LoadStorm:

Giới thiệu sơ lược:

LoadStorm là một công cụ kiểm tra tải dựa trên web của CustomerCentrix, LLC và tận dụng các dịch vụ Web của Amazon để mở rộng theo yêu cầu về sức mạnh xử lý và băng thông.

LoadStorm là một công cụ kiểm thử phần mềm giúp kiểm tra tải SaaS. Nó thử nghiệm hiệu suất theo yêu cầu, kiểm tra tải cho các trang web.

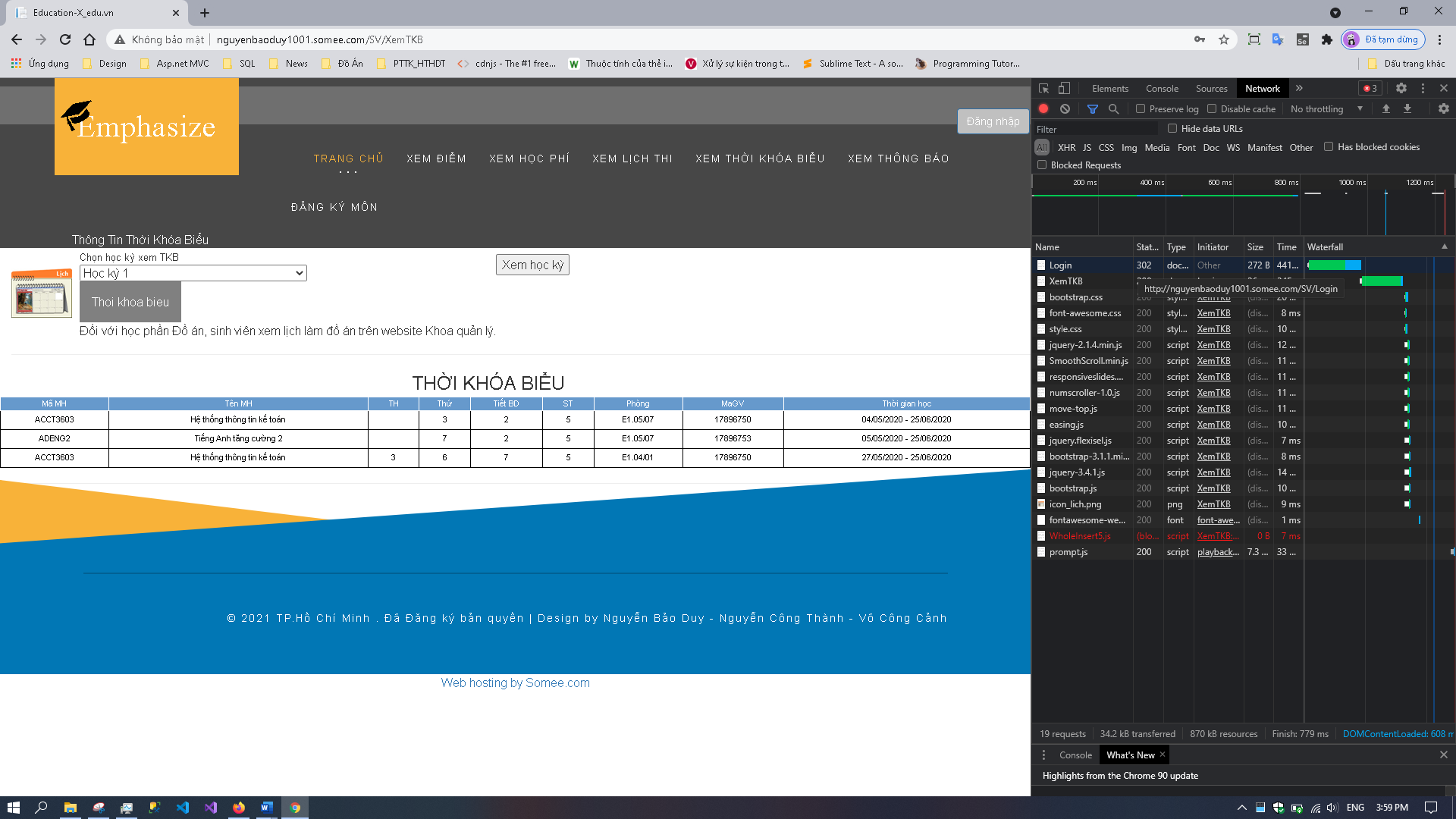
Mục tiêu của LoadStorm là tiện lợi và tiết kiệm.

