**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

รายงานการศึกษานี้จึงได้พัฒนาระบบเพื่อนำไปช่วยสนับสนุนการเช่ารถยนต์ของเต๊นท์เช่ารถให้มีประสิทธิภาพมากยิ่งขึ้น ข้อมูลทั้งหมดจะถูดจัดเก็บไว้ภายในฐานข้อมูล เพื่อสะดวกต่อการนำข้อมูลมาใช้งาน เพื่อป้องกันการเข้าถึงข้อมูลที่เป็นข้อมูลลับจึงต้องกำหนดสิทธิ์การเข้าถึงข้อมูลให้ผู้ใช้งานในตารางผู้ใช้งานโดยแบ่งออกเป็น3กลุ่มผู้ใช้งาน ได้แก่ กลุ่มแอดมิน กลุ่มผู้เช่า และกลุ่มผู้ให้เช่า

การพัฒนาระบบงานเว็บแอพพลิเคชั่น นักพัฒนาส่วนใหญ่จะมุ่งเน้นที่การพัฒนาระบบงานโดยอาจละเลยหรือไม่ได้ให้ความสนใจในเรื่องความปลอดภัยเท่าที่ควร ทำให้ผู้ไม่ประสงค์ดีสามารถโจมตีเว็บแอพพลิเคชั่น ในขั้นตอนการตรวจสอบการเข้าสู่ระบบ (Authentication) หรือป้อนคำสั่งโจมตีผ่านทางฟอร์มกรอกข้อมูลต่าง ๆ การโจมตี SQL Injection เกิดจากช่องรับข้อมูลต่างๆของเว็บเพจไม่สมบูรณ์จึงเป็นจุดอ่อนหรือช่องโหว่ที่Hackerสามารถส่ง SQL Injection เข้ามาในช่องรับข้อมูลเพื่อโจมตีข้อมูล จึงทำการศึกษาวิธีการโจมตีของ และวิธีการป้องกันข้อมูล ข้อดีของการป้องกันคือป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ทำให้ข้อมูลไม่สูญหายและระบบยังสามารถทำงานได้อย่างต่อเนื่อง ข้อเสียคือไม่สามารถป้องกันการโดนHackข้อมูลได้100เปอร์เซ็น อาจต้องมีการตรวจเช็คระบบและอัพเดตให้เป็นแพตช์ล่าสุดอยู่เสมอ

ดังนั้น เพื่อเป็นการแก้ไขปัญหาดังกล่าวผู้ศึกษาจึง….เพื่อการแก้ปัญหาการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตด้วยเครื่องมือ PDO ฟังก์ชันของ PHP โดยเลี่ยงการเอาตัวแปรที่รับค่าจากผู้ใช้งานจริง นำไปใส่คิวรี่ แก้โดยการนำตัวแปรที่รอรับข้อมูลจริงไปใส่ในคิวรี่แทน

**2.ทฤษฎีที่เกี่ยวข้อง**

**2.1 การกำหนดสิทธิ์ [1]**

2.1.1 การกำหนดสิทธิ์การเข้าถึง หมายถึง การควบคุมการเข้าถึงของผู้ใช้งานข้อมูลเป็นส่วนที่เจ้าของข้อมูลหรือหน่วยงานเพื่อควบคุมการเข้าถึงของผู้ใช้งาน หรือปิดสิทธิ์ไม่ให้ผู้ใช้งานเห็นข้อมูลนั้นๆ ผ่านการเข้ารหัสผ่าน การกำหนดขึ้นอยู่กับบทบาทของแต่ละบุคคล

2.1.2 access rights (แอคเซ็ซ ไรท์)  หรือสิทธิการเข้าถึง เป็นการกำหนดว่าให้บุคคลนี้เข้าถึงระบบได้แค่ไหน เห็นข้อมูลได้แค่ไหน สามารถกำหนดได้ว่าต้องการให้ลูกค้าคนนี้สามารถเข้ามาในระบบได้แค่ไหน ดูข้อมูลอะไรได้บ้าง และมีสิทธิทำอะไรได้บ้าง

**2.2 ความมั่นคงปลอดภัยของข้อมูล [2]**

**ความมั่นคงปลอดภัย (Security)** คือ สถานะที่มีความปลอดภัย ไร้กังวล อยู่ในสถานะที่ไม่มีอันตรายและได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือบังเอิญ เช่น ความมั่นคงปลอดภัยของประเทศ ย่อมเกิดขึ้นโดยมีระบบป้องกันหลายระดับ เพื่อปกป้องผู้น าประเทศ ทรัพย์สิน ทรัพยากร และประชาชนของประเทศ เป็นต้น **การรักษาความมั่นคงปลอดภัยของสารสนเทศ (Information Security)** คือผลที่เกิดขึ้นจาการใช้ระบบของนโยบายสำหรับการรักษาความมั่นคงปลอดภัยสารสนเทศ ควบคุม และป้องกันการเปิดเผย โดยไม่ได้รับอนุญาต **ภัยคุกคาม (Threat)** คือ วัตถุ สิ่งของ ตัวบุคคล หรือสิ่งอื่นใดที่เป็นตัวแทนของการกระทำอันตรายต่อทรัพย์สินขององค์กร หรือสิ่งที่อาจจะก่อให้เกิดเสียหายต่อคุณสมบัติของข้อมูลด้านใดด้านหนึ่งหรือมากกว่าหนึ่งด้าน ความลับ (Confidentiality), ความสมบูรณ์ (Integrity), ความพร้อมใช้ (Availability)

