# THỰC HÀNH MẠNG MÁY TÍNH

**LAB 8: KIỂM THỬ LỖ HỔNG SQL INJECTION**

Họ và tên: Trần Nguyễn Gia Long

Lớp: 10ĐH\_CNPM1

MSSV: 1050080059

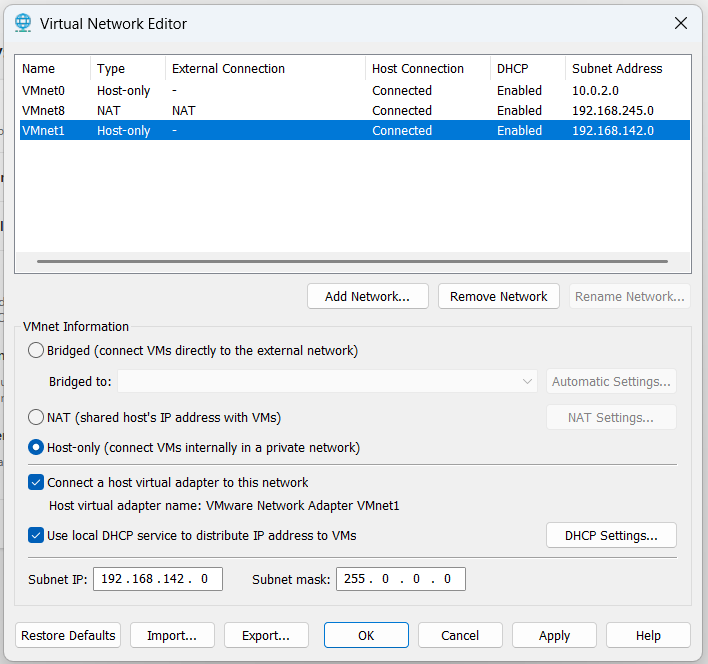
Link Github:

Link video Youtube: <https://youtu.be/46hfCEVV3Ds>

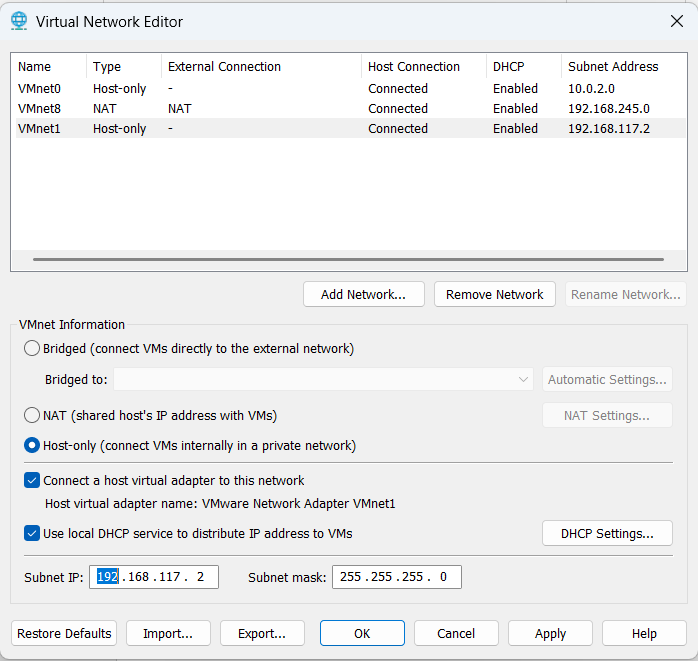
1.4 Cài đặt môi trường luyện tập

1.4.1. Cài đặt và cấu hình Vmware

Bước 4: Trên giao diện của Vmware, chọn Edit → Virtual Network Editor.



Tạo một network mới tên VMnet 1. Địa chỉ IP là 192.168.142.0 và mask là 255.255.255.0. Chọn kết nối Host Only.

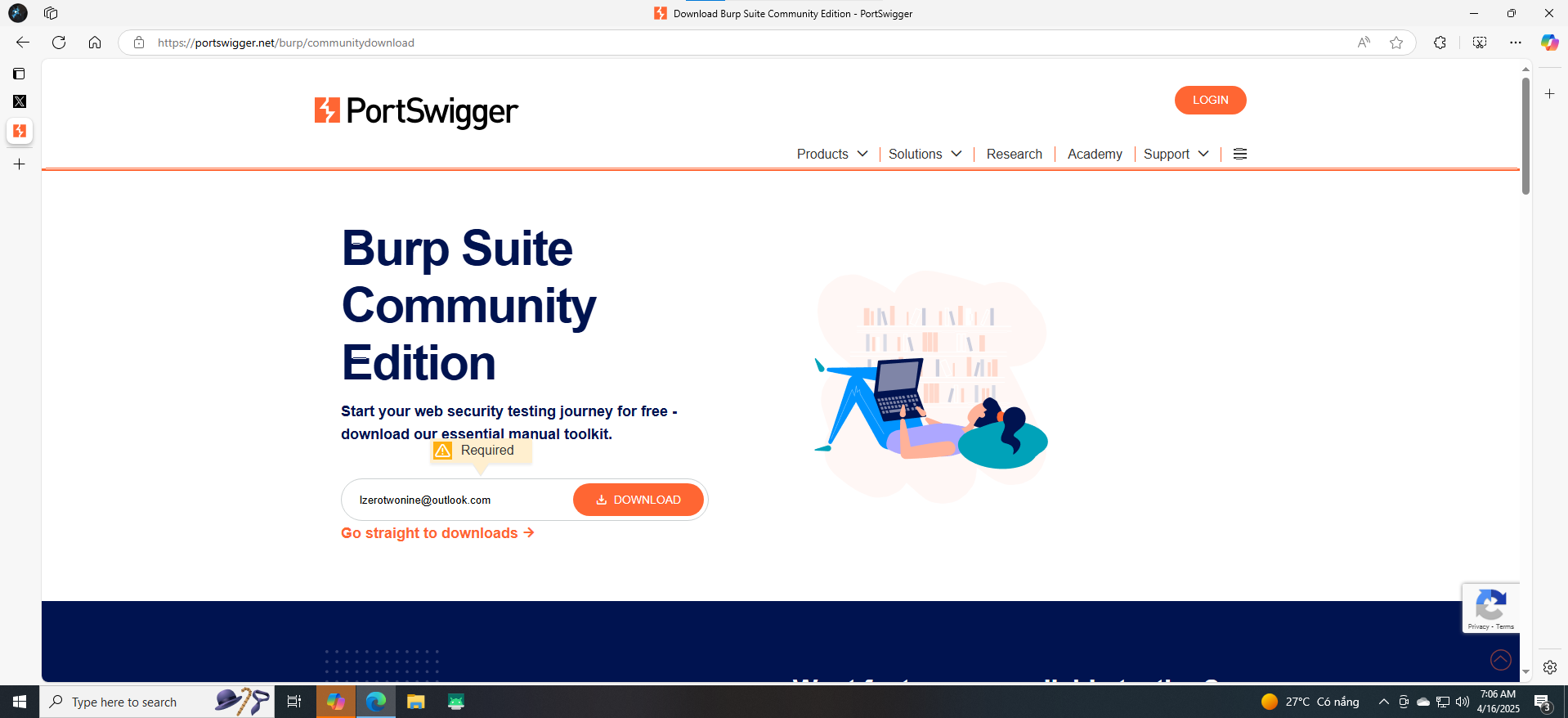


Trong DHCP Setting, ta chỉnh theo ip sau.

