

การศึกษาและจำลองการหาช่องโหว่ที่เกิดขึ้นในระบบ
ในรูปแบบ Capture The Flag (CTF)
Capture the flag practices model : identified
vulnerability in system

นายจักรพรรดิ สุวรรณโณ
(Jakkrapat Suwanno) 61070022

นายตินต์ โตสงวน
(Tin Tosanguan) 61070061

นายธนพล จันทร์ละออ
(Thanapon Chanlaor) 61070071

นายธนพล มาติกานนท์
(Thanapon Matikanon) 61070072

นายธนวัฒน์ เขมวัชรเลิศ
(Thanawat Kemwatcharalert) 61070074

นายอริณชัย อวยเจริญ
(Arin Auycharoen) 61070350

ABSTRACT – The purpose of this test is designed for those who want to seek Vulnerability in the system by the features of their website, Presented in the form of the CTF (Capture The Flag) that simulate an E-Commerce Website on PHP Which is a language that currently in use .This website has the basic subsystems of an e-commerce website, such as a search engine, add products, apply for membership, etc. We assumed that the developers of this website do not have enough knowledge of web security and there are vulnerabilities for attackers to attack the system. In this test suite, SQL Injection is used primarily for system attacks. When the player can attack the correct point, Players will receive a flag indicating that the Player has successfully attacked the system.

KEY WORDS – CTF, E-commerce, SQL Injection, Flag, Vulnerability

บทคัดย่อ – ชุดทดสอบนี้ มีจุดประสงค์จัดทำขึ้นเพื่อเป็นชุดทดสอบสำหรับผู้ที่ต้องการหาช่องโหว่เกี่ยวกับระบบเว็บไซต์ของตนเอง โดยมีการนำเสนอในรูปแบบของ CTF (Capture The Flag) ที่มีจำลองระบบ E-commerce ขึ้นมาในรูปแบบของเว็บไซต์บนภาษา PHP ซึ่งเป็นภาษาที่ในปัจจุบันนี้ยังมีการใช้งานอยู่ โดยเว็บไซต์นี้มีระบบย่อยที่เป็นพื้นฐานของเว็บไซต์ E-commerce เช่น ระบบค้นหาสินค้า เพิ่มสินค้า สมัครสมาชิก เป็นต้น โดยที่เราได้สมมติว่าผู้พัฒนาเว็บไซต์นี้ยังไม่มีความสามารถด้าน web security มากพอ ยังมีบางระบบหรือบางช่องทางที่ยังมีช่องโหว่ให้กับผู้ไม่หวังดีเข้าไปทำการโจมตีระบบได้ โดยในชุดทดสอบนี้จะมีการใช้หลักการ SQL Injection เป็นหลัก ในการโจมตีระบบ เมื่อผู้เล่นสามารถโจมตีจุดที่ถูกต้อง ผู้เล่นจะได้รับ Flag เพื่อบอกว่าผู้เล่นโจมตีระบบสำเร็จแล้ว เมื่อผู้เล่นโจมตีครบแล้ว ตามที่โจทย์ต้องการ เป็นอันสำเร็จของชุดทดสอบชุดนี้

คำสำคัญ – CTF, E-commerce, SQL Injection, Flag, ช่องโหว่

1. บทนำ

1.1. ความเป็นมา

ในการพัฒนาเว็บไซต์ขึ้นมา ตัวระบบนั้นควรจะมีการรักษาความปลอดภัยที่ดีพอเพื่อสร้างความเชื่อมั่นให้กับผู้ใช้ โดยเฉพาะเว็บไซต์ที่มีการเก็บข้อมูลส่วนตัวของผู้ใช้ ทั้ง ชื่อ ที่อยู่ บัตรประจำตัวประชาชน รหัสบัตรเครดิต และอื่นๆอีกมากมาย ที่ถือเป็นทรัพย์สินของผู้ใช้ ที่มีมูลค่า ดังนั้นแล้ว การสร้างความปลอดภัยให้เว็บไซต์ที่มีการเก็บข้อมูลดังกล่าว จึงจำเป็นอย่างยิ่งที่ต้องมีระบบความปลอดภัยที่ดีมากพอ ผู้ใช้จึงจะไว้วางใจและใช้บริการนั้นๆ นั่นเอง เพราะถ้าหากข้อมูลรั่วไหล จะส่งผลกระทบต่ออย่างร้ายแรงโดยเฉพาะอย่างยิ่ง ผู้ให้บริการเว็บไซต์นั้นๆ ที่มีอาจปกปิดความลับของผู้ใช้ได้

ดังนั้นแล้ว ทางพวกเรา ได้จัดทำเว็บไซต์จำลองซึ่งให้บริการด้าน E-Commerce ขึ้นมา ให้ผู้ใช้ได้ทำการทดลอง หาช่องโหว่ต่างๆที่อาจถูกดูดแล้วหรือยังไม่ได้ดูด เพื่อหา flag (ที่อาจหมายถึงข้อมูลสำคัญของ User) ในระบบ เพื่อเป็นการฝึกหาช่องโหว่ของระบบในเบื้องต้น เพื่อเป็นแนวทางในการป้องกันและพัฒนาเว็บไซต์ต่อไป โดยใช้หลักและวิธีที่เรียกว่า SQL Injection (SQLi)

