**แนวทางการป้องกันการโจมตีข้อมูลจากเอสคิวแอลอินเจคชันด้วยการกำหนดสิทธิ์การเข้าถึงข้อมูล**

**An Approach to Prevent SQL Injection Attacks Using Granting Permissions**

*ธนากร จงใจงาม (thanakorn jongjaingam)1 กรวีร์ เหล่าศรี (korawee laosri)2*

*ฉัตรบุศ ตระกูลนิ่มนวล (chattabut trakulnimnual)3และชุมพล โมฆรัตน์ (Chumpol Mokarat)4*

*สาขาวิชาเทคโนโลยีสารสนเทศ คณะบริหารธุรกิจและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก*

*1thanakorn.jon@rmutto.ac.th 2korawee.lao@rmutto.ac.th 3chattabut.tra@rmutto.ac.th 4chumpol\_mo@rmutto.ac.th*

**คำสำคัญ:** แอปพลิเคชันการเช่ารถ, กำหนดสิทธิ์การเข้าถึงข้อมูล, ความมั่นคงปลอดภัยของข้อมูล, เอสคิวแอลอินเจคชัน

**วัตถุประสงค์การดำเนินงาน :**

1.เพื่อควบคุมการเข้าถึงของผู้ใช้งาน หรือกำหนดสิทธิ์การใช้งานเพื่อเข้าถึงข้อมูล

2.เพื่อรักษาความปลอดภัยของฐานข้อมูลและป้องกันข้อมูลที่เป็นความลับ

3.เพื่อลดความเสี่ยงความเสียหายของข้อมูลจากการโดน Hack

4.เพื่อศึกษาการโจมตีข้อมูลและวิธีการป้องกันการโจมตีข้อมูลในรูปแบบ SQL Injection

**1.บทนำ**

การให้บริการเดิมของเต๊นท์เช่ารถยนต์คือ เมื่อลูกค้าจะทำการเช่ารถยนต์ในแต่ละครั้ง จะต้องมาดูรถที่เต๊นท์รถด้วยตัวเองซึ่งอาจมีระยะทางและค่าเดินทางค่อนข้างมากหากอยู่ไกล และเมื่อต้องการเช่าต้องเตรียมเอกสารมากมายเช่น บัตรประชาชน ใบอนุญาตขับขี่ หรือเอกสารต่างๆมาให้ทางร้าน ซึ่งบางครั้งหากเตรียมเอกสารไม่ครบจะทำให้เสียเวลาในการกลับไปเอาเอกสาร การเก็บเอกสารจำนวนมากมีความเสี่ยงที่เอกสารสำคัญจะสูญหายหรือยากต่อการค้นหาข้อมูลในแต่ละครั้ง และการเช่านั้นจะต้องมีพนักงานในการบริการ ซึ่งการบริการแต่ละครั้งก็จะต้องใช้พนักงานหนึ่งต่อลูกค้าหนึ่งคน ทำให้มีพนักงานไม่เพียงพอทำให้เกิดปัญหาความล่าช้าในการให้บริการกับลูกค้าเช่ารถยนต์ พนักงาน 1 คนได้ทำการเช่ารถยนต์หลายครั้ง จึงทำให้เกิดการสับสนหรือปัญหาในเรื่องของการให้เช่ารถผิดคัน จะเห็นได้ว่าการทำงานในระบบเดิมนั้นจะใช้แรงงานคนในทุกขั้นตอนการทำงาน

[ย่อหน้าที่ 2 ควรเพิ่มการอธิบายเกี่ยวกับการกำหนดสิทธิ์การเข้าถึงข้อมูล, ความมั่นคงปลอดภัยของข้อมูลและเอสคิวแอลอินเจคชันในภาพรวม ตลอดจนข้อดี/เสียประกอบด้วย]

