .th ถูกเจาะเพื่อเปลี่ยนแปลงเว็บไซต์หรือที่เรียกว่า Web Defacement ถึง 5,230 เว็บไซต์ นอกจากนี้ยังพบเหตุการณ์โจมตีในลักษณะอื่น ๆ อีกมากมาย ในทิศทางที่เพิ่มขึ้นเรื่อย ๆ อย่างต่อเนื่อง แสดงให้เห็นถึงความเสี่ยงต่อการถูกโจมตีของระบบในหน่วยงานต่าง ๆ จึงมีความจำเป็นต้องรับทราบมาตรการและการดำเนินการที่เกี่ยวข้องในการรับมือเมื่อเกิดเหตุการณ์โจมตีในลักษณะต่าง ๆ ที่อาจเกิดขึ้น

7.1 การรับมือภัยคุกคามที่เกิดขึ้นกับเว็บไซต์

โดยแนวทางการรับมือสถานการณ์ภัยคุกคามที่เกิดกับเว็บไซต์ตามเอกสารฉบับนี้ จำแนกออกเป็น 3 ประเภทของรูปแบบการโจมตีดังต่อไปนี้

7.1.1 กรณีเว็บไซต์ถูกบุกรุกและควบคุม (Intrusions)

ภัยคุกคามจากการบุกรุกและควบคุมเว็บไซต์ (Intrusions) สามารถพบเห็นและยืนยันได้ง่ายที่สุด เนื่องจากการโจมตีนั้นมักจะต้องมีการสร้างร่องรอยหรือหลักฐานที่เห็นได้อย่างชัดเจน ตามแต่ละจุดประสงค์ของผู้ประสงค์ร้าย ตัวอย่างเช่น การสร้างหน้าเว็บไซต์หลอกลวง (Phishing) เพื่อหวังผลทางการเงิน การเปลี่ยนแปลงข้อมูลต่าง ๆ บนเว็บไซต์ (Web Defacement) เพื่อหวังผลในการทำลายชื่อเสียง หรือแม้กระทั่งการเผยแพร่มัลแวร์บนเว็บไซต์

(Malware) เพื่อให้ผู้เข้าชมเว็บไซต์ติดมัลแวร์ เป็นต้น ซึ่งการรับมือสถานการณ์ภัยคุกคามในกรณีเว็บไซต์ถูกบุกรุกและควบคุมนี้สามารถดำเนินการได้ในลักษณะเดียวกัน ดังนั้น มาตรฐานฉบับนี้จึงมีข้อกำหนดที่เกี่ยวข้องดังนี้

(1) ปิดการเชื่อมต่อของเว็บไซต์
(2) สำเนาข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการถูกบุกรุกเพื่อนำมาใช้ในการวิเคราะห์ เช่น Web Log Sourcecode Database
(3) ตรวจสอบช่องทางการโจมตีและช่องโหว่ของเว็บไซต์ด้วยข้อมูลที่สำเนามา โดยในระหว่างที่ผู้ดูแลกำลังตรวจสอบช่องทางการโจมตี
(4) ระหว่างการตรวจสอบจัดสร้างเว็บเพจแบบ Static ขึ้นมาทดแทนเป็นการชั่วคราว เพื่อชี้แจงสถานการณ์การปิดปรับปรุง รวมไปถึงเพื่อให้หน่วยงานสามารถดำเนินภารกิจได้อย่างต่อเนื่อง โดยเว็บเพจดังกล่าวควรติดตั้งอยู่ในเครื่องบริการเว็บใหม่ เพื่อลดความเสี่ยงจากการที่เครื่องบริการเว็บเดิมถูกควบคุมและปรับเปลี่ยนการตั้งค่าต่าง ๆ เพื่อป้องกันไม่ให้มีผลกับข้อมูลต่าง ๆ ที่อยู่บนเครื่องเดิม
(5) กู้คืนโปรแกรมที่เกี่ยวข้อง ข้อมูลเว็บ และฐานข้อมูลที่เกี่ยวข้องกับเว็บไซต์เป็นเวอร์ชันก่อนหน้าที่จะถูกโจมตี
(6) ตรวจสอบช่องโหว่ของเว็บไซต์ (เวอร์ชั่นก่อนหน้าที่จะถูกโจมตี) ด้วยการทำ Vulnerability Assessment แก้ไขช่องโหว่ของเว็บไซต์ที่ทำให้ผู้ประสงค์ร้ายสามารถเจาะเพื่อเข้าควบคุมระบบได้
(7) บันทึกเหตุการณ์และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด เพื่อใช้เป็นข้อมูลในการป้องกันและการประสานงานกับหน่วยงานที่เกี่ยวข้องในกรณีที่จำเป็น

ในหลายครั้งพบว่าผู้ประสงค์ร้ายสามารถบุกรุกและเข้าควบคุมเว็บไซต์ได้มาเวลานานแล้วแต่เพิ่งมาสร้างร่องรอยหรือเปลี่ยนแปลงข้อมูลในเวลาต่อมา ส่งผลให้การวิเคราะห์ข้อมูลการโจมตีและช่องโหว่ของเว็บไซต์ผ่านข้อมูล Log นั้นทำได้ยากขึ้น เนื่องจากในบางหน่วยงานมีเก็บข้อมูล Log ไว้เพียงชั่วขณะหนึ่ง ทำให้การวิเคราะห์ข้อมูลในช่องเวลาที่มีการโจมตีจริง ๆ นั้นไม่สามารถทำได้ อย่างไรก็ตามผู้ดูแลต้องทบทวนข้อมูล Log อย่างสม่ำเสมอเพื่อตรวจสอบดูการโจมตีที่เกิดขึ้น

7.1.2 กรณีเว็บไซต์ถูกโจมตีในลักษณะ DoS (Denial of Service)

การโจมตีเว็บไซต์ในลักษณะ DoS นั้นกล่าวคือ การโจมตีเพื่อมุ่งเน้นให้เว็บไซต์ไม่สามารถให้บริการต่อได้ ซึ่งเป้าประสงค์สามารถเกิดได้จากหลายส่วน เช่น การลดความน่าเชื่อถือของหน่วยงาน การลดโอกาสในการทำธุรกิจ รวมถึงในปัจจุบันพบว่ามีเป้าประสงค์ในเชิงการเมืองการบริหารเข้ามาเกี่ยว ดังที่เห็นกลุ่มแฮกเกอร์ประกาศว่าจะโจมตีหน่วยงานราชการแบบไม่ให้เปิดบริการได้อีก ในปัจจุบันการโจมตีขยายตัวออกไปถึงการโจมตีที่เรียกว่า ดีดอส หรือ DDoS (Distributed Denial of Service) เป็นลักษณะการโจมตีเป็นกลุ่มที่เกิดจากเครื่องคอมพิวเตอร์หลาย ๆ เครื่องโจมตีเป้าหมายในเวลาเดียวกัน ซึ่งการรับมือสถานการณ์ภัยคุกคามในกรณีเว็บไซต์ถูกโจมตีในลักษณะ DDoS นั้น มาตรฐานฉบับนี้จึงมีข้อกำหนดที่เกี่ยวข้องดังนี้

(1) ปิดการเชื่อมต่อของเว็บไซต์
(2) สำเนาข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการถูกบุกรุกเพื่อนำมาใช้ในการวิเคราะห์ เช่น Web Log หรือ Firewall Log
(3) ตรวจสอบหมายเลขไอพีที่ต้องสงสัยว่าจะเป็นการโจมตีด้วยข้อมูลที่สำเนามา โดยปกติจะพบเห็นข้อมูลในลักษณะที่เกิดซ้ำ ๆ ในรูปแบบเดียวกัน เช่น มีการเรียกเว็บไซต์ด้วยยูอาร์แอลหนึ่งเป็นจำนวนมาก หรือมีการส่งข้อมูลมายังบริการหนึ่งซ้ำ ๆ เป็นจำนวนมาก

(4) ปิดกั้นการเข้าถึงจากไอพีแอดเดรสดังกล่าว และแจ้งไปยังผู้ให้บริการเครือข่ายอินเทอร์เน็ตเพื่อหามาตรการที่รองรับในกรณีที่อุปกรณ์ป้องกันของหน่วยงานไม่สามารถรองรับปริมาณข้อมูลที่มากมายได้

(5) บันทึกเหตุการณ์และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด เพื่อใช้เป็นข้อมูลในการป้องกันและการประสานงานกับหน่วยงานที่เกี่ยวข้องในกรณีที่จำเป็น

การจัดการกับเหตุการณ์ภัยคุกคามในกรณีถูกโจมตีด้วยเทคนิค DoS หรือ DDoS นั้น สิ่งสำคัญคือผู้ดูแลต้องมีทักษะในการพิจารณาและคัดแยกไอพีแอดเดรสที่คาดว่าจะเป็นการโจมตีที่รวดเร็วและถูกต้อง เพื่อป้องกันข้อผิดพลาดจากการปิดกั้นการเชื่อมต่อ โดยอาจอาศัยการประมวลผลในลักษณะสถิติ และลักษณะการเข้าใช้งานที่ผิดปกติ รวมถึงยังจำเป็นต้องมีความร่วมมือกับผู้ให้บริการอินเทอร์เน็ตเพื่อให้การป้องกันการโจมตีทำได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

7.1.3 กรณีโดเมนถูกขโมย (Domain Hijack)

การขโมยโดเมน (Domain Hijack) เป็นหนึ่งในรูปแบบการโจมตีที่มีมานานแล้ว และดูเหมือนว่ายังคงเป็นรูปแบบการโจมตีที่พบอยู่เสมอ เหยื่อที่ถูกขโมยโดเมนสามารถเป็นได้ตั้งแต่บริษัทขนาดเล็กและไม่เว้นแม้แต่บริษัทขนาดใหญ่ที่ดำเนินธุรกิจด้านเทคโนโลยีสารสนเทศที่ยังพบว่าตกเป็นเหยื่อในหลายครั้ง โดยจุดประสงค์ของการขโมยข้อมูลนั้นส่วนใหญ่มุ่งประโยชน์ไปยังการหาผลประโยชน์ในหลายลักษณะ ตัวอย่างเช่น ขโมยโดเมนเนมเพื่อนำไปหาประโยชน์โดยการเรียกค่าไถ่จากเจ้าของโดเมนตัวจริง นำไปใช้สร้างสถานการณ์การหลอกลวงหน้า Phishing เป็นต้น ซึ่งการรับมือสถานการณ์ภัยคุกคามในกรณีเว็บไซต์ถูกขโมยโดเมนนั้น สามารถดำเนินการได้ แต่อย่างไรก็ตามจำเป็นต้องมีข้อมูลที่เพียงพอเพื่อให้การแก้ปัญหาทำได้อย่างมีประสิทธิภาพ ดังนั้นมาตรฐานฉบับนี้จึงมีข้อกำหนดที่เกี่ยวข้องดังนี้

(1) เก็บรวบรวมหลักฐานที่เกิดขึ้นทั้งหมด เช่น วัน เดือน ปี ที่ข้อมูลโดเมนเปลี่ยนหน้าจอของโดเมนที่ใช้งาน

(2) ตรวจสอบกับผู้ลงทะเบียนโดเมนถึงสาเหตุของการเปลี่ยนแปลงโดเมน ในบางครั้งพบว่าผู้ดูแลถูกขโมยข้อมูลรหัสผ่านโดยการติดมัลแวร์ ทำให้ผู้ประสงค์ร้ายสามารถเข้าสู่เว็บไซต์บริหารจัดการโดเมนและทำการเปลี่ยนแปลงข้อมูลส่วนบุคคล

