รายงานสหกิจศึกษาฉบับสมบูรณ์

เว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่

Vulnerable Monitoring System

ศุภนัฐ เสนเนียม

SUPANUT SENNIUM

ภาควิชาวิศวกรรมคอมพิวเตอร์ สาขาวิชาวิศวกรรมสารสนเทศ

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2561

รายงานสหกิจศึกษาฉบับสมบูรณ์

เว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่

Vulnerable Monitoring System

ศุภนัฐ เสนเนียม

SUPANUT SENNIUM

ภาควิชาวิศวกรรมคอมพิวเตอร์ สาขาวิชาวิศวกรรมสารสนเทศ

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2561

ชื่อโครงงานสหกิจศึกษา	เว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่
ชื่อ-สกุลนักศึกษา	นายศุภนัฐ เสนเนียม
คณะ วิศวกรรมศาสตร์	**ภาควิชา** วิศวกรรมคอมพิวเตอร์ **สาขาวิชา** วิศวกรรมสารสนเทศ
ชื่อ-สกุล อาจารย์นิเทศน์	ผศ.ดร.สุธีรา พันธุ์ธีรานุรักษ์
ชื่อ-สกุล ผู้นิเทศน์งาน	คุณ กาญจนา ลิ้มวัฒนาชัย
ชื่อสถานประกอบการ	บริษัท เอก-ชัย ดีสทริบิวชั่น ซิสเทม จำกัด

บทคัดย่อ

ในปัจจุบันนี้ทางเทสโก้ โลตัส ได้มีการพัฒนาเว็บไซต์ออกมาในรูปแบบต่าง ๆ เพื่อเข้ามาช่วยในการทำงาน ช่วยในการประชาสัมพันธ์ข้อมูลข่าวสารต่าง ๆ ใช้ในการจำหน่ายสินค้าออนไลน์ รวมถึงใช้เป็นสื่อกลางเพื่อทำการติดต่อสื่อสารแลกเปลี่ยนข้อมูลระหว่างกัน ซึ่งในแต่ละเว็บไซต์นั้นล้วนเป็นข้อมูลที่สำคัญต่อองค์กร แต่ในทุกวันนี้ช่องโหว่จากเว็บไซต์นั้นมีจำนวนมาก ทำให้ง่ายต่อการโจรกรรมข้อมูลผ่านทางเว็บไซต์ และยากต่อการป้องกัน ทางองค์กรจึงได้มีโครงการที่จะจัดทำเว็บไซต์เพื่อรวบรวมและติดตามผลการแก้ไขช่องโหว่ (Vulnerable Monitoring System) เพื่อใช้เป็นศูนย์รวมในการจัดเก็บรายละเอียด และเป็นศูนย์รวมในการติดต่อเพื่อทำการแก้ไขช่องโหว่ที่ตรวจพบ โดยเว็บไซต์นี้จะช่วยแก้ปัญหาเรื่องความล่าช้าติดต่อกันระหว่างทีม และยังสามารถช่วยลดโอกาสในการถูกโจรกรรมข้อมูลขององค์กรได้เช่นกัน

Co-operative Title	Vulnerable Monitoring System
Student Intern Name	Supanut Sennium
Faculty Engineering	**Department** Computer Engineering **Major** Information Engineering
Advisor Name	Asst.Prof. Dr. Sutheera Puntheeranurak
Mentor Name	Kanchana Limwattanachai
Company	Ek-Chai Distribution System Co., Ltd

ABSTRACT

At present, Tesco Lotus has developed websites in various forms to help publicize information, use for online shopping and intermediary communication, and exchange information. Each site shows all the vital information for the organization, but there are a lot of vulnerabilities. Stealing data from the website is secure. For prevent the problem, the organization does a project to create a system to keep and monitor the results of the vulnerability issue. The system is called "Vulnerable Monitoring System" to use as a center for storing details and resolving the vulnerabilities detected. This system can decrease delayto contact between teams and can also reduce the chances of theft of corporate data as well.

กิตติกรรมประกาศ

ข้าพเจ้าได้รับผิดชอบและปฏิบัติหน้าที่ในบริษัท เอก-ชัย ดีสทริบิวชั่น ซิสเทม จำกัด ระหว่างวันที่ 1 มิถุนายน ถึงวันที่ 23 พฤศจิกายน พ.ศ.2561 ในโครงงานวิชาสหกิจศึกษาที่ทางคณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง และบริษัทฯ ร่วมมือกันจัดตั้งขึ้นในหัวข้อโครงงาน เว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่ซึ่งข้าพเจ้าได้รับความรู้ความเข้าใจและประสบการณ์ในการทำงานที่เป็นประโยชน์อย่างมาก อีกทั้งการดูแลและการช่วยเหลือต่าง ๆ ตลอดเวลาการทำงานโดยการปฏิบัติงานสหกิจศึกษาในครั้งนี้สำเร็จลุล่วงได้ เพราะมีการชี้แนะและได้รับความร่วมมือจากบุคคลต่าง ๆ ดังต่อไปนี้

พนักงานทีม Security Capability & Planning

- คุณ อุบลรัตน์ ปรีดาวัฒน์
- คุณ กาญจนา ลิ้มวัฒนาชัย
- คุณ วัชรินทร์ บูรพาอารยวงศ์
- คุณ กนก พูลเกษม
- คุณ ชาญณรงค์ ถ้วยแก้ว
- คุณ นพรัตน์ บุษบารัตน์
- คุณ นิพา พิมพ์เพ็ง

พนักงานแผนกทรัพยากรบุคคล

- คุณ วิชชุดา หัสรินทร์

และข้าพเจ้าขอขอบคุณอาจารย์ที่ปรึกษา ผศ.ดร.สุธีรา พัทธุ์ธีรานุรักษ์ ที่คอยให้คำแนะนำ คำปรึกษา คอยรับฟัง ช่วยเหลือปัญหาต่าง ๆ ในการทำโครงงานครั้งนี้ และท้ายที่สุดข้าพเจ้าขอขอบคุณครอบครัว เพื่อนนักศึกษาที่คอยให้กำลังใจที่ดีแก่ข้าพเจ้าเสมอมาทำให้ปริญญานิพนธ์ฉบับนี้ให้สำเร็จลุล่วงไปได้ด้วยดี

ศุภนัฐ เสนเนียม

สารบัญ

หน้า

สารบัญรูปภาพ

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญ

เนื่องจาก บริษัท เอก-ชัย ดีสทริบิวชั่น ซิสเทม จำกัด ได้จัดโครงงานสหกิจศึกษาระหว่างบริษัท เอก-ชัย ดีสทริบิวชั่น ซิสเทม จำกัด กับ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง โดยในส่วนงานของแผนกไอที หรืออินฟอเมชันเทคโนโลยี (Information Technology) ทีมรักษาความปลอดภัยและการวางแผนภายในองค์กร (Security Capability & Planning) หรือทีมรักษาความปลอดภัยของเทคโนโลยีสารสนเทศ (IT Security) มีโครงการที่จะจัดทำเว็บแอปพลิเคชัน (Web Application) เพื่อรวบรวมและติดตามผลการแก้ไขช่องโหว่ (Vulnerability) ที่เกิดขึ้นภายในองค์กร เนื่องจากเว็บไซต์และเว็บแอปพลิเคชันที่ใช้ภายในองค์กรมีจำนวนมาก รวมถึงการติดต่อเพื่อแก้ไขหรือปิดช่องโหว่ที่เกิดขึ้นกับผู้ดูแลเว็บไซต์นั้น ๆ ทำได้ยาก จึงได้มีการมอบหมายงานให้นักศึกษาออกแบบเว็บแอปพลิเคชันเพื่อให้ง่ายต่อการติดตามผลการแก้ไขแต่ละช่องโหว่ที่เกิดขึ้น และเก็บรวบรวมข้อมูลรายละเอียดต่าง ๆ ที่เป็นองค์ประกอบเพื่อใช้สำหรับพัฒนาเว็บแอปพลิเคชันให้มีความสมบูรณ์

1.2 วัตถุประสงค์ของการปฏิบัติงาน

เนื่องจากในทีมทีมรักษาความปลอดภัยของเทคโนโลยีสารสนเทศ (Security Capability & Planning หรือ IT Security) ได้มีการจัดทำเว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่ (Vulnerable Monitoring System) เพื่อนำมาใช้งานแทนการทำงานในรูปแบบเดิมที่เคยใช้งานอดีต โดยมีวัตถุประสงค์ดังนี้

1. เพื่อใช้ในการเก็บรวบรวมรายละเอียดของช่องโหว่ที่ตรวจพบจากเว็บไซต์และเว็บแอปพลิเคชันที่ใช้งานภายในองค์กร
2. เพื่อแก้ไขปัญหาช่องโหว่ที่ตรวจพบจำนวนมากให้มีการจัดการในเว็บแอปพลิเคชันที่เป็นศูนย์กลางพร้อมแนวทางการป้องกันเมื่อตรวจพบช่องโหว่ไม่ให้เกิดการโจรกรรมข้อมูลผ่านเว็บไซต์หรือเว็บแอปพลิเคชันขององค์กรได้
3. เพื่อทราบว่าแต่ละเว็บไซต์และเว็บแอปพลิเคชันมีช่องโหว่ประเภทใดเกิดขึ้น และความเสี่ยงที่ส่งผลต่อเว็บไซต์และเว็บแอปพลิเคชันอยู่ในระดับใด
4. เพื่อเก็บรายละเอียดของตัวเว็บไซต์และเว็บแอปพลิเคชันเองว่าช่องโหว่เกิดขึ้นนั้นทีมใดเป็นผู้ดูแลเว็บไซต์หรือเว็บแอปพลิเคชันนั้น ๆ อยู่มีการใช้งานอยู่ในแผนกใดภายในองค์กร

1.3 วิธีการดำเนินงาน

1. การศึกษาข้อมูลและจุดประสงค์ที่จะนำมาใช้พัฒนาเว็บแอปพลิเคชัน

- ศึกษาเกี่ยวกับปัญหาที่มา และความสำคัญที่ทำให้เกิดเป็นโปรเจคนี้ขึ้น พร้อมแนวทางการพัฒนาโปรเจคจากปัญหาเดิมที่มีอยู่
- ศึกษาเกี่ยวกับประเภทของช่องโหว่ตามมาตรฐานโอดับบลิวเอเอสพี (Open Web Application Security Project: OWASP) ซึ่งเป็นมาตรฐานสากลในด้านความปลอดภัยของเว็บแอปพลิเคชัน (Web Application Security) เพื่อให้เข้าใจถึงความหมาย และรูปแบบของการเกิดช่องโหว่
- ศึกษาโปรแกรมและภาษาของโปรแกรมที่จะนำใช้พัฒนาเว็บแอปพลิเคชัน
- ศึกษากระบวนการเมื่อตรวจพบช่องโหว่จากการใช้เครื่องมือ (Tools) ตรวจหาช่องโหว่จากเว็บไซต์หรือเว็บแอปพลิเคชันภายในองค์กร

2. การออกแบบและจัดเตรียมข้อมูลที่จะนำมาใช้พัฒนาเว็บแอปพลิเคชัน

3. การพัฒนาเว็บแอปพลิเคชัน

4. การทดสอบระบบและแก้ไขข้อผิดพลาดที่ตรวจพบ

5. การเผยแพร่เว็บแอปพลิเคชัน

6. การดูแลและบำรุงรักษาเว็บแอปพลิเคชัน

1.4 ขอบเขตของงาน

1. เว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่จะมีการเก็บข้อมูลเฉพาะเว็บไซต์และเว็บแอปพลิเคชันของเทสโก้ โลตัส (Tesco Lotus) ที่อยู่ในทวีปเอเชีย (Asia) เท่านั้น
2. เว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่จะมีการให้เข้าใช้งานในปัจจุบันเฉพาะในแผนกไอที (Information Technology: IT)
3. การกำหนดสิทธิ์การเข้าใช้งานของเว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่
   - กำหนดสิทธิ์ระหว่างผู้ดูแลเว็บแอปพลิเคชัน (Admin) กับผู้เข้าใช้งาน (User) ให้มีการเข้าถึงเว็บแอปพลิเคชันที่แตกต่างกัน
   - ผู้ดูแลเว็บแอปพลิเคชันสามารถเข้าดูรายละเอียดทั้งหมดของทุกเว็บไซต์และเว็บแอปพลิเคชันที่เกิดช่องโหว่ได้ สามารถสร้างบัญชีผู้ใช้ให้กับผู้เข้าใช้งานเว็บแอปพลิเคชันใหม่ได้ โดยสามารถกำหนดได้ว่าบัญชีผู้เข้าใช้งานเว็บแอปพลิเคชันใหม่นั้นตั้งค่าให้เป็นผู้ดูแลเว็บแอปพลิเคชันหรือเป็นเพียงผู้เข้าใช้งานเว็บเว็บแอปพลิเคชันได้

- ผู้เข้าใช้งานสามารถดูรายละเอียดของช่องโหว่เฉพาะเว็บไซต์หรือเว็บแอปพลิเคชันที่ตนเป็นผู้ดูแลเท่านั้น ไม่สามารถเข้าดูรายละเอียดของเว็บไซต์หรือเว็บแอปพลิเคชันที่ตนไม่ได้รับผิดชอบได้

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. ทำให้ในแผนกไอทีมีศูนย์กลางในการเก็บข้อมูลและตรวจสอบดูรายละเอียด ทำให้ง่ายต่อการติดต่อสื่อสารระหว่างทีมทีมรักษาความปลอดภัยของเทคโนโลยีสารสนเทศกับทีมของผู้ดูแลเว็บไซต์หรือเว็บแอปพลิเคชันที่เกิดช่องโหว่ขึ้น

2. ทีมทีมรักษาความปลอดภัยของเทคโนโลยีสารสนเทศสามารถแก้ไขหรือปิดช่องโหว่ที่เกิดขึ้นได้รวดเร็วยิ่งขึ้น

3. นักศึกษาได้รับประสบการณ์และความเข้าใจเกี่ยวกับงานทีมรักษาความปลอดภัยของเทคโนโลยีสารสนเทศมากขึ้น

4. นักศึกษาได้รับความรู้เรื่องการใช้โปรแกรม และภาษาทางโปรแกรมเพื่อใช้ในการพัฒนาเว็บไซต์

5. นักศึกษาได้รับประสบการณ์จากการทำงานจริง เพื่อที่จะนำไปใช้ต่อยอดในอนาคตได้

6. นักศึกษาได้รู้จักกับการแก้ปัญหาต่าง ๆ ที่เกิดขึ้นได้ด้วยตัวเอง

บทที่ 2

ทบทวนวรรณกรรม

2.1 กระบวนการพัฒนาเว็บไซต์

การที่จะสร้างพัฒนาเว็บไซต์ และนำเว็บไซต์ที่พัฒนาได้นั้นเข้าสู่ระบบเวิลด์ไวด์เว็บ (World Wide Web) ที่ใช้งานอยู่บนเว็บเบราว์เซอร์ (Web Browser) ต่าง ๆ ให้ผู้อื่นสามารถเข้ามาเยี่ยมชม และใช้งานได้นั้น มีหลักการออกแบบ และแบ่งออกเป็นขั้นตอนต่าง ๆ เพื่อใช้เป็นแนวทางสำหรับผู้เริ่มพัฒนาเว็บไซต์ในการสร้างและพัฒนาเว็บไซต์ให้มีความสมบูรณ์ ดังนี้

2.1.1 การวางแผน

ในขั้นตอนแรกก่อนที่จะลงมือพัฒนาเว็บไซต์ออกมาเผยแพร่เปิดให้ใช้งานได้นั้นต้องมีการวางแผนที่ดีก่อน เพื่อจะเป็นสิ่งที่ไว้กำหนดแนวทางในการปฏิบัติงาน ว่าเว็บไซต์นั้นควรมีขอบเขตของการพัฒนามากน้อยเพียงใด ซึ่งประกอบไปด้วยขั้นตอนต่าง ๆ ดังนี้

2.1.1.1 การกำหนดเนื้อหาและจุดประสงค์ของเว็บไซต์

ขั้นตอนแรกของการวางแผน คือ การกำหนดเนื้อหาและจุดประสงค์ของเว็บต์ว่าเนื้อหาที่จะนำไปแสดงให้ผู้เข้าชมเว็บไซต์ได้เห็นนั้น ผู้พัฒนาเว็บไซต์ (Developer) ต้องการนำเสนอข้อมูลแบบใด เว็บไซต์นี้มีไว้สำหรับการใช้งานประเภทใด เช่น เว็บไซต์ที่ใช้สำหรับซื้อขายสินค้าออนไลน์ เว็บไซต์ประชาสัมพันธ์ เว็บไซต์โรงเรียน เป็นต้น จะเห็นได้ว่าเว็บไซต์จุดประสงค์การใช้งานของแต่ละเว็บไซต์นั้นมีความต่างกัน ขั้นตอนนี้จึงเป็นขั้นตอนสำคัญสำหรับการเริ่มพัฒนาเว็บไซต์ และจะเป็นตัวกำหนดหน้าตา โครงสร้างเว็บไซต์ของผู้พัฒนาเองด้วย

2.1.1.2 การกำหนดกลุ่มเป้าหมาย

หลังจากการกำหนดเนื้อหาและจุดประสงค์แล้วผู้พัฒนาควรกำหนดกลุ่มเป้าหมายของเว็บไซต์ด้วย ว่าเว็บไซต์ที่พัฒนานั้นควรใช้งานกับกลุ่มเป้าหมายประเภทไหน เช่น เว็บไซต์ที่จะใช้งานในบริษัทกลุ่มเป้าหมายจะเป็นพนักงานภายในบริษัท เว็บไซต์โรงเรียนกลุ่มเป้าหมายจะเป็นอาจารย์และนักเรียน เพื่อให้เป็นที่สนใจและได้รับความนิยมต่อการใช้งานอย่างต่อเนื่อง

2.1.1.3 การเตรียมข้อมูล

การเตรียมข้อมูลเพื่อนำมาใส่ในตัวเว็บไซต์เพื่อให้เว็บไซต์มีความน่าสนใจเชิญชวนให้มีผู้อื่นเข้ามาเยี่ยมชม นั้นสิ่งแรกควรแบ่งประเภทข้อมูลที่เรามีออกเป็นหมวดหมู่ ทำการจัดลำดับว่าข้อมูลไหนมีความน่าสนใจ ข้อมูลไหนเป็นข้อมูลที่ล่าสุด เพื่อการจัดวางตำแหน่งให้มีความเหมาะสม และมีข้อควรระวัง คือ การนำข้อมูลมาสื่ออื่น เช่น หนังสือพิมพ์ เว็บไซต์ แมกกาซีน (Magazine) ควรขออนุญาตเจ้าของบทความก่อน เพื่อป้องกันเรื่องลิขสิทธิ์ด้วย หรือควรใส่อ้างอิงแหล่งที่มาไว้

2.1.1.4 การเตรียมสิ่งต่าง ๆ ที่จำเป็น

การจะพัฒนาออกมาเป็นเว็บไซต์ที่สามารถใช้งานได้นั้นจำเป็นต้องอาศัยหลาย ๆ ปัจจัย ได้แก่ โปรแกรมสำหรับพัฒนาเว็บไซต์ เครื่องมือ รูปภาพ สื่อมัลติมีเดีย (Multimedia) ต่าง ๆ รวมถึงผู้ให้บริการรับฝากเว็บไซต์ (Web Hosting) การจดชื่อโดเมน (Domain Name) ของเว็บไซต์ และรวมถึง 3 ปัจจัยหลัก ๆ ดังนี้

1. ระยะเวลาในการพัฒนาเว็บไซต์เป็นการกำหนดช่วงเวลาที่จะใช้ในการพัฒนาเว็บไซต์ ให้มีระยะเวลาที่มีความเหมาะสมกับเนื้องานที่ผู้พัฒนาต้องใช้ในการสร้างเว็บไซต์
2. งบประมาณเป็นการกำหนดค่าใช้จ่ายที่ใช้ในการพัฒนาเว็บไซต์
3. ปัญหาและอุปสรรคเป็นส่วนหนึ่งของขั้นตอนการวางแผน เพื่อเตรียมรับมือกับปัญหาและอุปสรรคที่อาจจะเกิดขึ้นได้ ซึ่งจะเป็นสิ่งที่เพิ่มระยะเวลาในการพัฒนาเว็บไซต์

2.1.1.5 การจัดโครงสร้างข้อมูล

เมื่อทำการรวบรวมข้อมูลต่าง ๆ ที่จำเป็นต่อการพัฒนาเว็บไซต์เรียบร้อยแล้ว ในขั้นตอนนี้ ผู้พัฒนาเว็บไซต์ต้องทำการจัดระบบเพื่อใช้เป็นกรอบสำหรับการออกแบบและดำเนินการในขั้นตอนต่อไป ซึ่งมีรายละเอียด ดังนี้

- การจัดโครงสร้างและสารบัญของเว็บไซต์
- การใช้ระบบนำผู้เข้าชมเว็บไซต์ไปยังส่วนต่าง ๆ ภายในเว็บไซต์ เรียกว่า ระบบนำทาง (Navigation)
- องค์ประกอบที่ต้องนำมาใช้ เช่น สื่อมัลติมีเดีย ภาพกราฟิก (Graphic) แบบฟอร์ม ต่าง ๆ

- การกำหนดรูปแบบ และลักษณะของตัวเว็บไซต์

- การกำหนดฐานข้อมูล ภาษาสคริปต์ (Script) หรือแอปพลิเคชัน (Application) ที่นำมาใช้ในเว็บไซต์

- การออกแบบเว็บไซต์ ว่าควรออกแบบรูปร่างโครงสร้างของเว็บไซต์อย่างไร ควรกำหนดโครงร่างว่ามีทั้งหมดกี่เว็บเพจ (Web Page) แต่ละเว็บเพจมีเนื้อหาอะไรบ้าง และลักษณะทางด้านกราฟิกของหน้าเว็บเพจ และองค์ประกอบต่าง ๆ เช่น ชื่อเว็บไซต์ โลโก้ รูปไอคอน ปุ่มไอคอน ภาพเคลื่อนไหว โฆษณา เป็นต้น

- การกำหนดสีสันและรูปแบบของส่วนประกอบต่าง ๆ ที่ไม่ใช่ภาพกราฟิก เช่น ขนาดของตัวอักษร สีของข้อความ สีพื้น ลวดลายของเส้นกรอบเพื่อความสวยงามและดึงดูดผู้เยี่ยมชมเว็บไซต์ด้วย

- การเลือกเว็บเบราว์เซอร์สำหรับแสดงผลเว็บไซต์เพื่อสะดวกต่อการกำหนดขนาดกว้าง ยาว และลักษณะการวางองค์ประกอบเว็บให้สวยงามและแสดงผลได้เร็ว

- ออกแบบหน้าตาเว็บเป็นขั้นตอนในการลงมือสร้างเว็บเพจแต่ละหน้าตามที่ได้ออกแบบไว้ พร้อมกับทดสอบผ่านเว็บเบราว์เซอร์แบบจำลองก่อนการนำไปใช้งานจริง

