ETDA สพธอ
www.etda.or.th

งานสัมมนา
“ยกระดับความมั่นคงปลอดภัยของเว็บไซต์ให้ได้มาตรฐาน”

โดย นายศุภโชค จันทรประทิน

วิทยากรจากทีม e-Standard Center สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

งานสัมมนา
“ยกระดับความมั่นคงปลอดภัยของเว็บไซต์ให้ได้มาตรฐาน”

หัวข้อการบรรยาย

- การวางแผนด้านความมั่นคงปลอดภัยเพื่อบริหารจัดการเว็บไซต์
- การใช้ Checklist สำหรับการวางแผนและตรวจสอบความมั่นคงปลอดภัยสำหรับเว็บไซต์
- เทคนิคและวิธีการตรวจประเมินความมั่นคงปลอดภัยของเว็บไซต์ด้วยตนเอง

Q&A

ดาวน์โหลดเอกสารที่เกี่ยวข้องได้ที่

https://standard.etda.or.th

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

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

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

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 **แบบฟอร์มสำหรับการแก้ไขรายการที่ยังต้องปรับปรุง (จากการตรวจสอบสถานะความมั่นคงปลอดภัย)** 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

เทคนิคและวิธีการตรวจประเมินความมั่นคงปลอดภัยของเว็บไซต์ด้วยตนเอง

หัวข้อ

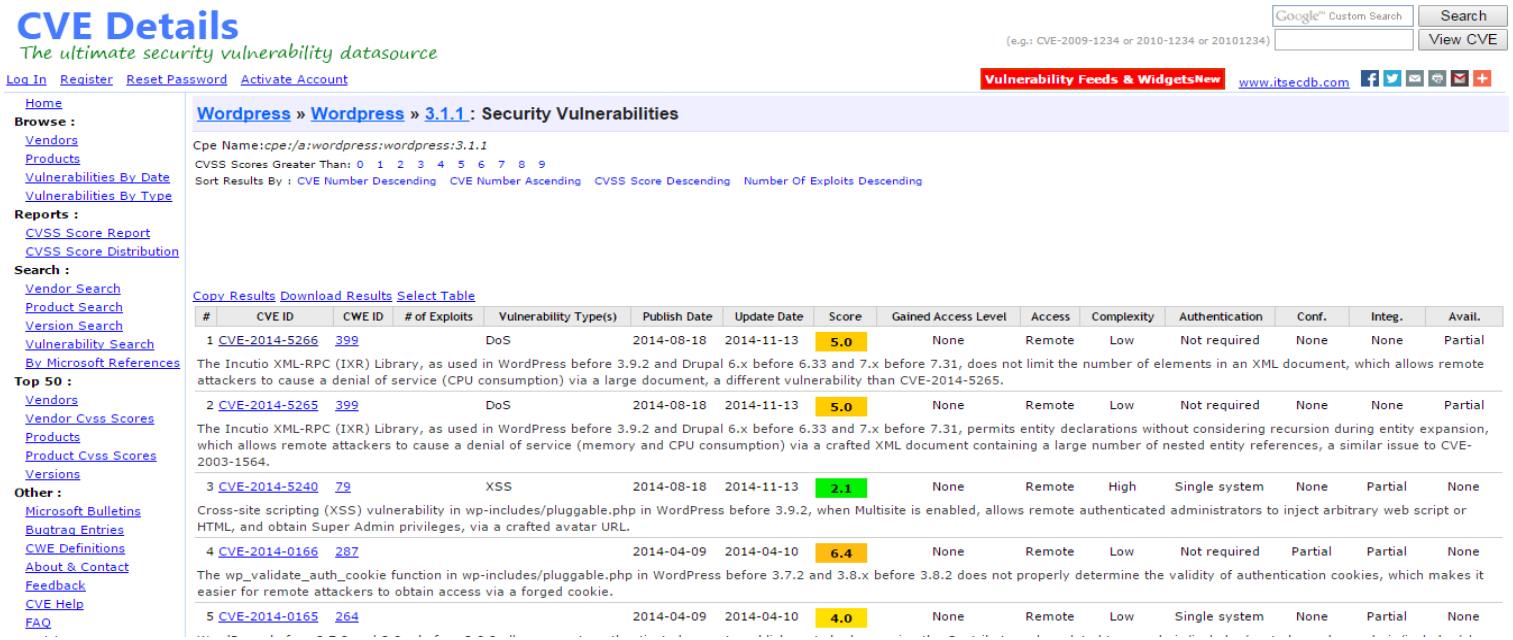
- การปรับปรุงโปรแกรมประยุกต์ต่างๆ ให้เป็นเวอร์ชั่นล่าสุด
- การทำ Input Validation ของโปรแกรมประยุกต์บนเว็บ
- การควบคุมข้อความแจ้งเตือนหรือข้อความแสดงข้อผิดพลาด (Error Message)
- การตรวจสอบและลบค่าเริ่มต้นของข้อมูลที่มาพร้อมกับการติดตั้ง หรือข้อมูลที่ไม่ได้ใช้งานในโปรแกรมประยุกต์ต่างๆ
- การกำหนดและรักษารหัสผ่าน
- การกำหนด Session ID ให้มีความมั่นคงปลอดภัย
- การจัดการ Permission / Access Control
- การรับมือสถานการณ์ภัยคุกคามที่เกิดจากการโจมตีเว็บไซต์ (Incident Handling)
    - การรับมือสถานการณ์ภัยคุกคาม
    - การใช้โปรแกรมตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์
    - การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์
    - การสำรองข้อมูลเว็บไซต์