ภาพที่ x xxx

**2.3 องค์ประกอบของความมั่นคงปลอดภัยของข้อมูล [3]**

*ความลับ (Confidentiality)* เป็นการรับประกันว่าผู้มีสิทธิ์และได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ องค์กรต้องมีมาตรการป้องกันการเข้าถึงสารสนเทศที่เป็นความลับ *ความสมบูรณ์( Integrity)*  ความสมบูรณ์ ครบถ้วน ถูกต้อง เป็นสารสนเทศที่นำไปใช้ประโยชน์ได้อย่างถูกต้องครบถ้วน  *ความพร้อมใช้(Availability)*  สารสนเทศจะถูกเข้าถึงหรือเรียกใช้งานได้อย่างราบรื่น และใช้งานได้ต่อเนื่องตลอดเวลาไม่มีข้อบกพร่อง ความถูกต้องแม่นยำ (Accuracy) สารสนเทศต้องไม่มีความผิดพลาด และต้องมีค่าตรงกับความคาดหวังของผู้ใช้เสมอ *เป็นของแท้ Authenticity* สารสนเทศที่ถูกจัดทำขึ้นจากแหล่งที่ถูกต้อง ไม่ถูกทำซ้ำโดยแหล่งอื่นที่ไม่ได้รับอนุญาต หรือแหล่งที่ไม่คุ้นเคยและไม่เคยทราบมา *ความเป็นส่วนตัว* สารสนเทศที่ถูกรวบรวม เรียกใช้ และจัดเก็บโดยองค์กร จะต้องถูกใช้ในวัตถุประสงค์ที่ผู้เป็นเข้าของสารสนเทศรับทราบ ณ ขณะที่มีการรวบรวมสารสนเทศนั้น

**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

ภาพที่ x xxx

MySQL

PHP Language

**3.งานวิจัยที่เกี่ยวข้อง**

**แววตา เตชาทวีวรรณ (2020) [5]** ได้ศึกษาเกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศที่สำคัญของห้องสมุด เพื่อศึกษาสภาพและปัญหาความมั่นคงปลอดภัยของระบบสารสนเทศ ตาม “แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ โดยงานวิจัยระยะที่1 ซึ่งใช้วิธีวิจัยเชิงคุณภาพแบบวิธีศึกษาเฉพาะกรณี แบบมุ่งการค้นหา พบว่า ห้องสมุดสถาบันอุดมศึกษาของรัฐให้ความสำคัญต่อการรักษาความมั่นคงปลอดภัยระบบสารสนเทศโดยมีการปฎิบัติแนวทางในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้สามารถดําเนินการต่าง ๆ ด้วยวิธีทางอิเล็กทรอนิกส์ โดยอาศัยอำนาจตามความในมาตรา 5 มาตรา 7 และมาตรา 8 โดยกําหนดสิทธิและระดับของบุคคล ทั้งทางกายภาพและทางอิเล็กทรอนิกส์ จึงต้องมีการป้องกันการเข้าถึงอุปกรณ์ต่าง ๆ โดยอนุญาตเฉพาะผู้ที่เกี่ยวข้องเข้าถึงอุปกรณ์ต่าง ๆ ได้ โดยกําหนดกฎระเบียบและใช้อุปกรณ์ป้องกันบุคคลอื่นเข้าถึงโดยไม่ได้รับอนุญาต นอกจากนี้การคุกคามทางระบบเครือข่ายสามารถกระทําได้โดยแฮคเกอร์ (Hacker) ทําให้ข้อมูลเสียหาย 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

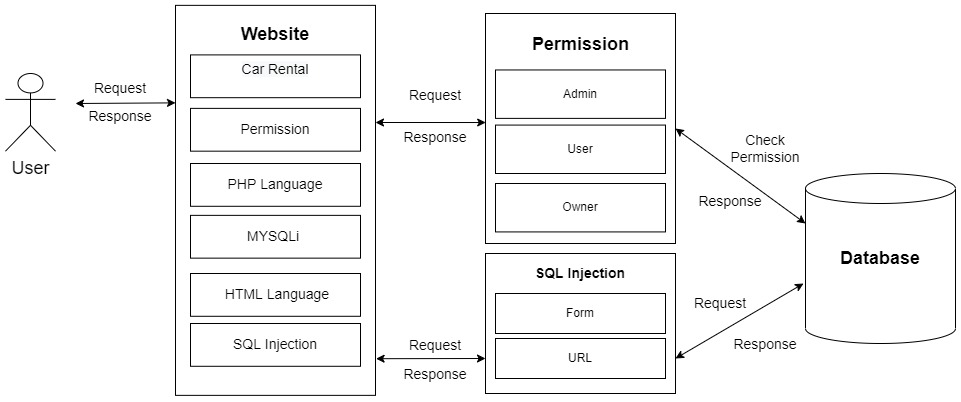
**กิตติศักดิ์ แก้วบุตรดี(2564)**[6] ได้ศึกษาเกี่ยวกับนการดูแลข้อมูลให้มีความมั่นคงปลอดภัยและการดำเนินโครงการความ มั่นคงปลอดภัยระบบสารสนเทศ (ISO/IEC27001: 2013) เพื่อกำกับดูแลระบบสารสนเทศ ให้มีความ มั่นคงและปลอดภัยตามมาตรฐานสากล ซึ่งประกอบไปด้วยองค์ประกอบพื้นฐานที่สำคัญ 3 ข้อ ความลับของข้อมูล (Confidentiality) ความพร้อมใช้งานของข้อมูลและระบบ สารสนเทศต่าง ๆ (Availability) ความถูกต้องสมบูรณ์ของข้อมูล (Integrity) โดยใช้หลักการวงจรบริหารคุณภาพ Plan-Do-Check-Act (PDCA) ย่อมา จาก Plan (การวางแผน) คือการวางแผน และ กำหนดขอบเขตการดำเนินการจัดตั้งโครงการ ความมั่นคงปลอดภัยระบบสารสนเทศ, Do (การปฏิบัติ)คือการจัดทำเอกสารการ ดำเนินโครงการและการลงมือปฏิบัติ ภายใต้กรอบของมาตรฐานความมั่นคงปลอดภัยระบบ สารสนเทศ, Check (การตรวจสอบ) คือการจัดทำเอกสารการ ลงมือปฏิบัติเพื่อให้ครอบคลุม ภายใต้กรอบของการ ดำเนินงานตามมาตรฐานความมั่นคงปลอดภัยระบบ สารสนเทศ) และ Act (การปรับปรุง) คือการติดตามข้อบกพร่อง ทบทวนและพิจารณาข้อกำหนด, วิธีปฏิบัติ และนโยบายความมั่นคงปลอดภัยสารสนเทศเพื่อใช้ใน การวางแผนการดำเนินงานภายใต้กรอบของการ ดำเนินงานโครงการความมั่นคงปลอดภัยระบบ สารสนเทศ

