ภาคผนวก ก. แบบประเมินสำหรับผู้พัฒนาโปรแกรมประยุกต์บนเว็บ

ก.1 แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

ข้อที่	ประเภทช่องโหว่	ประเภทการป้องกัน	Checkbox	รายละเอียดการป้องกัน	หัวข้อที่อ้างอิงถึง
1	SQL Injection (หัวข้อที่ 4.1)	การป้องกันการโจมตี	☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	มีการจัดทำ Prepared Statement และ/หรือ Stored Procedure	หัวข้อ 4.1.2.1 ข้อ 1
			☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	ไม่เขียนคำสั่ง SQL โดยตรงในตัวแปร (Parameter) ที่ส่งโดยตรงไปยังโปรแกรมประยุกต์บนเว็บ	หัวข้อ 4.1.2.1 ข้อ 2
		การลดความเสียหายที่เกิดจากการถูกโจมตี	☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	ควบคุมการแสดงผลข้อมูล Error Message	หัวข้อ 4.1.2.2 ข้อ 1
			☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	กำหนดสิทธิขั้นต่ำให้บัญชีผู้ใช้ของฐานข้อมูล	หัวข้อ 4.1.2.2 ข้อ 2
		การทดสอบ	☐ ทดสอบผ่าน ☐ ทดสอบไม่ผ่าน ☐ ยังไม่สามารถทดสอบได้ด้วยตนเอง	SQL Injection Testing (OTG-INPVAL-005)	หัวข้อ 4.1.3
2	OS Command Injection (หัวข้อที่ 4.2)	การป้องกันการโจมตี	☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	พัฒนาโปรแกรมประยุกต์บนเว็บโดยให้ปิดการใช้งานคำสั่งต่าง ๆ เพื่อป้องกันการเรียกใช้ที่ไม่พึงประสงค์	หัวข้อ 4.2.2.1
		การลดความเสียหายที่เกิดจากการถูกโจมตี	☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	(ในการณีที่มีการเรียกใช้คำสั่ง OS Command) ต้องตรวจสอบ Variables ที่จะใช้กับตัวแปรของ OS Command ก่อนนำไปประมวลผล	หัวข้อ 4.2.2.2
		การทดสอบ	☐ ทดสอบผ่าน ☐ ทดสอบไม่ผ่าน ☐ ยังไม่สามารถทดสอบได้ด้วยตนเอง	Testing for Command Injection (OTG-INPVAL-013)	หัวข้อที่ 4.2.3
3	Unchecked Path Parameter / Directory Traversal	การป้องกันการโจมตี	☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	ไม่อนุญาตให้ใส่ Filename เพื่อระบุถึงข้อมูลได้จาก External Parameter	หัวข้อ 4.3.2.1 ข้อ 1
			☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	ใช้ Fixed Directory ในการจัดการระบุชื่อไฟล์	หัวข้อ 4.3.2.1 ข้อ 2
		การลดความเสียหายที่เกิด	☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	กำหนด Permission การเข้าถึงไฟล์บนเครื่องบริการเว็บให้เหมาะสม	หัวข้อ 4.3.2.2 ข้อ 1