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

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

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

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

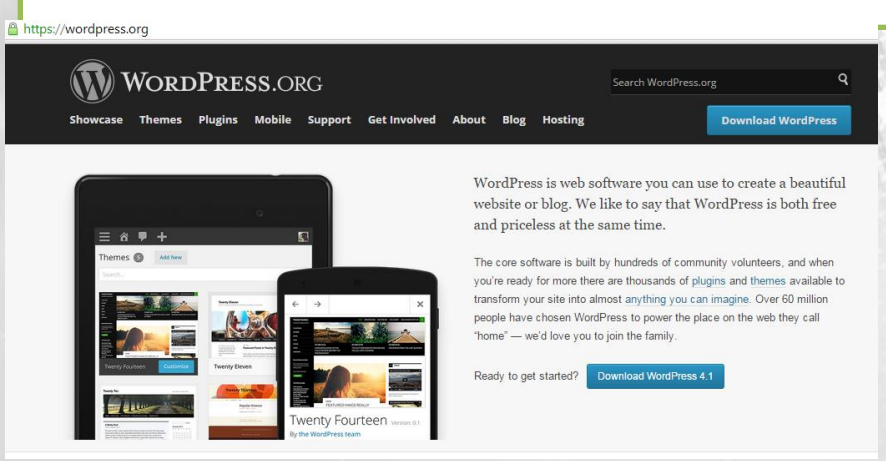
http://www.cvedetails.com/vulnerability-list/

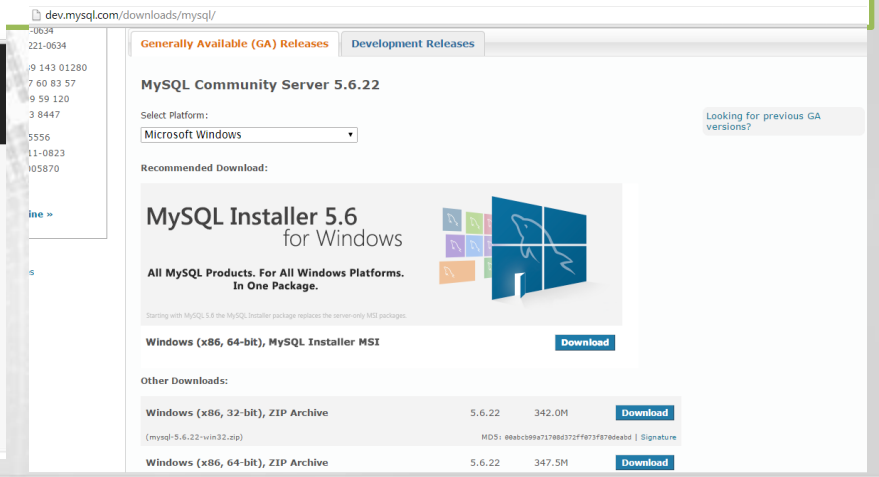
การปรับปรุงโปรแกรมประยุกต์ต่างๆ ให้เป็นเวอร์ชั่นล่าสุด (ต่อ)

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





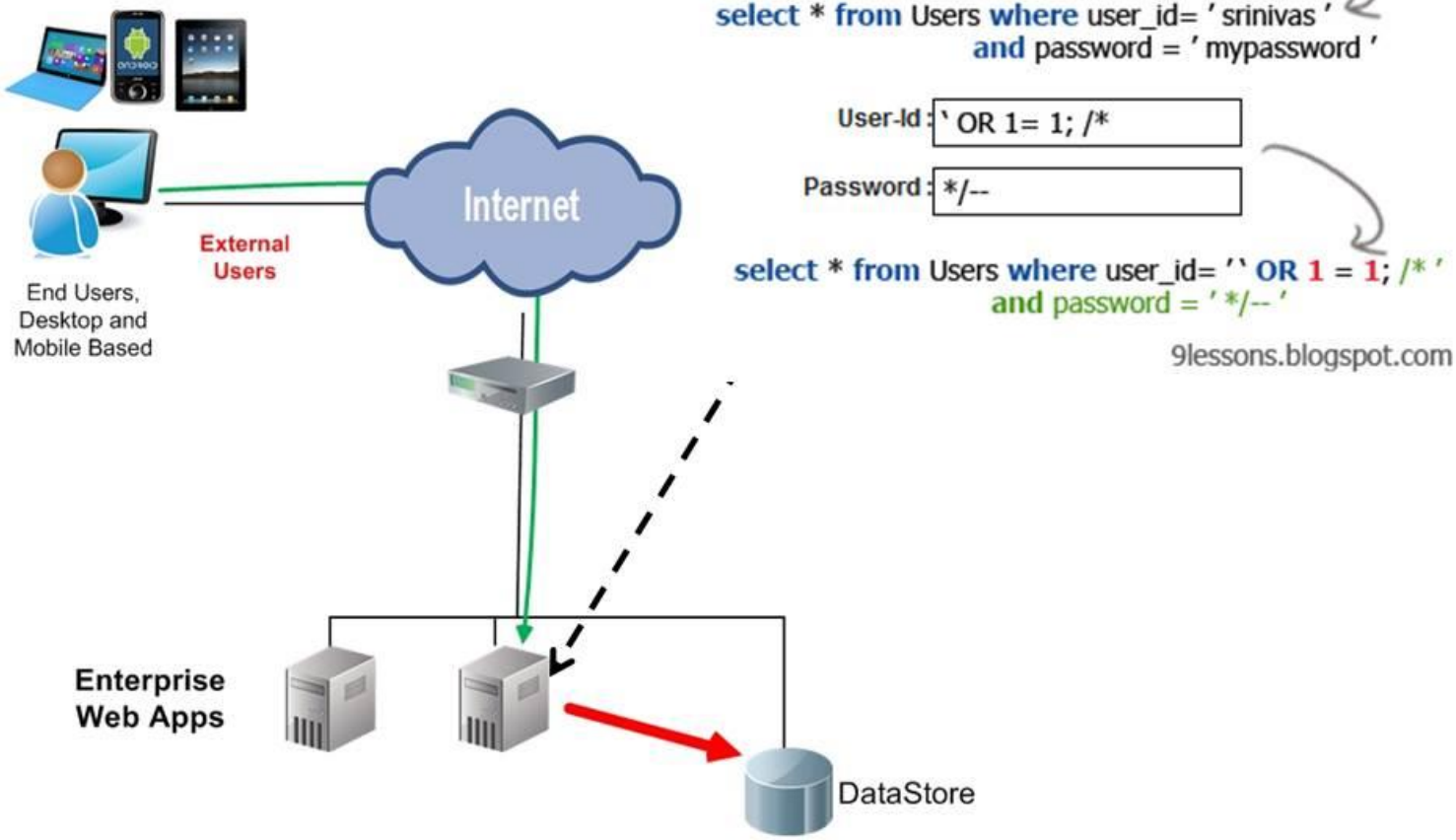
การทำ Input Validation ของโปรแกรมประยุกต์บนเว็บ