รายงานการศึกษานี้จึงได้พัฒนาระบบเพื่อนำไปช่วยสนับสนุนการเช่ารถยนต์ของเต๊นท์เช่ารถให้มีประสิทธิภาพมากยิ่งขึ้น ข้อมูลทั้งหมดจะถูดจัดเก็บไว้ภายในฐานข้อมูล เพื่อสะดวกต่อการนำข้อมูลมาใช้งาน เพื่อป้องกันการเข้าถึงข้อมูลที่เป็นข้อมูลลับจึงต้องกำหนดสิทธิ์การเข้าถึงข้อมูลให้ผู้ใช้งานผ่านการเข้ารหัสผ่านและอีเมล

การโจมตี SQL Injection เกิดจากช่องรับข้อมูลต่างๆของเว็บเพจไม่สมบูรณ์จึงเป็นจุดอ่อนหรือช่องโหว่ที่Hackerสามารถส่ง SQL Injection เข้ามาในช่องรับข้อมูลเพื่อโจมตีข้อมูล จึงทำการศึกษาวิธีการโจมตีของ และวิธีการป้องกันข้อมูล

[ย่อหน้าที่ 3 สรุปการดำเนินงานจะทำอะไร ด้วยเครื่องมือใดและแก้ปัญหาใดแบบกระชับ]

ดังนั้น เพื่อเป็นการแก้ไขปัญหาดังกล่าวผู้ศึกษาจึงเห็นถึงปัญหาที่เกิดขึ้น และแนวทางในการแก้ไขปัญหา

**2.ทฤษฎีที่เกี่ยวข้อง (\*ปรับแก้อีกครั้งควรเพิ่มการอธิบายในแต่ละทฤษฎี ระบุเอกสารอ้างอิงทุก ๆ ทฤษฎีที่เกี่ยวข้องและเพิ่มเติมทฤษฎีอื่น สรุปให้กระชับ สามารถเพิ่มรูปภาพประกอบการอธิบาย รวมถึงยกตัวอย่างประกอบด้วยจะดีมาก)**

**2.1 การกำหนดสิทธิ์ [1]**

2.1.1 สิทธิ์หมายถึง อำนาจที่กฎหมายรับรองให้กระทำการใด ๆ โดยสุจริตได้อย่างอิสระ แต่ต้องไม่กระทบกระเทือนถึงสิทธิของคนอื่น

2.1.2 สำนักงานราชบัณฑิตสภา (๒๗ มิถุนายน ๒๕๕๔) ให้ความหมายสิทธิว่า อำนาจที่จะกระทำการใดๆ ได้อย่างอิสระ โดยการรับรองจากกฎหมาย สิทธิ มีความหมายเหมือนคำว่าสิทธิ์ มักใช้ในภาษากฎหมาย หรือใช้ควบคู่กับคำอื่น เช่น สิทธิเสรีภาพ สิทธิและหน้าที่

2.1.3 การกำหนดสิทธิ์การเข้าถึง หมายถึง การควบคุมการเข้าถึงของผู้ใช้งานเพื่อควบคุมการเข้าถึงของผู้ใช้งาน หรือปิดสิทธิ์ไม่ใช้ผู้ใช้งานเห็นข้อมูลนั้นๆ ผ่านการเข้ารหัสผ่าน การกำหนดขึ้นอยู่กับบทบาทของแต่ละบุคคล

**2.2 ความมั่นคงปลอดภัยของข้อมูล [2]**

**2.2.1 ความมั่นคงปลอดภัย (Security)** คือ สถานะที่มีความปลอดภัย ไร้กังวล อยู่ในสถานะที่ไม่มีอันตรายและได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือบังเอิญ

2.2.2  **การรักษาความมั่นคงปลอดภัยของสารสนเทศ (Information Security)** คือผลที่เกิดขึ้นจาการใช้ระบบของนโยบาย หรือ ระเบียบปฏิบัติที่ใช้ในการพิสูจน์ทราบ  ควบคุม และป้องกันการเปิดเผยข้อมูล (ที่ได้รับคำสั่งให้มีการป้องกัน) โดยไม่ได้รับอนุญาต