1.2. ความมุ่งหมายและวัตถุประสงค์

ชุดทดสอบนี้ มีจุดประสงค์เพื่อที่จะให้ผู้ที่สนใจในด้าน Network Security หรือ หรืออื่น ๆ ได้ทำการทดลองหาช่องโหว่เบื้องต้นด้วยตนเอง เพื่อที่จะเป็นการประเมินความปลอดภัยแบบเบื้องต้นของเว็บไซต์ต่าง ๆ โดยเราคาดหวังว่า ผู้เข้าศึกษาโครงการนั้น จะได้ ความรู้ แนวคิดและไอเดียที่ได้ นำไปใช้ให้เกิดประโยชน์ ในด้านการพัฒนาความปลอดภัยของระบบทั้งของตนเองและผู้อื่นมากขึ้น และเป็นแนวทางที่ทำให้ผู้ศึกษาเข้าใจแนวทางความปลอดภัยของระบบต่อไป

2. ทบทวนวรรณกรรม

การทำ Capture The Flag หรือที่รู้จักกันในชื่อ CTF ถือเป็นการเรียนรู้รูปแบบหนึ่ง โดยให้ผู้เรียนได้ฝึกฝนด้วยการทำโจทย์ ทาง Cyber Security โดยใช้หลักการ Gamification ช่วยให้ผู้เรียนรู้สึกอยากทำโจทย์ ด้วยสภาพแวดล้อมของการแข่งขัน มีการเก็บคะแนน และจัดอันดับของผู้เรียน ซึ่งได้ผลดีกว่าการเรียนรู้โดยเป็นผู้รับสารอย่างเดียว เพราะเป็นการทำให้

ผู้เรียนไม่เบื่อในเนื้อหานั้นๆ ซึ่งโจทย์ของการทำ CTF นั้น มีได้หลากหลายรูปแบบตามแต่ผู้ออกโจทย์จะกำหนด โดยผู้ออกโจทย์จะกำหนดเพียงขอบเขตของโจทย์ในข้อนั้นๆ ซึ่งผู้จัดทำได้นำเรื่อง SQL Injection มาเป็นโจทย์ในการทำ CTF นี้ เพื่อให้หลายๆ คนได้เข้าใจถึงเนื้อหาของ SQL และ SQL Injection มากยิ่งขึ้น [1] ในเว็บไซต์และระบบหลายๆ อย่างที่อยู่บนอินเทอร์เน็ตทั่วโลก ใช้การเก็บข้อมูลลงบนฐานข้อมูล ที่เรียกว่า Relational Database ซึ่งการเก็บข้อมูลในรูปแบบข้างต้นสามารถถูกโจมตีได้จากการ SQL Injection ซึ่งการโจมตีดังกล่าวเป็นการโจมตีทางอ้อม โดยการเข้าถึงฐานข้อมูลด้วยวิธีดัดแปลง SQL Statements โดยการใส่คำสั่งเรียกข้อมูลจากฐานข้อมูล ผ่านทางช่องรับค่าข้อมูลของเว็บไซต์ที่ผู้ไม่หวังดีต้องการโจมตี ทางผู้จัดทำ จึงได้จำลองเว็บไซต์ที่เป็นระบบ E-commerce ขึ้นมา เพื่อใช้ในการศึกษาการทำ SQL Injection พร้อมทั้งได้ฝึกทำโจทย์ CTF ไปพร้อมกันด้วย[2][3]

3. แนวคิด / วิธีการที่นำเสนอ

3.1. เข้าถึงฐานข้อมูล ด้วยช่องทางที่ผู้พัฒนา อาจละเลยหรือประมาทในการอุดช่องโหว่

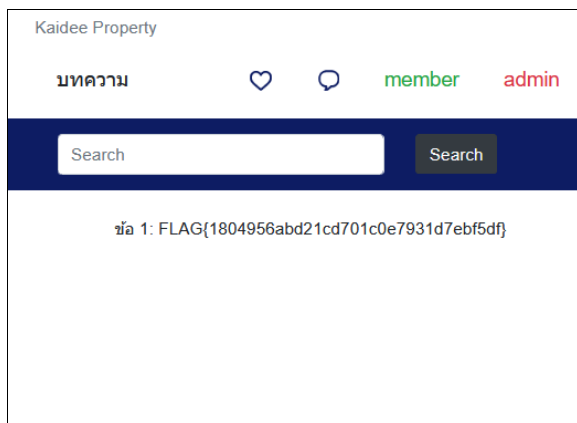
เว็บไซต์ส่วนมากนั้นมีการป้องกันการ SQL Injection ผ่านช่องทางการ Input ต่าง ๆ เช่น Login ซึ่งเป็น Input ที่ผู้ใช้แทบทุกคนต้องกรอกก่อนที่จะใช้งานเว็บไซต์ แต่ก็อาจมีบางกรณีที่ผู้พัฒนาอาจจะประมาทที่จะดัก Input และอาจไม่ได้ป้องกันการ SQLi ผ่านช่องทาง Input อื่น ๆ ที่มีการเข้าถึงฐานข้อมูลเหมือนกัน ในกรณีของโครงงานของเรานั้น มีการป้องกันการ SQLi ในส่วนของการ Log in / Register ไว้อย่างดี ซึ่งเราได้ทำการค้นช่องโหว่ ที่เป็น Input อื่น ๆ และเราได้ทำงานใช้ ช่องการค้นหา (Search Bar) เป็น Input หลักในการทำ SQLi

