FEDERAL UNIVERSITY OF TECHNOLOGY MINNA

DEPARTMENT OF CYBER SECURITY SCIENCE

CSS 418 - APPLICATION SECURITY

COURSE REGISTRATION AND PAYMENT WEB APP DOCUMENTATION

GROUP 4 – MEMBERS

ABDUSSAMAD AHMAD ABDULKADIR	**–**	**2019/1/75057CS**
AJAGBE PAMILERIN OLUWASOLA	**–**	**2019/1/75081CS**
ONWUKA SUSAN KELECHI	**–**	**2019/1/77014CS**
ABDULLATIF MUHAMMAD IDRIS	**–**	**2021/2/8020CS**
DANIEL ELIJAH	**–**	**2021/2/80012CS**

Course Lecturers: Mr Peter Anyaora and Mrs Emily

PROJECT OVERVIEW

This document outlines the functionalities and technical aspects of a web application designed to streamline the course registration and payment process for students. This secure and user-friendly application aims to improve efficiency and convenience for both students and administrators.

FEATURES

The core functionalities of the web app include:

Strong Authentication Login: Students must log in using a secure method before accessing course registration features.
Student Level Selection: Students choose their academic level (e.g., freshman, sophomore) before proceeding.
Fixed School Fee Display: The application displays the fixed school fee amount, which cannot be modified.
Course Registration: Students can search, browse, and register for offered courses.
Payment Processing: Students securely pay the fixed school fee using a variety of online payment methods.
Biodata and Profile Picture Upload: Students can upload their profile picture and fill out a biodata form (optional).
User Management: Students can view their registration details and payment history.

SYSTEM ARCHITECTURE

The web application will utilize a three-tier architecture:
Presentation Layer (Frontend): This layer consists of the user interface elements that students interact with.
Business Logic Layer (Backend): This layer handles the core functionalities of the application, including user authentication, level selection, course registration management, payment processing, and student data manipulation. We used JavaScript with a framework, ExpressJS.
Data Layer (Database): This layer stores all application data, such as student accounts, course information, registrations, payments, and biodata (optional).

FUNCTIONAL SPECIFICATIONS

1. Strong Authentication Login

Upon accessing the application, students are directed to a login page.

Students must enter a valid username or email address and a strong password to log in.

2. Biodata and Profile Picture Upload

Students can upload a profile picture to personalize their account.

The system provides a user-friendly interface for uploading the picture.

Students can also fill out a biodata form with additional information

students select their academic level from a dropdown menu or similar interface element.

Selecting the level is mandatory before proceeding to course registration or payment.

The level selection could trigger the display of relevant course offerings based on the student's program.

This information can be stored securely in the database.

3. School Fee Payment

The application displays the fixed school fee amount prominently on the registration page or throughout the process. This amount cannot be modified by students.

Students are directed to a secure payment gatew, a third-party payment gateway service, REMITTA was used, for processing payments securely.

Students can choose their preferred payment method (e.g., credit card, debit card, e-wallet) and complete the transaction.

The system verifies payment and updates student registration status upon successful completion.

4. Course Registration

After a successfully school fees payment, Students can search and browse offered courses based on their chosen level.

The system displays detailed information about each course (description, instructor, schedule, etc.).

Students can add and remove courses from their registration cart before finalizing their selection.

5. User Management

Students can access a dedicated section displaying their registered courses, payment status, and biodata, where can they print. (if applicable).

THREAT MODELLING AND SECURITY FEATURES

1. **HTTPS Encryption**: We Implemented HTTPS protocol to encrypt data transmitted between the web server and the client's browser, ensuring that sensitive information such as login credentials, payment details, and personal data are encrypted during transit.
2. **Authentication and Authorization**: We ensured strong authentication mechanisms, such as username/password authentication, multi-factor authentication (MFA), to verify the identity of users before granting access to the application. Additionally, we enforced proper authorization controls to restrict access to specific functionalities or data based on user roles and permissions.
3. **Secure User Sessions**: We Implemented secure session management techniques, session tokens with short expiration times, secure cookies, and anti-CSRF (Cross-Site Request Forgery) tokens, to prevent session hijacking and unauthorized access to user sessions.
4. **Input Validation and Sanitization**: It Validates and sanitizes all user input, including form submissions and file uploads, to prevent common security vulnerabilities such as SQL injection, XSS (Cross-Site Scripting), and file inclusion attacks. Use server-side validation and client-side validation to ensure data integrity and prevent malicious input.
5. **Secure File Uploads**: We Implemented strict file upload validation and enforce file type restrictions, file size limits, and malware scanning to prevent malicious file uploads and protect against file-based attacks such as malware injection and remote code execution.
6. **Secure Password Storage**: It hashes and salts user passwords using strong cryptographic hashing algorithms, to securely store passwords in the database. Avoid storing plain text passwords or using weak hashing algorithms that are susceptible to brute-force attacks.