**ภุมวุฒิ วิทวัสสำราญกุล (2020)[7]** การศึกษาวิเคราะห์พบว่าการใช้กรอบแนวคิดการจัดการความปลอดภัยข้อมูลสารสนเทศเพื่อพัฒนาแนวทางรักษาความปลอดภัยภายในศูนย์ปฏิบัติการเครือข่าย สามารถกำหนดแนวทางขั้นตอนปฏิบัติสำหรับอุปกรณ์ และระบบที่มีคุณสมบัติและการทำงานคล้ายกลึงกันได้อย่างมีประสิทธิภาพในระดับหนึ่ง โดยการแบ่งประเภทอุปกรณ์และระบบที่เหมาะสมมีความสำคัญอย่างมากในการดำเนินการ ข้อดีของการศึกษาพบว่า สามารถนำแนวทางรักษาความปลอดภัยดังกล่าวไปใช้จัดการความปลอดภัยข้อมูลสารสนเทศในภาพรวมได้อย่างรวดเร็ว และ ดำเนินการด้านการรักษาความปลอดภัยข้อมูลสารสนเทศ และ มีการดำเนินการตามมาตรฐาน ISO 27001 ทำให้สามารถพัฒนาเพื่อขอใบรับรองได้อีก ข้อจำกัดของการศึกษาพบว่าไม่สามารถศึกษาซอฟด์แวร์ต่าง ๆ ที่ติดตั้งใช้งานภายในศูนย์ปฏิบัติการเครือข่ายฯ เนื่องจากหน่วยงานราชการมีการพัฒนาซอฟต์แวร์ ที่ไม่เป็นไปตามกระบวนการมาตรฐาน และมีซอฟต์แวร์จำนวนมาก จึงกำหนดแนวทางรักษาความปลอดภัยทั่วไปสำหรับซอฟต์แวร์ ข้อจำกัดหรือจุดอ่อนที่สำคัญอีกประการหนึ่ง คือ สินทรัพย์ข้อมูลสารสนเทศที่มีรุ่นผลิตภัณฑ์แตกต่างกันมาก แม้จะเป็นยี่ห้อเดียวกันก็จะ ไม่สามารถใช้แนวทางรักษาความปลอดภัยข้อมูลสาร สนเทศได้ เนื่องจากความแตกต่างของเทคโนโลยี และการนำแนวทางการ รักษาความปลอดภัยแต่ละประ เภทไปใช้อาจเกิดข้อผิดพลาดเนื่องจากการกำหนด และเลือกประเภทของอุปกรณ์ และระบบไม่เหมาะสม การศึกษาโดยใช้ข้อมูลของสินทรัพย์ข้อมูลสารสนเทศภายในศูนย์ปฏิบัติงานเครือบ่ายซึ่งมีความอ่อนไหว และวัฒนธรรมองค์กรเกี่ยวกับกฎหมายที่มีการกำหนดโดยพฤตินัยไว้ว่า ถ้ายังไม่มีกฎระเบียบรองรับ หรือผ่านการพิจารณาของคณะกรรมการแล้วจะให้ยุติไว้ก่อน การขอข้อมูลเพื่อใช้ในการศึกษา และเผยแพร่จึงเป็นเรื่องยาก จึงขาดข้อมูลบางส่วน

**4. การดำเนินงานวิจัย**

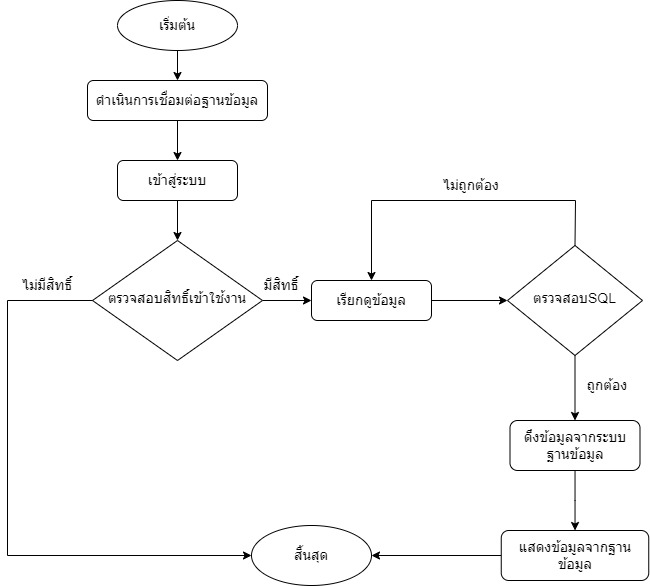
ในการดำเนินวิจัยฉบับนี้เป็นการนำเสนอแนวทางการแก้ไขปัญหาการHack ข้อมูล2ที่ คือ จากFormการเข้าสู่ระบบเช่น การป้อนข้อมูลบางอย่างโดยวิธีการใส่คำสั่ง or’1=1’ และการHack จาก URL โดยใส่คำสั่ง or’1=1’ ในช่องURL จะนำเสนอแนวทางสำหรับการกำหนดสิทธิ์ผู้ใช้งานและการป้องกันข้อมูลจากการ Hack ด้วยการ PDO ของ PHP ซึ่งประกอบด้วยขั้นตอน ดังนี้ 1.ขั้นตอนการจัดเตรียมข้อมูลนำเข้าใน phpMyAdmin 2.เขียนโค้ดPHPเพื่อเชื่อมต่อกับข้อมูลใน phpMyAdmin และ 3.เขียนโค้ดPHPเพื่อป้องกันและทดสอบระบบการป้องกัน