2.1.2 เทคนิคการออกแบบเว็บไซต์

เทคนิคการออกแบบเว็บไซต์นอกจากจะทำให้เว็บไซต์ผู้พัฒนามีความน่าสนใจแล้วยังสามารถใช้เป็นตัวแบ่งประเภทการออกแบบเว็บไซต์ได้อีกด้วยโดยสามารถแบ่งเทคนิคการออกแบบเว็บไซต์เป็น 3 ส่วน คือ

1. ออกแบบเว็บไซต์ที่เน้นเนื้อหา

เว็บไซต์บางประเภทจะเน้นเนื้อหา หรือ ข้อความเป็นหลัก ภายในเว็บไซต์จะประกอบด้วยตัวหนังสือเป็นส่วนใหญ่ขององค์ประกอบ และมีภาพประกอบเป็นส่วนน้อย

2. ออกแบบเว็บไซต์ที่เน้นภาพกราฟิก

เว็บไซต์ชนิดนี้จะเป็นภาพหรือกราฟิกในการนำเสนอเรื่องราว ส่วนข้อความตัวอักษรอาจมีเป็นส่วนประกอบบ้างเล็กน้อย

3. ออกแบบเว็บไซต์ที่เน้นทั้งภาพและเนื้อหา

เว็บไซต์ประเภทนี้จะประกอบด้วยข้อความและรูปภาพในสัดส่วนที่เท่า ๆ กัน

ส่วนประกอบของหน้าเว็บเพจ

ส่วนประกอบของหน้าเว็บเพจที่ใช้สำหรับเทคนิคการออกแบบเว็บไซต์นั้นจะสามารถจำแนกส่วนประกอบออกเป็น 3 ส่วน ดังนี้

1) ส่วนหัว (Page Header) โดยส่วนมากจะตั้งอยู่บริเวณบนสุดของหน้าเว็บเพจ หรือแล้วแต่การออกแบบของผู้พัฒนา เป็นส่วนที่แสดงชื่อเว็บไซต์ โลโก้ (Logo) โฆษณา และลิงก์ (Link) สำหรับข้ามไปยังหน้าเว็บอื่น

2) ส่วนเนื้อหา (Page Body) จะอยู่บริเวณส่วนกลางของหน้าเว็บเพจ ซึ่งเป็นส่วนที่แสดงเนื้อหาภายในหน้าเว็บเพจนั้น โดยประกอบด้วยข้อความ ข้อมูล ภาพเคลื่อนไหว กราฟ ตาราง เป็นต้น

3) ส่วนท้าย (Page Footer) จะอยู่บริเวณด้านล่างสุดของหน้าเว็บเพจ ส่วนมากใช้สำหรับลิงก์ข้อความสั้น ๆ เข้าใจง่าย หรือชื่อเจ้าของเว็บไซต์ ที่อยู่อีเมล (E-mail address) ของผู้ดูแลเว็บไซต์สำหรับติดต่อกับทางเว็บไซต์

2.1.3 แนวคิดในการออกแบบเว็บไซต์

แนวคิดในการออกแบบเว็บไซต์นั้นเป็นส่วนหนึ่งที่จะทำให้เว็บไซต์ของผู้พัฒนาเว็บไซต์มีความน่าสนใจสามารถดึงดูดให้ผู้ใช้งานเข้ามาใช้งานได้โดยผู้พัฒนาสามารถเพิ่มจุดเด่นหรือทำการศึกษาและวิเคราะห์ความสนใจต่าง ๆ ของผู้ใช้งานได้ดังต่อไปนี้

1. ดูจากเว็บไซต์อื่นเพื่อเป็นตัวอย่าง

การจะพัฒนาเว็บไซต์นั้นควรมีการศึกษาจากเว็บไซต์อื่นเพื่อใช้เป็นตัวอย่างสำหรับการพัฒนา เพื่อช่วยสำหรับการนำไปประยุกต์ใช้ให้มีความเหมาะสมกับเนื้อหาและกลุ่มเป้าหมายของตัวเว็บไซต์

2. ศึกษาจากสื่อสิ่งพิมพ์ในรูปแบบต่าง ๆ

การศึกษาจากสื่อสิ่งพิมพ์ว่ามีการใช้รูปแบบอย่างไรให้มีความน่าสนใจ ดึงดูดกับผู้ที่เข้ามารับชม สามารถนำมาประยุกต์ใช้ในการออกแบบเว็บไซต์ได้เช่นกัน เช่น แมกกาซีน โปสเตอร์โฆษณา โบรชัวร์ (Brochure) หนังสือ เป็นต้น

2.1.4 ทดสอบและปรับปรุงเว็บไซต์

การทดสอบและปรับปรุงเว็บไซต์ในที่นี้ หมายถึง การทดสอบแบบออฟไลน์ โดยที่ยังไม่ได้นำเว็บไซต์เข้าสู่อินเทอร์เน็ต (Internet) แต่ก็สามารถแสดงผลได้เหมือนจริงผ่านเว็บเบราว์เซอร์ เช่น การใช้กูเกิลโครม (Google Chrome) เพื่อตรวจสอบตัวอย่างเว็บที่สร้างไว้ เช่น การตรวจสอบการแสดงผลของขนาดตัวอักษร ขนาดภาพ การใช้สี ตาราง กราฟ ว่ามีความเหมาะสมหรือไม่ พร้อมกับการทำการปรับปรุงจนเป็นที่น่าพอใจ

2.1.5 เผยแพร่ผ่านเว็บไซต์

เป็นการเผยแพร่เว็บไซต์ที่พัฒนาเสร็จสมบูรณ์แล้วให้คนทั่วไปได้รู้จัก หรือเรียกว่าการอัพโหลด (Upload) ลงเซิร์ฟเวอร์ (Server) โดยเจ้าของเว็บไซต์หรือผู้พัฒนานั้นจะต้องจดทะเบียนชื่อโดเมนและเช่าพื้นที่โฮสต์ ก่อนนำเว็บเพจอัพโหลดขึ้นสู่อินเทอร์เน็ต และประชาสัมพันธ์ให้คนทั่วไปได้รู้จัก ซึ่งการที่จะทำให้คนรับรู้ และเข้ามาใช้บริการเว็บไซต์ได้มากนั้นจะต้องมีการประชาสัมพันธ์อย่างต่อเนื่องและใช้เวลาพอสมควร และควรมีเคาน์เตอร์ (Counter) หรือตัวจดสถิติผู้เข้าชมเว็บไซต์ จะสามารถช่วยประเมินได้ว่าเว็บไซต์ที่พัฒนาขึ้นมานั้นได้รับความสนใจมากน้อยเพียงใด

2.1.6 การพัฒนาเว็บไซต์ให้มีความทันสมัย

หลังจากทำการเผยแพร่เว็บไซต์ที่พัฒนาเสร็จสมบูรณ์แล้ว ขั้นตอนการพัฒนาเว็บไซต์ให้มีความทันสมัยถือเป็นขั้นตอนสำคัญ เพราะ ในปัจจุบันนี้ข้อมูลที่ใช้งานบนอินเทอร์เน็ตนั้นมีการเปลี่ยนแปลงอย่างรวดเร็วอยู่ตลอดเวลา ดังนั้น ถ้าเว็บไซต์ที่พัฒนาเสร็จแล้วไม่มีการพัฒนาปรับปรุงเนื้อหาให้มีความทันสมัยหรือขาดการอัพเดท (Update) เว็บไซต์ ก็จะส่งผลให้จำนวนของผู้เข้าชมเว็บไซต์ลดลงเช่นกัน

ดังนั้นการปรับปรุงเว็บไซต์อย่างสม่ำเสมอ โดยเพิ่มข้อมูลข่าวสารใหม่ ๆ อยู่เป็นประจำก็จะทำให้เว็บไซต์ทันสมัย ทำให้ผู้เข้าชมเป็นประจำและมากขึ้นจนสามารถพัฒนาเป็นเว็บไซต์ยอดนิยมได้ในที่สุด

2.2 โปรแกรมที่ใช้พัฒนาเว็บไซต์

ในการพัฒนาเว็บไซต์นั้นการเลือกโปรแกรมที่จะนำมาใช้ในการพัฒนาเว็บไซต์ให้มีความสมบูรณ์ของผู้พัฒนานั้น เป็นส่วนช่วยให้มีการทำงานที่มีความสะดวกและรวดเร็วยิ่งขึ้นสามารถลดระยะของการพัฒนาเว็บไซต์ให้อยู่ในขอบเขตของการวางแผน อีกทั้งผู้พัฒนายังสามารถเลือกใช้โปรแกรมตามความถนัดของตัวเอง

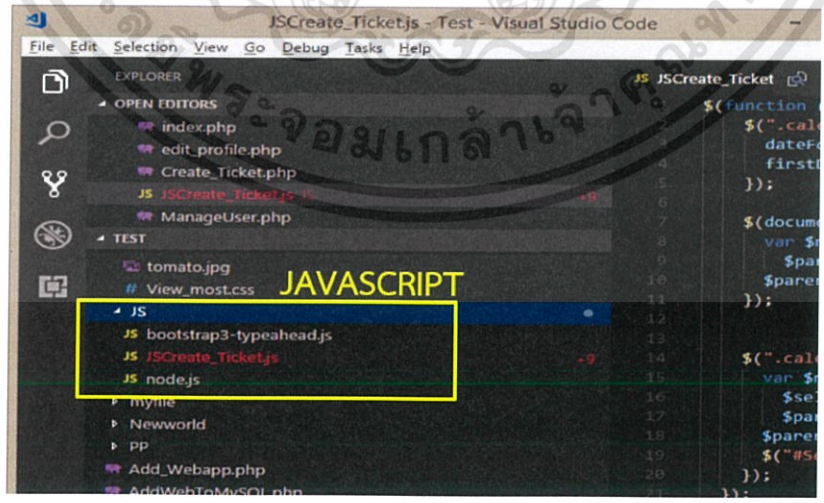
หรือสามารถเลือกใช้โปรแกรมที่เอื้ออำนวยต่อการนำไปปฏิบัติงานได้อีกด้วย โดยโปรแกรมที่ผู้พัฒนาเว็บไซต์เลือกใช้ในการพัฒนาโครงการมีดังนี้

2.2.1 โปรแกรมวิชวลสตูดิโอโค้ด (Visual Studio Code)

โปรแกรมวิชวลสตูดิโอโค้ด หรือ วีเอสโค้ด เป็นโปรแกรมโค้ดอิดิเตอร์ (Code Editor) ที่ใช้ในการเขียน การแก้ไขและปรับแต่งโค้ด (Code) จากไมโครซอฟท์ (Microsoft) มีการพัฒนาออกมาในรูปแบบของโอเพ่นซอร์ซ (Open Source) เปิดให้นักพัฒนาดาวน์โหลด (Download) นำมาใช้งานได้ฟรีโดยไม่เสียค่าใช้จ่าย เหมาะสำหรับผู้ที่ต้องการฝึกความเป็นมืออาชีพในด้านโปรแกรมเมอร์

อีกทั้ง โปรแกรมวิชวลสตูดิโอโค้ดนั้นเหมาะสำหรับนักพัฒนาโปรแกรมที่ต้องการใช้งานข้ามแพลตฟอร์ม และยังรองรับการใช้งานบนหลายระบบปฏิบัติการ วินโดว์ (Windows) แมคโอเอช (macOS) และ ลีนุกซ์ (Linux) อีกทั้งยังสนับสนุนทั้งภาษาจาวาสคริปต์ (JavaScript) ไทป์สคริปต์ (TypeScript) และโหนดดอทเจเอส (Node.js) ภาพแสดงการใช้งานจาวาสคริปต์บนโปรแกรมวิชวลสตูดิโอโค้ด แสดงดังภาพที่ 2.1 อีกทั้งยังสามารถนำมาใช้งานได้ง่ายไม่ซับซ้อน และมีเครื่องมือส่วนขยายต่าง ๆ ให้ใช้งานได้อย่างสมบูรณ์ ได้แก่

1. การเปิดใช้งานภาษาโปรแกรมอื่น ๆ ทั้ง ภาษา C++ C# Java Python PHP หรือ Go
2. ธีม (Themes)
3. ดีบักเกอร์ (Debugger)
4. คอมมานด์ (Commands)



ภาพที่ 2.1 การใช้งานจาวาสคริปต์บนโปรแกรมวิชวลสตูดิโอโค้ด (Visual Studio Code)

2.2.2 โปรแกรมเอ็กซ์เอเอ็มพีพี (XAMPP)

โปรแกรมที่มีไว้สำหรับจำลองเครื่องคอมพิวเตอร์เป็นเว็บเซิร์ฟเวอร์ (Web Server) เป็นโปรแกรมอาปาเช่เว็บเซิร์ฟเวอร์ (Apache Web Server) ทำหน้าที่จำลองเว็บเซิร์ฟเวอร์สำหรับการทดสอบสคริปต์หรือเว็บไซต์ที่กำลังพัฒนาในเครื่องของผู้พัฒนาก่อนจะนำลงเซิร์ฟเวอร์จริง โดยการจำลองเว็บเซิร์ฟเวอร์นี้ไม่จำเป็นต้องเชื่อมต่ออินเตอร์เน็ตและไม่ต้องเสียค่าใช้จ่ายใด ๆ อีกทั้งยังง่ายต่อการติดตั้ง และสะดวกต่อการใช้งาน

1. ระบบและภาษาที่ใช้ในการปฏิบัติการของโปรแกรมเอ็กซ์เอเอ็มพีพี

โปรแกรมเอ็กซ์เอเอ็มพีพีมีระบบและภาษาที่ใช้ในการปฏิบัติการต่าง ๆ ดังนี้

- ภาษาพีเอชพี (PHP) ภาษาที่ใช้สำหรับพัฒนาเว็บแอปลิเคชั่น
- ระบบมายเอสคิวแอล (MySQL) เพื่อใช้สำหรับการเรียกใช้ฐานข้อมูล
- อาปาเช่หน้าที่เป็นเว็บเซิร์ฟเวอร์
- ระบบโอเพ่นซอร์ซที่เปิดให้นักพัฒนาดาวน์โหลดและใช้งานได้ฟรี
- พีเอชพีมายแอดมิน (phpMyAdmin) ระบบบริหารฐานข้อมูลที่พัฒนาโดยภาษาพีเอชพีเพื่อใช้เชื่อมต่อไปยังฐานข้อมูล สนับสนุนฐานข้อมูลระบบมายเอสคิวแอล และเอชคิวไลต์ (SQLite)

2. ระบบปฏิบัติการของโปรแกรมเอ็กซ์เอเอ็มพีพี

โปรแกรมเอ็กซ์เอเอ็มพีพีสามารถใช้งานได้ 4 ระบบปฏิบัติการ ได้แก่

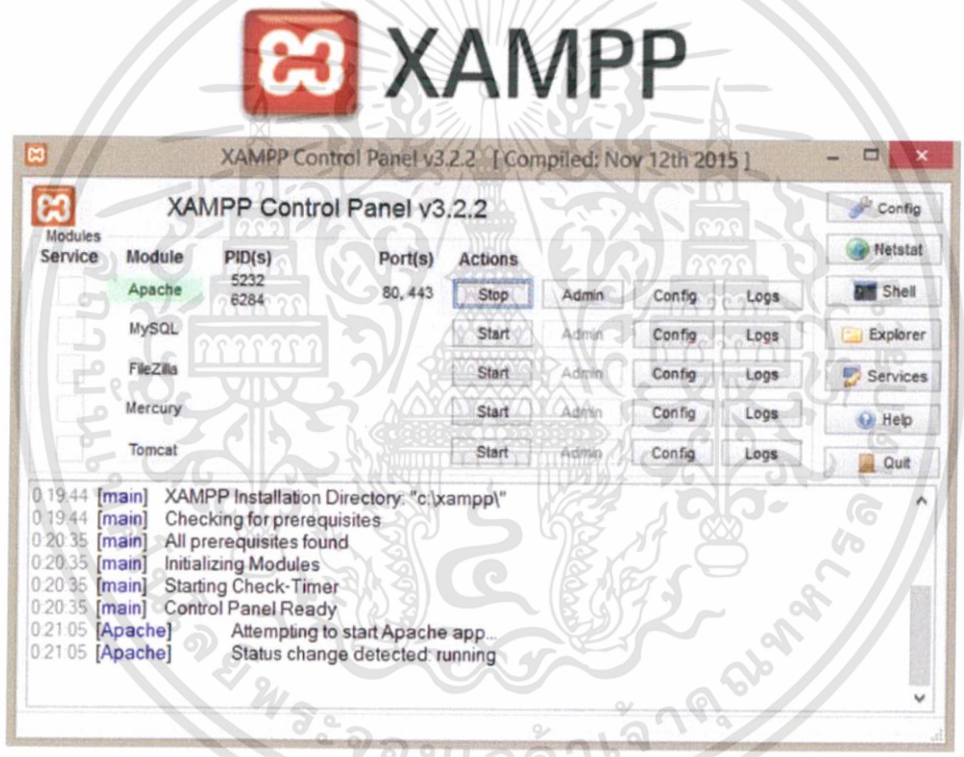
- สามารถใช้งานได้กับวินโดว์รุ่น 2000 วินโดว์รุ่น 2003 วินโดว์รุ่น xp วินโดว์รุ่น vista วินโดว์รุ่น 7 วินโดว์รุ่น 8 และวินโดว์รุ่น 10
- สามารถใช้งานได้กับลีนุกซ์สำหรับระบบการใช้งานภายในระดับองค์กรโดยเฉพาะ (SuSE Linux) ระบบการแบบซอฟต์แวร์โอเพ่นซอร์ส (RedHat) เป็นต้น
- สามารถใช้งานได้กับระบบปฏิบัติการแมคโอเอชเอ็ก (Mac OS X) ที่ถูกพัฒนาขึ้นโดยบริษัทแอปเปิ้ล (Apple Inc.) สำหรับใช้งานบนเครื่องคอมพิวเตอร์ตระกูลแมค (Mac OS)
- สามารถใช้งานได้กับระบบปฏิบัติการโซลาริส (Solaris) สำหรับ Solaris 8 และ Solaris 9

3. ข้อกำกัดด้านเทคนิคของโปรแกรมเอ็กซ์เอเอ็มพีพี

- เครื่องคอมพิวเตอร์ควรมีแรม (RAM) ไม่ต่ำกว่า 128 เมกะไบต์ (Megabyte)

- ฮาร์ดดิสก์ (Hard disk) มีพื้นที่มากกว่า 320 เมกะไบต์
- หน่วยประมวลผลกลาง (Central Processing Unit: CPU) ไม่กำหนดขั้นต่ำสำหรับการใช้งาน

ศูนย์กลางในการควบคุมของโปรแกรมเอ็กซ์เอเอ็มพีพี (XAMPP Control Panel) ในการเริ่มใช้งานนั้น ให้ทำการคลิกปุ่มเริ่มใช้งาน (Start) ของโปรแกรมอาปาเช่ (Apache) ต่อด้วยการสั่งให้โปรแกรมฐานข้อมูลทำงาน โดยคลิกปุ่มเริ่มใช้งานของมายเอสคิวแอล (MySQL) และยุติการทำงานของโปรแกรมสามารถทำได้โดยการคลิกปุ่มหยุดใช้งาน (Stop) การเข้าสู่หน้าเว็บทำได้โดยคลิกปุ่มแอดมิน (Admin) และการปรับแต่งระบบทำได้โดยคลิกปุ่มกำหนดค่า (Config) แสดงดังภาพที่ 2.2



ภาพที่ 2.2 ศูนย์กลางในการควบคุมของโปรแกรมเอ็กซ์เอเอ็มพีพี (XAMPP)

2.2.3 โปรแกรมพีเอชพีมายแอดมิน (phpMyAdmin)

โปรแกรมพีเอชพีมายแอดมิน คือ โปรแกรมที่ถูกพัฒนาโดยใช้ภาษาพีเอชพีเพื่อใช้ในการจัดการฐานข้อมูลมายเอสคิวแอลผ่านเว็บเบราว์เซอร์ โดยสามารถที่จะทำการสร้างฐานข้อมูลใหม่ หรือทำการสร้างตารางข้อมูลใหม่ และยังมีฟังก์ชั่นที่ใช้สำหรับการทดสอบการคิวรี่ (Query) อีกทั้งยังสามารถทำการเพิ่ม (Insert) ลบ (Delete) อัพเดท (Update) หรือแม้กระทั่งการใช้คำสั่งต่าง ๆ ได้เหมือนกับการใช้ภาษาเอสคิวแอ

ลในการสร้างตารางข้อมูล จึงสามารถใช้โปรแกรมนี้แทนการป้อนคำสั่งเอง เนื่องจากถ้าผู้ใช้งานจะเรียกใช้ฐานข้อมูลที่เป็นมายเอสคิวแอล บางครั้งจะเกิดความลำบากและยุ่งยากในการเรียกใช้งาน ดังนั้น พีเอชพีมายแอดมิน จึงมีเครื่องมือในการจัดการฐานข้อมูลจากระบบมายเอสคิวแอลขึ้นมาเพื่อให้สามารถจัดการกับระบบฐานข้อมูล (Database Management System: DBMS) ที่ทำงานได้ง่ายและสะดวกยิ่งขึ้นนั่นเอง กระบวนการทำงานของโปรแกรมพีเอชพีมายแอดมินแทนการป้อนคำสั่งเองจากมายเอสคิวแอลแสดงดังภาพที่ 2.3

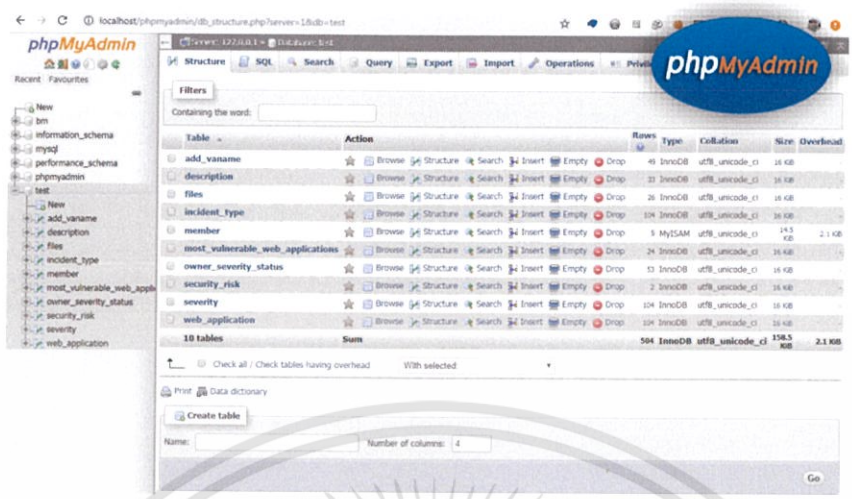
ภาพที่ 2.3 กระบวนการทำงานของโปรแกรมพีเอชพีมายแอดมินแทนการป้อนคำสั่งเองจากมายเอสคิวแอล

