TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

PROJECT 2

Phát triển công cụ phát hiện lỗ hổng SQL Injection

Sinh viên : Phan Thế Toàn - 20225415
GVHD : TS. Trần Quang Đức
Trần Đình Kiến Giang

MỤC LỤC

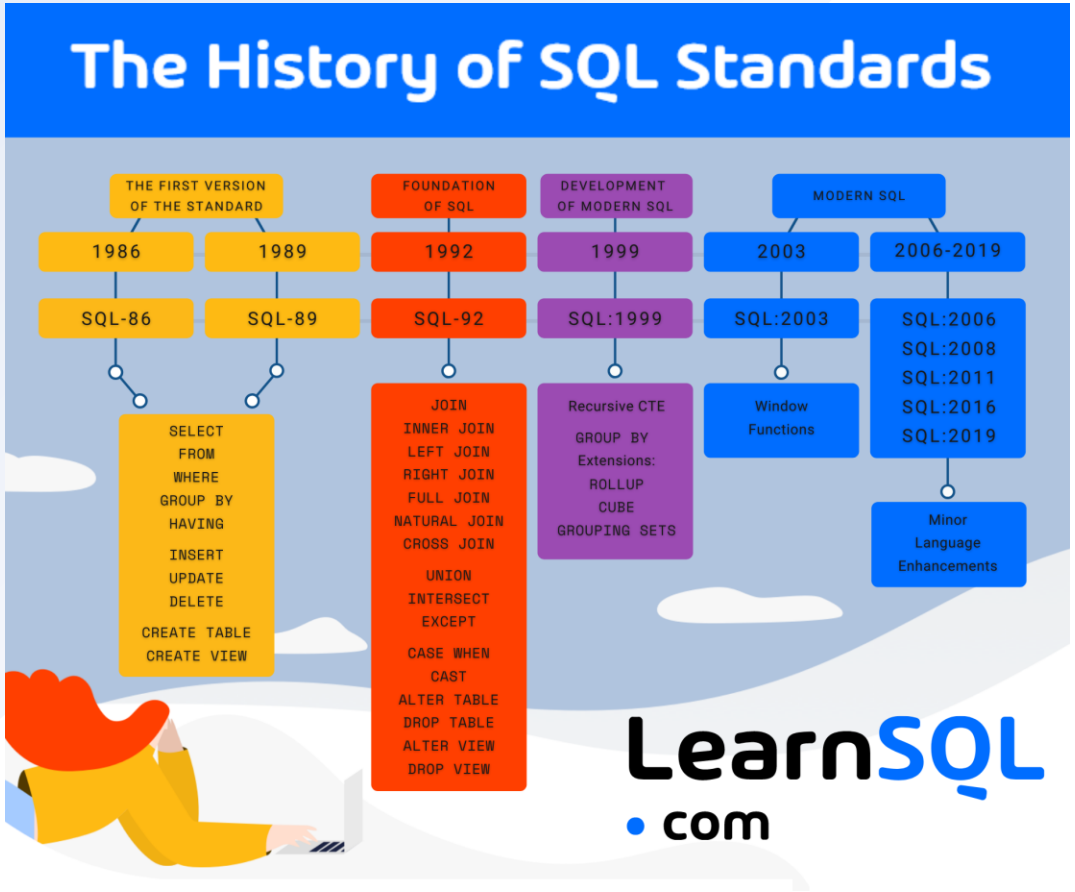
MỤC LỤC

SQL Injection

Tổng quan SQL

SQL hay Structured Query Language là ngôn ngữ được dùng để giao tiếp với database.

Trong quá khứ, để chuẩn hóa lại cú pháp của SQL, Viện Tiêu chuẩn Quốc gia Hoa Kỳ(ANSI) đã lựa chọn SQL-86 của IBM, mà hai nhà khoa học là Donald Chamberlin và Raymond Boyce đã công bố. SQL hiện nay đã phát triển dựa trên nền tảng này



Lịch sử phát triển của SQL Standards
(Nguồn: The History of SQL Standards | LearnSQL.com)

SQL Injection

Untrusted Data

SELECT * FROM users WHERE username = ‘conmeo’ AND password = ‘meow’

Có cách nào để mệnh đề WHERE có kết quả **TRUE** không?
Để làm gì? Vì Logic chương trình sẽ dựa vào điều kiện WHERE để quyết định có cho user này thực hiện đăng nhập thành công hay không!

