

ภาคผนวก ค
รหัสโปรแกรม

Index.php

```

<?
include "chkuser.php";
include "connect.php";
include "function.php";
?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-874" />
<title>&#3585;&#3634;&#3619;&#3592;&#3633;&#3604;&#3585;&#3634;&#3619;&#358
8;&#3623;&#3634;&#3617;&#3619;&#3641;&#3657;&#3585;&#3621;&#3640;&#3656;&#
3617;&#3591;&#3634;&#3609;&#3623;&#3636;&#3592;&#3633;&#3618;</title>
<style type="text/css">
<!--
@import url("css/rmutt.css");
body {
    margin-left: 0px;
    margin-top: 0px;
    margin-right: 0px;
    margin-bottom: 0px;
    background-color: #333333;
}
-->
</style>

<tr>
    <td><? include "menu.php";?></td>
<table width="970" border="0" align="center" cellpadding="0" cellspacing="0"
bgcolor="#FFFFFF" background="images/bg_stripe.gif">

```

```

<tr>
  <td width="970" align="center" valign="top"><table width="100%" border="0"
align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td colspan="2" align="left" valign="top"><table width="100%" border="0">
      <tr>
        <td width="74%" height="231" align="center" valign="top"></td>
        <td width="26%" valign="top" align="center"><table width="100%"
border="0" align="left" cellpadding="0" cellspacing="1">
          <tr>
            <td align="left" valign="top" ><? include "login.php";?></td>
          </tr>
        </table></td>
      </tr>
    </table></td>
  </tr>
</tr>
<tr>
  <td colspan="2"><table width="96%" border="0" align="left" cellpadding="0"
cellspacing="0">
    <tr>
      <td height="25"><? include "time.php";?></td>
    </tr>
  </table></td>
</tr>
<tr>
  <td width="230" align="center" valign="top" class="line-right"><? include
"left.php";?></td>
  <td width="740" valign="top"><table width="99%" border="0" align="center">
    <tr>

```

```

<td align="center" valign="top"><table border="0" cellspacing="0"
cellpadding="0">
  <tr>
    <td><div align="center"></div></td>
    <td align="left" valign="top"><table width="99%" border="0" align="left"
cellpadding="0" cellspacing="1">
      <tr>
        <td><table width="90%" height="174" border="0" align="center"
cellpadding="0" cellspacing="0">
          <tr>
            <td height="37" align="left" valign="middle" class="head-
register">&#3614;&#3621;&#3633;&#3591;&#3591;&#3634;&#3609;&#3607;&#3604;&#
3649;&#3607;&#3609;</td>
          </tr>
          <tr>
            <td height="108" align="left" valign="middle" class="font-
tite">&#3614;&#3621;&#3633;&#3591;&#3591;&#3634;&#3609;&#3608;&#3619;&#3619
&#3617;&#3594;&#3634;&#3605;&#3636;&#3611;&#3619;&#3632;&#3648;&#3616;&#3
607;&#3651;&#3594;&#3657;&#3652;&#3617;&#3656;&#3627;&#3617;&#3604;&#3648;
&#3611;&#3621;&#3639;&#3629;&#3591;&#3626;&#3634;&#3617;&#3634;&#3619;&#3
606;&#3627;&#3617;&#3640;&#3609;&#3648;&#3623;&#3637;&#3618;&#3609;&#3617;
&#3634;&#3651;&#3594;&#3657;&#3648;&#3611;&#3655;&#3609;&#3611;&#3619;&#3
632;&#3592;&#3635; &#3648;&#3594;&#3656;&#3609;
&#3614;&#3621;&#3633;&#3591;&#3591;&#3634;&#3609;&#3621;&#3617;
&#3614;&#3621;&#3633;&#3591;&#3591;&#3634;&#3609;&#3649;&#3626;&#3591;&#3
629;&#3634;&#3607;&#3636;&#3605;&#3618;&#3660;
&#3614;&#3621;&#3633;&#3591;&#3591;&#3634;&#3609;&#3585;&#3658;&#3634;&#3
595;&#3594;&#3637;&#3623;&#3616;&#3634;&#3614;&#3627;&#3619;&#3639;&#3629;
&#3614;&#3621;&#3633;&#3591;&#3591;&#3634;&#3609;&#3588;&#3621;&#3639;&#3
656;&#3609;&#3649;&#3621;&#3632;&#3629;&#3639;&#3656;&#3609;&#3654;