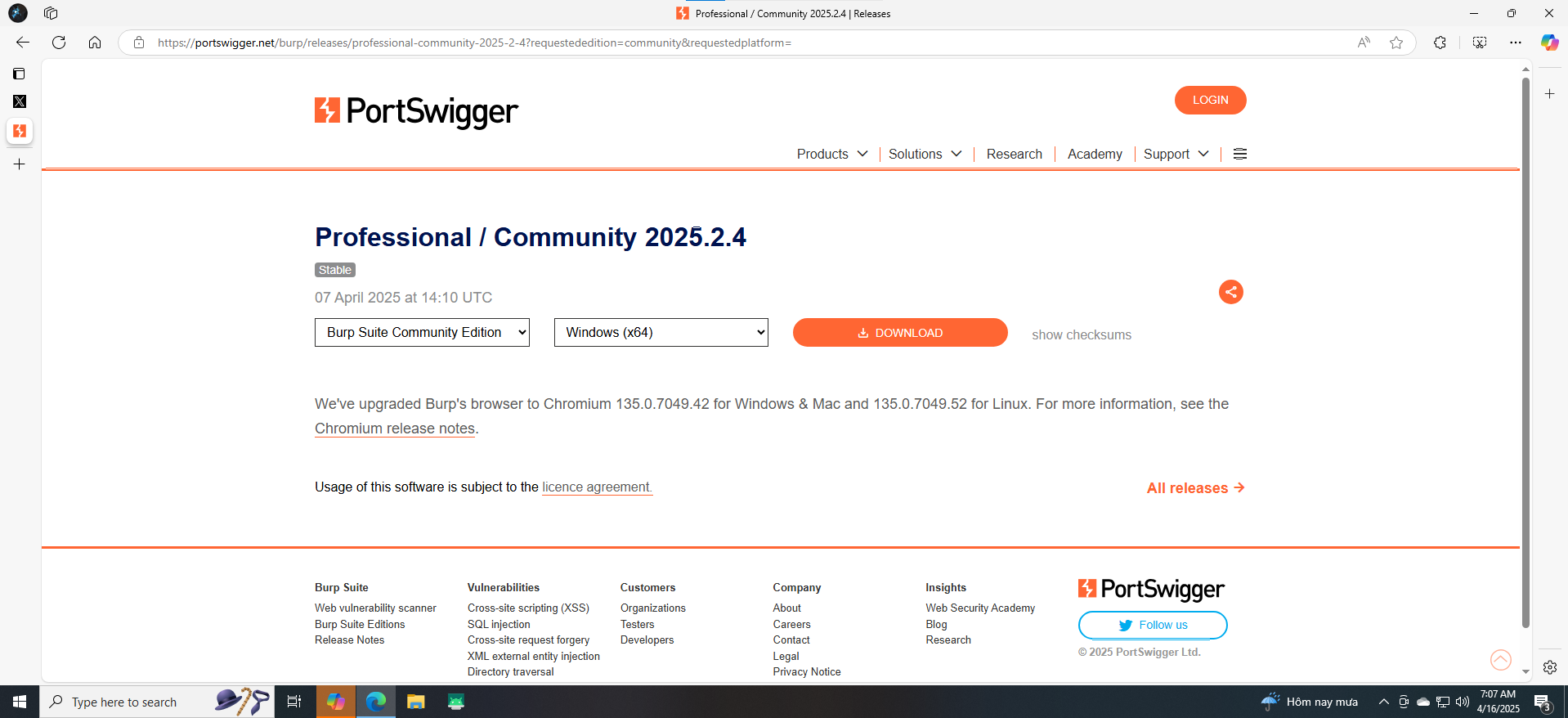
**1.4.2. Triển khai máy ảo Web Server**

**4. Sử dụng công cụ hỗ trợ kiểm thử Burpsuite.**

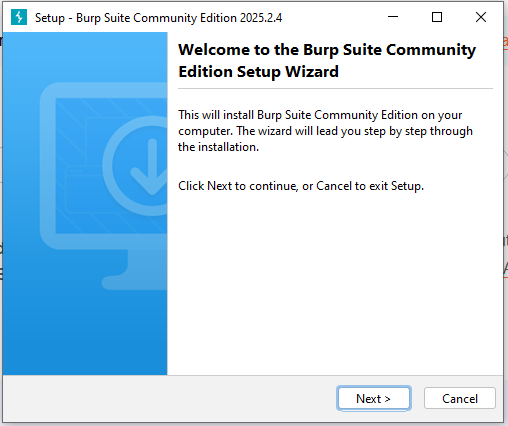
Download công cụ tại địa chỉ sau: <https://portswigger.net/burp/freedownload>



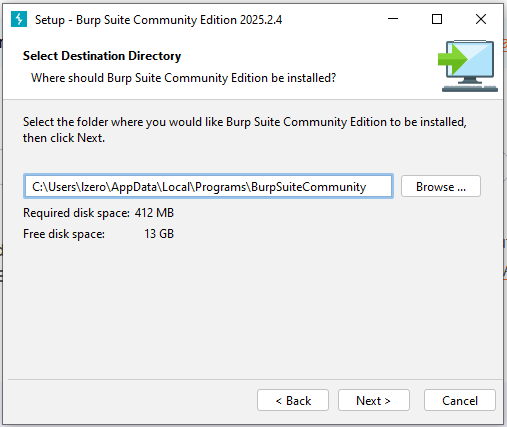
Nhập email để có thể tải về.



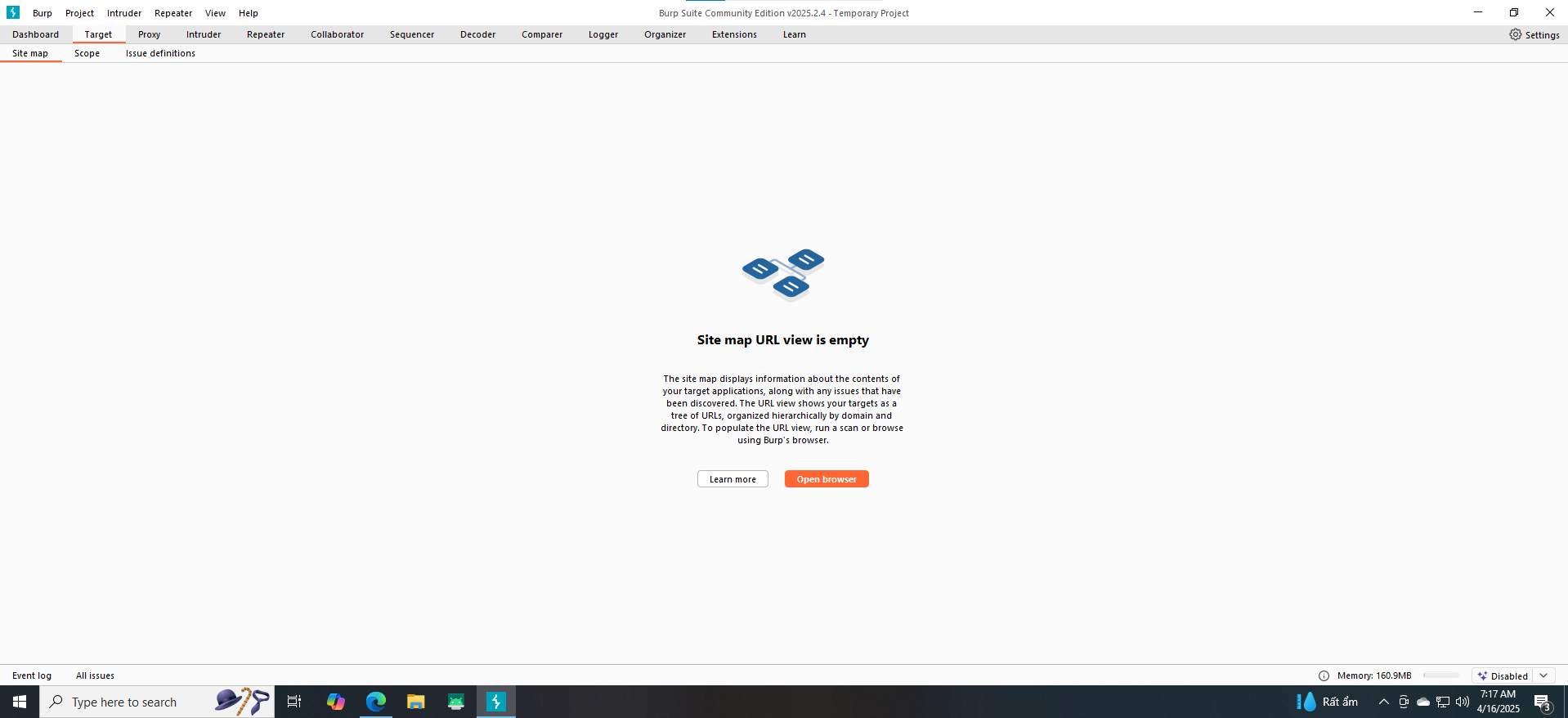
Tiến hành cài đặt.



