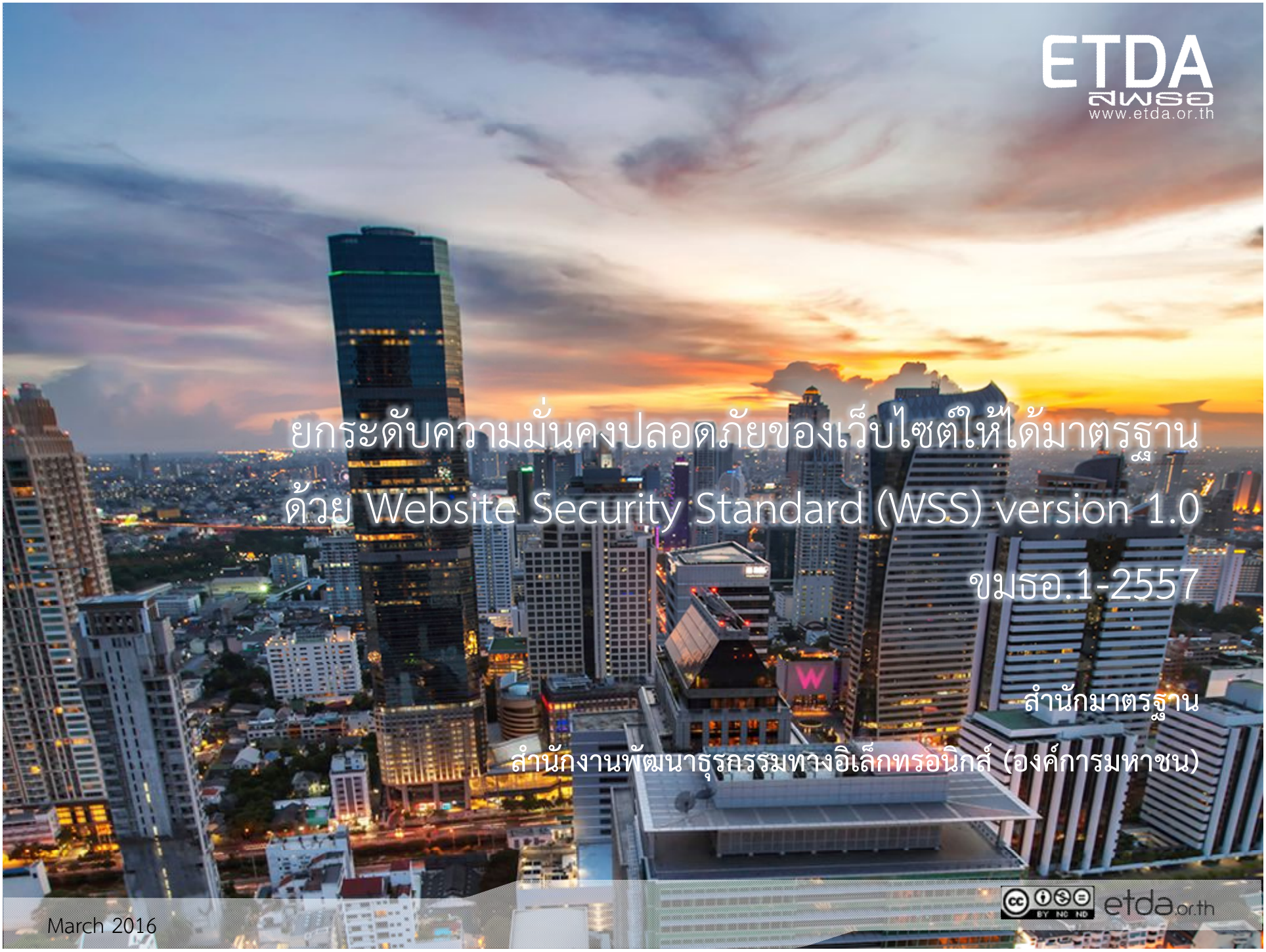


ยกระดับความมั่นคงปลอดภัยของเว็บไซต์ให้ได้มาตรฐาน ด้วย Website Security Standard (WSS) version 1.0

ขมธอ.1-2557

สำนักมาตรฐาน

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

March 2016

Agenda

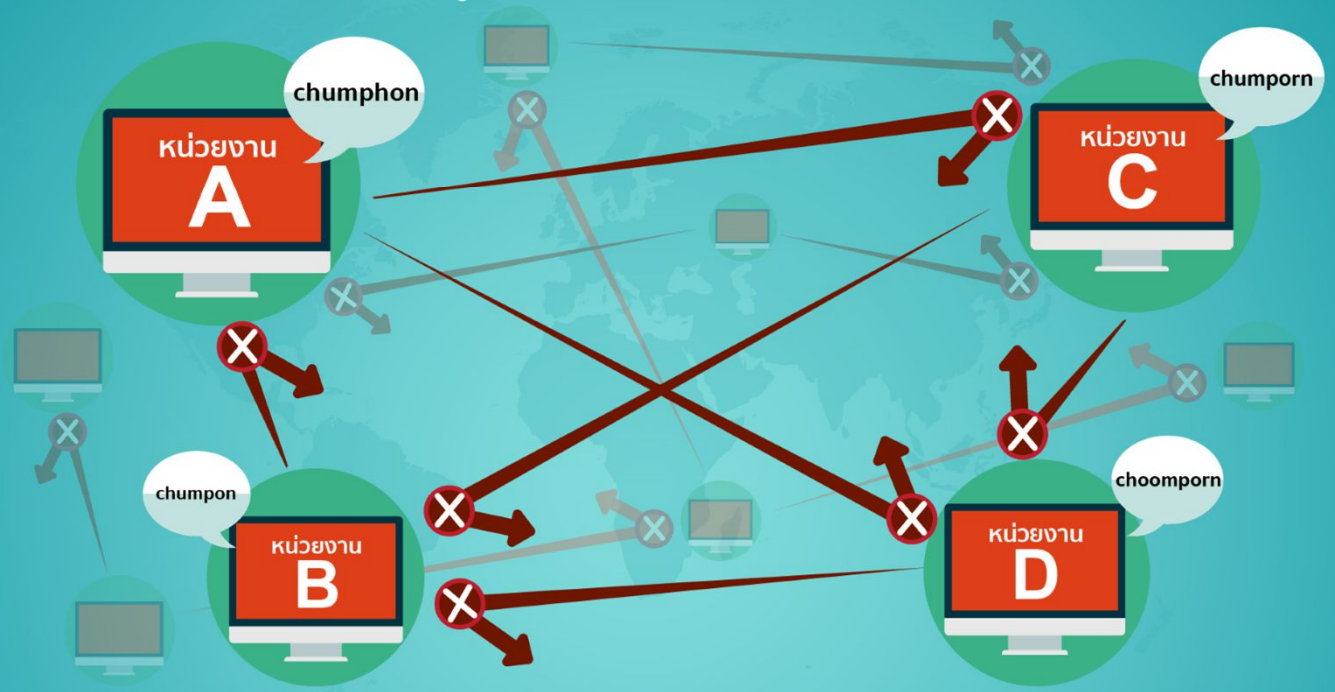
- Introduction to Standard Development Office / ETDA
- WSS Overview
- การวางแผนเพื่อบริหารจัดการเว็บไซต์
- การตั้งค่าเครื่องบริการเว็บอย่างมั่นคงปลอดภัย
- การพัฒนาโปรแกรมประยุกต์บนเครื่องบริการเว็บอย่างมั่นคงปลอดภัย
- การรับมือสถานการณ์ภัยคุกคามที่เกิดจากการโจมตีเว็บ (Incident Handling)
- การใช้ Checklist สำหรับการวางแผนและตรวจสอบความมั่นคงปลอดภัยสำหรับเว็บไซต์

Introduction to Standard Development Office / ETDA

มาตรฐานเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์
(e-Transaction Standard)

ปัญหาของการไม่มีมาตรฐาน

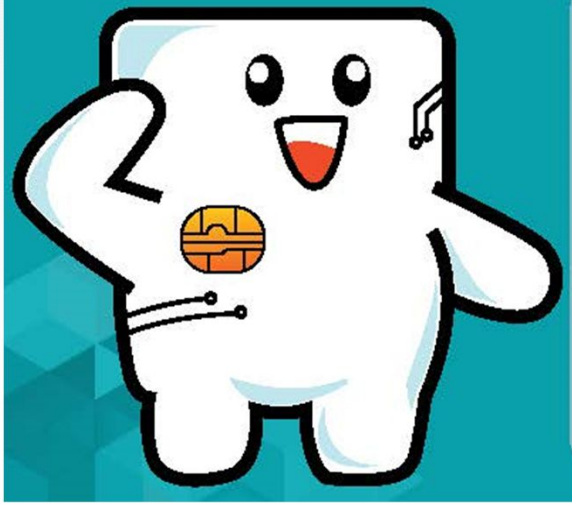
การแลกเปลี่ยนข้อมูลระหว่างระบบของหน่วยงานต่างๆ ไม่เข้าใจกัน



บริการด้านวิชาการ
ให้คำปรึกษาและวิจัยที่เกี่ยวกับมาตรฐาน

สำนักมาตรฐาน

เป็นหน่วยงานภายใต้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
มีหน้าที่หลักในการศึกษา วิจัย สำรวจเกี่ยวกับมาตรฐาน
และมีหน้าที่ในการสนับสนุนงานด้านการมาตรฐาน รวมถึงร่วมมือกับหน่วยงานต่าง ๆ
ในด้านการพัฒนา และส่งเสริมมาตรฐานที่เกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์
โดยมีผู้อำนวยการสำนักมาตรฐาน เป็นผู้บังคับบัญชารับผิดชอบ



ETDA
www.etda.or.th

OFFICE OF STANDARD

งานกลยุทธ์มาตรฐาน

ศึกษา วิจัย สำรวจมาตรฐานที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ และจัดทำข้อเสนอแนะเกี่ยวกับมาตรฐานที่จำเป็นต่อการทำธุรกรรมทางอิเล็กทรอนิกส์เพื่อนำไปประยุกต์ใช้งานในลักษณะ soft infrastructure รวมทั้งส่งเสริมให้การทำธุรกรรมทางอิเล็กทรอนิกส์ได้มาตรฐานที่กำหนด

งานพัฒนามาตรฐาน

กำหนดมาตรฐานการทำธุรกรรมของไทยขึ้นใช้งานโดยใช้กระบวนการ/ขั้นตอนที่ถูกต้องตามหลักสากล การทำงานเป็นเครือข่ายของผู้เชี่ยวชาญในประเทศ และงานตรวจสอบความถูกต้องเหมาะสมของการใช้มาตรฐาน

งานรับรองมาตรฐาน

การให้บริการรับรองบุคคล นิติบุคคล สินค้า บริการ ฯลฯ ว่าเป็นไปตามข้อกำหนดหลักเกณฑ์มาตรฐานที่กำหนดขึ้นใช้งาน

etda.or.th

WEB SECURITY STANDARD

1 WEBSITE SECURITY STANDARD (WSS)

ประกาศเป็น ETDA Rec. วันที่ 30 กย. 57

- เน้นที่การรักษาความมั่นคงปลอดภัย ของเว็บไซต์
- มีข้อกำหนดในการรักษาความมั่นคงปลอดภัยในส่วนต่าง ๆ ดังนี้
  โปรแกรมสำหรับให้บริการเว็บ (Web server software)
  ระบบบริหารจัดการเว็บไซต์ (CMS)
  ระบบฐานข้อมูล (Database system)
  และโปรแกรมประยุกต์บนเว็บ (Web applications)
  จากภัยคุกคามที่พบมากที่สุด (Top Threats)
- กำหนดแนวทางในการการรับมือสถานการณ์ภัยคุกคามที่เกิดจากการโจมตีเว็บไซต์ (security incident handling) และการสำรองข้อมูลเว็บไซต์
- มีแบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

2 WEB APPLICATION SECURITY STANDARD (WAS)

อยู่ระหว่างดำเนินการ

- เน้นที่การรักษาความมั่นคงปลอดภัย ในการพัฒนาและทดสอบโปรแกรมประยุกต์บนเว็บ
- มีข้อกำหนดและแนวทางในการพัฒนาและทดสอบโปรแกรมประยุกต์บนเว็บ ให้มีความมั่นคงปลอดภัย จากภัยคุกคามที่พบมากที่สุดบนโปรแกรมประยุกต์บนเว็บ (Top Threats)
- แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บ

3 THE STANDARD FOR SECURING e-COMMERCE WEBSITE (SEW)

ดำเนินการในอนาคต

- เน้นประเด็นด้านความมั่นคงปลอดภัย ของเว็บไซต์ด้าน e-Commerce
- มีข้อกำหนดของแนวทางในการพัฒนาร้านค้าและการชำระเงินออนไลน์ (Online Store and Payment)

WSS Overview

ETDA
สพธอ
www.etda.or.th

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)

ETDA
สพธอ
www.etda.or.th

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard for Electronic Transactions

ขมธอ.1 – 2557

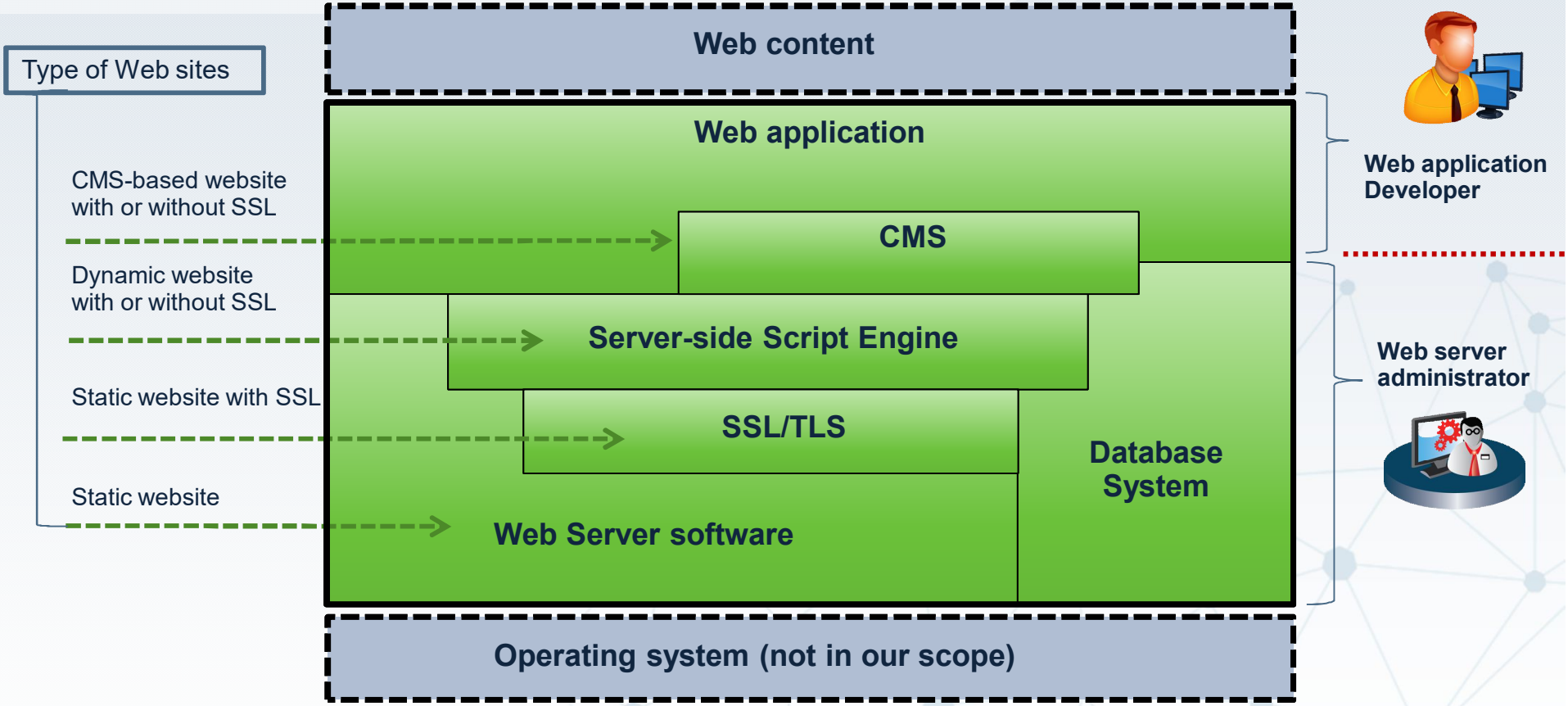
ว่าด้วยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์

Website Security Standard

เวอร์ชั่น 1.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

Scope of Website Security Standard



แนวทางการตรวจประเมินเว็บไซต์

1. ประเมินตนเอง (Self-assessment) และประกาศรับรองโดยตนเอง (Self-Declaration)
2. รับการยืนยันถึงความสอดคล้องกับมาตรฐานจากผู้มีส่วนได้ส่วนเสียกับเว็บไซต์
3. รับการยืนยันถึงการประกาศรับรองตนเองจากหน่วยงานภายนอก
4. ขอรับการรับรอง (certification) มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับผู้ดูแลและพัฒนาเว็บไซต์จากหน่วยตรวจสอบและรับรอง (Conformity assessment body)

เนื้อหาหลักในร่างมาตรฐาน

หัวข้อ 1 : ขอบเขต

หัวข้อ 2 : การนำไปใช้งาน

หัวข้อ 3 : นิยาม

กำหนดขอบเขตของมาตรฐาน วิธีการนำมาตรฐานไปใช้งาน และคำนิยามของศัพท์ซึ่งถูกอ้างอิงในมาตรฐานเพื่อให้เกิดความเข้าใจที่ตรงกันของผู้ปฏิบัติ

NIST SP 800-44

หัวข้อ 4 : การวางแผนเพื่อบริหารจัดการเว็บไซต์

- จัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของเว็บไซต์
- แนวทางการเลือกผู้รับจดทะเบียนชื่อโดเมน การเลือกบริการเว็บโฮสติ้ง และ CMS

ข้อกำหนดที่เกี่ยวกับแนวปฏิบัติในการรักษาความปลอดภัยของเว็บไซต์ และแนวทางการเลือกผู้รับจดทะเบียนชื่อโดเมน รวมถึงแนวทางการเลือกใช้บริการเว็บโฮสติ้ง

หัวข้อ 5 : การตั้งค่าเครื่องบริการเว็บอย่างมั่นคงปลอดภัย

ข้อกำหนดที่เกี่ยวข้องกับการติดตั้งและตั้งค่าของ Web server, Web server software, CMS, Database system และ Server-side script engine รวมถึงการกำหนดรหัสผ่าน

OWASP

หัวข้อ 6 : การพัฒนาโปรแกรมประยุกต์บนเครื่องบริการเว็บอย่างมั่นคงปลอดภัย

ข้อกำหนดที่เกี่ยวข้องการป้องกันการโจมตีเว็บไซต์จากเทคนิคและปัญหาหลัก ๆ ได้แก่ การป้องกันการโจมตีจากเทคนิค SQL Injection, Session Hijacking, Cross-site scripting, CSRF รวมถึงการป้องกันการโจมตีจากปัญหาข้อมูลลับรั่วไหล

ThaiCERT

NIST SP 800-44

หัวข้อ 7 : การรับมือสถานการณ์ภัยคุกคามเกิดจากการโจมตีเว็บไซต์

- การรับมือภัยคุกคามที่เกิดขึ้นกับเว็บไซต์ (Intrusion, Denial Of Service, Domain Hijack)
- การใช้โปรแกรมตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์
- การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log)
- การสำรองข้อมูลเว็บไซต์

ตรวจสอบว่ามีการวางแนวทางในการรับมือสถานการณ์ภัยคุกคามที่เกิดขึ้นกับเว็บไซต์ เพื่อให้รับทราบมาตรการและการดำเนินการที่เกี่ยวข้องในการรับมือเมื่อเกิดเหตุการณ์โจมตีในลักษณะต่างๆที่อาจเกิดขึ้นอย่างตรงกัน ทั้งแนวทางในการรับมือภัยคุกคามที่เกิดขึ้นกับเว็บไซต์, การใช้โปรแกรมตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์ และ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

NIST
- M. Tracy, W. Jansen, K. Scarfone, and T. Winograd, "Guidelines on Securing Public Web Server", National Institute of Standards and Technology, 2007. (NIST SP 800-44)

OWASP
- Open Web Application Security Project (OWASP). Available: https://www.owasp.org

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Self-assessment Checklist)

แบบประเมินสำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ
ตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

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	มีการตรวจสอบและปรับปรุงส่วนประกอบของโปรแกรมสำหรับให้บริการเว็บให้เป็นเวอร์ชันปัจจุบันอย่างสม่ำเสมอ (หัวข้อที่ 5.1 ข้อ 1)			
2.2	มีการควบคุมข้อความแจ้งเตือนหรือข้อความแสดงข้อผิดพลาด (Error Message) ไม่ให้แสดงข้อมูลที่เป็นประโยชน์ต่อผู้ประสงค์ร้าย (หัวข้อที่ 5.1 ข้อ 2)			
2.3	ได้กำหนดสิทธิในการเข้าถึงสารบบ (directory) ที่ใช้กับไฟล์หรือโปรแกรมต่าง ๆ ที่เกี่ยวข้องกับเครื่องบริการเว็บให้เหมาะสม เช่น กำหนดสิทธิไฟล์เตอร์ที่เก็บหน้าเว็บเพจของระบบหลังบ้าน อนุญาตให้เฉพาะผู้ดูแลเข้าถึงได้เท่านั้น (หัวข้อที่ 5.1 ข้อ 3)			
2.4	มีการตรวจสอบและจัดการลบ ตัวอย่างโปรแกรม ตัวอย่างไฟล์ข้อมูล บัญชีผู้ใช้ที่ไม่ได้ใช้งาน เช่น บัญชีซึ่งมีการใช้งานระหว่างกระบวนการติดตั้งเครื่องบริการเว็บทั้งหมด (หัวข้อที่ 5.1 ข้อ 4)			
2.5	ได้ตรวจสอบไม่ให้มีการใช้ค่าเริ่มต้นของ ชื่อสารบบ ชื่อไฟล์ข้อมูล ตำแหน่งไฟล์ข้อมูล รหัสผ่าน ที่มากับการติดตั้งเครื่องบริการเว็บ (หัวข้อที่ 5.1 ข้อ 5)			

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์
(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
2.6	มีการควบคุมการเข้าถึงเครื่องบริการเว็บ และจำกัดหมายเลขไอพีปลายทางหรือยูอาร์แอลที่อนุญาตให้เครื่องบริการเว็บสามารถเชื่อมต่อ เช่น การกำหนด IP Whitelist ที่สามารถเข้าถึงเครื่องบริการเว็บ (หัวข้อที่ 5.1 ข้อ 6)			
2.7	ปิดบริการต่างๆ 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	ตรวจสอบการอัพเดตเวอร์ชันของระบบบริหารจัดการเว็บไซต์อยู่เสมอ และอัพเดตเวอร์ชันให้เป็นปัจจุบัน (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)			
4.2	ควบคุมการเข้าถึงระบบฐานข้อมูลด้วยระบบรักษาความมั่นคงปลอดภัย เช่น ด่านกันขุกรุกหรือไฟร์วอลล์ (Firewall) (หัวข้อที่ 5.3 ข้อ 2)			
4.3	ตรวจสอบและปิดบริการ (Services, Extension) ที่ไม่จำเป็นหรือไม่ได้ใช้งาน ในระบบฐานข้อมูล เช่น phpMyAdmin (หัวข้อที่ 5.3 ข้อ 3)			