```

```

&#3595;&#3638;&#3656;&#3591;&#3609;&#3635;&#3617;&#3634;&#3651;&#3594;&#3
657;&#3649;&#3607;&#3609;&#3614;&#3621;&#3633;&#3591;&#3591;&#3634;&#3609;
&#3608;&#3619;&#3619;&#3617;&#3594;&#3634;&#3605;&#3636;&#3611;&#3619;&#3
632;&#3648;&#3616;&#3607;&#3651;&#3594;&#3657;&#3649;&#3621;&#3657;&#3623;
&#3627;&#3617;&#3604;&#3648;&#3611;&#3621;&#3639;&#3629;&#3591;
&#3595;&#3638;&#3656;&#3591;&#3651;&#3594;&#3657;&#3585;&#3633;&#3609;&#3
629;&#3618;&#3641;&#3656;&#3651;&#3609;&#3611;&#3633;&#3592;&#3592;&#3640;
&#3610;&#3633;&#3609; &#3648;&#3594;&#3656;&#3609;
&#3606;&#3656;&#3634;&#3609;&#3627;&#3636;&#3609;
&#3606;&#3656;&#3634;&#3609;&#3652;&#3617;&#3657; &#3615;&#3639;&#3609;
&#3649;&#3619;&#3656;&#3608;&#3634;&#3605;&#3640;
&#3585;&#3658;&#3634;&#3595;&#3608;&#3619;&#3619;&#3617;&#3594;&#3634;&#3
605;&#3636;
&#3609;&#3657;&#3635;&#3617;&#3633;&#3609;&#3648;&#3594;&#3639;&#3657;&#3
629;&#3648;&#3614;&#3621;&#3636;&#3591; . . .</td>

```

```
</tr>
```

```
</table></td>
```

```
</tr>
```

```
</table></td>
```

```
</tr>
```

```
</table></td>
```

```
</tr>
```

```
<tr>
```

```

<td align="center" valign="top"><table width="715" border="0" align="left"
cellpadding="0" cellspacing="0" bgcolor="#FFFFFF" class="line_around">

```

```
<tr>
```

```

<td width="728" height="42" align="left" valign="middle"></td>

```

```

<td width="45" valign="middle"><a href="pr.php" target="_blank"></a></td>

```

```
</tr>
```

```

<tr>
  <td height="7" colspan="2"><table width="99%" border="0" align="right"
cellpadding="0" cellspacing="0">
    <tr>
      <td><? include "in_pr_show.php";?>          </td>
    </tr>
  </table></td>
</tr>
<tr>
  <td height="8" colspan="2" align="right" valign="middle"></td>
</tr>
</table></td>
</tr>
<tr>
  <td valign="top"><table width="715" height="82" border="0" align="left"
cellpadding="0" cellspacing="0" bgcolor="#FFFFFF" class="line_around">
    <tr>
      <td height="39" colspan="2"><table width="100%" border="0"
cellspacing="0" cellpadding="0">
        <tr>
          <td width="90%" align="left" valign="middle"></td>
          <td width="10%" valign="middle"><a href="research.php"
target="_blank"></a></td>
        </tr>
      </table>
    </span></td>
  <td></td>