Biểu đồ và báo cáo mở rộng của LoadStorm hiển thị cho bạn thời gian phản hồi, tỷ lệ lỗi, yêu cầu mỗi giây, thời gian hoàn thành trang.

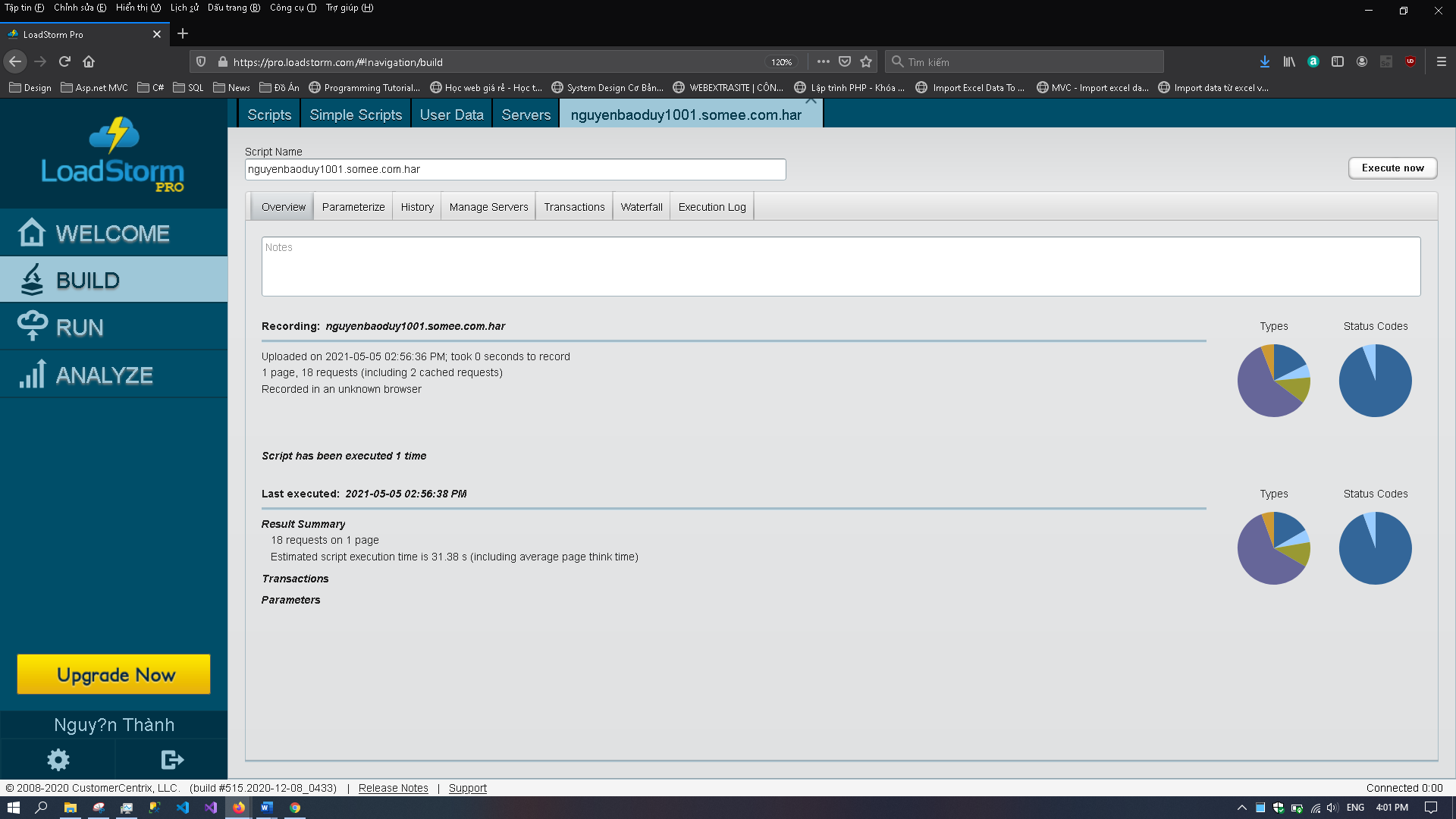
Áp dụng :

