**HƯỚNG DẪN LÀM PROJECT CUỐI KỲ MÔN BẢO MẬT WEB**

# Danh sách đề tài gợi ý:

1. Bảo mật hệ thống Website bán điện thoại
2. Bảo mật hệ thống Website tin tức
3. Bảo mật hệ thống Website thi trắc nghiệm
4. Bảo mật hệ thống Website bán đồ thời trang
5. Bảo mật hệ thống Website bán giày
6. Bảo mật hệ thống Website bán hải sàn
7. Bảo mật hệ thống Website bán hàng nội thất
8. Bảo mật hệ thống Website bán đồng hồ
9. Bảo mật hệ thống Website bán giày
10. Bảo mật hệ thống Website bán thức ăn nhanh
11. SV đề xuất

# Yêu cầu:

* Các nhóm (2 – 3 SV) chọn một Web project đã hoàn chỉnh, tấn công vào hệ thống này để phát hiện các lỗ hổng bảo mật và thực hiện các biện pháp vá lỗi, phòng chống.
* Việc tấn công vào hệ thống được thực hiện theo 02 phương pháp:

1. Manual

* Dùng các kỹ thuật tấn công Web đã được học để áp dụng trên hệ thống.

1. Tools

* SQL Map, ZAP, WebScarab, SV tự tìm một số tool (keyword: công cụ tấn công hệ thống Web tự động, Web Attack Tool…).
* Các nhóm liệt kê những lỗ hổng bảo mật tồn tại trong hệ thống của mình. Tìm cách khắc phục (sửa code), nếu không sửa được phải giải thích lý do (VD: phải thay đổi lại thiết kế chương trình mới tránh được lỗ hổng đó…). Nếu hệ thống không mắc phải những lỗi thông dụng phải giải thích lý do (đã dùng các công nghệ, framework, thư viện nâng cao nào mà tránh được các lỗ hổng đó).
* Yêu cầu nộp:

1. 02 Project (trước và sau khi sửa lỗi)
2. Database
3. File .docx mô tả đề tài
   1. Danh sách thành viên – phân chia công việc
   2. **Giới thiệu đề tài**
   3. Lược đồ Use – Case
   4. Lược đồ ERD

* **Lưu ý:**
* **Nhóm phải chia đều công việc. Tất cả thành viên phải tham gia phân tích lỗ hổng, tiến hành các giải pháp khắc phục… chứ không đơn thuần là kiếm tài liệu, làm file báo cáo…**