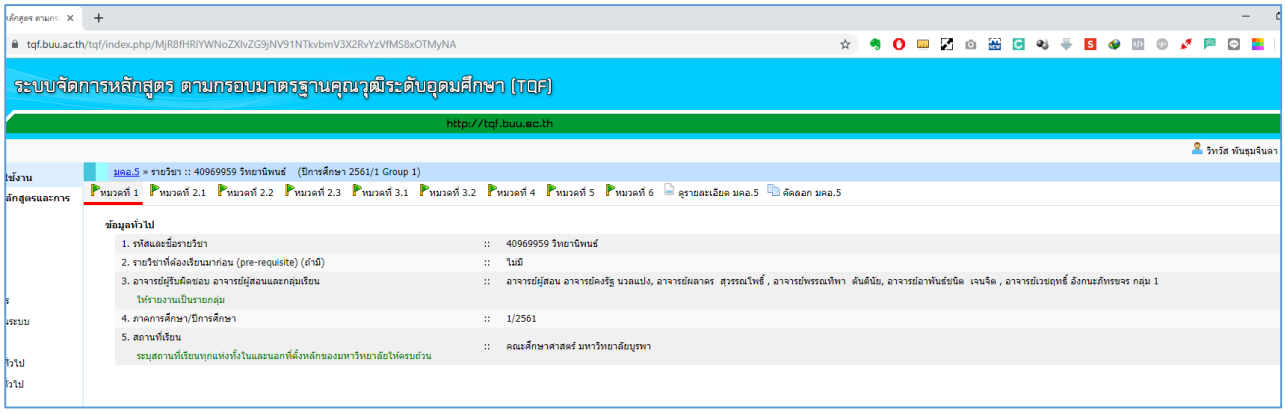
ชื่อเรื่อง การกำหนดการเข้าถึงข้อมูลในระบบ (Permission)
เล่าเรื่องโดย นางสาวนันท์นภัส วงก์กุลชัยชนะ

ที่มา/ประเด็นปัญหา

เนื่องจากการพัฒนาระบบจะต้องมีการกำหนดการเข้าถึงข้อมูลต่าง ๆ ในระบบ เช่น การเข้าใช้งานระบบเพื่อดูข้อมูลต่าง ๆ ซึ่งบางครั้งระบบที่พัฒนานั้น ไม่ได้กำหนดการเข้าถึงข้อมูลที่ไม่ใช่ของตัวเอง จึงทำให้เกิดความไม่ปลอดภัยของการแสดงข้อมูล เราจึงจำเป็นต้องกำหนดการเข้าถึงข้อมูล เพื่อรักษาความลับของข้อมูล ข้อมูลนั้นจะต้องถูกเปิดอ่านโดยบุคคลที่ได้รับอนุญาตเท่านั้น โดยไม่ให้ผู้ใช้บางท่าน หรือบางกลุ่มเข้าไปบันทึก หรือมองเห็นข้อมูล หรือเอกสารใด ๆ ที่ไม่ใช่ของตัวเอง ซึ่งการจำกัดสิทธิ์สามารถทำได้หลายวิธี เช่น การเช็คเงื่อนไขที่โปรแกรม การเข้ารหัส (Encrypt URL) เป็นต้น