ในการดำเนินงานการออกแบบและพัฒนาเว็บไซต์เช่ารถยนต์ ประกอบด้วยการดำเนินงานดังภาพ

****

ภาพที่1 แสดงภาพรวมการดำเนินงาน

การกำหนดสิทธิ์และการเข้าถึงข้อมูลมีเส้นทางการดำเนินงานดังรูป

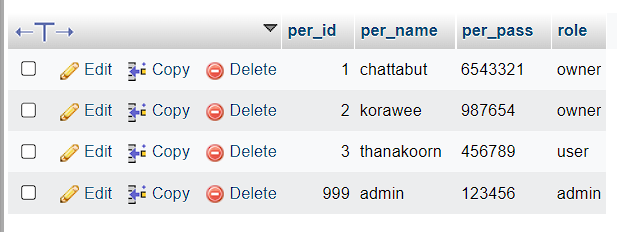


ภาพที่2 แสดงเส้นทางการประมวลผลข้อมูลเมื่อผู้ใช้เรียกดู

**1.ขั้นตอนการจัดเตรียมข้อมูลนำเข้าใน phpMyAdmin**

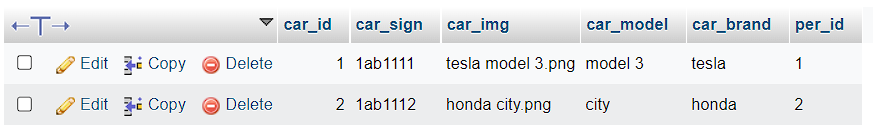
ข้อมูลนำเข้ามีดังนี้

ข้อมูลบุคคล



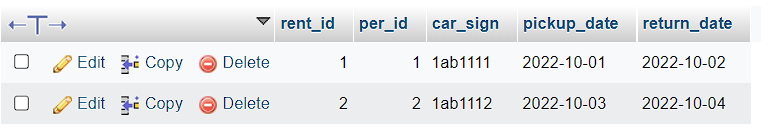
ภาพที่3 แสดงตารางข้อมูลบุคคล

ข้อมูลรายการถยนต์



ภาพที่4 แสดงตารางข้อมูลรายการรถยนต์

ข้อมูลรายการเช่ารถยนต์



ภาพที่5 แสดงตารางข้อมูลรายการเช่ารถยนต์

ภาพที่ x แผนภาพอีอาร์

**~~2.เขียนโค้ดPHPเพื่อเชื่อมต่อกับข้อมูลใน phpMyAdmin~~**

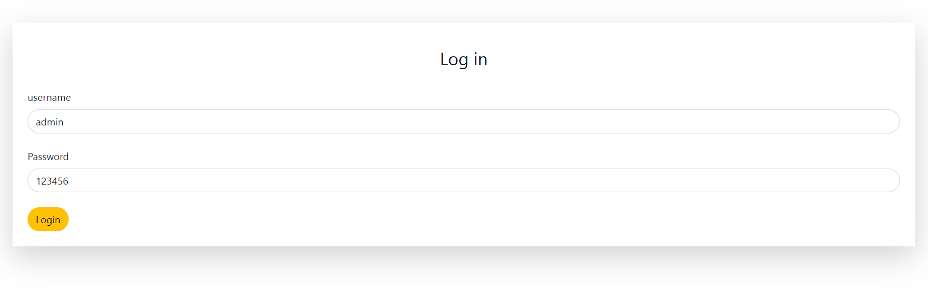


~~ภาพที่6 แสดงโค้ดส่วนที่เชื่อมต่อฐานข้อมูล~~

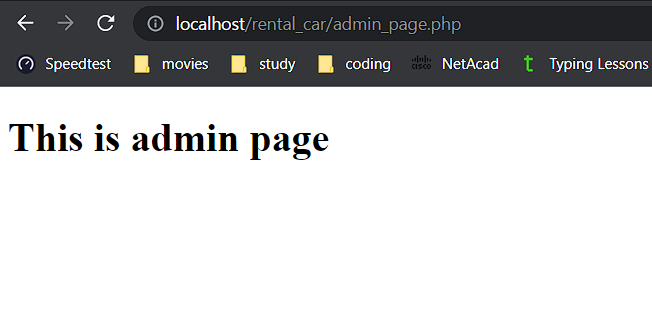
**3.เขียนโค้ดPHPเพื่อป้องกันและทดสอบระบบการป้องกัน**

ก่อนเขียนโค้ดPDO ฟังก์ชันของ PHP เพื่อป้องกันการ Hack ผ่าน Form การเข้าสู่ระบบ

เข้าสู่ระบบปกติ ใส่username และ password ที่ถูกต้อง

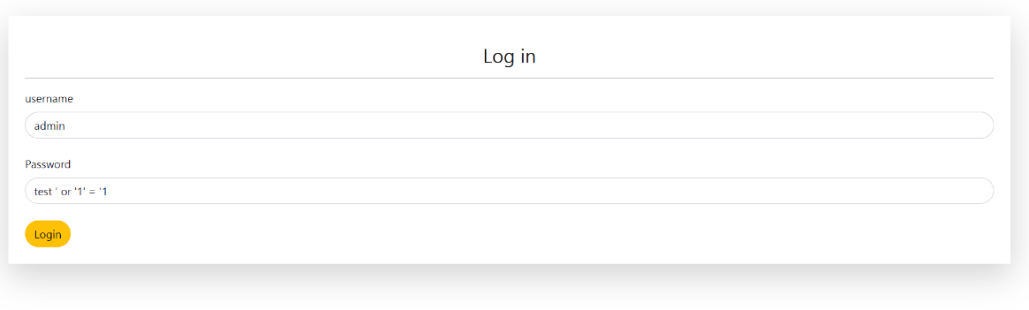


ภาพที่7 แสดงหน้าเข้าสู่ระบบ

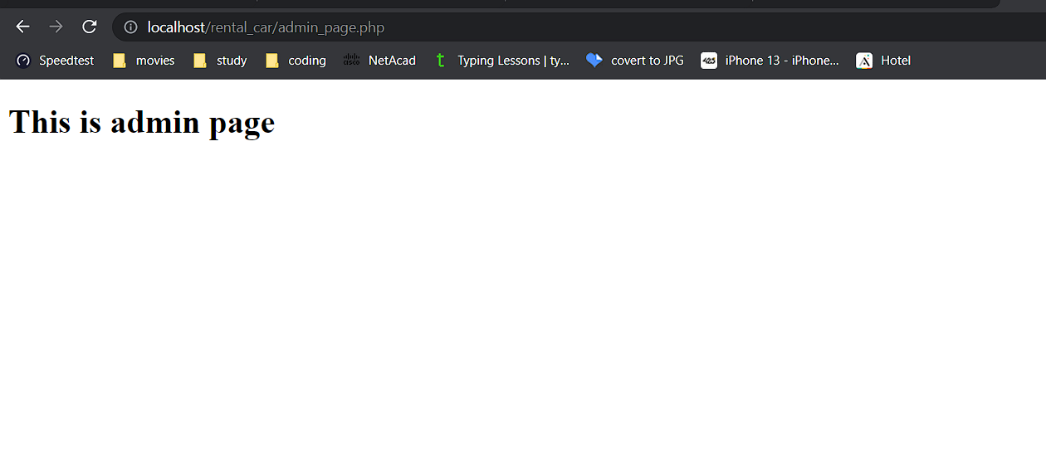


ภาพที่8 แสดงหน้าแอดมินเพจ

เข้าสู่ระบบโดยใช้คำสั่ง or‘1=1’