3.2. Piggy-backed Queries

เป็นการวิธีการที่สามารถ execute คำสั่ง SQL Query ได้หลายคำสั่งโดยไม่มีข้อจำกัด ซึ่งเป็นช่องโหว่ที่มีความร้ายแรงมาก เพราะสามารถทำอะไรกับฐานข้อมูลได้หมดเลย ไม่มีข้อจำกัด โดยที่ในชุดทดสอบนี้ได้เปิดช่องโหว่นี้ไว้บางส่วนเพื่อให้ผู้เล่นได้เข้าใจถึงวิธีการทำงานของมัน

4. ผลการทดลองและคำอธิบายรายละเอียด

ทำการเปลี่ยน Role จาก member ให้เป็น Admin โดยอาศัยช่องโหว่ผ่าน Input ในเว็บไซต์ ในที่นี้เราใช้ช่อง Search (ช่องค้นหาสินค้า) และทำการ SQL injection เข้าไป โดยใช้คำสั่ง Update เพื่อเปลี่ยนแปลงสถานะของผู้ใช้ให้เป็นระดับ Admin และมีสิทธิในการเข้าถึงข้อมูลต่างๆในเว็บ



รูปภาพ 1 ตัวอย่างการเข้าเข้าถึง role admin

5. บทสรุปและการอภิปราย

จากการทดลองพบว่าเว็บไซต์ที่ได้จำลองมานี้ ไม่มีความปลอดภัย ทั้งโครงสร้างเว็บและโครงสร้างฐานข้อมูล ซึ่งมันเป็นช่องโหว่ที่สามารถพบได้ในเว็บไซต์ที่สร้างมานานแล้ว หรือเว็บไซต์ที่ไม่ได้ป้องกันมากพอ ทางผู้จัดทำไม่ได้มีจุดประสงค์ที่จะให้ผู้เล่นนำความรู้เหล่านี้ไปโจมตีเว็บไซต์หรือระบบของผู้อื่น แต่ให้นำความรู้ที่ได้นี้ไปประยุกต์ใช้กับเว็บไซต์ของตัวเอง เพื่อให้เว็บไซต์ที่พัฒนาตลอดช่องโหว่ที่จะโดนโจมตี

เอกสารอ้างอิง

- [1] Lucas McDaniel, Erik Talvi, Brain Hay, "Capture the Flag as Cyber Security Introduction" Hawaii International Conference on System Sciences, IEEE, pp.5479-5480 2016
- [2] Rajashree A. Katole, Dr. Swati S. Sherekar, Dr. Vilas M. Thakare, "Detection of SQL Injection Attacks by Removing the Parameter Values of SQL Query" Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018), IEEE, pp.736, 2018
- [3] A. Sadeghian, M. Zamani, S. M. Abdullah, "A taxonomy of SQL Injection Attacks" International Conference on Informatics and Creative Multimedia, IEEE, pp.269, 2013

Appendix

1. ทำการติดตั้งตัว Project

1.1. ติดตั้ง docker และตรวจสอบว่าสามารถใช้งาน docker-compose ได้หรือไม่

Download - <https://docs.docker.com/get-docker/>

1.2. ทำการ clone <https://github.com/ongsuwannoo/secure>

1.3. แยกไฟล์ตัว Project ออกมา

1.4. การแก้ไขไฟล์ config.php เพื่อให้สามารถใช้งานฟังก์ชันการ forgot password ได้ เพราะต้องใช้ email จริงในการส่ง email หาผู้อื่น

1.4.1. ทำการ เปิด “การเข้าถึงของแอปที่มีความปลอดภัยน้อย” (กรณีเป็น Gmail)

ไปที่ <https://www.google.com/settings/u/0/security/lesssecureapps> และทำการเปิด

1.4.2. แก้ไขไฟล์ /www/secure/config.php

```
$CONFIG['email_username'] = '*****@gmail.com';  
$CONFIG['email_password'] = '*****';
```

