SECURE LOGIN AUTHENTICATION SYSTEM

BY

CHOW WEN CHAI

A REPORT

SUBMITTED TO

Universiti Tunku Abdul Rahman

in partial fulfillment of the requirements

for the degree of

BACHELOR OF COMPUTER SCIENCE (HONS)

Faculty of Information and Communication Technology
(Perak Campus)

JANUARY 2018

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF INFORMATION & COMMUNICATION TECHNOLOGY (PERAK CAMPUS)

CHECKLIST FOR FYP2 THESIS SUBMISSION

Student Id	14ACB05547
Student Name	CHOW WEN CHAI
Supervisor Name	DR. GAN MING LEE

TICK (√)	**DOCUMENT**
	Front Cover
	Signed Report Status Declaration Form
	Title Page
	Signed form of the Declaration of Originality
	Acknowledgement
	Abstract
	Table of Contents
	List of Figures (if applicable)
	List of Tables (if applicable)
	List of Symbols (if applicable)
	List of Abbreviations (if applicable)
	Chapters / Content
	Bibliography (or References)
	All references in bibliography are cited in the thesis, especially in the chapter of literature review
	Appendices (if applicable)
	Poster
	Signed Turnitin Report (Plagiarism Check Result - Form Number: FM-IAD-005)

*Include this form (checklist) in the thesis (Bind together as page 2)

(Signature of Student)
Date:

(Signature of Supervisor)
Date:

UNIVERSITI TUNKU ABDUL RAHMAN

REPORT STATUS DECLARATION FORM

Title: ____

____

____

Academic Session: _____________

I ____

(CAPITAL LETTER)

declare that I allow this Final Year Project Report to be kept in
Universiti Tunku Abdul Rahman Library subject to the regulations as follows:

1. The dissertation is a property of the Library.
2. The Library is allowed to make copies of this dissertation for academic purposes.

Verified by,

_________________________ _________________________

(Author's signature) (Supervisor's signature)

Address:

____

____

____

____

Supervisor's name

Date: _____________________ **Date**:____________________

SECURE LOGIN AUTHENTICATION SYSTEM

BY

CHOW WEN CHAI

A REPORT

SUBMITTED TO

Universiti Tunku Abdul Rahman

in partial fulfillment of the requirements

for the degree of

BACHELOR OF COMPUTER SCIENCE (HONS)

Faculty of Information and Communication Technology
(Perak Campus)

JANUARY 2018

DECLARATION OF ORIGINALITY

I declare that this report entitled "SECURE LOGIN AUTHENTICATION SYSTEM" is my own work except as cited in the references. The report has not been accepted for any degree and is not being submitted concurrently in candidature for any degree or other award.

Signature : ________________________

Name : CHOW WEN CHAI________

Date : 12th APRIL 2018___________

ACKNOWLEDGEMENTS

I would like to express my sincere thanks and appreciation to my supervisors, Dr. Gan Ming Lee who has given me this bright opportunity to engage to implement Secure Login Authentication System project. It is my first step to establish a career in network security field. A million thanks to you.

Finally, I must say thanks to my parents and my family for their love, support and continuous encouragement throughout the course.

ABSTRACT

With the rapid evolution of the wireless communication technology, user authentication is important in order to ensure the security of the wireless communication technology. Password play an important role in the process of authentication. In the process of authentication, the password enter by the user will be transmitted along the traffic to the authentication server in order to allow the server to grant access to the authorised user. The attackers will use the chance to attempt to sniff others person password in order to perform some illegal activities by using other's identity to keep them safe from trouble. Due to the issues, there are many solutions has been proposed to improve the security of wireless communication technology. In this paper, the previously proposed solution will be used to enhance the security of the system. The solution adopted is the one time password, hashing and two-factor authentication. There also a new solution will be added by using the QR code to help to save more data. The objective of the system outcome is to enhance the current login authentication system. It provides solutions for making password breaking more difficult as well as convinces users to choose and set hard-to-break passwords.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

MiTM	Man in the middle
QR	Quick Response
OTP	One time password
Et al.	And others
IOS	Iphone OS
wifi	Wireless Fidelity
URL	Uniform Resource Locator

Chapter 1 : INTRODUCTION

1.1 PROBLEM STATEMENT

Authentication is an activity to authenticate the person credential that wishes to perform the activity. In the process of authentication, the password enter by the user will be transmitted along the traffic to the authentication server in order to allow the server to grant access to the authorized user. When the password is transmitted, the attackers will try to sniff into the network to obtain data that include the user's password. Currently, there is rainbow table which able to trace the password with the hash algorithm to obtain the user's password. Once the password is succeeded to be decrypted, the attackers can use the user credential to do something illegal such as fraud others which will cause the user lost in credit.

According to Pagliery(2014), there is 47% of the American adults account been hacked in that year. Their personal information is exposed by the hackers. Due to the problem exists, there are more people no longer trust that password will be able to protect their online account. According to Sulleyman(2017), some of the attackers will sell the email account that is been hacked to others to gain profit.

It is important to protect our own account because our credit is priceless. It is hard to trace the attackers in the cyber world. The secure login system is needed to ensure the cybersafety. Therefore, this project would like to provide alternative ways to log in to a system because current login system is not secure enough.

1.2 BACKGROUND AND MOTIVATION

Authentication is an activity to authenticate the person credential that wishes to perform the activity. If the credential is matched, the process is completed and the user will be granted for the access. Generally, the user will need to provide their password to begin using a service of the system. According to Rouse (2014), user authentication authorizes human-to-machine interactions in operating systems and applications as well as both wired and wireless networks to enable access to networked and Internet-connected systems, applications and resources.

In their investigation of password evolution, Bonneau (2015) state that:

> The password is added to the sharing operating system in 1960s. However, the problem arose very quick due to the leakage of the unencrypted password master file. When reaching 1970s, the password started to be stored in the hashed form. In 1979, the hashed password was improved with the salting. With the mid-1990s introduce of the World Wide Web, the password is secure using the public-key cryptography via secure sockets layer (SSL) client certificates. The password is then started to link to the email and two-factor authentication is introduced. In the early of 2010s, the smartphone starts to be widely used. The reason for the implementation is also because of the free smartphone applications to act as a second factor based on the emerging time-based-one-time-pad (TOTP) standard. TOTP is an algorithm that computes a one-time password from a shared secret key and the current time. There are also services provided by sending codes via short message service (SMS) as a backup authentication mechanism.

In their investigation of password evolution, Denso (2016) state that:

> Quick Response(QR) code was created by 1994 in Japan. It is named after quick response because of the high-speed reading. QR code is an evolution of the barcodes. The evolution occurs due to the limitation of the barcodes which only can hold 20 alphanumeric characters. The project is then carried out by Masahiro Hara and his development team for 1 year and a half. The outcome of the QR code is a huge success due to it can store 7,000 numerals with the additional capability to code Kanji characters was finally created. With the current technology, the QR code is scanned can help to redirect to a website or coupon.

Figure 1-1 QR code

1.3 PROJECT OBJECTIVES

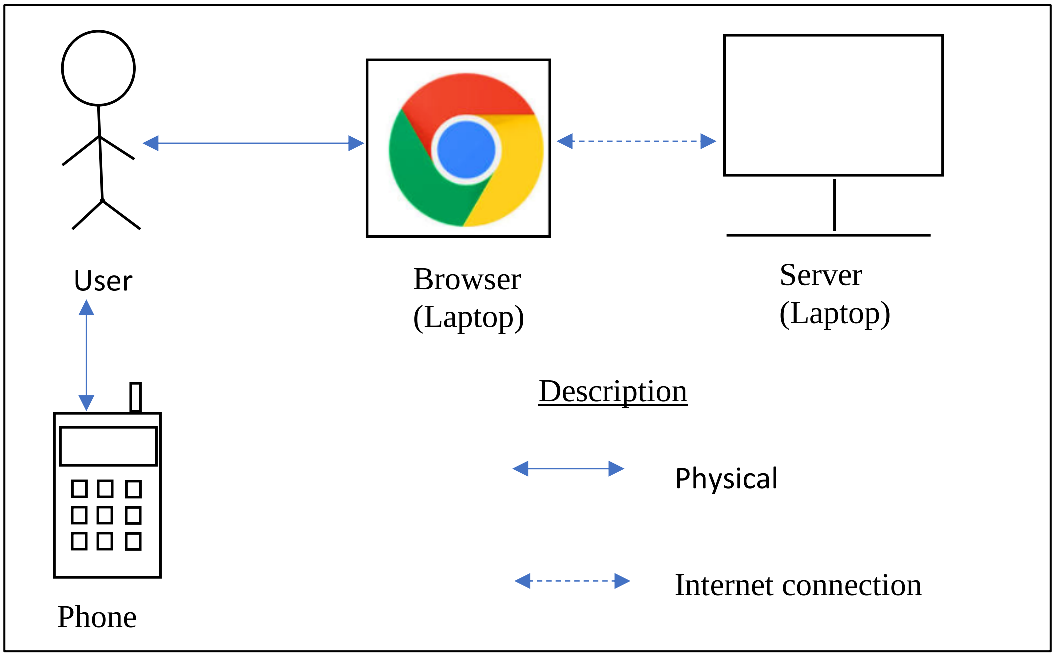
The 4 main objectives for this project:

1. The main objective is to implement a secure login authentication system with utilizing with two-factor authentications. By using the concept two-factor authentication could help to increase the strength of the login system. The attacker will need to pass through the next barrier of defence to success to log in. This system will help to enhance the login authentication system.
2. Next objective is to ensure login password will not be transmitted over the network. As compared to the previous solution, the password is just encrypted, but the attackers might succeed to decode the data and retrieve the password. So in order to prevent this happens, the password with the random key will need to be hash before the sender sends the password to the server. It is important to secure the password of the user.
3. Apart from that, the third objective will be to generate the one time password offline. This will help in perform the login procedure if there is a limited connection of wi-fi or mobile signal is weak. It will help the user who lives in the countryside which has a weak phone signal.
4. Lastly, the fourth objective is to ensure the system is protected from rainbow table attack. The rainbow table will act as a dictionary store and optimised for hashes and password. So once the random key is repeated, the password will be retrieved. So, the random key should be long enough to cause the attackers to use a longer time to generate the rainbow table.

1.4 PROPOSED APPROACH/STUDY

The proposed solution to enhance the security of login authentication system by implementing the new system. In the new system to be proposed, it will help to enhance the password security. The system will help to ensure the password will not be transmitted along the traffic. Therefore, this project would like to provide alternative ways for login to a system by using QR code as the random key when the user attempts to log in. By using this method, attackers will be hard to decrypt the password since they will need to generate a huge rainbow table if the random key is long enough.

Under the proposed system, the user will key in the username then the password will be obtained. The server will generate a random key with 40 characters in the form of QR code. The phone will then scan the QR code to obtain the random key. The password will then combines the random key and hash. The server will retrieve the password from the database then combine the random key and hash it. Both of these hash value generated will take the first 6 character as the OTP. Once it is both matches, the login is success.



1.5 REPORT ORGANISATION

The details of this research are shown in the following chapters. In Chapter 2, some existing solution for creating a secure login authentication is reviewed. The strength and weaknesses also discuss in chapter 2. In chapter 3, the system design is further elaborate with flowchart and sequence diagram. There is also discussion on tools used to implement the system and the system requirement needed to implement the system. Next, Chapter 4 is discussing the result of system testing. The interface of the system also been shown in the chapter. There is also some brief explanation of the code. In chapter 5, there is a discussion of the advantage of the system implemented compare to the existing system. There is also discussion of the reason to choose the tools to implement the system. Lastly, in chapter 6, some conclusion is made from based on the objective achieved in the system. There is also some explanation of problem encountered during the period of system implementation and the future work that can be done based on the new system.

Chapter 2 : LITERATURE REVIEW

2.1 EXISTING PROPOSED SOLUTIONS OVERVIEW

Authentication is a process to access to login account and accessing the service provided by the system or server using the password. It also has an alternative way to authenticate the user which is using biometric authentication by using fingerprint or iris recognition. However, human has the tendency to create easily remember password which it will lead to a problem.

By definition, authentication is the use of one or more mechanisms to confirm that you are the authenticated user. Once the identity of the human or machine is validated, access is granted. There are existing acknowledged three authentication factors are things the user know, things the user have and biometric authentication. Biometric-based authentication is a good way to authenticate the user but it is expensive and raises some privacy concern.

One Time Passwords (OTP) offers a promising alternative for two-factor authentication systems. A one-time password is a password that is valid for only one login session or transaction, on a computer system or other digital device (Cheng, X. R. et al. ,2005).

Two-factor authentication solution equips customers with a cost effective means of providing flexible and strong authentication to very large scale. The goal of computer security to maintain the integrity, availability and privacy of the information entrusted to the system can be obtained by adopting this authentication technique.

There is also company uses the hashing algorithm to store their password. In the transmission of the password, the password has already been hashed and become unreadable.

Lastly, most of the password is now encrypted when it is sent from the sender to the receiver. The password is encrypted so that the attackers will not easily obtaining the correct password since they will need another step to decrypt the data (Mathur, A. ,2012).

2.2 TWO FACTOR AUTHENTICATION

Two-factor authentication has been introduced long time ago. It is also known as the two-step verification. The organization will implement this method because it is easy the implement it. They can save the cost from replacing the existing system and increase security level by adding a layer of security that protects the existing authentication system.

The reason for the two-factor authentication is been started to use by many organizations is because of the ease of implementation of the method. They do not require to replace the existing system but just increase security level by adding a layer of security that protects the existing authentication system. The process will require 2 reliable authentication factors which is something the users knows such as alphanumeric password, something user has such as the phone and something the user is such as biological unique features (eg. Fingerprint).

Two-factor authentication is an evolvement from single-factor authentication which only requires the password of the user. However, single-factor authentication is no longer secure due to user tends to have the weak password which is common. Users also tend to have the same password for multiple accounts. This provides a chance for the hacker to succeed in password exploitation. The two-factor authentication helps to provide an additional layer of security.

In two factor authentication, the user provides dual means of identification, one of which is typically a physical token, such as a card and the other of which is typically something memorized, such as security code. The aim of the multifactor is to create a more difficult step for attackers/ unauthorized people to access a target. This mechanism still able to be secure if there is still existing a barrier to breach before accessing the target.

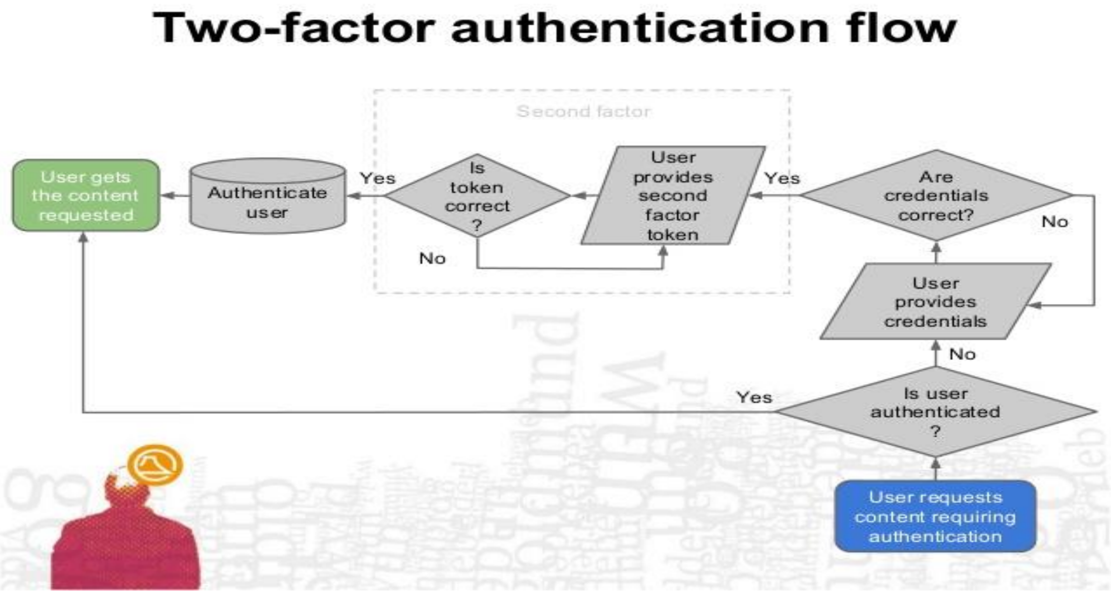

Two-factor authentication flow
Second factor
User gets the content requested
Authenticate user
Yes
Is token correct ?
No
User provides second factor token
Yes
Are credentials correct?
No
User provides credentials
No
Yes
Is user authenticated ?
User requests content requiring authentication

Figure 2-1Two-factor authentication flow. (Milton K., n.d.)

2.3 ONE TIME PASSWORD (OTP)

A one-time password is a password that is valid for only one login session or transaction, on a computer system or other digital device. The OTP authentication main idea is to provide infinite factors and create different password every time during user logging in to improve the security of the system. OTP is used in conjunction with a token. The token and corresponding authentication server share the same algorithm. The algorithm is different for each user's token to prevent attackers break the algorithm. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further.

The OTP authentication system is implemented by two main mechanisms. The first mechanism is the challenge-response mode. The system will generate a challenge to the user when the user is logging in. The OTP is generated by combining user keyed in the password and challenge generate by the system. The user will need to key in the OTP to log in successfully.

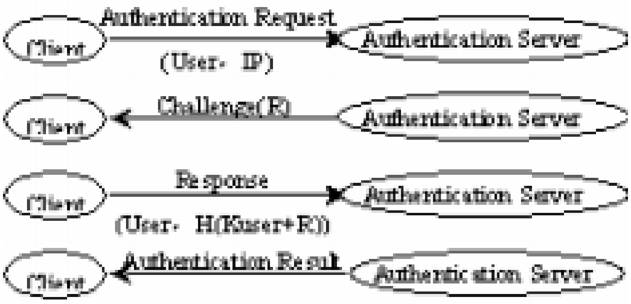


Figure 2-2 Challenge-response mechanism. (Cheng, X. R. et al. , 2005)

The next mechanism is time synchronization. This mechanism will use the user login time to generate the random number. The user can generate the password combining his passphrase. OTP also only valid for a short period of time only.

2.4 CRYPTOGRAPHY

Cryptography is the study to generate the secret message between the sender and the receiver. The main goal of the cryptography is authentication, privacy, integrity, non-repudiation and access control.

Encryption is a process that converts the message into unreadable using some algorithm. It is one of the processes that applying the cryptography. Encryption is a step that transforms or convert the data into a random and meaningless message. In another word, it can be said as is a process to convert plaintext into the ciphertext.

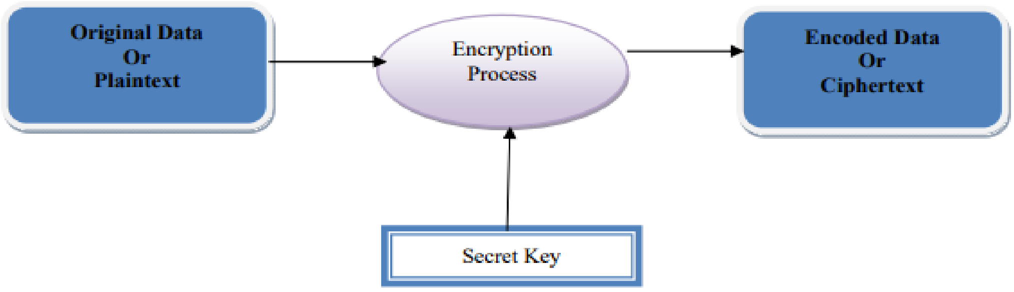


Figure 2-3 Encryption process flow. (Symmetric and Asymmetric Encryption – What are the difference?, n.d.)

Decryption is the vice versa of the encryption which will convert the data into the meaning form. It is a process to transform ciphertext into plain text.

In order to perform the cryptography, the cryptographic algorithm is needed to act as a mathematical function and steps to perform encryption and decryption. The purpose of the cryptography is to increases the difficulties for the attackers to decrypt the ciphertext.without given the actual key to be decrypted.

Many sites store the password in the encrypted form in their database on the server. They will use a special key to convert the password into a random string which is a ciphertext. If the user without the key, they will not able to obtain the password but just a random string. However, it is reversible where there is the chance of success decryption by attackers.

2.5 HASH FUNCTION

Hashing is a step that will use a hash algorithm such as the MD5 to turn a password into a long random string which consists of letters and numbers. The hashes are the opposite of encryption which is not reversible to be the original text. There is no algorithm exist to reverse back the hashes. However, the attackers can try the different combination of the password in order to match the user password. The combination password hashes are then collected to store into the rainbow table. This method will be very time exhausting.