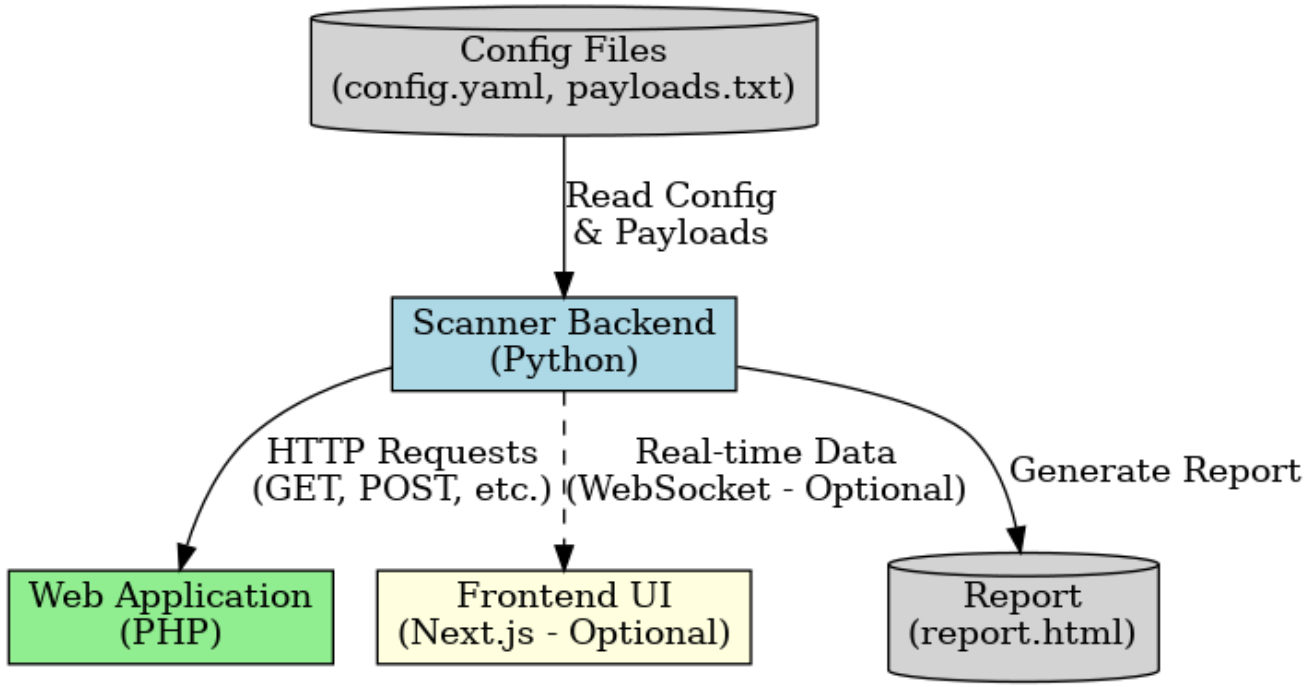
Nếu nhập input với ***username = conmeo’ OR ‘1’=‘1’ --***