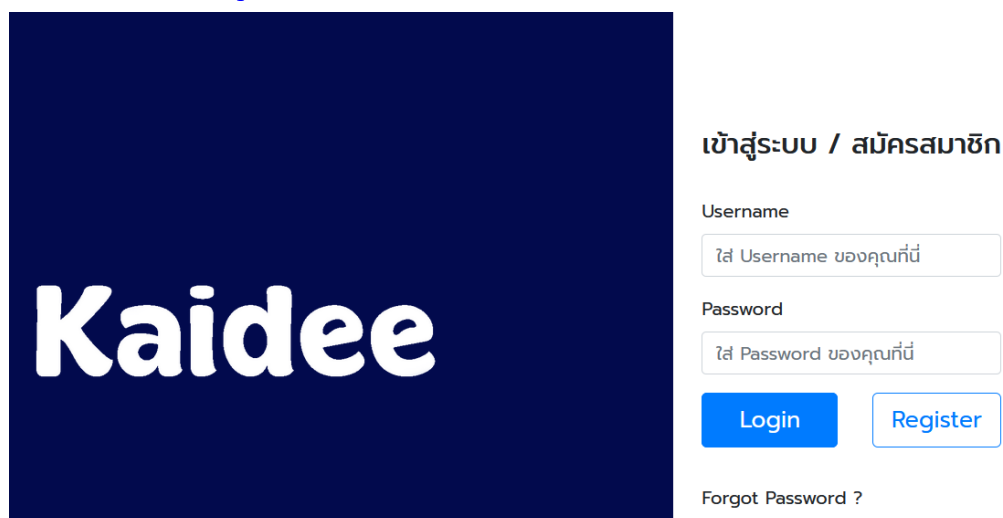
ให้เป็น Email ที่ใช้ได้

1.5. ใช้คำสั่ง docker-compose up -d เพื่อรัน docker

2. การเตรียมความพร้อมเพื่อใช้งานเว็บไซต์

2.1. การสมัครเพื่อเข้าถึงจอทซ์

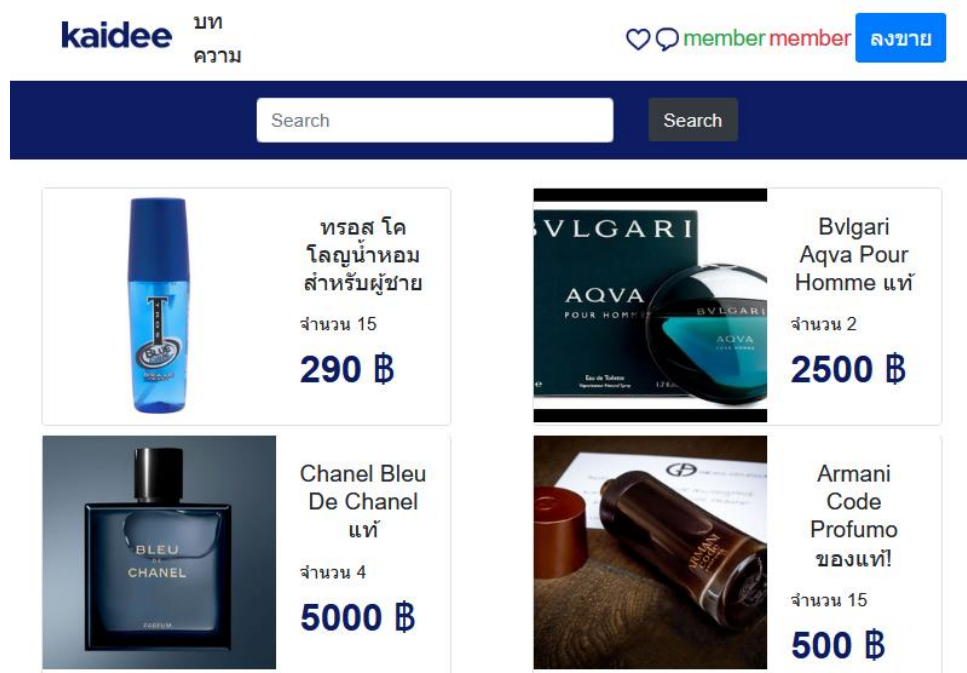
2.1.1. เปิด <http://127.0.0.1>



รูปภาพ 2 หน้า Login

2.1.2. เปิดเว็บมาจะเจอกับหน้า login ให้ทำการสมัคร user ให้เรียบร้อย

2.1.3. เมื่อ login แล้วจะเข้าสู่หน้า Index พร้อมทำชุดทดสอบแล้ว



รูปภาพ 3 หน้า Index หน้าหลักแสดงรายการสินค้า

2.2. การส่งคำตอบ

2.2.1. เปิด <https://fir-ca8a6.web.app/>

2.2.2. สมัครสมาชิกให้เรียบร้อยพร้อมส่ง Flag

Enter Flag

Check

Flag 1 Correct!!!

Flag 1

" ให้เปลี่ยน User ที่ตัวเองสมัครเป็น Role 'admin' "

Hint : ไม่มีค่าใบ้

Flag 2

" ให้เข้าสู่ระบบด้วย Username 'admin' ให้ได้ "

Hint : Reset password

Flag 3

" จงหา Flag ! "