1. ความสามารถของโปรแกรมพีเอชพีมายแอดมิน

ความสามารถของโปรแกรมพีเอชพีมายแอดมิน ได้แก่

- สามารถสร้าง และลบฐานข้อมูล (Database) ทั้งหมดได้
- สามารถสร้าง และจัดการตารางข้อมูล (Table) เช่น การแทรก Record การลบ Record การแก้ไข Record การลบตารางข้อมูล และการแก้ไข Field เป็นต้น
- สามารถนำไฟล์จากภายนอกเข้าไปเก็บเป็นข้อมูลในตารางได้ เช่น ไฟล์นามสกุล CSV เป็นต้น
- สามารถหาผลสรุปการคิวรี่ข้อมูลด้วยการใช้คำสั่งเอสคิวแอลได้

ตัวอย่างของโปรแกรมพีเอชพีมายแอดมิน (phpMyAdmin) ที่ใช้เป็นฐานข้อมูลสำหรับการเรียกใช้งาน แสดงดังภาพที่ 2.4

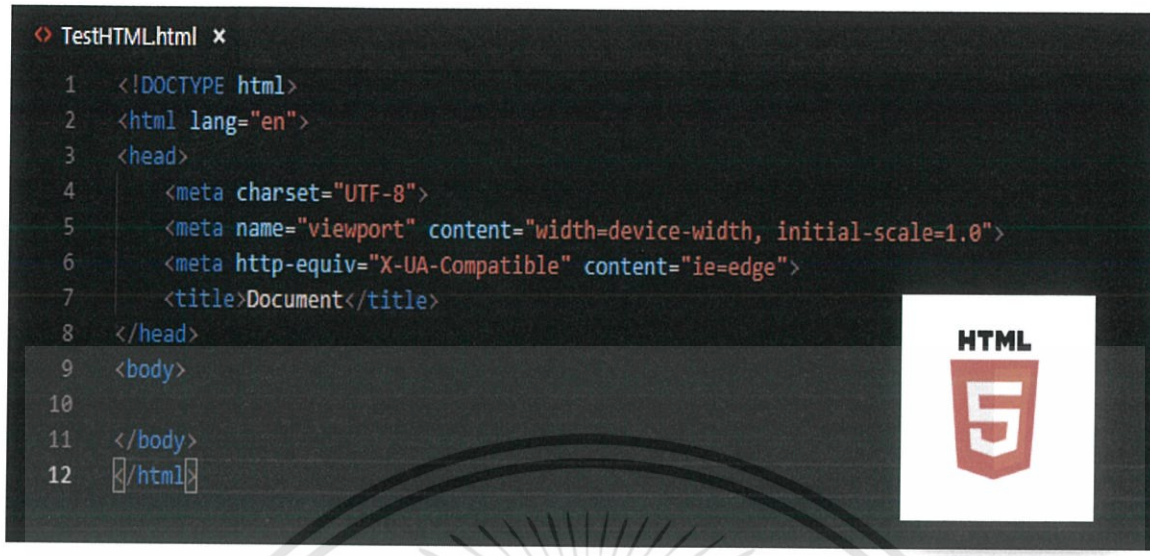


ภาพที่ 2.4 หน้าตาของโปรแกรมพีเอชพีมายแอดมิน (phpMyAdmin)

2.3 ภาษาทางโปรแกรมที่ใช้พัฒนาเว็บไซต์

2.3.1 ภาษาเอชทีเอ็มแอล (HTML)

ภาษาเอชทีเอ็มแอล หรือชื่อเต็ม เรียกว่า Hyper Text Markup Language เป็นภาษามาร์กอัป (Markup language) ทางคอมพิวเตอร์ที่ใช้ในการสร้าง และแสดงผลออกมาบนหน้าเว็บเพจหรือเรียกดูผ่านทางเว็บเบราว์เซอร์ได้ ถูกพัฒนา และกำหนดมาตรฐานโดยองค์กร World Wide Web Consortium (W3C) และพัฒนาทางด้านซอร์ฟแวร์ (Software) จากบริษัทไมโครซอฟ ภาษาเอชทีเอ็มแอลเป็นอีกภาษาหนึ่งที่ใช้เขียนโปรแกรม ซึ่งตัวโค้ดจะแสดงโครงสร้างของข้อมูล ในการแสดง หัวข้อ ลิงก์ ย่อหน้า รายการ รวมถึงการสร้างแบบฟอร์ม เชื่อมโยงภาพหรือวิดีโอด้วย โครงสร้างของโค้ดเอชทีเอ็มแอลจะอยู่ในลักษณะแท็กภายในวงเล็บสามเหลี่ยม (Tag HTML) สามารถทำโดยใช้โปรแกรมเทคอิดิเตอร์ (Text Editor) ต่าง ๆ เช่น Notepad Editplus หรือโปรแกรมที่เป็นเครื่องมือช่วยสร้างเว็บเพจ เช่น Microsoft FrontPage Dream Weaver ซึ่งจะช่วยอำนวยความสะดวกในการสร้างหน้าเอกสารเอชทีเอ็มแอล ส่วนการเรียกใช้งานหรือทดสอบการทำงานของเอกสาร เอชทีเอ็มแอลนั้น จะใช้โปรแกรมเว็บเบราเซอร์ในการเรียกดู เช่น Internet Explorer (IE) Mozilla Firefox Safari Opera และ Google Chrome เป็นต้น หน้าตาของแท็กภาษาเอชทีเอ็มแอลแสดงดังภาพที่ 2.5



ภาพที่ 2.5 หน้าตาของแท็กภาษาเอชทีเอ็มแอล (Tag HTML)

2.3.2 ภาษาพีเอชพี (PHP)

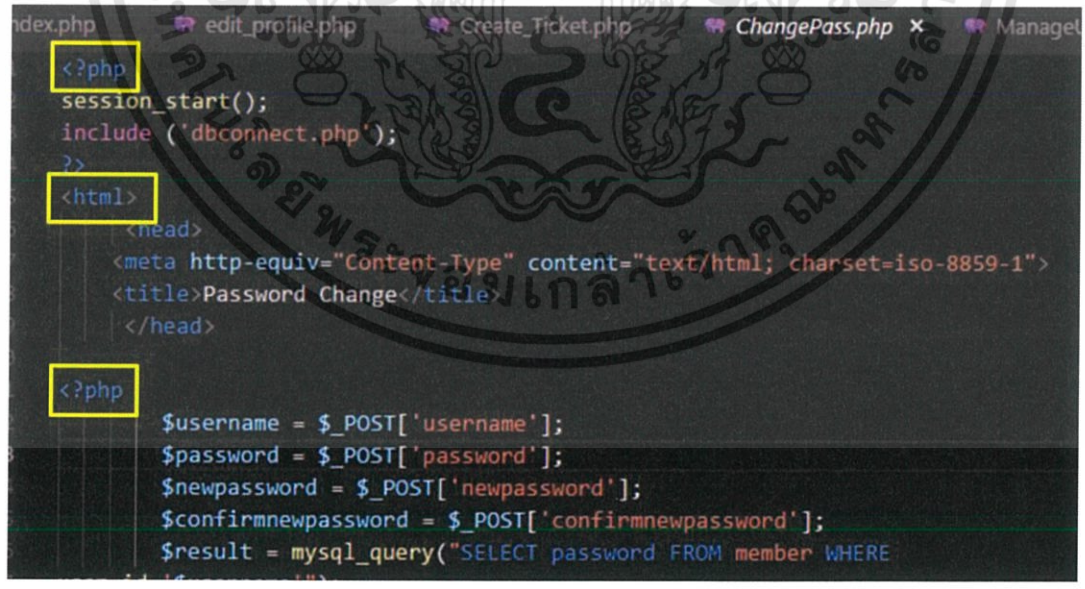
ภาษาพีเอชพี ย่อมาจาก PHP Hypertext Preprocessor ชื่อเดิมย่อมาจาก Personal Home Page Tools PHP ภาษาพีเอชพีเป็นภาษาคอมพิวเตอร์จำพวกภาษาสคริปต์ (scripting language) การเรียกใช้คำสั่งในการใช้งานต่าง ๆ จะเก็บอยู่ในไฟล์ที่เรียกว่า สคริปต์ และเมื่อต้องการเรียกใช้งานต้องอาศัยตัวแปรชุดคำสั่ง ตัวอย่างของภาษาสคริปต์ เช่น จาวาสคริปต์ เพิร์ค (Perl) เป็นต้น แต่ลักษณะของ ภาษาพีเอชพีนั้นแตกต่างจากภาษาสคริปต์แบบอื่น ๆ คือ ภาษาพีเอชพีได้รับการพัฒนาและออกแบบมา เพื่อใช้งานในการสร้างเอกสารแบบเอชทีเอ็มแอล โดยภาษาพีเอชพีนั้นสามารถเพิ่มหรือแก้ไขเข้าไปในเนื้อหาได้โดยอัตโนมัติ ดังนั้นภาษาพีเอชพีจึงเป็นภาษาที่เรียกว่า เซิร์ฟเวอร์-ไซด์ สคริปต์ (server – side script) หรือเรียกว่า HTML-embedded scripting language มีหลักการทำงาน คือ ก่อนการใช้งานเครื่องคอมพิวเตอร์ซึ่งให้บริการเป็นเว็บเซิร์ฟเวอร์จะทำหน้าที่ส่งหน้าเว็บเพจที่เขียนด้วยภาษาพีเอชพีให้ผู้ใช้งาน พร้อมทำการประมวลผลตามคำสั่งที่มีอยู่เสร็จเรียบร้อยก่อน แล้วจึงส่งผลลัพธ์ที่ได้ให้ผู้ใช้งานตามมา และผลลัพธ์ที่ได้นั้น คือ เว็บเพจที่ใช้งานนั่นเอง จึงถือได้ว่า ภาษาพีเอชพี เป็นเครื่องมือที่สำคัญชนิดหนึ่งที่ช่วยให้ผู้ใช้งานสามารถสร้างเว็บเพจที่มีการโต้ตอบกับผู้ใช้ (Dynamic Web pages) ได้อย่างมีประสิทธิภาพและมีลูกเล่นมากขึ้น

อีกทั้งภาษาพีเอชพีนั้นเปิดให้ใช้งานในรูปแบบของโอเพ่นซอร์ส ดังนั้น ภาษาพีเอชพีจึงมีการพัฒนาไปอย่างรวดเร็ว และเป็นที่แพร่หลายโดยเฉพาะอย่างยิ่งเมื่อใช้ร่วมกับ อาปาเช่เว็บเซิร์ฟเวอร์ ระบบปฏิบัติอย่าง เช่น ลีนุกซ์ หรือ ฟรีบีเอสดี (FreeBSD) เป็นต้น

1. ลักษณะเด่นของภาษาพีเอชพี

- เปิดใช้งานในรูปแบบของโอเพ่นซอร์สสามารถใช้งานได้ฟรี
- ภาษาพีเอชพีเป็นโปรแกรมทำงานไปพร้อมกับเซิร์ฟเวอร์ ดังนั้นขีดความสามารถในการทำงานจึงไม่จำกัด
- ภาษาพีเอชพีสามารถทำงานบนระบบปฏิบัติการแบบ UNIX Linux Windows ได้หมด
- เรียนรู้ได้ง่ายเนื่องจากภาษาพีเอชพีออกแบบมาเพื่อสร้างเอกสารแบบเอชทีเอ็มแอล มีการใช้โครงสร้างและไวยากรณ์ของภาษาที่ไม่ซับซ้อน
- รวดเร็วและมีประสิทธิภาพ โดยเฉพาะเมื่อใช้งานพร้อมกับอาปาเช่เว็บเซิร์ฟเวอร์ เพราะ การทำงานนั้นไม่ต้องใช้โปรแกรมจากภายนอกเข้ามาช่วย
- ใช้ร่วมกับภาษาเอ็กส์เอ็มแอล (Extensible Markup Language: XML) ได้
- ใช้ร่วมกับระบบฐานข้อมูลได้
- ใช้กับข้อมูลตัวอักษรได้อย่างมีประสิทธิภาพ
- ใช้กับโครงสร้างข้อมูล แบบ สเกลาร์อาเรย์ (Scalar Array) แอสโซซิเอทีฟอาเรย์ (Associative Array)
- ใช้กับการประมวลผลรูปภาพได้

ตัวอย่างการใช้งานภาษาพีเอชพี (PHP) บนเอกสารแบบเอชทีเอ็มแอล แสดงดังภาพที่ 2.6



ภาพที่ 2.6 ตัวอย่างการใช้งานภาษาพีเอชพี (PHP) บนเอกสารแบบเอชทีเอ็มแอล (HTML)

2.3.3 ภาษาเอสคิวแอล (SQL)

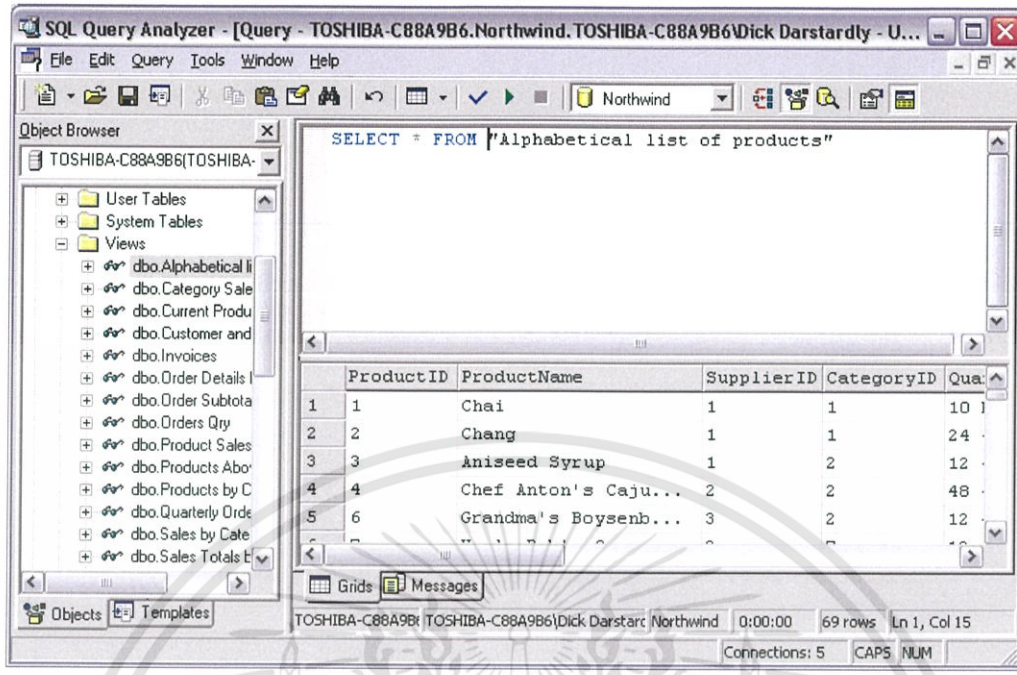
ภาษาเอสคิวแอล ย่อมาจาก Structured Query Language เป็นภาษาที่ใช้ในการเขียนโปรแกรมเพื่อเข้าถึงและจัดการกับฐานข้อมูล ผู้พัฒนานั้นสามารถใช้คำสั่งโดยใช้ภาษาเอสคิวแอลกับฐานข้อมูลชนิดใดก็ได้ และสามารถใช้คำสั่งงานเดียวกันทำการสั่งงานผ่านระบบฐานข้อมูลที่แตกต่างกันได้ มีการทำงานหลัก ๆ ได้แก่ ใช้สำหรับดึงข้อมูล (Select Query) ใช้สำหรับแก้ไขข้อมูล (Update Query) ใช้สำหรับการเพิ่มข้อมูล (Insert Query) ใช้สำหรับลบข้อมูล (Delete Query) ทำให้ผู้พัฒนาสามารถเลือกใช้ฐานข้อมูลชนิดใดก็ได้โดยไม่จำเป็นต้องติดยึดกับฐานข้อมูลใดฐานข้อมูลหนึ่ง นอกจากนี้ภาษาเอสคิวแอลยังเป็นชื่อโปรแกรมฐานข้อมูล ซึ่งโปรแกรมเอสคิวแอล เป็นโปรแกรมฐานข้อมูลที่มีโครงสร้างของภาษาที่เข้าใจง่าย ไม่ซับซ้อน มีประสิทธิภาพการทำงานสูง สามารถทำงานที่ซับซ้อนได้โดยใช้คำสั่งเพียงไม่กี่คำสั่ง โปรแกรมเอสคิวแอลจึงเหมาะที่จะใช้กับระบบฐานข้อมูลเชิงสัมพันธ์

ปัจจุบันมีซอฟต์แวร์ระบบจัดการฐานข้อมูล ที่สนับสนุนการใช้คำสั่งเอสคิวแอล เช่น ออราเคิล (Oracle) ไมโครซอฟท์แอคเซส (Microsoft-Access) ไมโครซอฟท์เอสคิวแอล (Microsoft-SQL) นอกจากนี้ภาษาเอสคิวแอล ถูกนำมาใช้เขียนร่วมกับโปรแกรมภาษาต่าง ๆ เช่น ภาษาซี/ซีพลัสพลัส (C/C++) วิชวลเบสิค (Visual Basic) และจาวา (Java)

1. ประโยชน์ของภาษาเอสคิวแอล

- ใช้สร้างฐานข้อมูล และตารางข้อมูล
- สนับสนุนการจัดการฐานข้อมูล ซึ่งประกอบด้วย การปรับปรุงแก้ไข การเพิ่มและการลบข้อมูล
- สนับสนุนการเรียกใช้หรือค้นหาข้อมูล
- ใช้สร้างเอสคิวแอววิว (SQL Views) ในฐานข้อมูลได้ สามารถทำได้ตั้งแต่การคิวรี่ข้อมูลทั้งหมดของตารางข้อมูลรวมถึงการทำเอสคิวแอลร่วม (SQL Join) การรวมของเอสคิวแอล (SQL Union) การตัดออกของเอสคิวแอล (SQL Intersect) และการยกเว้นส่วนของเอสคิว (SQL Except) ผลลัพธ์ที่ได้นั้นจะออกมาในรูปแบบของตารางข้อมูล
- ใช้กำหนดสิทธิ์ให้กับตารางข้อมูลโดยใช้กระบวนการของเอสคิวแอล (SQL Procedure) และเรียกดูข้อมูลจากฐานข้อมูล (SQL Views)

ตัวอย่างการใช้คำสั่งเอสคิวแอล (SQL) เพื่อเรียกดูข้อมูลจากฐานข้อมูล (SQL Views) จะเห็นได้ว่าเมื่อป้อนคำสั่งเอสคิวแอลลงไประบบจะเรียกดูข้อมูลจากฐานข้อมูลออกมาแสดงผลให้ผู้ใช้งานในรูปตารางแสดงดังภาพที่ 2.7



ภาพที่ 2.7 ตัวอย่างการใช้คำสั่งเอสคิวแอล (SQL) เพื่อเรียกดูข้อมูลจากฐานข้อมูล (SQL Views) [4]

2. ประเภทของคำสั่งภาษาเอสคิวแอล

- ภาษานิยามข้อมูล (Data Definition Language: DDL) ภาษานิยามข้อมูลเป็นลักษณะคำสั่งที่ใช้ในการสร้างฐานข้อมูล กำหนดโครงสร้างข้อมูลว่ามีแอตทริบิวต์ (Attribute) ประเภทใด รวมทั้งการเปลี่ยนแปลงตารางข้อมูล ตัวอย่างคำสั่ง : CREATE DROP ALTER

- ภาษาจัดการข้อมูล (Data Manipulation Language: DML) ภาษาชนิดนี้จะเป็นคำสั่งที่ใช้ในการเรียกใช้ข้อมูลจากฐานข้อมูลเพื่อทำการ เพิ่ม ลบ และเปลี่ยนแปลงข้อมูลในตารางข้อมูล ตัวอย่างคำสั่ง : SELECT INSERT UPDATE DELETE

- ภาษาควบคุมข้อมูล (Data Control Language: DCL) เป็นคำสั่งที่ใช้ในการกำหนดสิทธิ์การอนุญาติ หรือ ยกเลิกการเข้าถึงฐานข้อมูล เพื่อป้องกันความปลอดภัยในการเข้าถึงฐานข้อมูล ตัวอย่างคำสั่ง : GRANT REVOKE

3. การนำภาษาเอสคิวแอลไปใช้งานกับระบบต่าง ๆ

สามารถนำเอสคิวแอลไปใช้งานในระบบได้ดังต่อไปนี้

1. นำไปใช้กับเว็บไซต์ เพื่อใช้ในการแสดงผลข้อมูลโดยเรียกใช้จากฐานข้อมูล ตัวอย่างโปรแกรม เช่น ไมโครซอฟท์แอคเซส เอสคิวแอลเซิร์ฟเวอร์ มายเอสคิวแอล ออราเคิล

2. ใช้ร่วมกับระบบจัดการฐานข้อมูลเชิงสัมพันธ์ (Relational Database Management System: RDBMS)

3. ใช้ในการกำหนดในระบบวิเคราะห์ข้อมูล (Analysis Tools) ที่เปิดช่องให้ผู้ใช้งานสามารถทำการเพิ่ม หรือปรับปรุงเอสคิวแอลได้ด้วยตัวเอง

2.3.4 ภาษาจาวาสคริปต์ (JavaScript)

จาวาสคริปต์ เป็นภาษาคอมพิวเตอร์สำหรับเขียนโปรแกรมบนอินเทอร์เน็ต ที่ใช้ในการสร้างและพัฒนาเว็บไซต์จะใช้ร่วมกับเอชทีเอ็มแอล เพื่อช่วยในการพัฒนาเว็บไซต์ให้องค์กระกอบต่าง ๆ ดูมีการเคลื่อนไหว ช่วยให้ผู้พัฒนาสามารถสร้างเว็บเพจได้ตรงกับความต้องการ และมีความน่าสนใจ อีกทั้งยังทำให้ตอบสนองผู้ใช้งานได้มากขึ้น จาวาสคริปต์จึงได้รับความนิยมเป็นอย่างสูง มีการใช้งานอย่างกว้างขวาง

การทำงานของจาวาสคริปต์ นั้นจะต้องมีการแปลความคำสั่ง ซึ่งจัดการโดยการทำงานผ่านเบราว์เซอร์ เรียกว่า สคริปต์ฝั่งผู้ใช้งาน (Client-side script) ดังนั้นจาวาสคริปต์จึงสามารถทำงานได้ เฉพาะบนเบราว์เซอร์ที่สนับสนุน สิ่งที่ควรระวังในการใช้จาวาสคริปต์ คือ จาวาสคริปต์มีการพัฒนาเป็นเวอร์ชั่นใหม่ ๆ ออกมา (ปัจจุบันคือรุ่น 1.5) ดังนั้น ถ้านำโค้ดของเวอร์ชั่นใหม่ ไปใช้งานบนเบราว์เซอร์รุ่นเก่าที่ยังไม่สนับสนุน อาจจะทำให้เกิดเป็นข้อผิดพลาดทางโค้ด (Code error) ได้