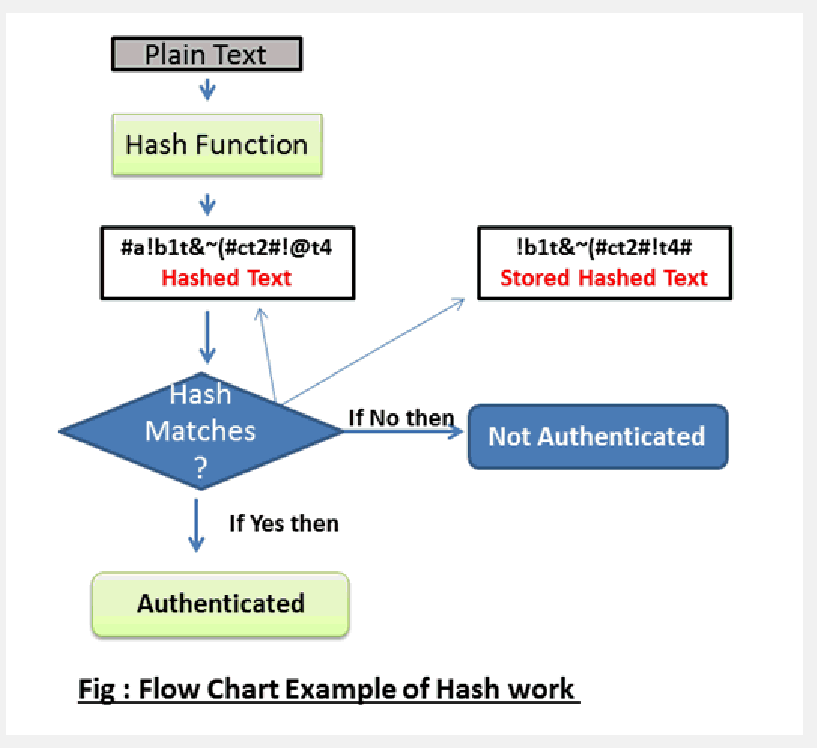


Figure 2-4 Flowchart of hash algorithm

2.6 COMPARISON BETWEEN PROPOSED SOLUTION

Proposed Solution	**Strength**	**Weakness**
Two factor authentication	• Increase the step for attackers to success	• If the email is hijacked, the process cannot continue until the email is been recovery.
One Time Password	• Not vulnerable to replay attack • Can be time limited	• Require internet or phone connection to complete the process • User will feel annoyed to wait for the message to reach if the connection is slow
Cryptography	• The attackers will need time to find the decryption key	• Attackers might succeed from retrieve decryption key • The key can be exposed by network admin to the attackers
Hash Function	• The password is not reversible • The password with the similar hashes is very rare • Time exhausting to crack the password	• Vulnerable to rainbow table attacks

Table 2-6-1 Strength and weaknesses of the proposed solution

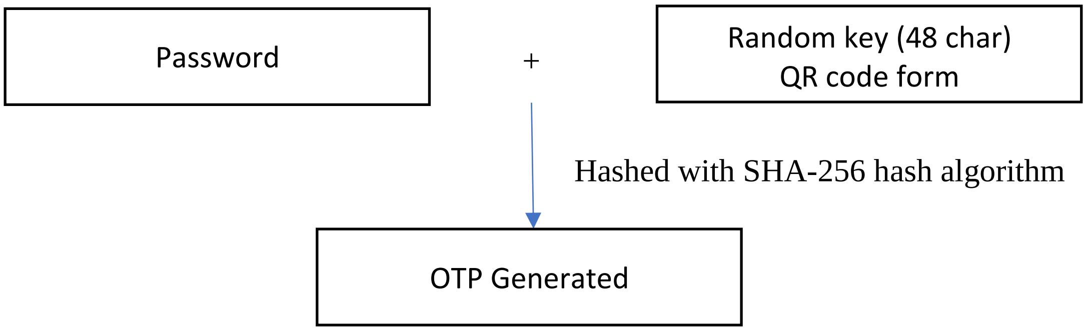
Chapter 3 : PROPOSED METHOD/APPROACH

3.1 DESIGN SPECIFICATIONS

Due to the importance to secure the password, I had implemented an enhanced version of the login authentication from the existing proposed solution. Under the existing system, the password whether it is encrypted or hashed, it still exists in the network traffic to reach the service. Once the attackers get the encrypted or hashed password, the attacker will have the chance to succeed to discover the algorithm to retrieve back the plain text.

This project needs 2 things which are the desktop sites and mobile application. The desktop designed to have 2 type of user input with username and OTP. The website will require the username first then only the password. Next, the system will need the implementation of server-side scripting. The server-side scripting will retrieve the password from database and generate the random key with 48 characters. The password and random key then combine and hashed. The server-side scripting will help to generate the QR code to be displayed on the website.

For the mobile application part, the user interface design is important to help the user to understand the step to use it. The application needs to implement the camera features to help the phone the retrieve random key when the QR code is scan. The alternative way to scan QR code is to screenshot the QR code and import into phone application to decode secret key. The application will then prompt the user password and the OTP will be generated.



In order to overcome the problem in the currently existing system, the server will generate a different random key in each and every time when the user logs in to the system to generate the OTP. So, the attackers will not possible to obtain the actual password. The login page should limit the attempt of the password in 5 times to decrease the chance of success brute force attacks.

3.2 SYSTEM DESIGN

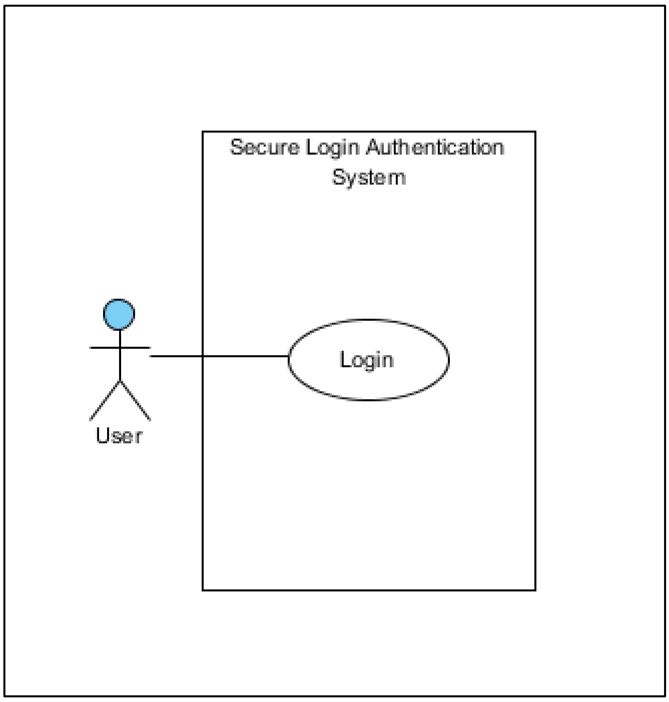


Figure 3-1 Use Case of system

Use Case ID	UC001	**Version**	1.0
Feature	F001 Login		
Purpose	To allow the user to log in their account.		
Actor	User		
Trigger	User surf the website.		
Precondition	Surf website		
Scenario Name	**Step**	**Action**	
Main Flow	1	User enter username	
	2	System check validity of the username	
	3	System retrieves login phrase	
	4	System display login phrase	
	5	User confirm with login phrase	
	6	System obtain random key	
	7	System display random key	
	8	User scan QR code	
	9	System prompt user enter the password	
	10	User enter password	
	11	System generated and display OTP	

	12	User enter OTP in website
	13	System check device validity of the account in the database
	14	System display “login successful”
Alternate Flow - Invalid Username	2.1.1	User enters an invalid username.
	2.1.2	System displays error message “This username doesn't exist, try again!”
	2.1.3	Back to main flow step 1.
Alternate Flow - Invalid OTP	12.1.1	User enters invalid OTP.
	12.1.2	System displays error message “Invalid OTP”
	12.1.3	System generate random key
	12.1.4	Back to main flow step 7.
Alternate Flow - Trial more than 5	12.1.1	User enters invalid OTP more than 5 times.
	12.1.2	System send email to user to inform account is locked
Alternate Flow - First Attempt Login of New Device	13.1.1	User use new device to attempt login
	13.1.2	System send email to user to verify device
Rules	i. Username must exist in the database. ii. OTP must be matched.	
Author	Chow Wen Chai	

Table 3-2-1 Use Case Description of system

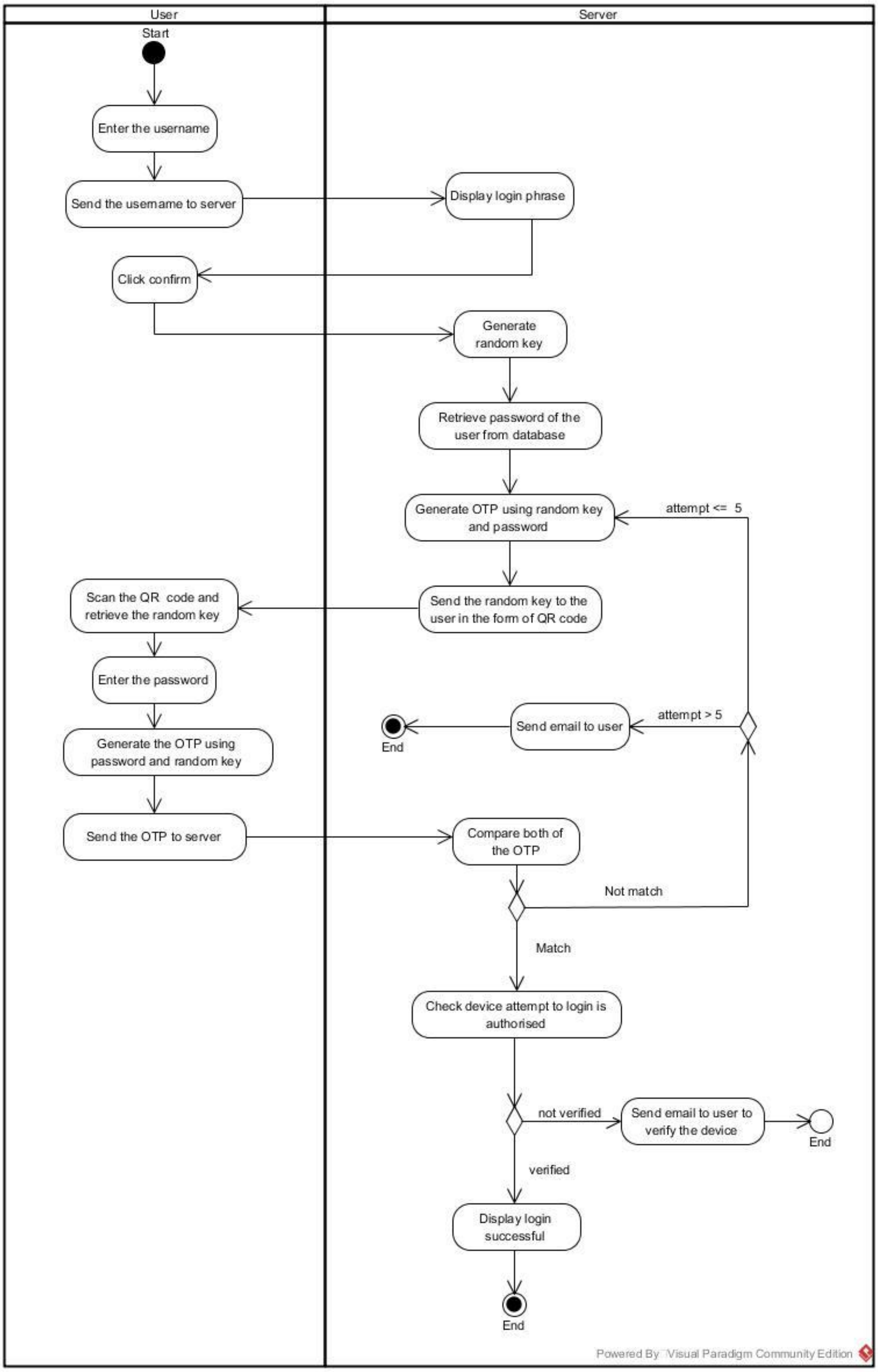

User
Server
Start
Enter the username
Send the usemame to server
Display login phrase
Click confirm
Generate random key
Retrieve password of the user from database
Generate OTP using random key and password
attempt <= 5
Send the random key to the user in the form of QR code
Scan the QR code and retrieve the random key
Enter the password
Generate the OTP using password and random key
Send email to user
attempt > 5
End
Send the OTP to server
Compare both of the OTP
Not match
Match
Check device attempt to login is authorised
not verified
Send email to user to verify the device
End
verified
Display login successful
End
Powered By: Visual Paradigm Community Edition

Figure 3-2 Flowchart of the system

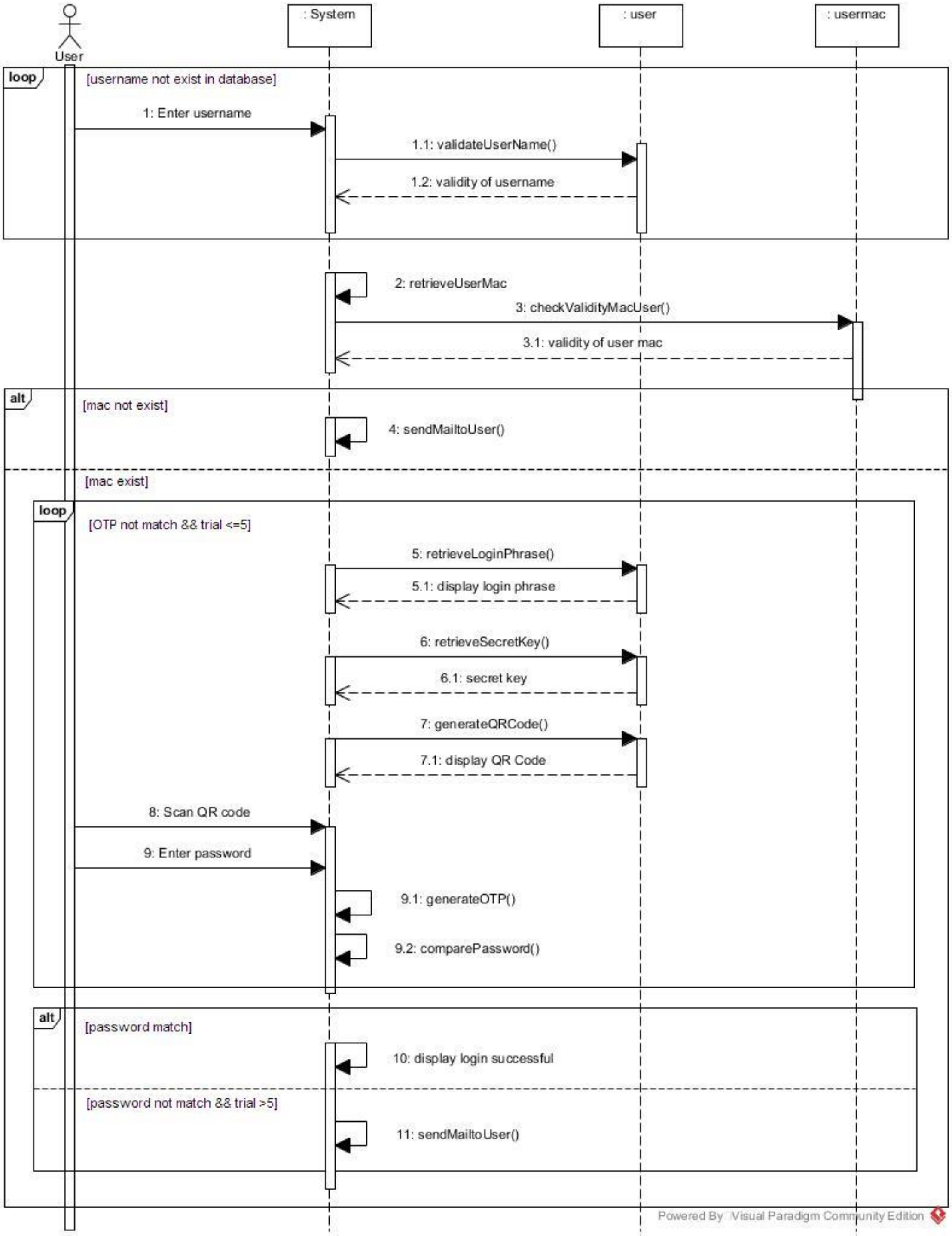


Figure 3-3 Sequence Diagram of system

The system start with the user wants to surf the web and perform the login activity. The user key in their own username and click next. The system will search the username in the database. The system will send an error message if the username does not exist in the database. Once if the username is valid in the database, the website will display the login phrase of the user. This method needs to do so in order to protect the user from the phishing attack. Next, the server will generate the random key with 48 characters. The random key will then display in the form of QR code on the webpage. The system also will retrieve the password of the user and combine it with the random key and hashed it.

Once the QR code is displayed in the web page, the user will need to use their own phone to scan the QR code or import QR code from phone gallery to obtain the key. Next, the phone will prompt the user to enter their actual password. The password is then entered and generate is clicked by the user. The OTP with the 6 character is then displayed on the phone screen. There might be a chance where same OTP is generated where the different password is entered with the same key. The attacker will need trial and error to confirm the password since there will be many possible passwords. The attacker will also hard to wait for the same key to be used to login for the same user since there is 2.12 X 10^{99} combination of the key will be generated. There is one important thing to be mention where the phone is not necessary to connect to wi-fi to complete the process of login. The phone also will not able to validate the password because it is just an application to help to generate the OTP and there is no point for the attacker to own or hack the application.

The user will need to key in the OTP generated in the web page. The system will compare the OTP generated and the user input. If the user input is the same, the user will be granted to use the service of the system. Once it is different, the system will generate the new random key and the user will need to re-scan the QR code using phone application and type in the password to obtain OTP and enter to the website again. The system only allows 5 user attempt to login to the system. If it is exceeded, the user account will be locked for temporary. The user will receive the email about there is an attacker is attempting hack into the account. The user can unlock the account by click on the link provided in the email.

The system also has extra features to enhance the security which if there is a new device login to the web page, it will prompt the email to the user to ensure the user credential. The user will need to click back the link to continue the login activity. Once the link is clicked, the mac address of the new device will save into the database.

3.3 SYSTEM REQUIREMENT

There is 2 device that requires respectives system requirement. For the laptop requirement suggested will be as listed as below.

OS	Window XP and later/Mac OS
RAM	2GB
Processor	Intel's dual-core Core i3-4130
Hard drive	1GB of free space

Apart from system requirement of the laptop, the project also requires a list of system requirement for the mobile. The suggested requirement is stated as shown below.

CPU type	Intel Pentium 4
RAM	1GB
OS	Android 6.0 above
Version	1GB of free space
Memory	500MB

3.4 IMPLEMENTATION ISSUES AND CHALLENGES

The major challenge of the project is the shortage of time because time is needed to learning the code and need to implement the system. The time also uses to find out the better solution from the others proposed solution. The proposed solution needed to study and find out their strength and weaknesses to be improved so that can learn from their problem.

The next challenge of the project will be the limitation of understanding the code used to implement the system. The coding will be a very fresh programming language for me since it is very new for me.

3.5 TIMELINE

This project will be divided into two parts which the first part will develop the mobile app, website and establish the server. While the second part will be added in the QR code features to establish a connection with security.

In previous semester, the first part will be implemented in order to perform normal login features. The first week of the semester is used to study the coding of android and php. The next week will be used to implement the mobile application and website with user interface design. In the third week will be used to set up the server using the xampp. When the fourth week is coming, the time will be used to test the functionality of the partially done system. Starting in week 5, the time will be used to prepare the final year project report and be checked and submitted.

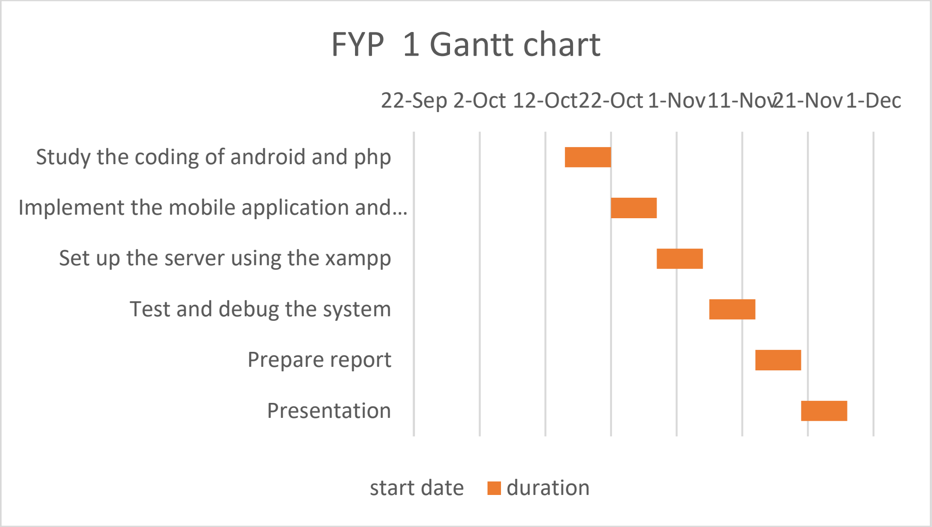


Figure 3-4 FYP1 Gantt Chart

In the current semester, I implement the login system with the QR code feature. I also enhance the login system with some features such 2 factor authentication for the first time device login attempt which will help to ensure the user credential. After the system is implemented, it is tested, debug and improve until the user comfortable to use the system. Next, the report needs to be prepared in 2 weeks of time. After that, the time is used to prepare the presentation.

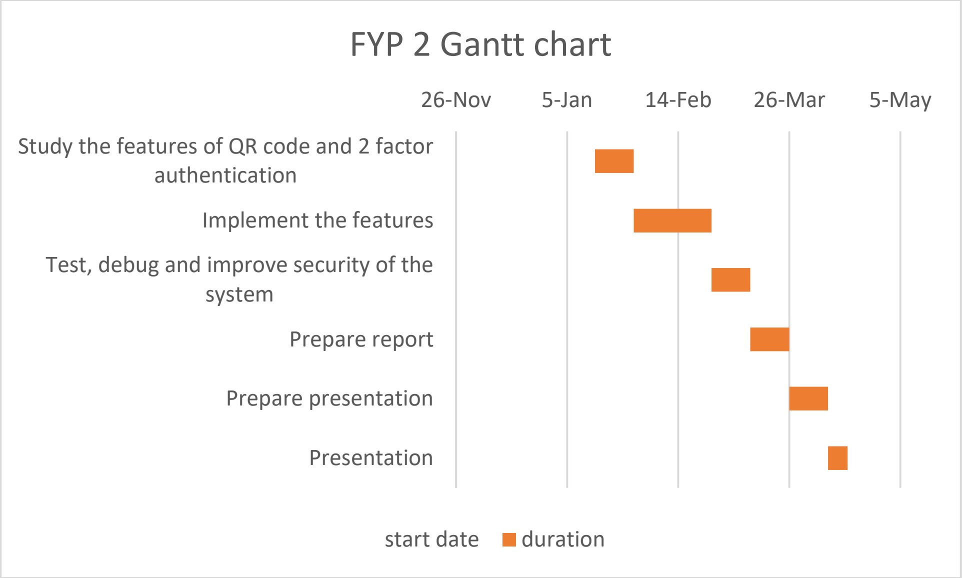


Figure 3-5 FYP2 Gantt Chart

Chapter 4 : IMPLEMENTATION AND TESTING

4.1 METHODOLOGY AND TOOLS

1. Smartphone

Figure 4-1 Smartphone

The phone is used to generate a random key when it's camera is used to scan with the QR code. So, the smartphone used with the features of can download and install a new application and must have a camera which can be used to scan QR code.

2. Laptop

Figure 4-2 Laptop

The system also requires a server to perform authentication service. Instead of using a real server to set up the system, the laptop is used to be a virtual server. The laptop also will be used to surf the site built to log in.