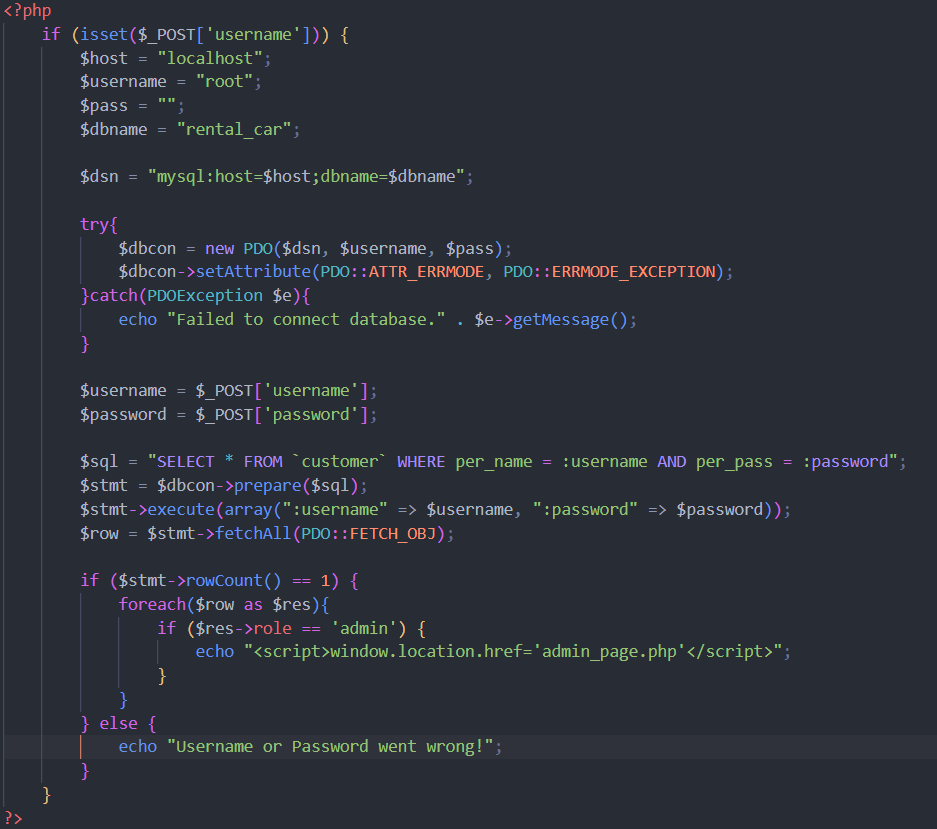
ภาพที่9 แสดงหน้าการเข้าสู่ระบบโดยใช้คำสั่ง or ‘1=1’



ภาพที่10 แสดงหน้าแอดมินเพจหลังจากเข้าสู่ระบบโดยใช้คำสั่ง or ‘1=1’

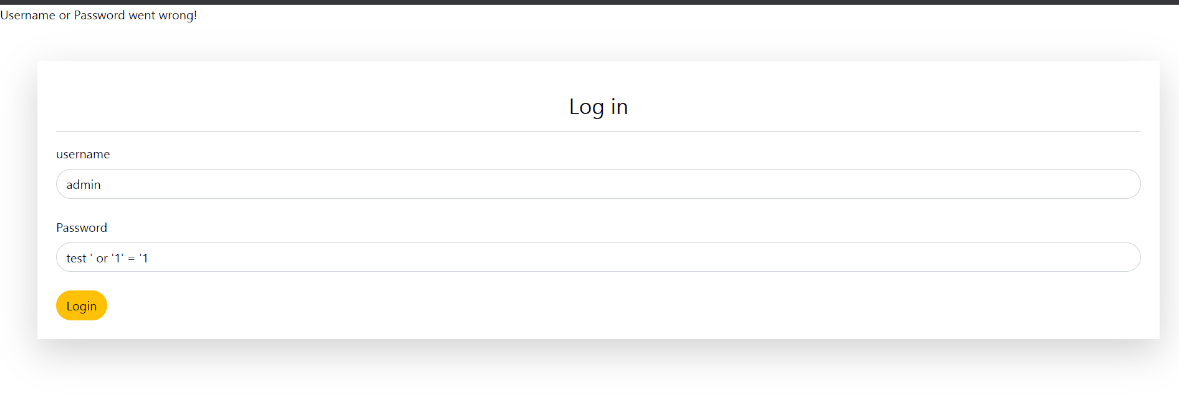
จากภาพที่ x-x ….

หลังจากเขียนโค้ดPDO ฟังก์ชันของ PHP เพื่อป้องกันการ Hack ผ่าน Form การเข้าสู่ระบบ



ภาพที่11 โค้ด PDO การเข้าสู่ระบบ

ผลลัพธ์ : ไม่สามารถเข้าระบบได้ และมีข้อความแจ้งเตือนขึ้นที่มุมบนซ้าย



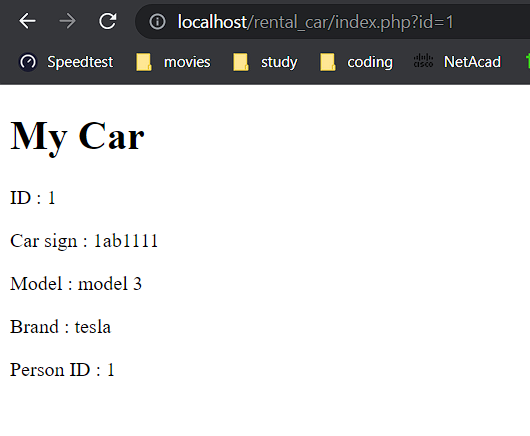
ภาพที่12 แสดงหน้าเข้าสู่ระบบที่มีข้อความแจ้งเตือน