(3) แจ้งการถูกขโมยข้อมูลโดเมนกับผู้ลงทะเบียนโดเมนที่เราใช้บริการ โดยนำหลักฐานที่เกี่ยวข้องแนบไปด้วย เช่น หลักฐานการโอนเงิน หลักฐานการตอบรับ เป็นต้น

(4) เมื่อได้รับสิทธิในการบริหารจัดการโดเมนคืนมาแล้ว ให้ตรวจสอบข้อมูลต่าง ๆ ที่ใช้ในการยืนยันตัวตน เช่น ข้อมูลอีเมลผู้จดทะเบียนโดเมน รวมถึงเปลี่ยนรหัสผ่านระบบบริหารจัดการโดเมน

(5) บันทึกเหตุการณ์และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด เพื่อใช้เป็นข้อมูลในการป้องกันและการประสานงานกับหน่วยงานที่เกี่ยวข้องในกรณีที่จำเป็น

ภายหลังจากถูกขโมยโดเมนแล้ว สิ่งที่ยากที่สุดสำหรับผู้ดูแลคือ การทำให้ผู้ให้บริการลงทะเบียนโดเมนเชื่อว่าโดเมนถูกขโมยจริง และยอมคืนสิทธิกลับคืนให้กับผู้ดูแลตัวจริง แต่อย่างไรก็ตามความสำคัญไม่น้อยไปกว่านั้นคือผู้ดูแลจำเป็นต้องทราบสาเหตุของการถูกขโมยโดเมนที่เกิดขึ้น เพื่อเป็นการป้องกันและรับมือสถานการณ์การโจมตีที่อาจเกิดซ้ำอีก

7.2 การใช้โปรแกรมตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์

การใช้โปรแกรมตรวจสอบความมั่นคงปลอดภัยของเครื่องบริการเว็บอย่างสม่ำเสมอจะช่วยให้ผู้ดูแลเครื่องบริการเว็บในการค้นหาข้อบกพร่องของเว็บไซต์ในเบื้องต้น มาตรฐานฉบับนี้จึงมีข้อกำหนดที่เกี่ยวข้องกับการใช้โปรแกรมตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์ดังนี้

(1) เลือกโปรแกรมที่น่าเชื่อถือ หรือ ได้รับการแนะนำจากหน่วยงานที่เกี่ยวข้อง

(2) ปรับรุ่นของโปรแกรมที่ใช้ในการตรวจสอบข้อบกพร่องให้เป็นรุ่นล่าสุดเพื่อที่จะได้ตรวจสอบช่องโหว่ใหม่ ๆ ได้

(3) หากการใช้โปรแกรมส่งผลกระทบกับการให้บริการของเครื่องบริการเว็บ ควรจะมีการสำรองข้อมูลทุกครั้งก่อนมีการใช้โปรแกรมตรวจสอบ

(4) ควรใช้โปรแกรมมากกว่าสองโปรแกรมขึ้นไปในการตรวจสอบเพื่อเปรียบเทียบผลลัพธ์ที่ได้จากการตรวจสอบ

7.3 การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

เว็บไซต์ที่ไม่มีการบันทึกข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลการใช้งานของผู้ใช้ (Log) เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยหรือเหตุขัดข้องทางเทคนิคขึ้นระหว่างการให้บริการ ก็จะไม่สามารถตรวจหาสาเหตุได้ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ หรือ ข้อมูลการเข้าใช้งานเว็บไซต์ (Log) ตามมาตรฐานฉบับนี้ ให้เป็นไปตามข้อกำหนดในพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 และ ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

7.4 การสำรองข้อมูลเว็บไซต์

เพื่อให้กิจกรรมต่าง ๆ ของเว็บไซต์ดำเนินไปได้อย่างราบรื่น การสำรองข้อมูลต่าง ๆ ที่เกี่ยวข้องกับเว็บไซต์อาจไม่ใช่วิธีการป้องกันการโจมตีที่เกิดขึ้น แต่เป็นวิธีที่มักจะมีส่วนเกี่ยวข้องมากที่สุดเมื่อมีเหตุการณ์การโจมตีหรือเหตุการณ์ฉุกเฉินกับเว็บไซต์ เพราะเมื่อพบว่าเว็บไซต์ถูกโจมตี สิ่งที่ทำได้ในเบื้องต้นคือการกู้คืนข้อมูลเวอร์ชั่นก่อนที่จะพบว่าถูกโจมตี เนื่องจากหน่วยงานไม่สามารถทราบได้ว่าการโจมตีที่เกิดขึ้นส่งผลกระทบต่อข้อมูลหรือการทำงานส่วนใดของเว็บไซต์บ้าง เช่น อาจถูกแก้ไขข้อมูลในฐานข้อมูลของเว็บไซต์ในส่วนที่ยากต่อการตรวจสอบโดยปกติ เป็นต้น ทั้งนี้หน้าที่สำคัญอย่างหนึ่งของผู้ดูแลเครื่องบริการเว็บ คือ การดูแลรักษาความสมบูรณ์ของข้อมูลบนเครื่องบริการเว็บ เนื่องจากเครื่องบริการเว็บเป็นเครื่องบริการที่ถูกเปิดเผยและมีความสำคัญมากที่สุดบนระบบเครือข่ายขององค์กร โดยองค์ประกอบหลักในการสำรองข้อมูลบนเครื่องบริการเว็บมี 2 องค์ประกอบ คือ การสำรองข้อมูลและระบบปฏิบัติการบนเครื่องบริการเว็บ และการดูแลรักษาข้อมูลสำรองที่เชื่อถือได้ (Authoritative Copy) ของเว็บไซต์ โดยมีการป้องกันแยกต่างหากจากเครื่องบริการเว็บ เพื่อให้เกิดความมั่นใจว่าจะสามารถกู้คืนเว็บไซต์ให้อยู่ในสภาพสมบูรณ์พร้อมใช้งานได้เหมือนเดิม

ผู้ดูแลเครื่องบริการเว็บจำเป็นต้องดำเนินการสำรองข้อมูลของเครื่องบริการเว็บอย่างสม่ำเสมอ เนื่องจากอาจจะเกิดความผิดพลาดขึ้นกับเครื่องบริการเว็บได้จากการกระทำที่ประสงค์ร้ายหรือโดยไม่ตั้งใจ หรือจากความขัดข้องของฮาร์ดแวร์และซอฟต์แวร์ นอกจากนี้ หน่วยงานภาครัฐหรือองค์กรต่าง ๆ ได้มีการกำหนดกฎเกณฑ์ข้อบังคับ

ในการสำรองและการเก็บรักษาข้อมูลของเครื่องบริการเว็บ องค์กรต่าง ๆ จำเป็นต้องสร้างนโยบายในการสำรองข้อมูลของเครื่องบริการเว็บ

ดังนั้นมาตรฐานฉบับนี้จึงมีข้อกำหนดที่เกี่ยวกับการจัดทำแนวปฏิบัติในการสำรองข้อมูลของเครื่องบริการเว็บ ซึ่งอ้างอิงจากแนวทางตามมาตรฐานของ NIST [1] ดังนี้

(1) แนวปฏิบัติต้องสอดคล้องกับข้อกำหนดทางกฎหมาย
(2) แนวปฏิบัติต้องสอดคล้องกับข้อผูกพันทางสัญญา
(3) แนวปฏิบัติต้องสอดคล้องกับแนวนโยบายที่เกี่ยวข้องขององค์กร
(4) จุดประสงค์และขอบเขตของแนวปฏิบัติ
(5) บทบาทและหน้าที่ของผู้เกี่ยวข้อง
(6) เครื่องบริการเว็บที่เกี่ยวข้องกับแนวปฏิบัติ
(7) คำนิยามของศัพท์เฉพาะ โดยเฉพาะในทางกฎหมายและทางเทคนิค
(8) รายละเอียดของกฎหมาย ข้อผูกพันสัญญา และแนวนโยบายขององค์กรที่เกี่ยวข้อง
(9) ความถี่ของการสำรองข้อมูล
(10) ขั้นตอนสำหรับยืนยันว่าข้อมูลที่มีการสำรองได้รับการดูแลรักษาและการป้องกันอย่างเหมาะสม
(11) ขั้นตอนสำหรับยืนยันว่าข้อมูลได้รับการทำลายหรือมีการเก็บรักษาเมื่อไม่มีความจำเป็นในการใช้งาน
(12) ขั้นตอนสำหรับยืนยันว่าข้อมูลที่มีการสำรองสามารถถูกเรียกออกมาใช้งานได้อย่างถูกต้องในกรณีที่มีการร้องขอ
(13) ความรับผิดชอบของผู้ที่มีส่วนร่วมในการเก็บรักษา การป้องกัน และการทำลายข้อมูล
(14) ระยะเวลาในการเก็บรักษาข้อมูลแต่ละประเภท
(15) หน้าที่รับผิดชอบของทีมสำรองข้อมูล ในกรณีที่องค์กรมีทีมดังกล่าว

ภาคผนวก ก. แบบประเมินสำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
การวางแผนเพื่อบริหารจัดการเว็บไซต์ (หัวข้อ 4)				
1	การวางแผนด้านความมั่นคงปลอดภัยของเว็บไซต์ (หัวข้อ 4.1)			
1.1	มีการวางแผนเพื่อบริหารจัดการเครื่องบริการเว็บ (หัวข้อ 4.1 ข้อ 1)			
1.2	จัดลำดับความเสี่ยงของภัยคุกคามที่คาดว่าจะเกิดขึ้นกับเว็บไซต์ (หัวข้อ 4.1 ข้อ 2)			
1.3	ได้กำหนดมาตรการที่เกี่ยวข้องเพื่อป้องกันภัยคุกคามที่มีความสำคัญ (หัวข้อ 4.1 ข้อ 3)			
การตั้งค่าเครื่องบริการเว็บอย่างมั่นคงปลอดภัย (หัวข้อที่ 5)				
2	การตั้งค่าโปรแกรมสำหรับให้บริการเว็บ (Web Server Software) (หัวข้อที่ 5.1)			
2.1	มีการตรวจสอบและปรับปรุงส่วนประกอบของโปรแกรมสำหรับให้บริการเว็บให้เป็นเวอร์ชั่นปัจจุบันอย่างสม่ำเสมอ (หัวข้อที่ 5.1 ข้อ 1)			
2.2	มีการควบคุมข้อความแจ้งเตือนหรือข้อความแสดงข้อผิดพลาด (Error Message) ไม่ให้แสดงข้อมูลที่เป็นประโยชน์ต่อผู้ประสงค์ร้าย (หัวข้อที่ 5.1 ข้อ 2)			
2.3	ได้กำหนดสิทธิในการเข้าถึงสารบบ (Directory) ที่ใช้เก็บไฟล์หรือโปรแกรมต่าง ๆ ที่เกี่ยวข้องกับเครื่องบริการเว็บให้เหมาะสม เช่น กำหนดสิทธิโฟลเดอร์ที่เก็บหน้าเว็บเพจของระบบหลังบ้าน อนุญาตให้เฉพาะผู้ดูแลเข้าถึงได้เท่านั้น (หัวข้อที่ 5.1 ข้อ 3)			
2.4	มีการตรวจสอบและจัดการลบ ตัวอย่างโปรแกรม ตัวอย่างไฟล์ข้อมูล บัญชีผู้ใช้ที่ไม่ได้ใช้งาน เช่น บัญชีซึ่งมีการใช้งานระหว่างกระบวนการติดตั้งเครื่องบริการเว็บทั้งหมด (หัวข้อที่ 5.1 ข้อ 4)			