Chọn địa chỉ cài đặt.



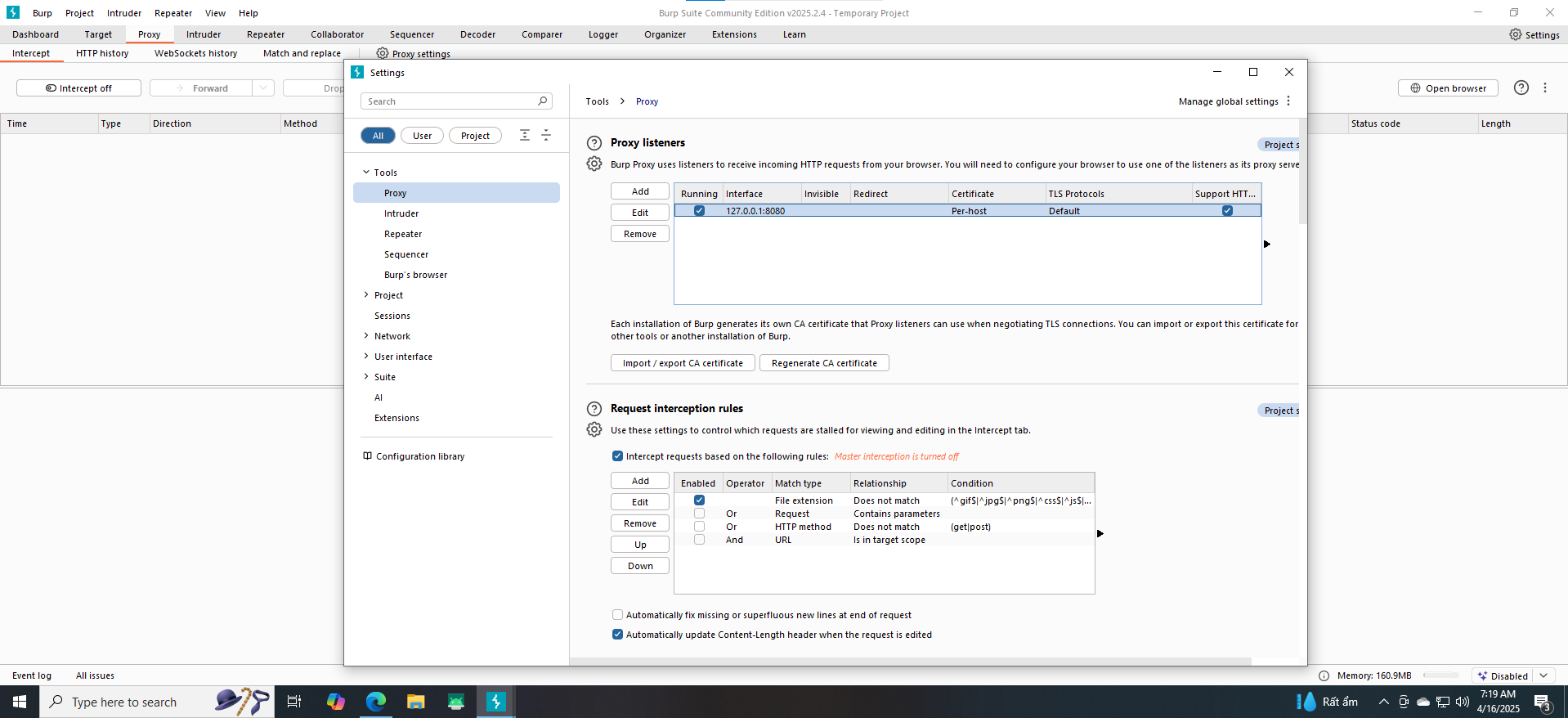
4.1. Cấu hình cơ bản



**Kiểm tra hoạt động Burp**

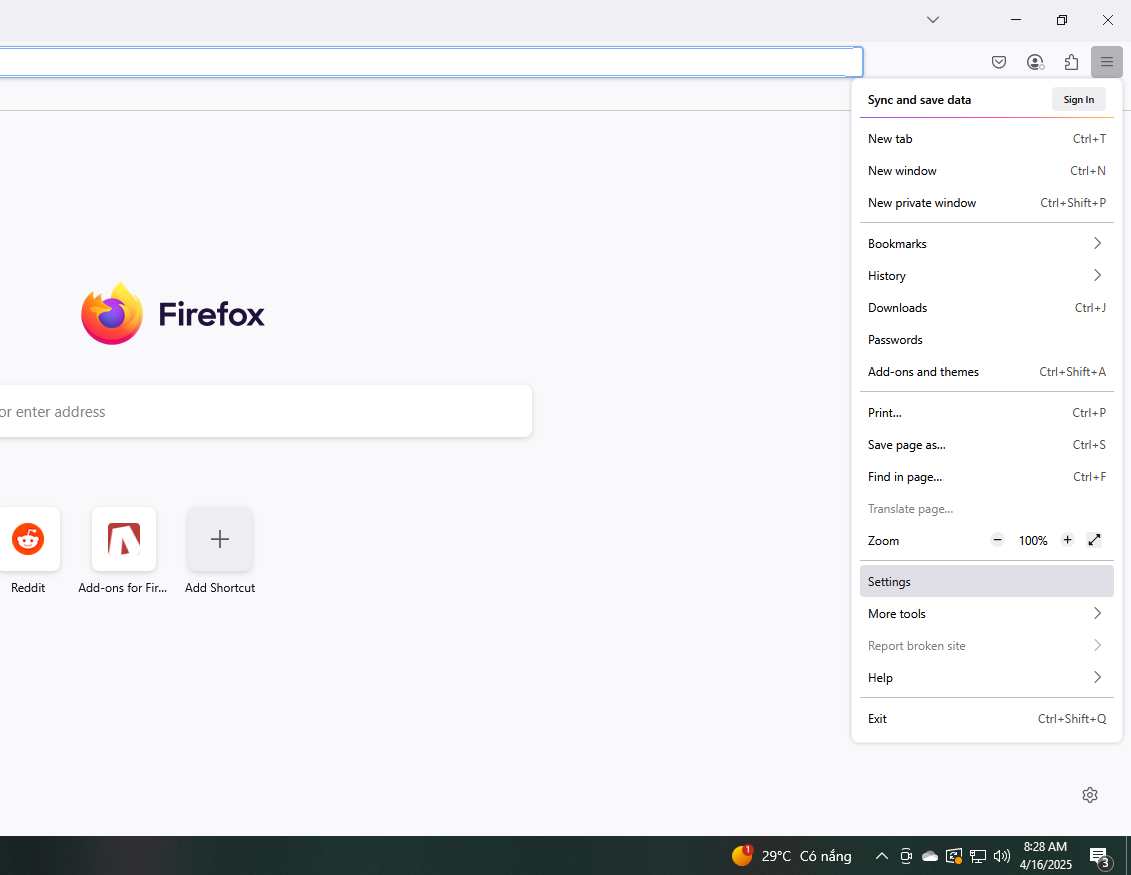
**Cấu hình tại Burp Proxy**

kiểm tra chắc chắn rằng không có chương trình hoặc dịch vụ nào khác đang lắng nghe trên cùng cổng 8080/TCP, ta thực hiện kiểm tra tại thẻ Proxy/ Proxy Settings.