ตัวอย่างการเข้าถึงข้อมูลที่ไม่ได้กำหนด Permission

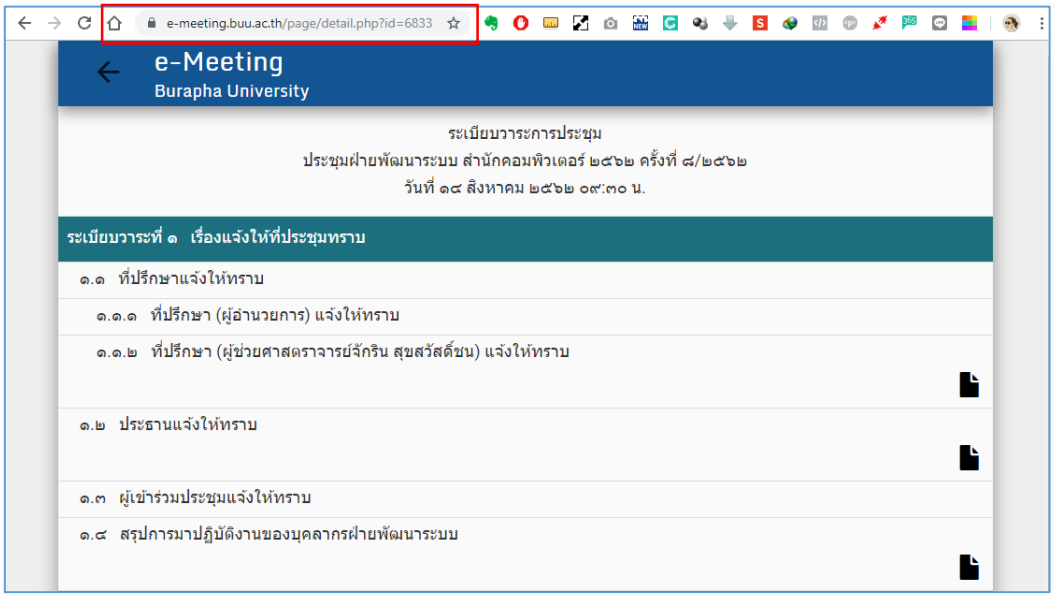


จากภาพตัวอย่างเมื่อทดลองแก้ไข URL แล้วสามารถเข้าถึงข้อมูลของผู้อื่นได้ ทำให้เกิดความไม่ปลอดภัย เราจึงจำเป็นต้องกำหนดการเข้าถึงข้อมูล

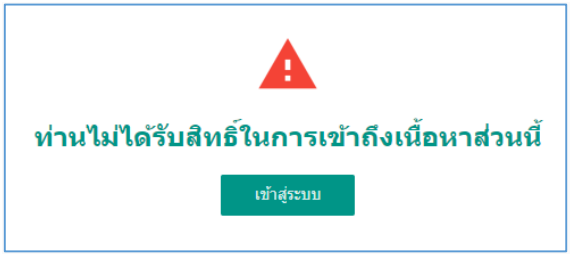
แนวทางการปัญหา

๑. เตรียมข้อมูลการเข้าถึงสิทธิ์การใช้งานของข้อมูล เช่น ข้อมูลต่าง ๆ หรือเอกสารที่สามารถเรียกดูได้ เป็นต้น
๒. เขียนโปรแกรมเช็คเงื่อนไข เพื่อให้เข้าถึงข้อมูลได้ตามที่มีสิทธิ์เท่านั้น
๓. การป้องกันโดยการเข้ารหัส (Encrypt URL) เพื่อป้องกันการเข้าถึงข้อมูลของผู้อื่น

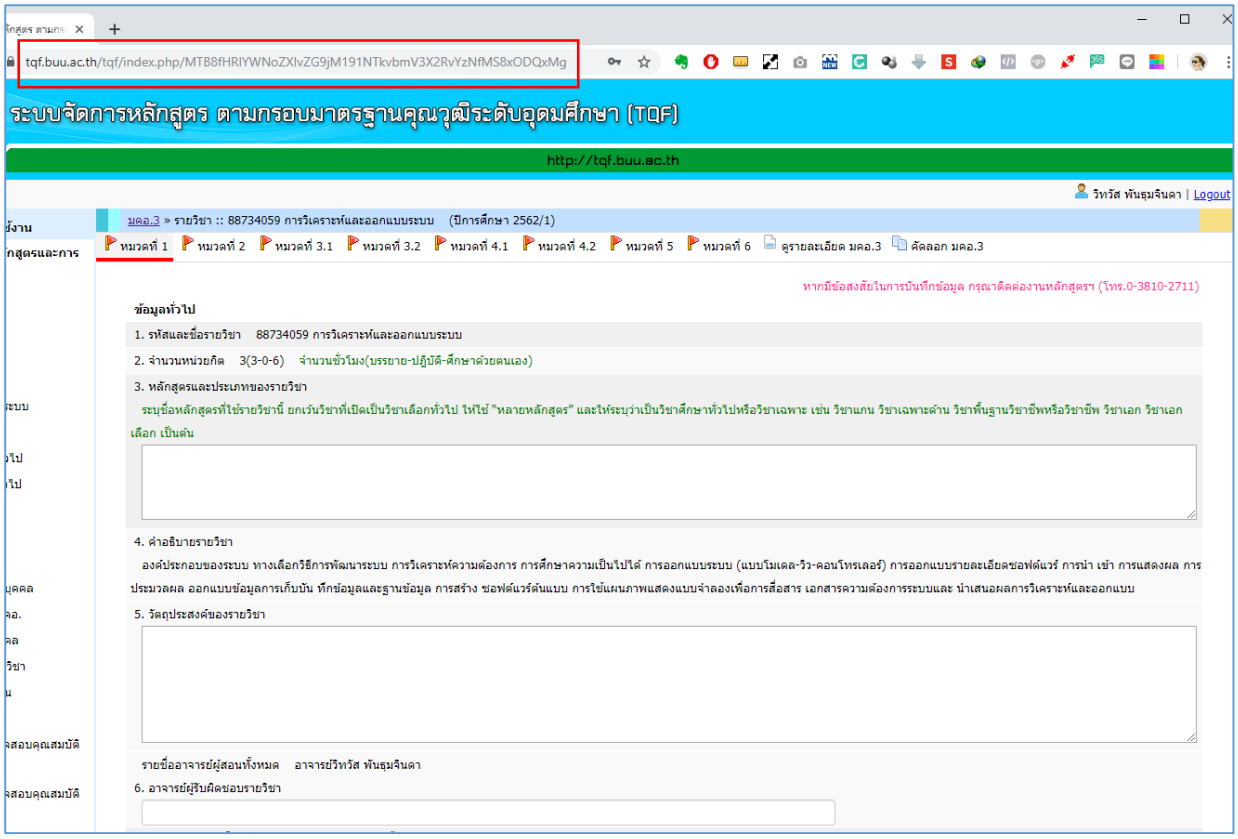
ตัวอย่างการเข้าถึงข้อมูลที่ได้กำหนด Permission