3. Android Studio

Figure 4-3 Android Studio

The Android studio is used to write the android application which can generate a random key when the QR code is scan. The application will help to combine the password and generated random key and finally hashed it to become an OTP.

4. XAMPP

Figure 4-4 XAMPP

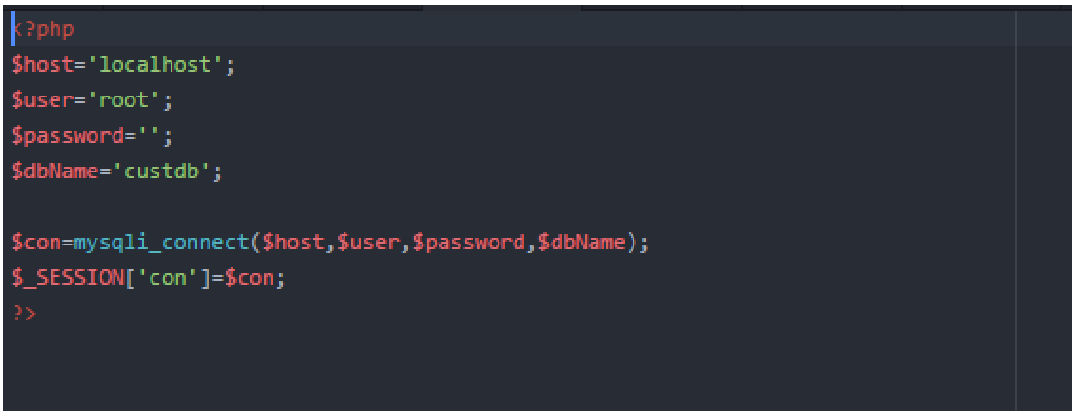
The XAMPP will be used to set up the web server with the MYSQL and Apache.

5. Atom IDE

The atom IDE uses to implement the website.

4.2 CODE IMPLEMENTATION

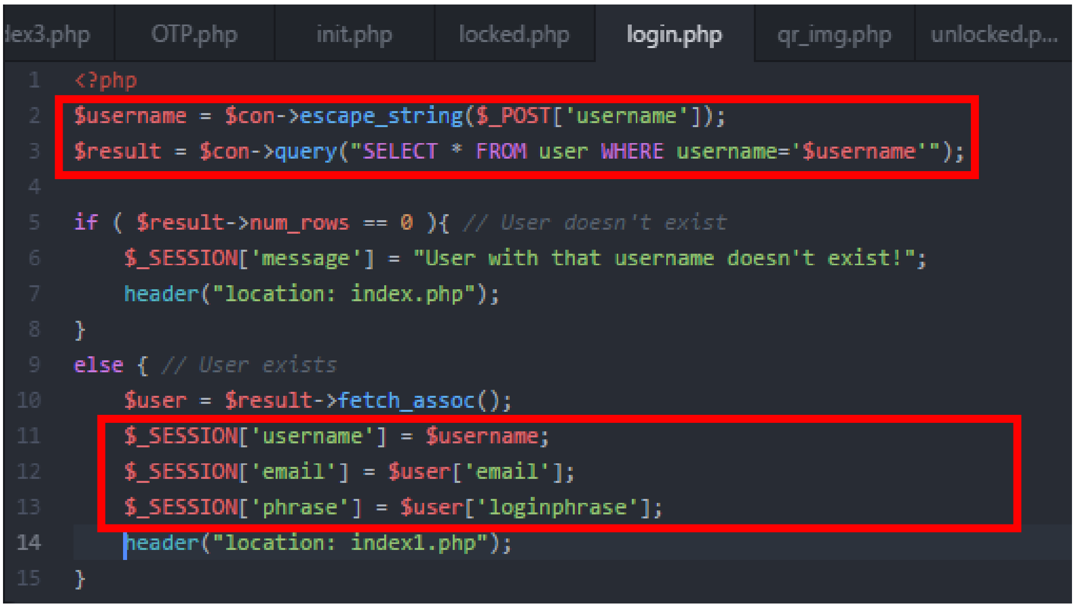
4.2.1 Website (Atom)



```php
<?php
$host='localhost';
$user='root';
$password='';
$dbName='custdb';

$con=mysqli_connect($host,$user,$password,$dbName);
$_SESSION['con']=$con;
?>
```

Figure 4-5 Code of database connection

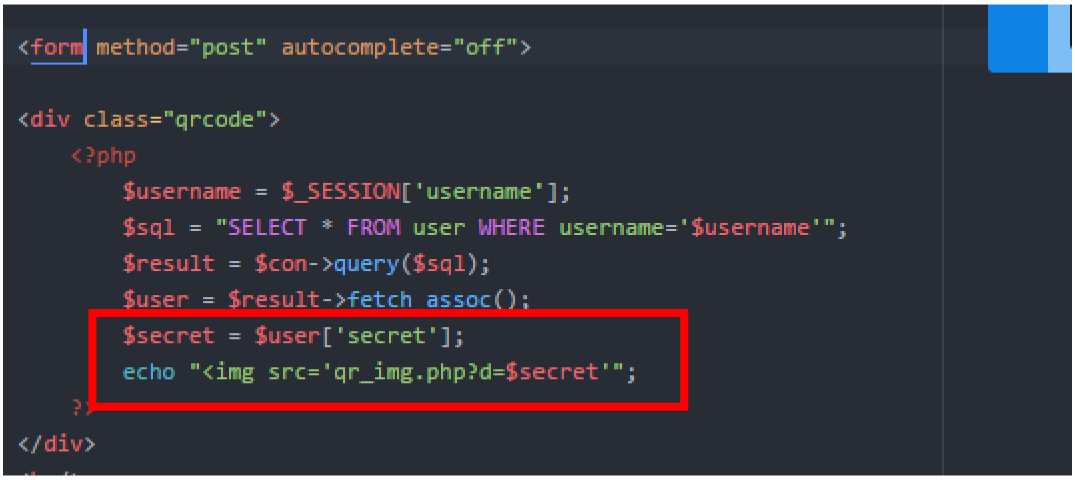
In the code above, it is needed to create a connection to the database in phpmyadmin. The required data such as username, password and database name is needed to establish the connection.



```php
<?php
$username = $con->escape_string($_POST['username']);
$result = $con->query("SELECT * FROM user WHERE username='$username'");

if ( $result->num_rows == 0 ){ // User doesn't exist
    $_SESSION['message'] = "User with that username doesn't exist!";
    header("location: index.php");
}
else { // User exists
    $user = $result->fetch_assoc();
    $_SESSION['username'] = $username;
    $_SESSION['email'] = $user['email'];
    $_SESSION['phrase'] = $user['loginphrase'];
    header("location: index1.php");
}
```

Figure 4-6 Code of query and declaration of the session attribute

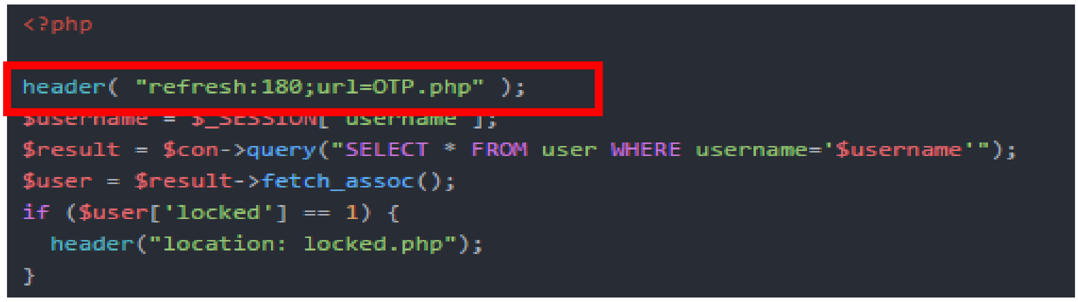
After the connection is done, the system able to run the query to retrieve data from the database. The system can retrieve the input from the user and then perform the query to obtain the result using escape_string. The result of the query will then be stored in session to reduce the network traffic between the client and database.



```
<form method="post" autocomplete="off">

<div class="qrcode">
    <?php
        $username = $_SESSION['username'];
        $sql = "SELECT * FROM user WHERE username='$username'";
        $result = $con->query($sql);
        $user = $result->fetch_assoc();
        $secret = $user['secret'];
        echo "<img src='qr_img.php?d=$secret'";
    ?>
</div>
```

Figure 4-7 Code of display QR code

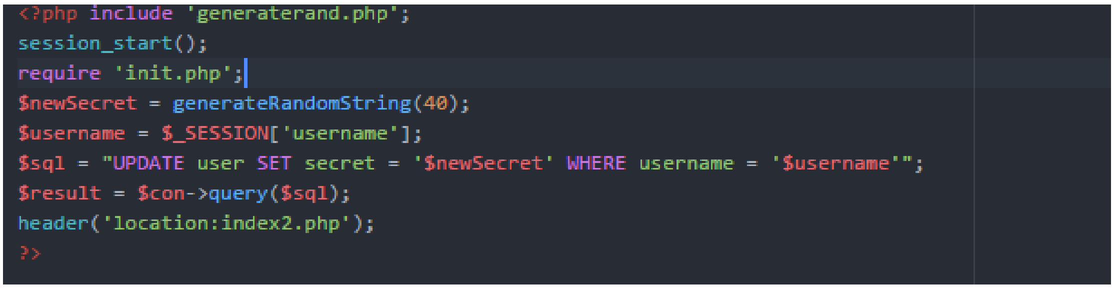
After retrieving the random key generated and stored from database, the random key will then converted into QR code with the help of qr_img.php and is displayed.



```
<?php

header( "refresh:180;url=OTP.php" );
$username = $_SESSION['username'];
$result = $con->query("SELECT * FROM user WHERE username='$username'");
$user = $result->fetch_assoc();
if ($user['locked'] == 1) {
  header("location: locked.php");
}
```

Figure 4-8 Code of refresh page

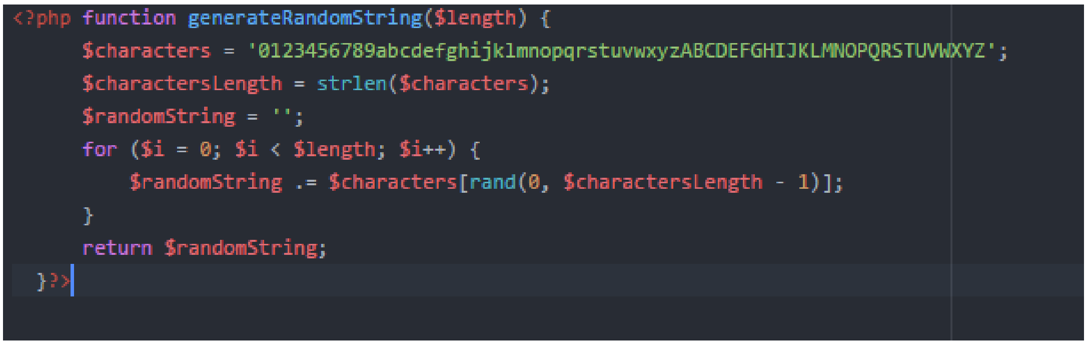
The QR code will be expire if the user remains on the same webpage more than 3 minutes. After the QR code is expired, the page will be forward to OTP.php to generate a new random key.



```
<?php include 'generaterand.php';
session_start();
require 'init.php';
$newSecret = generateRandomString(40);
$username = $_SESSION['username'];
$sql = "UPDATE user SET secret = '$newSecret' WHERE username = '$username'";
$result = $con->query($sql);
header('location:index2.php');
?>
```

Figure 4-9 Code of update random key

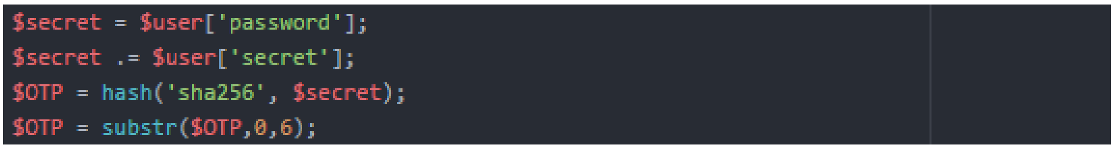
The function of generateRandomString will be called to create the random key. After the random key is generated, the random key will be replaced in the database and forward to the page to display QR code.



```php
<?php function generateRandomString($length) {
      $characters = '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';
      $charactersLength = strlen($characters);
      $randomString = '';
      for ($i = 0; $i < $length; $i++) {
          $randomString .= $characters[rand(0, $charactersLength - 1)];
      }
      return $randomString;
  }?>
```

Figure 4-10 Code for generating a random key

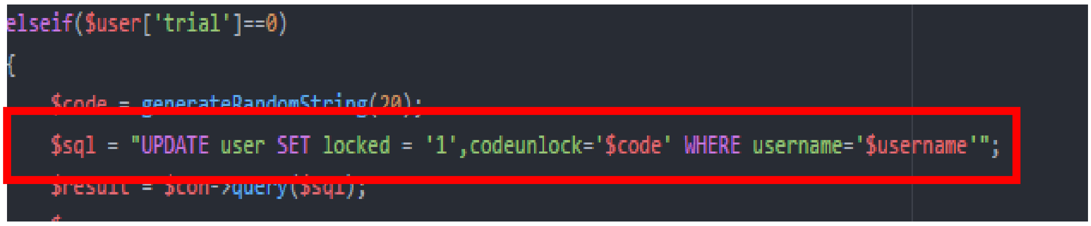
This is the function to generate a random key with the different combination of alphabets and digits. The function will require an input of length to determine the length of the random string.



```php
$secret = $user['password'];
$secret .= $user['secret'];
$OTP = hash('sha256', $secret);
$OTP = substr($OTP,0,6);
```

Figure 4-11 Code for generating OTP

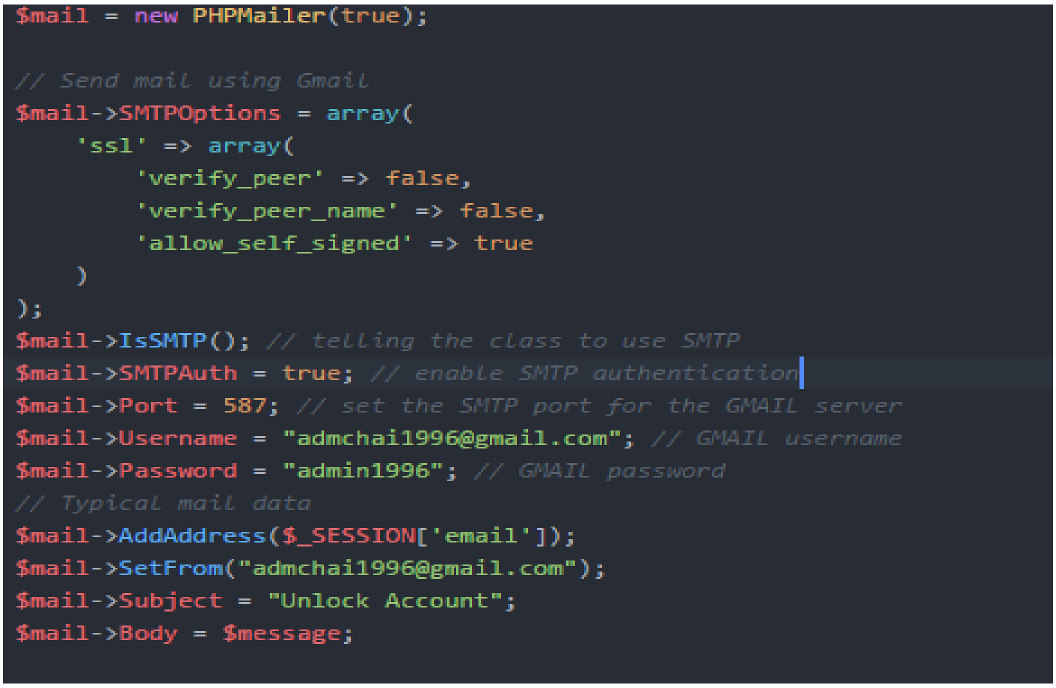
The password from the database is then combined with the random key to becoming a combined string. The combine string then hash by using SHA256 and the first 6 characters only will be chosen to become OTP. The system will then prompt OTP from the user and then compare with the OTP generate by the system. If it matches, the permission of access to service is granted. If it does not match, the permission of access to service is denied. The system will generate a new random key and forward the user to display QR code page.



```php
elseif($user['trial']==0)
{
    $code = generateRandomString(20);
    $sql = "UPDATE user SET locked = '1',codeunlock='$code' WHERE username='$username'";
    $result = $con->query($sql);
```

Figure 4-12 Code of the locked account

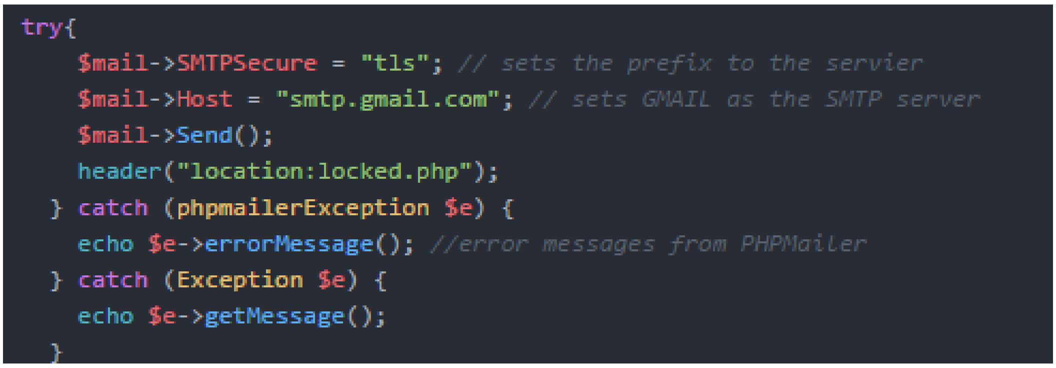
When the user enters the wrong OTP for more than 5 times, the system will lock the user account.



```
$mail = new PHPMailer(true);

// Send mail using Gmail
$mail->SMTPOptions = array(
    'ssl' => array(
        'verify_peer' => false,
        'verify_peer_name' => false,
        'allow_self_signed' => true
    )
);
$mail->IsSMTP(); // telling the class to use SMTP
$mail->SMTPAuth = true; // enable SMTP authentication
$mail->Port = 587; // set the SMTP port for the GMAIL server
$mail->Username = "admchai1996@gmail.com"; // GMAIL username
$mail->Password = "admin1996"; // GMAIL password
// Typical mail data
$mail->AddAddress($_SESSION['email']);
$mail->SetFrom("admchai1996@gmail.com");
$mail->Subject = "Unlock Account";
$mail->Body = $message;
```

Figure 4-13 Code of email set up

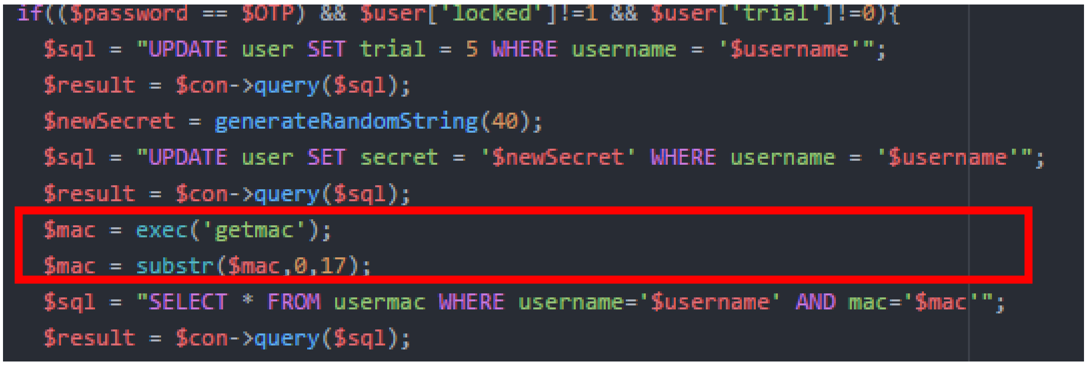
This is the step to set up the email configuration where the need to declare port used and email of the system admin and client. There is also a declaration of the subject and the content of the email.



```
try{
    $mail->SMTPSecure = "tls"; // sets the prefix to the servier
    $mail->Host = "smtp.gmail.com"; // sets GMAIL as the SMTP server
    $mail->Send();
    header("location:locked.php");
  } catch (phpmailerException $e) {
    echo $e->errorMessage(); //error messages from PHPMailer
  } catch (Exception $e) {
    echo $e->getMessage();
  }
```

Figure 4-14 Code of email send and catch exception

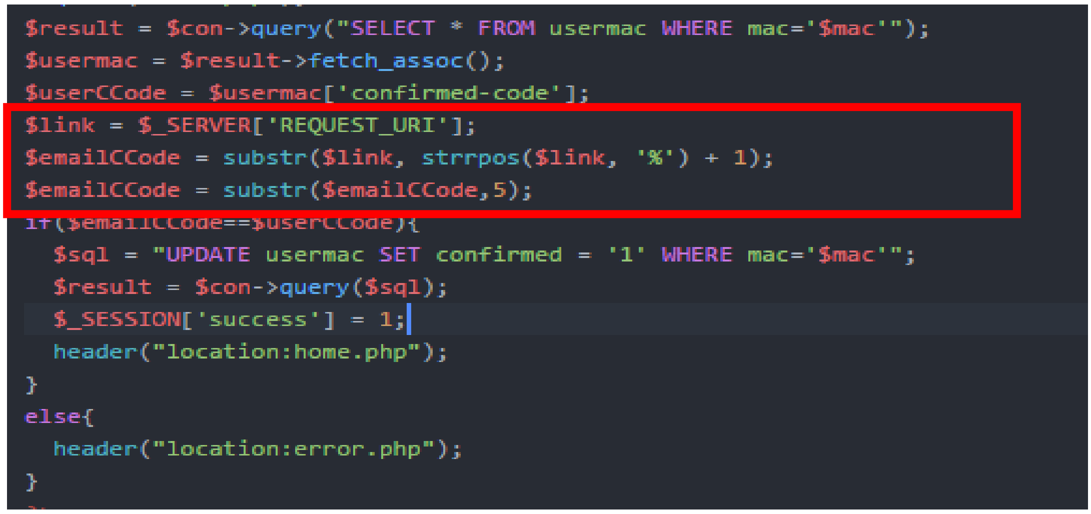
Once the mail can be sent successfully, the web page will be redirected to locked.php.



```
if(($password == $OTP) && $user['locked']!=1 && $user['trial']!=0){
  $sql = "UPDATE user SET trial = 5 WHERE username = '$username'";
  $result = $con->query($sql);
  $newSecret = generateRandomString(40);
  $sql = "UPDATE user SET secret = '$newSecret' WHERE username = '$username'";
  $result = $con->query($sql);
  $mac = exec('getmac');
  $mac = substr($mac,0,17);
  $sql = "SELECT * FROM usermac WHERE username='$username' AND mac='$mac'";
  $result = $con->query($sql);
```

Figure 4-15 Code of retrieve client's device mac address

This is the code that will able to retrieve the mac address of the device connected to the system. The mac address will then check with the database to ensure the device is verified or else the system will send the email to the user in order to verify the device.