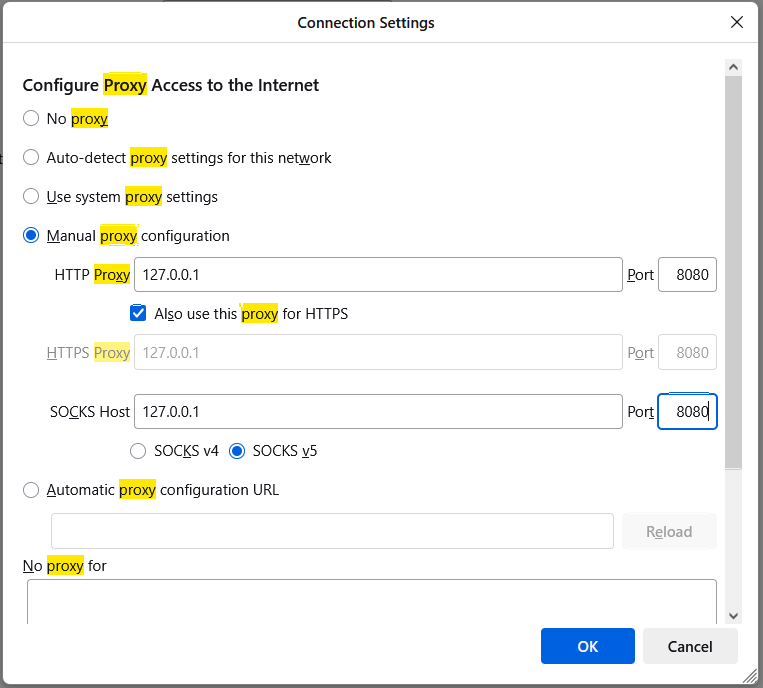


**Cấu hình tại trình duyệt**

Thực hiện cấu hình Proxy tại trình duyệt Firefox

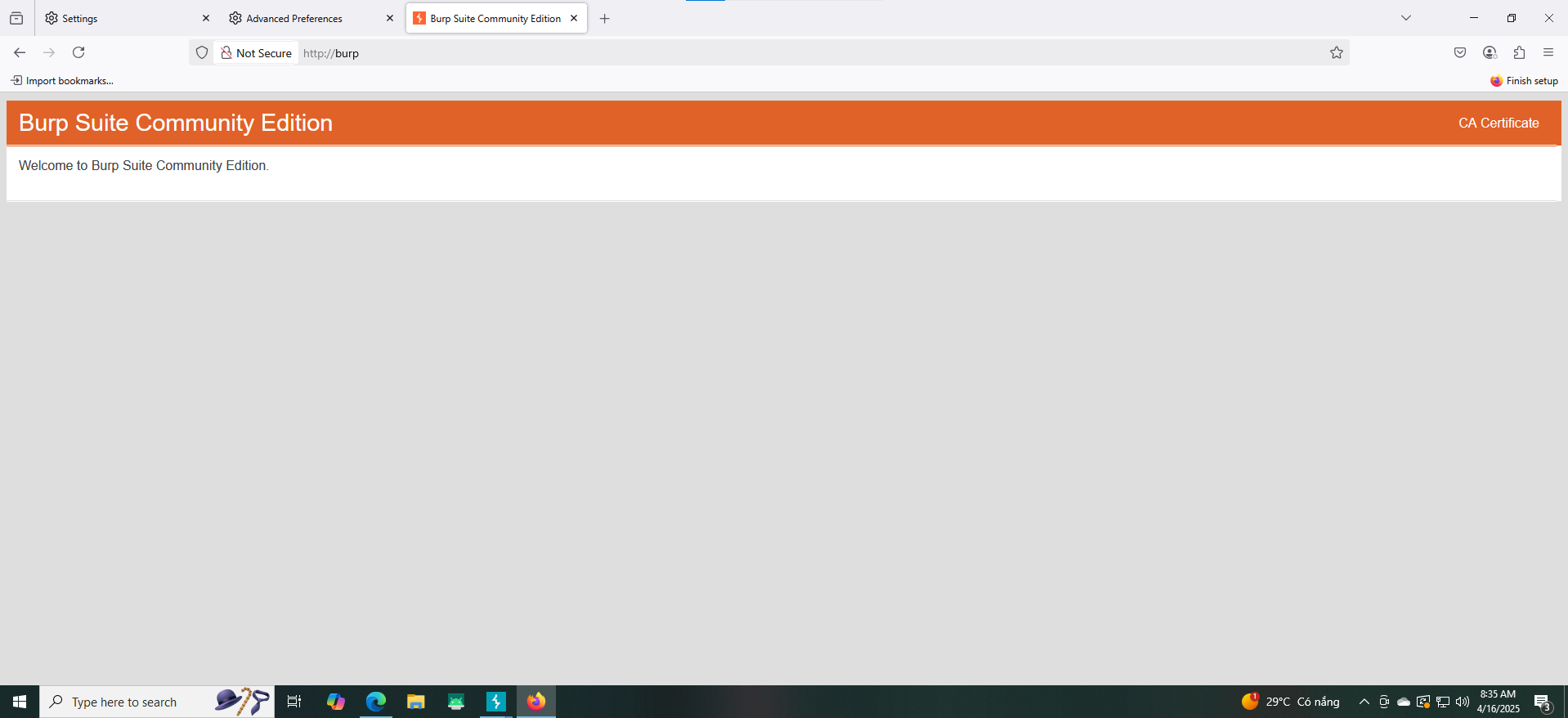


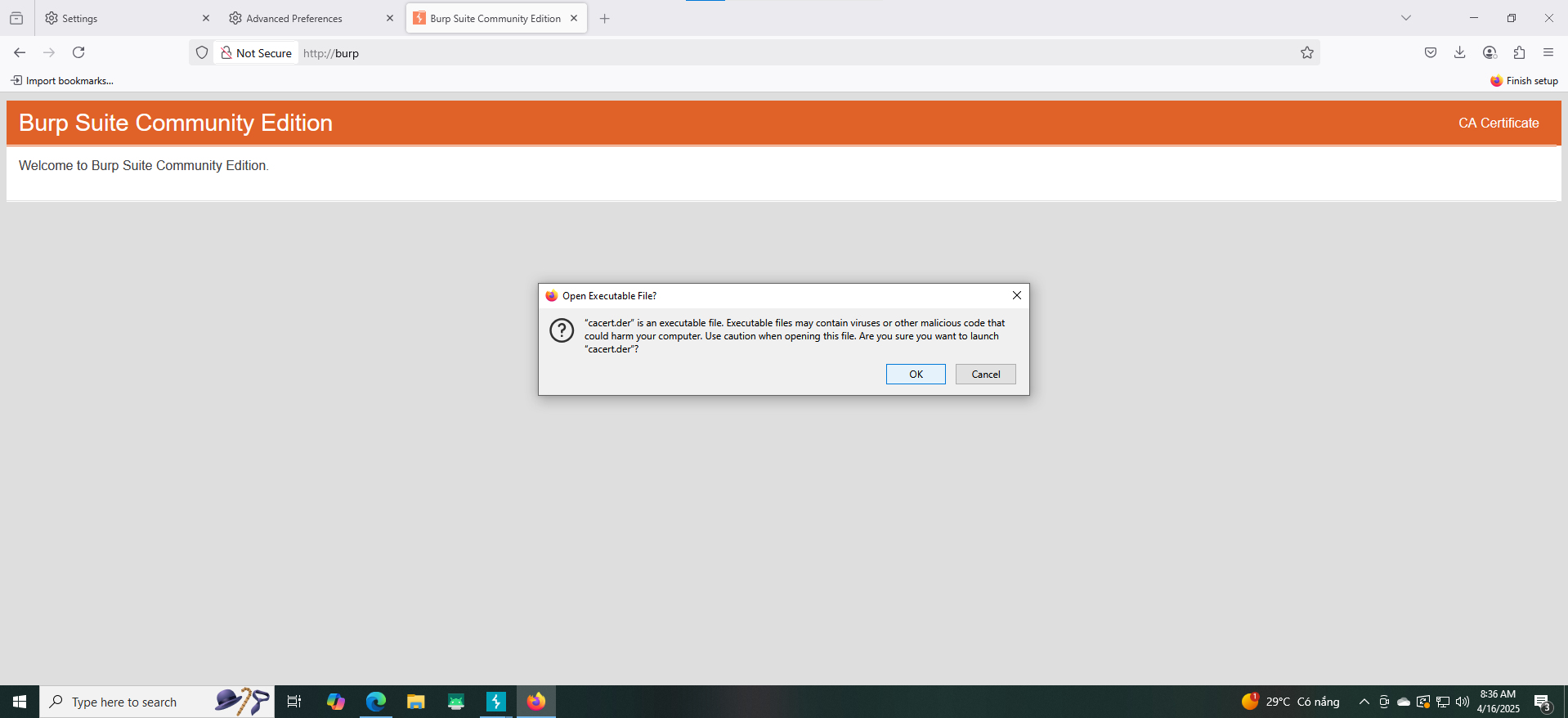
Chọn proxy setting trên máy. Chỉnh địa chỉ là 127.0.0.1 và port là 8080.