การวางแผนเพื่อบริหารจัดการเว็บไซต์

การวางแผนเพื่อบริหารจัดการเว็บไซต์

- **การวางแผนด้านความมั่นคงปลอดภัยเพื่อบริหารจัดการเว็บไซต์**
  1) การวางแผนเพื่อบริหารจัดการเครื่องบริการเว็บ
  2) จัดลำดับความเสี่ยงของภัยคุกคามที่คาดว่าจะเกิดขึ้นกับเว็บไซต์
  3) กำหนดมาตรการที่เกี่ยวข้องเพื่อป้องกันภัยคุกคามที่มีความสำคัญ

- **แนวทาง : การเลือกรูปแบบเครื่องบริการเว็บ**
- **แนวทาง : การเลือกระบบบริหารจัดการเว็บไซต์ (CMS)**
- **แนวทาง : การเลือกผู้รับจดทะเบียนโดเมน**

การวางแผนด้านความมั่นคงปลอดภัยเพื่อบริหารจัดการเว็บไซต์

1) การวางแผนเพื่อบริหารจัดการเครื่องบริการเว็บ :Checklist 1.1

หัวข้อ	ตัวอย่าง
จุดประสงค์ของการทำเว็บไซต์	เพื่อประชาสัมพันธ์องค์กรและเผยแพร่ข้อมูลที่เกี่ยวข้องแก่บุคคลทั่วไป
คุณสมบัติของเครื่องบริการเว็บ	เครื่องบริการเว็บที่ใช้คือ Internet Information Services (Microsoft IIS))
โปรแกรมประยุกต์บนเว็บสำหรับบริการด้านใด	- ฐานข้อมูล = MySQL เพื่อเก็บไฟล์ข้อมูลต่างๆ ของเว็บไซต์
การเก็บรักษาข้อมูลบนเว็บ	- เก็บข้อมูลต่างๆ ของเว็บไซต์ในฐานข้อมูล โดยป้องกันฐานข้อมูลด้วย Firewall และฐานข้อมูลต้องเข้ารหัสโดยผู้ที่เกี่ยวข้องเท่านั้น
การกำหนดหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้อง	- Web Server Administrator = นาย A หน้าที่ความรับผิดชอบ = ออกแบบ ตั้งค่าและดูแลจัดการเครื่องบริการเว็บให้มีความมั่นคงปลอดภัย - Web Developer = นาย B หน้าที่ความรับผิดชอบ = พัฒนาเว็บไซต์ให้มีประสิทธิภาพและมีความมั่นคงปลอดภัยตามจุดประสงค์ของการจัดทำเว็บไซต์ - IT Manager = นาย C หน้าที่ความรับผิดชอบ = วางแผนและดูแลให้การดำเนินงานเป็นไปตามระเบียบและข้อบังคับที่ระบุไว้ในนโยบายการรักษาความปลอดภัยขององค์กร

รายละเอียดเพิ่มเติมที่ หัวข้อที่ 3 “Planning and Managing Web Server” ของมาตรฐาน NIST SP 800-44

etda.or.th

2) จัดลำดับความเสี่ยงของภัยคุกคามที่คาดว่าจะเกิดขึ้นกับเว็บไซต์ : Checklist 1.2

2.1) จัดทำ list รายการของสินทรัพย์ของเว็บไซต์ (Asset Inventory) รวมถึงมูลค่าของสินทรัพย์ (Asset value) และผู้รับผิดชอบที่เกี่ยวข้อง

Example of Asset List [Annex B: ISO/IEC 27005]

- Business processes & activities
- Information
- Hardware
- Software
- Network
- Personnel
- Site
- Organization's structure

รายละเอียดเพิ่มเติมที่ มาตรฐาน ISO/IEC 27005:2011

ประเภทรายการสินทรัพย์	รายการสินทรัพย์	มูลค่าของสินทรัพย์	ผู้รับผิดชอบที่เกี่ยวข้อง
Hardware	เครื่องคอมพิวเตอร์ (PC)	30,000 บาท	นาย C (IT Manager)
Software	Operating System : คือ Windows 8	9,000 บาท	นาย A (Web Server Administrator)
	Database Management Software : คือ MySQL	1,000 บาท	นาย A (Web Server Administrator)
	Web Server Software : คือ Microsoft IIS	-	นาย A (Web Server Administrator)
	Content management system คือ WordPress	-	นาย A (Web Server Administrator)

2) จัดลำดับความเสี่ยงของภัยคุกคามที่คาดว่าจะเกิดขึ้นกับเว็บไซต์ (ต่อ) : Checklist 1.2

2.2) การระบุภัยคุกคาม (threat) ความเป็นไปได้ที่คาดว่าน่าจะเกิดภัยคุกคามดังกล่าวขึ้น และผลกระทบ (Impact) ต่อสินทรัพย์หากมีภัยคุกคามดังกล่าวเกิดขึ้น

Asset	Example Threat
Hardware	Equipment failure, Software malfunction, Dust, corrosion, freezing, Theft of equipment,
Software	Eavesdropping, Theft of media or document, Error in use (Complicated user interface), Abuse of Rights (wrong allocation of access right, well- know flow in the software), Denial of action, Illegal processing of data, Corruption of Data

รายละเอียดเพิ่มเติมที่ มาตรฐาน ISO/IEC 27005:2011

ประเภทรายการสินทรัพย์	รายการสินทรัพย์	ภัยคุกคาม	ความน่าจะเป็นในการเกิดภัยคุกคาม	ผลกระทบ (Impact) ต่อสินทรัพย์
Hardware	เครื่องคอมพิวเตอร์ (PC) 	equipment failure	Low	• The cost of acquisition • configuration and Installation of the new asset or back-up
Software	Content management system (CMS) [=WordPress] 	Denial of action	High	• The cost of suspended operations due to the incident until the service provided by the asset is restored.

ตัวอย่างภัยคุกคามที่พบ ใน Content management system (CMS)

ระวังภัย ช่องโหว่ใน Drupal และ WordPress ผู้ไม่หวังดีสามารถโจมตีระบบในลักษณะ DoS ได้

วันที่ประกาศ: 8 สิงหาคม 2557
เรื่อง: ระวังภัย ช่องโหว่ใน Drupal และ WordPress ผู้ไม่หวังดีสามารถโจมตีระบบในลักษณะ DoS ได้

ประเภทภัยคุกคาม: DoS (Denial-of-Service)

ข้อมูลทั่วไป

ในวันที่ 6 สิงหาคม 2557 เว็บไซต์ทางการของ Drupal ได้ประกาศว่าพบช่องโหว่ในซอฟต์แวร์ Drupal ซึ่งเป็นเครื่องมือในการจัดการเนื้อหา (CMS) โดยเกิดช่องโหว่ในส่วนประกอบของ XML-RPC และ OpenID ที่เปิดโอกาสให้ผู้ไม่หวังดีสามารถโจมตีเว็บไซต์ในลักษณะ DoS ผ่านช่องโหว่ดังกล่าวได้[1] โดยจะส่งผลให้การใช้งาน CPU และ Memory ตลอดจนการเชื่อมต่อฐานข้อมูลเพิ่มขึ้นมากผิดปกติ จนทำให้เว็บไซต์ไม่สามารถทำงานได้ตามปกติ จนต้องหยุดให้บริการในที่สุด

ช่องโหว่นี้ยังมีผลกระทบกับระบบ WordPress ด้วย เนื่องจากมีการใช้งานส่วนประกอบ XML-RPC เช่นกัน ดังที่มีการแจ้งเตือนในเว็บไซต์ของ WordPress ในวันเดียวกัน [2]

3) กำหนดมาตรการที่เกี่ยวข้องเพื่อป้องกันภัยคุกคามที่มีความสำคัญ : Checklist 1.3

ประเภทรายการสินทรัพย์	รายการสินทรัพย์	ภัยคุกคาม	ความน่าจะเป็นในการเกิดภัยคุกคาม	ผลกระทบ (Impact) ต่อสินทรัพย์
Software	Content management system (CMS) [=WordPress]	Denial of action	High	• The cost of suspended operations due to the incident until the service provided by the asset is restored.

Threat: Denial of action

มาตรการเพื่อป้องกันภัยคุกคาม :

1.อัพเดตซอฟต์แวร์เป็นรุ่นล่าสุดที่ได้รับการแก้ไขช่องโหว่นี้แล้ว จากเว็บไซต์ทางการของ Drupal และ WordPress

2.จัดทำแนวทางการรับมือภัยคุกคามเพื่อบริหารความต่อเนื่องทางธุรกิจ หรือ Business Continuity Plan (BCP) อ้างอิงแนวทางการจัดทำ BCP ได้จาก มาตรฐาน ISO 22301, Business continuity management และ ISO/IEC 27031:2011, Guidelines for information and communication technology readiness for business continuity

รายละเอียดเพิ่มเติมที่ มาตรฐาน ISO/IEC 27002:2013

แนวทาง : การเลือกรูปแบบเครื่องบริการเว็บ

➢ **การให้บริการเว็บโฮสติ้งมีการให้บริการระหว่าง Shared หรือ Dedicated**

Shared	Dedicated
ใช้เครื่องบริการเว็บร่วมกันระหว่างผู้ใช้บริการหลายๆ ราย	ผู้ใช้บริการแต่ละรายจะได้เครื่องบริการเว็บแยกกัน
มีค่าใช้จ่ายต่ำ	มีค่าใช้จ่ายสูง
มีความเสี่ยงจากการถูกโจมตีผ่านช่องโหว่ของเว็บไซต์อื่น	ป้องกันความเสี่ยงจากการถูกโจมตีผ่านช่องโหว่ของเว็บไซต์อื่นได้

➢ **การพิจารณาจากรูปแบบนโยบายการจัดการช่องโหว่**

- มีนโยบายที่ชัดเจนในการป้องกันความเสียหายที่อาจจะเกิดจากช่องโหว่ เช่น แจ้งให้ผู้ใช้บริการทราบในทันที การ patch หรือแก้ไขปัญหาเฉพาะหน้า (Workaround)
- ในกรณีที่เป็นช่องโหว่ที่ไม่สามารถหาวิธีแก้ไข ต้องมีการเตรียมแผนสำรอง
- มีการพิจารณาถึงความรับผิด (Liability) ที่ผู้ให้บริการอาจจะต้องชดเชยในกรณีที่เกิดความเสียหายแก่ผู้ใช้บริการในกรณีที่เกิดความบกพร่องในการจัดการกับช่องโหว่ด้วย

- **รูปแบบการให้บริการโอนย้ายไฟล์ข้อมูล (Remote file transfer)**
  - ช่องทางการโอนย้ายไฟล์ที่มั่นคงปลอดภัยและมีการเข้ารหัสเพื่อรักษาความลับของข้อมูลระหว่างการโอนย้าย เช่น มีบริการ Secure Transfer Protocol (SFTP)

- **การสำรองข้อมูลและการดูแลรักษาเครื่องบริการเว็บ**
  - มีการสำรองข้อมูลของเครื่องบริการเว็บที่อยู่ในความดูแลอย่างสม่ำเสมอ
  - มีนโยบายที่เกี่ยวข้องกับการสำรองและกู้คืนข้อมูลของผู้ให้บริการ

- **การติดต่อผู้ให้บริการเมื่อมีเหตุฉุกเฉิน**
  - มีช่องทางติดต่อเฉพาะสำหรับกรณีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัย เพื่อการประสานงานอย่างทันท่วงที

- **การให้บริการรูปแบบการสื่อสารอย่างมั่นคงปลอดภัยสำหรับเว็บไซต์ (บริการโพรโทคอล SSL/TLS)**
  - มีบริการโพรโทคอล SSL (Secure Socket Layer protocol) และ TLS (Transport Layer Security protocol) ซึ่งจะช่วยป้องกันการสื่อสารของโปรแกรมประยุกต์ในระบบรับ-ให้ (Client-Server system) จากการลอบฟัง การแก้ไขให้เสียหาย และ การปลอมแปลงข้อความที่ใช้ในการสื่อสาร

etda.or.th

แนวทาง : การเลือกระบบบริหารจัดการเว็บไซต์ (CMS)

ตัวเลือกที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย

- มีเอกสารแนะนำแนวทางการติดตั้งและการตั้งค่าเพื่อรักษาความมั่นคงปลอดภัย (Security best practice)
- มีแหล่งข้อมูลและเอกสารสนับสนุนที่เกี่ยวข้องกับการติดตั้ง การตั้งค่า และ แนวทางการรักษาความมั่นคงปลอดภัย

คุณภาพของประชาคมนักพัฒนา CMS

- ประชาคมนักพัฒนามีขนาดใหญ่ มีการสื่อสารภายใน และพัฒนาอย่างต่อเนื่อง (Active developer community) ก็จะเป็น CMS ที่มีฟังก์ชั่นการทำงานตอบสนองต่อความต้องการของผู้ใช้ได้มากกว่า
- มีการปรับเวอร์ชั่นหรือปรับปรุงระบบ เพื่อแก้ไขข้อบกพร่องและช่องโหว่ของ CMS อยู่เสมอ

แนวทาง : การเลือกผู้รับจดทะเบียนโดเมน

ผู้รับจดทะเบียนชื่อโดเมนมีกระบวนการยืนยันการลงทะเบียน เช่น ส่ง URL เพื่อยืนยันการลงทะเบียนแนบไปในอีเมล

มีมาตรการในการเพิ่มความมั่นคงปลอดภัยให้กับรหัสผ่าน (Strong Password)

มีการแจ้งเตือนและการยืนยันการเปลี่ยนแปลงข้อมูลการลงทะเบียน เพื่อช่วยป้องกันการเปลี่ยนแปลงจากผู้ประสงค์ร้าย

การตั้งค่าเครื่องบริการเว็บอย่างมั่นคงปลอดภัย

- Web Server Software
- Password
- Database System
- CMS
- Server-site Script Engine

การตั้งค่าโปรแกรมสำหรับให้บริการเว็บ (Web Server Software)

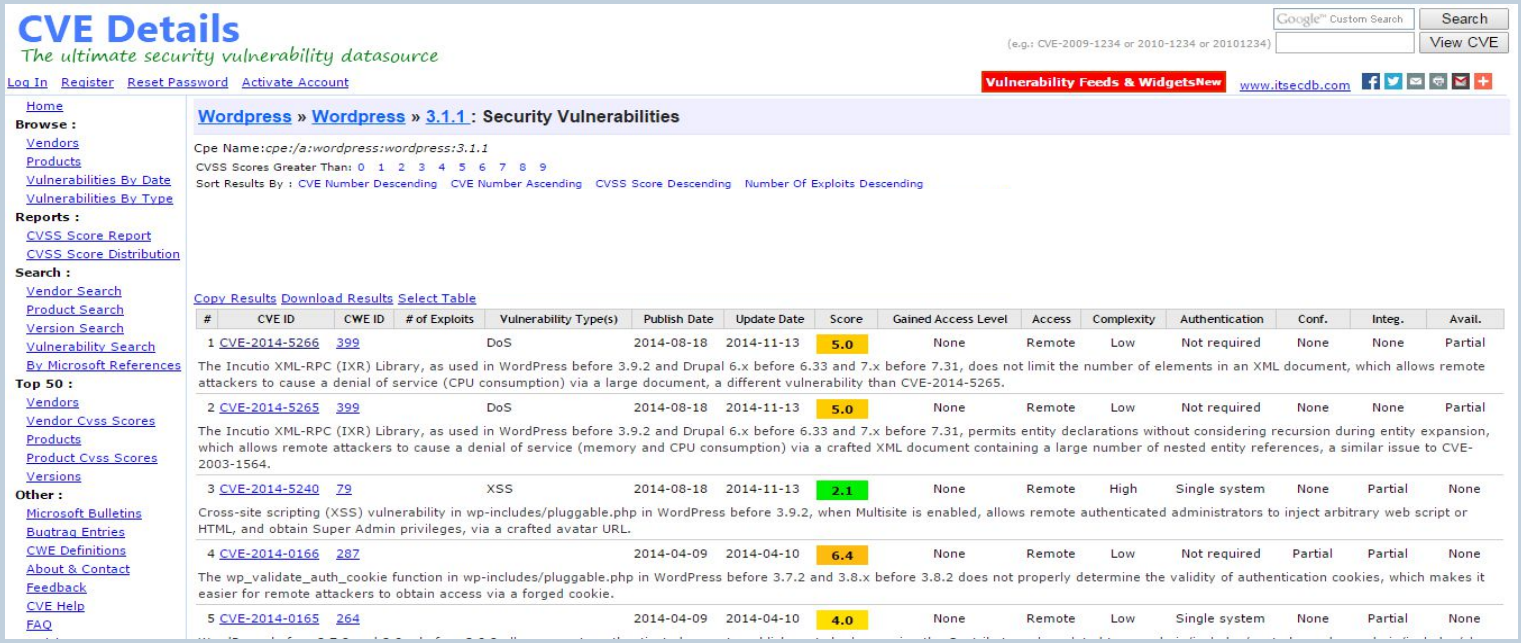
- ปรับปรุงส่วนประกอบของโปรแกรมสำหรับให้บริการอย่างสม่ำเสมอ (Update latest version/patch)
- ควบคุมข้อความแจ้งเตือนหรือข้อความแสดงข้อผิดพลาด (Error Message) ไม่ให้แสดงข้อมูลที่เป็นประโยชน์ต่อผู้ประสงค์ร้าย
- จัดหมวดหมู่ของสารบบ (Directory) ที่ใช้เก็บไพล์ข้อมูล เว็บเพจ ระบบปฏิบัติการ โปรแกรมสำหนับให้บริการเว็บ และโปรแกรมอื่น ๆ โดยจะต้องกำหนดสิทธิในการเข้าถึงให้เหมาะสมกับการใช้งาน
- ตรวจสอบและจัดการลบ ตัวอย่างโปรแกรม ตัวอย่างไฟล์ข้อมูล บัญชีผู้ใช้ที่ไม่ได้ใช้งานแล้ว
- ตรวจสอบไม่ให้มีการใช้ค่าเริ่มต้นของชื่อสารบบ ชื่อไฟล์ข้อมูล ตำแหน่งไฟล์ข้อมูล รหัสผ่าน ที่มากับการติดตั้งบริการเว็บ
- ควบคุมการเข้าถึงเครื่องให้บริการเว็บ และจำกัดหมายเลขไอพีปลายทาง หรือ ยูอาร์แอลที่อนุญาตให้เครื่องบริการเว็บสามารถเชื่อมต่อ (Whitelist)
- ปิดบริการต่าง ๆที่ไม่จำเป็นบนเครื่องบริการเว็บ เช่น Remote Desktop, Telnet, ftp

การปรับปรุงโปรแกรมประยุกต์ต่างๆ ให้เป็นเวอร์ชั่นล่าสุด

ปัญหาที่พบ

การใช้โปรแกรมประยุกต์ที่ไม่ใช่รุ่นล่าสุดมีความเสี่ยงที่จะถูกโจมตีจากผู้ประสงค์ร้ายได้ เช่น

- WordPress 3.1.1 (รุ่นเก่า) มีการประกาศรายการช่องโหว่บนเว็บไซต์ที่ทุกคนสามารถเข้าถึงได้



CVE Details

The ultimate security vulnerability datasource

Log In Register Reset Password Activate Account

Vulnerability Feeds & WidgetsNew www.itsecdb.com

Search View CVE (e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ

Wordpress » Wordpress » 3.1.1 : Security Vulnerabilities

Cpe Name:*cpe:/a:wordpress:wordpress:3.1.1*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results Select Table

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2014-5266	399		DoS	2014-08-18	2014-11-13	5.0	None	Remote	Low	Not required	None	None	Partial

The Incutio XML-RPC (IXR) Library, as used in WordPress before 3.9.2 and Drupal 6.x before 6.33 and 7.x before 7.31, does not limit the number of elements in an XML document, which allows remote attackers to cause a denial of service (CPU consumption) via a large document, a different vulnerability than CVE-2014-5265.

2	CVE-2014-5265	399		DoS	2014-08-18	2014-11-13	5.0	None	Remote	Low	Not required	None	None	Partial

The Incutio XML-RPC (IXR) Library, as used in WordPress before 3.9.2 and Drupal 6.x before 6.33 and 7.x before 7.31, permits entity declarations without considering recursion during entity expansion, which allows remote attackers to cause a denial of service (memory and CPU consumption) via a crafted XML document containing a large number of nested entity references, a similar issue to CVE-2003-1564.

3	CVE-2014-5240	79		XSS	2014-08-18	2014-11-13	2.1	None	Remote	High	Single system	None	Partial	None

Cross-site scripting (XSS) vulnerability in wp-includes/pluggable.php in WordPress before 3.9.2, when Multisite is enabled, allows remote authenticated administrators to inject arbitrary web script or HTML, and obtain Super Admin privileges, via a crafted avatar URL.

4	CVE-2014-0166	287			2014-04-09	2014-04-10	6.4	None	Remote	Low	Not required	Partial	Partial	None

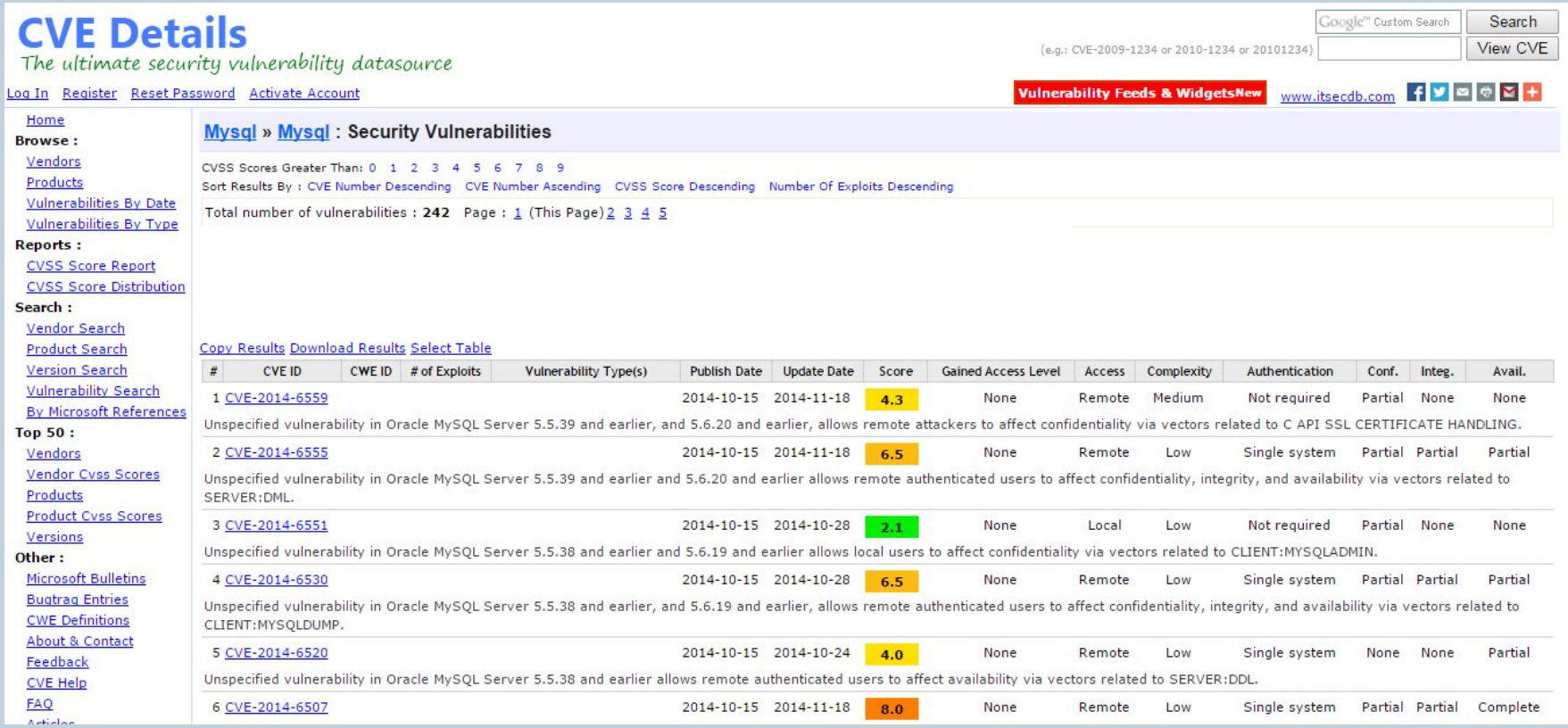
The wp_validate_auth_cookie function in wp-includes/pluggable.php in WordPress before 3.7.2 and 3.8.x before 3.8.2 does not properly determine the validity of authentication cookies, which makes it easier for remote attackers to obtain access via a forged cookie.