ข้อที่	ประเภทช่องโหว่	ประเภทการป้องกัน	Checkbox	รายละเอียดการป้องกัน	หัวข้อที่อ้างอิงถึง
	(หัวข้อที่ 4.3)	จากการถูกโจมตี	☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	ตรวจสอบ Filename เช่น มีการแปลง String ที่ระบุ Directory ได้ เช่น / -> % 2F	หัวข้อ 4.3.2.2 ข้อ 2
		การทดสอบ	☐ ทดสอบผ่าน ☐ ทดสอบไม่ผ่าน ☐ ยังไม่สามารถทดสอบได้ด้วยตนเอง	Testing Directory Traversal/File Include (OTG-AUTHZ-001)	หัวข้อที่ 4.3.3
4	Improper Session Management (หัวข้อที่ 4.4)	การป้องกันการโจมตี	☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	สร้าง Session ID เป็นที่ยากต่อการคาดเดา (ไม่ใช้ Algorithm ที่ง่ายเกินไป เช่น Pseudo Random Number)	หัวข้อ 4.4.2.1 ข้อ 1
			☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	ไม่ใช้ URL Parameter ในการเก็บ Session ID	หัวข้อ 4.4.2.1 ข้อ 2
			☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	เมื่อมีการใช้งาน HTTPS Protocol ใช้ Secure Attribute ของ Cookies	หัวข้อ 4.4.2.1 ข้อ 3
		การลดความเสียหายที่เกิดจากการถูกโจมตี	☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	กำหนดให้ Session ID เป็นค่าสุ่ม	หัวข้อ 4.4.2.2 ข้อ 1
			☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	กำหนดวันหมดอายุการใช้งานของ Cookies ที่เก็บ Session ID	หัวข้อ 4.4.2.2 ข้อ 2
		การทดสอบ	☐ ทดสอบผ่าน ☐ ทดสอบไม่ผ่าน ☐ ยังไม่สามารถทดสอบได้ด้วยตนเอง	1. Testing for Bypassing Session Management Schema (OTG-SESS-001) 2. Testing for Exposed Session Variables (OTG-SESS-004)	หัวข้อ 4.4.3
5	Cross-Site Scripting (หัวข้อที่ 4.5)	การป้องกันการโจมตี	☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	ทำ Output Validation ในลักษณะ Sanitization	หัวข้อ 4.5.2.1 ข้อ 1
			☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	ทำ HTML Entity Encoding หรือ URL Encoding กับข้อมูลที่จะแสดงผล	หัวข้อ 4.5.2.1 ข้อ 2
			☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	ตรวจสอบ Input Validation ไม่ให้ใช้ HTML Tag ใด ๆ เช่นไม่ Generate Content จาก Tag <script></script>	หัวข้อ 4.5.2.1 ข้อ 3
			☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	ไม่อนุญาตให้มีการเรียก Stylesheets จากเว็บไซต์ที่ไม่ได้ตรวจสอบก่อน	หัวข้อ 4.5.2.1 ข้อ 4
			☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	ตั้งค่า Charset Parameter ของ HTTP Content-Type Header	หัวข้อ 4.5.2.1 ข้อ 5
			☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	โปรแกรมประยุกต์บนเว็บต้องมีการตรวจสอบข้อมูลชุดคำสั่งในเว็บไซต์	หัวข้อ 4.5.2.1 ข้อ 6

ข้อที่	ประเภทช่องโหว่	ประเภทการป้องกัน	Checkbox	รายละเอียดการป้องกัน	หัวข้อที่อ้างอิงถึง
		การลดความเสียหายที่เกิดจากการถูกโจมตี	☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	มีการใช้งาน HTTPOnly Cookie Flag	หัวข้อ 4.5.2.2
		การทดสอบ	☐ ทดสอบผ่าน ☐ ทดสอบไม่ผ่าน ☐ ยังไม่สามารถทดสอบได้ด้วยตนเอง	Testing for Cross-Site Scripting	หัวข้อที่ 4.5.3
6	Cross-Site Script Forgery (หัวข้อที่ 4.6)	การป้องกันการโจมตี	☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	ฟังก์ชันต่าง ๆ ควรดำเนินการผ่าน POST Method และตรวจสอบความถูกต้องกับค่าที่ซ่อนอยู่ภายใน POST Method ก่อนจะดำเนินการต่อ	หัวข้อ 4.6.2.1 ข้อ 1
			☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	มีฟังก์ชันการยืนยันตัวตนของผู้ใช้งานอีกครั้งและให้กรอก Captcha เมื่อมีการเปลี่ยนแปลงสถานะการทำงานในฟังก์ชันที่สำคัญ ๆ	หัวข้อ 4.6.2.1 ข้อ 2
			☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	ต้องมีการใช้งาน Unique Token และ/หรือ ตรวจสอบ Referrer ร่วมกับการส่งข้อมูล หรือคำสั่งผ่านแบบฟอร์ม	หัวข้อ 4.6.2.1 ข้อ 3
		การลดความเสียหายที่เกิดจากการถูกโจมตี	☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	มีการส่งอีเมลอัตโนมัติ แจ้งผู้ใช้บริการทุกครั้งเมื่อการดำเนินการที่สำคัญทำสำเร็จ	หัวข้อ 4.6.2.2
		การทดสอบ	☐ ทดสอบผ่าน ☐ ทดสอบไม่ผ่าน ☐ ยังไม่สามารถทดสอบได้ด้วยตนเอง	Testing for Cross Site Request Forgery (CSRF) (OTG-SESS-005)	หัวข้อที่ 4.6.3
7	HTTP Header Injection (หัวข้อที่ 4.7)	การป้องกันการโจมตี	☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	ไม่ให้แสดงข้อมูล HTTP Header โดยตรง	หัวข้อ 4.7.2.1 ข้อ 1
			☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	(ถ้ามีการใช้งาน HTTP Header API) เพิ่มการป้องกัน Unexpected Line Feeds ด้วยตนเอง (กรณีไม่มีฟังก์ชัน Line Feed Neutralization)	หัวข้อ 4.7.2.1 ข้อ 2
		การลดความเสียหายที่เกิดจากการถูกโจมตี	☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	ลบ Line Feed Characters ทั้งหมดที่ ปรากฏใน External Text Input	หัวข้อ 4.7.2.2