URL thực hiện test: http://nguyenbaoduy1001.somee.com, thực hiện kiểm thử file .har với chức năng tìm kiếm.

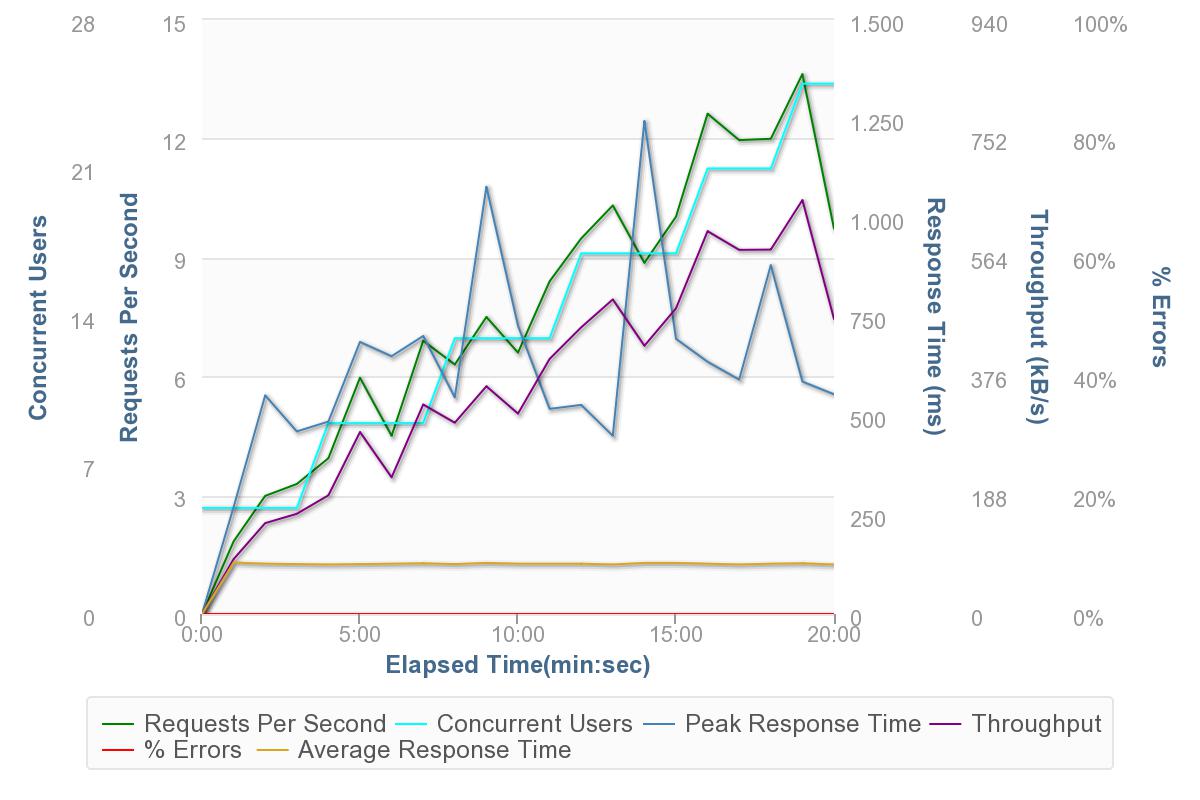
- Sử dụng tài khoản free trial của LoadStorm với tối đa 25 người dùng cao điểm



- Save file .har với chức năng tìm kiếm để chạy script loadstorm



- Sau khi chi chạy file .har loadstorm sẽ overview các resource và status codes của trang web

- Sau khi tiến hành test loadstorm sẽ thống kê các lỗi, response, request,…

Trong đó :

Throughput 466,89/s có nghĩa là server xử lý 17,45 yêu cầu trên 1 giây.