5	CVE-2014-0165	264			2014-04-09	2014-04-10	4.0	None	Remote	Low	Single system	None	Partial	None

http://www.cvedetails.com/vulnerability-list/

การปรับปรุงโปรแกรมประยุกต์ต่างๆ ให้เป็นเวอร์ชั่นล่าสุด (ต่อ)

- Oracle MySQL Server (รุ่นเก่า) มีการประกาศรายการช่องโหว่บนเว็บไซต์ที่ทุกคนสามารถเข้าถึงได้



CVE Details

The ultimate security vulnerability datasource

Google™ Custom Search | Search | (e.g.: CVE-2009-1234 or 2010-1234 or 20101234) | View CVE

Log In | Register | Reset Password | Activate Account

Vulnerability Feeds & WidgetsNew | www.itsecdb.com

Home

Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type

Reports :
CVSS Score Report
CVSS Score Distribution

Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References

Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions

Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ

Mysql » Mysql : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending | CVE Number Ascending | CVSS Score Descending | Number Of Exploits Descending

Total number of vulnerabilities : **242** Page : 1 (This Page) 2 3 4 5

Copy Results | Download Results | Select Table

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2014-6559				2014-10-15	2014-11-18	4.3	None	Remote	Medium	Not required	Partial	None	None
Unspecified vulnerability in Oracle MySQL Server 5.5.39 and earlier, and 5.6.20 and earlier, allows remote attackers to affect confidentiality via vectors related to C API SSL CERTIFICATE HANDLING.														
2	CVE-2014-6555				2014-10-15	2014-11-18	6.5	None	Remote	Low	Single system	Partial	Partial	Partial
Unspecified vulnerability in Oracle MySQL Server 5.5.39 and earlier and 5.6.20 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to SERVER:DML.														
3	CVE-2014-6551				2014-10-15	2014-10-28	2.1	None	Local	Low	Not required	Partial	None	None
Unspecified vulnerability in Oracle MySQL Server 5.5.38 and earlier and 5.6.19 and earlier allows local users to affect confidentiality via vectors related to CLIENT:MYSQLADMIN.														
4	CVE-2014-6530				2014-10-15	2014-10-28	6.5	None	Remote	Low	Single system	Partial	Partial	Partial
Unspecified vulnerability in Oracle MySQL Server 5.5.38 and earlier, and 5.6.19 and earlier, allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to CLIENT:MYSQLDUMP.														
5	CVE-2014-6520				2014-10-15	2014-10-24	4.0	None	Remote	Low	Single system	None	None	Partial
Unspecified vulnerability in Oracle MySQL Server 5.5.38 and earlier allows remote authenticated users to affect availability via vectors related to SERVER:DDL.														
6	CVE-2014-6507				2014-10-15	2014-11-18	8.0	None	Remote	Low	Single system	Partial	Partial	Complete

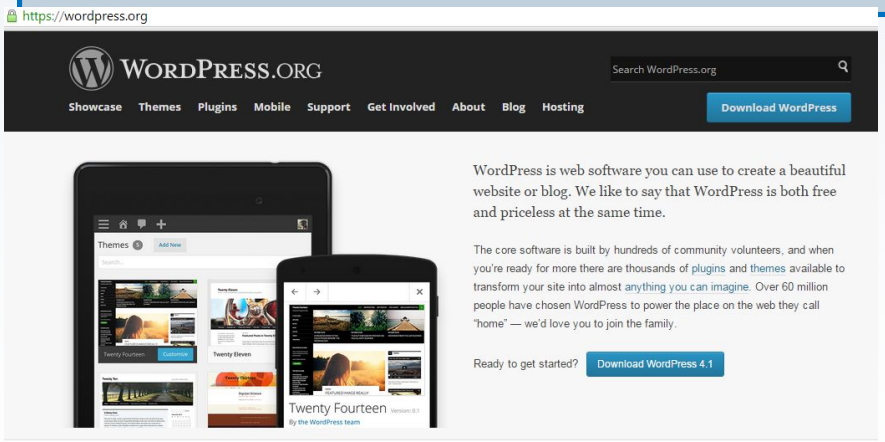
http://www.cvedetails.com/vulnerability-list/

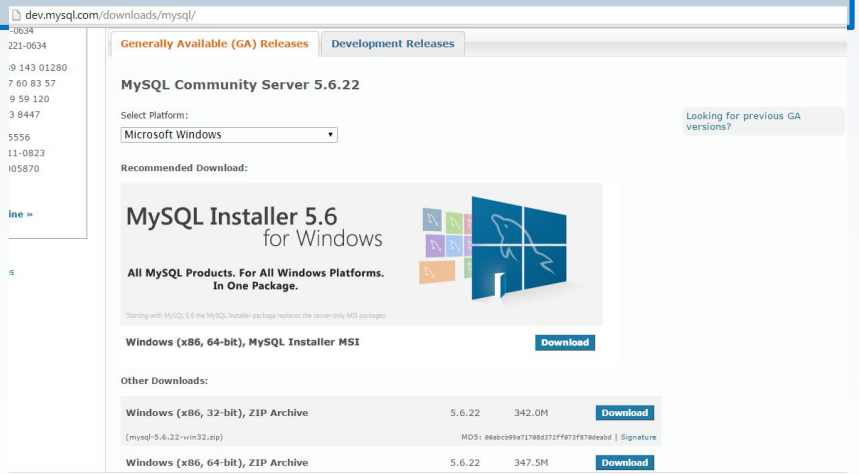
การปรับปรุงโปรแกรมประยุกต์ต่างๆ ให้เป็นเวอร์ชั่นล่าสุด (ต่อ)

ตัวอย่างวิธีการป้องกัน

- หมั่นตรวจสอบการอัพเดตเวอร์ชั่นของระบบบริหารจัดการเว็บไซต์อยู่เสมอ และอัพเดตเวอร์ชั่นให้เป็นปัจจุบัน ให้ดาวน์โหลดไฟล์จากเว็บไซต์หลักของผู้ให้บริการโปรแกรมประยุกต์นั้นๆ เท่านั้น
- อัพเดตโปรแกรมประยุกต์ที่ใช้งานและเกี่ยวข้องทั้งหมด เช่น Web Server Software, CMS, Database, Server-Side Script Engine, ปลั๊กอินเสริมในระบบ CMS เป็นต้น

<u>หัวข้อตาม Checklist ที่เกี่ยวข้อง</u> : Checklist 2.1, Checklist 3.3, Checklist 4.8, Checklist 5.2



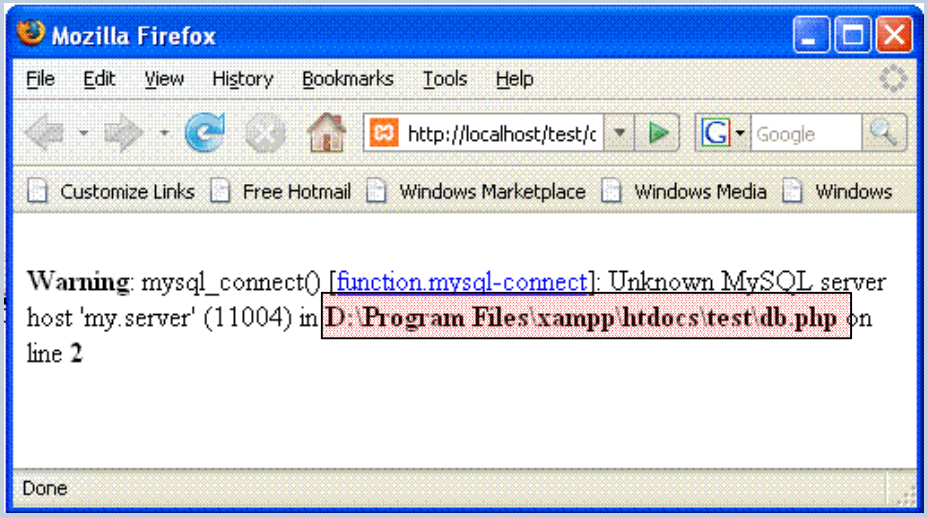


การควบคุมข้อความแจ้งเตือนหรือข้อความแสดงข้อผิดพลาด (Error Message)

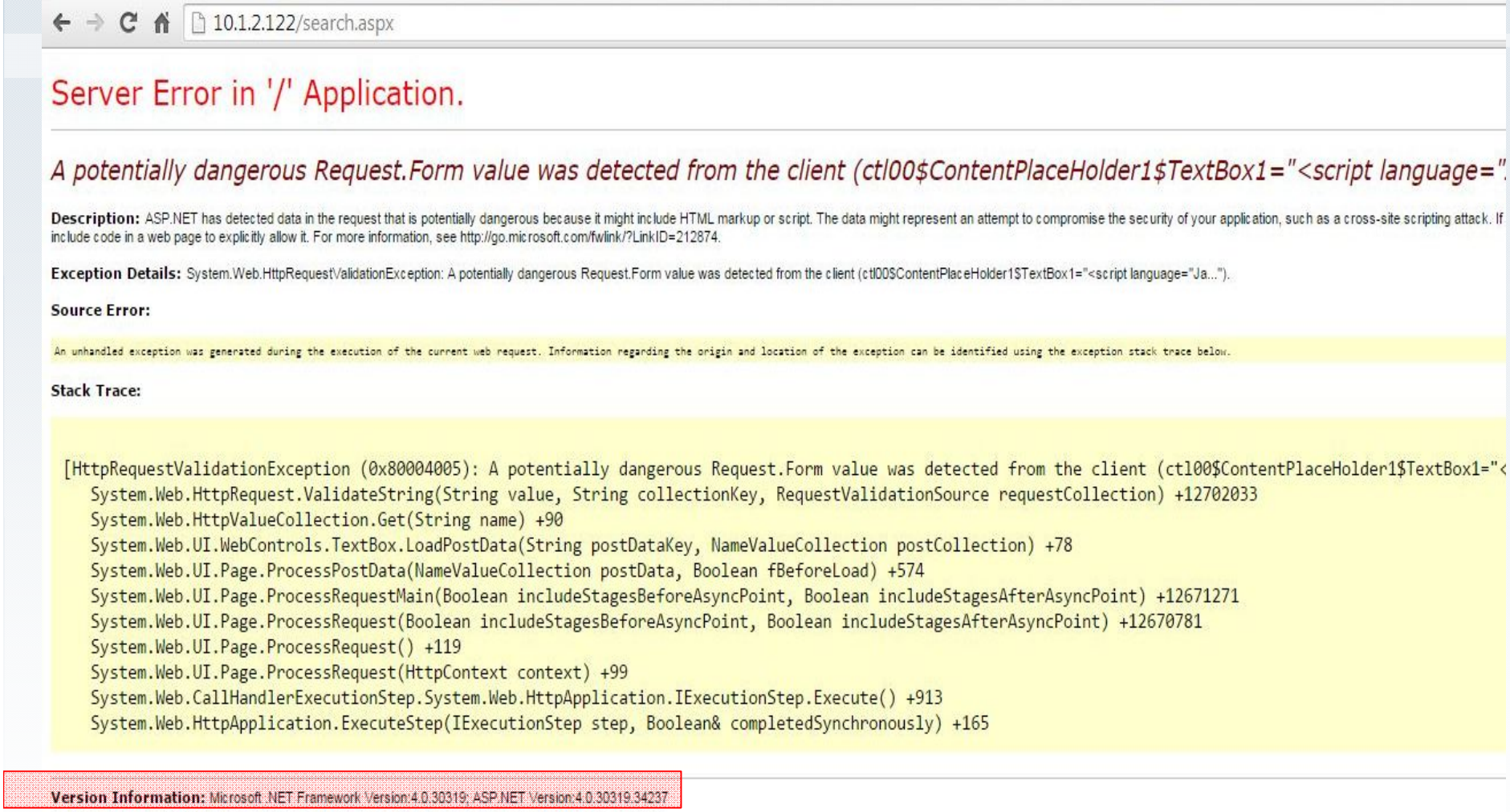
ปัญหาที่พบ

•การไม่ควบคุม Error Message ผู้ประสงค์ร้ายสามารถใช้ข้อมูลจาก Error Message คาดเดาข้อมูลการตั้งค่าของโปรแกรมและระบบที่เกี่ยวข้องได้ เช่น

Database Error Message



ตัวอย่าง Server Error Message



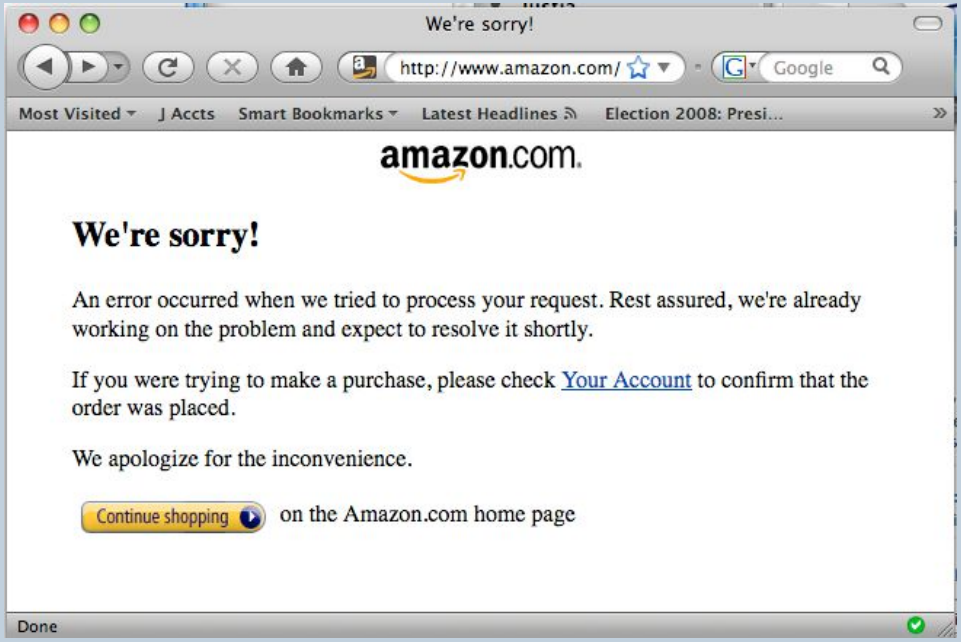
การควบคุมข้อความแจ้งเตือนหรือข้อความแสดงข้อผิดพลาด (Error Message) (ต่อ)

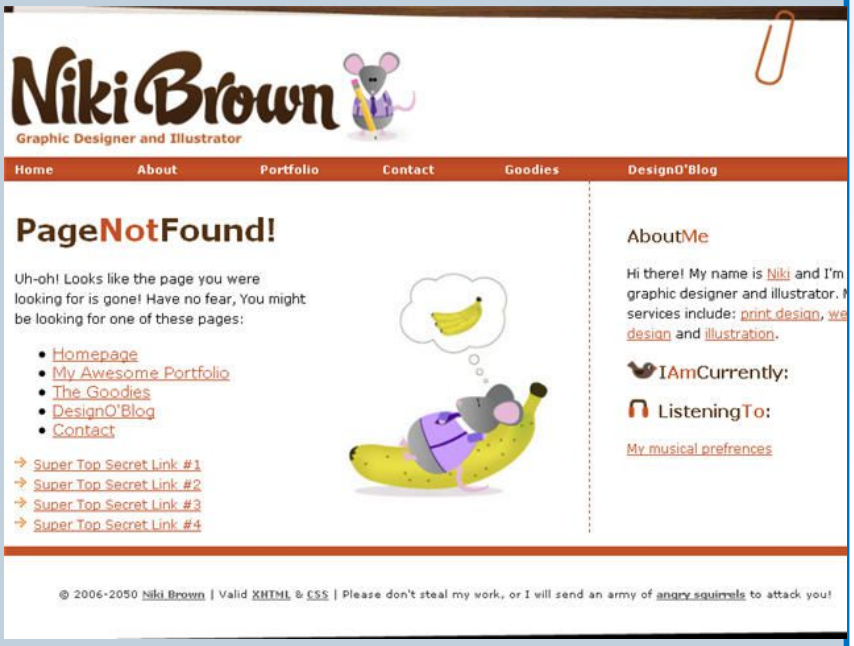
ตัวอย่างวิธีการป้องกัน

•ไม่ให้มีการแสดงรายละเอียดของข้อความแสดงข้อผิดพลาด (Error message) หากต้องมีรายละเอียดควรจะแสดงข้อมูลเท่าที่จำเป็นและไม่เป็นประโยชน์กับผู้ประสงค์ร้าย โดยสามารถตั้งค่าในส่วนนี้ได้ที่ Web Server Software, Server-side Script Engine เป็นต้น

<u>หัวข้อตาม Checklist ที่เกี่ยวข้อง</u> : Checklist 2.2, Checklist 5.4, Checklist 9.3, Checklist 11.1

ตัวอย่าง เว็บไซต์ที่มีการควบคุม Error Message





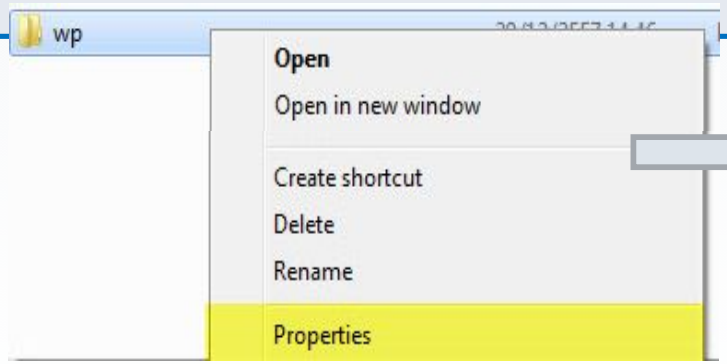
การจัดการ Permission / Access Control

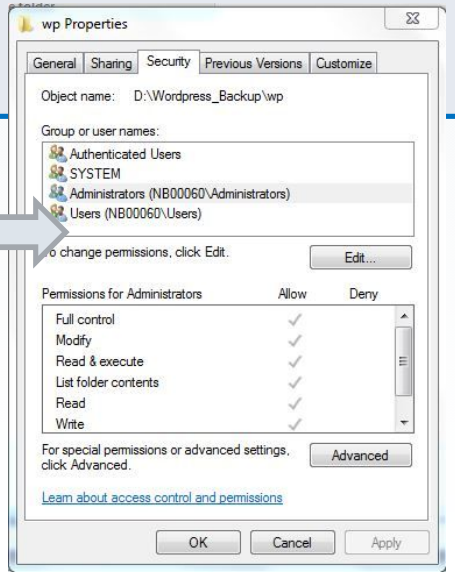
• หากไม่มีการควบคุมการเข้าถึงข้อมูลที่มีความสำคัญ เช่น ไฟล์ที่เก็บข้อมูลเว็บเพจ ผู้ใช้ทั่วไปต้องได้สิทธิแค่อ่านเท่านั้น หากสามารถแก้ไขได้ ผู้ใช้ที่ประสงค์ร้ายก็จะสามารถเข้าถึงและแทรกสคริปต์อันตราย หรือแก้ไขข้อมูลใดๆ ให้เกิดความเสียหายแก่เว็บไซต์ได้ เป็นต้น

ตัวอย่างวิธีการป้องกัน

• ต้องมีการกำหนดสิทธิการใช้งาน (permission) และการควบคุมการเข้าถึง (access control) ไฟล์ต่าง ๆ ให้เหมาะสมกับบทบาทและหน้าที่ของผู้ใช้บริการ เช่น

• ให้สิทธิการเข้าถึงไฟล์ หรือโฟลเดอร์ที่เก็บโปรแกรมแก่ผู้ใช้ที่เป็นเจ้าของไฟล์หรือนักพัฒนาซอฟต์แวร์เท่านั้น ผู้ใช้บริการทั่วไปได้รับสิทธิแค่อ่านและไม่สามารถแก้ไขได้ หรือผู้ดูแลเครื่องบริการเว็บได้รับสิทธิทั้งอ่าน เขียน และแก้ไขได้ เป็นต้น





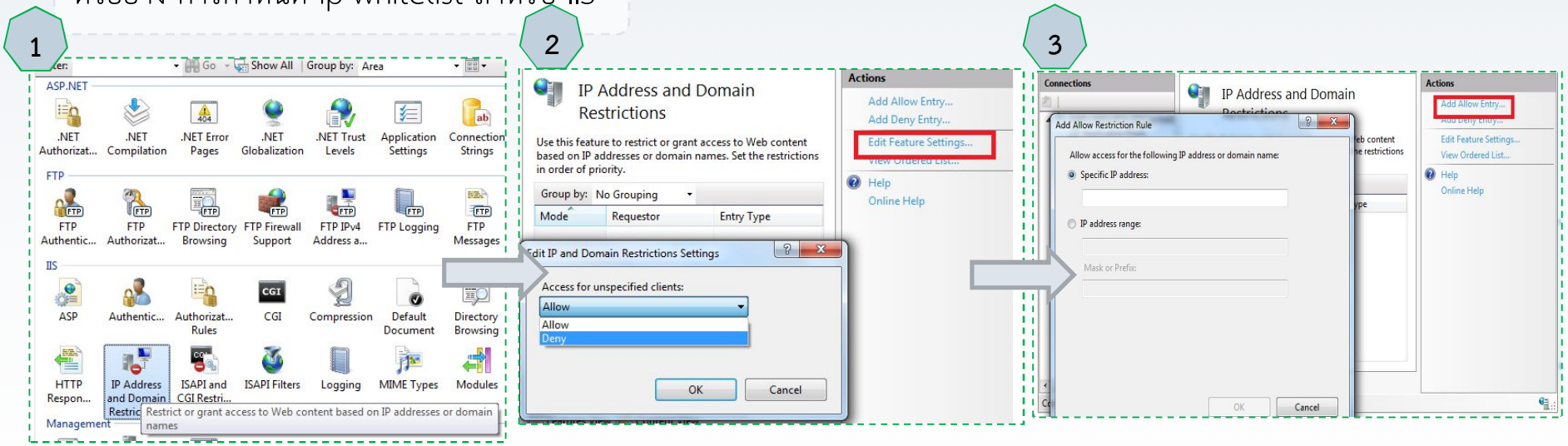
การจัดการ Permission / Access Control (ต่อ)

ตัวอย่างการจัดการ Access Control โดยการตั้งค่า IP Whitelist

- ควบคุมการเข้าถึงเครื่องบริการเว็บ และจำกัดหมายเลขไอพีปลายทางหรือยูอาร์แอล ที่อนุญาตให้เครื่องบริการเว็บสามารถเชื่อมต่อ (Whitelist)

<u>หัวข้อตาม Checklist ที่เกี่ยวข้อง</u> : Checklist 2.3, Checklist 2.6, Checklist 3.1 , Checklist 4.1 , Checklist 4.9 , Checklist 5.1