ปัญหาที่พบ

•หากเว็บไซต์ใดๆ การตรวจสอบข้อมูลที่ได้รับก่อนส่งมาประมวลผลจริง ยอมให้ผู้ใช้บริการสามารถป้อนข้อมูลได้โดยไม่มีการตรวจสอบก่อนแล้ว การโจมตีเว็บไซต์จะสามารถทำได้ง่าย

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

SQL Injection



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

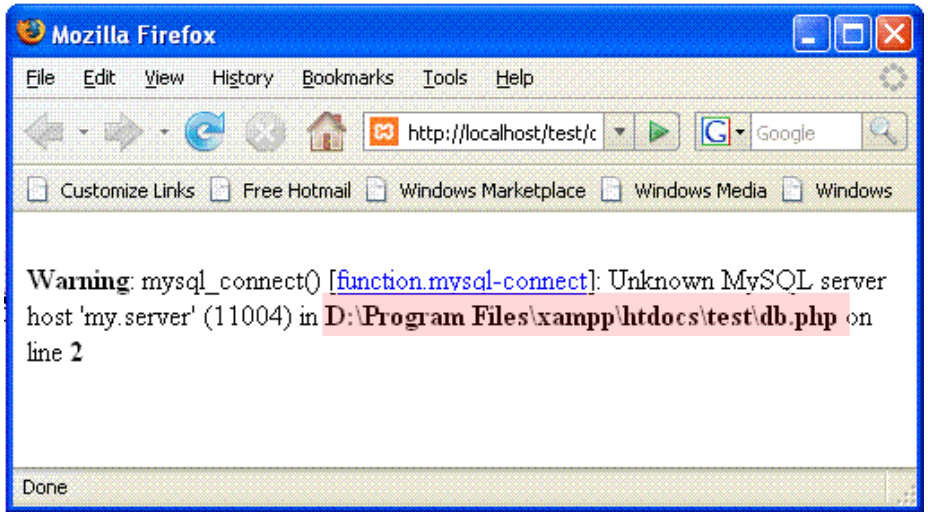
หัวข้อตาม Checklist ที่เกี่ยวข้อง : Checklist 7.2, Checklist 7.3, Checklist 9.1, Checklist 9.2

การควบคุมข้อความแจ้งเตือนหรือข้อความแสดงข้อผิดพลาด (Error Message)

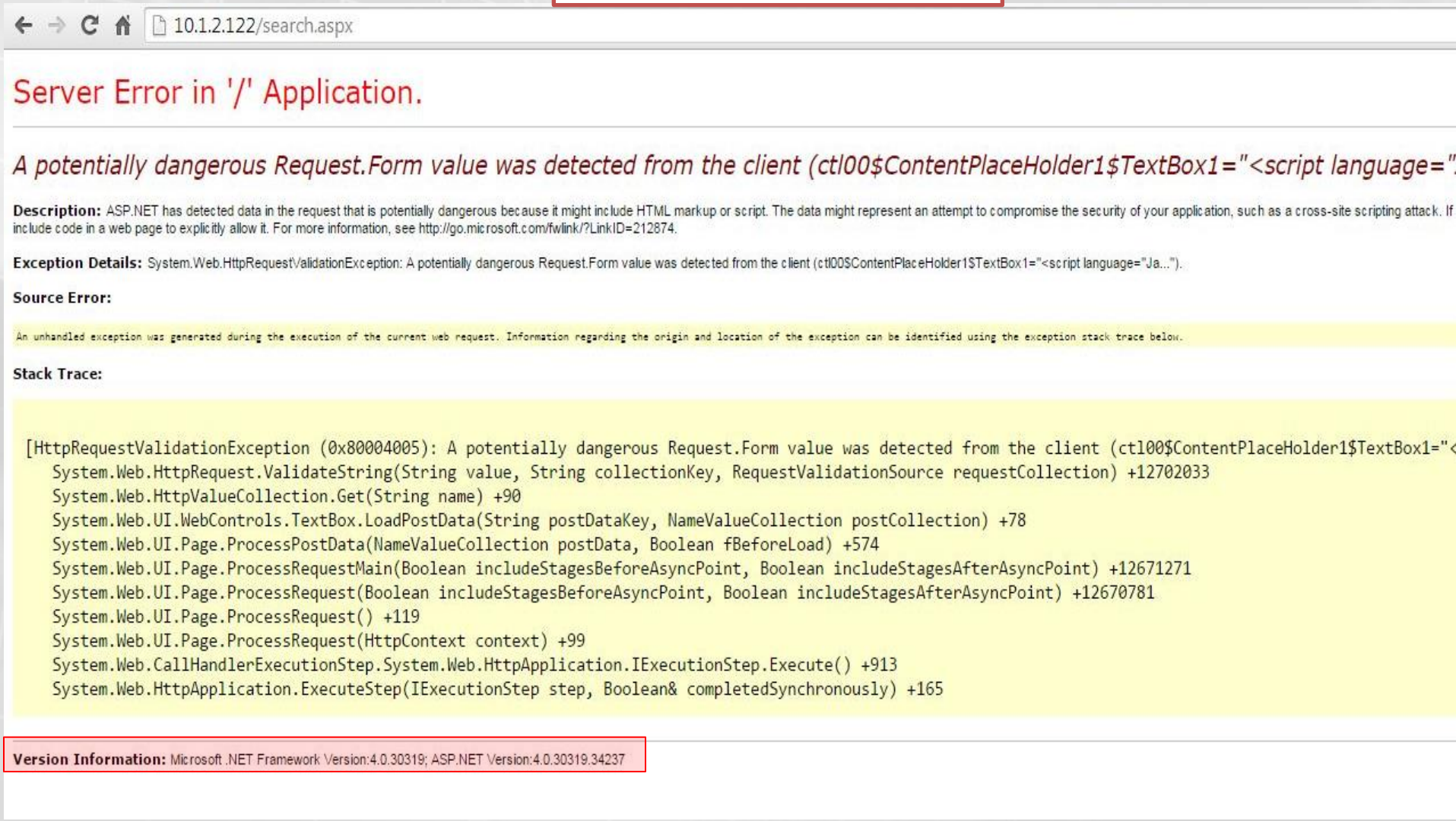
ปัญหาที่พบ

•การไม่ควบคุม Error Message ผู้ประสงค์ร้ายสามารถใช้ข้อมูลจาก Error Message คาดเดาข้อมูลการตั้งค่าของโปรแกรมและระบบที่เกี่ยวข้องได้ เช่น

