

HỌC VIỆN KỸ THUẬT MẬT MÃ

**KHOA AN TOÀN THÔNG TIN**



BÁO CÁO BÀI TẬP LỚN

**CHUYÊN ĐỀ AN TOÀN THÔNG TIN**

**Đề tài:**

**XÂY DỰNG BÀI TẬP THỰC HÀNH THU THẬP THÔNG TIN, DÒ QUÉT LỖ HỔNG**

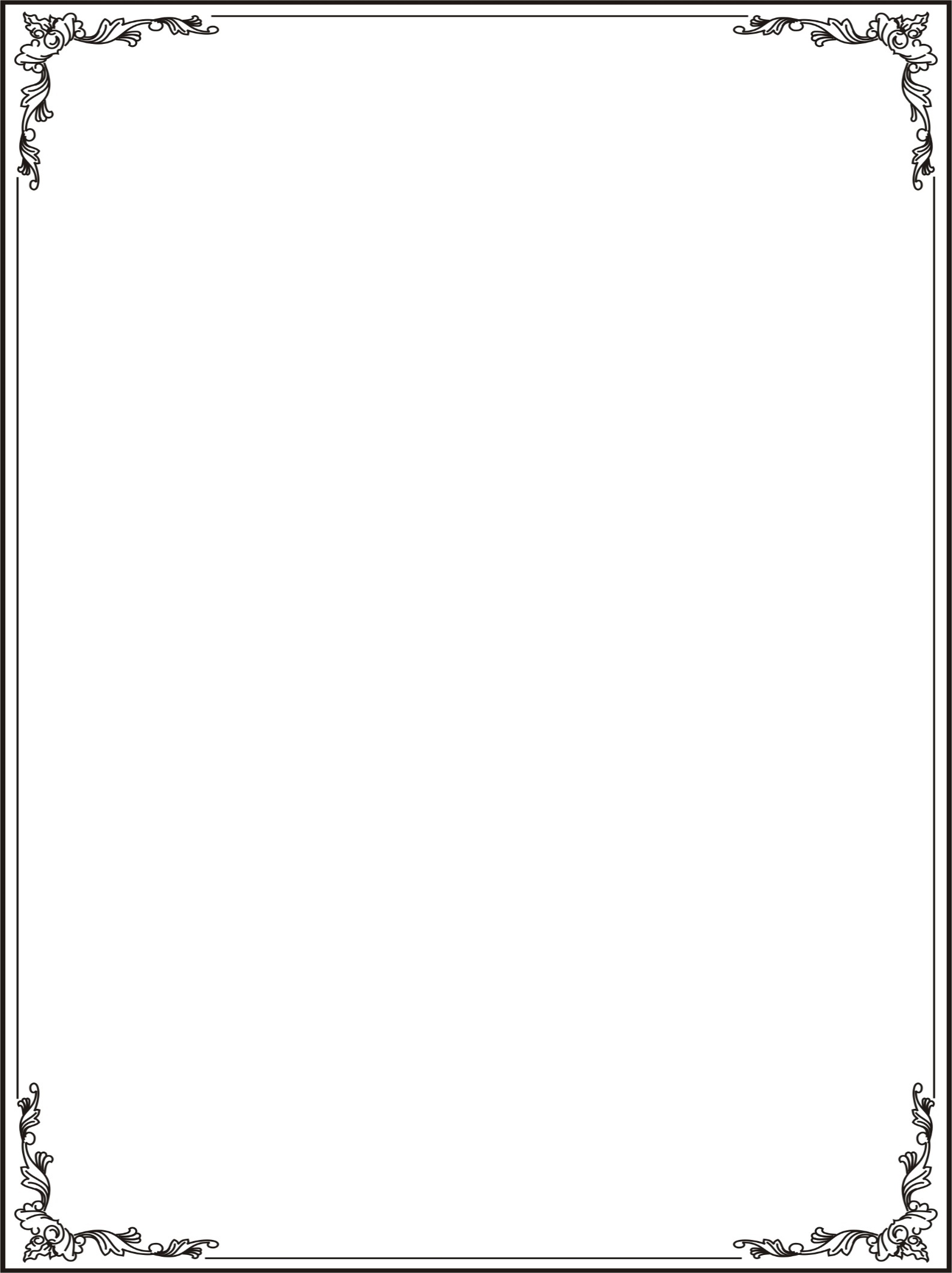
***Nhóm sinh viên thực hiện:*** Vũ Tiến Đạt AT170609