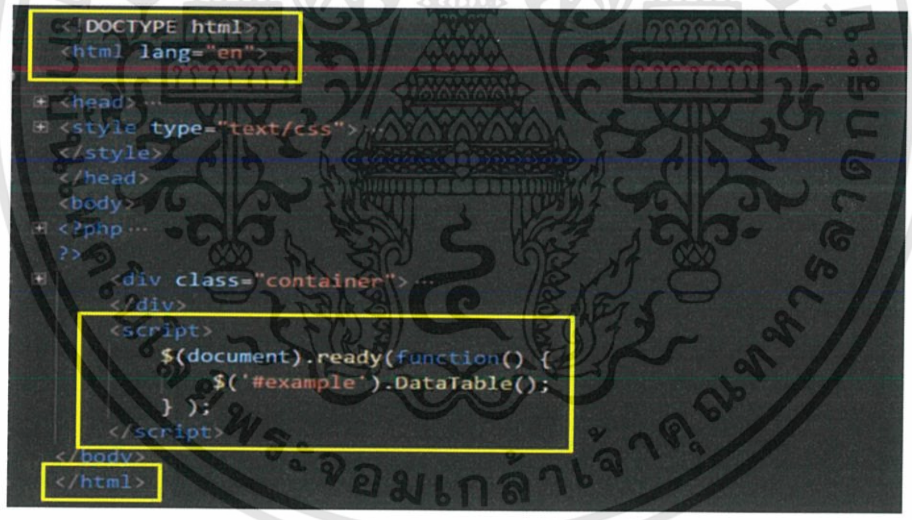
1. ประโยชน์ของจาวาสคริปต์

- จาวาสคริปต์ทำให้สามารถใช้เขียนโปรแกรมแบบง่าย ๆ ได้ โดยไม่ต้องใช้ภาษาอื่นมารองรับการทำงาน
- จาวาสคริปต์มีคำสั่งที่ตอบสนองต่อการใช้งานของผู้ใช้งาน เช่น เมื่อผู้ใช้ทำการคลิกที่ปุ่มก็สามารถสั่งให้เปิดหน้าใหม่โดยอัตโนมัติได้ ทำให้เว็บไซต์มีปฏิสัมพันธ์กับผู้ใช้งานมากขึ้น
- จาวาสคริปต์สามารถเขียนหรือเปลี่ยนแปลงเอกสารเอชทีเอมแอลได้ คือ ความสามารถในการเปลี่ยนแปลงรูปแบบการแสดงผลของเว็บไซต์ หรือทำให้หน้าแสดงเนื้อหาสามารถซ่อนหรือแสดงเนื้อหาได้
- จาวาสคริปต์สามารถใช้ตรวจสอบข้อมูลได้ ตัวอย่างเช่น การอีเมลกรอกข้อมูลในเว็บไซต์หากกรอกข้อมูลผิดจะมีหน้าต่างฟ้องขึ้นมาว่าผู้ใช้กรอกผิดหรือการกรอกรายระเอียดไม่ครบ เป็นต้น
- จาวาสคริปต์สามารถใช้ในการตรวจสอบผู้ใช้ได้ เช่น ตรวจสอบว่าผู้ใช้ทำการใช้งานเว็บเบราว์เซอร์ประเภทใด

- จาวาสคริปต์สร้างชิ้นส่วนของข้อมูลที่จัดเก็บไว้ในคอมพิวเตอร์ (Cookies) หรือการเก็บข้อมูลของผู้ใช้ในคอมพิวเตอร์ของผู้ใช้เองได้ เช่น การจดจำอีเมลของผู้ใช้ การจดจำชื่อผู้ใช้งาน (Username) ของผู้ใช้ เป็นต้น

2. ข้อดีและข้อเสียของจาวาสคริปต์

การทำงานของจาวาสคริปต์ เกิดขึ้นบนบราวเซอร์ หรือสคริปต์ด้านไคลเอนต์ ดังนั้นไม่ว่าจะใช้เซิร์ฟเวอร์ประเภทใด หรือใช้งานที่ไหน ก็ยังคงสามารถใช้จาวาสคริปต์บนเว็บเพจได้ ต่างกับภาษาสคริปต์อื่น เช่น ภาษาเพิร์ล ภาษาพีเอชพี ซึ่งต้องแปลความและทำงานที่ตัวเครื่องเซิร์ฟเวอร์ หรือเรียกว่าสคริปต์ด้านเซิร์ฟเวอร์ (Server-side script) จึงต้องมีการใช้งานบนเซิร์ฟเวอร์ที่สนับสนุนภาษาเหล่านี้เท่านั้น แต่จากคุณสมบัติดังกล่าวทำให้จาวาสคริปต์มีข้อจำกัด คือ ไม่สามารถรับและส่งข้อมูลต่าง ๆ กับเซิร์ฟเวอร์โดยตรงได้ เช่น การอ่านไฟล์จากเซิร์ฟเวอร์เพื่อนำมาแสดงบนเว็บเพจ หรือรับข้อมูลจากผู้เข้าชมเว็บเพจ เพื่อนำไปเก็บบนเซิร์ฟเวอร์ ดังนั้น ในการพัฒนาบางครั้งจึงต้องอาศัยภาษาสคริปต์ด้านเซิร์ฟเวอร์เข้ามาช่วยด้วยตัวอย่างการใช้งานภาษาจาวาสคริปต์บนเอกสารเอชทีเอ็มแอล แสดงดังภาพที่ 2.8



ภาพที่ 2.8 ตัวอย่างการใช้งานภาษาจาวาสคริปต์ (JavaScript) บนเอกสารเอชทีเอ็มแอล (HTML)

2.3.5 ภาษาซีเอสเอส (CSS)

ซีเอสเอส (CSS) ย่อมาจาก แคสเคดดิงสไตล์ชีตส์ (Cascading Style Sheet) หรือ ภาษาสไตล์ชีต เป็นภาษาที่ใช้ในการจัดรูปแบบการแสดงผลบนเอกสารเอชทีเอ็มแอล โดยที่ภาษาซีเอสเอสจะเป็นตัวกำหนดกฎเกณฑ์ในการระบุรูปแบบ (Style) ของเนื้อหาในส่วนต่าง ๆ ของเอกสาร เช่น สีพื้นหลัง สีของ

ข้อความ ประเภทตัวอักษร และตำแหน่งการจัดวางข้อความ เป็นต้น ซึ่งการกำหนดรูปแบบนี้ใช้หลักการของการแยกเนื้อหาบนเอกสารเอชทีเอ็มแอล ออกจากคำสั่งที่ใช้ในการจัดรูปแบบการแสดงผล โดยกำหนดให้รูปแบบของการแสดงผลเอกสาร ไม่ขึ้นอยู่กับเนื้อหาของเอกสาร เพื่อให้ง่ายต่อการจัดรูปแบบการแสดงผลลัพธ์ของเอกสารเอชทีเอ็มแอล โดยเฉพาะเมื่อเนื้อหาภายในเอกสารมีการเปลี่ยนแปลงบ่อย หรือใช้งานเมื่อต้องการควบคุมให้รูปแบบการแสดงผลเอกสารเอชทีเอ็มแอลมีลักษณะเดียวกันทุกหน้าเว็บเพจภายในเว็บไซต์เดียวกัน

1. ประโยชน์ของภาษาซีเอสเอส

- การใช้งานแท็กของภาษาซีเอสเอสมีคุณสมบัติมากกว่าแท็กของภาษาเอชทีเอ็มแอล เช่น การกำหนดกรอบให้ข้อความ รวมทั้งสี รูปแบบของข้อความ ถ้าใช้แท็กภาษาซีเอสเอสมาใช้แทนรูปแบบเดิมที่ใช้อยู่ รูปแบบของเว็บไซต์จะเปลี่ยนไปตามแท็กภาษาซีเอสเอสแทน

- ภาษาซีเอสเอสนั้นสามารถใช้ในการกำหนดที่ตั้งของไฟล์เอชทีเอ็มแอล การกำหนดครั้งเดียวหรือแค่จุดเดียวนั้นก็สามารถส่งผลกับการแสดงผลบนหน้าเอกสารทั้งหมดได้ ทำให้การแก้ไขหรือปรับปรุงทำได้สะดวก

- ภาษาซีเอสเอสสามารถกำหนดแยกไว้ต่างหากจากไฟล์เอกสารเอชทีเอ็มแอล และสามารถเรียกใช้งานร่วมกับเอกสารไฟล์อื่น ๆ ได้

ซีเอสเอส กับ เอชทีเอ็มแอล นั้นทำหน้าที่คนละอย่างกัน โดยภาษาเอชทีเอ็มแอลจะทำหน้าที่ในการวางโครงร่างเอกสารจะไม่เกี่ยวข้องกับการแสดงผล ส่วนซีเอสเอสจะทำหน้าที่ในการตกแต่งเอกสารให้สวยงาม เปรียบเสมือนเอชทีเอ็มแอล คือ ส่วนการลงโค้ดเพื่อวางโครงสร้าง (Coding) ส่วนซีเอสเอส คือ ส่วนการออกแบบตกแต่ง (Design) ตัวอย่างการเรียกใช้งานซีเอสเอส (CSS) มาใช้งานร่วมกับเอกสารเอชทีเอ็มแอล แสดงดังภาพที่ 2.9

```
<!DOCTYPE html>
<html lang="en">

<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="ie=edge">
  <title>Document</title>
  <link rel="stylesheet" href="asset/assetFontAwesome/all.css">
  <link rel="stylesheet" href="css/Create_Ticket.css" type="text/css">
</head>
```

ภาพที่ 2.9 ตัวอย่างการเรียกใช้งานซีเอสเอส (CSS) มาใช้งานร่วมกับเอกสารเอชทีเอ็มแอล

2.4 มาตรฐานโอดับบลิวเอเอสพี (Open Web Application Security Project: OWASP)

2.4.1 ที่มาของมาตรฐานโอดับบลิวเอเอสพี

โอดับบลิวเอเอสพี เป็นองค์การไม่แสวงหาผลกำไร (Non-profit organization) ถูกจัดตั้งขึ้นโดยมีจุดประสงค์เพื่อ จัดทำเป็นองค์กรสากลที่เป็นศูนย์รวมในการร่วมมือจากนักพัฒนาเว็บแอปพลิเคชันทั่วโลกในการสร้างเว็บแอปพลิเคชันให้มีความปลอดภัย โดยโอดับบลิวเอเอสพี ได้รับการสนับสนุนจากบริษัทไอทีชั้นนำทั่วโลกในการจัดสัมนา และการจัดอบรมเกี่ยวกับความปลอดภัยเว็บแอปพลิเคชัน

2.4.1.1 จุดเริ่มต้นด้านความปลอดภัยของเว็บแอปพลิเคชัน

ในปัจจุบันนี้อินเทอร์เน็ต และเว็บไซต์เป็นสิ่งที่ผู้คนนั้นใช้งานกันอย่างแพร่หลาย และมีการใช้งานเพิ่มขึ้นจากเดิมหลายเท่าตัวในช่วง 10 ปีที่ผ่านมา ทำให้มีการพัฒนาโปรแกรมทางคอมพิวเตอร์มาเพื่อสำหรับพัฒนาเว็บแอปพลิเคชันเพื่อให้สามารถใช้งานอินเทอร์เน็ตได้จากทุกที่ทุกเวลาทำให้เทคโนโลยีในการพัฒนาเว็บแอปพลิเคชันมีความก้าวหน้าและซับซ้อนกว่าการใช้งานในสมัยก่อนอย่างมาก ไม่เพียงแต่เว็บแอปพลิเคชันจะมีความซับซ้อนมากขึ้น ข้อมูลที่ถูกเก็บและใช้งานบนเว็บแอปพลิเคชันก็เริ่มที่จะมีความสำคัญมากขึ้นด้วยเช่นกัน ไม่ว่าจะเป็นข้อมูลการทำธุรกรรมการเงินผ่านอินเทอร์เน็ต การชำระเงินด้วยบัตรเครดิตเพื่อซื้อสินค้าออนไลน์ การเก็บข้อมูลที่เป็นความลับ เช่น ข้อมูลส่วนบุคคล ประวัติผู้ป่วย ไว้ในเว็บแอปพลิเคชันให้ผู้ใช้งานสามารถเข้าถึงได้สะดวกมากขึ้น ทำให้เว็บแอปพลิเคชันตกเป็นเป้าหมายลำดับต้น ๆ ของอาชกรรมบนอินเทอร์เน็ต (Cyber Crime) เนื่องด้วยข้อมูลสำคัญเหล่านี้มีคุณค่ามหาศาล โอดับบลิวเอเอสพีจึงได้มีการจัดอันดับช่องโหว่ที่มีความรุนแรงและพบเจอได้บ่อยในเว็บแอปพลิเคชัน 10 อันดับขึ้นมา (OWASP TOP 10)

2.4.1.2 การจัดอันดับช่องโหว่ที่ส่งผลกระทบรุนแรงต่อเว็บแอปพลิเคชันมากที่สุด 10 อันดับ (OWASP TOP 10)

โอดับบลิวเอเอสพีท็อปส์เท็น (OWASP Top 10) เป็นเอกสารงานวิจัยทางด้านความปลอดภัยของเว็บแอปพลิเคชันที่รวบรวม 10 อันดับช่องโหว่ที่ส่งผลกระทบรุนแรงต่อเว็บแอปพลิเคชันมากที่สุด จัดอันดับโดยผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยหลากหลายสาขาจากทั่วโลก ซึ่ง โอดับบลิวเอเอสพีท็อปส์เท็น เป็นเอกสารที่ทุกองค์กรควรนำไปใช้เพื่อเป็นแนวทางในการป้องกันช่องโหว่และรับมือกับภัยคุกคามที่อาจเกิดขึ้นบนเว็บแอปพลิเคชัน

ในปี ค.ศ. 2010 โอดับบลิวเอเอสพีได้ทำการจัดอันดับช่องโหว่ที่มีความรุนแรงและพบเจอได้บ่อยในเว็บแอปพลิเคชัน 10 อันดับขึ้นมาเป็นครั้งแรก และได้รับกระแสการตอบรับอย่างดีจากนักพัฒนาเว็บแอปพลิเคชันทั่วโลก โดย โอดับบลิวเอเอสพีท็อปส์เท็น ปี ค.ศ. 2010 ได้ถูกยอมรับให้เป็น

มาตรฐานการตรวจสอบช่องโหว่เว็บแอปพลิเคชันก่อนองค์กรอื่น ๆ และในปี ค.ศ. 2013 โอดับบลิวเอเอสพี ได้เผยแพร่เอกสาร โอดับบลิวเอเอสพี ท็อปส์ เท็น ปี ค.ศ. 2013 ที่อธิบายรายละเอียดช่องโหว่ที่พบได้บ่อยและมีความรุนแรง 10 อันดับแรกขึ้นมาอีกครั้ง

2.4.1.3 โอดับบลิวเอเอสพีท็อปส์เท็น (OWASP TOP 10) ปี ค.ศ. 2013

โอดับบลิวเอเอสพีท็อปส์เท็น ปี ค.ศ. 2013 มีการจัดลำดับช่องโหว่ที่ส่งผลต่อเว็บแอปพลิเคชันใหม่จาก ปี ค.ศ. 2010 เพื่อให้ตามทันการโจรกรรมข้อมูลผ่านสื่อออนไลน์ได้ ประกอบไปด้วยช่องโหว่ที่มีความร้ายแรงและพบได้บ่อยเรียงตามลำดับ ดังต่อไปนี้

1. การแทรกแซงเพื่อเข้าถึงข้อมูล (Injection) ช่องโหว่ประเภทอินเจคชั่นเป็นช่องโหว่ที่ถูกพบได้บ่อย และมีผลกระทบด้านความปลอดภัยอย่างรุนแรงต่อเว็บแอปพลิเคชัน ซึ่งช่องโหว่ประเภทนี้ประกอบไปด้วย การแทรกคำสั่งเอสคิวแอลลงไปเพื่อเข้าถึงฐานข้อมูล (SQL Injection) ที่อนุญาตให้ผู้ไม่หวังดีเรียกดูข้อมูลที่เป็นความลับในฐานข้อมูล หรือแม้กระทั้งการเข้าไปลบหรือแก้ไขข้อมูลในฐานข้อมูลบนเว็บไซต์ และ การแทรกโค้ดลงไปเพื่อเข้าถึงฐานข้อมูล (Code Injection) ที่อนุญาตให้ผู้ไม่หวังดีทำการส่งโค้ดขึ้นมาทำงานบนเซิร์ฟเวอร์ซึ่งอาจนำไปสู่การโจรกรรมข้อมูลจนไปถึงการเข้าควบคุมเครื่องเซิร์ฟเวอร์ได้

2. ช่องโหว่ของการยืนยันตัวตนและการจัดการกับสถานะผู้ใช้งาน (Broken Authentication and Session Management) ช่องโหว่ด้านความปลอดภัยประเภทนี้ได้รับการเลื่อนลำดับจากอันดับ 3 ในปี ค.ศ. 2010 ขึ้นมาเป็นอันดับ 2 ในปี ค.ศ. 2013 เนื่องจากเป็นกระบวนการพิสูจน์ตัวตน จึงมีความซับซ้อนขึ้นกว่าแต่ก่อน ตัวอย่างช่องโหว่ชนิดนี้ ได้แก่ การเก็บข้อมูลรหัสผ่าน (Password) ไว้ในชิ้นส่วนของข้อมูลที่จัดเก็บไว้ในคอมพิวเตอร์ (Cookies) ของผู้ใช้งานโดยไม่ได้ทำการเข้ารหัส หรือการแสดงส่วนของข้อมูลบนโปรแกรมชี้แหล่งทรัพยากรสากล (Universal Resource Locator: URL) ที่อาจจะถูกดักจับจากผู้ไม่หวังดีได้

3. การฝังสคริปต์ลงไปในไซต์ (Cross-Site Scripting: XSS) เป็นช่องโหว่ที่อยู่ในอันดับ 2 ในปี ค.ศ. 2010 และถูกลดอันดับลงมาเป็นอันดับ 3 ในปี ค.ศ. 2013 โดย ครอสไซต์สคริปต์ติ้ง เกิดจากการอนุญาตให้ผู้ใช้งานฝังจาวาสคริปต์ลงในเว็บไซต์ซึ่งนำไปสู่การขโมยข้อมูลเซสชั่นของผู้ใช้งานคนอื่นได้ แต่ ครอสไซต์สคริปต์ติ้ง จะไม่ได้ผลกระทบต่อตัวเว็บแอปพลิเคชันโดยตรง แต่จะก่อให้เกิดความเสียหายต่อผู้ใช้งานเว็บไซต์อย่างรุนแรงได้ เนื่องจากข้อมูลที่ถูกขโมยมานั้นอาจเป็นข้อมูลที่เป็นความลับ

4. การอ้างถึงวัตถุทางตรงแบบไม่ปลอดภัย (Insecure Direct Object References) ช่องโหว่ลำดับที่ 4 เกิดจากการที่ผู้พัฒนาอนุญาตให้ผู้ใช้งานเข้าถึงข้อมูลหรือเอกสารที่ไม่สมควร ตัวอย่างเช่น การเข้าถึงข้อมูลธุรกรรมทางการเงินผ่านทาง ไอดีผู้ใช้งาน (User ID) http://www.somebank.com?account_transaction.php?user_id=20 หากผู้ไม่หวังดีต้องการดูธุรกรรมทางการเงินของคนอื่นสามารถทำได้โดยการเปลี่ยน ไอดีผู้ใช้งาน จาก 20 เป็น 10 30 40 ในโปรแกรมชี้แหล่งทรัพยากรสากล (Universal Resource Locator: URL) ก็จะทำให้ข้อมูลความลับข้อผู้ใช้งานอื่นรั่วไหลได้

5. การกำหนดค่าความปลอดภัยผิดพลาด (Security Misconfiguration) ขอบเขตของช่องโหว่ประเภทนี้นั้นค่อนข้างกว้าง เพราะ เป็นการตั้งค่าความปลอดภัยทั้งในเว็บแอปพลิเคชัน เว็บเซิร์ฟเวอร์ ดาต้าเบส เว็บเซิร์ฟเวอร์ซอฟต์แวร์ (Web server software) เป็นต้น เกิดจากการตั้งค่าที่ผิดพลาดของส่วนประกอบต่าง ๆ ที่เกี่ยวข้อง เช่น การลืมลบค่าเริ่มต้นของผู้ใช้งาน (Default user) ไม่ทำการอัพเดทเวอร์ชั่นด้านความปลอดภัย (Security patch) ทำให้เว็บแอปพลิเคชันมีช่องโหว่ที่ปล่อยให้ผู้ไม่หวังดีทำการโจรกรรมข้อมูล หรือหยุดการทำงานของเว็บแอปพลิเคชันได้

6. การรั่วไหลของข้อมูล (Sensitive Data Exposure) ช่องโหว่ที่ 6 นี้เป็นช่องโหว่เกี่ยวกับการรั่วโหลของข้อมูลที่เก็บอยู่ในเซิร์ฟเวอร์และข้อมูลที่ส่งผ่านอินเทอร์เน็ต ตัวอย่างเช่น การเข้าใช้งาน (Login) เว็บไซต์ที่ไม่ได้ใช้ เอชทีทีพีเอส (HTTPS) ในการเข้ารหัสข้อมูล การเก็บข้อมูลรหัสผ่าน หรือข้อมูลที่เป็นความลับโดยไม่ได้เข้ารหัส หรือการใช้การเข้ารหัสที่มีความปลอดภัยต่ำ (Weak algorithm) เพื่อทำการเข้ารหัส ข้อผิดพลาดเหล่านี้ทำให้ข้อมูลที่เป็นความลับตกอยู่ในสภาวะเสี่ยงต่อการรั่วไหล

7. การขาดหายสิทธิ์เพื่อเข้าถึงระดับฟังก์ชั่น (Missing Function Level Access Control) ช่องโหว่นี้เป็นช่องโหว่เกี่ยวกับการจำกัดสิทธิ์ในการใช้งานเว็บแอปพลิเคชัน ตัวอย่างเช่น หากผู้ใช้งานสามารถเข้าถึง www.somebank.com/admin ได้โดยไม่ได้ทำการล็อกอิน ด้วยแอคเคาท์แอดมิน (Admin account) ก็เป็นการอนุญาตให้ใครก็ตามที่เป็นผู้ใช้งานเว็บไซต์สามารถเข้าไปใช้งานฟังก์ชันของแอดมินได้โดยไม่ได้รับอนุญาต