```

```
 <table width="100%" border="0" cellspacing="0" cellpadding="0"> | |
```

```
<td height="30"><? include "webboard_update.php";?></td>
</tr>
</table></td>
</tr>

</table></td>
</tr>
<tr>
<td colspan="2" align="center" valign="top"><table width="100%" border="0"
cellspacing="0" cellpadding="0">
<tr>
<td align="left" valign="top"><p><? include "footer.php"; ?></p></td>
</tr>
</table></td>
</tr>
</table></td>
</tr>
</table>

</body>
</html>
```


in_show_research.php

```

<?
include "connect.php";
?>

<? /* ตารางโชว์ ผลงานนักวิจัย -----
----- */

$sql="select * from research where
type='<?=$_SESSION["cat_id"]?>' order by id desc ";

$result=mysql_db_query($dbname,$sql);

for ($a=0; $a<10; $a++ ) {
    $data=mysql_fetch_array($result);
    $name=$data['name'];
    $ser=substr($name , 0,45);
    $date=$data['year'];
    $id=$data['id'];
    ?>

    <link href="css/rmutt.css" rel="stylesheet"
type="text/css" />

    <table width="100%" border="0" cellspacing="0"
cellpadding="0">
        <tr>
            <td height="25" width="4" align="center" ></td>
            <td width="24" align="center" class="border-down"></td>
            <td width="333" align="left" valign="middle" class="border-
down"><a href="show_research.php?id=<?=$id?>" target="_blank" class="font">
            &nbsp;<?=$ser?>
            ...</a></td>
            <td width="32" align="center" class="border-down">

```

```

        <div align="center"><span class="color">
        <?=$date?>
        </span></div></td>
    </tr>
    <? } ?>
</table>

        <table width="99%" border="0" cellspacing="0"
cellpadding="0">
        <tr>
        <td height="8"></td>
        </tr>
</table>

```

in_show_news.php

```

<?
include "connect.php";
?>

<? /* ตารางโชว์ ผลงานนักวิจัย -----
----- */

$hi='สาระทั่วไป';
$sql2="select * from news where news='$hi'
and kind='<?=$_SESSION["cat_id"]?>' order by id desc ";
$result2=mysql_db_query($dbname,$sql2);
for ($a=0;$a<10;$a++) {

    $data2=mysql_fetch_array($result2);
    $title=$data2['title'];
    $tit=substr($title , 0,50);
    $id=$data2['id'];
    ?>

    <link href="css/rmutt.css" rel="stylesheet"
type="text/css" />

    <table width="100%" border="0" cellspacing="0"
cellpadding="0">
        <tr>
            <td height="25" width="4" align="center" ></td>
            <td width="24" align="center" class="border-down"></td>
            <td width="333" align="left" valign="middle" class="border-down"><a
href="show_news.php?id=<?=$id?>" target="_blank" class="font"><?=$tit?>
...</a></td>
            <td width="32" align="center" class="border-down"></td>
        </tr>

```

```
<? } ?>
</table>
<table width="99%" border="0" cellspacing="0" cellpadding="0">
  <tr>
    <td height="8"></td>
  </tr>
</table>
```

Function.php

<?

```
function CheckRude($temp){
    $wordrude = array("ashole","a s h o l e","a.s.h.o.l.e","bitch","b i t c
h","b.i.t.c.h","shit","s h i t","s.h.i.t","fuck","dick","f u c k","d i c k","f.u.c.k","d.i.c.k","มึง","มี ง","
มี ง","มี ง","มี ง","มี_ง","มี-ง","มี+ง","กู","ควย","ค ว ย","ค.ว.ย","คอ วอ ยอ","คอ-วอ-ยอ","ปี้","
ห่วย","ไอ้ห่วย","เฮ้ย","ชาติหมา","ชาดหมา","ช ำ ด ห ม ำ","ช.ว.ด.ห.ม.ำ","ช ำ ตี ห ม ำ","ช.ว.ติ.ห.
ม.ำ","สัดหมา","สัด","เย็ด","หี","สันดาน","แม่ง","ระยำ","สันตীন","แดด");
    $wordchange = ("<font color=red>+++</font>");

    for ( $i=0 ; $i<sizeof($wordrude) ; $i++ ){
        $temp = eregi_replace ($wordrude[$i] ,$wordchange ,$temp);
    }
    return ( $temp );
}
```

