PROJECT REPORT

TITLE:

RENT-A-BIKE WEB APPLICATION

COURSE CODE	:	BIS20303
COURSE NAME	:	WEB SECURITY
FACULTY	:	FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
STUDENTS NAME	:	1. NIK NURHANI NADIRAH BINTI KAMALRUZAMAN (AI200093) 2. NOR AISYAH NAJWA BINTI AZIZAN (AI200085) 3. NURIN NABILAH BINTI RASYIHAN ANWAR (AI200073) 4. WAN NUR SYUHADA BINTI SAMMIO (AI200205) 5. MUHAMMAD AMIRUL BIN MD RASID (AI190110)
GROUP	:	2
SECTION	:	5
SEMESTER/SESION	:	SEMESTER 2/SESSION 2021/2022
LECTURER'S NAME	:	PROF. MADYA TS. DR. HAIRULNIZAM BIN MAHDIN
DUE DATE	:	9TH JUNE 2022

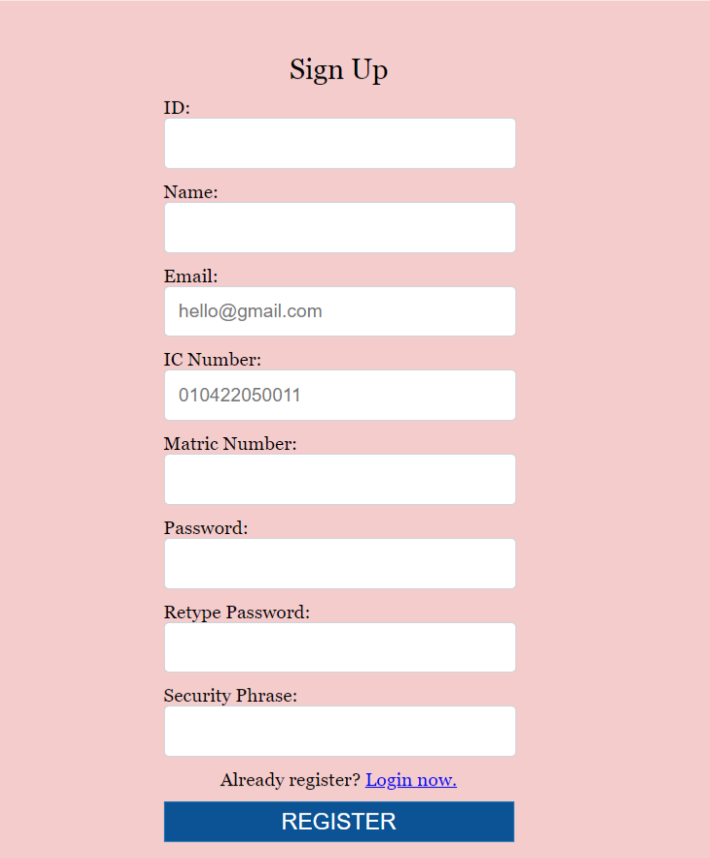
MARKS	

CONTENTS

ACTIVITY 1: REGISTRATION

1.1 Register

A signup page (also known as a registration page) allows individuals to register and acquire access to our system which is a bike renting web application. In order to have access to this web application system, users need to input their information into the registration form. Hence, if already registered, they can login instead. This web application registration page is developed using Hypertext Markup Language (HTML), Cascading Style Sheets (CSS) and Hypertext Preprocessor (PHP). This will allow users to register themselves with at least a user ID, email, password, name, UTHM Matric Number, IC number, and security phrase. Users will also need to retype the password to ensure the password's accuracy. Illustration 1.1 below shows the sign-up interface for the Rent-A-Bike web application.



Sign Up

ID:

Name:

Email: hello@gmail.com

IC Number: 010422050011

Matric Number:

Password:

Retype Password:

Security Phrase:

Already register? Login now.