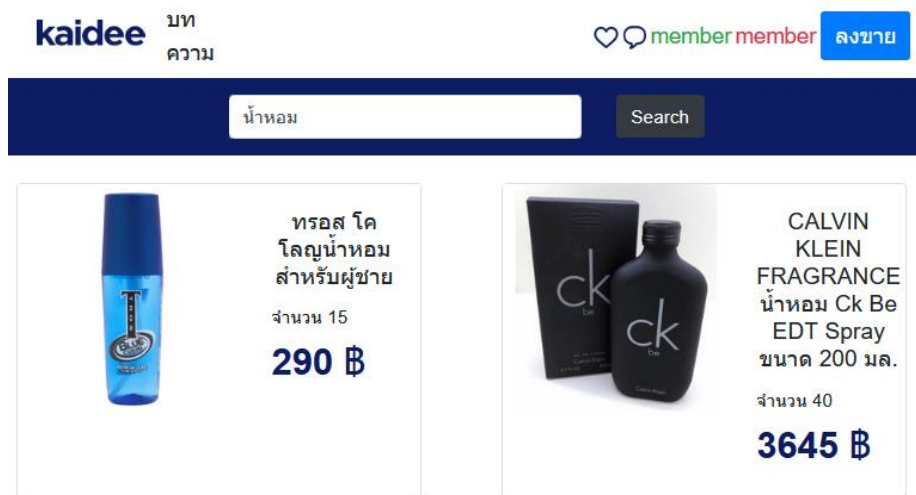
Hint : /secure_pass

รูปภาพ 4 เว็บสำหรับตรวจ Flag

2. เริ่มการทดสอบ

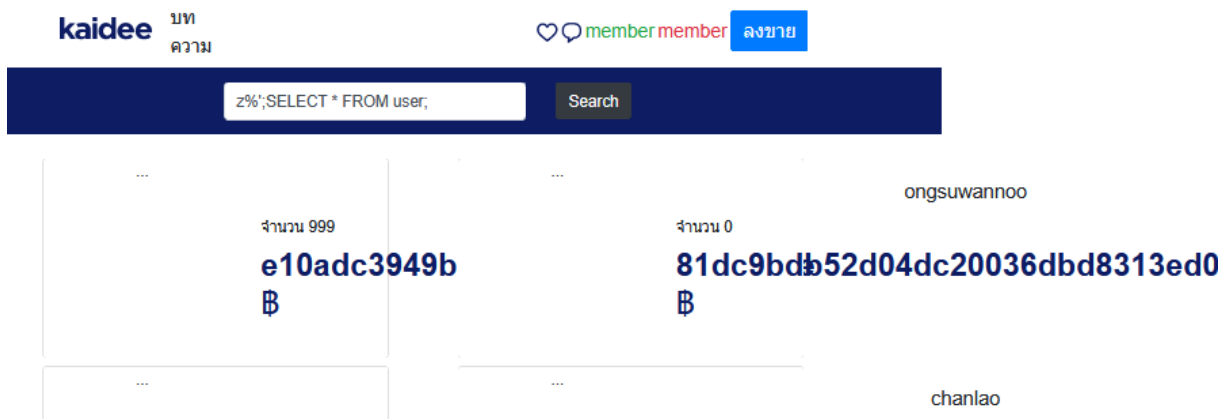
Lab - 1 ให้เปลี่ยน user ที่ตัวเองสมัคร เป็น role 'admin'

1. เข้าใช้งานที่ URL : <http://127.0.0.1/secure/index.php>
2. เมื่อลองใช้งาน search



รูปภาพ 5 ทดลองใช้งาน Search

- พบว่ามีการค้นหาผ่าน Name ที่มีตัวอักษรนั้นอยู่ในประโยค จึงคาดว่าจะใช้คำสั่ง `SQL LIKE %word%` ซึ่งการทำ search ด้วยวิธีนี้มันสามารถ เพิ่มคำสั่งเพื่อทำการ query ได้ จึงลอง injection เข้าไปด้วยคำสั่ง `z%';SELECT * FROM user;"`
- พบว่า สามารถใช้คำสั่ง query ได้มากกว่า 1 คำสั่ง



รูปภาพ 6 ทดลอง query

3. สังเกตได้ว่า column role มีการ set ค่าเป็น integer จึงคาดได้ว่าค่า role ต่างกัน จะมีเลขที่ต่างกัน จึงทำการ inspect ที่ role member

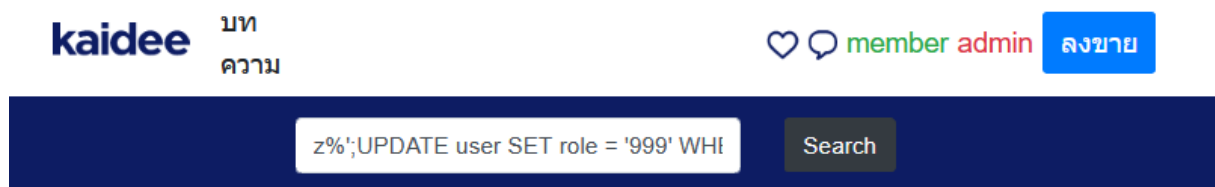
```
<script>
var xmlhttp = new XMLHttpRequest();
xmlhttp.onreadystatechange = function() {
  if (this.readyState == 4 && this.status == 200) {
    var myObj = JSON.parse(this.responseText);
    $("#username").html(myObj.username);
    $("#role").html(myObj.role == 0 ? 'member' : myObj.role == 999 ? 'admin' : myObj.role);
  }
};
xmlhttp.open("GET", "indexJson.php", true);
xmlhttp.send();
</script>
```

รูปภาพ 7 Script ของหน้า Index

มีการตั้งเงื่อนไขใน JS อยู่คือ 0 = member และ 999 = admin

ฉะนั้นหากเราต้องการจะเปลี่ยนเป็น role admin เราต้อง set role เป็น 999 โดยการทำ SQLi ด้วย `z%';UPDATE user SET role = 999 WHERE user.username = 'member';"`

4. เมื่อ set role เป็น 999 แล้ว role ของ user ก็จะเปลี่ยนเป็น admin (เมื่อค้นดูก็จะพบ Flag)