//(3) ฟังก์ชันแทรกรูปภาพสามารถเพิ่มรูปได้

```
function CheckSmile($temp){
    global $url;
    $text = array(

        ":em01:",":em02:",":em03:",":em04:",":em05:",":em06:",":em07:",":em08:",":em09:",
        ":em10:",":em11:",":em12:",":em13:",":em14:",

        ":em15:",":em16:",":em17:",":em18:",":em19:",":em20:",":em21:",":em22:",":em23:",
        ":em24:",":em25:",":em26:",":em27:",":em28:",

        ":em29:",":em30:",":em31:",":em32:",":em33:",":beer:");

    $pic = array(
```

```
"em01.gif","em02.gif","em03.gif","em04.gif","em05.gif","em06.gif","em07.gif","em08
.gif","em09.gif","em10.gif","em11.gif","em12.gif",
```

```
"em13.gif","em14.gif","em15.gif","em16.gif","em17.gif","em18.gif","em19.gif","em20
.gif","em21.gif","em22.gif","em23.gif","em24.gif",
```

```
"em25.gif","em26.gif","em27.gif","em28.gif","em29.gif","em30.gif","em31.gif","em32
.gif","em33.gif","beer.gif");
```

```
for ($i=0 ; $i<sizeof($text) ; $i++) {
    $temp = eregi_replace($text[$i],"<img
src=\"pic/$pic[$i]\">",$temp);
}
return($temp);
}
```

//(4) ฟังก์ชันตรวจสอบการแทรก Link และ Tag

```
function CheckTag($temp){
    global $url;
    $temp = stripslashes(htmlspecialchars($temp));
    $temp = eregi_replace ( "<" , "&lt;" , $temp ) ;
    $temp = eregi_replace ( ">" , "&gt;" , $temp ) ;

    //สำหรับเปลี่ยนอักขระที่กำหนด ให้เป็นแท็ก html ต่างๆ
    $temp = eregi_replace ( "\[b\]" , "<b>" , $temp ) ;
    $temp = eregi_replace ( "\[/b\]" , "</b>" , $temp ) ;
    $temp = eregi_replace ( "\[br\]" , "<br>" , $temp ) ;
    $temp = eregi_replace ( "\[i\]" , "<i>" , $temp ) ;
    $temp = eregi_replace ( "\[/i\]" , "</i>" , $temp ) ;
    $temp = eregi_replace ( "\[u\]" , "<u>" , $temp ) ;
```



```

$temp = eregi_replace (" ([:alnum:]]+)//(?:[:space:]]*)([:alnum:]]#?/=&=)
"," <a href=\"\\1:/^2\\3\" target=\"_blank\">\\1:/^2\\3</a> ",$temp ) ;

```

```

// สร้างลิ้งค์ URL ที่แทรกคำสั่งเข้ามา (ต่างกันที่การเว้นช่องว่างหลังอย่างเดียว)
$temp = eregi_replace (" ([:alnum:]]+)//(?:[:space:]]*)([:alnum:]]#?/=&=)
"," <a href=\"\\1:/^2\\3\" target=\"_blank\">\\1:/^2\\3</a> ",$temp ) ;

```

```

//สร้างลิ้งค์อีเมล
$temp = eregi_replace ("(?:[:space:]]*)@(?:[:space:]]*)([:alnum:]])", "<a
href=\"./mail2me/mail2me.php?wemail=\\1@\\2\\3&name=\\1@\\2\\3\"
target=\"_blank\">\\1@\\2\\3</a>",$temp ) ;

```

```

return ( $temp ) ;
}
function alert($msg){
    echo "<script type=\"text/javascript\">alert('$msg') </script>";
}

```

```

function go_re($go){
    ?>
    <script type="text/javascript">
    location.replace('<? echo $go ?>');
    </script>
    <?
}