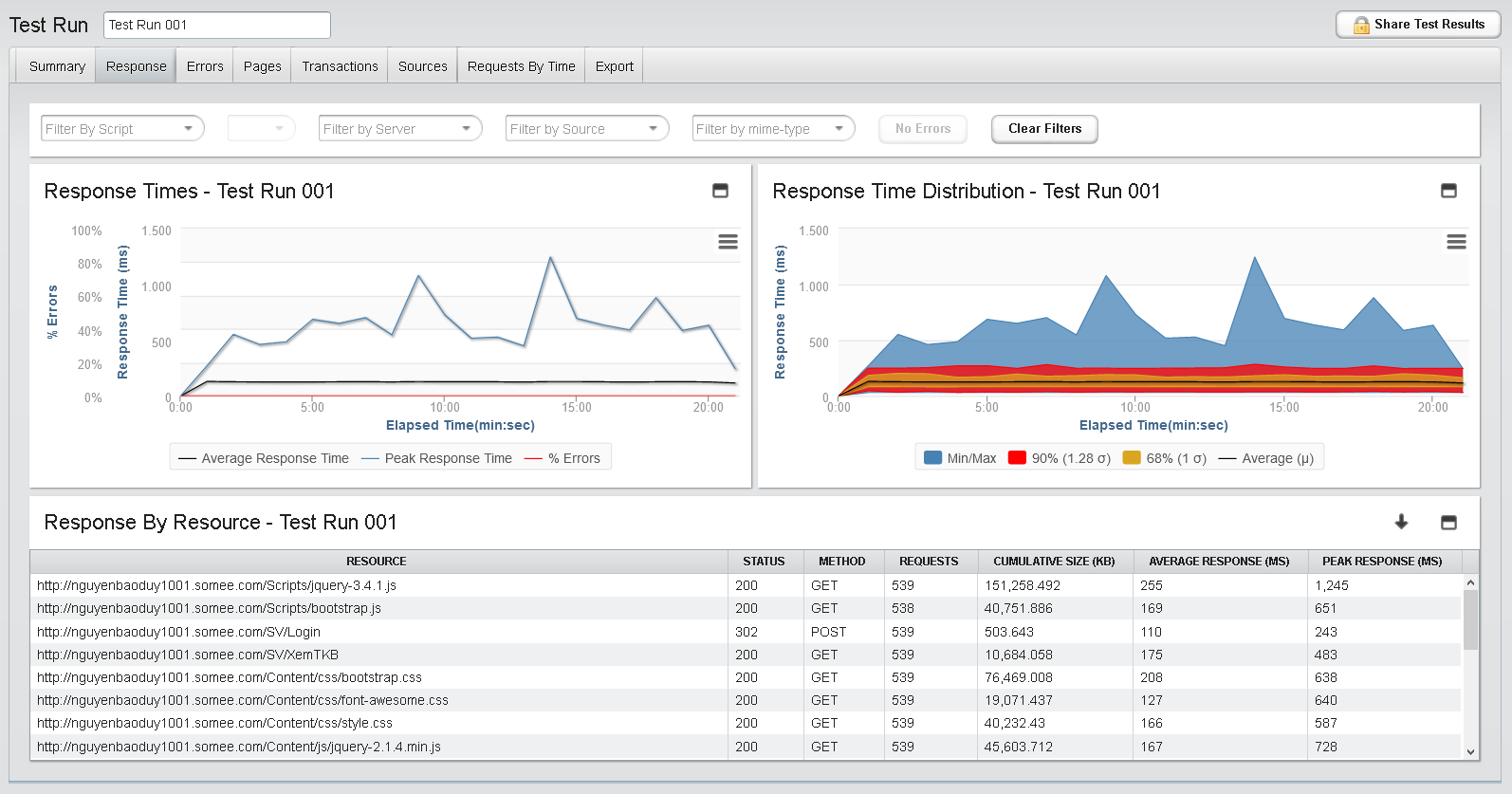
Error là tỉ lệ yêu cầu bị lỗi.