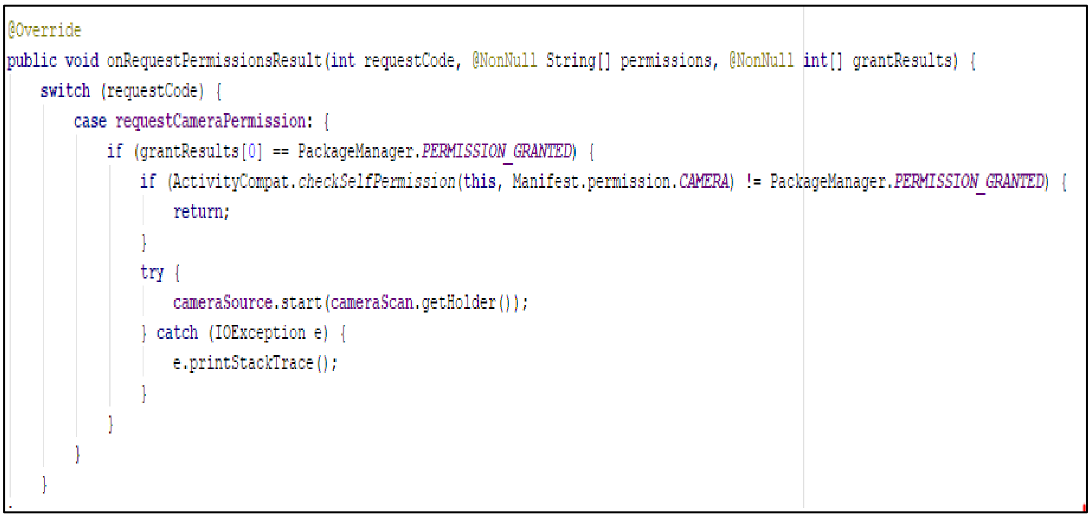


```
$result = $con->query("SELECT * FROM usermac WHERE mac='$mac'");
$usermac = $result->fetch_assoc();
$userCCode = $usermac['confirmed-code'];
$link = $_SERVER['REQUEST_URI'];
$emailCCode = substr($link, strrpos($link, '%') + 1);
$emailCCode = substr($emailCCode,5);
if($emailCCode==$userCCode){
  $sql = "UPDATE usermac SET confirmed = '1' WHERE mac='$mac'";
  $result = $con->query($sql);
  $_SESSION['success'] = 1;
  header("location:home.php");
}
else{
  header("location:error.php");
}
```

Figure 4-16 Code of retrieve confirm code from URL

The code is to retrieve the URL of the website and filter the confirm code in the URL. The system will then compare with the confirm code in the database. Once both of them match, the system will forward the user to home page.

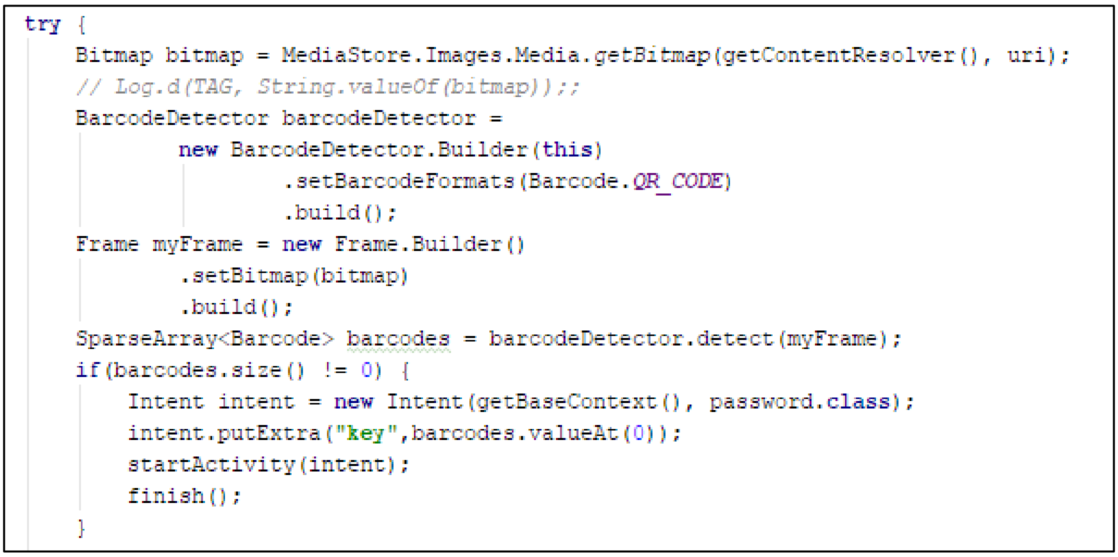
4.2.2 Android Studio



```
@Override
public void onRequestPermissionsResult(int requestCode, @NonNull String[] permissions, @NonNull int[] grantResults) {
    switch (requestCode) {
        case requestCameraPermission: {
            if (grantResults[0] == PackageManager.PERMISSION_GRANTED) {
                if (ActivityCompat.checkSelfPermission(this, Manifest.permission.CAMERA) != PackageManager.PERMISSION_GRANTED) {
                    return;
                }
                try {
                    cameraSource.start(cameraScan.getHolder());
                } catch (IOException e) {
                    e.printStackTrace();
                }
            }
        }
    }
```

Figure 4-17 Code of grant camera permission

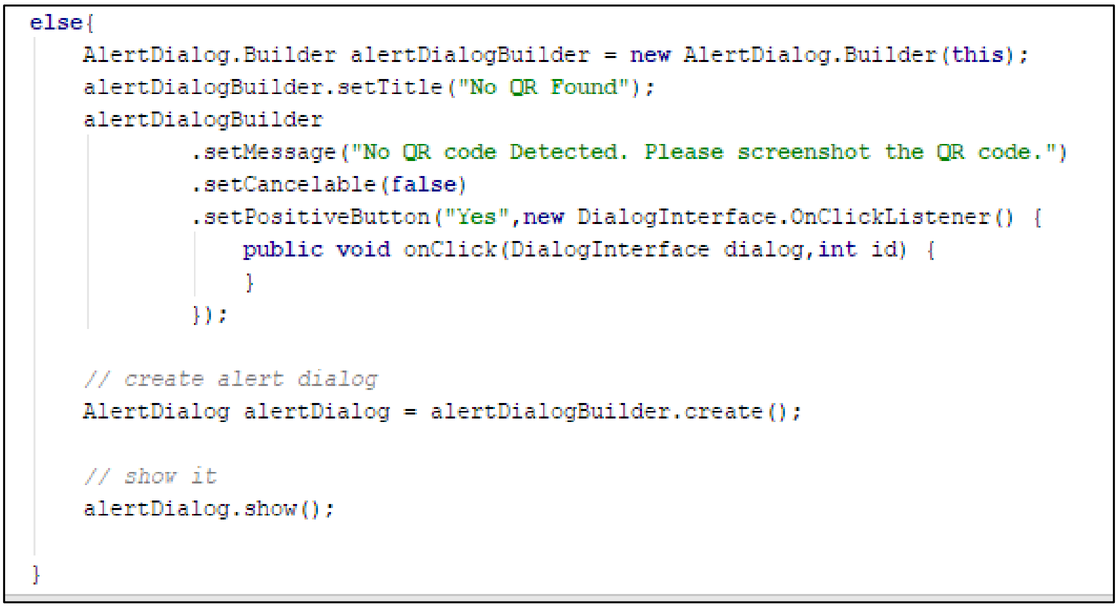
The code is to prompt permission from the user to allow the phone application to access the function of the camera. If the permission is granted, the user will not need to press allow again.



```
try {
    Bitmap bitmap = MediaStore.Images.Media.getBitmap(getContentResolver(), uri);
    // Log.d(TAG, String.valueOf(bitmap));;
    BarcodeDetector barcodeDetector =
            new BarcodeDetector.Builder(this)
                    .setBarcodeFormats(Barcode.QR_CODE)
                    .build();
    Frame myFrame = new Frame.Builder()
            .setBitmap(bitmap)
            .build();
    SparseArray<Barcode> barcodes = barcodeDetector.detect(myFrame);
    if(barcodes.size() != 0) {
        Intent intent = new Intent(getBaseContext(), password.class);
        intent.putExtra("key",barcodes.valueAt(0));
        startActivity(intent);
        finish();
    }
```

Figure 4-18 Code of detecting QR code from photo

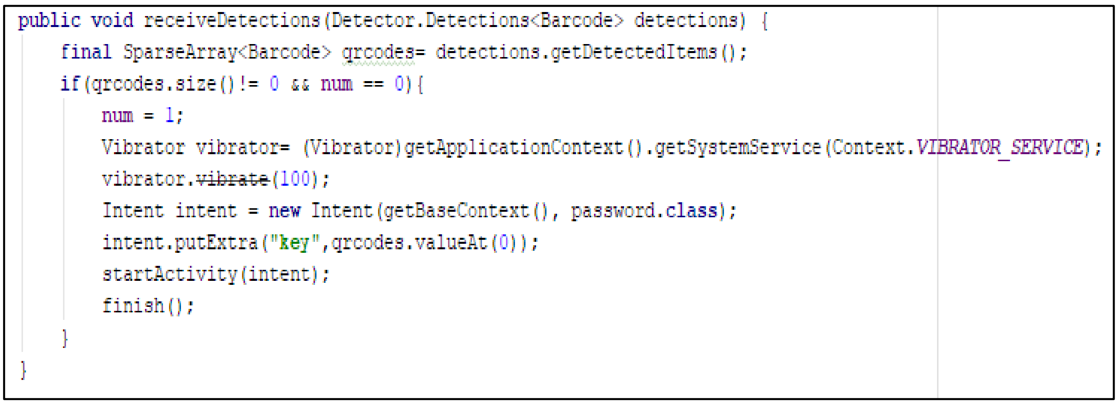
When the user chooses to browse the photo from the gallery to obtain the QR code, the application will read the photo in the form of bitmap and convert into a frame. Then, the type of bar code to detect is defined which is a QR code. After the implementation, the application can execute the function to detect the QR code in the photo. If the photo contains QR code, it will retrieve the data and forward to the next page.



```
else{
    AlertDialog.Builder alertDialogBuilder = new AlertDialog.Builder(this);
    alertDialogBuilder.setTitle("No QR Found");
    alertDialogBuilder
            .setMessage("No QR code Detected. Please screenshot the QR code.")
            .setCancelable(false)
            .setPositiveButton("Yes",new DialogInterface.OnClickListener() {
                public void onClick(DialogInterface dialog,int id) {
                }
            });

    // create alert dialog
    AlertDialog alertDialog = alertDialogBuilder.create();

    // show it
    alertDialog.show();

}
```

Figure 4-19 Code of display alert dialog

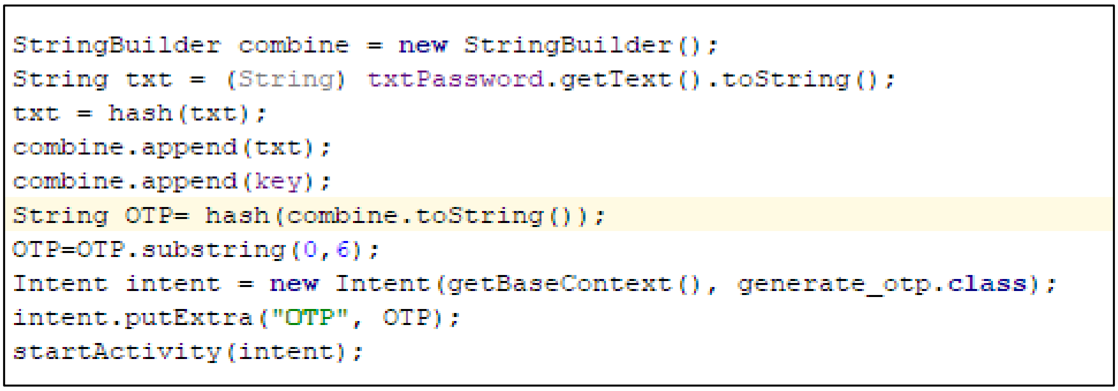
If there is no QR code detected from the photo, the alert dialog will be displayed to the user. The user will need to repeat to choose the photo again.



```
public void receiveDetections(Detector.Detections<Barcode> detections) {
    final SparseArray<Barcode> qrcodes= detections.getDetectedItems();
    if(qrcodes.size()!= 0 && num == 0){
        num = 1;
        Vibrator vibrator= (Vibrator)getApplicationContext().getSystemService(Context.VIBRATOR_SERVICE);
        vibrator.~~vibrate~~(100);
        Intent intent = new Intent(getBaseContext(), password.class);
        intent.putExtra("key",qrcodes.valueAt(0));
        startActivity(intent);
        finish();
    }
}
```

Figure 4-20 Code of detecting QR code using the camera

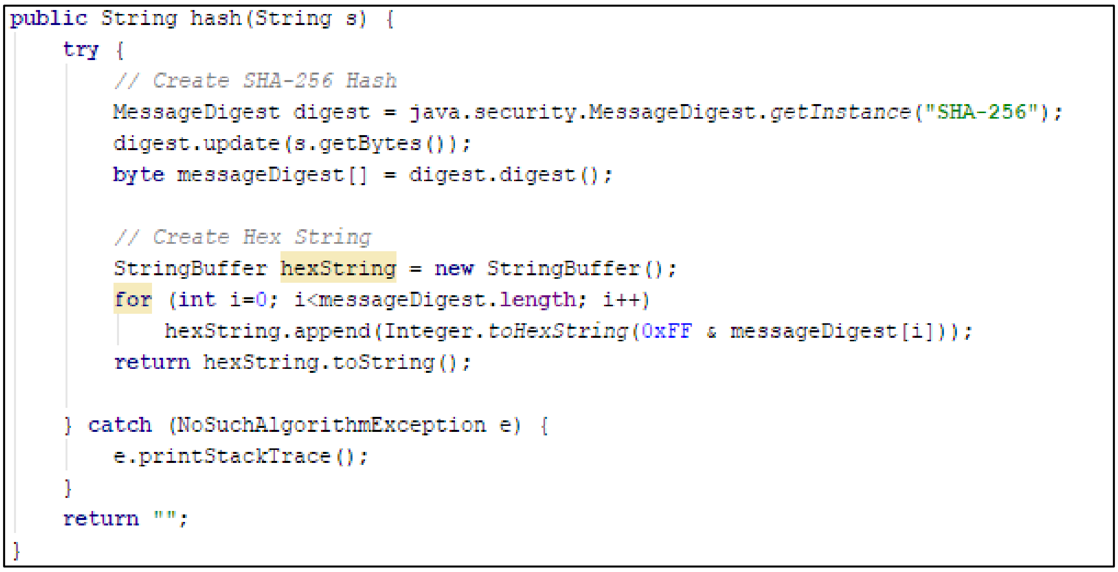
If the user not choosing to browse photo, the user will scan the QR code using the camera. Once the camera detects the QR code, the device will vibrate for one second, retrieve the data and forward to next page.



```
StringBuilder combine = new StringBuilder();
String txt = (String) txtPassword.getText().toString();
txt = hash(txt);
combine.append(txt);
combine.append(key);
String OTP= hash(combine.toString());
OTP=OTP.substring(0,6);
Intent intent = new Intent(getBaseContext(), generate_otp.class);
intent.putExtra("OTP", OTP);
startActivity(intent);
```

Figure 4-21 Code of generating OTP

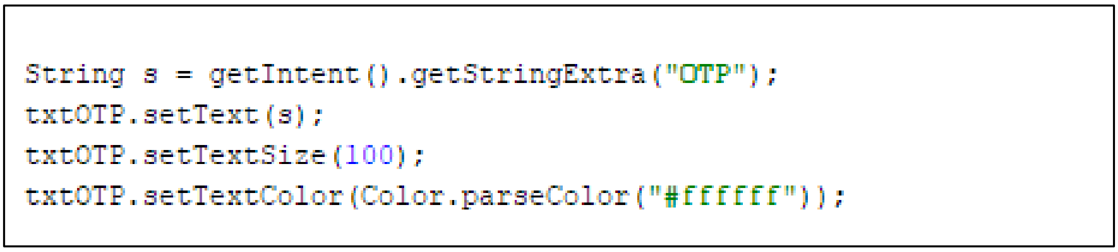
After the user enters the password, the system will obtain the input. The input and data received from the previous page will be combined using StringBuilder. After the combination of string, the hash function is called in order to create the OTP. The OTP will be only choosing the first six characters from the hashed value. The page will then forward to the next page



```
public String hash(String s) {
    try {
        // Create SHA-256 Hash
        MessageDigest digest = java.security.MessageDigest.getInstance("SHA-256");
        digest.update(s.getBytes());
        byte messageDigest[] = digest.digest();

        // Create Hex String
        StringBuffer hexString = new StringBuffer();
        for (int i=0; i<messageDigest.length; i++)
            hexString.append(Integer.toHexString(0xFF & messageDigest[i]));
        return hexString.toString();

    } catch (NoSuchAlgorithmException e) {
        e.printStackTrace();
    }
    return "";
}
```

Figure 4-22 Code of hash algorithm

This is the function to hash the combination of password and random key using SHA-256.



```
String s = getIntent().getStringExtra("OTP");
txtOTP.setText(s);
txtOTP.setTextSize(100);
txtOTP.setTextColor(Color.parseColor("#ffffff"));
```

Figure 4-23 Code of set text in the application interface

The OTP will then be displayed in the application by setText of the layout name txtOTP.

4.3 VERIFICATION PLANS/TEST CASES

Action	Steps	Input	Expected Result
User key in the correct username	1. User key in the username 2. User press next	admin	Redirect the page to display the QR code
User key in the incorrect username	1. User key in the username 2. User press next	adddmin	Display error message stated "no such username exist"
User scan the QR code	1. Web site display the QR code 2. User use phone to scan the QR code	-	Prompt the user password after the scan of QR code
User key in the correct password	1. User key in the password 2. User press login	admin	Redirect to the home page
User key in the incorrect password	1. User key in the password 2. User press login	admins	Display error message stated "Wrong password"
Wrong password exceeds 5 times	1. User key in the password 2. User press login 3. Repeat 5 times	-	Display message "The account is locked temporarily" and email is sent to the account owner
First time device login	1. User key in the username 2. User press next 3. User key in the OTP 4. User press login	-	The system will send verification towards the user account email. The link clicked will approve the user to login the system
Browse photo from gallery	1. User screenshot QR code using phone. 2. Select browse from gallery to obtain QR code information.	-	Forward user to prompt password to generate OTP

Table 4-3-1 Verification plan

4.4 SYSTEM TESTING

4.4.1 Use Case Testing

Main Flow(Normal flow)	Pass
Invalid Username	Pass
Invalid OTP	Pass
Trial more than 5 times	Pass
Not verified device login	Pass

Table 4-4-1 Result of Use Case Testing

4.4.2 Interface of Test Run of System

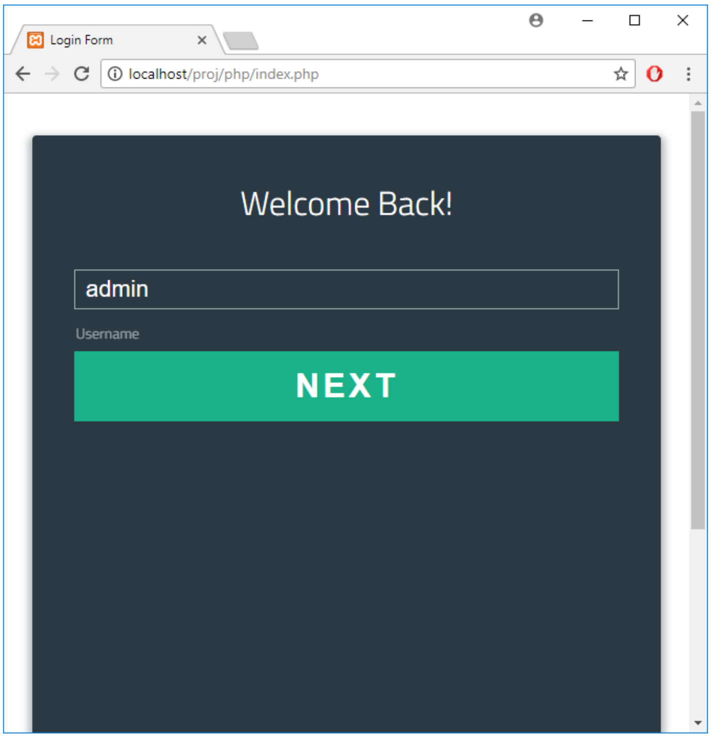
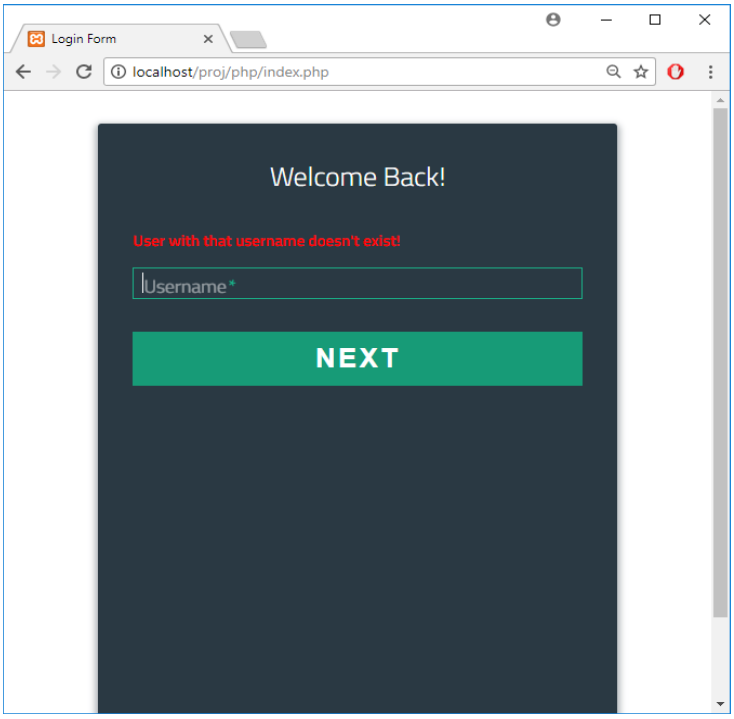


Figure 4-24 Website login page

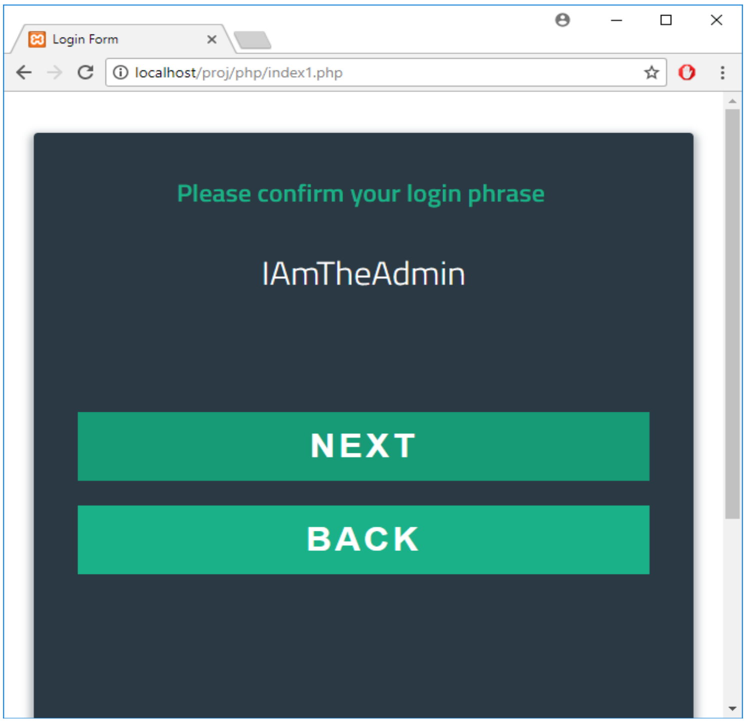
The first step of the system is website will prompt the user for the username.