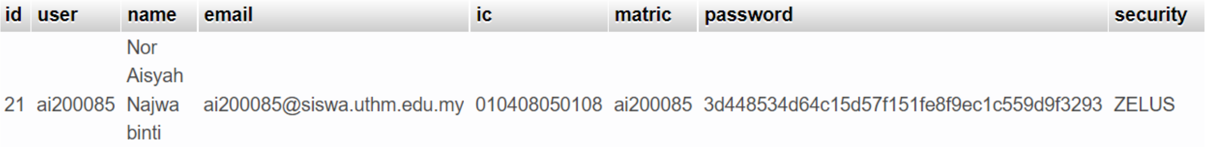
REGISTER

Illustration 1.1: Sign up page of Rent-A-Bike

1.2 Data Validation

Before accessing, importing, or otherwise processing data, it is necessary to validate it to ensure its validity and quality. Depending on the target restrictions or objectives, many methods of validation might be conducted. Validation is a type of data cleansing (Informatice, 2022). When migrating and merging data, it is critical to ensure that data from various sources and repositories conforms to business standards and does not become damaged owing to discrepancies in type or context. The objective is to generate data that is consistent, accurate, and full in order to avoid data loss and mistakes during a relocation. Data validation is an essential tool since it ensures that one can always rely on the datas they use to be correct, clean, and useful. Making certain that the data you use is correct is a proactive strategy to secure one of your most important, demand-generating assets (Adetiq, 2018).

We had done the whitelisting process for the web application. We have used our own group members data to test the data validation. Users will be whitelisted after they have undergone through a thorough sign-up data validation where the user's matric number must be the same as the user ID, password and retype password must be the same and since this is a university web application, users must use their student email. Illustration 1.2 below shows the data validation that user have to go through to register as a user.



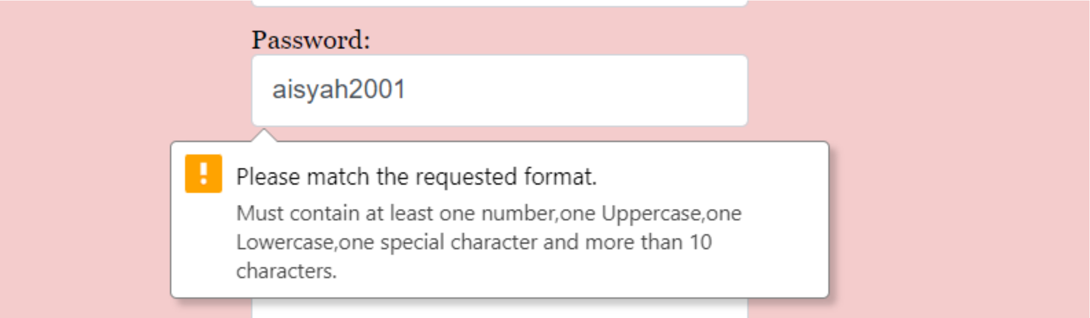
id	user	name	email	ic	matric	password	security
21	ai200085	Nor Aisyah Najwa binti	ai200085@siswa.uthm.edu.my	010408050108	ai200085	3d448534d64c15d57f151fe8f9ec1c559d9f3293	ZELUS

Illustration 1.2: Whitelist User

1.3 Password

A password is a string of characters that is used to validate a user's identity during the authentication process login to the web application system (Techtarget, 2022). Passwords are commonly used in conjunction with username, they are intended to be known only by the user and give that user access to Rent-A-Bike web application. A password is a basic application of challenge-response authentication that uses a vocal, written, or typed code to meet the challenge request. The sequence and diversity of characters in a password frequently influence its complexity or security strength.