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
2.5	ได้ตรวจสอบไม่ให้มีการใช้ค่าเริ่มต้นของ ชื่อสารบบ ชื่อไฟล์ข้อมูล ตำแหน่งไฟล์ข้อมูล รหัสผ่าน ที่มากับการติดตั้งเครื่องบริการเว็บ (หัวข้อที่ 5.1 ข้อ 5)			
2.6	มีการควบคุมการเข้าถึงเครื่องบริการเว็บ และจำกัดหมายเลขไอพีปลายทางหรือยูอาร์แอลที่อนุญาตให้เครื่องบริการเว็บสามารถเชื่อมต่อ เช่น การกำหนด IP Whitelist ที่สามารถเข้าถึงเครื่องบริการเว็บ (หัวข้อที่ 5.1 ข้อ 6)			
2.7	ปิดบริการต่าง ๆ ที่ไม่จำเป็นบนเครื่องบริการเว็บ โดยเฉพาะบริการประเภท Remote Access (หัวข้อที่ 5.1 ข้อ 7)			
3	การตั้งค่าระบบบริหารจัดการเว็บไซต์ (CMS) (หัวข้อที่ 5.2)			
3.1	มีการกำหนดสิทธิการใช้งาน (Permission) และการควบคุมการเข้าถึง (Access control) (หัวข้อที่ 5.2 ข้อ 1)			
3.2	ตรวจสอบว่ามีไฟล์หรือโปรแกรมเสริม (Plug-in Program) ที่ไม่จำเป็นหรือไม่ได้ใช้งานปรากฏอยู่หรือไม่ ถ้าตรวจพบผู้ดูแลเครื่องบริการเว็บต้องลบหรือถอนการติดตั้งไฟล์หรือโปรแกรมเสริมนั้นทันที (หัวข้อที่ 5.2 ข้อ 2)			
3.3	ตรวจสอบการอัพเดตเวอร์ชั่นของระบบบริหารจัดการเว็บไซต์อยู่เสมอ และอัพเดตเวอร์ชั่นให้เป็นปัจจุบัน (หัวข้อที่ 5.2 ข้อ 3)			
3.4	ลบบัญชีผู้ใช้ที่มากับการติดตั้งระบบบริหารจัดการเว็บไซต์ เปลี่ยนชื่อผู้ใช้ของบัญชีผู้ใช้นั้นหรือเปลี่ยนรหัสผ่านของบัญชีผู้ใช้นั้น ให้เป็นรหัสผ่านที่มีความมั่นคงปลอดภัยแทน (หัวข้อที่ 5.2 ข้อ 4)			
3.5	เปลี่ยน Table prefix ของฐานข้อมูลที่มาในระหว่างการติดตั้งระบบบริหารจัดการเว็บไซต์ (หัวข้อที่ 5.2 ข้อ 5)			
4	การตั้งค่าฐานข้อมูล (Database system) (หัวข้อที่ 5.3)			
4.1	มีการตั้งค่าฐานข้อมูล อนุญาตให้เฉพาะโปรแกรมประยุกต์ (Application) และเครื่องบริการเว็บที่เกี่ยวข้องเข้าถึงได้เท่านั้น (โปรแกรมประยุกต์ที่ใช้เกี่ยวข้องกับฐานข้อมูล เช่น MySQL Workbench) (หัวข้อที่ 5.3 ข้อ 1)			

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
4.2	ควบคุมการเข้าถึงระบบฐานข้อมูลด้วยระบบรักษาความมั่นคงปลอดภัย เช่น ด่านกันบุกรุกหรือไฟร์วอลล์ (Firewall) (หัวข้อที่ 5.3 ข้อ 2)			
4.3	ตรวจสอบและปิดบริการ (Services, Extension) ที่ไม่จำเป็นหรือไม่ได้ใช้งาน ในระบบฐานข้อมูล เช่น PHPMyAdmin (หัวข้อที่ 5.3 ข้อ 3)			
4.4	จัดให้มีการทบทวนบัญชีผู้ใช้ภายในฐานข้อมูลตามระยะเวลาที่กำหนด และลบบัญชีผู้ใช้ที่ไม่ได้มีการใช้งานออกจากระบบฐานข้อมูล (หัวข้อที่ 5.3 ข้อ 4)			
4.5	ปิดบัญชีผู้ใช้ที่มาพร้อมกับการติดตั้งฐานข้อมูล หรือเปลี่ยนรหัสผ่านของบัญชีผู้ใช้ดังกล่าว ให้เป็นรหัสผ่านที่มีความมั่นคงปลอดภัย (หัวข้อที่ 5.3 ข้อ 5)			
4.6	กำหนดค่าติดตั้งระบบฐานข้อมูลเพื่อไม่อนุญาตให้ใช้งานรหัสผ่านที่มีค่าว่าง (Null Password) (หัวข้อที่ 5.3 ข้อ 6)			
4.7	ตรวจสอบและลบแฟ้มชั่วคราว (Temporary File) ที่ถูกสร้างขึ้นระหว่างการติดตั้งระบบฐานข้อมูล (หัวข้อที่ 5.3 ข้อ 7)			
4.8	ปรับปรุงเวอร์ชั่นของโปรแกรมระบบฐานข้อมูล หรืออัพเดต Patch จากบริษัทผู้พัฒนาซอฟต์แวร์ให้เป็นเวอร์ชั่นล่าสุดเสมอ (หัวข้อที่ 5.3 ข้อ 8)			
4.9	กำหนดสิทธิการใช้งาน (Permission) และการควบคุมการเข้าถึง (Access Control) ให้เหมาะสมกับบทบาทและหน้าที่ของผู้ใช้ (หัวข้อที่ 5.3 ข้อ 9)			
4.10	รหัสผ่านที่เก็บในฐานข้อมูล ต้องมีการเข้ารหัสเสมอ (หัวข้อที่ 5.3 ข้อ 10)			
5	การตั้งค่า Server-Side Script Engine (หัวข้อที่ 5.4)			
5.1	มีการควบคุมการเข้าถึงไฟล์หรือสารบบต่าง ๆ ให้เหมาะสมกับบทบาทของผู้ใช้ (Permission and Access Control) (หัวข้อที่ 5.4 ข้อ 1)			
5.2	ปรับปรุงเวอร์ชั่นของ Server-Side Script Engine หรืออัพเดต Patch จากบริษัทผู้พัฒนาซอฟต์แวร์ให้เป็นเวอร์ชั่นล่าสุดเสมอ (หัวข้อที่ 5.4 ข้อ 2)			

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
5.3	กำหนดค่าติดตั้งไม่ให้ Server-Side Script Engine แสดงข้อมูลเวอร์ชั่นของ Server-Side Script Engine ที่เครื่องบริการเว็บใช้งาน ใน HTTP Header (หัวข้อที่ 5.4 ข้อ 3)			
5.4	กำหนดค่าติดตั้ง Server-Side Script Engine ไม่ให้มีการแสดงรายละเอียดของข้อความแสดงข้อผิดพลาด (Error message) หากต้องมีรายละเอียดควรจะแสดงข้อมูลเท่าที่จำเป็น (หัวข้อที่ 5.4 ข้อ 4)			
6	การกำหนดและรักษารหัสผ่าน (หัวข้อที่ 5.5)			
6.1	ได้มีการจัดทำนโยบายการตั้งค่ารหัสผ่านให้มีความมั่นคงปลอดภัย (Strong Password) (หัวข้อที่ 5.5 ข้อ 1)			
6.2	กำหนดนโยบายให้มีการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ (หัวข้อที่ 5.5 ข้อ 2)			
6.3	ไม่เก็บรหัสผ่านที่ไม่มีการเข้ารหัสลับบนเครื่องบริการเว็บ หากจำเป็นต้องมีการเก็บรหัสผ่านควรอยู่ในรูปที่มีการเข้ารหัสลับตามที่มาตรฐานด้านความมั่นคงปลอดภัยกำหนด (หัวข้อที่ 5.5 ข้อ 3)			
การพัฒนาโปรแกรมประยุกต์บนเครื่องบริการเว็บอย่างมั่นคงปลอดภัย (หัวข้อที่ 6)				
7	มีการป้องกันการโจมตีจากเทคนิค SQL Injection (หัวข้อที่ 6.1)			
7.1	มีการจัดทำ Prepared Statement และ/หรือ Stored Procedure ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.1 ข้อ 1)			
7.2	มีการจัดทำ Input Validation ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.1 ข้อ 2)			
7.3	มีการทำ Encoding หรือทำ Sanitization ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.1 ข้อ 3)			
8	การป้องกันการโจมตีจากเทคนิค Session Hijacking (หัวข้อที่ 6.2)			
8.1	Session ID ที่มีข้อมูลการรับรองตัวตนของผู้ใช้บริการ (User Authentication Credential) ต้องมีการเข้ารหัสลับ (หัวข้อที่ 6.2 ข้อ 1)			

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
8.2	ต้องกำหนด Session Timeout ในระยะเวลาที่เหมาะสมของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.2 ข้อ 2)			
8.3	กำหนดค่า Session ID เป็นค่าสุ่มที่คาดเดาไม่ได้และไม่มีการใช้ซ้ำในระยะเวลาที่เหมาะสม (หัวข้อที่ 6.2 ข้อ 3)			
8.4	ต้องส่งค่า Session ID ในช่องทางการสื่อสารที่มีการเข้ารหัสลับ (Encrypted connection) (หัวข้อที่ 6.2 ข้อ 4)			
9	การป้องกันการโจมตีจากเทคนิค Cross-Site Scripting ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.3)			
9.1	มีการทำ Input Validation ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.3 ข้อ 1)			
9.2	มีการตรวจสอบข้อมูลชุดคำสั่งในเว็บไซต์ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.3 ข้อ 2)			
9.3	มีการทำ Output Validation ในลักษณะ Sanitization ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.3 ข้อ 3)			
9.4	มีการใช้งาน HTTPOnly Cookie flag ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.3 ข้อ 4)			
10	การป้องกันการโจมตีจากเทคนิค CSRF (หัวข้อที่ 6.4)			
10.1	มีการใช้งาน Unique Token และ/หรือตรวจสอบ Referrer ร่วมกับการส่งข้อมูล หรือคำสั่งผ่านแบบฟอร์ม ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.4 ข้อ 1)			
10.2	มีการใช้ Captcha ของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.4 ข้อ 2)			
11	การป้องกันการโจมตีจากปัญหาข้อมูลลับรั่วไหล (Sensitive Data Exposure) (หัวข้อที่ 6.5)			
11.1	มีการออกแบบและควบคุมข้อความแจ้งเตือนหรือข้อความแสดงข้อผิดพลาด (Notification or Error Message) ไม่ให้แสดงข้อมูลที่เป็นประโยชน์ต่อผู้ประสงค์ร้ายของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.5 ข้อ 1)			
11.2	พัฒนาเว็บไซต์โดยไม่ให้มีการใช้งาน Autocomplete ในแบบฟอร์มสำคัญของโปรแกรมประยุกต์บนเว็บ (หัวข้อที่ 6.5 ข้อ 2)			