Database Error Message



ตัวอย่าง Server Error Message



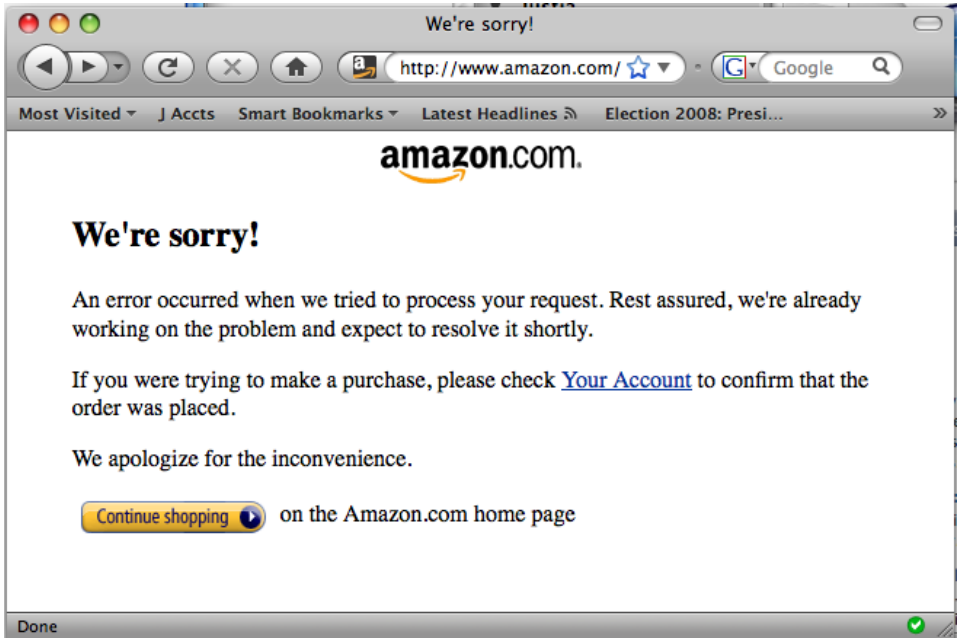
การควบคุมข้อความแจ้งเตือนหรือข้อความแสดงข้อผิดพลาด (Error Message) (ต่อ)

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

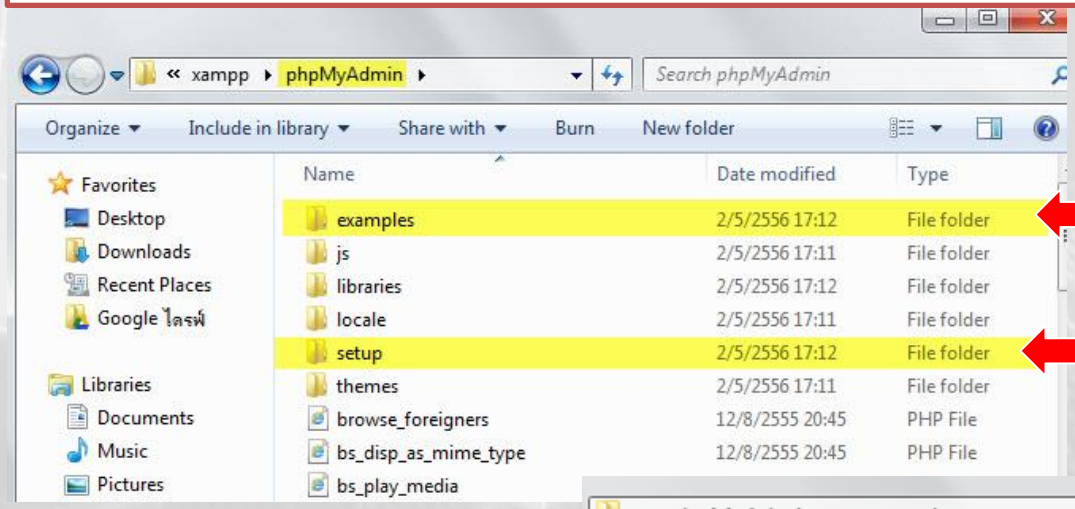


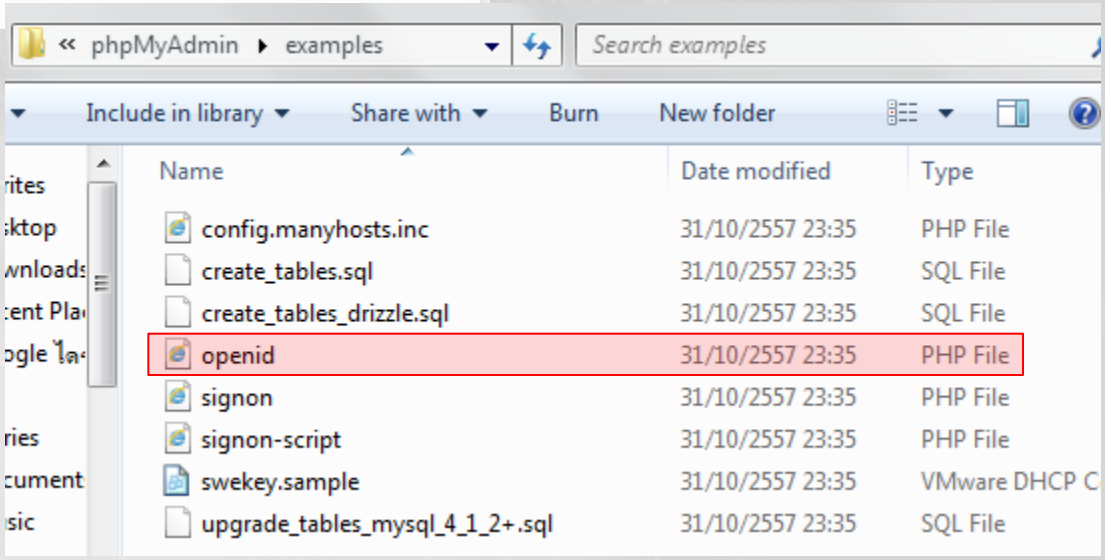
การตรวจสอบและลบค่าเริ่มต้นของข้อมูลที่มาพร้อมกับการติดตั้ง หรือข้อมูลที่ไม่ได้ใช้งานในโปรแกรมประยุกต์ต่างๆ

