Group Members:

Athanase Abayo

Mabinty Mambu

Olivier Kwizera

Victoria Ama Nyonator

Course Name: Web Technologies

Cohort B

OWASP Top 10 (2021): Executive Summary

Lecturer: Dr. Osafo-Maafo Kwadwo

Teacher Assistant: Barbara-Marie Doh

November 30, 2025

OWASP Top 10 (2021): Executive Summary

We built SwapIt with security at the center, following the OWASP Top 10 standards. Below is a lean, clear summary of the major controls we implemented and how we keep the system secure.

1. Broken Access Control

   We made sure users only see what belongs to them.

   We use session-based authentication, IP tracking, strict login requirements, and user-data isolation.

2. Cryptographic Failures

   We protect sensitive data using bcrypt hashing, secure cookies, and zero plaintext password storage.

3. Injection Prevention

   We prevent SQL injection and XSS by using prepared statements, validating inputs, and escaping all outputs on both client and server.

4. Insecure Design

   We designed SwapIt with safe defaults: login attempt limits, account lockouts, password rules, and 24-hour session expiry.

5. Security Misconfiguration

   We hardened the system with strong security headers, strict session settings, clean error messages, and consistent UTF-8 encoding.

6. Vulnerable & Outdated Components

   We still update external libraries manually.

   We plan to add automated audits, version locking, and a monthly maintenance workflow.

7. Identification & Authentication Failures

   We strengthened authentication with strong email checks, password rules, rate limiting, and IP-based suspicious activity detection.

8. Software & Data Integrity Failures

We secure file uploads with MIME validation, image integrity checks, type restrictions, and a 5MB size limit.

9. Security Logging & Monitoring

We log all major security actions: logins, updates, lockouts, file uploads, suspicious activity, and track IP, time, and user IDs for auditing.

10. SSRF

Not applicable because SwapIt does not fetch external URLs from user input.

We can add allowlists and IP blocking if needed later.

Security Testing Checklist

We test rate limits, session expiry, XSS/SQL injection, file upload protection, logging accuracy, password strength, and IP tracking before deployment.

Production Recommendations

We use environment variables, enforce HTTPS, rotate logs daily, and apply strict file permissions.