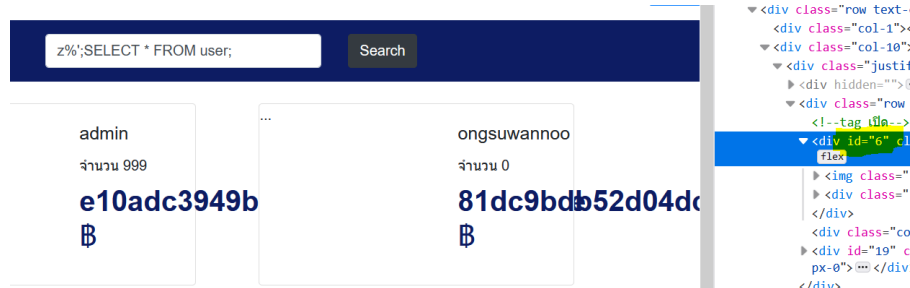


รูปภาพ 8 เปลี่ยน role เป็น admin

Lab - 2 ให้เข้าสู่ระบบด้วย username 'admin' ให้ได้

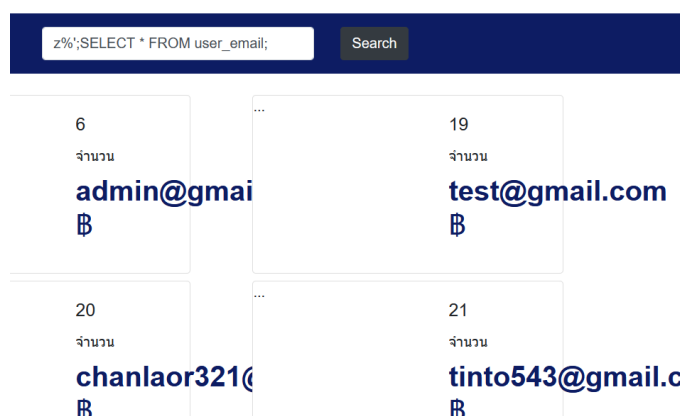
Hint : reset password / user_email

1. ทำการหา user id ของ admin โดยการ



รูปภาพ 9 ลองเช็คดูว่ามี username admin หรือไม่

2. เมื่อลองทำการ `SELECT * FROM user_email;` พบว่าสามารถเข้าถึงฐานข้อมูลเก็บ Email ของ user ได้



รูปภาพ 10 ลองดูตารางใน user_email ตามคำใบ้

3. จึงทำการอัปเดต Email ของ admin เพื่อให้สามารถแก้รหัสผ่านของ admin ได้

`z%';UPDATE user_email SET email = "test@gmail.com" WHERE userId = 6;`



รูปภาพ 11 หลังการอัปเดต Email

*หลังจากทำการอัปเดต ให้ลองเช็ค email ของ user ต่าง ๆ แล้วดูว่า email ของ user admin เปลี่ยนหรือไม่

4. กลับไปหน้า login กดไปยัง Forget Password และทำการกรอก email ไป

ลืมรหัสผ่าน ?

ท่านจำเป็นต้องเปลี่ยน Password เป็น Password ใหม่ โดยเราจะทำการส่งโค้ดสำหรับใช้เปลี่ยน Password ไปยัง Email ของท่าน

ใส่ Email ของคุณ

xxx@gmail.com

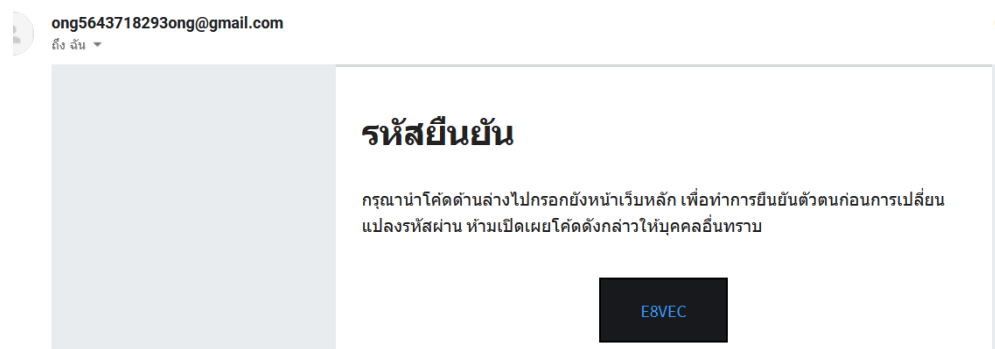
เราจะทำการส่งโค้ดสำหรับการเปลี่ยนรหัสผ่านไปยัง Email ที่ท่านกรอก

Send

[กลับไปยังหน้าล็อกอิน](#)

รูปภาพ 12 หน้าสำหรับกรอก email

5. ตรวจสอบใน Email ที่แก้ไขก่อนหน้านี้



รูปภาพ 13 รหัสที่ถูกส่งไปใน Email

6. นำรหัสยืนยันมากรอก

Your Email : ongsuwannoo@gmail.com

Enter Code

Code

Enter

รูปภาพ 14 นำรหัสมากรอกในช่อง

7. สามารถแก้รหัสใหม่ได้แล้ว

New Password

| | | |
|--------------------------|--------------------------|-------------------------------------|
| <input type="password"/> | <input type="password"/> | <input type="button" value="Send"/> |
|--------------------------|--------------------------|-------------------------------------|

รูปภาพ 15 เปลี่ยนรหัสผ่าน

8. เมื่อทำการ login ด้วย username admin พบ Flag ปรากฏขึ้น

Lab - 3 จงหา flag ! ในหน้า Add Product

Hint: `/etc/secure_pass`

1. ในการ เพิ่มสินค้า ต้องเพิ่มสินค้าที่มีอยู่ในรายชื่อเท่านั้น ซึ่งสามารถดูรายการสินค้าได้ผ่านช่อง search

ประเภทสินค้าที่ได้รับอนุญาตให้ลงขาย

*เฉพาะประเภทสินค้าใน List ด้านล่างเท่านั้นที่อนุญาตให้ลงขายสินค้า ท่านสามารถตรวจสอบประเภทสินค้าต่างๆได้ที่ช่องค้นหาด้านล่าง