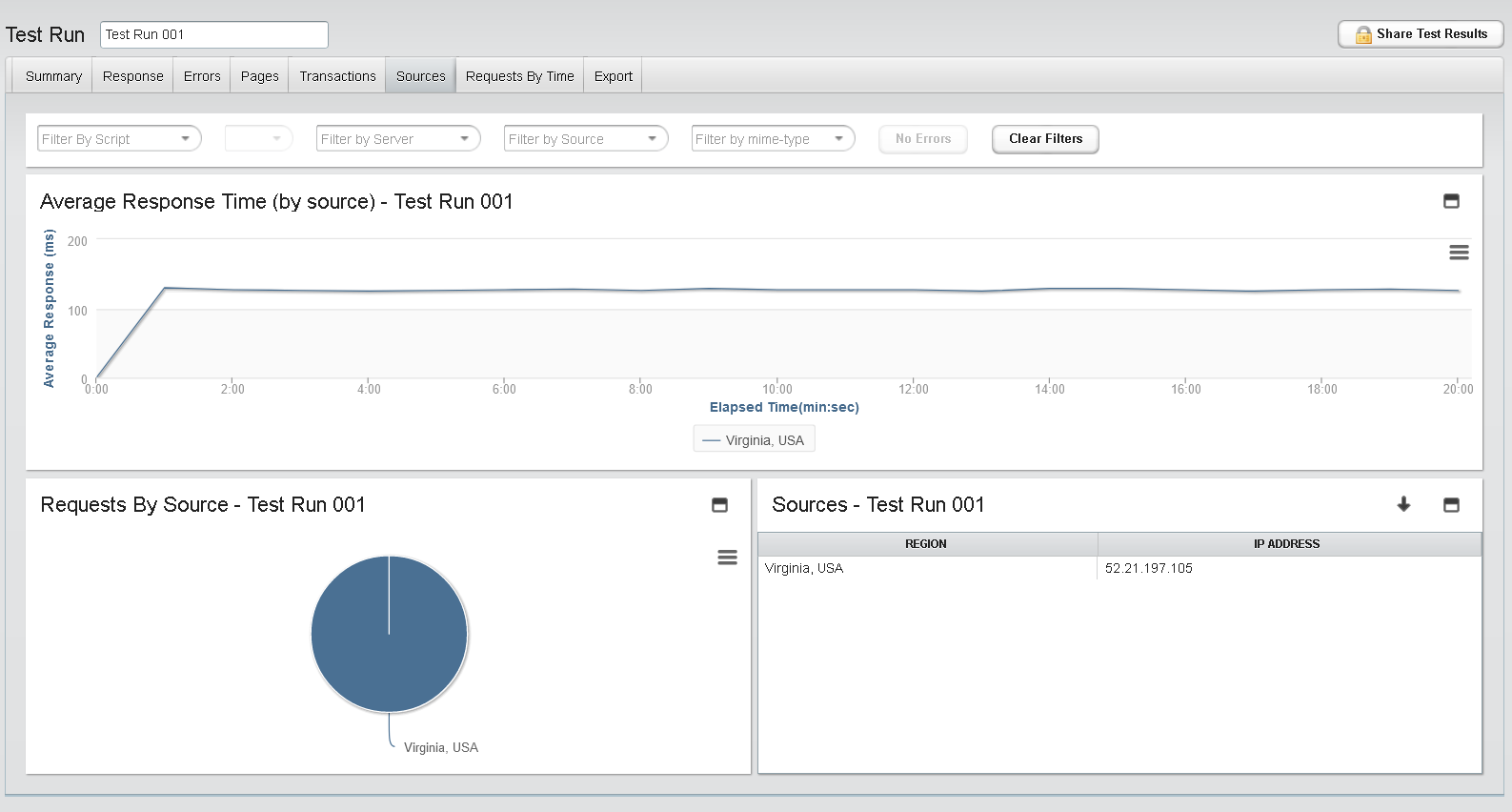
Request per second là yêu cầu mỗi giây

Concurrent user là số người sử dụng đồng thời