8. การปลอมแปลงคำขอข้ามไซต์ (Cross-Site Request Forgery) ลักษณะของช่องโหว่ประเภทนี้ คือ การที่ผู้ไม่หวังดีสั่งให้ผู้ใช้งานเว็บแอปพลิเคชันทำบางอย่างโดยที่ผู้ใช้งานไม่ได้ตั้งใจที่จะทำ เช่น การโอนเงิน ตัวอย่างเช่น นาย เอ เป็นผู้ใช้งานเว็บไซต์ธนาคารแห่งหนึ่ง www.somebank.com หลักจากที่นาย เอ ได้ทำการเข้าใช้งานกับทางเว็บไซด์ธนาคารแล้ว นาย เอ ไปเข้าเว็บไซต์ www.attacker.com ของนาย บี ซึ่งนาย บี ทำการเปลี่ยนเส้นทางการส่งข้อมูลของเว็บไซต์ (Redirect) นาย เอ ไปที่

www.somebank.com/transfer.php?to=B&amount=100000 เพื่อให้โอนเงินเข้าบัญชีนาย บี เป็นจำนวนเงิน 100,000 บาท โดยที่นาย บี ไม่ได้ตั้งใจ

9. การใช้ส่วนประกอบของเว็บแอปพลิเคชันที่มีช่องโหว่ที่เป็นที่รู้จัก (Using Components with Known Vulnerabilities) ช่องโหว่นี้เคยถูกรวมเป็นส่วนหนึ่งของการกำหนดค่าความปลอดภัยผิดพลาด (Security Misconfiguration) แต่ว่าถูกแยกออกมาในปี ค.ศ. 2013 โดยช่องโหว่ประเภทนี้จะเกิดจากการที่เว็บแอปพลิเคชันทำงานร่วมกับส่วนประกอบต่าง ๆ ที่มีช่องโหว่ เช่น ไลบรารี่ (Libraries) เฟรมเวิร์ค (Framework) ที่มีช่องโหว่ ดังนั้น ผู้ดูแลระบบควรตรวจสอบช่องโหว่ต่าง ๆ ก่อน และทำการอัพเดทแพทช์เพื่อปิดช่องโหว่เหล่านี้หากตรวจพบ

10. ช่องโหว่ด้านความปลอดภัยที่เว็บแอปพลิเคชันทำการเปลี่ยนเส้นทาง (Redirect) หรือส่งต่อ (Forward) ผู้ใช้งานไปยังเว็บไซต์อื่น (Unvalidated Redirects and Forwards) เป็นช่องโหว่ที่อนุญาตให้ผู้ไม่หวังดีทำการเปลี่ยนเส้นทาง ผู้ใช้งานเว็บไซต์ไปยังเว็บไซต์อันตราย ตัวอย่างเช่น หากเว็บไซต์ธนาคารแห่งหนึ่งมีหน้าที่ใช้ในการเปลี่ยนเส้นทาง ผู้ใช้งานไปยังเว็บไซต์ย่อยของแต่ละประเทศ www.somebank.com/redirect.php?target=th.somebank.com ผู้ไม่หวังดีอาจจะทำการแก้ไขลิงค์ (Link) เป็นwww.somebank.com/redirect.php?target=attacker.com ซึ่งเป็นเว็บไซต์ที่ร้องให้ผู้ใช้งานติดตั้งมัลแวร์ เนื่องจากผู้ใช้งานเข้าใจว่าเป็นเว็บไซต์ที่เปลี่ยนเส้นทางมาจากเว็บไซต์ธนาคารก็อาจจะตกเป็นเหยื่อของมัลแวร์ได้

2.4.1.4 โอดับบลิวเอเอสพีท็อปส์เท็น (OWASP TOP 10) ปี ค.ศ. ปี 2017

โอดับบลิวเอเอสพีท็อปส์เท็น ปี ค.ศ. 2017 นี้เป็นการรวบรวมความเสี่ยง หรือช่องโหว่ที่ส่งผลกระทบรุนแรงต่อเว็บแอปพลิเคชันฉบับล่าสุด และเป็นแนวทางปฏิบัติที่ดีที่สุดสำหรับรับมือกับภัยคุกคามบนเว็บแอปพลิเคชันซึ่งเป็นสิ่งที่ผู้ดูแลระบบสารสนเทศ (IT Admin) และนักพัฒนา (Developer) ต้องทำการศึกษาเพื่อที่จะได้ออกแบบแอปพลิเคชัน และระบบรักษาความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ ตารางแสดงผลการเปรียบเทียบโอดับบลิวเอเอสพีท็อปส์เท็น ปี ค.ศ. 2013 กับ ปี ค.ศ. 2017 แสดงดังภาพที่ 2.10

OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

ภาพที่ 2.10 ตารางแสดงผลการเปรียบเทียบโอดับบลิวเอเอสพีท็อปส์เท็น ปี ค.ศ. 2013 กับ ปี ค.ศ. 2017 [5]

จะเห็นว่าความเสี่ยงบางรายการของปี ค.ศ. 2013 ถูกรวมเข้ากับความเสี่ยงใหม่ในปี ค.ศ. 2017 ยกเว้น A10 – Unvalidated Redirects and Forwards ที่หายไป ในขณะที่โอดับบลิวเอเอสพีท็อปส์เท็น ปี ค.ศ. 2017 มีการเพิ่มความเสี่ยงใหม่เข้ามา 3 รายการ คือ

1. A4 – Broken Access Control เป็นความเสี่ยงทางด้านฟังก์ชันของแอปพลิเคชันที่เกี่ยวข้องกับการพิสูจน์ตัวตน และการบริหารจัดการเซสชันซึ่งถูกพัฒนาอย่างไม่ถูกต้อง ช่วยให้แฮ็คเกอร์สามารถเข้าถึงเพื่อทราบรหัสผ่าน และสามารถใช้กุญแจที่เข้ารหัสโทเค็นของเซสชัน หรือเจาะช่องโหว่เพื่อขโมยตัวตนของผู้ใช้งานได้

2. A7 – Insufficient Attack Protection ช่องโหว่ประเภทนี้เป็นช่องโหว่ที่แอปพลิเคชันและช่องทางการเชื่อมต่อกับเว็บไซต์ผู้ให้บริการ (Application Programming Interface: API) ขาดความสามารถพื้นฐานในการตรวจจับ และป้องกันโดยไม่ตอบสนองต่อการโจมตีแบบจัดการด้วยตัวเอง (Manual) และการโจมตีแบบอัตโนมัติ (Automated)

3. A10 – Underprotected APIs แอปพลิเคชันสมัยใหม่มีการใช้ผู้ใช้งานแอปพลิเคชัน (Client Applications) และช่องทางการเชื่อมต่อกับเว็บไซต์ผู้ให้บริการ (Application Programming Interface: API) เป็นจำนวนมาก เช่น จาวาสคริปต์ เอสโอเอพี/เอ็กส์เอ็มแอล (SOAP/XML) และอื่น ๆ ซึ่งช่องทางการเชื่อมต่อกับเว็บไซต์ผู้ให้บริการเหล่านี้ส่วนใหญ่ไม่ได้รับการป้องกัน หรือมีช่องโหว่เป็นจำนวนมากแอบแฝงอยู่

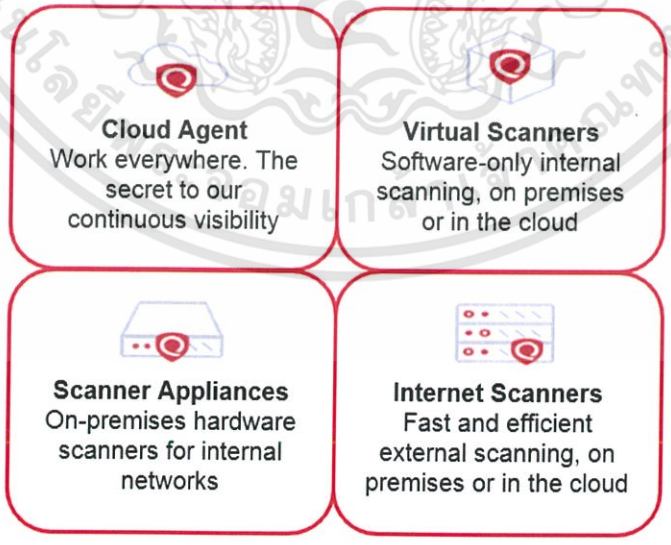
2.5 เครื่องมือที่ใช้ในการตรวจสอบหาช่องโหว่จากเว็บไซต์ภายในองค์กร

2.5.1 เครื่องมือควอริช (Qualys Tools)

เครื่องมือควอริชเป็นระบบคราวด์แพลตฟอร์ม (Cloud Platform) ทางเลือกสำหรับองค์กรในการจัดการด้านความปลอดภัย (Security) ในรูปแบบครบวงจร (End to End Solutions) โดยแอปพลิเคชันที่เปิดให้ใช้งานบนระบบคราวด์แพลตฟอร์ม นั้นสามารถตอบโจทย์การใช้งานในองค์กรที่หลากหลายตั้งแต่การติดตามการปฏิบัติตาม (Compliance Monitoring) การรักษาความปลอดภัยของเทคโนโลยีสารสนเทศ (IT Security) ความปลอดภัยของเว็บแอป (Web App Security) และการจัดการสินทรัพย์ขององค์กร (Asset Management) โดยคุณสมบัติของควอริชมี ดังนี้

2.5.1.1 ระบบเซนเซอร์ของควอริชที่สามารถเข้าตรวจสอบทรัพย์สินขององค์กรได้อย่างรวดเร็ว

ควอริชจะมีเซนเซอร์ระบบคราวด์แพลตฟอร์มสำหรับการใช้งานในรูปแบบต่าง ๆ ไม่ว่าจะเป็นรูปแบบระบบเซิร์ฟเวอร์ตั้งอยู่ที่ฝั่งของผู้ใช้บริการเอง (On-premise) ปลายทาง (Endpoint) หรือคราวด์ (Cloud) ซึ่งมีหลักการทำงานแบบออนไลน์ตลอดเวลา (Always-on) ดังนั้น ควอริชจึงสามารถเข้าถึงเพื่อทำการตรวจสอบทรัพย์สินต่าง ๆ ภายในองค์กรได้อย่างรวดเร็วความสามารถของเซนเซอร์ควอริช ได้แก่ สามารถเข้าใช้งานได้ทุกที่ทุกเวลา สามารถทำการเลือกรูปแบบการสแกนได้ทั้งสแกนภายใน สแกนเฉพาะฝั่งเซิร์ฟเวอร์ผู้ใช้บริการ หรือสแกนผ่านระบบคราวด์ก็ได้ และมาพร้อมกับการทำงานที่รวดเร็วและมีประสิทธิภาพอีกด้วย แสดงดังภาพที่ 2.11



ภาพที่ 2.11 ความสามารถของเซนเซอร์ควอริช [3]

2.5.1.2 สามารถเข้าตรวจสอบรายละเอียดทั้งหมดผ่านเว็บเบราว์เซอร์ได้

ควอริชคราวด์แพลตฟอร์มนั้นสามารถเข้าถึงได้โดยตรงจากเว็บเบราว์เซอร์ โดยไม่จำเป็นต้องมี โปรแกรมเสริมใด ๆ ผู้ดูแลระบบสามารถเข้าถึงข้อมูลทรัพย์สินภายในองค์กรทั้งหมดซึ่งจะมีการอัพเดทตลอดเวลาได้จากหน้าอินเทอร์เฟส (Interface) และเป็นการแสดงผลที่รวมทุกส่วนของโครงสร้างพื้นฐานมาไว้ด้วยกัน (Single-pane-of-glass interface) และยังเป็นการอัพเดทข้อมูลแบบตลอดเวลา (Real-time) อีกด้วย

2.5.1.3 ข้อดีของโครงสร้างพื้นฐานของระบบคราวด์ (Cloud-based architecture)

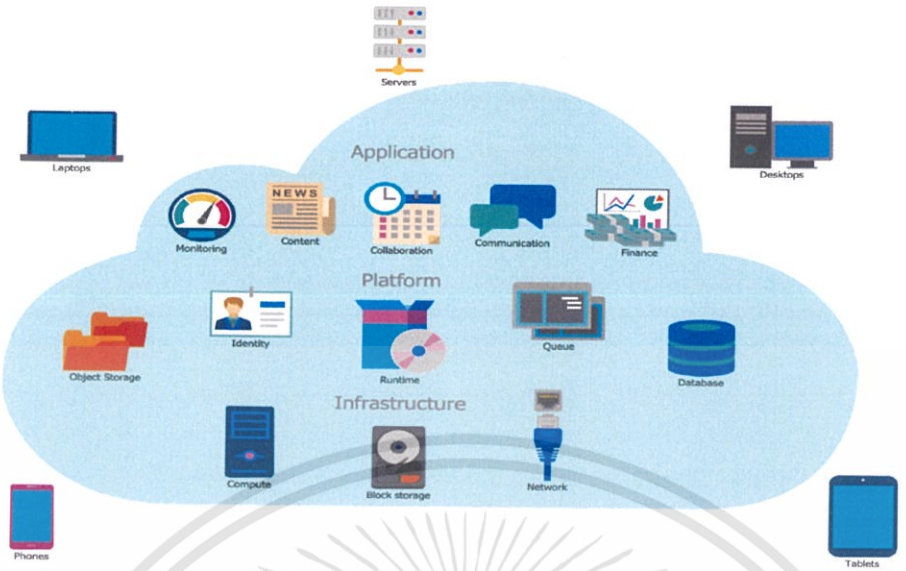
1. ไม่จำเป็นต้องมีการติดตั้งหรือจัดการอุปกรณ์ใด ๆ เพราะ บริการทั้งหมดนั้นอยู่บนคราวด์ และสามารถเข้าถึงได้ผ่านทางเว็บอินเทอร์เฟสได้

2. ระบบทั้งหมดอยู่บนคราวด์จึงไม่มีค่าใช้จ่ายเพิ่มเติม ไม่ต้องใช้ทรัพยากรบุคคลเพิ่มและไม่มีซอฟต์แวร์ หรืออุปกรณ์ต้องบำรุงรักษา

3. ควอริชคราวด์แพลตฟอร์มนั้นสามารถเพิ่มหรือลดจำนวนผู้ใช้ได้ และสามารถเพิ่มการบริการ (Service) ใหม่ได้ตามต้องการแม้จะมีการนำระบบไปเปิดใช้งานแล้วก็ตาม

4. ควอริชมีฐานข้อมูลเกี่ยวกับช่องโหว่ที่ใหญ่ที่สุด และในแต่ละปีนั้นมีการทำการตรวจสอบหรือสแกนเว็บไซต์ต่าง ๆ รวมกว่า 3 พันล้านที่อยู่ไอพี (IP Address) ต่อปี ฐานข้อมูลนั้นจึงมีการอัพเดทอยู่ตลอดเวลา

5. ข้อมูลช่องโหว่นั้นถูกประมวลผลและเก็บอย่างปลอดภัยบนระบบเชื่อมต่อโดยสมบูรณ์ในตัวควอริชเองรวมถึงการทำงานแต่ละรูปแบบ ข้อมูลที่ถูกจัดเก็บ การทำหน้าที่เป็นไคลเอ็นท์ (Client) และเซิร์ฟเวอร์ (Server) ทุกอย่างจะมีระบบการจัดการในตัวมันเอง (N-tiered architecture) อีกทั้งยังมีการทำระบบเซิร์ฟเวอร์ที่สามารถรองรับการทำงานที่มีปริมาณงานจำนวนมากได้ (Load-balance) อีกทั้งยังมีการเข้ารหัสที่ฐานข้อมูลด้วย โครงสร้างพื้นฐานของระบบคราวด์ แสดงดังภาพที่ 2.12



ภาพที่ 2.12 โครงสร้างพื้นฐานของระบบคราวด์ (Cloud-based architecture) [6]

2.5.1.4 ฟังก์ชั่นสแกนเว็บแอปพลิเคชันของควอริช (Qualys Web Application Scanner: WAS)

ในปัจจุบันเว็บแอปพลิเคชันที่ไม่มีความปลอดภัยนั้นเป็นที่ดึงดูดความสนใจของผู้โจมตี (Hacker) เนื่องจากเป็นช่องทางการโจมตีที่ง่ายต่อการเข้าถึง และเป็นจุดที่สามารถใช้ขยายผลการโจมตีเข้าไปภายในองค์กรได้ดี เว็บแอปพลิเคชันนั้นเป็นเป็นช่องทางที่สามารถทำให้เกิดข้อมูลภายในองค์กรรั่วไหลได้เป็นปริมาณมหาศาล ควอริชจึงมีฟังก์ชั่นสแกนเว็บแอปพลิเคชัน เข้ามาช่วยทำการป้องกันด้วยผลลัพธ์การตรวจสอบที่มีความแม่นยำ หลักแหลม ครอบคลุม และมีโอกาสผิดพลาดต่ำ โดยแบ่งการทำงานได้ดังนี้

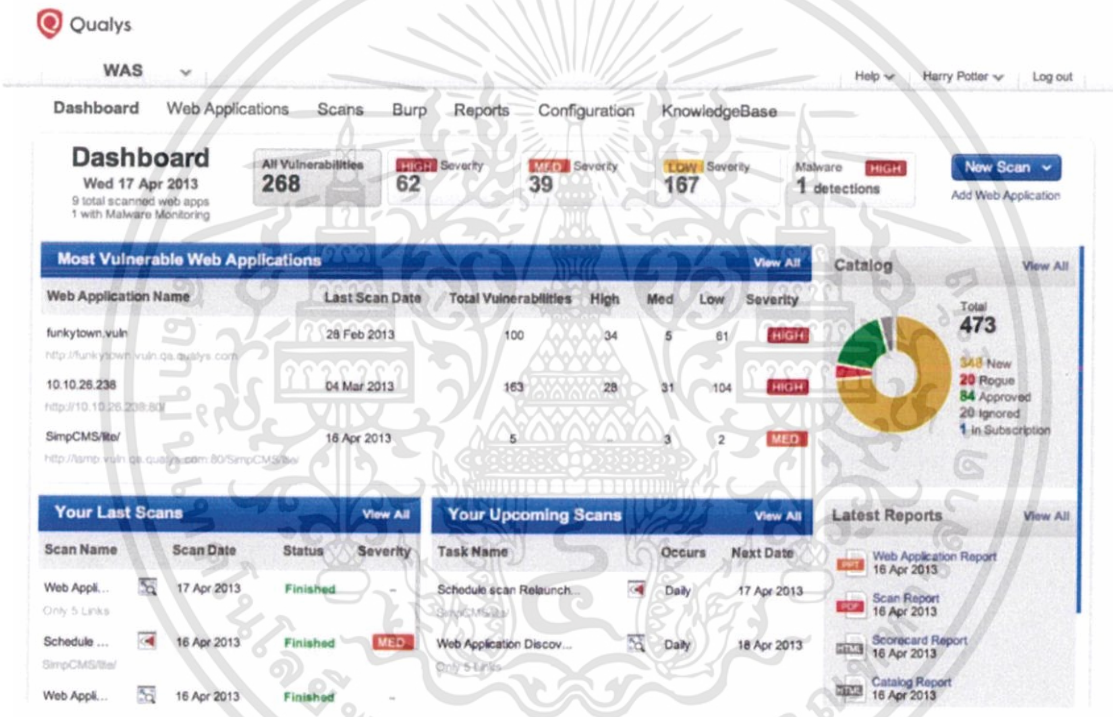
1. มีการตรวจสอบที่ครอบคลุมและละเอียด

ฟังก์ชันสแกนเว็บแอปพลิเคชันสามารถตรวจหาและจัดการเว็บแอปพลิเคชันภายในระบบอย่างหลากหลายรวมถึงจัดแบ่งหมวดหมู่ของแอปพลิเคชัน ด้วยการจัดประเภทก่อนจะทำการตรวจสอบข้อมูล เว็บแอปพลิเคชันที่กำหนดไว้ หรือทำการสร้างป้ายกำกับที่สามารถกำหนดเองได้ (Custom label) เผื่อไว้สำหรับการแบ่งแยก และสามารถจัดเรียงได้ตามต้องการ โดยพื้นฐานแล้วการตรวจหาช่องโหว่ควอริชเว็บแอปพลิเคชันจะใช้มาตราฐานโอดับบลิวเอเอสพีท็อปส์เท็น เป็นแกนหลักของการทำการสแกนเว็บแอปพลิเคชัน อีกทั้งเมื่อทำการตรวจสอบแอปพลิเคชั่นที่มีขนาดใหญ่มากนั้นก็สามารถที่จะทำการตรวจสอบในรูปแบบการสแกนข้อมูลทั้งหมด (Progressive scanning) ที่มีการสแกนอย่างละเอียด หรือทำการ

ตรวจสอบเพียงบางส่วนของเป้าหมายในการสแกนแต่ละครั้งก็ได้ เพื่อลดระยะเวลาการตรวจสอบซ้ำจากส่วนที่เคยตรวจสอบไปแล้ว

2. มีรูปแบบการแสดงผลที่สามารถปรับแต่งได้

สำหรับรายงานผลการทดสอบนั้นสามารถทำการปรับเปลี่ยนรูปแบบ (Template) ของรายงานได้เพื่อให้เหมาะสมกับผู้ที่รับชมรายงาน เช่น การแยกเล่มรายงานระหว่างรายงานสรุปสำหรับผู้บริหาร และรายงานสรุปสำหรับทีมเทคนิค ตัวอย่างหน้าจอแสดงผลของควอริชเว็บแอปพลิเคชันสแกนเนอร์แสดงดังภาพที่ 2.13



ภาพที่ 2.13 ตัวอย่างหน้าจอแสดงผลของควอริชเว็บแอปพลิเคชันสแกนเนอร์ [7]

บทที่ 3
ขั้นตอนการดำเนินงาน

วิธีการดำเนินงานสามารถแบ่งออกได้เป็น 6 ส่วนด้วยกัน คือ

1. การศึกษาข้อมูลและจุดประสงค์ที่จะนำมาใช้พัฒนาเว็บแอปพลิเคชัน
    - ศึกษาเกี่ยวกับปัญหาที่มาและความสำคัญ
    - ศึกษาเกี่ยวกับประเภทของช่องโหว่ตามมาตรฐานโอดับบลิวเอเอสพี (Open Web Application Security Project)
    - ศึกษาโปรแกรมและภาษาของโปรแกรมที่จะนำใช้พัฒนาเว็บแอปพลิเคชัน
    - ศึกษากระบวนการเมื่อตรวจพบช่องโหว่
2. การออกแบบและจัดเตรียมข้อมูลที่จะนำมาใช้พัฒนาเว็บแอปพลิเคชัน
3. การพัฒนาเว็บแอปพลิเคชัน
4. การทดสอบระบบและแก้ไขข้อผิดพลาดที่ตรวจพบ
5. การเผยแพร่เว็บแอปพลิเคชัน
6. การดูแลและบำรุงรักษาเว็บแอปพลิเคชัน