As a result, security systems frequently require users to establish passwords that include at least one capital letter, number, and symbol. A password's specifics must be kept secret for it to be an effective security device. Otherwise, unauthorized people might obtain access to the data and securities that are being protected. In order to login to the Rent-A-Bike web application, passwords must be at a minimum of 10 characters in length and must include letters, numbers, and special characters such as “SUPLEXcity2001!”, “GigabitA3!4”, and “ArnabDond@1”. These standards are intended to assist users in creating strong passwords and using guidelines for handling login credentials. Illustration 1.3 below shows the password requirements that the user must input.



Password:

aisyah2001

Please match the requested format.

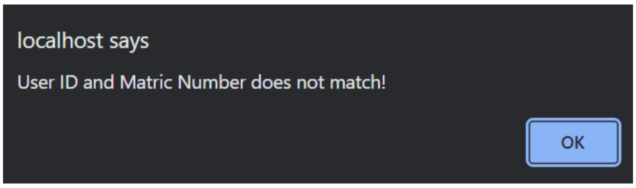
Must contain at least one number,one Uppercase,one Lowercase,one special character and more than 10 characters.

Illustration 1.3: Password Requirements

1.4 Error Message

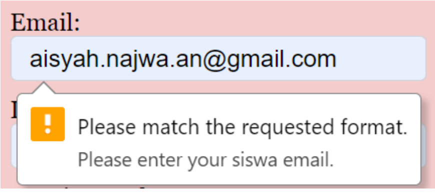
According to (Techopedia, 2022), When an unexpected event occurs, an operating system or application will display an error message to the user. In most circumstances, the operating system or programme will display error warnings via dialogue boxes. Error messages are essential when user intervention is required or when vital cautions must be given.

Error messages can be frustrating, users will make an error because it's unavoidable. If we ignore best practices of error messages, it will make the user upset in the process of accessing our web application system. Hence, it may trigger cortisol, well known as the primary stress hormone. Cortisol accumulation can lead users to give up on other processes. Thus, our web application will present an error message if the users have entered data that does not follow its specific requirements especially for user ID, email and password. Illustration below shows the error message that will pop up when the user input the wrong data.


localhost says

User ID and Matric Number does not match!

Illustration 1.4.1: User ID and Matric Number Mismatch

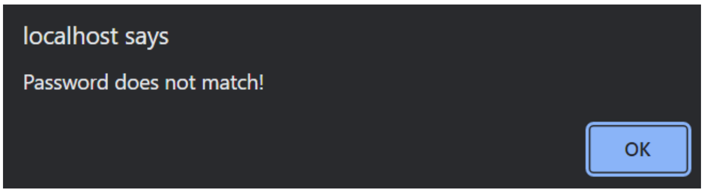

Email:

aisyah.najwa.an@gmail.com

Please match the requested format.

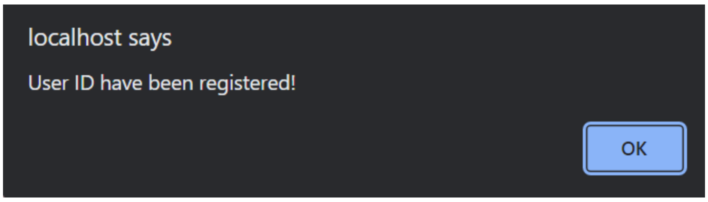
Please enter your siswa email.

Illustration 1.4.2: Wrong Email


localhost says

Password does not match!

Illustration 1.4.3: Password and Retype Password Mismatch


localhost says

User ID have been registered!

Illustration 1.4.4: User ID Taken

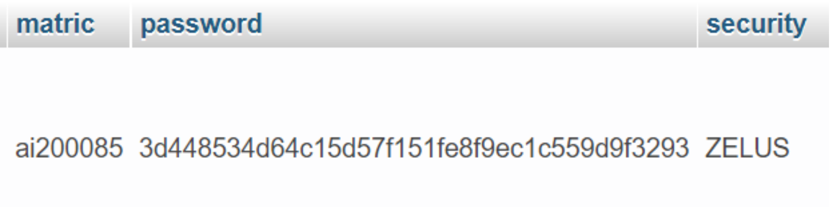
ACTIVITY 2: AUTHENTICATION

2.1 Salts

Salt is a piece of random data added to a password before it is hashed and stored. Salts are used to keep the password safe while being stored and it is randomly generated for each password in the database. It is used to prevent the plain text password entered by the users by converting the text into a code that cannot be read normally using hashing function.