ตัวอย่าง การกำหนด ip whitelist สำหรับ IIS



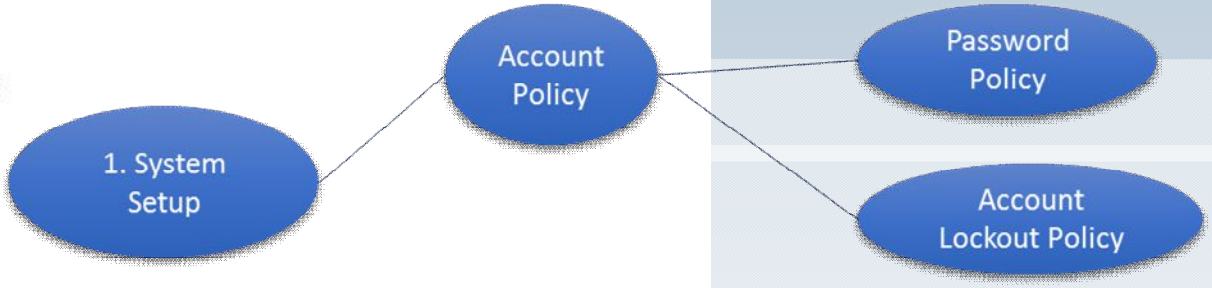
Hardening Guideline for Windows Server

- 1. System Setup
  - Account Policy
    - Password Policy
    - Account Lockout Policy
  - Local Policy
    - Audit Policy
    - Security Option
- 2. System Logs
  - Event Log
- 3. Network and Sharing
  - Internet Communication
  - SMB Protocol
  - TCP Timestamp
  - Network Share
- 4. Additional Security Setting
  - Autoplay
  - Windows Services

Microsoft Windows 2012 R2

Version - Release Levels/applicable to:

- Microsoft Windows Server 2012R2, Standard Edition
- Microsoft Windows Server 2012R2, Enterprise Edition
- Microsoft Windows Server 2012R2, Datacenter Edition
- Microsoft Windows Server 2012R2, Web Edition



1. System Setup

1.1 Account Policies (secpol.msc)

1.1.1 Password Policy

1. Run command "secpol.msc"
2. Expand "Account Polices" and Click on "Password Policy"

Figure 1 Password Policy

3. Setting these parameters :

System Value / Parameter	Default Setting	Recommended Setting	Remarks	Check
Enforce password history	24 (Domain), 0	5		✓
Maximum password age	42 days	90 days		✓
Minimum password age	0 days	1 days		✓
Minimum password length	0 characters	8 characters		✓
Password must meet complexity requirements	Enabled	Enabled		✓

1.1.2 Account Lockout Policy

1. Run command "secpol.msc"
2. Expand "Account Polices" and Click on "Account Lockout Policy"

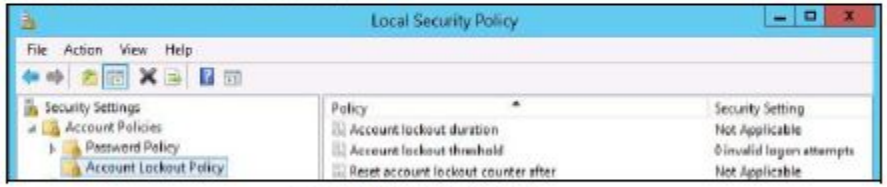


Figure 2 Account Lockout Policy

3. Setting these parameters :

System Value / Parameter	Default Setting	Recomended Setting	Remarks	Check
Account lockout duration	Not Applicable	30 minutes		✓
Account lockout threshold	0 attempts	5 attempts		✓
Reset account lockout counter after	Not Applicable	30 minutes		✓

1.2 Local Policies (secpol.msc)

1.2.1 Audit Policy

1. Run command "secpol.msc"
2. Expand "Local Polices" and Click on "Audit Policy"

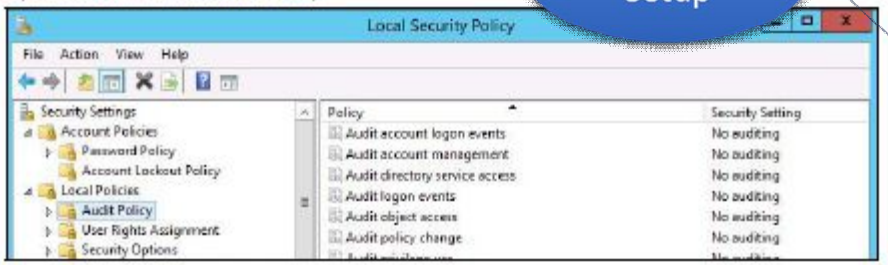


Figure 3 Audit Policy

3. Setting these parameters :

System Value / Parameter	Default Setting	Recomended Setting	Remarks	Check
Audit account logon events	Not Defined	Success, Failure		✓
Audit account management	Not Defined	Success, Failure		✓
Audit directory service access	Not Defined	Failure		✓
Audit logon events	Not Defined	Success, Failure		✓
Audit object access	Not Defined	Failure		✓
Audit policy change	Not Defined	Success, Failure		✓
Audit privilege use	Not Defined	Not Defined		✓
Audit process tracking	Not Defined	Not Defined		✓
Audit system events	Not Defined	Success, Failure		✓

1.2.2 Security Options

1. Run command "secpol.msc"
2. Expand "Local Polices" and Click on "Security Options"

Figure 4 Security Options

3. Setting these parameters :

System Value / Parameter	Default Setting	Recomended Setting	Remarks	Check
Accounts: Administrator account status	Enabled	Enabled		✓
Accounts: guest account status	Disabled	Disabled		✓
Accounts: Limit local account use of blank passwords to console logon only	Enabled	Enabled		✓
Devices: Restrict CD-ROM access to locally logged-on user only	Not Defined	Not Defined		✓
Interactive logon: Do not display last user name	Disabled	Enabled		✓
Interactive logon: Do not require CTRL+ALT+DEL	Disabled	Disabled		✓
Interactive logon : Message text for users attempting to log on	-	"This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of		✓

System Value / Parameter	Default Setting	Recomended Setting	Remarks	Check
		their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials"		
Interactive logon: Message title for users attempting to log on	-	Electronic Transactions Development Agency (Public Organization)		✓
Interactive logon: Prompt user to change password before expiration	5 days	5 days		✓
Microsoft network client: Digitally sign communications (always)	Disabled	Enabled		✓
Microsoft network client: Digitally sign communications (if server agrees)	Enabled	Enabled		✓
Microsoft network server: Digitally sign communications (always)	Disabled	Enabled		✓
Microsoft network server: Digitally sign communications (if client agrees)	Disabled	Enabled		✓
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControl	Not defined		✓
User Account Control : Admin Approval Mode for the Built-in Administrator account	Disabled	Disabled		✓
User Account Control : Behavior of the elevation prompt for standard users	Prompt for credentials	Prompt for credentials		✓

2. System Logs

2.1 Event Log (eventvwr.msc)

1. Run command "eventvwr.msc"
2. Expand "Windows Logs"

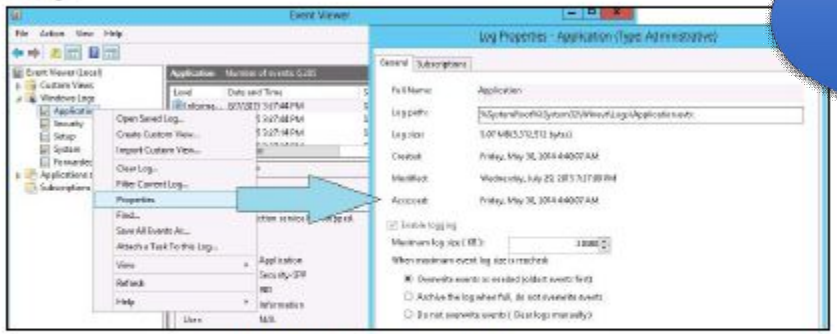
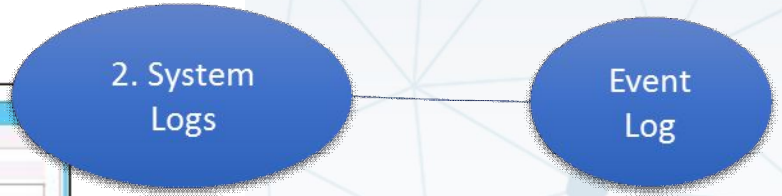


Figure 5 Application: Maximum Log Size

3. Right Click on Allication, Security, System and click properties then set maximum log size.

System Value / Parameter	Default Setting	Recomended Setting	Remarks	Check
Application: Maximum Log Size (KB)	20480	307200		✓
Security: Maximum Log Size (KB)	20480	307200		✓
System: Maximum Log Size (KB)	20480	307200		✓



3. Network and Sharing

3.1 Internet Communication

1. Run command "gpedit.msc"
2. Expand "Administrative Template -> System -> Internet Communication Management" and click on "Internet Communication settings"

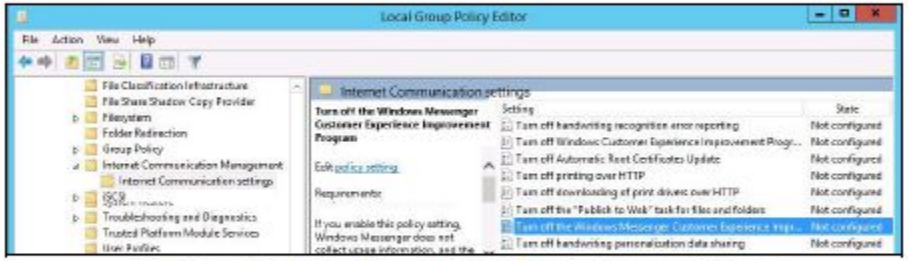
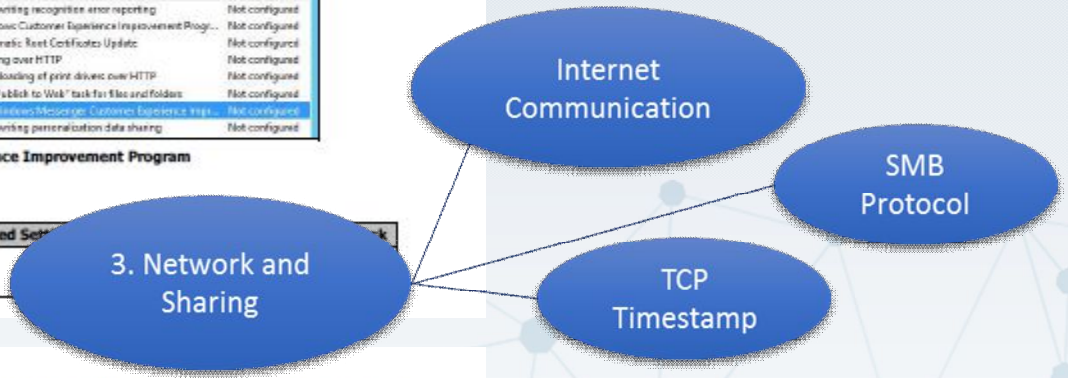


Figure 6 Turn off the Windows Messenger Customer Experience Improvement Program

3. Setting these parameters :

System Value / Parameter	Default Setting	Recomended Set	k
Turn off the Windows Messenger Customer Experience Improvement Program	Not configure	Enabled	



3.2 SMB protocol

The SMB protocol provides the basis for Microsoft file and print sharing and many other networking operations, such as remote Windows administration. To help prevent attacks that modify SMB packets in transit, the SMB protocol supports the digital signing of SMB packets. This policy setting determines whether SMB packet signing must be negotiated before further communication with an SMB client is permitted.

1. Run command "regedit.msc"
2. Setting these parameters :

System Value / Parameter	Default Setting	Recomended Setting	Remarks	Check
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature	0	1		✓
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature	0	1		✓

3.3 TCP timestamp

The remote host responded with a TCP timestamp. The TCP timestamp response can be used to approximate the remote host's uptime, potentially aiding in further attacks. Additionally, some operating systems can be fingerprinted based on the behavior of their TCP timestamps.

1. Open windows command with run as administrator
2. Run these commands :

System Value / Parameter	Default Setting	Recomended Setting	Remarks	Check
cmd : netsh int tcp set global timestamps=disable (Open CMD With admin option)	Enabled	Disabled		✓

3. Network and Sharing

3.4 Network Share (regedit.msc)

1. Run command "regedit.msc"
2. Setting these parameters :

System Value / Parameter	Default Setting	Recomended Setting	Remarks	Check
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer	Not Configure	0	Create new DWORD Value (if it is not already present) named AutoShareServer and set value 0 (disable network shares)	✓

Figure 7 AutoShareServer

Network Share

4. Additional Security Settings

4.1 Autoplay

1. Open Windows Control panel
2. Click AutoPlay and Uncheck "Use AutoPlay for all media and devices"

System Value / Parameter	Default Setting	Recomended Setting	Remarks	Check
Turn off Autoplay	Off	On		✓

Figure 8 AutoPlay

Autoplay

4. Additional Security Setting

4. Additional Security Setting

Windows Services

4.2 Windows Services

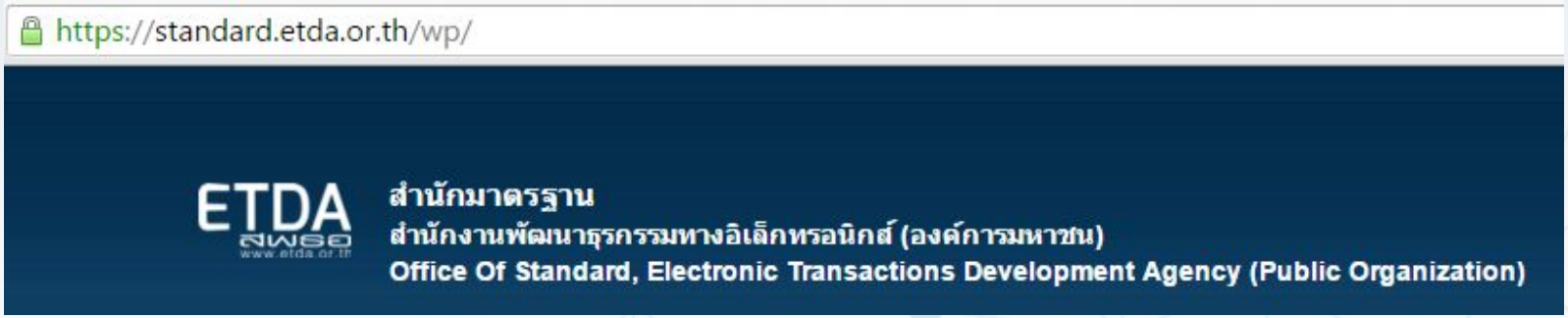
1. Run command "services.msc"
2. Setting these parameters :

System Value / Parameter	Default Setting	Recomended Setting	Remarks	Check
Dhcp client	Enabled	Disabled		✓
Print Spooler	Enabled	Disabled		✓
Application Layer Gateway Service	Disabled	Disabled		✓
Application Management	Disabled	Disabled		✓
Automatic Updates	Enabled	Enabled	Download and ask for install.	✓
Background Intelligent Transfer Service	Enabled	Enabled		✓
Computer Browser	Disabled	Disabled		✓
Cryptographic Services	Enabled	Enabled		✓
Distributed Transaction Coordinator	Enabled	Enabled		✓
DNS Client	Enabled	Enabled		✓
Net Logon Service	Enabled	Enabled		✓
Network Connections	Enabled	Enabled		✓
Protected Storage	Enabled	Enabled		✓
Remote Access Auto Connection Manager	Enabled	Enabled		✓
Remote Procedure Call	Enabled	Enabled		✓
Remote Registry Service	Enabled	Disabled		✓
Remote Desktop Service	Enabled	Enabled		✓
Security Accounts Manager	Enabled	Enabled		✓
Server	Enabled	Enabled		✓
Shell Hardware Detection	Enabled	Enabled		✓

System Value / Parameter	Default Setting	Recomended Setting	Remarks	Check
Task Scheduler	Enabled	Enabled		✓
Telephony	Enabled	Disabled		✓
Windows Management Instrumentation	Enabled	Enabled		✓
Windows Time	Enabled	Enabled		✓

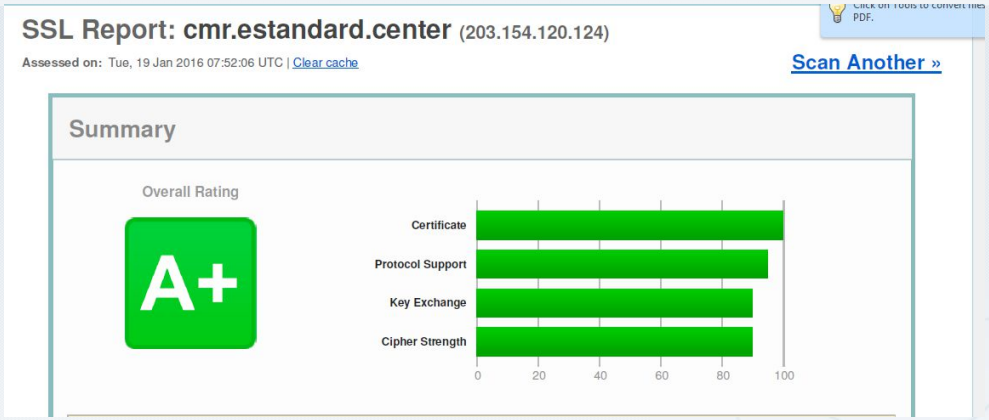
SSL Certificate

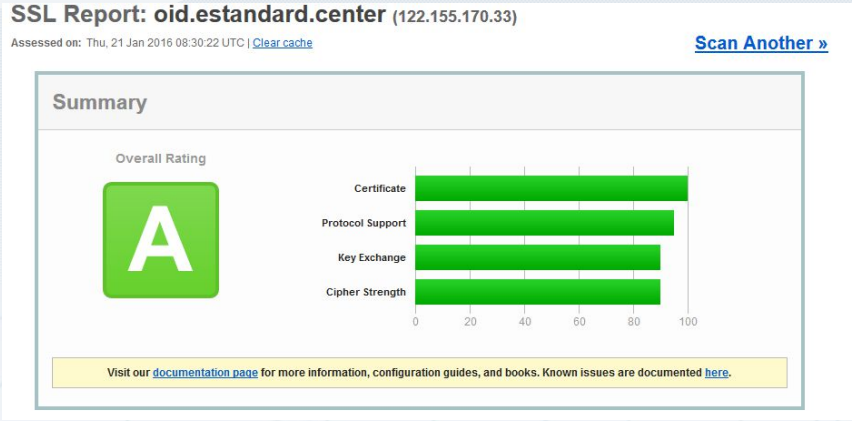
- กระบวนการยืนยันตัวตนเว็บไซต์โดยใช้ใบรับรองอิเล็กทรอนิกส์สำหรับเครื่องบริการเว็บ เป็นวิธีการหนึ่งที่ทำให้ผู้ใช้บริการเว็บไซต์มั่นใจได้ว่าเว็บไซต์ที่กำลังใช้บริการนั้นมีตัวตนอยู่จริงและได้รับการรับรองจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (CA) ที่น่าเชื่อถือ



- โพรโทคอล SSL/TLS : เข้ารหัสที่ช่องทางการรับส่งข้อมูลกันระหว่าง Wed Server และ Web Browser และสามารถตรวจสอบได้ว่าข้อมูลที่รับส่งนั้น ถูกแก้ไขหรือไม่ และมีการใช้ Cipher suite สำหรับกำหนดระดับความมั่นคงปลอดภัยของการติดต่อสื่อสารที่เกิดขึ้น

SSL Checker



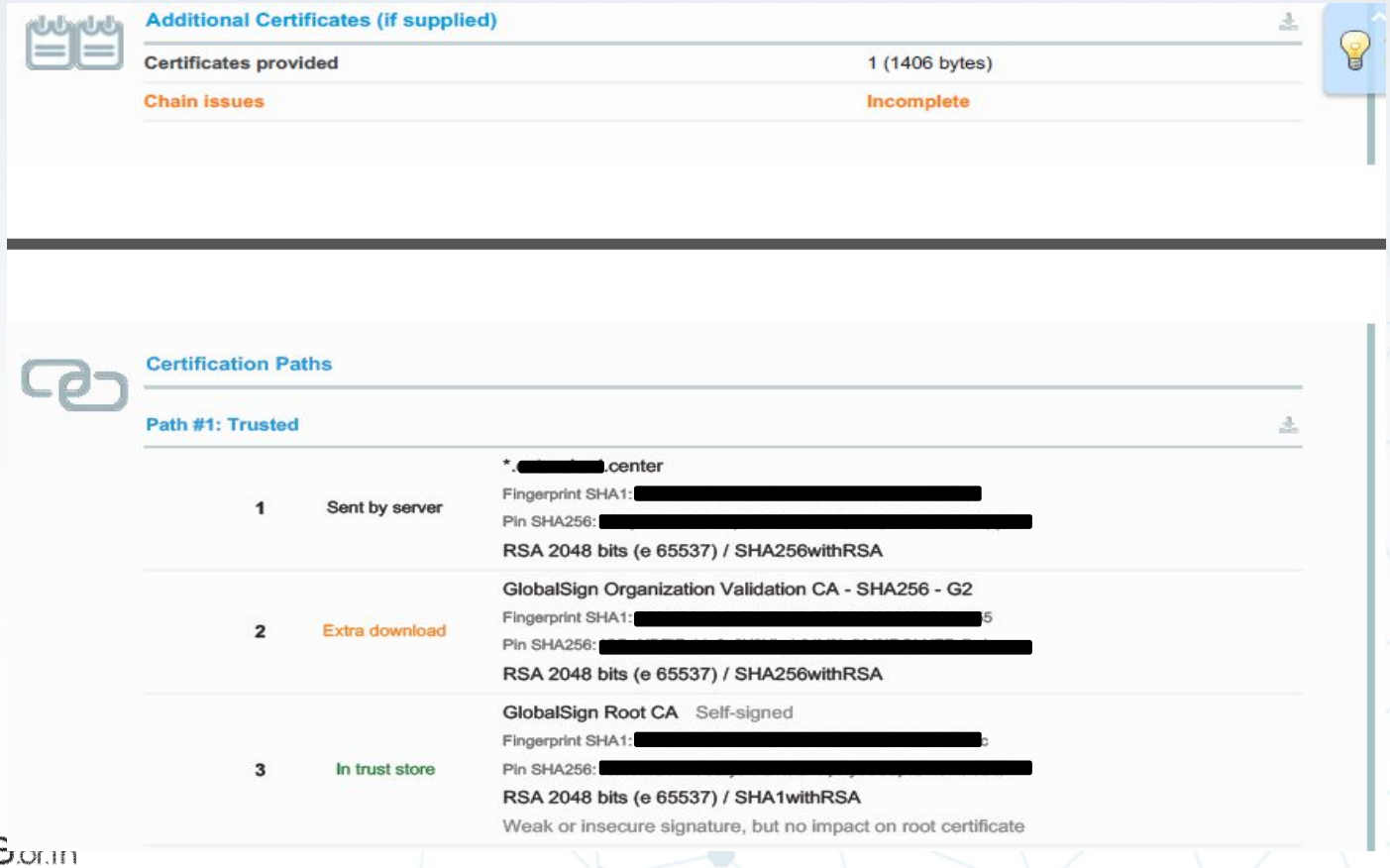


- อย่างน้อยควรได้ A-
- เว็บไซต์ที่เปิดให้ตรวจสอบ SSL Server Test
  - GlobalSign SSL Server Test by QUALYS SSL LABS (https://globalsign.ssllabs.com/)
  - SSL Server Test by QUALYS SSL LABS (https://www.ssllabs.com/ssltest/)
  - DigitCert SSL Installation Diagnostics Tool (https://www.digicert.com/help/)
  - Symantec CryptoReport (https://cryptoreport.websecurity.symantec.com/checker/views/certCheck.jsp)

ปัญหาส่วนใหญ่ที่พบ ที่ทำให้ไม่ได้ A- (เป็นอย่างน้อย)