2.2.3 **ภัยคุกคาม (Threat)** คือ วัตถุ สิ่งของ ตัวบุคคล หรือสิ่งอื่นใดที่เป็นตัวแทนของการกระทำอันตรายต่อทรัพย์สินขององค์กร หรือสิ่งที่อาจจะก่อให้เกิดเสียหายต่อคุณสมบัติของข้อมูลด้านใดด้านหนึ่งหรือมากกว่าหนึ่งด้าน ความลับ (Confidentiality), ความสมบูรณ์ (Integrity), ความพร้อมใช้ (Availability)

**2.3 องค์ประกอบของความมั่นคงปลอดภัยของข้อมูล [3]**

1. ความลับ Confidentiality เป็นการรับประกันว่าผู้มีสิทธิ์และได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ องค์กรต้องมีมาตรการป้องกันการเข้าถึงสารสนเทศที่เป็นความลับ เช่น การจัดประเภทของสารสนเทศ การรักษาความปลอดภัยในกับแหล่งจัดเก็บข้อมูล   กำหนดนโยบายรักษาความมั่นคงปลอดภัยและนำไปใช้ให้การศึกษาแก่ทีมงานความมั่นคงปลอดภัยและผู้ใช้

2.ความสมบูรณ์ Integrity  ความสมบูรณ์ คือ ความครบถ้วน ถูกต้อง และไม่มีสิ่งแปลกปลอม สารสนเทศที่มีความสมบูรณ์จึงเป็นสารสนเทศที่นำไปใช้ประโยชน์ได้อย่างถูกต้องครบถ้วน  สารสนเทศจะขาดความสมบูรณ์ ก็ต่อเมื่อสารสนเทศนั้นถูกนำไปเปลี่ยนแปลง ปลอมปนด้วยสารสนเทศอื่น ถูกทำให้เสียหาย ถูกทำลาย หรือถูกกระทำในรูปแบบอื่น ๆ เพื่อขัดขวางการพิสูจน์การเป็นสารสนเทศจริง

3.ความพร้อมใช้ Availability  ความพร้อมใช้ หมายถึง สารสนเทศจะถูกเข้าถึงหรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้หรือระบบอื่นที่ได้รับอนุญาตเท่านั้น หากเป็นผู้ใช้หรือระบบที่ไม่ได้รับอนุญาต การเข้าถึงหรือเรียกใช้งานจะถูกขัดขวางและล้มเหลงในที่สุด

4.ความถูกต้องแม่นยำ Accuracy  ความถูกต้องแม่นยำ หมายถึง สารสนเทศต้องไม่มีความผิดพลาด และต้องมีค่าตรงกับความคาดหวังของผู้ใช้เสมอ เมื่อใดก็ตามที่สารสนเทศมีค่าผิดเพี้ยนไปจากความคาดหวังของผู้ใช้ ไม่ว่าจะเกิดจากการแก้ไขด้วยความตั้งใจหรือไม่ก็ตาม เมื่อนั้นจะถือว่าสารสนเทศ “ไม่มีความถูกต้องแม่นยำ”

5.เป็นของแท้ Authenticity สารสนเทศที่เป็นของแท้ คือ สารสนเทศที่ถูกจัดทำขึ้นจากแหล่งที่ถูกต้อง ไม่ถูกทำซ้ำโดยแหล่งอื่นที่ไม่ได้รับอนุญาต หรือแหล่งที่ไม่คุ้นเคยและไม่เคยทราบมาก่อน   เทศที่เป็นของแท้ คือ สารสนเทศที่ถูกจัดทำขึ้นจากแหล่งที่ถูกต้อง ไม่ถูกทำซ้ำโดยแหล่งอื่นที่ไม่ได้รับอนุญาต หรือแหล่งที่ไม่คุ้นเคยและไม่เคยทราบมาก่อน