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



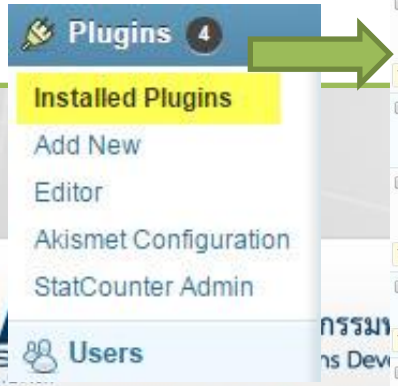


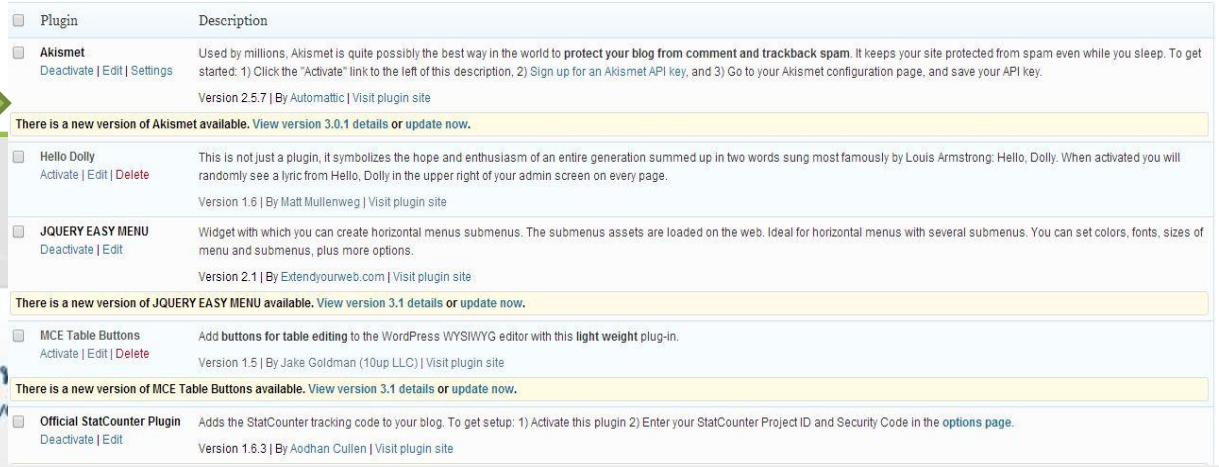
การตรวจสอบและลบค่าเริ่มต้นของข้อมูลที่มาพร้อมกับการติดตั้ง หรือข้อมูลที่ไม่ได้ใช้งานในโปรแกรมประยุกต์ต่างๆ (ต่อ)

ตัวอย่างวิธีการป้องกัน

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

<u>หัวข้อตาม Checklist ที่เกี่ยวข้อง</u> : Checklist 2.4, Checklist 2.5, Checklist 3.4, Checklist 3.5, Checklist 4.5, Checklist 4.7, Checklist 11.3