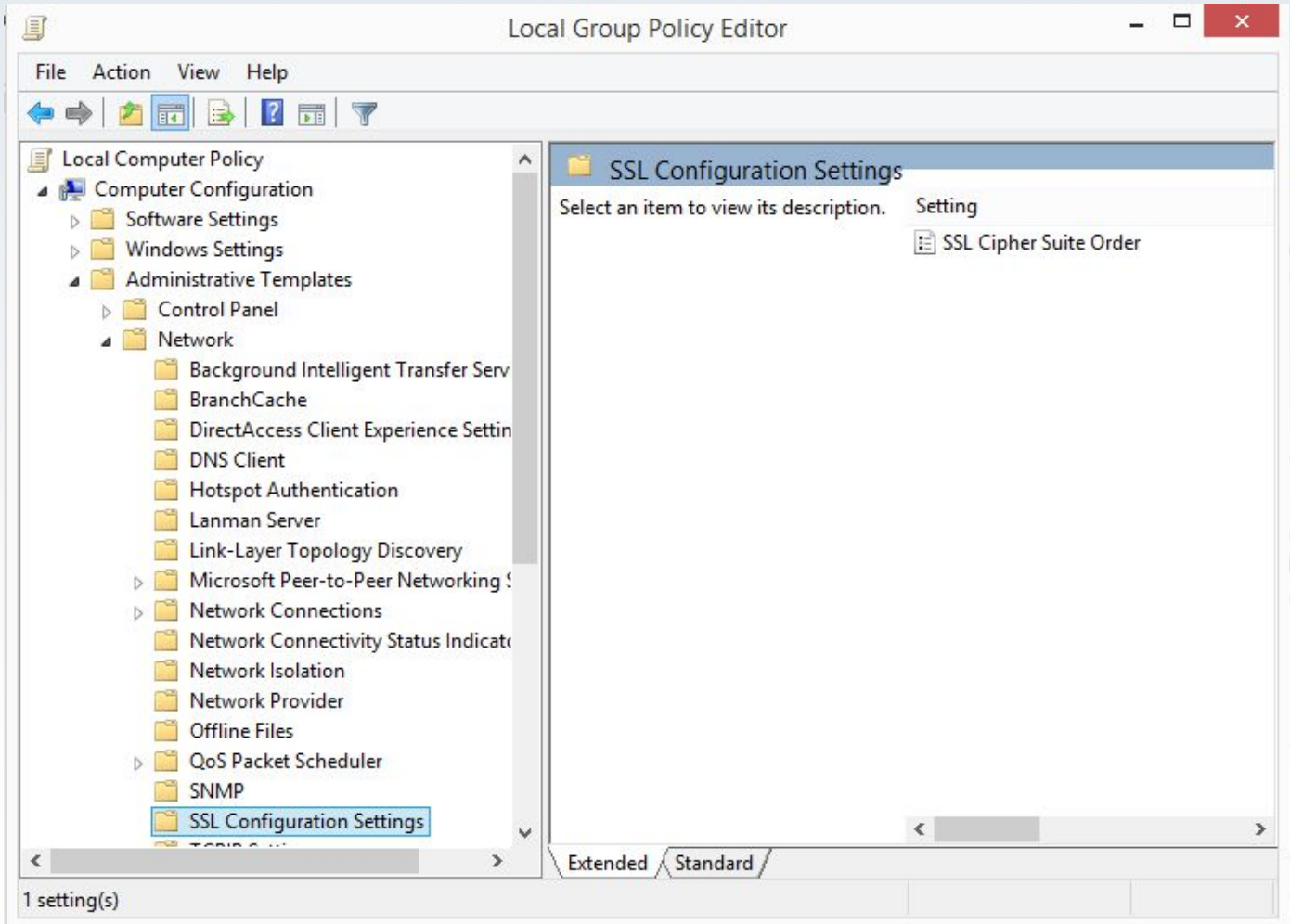
1. Certificate Chain incomplete

   – **<u>การแก้ไข</u>**. ดาวน์โหลด Intermediate Certificate ของหน่วยงาน Root CA ของเรา และติดตั้ง Intermediate Certificate



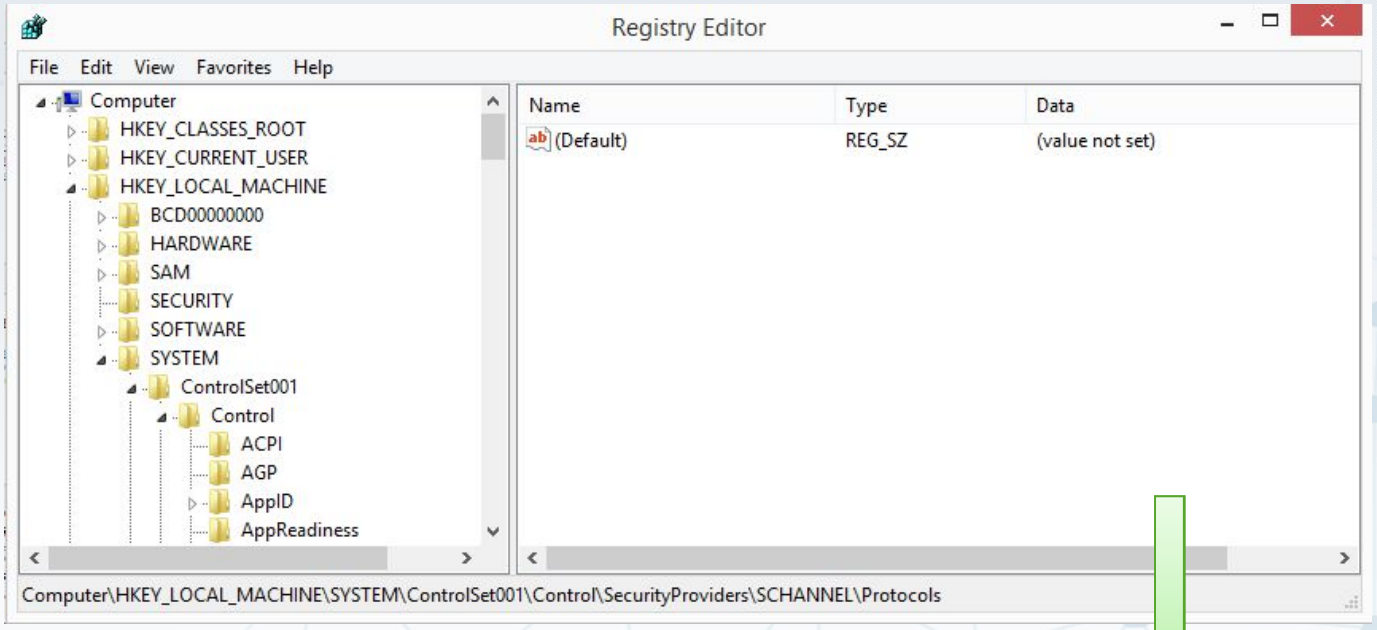
2. SSL Cipher Suite ยังไม่อัพเดต และยังใช้ Cipher ที่ Weak แล้วเช่น RC4

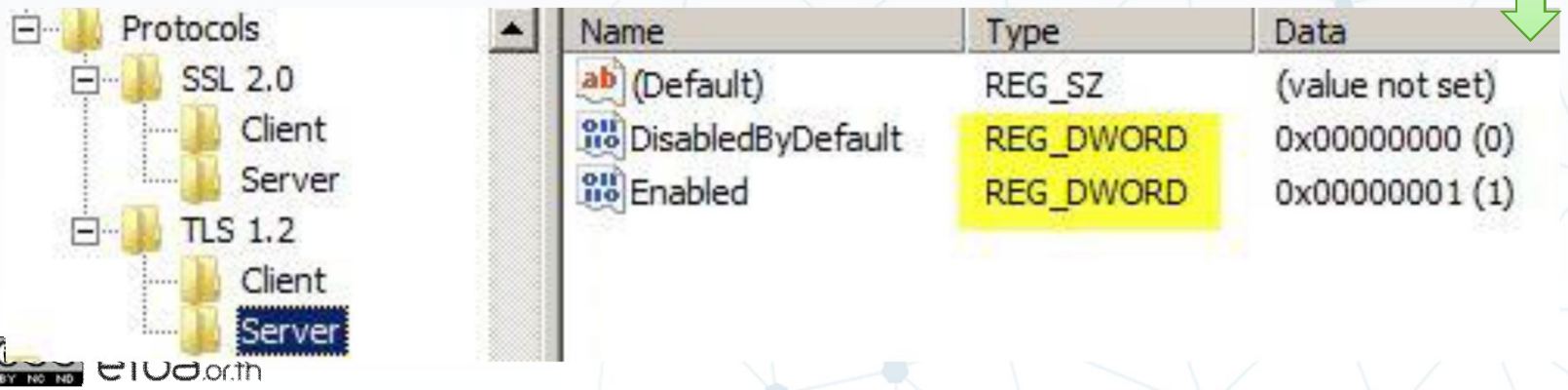
- **<u>วิธีการแก้ไข</u>** อัพเดตที่ gpedit.msc ของ Windows ในหัวข้อ SSL Configuration Settings



3. Server ยัง Support Protocol เก่า เช่น SSL2.0 และยังไม่อัพเดตให้รองรับ Protocol ใหม่ เช่น TLS1.2

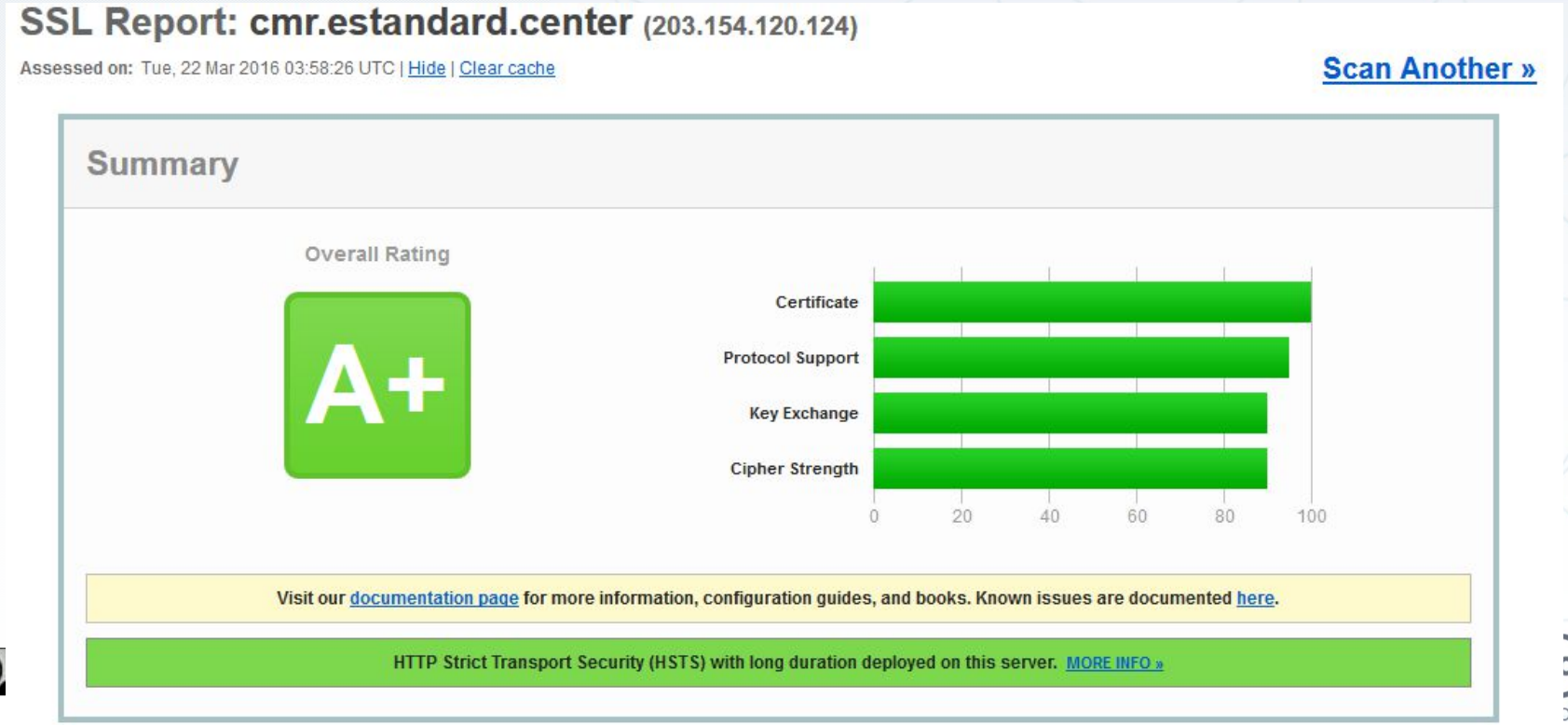
- **<u>วิธีการแก้ไข</u>** อัพเดตที่ regedit ของ Windows และเข้าไปอัพเดตค่า Registry ของ Protocol ที่ต้องการ





How To Get A+

- ปิด port ทั้งหมดที่นอกเหนือจาก port 443 จะทำให้มีการใช้งาน HTTP Strict Transport Security (HSTS)
- HSTS เป็นการให้เครื่องบริการเว็บ "บังคับ" ให้เบราว์เซอร์เชื่อมต่อกับเครื่องเว็บแบบเข้ารหัส (HTTPS) เสมอ



การตั้งค่าระบบบริหารจัดการเว็บไซต์ (CMS)

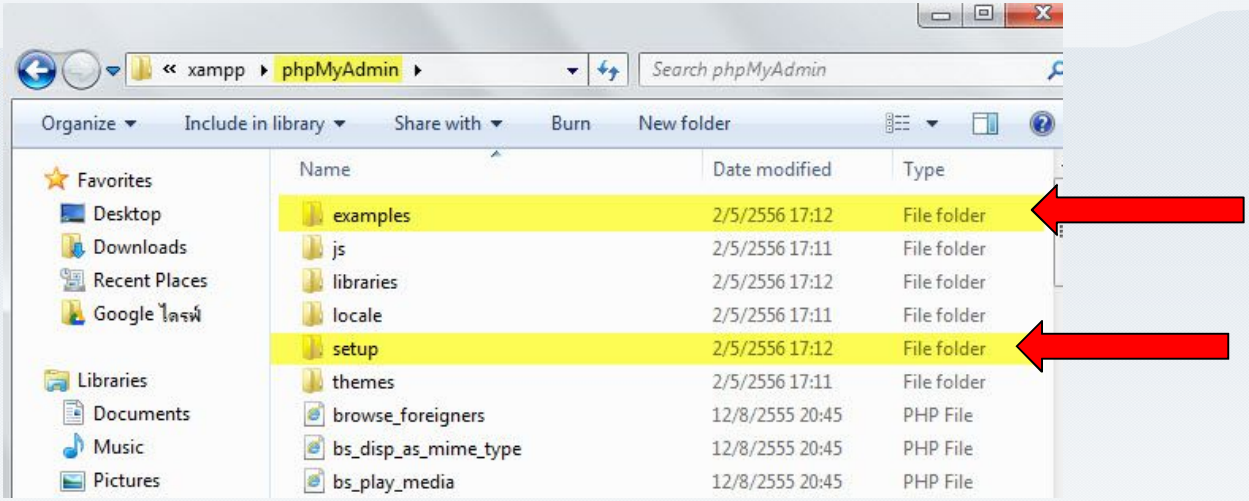
- ต้องมีการกำหนดสิทธิการใช้งาน (Permission) และการควบคุมการเข้าถึง (Access Control) ไฟล์ต่าง ๆ ให้เหมาะสมกับบทบาทและหน้าที่ของผู้ใช้บริการ (Access Control List)
- ตรวจสอบว่ามีไฟล์หรือโปรแกรมเสริม (Plug-in program) ที่ไม่จำเป็นหรือไม่ได้ใช้งานปรากฏอยู่หรือไม่ ถ้าตรวจพบ ต้องลบ หรือถอนการติดตั้งโปรแกรมนั้นทันที
- หมั่นตรวจสอบการอัพเดตเวอร์ชั่นของ CMS อยู่เสมอ และให้อัพเดตเป็นเวอร์ชั่นปัจจุบัน โดยให้ดาวน์โหลดจากเว็บไซต์หลักของ CMS นั้น ๆเท่านั้น
- ลบบัญชีผู้ใช้ที่มากับการติดตั้ง CMS โดยเปลี่ยนชื่อผู้ใช้ หรือรหัสผ่านให้มีความมั่นคงปลอดภัยแทน
- เปลี่ยน table prefix ของฐานข้อมูลที่มาในระหย่างการติดตั้ง CMS เช่น ใน wordpress table prefix ที่เป็นค่า default จะขึ้นต้นด้วย wp_xxx

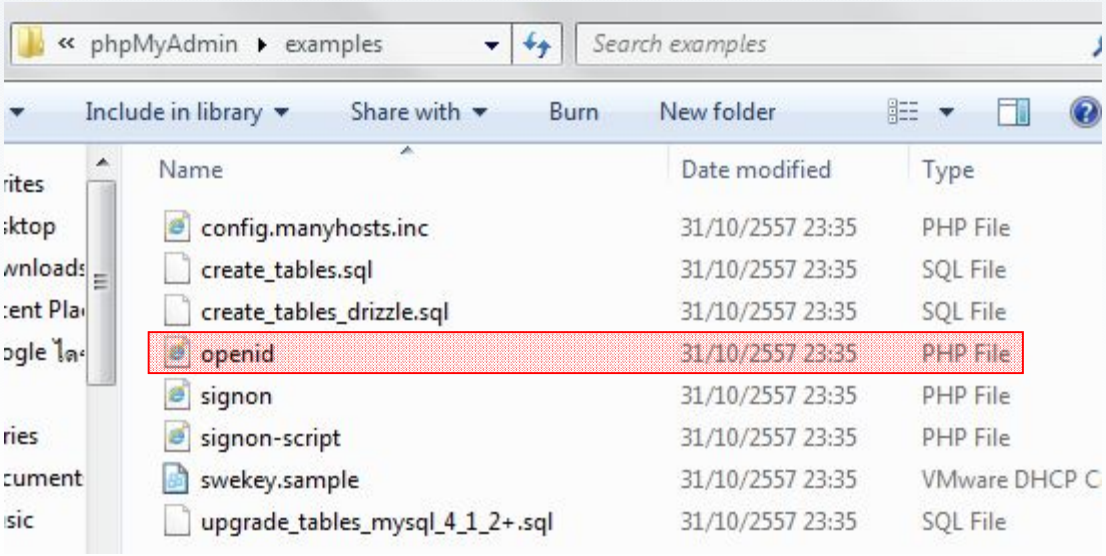
การตรวจสอบและลบค่าเริ่มต้นของข้อมูลที่มาพร้อมกับการติดตั้ง หรือข้อมูลที่ไม่ได้ใช้งานในโปรแกรมประยุกต์ต่างๆ

ปัญหาที่พบ

- การใช้ค่าเริ่มต้นที่มาพร้อมกับการติดตั้งโปรแกรมประยุกต์ เช่น บัญชีผู้ใช้ที่มาพร้อมฐานข้อมูล พวก Guest, Admin Account ผู้ประสงค์ร้ายสามารถคาดเดาได้
- การไม่ได้ลบไฟล์หรือโฟลเดอร์ที่มาพร้อมกับการติดตั้งโปรแกรมประยุกต์ เช่น โฟลเดอร์ examples, โฟลเดอร์ Setup สามารถเป็นช่องทางหนึ่งให้ผู้ประสงค์ร้ายสามารถเข้าถึงข้อมูลภายในได้
- มีข้อมูลที่ไม่ได้ใช้งานอยู่ในโปรแกรมประยุกต์ต่างๆ เช่น มีบัญชีผู้ใช้ที่ไม่ได้ใช้งาน ค้างอยู่ในระบบฐานข้อมูล หรือมีปลั๊กอินที่ไม่ได้ใช้งาน ค้างอยู่ใน CMS เป็นต้น

ตัวอย่างเช่น ตรวจสอบที่โฟล์เดอร์ phpMyAdmin ยังมี โฟลเดอร์ setup, โฟลเดอร์ file example เป็นต้น



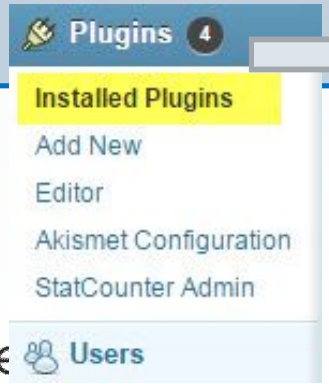


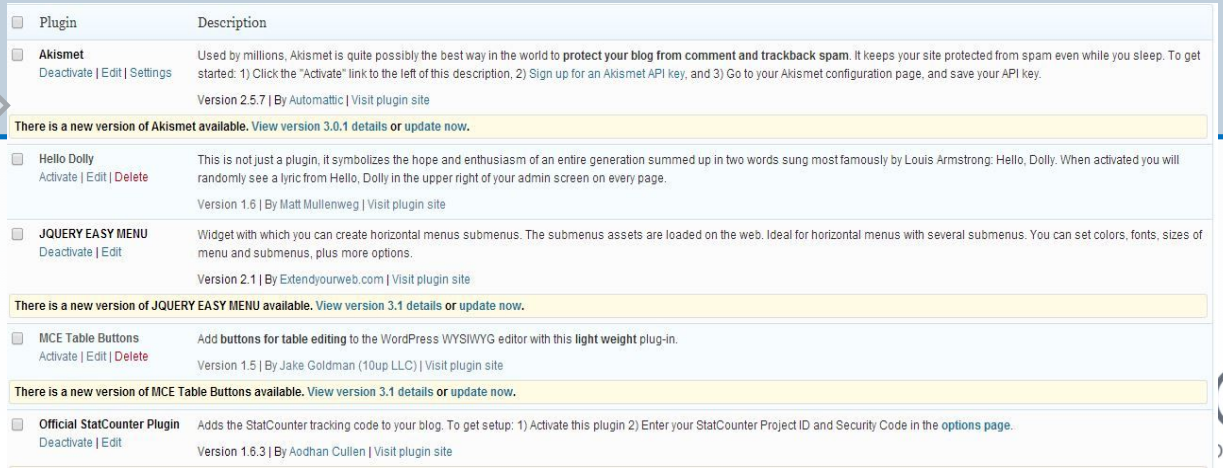
การตรวจสอบและลบค่าเริ่มต้นของข้อมูลที่มาพร้อมกับการติดตั้ง หรือข้อมูลที่ไม่ได้ใช้งานในโปรแกรมประยุกต์ต่างๆ (ต่อ)

ตัวอย่างวิธีการป้องกัน

- จัดให้มีการทบทวนบัญชีผู้ใช้ภายในโปรแกรมประยุกต์ตามระยะเวลาที่กำหนด และลบบัญชีผู้ใช้ที่ไม่ได้มีการใช้งาน
- ปิดบัญชีผู้ใช้ที่มาพร้อมกับการติดตั้งโปรแกรมประยุกต์หรือเปลี่ยนรหัสผ่านของบัญชีผู้ใช้ดังกล่าว ให้เป็นรหัสผ่านที่มีความมั่นคงปลอดภัย เช่น บัญชีผู้ใช้ในฐานข้อมูล, บัญชีผู้ใช้ในฐานข้อมูล CMS, บัญชีผู้ใช้ใน Web Server Software
- ตรวจสอบและลบแฟ้มชั่วคราว (temporary file) ที่ถูกสร้างขึ้นระหว่างการติดตั้งโปรแกรมประยุกต์ เช่น Web Server Software, ฐานข้อมูล หรือ CMS

หัวข้อตาม Checklist ที่เกี่ยวข้อง : Checklist 2.4, Checklist 2.5, Checklist 3.4, Checklist 3.5, Checklist 4.5, Checklist 4.7, Checklist 11.3





การตั้งค่าฐานข้อมูล (Database System)