A hash is a function that converts data into a string of numbers and letters. It is a one-way process, meaning that it cannot be de-hashed unlike encryption that is designed to be decrypted at some point. However, hash functions can be brute-forced and cracked. Meanwhile, salt is created to help the hash function to prevent it from being cracked. A salt is a method to improve a hash by making it more difficult to crack. It works by adding predefined data to the input such as password, making it harder and more likely impossible to crack.

In this project, we implemented salt authentication into passwords in order to prevent the plain text password being trace by the attacker if and only if the internal system is being hacked. By using X function in the coding, it will receive the password input by the user and convert it to a length of string that contains a combination of numbers, characters and special characters. The argument X is a constant that uses a X algorithm that is designed to change over time as new and stronger algorithms are added to PHP. After that, it will implement salt to make it harder to crack the password that has been hashed. Next, the password that has been salted is passed into the MySQL query to store in the database. Illustration 2.1 below shows passwords from registered users are hashed in the database.



matric	password	security
ai200085	3d448534d64c15d57f151fe8f9ec1c559d9f3293	ZELUS

Illustration 2.1: Password Hashed

2.2 Multifactor Authentication

Multi-factor authentication is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as application, online account and others. This type of authentication needs one or more verification factors as additional to a username and password inputs, which reduces the chances of a successful cyber-attack. There are many benefits of implementing multi-factor authentication as one of the cybersecurity methods. It will enhance the confidential information secure by requiring the users to identify themselves by more than a username and password. Since username and password are vulnerable to brute force attacks and can be stolen by third parties, enforcing the usage of multi-factor authentication such as insert PIN code increases its ability to protect against cyber attackers.

The implementation of hash function and “sha1” function that uses the US Secure Hash Algorithm 1 that will calculates the SHA-1 hash of a string is used to hash the password entered by the users. Other than that, an ‘I’m not a robot’ captcha is used to protect the web application from spam and abuse as captcha is a test to differentiate between bots and human. This will ensure safety from malicious software as it is not programmed to pass through a captcha verification. Illustration 2.2 below shows the interface used in sign-up webpage for captcha verification.

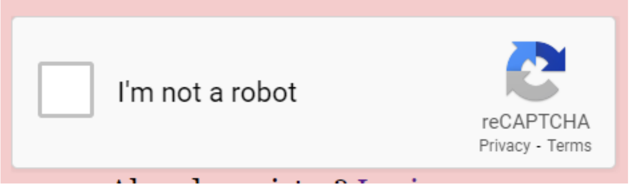
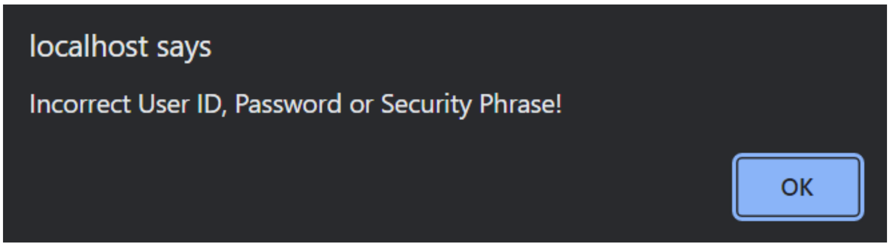