3.1 การศึกษาข้อมูลและจุดประสงค์ที่จะนำมาพัฒนาเว็บแอปพลิเคชัน

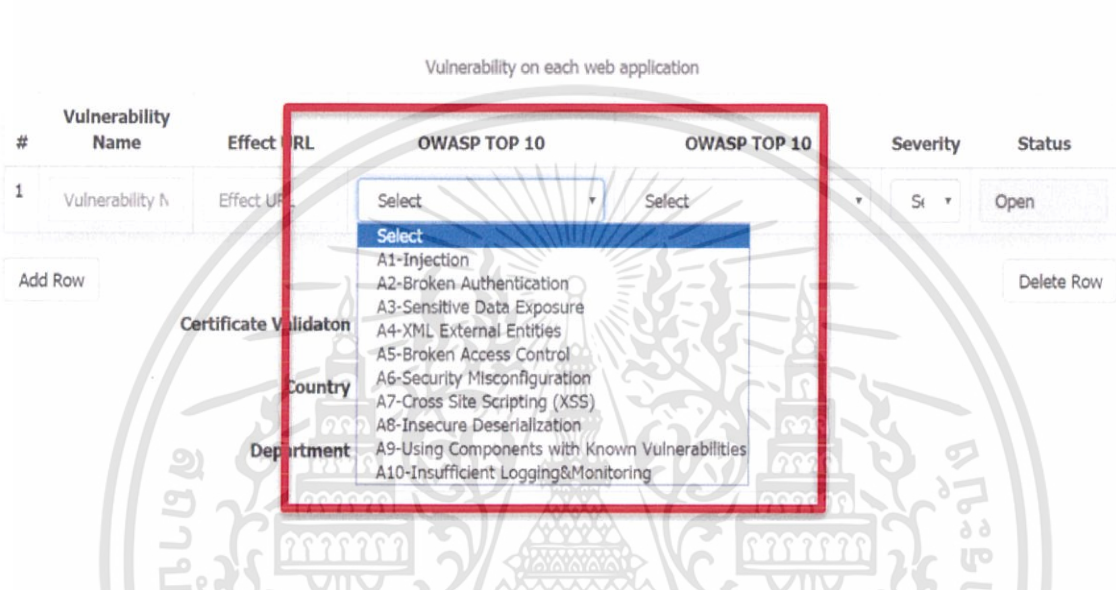
3.1.1 ศึกษาที่มาและความสำคัญ

ศึกษาเกี่ยวกับปัญหาที่มาและความสำคัญที่ทำให้เกิดเป็นโปรเจคนี้ขึ้น พร้อมแนวทางการพัฒนาโปรเจคจากปัญหาเดิมที่มีอยู่ ในขั้นตอนแรกเราจะต้องทำความเข้าใจเกี่ยวกับที่มาและความสำคัญของปัญหาที่ทำให้เกิดเป็นโปรเจคนี้ขึ้นมาว่าปัญหาเดิมที่เคยมีอยู่มีข้อบกพร่องอย่างไร ทำไมเราจึงต้องพัฒนาให้มีประสิทธิภาพที่ดีขึ้น พร้อมกับวางแผนหาแนวทางการแก้ไขจุดบกพร่องที่มีอยู่ให้มีการใช้งานที่สมบูรณ์และสะดวกยิ่งขึ้น ดังนั้นข้อมูลในส่วนนี้จึงเป็นส่วนสำคัญและจุดเริ่มต้นของการพัฒนาโปรเจค

3.1.2 ศึกษาเกี่ยวกับประเภทของช่องโหว่ตามมาตรฐานโอดับบลิวเอเอสพี (Open Web Application Security Project)

ซึ่งเป็นมาตรฐานสากลในด้านความปลอดภัยของเว็บแอปพลิเคชัน เพื่อให้เข้าใจถึงความหมายและรูปแบบของการเกิดช่องโหว่ โอดับบลิวเอเอสพี (Open Web Application Security Project) จะเป็นมาตรฐานที่รวบรวม 10 อันดับช่องโหว่ที่ส่งผลต่อเว็บแอปพลิเคชันมากที่สุด การทำความเข้าใจเกี่ยวกับช่องโหว่เหล่านี้จะช่วยให้เราเข้าใจถึงรูปแบบการโจมตีว่ามีวิธีการอย่างไรเพื่อสามารถเข้าถึงข้อมูลนั้น ๆ ได้

รวมถึงวิธีการป้องกันและการรับมือเมื่อเกิดช่องโหว่ขึ้นมา การจัดลำดับความเสี่ยงเมื่อเกิดการโจมตีจากช่องโหว่ ซึ่งเมื่อเราเข้าใจเกี่ยวกับประเภทของช่องโหว่ต่าง ๆ แล้ว จะช่วยทำให้ง่ายต่อขั้นตอนการออกแบบเว็บแอปพลิเคชันให้เหมาะสมต่อการใช้งาน และทำให้ง่ายต่อการใช้งานของผู้ใช้งานเว็บแอปพลิเคชันด้วย ตัวอย่างการออกแบบเว็บแอปพลิเคชันดรอปดาวเมนู (Dropdown Menu) โอดับบลิวเอเอสพีท็อปเท็นให้สะดวกต่อการใช้งาน แสดงดังภาพที่ 3.1



ภาพที่ 3.1 ตัวอย่างการออกแบบดรอปดาวเมนูโอดับบลิวเอเอสพีท็อปเท็นให้สะดวกต่อการใช้งาน

3.1.3 ศึกษาโปรแกรมและภาษาของโปรแกรมที่จะนำใช้พัฒนาเว็บแอปพลิเคชัน

ขั้นตอนการเลือกโปรแกรมและภาษาที่จะนำมาพัฒนาเว็บแอปพลิเคชันให้มีความเหมาะสม ง่ายต่อการใช้งานและสามารถแก้ไขหรือปรับปรุงพัฒนาเว็บแอปพลิเคชัน ในภายหลังได้

โปรแกรมที่เลือกใช้ในการพัฒนาเว็บแอปพลิเคชัน

- โปรแกรมวิชวล สตูดิโอ โค้ด
- โปรแกรมเอ็กซ์เอเอ็มพีพี
- โปรแกรมพีเอชพีมายแอดมิน

ภาษาทางโปรแกรมที่เลือกใช้ในการพัฒนาเว็บแอปพลิเคชัน

- ภาษาพีเอชพี
- ภาษาเอสคิวแอล

- ภาษาจาวาสคริปต์

3.1.4 ศึกษากระบวนการเมื่อตรวจพบช่องโหว่

เป็นขั้นตอนที่จะต้องทำความเข้าใจเกี่ยวกับช่องโหว่ที่ตรวจพบจากเว็บไซต์และเว็บแอปพลิเคชันภายในองค์กรโดยการตรวจสอบจากเครื่องมือที่ทำการตรวจหาว่าแต่ละเว็บไซต์หรือเว็บแอปพลิเคชันที่ใช้งานภายในองค์กรนั้นว่ามีช่องโหว่เกิดขึ้นหรือไม่ ถ้าตรวจเจอช่องโหว่จะมีขั้นตอนการแก้ไขอย่างไรให้รวดเร็วต่อการป้องกันการโจรกรรมข้อมูลผ่านเว็บไซต์และเว็บแอปพลิเคชันภายในองค์กรอย่างไร โดยขั้นตอนหลังจากตรวจพบช่องโหว่จากเว็บไซต์และเว็บแอปพลิเคชันนั้นจะต้องทำการติดต่อกับทีมต่าง ๆ ที่เกี่ยวข้องเพื่อให้ทราบเกี่ยวกับรายละเอียดของช่องโหว่ที่เกิดขึ้น แล้วทำการประสานงานเพื่อปิดช่องโหว่นั้น ๆ ว่ามีขั้นตอนการดำเนินการอย่างไร ซึ่งข้อมูลการทำงานเหล่านี้จะเป็นส่วนที่ใช้ในการต่อยอดเพื่อออกแบบเว็บแอปพลิเคชันและสามารถใช้กำหนดระดับการเข้าใช้งานเว็บแอปพลิเคชันของเรา ว่าแต่ละทีมที่เกี่ยวข้องสามารถเข้าดูช่องโหว่ที่ทีมตนเองมีส่วนเกี่ยวข้องเท่านั้น ไม่สามารถเข้าดูรายละเอียดของช่องโหว่เว็บไซต์หรือเว็บแอปพลิเคชันที่ตนไม่ได้รับผิดชอบได้

3.2 การออกแบบและการจัดเตรียมข้อมูลที่จะนำมาใช้พัฒนาเว็บแอปพลิเคชัน

หลังจากทำการศึกษาข้อมูลต่าง ๆ เพื่อที่จะนำมาพัฒนาเว็บแอปพลิเคชันแล้ว ขั้นตอนต่อไปเราจะต้องนำข้อมูลเหล่านั้นมาทำการวางแผนเพื่อที่จะทำการออกแบบเว็บแอปพลิเคชันที่จะใช้งานจริง โดยเป็นการออกแบบโครงสร้างของเว็บแอปพลิเคชัน และออกแบบการจัดวางเนื้อหาข้อมูลออกเป็นส่วนต่าง ๆ ว่าข้อมูลแต่ละส่วนนั้นควรนำไปใช้ในส่วนไหนของเว็บแอปพลิเคชันเราเพื่อให้มีความครบถ้วนของเนื้อหา ดูน่าสนใจสะดวกต่อการใช้งานและรวมถึงการกำหนดระยะเวลาที่จะใช้พัฒนาเว็บแอปพลิเคชันด้วย

3.3 การพัฒนาเว็บแอปพลิเคชัน

เมื่อเสร็จขั้นตอนการออกแบบแล้วจะเป็นขั้นตอนพัฒนาเว็บแอปพลิเคชันตามที่ได้ออกแบบไว้ ซึ่งการพัฒนาเว็บแอปพลิเคชันนี้จะต้องมีปัจจัยหลาย ๆ ด้วยกัน ได้แก่ การออกแบบหน้าตาเว็บแอปพลิเคชันให้เหมาะสมกับกลุ่มผู้ใช้งาน การจัดวางโครงสร้าง การรองรับภาษาในการใช้งานและส่วนต่าง ๆ ของเนื้อหาองค์ประกอบให้มีความสัมพันธ์กันสะดวกต่อการใช้งานของผู้ใช้ ซึ่งการพัฒนาเว็บแอปพลิเคชันผู้พัฒนาจำเป็นจะต้องคำนึงถึงข้อผิดพลาดที่อาจจะขึ้นขึ้นได้เมื่อนำไปใช้งาน ดังนั้นเว็บแอปพลิเคชันที่พัฒนาเสร็จแล้วต้องสามารถนำมาปรับปรุงหรือแก้ไขหากได้หากเกิดข้อผิดพลาด

3.4 การทดสอบระบบและแก้ไขข้อผิดพลาดที่ตรวจพบ

ขั้นตอนต่อจากการพัฒนาเว็บแอปพลิเคชัน ผู้พัฒนาจะต้องทำการตรวจสอบความถูกต้องของเนื้อหาภายในเว็บแอปพลิเคชัน ทดสอบระบบในส่วนต่าง ๆ ได่แก่ การทำงานของลิงค์และระบบนำทาง ตรวจสอบหาความผิดพลาดของโปรแกรมสคริปต์ ตรวจสอบการบันทึกและเรียกใช้ข้อมูลจากฐานข้อมูล ตรวจสอบความถูกตอ้งจากการทา งานของฟังก์ชั่นการทำงานที่พัฒนาขึ้น ตรวจสอบการทำงานของเว็บแอปพลิเคชันบนเบราร์เซอร์ต่าง ๆ ตรวจสอบความละเอียดของจอภาพที่สามารถทำงานได้เหมาะสม ตรวจสอบการแสดงผลของเว็บแอปพลิเคชันบนอุปกรณ์ที่มีขนาดหน้าจอแตกต่างกัน ตรวจสอบความเร็วในการแสดงผลของเว็บแอปพลิเคชัน ตรวจสอบเวลาตอบสนองเมื่อมีการเรียกใช้เว็บเพจแต่ละหน้า เพื่อป้องกันข้อผิดพลาดก่อนการนำไปใช้งานจริง

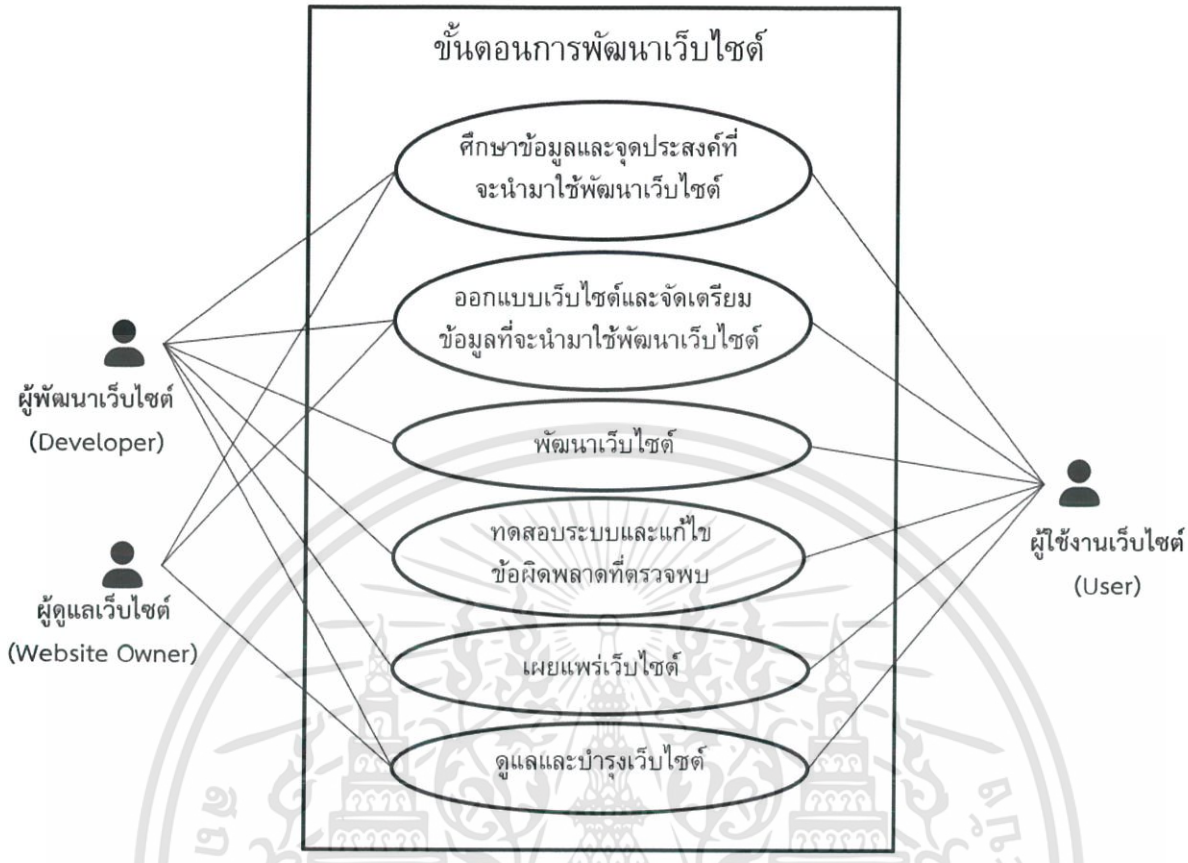
3.5 การเผยแพร่เว็บแอปพลิเคชัน

เป็นขั้นตอนการนำเว็บแอปพลิเคชันที่พัฒนาเรียบร้อยแล้ว อัพโหลดลงเซิฟเวอร์จริงขึ้นเผยแพร่บนเครือข่ายอินเทอร์เน็ต โดยการเผยแพร่นั้นจะต้องใช้พื่นที่ในการเก็บไฟล์เนื้อหาของเว็บแอปพลิเคชัน เราจะต้องใช้เว็บโฮสติ้ง (Web Hosting) และชื่อโดเมน (Domain Name) ของเว็บแอปพลิเคชันเราเพื่อใช้เป็นที่อยู่ของเว็บแอปพลิเคชัน หรือแทนด้วยไอพีแอดเดรส (IP Address) หมายเลขอินเทอร์เน็ต

3.6 การดูแลและบำรุงรักษาเว็บแอปพลิเคชัน

หลังจากเราทำการเผยแพร่เว็บแอปพลิเคชันให้ผู้ใช้สามารถเข้าใช้งานได้แล้ว ต้องมีอีกหนึ่งขั้นตอน คือ การดูแลและบำรุงรักษาเว็บแอปพลิเคชัน ผู้พัฒนาหรือเจ้าของเว็บแอปพลิเคชันจะต้องดูแลให้ข้อมูลที่นำเสนอบนเว็บแอปพลิเคชันเป็นปัจจุบันอยู่เสมอ หากตรวจพบข้อผิดพลาดควรรีบดำเนินการแก้ไขปรับปรุงเพื่อให้เว็บแอปพลิเคชันมีความน่าเชื่อถือต่อการใช้งาน และคอยเปลี่ยนแปลงหน้าตาของเว็บแอปพลิเคชันให้มีความทันสมัยน่าใช้งานเหมาะกับกลุ่มผู้ใช้งาน รวมถึงการติดตามและวิเคราะห์ลักษณะความต้องการของผู้ใช้ เพื่อเพิ่มเนื้อหาหรือปรับเปลี่ยนให้ตรงตามความต้องการของผู้ใช้งาน

จากขั้นตอนการทำงานใน 6 ขั้นตอนข้างต้น สามารถเขียนออกมาเป็นแผนภาพการทำงาน (Use Case Diagram) ของขั้นตอนการพัฒนาเว็บไซต์ ระหว่างความสัมพันธ์ของผู้พัฒนาเว็บไซต์ (Developer) ผู้ดูแลเว็บไซต์ (Website Owner) และผู้ใช้งานเว็บไซต์ (User) ได้ดังภาพที่ 3.2



ภาพที่ 3.2 แผนภาพการทำงาน (Use Case Diagram) ของขั้นตอนการพัฒนาเว็บไซต์

บทที่ 4

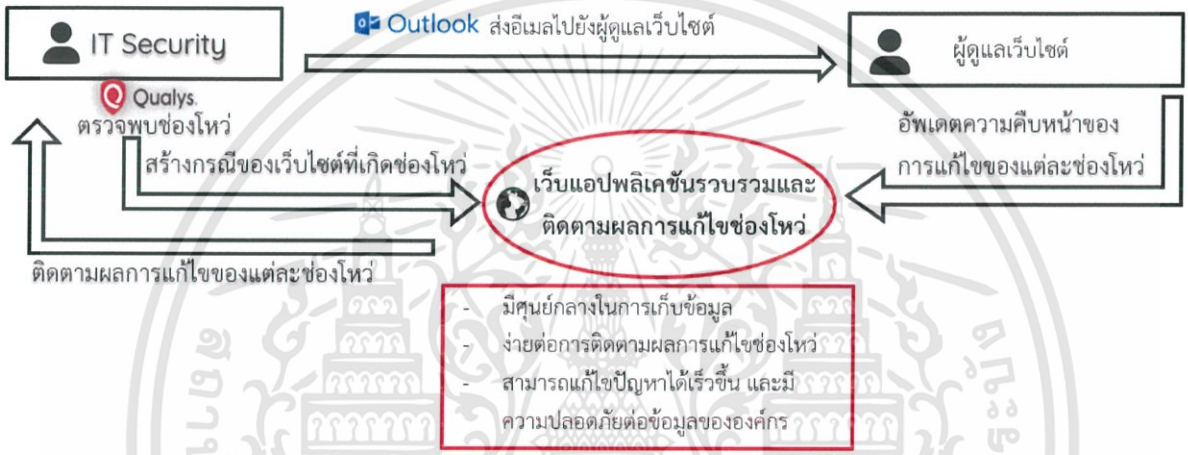
ผลการวิจัย

จากการศึกษาและพัฒนาออกมาเป็นเว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่ (Vulnerable Monitoring System) ภายในโครงการของแผนกไอที (IT) ทีมทีมรักษาความปลอดภัยของเทคโนโลยีสารสนเทศ (IT Security) ที่ต้องการจะจัดทำเว็บแอปพลิเคชันที่มีการจัดเก็บและรวบรวมข้อมูลที่เป็นศูนย์กลางเกี่ยวกับช่องโหว่ที่เกิดขึ้นจากเว็บไซต์และเว็บแอปพลิเคชันภายในองค์กร ให้มีการติดต่อเพื่อทำการแก้ไขหรือปิดช่องโหว่ระหว่างทีมทีมรักษาความปลอดภัยของเทคโนโลยีสารสนเทศไปยังทีมอื่น ๆ ที่เกี่ยวข้อง มีความสะดวก รวดเร็วและง่ายต่อการติดตามผลของการแก้ไขได้มีประสิทธิภาพมากขึ้น โดยจากผลการทดลองจะแบ่งออกเป็นหัวข้อ ดังต่อไปนี้

4.1 หลักการทำงานของระบบเมื่อเทียบกับการทำงานในอดีต

เริ่มแรกการทำงานในอดีตนั้นหลังจากเมื่อทีมทีมรักษาความปลอดภัยของเทคโนโลยีสารสนเทศใช้เครื่องมือควอริช ตรวจหาช่องโหว่จากเว็บไซต์และเว็บแอปพลิเคชัน แล้วจะต้องทำการส่งอีเมลไปยังผู้ดูแลเว็บไซต์ของเว็บไซต์ที่ตรวจพบช่องโหว่แต่ละคนแล้วให้กลับอัพเดทความคืบหน้าของการแก้ไขช่องโหว่โดยการตอบกลับอีเมลกลับมา แต่ปัญหา คือ เกิดความยากต่อการติดตามการแก้ไขช่องโหว่ เพราะ ช่องโหว่ที่ตรวจพบนั้นมีจำนวนมากและผู้ดูแลเว็บไซต์ก็มีหลายคนเช่นกัน จึงใช้เว็บไซต์รวบรวมและติดตามผลการแก้ไขช่องโหว่เข้ามาแก้ปัญหาดังกล่าว โดยหลักการทำงานของระบบในปัจจุบัน คือ เมื่อทีมทีมรักษาความปลอดภัยของเทคโนโลยีสารสนเทศทำการตรวจพบช่องโหว่จากเครื่องมือควอริช จะต้องทำการสร้างกรณีที่ตรวจพบขึ้นมาและส่งอีเมลไปยังผู้ดูแลเว็บไซต์ที่เกิดช่องโหว่นั้น ๆ เมื่อผู้ดูแลเว็บไซต์ได้รับรายละเอียดของช่องโหว่แล้วจะต้องเข้ามาทำการแก้ไขช่องโหว่ที่เกิดขึ้นมา แล้วทำการอัพเดทความคืบหน้าของการแก้ไขช่องโหว่ไปยังเว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่ ทำให้สะดวกต่อการติดตามความคืบหน้าของการแก้ไขช่องโหว่ของทีมทีมรักษาความปลอดภัยของเทคโนโลยีสารสนเทศภาพเปรียบเทียบกระบวนการทำงานเมื่อตรวจพบช่องโหว่ในอดีตกับปัจจุบัน แสดงดังภาพที่ 4.1 และ 4.2 ตามลำดับ