MỤC LỤC

Phân tích & Thiết kế

Các yêu cầu chức năng

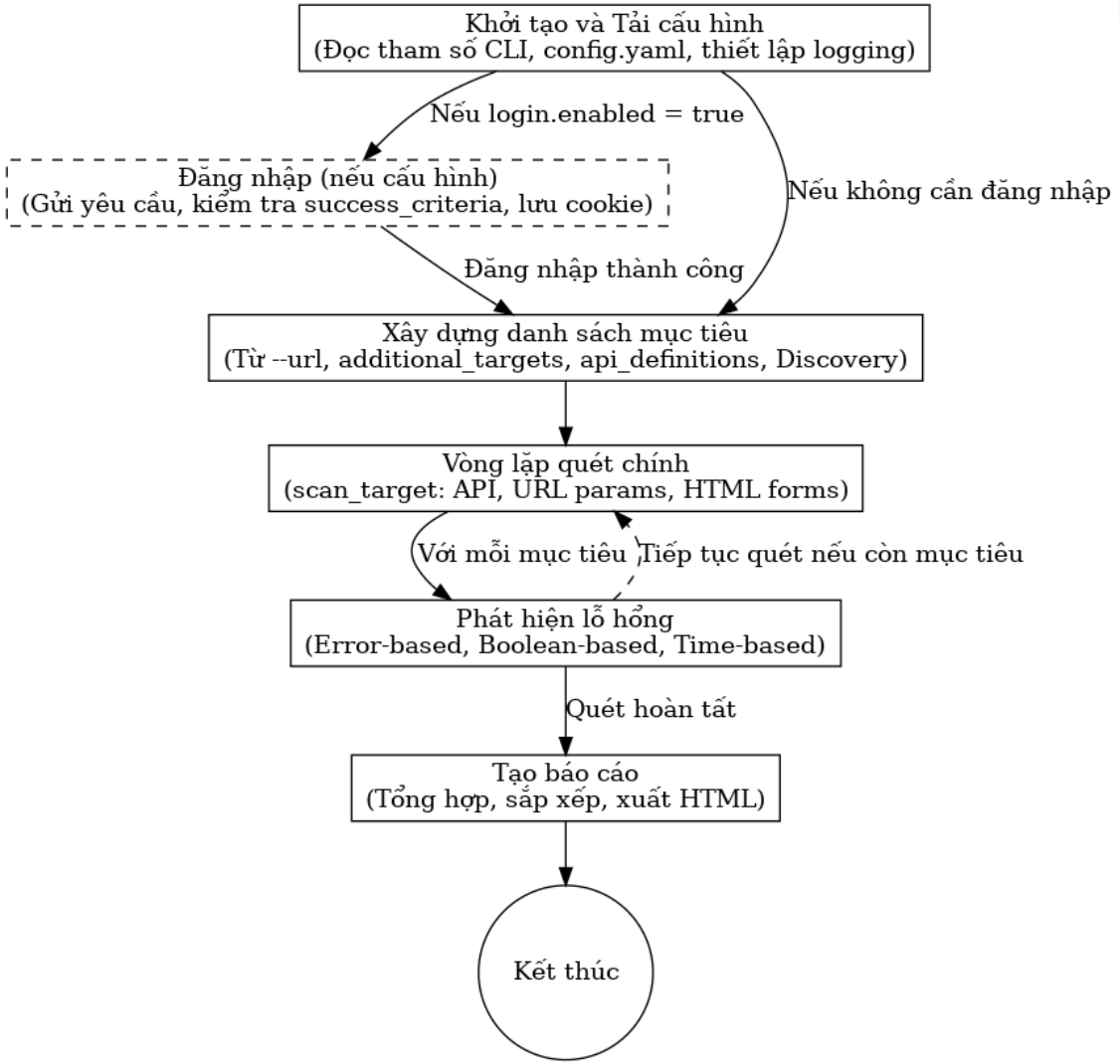
- Thu thập dữ liệu đầu vào và cấu hình
- Phân tích và Trích xuất mục tiêu
- Tạo và chèn Payload
- Gửi yêu cầu HTTP
- Khám phá đường dẫn/tệp tiềm năng
- Xử lý đăng nhập tự động
- Tạo báo cáo lỗ hổng