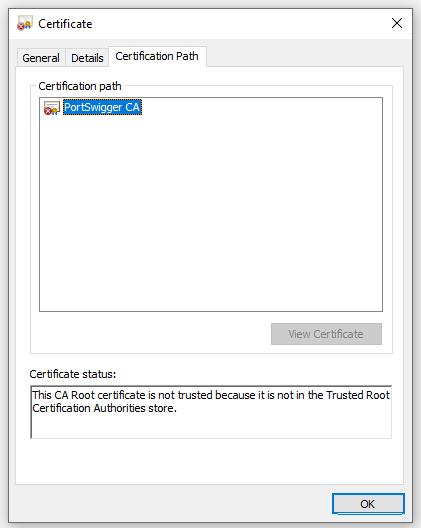


Import chứng chỉ SSL của Burp để kiểm thử HTTPS

Truy cập http://burp → tải CA Certificate → cài vào trình duyệt để tránh lỗi HTTPS.

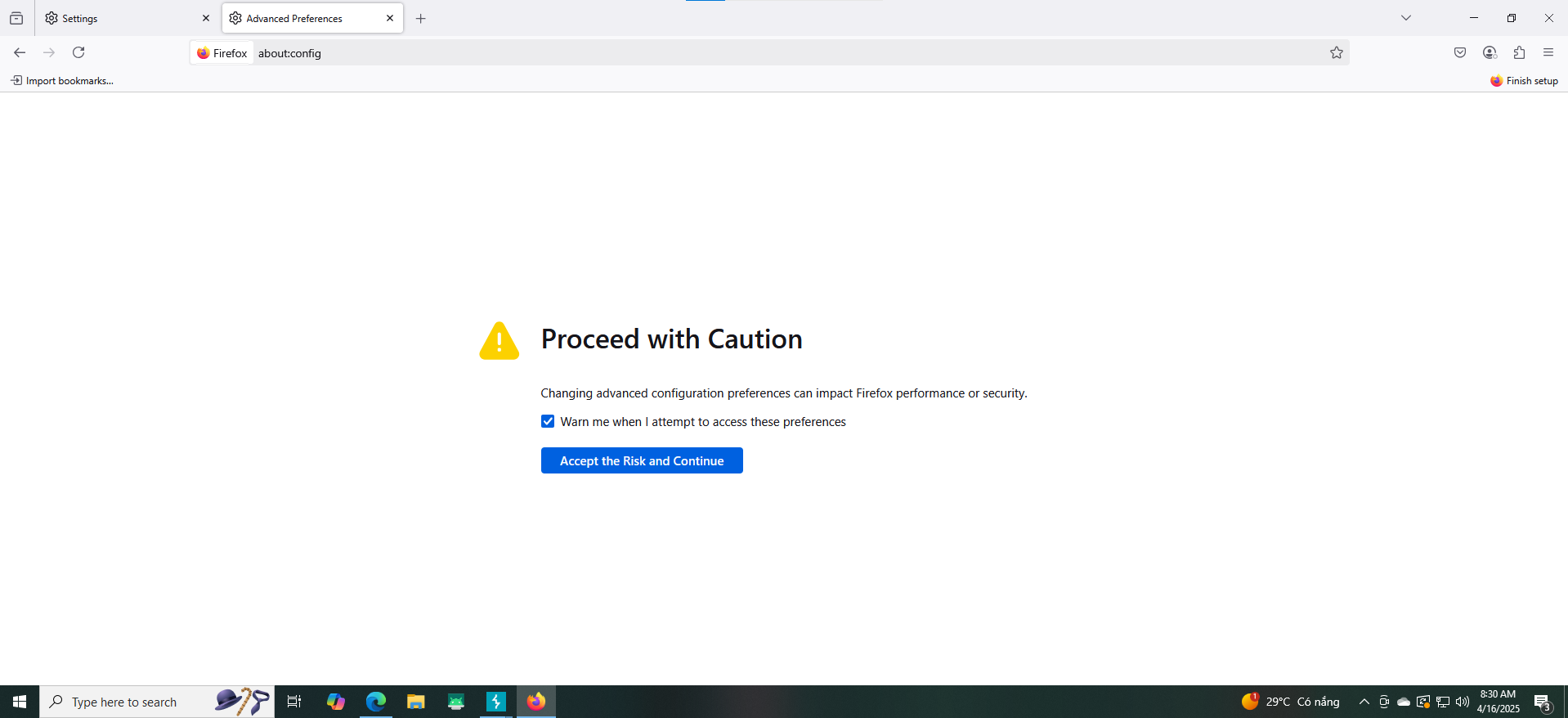


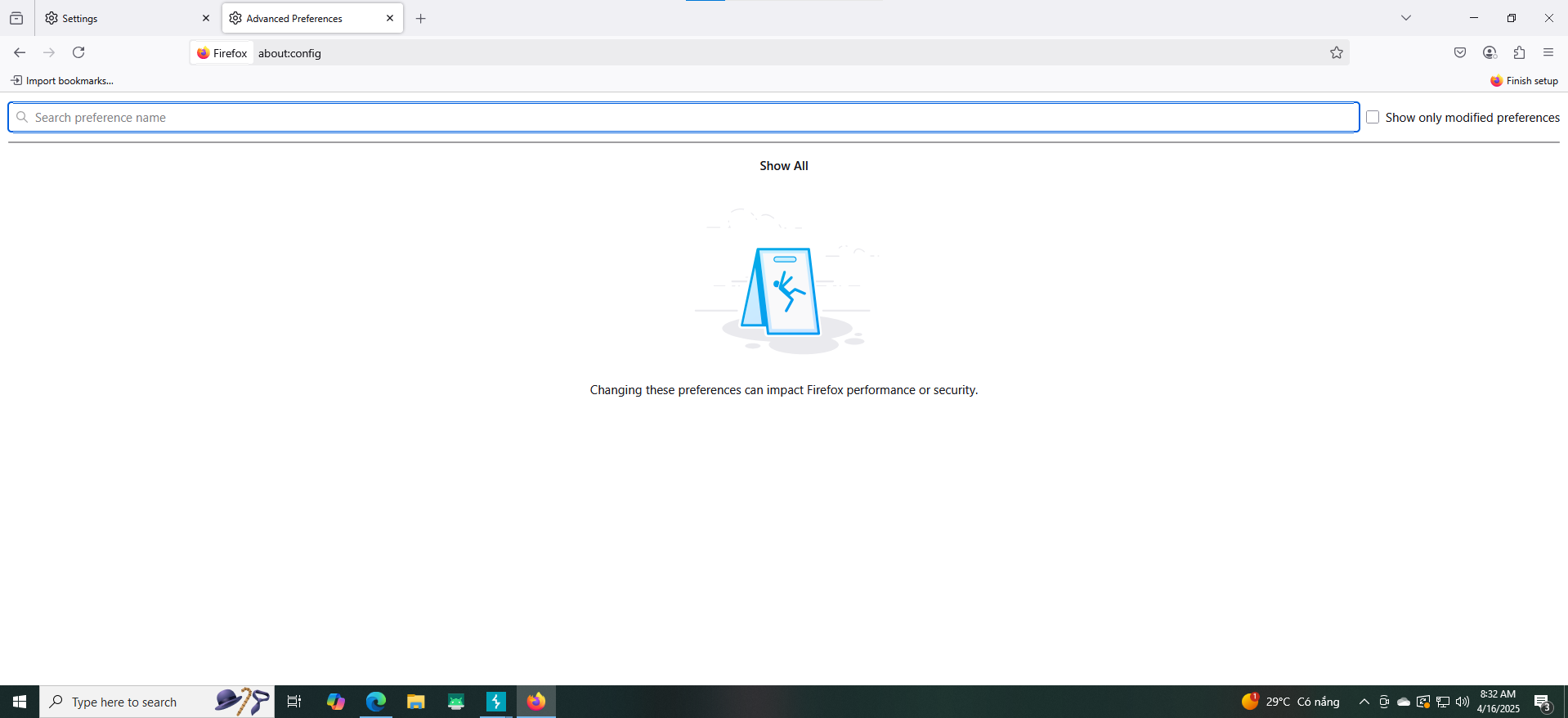




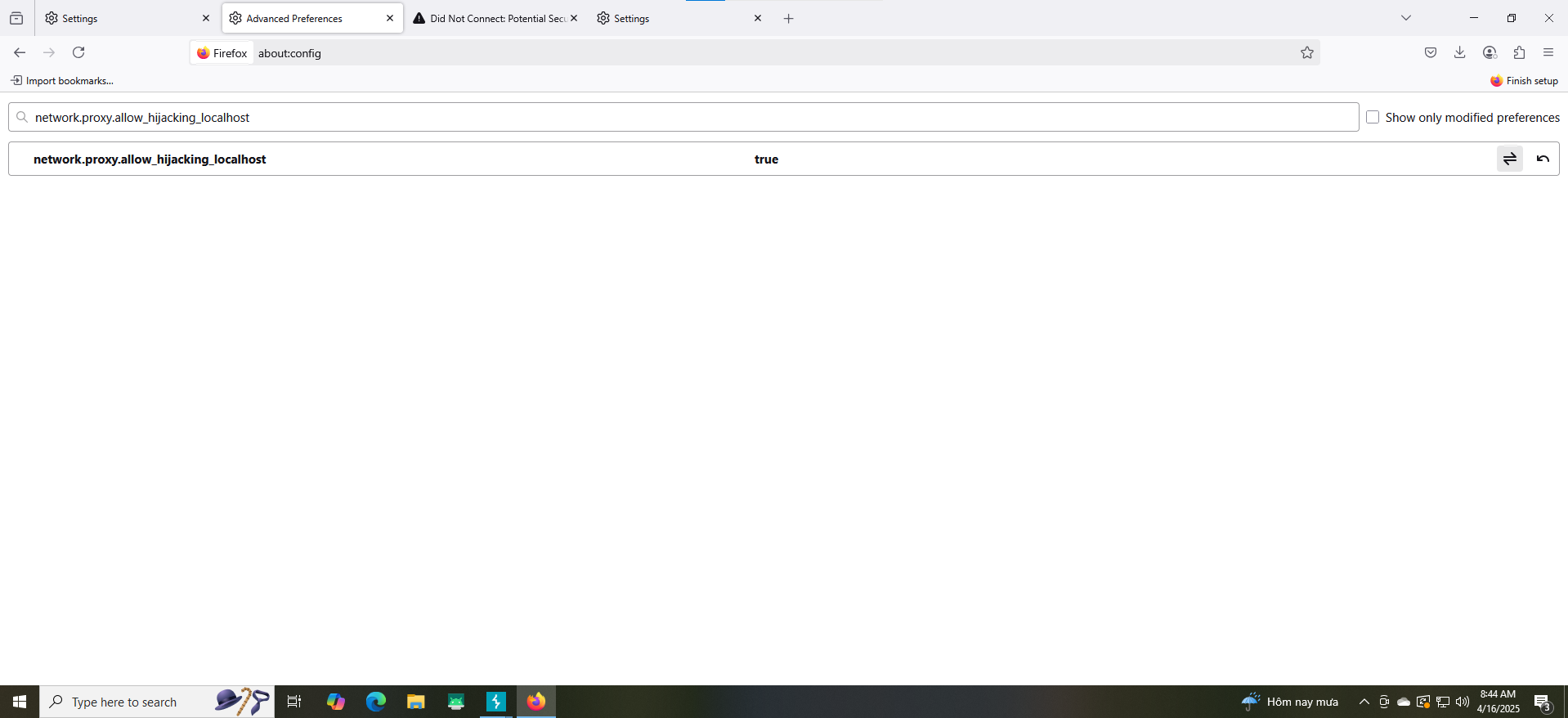