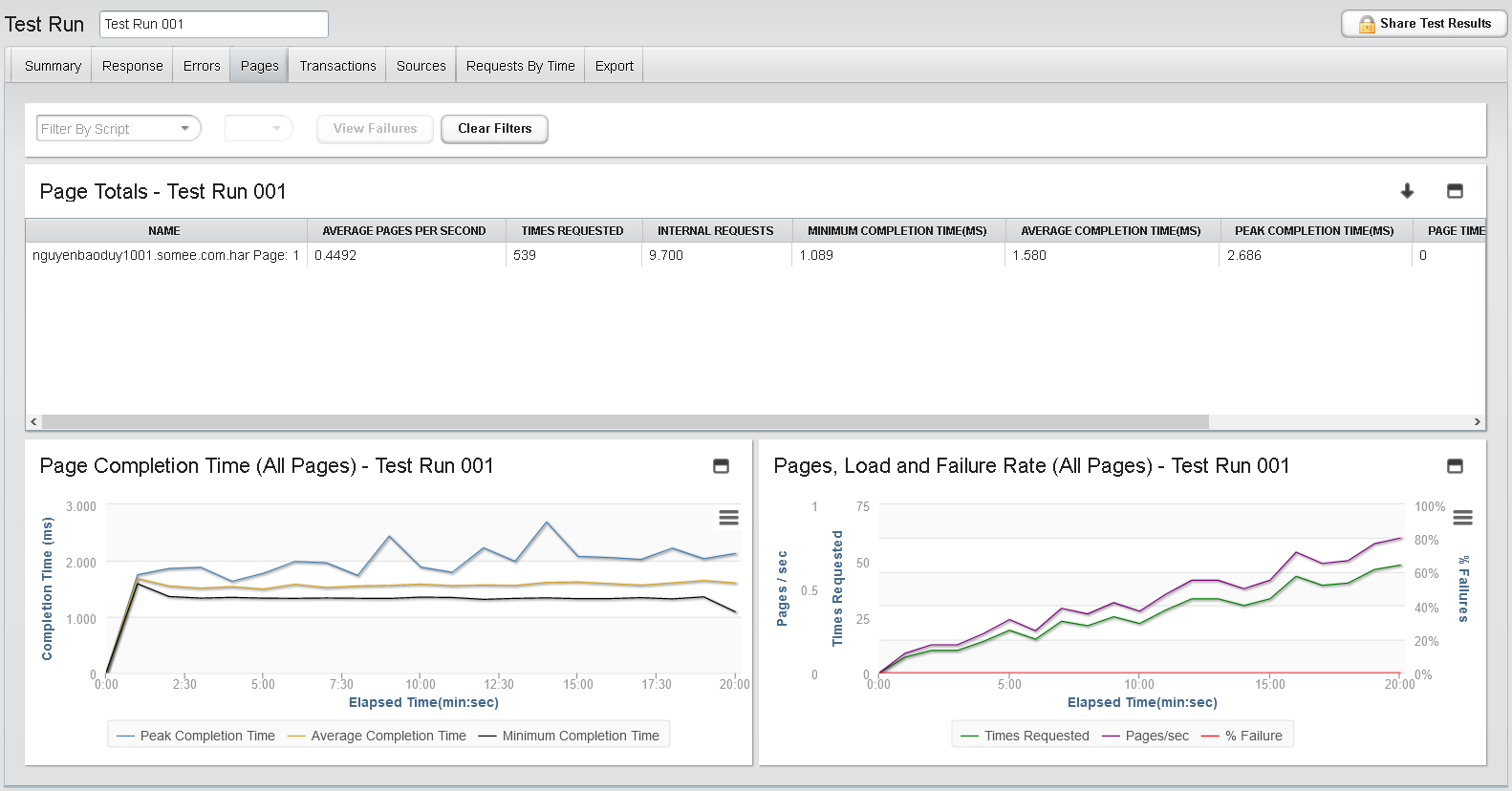
Average Response time là thời gian phản hồi trung bình.