Tổng quan kiến trúc hệ thống

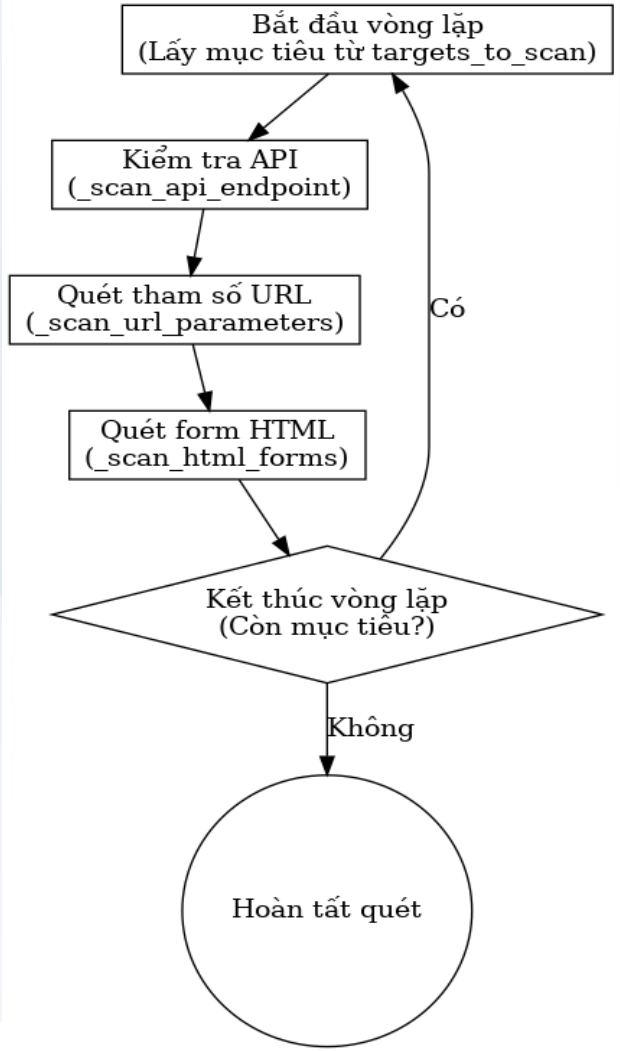
PHÂN TÍCH VÀ THIẾT KẾ

Luồng hoạt động chính



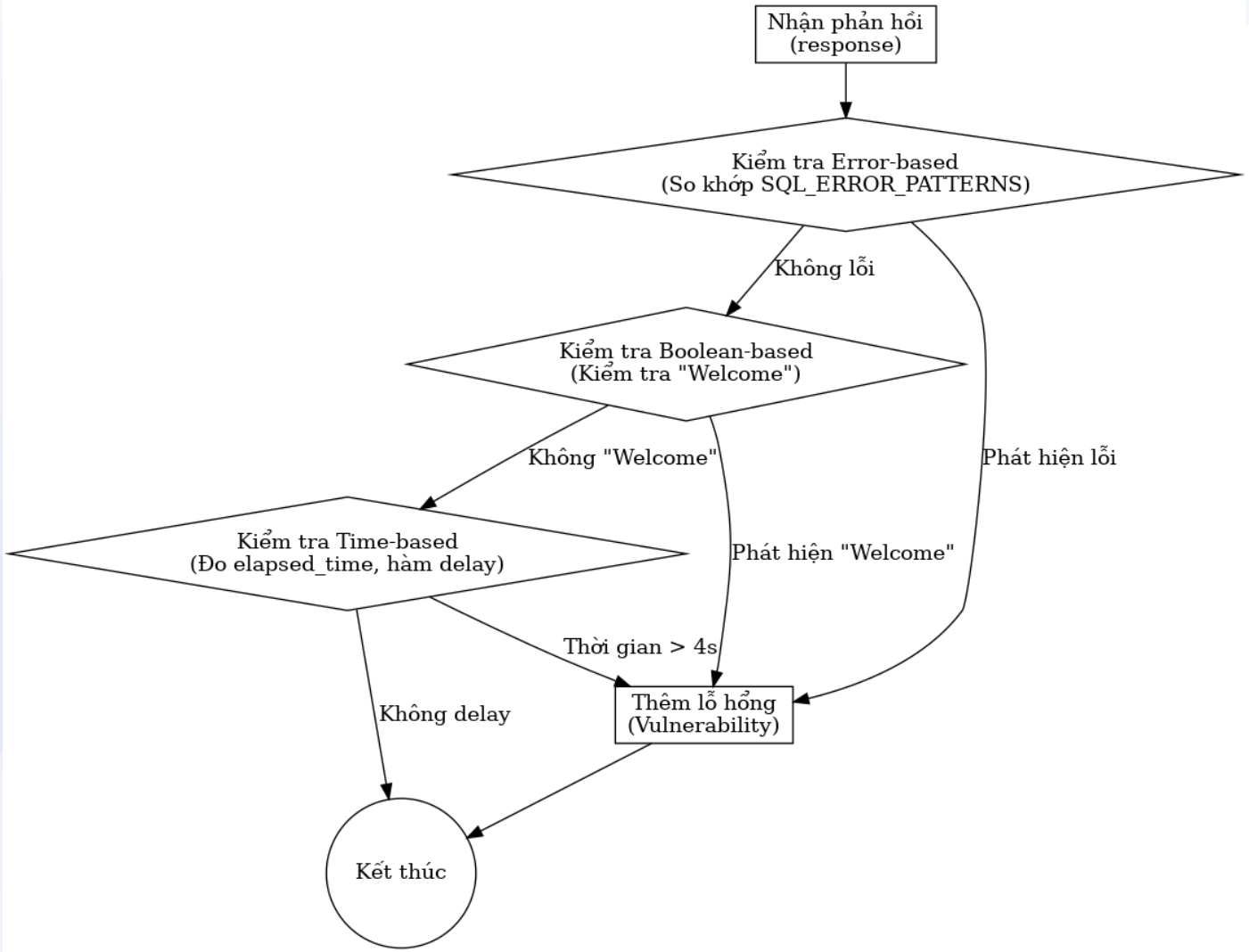
