**BÁO CÁO**

**THỰC NGHIỆM KHAI THÁC CÁC LỖI BẢO MẬT THEO OWASP**

Họ tên người thực hiện: Nguyễn Phan Ngọc Minh

Ngày thực hiện: 22/11/2023

1. **Tổng quan**
   1. *Mục tiêu*

Mục tiêu của thực nghiệm là kiểm tra và phát hiện các lỗ hổng bảo mật trong các bài tập lập trình web từ W04 đến W06, dựa trên các nguyên tắc và hướng dẫn từ OWASP. Đảm bảo rằng mọi khía cạnh của ứng dụng đều được kiểm tra, từ xử lý dữ liệu người dùng đến quản lý phiên làm việc và cấu hình an toàn.

* 1. *Phạm vi*

Phạm vi của thử nghiệm bao gồm các bài tập lập trình web từ W04 đến W06.

1. **Đánh giá**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lỗi Bài** | **W04** | **W05** | **W06** |
| Broken Access Control | Không kiểm soát quyền truy cập của người dùng, chưa phân quyền, bất kỳ ai cũng có thể truy cập và thêm hàng hóa  **Biện pháp:** Thêm chức năng đăng nhập, đăng ký và phân quyền người dùng | Không kiểm soát quyền truy cập của người dùng, chưa phân quyền, bất kỳ ai cũng có thể truy cập và thêm, sửa, xóa hàng hóa  **Biện pháp:** Thêm chức năng đăng nhập, đăng ký và phân quyền người dùng | Không kiểm soát quyền truy cập của người dùng, chưa phân quyền, bất kỳ ai cũng có thể truy cập và thêm, sửa, xóa hàng hóa  **Biện pháp:** Thêm chức năng đăng nhập, đăng ký và phân quyền người dùng |
| Cryptographic Failures | Không sử dụng các thuật toán mã hóa dữ liệu nhập từ web về database  **Biện pháp:** Sử dụng các thuật toán mã hóa mạnh và an toàn để ngăn chặn rò rỉ dữ liệu nhạy cảm | Không sử dụng các thuật toán mã hóa dữ liệu nhập từ web về database  **Biện pháp:** Sử dụng các thuật toán mã hóa mạnh và an toàn để ngăn chặn rò rỉ dữ liệu nhạy cảm | Không sử dụng các thuật toán mã hóa dữ liệu nhập từ web về database  **Biện pháp:** Sử dụng các thuật toán mã hóa mạnh và an toàn để ngăn chặn rò rỉ dữ liệu nhạy cảm |
| Injection |  |  |  |
| Insecure Design |  |  |  |
| Security Misconfiguration |  |  |  |
| Vulnerable and Outdated Components |  |  |  |
| Identification and Authentication Failures |  |  |  |
| Software and Data Integrity Failures |  |  |  |
| Security Logging and Monitoring Failures |  |  |  |
| Server-Side Request Forgery |  |  |  |

<https://owasp.org/www-project-top-ten/>