ภาพที่ 4.1 กระบวนการทำงานเมื่อตรวจพบช่องโหว่ในอดีต

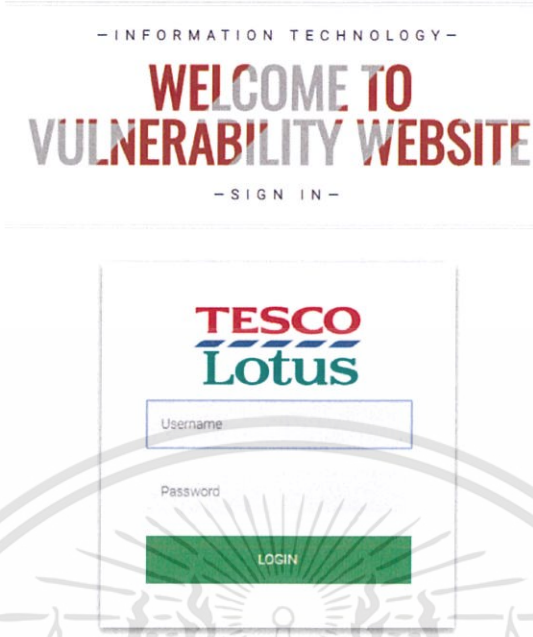


ภาพที่ 4.2 กระบวนการทำงานเมื่อตรวจพบช่องโหว่ในปัจจุบัน

4.2 การเข้าใช้งานและการกำหนดสิทธิ์เพื่อเข้าถึงข้อมูลในเว็บแอปพลิเคชัน

4.2.1 การเข้าใช้งานเว็บแอปพลิเคชัน

การจะเข้างานเว็บแอปพลิเคชันรวมรวมและติดตามผลการแก้ไขช่องโหว่ได้นั้นจะต้องมีการยืนยันตัวตนเพื่อป้องกันการเข้าถึงข้อมูลจากบุคคลภายนอกหรือป้องกันการโจรกรรมข้อมูล และยังใช้สำหรับแบ่งแยกระดับการเข้าถึงข้อมูลต่าง ๆ ในเว็บไซต์ได้อีกเช่นกัน ภาพแสดงหน้ายืนยันตัวตน (Login Page) ของเว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่ แสดงดังภาพที่ 4.3

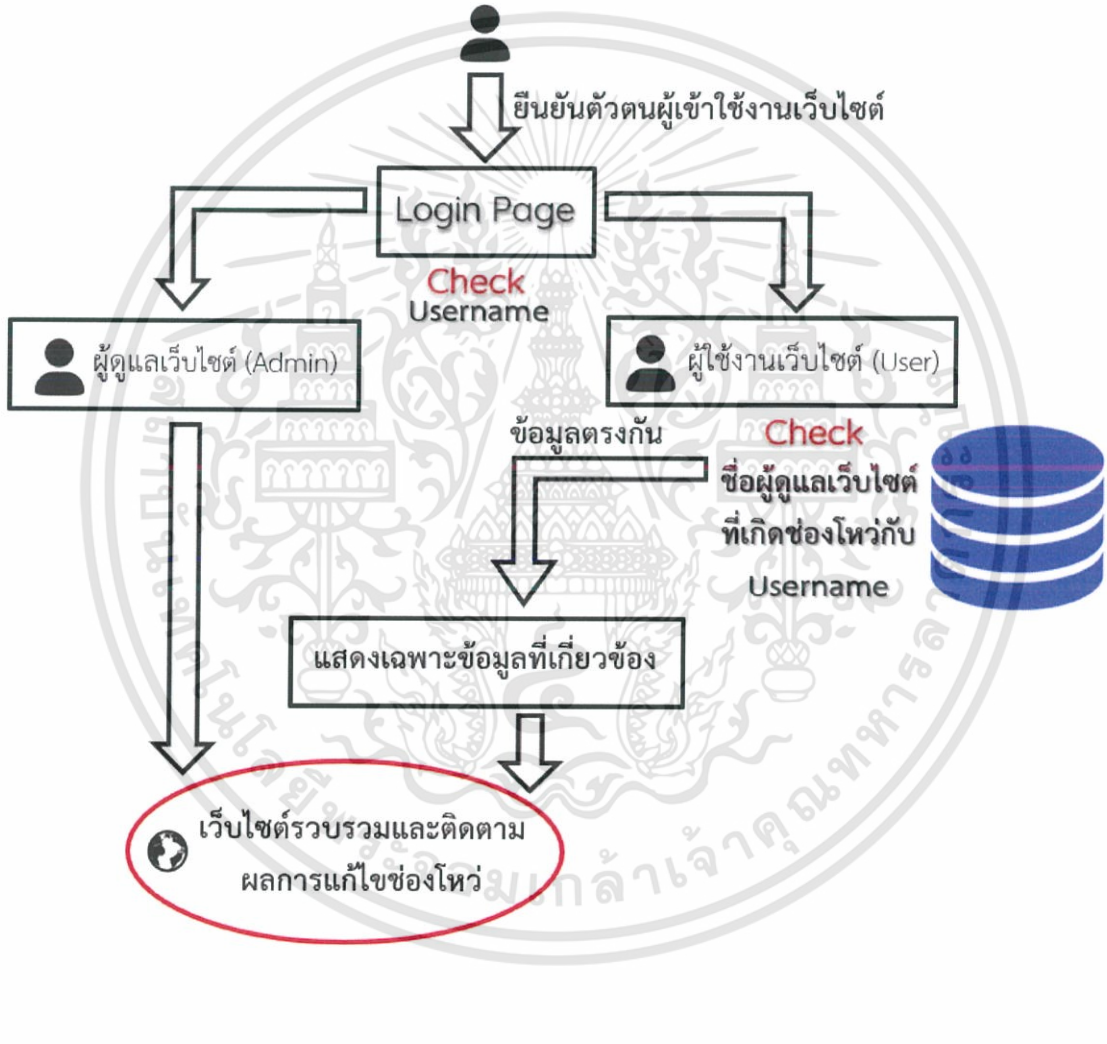


ภาพที่ 4.3 หน้ายืนยันตัวตน (Login Page) ของเว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่

4.2.2 การกำหนดสิทธิ์เพื่อเข้าถึงเว็บแอปพลิเคชัน

การเข้าถึงตัวเว็บแอปพลิเคชันนอกจากจะมีหน้าเพื่อไว้สำหรับยืนยันตัวตนผู้ใช้งานแล้วนั้น จะต้องมีการกำหนดสิทธิ์การเข้าถึงระดับข้อมูลด้วย โดยเว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่ (Vulnerable Monitoring System) มีกระบวนการกำหนดสิทธิ์ ดังนี้ ทีมทีมรักษาความปลอดภัยของเทคโนโลยีสารสนเทศจะเป็นผู้ดูแลเว็บแอปพลิเคชัน (Admin) ที่จะสามารถเข้าดูรายละเอียดของช่องโหว่ทั้งหมดได้ และให้ทีมอื่น ๆ เป็นเพียงผู้ใช้งานเว็บแอปพลิเคชัน (User) ที่จะสามารถเข้าดูได้แค่เฉพาะช่องโหว่ของเว็บไซต์หรือเว็บแอปพลิเคชันที่ตนเป็นผู้ดูแลเท่านั้น โดยก่อนจะเข้าถึงตัวเว็บแอปพลิเคชันได้นั้นผู้ดูแลเว็บแอปพลิเคชันจะเป็นคนจัดการเพิ่มสิทธิ์การเข้าถึงให้ผู้เข้าใช้งานเว็บแอปพลิเคชัน รวมถึงสามารถถอดถอนผู้เข้าใช้งานเว็บแอปพลิเคชันได้เช่นกัน โดยเริ่มแรกผู้ดูแลเว็บแอปพลิเคชันจะสร้างบัญชีผู้ใช้ขึ้นมาโดยกำหนดให้มีชื่อผู้ใช้งาน (Username) ให้อยู่ในรูปแบบของชื่อ.นามสกุล (Name.Surname) และกำหนดรหัสผ่านผู้ใช้งาน (Password) เริ่มต้นให้กับผู้ใช้งานเว็บแอปพลิเคชันหลังจากนั้นจะทำการส่ง ชื่อผู้ใช้งาน และรหัสผ่านผู้ใช้งานให้กับผู้ใช้งานเว็บแอปพลิเคชันแต่ละคนไปทำการตั้งค่าหรือรีเซตรหัสผ่านผู้ใช้งานใหม่ให้เป็นรหัสผ่านผู้ใช้งานของตนเองที่ไม่ให้ผู้อื่นสามารถคาดเดาได้ ส่วนชื่อผู้ใช้งานนั้นจะตั้งค่าให้อยู่ในรูปแบบเดิมเพื่อให้การเข้าใช้งานมีมาตราฐานแบบเดียวกันและง่ายต่อการจัดการการเข้าถึงข้อมูลและแบ่งแยกระดับของผู้ใช้งานเว็บแอปพลิเคชัน เมื่อผู้ใช้งานทำการยืนยันตัวตนผ่านหน้ายืนยันตัวตน เว็บไซต์จะทำตรวจสอบจากชื่อผู้ใช้งานว่า ชื่อ.นามสกุล

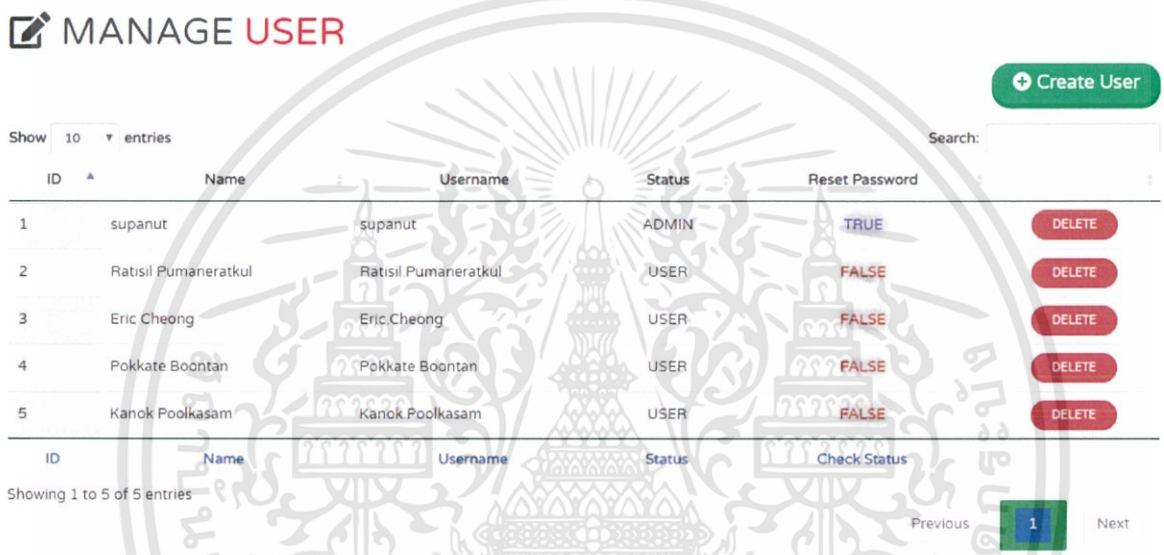
(Name.Surname) ของผู้เข้าใช้งานเว็บแอปพลิเคชันคนนี้ มีสถานะเป็นผู้ดูแลเว็บแอปพลิเคชัน หรือเป็นเพียงผู้เข้าใช้งานธรรมดา ถ้ามีสิทธิ์เป็นผู้ดูแลเว็บแอปพลิเคชันจะสามารถเข้าถึงเว็บแอปพลิเคชันได้ทุกส่วน และถ้าเป็นเพียงผู้ใช้งานธรรมดาเว็บแอปพลิเคชันจะตรวจสอบว่ามีกรณีของช่องโหว่ไหนมีชื่อผู้ดูแลเว็บแอปพลิเคชันที่เกิดช่องโหว่ตรงกับชื่อผู้ใช้งาน ของผู้เข้าใช้งานเว็บแอปพลิเคชันบ้างก็จะเรียกเฉพาะข้อมูลที่เกี่ยวข้องเท่านั้นขึ้นมาแสดงผลให้กับผู้เข้าใช้งานนั้น ๆ ได้ตรวจสอบดูรายละเอียดของข้อมูล มีกระบวนการยืนยันตัวตนผู้เข้าใช้งาน แสดงในภาพที่ 4.4



ภาพที่ 4.4 กระบวนการยืนยันผู้เข้าใช้งานเว็บแอปพลิเคชัน

และผู้พัฒนาเว็บแอปพลิเคชันมีการพัฒนาหน้าจัดการบัญชีผู้ใช้งาน (Manage User Page) ที่สามารถเข้าใช้งานได้เฉพาะผู้ดูแลเว็บแอปพลิเคชันเพื่อใช้สำหรับการเพิ่มหรือถอดถอนสิทธิ์ผู้เข้าใช้งานเว็บแอปพลิเคชัน และยังสามารถตรวจสอบได้อีกว่ารหัสผ่านเริ่มต้นของผู้ใช้งานทำการรีเซตเป็นรหัสผ่านใหม่แล้วหรือไม่ แสดงดังภาพที่ 4.5 จะแบ่งออกเป็น 2 สถานะ คือ

1. สถานะทรู (True) คือ ผู้ใช้งานคนนั้นทำการรีเซตรหัสผ่านแล้ว
2. สถานะเฟาสต์ (False) คือ ผู้ใช้งานคนนั้นยังไม่ได้ทำการรีเซตรหัสผ่าน

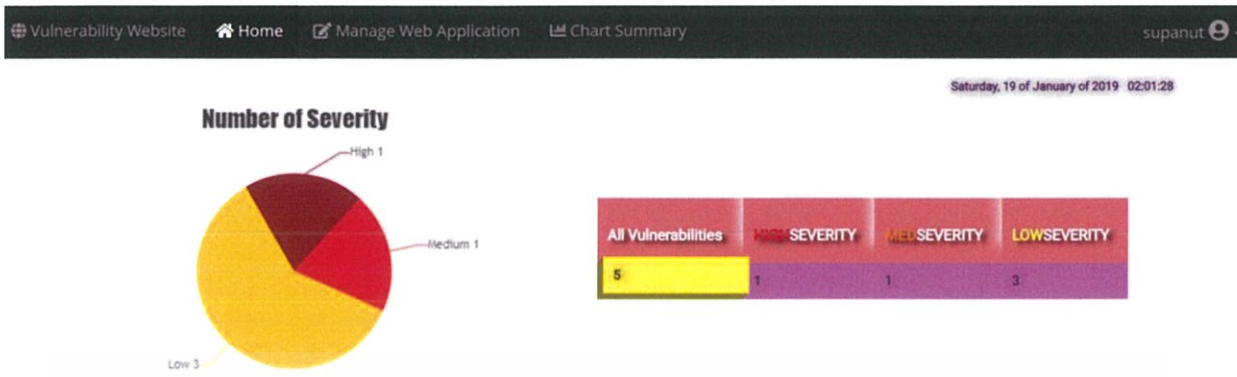


ภาพที่ 4.5 หน้าจัดการบัญชีผู้ใช้งาน (Manage User Page)

4.3 หน้าแสดงผลที่ทำหน้าที่รวบรวมข้อมูลต่าง ๆ

4.3.1 หน้าโฮมเพจ (Home Page)

เมื่อทำการเข้าถึงเว็บแอปพลิเคชันด้วยสิทธิ์ของผู้ดูแลเว็บไซต์ในหน้าโฮมเพจ (Home Page) ของตัวเว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่ จะมีกราฟและตารางแสดงสรุปรายละเอียดต่าง ๆ ของแต่ละช่องโหว่ทั้งหมดที่เกิดขึ้นมา โดยในส่วนที่ 1 จะแสดงจำนวนของเว็บไซต์และเว็บแอปพลิเคชันทั้งหมดที่เกิดช่องโหว่ขึ้นมา ซึ่งช่องโหว่ที่เกิดขึ้นนั้นจะแบ่งออกเป็น 3 ระดับ คือ ช่องโหว่ที่มีความเสี่ยงสูง ช่องโหว่ที่มีความเสี่ยงกลาง และช่องโหว่ที่มีความเสี่ยงต่ำ เพื่อที่จะกำหนดได้ว่าควรแก้ไขช่องโหว่ของเว็บไซต์หรือเว็บแอปพลิเคชันใดก่อน โดยจะเรียงลำดับ คือ ช่องโหว่ที่มีความเสี่ยงสูงจะต้องทำการแก้ไขก่อน ถัดไปจะเป็นระดับกลาง และต่ำตามลำดับ ส่วนที่ 1 ของหน้าโฮมเพจดังแสดงภาพที่ 4.6

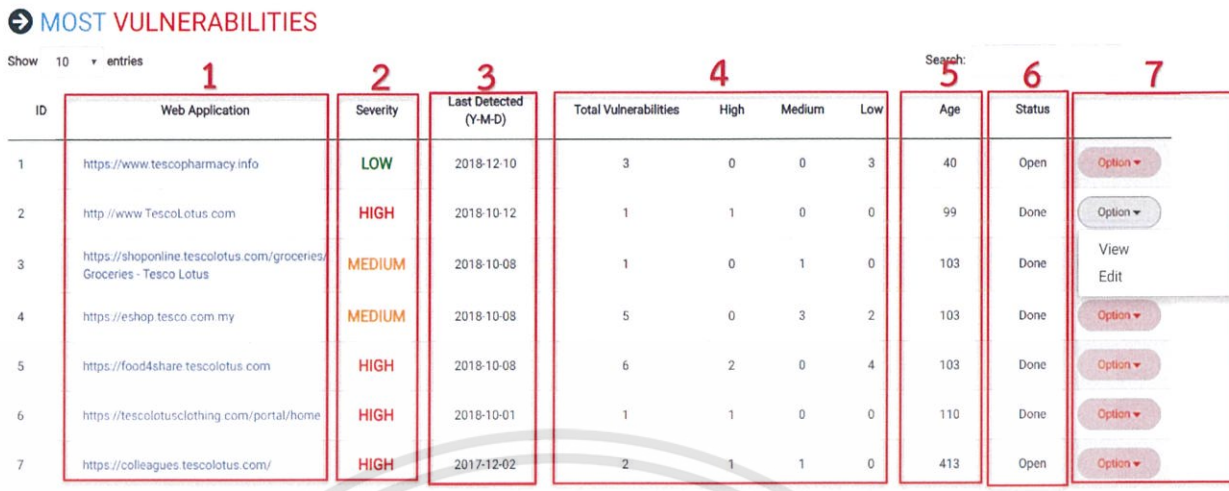


ภาพที่ 4.6 ส่วนที่ 1 ของหน้าโฮมเพจ

และในส่วนที่ 2 จะแสดงรายละเอียดของแต่ละช่องโหว่ โดยจะมีส่วนต่าง ๆ ดังนี้

1. ชื่อเว็บไซต์หรือเว็บแอปพลิเคชันที่เกิดช่องโหว่
2. ระดับความเสี่ยงของช่องโหว่ (สูง/กลาง/ต่ำ)
3. วันที่ตรวจพบช่องโหว่ของเว็บไซต์หรือเว็บแอปพลิเคชันนั้น ๆ
4. จำนวนช่องโหว่ที่เกิดขึ้นภายในหนึ่งเว็บไซต์หรือเว็บแอปพลิเคชัน ซึ่งจำนวนของช่องโหว่ที่เกิดขึ้นภายในเว็บไซต์หรือเว็บแอปพลิเคชันนี้จะแบ่งระดับออกเป็น สูง/กลาง/ต่ำ เช่นเดียวกัน
5. จำนวนวันหลังจากที่ตรวจพบช่องโหว่ของเว็บไซต์หรือเว็บแอปพลิเคชันนั้น ๆ
6. สถานะเพื่อทำการบอกว่าช่องโหว่ของเว็บไซต์หรือเว็บแอปพลิเคชันนี้ได้รับการแก้ไขหรือปิดช่องโหว่เรียบร้อยแล้วหรือไม่ (Open/Done)
7. ปุ่มตัวเลือกเพื่อทำการดูรายละเอียดของช่องโหว่และทำการแก้ไขจำนวนช่องโหว่ที่เกิดขึ้นภายในหนึ่งเว็บไซต์หรือเว็บแอปพลิเคชัน

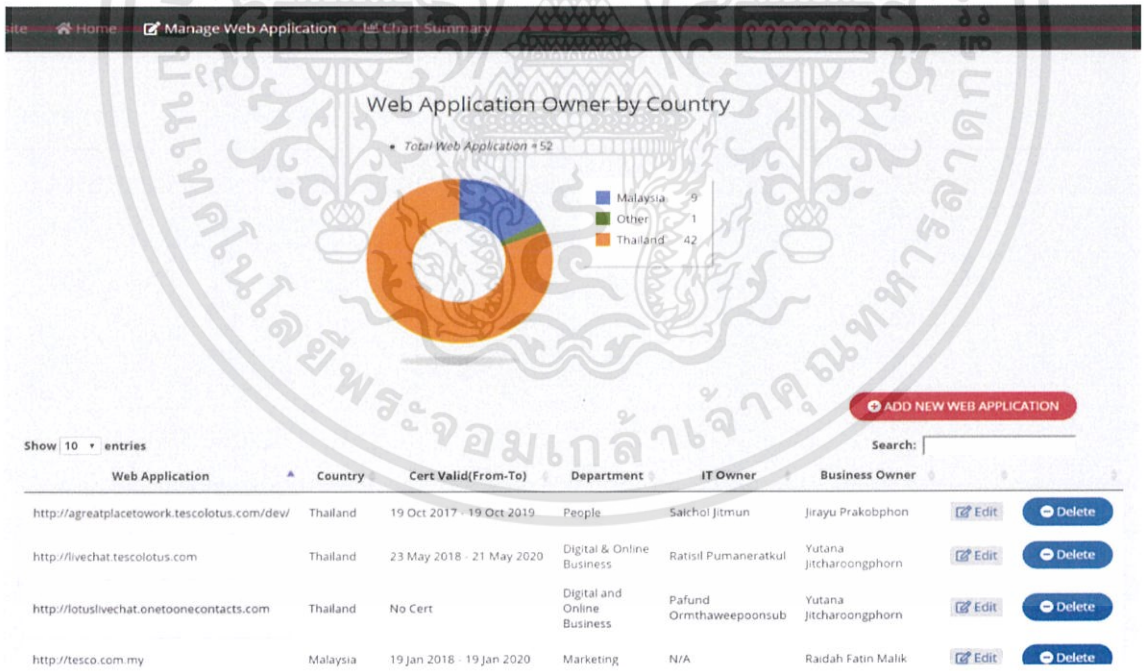
หน้าแสดงผลของแต่ละช่องโหว่ในส่วนที่ 2 ของหน้าโฮมเพจจะมรรายละเอียดแสดงดังภาพที่ 4.7



ภาพที่ 4.7 ส่วนที่ 2 ของหน้าโฮมเพจ

4.3.2 หน้าจัดการเว็บแอปพลิเคชัน (Manage Web Application Page)

เป็นหน้าที่แสดงรายละเอียดของทุกเว็บไซต์และเว็บแอปพลิเคชันที่อยู่ในองค์กร ซึ่งผู้ดูแลเว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่สามารถทำการเพิ่ม ลบ หรือทำการแก้ไขเว็บไซต์และเว็บแอปพลิเคชันภายในองค์กรได้