PHÂN TÍCH VÀ THIẾT KẾ

Sơ đồ hoạt động
Vòng lặp quét chính



PHÂN TÍCH VÀ THIẾT KẾ

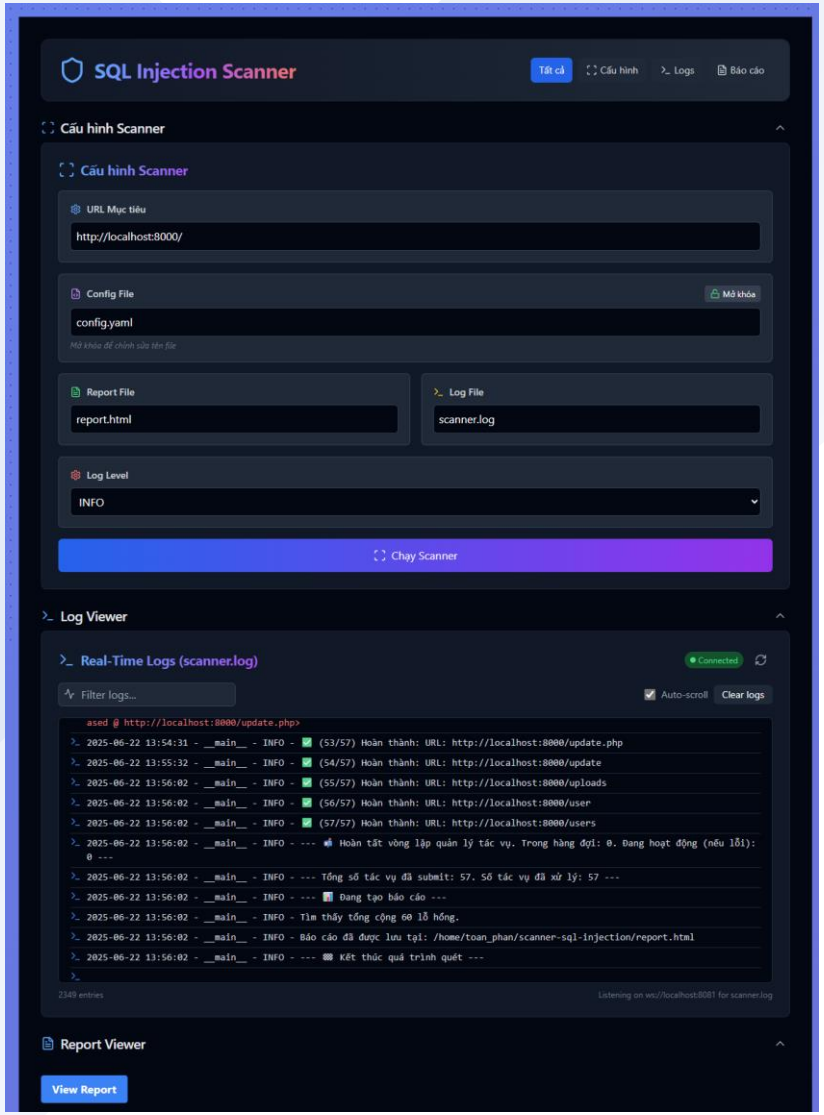
Quy trình phát hiện lỗ hổng SQL Injection