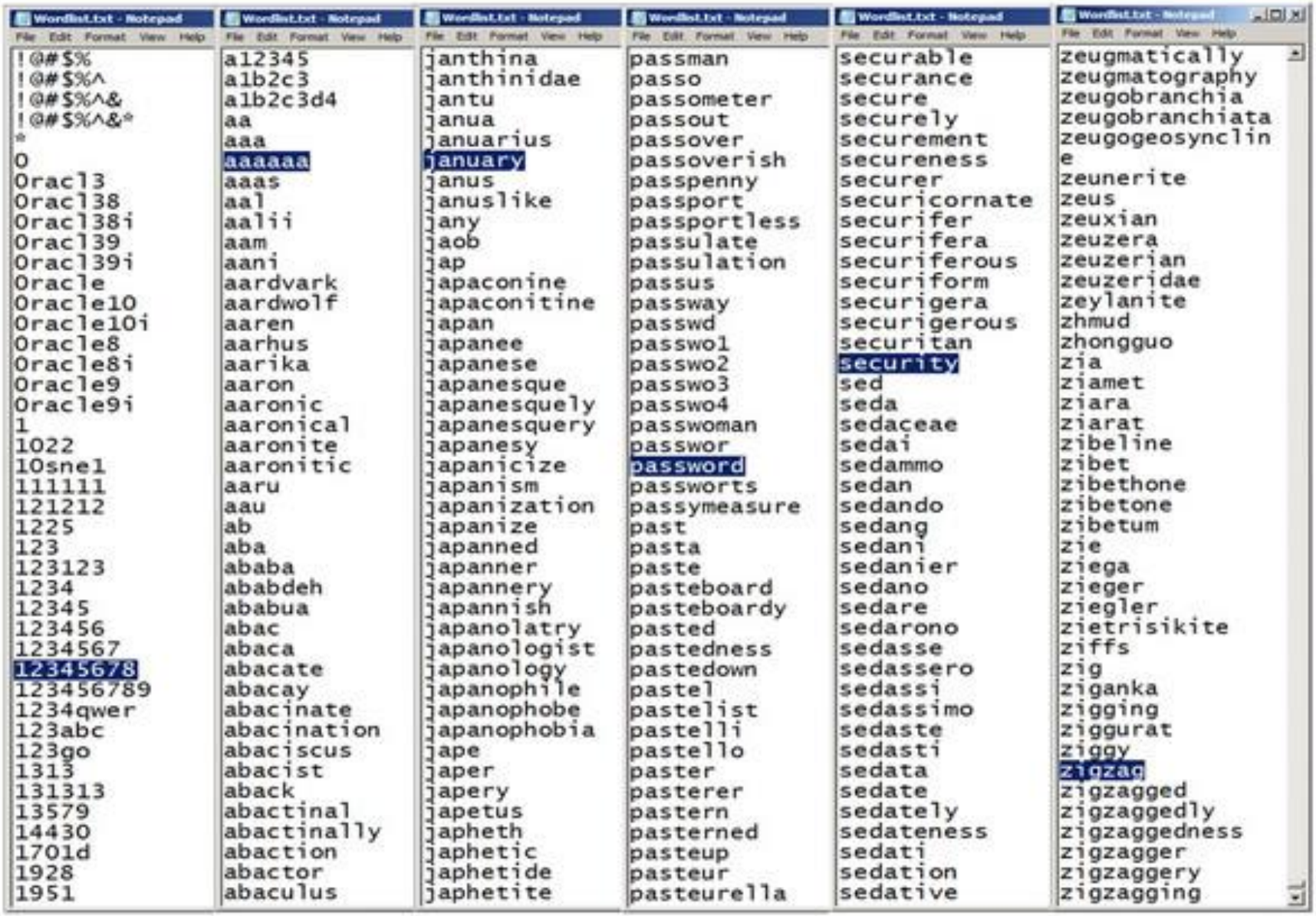
การกำหนดและรักษารหัสผ่าน

ปัญหาที่พบ

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

- 2. Brute Force Attack = คาดเดารหัสผ่านตามทุกความเป็นไปได้ของตัวอักษรในแต่ละหลัก ผู้ประสงค์ร้ายอาจเป็นผู้ลองกระทำเองหรืออาจจะใช้โปรแกรมอัตโนมัติทำงาน

Dictionary Attack (A - Z) for guessable simple password !!!



Wordlist.txt - Notepad

File Edit Format View Help

```
!@#$%
!@#$%^
!@#$%^&
!@#$%^&*
*
0
Oracl3
Oracl38
Oracl38i
Oracl39
Oracl39i
Oracle
Oracle10
Oracle10i
Oracle8
Oracle8i
Oracle9
Oracle9i
1
1022
10sne1
111111
121212
1225
123
123123
1234
12345
123456
1234567
12345678
123456789
1234qwer
123abc
123go
1313
131313
13579
14430
1701d
1928
1951
```

Wordlist.txt - Notepad

File Edit Format View Help

```
a12345
a1b2c3
a1b2c3d4
aa
aaa
aaaaaa
aaas
aal
aalii
aam
aani
aardvark
aardwolf
aaren
aarhus
aarika
aaron
aaronic
aaronical
aaronite
aaronitic
aaru
aau
ab
aba
ababa
ababdeh
ababua
abac
abaca
abacate
abacay
abacinate
abacination
abaciscus
abacist
aback
abactinal
abactinally
abaction
abactor
abaculus
```

Wordlist.txt - Notepad

File Edit Format View Help

```
janthina
janthinidae
jantu
janua
januarius
january
janus
januslike
jany
jaob
jap
japaconine
japaconitine
japan
japanee
japanese
japanesque
japanesquely
japanesquery
japanesy
japanicize
japanism
japanization
japanize
japanned
japanner
japannery
japannish
japanolatry
japanologist
japanology
japanophile
japanophobe
japanophobia
jape
japer
japery
japetus
japheth
japhetic
japhetide
japhetite
```

Wordlist.txt - Notepad

File Edit Format View Help

```
passman
passo
passometer
passout
passover
passoverish
passpenny
passport
passportless
passulate
passulation
passus
passway
passwd
passwo1
passwo2
passwo3
passwo4
passwoman
passwor
password
passworts
passymeasure
past
pasta
paste
pasteboard
pasteboardy
pasted
pastedness
pastedown
pastel
pastelist
pastelli
pastello
paster
pasterer
pastern
pasterned
pasteup
pasteur
pasteurella
```

Wordlist.txt - Notepad

File Edit Format View Help

```
securable
securance
secure
securely
securement
secureness
securer
securicornate
securifer
securifera
securiferous
securiform
securigera
securigerous
securitan
security
sed
seda
sedaceae
sedai
sedammo
sedan
sedando
sedang
sedani
sedanier
sedano
sedare
sedarono
sedasse
sedassero
sedassi
sedassimo
sedaste
sedasti
sedata
sedate
sedately
sedateness
sedati
sedation
sedative
```

Wordlist.txt - Notepad

File Edit Format View Help

```
zeugmatically
zeugmatography
zeugobranchia
zeugobranchiata
zeugogeosynclin
e
zeunerite
zeus
zeuxian
zeuzera
zeuzerian
zeuzeridae
zeylanite
zhmud
zhongguo
zia
ziamet
ziara
ziarat
zibeline
zibet
zibethone
zibetone
zibetum
zie
ziega
zieger
ziegler
zietrisikite
ziffs
zig
ziganka
zigging
ziggurat
ziggy
zigzag
zigzagged
zigzaggedly
zigzaggedness
zigzagger
zigzaggery
zigzagging
```

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

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

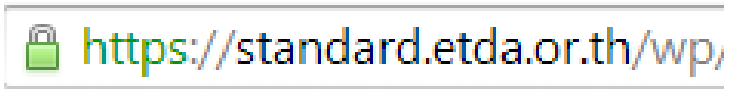
การกำหนด Session ID ให้มีความมั่นคงปลอดภัย (ต่อ)