User with that username doesn't exist!

Figure 4-25 Username does not exist in the database

After the username is entered, the system will check the username validity of username in the database. If it is invalid, the system will display the error message. If the username is valid, the system will forward to Figure 4-26.

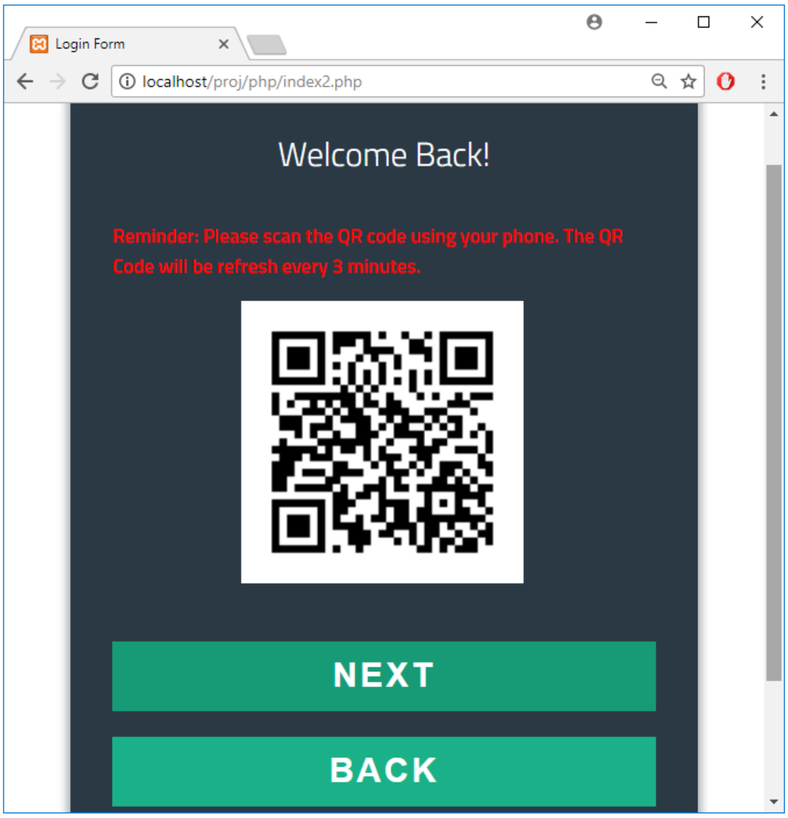


Please confirm your login phrase

IAmTheAdmin

Figure 4-26 Login phrase display

The login phrase will then retrieve from the database of the user details and display on the website. The user will need to confirm the login phrase is correct.

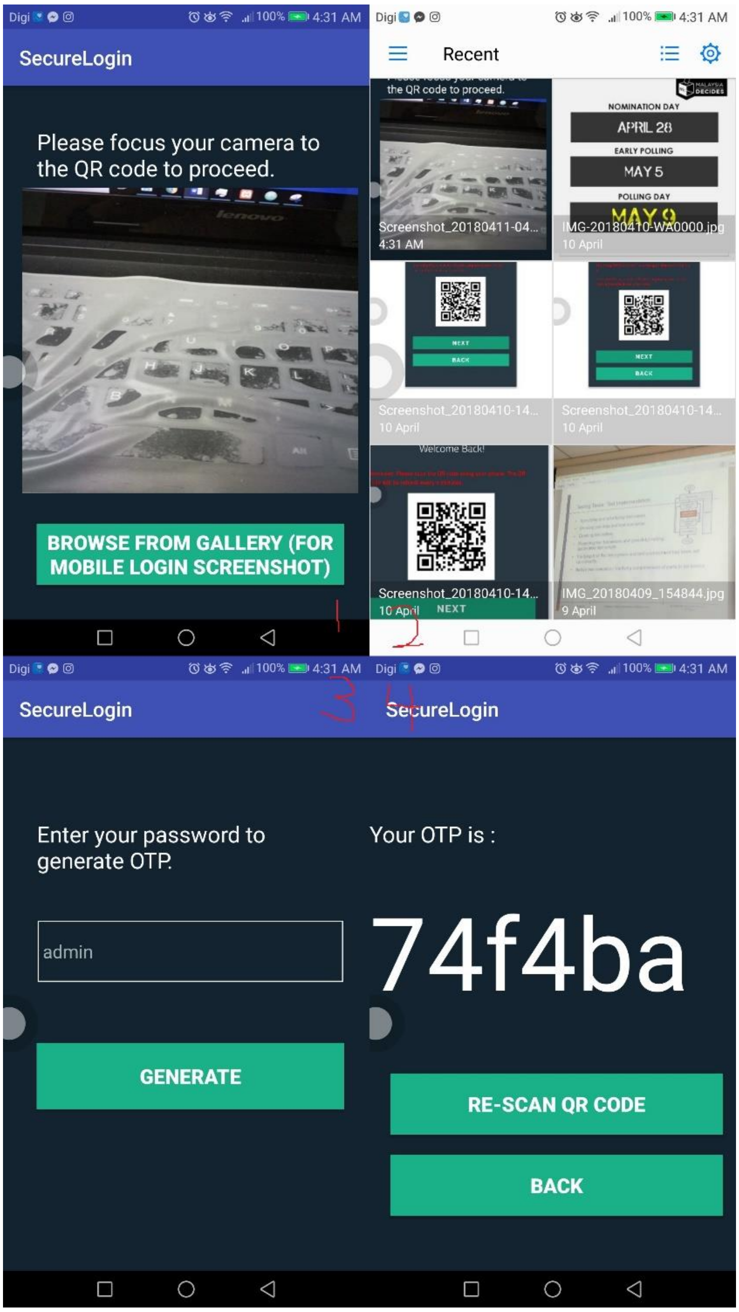


Welcome Back!

Reminder: Please scan the QR code using your phone. The QR Code will be refresh every 3 minutes.

Figure 4-27 QR code contains random key display

After the user confirms the login phrase and clicks next, the random key is retrieved from the database and convert into QR code and display on the website.



Please focus your camera to the QR code to proceed.

Enter your password to generate OTP.

admin

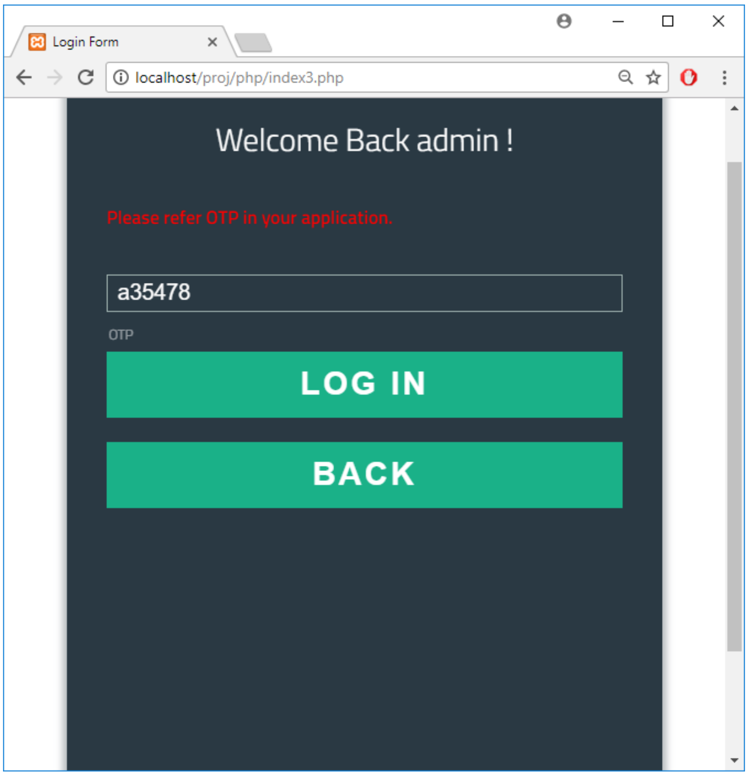
Your OTP is :

74f4ba

SecureLogin
BROWSE FROM GALLERY (FOR MOBILE LOGIN SCREENSHOT)
1
Recent
Screenshot_20180411-04... 4:31 AM
IMG-20180410-WA0000.jpg 10 April
Screenshot_20180410-14... 10 April
Screenshot_20180410-14... 10 April
Screenshot_20180410-14... 10 April
IMG_20180409_154844.jpg 9 April
2
3
4
SecureLogin
GENERATE
RE-SCAN QR CODE
BACK

Figure 4-28 Phone application interface to obtain OTP

The user starts the phone application. The user will then scan the QR code as frame 1 or choose to browse the QR code from the gallery after screenshot as frame 2. After the QR code is decoded, the phone application prompts the user to enter the actual password as frame 3. Next, the user click generate. Lastly, the phone application will display the OTP generated from the combination of secret key and actual password. The user may choose to back if the enter wrong password.



Welcome Back admin !

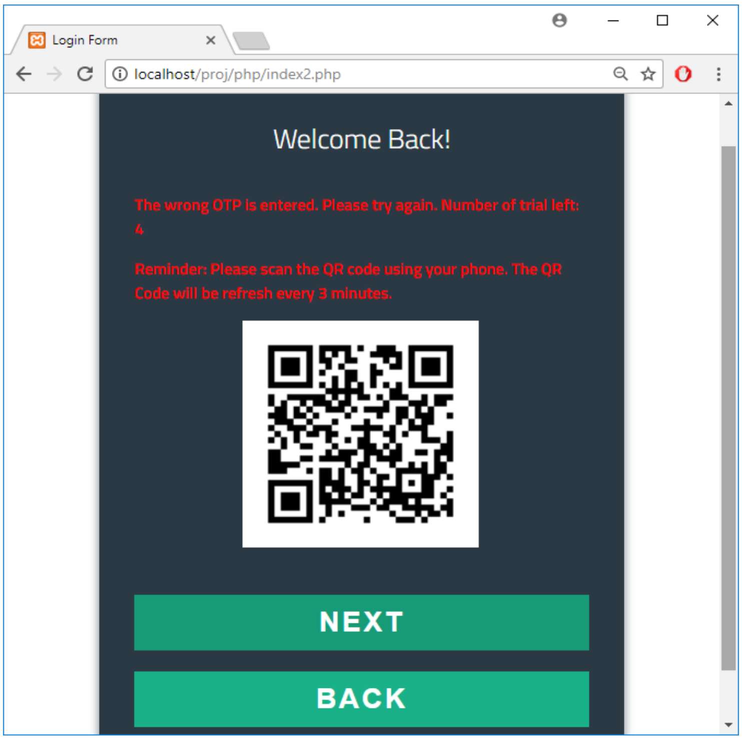
Please refer OTP in your application.

a35478

OTP

Figure 4-29 OTP Prompt

After the user click next in Figure 4-27, the website will prompt OTP from the user.



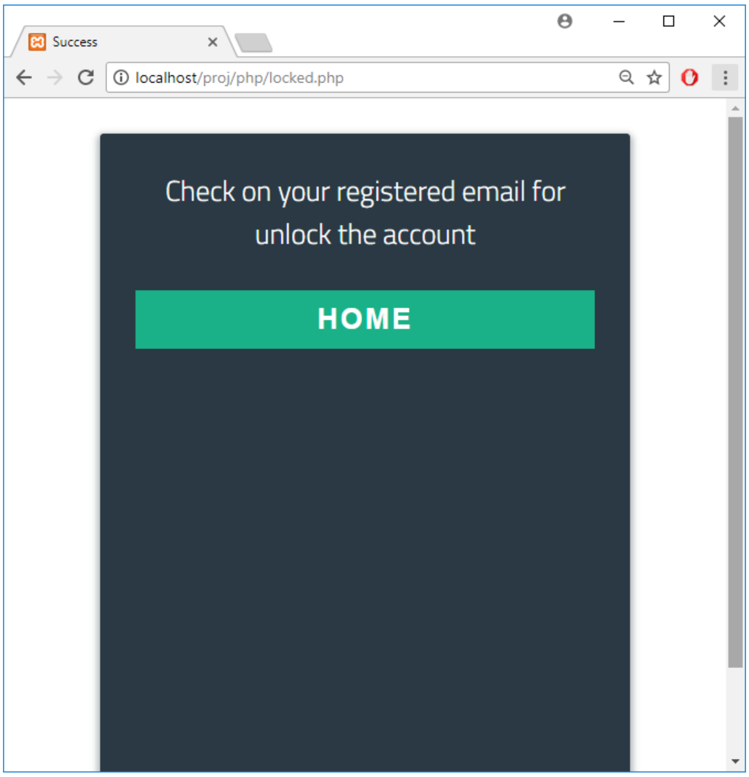
Welcome Back!

The wrong OTP is entered. Please try again. Number of trial left: 4

Reminder: Please scan the QR code using your phone. The QR Code will be refresh every 3 minutes.

Figure 4-30 Invalid OTP

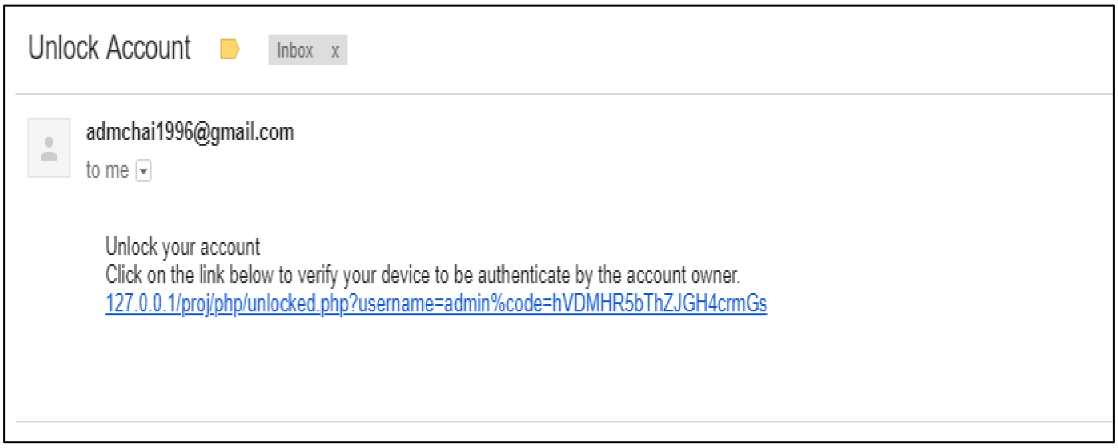
The system will then compare the OTP. If the OTP is not matched, the website will display error message and number of trial left.



Check on your registered email for unlock the account

Figure 4-31 Account locked display

After trial and error of entering OTP more than 5 times, the account of the user will be locked. The email will then be sent to user email as Figure 4-32.



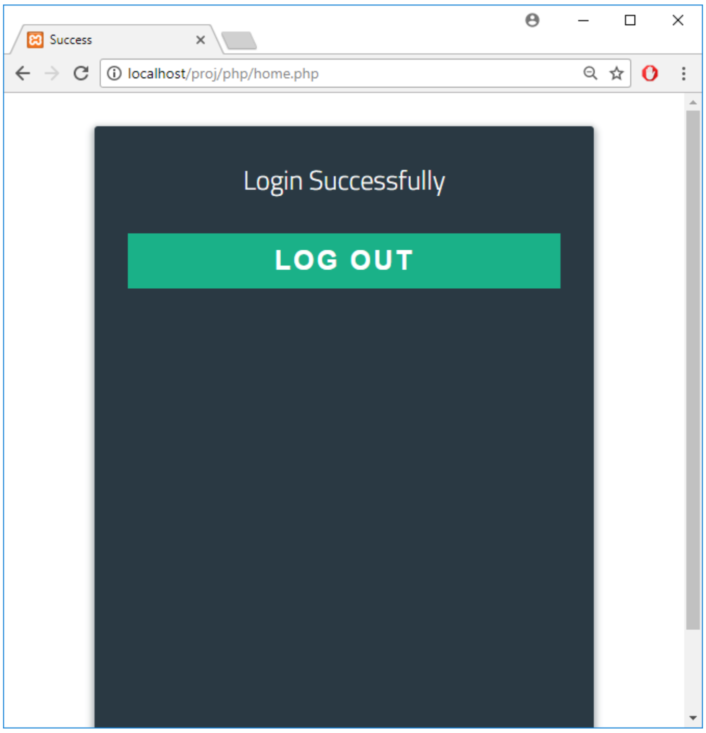
Unlock Account

admchai1996@gmail.com

to me

Unlock your account
Click on the link below to verify your device to be authenticate by the account owner.
127.0.0.1/proj/php/unlocked.php?username=admin%code=hVDMHR5bThZJGH4crmGs

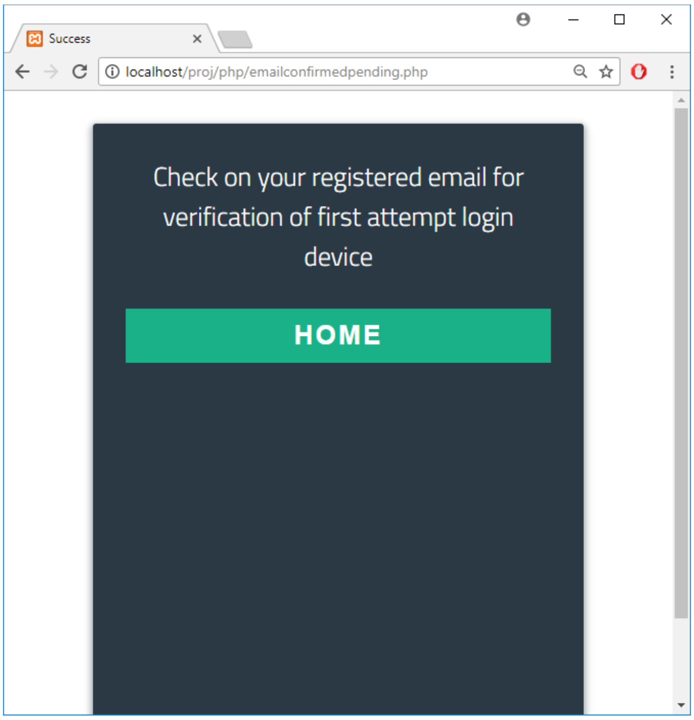
Figure 4-32 Email to unlock the account



Login Successfully

Figure 4-33 Home Page of the website

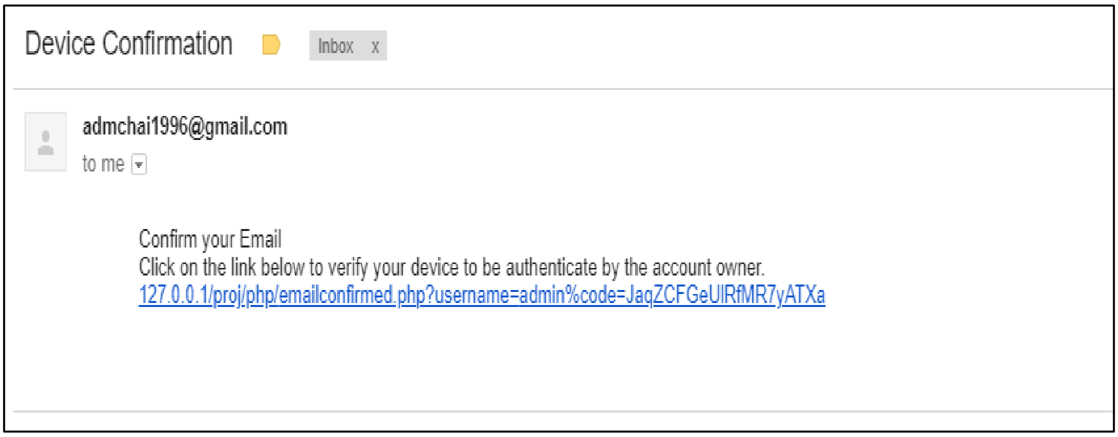
Once the OTP is matched within the trial of 5 times, the website will display login successful.