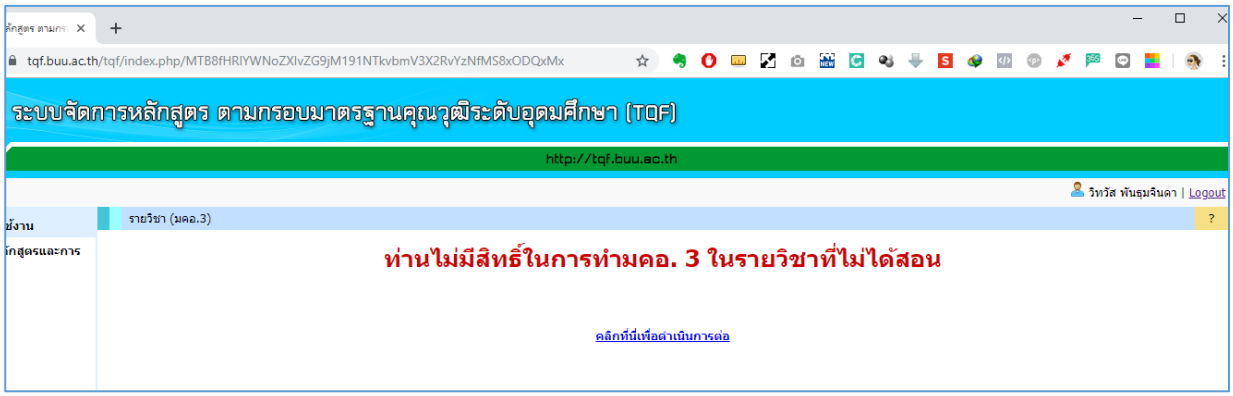


จากตัวอย่าง ในกรอบสีแดงจะเห็นว่า เราสามารถเปลี่ยนตัวเลข เพื่อต้องการเข้าถึงข้อมูลที่ไม่ใช่ของตัวเองได้ แต่เราจะต้องกำหนดการเข้าถึงข้อมูลที่โปรแกรมด้วย เมื่อลองเปลี่ยนแปลงข้อมูล แล้วไม่ใช่ข้อมูลที่จะสามารถเข้าถึงได้ จะต้องแจ้งต่อผู้ใช้งานด้วย ดังภาพ



หรือการป้องการด้วยการเข้ารหัส (Encrypt URL) เพื่อป้องกันการเข้าถึงข้อมูลของผู้อื่น