ตัวอย่างวิธีการป้องกัน

(1)Session ID ต้องใช้เป็นค่าสุ่ม /มีการเข้ารหัสลับ

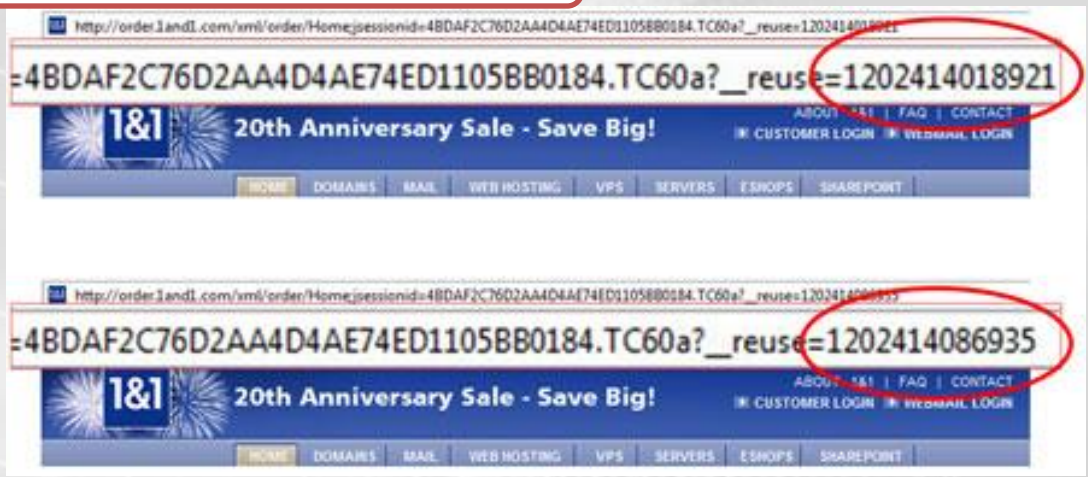
(2)กำหนด Session Timeout ในระยะเวลาที่เหมาะสม ระยะเวลาที่ใช้กำหนด Session Timeout ของแต่ละเว็บไซต์ขึ้นอยู่กับพฤติกรรมการใช้งานและความต้องการใช้งานของผู้ใช้บริการ ซึ่ง OWASP แนะนำดังนี้ “Common idle timeouts ranges are 2-5 minutes for high-value applications and 15- 30 minutes for low risk applications” *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%2FWJ17siQDonxj9YvXBYFNrIh1Ro5Gc7KZCnTkGCtn93q20pus8ibYQCuKP0dqrznv5uS%2FodmtwpsdT6uVPuo
O7yAWkKaZyFPdEE8F64e3ONGYELubAKAYbtyiA53ROftRpdy7geDoBqFcooGfcOk362jKKjU6UFkxnGmpCA3R1sDG93%2FIMguKGwRLY1%2BINlspp1Tub%
2FUB1ZMRC5A2gRckNr1XOvHZyrw1Yxc%2FaOtSB8LyOT%2B4cUs2%2Ff95K0BOmNW%2BW5QqGgd13g1G%2B%2BIRYapFThDhtR4VqY5NCTR2GOc2VvWixk3
qS2gvjI1CAOL9LNJnEo9ln%2BfLTO%2FS%2BKJw9s5Ww3fGEB8D8tSnYPiXMDsAShGGtU3DQCqgWWIwbew3EjBNs5IvflxARmhKTd1iafRZZpbEKVMfrX5a
xYfvS4udhf%2BgEXzsxUscuzLzSsEGJcRbnO%2Bm5ppYsC6wk9dUAxn5Qe2fAC9FG26m3%2B0LCk1tKEL8UEcVHRCE3zj2k4tmgs0NLrp8CrSEH8y730AGY
2JD8IUM65EmhF8TnjfBYggYssUPlwedyytLxc8javab7h0TsMeFYD7AFN1LPL0cjQIgaqdo9BpGw%3D%3D; _ga=GA1.2.352093538.1417076630; _ga
```

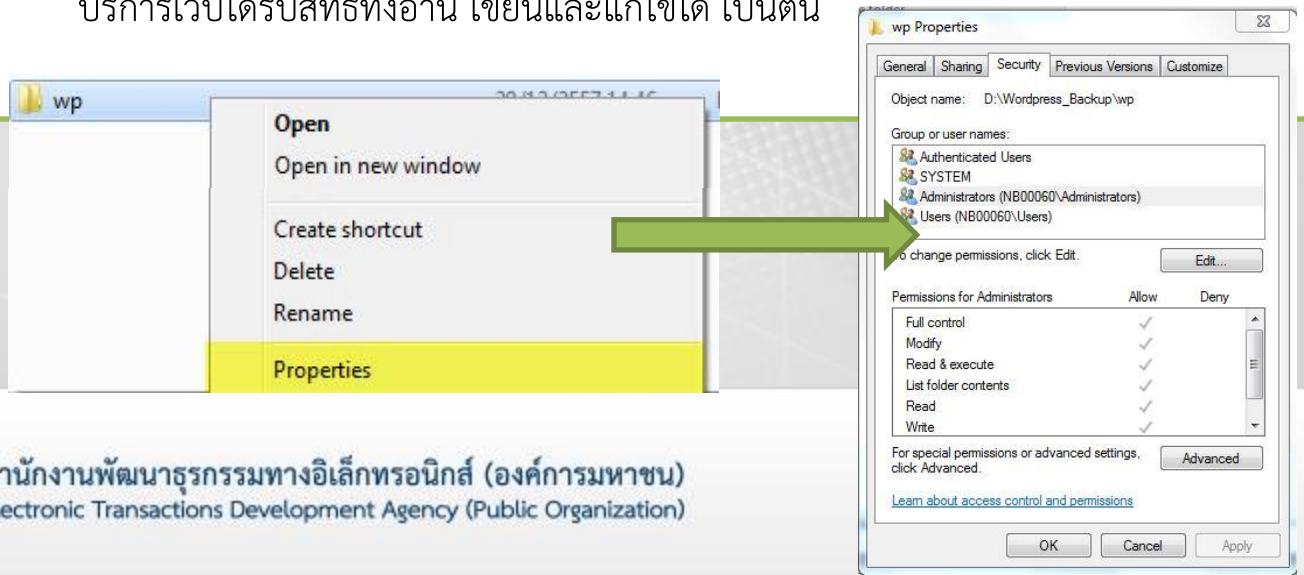
การจัดการ Permission / Access Control

•หากไม่มีการควบคุมการเข้าถึงข้อมูลที่มีความสำคัญ เช่น ไฟล์ที่เก็บข้อมูลเว็บเพจ ผู้ใช้ทั่วไปต้องได้สิทธิแค่อ่านเท่านั้น หากสามารถแก้ไขได้ ผู้ใช้ที่ประสงค์ร้ายก็จะสามารถเข้าถึงและแทรกสคริปต์อันตราย หรือแก้ไขข้อมูลใดๆ ให้เกิดความเสียหายแก่เว็บไซต์ได้ เป็นต้น

ตัวอย่างวิธีการป้องกัน

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

- ให้สิทธิการเข้าถึงไฟล์ หรือโฟลเดอร์ที่เก็บโปรแกรมแก่ผู้ใช้ที่เป็นเจ้าของไฟล์หรือนักพัฒนาซอฟต์แวร์เท่านั้น ผู้ใช้บริการทั่วไปได้รับสิทธิแค่อ่านและไม่สามารถแก้ไขได้ หรือผู้ดูแลเครื่องบริการเว็บได้รับสิทธิทั้งอ่าน เขียนและแก้ไขได้ เป็นต้น



การจัดการ Permission / Access Control (ต่อ)