Check on your registered email for verification of first attempt login device

Figure 4-34 Prompt verification of device login page

If the device attempts the login for the first time, the system will send the email to the user to ask the user to verify the device to be authorized as Figure 4-35.

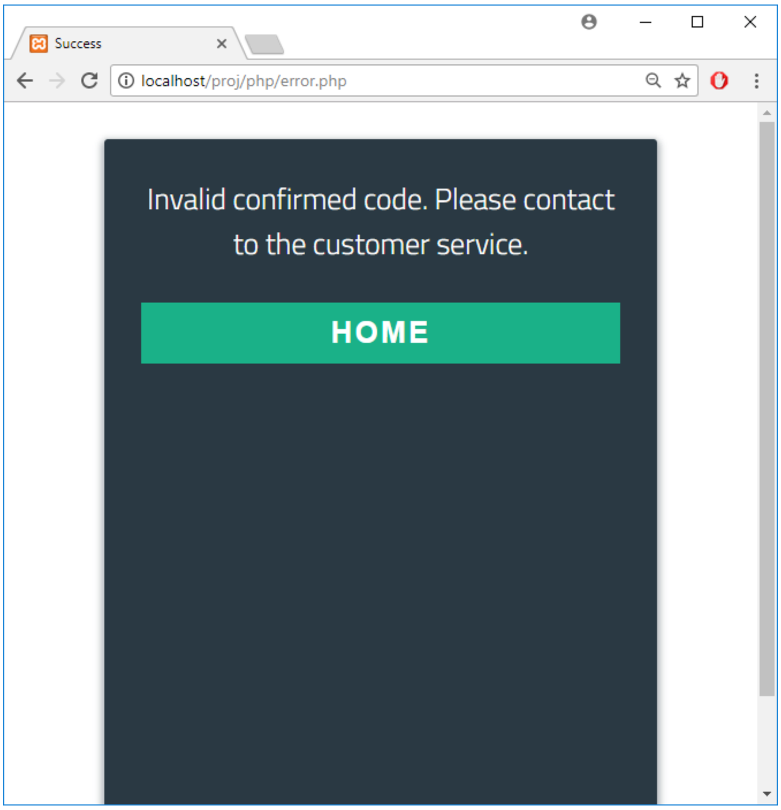

Device Confirmation

admchai1996@gmail.com

to me

Confirm your Email
Click on the link below to verify your device to be authenticate by the account owner.
127.0.0.1/proj/php/emailconfirmed.php?username=admin%code=JaqZCFGeUIRfMR7yATXa

Figure 4-35 Email to verify device to login



Invalid confirmed code. Please contact to the customer service.

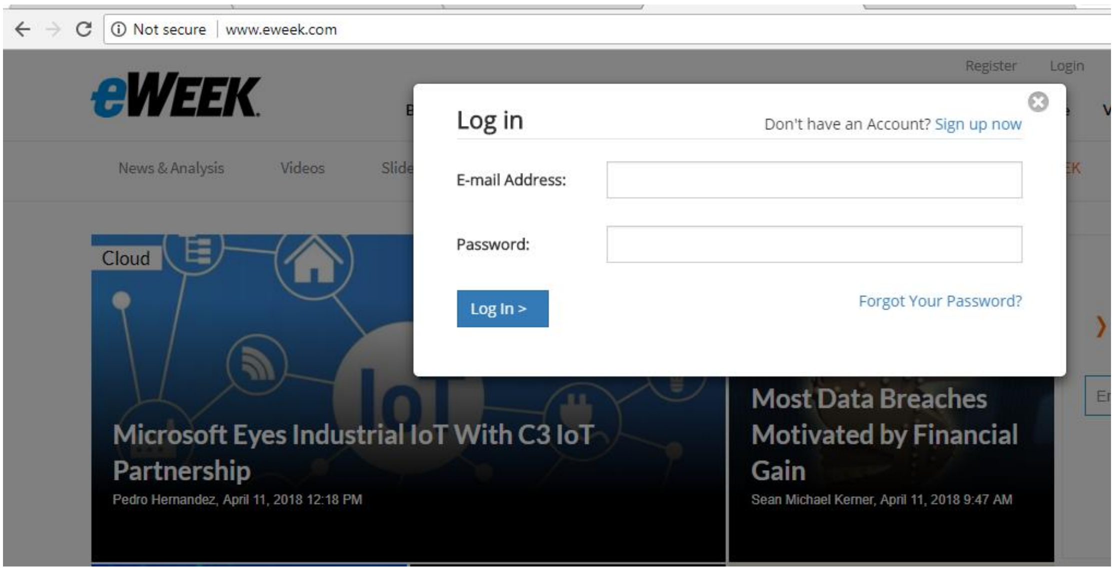
Figure 4-36 Invalid confirm code to verify device

If the confirm code of the link sent in the email is not matched as the database, the system will display the error message.

Chapter 5 : DISCUSSION

5.1 SECURITY ISSUES OF CURRENT LOGIN SYSTEM

In the current existing login authentication system, the password is still will be flowing in the network. The attackers are able to obtain the packet contain the username and password and grant access to the service. Figure 5-1-2 and Figure 5-1-3 show the packets captured in the network that contain username and password on the website.



Log in

Don't have an Account? Sign up now

E-mail Address:

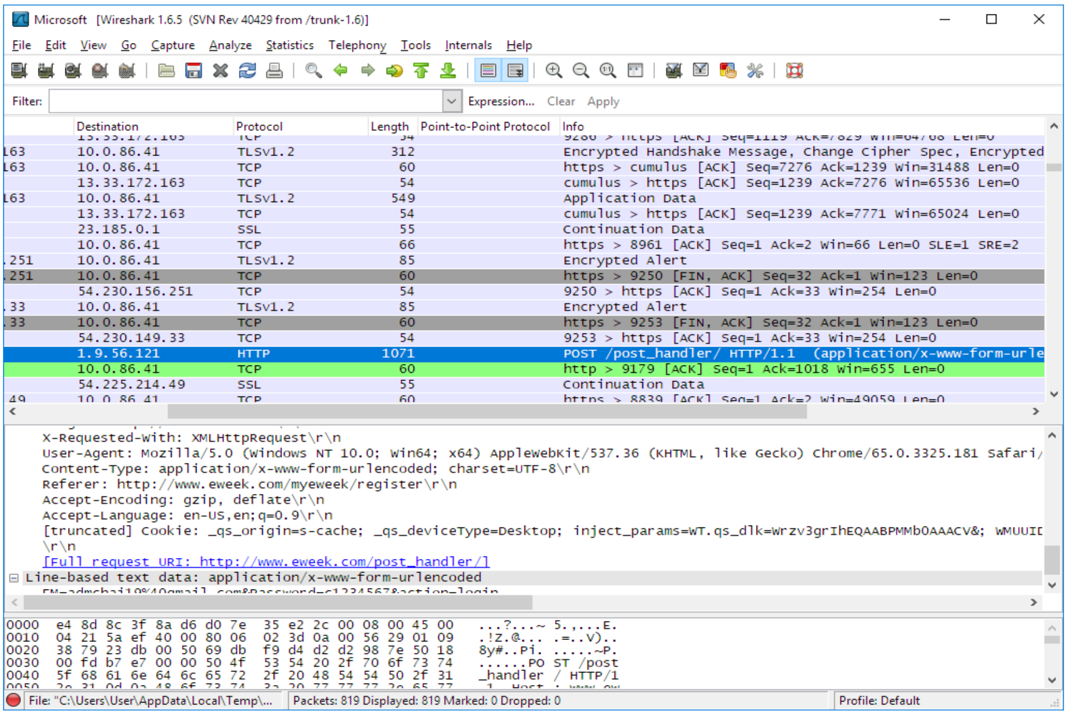
Password:

Log In >

Forgot Your Password?

Not secure
www.eweek.com
eWEEK
Register
Login
News & Analysis
Videos
Slide
Cloud
Microsoft Eyes Industrial IoT With C3 IoT Partnership
Pedro Hernandez, April 11, 2018 12:18 PM
Most Data Breaches Motivated by Financial Gain
Sean Michael Kerner, April 11, 2018 9:47 AM

Figure 5-1 Login interface of the existing system



Microsoft [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]

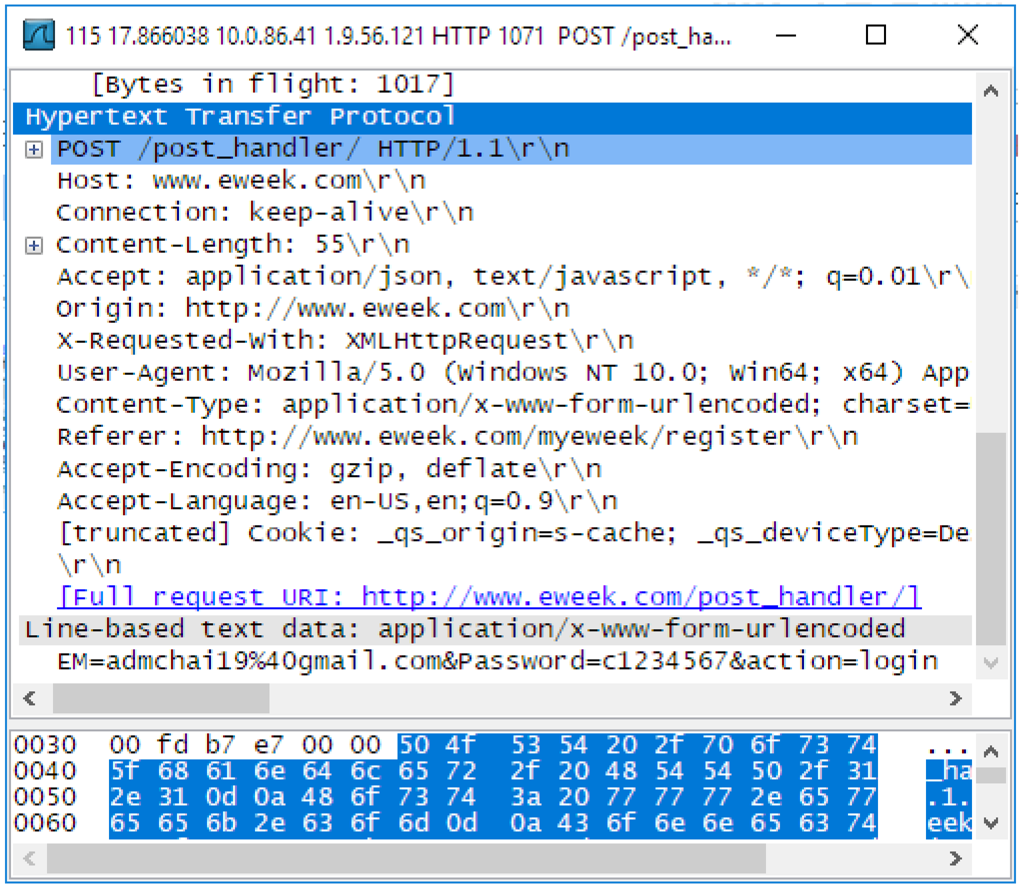
```
      Destination        Protocol      Length  Point-to-Point Protocol  Info
163   10.0.86.41         TLSv1.2       312                              Encrypted Handshake Message, Change Cipher Spec, Encrypted
163   10.0.86.41         TCP            60                              https > cumulus [ACK] Seq=7276 Ack=1239 Win=31488 Len=0
      13.33.172.163      TCP            54                              cumulus > https [ACK] Seq=1239 Ack=7276 Win=65536 Len=0
163   10.0.86.41         TLSv1.2       549                              Application Data
      13.33.172.163      TCP            54                              cumulus > https [ACK] Seq=1239 Ack=7771 Win=65024 Len=0
      23.185.0.1         SSL            55                              Continuation Data
      10.0.86.41         TCP            66                              https > 8961 [ACK] Seq=1 Ack=2 Win=66 Len=0 SLE=1 SRE=2
.251  10.0.86.41         TLSv1.2        85                              Encrypted Alert
.251  10.0.86.41         TCP            60                              https > 9250 [FIN, ACK] Seq=32 Ack=1 Win=123 Len=0
      54.230.156.251     TCP            54                              9250 > https [ACK] Seq=1 Ack=33 Win=254 Len=0
.33   10.0.86.41         TLSv1.2        85                              Encrypted Alert
.33   10.0.86.41         TCP            60                              https > 9253 [FIN, ACK] Seq=32 Ack=1 Win=123 Len=0
      54.230.149.33      TCP            54                              9253 > https [ACK] Seq=1 Ack=33 Win=254 Len=0
      1.9.56.121         HTTP         1071                              POST /post_handler/ HTTP/1.1  (application/x-www-form-urle
      10.0.86.41         TCP            60                              http > 9179 [ACK] Seq=1 Ack=1018 Win=655 Len=0
      54.225.214.49      SSL            55                              Continuation Data
49    10.0.86.41         TCP            60                              https > 8839 [ACK] Seq=1 Ack=2 Win=49059 Len=0
```

```
    X-Requested-With: XMLHttpRequest\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/
    Content-Type: application/x-www-form-urlencoded; charset=UTF-8\r\n
    Referer: http://www.eweek.com/myeweek/register\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    [truncated] Cookie: _qs_origin=s-cache; _qs_deviceType=Desktop; inject_params=WT.qs_dlk=Wrzv3grIhEQAABPMMb0AAACV&; WMUUID
    \r\n
    [Full request URI: http://www.eweek.com/post_handler/]
⊟ Line-based text data: application/x-www-form-urlencoded
```

```
0000  e4 8d 8c 3f 8a d6 d0 7e  35 e2 2c 00 08 00 45 00   ...?...~ 5.,....E.
0010  04 21 5a ef 40 00 80 06  02 3d 0a 00 56 29 01 09   .!Z.@... .=..V)..
0020  38 79 23 db 00 50 69 db  f9 d4 d2 d2 98 7e 50 18   8y#..Pi. .....~P.
0030  00 fd b7 e7 00 00 50 4f  53 54 20 2f 70 6f 73 74   ......PO ST /post
0040  5f 68 61 6e 64 6c 65 72  2f 20 48 54 54 50 2f 31   _handler / HTTP/1
```

File: "C:\Users\User\AppData\Local\Temp\... Packets: 819 Displayed: 819 Marked: 0 Dropped: 0 Profile: Default

Figure 5-2 Wireshark capture for HTTP



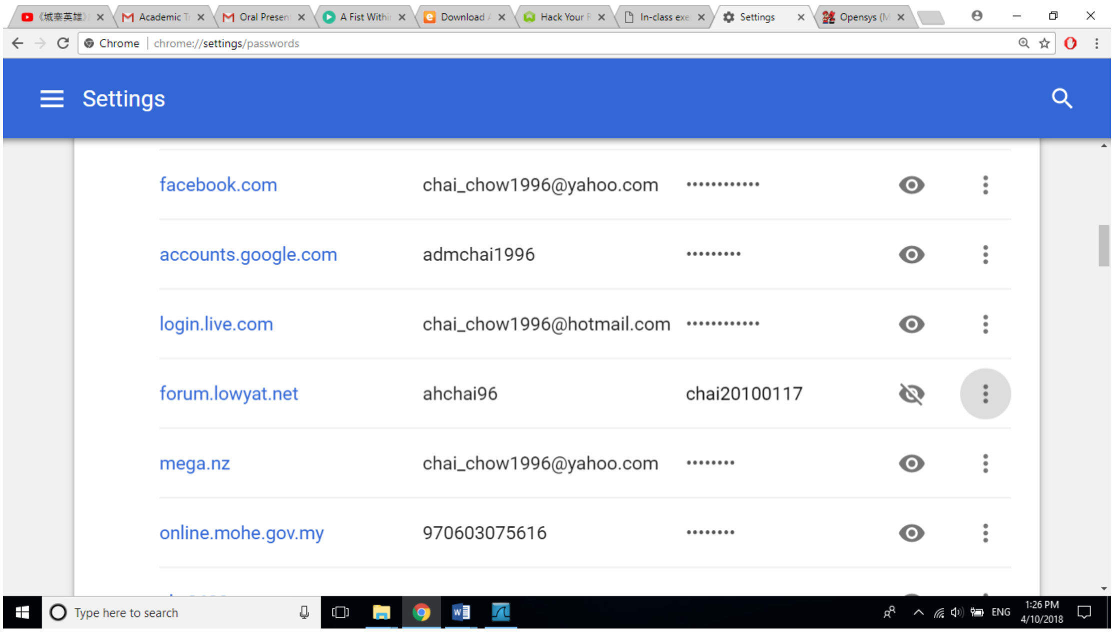
115 17.866038 10.0.86.41 1.9.56.121 HTTP 1071 POST /post_ha...

```
    [Bytes in flight: 1017]
Hypertext Transfer Protocol
⊞ POST /post_handler/ HTTP/1.1\r\n
  Host: www.eweek.com\r\n
  Connection: keep-alive\r\n
⊞ Content-Length: 55\r\n
  Accept: application/json, text/javascript, */*; q=0.01\r\
  Origin: http://www.eweek.com\r\n
  X-Requested-With: XMLHttpRequest\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) App
  Content-Type: application/x-www-form-urlencoded; charset=
  Referer: http://www.eweek.com/myeweek/register\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  [truncated] Cookie: _qs_origin=s-cache; _qs_deviceType=De
  \r\n
  [Full request URI: http://www.eweek.com/post_handler/]
Line-based text data: application/x-www-form-urlencoded
  EM=admchai19%40gmail.com&Password=c1234567&action=login
```

```
0030  00 fd b7 e7 00 00 50 4f  53 54 20 2f 70 6f 73 74   ...
0040  5f 68 61 6e 64 6c 65 72  2f 20 48 54 54 50 2f 31   _ha
0050  2e 31 0d 0a 48 6f 73 74  3a 20 77 77 77 2e 65 77   .1.
0060  65 65 6b 2e 63 6f 6d 0d  0a 43 6f 6e 6e 65 63 74   eek
```

Figure 5-3 Details of packet capture

Some of the users also tend to save password using the cookies in the browser. It is danger when the attackers able to retrieve the cookies since they able to get the username and password of the user on the site.



facebook.com chai_chow1996@yahoo.com ••••••••••••

accounts.google.com admchai1996 •••••••••

login.live.com chai_chow1996@hotmail.com ••••••••••••

forum.lowyat.net ahchai96 chai20100117

mega.nz chai_chow1996@yahoo.com ••••••••

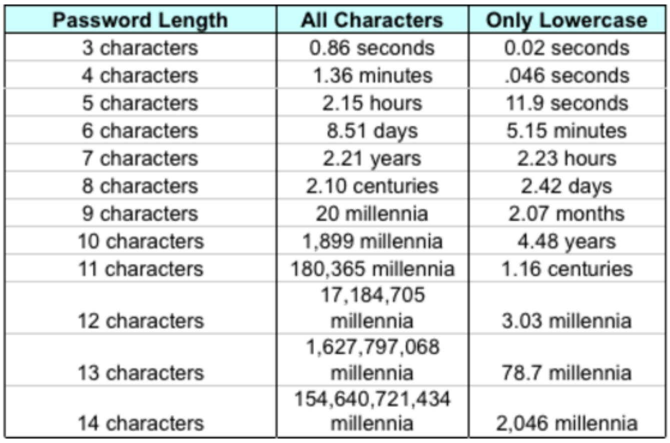
online.mohe.gov.my 970603075616 ••••••••

Figure 5-4 Cookies of username and password

CHAPTER 5: DISCUSSION

5.2 IMPROVEMENT OF PROPOSED LOGIN SYSTEM

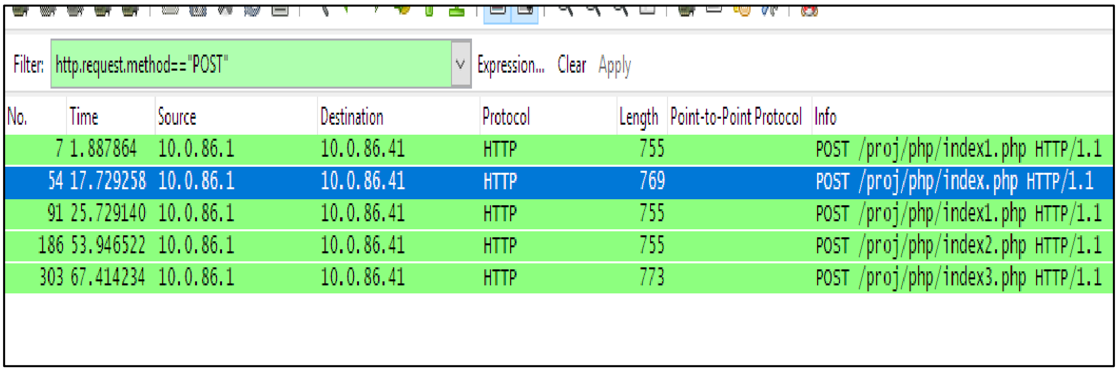
In the proposed login system, it can be proved that the rainbow table is successful to mitigate since there is a long random key generated which is alphanumeric with 40 characters. There are at least 2.12 X 10^{99} of the combination of the random key which is a huge rainbow table to be generated since the password is not included yet. There is improvement be done since the attackers can only limit to have 5 trials to brute force the OTP. By limiting the number of trial, attackers will not able to use tools to help to run brute force attack such as Hydra. It is believed where even if the system does not limit the number of trials, it also needs a very long time to run attack.



Password Length	All Characters	Only Lowercase
3 characters	0.86 seconds	0.02 seconds
4 characters	1.36 minutes	.046 seconds
5 characters	2.15 hours	11.9 seconds
6 characters	8.51 days	5.15 minutes
7 characters	2.21 years	2.23 hours
8 characters	2.10 centuries	2.42 days
9 characters	20 millennia	2.07 months
10 characters	1,899 millennia	4.48 years
11 characters	180,365 millennia	1.16 centuries
12 characters	17,184,705 millennia	3.03 millennia
13 characters	1,627,797,068 millennia	78.7 millennia
14 characters	154,640,721,434 millennia	2,046 millennia

Figure 5-5 Time requires to run dictionary attack with the different number of characters

The figures below show the packet capture in the new system implemented.