Thiết lập cấu hình để cho phép proxy hoạt động với các các lưu lượng cục bộ (localhost):

- Bước 1: Mở một tab mới và truy cập tới trang about:config. Bỏ qua các cảnh báo nếu có





- Bước 2: Điền giá trị network.proxy.allow\_hijacking\_localhost vào ô tìm kiếm và thiết lập giá trị true cho nó



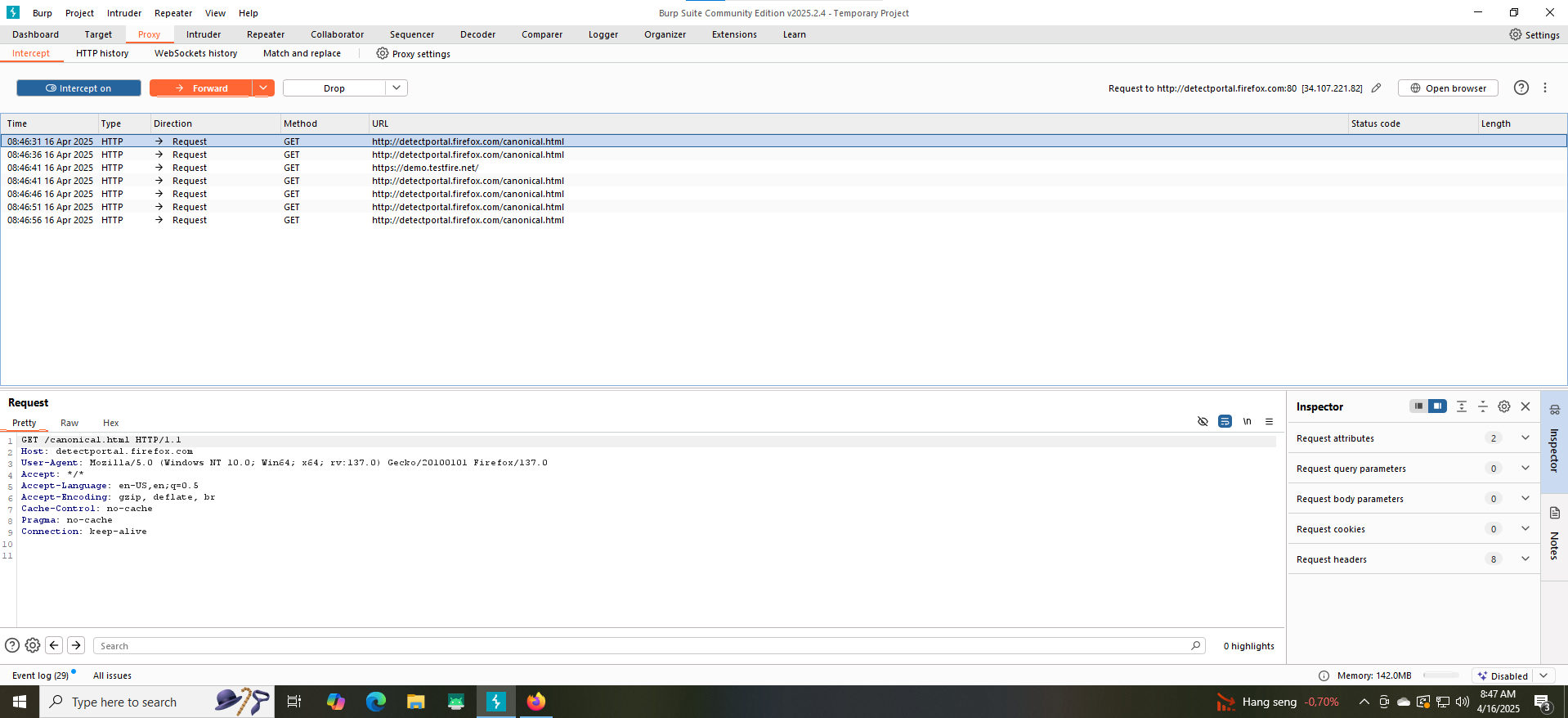
4.2. Sử dụng Burpsuite hỗ trợ kiểm thử SQL Injection