ภาพที่13 ข้อความแจ้งเตือน

ก่อนเขียนโค้ดPDO ฟังก์ชันของ PHP เพื่อป้องกันการHackระบบฐานข้อมูลรายการรถยนต์ ผ่าน URL

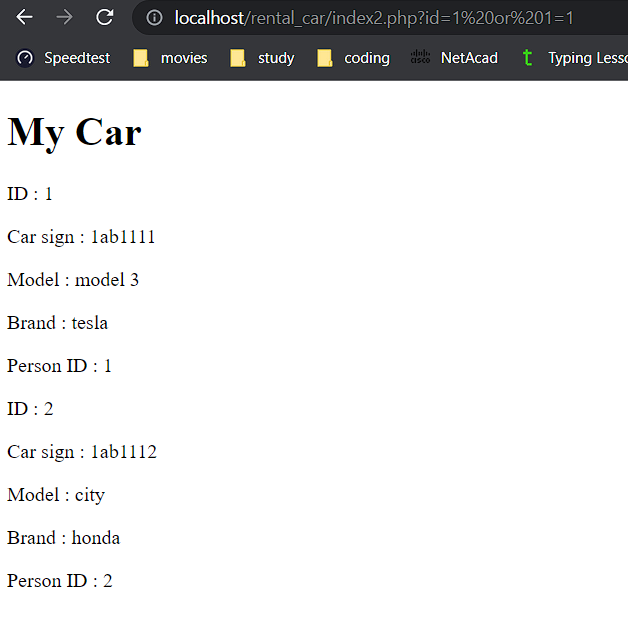
เข้าระบบและเข้าดูรายการรถยนต์แบบปกติ



ภาพที่14 แสดงข้อมูลรายการรถยนต์ของผู้ใช้งาน

เข้าระบบและเข้าดูรายการรถยนต์โดยใช้คำสั่ง or ‘1=1’ ในช่องURL

ผลลัพธ์ : แสดงข้อมูลรายการรถยนต์ของผู้อื่นทั้งหมด



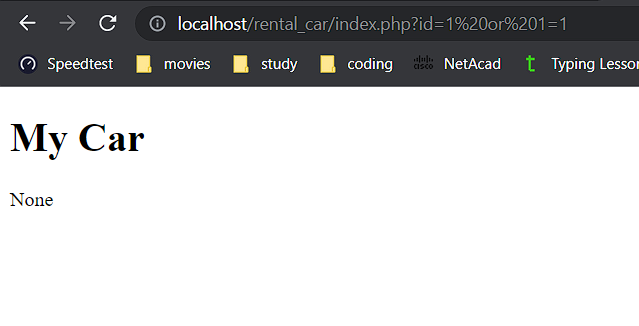
ภาพที่15 แสดงรายการข้อมูลรถยนต์ของผู้ใช้งานทั้งหมด

หลังจากเขียนโค้ดPDO ฟังก์ชันของ PHP เพื่อป้องกันการHackระบบฐานข้อมูลรายการรถยนต์ ผ่าน URL



ภาพที่16 แสดงโค้ด PDO ป้องกันการเข้าถึงข้อมูลรายการรถยนต์ของผู้อื่น

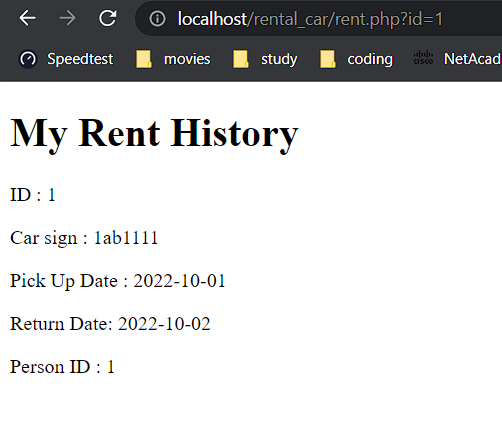
ผลลัพธ์: ไม่สามารถเข้าไปดูข้อมูลรายการรถยนต์ได้



ภาพที่17 แสดงหน้าเพจที่ไม่มีจ้อมูลรายการรถยนต์

ก่อนเขียนโค้ดPDO ฟังก์ชันของ PHP เพื่อป้องกันการHackระบบฐานข้อมูลรายการเช่ารถยนต์ผ่าน URL

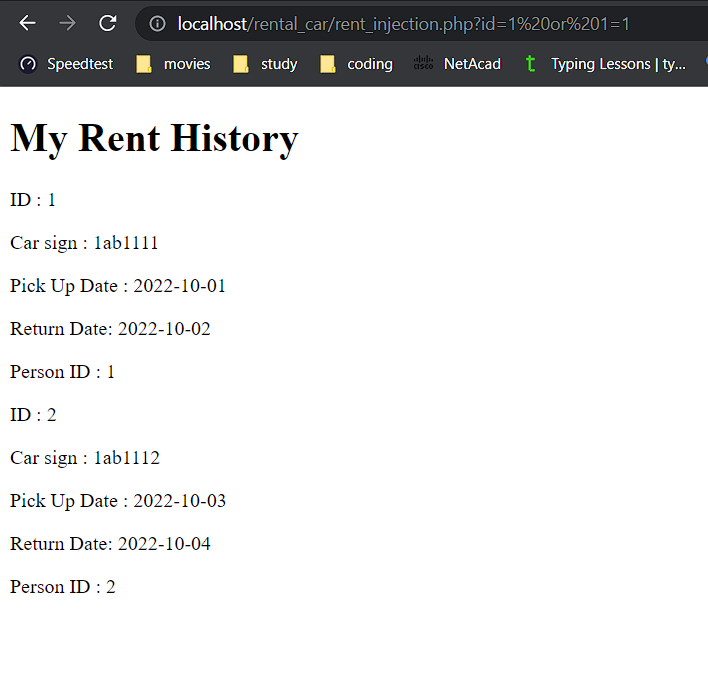
เข้าระบบและเข้าดูรายการเช่ารถยนต์แบบปกติ