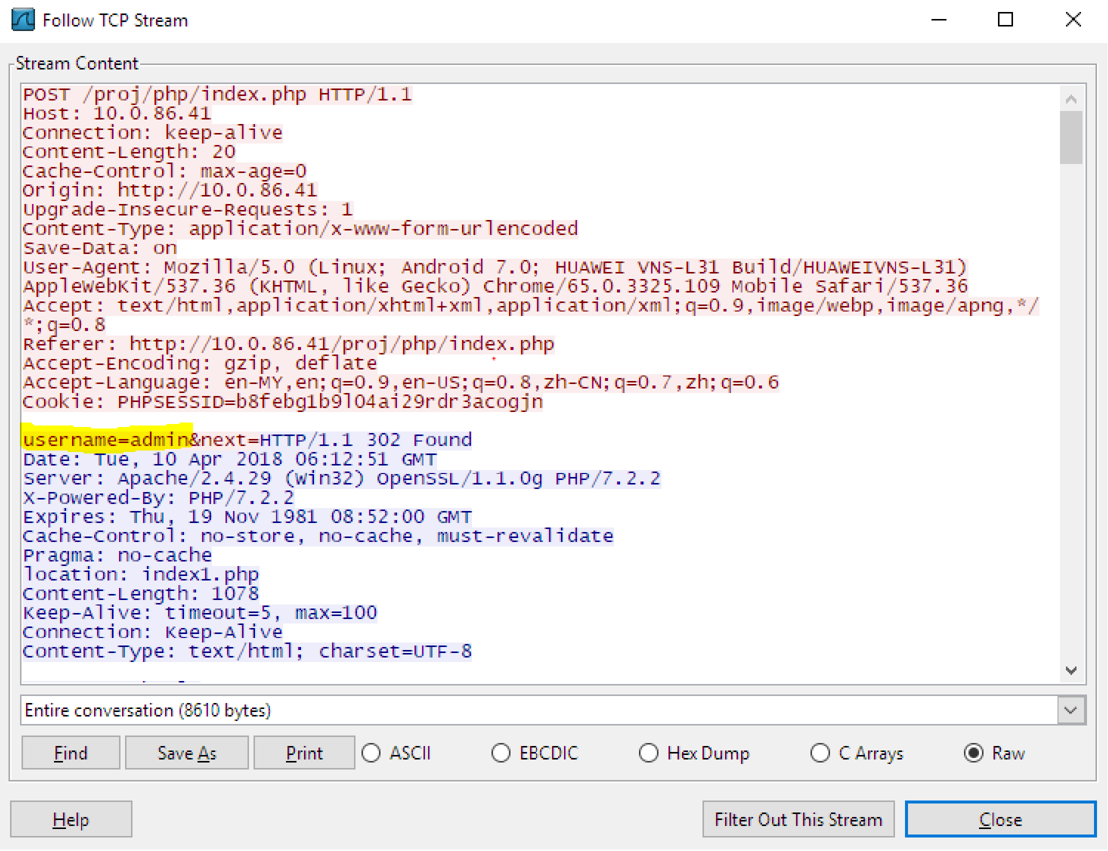


Filter: http.request.method=="POST"

No.	Time	Source	Destination	Protocol	Length	Point-to-Point Protocol	Info
7	1.887864	10.0.86.1	10.0.86.41	HTTP	755		POST /proj/php/index1.php HTTP/1.1
54	17.729258	10.0.86.1	10.0.86.41	HTTP	769		POST /proj/php/index.php HTTP/1.1
91	25.729140	10.0.86.1	10.0.86.41	HTTP	755		POST /proj/php/index1.php HTTP/1.1
186	53.946522	10.0.86.1	10.0.86.41	HTTP	755		POST /proj/php/index2.php HTTP/1.1
303	67.414234	10.0.86.1	10.0.86.41	HTTP	773		POST /proj/php/index3.php HTTP/1.1

Figure 5-6 Wireshark capture for implemented system

CHAPTER 5: DISCUSSION

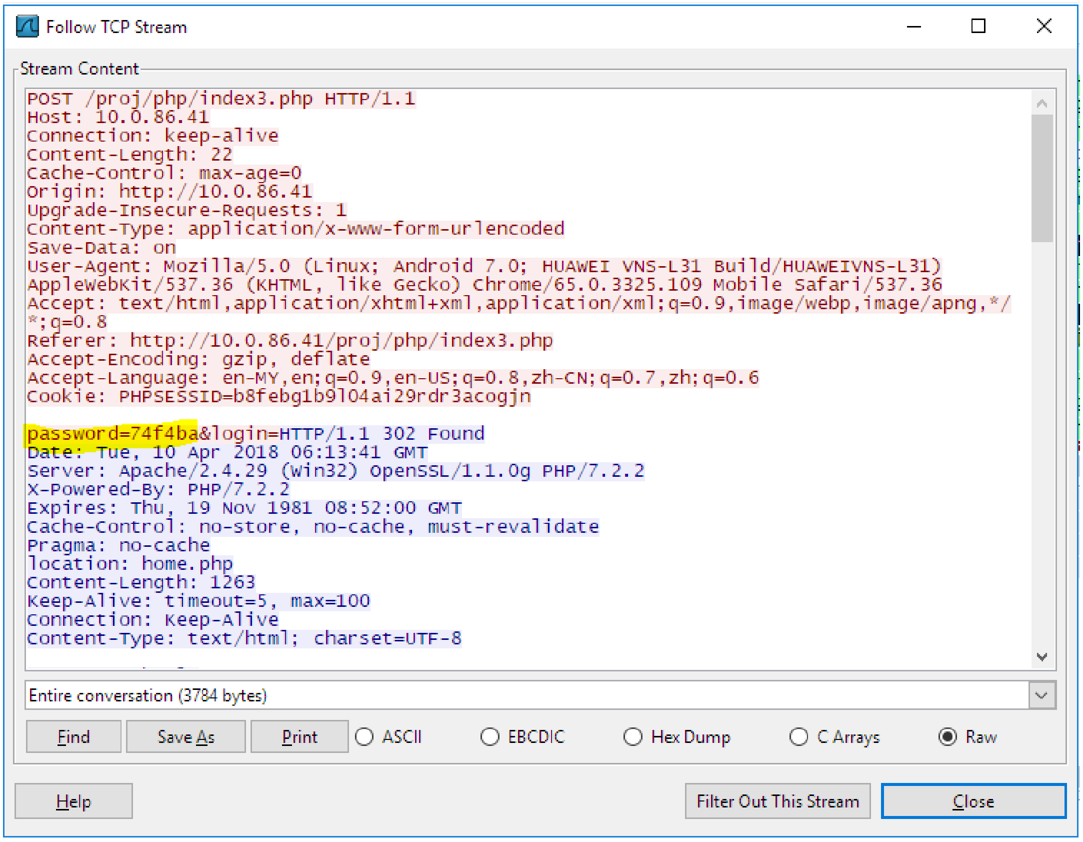


```
POST /proj/php/index.php HTTP/1.1
Host: 10.0.86.41
Connection: keep-alive
Content-Length: 20
Cache-Control: max-age=0
Origin: http://10.0.86.41
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Save-Data: on
User-Agent: Mozilla/5.0 (Linux; Android 7.0; HUAWEI VNS-L31 Build/HUAWEIVNS-L31)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.109 Mobile Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8
Referer: http://10.0.86.41/proj/php/index.php
Accept-Encoding: gzip, deflate
Accept-Language: en-MY,en;q=0.9,en-US;q=0.8,zh-CN;q=0.7,zh;q=0.6
Cookie: PHPSESSID=b8febg1b9l04ai29rdr3acogjn

username=admin&next=HTTP/1.1 302 Found
Date: Tue, 10 Apr 2018 06:12:51 GMT
Server: Apache/2.4.29 (Win32) OpenSSL/1.1.0g PHP/7.2.2
X-Powered-By: PHP/7.2.2
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
location: index1.php
Content-Length: 1078
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Entire conversation (8610 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Figure 5-7 Details of packet capture contain username



```
POST /proj/php/index3.php HTTP/1.1
Host: 10.0.86.41
Connection: keep-alive
Content-Length: 22
Cache-Control: max-age=0
Origin: http://10.0.86.41
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Save-Data: on
User-Agent: Mozilla/5.0 (Linux; Android 7.0; HUAWEI VNS-L31 Build/HUAWEIVNS-L31)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.109 Mobile Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8
Referer: http://10.0.86.41/proj/php/index3.php
Accept-Encoding: gzip, deflate
Accept-Language: en-MY,en;q=0.9,en-US;q=0.8,zh-CN;q=0.7,zh;q=0.6
Cookie: PHPSESSID=b8febg1b9l04ai29rdr3acogjn

password=74f4ba&login=HTTP/1.1 302 Found
Date: Tue, 10 Apr 2018 06:13:41 GMT
Server: Apache/2.4.29 (Win32) OpenSSL/1.1.0g PHP/7.2.2
X-Powered-By: PHP/7.2.2
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
location: home.php
Content-Length: 1263
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Entire conversation (3784 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Figure 5-8 Details of packet capture contain OTP

From the packet capture in Figure 5-2-3 and Figure 5-2-4, it is proved that the user is the username and OTP is exposed in the network. It is important to know that the OTP is only valid once for the user to login into the system. The OTP is not same as the password where the generation of OTP will require the actual password. So, there will be not much security issues if the OTP is exposed to the attackers since they cannot able to explore the actual password in the network.

5.3 REASON FOR SELECTION TOOLS

5.3.1 Reason of choosing PHP

There are few reasons to choose PHP as my project framework. The first reason PHP is chosen is because it is easy to work with and learn. There is a lot of tutorial of PHP can be surf in the website such as tutorialpoint.com.

Apart from that, PHP is an open source which is free. It is also a globally accepted in the website development.

Next, PHP also can work with different type of databases such as PHPMyAdmin and MYSQL. This can help to ease migration of database if there is maintenance occurs in the system.

Furthermore, PHP is a very flexible framework where it able to work with javascript and jQuery. It also compatible with HTML where it can interchange between HTML and PHP within the page.

Lastly, PHP also supports session storage. Session storage is a type of storage will expire when the user closes the browser which is different with cookies that expire in within a period of time. Session storage helps to reduce traffic flow between client and server which reduce the workload of the server.

5.3.2 Reason choose Android

I also choose Android to implement the phone application because it is an open source and can be implemented using a free software to implement the application. Apart from that, I choose android instead of IOS is because the price of phone support IOS is more expensive than phone support android. Android also easy to implement and easy to learn. There is also a lot of phone support android on the market instead of IOS such as Huawei and OPPO.

5.3.3 Reason choose QR code

The user will tend to enter a very short random key instead of a long string that is meaningless. According to Miller's Law, human will only tend to remember around 7 digits or 6 letters. The user will feel frustrated if they need look back and forth between the laptop screen and phone screen. However, if the random key generated is short, the attacker may easily to implement rainbow table to attack the system. So, the system will need a long string which suggested 40 characters of the random key. In order to save work of user to enter the random key manually, the system will use QR code which will ease the user to retrieve the random key.

CHAPTER 6: CONCLUSION

Chapter 6 : CONCLUSION

The project has achieved a huge success to mitigate with the rainbow table attack where the attackers will need to generate a huge rainbow table to exploit the system. A huge rainbow table will require a lot of time to be generated. Apart from that, the system also uses the 2 factor authentication where it requires the actual password and OTP to grant success to the system. Next, one of the huge success where will be the OTP can be generated without connection to internet which helps to prevent the attackers to able to retrieve the actual password from the network flow.

There is some problem faced when implementing the system where there is the shortage of time to complete and improve the system. One of the major problem faced is when the laptop to act as the server of the system is having some faulty. The faulty cause spends of time and money to be fixed where time is wasted for the period of fixing.

There is some improvement can be done by the system where synchronize the OTP with time in order to generate OTP by selecting the random position character of the hashed password. The login system also can be improved by ensuring the password of the user must be more than 8 characters and with the combination of upper and lower case, numbers and expression.

CHAPTER 7: BIBLIOGRAPHY

Chapter 7 : BIBLIOGRAPHY

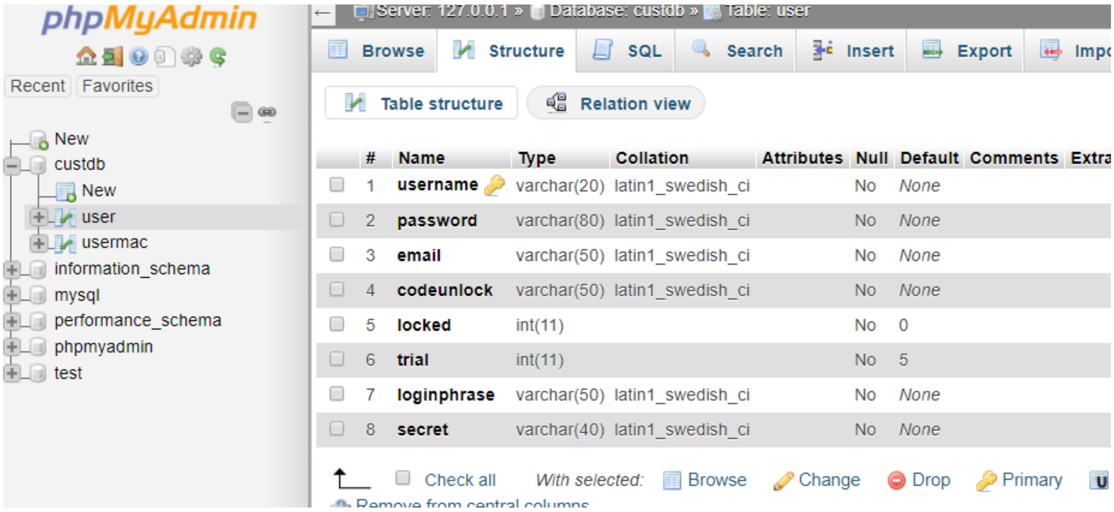
1. Milton K. (n.d.), Can a Hacker Bypass Encryption? , Available from: http://itstillworks.com/can-hacker-bypass-encryption-2996.html (Accessed: 18 November 2017).
2. Vaithyasubramanian, S., Christy, A. and Saravanan, D. (2015) 'Two Factor Authentications for Secured Login in Support of Effective Information Preservation', 10(5), pp. 2053–2056. Available from: http://www.arpnjournals.com/jeas/research_papers/rp_2015/jeas_0315_1713.pdf (Accessed: 18 November 2017).
3. Long A. (2011), How Hackers Take Your Encrypted Password & Crack Them, Available from: https://null-byte.wonderhowto.com/how-to/hackers-take-your-encrypted-passwords-crack-them-0130638/ (Accessed: 18 November 2017).
4. Cheng, X. R. *et al.* (2005) 'Research and realization of authentication technique based on OTP and Kerberos', *Proceedings - Eighth International Conference on High-Performance Computing in Asia-Pacific Region, HPC Asia 2005*, 2005, pp. 409–413. doi: 10.1109/HPCASIA.2005.86. Available from: http://ieeexplore.ieee.org/document/1592297/ (Accessed: 18 November 2017).
5. En.wikipedia.org. (2017). *Smartphone*. [online] Available at: https://en.wikipedia.org/wiki/Smartphone (Accessed: 18 November 2017)..
6. En.wikipedia.org. (2017). *Laptop*. [online] Available at: https://en.wikipedia.org/wiki/Laptop (Accessed: 18 November 2017).
7. Mathur, A. (2012) 'A Research paper : An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms', *International Journal on Computer Science and Engineering (IJCSE)*, 4(9), pp. 1650–1657. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.433.7344&rep=rep1&type=pdf (Accessed: 18 November 2017).
8. Margeret Rouse (2014) *Authentication.* Available at: http://searchsecurity.techtarget.com/definition/authentication/ (Accessed: 18 November 2017).
9. Cristofaro, E. *et al.* (2014) 'A Comparative Usability Study of Two-Factor Authentication', *cs.CR*, (February). doi: 10.14722/usec.2014.23025. Available

at:https://pdfs.semanticscholar.org/028a/70fc1836e113fd18f12b99e08fb024f6bb04.pdf (Accessed: 18 November 2017).

10. Evans J. (2017), Why is Android Studio still such a gruesome embarrassment?, Available from: https://techcrunch.com/2017/02/19/why-is-android-studio-still-such-a-gruesome-embarrassment/ (Accessed: 18 November 2017)..
11. Wallen J. (2017), How to make Apache more secure by hiding directory folders, Available from: http://www.techrepublic.com/article/how-to-make-apache-more-secure-by-hiding-directory-folders/ (Accessed: 18 November 2017)..
12. *Symmetric and Asymmetric Encryption – What are the difference?* n.d., Avaiable from: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences (Accessed: 18 November 2017).
13. *Understanding Login Authentication n.d.* Available from: http://lia.deis.unibo.it/Courses/TecnologieWeb0708/materiale/laboratorio/guide/j2ee14tutorial7/Security5.html (Accessed: 18 November 2017).
14. Chanda, K. (2016) 'Password Security: An Analysis of Password Strengths and Vulnerabilities', *International Journal of Computer Network and Information Security*, 8(7), pp. 23–30. doi: 10.5815/ijcnis.2016.07.04(Accessed: 18 November 2017)..
15. Pagliery, J. (2014) *Half of American adults hacked this year*. Available at: http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/index.html (Accessed: 18 November 2017).
16. Bonneau, J. *et al.* (2015) 'Passwords and the evolution of imperfect authentication', *Communications of the ACM*, 58(7), pp. 78–87. doi: 10.1145/2699390(Accessed: 18 November 2017).
17. Denso Wave (2016) *History of QR Code*, *Denso Wave Incorporated*. Available at: http://www.qrcode.com/en/history/ (Accessed: 18 November 2017).
18. Josel, H. et al(2017) 'Analysis of the use of Rainbow Tables to break hash'. doi: 10.3233/JIFS-169147.
19. Pozadzides, J. (2010) *How I'd Hack Your Weak Passwords*. Available at: https://lifehacker.com/5505400/how-id-hack-your-weak-passwords (Accessed: 12 April 2018).
20. Bradley, A. (2017) *Why Use PHP?* Available at: https://www.thoughtco.com/why-use-php-2694006 (Accessed: 12 April 2018).

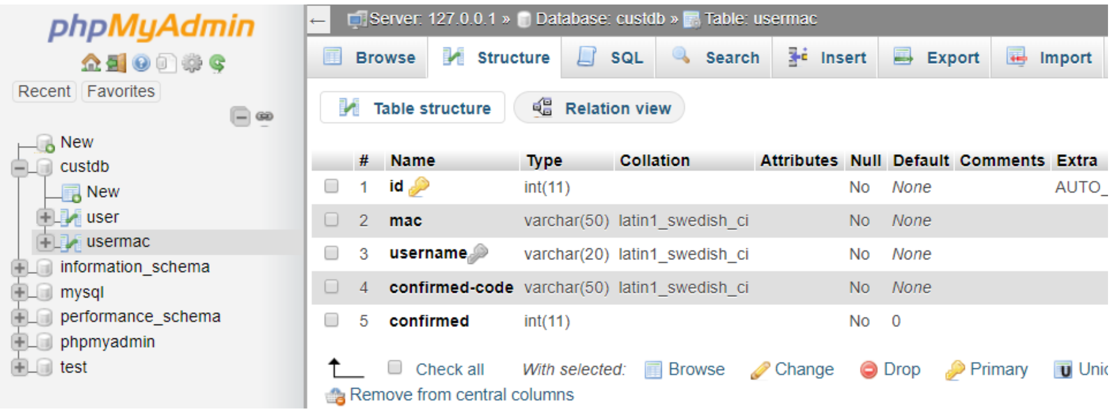
APPENDICES

Appendix-A :Database



	#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra
□	1	**username**	varchar(20)	latin1_swedish_ci		No	*None*		
□	2	**password**	varchar(80)	latin1_swedish_ci		No	*None*		
□	3	**email**	varchar(50)	latin1_swedish_ci		No	*None*		
□	4	**codeunlock**	varchar(50)	latin1_swedish_ci		No	*None*		
□	5	**locked**	int(11)			No	0		
□	6	**trial**	int(11)			No	5		
□	7	**loginphrase**	varchar(50)	latin1_swedish_ci		No	*None*		
□	8	**secret**	varchar(40)	latin1_swedish_ci		No	*None*		

Figure shows the database attribute in the user table



	#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra
□	1	**id**	int(11)			No	*None*		AUTO_
□	2	**mac**	varchar(50)	latin1_swedish_ci		No	*None*		
□	3	**username**	varchar(20)	latin1_swedish_ci		No	*None*		
□	4	**confirmed-code**	varchar(50)	latin1_swedish_ci		No	*None*		
□	5	**confirmed**	int(11)			No	0		

Figure shows the database attribute in the usermac table

APPENDICES

Appendix-B :Final Year Project Weekly Report

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: 3, 3	**Study week no.: 2**
Student Name & ID: CHOW WEN CHAI 140ACB5547	
Supervisor:DR. GAN MING LEE	
Project Title: SECURE LOGIN AUTHENTICATION SYSTEM	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Study the features of QR code
- Study the advantage of QR code

2. WORK TO BE DONE

- Implement QR code in website to act as a random key in website
- Implement android application to decode QR code

3. PROBLEMS ENCOUNTERED

- **(N/A)**

4. SELF EVALUATION OF THE PROGRESS

- Learnt the features of QR code

Supervisor's signature

Student's signature

APPENDICES

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: 3, 3	**Study week no.: 4**
Student Name & ID: CHOW WEN CHAI 140ACB5547	
Supervisor:DR. GAN MING LEE	
Project Title: SECURE LOGIN AUTHENTICATION SYSTEM	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Implement QR code in website to act as a random key in website
- Implement android application to decode QR code

2. WORK TO BE DONE

- Add features on limit number of trial to attempt to login
- Add features to check whether the device is verified to login
- Add mailing system

3. PROBLEMS ENCOUNTERED

- Import of library is not compatible in android
- Difficult to implement scan QR using phone camera

4. SELF EVALUATION OF THE PROGRESS

- Main objective of the is achieved
- 60% of the project is complete

Supervisor's signature

Student's signature

APPENDICES

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: 3, 3	**Study week no.: 6**
Student Name & ID: CHOW WEN CHAI 140ACB5547	
Supervisor:DR. GAN MING LEE	
Project Title: SECURE LOGIN AUTHENTICATION SYSTEM	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Add features on limit number of trial to attempt to login
- Add features to check whether the device is verified to login
- Add mailing system

