GROUP 2

APPLICATION SECURITY STANDPOINT

GROUP MEMBERS

Names	Matric No.
Beloved Adejuyigbe	2019/1/76747CS
Gloria Omojo Ode	2019/1/76083CS
Chikwendu Somtochukwu Chinedu	2019/1/75373CS
Sadiq Divinefavour Oyiza	2019/1/76407CS
Pascal Chigozie Ejiofor	2019/1/75464CS

SECURITY POLICY

Access Control Policy

We implemented a security system that regulates who can access or use resources or services, ensuring only authorized individuals or entities have permission.

User Guide:

- Only authorized users with valid credentials are allowed to access the system.
- Users must authenticate themselves using a combination of email, password, student ID, security question, and security answer.

Authentication Policy

We developed a system that confirms the identity of a user, the credentials used are stated in the user guide.

User Guide:

- Users must provide valid credentials (email, password, student ID, security question, and security answer) to authenticate themselves.
- Passwords must meet minimum complexity requirements (e.g., minimum length, combination of letters, numbers, and special characters).

Threat Modelling

Unauthorized Access

Threat: Attackers may attempt to gain unauthorized access to the system by guessing or brute-forcing user credentials.

Mitigation: We are going to Implement account lockout mechanisms after multiple failed logins attempts to prevent brute-force attacks. We will enforce strong password policies to reduce the risk of password guessing.

Injection Attacks

Threat: Attackers may attempt to exploit injection vulnerabilities to execute malicious code or SQL injection attacks.

Mitigation: We will sanitize and validate user input to prevent injection attacks as we use parameterized queries or prepared statements to avoid SQL injection vulnerabilities.

Session Hijacking

Threat: Attackers may attempt to hijack user sessions to gain unauthorized access to the system.

Mitigation: We are going to implement secure session management techniques such as using HTTPS for communication, generating secure session identifiers, and implementing session expiration and re-authentication mechanisms.

Information Leakage

Threat: Improper error handling may expose sensitive information such as usernames, passwords, or database details to attackers.

Mitigation: We will implement secure error handling mechanisms to provide generic error messages to users without revealing sensitive information as we avoid displaying detailed error messages that could aid attackers in exploiting vulnerabilities.

Insider Threats

Threat: Insiders with malicious intent may abuse their privileges to access or manipulate sensitive data.

Mitigation: We will implement least privilege principles to restrict access to sensitive resources by monitoring user activities and access logs regularly for suspicious behaviour and I will ensure I conduct background checks and enforce security awareness training for employees.

Cross-Site Scripting (XSS)

Threat: Attackers may inject malicious scripts into the application, which can be executed in users' browsers.

Mitigation: We will implement input validation and output encoding to prevent XSS attacks and use Content Security Policy (CSP) to mitigate the impact of XSS vulnerabilities.

Insecure Direct Object References (IDOR)

Threat: Attackers may manipulate object references in the application to access unauthorized data or perform unauthorized actions.

Mitigation: We will implement access controls and authorization checks to prevent IDOR vulnerabilities as we use indirect references instead of direct database identifiers to access resources.

Lack of Transport Layer Security (TLS)

Threat: Attackers may intercept sensitive data transmitted over insecure channels, leading to data exposure or eavesdropping.

Mitigation: We will use HTTPS to encrypt data transmitted between the client and server as we implement TLS protocols and ensure proper certificate management to establish secure communication channels.