Peak response time(ms) là thời gian đáp ứng cao nhất(mili giây)



- Thống kê resource và trả và status, method, requests,…

- Thống kê thời gian hoàn thành của 1 page và phần trăm load của trang:



Nessus:

Giới thiệu sơ lược:

Nessus là một công cụ quét lỗ hổng bảo mật độc quyền được phát triển bởi Công ty An ninh mạng Tenable, được phát hành miễn phí cho việc sử dụng phi thương mại.

Nessus còn là một trong những sản phẩm được đánh giá cao trên toàn thế giới, với tính năng đa dạng, thống kê toàn diện về hệ thống đầy đủ,phát hiện những dữ liệu nhạy cảm và phântích lỗ hổng, đáp ứng cao về nhu cầu bảo mật.

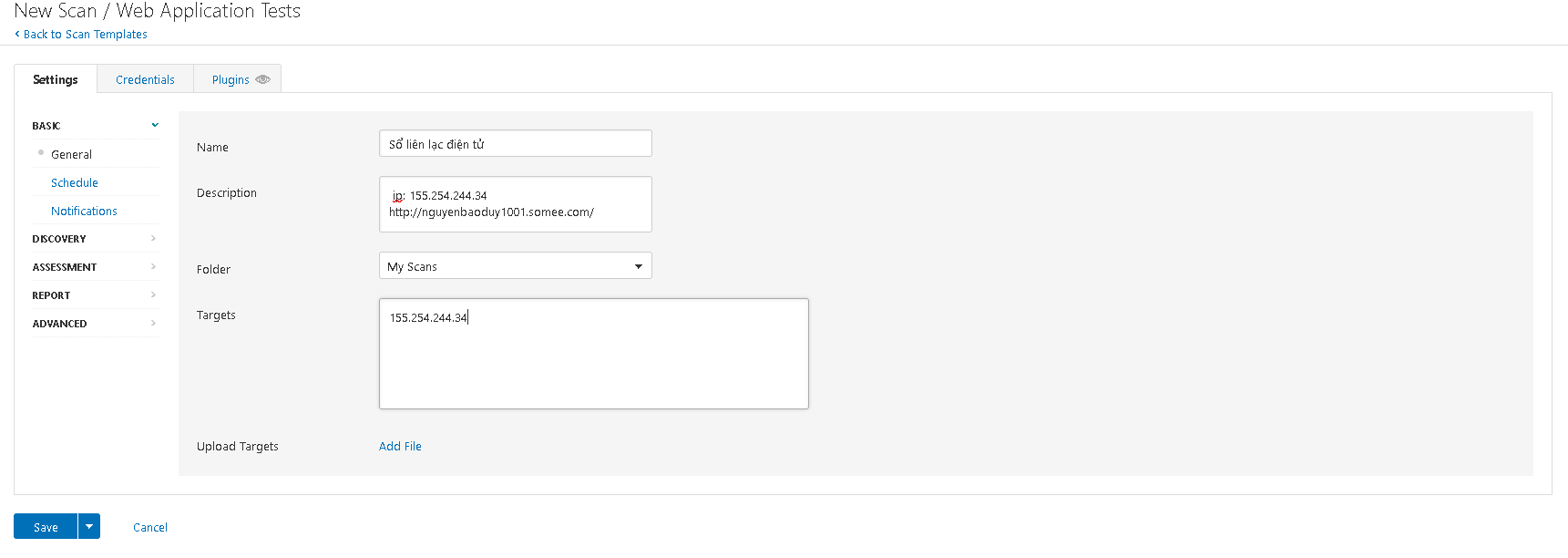
Nessus cho phép:Lỗ hổng cho phép một hacker từ xa kiểm soát hoặc truy cập dữ liệu nhạy cảm trên hệ thống.Cấu hình sai (vídụ như chuyển tiếp thư mở, các bản vá lỗi bị thiếu,...).Mật khẩu mặc định, một vài mật khẩu thường được sử dụng, và mật khẩu trống trên các tài khoản hệ thống. Nessus cũng có thể dùng Hydra (một công cụ bên thứ ba) để thực hiện một cuộc tấn công từ điển.

