

แบบบันทึกการแลกเปลี่ยนเรียนรู้ (KM)
เรื่อง WordPress Security
ของชุมชนนักปฏิบัติเทคโนโลยีสารสนเทศ
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
วันที่ ๓ พฤษภาคม ๒๕๖๒ เวลา ๐๙.๓๐ - ๑๒.๓๐

รายชื่อสมาชิก

คุณเอื้อ นายธนาวุฒิ นิลมณี
คุณอำนวย นางสาวเพชรภรณ์ เพ็ชรแก้ว
คุณกิจ นายปาโมกษ์ รัตนธัญญาภิบาล
คุณประสาน นายพนนรร์จ เนตรสกุลณี

สมาชิกในกลุ่ม

นางสาวเพชรภรณ์ เพ็ชรแก้ว
นายปาโมกษ์ รัตนธัญญาภิบาล
นายพนนรร์จ เนตรสกุลณี
น.ส.ศฤงญา แก้วขิม
นายฉัตรชัย ทองศิลป์

ผู้เล่า	รายละเอียดของเรื่อง	สรุปความรู้ที่ได้
นายปาโมกษ์ รัตนธัญญาภิบาล	การรักษาความปลอดภัย เว็บไซต์ โดยใช้ WordPress Security และ WPS Hide Login	ปัญหาการรักษาความปลอดภัยเว็บไซต์ คือ ขาดความปลอดภัย (โดน hack, แอบแทรกข้อมูล), เว็บ ล่ม, เว็บที่ตายไปแล้ว (มีเว็บเยอะ แต่ไม่มีคนดูแล) และอื่น ๆ ทำไมถึงโดน Hack เพราะเว็บไซต์เราอยู่บน Internet ทุกคนสามารถเข้าถึงได้ , WordPress เป็น Software ที่คนใช้เยอะ = เป็นเป้าใน การโจมตีเยอะ, WordPress ไม่ได้มีแค่ WordPress แต่ ยังมี Theme และ Plugin ที่ใคร ๆ ก็เขียนได้ และนำไป

ผู้เล่า	รายละเอียดของเรื่อง	สรุปความรู้ที่ได้
		<p>แจกจ่ายได้ ยิ่งติดตั้งเยอะ โอกาสเสี่ยงก็เยอะ, เมื่อมีการ Update Version แล้วไม่ได้ Update ตาม ช่องโหว่ เลย ไม่ถูกแก้ไข</p> <p>อาการโดน Hack มีอะไรบ้าง / ตรวจสอบได้ไหม</p> <p>มี Post หรือ Page แปลกปลอม หรือโฆษณา แทรกเข้ามา, Post หรือ Page เดิม ถูกเปลี่ยนแปลง หรือถูกแทรก Script, มี User แปลกปลอม, เว็บไซต์ ช้า ล่มบ่อย ๆ (ถูกแทรก Script แปลกปลอม), สามารถ Scan ได้ด้วย Plugin Wordfence Security</p> <p>Wordfence Security</p> <p>ช่วยป้องกัน WordPress ให้ปลอดภัย เช่น block การ Login ผิดบ่อย, ตรวจสอบความแข็งแรงของ Password (ความยาก, ต้องไม่ง่ายเกินไป), คอย Scan หาความผิดปกติของเว็บไซต์ เช่น ไม่ได้ Update, โดน hack, โดนแก้ไข Code, ในการติดตั้งครั้งแรก จะต้องสร้าง folder wflogs และปรับสิทธิตามที่ Plugin กำหนด</p> <p>WPS Hide Login</p> <p>เป็นการซ่อน URL Login ทำให้ผู้ที่โจรมติ หาเป้าโจมตี ไม่เจอ โดยผู้ดูแลเว็บไซต์ต้องตกลงร่วมกันว่า จะเปลี่ยนหน้า login ไปเป็น URL อะไร</p>