ข้อที่	ประเภทช่องโหว่	ประเภทการป้องกัน	Checkbox	รายละเอียดการป้องกัน	หัวข้อที่อ้างอิงถึง
		การทดสอบ	☐ ทดสอบผ่าน ☐ ทดสอบไม่ผ่าน ☐ ยังไม่สามารถทดสอบได้ด้วยตนเอง	HTTP Header Injection Testing (OTG-INPVAL-016)	หัวข้อที่ 4.7.3
8	Mail Header Injection (หัวข้อที่ 4.8)	การป้องกันการโจมตี	☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	กำหนดค่าคงที่ (Fixed Values) สำหรับองค์ประกอบของ Header เก็บค่าและแสดงผลที่รับมาจากผู้ใช้บริการในส่วนเนื้อความของอีเมล	หัวข้อ 4.8.2.1 ข้อ 1
			☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	(กรณีที่ไม่สามารถใช้การกำหนดค่าคงที่ (Fixed Header) ใน Header) ใช้ Email-sending API ที่สามารถใช้งานร่วมกับโปรแกรมประยุกต์บนเว็บหรือภาษาที่ใช้ในการพัฒนาได้	หัวข้อ 4.8.2.1 ข้อ 2
			☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	ไม่กำหนดชื่อที่อยู่อีเมลใน HTML	หัวข้อ 4.8.2.1 ข้อ 3
		การลดความเสียหายที่เกิดจากการถูกโจมตี	☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	ลบ Input Line Feed Character ทั้งหมดที่รับข้อมูลจากผู้ใช้บริการ	หัวข้อ 4.8.2.2
		การทดสอบ	☐ ทดสอบผ่าน ☐ ทดสอบไม่ผ่าน ☐ ยังไม่สามารถทดสอบได้ด้วยตนเอง	Mail Header Injection Testing (OTG-INPVAL-011)	หัวข้อที่ 4.8.3
9	Lack of Authentication and Authorization (หัวข้อที่ 4.9)	การป้องกันการโจมตี	☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	ระบุวิธีการยืนยันตัวตนของผู้ใช้บริการ (Authentication) ในกรณีที่มีการกำหนด Access Control	หัวข้อ 4.9.1.1 ข้อ 1
			☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	เก็บรหัสผ่านอยู่ในรูปที่มีการเข้ารหัสลับตามที่มาตรฐานด้านความมั่นคงปลอดภัยกำหนด	หัวข้อ 4.9.1.1 ข้อ 2
			☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	มีกระบวนการที่ชัดเจน เพื่อให้แน่ใจว่าผู้ใช้บริการที่เข้าสู่ระบบ ไม่สามารถเข้าถึงบัญชีผู้ใช้และข้อมูลของผู้ใช้คนอื่น ๆ ได้	หัวข้อ 4.9.2.1
		การลดความเสียหายที่เกิดจากการถูกโจมตี	☐ ยอมรับได้ ☐ ยังต้องปรับปรุง	รหัสผ่านที่ใช้ ต้องประกอบด้วยอักษรตัวเล็ก ตัวใหญ่ ตัวเลขและตัวอักขระพิเศษ และทั้งหมดต้องมีความยาวไม่น้อยกว่า 8 หลัก	หัวข้อ 4.9.1.2
		การทดสอบ	☐ ทดสอบผ่าน ☐ ทดสอบไม่ผ่าน	1. Testing for Default Credentials (OTG-AUTHN-002)	หัวข้อที่ 4.9.3

ข้อที่	ประเภทช่องโหว่	ประเภทการป้องกัน	Checkbox	รายละเอียดการป้องกัน	หัวข้อที่อ้างอิงถึง
			☐ ยังไม่สามารถทดสอบได้ด้วยตนเอง	2. Testing for Weak Password Policy (OTG-AUTHN-007) 3. Testing for Bypassing Authorization Schema (OTG-AUTHZ-002) 4. Testing for Privilege Escalation (OTG-AUTHZ-003)	

ก.2 แบบฟอร์มสำหรับการแก้ไขรายการที่ยังต้องปรับปรุง (จากการตรวจสอบสถานะความมั่นคงปลอดภัย)

ตัวอย่างของแบบฟอร์มสำหรับการแก้ไขรายการที่ยังต้องปรับปรุงซึ่งเกิดจากการตรวจสอบสถานะความมั่นคงปลอดภัยของเว็บไซต์ตามแนวทางในมาตรฐานฉบับนี้ และเมื่อพบรายการที่ไม่เป็นไปตามแนวทางที่กำหนดก็ให้ระบุรายการแก้ไขลงในแบบฟอร์มพร้อมกับกำหนดระยะเวลาในการแก้ไขเพื่อนำเสนอต่อผู้ที่เกี่ยวข้องต่อไป

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