tqf.buu.ac.th/tqf/index.php/MTB8fHRlYWNoZXIvZG9jM191NTkvbmV3X2RvYzNfMS8xODQxMg
ระบบจัดการหลักสูตร ตามกรอบมาตรฐานคุณวุฒิระดับอุดมศึกษา (TQF)
http://tqf.buu.ac.th
วิทวัส พันธุมจินดา | Logout
มคอ.3 » รายวิชา :: 88734059 การวิเคราะห์และออกแบบระบบ (ปีการศึกษา 2562/1)
หมวดที่ 1
หมวดที่ 2
หมวดที่ 3.1
หมวดที่ 3.2
หมวดที่ 4.1
หมวดที่ 4.2
หมวดที่ 5
หมวดที่ 6
ดูรายละเอียด มคอ.3
คัดลอก มคอ.3
หากมีข้อสงสัยในการบันทึกข้อมูล กรุณาติดต่องานหลักสูตรฯ (โทร.0-3810-2711)
ข้อมูลทั่วไป
1. รหัสและชื่อรายวิชา 88734059 การวิเคราะห์และออกแบบระบบ
2. จำนวนหน่วยกิต 3(3-0-6) จำนวนชั่วโมง(บรรยาย-ปฏิบัติ-ศึกษาด้วยตนเอง)
3. หลักสูตรและประเภทของรายวิชา
ระบุชื่อหลักสูตรที่ใช้รายวิชานี้ ยกเว้นวิชาที่เปิดเป็นวิชาเลือกทั่วไป ให้ใช้ "หลายหลักสูตร" และให้ระบุว่าเป็นวิชาศึกษาทั่วไปหรือวิชาเฉพาะ เช่น วิชาแกน วิชาเฉพาะด้าน วิชาพื้นฐานวิชาชีพหรือวิชาชีพ วิชาเอก วิชาเอกเลือก เป็นต้น
4. คำอธิบายรายวิชา
องค์ประกอบของระบบ ทางเลือกวิธีการพัฒนาระบบ การวิเคราะห์ความต้องการ การศึกษาความเป็นไปได้ การออกแบบระบบ (แบบโมเดล-วิว-คอนโทรเลอร์) การออกแบบรายละเอียดซอฟต์แวร์ การนำ เข้า การแสดงผล การประมวลผล ออกแบบข้อมูลการเก็บบัน ทึกข้อมูลและฐานข้อมูล การสร้าง ซอฟต์แวร์ต้นแบบ การใช้แผนภาพแสดงแบบจำลองเพื่อการสื่อสาร เอกสารความต้องการระบบและ นำเสนอผลการวิเคราะห์และออกแบบ
5. วัตถุประสงค์ของรายวิชา
รายชื่ออาจารย์ผู้สอนทั้งหมด อาจารย์วิทวัส พันธุมจินดา
6. อาจารย์ผู้รับผิดชอบรายวิชา


tqf.buu.ac.th/tqf/index.php/MTB8fHRlYWNoZXIvZG9jM191NTkvbmV3X2RvYzNfMS8xODQxMx
ระบบจัดการหลักสูตร ตามกรอบมาตรฐานคุณวุฒิระดับอุดมศึกษา (TQF)
http://tqf.buu.ac.th
วิทวัส พันธุมจินดา | Logout
รายวิชา (มคอ.3)
ท่านไม่มีสิทธิ์ในการทำมคอ. 3 ในรายวิชาที่ไม่ได้สอน
คลิกที่นี่เพื่อดำเนินการต่อ

Controller.php

เขียนฟังก์ชันเช็คเงื่อนไขเพื่อตรวจสอบสิทธิ์การเข้าถึงข้อมูล

```
    //ใช้ในการจัดการแท็บแต่ละแท็บ
    public function new_doc3_1($DOC3_ID='')
    {
        if($DOC3_ID=='')
        {
            $this->content = $this->load->view('teacher/doc3/no_access3_view', $this->data, TRUE);
            $this->output();
        }else{
            /************ Navigate **************/
            $this->load->model('tqftdoc3_u59_model', 'doc3');
            $doc3 = $this->doc3;
            $qry_doc3 = $doc3->get_by_doc3id($DOC3_ID);
            $data['row_d3'] = $row_d3 = $qry_doc3->row();
            /************ Navigate **************/

            /************ Check Permission **************/
            $PSN_ID = $this->session->userdata('PSN_ID');
            $this->load->model('tqftteach_model');
            $teach = $this->tqftteach_model;
            $qry_teacher = $teach->get_course_psn($PSN_ID,$row_d3->COU_ID, $row_d3->TEACH_YEAR, $row_d3->TEACH_SEMESTER, $row_d3->
REVISIONCODE);
            if($qry_teacher === FALSE)
            {
                $this->content = $this->load->view('teacher/doc3/no_access3_view', $this->data, TRUE);
                $this->output();
            }else{

                $data['DOC3_ID'] = $DOC3_ID;
                $data['method'] = 'add';
                $this->content = $this->load->view('teacher/doc3/doc3_u59_part1_add_view', $data, TRUE);
                $this->output();

            }
```

View.php

เขียนข้อความแจ้งเตือนถึงการละเมิดสิทธิ์การใช้งาน

```
<div align="center">
    <h1><font color="#CC0000"><?php echo 'ท่านไม่มีสิทธิ์ในการทำคอ. 3 ในรายวิชาที่ไม่ได้สอน ';?></font></h1>
    <br />
    <h4><?php echo anchor('logoutn/system_logout', 'คลิกที่นี่เพื่อดำเนินการต่อ') ;?></h4>
</div>
```