ภาพที่ 4.8 หน้าจัดการเว็บแอปพลิเคชัน (Manage Web Application Page)

4.3.3 หน้าสรุปผลในรูปแบบกราฟ (Chart Summary Page)

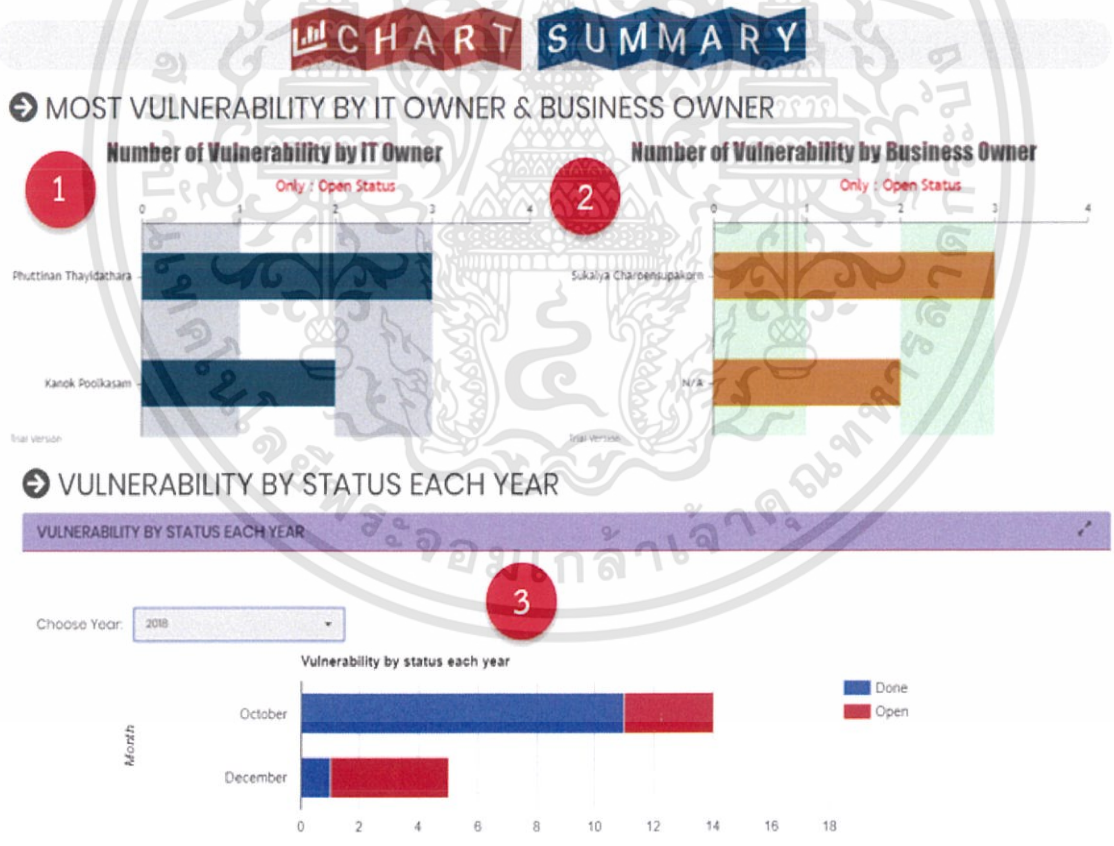
หน้าสรุปผลในรูปแบบกราฟ จะเป็นหน้าที่สรุปรายละเอียดของเว็บไซต์และเว็บแอปพลิเคชันเกิดช่องโหว่แสดงออกมาเป็นกราฟต่าง ๆ โดยจะแบ่งออกเป็น 3 ส่วนดังนี้

1. กราฟแสดงเว็บไซต์และเว็บแอปพลิเคชันที่เกิดช่องโหว่ที่มีผู้ดูแลเว็บไซต์อยู่ภายในแผนกไอที (Information Technology Department)

2. กราฟแสดงเว็บไซต์และเว็บแอปพลิเคชันที่เกิดช่องโหว่ที่มีผู้ดูแลเว็บไซต์หรือเว็บแอปพลิเคชันอยู่ภายในแผนกธุรกิจ (Business Department)

3. กราฟแสดงจำนวนของเว็บไซต์และเว็บแอปพลิเคชันทั้งหมดที่เกิดช่องโหว่ทั้งที่ได้รับการแก้ไขหรือปิดช่องโหว่แล้ว และที่ยังไม่ได้รับการแก้ไขหรือยังเป็นเว็บที่มีช่องโหว่อยู่ โดยจะสามารถเลือกแสดงข้อมูลออกเป็นแต่ปีได้

ภาพแสดงกราฟทั้ง 3 รูปแบบในหน้าสรุปผลในรูปแบบกราฟ แสดงดังภาพที่ 4.9



ภาพที่ 4.9 หน้าสรุปผลในรูปแบบกราฟ

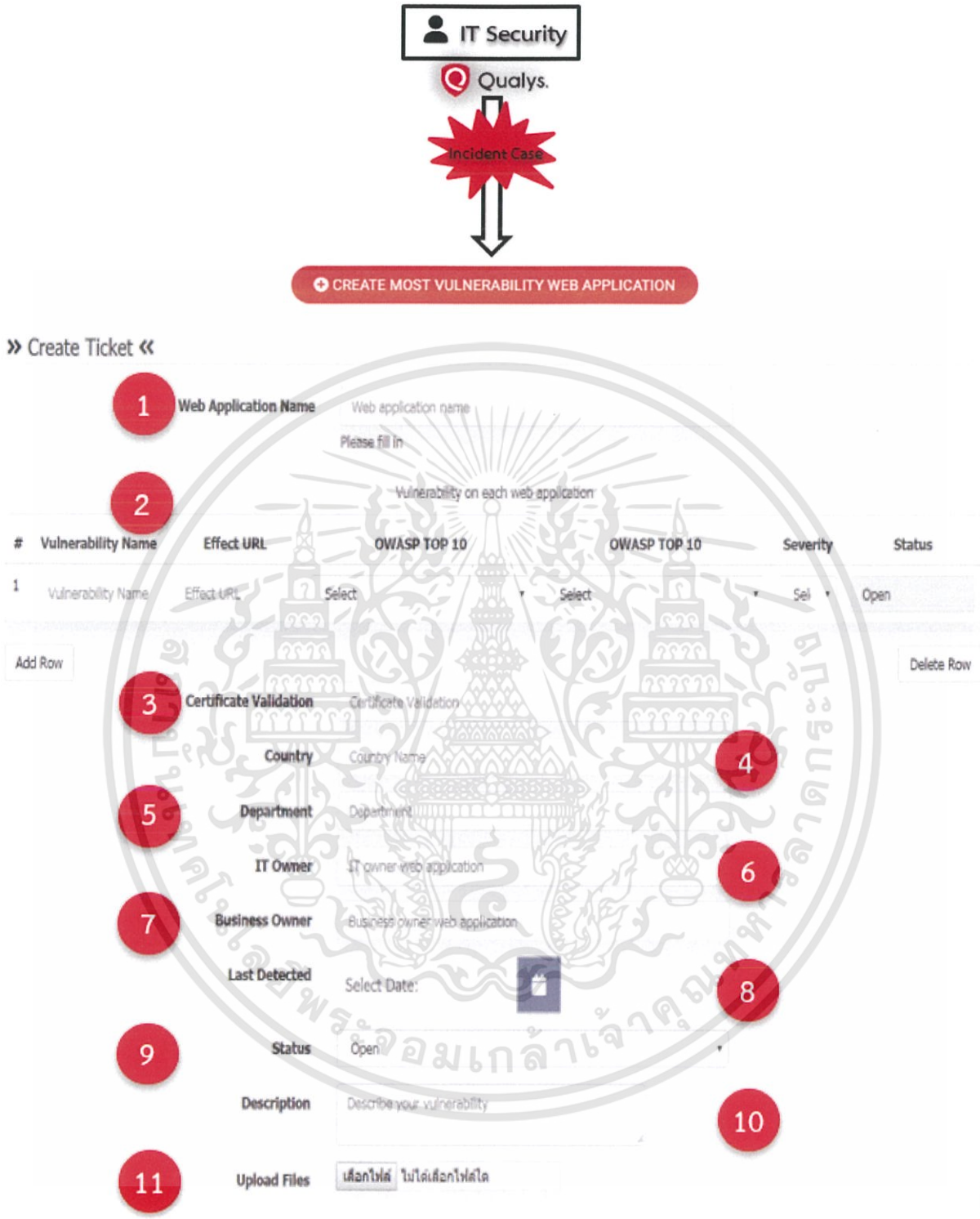
4.4 การสร้างกรณีเว็บไซต์และเว็บแอปพลิเคชันที่เกิดช่องโหว่เข้ามายังเว็บไซต์รวบรวมและติดตามผลการแก้ไขช่องโหว่

เมื่อทีมทีมรักษาความปลอดภัยของเทคโนโลยีสารสนเทศทำการตรวจหาช่องโหว่จากเว็บไซต์และเว็บแอปพลิเคชันทั้งหมดภายในองค์กรโดยการตรวจหาผ่านเครื่องมือควอริช เมื่อตรวจพบช่องโหว่จากเว็บไซต์หรือเว็บแอปพลิเคชันแล้วจะสร้างกรณีเข้าไปยังเว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่ โดยจะทำการกรอกรายละเอียดต่าง ๆ ดังนี้

1. ชื่อของเว็บไซต์หรือเว็บแอปพลิเคชันที่เกิดช่องโหว่
2. รายละเอียดของแต่ละช่องโหว่ที่เกิดขึ้นภายในเว็บไซต์หรือเว็บแอปพลิเคชันนั้น ๆ
3. อายุของใบรับรองเว็บไซต์หรือเว็บแอปพลิเคชัน (วันที่เผยแพร่ - วันหมดอายุ)
4. สังกัดของเว็บไซต์หรือเว็บแอปพลิเคชันว่ามีการใช้งานอยู่ในประเทศใด
5. สังกัดของเว็บไซต์หรือเว็บแอปพลิเคชันว่ามีการใช้งานอยู่ในแผนกใด
6. ชื่อของผู้ดูแลหรือเจ้าของเว็บไซต์และเว็บแอปพลิเคชันภายในแผนกไอที
7. ชื่อของผู้ดูแลหรือเจ้าของเว็บไซต์และเว็บแอปพลิเคชันภายในแผนกธุรกิจ
8. วันที่ตรวจพบช่องโหว่จากเว็บไซต์และเว็บแอปพลิเคชันนั้น ๆ
9. สถานะของเว็บไซต์และเว็บแอปพลิเคชันว่าช่องโหว่นี้ได้รับการแก้ไขหรือปิดช่องโหว่เรียบร้อยแล้วหรือไม่
10. รายละเอียดของช่องโหว่ที่เกิดขึ้น
11. แนบไฟล์เอกสารเกี่ยวกับช่องโหว่ที่เกิดขึ้น

เมื่อทำการกรอกรายละเอียดต่าง ๆ ครบถ้วนแล้ว กรณีของช่องโหว่ที่สร้างขึ้นมานั้นจะไปแสดงผลในส่วนที่ 2 ของหน้าโฮมเพจที่กล่าวไปข้างต้น

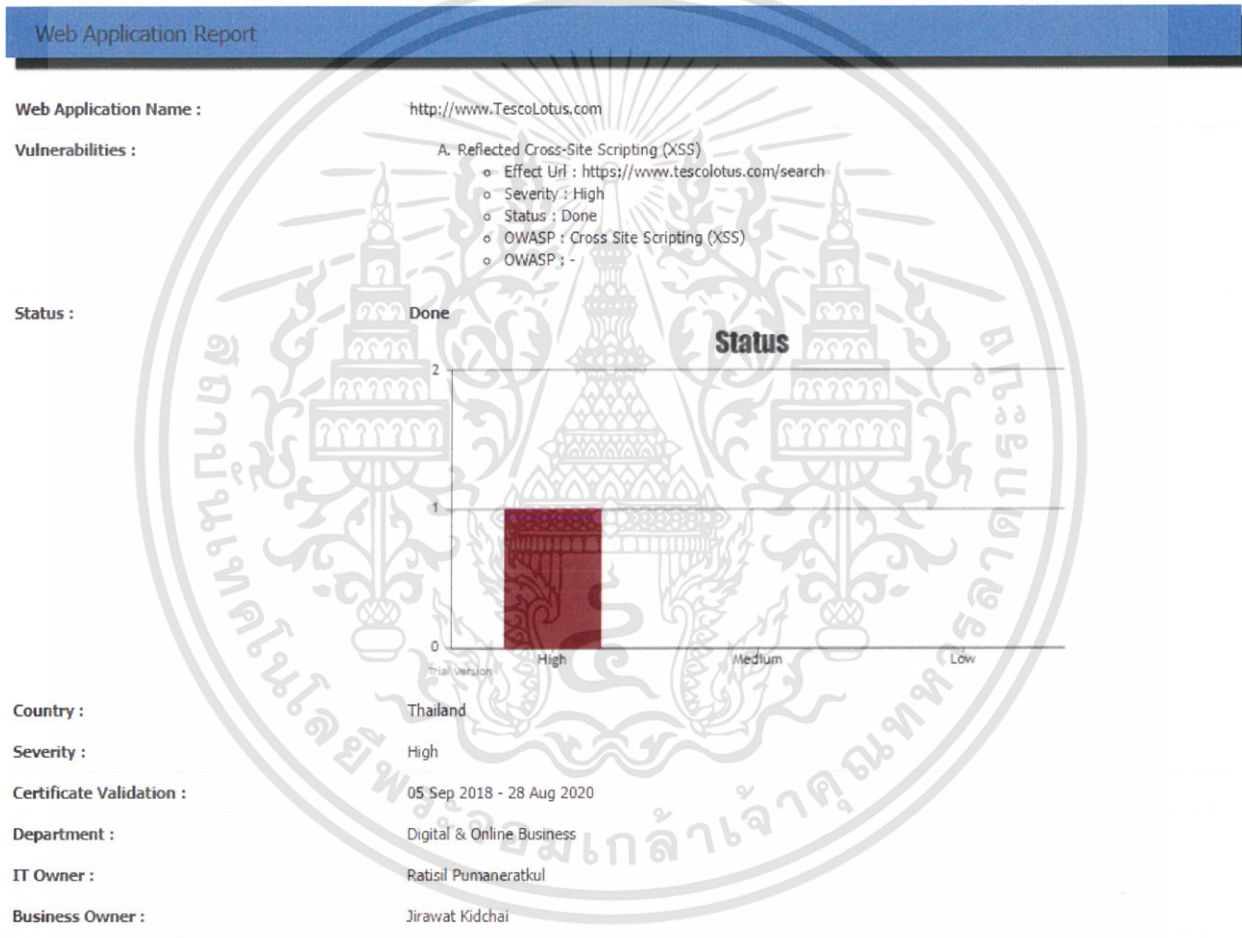
โดยกระบวนการทำงานของการสร้างกรณีของเว็บไซต์และเว็บแอปพลิเคชันที่เกิดช่องโหว่เข้าไปยังเว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่มีขั้นตอนการทำงาน แสดงดังภาพที่ 4.10



ภาพที่ 4.10 การสร้างกรณีของเว็บไซต์และเว็บแอปพลิเคชันที่เกิดช่องโหว่เข้าไปยังเว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่

4.5 หน้าส่วนกลางเพื่อทำการติดต่อกันระหว่างทีม (View Details Page)

หลังจากทีมทีมรักษาความปลอดภัยของเทคโนโลยีสารสนเทศ ทำการสร้างกรณีของเว็บไซต์และเว็บแอปพลิเคชันที่เกิดช่องโหว่เข้าไปยังเว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่ จะต้องทำการติดต่อประสานงานไปยังทีมอื่น ๆ ที่เป็นเจ้าของเว็บไซต์และเว็บแอปพลิเคชันนั้น ๆ ให้เข้ามาดูรายละเอียดของช่องโหว่ที่เกิดขึ้นมา โดยจะมีหน้าที่ใช้สำหรับเป็นส่วนกลางที่จะสามารถให้ทีมทั้งหมดที่เกี่ยวข้องเข้ามาแสดงความคิดเห็นติดต่อกัน ทำการอัพเดทสถานะความคืบหน้าว่ามีการแก้ไขช่องโหว่ที่เกิดไปถึงขั้นตอนใด แสดงดังภาพที่ 4.11 และ 4.12 ตามลำดับ



ภาพที่ 4.11 หน้าส่วนกลางเพื่อทำการติดต่อกันระหว่างทีม (1)

Date : ▪ **Create :**	**D-M-Y** 12-10-2018
URL :	LINK TO QUALYS
Download file :	**Files Name** QualysReportTescoLotus.com 12.10.61.pdf

Details

COMMENTS

Ratisil.Pumaneratkul : 2019-01-28 00:53:29
Comment A

supanut : 2019-01-28 00:54:46
Comment B

supanut : 2019-01-28 00:55:53
Comment C link

Ratisil.Pumaneratkul : 2019-01-28 01:01:58

- **Comment D**
-
-
-

1
2
3

ADD A COMMENT :

Type something

Comment

ภาพที่ 4.122 หน้าส่วนกลางเพื่อทำการติดต่อกันระหว่างทีม (2)

บทที่ 5

สรุปผลการวิจัยและข้อเสนอแนะ

5.1 สรุปผลการวิจัย

จากผลการวิจัยพบว่าหลังจากนำเว็บแอปพลิเคชันรวบรวมและติดตามผลการแก้ไขช่องโหว่ (Vulnerable Monitoring System) เข้ามาใช้งานแทนการทำงานในอดีต พบว่าสามารถช่วยแก้ปัญหาเดิมที่มีอยู่ได้ โดยทำให้ทีมทีมรักษาความปลอดภัยของเทคโนโลยีสารสนเทศ (IT Security) สะดวกต่อการติดต่อสื่อสารกับทีมอื่น ๆ อีกทั้งยังสามารถแก้ไขช่องโหว่ได้รวดเร็วยิ่งขึ้นกว่าในอดีต ซึ่งเป็นผลดีกับองค์กรในการป้องกันการโจรกรรมข้อมูลที่อาจจะเกิดขึ้นได้ และยังสะดวกต่อการเข้ามาติดตามรายละเอียดของผู้เข้าใช้งานเว็บแอปพลิเคชันโดยมีหน้าแสดงผลข้อมูลต่าง ๆ ที่ชัดเจน ทำให้ได้รับข้อมูลที่ครบถ้วน

ดังนั้นเว็บแอปพลิเคชันนี้จึงเป็นโปรเจคที่ถูกคิดค้นเพื่อเข้ามาช่วยในการแก้ปัญหาเดิมที่เคยมีมาให้มีการทำงานในปัจจุบันที่ดี สะดวกต่อการใช้งานและมีประสิทธิภาพยิ่งขึ้น

5.2 ปัญหาที่พบระหว่างการดำเนินงาน

- ในการออกแบบเว็บแอปพลิเคชันให้กับองค์กรนั้น เมื่อนำไปเสนอกับผู้ที่จะใช้งานนั้นยังไม่ตรงตามความต้องการของผู้ใช้ ทำให้ต้องทำการออกแบบใหม่หลายครั้ง และต้องใช้เวลาในการออกแบบนาน

- การรวบรวมข้อมูลต่าง ๆ ที่จะนำมาใช้พัฒนาเว็บแอปพลิเคชันนั้นทำได้ยาก เช่น การหาข้อมูลเกี่ยวกับชื่อผู้ดูแลเว็บไซต์หรือเว็บแอปพลิเคชัน การแยกว่าเว็บไซต์มีขอบเขตการใช้งานอยู่ในประเทศใด เป็นต้น

5.3 วิธีการแก้ไขปัญหาที่พบระหว่างการดำเนินงาน

- ทำการหาข้อตกลงในการออกแบบระหว่างผู้พัฒนาเว็บแอปพลิเคชันกับผู้ใช้งาน ให้อยู่ในขอบเขตที่ทั้ง 2 ฝ่ายสามารถยอมรับได้

- ทำการขอความร่วมมือกับผู้ที่เกี่ยวข้องทั้งหมดในการช่วยหาข้อมูล

5.4 ข้อเสนอแนะ

- อยากให้มีการลงมือปฏิบัติงานจริงในชั้นเรียนมากขึ้น เนื่องจากส่วนใหญ่นักศึกษามักจะได้เรียนรู้เฉพาะทฤษฎีแต่เมื่อไปทำงานจริงนักศึกษาจะขาดทักษะด้านการปฏิบัติ

- อยากให้ทางหลักสูตรมีการพานักศึกษาไปเข้าร่วมกับสถานที่วิจัยต่าง ๆ เพื่อจะได้ศึกษาเกี่ยวกับเทคโนโลยีใหม่ ๆ และได้ฝึกประสบการณ์นอกจากในชั้นเรียน

เอกสารอ้างอิง

[1] “บทเรียนออนไลน์” [ออนไลน์] เข้าถึงได้จาก

https://www.mindphp.com/

(วันที่ค้นหาข้อมูล 1 ธันวาคม 2561)

[2] “OWASP Top 10 ฉบับปี 2017” [ออนไลน์] เข้าถึงได้จาก

https://www.techtalkthai.com/

(วันที่ค้นหาข้อมูล 1 ธันวาคม 2561)

[3] “Qualys Cloud Platform” [ออนไลน์] เข้าถึงได้จาก

https://www.qualys.com/

(วันที่ค้นหาข้อมูล 1 ธันวาคม 2561)

[4] “SQL Server - Views” [ออนไลน์] เข้าถึงได้จาก

www.quackit.com

(วันที่ค้นหาข้อมูล 1 ธันวาคม 2561)

[5] “OWASP Top 10 ฉบับปี 2017 ล่าสุด เปิดให้ดาวน์โหลดเวอร์ชัน RC แล้ว” [ออนไลน์] เข้าถึงได้จาก

www.techtalkthai.com

(วันที่ค้นหาข้อมูล 1 ธันวาคม 2561)

เอกสารอ้างอิง (ต่อ)

[6] "Cloud Computing Architecture" [ออนไลน์] เข้าถึงได้จาก

www.conceptdraw.com

(วันที่ค้นหาข้อมูล 1 ธันวาคม 2561)

[7] "Visualize and document your web app security status with actionable data" [ออนไลน์] เข้าถึงได้จาก

https://www.qualys.com/

(วันที่ค้นหาข้อมูล 1 ธันวาคม 2561)

[8] "Qualys Web Application Scanner (WAS)" [ออนไลน์] เข้าถึงได้จาก

https://www.acinfotec.com/

(วันที่ค้นหาข้อมูล 1 ธันวาคม 2561)

[9] "รู้จักกับ OWASP TOP 10" [ออนไลน์] เข้าถึงได้จาก

https://blog.tamacorp.co/

(วันที่ค้นหาข้อมูล 1 ธันวาคม 2561)

[10] "กระบวนการพัฒนาเว็บไซต์" [ออนไลน์] เข้าถึงได้จาก

https://sites.google.com/

(วันที่ค้นหาข้อมูล 1 ธันวาคม 2561)