- ตั้งค่าฐานข้อมูล อนุญาตให้เฉพาะโปรแกรมประยุกต์ (Application) และเครื่องบริการเว็บที่เกี่ยวข้องเข้าถึงได้เท่านั้น
- ควบคุมการเข้าถึงระบบฐานข้อมูลด้วยระบบรักษาความมั่นคงปลอดภัย เช่น ป้องกันการบุกรุกด้วยไฟล์วอลล์ (Filewall)
- ตรวจสอบและปิดบริการ (Services) ที่ไม่จำเป็นหรือไม่ได้ใช้งาน
- จัดให้มีการทบทวนบัญชีผู้ใช้ภายในฐานข้อมูลตามระยะเวลาที่กำหนด และลบบัญชีผู้ใช้ที่ไม่ได้มีการใช้งานออกจากระบบฐานข้อมูล
- ปิดบัญชีผู้ใช้ที่มาพร้อมกับการติดตั้งฐานข้อมูล หรือเปลี่ยนรหัสผ่านให้มีความมั่นคงปลอดภัย
- กำหนดค่าติดตั้งระบบฐานข้อมูลไม่อนุญาตให้ใช้งานรหัสผ่านที่มีค่าว่าง (Null password)
- ตรวจสอบลบไฟล์ชั่วคราว (Temporary file) ที่ถูกสร้างขึ้นระหว่างการติดตั้งระบบฐานข้อมูล
- ปรับปรุงเวอร์ชั่น หรืออัพเดต patch ของโปรแกรมฐานข้อมูล จากบริษัทผู้ผลิตซอฟต์แวร์ ให้เป็นเวอร์ชั่นล่าสุดอยู่เสมอ
- กำหนดสิทธิการใช้งาน (Permission) และการควบคุมการเข้าถึง (Access Control) ให้เหมาะสมกับบทบาทและหน้าที่ของผู้ใช้
- รหัสผ่านที่เก็บในฐานข้อมูล ต้องมีการเข้ารหัส หรือ Hashing

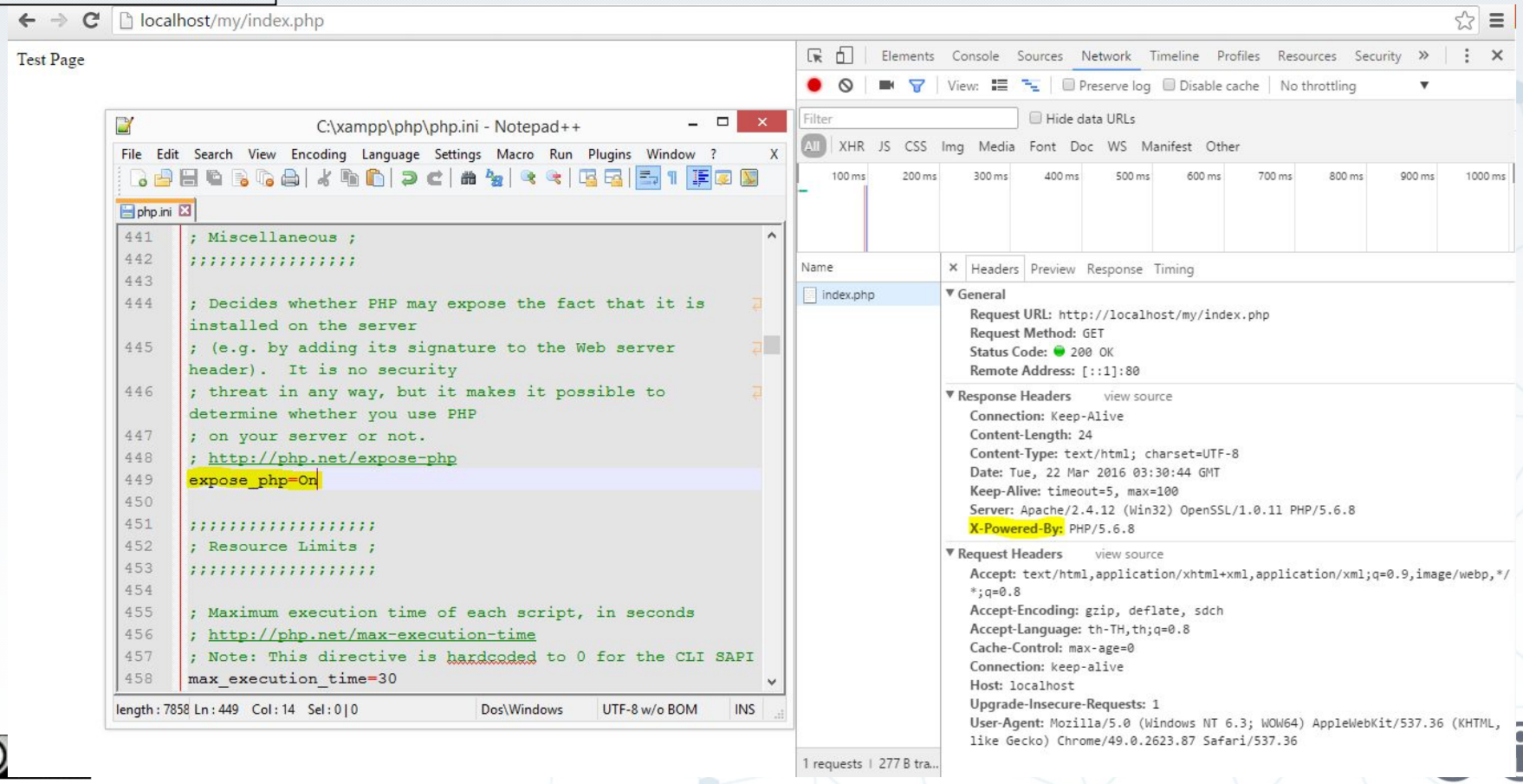
การตั้งค่า Server-side Script Engine

- ควบคุมการเข้าถึงไฟล์หรือสารบบต่าง ๆ ให้เหมาะสมกับบทบาทของผู้ใช้
- ปรับปรุงเวอร์ชั่น หรือ อัพเดต patch ของ Server-side Script Engine จากบริษัทผู้ผลิตซอฟต์แวร์ให้เป็นเวอร์ชั่นล่าสุดอยู่เสมอ
- กำหนดค่าติดตั้ง ไม่ให้แสดงข้อมูลเวอร์ชั่นที่เครื่องบริการเว็บ (HTTP Header)
- กำหนดค่าติดตั้ง ไม่ให้มีการแสดงรายละเอียดของข้อความ หรือแสดงข้อผิดพลาด (Error Message) ที่เป็นประโยชน์กับผู้ประสงค์ร้าย โดยให้แสดงข้อมูลเท่าที่จำเป็น

กำหนดค่าติดตั้งไม่ให้ Server-side Script Engine แสดงข้อมูลเวอร์ชั่นของ Server-side Script Engine ที่เครื่องบริการเว็บใช้งาน ใน HTTP Header

ฟังก์ชั่น expose_php ในไฟล์ php.ini หากฟังก์ชั่น expose_php เปิดอยู่ ทำให้ HTTP Header ในส่วน Response Header แสดงค่า X-Power By ซึ่งจะแสดงเวอร์ชั่นของ php ที่ใช้ โดยให้เปลี่ยนค่าตรง expose_php=On เป็น Off

Expose_php=On



Expose_php=Off

localhost/my/index.php

Test Page

C:\xampp\php\php.ini - Notepad++

File Edit Search View Encoding Language Settings Macro Run Plugins Window ? X

php.ini

```
441 ; Miscellaneous ;
442 ;;;;;;;;;;;;;;;;;
443
444 ; Decides whether PHP may expose the fact that it is
    installed on the server
445 ; (e.g. by adding its signature to the Web server
    header).  It is no security
446 ; threat in any way, but it makes it possible to
    determine whether you use PHP
447 ; on your server or not.
448 ; http://php.net/expose-php
449 expose_php=Off
450
451 ;;;;;;;;;;;;;;;;;;;
452 ; Resource Limits ;
453 ;;;;;;;;;;;;;;;;;;;
454
455 ; Maximum execution time of each script, in seconds
456 ; http://php.net/max-execution-time
457 ; Note: This directive is hardcoded to 0 for the CLI SAPI
458 max_execution_time=30
```

length : 7859 Ln : 449 Col : 15 Sel : 0 | 0 Dos\Windows UTF-8 w/o BOM INS

Elements Console Sources Network Timeline Profiles

Preserve log Disable cache No throttling

Filter Hide data URLs

All XHR JS CSS Img Media Font Doc WS Manifest Other

200 ms 400 ms 600 ms 800 ms 1000 ms

Name

index.php

Headers Preview Response Timing

General

Request URL: http://localhost/my/index.php
Request Method: GET
Status Code: 200 OK
Remote Address: [::1]:80

Response Headers view source

Connection: Keep-Alive
Content-Length: 24
Content-Type: text/html; charset=UTF-8
Date: Tue, 22 Mar 2016 03:32:43 GMT
Keep-Alive: timeout=5, max=100
Server: Apache/2.4.12 (Win32) OpenSSL/1.0.11

Request Headers view source

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: th-TH,th;q=0.8
Cache-Control: max-age=0
Connection: keep-alive
Host: localhost
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.87 Safari/537.36

1 requests | 242 B tra...

etda.or.th

การกำหนดและรักษารหัสผ่าน

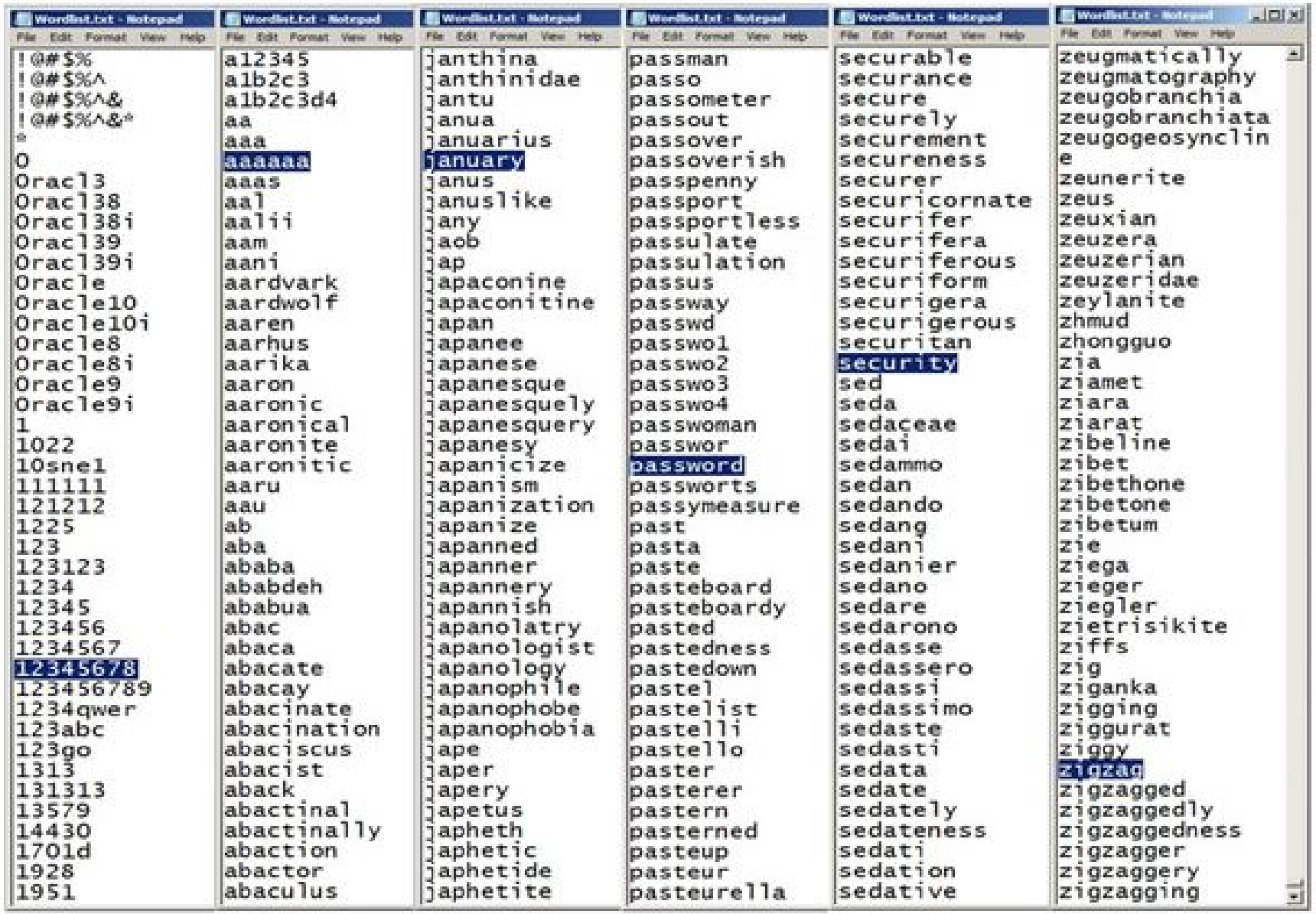
- ตั้งค่ารหัสผ่านให้มีความมั่นคงปลอดภัย (Strong password) โดยรหัสผ่านควรประกอบด้วยตัวอักษรทั้งตัวเล็ก ตัวใหญ่ ตัวเลขและสัญลักษณ์พิเศษ และมีความยาวไม่น้อยกว่า 8 หลัก
- กำหนดให้มีการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ
- ไม่เก็บรหัสผ่านที่มีมีการเข้ารหัสลับบนเครื่องบริการเว็บ
  - ถ้าเข้ารหัสควรใช้ Algorithm อย่างน้อย AES หรือ Triple DES
  - ถ้าใช้ Hash ควรใช้ Algorithm อย่างน้อย SHA256

การกำหนดและรักษารหัสผ่าน

ปัญหาที่พบ

- การตั้งรหัสผ่านที่ไม่มีความมั่นคงปลอดภัย จะเป็นการเปิดโอกาสให้ผู้ประสงค์ร้ายโจมตีเพื่อคาดเดารหัสผ่านได้ง่าย ซึ่งมี 2 วิธี
- 1. Dictionary Attack = สุ่มเดาข้อมูลหรือรหัสผ่านจากคำศัพท์ที่อยู่ใน Dictionary และคำศัพท์ที่ผู้ประสงค์ร้ายนำไปใช้ เรียกว่า “Word list”
- 2. Brute Force Attack = คาดเดารหัสผ่านตามทุกความเป็นไปได้ของตัวอักษรในแต่ละหลัก ผู้ประสงค์ร้ายอาจเป็นผู้ลองกระทำเองหรืออาจจะใช้โปรแกรมอัตโนมัติทำงาน

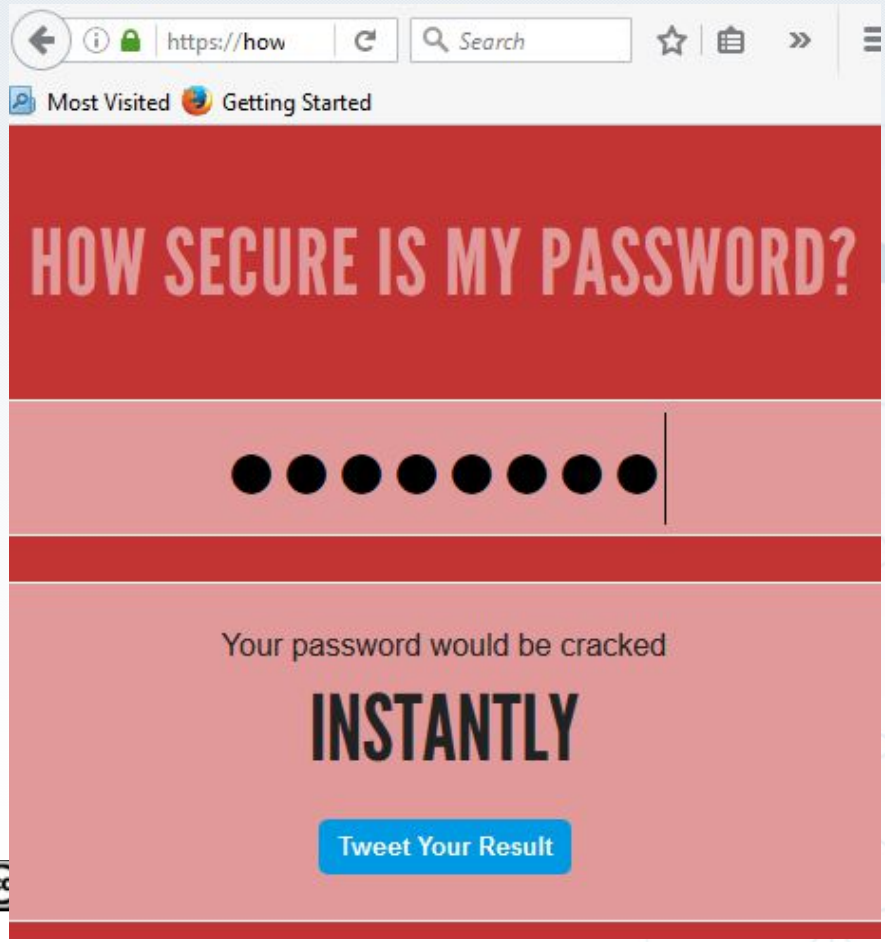
Dictionary Attack (ง่าย) for guessable simple password !!!



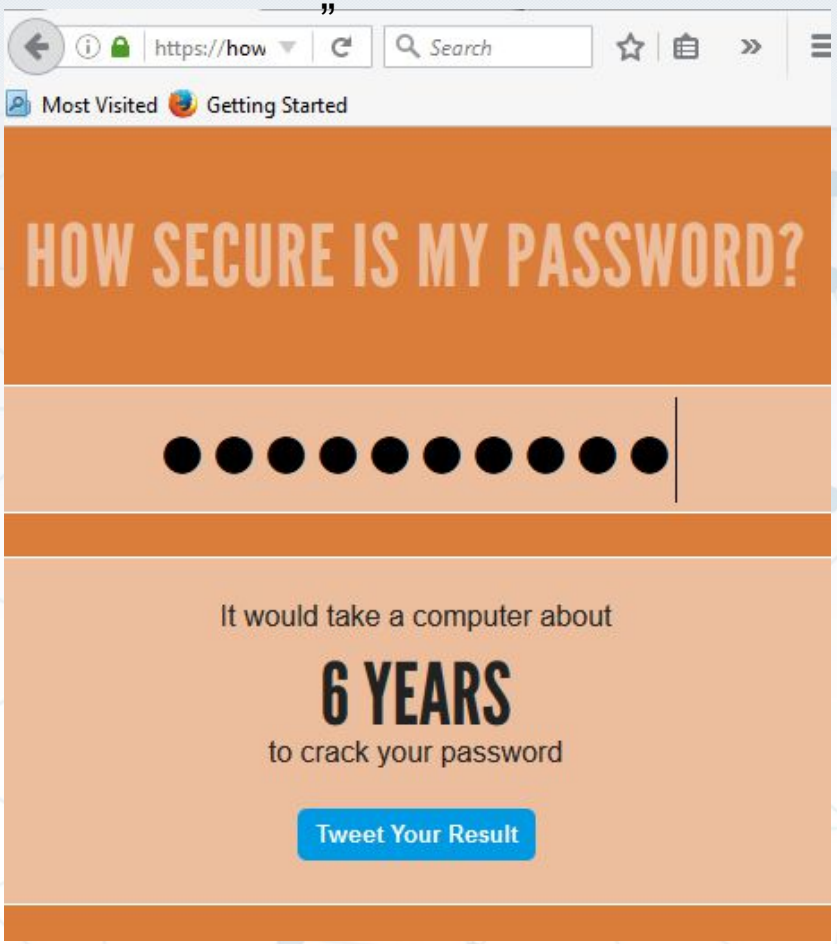
Try your Password !

- https://howsecureismypassword.net/

"password"



"P@ssw0rd1!"



การกำหนดและรักษารหัสผ่าน (ต่อ)

ป้องกันได้โดย

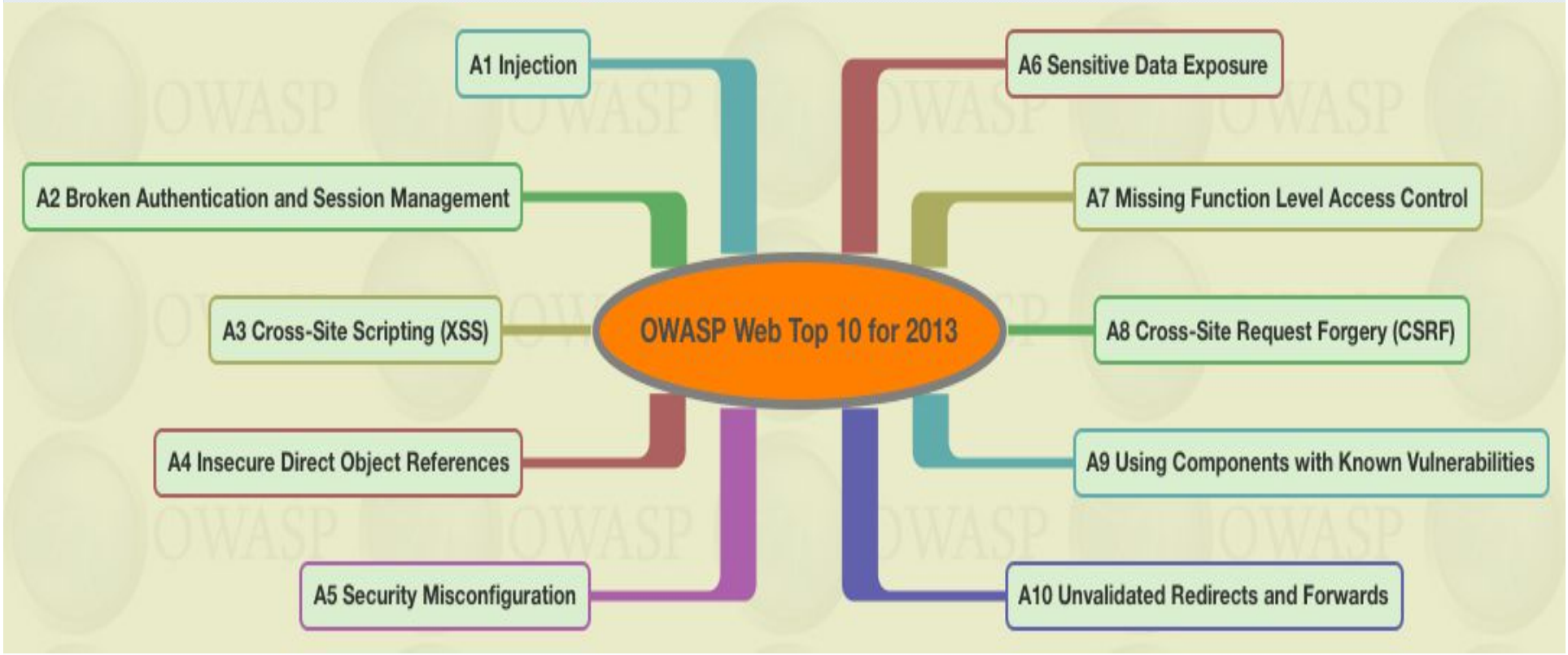
(1)ตั้งค่ารหัสผ่านให้มีความมั่นคงปลอดภัย (Strong password) โดยรหัสผ่านควรประกอบด้วยตัวอักษรทั้งตัวเล็กและตัวใหญ่ผสมกัน มีตัวเลขและสัญลักษณ์พิเศษอย่างน้อย 1 หลัก และต้องมีความยาวทั้งหมดไม่น้อยกว่า 8 หลัก

(2)กำหนดให้มีการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอจะช่วยลดโอกาสจากการถูกคาดเดารหัสผ่าน

(3)การเก็บรหัสผ่านควรอยู่ในรูปที่มีการเข้ารหัสลับตามที่มาตรฐานด้านความมั่นคงปลอดภัยกำหนด เช่น เช่น md5 หรือ sha-256

<u>หัวข้อตาม Checklist ที่เกี่ยวข้อง</u> : Checklist 6 (Checklist 6.1, Checklist 6.2, Checklist 6.3), Checklist 4.10