Tấn công từ chối dịch vụ bộ nhớ stack TCP/IP bằng gói tin độc hại.

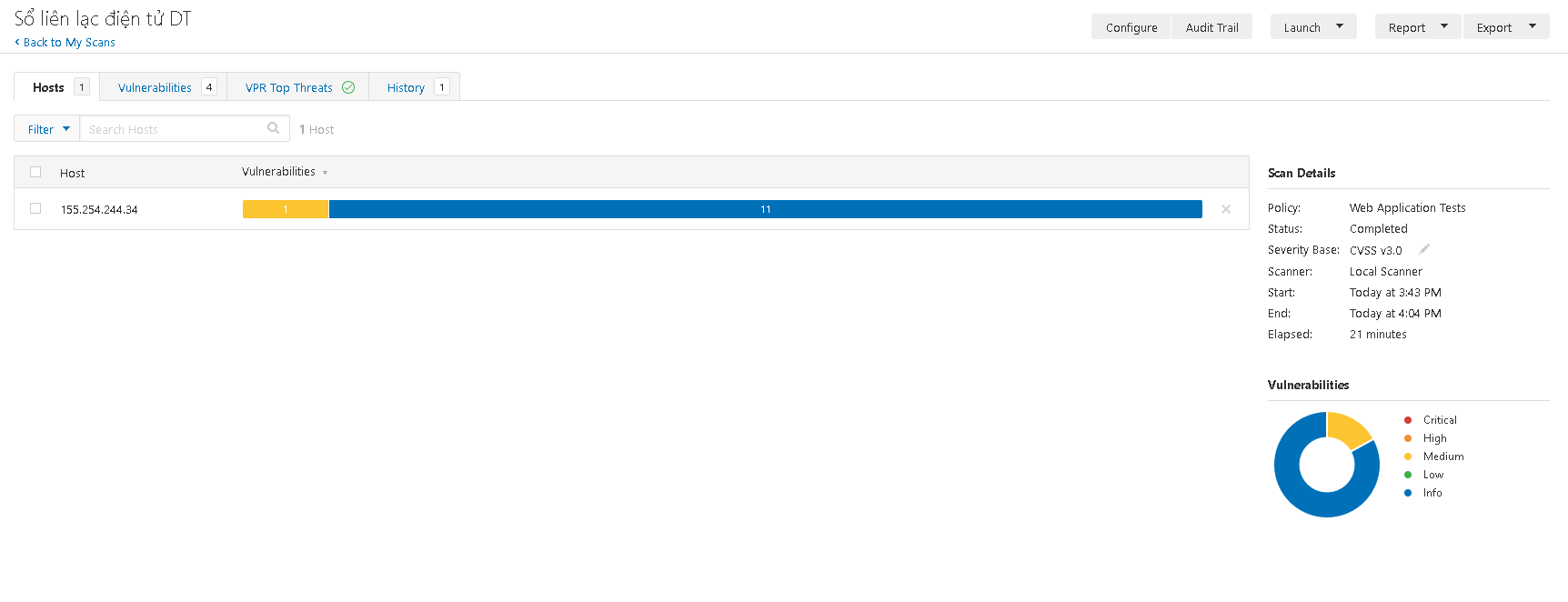
Chuẩn bị cho việc kiểm tra bảo mật (PSI DSS).

Áp dụng :

# -Tạo New Scan / Web Application Tests



-Thống kê vấn đề của trang web



-Thống kê lỗ hổng của web