MỤC LỤC

ĐÁNH GIÁ KẾT QUẢ

Giao diện & Mục tiêu

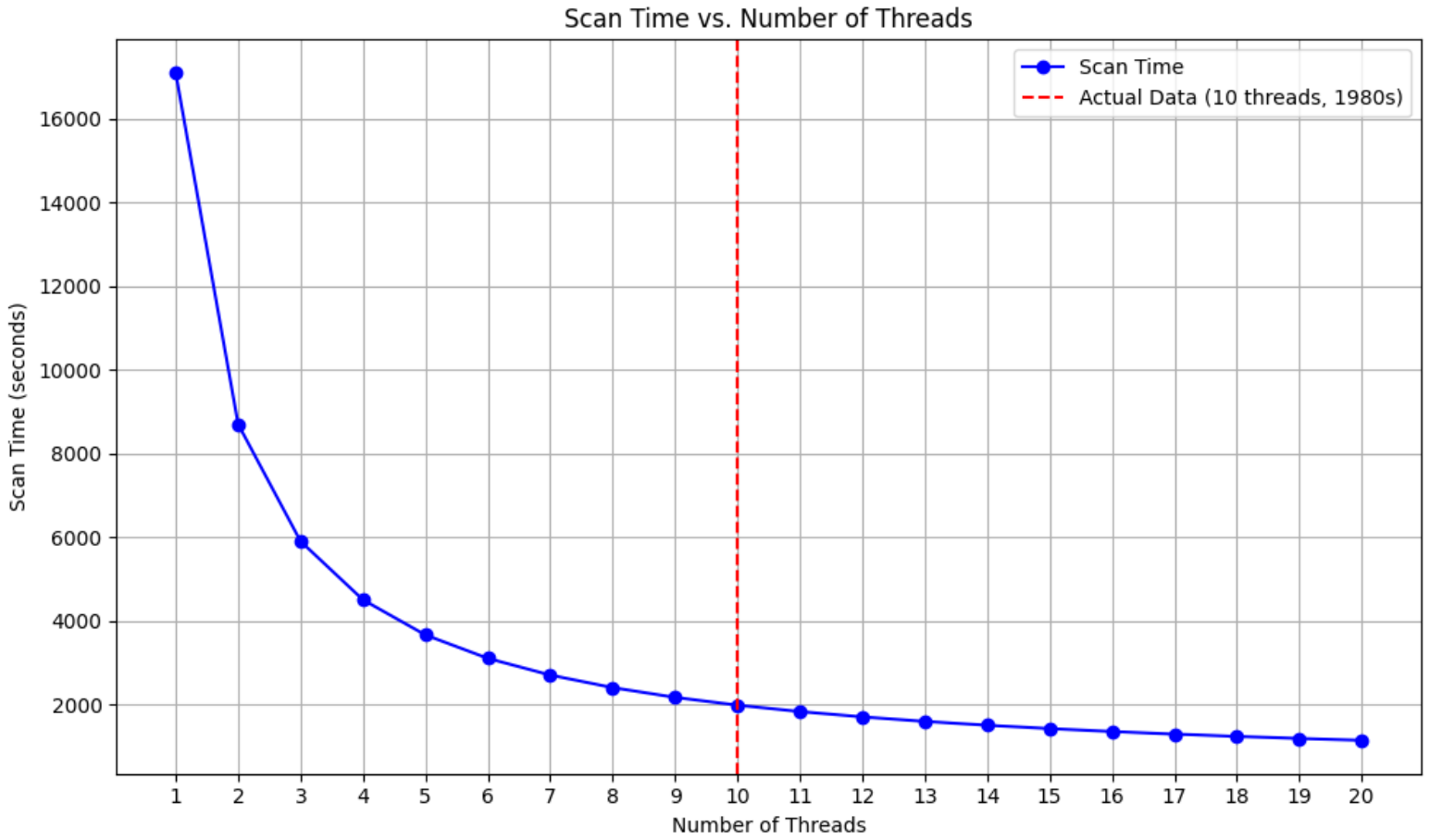


ĐÁNH GIÁ KẾT QUẢ

Thử nghiệm được thực hiện trên một môi trường mô phỏng với các ứng dụng web PHP chạy trên máy chủ localhost (http://localhost:8000)

ĐÁNH GIÁ KẾT QUẢ

Biểu đồ đánh giá thời gian hoạt động đa luồng



MỤC LỤC

DEMO CÔNG CỤ
SCAN SQL Injection

THANK YOU!

20225415 - PTT