ยา
ยาพารา
ยาบพารา
ยาไม่ได้นอน

รูปภาพ 16 ทดลองใช้ search product

```
<p>
  <input type="text" name="price" placeholder="Price" required></input>
</p>
Count
<p>
  <input type="number" name="count" placeholder="Count" required></input>
</p>
<button type="submit" name="form" value="add">Add</button>
</form>

<form method="post">
  Search Product name
  <input type="text" name="search" placeholder="Search" required></input>
  <button type="submit" name="form" value="search">search</button>
</form>

<pre>
<?
  $key = "";

  if(array_key_exists("search", $_REQUEST)) {
    $key = $_REQUEST["search"];
  }

  if($key != "") {
    passthru("grep -i $key test.txt");
  }
?>
</pre>
```

รูปภาพ 17 source code

- สังเกตได้ว่าการใช้คำสั่ง passthru ในการ search ซึ่งเป็นคำสั่งที่ของ PHP ที่จะส่งเข้าไป execute
- passthru สามารถส่งคำสั่งเข้าไป execute ก็คำสั่งก็ได้ เราจึงทำการ injection เพิ่มคำสั่งเข้าไป
a; cat /etc/secure_pass

ประเภทสินค้าที่ได้รับอนุญาตให้ลงขาย

*เฉพาะประเภทสินค้าใน List ด้านล่างเท่านั้นที่อนุญาตให้ลงขายสินค้า ท่านสามารถตรวจสอบประเภทสินค้าต่างๆได้ที่ช่องค้นหาด้านล่าง

```
a; cat /etc/secure_pass
```

```
GNU nano 4.8
thanu:!:17965:0:99999:7:::
renu:$6$hvf089w7$lBhBB7DUkJZ.zU2ekY3M1AW
ntp:!:17982:0:99999:7:::
_chrony:!:17983:0:99999:7:::
FLAG{3283ba80ac38583eea8d5834bc4728fc}
Debian-exim:!:18056:0:99999:7:::
u1:$6$hwt8cQ6t$7a.Y1P0QbpeTh2gY0uqWMvQte
ยา
ยาพารา
```

รูปภาพ 18 ทำการ cat /etc/secure_pass ออกมา


- ได้ Flag มาแล้ว

สัดส่วนการแบ่งงาน

| | |
|---|---|
|  <p>นายจักรพรรดิ สุวรรณโน (Jakkrapat Suwanno) 61070022</p> | - คิดตั้งตัวโปรเจกให้พร้อมสำหรับการพัฒนา |
| | - ดูแลเรื่องการระบบต่าง ๆ (การสร้าง database, การเชื่อม database) |
| | - จัดการเรื่องเกี่ยวกับระบบปฏิบัติการ Linux (Flag ข้อ 3) |
| | - นำตัวโปรเจกไปไว้บน docker เพื่อให้ผู้ที่สนใจนำไปพัฒนาต่อ |
|  <p>นายตินต์ โตสงวน (Tin Tosanguan) 61070061</p> | - ทำเว็บไซต์ที่ไว้สำหรับตรวจสอบ Flag |
| | - เชื่อมต่อ Firebase กับเว็บตรวจ |
| | - จัดทำในส่วนการเข้าสู่ระบบ |
| | - ช่วยทำส่วนของเนื้อหาในรายงาน |
|  <p>นายชนพล จันทร์ละออ (Thanapon Chanlaor) 61070071</p> | - จัดทำเว็บไซต์ Flag Site (ในส่วน Flag ข้อ 1) |
| | - ช่วยคิดโจทย์ส่วน Flag ข้อ 1 |
| | - จัดทำเว็บไซต์หน้า Forget Password |
| | - ช่วยทำส่วนของเนื้อหาในรายงาน |

| | |
|--|--|
|  <p>นายธนพล มาติกานนท์ (Thanapon Matikanon) 61070072</p> | - รับผิดชอบทำเว็บไซต์หา Flag หน้าหลัก |
| | - รับผิดชอบ Flag ข้อ 1 |
| | - รับผิดชอบหน้าการลงขายสินค้า |
| | ช่วยทำส่วนของเนื้อหาในรายงาน |
|  <p>นายธนวัฒน์ เขมวัชรเลิศ (Thanawat Kemwatcharalert) 61070074</p> | - ทำเว็บไซต์ที่ไว้สำหรับตรวจสอบ Flag |
| | - Literature Reviews งานวิจัย |
| | - เชื่อมต่อ Firebase กับเว็บตรวจ |
| | - ช่วยทำส่วนของเนื้อหาในรายงาน |
|  <p>นายอริชญ์ อวยเจริญ (Arin Auycharoen) 61070350</p> | - รับผิดชอบทำ site web ส่วนหน้าเว็บย่อย (หน้าค้นหาสินค้า, หน้าลงขาย, ลิ้มรหัสผู้ใช้) |
| | - รับผิดชอบโจทย์แฟลกข้อสอง |
| | - Literature Reviews งานวิจัย |
| | - ช่วยทำส่วนของเนื้อหาในรายงาน |

ผลการตรวจ Plagiarism

 thanapon chanlaor | รายงาน Security_กลุ่ม10

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

การศึกษาและจำลองการหาช่องโหว่ที่เกิดขึ้นในระบบ

ในรูปแบบ Capture The Flag (CTF)