ภาพที่18 แสดงข้อมูลรายการเช่ารถยนต์ของผู้ใช้งาน

เข้าระบบและเข้าดูรายการเช่ารถยนต์โดยใช้คำสั่ง or ‘1=1’ ในช่องURL

ผลลัพธ์ : แสดงข้อมูลรายการเช่ารถยนต์ของผู้อื่นทั้งหมด



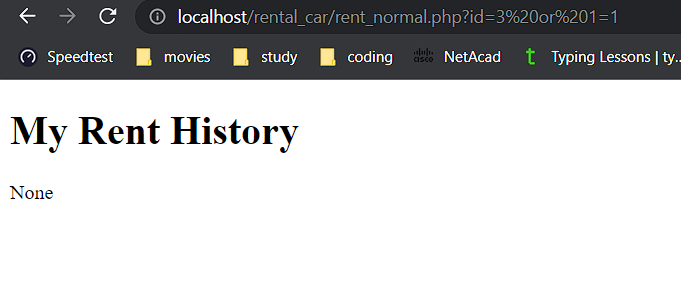
ภาพที่19 แสดงข้อมูลรายการเช่ารถยนต์ของผู้ใช้งานของผู้อื่น

หลังจากเขียนโค้ดPDO ฟังก์ชันของ PHP เพื่อป้องกันการHackระบบฐานข้อมูลรายการเช่ารถยนต์ผ่าน URL



ภาพที่20 แสดงโค้ด PDO ป้องกันการเข้าถึงข้อมูลรายการเช่ารถยนต์ของผู้อื่น

ผลลัพธ์: ไม่สามารถเข้าไปดูข้อมูลรายการเช่ารถยนต์ได้



ภาพที่17 แสดงหน้าเพจที่ไม่มีข้อมูลรายการเช่ารถยนต์

**สรุปผลวิจัย**

จากการวิจัยการแก้ปัญหาการโดน Hack ด้วยวิธีการแบบ SQL Injection จึงได้นำโค้ด PDO ที่เป็นฟังก์ชันของ PHP มาปรับใช้เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ได้ผลสรุปโดยใช้ Test Case ดังนี้

ตาราง Test Case: การเข้าสู่ระบบแบบที่ยังไม่มีการป้องกัน ดังตารางที่ 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Input** |  |  |  |  |
| **Test ID** | **User** | **Password** | **Expected Results** | **Actual Results** | **Accepted Results** |
| TC001 | admin | 123456 | **PASS** | **PASS** | **PASS** |
| TC002 | admin | or‘1=1’ | **FAIL** | **PASS** | **FAIL** |
| TC003 | or‘1=1’ | 123456 | **FAIL** | **PASS** | **FAIL** |
| TC004 | or‘1=1’ | or‘1=1’ | **FAIL** | **PASS** | **FAIL** |

ตารางที่1 แสดงผลTest Case การเข้าสู่ระบบแบบที่ยังไม่มีการป้องกัน

จากตาราที่ 1 แสดงการเข้าสู่ระบบแบบที่ยังไม่มีการป้องกัน TC001 ใส่ชื่อและรหัสผ่านถูกต้อง จึงสามารถเข้าสู่ระบบได้ , TC002 ใส่ชื่อถูกต้อง ใส่รหัสผ่านไม่ถูกต้องโดยใส่เป็นคำสั่ง or‘1=1’ จึงทำให้เข้าสู่ระบบได้ , TC003 ใส่รหัสผ่านถูกต้อง ใส่ชื่อไม่ถูกต้องโดยใส่เป็นคำสั่ง or‘1=1’ จึงทำให้เข้าสู่ระบบได้ และ TC004 ใส่คำสั่ง or‘1=1’ทั้งในชื่อและรหัสผ่าน จึงทำให้สามารถเข้าสู่ระบบได้

ตาราง Test Case: การเข้าสู่ระบบแบบที่มีการป้องกันแล้ว ดังตารางที่ 2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Input** |  |  |  |  |
| **Test ID** | **User** | **Password** | **Expected Results** | **Actual Results** | **Accepted Results** |
| TC005 | admin | 123456 | **PASS** | **PASS** | **PASS** |
| TC006 | admin | or‘1=1’ | **FAIL** | **FAIL** | **PASS** |
| TC007 | or‘1=1’ | 123456 | **FAIL** | **FAIL** | **PASS** |
| TC008 | or‘1=1’ | or‘1=1’ | **FAIL** | **FAIL** | **PASS** |

ตารางที่2 แสดงผลTest Case การเข้าสู่ระบบแบบที่มีการป้องกันแล้ว

จากตาราที่ 2 แสดงการเข้าสู่ระบบแบบที่มีการป้องกันแล้ว TC005 ใส่ชื่อและรหัสผ่านถูกต้อง จึงสามารถเข้าสู่ระบบได้ปกติ , TC006 ใส่ชื่อถูกต้อง ใส่รหัสผ่านไม่ถูกต้องโดยใส่เป็นคำสั่ง or‘1=1’ ก็ไม่สามารถเข้าสู่ระบบได้ , TC007 ใส่รหัสผ่านถูกต้อง ใส่ชื่อไม่ถูกต้องโดยใส่เป็นคำสั่ง or‘1=1’ ก็ไม่สามารถเข้าสู่ระบบได้ และ TC008 ใส่คำสั่ง or‘1=1’ทั้งในชื่อและรหัสผ่าน ก็ทำให้ไม่สามารถเข้าสู่ระบบได้

ตาราง Test Case: การเข้าถึงข้อมูลรายการรถยนต์แบบที่ยังไม่มีการป้องกัน ดังตารางที่ 3

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test ID** | **Test Steps** | **Expected Results** | **Actual Results** | **Accepted Results** |
| TC009 | 1.เข้าสู่ระบบ  2.คลิกปุ่มรายการรถยยนต์ | แสดงรายการรถยนต์เฉพาะของตัวเองเท่านั้น | แสดงรายการรถยนต์เฉพาะของตัวเอง | **PASS** |
| TC010 | 1.เข้าสู่ระบบ  2.คลิกปุ่มรายการรถยยนต์  3.ใส่คำสั่ง or‘1=1’ในช่องURL | แสดงรายการรถยนต์เฉพาะของตัวเองเท่านั้น | แสดงรายการรถยนต์ของผู้อื่นด้วย | **FAIL** |