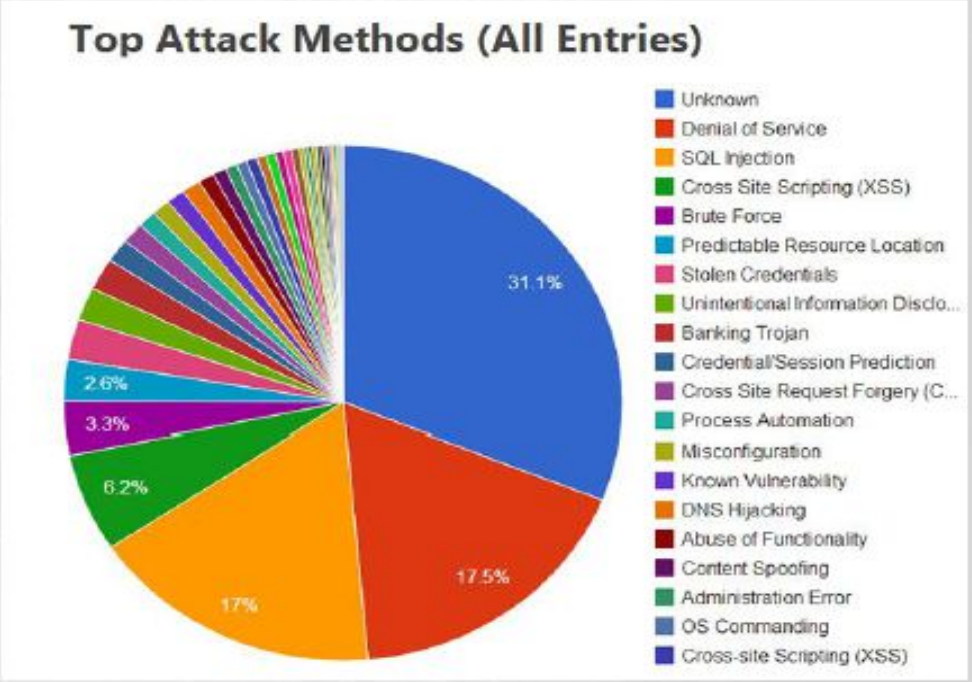
สถิติ OWASP TOP 10 2013



Refer : *https://www.owasp.org/index.php/Top_10_2013-Top_10*

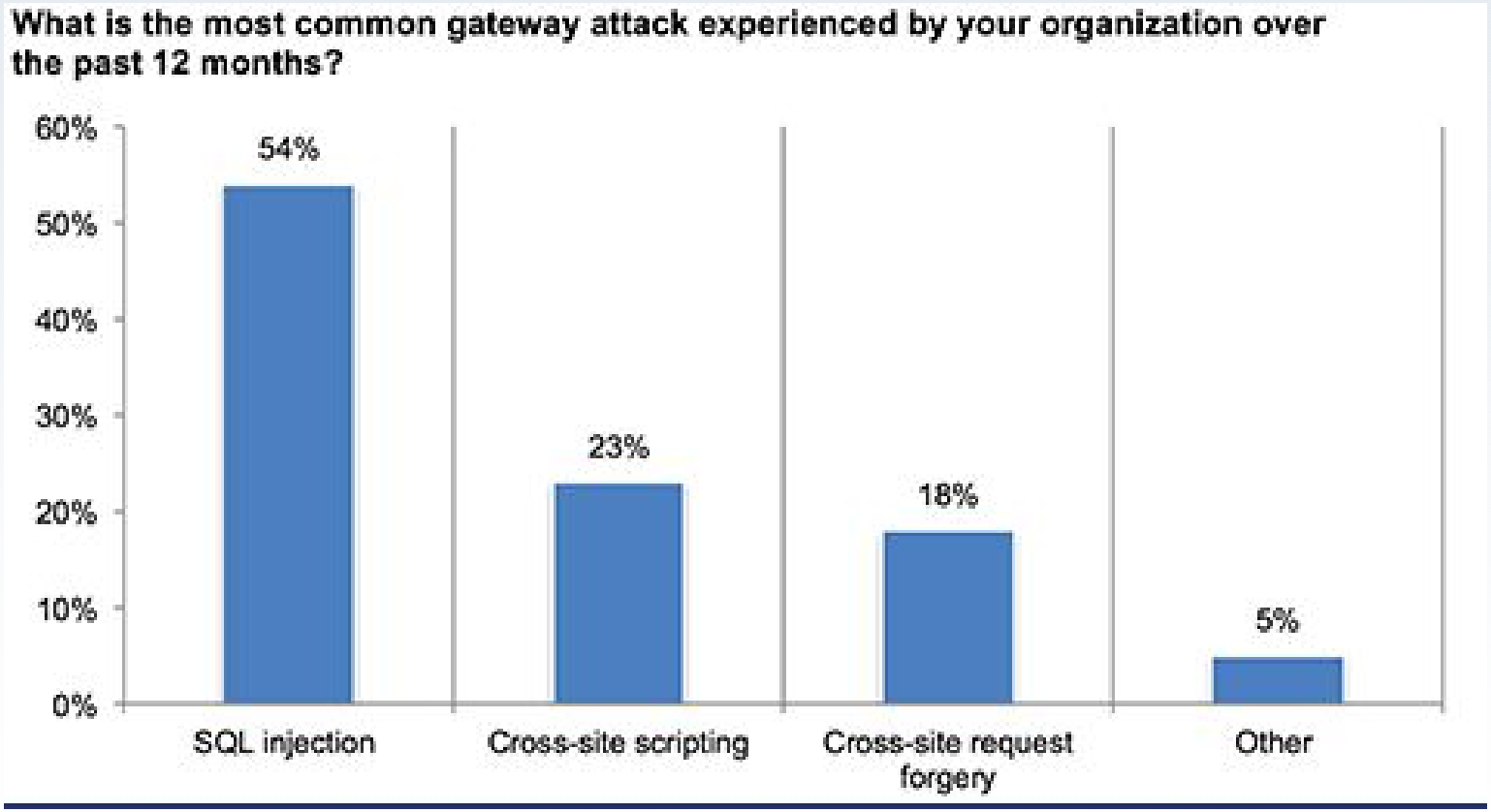
สถิติการแฮกเว็บไซต์ด้วยเทคนิคต่างๆจาก Trustwave

ในปี 2556 พบรูปแบบการโจมตีเว็บไซต์ด้วยเทคนิค DoS (17.5%) SQL Injection (17%) และ Cross-site scripting (6.2%) ถูกแจ้งใน 3 อันดับแรก ตามลำดับ จากรายงานของ Trustwave



Refer :https://www.thaicert.or.th/downloads/presentations/20150507_Seminar_Dataone_.pdf

สถิติภัยคุกคามที่เกิดขึ้นมากที่สุดในปี 2015 จากสถาบันวิจัยด้านความปลอดภัยข้อมูล สหรัฐอเมริกา



Refer : http://www.net-security.org/secworld.php?id=19220

etda.or.th

การพัฒนาโปรแกรมประยุกต์บนเครื่องบริการเว็บอย่างมั่นคงปลอดภัย

- SQL Injection
- CSRF
- Session Hijacking
- Sensitive Data Exposure
- Cross-site Scripting (XSS)

OWASP
The Open Web Application Security Project

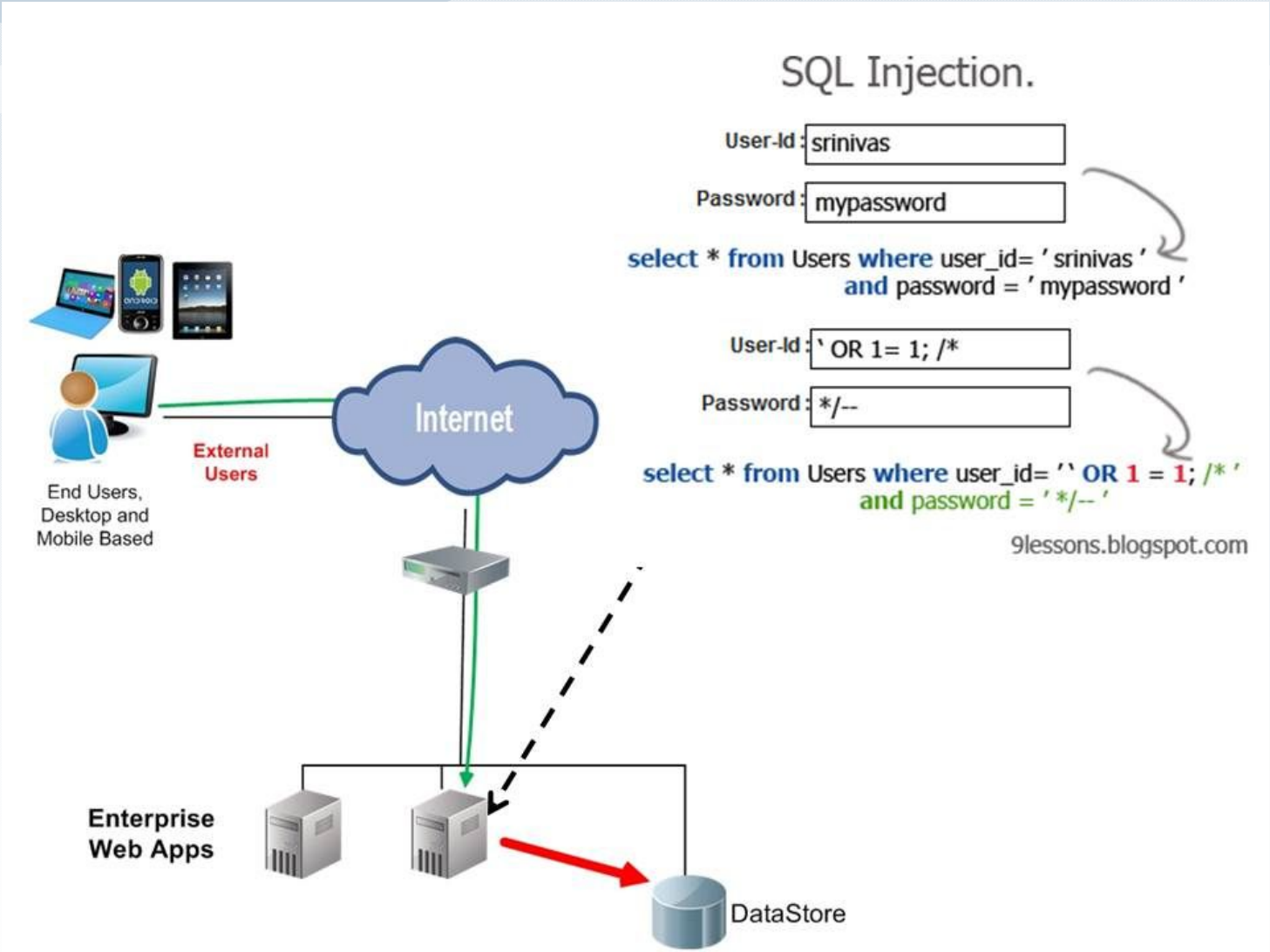
T10 OWASP Top 10 Application Security Risks – 2013

A1 – Injection	•Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.
A2 – Broken Authentication and Session Management	•Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities.
A3 – Cross-Site Scripting (XSS)	•XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A4 – Insecure Direct Object References	•A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
A5 – Security Misconfiguration	•Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date.
A6 – Sensitive Data Exposure	•Many web applications do not properly protect sensitive data, such as credit cards, tax ids, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
A7 – Missing Function Level Access Control	•Virtually all web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access unauthorized functionality.
A8 - Cross-Site Request Forgery (CSRF)	•A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.
A9 - Using Components with Known Vulnerabilities	•Vulnerable components, such as libraries, frameworks, and other software modules almost always run with full privilege. So, if exploited, they can cause serious data loss or server takeover. Applications using these vulnerable components may undermine their defenses and enable a range of possible attacks and impacts.
A10 – Unvalidated Redirects and Forwards	•Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

การป้องกันการโจมตีจาก SQL Injection

- จัดทำ Prepared statement หรือ Stored procedure เป็นวิธีการแยกคำสั่งในการประมวลผลและค่าที่จะนำไปประมวลผลออกจากกัน
- จัดทำ Input validation เป็นวิธีการที่ใช้ในการตรวจสอบข้อมูลก่อนส่งมาประมวลผลจริง เช่น ไม่อนุญาตให้ใส่เครื่องหมาย < > ‘ “ = \ * เป็นต้น
  - Whitelist validation เช่นอนุญาตให้ upload ไฟล์นามสกุล .txt .pdf .docx .xlsx เท่านั้น
  - Blacklist validation เช่น ไม่อนุญาตให้ใส่เครื่องหมาย < > หรือ <script>
- ทำ Encode หรือ Sanitization ก่อนนำค่ามาแปลงก่อนที่จะส่งไปประมวลผล ซึ่งข้อมูลที่ผ่านการแปลงจะอยู่ในรูปแบบที่ไม่เป็นอันตรายต่อระบบที่จะนำไปประมวลผลต่อไป

SQL Injection



SQL Injection Example

- Example : http://sqlzoo.net/hack/

การทำ Input Validation ของโปรแกรมประยุกต์บนเว็บ

ปัญหาที่พบ

•หากเว็บไซต์ใดๆ การตรวจสอบข้อมูลที่ได้รับก่อนส่งมาประมวลผลจริง ยอมให้ผู้ใช้บริการสามารถป้อนข้อมูลได้โดยไม่มีการตรวจสอบก่อนแล้ว การโจมตีเว็บไซต์จะสามารถทำได้ง่าย

•ยกตัวอย่างเช่น เว็บไซต์เชื่อมต่อกับฐานข้อมูลทุกครั้งที่มีการเรียกหน้าเว็บเพจ เป็นสาเหตุให้เกิดการโจมตีเว็บไซต์ด้วยเทคนิค SQL Injection ซึ่งการโจมตีด้วยเทคนิค SQL Injection นี้ ผู้ประสงค์ร้ายแทรกคำสั่ง SQL เข้าไปทาง input form บนเว็บเพจ

การทำ Input Validation ของโปรแกรมประยุกต์บนเว็บ (ต่อ)

ตัวอย่างวิธีการป้องกัน

- ตรวจสอบข้อมูลที่ได้รับก่อนส่งมาประมวลผลจริง หลักการคือให้ระบุรูปแบบของข้อมูลที่อนุญาต (Whitelist) หรือไม่อนุญาต (Blacklist) ให้ป้อนเข้าสู่ระบบ
- มีการทำ Encoding หรือทำ Sanitization ก่อนนำค่ามาประมวลผล เพื่อป้องกันการโจมตีด้วยเทคนิคต่าง ๆ ข้อมูลที่ผ่านกระบวนการดังกล่าวจะถูกแปลงรูปแบบของข้อมูลที่ส่งมาจากฝั่งผู้ใช้บริการให้อยู่ในรูปแบบที่ระบบนำไปประมวลผลได้โดยไม่อันตราย เช่น หากผู้ประสงค์ร้ายป้อนข้อมูลที่ใช้ในการโจมตีระบบเป็น ' OR 1=1 --' ระบบจะแปลงค่าเป็น \' OR 1=1 --\‘
- คัดกรองเครื่องหมายอักขระพิเศษต่างๆ เช่น < > ? & # เป็นต้น ก่อนที่จะนำไปประมวลผลที่เครื่องบริการเว็บ คือ แปลงพวก "Non-alphanumeric data" ให้กลายเป็น HTML character เสียก่อน เช่น เครื่องหมายน้อยกว่า "<" ควรถูกแปลงเป็น "& l t ;" เป็นต้น
- ตัวอย่างการโจมตีที่จะป้องกันได้ : SQL Injection, Cross-site Scripting

หัวข้อตาม Checklist ที่เกี่ยวข้อง : Checklist 7.2, Checklist 7.3, Checklist 9.1, Checklist 9.2

Session Hijacking

การป้องกันการโจมตีจาก Session Hijacking

- Session ID มีการเข้ารหัส หรือ Hashing
- กำหนด Session Timeout ในระยะเวลาที่เหมาะสม
- กำหนดค่า Session ID เป็นค่าสุ่มที่คาดเดาไม่ได้ (Random value) และไม่มีการใช้ซ้ำในระยะเวลาที่เหมาะสม
- ต้องส่งค่า Session ID ในช่องทางการสื่อสารที่มีการเข้ารหัส (SSL) เพื่อป้องกันการดักรับข้อมูลโดยผู้ประสงค์ร้าย

การกำหนด Session ID ให้มีความมั่นคงปลอดภัย

- เมื่อผู้ใช้บริการเข้าระบบสำเร็จ จะมีการสร้างโทเค็น (token) ซึ่งใช้เป็นข้อมูลการรับรองตัวตนของผู้ใช้บริการ (User authentication credential) เรียกว่า Session ID ถูกนำไปใช้ในการอ้างอิงและตรวจสอบสิทธิในการเข้าถึงหน้าเว็บเพจต่าง ๆ ในเว็บไซต์ที่ผู้ใช้บริการเข้าเยี่ยมชม

- Session ID นี้จะถูกใช้จนกว่าผู้ใช้บริการจะปิดหน้าต่างโปรแกรมค้นดูเว็บ ก็ถือจะเป็นการลบ Session ID นั้นไป

- ตราบเท่าที่โปรแกรมค้นดูเว็บยังไม่ถูกปิด ผู้ประสงค์ร้ายสามารถอาศัยช่องโหว่นี้ในการโจมตีเว็บไซต์ด้วย วิธี **Session Hijack** ได้นั่นก็คือการดักขโมย Session ID ของผู้ใช้บริการ ไปใช้ในการเข้าเว็บไซต์ด้วยสิทธิของเจ้าของ session ได้

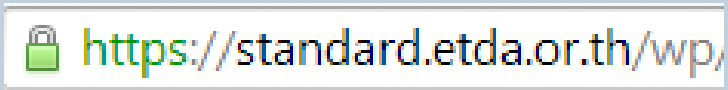
การกำหนด Session ID ให้มีความมั่นคงปลอดภัย (ต่อ)

ตัวอย่างวิธีการป้องกัน

(1)Session ID ต้องใช้เป็นค่าสุ่ม /มีการเข้ารหัสลับ

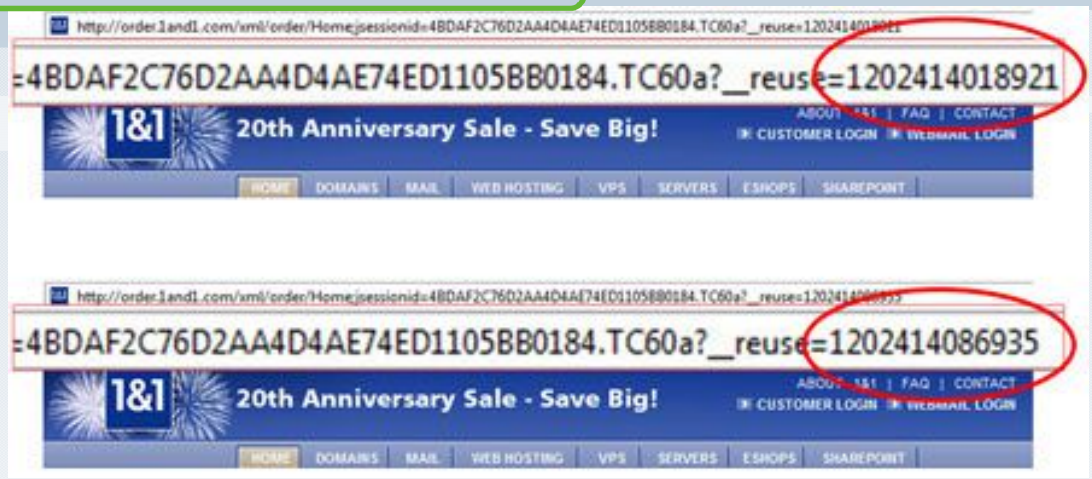
(2)กำหนด Session Timeout ในระยะเวลาที่เหมาะสม ระยะเวลาที่ใช้กำหนด Session Timeout ของแต่ละเว็บไซต์ขึ้นอยู่กับพฤติกรรมการใช้งานและความต้องการใช้งานของผู้ใช้บริการ ซึ่ง OWASP แนะนำดังนี้ “Common idle timeouts ranges are 2-5 minutes for high-value applications and 15- 30 minutes for low risk applications” *ข้อมูลเพิ่มเติมที่* *https://www.owasp.org/index.php/Session_Management_Cheat_Sheet*

(3)ส่งค่า Session ID ในช่องทางการสื่อสารที่มีการเข้ารหัสลับ (Encrypted connection) เช่น โพรโทคอล https



<u>หัวข้อตาม Checklist ที่เกี่ยวข้อง</u> : Checklist 8 (Checklist 8.1, Checklist 8.2, Checklist 8.3 , Checklist 8.4)

ตัวอย่างของ Session ID ที่เป็นค่าสุ่มแต่ไม่ได้เข้ารหัสลับ



ตัวอย่างของ Session ID ที่มีการเข้ารหัสลับ

```
; pantip_sessions=ozUjcaV3LPj%2BQ%2B0134ecTIhcu1jv2X4H5ZIIOseuGjuOVrVyudcKnB13wpVcgEK7V61gj28NXi%2BU8NIt%2B4Tg%2FX57kqa
9mBshXCTaMPh%2BYhk6Q5tLa5STOurT%2FWJ17siQDonxj9YvXBYFNrIhlRo5Gc7KZCnTkGCtn93q20pus8ibYQCuKP0dqrznv5uS%2FodmtwpsdT6uVPuo
O7yAWkKaZyFPdEE8F64e3ONGYELubAKAYbtyiA53ROftRpdy7geDoBqFcooGfcOk362jKKjU6UFkxnGmpCA3RlsDG93%2FIMguKGwRLY1%2BINlspp1Tub%
2FUBlZMRC5A2gRckNr1XOvHZyrw1Yxc%2FaOtSB8LyOT%2B4cUs2%2Ff95K0BOmNW%2BW5QqGgdl3g1G%2B%2BIRYapFThDhtR4VqY5NCTR2GOc2VvWixk3
qS2gvjI1CAOL9LNJnEo9ln%2BfLTO%2FS%2BKJw9s5Ww3fGEB8D8tSnYPiXMDsAShGGtU3DQCqgWWIwbew3EjBNs5IvflxARmhKTd1iafRZZpbEKVMfrX5a
xYfvS4udhf%2BgEXzsxUscuzLzSsEGJcRbnO%2Bm5ppYsC6wk9dUAxn5Qe2fAC9FG26m3%2B0LCk1tKEL8UEcVHRCE3zj2k4tmgs0NLrp8CrSEH8y730AGY
2JD8IUM65EmhF8TnjfBYggYssUPlwedyytLxc8javab7h0TsMeFYD7AFN1LPL0cjQIgaqdo9BpGw%3D%3D; _ga=GA1.2.352093538.1417076630; _ga
```

การป้องกันการโจมตีจาก Cross-site Scripting

- ทำ Input validation (Whitelist หรือ Blacklist)
- มีการตรวจสอบข้อมูลชุดคำสั่งที่ได้รับเป็นข้อมูลที่ผิดปกติ หรือ เป็นสคริปต์ที่อันตรายหรือไม่ ป้องกันไม่ให้มีการวางสคริปต์ใด ๆ ลงในเว็บได้ มีการแปลง Non-alphanumeric data ให้เป็น HTMS Character เสียก่อน เช่น เครื่องหมาย < ให้แปลงเป็น <
- ทำ Output validation ในลักษณะ Sanitization
- ต้องมีการใช้งาน HTTPOnly Cookie flag

