3.2. Data Collection Methods

Phương pháp thu thập dữ liệu được xây dựng theo hướng kết hợp lý thuyết và thực nghiệm để đảm bảo thu thập đầy đủ và chính xác thông tin cần thiết. Dưới đây là các bước chi tiết trong quy trình thu thập dữ liệu:

3.2.1. Phân tích lý thuyết

- **Mục tiêu:** Tìm hiểu và xây dựng cơ sở lý luận cho nghiên cứu, đảm bảo rằng mọi phương pháp và công cụ được sử dụng đều có căn cứ khoa học rõ ràng.
- **Nguồn dữ liệu:**
    - Các tài liệu học thuật từ cơ sở dữ liệu khoa học (Google Scholar, IEEE Xplore).
    - Tài liệu chính thức từ tổ chức OWASP, nơi cung cấp các tiêu chuẩn và hướng dẫn bảo mật ứng dụng web.
    - Các bài báo, sách tham khảo và báo cáo về các công cụ kiểm thử bảo mật như OWASP ZAP, Burp Suite, và Nikto.
- **Phương pháp thu thập:**
    - Lọc và chọn lọc các tài liệu liên quan đến bảo mật ứng dụng web, kiểm thử xâm nhập (penetration testing), và đánh giá lỗ hổng (vulnerability assessment).
    - Đọc hiểu nội dung để trích xuất các tiêu chuẩn kiểm thử và phương pháp tốt nhất áp dụng cho nghiên cứu.

3.2.2. Thực nghiệm

- **Mục tiêu:** Tạo ra một môi trường kiểm thử an toàn để thực hiện các thử nghiệm và thu thập dữ liệu thực tế từ các công cụ kiểm thử bảo mật.
- **Quy trình thực hiện:**
    - **Thiết lập môi trường:**
        - Triển khai các công cụ kiểm thử trên hệ thống ảo hóa để đảm bảo an toàn và kiểm soát.
        - Cấu hình các ứng dụng mục tiêu (DVWA, WordPress) với các lỗ hổng phổ biến để phục vụ kiểm thử.
    - **Kiểm thử lỗ hổng:**
        - Sử dụng các công cụ kiểm thử bảo mật để quét và khai thác các lỗ hổng tiềm ẩn.

        - Thực hiện kiểm thử theo quy trình chuẩn (thu thập thông tin, kiểm tra lỗ hổng, khai thác thử nghiệm).
    - **Thu thập thông tin:**
        - Ghi nhận tất cả các dữ liệu từ công cụ kiểm thử, bao gồm log chi tiết, báo cáo kết quả, và phản hồi từ các ứng dụng mục tiêu.

3.2.3. Thu thập dữ liệu kiểm thử

- **Mục tiêu:** Đảm bảo rằng tất cả thông tin từ các thử nghiệm được lưu trữ và tổ chức một cách có hệ thống để phục vụ phân tích.
- **Phương pháp thu thập:**
    - Sử dụng chức năng xuất báo cáo (export reports) từ các công cụ kiểm thử.
    - Ghi nhận thủ công các dữ liệu quan trọng không được công cụ tự động lưu trữ.
    - Tích hợp và tổ chức dữ liệu trong các bảng tính hoặc phần mềm quản lý dữ liệu.
- **Nội dung dữ liệu:**
    - Kết quả phát hiện lỗ hổng, bao gồm loại lỗ hổng, vị trí, và mức độ nghiêm trọng.
    - Tỷ lệ lỗi giả (false positive) và lỗi sót (false negative).
    - Thời gian và tài nguyên cần thiết để hoàn thành kiểm thử.

3.2.4. Phân tích kết quả

- **Mục tiêu:** Chuyển đổi dữ liệu thu thập được thành thông tin có giá trị, phục vụ đánh giá hiệu quả của các công cụ và phương pháp kiểm thử.
- **Phương pháp phân tích:**
    - Tập hợp dữ liệu từ các nguồn khác nhau và tổ chức thành bảng biểu hoặc biểu đồ.
    - So sánh kết quả giữa các công cụ kiểm thử để xác định hiệu quả và tính nhất quán.
    - Xác định các ưu điểm và hạn chế của từng công cụ hoặc phương pháp kiểm thử.
- **Tiêu chí đánh giá:**
    - Độ chính xác của công cụ (tỷ lệ phát hiện lỗ hổng chính xác).
    - Khả năng phát hiện nhiều loại lỗ hổng (SQL Injection, XSS, CSRF,...).
    - Độ dễ sử dụng và khả năng áp dụng thực tế của công cụ.

3.2.5. Công cụ và tài nguyên hỗ trợ

- **Mục tiêu:** Sử dụng các công cụ hỗ trợ để lưu trữ, tổ chức và trình bày dữ liệu một cách rõ ràng, dễ hiểu.
- **Công cụ sử dụng:**
    - **Phần mềm kiểm thử:** OWASP ZAP, Burp Suite, Nikto.
    - **Phần mềm xử lý dữ liệu:** Microsoft Excel/Google Sheets để lưu trữ và phân tích dữ liệu thử nghiệm.
    - **Phần mềm soạn thảo:** Microsoft Word/LaTeX để viết báo cáo và trình bày kết quả.
    - **Hệ thống ảo hóa:** VMware Workstation Pro để triển khai các ứng dụng mục tiêu và công cụ kiểm thử trong môi trường an toàn.