Illustration 2.2: Verification

2.3 Error Message

Authentication error message while registration is a form of ways to secure the account. Forms authentication allows us to authenticate users and maintain an authentication token in a cookie or in a page URL. In registration, an error message will be shown when the user input data that does not follow the requirements or when the email or user ID have been taken. Then, the Rent-A-Bike web application will have another error message when the user entered the wrong user ID, password and security phrase. Illustration 2.3 below shows the error message displayed when a user entered the wrong user ID, password or security phrase.



localhost says

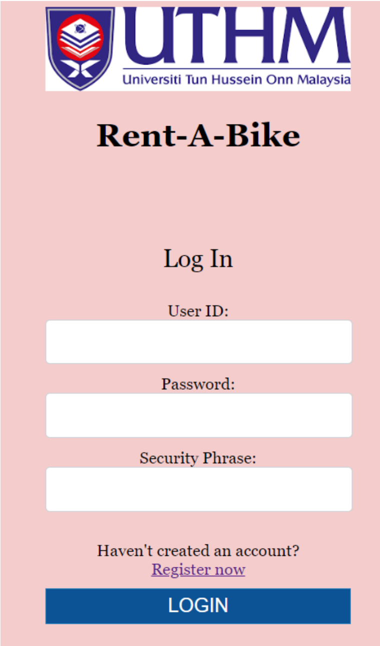
Incorrect User ID, Password or Security Phrase!

Illustration 2.3: Authenticate Error Message

ACTIVITY 3: PARAMETERIZED QUERY

Parameterized query is a SQL query that requires at least one parameter for the execution. Normally, placeholder is used for the parameter in the SQL query. Then, the parameter is passed to the query in a separate statement. Parameterized query is used to protect the database from SQL Injection attacks. Besides, it is used to make queries more readable. Generally, parameterized query is SQL query that is able to accept any parameter from the user. There are many advantages of using parameterized query. One of them is better performance. By applying parameterized query in SQL query, the time taken to get the result is only for retrieving the data in the database. It does not involve the time required for parsing, optimizing, and compiling for each value that is passed since the query is already parsed, optimized and compiled at the beginning.

After that, parameterized query can be used to prevent SQL Injection attack. It prevents the hackers from adding any malicious data into the query. Since all the values are parameterized, it accepts only defined length of data and defined type of data. Hence, it avoids the hackers from inserting any extra malicious data into the parameter value of the parameterized query. Due to all the processes that have been done, the user can easily login into the web application without the need to verify anything. Illustration 3.1 below shows the login interface that only requires the user to input their user ID, password and security phrase.



Rent-A-Bike

Log In

User ID:

Password:

Security Phrase:

Haven't created an account?
Register now

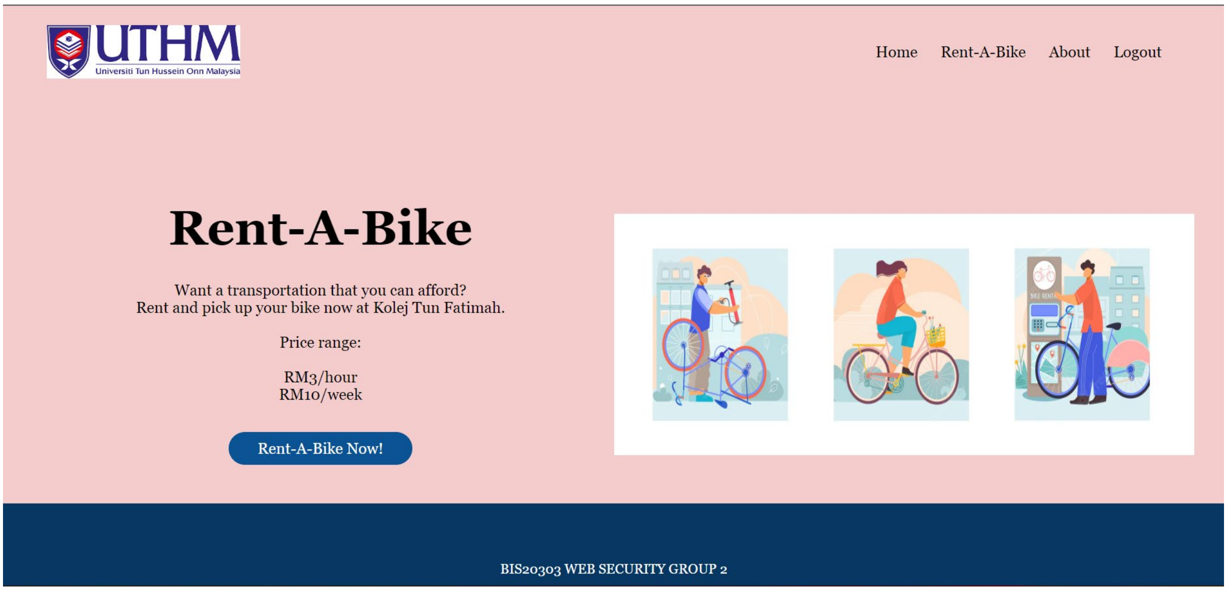
Illustration 3.1: Login Interface

ACTIVITY 4: LOGIN

This web application will only display the homepage, Rent-A-Bike web page and ‘About’ web page when the registration and login process is successful. At the very top of all the web pages consist of a navigation header where users can switch to different web pages easily. Below every web page is the footer that displays the copyright of the web application. Users can also logout of the web application by clicking the ‘Logout’ button at the header and it will redirect the user to the login web page.

4.1 Homepage

The homepage is where the information regarding the web application resides. Users can be redirected to the Rent-A-Bike web page by clicking on the button of ‘Rent-A-Bike Now!’. Illustration 4.1 below shows the homepage interface.



Rent-A-Bike

Want a transportation that you can afford?
Rent and pick up your bike now at Kolej Tun Fatimah.

Price range:

