ใบงานการทดลอง

วิทยาการเข้ารหัสลับ (Cryptography)

จุดประสงค์การเรียนรู้

1. เพื่อศึกษาการออกแบบและใช้งาน Cryptography ขั้นพื้นฐาน
2. เพื่อศึกษาการประยุกต์การใช้ Cryptography สำหรับเว็บไซต์

คำอธิบาย ขั้นตอน/วิธีการ

การศึกษาครั้งนี้ใช้ภาษา PHP สำหรับเขียนเว็บไซต์เพื่อทดสอบการเข้ารหัสและถอดรหัสข้อมูล โดยให้นักศึกษาทำการเขียนโปรแกรมตามโจทย์ที่กำหนดไว้ พร้อมตอบคำถาม หากทำเสร็จแล้วสามารถเรียกตรวจและส่งใบงานได้

ตอนที่ 1 การรับส่งข้อมูลแบบ GET และ POST

1. ติดตั้งโปรแกรม AMPPS เพื่อทำหน้าที่เป็นเว็บเซิร์ฟเวอร์
2. เขียนโปรแกรมตามตัวอย่างและบันทึกไว้ที่ตำแหน่ง C:\Program Files (x86)\Ampps\www

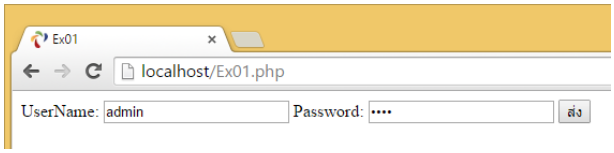
Ex01.php

```php
<html>
<head>
  <title>Ex01</title>
</head>

<body>
<form action="Ex02.php" method="get">
UserName: <input type="text" name="username" />
Password: <input type="password" name="password" />
<input type="submit" />
</form>

</body>
</html>
```

Ex02.php

```php
<?php

echo "Name : ".$_GET["username"]."<br>";
echo "Age : ".$_GET["password"]."<br>";

?>
```

3. เปิด Browser เพื่อรันไฟล์ Ex01.php และป้อนชื่อผู้ใช้และรหัสผ่าน ตัวอย่างดังภาพ



Address Bar ของ Browser โชว์ตัวแปรและข้อมูล .....

4. เขียนโปรแกรมตามตัวอย่างและบันทึกไว้ที่ตำแหน่ง C:\Program Files (x86)\Ampps\www

Ex03.php

```php
<html>
<head>
  <title>Ex03</title>
</head>

<body>
<form action="Ex04.php" method="post">
UserName: <input type="text" name="username" />
Password: <input type="password" name="password" />
<input type="submit" />
</form>

</body>
</html>
```

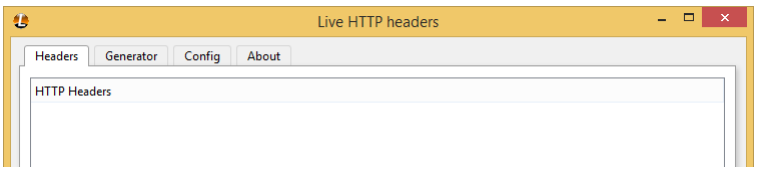
Ex04.php

```php
<?php

echo "Name : ".$_POST["username"]."<br>";
echo "Password : ".$_POST["password"]."<br>";

?>
```

5. เปิด Browser เพื่อรันไฟล์ Ex03.php และป้อนชื่อผู้ใช้และรหัสผ่าน

Address Bar ของ Browser โชว์ตัวแปรและข้อมูล .....

6. ติดตั้งโปรแกรม OWASP Mantra Security Toolkit (http://www.getmantra.com/owasp-mantra.html) เปิดโปรแกรมและกดที่ไอคอน  (Live HTTP headers) จะแถบหน้าต่างดังภาพ



7. รันไฟล์ Ex03.php พร้อมป้อนชื่อผู้ใช้และรหัสผ่าน และตรวจสอบข้อมูลที่หน้าต่าง Live HTTP headers

Method : .....

Host : .....

User-Agent : .....

Referer : .....

Content-Length : .....

การใช้ Method POST ข้างต้นสามารถรักษาความลับของข้อมูลได้หรือไม่เพราะเหตุใด.....

.....

.....

.....

ตอนที่ 2 การใช้การเข้ารหัสสำหรับการรับ/ส่งข้อมูลบนเว็บไซต์

1. เขียนโปรแกรมตามตัวอย่างและบันทึกไว้ที่ตำแหน่ง C:\Program Files (x86)\Ampps\www

Function.php

```php
<?php
function encrypt_decrypt($action, $string) {
    $output = false;

    $encrypt_method = "AES-256-CBC";
    $secret_key = 'SecretKey';
    $secret_iv = 'SecretIV';

    // hash
    $key = hash('sha256', $secret_key);

    // iv - encrypt method AES-256-CBC expects 16 bytes - else you will get a warning
    $iv = substr(hash('sha256', $secret_iv), 0, 16);

    if( $action == 'encrypt' ) {
        $output = openssl_encrypt($string, $encrypt_method, $key, 0, $iv);
        $output = base64_encode($output);
    }
    else if( $action == 'decrypt' ){
        $output = openssl_decrypt(base64_decode($string), $encrypt_method, $key, 0, $iv);
    }
    return $output;
}
?>
```

Ex05.php

```php
<html>
<head>
  <title>Ex05</title>
</head>
<body>
<?php
include ("Function.php");
$username = encrypt_decrypt("encrypt","admin");
$password = encrypt_decrypt("encrypt","myPassword1234");

?>
<a href="Ex06.php?username=<?php echo $username; ?>&password=<?php echo $password; ?>">Login</a>

</body>
</html>
```

Ex06.php

```php
<?php

include ("Function.php");

echo "UserName : ".$_GET["username"]."<br>";
echo "Password : ".$_GET["password"]."<br>";
echo "UserName Decrypt : ".encrypt_decrypt("decrypt",$_GET["username"])."<br>";
echo "Password Decrypt : ".encrypt_decrypt("decrypt",$_GET["password"]);

?>
```

2. เปิด Browser เพื่อรันไฟล์ Ex05.php และป้อนชื่อผู้ใช้และรหัสผ่าน

3. ใช้ OWASP Mantra Security Toolkit เลือก Live HTTP headers เพื่อ Capture http header
หากมีการดักจับข้อมูล สามารถเข้าใจเนื้อหาของ username และ password ได้หรือไม่ เพราะเหตุใด.....

.....

.....

.....

.....

.....

4. หากต้องการเข้ารหัสข้อมูลของฟอร์ม(POST,GET) ก่อนส่งข้อมูลไปยังเซิร์ฟเวอร์ สามารถทำด้วยวิธีการใดได้บ้าง อย่างไร จงอธิบาย

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

ชื่อ.....สกุล.....รหัสนักศึกษา..... .....สาขา.....