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
11.3	ไม่ใช้ชื่อ URL ที่คาดเดาได้ง่ายซึ่งใช้ในการเข้าถึงหน้าเว็บสำหรับผู้ดูแลเครื่องบริการเว็บ (Administrator Control Panel Web Page) (หัวข้อที่ 6.5 ข้อ 3)			
การรับมือสถานการณ์ภัยคุกคามที่เกิดจากการโจมตีเว็บไซต์ (Security Incident Handling) (หัวข้อที่ 7)				
12	การรับมือภัยคุกคามที่เกิดขึ้นกับเว็บไซต์ (หัวข้อที่ 7.1)			
12.1	กรณีเว็บไซต์ถูกบุกรุกและควบคุม (Intrusions) (หัวข้อที่ 7.1.1)			
12.1.1	ปิดการเชื่อมต่อของเว็บไซต์ (หัวข้อที่ 7.1.1 ข้อ 1)			
12.1.2	สำเนาข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการถูกบุกรุกเพื่อนำมาใช้ในการวิเคราะห์ (หัวข้อที่ 7.1.1 ข้อ 2)			
12.1.3	ตรวจสอบช่องทางการโจมตีและช่องโหว่ของเว็บไซต์ด้วยข้อมูลที่สำเนามา (หัวข้อที่ 7.1.1 ข้อ 3)			
12.1.4	ระหว่างการตรวจสอบจัดสร้างเว็บเพจแบบ Static ขึ้นมาทดแทนเป็นการชั่วคราว เพื่อชี้แจงสถานการณ์การปิดปรับปรุง (หัวข้อที่ 7.1.1 ข้อ 4)			
12.1.5	กู้คืนโปรแกรมที่เกี่ยวข้อง ข้อมูลเว็บ และฐานข้อมูลที่เกี่ยวข้องกับเว็บไซต์เป็นเวอร์ชั่นก่อนหน้าที่จะถูกโจมตี (หัวข้อที่ 7.1.1 ข้อ 5)			
12.1.6	ตรวจสอบช่องโหว่ของเว็บไซต์ (เวอร์ชั่นก่อนหน้าที่จะถูกโจมตี) ด้วยการทำ Vulnerability Assessment (หัวข้อที่ 7.1.1 ข้อ 6)			
12.1.7	แก้ไขช่องโหว่ของเว็บไซต์ที่ทำให้ผู้ประสงค์ร้ายสามารถเจาะเพื่อเข้าควบคุมระบบได้ (หัวข้อที่ 7.1.1 ข้อ 7)			
12.1.8	บันทึกเหตุการณ์และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด (หัวข้อที่ 7.1.1 ข้อ 8)			
12.2	กรณีเว็บไซต์ถูกโจมตีในลักษณะ DoS (Denial of Service) (หัวข้อที่ 7.1.2)			
12.2.1	ปิดการเชื่อมต่อของเว็บไซต์ (หัวข้อที่ 7.1.2 ข้อ 1)			

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
12.2.2	สำเนาข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการถูกบุกรุกเพื่อนำมาใช้ในการวิเคราะห์ (หัวข้อที่ 7.1.2 ข้อ 2)			
12.2.3	ตรวจสอบหมายเลขไอพีที่ต้องสงสัยว่าจะเป็นการโจมตีด้วยข้อมูลที่สำเนามา (หัวข้อที่ 7.1.2 ข้อ 3)			
12.2.4	ปิดกั้นการเข้าถึงจากไอพีแอดเดรสดังกล่าว และแจ้งไปยังผู้ให้บริการเครือข่ายอินเทอร์เน็ตเพื่อหามาตรการที่รองรับ (หัวข้อที่ 7.1.2 ข้อ 4)			
12.2.5	บันทึกเหตุการณ์และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด (หัวข้อที่ 7.1.2 ข้อ 5)			
12.3	กรณีโดเมนถูกขโมย (Domain Hijack) (หัวข้อที่ 7.1.3)			
12.3.1	เก็บรวบรวมหลักฐานที่เกิดขึ้นทั้งหมด เช่น วัน เดือน ปีที่ข้อมูลโดเมนเปลี่ยน หน้าจอของโดเมนที่ใช้งาน (หัวข้อที่ 7.1.3 ข้อ 1)			
12.3.2	ตรวจสอบกับผู้ลงทะเบียนโดเมนถึงสาเหตุของการเปลี่ยนแปลงโดเมน (หัวข้อที่ 7.1.3 ข้อ 2)			
12.3.3	แจ้งการถูกขโมยข้อมูลโดเมนกับผู้ลงทะเบียนโดเมนที่ใช้บริการโดยนำหลักฐานที่เกี่ยวข้องแนบไปด้วย (หัวข้อที่ 7.1.3 ข้อ 3)			
12.3.4	เมื่อได้รับสิทธิในการบริหารจัดการโดเมนคืนมาแล้ว ให้ตรวจสอบข้อมูลต่าง ๆ ที่ใช้ในการยืนยันตัวตน รวมถึงเปลี่ยนรหัสผ่านระบบบริหารจัดการโดเมน (หัวข้อที่ 7.1.3 ข้อ 4)			
12.3.5	บันทึกเหตุการณ์และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด (หัวข้อที่ 7.1.3 ข้อ 5)			
13	การใช้โปรแกรมตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์ (หัวข้อที่ 7.2)			
13.1	เลือกโปรแกรมที่น่าเชื่อถือ หรือ ได้รับการแนะนำจากหน่วยงานที่เกี่ยวข้อง (หัวข้อที่ 7.2 ข้อ 1)			
13.2	ปรับรุ่นของโปรแกรมที่ใช้ในการตรวจสอบข้อบกพร่องให้เป็นรุ่นล่าสุด (หัวข้อที่ 7.2 ข้อ 2)			

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
13.3	หากการใช้โปรแกรมส่งผลกระทบกับการให้บริการของเครื่องบริการเว็บ ควรจะมีการสำรองข้อมูลทุกครั้งก่อนมีการใช้โปรแกรมตรวจสอบ (หัวข้อที่ 7.2 ข้อ 3)			
13.4	ควรใช้โปรแกรมมากกว่าสองโปรแกรมขึ้นไปในการตรวจสอบเพื่อเปรียบเทียบผลลัพธ์ที่ได้จาก (หัวข้อที่ 7.2 ข้อ 4)			
14	การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (หัวข้อที่ 7.3)			
14.1	การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ หรือ ข้อมูลการใช้งานของผู้ใช้ (Log) ตามมาตรฐานฉบับนี้ ปฏิบัติตามข้อกำหนดในพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 และ ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 (หัวข้อที่ 7.3)			
15	การสำรองข้อมูลเว็บไซต์ (หัวข้อที่ 7.4)			
15.1	มีการจัดทำแนวปฏิบัติในการสำรองข้อมูลของเครื่องบริการเว็บ (1) แนวปฏิบัติต้องสอดคล้องกับข้อกำหนดทางกฎหมาย (2) แนวปฏิบัติต้องสอดคล้องกับข้อผูกพันทางสัญญา (3) แนวปฏิบัติต้องสอดคล้องกับแนวนโยบายที่เกี่ยวข้องขององค์กร (4) จุดประสงค์และขอบเขตของแนวปฏิบัติ (5) บทบาทและหน้าที่ของผู้เกี่ยวข้อง (6) เครื่องบริการเว็บที่เกี่ยวข้องกับแนวปฏิบัติ (7) คำนิยามของศัพท์เฉพาะ โดยเฉพาะในทางกฎหมายและทางเทคนิค (8) รายละเอียดของกฎหมาย ข้อผูกพันสัญญา และแนวนโยบายขององค์กรที่เกี่ยวข้อง (9) ความถี่ของการสำรองข้อมูล (10) ขั้นตอนสำหรับยืนยันว่าข้อมูลที่มีการสำรองได้รับการดูแลรักษาและการป้องกันอย่างเหมาะสม			

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์
(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
	(11) ขั้นตอนสำหรับยืนยันว่าข้อมูลได้รับการทำลายหรือมีการเก็บรักษาเมื่อไม่มีความจำเป็นในการใช้งาน (12) ขั้นตอนสำหรับยืนยันว่าข้อมูลที่มีการสำรองสามารถถูกเรียกออกมาใช้งานได้อย่างถูกต้องในกรณีที่มีการร้องขอ (13) ความรับผิดชอบของผู้ที่มีส่วนร่วมในการเก็บรักษา การป้องกัน และการทำลายข้อมูล (14) ระยะเวลาในการเก็บรักษาข้อมูลแต่ละประเภท (15) หน้าที่รับผิดชอบของทีมสำรองข้อมูล (หากมี)			

แบบฟอร์มสำหรับการแก้ไขรายการที่ยังต้องปรับปรุง (จากการตรวจสอบสถานะความมั่นคงปลอดภัย)

ตัวอย่างของแบบฟอร์มสำหรับการแก้ไขรายการที่ยังต้องปรับปรุงซึ่งเกิดจากการตรวจสอบสถานะความมั่นคงปลอดภัยของเว็บไซต์ตามข้อกำหนดและแนวทางในมาตรฐานฉบับนี้ และเมื่อพบรายการที่ไม่เป็นไปตามข้อกำหนดก็ให้ระบุรายการแก้ไขลงในแบบฟอร์มพร้อมกับกำหนดระยะเวลาในการแก้ไขเพื่อนำเสนอต่อผู้ที่เกี่ยวข้องต่อไป

วันที่ตรวจสอบสถานะ			**เว็บไซต์**				
โดยหน่วยงาน							
ลำดับที่	**วันที่รายงาน**	**คำอธิบายรายการที่ยังต้องปรับปรุง**	**สาเหตุ**	**การแก้ไขชั่วคราว**	**สิ่งที่ต้องแก้ไข**		
					รายการแก้ไข	**รับผิดชอบโดย**	**วันที่แล้วเสร็จ**

ภาคผนวก ข. รูปแบบการสื่อสารอย่างมั่นคงปลอดภัยระหว่างโปรแกรมค้นดูเว็บและเครื่องบริการเว็บ

โพรโทคอล SSL (Secure Socket Layer Protocol) และ TLS (Transport Layer Security Protocol) เป็นโพรโทคอลที่กำหนดรูปแบบการสื่อสารที่มีความมั่นคงปลอดภัย ซึ่งสามารถป้องกันการสื่อสารของโปรแกรมประยุกต์ในระบบรับ-ให้ (Client-Server System) จากการลอบฟัง (Eavesdropping) การแก้ไขให้เสียหาย (Tampering) และ การปลอมแปลงข้อความที่ใช้ในการสื่อสาร (Message Forgery) โพรโทคอล SSL ถูกนำมาใช้งานครั้งแรกในปี 1994 โดยบริษัท Netscape Communications และที่ผ่านมาได้มีการปรับปรุงเพื่อแก้ไขปัญหาความมั่นคงปลอดภัยของโพรโทคอลไป 2 ครั้ง และเวอร์ชั่นสุดท้ายของ SSL คือเวอร์ชั่น 3 ซึ่งถูกพัฒนาในปี 1996 ตามเอกสาร RFC 6101 [8] ในขณะที่โพรโทคอล TLS ถูกพัฒนาต่อยอดเพื่อแก้ไขปัญหาความมั่นคงปลอดภัยในโพรโทคอล SSL ในปี 1999 โดย IETF ซึ่งได้มีการกำหนดเป็นมาตรฐานและได้มีการพัฒนาปรับปรุงต่อเนื่องกันมาเป็น TLS เวอร์ชั่น 1.2 ในปี 2008 ตาม RFC 5246 [9] เป็นเวอร์ชั่นปัจจุบันที่ได้รับการยอมรับในเรื่องของความมั่นคงปลอดภัยมากที่สุด อย่างไรก็ตามในปัจจุบันเครื่องบริการเว็บและโปรแกรมค้นดูเว็บไม่ได้รองรับโพรโทคอล SSL/TLS ทุกเวอร์ชั่น ทั้งนี้จากผลการสำรวจเว็บไซต์ทั่วไป [10] เมื่อเดือนมกราคม พ.ศ. 2557 พบว่าเว็บไซต์มากกว่าร้อยละ 99 รองรับโพรโทคอล TLS 1.0 และ SSL 3.0 ในขณะที่เว็บไซต์ที่รองรับ TLS 1.1 และ TLS 1.2 มีจำนวนร้อยละ 23 และร้อยละ 25 ตามลำดับ