6.ความเป็นส่วนตัว Privacy ความเป็นส่วนตัว คือ สารสนเทศที่ถูกรวบรวม เรียกใช้ และจัดเก็บโดยองค์กร จะต้องถูกใช้ในวัตถุประสงค์ที่ผู้เป็นเข้าของสารสนเทศรับทราบ ณ ขณะที่มีการรวบรวมสารสนเทศนั้น มิฉะนั้นจะถือว่าเป็นการละเมิดสิทธิส่วนบุคคลด้านสารสนเทศ

**2.4 องค์ประกอบของระบบสารสนเทศกับความมั่นคงปลอดภัย [3]**

Softwareย่อมต้องอยู่ภายใต้เงื่อนไขของการบริหารโครงการ ภายใต้เวลา ต้นทุน และกำลังคนที่จำกัด ซึ่งมักจะทำภายหลังจากการพัฒนาซอฟต์แวร์เสร็จแล้ว

Hardware จะใช้นโยบายเดียวกับสินทรัพย์ที่จับต้องได้ขององค์กร คือการป้องกันจากการลักขโมยหรือภัยอันตรายต่าง ๆ รวมถึงการจัดสถานที่ที่ปลอดภัยให้กับอุปกรณ์หรือฮาร์ดแวร์

Data  ข้อมูล/สารสนเทศ เป็นทรัพยากรที่มีค่าขององค์กร การป้องกันที่แน่นหนาก็มีความจำเป็นสำหรับข้อมูลที่เป็นความลับ ซึ่งต้องอาศัยนโยบายความปลอดภัยและกลไกป้องกันที่ดีควบคู่กัน

People  บุคลากร คือภัยคุกคามต่อสารสนเทศที่ถูกมองข้ามมากที่สุด  โดยเฉพาะบุคลากรที่ไม่มีจรรยาบรรณในอาชีพ ก็เป็นจุดอ่อนต่อการโจมตีได้ จึงได้มีการศึกษากันอย่างจริงจัง เรียกว่า Social Engineering ซึ่งเป็นการป้องการการหลอกหลวงบุคลากร เพื่อเปิดเผยข้อมูลบางอย่างเข้าสู่ระบบได้

Procedure  ขั้นตอนการทำงาน เป็นอีกหนึ่งองค์ประกอบที่ถูกมองข้าม  หากมิจฉาชีพทราบขั้นตอนการทำงาน ก็จะสามารถค้นหาจุดอ่อนเพื่อนกระทำการอันก่อนให้เกิดความเสียหายต่อองค์กรและลูกค้าขององค์กรได้

Network  เครือข่ายคอมพิวเตอร์  การเชื่อมต่อระหว่างคอมพิวเตอร์และระหว่างเครือข่ายคอมพิวเตอร์ ทำให้เกิดอาชญากรรมและภัยคุกคามคอมพิวเตอร์ โดยเฉพาะการเชื่อมต่อระบบสารสนเทศเข้ากับเครือข่ายอินเตอร์เน็ต

**2.5 SQL Injection [4]**

2.5.1 SQL Injection (SQLi) เป็นการโจมตีแบบฉีดซึ่งผู้โจมตีดำเนินการคำสั่ง SQL ที่เป็นอันตรายเพื่อควบคุมเซิร์ฟเวอร์ฐานข้อมูลของเว็บแอปพลิเคชัน ดังนั้นจึงเข้าถึง แก้ไข และลบข้อมูลที่ไม่ได้รับอนุญาต