Capture the flag practices model : identified vulnerability in system

นายจักรพรรดิ สุวรรณโณ
(Jakkrapat Suwannano) 61070022

นายธนพล มาตีกานนท์
(Thanapon Matikanon) 61070072

นายตินต์ โตสงวน
(Tin Tosanguan) 61070061

นายธนพล จันทร์ละออ
(Thanapon Chanlaor) 61070071

นายธนวัฒน์ เขมวชิรเลิศ
(Thanawat Kemwatcharalert) 61070074

นายอริยชัย อวยเจริญ
(Arim Auycharoen) 61070350

ABSTRACT – The purpose of this test is designed for those who want to seek Vulnerability in the system by the features of their website, Presented in the form of the CTF (Capture The Flag) that simulate an E-Commerce Website on PHP Which is a language that currently in use .This website has the basic subsystems of an e-commerce website, such as a search engine, add products, apply for membership, etc. We assumed that the developers of this website do not have enough knowledge of web security and there are vulnerabilities for attackers to attack the system. In this test write SQL Injection is used vulnerability for system attacks. When the developer

Match Overview

2%




Match 1 of 1

1 Submitted to Pace Univ... Student Paper 1% >

2 Shubham Mukherjee, P... Publication 1% >

3 Marta Beltran, Miguel C... Publication 1% >

Page: 1 of 11 Word Count: 2194 Text-only Report High Resolution On

| Assignment Inbox: 06016309 INFORMATION SYSTEM SECURITY AND IT LAWS | | | | | |
|--|---|-------|---------------------|--|---|
| Assignment Title | Info | Dates | | Similarity | Actions |
| Group Assignment |  | Start | 11-Nov-2020 12:51AM | 2%  | Resubmit View  |
| | | Due | 31-Dec-2020 11:59PM | | |
| | | Post | 31-Dec-2020 11:59PM | | |



Digital Receipt

This receipt acknowledges that **Turnitin** received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author: thanapon chanlaor
Assignment title: Group Assignment
Submission title: รายงาน Security_กลุ่ม10
File name: 10__-Capture-The-Flag-CTF.pdf
File size: 662.99K
Page count: 11
Word count: 2,194
Character count: 6,588
Submission date: 20-Nov-2020 10:53PM (UTC+0700)
Submission ID: 1450044842

การศึกษาระบบจำลองการโจมตีที่เกิดขึ้นในระบบ
ในรูปแบบ Capture The Flag (CTF)
Capture the flag practices model : identified
vulnerability in system

| | |
|---|--|
| นายจักรพรรดิ สุวรรณโณ (Jakkrapot Sawanno) 61070022 | นายชนพล นาคินนันทน์ (Thanapon Matikanon) 61070072 |
| นายคณิน ใสธรรม (Tin Tosangman) 61070061 | นายธนวิทย์ เชนวิฑูรย์ (Thanawat Kemsuwancharakert) 61070074 |
| นายชนพล จันทิระเดช (Thanapon Chanlaor) 61070071 | นายวิญญู อวยเจริญ (Arin Auycharoen) 61070350 |

ABSTRACT – The purpose of this test is designed for those who want to seek Vulnerability in the system by the features of their website, Presented in the form of the CTF (Capture The Flag) that simulate an E-Commerce Website on PHP Which is a language that currently in use .This website has the basic subsystems of an e-commerce website, such as a search engine, add products, apply for membership, etc. We assumed that the developers of this website do not have enough knowledge of web security and there are vulnerabilities for attackers to attack the system. In this test suite, SQL Injection is used primarily for system attacks. When the player can attack the correct point, Players will receive a flag indicating that the Player has successfully attacked the system.

KEY WORDS – CTF, E-commerce, SQL Injection, Flag, Vulnerability

บทคัดย่อ – จุดประสงค์ของงานวิจัยนี้เพื่อศึกษาการโจมตีที่เกิดขึ้นในระบบเว็บไซต์ของระบบจำลองการโจมตีในรูปแบบของ CTF (Capture The Flag) ที่จำลองระบบ E-commerce ขึ้นมาในรูปแบบของเว็บไซต์บนภาษา PHP ซึ่งเป็นภาษาที่มีผู้ใช้งานอยู่ โดยเว็บไซต์นี้มีระบบย่อยที่เป็นฟังก์ชันของเว็บไซต์ E-commerce เช่น ระบบค้นหาสินค้า, เพิ่มสินค้า, จัดการสมาชิก เป็นต้น โดยที่เว็บไซต์นี้ไม่ได้มีความปลอดภัยใน web security มากพอ อันเนื่องจากระบบหรือเว็บไซต์ที่สร้างขึ้นโดยนักพัฒนาเว็บไซต์ไม่ได้มีการใช้ความรู้ในการโจมตีระบบ SQL Injection เป็นหลัก ในการโจมตีระบบ นักวิจัยสามารถโจมตีจุดที่ถูกต้อง ผู้ใช้จะได้รับ Flag เพื่อยืนยันว่าโจมตีระบบสำเร็จแล้ว เมื่อผู้โจมตีสามารถเข้าถึง ระบบที่โจมตีต้องการ เป็นอันดับแรกของจุดทดสอบนี้

คำสำคัญ – CTF, E-commerce, SQL Injection, Flag, ขังใจ