โพรโทคอล SSL/TLS กำหนดรูปแบบการสื่อสารที่มีความมั่นคงปลอดภัยด้วยกระบวนการพื้นฐานที่สำคัญ 3 กระบวนการซึ่งได้แก่

1. การยืนยันตัวตนของเครื่องบริการเว็บ

   โพรโทคอล SSL/TLS อนุญาตให้ผู้ใช้บริการยืนยันเอกลักษณ์ของเครื่องบริการเว็บ (Web Server's Identity) โดยใช้เทคนิคของการเข้ารหัสโดยใช้กุญแจสาธารณะตรวจสอบใบรับรองอิเล็กทรอนิกส์ของเครื่องบริการเว็บว่าออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ที่น่าเชื่อถือหรือไม่และใบรับรองอิเล็กทรอนิกส์ดังกล่าวยังสามารถใช้งานได้ ไม่หมดอายุหรืออยู่ในรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์
2. การยืนยันตัวตนของผู้ใช้บริการ

   เครื่องบริการเว็บสามารถยืนยันเอกลักษณ์ของผู้ใช้บริการ ด้วยการตรวจสอบใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการด้วยเทคนิคของการเข้ารหัสโดยใช้กุญแจสาธารณะเช่นกัน ส่วนใหญ่แล้วในกรณีที่มีการยืนยันตัวตนของผู้ใช้บริการ ผู้ใช้บริการจะมีการยืนยันตัวตนของเครื่องบริการเว็บควบคู่กันไป ซึ่งเป็นการยืนยันตัวตนทั้งสองฝ่าย (Mutual Authentication)
3. การเข้ารหัสข้อมูลที่ใช้ในการสื่อสาร

   โพรโทคอล SSL/TLS สามารถใช้ในการเข้ารหัสข้อมูลที่ใช้รับส่งกันระหว่างเครื่องบริการเว็บและโปรแกรมค้นดูเว็บ โดยการเลือกกระบวนการเข้ารหัสข้อมูลที่มีความมั่นคงปลอดภัยและเหมาะสมกับการสื่อสาร นอกจากนี้ยังสามารถตรวจสอบได้ว่าข้อมูลที่มีการรับส่งนั้นมีการแก้ไขหรือปลอมแปลงหรือไม่

เว็บไซต์ที่ไม่ได้มีการนำ SSL/TLS มาใช้งาน จะเปิดโอกาสให้ผู้ประสงค์ร้ายสามารถลอบฟัง แก้ไขและปลอมแปลงข้อมูลที่ใช้รับ-ส่งระหว่างเครื่องบริการเว็บและผู้ใช้บริการได้

1. การเลือกเวอร์ชั่นของ SSL/TLS ที่เหมาะสม

1.1 โพรโทคอล SSL/TLS มีหลายเวอร์ชั่น แต่ละเวอร์ชั่นมีคุณสมบัติด้านความมั่นคงปลอดภัยไม่เหมือนกัน ซึ่งในแต่ละเวอร์ชั่นของ SSL/TLS มีรายละเอียดดังนี้

(1) SSL เวอร์ชั่น 2 มีความมั่นคงปลอดภัยต่ำและปัจจุบันไม่มีการใช้งาน

(2) SSL เวอร์ชั่น 3 พัฒนามาจาก SSL เวอร์ชั่น 2 แต่ในปัจจุบันหน่วยงานส่วนใหญ่ไม่นิยมใช้งาน SSL เวอร์ชั่น 3 เนื่องจาก SSL เวอร์ชั่นนี้ไม่มีคุณสมบัติที่สำคัญบางอย่าง อีกทั้งผู้ใช้บริการส่วนใหญ่หันไปใช้งาน TLS v1.0

(3) TLS เวอร์ชั่น 1.0 พัฒนามาจาก SSL เวอร์ชั่น 3 คุณสมบัติส่วนใหญ่แล้วมีความมั่นคงปลอดภัย เมื่อใช้งานกับองค์ประกอบอื่น ๆ อย่างระมัดระวัง ผ่านโพรโทคอล HTTP

(4) TLS เวอร์ชั่น 1.1 และ 1.2 แก้ไขปัญหาในด้านความมั่นคงปลอดภัยที่เป็นที่รู้จักทั้งหมด

ในปัจจุบันโปรแกรมค้นดูเว็บมีการรองรับ SSL/TLS ในแต่ละเวอร์ชั่นดังต่อไปนี้

(1) Mozilla Firefox เวอร์ชั่น 27 ขึ้นไป รองรับ TLS v1.2 เวอร์ชั่นที่ต่ำกว่านั้นรองรับเฉพาะ SSL 3.0 และ TLS 1.0

(2) Google Chrome เวอร์ชั่น 30 ขึ้นไป รองรับ TLS v1.2

(3) Internet Explorer เวอร์ชั่น 8 ขึ้นไป รองรับ SSL 2.0, SSL 3.0, TLS v1.0, TLS v1.1, TLS v1.2

1.2 แนวทางการเลือกใช้เวอร์ชั่นของโพรโทคอล SSL/TLS มีดังนี้

(1) TLS v1.2 ควรจะนำมาใช้เป็นโพรโทคอลหลัก เนื่องจากในเวอร์ชั่นนี้ มีองค์ประกอบและมีการแก้ปัญหาในด้านความมั่นคงปลอดภัยที่ไม่มีในโพรโทคอลเวอร์ชั่นก่อน ๆ ซึ่งถ้า แพลตฟอร์มของเครื่องบริการเว็บไม่รองรับ TLS v1.2 ก็ให้วางแผนเพื่อปรับปรุง หรือถ้าบริการของผู้ให้บริการไม่รองรับ ก็ให้เสนอไปยังผู้ให้บริการนั้น ๆ เพื่ออัพเดตต่อไปในอนาคต

(2) ในขั้นต้น แนะนำว่าเครื่องบริการเว็บต้องรองรับ TLS v1.0/ TLS v1.1 เนื่องจากยังมี เครื่องผู้ใช้บริการใช้โพรโทคอลเวอร์ชั่นอื่น ๆ อย่างหลากหลาย ซึ่ง TLS ของทั้ง 2 เวอร์ชั่นนี้ จะรองรับความมั่นคงปลอดภัยในการใช้งานที่เพียงพอสำหรับเว็บไซต์

2. การเลือกวิธีการเข้ารหัสของ SSL/TLS ที่เหมาะสม

ในการติดต่อสื่อสารและแลกเปลี่ยนข้อมูลอย่างมั่นคงปลอดภัย จะต้องทำให้แน่ใจได้ว่าการติดต่อสื่อสารนั้นเกิดขึ้นโดยตรงระหว่างผู้ส่งข้อมูลและผู้รับข้อมูลที่ต้องการและไม่มีการดักฟังข้อมูลโดยบุคคลอื่น ซึ่งในโพรโทคอล SSL และ TLS ได้มีการใช้ Cipher Suite สำหรับกำหนดระดับความมั่นคงปลอดภัยของการติดต่อสื่อสารที่เกิดขึ้น โดย Cipher Suite จะประกอบด้วยหน่วยโครงสร้างต่าง ๆ ที่นำมาประกอบกันทำให้เกิดความมั่นคงปลอดภัยในระดับต่าง ๆ ซึ่งสามารถปรับเปลี่ยนหน่วยโครงสร้างหน่วยใดหน่วยหนึ่งได้ หากตรวจพบว่าไม่มีระดับความมั่นคงปลอดภัยเพียงพอ โดยโพรโทคอล SSL/TLS จะมีการใช้โพรโทคอล Handshake ในการตกลงวิธีการสื่อสารระหว่างเครื่องบริการเว็บและเครื่องรับบริการเว็บด้วยการเลือก Cipher Suite ไปใช้งาน เพื่อการยืนยันตัวตนของแต่ละฝ่าย การส่งใบรับรองอิเล็กทรอนิกส์ระหว่างกัน และการสร้าง Session Key ต่าง ๆ ทั้งนี้ การเลือกวิธีการเข้ารหัสของ SSL/TLS

ที่เหมาะสมขึ้นอยู่กับหลายปัจจัยตามแต่ละองค์กร ซึ่งไม่จำเป็นที่จะต้องใช้วิธีการเข้ารหัสที่มีความมั่นคงปลอดภัยสูงสุดเสมอไป โดยปัจจัยเบื้องต้นในการเลือกใช้ขั้นตอนวิธีการเข้ารหัสมีดังนี้

(1) ความมั่นคงปลอดภัยที่ต้องการ
   ก. ความสำคัญของข้อมูล โดยหากข้อมูลมีความสำคัญมาก ควรใช้วิธีการเข้ารหัสที่มีความมั่นคงปลอดภัยสูง
   ข. ระยะเวลาของข้อมูล โดยหากข้อมูลมีความสำคัญแต่อยู่ในระยะเวลาสั้น (เช่น หลักวันแทนที่จะเป็นหลักปี) ก็สามารถใช้วิธีการเข้ารหัสที่มีระดับความมั่นคงปลอดภัยลดลงมา
   ค. ภัยคุกคามต่อข้อมูล โดยหากข้อมูลมีระดับภัยคุกคามสูง ก็ควรใช้วิธีการเข้ารหัสที่มีความมั่นคงปลอดภัยสูง
   ง. มาตรการการป้องกันอื่น ๆ ซึ่งสามารถใช้แทนเพื่อลดความจำเป็นในการใช้วิธีการเข้ารหัสที่มีความมั่นคงปลอดภัยสูง เช่น การเลือกใช้วิธีการติดต่อสื่อสารที่มีการป้องกัน โดยอาจเป็นการใช้งานอินเทอร์เน็ตแบบจำกัดขอบเขตแทนการใช้งานอินเทอร์เน็ตสาธารณะ

(2) สมรรถนะที่ต้องการ (Required Performance) โดยหากต้องการสมรรถนะที่สูง อาจจะต้องจัดหาทรัพยากรของระบบเพิ่มเติม หรืออาจจำเป็นต้องลดระดับความมั่นคงปลอดภัยของวิธีการเข้ารหัส

(3) ทรัพยากรของระบบ โดยหากมีทรัพยากร เช่น กระบวนการ หรือหน่วยความจำ ไม่มาก ก็สามารถใช้วิธีการเข้ารหัสที่มีระดับความมั่นคงปลอดภัยลดลงมาได้

(4) ข้อจำกัดด้านการนำเข้า การส่งออก และการใช้งานวิธีการเข้ารหัสของแต่ละประเทศ

(5) การรองรับวิธีการเข้ารหัสแบบต่าง ๆ โดยโปรแกรมประยุกต์บนเว็บ

(6) การรองรับวิธีการเข้ารหัสแบบต่าง ๆ โดยโปรแกรมค้นดูเว็บของกลุ่มผู้ใช้บริการเป้าหมาย

โดยมีตัวอย่างการเลือกใช้ SSL/TLS Cipher Suite ตามลักษณะการใช้งานและความมั่นคงปลอดภัยที่แนะนำไว้ใน Guideline on Securing Public Web Servers มีดังนี้