2.5.2 แนวคิดเกี่ยวกับการโจมตีเว็บไซต์ด้วยวิธี SQL Injection

การอาศัยช่องโหว่และข้อผิดพลาดของโปรแกรมเมื่อ Hacker ได้ส่งคำสั่ง SQL interpreter ซึ่งทำการ Compile ของโปรแกรมทีละบรรทัดลงมาเรื่อยๆ เป็นส่วนหนึ่งของ SQL คิวรี่ที่เรียกใช้งานในหน้าเว็บไซต์ที่มีการรับข้อมูล ถ้าเจอ error ก็จะแจ้งกับมาทันทีทางหน้า เว็บไซต์ที่เรียกใช้งานเพื่อเปลี่ยนแปลงรูปแบบการโจมตี SQL Injection รูปแบบต่างๆ ให้ เหมาะสมสำหรับหน้าเว็บไซต์นั้นให้ได้สิทธิผู้ดูแลระบบสามารถแก้ไข เพิ่ม ลบ ข้อมูลได้

2.5.3 รูปแบบการโจมตี SQL Injection

ผู้โจมตีจะค้นหารูปแบบ Input ของผู้ใช้ที่มีช่องโหว่ภายใน Web Application ก่อน หลังจากนั้นผู้โจมตี จะส่ง Input ที่มีรูปแบบที่ถูกต้องตรงเข้าไปที่ Database โดยไม่ต้องผ่านหน้า Web application ปกติซึ่งถ้าทำได้ ผู้โจมตีจะสามารถส่ง คำสั่ง SQL ที่เป็นอันตรายจะถูกดำเนินการในฐานข้อมูล

* ผู้โจมตีสามารถ ปลอมตัวเป็น Admin หรือ User คนอื่นได้
* ผู้โจมตีจะเข้าถึงข้อมูลทั้งหมดได้อย่างสมบูรณ์
* สามารถปรับเปลี่ยนตัวเลขทางบัญชีทั้งหมดในระบบ

2.5.4 การรักษาความปลอดภัยและปกป้องข้อมูล

การรักษาความปลอดภัยทางไซเบอร์ทำงานเหมือนกับการรักษาความปลอดภัยแบบออฟไลน์ทั่วไป กล่าวคือ มีวัตถุประสงค์เพื่อให้ผู้ใช้และระบบคอมพิวเตอร์ปลอดภัย อาชญากรรมไซเบอร์ได้รับแรงจูงใจจากเงินและนำไปสู่วิธีการต่างๆมากมายในการทำให้ผู้ใช้บริการสูญเสียเงิน ในบางกรณี อาจทำได้ง่ายๆ เพียงแค่กำหนดเป้าหมายบัญชีธนาคารของคุณ ในกรณีอื่นๆ

**3.งานวิจัยที่เกี่ยวข้อง (\*ปรับแก้อีกครั้งควรระบุเอกสารอ้างอิงทุก ๆ งานวิจัย และอย่างน้อยควรมี 3 งานวิจัย สรุปให้กระชับ)**