Nguyễn Minh Trang AT170350

Nhóm

***Giảng viên hướng dẫn****:* ThS. Đồng Thị Thùy Linh

Hà Nội, -2023



HỌC VIỆN KỸ THUẬT MẬT MÃ

**KHOA AN TOÀN THÔNG TIN**



BÁO CÁO BÀI TẬP LỚN

**CHUYÊN ĐỀ AN TOÀN THÔNG TIN**

**Đề tài:**

**XÂY DỰNG BÀI TẬP THỰC HÀNH THU THẬP THÔNG TIN, DÒ QUÉT LỖ HỔNG**

***Nhóm sinh viên thực hiện:*** Vũ Tiến Đạt AT170609

Nguyễn Minh Trang AT170350

Nhóm

***Giảng viên hướng dẫn****:* ThS. Đồng Thị Thùy Linh

Hà Nội, 2023

# MỤC LỤC

# LỜI CẢM ƠN

Nhóm chúng em xin gửi lời cảm ơn chân thành tới cô giáo trong Khoa Công nghệ thông tin đã tạo điều kiện thuận lợi cho nhóm em trong quá trình thực hiện đề tài.

Chúng em xin gửi lời cảm ơn đặc biệt đến Thạc sĩ cô: Đồng Thị Thùy Linh đã nhiệt tình hướng dẫn và chỉ bảo nhóm trong suốt thời gian thực hiện để tài, giúp chúng em có thể hoàn thành tốt đề tài chuyên đề cơ sở lần này.

|  |  |
| --- | --- |
| **GIẢNG VIÊN HƯỚNG DẪN** | **NHÓM SINH VIÊN THỰC HIỆN** |
|  | Vũ Tiến Đạt |
| ThS. Đồng Thị Thùy Linh | Nguyễn Minh Trang |

# LỜI MỞ ĐẦU

**1. Tính cấp thiết của đề tài.**

**2. Mục tiêu nghiên cứu của đề tài**

Nghiên cứu dò quét lỗ hổng website.

**3. Đối tượng và phạm vi nghiên cứu**

Đối tượng: các ứng dụng web hoặc trang web

Phạm vi: Nghiên cứu các phương pháp, công cụ và kỹ thuật để thiết kế, triển khai và thực thi các kịch bản thu thập thông tin, dò quét lỗ hổng.

**4. Các nhiệm vụ chính cần thực hiện**

Nội dung nghiên cứu được tập trung vào các nội dung chính như sau:

- Khảo sát, tổng hợp kiến thức nền tảng về website

- Thiết kế và triển khai các kịch bản

- Thực thi các kịch bản

- Đánh giá và báo cáo kết quả

- Cài đặt, thử nghiệm, đánh giá

**5. Kết quả dự kiến**

**Lý thuyết:**

- Tổng quan về một số lỗ hổng Web:

**Thực nghiệm:**

- Áp dụng kiến thức đã tìm hiểu để kiểm thử chức năng của ứng dụng Web.

- Viết script để kiểm thử tự động chức năng cơ bản của ứng dụng Web.

- Tấn công path traversal; SQLi và XSS

# TỔNG QUAN VỀ THU THẬP THÔNG TIN VÀ DÒ QUÉT LỖ HỔNG

## Tổng quan về thu thập thông tin

### Khái niệm

### Phân loại

### Mục tiêu

### Vai trò

### Các kỹ thuật

## Tổng quan về dò quét lỗ hổng

### Khái niệm

### Phân loại

### Mục tiêu

### Vai trò

### Các kỹ thuật

### Quy trình

# DÒ QUÉT LỖ HỔNG WEBSITE

## TỔNG QUAN VỀ DÒ QUÉT LỖ HỔNG WEBSITE

### Khái niệm

### Quy trình

### Các công cụ dò quét phổ biến

### Ưu điểm và nhược điểm

## Top 10 lỗ hổng website

# THỰC NGHIỆM