ลักษณะการใช้งาน	Cipher Suite	ใบรับรองอิเล็กทรอนิกส์สำหรับเครื่องบริการเว็บ
ความมั่นคงปลอดภัยสูงสุด	วิธีการเข้ารหัส: การเข้ารหัสแบบ Advanced Encryption Standard (AES) ด้วยกุญแจขนาด 128 บิตขึ้นไป หรือเลือกเป็นการเข้ารหัสแบบ Triple Data Encryption Standard (3DES) ด้วยกุญแจขนาด 168 บิต (ใช้กุญแจ 3 อัน) โดยการเข้ารหัสแบบ 3DES จะช้ากว่าแบบ AES HMAC: Secure Hash Algorithm 1 (SHA-1) หรือ SHA-256 วิธีการยืนยันตัวตน: Digital Signature Standard (DSS) หรือ RSA	DSS หรือ RSA ด้วยกุญแจขนาด 2048 บิตขึ้นไป และ Hash function แบบ SHA-1 หรือ SHA-256 ทั้งนี้ การใช้ SHA-256 ในใบรับรองอิเล็กทรอนิกส์อาจทำงานร่วมกันไม่ได้กับผู้ใช้บริการเวอร์ชั่นเก่า
ความมั่นคงปลอดภัยและสมรรถนะ (Security and Preformance)	วิธีการเข้ารหัส: การเข้ารหัสแบบ AES ด้วยกุญแจขนาด 128 บิต HMAC: SHA-1 วิธีการยืนยันตัวตน: DSS หรือ RSA	DSS หรือ RSA ด้วยกุญแจขนาด 1024 บิตขึ้นไป และ Hash function แบบ SHA-1
ความมั่นคงปลอดภัยและความเข้ากันได้ร่วมกันได้ของระบบ (Security and Compatability)	วิธีการเข้ารหัส: การเข้ารหัสแบบ AES ด้วยกุญแจขนาด 128 บิต หรือเลือกเป็นการเข้ารหัสแบบ 3DES ด้วยกุญแจขนาด 168 บิต (ใช้กุญแจ 3 อัน) HMAC: SHA-1 วิธีการยืนยันตัวตน: DSS หรือ RSA	DSS หรือ RSA ด้วยกุญแจขนาด 1024 บิตขึ้นไป และ Hash function แบบ SHA-1
การยืนยันตัวตนและการป้องกันการปลอมแปลง	HMAC: SHA-1 วิธีการยืนยันตัวตน: DSS หรือ RSA	DSS หรือ RSA ด้วยกุญแจขนาด 1024 บิตขึ้นไป และ Hash function แบบ SHA-1

ตารางที่ 1 ลักษณะการใช้งานและความมั่นคงปลอดภัยที่แนะนำไว้ใน Guideline on Securing Public Web Servers

อย่างไรก็ตาม SSL รองรับเฉพาะ Cipher Suites ที่เป็น RSA, Diffie-Hellman, และ Fortezza/DMS เพื่อนำไปใช้ร่วมกับตัวแปรอื่น ๆ ในการสร้างรหัสลับ ส่วน TLS ได้หยุดการรองรับ cipher suite ที่เป็น Fortezza/DLS แต่อนุญาตให้สามารถเพิ่ม Cipher Suites เข้าไปในโพรโทคอล TLS เวอร์ชั่นต่อไปได้

ภาคผนวก ค. การใช้งานใบรับรองอิเล็กทรอนิกส์สำหรับการสื่อสารอย่างมั่นคงปลอดภัย

ในการติดตั้งและใช้งาน SSL/TLS นั้นมีความแตกต่างกันไปในตามประเภทของเครื่องบริการเว็บ ซึ่งผู้ดูแลเครื่องบริการเว็บ ควรเลือกใช้งานใบรับรองอิเล็กทรอนิกส์ตามประเภทธุรกิจและลักษณะเนื้อหาของเว็บไซต์ โดยใบรับรองอิเล็กทรอนิกส์สำหรับเว็บไซต์มีอยู่ 3 ประเภท ได้แก่

ประเภทที่ 1 Domain Validation : เป็นใบรับรองที่เข้ารหัสระดับ 128-256 บิต ตรวจสอบความเป็นเจ้าของ โดเมนว่าตรงกับข้อมูลผู้ขอใบรับรอง SSL หรือไม่ก่อนการอนุมัติ ทำให้มีความมั่นคงปลอดภัยและมีความน่าเชื่อถือ

ประเภทที่ 2 Organization Validation : เป็นใบรับรองสำหรับองค์กรที่ต้องการเพิ่มความน่าเชื่อถือ โดยมีการตรวจสอบองค์กรที่ขอใบรับรอง SSL ว่ามีอยู่จริงหรือไม่ มีการยืนยันข้อมูลผู้ขอใบรับรอง SSL ทางโทรศัพท์ (Verify Call) โดยขั้นต้นเข้ารหัสลับที่ 128 บิต และ สูงสุดที่ 256 บิต ทำให้มีความมั่นคงปลอดภัยและมีความน่าเชื่อถือสูง

ประเภทที่ 3 Extended Validation : เป็นใบรับรองระดับสูงสุด โดยมีการตรวจสอบข้อมูลอย่างเข้มงวดถึงความเป็นเจ้าของโดเมนและตรวจสอบตัวตนขององค์กร เช่น การตรวจสอบว่าองค์กรมีอยู่จริง โดยอาจจะมีการขอเอกสารทางกฎหมายอื่น ๆ ของหน่วยงาน, การให้เจ้าหน้าที่มาตรวจสอบที่อยู่ขององค์กรว่ามีตัวตนตั้งอยู่ตามที่อยู่ที่ลงทะเบียนไว้หรือไม่ เป็นต้น โดยต้องให้นักกฎหมาย (Third Party) ซึ่งในประเทศไทยนักกฎหมายหรือผู้ที่มีตั๋วทนายจากสภาทนายความแห่งประเทศไทย ลงนามรับรองเอกสารขององค์กรด้วย โดยขั้นต้นเข้ารหัสลับที่ 128 บิต และ สูงสุดที่ 256 บิต ซึ่งเหมาะกับองค์กรที่ต้องการความน่าเชื่อถือสูง เช่น เว็บไซต์ธนาคาร เป็นต้น

เมื่อเลือกประเภทของใบรับรองอิเล็กทรอนิกส์ที่เหมาะสมได้แล้ว ก็จะเข้าสู่กระบวนการส่งคำร้องขอใช้งานใบรับรองอิเล็กทรอนิกส์และการติดตั้งใบรับรองอิเล็กทรอนิกส์ ซึ่งมีขั้นตอนดังต่อไปนี้

1. การขอใบรับรองอิเล็กทรอนิกส์สำหรับเครื่องบริการเว็บเพื่อติดตั้ง SSL/TLS

ในปัจจุบันเว็บไซต์หลอกลวงมีมากมาย จนผู้ใช้บริการไม่สามารถแยกแยะได้ว่าเว็บไซต์ใดมีความน่าเชื่อถือหรือเว็บไซต์ใดไม่น่าเชื่อถือ กระบวนการยืนยันตัวตนเว็บไซต์โดยใช้ใบรับรองอิเล็กทรอนิกส์สำหรับเครื่องบริการเว็บจึงเป็นวิธีการหนึ่งที่จะทำให้ผู้ใช้บริการเว็บไซต์สามารถมั่นใจได้ว่าเว็บไซต์ที่ตัวเองกำลังใช้บริการนั้นมีตัวตนอยู่จริงและได้รับการรับรองจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ที่น่าเชื่อถือ กระบวนการรักษาความมั่นคงปลอดภัยของโพรโทคอล SSL/TLS ไม่ว่าจะเป็นการเข้ารหัสข้อมูลที่ใช้ในการสื่อสาร และการยืนยันตัวตนล้วนขึ้นอยู่กับกุญแจสาธารณะที่อยู่ในใบรับรองอิเล็กทรอนิกส์สำหรับเครื่องบริการเว็บซึ่งเป็นใบรับรองที่ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certificate Authority) รับรองกุญแจสาธารณะ (Public Key) ที่ใช้งานว่าเป็นของเว็บไซต์ที่มีบุคคลหรือนิติบุคคลที่เกี่ยวข้องเป็นเจ้าของและเป็นผู้รับผิดชอบ เมื่อผู้ใช้บริการใช้โปรแกรมค้นดูเว็บติดต่อกับเครื่องบริการเว็บที่ใช้โพรโทคอล SSL/TLS ก่อนที่จะดำเนินการเข้ารหัสข้อมูลเพื่อการสื่อสารระหว่างกันนั้น โปรแกรมค้นดูเว็บจะตรวจสอบความถูกต้องของใบรับรองอิเล็กทรอนิกส์ซึ่งได้แก่ตรวจสอบว่าเป็นใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรองที่โปรแกรมค้นดูเว็บนั้น ๆ เชื่อถือหรือไม่ หรือ ตรวจสอบว่าใบรับรองดังกล่าวได้ถูกยกเลิกการใช้งานหรือ

หมดอายุหรือไม่ เป็นต้น การเลือกผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์เป็นตัวแปรหนึ่งที่มีความสำคัญต่อความมั่นคงปลอดภัยซึ่งแนวทางสำหรับการเลือกใช้บริการจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์สำหรับเครื่องบริการเว็บมีดังต่อไปนี้

(1) สำหรับการเลือกผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ที่น่าเชื่อถือภายในประเทศไทย เจ้าของเว็บไซต์หรือผู้ดูแลเครื่องบริการเว็บควรขอใบรับรองอิเล็กทรอนิกส์จากผู้ให้บริการที่ได้รับการรับรองจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติ (Thailand National Root Certification Authority) ซึ่งสามารถตรวจสอบรายชื่อของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ที่ได้รับการรับรองจาก URL: http://www.nrca.go.th

(2) สำหรับการเลือกผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ในต่างประเทศ เจ้าของเว็บไซต์หรือผู้ดูแลเครื่องบริการเว็บควรเลือกผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ที่ผ่านการตรวจประเมินการดำเนินกิจการตามมาตรฐานสากลเช่น มาตรฐาน Web Trust เป็นต้น

(3) เจ้าของเว็บไซต์หรือผู้ดูแลเครื่องบริการเว็บที่ขอใช้บริการควรศึกษารายละเอียดของแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์อย่างรอบคอบ รวมถึงศึกษารายละเอียดและเงื่อนไขการให้บริการของใบรับรองอิเล็กทรอนิกส์แต่ละประเภท

(4) ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์อย่างน้อยต้องให้บริการข้อมูลของรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation List (CRL)) โดยในส่วนของบริการอื่น ๆ ผู้ใช้บริการสามารถนำมาใช้ในการพิจารณาเลือกใช้บริการได้เช่น มีบริการโพรโทคอลโอซีเอสพี (Online Certificate Status Protocol (OCSP)) สำหรับการตรวจสอบสถานะของใบรับรองอิเล็กทรอนิกส์หรือบริการออกใบรับรองอิเล็กทรอนิกส์ประเภท Domain-validated และใบรับรองอิเล็กทรอนิกส์ประเภท Extended Validation เป็นต้น [11]

2. การส่งคำร้องขอใช้งานใบรับรองอิเล็กทรอนิกส์

หลังจากที่เลือกผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ที่น่าเชื่อถือแล้วนั้น ในส่วนของขั้นตอนการส่งคำร้องเพื่อขอใช้งาน Certificate นั้น มีรายละเอียดดังต่อไปนี้

(1) ผู้ดูแลเครื่องบริการเว็บ สร้างกุญแจคู่รหัส (Key Pair) ขึ้น โดยกุญแจสาธารณะนั้นจะประกอบด้วย Public Key และ Private Key ของเครื่องบริการเว็บ เพื่อนำมาใช้ในขั้นตอนการสร้างไฟล์ Certificate Signing Request