**แววตา เตชาทวีวรรณ (2020) [x]** ได้ศึกษาเกี่ยวกับความมั่นคงปลอกภัยของสารสนเทศที่สำคัญของห้องสมุด เพื่อศึกษาสภาพและปัญหาความมั่นคงปลอดภัยของระบบสารสนเทศ ตาม “แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553” ของห้องสมุดอุดมศึกษาของรัฐ โดยงานวิจัยระยะที่1 ซึ่งใช้วิธีวิจัยเชิงคุณภาพแบบวิธีศึกษาเฉพาะกรณี แบบมุ่งการค้นหา พบว่า ห้องสมุด สถาบันอุดมศึกษาของรัฐให้ความสําคัญต่อการรักษาความมั่นคงปลอดภัยระบบสารสนเทศโดยมีการปฏิบัติแนวทางในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้สามารถดําเนินการต่าง ๆ ด้วยวิธีทางอิเล็กทรอนิกส์ โดยอาศัยอำนาจตามความในมาตรา 5 มาตรา 7 และมาตรา 8 แห่งพระราชกฤษฎีกากําหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ที่กําหนดให้มีผลโดยชอบด้วยกฎหมายนโยบายรักษาความมั่นคงระบบสารสนเทศถูกกําหนดอย่างเป็นลายลักษณ์อักษรโดยห้องสมุดหรือสํานัก คอมพิวเตอร์ของมหาวิทยาลัยเพื่อให้บุคลากรทุกคนปฏิบัติตาม ห้องสมุดสถาบันอุดมศึกษาของรัฐกําหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ การบริหารจัดการ การเข้าถึงระบบสารสนเทศของผู้ใช้งาน และการควบคุมการเข้าถึงเครือข่าย โดยกําหนดสิทธิและระดับของบุคคล ทั้งทางกายภาพและทางอิเล็กทรอนิกส์ เนื่องจากระบบสารสนเทศประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์ ฐานข้อมูล เครือข่าย และบุคคล (Zwass, 2020) การดําเนินธุรกรรมต่าง ๆ ผ่านระบบเครือข่ายที่เชื่อมโยงเครื่องคอมพิวเตอร์ แม่ข่ายกับเครื่องลูกข่าย ซึ่งมีห้องควบคุมส่วนกลางที่จัดวางเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่าง ๆ จึงต้องมีการป้องกันการเข้าถึงอุปกรณ์ต่าง ๆ โดยอนุญาตเฉพาะผู้ที่เกี่ยวข้องเข้าถึงอุปกรณ์ต่าง ๆ ได้ โดยกําหนดกฎระเบียบและใช้อุปกรณ์ป้องกันบุคคลอื่นเข้าถึงโดยไม่ได้รับอนุญาต นอกจากนี้การคุกคามทางระบบเครือข่ายสามารถกระทําได้โดยแฮคเกอร์ (Hacker) ซึ่งกระทําได้หลายรูปแบบ ได้แก่ การขโมยข้อมูล ทําให้ข้อมูล เสียหาย หรือรบกวนการทํางาน โดยใช้ซอฟต์แวร์ เช่น ไวรัสคอมพิวเตอร์ มัลแวร์ (Malware) รันซัมแวร์ (Ransomware) สนิฟเฟอร์ (Sniffer) เป็นต้น ผู้ปฏิบัติงานต้องระมัดระวังเรื่องการใช้ซอฟต์แวร์ คอมพิวเตอร์ และ อินเทอร์เน็ต เพื่อเลี่ยงความเสี่ยงที่จะเกิดขึ้น (Rhee, Kim, & Ryu, 2009) ห้องสมุดจึงจําเป็นต้องมีมาตรการป้องกัน การเข้าถึงระบบสารสนเทศโดยไม่ชอบดังกล่าว รวมทั้งการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ โดยให้บุคลากรกําหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สําหรับเครื่องคอมพิวเตอร์ที่ตนใช้ปฏิบัติงาน รวมทั้งติดตั้งโปรแกรม คอมพิวเตอร์ลิขสิทธิ์สําหรับใช้ในการปฏิบัติงานตามความจําเป็น