การป้องกันการโจมตีจาก CSRF

- ต้องมีการใช้งาน Unique Token หรือตรวจสอบ Referrer ร่วมกับการส่งข้อมูลหรือคำสั่งผ่านแบบฟอร์ม เพื่อยืนยันว่าข้อมูลในแบบฟอร์มที่ส่งมาประมวลผลแต่ละครั้งเกิดจากผู้ใช้บริการจริง หรือมีการใช้ OTP ร่วมกับการทำรายการ เพื่อยืนยันว่าการทำรายการเกิดจากผู้ใช้บริการจริง
- มีการใช้ Captcha เมื่อมีการเปลี่ยนแปลงสถานการณ์ทำงานในฟังก์ชั่นที่สำคัญ เช่นการชำระเงิน ระบบจะให้ผู้ใช้บริการ ยืนยันตัวตนอีกครั้ง เช่นให้กรอกรหัสผ่านใหม่ พร้อมกับการใช้ Captcha

Sensitive Data Exposure

การป้องกันการโจมตีจากข้อมูลรั่วไหล (Sensitive Data Exposure)

- มีการออกแบบและควบคุมข้อความแจ้งเตือน หรือข้อความแสดงข้อผิดพลาด (Notification or Error Message) ไม่ให้แสดงข้อมูลที่เป็นประโยชน์ต่อผู้ประสงค์ร้าย
- ไม่ให้มีการใช้งาน Auto Complete ในแบบฟอร์มสำคัญ เช่น แบบฟอร์มสำหรับการลงทะเบียนระบบที่มีการใส่รหัสผ่าน หรือแบบฟอร์มการรับชำระเงิน
- ไม่ใช้ชื่อ URL ที่คาดเดาได้ง่าย ซึ่งใช้ในการเข้าถึงหน้าเว็บที่สำคัญ เช่น หน้าเว็บสำหรับผู้ดูแลระบบ (Admin control panel page) ใช้ชื่อ admin.php

การรับมือสถานการณ์ภัยคุกคามที่เกิดจากการโจมตีเว็บ (Incident Handling)

- ภัยคุกคามที่เกิดขึ้นกับเว็บไซต์
- การเก็บข้อมูลจราจรทางคอมพิวเตอร์
- การใช้โปรแกรมตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์
- การสำรองข้อมูลเว็บไซต์

การรับมือภัยคุกคามที่เกิดขึ้นกับเว็บไซต์

มีการจัดทำแนวทางการรับมือสถานการณ์ภัยคุกคามที่เกิดกับเว็บไซต์ ในกรณีต่าง ๆ ดังนี้

1)Checklist 12.1: กรณีเว็บไซต์ถูกบุกรุกและควบคุม (Intrusions)
2)Checklist 12.2: กรณีเว็บไซต์ถูกโจมตีในลักษณะ DoS (Denial Of Service)
3)Checklist 12.3: กรณีโดเมนถูกขโมย (Domain Hijack)

หัวข้อตาม Checklist ที่เกี่ยวข้อง : Checklist 12 (Checklist 12.1, Checklist 12.2, Checklist 12.3)

การรับมือภัยคุกคามที่เกิดขึ้นกับเว็บไซต์

- กรณีเว็บไซต์ถูกบุกรุกและควบคุม (Intrusions)
  - ปิดการเชื่อมต่อ
  - สำเนาข้อมูลที่เกี่ยวข้องกับการถูกบุกรุก เพื่อนำไปวิเคราะห์
  - ตรวจสอบช่องทางการโจมตีและช่องโหว่ด้วยข้อมูลที่สำเนามา
  - สร้างหน้าเว็บไซต์แบบ Static ขึ้นมาทดแทนเป็นการชั่วคราว เพื่อแจ้งสถานการณ์การปิดปรับปรุง (ควรใช้เครื่องบริการเว็บเครื่องใหม่)
  - กู้คืนโปรแกรมที่เกี่ยวข้อง ข้อมูลเว็บ และฐานข้อมูลเป็นเวอร์ชั่นก่อนที่จะถูกโจมตี
  - ตรวจสอบช่องโหว่ด้วยการทำ Vulnerability Assessment (VA Scan) เพื่อหาช่องโหว่ และแก้ไข
  - บันทึกเหตุการณ์ และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด เพื่อเป็นข้อมูลในการป้องกันและประสานงานกับหน่วยงานที่เกี่ยวข้องในกรณีที่จำเป็น
- กรณีเว็บไซต์ถูกโจมตีในลักษณะ Dos (Denial of Service)
  - ปิดการเชื่อมต่อ
  - สำเนาข้อมูลที่เกี่ยวข้องกับการถูกบุกรุก เพื่อนำไปวิเคราะห์
  - ตรวจสอบหมายเลข ไอพี ที่ต้องสงสัยว่าจะเป็นการโจมตีจากข้อมูลที่ทำสำเนามา
  - ปิดกันการเข้าถึงจาก ไอพีแอดเดรสที่ตรวจพบ และแจ้งไปยังผู้ให้บริการเครือข่ายอินเตอร์เน็ตเพื่อหามาตรการที่รองรับ
  - บันทึกเหตุการณ์ และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด เพื่อเป็นข้อมูลในการป้องกันต่อไป
  - บันทึกเหตุการณ์ และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด เพื่อเป็นข้อมูลในการป้องกันและประสานงานกับหน่วยงานที่เกี่ยวข้องในกรณีที่จำเป็น

การรับมือภัยคุกคามที่เกิดขึ้นกับเว็บไซต์

- กรณีโดเมยถูกขโมย (Domain Hijack)
  - เก็บรวบรวมหลักฐานที่เกิดขึ้นทั้งหมด เช่นวัน เดือน ปี ที่ข้อมูลโดเมนเปลี่ยน
  - ตรวจสอบกับผู้ลงทะเบียนโดเมน ถึงสาเหตุการเปลี่ยนแปลงโดเมน บางครั้งพบว่าผู้ดูแลถูกขโมยข้อมูลรหัสผ่านโดยการติดมัลแวร์ ทำให้ผู้ประสงค์ร้ายสามารถเข้าสู่เว็บไซต์บริหารจัดการโดเมนและทำการเปลี่ยนแปลงข้อมูลส่วนบุคคล
  - แจ้งการถูกขโมยโดเมนกับผู้ลงทะเบียนโดเมนที่ใช้บริการ โดยนำหลักฐานที่เกี่ยวข้องแนบไปด้วย เช่นหลักฐานการโอนเงิน หลักฐานการตอบรับการจดทะเบียนโดเมน เป็นต้น
  - เมื่อได้รับสิทธิในการบริหารจัดการโดเมนคืนมาแล้ว ให้ตรวจสอบข้อมูลที่ใช้ยืนยันตัวตน เช่น ข้อมูลอีเมลผู้จดทะเบียนโดเมน รวมถึงเปลี่ยนรหัสผ่านในระบบบริหารจัดการโดเมน
  - บันทึกเหตุการณ์ และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด เพื่อเป็นข้อมูลในการป้องกันและประสานงานกับหน่วยงานที่เกี่ยวข้องในกรณีที่จำเป็น

การใช้โปรแกรมตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์

- เลือกโปรแกรมที่น่าเชื่อถือ หรือ ได้รับการแนะนำจากหน่วยงานที่เกี่ยวข้อง พร้อมกับตรวจสอบและอัปเดตโปรแกรมให้เป็นเวอร์ชั่นล่าสุดเสมอ
- สำรองข้อมูลทุกครั้งก่อนมีการใช้โปรแกรมตรวจสอบ
- ใช้โปรแกรมมากกว่าสองโปรแกรมขึ้นไปในการตรวจสอบเพื่อเปรียบเทียบผลลัพธ์ที่ได้

โปรแกรมตรวจสอบความมั่นคงปลอดภัยที่มีความน่าเชื่อถือ เช่น Acunetix Web Vulnerability Scanner ,Vega หรือ OWASP ZAP

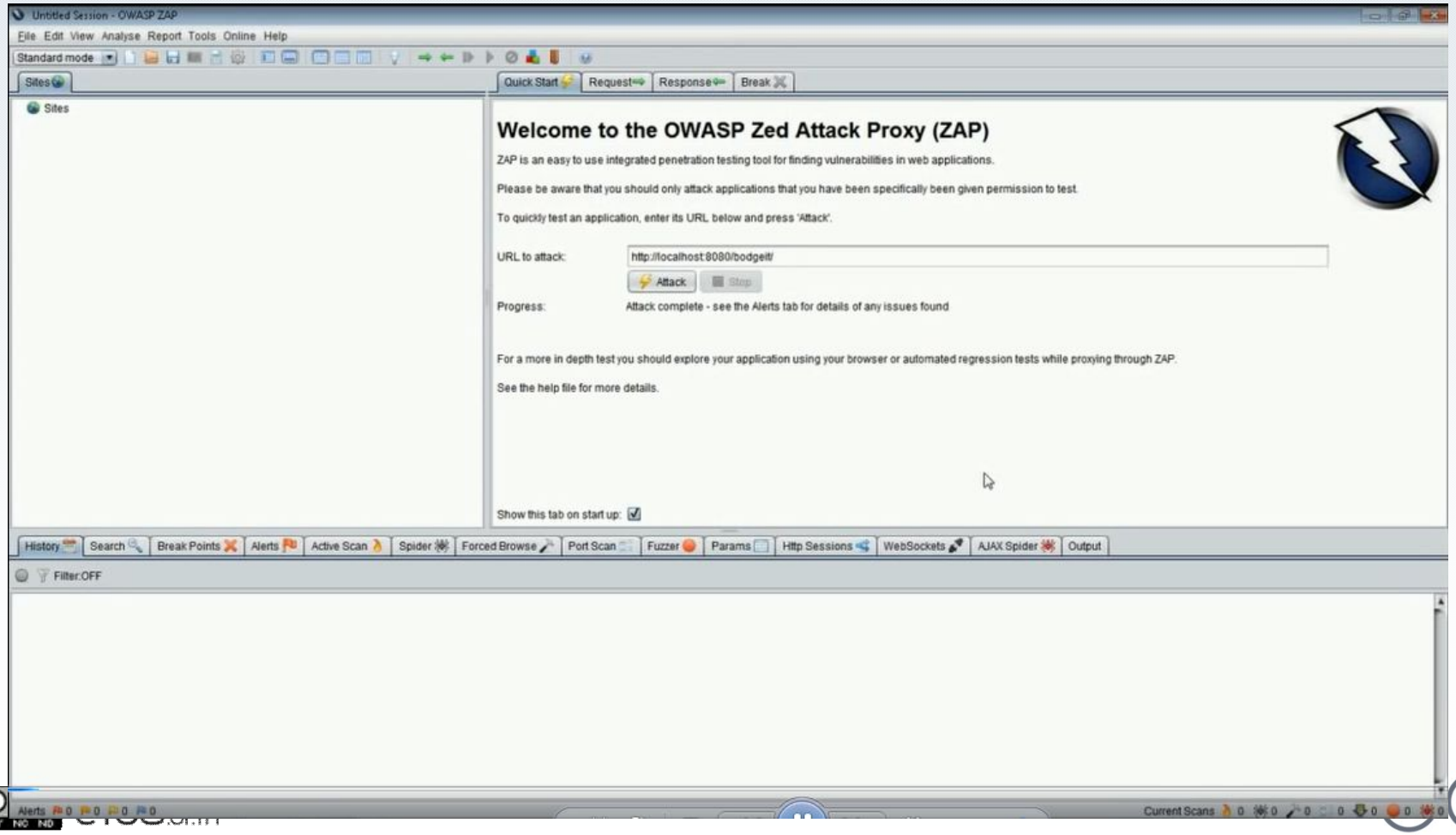
acunetix WEB APPLICATION SECURITY

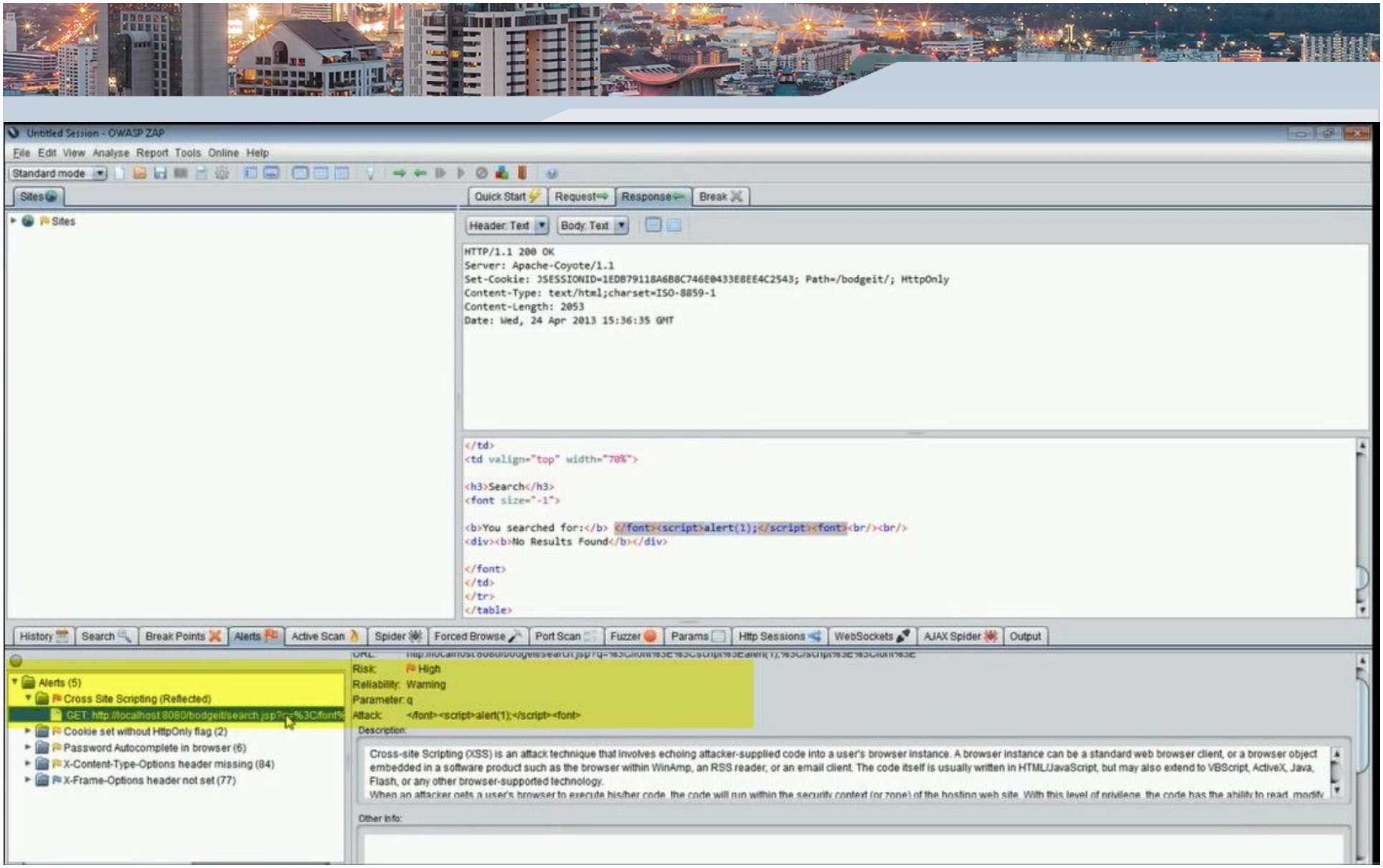
VEGA BETA RELEASE
OPEN SOURCE WEB APPLICATION VULNERABILITY SCANNER, PROXY AND PLATFORM

OWASP ZAP

<u>หัวข้อตาม Checklist ที่เกี่ยวข้อง</u> : Checklist 13 (Checklist 13.1, Checklist 13.2, Checklist 13.3, Checklist 13.4)

การใช้โปรแกรม OWASP ZAP สำหรับตรวจสอบความมั่นคงปลอดภัยสำหรับเว็บไซต์





etda.or.th

การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

มีการบันทึกข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลการใช้งานของผู้ใช้ (Log) ที่เป็นไปตาม

- ข้อกำหนดในพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550
- ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 (มาตรา 26)
- ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า เก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์

หัวข้อตาม Checklist ที่เกี่ยวข้อง : Checklist 15 (Checklist 15.1)

การสำรองข้อมูลเว็บไซต์

- เมื่อพบว่าเว็บไซต์ถูกโจมตี สิ่งที่ทำได้ในเบื้องต้นคือ ผู้ดูแลเครื่องบริการเว็บกู้คืนข้อมูลเวอร์ชั่นก่อนที่จะพบว่าถูกโจมตี ที่ได้สำรองข้อมูลไว้

- องค์ประกอบหลักในการสำรองข้อมูลบนเครื่องบริการเว็บมี 2 องค์ประกอบ
    1. การสำรองข้อมูลและระบบปฏิบัติการบนเครื่องบริการเว็บอย่างสม่ำเสมอตามนโยบายของหน่วยงาน
    2. การดูแลรักษาข้อมูลสำรองที่เชื่อถือได้ (Authoritative copy) เช่น บนเครื่องบริการที่เข้าถึงได้เฉพาะ IP Address ที่ได้รับอนุญาตเท่านั้น

- หน่วยงานมีการจัดทำนโยบายในการสำรองข้อมูลของเครื่องบริการเว็บ โดยให้สอดคล้องกับข้อกฎหมาย ข้อผูกพันทางสัญญา และนโยบายของหน่วยงาน

<u>หัวข้อตาม Checklist ที่เกี่ยวข้อง</u> : Checklist 16 (Checklist 16.1)

การใช้ Checklist สำหรับการวางแผนและตรวจสอบความมั่นคงปลอดภัยสำหรับเว็บไซต์

การใช้ Check list สำหรับการวางแผนและตรวจสอบความมั่นคงปลอดภัยสำหรับเว็บไซต์

สามารถใช้ checklist ในการตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์ ในหัวข้อดังนี้

1. การวางแผนเพื่อบริหารจัดการเว็บไซต์
2. การตั้งค่าเครื่องบริการเว็บอย่างมั่นคงปลอดภัย
3. การพัฒนาโปรแกรมประยุกต์บนเว็บอย่างมั่นคงปลอดภัย
4. การรับมือสถานการณ์ภัยคุกคามที่เกิดจากการโจมตีเว็บไซต์

โดยสามารถประเมินได้ด้วยตนเอง ยกตัวอย่างเช่น

1) ท่านมีการวางแผนเพื่อบริหารจัดการเครื่องบริการเว็บที่ยอมรับได้ในหน่วยงาน หรือไม่ ถ้ามีให้เลือก “ยอมรับได้”

2) หรือถ้ายังไม่มี ให้เลือกที่ช่อง “ยังต้องปรับปรุง”

3) และเมื่อพบข้อที่ยังต้องปรับปรุงเพิ่มเติม ให้นำรายละเอียดใส่ใน **<u>แบบฟอร์มสำหรับการแก้ไขรายการที่ยังต้องปรับปรุง (จากการตรวจสอบสถานะความมั่นคงปลอดภัย)</u>** เพื่อปรับปรุงแก้ไขต่อไป

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			

แบบฟอร์มตรวจสอบสถานะความมั่นคงปลอดภัยสำหรับเว็บไซต์

(สำหรับผู้ดูแลเครื่องบริการเว็บและผู้พัฒนาโปรแกรมประยุกต์บนเว็บ)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
	อบริหารจัดการเว็บไซต์ (หัวข้อ 4)			
1	แผนด้านความมั่นคงปลอดภัยของเว็บไซต์ (หัวข้อ 4.1)			
1.1	มีการวางแผนเพื่อบริหารจัดการเครื่องบริการเว็บ (หัวข้อ 4.1 ข้อ 1)		✔	
1.2	จัดลำดับความเสี่ยงของภัยคุกคามที่คาดว่าจะเกิดขึ้นกับเว็บไซต์			

วันที่ตรวจสอบสถานะ		เว็บไซต์:	
โดยหน่วยงาน			

ลำดับที่	วันที่รายงาน	คำอธิบายรายการที่ยังต้องปรับปรุง	สาเหตุ	การแก้ไขชั่วคราว	สิ่งที่ต้องแก้ไข		
					รายการแก้ไข	รับผิดชอบโดย	วันที่แล้วเสร็จ

ตัวอย่างการกรอกและใช้งานแบบฟอร์มสำหรับการแก้ไขรายการที่ยังต้องปรับปรุง (จากการตรวจสอบสถานะความมั่นคงปลอดภัย)

	หัวข้อ	ยอมรับได้	ยังต้องปรับปรุง	หมายเหตุ
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)	✔		

เมื่อพบรายการที่ไม่เป็นไปตามข้อกำหนด **ให้ระบุรายการแก้ไขลงในแบบฟอร์มสำหรับการแก้ไขรายการที่ยังต้องปรับปรุง** พร้อมกับกำหนดระยะเวลาในการแก้ไขเพื่อนำเสนอต่อผู้ที่เกี่ยวข้องต่อไป ดังนี้

การใช้แบบฟอร์มสำหรับการแก้ไขรายการที่ยังต้องปรับปรุง
(จากการตรวจสอบสถานะความมั่นคงปลอดภัย)

กรอกวันที่ตรวจสอบสถานะความมั่นคงปลอดภัยของเว็บไซต์

กรอกชื่อเว็บไซต์ของหน่วยงาน

วันที่ตรวจสอบสถานะ		เว็บไซต์	
โดยหน่วยงาน			

กรอกชื่อหน่วยงาน

กรอกรายละเอียดของสิ่งที่ต้องแก้ไข

ลำดับที่	วันที่รายงาน	คำอธิบายรายการที่ยังต้องปรับปรุง	สาเหตุ	การแก้ไขชั่วคราว	สิ่งที่ต้องแก้ไข		
					รายการแก้ไข	รับผิดชอบโดย	วันที่แล้วเสร็จ

วันที่จัดทำรายงานของรายการนี้

หัวข้อและรายละเอียดของรายการที่ประเมิน ‘ยังต้องปรับปรุง’

ระบุสาเหตุที่ทำให้หัวข้อนี้ ‘ยังต้องปรับปรุง’

รายละเอียดของการแก้ไขในเบื้องต้น

ตัวอย่างการกรอกแบบฟอร์มสำหรับการแก้ไขรายการที่ยังต้องปรับปรุง (จากการตรวจสอบสถานะความมั่นคงปลอดภัย)

วันที่ตรวจสอบสถานะ	5 ม.ค. 2558	เว็บไซต์	www.example.com
โดยหน่วยงาน	กรม A		

ลำดับที่	วันที่รายงาน	คำอธิบายรายการที่ยังต้องปรับปรุง	สาเหตุ	การแก้ไขชั่วคราว	สิ่งที่ต้องแก้ไข		
					รายการแก้ไข	รับผิดชอบโดย	วันที่แล้วเสร็จ
1	6 ม.ค. 58	(หัวข้อที่ 5.3 ข้อ 4) จัดให้มีการทบทวนบัญชีผู้ใช้ภายในฐานข้อมูลตามระยะเวลาที่กำหนดและลบบัญชีผู้ใช้ที่ไม่ได้มีการใช้งานออกจากระบบฐานข้อมูล	ยังมีบัญชีผู้ใช้ที่ไม่ได้ใช้งานแล้ว ปรากฏอยู่ในฐานข้อมูล	จัดการลด permission ของบัญชีผู้ใช้ที่ไม่ได้ใช้งานให้เป็น NONE	จัดให้มีการทบทวนบัญชีผู้ใช้ภายในฐานข้อมูลและลบบัญชีผู้ใช้ที่ไม่ได้มีการใช้งานออกจากระบบฐานข้อมูล	สมชาย	8 ม.ค. 58


ETDA
สพธอ
www.etda.or.th
THANK YOU
ดาวน์โหลดเอกสารประกอบการอบรม
https://standard.etda.or.th/wp/?page_id=5620
สอบถามข้อมูลเพิ่มเติม
สำนักมาตรฐาน
เว็บไซต์: https://standard.etda.or.th
อีเมล: estandard.center@etda.or.th