ตารางที่3 แสดงผล Test Case การเข้าถึงข้อมูลรายการรถยนต์แบบที่ยังไม่มีการป้องกัน

จากตาราที่ 3 แสดงการเข้าถึงข้อมูลรายการรถยนต์แบบที่ยังไม่มีการป้องกันโดย TC009 เข้าสู่ระบบและคลิกดูรายการรถยนต์ของตนเอง แสดงรายการรถยนต์เฉพาะของตัวเอง TC010 เข้าสู่ระบบและคลิกดูรายการรถยนต์ของตนเอง มีการเพิ่มคำสั่ง or ‘1=1’ในช่องURL ระบบต้องแสดงเฉพาะของตัวเองแต่ระบบแสดงรายการรถยนต์ของผู้อื่นด้วย

ตาราง Test Case: การเข้าถึงข้อมูลรายการรถยนต์แบบที่มีการป้องกันแล้ว ดังตารางที่ 4

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test ID** | **Test Steps** | **Expected Results** | **Actual Results** | **Accepted Results** |
| TC011 | 1.เข้าสู่ระบบ  2.คลิกปุ่มรายการรถยยนต์ | แสดงรายการรถยนต์เฉพาะของตัวเองเท่านั้น | แสดงรายการรถยนต์เฉพาะของตัวเอง | **PASS** |
| TC012 | 1.เข้าสู่ระบบ  2.คลิกปุ่มรายการรถยยนต์  3.ใส่คำสั่ง or’1=1’ในช่องURL | ไม่แสดงข้อมูลรายการรถยนต์ผู้อื่น | ไม่แสดงรายการรถยนต์ | **PASS** |

ตารางที่4 Test Case การเข้าถึงข้อมูลรายการรถยนต์แบบที่มีการป้องกันแล้ว

จากตาราที่ 4 แสดงการเข้าถึงข้อมูลรายการรถยนต์แบบที่มีการป้องกันแล้ว โดย TC011 เข้าสู่ระบบและคลิกดูรายการรถยนต์ของตนเอง แสดงรายการรถยนต์เฉพาะของตัวเอง TC012 เข้าสู่ระบบและคลิกดูรายการรถยนต์ของตนเอง มีการเพิ่มคำสั่ง or ‘1=1’ในช่องURL ระบบต้องไม่แสดงรายการรถยนต์ผู้อื่น ผลคือระบบไม่แสดงรายการรถยนต์

ตาราง Test Case: การเข้าถึงข้อมูลรายการเช่ารถยนต์แบบที่ยังไม่มีการป้องกัน ดังตารางที่ 5

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test ID** | **Test Steps** | **Expected Results** | **Actual Results** | **Accepted Results** |
| TC013 | 1.เข้าสู่ระบบ  2.คลิกปุ่มรายการเช่า | แสดงรายการเช่ารถยนต์เฉพาะของตัวเองเท่านั้น | แสดงรายการเช่ารถยนต์เฉพาะของตัวเอง | **PASS** |
| TC014 | 1.เข้าสู่ระบบ  2.คลิกปุ่มรายการเช่ารถยยนต์  3.ใส่คำสั่ง or’1=1’ในช่องURL | ไม่แสดงข้อมูลรายการเช่ารถยนต์ผู้อื่น | แสดงรายการเช่ารถยนต์ของผู้อื่น | **FAIL** |

ตารางที่5 แสดงผล Test Case การเข้าถึงข้อมูลรายการเช่ารถยนต์แบบที่ยังไม่มีการป้องกัน

จากตาราที่ 5 แสดงการเข้าถึงข้อมูลรายการเช่ารถยนต์แบบที่ยังไม่มีการป้องกันโดย TC013 เข้าสู่ระบบและคลิกดูรายการเช่ารถยนต์ของตนเอง แสดงรายการเช่ารถยนต์เฉพาะของตัวเอง TC014 เข้าสู่ระบบและคลิกดูรายการเช่ารถยนต์ของตนเอง มีการเพิ่มคำสั่ง or ‘1=1’ในช่องURL ระบบต้องแสดงเฉพาะของตัวเองแต่ระบบแสดงรายการเช่ารถยนต์ของผู้อื่นด้วย

ตาราง Test Case: การเข้าถึงข้อมูลรายการเช่ารถยนต์แบบที่มีการป้องกันแล้ว ดังตารางที่ 6

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test ID** | **Test Steps** | **Expected Results** | **Actual Results** | **Accepted Results** |
| TC015 | 1.เข้าสู่ระบบ  2.คลิกปุ่มรายการเช่า | แสดงรายการเช่ารถยนต์เฉพาะของตัวเองเท่านั้น | แสดงรายการเช่ารถยนต์เฉพาะของตัวเอง | **PASS** |
| TC016 | 1.เข้าสู่ระบบ  2.คลิกปุ่มรายการเช่ารถยยนต์  3.ใส่คำสั่ง or’1=1’ในช่องURL | ไม่แสดงข้อมูลรายการเช่ารถยนต์ผู้อื่น | ไม่แสดงรายการเช่ารถยนต์ | **PASS** |

ตารางที่6 แสดงผล Test Case การเข้าถึงข้อมูลรายการเช่ารถยนต์แบบที่มีการป้องกันแล้ว

จากตาราที่ 6 แสดงการเข้าถึงข้อมูลรายการเช่ารถยนต์แบบที่มีการป้องกันแล้ว โดย TC015 เข้าสู่ระบบและคลิกดูรายการเช่ารถยนต์ของตนเอง แสดงรายการเช่ารถยนต์เฉพาะของตัวเอง TC016 เข้าสู่ระบบและคลิกดูรายการเช่ารถยนต์ของตนเอง มีการเพิ่มคำสั่ง or ‘1=1’ในช่องURL ระบบต้องไม่แสดงรายการเช่ารถยนต์ผู้อื่น ผลคือระบบไม่แสดงรายการเช่ารถยนต์

**5. รายการอ้างอิง**

[1]access rights หรือสิทธิการเข้าถึงคืออะไร, (2560,2 กุมภาพันธ์). Access rights (แอคเซ็ซ ไรท์) หรือสิทธิการเข้าถึง.<https://www.mindphp.com/%E0%B8%84%E0%B8%B9%E0%B9%88%E0%B8%A1%E0%B8%B7%E0%B8%AD/73-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3/3937-access-rights.html>

[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>

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

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

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