**กิตติศักดิ์ แก้วบุตรดี(2564)** **[x]** ได้ศึกษาเกี่ยวกับนการดูแลข้อมูลให้มีความมั่นคงปลอดภัยและการดำเนินโครงการความ มั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC27001: 2013) เพื่อกำกับดูแลระบบสารสนเทศ และข้อมูลต่าง ๆ ให้มีความ มั่นคงและปลอดภัยตามมาตรฐานสากล คณะแพทยศาสตร์ศิริราชพยาบาลสำเร็จลุล่วงตามเป้าหมาย การรักษาความมั่นคงปลอดภัยของทรัพย์สินที่เกี่ยวข้อง กับระบบสารสนเทศ เช่น เครื่องคอมพิวเตอร์ อุปกรณ์ เครือข่าย หรือข้อมูลสารสนเทศให้มีความมั่นคงและ ปลอดภัยประกอบไปด้วยองค์ประกอบพื้นฐานที่สำคัญ3 ข้อ ความลับของข้อมูล (Confidentiality) ความพร้อมใช้งานของข้อมูลและระบบ สำรสนเทศต่ำง ๆ (Availability) ควำมถูกต้องสมบูรณ์ของข้อมูล (Integrity) โดยใช้หลักการวงจรบริหารคุณภาพ Plan-Do-Check-Act (PDCA) ย่ อม า จ า ก Plan (ก า ร วางแผน)คือการวางแผน และ กำหนดขอบเขตการดำเนินการจัดตั้งโครงการโครงการ ความมั่นคงปลอดภัยระบบสารสนเทศ, Do (การปฏิบัติ)คือการจัดทำเอกสารการ ดำเนินโครงการและการลงมือปฏิบัติเพื่อให้ครอบคลุม ถูกต้องตามข้อกำหนดต่าง ๆ ภายใต้กรอบของการ ดำเนินงานตามมาตรฐานความมั่นคงปลอดภัยระบบ สารสนเทศ, Check (การตรวจสอบ, การประเมินคือการจัดทำเอกสารการ ดำเนินโครงการและการลงมือปฏิบัติเพื่อให้ครอบคลุม ถูกต้องตามข้อกำหนดต่าง ๆ ภายใต้กรอบของการ ดำเนินงานตามมาตรฐานความมั่นคงปลอดภัยระบบ สารสนเทศ) และ Act (การปรับปรุงคือ การติดตามปรับปรุง ข้อบกพร่อง ทบทวนและพิจารณาข้อกำหนด, วิธีปฏิบัติ และนโยบายความมั่นคงปลอดภัยสารสนเทศเพื่อใช้ใน การวางแผนการดำเนินงานภายใต้กรอบของการ ดำเนินงานโครงการความมั่นคงปลอดภัยระบบ สารสนเทศ

**4. การดำเนินงานวิจัย**

**5. รายการอ้างอิง**

[1] บทวิทยาการ “รู้ รัก ภาษาไทย”, (2554,27 มิถุนายน); สำนักราชบัณฑิตยสภา, (2544,27 มิถุนายน). สิทธิ. <http://legacy.orst.go.th/?knowledges>

[2] ณัฐกฤตา โกมลนาค.(2565, 17 กันยายน). การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำหรับผู้ดูแลระบบ. มหาวิทยาลัยแม่โจ้. <https://erp.mju.ac.th/acticleDetail.aspx?qid=549>

[3] ความมั่นคงปลอดภัยของระบบสารสนเทศ. (ม.ป.ป.).องค์ประกอบของระบบสารสนเทศกับความมั่นคงปลอดภัย. <https://sites.google.com/site/kanokwant551/khwam-mankhng-plxdphay-khxng-rabb-sarsnthes>

[4] การโจมตีด้วยการฉีด SQLคืออะไรและจะป้องกันได้อย่างไร. (ม.ป.ป.). QUISH. <https://th.quish.tv/what-are-sql-injection-attacks>

[x] แววตา เตชาทวีวรรณ. (2020). สภาพและปัญหาการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของห้องสมุดสถาบันอุดมศึกษาของรัฐ, 13(2)

[x] กิตติศักดิ์ แก้วบุตรดี. (2020). ความมั่นคงปลอดภัยระบบสารสนเทศ(ISO27001: 2013)– มิติใหม่ของการบริหารจัดการโรงพยาบาล, 8(2)

[x] ภุมวุฒิ วิทวัสสำราญกุล. (2563). //แนวทางการพัฒนาระบบรักษาความปลอดภัยข้อมูลสารสนเทศโดยใช้กรอบแนวคิดระบบจัดการความปลอดภัยข้อมูลสารสนเทศ. / สารนิพนธ์/ (วิศวกรรมเว็บและการพัฒนาแอปพลิเคชันบนอุปกรณ์พกพา)./มหาวิทยาลัยธุรกิจบัณฑิตย์//ถ่ายเอกสาร.