(2) ผู้ดูแลเครื่องบริการเว็บ สร้าง Certificate Signing Request (CSR) โดยไฟล์ CSR ที่มีรูปแบบตามมาตรฐาน RFC 2986 และ PKCS#10 โดยไฟล์ CSR จะประกอบไปด้วย 3 องค์ประกอบหลักดังนี้

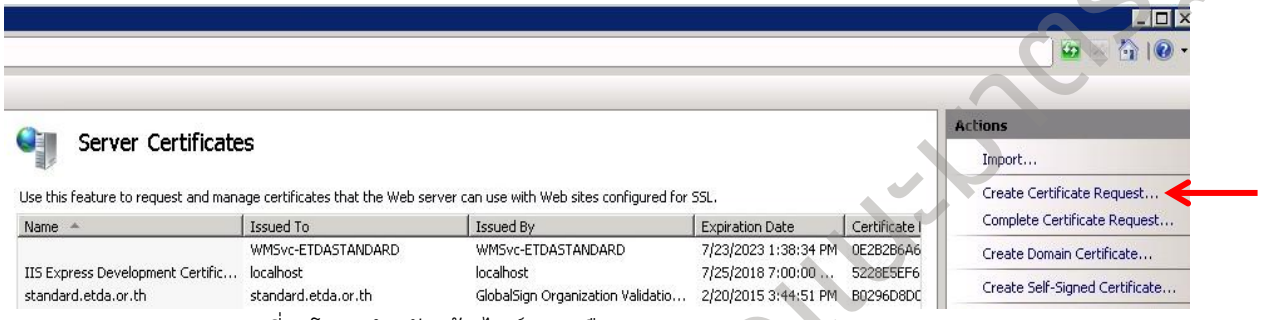
ก. Certificate Request Information (CRI) ซึ่ง CRI นี้จะประกอบไปด้วย Distinguish Name, Public Key ของเครื่องบริการเว็บ และ Attribute อื่น ๆ เช่น รายละเอียดขององค์กร เป็นต้น (Optional)

ข. Signature Algorithm Identifier

ค. Digital Signature : เป็นการ Sign ด้วย Private Key ของเครื่องบริการเว็บ เพื่อเป็นการรับรองข้อมูลว่าเป็นความจริง

เมื่อมีข้อมูลครบทั้ง 3 ส่วน เครื่องบริการเว็บจะสร้างไฟล์ CSR โดยในแต่ละบริษัทผู้ให้บริการเครื่องบริการเว็บจะมีวิธีการสร้างไฟล์ CSR แตกต่างกันไป ยกตัวอย่างเช่น

ใน Microsoft IIS จะมีโปรแกรม IIS Manager เพื่อใช้ในการจัดการข้อมูลต่าง ๆ ที่เกี่ยวกับเครื่องบริการเว็บ และจะมีโมดูลสำหรับสร้างไฟล์ CSR คือ Create Certificate Request ดังรูป



ภาพที่ 2 โมดูลสำหรับสร้างไฟล์ CSR คือ Create Certificate Request

ใน Apache ผู้ดูแลเครื่องบริการเว็บใช้โมดูลของ Apache ที่ชื่อ Apache OpenSSL ในการสร้างไฟล์ CSR ซึ่ง OpenSSL นี้จะถูกติดตั้งมาแล้ว อยู่ภายใต้ /usr/local/ssl/bin และใช้ Command Line ในการสร้างทั้งกุญแจคู่รหัสไฟล์ CSR ดังรูป

ภาพที่ 3 การใช้ command line ในการสร้างทั้งกุญแจคู่รหัสไฟล์ CSR

(3) ผู้ดูแลเครื่องบริการเว็บนำไฟล์ CSR นี้ส่งไปยังผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เพื่อส่งคำร้องขอใช้งานใบรับรองอิเล็กทรอนิกส์ ซึ่งในการส่งคำร้องขอใช้งานใบรับรองอิเล็กทรอนิกส์นั้น มีข้อสังเกต ดังนี้

ก. ถ้าองค์กรของท่านเป็นหน่วยงานของรัฐ จะต้องทำการซื้อใบรับรองอิเล็กทรอนิกส์ผ่านตัวแทนในประเทศไทย ซึ่งผู้ดูแลเครื่องบริการเว็บต้องส่งแบบฟอร์มคำร้องขอใช้งาน ไปพร้อมกับไฟล์ CSR ด้วย เช่น บริษัท iNET เป็นตัวแทนจำหน่าย ใบรับรองอิเล็กทรอนิกส์ของ GlobalSign เป็นต้น

ข. ถ้าองค์กรของท่านเป็นหน่วยงานเอกชน สามารถทำการซื้อ ใบรับรองอิเล็กทรอนิกส์ได้โดยตรงจาก Certificate Authority หรือจะทำการซื้อผ่านบริษัทตัวแทนของประเทศไทยก็ได้

ค. ปัจจุบัน บริษัท Thai Digital ID หรือ TDID เป็นผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์รายแรกของประเทศไทยที่ได้รับการรับรองตามมาตรฐานสากล Trust Service Principles and Criteria for Certification Authorities Version2.0 (WebTrust for CAs) เช่นเดียวกับผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ทั่วโลก ตั้งแต่ปี 2013 ซึ่งสามารถยื่นคำร้องขอใช้งาน ใบรับรองอิเล็กทรอนิกส์พร้อม

ทั้งเอกสารอื่น ๆ ได้เช่นเดียวกัน รายละเอียดเพิ่มเติมตาม URL http://www.thaidigitalid.com/index.jsp?page=registration_ssl.jsp

(4) ผู้ดูแลเครื่องบริการเว็บต้องทำการสำรองข้อมูลไฟล์ CSR และ Key-pair ไว้ด้วย โดยข้อมูลในส่วนนี้ต้องเก็บเป็นความลับ

3. การติดตั้งใบรับรองอิเล็กทรอนิกส์

เมื่อผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ตรวจสอบตัวตนของผู้ขอใช้บริการและดำเนินการในขั้นตอนต่าง ๆ เพื่ออนุมัติ ใบรับรองอิเล็กทรอนิกส์ให้แก่ผู้ขอใช้บริการตามรูปแบบของ X.509 เรียบร้อย ก็จะสามารถเข้าสู่ขั้นตอนการติดตั้งใบรับรองอิเล็กทรอนิกส์ได้ โดยผู้ดูแลเครื่องบริการเว็บจะได้รับอีเมลจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ เป็นลักษณะไฟล์หรือชุดรหัสข้อความแนบมาพร้อมกับอีเมล ซึ่งจะทำการส่งถึงอีเมลของผู้ขอใบรับรองอิเล็กทรอนิกส์โดยตรงหรือผ่านตัวแทนจำหน่าย ซึ่งรูปแบบจะแตกต่างกันออกไปตามแต่ละบริษัทผู้ให้บริการเครื่องบริการเว็บ ในอีเมลมีรายละเอียดของใบรับรองอิเล็กทรอนิกส์พร้อมวิธีการติดตั้ง SSL ซึ่งโดยหลักแล้วจะมีวิธีการดังนี้

(1) ผู้ดูแลเครื่องบริการเว็บตรวจสอบก่อนการติดตั้ง ให้แน่ใจว่ามีไฟล์ Certificate สำหรับเตรียมติดตั้งครบถ้วน โดยทั่วไปมักได้แก่
   ก. Intermediate Certificate : เป็น Certificate ที่มีมาเพื่อรับรององค์กรที่ร้องขอใช้งานใบรับรองอิเล็กทรอนิกส์ว่ามีตัวตนจริง โดย Intermediate Certificate จะออกผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (GlobalSign) ซึ่งได้รับการรับรองผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Root CA)
   ข. SSL Certificate เป็นใบรับรองอิเล็กทรอนิกส์ของโดเมนเนมที่ร้องขอใช้งาน SSL Certificate
(2) ผู้ดูแลเครื่องบริการเว็บติดตั้ง Intermediate Certificate และ SSL Certificate ตามคู่มือการติดตั้งของบริษัทผู้ให้บริการเครื่องบริการเว็บแต่ละบริษัท ซึ่งวิธีการติดตั้งจะมีอยู่ในอีเมลที่ผู้ดูแลเครื่องบริการเว็บได้รับจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์
(3) เมื่อติดตั้งเสร็จเรียบร้อยแล้ว ผู้ดูแลเครื่องบริการเว็บรีสตาร์ทเครื่องบริการเว็บ

4. การปรับแต่งค่าติดตั้งที่เกี่ยวกับ SSL/TLS

ผู้ดูแลเครื่องบริการเว็บปรับแต่งค่าต่าง ๆ ของเครื่องบริการเว็บ เพื่อให้เว็บไซต์ใช้งานใบรับรองอิเล็กทรอนิกส์ได้อย่างสมบูรณ์ โดยการใช้บริการ Configuration Checker จากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์เพื่อเป็นการตรวจสอบความครบถ้วนของการปรับแต่งค่าเครื่องบริการเว็บ เช่น GlobalSign จะมีบริการตรวจสอบความครบถ้วนในการติดตั้งและปรับแต่งค่าเพื่อใช้งาน SSL ตาม URL: https://sslcheck.globalsign.com/en_US โดยสามารถใส่ URL ของเว็บไซต์ที่ต้องการทดสอบ เมื่อประมวลผลเสร็จก็จะแสดงระดับที่เว็บไซต์นั้นได้รับ A-F และมีรายการของข้อบกพร่องที่ต้องแก้ไขเพิ่มเติมพร้อมทั้งรายละเอียดโดยคร่าว ผู้ดูแลเครื่องบริการเว็บสามารถนำรายการข้อบกพร่องที่พบทั้งหมดไปปรับปรุงเพิ่มได้ ซึ่งขั้นตอนการปรับแต่งค่าบางอย่างของเครื่องบริการเว็บและเว็บไซต์จะแตกต่างกันไปตามบริษัทผู้ให้บริการของเครื่องบริการเว็บแต่ละบริษัท และใช้เครื่องมือของโปรแกรมค้นดูเว็บ Google Chrome ที่ชื่อว่า JavaScript Console เพื่อช่วยในการตรวจสอบหน้าเว็บเพจ ว่ามีส่วนใดที่ต้องปรับปรุงแก้ไขเพื่อให้ใช้งานใบรับรองอิเล็กทรอนิกส์ได้อย่างเต็ม

ประสิทธิภาพ โดยเปิด Google Chrome แล้วกดปุ่ม เลือก Tool > JavaScript Console ก็จะปรากฏหน้าต่างดังภาพ ซึ่งถ้ามีข้อบกพร่องใด ๆ ก็จะปรากฏในหน้าต่างนี้

ภาพที่ 4 เครื่องมือของโปรแกรมค้นดูเว็บ Google Chrome ที่ชื่อว่า JavaScript Console

ซึ่งส่วนใหญ่ข้อกำหนดพื้นฐานที่ผู้ดูแลเครื่องบริการเว็บต้องนำไปปฏิบัติตาม มีดังนี้

ก. Disable การใช้งาน PCT1.0, SSL2.0, SSL3.0

ข. Enable การใช้งาน TLS1.0, TLS1.1, TLS1.2

ค. กำหนดรูปแบบการเข้ารหัสลับในการรับ-ส่งข้อมูลผ่านโพรโทคอล HTTPS ตาม Cipher Suite ที่เลือก (รายละเอียดตาม 5.1.3)

ง. ปรับค่าเครื่องบริการเว็บให้รับ-ส่งข้อมูลจาก Port 443 ซึ่งเป็น Port พื้นฐานของการใช้โพรโทคอล HTTPS ซึ่งถ้าก่อนหน้านี้ เครื่องบริการเว็บไม่เคยใช้งาน Port 443 นี้มาก่อน Port 443 จะถูกปิดอยู่