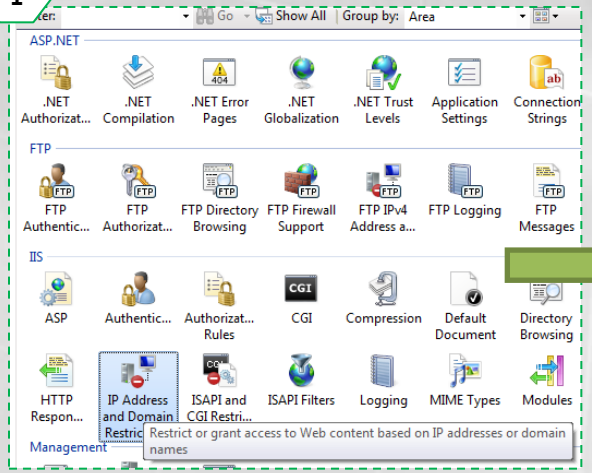
ตัวอย่างการจัดการ Access Control โดยการตั้งค่า IP Whitelist

- ควบคุมการเข้าถึงเครื่องบริการเว็บ และจำกัดหมายเลขไอพีปลายทางหรือยูอาร์แอล ที่อนุญาตให้เครื่องบริการเว็บสามารถเชื่อมต่อ (Whitelist)

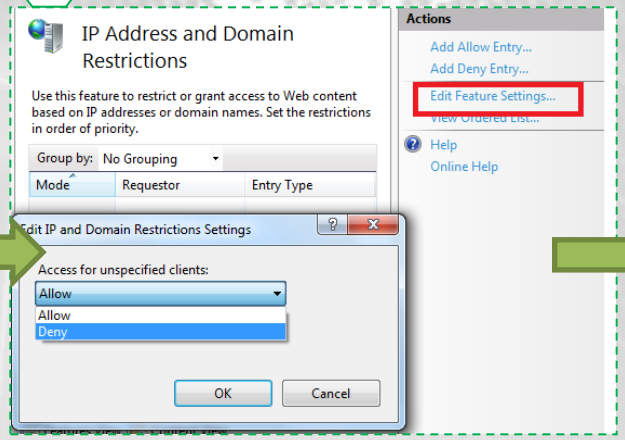
หัวข้อตาม Checklist ที่เกี่ยวข้อง : Checklist 2.3, Checklist 2.6, Checklist 3.1 , Checklist 4.1 , Checklist 4.9 , Checklist 5.1

ตัวอย่าง การกำหนด ip whitelist สำหรับ IIS

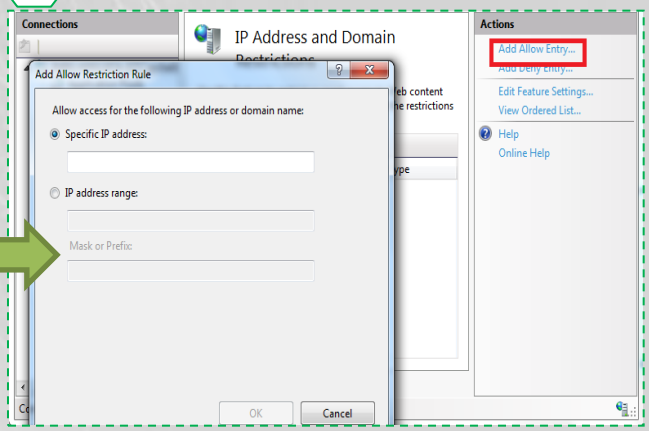
1



2



3



การรับมือสถานการณ์ภัยคุกคามที่เกิดจากการโจมตีเว็บไซต์ (Incident Handling)

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)

การใช้โปรแกรมตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์

- เลือกโปรแกรมที่น่าเชื่อถือ หรือ ได้รับการแนะนำจากหน่วยงานที่เกี่ยวข้อง พร้อมกับตรวจสอบและอัปเดตโปรแกรมให้เป็นเวอร์ชั่นล่าสุดเสมอ
- สำรองข้อมูลทุกครั้งก่อนมีการใช้โปรแกรมตรวจสอบ
- ใช้โปรแกรมมากกว่าสองโปรแกรมขึ้นไปในการตรวจสอบเพื่อเปรียบเทียบผลลัพธ์ที่ได้

โปรแกรมตรวจสอบความมั่นคงปลอดภัยที่ได้รับคำแนะนำจาก OWASP เช่น Acunetix Web Vulnerability Scanner หรือ Vega

acunetix
WEB APPLICATION SECURITY

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

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

การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

มีการบันทึกข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลการใช้งานของผู้ใช้ (Log) ที่เป็นไปตาม

- ข้อกำหนดในพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550

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

- ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า เก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์

<u>หัวข้อตาม Checklist ที่เกี่ยวข้อง</u> : 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)

Q & A

ติดต่อ สอบถามข้อมูลเพิ่มเติม

สำนักมาตรฐาน

เว็บไซต์: https://standard.etda.or.th

อีเมล: osd@etda.or.th

Thank You

ETDA

สพธอ

www.etda.or.th