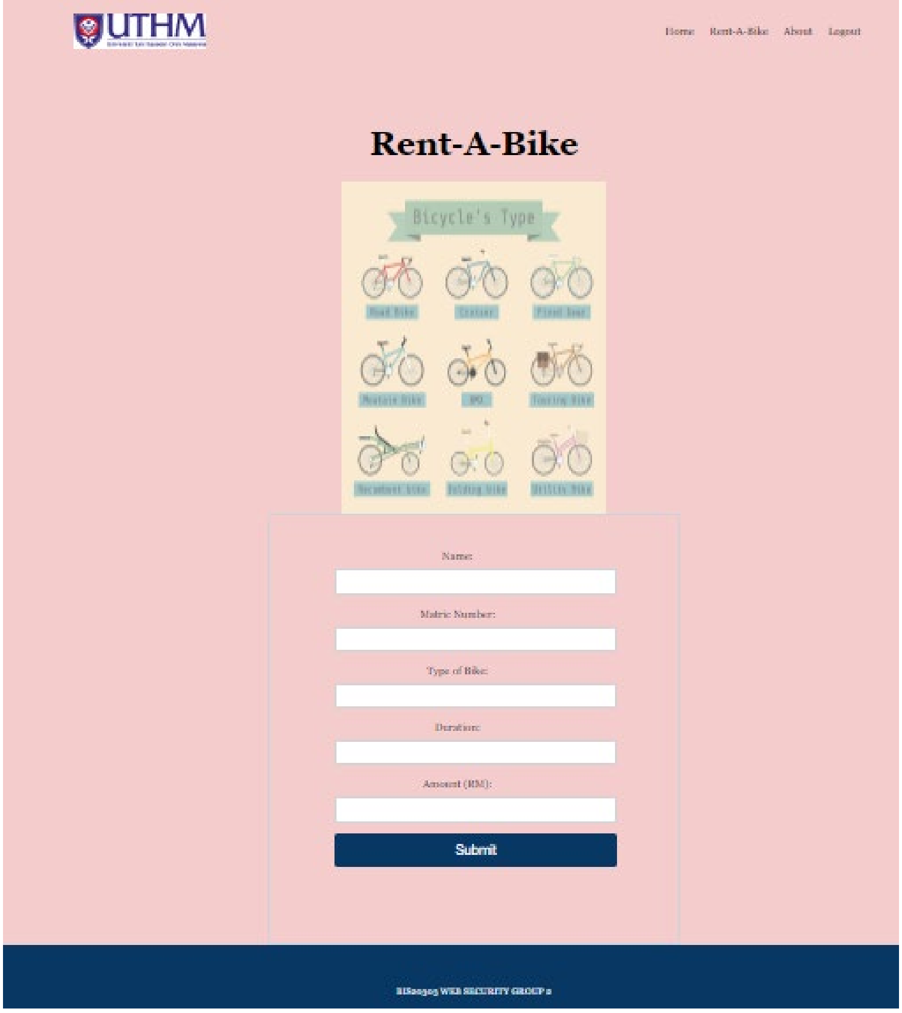
RM3/hour
RM10/week

BIS20303 WEB SECURITY GROUP 2

Illustration 4.1: Homepage Interface

4.2 Rent-A-Bike

For the Rent-A-Bike web page, it consists of a form where users can enter their info and rent the bike that they want. They can also pay the total renting price after calculating the amount of days or hours that they want to rent. Illustration 4.2 below shows the Rent-A-Bike interface.



Rent-A-Bike

Name:

Matric Number:

Type of Bike:

Duration:

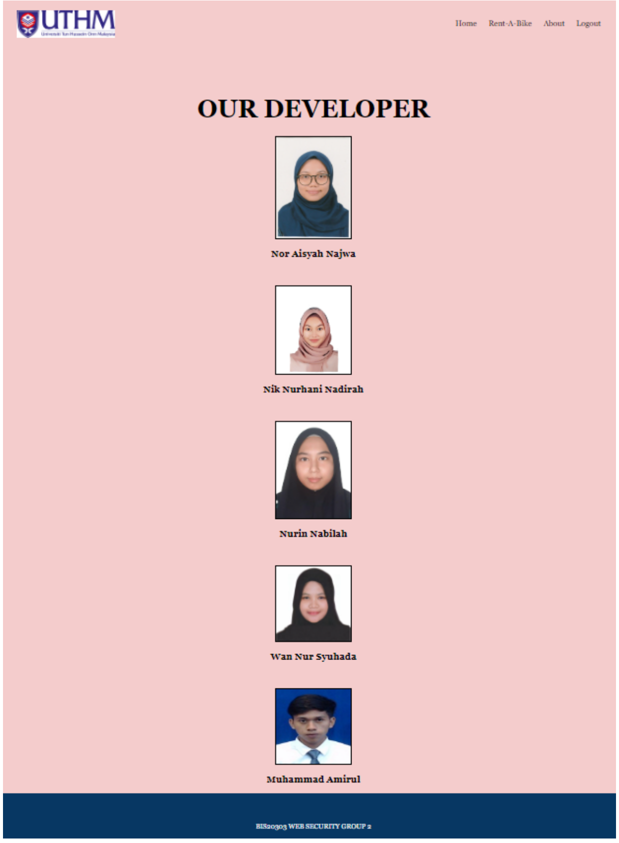
Amount (RM):

BIS20303 WEB SECURITY GROUP 2

Illustration 4.2: Rent-A-Bike Interface

4.3 About

The ‘About’ web page shows the developers that are involved in the creation of the Rent-A-Bike web application. Illustration 4.3 below shows the ‘About’ interface.



OUR DEVELOPER

Nor Aisyah Najwa

Nik Nurhani Nadirah

Nurin Nabilah

Wan Nur Syuhada

Muhammad Amirul

BIS20303 WEB SECURITY GROUP 2

Illustration 4.3: About Interface