Phần này sẽ minh họa việc sử dụng Burpsuite để tương tác với website khi kiểm thử SQL Injection

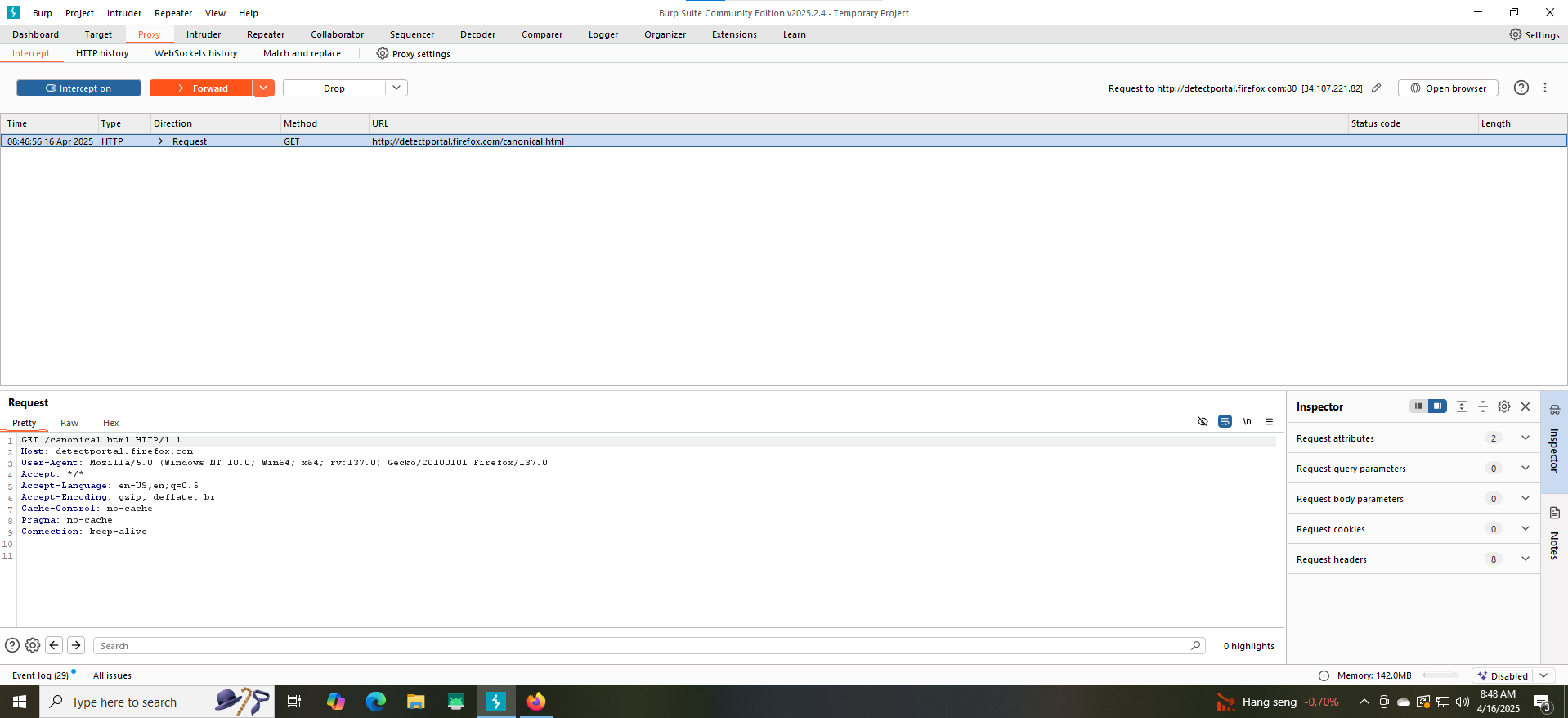
1. Bước 1: Cấu hình và khởi động Burpsuite như hướng dẫn ở phần trước
2. Bước 2: Trên cửa sổ công cụ Burpsuite, mở thẻ Proxy → Intercept và chắc chắn tính năng Intercept is on đã được bật
3. Bước 3: Mở địa chỉ trang Web cần kiểm thử. Ví dụ dưới đây là giao diện kiểm tra lỗ hổng SQL Injecion trên website https://demo.testfire.net/.

https://demo.testfire.net/

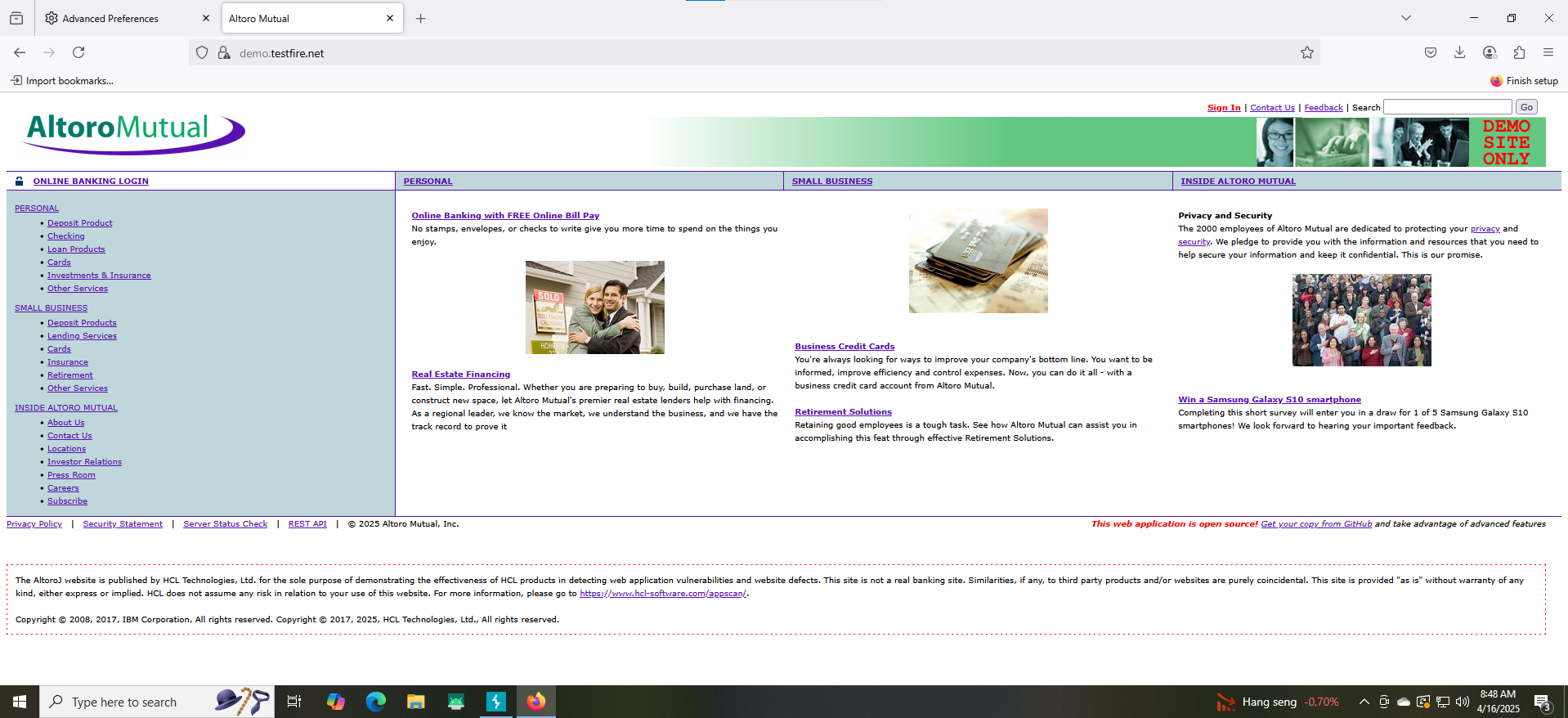
Bước 4: Điền các giá trị bất kỳ nào đó và gửi yêu cầu từ trình duyệt