```

```

function getIP(){
    // ตรวจสอบ IP กรณีการใช้งาน share internet
    if(!empty($_SERVER['HTTP_CLIENT_IP'])){
        $ip=$_SERVER['HTTP_CLIENT_IP'];
    }else{
        $ip=$_SERVER['REMOTE_ADDR'];
    }
}

```



```

        return $ip;
    }

    function set_log($event,$detail,$page,$address){
        include "connect.php";
        $sql="insert into
security_log(event,detail,page,address)values('$event','$detail','$page','$address') ";
        $result=mysql_db_query($dbname,$sql);
    }

    function atk_check($str){
        if((strrpos($str, '"') != false) || (strrpos($str, "'") != false) || (strrpos($str, ';')!=
false)){
            //echo '<script> alert("atk"); </script>';
            set_log("injection",$str,curPageURL(),getIP());
        }
    }

    function curPageURL() {
        $pageURL = 'http';
        if ($_SERVER["HTTPS"] == "on") {$pageURL .= "s";}
        $pageURL .= "://";
        if ($_SERVER["SERVER_PORT"] != "80") {
            $pageURL .=
$_SERVER["SERVER_NAME"].":".$_SERVER["SERVER_PORT"].$_SERVER["REQUEST_URI"];
        } else {
            $pageURL .= $_SERVER["SERVER_NAME"].$_SERVER["REQUEST_URI"];
        }
        return $pageURL;
    }

    function curPageName() {
        return substr($_SERVER["SCRIPT_NAME"],strrpos($_SERVER["SCRIPT_NAME"],"/")+1);
    }

?>

```

Login_get.php

```

<?
session_start();
?>

<meta http-equiv="Content-Type" content="text/html; charset=windows-874" />
<?

include "connect.php";
include "function.php";
$user=$_REQUEST['user'];
$pass=$_REQUEST['pass'];

$user_fix = mysql_real_escape_string($user); //แปลงข้อมูลที่รับเข้าเพื่อป้องกันการโจมตีทาง
input
$pass_fix = mysql_real_escape_string($pass); //แปลงข้อมูลที่รับเข้าเพื่อป้องกันการโจมตีทาง
input

atk_check($user_fix);          //ตรวจสอบการโจมตีพร้อมทั้งบันทึกการโจมตีลงฐานข้อมูล
atk_check($pass_fix);          //ตรวจสอบการโจมตีพร้อมทั้งบันทึกการโจมตีลงฐานข้อมูล

// เปรียบค่าที่ส่งมา ว่าว่างหรือไม่
if ($user=="" or $pass=="") {
    echo '<script> alert("กรอกข้อมูลไม่ครบค่ะ"); </script>';
    echo "<script>window.location.href='index.php'</script>";
    die;
}

//เข้ารหัสและเทียบ username และ password
$pass=md5(base64_encode($pass_fix));
$sql="select * from register WHERE username='$user_fix' and password='$pass' ";
$result=mysql_db_query($dbname,$sql);
$ses=mysql_fetch_array($result);
$id =$ses['id'];
$member=$ses['member'];

```

```

if (!$ses) {
    echo '<script> alert("Password ผิด ! หรือ ID นี้ไม่มีอยู่ในระบบ"); </script>';
    echo "<script>window.location.href='index.php'</script>";
    die();
}
// ถ้าไม่ใช่สมาชิก นักวิจัย หรือ ผู้ดูแลระบบ จะเข้าเงื่อนไขนี้
if ($member != 'รออนิน') {

    $_SESSION[comid]=session_id();
    $_SESSION[userlogin]=$user;
    $_SESSION[u_type]=$member;

    ////////////////////////////////////* เก็บค่าแบบคุกกี้ *////////////////////////////////////
    //setcookie("username",$user,time()+3600);
    echo "<script>window.location.href='index.php'</script>";
} else {
    echo '<script> alert("กรุณารอการตอบรับของผู้ดูแลค่ะ"); </script>';
    echo "<script>window.location.href='index.php'</script>";
}
mysql_close();
?>

```