2. WORK TO BE DONE

- Add import photo from gallery to decode QR code in phone application

3. PROBLEMS ENCOUNTERED

- No knowledge of mailing system
- Need to by pass proxy to implement workable mailing system

4. SELF EVALUATION OF THE PROGRESS

- 90% of the project is complete

Supervisor's signature

Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: 3, 3	**Study week no.: 8**
Student Name & ID: CHOW WEN CHAI 140ACB5547	
Supervisor:DR. GAN MING LEE	
Project Title: SECURE LOGIN AUTHENTICATION SYSTEM	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Add import photo from gallery to decode QR code in phone application

2. WORK TO BE DONE

- Test the system
- Debug and improve the system

3. PROBLEMS ENCOUNTERED

- No much information gain from google to implement this features

4. SELF EVALUATION OF THE PROGRESS

- The project is completed

__________________________ Supervisor's signature

__________________________ Student's signature

APPENDICES

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: 3, 3	**Study week no.: 10**
Student Name & ID: CHOW WEN CHAI 140ACB5547	
Supervisor:DR. GAN MING LEE	
Project Title: SECURE LOGIN AUTHENTICATION SYSTEM	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Test the system
- Debug and improve the system

2. WORK TO BE DONE

- Prepare report

3. PROBLEMS ENCOUNTERED

(N/A)

4. SELF EVALUATION OF THE PROGRESS

- The system is fully tested which is achieved all the expected outcome

Supervisor's signature

Student's signature

APPENDICES

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: 3, 3	**Study week no.: 12**
Student Name & ID: CHOW WEN CHAI 140ACB5547	
Supervisor:DR. GAN MING LEE	
Project Title: SECURE LOGIN AUTHENTICATION SYSTEM	

1. WORK DONE

- Prepare report

2. WORK TO BE DONE

- Complete the report
- Prepare for poster
- Prepare presentation slide

3. PROBLEMS ENCOUNTERED

(N/A)

4. SELF EVALUATION OF THE PROGRESS

- 60% of the report is complete

___________________________ Supervisor's signature

___________________________ Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: 3, 3	**Study week no.: 13**
Student Name & ID: CHOW WEN CHAI 140ACB5547	
Supervisor:DR. GAN MING LEE	
Project Title: SECURE LOGIN AUTHENTICATION SYSTEM	

1. WORK DONE

- Complete the report
- Prepare for poster
- Prepare presentation slide
- Burn report and program into CD

2. WORK TO BE DONE

- Prepare for presentation

3. PROBLEMS ENCOUNTERED

(N/A)

4. SELF EVALUATION OF THE PROGRESS

- The report is completed

__________________________ __________________________

Supervisor’s signature Student’s signature

APPENDICES

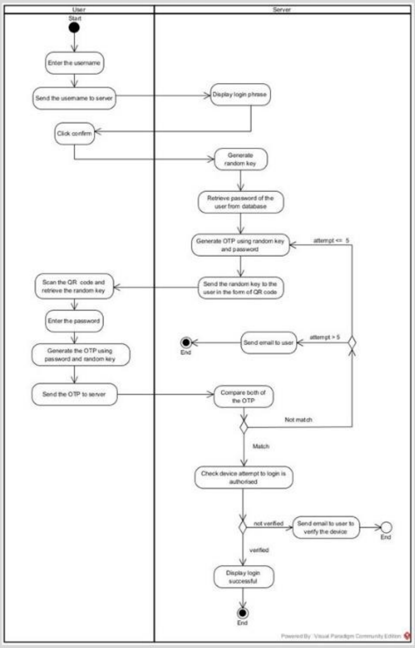
Appendix-C : Poster

Secure Authentication Login System

Introduction

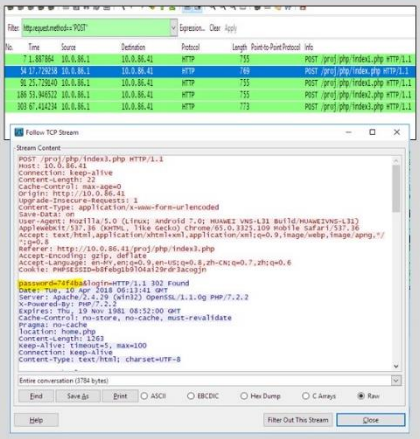
Authentication is a process to authenticate the user who wishes to use to perform activity. In the era of rapid evolution of the wireless technology, the safety of the user account is no longer secure by only using the password because of discovery method to crack the solution.

Methodology



User
Server
Start
Enter the username
Send the username to server
Display login phrase
Click confirm
Generate random key
Retrieve password of the user from database
Generate OTP using random key and password
attempt <= 5
Send the random key to the user in the form of QR code
Scan the QR code and retrieve the random key
Enter the password
Send email to user
attempt > 5
End
Generate the OTP using password and random key
Send the OTP to server
Compare both of the OTP
Not match
Match
Check device attempt to login is authorised
not verified
Send email to user to verify the device
End
verified
Display login successful
End
Powered By: Visual Paradigm Community Edition

Result



```
No.  Time       Source     Destination  Protocol  Length  Point-to-Point Protocol  Info
  7  1.887864   10.0.86.1  10.0.86.41   HTTP      755                              POST /proj/php/index1.php HTTP/1.1
 54  17.729258  10.0.86.1  10.0.86.41   HTTP      769                              POST /proj/php/index.php HTTP/1.1
 91  25.729140  10.0.86.1  10.0.86.41   HTTP      755                              POST /proj/php/index1.php HTTP/1.1
186  53.946522  10.0.86.1  10.0.86.41   HTTP      755                              POST /proj/php/index2.php HTTP/1.1
303  67.414234  10.0.86.1  10.0.86.41   HTTP      773                              POST /proj/php/index3.php HTTP/1.1
```

```
POST /proj/php/index3.php HTTP/1.1
Host: 10.0.86.41
Connection: keep-alive
Content-Length: 22
Cache-Control: max-age=0
Origin: http://10.0.86.41
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Save-Data: on
User-Agent: Mozilla/5.0 (Linux; Android 7.0; HUAWEI VNS-L31 Build/HUAWEIVNS-L31)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.109 Mobile Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8
Referer: http://10.0.86.41/proj/php/index3.php
Accept-Encoding: gzip, deflate
Accept-Language: en-MY,en;q=0.9,en-US;q=0.8,zh-CN;q=0.7,zh;q=0.6
Cookie: PHPSESSID=b8febg1b9l04ai29rdr3acogjn

password=74f4ba&login=HTTP/1.1 302 Found
Date: Tue, 10 Apr 2018 06:13:41 GMT
Server: Apache/2.4.29 (Win32) OpenSSL/1.1.0g PHP/7.2.2
X-Powered-By: PHP/7.2.2
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
location: home.php
Content-Length: 1263
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

From the result above, it can be proved that the actual password is not flow in the network.

Discussion

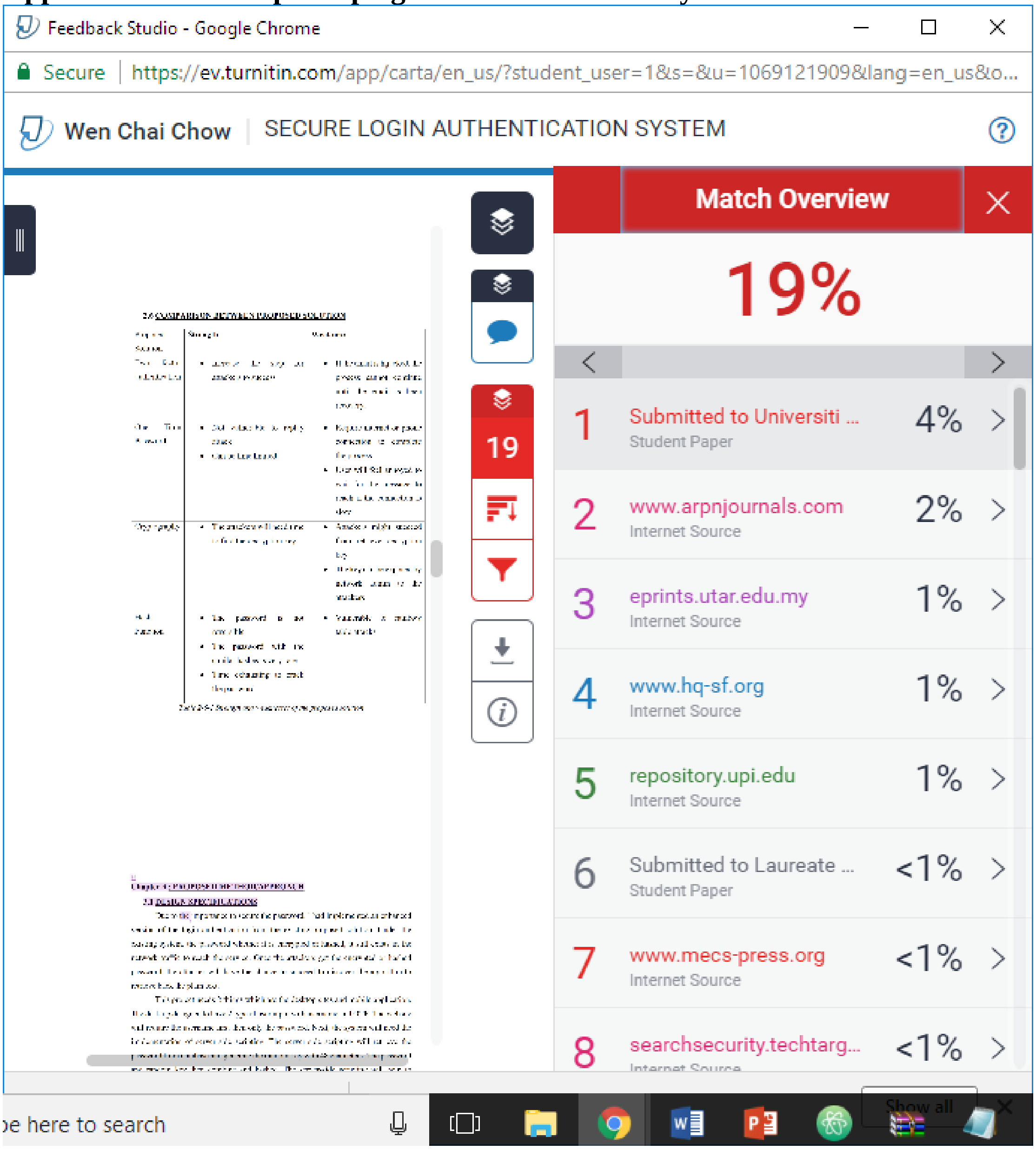
It is a solution which utilize the features of the QR code and two-factor authentication. It also ensure the password will not flow in the network. It is a very secure authentication login system because it only allows the user to enter once OTP for each random key. The random key generated in the system also is very long which will require the attackers to generate a huge rainbow table. The random key will be displayed in QR code form and the user will need to scan for QR code for retrieving the random key. In this proposed solution, the system able to defend from rainbow table attack and replay attack.

Conclusion

It is important to have a secure authentication login system because the organization has the responsibility to secure the user's detail from the attackers. The proposed system believed will be able to protect the user from been hacked by attackers because of the time exhaustion in generating rainbow table.

APPENDICES

Appendix-D : Example of plagiarism check summary



Feedback Studio - Google Chrome

Secure | https://ev.turnitin.com/app/carta/en_us/?student_user=1&s=&u=1069121909&lang=en_us&o...

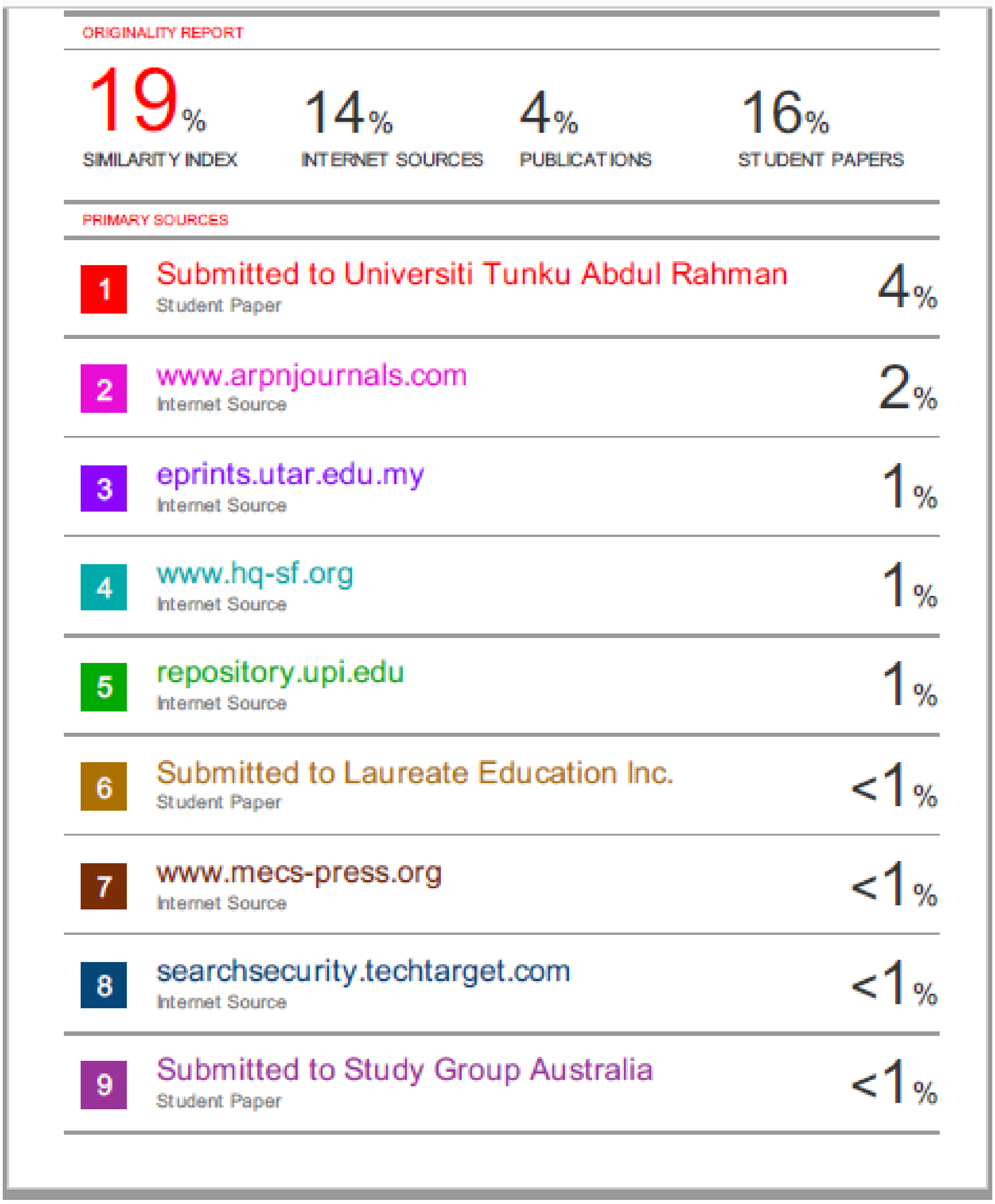
Wen Chai Chow | SECURE LOGIN AUTHENTICATION SYSTEM

Match Overview

19%

1	Submitted to Universiti ... Student Paper	4%
2	www.arpnjournals.com Internet Source	2%
3	eprints.utar.edu.my Internet Source	1%
4	www.hq-sf.org Internet Source	1%
5	repository.upi.edu Internet Source	1%
6	Submitted to Laureate ... Student Paper	<1%
7	www.mecs-press.org Internet Source	<1%
8	searchsecurity.techtarg... Internet Source	<1%

APPENDICES

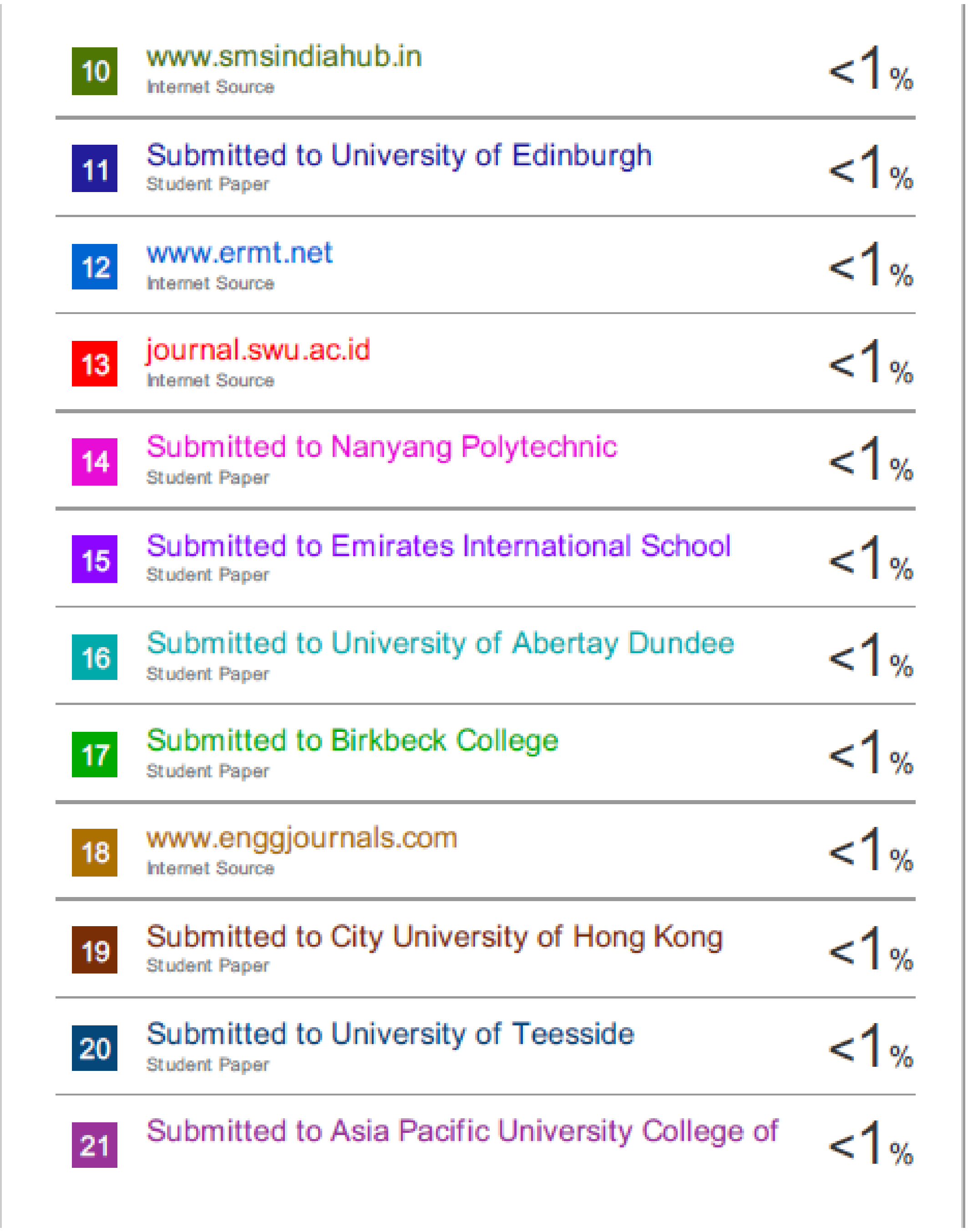


ORIGINALITY REPORT

19%	14%	4%	16%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universiti Tunku Abdul Rahman Student Paper	4%
2	www.arpnjournals.com Internet Source	2%
3	eprints.utar.edu.my Internet Source	1%
4	www.hq-sf.org Internet Source	1%
5	repository.upi.edu Internet Source	1%
6	Submitted to Laureate Education Inc. Student Paper	<1%
7	www.mecs-press.org Internet Source	<1%
8	searchsecurity.techtarget.com Internet Source	<1%
9	Submitted to Study Group Australia Student Paper	<1%



10	www.smsindiahub.in Internet Source	<1%
11	Submitted to University of Edinburgh Student Paper	<1%
12	www.ermt.net Internet Source	<1%
13	journal.swu.ac.id Internet Source	<1%
14	Submitted to Nanyang Polytechnic Student Paper	<1%
15	Submitted to Emirates International School Student Paper	<1%
16	Submitted to University of Abertay Dundee Student Paper	<1%
17	Submitted to Birkbeck College Student Paper	<1%
18	www.enggjournals.com Internet Source	<1%
19	Submitted to City University of Hong Kong Student Paper	<1%
20	Submitted to University of Teesside Student Paper	<1%
21	Submitted to Asia Pacific University College of	<1%

APPENDICES

Form Number: FM-IAD-005	Rev No.: 0	Effective Date: 01/10/2013	Page No.: 1of 1

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

Full Name(s) of Candidate(s)	CHOW WEN CHAI
ID Number(s)	14ACB05547
Programme / Course	BACHELOR OF COMPUTER SCIENCE(HONS)
Title of Final Year Project	SECURE LOGIN AUTHENTICATION SYSTEM

Similarity	**Supervisor's Comments** **(Compulsory if parameters of originality exceeds the limits approved by UTAR)**
Overall similarity index: __19_____ **%** **Similarity by source** Internet Sources: __14_________% Publications: ___4________ % Student Papers: __16________ %	
Number of individual sources listed of more than 3% similarity: ___1_____	
Parameters of originality required and limits approved by UTAR are as Follows: **(i) Overall similarity index is 20% and below, and** **(ii) Matching of individual sources listed must be less than 3% each, and** **(iii) Matching texts in continuous block must not exceed 8 words** ***Note: Parameters (i) – (ii) shall exclude quotes, bibliography and text matches which are less than 8 words.***	

Note Supervisor/Candidate(s) is/are required to provide softcopy of full set of the originality report to Faculty/Institute

Based on the above results, I hereby declare that I am satisfied with the originality of the Final Year Project Report submitted by my student(s) as named above.

______________________________	______________________________
Signature of Supervisor	Signature of Co-Supervisor
Name: Dr. GAN MING LEE	Name: ______________
Date: 12 March 2018_____	Date: __________________