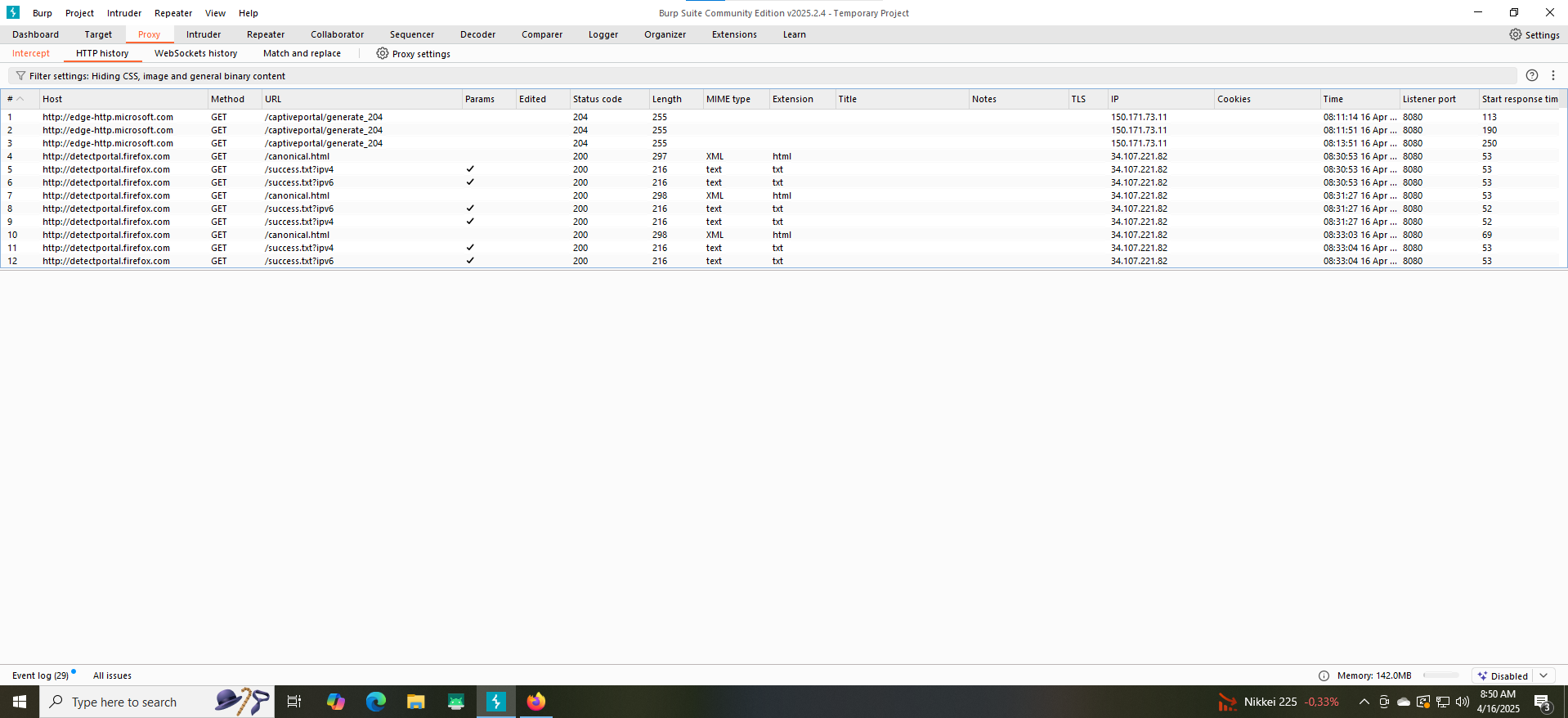
Bước 5: Trên thẻ Proxy → Intercept, nhấn nút Forward để chuyển tiếp yêu cầu

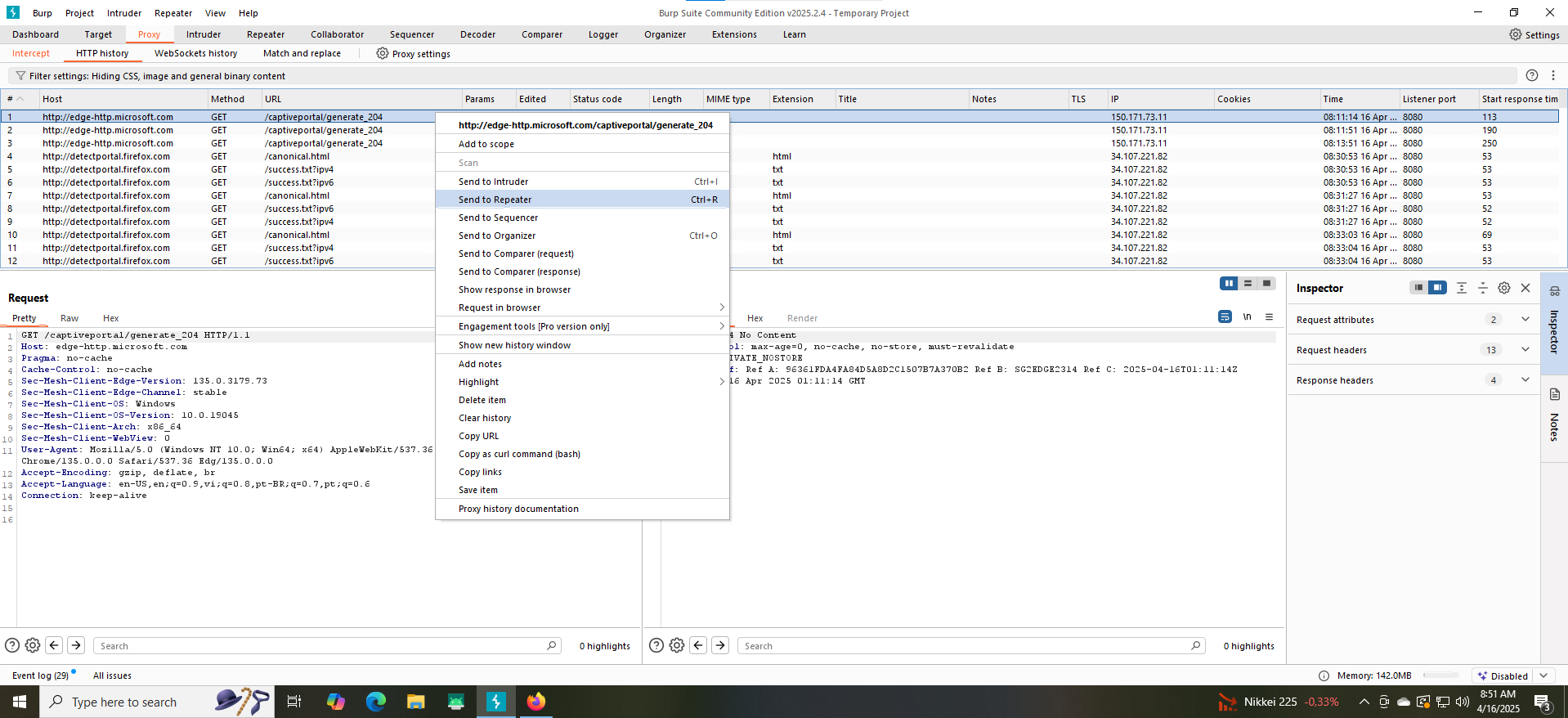


Sau khi chuyển tiếp, trang web từ đang load đã hiện lên.



Bước 6: Mở thẻ Proxy → HTTP history, chúng ta sẽ thấy danh sách các thông điệp HTTP mà Burpsuite đã bắt được. Chọn thông điệp HTTP Request tương ứng ở bước 4, nhấn chuột phải và chọn Send to Repeater





Bước 7: Chọn thẻ Repeater. Thẻ này cho phép chúng ta thay đổi nội dung của HTTP Request và phát lại tới máy chủ. Thẻ con Params liệt kê danh sách các giá trị trên HTTP Header có thể là tham số đầu vào.