จ. ปิด Port ทั้งหมดที่นอกเหนือจาก Port 443 และ อัพเดตโครงสร้างระบบเครือข่าย เช่น firewall ควร Block Request ทั้งหมดที่พยายามเชื่อมต่อมาทาง Port อื่น ๆ แต่ถ้าเครื่องบริการเว็บเป็นแม่ข่ายให้ทั้ง HTTP และ HTTPS ก็ควรเปิด port 80 ไว้ด้วย

ฉ. ปรับแต่งค่าโครงสร้างเว็บไซต์เพื่อให้รองรับ SSL/TLS เช่น ตรวจสอบและแก้ไข URL ทั้งหมดในเว็บไซต์ให้มีการเรียกใช้จากโพรโทคอล HTTPS เท่านั้น และตรวจสอบการเรียกใช้ URL จากภายนอกที่โพรโทคอล HTTPS แจ้งเตือนว่าไม่มั่นคงปลอดภัย

เมื่อติดตั้งและปรับแต่งค่าทั้งหมดเสร็จเรียบร้อย ผู้ดูแลเครื่องบริการเว็บทดลองเข้าเว็บไซต์จากโปรแกรมค้นดูเว็บต่าง ๆ เพื่อตรวจสอบเว็บไซต์ว่าสามารถเข้าถึงด้วยโพรโทคอล HTTPS หรือไม่ ซึ่งถ้ากระบวนการต่าง ๆ เสร็จสมบูรณ์จะปรากฏลักษณะต่าง ๆ ซึ่งจะแตกต่างกันไปตามประเภทของ ใบรับรองอิเล็กทรอนิกส์ที่เลือกใช้ ในที่นี้จะขอยกตัวอย่าง ใบรับรองอิเล็กทรอนิกส์ประเภท Organization Validation จะมีลักษณะปรากฏ ดังนี้

ช. Google Chrome 

ภาพที่ 5 ตัวอย่างสัญลักษณ์กุญแจสีเขียวจากโปรแกรมค้นดูเว็บ Google Chrome

ในกรณีที่ไม่เป็นสัญลักษณ์กุญแจสีเขียว สามารถตรวจสอบสาเหตุได้ตาม URL: https://support.google.com/chrome/answer/95617?hl=en&topic=14666&ctx=topic

ซ. Internet Explorer 

ภาพที่ 6 ตัวอย่างสัญลักษณ์กุญแจสีเขียวจากโปรแกรมค้นดูเว็บ Internet Exploer

ฌ. Mozilla Firefox 

ภาพที่ 7 ตัวอย่างสัญลักษณ์กุญแจสีเขียวจากโปรแกรมค้นดูเว็บ Mozilla Firefox

และผู้ดูแลเครื่องบริการเว็บต้องทำการสำรองข้อมูลไฟล์ SSL Certificate ไว้ด้วย โดยข้อมูลในส่วนนี้ต้องเก็บเป็นความลับ

5. การบำรุงรักษาใบรับรองอิเล็กทรอนิกส์

เมื่อติดตั้งและปรับแต่งค่าเครื่องบริการเว็บและเว็บไซต์เพื่อให้ใช้งานใบรับรองอิเล็กทรอนิกส์เรียบร้อย ผู้ดูแลเครื่องบริการเว็บต้องปฏิบัติตามข้อกำหนดต่อไปนี้เพื่อบำรุงรักษาใบรับรองอิเล็กทรอนิกส์

(1) หมั่นตรวจสอบวันหมดอายุของใบรับรองอิเล็กทรอนิกส์

เนื่องจากใบรับรองอิเล็กทรอนิกส์จะมีอายุใช้งานคราวละ 1 ปี ทำให้เมื่อใกล้ครบอายุ ผู้ดูแลเครื่องบริการเว็บต้องทำการ Renew Certificate จากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์เดิม โดยขั้นตอนการ Renew Certificate ก็จะเหมือนกับขั้นตอนการขอใช้งานใบรับรองอิเล็กทรอนิกส์ใหม่ เริ่มต้นตั้งแต่การส่งคำร้องขอใช้งานใบรับรองอิเล็กทรอนิกส์ เพราะในการต่ออายุใบรับรองอิเล็กทรอนิกส์นั้น จะดำเนินการสร้างกุญแจคู่รหัสขึ้นมาใหม่และออกใบรับรองอิเล็กทรอนิกส์ใบใหม่แทนใบเดิมที่หมดอายุ

(2) หมั่นตรวจสอบความต้องการและลักษณะขององค์กรเสมอ ว่าต้องการใบรับรองอิเล็กทรอนิกส์ที่มั่นคงปลอดภัยมากขึ้นหรือไม่

หมั่นตรวจสอบข่าวสารของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์อยู่เสมอ ว่ามีความน่าเชื่อถือมากขึ้นหรือน้อยลงอย่างไร เพื่อช่วยเลือกใช้บริการกับผู้ให้บริการฯ ที่น่าเชื่อถือที่สุด โดยผู้ดูแลเครื่องบริการเว็บสามารถเปลี่ยนผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ได้ โดยขั้นตอนนั้นก็จะเหมือนกับขั้นตอนการขอใช้งานใบรับรองอิเล็กทรอนิกส์ใหม่นั้นเอง

รายการแก้ไขเอกสาร

เวอร์ชั่นเอกสาร	วันที่แก้ไข	รายละเอียดการแก้ไข
Version 0.1 DD prepared	26/01/2557	จัดทำเนื้อหาโดยสำนักมาตรฐาน สพธอ. ในรูปแบบของร่างข้อเสนอแนะเพื่อจัดทำมาตรฐาน ตามเอกสารขั้นตอนการจัดทำข้อเสนอแนะเกี่ยวกับมาตรฐานเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ (ตามนิยามใน ข้อ 2.7 และขั้นตอนการพิจารณาร่างข้อเสนอแนะฯ ตามภาคผนวก ก.1)
Version 0.2 DD approved	07/05/2557	ผ่านการพิจารณาจาก ผอ. สำนักมาตรฐาน
Version 0.3 PRD approved	08/05/2557	ผ่านการพิจารณาจากคณะทำงานพิจารณาร่างข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ครั้งที่ 1/2557 เมื่อวันที่ 8 พฤษภาคม 2557
Version 0.4 FDD (1) approved	08/09/2557	อนุมัติในหลักการโดยคณะทำงานพิจารณาร่างข้อเสนอแนะฯ ตามมติของการประชุมผู้บริหารระดับสูงและผู้บริหารระดับกลาง สพธอ. ครั้งที่ 44/2557 เมื่อวันที่ 8 กันยายน 2557 และให้ปรับแก้ไขตามความเห็นของการเวียนร่าง และตามมติของคณะทำงานพิจารณาร่างข้อเสนอแนะฯ
Version 0.5 FDD (2) approved	26/09/2557	พิจารณาและปรับปรุงเพิ่มเติมโดยสำนักกฎหมาย ดังนี้ ปกหน้า, ปกใน, เกริ่นนำ, หน้าประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), ขอบเขต, การนำไปใช้งาน
Version 0.6 FDD (2) approved	30/09/2557	อนุมัติโดย ผอ. สพธอ. และมีส่วนที่ปรับปรุงเพิ่มเติม ดังนี้ เกริ่นนำ, บทนำ, ขอบเขต, การนำไปใช้งาน, แนวทางการเลือกรูปแบบเครื่องบริการเว็บ และการรับมือภัยคุกคามที่เกิดขึ้นกับเว็บไซต์, การป้องกันการโจมตีจากเทคนิค Cross-side Scripting, การป้องกันการโจมตีจากเทคนิค CSRF, ภาคผนวก ก. แบบประเมินสำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ และภาคผนวก ข. รูปแบบการสื่อสารอย่างมั่นคงปลอดภัยระหว่างโปรแกรมค้นดูเว็บและเครื่องบริการเว็บ เพื่อให้เนื้อหามีความชัดเจนและตรงประเด็นในแง่การใช้งานมากขึ้น
Version 1.0 EDR approved	30/09/2557	ประกาศเป็น ETDA Recommendation

บรรณานุกรม

[1] *M. Tracy, W. Jansen, K. Scarfone, and T. Winograd, "Guidelines on Securing Public Web Server", National Institute of Standards and Technology, 2007.*

[2] *Open Web Application Security Project (OWASP), "Brute force attack", 12 August 2013. [Online]. Available: https://www.owasp.org/index. PHP/Brute_force_attack.*

[3] *ICANN Security and Stability Advisor Committee (SSAC), "SAC 40 Measure to Protect Domain Registration Services Against Exploitation or Misuse", 2009.*

[4] *Google Inc., "Google Trends" , [Online]. Available: http://trends.google.com/trends.*

[5] *National Institute of Standards and Technology, "NIST", [Online]. Available: http://www.nist.gov/.*

[6] *GSA's Office of Citizen Services and Innovative Technologies and the Federal Web Managers Council, "choosing CMS", 31 October 2013. [Online]. Available: http://www.howto.gov/web-content/technology.*

[7] *National Vulnerability Database, "National Vulnerability Database-CVE Static (Wordpress, Joomla!, Drupal)", NIST, [Online]. Available: http://web.nvd.nist.gov.*

[8] *A. Freier, P. Karlton and P. Kocher, "RFC 6160 - The Secure Sockets Layer (SSL) Protocol Version 3.0", August 2011. [Online]. Available: http://tools.ietf.org/html/rfc6101.*

[9] *T. Dierks and E. Rescorla, "RFC 5246 - The Transport Layer Security (TLS) Protocol", August 2008. [Online]. Available: http://tools.ietf.org/html/rfc5246.*

[10] *Trustworthy Internet Movement (TIM), "Survey of the SSL Implementation of the Most Popular Web Sites", 3 January 2014. [Online]. Available: https://www.trustworthyinternet.org/ssl-pulse/.*

[11] *I. Ristić, "SSL/TLS Deployment Best Practices",vol. 1.3, 17 September 2013.*

[12] *WordPress, "Hardening WordPress", [Online]. Available: http://codex.wordpress.org/Hardening_WordPress.*

[13] *Joomla!, "Security Checklist/Joomla! Setup", 14 March 2014. [Online]. Available: http://docs.joomla.org/.*

[14] *Drupal, "Securing your site", 12 November 2013. [Online]. Available: https://drupal.org/.*

[15] *Oracle Corporation, "Oracle Database Security Checklist", June 2008. [Online]. Available: http://www.oracle.com/technetwork/database/security.*

[16] *T. Baccam, "Making Database Security an IT Security Priority", SANS Institute , November 2009. [Online]. Available: https://www.sans.org/reading-room/.*

[17] *D. Sarel and C. L. Grand, "Database Security, Compliance and Audit", Information System Control Journal, ISACA, vol. V, pp. 1-5, 2008.*

[18] *Open Web Application Security Project (OWASP), " PHP Security Cheat Sheet", 25 March 2014. [Online]. Available: https://www.owasp.org/index. PHP/ PHP_Security_Cheat_Sheet.*

[19] *Microsoft, "Securing ASP.NET Configuration", [Online]. Available: http://msdn.microsoft.com/en-us/library/.*

[20] *Oracle, "Creating and Configuring JSPs", [Online]. Available: http://docs.oracle.com.*

[21] *World Wide Web Consortium (W3C), "HTTP/1.1 header fields", [Online]. Available: http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html.*

[22] *E. Barker and A. Roginsky, "NIST Special Publication 800-131A", National Institute of Standards and Technology (NIST), U.S. Department of Commerce , 2011.*